



GS3700 / XGS3700 Series

GbE L2+ Switch

Version 4.20
Edition 1, 1/2015

User's Guide

Default Login Details

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

IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

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

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

Related Documentation

- Fan Module Hardware Installation Guide
This guide shows how to install and remove the fan module in the Switch.
- Power Supply Module Hardware Installation Guide
This guide shows how to install and remove the power supply module in the Switch.
- Rack Mounting Hardware Installation Guide
This guide shows how to use the rack mounting kit to install the Switch in a rack.
- CLI Reference Guide
This guide explains how to use the Command-Line Interface (CLI) to configure the Switch.

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

- Web Configurator Online Help
Click the help icon in any screen for help in configuring that screen and supplementary information.

Contents Overview

User's Guide	18
Getting to Know Your Switch	19
Hardware Installation and Connection	24
Hardware Overview	28
The Web Configurator	35
Technical Reference	44
ZON Utility, ZON Neighbor Management and Port Status	45
Basic Setting	54
VLAN	94
Static MAC Forward Setup	117
Static Multicast Forward Setup	120
Filtering	123
Spanning Tree Protocol	125
Bandwidth Control	146
Broadcast Storm Control	149
Mirroring	151
Link Aggregation	163
Port Authentication	173
Port Security	182
Time Range	186
Classifier	188
Policy Rule	196
Queuing Method	202
VLAN Stacking	206
Multicast	214
AAA	241
IP Source Guard	254
Loop Guard	277
VLAN Mapping	281
Layer 2 Protocol Tunneling	285
sFlow	290
PPPoE	294
Error Disable	303
MAC Pinning	311
Private VLAN	314
Green Ethernet	318
Link Layer Discovery Protocol (LLDP)	321

Static Route	352
Policy Routing	356
Differentiated Services	360
DHCP	369
VRRP	384
Load Sharing	393
ARP Setup	395
Maintenance	401
Access Control	412
Diagnostic	435
Syslog	437
Cluster Management	440
MAC Table	446
IP Table	449
ARP Table	451
Routing Table	453
Path MTU Table	454
Configure Clone	455
Neighbor Table	458
Troubleshooting	460

Table of Contents

Contents Overview	3
Table of Contents	5
 Part I: User's Guide	 18
Chapter 1	
Getting to Know Your Switch.....	19
1.1 Introduction	19
1.1.1 Bridging Example	20
1.1.2 High Performance Switching Example	20
1.1.3 Gigabit Ethernet to the Desktop	21
1.1.4 IEEE 802.1Q VLAN Application Example	21
1.1.5 IPv6 Support	22
1.2 Ways to Manage the Switch	22
1.3 Good Habits for Managing the Switch	23
 Chapter 2	
Hardware Installation and Connection	24
2.1 Freestanding Installation	24
2.2 Mounting the Switch on a Rack	25
2.3 Installation Requirements	25
2.3.1 Precautions	25
2.4 Attaching the Brackets to the Switch	25
2.5 Mounting the Switch on a Rack	26
2.6 Power Module Installation	27
 Chapter 3	
Hardware Overview	28
3.1 Front Panel Connections	28
3.1.1 Ethernet Ports	29
3.1.2 SFP/SFP+ Slots	30
3.1.3 Management Port	31
3.1.4 Console Port	31
3.2 Rear Panel	32
3.2.1 Removing and Installing the Fan Module	32
3.2.2 Power Connection	32
3.3 LEDs	33

Chapter 4

The Web Configurator	35
4.1 Introduction	35
4.2 System Login	35
4.3 The Web Configurator Layout	36
4.3.1 Change Your Password	40
4.4 Saving Your Configuration	41
4.5 Switch Lockout	41
4.6 Resetting the Switch	41
4.6.1 Reload the Configuration File	41
4.7 Logging Out of the Web Configurator	42
4.8 Help	43

Part II: Technical Reference.....	44

Chapter 5

ZON Utility, ZON Neighbor Management and Port Status.....	45
5.1 Overview	45
5.2 ZyXEL One Network (ZON) Utility Screen	45
5.3 ZON Neighbor Management Screen	46
5.4 Status Summary	47
5.4.1 Port Status	48
5.4.2 Status: Port Details	50

Chapter 6

Basic Setting	54
6.1 System Information	54
6.1.1 System Information Stacking Hardware Monitor	56
6.2 General Setup	58
6.3 Introduction to VLANs	60
6.4 Switch Setup	60
6.5 IP Setup	62
6.5.1 IP Interfaces	62
6.6 Port Setup	64
6.7 PoE	67
6.7.1 PoE Setup	70
6.8 Interface Setup	73
6.9 IPv6	74
6.9.1 IPv6 Interface Status	74
6.9.2 IPv6 Configuration	77
6.9.3 IPv6 Global Setup	78

6.9.4 IPv6 Interface Setup	78
6.9.5 IPv6 Link-Local Address Setup	79
6.9.6 IPv6 Global Address Setup	80
6.9.7 IPv6 Neighbor Discovery Setup	81
6.9.8 IPv6 Router Discovery Setup	82
6.9.9 IPv6 Prefix Setup	84
6.9.10 IPv6 Neighbor Setup	85
6.9.11 DHCPv6 Client Setup	86
6.10 Stacking	88
6.10.1 Stacking Status	89
6.10.2 Stacking Slot	90
6.10.3 Stacking Configuration	91
Chapter 7	
VLAN	94
7.1 Introduction to IEEE 802.1Q Tagged VLANs	94
7.1.1 Forwarding Tagged and Untagged Frames	94
7.2 Automatic VLAN Registration	95
7.2.1 GARP	95
7.2.2 GVRP	95
7.3 Port VLAN Trunking	96
7.4 Select the VLAN Type	96
7.5 802.1Q Static VLAN	96
7.5.1 VLAN Status	97
7.5.2 VLAN Details	98
7.6 VLAN Configuration	99
7.6.1 Configure a Static VLAN or Private VLAN	99
7.6.2 Configure VLAN Port Settings	101
7.6.3 Subnet Based VLANs	103
7.6.4 Protocol Based VLANs	106
7.6.5 View Private VLAN Status	109
7.7 Port-based VLAN Setup (Standalone Mode)	109
7.7.1 Configure a Port-based VLAN	110
7.8 Voice VLAN	113
7.9 MAC-based VLAN	115
Chapter 8	
Static MAC Forward Setup.....	117
8.1 Overview	117
8.2 Configuring Static MAC Forwarding	117
Chapter 9	
Static Multicast Forward Setup	120

9.1 Static Multicast Forwarding Overview	120
9.2 Configuring Static Multicast Forwarding	121
Chapter 10	
Filtering.....	123
10.1 Configure a Filtering Rule	123
Chapter 11	
Spanning Tree Protocol.....	125
11.1 STP/RSTP Overview	125
11.1.1 STP Terminology	125
11.1.2 How STP Works	126
11.1.3 STP Port States	126
11.1.4 Multiple RSTP	126
11.1.5 Multiple STP	127
11.2 Spanning Tree Protocol Status Screen	129
11.3 Spanning Tree Configuration	130
11.4 Configure Rapid Spanning Tree Protocol	131
11.5 Rapid Spanning Tree Protocol Status	133
11.6 Configure Multiple Rapid Spanning Tree Protocol	134
11.7 Multiple Rapid Spanning Tree Protocol Status	137
11.8 Configure Multiple Spanning Tree Protocol	138
11.8.1 Multiple Spanning Tree Protocol Port Configuration	142
11.9 Multiple Spanning Tree Protocol Status	144
Chapter 12	
Bandwidth Control.....	146
12.1 Bandwidth Control Overview	146
12.1.1 CIR and PIR	146
12.2 Bandwidth Control Setup	146
Chapter 13	
Broadcast Storm Control	149
13.1 Broadcast Storm Control Setup	149
Chapter 14	
Mirroring	151
14.1 Port Mirroring	151
14.1.1 Local Port Mirroring	154
14.1.2 Remote Port Mirroring	155
14.1.3 Source	156
14.1.4 Destination	159
14.1.5 Connected Port	160

Chapter 15	
Link Aggregation	163
15.1 Link Aggregation Overview	163
15.2 Dynamic Link Aggregation	163
15.2.1 Link Aggregation ID	164
15.3 Link Aggregation Status	164
15.4 Link Aggregation Setting	165
15.5 Link Aggregation Control Protocol	168
15.6 Static Trunking Example	171
Chapter 16	
Port Authentication	173
16.1 Port Authentication Overview	173
16.1.1 IEEE 802.1x Authentication	173
16.1.2 MAC Authentication	174
16.2 Port Authentication Configuration	175
16.2.1 Activate IEEE 802.1x Security	175
16.2.2 Guest VLAN	177
16.2.3 Activate MAC Authentication	180
Chapter 17	
Port Security	182
17.1 About Port Security	182
17.2 Port Security Setup	182
17.3 VLAN MAC Address Limit	184
Chapter 18	
Time Range	186
18.1 About Time Range	186
18.2 Time Range Setup	186
Chapter 19	
Classifier	188
19.1 About the Classifier and QoS	188
19.2 Classifier Status	188
19.3 Classifier Configuration	189
19.4 Viewing and Editing Classifier Configuration	192
19.4.1 Classifier Global Setting Configuration	194
19.5 Classifier Example	194
Chapter 20	
Policy Rule	196
20.1 Policy Rules Overview	196

20.1.1 DiffServ	196
20.1.2 DSCP and Per-Hop Behavior	196
20.2 Configuring Policy Rules	196
20.2.1 Viewing and Editing Policy Configuration	199
20.3 Policy Example	200
Chapter 21	
Queuing Method	202
21.1 Queuing Method Overview	202
21.1.1 Strictly Priority	202
21.1.2 Weighted Fair Queuing	202
21.1.3 Weighted Round Robin Scheduling (WRR)	203
21.2 Configuring Queuing	203
Chapter 22	
VLAN Stacking	206
22.1 VLAN Stacking Overview	206
22.1.1 VLAN Stacking Example	206
22.2 VLAN Stacking Port Roles	207
22.3 VLAN Tag Format	207
22.3.1 Frame Format	208
22.4 Configuring VLAN Stacking	208
22.4.1 Port-based Q-in-Q	210
22.4.2 Selective Q-in-Q	212
Chapter 23	
Multicast	214
23.1 Multicast Overview	214
23.1.1 IP Multicast Addresses	214
23.1.2 IGMP Filtering	214
23.1.3 IGMP Snooping	215
23.1.4 IGMP Snooping and VLANs	215
23.1.5 MLD Snooping-Proxy	215
23.1.6 MLD Messages	216
23.2 Multicast Setup	216
23.3 IPv4 Multicast Status	217
23.3.1 IGMP Snooping	217
23.3.2 IGMP Snooping VLAN	221
23.3.3 IGMP Filtering Profile	223
23.4 IPv6 Multicast Status	224
23.4.1 MLD Snooping-proxy	225
23.4.2 MLD Snooping-proxy VLAN	225
23.4.3 MLD Snooping-proxy VLAN Port Role Setting	227

23.4.4 MLD Snooping-proxy Filtering	229
23.4.5 MLD Snooping-proxy Filtering Profile	231
23.5 MVR Overview	232
23.5.1 Types of MVR Ports	233
23.5.2 MVR Modes	233
23.5.3 How MVR Works	233
23.6 General MVR Configuration	234
23.6.1 MVR Group Configuration	237
23.6.2 MVR Configuration Example	239
Chapter 24	
AAA	241
24.1 Authentication, Authorization and Accounting (AAA)	241
24.1.1 Local User Accounts	241
24.1.2 RADIUS and TACACS+	242
24.2 AAA Screens	242
24.2.1 RADIUS Server Setup	242
24.2.2 TACACS+ Server Setup	244
24.2.3 AAA Setup	246
24.2.4 Vendor Specific Attribute	249
24.2.5 Tunnel Protocol Attribute	250
24.3 Supported RADIUS Attributes	250
24.3.1 Attributes Used for Authentication	251
24.3.2 Attributes Used for Accounting	251
Chapter 25	
IP Source Guard.....	254
25.1 IP Source Guard Overview	254
25.1.1 DHCP Snooping Overview	254
25.1.2 ARP Inspection Overview	256
25.2 IP Source Guard	258
25.3 IP Source Guard Static Binding	258
25.4 DHCP Snooping	261
25.5 DHCP Snooping Configure	264
25.5.1 DHCP Snooping Port Configure	266
25.5.2 DHCP Snooping VLAN Configure	267
25.5.3	268
25.6 ARP Inspection Status	270
25.6.1 ARP Inspection VLAN Status	270
25.6.2 ARP Inspection Log Status	271
25.7 ARP Inspection Configure	273
25.7.1 ARP Inspection Port Configure	274
25.7.2 ARP Inspection VLAN Configure	276

Chapter 26	
Loop Guard	277
26.1 Loop Guard Overview	277
26.2 Loop Guard Setup	279
Chapter 27	
VLAN Mapping	281
27.1 VLAN Mapping Overview	281
27.1.1 VLAN Mapping Example	281
27.2 Enabling VLAN Mapping	281
27.3 Configuring VLAN Mapping	283
Chapter 28	
Layer 2 Protocol Tunneling.....	285
28.1 Layer 2 Protocol Tunneling Overview	285
28.1.1 Layer-2 Protocol Tunneling Mode	286
28.2 Configuring Layer 2 Protocol Tunneling	286
Chapter 29	
sFlow.....	290
29.1 sFlow Overview	290
29.2 sFlow Port Configuration	290
29.2.1 sFlow Collector Configuration	292
Chapter 30	
PPPoE	294
30.1 PPPoE Intermediate Agent Overview	294
30.1.1 PPPoE Intermediate Agent Tag Format	294
30.1.2 Sub-Option Format	294
30.1.3 Port State	295
30.2 The PPPoE Screen	296
30.3 PPPoE Intermediate Agent	296
30.3.1 PPPoE IA Per-Port	298
30.3.2 PPPoE IA Per-Port Per-VLAN	300
30.3.3 PPPoE IA for VLAN	301
Chapter 31	
Error Disable	303
31.1 CPU Protection Overview	303
31.2 Error-Disable Recovery Overview	303
31.3 The Error Disable Screen	303
31.4 Error-Disable Status	304
31.5 CPU Protection Configuration	306

31.6 Error-Disable Detect Configuration	308
31.7 Error-Disable Recovery Configuration	309
Chapter 32	
MAC Pinning	311
32.1 MAC Pinning Overview	311
32.2 MAC Pinning Configuration	311
Chapter 33	
Private VLAN	314
33.1 Private VLAN Overview	314
33.1.1 Configuration	316
Chapter 34	
Green Ethernet	318
34.1 Green Ethernet Overview	318
34.2 Configuring Green Ethernet	318
Chapter 35	
Link Layer Discovery Protocol (LLDP)	321
35.1 LLDP Overview	321
35.2 LLDP-MED Overview	322
35.3 LLDP Screens	323
35.4 LLDP Local Status	324
35.4.1 LLDP Local Port Status Detail	327
35.5 LLDP Remote Status	331
35.5.1 LLDP Remote Port Status Detail	332
35.6 LLDP Configuration	338
35.6.1 LLDP Configuration Basic TLV Setting	341
35.6.2 LLDP Configuration Basic Org-specific TLV Setting	342
35.7 LLDP-MED Configuration	344
35.8 LLDP-MED Network Policy	346
35.9 LLDP-MED Location	348
Chapter 36	
Static Route	352
36.1 Static Routing Overview	352
36.2 Static Routing	352
36.3 Configuring IPv4 Static Routing	353
36.4 Configuring IPv6 Static Routing	354
Chapter 37	
Policy Routing	356

37.1 Policy Route Overview	356
37.1.1 Benefits	356
37.2 Configuring Policy Routing Profile	356
37.2.1 Policy Routing Rule Configuration	357
Chapter 38	
Differentiated Services	360
38.1 DiffServ Overview	360
38.1.1 DSCP and Per-Hop Behavior	360
38.1.2 DiffServ Network Example	360
38.2 Two Rate Three Color Marker Traffic Policing	361
38.2.1 TRTCM - Color-blind Mode	362
38.2.2 TRTCM - Color-aware Mode	362
38.3 Activating DiffServ	362
38.3.1 Configuring 2-Rate 3 Color Marker Settings	364
38.3.2 DSCP Profile	366
38.4 DSCP-to-IEEE 802.1p Priority Settings	367
38.4.1 Configuring DSCP Settings	367
Chapter 39	
DHCP	369
39.1 DHCP Overview	369
39.1.1 DHCP Modes	369
39.1.2 DHCP Configuration Options	369
39.2 DHCP Configuration	369
39.3 DHCPv4 Status	370
39.3.1 DHCPv4 Server Status Detail	370
39.4 DHCPv4 Relay	371
39.4.1 DHCPv4 Relay Agent Information	372
39.4.2 DHCPv4 Option 82 Profile	372
39.4.3 Configuring DHCPv4 Global Relay	374
39.4.4 DHCPv4 Global Relay Port Configure	375
39.4.5 Global DHCP Relay Configuration Example	376
39.5 Configuring DHCP VLAN Settings	377
39.5.1 DHCPv4 VLAN Port Configure	379
39.5.2 Example: DHCP Relay for Two VLANs	380
39.6 DHCPv6 Relay	381
Chapter 40	
VRRP	384
40.1 VRRP Overview	384
40.2 VRRP Status	385
40.3 VRRP Configuration	385

40.3.1 IP Interface Setup	385
40.3.2 VRRP Parameters	387
40.3.3 Configuring VRRP Parameters	387
40.3.4 Viewing VRRP Summary	389
40.4 VRRP Configuration Examples	389
40.4.1 One Subnet Network Example	389
40.4.2 Two Subnets Example	391
Chapter 41	
Load Sharing	393
41.1 Load Sharing Overview	393
41.2 Configuring Load Sharing	393
Chapter 42	
ARP Setup	395
42.1 ARP Overview	395
42.1.1 How ARP Works	395
42.1.2 ARP Learning Mode	395
42.2 ARP Setup	397
42.2.1 ARP Learning	397
42.2.2 Static ARP	399
Chapter 43	
Maintenance	401
43.1 The Maintenance Screen	401
43.2 Firmware Upgrade	402
43.3 Restore a Configuration File	404
43.4 Backup a Configuration File	405
43.5 Erase Running-Configuration	405
43.6 Save Configuration	406
43.7 Reboot System	406
43.7.1 Load Stacking Default	406
43.7.2 Load Factory Default	407
43.8 Tech-Support	407
43.9 FTP Command Line	409
43.9.1 Filename Conventions	409
43.9.2 FTP Command Line Procedure	410
43.9.3 GUI-based FTP Clients	410
43.9.4 FTP Restrictions	411
Chapter 44	
Access Control	412
44.1 Access Control Overview	412

44.2 The Access Control Main Screen	412
44.3 About SNMP	412
44.3.1 SNMP v3 and Security	413
44.3.2 Supported MIBs	414
44.3.3 SNMP Traps	414
44.3.4 Configuring SNMP	418
44.3.5 Configuring SNMP Trap Group	420
44.3.6 Enabling/Disabling Sending of SNMP Traps on a Port	421
44.3.7 Configuring SNMP User	422
44.4 Setting Up Login Accounts	424
44.5 SSH Overview	425
44.6 How SSH works	426
44.7 SSH Implementation on the Switch	427
44.7.1 Requirements for Using SSH	427
44.8 Introduction to HTTPS	427
44.9 HTTPS Example	428
44.9.1 Internet Explorer Warning Messages	428
44.9.2 Mozilla Firefox Warning Messages	430
44.9.3 The Main Screen	431
44.10 Service Access Control	432
44.11 Remote Management	433
 Chapter 45	
Diagnostic	435
45.1 Diagnostic	435
 Chapter 46	
Syslog	437
46.1 Syslog Overview	437
46.2 Syslog Setup	437
46.3 Syslog Server Setup	438
 Chapter 47	
Cluster Management	440
47.1 Clustering Management Status Overview	440
47.2 Cluster Management Status	441
47.2.1 Cluster Member Switch Management	442
47.3 Clustering Management Configuration	444
 Chapter 48	
MAC Table	446
48.1 MAC Table Overview	446
48.2 Viewing the MAC Table	447

Chapter 49	
IP Table	449
49.1 IP Table Overview	449
49.2 Viewing the IP Table	450
Chapter 50	
ARP Table	451
50.1 ARP Table Overview	451
50.1.1 How ARP Works	451
50.2 The ARP Table Screen	451
Chapter 51	
Routing Table	453
51.1 Overview	453
51.2 Viewing the Routing Table Status	453
Chapter 52	
Path MTU Table	454
52.1 Path MTU Overview	454
52.2 Viewing the Path MTU Table	454
Chapter 53	
Configure Clone	455
53.1 Configure Clone	455
Chapter 54	
Neighbor Table	458
54.1 IPv6 Neighbor Table Overview	458
54.2 Viewing the IPv6 Neighbor Table	458
Chapter 55	
Troubleshooting	460
55.1 Power, Hardware Connections, and LEDs	460
55.2 Switch Access and Login	461
55.3 Switch Configuration	463
Appendix A Common Services	464
Appendix B IPv6	467
Appendix C Customer Support	476
Appendix D Legal Information	482
Index	487

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

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

Table 1 Switch Comparison Table

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

With its built-in web configurator, including the ZyXEL One Network (ZON) Neighbor Management feature ([Section 5.3 on page 46](#)), viewing, managing and configuring the Switch and its neighboring devices is easy. In addition, the Switch can also be managed via Telnet, any terminal emulator program on the console port, or third-party SNMP management.

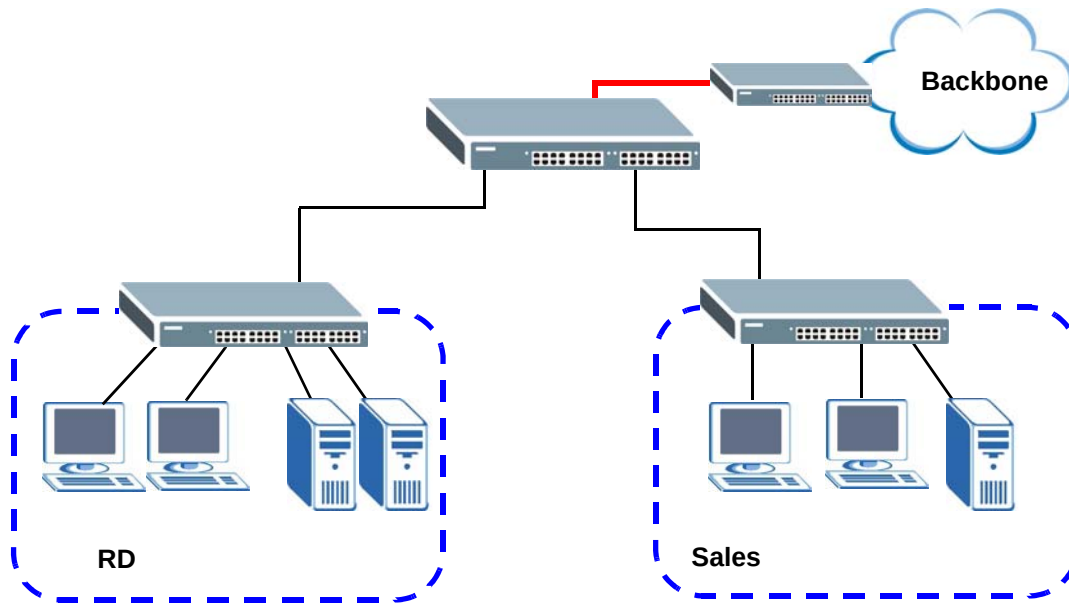
In addition, ZyXEL offers a proprietary software program called ZyXEL One Network (ZON) Utility, it is a utility tool that assists you to set up and maintain network devices in a more simple and efficient way. You can download the ZON Utility at www.zyxel.com and install it on a PC. For more information on ZON Utility see [Section 5.2 on page 45](#).

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

1.1.1 Bridging Example

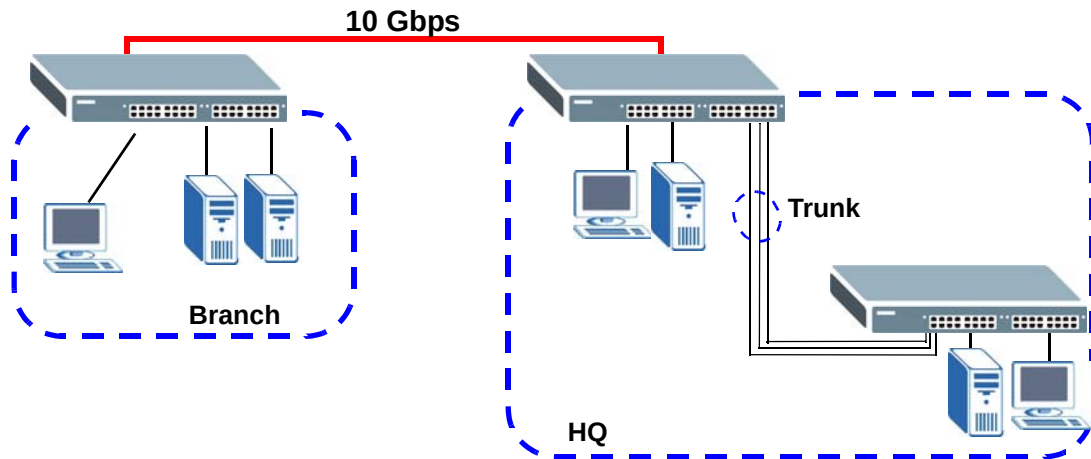
In this example the Switch connects different company departments (**RD** and **Sales**) to the corporate backbone. It can alleviate bandwidth contention and eliminate server and network bottlenecks. All users that need high bandwidth can connect to high-speed department servers via the Switch. You can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

Figure 1 Bridging Application



1.1.2 High Performance Switching Example

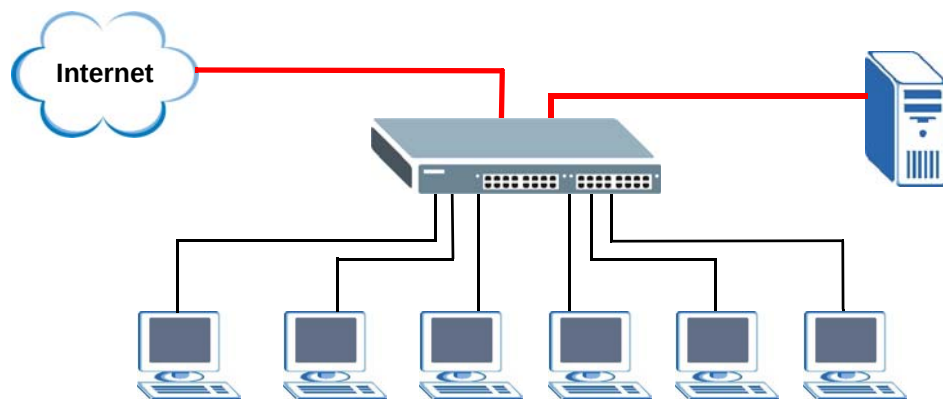
The Switch is ideal for connecting two geographically dispersed networks that need high bandwidth. In the following example, a company uses the optional 10 Gigabit uplink modules to connect the headquarters to a branch office network. Within the headquarters network, a company can use trunking to group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

Figure 2 High Performance Switching

1.1.3 Gigabit Ethernet to the Desktop

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

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

Figure 3 Gigabit to the Desktop

1.1.4 IEEE 802.1Q VLAN Application Example

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

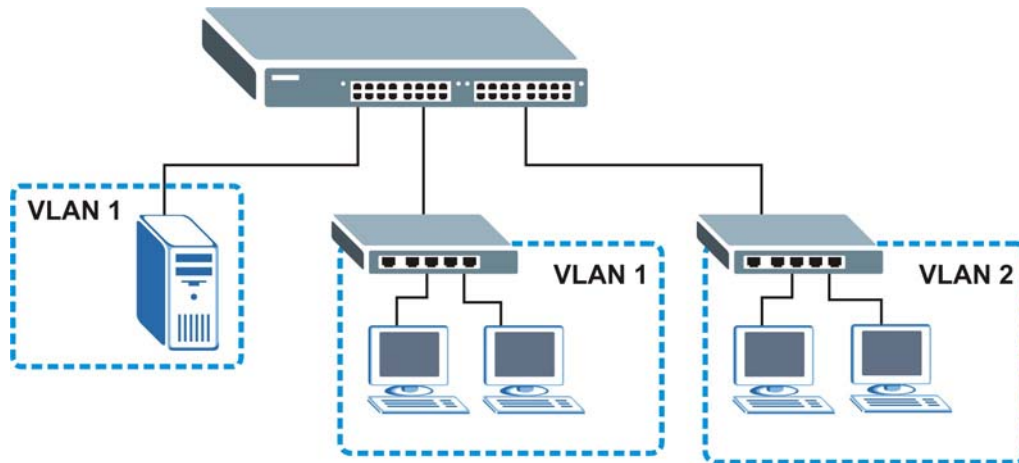
For more information on VLANs, refer to [Chapter 7 on page 94](#).

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 [Appendix B on page 467](#) and the CLI Reference Guide.

1.2 Ways to Manage the Switch

Use any of the following methods to manage the Switch.

- Web Configurator. This is recommended for everyday management of the Switch using a (supported) web browser. See [Chapter 4 on page 35](#).
- 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 43.9 on page 409](#).
- SNMP. The device can be monitored and/or managed by an SNMP manager. See [Section 44.3 on page 412](#).

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.

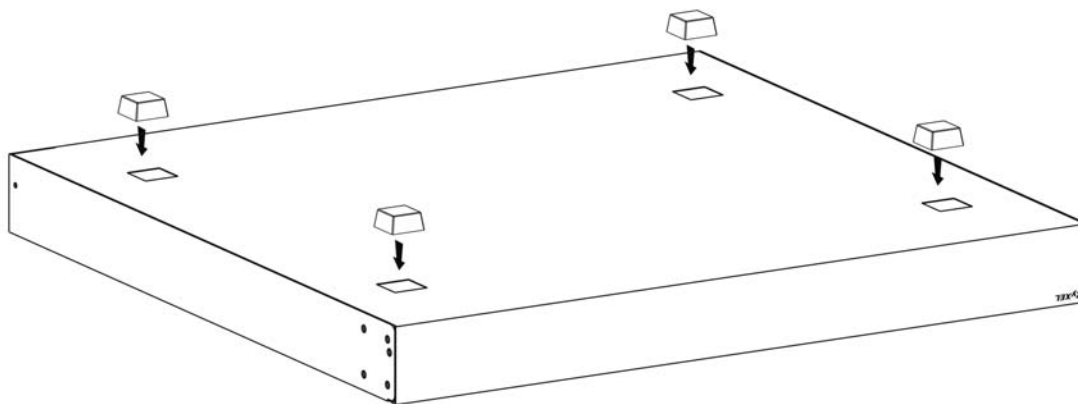
Hardware Installation and Connection

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 of how to mount the Switch in a 19-inch rack with the included rack mounting kit.

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

2.3 Installation Requirements

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

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

2.3.1 Precautions

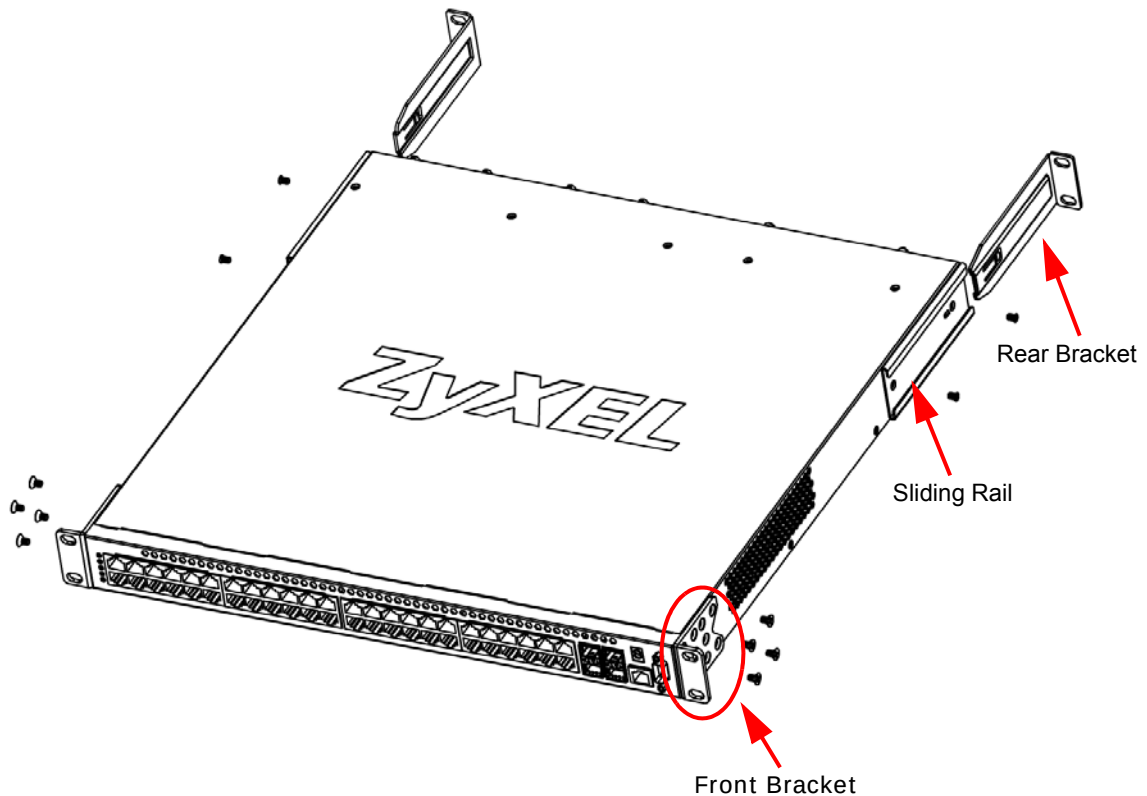
- Make sure the rack will safely support the combined weight of all the equipment it contains. The maximum weight a bracket can hold is 27 Kg.
- Make sure the position of the Switch does not make the rack unstable or top-heavy. Take all necessary precautions to anchor the rack securely before installing the unit.

2.4 Attaching the Brackets to the Switch

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

- 1 Position the smaller front mounting bracket on one side of the Switch, lining up the four screw holes on the bracket with the screw holes on the side of the Switch.
- 2 Use a #2 Philips screwdriver to install the M4 screws with large heads through the mounting bracket holes into the Switch.
- 3 Repeat steps 1 and 2 to install the second front mounting bracket on the other side of the Switch.
- 4 Position a sliding rail on one side at the rear of the Switch, lining up the two screw holes on the sliding rail with the screw holes on the side of the Switch.
- 5 Use a screwdriver to install the M4 screws with small heads through the sliding rail holes into the Switch.
- 6 Repeat steps 1 and 2 to install the second sliding rail on the other side of the Switch.

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

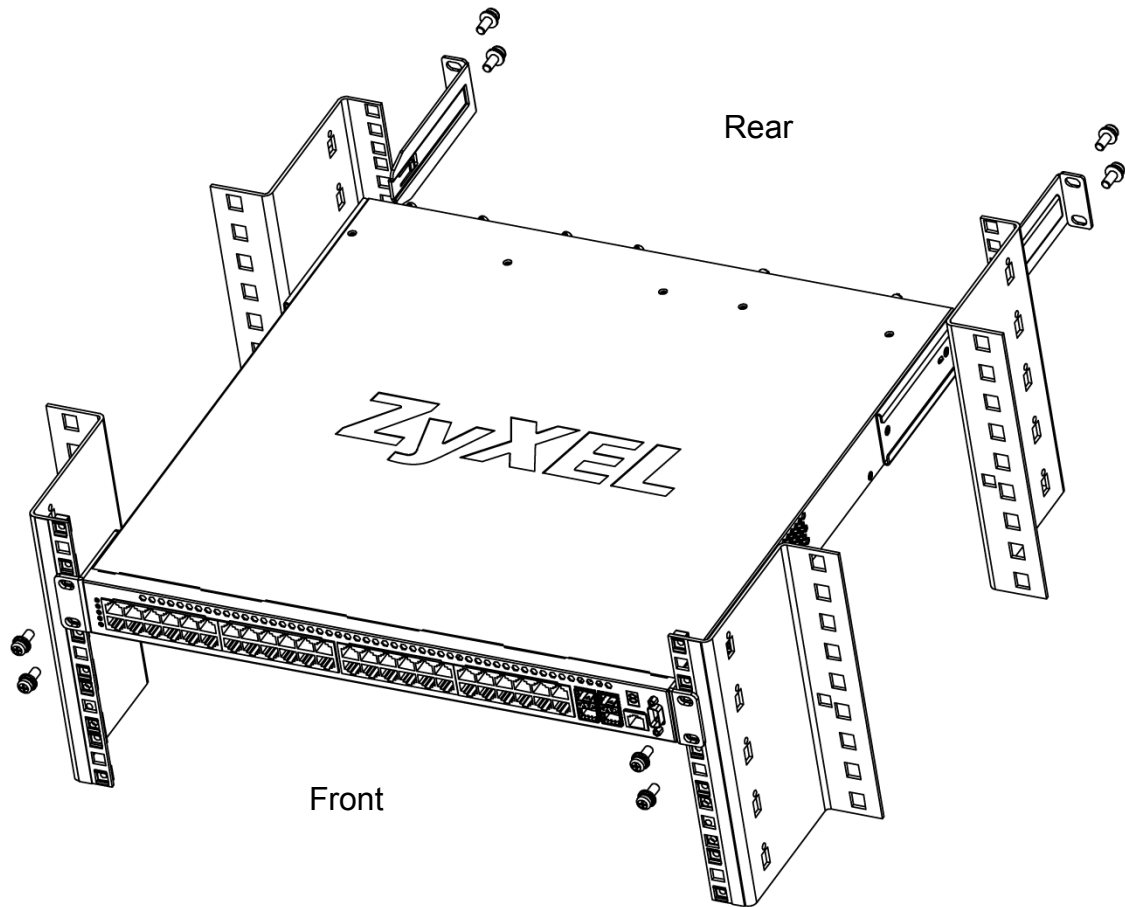


You may now mount the Switch on a rack. Proceed to the next section.

2.5 Mounting the Switch on a Rack

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

- 1 Position a front mounting bracket (that is already attached to the Switch) on one side of the rack, lining up the two screw holes on the bracket with the screw holes at the front of the rack.
- 2 Use a screwdriver to install the rack screws through the mounting bracket holes into the rack.
- 3 Repeat steps 1 and 2 to attach the other front mounting bracket on the other side of the rack.
- 4 Position a rear mounting bracket (that is already attached to the Switch) on one side of the rack, lining up the two screw holes on the bracket with the screw holes at the rear of the rack.
- 5 Use a screwdriver to install the rack screws through the mounting bracket holes into the rack.
- 6 Repeat steps 4 and 5 to attach the other rear mounting bracket on the other side of the rack.



2.6 Power Module Installation

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

Hardware Overview

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

3.1 Front Panel Connections

The figure below shows the front panel of the Switch.

Figure 6 Front Panel: GS3700 Series

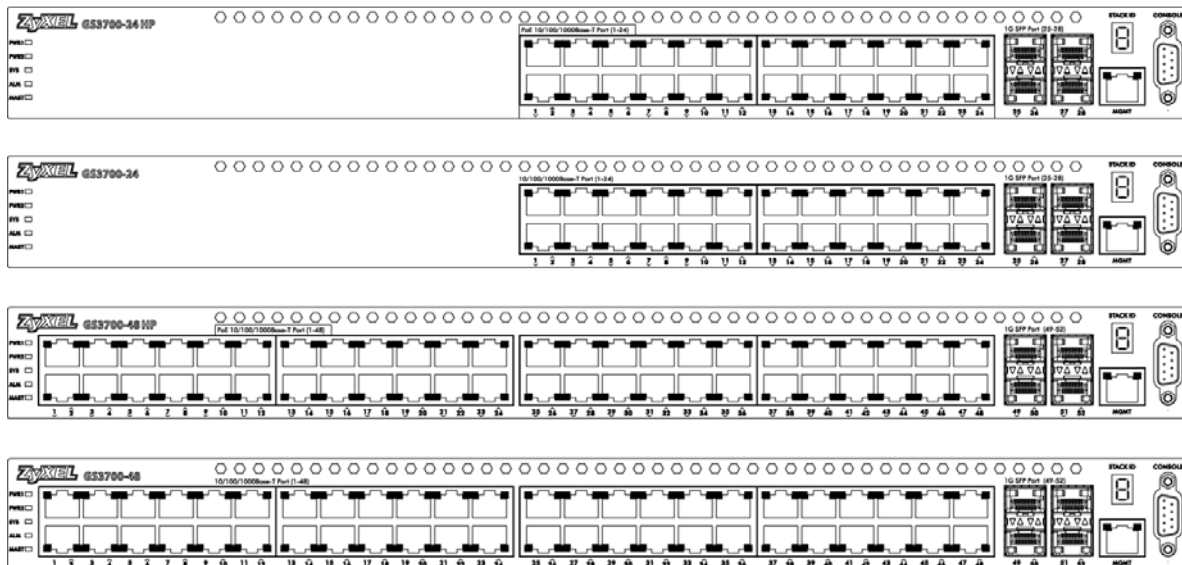
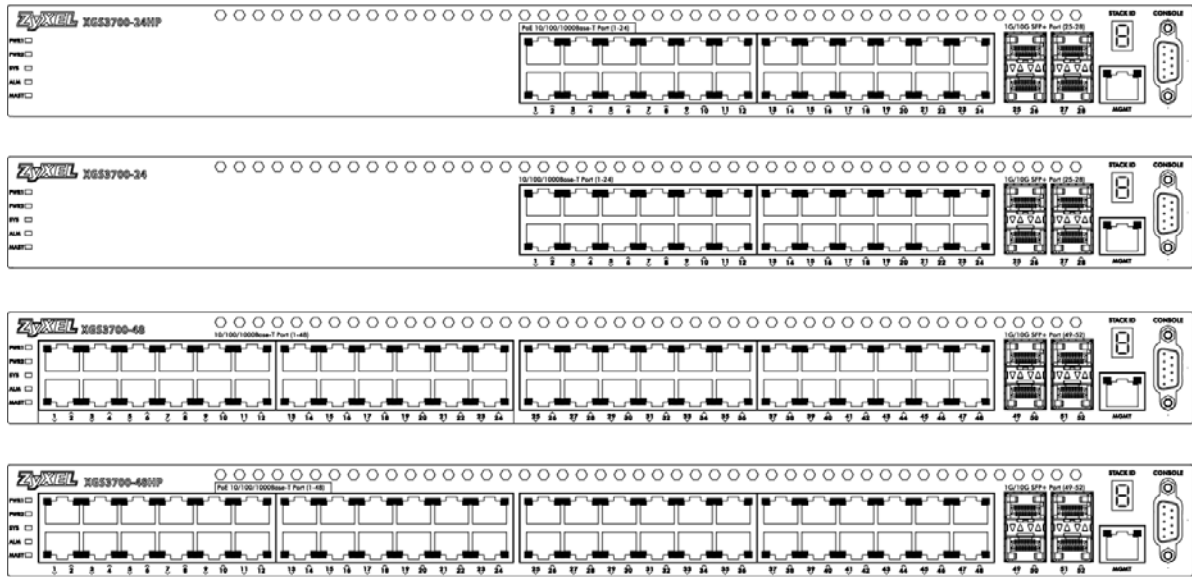


Figure 7 Front Panel: XGS3700 Series

The following table describes the ports.

Table 2 Panel Connections

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

3.1.1 Ethernet Ports

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

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

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

3.1.1.1 Default Ethernet Settings

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

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

3.1.2 SFP/SFP+ Slots

These are four slots for Small Form-Factor Pluggable (SFP) or SFP+ modules, such as an SFP/SFP+ transceiver. The SFP+ (SFP Plus) is an enhanced version of the SFP and supports data rates of 10 Gbps. A transceiver is a single unit that houses a transmitter and a receiver. Use a transceiver to connect a fiber-optic cable to the Switch. The Switch does not come with transceivers. You must use transceivers that comply with the Small Form-Factor Pluggable (SFP) Transceiver MultiSource Agreement (MSA). See the SFF committee's INF-8074i specification Rev 1.0 for details.

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

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

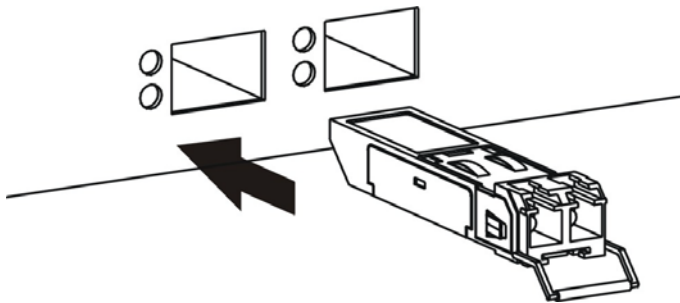
To avoid possible eye injury, do not look into an operating fiber-optic module's connectors.

3.1.2.1 Transceiver Installation

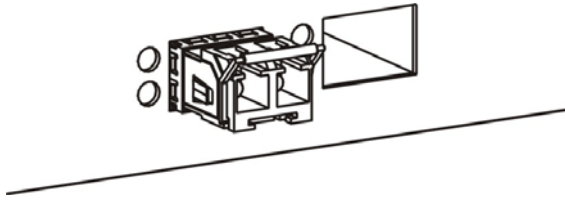
Use the following steps to install a transceiver.

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

Figure 8 Transceiver Installation Example



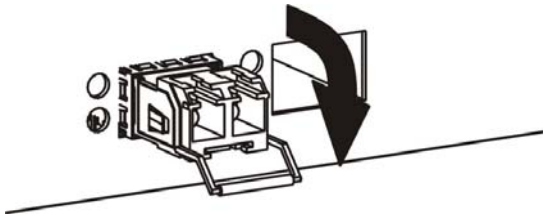
- 2 Press the transceiver firmly until it clicks into place.
- 3 The Switch automatically detects the installed transceiver. Check the LEDs to verify that it is functioning properly.

Figure 9 Installed Transceiver

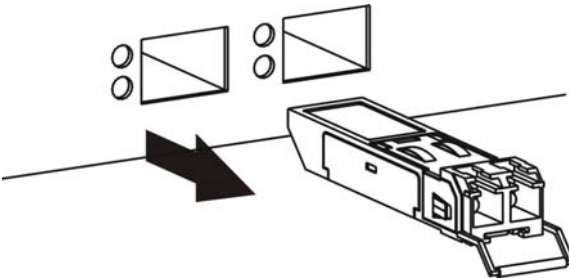
3.1.2.2 Transceiver Removal

Use the following steps to remove a transceiver.

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

Figure 10 Opening the Transceiver's Latch Example

- 2 Pull the transceiver out of the slot.

Figure 11 Transceiver Removal Example

3.1.3 Management Port

The 100Base-T Ethernet **MGMT** (management) port is used for local management. Connect directly to this port using an Ethernet cable. You can configure the Switch via Telnet or the web configurator.

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

3.1.4 Console Port

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

- VT100 terminal emulation
- 9600 bps

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

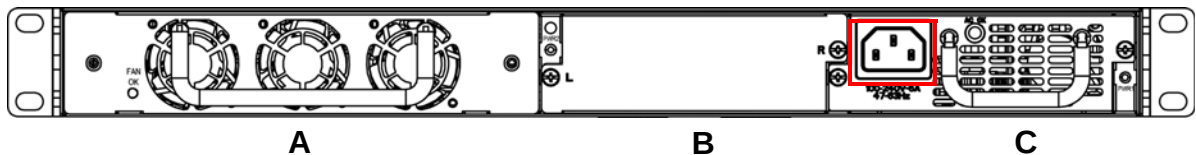
Connect the male 9-pin end of the RS-232 console cable to the console port of the Switch. Connect the female end to a serial port (COM1, COM2 or other COM port) of your computer.

3.2 Rear Panel

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

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

Figure 12 Rear Panel



3.2.1 Removing and Installing the Fan Module

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

3.2.2 Power Connection

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

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

Connecting the Power

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

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

- 1 Connect the female end of the power cord to the AC power socket.
- 2 Connect the other end of the cord to a power outlet.

Disconnecting the Power

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

- 1 Disconnect the power cord from the power outlet.
- 2 Disconnect the power cord from the AC power socket.

3.3 LEDs

The following table describes the LEDs.

Table 3 LEDs

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

Table 3 LEDs (continued)

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

The Web Configurator

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

4.1 Introduction

The web configurator is an HTML-based management interface that allows easy Switch setup and management via Internet browser. Supported browsers at the time of writing are:

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

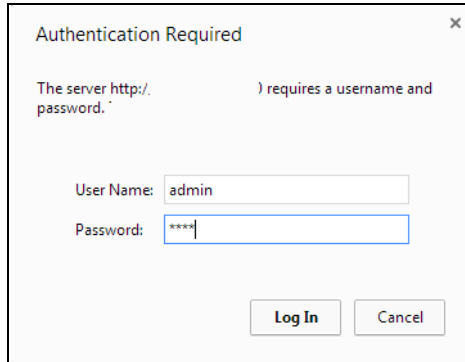
The recommended screen resolution is 1024 by 768 pixels. In order to use the web configurator you need to allow:

- Web browser pop-up windows from your device. Web pop-up blocking is enabled by default in some browsers.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

4.2 System Login

- 1 Start your web browser.
- 2 Type "http://" and the IP address of the Switch (for example, the default management IP address is 192.168.1.1 through an in-band (non-**MGMT**) port and 192.168.0.1 through the **MGMT** port) in the Location or Address field. Press [ENTER].
- 3 The login screen appears. The default username is **admin** and associated default password is **1234**. The date and time display as shown if you have not configured a time server nor manually entered a time and date in the **General Setup** screen.

Figure 13 Web Configurator: Login



Authentication Required

The server http://.) requires a username and password.

User Name:

Password:

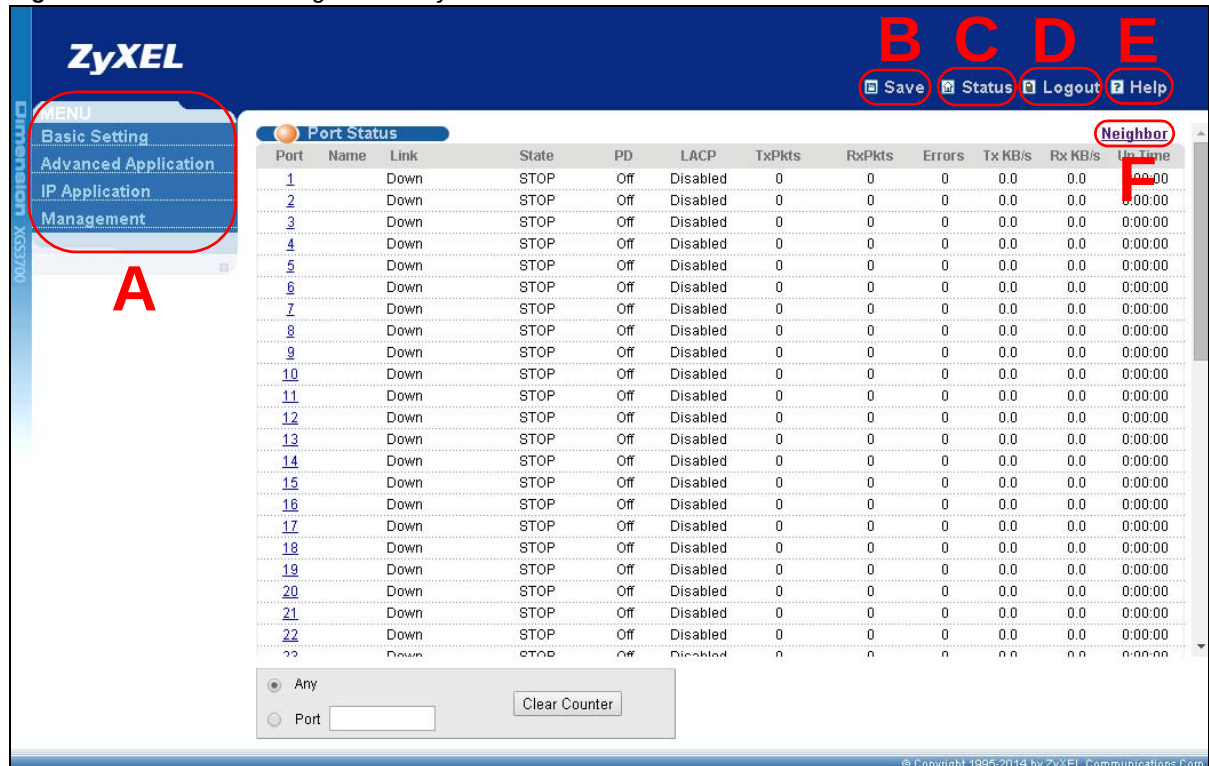
- Click **OK** to view the first web configurator screen.

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 GS3700-48HP screens as an example. The screens may vary slightly for different models.

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

Figure 14 The Web Configurator Layout



The screenshot shows the ZyXEL web configurator interface. The top navigation bar includes buttons for **Save**, **Status**, **Logout**, and **Help**. The left sidebar contains a **MENU** with options: **Basic Setting**, **Advanced Application**, **IP Application**, and **Management**. The main content area displays the **Port Status** table, which lists 24 ports with columns for Port, Name, Link, State, PD, LACP, TxPkts, RxPkts, Errors, Tx KB/s, Rx KB/s, and Up Time. A **Neighbor** button is located at the top right of the table. At the bottom, there are radio buttons for **Any** and **Port**, and a **Clear Counter** button.

Port	Name	Link	State	PD	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Time
1		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
2		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
3		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
4		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
5		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
6		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
7		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
8		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
9		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
10		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
11		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
12		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
13		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
14		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
15		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
16		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
17		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
18		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
19		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
20		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
21		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
22		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
23		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
24		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00

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 43.6 on page 406](#) for information on saving your settings to a specific configuration file.

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

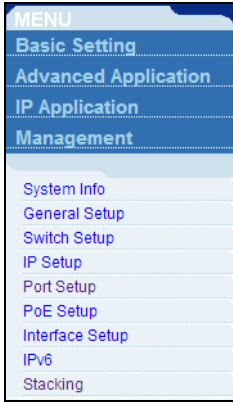
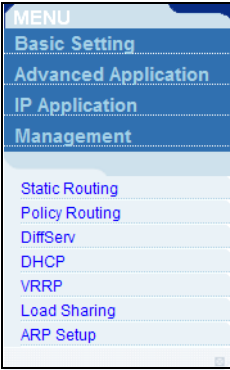
D - Click this link to log out of the web configurator.

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

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

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

Table 4 Navigation Panel Sub-links Overview

BASIC SETTING	ADVANCED APPLICATION	IP APPLICATION	MANAGEMENT
			

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.
PoE Setup	This link takes you to a screen where you can configure the Switch to supply power over Ethernet.
Interface Setup	This link takes you to a screen where you can create IPv6 interfaces on the Switch.
IPv6	This link takes you to a screen where you can enable an IPv6 interface and configure the IPv6 settings on the Switch.
Stacking	This link takes you to a screen where you can view and configure stacking system for the Switch.
Advanced Application	
VLAN	This link takes you to screens where you can configure port-based or 802.1Q VLAN (depending on what you configured in the Switch Setup menu). You can also configure a protocol based VLAN or a subnet based VLAN in these screens.
Static MAC Forwarding	This link takes you to screens where you can configure static MAC addresses for a port. These static MAC addresses do not age out.
Static Multicast Forwarding	This link takes you to a screen where you can configure static multicast MAC addresses for port(s). These static multicast MAC addresses do not age out.
Filtering	This link takes you to a screen to set up filtering rules.
Spanning Tree Protocol	This link takes you to screens where you can configure the RSTP/MRSTP/MSTP to prevent network loops.
Bandwidth Control	This link takes you to screens where you can cap the maximum bandwidth allowed on a port.
Broadcast Storm Control	This link takes you to a screen to set up broadcast filters.
Mirroring	This link takes you to screens where you can copy traffic from one port or ports to another port in order that you can examine the traffic from the first port without interference.
Link Aggregation	This link takes you to screen where you can logically aggregate physical links to form one logical, higher-bandwidth link.
Port Authentication	This link takes you to a screen where you can configure IEEE 802.1x port authentication as well as MAC authentication for clients communicating via the Switch.
Port Security	This link takes you to a screen where you can activate MAC address learning and set the maximum number of MAC addresses to learn on a port.
Time Range	This link takes you to a screen where you can configure time range for time-oriented features like Classifier.
Classifier	This link takes you to a screen where you can configure the Switch to group packets based on the specified criteria.

Table 5 Navigation Panel Links (continued)

LINK	DESCRIPTION
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.
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.
MAC Pinning	This link takes you to a screen where you can set specific ports to have priority over other ports in MAC address learning.
Private VLAN	This link takes you to a screen where you can block traffic between ports in a VLAN on the Switch.
Green Ethernet	This link takes you to a screen where you can configure the Switch to reduce port power consumption.
LLDP	This link takes you to a screen where you can configure LLDP settings.
IP Application	
Static Routing	This link takes you to a screen where you can configure static routes. A static route defines how the Switch should forward traffic by configuring the TCP/IP parameters manually.
Policy Routing	This link takes you to screens where you can configure policy routing rules.
DiffServ	This link takes you to screens where you can enable DiffServ, configure marking rules and set DSCP-to-IEEE802.1p mappings.
DHCP	This link takes you to screens where you can configure the DHCP settings.
VRRP	This link takes you to screens where you can configure redundant virtual router for your network.
Load Sharing	This link takes you to a screen where you can enable Equal-Cost MultiPath (ECMP) routing and set the criteria the Switch uses to determine the routing path for a packet.
ARP Setup	This link takes you to a screen where you can configure ARP learning mode on a per-port basis and create static ARP entries which do not age out.
Management	
Maintenance	This link takes you to screens where you can perform firmware and configuration file maintenance as well as reboot the system.

Table 5 Navigation Panel Links (continued)

LINK	DESCRIPTION
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).
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.
Path MTU Table	This link takes you to a screen where you can view the IPv6 path MTU table.
Configure Clone	This link takes you to a screen where you can copy attributes of one port to (an)other port(s).
Neighbor Table	This link takes you to a screen where you can view the Switch's IPv6 neighbor table.

4.3.1 Change Your Password

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

Figure 15 Change Administrator Login Password

The screenshot shows the 'Logins' page with a navigation bar at the top containing 'Logins' (selected) and 'Access Control'. Below the navigation bar, the 'Administrator' section is highlighted with a red box. It contains three input fields: 'Old Password', 'New Password', and 'Retype to confirm'. Below these fields is a red warning message: 'Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.' At the bottom of the page, there is an 'Edit Logins' section with a table for managing other login accounts. The table has columns for 'Login', 'User Name', 'Password', 'Retype to confirm', and 'Privilege'. There are four rows of input fields for these accounts. At the very bottom, there are 'Apply' and 'Cancel' buttons.

Login	User Name	Password	Retype to confirm	Privilege
1				
2				
3				
4				

Apply Cancel

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

Figure 16 Resetting the Switch: Via the Console Port

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

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

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



4.8 Help

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

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

PART II

Technical Reference

ZON Utility, ZON Neighbor Management and Port Status

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

5.1 Overview

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

5.2 ZyXEL One Network (ZON) Utility Screen

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

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

The following figure shows the ZON Utility screen.

Figure 18 ZON Utility Screen



Type	Model	FW Version	MAC	IP	Sys Name	Location	Last Status
☐	GS2210-24	V4.10(AAND.1)...	00-19-CB-B0-22-01	192.168.1.100	GS2210		
☐	GS2210-24	V4.10(AAND.1)...	00-19-CB-24-12-31	192.168.1.40	GS2210		
☐	GS1900-24P	V2.00(AAHL.0)b1	00-E0-4C-00-00-00	192.168.1.30	Switch	Location	
☐	GS1900-8HP	V2.00(AAHL.0)b1	FC-F5-28-52-D2-BF	192.168.1.10	Switch	Location	
☐	NWA5123-NI	V4.11(AAHY.0)l...	10-7B-EF-D1-5D-51	192.168.1.50	nwa5123-ni	Hsinchu,Taiw...	

5.3 ZON Neighbor Management Screen

The ZON Neighbor Management screen allows you to view and manage the SwitchSwitch's neighboring devices more conveniently. It uses Layer Link Discovery Protocol (LLDP) to discover all neighbor devices connected to the SwitchSwitch including non-ZyXEL devices. You can perform tasks on the neighboring devices like login, reboot (turn the power off and then back on again), and reset to factory default settings in the Neighbor Management screen. For more information on LLDP, see [Section 35.2 on page 322](#).

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

Figure 19 Status > Neighbor

Neighbor

Port Status

Local			Remote								
Port	Name	PoE Draw	Model Name	Sys. Name	FW Version	Port	Port Description	IP	MAC	PWR Cycle	Reset to Default
7	-	1.9 W	NWA5121-NI	nwa5121-ni	V4.11(AAID.0)IT_20140514145838	1	lan	192.168.1.2	B0-B2-DC-6E-C4-61	Cycle	Reset
14	-	-	XGS3700-24	XGS3700	V4.10(AAGC.5)b2 06/16/2014	13	-	192.168.1.10	00-19-cb-37-00-25	-	-
25	-	-	GS2210-24	GS2210	V4.10(AAND.1)b4 06/10/2014	16	-	192.168.1.1	00-19-cb-00-00-01	-	-

The following table describes the fields in the above screen.

Table 6 Status > Neighbor

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

5.4 Status Summary

In Stacking mode, click **Status** in the top of the web configurator to display the **Status** screen as shown next.

Figure 20 Status Summary (Stacking)

Slot	Name	Status	Up Time
1	XGS3700-48HP	active	12:02:43:37
2			
3			
4			
5			
6			
7			
8			

The following table describes the labels in this screen.

Table 7 Status Summary (Stacking)

LABEL	DESCRIPTION
System Up Time	This is the boot-up time in hours, minutes and seconds of the master Switch.
Slot	This identifies the Switch in the stack. Click an occupied slot number to display the Port Status screen (refer to Figure 22 on page 49).
Name	This is the System Name you assigned to the Switch in the Basic Setting > General Setup screen.
Status	This field displays one of the following: • Active: when the slot Switch has Stacking enabled and is on in the stack • Inactive: when the slot Switch has Stacking enabled but is not on in the stack • Init: when the master Switch is initializing the slot.
Up Time	This field shows the boot-up time in days, hours, minutes and seconds of the Switch identified by the slot.

5.4.1 Port Status

In Standalone mode, click **Status** to view port statistics. In Stacking mode, click an occupied slot number in the **Status** screen to view port statistics.

Port Status											Neighbor
Port	Name	Link	State	PD	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Time
1		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
2		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
3		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
4		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
5		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
6		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
7		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
8		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
9		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
10		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
11		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
12		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
13		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
14		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
15		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
16		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
17		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00

Port Status Status

SLOT 1 ▾

Port	Name	Link	State	PD	LACP	TxPkts	RxPkts	Errors	Tx KB/s	Rx KB/s	Up Time
1/1		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
1/2		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
1/3		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
1/4		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
1/5		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
1/6		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
1/7		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
1/8		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00

☒ Any
 ☐ Port

Label	Description
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port	This identifies the Ethernet port. In stacking mode, the first number represents the slot and the second the port number. Click a port number to display the Port Details screen (refer to Figure 23 on page 51).
Name	This is the name you assigned to this port in the Basic Setting > Port Setup screen.
Link	This field displays the speed (such as 100M for 100 Mbps, 1000M for 1000 Mbps, or 10G for 10 Gbps) and the duplex (F for full duplex). This field displays Down if the port is not connected to any device.

Table 8 Status (Standalone mode) and Port Status (Stacking mode) (continued)

LABEL	DESCRIPTION
State	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port. (See Section 11.1.3 on page 126 for more information). If STP is disabled, this field displays FORWARDING if the link is up, otherwise, it displays STOP .
PD	(For PoE models only) This field displays whether or not a powered device (PD) is allowed to receive power from the Switch on this port.
LACP	This 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.

5.4.2 Status: Port Details

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

Figure 23 Status: Port Details

Port Details			Port Status
Port Info	Port NO.	1	
	Name		
	Link	Down	
	State	STOP	
	LACP	Disabled	
	TxPkts	0	
	RxPkts	0	
	Errors	0	
	Tx KBs/s	0.0	
	Rx KBs/s	0.0	
	Up Time	0:00:00	
TX Packet	Unicast	0	
	Multicast	0	
	Broadcast	0	
	Pause	0	
	Tagged	0	
RX Packet	Unicast	0	
	Multicast	0	
	Broadcast	0	
	Pause	0	
	Control	0	
TX Collision	Single	0	
	Multiple	0	
	Excessive	0	
	Late	0	
Error Packet	RX CRC	0	
	Length	0	
	Runt	0	
Distribution	64	0	
	65 to 127	0	
	128 to 255	0	
	256 to 511	0	
	512 to 1023	0	
	1024 to 1518	0	
	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. In stacking mode, the first number represents the slot and the second the port number.
Name	This field displays the name of the port.
Link	This field displays the speed (such as 100M for 100Mbps, 1000M for 1000 Mbps, or 10G for 10 Gbps) and the duplex (F for full duplex).
State	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port (see Section 11.1.3 on page 126 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 KBs/s	This field shows the transmission speed of data sent on this port in kilobytes per second.

Table 9 Status > Port Details (continued)

LABEL	DESCRIPTION
Rx KBs/s	This field shows the transmission speed of data received on this port in kilobytes per second.
Up Time	This field shows the total amount of time the connection has been up.
Tx Packet	
The following fields display detailed information about packets transmitted.	
Unicast	This field shows the number of good unicast packets transmitted.
Multicast	This field shows the number of good multicast packets transmitted.
Broadcast	This field shows the number of good broadcast packets transmitted.
Pause	This field shows the number of 802.3x Pause packets transmitted.
Tagged	This field shows the number of packets with VLAN tags transmitted.
Rx Packet	
The following fields display detailed information about packets received.	
Unicast	This field shows the number of good unicast packets received.
Multicast	This field shows the number of good multicast packets received.
Broadcast	This field shows the number of good broadcast packets received.
Pause	This field shows the number of 802.3x Pause packets received.
Control	This field shows the number of control packets received (including those with CRC error) but it does not include the 802.3x Pause packets.
TX Collision	
The following fields display information on collisions while transmitting.	
Single	This is a count of successfully transmitted packets for which transmission is inhibited by exactly one collision.
Multiple	This is a count of successfully transmitted packets for which transmission was inhibited by more than one collision.
Excessive	This is a count of packets for which transmission failed due to excessive collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
Late	This is the number of times a late collision is detected, that is, after 512 bits of the packets have already been transmitted.
Error Packet	
The following fields display detailed information about packets received that were in error.	
RX CRC	This field shows the number of packets received with CRC (Cyclic Redundant Check) error(s).
Length	This field shows the number of packets received with a length that was out of range.
Runt	This field shows the number of packets received that were too short (shorter than 64 octets), including the ones with CRC errors.
Distribution	
64	This field shows the number of packets (including bad packets) received that were 64 octets in length.
65-127	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.

Table 9 Status > Port Details (continued)

LABEL	DESCRIPTION
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.

Basic Setting

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

6.1 System Information

In the navigation panel, click **Basic Setting** > **System Info** to display the screen as shown.

You can check the firmware version number and monitor the Switch temperature, fan speeds and voltage in this screen.

Figure 24 Basic Setting > System Info (Standalone Mode)

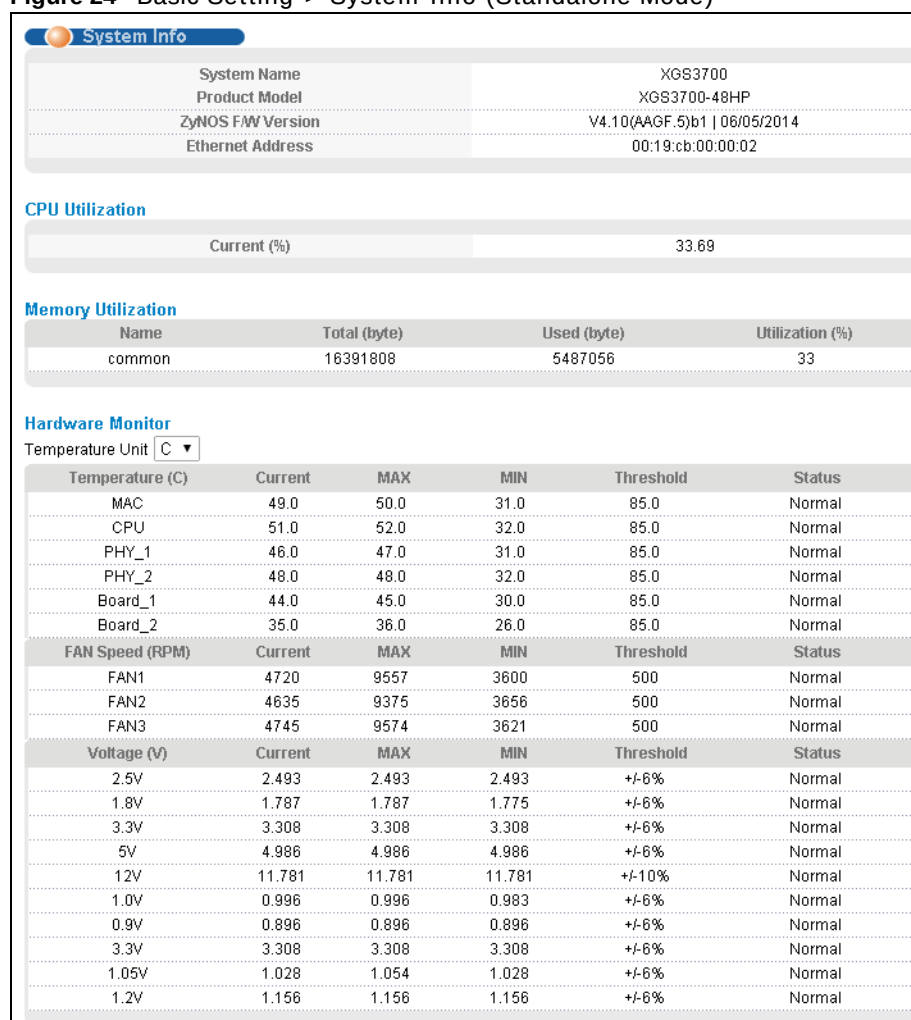


Figure 25 Basic Setting > System Info (Stacking Mode)

System Info

System Name	XGS3700
Product Model	XGS3700-48HP
ZyNOS F/W Version	V4.20(AAGF.0)b4 08/12/2014
Ethernet Address	00:19:cb:00:00:02

CPU Utilization

Current (%)	31.71

Memory Utilization

Name	Total (byte)	Used (byte)	Utilization (%)
common	36240512	19710304	54

Hardware Status

Slot	Name	Voltage	Temperature	Fan
1	XGS3700-48HP	Normal	Normal	Normal

The following table describes the labels in these screens.

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

LABEL	DESCRIPTION
System Name	This field displays the descriptive name of the Switch for identification purposes.
Product Model	This field displays the product model of the Switch. Use this information when searching for firmware upgrade or looking for other support information in the website.
ZyNOS F/W Version	This field displays the version number of the Switch 's current firmware including the date created.
Ethernet Address	This field refers to the Ethernet MAC (Media Access Control) address of the Switch.
CPU Utilization	CPU utilization quantifies how busy the system is. Current (%) displays the current percentage of CPU utilization.
Memory Utilization	Memory Utilization shows how much DRAM memory is available and in use. It also displays the current percentage of memory utilization.
Name	This field displays the name of memory pool.
Total	This field displays the total number of bytes in this memory pool.
Used	This field displays the number of bytes being used in this memory pool.
Utilization	This field displays the percentage (%) of memory being used in this memory pool.
Hardware Monitor (Standalone Mode)	
Temperature Unit	The Switch has temperature sensors that are capable of detecting and reporting if the temperature rises above the threshold. You may choose the temperature unit (Centigrade or Fahrenheit) in this field.
Temperature	BOARD, MAC and PHY refer to the location of the temperature sensors on the Switch printed circuit board.
Current	This shows the current temperature at this sensor.
MAX	This field displays the maximum temperature measured at this sensor.
MIN	This field displays the minimum temperature measured at this sensor.
Threshold	This field displays the upper temperature limit at this sensor.
Status	This field displays Normal for temperatures below the threshold and Error for those above.

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

LABEL	DESCRIPTION
Fan Speed (RPM)	A properly functioning fan is an essential component (along with a sufficiently ventilated, cool operating environment) in order for the device to stay within the temperature threshold. Each fan has a sensor that is capable of detecting and reporting if the fan speed falls below the threshold shown.
Current	This field displays this fan's current speed in Revolutions Per Minute (RPM).
MAX	This field displays this fan's maximum speed measured in Revolutions Per Minute (RPM).
MIN	This field displays this fan's minimum speed measured in Revolutions Per Minute (RPM). "<41" is displayed for speeds too small to measure (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.
Hardware Status (Stacking Mode)	
Slot	This number identifies the Switch in the stack. Click the number to see more detailed information on the Switch.
Name	This is the system name of the Switch in the stack.
Voltage	This shows if the power supply voltage sensor is within normal tolerance range.
Temperature	This shows if the temperature sensors on the Switch printed circuit board are within normal tolerance range.
Fan	This shows if the fan sensors are within normal tolerance range.

6.1.1 System Information Stacking Hardware Monitor

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

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

Hardware Monitor						System Info
SLOT 1						
Temperature Unit C						
Temperature (C)	Current	MAX	MIN	Threshold	Status	
1/MAC	47.0	51.0	35.0	85.0	Normal	
1/CPU	48.0	52.0	36.0	85.0	Normal	
1/PHY_1	45.0	49.0	35.0	85.0	Normal	
1/PHY_2	46.0	50.0	36.0	85.0	Normal	
1/Board_1	42.0	46.0	34.0	85.0	Normal	
1/Board_2	34.0	38.0	29.0	85.0	Normal	
FAN Speed (RPM)	Current	MAX	MIN	Threshold	Status	
1/FAN1	4830	9557	3643	500	Normal	
1/FAN2	4770	9342	3686	500	Normal	
1/FAN3	4757	9523	3673	500	Normal	
Voltage (V)	Current	MAX	MIN	Threshold	Status	
1/2.5V	2.493	2.493	2.493	+/-6%	Normal	
1/1.8V	1.787	1.787	1.775	+/-6%	Normal	
1/3.3V	3.308	3.308	3.308	+/-6%	Normal	
1/5V	4.986	4.986	4.986	+/-6%	Normal	
1/12V	11.781	11.781	11.781	+/-10%	Normal	
1/1.0V	0.983	0.996	0.983	+/-6%	Normal	
1/0.9V	0.896	0.896	0.896	+/-6%	Normal	
1/3.3V	3.308	3.308	3.308	+/-6%	Normal	
1/1.05V	1.028	1.054	1.028	+/-6%	Normal	
1/1.2V	1.156	1.156	1.156	+/-6%	Normal	

The following table describes the labels in this screen.

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

LABEL	DESCRIPTION
SLOT	This number identifies the Switch in the stack.
Temperature Unit	The Switch has temperature sensors that are capable of detecting and reporting if the temperature rises above the threshold. You may choose the temperature unit (Centigrade or Fahrenheit) in this field.
Temperature	BOARD , PHY , CPU and MAC refer to the location of the temperature sensors on the Switch printed circuit board.
Current	This shows the current temperature at this sensor.
MAX	This field displays the maximum temperature measured at this sensor.
MIN	This field displays the minimum temperature measured at this sensor.
Threshold	This field displays the upper temperature limit at this sensor.
Status	This field displays Normal for temperatures below the threshold and Error for those above.
Fan Speed (RPM)	A properly functioning fan is an essential component (along with a sufficiently ventilated, cool operating environment) in order for the device to stay within the temperature threshold. Each fan has a sensor that is capable of detecting and reporting if the fan speed falls below the threshold shown.
Current	This field displays this fan's current speed in Revolutions Per Minute (RPM).
MAX	This field displays this fan's maximum speed measured in RPM.
MIN	This field displays this fan's minimum speed measured in RPM. "<41" is displayed for speeds too small to measure (under 2000 RPM).
Threshold	This field displays the minimum speed at which a normal fan should work.
Status	Normal indicates that this fan is functioning above the minimum speed. Error indicates that this fan is functioning below the minimum speed.
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.

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

LABEL	DESCRIPTION
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.

6.2 General Setup

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

Figure 27 Basic Setting > General Setup

The following table describes the labels in this screen.

Table 12 Basic Setting > General Setup

LABEL	DESCRIPTION
System Name	Type a descriptive name for identification purposes. This name consists of up to 64 printable ASCII characters; spaces are allowed.
Location	Type the geographic location of your Switch. You can use up to 32 printable ASCII characters; spaces are allowed.
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 12 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).
End Date	Configure the day and time when Daylight Saving Time ends if you selected Daylight Saving Time. The time field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the last Sunday of October. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select First, Sunday, November and 2:00. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, October and the last field depends on your time zone. In Germany for instance, you would select 2:00 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

Table 12 Basic Setting > General Setup (continued)

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

6.3 Introduction to VLANs

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

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

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

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

See [Chapter 7 on page 94](#) for information on port-based and 802.1Q tagged VLANs.

6.4 Switch Setup

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

Figure 28 Basic Setting > Switch Setup

The following table describes the labels in this screen.

Table 13 Basic Setting > Switch Setup

LABEL	DESCRIPTION
VLAN Type (Standalone mode only)	Choose 802.1Q or Port Based . The VLAN Setup screen changes depending on whether you choose 802.1Q VLAN type or Port Based VLAN type in this screen. See Chapter 7 on page 94 for more information. The Switch does not have port-based VLAN available in stacking mode (Active is enabled in Basic Setting > Stacking > Configuration), so this field does not display in stacking mode.
Bridge Control Protocol Transparency	Select Active to allow the Switch to handle bridging control protocols (STP, for example). You also need to define how to treat a BPDU in the Port Setup screen.
MAC Address Learning	MAC address learning reduces outgoing traffic broadcasts. For MAC address learning to occur on a port, the port must be active.
Aging Time	Enter a time from 10 to 1000000 seconds. This is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be relearned).
ARP Aging Time	
Aging Time	Enter a time from 60 to 1000000 seconds. This is how long dynamically learned ARP entries remain in the ARP table before they age out (and must be relearned). The setting here applies to ARP entries which are newly added in the ARP table after you click Apply .
GARP Timer: Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values. See Chapter 7 on page 94 for more background information.	
Join Timer	Join Timer sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a Join Period timer. The allowed Join Time range is between 100 and 65535 milliseconds; the default is 200 milliseconds. See Chapter 7 on page 94 for more background information.
Leave Timer	Leave Time sets the duration of the Leave Period timer for GVRP in milliseconds. Each port has a single Leave Period timer. Leave Time must be two times larger than Join Timer ; the default is 600 milliseconds.

Table 13 Basic Setting > Switch Setup (continued)

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

6.5 IP Setup

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

6.5.1 IP Interfaces

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

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

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

You can configure up to 128 IP domains which are used to access and manage the Switch from the ports belonging to the pre-defined VLAN(s).

Note: You must configure a VLAN first.

Figure 29 Basic Setting > IP Setup

The following table describes the labels in this screen.

Table 14 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.
Out-of-band Management IP Address	
Use these fields to set the settings for the out-of-band management port.	

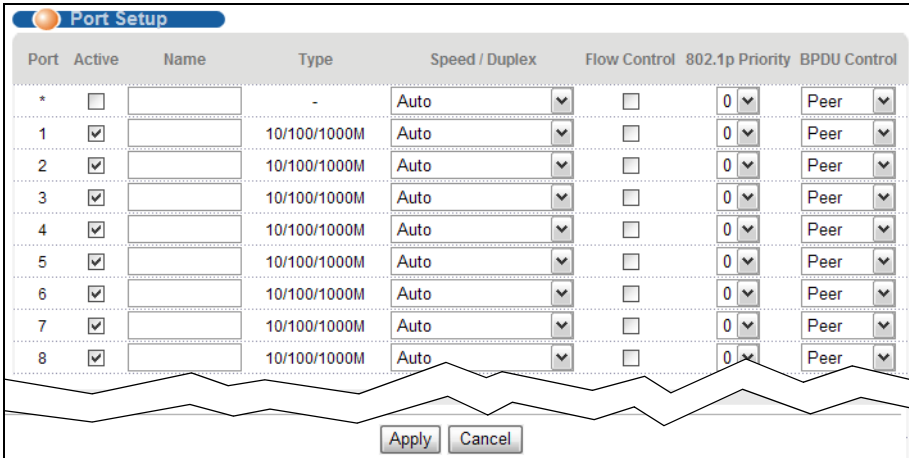
Table 14 Basic Setting > IP Setup (continued)

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 this to create a new entry. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Index	This field displays the index number of an entry.
IP Address	This field displays IP address of the Switch in the IP domain.
IP Subnet Mask	This field displays the subnet mask of the Switch in the IP domain.
VID	This field displays the VLAN identification number of the IP domain on the Switch.
Delete	Select the entries you want to remove.
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.

6.6 Port Setup

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

Figure 30 Basic Setting > Port Setup (GS3700 Series)

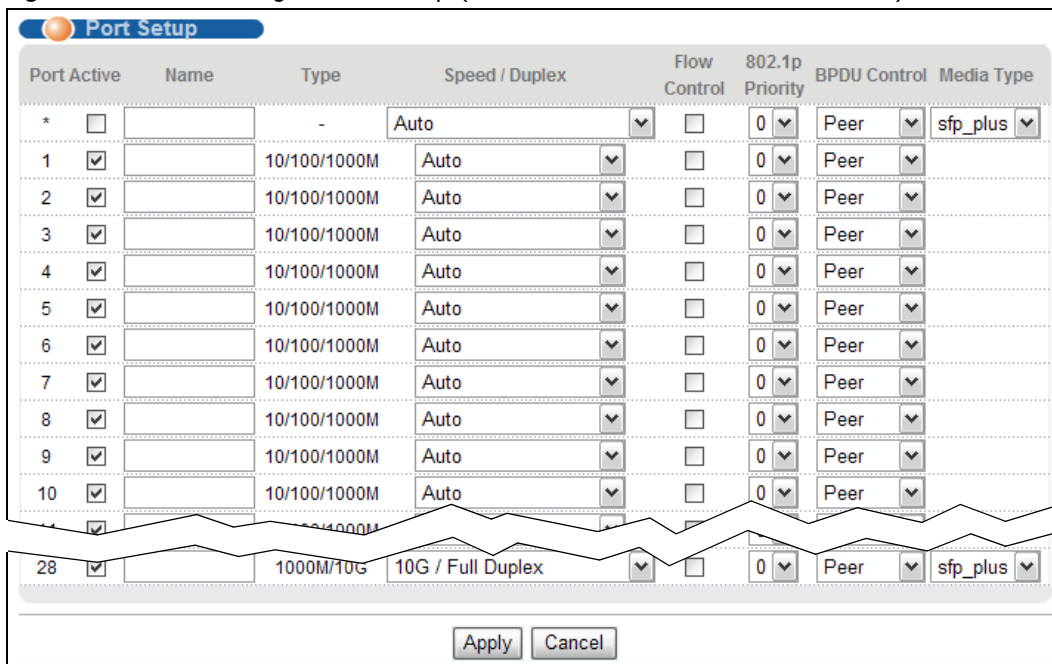


Port Setup

Port	Active	Name	Type	Speed / Duplex	Flow Control	802.1p Priority	BPDU Control
*	☐		-	Auto	☐	0	Peer
1	☒		10/100/1000M	Auto	☐	0	Peer
2	☒		10/100/1000M	Auto	☐	0	Peer
3	☒		10/100/1000M	Auto	☐	0	Peer
4	☒		10/100/1000M	Auto	☐	0	Peer
5	☒		10/100/1000M	Auto	☐	0	Peer
6	☒		10/100/1000M	Auto	☐	0	Peer
7	☒		10/100/1000M	Auto	☐	0	Peer
8	☒		10/100/1000M	Auto	☐	0	Peer

Apply Cancel

Figure 31 Basic Setting > Port Setup (XGS3700 Series: Standalone mode)



Port Setup

Port	Active	Name	Type	Speed / Duplex	Flow Control	802.1p Priority	BPDU Control	Media Type
*	☐		-	Auto	☐	0	Peer	sfp_plus
1	☒		10/100/1000M	Auto	☐	0	Peer	
2	☒		10/100/1000M	Auto	☐	0	Peer	
3	☒		10/100/1000M	Auto	☐	0	Peer	
4	☒		10/100/1000M	Auto	☐	0	Peer	
5	☒		10/100/1000M	Auto	☐	0	Peer	
6	☒		10/100/1000M	Auto	☐	0	Peer	
7	☒		10/100/1000M	Auto	☐	0	Peer	
8	☒		10/100/1000M	Auto	☐	0	Peer	
9	☒		10/100/1000M	Auto	☐	0	Peer	
10	☒		10/100/1000M	Auto	☐	0	Peer	
28	☒		1000M/10G	10G / Full Duplex	☐	0	Peer	sfp_plus

Apply Cancel

Figure 32 Basic Setting > Port Setup (XGS3700 Series: Stacking mode)

Port	Active	Name	Type	Speed / Duplex	Flow Control	802.1p Priority	BPDU Control	Media Type
1*	☐		-	Auto	☐	0	Peer	sfp_plus
1/1	☒		10/100/1000M	Auto	☐	0	Peer	
1/2	☒		10/100/1000M	Auto	☐	0	Peer	
1/3	☒		10/100/1000M		☐	0	Peer	
1/48	☒		10/100/1000M	Auto	☐	0	Peer	
1/49	☒		1000M/10G	10G / Full Duplex	☐	0	Peer	sfp_plus
1/50	☒		1000M/10G	10G / Full Duplex	☐	0	Peer	sfp_plus

Apply Cancel

The following table describes the labels in this screen.

Table 15 Basic Setting > Port Setup

LABEL	DESCRIPTION
Port	This is the port index number. In stacking mode, the first number is the slot ID and the second is the port number. * means all ports.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable a port. The factory default for all ports is enabled. A port must be enabled for data transmission to occur.
Name	Type a descriptive name that identifies this port. You can enter up to 64 alpha-numerical characters. Note: Due to space limitations, the port name may be truncated in some web configurator screens.
Type	This field displays 10M / 100M / 1000M for a 1000Base-T connection, 1000M for a 1000Base-X connection, and 10G for a 10 Gigabit connection (available only on the Switch that has a 10 Gigabit interface).
Speed/Duplex	Select the speed and the duplex mode of the Ethernet connection on this port. The choices are Auto, 10M / Half Duplex, 10M / Full Duplex, 100M / Half Duplex and 100M / Full Duplex for a 100Base-T connection. 1000M / Full Duplex is supported by both 1000Base-T and 1000Base-X connections. 10G / Full Duplex is supported by the 10 Gigabit Ethernet connections on the Switch that has a 10 Gigabit interface. Selecting Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the Switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the Switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.

Table 15 Basic Setting > Port Setup (continued)

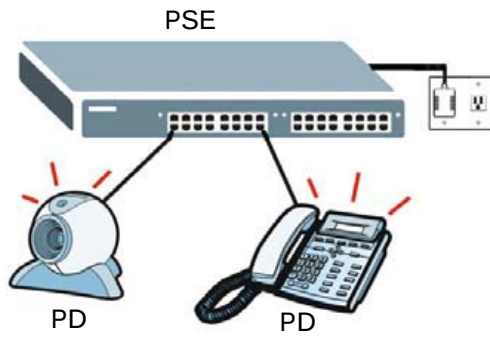
LABEL	DESCRIPTION
Flow Control	A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port. The Switch uses IEEE 802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE 802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. Select Flow Control to enable it.
802.1p Priority	This priority value is added to incoming frames without a (802.1p) priority queue tag. See Priority Queue Assignment in Table 13 on page 61 for more information.
BPDU Control	Configure the way to treat BPDUs received on this port. You must activate bridging control protocol transparency in the Switch Setup screen first. Select Peer to process any BPDU (Bridge Protocol Data Units) received on this port. Select Tunnel to forward BPDUs received on this port. Select Discard to drop any BPDU received on this port. Select Network to process a BPDU with no VLAN tag and forward a tagged BPDU.
Media Type	On the Switch that has a 10 Gigabit interface, such as the SFP+ slot, you can insert either an SFP+ transceiver or an SFP+ Direct Attach Copper (DAC). An SFP+ Direct Attach Copper (DAC) is an SFP+ housing that has no optical module but uses a fixed-length passive copper cable assembly, which reduces cost and power significantly. Select the media type (sfp_plus or dac10g) of the SFP+ module that is attached to the 10 Gigabit interface.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

6.7 PoE

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

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

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

Figure 33 Powered Device Examples

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

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

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

Figure 34 Basic Setting > PoE Status (Standalone mode)

PoE Status				Consumption		
PoE Mode				Consumption		
Total Power (W)				460.0		
Consuming Power (W)				0.0		
Allocated Power (W)				NA		
Remaining Power (W)				460.0		

Port	State	Class	PD Priority	Consuming Power (mW)	Max Power (mW)	Max Current (mA)
1	Enable	0	Low	0	0	0
2	Enable	0	Low	0	0	0
3	Enable	0	Low	0	0	0
4	Enable	0	Low	0	0	0
5	Enable	0	Low	0	0	0
6	Enable	0	Low	0	0	0
7	Enable	0	Low	0	0	0
8	Enable	0	Low	0	0	0
9	Enable	0	Low	0	0	0
10	Enable	0	Low	0	0	0
11	Enable	0	Low	0	0	0
12	Enable	0	Low	0	0	0
13	Enable	0	Low	0	0	0
14	Enable	0	Low	0	0	0
15	Enable	0	Low	0	0	0
16	Enable	0	Low	0	0	0

Figure 35 Basic Setting > PoE Status (Stacking mode)

PoE Status		PoE Setup				
SLOT 1 ▼						
PoE Mode		Consumption				
Total Power (W)		460.0				
Consuming Power (W)		0.0				
Allocated Power (W)		NA				
Remaining Power (W)		460.0				
Port	State	Class	PD Priority	Consuming Power (mW)	Max Power (mW)	Max Current (mA)
1/1	Enable	0	Low	0	0	0
1/2	Enable	0	Low	0	0	0
1/3	Enable	0	Low	0	0	0
1/4	Enable	0	Low	0	0	0
1/47	Enable	0	Low	0	0	0
1/48	Enable	0	Low	0	0	0

The following table describes the labels in this screen.

Table 16 Basic Setting > PoE Status

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

Table 16 Basic Setting > PoE Status

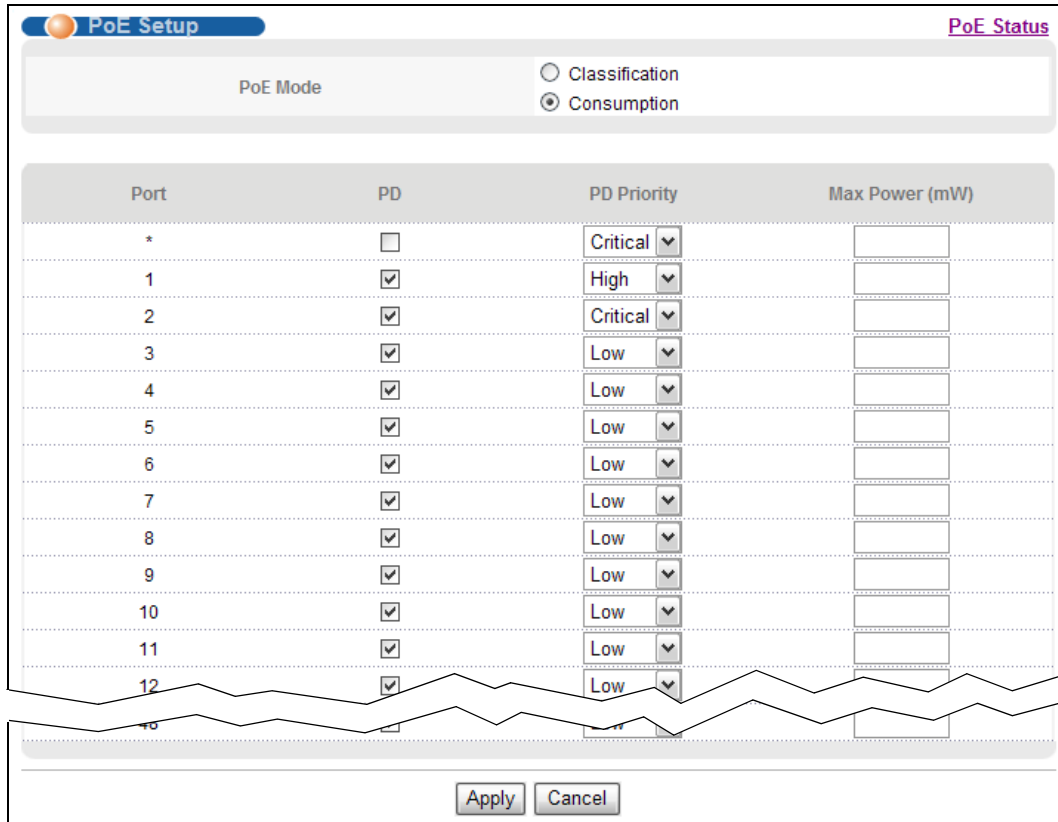
LABEL	DESCRIPTION
Class	This shows the power classification of the PD. This is a number from 0 to 4, where each value represents a range of power (W) and current (mA) that the PD requires to function. The ranges are as follows. • Class 0 - Default, 0.44 to 12.94 • Class 1 - Optional, 0.44 to 3.84 • Class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

6.7.1 PoE Setup

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

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

Figure 36 Basic Setting > PoE Status > PoE Setup (Standalone mode)



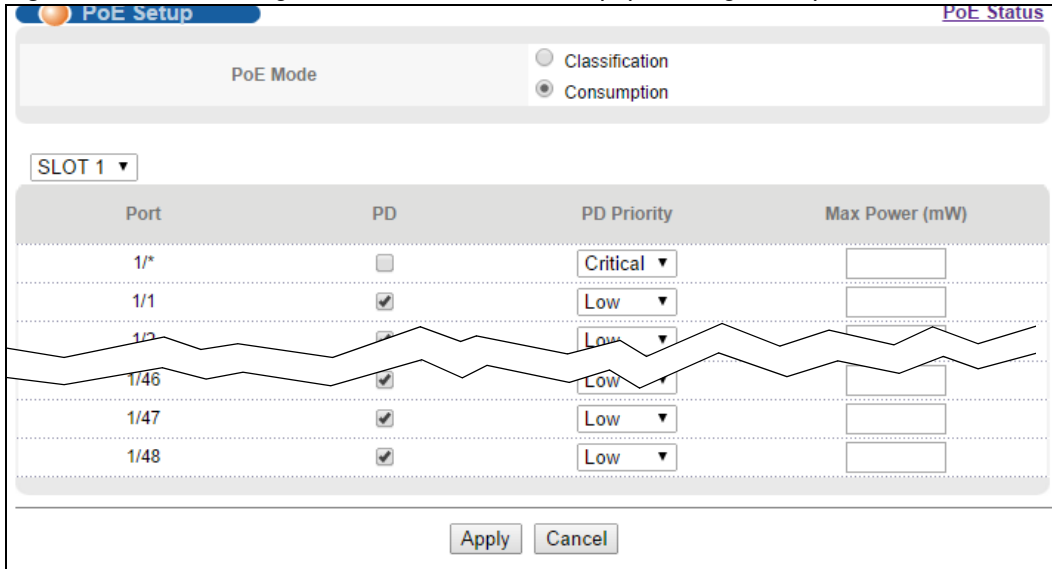
PoE Setup PoE Status

PoE Mode: ☐ Classification ☒ Consumption

Port	PD	PD Priority	Max Power (mW)
*	☐	Critical ▼	
1	☒	High ▼	
2	☒	Critical ▼	
3	☒	Low ▼	
4	☒	Low ▼	
5	☒	Low ▼	
6	☒	Low ▼	
7	☒	Low ▼	
8	☒	Low ▼	
9	☒	Low ▼	
10	☒	Low ▼	
11	☒	Low ▼	
12	☒	Low ▼	

Apply Cancel

Figure 37 Basic Setting > PoE Status > PoE Setup (Stacking mode)



PoE Setup PoE Status

PoE Mode: ☐ Classification ☒ Consumption

SLOT 1 ▼

Port	PD	PD Priority	Max Power (mW)
1/*	☐	Critical ▼	
1/1	☒	Low ▼	
1/2	☒	Low ▼	
1/46	☒	Low ▼	
1/47	☒	Low ▼	
1/48	☒	Low ▼	

Apply Cancel

The following table describes the labels in this screen.

Table 17 Basic Setting > PoE Status > PoE Setup

LABEL	DESCRIPTION
PoE Mode	Select the power management mode you want the Switch to use. • Classification - Select this if you want the Switch to reserve the Max Power (mW) to each PD according to the power classification of the PD. If the total power supply available is not enough to supply all connected PDs, then PDs with lower priority do not get power to function. • Consumption - Select this if you want the Switch to manage the total power supply so that each connected PD gets a resource. However, the power allocated by the Switch may be less than the Max Power (mW) of the PD. PDs with higher priority also get more power than those with lower priority levels.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or Stacking mode)	This is the port index number. In stacking mode, the first box field is the slot ID and the second field is the port number. * means all ports (on the same Switch).
PD	Select this to provide power to a PD connected to the port. If left unchecked, the PD connected to the port cannot receive power from the Switch.
PD Priority	This field is not available for the SFP or SFP+ ports. When the total power requested by the PDs exceeds the total PoE power budget on the Switch, you can set the PD priority to allow the Switch to provide power to ports with higher priority. Select Critical to give the PD connected to this port the highest priority. Select High to set the Switch to assign the remaining power to the port after all critical priority ports are served. Select Low to set the Switch to assign the remaining power to the port after all critical and high priority ports are served.
Max Power (mW)	Set the maximum amount of power (from 1000 to 33000) the PD could use from the Switch on this port. Otherwise, leave the field blank to allow the connected PD to use power up to 33W in Consumption mode and 30W in Classification mode.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

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

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

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

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

6.8 Interface Setup

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

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

Figure 38 Basic Setting > Interface Setup

Index	Interface Type	Interface ID	Interface	Delete
1	VLAN	123	VLAN123	☐
2	VLAN	1111	VLAN1111	☐

The following table describes the labels in this screen.

Table 18 Basic Setting > Interface Setup

LABEL	DESCRIPTION
Interface Type	Select the type of IPv6 interface for which you want to configure. The Switch supports the VLAN interface type for IPv6 at the time of writing.
Interface ID	Specify a unique identification number (from 1 to 4094) for the interface. Note: To have IPv6 function properly, you should configure a static VLAN with the same ID number in the Advanced Setup > VLAN screens.
Add	Click this to create a new entry. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Index	This field displays the index number of an entry.
Interface Type	This field displays the type of interface.
Interface ID	This field displays the identification number of the interface.
Interface	This field displays the interface's descriptive name which is generated automatically by the Switch. The name is from a combination of the interface type and ID number.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

6.9 IPv6

Use this screen to view the IPv6 interface status and configure Switch's management IPv6 addresses. See [Appendix B on page 467](#) for more information about IPv6.

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

Figure 39 Basic Setting > IPv6 Status

Index	Interface	Active
1	VLAN1	No
2	VLAN123	Yes
3	VLAN463	No
4	VLAN1111	No

The following table describes the labels in this screen.

Table 19 Basic Setting > IPv6 Status

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

6.9.1 IPv6 Interface Status

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

Figure 40 Basic Setting > IPv6 Interface Status

IPv6 Interface Status
 Interface: VLAN123

IPv6 Status

IPv6 Active	enable
MTU Size	1500
ICMPv6 Rate Limit Bucket Size	100
ICMPv6 Rate Limit Error Interval	1000
Stateless Address Autoconfig	enable
Link Local Address	fe80::219:cbff:fe37:49/64 [preferred]
Global Unicast Address(es)	
Joined Group Address(es)	ff02::2 ff01::1 ff02::1 ff02::1:ff37:49
ND DAD Active	enable
Number of DAD Attempts	1
NS-Interval (millisecond)	1000
ND Reachable Time (millisecond)	30000

DHCPv6 Client Active		Yes
Identity Association	IA Type	IA-NA
	IAID	1231
	T1	0
	T2	0
	State	
	SID	
	Address	
	Preferred Lifetime	0
Valid Lifetime	0	
DNS		
Domain List		

Restart DHCPv6 Client

[Click Here](#)

The following table describes the labels in this screen.

Table 20 Basic Setting > IPv6 Interface Status

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

Table 20 Basic Setting > IPv6 Interface Status (continued)

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

Table 20 Basic Setting > IPv6 Interface Status (continued)

LABEL	DESCRIPTION
Domain List	This field displays the address record when the Switch queries the DNS server to resolve domain names.
Restart DHCPv6 Client	Click Click Here to send a new DHCP request to the DHCPv6 server and update the IPv6 address and DNS information for this interface.

6.9.2 IPv6 Configuration

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

Figure 41 Basic Setting > IPv6 > IPv6 Configuration

The following table describes the labels in this screen.

Table 21 Basic Setting > IPv6 > IPv6 Configuration

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

6.9.3 IPv6 Global Setup

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

Figure 42 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Setup

IPv6 Global Setup		IPv6 Configuration
IPv6 Hop Limit	64	
ICMPv6 Rate Limit Bucket Size	100	
ICMPv6 Rate Limit Error Interval	1000	milliseconds
Apply Cancel Clear		

The following table describes the labels in this screen.

Table 22 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Setup

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

6.9.4 IPv6 Interface Setup

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

Figure 43 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Interface Setup

Index	Interface	Active	Address Autoconfig
1	VLAN123	No	No
2	VLAN2222	No	No

The following table describes the labels in this screen.

Table 23 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Interface Setup

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

6.9.5 IPv6 Link-Local Address Setup

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

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

Figure 44 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Link-Local Address Setup

Index	Interface	IPv6 Link-Local Address	IPv6 Default Gateway
1	VLAN123		
2	VLAN2222		

The following table describes the labels in this screen.

Table 24 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Link-Local Address Setup

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

6.9.6 IPv6 Global Address Setup

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

Figure 45 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Address Setup

The screenshot shows the 'IPv6 Global Address Setup' configuration page. At the top, there's a title bar with an orange icon and the text 'IPv6 Global Address Setup'. To the right is a link 'IPv6 Configuration'. The main form area has several input fields: 'Interface' with a dropdown menu showing 'VLAN123', 'IPv6 Global Address' with a text box, 'Prefix Length' with a text box, and an 'EUI-64' checkbox. Below these fields are three buttons: 'Add', 'Cancel', and 'Clear'. At the bottom of the screen, there is a table with the following columns: 'Index', 'Interface', 'IPv6 Global Address/Prefix Length', 'EUI-64', and 'Delete'. Below the table are two buttons: 'Delete' and 'Cancel'.

The following table describes the labels in this screen.

Table 25 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Address Setup

LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
IPv6 Global Address	Manually configure a static IPv6 global address for the interface.
Prefix Length	Specify an IPv6 prefix length that specifies how many most significant bits (start from the left) in the address compose the network address.
EUI-64	Select this option to have the interface ID be generated automatically using the EUI-64 format.
Add	Click Add to create a new entry or update an existing one.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to reset the fields to the factory defaults.
Index	This is the interface index number. Click on an index number to change the settings.
Interface	This is the name of the IPv6 interface you created.
IPv6 Global Address/ Prefix Length	This field displays the IPv6 global address and prefix length for the interface.
EUI-64	This shows whether the interface ID of the global address is generated using the EUI-64 format.
Delete	Check the entry(ies) that you want to remove in the Delete column and then click Delete to remove the selected entry(ies) from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

6.9.7 IPv6 Neighbor Discovery Setup

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

Figure 46 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Discovery Setup

Index	Interface	DAD Attempts	NS Interval	Reachable Time
1	VLAN123	1	1000	30000
2	VLAN2222	1	1000	30000

The following table describes the labels in this screen.

Table 26 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Discovery Setup

LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
DAD Attempts	The Switch uses Duplicate Address Detection (DAD) with neighbor solicitation and advertisement messages to check whether an IPv6 address is already in use before assigning it to an interface, such as the link-local address it creates through stateless address autoconfiguration. Specify the number of consecutive neighbor solicitations (from 0 to 600) the Switch sends for this interface. Enter 0 to turn off DAD.
NS Interval	Specify the time interval (from 1000 to 3600000 milliseconds) at which neighbor solicitations are re-sent for this interface.
Reachable Time	Specify how long (from 1000 to 3600000 milliseconds) a neighbor is considered reachable for this interface.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to reset the fields to the factory defaults.
Index	This is the interface index number. Click on an index number to change the settings.
Interface	This is the name of the IPv6 interface you created.
DAD Attempts	This field displays the number of consecutive neighbor solicitations the Switch sends for this interface.
NS Interval	This field displays the time interval (in milliseconds) at which neighbor solicitations are re-sent for this interface.
Reachable Time	This field displays how long (in milliseconds) a neighbor is considered reachable for this interface.

6.9.8 IPv6 Router Discovery Setup

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

Figure 47 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Router Discovery Setup

Index	Interface	Flags	Minimum Interval	Maximum Interval	Lifetime	Suppress
1	VLAN123		200	600	1800	No
2	VLAN2222		200	600	1800	No

The following table describes the labels in this screen.

Table 27 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Router Discovery Setup

LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
Flags	Select the Managed Config Flag option to have the Switch set the "managed address configuration" flag (the M flag) to 1 in IPv6 router advertisements, which means IPv6 hosts use DHCPv6 to obtain IPv6 stateful addresses. Deselect the option to set the flag to 0 and the host will not use DHCPv6 to obtain IPv6 stateful addresses. Select the Other Config Flag option to have the Switch set the "Other stateful configuration" flag (the O flag) to 1 in IPv6 router advertisements, which means IPv6 hosts use DHCPv6 to obtain additional configuration settings, such as DNS information. Deselect the option to set the flag to 0 and the host will not use DHCPv6 to obtain additional configuration settings.
Minimum Interval	Specify the minimum time interval (from 3 to 1350 seconds) at which the Switch sends router advertisements for this interface. Note: The minimum time interval cannot be greater than three-quarters of the maximum time interval.
Maximum Interval	Specify the maximum time interval (from 4 to 1800 seconds) at which the Switch sends router advertisements for this interface.
Lifetime	Specify how long (from 0 to 9000 seconds) the router in router advertisements can be used as a default router for this interface.
Suppress	Select this option to set the Switch to not send router advertisements and responses to router solicitations on this interface.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to reset the fields to the factory defaults.
Index	This is the interface index number. Click on an index number to change the settings.
Interface	This is the name of the IPv6 interface you created.

Table 27 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Router Discovery Setup (continued)

LABEL	DESCRIPTION
Flags	This field displays whether IPv6 hosts use DHCPv6 to obtain IPv6 stateful addresses (M) and/or additional configuration settings (O).
Minimum Interval	This field displays the minimum time interval at which the Switch sends router advertisements for this interface.
Maximum Interval	This field displays the maximum time interval at which the Switch sends router advertisements for this interface.
Lifetime	This field displays how long the router in router advertisements can be used as a default router for this interface.
Suppress	This field displays whether the Switch sends router advertisements and responses to router solicitations on this interface (No) or not (Yes).

6.9.9 IPv6 Prefix Setup

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

Figure 48 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Prefix Setup

IPv6 Prefix Setup [IPv6 Configuration](#)

Interface: VLAN123

Prefix:

Prefix Length:

Valid Lifetime: 2592000 seconds

Preferred Lifetime: 604800 seconds

Flags:

- ☐ No-Autoconfig Flag
- ☐ No-Onlink Flag
- ☐ No-Advertise Flag

Add Cancel Clear

Index	Interface	Prefix/Prefix Length	Valid Lifetime	Preferred Lifetime	Delete

Delete Cancel

The following table describes the labels in this screen.

Table 28 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Prefix Setup

LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
Prefix	Set the IPv6 prefix that the Switch includes in router advertisements for this interface.
Prefix Length	Set the prefix length that the Switch includes in router advertisements for this interface.
Valid Lifetime	Specify how long (from 0 to 4294967295 seconds) the prefix is valid for on-link determination.

Table 28 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Prefix Setup (continued)

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

6.9.10 IPv6 Neighbor Setup

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

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

The screenshot shows the 'IPv6 Neighbor Setup' configuration page. At the top, there's a navigation bar with 'IPv6 Neighbor Setup' and a link to 'IPv6 Configuration'. Below this, there are four input fields: 'Interface Type' (a dropdown menu currently showing 'VLAN'), 'Interface ID' (a text input field), 'Neighbor Address' (a text input field), and 'MAC' (a text input field with a colon-separated format). Below these fields are three buttons: 'Add', 'Cancel', and 'Clear'. At the bottom of the page, there is a table with five columns: 'Index', 'Interface', 'Neighbor Address', 'MAC', and 'Delete'. Below the table are two buttons: 'Delete' and 'Cancel'.

The following table describes the labels in this screen.

Table 29 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Setup

LABEL	DESCRIPTION
Interface Type	Select the type of IPv6 interface for which you want to configure. The Switch supports the VLAN interface type for IPv6 at the time of writing.
Interface ID	Specify a unique identification number (from 1 to 4094) for the interface. Note: A static IPv6 neighbor entry displays in the Management > Neighbor Table screen only when the interface ID is also created in the Basic Setup > Interface Setup screen. Note: To have IPv6 function properly, you should configure a static VLAN with the same ID number in the Advanced Setup > VLAN screens.
Neighbor Address	Specify the IPv6 address of the neighboring device which can be reached through the interface.
MAC	Specify the MAC address of the neighboring device which can be reached through the interface.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to reset the fields to the factory defaults.
Index	This is the interface index number. Click on an index number to change the settings.
Interface	This is the name of the IPv6 interface you created.
Neighbor Address	This field displays the IPv6 address of the neighboring device which can be reached through the interface
MAC	This field displays the MAC address of the neighboring device which can be reached through the interface.
Delete	Check the entry(ies) that you want to remove in the Delete column and then click Delete to remove the selected entry(ies) from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

6.9.11 DHCPv6 Client Setup

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

Figure 50 Basic Setting > IPv6 > IPv6 Configuration > DHCPv6 Client Setup

Index	Interface	IA-NA	Rapid-Commit	DNS	Domain-List	Information Refresh Minimum
1	VLAN123	No	No	No	No	86400
2	VLAN222	No	No	No	No	86400

The following table describes the labels in this screen.

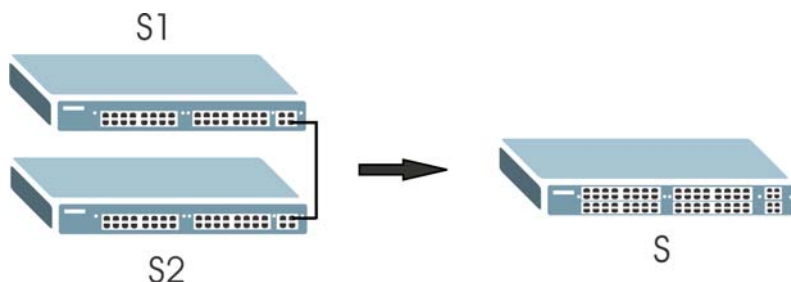
Table 30 Basic Setting > IPv6 > IPv6 Configuration > DHCPv6 Client Setup

LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
IA Type	Select IA-NA to set the Switch to get a non-temporary IP address from the DHCPv6 server for this interface. Optionally, you can also select Rapid-Commit to have the Switch send its DHCPv6 Solicit message with a Rapid Commit option to obtain information from the DHCPv6 server by a rapid two-message exchange. The Switch discards any Reply messages that do not include a Rapid Commit option. The DHCPv6 server should also support the Rapid Commit option to have it work well.
Options	Select DNS to have the Switch obtain DNS server IPv6 addresses and/or select Domain-List to have the Switch obtain a list of domain names from the DHCP server.
Information Refresh Minimum	Specify the time interval (from 600 to 4294967295 seconds) at which the Switch exchanges other configuration information with a DHCPv6 server again.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to reset the fields to the factory defaults.
Index	This is the interface index number. Click on an index number to change the settings.
Interface	This is the name of the IPv6 interface you created.
IA-NA	This field displays whether the Switch obtains a non-temporary IP address from the DHCPv6 server.
Rapid-Commit	This field displays whether the Switch obtains information from the DHCPv6 server by a rapid two-message exchange.
DNS	This field displays whether the Switch obtains DNS server IPv6 addresses from the DHCPv6 server.
Domain-List	This field displays whether the Switch obtains a list of domain names from the DHCP server.
Information Refresh Minimum	This field displays the time interval (in seconds) at which the Switch exchanges other configuration information with a DHCPv6 server again.

6.10 Stacking

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

Figure 51 Switch Stacking Concept



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

Table 31 Switch Stacking

MODELS WITH STACKING SUPPORT
XGS3700-24
XGS3700-24HP
XGS3700-48
XGS3700-48HP

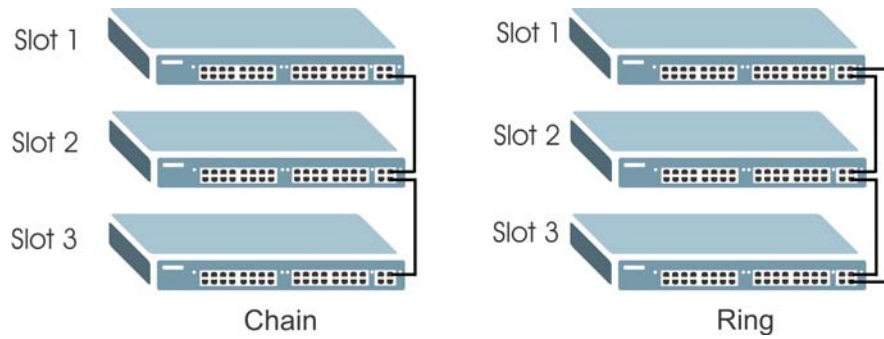
Note: Up to 8 Switches per stack are allowed.

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

The advantages of stacking are:

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

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

Figure 52 Stacking Topology

6.10.1 Stacking Status

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

Figure 53 Basic Setting > Stacking Status

Stacking Status					Configuration
Slot	Name	Status	MAC address	Role	
1	XGS3700-24	active	00:19:cb:00:01:01	master	
2	XGS3700-24HP	active	00:19:cb:00:02:01	backup	
3	XGS3700-48HP	active	00:19:cb:00:03:01	linecard	
4	XGS3700-24	active	00:19:cb:00:04:01	linecard	
5	XGS3700-24HP	active	00:19:cb:00:05:01	linecard	
6	XGS3700-24	active	00:19:cb:00:06:01	linecard	
7	XGS3700-48HP	active	00:19:cb:00:07:01	linecard	
8	XGS3700-48HP	active	00:19:cb:00:08:01	linecard	

StackingTopology : Ring				
Slot No.	Stacking Channel 1		Stacking Channel 2	
	Neighbor	Speed	Neighbor	Speed
1	slot 2	10G	slot 8	10G
2	slot 3	10G	slot 1	10G
3	slot 4	10G	slot 2	10G
4	slot 5	10G	slot 3	10G
5	slot 6	10G	slot 4	10G
6	slot 7	10G	slot 5	10G
7	slot 8	10G	slot 6	10G
8	slot 1	10G	slot 7	10G

The following table describes the labels in this screen.

Table 32 Basic Setting > Stacking > Stacking Status

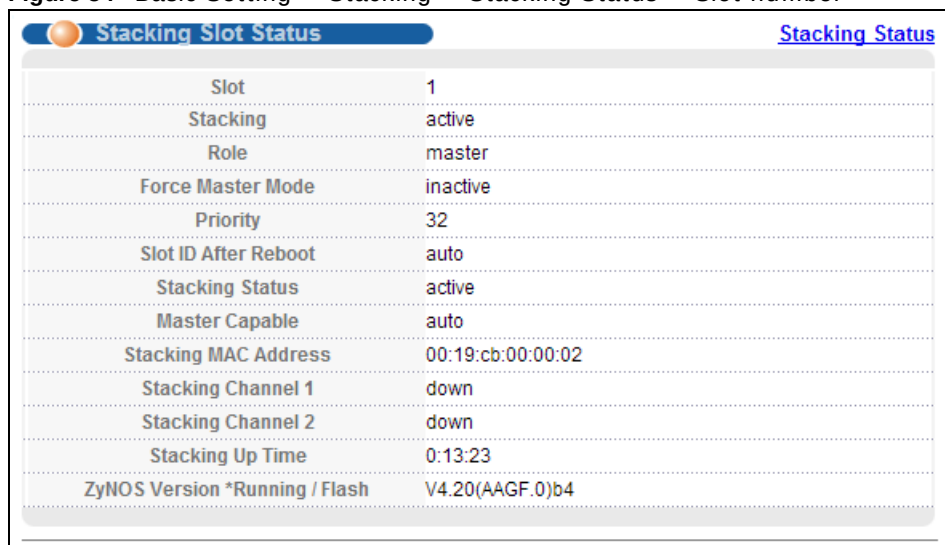
LABEL	DESCRIPTION
Slot	'Slot' refers to a Switch in the the 'virtual chassis' stack. This field displays the slot ID of the stacked Switch. You can click the ID number to go to the Stacking Slot Status screen.
Name	This field displays the model name of the stacked Switch.
Status	This field displays whether the stacked Switch is active or inactive in a stack system. Init means the slot ID is initialized by the master Switch.
MAC address	This field displays the MAC address of the stacked Switch.

Table 32 Basic Setting > Stacking > Stacking Status (continued)

LABEL	DESCRIPTION
Role	This field displays whether the Switch is a master, backup or linecard. There's only one master and one backup Switch in the stacking model; all others are linecard Switches.
Stacking Topology: Ring/Chain	
Slot No.	This field displays the slot ID number of the stacked Switch.
Stacking Channel1	
Neighbor	This field displays the neighbor Switch that is connected using slot channel 1 of the Switch.
Speed	This field displays the Ethernet speed of stacking channel 1 of the Switch.
Stacking Channel2	
Neighbor	This field displays the neighbor Switch that is connected to slot channel 2 of the Switch.
Speed	This field displays the Ethernet speed of stacking channel 2 of the Switch.

6.10.2 Stacking Slot

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

Figure 54 Basic Setting > Stacking > Stacking Status > Slot number


Slot	1
Stacking	active
Role	master
Force Master Mode	inactive
Priority	32
Slot ID After Reboot	auto
Stacking Status	active
Master Capable	auto
Stacking MAC Address	00:19:cb:00:00:02
Stacking Channel 1	down
Stacking Channel 2	down
Stacking Up Time	0:13:23
ZyNOS Version *Running / Flash	V4.20(AAGF.0)b4

The following table describes the labels in this screen.

Table 33 Basic Setting > Stacking > Stacking Status > Slot number

LABEL	DESCRIPTION
Slot	This field displays the slot ID of the Switch.
Stacking	This field displays whether the Switch is active in the stacking system.
Role	This field displays whether the stacked Switch is a master or linecard Switch.
Force Master Mode	This field displays whether the Force Master Mode is enabled or disabled on this Switch. The Active Force Master Mode forces this Switch to become a master Switch. This Switch will have the highest priority over all other Switch in the stack. If two Switches are set as masters, they will have the same priority level, but the Switch that has the longest active run-time will be selected as the master Switch automatically.

Table 33 Basic Setting > Stacking > Stacking Status > Slot number (continued)

LABEL	DESCRIPTION
Priority	This field displays the priority level of the Switch. A higher number represents higher priority.
Slot ID After Reboot	This field displays the slot ID of the Switch after a reboot. You can save the slot ID of the Switch after a reboot by clicking Freeze in the Stacking Configuration screen. See Section 6.10.3 on page 91 .
Stacking Status	This field displays whether the stacked Switch is active or inactive in a stack. Init means the slot ID is initialized by the master Switch.
Master Capable	This field displays whether the Switch has capacity to become a master Switch. Auto means the stack system master election process will determine if the Switch can be assigned as a master Switch.
Stacking MAC Address	This field displays the stacking Switch MAC address.
Stacking Channel 1	This field displays the status of the port stacking channel 1 of the Switch. It will display up for active or down for inactive.
Stacking Channel 2	This field displays the status of the port stacking channel 2 of the Switch. It will display up for active or down for inactive.
Stacking Up Time	This field displays the time that the active Switch in a stack has been running.
ZyNOS version *Running/Flash	This field displays the ZyNOS firmware that is currently running on the Switch.

6.10.3 Stacking Configuration

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

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

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

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

This is the master election priority in a stack system:

- 1 **Active Force Master Mode**
- 2 Highest **Stacking Priority**
- 3 Longest **System Up Time**

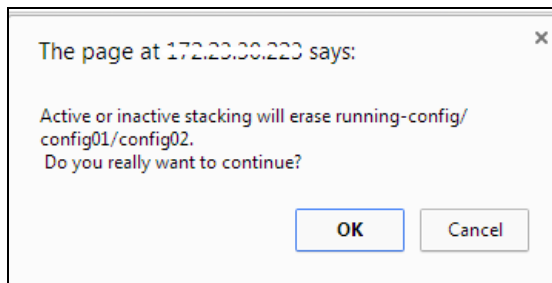
4 Lowest MAC Address

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

- a stacking port cable is disconnected
- a Switch in the stack reboots (as happens after you change stacking mode to standalone)
- you add a Switch to the stack or
- a Switch in the stack shuts down.

Use the following procedure to create a stack:

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



- 2 After reboot completes, the master LED will turn on.
- 3 Configure the Switch stacking priority to a high value, such as 63.
- 4 Change a second Switch to stacking mode and wait for it to finish rebooting automatically. This master LED will also turn on.
- 5 Connect the two Switches using the stacking ports for the Switch defined.
- 6 The second Switch master LED will then turn off, and its **Sys** LED will blink while it's initializing. Please wait until it stops blinking, indicating that it has joined the stack.
- 7 Repeat steps 4 to 6 to connect other Switches to the stack.

When the Switch is in Stacking mode, the web configurator will change port and VLAN port settings to support the stacking mode. See [Section 6.6 on page 64](#) and [Section 7.6 on page 99](#) for details on the port settings.

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

Figure 55 Basic Setting > Stacking > Configuration

Stacking Configuration [Stacking Status](#)

Active ☒

Apply Cancel

Active Force Master Mode ☐

System Priority

Apply Cancel

Slot ID :

Slot ID Freeze ☐ Freeze

Slot	MAC Address	Type	Slot ID After Reboot
1	00:19:cb:00:00:02	XGS3700-48HP	Auto ▼

Apply Cancel

The following table describes the labels in this screen.

Table 34 Basic Setting > Stacking > Configuration

LABEL	DESCRIPTION
Active	Select the Active check box to put the Switch in stacking mode. This will erase the running configuration, config01 and config02. The master Switch's login will remain unchanged. If you want to reload a previous configuration, please back one up first.
Apply	Click Apply to activate the stacking mode.
Cancel	Click Cancel to clear the Active check box.
Active Force Master Mode	Select the Active Force Master Mode check box to force this Switch to become a master Switch.
System Priority	Enter a number (from 1 to 63) to assign a priority for the stacking Switch. The higher the number, the higher the priority.
Apply	Click Apply to save the Active Force Master Mode and System Priority fields.
Cancel	Click Cancel to clear the Active Force Master Mode and System Priority fields.
Slot ID Freeze	Click the Freeze button to have the Switch retain its slot ID after reboot.
Slot	This field displays the slot or port channel of the stacked Switch.
MAC Address	This field displays the MAC address of the stacked Switch.
Type	This field displays the model name of the Switch.
Slot ID After Reboot	Choose Auto to have a new slot ID assigned after reboot. If you want to keep the original slot ID after reboot, you can click Freeze or select an ID in the Slot ID After Reboot list box.
Apply	Click Apply to save the Slot ID After reboot field.
Cancel	Click Cancel to clear the Slot ID After reboot field.

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

7.1 Introduction to IEEE 802.1Q Tagged VLANs

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

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

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

7.1.1 Forwarding Tagged and Untagged Frames

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

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

7.2 Automatic VLAN Registration

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

7.2.1 GARP

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

7.2.1.1 GARP Timers

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

7.2.2 GVRP

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

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

Table 35 IEEE 802.1Q VLAN Terminology

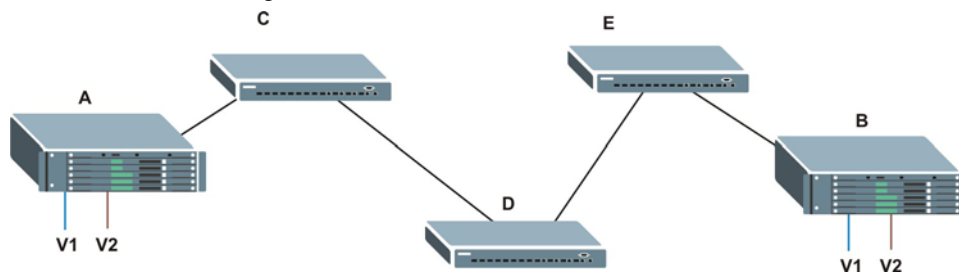
VLAN PARAMETER	TERM	DESCRIPTION
VLAN Type	Permanent VLAN	This is a static VLAN created manually.
	Dynamic VLAN	This is a VLAN configured by a GVRP registration/deregistration process.
VLAN Administrative Control	Registration Fixed	Fixed registration ports are permanent VLAN members.
	Registration Forbidden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

7.3 Port VLAN Trunking

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

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

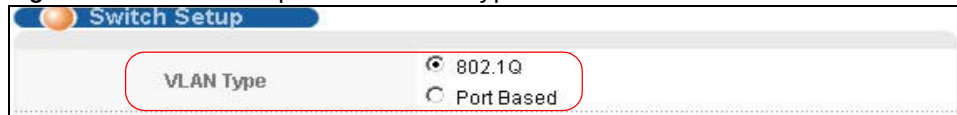
Figure 56 Port VLAN Trunking



7.4 Select the VLAN Type

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

Figure 57 Switch Setup: Select VLAN Type



7.5 802.1Q Static VLAN

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

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

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

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

7.5.1 VLAN Status

See [Section 7.1 on page 94](#) for more information on 802.1Q VLAN. Click **Advanced Application > VLAN** from the navigation panel to display the **VLAN Status** screen as shown next.

Figure 58 Advanced Application > VLAN: VLAN Status

Index	VID	Elapsed Time	Status
1	1	1:57:22	Static
2	463	1:57:21	Static
3	464	1:57:21	Static
4	465	1:57:21	Static
5	1111	0:10:32	Private
6	1234	1:57:21	Static

The following table describes the labels in this screen.

Table 36 Advanced Application > VLAN: VLAN Status

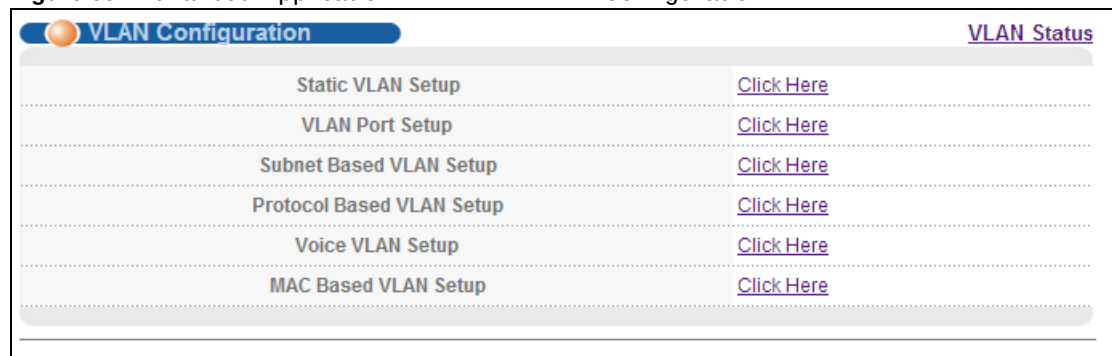
LABEL	DESCRIPTION
VLAN Search by VID	Enter an existing VLAN ID number(s) (separated by a comma) and click Search to display only the specified VLAN(s) in the list below. Leave this field blank and click Search to display all VLANs configured on the Switch.
The Number of VLAN	This is the number of VLANs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

Table 37 Advanced Application > VLAN > VLAN Detail (continued)

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

7.6 VLAN Configuration

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

Figure 60 Advanced Application > VLAN > VLAN Configuration

The following table describes the labels in the above screen.

Table 38 Advanced Application > VLAN > VLAN Configuration

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

7.6.1 Configure a Static VLAN or Private VLAN

Use this screen to create 802.1Q VLAN IDs and set VLAN members for **Normal** (static) or **Private** (**Primary**, **Isolated** or **Community**) VLANs. You must create VLAN IDs for **Private** (**Primary**, **Isolated** or **Community**) VLANs before configuring **Advanced Application > Private VLAN**. See [Section 7.1 on page 94](#) for more information on 802.1Q VLAN.

To configure a static or private VLAN, click **Static VLAN Setup** in the **VLAN Configuration** screen to display the screen as shown next.

Figure 61 Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup

Static VLAN VLAN Configuration

ACTIVE ☐

Name

VLAN Group ID

VLAN Type
☒ Normal
☐ Private

Association VLAN List

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 Cancel Clear

VID	Active	Name	VLAN Type	Association VLAN List	Delete
1	Yes	1	Normal		☐
221	Yes	C1	Private-Community		☐
463	Yes		Normal		☐
464	Yes		Normal		☐
465	Yes		Normal		☐
1111	Yes	PV1111	Private-Primary	221	☐
1234	Yes	V1234	Normal		☐

Delete Cancel

The following table describes the related labels in this screen.

Table 39 Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup

LABEL	DESCRIPTION
ACTIVE	Select this check box to activate the VLAN settings.
Name	Enter a descriptive name for the VLAN group for identification purposes. This name consists of up to 64 printable characters; spaces are allowed.
VLAN Group ID	Enter the VLAN ID for this static entry; the valid range is between 1 and 4094.
VLAN Type	Select Normal (static) or Private . For Private VLANs, select Primary , Isolated or Community .

Table 39 Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup (continued)

LABEL	DESCRIPTION
Association VLAN List	Primary private VLANs can associate with several (secondary) Community private VLANs and up to one (secondary) Isolated private VLAN. You only configure VLAN Association List for Primary private VLANs. Use a dash to associate consecutive VLANs and a comma (no spaces) to associate non-consecutive VLANs. For example, 51-53 includes 51, 52 and 53, but 51,53 does not include 52. Secondary private VLANs can only be associated with one primary private VLAN.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port	The port number identifies the port you are configuring. In stacking mode, the first number represents the slot and the second the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Control	Select Normal for the port to dynamically join this VLAN group using GVRP. This is the default selection. Select Fixed for the port to be a permanent member of this VLAN group. Select Forbidden if you want to prohibit the port from joining this VLAN group.
Tagging	Select TX Tagging if you want the port to tag all outgoing frames transmitted with this VLAN Group ID.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to reset the fields to the factory defaults.
VID	This field displays the ID number of the VLAN group. Click the number to edit the VLAN settings.
Active	This field indicates whether the VLAN settings are enabled (Yes) or disabled (No).
Name	This field displays the descriptive name for this VLAN group.
VLAN Type	This field displays the Normal or Private (Primary, Isolated or Community) type VLAN configured in the top part of this screen.
Association VLAN List	This field displays which secondary private VLANs are associated with a primary private VLAN configured in the top part of this screen.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

7.6.2 Configure VLAN Port Settings

Use the VLAN Port Setting screen to configure the static VLAN (IEEE 802.1Q) settings on a port. See [Section 7.1 on page 94](#) for more information on 802.1Q VLAN. Click the **VLAN Port Setup** link in the **VLAN Configuration** screen.

Figure 62 Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup: Standalone mode

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

Figure 63 Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup: Stacking mode

Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking	Isolation
1/*	☐		☐	All	☐	☐
1/1	☐	1	☐	All	☐	☐
1/2	☐	1	☐	All	☐	☐
1/3	☐	1	☐	All	☐	☐
1/48	☐	1	☐	All	☐	☐
1/9	☐	1	☐	All	☐	☐

Apply Cancel

The following table describes the labels in this screen.

Table 40 Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup: Standalone/ Stacking mode

LABEL	DESCRIPTION
GVRP	GVRP (GARP VLAN Registration Protocol) is a registration protocol that defines a way for switches to register necessary VLAN members on ports across the network. Select this check box to permit VLAN groups beyond the local Switch.
SLOT1	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch.

Table 40 Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup: Standalone/ Stacking mode (continued)

LABEL	DESCRIPTION
Port	This field displays the port number of the Switch. In stacking mode, the first number represents the slot and the second the port number. Please note that the default stacking ports (the last two ports of your Switch) cannot be configured. They are reserved for stacking only.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Ingress Check	If this check box is selected for a port, the Switch discards incoming frames for VLANs that do not include this port in its member set. Clear this check box to disable ingress filtering.
PVID	A PVID (Port VLAN ID) is a tag that adds to incoming untagged frames received on a port so that the frames are forwarded to the VLAN group that the tag defines. Enter a number between 1 and 4094 as the port VLAN ID.
GVRP	Select this check box to allow GVRP on this port.
Acceptable Frame Type	Specify the type of frames allowed on a port. Choices are All , Tag Only and Untag Only . Select All from the drop-down list box to accept all untagged or tagged frames on this port. This is the default setting. Select Tag Only to accept only tagged frames on this port. All untagged frames will be dropped. Select Untag Only to accept only untagged frames on this port. All tagged frames will be dropped. Note that when the Switch is in stacking mode and the master Switch has VLAN1, all other ports will be configured to untagged port.
VLAN Trunking	Enable VLAN Trunking on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the Switch.
Isolation	Select this to allows this port to communicate only with the CPU management port and the ports on which the isolation feature is not enabled.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

7.6.3 Subnet Based VLANs

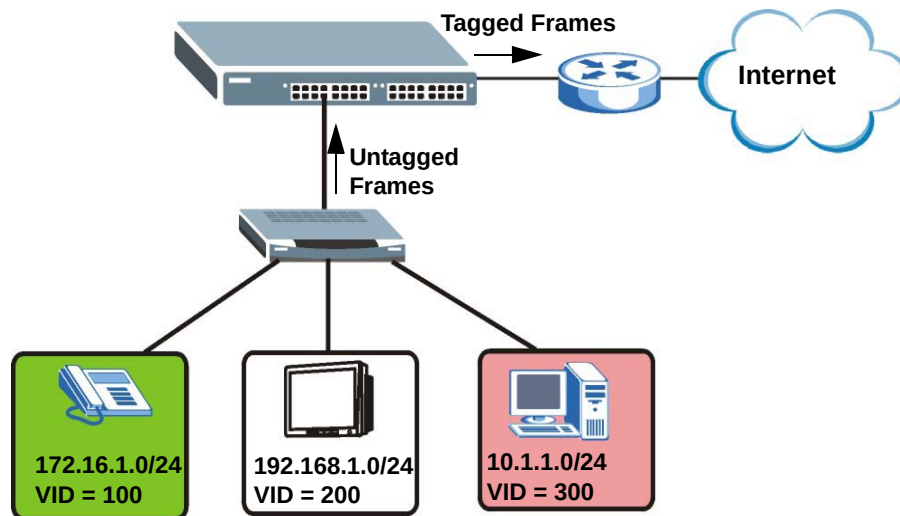
Subnet based VLANs allow you to group traffic into logical VLANs based on the source IP subnet you specify. When a frame is received on a port, the Switch checks if a tag is added already and the IP subnet it came from. The untagged packets from the same IP subnet are then placed in the same subnet based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

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

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

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

Figure 64 Subnet Based VLAN Application Example



7.6.3.1 Configuring Subnet Based VLAN

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

Figure 65 Advanced Application > VLAN > VLAN Configuration > > Subnet Based VLAN Setup

Subnet Based VLAN [VLAN Configuration](#)

Active ☐

DHCP-Vlan Override ☐

Apply

Active ☐

Name

IP

Mask-Bits

VID

Priority

Add Cancel

Index	Active	Name	IP	Mask-Bits	VID	Priority	Delete
Delete Cancel							

The following table describes the labels in this screen.

Table 41 Advanced Application > VLAN > VLAN Configuration > Subnet Based VLAN Setup

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

Table 41 Advanced Application > VLAN > VLAN Configuration > Subnet Based VLAN Setup

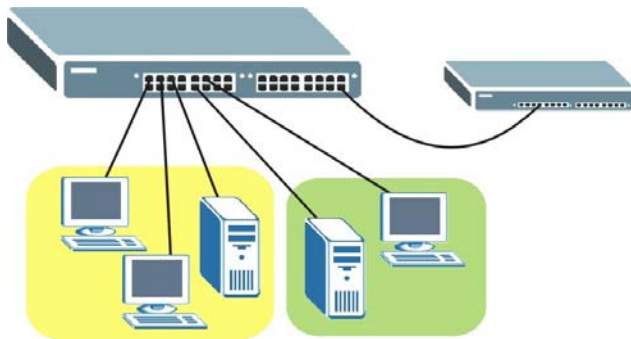
LABEL	DESCRIPTION
Index	This is the index number identifying this subnet based VLAN. Click on any of these numbers to edit an existing subnet based VLAN.
Active	This field shows whether the subnet based VLAN is active or not.
Name	This field shows the name the subnet based VLAN.
IP	This field shows the 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.

7.6.4 Protocol Based VLANs

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

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

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

Figure 66 Protocol Based VLAN Application Example

7.6.4.1 Configuring Protocol Based VLAN

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

Figure 67 Advanced Application > VLAN > VLAN Configuration > Protocol Based VLAN Setup

The following table describes the labels in this screen.

Table 42 Advanced Application > VLAN > VLAN Configuration > Protocol Based VLAN Setup

LABEL	DESCRIPTION
Active	Select this check box to activate this protocol based VLAN.
Port	Type a port number to be included in this protocol based VLAN. In stacking mode, the first box field is the slot ID and the second field is the port number. This port must belong to a static VLAN in order to participate in a protocol based VLAN. See Chapter 7 on page 94 for more details on setting up VLANs.
Name	Enter up to 32 alphanumeric characters to identify this protocol based VLAN.
Ethernet-type	Use the drop down list box to select a predefined protocol to be included in this protocol based VLAN or select Others and type the protocol number in hexadecimal notation. For example, the IP protocol in hexadecimal notation is 0800, and Novell IPX protocol is 8137. Note: Protocols in the hexadecimal number range of 0x0000 to 0x05ff are not allowed to be used for protocol based VLANs.
VID	Enter the ID of a VLAN to which the port belongs. This must be an existing VLAN which you defined in the Advanced Application > VLAN > Static VLAN screen.
Priority	Select the priority level that the Switch will assign to frames belonging to this VLAN.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Index	This is the index number identifying this protocol based VLAN. Click on any of these numbers to edit an existing protocol based VLAN.
Active	This field shows whether the protocol based VLAN is active or not.
Port	This field shows which port belongs to this protocol based VLAN. In stacking mode, the first number represents the slot and the second the port number.

Table 42 Advanced Application > VLAN > VLAN Configuration > Protocol Based VLAN Setup

LABEL	DESCRIPTION
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.

7.6.4.2 Create an IP-based VLAN Example

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

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

Figure 68 Protocol Based VLAN Configuration Example

Protocol Based VLAN

Active ☒

Port

Name

Ethernet-type ☒ IP ☐ Others (Hex)

VID

Priority

Index	Active	Port	Name	Ethernet-type	VID	Priority	Delete

EXAMPLE

To add more ports to this protocol based VLAN.

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

- 3 Click **Add**.

7.6.5 View Private VLAN Status

Use this screen to view all private VLANs created on the Switch. See also **Advanced Application > Private VLAN**.

Click **Private VLAN Status** in the **VLAN Status** screen to display the screen as shown next.

Figure 69 Advanced Application > VLAN > Private VLAN Status

Primary VLAN	Secondary VLAN	Type	Port List
1111		Primary	1-4
1111	221	Community	

Change Pages: Previous Next

The following table describes the labels in this screen.

Table 43 Advanced Application > VLAN > Private VLAN Status

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

7.7 Port-based VLAN Setup (Standalone Mode)

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

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

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

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

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

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

7.7.1 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.

[illegible]

[illegible]

The following table describes the labels in this screen.

Advanced Application > VLAN: Port Based VLAN Setup

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

7.8 Voice VLAN

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

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

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

Figure 72 Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup

Voice VLAN Setup [VLAN Configuration](#)

Voice VLAN Global Setup

Voice VLAN ☒ Disable

Priority

Voice VLAN OUI Setup

OUI address

OUI mask

Description

Index	OUI address	OUI mask	Description	Delete

The following table describes the fields in the above screen.

Table 44 Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup

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

Table 44 Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup

LABEL	DESCRIPTION
OUI mask	This field displays the OUI mask address of the Voice VLAN.
Description	This field displays the description of the Voice VLAN with OUI address.
Delete	Click the Delete check box to select Voice VLAN OUI entry you wish to remove.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

7.9 MAC-based VLAN

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

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

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

Figure 73 Advanced Application > VLAN > VLAN Configuration > MAC-based VLAN Setup

The following table describes the fields in the above screen.

Table 45 Advanced Application > VLAN > VLAN Configuration > MAC-based VLAN Setup

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

Table 45 Advanced Application > VLAN > VLAN Configuration > MAC-based VLAN Setup

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

Static MAC Forward Setup

Use these screens to configure static MAC address forwarding.

8.1 Overview

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

8.2 Configuring Static MAC Forwarding

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

Static MAC address forwarding together with port security allows only computers in the MAC address table on a port to access the Switch. See [Chapter 17 on page 182](#) for more information on port security.

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

Figure 74 Advanced Application > Static MAC Forwarding (Standalone mode)

Static MAC Forwarding

Active ☐

Name

MAC Address : : : : :

VID

Port

Add Cancel Clear

Index	Active	Name	MAC Address	VID	Port	Delete
Delete Cancel						

Figure 75 Advanced Application > Static MAC Forwarding (Stacking mode)

Static MAC Forwarding

Active ☒

Name

MAC Address : : : : :

VID

Port /

Index	Active	Name	MAC Address	VID	Port	Delete
Delete Cancel						

The following table describes the labels in this screen.

Table 46 Advanced Application > Static MAC Forwarding

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Enter a descriptive name for identification purposes for this static MAC address forwarding rule.
MAC Address	Enter the MAC address in valid MAC address format, that is, six hexadecimal character pairs. Note: Static MAC addresses do not age out.
VID	Enter the VLAN identification number.
Port(standalone or stacking mode)	Enter the port where the MAC address entered in the previous field will be automatically forwarded. In stacking mode, the first box field is the slot ID and the second field is the port number.
Add	Click this to create a new entry or to update an existing one. This saves your rule to the Switch's run-time memory. The Switch loses this rule if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to reset the fields to the factory defaults.
Index	Click an index number to modify a static MAC address rule for a port.
Active	This field displays whether this static MAC address forwarding rule is active (Yes) or not (No). You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for this static MAC address-forwarding rule.
MAC Address	This field displays the MAC address that will be forwarded and the VLAN identification number to which the MAC address belongs.
VID	This field displays the ID number of the VLAN group.
Port	This field displays the port where the MAC address shown in the next field will be forwarded. In stacking mode, the first number represents the slot and the second the port number.

Table 46 Advanced Application > Static MAC Forwarding (continued)

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

Static Multicast Forward Setup

Use these screens to configure static multicast address forwarding.

9.1 Static Multicast Forwarding Overview

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

If a multicast group has no members, then the switch will either flood the multicast frames to all ports or drop them. You can configure this in the **Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping** screen (see [Section 23.3.1 on page 217](#)). [Figure 76](#) 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 77](#) shows frames being forwarded to devices connected to port 3. [Figure 78](#) shows frames being forwarded to ports 2 and 3 within VLAN group 4.

Figure 76 No Static Multicast Forwarding

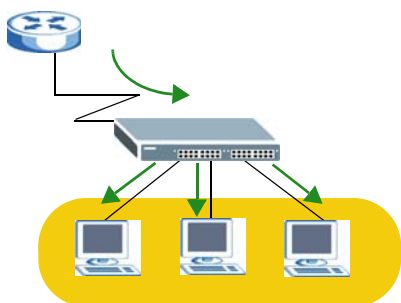


Figure 77 Static Multicast Forwarding to A Single Port

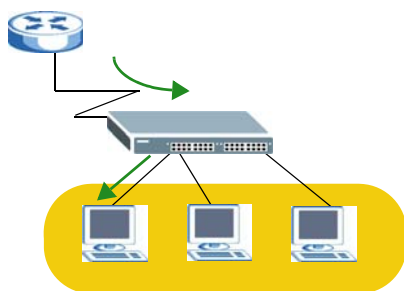
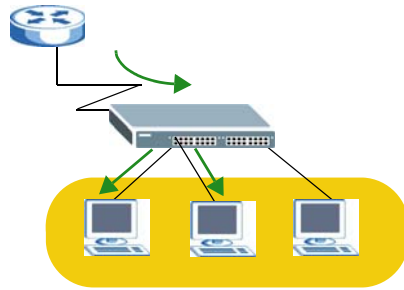


Figure 78 Static Multicast Forwarding to Multiple Ports

9.2 Configuring Static Multicast Forwarding

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

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

Figure 79 Advanced Application > Static Multicast Forwarding

The following table describes the labels in this screen.

Table 47 Advanced Application > Static Multicast Forwarding

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Type a descriptive name (up to 32 printable ASCII characters) for this static multicast MAC address forwarding rule. This is for identification only.
MAC Address	Enter a multicast MAC address which identifies the multicast group. The last binary bit of the first octet pair in a multicast MAC address must be 1. For example, the first octet pair 00000001 is 01 and 00000011 is 03 in hexadecimal, so 01:00:5e:00:00:0A and 03:00:5e:00:00:27 are valid multicast MAC addresses.
VID	You can forward frames with matching destination MAC address to port(s) within a VLAN group. Enter the ID that identifies the VLAN group here. If you don't have a specific target VLAN, enter 1.

Table 47 Advanced Application > Static Multicast Forwarding (continued)

LABEL	DESCRIPTION
Port	Enter the port(s) where frames with destination MAC address that matched the entry above are forwarded. You can enter multiple ports separated by (no space) comma (,) or hyphen for a range. For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7. In stacking mode, the first number represents the slot and the second the port number. Enter 1/1-1/24,2/28 for ports 1 to 24 for the Switch in slot 1 and port 28 for the Switch in slot 2, for example.
Add	Click this to create a new entry or to update an existing one. This saves your rule to the Switch's run-time memory. The Switch loses this rule if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to their last saved values.
Clear	Click Clear to reset the fields to the factory defaults.
Index	Click an index number to modify a static multicast MAC address rule for port(s).
Active	This field displays whether a static multicast MAC address forwarding rule is active (Yes) or not (No). You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for a static multicast MAC address-forwarding rule.
MAC Address	This field displays the multicast MAC address that identifies a multicast group.
VID	This field displays the ID number of a VLAN group to which frames containing the specified multicast MAC address will be forwarded.
Port	This field displays the port(s) within a identified VLAN group to which frames containing the specified multicast MAC address will be forwarded.
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.

10.1 Configure a Filtering Rule

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

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

Figure 80 Advanced Application > Filtering

The following table describes the related labels in this screen.

Table 48 Advanced Application > Filtering

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

Table 48 Advanced Application > Filtering (continued)

LABEL	DESCRIPTION
MAC	Type a MAC address in a valid MAC address format, that is, six hexadecimal character pairs.
VID	Type the VLAN group identification number.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to reset the fields to the factory defaults.
Index	This field displays the index number of the rule. Click an index number to change the settings.
Active	This field displays Yes when the rule is activated and No when is it deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purposes only.
MAC Address	This field displays the source/destination MAC address with the VLAN identification number to which the MAC address belongs.
VID	This field displays the VLAN group identification number.
Action	This field displays Discard source , Discard destination , or Discard both depending on what you configured above.
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.

11.1 STP/RSTP Overview

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

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

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

11.1.1 STP Terminology

The root bridge is the base of the spanning tree.

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

Table 49 STP Path Costs

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

Table 49 STP Path Costs

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

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

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

11.1.2 How STP Works

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

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

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

11.1.3 STP Port States

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

Table 50 STP Port States

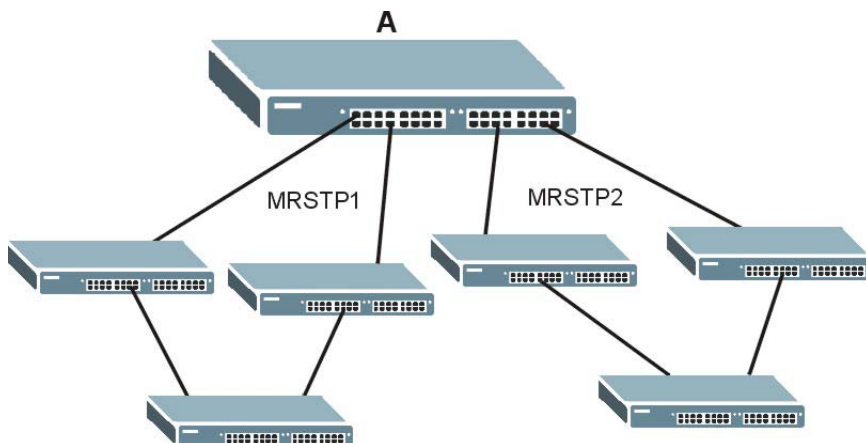
PORT STATE	DESCRIPTION
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.
Listening	All BPDUs are received and processed. Note: The listening state does not exist in RSTP.
Learning	All BPDUs are received and processed. Information frames are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

11.1.4 Multiple RSTP

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

In the following example, there are two RSTP instances (**MRSTP1** and **MRSTP2**) on switch **A**.

Figure 81 MRSTP Network Example



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

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

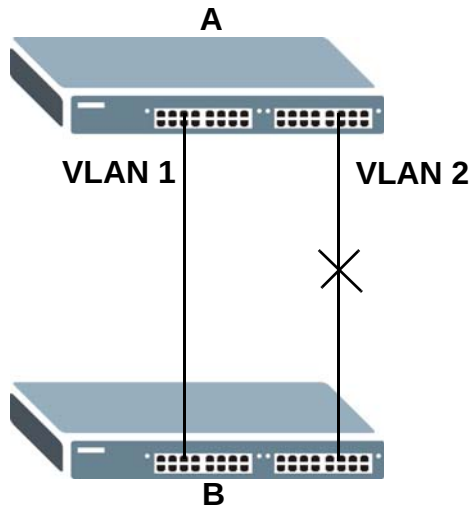
11.1.5 Multiple STP

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

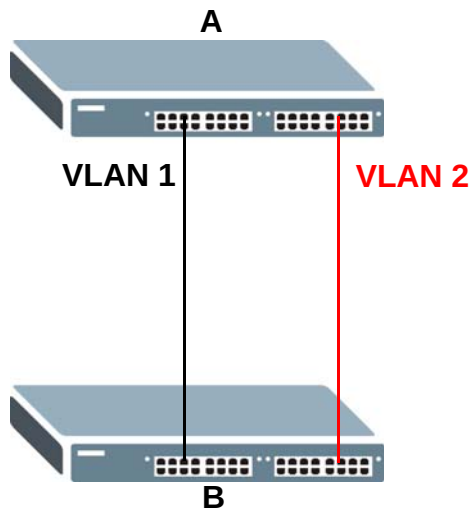
- One Common and Internal Spanning Tree (CIST) that represents the entire network's connectivity.
- Grouping of multiple bridges (or switching devices) into regions that appear as one single bridge on the network.
- A VLAN can be mapped to a specific Multiple Spanning Tree Instance (MSTI). MSTI allows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

11.1.5.1 MSTP Network Example

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

Figure 82 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 83 MSTP Network Example

11.1.5.2 MST Region

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

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

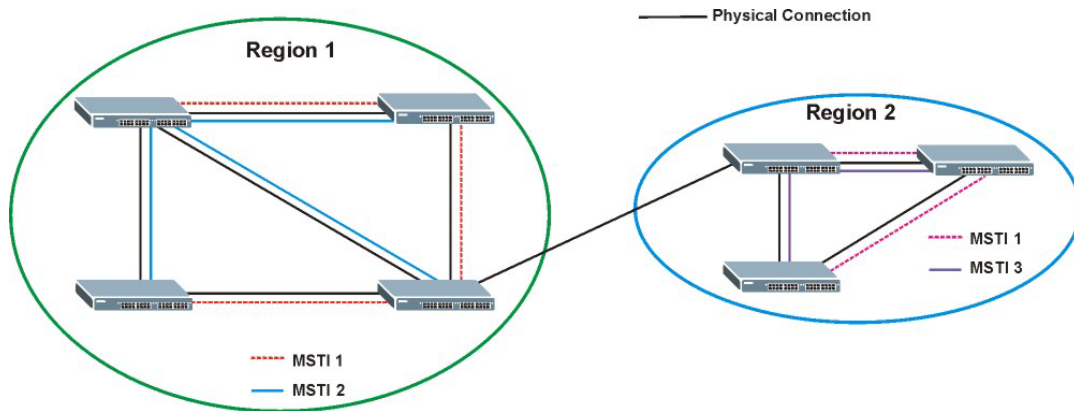
- Name of the MST region
- Revision level as the unique number for the MST region
- VLAN-to-MST Instance mapping

11.1.5.3 MST Instance

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

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

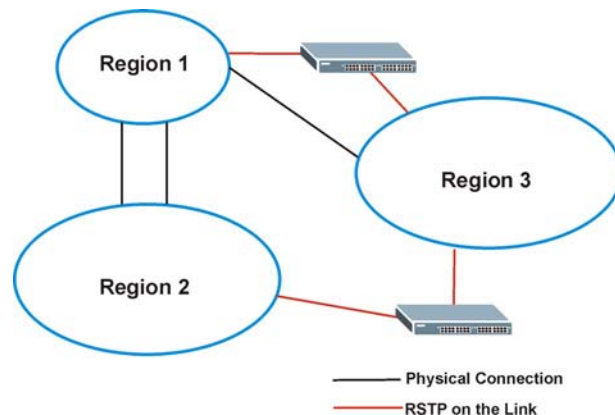
Figure 84 MSTIs in Different Regions



11.1.5.4 Common and Internal Spanning Tree (CIST)

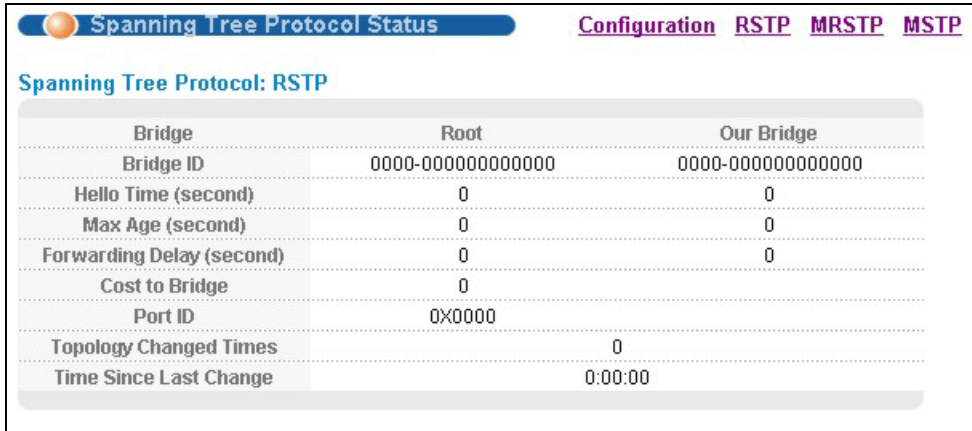
A CIST represents the connectivity of the entire network and it is equivalent to a spanning tree in an STP/RSTP. The CIST is the default MST instance (MSTID 0). Any VLANs that are not members of an MST instance are members of the CIST. In an MSTP-enabled network, there is only one CIST that runs between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

Figure 85 MSTP and Legacy RSTP Network Example



11.2 Spanning Tree Protocol Status Screen

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

Figure 86 Advanced Application > Spanning Tree Protocol


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.

11.3 Spanning Tree Configuration

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

Figure 87 Advanced Application > Spanning Tree Protocol > Configuration


Spanning Tree Mode

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

Apply Cancel

The following table describes the labels in this screen.

Table 51 Advanced Application > Spanning Tree Protocol > Configuration

LABEL	DESCRIPTION
Spanning Tree Mode	You can activate one of the STP modes on the Switch. Select Rapid Spanning Tree , Multiple Rapid Spanning Tree or Multiple Spanning Tree . See Section 11.1 on page 125 for background information on STP.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

11.4 Configure Rapid Spanning Tree Protocol

Use this screen to configure RSTP settings, see [Section 11.1 on page 125](#) for more information on RSTP. Click **RSTP** in the **Advanced Application > Spanning Tree Protocol** screen.

Figure 88 Advanced Application > Spanning Tree Protocol > RSTP (Standalone mode)

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
8	☐	☐	128	4

Figure 89 Advanced Application > Spanning Tree Protocol > RSTP (Stacking mode)

Rapid Spanning Tree Protocol [Status](#)

Active ☐

Bridge Priority

Hello Time Seconds

MAX Age Seconds

Forwarding Delay Seconds

SLOT 1

Port	Active	Edge	Priority	Path Cost
*	☐	☐		
1/1	☐	☐	128	4
1/2	☐	☐	128	2
1/3	☐	☐	128	2
1/4	☐	☐	128	2

The following table describes the labels in this screen.

Table 52 Advanced Application > Spanning Tree Protocol > RSTP

LABEL	DESCRIPTION
Status	Click Status to display the RSTP Status screen (see Figure 90 on page 134).
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.

Table 52 Advanced Application > Spanning Tree Protocol > RSTP (continued)

LABEL	DESCRIPTION
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: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone and stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to activate RSTP on this port.
Edge	Select this check box to configure a port as an edge port when it is directly attached to a computer. An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).
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 49 on page 125 for more information.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

11.5 Rapid Spanning Tree Protocol Status

Click **Advanced Application > Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See [Section 11.1 on page 125](#) for more information on RSTP.

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

Figure 90 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 53 Advanced Application > Spanning Tree Protocol > Status: RSTP

LABEL	DESCRIPTION
Configuration	Click Configuration to specify which STP mode you want to activate. Click RSTP to edit RSTP settings on the Switch.
Bridge	Root refers to the base of the spanning tree (the root bridge). Our Bridge is this Switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of the bridge priority plus the MAC address. This ID is the same for Root and Our Bridge if the Switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay.
Max Age (second)	This is the maximum time (in seconds) a switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding). See Section 11.1.3 on page 126 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.

11.6 Configure Multiple Rapid Spanning Tree Protocol

To configure MRSTP, click **MRSTP** in the **Advanced Application > Spanning Tree Protocol** screen. See [Section 11.1 on page 125](#) for more information on MRSTP.

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

Multiple Rapid Spanning Tree Protocol Status

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 ▼
6	☐	☐	128	4	1 ▼
7	☐	☐	128	4	1 ▼
8	☐	☐			

Apply Cancel

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

Multiple Rapid Spanning Tree Protocol Status

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

SLOT 1 ▼

Port	Active	Edge	Priority	Path Cost	Tree
1/*	☐	☐			1 ▼
1/1	☐	☐	128	4	1 ▼
1/2	☐	☐	128	4	1 ▼
1/49	☐	☐	128	2	1 ▼
1/50	☐	☐	128	2	1 ▼

Apply Cancel

The following table describes the labels in this screen.

Table 54 Advanced Application > Spanning Tree Protocol > MRSTP

LABEL	DESCRIPTION
Status	Click Status to display the MRSTP Status screen (see Figure 93 on page 137).
Tree	This is a read only index number of the STP trees.
Active	Select this check box to activate an STP tree. Clear this checkbox to disable an STP tree. Note: You must also activate Multiple Rapid Spanning Tree in the Advanced Application > Spanning Tree Protocol > Configuration screen to enable MRSTP on the Switch.
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Max Age	This is the maximum time (in seconds) a switch can wait without receiving a BPDU before attempting to reconfigure. All switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) a switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: Note: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to activate STP on this port.
Edge	Select this check box to configure a port as an edge port when it is directly attached to a computer. An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).

Table 54 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 49 on page 125 for more information.
Tree	Select which STP tree configuration this port should participate in.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

11.7 Multiple Rapid Spanning Tree Protocol Status

Click **Advanced Application > Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See [Section 11.1 on page 125](#) for more information on MRSTP.

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

Figure 93 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 55 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.

Table 55 Advanced Application > Spanning Tree Protocol > Status: MRSTP (continued)

LABEL	DESCRIPTION
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.

11.8 Configure Multiple Spanning Tree Protocol

To configure MSTP, click **MSTP** in the **Advanced Application > Spanning Tree Protocol** screen. See [Section 11.1.5 on page 127](#) for more information on MSTP.

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

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	0019cb004701
Revision Number	0

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
7	☐	128	4

Instance	VLAN	Active Port	Delete
0	1-4094	-	Delete Cancel

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

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	0019cb000002
Revision Number	0

Instance:

Instance	
Bridge Priority	32768 ▼
VLAN Range	Start End Add Remove
	Clear
Enabled VLAN(s)	

SLOT 1 ▼

Port	Active	Priority	Path Cost
*	☐		
1/1	☐	128	4
1/2	☐	128	4
1/48	☐	128	4
1/49	☐	128	2

Instance	VLAN	Active Port	Delete
0	1-4094	-	Delete

The following table describes the labels in this screen.

Table 56 Advanced Application > Spanning Tree Protocol > MSTP

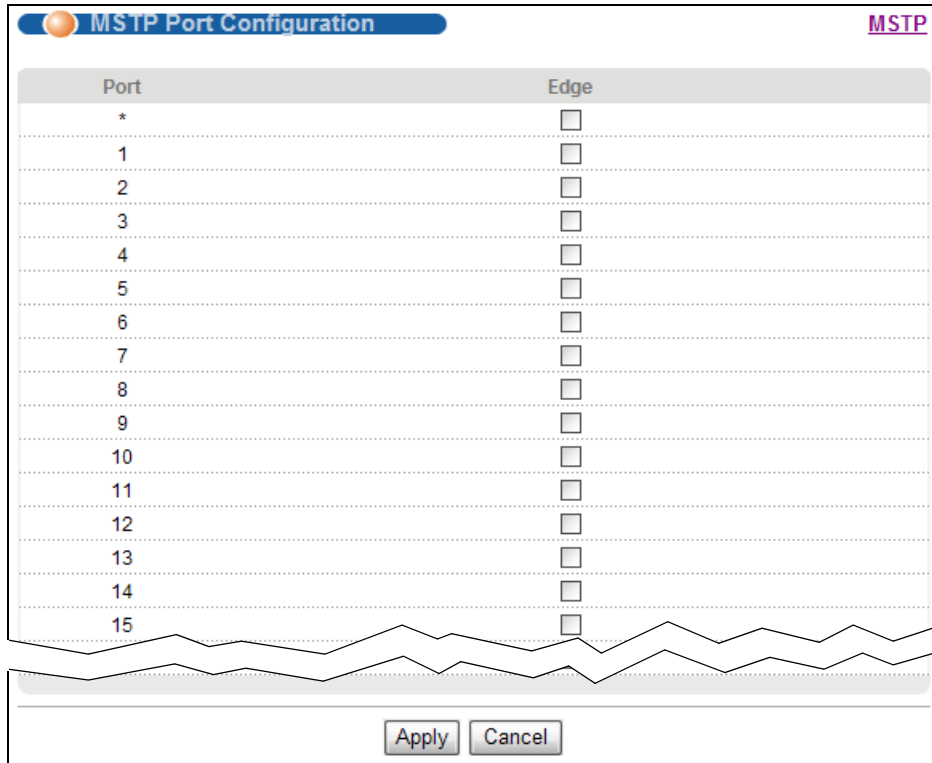
LABEL	DESCRIPTION
Status	Click Status to display the MSTP Status screen (see Figure 98 on page 144).
Active	Select this check box to activate MSTP on the Switch. Clear this checkbox to disable MSTP on the Switch. Note: You must also activate Multiple Spanning Tree in the Advanced Application > Spanning 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.
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.

Table 56 Advanced Application > Spanning Tree Protocol > MSTP (continued)

LABEL	DESCRIPTION
Enabled VLAN(s)	This field displays which VLAN(s) are mapped to this MST instance.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
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 49 on page 125 for more information.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses this change if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Instance	This field displays the ID of an MST instance.
VLAN	This field displays the VID (or VID ranges) to which the MST instance is mapped.
Active Port	This field display the ports configured to participate in the MST instance.
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.

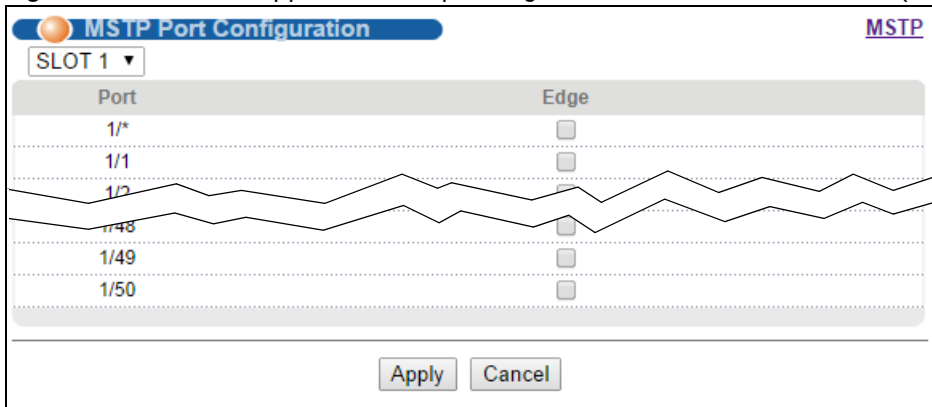
11.8.1 Multiple Spanning Tree Protocol Port Configuration

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

Figure 96 Advanced Application > Spanning Tree Protocol > MSTP > Port (Standalone mode)


The screenshot shows the 'MSTP Port Configuration' window in standalone mode. It features a table with two columns: 'Port' and 'Edge'. The 'Port' column lists ports from 1 to 15, with a '*' symbol above the first row. The 'Edge' column contains checkboxes for each port. At the bottom, there are 'Apply' and 'Cancel' buttons.

Port	Edge
*	☐
1	☐
2	☐
3	☐
4	☐
5	☐
6	☐
7	☐
8	☐
9	☐
10	☐
11	☐
12	☐
13	☐
14	☐
15	☐

Figure 97 Advanced Application > Spanning Tree Protocol > MSTP > Port (Stacking mode)


The screenshot shows the 'MSTP Port Configuration' window in stacking mode. It includes a 'SLOT 1' drop-down menu at the top left. The table below has two columns: 'Port' and 'Edge'. The 'Port' column lists ports 1/*, 1/1, 1/2, 1/48, 1/49, and 1/50. The 'Edge' column contains checkboxes for each port. At the bottom, there are 'Apply' and 'Cancel' buttons.

Port	Edge
1/*	☐
1/1	☐
1/2	☐
1/48	☐
1/49	☐
1/50	☐

The following table describes the labels in this screen.

Table 57 Advanced Application > Spanning Tree Protocol > MSTP > Port

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.

Table 57 Advanced Application > Spanning Tree Protocol > MSTP > Port (continued)

LABEL	DESCRIPTION
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
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.

11.9 Multiple Spanning Tree Protocol Status

Click **Advanced Application > Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See [Section 11.1.5 on page 127](#) for more information on MSTP.

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

Figure 98 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 58 Advanced Application > Spanning Tree Protocol > Status: MSTP

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

Bandwidth Control

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

12.1 Bandwidth Control Overview

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

12.1.1 CIR and PIR

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

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

Note: The CIR should be less than the PIR.

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

12.2 Bandwidth Control Setup

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

Figure 99 Advanced Application > Bandwidth Control (Standalone mode)

Port	Active	Ingress Rate				Active	Egress Rate	
		Commit Rate	Active	Peak Rate	Active			
*	☐		Kbps ☐		Kbps ☐	☐		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
9	☐	1	Kbps ☐	1	Kbps ☐	☐	1	Kbps

Apply Cancel

Figure 100 Advanced Application > Bandwidth Control (Stacking mode)

Port	Active	Ingress Rate				Active	Egress Rate	
		Commit Rate	Active	Peak Rate	Active			
1/*	☐		Kbps ☐		Kbps ☐	☐		Kbps
1/1	☐	1	Kbps ☐	1	Kbps ☐	☐	1	Kbps
1/2	☐	1	Kbps ☐	1	Kbps ☐	☐	1	Kbps
1/3	☐		Kbps ☐		Kbps ☐	☐		Kbps
1/4	☐		Kbps ☐		Kbps ☐	☐		Kbps
1/5	☐	1	Kbps ☐	1	Kbps ☐	☐	1	Kbps
1/6	☐		Kbps ☐		Kbps ☐	☐		Kbps
1/7	☐		Kbps ☐		Kbps ☐	☐		Kbps
1/8	☐		Kbps ☐		Kbps ☐	☐		Kbps
1/9	☐		Kbps ☐		Kbps ☐	☐		Kbps
1/10	☐	1	Kbps ☐	1	Kbps ☐	☐	1	Kbps

Apply Cancel

The following table describes the related labels in this screen.

Table 59 Advanced Application > Bandwidth Control

LABEL	DESCRIPTION
Active	Select this check box to enable bandwidth control on the Switch.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.

Table 59 Advanced Application > Bandwidth Control (continued)

LABEL	DESCRIPTION
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Ingress Rate	
Active	Select this check box to activate commit rate limits on this port.
Commit Rate	Specify the guaranteed bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port. The commit rate should be less than the peak rate. The sum of commit rates cannot be greater than or equal to the uplink bandwidth.
Active	Select this check box to activate peak rate limits on this port.
Peak Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port.
Active	Select this check box to activate egress rate limits on this port.
Egress Rate	Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the out-going traffic flow on a port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

Broadcast Storm Control

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

13.1 Broadcast Storm Control Setup

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

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

Figure 101 Advanced Application > Broadcast Storm Control (Standalone mode)

Broadcast Storm Control

Active ☐

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
9	☐ 0	☐ 0	☐ 0

Apply Cancel

Figure 102 Advanced Application > Broadcast Storm Control (Stacking mode)

Broadcast Storm Control

Active ☐

SLOT 1 ▼

Port	Broadcast (pkt/s)	Multicast (pkt/s)	DLF (pkt/s)
1/*	☐	☐	☐
1/1	☐ 0	☐ 0	☐ 0
1/2	☐ 0	☐ 0	☐ 0
1/49	☐ 0	☐ 0	☐ 0

Apply Cancel

The following table describes the labels in this screen.

Table 60 Advanced Application > Broadcast Storm Control

LABEL	DESCRIPTION
Active	Select this check box to enable traffic storm control on the Switch. Clear this check box to disable this feature.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Broadcast (pkt/s)	Select this option and specify how many broadcast packets the port receives per second.
Multicast (pkt/s)	Select this option and specify how many multicast packets the port receives per second.
DLF (pkt/s)	Select this option and specify how many destination lookup failure (DLF) packets the port receives per second.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

Mirroring

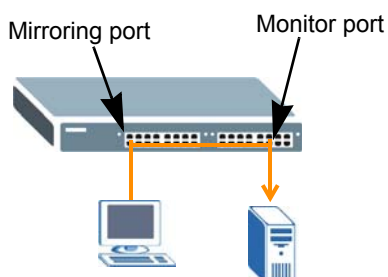
This chapter discusses port mirroring setup screens.

14.1 Port Mirroring

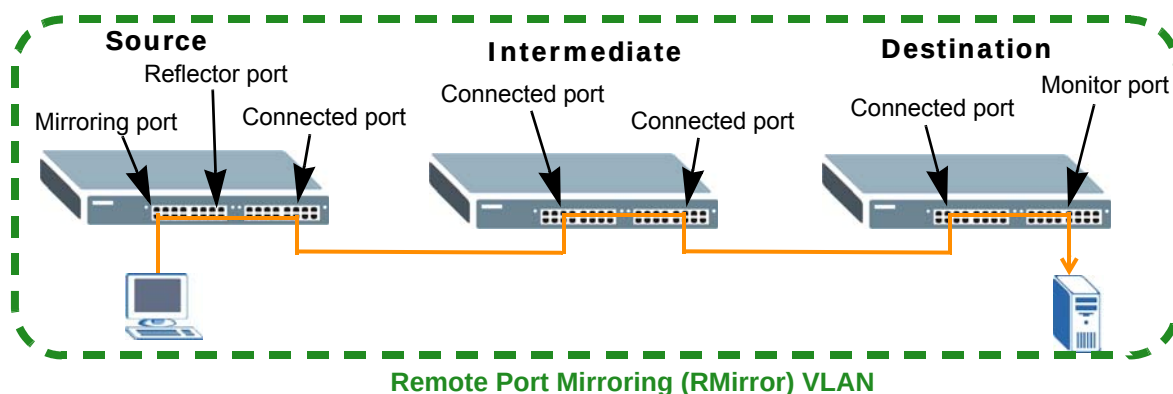
Port mirroring allows you to copy a traffic flow to a monitor port (the port you copy the traffic to) in order that you can examine the traffic from the monitor port without interference.

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

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

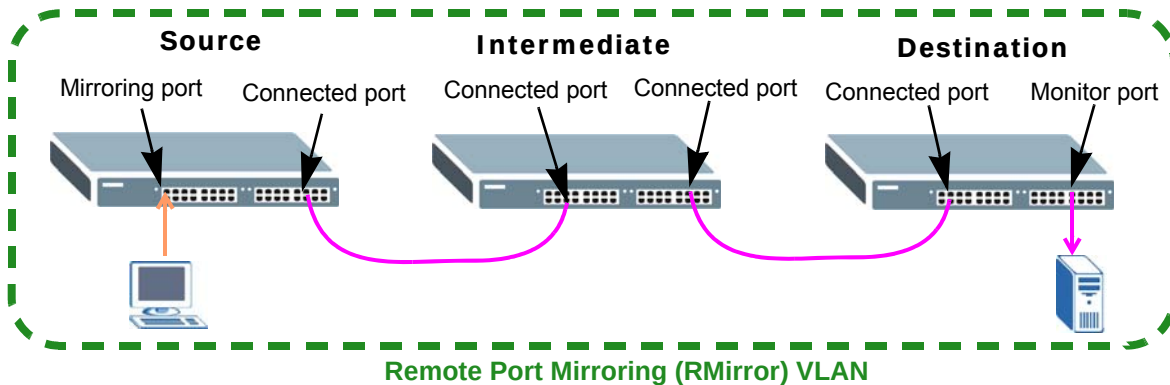


In remote port mirroring (RMirror), the mirroring ports and monitor port can be on different devices in a network. You can use it to monitor multiple switches across your network. The traffic from the source device's mirroring port(s) is sent to a reflector port for VLAN tagging and copied to the connected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



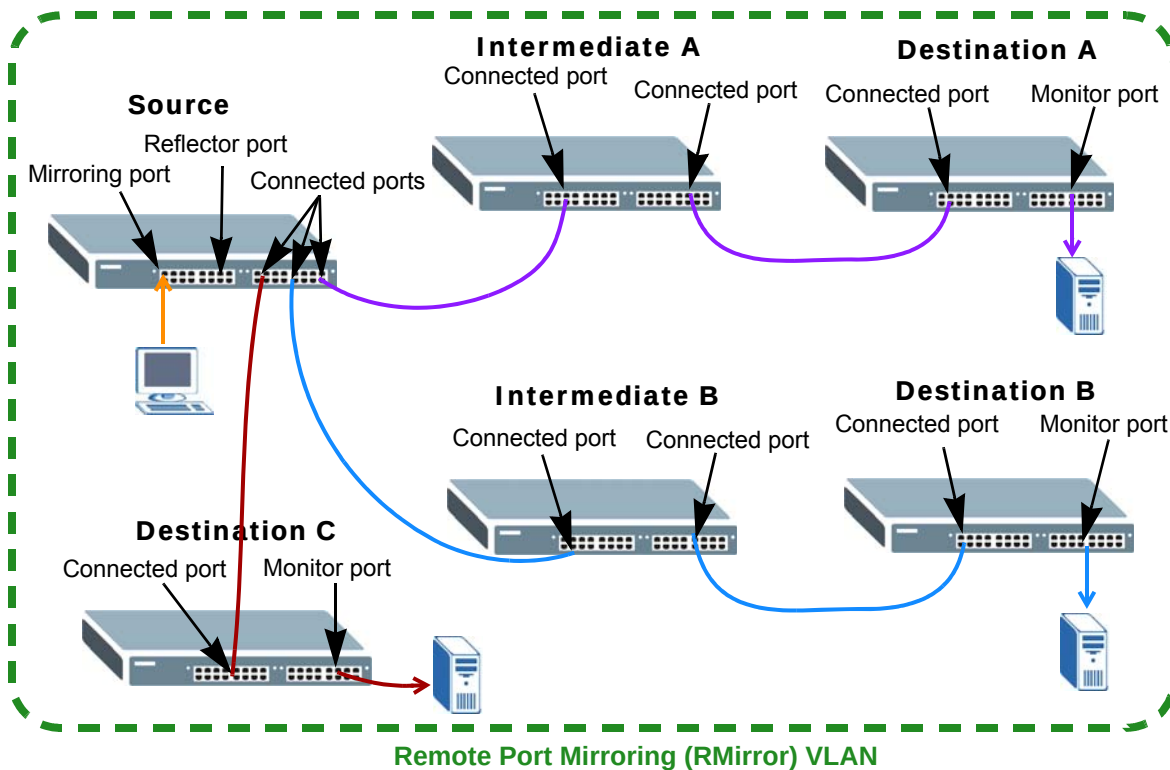
Single-Destination RMirror

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



Multi-Destination RMirror

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



Port Rules in Port Mirroring

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

Table 61 Port Rules between Different Remote Port Mirroring VLANs

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

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

Table 62 Port Rules between Remote and Local Port Mirroring

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

14.1.1 Local Port Mirroring

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

Figure 103 Advanced Application > Mirroring (Standalone mode)

Mirroring [RMirror](#)

Active ☒

Monitor Port

Port	Mirrored	Direction
*	☐	Ingress ▼
1	☐	Ingress ▼
2	☐	Ingress ▼
3	☐	Ingress ▼
4	☐	Ingress ▼
5	☐	Ingress ▼
6	☐	Ingress ▼
7	☐	Ingress ▼
8	☐	Ingress ▼
9	☐	Ingress ▼
10	☐	Ingress ▼
11	☐	Ingress ▼
12	☐	Ingress ▼
13	☐	Ingress ▼

Figure 104 Advanced Application > Mirroring (Stacking mode)

Mirroring [RMirror](#)

Active ☒

Monitor Port

SLOT 1 ▼

Port	Mirrored	Direction
1/*	☐	Ingress ▼
1/1	☐	Ingress ▼
1/2	☐	Ingress ▼
1/48	☐	Ingress ▼
1/50	☐	Ingress ▼

The following table describes the labels in this screen.

Table 63 Advanced Application > Mirroring

LABEL	DESCRIPTION
Active	Select this check box to activate port mirroring on the Switch. Clear this check box to disable the feature.
Monitor Port	The monitor port is the port you copy the traffic to in order to examine it in more detail without interfering with the traffic flow on the original port(s). Type the port number of the monitor port. In stacking mode, the first number represents the slot and the second the port number.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Mirrored	Select this option to mirror the traffic on a port.
Direction	Specify the direction of the traffic to mirror by selecting from the drop-down list box. Choices are Egress (outgoing), Ingress (incoming) and Both .
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

14.1.2 Remote Port Mirroring

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

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

Figure 105 Advanced Application > Mirroring > RMirror

The screenshot shows the RMirror configuration interface. At the top, there's a navigation bar with tabs: RMirror (active), Mirroring, Source, Destination, and Connected Port. Below the tabs, there's a section for 'Active' with a checkbox and 'RMirror VLAN ID' with a text input field. Below this are 'Apply' and 'Cancel' buttons. At the bottom, there's a table with columns 'VLAN', 'Active', and 'Delete'. The table contains one row with '333' in the VLAN column, 'Yes' in the Active column, and a checkbox in the Delete column. Below the table are 'Delete' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 64 Advanced Application > Mirroring > RMirror

LABEL	DESCRIPTION
Active	Select the option to enable the VLAN.
RMirror VLAN ID	Specify the ID number of remote port mirroring (RMirror) VLAN.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
VLAN	This field displays the ID number of the RMirror VLAN. Click on the VLAN ID number to change the settings.
Active	This field displays whether the VLAN is enabled or not.
Delete	Check the rule(s) that you want to remove in the Delete column and then click the Delete button.
Cancel	Click Cancel to begin configuring this screen afresh.

14.1.3 Source

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

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

Figure 106 Advanced Application > Mirroring > RMirror > Source (Standalone mode)

Source

RMirror

RMirror VLAN ID

100

Priority

3

Reflector Port

Active

Port

5

Port	Mirrored	Direction
*	☐	Both
1	☒	Both
2	☒	Both
3	☐	Both
4	☐	Both
5	☐	Both
6	☐	Both
7	☐	Both
8	☐	Both
9	☐	Both
10	☐	Both
11	☐	Both
12	☐	Both

Apply

Cancel

VLAN	Priority	Mirror Port			Reflector Port	
		Ingress	Egress	Both	Active	Port

Figure 107 Advanced Application > Mirroring > RMirror > Source (Stacking mode)

Source RMirror

RMirror VLAN ID ▼

Priority 0 ▼

Reflector Port Active ☐ Port 1 ▼

SLOT 1 ▼

Port	Mirrored	Direction
1/*	☐	Both ▼
1/1	☐	Both ▼
1/2	☐	Both ▼
1/3	☐	Both ▼
1/4	☐	Both ▼
1/5	☐	Both ▼
1/6	☐	Both ▼
1/7	☐	Both ▼
1/8	☐	Both ▼

Apply Cancel

VLAN Priority Mirror Port Reflector Port

Ingress Egress Both Active Port

The following table describes the labels in this screen.

Table 65 Advanced Application > Mirroring > RMirror > Source

LABEL	DESCRIPTION
RMirror VLAN ID	Select the RMirror VLAN over which the mirrored traffic is forwarded.
Priority	Enter the priority of the mirrored traffic.
Reflector Port	Select the check box to enable the specified reflector port. Enter the number of reflector port that adds the RMirror VLAN tag to all mirrored traffic and forwards traffic to the connected port(s) in the same RMirror VLAN.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Mirrored	Select this option to mirror the traffic on a port.
Direction	Specify the direction of the traffic to mirror by selecting from the drop-down list box. Choices are Egress (outgoing), Ingress (incoming) and Both .

Table 65 Advanced Application > Mirroring > RMirror > Source (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
VLAN	This field displays the ID number of RMirror VLAN over which the mirrored traffic is forwarded.
Priority	This field displays the priority of the mirrored traffic.
Mirror Port	
Ingress	This field displays the number of port(s) on which the incoming traffic is mirrored.
Egress	This field displays the number of port(s) on which the outgoing traffic is mirrored.
Both	This field displays the number of port(s) on which the incoming and outgoing traffic is mirrored.
Reflector Port	This field displays whether the reflector port is enabled and the number of reflector port in this RMirror VLAN.

14.1.4 Destination

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

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

Figure 108 Advanced Application > Mirroring > RMirror > Destination

The screenshot shows the 'Destination' configuration screen for RMirror. At the top, there's a blue header with an orange circle icon and the word 'Destination'. To the right, 'RMirror' is written in purple. Below the header, there are three rows of configuration fields: 'RMirror VLAN ID' with a dropdown menu showing '444', 'Monitor Port' with a text box containing '11', and 'Tagging' with radio buttons for 'Untagged' (selected) and 'Tagged'. Below these fields are 'Apply' and 'Cancel' buttons. Underneath is a table with four columns: 'VLAN', 'Monitor Port', 'Tagging', and 'Delete'. The table contains one row with the values '444', '11', 'Untagged', and a checkbox. At the bottom of the table are 'Delete' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 66 Advanced Application > Mirroring > RMirror > Destination

LABEL	DESCRIPTION
RMirror VLAN ID	Select the RMirror VLAN over which the mirrored traffic is forwarded.
Monitor Port	Specify the port to which you copy the traffic in order to examine it in more detail without interfering with the traffic flow on the original port(s).
Tagging	Select whether to add the RMirror VLAN tag to mirrored traffic on the monitor port.

Table 66 Advanced Application > Mirroring > RMirror > Destination (continued)

LABEL	DESCRIPTION
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
VLAN	This field displays the ID number of RMirror VLAN over which the mirrored traffic is forwarded.
Monitor Port	This field displays the number of port that receives the mirrored traffic from the source device for analysis.
Tagging	This field displays whether the mirrored traffic is tagged with the RMirror VLAN ID.
Delete	Check the rule(s) that you want to remove in the Delete column and then click the Delete button.
Cancel	Click Cancel to begin configuring this screen afresh.

14.1.5 Connected Port

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

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

Figure 109 Advanced Application > Mirroring > RMirror > Connected Port(Standalone mode)

Connected Port RMirror

RMirror VLAN ID: 444

Port	Connected Port
*	☐
1	☐
2	☐
3	☐
4	☐
5	☐
6	☐
7	☐
8	☐
9	☐

Apply Cancel

VLAN	Connected Port
333	5-6
444	

Figure 110 Advanced Application > Mirroring > RMirror > Connected Port (Stacking mode)

The screenshot shows the 'Connected Port' configuration interface. At the top, there's a blue header with an orange circle icon and the text 'Connected Port'. To the right is a link 'RMirror'. Below this is a 'RMirror VLAN ID' dropdown menu. Underneath is a 'SLOT 1' dropdown. The main area contains a table with two columns: 'Port' and 'Connected Port'. The 'Port' column has four rows: '1/*', '1/1', '1/2', and '1/50'. The 'Connected Port' column has checkboxes for each row. Below the table are 'Apply' and 'Cancel' buttons. At the bottom, there's a section with 'VLAN' and 'Connected Port' labels.

The following table describes the labels in this screen.

Table 67 Advanced Application > Mirroring > RMirror > Connected Port

LABEL	DESCRIPTION
RMirror VLAN ID	Select the RMirror VLAN over which the mirrored traffic is forwarded.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Connected Port	When the Switch is a source device in remote port mirroring, select this option to have the port help forward mirrored traffic to the connected port of the intermediate or destination device in the same RMirror VLAN. When the Switch is an intermediate device in remote port mirroring, select this option to have the port receive mirrored traffic from the connected source or another intermediate device or forward mirrored traffic to the connected destination or another intermediate device in the same RMirror VLAN. When the Switch is a destination device in remote port mirroring, select this option to have the port receive mirrored traffic from the connected source or intermediate device in the same RMirror VLAN.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

Table 67 Advanced Application > Mirroring > RMirror > Connected Port (continued)

LABEL	DESCRIPTION
VLAN	This field displays the ID number of port mirroring VLAN over which the mirrored traffic is forwarded.
Connected Port	This field displays the number of port(s) that helps forward mirrored traffic to other connected switches.

Link Aggregation

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

15.1 Link Aggregation Overview

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

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

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

The Switch supports both static and dynamic link aggregation.

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

See [Section 15.6 on page 171](#) for a static port trunking example.

15.2 Dynamic Link Aggregation

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

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

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

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

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

15.2.1 Link Aggregation ID

LACP aggregation ID consists of the following information¹:

Table 68 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 69 Link Aggregation ID: Peer Switch

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

15.3 Link Aggregation Status

Click **Advanced Application** > **Link Aggregation** in the navigation panel. The **Link Aggregation Status** screen displays by default. See [Section 15.1 on page 163](#) for more information.

Figure 111 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)] [(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	-

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

The following table describes the labels in this screen.

Table 70 Advanced Application > Link Aggregation Status

LABEL	DESCRIPTION
Group ID	This field displays the group ID to identify a trunk group, that is, one logical link containing multiple ports.
Enabled Port	These are the ports you have configured in the Link Aggregation screen to be in the trunk group. The port number(s) displays only when this trunk group is activated and there is a port belonging to this group.
Synchronized Ports	These are the ports that are currently transmitting data as one logical link in this trunk group.
Aggregator ID	Link Aggregator ID consists of the following: system priority, MAC address, key, port priority and port number. Refer to Section 15.2.1 on page 164 for more information on this field. The ID displays only when there is a port belonging to this trunk group and LACP is also enabled for this group.
Criteria	This shows the outgoing traffic distribution algorithm used in this trunk group. Packets from the same source and/or to the same destination are sent over the same link within the trunk. src-mac means the Switch distributes traffic based on the packet's source MAC address. dst-mac means the Switch distributes traffic based on the packet's destination MAC address. src-dst-mac means the Switch distributes traffic based on a combination of the packet's source and destination MAC addresses. src-ip means the Switch distributes traffic based on the packet's source IP address. dst-ip means the Switch distributes traffic based on the packet's destination IP address. src-dst-ip means the Switch distributes traffic based on a combination of the packet's source and destination IP addresses.
Status	This field displays how these ports were added to the trunk group. It displays: • Static - if the ports are configured as static members of a trunk group. • LACP - if the ports are configured to join a trunk group via LACP.

15.4 Link Aggregation Setting

Click **Advanced Application > Link Aggregation > Link Aggregation Setting** to display the screen shown next. See [Section 15.1 on page 163](#) for more information on link aggregation.

Figure 112 Advanced Application > Link Aggregation > Link Aggregation Setting (Standalone mode)

Link Aggregation Setting

Status LACP

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 ▼

Port	Group
1	None ▼
2	None ▼
3	None ▼
4	None ▼
5	None ▼
6	None ▼

Apply

Cancel

Figure 113 Advanced Application > Link Aggregation > Link Aggregation Setting (Stacking mode)

Link Aggregation Setting Status LACP

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 ▼

SLOT 1 ▼

Port	Group
1/1	None ▼
1/2	None ▼
1/3	None ▼

Apply Cancel

The following table describes the labels in this screen.

Table 71 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 71 Advanced Application > Link Aggregation > Link Aggregation Setting (continued)

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

15.5 Link Aggregation Control Protocol

Click in the **Advanced Application > Link Aggregation > Link Aggregation Setting > LACP** to display the screen shown next. See [Section 15.2 on page 163](#) for more information on dynamic link aggregation.

Figure 114 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP (Standalone mode)

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	☐

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

Apply

Cancel

Figure 115 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP (Stacking mode)

Link Aggregation Control Protocol Link Aggregation Setting

Active ☐

System Priority

Group ID	LACP Active
T1	☐
T2	☐
T3	☐
T4	☐
T5	☐
T6	☐
T7	☐
T8	☐
T9	☐
T10	☐
T11	☐
T12	☐
T13	☐
T14	☐
T15	☐
T16	☐
T17	☐
T18	☐
T19	☐
T20	☐
T21	☐
T22	☐
T23	☐
T24	☐

SLOT 1 ▾

Port	LACP Timeout
1/*	30 ▾ seconds
1/1	30 ▾ seconds
1/2	30 ▾ seconds
1/48	30 ▾ seconds
1/49	30 ▾ seconds
1/50	30 ▾ seconds

Apply Cancel

The following table describes the labels in this screen.

Table 72 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.

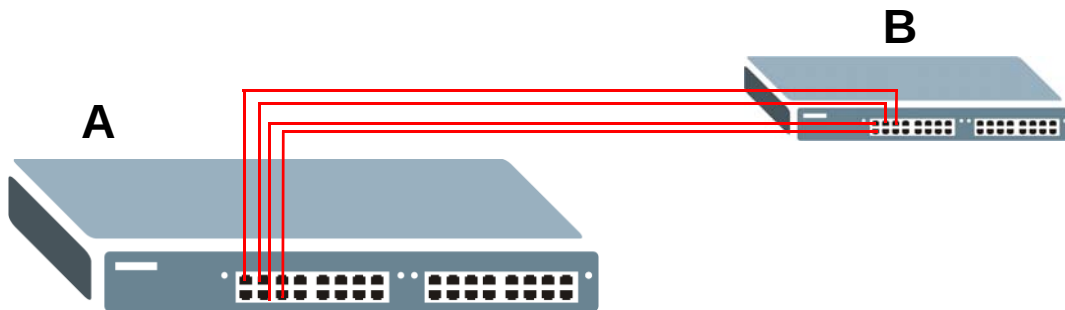
Table 72 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP (continued)

LABEL	DESCRIPTION
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports.
LACP Active	Select this option to enable LACP for a trunk.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
LACP Timeout	Timeout is the time interval between the individual port exchanges of LACP packets in order to check that the peer port in the trunk group is still up. If a port does not respond after three tries, then it is deemed to be “down” and is removed from the trunk. Set a short timeout (one second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible. Select either 1 second or 30 seconds.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

15.6 Static Trunking Example

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

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

Figure 116 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 117 Trunking Example - Configuration Screen

Link Aggregation Setting Status LACP

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

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

EXAMPLE

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

Port Authentication

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

16.1 Port Authentication Overview

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

- **IEEE 802.1x²** - 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.

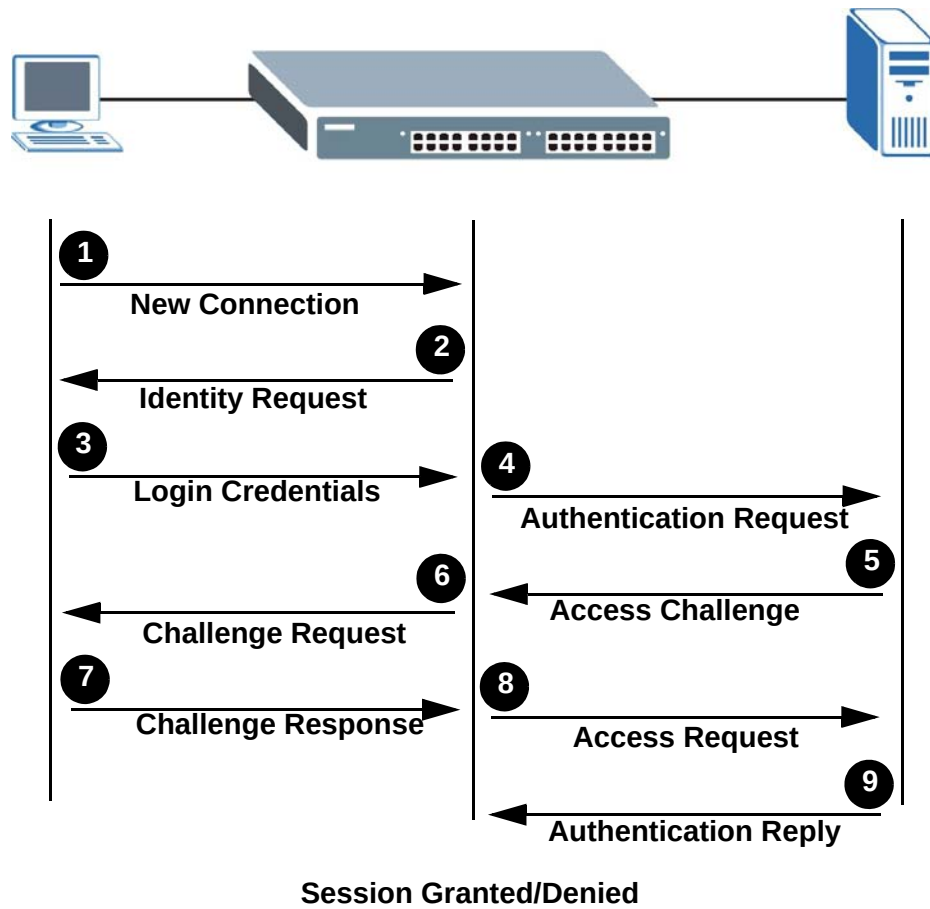
Both types of authentication use the RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) protocol to validate users. See [Section 24.1.2 on page 242](#) for more information on configuring your RADIUS server settings.

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

16.1.1 IEEE 802.1x Authentication

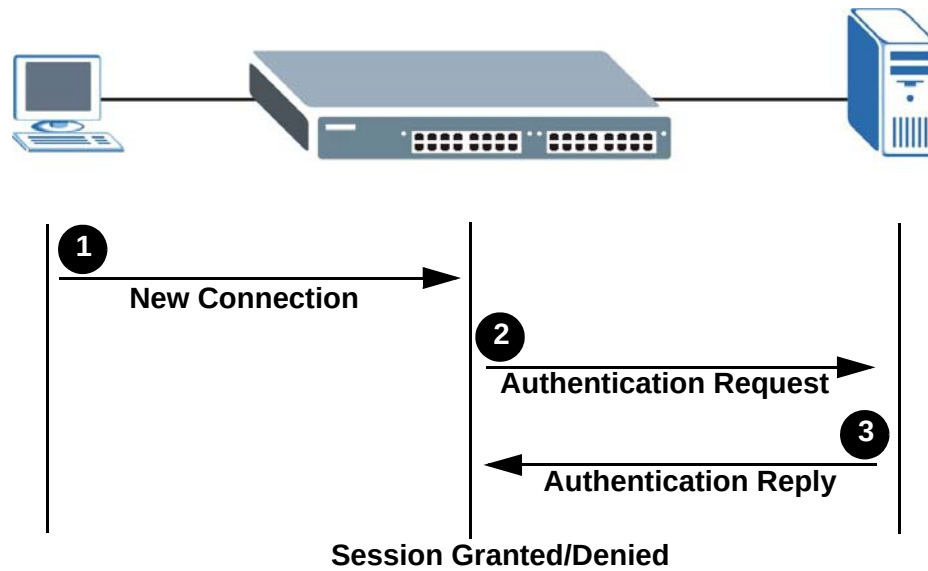
The following figure illustrates how a client connecting to an IEEE 802.1x authentication enabled port goes through a validation process. The Switch prompts the client for login information in the form of a user name and password after the client responds to its identity request. When the client provides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

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.

Figure 118 IEEE 802.1x Authentication Process

16.1.2 MAC Authentication

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

Figure 119 MAC Authentication Process

16.2 Port Authentication Configuration

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

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

Figure 120 Advanced Application > Port Authentication

16.2.1 Activate IEEE 802.1x Security

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

Figure 121 Advanced Application > Port Authentication > 802.1x (Standalone mode)

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
11	☐	2	On ▼	3600	60	30	30

Apply Cancel

Figure 122 Advanced Application > Port Authentication > 802.1x (Stacking mode)

802.1x Port Authentication [Guest Vlan](#)

Active ☐

SLOT 1 ▼

Port	Active	Max-Req	Reauth	Reauth-period secs	Quiet-period secs	Tx-period secs	Supp-Timeout secs
1/*	☐		On ▼				
1/1	☐	2	On ▼	3600	60	30	30
1/2	☐	2	On ▼	3600	60	30	30
1/48	☐	2	On ▼	3600	60	30	30
1/49	☐	2	On ▼	3600	60	30	30

Apply Cancel

The following table describes the labels in this screen.

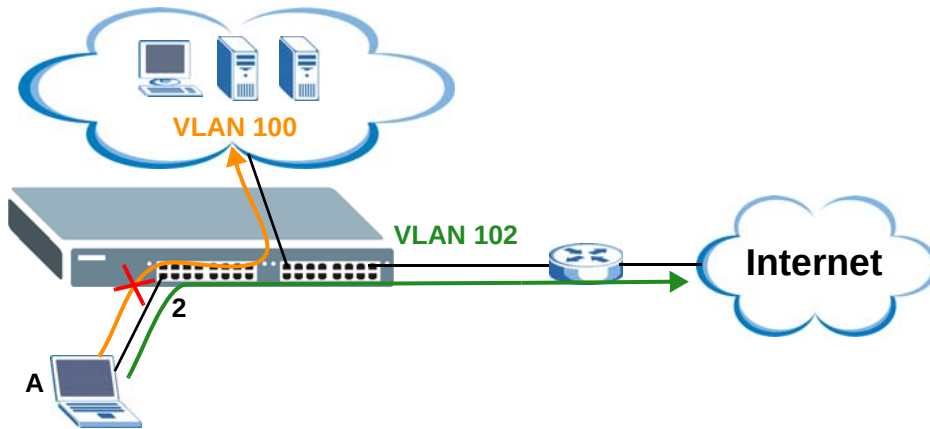
Table 73 Advanced Application > Port Authentication > 802.1x

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

16.2.2 Guest VLAN

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

Figure 123 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 124 Advanced Application > Port Authentication > 802.1x > Guest VLAN (Standalone mode)

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
11	☐	1	Multi-Host	1
12	☐	1	Multi-Host	1
13	☐	1	Multi-Host	1
14	☐	1	Multi-Host	1

Figure 125 Advanced Application > Port Authentication > 802.1x > Guest VLAN (Stacking mode)

The screenshot shows the 'Guest Vlan' configuration page for slot 1. The table lists ports 1/*, 1/1, 1/2, 1/48, and 1/50. For each port, there is an 'Active' checkbox, a 'Guest Vlan' input field (with '1' entered for 1/1, 1/2, 1/48, and 1/50), a 'Host-mode' dropdown (with 'Multi-Host' selected for 1/1, 1/2, 1/48, and 1/50), and a 'Multi-Secure Num' input field (with '1' entered for 1/1, 1/2, 1/48, and 1/50). The '1/*' row is for global settings. 'Apply' and 'Cancel' buttons are at the bottom.

The following table describes the labels in this screen.

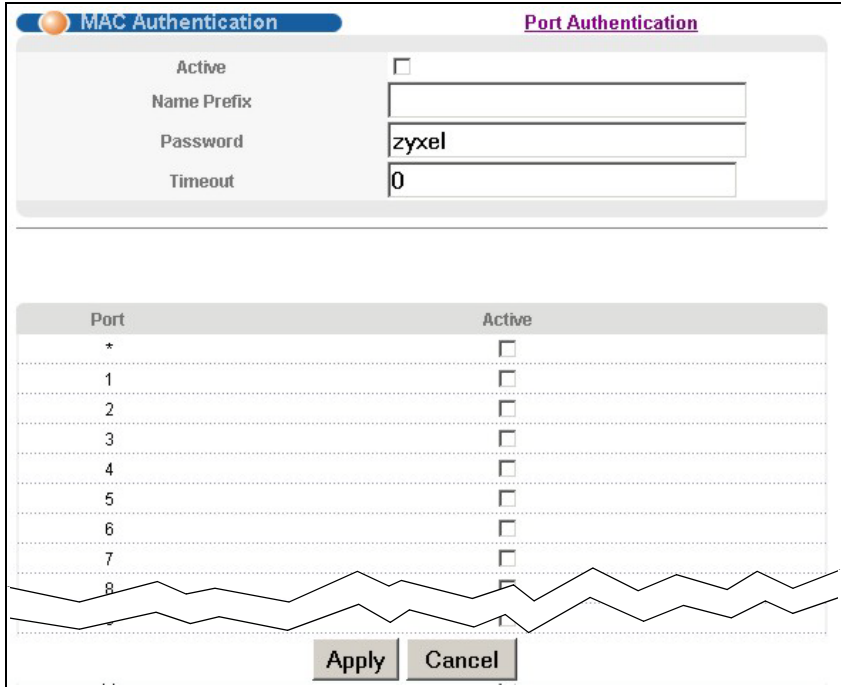
Table 74 Advanced Application > Port Authentication > 802.1x > Guest VLAN

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to enable the guest VLAN feature on this port. Clients that fail authentication are placed in the guest VLAN and can receive limited services.
Guest Vlan	A guest VLAN is a pre-configured VLAN on the Switch that allows non-authenticated users to access limited network resources through the Switch. You must also enable IEEE 802.1x authentication on the Switch and the associated ports. Enter the number that identifies the guest VLAN. Make sure this is a VLAN recognized in your network.
Host-mode	Specify how the Switch authenticates users when more than one user connect to the port (using a hub). Select Multi-Host to authenticate only the first user that connects to this port. If the first user enters the correct credential, any other users are allowed to access the port without authentication. If the first user fails to enter the correct credential, they are all put in the guest VLAN. Once the first user who did authentication logs out or disconnects from the port, rest of the users are blocked until a user does the authentication process again. Select Multi-Secure to authenticate each user that connects to this port.
Multi-Secure Num	If you set Host-mode to Multi-Secure , specify the maximum number of users (between 1 and 24) that the Switch will authenticate on this port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

16.2.3 Activate MAC Authentication

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

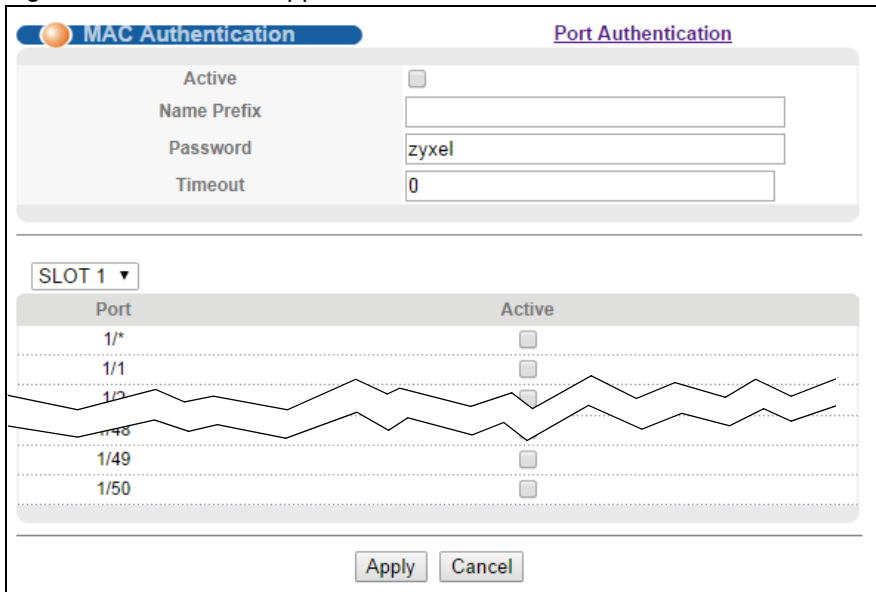
Figure 126 Advanced Application > Port Authentication > MAC Authentication (Standalone mode)



The screenshot shows the 'MAC Authentication' configuration screen in Standalone mode. At the top, there are two tabs: 'MAC Authentication' (selected) and 'Port Authentication'. Below the tabs, there are four configuration fields: 'Active' (checkbox), 'Name Prefix' (text box), 'Password' (text box with 'zyxel' entered), and 'Timeout' (text box with '0' entered). Below these fields is a table with two columns: 'Port' and 'Active'. The 'Port' column lists ports from 1 to 8, with a '*' at the top. The 'Active' column contains checkboxes for each port. At the bottom of the screen are 'Apply' and 'Cancel' buttons.

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

Figure 127 Advanced Application > Port Authentication > MAC Authentication (Stacking mode)



The screenshot shows the 'MAC Authentication' configuration screen in Stacking mode. At the top, there are two tabs: 'MAC Authentication' (selected) and 'Port Authentication'. Below the tabs, there are four configuration fields: 'Active' (checkbox), 'Name Prefix' (text box), 'Password' (text box with 'zyxel' entered), and 'Timeout' (text box with '0' entered). Below these fields is a dropdown menu labeled 'SLOT 1'. Below the dropdown is a table with two columns: 'Port' and 'Active'. The 'Port' column lists ports: '1/*', '1/1', '1/2', '1/48', '1/49', and '1/50'. The 'Active' column contains checkboxes for each port. At the bottom of the screen are 'Apply' and 'Cancel' buttons.

Port	Active
1/*	☐
1/1	☐
1/2	☐
1/48	☐
1/49	☐
1/50	☐

The following table describes the labels in this screen.

Table 75 Advanced Application > Port Authentication > MAC Authentication

LABEL	DESCRIPTION
Active	Select this check box to permit MAC authentication on the Switch. Note: You must first enable MAC authentication on the Switch before configuring it on each port.
Name Prefix	Type the prefix that is appended to all MAC addresses sent to the RADIUS server for authentication. You can enter up to 32 printable ASCII characters. If you leave this field blank, then only the MAC address of the client is forwarded to the RADIUS server.
Password	Type the password the Switch sends along with the MAC address of a client for authentication with the RADIUS server. You can enter up to 32 printable ASCII characters.
Timeout	Specify the amount of time before the Switch allows a client MAC address that fails authentication to try and authenticate again. Maximum time is 3000 seconds. When a client fails MAC authentication, its MAC address is learned by the MAC address table with a status of denied. The timeout period you specify here is the time the MAC address entry stays in the MAC address table until it is cleared. If you specify 0 for the timeout value, 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 6.4 on page 60 .
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to 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.

17.1 About Port Security

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

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

17.2 Port Security Setup

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

Figure 128 Advanced Application > Port Security (Standalone mode)

Port Security [VLAN MAC Address Limit](#)

MAC Freeze :

Port List

Port Security :

Active ☐

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

Figure 129 Advanced Application > Port Security (Stacking mode)

Port Security [VLAN MAC Address Limit](#)

MAC Freeze :

Port List

Port Security : ☐ Active

SLOT 1 ▼

Port	Active	Address Learning	Limited Number of Learned MAC Address
1/*	☐	☒	
1/1	☐	☒	0
1/2	☐	☒	0
1/48	☐	☒	0
1/49	☐	☒	0
1/50	☐	☒	0

The following table describes the labels in this screen.

Table 76 Advanced Application > Port Security

LABEL	DESCRIPTION
Port List	Enter the number of the port(s) (separated by a comma) on which you want to enable port security and disable MAC address learning. In stacking mode, the first number represents the slot and the second the port number. Enter 1/1-1/24,2/28 for ports 1 to 24 for the Switch in slot 1 and port 28 for the Switch in slot 2, for example. After you click MAC freeze , all previously learned MAC addresses on the specified port(s) will become static MAC addresses and display in the Static MAC Forwarding screen.
MAC freeze	Click MAC freeze to have the Switch automatically select the Active check boxes and clear the Address Learning check boxes only for the ports specified in the Port list .
Active	Select this option to enable port security on the Switch.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some of the settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable the port security feature on this port. The Switch forwards packets whose MAC address(es) is in the MAC address table on this port. Packets with no matching MAC address(es) are dropped. Clear this check box to disable the port security feature. The Switch forwards all packets on this port.
Address Learning	MAC address learning reduces outgoing broadcast traffic. For MAC address learning to occur on a port, the port itself must be active with address learning enabled.

Table 76 Advanced Application > Port Security (continued)

LABEL	DESCRIPTION
Limited Number of Learned MAC Address	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device must wait until one of the five learned MAC addresses ages out. MAC address aging out time can be set in the Switch Setup screen. The valid range is from "0" to "16K". "0" means this feature is disabled.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

17.3 VLAN MAC Address Limit

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

Figure 130 Advanced Application > Port Security > VLAN MAC Address Limit

The following table describes the labels in this screen.

Table 77 Advanced Application > Port Security > VLAN MAC Address Limit

LABEL	DESCRIPTION
Active	Select this option to activate this rule.
Port	Enter the number of the port to which this rule is applied. In stacking mode, the first number represents the slot and the second the port number.
VID	Enter the VLAN identification number.
Limit Number	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port in a specified VLAN. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device would have to wait until one of the five learned MAC addresses aged out. MAC address aging out time can be set in the Switch Setup screen. The valid range is from "0" to "16K". "0" means this feature is disabled.

Table 77 Advanced Application > Port Security > VLAN MAC Address Limit (continued)

LABEL	DESCRIPTION
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Clear	Click Clear to reset the fields to the factory defaults.
Index	This 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.

Time Range

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

18.1 About Time Range

You can set a time range for time-oriented features such as Classifier ACL (Access Control List) rule which categorizes data packets into different network traffic flow. The advantage of the time range feature is that it allows you to schedule the active time of configurations. For example, see [Section 19.2 on page 188](#) to configure the classifier rule with time range.

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

18.2 Time Range Setup

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

Figure 131 Advanced Application > Time Range


Time Range

Name

Type

☒ Absolute
☐ Periodic

Absolute

Start

1970

01

01

00

:

00

End

1970

01

01

00

:

00

Periodic

☒

Monday

00

:

00

to

Monday

00

:

00

☐ Mon
☐ Tue
☐ Wed
☐ Thu
☐ Fri
☐ Sat
☐ Sun
☐ Weekdays
☐ Weekend
☐ Daily

☐

00

:

00

to

00

:

00

Add

Cancel

Clear

Index	Name	Type	Range	Delete

Delete

Cancel

The following table describes the labels in this screen.

Table 78 Advanced Application > Time Range

LABEL	DESCRIPTION
Name	Type a name for this time range rule.
Type	Select a time range type. Absolute is a fixed time range that has a set start and end date. Periodic is recurrence of a time range.
Absolute	This sets a fixed time range.
Start/End Days of the week	Use the drop-down list box to select a start date, time, an end date, time and days of the week for this time range rule.
Periodic	This sets a recurrent time range.
Days of the week Time	Use the check boxes and drop-down list boxes to set the periodic time range. This is a recurrence time range.
Add	Click Add to save the time range you entered.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to reset the fields to the factory defaults.
Index	This field displays the index number of the rule. Click an index number to change the settings.
Name	This field displays the name of the time range rule.
Type	This field displays whether the time range rule is absolute or periodic.
Range	This field displays the time range you entered for this rule.
Delete	You can delete this time range by clicking the check box of this time range rule and click Delete button below.
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.

19.1 About the Classifier and QoS

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

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

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

- 1 Configure classifiers to sort traffic into different flows.
- 2 Configure policy rules to define actions to be performed for a classified traffic flow (refer to [Chapter 20 on page 196](#) to configure policy rules).

You can also configure policy routing to forward a classified traffic flow to a different gateway for cost savings and load sharing. See [Chapter 37 on page 356](#) for how to configure policy routing.

19.2 Classifier Status

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 20 on page 196](#).

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

Figure 132 Advanced Application > Classifier > Classifier Status

The following table describes the labels in this screen.

Table 79 Advanced Application > Classifier > Classifier Status

LABEL	DESCRIPTION
Index	This field displays the index number of the Classifier rule.
Active	This field displays Yes when the rule is activated and No when it is deactivated.
Weight	This field displays the weight the priority of the Classifier rule when the match order is in manual mode. A higher weight means a higher priority.
Name	This field displays the name of the Classifier rule.
Match Count	This field displays the number of packets that matched this rule. It displays '-' if the rule does not have count enabled.
Rule	This field displays the name of the Access Control List rule.
Any	Select Any , then click Clear to clear the matched count for all classifiers.
Classifier	Select Classifier , type a classifier name in the text box, then click Clear to clear the matched count for that classifier.

19.3 Classifier Configuration

Click **Classifier Configuration** in the Classifier Status screen to display the configuration screen as shown.

Figure 133 Advanced Application > Classifier > Classifier Configuration

Classifier Configuration		Classifier Global Setting	Classifier Status
Active	☐		
Name			
Weight	32767		
Log	☐		
Count	☐		
Time Range	None		
Ingress Port	Port ☒ Any ☐		
	Trunk ☒ Any ☐		
Packet Format	All		
Layer 2	VLAN ☒ Any ☐ Inner VLAN ☒ Any ☐ Priority ☒ Any ☐ 0 Inner Priority ☒ Any ☐ 0 Ethernet Type ☒ All ☐ Others (Hex)		
	Source MAC Address ☒ Any ☐ MAC : : : : : /Mask : : : : : Destination MAC Address ☒ Any ☐ MAC : : : : : /Mask : : : : :		
	IP Packet Length ☒ Any ☐ To Bytes DSCP IPv4 ☒ Any ☐ IPv6 ☒ Any ☐		
Layer 3	Precedence ☒ Any ☐ ToS ☒ Any ☐ IP Protocol ☒ All Establish Only ☐ Others (Dec)		
	Source IP Address / Address Prefix / Destination IP Address / Address Prefix /		
Layer 4	Source Socket Number ☒ Any ☐ To Destination Socket Number ☒ Any ☐ To		

The following table describes the labels in this screen.

Table 80 Advanced Application > Classifier > Classifier Configuration

LABEL	DESCRIPTION
Active	Select this option to enable this rule.
Name	Enter a descriptive name for this rule for identifying purposes.
Weight	Enter a number from 0-65535 for the order priority of the Classifier rule. When the match order is in manual mode, a higher weight means a higher priority. When the match order is in auto mode, the priority depends on the layer of the item configured in the qualifier, with layer-4 having a higher priority than layer-3, and layer-3 having a higher priority than layer-2.
Log	Click the Log check box to record the number of matched packets in a particular time interval.
Count	Click the Count check box to have the Switch count the number of matched packets.
Time Range	You must have configured a time range in the Time Range screen first. Select the name of the time range rule from the drop-down list box to apply a time range to the Classifier rule.
Ingress Port	
Port	Choose Any for all ports or enter the ports manually to have the Switch apply the Classifier rule on the ports. In stacking mode, the first number represents the slot and the second the port number.
Trunk	Choose Any for all trunks or enter the trunks manually to have the Switch apply the Classifier rule on the trunks.
Packet Format	Specify the format of the packet. Choices are All , 802.3 tagged , 802.3 untagged , Ethernet II tagged and Ethernet II untagged . A value of 802.3 indicates that the packets are formatted according to the IEEE 802.3 standards. A value of Ethernet II indicates that the packets are formatted according to RFC 894, Ethernet II encapsulation.
Layer 2	
Specify the fields below to configure a layer-2 classifier.	
VLAN	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 Others and enter the Ethernet type number in hexadecimal value. Refer to Table 82 on page 193 for information.
Source	
MAC Address	Select Any to apply the rule to all MAC addresses. To specify a source, select the MAC button and type a MAC address in valid MAC address format (six hexadecimal character pairs).
Mask	Manually type the source MAC mask to which the rule should be applied. You may choose one MAC mask only or all masks (Any).
Destination	
MAC Address	Select Any to apply the rule to all MAC addresses. To specify a destination, select the MAC button and type a MAC address in valid MAC address format (six hexadecimal character pairs).
Mask	Manually type the source MAC mask to which the rule should be applied. You may choose one MAC mask only or all masks (Any).
Layer 3	
Specify the fields below to configure a layer-3 classifier.	

Table 80 Advanced Application > Classifier > Classifier Configuration (continued)

LABEL	DESCRIPTION
IP Packet Length	Click Any to classify any size of packet length or manually enter a range of number (from/to) of packet size in the field provided.
DSCP	Select Any to classify traffic from any DSCP or select the second option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
Precedence	Click Any to classify all packet precedence or select the second option and specify a precedence level in the field provided.
ToS	Click Any to classify all ToS (Type of Service) or select the second option and specify a ToS level in the field provided.
IP Protocol	Select an IPv4 protocol type or select Other and enter the protocol number in decimal value. Refer to Table 83 on page 193 for more information. You may select Establish Only for TCP protocol type. This means that the Switch will identify packets that initiate or acknowledge (establish) TCP connections.
IPv6 Next Header	Select an IPv6 protocol type or select Other and enter an 8-bit next header in the IPv6 packet. The Next Header field is similar to the IPv4 Protocol field. The IPv6 protocol number ranges from 1 to 255. You may select Establish Only for TCP protocol type. This means that the Switch will identify packets that initiate or acknowledge (establish) TCP connections.
Source	
IP Address/ Address Prefix	Enter a source IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Destination	
IP Address/ Address Prefix	Enter a destination IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Layer 4	
Specify the fields below to configure a layer-3 classifier.	
Source/ Destination Socket Number	Note: You must select either UDP or TCP in the IP Protocol field before you configure the socket numbers. Select Any to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to set the above fields back to the factory defaults.

19.4 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 134 Advanced Application > Classifier > Classifier Configuration: Summary Table

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

The following table describes the labels in this screen.

Table 81 Advanced Application > Classifier > Classifier Configuration: Summary Table

LABEL	DESCRIPTION
Index	This field displays the index number of the rule. Click an index number to edit the rule.
Active	This field displays Yes when the rule is activated and No when it is deactivated.
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.
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 82 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 83 Common IP Ports

PORT NUMBER	PORT NAME
21	FTP
23	Telnet
25	SMTP
53	DNS

Table 83 Common IP Ports

PORT NUMBER	PORT NAME
80	HTTP
110	POP3

19.4.1 Classifier Global Setting 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 135 Advanced Application > Classifier > Classifier Configuration > Classifier Global Setting

The following table describes the labels in this screen.

Table 84 Advanced Application > Classifier > Classifier Configuration > Classifier Global Setting

LABEL	DESCRIPTION
Match Order	Select manual to have classifier rules applied according to the weight of each rule you configured in Advanced Application > Classifier > Classifier Configuration . Alternatively, select auto to have classifier rules applied according to the layer of the item configured in the rule. Layer-4 items have the highest priority.
Logging	
Active	Select this to create a log when packets match a classifier rule during a defined time interval.
Interval	Select the length of the time period (in seconds) to count matched packets for a classifier rule. Enter an integer from 0-65535. 0 means that no logging is done.
Apply	Click Apply to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

19.5 Classifier Example

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

Figure 136 Classifier: Example

Classifier Configuration [Classifier Global Setting](#) [Classifier Status](#)

Active ☒

Name

Weight

Log ☐

Count ☐

Time Range

Port ☐ Any ☒

Ingress Port ☒ Any ☐

Trunk ☐

Packet Format

Layer 2

VLAN ☒ Any ☐

Inner VLAN ☒ Any ☐

Priority ☒ Any ☐

Inner Priority ☒ Any ☐

Ethernet Type ☒ All ☐ Others (Hex)

Source MAC Address ☒ MAC : : : : : ☐ Mask : : : : :

Destination MAC Address ☒ MAC : : : : : ☐ Mask : : : : :

IP Packet Length ☒ Any ☐ To Bytes

DSCP IPv4 ☒ Any ☐

IPv6 ☒ Any ☐

Layer 3

Precedence ☒ Any ☐

ToS ☒ Any ☐

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

Source IP Address / Address Prefix /

Destination IP Address / Address Prefix /

Layer 4

Source Socket Number ☒ Any ☐ To

Destination Socket Number ☒ Any ☐ To

EXAMPLE

After you have configured a classifier, you can configure a policy to define action(s) on the classified traffic flow. See [Chapter 20 on page 196](#) for information on configuring a policy rule.

Policy Rule

This chapter shows you how to configure policy rules.

20.1 Policy Rules Overview

A classifier distinguishes traffic into flows based on the configured criteria (refer to [Chapter 19 on page 188](#) for more information). A policy rule ensures that a traffic flow gets the requested treatment in the network.

20.1.1 DiffServ

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

20.1.2 DSCP and Per-Hop Behavior

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

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

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.

20.2 Configuring Policy Rules

You must first configure a classifier in the **Classifier** screen. Refer to [Section 19.2 on page 188](#) for more information.

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

Figure 137 Advanced Application > Policy Rule

Policy

Active ☐

Name

Classifier(s)

Parameters

General

Egress Port

Priority

DSCP

TOS

Metering

Bandwidth

Kbps

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

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

☐ Replace the 802.1p priority field with the inner 802.1p priority value

Queue

☒ No change

☐ Send the packet to priority queue

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 85 Advanced Application > Policy Rule

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

Table 85 Advanced Application > Policy Rule (continued)

LABEL	DESCRIPTION
Diffserv	Select No change to keep the TOS and/or DSCP fields in the packets. Select Set the packet's TOS field to set the TOS field with the value you configure in the TOS field. Select Replace the IP TOS with the 802.1p priority value to replace the TOS field with the value you configure in the Priority field. Select Set the Diffserv Codepoint field in the frame to set the DSCP field with the value you configure in the DSCP field.
Outgoing	Select Send the packet to the mirror port to send the packet to the mirror port. Select Send the packet to the egress port to send the packet to the egress port.
Metering	Select Enable to activate bandwidth limitation on the traffic flow(s) then set the actions to be taken on out-of-profile packets.
Out-of-profile action	Select the action(s) to be performed for out-of-profile traffic. Select Drop the packet to discard the out-of-profile traffic. Select Change the DSCP value to replace the DSCP field with the value specified in the Out of profile DSCP field. Select Set Out-Drop Precedence to mark out-of-profile traffic and drop it when network is congested. Select Do not drop the matching frame previously marked for dropping to queue the frames that are marked to be dropped.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to set the above fields back to the factory defaults.

20.2.1 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 138 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 86 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.

Table 86 Policy: Summary Table (continued)

LABEL	DESCRIPTION
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.

20.3 Policy Example

The figure below shows an example **Policy** screen where you configure a policy to limit bandwidth and discard out-of-profile traffic on a traffic flow classified using the **Example** classifier (refer to [Section 19.5 on page 194](#)).

Figure 139 Policy Example

Policy	
Active	☒
Name	Test
Classifier(s)	Example
Parameters	General Metering Bandwidth: 10000 Kbps Egress Port: 1 Out-of-Profile DSCP: Priority: 0 ▼ DSCP: TOS: 0 ▼
	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 ☐ Replace the 802.1p priority field with the IP TOS value ☐ Replace the 802.1p priority field with the inner 802.1p priority value
Action	Queue
	☒ No change ☐ Send the packet to priority queue
	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
EXAMPLE	
Add Cancel Clear	

Queuing Method

This chapter introduces the queuing methods supported.

21.1 Queuing Method Overview

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

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

21.1.1 Strictly Priority

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

21.1.2 Weighted Fair Queuing

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

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

Weight x 2 KB

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

$5 \times 2\text{KB} = 10\text{ KB}$

21.1.3 Weighted Round Robin Scheduling (WRR)

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

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

21.2 Configuring Queuing

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

Figure 140 Advanced Application > Queuing Method (Standalone mode)

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

Figure 141 Advanced Application > Queuing Method (Stacking mode)

Queuing Method

SLOT 1 ▾

Port	Method	Weight								Hybrid-SPQ
		Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Lowest-Queue
1/*	SPQ ▾									None ▾
1/1	☒ SPQ ☐ WFQ ☐ WRR	1	2	3	4	5	6	7	8	None ▾
1/2	☒ SPQ ☐ WFQ ☐ WRR	1	2	3	4	5	6	7	8	None ▾
1/48	☐ SPQ ☐ WFQ ☐ WRR	1	2	3	4	5	6	7	8	None ▾
1/49	☒ SPQ ☐ WFQ ☐ WRR	1	2	3	4	5	6	7	8	None ▾
1/50	☒ SPQ ☐ WFQ ☐ WRR	1	2	3	4	5	6	7	8	None ▾

Apply Cancel

The following table describes the labels in this screen.

Table 87 Advanced Application > Queuing Method

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Method	Select SPQ (Strictly Priority Queuing), WFQ (Weighted Fair Queuing) or WRR (Weighted Round Robin). Strictly Priority services queues based on priority only. When the highest priority queue empties, traffic on the next highest-priority queue begins. Q7 has the highest priority and Q0 the lowest. Weighted Fair Queuing is used to guarantee each queue's minimum bandwidth based on their bandwidth weight (the number you configure in the Weight field). Queues with larger weights get more guaranteed bandwidth than queues with smaller weights. Weighted Round Robin Scheduling services queues on a rotating basis based on their queue weight (the number you configure in the queue Weight field). Queues with larger weights get more service than queues with smaller weights.
Weight Q0-Q7	When you select WFQ or WRR enter the queue weight here. Bandwidth is divided across the different traffic queues according to their weights.

Table 87 Advanced Application > Queuing Method (continued)

LABEL	DESCRIPTION
Hybrid-SPQ Lowest-Queue	This field is applicable only when you select WFQ or WRR. Select a queue (Q0 to Q7) to have the Switch use SPQ to service the subsequent queue(s) after and including the specified queue for the 1000Base-T, 1000Base-X and 10 Gigabit Ethernet ports. For example, if you select Q5, the Switch services traffic on Q5, Q6 and Q7 using SPQ. Select None to always use WFQ or WRR.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

VLAN Stacking

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

22.1 VLAN Stacking Overview

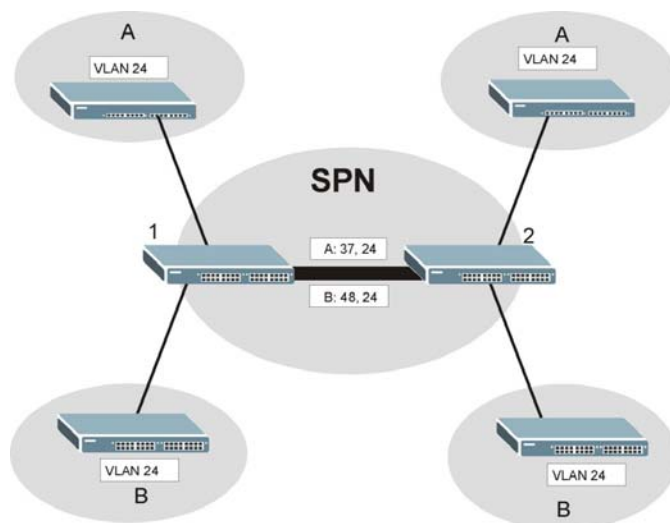
A service provider can use VLAN stacking to allow it to distinguish multiple customers VLANs, even those with the same (customer-assigned) VLAN ID, within its network.

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

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

22.1.1 VLAN Stacking Example

In the following example figure, both **A** and **B** are Service Provider's Network (SPN) customers with VPN tunnels between their head offices and branch offices respectively. Both have an identical VLAN tag for their VLAN group. The service provider can separate these two VLANs within its network by adding tag 37 to distinguish customer **A** and tag 48 to distinguish customer **B** at edge device **1** and then stripping those tags at edge device **2** as the data frames leave the network.

Figure 142 VLAN Stacking Example

22.2 VLAN Stacking Port Roles

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

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

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

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

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

22.3 VLAN Tag Format

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

Table 88 VLAN Tag Format

Type	Priority	VID

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

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

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

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

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

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

22.3.1 Frame Format

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

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

Table 89 Single and Double Tagged 802.1Q Frame Format

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

Table 90 802.1Q Frame

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

22.4 Configuring VLAN Stacking

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

Figure 143 Advanced Application > VLAN Stacking (Standalone mode)

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

Figure 144 Advanced Application > VLAN Stacking (Stacking mode)

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

Active ☐

SLOT 1 ▾

Port	Role	Tunnel TPID
1/*	Normal	
1/1	Normal	8100
1/2	Normal	8100
1/49	Normal	8100
1/50	Normal	8100

Apply Cancel

The following table describes the labels in this screen.

Table 91 Advanced Application > VLAN Stacking

LABEL	DESCRIPTION
Active	Select this checkbox to enable VLAN stacking on the Switch.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.

Table 91 Advanced Application > VLAN Stacking (continued)

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

22.4.1 Port-based Q-in-Q

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

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

Figure 145 Advanced Application > VLAN Stacking > Port-based QinQ (Standalone mode)

Port	SPVID	Priority
*		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

Figure 146 Advanced Application > VLAN Stacking > Port-based QinQ (Stacking mode)

Port	SPVID	Priority
1/*		0
1/1	1	0
1/2	1	0
1/49	1	0
1/50	1	0

Apply Cancel

The following table describes the labels in this screen.

Table 92 Advanced Application > VLAN Stacking > Port-based QinQ

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number. * means all ports (on the same Switch).
SPVID	SPVID is the service provider's VLAN ID (the outer VLAN tag). Enter the service provider ID (from 1 to 4094) for frames received on this port. See Chapter 7 on page 94 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.

Table 92 Advanced Application > VLAN Stacking > Port-based QinQ (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.

22.4.2 Selective Q-in-Q

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

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

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

Figure 147 Advanced Application > VLAN Stacking > Selective QinQ

The following table describes the labels in this screen.

Table 93 Advanced Application > VLAN Stacking > Selective QinQ

LABEL	DESCRIPTION
Active	Check this box to activate this rule.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Port	The port number identifies the port you are configuring. In stacking mode, the first field is the slot ID and the second field is the port number.
CVID	Enter a customer VLAN ID (the inner VLAN tag) from 1 to 4094. This is the VLAN tag carried in the packets from the subscribers.
SPVID	SPVID is the service provider's VLAN ID (the outer VLAN tag). Enter the service provider ID (from 1 to 4094) for frames received on this port. See Chapter 7 on page 94 for more background information on VLAN ID.

Table 93 Advanced Application > VLAN Stacking > Selective QinQ (continued)

LABEL	DESCRIPTION
Priority	Select a priority level (from 0 to 7). This is the service provider's priority level that adds to the frames received on this port. "0" is the lowest priority level and "7" is the highest.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Index	This is the number of the selective VLAN stacking rule. Click on an index number to change the settings.
Active	This shows whether this rule is activated or not.
Name	This is the descriptive name for this rule.
Port	This is the port number to which this rule is applied. In stacking mode, the first number represents the slot and the second the port number.
CVID	This is the customer VLAN ID in the incoming packets.
SPVID	This is the service provider's VLAN ID that adds to the packets from the subscribers.
Priority	This is the service provider's priority level in the packets.
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.

23.1 Multicast Overview

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

IGMP (Internet Group Management Protocol) is a network-layer protocol used to establish membership in an IPv4 multicast group - it is not used to carry user data. Refer to RFC 1112, RFC 2236 and RFC 3376 for information on IGMP versions 1, 2 and 3 respectively.

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is similar to IGMPv2 and MLDv2 is similar to IGMPv3. MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4. MLD filtering controls which multicast groups a port can join.

23.1.1 IP Multicast Addresses

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

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

23.1.2 IGMP Filtering

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

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

23.1.3 IGMP Snooping

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

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

23.1.4 IGMP Snooping and VLANs

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

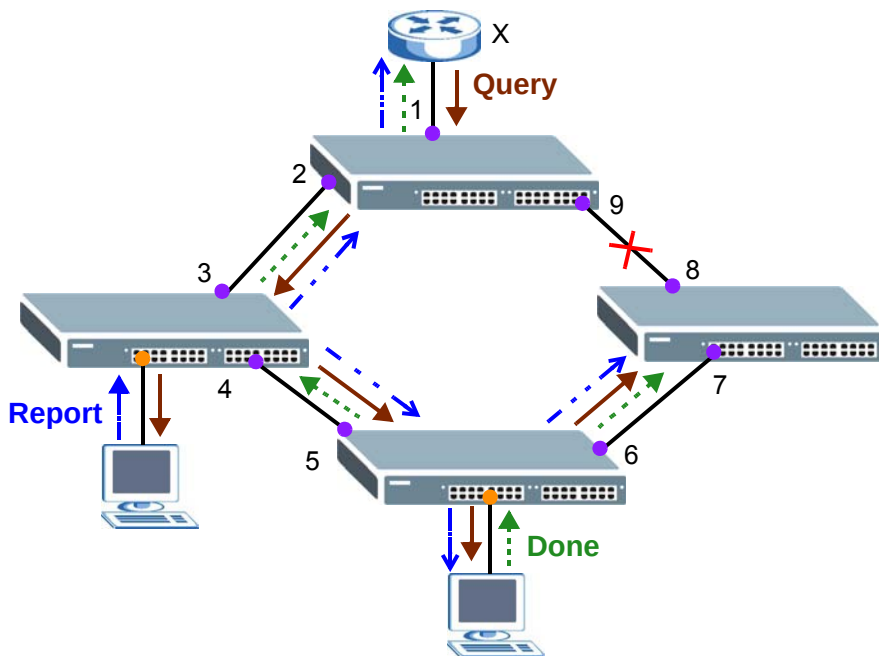
23.1.5 MLD Snooping-Proxy

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

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

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

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



23.1.6 MLD Messages

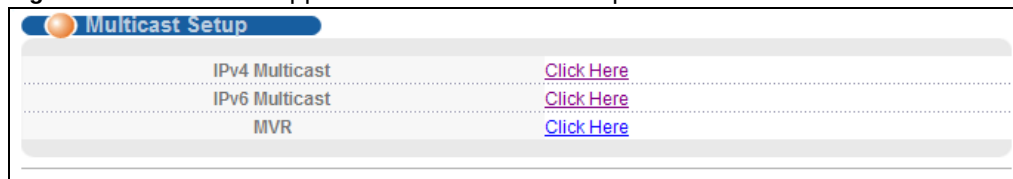
A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

An MLD Done message is similar to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. If the leave mode is not set to **Immediate**, the router or switch sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

23.2 Multicast Setup

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

Figure 148 Advanced Application > Multicast Setup



The following table describes the labels in this screen.

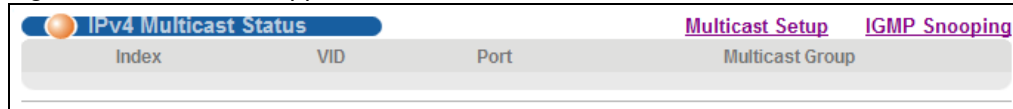
Table 94 Advanced Application > Multicast Setup

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

23.3 IPv4 Multicast Status

Click **Advanced Application > Multicast > IPv4 Multicast** to display the screen as shown. This screen shows the IPv4 multicast group information. See [Section 23.1 on page 214](#) for more information on multicasting.

Figure 149 Advanced Application > Multicast > IPv4 Multicast



Index	VID	Port	Multicast Group

The following table describes the labels in this screen.

Table 95 Advanced Application > Multicast > IPv4 Multicast

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

23.3.1 IGMP Snooping

Click the **IGMP Snooping** link in the **Advanced Application > Multicast > IPv4 Multicast** screen to display the screen as shown. See [Section 23.1 on page 214](#) for more information on multicasting.

Figure 150 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping (Standalone mode)

IGMP Snooping [IPv4 Multicast Status](#) [IGMP Snooping VLAN](#) [IGMP Filtering Profile](#)

IGMP Snooping		Active	☒
		Querier	☐
		Host Timeout	260
		802.1p Priority	No-Change
IGMP Filtering		Active	☐
Unknown Multicast Frame		☒ Flooding	☐ Drop
Reserved Multicast Group		☒ Flooding	☐ Drop

Port	Immed. Leave	Normal Leave	Fast Leave	Group Limited	Max Group Num.	Throttling	IGMP Filtering Profile	IGMP Querier Mode
*	☐	☒	☐	☐		Deny	Default	Auto
1	☐	☒	☐	☐	0	Deny	Default	Auto
2	☐	☒	☐	☐	0	Deny	Default	Auto
3	☐	☒	☐	☐	0	Deny	Default	Auto
4	☐	☒	☐	☐	0	Deny	Default	Auto
5	☐	☒	☐	☐	0	Deny	Default	Auto
6	☐	☒	☐	☐	0	Deny	Default	Auto
7	☐	☒	☐	☐	0	Deny	Default	Auto
8	☐	☒	☐	☐	0	Deny	Default	Auto
9	☐	☒	☐	☐	0	Deny	Default	Auto
10	☐	☒	☐	☐	0	Deny	Default	Auto

Figure 151 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping (Stacking mode)

IGMP Snooping [IPv4 Multicast Status](#) [IGMP Snooping VLAN](#) [IGMP Filtering Profile](#)

IGMP Snooping

Active ☐

Querier ☐

Host Timeout

802.1p Priority

IGMP Filtering

Unknown Multicast Frame

Reserved Multicast Group

Active ☐

☒ Flooding ☐ Drop

☒ Flooding ☐ Drop

SLOT 1 ▼

Port	Immed. Leave	Normal Leave	Fast Leave	Group Limited	Max Group Num.	Throttling	IGMP Filtering Profile	IGMP Querier Mode
1/*	☐			☐		Deny	Default	Auto
1/1	☐	4000	200	☐	0	Deny	Default	Auto
1/2	☐			☐				
1/48	☐	4000	200	☐	0	Deny	Default	Auto
1/49	☐	4000	200	☐	0	Deny	Default	Auto
1/50	☐	4000	200	☐	0	Deny	Default	Auto

The following table describes the labels in this screen.

Table 96 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping

LABEL	DESCRIPTION
IGMP Snooping	Use these settings to configure IGMP snooping.
Active	Select Active to enable IGMP Snooping to forward group multicast traffic only to ports that are members of that group.
Querier	Select this option to allow the Switch to send IGMP General Query messages to the VLANs with the multicast hosts attached.
Host Timeout	Specify the time (from 1 to 16 711 450) in seconds that elapses before the Switch removes an IGMP group membership entry if it does not receive report messages from the port.
802.1p Priority	Select a priority level (0-7) to which the Switch changes the priority in outgoing IGMP control packets. Otherwise, select No-Change to not replace the priority.
IGMP Filtering	Select Active to enable IGMP filtering to control which IGMP groups a subscriber on a port can join. Note: If you enable IGMP filtering, you must create and assign IGMP filtering profiles for the ports that you want to allow to join multicast groups.
Unknown Multicast Frame	Specify the action to perform when the Switch receives an unknown multicast frame. Select Drop to discard the frame(s). Select Flooding to send the frame(s) to all ports.

Table 96 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping (continued)

LABEL	DESCRIPTION
Reserved Multicast Group	The IP address range of 224.0.0.0 to 224.0.0.255 are reserved for multicasting on the local network only. For example, 224.0.0.1 is for all hosts on a local network segment and 224.0.0.9 is used to send RIP routing information to all RIP v2 routers on the same network segment. A multicast router will not forward a packet with the destination IP address within this range to other networks. See the IANA web site for more information. The layer-2 multicast MAC addresses used by Cisco layer-2 protocols, 01:00:0C:CC:CC:CC and 01:00:0C:CC:CC:CD, are also included in this group. Specify the action to perform when the Switch receives a frame with a reserved multicast address. Select Drop to discard the frame(s). Select Flooding to send the frame(s) to all ports.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first field is the slot ID and the second field is the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Immed. Leave	Select this option to set the Switch to remove this port from the multicast tree when an IGMP version 2 leave message is received on this port. Select this option if there is only one host connected to this port.
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, it forwards the message to the multicast router. The multicast router then sends out an IGMP Group-Specific Query (GSQ) message to determine whether other hosts connected to the port should remain in the specific multicast group. The Switch forwards the query message to all hosts connected to the port and waits for IGMP reports from hosts to update the forwarding table. This defines how many seconds the Switch waits for an IGMP report before removing an IGMP snooping membership entry when an IGMP leave message is received on this port from a host.
Fast Leave	Enter an IGMP fast leave timeout value (from 200 to 6,348,800) in 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 itself sends out an IGMP Group-Specific Query (GSQ) message to determine whether other hosts connected to the port should remain in the specific multicast group. This helps speed up the leave process. This defines how many seconds the Switch waits for an IGMP report before removing an IGMP snooping membership entry when an IGMP leave message is received on this port from a host.
Group Limited	Select this option to limit the number of multicast groups this port is allowed to join.
Max Group Num.	Enter the number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new IGMP join report frame(s) is dropped on this port.

Table 96 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping (continued)

LABEL	DESCRIPTION
Throttling	IGMP throttling controls how the Switch deals with the IGMP reports when the maximum number of the IGMP groups a port can join is reached. Select Deny to drop any new IGMP join report received on this port until an existing multicast forwarding table entry is aged out. Select Replace to replace an existing entry in the multicast forwarding table with the new IGMP report(s) received on this port.
IGMP Filtering Profile	Select the name of the IGMP filtering profile to use for this port. Otherwise, select Default to prohibit the port from joining any multicast group. You can create IGMP filtering profiles in the Multicast > IPv4 Multicast > IGMP Snooping > IGMP Filtering Profile screen.
IGMP Querier Mode	The Switch treats an IGMP query port as being connected to an IGMP multicast router (or server). The Switch forwards IGMP join or leave packets to an IGMP query port. Select Auto to have the Switch use the port as an IGMP query port if the port receives IGMP query packets. Select Fixed to have the Switch always use the port as an IGMP query port. Select this when you connect an IGMP multicast server to the port. Select Edge to stop the Switch from using the port as an IGMP query port. The Switch will not keep any record of an IGMP router being connected to this port. The Switch does not forward IGMP join or leave packets to this port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

23.3.2 IGMP Snooping VLAN

Click **Advanced Application > Multicast > IPv4 Multicast** in the navigation panel. Click the **IGMP Snooping** link and then the **IGMP Snooping VLAN** link to display the screen as shown. See [Section 23.1.4 on page 215](#) for more information on IGMP Snooping VLAN.

Figure 152 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Snooping VLAN

IGMP Snooping VLAN IGMP Snooping

Mode ☒ auto ☐ fixed

Apply Cancel

VLAN

Name

VID

Add Cancel Clear

Index	Name	VID	Delete
Delete Cancel			

The following table describes the labels in this screen.

Table 97 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Snooping VLAN

LABEL	DESCRIPTION
Mode	Select auto to have the Switch learn multicast group membership information of any VLANs automatically. Select fixed to have the Switch only learn multicast group membership information of the VLAN(s) that you specify below. In either auto or fixed mode, the Switch can learn up to 16 VLANs (including up to five VLANs you configured in the MVR screen). For example, if you have configured one multicast VLAN in the MVR screen, you can only specify up to 15 VLANs in this screen. The Switch drops any IGMP control messages which do not belong to these 16 VLANs. Note: You must also enable IGMP snooping in the Multicast > IPv4 Multicast > IGMP Snooping screen first.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
VLAN	Use this section of the screen to add VLANs upon which the Switch is to perform IGMP snooping.
Name	Enter the descriptive name of the VLAN for identification purposes.
VID	Enter the ID of a static VLAN; the valid range is between 1 and 4094. Note: You cannot configure the same VLAN ID as in the MVR screen.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.

Table 97 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Snooping VLAN (continued)

LABEL	DESCRIPTION
Clear	Click Clear to reset the fields to the factory defaults.
Index	This is the index number of the IGMP snooping VLAN entry in the table.
Name	This field displays the descriptive name for this VLAN group.
VID	This field displays the ID number of the VLAN group.
Delete	Check the entry(ies) that you want to remove in the Delete column, then click the Delete button.
Cancel	Click Cancel to clear the Delete check boxes.

23.3.3 IGMP Filtering Profile

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

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

Figure 153 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Filtering Profile

The following table describes the labels in this screen.

Table 98 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Filtering Profile

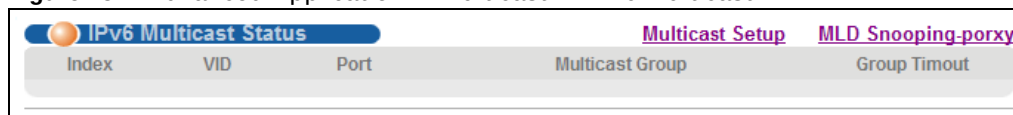
LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile for identification purposes. To configure additional rule(s) for a profile that you have already added, enter the profile name and specify a different IP multicast address range.
Start Address	Type the starting multicast IP address for a range of multicast IP addresses that you want to belong to the IGMP filter profile.

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

LABEL	DESCRIPTION
End Address	Type the ending multicast IP address for a range of IP addresses that you want to belong to the IGMP filter profile. If you want to add a single multicast IP address, enter it in both the Start Address and End Address fields.
Add	Click this to create a new entry. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to reset the fields to the factory defaults.
Profile Name	This field displays the descriptive name of the profile.
Start Address	This field displays the start of the multicast address range.
End Address	This field displays the end of the multicast address range.
Delete	To delete the profile(s) and all the accompanying rules, select the profile(s) that you want to remove in the Delete Profile column, then click the Delete button. To delete a rule(s) from a profile, select the rule(s) that you want to remove in the Delete Rule column, then click the Delete button.
Cancel	Click Cancel to clear the Delete Profile/Delete Rule check boxes.

23.4 IPv6 Multicast Status

Click **Advanced Application > Multicast > IPv6 Multicast** to display the screen as shown. This screen shows the IPv6 multicast group information. See [Section 23.1 on page 214](#) for more information on multicasting.

Figure 154 Advanced Application > Multicast > IPv6 Multicast


IPv6 Multicast Status					Multicast Setup	MLD Snooping-proxy
Index	VID	Port	Multicast Group	Group Timeout		

The following table describes the labels in this screen.

Table 99 Advanced Application > Multicast > IPv6 Multicast

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

23.4.1 MLD Snooping-proxy

Click the **MLD Snooping-proxy** link in the **Advanced Application > Multicast > IPv6 Multicast** screen to display the screen as shown. See [Section 23.1 on page 214](#) for more information on multicasting.

Figure 155 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy

The following table describes the labels in this screen.

Table 100 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy

LABEL	DESCRIPTION
MLD Snooping-proxy	Use these settings to configure MLD snooping-proxy.
Active	Select Active to enable MLD snooping-proxy on the Switch to minimize MLD control messages and allow better network performance.
802.1p Priority	Select a priority level (0-7) to which the Switch changes the priority in outgoing MLD messages.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

23.4.2 MLD Snooping-proxy VLAN

Click the **MLD Snooping-proxy** link and then the **VLAN** link in the **Advanced Application > Multicast > IPv6 Multicast** screen to display the screen as shown. See [Section 23.1 on page 214](#) for more information on multicasting.

Figure 156 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN

VLAN MLD Snooping-proxy Port Role Setting

VID:

Upstream	Query Interval	125000	milliseconds
	Maximum Response Delay	10000	milliseconds
	Robustness Variable	2	
Downstream	Query Interval	125000	milliseconds
	Maximum Response Delay	10000	milliseconds
	Robustness Variable	2	

Add Cancel Clear

Index	VID	Delete
1	1234	☐

Delete Cancel

The following table describes the labels in this screen.

Table 101 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN

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

Table 101 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN

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

23.4.3 MLD Snooping-proxy VLAN Port Role Setting

Click the **Port Role Setting** link in the **Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN** screen to display the screen as shown. See [Section 23.1 on page 214](#) for more information on multicasting.

Figure 157 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN > Port Role Setting (Standalone mode)

Port Role Setting VLAN

MLD Snooping-proxy VLAN ID

Port	Port Role	Leave Mode	Leave Timeout	Fast Leave Timeout
*	None	Normal		
1	None	Immediate	4000	200
2	Upstream	Immediate	4000	200
3	Upstream	Immediate	4000	200
4	None	Immediate	4000	200
5	None	Immediate	4000	200
6	Downstream	Immediate	4000	200
7	None	Immediate	4000	200
8	None	Immediate	4000	200
9	None	Immediate	4000	200
10	None	Immediate	4000	200

Apply Cancel

Figure 158 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN > Port Role Setting (Stacking mode)

Port Role Setting VLAN

MLD Snooping-proxy VLAN ID

SLOT 1

Port	Port Role	Leave Mode	Leave Timeout	Fast Leave Timeout
	None	Normal		
1/1	None	Normal	4000	4000
1/2	None	Normal	4000	4000
	None	Normal	4000	4000
1/48	None	Normal	4000	4000
1/49	None	Normal	4000	4000
1/50	None	Normal	4000	4000

Apply Cancel

The following table describes the labels in this screen.

Table 102 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > VLAN > Port Role Setting

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

23.4.4 MLD Snooping-proxy Filtering

Use this screen to configure the Switch's MLD filtering settings. Click the **MLD Snooping-proxy** link and then the **Filtering** link in the **Advanced Application > Multicast > IPv6 Multicast** screen to display the screen as shown. See [Section 23.1 on page 214](#) for more information on multicasting.

Figure 159 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering (Standalone mode)

Port	Group Limit	Max Group Num.	Filtering Profile
*	☐		Default ▼
1	☐	0	Default ▼
2	☐	0	Default ▼
3	☐	0	Default ▼
4	☐	0	Default ▼
5	☐	0	Default ▼
6	☐	0	Default ▼
7	☐	0	Default ▼
8	☐	0	Default ▼
9	☐	0	Default ▼
10	☐	0	Default ▼
11	☐	0	Default ▼

Figure 160 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering (Stacking mode)

Port	Group Limit	Max Group Num.	Filtering Profile
1/*	☐		Default ▼
1/1	☐	0	Default ▼
1/2	☐		Default ▼
1/49	☐	0	Default ▼
1/49	☐	0	Default ▼
1/50	☐	0	Default ▼

The following table describes the labels in this screen.

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

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

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

LABEL	DESCRIPTION
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Group Limit	Select this option to limit the number of multicast groups this port is allowed to join.
Max Group Num.	Enter the number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new MLD Report message is dropped on this port.
Filtering Profile	Select the name of the MLD filtering profile to use for this port. Otherwise, select Default to prohibit the port from joining any multicast group. You can create MLD filtering profiles in the Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering > Filtering Profile screen.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.

23.4.5 MLD Snooping-proxy Filtering Profile

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

Figure 161 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering > Filtering Profile

Filtering Profile Filtering

Profile Setup

Profile Name

Start Address

End Address

Profile Name	Start Address	End Address	Delete
Default	0:0:0:0:0:0	0:0:0:0:0:0	☐

The following table describes the labels in this screen.

Table 104 Advanced Application > Multicast > IPv6 Multicast > MLD Snooping-proxy > Filtering > Filtering Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile for identification purposes. To configure additional rule(s) for a profile that you have already added, enter the profile name and specify a different IP multicast address range.
Start Address	Type the starting multicast IPv6 address for a range of multicast IPv6 addresses that you want to belong to the MLD filtering profile.
End Address	Type the ending multicast IPv6 address for a range of IPv6 addresses that you want to belong to the MLD filtering profile. If you want to add a single multicast IPv6 address, enter it in both the Start Address and End Address fields.
Add	Click this to create a new entry. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to reset the fields to the factory defaults.
Profile Name	This field displays the descriptive name of the profile.
Start Address	This field displays the start of the multicast IPv6 address range.
End Address	This field displays the end of the multicast IPv6 address range.
Delete	To delete the profile(s) and all the accompanying rules, select the profile(s) that you want to remove in the Delete Profile column, then click the Delete button. To delete a rule(s) from a profile, select the rule(s) that you want to remove in the Delete Rule column, then click the Delete button.
Cancel	Click Cancel to clear the Delete Profile/Delete Rule check boxes.

23.5 MVR Overview

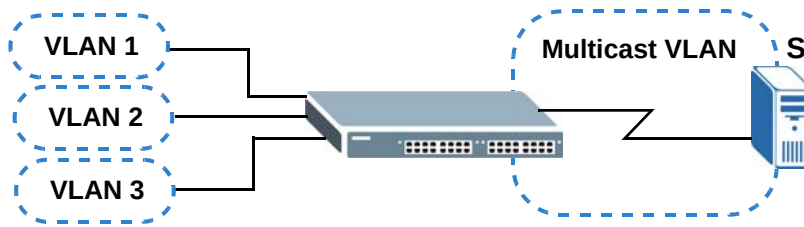
Multicast VLAN Registration (MVR) is designed for applications (such as Media-on-Demand (MoD)) that use multicast traffic across an Ethernet ring-based service provider network.

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

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

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

Figure 162 MVR Network Example



23.5.1 Types of MVR Ports

In MVR, a source port is a port on the Switch that can send and receive multicast traffic in a multicast VLAN while a receiver port can only receive multicast traffic. Once configured, the Switch maintains a forwarding table that matches the multicast stream to the associated multicast group.

23.5.2 MVR Modes

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

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

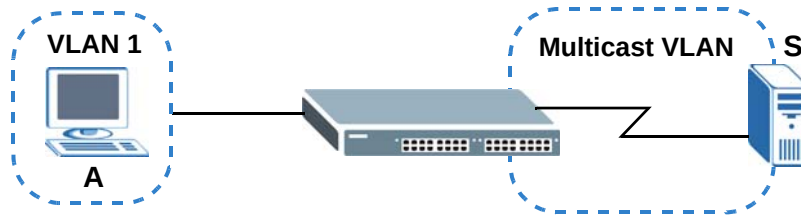
In compatible mode, the Switch does not send any IGMP reports. In this case, you must manually configure the forwarding settings on the multicast devices in the multicast VLAN.

23.5.3 How MVR Works

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

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

When the subscriber changes the channel or turns off the computer, an IGMP leave message is sent to the Switch to leave the multicast group. The Switch sends a query to VLAN 1 on the receiver port (in this case, an uplink port on the Switch). If there is another subscriber device connected to this port in the same subscriber VLAN, the receiving port will still be on the list of forwarding destination for the multicast traffic. Otherwise, the Switch removes the receiver port from the forwarding table.

Figure 163 MVR Multicast Television Example

23.6 General MVR Configuration

Use the **MVR** screen to create multicast VLANs and select the receiver port(s) and a source port for each multicast VLAN. Click **Advanced Application > Multicast > Multicast Setup > MVR** to display the screen as shown next.

Note: You can create up to five multicast VLANs and up to 256 multicast rules on the Switch.

Note: Your Switch automatically creates a static VLAN (with the same VID) when you create a multicast VLAN in this screen.

Figure 164 Advanced Application > Multicast > Multicast Setup > MVR (Standalone mode)

MVR

Multicast SetupGroup Configuration

Active☐

Group Name

Multicast VLAN ID

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	☐	☐	☒	☐

Add

Cancel

VLAN	Active	Name	Mode	Source Port	Receiver Port	802.1p	Delete

Delete

Cancel

Figure 165 Advanced Application > Multicast > Multicast Setup > MVR (Stacking mode)

MVR [Multicast Setup](#) [Group Configuration](#)

Active ☐

Group Name

Multicast VLAN ID

802.1p Priority

Mode ☒ Dynamic ☐ Compatible

SLOT 1 ▼

Port	Source Port	Receiver Port	None	Tagging
1/*		None ▼		☐
1/1	☐	☐	☐	☐
1/2	☐	☐	☐	☐
1/49	☐	☐	☐	☐
1/50	☐	☐	☐	☐

Add Cancel

VLAN	Active	Name	Mode	Source Port	Receiver Port	802.1p	Delete

Delete Cancel

The following table describes the related labels in this screen.

Table 105 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.
Group Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Multicast VLAN ID	Enter the VLAN ID (1 to 4094) of the multicast VLAN.
802.1p Priority	Select a priority level (0-7) with which the Switch replaces the priority in outgoing IGMP or MLD control packets (belonging to this multicast VLAN).
Mode	Specify the MVR mode on the Switch. Choices are Dynamic and Compatible . Select Dynamic to send IGMP reports or MLD messages to all MVR source ports in the multicast VLAN. Select Compatible to set the Switch not to send IGMP reports or MLD messages.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.

Table 105 Advanced Application > Multicast > Multicast Setting > MVR (continued)

LABEL	DESCRIPTION
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Source Port	Select this option to set this port as the MVR source port that sends and receives multicast traffic. All source ports must belong to a single multicast VLAN.
Receiver Port	Select this option to set this port as a receiver port that only receives multicast traffic.
None	Select this option to set the port not to participate in MVR. No MVR multicast traffic is sent or received on this port.
Tagging	Select this checkbox if you want the port to tag the VLAN ID in all outgoing frames transmitted.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
VLAN	This field displays the multicast VLAN ID. Click on an index number to change the settings.
Active	This field displays whether the multicast group is enabled or not.
Name	This field displays the descriptive name for this setting.
Mode	This field displays the MVR mode.
Source Port	This field displays the source port number(s).
Receiver Port	This field displays the receiver port number(s).
802.1p	This field displays the priority level.
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.

23.6.1 MVR Group Configuration

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

Use this screen to configure MVR IP multicast group address(es). Click the **Group Configuration** link in the **MVR** screen.

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

Figure 166 Advanced Application > Multicast > Multicast Setup > MVR > Group Configuration

The following table describes the labels in this screen.

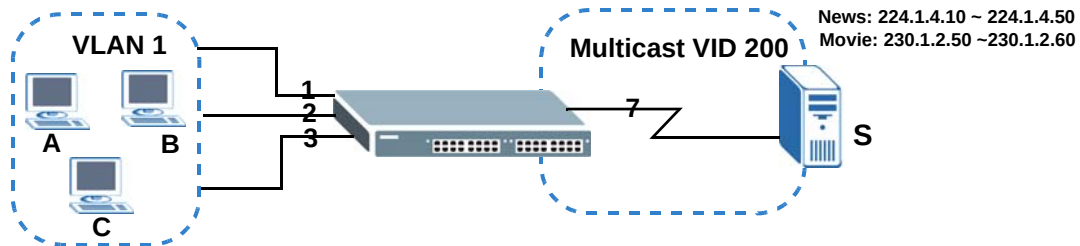
Table 106 Advanced Application > Multicast > Multicast Setup > MVR > Group Configuration

LABEL	DESCRIPTION
Multicast VLAN ID	Select a multicast VLAN ID (that you configured in the MVR screen) from the drop-down list box.
Group Name	Enter a descriptive name for identification purposes.
Start Address	Enter the starting IP multicast address of the multicast group in dotted decimal notation. Refer to Section 23.1.1 on page 214 for more information on IP multicast addresses.
End Address	Enter the ending IP multicast address of the multicast group in dotted decimal notation. Enter the same IP address as the Start Address field if you want to configure only one IP address for a multicast group. Refer to Section 23.1.1 on page 214 for more information on IP multicast addresses.
Add	Click this to create a new entry. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
MVLAN	This field displays the multicast VLAN ID.
Group Name	This field displays the descriptive name for this setting.
Start Address	This field displays the starting IP address of the multicast group.
End Address	This field displays the ending IP address of the multicast group.
Delete	Select the entry(ies) that you want to remove in the Delete column, then click the Delete button to remove the selected entry(ies) from the table. Note: If you delete a multicast VLAN, all multicast groups in this VLAN will also be removed.
Cancel	Select Cancel to clear the checkbox(es) in the table.

23.6.2 MVR Configuration Example

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

Figure 167 MVR Configuration Example



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

Figure 168 MVR Configuration Example

The screenshot shows the 'MVR' configuration page with the 'Multicast Setup' tab selected. The configuration includes:

- Active:** ☒
- Group Name:** Premium
- Multicast VLAN ID:** 200
- 802.1p Priority:** 0
- Mode:** ☒ Dynamic ☐ Compatible

 Below this is a table for port configuration:

Port	Source Port	Receiver Port	None	Tagging
*		Receiver		☐
1	☐	☒	☐	☐
2	☐	☒	☐	☐
3	☐	☒	☐	☐
4	☐	☐	☒	☐
5	☐	☐	☒	☐
6	☐	☐	☒	☐
7	☒	☐	☐	☒
8	☐	☐	☒	☐
9	☐	☐	☒	☐
10	☐	☐	☒	☐

 At the bottom, there are 'Add' and 'Cancel' buttons, and a large red 'EXAMPLE' stamp.

To set the Switch to forward the multicast group traffic to the subscribers, configure multicast group settings in the **Group Configuration** screen. The following figure shows an example where two IPv4 multicast groups (**News** and **Movie**) are configured for the multicast VLAN 200.

Figure 169 MVR Group Configuration Example

Group Configuration MVR

Multicast VLAN ID 200

Group Name	Movie
Start Address	230.1.2.50
End Address	230.1.2.60

Add Cancel

EXAMPLE

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

Delete Cancel

Figure 170 MVR Group Configuration Example

Group Configuration MVR

Multicast VLAN ID 11

Group Name	
Start Address	
End Address	

Add Cancel

EXAMPLE

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

Delete Cancel

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

24.1 Authentication, Authorization and Accounting (AAA)

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

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

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

The external servers that perform authentication, authorization and accounting functions are known as AAA servers. The Switch supports RADIUS (Remote Authentication Dial-In User Service, see [Section 24.1.2 on page 242](#)) and TACACS+ (Terminal Access Controller Access-Control System Plus, see [Section 24.1.2 on page 242](#)) as external authentication, authorization and accounting servers.

Figure 171 AAA Server



24.1.1 Local User Accounts

By storing user profiles locally on the Switch, your Switch is able to authenticate and authorize users without interacting with a network AAA server. However, there is a limit on the number of users you may authenticate in this way (See [Chapter 44 on page 412](#)).

24.1.2 RADIUS and TACACS+

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

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

Table 107 RADIUS vs TACACS+

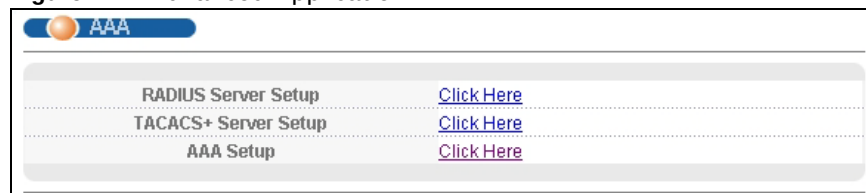
	RADIUS	TACACS+
Transport Protocol	UDP (User Datagram Protocol)	TCP (Transmission Control Protocol)
Encryption	Encrypts the password sent for authentication.	All communication between the client (the Switch) and the TACACS server is encrypted.

24.2 AAA Screens

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

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

Figure 172 Advanced Application > AAA



24.2.1 RADIUS Server Setup

Use this screen to configure your RADIUS server settings. See [Section 24.1.2 on page 242](#) for more information on RADIUS servers and [Section 24.3 on page 250](#) 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 173 Advanced Application > AAA > RADIUS Server Setup

RADIUS Server Setup AAA

Authentication Server

Mode: index-priority

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 108 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 .

Table 108 Advanced Application > AAA > RADIUS Server 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.
Accounting Server	Use this section to configure your RADIUS accounting server settings.
Timeout	Specify the amount of time in seconds that the Switch waits for an accounting request response from the RADIUS accounting server.
Index	This is a read-only number representing a RADIUS accounting server entry.
IP Address	Enter the IP address of an external RADIUS accounting server in dotted decimal notation.
UDP Port	The default port of a RADIUS accounting server for accounting is 1813 . You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS accounting server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS accounting server and the Switch.
Delete	Check this box if you want to remove an existing RADIUS accounting server entry from the Switch. This entry is deleted when you click Apply .
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

24.2.2 TACACS+ Server Setup

Use this screen to configure your TACACS+ server settings. See [Section 24.1.2 on page 242](#) 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 174 Advanced Application > AAA > TACACS+ Server Setup

TACACS+ Server Setup AAA

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 109 Advanced Application > AAA > TACACS+ Server Setup

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

Table 109 Advanced Application > AAA > TACACS+ Server Setup (continued)

LABEL	DESCRIPTION
Delete	Check this box if you want to remove an existing TACACS+ server entry from the Switch. This entry is deleted when you click Apply .
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation 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.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external TACACS+ accounting server and the Switch. This key is not sent over the network. This key must be the same on the external TACACS+ accounting server and the Switch.
Delete	Check this box if you want to remove an existing TACACS+ accounting server entry from the Switch. This entry is deleted when you click Apply .
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

24.2.3 AAA Setup

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

Figure 175 Advanced Application > AAA > AAA Setup

AAA Setup AAA

Authentication

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

Authorization

Type	Active	Console	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 ▼

The following table describes the labels in this screen.

Table 110 Advanced Application > AAA > AAA Setup

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

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

LABEL	DESCRIPTION
Login	These fields specify which database the Switch should use (first, second and third) to authenticate administrator accounts (users for Switch management). Configure the local user accounts in the Access Control > Logins screen. The TACACS+ and RADIUS are external servers. Before you specify the priority, make sure you have set up the corresponding database correctly first. You can specify up to three methods for the Switch to authenticate administrator accounts. The Switch checks the methods in the order you configure them (first Method 1, then Method 2 and finally Method 3). You must configure the settings in the Method 1 field. If you want the Switch to check other sources for administrator accounts, specify them in Method 2 and Method 3 fields. Select local to have the Switch check the administrator accounts configured in the Access Control > Logins screen. Select radius to have the Switch check the administrator accounts configured via the RADIUS Server. Select tacacs+ to have the Switch check the administrator accounts configured via the TACACS+ Server.
Authorization	Use this section to configure authorization settings on the Switch.
Type	Set whether the Switch provides the following services to a user. • Exec: Allow an administrator which logs in the Switch through Telnet or SSH to have different access privilege level assigned via the external server. • Dot1x: Allow an IEEE 802.1x client to have different bandwidth limit or VLAN ID assigned via the external server.
Active	Select this to activate authorization for a specified event types.
Console	Select this to allow an administrator which logs in the Switch through the console port to have different access privilege level assigned via the external server.
Method	Select whether you want to use RADIUS or TACACS+ for authorization of specific types of events. RADIUS is the only method for IEEE 802.1x authorization.
Accounting	Use this section to configure accounting settings on the Switch.
Update Period	This is the amount of time in minutes before the Switch sends an update to the accounting server. This is only valid if you select the start-stop option for the Exec or Dot1x entries.
Type	The Switch supports the following types of events to be sent to the accounting server(s): • System - Configure the Switch to send information when the following system events occur: system boots up, system shuts down, system accounting is enabled, system accounting is disabled • Exec - Configure the Switch to send information when an administrator logs in and logs out via the console port, telnet or SSH. • Dot1x - Configure the Switch to send information when an IEEE 802.1x client begins a session (authenticates via the Switch), ends a session as well as interim updates of a session. • Commands - Configure the Switch to send information when commands of specified privilege level and higher are executed on the Switch.
Active	Select this to activate accounting for a specified event types.
Broadcast	Select this to have the Switch send accounting information to all configured accounting servers at the same time. If you don't select this and you have two accounting servers set up, then the Switch sends information to the first accounting server and if it doesn't get a response from the accounting server then it tries the second accounting server.

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

LABEL	DESCRIPTION
Mode	The Switch supports two modes of recording login events. Select: • start-stop - to have the Switch send information to the accounting server when a user begins a session, during a user's session (if it lasts past the Update Period), and when a user ends a session. • stop-only - to have the Switch send information to the accounting server only when a user ends a session.
Method	Select whether you want to use RADIUS or TACACS+ for accounting of specific types of events. TACACS+ is the only method for recording Commands type of event.
Privilege	This field is only configurable for Commands type of event. Select the threshold command privilege level for which the Switch should send accounting information. The Switch will send accounting information when commands at the level you specify and higher are executed on the Switch.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

24.2.4 Vendor Specific Attribute

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

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

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

The VSAs are composed of the following:

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

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

The following table describes the VSAs supported on the Switch. Note that these attributes only work when you enable authorization (see [Section 24.2.3 on page 246](#)).

Table 111 Supported VSAs

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

24.2.5 Tunnel Protocol Attribute

You can configure tunnel protocol attributes on the RADIUS server (refer to your RADIUS server documentation) to assign a port on the Switch to a VLAN based on IEEE 802.1x authentication. The port VLAN settings are fixed and untagged. This will also set the port's VID. The following table describes the values you need to configure. Note that these attributes only work when you enable authorization (see [Section 24.2.3 on page 246](#)).

Table 112 Supported Tunnel Protocol Attribute

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

24.3 Supported RADIUS Attributes

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

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

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

24.3.1 Attributes Used for Authentication

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

24.3.1.1 Attributes Used for Authenticating Privilege Access

User-Name

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

User-Password

NAS-Identifier

NAS-IP-Address

24.3.1.2 Attributes Used to Login Users

User-Name

User-Password

NAS-Identifier

NAS-IP-Address

24.3.1.3 Attributes Used by the IEEE 802.1x Authentication

User-Name

NAS-Identifier

NAS-IP-Address

NAS-Port

NAS-Port-Type

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

Calling-Station-Id

Frame-MTU

EAP-Message

State

Message-Authenticator

24.3.2 Attributes Used for Accounting

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

24.3.2.1 Attributes Used for Accounting System Events

NAS-IP-Address

NAS-Identifier

Acct-Status-Type

Acct-Session-ID

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

Acct-Delay-Time

24.3.2.2 Attributes Used for Accounting Exec Events

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

Table 113 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 114 RADIUS Attributes - Exec Events via Telnet/SSH

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

24.3.2.3 Attributes Used for Accounting IEEE 802.1x Events

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

Table 115 RADIUS Attributes - Exec Events via Console

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

IP Source Guard

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

25.1 IP Source Guard Overview

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

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

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

The Switch builds the binding table by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings).

IP source guard consists of the following features:

- Static bindings. Use this to create static bindings in the binding table.
- DHCP snooping. Use this to filter unauthorized DHCP packets on the network and to build the binding table dynamically.
- ARP inspection. Use this to filter unauthorized ARP packets on the network.

If you want to use dynamic bindings to filter unauthorized ARP packets (typical implementation), you have to enable DHCP snooping before you enable ARP inspection.

25.1.1 DHCP Snooping Overview

Use DHCP snooping to filter unauthorized DHCP packets on the network and to build the binding table dynamically. This can prevent clients from getting IP addresses from unauthorized DHCP servers.

25.1.1.1 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.

25.1.1.2 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 176 DHCP Snooping Database File Format

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<binding-1> <checksum-1>
<binding-2> <checksum-1-2>
...
...
<binding-n> <checksum-1-2-...-n>
END
```

The <initial-checksum> helps distinguish between the bindings in the latest update and the bindings from previous updates. Each binding consists of 72 bytes, a space, and another checksum that is used to validate the binding when it is read. If the calculated checksum is not equal to the checksum in the file, that binding and all others after it are ignored.

25.1.1.3 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 39 on page 369](#) 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 39 on page 369](#)).

25.1.1.4 Configuring DHCP Snooping

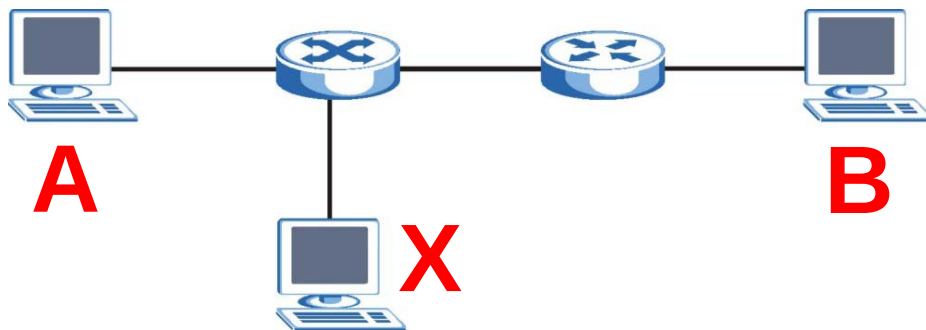
Follow these steps to configure DHCP snooping on the Switch.

- 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.

25.1.2 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 177 Example: Man-in-the-middle Attack



In this example, computer **B** tries to establish a connection with computer **A**. Computer **X** is in the same broadcast domain as computer **A** and intercepts the ARP request for computer **A**. Then, computer **X** does the following things:

- It pretends to be computer **A** and responds to computer **B**.
- It pretends to be computer **B** and sends a message to computer **A**.

As a result, all the communication between computer **A** and computer **B** passes through computer **X**. Computer **X** can read and alter the information passed between them.

25.1.2.1 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 10 on page 123](#)).

- They are stored only in volatile memory.
- They do not use the same space in memory that regular MAC address filters use.
- They appear only in the **ARP Inspection** screens and commands, not in the **MAC Address Filter** screens and commands.

25.1.2.2 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.

25.1.2.3 Syslog

The Switch can send syslog messages to the specified syslog server ([Chapter 46 on page 437](#)) when it forwards or discards ARP packets. The Switch can consolidate log messages and send log messages in batches to make this mechanism more efficient.

25.1.2.4 Configuring ARP Inspection

Follow these steps to configure ARP inspection on the Switch.

- 1 Configure DHCP snooping. See [Section 25.1.1.4 on page 256](#).

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.

25.2 IP Source Guard

Use this screen to look at the current bindings for DHCP snooping and ARP inspection. Bindings are used by DHCP snooping and ARP inspection to distinguish between authorized and unauthorized packets in the network. The Switch learns the bindings by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings). To open this screen, click **Advanced Application > IP Source Guard**.

Figure 178 IP Source Guard

IP Source Guard						
Static Binding DHCP Snooping ARP Inspection						
Index	MAC Address	IP Address	Lease	Type	VID	Port
1	00:23:5a:1e:c6:89	172.16.1.2	infinity	static	12	3

The following table describes the labels in this screen.

Table 116 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. In stacking mode, the first number represents the slot and the second the port number.

25.3 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 179 IP Source Guard > Static Binding (Standalone mode)

IP Source Guard Static Binding IPSG

ARP Freeze :

Condition ☐ All ☐ Port List ☐ VLAN List

Static Binding :

MAC Address : : : : :

IP Address

VLAN

Port ☐ ☒ Any

Index	MAC Address	IP Address	Lease	Type	VLAN	Port	Delete
1	00:23:5a:1e:c6:89	172.16.1.2	infinity	static	12	3	☐

Figure 180 IP Source Guard > Static Binding (Stacking mode)

IP Source Guard Static Binding IPSG

ARP Freeze :

Condition

☐ All

☐ Port List **ARP Freeze**

☐ VLAN List

Static Binding :

MAC Address : : : : :

IP Address

VLAN

Port ☐ SLOT 1 ▾ /

☒ Any

Add Cancel Clear

Index	MAC Address	IP Address	Lease	Type	VLAN	Port	Delete
Delete Cancel							

The following table describes the labels in this screen.

Table 117 IP Source Guard > Static Binding

LABEL	DESCRIPTION
ARP Freeze	ARP Freeze allows you to automatically create static bindings from the current ARP entries (either dynamically learned or static ARP entries) until the Switch's binding table is full. Note: The ARP learning mode should be set to ARP-Request in the IP Application > ARP Setup > ARP Learning screen before you use the ARP Freeze feature.
Condition	All - Select this and click ARP Freeze to have the Switch automatically add all the current ARP entries to the static bindings table. Port List - Select this and enter the number of the port(s) (separated by a comma). In stacking mode, the first number represents the slot and the second the port number. Enter 1/1-1/24,2/28 for ports 1 to 24 for the Switch in slot 1 and port 28 for the Switch in slot 2, for example. ARP entries learned on the specified port(s) are added to the static bindings table after you click ARP Freeze. VLAN List - Select this and enter the ID number of the VLAN(s) (separated by a comma). ARP entries for the specified VLAN(s) are added to the static bindings table after you click ARP Freeze.
Static Binding	
MAC Address	Enter the source MAC address in the binding.
IP Address	Enter the IP address assigned to the MAC address in the binding.
VLAN	Enter the source VLAN ID in the binding.

Table 117 IP Source Guard > Static Binding (continued)

LABEL	DESCRIPTION
Port	Specify the port(s) in the binding. If this binding has one port, select the first radio button and enter the port number in the field to the right. In stacking mode, the first field is the slot ID and the second field is the port number. If this binding applies to all ports, select Any .
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values above based on the last selected static binding or, if not applicable, to clear the fields above.
Clear	Click Clear to reset the fields to the factory defaults.
Index	This field displays a sequential number for each binding. Click on an index number to view more details or change the settings.
MAC Address	This field displays the source MAC address in the binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
Lease	This field displays how long the binding is valid.
Type	This field displays how the Switch learned the binding. static : This binding was learned from information provided manually by an administrator.
VLAN	This field displays the source VLAN ID in the binding.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.
Delete	Select the entry(ies) that you want to remove in the Delete column, then click the Delete button to remove the selected entry(ies) from the table.
Cancel	Click this to clear the Delete check boxes above.

25.4 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 181 IP Source Guard > DHCP Snooping


DHCP Snooping

[Configure](#)

[IPSG](#)

Database Status

Description	Status
Agent URL	
Write delay timer	300 seconds
Abort timer	300 seconds
Agent running	
Delay timer expiry	Not Running
Abort timer expiry	Not Running
Last succeeded time	
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 118 IP Source Guard > DHCP Snooping

LABEL	DESCRIPTION
Database Status	
	This section displays the current settings for the DHCP snooping database. You can configure them in the DHCP Snooping Configure screen. See Section 25.5 on page 264 .
Agent URL	This field displays the location of the DHCP snooping database.
Write delay timer	This field displays how long (in seconds) the Switch tries to complete a specific update in the DHCP snooping database before it gives up.
Abort timer	This field displays how long (in seconds) the Switch waits to update the DHCP snooping database after the current bindings change.
	This section displays information about the current update and the next update of the DHCP snooping database.

Table 118 IP Source Guard > DHCP Snooping (continued)

LABEL	DESCRIPTION
Agent running	This field displays the status of the current update or access of the DHCP snooping database. none : The Switch is not accessing the DHCP snooping database. read : The Switch is loading dynamic bindings from the DHCP snooping database. write : The Switch is updating the DHCP snooping database.
Delay timer expiry	This field displays how much longer (in seconds) the Switch tries to complete the current update before it gives up. It displays Not Running if the Switch is not updating the DHCP snooping database right now.
Abort timer expiry	This field displays when (in seconds) the Switch is going to update the DHCP snooping database again. It displays Not Running if the current bindings have not changed since the last update.
	This section displays information about the last time the Switch updated the DHCP snooping database.
Last succeeded time	This field displays the last time the Switch updated the DHCP snooping database successfully.
Last failed time	This field displays the last time the Switch updated the DHCP snooping database unsuccessfully.
Last failed reason	This field displays the reason the Switch updated the DHCP snooping database unsuccessfully.
	This section displays historical information about the number of times the Switch successfully or unsuccessfully read or updated the DHCP snooping database.
Total attempts	This field displays the number of times the Switch has tried to access the DHCP snooping database for any reason.
Startup failures	This field displays the number of times the Switch could not create or read the DHCP snooping database when the Switch started up or a new URL is configured for the DHCP snooping database.
Successful transfers	This field displays the number of times the Switch read bindings from or updated the bindings in the DHCP snooping database successfully.
Failed transfers	This field displays the number of times the Switch was unable to read bindings from or update the bindings in the DHCP snooping database.
Successful reads	This field displays the number of times the Switch read bindings from the DHCP snooping database successfully.
Failed reads	This field displays the number of times the Switch was unable to read bindings from the DHCP snooping database.
Successful writes	This field displays the number of times the Switch updated the bindings in the DHCP snooping database successfully.
Failed writes	This field displays the number of times the Switch was unable to update the bindings in the DHCP snooping database.
Database detail	
First successful access	This field displays the first time the Switch accessed the DHCP snooping database for any reason.
Last ignored bindings counters	This section displays the number of times and the reasons the Switch ignored bindings the last time it read bindings from the DHCP binding database. You can clear these counters by restarting the Switch or using CLI commands. See the Ethernet Switch CLI Reference Guide.
Binding collisions	This field displays the number of bindings the Switch ignored because the Switch already had a binding with the same MAC address and VLAN ID.
Invalid interfaces	This field displays the number of bindings the Switch ignored because the port number was a trusted interface or does not exist anymore.

Table 118 IP Source Guard > DHCP Snooping (continued)

LABEL	DESCRIPTION
Parse failures	This field displays the number of bindings the Switch ignored because the Switch was unable to understand the binding in the DHCP binding database.
Expired leases	This field displays the number of bindings the Switch ignored because the lease time had already expired.
Unsupported vlans	This field displays the number of bindings the Switch ignored because the VLAN ID does not exist anymore.
Last ignored time	This field displays the last time the Switch ignored any bindings for any reason from the DHCP binding database.
Total ignored bindings counters	This section displays the reasons the Switch has ignored bindings any time it read bindings from the DHCP binding database. You can clear these counters by restarting the Switch or using CLI commands. See the Ethernet Switch CLI Reference Guide.
Binding collisions	This field displays the number of bindings the Switch has ignored because the Switch already had a binding with the same MAC address and VLAN ID.
Invalid interfaces	This field displays the number of bindings the Switch has ignored because the port number was a trusted interface or does not exist anymore.
Parse failures	This field displays the number of bindings the Switch has ignored because the Switch was unable to understand the binding in the DHCP binding database.
Expired leases	This field displays the number of bindings the Switch has ignored because the lease time had already expired.
Unsupported vlans	This field displays the number of bindings the Switch has ignored because the VLAN ID does not exist anymore.

25.5 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 182 IP Source Guard > DHCP Snooping > Configure

DHCP Snooping Configure **Port** **VLAN** **DHCP Snooping**

Active ☐

DHCP Vlan ☐ Disable

Database

Agent URL

Timeout interval seconds

Write delay interval seconds

Renew DHCP Snooping URL

The following table describes the labels in this screen.

Table 119 IP Source Guard > DHCP Snooping > Configure

LABEL	DESCRIPTION
Active	Select this to enable DHCP snooping on the Switch. You still have to enable DHCP snooping on specific VLAN and specify trusted ports. Note: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.
DHCP Vlan	Select a VLAN ID if you want the Switch to forward DHCP packets to DHCP servers on a specific VLAN. Note: You have to enable DHCP snooping on the DHCP VLAN too. You can select an option 82 profile in the DHCP Snooping VLAN Configure screen (Section 25.5.2 on page 267) to help the DHCP servers distinguish between DHCP requests from different VLAN. Select Disable if you do not want the Switch to forward DHCP packets to a specific VLAN.
Database	If Timeout interval is greater than Write delay interval, it is possible that the next update is scheduled to occur before the current update has finished successfully or timed out. In this case, the Switch waits to start the next update until it completes the current one.
Agent URL	Enter the location of the DHCP snooping database. The location should be expressed like this: tftp:// {domain name or IP address} / directory, if applicable / file name; for example, tftp://192.168.10.1/database.txt.
Timeout interval	Enter how long (10-65535 seconds) the Switch tries to complete a specific update in the DHCP snooping database before it gives up.
Write delay interval	Enter how long (10-65535 seconds) the Switch waits to update the DHCP snooping database the first time the current bindings change after an update. Once the next update is scheduled, additional changes in current bindings are automatically included in the next update.

Table 119 IP Source Guard > DHCP Snooping > Configure (continued)

LABEL	DESCRIPTION
Renew DHCP Snooping URL	Enter the location of a DHCP snooping database, and click Renew if you want the Switch to load it. You can use this to load dynamic bindings from a different DHCP snooping database than the one specified in Agent URL . When the Switch loads dynamic bindings from a DHCP snooping database, it does not discard the current dynamic bindings first. If there is a conflict, the Switch keeps the dynamic binding in volatile memory and updates the Binding collisions counter in the DHCP Snooping screen (Section 25.4 on page 261).
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

25.5.1 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 183 IP Source Guard > DHCP Snooping Port Configure (Standalone mode)

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

Apply Cancel

Figure 184 IP Source Guard > DHCP Snooping Port Configure (Stacking mode)

DHCP Snooping Port Configure [Configure](#)

SLOT 1 ▼

Port	Server Trusted state	Rate (pps)
1/*	Untrusted ▼	
1/1	Untrusted ▼	0
1/2	Untrusted ▼	0
1/48	Untrusted ▼	0
1/49	Untrusted ▼	0
1/50	Untrusted ▼	0

Apply Cancel

The following table describes the labels in this screen.

Table 120 IP Source Guard > DHCP Snooping Port Configure

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number. * means all ports (on the same Switch).
Server Trusted state	Select whether this port is a trusted port (Trusted) or an untrusted port (Untrusted). Trusted ports are connected to DHCP servers or other switches, and the Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. Untrusted ports are connected to subscribers, and the Switch discards DHCP packets from untrusted ports in the following situations: - The packet is a DHCP server packet (for example, OFFER, ACK, or NACK). - The source MAC address and source IP address in the packet do not match any of the current bindings. - The packet is a RELEASE or DECLINE packet, and the source MAC address and source port do not match any of the current bindings. - The rate at which DHCP packets arrive is too high.
Rate (pps)	Specify the maximum number for DHCP packets (1-2048) that the Switch receives from each port each second. The Switch discards any additional DHCP packets. Enter 0 to disable this limit, which is recommended for trusted ports.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

25.5.2 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 39 on page 369](#)) 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 185 IP Source Guard > DHCP Snooping VLAN Configure

DHCP Snooping VLAN Configure [Port Configure](#)

Show VLAN Start VID End VID

VID	Enabled	Option 82 Profile
*	No v	v

The following table describes the labels in this screen.

Table 121 IP Source Guard > 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.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to all ports in the specified VLAN(s). The Switch adds the information (such as slot number, port number, VLAN ID and/or system name) specified in the profile to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN. You can specify the DHCP VLAN in the DHCP Snooping Configure screen (see Section 25.5 on page 264).
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

25.5.3

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

Figure 186 IP Source Guard >

Port DHCP Snooping VLAN Configure

VID

Port

Option 82 Profile

Add Cancel Clear

Index	VID	Port	Profile Name	Delete
1	777	7	default1	☐

Delete Cancel

The following table describes the labels in this screen.

Table 122 IP Source Guard >

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN you want to configure here.
Port	Enter the number of port(s) to which you want to apply the specified DHCP option 82 profile. You can enter multiple ports separated by (no space) comma (,) or hyphen (-) for a range. For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7. In stacking mode, the first number represents the slot and the second the port number. Enter 1/1-1/24,2/28 for ports 1 to 24 for the Switch in slot 1 and port 28 for the Switch in slot 2, for example.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to the specified port(s) in this VLAN. The Switch adds the information (such as slot number, port number, VLAN ID and/or system name) specified in the profile to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN. You can specify the DHCP VLAN in the DHCP Snooping Configure screen (see Section 25.5 on page 264). Note: The profile you select here has priority over the one you select in the DHCP Snooping > Configure > VLAN screen.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values above based on the last selected entry or, if not applicable, to clear the fields above.
Clear	Click Clear to reset the fields to the factory defaults.
Index	This field displays a sequential number for each entry. Click an index number to change the settings.
VID	This field displays the VLAN to which the port(s) belongs.
Port	This field displays the port(s) to which the Switch applies the settings. In stacking mode, the first number represents the slot and the second the port number.
Profile Name	This field displays the DHCP option 82 profile that the Switch applies to the port(s).
Delete	Select the entry(ies) that you want to remove in the Delete column, then click the Delete button to remove the selected entry(ies) from the table.
Cancel	Click this to clear the Delete check boxes above.

25.6 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 187 IP Source Guard > ARP Inspection Status

The following table describes the labels in this screen.

Table 123 IP Source Guard > ARP Inspection Status

LABEL	DESCRIPTION
Total number of filters	This field displays the current number of MAC address filters that were created because the Switch identified unauthorized ARP packets.
Index	This field displays a sequential number for each MAC address filter.
MAC Address	This field displays the source MAC address in the MAC address filter.
VID	This field displays the source VLAN ID in the MAC address filter.
Port	This field displays the source port of the discarded ARP packet. In stacking mode, the first field is the slot ID and the second field is the port number.
Expiry (sec)	This field displays how long (in seconds) the MAC address filter remains in the Switch. You can also delete the record manually (Delete).
Reason	This field displays the reason the ARP packet was discarded. MAC+VLAN: The MAC address and VLAN ID were not in the binding table. IP: The MAC address and VLAN ID were in the binding table, but the IP address was not valid. Port: The MAC address, VLAN ID, and IP address were in the binding table, but the port number was not valid.
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.
Change Pages	Click Previous or Next to show the previous/next screen if all status information cannot be seen in one screen.

25.6.1 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 188 IP Source Guard > ARP Inspection VLAN Status

The following table describes the labels in this screen.

Table 124 IP Source Guard > ARP Inspection VLAN Status

LABEL	DESCRIPTION
Show VLAN range	Use this section to specify the VLANs you want to look at in the section below.
Enabled VLAN	Select this to look at all the VLANs on which ARP inspection is enabled in the section below.
Selected VLAN	Select this to look at all the VLANs in a specific range in the section below. Then, enter the lowest VLAN ID (Start VID) and the highest VLAN ID (End VID) you want to look at.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above.
Received	This field displays the total number of ARP packets received from the VLAN since the Switch last restarted.
Request	This field displays the total number of ARP Request packets received from the VLAN since the Switch last restarted.
Reply	This field displays the total number of ARP Reply packets received from the VLAN since the Switch last restarted.
Forwarded	This field displays the total number of ARP packets the Switch forwarded for the VLAN since the Switch last restarted.
Dropped	This field displays the total number of ARP packets the Switch discarded for the VLAN since the Switch last restarted.

25.6.2 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 189 IP Source Guard > ARP Inspection Log Status

ARP Inspection Log Status [Status](#)

Clearing log status table

Total number of logs = 0

Index	Port	VID	Sender Mac	Sender IP	Num Pkts	Reason	Time

The following table describes the labels in this screen.

Table 125 IP Source Guard > ARP Inspection Log Status

LABEL	DESCRIPTION
Clearing log status table	Click Apply to remove all the log messages that were generated by ARP packets and that have not been sent to the syslog server yet.
Total number of logs	This field displays the number of log messages that were generated by ARP packets and that have not been sent to the syslog server yet. If one or more log messages are dropped due to unavailable buffer, there is an entry called overflow with the current number of dropped log messages.
Index	This field displays a sequential number for each log message.
Port	This field displays the source port of the ARP packet. In stacking mode, the first field is the slot ID and the second field is the port number.
VID	This field displays the source VLAN ID of the ARP packet.
Sender Mac	This field displays the source MAC address of the ARP packet.
Sender IP	This field displays the source IP address of the ARP packet.
Num Pkts	This field displays the number of ARP packets that were consolidated into this log message. The Switch consolidates identical log messages generated by ARP packets in the log consolidation interval into one log message. You can configure this interval in the ARP Inspection Configure screen. See Section 25.7 on page 273 .
Reason	This field displays the reason the log message was generated. dhcp deny: An ARP packet was discarded because it violated a dynamic binding with the same MAC address and VLAN ID. static deny: An ARP packet was discarded because it violated a static binding with the same MAC address and VLAN ID. deny: An ARP packet was discarded because there were no bindings with the same MAC address and VLAN ID. dhcp permit: An ARP packet was forwarded because it matched a dynamic binding. static permit: An ARP packet was forwarded because it matched a static binding. In the ARP Inspection VLAN Configure screen, you can configure the Switch to generate log messages when ARP packets are discarded or forwarded based on the VLAN ID of the ARP packet. See Section 25.7.2 on page 276.
Time	This field displays when the log message was generated.

25.7 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 190 IP Source Guard > ARP Inspection Configure

The following table describes the labels in this screen.

Table 126 IP Source Guard > ARP Inspection Configure

LABEL	DESCRIPTION
Active	Select this to enable ARP inspection on the Switch. You still have to enable ARP inspection on specific VLAN and specify trusted ports.
Filter Aging Time	
Filter aging time	This setting has no effect on existing MAC address filters. Enter how long (1-2147483647 seconds) the MAC address filter remains in the Switch after the Switch identifies an unauthorized ARP packet. The Switch automatically deletes the MAC address filter afterwards. Type 0 if you want the MAC address filter to be permanent.
Log Profile	
Log buffer size	Enter the maximum number (1-1024) of log messages that were generated by ARP packets and have not been sent to the syslog server yet. Make sure this number is appropriate for the specified Syslog rate and Log interval . If the number of log messages in the Switch exceeds this number, the Switch stops recording log messages and simply starts counting the number of entries that were dropped due to unavailable buffer. Click Clearing log status table in the ARP Inspection Log Status screen to clear the log and reset this counter. See Section 25.6.2 on page 271 .

Table 126 IP Source Guard > ARP Inspection Configure (continued)

LABEL	DESCRIPTION
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 46 on page 437) 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.

25.7.1 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 191 IP Source Guard > ARP Inspection Port Configure (Standalone mode)

The screenshot displays the 'ARP Inspection Port Configure' interface. At the top, there is a title bar with an orange icon and the text 'ARP Inspection Port Configure', and a 'Configure' link on the right. Below the title bar is a table with the following structure:

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

At the bottom of the screen, there are two buttons: 'Apply' and 'Cancel'.

Figure 192 IP Source Guard > ARP Inspection Port Configure (Stacking mode)

ARP Inspection Port Configure [Configure](#)

SLOT 1 ▼

Port	Trusted State	Limit	
		Rate (pps)	Burst interval (seconds)
1/*	Untrusted ▼		
1/1	Untrusted ▼	15	1
1/2	Untrusted ▼	15	1
1/49	Untrusted ▼	15	1
1/50	Untrusted ▼	15	1

[Apply](#) [Cancel](#)

The following table describes the labels in this screen.

Table 127 IP Source Guard > ARP Inspection Port Configure

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first field is the slot ID and the second field is the port number. * means all ports (on the same Switch).
Trusted State	Select whether this port is a trusted port (Trusted) or an untrusted port (Untrusted). The Switch does not discard ARP packets on trusted ports for any reason. The Switch discards ARP packets on untrusted ports in the following situations: - The sender's information in the ARP packet does not match any of the current bindings. - The rate at which ARP packets arrive is too high. You can specify the maximum rate at which ARP packets can arrive on untrusted ports.
Limit	Rate and Burst Interval settings have no effect on trusted ports.
Rate (pps)	Specify the maximum rate (1-2048 packets per second) at which the Switch receives ARP packets from each port. The Switch discards any additional ARP packets. Enter 0 to disable this limit.
Burst interval (seconds)	The burst interval is the length of time over which the rate of ARP packets is monitored for each port. For example, if the Rate is 15 pps and the burst interval is 1 second, then the Switch accepts a maximum of 15 ARP packets in every one-second interval. If the burst interval is 5 seconds, then the Switch accepts a maximum of 75 ARP packets in every five-second interval. Enter the length (1-15 seconds) of the burst interval.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

25.7.2 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 193 IP Source Guard > ARP Inspection VLAN Configure

The following table describes the labels in this screen.

Table 128 IP Source Guard > ARP Inspection VLAN Configure

LABEL	DESCRIPTION
VLAN	Use this section to specify the VLANs you want to manage in the section below.
Start VID	Enter the lowest VLAN ID you want to manage in the section below.
End VID	Enter the highest VLAN ID you want to manage in the section below.
Apply	Click this to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the * VLAN, the settings are applied to all VLANs.
Enabled	Select 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.

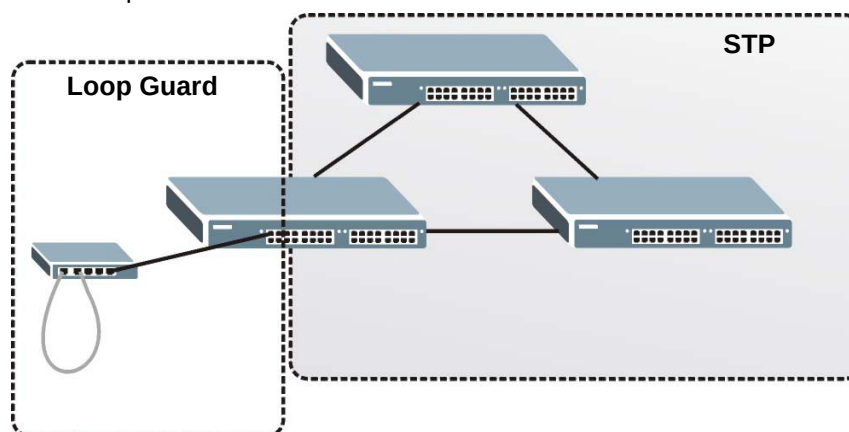
Loop Guard

This chapter shows you how to configure the Switch to guard against loops on the edge of your network.

26.1 Loop Guard Overview

Loop guard allows you to configure the Switch to shut down a port if it detects that packets sent out on that port loop back to the Switch. While you can use Spanning Tree Protocol (STP) to prevent loops in the core of your network. STP cannot prevent loops that occur on the edge of your network.

Figure 194 Loop Guard vs STP

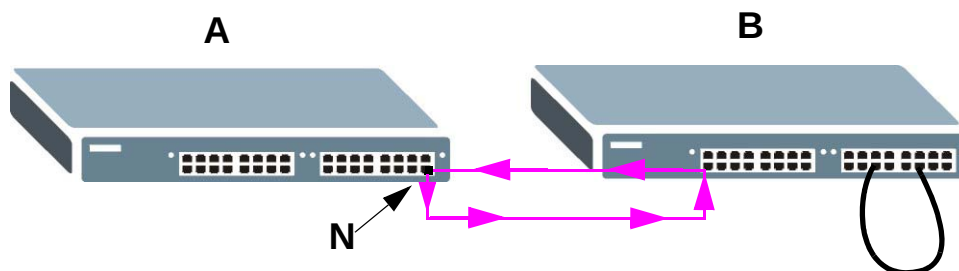


Loop guard is designed to handle loop problems on the edge of your network. This can occur when a port is connected to a Switch that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in loop state sends 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:

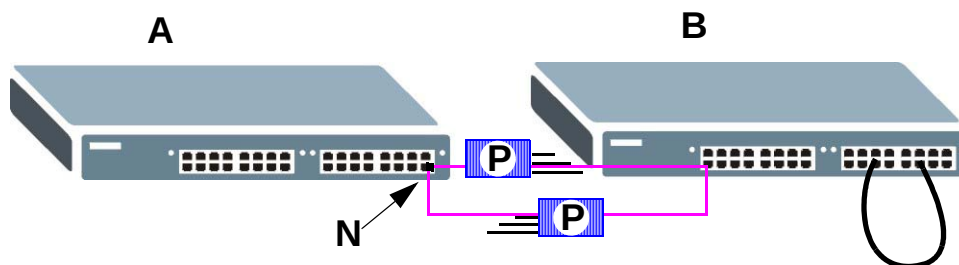
- It will receive broadcast messages sent out from the switch in loop state.
- It will receive its own broadcast messages that it sends out as they loop back. It will then re-broadcast those messages again.

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**.

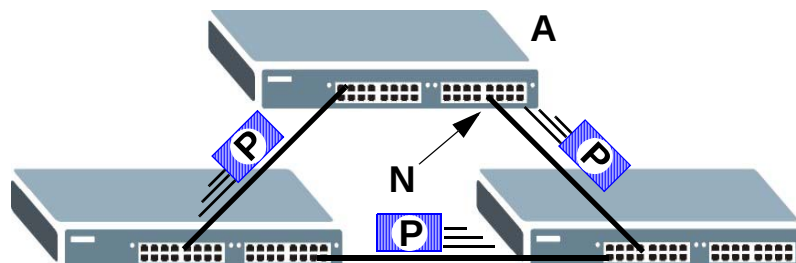
Figure 195 Switch in Loop State

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 196 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 197 Loop Guard - Network Loop

Note: After resolving the loop problem on your network you can re-activate the disabled port via the web configurator (see [Section 6.6 on page 64](#)) or via commands (see the Ethernet Switch CLI Reference Guide).

26.2 Loop Guard Setup

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

Note: The loop guard feature can not be enabled on the ports that have Spanning Tree Protocol (RSTP, MRSTP or MSTP) enabled.

Figure 198 Advanced Application > Loop Guard (Standalone mode)

Loop Guard

Active ☐

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

Apply Cancel

Figure 199 Advanced Application > Loop Guard (Stacking mode)

Loop Guard

Active ☐

SLOT 1 ▼

Port	Active
1/*	☐
1/1	☐
1/2	☐
1/48	☐
1/49	☐
1/50	☐

Apply Cancel

The following table describes the labels in this screen.

Table 129 Advanced Application > Loop Guard

LABEL	DESCRIPTION
Active	Select this option to enable loop guard on the Switch. The Switch generates syslog, internal log messages as well as SNMP traps when it shuts down a port via the loop guard feature.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable the loop guard feature on this port. The Switch sends probe packets from this port to check if the Switch it is connected to is in loop state. If the Switch that this port is connected is in loop state the Switch will shut down this port. Clear this check box to disable the loop guard feature.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

VLAN Mapping

This chapter shows you how to configure VLAN mapping on the Switch.

27.1 VLAN Mapping Overview

With VLAN mapping enabled, the Switch can map the VLAN ID and priority level of packets received from a private network to those used in the service provider's network.

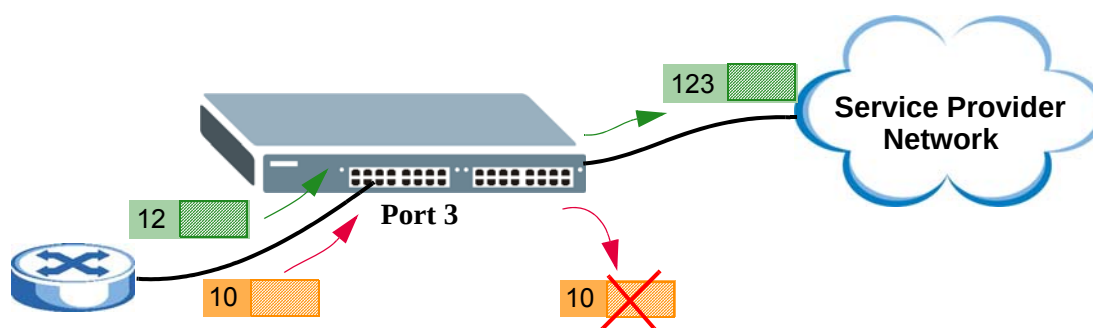
The Switch checks incoming traffic from the switch ports (non-management ports) against the VLAN mapping table first, the MAC learning table and then the VLAN table before forwarding them through the Gigabit uplink port. When VLAN mapping is enabled, the Switch discards the tagged packets that do not match an entry in the VLAN mapping table. If the incoming packets are untagged, the Switch adds a PVID based on the VLAN setting.

Note: You can not enable VLAN mapping and VLAN stacking at the same time.

27.1.1 VLAN Mapping Example

In the following example figure, packets that carry VLAN ID 12 and are received on port 3 match a pre-configured VLAN mapping rule. The Switch translates the VLAN ID from 12 into 123 before forwarding the packets. Any packets carrying a VLAN tag other than 12 (such as 10) and received on port 3 will be dropped.

Figure 200 VLAN mapping example



27.2 Enabling VLAN Mapping

Click **Advanced Application** and then **VLAN Mapping** in the navigation panel to display the screen as shown.

Figure 201 VLAN Mapping (Standalone mode)

VLAN Mapping Configure

Active ☐

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

Apply Cancel

Figure 202 VLAN Mapping (Stacking mode)

VLAN Mapping Configure

Active ☐

SLOT 1 ▼

Port	Active
1/*	☐
1/1	☐
1/2	☐
1/3	☐
1/49	☐
1/50	☐

Apply Cancel

The following table describes the labels in this screen.

Table 130 VLAN Mapping

LABEL	DESCRIPTION
Active	Select this option to enable VLAN mapping on the Switch.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable the VLAN mapping feature on this port. Clear this check box to disable the VLAN mapping feature.

Table 130 VLAN Mapping (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.

27.3 Configuring VLAN Mapping

Click the **VLAN Mapping Configure** link in the **VLAN Mapping** screen to display the screen as shown. Use this screen to enable and edit the VLAN mapping rule(s).

Figure 203 VLAN Mapping Configuration (Standalone mode)

The screenshot shows the 'VLAN Mapping Configure' interface in standalone mode. At the top, there's a blue header bar with an orange circle icon and the text 'VLAN Mapping Configure'. To the right, there's a link 'VLAN Mapping'. Below the header, there's a form with the following fields: 'Active' (checkbox), 'Name' (text input), 'Port' (text input), 'VID' (text input), 'Translated VID' (text input), and 'Priority' (dropdown menu with '0' selected). Below the form, there are 'Add' and 'Cancel' buttons. At the bottom, there's a table with columns: Index, Active, Name, Port, VID, Translated VID, Priority, and Delete. Below the table, there are 'Delete' and 'Cancel' buttons.

Figure 204 VLAN Mapping Configuration (Stacking mode)

The screenshot shows the 'VLAN Mapping Configure' interface in stacking mode. At the top, there's a blue header bar with an orange circle icon and the text 'VLAN Mapping Configure'. To the right, there's a link 'VLAN Mapping'. Below the header, there's a form with the following fields: 'Active' (checkbox), 'Name' (text input), 'Port' (dropdown menu with '1' selected and a text input), 'VID' (text input), 'Translated VID' (text input), and 'Priority' (dropdown menu with '0' selected). Below the form, there are 'Add' and 'Cancel' buttons. At the bottom, there's a table with columns: Index, Active, Name, Port, VID, Translated VID, Priority, and Delete. Below the table, there are 'Delete' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 131 VLAN Mapping Configuration

LABEL	DESCRIPTION
Active	Check this box to activate this rule.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Port	Type a port to be included in this rule. For stacking mode, the first field is the slot ID, the second field is the port number.
VID	Enter a VLAN ID from 1 to 4094. This is the VLAN tag carried in the packets and will be translated into the VID you specified in the Translated VID field.
Translated VID	Enter a VLAN ID (from 1 to 4094) into which the customer VID carried in the packets will be translated.
Priority	Select a priority level (from 0 to 7). This is the priority level that replaces the customer priority level in the tagged packets or adds to the untagged packets.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Index	This is the number of the VLAN mapping entry in the table. Click on an index number to change the settings.
Active	This shows whether this entry is activated or not.
Name	This is the descriptive name for this rule.
Port	This is the port number to which this rule is applied. In stacking mode, the first number represents the slot and the second the port number.
VID	This is the customer VLAN ID in the incoming packets.
Translated VID	This is the VLAN ID that replaces the customer VLAN ID in the tagged packets.
Priority	This is the priority level that replaces the customer priority level in the tagged packets.
Delete	Check the rule(s) that you want to remove in the Delete column and then click the Delete button.
Cancel	Click Cancel to clear the Delete check boxes.

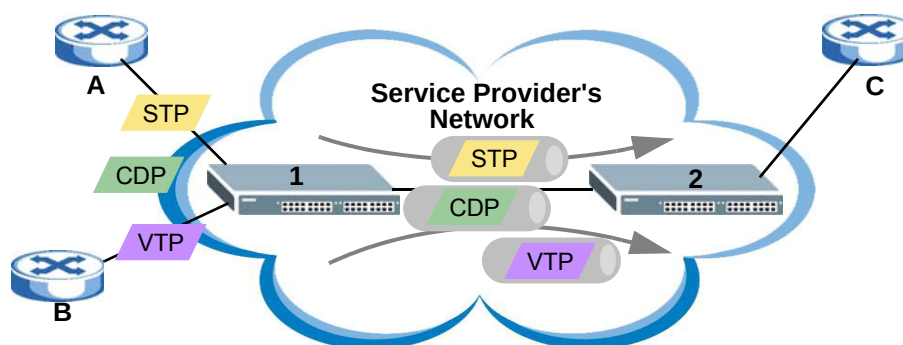
Layer 2 Protocol Tunneling

This chapter shows you how to configure layer-2 protocol tunneling on the Switch.

28.1 Layer 2 Protocol Tunneling Overview

Layer-2 protocol tunneling (L2PT) is used on the service provider's edge devices. L2PT allows edge switches (**1** and **2** in the following figure) to tunnel layer-2 STP (Spanning Tree Protocol), CDP (Cisco Discovery Protocol) and VTP (VLAN Trunking Protocol) packets between customer switches (**A**, **B** and **C** in the following figure) connected through the service provider's network. The edge switch encapsulates layer-2 protocol packets with a specific MAC address before sending them across the service provider's network to other edge switches.

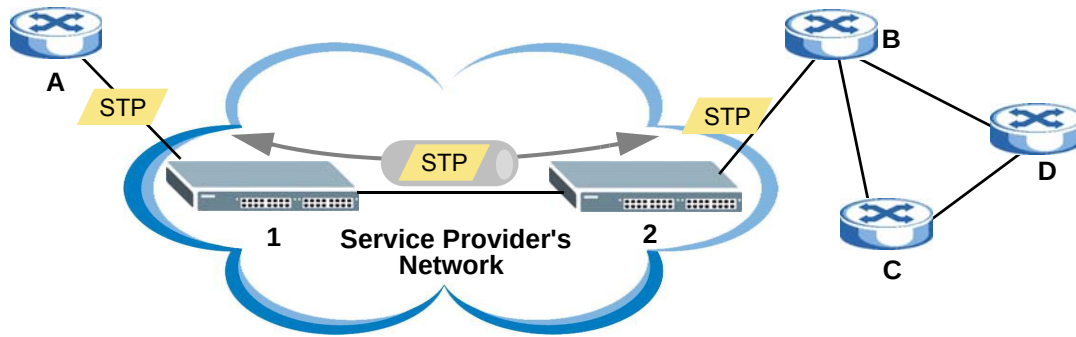
Figure 205 Layer-2 Protocol Tunneling Network Scenario



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 206 L2PT Network Example



28.1.1 Layer-2 Protocol Tunneling Mode

Each port can have two layer-2 protocol tunneling modes, **Access** and **Tunnel**.

- The **Access** port is an ingress port on the service provider's edge device (**1** or **2** in [Figure 206 on page 286](#)) and connected to a customer switch (**A** or **B**). Incoming layer-2 protocol packets received on an access port are encapsulated and forwarded to the tunnel ports.
- The **Tunnel** port is an egress port at the edge of the service provider's network and connected to another service provider's switch. Incoming encapsulated layer-2 protocol packets received on a tunnel port are decapsulated and sent to an access port.

28.2 Configuring Layer 2 Protocol Tunneling

Click **Advanced Application > Layer 2 Protocol Tunneling** in the navigation panel to display the screen as shown.

Figure 207 Advanced Application > Layer 2 Protocol Tunneling (Standalone mode)

Layer 2 Protocol Tunnel

Active ☐

Destination MAC Address 00 : 00 : 00 : 00 : 00 : 00

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 ▼

Apply Cancel

Figure 208 Advanced Application > Layer 2 Protocol Tunneling (Stacking mode)

Layer 2 Protocol Tunnel

Active ☐

Destination MAC Address 00 : 00 : 00 : 00 : 00 : 00

SLOT 1 ▼

Port	CDP	STP	VTP	Point to Point			Mode
				PAGP	LACP	UDLD	
*	☐	☐	☐	☐	☐	☐	Access ▼
1/1	☐	☐	☐	☐	☐	☐	Access ▼
1/2	☐	☐	☐	☐	☐	☐	Access ▼
1/48	☐	☐	☐	☐	☐	☐	Access ▼
1/49	☐	☐	☐	☐	☐	☐	Access ▼
1/50	☐	☐	☐	☐	☐	☐	Access ▼

Apply Cancel

The following table describes the labels in this screen.

Table 132 Advanced Application > Layer 2 Protocol Tunneling

LABEL	DESCRIPTION
Active	Select this to enable layer-2 protocol tunneling on the Switch.
Destination MAC Address	Specify an MAC address with which the Switch uses to encapsulate the layer-2 protocol packets by replacing the destination MAC address in the packets. Note: The MAC address can be either a unicast MAC address or multicast MAC address. If you use a unicast MAC address, make sure the MAC address does not exist in the address table of a switch on the service provider's network. Note: All the edge switches in the service provider's network should be set to use the same MAC address for encapsulation.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
CDP	Select this option to have the Switch tunnel CDP (Cisco Discovery Protocol) packets so that other Cisco devices can be discovered through the service provider's network.
STP	Select this option to have the Switch tunnel STP (Spanning Tree Protocol) packets so that STP can run properly across the service provider's network and spanning trees can be set up based on bridge information from all (local and remote) networks.
VTP	Select this option to have the Switch tunnel VTP (VLAN Trunking Protocol) packets so that all customer switches can use consistent VLAN configuration through the service provider's network.
Point to Point	The Switch supports PAGP (Port Aggregation Protocol), LACP (Link Aggregation Control Protocol) and UDLD (UniDirectional Link Detection) tunneling for a point-to-point topology. Both PAGP and UDLD are Cisco's proprietary data link layer protocols. PAGP is similar to LACP and used to set up a logical aggregation of Ethernet ports automatically. UDLD is to determine the link's physical status and detect a unidirectional link.
PAGP	Select this option to have the Switch send PAGP packets to a peer to automatically negotiate and build a logical port aggregation.
LACP	Select this option to have the Switch send LACP packets to a peer to dynamically creates and manages trunk groups.
UDLD	Select this option to have the Switch send UDLD packets to a peer's port it connected to monitor the physical status of a link.
Mode	Select Access to have the Switch encapsulate the incoming layer-2 protocol packets and forward them to the tunnel port(s). Select Access for ingress ports at the edge of the service provider's network. Note: You can enable L2PT services for STP, LACP, VTP, CDP, UDLD, and PAGP on the access port(s) only. Select Tunnel for egress ports at the edge of the service provider's network. The Switch decapsulates the encapsulated layer-2 protocol packets received on a tunnel port by changing the destination MAC address to the original one, and then forward them to an access port. If the service(s) is not enabled on an access port, the protocol packets are dropped.

Table 132 Advanced Application > Layer 2 Protocol Tunneling (continued)

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

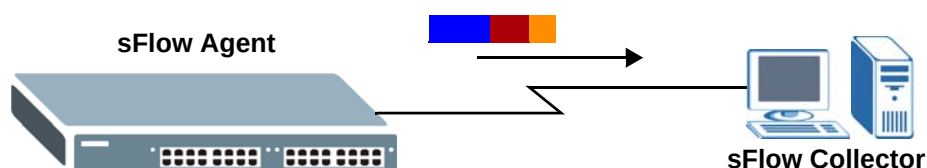
This chapter shows you how to configure sFlow to have the Switch monitor traffic in a network and send information to an sFlow collector for analysis.

29.1 sFlow Overview

sFlow (RFC 3176) is a standard technology for monitoring switched networks. An sFlow agent embedded on a switch or router gets sample data and packet statistics from traffic forwarded through its ports. The sFlow agent then creates sFlow data and sends it to an sFlow collector. The sFlow collector is a server that collects and analyzes sFlow datagram. An sFlow datagram includes packet header, input and output interface, sampling process parameters and forwarding information.

sFlow minimizes impact on CPU load of the Switch as it analyzes sample data only. sFlow can continuously monitor network traffic and create reports for network performance analysis and troubleshooting. For example, you can use it to know which IP address or which type of traffic caused network congestion.

Figure 209 sFlow Application



29.2 sFlow Port Configuration

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

Figure 210 Advanced Application > sFlow (Standalone mode)

sFlowCollector

Active☐

ApplyCancel

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	
8	☐	32768	120	
9	☐	32768	120	
10	☐	32768	120	

ApplyCancel

Figure 211 Advanced Application > sFlow (Stacking mode)

sFlowCollector

Active☐

ApplyCancel

SLOT 1 ▾

Port	Active	Sample-rate	poll-interval	Collector Address
1/*	☐			
1/1	☐	32768	120	
1/2	☐	32768	120	
1/3	☐	32768	120	
1/49	☐	32768	120	
1/50	☐	32768	120	

ApplyCancel

The following table describes the labels in this screen.

Table 133 Advanced Application > sFlow

LABEL	DESCRIPTION
Active	Select this to enable the sFlow agent on the Switch.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this to allow the Switch to monitor traffic on this port and generate and send sFlow datagram to the specified collector.
Sample-rate	Enter a number (N) from 256 to 65535. The Switch captures every one out of N packets for this port and creates sFlow datagram.
poll-interval	Specify a time interval (from 20 to 120 in seconds) the Switch waits before sending the sFlow datagram and packet counters for this port to the collector.
Collector Address	Enter the IP address of the sFlow collector. Note: You must have the sFlow collector already configured in the sFlow > Collector screen. The sFlow collector does not need to be in the same subnet as the Switch, but it must be accessible from the Switch. Note: Configure UDP port 6343 (the default) on a NAT router to allow port forwarding if the collector is behind a NAT router. Configure a firewall rule for UDP port 6343 (the default) to allow incoming traffic if the collector is behind a firewall.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

29.2.1 sFlow Collector Configuration

Click the **Collector** link in the **sFlow** screen to display the screen as shown. You can configure up to four sFlow collectors in this screen. You may want to configure more than one collector if the traffic load to be monitored is more than one collector can manage.

Figure 212 Advanced Application > sFlow > Collector

The screenshot shows the 'sflow Collector' configuration interface. At the top, there's a header with 'sflow' and 'Collector' tabs. Below the header, there are two input fields: 'Collector Address' with the value '0.0.0.0' and 'UDP Port' with the value '6343'. Below these fields are three buttons: 'Add', 'Cancel', and 'Clear'. Below these buttons is a table with four columns: 'Index', 'Collector Address', 'UDP Port', and 'Delete'. The table contains one row with index '1', collector address '1.2.3.4', and UDP port '6343'. The 'Delete' column has a checkbox. Below the table are two buttons: 'Delete' and 'Cancel'.

The following table describes the labels in this screen.

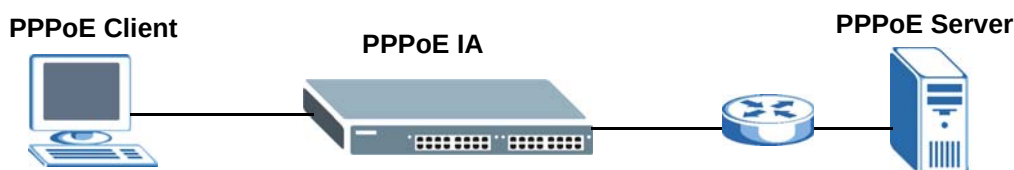
Table 134 Advanced Application > sFlow > Collector

LABEL	DESCRIPTION
Collector Address	Enter the IP address of the sFlow collector.
UDP Port	Enter a UDP port number the Switch uses to send sFlow datagram to the collector. If you change the port here, make sure you change it on the collector, too. The default port is 6343.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Clear	Click Clear to reset the fields to the factory defaults.
Index	This field displays the index number of this entry. Click on an index number to change the settings.
Collector Address	This field displays IP address of the sFlow collector.
UDP Port	This field displays port number the Switch uses to send sFlow datagram to the collector.
Delete	Check the rule(s) that you want to remove in the Delete column and then click the Delete button.
Cancel	Click Cancel to begin configuring this screen afresh.

This chapter describes how the Switch gives a PPPoE termination server additional information that the server can use to identify and authenticate a PPPoE client.

30.1 PPPoE Intermediate Agent Overview

A PPPoE Intermediate Agent (PPPoE IA) is deployed between a PPPoE server and PPPoE clients. It helps the PPPoE server identify and authenticate clients by adding subscriber line specific information to PPPoE discovery packets from clients on a per-port or per-port-per-VLAN basis before forwarding them to the PPPoE server.



30.1.1 PPPoE Intermediate Agent Tag Format

If the PPPoE Intermediate Agent is enabled, the Switch adds a vendor-specific tag to PADI (PPPoE Active Discovery Initialization) and PADR (PPPoE Active Discovery Request) packets from PPPoE clients. This tag is defined in RFC 2516 and has the following format for this feature.

Table 135 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.

30.1.2 Sub-Option Format

There are two types of sub-option: “Agent Circuit ID Sub-option” and “Agent Remote ID Sub-option”. They have the following formats.

Table 136 PPPoE IA Circuit ID Sub-option Format: User-defined String

SubOpt	Length	Value
0x01 (1 byte)	N (1 byte)	String (63 bytes)

Table 137 PPPoE IA Remote ID Sub-option Format

SubOpt	Length	Value
0x02 (1 byte)	N (1 byte)	MAC Address or String (63 bytes)

The 1 in the first field identifies this as an Agent Circuit ID sub-option and 2 identifies this as an Agent Remote ID sub-option. The next field specifies the length of the field. The Switch takes the Circuit ID string you manually configure for a VLAN on a port as the highest priority and the Circuit ID string for a port as the second priority. In addition, the Switch puts the PPPoE client's MAC address into the Agent Remote ID Sub-option if you do not specify any user-defined string.

30.1.2.1 Flexible Circuit ID Syntax with Identifier String and Variables

If you do not configure a Circuit ID string for a VLAN on a specific port or for a specific port, the Switch adds the user-defined identifier string and variables into the Agent Circuit ID Sub-option. The variables can be the slot ID of the PPPoE client, the port number of the PPPoE client and/or the VLAN ID on the PPPoE packet.

The identifier-string, slot ID, port number and VLAN ID are separated from each other by a pound key (#), semi-colon (;), period (.), comma (,), forward slash (/) or space. An Agent Circuit ID Sub-option example is "Switch/07/0123" and indicates the PPPoE packets come from a PPPoE client which is connected to the Switch's port 7 and belong to VLAN 123.

Table 138 PPPoE IA Circuit ID Sub-option Format: Using Identifier String and Variables

SubOpt	Length	Value						
0x01 (1 byte)	N (1 byte)	Identifier String (53 byte)	delimiter (1 byte)	Slot ID (1 byte)	delimiter (1 byte)	Port No (2 byte)	delimiter (1 byte)	VLAN ID (4 bytes)

30.1.2.2 WT-101 Default Circuit ID Syntax

If you do not configure a Circuit ID string for a specific VLAN on a port or for a specific port, and disable the flexible Circuit ID syntax in the **PPPoE > Intermediate Agent** screen, the Switch automatically generates a Circuit ID string according to the default Circuit ID syntax which is defined in the DSL Forum Working Text (WT)-101. The default access node identifier is the host name of the PPPoE intermediate agent and the eth indicates "Ethernet".

Table 139 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)	/	Port No (2 byte)	:	VLAN ID (4 bytes)

30.1.3 Port State

Every port is either a trusted port or an untrusted port for the PPPoE intermediate agent. This setting is independent of the trusted/untrusted setting for DHCP snooping or ARP inspection. You can also specify the agent sub-options (circuit ID and remote ID) that the Switch adds to PADL and PADR packets from PPPoE clients.

Trusted ports are connected to PPPoE servers.

- If a PADO (PPPoE Active Discovery Offer), PADS (PPPoE Active Discovery Session-confirmation), or PADT (PPPoE Active Discovery Terminate) packet is sent from a PPPoE server and received on a trusted port, the Switch forwards it to all other ports.
- If a PADI or PADR packet is sent from a PPPoE client but received on a trusted port, the Switch forwards it to other trusted port(s).

Note: The Switch will drop all PPPoE discovery packets if you enable the PPPoE intermediate agent and there are no trusted ports.

Untrusted ports are connected to subscribers.

- If a PADI, PADR, or PADT packet is sent from a PPPoE client and received on an untrusted port, the Switch adds a vendor-specific tag to the packet and then forwards it to the trusted port(s).
- The Switch discards PADO and PADS packets which are sent from a PPPoE server but received on an untrusted port.

30.2 The PPPoE Screen

Use this screen to configure the PPPoE Intermediate Agent on the Switch.

Click **Advanced Application > PPPoE** in the navigation panel to display the screen as shown. Click **Click Here** to go to the **Intermediate Agent** screen.

Figure 213 Advanced Application > PPPoE Intermediate Agent



30.3 PPPoE Intermediate Agent

Use this screen to configure the Switch to give a PPPoE termination server additional subscriber information that the server can use to identify and authenticate a PPPoE client.

Click **Advanced Application > PPPoE > Intermediate Agent** in the navigation panel to display the screen as shown.

Figure 214 Advanced Application > PPPoE > Intermediate Agent

The following table describes the labels in this screen.

Table 140 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.

Table 140 Advanced Application > PPPoE > Intermediate Agent (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.

30.3.1 PPPoE IA Per-Port

Use this screen to specify whether individual ports are trusted or untrusted ports and have the Switch add extra information to PPPoE discovery packets from PPPoE clients on a per-port basis.

Note: The Switch will drop all PPPoE packets if you enable the PPPoE Intermediate Agent on the Switch and there are no trusted ports.

Click the **Port** link in the **Intermediate Agent** screen to display the screen as shown.

Figure 215 Advanced Application > PPPoE > Intermediate Agent > Port (Standalone mode)

The screenshot displays the 'Port' configuration interface. At the top, there are navigation links: 'Port' (active), 'VLAN', and 'Intermediate Agent'. Below these is a table with the following structure:

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 ▼		

At the bottom of the screen, there are two buttons: 'Apply' and 'Cancel'.

 Port

[VLAN](#)
[Intermediate Agent](#)

SLOT 1 ▾

Port	Server Trusted State	Circuit-id	Remote-id
1/*	Untrusted ▾		
1/1	Untrusted ▾		
1/2	Untrusted ▾		
1/3	Untrusted ▾		
1/49	Untrusted ▾		
1/50	Untrusted ▾		

Apply

Cancel

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Server Trusted State	Select whether this port is a trusted port (Trusted) or an untrusted port (Untrusted). Trusted ports are uplink ports connected to PPPoE servers. - If a PADO (PPPoE Active Discovery Offer), PADS (PPPoE Active Discovery Session-confirmation), or PADT (PPPoE Active Discovery Terminate) packet is sent from a PPPoE server and received on a trusted port, the Switch forwards it to all other ports. - If a PADI or PADR packet is sent from a PPPoE client but received on a trusted port, the Switch forwards it to other trusted port(s). Untrusted ports are downlink ports connected to subscribers. - If a PADI, PADR, or PADT packet is sent from a PPPoE client and received on an untrusted port, the Switch adds a vendor-specific tag to the packet and then forwards it to the trusted port(s). - The Switch discards PADO and PADS packets which are sent from a PPPoE server but received on an untrusted port.
Circuit-id	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Circuit ID sub-option for PPPoE discovery packets received on this port. Spaces are allowed. The Circuit ID you configure for a specific VLAN on a port (in the Advanced Application > PPPoE > Intermediate Agent > Port > VLAN screen) has the highest priority.
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.

Table 141 Advanced Application > PPPoE > Intermediate Agent > Port (continued)

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

30.3.2 PPPoE IA Per-Port Per-VLAN

Use this screen to configure PPPoE IA settings that apply to a specific VLAN on a port.

Click the **VLAN** link in the **Intermediate Agent > Port** screen to display the screen as shown.

Figure 217 Advanced Application > PPPoE > Intermediate Agent > Port > VLAN (Standalone mode)

VLAN [Port](#)

Show Port Port

Show VLAN Start VID End VID

Port: 2

VID	Circuit-id	Remote-id
*		
10		
11		

Figure 218 Advanced Application > PPPoE > Intermediate Agent > Port > VLAN (Stacking mode)

VLAN [Port](#)

Show Port Port /

Show VLAN Start VID End VID

Slot: 0 / Port: 0

VID	Circuit-id	Remote-id
*		

The following table describes the labels in this screen.

Table 142 Advanced Application > PPPoE > Intermediate Agent > Port > VLAN

LABEL	DESCRIPTION
Show Port	Enter a port number to show the PPPoE Intermediate Agent settings for the specified VLAN(s) on the port. For Stacking mode, the first field box is the Slot ID, the second field box is the port.
Show VLAN	Use this section to specify the VLANs you want to configure in the section below.
Start VID	Enter the lowest VLAN ID you want to configure in the section below.
End VID	Enter the highest VLAN ID you want to configure in the section below.
Slot / Port	For Stacking mode, the first field box displays a the Slot ID, the second field box displays the port number.
Apply	Click Apply to display the specified range of VLANs in the section below.
Port	This field displays the port number specified above.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the * VLAN, the settings are applied to all VLANs.
*	Use this row to make the setting the same for all VLANs. Use this row first and then make adjustments on a VLAN-by-VLAN basis. Note: Changes in this row are copied to all the VLANs as soon as you make them.
Circuit-id	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Circuit ID sub-option for this VLAN on the specified port. Spaces are allowed. The Circuit ID you configure here has the highest priority.
Remote-id	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Remote ID sub-option for this VLAN on the specified port. Spaces are allowed. If you do not specify a string here or in the Remote-id field for a specific port, the Switch automatically uses the PPPoE client's MAC address. The Remote ID you configure here has the highest priority.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

30.3.3 PPPoE IA for VLAN

Use this screen to set whether the PPPoE Intermediate Agent is enabled on a VLAN and whether the Switch appends the Circuit ID and/or Remote ID to PPPoE discovery packets from a specific VLAN.

Click the **VLAN** link in the **Intermediate Agent** screen to display the screen as shown.

Figure 219 Advanced Application > PPPoE > Intermediate Agent > VLAN

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 143 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.

31.1 CPU Protection Overview

Switches exchange protocol control packets in a network to get the latest networking information. If a switch receives large numbers of control packets, such as ARP, BPDU or IGMP packets, which are to be processed by the CPU, the CPU may become overloaded and be unable to handle regular tasks properly.

The CPU protection feature allows you to limit the rate of ARP, BPDU and IGMP packets to be delivered to the CPU on a port. This enhances the CPU efficiency and protects against potential DoS attacks or errors from other network(s). You then can choose to drop control packets that exceed the specified rate limit or disable a port on which the packets are received.

31.2 Error-Disable Recovery Overview

Some features, such as loop guard or CPU protection, allow the Switch to shut down a port or discard specific packets on a port when an error is detected on the port. For example, if the Switch detects that packets sent out the port(s) loop back to the Switch, the Switch can shut down the port(s) automatically. After that, you need to enable the port(s) or allow the packets on a port manually via the web configurator or the commands. With error-disable recovery, you can set the disabled port(s) to become active or start receiving the packets again after the time interval you specify.

31.3 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 220 Advanced Application > Errdisable



31.4 Error-Disable Status

Use this screen to view whether the Switch detected that control packets exceeded the rate limit configured for a port and related information. Click the **Click here** link next to **Errdisable Status** in the **Advanced Application > Errdisable** screen to display the screen as shown.

Figure 221 Advanced Application > Errdisable > Errdisable Status (Standalone mode)

Port	Cause	Active	Mode	Rate	Status	Recovery Time Left (secs)	Total Dropped
1	ARP	NO	inactive-port	0	Forwarding	-	-
	BPDU	NO	inactive-port	0	Forwarding	-	-
	IGMP	NO	inactive-port	0	Forwarding	-	-
	Loop Guard	NO	inactive-port	-	Forwarding	-	-
2	ARP	NO	inactive-port	0	Forwarding	-	-
	BPDU	NO	inactive-port	0	Forwarding	-	-
	IGMP	NO	inactive-port	0	Forwarding	-	-
	Loop Guard	NO	inactive-port	-	Forwarding	-	-
3	ARP	NO	inactive-port	0	Forwarding	-	-
	BPDU	NO	inactive-port	0	Forwarding	-	-
	IGMP	NO	inactive-port	0	Forwarding	-	-
	Loop Guard	NO	inactive-port	-	Forwarding	-	-
4	ARP	NO	inactive-port	0	Forwarding	-	-
	BPDU	NO	inactive-port	0	Forwarding	-	-
	IGMP	NO	inactive-port	0	Forwarding	-	-
	Loop Guard	NO	inactive-port	-	Forwarding	-	-
5	ARP	NO	inactive-port	0	Forwarding	-	-
	BPDU	NO	inactive-port	0	Forwarding	-	-
	IGMP	NO	inactive-port	0	Forwarding	-	-
	Loop Guard	NO	inactive-port	-	Forwarding	-	-
6	ARP	NO	inactive-port	0	Forwarding	-	-
	BPDU	NO	inactive-port	0	Forwarding	-	-
	IGMP	NO	inactive-port	0	Forwarding	-	-
	Loop Guard	NO	inactive-port	-	Forwarding	-	-

Figure 222 Advanced Application > Errdisable > Errdisable Status (Stacking mode)

Errdisable Status
Inactive-reason mode reset :

Port List Cause ARP ▼ Reset

Errdisable Status :
SLOT 1 ▼

Port	Cause	Active	Mode	Rate	Status	Recovery Time Left (secs)	Total Dropped
1/1	ARP	NO	inactive-port	0	Forwarding	-	-
	BPDU	NO	inactive-port	0	Forwarding	-	-
	IGMP	NO	inactive-port	0	Forwarding	-	-
	Loop Guard	NO	inactive-port	-	Forwarding	-	-
1/2	ARP	NO	inactive-port	0	Forwarding	-	-
	BPDU	NO	inactive-port	0	Forwarding	-	-
	IGMP	NO	inactive-port	0	Forwarding	-	-
	Loop Guard	NO	inactive-port	-	Forwarding	-	-
1/49	ARP	NO	inactive-port	0	Forwarding	-	-
	BPDU	NO	inactive-port	0	Forwarding	-	-
	IGMP	NO	inactive-port	0	Forwarding	-	-
	Loop Guard	NO	inactive-port	-	Forwarding	-	-
1/50	ARP	NO	inactive-port	0	Forwarding	-	-
	BPDU	NO	inactive-port	0	Forwarding	-	-
	IGMP	NO	inactive-port	0	Forwarding	-	-
	Loop Guard	NO	inactive-port	-	Forwarding	-	-

The following table describes the labels in this screen.

Table 144 Advanced Application > Errdisable > Errdisable Status

LABEL	DESCRIPTION
Inactive-reason mode reset	
Port List	Enter the number of the port(s) (separated by a comma) on which you want to reset inactive-reason status. In stacking mode, the first number represents the slot and the second the port number. Enter 1/1-1/24,2/28 for ports 1 to 24 for the Switch in slot 1 and port 28 for the Switch in slot 2, for example.
Cause	Select the cause of inactive-reason mode you want to reset here.
Reset	Press to reset the specified port(s) to handle ARP, BPDU or IGMP packets instead of ignoring them, if the port(s) is in inactive-reason mode.
Errdisable Status	
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number.
Cause	This refers to the cause of Errdisable Detect or Errdisable Recovery on the Switch.
Active	This field displays whether ARP, BPDU, IGMP and LOOP GUARD on the port is being detected or not.

Table 144 Advanced Application > Errdisable > Errdisable Status (continued)

LABEL	DESCRIPTION
Mode	This field shows the mode of the cause. • inactive-port - The Switch disables the port on which the control packets are received. • inactive-reason - The Switch drops all the specified control packets (such as BPDU) on the port. • rate-limitation - The Switch drops the additional control packets the port(s) has to handle in every one second.
Rate	This field displays how many control packets this port can receive or transmit per second. It can be adjusted in CPU Protection. 0 means no rate limit.
Status	This field displays the errdisable status • Forwarding: The Switch is forwarding packets. Rate-limitation mode is always in Forwarding status. • Err-disable: The Switch disables the port on which the control packets are received (inactive-port) or drops specified control packets on the port (inactive-reason)
Recovery Time	This field displays the time (seconds) left before the port(s) becomes active of Errdisable Recovery.
Total Dropped	This field displays the total packet number dropped by this port where the packet rate exceeds the rate of mode rate-limitation.

31.5 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 223 Advanced Application > Errdisable > CPU protection (Standalone mode)

Port	Rate Limit (pkt/s)
*	
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0

Figure 224 Advanced Application > Errdisable > CPU protection (Stacking mode)

Port	Rate Limit (pkt/s)
1/*	
1/1	0
1/2	0
1/49	0
1/50	0

The following table describes the labels in this screen.

Table 145 Advanced Application > Errdisable > CPU protection

LABEL	DESCRIPTION
Reason	Select the type of control packet you want to configure here.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number. * means all ports (on the same Switch).
1/ *	Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Note: Changes in this row are copied to all the ports as soon as you make them.

Table 145 Advanced Application > Errdisable > CPU protection (continued)

LABEL	DESCRIPTION
Rate Limit (pkt/s)	Enter a number from 0 to 256 to specify how many control packets this port can receive or transmit per second. 0 means no rate limit. You can configure the action that the Switch takes when the limit is exceeded. See Section 31.6 on page 308 for detailed information.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

31.6 Error-Disable Detect Configuration

Use this screen to have the Switch detect whether the control packets exceed the rate limit configured for a port and configure the action to take once the limit is exceeded. Click the **Click Here** link next to **Errdisable Detect** link in the **Advanced Application > Errdisable** screen to display the screen as shown.

Figure 225 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 146 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.

Table 146 Advanced Application > Errdisable > Errdisable Detect (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.

31.7 Error-Disable Recovery Configuration

Use this screen to configure the Switch to automatically undo an action after the error is gone. Click the **Click Here** link next to **Errdisable Recovery** in the **Advanced Application > Errdisable** screen to display the screen as shown.

Figure 226 Advanced Application > Errdisable > Errdisable Recovery

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

The following table describes the labels in this screen.

Table 147 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.

MAC Pinning

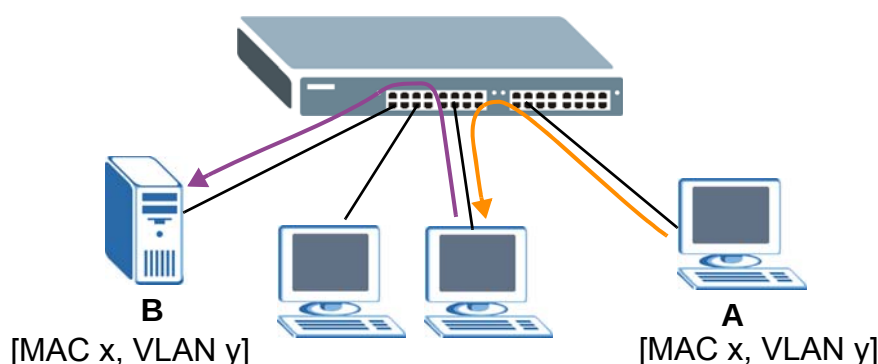
This chapter shows you how to configure MAC pinning on the Switch.

32.1 MAC Pinning Overview

When the Switch obtains a connected device's MAC address, it adds an entry in the MAC address forwarding table and uses the table to determine how to forward frames. In addition to the source MAC address of a received frame, the Switch also learns the VLAN to which the device belongs and the port on which the frame is received. If the Switch learns the same MAC address and same VLAN ID on another port, it updates the MAC address table immediately.

MAC pinning allows you to set a port or multiple ports to have priority over other ports in MAC address learning. That means when a MAC address (and VLAN ID) is learned on a MAC-pinning-enabled port, the MAC address will not be learned on any other port until the aging time for the dynamically learned MAC address in the table expires.

This helps enhance security. For example, when an attacker (**A**) sends packets to all connected clients by spoofing the source MAC address of a server (**B**) connected to one of the Switch's ports, on which MAC pinning is enabled, the responses from clients will still be forwarded to the server according to the Switch's MAC forwarding table.



32.2 MAC Pinning Configuration

Use this screen to enable MAC pinning on the Switch and on specific ports. Click **Advanced Application > MAC Pinning** in the navigation panel to open the following screen.

Figure 227 Advanced Application > MAC Pinning (Standalone mode)

MAC Pinning

Active ☐

Port	Active
*	☐
1	☐
2	☐
3	☐
4	☐
5	☐
6	☐
7	☐
8	☐
9	☐
10	☐
11	☐
12	☐
13	☐
14	☐

Apply Cancel

Figure 228 Advanced Application > MAC Pinning (Stacking mode)

MAC Pinning

Active ☐

SLOT 1 ▼

Port	Active
1/*	☐
1/1	☐
1/2	☐
1/48	☐
1/49	☐
1/50	☐

Apply Cancel

The following table describes the labels in this screen.

Table 148 Advanced Application > MAC Pinning

LABEL	DESCRIPTION
Active	Select this option to turn on the MAC pinning function on the Switch.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first field is the slot ID and the second field is the port number. * means all ports (on the same Switch).

Table 148 Advanced Application > MAC Pinning (continued)

LABEL	DESCRIPTION
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable MAC pinning on this port. The port then has priority over other ports in MAC address learning. Clear this check box to disable MAC pinning.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

Private VLAN

33.1 Private VLAN Overview

Use private VLAN if you want you to block traffic between ports in the same VLAN. **Community** and **Isolated** VLANs are secondary private VLANs that must be associated with a **Primary** private VLAN.

- **Primary:** Ports in a **Primary** VLAN are promiscuous and they can communicate with all promiscuous ports in the same primary VLAN, and all ports in associated community and isolated VLANs. They cannot communicate with ports in different primary VLANs.
- **Community:** Ports in a **Community** VLAN can communicate with promiscuous ports in an associated **Primary** VLAN and other community ports in the same **Community** VLAN. They cannot communicate with ports in **Isolated** VLANs, non-associated **Primary** VLAN promiscuous ports nor community ports in different **Community** VLANs.
- **Isolated:** Ports in an **Isolated** VLAN can communicate with promiscuous ports in an associated **Primary** VLAN only. They cannot communicate with other isolated ports in the same **Isolated** VLAN, non-associated **Primary** VLAN promiscuous ports nor any community ports.

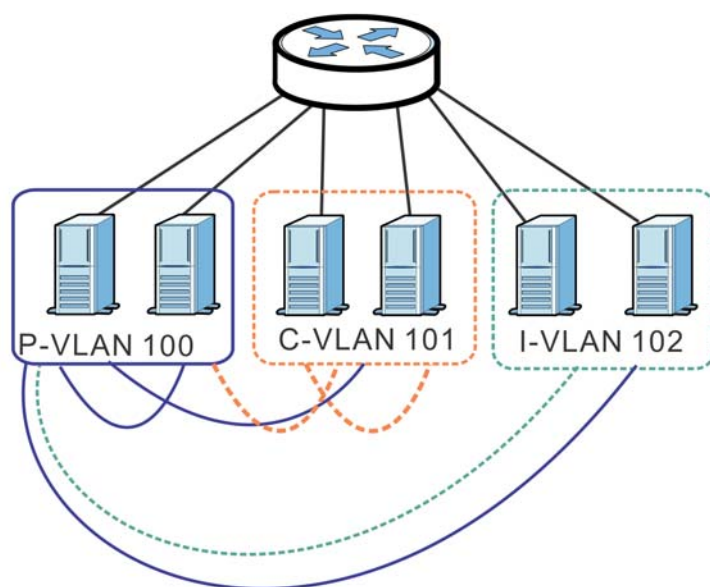


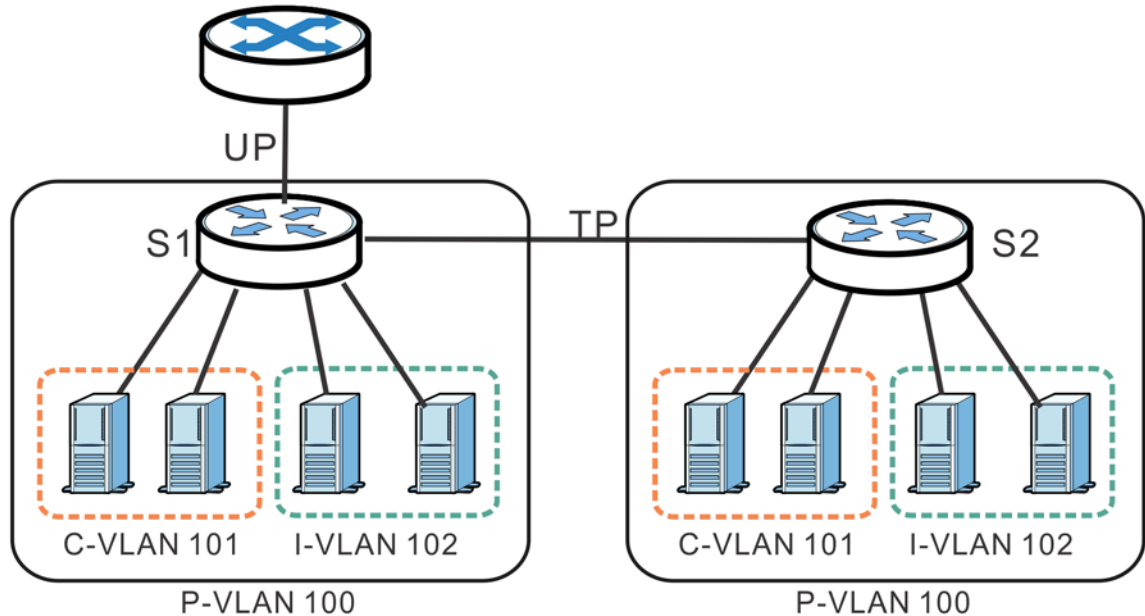
Table 149 PVLAN Graphic Key

LABEL	DESCRIPTION
P-VLAN 100	Primary private VLAN

Table 149 PVLAN Graphic Key (continued)

LABEL	DESCRIPTION
C-VLAN 101	Community private VLAN
I-VLAN 102	Isolated private VLAN

Tagged Private VLANs can span switches but trunking ports must be VLAN-trunking ports - see **Advanced > VLAN > VLAN Port Setting**.

**Table 150** Spanning PVLAN Graphic Key

LABEL	DESCRIPTION
UP	Uplink promiscuous port
TP	VLAN-trunking ports
S1, S2	Switch 1, Switch 2
P-VLAN 100	Primary private VLAN with VLAN ID tag of 100
C-VLAN 101	Community private VLAN with VLAN ID tag of 101
I-VLAN 102	Isolated private VLAN with VLAN ID tag of 102

This is the communication process if primary VLAN **P-VLAN 100** is associated with community VLAN **C-VLAN 101** and isolated VLAN **I-VLAN 102**.

- Promiscuous ports in **P-VLAN 100** can communicate with all ports in **P-VLAN 100** including community ports in **C-VLAN 101** and isolated ports in **I-VLAN 102**.
- Community ports in **C-VLAN 101** can communicate with promiscuous ports in **P-VLAN 100** and other community ports in **C-VLAN 101**. They cannot communicate with isolated ports in **I-VLAN 102**.
- Isolated ports can communicate with promiscuous ports in **P-VLAN 100**. They cannot communicate with other isolated ports in **I-VLAN 102** nor community ports in **C-VLAN 101**.

Note: **Isolation** in **VLAN > VLAN Port Setting** (see [Section 7.6.2 on page 101](#)) has a higher priority than private VLAN settings, so promiscuous ports with **Isolation** in **VLAN > VLAN Port Setting** enabled will not be able to communicate with each other.

33.1.1 Configuration

You must go to the **Static VLAN** screen first (see [Section 7.6 on page 99](#)) to create VLAN IDs for **Primary**, **Isolated** or **Community** VLANs.

Click **Advanced Application > Private VLAN** to display the following screen.

Figure 229 Advanced Application > Private VLAN (Standalone mode)

Port	Mode	Associated VLAN	Tagged
*	Normal		☐
1	Normal	0	☐
2	Normal	0	☐
3	Normal	0	☐
4	Normal	0	☐
5	Normal	0	☐
6	Normal	0	☐
7	Normal	0	☐
8	Normal	0	☐
9	Normal	0	☐
10	Normal	0	☐
11	Normal	0	☐
12	Normal	0	☐
13	Normal	0	☐
14	Normal	0	☐

Apply Cancel

Figure 230 Advanced Application > Private VLAN (Stacking mode)

Port	Mode	Associated VLAN	Tagged
1/*	Normal		☐
1/1	Normal	0	☐
1/2	Normal	0	☐
1/48	Normal	0	☐
1/49	Normal	0	☐
1/50	Normal	0	☐

Apply Cancel

The following table describes the labels in this screen.

Table 151 Advanced Application > Private VLAN

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number. * means all ports (on the same Switch).
Mode	This is the type of VLAN mapped to this port. Normal: These are ports in a static VLAN. This is not a private VLAN. Promiscuous: Ports in a Primary VLAN are Promiscuous. They can communicate with all ports in the Primary VLAN and associated Community and Isolated VLANs. They cannot communicate with Promiscuous ports in different primary VLANs. Community: Ports in a Community VLAN can communicate with Promiscuous ports in an associated Primary VLAN and other community ports in the same Community VLAN. They cannot communicate with ports in an Isolated VLAN, non-associated Primary VLAN Promiscuous ports nor Community ports in different Community VLANs. Isolated: Ports in an Isolated VLAN can communicate with Promiscuous ports in an associated Primary VLAN only. They cannot communicate with other Isolated ports in the same Isolated VLAN, non-associated Primary VLAN Promiscuous ports nor any Community ports.
Associated VLAN	Enter the VLAN ID of a previously created VLAN here. Note: The VLAN ID and Mode selected here must be the same as the VLAN ID and VLAN Type created in Advanced Application > VLAN > Static VLAN.
Tagged	A VLAN ID tag identifies VLAN membership of a frame across switches. Select this if the VLAN includes ports on multiple switches. The Switch forwards tagged frames through this port; it adds the PVID to untagged frames before sending them out. Clear this if the VLAN includes ports on this Switch only. The Switch forwards untagged frames through this port; it removes the VLAN ID from tagged frames before sending them out.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

Green Ethernet

This chapter shows you how to configure the Switch to reduce the power consumed by switch ports.

34.1 Green Ethernet Overview

Green Ethernet reduces switch port power consumption in the following ways.

- IEEE 802.3az Energy Efficient Ethernet (EEE)

If EEE is enabled, both sides of a link support EEE and there is no traffic, the port enters Low Power Idle (LPI) mode. LPI mode turns off some functions of the physical layer (becomes quiet) to save power. Periodically the port transmits a REFRESH signal to allow the link partner to keep the link alive. When there is traffic to be sent, a WAKE signal is sent to the link partner to return the link to active mode.

- Auto Power Down

Auto Power Down turns off almost all functions of the port's physical layer functions when the link is down, so the port only uses power to check for a link up pulse from the link partner. After the link up pulse is detected, the port wakes up from **Auto Power Down** and operates normally.

- Short Reach

Traditional Ethernet transmits all data with enough power to reach the maximum cable length. Shorter cables lose less power, so **Short Reach** saves power by adjusting the transmit power of each port according to the length of cable attached to that port.

34.2 Configuring Green Ethernet

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

Note: EEE, Auto Power Down and Short Reach are not supported on an uplink port.

Figure 231 Advanced Application > Green Ethernet (Standalone mode)

Green Ethernet

EEE ☒

Auto Power Down ☒

Short Reach ☒

Port	EEE	Auto Power Down	Short Reach
*	☐	☐	☐
1	☐	☐	☐
2	☐	☐	☐
3	☐	☐	☐
4	☐	☐	☐
5	☐	☐	☐
6	☐	☐	☐
7	☐	☐	☐
8	☐	☐	☐
9	☐	☐	☐
10	☐	☐	☐
11	☐	☐	☐
12	☐	☐	☐
52	☐	☐	☐

Apply Cancel

Figure 232 Advanced Application > Green Ethernet (Stacking mode)

Green Ethernet

EEE ☐

Auto Power Down ☐

Short Reach ☐

SLOT 1 ▼

Port	EEE	Auto Power Down	Short Reach
1/*	☐	☐	☐
1/1	☐	☐	☐
1/2	☐	☐	☐
1/49	☐	☐	☐
1/50	☐	☐	☐

Apply Cancel

The following table describes the labels in this screen.

Table 152 Advanced Application > Green Ethernet

LABEL	DESCRIPTION
EEE	Select this to activate Energy Efficient Ethernet globally.
Auto Power Down	Select this to activate Auto Power Down globally.
Short Reach	Select this to activate Short Reach globally.

Table 152 Advanced Application > Green Ethernet

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port (Standalone or stacking mode)	This field displays the port number. In stacking mode, the first box field is the slot ID and the second field is the port number. * means all ports (on the same Switch).
1/ *	Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Note: Changes in this row are copied to all the ports as soon as you make them.
EEE	Select this to activate Energy Efficient Ethernet on this port.
Auto Power Down	Select this to activate Auto Power Down on this port.
Short Reach	Select this to activate Short Reach on this port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

Link Layer Discovery Protocol (LLDP)

35.1 LLDP Overview

The LLDP (Link Layer Discovery Protocol) is a layer 2 protocol. It allows a network device to advertise its identity and capabilities on the local network. It also allows the device to maintain and store information from adjacent devices which are directly connected to the network device. This helps an administrator discover network changes and perform necessary network reconfiguration and management. The device information is encapsulated in the LLDPDUs (LLDP data units) in the form of TLV (Type, Length, Value). Device information carried in the received LLDPDUs is stored in the standard MIB.

The Switch supports these basic management TLVs.

- End of LLDPDU (mandatory)
- Chassis ID (mandatory)
- Port ID (mandatory)
- Time to Live (mandatory)
- Port Description (optional)
- System Name (optional)
- System Description (optional)
- System Capabilities (optional)
- Management Address (optional)

The Switch also supports the IEEE 802.1 and IEEE 802.3 organizationally-specific TLVs.

IEEE 802.1 specific TLVs:

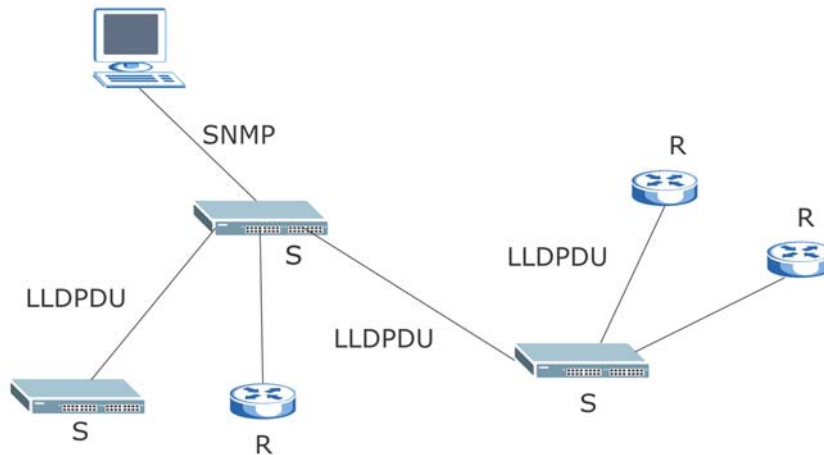
- Port VLAN ID TLV (optional)
- Port and Protocol VLAN ID TLV (optional)

IEEE 802.3 specific TLVs:

- MAC/PHY Configuration/Status TLV (optional)
- Power via MDI TLV (optional, For PoE models only)
- Link Aggregation TLV (optional)
- Maximum Frame Size TLV (optional)

The optional TLVs are inserted between the Time To Live TLV and the End of LLDPDU TLV.

The next figure demonstrates that the network devices Switches and Routers (S and R) transmit and receive device information via LLDPDU and the network manager can query the information using Simple Network Management Protocol (SNMP).

Figure 233 LLDP Overview

35.2 LLDP-MED Overview

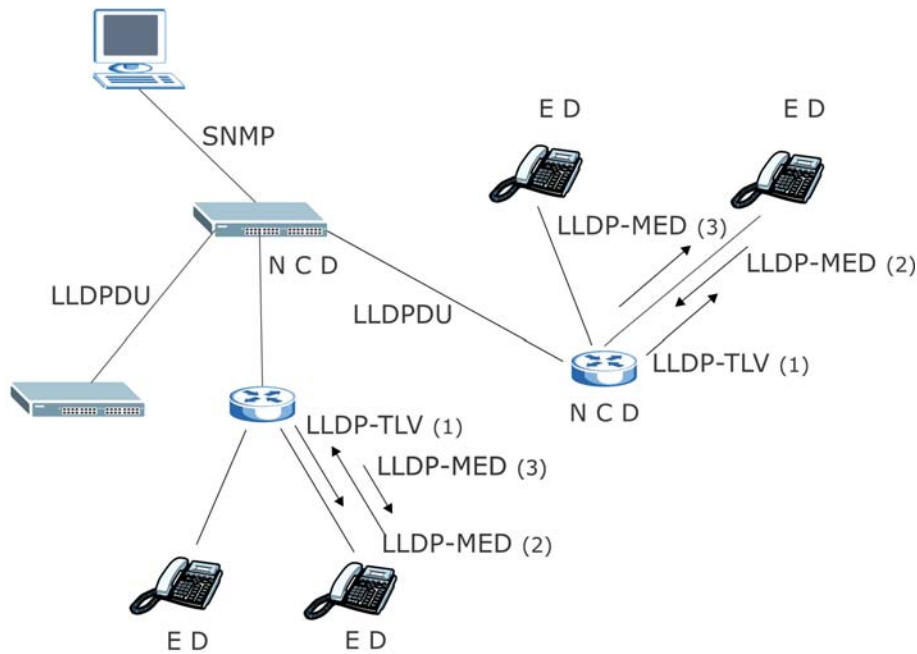
LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) is an extension to the standard LLDP developed by the Telecommunications Industry Association (TIA) TR-41.4 subcommittee which defines the enhanced discovery capabilities, such as VoIP applications, to enable network administrators manage their network topology application more efficiently. Unlike the traditional LLDP, which has some limitations when handling multiple application devices, the LLDP-MED offers display of accurate physical topology, interoperability of devices, and easy trouble shooting for misconfigured IP addresses. There are three classes of endpoint devices that the LLDP-MED supports:

Class I: IP Communications Controllers or other communication related servers

Class II: Voice Gateways, Conference Bridges or Media Servers

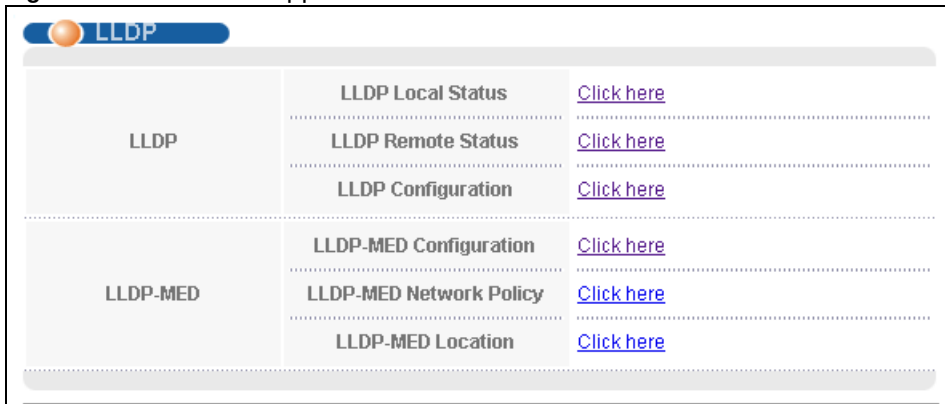
Class III: IP-Phones, PC-based Softphones, End user Communication Appliances supporting IP Media

The following figure shows that with the LLDP-MED, network connectivity devices (NCD) like Switches and Routers will transmit LLDP TLV to endpoint device (ED) like IP Phone first (1), to get its device type and capabilities information, then it will receive that information in LLDP-MED TLV back from endpoint devices (2), after that the network connectivity devices will transmit LLDP-MED TLV (3) to provision the endpoint device to such that the endpoint device's network policy and location identification information is updated. Since LLDPDU updates status and configuration information periodically, network managers may check the result of provision via remote status. The remote status is updated by receiving LLDP-MED TLVs from endpoint devices.

Figure 234 LLDP-MED Overview

35.3 LLDP Screens

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

Figure 235 Advanced Application > LLDP

The following table describes the labels in this screen.

Table 153 Advanced Application > LLDP

LABEL	DESCRIPTION
LLDP	
LLDP Local Status	Click here to show a screen with the Switch's LLDP information.
LLDP Remote Status	Click here to show a screen with LLDP information from the neighboring devices.

Table 153 Advanced Application > LLDP (continued)

LABEL	DESCRIPTION
LLDP Configuration	Click here to show a screen to configure LLDP parameters.
LLDP-MED	
LLDP-MED Configuration	Click here to show a screen to configure LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) parameters.
LLDP-MED Network Policy	Click here to show a screen to configure LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) network policy parameters.
LLDP-MED Location	Click here to show a screen to configure LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) location parameters.

35.4 LLDP Local Status

This screen displays a summary of LLDP status on this Switch. Click **Advanced Application > LLDP > LLDP Local Status** to display the screen as shown next.

Figure 236 Advanced Application > LLDP > LLDP Local Status (Standalone mode)


LLDP Local Status

LLDP

LLDP System Information

Basic TLV

Chassis ID TLV	Chassis ID Subtype	mac-address
	Chassis ID	00:19:cb:00:00:02
System Name TLV	System Name	XGS3700
System Description TLV	System Description	V4.10(AAGF.5)b1 06/05/2014
System Capabilities TLV	System Capabilities Supported	Bridge
	System Capabilities Enabled	Bridge
Management Address TLV	Management Address Subtype	ipv4 / all-802
	Interface Number Subtype	unknown
	Interface Number	0
	Object Identifier	0

LLDP Port Information

Local Port	Port ID Subtype	Port ID	Port Description
1	local-assigned	1	
2	local-assigned	2	
3	local-assigned	3	
4	local-assigned	4	
5	local-assigned	5	
6	local-assigned	6	
7	local-assigned	7	
8	local-assigned	8	

Figure 237 Advanced Application > LLDP > LLDP Local Status (Stacking mode)

LLDP Local Status [LLDP](#)

LLDP System Information

Basic TLV		
Chassis ID TLV	Chassis ID Subtype	mac-address
	Chassis ID	00:19:cb:00:00:02
System Name TLV	System Name	XGS3700
System Description TLV	System Description	V4.20(AAGF.0)b4 08/12/2014
System Capabilities TLV	System Capabilities Supported	Bridge
	System Capabilities Enabled	Bridge
Management Address TLV	Management Address Subtype	ipv4 / all-802
	Interface Number Subtype	unknown
	Interface Number	0
	Object Identifier	0

LLDP Port Information

SLOT 1 ▼

Local Port	Port ID Subtype	Port ID	Port Description
1/1	local-assigned	1/1	
1/2	local-assigned	1/2	
1/3	local-assigned	1/3	
1/49	local-assigned	1/49	
1/50	local-assigned	1/50	

The following table describes the labels in this screen.

Table 154 Advanced Application > LLDP > LLDP Local Status

LABEL	DESCRIPTION
Basic TLV	
Chassis ID TLV	This displays the chassis ID of the local Switch, that is the Switch you're configuring. The chassis ID is identified by the chassis ID subtype. Chassis ID Subtype - this displays how the chassis of the remote Switch is identified. Chassis ID - This displays the chassis ID of the local Switch. The chassis ID is identified by the chassis ID subtype.
System Name TLV	This shows the Host Name of the Switch.
System Description TLV	This shows the System Description which is the firmware version of the Switch.
System Capabilities TLV	This shows the System Capabilities enabled and supported on the local Switch. - System Capabilities Supported - Bridge - System Capabilities Enabled - Bridge

Table 154 Advanced Application > LLDP > LLDP Local Status

LABEL	DESCRIPTION
Management Address TLV	The Management Address TLV identifies an address associated with the local LLDP agent that may be used to reach higher layer entities to assist discovery by network management. The TLV may also include the system interface number and an object identifier (OID) that are associated with this management address. This field displays the Management Address settings on the specified port(s). • Management Address Subtype - ipv4 / all-802 • Interface Number Subtype - unknown • Interface Number - 0 (not supported) • Object Number - 0 (not supported)
LLDP Port Information	This displays the local port information.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Local Port	This displays the local port number which receives the LLDPDU from the remote device. Click a port number to view the detailed LLDP status on this port at LLDP Local Port Status Detail screen. For Stacking mode, the first field box is the Slot ID, the second field box is the port.
Port ID Subtype	This indicates how the port ID field is identified.
Port ID	This is an alpha-numeric string that contains the specific identifier for the port from which this LLDPDU was transmitted.
Port Description	This shows the port description that the Switch will advertise from this port.

35.4.1 LLDP Local Port Status Detail

This screen displays detailed LLDP status for each port on this Switch. Click **Advanced Application > LLDP > LLDP Local Status** and then click a port number, for example 1 (Port) in the **Local Port** column to display the screen as shown next.

Figure 238 Advanced Application > LLDP > LLDP Local Status > LLDP Local Port Status Detail (Basic TLV)

LLDP Local Port Status Detail		LLDP Local Status
Local Port: 1		
Basic TLV		
Port ID TLV	Port ID Subtype	local-assigned
	Port ID	1
Port Description TLV	Port Description	12345678901234567890123456789012345678901234567890abcd
Dot1 TLV		
Port VLAN ID TLV	Port VLAN ID	100
Port-Protocol VLAN ID TLV	Port-Protocol VLAN ID	10
Dot3 TLV		
MAC PHY Configuration & Status TLV	AN Supported	Yes
	AN Enabled	Yes
	AN Advertised Capability	10baseT 10baseTFD 100baseTX 100baseTXFD 1000baseTFD
	Oper MAU Type	30
Link Aggregation TLV	Aggregation Capability	Yes
	Aggregation Status	No
	Aggregated Port ID	0
Max Frame Size TLV	Max Frame Size	1518

Figure 239 Advanced Application > LLDP > LLDP Local Status > LLDP Local Port Status Detail (MED TLV)

MED TLV		
Capabilities TLV	Network Policy	Yes
	Location	Yes
	Extend Power via MDI PSE	No
	Extend Power via MDI PD	No
	Inventory Management	No
Device Type TLV	Device Type	Network Connectivity
Network Policy TLV	Voice	VLAN ID 10, tagged, L2-priority 7, DSCP 63
	Voice-Signaling	VLAN ID 100, tagged, L2-priority 2, DSCP 10
	Guest-Voice	VLAN ID 20, tagged, L2-priority 3, DSCP 12
	Guest-Voice-Signaling	VLAN ID 0, untagged, L2-priority 0, DSCP 0
	Softphone-Voice	VLAN ID 200, tagged, L2-priority 1, DSCP 1
	Video-Conferencing	VLAN ID 0, untagged, L2-priority 0, DSCP 0
	Streaming-Video	VLAN ID 300, tagged, L2-priority 4, DSCP 20
	Video-Signaling	VLAN ID 400, tagged, L2-priority 6, DSCP 55
Location Identification TLV	Coordinate-base LCI	latitude north 24.0 longitude east 120.0 altitude meter 13.0 datum WGS84
	Civic LCI	country TW city HSINCHU building ZYXEL
	ELIN	1234567890

The following table describes the labels in this screen.

Table 155 Advanced Application > LLDP > LLDP Local Status > LLDP Local Port Status Detail

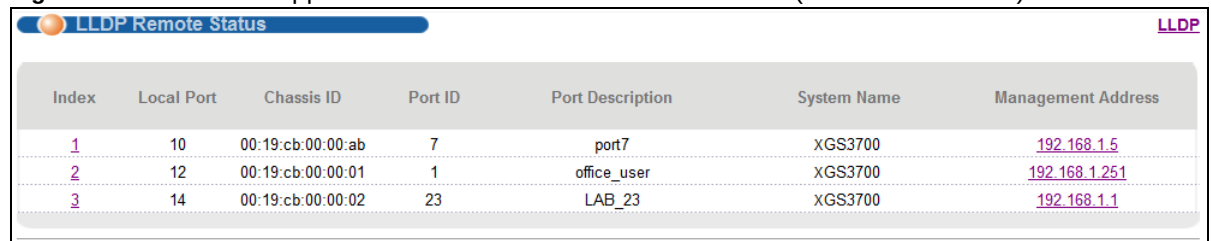
LABEL	DESCRIPTION
Basic TLV	These are the Basic TLV flags
Port ID TLV	The port ID TLV identifies the specific port that transmitted the LLDP frame. - Port ID Subtype: This shows how the port is identified. - Port ID: This is the ID of the port. In stacking mode, the first number represents the slot and the second the port number.
Port Description TLV	This displays the local port description.
Dot1 TLV	
Port VLAN ID TLV	This displays the VLAN ID sent by the IEEE 802.1 Port VLAN ID TLV.
Port-Protocol VLAN ID TLV	This displays the IEEE 802.1 Port Protocol VLAN ID TLVs, which indicates whether the VLAN is enabled and supported.
Dot3 TLV	
MAC PHY Configuration & Status TLV	The MAC/PHY Configuration/Status TLV advertises the bit-rate and duplex capability of the sending 802.3 node. It also advertises the current duplex and bit-rating of the sending node. Lastly, it advertises whether these setting were the result of auto-negotiation during link initiation or manual override. - AN Supported - Displays if the port supports or does not support auto-negotiation. - AN Enabled - The current auto-negotiation status of the port. - AN Advertised Capability - The auto-negotiation capabilities of the port. - Oper MAU Type - The current Medium Attachment Unit (MAU) type of the port.
Link Aggregation TLV	The Link Aggregation TLV indicates whether the link is capable of being aggregated, whether the link is currently in an aggregation, and if in an aggregation, the port identification of the aggregation. - Aggregation Capability — The current aggregation capability of the port. - Aggregation Status — The current aggregation status of the port. - Aggregation Port ID — The aggregation ID of the current port.
Max Frame Size TLV	This displays the maximum supported frame size in octets.
MED TLV	LLDP Media Endpoint Discovery (MED) is an extension of LLDP that provides additional capabilities to support media endpoint devices. MED enables advertisement and discovery of network policies, device location discovery to allow creation of location databases, and information for troubleshooting.
Capabilities TLV	This field displays which LLDP-MED TLV are capable to transmit on the Switch. - Network Policy - Location - Extend Power via MDI PSE - Extend Power via MDI PD - Inventory Management
Device Type TLV	This is the LLDP-MED device class. The ZyXEL Switch device type is: Network Connectivity

Table 155 Advanced Application > LLDP > LLDP Local Status > LLDP Local Port Status Detail

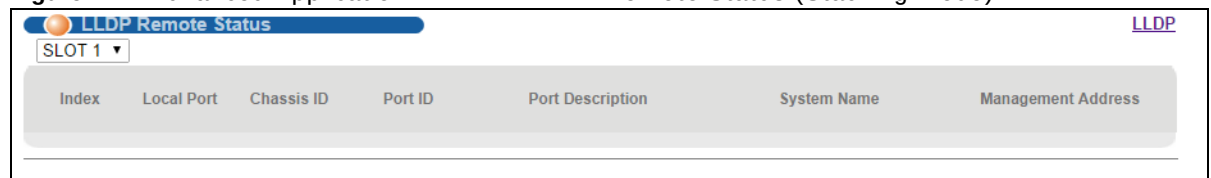
LABEL	DESCRIPTION
Network Policy TLV	This displays a network policy for the specified application. - Voice - Voice-Signaling - Guest-Voice - Guest-Voice-Signaling - Softphone-Voice - Video-Conferencing - Streaming-Video - Video-Signaling
Location Identification TLV	This shows the location information of a caller by its ELIN (Emergency Location Identifier Number) or the IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI). - Coordinate-base LCI - latitude, longitude and altitude coordinates of the location Configuration Information (LCI) - Civic LCI - IETF Geopriv Civic Address based Location Configuration Information - ELIN - (Emergency Location Identifier Number)

35.5 LLDP Remote Status

This screen displays a summary of LLDP status for each LLDP connection to a neighboring Switch. Click **Advanced Application > LLDP > LLDP Remote Status** to display the screen as shown next.

Figure 240 Advanced Application > LLDP > LLDP Remote Status (Standalone mode)


Index	Local Port	Chassis ID	Port ID	Port Description	System Name	Management Address
1	10	00:19:cb:00:00:ab	7	port7	XGS3700	192.168.1.5
2	12	00:19:cb:00:00:01	1	office_user	XGS3700	192.168.1.251
3	14	00:19:cb:00:00:02	23	LAB_23	XGS3700	192.168.1.1

Figure 241 Advanced Application > LLDP > LLDP Remote Status (Stacking mode)


Index	Local Port	Chassis ID	Port ID	Port Description	System Name	Management Address

The following table describes the labels in this screen.

Table 156 Advanced Application > LLDP > LLDP Remote Status

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Index	The index number shows the number of remote devices that are connected to the Switch. Click on an index number to view the detailed LLDP status for this remote device at LLDP Remote Port Status Detail screen.

Table 156 Advanced Application > LLDP > LLDP Remote Status

LABEL	DESCRIPTION
Local Port	This is the port number of local Switch that received LLDPDU from the remote device. In stacking mode, the first number represents the slot and the second the port number.
Chassis ID	This displays the chassis ID of the remote device associated with the transmitting LLDP agent. The chassis ID is identified by the chassis ID subtype. For example, the MAC address of the remote device.
Port ID	This is an alpha-numeric string that contains the specific identifier for the port from which this LLDPDU was transmitted. The port ID is identified by the port ID subtype.
Port Description	This displays a description for the port from which this LLDPDU was transmitted.
System Name	This displays the system name of the remote device.
Management Address	This displays the management address of the remote device. It could be the MAC address or IP address. You can click on the IP address hyperlink directly.

35.5.1 LLDP Remote Port Status Detail

This screen displays detailed LLDP status received from remote device. Click **Advanced Application > LLDP > LLDP Remote Status** and then click an index number, for example 1, in the **Index** column in the **LLDP Remote Status** screen to display the screen as shown next.

Figure 242 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Basic TLV)

LLDP Remote Port Status Detail		LLDP Remote Status
Local Port: 1		
Basic TLV		
Chassis ID TLV	Chassis ID Subtype	mac-address
	Chassis ID	00:19:cb:00:00:02
Port ID TLV	Port ID Subtype	local-assigned
	Port ID	1
Time To Live TLV	Time To Live	120
Port Description TLV	Port Description	12345678901234567890123456789012345678901234567890abcd
System Name TLV	System Name	GS3700
System Description TLV	System Description	V4.10(AAFZ.2) 05/16/2013
System Capabilities TLV	System Capabilities Supported	bridge
	System Capabilities Enabled	bridge
Management Address TLV	Management Address Subtype	ALL_802
	Management Address	00:19:cb:00:00:02
	Interface Number Subtype	unknown
	Interface Number	0
	Object Identifier	0

The following table describes the labels in Basic TLV part of the screen.

Table 157 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Basic TLV)

LABEL	DESCRIPTION
Basic TLV	
Chassis ID TLV	- Chassis ID Subtype - this displays how the chassis of the remote device is identified. - Chassis ID - this displays the chassis ID of the remote device. The chassis ID is identified by the chassis ID subtype
Port ID TLV	- Port ID Subtype - this displays how the port of the remote device is identified. - Port ID - this displays the port ID of the remote device. The port ID is identified by the port ID subtype.
Time To Live TLV	This displays the time-to-live (TTL) multiplier of LLDP frames. The device information on the neighboring devices ages out and is discarded when its corresponding TTL expires. The TTL value is to multiply the TTL multiplier by the LLDP frames transmitting interval.
Port Description TLV	This displays the remote port description.
System Name TLV	This displays the system name of the remote device.

Table 157 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Basic TLV)

LABEL	DESCRIPTION
System Description TLV	This displays the system description of the remote device.
System Capabilities TLV	This displays whether the system capabilities are enabled and supported on the remote device. - System Capabilities Supported - System Capabilities Enabled
Management Address TLV	This displays the following management address parameters of the remote device. - Management Address Subtype - Management Address - Interface Number Subtype - Interface Number - Object Identifier

Figure 243 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail > (Dot 1 and Dot3 TLV)

Dot1 TLV		
Port VLAN ID TLV	Port VLAN ID	100
Port-Protocol VLAN ID TLV	Port-Protocol VLAN ID	200
	Port-Protocol VLAN ID Supported	Yes
	Port-Protocol VLAN ID Enabled	Yes
Vlan Name TLV	VLAN ID	1
	VLAN Name	client 1
Protocol Identity TLV	Protocol ID	1
Dot3 TLV		
MAC PHY Configuration & Status TLV	AN Supported	Yes
	AN Enabled	Yes
	AN Advertised Capability	10baseT 10baseTFD 100baseTX 100baseTXFD 1000baseTFD
	Oper MAU type	30
Link Aggregation TLV	Aggregation Capability	Yes
	Aggregation Status	Yes
	Aggregated Port ID	1
Power Via MDI TLV	Port Class	PSE
	MDI Supported	Yes
	MDI Enabled	Yes
	Pair Controlable	No
	PSE Power Pairs	1
	Power Class	1
Max Frame Size TLV	Max Frame Size	1518

The following table describes the labels in the Dot1 and Dot3 parts of the screen.

Table 158 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Dot1 and Dot3 TLV)

LABEL	DESCRIPTION
Dot1 TLV	
Port VLAN ID TLV	This displays the VLAN ID of this port on the remote device.
Port-Protocol VLAN ID TLV	This displays the IEEE 802.1 Port Protocol VLAN ID TLV, which indicates whether the VLAN ID and whether it is enabled and supported on the port of remote Switch which sent the LLDPDU. - Port-Protocol VLAN ID - Port-Protocol VLAN ID Supported - Port-Protocol VLAN ID Enabled
Vlan Name TLV	This shows the VLAN ID and name for remote device port. - VLAN ID - VLAN Name
Protocol Identity TLV	The Protocol Identity TLV allows the Switch to advertise the particular protocols that are accessible through its port.
Dot3 TLV	
MAC PHY Configuration & Status TLV	The MAC/PHY Configuration/Status TLV advertises the bit-rate and duplex capability of the sending 802.3 node. It also advertises the current duplex and bit-rating of the sending node. Lastly, it advertises whether these setting were the result of auto-negotiation during link initiation or manual override. - AN Supported - Displays if the port supports or does not support auto-negotiation. - AN Enabled - The current auto-negotiation status of the port. - AN Advertised Capability - The auto-negotiation capabilities of the port. - Oper MAU Type - The current Medium Attachment Unit (MAU) type of the port
Link Aggregation TLV	The Link Aggregation TLV indicates whether the link is capable of being aggregated, whether the link is currently in an aggregation, and if in an aggregation, the port identification of the aggregation. - Aggregation Capability — The current aggregation capability of the port. - Aggregation Status — The current aggregation status of the port. - Aggregation Port ID — The aggregation ID of the current port.
Power Via MDI TLV	The Power Via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending port on the remote device. - Port Class - MDI Supported - MDI Enabled - Pair Controlable - PSE Power Pairs - Power Class
Max Frame Size TLV	This displays the maximum supported frame size in octets.

Figure 244 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (MED TLV)

MED TLV		
Capabilities TLV	Network Policy	Yes
	Location	Yes
	Extend Power via MDI PSE	No
	Extend Power via MDI PD	No
	Inventory Management	No
Device Type TLV	Device Type	Network Connectivity
Network Policy TLV	Voice	VLAN ID 10, tagged, known, L2-priority 7, DSCP 63
	Voice-Signaling	VLAN ID 100, tagged, known, L2-priority 2, DSCP 10
	Guest-Voice	VLAN ID 20, tagged, known, L2-priority 3, DSCP 12
	Guest-Voice-Signaling	VLAN ID 0, untagged, known, L2-priority 0, DSCP 0
	Softphone-Voice	VLAN ID 200, tagged, known, L2-priority 1, DSCP 1
	Video-Conferencing	VLAN ID 0, untagged, known, L2-priority 0, DSCP 0
	Streaming-Video	VLAN ID 300, tagged, known, L2-priority 4, DSCP 20
	Video-Signaling	VLAN ID 400, tagged, known, L2-priority 6, DSCP 55
Location Identification TLV	Coordinate-base LCI	latitude north 0.0 longitude east 0.9995 altitude meters 0.0 datum NAD83-MLLW
	Civic LCI	country TW city HSINCHU building ZYXEL
	ELIN	1234567890
Inventory TLV	Hardware Revision	V20131114 11/14/2013
	Software Revision	V4.10(AAOA.0) 11/15/2013
	Firmware Revision	V4.10(AAOA.0) 11/15/2013
	Model Name	GS3700-HP
	Manufacturer	123456789

The following table describes the labels in the MED TLV part of the screen.

Table 159 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (MED TLV)

LABEL	DESCRIPTION
MED TLV	LLDP Media Endpoint Discovery (MED) is an extension of LLDP that provides additional capabilities to support media endpoint devices. MED enables advertisement and discovery of network policies, device location discovery to allow creation of location databases, and information for troubleshooting.
Capabilities TLV	This displays the MED capabilities the remote port supports. • Network Policy • Location • Extend Power via MDI PSE • Extend Power via MDI PD • Inventory Management
Device Type TLV	LLDP-MED endpoint device classes: • Endpoint Class I • Endpoint Class II • Endpoint Class III • Network Connectivity
Network Policy TLV	This displays a network policy for the specified application. • Voice • Voice-Signaling • Guest-Voice • Guest-Voice-Signaling • Softphone-Voice • Video-Conferencing • Streaming-Video • Video-Signaling
Location Identification TLV	This shows the location information of a caller by its: • Coordinate-base LCI - latitude and longitude coordinates of the Location Configuration Information (LCI) • Civic LCI - IETF Geopriv Civic Address based Location Configuration Information • ELIN - (Emergency Location Identifier Number)

Table 159 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (MED TLV) (continued)

LABEL	DESCRIPTION
Inventory TLV	The majority of IP Phones lack support of management protocols such as SNMP, so LLDP-MED inventory TLVs are used to provide their inventory information to the Network Connectivity Devices such as the Switch. The Inventory TLV may contain the following information. • Hardware Revision • Software Revision • Firmware Revision • Model Name • Manufacturer • Serial Number • Asset ID
Extended Power via MDI TLV	Extended Power Via MDI Discovery enables detailed power information to be advertised by Media Endpoints, such as IP phones and Network Connectivity Devices such as the Switch. • Power Type - whether it is currently operating from primary power or is on backup power (backup power may indicate to the Endpoint Device that it should move to a power conservation mode). • Power Source - whether or not the Endpoint is currently operating from an external power source. • Power Priority - the Endpoint Device's power priority (which the Network Connectivity Device may use to prioritize which devices will remain in service during power shortages) • Power Value - power requirement, in fractions of Watts, in current configuration

35.6 LLDP Configuration

Use this screen to configure global LLDP settings on the Switch. Click **Advanced Application > LLDP > LLDP Configuration** to display the screen as shown next.

Figure 245 Advanced Application > LLDP > LLDP Configuration (Standalone mode)

LLDP Configuration

Basic TLV Setting

Org-specific TLV Setting

LLDP

Active

☒

Transmit Interval

30

seconds

Transmit Hold

4

times

Transmit Delay

2

seconds

Reinitialize Delay

2

seconds

Apply

Cancel

Port	Admin Status	Notification
*	Disable ▾	☐
1	Tx-Rx ▾	☐
2	Tx-Rx ▾	☐
3	Tx-Rx ▾	☐
4	Tx-Rx ▾	☐
5	Tx-Rx ▾	☐
6	Tx-Rx ▾	☐
7	Tx-Rx ▾	☐
8	Tx-Rx ▾	☐
9	Tx-Rx ▾	☐
10	Tx-Rx ▾	☐

Apply

Cancel

Figure 246 Advanced Application > LLDP > LLDP Configuration (Stacking mode)

LLDP Configuration [Basic TLV Setting](#) [Org-specific TLV Setting](#) [LLDP](#)

Active ☒

Transmit Interval seconds

Transmit Hold times

Transmit Delay seconds

Reinitialize Delay seconds

SLOT 1 ▼

Port	Admin Status	Notification
1/*	Disable ▼	☐
1/1	Tx-Rx ▼	☐
1/2	Rx ▼	☐
1/48	Tx-Rx ▼	☐
1/49	Tx-Rx ▼	☐
1/50	Tx-Rx ▼	☐

The following table describes the labels in this screen.

Table 160 Advanced Application > LLDP > LLDP Configuration

LABEL	DESCRIPTION
Active	Select to enable LLDP on the Switch. It is enabled by default.
Transmit Interval	Enter how many seconds the Switch waits before sending LLDP packets.
Transmit Hold	Enter the time-to-live (TTL) multiplier of LLDP frames. The device information on the neighboring devices ages out and is discarded when its corresponding TTL expires. The TTL value is to multiply the TTL multiplier by the LLDP packets transmitting interval.
Transmit Delay	Enter the delay (in seconds) between successive LLDPDU transmissions initiated by value or status changes in the Switch MIB.
Reinitialize Delay	Enter the number of seconds for LLDP to wait before initializing on a port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port	This displays the port number with this LLDP configuration. * means all ports (on the same Switch). In Stacking mode, the first number means Slot ID and the second is the port.

Table 160 Advanced Application > LLDP > LLDP Configuration

LABEL	DESCRIPTION
Admin Status	Select whether LLDP transmission and/or reception is allowed on this port. • Disable - not allowed • Tx-Only - transmit only • Rx-Only - receive only • Tx-Rx - transmit and receive
Notification	Select whether LLDP notification is enabled on this port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

35.6.1 LLDP Configuration Basic TLV Setting

Use this screen to configure Basic TLV settings. Click **Advanced Application > LLDP > LLDP Configuration > Basic TLV Setting** to display the screen as shown next.

Figure 247 Advanced Application > LLDP > LLDP Configuration> Basic TLV Setting (Standalone mode)

The screenshot shows the 'Basic TLV Setting' configuration screen. The title bar includes a 'Basic TLV Setting' tab and a 'LLDP Configuration' link. The main area is a table with 20 rows, each representing a port. The columns are: Port, Management Address, Port Description, System Capabilities, System Description, and System Name. Each row has checkboxes for each column. The 'Port' column lists ports from 1 to 20, with a '*' for the first row. The 'Management Address' column has checkboxes. The 'Port Description' column has checkboxes. The 'System Capabilities' column has checkboxes. The 'System Description' column has checkboxes. The 'System Name' column has checkboxes. At the bottom, there are 'Apply' and 'Cancel' buttons.

Port	Management Address	Port Description	System Capabilities	System Description	System Name
*	☐	☐	☐	☐	☐
1	☒	☒	☒	☒	☒
2	☒	☒	☒	☒	☒
3	☒	☒	☒	☒	☒
4	☒	☒	☒	☒	☒
5	☒	☒	☒	☒	☒
6	☒	☒	☒	☒	☒
7	☒	☒	☒	☒	☒
8	☒	☒	☒	☒	☒
9	☒	☒	☒	☒	☒
10	☒	☒	☒	☒	☒
11	☒	☒	☒	☒	☒
12	☒	☒	☒	☒	☒
13	☒	☒	☒	☒	☒
14	☒	☒	☒	☒	☒
15	☒	☒	☒	☒	☒
16	☒	☒	☒	☒	☒
17	☒	☒	☒	☒	☒
18	☒	☒	☒	☒	☒
19	☒	☒	☒	☒	☒
20	☒	☒	☒	☒	☒

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

Figure 248 Advanced Application > LLDP > LLDP Configuration> Basic TLV Setting (Stacking mode)

Port	Management Address	Port Description	System Capabilities	System Description	System Name
1/*	☐	☐	☐	☐	☐
1/1	☒	☒	☒	☒	☒
1/2	☒	☒	☒	☒	☒
1/49	☒	☒	☒	☒	☒
1/50	☒	☒	☒	☒	☒

The following table describes the labels in this screen.

Table 161 Advanced Application > LLDP > LLDP Configuration > Basic TLV Setting

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port	This displays the port number with this LLDP configuration. * means all ports (on the same Switch). In Stacking mode, the first number means Slot ID and the second is the port.
Management Address	Select check box to enable or disable the sending of Management Address TLVs on the port(s).
Port Description	Select check box to enable or disable the sending of Port Description TLVs on the port(s).
System Capabilities	Select check box to enable or disable the sending of System Capabilities TLVs on the port(s).
System Description	Select check box to enable or disable the sending of System Description TLVs on the port(s).
System Name	Select check box to enable or disable the sending of System Name TLVs on the port(s).
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

35.6.2 LLDP Configuration Basic Org-specific TLV Setting

Use this screen to configure organization-specific TLV settings. Click **Advanced Application > LLDP > LLDP Configuration > Org-specific TLV Setting** to display the screen as shown next.

Figure 249 Advanced Application > LLDP > LLDP Configuration> Org-specific TLV Setting (Standalone mode)

Org-specific TLV Setting [LLDP Configuration](#)

Port	Dot1 TLV			Dot3 TLV		
	Port-Protocol VLAN ID	Port VLAN ID	Link Aggregation	MAC/PHY	Max Frame Size	Power Via MDI
*	☐	☐	☐	☐	☐	☐
1	☐	☒	☐	☒	☐	☐
2	☐	☒	☐	☒	☐	☐
3	☐	☒	☐	☒	☐	☐
4	☐	☒	☐	☒	☐	☐
5	☐	☒	☐	☒	☐	☐
6	☐	☒	☐	☒	☐	☐
7	☐	☒	☐	☒	☐	☐
8	☐	☒	☐	☒	☐	☐
9	☐	☒	☐	☒	☐	☐
10	☐	☒	☐	☒	☐	☐
11	☐	☒	☐	☒	☐	☐
12	☐	☒	☐	☒	☐	☐
13	☐	☒	☐	☒	☐	☐
14	☐	☒	☐	☒	☐	☐
15	☐	☒	☐	☒	☐	☐
16	☐	☒	☐	☒	☐	☐
17	☐	☒	☐	☒	☐	☐
18	☐	☒	☐	☒	☐	☐
19	☐	☒	☐	☒	☐	☐
20	☐	☒	☐	☒	☐	☐
21	☐	☒	☐	☒	☐	☐
22	☐	☒	☐	☒	☐	☐

Apply Cancel

Figure 250 Advanced Application > LLDP > LLDP Configuration> Org-specific TLV Setting (Stacking mode)

Org-specific TLV Setting [LLDP Configuration](#)

SLOT 1 ▾

Port	Dot1 TLV			Dot3 TLV		
	Port-Protocol VLAN ID	Port VLAN ID	Link Aggregation	MAC/PHY	Max Frame Size	Power Via MDI
1/*	☐	☐	☐	☐	☐	☐
1/1	☐	☒	☐	☒	☐	☐
1/2	☐	☒	☐	☒	☐	☐
1/49	☐	☒	☐	☒	☐	☐
1/50	☐	☒	☐	☒	☐	☐

Apply Cancel

The following table describes the labels in this screen.

Table 162 Advanced Application > LLDP > LLDP Configuration > Org-specific TLV Setting

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port	This displays the port number on which you're configuring LLDP. Select check boxes in the * row (on the same Switch) to configure all ports simultaneously. In Stacking mode, the first number means Slot ID and the second is the port.
Dot1 TLV	

Table 162 Advanced Application > LLDP > LLDP Configuration > Org-specific TLV Setting

LABEL	DESCRIPTION
Port-Protocol VLAN ID	Select check box to enable or disable the sending of IEEE 802.1 Port and Protocol VLAN ID TLVs on the port(s).
Port VLAN ID	Select check box to enable or disable the sending of IEEE 802.1 Port VLAN ID TLVs on the port(s). All check boxes in this column are enabled by default.
Dot3 TLV	
Link Aggregation	Select check box to enable or disable the sending of IEEE 802.3 Link Aggregation TLVs on the port(s).
MAC/PHY	Select check box to enable or disable the sending of IEEE 802.3 MAC/PHY Configuration/Status TLVs on the port(s). All check boxes in this column are enabled by default.
Max Frame Size	Select check box to enable or disable the sending of IEEE 802.3 Max Frame Size TLVs on the port(s).
Power Via MDI	Note: For PoE models only. The Power Via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending port on the remote device. • Port Class • MDI Supported • MDI Enabled • Pair Controlable • PSE Power Pairs • Power Class
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

35.7 LLDP-MED Configuration

Click **Advanced Application > LLDP > LLDP-MED Configuration** to display the screen as shown next.

Figure 251 Advanced Application > LLDP > LLDP-MED Configuration (Standalone mode)

Port	Notification	MED TLV Setting	
	Topology Change	Location	Network Policy
*	☐	☐	☐
1	☐	☐	☐
2	☐	☐	☐
3	☐	☐	☐
4	☐	☐	☐
5	☐	☐	☐
6	☐	☐	☐
7	☐	☐	☐
8	☐	☐	☐
9	☐	☐	☐
10	☐	☐	☐
11	☐	☐	☐
12	☐	☐	☐
13	☐	☐	☐
14	☐	☐	☐
15	☐	☐	☐
16	☐	☐	☐
17	☐	☐	☐
18	☐	☐	☐
19	☐	☐	☐

Apply Cancel

Figure 252 Advanced Application > LLDP > LLDP-MED Configuration (Stacking mode)

Port	Notification	MED TLV Setting	
	Topology Change	Location	Network Policy
1/*	☐	☐	☐
1/1	☐	☐	☐
1/2	☐	☐	☐
1/49	☐	☐	☐
1/50	☐	☐	☐

Apply Cancel

The following table describes the labels in this screen.

Table 163 Advanced Application > LLDP > LLDP-MED Configuration

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port	This displays the port number on which you're configuring LLDP-MED. Select * to configure all ports (in the same Switch) simultaneously. In Stacking mode, the first number means Slot ID and the second is the port.
Notification	

Table 163 Advanced Application > LLDP > LLDP-MED Configuration

LABEL	DESCRIPTION
Topology Change	Select to enable LLDP-MED topology change traps on this port.
MED TLV Setting	
Location	Select to enable transmitting LLDP-MED location TLV.
Network Policy	Select to enable transmitting LLDP-MED Network Policy TLV.
Apply	Click Apply to save the changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

35.8 LLDP-MED Network Policy

Click **Advanced Application > LLDP > LLDP-MED Network Policy** to display the screen as shown next.

Figure 253 Advanced Application > LLDP > LLDP-MED Network Policy (Standalone mode)

LLDP-MED Network Policy LLDP

Port: 2

Application Type: voice

Tag: tagged

VLAN: 144

DSCP: 56

Priority: 4

Add Cancel

Index	Port	Application Type	Tag	VLAN	Priority	DSCP	Delete
1	2	voice	tagged	144	4	56	

Delete Cancel

Figure 254 Advanced Application > LLDP > LLDP-MED Network Policy (Stacking mode)

LLDP-MED Network Policy [LLDP](#)

Port: 1 /

Application Type: voice

Tag: tagged

VLAN:

DSCP:

Priority: 0

[Add](#) [Cancel](#)

Index	Port	Application Type	Tag	VLAN	Priority	DSCP	Delete

[Delete](#) [Cancel](#)

The following table describes the labels in this screen.

Table 164 Advanced Application > LLDP > LLDP-MED Network Policy

LABEL	DESCRIPTION
Port	Enter the port number to set up the LLDP-MED network policy. For Stacking mode the first field box is the Slot ID, the second field box is the port.
Application Type	Select the type of application used in the network policy. - voice - voice-signaling - guest-voice - guest-voice-signaling - softphone-voice - video-conferencing - streaming-video - video-signaling
Tag	Select to tag or untag in the network policy. - tagged - untagged
VLAN	Enter the VLAN ID number. It should be from 1 to 4094. For priority tagged frames, enter "0".
DSCP	Enter the DSCP value of the network policy. The value is defined from 0 through 63 with the 0 representing use of the default DSCP value.
Priority	Enter the priority value for the network policy.
Add	Click Add after finish entering the network policy information. A summary table will list all the Switch you've added.
Cancel	Click Cancel to begin entering the information afresh.
Index	This field displays the of index number of the network policy. Click an index number to edit the rule.
Port	This field displays the port number of the network policy. In stacking mode, the first number represents the slot and the second the port number.
Application Type	This field displays the application type of the network policy.
Tag	This field displays the Tag Status of the network policy.

Table 164 Advanced Application > LLDP > LLDP-MED Network Policy

LABEL	DESCRIPTION
VLAN	This field displays the VLANID of the network policy.
Priority	This field displays the priority value of the network policy.
DSCP	This field displays the DSCP value of the network policy.
Delete	Check the rules that you want to remove in the delete column, then click the Delete button.
Cancel	Click Cancel to clear the selected checkboxes in the Delete column.

35.9 LLDP-MED Location

Click **Advanced Application > LLDP > LLDP-MED Location** to display the screen as shown next.

Figure 255 Advanced Application > LLDP > LLDP-MED Location (Standalone mode)

LLDP-MED Location LLDP

Port:

Location Coordinates:

- Latitude:
- Longitude:
- Altitude:
- Datum:

Civic Address:

- Country: State:
- County: City:
- Division: Neighbor:
- Street: Leading-Street-Direction:
- Street-Suffix: Trailing-Street-Suffix:
- House-Number: House-Number-Suffix:
- Landmark: Additional-Location:
- Name: Zip-Code:
- Building: Unit:
- Floor: Room-Number:
- Place-Type: Postal-Community-Name:
- Post-Office-Box: Additional-Code:

ELIN Number:

Index	Port	Location Coordinates	Civic Address	ELIN Number	Delete
1	20	latitude north 24.7500 longi...	country TW building ZYXEL fl...	123456789111111	☐

Figure 256 Advanced Application > LLDP > LLDP-MED Location (Stacking mode)

LLDP-MED Location LLDP

Port: /

Location Coordinates

Latitude: north ▼

Longitude: west ▼

Altitude: meters ▼

Datum: WGS84 ▼

Civic Address

Country: State:

County: City:

Division: Neighbor:

Street: Leading-Street-Direction:

Street-Suffix: Trailing-Street-Suffix:

House-Number: House-Number-Suffix:

Landmark: Additional-Location:

Name: Zip-Code:

Building: Unit:

Floor: Room-Number:

Place-Type: Postal-Community-Name:

Post-Office-Box: Additional-Code:

ELIN Number:

Index	Port	Location Coordinates	Civic Address	ELIN Number	Delete

The following table describes the labels in this screen.

Table 165 Advanced Application > LLDP > LLDP-MED Location

LABEL	DESCRIPTION
Port	Enter the port number you want to set up the location within the LLDP-MED network. For Stacking mode the first field box is the Slot ID, the second field box is the port.
Location Coordinates	The LLDP-MED uses geographical coordinates and Civic Address to set the location information of the remote device. Geographical based coordinates includes latitude, longitude, altitude and datum. Civic Address includes Country, State, County, City, Street and other related information.
Latitude	Enter the latitude information. The value should be from 0° to 90°. - north - south
Longitude	Enter the longitude information. The value should be from 0° to 180°. - west - east

Table 165 Advanced Application > LLDP > LLDP-MED Location

LABEL	DESCRIPTION
Altitude	Enter the altitude information. The value should be from -2097151 to 2097151 in meters or in floors. • meters • floor
Datum	Select the appropriate geodetic datum used by GPS. • WGS84 • NAD83-NAVD88 • NAD83-MLLW
Civic Address	Enter the Civic Address by providing information such as Country, State, County, City, Street, Number, ZIP code and other additional information. Enter at least two field in this configuration including the Country. The valid length of the Country field is 2 characters and all other fields are up to 32 characters. • Country • State • County • City • Division • Neighbor • Street • Leading-Street-Direction • Street-Suffix • Trailing-Street-Suffix • House-Number • House-Number-Suffix • Landmark • Additional-Location • Name • Zip-Code • Building • Unit • Floor • Room-Number • Place-Type • Postal-Community-Name • Post-Office-Box • Additional-Code
ELIN Number	Enter a numerical digit string, corresponding to the ELIN identifier which is used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. The valid length is from 10 characters to 25 characters.
Add	Click Add after finish entering the location information.
Cancel	Click Cancel to begin entering the location information afresh.
Index	This lists the index number of the location configuration. Click an index number to view or edit the location.
Port	This lists the port number of the location configuration. In stacking mode, the first number represents the slot and the second the port number.
Location Coordinates	This field displays the location configuration information based on geographical coordinates that includes longitude, latitude, altitude and datum.
Civic Address	This field displays the Civic Address for the remote device using information such as Country, State, County, City, Street, Number, ZIP code and additional information.

Table 165 Advanced Application > LLDP > LLDP-MED Location

LABEL	DESCRIPTION
ELIN Number	This field shows the Emergency Location Identification Number (ELIN), which is used to identify endpoint devices when they issue emergency call services. The valid length is from 10 characters to 25 characters.
Delete	Check the locations that you want to remove in the Delete column, then click the Delete button.
Cancel	Click Cancel to clear the selected check boxes in the delete column.

Static Route

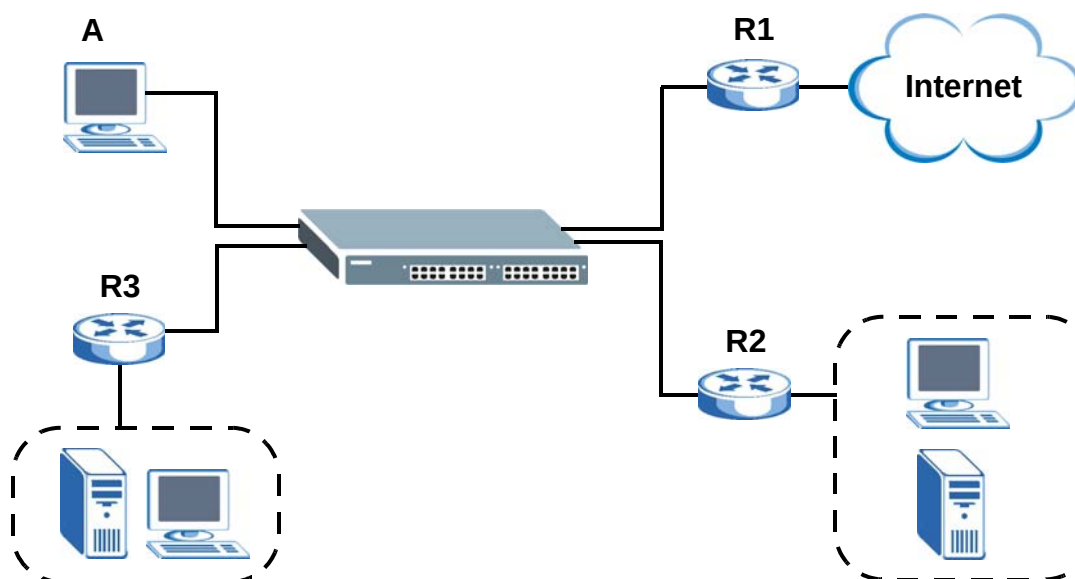
This chapter shows you how to configure static routes.

36.1 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.

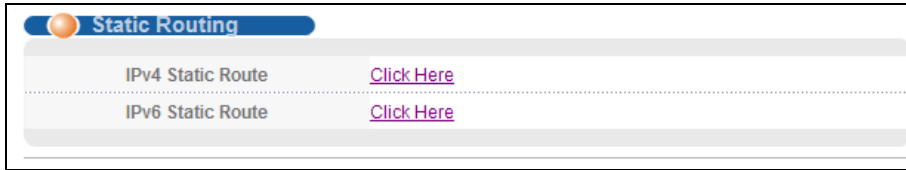
For example, the next figure shows a computer (**A**) connected to the Switch. The Switch routes most traffic from **A** to the Internet through the Switch's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the Switch.

Figure 257 Example of Static Routing Topology



36.2 Static Routing

Click **IP Application** > **Static Routing** in the navigation panel to display the screen as shown. Click the link next to **IPv4 Static Route** to open a screen where you can create IPv4 static routing rules. Click the link next to **IPv6 Static Route** to open a screen where you can create IPv6 static routing rules.

Figure 258 IP Application > Static Routing

36.3 Configuring IPv4 Static Routing

Click the link next to **IPv4 Static Route** in the **IP Application > Static Routing** screen to display the screen as shown.

Figure 259 IP Application > Static Routing > IPv4 Static Route

Index	Active	Name	Destination Address	Subnet Mask	Gateway Address	Metric	Delete
1	NO	example	172.16.1.2	255.255.255.0	192.168.1.2	2	☐

The following table describes the related labels you use to create a static route.

Table 166 IP Application > Static Routing > IPv4 Static Route

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Name	Enter a descriptive name (up to 10 printable ASCII characters) for identification purposes.
Destination IP Address	This parameter specifies the IP network address of the final destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
IP Subnet Mask	Enter the subnet mask for this destination.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your Switch that will forward the packet to the destination. The gateway must be a router on the same segment as your Switch.

Table 166 IP Application > Static Routing > IPv4 Static Route (continued)

LABEL	DESCRIPTION
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.
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.

36.4 Configuring IPv6 Static Routing

Click the link next to **IPv6 Static Route** in the **IP Application > Static Routing** screen to display the screen as shown.

Figure 260 IP Application > Static Routing > IPv6 Static Route

IPv6 Static Route [Static Routing](#)

Route Destination:

Prefix Length:

Next Hop:

Interface Type: **VLAN** ▼

Interface ID:

Index	Interface	Route Destination/Prefix Length	Next Hop	Delete
1	VLAN123	2001:db8::/32	fe80::219:cbff:fe37:49	☐
2	VLAN123	2001:db8:1a2b:15::/64	fe80::219:cbff:fe37:49	☐

The following table describes the related labels you use to create a static route.

Table 167 IP Application > Static Routing > IPv6 Static Route

LABEL	DESCRIPTION
Route Destination	Enter the IPv6 address of the final destination.
Prefix Length	Enter the prefix length number of up to 64 for this destination.
Next Hop	Enter the IPv6 address of the next-hop router.
Interface Type	Select the type of the IPv6 interface through which the IPv6 packets are forwarded. The Switch supports only the VLAN interface type at the time of writing.
Interface ID	Enter the ID number of the IPv6 interface through which the IPv6 packets are forwarded.
Add	Click Add to insert a new static route to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Index	This field displays the index number of the route. Click a number to edit the static route entry.
Interface	This field displays the descriptive name of the interface that is used to forward the packets to the destination.
Route Destination/ Prefix Length	This field displays the IPv6 subnet prefix and prefix length of the final destination.
Next Hop	This field displays the IPv6 address of the gateway that helps forward the packet to the destination.
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.

37.1 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.

37.1.1 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.

37.2 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 261 IP Application > Policy Routing

Policy Route [Rule Configuration](#)

Active ☐

Profile Name

Add Cancel Clear

Index	Active	Profile name	Delete
1	Yes	test	☐

Delete Cancel

The following table describes the labels in this screen.

Table 168 IP Application > Policy Routing

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this policy routing profile and rules in the profile.
Profile Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes. Spaces are allowed.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Clear	Click Clear to set the above fields back to the factory defaults.
Index	This field displays the index number of the policy routing profile. Click a number to edit the policy routing profile entry.
Active	This field displays Yes when the policy routing profile is activated and No when it is deactivated.
Profile Name	This field displays the descriptive name for this profile. This is for identification purposes only.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

37.2.1 Policy Routing Rule Configuration

You must first configure a layer-3 classifier in the **Classifier** screen (see [Section 19.2 on page 188](#)) and a policy routing profile in the **Policy Routing** screen (see [Section 37.2 on page 356](#)).

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 262 IP Application > Policy Routing > Rule Configuration

The following table describes the labels in this screen.

Table 169 IP Application > Policy Routing > Rule Configuration

LABEL	DESCRIPTION
Profile Name	This field displays the policy routing profile(s) you configure in the IP Application > Policy Routing screen. Select a profile for which you want to configure a policy routing rule.
Sequence	Enter the rule number from 1 to 64. The ordering of your rules is important as rules are applied in turn. You can not specify a number already in use by another rule.
Statement	Select Permit to forward traffic that matches this rule to the gateway specified in the rule. Select Deny to disable the rule action and forward traffic that matches this rule according to the routing table on the Switch.
Classifier	This field displays the available active classifiers you configure in the Classifier screen (see Chapter 19 on page 188), 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.

Table 169 IP Application > Policy Routing > Rule Configuration (continued)

LABEL	DESCRIPTION
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Clear	Click Clear to set the above fields back to the factory defaults.
Active	This field displays whether the policy route profile is enabled or not.
Profile Name	This field displays the name of the policy route profile with which the rule is associated.
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.

Differentiated Services

This chapter shows you how to configure Differentiated Services (DiffServ) on the Switch.

38.1 DiffServ Overview

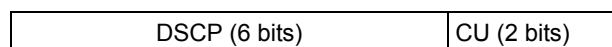
Quality of Service (QoS) is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

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.

38.1.1 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 263 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.

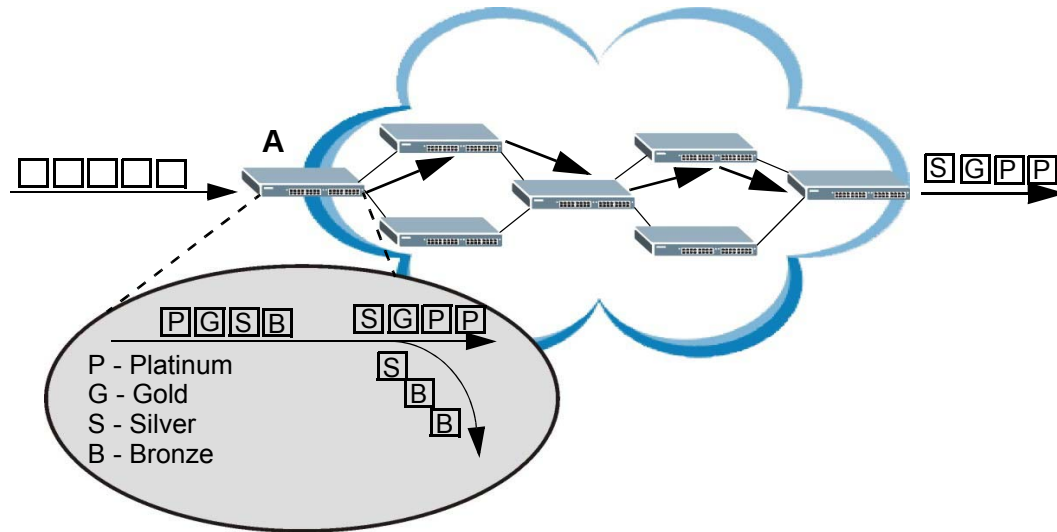
The DSCP value determines the PHB (Per-Hop Behavior), that each packet gets as it is forwarded across the DiffServ network. Based on the marking rule different kinds of traffic can be marked for different priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured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

38.1.2 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 264](#)) 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 264 DiffServ Network



38.2 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:

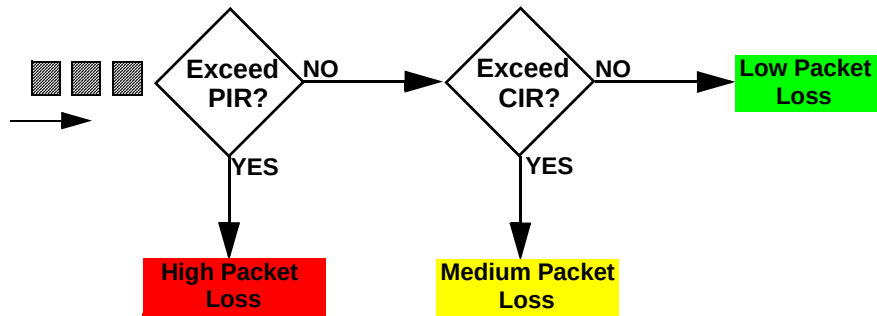
- Red (high loss priority level) packets are dropped.
- Yellow (medium loss priority level) packets are dropped if there is congestion on the network.
- Green (low loss priority level) packets are forwarded.

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.

38.2.1 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 265 TRTCM - Color-blind Mode

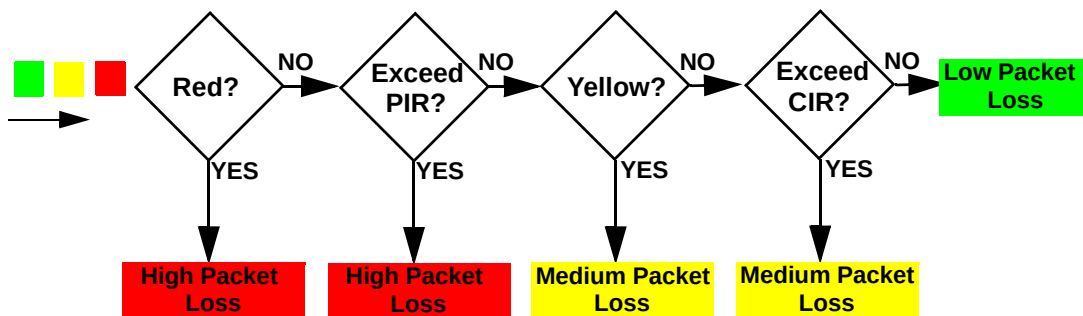


38.2.2 TRTCM - Color-aware Mode

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 266 TRTCM - Color-aware Mode



38.3 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 267 IP Application > DiffServ (Standalone mode)

Diffserv [2-rate 3 Color Marker](#) [DSCP Setting](#)

Active ☐

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

Apply Cancel

Figure 268 IP Application > DiffServ (Stacking mode)

Diffserv [2-rate 3 Color Marker](#) [DSCP Setting](#)

Active ☐

SLOT 1 ▼

Port	Active
1/*	☐
1/1	☐
1/48	☐
1/49	☐
1/50	☐

Apply Cancel

The following table describes the labels in this screen.

Table 170 IP Application > DiffServ

LABEL	DESCRIPTION
Active	Select this option to enable DiffServ on the Switch.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port	This field displays the index number of a port on the Switch. In stacking mode, the first number represents the slot and the second the port number. * means all ports (on the same Switch).
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select Active to enable DiffServ on the port.

Table 170 IP Application > DiffServ (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.

38.3.1 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 269 IP Application > DiffServ > 2-rate 3 Color Marker (Standalone mode)

2-Rate 3 Color Marker [DSCP Profile](#) [Diffserv](#)

Active ☐

Mode ☒ color-blind ☐ color-aware

Port	Active	Commit Rate	Peak Rate	DSCP
*	☐	Kbps	Kbps	Default ▼
1	☐	1 Kbps	1 Kbps	Default ▼
2	☐	1 Kbps	1 Kbps	Default ▼
3	☐	1 Kbps	1 Kbps	Default ▼
4	☐	1 Kbps	1 Kbps	Default ▼
5	☐	1 Kbps	1 Kbps	Default ▼
6	☐	1 Kbps	1 Kbps	Default ▼
7	☐	1 Kbps	1 Kbps	Default ▼
8	☐	1 Kbps	1 Kbps	Default ▼
9	☐	1 Kbps	1 Kbps	Default ▼
10	☐	1 Kbps	1 Kbps	Default ▼
11	☐	1 Kbps	1 Kbps	Default ▼

Apply Cancel

Figure 270 IP Application > DiffServ > 2-rate 3 Color Marker (Stacking mode)

2-Rate 3 Color Marker [DSCP Profile](#) [Diffserv](#)

Active ☐

Mode

☒ color-blind

☐ color-aware

SLOT 1 ▼

Port	Active	Commit Rate	Peak Rate	DSCP
1/*	☐	Kbps	Kbps	Default ▼
1/1	☐	1 Kbps	1 Kbps	Default ▼
1/2	☐	1 Kbps	1 Kbps	Default ▼
1/49	☐	1 Kbps	1 Kbps	Default ▼
1/50	☐	1 Kbps	1 Kbps	Default ▼

Apply **Cancel**

The following table describes the labels in this screen.

Table 171 IP Application > DiffServ > 2-rate 3 Color Marker

LABEL	DESCRIPTION
Active	Select this to activate TRTCM (Two Rate Three Color Marker) on the Switch. The Switch evaluates and marks the packets based on the TRTCM settings. Note: You must also activate DiffServ on the Switch and the individual ports for the Switch to drop red (high loss priority) colored packets.
Mode	Select color-blind to have the Switch treat all incoming packets as uncolored. All incoming packets are evaluated against the CIR and PIR. Select color-aware to treat the packets as marked by some preceding entity. Incoming packets are evaluated based on their existing color. Incoming packets that are not marked proceed through the Switch.
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port	This field displays the index number of a port on the Switch. In stacking mode, the first number represents the slot and the second the port number. * means all ports (on the same Switch).
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this to activate TRTCM on the port.
Commit Rate	Specify the Commit Information Rate (CIR) for this port.
Peak Rate	Specify the Peak Information Rate (PIR) for this port.
DSCP	Select a pre-defined DSCP profile. The Switch assigns the DSCP values defined in the profile to packets based on the color they are marked via TRTCM.

Table 171 IP Application > DiffServ > 2-rate 3 Color Marker (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.

38.3.2 DSCP Profile

Use this screen to create DSCP profiles. To open this screen, click the **DSCP Profile** link in the **IP Application > DiffServ > 2-rate 3 Color Marker** screen.

Figure 271 IP Application > DiffServ > 2-rate 3 Color Marker > DSCP Profile

The screenshot shows the 'DSCP Profile' configuration interface. At the top, there's a navigation bar with 'DSCP Profile' and a link to 'Two-Rate Three Color Marker'. Below this is the 'DSCP Setup' section. It features four input fields for 'Profile Name', 'Green', 'Yellow', and 'Red', each containing the value '0'. Below these fields are 'Add' and 'Cancel' buttons. At the bottom, there's a table with columns: 'Profile Name', 'Green', 'Yellow', 'Red', and 'Delete Profile'. The table has one row with 'Default' as the profile name and '0' for the other three values. Below the table are 'Delete' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 172 IP Application > DiffServ > 2-rate 3 Color Marker > DSCP Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile for identification purposes.
DSCP	Use this section to specify the DSCP values that you want to assign to packets based on the color they are marked via TRTCM.
Green	Specify the DSCP value to use for packets with low packet loss priority.
Yellow	Specify the DSCP value to use for packets with medium packet loss priority.
Red	Specify the DSCP value to use for packets with high packet loss priority.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the fields to your previous configuration.
Profile Name	This field displays the descriptive name of the profile. Click the profile name to change the settings.
Green	This field displays the DSCP value to use for packets with low packet loss priority.
Yellow	This field displays the DSCP value to use for packets with medium packet loss priority.
Red	This field displays the DSCP value to use for packets with high packet loss priority.

Table 172 IP Application > DiffServ > 2-rate 3 Color Marker > DSCP Profile (continued)

LABEL	DESCRIPTION
Delete Profile	Select the entry(ies) that you want to remove in the Delete Profile column.
Delete	Click the Delete button to remove the selected entry(ies) from the table.
Cancel	Click this to revert the fields to the previous configuration.

38.4 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 173 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

38.4.1 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 272 IP Application > DiffServ > DSCP Setting

DSCP Setting

DSCP to 802.1p Mapping

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

Apply Cancel

The following table describes the labels in this screen.

Table 174 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.

39.1 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.

39.1.1 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.

39.1.2 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:

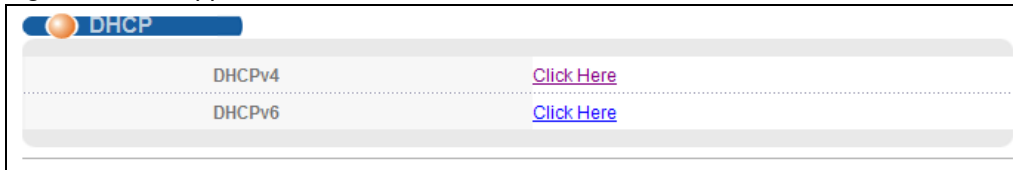
- **Global** - The Switch forwards all DHCP requests to the same DHCP server.
- **VLAN** - The Switch is configured on a VLAN by VLAN basis. The Switch can be configured as a DHCP server for one VLAN and at the same time the Switch can be configured to relay DHCP requests for clients in another VLAN.

39.2 DHCP Configuration

Click **IP Application > DHCP** in the navigation panel to display the screen as shown. Click the link next to **DHCPv4** to open screens where you can enable and configure DHCPv4 server/relay settings

and create option 82 profiles. Click the link next to **DHCPv6** to open a screen where you can configure DHCPv6 relay settings.

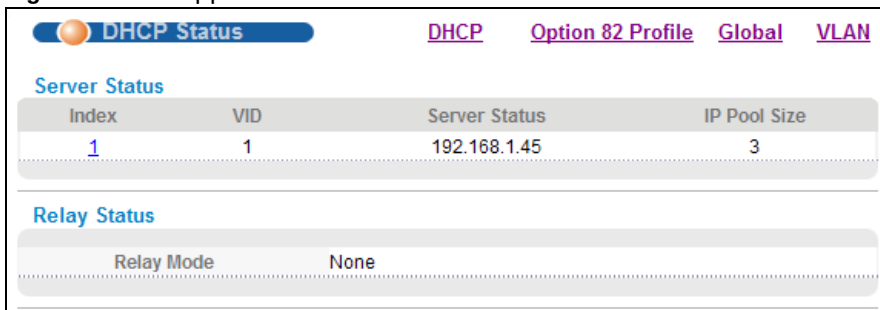
Figure 273 IP Application > DHCP



39.3 DHCPv4 Status

Click **IP Application > DHCP > DHCPv4** in the navigation panel. The **DHCP Status** screen displays.

Figure 274 IP Application > DHCP > DHCPv4



The following table describes the labels in this screen.

Table 175 IP Application > DHCP > DHCPv4

LABEL	DESCRIPTION
Server Status	This section displays configuration settings related to the Switch's DHCP server mode.
Index	This is the index number. Click an index number to change the settings.
VID	This field displays the VLAN ID for which the Switch is a DHCP server.
Server Status	This field displays the starting DHCP client IP address.
IP Pool Size	This field displays the number of IP addresses that can be assigned to clients.
Relay Status	This section displays configuration settings related to the Switch's DHCP relay mode.
Relay Mode	This field displays: • None - if the Switch is not configured as a DHCP relay agent. • Global - if the Switch is configured as a DHCP relay agent only. • VLAN - followed by a VLAN ID or multiple VLAN IDs if it is configured as a relay agent for specific VLAN(s).

39.3.1 DHCPv4 Server Status Detail

Click **IP Application > DHCP > DHCPv4** in the navigation panel and then click an existing index number of a DHCP server configuration to view the screen as shown. Use this screen to view details regarding DHCP server settings configured on the Switch.

Figure 275 IP Application > DHCP > DHCPv4 > Server Status Detail

Server Status Detail		DHCP Status
Start IP Address	192.168.1.45	
End IP Address	192.168.1.47	
Subnet Mask	255.255.255.0	
Default Gateway	0.0.0.0	
Primary DNS Server	0.0.0.0	
Secondary DNS Server	0.0.0.0	
Address Leases		
Index	IP Address	Timer
Hardware Address	Hostname	

The following table describes the labels in this screen.

Table 176 IP Application > DHCP > DHCPv4 > Server Status Detail

LABEL	DESCRIPTION
Start IP Address	This field displays the starting IP address of the IP address pool configured for this DHCP server instance.
End IP Address	This field displays the last IP address of the IP address pool configured for this DHCP server instance.
Subnet Mask	This field displays the subnet mask value sent to clients from this DHCP server instance.
Default Gateway	This field displays the default gateway value sent to clients from this DHCP server instance.
Primary DNS Server	This field displays the primary DNS server value sent to clients from this DHCP server instance.
Secondary DNS Server	This field displays the secondary DNS server value sent to clients from this DHCP server instance.
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.

39.4 DHCPv4 Relay

Configure DHCP relay on the Switch if the DHCP clients and the DHCP server are not in the same broadcast domain. During the initial IP address leasing, the Switch helps to relay network information (such as the IP address and subnet mask) between a DHCP client and a DHCP server. Once the DHCP client obtains an IP address and can connect to the network, network information renewal is done between the DHCP client and the DHCP server without the help of the Switch.

The Switch can be configured as a global DHCP relay. This means that the Switch forwards all DHCP requests from all domains to the same DHCP server. You can also configure the Switch to relay DHCP information based on the VLAN membership of the DHCP clients.

39.4.1 DHCPv4 Relay Agent Information

The Switch can add information about the source of client DHCP requests that it relays to a DHCP server by adding **Relay Agent Information**. This helps provide authentication about the source of the requests. The DHCP server can then provide an IP address based on this information. Please refer to RFC 3046 for more details.

The DHCP **Relay Agent Information** feature adds an Agent Information field (also known as the **Option 82** field) to DHCP requests. The **Option 82** field is in the DHCP headers of client DHCP request frames that the Switch relays to a DHCP server.

39.4.1.1 DHCPv4 Relay Agent Information Format

A DHCP Relay Agent Information option has the following format.

Table 177 DHCP Relay Agent Information Option Format

Code (82)	Length (N)	i1	i2	...	iN

i1, i2 and iN are DHCP relay agent sub-options, which contain additional information about the DHCP client. You need to define at least one sub-option.

39.4.1.2 Sub-Option Format

There are two types of sub-option: "Agent Circuit ID Sub-option" and "Agent Remote ID Sub-option". They have the following formats.

Table 178 DHCP Relay Agent Circuit ID Sub-option Format

SubOpt Code	Length	Value
1 (1 byte)	N (1 byte)	Slot ID, Port ID, VLAN ID, System Name or String

Table 179 DHCP Relay Agent Remote ID Sub-option Format

SubOpt Code	Length	Value
2 (1 byte)	N (1 byte)	MAC Address or String

The 1 in the first field identifies this as an Agent Circuit ID sub-option and 2 identifies this as an Agent Remote ID sub-option. The next field specifies the length of the field.

39.4.2 DHCPv4 Option 82 Profile

Use this screen to create DHCPv4 option 82 profiles. Click **IP Application > DHCP > DHCPv4** in the navigation panel and click the **Option 82 Profile** link to display the screen as shown.

Figure 276 IP Application > DHCP > DHCPv4 > Option 82 Profile

DHCP Option 82 Profile DHCP Setting

Profile Setup

Name

Circuit-ID ☐ Enable
☐ slot-port ☐ vlan ☐ hostname
 string

Remote-ID ☐ Enable
☐ mac
 string

Profile Name	Enable	Circuit-ID Field	Remote-ID Field	Delete
default1	Yes	slot-port, vlan	-	☐
default2	Yes	slot-port, vlan, hostname	-	☐

The following table describes the labels in this screen.

Table 180 IP Application > DHCP > DHCPv4 > Option 82 Profile

LABEL	DESCRIPTION
Name	Enter a descriptive name for the profile for identification purposes. You can use up to 32 ASCII characters. Spaces are allowed.
Circuit-ID	Use this section to configure the Circuit ID sub-option to include information that is specific to the relay agent (the Switch).
Enable	Select this option to have the Switch add the Circuit ID sub-option to client DHCP requests that it relays to a DHCP server.
slot-port	Select this option to have the Switch add the number of port that the DHCP client is connected to.
vlan	Select this option to have the Switch add the ID of VLAN which the port belongs to.
hostname	This is the system name you configure in the Basic Setting > General Setup screen. Select this option for the Switch to add the system name to the client DHCP requests that it relays to a DHCP server.
string	Enter a string of up to 64 ASCII characters that the Switch adds into the client DHCP requests. Spaces are allowed.
Remote-ID	Use this section to configure the Remote ID sub-option to include information that identifies the relay agent (the Switch).
Enable	Select this option to have the Switch append the Remote ID sub-option to the option 82 field of DHCP requests.
mac	Select this option to have the Switch add its MAC address to the client DHCP requests that it relays to a DHCP server.
string	Enter a string of up to 64 ASCII characters for the remote ID information in this field. Spaces are allowed.

Table 180 IP Application > DHCP > DHCPv4 > Option 82 Profile (continued)

LABEL	DESCRIPTION
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to their last saved values.
Profile Name	This field displays the descriptive name of the profile. Click the name to change the settings.
Circuit-ID	
Enable	This field displays whether the Circuit ID sub-option is added to client DHCP requests.
Field	This field displays the information that is included in the Circuit ID sub-option.
Remote-ID	
Enable	This field displays whether the Remote ID sub-option is added to client DHCP requests.
Field	This field displays the information that is included in the Remote ID sub-option.
Delete	Check the entry(ies) 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.

39.4.3 Configuring DHCPv4 Global Relay

Use this screen to configure global DHCPv4 relay. Click **IP Application > DHCP > DHCPv4** in the navigation panel and click the **Global** link to display the screen as shown.

Figure 277 IP Application > DHCP > DHCPv4 > Global

The screenshot shows the 'DHCP Relay' configuration page. At the top, there's a blue header with an orange circle icon and the text 'DHCP Relay'. To the right of the header are links for 'Port' and 'Status'. Below the header, there's a section with the following fields:

- Active:** A checkbox that is checked.
- Remote DHCP Server 1:** A text input field containing '192.168.2.2'.
- Remote DHCP Server 2:** A text input field containing '0.0.0.0'.
- Remote DHCP Server 3:** A text input field containing '0.0.0.0'.
- Option 82 Profile:** A dropdown menu showing 'default1'.

At the bottom of the form, there are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

Table 181 IP Application > DHCP > DHCPv4 > Global

LABEL	DESCRIPTION
Active	Select this check box to enable DHCPv4 relay.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCPv4 server in dotted decimal notation.
Option 82 Profile	Select a pre-defined DHCPv4 option 82 profile that the Switch applies to all ports. The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server.

Table 181 IP Application > DHCP > DHCPv4 > Global (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.

39.4.4 DHCPv4 Global Relay Port Configure

Use this screen to apply a different DHCP option 82 profile to certain ports on the Switch. To open this screen, click **IP Application > DHCP > DHCPv4 > Global > Port**.

Figure 278 IP Application > DHCP > DHCPv4 > Global > Port

The screenshot shows the 'Port' configuration screen for DHCPv4 Global Relay. The top navigation bar includes 'Port' (selected) and 'DHCP relay'. The main area contains two input fields: 'Port' and 'Option 82 Profile'. Below these fields are three buttons: 'Add', 'Cancel', and 'Clear'. A table below shows a single entry with index 1, port 3,5-8, and profile name default1. At the bottom of the table are 'Delete' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 182 IP Application > DHCP > DHCPv4 > Global > Port

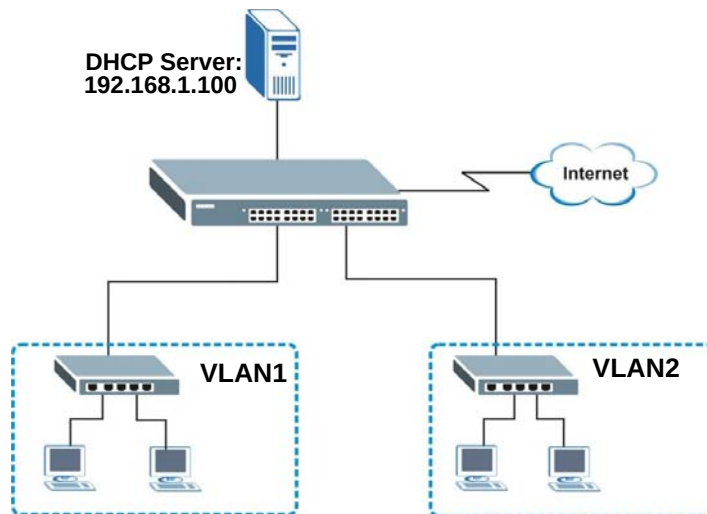
LABEL	DESCRIPTION
Port	Enter the number of port(s) to which you want to apply the specified DHCP option 82 profile. You can enter multiple ports separated by (no space) comma (,) or hyphen (-) for a range. For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7. In stacking mode, the first number represents the slot and the second the port number. Enter 1/1-1/24,2/28 for ports 1 to 24 for the Switch in slot 1 and port 28 for the Switch in slot 2, for example.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to the specified port(s). The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server. Note: The profile you select here has priority over the one you select in the DHCP > DHCPv4 > Global screen.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values above based on the last selected entry or, if not applicable, to clear the fields above.
Clear	Click Clear to reset the fields to the factory defaults.

Table 182 IP Application > DHCP > DHCPv4 > Global > Port (continued)

LABEL	DESCRIPTION
Index	This field displays a sequential number for each entry. Click an index number to change the settings.
Port	This field displays the port(s) to which the Switch applies the settings. In stacking mode, the first number represents the slot and the second the port number.
Profile Name	This field displays the DHCP option 82 profile that the Switch applies to the port(s).
Delete	Select the entry(ies) that you want to remove in the Delete column, then click the Delete button to remove the selected entry(ies) from the table.
Cancel	Click this to clear the Delete check boxes above.

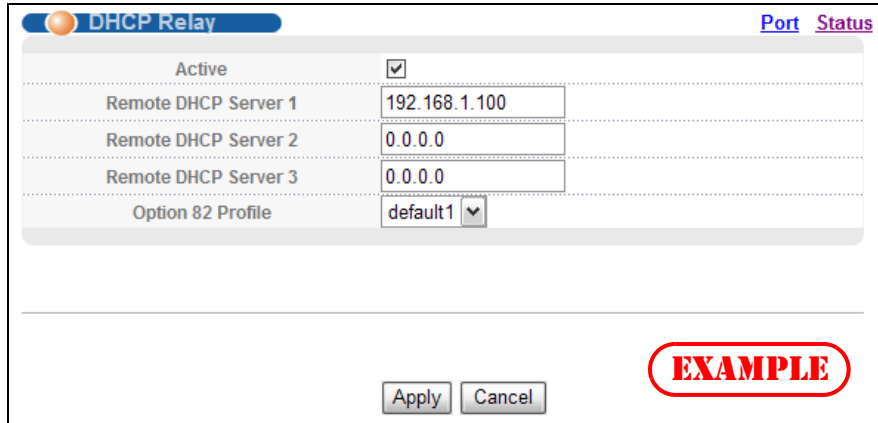
39.4.5 Global DHCP Relay Configuration Example

The follow figure shows a network example where the Switch is used to relay DHCP requests for the **VLAN1** and **VLAN2** domains. There is only one DHCP server that services the DHCP clients in both domains.

Figure 279 Global DHCP Relay Network Example

Configure the **DHCP Relay** screen as shown. Make sure you select a DHCP option 82 profile (**default1** in this example) to set the Switch to send additional information (such as the VLAN ID) together with the DHCP requests to the DHCP server. This allows the DHCP server to assign the appropriate IP address according to the VLAN ID.

Figure 280 DHCP Relay Configuration Example



The image shows a web-based configuration interface for DHCP Relay. At the top, there is a header bar with an orange circle icon, the text "DHCP Relay", and two links: "Port" and "Status". Below the header is a table with the following rows:

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
Option 82 Profile	default1 ▼

At the bottom of the form, there are two buttons: "Apply" and "Cancel". To the right of these buttons, there is a red oval containing the word "EXAMPLE" in red capital letters.

39.5 Configuring DHCP VLAN Settings

Use this screen to configure your DHCP settings based on the VLAN domain of the DHCP clients. Click **IP Application** > **DHCP** > **DHCPv4** in the navigation panel, then click the **VLAN** link in the **DHCP Status** screen that displays.

Note: You must set up a management IP address for each VLAN that you want to configure DHCP settings for on the Switch. See [Section 6.5 on page 62](#) for information on how to do this.

Figure 281 IP Application > DHCP > DHCPv4 > VLAN

VLAN Setting Port Status

VID: 1234

DHCP Status: ☐ Server ☒ Relay

Server

Client IP Pool Starting Address: 0.0.0.0

Size of Client IP Pool: [Slider]

IP Subnet Mask: 0.0.0.0

Default Gateway: 0.0.0.0

Primary DNS Server: 0.0.0.0

Secondary DNS Server: 0.0.0.0

Relay

Remote DHCP Server 1: 192.168.1.6

Remote DHCP Server 2: 0.0.0.0

Remote DHCP Server 3: 0.0.0.0

Option 82 Profile: default1

[Add] [Cancel] [Clear]

VID	Type	DHCP Status	Delete
1234	Relay	192.168.1.6	☐

[Delete] [Cancel]

The following table describes the labels in this screen.

Table 183 IP Application > DHCP > DHCPv4 > VLAN

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN to which these DHCP settings apply.
DHCP Status	Select whether the Switch should function as a DHCP Server or Relay for the specified VID. If you select Server then fields related to DHCP relay configuration are grayed out and vice versa.
Server	Use this section if you want to configure the Switch to function as a DHCP server for this VLAN.
Client IP Pool Starting Address	Specify the first of the contiguous addresses in the IP address pool.
Size of Client IP Pool	Specify the size, or count of the IP address pool. The Switch can issue from 1 to 253 IP addresses to DHCP clients.
IP Subnet Mask	Enter the subnet mask for the client IP pool.
Default Gateway	Enter the IP address of the default gateway device.
Primary/Secondary DNS Server	Enter the IP addresses of the DNS servers. The DNS servers are passed to the DHCP clients along with the IP address and the subnet mask.
Relay	Use this section if you want to configure the Switch to function as a DHCP relay for this VLAN.

Table 183 IP Application > DHCP > DHCPv4 > VLAN (continued)

LABEL	DESCRIPTION
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCP server in dotted decimal notation.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to all ports in this VLAN. The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to reset the fields to the factory defaults.
VID	This field displays the ID number of the VLAN group to which this DHCP settings apply.
Type	This field displays Server or Relay for the DHCP mode.
DHCP Status	For DHCP server configuration, this field displays the starting IP address and the size of the IP address pool. For DHCP relay configuration, this field displays the first remote DHCP server IP address.
Delete	Select the configuration entries you want to remove and click Delete to remove them.
Cancel	Click Cancel to clear the Delete check boxes.

39.5.1 DHCPv4 VLAN Port Configure

Use this screen to apply a different DHCP option 82 profile to certain ports in a VLAN. To open this screen, click **IP Application > DHCP > DHCPv4 > VLAN > Port**.

Figure 282 IP Application > DHCP > DHCPv4 > VLAN > Port

The screenshot shows the 'Port' configuration page for DHCPv4 VLAN. The top navigation bar includes 'Port' and 'VLAN Setting'. The main configuration area has three fields: 'VID', 'Port', and 'Option 82 Profile' (a dropdown menu). Below these fields are three buttons: 'Add', 'Cancel', and 'Clear'. At the bottom, there is a table with columns: 'Index', 'VID', 'Port', 'Profile Name', and 'Delete'. Below the table are two buttons: 'Delete' and 'Cancel'.

The following table describes the labels in this screen.

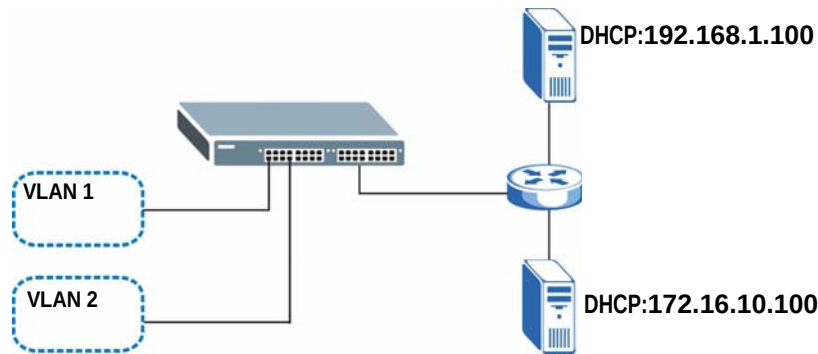
Table 184 IP Application > DHCP > DHCPv4 > VLAN > Port

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN you want to configure here.
Port	Enter the number of port(s) to which you want to apply the specified DHCP option 82 profile. You can enter multiple ports separated by (no space) comma (,) or hyphen (-) for a range. For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7. In stacking mode, the first number represents the slot and the second the port number. Enter 1/1-1/24,2/28 for ports 1 to 24 for the Switch in slot 1 and port 28 for the Switch in slot 2, for example.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to the specified port(s) in this VLAN. The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server. Note: The profile you select here has priority over the one you select in the DHCP > DHCPv4 > VLAN screen.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values above based on the last selected entry or, if not applicable, to clear the fields above.
Clear	Click Clear to reset the fields to the factory defaults.
Index	This field displays a sequential number for each entry. Click an index number to change the settings.
VID	This field displays the VLAN to which the port(s) belongs.
Port	This field displays the port(s) to which the Switch applies the settings.
Profile Name	This field displays the DHCP option 82 profile that the Switch applies to the port(s) in this VLAN.
Delete	Select the entry(ies) that you want to remove in the Delete column, then click the Delete button to remove the selected entry(ies) from the table.
Cancel	Click this to clear the Delete check boxes above.

39.5.2 Example: DHCP Relay for Two VLANs

The following example displays two VLANs (VIDs 1 and 2) for a campus network. Two DHCP servers are installed to serve each VLAN. The system is set up to forward DHCP requests from the dormitory rooms (VLAN 1) to the DHCP server with an IP address of 192.168.1.100. Requests from the academic buildings (VLAN 2) are sent to the other DHCP server with an IP address of 172.16.10.100.

Figure 283 DHCP Relay for Two VLANs



For the example network, configure the **VLAN Setting** screen as shown.

Figure 284 DHCP Relay for Two VLANs Configuration Example

VLAN Setting Port Status

VID	2
DHCP Status	☐ Server ☒ Relay
Server	
Client IP Pool Starting Address	0.0.0.0
Size of Client IP Pool	
IP Subnet Mask	0.0.0.0
Default Gateway	0.0.0.0
Primary DNS Server	0.0.0.0
Secondary DNS Server	0.0.0.0
Relay	
Remote DHCP Server 1	172.16.10.100
Remote DHCP Server 2	0.0.0.0
Remote DHCP Server 3	0.0.0.0
Option 82 Profile	

VID	Type	DHCP Status	Delete
1	Relay	192.168.1.100	☐

EXAMPLE

39.6 DHCPv6 Relay

A DHCPv6 relay agent is on the same network as the DHCPv6 clients and helps forward messages between the DHCPv6 server and clients. When a client cannot use its link-local address and a well-

known multicast address to locate a DHCPv6 server on its network, it then needs a DHCPv6 relay agent to send a message to a DHCPv6 server that is not attached to the same network.

The DHCPv6 relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCPv6 server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Use this screen to configure DHCPv6 relay settings for a specific VLAN on the Switch. Click **IP Application > DHCP > DHCPv6** in the navigation panel to display the screen as shown.

Figure 285 IP Application > DHCP > DHCPv6

The screenshot shows the DHCPv6 Relay configuration interface. At the top, there's a title bar with 'DHCPv6 Relay' and a 'DHCP' link. Below this, there are input fields for 'VID', 'Helper Address', and 'Remote ID'. A checkbox for 'Interface ID' is located under the 'Options' section. Below these fields are 'Add', 'Cancel', and 'Clear' buttons. At the bottom, there is a table with columns: VID, Helper Address, Interface ID, Remote ID, and Delete. Below the table are 'Delete' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 185 IP Application > DHCP > DHCPv6

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN you want to configure here.
Helper Address	Enter the remote DHCPv6 server address for the specified VLAN.
Options	
Interface ID	Select this option to have the Switch add the interface-ID option in the DHCPv6 requests from the clients in the specified VLAN before the Switch forwards them to a DHCPv6 server.
Remote ID	Enter a string of up to 64 printable characters to be carried in the remote-ID option. The Switch adds the remote-ID option in the DHCPv6 requests from the clients in the specified VLAN before the Switch forwards them to a DHCPv6 server.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to their last saved values.
Clear	Click Clear to reset the fields to the factory defaults.
VID	This field displays the VLAN ID number. Click the VLAN ID to change the settings.

Table 185 IP Application > DHCP > DHCPv6 (continued)

LABEL	DESCRIPTION
Helper Address	This field displays the IPv6 address of the remote DHCPv6 server for this VLAN.
Interface ID	This field displays whether the interface-ID option is added to DHCPv6 requests from clients in this VLAN.
Remote ID	This field displays whether the remote-ID option is added to DHCPv6 requests from clients in this VLAN.
Delete	Check the entry(ies) 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.

This chapter shows you how to configure and monitor the Virtual Router Redundancy Protocol (VRRP) on the Switch.

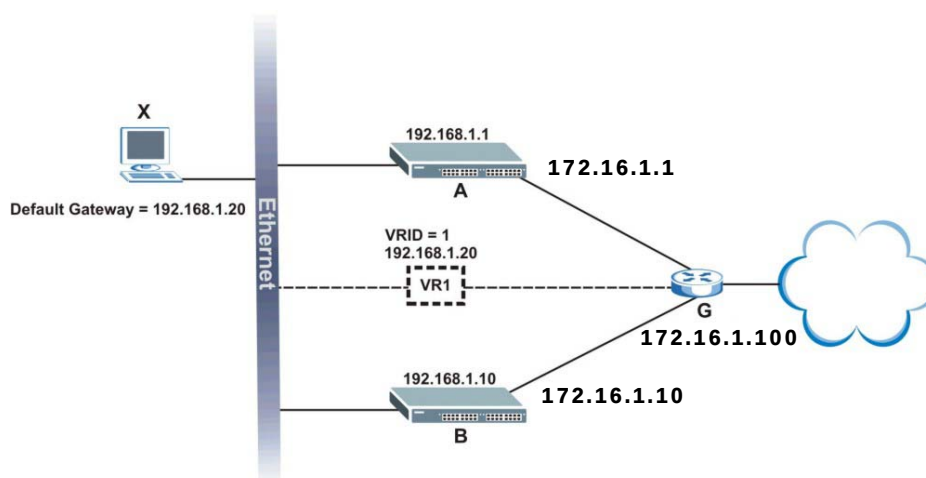
40.1 VRRP Overview

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 286 VRRP: Example 1



If switch **A** (the master router) is unavailable, switch **B** takes over. Traffic is then processed by switch **B**.

40.2 VRRP Status

Click **IP Application** > **VRRP** in the navigation panel to display the **VRRP Status** screen as shown next.

Figure 287 IP Application > VRRP Status

Index	Network	VRID	VR Status	Uplink Status
1	192.168.1.1/24	1	Master	Alive

Poll Interval(s)

The following table describes the labels in this screen.

Table 186 IP Application > VRRP Status

LABEL	DESCRIPTION
Index	This field displays the index number of a rule.
Network	This field displays the IP address and the subnet mask bits of an IP routing domain that is associated to a virtual router.
VRID	This field displays the ID number of the virtual router.
VR Status	This field displays the status of the virtual router. This field is Master indicating that this Switch functions as the master router. This field is Backup indicating that this Switch functions as a backup router. This field displays Init when this Switch is initiating the VRRP protocol or when the Uplink Status field displays Dead.
Uplink Status	This field displays the status of the link between this Switch and the uplink gateway. This field is Alive indicating that the link between this Switch and the uplink gateway is up. Otherwise, this field is Dead. This field displays Probe when this Switch is check for the link state.
Poll Interval(s)	The text box displays how often (in seconds) this screen refreshes. You may change the refresh interval by typing a new number in the text box and then clicking Set Interval .
Stop	Click Stop to halt system statistic polling.

40.3 VRRP Configuration

The following sections describe the different parts of the VRRP Configuration screen.

40.3.1 IP Interface Setup

Before configuring VRRP, first create an IP interface (or routing domain) in the **IP Setup** screen (see the [Section 6.5 on page 62](#) 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 288 IP Application > VRRP Configuration: IP Interface

VRRP Configuration Status

Index	Network	Authentication	Key
1	192.168.1.1/24	None	
2	192.168.2.1/24	None	

[Apply] [Cancel]

Active ☐

Name

Network

Virtual Router ID

Advertisement Interval

Preempt Mode ☒

Priority

Uplink Gateway

Response Ping ☐

Primary Virtual IP

Secondary Virtual IP

[Add] [Cancel] [Clear]

Index	Active	Name	Network	VRID	Primary VIP	Uplink Gateway	Priority	Delete

[Delete] [Cancel]

The following table describes the labels in this screen.

Table 187 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.

Table 187 IP Application > VRRP Configuration: IP Interface (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 discard all changes made in this table.

40.3.2 VRRP Parameters

This section describes the VRRP parameters.

40.3.2.1 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.

40.3.2.2 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.

40.3.2.3 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.

40.3.3 Configuring VRRP Parameters

After you set up an IP interface, configure the VRRP parameters in the **VRRP Configuration** screen.

Figure 289 IP Application > VRRP Configuration: VRRP Parameters

Active	☐
Name	name
Network	192.168.1.1/24
Virtual Router ID	1
Advertisement Interval	1
Preempt Mode	☒
Priority	100
Uplink Gateway	0.0.0.0
Response Ping	☐
Primary Virtual IP	0.0.0.0
Secondary Virtual IP	0.0.0.0

Add Cancel Clear

The following table describes the labels in this screen.

Table 188 IP Application > VRRP Configuration: VRRP Parameters

LABEL	DESCRIPTION
Active	Select this option to enable this VRRP entry.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
Network	Select an IP domain to which this VRRP entry applies.
Virtual Router ID	Select a virtual router number (1 to 7) for which this VRRP entry is created. You can configure up to seven virtual routers for one network.
Advertisement Interval	Specify the number of seconds between Hello message transmissions. The default is 1 .
Preempt Mode	Select this option to activate preempt mode.
Priority	Enter a number (between 1 and 254) to set the priority level. The bigger the number, the higher the priority. This field is 100 by default.
Uplink Gateway	Enter the IP address of the uplink gateway in dotted decimal notation. The Switch checks the link to the uplink gateway.
Response Ping	Select this option to have the Switch respond to a ping that is sent to the virtual IP address.
Primary Virtual IP	Enter the IP address of the primary virtual router in dotted decimal notation.
Secondary Virtual IP	This field is optional. Enter the IP address of a secondary virtual router in dotted decimal notation. This field is ignored when you enter 0.0.0.0 .
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to discard all changes made in this table.
Clear	Click Clear to set the above fields back to the factory defaults.

40.3.4 Viewing VRRP Summary

View the VRRP configuration summary at the bottom of the screen.

Figure 290 IP Application > 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	☐

Delete
Cancel

The following table describes the labels in this screen.

Table 189 IP Application > VRRP Configuration: Summary

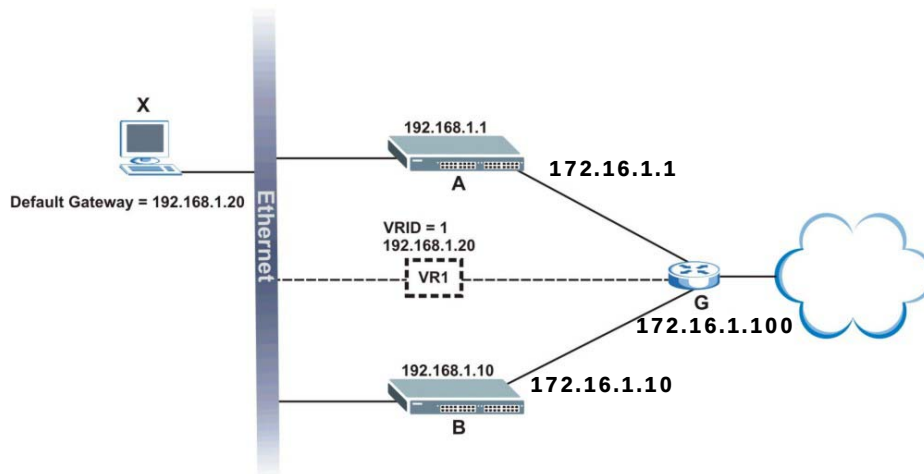
LABEL	DESCRIPTION
Index	This field displays the index number of an entry. Click an index number to change the settings.
Active	This field shows whether a VRRP entry is enabled (Yes) or disabled (No).
Name	This field displays a descriptive name of an entry.
Network	This field displays the IP address and 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.

40.4 VRRP Configuration Examples

The following sections show two VRRP configuration examples on the Switch.

40.4.1 One Subnet Network Example

The figure below shows a simple VRRP network with only one virtual router **VR1** (VRID =1) and two switches. The network is connected to the WAN via an uplink gateway **G** (172.16.1.100). The host computer **X** is set to use **VR1** as the default gateway.

Figure 291 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 292 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	172.16.1.100
Response Ping	☒
Primary Virtual IP	192.168.1.20
Secondary Virtual IP	0.0.0.0

EXAMPLE

Figure 293 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	172.16.1.100
Response Ping	☒
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 294 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 295 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

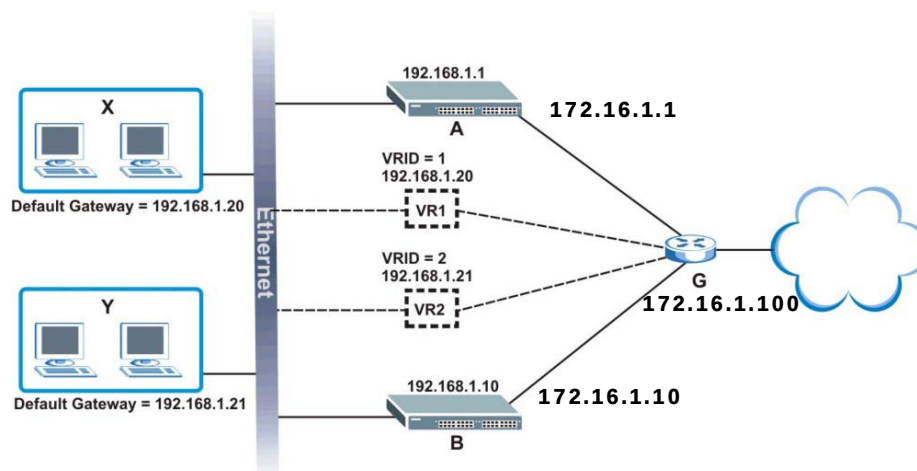
EXAMPLE

40.4.2 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 296 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 40.4.2 on page 391](#)). Configure the VRRP parameters on the switches as shown in the figures below.

Figure 297 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	172.16.1.100
Response Ping	☒
Primary Virtual IP	192.168.1.21
Secondary Virtual IP	0.0.0.0

EXAMPLE

Figure 298 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	172.16.1.100
Response Ping	☒
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 299 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 300 VRRP Example 2: VRRP Status on Switch B

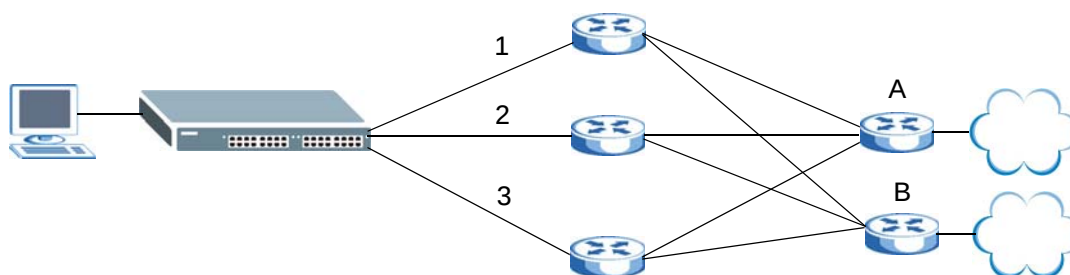
VRRP Status					Configuration
Index	Active	Network	VRID	VR Status	Uplink Status
1	Yes	192.168.1.10/24	2	Master	Alive
2	Yes	192.168.1.10/24	1	Backup	Alive

EXAMPLE

Load Sharing

41.1 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.

41.2 Configuring Load Sharing

Click **IP Application > Load Sharing** in the navigation panel to display the screen as shown next.

Figure 301 IP Application > Load Sharing

Active	☐
Criteria	src-dst-ip ▼
Aging Time	1200 seconds
Discover Time	3600 seconds
Maximum Paths	8

Apply Cancel

The following table describes the labels in this screen.

Table 190 IP Application > Load Sharing

LABEL	DESCRIPTION
Active	Select this option to enable Equal-Cost MultiPath (ECMP) routing on the Switch.
Criteria	Select the criteria the Switch uses to determine the routing path for a packet. Select src-ip to have the Switch use a hash algorithm to convert a packet's source IP address into a hash value which acts as an index to a route path. Select src-dst-ip to have the Switch use a hash algorithm to convert a packet's source and destination IP addresses into a hash value which acts as an index to a route path.
Aging Time	Specify the time interval (from 0 to 86400 in increments of 10) in seconds at which the Switch sends an ARP request to update a resolved next-hop's MAC address.
Discover Time	Specify the time interval (from 0 to 86400 in increments of 10) in seconds at which the Switch sends an ARP request to update an unresolved next-hop's MAC address.
Maximum Paths	Set the maximum number of paths for one ECMP (Equal-Cost MultiPath) route. The maximum number varies by Switch. A smaller number of maximum-paths means more ECMP routes are allowed and a larger number of maximum-paths means fewer ECMP routes are allowed. The number of paths for a static route for ECMP cannot be bigger than the maximum-paths value configured here. Throughput may be influenced while configuring ECMP maximum-paths.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

ARP Setup

42.1 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.

42.1.1 How ARP Works

When an incoming packet destined for a host device on a local area network arrives at the Switch, the Switch 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.

42.1.2 ARP Learning Mode

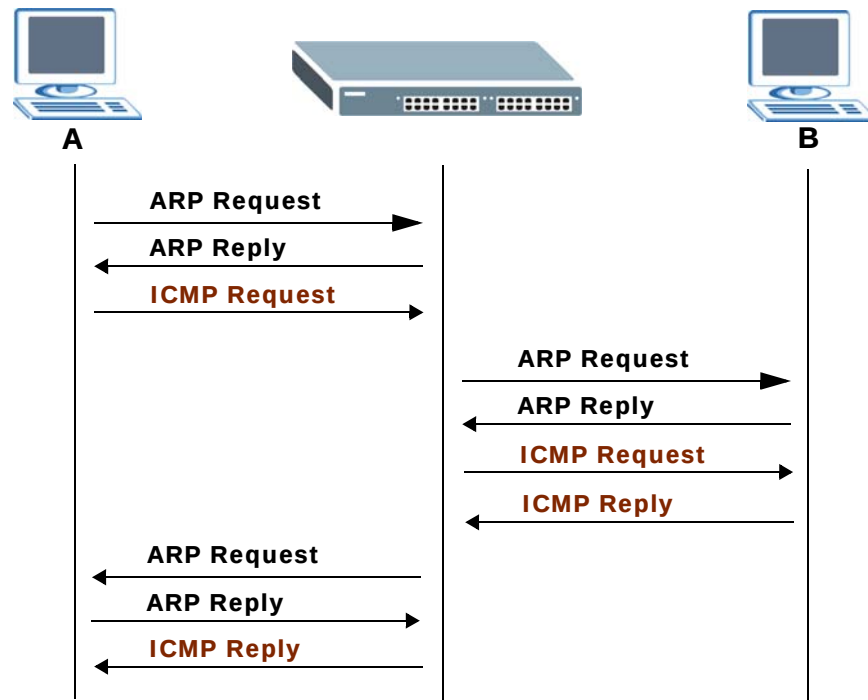
The Switch supports three ARP learning modes: ARP-Reply, Gratuitous-ARP, and ARP-Request.

42.1.2.1 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**.



42.1.2.2 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.

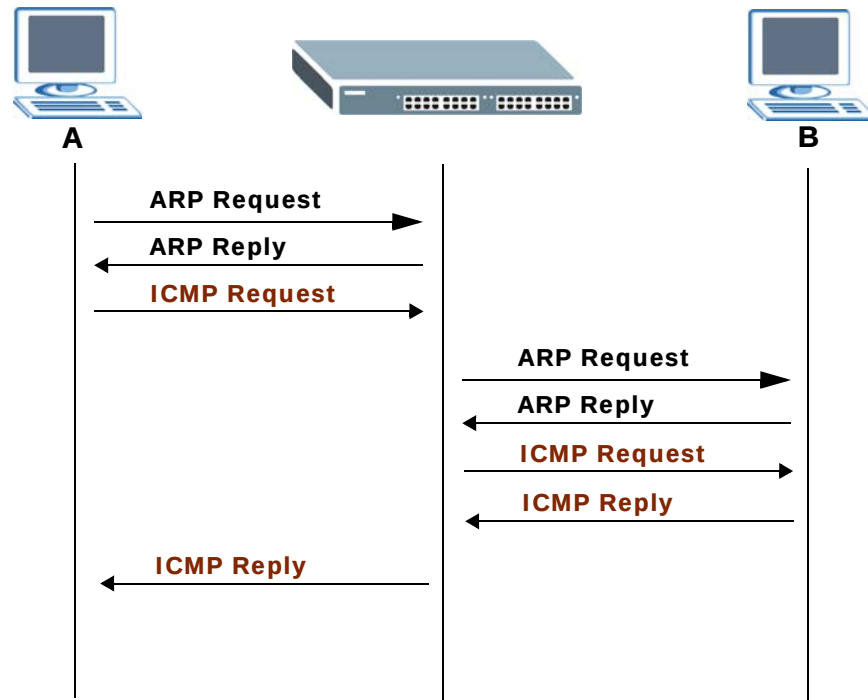
A device may send a gratuitous ARP packet to detect IP collisions. If a device restarts or its MAC address is changed, it can also use gratuitous ARP to inform other devices in the same network to update their ARP table with the new mapping information.

In Gratuitous-ARP learning mode, the Switch updates its ARP table with either an ARP reply or a gratuitous ARP request.

42.1.2.3 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.

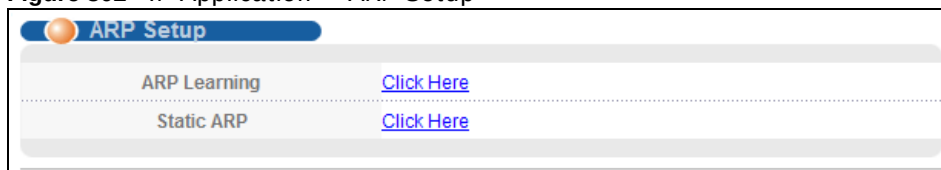
Therefore in the following example, the Switch can learn host **A**'s MAC address from the ARP request sent by host **A**. The Switch then forwards host **B**'s ICMP reply to host **A** right after getting host **B**'s MAC address and ICMP reply.



42.2 ARP Setup

Click **IP Application > ARP Setup** in the navigation panel to display the screen as shown. Click the link next to **ARP Learning** to open a screen where you can set the ARP learning mode for each port. Click the link next to **Static ARP** to open a screen where you can create static ARP entries on the Switch.

Figure 302 IP Application > ARP Setup



42.2.1 ARP Learning

Use this screen to configure each port's ARP learning mode. Click the link next to **ARP Learning** in the **IP Application > ARP Setup** screen to display the screen as shown next.

Figure 303 IP Application > ARP Setup > 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
12	ARP-Reply
13	ARP-Reply
14	ARP-Reply
15	ARP-Reply
16	ARP-Reply

Apply Cancel

The following table describes the labels in this screen.

Table 191 IP Application > ARP Setup > ARP Learning

LABEL	DESCRIPTION
Slot (Stacking mode)	This field appears only in stacking mode. Click the drop-down list to choose the slot number of the Switch in a stack.
Port	This field displays the port number. In stacking mode, the first number represents the slot and the second the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
ARP Learning Mode	Select the ARP learning mode the Switch uses on the port. Select ARP-Reply to have the Switch update the ARP table only with the ARP replies to the ARP requests sent by the Switch. Select Gratuitous-ARP to have the Switch update its ARP table with either an ARP reply or a gratuitous ARP request. Select ARP-Request to have the Switch update the ARP table with both ARP replies, gratuitous ARP requests and ARP requests.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

42.2.2 Static ARP

Use this screen to create static ARP entries that will display in the **Management > ARP Table** screen and will not age out. Click the link next to **Static ARP** in the **IP Application > ARP Setup** screen to display the screen as shown.

Figure 304 IP Application > ARP Setup > Static ARP

The following table describes the related labels in this screen.

Table 192 IP Application > ARP Setup > Static ARP

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
IP Address	Enter the IP address of a device connected to a Switch port with the corresponding MAC address below.
MAC Address	Enter the MAC address of the device with the corresponding IP address above.
VID	Enter the ID number of VLAN to which the device belongs.
Port	Enter the number of port to which the device connects. In stacking mode, the first number represents the slot and the second the port number.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to set the above fields back to the factory defaults.
Index	This field displays the index number of an entry. Click an index number to change the settings.
Active	This field displays Yes when the entry is activated and NO when it is deactivated.
Name	This field displays the descriptive name for this entry. This is for identification purposes only.

Table 192 IP Application > ARP Setup > Static ARP (continued)

LABEL	DESCRIPTION
IP Address	This is the IP address of a device connected to a Switch port with the corresponding MAC address below.
MAC Address	This is the MAC address of the device with the corresponding IP address above.
VID	This field displays the VLAN to which the device belongs.
Port	This field displays the port to which the device connects.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the Delete check boxes.

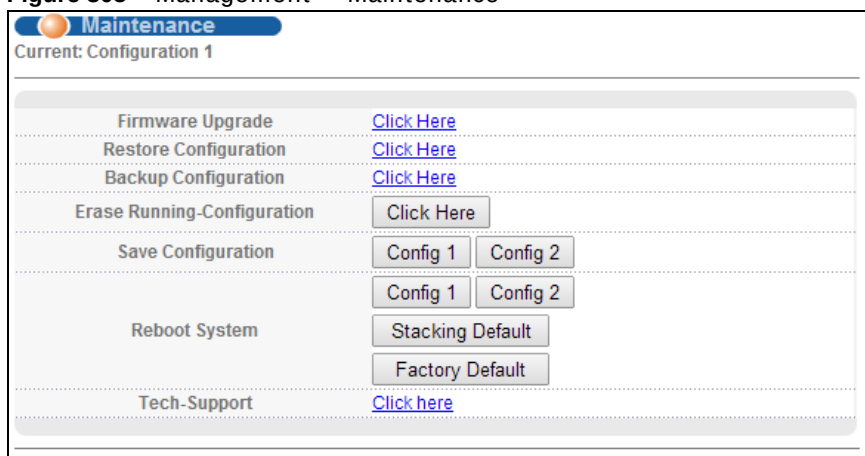
Maintenance

This chapter explains how to configure the maintenance screens that let you maintain the firmware and configuration files.

43.1 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 305 Management > Maintenance



The following table describes the labels in this screen.

Table 193 Management > Maintenance

LABEL	DESCRIPTION
Current	This field displays which configuration (Configuration 1 or Configuration 2) is currently operating on the Switch.
Firmware Upgrade	Click Click Here to go to the Firmware Upgrade screen.
Restore Configuration	Click Click Here to go to the Restore Configuration screen.
Backup Configuration	Click Click Here to go to the Backup Configuration screen.
Erase Running-Configuration	Click Click Here to reset the current configuration of the Switch. Note that this will not reset the configuration to the factory default settings.
Save Configuration	Click Config 1 to save the current configuration settings to Configuration 1 on the Switch. Click Config 2 to save the current configuration settings to Configuration 2 on the Switch.

Table 193 Management > Maintenance (continued)

LABEL	DESCRIPTION
Reboot System	Click Config 1 to reboot the system and load Configuration 1 on the Switch. Click Config 2 to reboot the system and load Configuration 2 on the Switch. Click Stacking Default to reboot the system and load stacking configurations on the Switch. Click Factory Default to reboot the system and load the factory default configuration on the Switch. Note: Make sure to click the Save button in any screen to save your settings to the current configuration on the Switch.
Tech-Support	Click Click Here to see the Tech-Support screen. You can set CPU and memory thresholds for log reports and download related log reports for issue analysis. Log reports include CPU history and utilization, crash and memory.

43.2 Firmware Upgrade

Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

The Switch supports dual firmware images, **Firmware 1** and **Firmware 2**. Use this screen to specify which image is updated when firmware is uploaded using the web configurator and to specify which image is loaded when the Switch starts up.

Click **Management > Maintenance > Firmware Upgrade** to view the screen as shown next.

Figure 306 Management > Maintenance > Firmware Upgrade (Standalone mode)

Name	Version
XGS3700-48HP	Running
	V4.20(AAGF.0)b4 08/12/2014
	Firmware 1
	V4.20(AAGF.0)b4 08/12/2014
	Firmware 2
	V4.10(AAGF.5)b1 06/05/2014

Current Boot Image: Firmware 1

Config Boot Image: Firmware 1

Apply Cancel

To upgrade the internal switch firmware, browse the location of the binary (.BIN) file and click Upgrade button.

Firmware: 1 File Path: Choose File No file chosen

Upgrade

Figure 307 Management > Maintenance > Firmware Upgrade (Stacking mode)

Firmware Upgrade			Maintenance	
Slot	Name	Status	Version	
1	XGS3700-48HP	active	Running	V4.20(AAGF.0)b4 08/12/2014
			Firmware 1	V4.20(AAGF.0)b4 08/12/2014
			Firmware 2	V4.20(AAGF.0) 01/06/2015
2	XGS3700-24	inactive	Running	
			Firmware 1	
			Firmware 2	
3		inactive	Running	
			Firmware 1	
			Firmware 2	
4		inactive	Running	
			Firmware 1	
			Firmware 2	
5		inactive	Running	
			Firmware 1	
			Firmware 2	
6		inactive	Running	
			Firmware 1	
			Firmware 2	
7		inactive	Running	
			Firmware 1	
			Firmware 2	
8		inactive	Running	
			Firmware 1	
			Firmware 2	
Current Boot Image Firmware 1 Config Boot Image Firmware 1 ▼ Apply Cancel				
To upgrade the internal switch firmware, browse the location of the binary (.BIN) file and click Upgrade button. All ▼ Firmware 1 ▼ File Path Choose File No file chosen Upgrade				

The top of firmware upgrade screen shows which firmware version is currently running on the Switch. Type the path and file name of the firmware file you wish to upload to the Switch in the **File Path** text box or click **Browse** to locate it. Firmware upgrades are only applied after a reboot. Click **Upgrade** to load the new firmware. Select the **Config Boot Image** drop-down list box if you want to reboot the Switch and click **Apply** to apply the new firmware immediately. Click **Upgrade** to load the new firmware.

After the firmware upgrade process is complete, see the **System Info** screen to verify your current firmware version number.

Table 194 Management > Maintenance> Firmware Upgrade

LABEL	DESCRIPTION
Name	This is the name of the Switch that you're configuring.
Version	The Switch has two firmware sets, Firmware 1 and Firmware 2, residing in flash. Running shows the version number (and model code) and MM/DD/YYYY creation date of the firmware currently in use on the Switch (Firmware 1 or Firmware 2). The firmware information is also displayed at System Information in Basic Settings. Firmware 1 shows its version number (and model code) and MM/DD/YYYY creation date. Firmware 2 shows its version number (and model code) and MM/DD/YYYY creation date.
Current Boot Image	This displays which firmware is currently in use on the Switch (Firmware 1 or Firmware 2).
Config Boot Image	Select which firmware (Firmware 1 or Firmware 2) should load after rebooting. Click Apply and reboot the Switch to see changes including in the Current Boot Image field.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Firmware	Choose the Switch(es) to upload firmware to and then choose to upload the new firmware to (Firmware) 1 or (Firmware) 2 .
Choose File	Click this and locate the path and file name of the firmware file you wish to upload to the Switch.
Upgrade	Click Upgrade to load the new firmware. Firmware upgrades are only applied after a reboot. To reboot, go to Management > Maintenance > Reboot System . You may also click Config 1 or Config 2 to select which configuration file to upload after reboot.

43.3 Restore a Configuration File

Restore a previously saved configuration from your computer to the Switch using the **Restore Configuration** screen.

Figure 308 Management > Maintenance > Restore Configuration

Restore Configuration Maintenance

To restore the device's configuration from a file, browse the location of the configuration file and click Restore button.

File Path No file chosen

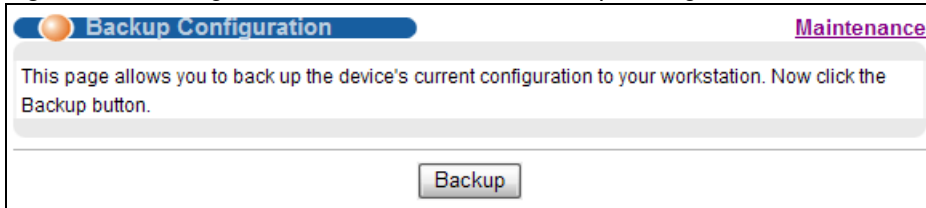
Click Choose File button to uploadType the path and file name of the configuration file you wish to restore in the **File Path** text box or click **Browse** to display the **Choose File** screen from which you can locate itSwitch. After you have specified the file, click **Restore**. "config" is the name of the configuration file on the Switch, so your backup configuration file is automatically renamed when you restore using this screen.

43.4 Backup a Configuration File

Backing up your Switch configurations allows you to create various “snapshots” of your device from which you may restore at a later date.

Back up your current Switch configuration to a computer using the **Backup Configuration** screen.

Figure 309 Management > Maintenance > Backup Configuration



Follow the steps below to back up the current Switch configuration to your computer in this screen.

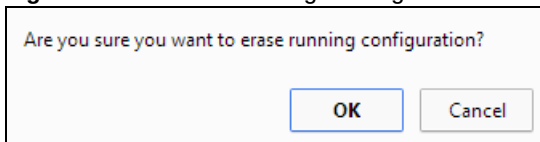
- 1 Click **Backup**.
- 2 Click **Save** to display the **Save As** screen.
- 3 Choose a location to save the file on your computer from the **Save in** drop-down list box and type a descriptive name for it in the **File name** list box. Click **Save** to save the configuration file to your computer.

43.5 Erase Running-Configuration

Follow the steps below to clear current configuration on the Switch. Note that this will NOT reset the Switch back to its factory defaults. For example, if your Switch is set to stacking mode and you click erase running-configuration, after the the Switch restarts, it will remain in stacking mode. If you want to change the Switch to its factory default mode, click Factory Default button in Reboot System. See (Section 43.7.1 on page 406).

- 1 In the **Maintenance** screen, click the **Click Here** button next to **Erase Running-Configuration** to clear all Switch configuration information you configured on the Switch..
- 2 Click **OK** to reset all Switch configurations.

Figure 310 Erase Running-Configuration: Confirmation



- 3 In the web configurator, click the **Save** button in the top of the screen to make the changes take effect. If you want to access the Switch web configurator again, you may need to change the IP address of your computer to be in the same subnet as that of the default Switch IP address (192.168.1.1).

43.6 Save Configuration

Click **Config 1** to save the current configuration settings permanently to configuration one on the Switch.

Click **Config 2** to save the current configuration settings to configuration two on the Switch.

Alternatively, click **Save** on the top right-hand corner in any screen to save the configuration changes to the current configuration.

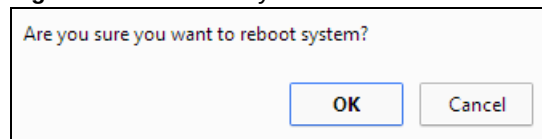
Note: Clicking the **Apply** or **Add** button does NOT save the changes permanently. All unsaved changes are erased after you reboot the Switch.

43.7 Reboot System

Reboot System allows you to restart the Switch without physically turning the power off. It also allows you to load configuration one (**Config 1**), configuration two (**Config 2**), stacking default, or factory default when you reboot. Follow the steps below to reboot the Switch.

- 1 In the **Maintenance** screen, click the **Config 1** button next to **Reboot System** to reboot and load configuration one. The following screen displays.

Figure 311 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.

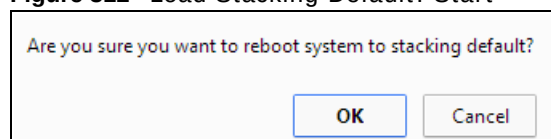
Click **Config 2** and follow steps 1 to 2 to reboot and load configuration two on the Switch.

43.7.1 Load Stacking Default

Follow the steps below to reset the Switch back to the stacking defaults. The master Switch login information will not be reset.

- 1 In the click the **Stacking Default** button to clear all Switch configuration information you configured and return to the stacking defaults.
- 2 Click **OK** to reset all Switch configurations to the stacking defaults.

Figure 312 Load Stacking Default: Start



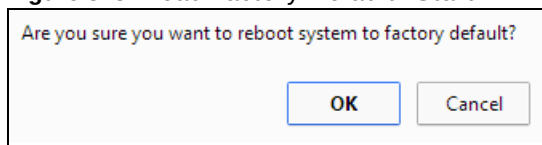
- 3 In the web configurator, click the **Save** button in the top of the screen to make the changes take effect. If you want to access the Switch web configurator again, you may need to change the IP address of your computer to be in the same subnet as that of the default Switch IP address (192.168.1.1).

43.7.2 Load Factory Default

Follow the steps below to reset the Switch back to the factory defaults.

- 1 In the click the **Factory Default** button to clear all Switch configuration information you configured and return to the factory defaults.
- 2 Click **OK** to reset all Switch configurations to the factory defaults.

Figure 313 Load Factory Default: Start



- 3 In the web configurator, click the **Save** button in the top of the screen to make the changes take effect. If you want to access the Switch web configurator again, you may need to change the IP address of your computer to be in the same subnet as that of the default Switch IP address (192.168.1.1).

43.8 Tech-Support

The Tech-Support feature is a log enhancement tool that logs useful information such as CPU utilization history, memory and Mbuf (Memory Buffer) log and crash reports for issue analysis by customer support should you have difficulty with your Switch. The Tech Support menu eases your effort in obtaining reports and it is also available in CLI command by typing "Show tech-support" command.

Click **Menu > Management > Maintenance > Tech-Support** to see the following screen.

Figure 314 Management > Maintenance > Tech-Support

Tech-Support	
CPU	threshold 80 keep 5 seconds
Mbuf	threshold 50 %
Apply Cancel	
All	Download
Crash	Download
CPU history	Download
Memory section	Download
Mbuf	Download
ROM	Download

You may need WordPad or similar software to see the log report correctly. The table below describes the fields in the above screen.

Table 195 Management > Maintenance > Tech-Support

LABEL	DESCRIPTION
CPU	Type a number ranging from 50 to 100 in the CPU threshold box, and type another number ranging from 5 to 60 in the seconds box then click Apply. For example, 80 for CPU threshold and 5 for seconds means a log will be created when CPU utilization reaches over 80% and lasts for 5 seconds. The log report holds 7 days of CPU log data and is stored in volatile memory (RAM). The data is lost if the Switch is turned off or in event of power outage. After 7 days, the logs wrap around and new ones replace the earliest ones. The higher the CPU threshold number, the fewer logs will be created, and the less data technical support will have to analyze and vice versa.
Mbuf	Type a number ranging from 50 to 100 in the Mbuf (Memory Buffer) threshold box. The Mbuf log report is stored in flash (permanent) memory. For example, Mbuf 50 means a log will be created when the Mbuf utilization is over 50%. The higher the Mbuf threshold number, the fewer logs will be created, and the less data technical support will have to analyze and vice versa.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
All	Click Download to see all the log report and system status. This log report is stored in flash memory. If the All log report is too large, you can download the log reports separately below.
Crash	Click Download to see the crash log report. The log will include information of the last crash and is stored in flash memory.
CPU history	Click Download to see the CPU history log report. The 7-days log is stored in RAM and you will need to save it, otherwise it will be lost in event of Switch shutdown or power outage.

Table 195 Management > Maintenance > Tech-Support

LABEL	DESCRIPTION
Memory Section	Click Download to see the memory section log report. This log report is stored in flash memory.
Mbuf	Click Download to see the Mbuf log report. The log includes Mbuf over threshold information. This log report is stored in flash memory.
ROM	Click Download to see the Read Only Memory (ROM) log report. This report is stored in flash memory.

43.9 FTP Command Line

This section shows some examples of uploading to or downloading files from the Switch using FTP commands. First, understand the filename conventions.

43.9.1 Filename Conventions

The configuration file (also known as the romfile or ROM) contains the factory default settings in the screens such as password, Switch setup, IP Setup, and so on. Once you have customized the Switch's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (ZyXEL Network Operating System, sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension.

Table 196 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	config	.cfg	This is the configuration (config) filename on the Switch. Uploading the config file replaces the specified configuration file system, including your Switch configurations, system-related data (including the default password), the error log and the trace log.
Firmware	ras-0 ras-1	*.bin	This is the generic name for the ZyNOS firmware on the Switch. ras-0 is image 1; ras-1 is image 2.

You can store up to two images, or firmware files of the same device model, on the Switch. Only one image is used at a time.

- Run the `boot image <1|2>` command to specify which image is updated when firmware is loaded using the web configurator and to specify which image is loaded when the Switch starts up.
- You can also use FTP commands to upload firmware to any image.

The Switch supports dual firmware images, ras-0 and ras-1. You can switch from one to the other by using the `boot image <index>` command, where <index> is 1 (ras-0) or 2 (ras-1). See the CLI Reference Guide for more information about using commands. The system does not reboot after it switches from one image to the other.

43.9.1.1 Example FTP Commands

```
ftp> put firmware.bin ras-0
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the Switch.

```
ftp> get config config.cfg
```

This is a sample FTP session saving the current configuration to a file called "config.cfg" on your computer.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the Switch only recognizes "config", "ras-0", and "ras-1". Be sure you keep unaltered copies of both files for later use.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

43.9.2 FTP Command Line Procedure

- 1 Launch the FTP client on your computer.
- 2 Enter open, followed by a space and the IP address of your Switch.
- 3 Press [ENTER] when prompted for a username (the default is "admin").
- 4 Enter your password as requested (the default is "1234").
- 5 Enter bin to set transfer mode to binary.
- 6 Use put to transfer files from the computer to the Switch, for example, put firmware.bin ras-0 transfers the firmware on your computer (firmware.bin) to the Switch and renames it to "ras-0". Similarly, put config.cfg config transfers the configuration file on your computer (config.cfg) to the Switch and renames it to "config". Likewise get config config.cfg transfers the configuration file on the Switch to your computer and renames it to "config.cfg". See [Table 196 on page 409](#) for more information on filename conventions.
- 7 Enter quit to exit the ftp prompt.

43.9.3 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 197 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.

Table 197 General Commands for GUI-based FTP Clients (continued)

COMMAND	DESCRIPTION
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

43.9.4 FTP Restrictions

FTP will not work when:

- FTP service is disabled in the **Service Access Control** screen.
- The IP address(es) in the **Remote Management** screen does not match the client IP address. If it does not match, the Switch will disconnect the FTP session immediately.

Access Control

This chapter describes how to control access to the Switch.

44.1 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 198 Access Control Overview

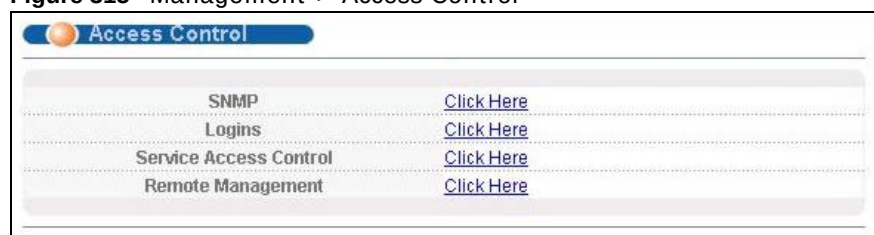
Console Port	SSH	Telnet	FTP	Web	SNMP
One session	Share up to nine sessions		One session	Up to five accounts	No limit

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.

44.2 The Access Control Main Screen

Click **Management > Access Control** in the navigation panel to display the main screen as shown.

Figure 315 Management > Access Control

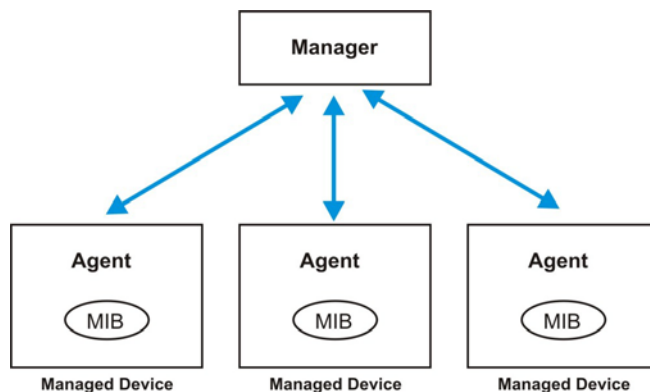


44.3 About SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol used to manage and monitor TCP/IP-based devices. SNMP is used to exchange management information between the network management system (NMS) and a network element (NE). A manager station can manage and monitor the Switch through the network via SNMP version 1 (SNMPv1), SNMP version 2c or

SNMP version 3. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 316 SNMP Management Model



An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed Switch (the Switch). An agent translates the local management information from the managed Switch into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables/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 199 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.

44.3.1 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.

44.3.2 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

44.3.3 SNMP Traps

The Switch sends traps to an SNMP manager when an event occurs. The following tables outline the SNMP traps by category.

An OID (Object ID) that begins with “**1.3.6.1.4.1.890.1.15**” is defined in private MIBs. Otherwise, it is a standard MIB OID.

Table 200 SNMP System Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
coldstart	coldStart	1.3.6.1.6.3.1.1.5.1	This trap is sent when the Switch is turned on.
warmstart	warmStart	1.3.6.1.6.3.1.1.5.2	This trap is sent when the Switch restarts.
fanspeed	zyHwMonitorFanSpeedOutOfRange	1.3.6.1.4.1.890.1.15.3.26.2.1	This trap is sent when the fan speed goes above or below the normal operating range.
poe (For PoE models only)	zyPoePowerPortOverload	1.3.6.1.4.1.890.1.15.3.59.4.1	This trap is sent when the port is turned off to supply power due to overloading.
	zyPoePowerPortShortCircuit	1.3.6.1.4.1.890.1.15.3.59.4.2	This trap is sent when the port is turned off to supply power due to short circuit.
	zyPoePowerPortOverSystemBudget	1.3.6.1.4.1.890.1.15.3.59.4.3	This trap is sent when the port is turned off to supply power because the requested power exceeds the total PoE power budget on the Switch.
temperature	zyHwMonitorTemperatureOutOfRange	1.3.6.1.4.1.890.1.15.3.26.2.2	This trap is sent when the temperature goes above or below the normal operating range.
voltage	zyHwMonitorPowerSupplyVoltageOutOfRange	1.3.6.1.4.1.890.1.15.3.26.2.3	This trap is sent when the voltage goes above or below the normal operating range.

Table 200 SNMP System Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
reset	zySysMgmtUncontrolledSystemReset	1.3.6.1.4.1.890.1.15.3.49.2.1	This trap is sent when the Switch automatically resets.
	zySysMgmtControlledSystemReset	1.3.6.1.4.1.890.1.15.3.49.2.2	This trap is sent when the Switch resets by an administrator through a management interface.
	zySysMgmtBootImageInconsistence	1.3.6.1.4.1.890.1.15.3.49.2.3	This trap is sent when the index number of image which is loaded when the Switch starts up is different from what is specified via the CLI.
	RebootEvent	1.3.6.1.4.1.890.1.5.1.1.2	This trap is sent when the Switch reboots by an administrator through a management interface.
timesync	zyDateTimeTrapTimeServerNotReachable	1.3.6.1.4.1.890.1.15.3.82.3.1	This trap is sent when the Switch's date and time is not manually entered or the specified time server is not reachable.
intrusionlock	zyPortIntrusionLock	1.3.6.1.4.1.890.1.15.3.61.3.2	This trap is sent when intrusion lock occurs on a port.
loopguard	zyLoopGuardLoopDetect	1.3.6.1.4.1.890.1.15.3.45.2.1	This trap is sent when loopguard shuts down a port.
errdisable	zyErrdisableDetect	1.3.6.1.4.1.890.1.15.3.24.4.1	This trap is sent when an error is detected on a port, such as a loop occurs or the rate limit for specific control packets is exceeded.
	zyErrdisableRecovery	1.3.6.1.4.1.890.1.15.3.24.4.2	This trap is sent when the Switch ceases the action taken on a port, such as shutting down the port or discarding packets on the port, after the specified recovery interval.
dyinggasp	zyHwMonitorDyingGasp	1.3.6.1.4.1.890.1.15.3.26.2.5	The trap is sent when the device power goes below the normal value.

Table 201 SNMP Stacking Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
Channel	zyStackingChannelUp	1.3.6.1.4.1.890.1.15.3.97.4.1	stacking channel up
	zyStackingChannelDown	1.3.6.1.4.1.890.1.15.3.97.4.2	stacking channel down
Slot	zyStackingSlotAttach	1.3.6.1.4.1.890.1.15.3.97.4.3	stacking slot attached success
	zyStackingSlotDetach	1.3.6.1.4.1.890.1.15.3.97.4.4	stacking slot detached
Master	zyStackingNewMaster	1.3.6.1.4.1.890.1.15.3.97.4.5	backup takeover as master
Upgrade Firmware	zyStackingUpgradeFirmwareFail	1.3.6.1.4.1.890.1.15.3.97.4.6	Upgrade Firmware fail with correspond slot ID.

Table 201 SNMP Stacking Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
Backup	zyStackingNewBackup	1.3.6.1.4.1.890.1.15.3.9 7.4.7	New Backup with correspond slot ID.
	zyStackingBackupTakeover	1.3.6.1.4.1.890.1.15.3.9 7.4.8	Replaced master with correspond slot ID.
Master	zyStackingNewMasterFromTakeover	1.3.6.1.4.1.890.1.15.3.9 7.4.9	New master from taking over with correspond slot ID.
Fail	zyStackingSyncConfFail	1.3.6.1.4.1.890.1.15.3.9 7.4.10	Sync. configuration fail with correspond slot ID.
	zyStackingSysRestoreConfFail	1.3.6.1.4.1.890.1.15.3.9 7.4.11	Stacking backup takeover restore configuration fail.
	zyStackingSlotInitFail	1.3.6.1.4.1.890.1.15.3.9 7.4.12	Stacking Slot init fail.
Change	zyStackingSlotChangeIndex	1.3.6.1.4.1.890.1.15.3.9 7.4.13	Stacking change slot index.
	zyStackingPriorityChange	1.3.6.1.4.1.890.1.15.3.9 7.4.14	Stacking priority change.
	zyStackingTopologyChange	1.3.6.1.4.1.890.1.15.3.9 7.4.15	Stacking topology change.

Table 202 SNMP InterfaceTraps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
linkup	linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
linkdown	linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
autonegotiation	zyPortAutonegotiationFailed	1.3.6.1.4.1.890.1.15.3.61.3.1	This trap is sent when an Ethernet interface fails to auto-negotiate with the peer Ethernet interface.
lldp	lldpRemTablesChange	1.0.8802.1.1.2.0.0.1	The trap is sent when entries in the remote database have any updates. Link Layer Discovery Protocol (LLDP), defined as IEEE 802.1ab, enables LAN devices that support LLDP to exchange their configured settings. This helps eliminate configuration mismatch issues.

Table 202 SNMP InterfaceTraps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
transceiver-ddm	zyTransceiverDdmiTemperatureOutOfRange	1.3.6.1.4.1.890.1.15.3.84.3.1	This trap is sent when the transceiver temperature is above or below the normal operating range.
	zyTransceiverDdmiTxPowerOutOfRange	1.3.6.1.4.1.890.1.15.3.84.3.2	This trap is sent when the transmitted optical power is above or below the normal operating range.
	zyTransceiverDdmiRxPowerOutOfRange	1.3.6.1.4.1.890.1.15.3.84.3.3	This trap is sent when the received optical power is above or below the normal operating range.
	zyTransceiverDdmiVoltageOutOfRange	1.3.6.1.4.1.890.1.15.3.84.3.4	This trap is sent when the transceiver supply voltage is above or below the normal operating range.
	zyTransceiverDdmiTxBiasOutOfRange	1.3.6.1.4.1.890.1.15.3.84.3.5	This trap is sent when the transmitter laser bias current is above or below the normal operating range.

Table 203 AAA Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
authentication	authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when authentication fails due to incorrect user name and/or password.
	zyAaaAuthenticationFailure	1.3.6.1.4.1.890.1.15.3.8.3.1	This trap is sent when authentication fails due to incorrect user name and/or password.
	zyRadiusServerAuthenticationServerNotReachable	1.3.6.1.4.1.890.1.15.3.71.2.1	This trap is sent when there is no response message from the RADIUS authentication server.
	zyTacacsServerAuthenticationServerUnreachable	1.3.6.1.4.1.890.1.15.3.83.2.1	This trap is sent when there is no response message from the TACACS+ authentication server.
authorization	zyAaaAuthorizationFailure	1.3.6.1.4.1.890.1.15.3.8.3.2	This trap is sent when management connection authorization failed.
accounting	zyRadiusServerAccountingServerNotReachable	1.3.6.1.4.1.890.1.15.3.71.2.2	This trap is sent when there is no response message from the RADIUS accounting server.
	zyTacacsServerAccountingServerUnreachable	1.3.6.1.4.1.890.1.15.3.83.2.2	This trap is sent when there is no response message from the TACACS+ accounting server.

Table 204 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 205 SNMP Switch Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
stp	STPNewRoot	1.3.6.1.2.1.17.0.1	This trap is sent when the STP root switch changes.
	zyMrstpNewRoot	1.3.6.1.4.1.890.1.15.3.52.3.1	This trap is sent when the MRSTP root switch changes.
	zyMstpNewRoot	1.3.6.1.4.1.890.1.15.3.53.3.1	This trap is sent when the MSTP root switch changes.
	STPTopologyChange	1.3.6.1.2.1.17.0.2	This trap is sent when the STP topology changes.
	zyMrstpTopologyChange	1.3.6.1.4.1.890.1.15.3.52.3.2	This trap is sent when the MRSTP topology changes.
	zyMstpTopologyChange	1.3.6.1.4.1.890.1.15.3.53.3.2	This trap is sent when the MSTP root switch changes.
mactable	zyMacForwardingTableFull	1.3.6.1.4.1.890.1.15.3.48.2.1	This trap is sent when more than 99% of the MAC table is used.
rmon	RmonRisingAlarm	1.3.6.1.2.1.16.0.1	This trap is sent when a variable goes over the RMON "rising" threshold.
	RmonFallingAlarm	1.3.6.1.2.1.16.0.2	This trap is sent when the variable falls below the RMON "falling" threshold.
cfm	dot1agCfmFaultAlarm	1.3.111.2.802.1.1.8.0.1	The trap is sent when the Switch detects a connectivity fault.

44.3.4 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 317 Management > Access Control > SNMP

SNMP [Access Control](#) [Trap Group](#) [User](#)

General Setting

Version	v2c
Get Community	public
Set Community	public
Trap Community	public

Trap Destination

Version	IP	Port	Username
v2c	0.0.0.0	162	
v2c	0.0.0.0	162	
v2c	0.0.0.0	162	
v2c	0.0.0.0	162	

Apply Cancel

The following table describes the labels in this screen.

Table 206 Management > Access Control > SNMP

LABEL	DESCRIPTION
General Setting	Use this section to specify the SNMP version and community (password) values.
Version	Select the SNMP version for the Switch. The SNMP version on the Switch must match the version on the SNMP manager. Choose SNMP version 2c (v2c), SNMP version 3 (v3) or both (v3v2c). Note: SNMP version 2c is backwards compatible with SNMP version 1.
Get Community	Enter the Get Community string, which is the password for the incoming Get- and GetNext- requests from the management station. The Get Community string is only used by SNMP managers using SNMP version 2c or lower.
Set Community	Enter the Set Community string, which is the password for the incoming Set- requests from the management station. The Set Community string is only used by SNMP managers using SNMP version 2c or lower.
Trap Community	Enter the Trap Community string, which is the password sent with each trap to the SNMP manager. The Trap Community string is only used by SNMP managers using SNMP version 2c or lower.
Trap Destination	Use this section to configure where to send SNMP traps from the Switch.
Version	Specify the version of the SNMP trap messages.
IP	Enter the IP addresses of up to four managers to send your SNMP traps to.
Port	Enter the port number upon which the manager listens for SNMP traps.
Username	Enter the username to be sent to the SNMP manager along with the SNMP v3 trap. Note: This username must match an existing account on the Switch (configured in the Management > Access Control > SNMP > User screen).

Table 206 Management > Access Control > SNMP (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.

44.3.5 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 318 Management > Access Control > SNMP > Trap Group

The following table describes the labels in this screen.

Table 207 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 44.3.3 on page 414 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.

44.3.6 Enabling/Disabling Sending of SNMP Traps on a Port

From the **SNMP > Trap Group** screen, click **Port** to view the screen as shown. Use this screen to set whether a trap received on the port(s) would be sent to the SNMP manager.

Figure 319 Management > Access Control > SNMP > Trap Group > Port (Standalone mode)

Option: intrusionlock ▼

Port	Active
*	☐
1	☒
2	☒
3	☒
4	☒
5	☒
6	☒
7	☒
8	☒
9	☒
10	☒
11	☒
12	☒
13	☒
14	☒
15	☒

Apply Cancel

Figure 320 Management > Access Control > SNMP > Trap Group > Port (Stacking mode)

Option: intrusionlock ▼

SLOT 1 ▼

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

Apply Cancel

The following table describes the labels in this screen.

Table 208 Management > Access Control > SNMP > Trap Group > Port

LABEL	DESCRIPTION
Option	Select the trap type you want to configure here.
Slot	Select the slot number that represents the Switch in a stack.
Port	This field displays a port number. In stacking mode, the first number represents the slot and the second the port number.
1/*	Settings in this row apply to all ports for the Switch represented by the slot ID (in stacking mode). Use this row only if you want to make some of the settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable the sending of SNMP traps on this port. The Switch sends the related traps received on this port to the SNMP manager. Clear this check box to disable the sending of SNMP traps on this port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

44.3.7 Configuring SNMP User

From the **SNMP** screen, click **User** to view the screen as shown. Use the **User** screen to create SNMP users for authentication with managers using SNMP v3 and associate them to SNMP groups. An SNMP user is an SNMP manager.

Figure 321 Management > Access Control > SNMP > User

User Information **SNMP Setting**

Username:

Security Level:

Authentication: Password:

Privacy: Password:

Group:

Add Cancel Clear

Index	Username	SecurityLevel	Authentication	Privacy	Group	Delete
1	test	noauth	MD5	DES	readwrite	☐

Delete Cancel

The following table describes the labels in this screen.

Table 209 Management > Access Control > SNMP > User

LABEL	DESCRIPTION
User Information	Note: Use the username and password of the login accounts you specify in this screen to create accounts on the SNMP v3 manager.
Username	Specify the username of a login account on the Switch.
Security Level	Select whether you want to implement authentication and/or encryption for SNMP communication from this user. Choose: • noauth - to use the username as the password string to send to the SNMP manager. This is equivalent to the Get, Set and Trap Community in SNMP v2c. This is the lowest security level. • auth - to implement an authentication algorithm for SNMP messages sent by this user. • priv - to implement authentication and encryption for SNMP messages sent by this user. This is the highest security level. Note: The settings on the SNMP manager must be set at the same security level or higher than the security level settings on the Switch.
Authentication	Select an authentication algorithm. MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. SHA authentication is generally considered stronger than MD5, but is slower.
Password	Enter the password of up to 32 ASCII characters for SNMP user authentication.
Privacy	Specify the encryption method for SNMP communication from this user. You can choose one of the following: • DES - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data. • AES - Advanced Encryption Standard is another method for data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data.
Password	Enter the password of up to 32 ASCII characters for encrypting SNMP packets.
Group	SNMP v3 adopts the concept of View-based Access Control Model (VACM) group. SNMP managers in one group are assigned common access rights to MIBs. Specify in which SNMP group this user is. admin - Members of this group can perform all types of system configuration, including the management of administrator accounts. readwrite - Members of this group have read and write rights, meaning that the user can create and edit the MIBs on the Switch, except the user account and AAA configuration. readonly - Members of this group have read rights only, meaning the user can collect information from the Switch.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Clear	Click Clear to reset the fields to the factory defaults.
Index	This is a read-only number identifying a login account on the Switch. Click on an index number to view more details and edit an existing account.
Username	This field displays the username of a login account on the Switch.
Security Level	This field displays whether you want to implement authentication and/or encryption for SNMP communication with this user.
Authentication	This field displays the authentication algorithm used for SNMP communication with this user.

Table 209 Management > Access Control > SNMP > User (continued)

LABEL	DESCRIPTION
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.

44.4 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 322 Management > Access Control > Logins

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	Privilege
1				
2				
3				
4				

The following table describes the labels in this screen.

Table 210 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
Edit Logins	You may configure passwords for up to four users. These users have read-only access. You can give users higher privileges via the CLI. For more information on assigning privileges see the Ethernet Switch CLI Reference Guide.
User Name	Set a user name (up to 32 ASCII characters long).
Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
Privilege	Type the privilege level for this user. At the time of writing, users may have a privilege level of 0, 3, 13, or 14 representing different configuration rights as shown below. • 0 - Display basic system information. • 3 - Display configuration or status. • 13 - Configure features except for login accounts, SNMP user accounts, the authentication method sequence and authorization settings, multiple logins, administrator and enable passwords, and configuration information display. • 14 - Configure login accounts, SNMP user accounts, the authentication method sequence and authorization settings, multiple logins, and administrator and enable passwords, and display configuration information. Users can run command lines if the session's privilege level is greater than or equal to the command's privilege level. The session privilege initially comes from the privilege of the login account. For example, if the user has a privilege of 5, he/she can run commands that requires privilege level of 5 or less but not more.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

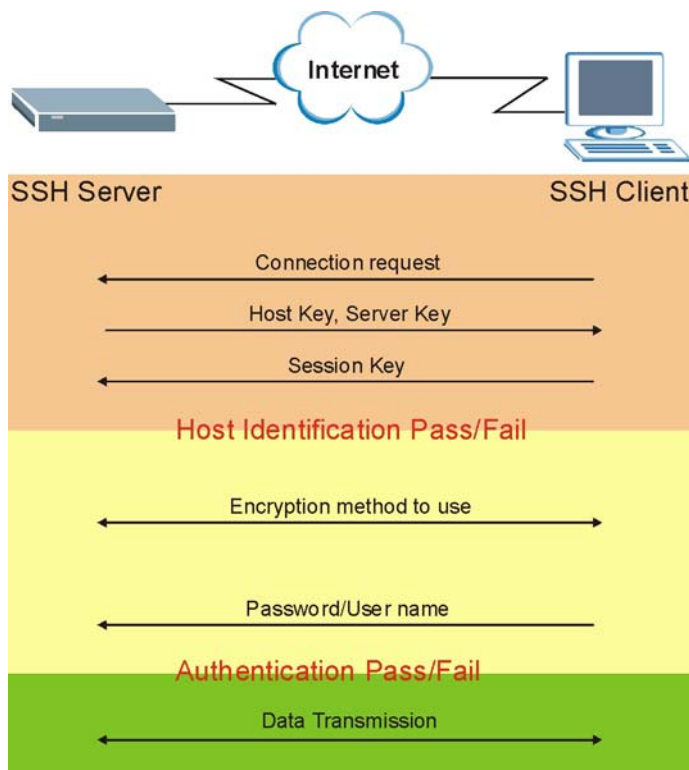
44.5 SSH Overview

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 323 SSH Communication Example

44.6 How SSH works

The following table summarizes how a secure connection is established between two remote hosts.

Figure 324 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.

44.7 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.

44.7.1 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.

44.8 Introduction to HTTPS

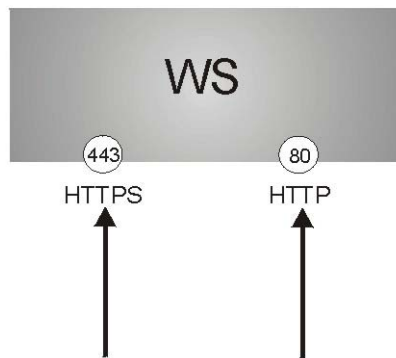
HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the 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 325 HTTPS Implementation

Note: If you disable **HTTP** in the **Service Access Control** screen, then the Switch blocks all HTTP connection attempts.

44.9 HTTPS Example

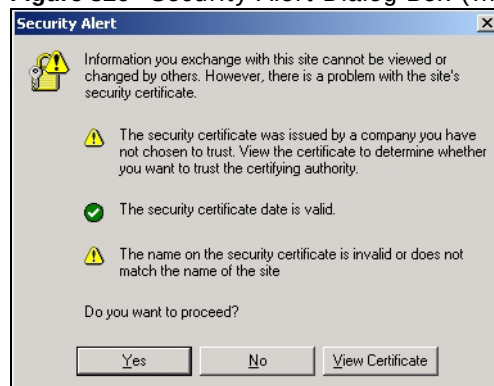
If you haven't changed the default HTTPS port on the Switch, then in your browser enter "https:// Switch IP Address/" as the web site address where "Switch IP Address" is the IP address or domain name of the Switch you wish to access.

44.9.1 Internet Explorer Warning Messages

44.9.1.1 Internet Explorer 6

When you attempt to access the Switch HTTPS server, a Windows dialog box pops up asking if you trust the server certificate.

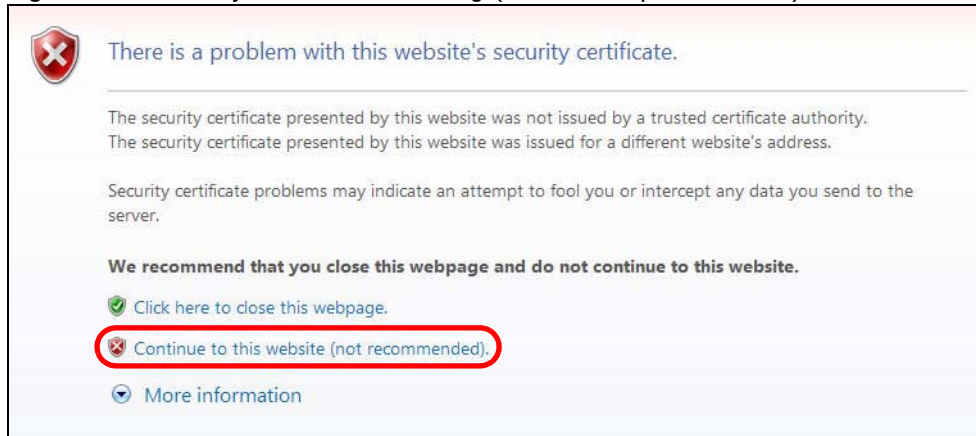
You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the web configurator login screen; if you select **No**, then web configurator access is blocked.

Figure 326 Security Alert Dialog Box (Internet Explorer 6)

44.9.1.2 Internet Explorer 7 or 8

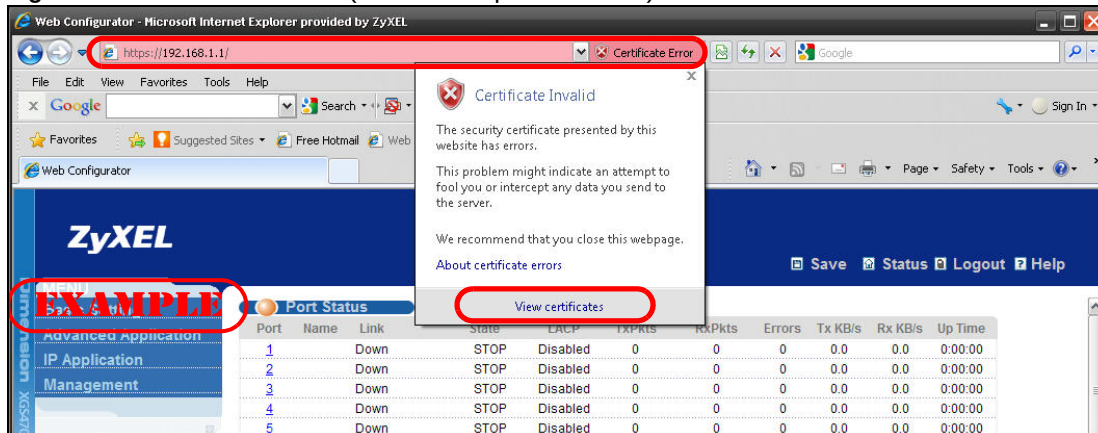
When you attempt to access the Switch HTTPS server, a screen with the message "There is a problem with this website's security certificate." may display. If that is the case, click **Continue to this website (not recommended)** to proceed to the web configurator login screen.

Figure 327 Security Certificate Warning (Internet Explorer 7 or 8)



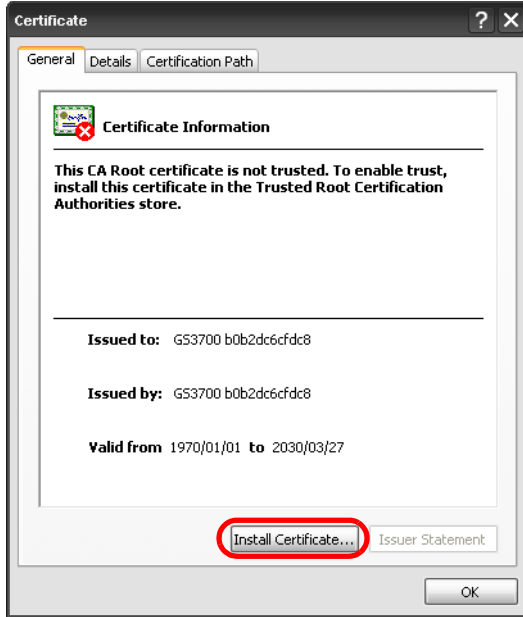
After you log in, you will see the red address bar with the message **Certificate Error**. Click on **Certificate Error** next to the address bar and click **View certificates**.

Figure 328 Certificate Error (Internet Explorer 7 or 8)



Click **Install Certificate...** and follow the on-screen instructions to install the certificate in your browser.

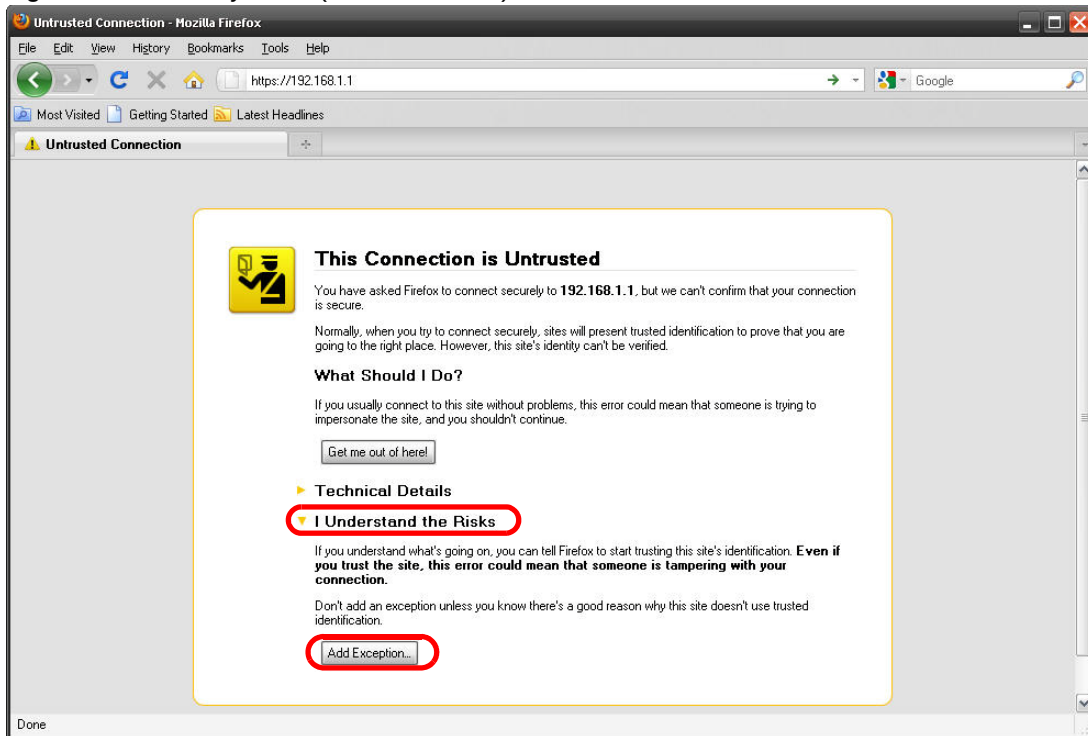
Figure 329 Certificate (Internet Explorer 7 or 8)



44.9.2 Mozilla Firefox Warning Messages

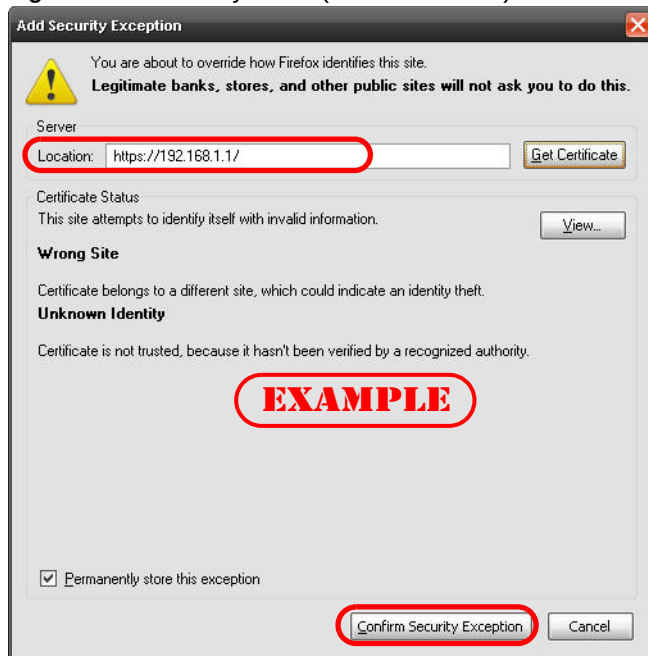
When you attempt to access the Switch HTTPS server, a **This Connection is Untrusted** screen may display. If that is the case, click **I Understand the Risks** and then the **Add Exception...** button.

Figure 330 Security Alert (Mozilla Firefox)



Confirm the HTTPS server URL matches. Click **Confirm Security Exception** to proceed to the web configurator login screen.

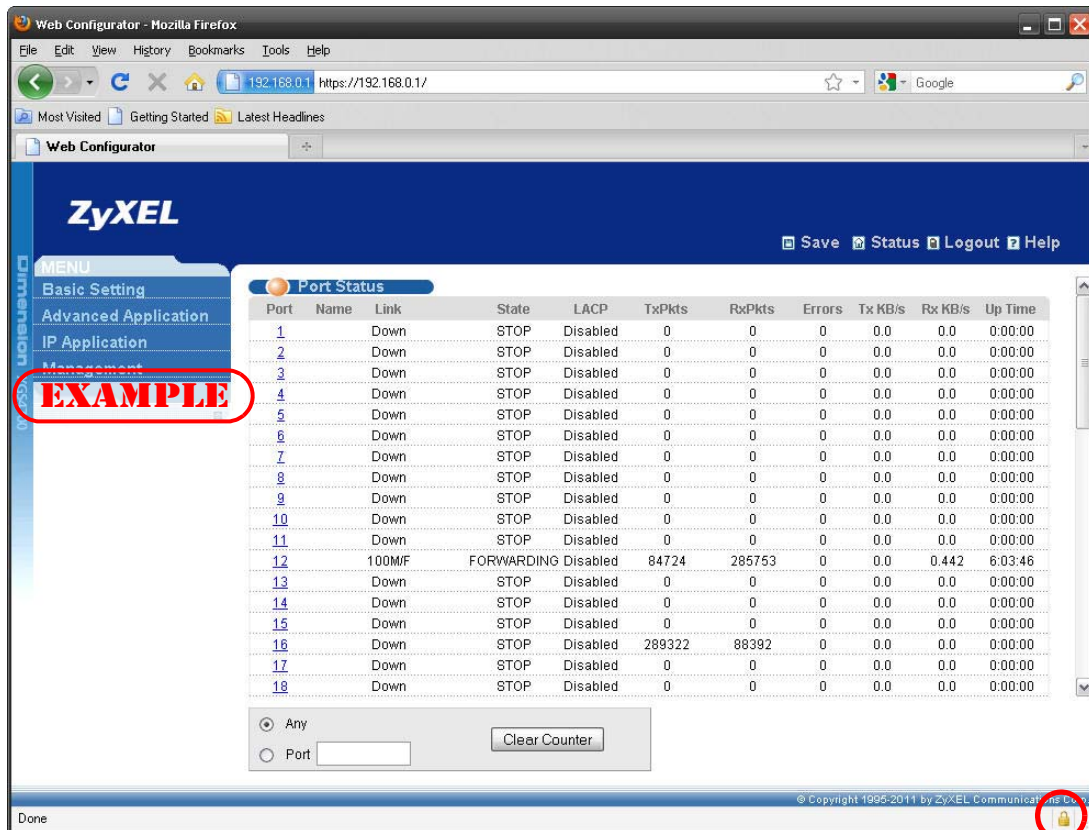
Figure 331 Security Alert (Mozilla Firefox)



44.9.3 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 (in Internet Explorer 6 or Mozilla Firefox) or next to the address bar (in Internet Explorer 7 or 8) denotes a secure connection.

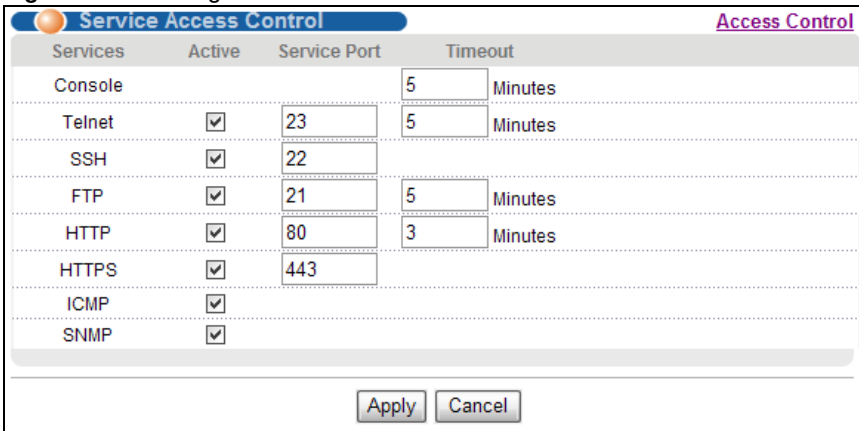
Figure 332 Example: Lock Denoting a Secure Connection



44.10 Service Access Control

Service Access Control allows you to decide what services you may use to access the Switch. You may also change the default service port and configure “trusted computer(s)” for each service in the **Remote Management** screen (discussed later). Click **Access Control** to go back to the main **Access Control** screen.

Figure 333 Management > Access Control > Service Access Control



The following table describes the fields in this screen.

Table 211 Management > Access Control > Service Access Control

LABEL	DESCRIPTION
Services	Services you may use to access the Switch are listed here.
Active	Select this option for the corresponding services that you want to allow to access the Switch.
Service Port	For Telnet, SSH, FTP, HTTP or HTTPS services, you may change the default service port by typing the new port number in the Service Port field. If you change the default port number then you will have to let people (who wish to use the service) know the new port number for that service.
Timeout	Type how many minutes (from 1 to 255) a management session can be left idle before the session times out. After it times out you have to log in with your password again. Very long idle timeouts may have security risks.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

44.11 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 334 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	☐	☐	☐	☐	☐	☐	☐

The following table describes the labels in this screen.

Table 212 Management > Access Control > Remote Management

LABEL	DESCRIPTION
Entry	This is the client set index number. A “client set” is a group of one or more “trusted computers” from which an administrator may use a service to manage the Switch.
Active	Select this check box to activate this secured client set. Clear the check box if you wish to temporarily disable the set without deleting it.
Start Address End Address	Configure the IP address range of trusted computers from which you can manage this Switch. The Switch checks if the client IP address of a computer requesting a service or protocol matches the range set here. The Switch immediately disconnects the session if it does not match.
Telnet/FTP/ HTTP/ICMP/ SNMP/SSH/ HTTPS	Select services that may be used for managing the Switch from the specified trusted computers.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

Diagnostic

This chapter explains the **Diagnostic** screen.

45.1 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 335 Management > Diagnostic

The screenshot shows the 'Diagnostic' screen with a title bar and a large text area labeled '- Info -'. Below this are four sections: 'System Log' with 'Display' and 'Clear' buttons; 'Ping Test' with radio buttons for 'IPv4' and 'IPv6', dropdown menus for IP addresses, and a 'Ping' button; 'Ethernet Port Test' with a 'Port' dropdown and a 'Port Test' button; and 'Cable Diagnostics' with a 'Port' dropdown and a 'Diagnose' button.

The following table describes the labels in this screen.

Table 213 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.
Ping Test	

Table 213 Management > Diagnostic (continued)

LABEL	DESCRIPTION
IPv4	Select this option if you want to ping an IPv4 address, and select which traffic flow (in-band or out-of-band) the Switch is to send ping frames. If you select in-band, the Switch sends the frames to all ports except the management port (labelled MGMT). If you select out-of-band, the Switch sends the frames to the management port (labelled MGMT).
IPv6	Select this option if you want to ping an IPv6 address. You also need to select the IPv6 interface type and specify the ID number of interface through which the Switch is to send ping frames.
IP Address	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.
Cable Diagnostics	Enter a port number and click Diagnose to perform a physical wire-pair test of the Ethernet connections on the specified port(s). The following fields display when you diagnose a port.
Port	This is the number of the physical Ethernet port on the Switch.

This chapter explains the syslog screens.

46.1 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 214 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.

46.2 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 336 Management > Syslog

Syslog Setup [Syslog Server Setup](#)

Syslog Active ☒

Logging type	Active	Facility
System	☒	local use 0
Interface	☒	local use 0
Switch	☒	local use 0
AAA	☒	local use 0
IP	☒	local use 0

Apply Cancel

The following table describes the labels in this screen.

Table 215 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.

46.3 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 337 Management > Syslog > Server Setup

Syslog Server Setup [Syslog Setup](#)

Active ☐

Server Address

Log Level

Index	Active	IP Address	Log Level	Delete
Delete Cancel				

The following table describes the labels in this screen.

Table 216 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.

Cluster Management

This chapter introduces cluster management.

47.1 Clustering Management Status Overview

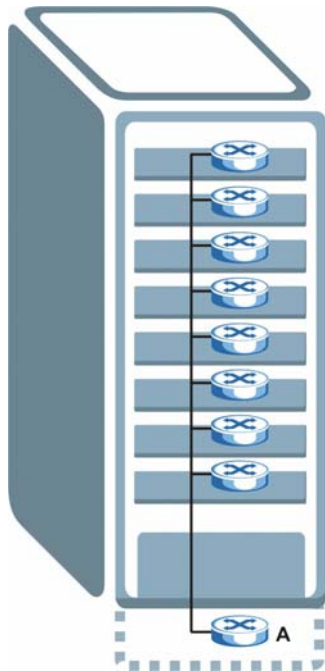
Cluster Management allows you to manage switches through one Switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

Table 217 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 338 Clustering Application Example



47.2 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 339 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 218 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 340 on page 443).
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)

47.2.1 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 340 Cluster Management: Cluster Member Web Configurator Screen

47.2.1.1 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 341 Example: Uploading Firmware to a Cluster Member Switch

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 Switch FTP version 1.0 ready at Thu Jan  1 00:58:46 1970
User (192.168.0.1:(none)): admin
331 Enter PASS command
Password:
230 Logged in
ftp> ls
200 Port command okay
150 Opening data connection for LIST
--w--w--w-  1 owner   group      6173152 Jul 01 12:00 ras-0
--w--w--w-  1 owner   group      6173152 Jul 01 12:00 ras-1
-rw-rw-rw-  1 owner   group     33554432 Jul 01 12:00 config
--w--w--w-  1 owner   group           0 Jul 01 12:00 ras-00-a0-c5-01-23-46
-rw-rw-rw-  1 owner   group           0 Jul 01 12:00 config-00-a0-c5-01-23-46
226 File sent OK
ftp: 297 bytes received in 0.00Seconds 297000.00Kbytes/sec.
ftp> bin
200 Type I OK
ftp> put 410AAGB0.bin ras-00-a0-c5-01-23-46
200 Port command okay
150 Opening data connection for STOR ras-00-a0-c5-01-23-46
226 File received OK
ftp: 262144 bytes sent in 0.63Seconds 415.44Kbytes/sec.
ftp>
```

The following table explains some of the FTP parameters.

Table 219 FTP Upload to Cluster Member Example

FTP PARAMETER	DESCRIPTION
User	Enter "admin".
Password	The web configurator password default is 1234.
ls	Enter this command to list the name of cluster member switch's firmware and configuration file.
410AAGB0.bin	This is the name of the firmware file you want to upload to the cluster member switch.
ras-00-a0-c5-01-23-46	This is the cluster member switch's firmware name as seen in the cluster manager switch.
config-00-a0-c5-01-23-46	This is the cluster member switch's configuration file name as seen in the cluster manager switch.

47.3 Clustering Management Configuration

Use this screen to configure clustering management. Click **Configuration** from the **Cluster Management** screen to display the next screen.

Figure 342 Management > Clustering Management > Configuration

Clustering Management Configuration [Status](#)

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-2114-V/GS-2114-V

EXAMPLE

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 220 Management > Clustering Management > Configuration

LABEL	DESCRIPTION
Clustering Manager	
Active	Select Active to have this Switch become the cluster manager switch. A cluster can only have one manager. Other (directly connected) switches that are set to be cluster managers will not be visible in the Clustering Candidates list. If a switch that was previously a cluster member is later set to become a cluster manager, then its Status is displayed as Error in the Cluster Management Status screen appears in the member summary list below.
Name	Type a name to identify the Clustering Manager . You may use up to 32 printable characters (spaces are allowed).
VID	This is the VLAN ID and is only applicable if the Switch is set to 802.1Q VLAN. All switches must be directly connected and in the same VLAN group to belong to the same cluster. Switches that are not in the same VLAN group are not visible in the Clustering Candidates list. This field is ignored if the Clustering Manager is using Port-based VLAN.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clustering Candidate	The following fields relate to the switches that are potential cluster members.
List	A list of suitable candidates found by auto-discovery is shown here. The switches must be directly connected. Directly connected switches that are set to be cluster managers will not be visible in the Clustering Candidate list. Switches that are not in the same management VLAN group will not be visible in the Clustering Candidate list.
Password	Each cluster member's password is its web configurator password. Select a member in the Clustering Candidate list and then enter its web configurator password. If that switch administrator changes the web configurator password afterwards, then it cannot be managed from the Cluster Manager . Its Status is displayed as Error in the Cluster Management Status screen. If multiple devices have the same password then hold [SHIFT] and click those switches to select them. Then enter their common web configurator password.
Add	Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Refresh	Click Refresh to perform auto-discovery again to list potential cluster members.
The next summary table shows the information for the clustering members configured.	
Index	This is the index number of a cluster member switch.
MacAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's System Name .
Model	This is the cluster member switch's model name.
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.

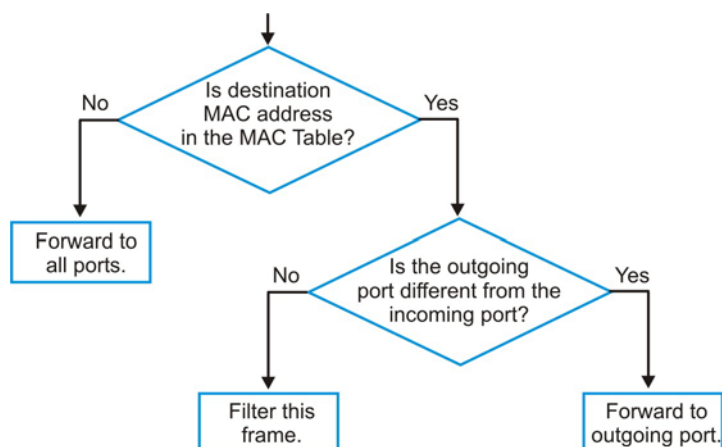
48.1 MAC Table Overview

The **MAC Table** screen (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the Switch's ports. When a device (which may belong to a VLAN group) sends a packet which is forwarded to a port on the Switch, the MAC address of the device is shown on the Switch's **MAC Table**. It also shows whether the MAC address is dynamic (learned by the Switch) or static (manually entered in the **Static MAC Forwarding** screen).

The Switch uses the **MAC Table** to determine how to forward frames. See the following figure.

- 1 The Switch examines a received frame and learns the port from which this source MAC address came.
- 2 The Switch checks to see if the frame's destination MAC address matches a source MAC address already learned in the **MAC Table**.
 - If the Switch has already learned the port for this MAC address, then it forwards the frame to that port.
 - If the Switch has not already learned the port for this MAC address, then the frame is flooded to all ports. Too much port flooding leads to network congestion then the Switch sends an ARP to request the MAC address. The Switch then learns the port that replies with the MAC address.
 - If the Switch has already learned the port for this MAC address, but the destination port is the same as the port it came in on, then it filters the frame.

Figure 343 MAC Table Flowchart



48.2 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 344 Management > MAC Table

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	00:0fe:1e:00:11	1	1	dynamic

The following table describes the labels in this screen.

Table 221 Management > MAC Table

LABEL	DESCRIPTION
Condition	Select All to display all MAC addresses in the MAC table. Select Static to only display static MAC address(es) in this screen. Select MAC and enter a valid MAC address (six hexadecimal character pairs) to display the MAC address information in this screen. Select VID and type a VLAN identification number to display all MAC addresses in the VLAN. Select Port and type the number of a port to display all MAC addresses learned from the port.
Sort by	Select this to display and arrange the data according to MAC address (MAC), VLAN group (VID) or port number (Port). The information is then displayed in the summary table below.
Transfer Type	Select Dynamic to MAC forwarding and click Transfer to add the relative dynamic MAC address(es) you select the criteria here into the static MAC forwarding table (see Section 8.2 on page 117). The type of the MAC address(es) will be changed to "static". Select Dynamic to MAC filtering and click Transfer to add the relative dynamic MAC address(es) you make the search here into the static MAC filtering table (see Section 10.1 on page 123). 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.

Table 221 Management > MAC Table (continued)

LABEL	DESCRIPTION
Index	This is the incoming frame index number.
MAC Address	This is the MAC address of the device from which this incoming frame came.
VID	This is the VLAN group to which this frame belongs.
Port	This is the port from which the above MAC address was learned. In stacking mode, the first number represents the slot and the second the port number.
Type	This shows whether the MAC address is dynamic (learned by the Switch) or static (manually entered in the Static MAC Forwarding screen).

IP Table

This chapter introduces the IP table.

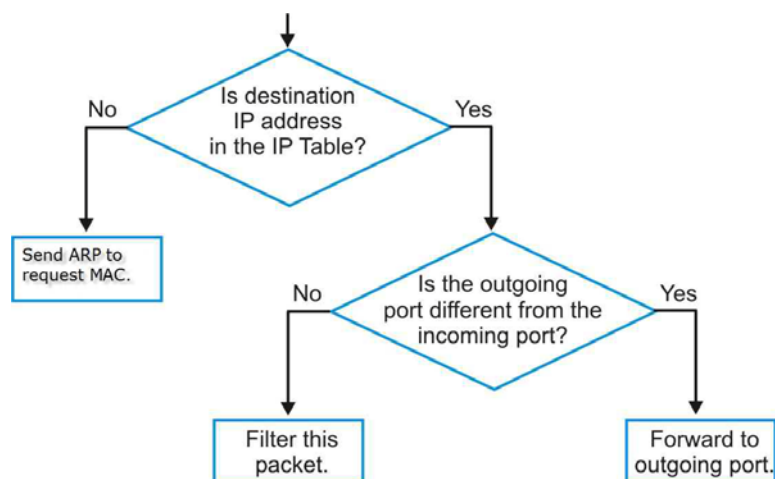
49.1 IP Table Overview

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 then the Switch sends an ARP to request the MAC address. The Switch then learns the port that replies with the MAC address.
 - If the Switch has already learned the port for this IP address, but the destination port is the same as the port it came in on, then it filters the packet.

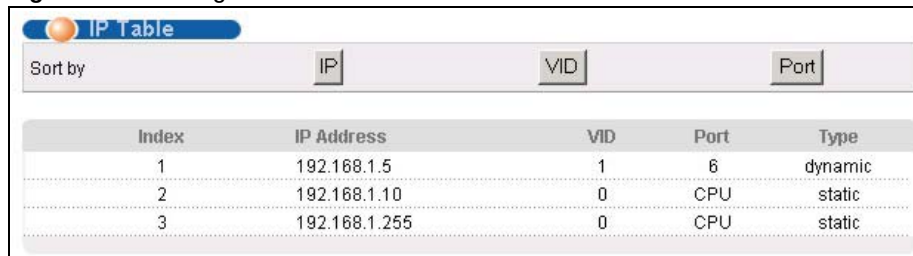
Figure 345 IP Table Flowchart



49.2 Viewing the IP Table

Click **Management > IP Table** in the navigation panel to display the following screen.

Figure 346 Management > IP Table



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 222 Management > IP Table

LABEL	DESCRIPTION
Sort by	Click one of the following buttons to display and arrange the data according to that button type. The information is then displayed in the summary table below.
IP	Click this button to display and arrange the data according to IP address.
VID	Click this button to display and arrange the data according to VLAN group.
Port	Click this button to display and arrange the data according to port number.
Index	This field displays the index number.
IP Address	This is the IP address of the device from which the incoming packets came.
VID	This is the VLAN group to which the packet belongs.
Port	This is the port from which the above IP address was learned. This field displays CPU to indicate the IP address belongs to the Switch. In stacking mode, the first number represents the slot and the second the port number.
Type	This shows whether the IP address is dynamic (learned by the Switch) or static (belonging to the Switch).

ARP Table

This chapter introduces ARP Table.

50.1 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.

50.1.1 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.

50.2 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 347 Management > ARP Table

Index	IP Address	MAC Address	VID	Port	Age(s)	Type
1	172.16.30.27	00:21:85:0c:44:4b	1234	45	285	dynamic
2	172.16.30.221	00:19:cb:37:00:49	1234	CPU	0	static
3	192.168.1.1	00:19:cb:37:00:49	1	CPU	0	static
4	192.168.2.1	00:19:cb:37:00:49	465	CPU	0	static

The following table describes the labels in this screen.

Table 223 Management > ARP Table

LABEL	DESCRIPTION
Condition	Specify how you want the Switch to remove ARP entries when you click Flush . Select All to remove all of the dynamic entries from the ARP table. Select IP Address and enter an IP address to remove the dynamic entries learned with the specified IP address. Select Port and enter a port number to remove the dynamic entries learned on the specified port.
Flush	Click Flush to remove the ARP entries according to the condition you specified.
Cancel	Click Cancel to return the fields to the factory defaults.
Index	This is the ARP table entry number.
IP Address	This is the IP address of a device connected to a Switch port with the corresponding MAC address below.
MAC Address	This is the MAC address of the device with the corresponding IP address above.
VID	This field displays the VLAN to which the device belongs.
Port	This field displays the port to which the device connects. CPU means this IP address is the Switch's management IP address. In stacking mode, the first number represents the slot and the second the port number.
Age(s)	This field displays how long (in seconds) an entry can still remain in the ARP table before it ages out and needs to be relearned. This shows 0 for a static entry.
Type	This shows whether the IP address is dynamic (learned by the Switch) or static (manually configured in the Basic Setting > IP Setup or IP Application > ARP Setup > Static ARP screen).

Routing Table

This chapter introduces the routing table.

51.1 Overview

The routing table contains the route information to the network(s) that the Switch can reach.

51.2 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 348 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 224 Management > Routing Table

LABEL	DESCRIPTION
Index	This field displays the index number.
Destination	This field displays the destination IP routing domain.
Gateway	This field displays the IP address of the gateway device.
Interface	This field displays the IP address of the Interface.
Metric	This field displays the cost of the route.
Type	This field displays the method used to learn the route. STATIC - added as a static entry.

Path MTU Table

This chapter introduces the IPv6 Path MTU table.

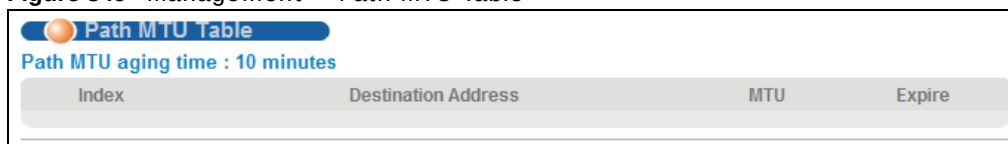
52.1 Path MTU Overview

The largest size (in bytes) of a packet that can be transferred over a data link is called the maximum transmission unit (MTU). The Switch uses Path MTU Discovery to discover Path MTU (PMTU), that is, the minimum link MTU of all the links in a path to the destination. If the Switch receives an ICMPv6 Packet Too Big error message after sending a packet, it fragments the next packet according to the suggested MTU in the error message.

52.2 Viewing the Path MTU Table

Use this screen to view IPv6 path MTU information on the Switch. Click **Management > Path MTU Table** in the navigation panel to display the screen as shown.

Figure 349 Management > Path MTU Table



The following table describes the labels in this screen.

Table 225 Management > Path MTU Table

LABEL	DESCRIPTION
Path MTU aging time	This field displays how long an entry remains in the Path MTU table before it ages out and needs to be relearned.
Index	This field displays the index number of each entry in the table.
Destination Address	This field displays the destination IPv6 address of each path/entry.
MTU	This field displays the maximum transmission unit of the links in the path.
Expire	This field displays how long (in minutes) an entry can still remain in the Path MTU table before it ages out and needs to be relearned.

Configure Clone

This chapter shows you how you can copy the settings of one port onto other ports.

53.1 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 350 Management > Configure Clone (Standalone)

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
- ☐ Multiple Rapid Spanning Tree Protocol
- ☐ Protocol-based VLAN
- ☐ Port-based VLAN
- ☐ MAC Authentication
- ☐ Storm
- ☐ MAC Pinning
- ☐ Green Ethernet

Figure 351 Management > Configure Clone (Stacking)

The following table describes the labels in this screen.

Table 226 Management > Configure Clone

LABEL	DESCRIPTION
Source/ Destination	In stacking mode, a port is defined by a slot ID representing the Switch in the stack and a port number.
Port / Slot (Stacking)	Select the source port and slot (in stacking mode) under the Source label. This port's attributes are copied. Enter the destination port or ports under the Destination label. These are the ports which are going to have the same attributes as the source port. You can enter individual ports separated by a comma or a range of ports by using a hyphen. For example, 2, 4, 6 indicates that ports 2, 4 and 6 are the destination ports. 2-6 indicates that ports 2 through 6 are the destination ports. In stacking mode, you can select multiple destination slots.
Basic Setting	Select which port settings (configured in the Basic Setting menus) should be copied to the destination port(s).
Advanced Application	Select which port settings (configured in the Advanced Application menus) should be copied to the destination ports.

Table 226 Management > Configure Clone (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.

Neighbor Table

This chapter introduces the IPv6 neighbor table.

54.1 IPv6 Neighbor Table Overview

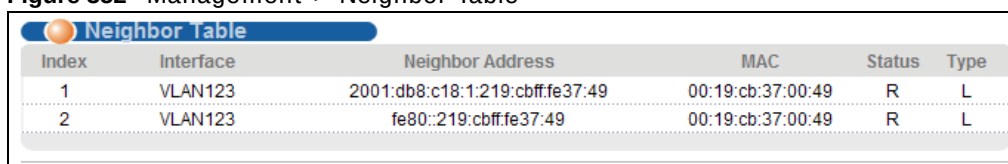
An IPv6 host is required to have a neighbor table. If there is an address to be resolved or verified, the Switch sends out a neighbor solicitation message. When the Switch receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor table. You can also manually create a static IPv6 neighbor entry using the **Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Setup** screen.

When the Switch needs to send a packet, it first consults other table to determine the next hop. Once the next hop IPv6 address is known, the Switch looks into the neighbor table to get the link-layer address and sends the packet when the neighbor is reachable. If the Switch cannot find an entry in the neighbor table or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

54.2 Viewing the IPv6 Neighbor Table

Use this screen to view IPv6 neighbor information on the Switch. Click **Management > Neighbor Table** in the navigation panel to display the screen as shown.

Figure 352 Management > Neighbor Table



Index	Interface	Neighbor Address	MAC	Status	Type
1	VLAN123	2001:db8:c18:1:219:cbff:fe37:49	00:19:cb:37:00:49	R	L
2	VLAN123	fe80::219:cbff:fe37:49	00:19:cb:37:00:49	R	L

The following table describes the labels in this screen.

Table 227 Management > Neighbor Table

LABEL	DESCRIPTION
Index	This field displays the index number of each entry in the table.
Interface	This field displays the ID number of the IPv6 interface on which the IPv6 address is created or through which the neighboring device can be reached.
Neighbor Address	This field displays the IPv6 address of the Switch or a neighboring device.
MAC	This field displays the MAC address of the IPv6 interface on which the IPv6 address is configure or the MAC address of the neighboring device.

Table 227 Management > Neighbor Table (continued)

LABEL	DESCRIPTION
Status	This field displays whether the neighbor IPv6 interface is reachable. In IPv6, “reachable” means an IPv6 packet can be correctly forwarded to a neighbor node (host or router) and the neighbor can successfully receive and handle the packet. The available options in this field are: • reachable (R): The interface of the neighboring device is reachable. (The Switch has received a response to the initial request.) • stale (S): The last reachable time has expired and the Switch is waiting for a response to another initial request. The field displays this also when the Switch receives an unrequested response from the neighbor's interface. • delay (D): The neighboring interface is no longer known to be reachable, and traffic has been sent to the neighbor recently. The Switch delays sending request packets for a short to give upper-layer protocols a chance to determine reachability. • probe (P): The Switch is sending request packets and waiting for the neighbor's response. • invalid (IV): The neighbor address is with an invalid IPv6 address. • unknown (?): The status of the neighboring interface can not be determined for some reason. • incomplete (I): Address resolution is in progress and the link-layer address of the neighbor has not yet been determined. The interface of the neighboring device did not give a complete response.
Type	This field displays the type of an address mapping to a neighbor interface. The available options in this field are: • other (O): none of the following type. • local (L): A Switch interface is using the address. • dynamic (D): The IP address to MAC address can be successfully resolved using IPv6 Neighbor Discovery protocol. Is it similar as IPv4 ARP (Address Resolution protocol). • static (S): The interface address is statically configured.

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 33](#).
- 2 Check the hardware connections. See [Section 3.1 on page 28](#).
- 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 41](#).

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 41](#).

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 33](#).
 - 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 41](#).
 - 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 41](#).

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 44.11 on page 433](#)). 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 43.6 on page 406](#) for more information about how to save your configuration.



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 228 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by e-mail.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol - a client/server protocol for the world wide web.

Table 228 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet INternet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one e-mail server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).

Table 228 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

Overview

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

IPv6 Addressing

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

IPv6 addresses can be abbreviated in two ways:

- Leading zeros in a block can be omitted. So 2001:0db8:1a2b:0015:0000:0000:1a2f:0000 can be written as 2001:db8:1a2b:15:0:0:1a2f:0.
- Any number of consecutive blocks of zeros can be replaced by a double colon. A double colon can only appear once in an IPv6 address. So 2001:0db8:0000:0000:1a2f:0000:0000:0015 can be written as 2001:0db8::1a2f:0000:0000:0015, 2001:0db8:0000:0000:1a2f::0015, 2001:db8::1a2f:0:0:15 or 2001:db8:0:0:1a2f::15.

Prefix and Prefix Length

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

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

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

Link-local Address

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

Table 229 Link-local Unicast Address Format

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

Global Address

A global address uniquely identifies a device on the Internet. It is similar to a “public IP address” in IPv4. A global unicast address starts with a 2 or 3.

Unspecified Address

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

Loopback Address

A loopback address (0:0:0:0:0:0:0:1 or ::1) allows a host to send packets to itself. It is similar to “127.0.0.1” in IPv4.

Multicast Address

In IPv6, multicast addresses provide the same functionality as IPv4 broadcast addresses. Broadcasting is not supported in IPv6. A multicast address allows a host to send packets to all hosts in a multicast group.

Multicast scope allows you to determine the size of the multicast group. A multicast address has a predefined prefix of ff00::/8. The following table describes some of the predefined multicast addresses.

Table 230 Predefined Multicast Address

MULTICAST ADDRESS	DESCRIPTION
FF01:0:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP servers on a local site.

The following table describes the multicast addresses which are reserved and can not be assigned to a multicast group.

Table 231 Reserved Multicast Address

MULTICAST ADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0

Table 231 Reserved Multicast Address (continued)

MULTICAST ADDRESS
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Subnet Masking

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

Interface ID

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

EUI-64

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

Table 232

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

Table 233

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

Stateless Autoconfiguration

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

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

When the interface is connected to a network with a router and the Switch is set to automatically obtain an IPv6 network prefix from the router for the interface, it generates ³another address which

combines its interface ID and global and subnet information advertised from the router. This is a routable global IP address.

DHCPv6

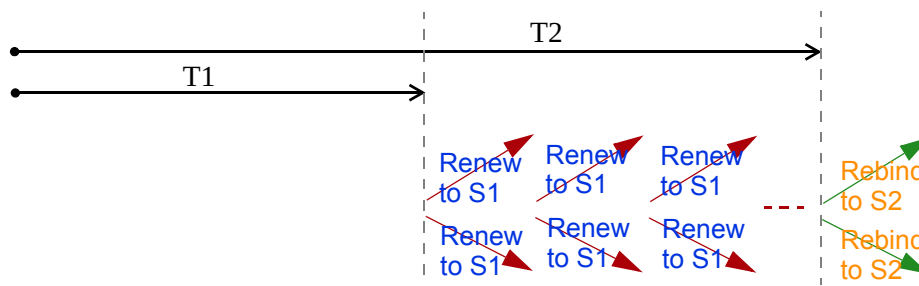
The Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 3315) is a server-client protocol that allows a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients. DHCPv6 servers and clients exchange DHCP messages using UDP.

Each DHCP client and server has a unique DHCP Unique Identifier (DUID), which is used for identification when they are exchanging DHCPv6 messages. The DUID is generated from the MAC address, time, vendor assigned ID and/or the vendor's private enterprise number registered with the IANA. It should not change over time even after you reboot the device.

Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.

The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.



DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string,

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

such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The Switch uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the Switch passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor's reachability in a network. An IPv6 device uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor's link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being "reachable" means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.
- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.
- Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The Switch maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the Switch configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the Switch also sends out a neighbor solicitation message. When the Switch receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the Switch uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The Switch creates an entry in the default router list cache if the router can be used as a default router.

When the Switch needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the Switch uses the prefix list to

determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is onlink, the address is considered as the next hop. Otherwise, the Switch determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the Switch looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the Switch cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which multicast groups a port can join.

MLD Messages

A multicast router or switch periodically sends general queries to MLD hosts to update the multicast forwarding table. When an MLD host wants to join a multicast group, it sends an MLD Report message for that address.

An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

Example - Enabling IPv6 on Windows XP/2003/Vista

By default, Windows XP and Windows 2003 support IPv6. This example shows you how to use the `ipv6 install` command on Windows XP/2003 to enable IPv6. This also displays how to use the `ipconfig` command to see auto-generated IP addresses.

```
C:\>ipv6 install
Installing...
Succeeded.

C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 10.1.1.46
    Subnet Mask . . . . . : 255.255.255.0
    IP Address. . . . . : fe80::2d0:59ff:feb8:103c%4
    Default Gateway . . . . . : 10.1.1.254
```

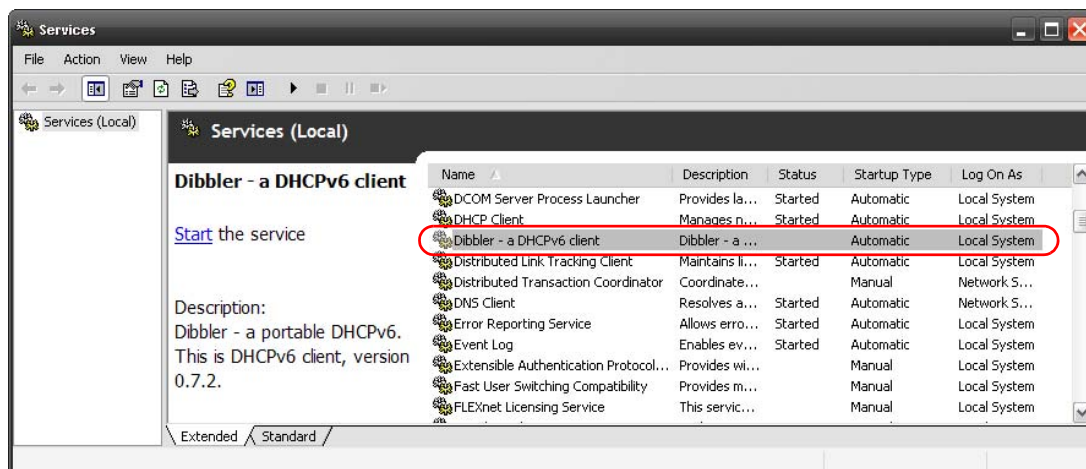
IPv6 is installed and enabled by default in Windows Vista. Use the `ipconfig` command to check your automatic configured IPv6 address as well. You should see at least one IPv6 address available for the interface on your computer.

Example - Enabling DHCPv6 on Windows XP

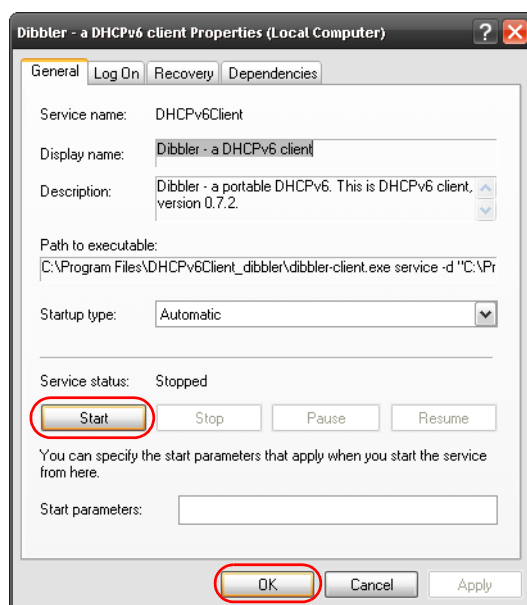
Windows XP does not support DHCPv6. If your network uses DHCPv6 for IP address assignment, you have to additionally install a DHCPv6 client software on your Windows XP. (Note: If you use static IP addresses or Router Advertisement for IPv6 address assignment in your network, ignore this section.)

This example uses Dibbler as the DHCPv6 client. To enable DHCPv6 client on your computer:

- 1 Install Dibbler and select the DHCPv6 client option on your computer.
- 2 After the installation is complete, select **Start > All Programs > Dibbler-DHCPv6 > Client Install as service**.
- 3 Select **Start > Control Panel > Administrative Tools > Services**.
- 4 Double click **Dibbler - a DHCPv6 client**.



- 5 Click **Start** and then **OK**.



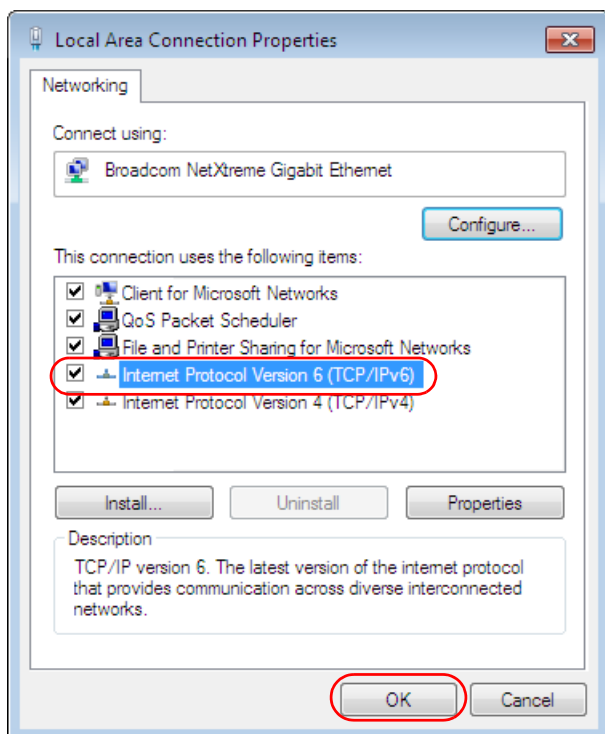
- 6 Now your computer can obtain an IPv6 address from a DHCPv6 server.

Example - Enabling IPv6 on Windows 7

Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

- 1 Select **Control Panel > Network and Sharing Center > Local Area Connection**.
- 2 Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.
- 3 Click **OK** to save the change.



- 4 Click **Close** to exit the **Local Area Connection Status** screen.
- 5 Select **Start > All Programs > Accessories > Command Prompt**.
- 6 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:b021:2d::1000
    Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
    IPv4 Address. . . . . : 172.16.100.61
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::213:49ff:feaa:7125%11
                                172.16.100.254
```

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a ZyXEL office for the region in which you bought the device.

Regional websites are listed below. Please have the following information ready when you contact an office. (See also http://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml).

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

Taiwan

- ZyXEL Communications Corporation
- <http://www.zyxel.com>

Asia

China

- ZyXEL Communications (Shanghai) Corp.
- ZyXEL Communications (Beijing) Corp.
- ZyXEL Communications (Tianjin) Corp.
- <http://www.zyxel.cn>

India

- ZyXEL Technology India Pvt Ltd
- <http://www.zyxel.in>

Kazakhstan

- ZyXEL Kazakhstan
- <http://www.zyxel.kz>

Korea

- ZyXEL Korea Corp.
- <http://www.zyxel.kr>

Malaysia

- ZyXEL Malaysia Sdn Bhd.
- <http://www.zyxel.com.my>

Pakistan

- ZyXEL Pakistan (Pvt.) Ltd.
- <http://www.zyxel.com.pk>

Philippines

- ZyXEL Philippines
- <http://www.zyxel.com.ph>

Singapore

- ZyXEL Singapore Pte Ltd.
- <http://www.zyxel.com.sg>

Taiwan

- ZyXEL Communications Corporation
- <http://www.zyxel.com>

Thailand

- ZyXEL Thailand Co., Ltd
- <http://www.zyxel.co.th>

Vietnam

- ZyXEL Communications Corporation-Vietnam Office
- <http://www.zyxel.com/vn/vi>

Europe

Austria

- ZyXEL Deutschland GmbH
- <http://www.zyxel.de>

Belarus

- ZyXEL BY
- <http://www.zyxel.by>

Belgium

- ZyXEL Communications B.V.
- <http://www.zyxel.com/be/nl/>

Bulgaria

- ZyXEL България
- <http://www.zyxel.com/bg/bg/>

Czech

- ZyXEL Communications Czech s.r.o
- <http://www.zyxel.cz>

Denmark

- ZyXEL Communications A/S
- <http://www.zyxel.dk>

Estonia

- ZyXEL Estonia
- <http://www.zyxel.com/ee/et/>

Finland

- ZyXEL Communications
- <http://www.zyxel.fi>

France

- ZyXEL France
- <http://www.zyxel.fr>

Germany

- ZyXEL Deutschland GmbH
- <http://www.zyxel.de>

Hungary

- ZyXEL Hungary & SEE
- <http://www.zyxel.hu>

Latvia

- ZyXEL Latvia
- <http://www.zyxel.com/lv/lv/homepage.shtml>

Lithuania

- ZyXEL Lithuania
- <http://www.zyxel.com/lt/lt/homepage.shtml>

Netherlands

- ZyXEL Benelux
- <http://www.zyxel.nl>

Norway

- ZyXEL Communications
- <http://www.zyxel.no>

Poland

- ZyXEL Communications Poland
- <http://www.zyxel.pl>

Romania

- ZyXEL Romania
- <http://www.zyxel.com/ro/ro>

Russia

- ZyXEL Russia
- <http://www.zyxel.ru>

Slovakia

- ZyXEL Communications Czech s.r.o. organizacna zlozka
- <http://www.zyxel.sk>

Spain

- ZyXEL Spain
- <http://www.zyxel.es>

Sweden

- ZyXEL Communications
- <http://www.zyxel.se>

Switzerland

- Studerus AG
- <http://www.zyxel.ch/>

Turkey

- ZyXEL Turkey A.S.
- <http://www.zyxel.com.tr>

UK

- ZyXEL Communications UK Ltd.
- <http://www.zyxel.co.uk>

Ukraine

- ZyXEL Ukraine
- <http://www.ua.zyxel.com>

Latin America

Argentina

- ZyXEL Communication Corporation
- <http://www.zyxel.com/ec/es/>

Ecuador

- ZyXEL Communication Corporation
- <http://www.zyxel.com/ec/es/>

Middle East

Egypt

- ZyXEL Communication Corporation
- <http://www.zyxel.com/homepage.shtml>

Middle East

- ZyXEL Communication Corporation
- <http://www.zyxel.com/homepage.shtml>

North America

USA

- ZyXEL Communications, Inc. - North America Headquarters
- <http://www.us.zyxel.com/>

Oceania

Australia

- ZyXEL Communications Corporation
- <http://www.zyxel.com/au/en/>

Africa

South Africa

- Nology (Pty) Ltd.
- <http://www.zyxel.co.za>

Legal Information

Copyright

Copyright © 2015 by ZyXEL Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of ZyXEL Communications Corporation.

Published by ZyXEL Communications Corporation. All rights reserved.

Disclaimer

ZyXEL does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. ZyXEL further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Regulatory Notice and Statement (Class A)

United States of America



Federal Communications Commission (FCC) EMC Statement

- This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:
 - (1) This device may not cause harmful interference.
 - (2) This device must accept any interference received, including interference that may cause undesired operations.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
- This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canada

The following information applies if you use the product within Canada area

Industry Canada ICES statement

CAN ICES-3 (A)/NMB-3(A)

European Union



The following information applies if you use the product within the European Union.

CE EMC statement

This is Class A Product. In domestic environment this product may cause radio interference in which case the user may be required to take adequate measures.

List of National Codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Malta	MT
Belgium	BE	Netherlands	NL
Cyprus	CY	Poland	PL
Czech Republic	CR	Portugal	PT
Denmark	DK	Slovakia	SK
Estonia	EE	Slovenia	SI
Finland	FI	Spain	ES
France	FR	Sweden	SE
Germany	DE	United Kingdom	GB
Greece	GR	Iceland	IS
Hungary	HU	Liechtenstein	LI
Ireland	IE	Norway	NO
Italy	IT	Switzerland	CH
Latvia	LV	Bulgaria	BG
Lithuania	LT	Romania	RO
Luxembourg	LU	Turkey	TR

Notices

CLASS 1 LASER PRODUCT

APPAREIL À LASER DE CLASS 1

PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.

PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

Safety Warnings

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

Environment Statment**WEEE Directive**

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.



"INFORMAZIONI AGLI UTENTI"

Ai sensi della Direttiva 2012/19/UE del Parlamento europeo e del Consiglio, del 4 luglio 2012, sui rifiuti di apparecchiature elettriche ed elettroniche (RAEE)

Il simbolo del cassonetto barrato riportato sull'apparecchiatura o sulla sua confezione indica che il prodotto alla fine della propria vita utile deve essere raccolto separatamente dagli altri rifiuti.

La raccolta differenziata della presente apparecchiatura giunta a fine vita è organizzata e gestita dal produttore. L'utente che vorrà disfarsi della presente apparecchiatura dovrà quindi contattare il

produttore e seguire il sistema che questo ha adottato per consentire la raccolta separata dell'apparecchiatura giunta a fine vita.

L'adeguata raccolta differenziata per l'avvio successivo dell'apparecchiatura dismessa al riciclaggio, al trattamento e allo smaltimento ambientalmente compatibile contribuisce ad evitare possibili effetti negativi sull'ambiente e sulla salute e favorisce il reimpiego e/o riciclo dei materiali di cui è composta l'apparecchiatura.

Lo smaltimento abusivo del prodotto da parte del detentore comporta l'applicazione delle sanzioni amministrative previste dalla normativa vigente."

Environmental Product Declaration

Български (Bulgarian)	Čeština (Czech)	Dansk (Danish)	Deutsch (German)
Екологична продуктова декларация RoHS Директива 2011/65/ЕС WEEE Директива 2012/19/ЕС PPW Директива 94/62/ЕО REACH Регламент (ЕО) № 1907/2006 Име/име : Richard Hsu / Quality Management Division Senior Manager Подпис : Дата (dd/mm/yyyy) : 01/10/2014  	Environmentální prohlášení o produktu RoHS Směrnice 2011/65/EU WEEE Směrnice 2012/19/EU PPW Směrnice 94/62/ES REACH Nařízení (ES) č. 1907/2006 Jméno/štit : Richard Hsu / Quality Management Division Senior Manager Podpis : Datum (dd/mm/yyyy) : 01/10/2014  	Miljøvaredeklaration RoHS Direktiv 2011/65/EU WEEE Direktiv 2012/19/EU PPW Direktiv 94/62/EF REACH Forordning (EF) nr. 1907/2006 Navn/štit : Richard Hsu / Quality Management Division Senior Manager Underskrift : Dato (dd/mm/åååå) : 01/10/2014  	Produkt-Umweltdeklaration RoHS Richtlinie 2011/65/EU WEEE Richtlinie 2012/19/EU PPW Richtlinie 94/62/EG REACH VERORDNUNG (EG) Nr. 1907/2006 Name/štit : Richard Hsu / Quality Management Division Senior Manager Unterschrift : Datum (dd/mm/yyyy) : 01/10/2014  
Toote keskkonnadeklaratsioon RoHS Direktiv 2011/65/EL WEEE Direktiv 2012/19/EL PPW Direktiv 94/62/EÜ REACH MÄÄRUS (EÜ) nr 1907/2006 Nimi/štit : Richard Hsu / Quality Management Division Senior Manager Allkiri : Kuupäev (pp/kk/aaaa) : 01/10/2014  	Environmental product declaration RoHS Directive 2011/65/EU WEEE Directive 2012/19/EU PPW Directive 94/62/EC REACH Regulation (EC) No 1907/2006 Name/štit : Richard Hsu / Quality Management Division Senior Manager Signature : Date (dd/mm/yyyy) : 01/10/2014  	Declaraciones Ambientales de Producto RoHS Directiva 2011/65/UE WEEE Directiva 2012/19/UE PPW Directiva 94/62/CE REACH REGLAMENTO (CE) nº 1907/2006 Nombre/štit : Richard Hsu / Quality Management Division Senior Manager Firma : Fecha (aaaa/mm/dd) : 2014/10/01  	Profil environnemental de produit RoHS Directive 2011/65/UE WEEE Directive 2012/19/UE PPW Directive 94/62/CE REACH RÈGLEMENT (CE) N° 1907/2006 Nom/štit : Richard Hsu / Quality Management Division Senior Manager Signature : Date (aaaa/mm/jj) : 2014/10/01  
Deklaraciju o zbirjavanju proizvoda RoHS Direktiva 2011/65/EU WEEE Direktiva 2012/19/EU PPW Direktiva 94/62/EZ REACH Uredbe (EZ) br. 1907/2006 Ime/štit : Richard Hsu / Quality Management Division Senior Manager Podpis : Datum (dd/mm/yyyy) : 01/10/2014  	Dichiarazione ambientale di prodotto RoHS Direttiva 2011/65/UE WEEE Direttiva 2012/19/UE PPW Direttiva 94/62/CE REACH REGOLAMENTO (CE) n. 1907/2006 Nome/štit : Richard Hsu / Quality Management Division Senior Manager Firma : Data (aaaa/mm/gggg) : 2014/10/01  	Produkta vides ietekmējuma deklarācija RoHS Direktīva 2011/65/ES WEEE Direktīva 2012/19/ES PPW Direktīva 94/62/EK REACH Regula (EK) Nr. 1907/2006 Nosaukums/štit : Richard Hsu / Quality Management Division Senior Manager Paraksts : Datums (dd/mm/gggg) : 01/10/2014  	Aplinkosauginis gaminto deklaracija RoHS Direktyva 2011/65/ES WEEE Direktyva 2012/19/ES PPW Direktyva 94/62/EB REACH REGLAMENTAS (EB) Nr. 1907/2006 Vardas/štit : Richard Hsu / Quality Management Division Senior Manager Parašas : Data (dd/mm/yyyy) : 01/10/2014  
Környezetvédelmi terméknyilatkozat RoHS 2011/65/EU irányelve WEEE 2012/19/EU irányelve PPW 94/62/EK irányelve REACH 1907/2006/EK Rendelet Név/štit : Richard Hsu / Quality Management Division Senior Manager Aláírás : Dátum (aaaa/hh/nn) : 2014/10/01  	Dikjarazzjoni Ambjentali dwar il-Prodott RoHS Direttiva 2011/65/UE WEEE Direttiva 2012/19/UE PPW Direttiva 94/62/CE REACH REGOLAMENTO (CE) NRJ 1907/2006 Isim/štit : Richard Hsu / Quality Management Division Senior Manager Firma : Data (aaaa/xx/yy) : 2014/10/01  	Milieuproductverklaring RoHS Richtlijn 2011/65/EU WEEE Richtlijn 2012/19/EU PPW Richtlijn 94/62/EG REACH Verordening (EG) nr. 1907/2006 Naam/štit : Richard Hsu / Quality Management Division Senior Manager Handtekening : Datum (dd/mm/jaar) : 01/10/2014  	Deklarację środowiskową produktu RoHS Dyrektywa 2011/65/UE WEEE Dyrektywa 2012/19/UE PPW Dyrektywa 94/62/WE REACH Rozporządzenie (WE) nr 1907/2006 Nazwisko/štit : Richard Hsu / Quality Management Division Senior Manager Podpis : Data (mm/nn/rrrr) : 2014/10/01  
Declaração ambiental do produto RoHS Diretiva 2011/65/UE WEEE Diretiva 2012/19/UE PPW Diretiva 94/62/CE REACH Regulamento (CE) n.º 1907/2006 Nome/štit : Richard Hsu / Quality Management Division Senior Manager Assinatura : Data (dd/mm/aaaa) : 01/10/2014  	Declarație de mediu privind produsele RoHS Directiva 2011/65/UE WEEE Directiva 2012/19/UE PPW Directiva 94/62/CE REACH REGULAMENTUL (CE) NR. 1907/2006 Numel/štit : Richard Hsu / Quality Management Division Senior Manager Semnatura : Data (zz/aa/aaaa) : 01/10/2014  	Vyhlasenie o environmentálnom výrobku RoHS Smernica 2011/65/EU WEEE Smernica 2012/19/EU PPW Smernica 94/62/ES REACH Naariadenie (ES) č. 1907/2006 Menor/štit : Richard Hsu / Quality Management Division Senior Manager Podpis : Datum (dd/mm/yyyy) : 01/10/2014  	Okoljsko deklaracijo izdelka RoHS Direktiva 2011/65/EU WEEE Direktiva 2012/19/EU PPW Direktiva 94/62/ES REACH Uredba (ES) č. 1907/2006 Ime/štit : Richard Hsu / Quality Management Division Senior Manager Podpis : Datum (dd/mm/rrrr) : 01/10/2014  
Standardin perustava ympäristötutusteloste RoHS Direktiivi 2011/65/EU WEEE Direktiivi 2012/19/EU PPW Direktiivi 94/62/EY REACH ASETUS (EY) N:o 1907/2006 Nimi/štit : Richard Hsu / Quality Management Division Senior Manager Ala kirjitus : Päivämäärä (pp/kk/vvvv) : 01/10/2014  	Miljöproduktdeklaration RoHS Direktiv 2011/65/EU WEEE Direktiv 2012/19/EU PPW Direktiv 94/62/EG REACH Förordning (EG) nr 1907/2006 Name/štit : Richard Hsu / Quality Management Division Senior Manager Namnteckning : Datum (dd/mm/åååå) : 01/10/2014  	Περιβαλλοντική δήλωση προϊόντος RoHS Οδηγία 2011/65/ΕΕ WEEE Οδηγία 2012/19/ΕΕ PPW Οδηγία 94/62/ΕΚ REACH Κανονισμός (ΕΚ) αριθ. 1907/2006 Όνομα/štit : Richard Hsu / Quality Management Division Senior Manager Υπογραφή : Ημερομηνία (ηη/μμ/εεεε) : 01/10/2014  	Miljødeklarasjon RoHS Direktiv 2011/65/EU WEEE Direktiv 2012/19/EU PPW Direktiv 94/62/EF REACH Forordning (EF) nr. 1907/2006 Navn/štit : Richard Hsu / Quality Management Division Senior Manager Signatur : Dato (dd/mm/åååå) : 01/10/2014  

Taiwanese BSMI (Bureau of Standards, Metrology and Inspection) A Warning:

警告使用者

這是甲類的資訊產品，在居住的環境使用時，
可能造成射頻干擾，在這種情況下，
使用者會被要求採取某些適當的對策。

Viewing Certifications

Go to <http://www.zyxel.com> to view this product's documentation and certifications.

ZyXEL Limited Warranty

ZyXEL warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized ZyXEL local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, ZyXEL will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of ZyXEL. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. ZyXEL shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Trademarks

ZyNOS (ZyXEL Network Operating System) and ZON (ZyXEL One Network) are registered trademarks of ZyXEL Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. To obtain the source code covered under those Licenses, please contact support@zyxel.com.tw to get it.

Index

Numbers

802.1P priority [67](#)

802.3az [318](#)

A

access control

 limitations [412](#)

 login account [424](#)

 remote management [433](#)

 service port [432](#)

 SNMP [412](#)

accounting

 setup [246](#)

address learning, MAC [104](#), [106](#)

Address Resolution Protocol (ARP) [395](#), [451](#), [455](#),
[456](#)

administrator password [425](#)

age [141](#)

aggregator ID [165](#), [168](#)

aging time [61](#)

applications

 bridging [20](#)

 IEEE 802.1Q VLAN [21](#)

 switched workgroup [20](#)

ARP

 how it works [395](#), [451](#)

 table [451](#)

ARP (Address Resolution Protocol) [395](#), [451](#)

ARP inspection [254](#), [256](#)

 and MAC filter [257](#)

 configuring [257](#)

 syslog messages [257](#)

 trusted ports [257](#)

authentication

 and RADIUS [242](#)

 setup [246](#)

authorization

 privilege levels [249](#)

 setup [246](#)

automatic VLAN registration [95](#)

B

back up, configuration file [405](#)

basic settings [54](#)

binding [254](#)

binding table [254](#)

 building [254](#)

BPDUs (Bridge Protocol Data Units) [126](#)

Bridge Protocol Data Units (BPDUs) [126](#)

C

CDP [288](#)

certifications

 notices [483](#)

 viewing [486](#)

CFI (Canonical Format Indicator) [94](#)

changing the password [40](#)

Cisco Discovery Protocol, see CDP

CIST [129](#)

CIST (Common and Internal Spanning Tree) [127](#)

Class of Service (CoS) [360](#)

classifier [188](#), [192](#)

 and QoS [188](#)

 editing [192](#), [194](#)

 example [194](#)

 overview [188](#)

 setup [188](#), [192](#), [194](#)

 viewing [192](#), [194](#)

cloning a port See port cloning

cluster management [440](#)

 and switch passwords [445](#)

 cluster manager [440](#), [445](#)

 cluster member [440](#), [445](#)

 cluster member firmware upgrade [443](#)

- network example [440](#)
- setup [444](#)
- specification [440](#)
- status [441](#)
- switch models [440](#)
- VID [445](#)
- web configurator [442](#)
- cluster manager [440](#)
- cluster member [440](#)
- command interface [23](#)
- Common and Internal Spanning Tree (CIST) [127](#)
- Common and Internal Spanning Tree, See CIST [129](#)
- configuration [354](#)
 - change running config [406](#)
- configuration file [41](#)
 - backup [405](#)
 - restore [41](#), [404](#)
 - saving [406](#)
- configuration, saving [41](#)
- console port
 - settings [31](#)
- contact information [476](#)
- copying port settings, See port cloning
- copyright [482](#)
- CPU management port [110](#)
- CPU protection
 - configuration [306](#)
 - overview [303](#)
- current date [59](#)
- current time [59](#)
- customer support [476](#)

D

- daylight saving time [59](#)
- default gateway [378](#)
- default IP address [31](#)
- DHCP [369](#)
 - client IP pool [378](#)
 - configuration options [369](#)
 - modes [369](#)
 - relay agent [369](#)
 - relay example [380](#)
 - server [369](#)

- setup [377](#)
- DHCP (Dynamic Host Configuration Protocol) [369](#)
- DHCP relay option 82 [256](#)
- DHCP snooping [254](#)
 - configuring [256](#)
 - DHCP relay option 82 [256](#)
 - trusted ports [255](#)
 - untrusted ports [255](#)
- DHCP snooping database [255](#)
- diagnostics [435](#)
 - Ethernet port test [436](#)
 - ping [435](#)
 - system log [435](#)
- Differentiated Service (DiffServ) [360](#)
- DiffServ [360](#)
 - activate [362](#)
 - and TRTCM [365](#)
 - DS field [360](#)
 - DSCP [360](#)
 - DSCP-to-IEEE802.1p mapping [367](#)
 - network example [360](#)
 - PHB [360](#)
- disclaimer [482](#)
- documentation
 - related [2](#)
- double-tagged frames [206](#)
- DS (Differentiated Services) [360](#)
- DSCP
 - DSCP-to-IEEE802.1p mapping [367](#)
 - service level [360](#)
 - what it does [360](#)
- DSCP (DiffServ Code Point) [360](#)
- dynamic link aggregation [163](#)

E

- EEE [318](#)
- egress port [113](#)
- Energy Efficient Ethernet [318](#)
- error disable detect [304](#), [308](#)
- error disable recovery
 - configuration [309](#)
 - overview [303](#)
- Ethernet broadcast address [395](#), [451](#)
- Ethernet port test [436](#)

Ethernet ports
 default settings [29](#)
external authentication server [242](#)

F

Fan Module [32](#)
fan speed [56, 57](#)
FCC interference statement [482](#)
file transfer using FTP
 command example [409](#)
filename convention, configuration
 configuration
 file names [409](#)
filtering [123](#)
 rules [123](#)
filtering database, MAC table [446](#)
firmware [55](#)
 upgrade [402, 443](#)
flow control [67](#)
 back pressure [67](#)
 IEEE802.3x [67](#)
forwarding
 delay [141](#)
frames
 tagged [103](#)
 untagged [103](#)
front panel [28](#)
FTP [23, 409](#)
 file transfer procedure [410](#)
 restrictions over WAN [411](#)

G

GARP [95](#)
GARP (Generic Attribute Registration Protocol) [95](#)
GARP terminology [95](#)
GARP timer [61, 95](#)
general setup [58](#)
getting help [43](#)
GMT (Greenwich Mean Time) [59](#)
Green Ethernet [318](#)
GVRP [95, 102, 103](#)

 and port assignment [103](#)
GVRP (GARP VLAN Registration Protocol) [95](#)

H

hardware installation [24](#)
hardware monitor [55, 56, 57](#)
hardware overview [28](#)
hello time [141](#)
hops [141](#)
HTTPS [427](#)
 certificates [427](#)
 implementation [427](#)
 public keys, private keys [427](#)
HTTPS example [428](#)

I

IEEE 802.1p, priority [62](#)
IEEE 802.1x
 activate [175, 180, 244](#)
 reauthentication [177](#)
IEEE 802.1x, port authentication [173](#)
IGMP
 version [214](#)
IGMP (Internet Group Management Protocol) [214](#)
IGMP filtering [214](#)
 profile [223](#)
 profiles [219, 225, 226, 229, 230](#)
IGMP leave timeout
 fast [220](#)
 normal [220](#)
IGMP snooping [215](#)
 MVR [232](#)
IGMP throttling [221](#)
ingress port [113](#)
Installation
 Rack-mounting [25](#)
installation
 freestanding [24](#)
 precautions [25](#)
Installing the Fan Module [32](#)
Internet Protocol version 6, see IPv6

introduction [19](#)

IP

- interface [62, 385](#)
- routing domain [62](#)
- setup [62](#)

IP source guard [254](#)

- ARP inspection [254, 256](#)
- DHCP snooping [254](#)
- static bindings [254](#)

IP table [449](#)

- how it works [449](#)

IPv4 static route

- configuration [353](#)

IPv6 [22, 467](#)

- addressing [467](#)
- EUI-64 [469](#)
- global address [468](#)
- interface ID [469](#)
- link-local address [467](#)
- Neighbor Discovery Protocol [22, 467](#)
- ping [22, 467](#)
- prefix [467](#)
- prefix length [467](#)
- stateless autoconfiguration [469](#)
- unspecified address [468](#)

IPv6 static route

- configuration [354](#)

L

L2PT [285](#)

- access port [286](#)
- CDP [285](#)
- configuration [286](#)
- encapsulation [285](#)
- LACP [285](#)
- MAC address [285](#)
- mode [286](#)
- overview [285](#)
- PAgP [285](#)
- point to point [285](#)
- STP [285](#)
- tunnel port [286](#)
- UDLD [285](#)
- VTP [285](#)

LACP [163, 288](#)

- system priority [170](#)

- timeout [171](#)

Layer 2 protocol tunneling, see L2PT

LEDs [33](#)

limit MAC address learning [184](#)

Link Aggregate Control Protocol (LACP) [163](#)

link aggregation [163](#)

- dynamic [163](#)
- ID information [164](#)
- setup [165, 168](#)
- status [165](#)
- traffic distribution algorithm [165](#)
- traffic distribution type [168](#)

Link Layer Discovery Protocol (LLDP) [321, 322](#)

LLDP (Link Layer Discovery Protocol) [321](#)

LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) [322](#)

local port mirroring [151](#)

lockout [41](#)

log [435](#)

login [35](#)

- password [40](#)

login account

- Administrator [424](#)
- non-administrator [424](#)

login accounts [424](#)

- configuring via web configurator [424](#)
- multiple [424](#)
- number of [424](#)

login password [425](#)

loop guard [277](#)

- how it works [278](#)
- port shut down [278](#)
- probe packet [278](#)

loop guard, vs STP [277](#)

M

MAC (Media Access Control) [55](#)

MAC address [55, 395, 451](#)

- maximum number per port [184](#)

MAC address learning [61, 104, 106, 117, 183](#)

- specify limit [184](#)

MAC authentication [174](#)

- aging time [181](#)

MAC filter

- and ARP inspection [257](#)
 - MAC freeze [183](#)
 - MAC table [446](#)
 - how it works [446](#)
 - viewing [447](#)
 - MAC-based VLAN [115](#)
 - maintenance
 - configuration backup [405](#)
 - firmware [402](#)
 - restoring configuration [404](#)
 - maintenance [401](#)
 - current configuration [401](#)
 - main screen [401](#)
 - Management Information Base (MIB) [413](#)
 - management port [31](#), [113](#)
 - default IP address [31](#)
 - managing the device
 - good habits [23](#)
 - 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 [256](#)
 - max
 - age [141](#)
 - hops [141](#)
 - maximum transmission unit [454](#)
 - Memory Buffer [407](#)
 - MGMT port [31](#)
 - MIB
 - and SNMP [413](#)
 - supported MIBs [414](#)
 - MIB (Management Information Base) [413](#)
 - mini GBIC ports [30](#)
 - connection speed [30](#)
 - connector type [30](#)
 - transceiver installation [30](#)
 - transceiver removal [31](#)
 - mirroring ports [151](#)
 - monitor port [154](#), [155](#)
 - MSA (MultiSource Agreement) [30](#)
 - MST Instance, See MSTI [129](#)
 - MST region [128](#)
 - MSTI [129](#)
 - MST ID [129](#)
 - MSTI (Multiple Spanning Tree Instance) [127](#)
 - MSTP [125](#), [127](#)
 - bridge ID [145](#)
 - configuration [138](#), [142](#)
 - configuration digest [145](#)
 - forwarding delay [141](#)
 - Hello Time [145](#)
 - hello time [141](#)
 - Max Age [145](#)
 - max age [141](#)
 - max hops [141](#)
 - MST region [128](#)
 - network example [127](#)
 - path cost [142](#)
 - port priority [142](#)
 - revision level [141](#)
 - MSTP (Multiple Spanning Tree Protocol) [125](#)
 - MTU [454](#)
 - MTU (Multi-Tenant Unit) [60](#)
 - multicast [214](#)
 - 802.1 priority [219](#), [225](#), [226](#), [229](#), [230](#)
 - and IGMP [214](#)
 - IGMP throttling [221](#)
 - IP addresses [214](#)
 - overview [214](#)
 - setup [217](#), [219](#), [225](#), [226](#), [227](#), [229](#), [230](#)
 - multicast group [223](#)
 - multicast VLAN [237](#)
 - Multiple Spanning Tree Instance, See MSTI [127](#)
 - Multiple Spanning Tree Protocol [126](#)
 - Multiple Spanning Tree Protocol, See MSTP. [125](#)
 - Multiple STP [126](#)
 - Multiple STP, see MSTP [127](#)
 - MVR [232](#)
 - configuration [234](#)
 - group configuration [237](#)
 - network example [232](#)
 - MVR (Multicast VLAN Registration) [232](#)
- ## N
- network management system (NMS) [412](#)
 - NTP (RFC-1305) [59](#)

O

other documentation [2](#)

P

PAGP [288](#)

password [40](#)
 administrator [425](#)

Path MTU [454](#)

Path MTU Discovery [454](#)

PHB (Per-Hop Behavior) [360](#)

ping, test connection [435](#)

PoE [67](#)

policy [198, 199, 358](#)
 and classifier [198, 358](#)
 and DiffServ [196](#)
 configuration [198, 358](#)
 example [200](#)
 overview [196](#)
 rules [196](#)
 viewing [199](#)

policy configuration [199](#)

policy routing
 benefits [356](#)
 cost savings [356](#)
 load sharing [356](#)
 overview [356](#)

policy-based routing [356](#)

Port Aggregation Protocol, see PAGP

port authentication [173](#)
 and RADIUS [242](#)
 IEEE802.1x [175, 180, 244](#)
 MAC authentication [174](#)

port based VLAN type [61](#)

port cloning [455, 456](#)
 advanced settings [455, 456](#)
 basic settings [455, 456](#)

port details [50](#)

port isolation [113](#)

port mirroring [151, 155](#)
 direction [155, 158](#)
 egress [155, 158](#)
 ingress [155, 158](#)

port redundancy [163](#)

port security [182, 186](#)
 address learning [183](#)
 limit MAC address learning [184](#)
 MAC address learning [182, 186](#)
 overview [182, 186](#)
 setup [182, 186, 279, 286](#)

port setup [64](#)

port status [47](#)

port VLAN trunking [96](#)

port-based VLAN [109](#)
 all connected [113](#)
 port isolation [113](#)
 settings wizard [113](#)

ports
 “standby” [163](#)
 diagnostics [436](#)
 mirroring [151](#)
 speed/duplex [66](#)

power
 voltage [56, 57](#)

power module
 disconnecting [32](#)

Power over Ethernet [67](#)

power status [56, 57](#)

PPPoE IA
 trusted ports [296](#)
 untrusted ports [296](#)

priority level [62](#)

priority, queue assignment [62](#)

private VLAN status [109](#)

product registration [486](#)

protocol based VLAN [106](#)
 and IEEE 802.1Q tagging [106](#)
 example [108](#)
 hexadecimal notation for protocols [105, 107](#)
 isolate traffic [106](#)
 priority [105, 107](#)

PVID [94, 103](#)

PVID (Priority Frame) [94](#)

Q

QoS
 and classifier [188](#)
 queue weight [203](#)

queuing [202](#)

 SPQ [203](#)

 WFQ [203](#)

 WRR [203](#)

queuing method [202](#), [204](#)

R

RADIUS [242](#)

 advantages [242](#)

 and authentication [242](#)

 Network example [241](#)

 server [242](#)

 settings [242](#)

 setup [242](#)

Rapid Spanning Tree Protocol, See RSTP. [125](#)

reboot

 load configuration [406](#)

reboot system [406](#)

reflector port [151](#)

registration

 product [486](#)

related documentation [2](#)

remote management [433](#)

 service [434](#)

 trusted computers [434](#)

remote port mirroring [151](#), [155](#)

Removing the Fan Module [32](#)

resetting [41](#), [405](#), [406](#), [407](#)

 to factory default settings [405](#), [406](#), [407](#)

restoring configuration [41](#), [404](#)

RFC 3164 [437](#)

RMirror [151](#)

 monitor port [156](#)

 reflector port [156](#)

 source [156](#)

RMirror, see also remote port mirroring [155](#)

Round Robin Scheduling [203](#)

routing domain [63](#), [385](#)

routing table [453](#)

RSTP [125](#)

rubber feet [24](#)

S

save configuration [41](#), [406](#)

Secure Shell See SSH

service access control [432](#)

 service port [433](#)

sFlow [290](#)

 collector [292](#)

 configuration [290](#)

 datagram [290](#)

 overview [290](#)

 poll interval [292](#)

 sample rate [292](#)

 UDP port [293](#)

sFlow agent [290](#)

sFlow collector [290](#)

Simple Network Management Protocol, see SNMP

SNMP [23](#), [412](#)

 agent [413](#)

 and MIB [413](#)

 authentication [423](#)

 communities [419](#)

 management model [413](#)

 manager [413](#)

 MIB [414](#)

 network components [413](#)

 object variables [413](#)

 protocol operations [413](#)

 security [423](#)

 setup [418](#)

 traps [420](#)

 users [422](#)

 version 3 and security [413](#)

 versions supported [412](#)

SNMP traps [414](#)

 supported [414](#), [416](#), [418](#)

source-based routing [356](#)

Spanning Tree Protocol, See STP. [125](#)

SPQ (Strict Priority Queuing) [203](#)

SSH

 encryption methods [427](#)

 how it works [426](#)

 implementation [427](#)

SSH (Secure Shell) [425](#)

SSL (Secure Socket Layer) [427](#)

standby ports [163](#)

static bindings [254](#)

- static MAC address [117](#)
- static MAC forwarding [104](#), [106](#), [117](#)
- static multicast address [120](#)
- static multicast forwarding [120](#)
- static route
 - overview [352](#)
- static routes [354](#)
- static trunking example [171](#)
- Static VLAN [99](#)
- static VLAN
 - control [101](#)
 - tagging [101](#)
- status [47](#)
 - LED [33](#)
 - link aggregation [165](#)
 - port [47](#)
 - port details [50](#)
 - power [56](#), [57](#)
 - STP [133](#), [137](#), [144](#)
 - VLAN [97](#)
 - VRRP [385](#)
- STP [125](#), [288](#)
 - bridge ID [134](#), [137](#)
 - bridge priority [132](#), [136](#)
 - configuration [131](#), [134](#), [138](#)
 - designated bridge [126](#)
 - forwarding delay [133](#), [136](#)
 - Hello BPDU [126](#)
 - Hello Time [132](#), [134](#), [136](#), [138](#)
 - how it works [126](#)
 - Max Age [132](#), [134](#), [136](#), [138](#)
 - path cost [125](#), [133](#), [137](#)
 - port priority [133](#), [137](#)
 - port state [126](#)
 - root port [126](#)
 - status [133](#), [137](#), [144](#)
 - terminology [125](#)
 - vs loop guard [277](#)
- subnet based VLANs [103](#)
 - and DHCP VLAN [105](#)
 - and priority [104](#)
 - configuration [104](#)
- switch lockout [41](#)
- switch reset [41](#)
- switch setup [60](#)
- syslog [257](#), [437](#)
 - protocol [437](#)

- server setup [438](#)
- settings [437](#)
- setup [437](#)
- severity levels [437](#)
- system information [54](#)
- system log [435](#)
- system reboot [406](#)

T

- TACACS+ [242](#)
 - setup [244](#)
- TACACS+ (Terminal Access Controller Access-Control System Plus) [241](#)
- tagged VLAN [94](#)
- Tech-Support [407](#)
- temperature indicator [55](#), [56](#), [57](#)
- time
 - current [59](#)
 - time zone [59](#)
- Time (RFC-868) [59](#)
- time server [59](#)
- time service protocol [59](#)
 - format [59](#)
- trademarks [486](#)
- transceiver
 - installation [30](#)
 - removal [31](#)
- traps
 - destination [419](#)
- TRTCM
 - and bandwidth control [364](#)
 - and DiffServ [365](#)
 - color-aware mode [362](#)
 - color-blind mode [362](#)
 - setup [364](#)
- trunk group [163](#)
- trunking [163](#)
 - example [171](#)
- trusted ports
 - ARP inspection [257](#)
 - DHCP snooping [255](#)
 - PPPoE IA [296](#)
- Tunnel Protocol Attribute, and RADIUS [250](#)
- Two Rate Three Color Marker (TRTCM) [361](#)

Two Rate Three Color Marker, see TRTCM [361](#)
Type of Service (ToS) [360](#)

U

UDLD [288](#)
UniDirectional Link Detection, see UDLD
untrusted ports
 ARP inspection [257](#)
 DHCP snooping [255](#)
 PPPoE IA [296](#)
user profiles [241](#)

V

Vendor Specific Attribute See VSA
ventilation holes [24](#)
VID [64](#), [94](#), [97](#), [98](#), [208](#)
 number of possible VIDs [94](#)
 priority frame [94](#)
VID (VLAN Identifier) [94](#)
Virtual Router
 status [385](#)
Virtual Router (VR) [384](#)
Virtual Router Redundancy Protocol (VRRP) [384](#)
VLAN [60](#), [94](#)
 acceptable frame type [103](#)
 automatic registration [95](#)
 ID [94](#)
 ingress filtering [103](#)
 introduction [60](#)
 number of VLANs [97](#)
 port number [98](#)
 port settings [101](#)
 port-based VLAN [109](#)
 port-based, all connected [113](#)
 port-based, isolation [113](#)
 port-based, wizard [113](#)
 private VLAN [109](#)
 static VLAN [99](#)
 status [97](#), [98](#)
 tagged [94](#)
 trunking [96](#), [103](#)
 type [61](#), [96](#)

VLAN (Virtual Local Area Network) [60](#)
VLAN mapping [281](#)
 activating [281](#)
 configuration [283](#)
 example [281](#)
 priority level [281](#)
 tagged [281](#)
 traffic flow [281](#)
 untagged [281](#)
 VLAN ID [281](#)
VLAN number [64](#)
VLAN stacking [206](#), [208](#)
 configuration [208](#)
 example [206](#)
 frame format [208](#)
 port roles [207](#), [210](#)
 port-based Q-in-Q [210](#)
 priority [208](#)
 selective Q-in-Q [212](#)
VLAN Trunking Protocol, see VTP
VLAN, protocol based, See protocol based VLAN
VLAN, subnet based, See subnet based VLANs [103](#)
VRID (Virtual Router ID) [385](#)
VRRP [384](#)
 advertisement interval [387](#)
 authentication [386](#)
 backup router [384](#)
 configuration example [389](#)
 Hello message [387](#)
 how it works [384](#)
 interface setup [385](#)
 master router [384](#)
 network example [384](#), [389](#)
 parameters [387](#)
 preempt mode [387](#), [388](#)
 priority [387](#), [388](#)
 status [385](#)
 uplink gateway [388](#)
 uplink status [385](#)
 Virtual Router [384](#)
 Virtual Router ID [388](#)
 VRID [385](#)
VSA [249](#)
VTP [288](#)

W

warranty [486](#)

note [486](#)

web configurator [23](#), [35](#)

getting help [43](#)

layout [36](#)

login [35](#)

logout [42](#)

navigation panel [37](#)

weight, queuing [203](#)

Weighted Round Robin Scheduling (WRR) [203](#)

WFQ (Weighted Fair Queuing) [203](#)

WRR (Weighted Round Robin Scheduling) [203](#)

Z

ZON Neighbor Management [46](#)

ZON Utility [45](#)

ZyNOS (ZyXEL Network Operating System) [409](#)