

User's Guide

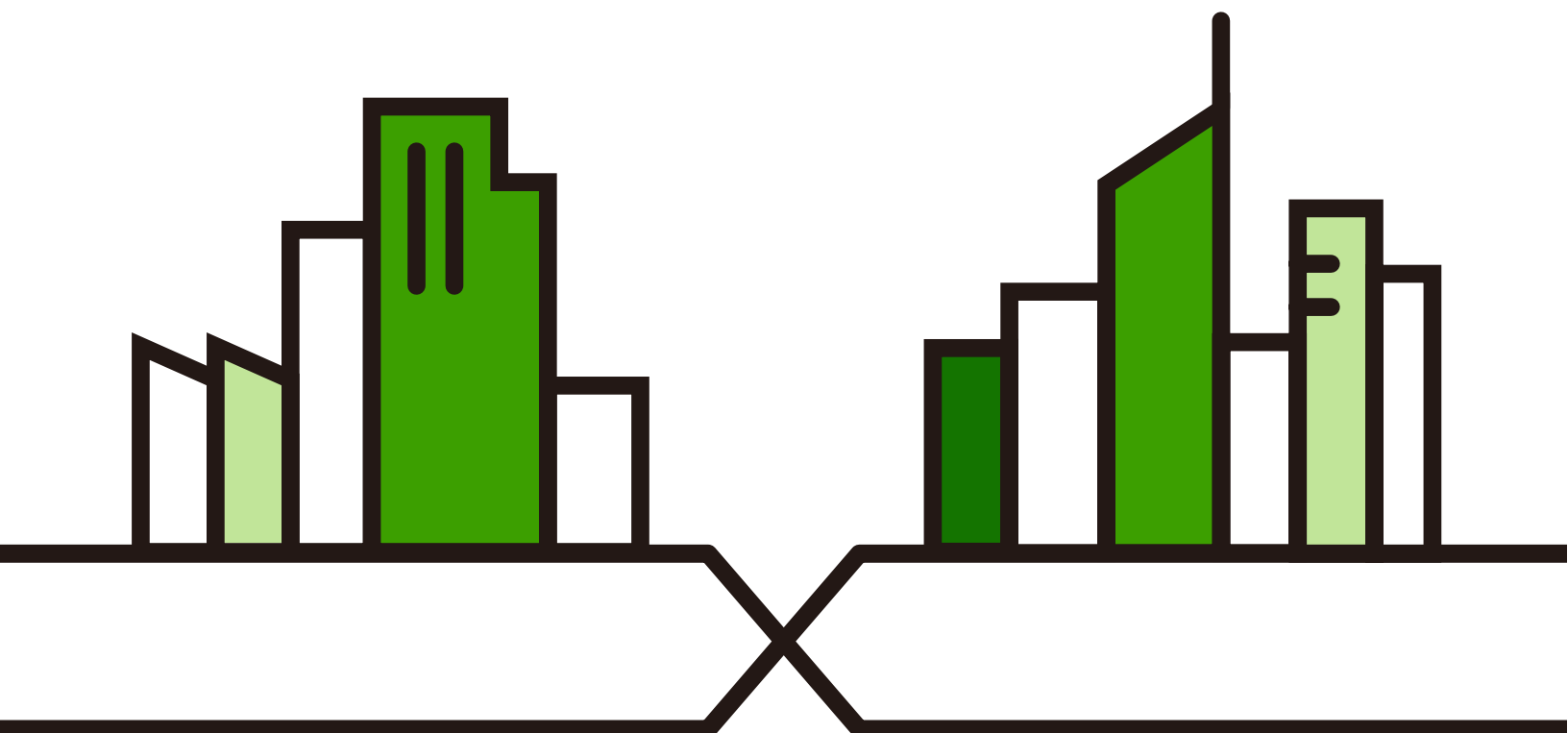
CX4800-56F

48-port 10G/25G L3 Aggregation Fiber Switch with 8 100G Uplinks

Default Login Details

Version 1.00 Edition 2, 03/2025

LAN IP Address	https://setup.zyxel or https://DHCP-assigned IP or https://192.168.1.1
User Name	admin
Password	On the back label on the Switch or Local Credential Password (Cloud Mode)



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

This User's Guide is for the platform version listed on the cover. 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.

Note: The version number on the cover page refers to the Switch's latest firmware version to which this User's Guide applies.

Related Documentation

- Quick Start Guide

The Quick Start Guide shows how to connect the Switch.

- Web Configurator Online Help

Click the help link for a description of the fields in the Switch menus.

- Nebula Control Center (NCC) User's Guide

Go to nebula.zyxel.com or support.zyxel.com to get this User's Guide on how to configure the Switch using Nebula.

- More Information

Go to <https://community.zyxel.com/en> for product discussions.

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



Document Conventions

Warnings and Notes

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

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

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

Syntax Conventions

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

Icons Used in Figures

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

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

Contents Overview

User's Guide	23
Getting to Know Your Switch	24
Hardware Installation and Connection	33
Hardware Panels	37
Technical Reference	48
Web Configurator	49
Initial Setup Example	82
DASHBOARD	99
MONITOR	104
ARP Table	105
IP Table	107
MAC Table	109
Neighbor	112
Port Status	116
Routing Table	123
System Information	125
System Log	129
SYSTEM	130
Cloud Management	131
General Setup	133
IP Setup	137
Logins	145
SNMP	147
Switch Setup	159
Syslog Setup	162
Time Range	165
PORT	168
Flex Link	169
Link Aggregation	172
Link Layer Discovery Protocol (LLDP)	180
Port Setup	202
SWITCHING	206
Loop Guard	207
Mirroring	210
Multicast	213
Static Multicast Forwarding	231
Private VLAN	234

Differentiated Services	238
Queuing Method	242
Priority Queue	245
sFlow	247
Spanning Tree Protocol	251
Static MAC Filtering	274
Static MAC Forwarding	276
VLAN	278
VLAN Mapping	297
VLAN Stacking	301
WoL Relay	308
NETWORKING	310
ARP Setup	311
DHCP	317
Static Route	334
SECURITY	337
AAA	338
Access Control	352
Classifier	362
Policy Rule	372
Anti-Arpscan	378
BPDU Guard	384
Storm Control	387
Error-Disable	389
IP Source Guard	395
DHCP Snooping	400
ARP Inspection	412
Port Authentication	420
Port Security	432
MAINTENANCE	436
Networked AV Mode	466
Troubleshooting and Appendices	525
Troubleshooting	526

Table of Contents

Document Conventions	3
Contents Overview	4
Table of Contents	6
Part I: User's Guide.....	23
Chapter 1	
Getting to Know Your Switch	24
1.1 Introduction	24
1.2 Example Applications	24
1.2.1 Backbone Example Application	25
1.2.2 Bridging with Fiber Optic Uplink Example Application	25
1.2.3 High Performance Switching Example	26
1.2.4 IEEE 802.1Q VLAN Application Examples	26
1.3 Ways to Manage the Switch	27
1.4 Management Modes	27
1.4.1 Mode Changing	29
1.4.2 ZON Utility	31
1.4.3 Web Configurator Networked AV Mode	32
1.5 Good Habits for Managing the Switch	32
Chapter 2	
Hardware Installation and Connection	33
2.1 Safety Precautions	33
2.2 Freestanding Installation Procedure	33
2.3 Mount the Switch on a Rack	34
2.3.1 Installation Requirements	34
2.3.2 Precautions	34
2.3.3 Attaching the Mounting Brackets to the Switch	34
2.3.4 Mounting the Switch on a Rack	35
Chapter 3	
Hardware Panels.....	37
3.1 Switch Hardware Features	37
3.2 Front Panel Connections	37
3.2.1 SFP28 / QSFP28 Slots	38

3.2.2 Management Port	40
3.2.3 Console Port	40
3.3 Rear Panel	40
3.3.1 Grounding	41
3.3.2 Power Module Installation and Removal	42
3.3.3 AC Power Connection (AC Models Only)	44
3.3.4 DC Power Connection (DC Models Only)	44
3.3.5 Fan Installation and Removal	45
3.4 LEDs	46

Part II: Technical Reference..... 48

Chapter 4 Web Configurator.....49

4.1 Overview	49
4.2 System Login	49
4.3 Zyxel One Network (ZON) Utility	56
4.3.1 Requirements	56
4.3.2 Run the ZON Utility	56
4.4 Networked AV Mode Wizard	59
4.4.1 Basic Settings	60
4.4.2 Advanced Settings	65
4.5 Web Configurator Layout	70
4.5.1 Tables and Lists	78
4.6 Save Your Configuration	79
4.7 Switch Lockout	79
4.8 Restoring the Switch to the Factory Defaults	80
4.8.1 Reboot the Switch	80
4.9 Log Out of the Web Configurator	81
4.10 Help	81

Chapter 5 Initial Setup Example 82

5.1 Overview	82
5.2 Configure Switch Management IP Address	82
5.3 Change the Administrator Login Password	84
5.4 Create a VLAN	84
5.5 Set Port VID	85
5.5.1 Configure Switch Management IP Address	86
5.6 How to Use DHCPv4 Relay on the Switch	88
5.6.1 DHCP Relay Tutorial Introduction	88

5.6.2 Create a VLAN	89
5.6.3 Configure DHCPv4 Relay	91
5.6.4 Troubleshooting	91
5.7 How to Use Auto Configuration through a DHCP Server on the Switch	92
5.8 How to Back Up the Configuration	94
5.9 How to Restore the Configuration	95
5.10 How to Upgrade the Firmware	96
5.10.1 Firmware Upgrade Through NCC	96
5.10.2 Firmware Upgrade Through the Web Configurator	97
Chapter 6	
DASHBOARD	99
6.1 User Interface	99
6.2 DASHBOARD	99
6.2.1 Port Status	102
6.2.2 Quick Links to Use	102
Chapter 7	
MONITOR.....	104
Chapter 8	
ARP Table.....	105
8.1 ARP Table Overview	105
8.1.1 What You Can Do	105
8.1.2 What You Need to Know	105
8.2 Viewing the ARP Table	105
Chapter 9	
IP Table.....	107
9.1 IP Table Overview	107
9.2 Viewing the IP Table	108
Chapter 10	
MAC Table	109
10.1 MAC Table Overview	109
10.1.1 What You Can Do	109
10.1.2 What You Need to Know	109
10.2 Viewing the MAC Table	110
Chapter 11	
Neighbor	112
11.1 Neighbor Overview	112
11.1.1 What You Can Do	112
11.2 Neighbor	112

11.2.1 Neighbor Details	113
Chapter 12	
Port Status	116
12.0.1 What You Can Do	116
12.1 Port Status	116
12.1.1 Port Details	117
12.2 DDMI	119
12.2.1 DDMI Details	120
12.3 Port Utilization	121
Chapter 13	
Routing Table.....	123
13.1 Routing Table Overview	123
13.1.1 What You Can Do	123
13.2 IPv4 Routing Table	123
Chapter 14	
System Information	125
14.0.1 What You Can Do	125
14.1 System Information	125
Chapter 15	
System Log.....	129
15.1 System Log Overview	129
15.2 System Log	129
Chapter 16	
SYSTEM	130
Chapter 17	
Cloud Management.....	131
17.1 Cloud Management Overview	131
17.2 Nebula Center Control Discovery	131
Chapter 18	
General Setup	133
18.1 General Setup	133
18.2 Hardware Monitor Setup	135
Chapter 19	
IP Setup	137
19.1 IP Setup Overview	137
19.1.1 What You Can Do	137

19.1.2 IP Interfaces	137
19.2 IP Status	138
19.2.1 IP Status Details	138
19.3 IP Setup	140
19.3.1 Add/Edit IP Interfaces	142
19.4 Network Proxy Configuration	143
Chapter 20	
Logins	145
20.1 Set Up Login Accounts	145
Chapter 21	
SNMP	147
21.1 SNMP Overview	147
21.1.1 What You Can Do	147
21.2 Configure SNMP	147
21.3 Configure SNMP User	149
21.3.1 Add/Edit SNMP User	150
21.4 SNMP Trap Group	151
21.5 Enable or Disable Sending of SNMP Traps on a Port	152
21.6 Technical Reference	153
21.6.1 About SNMP	153
Chapter 22	
Switch Setup	159
22.1 Switch Setup Overview	159
22.1.1 Introduction to VLANs	159
22.2 Switch Setup	159
Chapter 23	
Syslog Setup	162
23.1 Syslog Overview	162
23.1.1 What You Can Do	162
23.2 Syslog Setup	162
23.2.1 Add/Edit a Syslog Server	164
Chapter 24	
Time Range	165
24.1 Time Range Overview	165
24.1.1 What You Can Do	165
24.2 Configure a Time Range	165
24.2.1 Add/Edit Time Range	166

Chapter 25	
PORT	168
Chapter 26	
Flex Link	169
26.1 Flex Link Overview	169
26.1.1 What You Can Do	169
26.2 Flex Link Status	169
26.3 Flex Link Setup	170
26.3.1 Add/Edit Flex Link	171
Chapter 27	
Link Aggregation	172
27.1 Link Aggregation Overview	172
27.1.1 What You Can Do	172
27.1.2 What You Need to Know	172
27.2 Link Aggregation Status	173
27.3 Link Aggregation Setting	175
27.4 Link Aggregation Control Protocol	176
27.5 Technical Reference	178
27.5.1 Static Trunking Example	178
Chapter 28	
Link Layer Discovery Protocol (LLDP)	180
28.1 LLDP Overview	180
28.2 LLDP-MED Overview	181
28.2.1 What You Can Do – LLDP	182
28.2.2 What You Can Do – LLDP MED	182
28.3 LLDP Local Status	182
28.3.1 LLDP Local Port Status Details	184
28.4 LLDP Remote Status	187
28.4.1 LLDP Remote Port Status Details	188
28.5 LLDP Setup	192
28.6 Basic TLV Setting	194
28.7 Org-specific TLV Setting	195
28.8 LLDP-MED Setup	196
28.9 LLDP-MED Network Policy	197
28.9.1 Add/Edit LLDP-MED Network Policy	197
28.10 LLDP-MED Location	198
28.10.1 Add/Edit LLDP-MED Location	199
Chapter 29	
Port Setup.....	202

29.1 Port Setup	202
29.2 Technical Reference	204
29.2.1 CL (Clause) Types and Applications	204
29.2.2 FEC Types and Transceivers	205
29.2.3 FEC Types and Negotiation Results	205
Chapter 30	
SWITCHING.....	206
Chapter 31	
Loop Guard	207
31.1 Loop Guard Overview	207
31.1.1 What You Can Do	207
31.1.2 What You Need to Know	207
31.2 Loop Guard Setup	208
Chapter 32	
Mirroring.....	210
32.1 Mirroring Overview	210
32.1.1 What You Need to Know	210
32.2 Local Port Mirroring	211
Chapter 33	
Multicast.....	213
33.1 Multicast Overview	213
33.1.1 What You Can Do – IPv4 Multicast	213
33.1.2 What You Can Do – MVR	213
33.1.3 What You Need to Know	213
33.2 IPv4 Multicast Status	217
33.3 IGMP Snooping	217
33.4 IGMP Snooping VLAN	221
33.4.1 Add/Edit IGMP Snooping VLANs	222
33.5 IGMP Filtering Profile	222
33.5.1 Add IGMP Filtering Profile	223
33.5.2 Add IGMP Filtering Rule	224
33.6 MVR Configuration	225
33.6.1 Add/Edit MVR	225
33.7 MVR Group Setup	227
33.7.1 Add/Edit MVR Group	228
33.7.2 MVR Configuration Example	228
Chapter 34	
Static Multicast Forwarding.....	231
34.1 Static Multicast Forwarding Overview	231

34.1.1 What You Can Do	231
34.1.2 What You Need To Know	231
34.2 Static Multicast Forwarding By MAC	232
34.2.1 Add/Edit Static Multicast Forwarding By MAC	232
Chapter 35	
Private VLAN.....	234
35.1 Private VLAN Overview	234
35.1.1 Private VLAN Configuration	235
Chapter 36	
Differentiated Services	238
36.1 DiffServ Overview	238
36.1.1 What You Can Do	238
36.1.2 What You Need to Know	238
36.2 Activate DiffServ	239
36.3 DSCP-to-IEEE 802.1p Priority Settings	240
36.3.1 Configure DSCP Settings	241
Chapter 37	
Queuing Method.....	242
37.1 Queuing Method Overview	242
37.1.1 What You Can Do	242
37.1.2 What You Need to Know	242
37.2 Configure Queuing	243
Chapter 38	
Priority Queue.....	245
38.1 Priority Queue Overview	245
38.1.1 What You Can Do	245
38.2 Assign Priority Queue	245
Chapter 39	
sFlow.....	247
39.1 sFlow Overview	247
39.2 sFlow Port Configuration	247
39.3 sFlow Collector Configuration	249
39.3.1 Add/Edit sFlow Collector	249
Chapter 40	
Spanning Tree Protocol	251
40.1 Spanning Tree Protocol Overview	251
40.1.1 What You Can Do	251

40.1.2 What You Need to Know	251
40.2 Spanning Tree Protocol Status	254
40.3 Spanning Tree Setup	254
40.4 Rapid Spanning Tree Protocol Status	256
40.5 Configure Rapid Spanning Tree Protocol	258
40.6 Multiple Rapid Spanning Tree Protocol	260
40.7 Configure Multiple Rapid Spanning Tree Protocol	262
40.8 Multiple Spanning Tree Protocol Status	265
40.9 Configure Multiple Spanning Tree Protocol	267
40.9.1 Add/Edit Multiple Spanning Tree	269
40.10 Multiple Spanning Tree Protocol Port Setup	270
40.11 Technical Reference	271
40.11.1 MSTP Network Example	272
40.11.2 MST Region	272
40.11.3 MST Instance	272
40.11.4 Common and Internal Spanning Tree (CIST)	273
Chapter 41	
Static MAC Filtering.....	274
41.1 Static MAC Filtering Overview	274
41.1.1 What You Can Do	274
41.2 Configure a Static MAC Filtering Rule	274
41.2.1 Add/Edit a Static MAC Filtering Rule	275
Chapter 42	
Static MAC Forwarding.....	276
42.1 Static MAC Forwarding Overview	276
42.1.1 What You Can Do	276
42.2 Configure Static MAC Forwarding	276
42.2.1 Add/Edit Static MAC Forwarding Rules	277
Chapter 43	
VLAN.....	278
43.1 VLAN Overview	278
43.1.1 What You Can Do	278
43.1.2 What You Need to Know	278
43.2 Introduction to IEEE 802.1Q Tagged VLANs	278
43.3 VLAN Status	281
43.3.1 VLAN Details	282
43.4 Private VLAN Status	283
43.5 Configure a Static VLAN	284
43.5.1 Add/Edit a Static VLAN	285
43.6 VLAN Port Setup	286

43.7 Configure GVRP	288
43.8 Subnet Based VLAN	289
43.9 Configuring Subnet Based VLAN	290
43.9.1 Add/Edit Subnet Based VLAN	290
43.10 Protocol Based VLAN	291
43.11 Configuring Protocol Based VLAN	292
43.11.1 Add/Edit a Protocol Based VLAN	293
43.12 MAC Based VLAN	294
43.12.1 Add/Edit a MAC Based VLAN	295
Chapter 44	
VLAN Mapping	297
44.1 VLAN Mapping Overview	297
44.1.1 VLAN Mapping Example	297
44.1.2 What You Can Do	297
44.2 Enable VLAN Mapping	298
44.3 VLAN Mapping Setup	298
44.3.1 Add/Edit VLAN Mapping	299
Chapter 45	
VLAN Stacking	301
45.1 VLAN Stacking Overview	301
45.1.1 VLAN Stacking Example	301
45.2 VLAN Stacking Port Roles	302
45.3 VLAN Tag Format	303
45.3.1 Frame Format	303
45.4 Configuring VLAN Stacking	304
45.5 Port-Based Q-in-Q	305
45.6 Selective Q-in-Q	306
45.6.1 Add/Edit Selective Q-in-Q	307
Chapter 46	
WoL Relay	308
46.1 WoL Relay Overview	308
46.2 WoL Relay	308
46.2.1 Add/Edit WoL Relay	309
Chapter 47	
NETWORKING	310
Chapter 48	
ARP Setup	311
48.1 ARP Overview	311
48.1.1 What You Can Do	311

48.1.2 What You Need to Know	311
48.2 ARP Learning	313
48.3 Static ARP	314
48.3.1 Add/Edit Static ARP	315
Chapter 49	
DHCP	317
49.1 DHCP Overview	317
49.1.1 What You Can Do	317
49.1.2 What You Need to Know	317
49.2 DHCPv4 Relay Status	318
49.3 DHCPv4 Relay	318
49.3.1 DHCPv4 Relay Agent Information	319
49.4 DHCPv4 Option 82 Profile	320
49.4.1 Add/Edit a DHCPv4 Option 82 Profile	320
49.5 Configure a DHCPv4 Smart Relay	322
49.5.1 Add/Edit DHCPv4 Global Relay Port	323
49.5.2 DHCP Smart Relay Configuration Example	323
49.6 DHCPv4 VLAN Setting	324
49.6.1 Add/Edit DHCPv4 VLAN Setting	325
49.6.2 Add/Edit DHCPv4 VLAN Port	326
49.7 DHCPv4 Server Status	327
49.7.1 DHCPv4 Server Status Details	328
49.8 DHCPv4 Server Setup	329
49.8.1 Add/Edit DHCPv4 Server	330
49.8.2 Example: DHCP Relay for Two VLANs	331
49.9 DHCP Server Guard	332
Chapter 50	
Static Route.....	334
50.1 Static Routing Overview	334
50.1.1 What You Can Do	334
50.2 IPv4 Static Route	335
50.2.1 Add/Edit IPv4 Static Route	335
Chapter 51	
SECURITY	337
Chapter 52	
AAA	338
52.1 Authentication, Authorization and Accounting (AAA)	338
52.1.1 What You Can Do	338
52.1.2 What You Need to Know	338
52.2 RADIUS Server Setup	339

52.3 TACACS+ Server Setup	341
52.4 AAA Setup	343
52.5 Technical Reference	346
52.5.1 Vendor Specific Attribute	346
52.5.2 Supported RADIUS Attributes	348
52.5.3 Attributes Used for Authentication	348
52.5.4 Attributes Used for Accounting	349
Chapter 53	
Access Control.....	352
53.1 Access Control Overview	352
53.1.1 What You Can Do	352
53.2 Service Access Control	352
53.3 Remote Management (IPv4)	353
53.4 Account Security	355
53.5 Technical Reference	356
53.5.1 SSH Overview	356
53.5.2 Introduction to HTTPS	358
53.5.3 Google Chrome Warning Messages	360
Chapter 54	
Classifier.....	362
54.1 Classifier Overview	362
54.1.1 What You Can Do	362
54.1.2 What You Need to Know	362
54.2 Classifier Status	363
54.3 Classifier Setup	363
54.3.1 Add/Edit a Classifier	365
54.4 Classifier Global Setting	369
54.5 Classifier Example	370
Chapter 55	
Policy Rule	372
55.1 Policy Rules Overview	372
55.1.1 What You Can Do	372
55.1.2 DiffServ	372
55.1.3 DSCP and Per-Hop Behavior	372
55.2 Policy Rules	373
55.2.1 Add/Edit a Policy Rule	373
55.3 Policy Example	376
Chapter 56	
Anti-Arpscan	378

56.1 Anti-Arpscan Overview	378
56.1.1 What You Can Do	378
56.1.2 What You Need to Know	378
56.2 Anti-Arpscan Status	379
56.3 Anti-Arpscan Host Status	379
56.4 Anti-Arpscan Setup	380
56.5 Anti-Arpscan Trust Host	382
56.5.1 Add/Edit Anti-Arpscan Trust Hosts	382
Chapter 57	
BPDU Guard	384
57.1 BPDU Guard Overview	384
57.1.1 What You Can Do	384
57.2 BPDU Guard Status	384
57.3 BPDU Guard Setup	385
Chapter 58	
Storm Control.....	387
58.1 Storm Control Overview	387
58.1.1 What You Can Do	387
58.2 Storm Control Setup	387
Chapter 59	
Error-Disable	389
59.1 Error-Disable Overview	389
59.1.1 CPU Protection Overview	389
59.1.2 Error-Disable Recovery Overview	389
59.1.3 What You Can Do	389
59.2 Error-Disable Status	390
59.3 CPU Protection Setup	391
59.4 Error-Disable Detect Setup	392
59.5 Error-Disable Recovery Setup	393
Chapter 60	
IP Source Guard	395
60.1 IP Source Guard Overview	395
60.1.1 What You Can Do	396
60.2 IPv4 Source Guard	396
60.3 IPv4 Source Guard Static Binding	397
60.3.1 Add/Edit IPv4 Source Guard Static Binding	398
Chapter 61	
DHCP Snooping	400

61.1 DHCP Snooping Overview	400
61.1.1 What You Can Do	401
61.2 DHCP Snooping Status	401
61.3 DHCP Snooping Setup	404
61.4 DHCP Snooping Port Setup	405
61.5 DHCP Snooping VLAN Setup	407
61.6 DHCP Snooping VLAN Port Setup	408
61.6.1 Add/EDIT DHCP Snooping VLAN Ports	408
61.7 Technical Reference	409
61.7.1 DHCP Snooping Overview	409
Chapter 62	
ARP Inspection	412
62.1 ARP Inspection Status	412
62.2 ARP Inspection VLAN Status	413
62.3 ARP Inspection Log Status	413
62.4 ARP Inspection Setup	414
62.5 ARP Inspection Port Setup	416
62.6 ARP Inspection VLAN Setup	417
62.7 Technical Reference	418
62.7.1 ARP Inspection Overview	418
Chapter 63	
Port Authentication	420
63.1 Port Authentication Overview	420
63.1.1 What You Can Do	420
63.1.2 What You Need to Know	421
63.1.3 MAC Authentication	421
63.2 Activate IEEE 802.1x Security	422
63.3 Activate MAC Authentication	423
63.4 Guest VLAN	425
63.5 Compound Authentication	427
63.6 Technical Reference	428
63.6.1 IEEE 802.1x	429
63.6.2 RADIUS	429
63.6.3 EAP (Extensible Authentication Protocol) Authentication	430
63.6.4 EAPOL (EAP over LAN)	431
Chapter 64	
Port Security	432
64.1 Port Security Overview	432
64.2 About Port Security	432
64.3 Port Security Setup	432

64.4 VLAN MAC Address Limit	434
64.4.1 VLAN MAC Address Limit	435

Chapter 65

MAINTENANCE.....436

65.1 Overview	436
65.1.1 What You Can Do	436
65.2 Certificates	437
65.2.1 Install Certificates	438
65.2.2 HTTPS Certificates	438
65.3 Technical Reference	438
65.3.1 FTP Command Line	438
65.3.2 Filename Conventions	439
65.3.3 FTP Command Line Procedure	439
65.3.4 GUI-based FTP Clients	440
65.3.5 FTP Restrictions	440
65.4 Cluster Management Overview	441
65.4.1 What You Can Do	441
65.5 Cluster Management Status	441
65.6 Clustering Management Setup	442
65.7 Technical Reference	444
65.7.1 Cluster Member Switch Management	444
65.8 Restore Configuration	446
65.9 Backup Configuration	446
65.10 Auto Configuration	447
65.11 Erase Running-Configuration	449
65.12 Save Configuration	449
65.13 Configure Clone	450
65.14 Diagnostic	452
65.15 Firmware Upgrade	453
65.16 Reboot System	455
65.17 SSH Authorized Keys	456
65.17.1 Generate the SSH Authorized Keys	457
65.18 SSH Host Keys	463
65.19 Tech-Support	463
65.19.1 Tech-Support Download	465

Chapter 66

Networked AV Mode.....466

66.1 Overview	466
66.2 Help	466
66.3 Summary	466
66.4 MONITOR	469

66.5 What You Can Do	469
66.6 System Information	469
66.7 SYSTEM	472
66.8 What You Can Do	472
66.9 Cloud Management	472
66.10 General Setup	474
66.11 IP Setup	476
66.11.1 Add/Edit IP Interfaces	477
66.12 Logins	478
66.13 Configure SNMP	480
66.14 Configure SNMP User	482
66.14.1 Add/Edit SNMP User	483
66.15 Configure SNMP Trap Group	484
66.16 Enable or Disable Sending of SNMP Traps on a Port	485
66.17 PORT	486
66.18 Link Aggregation	487
66.18.1 What You Can Do	487
66.19 Link Aggregation Status	487
66.20 Link Aggregation Setting	489
66.21 Link Aggregation Control Protocol	490
66.22 Port Setup	492
66.23 SWITCHING	494
66.24 Differentiated Services	494
66.25 DSCP-to-IEEE 802.1p Priority Settings	495
66.26 Port Mirroring	496
66.27 Multicast	498
66.27.1 What You Can Do	498
66.28 IPv4 Multicast Status	498
66.29 IGMP Snooping	499
66.30 IGMP Snooping VLAN	502
66.30.1 Add/Edit IGMP Snooping VLANs	503
66.31 IGMP Filtering Profile	504
66.31.1 Add IGMP Filtering Profile	505
66.31.2 Add IGMP Filtering Rule	506
66.32 Static Multicast Forwarding By MAC	506
66.33 VLAN	507
66.33.1 What You Can Do	507
66.33.2 What You Need to Know	507
66.34 VLAN Status	510
66.34.1 VLAN Details	511
66.35 Configure a Static VLAN	511
66.35.1 Add/Edit a Static VLAN	512
66.36 VLAN Port Setup	514

66.37 SECURITY	515
66.38 Access Control	515
66.38.1 What You Can Do	516
66.39 Service Access Control	516
66.40 Remote Management	517
66.41 Storm Control	519
66.42 MAINTENANCE	520
66.43 What You Can Do	520
66.44 Restore Configuration	520
66.45 Backup Configuration	521
66.46 Save Configuration	521
66.47 Firmware Upgrade	522
66.48 Reboot System	523
66.49 Tech-Support	524
66.49.1 Tech-Support Download	524

Part III: Troubleshooting and Appendices..... 525

Chapter 67

Troubleshooting.....526

67.1 Power, Hardware Connections, and LEDs	526
67.2 Switch Access and Login	527
67.3 Switch Configuration	529
67.4 Nebula Registration	531

Appendix A Customer Support 532

Appendix B Common Services..... 537

Appendix C IPv6..... 540

Appendix D Importing a Certificate 548

Appendix E Legal Information 561

Index 566

PART I

User's Guide

CHAPTER 1

Getting to Know Your Switch

1.1 Introduction

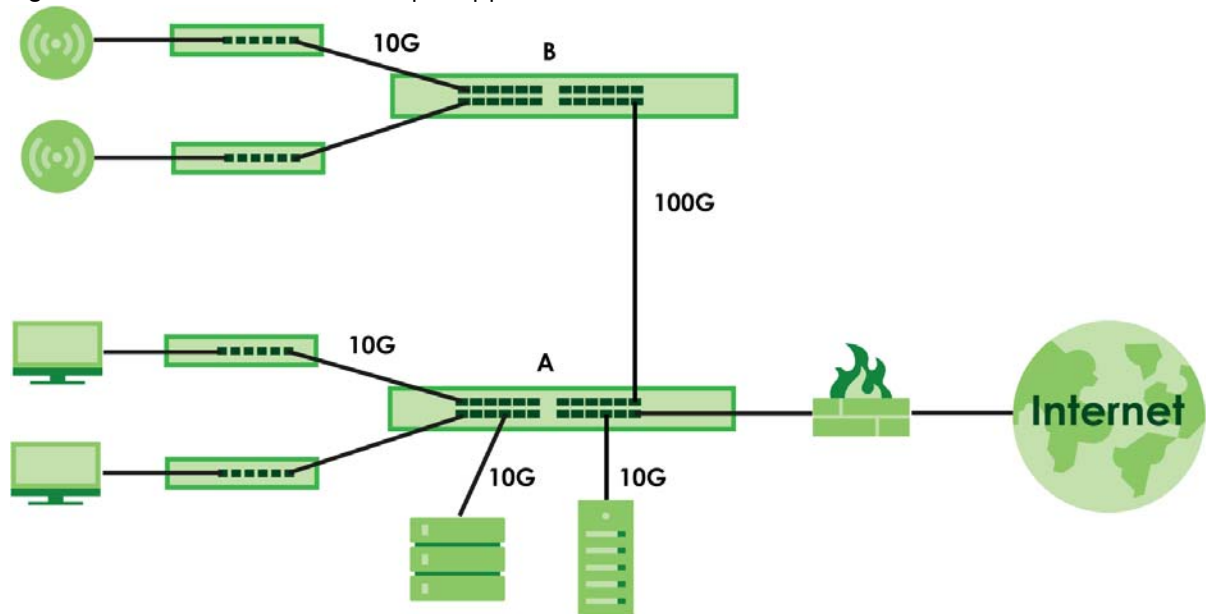
This User Guide is for the platform version listed on the cover. This chapter introduces the main features and applications of the Switch. CX4800-56F is referred to as the “Switch” in this guide.

Your Switch is a layer-3 100G managed fiber Switch. By integrating router functions, the Switch performs wire-speed layer-3 routing in addition to layer-2 switching.

The Switch uses redundant power supplies with hot-swappable capability to ensure no Switch downtimes in case of a power supply outage. The Switch also uses four hot-swappable fan modules to safeguard against fan failure and high operating temperatures.

In this example, there are two 100G Switches. A 100G port on one Switch (**A**) is connected to a 100G port on the other Switch (**B**). This connection provides a 100G uplink, suitable for high-speed data transmission in campus and enterprise network environments.

Figure 1 Two 100G Switches Example Application



1.2 Example Applications

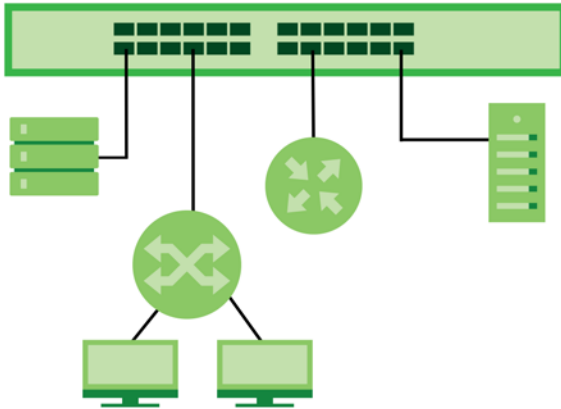
This section shows a few examples of using the Switch in various network environments. Note that the Switch in the figure is just an example Switch and not your actual Switch.

1.2.1 Backbone Example Application

The Switch is an ideal solution for small to medium-size networks with rapid growth. The Switch can be used standalone for a group of heavy traffic users. You can connect servers or other switches to the Switch.

In this example, all computers can share high speed applications across different networks. To expand the network, simply add more networking devices such as switches or routers.

Figure 2 Backbone Application

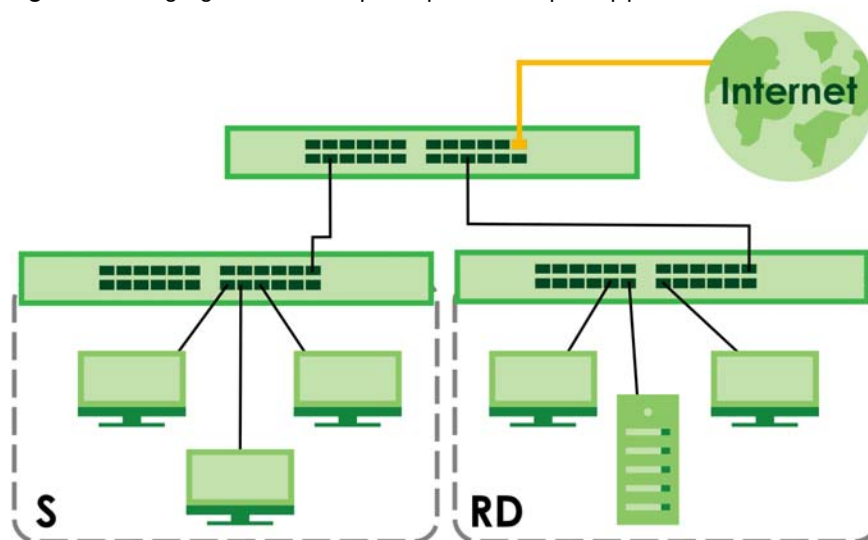


1.2.2 Bridging with Fiber Optic Uplink Example Application

In this example, the Switch connects different company departments (**RD** and Sales(**S**)) 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 through the Switch.

Moreover, the Switch eases supervision and maintenance by allowing network managers to centralize multiple servers at a single location.

Figure 3 Bridging with Fiber Optic Uplink Example Application



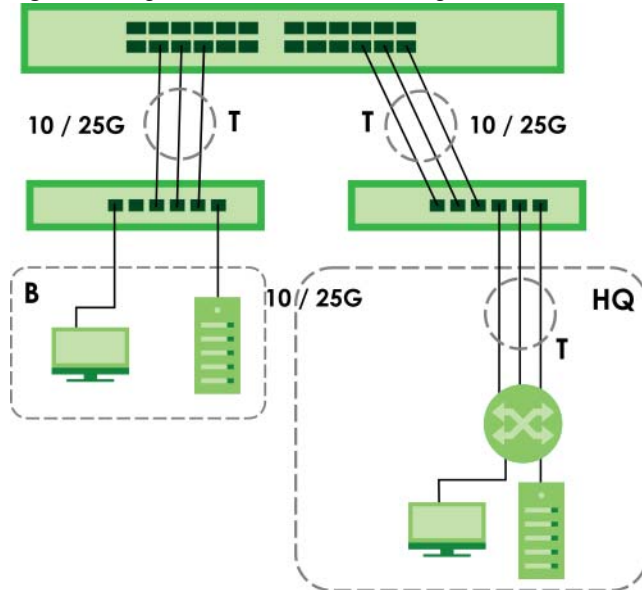
1.2.3 High Performance Switching Example

The Switch is ideal for connecting two geographically dispersed networks that need high bandwidth. In this example, a company uses the 10 or 25 Gigabit uplink ports to connect the headquarters (HQ) to a branch office (B) network. Within the headquarters network, a company can use trunking (T) to group several physical ports into one logical higher-capacity link. Trunking (T) 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.

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

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

Figure 4 High Performance Switching



1.2.4 IEEE 802.1Q VLAN Application Examples

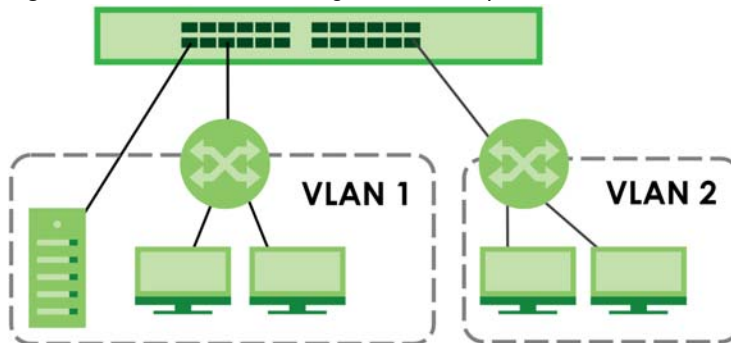
A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one or more groups. With VLAN, a station cannot directly talk to or hear from stations that are not in the same groups unless such traffic first goes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

1.2.4.1 Tag-based VLAN Example

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

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

Figure 5 Shared Server Using VLAN Example



1.3 Ways to Manage the Switch

Use any of the following methods to manage the Switch.

- **NCC (Zyxel Nebula Control Center).** With the NCC, you can remotely manage and monitor the Switch through a cloud-based network management system. See the NCC User's Guide for detailed information on how to access the NCC, manage your Switch through the NCC, and configure Nebula managed devices.
- **Web Configurator.** This is recommended for everyday management of the Switch using a (supported) web browser. See [Chapter 4 on page 49](#).
- **Command Line Interface.** Line commands offer an alternative to the Web Configurator and in some cases are necessary to configure advanced features. See the CLI Reference Guide.
- **FTP.** Use File Transfer Protocol for firmware upgrades and configuration backup or restore. See [Section 65.3.1 on page 438](#).
- **SNMP.** The Switch can be monitored and/or managed by an SNMP manager. See [Section 21.6.1 on page 153](#).
- **Cluster Management.** Cluster Management allows you to manage multiple switches through one switch, called the cluster manager. See [Chapter 65 on page 436](#).
- **ZON Utility.** ZON Utility is a program designed to help you deploy and perform initial setup on a network more efficiently. See [Section 4.3 on page 56](#).

Note: Telnet and SNMP management are disabled by default.

1.4 Management Modes

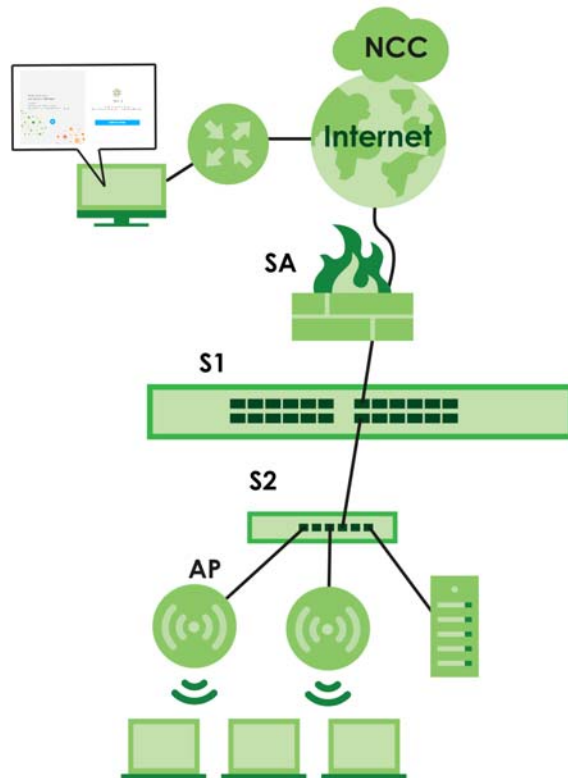
The Switch can operate in either standalone or Nebula cloud management mode. When the Switch is in standalone mode, it can be configured and managed by the Web Configurator. When the Switch is in Nebula cloud management mode, it can be managed and provisioned by the Zyxel Nebula Control Center (NCC).

Use the DHCP-assigned IP address or 192.168.1.1 to access the Web Configurator. To know the IP address, use the NCC, the ZON utility, or the console port if available. You can also use the domain name “setup.zyxel” to access the Web Configurator when you are directly connected to the Switch.

Note: Make sure your computer can connect to a DNS server through the Switch.

Use the Web Configurator to configure and manage the Switch directly in standalone mode or use Nebula Control Center (NCC) to configure and manage the Switch in cloud mode. The Nebula Control Center (NCC) is an alternative cloud-based network management system that allows you to remotely manage and monitor the Zyxel Nebula Security Appliances (**SA**), Ethernet Switches (**S1** and **S2**), and Access Points (**AP**). You may also access the Web Configurator in cloud mode.

Figure 6 NCC Example Network Topology



Nebula Cloud Management

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

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

See the NCC User’s Guide for how to configure the Switch using Nebula.

1.4.1 Mode Changing

This section describes how to change the Switch's management mode. Refer to the Switch's standalone mode User's Guide for LED descriptions, including **CLOUD** LED behavior.

From Standalone to Nebula Cloud Management

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

See the following steps or the Switch Quick Start Guide for registering the Switch.

Go to the NCC to Register the Switch

- 1 Go to the Nebula web portal in one of three ways.
 - Enter <https://nebula.zyxel.com> in a supported web browser. See the Nebula User's Guide for more information about supported browsers.
 - Click **Visit Nebula** in the Switch's login page.
 - Click the **Nebula Control Center** icon in the upper right of the Switch's Web Configurator.
- 2 Click **Get Started** in the Nebula web portal. Enter your Zyxel Account information. You will be redirected to another screen where you can sign up for a Zyxel Account if you do not have one.
- 3 Create an organization and a site (using the Nebula setup wizard) or select an existing site.
- 4 Register the Switch by entering its Registration MAC address and serial number and assign it to the site. The serial number and Registration MAC address can be found in the **DASHBOARD** screen or the device back label on the Switch.

Use the Zyxel Nebula Mobile App to Register the Switch

- 1 Download and open the Zyxel Nebula Mobile app in your mobile device (see [Section 17.2 on page 131](#) to download the app). Click **Start** on the first page. Click **Create account** to create a Zyxel Account or enter your existing account information to log in.
- 2 Create an organization and site, or select an existing site using the Zyxel Nebula Mobile app.
- 3 Select a site and scan the Switch's QR code or manually enter the information to add it to the site. You can find the QR code:
 - On a label on the Switch or
 - On its box or
 - In the Web Configurator at **SYSTEM > Cloud Management**.

Local Credentials Password

The Switch goes into Cloud mode automatically after it can access the Nebula web portal and is successfully registered there. Its login password and settings are then overwritten with what you have configured in the Nebula web portal. To access the Web Configurator when the Switch is in Cloud mode, use the Local credentials password to login.

Note: The **Local credentials: Password** can be found in **Site-wide > Configure > Site settings > Device configuration** in the NCC portal. See the NCC User's Guide for more information.

Figure 7 Site-wide > Configure > Site settings: Device configuration: Local credentials

Site-wide > Configure > **Site settings**

Site settings

Site information

Site name: ZyNet TW-2

Local time zone: Taiwan Asia - Taipei (UTC +8.0)

Site location: [Empty field]

[What is this?](#)

This site location will apply to your new added device(s) as address on map automatically.

Device configuration

Local credentials

Username: admin

Password: [Masked]

Password must be at least 8 characters in length and consists of letters and numerals. The valid characters are letters, numerals and symbols as follow: ~ ! @ # \$ % ^ & * () _ + ' - = { } ; : < > .

Table 1 Management Method Comparison

MODE	ACCESS	LOGIN USER NAME	LOGIN PASSWORD	LOGIN IP ADDRESS/URL/ DOMAIN NAME
Cloud mode	NCC (Nebula Control Center) portal	Zyxel Account email	Zyxel Account password	https://nebula.zyxel.com
	Web Configurator (Local GUI)	admin	Local credentials password	https://setup.zyxel OR https://DHCP-assigned IP OR a configured static IP address

Table 1 Management Method Comparison (continued)

MODE	ACCESS	LOGIN USER NAME	LOGIN PASSWORD	LOGIN IP ADDRESS/URL/ DOMAIN NAME
You can configure the Switch using both the NCC and the Web Configurator. Note: The latest configuration made in either the NCC or the Web Configurator will be applied to the Switch. Settings are pushed from the NCC to the Switch, but not from the Switch to the NCC. - The settings you configure in the NCC will appear in the Web Configurator settings and will be applied to the Switch. - The settings you configure in the Web Configurator will not appear in the NCC settings, but will be applied to the Switch. To avoid inconsistency, we recommend you use NCC to configure the Switch. Only use the Web Configurator for advanced settings not available in the NCC or for troubleshooting if you cannot access the NCC.				
Standalone mode	Web Configurator	admin	On the label on the back of the Switch	https://setup.zyxel OR https://DHCP-assigned IP OR https://192.168.1.1

From Nebula-managed to Standalone Mode

To return to direct management standalone mode, remove (unregister) the Switch from the inventory in the Nebula web portal.

Note: When you change the Switch's management mode from Cloud mode to standalone mode, the Switch will reboot and restore its factory-default settings.

To unregister the Switch:

- 1 Go to the Nebula Control Center (<https://nebula.zyxel.com>).
- 2 Go to the **Organization-wide > License & inventory > Devices** screen.
- 3 Select the Switch you want to remove (unregister) from the organization.
- 4 Click **Actions**, then click **Remove from organization**.

It will take a while for the Switch to reboot and reset to factory default.

1.4.2 ZON Utility

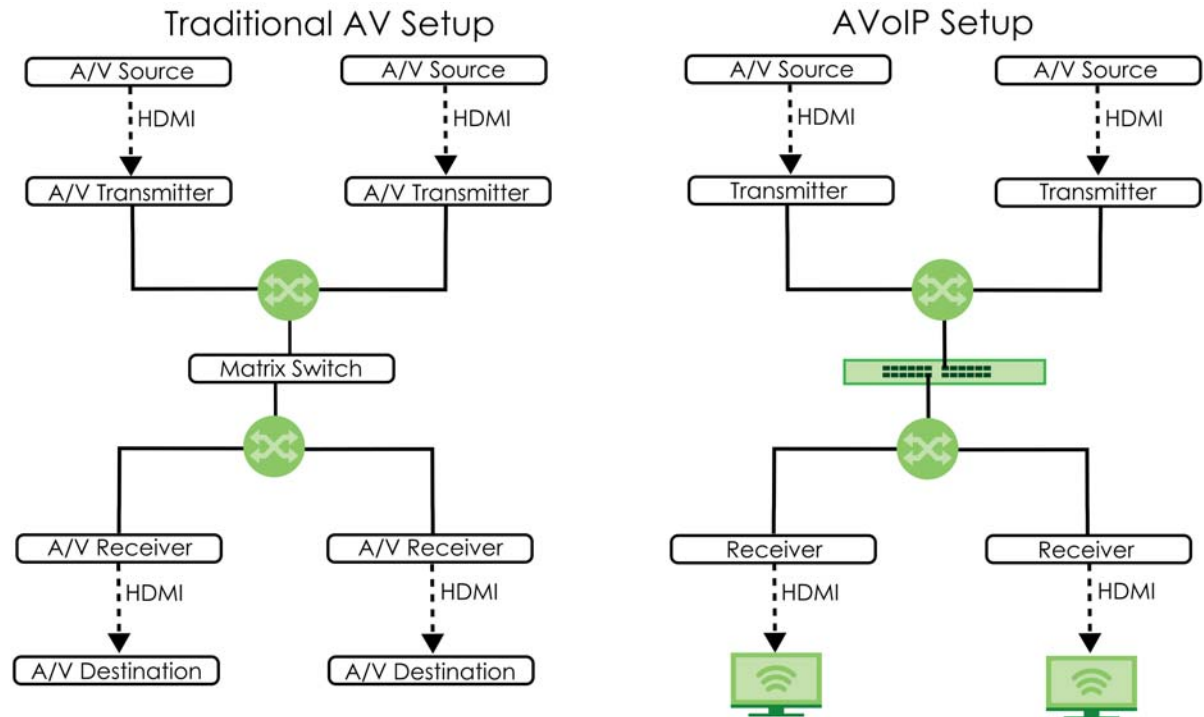
With its built-in Web Configurator, including the Neighbor Management feature ([Section 11.1 on page 112](#)), viewing, managing and configuring the Switch and its neighboring devices is simplified.

In addition, Zyxel offers a proprietary software program called Zyxel One Network (ZON) Utility, it is a utility tool that assists you to set up and maintain network devices in a more simple and efficient way. You can download the ZON Utility at www.zyxel.com and install it on a PC (Windows operation system). For more information on ZON Utility see [Section 4.3 on page 56](#).

1.4.3 Web Configurator Networked AV Mode

Aside from the Web Configurator in Standard mode, you can switch to Networked AV mode that is specifically designed to simplify configuration and management of the Switch for AVoIP (Audio-Video over Internet Protocol) application. In AV over IP, the AV transmitter is the transmitter, the AV receiver is the receiver, and the matrix switch is a standard IP Switch. See [Section 4.4 on page 59](#) for details on using the Setup Wizard screen for configuring the Switch's Networked AV mode's basic and advanced settings.

Figure 8 Comparison Between Traditional AV and AVoIP Setups



1.5 Good Habits for Managing the Switch

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

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

CHAPTER 2

Hardware Installation and Connection

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

The Switch can be:

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

2.1 Safety Precautions

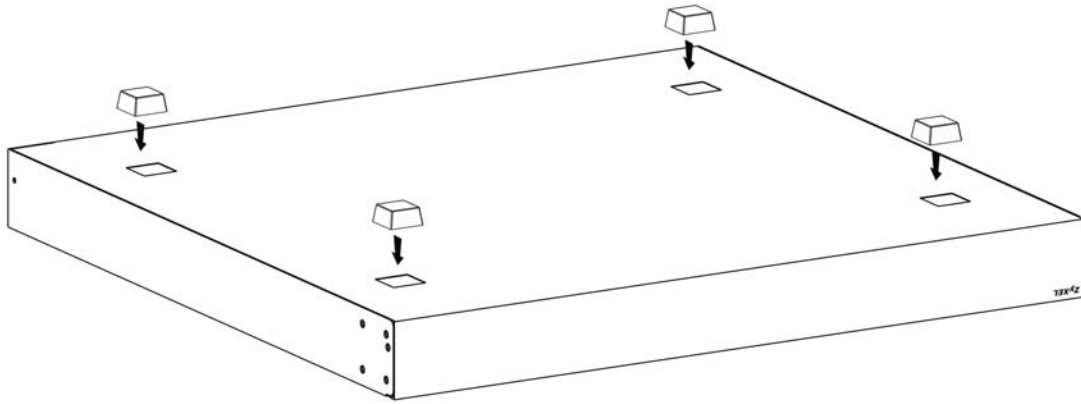
Please observe the following before using the Switch:

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

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

2.2 Freestanding Installation Procedure

- 1 Make sure the Switch is clean and dry.
- 2 Remove the adhesive backing from the rubber feet.
- 3 Attach the rubber feet to each corner on the bottom of the Switch. These rubber feet help protect the Switch from shock or vibration and ensure space between devices when stacking.

Figure 9 Attaching Rubber Feet

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

Cautions:

- Ensure enough clearance around the Switch to allow air circulation for cooling.
- Do NOT remove the rubber feet as it provides space for air circulation.

2.3 Mount the Switch on a Rack

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

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

2.3.1 Installation Requirements

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

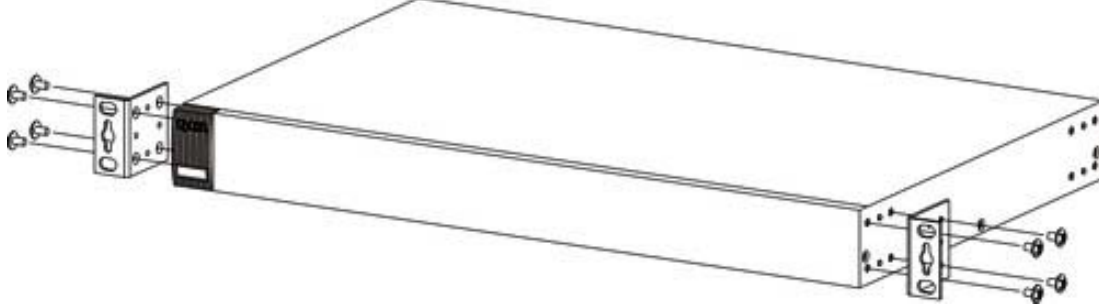
2.3.2 Precautions

- Make sure the rack will safely support the combined weight of all the equipment it contains. The maximum weight a bracket can hold is 21.5 kg.
- Make sure the position of the Switch does not make the rack unstable or top-heavy. Take all necessary precautions to anchor the rack securely before installing the unit.

2.3.3 Attaching the Mounting Brackets to the Switch

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

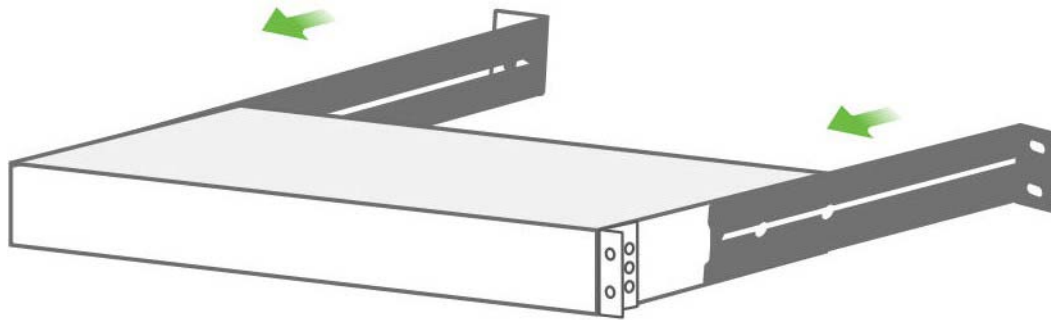
Figure 10 Attaching the Mounting Brackets



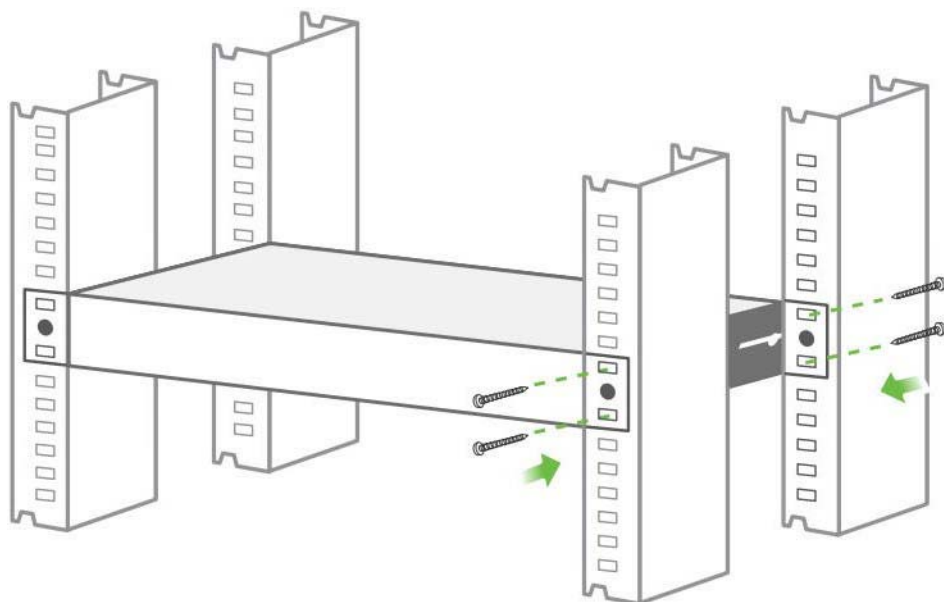
- 2 Using a #2 Philips screwdriver, install the M3 flat head screws through the mounting bracket holes into the Switch.
- 3 Repeat steps 1 and 2 to install the second mounting bracket on the other side of the Switch.
- 4 You may now mount the Switch on a rack. Proceed to the next section.

2.3.4 Mounting the Switch on a Rack

- 1 Slide the rails onto two sides of the Switch.



- 2 Adjust the rails to fit the rack. Align the two screw holes on a mounting bracket onto the rack. Then, screw the rail onto the rack at the back of the Switch. Repeat for the second mounting bracket on the other side of the Switch.



CHAPTER 3

Hardware Panels

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

3.1 Switch Hardware Features

The following table describes the hardware features of the Switch.

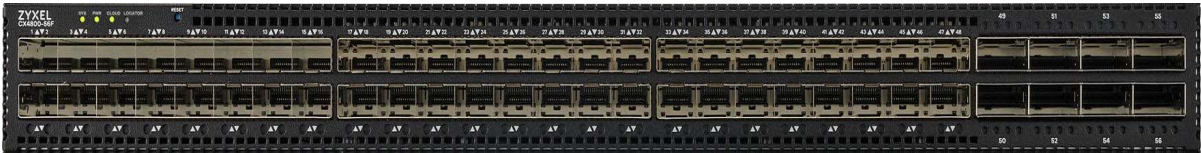
Table 2 CX4800-56F Feature Table

FEATURE	CX4800-56F
1/10/25 Gbps SFP28 Interface	48
25/100 Gbps QSFP28 Interface	8
Smart FAN	4
Console Port	RJ-45
Rack-mount	Yes
Management Port	Device back

3.2 Front Panel Connections

The following figure shows the front panel of the Switch.

Figure 11 Front Panel: CX4800-56F



The following table describes the ports.

Table 3 CX4800-56F Panel Connections

CONNECTOR	DESCRIPTION
Port 1 - 48 1G/10G/25G SFP28 Slots	Use SFP28 transceivers in these ports for high-bandwidth backbone connections.
Port 49 - 56 25G/100G QSFP28 Slots	Use QSFP28 transceivers in these ports for high-bandwidth backbone connections.
Reset	Press the RESET button for more than 5 seconds to reboot the Switch without turning the power off. See Section 3.4 on page 46 for more information about the LED behavior.
Console Port	Only connect this port to your computer (using a RJ-45 to RS-232 console cable) if you want to configure the Switch using a computer with terminal emulation software through the console port.

3.2.1 SFP28 / QSFP28 Slots

These are slots for SFP28 (Small Form-Factor Pluggable 28) transceivers. A transceiver is a single unit that houses a transmitter and a receiver. The Switch does not come with transceivers. You must use transceivers that comply with the Small Form-factor Pluggable 28 (SFP28) Transceiver MultiSource Agreement (MSA). See the SFF committee's specifications.

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

- Type: SFP28 or QSFP28 connection interface
- Connection speed: 1, 10, 25 or 100 Gigabit per second

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

HANDLING! All transceivers are static sensitive. To prevent damage from electrostatic discharge (ESD), it is recommended you attach an ESD preventive wrist strap to your wrist and to a bare metal surface when you install or remove a transceiver.

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

3.2.1.1 Transceiver Installation

Use the following steps to install a transceiver.

- 1 Attach an ESD preventive wrist strap to your wrist and to a bare metal surface.
- 2 Align the transceiver in front of the slot opening.
- 3 Make sure the latch is in the lock position (latch styles vary), then insert the transceiver into the slot with the exposed section of PCB board facing down.

- 4 Press the transceiver firmly until it clicks into place.
- 5 The Switch automatically detects the installed transceiver. Check the LEDs to verify that it is functioning properly.
- 6 Remove the dust plugs from the transceiver and cables (dust plug styles vary).
- 7 Identify the signal transmission direction of the fiber optic cables and the transceiver. Insert the fiber optic cable into the transceiver.

Figure 12 Latch in the Lock Position

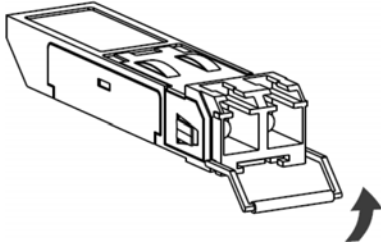


Figure 13 Transceiver Installation Example

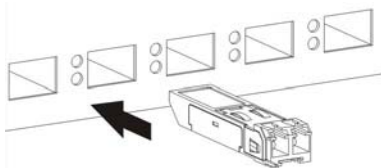
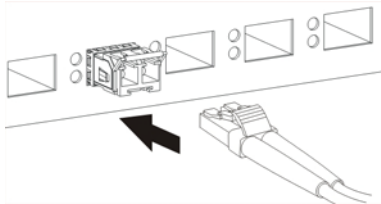


Figure 14 Connecting the Fiber Optic Cables



3.2.1.2 Transceiver Removal

Use the following steps to remove an SFP transceiver.

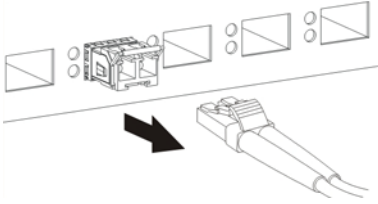
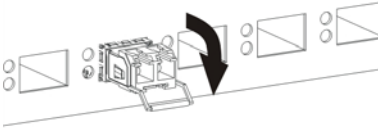
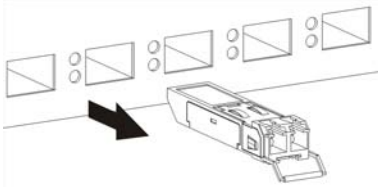
- 1 Attach an ESD preventive wrist strap to your wrist and to a bare metal surface on the chassis.
- 2 Remove the fiber optic cables from the transceiver.
- 3 Pull out the latch and down to unlock the transceiver (latch styles vary).

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

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

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

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

Figure 15 Removing the Fiber Optic Cables**Figure 16** Opening the Transceiver's Latch Example**Figure 17** Transceiver Removal Example

3.2.2 Management Port

The 1000Base-T Ethernet **MGMT** (management) port is used for local management. Connect directly to this port using an Ethernet cable. You can configure the Switch through 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.

3.2.3 Console Port

To configure the Switch using the Command Line Interface (CLI), connect the Type-C end of the console cable to the console port of the Switch. Connect the other end to your computer. You can use a computer with terminal emulation software configured to the following parameters:

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

3.3 Rear Panel

The following figures show the rear panel of the Switch. The rear panel contains:

Figure 18 Rear Panel: CX4800-56F (AC model)**Figure 19** Rear Panel: CX4800-56F (DC model)

3.3.1 Grounding

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

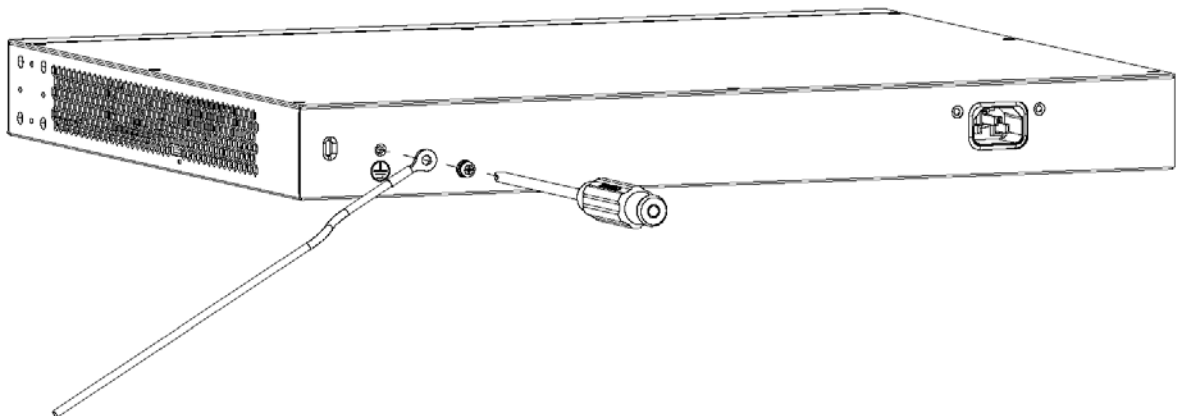
The grounding terminal and AC power ground where you install the Switch must follow your country's regulations. Qualified service personnel must ensure the building's protective earthing terminals are valid terminals.

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

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

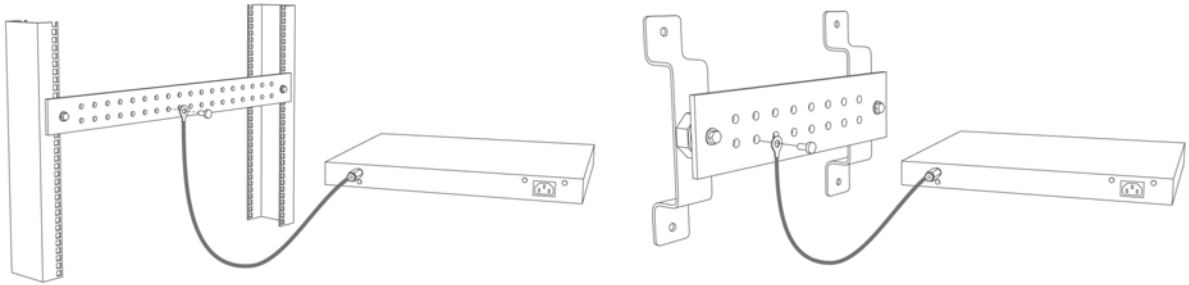
Note: The specification for surge or ESD protection assumes that the Switch is properly grounded.

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

Figure 20 Grounding

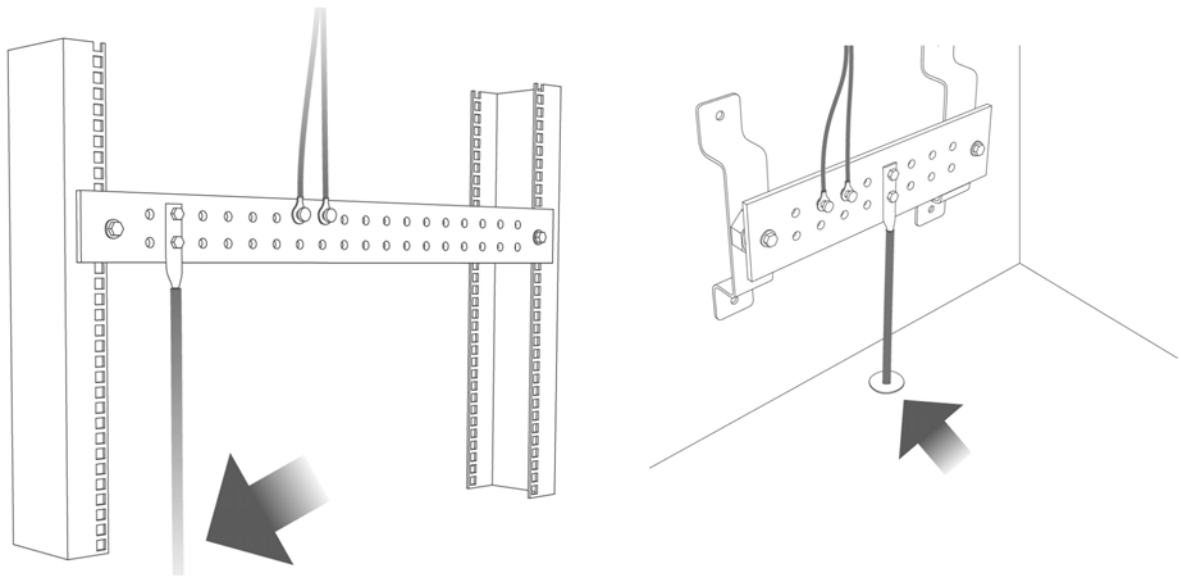
- 3 Attach the other end of the ground cable to a grounding bar located on the rack where you install the Switch or to an on-site grounding terminal.

Figure 21 Attach Ground Cable to Grounding Bar or On-site Grounding Terminal



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

Figure 22 Connecting to the Building's Main Grounding Electrode



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

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

3.3.2 Power Module Installation and Removal

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. It is recommended to replace the faulty power module promptly to prevent potential risks.

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

Install a Power Module and Connect the Power

Use the following procedures to install a power module and connect the Switch to a power source.

- 1 Find the power slot on the rear panel of the Switch. Gently push the power module into the slot, ensuring the latch secures tightly.
- 2 Connect the female end of the power cord to the power module, and connect the other end to a power outlet. See [Section 3.3.3 on page 44](#) for more information on AC power connection, and [Section 3.3.4 on page 44](#) on DC power connection.

Disconnect the Power and Remove a Power Module

- 1 Disconnect the power cord from the power outlet, then from the power module.
- 2 Press the latch (1) on the power module and gently pull (2) the power module out of the slot.

Figure 23 Removing the AC Power Module

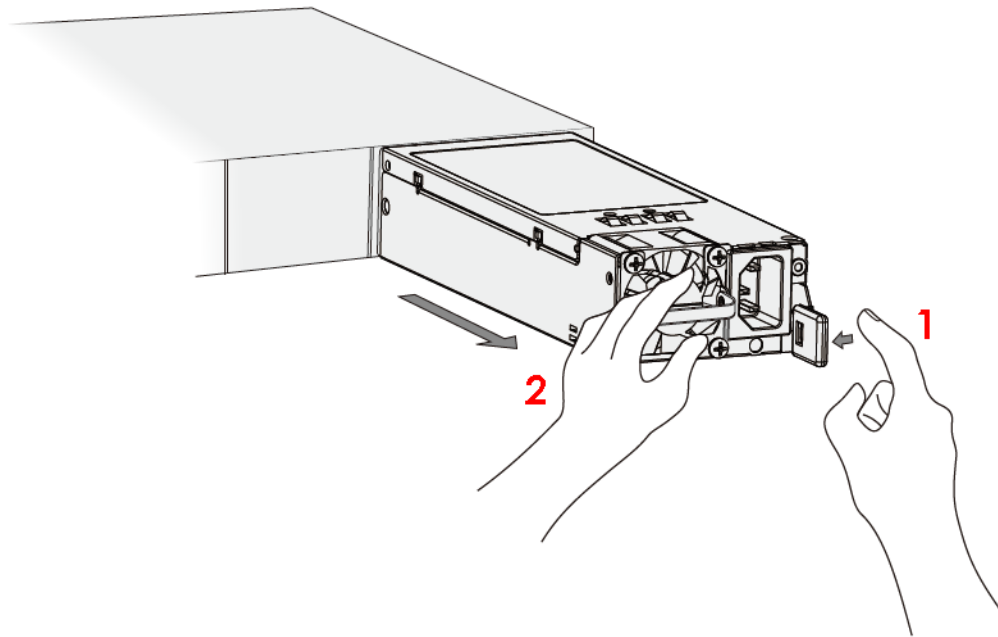
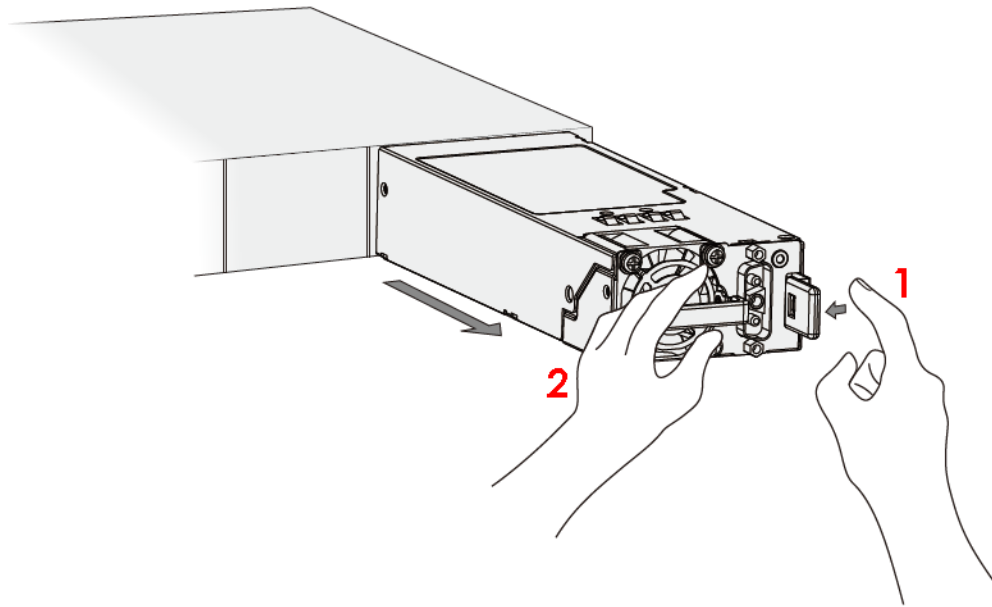


Figure 24 Removing the DC Power Module

3.3.3 AC Power Connection (AC Models Only)

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

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

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.

3.3.4 DC Power Connection (DC Models Only)

The Switch uses a single D-sub series terminal block plug with four pins. Use three wires to connect to the three terminal blocks: one for the positive terminal, one for the negative terminal, and one for the ground.

Note: The current rating of the power wires must be greater than 16 AWG. The power supply to which the Switch connects must have a built-in circuit breaker or switch to toggle the power.

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

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

To connect a power supply:

- 1 Use a screwdriver to loosen the captive screws on the D-sub's terminal block.
- 2 Connect one end of the grounding cable to the terminal block's grounding pin and tighten the captive screws.
- 3 Connect the other end of the grounding cable to the building's main grounding electrode.
- 4 Connect one end of a power wire to the Switch's RTN (return) pin and tighten the captive screws.
- 5 Connect the other end of the power wire to the positive terminal on the DC power supply.
- 6 Connect one end of a power wire to the Switch's -48 V (input) pin and tighten the captive screws.
- 7 Connect the other end of the power wire to the negative terminal on the power supply.
- 8 Insert the D-sub cable male connector plug in the Switch's power module female D-sub connector and tighten the captive bolt.

3.3.5 Fan Installation and Removal

There are four hot-swappable fan modules on the rear panel of the Switch. Hot-swappable fans are fans that can be installed or removed from the Switch without powering the Switch off.

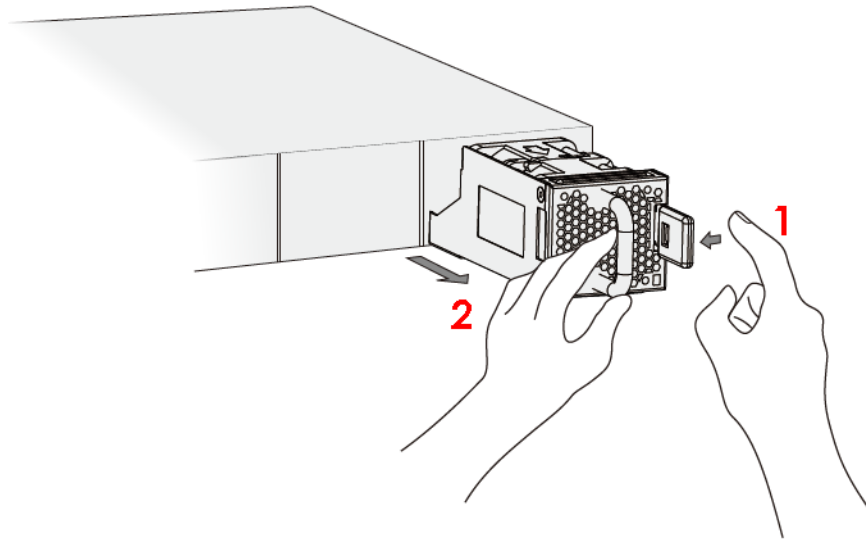
Install a Fan onto the Switch

- 1 Find the fan slot on the rear panel of the Switch.
- 2 Gently push the fan module into the slot, ensuring the latch secures tightly.
- 3 Ensure the fan is working properly without unusual noises. Make sure that no objects obstruct the airflow of the fan.

Remove a Fan from the Switch

Fans help maintain safe operating temperatures. Removing a fan from the Switch could lead to overheating and potential damage to the Switch.

- 1 Find the fan module on the rear panel of the Switch.
- 2 Press the latch (1) on the fan module and gently pull (2) the fan module out of the slot.

Figure 25 Removing the Fan Module

3.4 LEDs

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

Table 4 CX4800-56F LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The Switch is receiving power from power modules in the two power slots.
		Blinking	The Switch is receiving power from the power module in one power slot, while another power module in the power slot is not receiving power.
	Amber	On	The power module in the first power slot is connected but not supplying power to the Switch.
		Blinking	The power module in the second power slot is connected but not supplying power to the Switch.
		Off	The Switch is off.
SYS	Green	On	The Switch is on and functioning properly.
		Blinking	The Switch is rebooting and performing self-diagnostic tests.
	Amber	On	The Switch is functioning abnormally.
		Off	The power is off or the Switch is not ready or malfunctioning.

Table 4 CX4800-56F LED Descriptions (continued)

LED	COLOR	STATUS	DESCRIPTION
CLOUD	Green	On	The Switch has successfully connected to the NCC (Nebula Control Center).
		Blinking	The Switch cannot connect to the NCC because it is not registered.
	Amber	On	The Switch is registered at NCC but cannot connect to the NCC. Please check the Internet connection of the Switch.
		Blinking	The Switch is not registered at NCC and cannot connect to the NCC. Please check the Internet connection of the Switch and register the Switch at NCC.
		Off	The Switch is operating in standalone mode. Nebula Control Center Discovery is disabled in SYSTEM > Cloud Management in the Switch's Web Configurator.
LOCATOR	Green	On	The Switch is uploading firmware. While the Switch is doing this, do NOT turn off the power.
		Blinking	Shows the actual location of the Switch between several devices in a rack. The default timer is 30 minutes when you are configuring the Switch.
	Amber	On	The Switch is acting as the master in stacking.
		Off	The locator is not functioning or malfunctioning.
Power Supply	Green	On	The power slot is receiving AC/DC input normally.
	Amber	On	The power slot is not receiving AC/DC input normally.
MGMT (Left)	Green	On	The port is linking at 1000 Mbps.
	Amber	On	The port is linking at 10/100 Mbps.
		Off	There is no link or port.
MGMT (Right)	Green	Blinking	The port is receiving or transmitting data.
Port 1 – 48 1G / 10G / 25G SFP28 Fiber Port	White	On	The link to a 25 Gbps network is up.
		Blinking	The port is transmitting or receiving data at 25 Gbps.
	Blue	On	The link to a 10 Gbps network is up.
		Blinking	The port is transmitting or receiving data at 10 Gbps.
	Green	On	The link to a 1 Gbps network is up.
		Blinking	The port is transmitting or receiving data at 1 Gbps.
		Off	There is no link or the port is shut down.
Port 49 – 56 100G QSFP28 Fiber Port	White	On	The link to a 100 Gbps network is up.
		Blinking	The port is transmitting or receiving data at 100 Gbps.
		Off	There is no link or the port is shut down.
Fan	Green	On	The fan is on and functioning properly.
	Amber	On	The fan is not functioning at a proper speed or malfunctioning.

PART II

Technical Reference

CHAPTER 4

Web Configurator

4.1 Overview

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

The Web Configurator is an HTML-based management interface that allows easy system setup and management through a web browser. Use a web browser that supports HTML5, such as Microsoft Edge, Mozilla Firefox, or Google Chrome. The recommended minimum screen resolution is 1024 by 768 pixels.

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

- Web browser pop-up windows on your computer.
- JavaScript (enabled by default).
- Java permissions (enabled by default).

Note: In Cloud mode, the settings you configure in the Web Configurator will apply to the Switch but will not appear in the Nebula settings. The settings you configure in Nebula will overwrite the Web Configurator settings. It is the latest settings that will apply to the Switch.

Note: To avoid inconsistency, we recommend you use Nebula to configure the Switch and only use the Web Configurator for troubleshooting.

4.2 System Login

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

Note: You can always use the domain name "setup.zyxel" to access the Web Configurator whether the Switch is using a DHCP-assigned IP or static IP address. This requires your computer to be directly connected to the Switch. Make sure your computer can connect to a DNS server through the Switch.

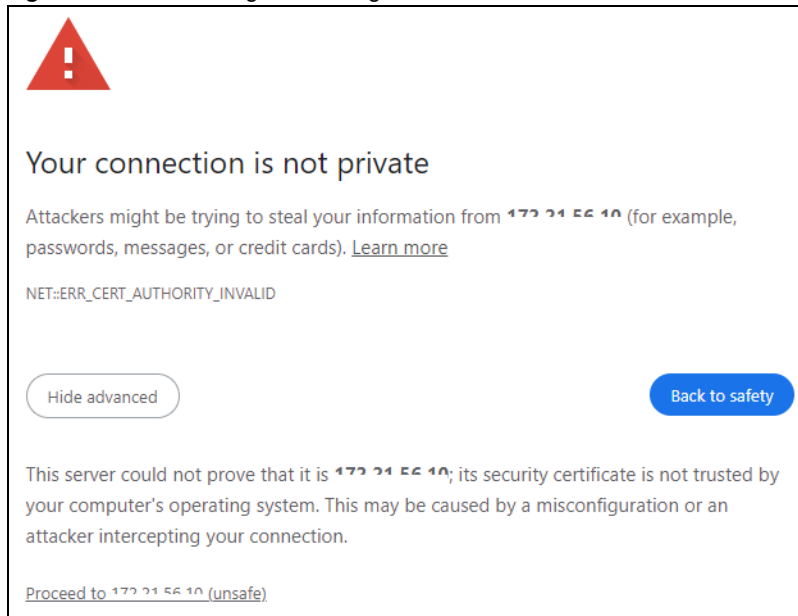
If the Switch is not connected to a DHCP server, type "http://static IP address" of the Switch (for example, the default management IP address is 192.168.1.1 through an in-band (non-**MGMT**) port and 192.168.0.1 through the **MGMT** port) in the **Location** or **Address** field. Press [ENTER]. Your computer must be in the same subnet in order to access this website address.

Also, you can use the ZON Utility to check your Switch's IP address. See [Section 4.3 on page 56](#) for more information on the ZON utility.

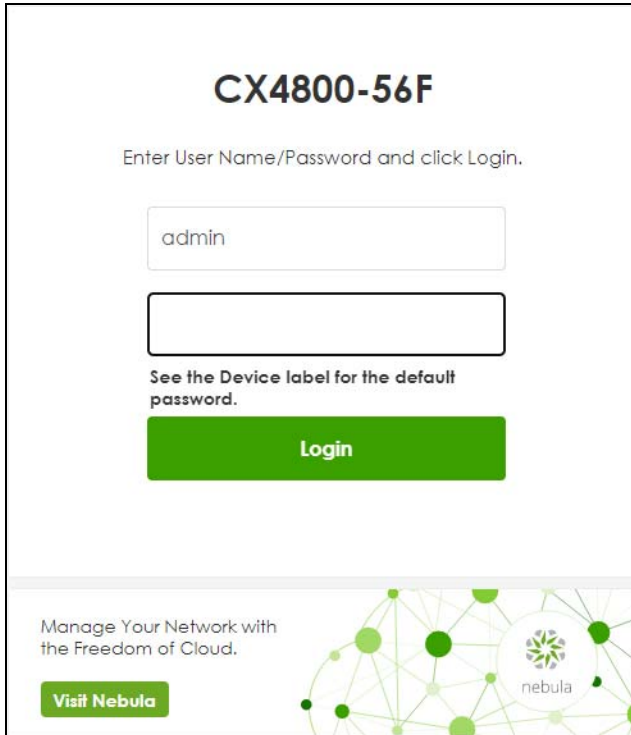
- 3 If a “Your connection is not private” screen appears, click **Advanced** and **Proceed to DHCP-assigned IP (unsafe)** to go to the **Login** screen. This screen appears as the Zyxel Device uses a certificate for the HTTPS connection. See [Section 65.2 on page 437](#) for information on using an HTTPS certificate verified by a third party to create secure HTTPS connections between your computer and the Switch.

Note: If you see this warning page, it indicates that your browser has failed to verify the Secure Sockets Layer (SSL) certificate, which opens an encrypted connection. You can ignore this message and proceed to the login IP address.

Figure 26 Unsafe Login Warning



The **Login** screen appears.

Figure 27 Web Configurator: Login (Standalone mode)

CX4800-56F

Enter User Name/Password and click Login.

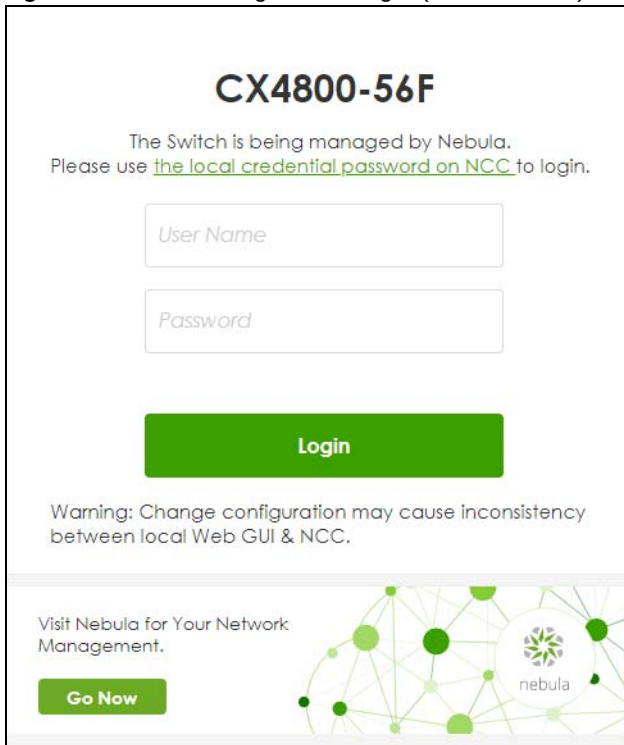
See the Device label for the default password.

Login

Manage Your Network with the Freedom of Cloud.

Visit Nebula

nebul

Figure 28 Web Configurator: Login (Cloud mode)

CX4800-56F

The Switch is being managed by Nebula.
Please use the local credential password on NCC to login.

Login

Warning: Change configuration may cause inconsistency between local Web GUI & NCC.

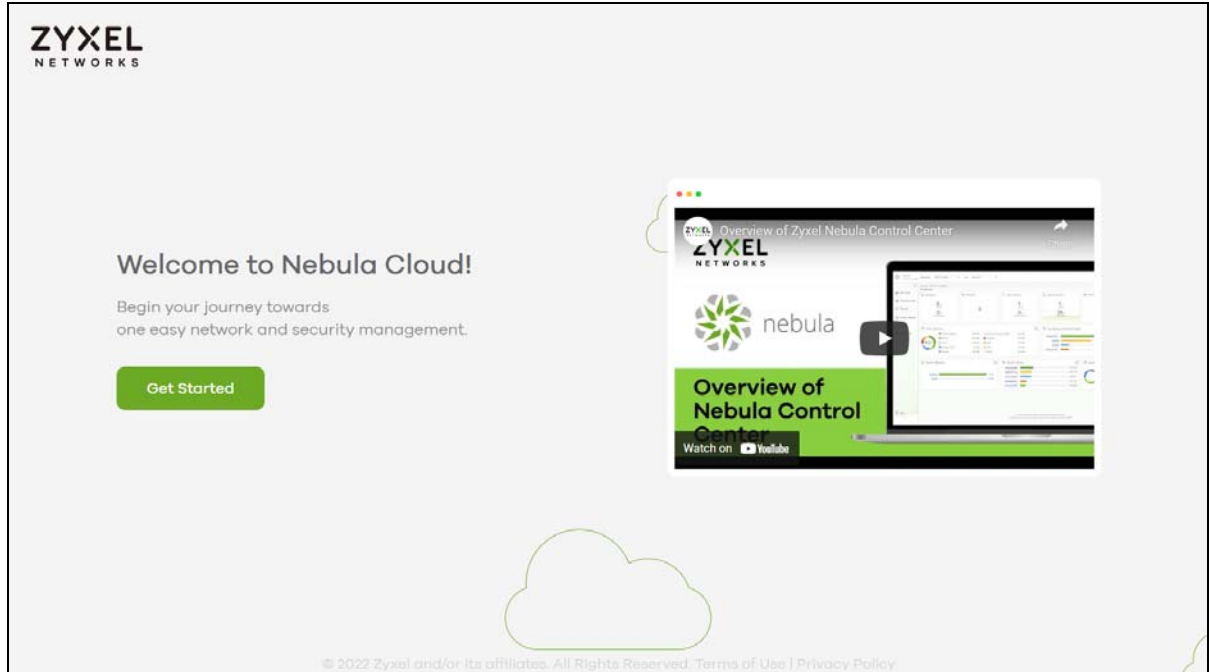
Visit Nebula for Your Network Management.

Go Now

nebul

- 4 In Standalone mode, click the **Visit Nebula** button if you want to open the Zyxel Nebula Control Center (NCC) login page in a new tab or window. In Cloud mode, click the **Go Now** button. The NCC is a cloud-based network management system that allows you to remotely manage and monitor the Switch. See [Section 1.4.1 on page 29](#) for information on changing your Switch to Nebula Cloud management.

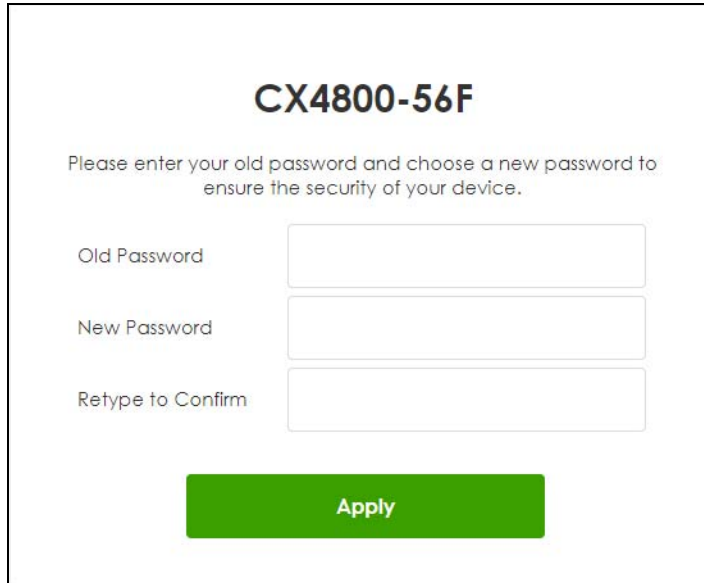
Figure 29 Visit Nebula



- 5 Alternatively, click **Login** to log into the Web Configurator to manage the Switch directly.
 In Standalone mode, the default user name is **admin** and associated default password is on the label on the bottom of the Switch.
 In Cloud mode, use the **Local credentials: password** to login. The **Local credentials: Password** can be found in **Site-wide > Configure > Site settings > Device configuration** in the NCC portal. See the NCC User's Guide for more information.

In Standalone mode, the change password screen appears the first time you log in using the default password.

Note: The allowed string length is 4 to 32 for the new password and should not contain [?], [|], ['], ["], [,], [[], []], or [space].

Figure 30 Change Password Screen


CX4800-56F

Please enter your old password and choose a new password to ensure the security of your device.

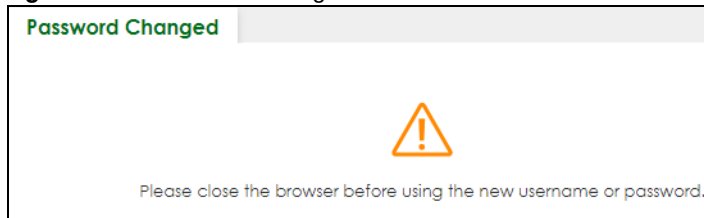
Old Password

New Password

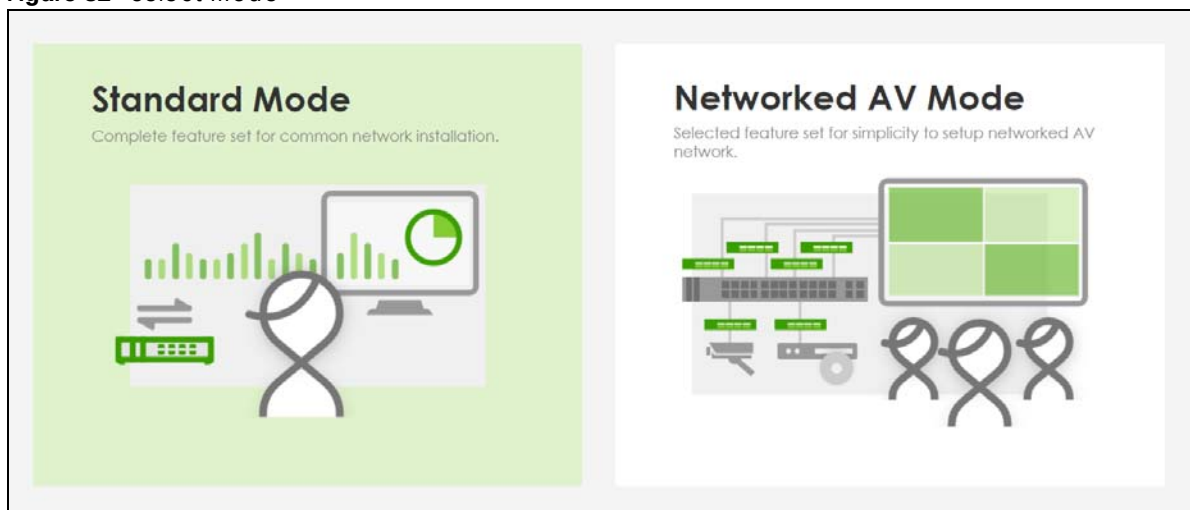
Retype to Confirm

Apply

- After setting the new password, close and restart your web browser. Enter the 'https://DHCP-assigned IP' in the URL field and press [ENTER]. When the login screen appears, enter the user name (default: 'admin') and new password.

Figure 31 Password Changed Screen

When in Standalone mode, the **Select Mode** screen appears.

Figure 32 Select Mode

- Select the Web Configurator in **Standard Mode** that has a complete set of configuration for network installation. Or select the Web Configurator in **Networked AV Mode** that has a set of menus specifically

designed to simplify configuration and management of the Switch for AVoIP (Audio-Video over Internet Protocol) application.

- 8 The **Setup Wizard** screen will appear after selecting the **Networked AV Mode**. You can use the **Setup Wizard** screen in Networked AV mode to configure the Switch's Networked AV mode's basic or advanced settings (see [Section 4.4 on page 59](#) for details).

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

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

Otherwise, click the **Exit** button. You can select the **Ignore this wizard next time** checkbox and click **Apply & Save** if you do not want the **Setup Wizard** screen to appear the next time you log in. If you want to open the **Setup Wizard** screen later, click the **Wizard** icon in the upper right hand corner of the Web Configurator.

- 9 If you did not change the default SNMP community values and enabled **SNMP** in **SECURITY > Access Control > Service Access Control**, a warning screen displays each time you log into the Web Configurator. Click **SNMP** to open a screen where you can change the SNMP community string, see [Section 21.2 on page 147](#) for more information. Otherwise, click **Ignore** to close it.

SNMP Setting

Figure 33 Web Configurator: Warning

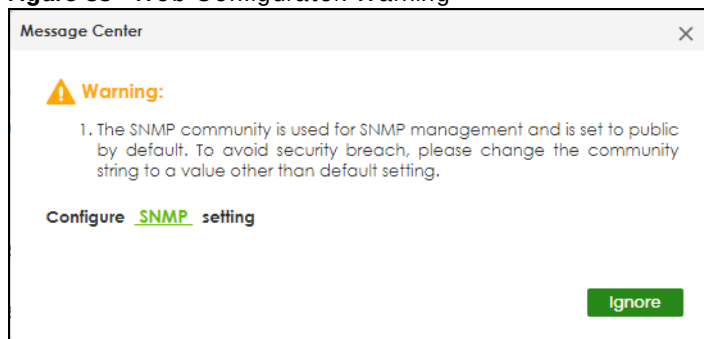


Figure 34 SYSTEM > SNMP

SNMP SNMP User SNMP Trap Group SNMP Trap Port

General Setting

Version: v2c ▼

Get Community: public

Set Community: public

Trap Community: public

Trap Destination

Index	Version	IP	Port	Username
1	v2c ▼	0.0.0.0	162	
2	v2c ▼	0.0.0.0	162	
3	v2c ▼	0.0.0.0	162	
4	v2c ▼	0.0.0.0	162	

Apply Cancel

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

Figure 35 Web Configurator: Wizard

Setup Wizard

Select Networked AV Mode

Basic Settings

Green gear icon and a 4x4 grid of squares.

Advanced Settings

Gray gear icon and a 4x4 grid of squares.

Next Exit

4.3 Zyxel One Network (ZON) Utility

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

The ZON Utility issues requests through 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 <https://www.zyxel.com/global/en/form/zon-utility-download> and unzip it first before installing it in a computer (Windows operating system).

4.3.1 Requirements

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

Operating System

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

- Windows 7 (both 32-bit / 64-bit versions)
- Windows 8 (both 32-bit / 64-bit versions)
- Windows 8.1 (both 32-bit / 64-bit versions)
- Windows 10 (both 32-bit / 64-bit versions)
- Windows 11 (64-bit version)

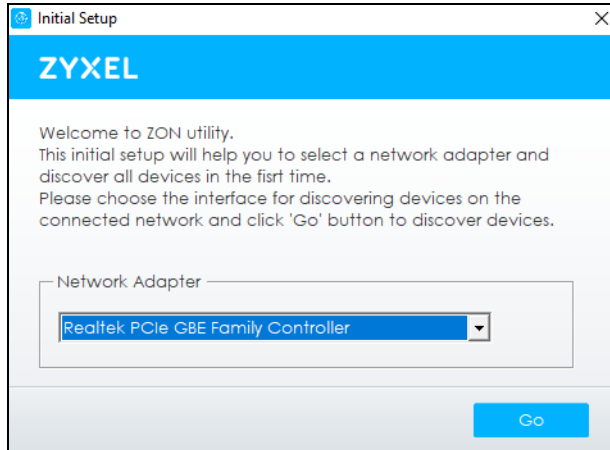
Hardware

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

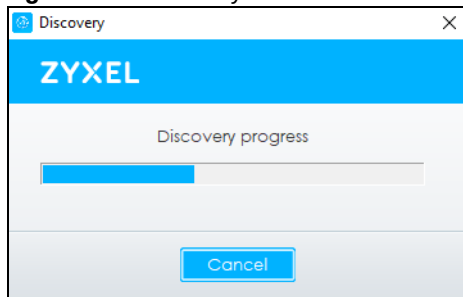
- Core i3 processor
- 2 GB RAM
- 100 MB free hard disk
- WXGA (Wide XGA 1280 by 800)

4.3.2 Run the ZON Utility

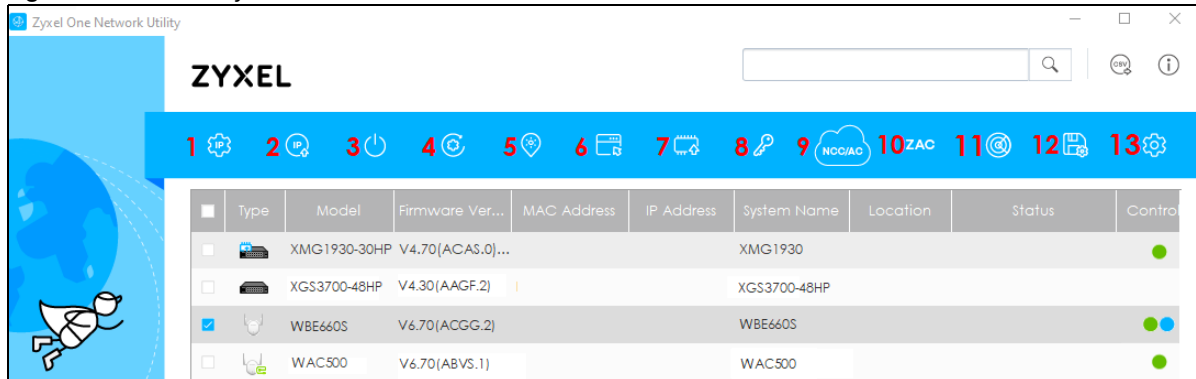
- 1 Double-click the ZON Utility to run it.
- 2 Select a network adapter to which your supported devices are connected.

Figure 36 Network Adapter

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

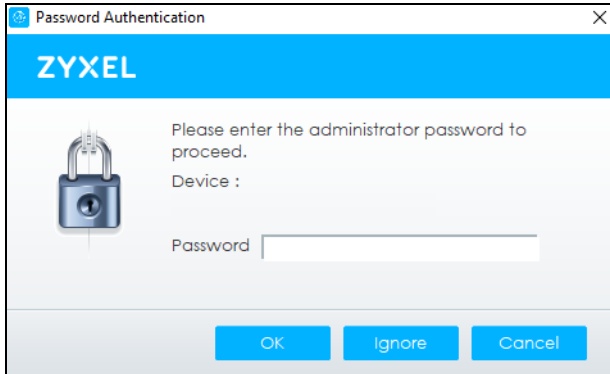
Figure 37 Discovery

- The ZON Utility screen shows the devices discovered.

Figure 38 ZON Utility Screen

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

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

Figure 39 Password Prompt

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

Table 5 ZON Utility Icons

ICON	DESCRIPTION
1 IP Configuration	Change the selected device's IP address.
2 Renew IP Address	Update a DHCP-assigned dynamic IP address.
3 Reboot Device	Use this icon to restart the selected devices. This may be useful when troubleshooting or upgrading new firmware.
4 Reset Configuration to Default	Use this icon to reload the factory-default configuration file. This means that you will lose all previous configurations.
5 Locator LED	Use this icon to locate the selected device by causing its Locator LED to blink.
6 Web GUI	Use this to access the selected device Web Configurator from your browser. You will need a user name and password to log in.
7 Firmware Upgrade	Use this icon to upgrade new firmware to selected devices of the same model. Make sure you have downloaded the firmware from the Zyxel website to your computer and unzipped it in advance.
8 Change Password	Use this icon to change the admin password of the selected device. You must know the current admin password before changing to a new one.
9 Configure NCC Discovery	You must have Internet access to use this feature. Use this icon to enable or disable the Nebula Control Center (NCC) discovery feature on the selected device. If it is enabled, the selected device will try to connect to the NCC. Once the selected device is connected to and has registered in the NCC, it will go into the Nebula cloud management mode.
10 ZAC	Use this icon to run the Zyxel AP Configurator of the selected AP.
11 Clear and Rescan	Use this icon to clear the list and discover all devices on the connected network again.
12 Save Configuration	Use this icon to save configuration changes to permanent memory on a selected device.
13 Settings	Use this icon to select a network adapter for the computer on which the ZON utility is installed, and the utility language.

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

Table 6 ZON Utility Fields

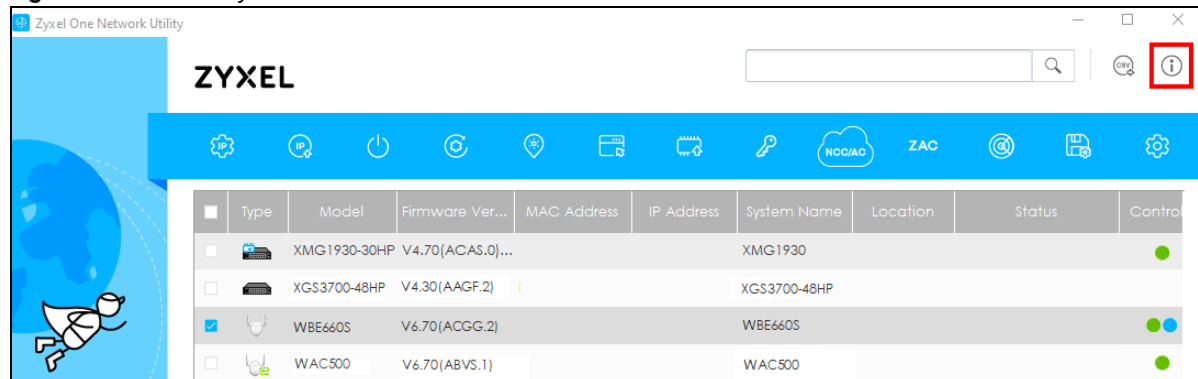
LABEL	DESCRIPTION
Type	This field displays an icon of the kind of device discovered.
Model	This field displays the model name of the discovered device.
Firmware Version	This field displays the firmware version of the discovered device.
MAC Address	This field displays the MAC address of the discovered device.

Table 6 ZON Utility Fields (continued)

LABEL	DESCRIPTION
IP Address	This field displays the IP address of an internal interface on the discovered device that first received a ZDP discovery request from the ZON Utility.
System Name	This field displays the system name of the discovered device.
Location	This field displays where the discovered device is.
Status	This field displays whether changes to the discovered device have been done successfully. As the Switch does not support IP Configuration , Renew IP address and Flash Locator LED , this field displays "Update failed", "Not support Renew IP address" and "Not support Flash Locator LED" respectively.
Controller Discovery	This field displays if the discovered device supports the Nebula Control Center (NCC) discovery feature. If it is enabled, the selected device will try to connect to the NCC. Once the selected device is connected to and has registered in the NCC, it will go into the Nebula cloud management mode.
Serial Number	Enter the admin password of the discovered device to display its serial number.
Hardware Version	This field displays the hardware version of the discovered device.
IPv6 Address	This field displays the IPv6 address on the discovered device that first received a ZDP discovery request from the ZON Utility.

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

Figure 40 ZON Utility Screen

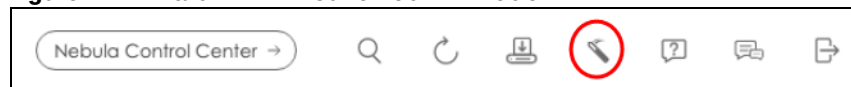


4.4 Networked AV Mode Wizard

The **Setup Wizard** can be accessed using the following methods:

- When the Switch is in its factory-default state, selecting Networked AV mode will automatically access the **Setup Wizard**.
- When in Networked AV mode, click the **Wizard** link to access the **Setup Wizard**.

Figure 41 Wizard Link in Networked AV Mode



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

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

4.4.1 Basic Settings

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

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

Figure 42 Wizard > Basic Settings > Step 1 IP

1 STEP IP **2** Password **3** Networked AV **4** Summary

Setup IP

Host Name:

IP Interface: ☐ Static IP Interface ☒ DHCP Client

VID:

IP Address:

IP Subnet Mask:

Default Gateway:

DNS Server:

Next **Cancel**

Each field is described in the following table.

Table 7 Wizard > Basic Settings > Step 1 IP

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

Table 7 Wizard > Basic Settings > Step 1 IP (continued)

LABEL	DESCRIPTION
DNS Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. Enter a domain name server IP address in order to be able to use a domain name instead of an IP address.
Next	Click Next to show the next screen.
Cancel	Click Cancel to exit this screen without saving.

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

Figure 43 Wizard > Basic Settings > Step 2 Password

Note: The input string of any field in this screen should not contain [?], [|], ['], ["], or [,]. In the **Password** fields, [space], [[], or []] are also not allowed.

Each field is described in the following table.

Table 8 Wizard > Basic Settings > Step 2 Password

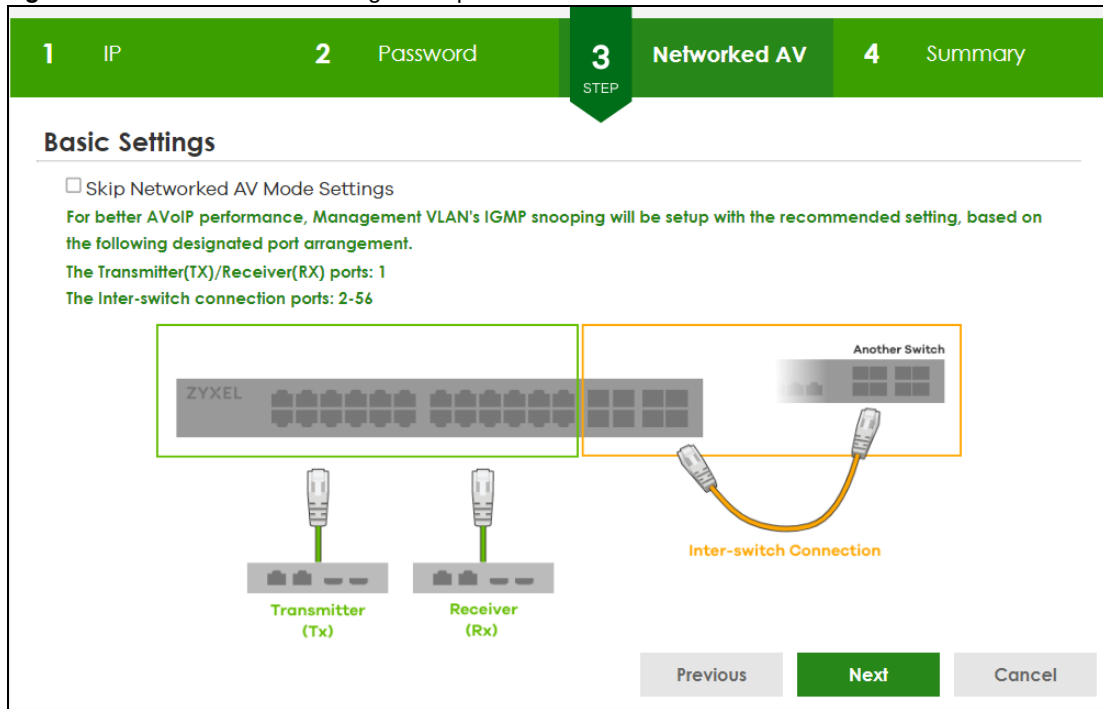
LABEL	DESCRIPTION
Administrator's Password	
Current password	Enter the existing system password (the default password is on the label on the back of the Switch).
New password	Enter your new system password. 4 to 32 printable ASCII characters are allowed for the new password.
Confirm password	Re-enter your new system password for confirmation.
SNMP	
SNMP	Select Enabled to let the Switch act as an SNMP agent, which allows a manager station to manage and monitor the Switch through the network. Select Disabled to turn this feature off.

Table 8 Wizard > Basic Settings > Step 2 Password (continued)

LABEL	DESCRIPTION
Version	Select the SNMP version for the Switch. The SNMP version on the Switch must match the version on the SNMP manager. Choose SNMP version 2c (v2c), SNMP version 3 (v3) or both (v3v2c). Note: SNMP version 2c is backwards compatible with SNMP version 1.
Get Community	Enter the Get Community string, which is the password for the incoming Get- and GetNextrequests from the management station. The Get Community string is only used by SNMP managers using SNMP version 2c or lower.
Set Community	Enter the Set Community string, which is the password for the incoming Set- requests from the management station. The Set Community string is only used by SNMP managers using SNMP version 2c or lower.
Trap Community	Enter the Trap Community string, which is the password sent with each trap to the SNMP manager. The Trap Community string is only used by SNMP managers using SNMP version 2c or lower.
Previous	Click Previous to show the previous screen.
Next	Click Next to show the next screen.
Cancel	Click Cancel to exit this screen without saving.

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

Figure 44 Wizard > Basic Settings > Step 3 Networked AV



Each field is described in the following table.

Table 9 Wizard > Basic Settings > Step 3 Networked AV

LABEL	DESCRIPTION
Skip Networked AV Mode Settings	Click this option to avoid using the basic default AVoIP settings. The default AVoIP settings can be seen in Step 4 Summary under Networked AV – Basic Settings . Otherwise, clear the checkbox and follow the diagram for connecting RJ45 ports to audio and video equipment. The Inter-switch Connection is for connecting to another switch. Note: Use the Wizard > Advanced Settings > Step 3 Networked AV to configure connections for non-Audio-Video equipment (for example computer, NAS) to the RJ45 ports.
Previous	Click Previous to show the previous screen.
Next	Click Next to show the next screen.
Cancel	Click Cancel to exit this screen without saving.

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

Figure 45 Wizard > Basic Settings > Step 4 Summary

Summary

Setup IP		Change administrator's password and activate SNMP		Networked AV - Basic Settings	
Host Name:	CX4800	New password:		Networked AV VLAN:	1
IP Interface:	DHCP Client	SNMP:	Disabled	Networked AV VLAN IP:	
VID:	1	Version:	v2c	IGMP Snooping:	Active
IP Address:		Get Community:	public	IGMP Snooping Querier:	Active
IP Subnet Mask:		Set Community:	public	Unknown Multicast Frame:	Drop
Default Gateway:		Trap Community:	public	Transmitter/Receiver Connected Port:	5,8-10,12,16-18,21-23,28-29,31,3
DNS Server:				Inter-switch Connected Port:	1-4,6-7,11,13-15,19-20,24-27,30,
				Diffserv:	Active
				Static Multicast Forwarding:	PTP, SAP

Previous Finish Cancel

Each field is described in the following table.

Table 10 Wizard > Basic Settings > Step 4 Summary

LABEL	DESCRIPTION
Setup IP	
Host Name	This field displays a host name.
IP Interface	This field displays whether the WAN interface is using a DHCP IP address or a static IP address.
VID	This field displays the VLAN ID.
IP Address	This field displays the Switch's IP address for it to be managed over the network.

Table 10 Wizard > Basic Settings > Step 4 Summary (continued)

LABEL	DESCRIPTION
IP Subnet Mask	This field displays the subnet mask that specifies the network number portion of an IP address.
Default Gateway	This field displays the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
DNS Server	This field displays the DNS (Domain Name System) for mapping a domain name to its corresponding IP address and so forth.
Change administrator's password and activate SNMP	
New Password	This field displays asterisks when a new password has been created.
SNMP	This field displays whether the Switch acts as an SNMP agent.
Version	This field displays the SNMP version for the Switch.
Get Community	This field displays the Get Community string.
Set Community	This field displays the Set Community string.
Trap Community	This field displays the Trap Community string.
Networked AV – Basic Settings	
Networked AV VLAN	This field displays the VLAN ID for the AVoIP network.
Networked AV VLAN IP	This field displays the Switch's IP address for it to be managed over the AVoIP network.
IGMP Snooping	This field displays Active when IGMP Snooping is enabled to forward group multicast traffic only to ports that are members of that group. Otherwise, it displays Inactive .
IGMP Snooping Querier	This field displays Active when the Switch is allowed to send IGMP General Query messages to the VLANs with the multicast hosts attached. Otherwise, it displays Inactive .
Unknown Multicast Frame	This field displays the action to perform when the Switch receives an unknown multicast frame. It displays Drop when the frames are discarded. It displays Flooding when the frames are sent to all ports.
Transmitter/ Receiver Connected Port	This field shows the Switch's port numbers for connection to networked audio and video equipment.
Inter-switch Connected Port	This field shows the Switch's port numbers for connection to another switch.
Diffserv	This field displays Active . This means that IEEE 802.1p priority mapping in Quality of Service (QoS) is applied on the selected ports on the Switch. See Section 36.1 on page 238 for more information on QoS.
Static Multicast Forwarding	This field displays PTP, SAP . PTP (Precision Time Protocol). The Switch allows the client devices to forward the PTP multicast packets to audio-over-IP devices to sync the time clock. SAP (Session Announcement Protocol) for advertising multicast session information. The Switch allows AES67 (Audio Engineering Society 67) multicast packets to be directly forwarded to audio-over-IP devices. See Section 34.1 on page 231 for more information on Static Multicast Forwarding.
Previous	Click Previous to show the previous screen.
Finish	Review the information and click Finish to create the task.
Cancel	Click Cancel to exit this screen without saving.

4.4.2 Advanced Settings

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

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

Figure 46 Wizard > Advanced Settings > Step 1 IP

The screenshot shows the 'Setup IP' configuration screen. At the top, there is a green navigation bar with four steps: 1 IP, 2 Password, 3 Networked AV, and 4 Summary. Step 1 is highlighted. Below the navigation bar, the title 'Setup IP' is displayed. The main area contains several configuration fields: Host Name (CX4800), IP Interface (Static IP Interface and DHCP Client), VID (1), IP Address (172.21.56.10), IP Subnet Mask (255.255.252.0), Default Gateway (172.21.59.254), and DNS Server (172.21.10.1). At the bottom right, there are 'Next' and 'Cancel' buttons.

Each field is described in the following table.

Table 11 Wizard > Advanced Settings > Step 1 IP

LABEL	DESCRIPTION
Host Name	This field displays a host name. You can enter a new host name here. Up to 64 printable ASCII characters are allowed except [?], [], ['], ["], or [,].
IP Interface	Select DHCP Client if the Switch is connected to a router with the DHCP server enabled. You then need to check the router for the IP address assigned to the Switch in order to access the Switch's Web Configurator again. Select Static IP Interface when the Switch is NOT connected to a router or you want to assign it a fixed IP address.
VID	This field displays the VLAN ID.
IP Address	The Switch needs an IP address for it to be managed over the network.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address.
Default Gateway	Type the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
DNS Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and so forth. Enter a domain name server IP address in order to be able to use a domain name instead of an IP address.

Table 11 Wizard > Advanced Settings > Step 1 IP (continued)

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

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

Figure 47 Wizard > Advanced Settings > Step 2 Password

Note: The input string of any field in this screen should not contain [?], [|], ['], ["], or [,]. In the **Password** fields, [space], [[], or []] are also not allowed.

Each field is described in the following table.

Table 12 Wizard > Advanced Settings > Step 2 Password

LABEL	DESCRIPTION
Administrator's Password	
Current password	Enter the existing system password (the default password is on the label on the back of the Switch).
New password	Enter your new system password. 4 to 32 printable ASCII characters are allowed for the new password.
Confirm password	Re-enter your new system password for confirmation.
SNMP	
SNMP	Select Enabled to let the Switch act as an SNMP agent, which allows a manager station to manage and monitor the Switch through the network. Select Disabled to turn this feature off.

Table 12 Wizard > Advanced Settings > Step 2 Password (continued)

LABEL	DESCRIPTION
Version	Select the SNMP version for the Switch. The SNMP version on the Switch must match the version on the SNMP manager. Choose SNMP version 2c (v2c), SNMP version 3 (v3) or both (v3v2c). Note: SNMP version 2c is backwards compatible with SNMP version 1.
Get Community	Enter the Get Community string, which is the password for the incoming Get- and GetNextrequests from the management station. The Get Community string is only used by SNMP managers using SNMP version 2c or lower.
Set Community	Enter the Set Community string, which is the password for the incoming Set- requests from the management station. The Set Community string is only used by SNMP managers using SNMP version 2c or lower.
Trap Community	Enter the Trap Community string, which is the password sent with each trap to the SNMP manager. The Trap Community string is only used by SNMP managers using SNMP version 2c or lower.
Previous	Click Previous to show the previous screen.
Next	Click Next to show the next screen.
Cancel	Click Cancel to exit this screen without saving.

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

Figure 48 Wizard > Advanced Settings > Step 3 Networked AV

1 IP **2** Password **3** **Networked AV** **4** Summary

Advanced Settings

Allocate networked AV service to a VLAN

Networked AV VLAN:

IP Address: (Optional)

IP Subnet Mask: (Optional)

Select Ports and Assign a Port Role ⓘ

Select all ports ☐

Grid of 50 port icons (2 rows of 25).

Tx/Rx Inter-switch Management ☐ Link aggregate

Previous **Next** Cancel

Each field is described in the following table.

Table 13 Wizard > Advanced Settings > Step 3 Networked AV

LABEL	DESCRIPTION
Allocate networked AV service to a VLAN	
Networked AV VLAN	Enter a number between 1 and 4094 to create a VLAN for the AVoIP network.
IP Address (Optional)	You must enter a different VLAN ID in the previous field (Networked AV VLAN) to be able to assign another IP address for the Switch to be managed over the AVoIP network.
IP Subnet Mask (Optional)	You must enter a different VLAN ID in the Networked AV VLAN field to be able to assign another subnet mask that specifies the network number portion of an IP address.
Select Ports and Assign a Port Role	
Select all ports	After you create a VLAN, select the ports to be assigned to the Networked AV VLAN. Select all ports to assign the same role to all ports. You can select a port by clicking it. Then click any of the following: Click Tx/Rx to assign the ports for connecting to audio and video equipment. Click Inter-switch to assign the ports for connecting to other switches or gateway. Click Management to assign the ports for connecting to non-Audio-Video equipment (for example, computer and NAS) if your Networked AV VLAN is different from management VLAN.
Link aggregate	Select this option to aggregate multiple port bandwidth if you are connecting to another switch. Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link.
Previous	Click Previous to show the previous screen.
Next	Click Next to show the next screen.
Cancel	Click Cancel to exit this screen without saving.

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

Figure 49 Wizard > Advanced Settings > Step 4 Summary

1	2	3	4
IP	Password	Networked AV	Summary
STEP Summary			
Setup IP		Change administrator's password and activate SNMP	
Host Name: CX4800 IP Interface: DHCP Client VID: 1 IP Address: IP Subnet Mask: Default Gateway: DNS Server:		New password: SNMP: Disabled Version: v2c Get Community: public Set Community: public Trap Community: public	
		Networked AV - Advanced Settings	
		Networked AV VLAN: 1 Networked AV VLAN IP: IGMP Snooping: Active IGMP Snooping Querier: Active Unknown Multicast Frame: Drop Transmitter/Receiver Connected Port: Inter-switch Connected Port: Diffserv: Active Static Multicast Forwarding: PTP, SAP	
		Previous Finish Cancel	

Each field is described in the following table.

Table 14 Wizard > Advanced Settings > Step 4 Summary

LABEL	DESCRIPTION
Setup IP	
Host Name	This field displays a host name.
IP Interface	This field displays whether the WAN interface is using a DHCP IP address or a static IP address.
VID	This field displays the VLAN ID.
IP Address	This field displays the Switches' IP address for it to be managed over the network.
IP Subnet Mask	This field displays the subnet mask that specifies the network number portion of an IP address.
Default Gateway	This field displays the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
DNS Server	This field displays the DNS (Domain Name System) for mapping a domain name to its corresponding IP address and so forth.
Change administrator's password and activate SNMP	
New Password	This field displays asterisks when a new password has been created.
SNMP	This field displays whether the Switch acts as an SNMP agent.
Version	This field displays the SNMP version for the Switch.
Get Community	This field displays the Get Community string.
Set Community	This field displays the Set Community string.
Trap Community	This field displays the Trap Community string.
Networked AV – Advanced Settings	
Networked AV VLAN	This field displays the VLAN ID for the AVoIP network.

Table 14 Wizard > Advanced Settings > Step 4 Summary (continued)

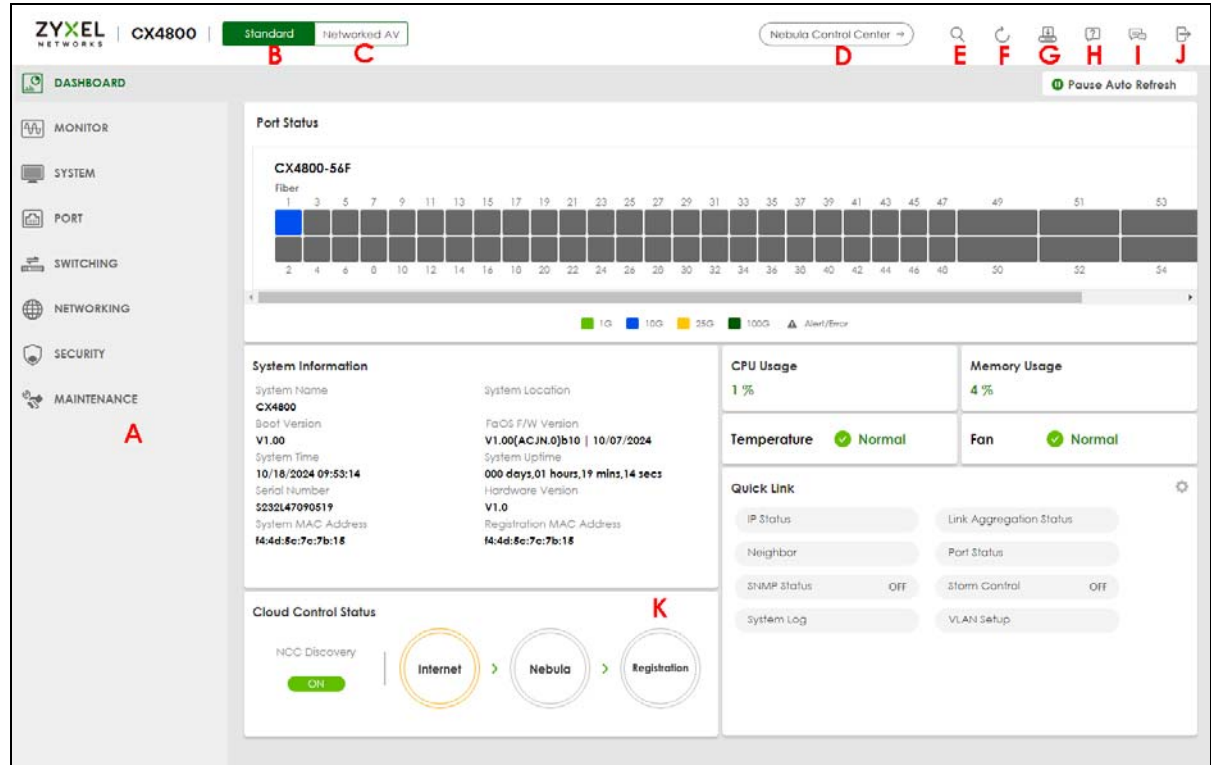
LABEL	DESCRIPTION
Networked AV VLAN IP	This field displays the corresponding VLAN ID's IP address for the AVoIP network.
IGMP Snooping	This field displays Active when IGMP Snooping is enabled to forward group multicast traffic only to ports that are members of that group. Otherwise, it displays Inactive .
IGMP Snooping Querier	This field displays Active when the Switch is allowed to send IGMP General Query messages to the VLANs with the multicast hosts attached. Otherwise, it displays Inactive .
Unknown Multicast Frame	This field displays the action to perform when the Switch receives an unknown multicast frame. It displays Drop when the frames are discarded. It displays Flooding when the frames are sent to all ports.
Transmitter/Receiver Connected Port	This field shows the Switches' port numbers for connection to networked audio and video equipment.
Inter-switch Connected Port (Link Aggregation)	This field shows the Switches' port numbers for connection to another switch.
Diffserv	This field displays Active . This means that IEEE 802.1p priority mapping in Quality of Service (QoS) is applied on the selected ports on the Switch. See Section 36.1 on page 238 for more information on QoS.
Static Multicast Forwarding	This field displays PTP, SAP . PTP (Precision Time Protocol). The Switch allows the client devices to forward the PTP multicast packets to audio-over-IP devices to sync the time clock. SAP (Session Announcement Protocol) for advertising multicast session information. The Switch allows AES67 (Audio Engineering Society 67) multicast packets to be directly forwarded to audio-over-IP devices. See Section 34.1 on page 231 for more information on Static Multicast Forwarding.
Previous	Click Previous to show the previous screen.
Finish	Review the information and click Finish to create the task.
Cancel	Click Cancel to exit this screen without saving.

4.5 Web Configurator Layout

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

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

Figure 50 Web Configurator Layout



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

B, C, D, E, F, G, H, I, J, K – These are quick links which allow you to perform certain tasks no matter which screen you are currently working in.

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

D – Click this icon to go to the NCC (Nebula Control Center) portal website.

E – Click this icon to search for specific configurations or status you are looking for. Enter the keywords and click the result link. This will direct you to the specific configuration or status page.

F – Click this icon to update the information in the screen you are currently viewing.

G – Click this icon to save your configuration into the Switch's non-volatile memory. Non-volatile memory is the configuration of your Switch that stays the same even if the Switch's power is turned off.

H – Click this icon to display web help pages. The help pages provide descriptions for all of the configuration screens.

I – Click this icon to go to the Zyxel Community Biz Forum.

J – Click this icon to log out of the Web Configurator.

K – This displays the Nebula Cloud Control Status. The ON/OFF switch displays if **NCC Discovery** is enabled. If a status circle turns Orange, it means the Switch is unable to connect to NCC. Hover the mouse over the status circle to check the diagnostic message. You can also click the ON/OFF switch to

go to the **SYSTEM > Cloud Management > Cloud Management** screen and check the diagnostic messages. See [Table 31 on page 132](#) for more information.

In the navigation panel, click a main link to reveal a list of sub-menu links.

The following table describes the links in the navigation panel. The navigation panel varies depending on the product model you use.

Table 15 Navigation Panel Links

LINK	DESCRIPTION
DASHBOARD	This link takes you to the main dashboard screen that displays general system and device information.
MONITOR	
ARP Table	This link takes you to a screen that displays the current ARP table of the Switch. You can view the IP and MAC address mapping, VLAN ID, ARP aging time, and ARP entry type of a device attached to a port.
IP Table	This link takes you to a screen where you can view the IP address and VLAN ID of a device attached to a port.
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.
Neighbor	This link takes you to a screen where you can view neighbor devices (including non-Zyxel devices) connected to the Switch.
Port Status	This link takes you to a screen where you can view the port statistics.
Routing Table	Click the link to unfold the following sub-link menu.
IPv4 Routing Table	This link takes you to a screen where you can view the IPv4 routing table for routing information including IP interface and hop count to certain network destinations.
System Information	This link takes you to a screen that displays general system information.
System Log	This link takes you to a screen where you can view the system log including fail log and system status.
SYSTEM	
Cloud Management	This link takes you to a screen where you can enable or disable the Nebula Control Center (NCC) Discovery feature and view the NCC connection status. If Nebula Control Center (NCC) Discovery is enabled, you can have the Switch search for the NCC (Nebula Control Center). The screen also displays a QR code containing the Switch's serial number and MAC address for handy registration of the Switch at NCC.
General Setup	This link takes you to a screen where you can configure general identification information about the Switch.
Hardware Monitor Setup	This link takes you to a screen where you can configure hardware monitor related features such as SFP Detect .
IP Setup	This link takes you to a screen where you can configure the DHCP client, and a static IP address (IP address and subnet mask).
Logins	This link takes you to a screen where you can change the system login password, as well as configure up to four login details.
SNMP	This link takes you to screens where you can specify the SNMP version and community (password) values, configure where to send SNMP traps from the Switch, enable loopguard/errdisable/poe/linkup/linkdown/lldp/transceiver-ddm/storm-control on the Switch, specify the types of SNMP traps that should be sent to each SNMP manager, and add/edit user information.
Switch Setup	This link takes you to a screen where you can set up global Switch parameters such as VLAN type.
Syslog Setup	This link takes you to a screen where you can configure the Switch's system logging settings and configure a list of external syslog servers.

Table 15 Navigation Panel Links (continued)

LINK	DESCRIPTION
Time Range	This link takes you to a screen where you can configure time range for time-oriented features like Classifier.
PORT	
Flex Link	This screen takes you to a screen where you can view configure backup links in the Data Link layer.
Link Aggregation	This link takes you to a screen where you can logically aggregate physical links to form one logical, higher-bandwidth link.
LLDP	Click the link to unfold the following sub-link menu.
LLDP	This link takes you to screens where you can view LLDP information and configure LLDP and TLV settings.
LLDP MED	This link takes you to screens where you can configure LLDP-MED parameters.
Port Setup	This link takes you to a screen where you can configure settings for individual Switch ports.
SWITCHING	
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.
Mirroring	Click the link to unfold the following sub-link menu.
Mirroring	This link take you to a screen where you can copy traffic from one port or ports to another port in order to examine the traffic from the first port without interference.
Multicast	Click the link to unfold the following sub-link menu.
IPv4 Multicast	This link takes you to screens where you can configure various IPv4 multicast features, IGMP snooping, filtering and create multicast VLANs.
MVR	This link takes you to screens where you can create multicast VLANs and select the receiver ports and a source port for each multicast VLAN.
Static Multicast Forwarding By MAC	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.
Private VLAN	This link takes you to a screen where you can block traffic between ports in a VLAN on the Switch.
QoS	Click the link to unfold the following sub-link menu.
Diffserv	This link takes you to screens where you can enable DiffServ, configure marking rules and set DSCP-to-IEEE802.1p mappings.
Queuing Method	This link takes you to a screen where you can set priorities for the queues of the Switch. This distributes bandwidth across the different traffic queues.
Priority Queue	This link takes you to a screen where you can set priority tags for different traffic types and specify the priority levels.
sFlow	This link takes you to screens where you can configure sFlow settings on the Switch.
Spanning Tree Protocol	Click the link to unfold the following sub-link menu.
Spanning Tree Protocol Status	This link takes you to a screen where you can view the STP status in the different STP modes (RSTP or MSTP) you can configure on the Switch.
Spanning Tree Setup	This link takes you to a screen where you can activate one of the STP modes (RSTP or MSTP) on the Switch.
RSTP	This link takes you to a screen where you can configure the RSTP (Rapid Spanning Tree Protocol) settings on the Switch.
MRSTP	This link takes you to a screen where you can configure the MRSTP (Multiple Rapid Spanning Tree Protocol) settings on the Switch.
MSTP	This link takes you to a screen where you can configure the MSTP (Multiple Spanning Tree Protocol) settings on the Switch.

Table 15 Navigation Panel Links (continued)

LINK	DESCRIPTION
Static MAC Filtering	This link takes you to a screen to set up static MAC filtering rules.
Static MAC Forwarding	This link takes you to a screen where you can configure static MAC addresses for a port. These static MAC addresses do not age out.
VLAN	Click the link to unfold the following sub-link menu.
VLAN Status	This link takes you to a screen where you can view and search all VLAN groups.
VLAN Setup	This link takes you to screens where you can: • configure port-based or 802.1Q VLAN. • view detailed port settings and status of the VLAN group. • configure and view 802.1Q VLAN parameters for the Switch. • configure the static VLAN settings on a port.
Subnet Based VLAN Setup	This link takes you to a screen where you can set up VLANs that allow you to group traffic into logical VLANs based on the source IP subnet you specify.
Protocol Based VLAN Setup	This link takes you to a screen where you can set up VLANs that allow you to group traffic into logical VLANs based on the protocol you specify.
Voice VLAN Setup	This link takes you to a screen where you can set up VLANs that allow you to group voice traffic with defined priority and enable the Switch port to carry the voice traffic separately from data traffic to ensure the sound quality does NOT deteriorate.
MAC Based VLAN Setup	This link takes you to a screen where you can set up VLANs that allow you to group untagged packets into logical VLANs based on the source MAC address of the packet. This eliminates the need to reconfigure the Switch when you change ports. The Switch will forward the packets based on the source MAC address you set up previously.
VLAN Mapping	This link takes you to screens where you can configure VLAN mapping settings on the Switch.
VLAN Stacking	This link takes you to screens where you can activate and configure VLAN stacking.
WoL Relay	This link takes you to a screen where you can configure settings on Wake on LAN Relay.
NETWORKING	
ARP Setup	Click the link to unfold the following sub-link menu.
ARP Learning	This link takes you to a screen where you can configure ARP learning mode on a per-port basis.
Static ARP	This link takes you to a screen where you can create static ARP entries which do not age out.
DHCP	Click the link to unfold the following sub-link menu.
DHCPv4 Relay	This link takes you to screens where you can view DHCPv4 relay status, mode, and configure DHCPv4 relay settings.
DHCPv4 Server	This link takes you to screens where you can view DHCPv4 server status and configure the Switch as a DHCPv4 server.
DHCP Server Guard	This link takes you to a screen where you can specify whether ports are trusted or untrusted ports for DHCP packets.
Static Routing	Click the link to unfold the following sub-link menu.
IPv4 Static Route	This link takes you to a screen where you can configure IPv4 static routes. A static route defines how the Switch should forward traffic by destination IP address and subnet mask.
SECURITY	
AAA	Click the link to unfold the following sub-link menu.
RADIUS Server Setup	This link takes you to a screen where you can configure your RADIUS (Remote Authentication Dial-In User Service) server settings for authentication.

Table 15 Navigation Panel Links (continued)

LINK	DESCRIPTION
TACACS+ Server Setup	This link takes you to a screen where you can configure your TACACS+ (Terminal Access Controller Access Control System Plus) server settings for authentication.
AAA Setup	This link takes you to a screen where you can configure authentication, authorization and accounting services through external servers. The external servers can be either RADIUS or TACACS+ (Terminal Access Controller Access Control System Plus).
Access Control	Click the link to unfold the following sub-link menu.
Service Access Control	This link takes you to a screen where you can decide what services you may use to access the Switch.
Remote Management	This link takes you to a screen where you can specify a group of one or more “trusted computers” from which an administrator may use a service to manage the Switch.
Account Security	This link takes you to a screen where you can configure account security settings on the Switch.
ACL	Click the link to unfold the following sub-link menu.
Classifier	This link takes you to screens where you can configure the Switch to group packets based on the specified criteria.
Policy Rule	This link takes you to a screen where you can configure the Switch to perform special treatment on the grouped packets.
Anti-Arpscan	This link takes you to screens where you can enable anti-arpscan on the Switch and ports, and view the port state. You can also create trusted hosts, view blocked hosts and unblock them.
BPDUGuard	This link takes you to screens where you can enable BPDU guard on the Switch and ports, and view the port state.
Storm Control	This link takes you to a screen to set up broadcast filters.
Errdisable	This link takes you to screens where you can view errdisable status and configure errdisable settings in CPU protection, errdisable detect, and errdisable recovery.
IPv4 Source Guard	Click the link to unfold the following sub-link menu.
IP Source Guard	This link takes you to screens where you can configure filtering of unauthorized DHCP and ARP packets in your network.
DHCP Snooping	This link takes you to screens where you can view DHCP snooping database details and configure DHCP snooping settings on ports or VLANs. You can use DHCP snooping to filter unauthorized DHCP packets on the network and to build the binding table dynamically.
ARP Inspection	This link takes you to screens where you can view ARP inspection status, and configure ARP inspection settings on ports or VLANs. You can use ARP inspection to filter unauthorized ARP packets on the network.
Port Authentication	Click the link to unfold the following sub-link menu. These links take you to screens where you can configure IEEE 802.1x port authentication as well as MAC authentication for clients communicating through the Switch.
802.1x	The link takes you to a screen where you can activate IEEE 802.1x security on a port.
MAC Authentication	The link takes you to a screen where you can activate MAC authentication on a port.
Guest VLAN	The link takes you to a screen where you can activate enable and assign a guest VLAN to a port.
Compound Authentication Mode	The link takes you to a screen where you can allow network access for clients that pass either IEEE 802.1x authentication or MAC authentication, or pass both IEEE 802.1x authentication and MAC authentication.
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.

Table 15 Navigation Panel Links (continued)

LINK	DESCRIPTION
MAINTENANCE	
Certificates	The link takes you to a screen where you can import the Switch's CA-signed certificates.
Cluster Management	This link takes you to a screen where you can configure clustering management and view its status.
Configuration	Click the link to unfold the following sub-link menu.
Restore Configuration	This link takes you to a screen where you can upload a stored device configuration file.
Backup Configuration	This link takes you to a screen where you can save your Switch's configurations (settings) for later use.
Auto Configuration	This link takes you to a screen where you can overwrite the running configuration stored in the Switch's RAM.
Erase Running-Configuration	This link takes you to a screen where you can reset the configuration to the Zyxel default configuration settings.
Save Configuration	This link takes you to a screen where you can save the current configuration (settings) to a specific configuration file on the Switch.
Configure Clone	This link takes you to a screen where you can copy the basic and advanced settings from a source port to a destination port or ports.
Diagnostic	This link takes you to a screen where you can ping IP addresses, run traceroute, test ports and show the location of the Switch.
Firmware Upgrade	This link takes you to a screen to upload firmware to your Switch.
Reboot System	This link takes you to a screen to reboot the Switch without turning the power off.
SSH Authorized Keys	This link takes you to a screen where you can authenticate secure SSH connections between a client computer and the Switch (also called the server) without needing a password to connect to the Switch.
SSH Host Keys	This link takes you to a screen where you can regenerate the Switch's SSH host key.
Tech-Support	This link takes you to a screen where you can download related log reports for issue analysis. Log reports include CPU history and utilization, crash and memory.

The following table describes the links in the navigation panel when the Switch is in Networked AV mode.

Table 16 Navigation Panel Links (Networked AV Mode)

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

Table 16 Navigation Panel Links (Networked AV Mode) (continued)

LINK	DESCRIPTION
IP Setup	This screen allows you to configure the IP address and subnet mask (necessary for Switch management) and set up to 64 IP routing domains.
Logins	This link takes you to a screen where you can change the system login password, as well as configure up to four login details.
SNMP	This link takes you to screens where you can specify the SNMP version and community (password) values, configure where to send SNMP traps from the Switch, enable loopguard/errdisable/poe/linkup/linkdown/ldp/transceiver-dm/storm-control on the Switch, specify the types of SNMP traps that should be sent to each SNMP manager, and add/edit user information.
PORT	
Link Aggregation	This link takes you to screens where you can logically aggregate physical links to form one logical, higher-bandwidth link.
Port Setup	This screen allows you to configure settings for individual Switch ports.
SWITCHING	
Diffserv	This link takes you to screens where you can enable DiffServ, configure marking rules and set DSCP-to-IEEE802.1p mappings.
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.
Multicast	This link takes you to screens where you can view multicast group information, configure various multicast features like IGMP snooping and filtering profile, and create multicast VLANs.
IPv4 Multicast	This link takes you to screens where you can configure various IPv4 multicast features, IGMP snooping, filtering and create multicast VLANs.
Static Multicast Forwarding By MAC	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.
VLAN	This link takes you to screens where you can view and search all static VLAN groups, view detailed port settings and status of the static VLAN group, configure a static VLAN for the Switch, and configure the static VLAN (IEEE 802.1Q) settings on a port.
SECURITY	
Access Control	
Service Access Control	This link takes you to a screen where you can decide what services you may use to access the Switch.
Remote Management	This link takes you to a screen where you can specify a group of one or more “trusted computers” from which an administrator may use a service to manage the Switch.
Storm Control	This link takes you to a screen to set up broadcast filters.
MAINTENANCE	
Configuration	
Restore Configuration	This link takes you to a screen where you can upload a stored device configuration file.
Backup Configuration	This link takes you to a screen where you can save your Switch's configurations (settings) for later use.
Save Configuration	This link takes you to a screen where you can save the current configuration (settings) to a specific configuration file on the Switch.
Firmware Upgrade	This link takes you to a screen to upload firmware to your Switch.
Reboot System	This link takes you to a screen to reboot the Switch without turning the power off.
Tech-Support	This link takes you to a screen where you can download related log reports for issue analysis. Log reports include CPU history and utilization, crash and memory.

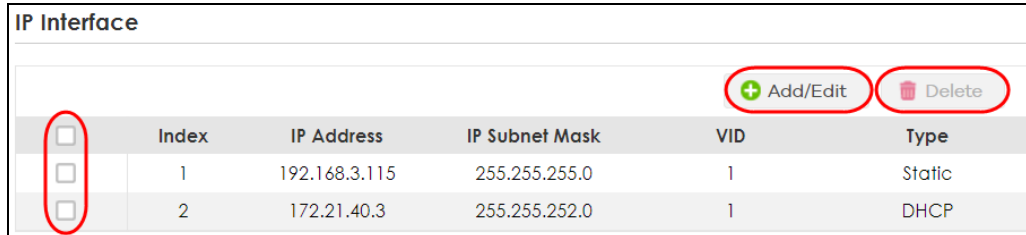
4.5.1 Tables and Lists

The Web Configurator tables and lists provide several options for how to work with their entries.

4.5.1.1 Working with Table Entries

Tables have tool icons for working with table entries as shown next. You can select one or more entries, or select the checkbox in the heading row to select all entries. Use the tool icons to modify the selected entries.

Figure 51 Working with a Table



IP Interface					
☐	Index	IP Address	IP Subnet Mask	VID	Type
☐	1	192.168.3.115	255.255.255.0	1	Static
☐	2	172.21.40.3	255.255.252.0	1	DHCP

The following table describes the most common table icons.

Table 17 Common Table Icons

LABEL	DESCRIPTION
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click this to create a new entry or edit a selected entry. A configuration screen where you can add a new entry or modify the settings of the selected entry will open. In some configuration screens, the Add/Edit button is replaced by the Edit button. This means you can only edit the existing entries in the table.
Delete	To remove entries, select the entries and click Delete .

When viewing a list, you can click on an index number to view more details about the entry. If the list has more than one page, click the arrow button to navigate to different pages of entries.

Figure 52 Working on a List

The Number of VLAN: 13

⏪ < Page 1 of 2 > ⏩						
Index	VID	Name	Tagged Port	Untagged Port	Elapsed Time	Status
1	1	1		1-28	19:35:49	Static
2	2	2			0:01:36	Static
3	3	3			0:01:30	Static
4	4	4			0:01:22	Static
5	8	8			0:00:57	Static
6	9	9			0:00:52	Static
7	10	10			0:00:45	Static
8	11	11			0:00:40	Static
9	12	12			0:00:34	Static
10	13	13			0:00:21	Static
⏪ < Page 1 of 2 > ⏩						

4.6 Save Your Configuration

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

Click the **Save** link in the upper right of the Web Configurator to save your configuration to non-volatile memory. Non-volatile memory refers to the Switch's storage that remains even if the Switch's power is turned off.

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

4.7 Switch Lockout

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

- 1 Delete the management VLAN (default is VLAN 1).
- 2 Delete all port-based VLANs with the CPU port as a member. The "CPU port" is the management port of the Switch.
- 3 Filter all traffic to the CPU port.
- 4 Disable all ports.
- 5 Misconfigure the text configuration file.
- 6 Forget the password and/or IP address.

- 7 Prevent all services from accessing the Switch.
- 8 Change a service port number but forget it.
- 9 You forgot to log out of the Switch from a computer before logging in again on another computer.

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

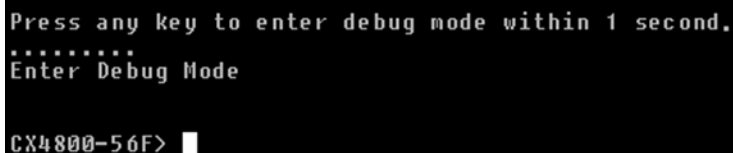
4.8 Restoring the Switch to the Factory Defaults

If you lock yourself (and others) from the Switch or forget the administrator password, you will need to restore the Switch back to the factory defaults.

Restoring the Switch to the factory defaults replaces the current configuration file with the factory-default configuration file. This means that you will lose all previous configurations. The password will be reset to the default value (see the bottom label on the Switch) and the IP address to '192.168.1.1'.

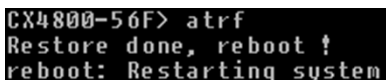
To restore the Switch back to the factory defaults, do the following:

- 1 Connect to the console port using a computer with terminal emulation software. See [Section 3.2.3 on page 40](#) 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 of the terminal emulation software.
- 3 When you see the message 'Press any key to enter debug mode within 1 second', press any key to stop the automatic boot.



```
Press any key to enter debug mode within 1 second.
.....
Enter Debug Mode
CX4800-56F> █
```

- 4 In debug mode, enter 'atrf'. The Switch will restart and load the factory-default configurations.



```
CX4800-56F> atrf
Restore done, reboot !
reboot: Restarting system
```

4.8.1 Reboot the Switch

Press the **RESET** button to reboot the Switch without turning the power off. See [Section 3.4 on page 46](#) for more information about the LED behavior.

4.9 Log Out of the Web Configurator

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

Figure 53 Logout button



4.10 Help

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

Click the **Help** icon on a Web Configurator screen to view an online help description (shown as below) of that screen.

Figure 54 Online Web Help

DASHBOARD

This screen displays general device information, system status, system resource usage, and port status.

The following table describes the labels in this screen.

LABEL	DESCRIPTION
Pause Auto Refresh	The DASHBOARD screen automatically refreshes every 30 seconds. Click this to disable the auto refresh. Click Resume Auto Refresh to enable.
Port Status	This displays individual port type, status, and connection speed of the Switch. Click on a port to open the port's status panel. Use the status panel to enable/disable a port and view its basic information. For example, link speed and port utilization. In Stacking mode, this displays the port status of the slot (Switch) selected in the SLOT field.

CHAPTER 5

Initial Setup Example

5.1 Overview

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

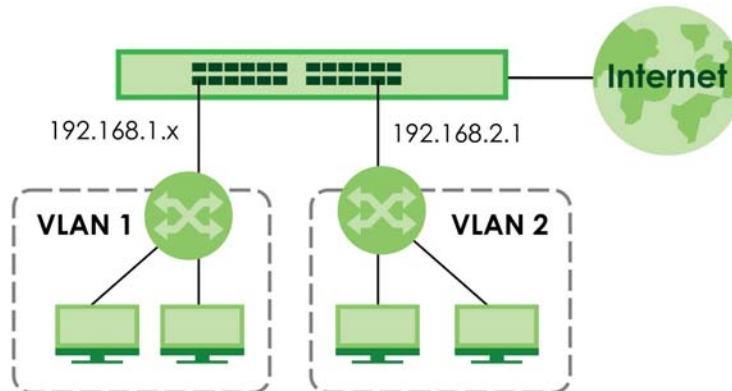
The following lists the configuration steps for the initial setup:

- [Configure Switch Management IP Address](#)
- [Change the Administrator Login Password](#)
- [Create a VLAN](#)
- [Set Port VID](#)
- [How to Use DHCPv4 Relay on the Switch](#)
- [How to Use Auto Configuration through a DHCP Server on the Switch](#)
- [How to Back Up the Configuration](#)
- [How to Restore the Configuration](#)
- [How to Upgrade the Firmware](#)

5.2 Configure Switch Management IP Address

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

Figure 55 Getting Started: Management IP Address



- 1 Connect your computer to any Ethernet port on the Switch. Make sure your computer is in the same subnet as the Switch.
- 2 Open your web browser and enter "setup.zyxel" or "192.168.1.1" (the default IP address) in the address bar to access the Web Configurator. See [Section 4.2 on page 49](#) for more information.

Note: You can always use the domain name "setup.zyxel" to access the Web Configurator whether the Switch is using a DHCP-assigned IP or static IP address. This requires your PC to be directly connected to the Switch.

- 3 Go to the **SYSTEM > IP Setup > IP Setup** screen. Click **Add/Edit**.

IP Setup

Default Gateway: 0.0.0.0

Domain Name Server 1:

Domain Name Server 2:

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

Out-of-band Management IP Address

IP Address: 192.168.0.1

IP Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

IP Interface

	Index	IP Address	IP Subnet Mask	VID	Type
☐	1	172.21.40.8	255.255.252.0	1	DHCP

The following screen appears.

☐ DHCP Client

Option-60: ☒

Class-ID: Zyxel Corporation

☒ Static IP Address

IP Address: 192.168.2.1

IP Subnet Mask: 255.255.255.0

VID: 2

Apply Clear Cancel

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

- 5 In the **VID** field, enter the ID of the VLAN group to which you want this management IP address to belong. In this example, enter VLAN ID 2. This is the same as the VLAN ID you configure in the **Static VLAN** screen. See [Section 5.4 on page 84](#) for more information.
- 6 Click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

5.3 Change the Administrator Login Password

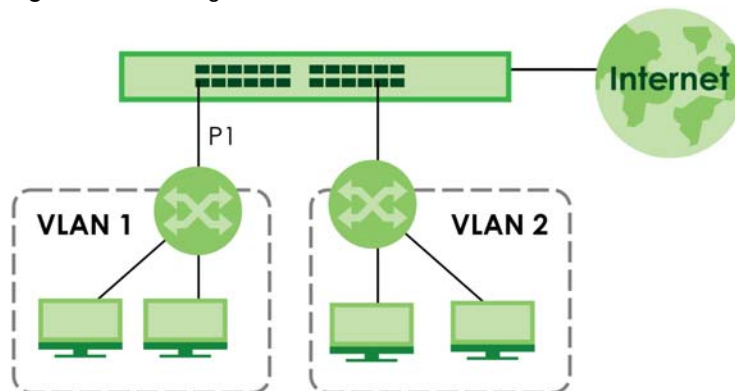
You can change the administrator login password regularly to ensure the security of your Switch. See [Section 20.1 on page 145](#) for more information.

5.4 Create a VLAN

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

In this example, you want to configure port 1 (**P1**) as a member of VLAN 2.

Figure 56 Getting Started: VLAN



- 1 Go to the **SWITCHING > VLAN > Static VLAN** screen. Click **Add/Edit**.

Static VLAN			
VLAN Port Setup		GVRP	
		+ Add/Edit Delete	
☐	VID	Active	Name
☐	1	ON	1

- 2 The following screen appears. Click the switch to set this VLAN to **Active**, enter a descriptive name in the **Name** field and enter "2" in the **VLAN Group ID** field for the **VLAN2** network.

Active ☒ ON

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

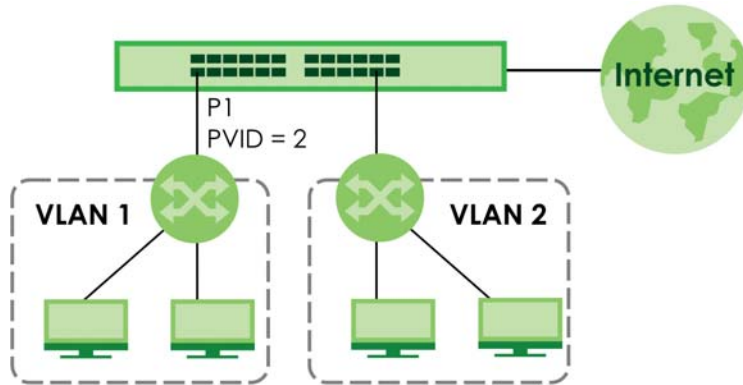
Note: The **VLAN Group ID** field in this screen and the **VID** field in the **SYSTEM > IP Setup > IP Status** screen refer to the same VLAN ID.

- 3 Since the **VLAN2** network is connected to port 1 on the Switch, select **Fixed** to configure port 1 to be a permanent member of the VLAN only.
- 4 To ensure that VLAN-unaware devices (such as computers and hubs) can receive frames properly, clear the **Tx Tagging** checkbox to set the Switch to remove VLAN tags before sending.
- 5 Click **Apply** to save the settings to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

5.5 Set Port VID

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

In the example network, configure **2** as the port VID (**PVID**) on port 1 (**P1**) so that any untagged frames received on that port get sent to VLAN 1.

Figure 57 Getting Started: Port VID

- 1 Go to the **SWITCHING > VLAN > VLAN Setup > VLAN Port Setup** screen.

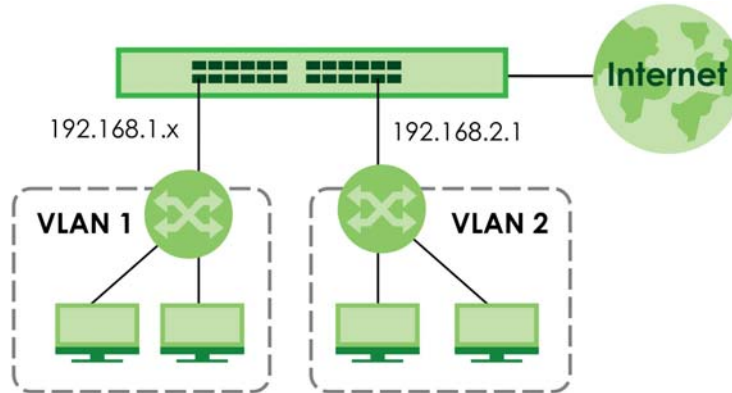
Static VLAN **VLAN Port Setup** GVRP

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

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

5.5.1 Configure Switch Management IP Address

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

Figure 58 Getting Started: Management IP Address

- 1 Connect your computer to any Ethernet port on the Switch. Make sure your computer is in the same subnet as the Switch.
- 2 Open your web browser and enter “setup.zyxel” or “192.168.1.1” (the default IP address) in the address bar to access the Web Configurator. See [Section 4.2 on page 49](#) for more information.

Note: You can always **use** the domain name “setup.zyxel” to access the Web Configurator whether the Switch is using a DHCP-assigned IP or static IP address. This requires your PC to be directly connected to the Switch.

- 3 Go to the **SYSTEM > IP Setup > IP Setup** screen. Click **Add/Edit**.

IP Status **IP Setup** Network Proxy Configuration

IP Setup

Default Gateway:

Domain Name Server 1:

Domain Name Server 2:

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

Apply **Cancel**

Out-of-band Management IP Address

IP Address:

IP Subnet Mask:

Default Gateway:

Apply **Cancel**

IP Interface

	Index	IP Address	IP Subnet Mask	VID	Type
☐	1	172.21.40.8	255.255.252.0	1	DHCP

+ Add/Edit **Delete**

The following screen appears.

☐ DHCP Client
 Option-60 ☒
 Class-ID Zyxel Corporation
☒ Static IP Address
 IP Address 192.168.2.1
 IP Subnet Mask 255.255.255.0
 VID 2

- 4 For the **VLAN2** network, enter 192.168.2.1 as the IP address and 255.255.255.0 as the subnet mask.
- 5 In the **VID** field, enter the ID of the VLAN group to which you want this management IP address to belong. In this example, enter VLAN ID 2. This is the same as the VLAN ID you configure in the **Static VLAN** screen.
- 6 Click **Apply** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

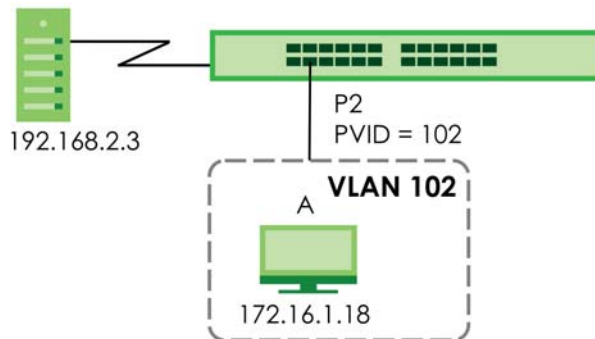
5.6 How to Use DHCPv4 Relay on the Switch

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

5.6.1 DHCP Relay Tutorial Introduction

In this example, you have configured your DHCP server (192.168.2.3) and want to have it assign a specific IP address (say 172.16.1.18) to DHCP client **A** based on the system name, VLAN ID and port number in the DHCP request. Client **A** connects to the Switch's port 2 (**P2**) in VLAN 102.

Figure 59 Getting Started: DHCP Relay Scenario



5.6.2 Create a VLAN

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

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

- 3 Go to **SWITCHING > VLAN > VLAN Setup > Static VLAN**. Click **Add/Edit**.

VID	Active	Name
1	ON	1

- 4 The following screen appears. Enable the switch button to set this VLAN to **Active**. Enter a descriptive name (VLAN 102 for example) in the **Name** field and enter "102" in the **VLAN Group ID** field.

Active ☒ ON

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

- 5 Set port 2 to be a permanent member of this VLAN by selecting **Fixed** in the **Control** field.
- 6 Clear the **Tx Tagging** checkbox to set the Switch to remove VLAN tags before sending.
- 7 Click **Apply** to save the settings to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.
- 8 Go to **VLAN > VLAN Setup > VLAN Port Setup**. Enter "102" in the **PVID** field for port 2 to add a tag to incoming untagged frames received on that port so that the frames are forwarded to the VLAN group that the tag defines.

Static VLAN **VLAN Port Setup** GVRP

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

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

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

5.6.3 Configure DHCPv4 Relay

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

- 1 Click **NETWORKING > DHCP > DHCPv4 Relay > DHCP Smart Relay**. Enable the **Active** switch button.

The screenshot shows the 'DHCP Smart Relay' configuration page. The 'Active' toggle is turned ON. The 'Remote DHCP Server 1' field is set to '192.168.2.1'. The 'Remote DHCP Server 2' and 'Remote DHCP Server 3' fields are set to '0.0.0.0'. The 'Option 82 Profile' dropdown is set to 'default1'. The 'Apply' button is highlighted with a red circle. Below the configuration fields is a table with columns 'Index', 'Port', and 'Profile Name'.

Index	Port	Profile Name

- 2 Enter the DHCP server's IP address (192.168.2.3 in this example) in the **Remote DHCP Server 1** field.
- 3 Select **default1** or **default2** in the **Option 82 Profile** field.
- 4 Click **Apply** to save your changes back to the run-time memory.
- 5 Click the **Save** link in the upper right of the Web Configurator to save your configuration permanently.
- 6 The DHCP server can then assign a specific IP address based on the DHCP request.

5.6.4 Troubleshooting

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

- 1 Client **A** is connected to the Switch's port 2 in VLAN 102.
- 2 You configured the correct VLAN ID, port number and system name for DHCP relay on both the DHCP server and the Switch.
- 3 You clicked the **Save** link on the Switch to have your settings take effect.

5.7 How to Use Auto Configuration through a DHCP Server on the Switch

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

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

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

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

Setting up a DHCP Server

- 1 Set up a dynamic IP addresses pool so the DHCP server will assign an IP address to the Switch in that range.
- 2 Set up a TFTP server IP address, so the Switch will know where to load the auto configuration file.
- 3 Set up the filename of the auto configuration file, so the Switch will know which file to load when you reboot the Switch.
 - Enter the filename of an auto configuration file. The Switch will load this auto configuration file when rebooting with DHCP option 60 disabled.
 - If you want to load the auto configuration file with DHCP option 60 enabled and a Vendor Class Identifier assigned when you reboot the Switch, follow the instruction below. Otherwise, skip this step.
Enter the filename of an auto configuration file. Set up a Vendor Class Identifier. To have the Switch load this auto configuration file, two conditions listed above must be met. Please refer to the following steps to see how to set up a Vendor Class Identifier on the Switch.

Setting up a TFTP Server

- 1 Select a directory on the TFTP server.
- 2 Put the configuration files in that directory.

Setting Up the Switch

- 1 Open the Web Configurator. Go to the **MAINTENANCE > Configuration > Auto Configuration > Auto Configuration** screen.
- 2 Enable the switch button in the **Active** field to enable auto configuration. Select **DHCP** in the **Mode** field, and enter the VLAN ID where the DHCP server belongs to in the **DHCP VLAN ID** field. Click **Apply** to save your changes.

Auto Configuration

Mode: None
State: None
Filename:

Active: ☒ ON
Mode:
DHCP VLAN ID:
HTTPS URL:

Apply Cancel

- 3 Go to the **SYSTEM > IP Setup > IP Setup** screen. Click the **Add/Edit** button in the **IP Interface** table to open the configuration screen.
- 4 Select **DHCP Client**.
- 5 If you want to load the auto configuration file with DHCP option 60 enabled and a Vendor Class Identifier assigned when you reboot the Switch, follow the instruction below. Otherwise, skip this step. In the **SYSTEM > IP Setup > IP Setup > Add/Edit** screen, select the checkbox in the **Option-60** field. Enter a Vendor Class Identifier in the **Class-ID** field, and specify the VLAN interface in the **VID** field. In this example, we use "Zyxel Corp" and **VID 1**. Click **Apply**.

☒ **DHCP Client**
Option-60: ☒
Class-ID:
☐ Static IP Address
IP Address:
IP Subnet Mask:
VID:

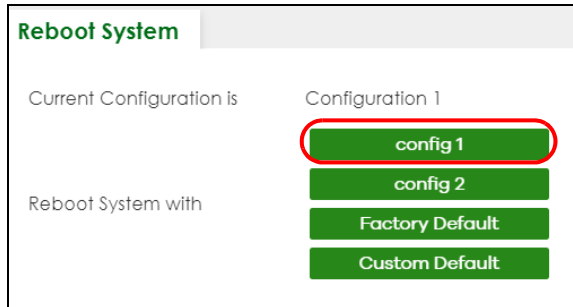
Apply Clear Cancel

- 6 You need to save the current configuration in a configuration file, so the Switch will load the auto configuration file from the TFTP server automatically when rebooting. Go to the **MAINTENANCE > Configuration > Save Configuration > Save Configuration** screen. Click the **Config 1**, **Config 2**, or **Custom Default** button.

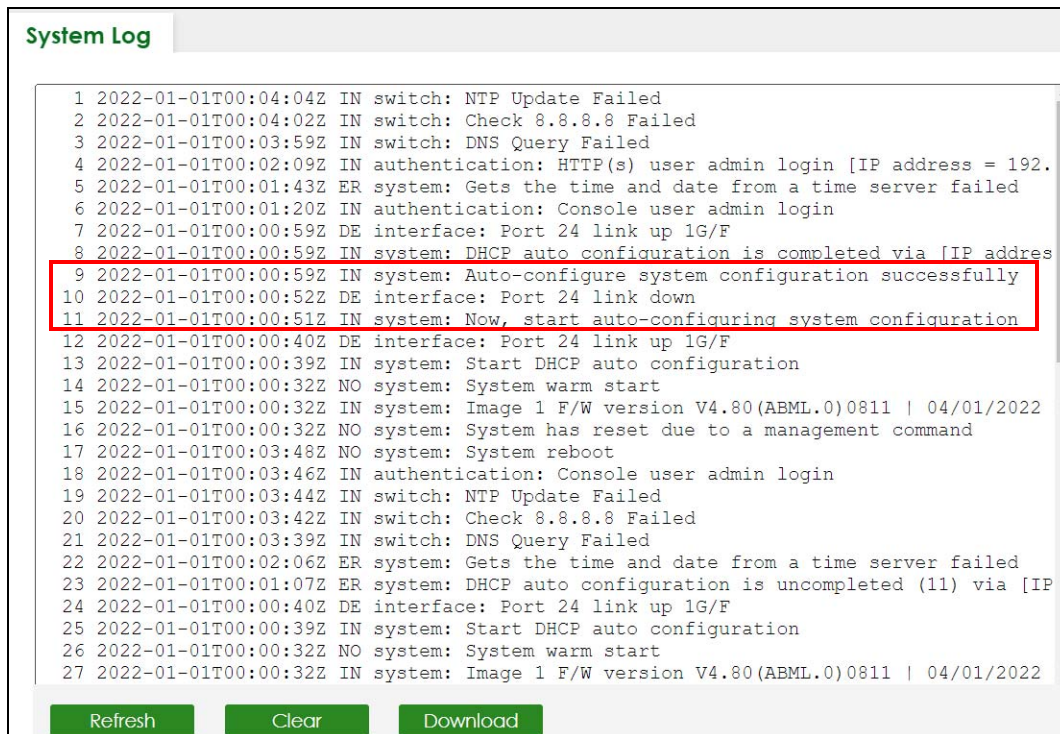
Save Configuration

Save Configuration as: **Config 1** --
Config 2 --
Custom Default --

- 7 Click the same button in the **MAINTENANCE > Reboot System > Reboot System** screen to reboot the Switch, and load the auto configuration setting as configured before. For example, if you save the auto configuration setting to **Config 1**, you need to click the **Config 1** button in the **Reboot System** screen.



- 8 Go to the **MONITOR > System Log > System Log** screen to see if auto configuration was performed successfully.

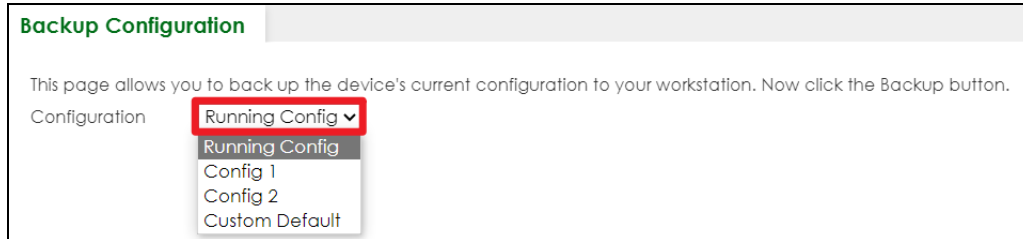


- 9 Check the screens to see if it is the configuration file you want to load. If it is not, go through the steps above to check your configurations. If it is, click **Save** at the top right corner of the Web Configurator to save the configuration permanently.

5.8 How to Back Up the Configuration

This section shows you how to back up the configuration. You should regularly back up your configuration especially before you make major configuration changes.

- 1 Log into the Web Configurator. Go to **MAINTENANCE > Configuration > Backup Configuration > Backup Configuration**.
- 2 Select the configuration you want to back up from the drop-down list. In this tutorial, you want to back up the currently running configuration, select **Running Config**.



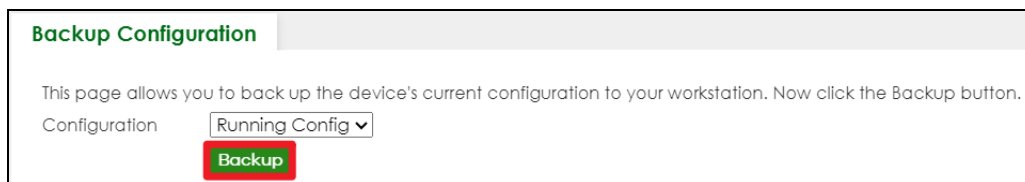
Backup Configuration

This page allows you to back up the device's current configuration to your workstation. Now click the Backup button.

Configuration **Running Config ▼**

- Running Config
- Config 1
- Config 2
- Custom Default

- 3 Click **Backup**.



Backup Configuration

This page allows you to back up the device's current configuration to your workstation. Now click the Backup button.

Configuration **Running Config ▼**

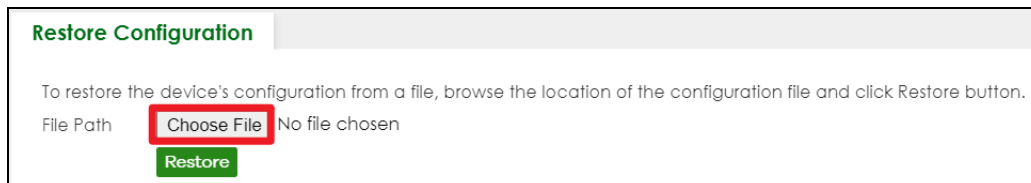
Backup

- 4 Save the downloaded file to your computer.

5.9 How to Restore the Configuration

This section shows you how to restore a previously saved configuration file from your computer to the Switch.

- 1 Log into the Web Configurator. Go to **MAINTENANCE > Configuration > Restore Configuration > Restore Configuration**.
- 2 Click **Choose File** and select the previously saved configuration file.



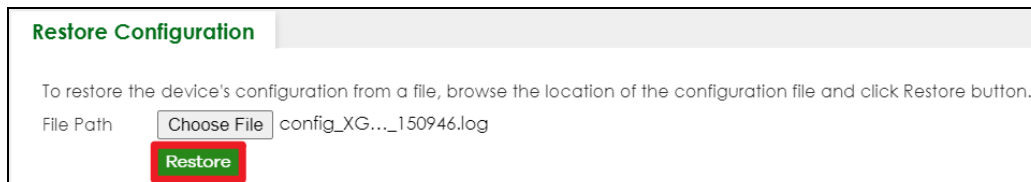
Restore Configuration

To restore the device's configuration from a file, browse the location of the configuration file and click Restore button.

File Path **Choose File** No file chosen

Restore

- 3 Click **Restore**.



Restore Configuration

To restore the device's configuration from a file, browse the location of the configuration file and click Restore button.

File Path **Choose File** config_XG..._150946.log

Restore

- Wait for the configuration to be restored. The screen will go to the login page. Log in with the default user name, **admin**, and default password on the label on the bottom of the Switch. Set up a new password to re-login.
- The Switch is now running with the uploaded configuration.

Restore Configuration

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

 Restore Configuration successfully.

5.10 How to Upgrade the Firmware

This section shows you how to upgrade the Switch's firmware through NCC, the Web Configurator. You should always use the most recent firmware to get the latest features, improvements, and bug fixes.

5.10.1 Firmware Upgrade Through NCC

Follow the steps below to upgrade the firmware to the Switch.

- Log into the NCC. Go to **Site-wide > Configure > Firmware management > Devices**. Find the Switch in the device list. The **Availability** of the Switch is **Upgrade available** when a newer firmware is available.

Firmware management

Overview
Devices

Status: Any Device type: Any Tag: Any Model: Any Current version: Any Firmware status: Any Firmware type: Any Availability: Any Locked: Any

1 selected in 7 devices

Status	Device type	Model	MAC address	S/N	Current version	Firmware status	Availability	Firmware type	Upgrade
☐	Switch	XGS1935-28HP	00000000000000000000	0000000000000000	V4.90(ACJX.0)b5 05/15/2024	Good	Upgrade available	Stable	No
☐	Access point	WAX510D	00000000000000000000	0000000000000000	V6.00(ABTF.0)IT_20221019121600	Custom	Upgrade available	General Availability	No

- Select the checkbox of the Switch, then click **Upgrade now**.

Firmware management

Overview
Devices

Status: Any Device type: Any Tag: Any Model: Any Current version: Any Firmware status: Any Firmware type: Any Availability: Any Locked: Any

1 selected in 7 devices

Status	Device type	Model	MAC address	S/N	Current version	Firmware status	Availability	Firmware type	Upgrade
☒	Switch	XGS1935-28HP	00000000000000000000	0000000000000000	V4.90(ACJX.0)b5 05/15/2024	Good	Upgrade available	Stable	No
☐	Access point	WAX510D	00000000000000000000	0000000000000000	V6.00(ABTF.0)IT_20221019121600	Custom	Upgrade available	General Availability	No

- Check that the **Availability** of the Switch is **Up to date**.

Firmware management

Overview

Devices

Status

Any

Device type

Any

Tag

Any

Model

Any

Current version

Any

Firmware status

Any

Firmware type

Any

Availability

Any

Locked

Any

Upgrade now

+ Schedule upgrade

Reset

1 selected in 7 devices

☐	Status	Device type	Model	MAC address	S/N	Current version	Firmware status	Availability	Firmware type	Upgrade
☐		Switch	XGS1935-28HP	XXXXXXXXXX	XXXXXXXXXX	V4.90(ACJX.0)b6 05/30/2024	Good	Up to date	Latest	No
☐		Access point	WAX510D	XXXXXXXXXX	XXXXXXXXXX	V6.00(ABTF.0)IT_20221019121600	Custom	Upgrade available	General Availability	No

5.10.2 Firmware Upgrade Through the Web Configurator

Follow the steps below to download the firmware from the Zyxel website first, then upgrade the Switch's firmware through the Web Configurator.

Download the Firmware

Follow the steps below to download the firmware.

- 1 Go to <https://www.zyxel.com/global/en/support> > **Support & Training** > **Download Library**.
- 2 Search for the model number of the Switch.
- 3 Download the firmware to your computer and then unzip it.

Upgrade the Firmware

The Switch supports dual firmware images, **Firmware 1** and **Firmware 2**. You can apply one of these images as an active image, and the other one as a backup image. Follow the steps below to upload and apply the firmware to the Switch.

Note: Only the active image is loaded when the Switch starts up.

- 1 Log into the Web Configurator. Go to **MAINTENANCE** > **Firmware Upgrade** > **Firmware Upgrade**.
- 2 Select the firmware you want to upgrade from the drop-down list. In this tutorial, you want to upload the downloaded firmware to Firmware 1 on the Switch. Select **1**.

To upgrade the switch firmware, browse the location of the binary (.BIN) file and click Upgrade button.

Firmware 1 ▼

File Path Choose File No file chosen

Upgrade

- 3 Click **Choose File** and select the downloaded, unzipped firmware file.

To upgrade the switch firmware, browse the location of the binary (.BIN) file and click Upgrade button.

Firmware 1 ▼

File Path Choose File No file chosen

Upgrade

- 4 Click **Upgrade** to upload the new firmware.

To upgrade the switch firmware, browse the location of the binary (.BIN) file and click Upgrade button.

Firmware 1 ▾

File Path Choose File 100ACJN0b6.bin

Upgrade

- 5 The upgraded firmware will display in **Firmware Upgrade**. Check that the version is correct for **Firmware 1**.

Firmware Upgrade		
Name	Version	
CX4800-56F	Running	V1.00[ACJN.0]b5 07/02/2024
	Firmware 1	V1.00[ACJN.0]b6 07/12/2024
	Firmware 2	V1.00[ACJN.0]b5 07/02/2024

- 6 The Switch is currently using Firmware 2. To allow the Switch to use Firmware 1, select **1** from **Config Boot Image**, then click **Apply**.

Boot Image

Current Boot Image Firmware 2

Config Boot Image Firmware 1 ▾

Apply Cancel

- 7 Unplug the power cable and then plug it back into the Switch. Close the current window of the Web Configurator, then log into the Web Configurator with a new window.
- 8 Go to **MAINTENANCE > Firmware Upgrade > Firmware Upgrade**. Check that the **Running** firmware is the same as **Firmware 1** version.

Firmware Upgrade		
Name	Version	
CX4800-56F	Running	V1.00[ACJN.0]b6 07/12/2024
	Firmware 1	V1.00[ACJN.0]b6 07/12/2024
	Firmware 2	V1.00[ACJN.0]b5 07/02/2024

CHAPTER 6

DASHBOARD

This chapter gives a quick introduction on the **DASHBOARD** screen.

The **DASHBOARD** screen automatically appears after you log into the Web Configurator.

6.1 User Interface

In the **DASHBOARD** screen, you can easily monitor the system status with the following tools (see [DASHBOARD](#) for more information):

- Visualized **Port Status** section with clickable port icons that provide information of that port, an ON/OFF switch button to enable/disable the port (see [Port Status](#)).
- Visualized **Cloud Control Status** section that displays the NCC connection status using three connection-stage circles.
- Clickable hardware status monitoring sections that directly link to the **MONITOR > System Information** screen.
- Editable **Quick Link** section which provides shortcuts to configuration screens that you might frequently use (See [Quick Links to Use](#)).
- A **Search** tool on the upper right of the screen that you can use to search for the configuration screens you want to access (see [Web Configurator Layout](#)).

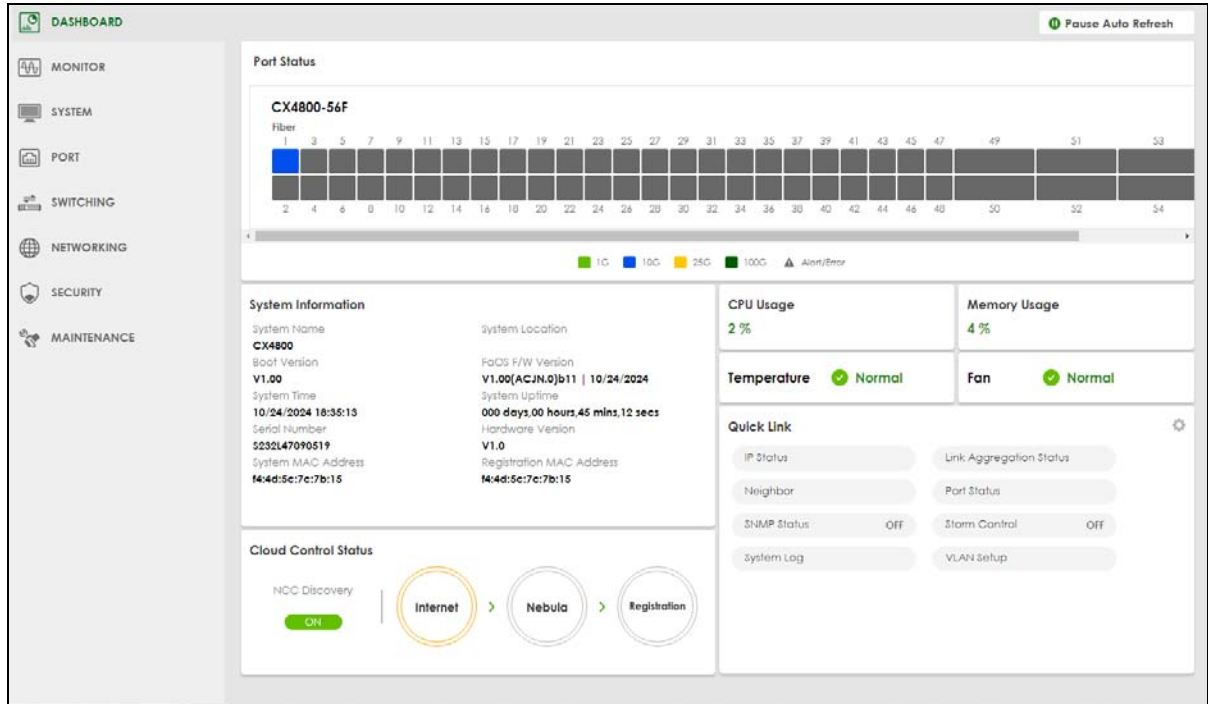
The left navigation panel is structured into a task-based UI. You can display the sub-menu in the **MONITOR**, **SYSTEM**, **PORT**, **SWITCHING**, **NETWORKING**, **SECURITY**, or the **MAINTENANCE** section by clicking their icons. See [Web Configurator Layout](#) for more information.

Find the latest release notes in: [Download Library](#).

6.2 DASHBOARD

This screen displays general device information, system status, system resource usage, and port status.

Click **DASHBOARD** in the navigation panel to open the following screen.

Figure 60 DASHBOARD

The following table describes the labels in this screen.

Table 18 DASHBOARD

LABEL	DESCRIPTION
Pause Auto Refresh	The DASHBOARD screen automatically refreshes every 30 seconds. Click this to disable the auto refresh. Click Resume Auto Refresh to enable.
Port Status	This displays individual port type, status, and connection speed of the Switch. Click on a port to open the port's status panel. Use the status panel to enable/disable a port and view its basic information. For example, link speed, port utilization, and uptime.
System Information	
System Name	This field displays the name used to identify the Switch on any network.
System Location	This field displays the geographic location name you set for the Switch.
Boot Version	This field displays the version number and date of the boot module that is currently on the Switch.
FaOS F/W Version	This field displays the version number and date of the firmware the Switch is currently running.
System Time	This field displays the current date and time in the UAG. The format is mm/dd/yyyy hh:mm:ss.
System Uptime	This field displays how long the Switch has been running since it last restarted or was turned on.
Serial Number	This field displays the serial number of this Switch. The serial number is used for device tracking and control.
Hardware Version	This field displays the hardware version of the Switch.
System MAC Address	This field displays the MAC address of the Switch.

Table 18 DASHBOARD (continued)

LABEL	DESCRIPTION
Registration MAC Address	This is the MAC address reserved for NCC registration. Use this MAC address to register the Switch on NCC.
Cloud Control Status	This field displays: • The Switch Internet connection status. • The connection status between the Switch and NCC. • The Switch registration status on NCC. Mouse over the circles to display detailed information. To pass your Switch management to NCC, first make sure your Switch is connected to the Internet. Then go to NCC and register your Switch. Click Cloud Control Status or the switch button to go to the SYSTEM > Cloud Management screen. You can enable/disable NCC Discovery or view the NCC connection status in the Cloud Management screen. 1. Internet Green – The Switch is connected to the Internet. Orange – The Switch is not connected to the Internet. 2. Nebula Green – The Switch is connected to NCC. Gray – The Switch is not connected to NCC. 3. Registration Green – The Switch is registered on NCC. Gray – The Switch is not registered on NCC. Note: All circles will gray out if you disable Nebula Discovery. Note: If a circle displays orange or gray, hover the mouse over the circle to check the diagnostic message.
NCC Discovery	This displays if NCC discovery is enabled on the Switch. The Switch will connect to NCC and change to the NCC management mode if it: • is connected to the Internet. • has been registered on NCC.
CPU Usage	This displays the current CPU usage percentage. Click to go to the MONITOR > System Information > System Information screen to check the detailed information.
Memory Usage	This displays the current RAM usage percentage. Click to go to the MONITOR > System Information > System Information screen to check the detailed information.
Temperature	The Switch has temperature sensors that are capable of detecting and reporting if the temperature rises above the threshold. This displays the Switch's current device temperature level. Click to go to the MONITOR > System Information > System Information screen to check the detailed information.

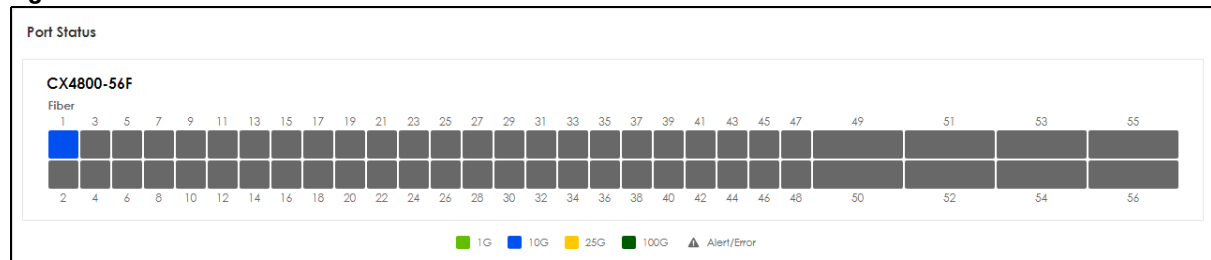
Table 18 DASHBOARD (continued)

LABEL	DESCRIPTION
Fan	Each fan of the Switch has a sensor that is capable of detecting and reporting if the fan speed falls below the threshold. This displays the Switch's overall fan speed status. Click to go to the MONITOR > System Information > System Information screen to check the detailed information.
Quick Link	This section provides shortcut links to specific configuration screens. Click the edit button to choose the quick links to show.

6.2.1 Port Status

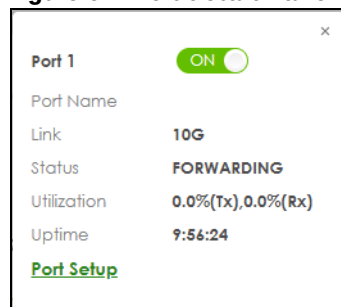
The **Port Status** section provides visualized port status for monitoring. Each port displays a status color determined by the their link speed.

Figure 61 Port Status



Click on a port to display a port's status panel.

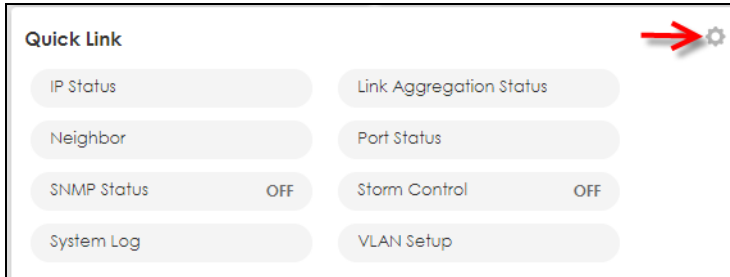
Figure 62 Port details Panel



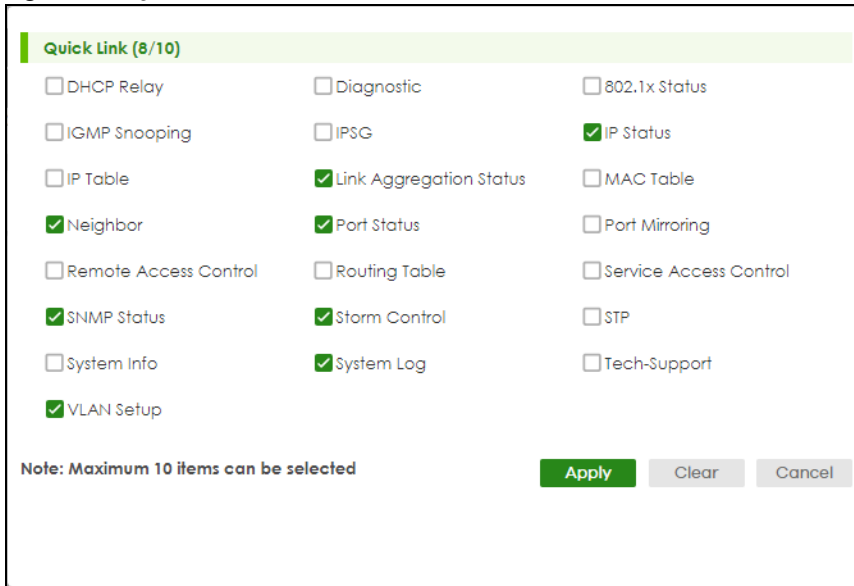
The port details pane displays status information such as link speed, port utilization, uptime, and has an ON/OFF switch button. Click the switch button to enable/disable the port.

6.2.2 Quick Links to Use

The quick links in the **Quick Link** section provide shortcuts to specific configuration screens. You can use the quick links to directly access the screens that you would frequently use. You can also decide which quick links to be put on the **DASHBOARD** screen using the **Edit** button.

Figure 63 Quick Links

The setup panel displays after you click the **Edit** button.

Figure 64 Quick Link Selection

Select the quick links you want and click **Apply**. The selected quick links will be displayed in the **Quick Link** section on the **DASHBOARD** screen.

CHAPTER 7

MONITOR

The following chapters introduces the configurations of the links under the **MONITOR** navigation panel.

Quick links to chapters:

- [ARP Table](#)
- [IP Table](#)
- [MAC Table](#)
- [Neighbor](#)
- [Port Status](#)
- [Routing Table](#)
- [System Information](#)
- [System Log](#)

CHAPTER 8

ARP Table

8.1 ARP Table Overview

This chapter introduces the ARP Table.

Address Resolution Protocol (ARP) is a protocol for mapping an Internet Protocol address (IP address) to a physical machine address, also known as a Media Access Control or MAC address, on the local area network.

An IP (version 4) address is 32 bits long. In an Ethernet LAN, MAC addresses are 48 bits long. The ARP Table maintains an association between each MAC address and its corresponding IP address.

8.1.1 What You Can Do

Use the **ARP Table** screen ([Section 8.2 on page 105](#)) to view IP-to-MAC address mappings.

8.1.2 What You Need to Know

When an incoming packet destined for a host device on a local area network arrives at the Switch, the Switch's ARP program looks in the ARP Table and if it finds the address, it sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The Switch fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the Switch puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

8.2 Viewing the ARP Table

Use the ARP table to view IP-to-MAC address mappings and remove specific dynamic ARP entries.

Click **MONITOR > ARP Table > ARP Table** in the navigation panel to open the following screen.

Figure 65 MONITOR > ARP Table > ARP Table

Index	IP Address	MAC Address	VID	Port	Age(s)	Type
1	172.21.56.10	f4:4d:5c:7c:7b:15	1	CPU	0	static
2	172.21.56.36	dc:4a:3e:40:ec:5f	1	1	270	dynamic
3	172.21.59.254	00:00:5e:00:01:04	1	1	205	dynamic

The following table describes the labels in this screen.

Table 19 MONITOR > ARP Table > 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. 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.
Flush	Click Flush to remove the ARP entries according to the condition you specified.
Cancel	Click Cancel to return the fields to the factory defaults.
Index	This is the ARP table entry number.
IP Address	This is the IP address of a device connected to a Switch port with the corresponding MAC address below.
MAC Address	This is the MAC address of the device with the corresponding IP address above.
VID	This field displays the VLAN to which the device belongs.
Port	This field displays the port to which the device connects. CPU means this IP address is the Switch's management IP address.
Age(s)	This field displays how long (in seconds) an entry can still remain in the ARP table before it ages out and needs to be relearned. This shows 0 for a static entry.
Type	This shows whether the IP address is dynamic (learned by the Switch) or static (manually configured in SYSTEM > IP Setup > IP Setup or NETWORKING > ARP Setup > Static ARP).

CHAPTER 9

IP Table

This chapter introduces the **IP table** screen.

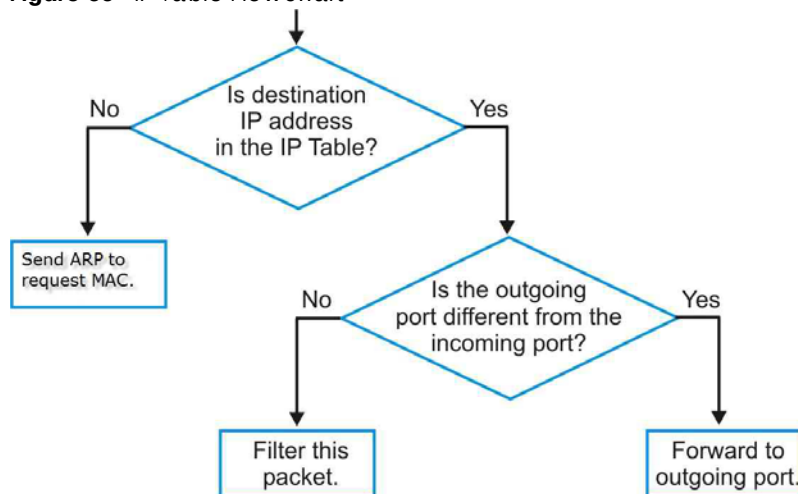
9.1 IP Table Overview

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 66 IP Table Flowchart



9.2 Viewing the IP Table

Click **MONITOR > IP Table > IP Table** in the navigation panel to display the following screen.

Figure 67 MONITOR > IP Table > IP Table

IP Table				
Index	IP Address	VID	Port	Type
1	192.168.2.1	1	22	Dynamic
2	192.168.2.115	1	CPU	Static
3	192.168.2.241	1	18	Dynamic
4	192.168.3.115	100	CPU	Static

Sorting by: IP VID Port

The following table describes the labels in this screen.

Table 20 MONITOR > IP Table > IP Table

LABEL	DESCRIPTION
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.
Type	This shows whether the IP address is Dynamic (learned by the Switch) or Static (belonging to the Switch).
Sorting by	Click one of the following buttons to display and arrange the data according to that button type. The result is then displayed in the IP table.
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.

CHAPTER 10

MAC Table

10.1 MAC Table Overview

This chapter introduces the **MAC Table** screen.

The **MAC Table** screen (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the Switch's ports. 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 **SWITCHING > Static MAC Forwarding** screen).

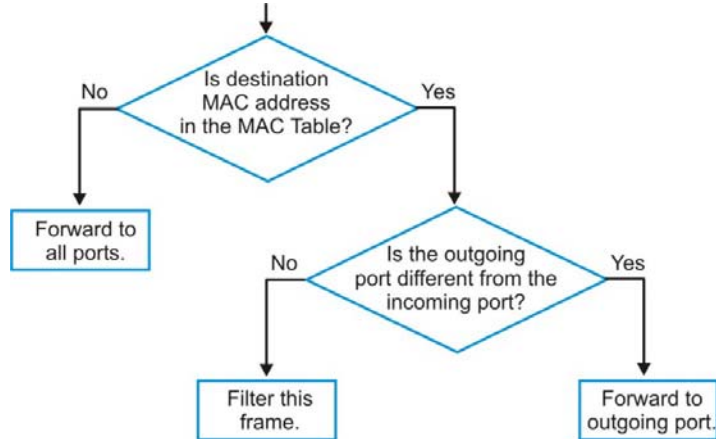
10.1.1 What You Can Do

Use the **MAC Table** screen ([Section 10.2 on page 110](#)) to check whether the MAC address is dynamic or static.

10.1.2 What You Need to Know

The Switch uses the **MAC Table** to determine how to forward frames. See the following figure.

- 1 The Switch examines a received frame and learns the port on which this source MAC address came.
- 2 The Switch checks to see if the frame's destination MAC address matches a source MAC address already learned in the **MAC Table**.
 - If the Switch has already learned the port for this MAC address, then it forwards the frame to that port.
 - If the Switch has not already learned the port for this MAC address, then the frame is flooded to all ports. Too much port flooding leads to network congestion, then the Switch sends an ARP to request the MAC address. The Switch then learns the port that replies with the MAC address.
 - If the Switch has already learned the port for this MAC address, but the destination port is the same as the port it came in on, then it filters the frame.

Figure 68 MAC Table Flowchart

10.2 Viewing the MAC Table

Use this screen to search specific MAC addresses. You can also directly add dynamic MAC addresses into the static MAC forwarding table or MAC filtering table from the MAC table using this screen.

Click **MONITOR > MAC Table > MAC Table** in the navigation panel to display the following screen.

Figure 69 MONITOR > MAC Table > MAC Table

MAC Table

☒ All
 ☐ Static
 ☐ MAC

☐ VID

☐ Port

☐ Trunk

Condition

Sort by

MAC ▼

Type Transfer

☒ Dynamic to MAC forwarding
 ☐ Dynamic to MAC filtering

Search

Transfer

Cancel

Index	MAC Address	VID	Port	Type
1	00-00-5e-00-01-04	1	2	Dynamic
2	00-04-96-9e-3e-1e	1	2	Dynamic
3	00-11-22-33-44-55	1	2	Dynamic

The following table describes the labels in this screen.

Table 21 MONITOR > MAC Table > MAC Table

LABEL	DESCRIPTION
Condition	Select one of the below search conditions and click Search to only display the data which matches the criteria you specified. Select All to display any entry in the MAC table of the Switch. Select Static to display the MAC entries manually configured on the Switch. Select MAC and enter a MAC address in the field provided to display a specified MAC entry. Select VID and enter a VLAN ID in the field provided to display the MAC entries belonging to the specified VLAN. Select Port and enter a port number in the field provided to display the MAC addresses which are forwarded on the specified port. Select Trunk and type the ID of a trunk group to display all MAC addresses learned from the ports in the trunk group.
Sort by	Define how the Switch displays and arranges the data in the summary table below. Select MAC to display and arrange the data according to MAC address. Select VID to display and arrange the data according to VLAN group. Select PORT to display and arrange the data according to port number.
Type Transfer	Select Dynamic to MAC forwarding and click the Transfer button to change all dynamically learned MAC address entries in the summary table below into static entries. They also display in the SWITCHING > Static MAC Forwarding > Static MAC Forwarding screen. Select Dynamic to MAC filtering and click the Transfer button to change all dynamically learned MAC address entries in the summary table below into MAC filtering entries. These entries will then display only in the SWITCHING > Static MAC Filtering > Static MAC Filtering screen and the default filtering action is Discard source.
Search	Click this to search data in the MAC table according to your input criteria.
Transfer	Click this to perform the MAC address transferring you selected in the Type Transfer field.
Cancel	Click Cancel to change the fields back to their last saved values.
Index	This is the incoming frame index number.
MAC Address	This is the MAC address of the device from which this incoming frame came.
VID	This is the VLAN group to which this frame belongs.
Port	This is the port where the above MAC address is forwarded.
Type	This shows whether the MAC address is Dynamic (learned by the Switch) or Static (manually entered in the SWITCHING > Static MAC Forwarding > Static MAC Forwarding screen).

CHAPTER 11

Neighbor

11.1 Neighbor Overview

The **Neighbor** screen allows you to view a summary and manage the Switch's neighboring devices. It uses Layer Link Discovery Protocol (LLDP) to discover all neighbor devices connected to the Switch including non-Zyxel devices. You can use this screen to perform tasks on the neighboring devices like login.

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

11.1.1 What You Can Do

Use the **Neighbor** screen ([Section 11.2 on page 112](#)) to view a summary and manage the Switch's neighbor devices.

Use the **Neighbor Details** screen ([Section 11.2.1 on page 113](#)) to view more detailed information on the Switch's neighbor devices.

11.2 Neighbor

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

Figure 70 MONITOR > Neighbor > Neighbor

Neighbor				
Neighbor Details				
Port	Port Name	Link	System Name	IPv4
1		10G/F	GS2220	172.21.56.39
2		Down	--	
3		Down	--	
4		Down	--	
5		Down	--	
6		Down	--	
7		Down	--	
8		Down	--	

The following table describes the fields in the above screen.

Table 22 MONITOR > Neighbor > Neighbor

LABEL	DESCRIPTION
Port	This shows the port of the Switch, on which the neighboring device is discovered.
Port Name	This shows the port description of the Switch.
Link	This shows the speed (either 1G for 1 Gbps, 10G for 10 Gbps, 25G for 25 Gbps, or 100G for 100 Gbps) and the duplex (F for full duplex or H for half). This field displays Down if the port is not connected to any device.
System Name	This shows the system name of the neighbor device.
IPv4	This shows the IPv4 address of the neighbor device. The IPv4 address is a hyper link that you can click to log into and manage the neighbor device through its Web Configurator.

11.2.1 Neighbor Details

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

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

Click **MONITOR > Neighbor > Neighbor Details** to see the following screen.

Figure 71 MONITOR > Neighbor > Neighbor Details

Neighbor Neighbor Details

Search Ports...

Port 1

Desc.: -- Link Speed: 10G/F

Remote				
System Name:	Port Bridge:	Model:	MAC:	Firmware:
--	dc:4a:3e:40:ec:5f	--	dc:4a:3e:40:ec:5f	--
Location:	Desc.:	IPv4:		
--	--	--		
System Name:	Port Bridge:	Model:	MAC:	Firmware:
GS2220	1	GS2220-28HP	00-19-CB-00-00-01	V5.00(ABRR.0)20241001 10/01/2024
Location:	Desc.:	IPv4:		
--	--	172.21.56.39		
System Name:	Port Bridge:	Model:	MAC:	Firmware:
22A4_131	24	XGS3700-48HP	E4-18-68-F8-20-EB	V4.30(AAGF.2)_2023021 4 02/14/2023
Location:	Desc.:	IPv4:		
HQ2_R202	--	0.0.0.0		

Port 2

Port 3

Port 4

Port 5

Port 6

Port 7

The following table describes the fields in the above screen.

Table 23 MONITOR > Neighbor > Neighbor Details

LABEL	DESCRIPTION
Search Ports...	Enter the port number to search and display the ports you specified. The result will display in the below list. You can enter multiple ports separated by 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.
Port	This shows the port of the Switch, on which the neighboring device is discovered.
Desc.	This shows the port description of the Switch.
Link Speed	This shows the speed (1G for 1 Gbps, 10G for 10 Gbps, 25G for 25 Gbps, or 100G for 100 Gbps) and the duplex (F for full duplex or H for half). This field displays Down if the port is not connected to any device.
Remote	
System Name	This shows the system name of the neighbor device.
Port Bridge	This shows the neighboring device's MAC address or the port number connected to the Switch.
Model	This shows the model name of the neighbor device. This field will show "--" for devices that do not support the ZON utility.
MAC	This shows the MAC address of the neighbor device.
Firmware	This shows the firmware version of the neighbor device. This field will show "--" for devices that do not support the ZON utility.

Table 23 MONITOR > Neighbor > Neighbor Details (continued)

LABEL	DESCRIPTION
Location	This shows the geographic location of the neighbor device. This field will show “–” for devices that do not support the ZON utility.
Desc.	This shows the description of the neighbor device's port which is connected to the Switch.
IPv4	This shows the IPv4 address of the neighbor device. The IPv4 address is a hyper link that you can click to log into and manage the neighbor device through its Web Configurator.
Flush	Click the Flush button on the port tab to remove information about neighbors learned on a specific ports.
Flush All	Click the Flush All button to remove information about neighbors learned on all ports.

CHAPTER 12

Port Status

This chapter introduces the **Port Status** screens.

12.0.1 What You Can Do

Use the **Port Status** screen ([Section 12.1 on page 116](#)) to view the port status of the Switch.

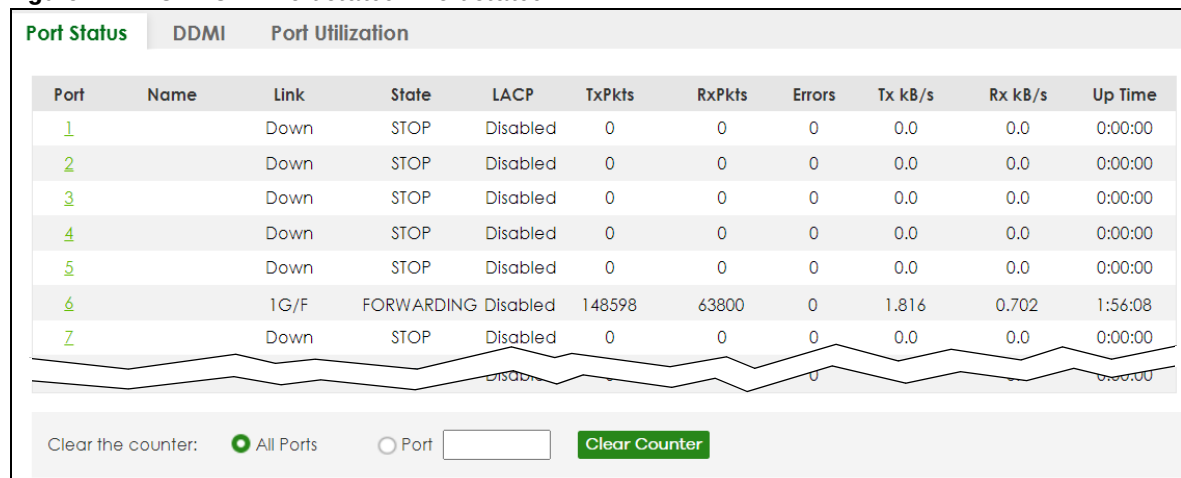
Use the **DDMI** screen ([Section 12.2 on page 119](#)) to view the DDMI (Digital Diagnostics Monitoring Interface) status of the SFP transceivers on the Switch.

Use the **Port Utilization** screen ([Section 12.3 on page 121](#)) to view the current data rate and utilization percentage of each port on the Switch.

12.1 Port Status

This screen displays a port statistical summary with links to each port showing statistical details. To view the port statistics, click **MONITOR > Port Status > Port Status** to display the **Port Status** screen as shown next. You can also click the **Port Status** link in the **Quick Link** section of the **DASHBOARD** screen to see the following screen.

Figure 72 MONITOR > Port Status > Port Status



The following table describes the labels in this screen.

Table 24 MONITOR > Port Status > Port Status

LABEL	DESCRIPTION
Port	This identifies the Ethernet port. Click a port number to display the Port Details screen.
Name	This is the name you assigned to this port in the PORT > Port Setup screen.
Link	This field displays the speed (1G for 1 Gbps, 10G for 10 Gbps, 25G for 25 Gbps, or 100G for 100 Gbps) and the duplex (F for full duplex). This field displays Down if the port is not connected to any device.
State	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port. If STP is disabled, this field displays FORWARDING if the link is up, otherwise, it displays STOP . When LACP (Link Aggregation Control Protocol) and STP are in blocking state, it displays BLOCKING .
LACP	This fields displays whether LACP (Link Aggregation Control Protocol) has been enabled on the port.
TxPkts	This field shows the number of transmitted frames on this port.
RxPkts	This field shows the number of received frames on this port.
Errors	This field shows the number of received errors on this port.
Tx kB/s	This field shows the number of kilobytes per second transmitted on this port.
Rx kB/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time in hours, minutes and seconds the port has been up.
Clear the counter	Select Port , enter a port number and then click Clear Counter to erase the recorded statistical information for that port, or select ALL Ports to clear statistics for all ports.

12.1.1 Port Details

Click an index in the **Port** column in the **MONITOR > Port Status > 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 73 MONITOR > Port Status > Port Status > Port Details

Port Status

DDMI

Port Utilization

Port Status > Port Details

Port Info

Port NO.

3

Name

Link

25G/F

FEC

CL91

State

FORWARDING

LACP

Disabled

TxPkts

142988

RxPkts

142988

Errors

0

Tx kB/s

5.456

Tx Utilization%

0.0

Rx kB/s

5.456

Rx Utilization%

0.0

Up Time

0:28:45

TX Packet

Unicast

1248

Multicast

75

Broadcast

141665

Pause

0

RX Packet

Unicast

1248

Multicast

75

Broadcast

141665

Pause

0

TX Collision

Single

0

Multiple

0

Excessive

0

Late

0

Error Packet

RX CRC

0

Length

0

Runt

0

Distribution

64

203794

65 to 127

84

128 to 255

82

256 to 511

360

512 to 1023

34

1024 to 1518

1422

Giant

0

The following table describes the labels in this screen.

Table 25 MONITOR > Port Status > Port Status > Port Details

LABEL	DESCRIPTION
Port Info	
Port NO.	This field displays the port number you are viewing.
Name	This field displays the name of the port.
Link	This field displays the speed (1G for 1 Gbps, 10G for 10 Gbps, 25G for 25 Gbps, or 100G for 100 Gbps) and the duplex (F for full duplex). This field displays Down if the port is not connected to any device.
FEC	This field displays the FEC (Forward Error Correction) negotiation result between the port and the connected device such as the following: • CL74 indicates that both connected ports negotiate through FEC clause 74. • CL91 indicates that both connected ports negotiate through FEC clause 91. • CL108 indicates that both connected ports negotiate through FEC clause 108. • N/A when FEC is not required for both connected ports. See Section 29.2.1 on page 204 for more information on the Clause types.
State	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port. If STP is disabled, this field displays FORWARDING if the link is up, otherwise, it displays STOP. When LACP (Link Aggregation Control Protocol), STP, and dot1x are in blocking state, it displays BLOCKING.
LACP	This field shows if LACP is enabled on this port or not.
TxPkts	This field shows the number of transmitted frames on this port.
RxPkts	This field shows the number of received frames on this port.
Errors	This field shows the number of received errors on this port.
Tx kB/s	This field shows the number of kilobytes per second transmitted on this port.
Tx Utilization%	This field shows the percentage of actual transmitted frames on this port as a percentage of the Link speed.
Rx kB/s	This field shows the number of kilobytes per second received on this port.
Rx Utilization%	This field shows the percentage of actual received frames on this port as a percentage of the Link speed.
Up Time	This field shows the total amount of time the connection has been up.
TX Packet	
The following fields display detailed information about packets transmitted.	
Unicast	This field shows the number of good unicast packets transmitted.
Multicast	This field shows the number of good Multicast packets transmitted.
Broadcast	This field shows the number of good broadcast packets transmitted.
Pause	This field shows the number of 802.3x pause packets transmitted.
RX Packet	
The following fields display detailed information about packets received.	
Unicast	This field shows the number of good unicast packets received.
Multicast	This field shows the number of good Multicast packets received.
Broadcast	This field shows the number of good broadcast packets received.
Pause	This field shows the number of 802.3x pause packets received.
TX Collision	
The following fields display information on collisions while transmitting.	

Table 25 MONITOR > Port Status > Port Status > Port Details (continued)

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

12.2 DDMI

The optical SFP transceiver's support for the Digital Diagnostics Monitoring Interface (DDMI) function lets you monitor the transceiver's parameters to perform component monitoring, fault isolation and failure prediction tasks. This allows proactive, preventative network maintenance to help ensure service continuity.

Use this screen to view the DDMI status of the Switch's SFP transceivers. Click **MONITOR > Port Status > DDMI** to see the following screen. Alternatively, click **DASHBOARD** from any Web Configurator screen and then the **Port Status** link in the **Quick Link** section of the **DASHBOARD** screen to display the **Port Status** screen and then click the **DDMI** link tab.

Figure 74 MONITOR > Port Status > DDMI

Port Status	DDMI	Port Utilization				
Port	Vendor	Part Number	Serial Number	Revision	Date Code	Transceiver
1	ZYXEL	SFP10G-T	S223Q39500057	J1.0	2022-11-06	Others

The following table describes the labels in this screen.

Table 26 MONITOR > Port Status > DDMI

LABEL	DESCRIPTION
Port	This identifies the SFP port. Click a port number to display the DDMI Details screen.
Vendor	This displays the vendor name of the optical transceiver.
Part Number	This displays the part number of the optical transceiver.
Serial Number	This displays the serial number of the optical transceiver.
Revision	This displays the revision number of the optical transceiver.
Date Code	This displays the date when the optical transceiver was manufactured.
Transceiver	This displays the type of optical transceiver installed in the SFP slot.

12.2.1 DDMI Details

Use this screen to view the real-time SFP (Small Form Factor Pluggable) transceiver information and operating parameters on the SFP port. The parameters include, for example, transmitting and receiving power, and module temperature.

Click an index in the **Port** column in the **DDMI** screen to view current transceivers' status.

Figure 75 MONITOR > Port Status > DDMI > DDMI Details

Port Status

DDMI

Port Utilization

DDMI > DDMI Details

Transceiver Information

Port No	1
Connector Type	SFP
Vendor	ZYXEL
Part Number	SFP10G-T
Serial Number	S223Q39500057
Revision	J1.0
Date Code	2022-11-06
Transceiver	Others
Calibration	Internal

DDMI Information

Type	Current	High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold
Temperature(C)	38.72	80.00	75.00	-5.00	-10.00
Voltage(V)	3.28	3.60	3.50	3.00	2.90
TX Bias(mA)	-- 6.00	131.07	131.07	131.07	131.07
TX Power(dbm)	-- -3.01	8.16	8.16	8.16	8.16
RX Power(dbm)	-- -3.98	8.16	8.16	8.16	8.16

The following table describes the labels in this screen.

Table 27 MONITOR > Port Status > DDMI > DDMI Details

LABEL	DESCRIPTION
Transceiver Information	
Port No	This identifies the SFP port.
Connector Type	This displays the connector type of the optical transceiver.
Vendor	This displays the vendor name of the optical transceiver.
Part Number	This displays the part number of the optical transceiver.
Serial Number	This displays the serial number of the optical transceiver.
Revision	This displays the revision number of the optical transceiver.
Date Code	This displays the date when the optical transceiver was manufactured.
Transceiver	This displays details about the type of transceiver installed in the SFP slot.
Calibration	This field is available only when an SFP transceiver is inserted into the SFP slot. Internal displays if the measurement values are calibrated by the transceiver. External displays if the measurement values are raw data which the Switch calibrates.
DDMI Information	
Type	This displays the DDMI parameter.
Temperature (C)	This displays the temperature inside the SFP transceiver in degrees Celsius.
Voltage (V)	This displays the level of voltage being supplied to the SFP transceiver.
TX Bias (mA)	This displays the milliamps (mA) being supplied to the SFP transceiver's Laser Diode Transmitter.
TX Power (dbm)	This displays the amount of power the SFP transceiver is transmitting.
RX Power (dbm)	This displays the amount of power the SFP transceiver is receiving from the fiber cable.
Current	This displays the current status for each monitored DDMI parameter.
High Alarm Threshold	This displays the high value alarm threshold for each monitored DDMI parameter. An alarm signal is reported to the Switch if the monitored DDMI parameter reaches this value.
High Warn Threshold	This displays the high value warning threshold for each monitored DDMI parameter. A warning signal is reported to the Switch if the monitored DDMI parameter reaches this value.
Low Warn Threshold	This displays the low value warning threshold for each monitored DDMI parameter. A warning signal is reported to the Switch if the monitored DDMI parameter reaches this value.
Low Alarm Threshold	This displays the low value alarm threshold for each monitored DDMI parameter. An alarm signal is reported to the Switch if the monitored DDMI parameter reaches this value.

12.3 Port Utilization

This screen displays the percentage of actual transmitted or received frames on a port as a percentage of the **Link** speed. To view port utilization, click **MONITOR > Port Status > Port Utilization** to see the following screen. Alternatively, click **DASHBOARD** from any Web Configurator screen and then the **Port Status** link in the **Quick Link** section of the **DASHBOARD** screen to display the **Port Status** screen and then click the **Port Utilization** link tab.

Figure 76 MONITOR > Port Status > Port Utilization

Port Status	DDMI	Port Utilization			
Port	Link	Tx kB/s	Tx utilization%	Rx kB/s	Rx utilization%
1	Down	0.0	0.0	0.0	0.0
2	Down	0.0	0.0	0.0	0.0
3	Down	0.0	0.0	0.0	0.0
4	1G/F	0.824	0.0	0.347	0.0
5	Down	0.0	0.0	0.0	0.0
6	Down	0.0	0.0	0.0	0.0
7	Down	0.0	0.0	0.0	0.0

The following table describes the labels in this screen.

Table 28 MONITOR > Port Status > Port Utilization

LABEL	DESCRIPTION
Port	This identifies the Ethernet port.
Link	This field displays the speed (1G for 1 Gbps, 10G for 10 Gbps, 25G for 25 Gbps, or 100G for 100 Gbps) and the duplex (F for full duplex or H for half). It also shows the cable type (Copper or Fiber) for the combo ports. This field displays Down if the port is not connected to any device.
Tx kB/s	This field shows the transmission speed of data sent on this port in kilobytes per second.
Tx Utilization%	This field shows the percentage of actual transmitted frames on this port as a percentage of the Link speed.
Rx kB/s	This field shows the transmission speed of data received on this port in kilobytes per second.
Rx Utilization%	This field shows the percentage of actual received frames on this port as a percentage of the Link speed.

CHAPTER 13

Routing Table

13.1 Routing Table Overview

This chapter introduces the IPv4 routing tables.

The IPv4 routing tables record routing information of the best path to destinations where packets were forwarded. Use this table to check information like routing destination, gateway, interface IP addresses, hop count, and routing methods.

13.1.1 What You Can Do

Use the **IPv4 Routing Table** screen ([Section 13.2 on page 123](#)) to view the Switch's IPv4 routing table information.

13.2 IPv4 Routing Table

Use this screen to view IPv4 routing table information. Click **MONITOR > Routing Table > IPv4 Routing Table** in the navigation panel to display the screen as shown.

Figure 77 MONITOR > Routing Table > IPv4 Routing Table

IPv4 Routing Table						
Index	Destination	Gateway	Interface	Metric	Type	Uptime
1	192.168.2.0/24	192.168.2.116	192.168.2.116	1	LOCAL	1:40:28
2	127.0.0.0/16	127.0.0.1	127.0.0.1	1	LOCAL	1:40:53
3	default	192.168.2.1	192.168.2.116	2	STATIC	1:40:28

The following table describes the labels in this screen.

Table 29 MONITOR > Routing Table > IPv4 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 IPv4 Interface.
Metric	This field displays the cost of the route.

Table 29 MONITOR > Routing Table > IPv4 Routing Table (continued)

LABEL	DESCRIPTION
Type	This field displays the method used to learn the route. STATIC – added as a static entry. LOCAL – added as a local interface entry.
Uptime	This field displays how long the route has been running since the Switch learned the route and added an entry in the routing table.

CHAPTER 14

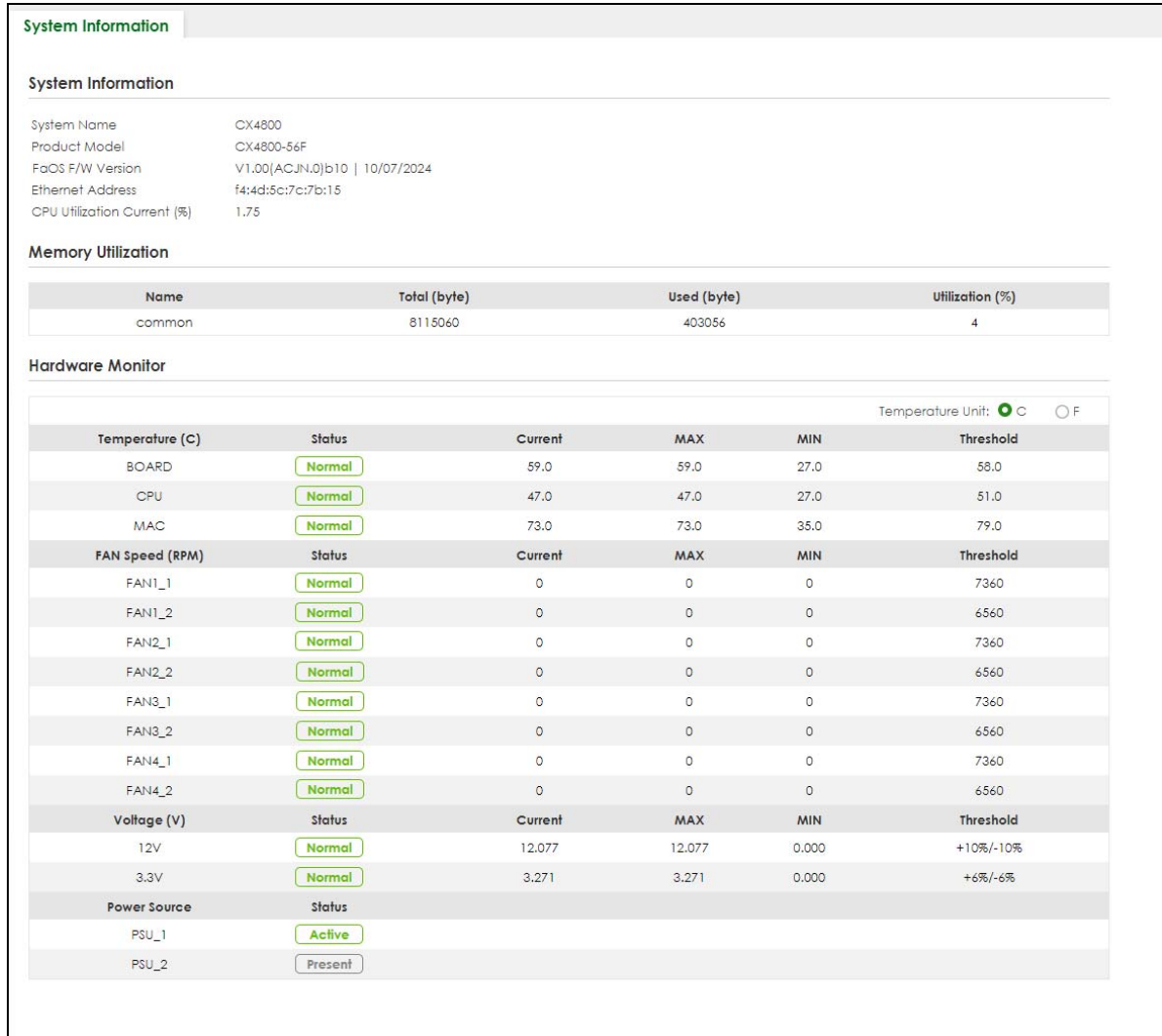
System Information

14.0.1 What You Can Do

Use the **System Information** screen ([Section 14.1 on page 125](#)) to view general system information and hardware status of the Switch.

14.1 System Information

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

Figure 78 MONITOR > System Information

The following table describes the labels in this screen.

Table 30 MONITOR > System Information > System Information

LABEL	DESCRIPTION
System Information	
System Name	This displays the descriptive name of the Switch for identification purposes.
Product Model	This displays the product model of the Switch. Use this information when searching for firmware upgrade or looking for other support information in the website.
FaOS F/W Version	This displays the version number of the Switch 's current firmware including the date created.
Ethernet Address	This refers to the Ethernet MAC (Media Access Control) address of the Switch.
CPU Utilization Current (%)	This displays the current percentage of CPU utilization.

Table 30 MONITOR > System Information > System Information (continued)

LABEL	DESCRIPTION
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 displays the name of the memory pool.
Total (byte)	This displays the total number of bytes in this memory pool.
Used (byte)	This displays the number of bytes being used in this memory pool.
Utilization (%)	This displays the percentage (%) of memory being used in this memory pool.
Hardware Monitor	
Temperature Unit	The Switch has temperature sensors that are capable of detecting and reporting if the temperature rises above the threshold. You may choose the temperature unit (Centigrade or Fahrenheit) in this field.
Temperature (C/F)	BOARD / CPU / MAC refers to the location of the temperature sensor on the Switch printed circuit board.
Status	This field displays Normal for temperatures below the threshold and Error for those above.
Current	This shows the current temperature at this sensor.
MAX	This field displays the maximum temperature measured at this sensor.
MIN	This field displays the minimum temperature measured at this sensor.
Threshold	This field displays the upper temperature limit at this sensor.
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. See Section 3.3 on page 40 for the location of the fans.
Status	Normal indicates that this fan is functioning above the minimum speed. Error indicates that this fan is functioning below the minimum speed.
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.
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.
Status	Normal indicates that the voltage is within an acceptable operating range at this point; otherwise Error is displayed.
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.

Table 30 MONITOR > System Information > System Information (continued)

LABEL	DESCRIPTION
Power Source	This field lists the power supply modules installed in the Switch. PSU_1 is PWR1 , and PSU_2 is PWR2 . See Section 3.3 on page 40 for the location of the power supply modules.
Status	Active indicates the Switch is currently operating from the power source to which the power module is connected. Present is displayed when the power module is connected to the Switch, but is not connected to a power source and there is no available power. Absent is displayed when there is no power module connected to the Switch. Error indicates that this power module is functioning below the power requirement. Or, the fan in this power module is not working.

CHAPTER 15

System Log

15.1 System Log Overview

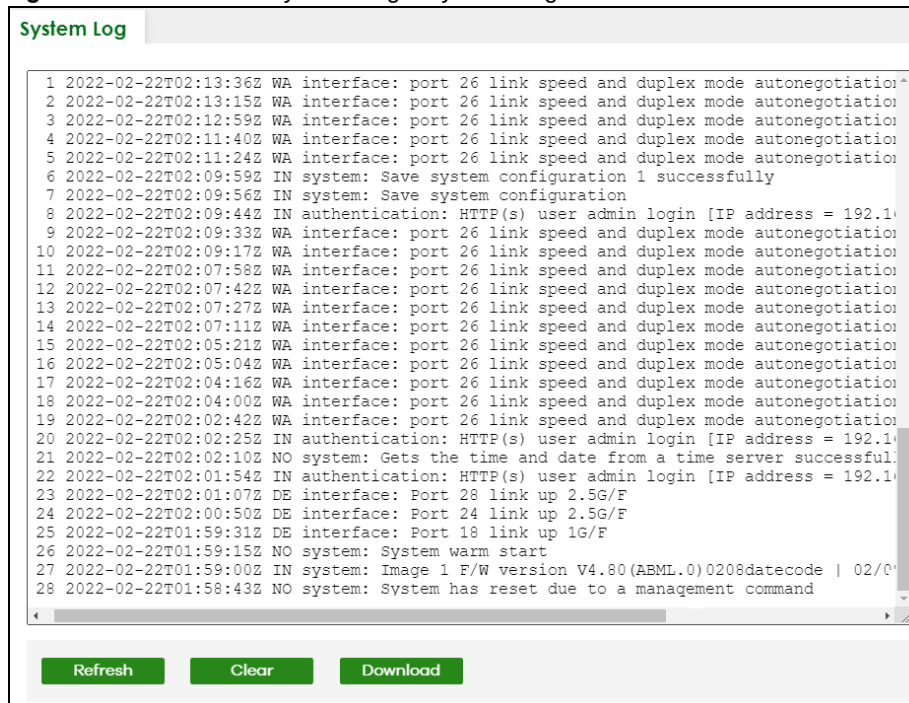
A log message stores the system history information for viewing.

15.2 System Log

Click **MONITOR > System Log > System Log** in the navigation panel to open this screen. Use this screen to check current system logs.

Note: When a log reaches the maximum number of log messages, new log messages automatically overwrite existing log messages, starting with the oldest existing log message first.

Figure 79 MONITOR > System Log > System Log



The summary table shows the time the log message was recorded and the reason the log message was generated. Click **Refresh** to update this screen. Click **Clear** to clear the whole log, regardless of what is currently displayed on the screen. Click **Download** to save the log to your computer.

CHAPTER 16

SYSTEM

The following chapters introduces the configurations of the links under the **SYSTEM** navigation panel.

Quick links to chapters:

- [Cloud Management](#)
- [General Setup](#)
- [Hardware Monitor Setup](#)
- [IP Setup](#)
- [Logins](#)
- [SNMP](#)
- [Switch Setup](#)
- [Syslog Setup](#)
- [Time Range](#)

CHAPTER 17

Cloud Management

17.1 Cloud Management Overview

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

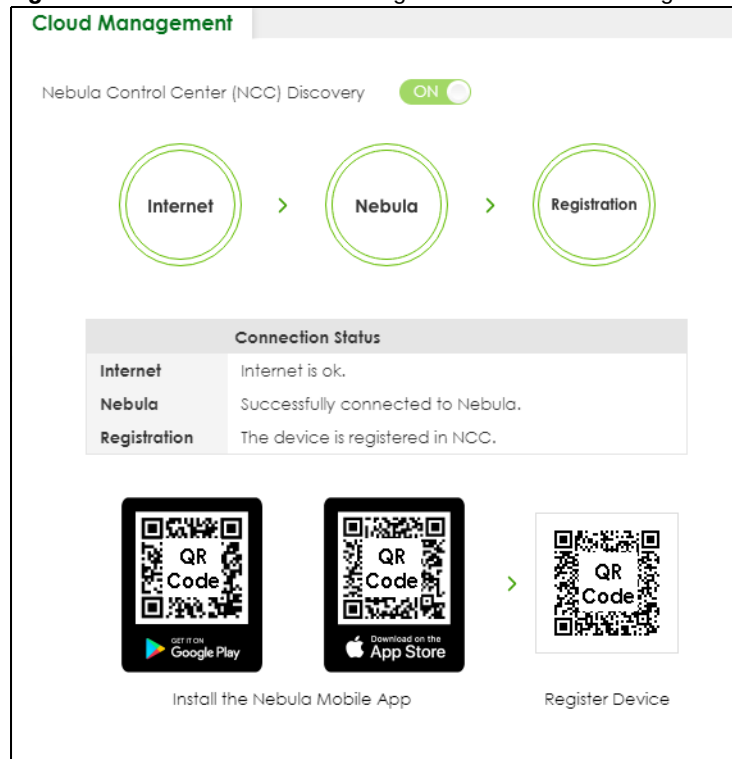
The Switch is managed and provisioned automatically by the NCC (Nebula Control Center) when:

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

17.2 Nebula Center Control Discovery

Click **SYSTEM > Cloud Management > Cloud Management** to display this screen.

Figure 80 SYSTEM > Cloud Management > Cloud Management



The following table describes the labels in this screen.

Table 31 SYSTEM > Cloud Management > Cloud Management

LABEL	DESCRIPTION
Nebula Control Center (NCC) Discovery	Enable the switch button to turn on Nebula Control Center (NCC) discovery on the Switch. This field displays: • The Switch Internet connection status. • The connection status between the Switch and NCC. • The Switch registration status on NCC. To pass your Switch management to NCC, first make sure your Switch is connected to the Internet. Then go to NCC and register your Switch. 1. Internet Green – The Switch is connected to the Internet. Orange – The Switch is not connected to the Internet. 2. Nebula Green – The Switch is connected to NCC. Orange – The Switch is not connected to NCC. 3. Registration Green – The Switch is registered on NCC. Gray – The Switch is not registered on NCC. Note: All circles will gray out if you disable Nebula Discovery.
Connection Status	This table displays the NCC connection status information. Use status logs in the Internet, Nebula, and Registration fields for connection troubleshooting.

Cloud Management Mode

Enable the switch button to turn on NCC discovery on the Switch. If the Switch has Internet access and has been registered on the NCC, it will automatically go into cloud management mode. Follow the steps to register your Switch on NCC:

1 Download the Nebula Mobile App

First, download the app from the Google Play store for Android devices or the App Store for iOS devices and create an organization and site.

You can scan an app store QR code to open the app installation page on the app store.

2 Scan the Device QR code

The **Register Device** QR code in this screen contains the Switch's serial number and the registration MAC address for handy NCC registration of the Switch using the Nebula Mobile app.

Follow the wizard in the Nebula Mobile app to scan the QR code to register the Switch on NCC and add the Switch into a site.

If **Nebula Control Center (NCC) Discovery** is disabled, the Switch will NOT discover the NCC and remain in Standalone mode.

CHAPTER 18

General Setup

18.1 General Setup

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

Figure 81 SYSTEM > General Setup

General Setup

System Name: CX4800

Location:

Contact Person's Name:

Use Time Server when Bootup: NTP(RFC-1305) ▼

Time Server 1: 0.pool.ntp.org

Time Server 2: 1.pool.ntp.org

Time Server 3: time.google.com

Time Server Sync Interval: 1440 minutes

Current Time: 14 : 32 : 40 UTC+00:00

New Time (hh:mm:ss): 14 : 32 : 40

Current Date: 2024 - 11 - 21

New Date (yyyy-mm-dd): 2024 - 11 - 21

Time Zone: UTC ▼

Daylight Saving Time: ☐ OFF

Start Date: First ▼ Sunday ▼ of January ▼ at 0:00 ▼

End Date: First ▼ Sunday ▼ of January ▼ at 0:00 ▼

Apply **Cancel**

Note: The input string of any field in this screen should not contain [?], [|], ['], ["], or [,].

The following table describes the labels in this screen.

Table 32 SYSTEM > General Setup > General Setup

LABEL	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. This name consists of up to 64 printable ASCII characters; spaces are allowed.
Location	Enter the geographic location of your Switch. You can use up to 128 printable ASCII characters; spaces are allowed.
Contact Person's Name	Enter the name of the person in charge of this Switch. You can use up to 32 printable ASCII characters; spaces are allowed.

Table 32 SYSTEM > General Setup > General Setup (continued)

LABEL	DESCRIPTION
Use Time Server when Bootup	Enter the time service protocol that your time server uses. Not all time servers support all protocols, so you may have to use trial and error to find a protocol that works. The main differences between them are the time format. When you select the Daytime (RFC-867) format, the Switch displays the day, month, year and time with no time zone adjustment. When you use this format it is recommended that you use a Daytime timeserver within your geographical time zone. Time (RFC-868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 00:00:00. 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 2022-01-01 00:00:00.
Time Server 1/2/3	Enter the IPv4 / IPv6 address or domain name of your time server. The Switch searches for the first, then the second, then the third time server for around 60 seconds.
Time Server Sync Interval	Enter the period in minutes between each time server synchronization. The Switch checks the time server after every synchronization interval.
Current Time	This field displays the time you open this menu (or refresh the menu).
New Time (hh:mm:ss)	Enter the new time in hour, minute and second format. The new time then appears in the Current Time field after you click Apply .
Current Date	This field displays the date you open this menu.
New Date (yyyy-mm-dd)	Enter the new date in year, month and day format. The new date then appears in the Current Date field after you click Apply .
Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone from the drop-down list box.
Daylight Saving Time	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Enable the switch button if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected Daylight Saving Time. The time is displayed in the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select Second, Sunday, March and 2:00. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, March and the last field depends on your time zone. In Germany for instance, you would select 2:00 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected Daylight Saving Time. The time field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select First, Sunday, November and 2:00. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, October and the last field depends on your time zone. In Germany for instance, you would select 2:00 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).

Table 32 SYSTEM > General Setup > 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.

18.2 Hardware Monitor Setup

This section introduces **Fan Control** for the temperature of the SFP transceiver inserted in the Switch.

When the SFP transceiver temperature exceeds the temperature threshold (see your transceiver documentation), the Switch automatically turns on the fans with maximum fan speed to cool down the system.

The fans do not automatically turn off after the SFP transceiver temperature returns below threshold. To turn off the fans, you have to temporarily disable **SFP Detect** or reboot the Switch.

Click **SYSTEM > Hardware Monitor Setup** to display the screen as shown below.

Note: The **SFP Detect** feature only functions if at least one of your SFP transceiver(s) support DDMI (Digital Diagnostic Monitoring Interface). See the transceiver documentation.

Figure 82 SYSTEM > Hardware Monitor Setup

The following table describes the labels in this screen.

Table 33 SYSTEM > Hardware Monitor Setup

LABEL	DESCRIPTION
Fan Control	
SFP Detect	Enable the switch button to enable SFP Detect 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.

You will see SFP warning icons next to the **FANs** in the **MONITOR > System Information** screen when **SFP Detect** has triggered the fans.

Figure 83 Hardware Monitor: SFP Module Temperature Warning

Hardware Monitor

Temperature Unit: ☒ C ☐ F

Temperature (C)	Status		Current	MAX	MIN	Threshold
BOARD	Normal		58.0	58.0	27.0	58.0
CPU	Normal		48.0	48.0	27.0	51.0
MAC	Normal		72.0	72.0	36.0	79.0
FAN Speed (RPM)	Status		Current	MAX	MIN	Threshold
FAN1_1	Normal	SFP	11139	22405	9637	7360
FAN1_2	Normal	SFP	9805	18950	10056	6560
FAN2_1	Normal	SFP	11045	22411	10082	7360
FAN2_2	Normal	SFP	11139	18950	9637	6560
FAN3_1	Normal		11014	22405	10056	7360
FAN3_2	Normal		9781	22533	8957	6560

CHAPTER 19

IP Setup

19.1 IP Setup Overview

This chapter shows you how to configure IP settings and set up IP interfaces on the Switch using the **IP Setup** screens.

19.1.1 What You Can Do

- Use the **IP Status** screen ([Section 19.2 on page 138](#)) to view the current IP interfaces and DNS server settings on the Switch.
- Use the **IP Setup** screen ([Section 19.3 on page 140](#)) to configure the default gateway device, the default domain name server and add IP domains.
- Use the **Network Proxy Configuration** screen ([Section 19.4 on page 143](#)) to configure network proxy configurations.

19.1.2 IP Interfaces

The Switch needs an IP address for it to be managed over the network. When the Switch fails to obtain an IP address from a DHCP server, the default static IP address 192.168.1.1 will be automatically added and used as the Switch's management IP address. 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 VLANs.

Note: You must configure a VLAN first before adding a management IP address. Each VLAN can have multiple management IP addresses, and you can log into the Switch through different management IP addresses simultaneously.

19.2 IP Status

Click **SYSTEM > IP Setup > IP Status** to display the screen as shown.

Figure 84 SYSTEM > IP Setup > IP Status

IP Status **IP Setup** **Network Proxy Configuration**

Domain Name Server

Domain Name Server	Source
172.21.10.1	DHCPv4

IP Interface

Index	IP Address	IP Subnet Mask	VID	Type	Action
1	192.168.2.115	255.255.255.0	100	Static	
2	172.21.40.22	255.255.252.0	1	DHCP	Renew Release

The following table describes the labels in this screen.

Table 34 SYSTEM > IP Setup > IP Status

LABEL	DESCRIPTION
Domain Name Server	
Domain Name Server	This field displays the IP address of the DNS server.
Source	This field displays whether the DNS server address is configured manually (Static) or obtained automatically using DHCPv4 .
IP Interface	
Index	This field displays the index number of an entry.
IP Address	This field displays the IP address of the Switch in the IP domain.
IP Subnet Mask	This field displays the subnet mask of the Switch in the IP domain.
VID	This field displays the VLAN identification number of the IP domain on the Switch.
Type	This shows whether this IP address is dynamically assigned from a DHCP server (DHCP) or manually assigned (Static).
Renew	Click this to renew the dynamic IP address.
Release	Click this to release the dynamic IP address.

19.2.1 IP Status Details

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

Figure 85 SYSTEM > IP Setup > IP Status > IP Status Details: Static

IP Status **IP Setup** **Network Proxy Configuration**

[IP Status](#) > IP Status Details

IP Status Details

Type	Static
VID	100
IP Address	192.168.2.115
IP Subnet Mask	255.255.255.0

The following table describes the labels in this screen.

Table 35 SYSTEM > IP Setup > IP Status > IP Status Details: Static

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

Figure 86 SYSTEM > IP Setup > IP Status > IP Status Details: DHCP

IP Status **IP Setup** **Network Proxy Configuration**

[IP Status](#) > IP Status Details

IP Status Details

Type	DHCP
VID	1
IP Address	192.168.1.100
IP Subnet Mask	255.255.255.0
Lease Time	172800 seconds
Renew Time	86400 seconds
Rebind Time	138240 seconds
Lease Time Start	2022-01-01 03:57:48
Lease Time End	2022-01-03 03:57:48
Default Gateway	192.168.1.250
Primary DNS Server	192.168.1.254
Secondary DNS Server	0.0.0.0

The following table describes the labels in this screen.

Table 36 SYSTEM > IP Setup > IP Status > IP Status Details: DHCP

LABEL	DESCRIPTION
Type	This shows the IP address is dynamically assigned from a DHCP server (DHCP).
VID	This is the VLAN identification number to which an IP routing domain belongs.
IP Address	This is the IP address of your Switch in dotted decimal notation for example 192.168.1.1.
IP Subnet Mask	This is the IP subnet mask of your Switch in dotted decimal notation for example 255.255.255.0.
Lease Time	This displays the length of time in seconds that this interface can use the current dynamic IP address from the DHCP server.

Table 36 SYSTEM > IP Setup > IP Status > IP Status Details: DHCP (continued)

LABEL	DESCRIPTION
Renew Time	This displays the length of time from the lease start that the Switch will request to renew its current dynamic IP address from the DHCP server.
Rebind Time	This displays the length of time from the lease start that the Switch will request to get any dynamic IP address from the DHCP server.
Lease Time Start	This displays the date and time that the current dynamic IP address assignment from the DHCP server began. You should configure date and time in SYSTEM > General Setup > General Setup .
Lease Time End	This displays the date and time that the current dynamic IP address assignment from the DHCP server will end. You should configure date and time in SYSTEM > General Setup > General Setup .
Default Gateway	This displays the IP address of the default gateway assigned by the DHCP server. 0.0.0.0 means no gateway is assigned.
Primary / Secondary DNS Server	This displays the IP address of the primary and secondary DNS servers assigned by the DHCP server. 0.0.0.0 means no DNS server is assigned.

19.3 IP Setup

Use this screen to configure the default gateway device, the default domain name server and add IP domains. Click **SYSTEM > IP Setup > IP Setup** in the navigation panel to display the screen as shown.

Note: The Switch allows you to set a static IP interface in the same subnet that already has a DHCP-assigned IP interface on the Switch. The Switch will use the static IP you set and the DHCP-assigned IP will be set to 0.0.0.0.

Figure 87 SYSTEM > IP Setup > IP Setup

IP Setup

Default Gateway: 0.0.0.0

Domain Name Server 1:

Domain Name Server 2:

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

Apply Cancel

Out-of-band Management IP Address

IP Address: 192.168.0.1

IP Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

Apply Cancel

IP Interface

	Index	IP Address	IP Subnet Mask	VID	Type
☐	1	192.168.2.115	255.255.255.0	100	Static
☐	2	172.21.40.22	255.255.252.0	1	DHCP

+ Add/Edit Delete

The following table describes the labels in this screen.

Table 37 SYSTEM > IP Setup > IP Setup

LABEL	DESCRIPTION
IP Setup	
Default Gateway	Type the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
Domain Name Server 1/2	Enter a domain name server IPv4 address in order to be able to use a domain name instead of an IP address.
Default Management	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 labeled MGMT . This means that devices connected to the other ports do not receive these packets. Select In-band to have the Switch send the packets to all ports except the management port (labeled MGMT) to which connected devices do not receive these packets.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Out-of-band Management IP Address	
Use these fields to set the settings for the out-of-band management port.	
IP Address	Enter the out-of-band management IP address of your Switch in dotted decimal notation. For example, 192.168.0.1.

Table 37 SYSTEM > IP Setup > IP Setup (continued)

LABEL	DESCRIPTION
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 this section to view and configure IP routing domains on the Switch.	
Index	This field displays the index number of an entry.
IP Address	This field displays the IP address of the Switch in the IP domain.
IP Subnet Mask	This field displays the subnet mask of the Switch in the IP domain.
VID	This field displays the VLAN identification number of the IP domain on the Switch.
Type	This field displays the type of IP address status. Static or DHCP .
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new IP interface or edit a selected one.
Delete	Click Delete to remove the selected IP interfaces.

19.3.1 Add/Edit IP Interfaces

Use this screen to add or edit IP interfaces. Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SYSTEM > IP Setup > IP Setup** screen to display this screen.

Figure 88 SYSTEM > IP Setup > IP Setup > Add/Edit

☒ DHCP Client
 Option-60 ☒
 Class-ID
☐ Static IP Address
 IP Address
 IP Subnet Mask
 VID

The following table describes the labels in this screen.

Table 38 SYSTEM > IP Setup > IP Setup > Add/Edit

LABEL	DESCRIPTION
DHCP Client	Select this option if you have a DHCP server that can assign the Switch an IP address, subnet mask, a default gateway IP address and a domain name server IP address automatically.
Option-60	DHCP Option 60 is used by the Switch for identification to the DHCP server using the VCI (Vendor Class Identifier) on the DHCP server. The Switch adds it in the initial DHCP discovery message that a DHCP client broadcasts in search of an IP address. The DHCP server can assign different IP addresses or options to clients with the specific VCI or reject the request from clients without the specific VCI. Select this and enter the device identity you want the Switch to add in the DHCP discovery frames that go to the DHCP server. This allows the Switch to identify itself to the DHCP server.
Class-ID	Enter a string of up to 32 printable ASCII characters to identify this Switch to the DHCP server. For example, Zyxel-TW. The string should not contain [?], [], ['], ["], or [,].
Static IP Address	Select this option if you do not have a DHCP server or if you wish to assign static IP address information to the Switch. You need to fill in the following fields when you select this option.
IP Address	Enter the IP address of your Switch in dotted decimal notation, for example, 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.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

19.4 Network Proxy Configuration

The proxy server of an organization may prohibit communication between the Switch and NCC (Nebula Control Center) (See [Section 17.1 on page 131](#)). Use this screen to enable communication between the Switch and NCC through the proxy server (P).

Figure 89 Network Proxy Configuration Application



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

Figure 90 SYSTEM > IP Setup > Network Proxy Configuration

The following table describes the labels in this screen.

Table 39 SYSTEM > IP Setup > Network Proxy Configuration

LABEL	DESCRIPTION
Active	Enable the switch button to enable communication between the Switch and NCC through a proxy server.
Server	Enter the IP address (dotted decimal notation) or host name of the proxy server. When entering the host name, up to 128 alphanumeric characters are allowed for the Server except [?], [], ['], or ["].
Port	Enter the port number of the proxy server (1 – 65535).
Authentication	Enable the switch button to enable proxy server authentication using a Username and Password .
Username	Enter a login user name from the proxy server administrator. Up to 32 alphanumeric characters are allowed for the Username . The string should not contain [?], [], ['], ["], [,], [:], or space.
Password	Enter a login password from the proxy server administrator. Up to 32 alphanumeric characters are allowed for the Password except [?], [], ['], and ["].
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save 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.

CHAPTER 20

Logins

20.1 Set Up Login Accounts

Up to five people (one administrator and four non-administrators) may access the Switch through Web Configurator at any one time.

- An administrator is someone who can both view and configure Switch changes. The default user name for the Administrator is **admin**. See the default administrator password on the back label of the Switch.
- A non-administrator (user name is something other than **admin**) is someone who can view and/or configure Switch settings. The configuration right varies depending on the user's privilege level.

Click **SYSTEM > Logins > Logins** to view the screen as shown.

Figure 91 SYSTEM > Logins > Logins

Logins

Administrator

User Name

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				

Apply

Cancel

The following table describes the labels in this screen.

Table 40 SYSTEM > Logins > Logins

LABEL	DESCRIPTION
Administrator This is the default administrator account with the “admin” user name. You can change the default administrator user name.	
User Name	Change the default “admin” system user name (up to 32 printable ASCII characters except [?], [], ['], ["], [space], [,], or [:]).
Old Password	Enter the existing system password (see the back label on the Switch for the default password).
Old Password	Enter the existing system password (the default password is on the label on the bottom of the Switch).
New Password	Enter your new system password. The password rules are: • 4 to 32 characters in length • [?], [], ['], ["], [,], [[], []] and space are not allowed
Retype to confirm	Retype your new system password for confirmation. You can enter up to 32 printable ASCII characters.
Edit Logins You may configure passwords for up to four users. These users can have read-only or read/write access. Note: You can give users higher privileges through the Web Configurator or the CLI. For more information on assigning privileges through the CLI see the Ethernet Switch CLI Reference Guide.	
Login	This is the index of an user account.
User Name	Specify the user name (up to 32 printable ASCII characters except [?], [], ['], ["], [space], [,], or [:]).
Password	Enter your new system password. The password rules are: • 4 to 32 characters in length • [?], [], ['], ["], [,], [[], []] and space are not allowed
Retype to confirm	Retype your new system password for confirmation.
Privilege	Type the privilege level for this user. At the time of writing, users may have a privilege level of 0, 3, 13, or 14 representing different configuration rights as shown below. • 0 – Display basic system information. • 3 – Display configuration or status. • 13 – Configure features except for login accounts, SNMP user accounts, the authentication method sequence and authorization settings, multiple logins, administrator and enable passwords, and configuration information display. • 14 – Configure login accounts, SNMP user accounts, the authentication method sequence and authorization settings, multiple logins, and administrator and enable passwords, and display configuration information. Users can run command lines if the session's privilege level is greater than or equal to the command's privilege level. The session privilege initially comes from the privilege of the login account. For example, if the user has a privilege of 5, he or she can run commands that requires privilege level of 5 or less but not more.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 21

SNMP

21.1 SNMP Overview

This chapter introduces the SNMP screens and shows you how to setup SNMP settings for management.

21.1.1 What You Can Do

- Use the **SNMP** screen ([Section 21.2 on page 147](#)) to configure general SNMP settings.
- Use the **SNMP User** screen ([Section 21.3 on page 149](#)) to create SNMP users for authentication with managers using SNMP v3 and associate them to SNMP groups.
- Use the **SNMP Trap Group** screen ([Section 21.4 on page 151](#)) to specify the types of SNMP traps that should be sent to each SNMP manager.
- Use the **SNMP Trap Port** screen ([Section 21.5 on page 152](#)) to enable/disable sending SNMP traps on a port.

21.2 Configure SNMP

Use this screen to configure your SNMP settings.

Click **SYSTEM > SNMP > SNMP** to view the screen as shown.

Figure 92 SYSTEM > SNMP > SNMP

The screenshot shows the 'SNMP' configuration page with tabs for 'SNMP User', 'SNMP Trap Group', and 'SNMP Trap Port'. The 'General Setting' section includes fields for Version (v2c), Get Community (public), Set Community (public), and Trap Community (public). The 'Trap Destination' section contains a table with 4 rows for configuring trap destinations.

Index	Version	IP	Port	Username
1	v2c	0.0.0.0	162	
2	v2c	0.0.0.0	162	
3	v2c	0.0.0.0	162	
4	v2c	0.0.0.0	162	

Buttons: Apply, Cancel

Note: The string of any field in this screen should not contain [?], [|], ['], ["], or [,].

The following table describes the labels in this screen.

Table 41 SYSTEM > SNMP > SNMP

LABEL	DESCRIPTION
General Setting	
Use this section to specify the SNMP version and community (password) values.	
Version	Select the SNMP version for the Switch. The SNMP version on the Switch must match the version on the SNMP manager. Choose SNMP version 2c (v2c), SNMP version 3 (v3) or both (v3v2c). SNMP version 2c is backwards compatible with SNMP version 1.
Get Community	Enter the Get Community string, which is the password for the incoming Get- and GetNext-requests from the management station. The Get Community string is only used by SNMP managers using SNMP version 2c or lower.
Set Community	Enter the Set Community string, which is the password for incoming Set- requests from the management station. The Set Community string is only used by SNMP managers using SNMP version 2c or lower.
Trap Community	Enter the Trap Community string, which is the password sent with each trap to the SNMP manager. The Trap Community string is only used by SNMP managers using SNMP version 2c or lower.
Trap Destination	
Use this section to configure where to send SNMP traps from the Switch.	
Index	This is the index of a trap destination.
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.

Table 41 SYSTEM > SNMP > SNMP (continued)

LABEL	DESCRIPTION
Port	Enter the port number upon which the manager listens for SNMP traps.
Username	Enter the user name to be sent to the SNMP manager along with the SNMP v3 trap. The string should not contain [?], [], ['], ["], [,], [:], or space. This user name must match an existing account on the Switch (configured in the SYSTEM > SNMP > SNMP User screen).
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

21.3 Configure SNMP User

Use this 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. Click **SYSTEM > SNMP > SNMP User** to view the screen as shown.

Figure 93 SYSTEM > SNMP > SNMP User

The following table describes the labels in this screen.

Table 42 SYSTEM > SNMP > SNMP User

LABEL	DESCRIPTION
Index	This is a read-only number identifying a login account on the Switch.
Username	This field displays the user name of a login account on the Switch.
Security Level	This field displays whether you want to implement authentication and/or encryption for SNMP communication with this user.
Authentication	This field displays the authentication algorithm used for SNMP communication with this user.
Privacy	This field displays the encryption method used for SNMP communication with this user.
Group	This field displays the SNMP group to which this user belongs.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new entry or edit a selected one.
Delete	Click Delete to remove the selected entries.

21.3.1 Add/Edit SNMP User

Use this 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. Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SYSTEM > SNMP > SNMP User** screen to view the screen.

Note: Use the user name and password of the login accounts you specify in this screen to create accounts on the SNMP v3 manager.

Figure 94 SYSTEM > SNMP > SNMP User > Add/Edit

The screenshot shows a web form for adding or editing an SNMP user. The fields are as follows:

- Username:** A text input field.
- Security Level:** A dropdown menu with 'no auth' selected.
- Authentication:** A dropdown menu with 'MD5' selected.
- Privacy:** A dropdown menu with 'DES' selected.
- Group:** A dropdown menu with 'admin' selected.
- Password:** Two text input fields for password entry.
- Buttons:** 'Apply' (green), 'Clear' (grey), and 'Cancel' (grey) buttons at the bottom right.

The following table describes the labels in this screen.

Table 43 SYSTEM > SNMP > SNMP User > Add/Edit

LABEL	DESCRIPTION
Username	Specify the user name (up to 32 printable ASCII characters) of a login account on the Switch. The string should not contain [?], [], ['], ["], [space], [,], or [:].
Security Level	Select whether you want to implement authentication and/or encryption for SNMP communication from this user. Choose: no auth – to use the user name 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 printable ASCII characters (except [?], [], ['], ["], [space], [,], [[], or []]) 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 printable ASCII characters (except [?], [], ['], ["], [space], [,], [[], or []]) for encrypting SNMP packets.

Table 43 SYSTEM > SNMP > SNMP User > Add/Edit (continued)

LABEL	DESCRIPTION
Group	SNMP v3 adopts the concept of View-based Access Control Model (VACM) group. SNMP managers in one group are assigned common access rights to MIBs. Specify in which SNMP group this user is. admin – Members of this group can perform all types of system configuration, including the management of administrator accounts. read-write – 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. read-only – Members of this group have read rights only, meaning the user can collect information from 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.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

21.4 SNMP Trap Group

Use this screen to specify the types of SNMP traps that should be sent to each SNMP manager. Click **SYSTEM > SNMP > SNMP Trap Group** to view the screen as shown.

Figure 95 SYSTEM > SNMP > SNMP Trap Group

SNMP SNMP User **SNMP Trap Group** SNMP Trap Port

Trap Destination IP

☐ **System**

☐ coldstart ☐ warmstart ☐ fanspeed
☐ temperature ☐ voltage ☐ reset
☐ timesync ☐ loopguard ☐ erdisable
☐ powersource ☐ loginrecord ☐ custom-ca

☐ **Interface**

☐ linkup ☐ linkdown ☐ autonegotiation
☐ lldp ☐ transceiver-ddm ☐ storm-control
☐ flex-link

☐ **AAA**

☐ authentication ☐ authorization ☐ accounting

☐ **IP**

☐ ping ☐ traceroute

☐ **Switch**

☐ stp ☐ mactable ☐ rmon
☐ classifier

The following table describes the labels in this screen.

Table 44 SYSTEM > SNMP > 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 SYSTEM > SNMP > SNMP screen. Use the rest of the screen to select which traps the Switch sends to that SNMP manager.
Options	Select the individual SNMP traps that the Switch is to send to the SNMP station. The traps are grouped by category. Selecting a category in the heading row automatically selects all of the SNMP traps under that category. Clear the checkboxes for individual traps that you do not want the Switch to send to the SNMP station. Clearing a category's checkbox automatically clears all of the category's trap checkboxes (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.

21.5 Enable or Disable Sending of SNMP Traps on a Port

Click **SYSTEM > SNMP > SNMP Trap Port** to view the screen as shown. Use this screen to set whether a trap received on the ports would be sent to the SNMP manager.

Figure 96 SYSTEM > SNMP > SNMP Trap Port

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

The following table describes the labels in this screen.

Table 45 SYSTEM > SNMP > SNMP Trap Port

LABEL	DESCRIPTION
Options	Select the trap type you want to configure here.
Port	This field displays a port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some of the settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to enable the trap type of SNMP traps on this port. The Switch sends the related traps received on this port to the SNMP manager. Clear this checkbox 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.

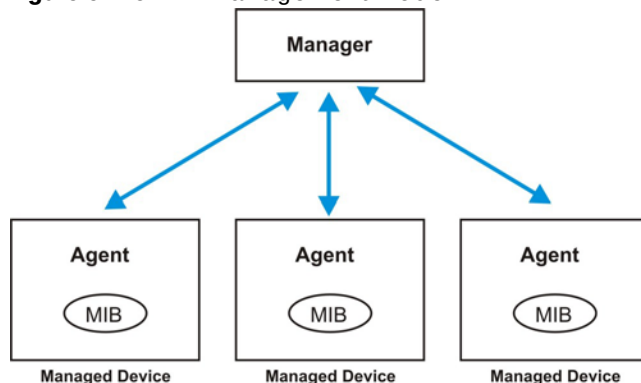
21.6 Technical Reference

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

21.6.1 About SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol used to manage and monitor TCP/IP-based devices. SNMP is used to exchange management information between the network management system (NMS) and a network element (NE). A manager station can manage and monitor the Switch through the network through 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 97 SNMP Management Model



An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed Switch (the Switch). An agent translates the local management information from the managed Switch into a form compatible with

SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables or managed objects that define each piece of information to be collected about a Switch. Examples of variables include number of packets received, node port status, and so on. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request or response protocol based on the manager or agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 46 SNMP Commands

LABEL	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

SNMP v3 and Security

SNMP v3 enhances security for SNMP management. SNMP managers can be required to authenticate with agents before conducting SNMP management sessions.

Security can be further enhanced by encrypting the SNMP messages sent from the managers. Encryption protects the contents of the SNMP messages. When the contents of the SNMP messages are encrypted, only the intended recipients can read them.

Supported MIBs

A MIB is a collection of managed objects that is organized according to hierarchy. The objects define the attributes of the managed device, which includes the names, status, access rights, and data types. Each object can be addressed through an object identifier (OID). An OID that begins with “1.3.6.1.4.1.890.1.15” is a Zyxel-defined private MIB. Otherwise, it is a standard MIB OID.

MIBs let administrators collect statistics and monitor status and performance. The Switch uses standard public (RFC-defined) MIBs for standard functionality, and private MIBs that support additional Switch functionality. Private MIBs contain Switch specific managed objects.

To view a list of standard MIBs supported by your Switch, see the product datasheet at www.zyxel.com (**Support > Download Library > Datasheet**).

To get the private MIBs supported by your Switch, download (and unzip) the correct model MIB from www.zyxel.com (**Support > Download Library > MIB File**).

SNMP Traps

The Switch sends traps to an SNMP manager when an event occurs. The following tables outline the SNMP traps by category.

Table 47 SNMP System Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
coldstart	coldStart	1.3.6.1.6.3.1.1.5.1	This trap is sent when the Switch is turned on.
warmstart	warmStart	1.3.6.1.6.3.1.1.5.2	This trap is sent when the Switch restarts.
fanspeed	zyHwMonitorFanSpeedOutOfRange	1.3.6.1.4.1.890.1.15.3.26.2.1	This trap is sent when the fan speed goes above or below the normal operating range.
	zyHwMonitorFANSpeedOutOfRangeRecovered	1.3.6.1.4.1.890.1.15.3.26.2.6	This trap is sent when the fan speed is recovered from the out of range to normal operating range.
temperature	zyHwMonitorTemperatureOutOfRange	1.3.6.1.4.1.890.1.15.3.26.2.2	This trap is sent when the temperature goes above or below the normal operating range.
	zyHwMonitorTemperatureOutOfRangeRecovered	1.3.6.1.4.1.890.1.15.3.26.2.7	This trap is sent when the temperature is recovered from the out of range to normal operating range.
voltage	zyHwMonitorPowerSupplyVoltageOutOfRange	1.3.6.1.4.1.890.1.15.3.26.2.3	This trap is sent when the voltage goes above or below the normal operating range.
reset	zySysMgmtUncontrolledSystemReset	1.3.6.1.4.1.890.1.15.3.49.2.1	This trap is sent when the Switch automatically resets.
	zySysMgmtControlledSystemReset	1.3.6.1.4.1.890.1.15.3.49.2.2	This trap is sent when the Switch resets by an administrator through a management interface.
	zySysMgmtBootImageInconsistence	1.3.6.1.4.1.890.1.15.3.49.2.3	This trap is sent when the index number of image which is loaded when the Switch starts up is different from what is specified through the CLI.
	RebootEvent	1.3.6.1.4.1.890.1.5.1.1.2	This trap is sent when the Switch reboots by an administrator through a management interface.
timesync	zyDateTimeTrapTimeServerNotReachable	1.3.6.1.4.1.890.1.15.3.82.3.1	This trap is sent when the Switch's date and time is not manually entered or the specified time server is not reachable.
	zyDateTimeTrapTimeServerNotReachableRecovered	1.3.6.1.4.1.890.1.15.3.82.3.2	This trap is sent when the Switch's real time clock is up to date.
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.
powersource	zyHwMonitorPowerSourceAbnormal	1.3.6.1.4.1.890.1.15.3.26.2.10	This trap is sent when the power source status has an abnormal change.
	zyHwMonitorPowerSourceAbnormalRecovered	1.3.6.1.4.1.890.1.15.3.26.2.11	This trap is sent when the power source status is changed to normal.

Table 47 SNMP System Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
	zyHwMonitorPowerSourceStatusChange	1.3.6.1.4.1.890.1.15.3.26.2.12	This trap is sent when the power source status is changed.
loginrecord	zyAccessControlLoginRecord	1.3.6.1.4.1.890.1.15.3.9.4.1	This trap is sent when users log in.
	zyAccessControlLogoutRecord	1.3.6.1.4.1.890.1.15.3.9.4.2	This trap is sent when users log out.
	zyAccessControlLoginFail	1.3.6.1.4.1.890.1.15.3.9.4.3	This trap is sent when users fail in login.
custom-ca	zySysMgmtReloadCustomCAFail	1.3.6.1.4.1.890.1.15.3.49.2.4	This trap is sent when the uploaded HTTPS certificate fails to load during the Switch restart.

Table 48 SNMP Interface Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
linkup	linkUp	1.3.6.1.6.3.1.1.5.4	This trap is sent when the Ethernet link is up.
linkdown	linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
autonegotiation	zyPortAutonegotiationFailed	1.3.6.1.4.1.890.1.15.3.61.3.1	This trap is sent when an Ethernet interface fails to auto-negotiate with the peer Ethernet interface.
	zyPortAutonegotiationFailedRecovered	1.3.6.1.4.1.890.1.15.3.61.3.3	This trap is sent when the Ethernet interface auto-negotiation link speed and duplex mode have recovered.
lldp	lldpRemTablesChange	1.0.8802.1.1.2.0.0.1	The trap is sent when entries in the remote database have any updates. Link Layer Discovery Protocol (LLDP), defined as IEEE 802.1ab, enables LAN devices that support LLDP to exchange their configured settings. This helps eliminate configuration mismatch issues.
transceiver-ddm	zyTransceiverDdmiTemperatureOutOfRange	1.3.6.1.4.1.890.1.15.3.84.3.1	This trap is sent when the transceiver temperature is above or below the normal operating range.
	zyTransceiverDdmiTxPowerOutOfRange	1.3.6.1.4.1.890.1.15.3.84.3.2	This trap is sent when the transmitted optical power is above or below the normal operating range.
	zyTransceiverDdmiRxPowerOutOfRange	1.3.6.1.4.1.890.1.15.3.84.3.3	This trap is sent when the received optical power is above or below the normal operating range.
	zyTransceiverDdmiVoltageOutOfRange	1.3.6.1.4.1.890.1.15.3.84.3.4	This trap is sent when the transceiver supply voltage is above or below the normal operating range.
	zyTransceiverDdmiTxBiasOutOfRange	1.3.6.1.4.1.890.1.15.3.84.3.5	This trap is sent when the transmitter laser bias current is above or below the normal operating range.
	zyTransceiverDdmiTemperatureOutOfRangeRecovered	1.3.6.1.4.1.890.1.15.3.84.3.6	This trap is sent when the transceiver temperature is recovered from the out of normal operating range.

Table 48 SNMP Interface Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
	zyTransceiverDdmiTxPowerOutOfRangeRecovered	1.3.6.1.4.1.890.1.15.3.84.3.7	This trap is sent when the transmitted optical power is recovered from the out of normal operating range.
	zyTransceiverDdmiRxPowerOutOfRangeRecovered	1.3.6.1.4.1.890.1.15.3.84.3.8	This trap is sent when the received optical power is recovered from the out of normal operating range.
	zyTransceiverDdmiVoltageOutOfRangeRecovered	1.3.6.1.4.1.890.1.15.3.84.3.9	This trap is sent when the transceiver supply voltage is recovered from the out of normal operating range.
	zyTransceiverDdmiTxBiasOutOfRangeRecovered	1.3.6.1.4.1.890.1.15.3.84.3.10	This trap is sent when the transmitter laser bias current is recovered from the out of normal operating range.
storm-control	zyPortStormControlTrap	1.3.6.1.4.1.890.1.15.3.78.2.1	This trap is sent when storm control is detected on a specific port. A packet filter action has been applied on the interface.
flex-link	zyFlexLinkPortStateChange	1.3.6.1.4.1.890.1.15.3.124.4.1	This trap is sent when the port state of a flex link pair changes.

Table 49 SNMP AAA Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
authentication	zyRadiusServerAuthenticationServerNotReachable	1.3.6.1.4.1.890.1.15.3.71.2.1	This trap is sent when there is no response message from the RADIUS authentication server.
	zyRadiusServerAuthenticationServerNotReachableRecovered	1.3.6.1.4.1.890.1.15.3.71.2.3	This trap is sent when there is a response message from the previously unreachable RADIUS authentication server.
	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.
	zyTacacsServerAuthenticationServerUnreachableRecovered	1.3.6.1.4.1.890.1.15.3.83.2.3	This trap is sent when there is a response message from the previously unreachable TACACS+ authentication server.
	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.
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.
	zyRadiusServerAccountingServerNotReachableRecovered	1.3.6.1.4.1.890.1.15.3.71.2.4	This trap is sent when there is a response message from the previously unreachable RADIUS accounting server.
	zyTacacsServerAccountingServerUnreachableRecovered	1.3.6.1.4.1.890.1.15.3.83.2.4	This trap is sent when there is a response message from the previously unreachable TACACS+ accounting server.

Table 50 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 51 SNMP Switch Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
stp	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.
	zyMrstpTopologyChange	1.3.6.1.4.1.890.1.15 .3.52.3.2	This trap is sent when the MRSTP topology changes.
	zyStpRootGuardDetect	1.3.6.1.4.1.890.1.15 .3.79.3.1	This trap is sent when the STP root switch detects superior BPDUs on a root guard enabled port and blocks the port.
	zyStpRootGuardRecovered	1.3.6.1.4.1.890.1.15 .3.79.3.2	This trap is sent when a port blocked by root guard stops sending superior BPDUs and is enabled again.
	zyMstpTopologyChange	1.3.6.1.4.1.890.1.15 .3.53.3.2	This trap is sent when the MSTP root switch changes.
mactable	zyMacForwardingTableFull	1.3.6.1.4.1.890.1.15 .3.48.2.1	This trap is sent when more than 99% of the MAC table is used.
	zyMacForwardingTableFullRecovered	1.3.6.1.4.1.890.1.15 .3.48.2.2	This trap is sent when the MAC address switching table has become normal from full.
rmon	RmonRisingAlarm	1.3.6.1.2.1.16.0.1	This trap is sent when a variable goes over the RMON "rising" threshold.
	RmonFallingAlarm	1.3.6.1.2.1.16.0.2	This trap is sent when the variable falls below the RMON "falling" threshold.
classifier	zyAcIV2ClassifierLogNotification	1.3.6.1.4.1.890.1.15 .3.105.4.1	This trap is sent when the Switch detects classifier log information.

CHAPTER 22

Switch Setup

22.1 Switch Setup Overview

Use this screen to do the Switch's basic setup configuration, for example, VLAN (Virtual Local Area Network) type, enabling switching protocols, and MAC learning aging time setup.

22.1.1 Introduction to VLANs

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

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

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

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

22.2 Switch Setup

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

Figure 98 SYSTEM > Switch Setup > Switch Setup

Switch Setup

VLAN Type ☒ 802.1Q ☐ Port Based

Bridge Control Protocol Transparency ☐ OFF

MAC Address Learning

Aging Time seconds

ARP Aging Time

Aging Time seconds

GARP Timer

Join Timer milliseconds

Leave Timer milliseconds

Leave All Timer milliseconds

Apply **Cancel**

The following table describes the labels in this screen.

Table 52 SYSTEM > Switch Setup > Switch Setup

LABEL	DESCRIPTION
VLAN Type	Choose 802.1Q or Port Based . The SWITCHING > VLAN link and its sub-links only appears when you choose 802.1Q VLAN type in this screen.
Bridge Control Protocol Transparency	Enable the ON/OFF switch 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 > Port Setup > Port Setup screen. Note: BPDU control is only available in Standalone mode.
MAC Address Learning	
MAC address learning reduces outgoing traffic broadcasts. For MAC address learning to occur on a port, the port must be active.	
Aging Time	Enter a time from 10 to 1000000 seconds. This is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be relearned).
ARP Aging Time	
Aging Time	Enter a time from 60 to 1000000 seconds. This is how long dynamically learned ARP entries remain in the ARP table before they age out (and must be relearned). The setting here applies to ARP entries which are newly added in the ARP table after you click Apply .
GARP Timer: Switches join VLANs by making a declaration. A declaration is made by issuing a Join message using GARP. Declarations are withdrawn by issuing a Leave message. A Leave All message terminates all registrations. GARP timers set declaration timeout values. See the chapter on VLAN setup for more background information.	
Join Timer	Join Timer sets the duration of the Join Period timer for GVRP in milliseconds. Each port has a Join Period timer. The allowed Join Time range is between 100 and 65535 milliseconds; the default is 200 milliseconds. See the chapter on VLAN setup for more background information.
Leave Timer	Leave Timer 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 52 SYSTEM > Switch Setup > 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 .
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 23

Syslog Setup

23.1 Syslog Overview

This chapter explains the **Syslog** screens.

The syslog protocol allows devices to send event notification messages across an IP network to syslog servers that collect the event messages. A syslog-enabled device can generate a syslog message and send it to a syslog server.

Syslog is defined in RFC 3164. The RFC defines the packet format, content and system log related information of syslog messages. Each syslog message has a facility and severity level. The syslog facility identifies a file in the syslog server. Refer to the documentation of your syslog program for details. The following table describes the syslog severity levels.

Table 53 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.

23.1.1 What You Can Do

Use the **Syslog Setup** screen ([Section 23.2 on page 162](#)) to configure the device's system logging settings and configure a list of external syslog servers.

23.2 Syslog Setup

The syslog feature sends logs to an external syslog server. Use this screen to configure the device's system logging settings and configure a list of external syslog servers.

Click **SYSTEM > Syslog Setup > Syslog Setup** in the navigation panel to display this screen.

Figure 99 SYSTEM > Syslog Setup > Syslog Setup

Syslog Setup

Active ☐ OFF

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**

Syslog Server Setup

+ Add/Edit **Delete**

☐	Index	Active	IP Address	UDP Port	Log Level

The following table describes the labels in this screen.

Table 54 SYSTEM > Syslog Setup > Syslog Setup

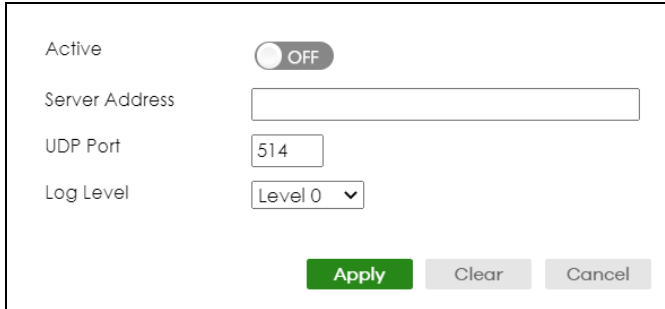
LABEL	DESCRIPTION
Syslog Setup	
Active	Enable the switch button to turn on syslog (system logging) and then configure the syslog setting.
Logging Type	This column displays the names of the categories of logs that the device can generate.
Active	Select this option to set the device to generate logs for the corresponding category.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Syslog Server Setup	
Index	This is the index number of a syslog server entry.
Active	This field displays if the device is activated to send logs to the syslog server.
IP Address	This field displays the IP address of the syslog server.
UDP Port	This field displays the port of the syslog server.
Log Level	This field displays the severity level of the logs that the device is to send to this syslog server.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new entry or edit a selected one.
Delete	Click Delete to remove the selected entries.

23.2.1 Add/Edit a Syslog Server

Use this screen to configure an external syslog server.

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SYSTEM > Syslog Setup > Syslog Setup** screen to display this screen.

Figure 100 SYSTEM > Syslog Setup > Syslog Setup > Add/Edit



The following table describes the labels in this screen.

Table 55 SYSTEM > Syslog Setup > Syslog Setup > Add/Edit

LABEL	DESCRIPTION
Active	Enable the switch button to have the device send logs to this syslog server. Clear the checkbox if you want to create a syslog server entry but not have the device send logs to it (you can edit the entry later).
Server Address	Enter the IPv4 address of the syslog server.
UDP Port	The default syslog server port is 514. If your syslog server uses a different port, configure the one it uses here.
Log Level	Select the severity levels of the logs that you want the device to send to this syslog server. The lower the number, the more critical the logs are.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

CHAPTER 24

Time Range

24.1 Time Range Overview

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 does not have an end time.

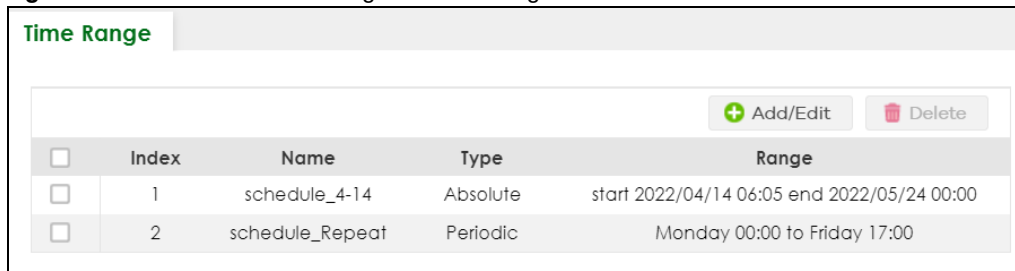
24.1.1 What You Can Do

Use the **Time Range** screen ([Section 24.2 on page 165](#)) to view or define a schedule on the Switch.

24.2 Configure a Time Range

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

Figure 101 SYSTEM > Time Range > Time Range



☐	Index	Name	Type	Range
☐	1	schedule_4-14	Absolute	start 2022/04/14 06:05 end 2022/05/24 00:00
☐	2	schedule_Repeat	Periodic	Monday 00:00 to Friday 17:00

The following table describes the labels in this screen.

Table 56 SYSTEM > Time Range > Time Range

LABEL	DESCRIPTION
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Index	This field displays the index number of the rule.
Name	This field displays the descriptive name for this rule. This is for identification purpose only. You can enter up to 32 printable ASCII characters except [?], [], ['], ["], or [,].

Table 56 SYSTEM > Time Range > Time Range (continued)

LABEL	DESCRIPTION
Type	This displays the schedule type of the time range rule. Absolute An one-time schedule. One-time schedules begin on a specific start date and time and end on a specific stop date and time. One-time schedules are useful for long holidays and vacation periods. Periodic A recurring schedule. Recurring schedules begin at a specific start time and end at a specific stop time on selected days of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday). Recurring schedules are useful for defining the workday and off-work hours.
Range	This field displays the time periods to which this schedule applies.
Add/Edit	Click Add/Edit to add a new schedule rule or edit a selected one.
Delete	Click Delete to remove the selected rules.

24.2.1 Add/Edit Time Range

This screen allows you to create a new time range or edit an existing one.

To access this screen, click the **Add/Edit** button or select an entry from the list and click the **Add/Edit** button.

Figure 102 SYSTEM > Time Range > Time Range > Add/Edit

Name

Type ☒ Absolute

Start 2022 02 23 00 : 00

End 2022 02 23 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

Apply Clear Cancel

The following table describes the labels in this screen.

Table 57 SYSTEM > Time Range > Time Range > Add/Edit

LABEL	DESCRIPTION
Name	Enter a descriptive name for this rule for identifying purposes. The string should not contain [?], [], ['], ["], or [,].
Type	Select Absolute to create a one-time schedule. One-time schedules begin on a specific start date and time and end on a specific stop date and time. One-time schedules are useful for long holidays and vacation periods. Alternatively, select Periodic to create a recurring schedule. Recurring schedules begin at a specific start time and end at a specific stop time on selected days of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday). Recurring schedules are useful for defining the workday and off-work hours.

Table 57 SYSTEM > Time Range > Time Range > Add/Edit (continued)

LABEL	DESCRIPTION
Absolute	This section is available only when you set Type to Absolute .
Start	Specify the year, month, day, hour and minute when the schedule begins.
End	Specify the year, month, day, hour and minute when the schedule ends.
Periodic	This section is available only when you set Type to Periodic. Select the first option if you want to define a recurring schedule for a consecutive time period. You then select the day of the week, hour and minute when the schedule begins and ends respectively. Select the second option if you want to define a recurring schedule for multiple non-consecutive time periods. You need to select each day of the week the recurring schedule is effective. You also need to specify the hour and minute when the schedule begins and ends each day. The schedule begins and ends in the same day.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

CHAPTER 25

PORT

The following chapters introduces the configurations of the links under the **PORT** navigation panel.

Quick links to chapters:

- [Flex Link](#)
- [Link Aggregation](#)
- [Link Layer Discovery Protocol \(LLDP\)](#)
- [Port Setup](#)

CHAPTER 26

Flex Link

This chapter introduces how to set up a backup link for a primary link using Flex Links.

26.1 Flex Link Overview

A flex link pair consists of a primary link and a backup link on a layer-2 interface. A primary link runs on a **Primary Port**; a backup link runs on a **Backup Port**. The ports have two states: FORWARDING and BLOCKING. When one link is up and running (port state: FORWARDING), the other link is in down or in standby mode (port state: BLOCKING). Only one port is forwarding traffic (FORWARDING) at a time.

When the primary link goes down, the backup link automatically goes up and is able to forward traffic.

Preemption

Enable **Preemption** to have the Switch automatically return the primary port to FORWARDING state after the connection from the primary port resumes, and the backup port return to BLOCKING. The Switch will wait for the specified **Preemption Delay Time** before changing the primary port state to FORWARDING and backup port state to BLOCKING. See [Table 60 on page 171](#) for more information.

26.1.1 What You Can Do

- Use the **Flex Link Status** screen ([Section 26.2 on page 169](#)) to view the flex link status on the Switch.
- Use the **Flex Link Setup** screen ([Section 26.3 on page 170](#)) to configure flex links for back up links on the Switch.

26.2 Flex Link Status

Click **PORT > Flex Link > Flex Link Status** to display this screen.

Figure 103 PORT > Flex Link > Flex Link Status

Flex Link Status		Flex Link Setup	
Index	Primary Port	Backup Port	State
1	1	2	Primary Down / Backup Down
2	24	26	Primary Down / Backup Up

The following table describes the labels in this screen.

Table 58 PORT > Flex Link > Flex Link Status

LABEL	DESCRIPTION
Index	This displays the index number of a flex link pair.
Primary Port	This displays the port number of the primary link.
Backup Port	This displays the port number of the backup link.
State	This displays the link status of the Primary port and Backup port. Down – The link is down. Up – The link is up and the port state is FORWARDING. Standby – The link is up and the port state is BLOCKING. Note: Only one port can be up in a flex link pair.

26.3 Flex Link Setup

Click **PORT > Flex Link > Flex Link Setup** to display this screen.

Note: The Flex Link (**PORT > Flex Link**), STP (**SWITCHING > Spanning Tree Protocol**), Loop Guard (**SWITCHING > Loop Guard**) and Link Aggregation (**PORT > Link Aggregation**) features cannot be configured together on the same port. When one of the above functions is enabled, the Switch will not let you enable the others.

Note: You can configure up to five pairs of flex links.

Figure 104 PORT > Flex Link > Flex Link Setup

Flex Link Status Flex Link Setup					
+ Add/Edit Delete					
☐	Index	Primary Port	Backup Port	Preemption	Preemption Delay Time
☐	1	1	2	Yes	30
☐	2	24	26	No	30

The following table describes the labels in this screen.

Table 59 PORT > Flex Link > Flex Link Setup

LABEL	DESCRIPTION
Index	This displays the index number of an entry.
Primary Port	This displays the port number of the primary link.
Backup Port	This displays the port number of the backup link.
Preemption	This displays if Preemption is enabled on the flex link pair. If Preemption is enabled, when the primary port comes back up, the backup port will go into BLOCKING state and the primary port will go into FORWARDING state after the Preemption Delay Time interval.
Preemption Delay Time	This displays the preemption delay time configured for this flex link pair.

Table 59 PORT > Flex Link > Flex Link Setup (continued)

LABEL	DESCRIPTION
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new entry or edit a selected one.
Delete	Click Delete to remove the selected entry.

26.3.1 Add/Edit Flex Link

To access this screen, click the **Add/Edit** button or select an entry from the list and click the **Add/Edit** button.

Note: A port can only be in one flex link pair. If a port has already been set as a flex link pair's primary/backup port, the port can not be used by other flex links. Check the **PORT > Flex Link > Flex Link Setup** screen to see what ports are already in other flex link pairs.

Figure 105 PORT > Flex Link > Flex Link Setup > Add/Edit

Primary Port

Backup Port

Preemption ☐

Preemption Delay Time

Apply Clear Cancel

The following table describes the labels in this screen.

Table 60 PORT > Flex Link > Flex Link Setup > Add/Edit

LABEL	DESCRIPTION
Primary Port	Enter a port number to be the primary port.
Backup Port	Enter a port number to be the backup port.
Preemption	Select this to enable the Preemption mode on the flex link pair. If Preemption is disabled, if the primary port is down, then comes back up, it will remain in the BLOCKING state even after the Preemption Delay Time .
Preemption Delay Time	Enter the delay time (in seconds) which you want the primary port to wait before changing back to FORWARDING state (when available). The range is 1 – 300 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.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

CHAPTER 27

Link Aggregation

27.1 Link Aggregation Overview

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

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

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

27.1.1 What You Can Do

- Use the **Link Aggregation Status** screen ([Section 27.2 on page 173](#)) to view ports you have configured to be in the trunk group, ports that are currently transmitting data as one logical link in the trunk group and so on.
- Use the **Link Aggregation Setting** screen ([Section 27.3 on page 175](#)) to configure static link aggregation.
- Use the **Link Aggregation Control Protocol** screen ([Section 27.4 on page 176](#)) to enable Link Aggregation Control Protocol (LACP).

27.1.2 What You Need to Know

The Switch supports both static and dynamic link aggregation.

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

See [Section 27.5.1 on page 178](#) for a static port trunking example.

Dynamic Link Aggregation

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

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

When you enable LACP link aggregation on a port, the port can automatically negotiate with the ports at the remote end of a link to establish trunk groups. LACP also allows port redundancy, that is, if an

operational port fails, then one of the “standby” ports become operational without user intervention. Please note that:

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

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

Link Aggregation ID

LACP aggregation ID consists of the following information¹:

Table 61 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 62 Link Aggregation ID: Peer Switch

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

Traffic Distribution Criteria

The Switch supports both unicast and non-unicast traffic (broadcast and multicast) network load sharing over link aggregation. Load sharing works by statically splitting the traffic based on source or destination IP/MAC address, and then distributing the load across multiple paths. In link aggregation, this allows the trunk group (ports) to transmit data as one logical link to a single or group of hosts on the network.

Unicast and non-unicast traffic network load sharing over link aggregation (trunking) is enabled by default.

27.2 Link Aggregation Status

Click **PORT > Link Aggregation > Link Aggregation Status** in the navigation panel to display the screen as shown. See [Section 27.1 on page 172](#) for more information.

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

Figure 106 PORT > Link Aggregation > Link Aggregation Status

Link Aggregation Status					
Link Aggregation Setting			Link Aggregation Control Protocol		
Group ID	Enabled Ports	Synchronized Ports	Aggregator ID	Criteria	Status
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	-
				src-dst-mac	-

The following table describes the labels in this screen.

Table 63 PORT > Link Aggregation > Link Aggregation Status

LABEL	DESCRIPTION
Group ID	This field displays the group ID to identify a trunk group, that is, one logical link containing multiple ports.
Enabled Ports	These are the ports you have configured in the Link Aggregation Setting screen to be in the trunk group. The port numbers displays only when this trunk group is activated and there is a port belonging to this group.
Synchronized Ports	These are the ports that are currently transmitting data as one logical link in this trunk group.
Aggregator ID	Link Aggregator ID consists of the following: system priority, MAC address, key, port priority and port number. The ID displays only when there is a port belonging to this trunk group and LACP is also enabled for this group.
Criteria	This shows the outgoing traffic distribution algorithm types used in this trunk group. Sending of packets are from the same source and/or to the same destination 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 through LACP.

27.3 Link Aggregation Setting

Click **PORT > Link Aggregation > Link Aggregation Setting** to display the screen shown next. See [Section 27.1 on page 172](#) for more information on link aggregation.

Figure 107 PORT > Link Aggregation > Link Aggregation Setting

Group ID	Active	Criteria
T1	☒	src-dst-mac ▼
T2	☐	src-dst-mac ▼
T3	☐	src-dst-mac ▼
T4	☐	src-dst-mac ▼
T5	☐	src-dst-mac ▼
T6	☐	src-dst-mac ▼
T7	☐	src-dst-mac ▼

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

The following table describes the labels in this screen.

Table 64 PORT > Link Aggregation > Link Aggregation Setting

LABEL	DESCRIPTION
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 to activate a trunk group.

Table 64 PORT > Link Aggregation > Link Aggregation Setting (continued)

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

27.4 Link Aggregation Control Protocol

Click **PORT > Link Aggregation > Link Aggregation Control Protocol** to display the screen shown next. See [Dynamic Link Aggregation on page 172](#) for more information on dynamic link aggregation.

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

Figure 108 PORT > Link Aggregation > Link Aggregation Control Protocol

Status Link Aggregation Setting **Link Aggregation Control Protocol**

Active ON

System Priority

Group ID	LACP Active
T1	☐
T2	☐
T3	☐
T4	☐
T5	☐
T6	☐
T7	☐

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

The following table describes the labels in this screen.

Table 65 PORT > Link Aggregation > Link Aggregation Control Protocol

LABEL	DESCRIPTION
Active	Enable the switch button to enable Link Aggregation Control Protocol (LACP).
System Priority	LACP system priority is a number between 1 and 65535. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP “server”. The LACP “server” controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregation Control Protocol (LACP). The smaller the number, the higher the priority level.
Use this section to enable LACP on trunks.	
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.
Use this section to configure LACP timeout on ports.	
Port	This field displays the port number.

Table 65 PORT > Link Aggregation > Link Aggregation Control Protocol (continued)

LABEL	DESCRIPTION
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
LACP Timeout	Timeout is the time interval between the individual port exchanges of LACP packets in order to check that the peer port in the trunk group is still up. If a port does not respond after three tries, then it is deemed to be “down” and is removed from the trunk. Set a short timeout (1 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.

27.5 Technical Reference

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

27.5.1 Static Trunking Example

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

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

Figure 109 Trunking Example – Physical Connections



- 2 **Configure static trunking** – Click **PORT > 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 110 Trunking Example – Configuration Screen

The configuration screen is divided into two main sections. The top section, titled 'Link Aggregation Setting', contains a table with three columns: 'Group ID', 'Active', and 'Criteria'. The bottom section contains a table with two columns: 'Port' and 'Group'. At the bottom of the screen, there are 'Apply' and 'Cancel' buttons.

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 ▼

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

Apply Cancel

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

CHAPTER 28

Link Layer Discovery Protocol (LLDP)

28.1 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)

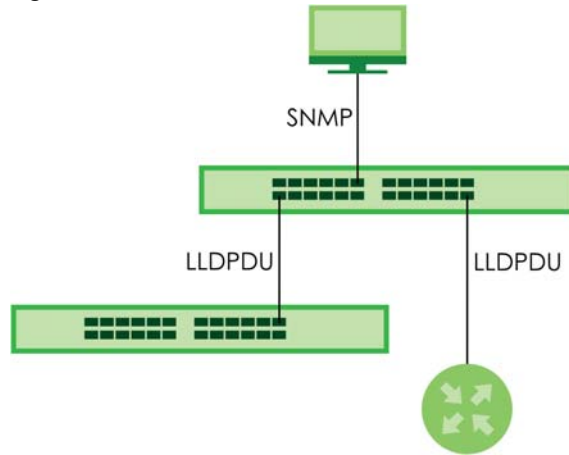
IEEE 802.3 specific TLVs:

- MAC/PHY Configuration/Status TLV (optional)
- 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 through LLDPDU and the network manager can query the information using Simple Network Management Protocol (SNMP).

Figure 111 LLDP Overview



28.2 LLDP-MED Overview

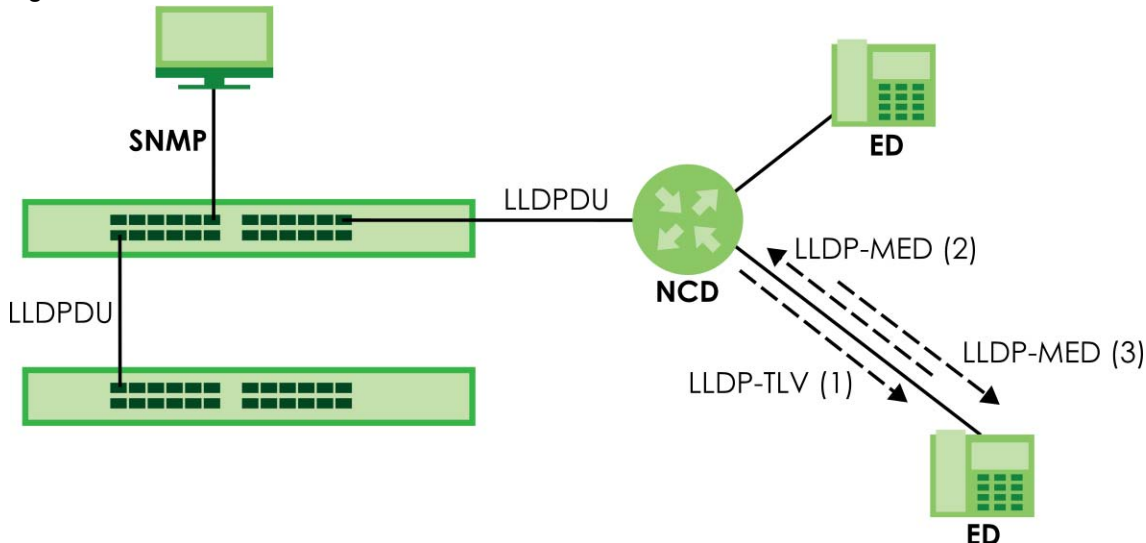
LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) is an extension to the standard LLDP developed by the Telecommunications Industry Association (TIA) TR-41.4 subcommittee which defines the enhanced discovery capabilities, such as VoIP applications, to enable network administrators manage their network topology application more efficiently. Unlike the traditional LLDP, which has some limitations when handling multiple application devices, the LLDP-MED offers display of accurate physical topology, interoperability of devices, and easy trouble shooting for mis-configured IP addresses. There are three classes of endpoint devices that the LLDP-MED supports:

Class I: IP Communications Controllers or other communication related servers

Class II: Voice Gateways, Conference Bridges or Media Servers

Class III: IP-Phones, PC-based Softphones, End user Communication Appliances supporting IP Media

The following figure shows that with the LLDP-MED, network connectivity devices (NCD) like Switches and Routers will transmit LLDP TLV to endpoint device (ED) like IP Phone first (1), to get its device type and capabilities information, then it will receive that information in LLDP-MED TLV back from endpoint devices (2), after that the network connectivity devices will transmit LLDP-MED TLV (3) to provision the endpoint device to such that the endpoint device's network policy and location identification information is updated. Since LLDPDU updates status and configuration information periodically, network managers may check the result of provision through remote status. The remote status is updated by receiving LLDP-MED TLVs from endpoint devices.

Figure 112 LLDP-MED Overview

28.2.1 What You Can Do – LLDP

- Use the **LLDP Local Status** screen ([Section 28.3 on page 182](#)) to view the Switch's LLDP information.
- Use the **LLDP Remote Status** screen ([Section 28.4 on page 187](#)) to view LLDP information from the neighboring devices.
- Use the **LLDP Setup** screen ([Section 28.5 on page 192](#)) to configure LLDP on the Switch.
- Use the **Basic TLV Setting** screen ([Section 28.6 on page 194](#)) to configure basic TLV settings on each port.
- Use the **Org-specific TLV Setting** screen ([Section 28.7 on page 195](#)) to configure organization-specific TLV settings on each port.

28.2.2 What You Can Do – LLDP MED

- Use the **LLDP-MED Setup** screen ([Section 28.8 on page 196](#)) to configure LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) parameters.
- Use the **LLDP-MED Network Policy** screen ([Section 28.9 on page 197](#)) to configure LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) network policy parameters.
- Use the **LLDP-MED Location** screen ([Section 28.10 on page 198](#)) to configure LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) location parameters.

28.3 LLDP Local Status

This screen displays a summary of LLDP status on this Switch. Click **PORT > LLDP > LLDP > LLDP Local Status** to display the screen as shown next.

Figure 113 PORT > LLDP > LLDP > LLDP Local Status

LLDP Local Status

LLDP Remote Status

LLDP Setup

Basic TLV Setting

Org-specific TLV Setting

Basic TLV

Chassis ID TLV

Chassis ID Subtype

mac-address

Chassis ID

f4:4d:5c:7c:7b:15

System Name TLV

System Name

CX4800

System Description TLV

System Description

V1.00(ACJN.0)b6 | 07/12/2024

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	

The following table describes the labels in this screen.

Table 66 PORT > LLDP > LLDP > LLDP Local Status

LABEL	DESCRIPTION
Basic TLV	
Chassis ID TLV	This displays the chassis ID of the local Switch, that is the Switch you are configuring. The chassis ID is identified by the chassis ID subtype. Chassis ID Subtype – This displays how the chassis of the Switch is identified. Chassis ID – This displays the chassis ID of the local Switch.
System Name TLV	System Name – This shows the host name of the Switch.
System Description TLV	System Description – This shows the firmware version of the Switch.
System Capabilities TLV	This shows the System Capabilities enabled and supported on the local Switch. System Capabilities Supported – Bridge System Capabilities Enabled – Bridge

Table 66 PORT > LLDP > LLDP > LLDP Local Status (continued)

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 ports. • Management Address Subtype – ipv4 or all-802 • Interface Number Subtype – unknown • Interface Number – 0 (not supported) • Object Identifier – 0 (not supported)
LLDP Port Information This displays the local port information.	
Local Port	This displays the number of the Switch port which receives the LLDPDU from the remote device. Click a port number to view the detailed LLDP status on this port in the LLDP Local Port Status Details screen.
Port ID Subtype	This indicates how the port ID field is identified.
Port ID	This is an alpha-numeric string that contains the specific identifier for the port from which this LLDPDU was transmitted.
Port Description	This shows the port description that the Switch will advertise from this port.

28.3.1 LLDP Local Port Status Details

This screen displays detailed LLDP status for each port on this Switch. Click **PORT > LLDP > LLDP > LLDP Local Status** and then, click a port number, for example 1 in the local port column to display the screen as shown next.

Figure 114 PORT > LLDP > LLDP > LLDP Local Status > LLDP Local Port Status Detail

LLDP Local Status

LLDP Remote Status

LLDP Setup

Basic TLV Setting

LLDP Local Status

> LLDP Local Port Status Detail

Local Port: 1

Basic TLV

Port ID TLV

Port ID Subtype

local-assigned

Port ID

1

Port Description TLV

Port Description

Dot1 TLV

Port VLAN ID TLV

Port VLAN ID

1

Port-Protocol VLAN ID TLV

Port-Protocol VLAN ID

Dot3 TLV

MAC PHY Configuration & Status TLV

AN Supported

Yes

AN Enabled

No

AN Advertised Capability

Oper MAU Type

36

Link Aggregation TLV

Aggregation Capability

Yes

Aggregation Status

No

Aggregated Port ID

0

Max Frame Size TLV

Max Frame Size

1518

MED TLV

Capabilities TLV

Network Policy

Yes

Location

Yes

Extend Power via MDI PSE

No

Extend Power via MDI PD

No

Inventory Management

No

Network Policy TLV

Voice

Voice-Signaling

Guest-Voice

Guest-Voice-Signaling

Softphone-Voice

Video-Conferencing

Streaming-Video

Video-Signaling

Device Type TLV

Device Type

Network Connectivity

Location Identification TLV

Coordinate-base LCI

Civic LCI

ELIN

The following table describes the labels in this screen.

Table 67 PORT > LLDP > LLDP > LLDP Local Status > LLDP Local Port Status Details

LABEL	DESCRIPTION
Local Port	This displays the number of the Switch's port.
Basic TLV	
These are the Basic TLV flags	
Port ID TLV	The port ID TLV identifies the specific port that transmitted the LLDP frame. • Port ID Subtype – This shows how the port is identified. • Port ID – This is the ID of the port.
Port Description TLV	Port Description – This displays the local port description.
Dot1 TLV	
Port VLAN ID TLV	Port VLAN ID – This displays the VLAN ID sent by the IEEE 802.1 Port VLAN ID TLV.
Port-Protocol VLAN ID TLV	Port-Protocol VLAN ID – 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	Max Frame Size – 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

Table 67 PORT > LLDP > LLDP > LLDP Local Status > LLDP Local Port Status Details (continued)

LABEL	DESCRIPTION
Network Policy TLV	This displays a network policy for the specified application. • Voice • Voice-Signaling • Guest-Voice • Guest-Voice-Signaling • Softphone-Voice • Video-Conferencing • Streaming-Video • Video-Signaling
Device Type TLV	Device Type – This is the LLDP-MED device class. The Zyxel Switch device type is: • Network Connectivity
Location Identification TLV	This shows the location information of a caller by its ELIN (Emergency Location Identifier Number) or the IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI). • Coordinate-based LCI – Latitude, longitude and altitude coordinates of the location Configuration Information (LCI) • Civic LCI – IETF Geopriv Civic Address based Location Configuration Information • ELIN – (Emergency Location Identifier Number)

28.4 LLDP Remote Status

This screen displays a summary of LLDP status for each LLDP connection to a neighboring Switch. Click **PORT > LLDP > LLDP > LLDP Remote Status** to display the screen as shown next.

Figure 115 PORT > LLDP > LLDP > LLDP Remote Status

LLDP Local Status LLDP Remote Status LLDP Setup Basic TLV Setting Org-specific TLV Setting						
Index	Local Port	Chassis ID	Port ID	Port Description	System Name	Management Address
1	1	dc:4a:3e:40:ec:5f	dc:4a:3e:40:ec:5f			
2	1	e4:18:6b:f8:20:eb	24		22A4_131	e4:18:6b:f8:20:eb
3	1	f4:4d:5c:7c:7b:15	1		CX4800	172.21.56.10

The following table describes the labels in this screen.

Table 68 PORT > LLDP > LLDP > LLDP Remote Status

LABEL	DESCRIPTION
Index	The index number shows the number of remote devices that are connected to the Switch. Click on an index number to view the detailed LLDP status for this remote device in the LLDP Remote Port Status Details screen.
Local Port	This is the number of the Switch's port that received LLDPDU from the remote device.
Chassis ID	This displays the chassis ID of the remote device associated with the transmitting LLDP agent. The chassis ID is identified by the chassis ID subtype. For example, the MAC address of the remote device.
Port ID	This is an alpha-numeric string that contains the specific identifier for the port from which this LLDPDU was transmitted. The port ID is identified by the port ID subtype.
Port Description	This displays a description for the port from which this LLDPDU was transmitted.

Table 68 PORT > LLDP > LLDP > LLDP Remote Status (continued)

LABEL	DESCRIPTION
System Name	This displays the system name of the remote device.
Management Address	This displays the management address of the remote device. It could be the MAC address or IP address.

28.4.1 LLDP Remote Port Status Details

This screen displays detailed LLDP status of the remote device connected to the Switch. Click **PORT > LLDP > 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 116 PORT > LLDP > LLDP > LLDP Remote Status > LLDP Remote Port Status Details (Basic TLV)

LLDP Local Status

LLDP Remote Status

LLDP Setup

Basic TLV Setting

Org-specific TLV Setting

LLDP Remote Status

> LLDP Remote Port Status Details

Local Port: 2

Basic TLV

Chassis ID TLV

Chassis ID Subtype

mac-address

Chassis ID

Port ID TLV

Port ID Subtype

local-assigned

Port ID

11

Time To Live TLV

Time To Live

120

Port Description TLV

Port Description

System Name TLV

System Name

22A4_121

System Description TLV

System Description

V4.30(AAGF.2)_20200930 | 09/30/2020

System Capabilities TLV

System Capabilities Supported

bridge

System Capabilities Enabled

bridge

Management Address TLV

Management Address Subtype

ALL_802

Management Address

Interface Number Subtype

unknown

Interface Number

0

Object Identifier

The following table describes the labels in Basic TLV part of the screen.

Table 69 PORT > LLDP > LLDP > LLDP Remote Status > LLDP Remote Port Status Details (Basic TLV)

LABEL	DESCRIPTION
Local Port	This displays the number of the Switch's port to which the remote device is connected.
Basic TLV	
Chassis ID TLV	Chassis ID Subtype – This displays how the chassis of the remote device is identified. Chassis ID – This displays the chassis ID of the remote device. The chassis ID is identified by the chassis ID subtype.
Port ID TLV	Port ID Subtype – This displays how the port of the remote device is identified. Port ID – This displays the port ID of the remote device. The port ID is identified by the port ID subtype.
Time To Live TLV	Time To Live – 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	Port Description – This displays the remote port description.
System Name TLV	System Name – This displays the system name of the remote device.

Table 69 PORT > LLDP > LLDP Remote Status > LLDP Remote Port Status Details (Basic TLV)

LABEL	DESCRIPTION
System Description TLV	System Description – This displays the system description of the remote device.
System Capabilities TLV	This displays whether the system capabilities are enabled and supported on the remote device. • System Capabilities Supported • System Capabilities Enabled
Management Address TLV	This displays the management address (IPv4 and IPv6) of the remote device. • Management Address Subtype • Management Address • Interface Number Subtype • Interface Number • Object Identifier

Figure 117 PORT > LLDP > LLDP Remote Status > LLDP Remote Port Status Details (Dot1 and Dot3 TLV)

Dot1 TLV		
Port VLAN ID TLV		VLAN Name TLV
Port VLAN ID		VLAN ID
		VLAN Name
Protocol Identity TLV		Port-Protocol VLAN ID TLV
Protocol ID		Port-Protocol VLAN ID
		Port-Protocol VLAN ID Supported
		Port-Protocol VLAN ID Enabled
Dot3 TLV		
MAC PHY Configuration & Status TLV		Max Frame Size TLV
AN Supported	Yes	Max Frame Size
AN Enabled	Yes	
AN Advertised Capability	1000baseTFD	Link Aggregation TLV
Oper MAU type	0	Aggregation Capability
		Aggregation Status
		Aggregated Port ID
Power Via MDI TLV		
Port Class		
MDI Supported		
MDI Enabled		
Pair Controllable		
PSE Power Pairs		
Power Class		

The following table describes the labels in the Dot1 and Dot3 parts of the screen.

Table 70 PORT > LLDP > LLDP > LLDP Remote Status > LLDP Remote Port Status Details (Dot1 and Dot3 TLV)

LABEL	DESCRIPTION
Dot1 TLV	
Port VLAN ID TLV	Port VLAN ID – This displays the VLAN ID of this port on the remote device.
Vlan Name TLV	This shows the VLAN ID and name for remote device port. VLAN ID VLAN Name
Protocol Identity TLV	Protocol ID – The Protocol Identity TLV allows the Switch to advertise the particular protocols that are accessible through its port.
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
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.
Max Frame Size TLV	Max Frame Size – This displays the maximum supported frame size in octets.
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. Aggregated Port ID – The aggregation ID of the current port.
Power Via MDI TLV	The Power Via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending port on the remote device. Port Class MDI Supported MDI Enabled Pair Controllable PSE Power Pairs Power Class

Figure 118 PORT > LLDP > LLDP > LLDP Remote Status > LLDP Remote Port Status Details (MED TLV)

MED TLV	
Capabilities TLV Network Policy Location Extend Power via MDI PSE Extend Power via MDI PD Inventory Management	Device Type TLV Device Type Location Identification TLV Coordinate-base LCI Civic LCI ELIN
Extended Power via MDI TLV Power Type Power Source Power Priority Power Value	Network Policy TLV Voice Voice-Signaling Guest-Voice Guest-Voice-Signaling Softphone-Voice Video-Conferencing Streaming-Video Video-Signaling
Inventory TLV Hardware Revision Software Revision Firmware Revision Model Name Manufacturer Serial Number Asset ID	

The following table describes the labels in the MED TLV part of the screen.

Table 71 PORT > LLDP > LLDP > LLDP Remote Status > LLDP Remote Port Status Details (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

Table 71 PORT > LLDP > LLDP > LLDP Remote Status > LLDP Remote Port Status Details (MED TLV)

LABEL	DESCRIPTION
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)
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.
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
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

28.5 LLDP Setup

Use this screen to configure global LLDP settings on the Switch. Click **PORT > LLDP > LLDP > LLDP Setup** to display the screen as shown next.

Figure 119 PORT > LLDP > LLDP > LLDP Setup

LLDP Local Status **LLDP Remote Status** **LLDP Setup** **Basic TLV Setting**

Active ☒ ON

Transmit Interval seconds

Transmit Hold times

Transmit Delay seconds

Reinitialize Delay seconds

Apply **Cancel**

Port	Admin Status	Notification
*	Tx-Rx	☐
1	Tx-Rx	☐
2	Tx-Rx	☐
3	Tx-Rx	☐
4	Tx-Rx	☐
5	Tx-Rx	☐
6	Tx-Rx	☐
7	Tx-Rx	☐

Apply **Cancel**

The following table describes the labels in this screen.

Table 72 PORT > LLDP > LLDP > LLDP Setup

LABEL	DESCRIPTION
Active	Select to enable LLDP on the Switch. It is enabled by default.
Transmit Interval	Enter how many seconds the Switch waits before sending LLDP packets.
Transmit Hold	Enter the time-to-live (TTL) multiplier of LLDP frames. The device information on the neighboring devices ages out and is discarded when its corresponding TTL expires. The TTL value is to multiply the TTL multiplier by the LLDP packets transmitting interval.
Transmit Delay	Enter the delay (in seconds) between successive LLDPDU transmissions initiated by value or status changes in the Switch MIB.
Reinitialize Delay	Enter the number of seconds for LLDP to wait before initializing on a port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Port	This displays the Switch's port number. * means all ports.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Changes in this row are copied to all the ports as soon as you make them.

Table 72 PORT > LLDP > LLDP > LLDP Setup (continued)

LABEL	DESCRIPTION
Admin Status	Select whether LLDP transmission and/or reception is allowed on this port. • Disable – not allowed • Tx-Only – transmit only • Rx-Only – receive only • Tx-Rx – transmit and receive
Notification	Select whether LLDP notification is enabled on this port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

28.6 Basic TLV Setting

Use this screen to configure Basic TLV settings. Click **PORT > LLDP > LLDP > Basic TLV Setting** to display the screen as shown next.

Figure 120 PORT > LLDP > LLDP > Basic TLV Setting

Port	Management Address	Port Description	System Capabilities	System Description	System Name
*	☐	☐	☐	☐	☐
1	☒	☒	☒	☒	☒
2	☒	☒	☒	☒	☒
3	☒	☒	☒	☒	☒
4	☒	☒	☒	☒	☒
5	☒	☒	☒	☒	☒
6	☒	☒	☒	☒	☒
7	☒	☒	☒	☒	☒

The following table describes the labels in this screen.

Table 73 PORT > LLDP > LLDP > Basic TLV Setting

LABEL	DESCRIPTION
Port	This displays the Switch's port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Changes in this row are copied to all the ports as soon as you make them.
Management Address	Select the checkboxes to enable or disable the sending of Management Address TLVs on the ports.
Port Description	Select the checkboxes to enable or disable the sending of Port Description TLVs on the ports.
System Capabilities	Select the checkboxes to enable or to disable the sending of System Capabilities TLVs on the ports.
System Description	Select the checkboxes to enable or to disable the sending of System Description TLVs on the ports.
System Name	Select the checkboxes to enable or to disable the sending of System Name TLVs on the ports.

Table 73 PORT > LLDP > LLDP > Basic TLV Setting (continued)

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

28.7 Org-specific TLV Setting

Use this screen to configure organization-specific TLV settings. Click **PORT > LLDP > LLDP > Org-specific TLV Setting** to display the screen as shown next.

Figure 121 PORT > LLDP > LLDP > Org-specific TLV Setting

Port	Port-Protocol VLAN ID	Port VLAN ID	Link Aggregation	MAC/PHY	Max Frame Size
*	☐	☐	☐	☐	☐
1	☐	☒	☐	☒	☐
2	☐	☒	☐	☒	☐
3	☐	☒	☐	☒	☐
4	☐	☒	☐	☒	☐
5	☐	☒	☐	☒	☐
6	☐	☒	☐	☒	☐
7	☐	☒	☐	☒	☐

The following table describes the labels in this screen.

Table 74 PORT > LLDP > LLDP > Org-specific TLV Setting

LABEL	DESCRIPTION
Port	This displays the Switch's port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Changes in this row are copied to all the ports as soon as you make them.
Dot1 TLV	
Port-Protocol VLAN ID	Select the checkboxes to enable or disable the sending of IEEE 802.1 Port and Protocol VLAN ID TLVs on the ports.
Port VLAN ID	Select the checkboxes to enable or disable the sending of IEEE 802.1 Port VLAN ID TLVs on the ports. All checkboxes in this column are enabled by default.
Dot3 TLV	
Link Aggregation	Select the checkboxes to enable or disable the sending of IEEE 802.3 Link Aggregation TLVs on the ports.

Table 74 PORT > LLDP > LLDP > Org-specific TLV Setting (continued)

LABEL	DESCRIPTION
MAC/PHY	Select the checkboxes to enable or disable the sending of IEEE 802.3 MAC/PHY Configuration/Status TLVs on the ports. All checkboxes in this column are enabled by default.
Max Frame Size	Select the checkboxes to enable or disable the sending of IEEE 802.3 Max Frame Size TLVs on the ports.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

28.8 LLDP-MED Setup

Click **PORT > LLDP > LLDP MED > LLDP-MED Setup** to display the screen as shown next.

Figure 122 PORT > LLDP > LLDP MED > LLDP-MED Setup

Port	Notification	MED TLV Setting	
	Topology Change	Location	Network Policy
*	☐	☐	☐
1	☐	☐	☐
2	☐	☐	☐
3	☐	☐	☐
4	☐	☐	☐
5	☐	☐	☐
6	☐	☐	☐
7	☐	☐	☐

The following table describes the labels in this screen.

Table 75 PORT > LLDP > LLDP MED > LLDP-MED Setup

LABEL	DESCRIPTION
Port	This displays the Switch's port number. Select * to configure all ports simultaneously.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Changes in this row are copied to all the ports as soon as you make them.
Notification	
Topology Change	Select to enable LLDP-MED topology change traps on this port.
MED TLV Setting	
Location	Select to enable transmitting LLDP-MED location TLV.

Table 75 PORT > LLDP > LLDP MED > LLDP-MED Setup (continued)

LABEL	DESCRIPTION
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.

28.9 LLDP-MED Network Policy

Click **PORT > LLDP > LLDP MED > LLDP-MED Network Policy** to display the screen as shown next.

Figure 123 PORT > LLDP > LLDP MED > LLDP-MED Network Policy

	Index	Port	Application Type	Tag	VLAN	DSCP	Priority
☐	1	1	voice	tagged	1	10	0

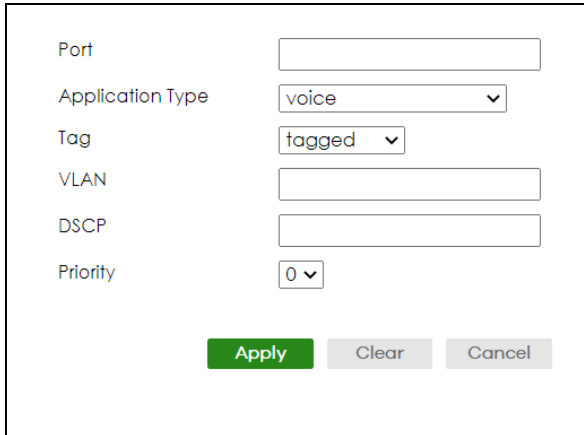
The following table describes the labels in this screen.

Table 76 PORT > LLDP > LLDP MED > LLDP-MED Network Policy

LABEL	DESCRIPTION
Index	This field displays the of index number of the network policy. Click an index number to edit the rule.
Port	This field displays the port number of the network policy.
Application Type	This field displays the application type of the network policy.
Tag	This field displays the Tag Status of the network policy.
VLAN	This field displays the VLAN ID of the network policy.
DSCP	This field displays the DSCP value of the network policy.
Priority	This field displays the priority value of the network policy.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new schedule rule or edit a selected one.
Delete	Select the rules that you want to remove, then click Delete .

28.9.1 Add/Edit LLDP-MED Network Policy

To access this screen, click the **Add/Edit** button or select an entry from the list and click the **Add/Edit** button.

Figure 124 PORT > LLDP > LLDP MED > LLDP-MED Network Policy > Add/Edit


The following table describes the labels in this screen.

Table 77 PORT > LLDP > LLDP MED > LLDP-MED Network Policy > Add/Edit

LABEL	DESCRIPTION
Port	Enter the port number to set up the LLDP-MED network policy. 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.
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.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

28.10 LLDP-MED Location

Click **PORT > LLDP > LLDP MED > LLDP-MED Location** to display the screen as shown next.

Figure 125 PORT > LLDP > LLDP MED > LLDP-MED Location

☐	Index	Port	Location Coordinates	Civic Address	ELIN Number

The following table describes the labels in this screen.

Table 78 PORT > LLDP > LLDP MED > LLDP-MED Location

LABEL	DESCRIPTION
Index	This lists the index number of the location configuration. Click an index number to view or edit the location.
Port	This lists the port number of the location configuration.
Location Coordinates	This field displays the location configuration information based on geographical coordinates that includes longitude, latitude, altitude and datum.
Civic Address	This field displays the Civic Address for the remote device using information such as Country, State, County, City, Street, Number, ZIP code and additional information.
ELIN Number	This field shows the Emergency Location Identification Number (ELIN), which is used to identify endpoint devices when they issue emergency call services. The valid length is form 10 to 25 characters.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new location or edit a selected one.
Delete	Select the locations that you want to remove, then click Delete .

28.10.1 Add/Edit LLDP-MED Location

To access this screen, click the **Add/Edit** button or select an entry from the list and click the **Add/Edit** button.

Figure 126 PORT > LLDP > LLDP MED > LLDP-MED Location > Add/Edit

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			
ELIN Number			
Apply Clear Cancel			

The following table describes the labels in this screen.

Table 79 PORT > LLDP > LLDP MED > LLDP-MED Location > Add/Edit

LABEL	DESCRIPTION
Port	Enter the port number you want to set up the location within the LLDP-MED network.
Location Coordinates The LLDP-MED uses geographical coordinates and Civic Address to set the location information of the remote device. Geographical based coordinates includes latitude, longitude, altitude and datum. Civic Address includes Country, State, County, City, Street and other related information.	
Latitude	Enter the latitude information. The value should be from 0° to 90°. • north • south

Table 79 PORT > LLDP > LLDP MED > LLDP-MED Location > Add/Edit (continued)

LABEL	DESCRIPTION
Longitude	Enter the longitude information. The value should be from 0° to 180°. • west • east
Altitude	Enter the altitude information. The value should be from –2097151 to 2097151 in meters or in floors. • meters • floor
Datum	Select the appropriate geodetic datum used by GPS. • WGS84 • NAD83-NAVD88 • NAD83-MLLW
Civic Address	Enter the Civic Address by providing information such as Country, State, County, City, Street, Number, ZIP code and other additional information. Enter at least 2 fields in this configuration including the Country. The valid length of the Country field is 2 characters and all other fields are up to 32 characters. • Country • State • County • City • Division • Neighbor • Street • Leading-Street-Direction • Street-Suffix • Trailing-Street-Suffix • House-Number • House-Number-Suffix • Landmark • Additional-Location • Name • Zip-Code • Building • Unit • Floor • Room-Number • Place-Type • Postal-Community-Name • Post-Office-Box • Additional-Code
ELIN Number	Enter a numerical digit string, corresponding to the ELIN identifier which is used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. The valid length is from 10 to 25 characters.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

CHAPTER 29

Port Setup

29.1 Port Setup

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

Figure 127 PORT > Port Setup > Port Setup

Port	Active	Name	Speed / Duplex	FEC	802.1p Priority	BPDU Ctrl
*	☐		Auto	Auto	0	Peer
1	☒		Auto	Auto	0	Peer
2	☒		Auto	Auto	0	Peer
3	☒		Auto	Auto	0	Peer
4	☒		Auto	Auto	0	Peer
5	☒		Auto	Auto	0	Peer
6	☒		Auto	Auto	0	Peer
48	☒		Auto	Auto	0	Peer
49	☒		100G / Full Duplex	Auto	0	Peer
50	☒		100G / Full Duplex	Auto	0	Peer
51	☒		100G / Full Duplex	Auto	0	Peer
52	☒		100G / Full Duplex	Auto	0	Peer
53	☒		100G / Full Duplex	Auto	0	Peer
54	☒		100G / Full Duplex	Auto	0	Peer
55	☒		100G / Full Duplex	Auto	0	Peer
56	☒		100G / Full Duplex	Auto	0	Peer

The following table describes the labels in this screen.

Table 80 PORT > Port Setup > Port Setup

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

Table 80 PORT > Port Setup > Port Setup (continued)

LABEL	DESCRIPTION
Active	Select this checkbox 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 128 printable ASCII characters except [?], [], ['] or ["]. Note: Due to space limitations, the port name may be truncated in some Web Configurator screens.
Speed/Duplex	Select the speed and the duplex mode of the connection on this port. For an SFP28 fiber port, the choices are Auto, 1G / Full Duplex, 10G / Full Duplex, 25G-an (25G/ auto-negotiation), and 25G / Full Duplex. For a QSFP28 fiber port, the choices are 100G-an (100G/auto-negotiation), and 100G / Full Duplex. 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.
FEC	To minimize signal degradation of data at high transmission speeds (for example, 25 Gbps or 100 Gbps), set the same FEC (Forward Error Correction) type between the Switch and the connected device. Select Auto to allow both connected ports to automatically set the FEC type according to the following rules: - For 10G transceivers, the FEC type on the port will automatically be None. - For 25G transceivers, the FEC type on the port will automatically be CL108. - For 100G transceivers, the FEC type on the port will automatically be None if the transceiver type is 100G LR4/ER4; all other types of transceiver will automatically be CL91. Select CL74 when both connected ports support 25 Gbps speed and require low latency in data transmission. Select CL91 when both connected ports support 25 Gbps and 100 Gbps speeds. Select CL108 when both connected ports support 25 Gbps speed but low latency in data transmission is not required. Alternatively, select None when you do not need to set the FEC type. Note: Make sure to set the correct Speed/Duplex on this screen.
802.1p Priority	This priority value is added to incoming frames without a (802.1p) tag.
BPDU Ctrl	Configure the way to treat BPDUs received on this port. You must activate Bridging Control Protocol Transparency in the SYSTEM > Switch Setup > 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. Note: BPDU control is only available in Standalone mode.

Table 80 PORT > Port Setup > Port Setup (continued)

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

29.2 Technical Reference

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

29.2.1 CL (Clause) Types and Applications

The following table lists the types of FEC algorithms, also known as CLs (Clauses), and its applications.

Table 81 CL (Clause) Types and Applications

CLAUSE	APPLICATION
CL74	Support for 25 Gbps transmission speed only. Select CL74 for applications that require real-time data transmission such as VoIP services. VoIP packets need to be prioritized to prevent dropped calls and ensure crystal-clear audio quality.
CL91	Support for both 25 Gbps and 100 Gbps transmission speeds. Select CL91 for applications that require 100 Gbps transmission speed. The 100 Gbps ports can use any of the following transceivers. 100 Gbps SR4. SR4 (Short Range 4) are for connections up to 100 meters over OM3 (Optical Fiber Cable Specification for Multi-Mode 3) fiber optic cables, or connections up to 150 meters over OM4 (Optical Fiber Cable Specification for Multi-Mode 4) fiber optic cables. 100 Gbps CR4. CR4 (Copper 4) are for connections up to 7 meters for passive DAC type transceivers, or connections up to 10 meters for active DAC type transceivers. Passive DAC type transceivers uses less than 0.15 watt of power. Active DAC type transceivers uses more power from 0.5 to 1.0 watt. 100 Gbps fan-out cable. A fan-out cable is a transceiver that can connect to four 25 Gbps devices. Use a fan-out cable to aggregate four 25 Gbps ports into one logical interface to provide higher bandwidth, load balancing, and link redundancy.
CL108	Support for 25 Gbps transmission speed only. Select CL108 for applications that do not require real-time data transmission such as web browsing, emails, file transfers and software updates.

29.2.2 FEC Types and Transceivers

The following table lists the FEC types and the corresponding types of transceivers to use.

Table 82 FEC Types and Transceivers

FEC TYPE	TRANSCEIVER TYPE
CL74	25G DAC CA-S 3m 25G AOC 1-10m 25G-CR CA-25G-S
CL91	25G DAC CA-L 5m 25G-CR CA-25G-L The above two fan-out cable transceivers can connect to four 25 Gbps devices. A fan-out cable can aggregate four 25 Gbps ports into one logical interface, providing higher bandwidth, load balancing, and link redundancy. 100G-CR4 (Copper 4) Use this for connections up to 7 meters for passive DAC type transceivers, or connections up to 10 meters for active DAC type transceivers. Passive DAC type transceivers uses less than 0.15 watt of power. Active DAC type transceivers uses more power from 0.5 to 1.0 watt. 100G-SR4 (Short Range 4) Use this for connections up to 100 meters over OM3 (Optical Fiber Cable Specification for Multi-Mode 3) fiber optic cables, or connections up to 150 meters over OM4 (Optical Fiber Cable Specification for Multi-Mode 4) fiber optic cables.
CL108	25G-SR 25G-LR 25G-ER
None (No FEC)	10G 25G DAC CA-N 1-3m 25G-CR CA-25G-N 100G-LR4 100G-ER4

29.2.3 FEC Types and Negotiation Results

The following table lists the FEC types of transmitting and receiving ports and the result of connection speed and duplex negotiation at 25 Gbps and 100 Gbps transmission speeds.

Table 83 FEC Types and Negotiation Results

PORT A	PORT B	NEGOTIATION RESULT
25 Gbps		
CL108	CL108	CL108
CL74	CL74	CL74
None (No FEC)	None (No FEC)	None (No FEC)
None (No FEC)	CL108	CL108
None (No FEC)	CL74	CL74
CL74	CL108	CL108
100 Gbps		
CL91	CL91	CL91
None (No FEC)	None (No FEC)	CL91
None (No FEC)	CL91	CL91

CHAPTER 30

SWITCHING

The following chapters introduces the configurations of the links under the **SWITCHING** navigation panel.

Quick links to chapters:

- [Loop Guard](#)
- [Mirroring](#)
- [Multicast](#)
- [Static Multicast Forwarding](#)
- [Private VLAN](#)
- [Differentiated Services](#)
- [Queuing Method](#)
- [Priority Queue Overview](#)
- [sFlow](#)
- [Spanning Tree Protocol](#)
- [Static MAC Filtering](#)
- [Static MAC Forwarding](#)
- [VLAN](#)
- [VLAN Mapping](#)
- [VLAN Stacking](#)
- [WoL Relay](#)

CHAPTER 31

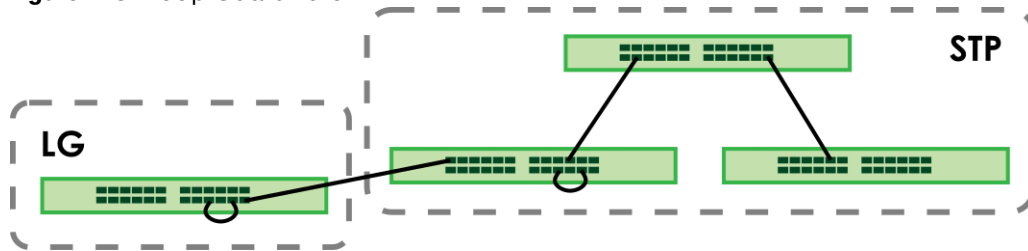
Loop Guard

31.1 Loop Guard Overview

This chapter shows you how to configure the Switch to guard against loops on the edge of your network.

Loop guard (**LG**) 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 128 Loop Guard vs. STP



Refer to [Section 31.1.2 on page 207](#) for more information.

31.1.1 What You Can Do

Use the **Loop Guard** screen ([Section 31.2 on page 208](#)) to enable loop guard on the Switch and in specific ports.

31.1.2 What You Need to Know

Loop guard is designed to handle loop problems on the edge of your network. This can occur when a port is connected to a Switch that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in loop state sends out broadcast messages the messages loop back to the switch and are re-broadcast again and again causing a broadcast storm.

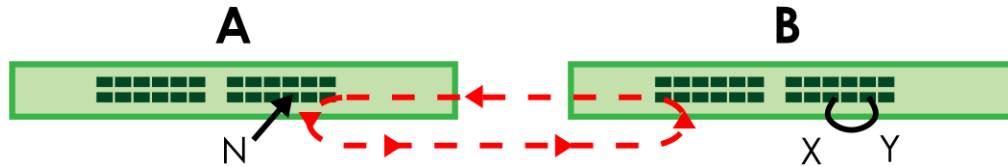
If a switch (not in loop state) connects to a switch in loop state, then it will be affected by the switch in loop state in the following way:

- The switch (not in loop state) will receive broadcast messages sent out from the switch in loop state.
- The switch (not in loop state) will receive its own broadcast messages that it sends out as they loop back. It will then re-broadcast those messages again.

The following figure shows port **N** on switch **A** connected to switch **B**. Switch **B** has two ports, **X** and **Y**, mistakenly connected to each other. It forms a loop. When broadcast or multicast packets leave port **N**

and reach switch **B**, they are sent back to port **N** on **A** as they are rebroadcast from **B**.

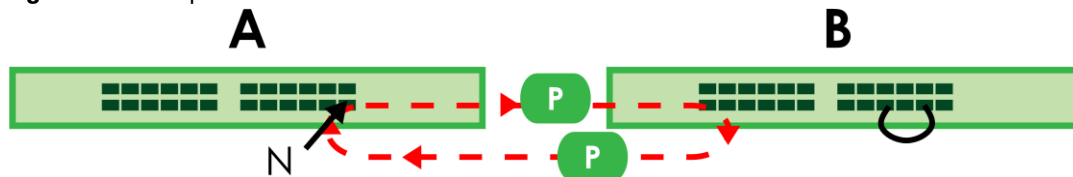
Figure 129 Switch in Loop State



The loop guard feature checks to see if a loop guard enabled port is connected to a Switch in loop state. This is accomplished by periodically sending a probe packet and seeing if the packet returns on the same port. If this is the case, the Switch will shut down the port connected to the switch in loop state.

Loop guard can be enabled on both Ethernet ports. The following figure shows a loop guard enabled port **N** on switch **A** sending a probe packet **P** to switch **B**. Since switch **B** is in loop state, the probe packet **P** returns to port **N** on **A**. The Switch then shuts down port **N** to ensure that the rest of the network is not affected by the switch in loop state.

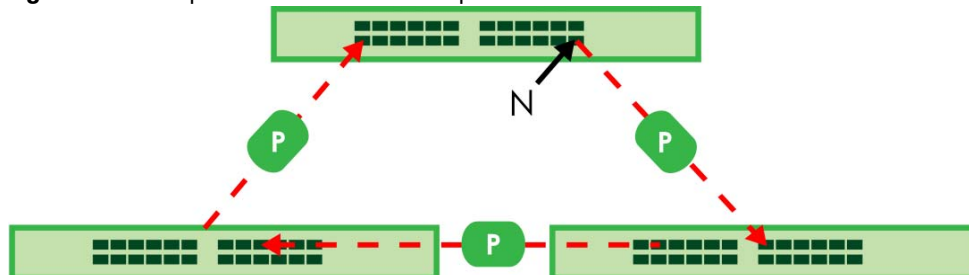
Figure 130 Loop Guard – Probe Packet



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 131 Loop Guard – Network Loop



Note: After resolving the loop problem on your network you can re-activate the disabled port through the Web Configurator or through commands (See the CLI Reference Guide).

31.2 Loop Guard Setup

Click **SWITCHING** > **Loop Guard** > **Loop Guard** in the navigation panel to display the screen as shown.

Note: The loop guard feature cannot be enabled on the ports that have Spanning Tree Protocol (RSTP, MRSTP or MSTP) enabled.

Figure 132 SWITCHING > Loop Guard > Loop Guard

Loop Guard

Active ☐ OFF

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

Apply Cancel

The following table describes the labels in this screen.

Table 84 SWITCHING > Loop Guard > Loop Guard

LABEL	DESCRIPTION
Active	Enable the switch button to activate loop guard function on the Switch. The Switch generates syslog, internal log messages as well as SNMP traps when it shuts down a port through the loop guard feature.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to enable the loop guard feature on this port. The Switch sends broadcast and multicast probe packets from this port to check if the switch it is connected to is in loop state. If the switch that this port is connected is in loop state the Switch will shut down this port. Clear this checkbox to disable the loop guard feature.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 32

Mirroring

32.1 Mirroring Overview

This chapter discusses port mirroring setup screens.

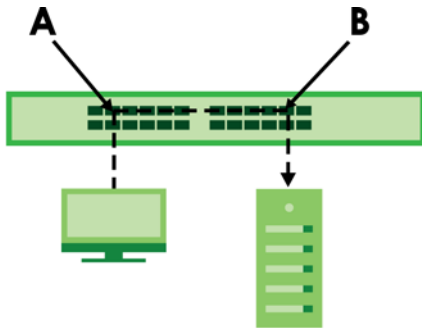
Port mirroring allows you to copy a traffic flow to a monitor port (the port you copy the traffic to) in order that you can examine the traffic from the monitor port without interference.

32.1.1 What You Need to Know

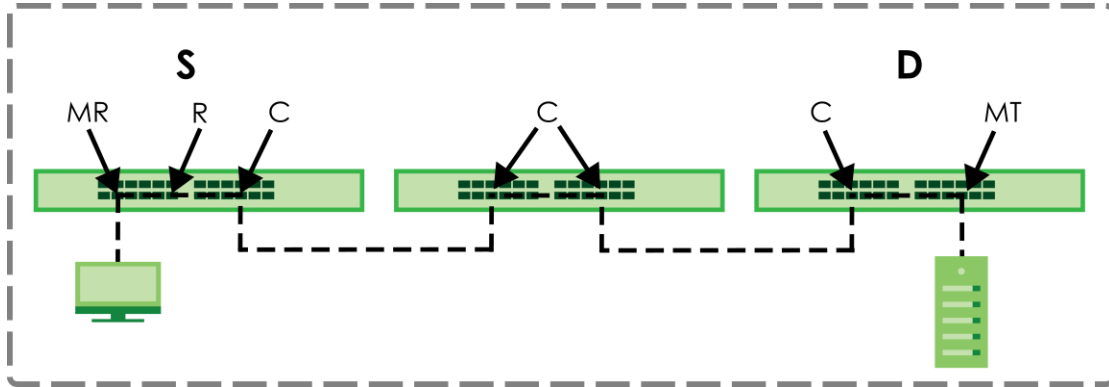
Read on for concepts on Mirroring that can help you configure the screens in this chapter.

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

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

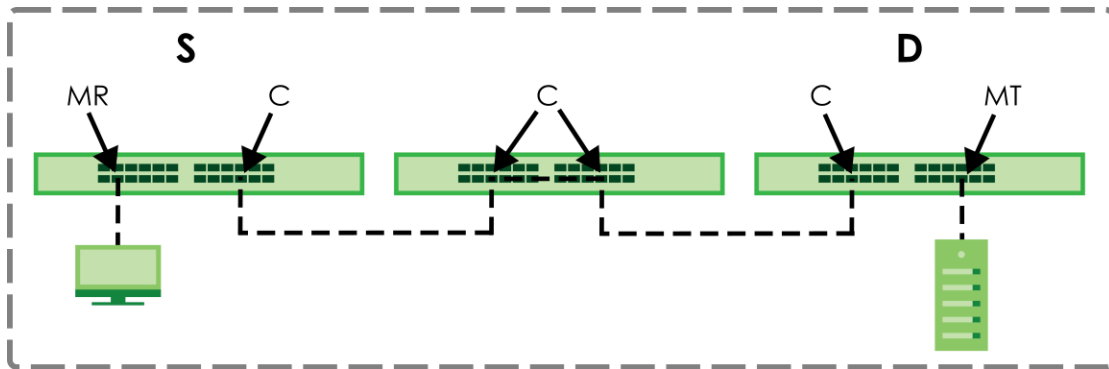


In remote port mirroring (RMirror), the mirroring ports (**MR**) and monitor port (**MT**) can be on different devices in a network. You can use it to monitor multiple switches across your network. The traffic from the source device's (**S**) mirroring ports (**MR**) is sent to a reflector port (**R**)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



Single-Destination RMirror

If the mirrored traffic is forwarded to one single destination Switch (**D**), you can disable the reflector port (**R**). The Switch adds RMirror VLAN tag and forwards mirrored traffic from the mirroring port (**MR**) to the connected port (**C**) directly.



32.2 Local Port Mirroring

Click **SWITCHING** > **Mirroring** > **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 133 SWITCHING > Mirroring > Mirroring

Mirroring

Active ☐ OFF

Monitor Port

Port	Mirrored	Direction
*	☐	ingress ▼
1	☐	ingress ▼
2	☐	ingress ▼
3	☐	ingress ▼
4	☐	ingress ▼
5	☐	ingress ▼
6	☐	ingress ▼
7	☐	ingress ▼

Apply Cancel

The following table describes the labels in this screen.

Table 85 SWITCHING > Mirroring > Mirroring

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

CHAPTER 33

Multicast

33.1 Multicast Overview

This chapter shows you how to configure various multicast features.

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

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

33.1.1 What You Can Do – IPv4 Multicast

- Use the **IPv4 Multicast Status** screen ([Section 33.2 on page 217](#)) to view IPv4 multicast group information.
- Use the **IGMP Snooping** screen ([Section 33.3 on page 217](#)) to enable IGMP snooping to forward group multicast traffic only to ports that are members of that group.
- Use the **IGMP Snooping VLAN** screen ([Section 33.4 on page 221](#)) to perform IGMP snooping on VLANs.
- Use the **IGMP Filtering Profile** ([Section 33.5 on page 222](#)) to specify a range of multicast groups that clients connected to the Switch are able to join.

33.1.2 What You Can Do – MVR

- Use the **MVR** screen ([Section 33.6 on page 225](#)) to create multicast VLANs and select the receiver ports and a source port for each multicast VLAN.
- Use the **Group Setup** screen ([Section 33.6 on page 225](#)) to configure MVR IP multicast group addresses.

33.1.3 What You Need to Know

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

IP Multicast Addresses

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

IGMP 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.

IGMP Snooping

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

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

IGMP Snooping and VLANs

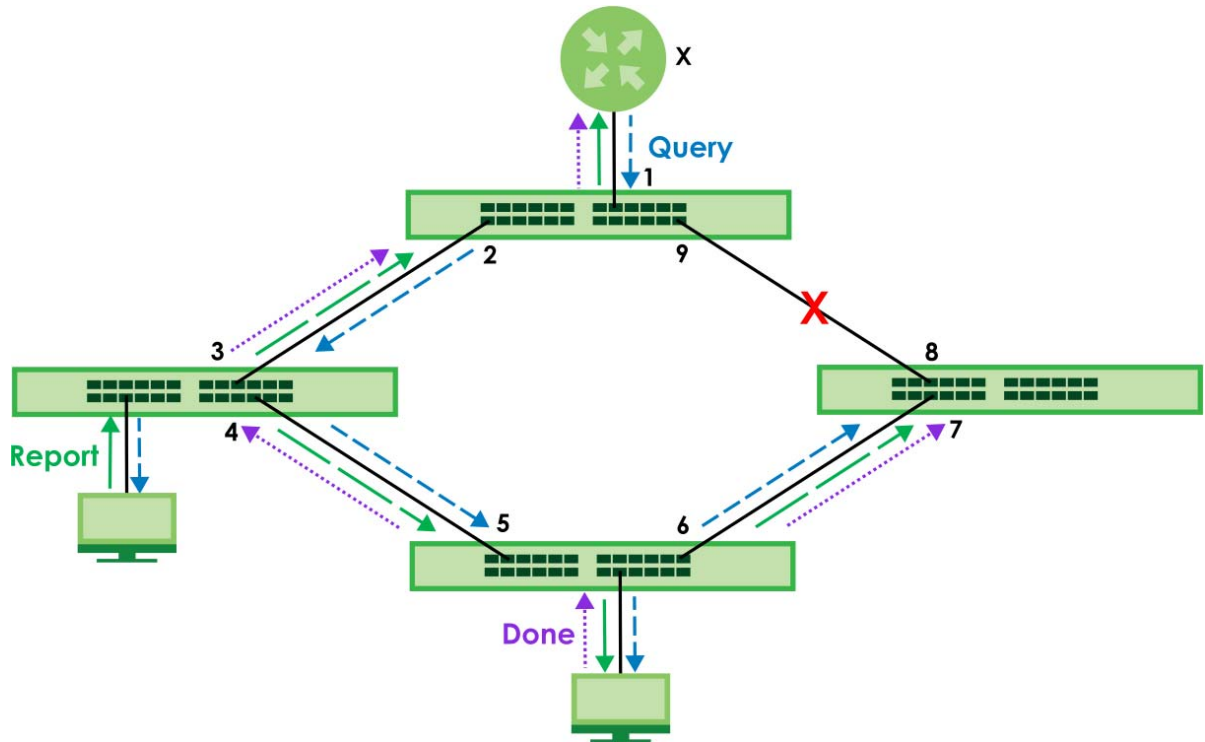
The Switch can perform IGMP snooping on up to 16 VLANs. You can configure the Switch to automatically learn multicast group membership of any VLANs. The Switch then performs IGMP snooping on the first 16 VLANs that send IGMP packets. This is referred to as auto mode. Alternatively, you can specify the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

MLD Snooping-proxy

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

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

In the following MLD snooping-proxy example, all connected upstream ports (**1 – 7**) are treated as one interface. The connection between ports **8** and **9** is blocked by STP to break the loop. If there is one **Query** from a router (**X**) or MLD **Done** or **Report** message from any upstream port, it will be broadcast to all connected upstream ports.



MLD Messages

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

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

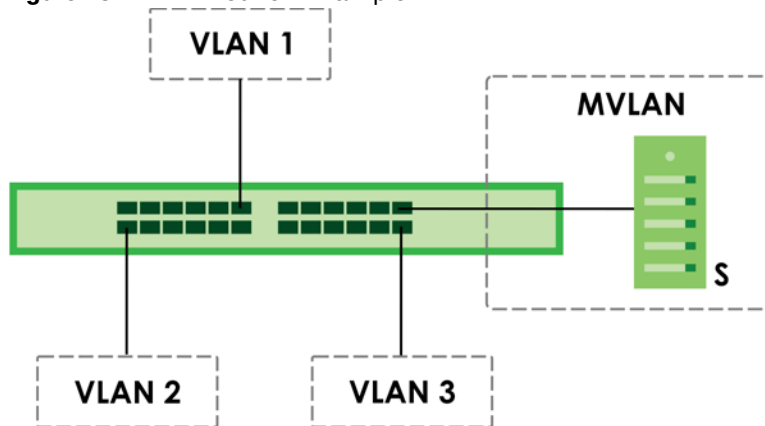
MVR Overview

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

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

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

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

Figure 134 MVR Network Example

Types of MVR Ports

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

MVR Modes

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

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

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

How MVR Works

The following figure shows a multicast television example where a subscriber device (such as a computer) in **VLAN 1** receives multicast traffic from the streaming media server (**S**), through 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 135 MVR Multicast Television Example

33.2 IPv4 Multicast Status

Click **SWITCHING > Multicast > IPv4 Multicast > IPv4 Multicast Status** to display the screen as shown. This screen shows the IPv4 multicast group information. See [Section 33.1 on page 213](#) for more information on multicasting.

Figure 136 SWITCHING > Multicast > IPv4 Multicast > IPv4 Multicast Status

IPv4 Multicast Status			
IGMP Snooping		IGMP Snooping VLAN	
Index	VID	Port	Multicast Group
1	1	18	224.0.0.251
2	1	18	224.0.0.252
3	1	18	239.255.255.250

The following table describes the labels in this screen.

Table 86 SWITCHING > Multicast > IPv4 Multicast > IPv4 Multicast Status

LABEL	DESCRIPTION
Index	This is the index number of the entry.
VID	This field displays the multicast VLAN ID.
Port	This field displays the port number that belongs to the multicast group.
Multicast Group	This field displays IP multicast group addresses.

33.3 IGMP Snooping

Click **SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping** to display the screen as shown. See [Section 33.1 on page 213](#) for more information on multicasting.

Figure 137 SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping

IPv4 Multicast Status | **IGMP Snooping** | IGMP Snooping VLAN | IGMP Filtering Profile

Active: ☒ ON

Querier: ☒

Querier Version: v3

Querier Query Interval: 125 seconds

Report Proxy: ☒

Host Timeout: 260 seconds

802.1p Priority: No-Change

IGMP Filtering Active: ☒ ON

IGMP Snooping Smart Forward Active: ☒ ON

Unknown Multicast Frame: ☐ Flooding ☐ Drop ☒ Drop on VLAN

Unknown Multicast Frame to Querier Port: ☐ Drop ☐ Forwarding ☒ Forwarding on VLAN

Reserved Multicast Group: ☒ Flooding ☐ Drop

Port	Immediate Leave	Normal Leave	Fast Leave	Group Limited	Max Group Number	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

Apply Cancel

The following table describes the labels in this screen.

Table 87 SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping

LABEL	DESCRIPTION
Active	Enable the switch button to enable IGMP Snooping to forward group multicast traffic only to ports that are members of that group.
Querier	Select this to allow the Switch to send IGMP General Query messages to the VLANs with the multicast hosts attached.
Querier Version	IGMP snooping query works only when both host and Switch support the same IGMP version. Select v2 to allow the Switch to send IGMPv2 queries only. Select v3 to allow the Switch to send IGMPv3 queries only.
Querier Query Interval	Enter the period in seconds between each IGMP snooping query (1–65535).
Report Proxy	Select this to allow the Switch to act as the IGMP report proxy and leave proxy. It will report group changes to a connected multicast router. The Switch not only checks IGMP packets between multicast routers or switches and multicast hosts to learn the multicast group membership, but also replaces the source MAC address in an IGMP v1/v2 report with its own MAC address before forwarding to the multicast router or switch. When the Switch receives more than one IGMP v1/v2 join report that requests to join the same multicast group, it only sends a new join report with its MAC address. This helps reduce the number of multicast join reports passed to the multicast router or switch. The Switch sends a leave message with its MAC address to the multicast router or switch only when it receives the leave message from the last host in a multicast group.

Table 87 SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping (continued)

LABEL	DESCRIPTION
Host Timeout	Specify the time (from 1 to 16711450) in seconds that elapses before the Switch removes an IGMP group membership entry if it does not receive report messages from the port.
802.1p Priority	Select a priority level (0 – 7) to which the Switch changes the priority in outgoing IGMP control packets. Otherwise, select No-Change to not replace the priority.
IGMP Filtering Active	Enable the switch button to enable IGMP filtering to control which IGMP groups a subscriber on a port can join. If you enable IGMP filtering, you must create and assign IGMP filtering profiles for the ports that you want to allow to join multicast groups.
IGMP Snooping Smart Forward Active	Enable the switch button to enable sending of multicast frame to querier port and IGMP subscriber groups. Otherwise, the querier port forwards the frames only when it receives a join report and it belongs to the IGMP group.
Unknown Multicast Frame	Specify the action to perform when the Switch receives an unknown multicast frame. - Select Flooding to send the frames to all ports. - Select Drop to discard the frames. - Select Drop on VLAN and enter the VLAN ID numbers to discard the frames on the specified VLANs. Use a dash to specify consecutive VLANs and a comma (no spaces) to specify non-consecutive VLANs. For example, 51–53 includes 51, 52 and 53, but 51,53 does not include 52.
Unknown Multicast Frame to Querier Port	Specify the action to perform when Unknown Multicast Frame is set to Drop . - Select Drop to discard the frames. - Select Forwarding to send the frames to all querier ports. - Select Forwarding on VLAN and enter the VLAN ID numbers to send the frames to the ports which are used as an IGMP query port on the specified VLANs. Use a dash to specify consecutive VLANs and a comma (no spaces) to specify non-consecutive VLANs. For example, 51–53 includes 51, 52 and 53, but 51,53 does not include 52.
Reserved Multicast Group	The IP address range of 224.0.0.0 to 224.0.0.255 are reserved for multicasting on the local network only. For example, 224.0.0.1 is for all hosts on a local network segment and 224.0.0.9 is used to send RIP routing information to all RIP v2 routers on the same network segment. A multicast router will not forward a packet with the destination IP address within this range to other networks. See the IANA web site for more information. The layer-2 multicast MAC addresses used by Cisco layer-2 protocols, 01:00:0C:CC:CC:CC and 01:00:0C:CC:CC:CD, are also included in this group. Specify the action to perform when the Switch receives a frame with a reserved multicast address. - Select Flooding to send the frames to all ports. - Select Drop to discard the frames.
Use this section to configure IGMP Snooping on each port.	
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Immediate Leave	Select this to set the Switch to remove this port from the multicast tree when an IGMP version 2 leave message is received on this port. Select this option if there is only one host connected to this port.

Table 87 SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping (continued)

LABEL	DESCRIPTION
Normal Leave	Enter an IGMP normal leave timeout value (from 200 to 6348800) 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 6348800) 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 Number	Enter the number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new IGMP join report frames is dropped on this port.
Throttling	IGMP throttling controls how the Switch deals with the IGMP reports when the maximum number of the IGMP groups a port can join is reached. Select Deny to drop any new IGMP join report received on this port until an existing multicast forwarding table entry is aged out. Select Replace to replace an existing entry in the multicast forwarding table with the new IGMP reports received on this port.
IGMP Filtering Profile	Select the name of the IGMP filtering profile to use for this port. Otherwise, select Default to prohibit the port from joining any multicast group. You can create IGMP filtering profiles in the SWITCHING > Multicast > IPv4 Multicast > IGMP Filtering Profile screen.
IGMP Querier Mode	The Switch treats an IGMP query port as being connected to an IGMP multicast router (or server). The Switch forwards IGMP join or leave packets to an IGMP query port. Select Auto to have the Switch use the port as an IGMP query port if the port receives IGMP query packets. Select Fixed to have the Switch always use the port as an IGMP query port. Select this when you connect an IGMP multicast server to the port. Select Edge to stop the Switch from using the port as an IGMP query port. The Switch will not keep any record of an IGMP router being connected to this port. The Switch does not forward IGMP join or leave packets to this port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

33.4 IGMP Snooping VLAN

Click **SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping VLAN** to display the screen as shown. See [IGMP Snooping and VLANs on page 214](#) for more information on IGMP Snooping VLAN.

Note: You can perform IGMP snooping on up to 16 VLANs.

Figure 138 SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping VLAN

IGMP Snooping VLAN

Mode ☒ auto ☐ fixed

Apply **Cancel**

VLAN

+ Add/Edit **Delete**

☐	Index	Name	VID
☐	1	VLAN66	66

The following table describes the labels in this screen.

Table 88 SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping VLAN

LABEL	DESCRIPTION
IGMP Snooping VLAN	
Mode	Select auto to have the Switch learn multicast group membership information of any VLANs automatically. Select fixed to have the Switch only learn multicast group membership information of the VLANs that you specify below. In either auto or fixed mode, the Switch can learn up to 16 VLANs (including up to five VLANs you configured in the MVR screen). For example, if you have configured one multicast VLAN in the SWITCHING > Multicast > 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. You must also enable IGMP snooping in the SWITCHING > 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 on which the Switch is to perform IGMP snooping.	
Index	This is the index number of the IGMP snooping VLAN entry in the table.
Name	This field displays the descriptive name for this VLAN group.
VID	This field displays the ID number of the VLAN group.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.

Table 88 SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping VLAN (continued)

LABEL	DESCRIPTION
Add/Edit	Click Add/Edit to create a new entry or edit a selected one.
Delete	Click Delete to remove the selected entries.

33.4.1 Add/Edit IGMP Snooping VLANs

This screen allows you to add an IGMP snooping VLAN or edit an existing one.

To access this screen, click the **Add/Edit** button or select an entry from the list and click the **Add/Edit** button.

Figure 139 SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping VLAN > Add/Edit

The following table describes the labels in this screen.

Table 89 SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping VLAN > Add/Edit

LABEL	DESCRIPTION
Name	Enter the descriptive name of the VLAN for identification purposes. You can enter up to 32 printable ASCII characters except [?], [], ['], ["] or [,].
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 SWITCHING > Multicast > MVR 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.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

33.5 IGMP Filtering Profile

An IGMP filtering profile specifies a range of multicast groups that clients connected to the Switch are able to join. A profile contains a range of multicast IP addresses which you want clients to be able to join. Profiles are assigned to ports (in the **SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping** screen). Clients connected to those ports are then able to join the multicast groups specified in the profile. Each port can be assigned a single profile. A profile can be assigned to multiple ports.

Click **SWITCHING > Multicast > IPv4 Multicast > IGMP Filtering Profile** link to display the screen as shown.

Figure 140 SWITCHING > Multicast > IPv4 Multicast > IGMP Filtering Profile

IPv4 Multicast Status IGMP Snooping IGMP Snooping VLAN IGMP Filtering Profile			
+ Add Profile + Add Rule Delete			
☐	Profile Name	Start Address	End Address
	Default	0.0.0.0	0.0.0.0
☐	Profile 1		
☐		224.0.0.0	224.0.0.0
☐		225.0.0.0	225.225.0.0

The following table describes the labels in this screen.

Table 90 SWITCHING > Multicast > IPv4 Multicast > IGMP Filtering Profile

LABEL	DESCRIPTION
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.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add Profile	Click this to add a new IGMP filtering profile.
Add Rule	Click Add Rule to add a new rule and specify the profile it belongs to in the Add Rule screen. You can also select a profile entry and click Add Rule to add an additional rule for the selected profile.
Delete	Select a profile and click Delete to remove the selected profile and the accompanying rules. Select a rule from a profile and click Delete to remove the selected rule.

33.5.1 Add IGMP Filtering Profile

To access this screen, click the **Add Profile** button in the **SWITCHING > Multicast > IPv4 Multicast > IGMP Filtering Profile** screen.

Figure 141 SWITCHING > Multicast > IPv4 Multicast > IGMP Filtering Profile > Add Profile

Profile Name
 Start Address
 End Address

The following table describes the labels in this screen.

Table 91 SWITCHING > Multicast > IPv4 Multicast > IGMP Filtering Profile > Add Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile for identification purposes. You can enter up to 32 printable ASCII characters except [?], [], ['], ["], or [,].
Start Address	Enter the starting multicast IP address for a range of multicast IP addresses that you want to belong to the IGMP filter profile.
End Address	Enter 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.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

33.5.2 Add IGMP Filtering Rule

Click **Add Rule** in the **SWITCHING > Multicast > IPv4 Multicast > IGMP Filtering Profile** screen to access this screen.

Figure 142 SWITCHING > Multicast > IPv4 Multicast > IGMP Filtering Profile > Add Rule

The following table describes the labels in this screen.

Table 92 SWITCHING > Multicast > IPv4 Multicast > IGMP Filtering Profile > Add Rule

LABEL	DESCRIPTION
Profile Name	Select a profile from the drop-down list to add a additional rule for the existing profile.
Start Address	Enter the starting multicast IP address for a range of multicast IP addresses that you want to belong to the IGMP filter profile.
End Address	Enter 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.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

33.6 MVR Configuration

Use this screen to view and create multicast VLANs.

Click **SWITCHING > Multicast > MVR > 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 143 SWITCHING > Multicast > MVR > MVR

☐	VLAN	Active	Name	Mode	Source Port	Receiver Port	802.1p Priority
☐	5	ON	GroupExample	Dynamic			0

The following table describes the related labels in this screen.

Table 93 SWITCHING > Multicast > MVR > MVR

LABEL	DESCRIPTION
VLAN	This field displays the multicast VLAN ID.
Active	This field displays whether the multicast group is enabled or not.
Name	This field displays the descriptive name for this setting.
Mode	This field displays the MVR mode.
Source Port	This field displays the source port numbers.
Receiver Port	This field displays the receiver port numbers.
802.1p Priority	This field displays the priority level.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new multicast VLAN or edit a selected one.
Delete	Select the entries that you want to remove, then click Delete to delete multicast VLANs.

33.6.1 Add/Edit MVR

Use this screen to create or edit multicast VLANs and select the receiver ports and a source port for each multicast VLAN.

To access this screen, click **Add/Edit** or select an existing entry and click **Add/Edit** in the **SWITCHING > Multicast > MVR > MVR** screen.

Figure 144 SWITCHING > Multicast > MVR > MVR > Add/Edit

Active ☐ OFF

Group Name

Multicast VLAN ID

802.1p Priority

Mode ☒ Dynamic ☐ Compatible

Port	Source Port	Receiver Port	None	Tagging
*		None		☐
1	☐	☐	☒	☐
2	☐	☐	☒	☐
3	☐	☐	☒	☐
4	☐	☐	☒	☐
5	☐	☐	☒	☐
6	☐	☐	☒	☐
7	☐	☐	☒	☐

Apply Clear Cancel

The following table describes the related labels in this screen.

Table 94 SWITCHING > Multicast > MVR > MVR > Add/Edit

LABEL	DESCRIPTION
Active	Enable the switch button 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 except [?], [], ['], ["], or [,]) 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.
Use this section to configure MVR settings on each port.	
Port	This field displays the port number on the Switch.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
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.

Table 94 SWITCHING > Multicast > MVR > MVR > Add/Edit (continued)

LABEL	DESCRIPTION
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.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

33.7 MVR Group Setup

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

Use this screen to view and configure MVR IP multicast group settings. Click **SWITCHING > Multicast > MVR > Group Setup** to access this screen.

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

Figure 145 SWITCHING > Multicast > MVR > Group Setup

☐	MVLAN	Group Name	Start Address	End Address
☐	5			
☐		Group1	224.0.0.0	224.0.0.0
☐		Group2	ff02::1	ff02::1
☐	6			
☐		Group3	ff02::2	ff02::2

The following table describes the labels in this screen.

Table 95 SWITCHING > Multicast > MVR > Group Setup

LABEL	DESCRIPTION
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.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.

Table 95 SWITCHING > Multicast > MVR > Group Setup (continued)

LABEL	DESCRIPTION
Add/Edit	Click Add/Edit to add a new multicast group or edit a selected one.
Delete	Select the group entries that you want to remove, then click Delete to delete the selected multicast groups. If you delete a multicast VLAN, all multicast groups in this VLAN will also be removed.

33.7.1 Add/Edit MVR Group

Use this screen to configure MVR IP multicast group addresses. To access this screen, click the **Add/Edit** button or select an entry from the list and click the **Add/Edit** button.

Figure 146 SWITCHING > Multicast > MVR > Group Setup > Add/Edit

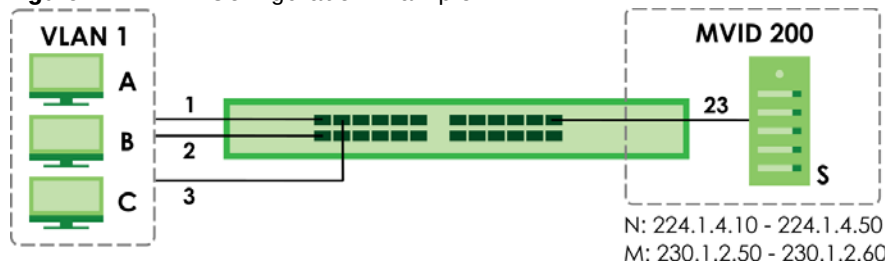
The following table describes the labels in this screen.

Table 96 SWITCHING > Multicast > MVR > Group Setup > Add/Edit

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. You can enter up to 32 printable ASCII characters except [?], [], ['], ["], or [,].
Start Address	Enter the starting IP multicast address of the multicast group in dotted decimal notation.
End Address	Enter the ending IP multicast address of the multicast group in dotted decimal notation. Enter the same IP address as the Start Address field if you want to configure only one IP address for a multicast group.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

33.7.2 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 **23** belongs to the multicast group with **VID 200 (MVID 200)** to receive multicast traffic (the News (**N**) and Movie (**M**) channels) from the remote streaming media server (**S**). Computers **A**, **B** and **C** in **VLAN 1** are able to receive the traffic.

Figure 147 MVR Configuration Example

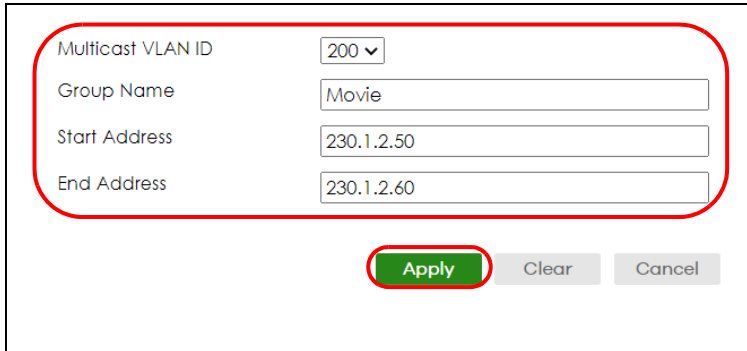
To configure the MVR settings on the Switch, click the **Add/Edit** button in the **SWITCHING > Multicast > MVR > MVR** screen. Create a multicast VLAN and set the receiver and source ports.

Figure 148 MVR Configuration Example

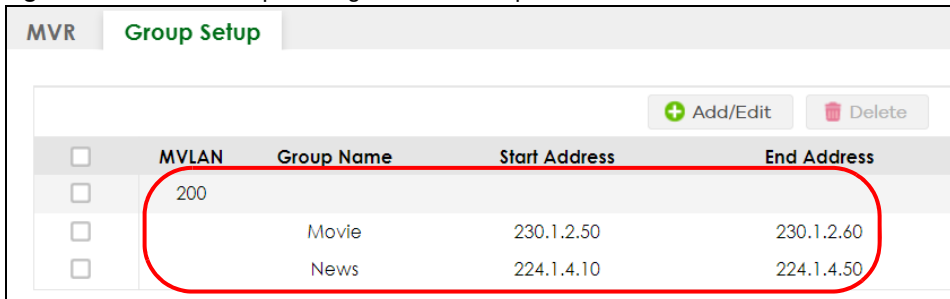
The screenshot shows the MVR configuration interface. At the top, there are several settings: 'Active' is a toggle switch set to 'ON'; 'Group Name' is a text field containing 'Premium'; 'Multicast VLAN ID' is a text field containing '200'; '802.1p Priority' is a dropdown menu set to '0'; and 'Mode' has two radio buttons, 'Dynamic' (selected) and 'Compatible'. Below these settings is a table with columns: 'Port', 'Source Port', 'Receiver Port', 'None', and 'Tagging'. The table has 8 rows, numbered 1 to 8. In row 7, the 'Source Port' and 'Receiver Port' are both set to 7, and the 'Tagging' checkbox is checked. A red oval highlights the configuration for ports 1, 2, and 3, and another red oval highlights the configuration for port 7. At the bottom right, there are three buttons: 'Apply' (highlighted with a red oval), 'Clear', and 'Cancel'.

Port	Source Port	Receiver Port	None	Tagging
*		Receiver Port ▼		☐
1	☐	☒	☐	☐
2	☐	☒	☐	☐
3	☐	☒	☐	☐
4	☐	☐	☒	☐
5	☐	☐	☒	☐
6	☐	☐	☒	☐
7	☒	☐	☐	☒
8	☐	☒	☐	☐

To set the Switch to forward the multicast group traffic to the subscribers, click **Add/Edit** in the **SWITCHING > Multicast > MVR > Group Setup** screen and configure multicast group settings. The following figure shows an example where two IPv4 multicast groups (**News** and **Movie**) are configured for the multicast VLAN 200.

Figure 149 MVR Group Configuration Example – Add

A screenshot of the 'Add' configuration page for an MVR group. The page contains four input fields: 'Multicast VLAN ID' with a dropdown menu showing '200', 'Group Name' with a text box containing 'Movie', 'Start Address' with a text box containing '230.1.2.50', and 'End Address' with a text box containing '230.1.2.60'. These fields are enclosed in a red rounded rectangle. Below the fields are three buttons: 'Apply' (highlighted with a red rounded rectangle), 'Clear', and 'Cancel'.

Figure 150 MVR Group Configuration Example – View

A screenshot of the 'View' configuration page for an MVR group. The page has two tabs: 'MVR' and 'Group Setup' (which is active). Below the tabs is a table with columns: 'MVLAN', 'Group Name', 'Start Address', and 'End Address'. The table contains three rows: a header row, a row with '200' in the 'MVLAN' column, and a row with 'Movie' in the 'Group Name' column. The 'Start Address' and 'End Address' for the 'Movie' group are '230.1.2.50' and '230.1.2.60' respectively. The table is enclosed in a red rounded rectangle. Above the table are two buttons: '+ Add/Edit' and 'Delete'.

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

CHAPTER 34

Static Multicast Forwarding

34.1 Static Multicast Forwarding Overview

This chapter discusses how to configure static multicast forwarding rules based on multicast MAC addresses or multicast IPv4 addresses.

Use these screens to configure static multicast address forwarding by defining the ports and VLANs that multicast traffic can pass through the Switch. If a subscriber is on a different port or VLAN, then the subscriber will not get the multicast.

34.1.1 What You Can Do

Use the **Static Multicast Forwarding By MAC** screen ([Section 34.2 on page 232](#)) to configure rules to forward specific multicast frames, such as streaming or control frames, to specific ports.

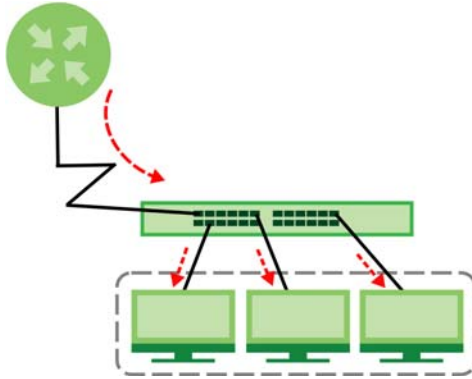
34.1.2 What You Need To Know

A multicast MAC address or multicast IP address is the MAC address or IP address of a multicast group, and not a receiving device.

A static multicast address is a multicast MAC address or multicast IPv4 address that has been manually entered in the multicast table. This identifies the destination of the multicast content. Multicast IPv4 addresses use the Class D IP addresses range 224.0.0.0 to 239.255.255.255. Multicast MAC addresses have a “1” as the last binary bit of the first octet pair (for example, 01:00:5e:00:00:0A). Static multicast addresses do not age out. See [IP Multicast Addresses on page 213](#) for more information on IP multicast addresses.

Note: Static (manual) 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 cannot forward to specific ports unless you configure static (manual) multicast entries. The Switch will either flood the multicast frames to all ports (default) or drop them. [Figure 151 on page 232](#) shows such unknown multicast frames flooded to all ports. With static multicast forwarding, you can forward these multicasts to ports within a VLAN group.

Figure 151 No Multicast Forwarding

34.2 Static Multicast Forwarding By MAC

Use this screen to view and configure static multicast MAC addresses for ports to receive the multicast stream. Click **SWITCHING > Multicast > Static Multicast Forwarding By MAC** to display the screen as shown next.

Figure 152 SWITCHING > Multicast > Static Multicast Forwarding By MAC

The following table describes the labels in this screen.

Table 97 SWITCHING > Multicast > Static Multicast Forwarding By MAC

LABEL	DESCRIPTION
Index	This is the index number of the static multicast MAC address rule.
Active	This field displays whether a static multicast MAC address forwarding rule is active or not. You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for a static multicast MAC address-forwarding rule.
MAC Address	This field displays the multicast MAC address that identifies a multicast group.
VID	This field displays the ID number of a VLAN group to which frames containing the specified multicast MAC address will be forwarded.
Port	This field displays the ports within an identified VLAN group to which frames containing the specified multicast MAC address will be forwarded.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new rule or edit a selected one.
Delete	Click Delete to remove the selected rules.

34.2.1 Add/Edit Static Multicast Forwarding By MAC

Use this screen to add a static multicast MAC address rule for ports to receive the multicast stream.

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SWITCHING > Multicast > Static Multicast Forwarding By MAC** to display this screen.

Figure 153 SWITCHING > Multicast > Static Multicast Forwarding By MAC > Add/Edit

The screenshot shows a configuration form with the following elements:

- Active:** A toggle switch currently set to OFF.
- Name:** A text input field.
- MAC Address:** A text input field.
- VID:** A small text input field.
- Port:** A text input field.
- Buttons:** 'Apply' (green), 'Clear' (grey), and 'Cancel' (grey) at the bottom.

The following table describes the labels in this screen

Table 98 SWITCHING > Multicast > Static Multicast Forwarding By MAC > Add/Edit

LABEL	DESCRIPTION
Active	Enable the switch button to activate your rule. You may temporarily deactivate a rule without deleting it by disabling the switch.
Name	Enter a descriptive name (up to 32 printable ASCII characters except [?], [], ['], ["], or [,]) 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 in hexadecimal, so 01:00:5e:00:00:0A and 01:00:5e:00:00:27 are valid multicast MAC addresses.
VID	You can forward frames with matching destination multicast MAC address to ports within a VLAN group. Enter the ID that identifies the VLAN group here. If you do NOT have a specific target VLAN, enter 1.
Port	Enter the ports where frames with destination multicast MAC address that matched the entry above are forwarded. You can enter multiple ports separated by (no space) comma (,) or hyphen (-). For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

CHAPTER 35

Private VLAN

35.1 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.

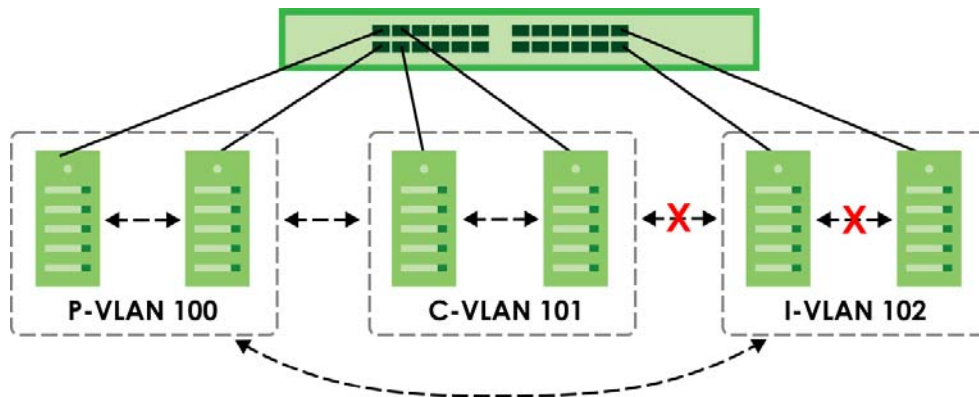


Table 99 PVLAN Graphic Key

LABEL	DESCRIPTION
P-VLAN 100	Primary private VLAN
C-VLAN 101	Community private VLAN
I-VLAN 102	Isolated private VLAN

Tagged Private VLANs can span switches but trunking ports must be VLAN-trunking ports – see **SWITCHING > VLAN > VLAN Setup > VLAN Port Setup**.

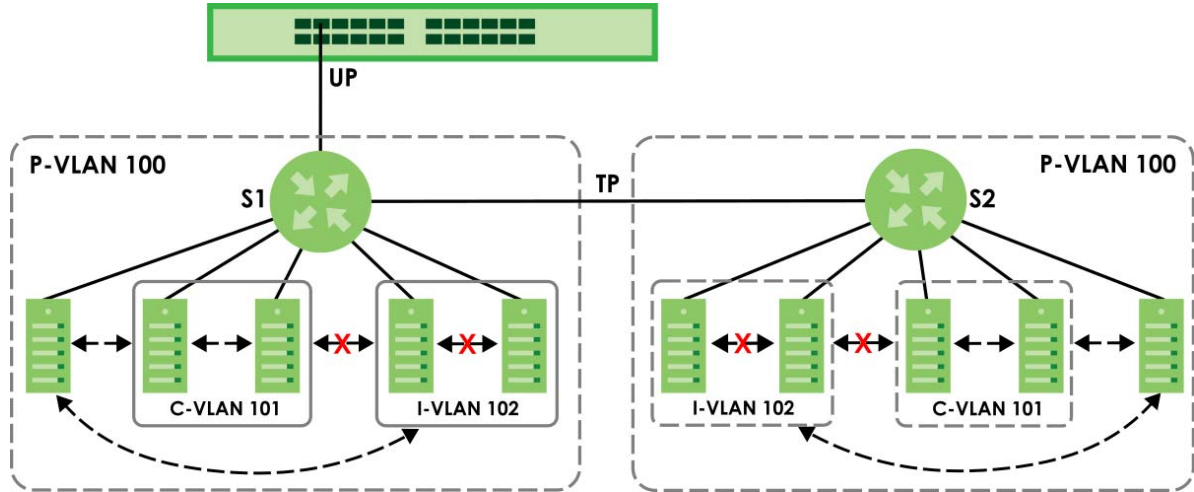


Table 100 Spanning PVLAN Graphic Key

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 **SWITCHING > VLAN > VLAN Setup > VLAN Port Setup** has a higher priority than private VLAN settings, so promiscuous ports with **Isolation** in **SWITCHING > VLAN > VLAN Setup > VLAN Port Setup** enabled will not be able to communicate with each other.

35.1.1 Private VLAN Configuration

You must go to the **SWITCHING > VLAN > VLAN Setup > Static VLAN** screen first to create VLAN IDs for **Primary**, **Isolated** or **Community** VLANs.

Click **SWITCHING > Private VLAN** to display the following screen.

Figure 154 SWITCHING > Private VLAN

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	☐

Apply Cancel

The following table describes the labels in this screen.

Table 101 SWITCHING > Private VLAN

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

Table 101 SWITCHING > Private VLAN (continued)

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

CHAPTER 36

Differentiated Services

36.1 DiffServ Overview

This chapter shows you how to configure Differentiated Services (DiffServ) on the Switch.

Quality of Service (QoS) is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

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

36.1.1 What You Can Do

- Use the **Diffserv** screen ([Section 36.1 on page 238](#)) to activate DiffServ to apply marking rules or IEEE 802.1p priority mapping on the Switch.
- Use the **DSCP Setting** screen ([Section 36.3.1 on page 241](#)) to change the DSCP-IEEE 802.1p mapping.

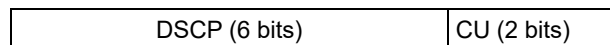
36.1.2 What You Need to Know

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

DSCP and Per-Hop Behavior

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

Figure 155 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.

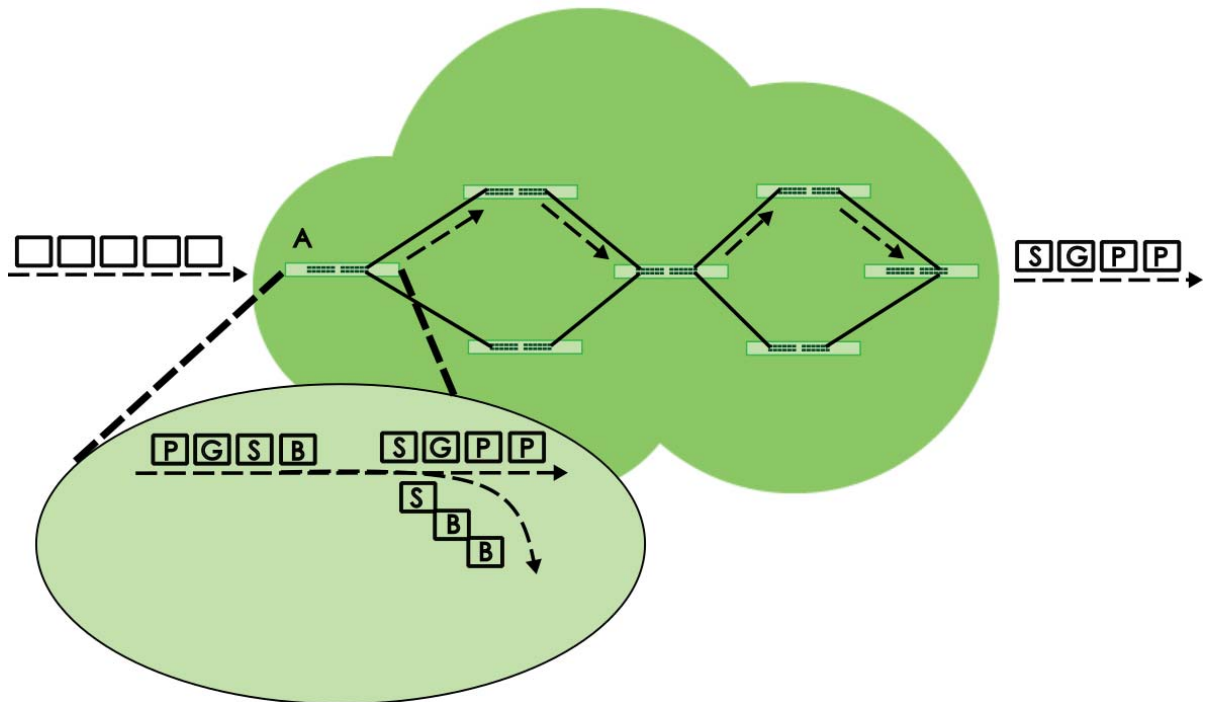
The DSCP value determines the PHB (Per-Hop Behavior), that each packet gets as it is forwarded across the DiffServ network. Based on the marking rule different kinds of traffic can be marked for different

priorities of forwarding. Resources can then be allocated according to the DSCP values and the configured policies.

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 156) in a DiffServ network classifies (marks with a DSCP value) the incoming packets into different traffic flows (**Platinum, Gold, Silver, Bronze**) based on the configured marking rules. A network administrator can then apply various traffic policies to the traffic flows. An example traffic policy, is to give higher drop precedence to one traffic flow over others. In our example, packets in the **Bronze** traffic flow are more likely to be dropped when congestion occurs than the packets in the **Platinum** traffic flow as they move across the DiffServ network.

Figure 156 DiffServ Network



36.2 Activate DiffServ

Activate DiffServ to apply marking rules or IEEE 802.1p priority mapping on the selected ports.

Click **SWITCHING** > **QoS** > **Diffserv** to display the screen as shown.

Figure 157 SWITCHING > QoS > Diffserv

Diffserv DSCP Setting

Active ☐ OFF

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

Apply Cancel

The following table describes the labels in this screen.

Table 102 SWITCHING > QoS > Diffserv

LABEL	DESCRIPTION
Active	Enable the switch button to enable Diffserv on the Switch.
Port	This field displays the index number of a port on the Switch.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Active	Select Active to enable Diffserv on the port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

36.3 DSCP-to-IEEE 802.1p Priority Settings

You can configure the DSCP to IEEE 802.1p mapping to allow the Switch to prioritize all traffic based on the incoming DSCP value according to the DiffServ to IEEE 802.1p mapping table.

The following table shows the default DSCP-to-IEEE802.1p mapping.

Table 103 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

36.3.1 Configure DSCP Settings

To change the DSCP-IEEE 802.1p mapping click **SWITCHING > QoS > Diffserv > DSCP Setting** to display the screen as shown next.

Figure 158 SWITCHING > QoS > 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 104 SWITCHING > QoS > Diffserv > DSCP Setting

LABEL	DESCRIPTION
0 ... 63	This is the DSCP classification identification number. To set the IEEE 802.1p priority mapping, select the priority level from the drop-down list box.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 37

Queuing Method

37.1 Queuing Method Overview

This section introduces the queuing methods supported.

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

37.1.1 What You Can Do

Use the **Queuing Method** screen ([Section 37.2 on page 243](#)) to set priorities for the queues of the Switch. This distributes bandwidth across the different traffic queues.

37.1.2 What You Need to Know

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

Strictly Priority Queuing

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

Weighted Fair Queuing

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

Weighted Round Robin Scheduling (WRR)

Round Robin Scheduling services queues on a rotating basis and is activated only when a port has more traffic than it can handle. A queue is 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.

37.2 Configure Queuing

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

Click **SWITCHING > QoS > Queuing Method** to display the screen as shown below.

Figure 159 SWITCHING > QoS > Queuing Method

Port	Method	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Hybrid-SPQ Lowest-Queue
*	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 ▼

The following table describes the labels in this screen.

Table 105 SWITCHING > QoS > Queuing Method

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

Table 105 SWITCHING > QoS > Queuing Method (continued)

LABEL	DESCRIPTION
Method	Select SPQ (Strictly Priority Queuing), WFQ (Weighted Fair Queuing) or WRR (Weighted Round Robin). Strictly Priority Queuing services queues based on priority only. When the highest priority queue empties, traffic on the next highest-priority queue begins. Q7 has the highest priority and Q0 the lowest. Weighted Fair Queuing is used to guarantee each queue's minimum bandwidth based on their bandwidth portion (weight) (the number you configure in the Weight field). Queues with larger weights get more guaranteed bandwidth than queues with smaller weights. Weighted Round Robin Scheduling services queues on a rotating basis based on their queue weight (the number you configure in the queue Weight field). Queues with larger weights get more service than queues with smaller weights.
Weight	When you select WFQ or WRR , enter the queue weight here. Bandwidth is divided across the different traffic queues according to their weights.
Hybrid-SPQ Lowest-Queue	This field is applicable only when you select WFQ or WRR. Select a queue (Q0 to Q7) to have the Switch use SPQ to service the subsequent queues after and including the specified queue for the port. For example, if you select Q5, the Switch services traffic on Q5, Q6 and Q7 using SPQ. Select None to always use WFQ or WRR for the port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 38

Priority Queue

38.1 Priority Queue Overview

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 this screen to configure the priority level-to-physical queue mapping. The Switch has eight physical queues that you can map to the eight priority levels.

On the Switch, traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested.

38.1.1 What You Can Do

Use the **Priority Queue** screen ([Section 38.2 on page 245](#)) to configure the priority level-to-physical queue mapping.

38.2 Assign Priority Queue

Use this screen to assign priority level to each queue.

Click **SWITCHING > QoS > Priority Queue** to open this screen.

Figure 160 SWITCHING > QoS > Priority Queue

Priority Queue Assignment	
Priority7	7
Priority6	6
Priority5	5
Priority4	4
Priority3	3
Priority2	1
Priority1	0
Priority0	2

Apply Cancel

The following table describes the related labels in this screen.

Table 106 SWITCHING > QoS > Priority Queue

LABEL	DESCRIPTION
Priority Queue Assignment The following descriptions are based on the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p). To map a priority level to a physical queue, select a physical queue from the drop-down menu on the right.	
Priority 7	Typically used for network control traffic such as router configuration messages.
Priority 6	Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay).
Priority 5	Typically used for video that consumes high bandwidth and is sensitive to jitter.
Priority 4	Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions.
Priority 3	Typically used for “excellent effort” or better than best effort and would include important business traffic that can tolerate some delay.
Priority 2	This is for “spare bandwidth”.
Priority 1	This is typically used for non-critical “background” traffic such as bulk transfers that are allowed but that should not affect other applications and users.
Priority 0	Typically used for best-effort traffic.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields.

CHAPTER 39

sFlow

This chapter shows you how to configure sFlow to have the Switch monitor traffic in a network and send information to an sFlow collector for analysis.

39.1 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 161 sFlow Application



39.2 sFlow Port Configuration

Click **SWITCHING** > **sFlow** in the navigation panel to display the screen as shown.

Figure 162 SWITCHING > sFlow

Port	Active	Sample-rate	Poll-interval	Collector Address
*	☐			
1	☐	32768	120	
2	☐	32768	120	
3	☐	32768	120	
4	☐	32768	120	
5	☐	32768	120	
6	☐	32768	120	
7	☐	32768	120	

The following table describes the labels in this screen.

Table 107 SWITCHING > sFlow

LABEL	DESCRIPTION
Active	Enable the switch button to enable the sFlow agent on the Switch.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this to 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 SWITCHING > 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.

Table 107 SWITCHING > sFlow (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.

39.3 sFlow Collector Configuration

Click **SWITCHING > sFlow > Collector** to display the screen as shown. You may want to configure more than one collector if the traffic load to be monitored is more than one collector can manage.

Note: You can configure up to four sFlow collectors in this screen.

Figure 163 SWITCHING > sFlow > Collector

The following table describes the labels in this screen.

Table 108 SWITCHING > sFlow > Collector

LABEL	DESCRIPTION
Index	This field displays the index number of this entry.
Collector Address	This field displays IP address of the sFlow collector.
UDP Port	This field displays port number the Switch uses to send sFlow datagram to the collector.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new entry or edit a selected one.
Delete	Click Delete to remove the selected entries.

39.3.1 Add/Edit sFlow Collector

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SWITCHING > sFlow > Collector** screen to display this screen.

Figure 164 SWITCHING > sFlow > Collector > Add/Edit

The following table describes the labels in this screen.

Table 109 SWITCHING > sFlow > Collector > Add/Edit

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.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

CHAPTER 40

Spanning Tree Protocol

40.1 Spanning Tree Protocol Overview

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

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

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

40.1.1 What You Can Do

- Use the **Spanning Tree Protocol Status** screen ([Section 40.2 on page 254](#)) to view the STP status in the different STP modes (RSTP, MRSTP or MSTP) you can configure on the Switch.
- Use the **Spanning Tree Setup** screen ([Section 40.3 on page 254](#)) to activate one of the STP modes on the Switch.
- Use the **Rapid Spanning Tree Protocol Status** screen ([Section 40.4 on page 256](#)) to view the RSTP status.
- Use the **Rapid Spanning Tree Protocol** screen ([Section 40.5 on page 258](#)) to configure RSTP settings.
- Use the **Multiple Rapid Spanning Tree Protocol Status** screen ([Section 40.6 on page 260](#)) to view the MRSTP status.
- Use the **Multiple Rapid Spanning Tree Protocol** screen ([Section 40.7 on page 262](#)) to configure MRSTP.
- Use the **Multiple Spanning Tree Protocol Status** screen ([Section 40.8 on page 265](#)) to view the MSTP status.
- Use the **Multiple Spanning Tree Protocol** screen ([Section 40.9 on page 267](#)) to configure MSTP.
- Use the **Multiple Spanning Tree Protocol Port Setup** screen ([Section 40.10 on page 270](#)) to configure MSTP ports.

40.1.2 What You Need to Know

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

(Rapid) Spanning Tree Protocol

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

The Switch uses IEEE 802.1w RSTP (Rapid Spanning Tree Protocol) that allows faster convergence of the

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

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

STP Terminology

The root bridge is the base of the spanning tree.

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

Table 110 STP Path Costs

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

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

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

How STP Works

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

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

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

STP Port States

STP assigns five port states to eliminate packet looping. A bridge port is not allowed to go directly from

blocking state to forwarding state so as to eliminate transient loops.

Table 111 STP Port States

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

Multiple RSTP

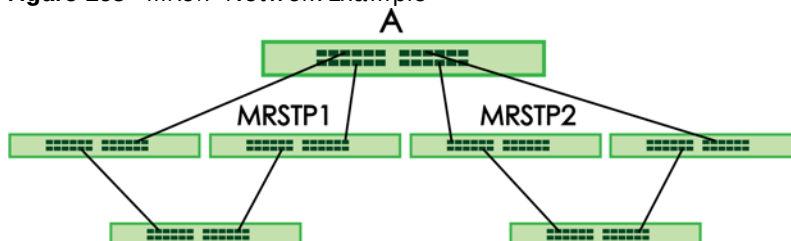
MRSTP (Multiple RSTP) is Zyxel's proprietary feature that is compatible with RSTP and STP. With MRSTP, you can have more than one spanning tree on your Switch and assign ports to each tree. Each spanning tree operates independently with its own bridge information.

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

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

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

Figure 165 MRSTP Network Example



Multiple STP

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

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

40.2 Spanning Tree Protocol Status

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

Figure 166 SWITCHING > Spanning Tree Protocol > Spanning Tree Protocol Status

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

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 ([Section 40.4 on page 256](#), [Section 40.6 on page 260](#), and [Section 40.8 on page 265](#)) that follows the configuration section for each STP mode. Use the **SWITCHING > Spanning Tree Protocol > Spanning Tree Setup** screen to activate one of the STP standards on the Switch.

40.3 Spanning Tree Setup

There are three **Auto path-cost Modes** (see [Table 115 on page 256](#)). Choose the **Auto Path-cost Mode** according to the device average link speeds in the STP network.

The path cost values are described in the following tables.

The Switch defines the following **Short** mode path costs.

Table 112 Auto Path Cost Mode: Short

LINK SPEED	AUTO PATH COST VALUE
Up to 1 Gbps	4
Up to 10 Gbps	2

Table 112 Auto Path Cost Mode: Short (continued)

LINK SPEED	AUTO PATH COST VALUE
Up to 25 Gbps	1
Up to 100 Gbps	1

The Switch defines the following **Long** mode path costs.

Table 113 Auto Path Cost Mode: Long

LINK SPEED	AUTO PATH COST VALUE
Up to 1 Gbps	20000
Up to 10 Gbps	2000
Up to 25 Gbps	800
Up to 100 Gbps	200

If you do not configure the auto path cost values for **User-defined** mode, the Switch uses the following default values.

Table 114 Auto Path Cost Mode: User-defined

LINK SPEED	AUTO PATH COST VALUE
Up to 1 Gbps	20000
Up to 10 Gbps	2000
Up to 25 Gbps	800
Up to 100 Gbps	200

Use the this screen to activate one of the STP modes on the Switch. Click **SWITCHING > Spanning Tree Protocol > Spanning Tree Setup** to display the screen as shown.

Figure 167 SWITCHING > Spanning Tree Protocol > Spanning Tree Setup

Spanning Tree Setup

Spanning Tree Mode

- ☒ Rapid Spanning Tree (RSTP)
- ☐ Multiple Rapid Spanning Tree (MRSTP)
- ☐ Multiple Spanning Tree (MSTP)

Auto Path-cost Mode

- ☐ Short
- ☒ Long
- ☐ User-defined:
 - 1G:
 - 10G:
 - 25G:
 - 100G:

Apply **Cancel**

The following table describes the labels in this screen.

Table 115 SWITCHING > Spanning Tree Protocol > Spanning Tree Setup

LABEL	DESCRIPTION
Spanning Tree Mode	You can activate one of the STP modes on the Switch. Select Rapid Spanning Tree (RSTP) , Multiple Rapid Spanning Tree (MRSTP) or Multiple Spanning Tree (MSTP) .
Auto Path-cost Mode	Auto Path-cost Mode allows you to have the Switch automatically set the path cost for each port according to their link speed. The Switch uses the path costs to determine the best path to the root bridge in a spanning tree. There are three Auto Path-cost Modes that supports different path cost lengths: • Short (16-bit) • Long (32-bit) • User-defined (32-bit). The auto path cost values of each mode are described in Section 40.3 on page 254. Note: It is recommended to use the same Auto Path-cost Mode on all switches within the spanning tree network system. To use the auto path-cost feature, select the Auto Path-cost mode (Short, Long, User-defined), set a port's Path Cost (in the SWITCHING > Spanning Tree Protocol > RSTP and MSTP screens) to "0". The Switch will automatically set the port's path cost to the auto path cost value defined by the Auto Path-cost Mode you select.
Short	Select this mode if you want to use the 16-bit auto path cost values the Switch defines.
Long	Select this mode if you want to use the 32-bit auto path cost values the Switch defines.
User-defined	Select this mode to manually set the auto path costs for each link speed. Enter the path cost value for each link speed. The range is from 1 – 200000000. It is recommended to assign this value according to link speeds. The slower the speed, the higher the cost.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

40.4 Rapid Spanning Tree Protocol Status

The Spanning Tree Protocol status screen changes depending on what standard you choose to implement on your network. Click **SWITCHING > Spanning Tree Protocol > Spanning Tree Protocol Status** in the navigation panel to display the status screen as shown next. See [Section 40.1 on page 251](#) for more information on RSTP.

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

Figure 168 SWITCHING > Spanning Tree Protocol > Spanning Tree Protocol Status: RSTP

Spanning Tree Protocol Status						
Spanning Tree Protocol: RSTP						
	Root Bridge			Our Bridge		
Bridge ID	6666-bc6666cbc666			6666-bc6666cbc666		
Hello Time (seconds)	2			2		
Max Age (seconds)	20			20		
Forwarding Delay (seconds)	15			15		
Cost to Bridge	0					
Port ID	0x0000					
Topology Changed Times	2					
Time Since Last Change	0:01:33					
Port	Port State	Port Role	Designated Bridge ID	Designated Port ID	Designated Cost	Root Guard State
1	DISCARDING	Disabled	0000-000000000000	0x0000	0	Forwarding
2	DISCARDING	Disabled	0000-000000000000	0x0000	0	Forwarding
3	DISCARDING	Disabled	0000-000000000000	0x0000	0	Forwarding
4	DISCARDING	Disabled	0000-000000000000	0x0000	0	Forwarding
5	DISCARDING	Disabled	0000-000000000000	0x0000	0	Forwarding
6	FORWARDING	Designated	6666-bc6666cbc666	0x8012	0	Forwarding
7	DISCARDING	Disabled	0000-000000000000	0x0000	0	Forwarding
8	FORWARDING	Designated	6666-bc6666cbc666	0x8016	0	Forwarding

The following table describes the labels in this screen.

Table 116 SWITCHING > Spanning Tree Protocol > Spanning Tree Protocol Status: RSTP

LABEL	DESCRIPTION
Bridge	Root Bridge 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 Bridge and Our Bridge if the Switch is the root switch.
Hello Time (seconds)	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 (seconds)	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (seconds)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding). Note: The listening state does NOT exist in RSTP.
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.
Port	This field displays the number of the port on the Switch.

Table 116 SWITCHING > Spanning Tree Protocol > Spanning Tree Protocol Status: RSTP (continued)

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

40.5 Configure Rapid Spanning Tree Protocol

Use this screen to configure RSTP settings, see [Section 40.1 on page 251](#) for more information on RSTP. Click **SWITCHING > Spanning Tree Protocol > RSTP** in the navigation panel to display the screen as shown.

Figure 169 SWITCHING > Spanning Tree Protocol > RSTP

Rapid Spanning Tree Protocol

Active ☐ OFF

Bridge Priority ▼

Hello Time seconds

MAX Age seconds

Forwarding Delay seconds

Port	Active	Edge	Root Guard	Priority	Path Cost
*	☐	☐	☐		
1	☐	☐	☐	128	2
2	☐	☐	☐	128	2
3	☐	☐	☐	128	2
4	☐	☐	☐	128	2
5	☐	☐	☐	128	2
6	☐	☐	☐	128	2
7	☐	☐	☐	128	2

The following table describes the labels in this screen.

Table 117 SWITCHING > Spanning Tree Protocol > RSTP

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

Table 117 SWITCHING > Spanning Tree Protocol > RSTP (continued)

LABEL	DESCRIPTION
Forwarding Delay	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every Switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to activate RSTP on this port.
Edge	Select this checkbox to configure a port as an edge port when it is directly attached to a computer. An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).
Root Guard	Select this checkbox to enable root guard on this port in order to prevent the switches attached to the port from becoming the root bridge. With root guard enabled, a port is blocked when the Switch receives a superior BPDU on it. The Switch allows traffic to pass through this port again when the switch connected to the port stops to send superior BPDUs.
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost. Note: Set the value to 0 to use the auto path cost you set in the SWITCHING > Spanning Tree Protocol > Spanning Tree Setup screen.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

40.6 Multiple Rapid Spanning Tree Protocol

Click **SWITCHING > Spanning Tree Protocol > Spanning Tree Protocol Status** in the navigation panel to display the status screen as shown next. See [Section 40.6 on page 260](#) for more information on MRSTP.

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

Figure 170 SWITCHING > Spanning Tree Protocol > Spanning Tree Protocol Status: MRSTP

Spanning Tree Protocol Status						
Spanning Tree Protocol: MRSTP						
Tree 1 ▼						
	Root Bridge			Our Bridge		
Bridge ID	6666-bc6666cbc666			6666-bc6666cbc666		
Hello Time (seconds)	2			2		
Max Age (seconds)	20			20		
Forwarding Delay (seconds)	15			15		
Cost to Bridge	0					
Port ID	0x0000					
Topology Changed Times	4					
Time Since Last Change	0:02:12					
Port	Port State	Port Role	Designated Bridge ID	Designated Port ID	Designated Cost	Root Guard State
1	DISCARDING	Disabled	0000-000000000000	0x0000	0	Forwarding
2	FORWARDING	Designated	6666-bc6666cbc666	0x8012	0	Forwarding
5	DISCARDING	Disabled	0000-000000000000	0x0000	0	Forwarding
6	FORWARDING	Designated	6666-bc6666cbc666	0x8016	0	Forwarding
7	DISCARDING	Disabled	0000-000000000000	0x0000	0	Forwarding

The following table describes the labels in this screen.

Table 118 SWITCHING > Spanning Tree Protocol > Spanning Tree Protocol Status: MRSTP

LABEL	DESCRIPTION
Tree	Select which STP tree configuration you want to view.
Bridge	Root Bridge 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 Bridge and Our Bridge if the Switch is the root switch.
Hello Time (seconds)	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 (seconds)	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (seconds)	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.

Table 118 SWITCHING > Spanning Tree Protocol > Spanning Tree Protocol Status: MRSTP (continued)

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

40.7 Configure Multiple Rapid Spanning Tree Protocol

To configure MRSTP, click **SWITCHING > Spanning Tree Protocol > MRSTP** in the navigation panel to display the screen as shown.

Figure 171 SWITCHING > Spanning Tree Protocol > MRSTP

Multiple Rapid Spanning Tree Protocol

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

Port	Active	Edge	Root Guard	Priority	Path Cost	Tree
*	☐	☐	☐			1 ▼
1	☐	☐	☐	128	2	1 ▼
2	☐	☐	☐	128	2	1 ▼
3	☐	☐	☐	128	2	1 ▼
4	☐	☐	☐	128	2	1 ▼
5	☐	☐	☐	128	2	1 ▼
6	☐	☐	☐	128	2	1 ▼
7	☐	☐	☐	128	2	1 ▼

The following table describes the labels in this screen.

Table 119 SWITCHING > Spanning Tree Protocol > MRSTP

LABEL	DESCRIPTION
Tree	This is the index number of the STP trees.
Active	Select this checkbox to activate an STP tree. Clear this checkbox to disable an STP tree. Note: You must also activate Multiple Rapid Spanning Tree (MRSTP) in the SWITCHING > Spanning Tree Protocol > Spanning Tree Setup 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.

Table 119 SWITCHING > Spanning Tree Protocol > MRSTP (continued)

LABEL	DESCRIPTION
Max Age	This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to activate STP on this port.
Edge	Select this checkbox to configure a port as an edge port when it is directly attached to a computer. An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).
Root Guard	Select this checkbox to enable root guard on this port in order to prevent the switch(es) attached to the port from becoming the root bridge. With root guard enabled, a port is blocked when the Switch receives a superior BPDU on it. The Switch allows traffic to pass through this port again when the switch connected to the port stops to send superior BPDUs.
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost. Note: Set the value to 0 to use the auto path cost you set in the SWITCHING > Spanning Tree Protocol > Spanning Tree Setup screen.
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.

40.8 Multiple Spanning Tree Protocol Status

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

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

Figure 172 SWITCHING > Spanning Tree Protocol > Spanning Tree Protocol Status: MSTP

Spanning Tree Protocol Status

Spanning Tree Protocol: MSTP

CST

	Root Bridge	Our Bridge
Bridge ID	6666-bc6666cbc666	6666-bc6666cbc666
Hello Time (seconds)	2	2
Max Age (seconds)	20	20
Forwarding Delay (seconds)	15	15
Cost to Bridge	0	0
Port ID	0x0000	0x0000
Configuration Name	bc6666cbc666	
Revision Number	0	
Configuration Digest	AC36177F50283CD4B83821D8AB26DE62	
Topology Changed Times	0	
Time Since Last Change	0:22:49	

Instance

Instance	VLAN
0	1-4094

MSTI 1

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

Port	Port State	Port Role	Designated Bridge ID	Designated Port ID	Designated Cost	Root Guard State

The following table describes the labels in this screen.

Table 120 SWITCHING > Spanning Tree Protocol > Spanning Tree Protocol Status: MSTP

LABEL	DESCRIPTION
CST	This section describes the Common Spanning Tree settings.
Bridge	Root Bridge 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 Bridge and Our Bridge if the Switch is the root switch.
Hello Time (seconds)	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 (seconds)	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (seconds)	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	
MSTI	Select the MST instance settings you want to view.
	Regional 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 Regional Root and Our Bridge if the Switch is the root switch.
Internal Cost	This is the path cost from the root port in this MST instance to the regional root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the MST instance.
Port	This field displays the number of the port on the Switch.
Port State	This field displays the port state in STP. • DISCARDING – The port does not forward or process received frames or learn MAC addresses, but still listens for BPDUs. • LEARNING – The port learns MAC addresses and processes BPDUs, but does not forward frames yet. • FORWARDING – The port is operating normally. It learns MAC addresses, processes BPDUs and forwards received frames.

Table 120 SWITCHING > Spanning Tree Protocol > Spanning Tree Protocol Status: MSTP (continued)

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

40.9 Configure Multiple Spanning Tree Protocol

To configure MSTP, click **SWITCHING > Spanning Tree Protocol > MSTP** in the navigation panel to display the screen as shown.

Figure 173 SWITCHING > Spanning Tree Protocol > MSTP > Multiple Spanning Tree Protocol

Multiple Spanning Tree Protocol **MSTP Port Setup**

Bridge

Active ☒ ON

Hello Time seconds

MAX Age seconds

Forwarding Delay seconds

Maximum Hops

Configuration Name

Revision Number

Apply **Cancel**

Instance

☒ Add/Edit ☒ Delete

☐	Instance	VLAN	Active Port
☐	0	1-4094	-

The following table describes the labels in this screen.

Table 121 SWITCHING > Spanning Tree Protocol > MSTP > Multiple Spanning Tree Protocol

LABEL	DESCRIPTION
Bridge	
Active	Enable the switch button to activate MSTP on the Switch. Disable the switch to disable MSTP on the Switch. Note: You must also activate Multiple Spanning Tree (MSTP) in the SWITCHING > Spanning Tree Protocol > Spanning Tree Setup screen to enable MSTP on the Switch.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Max Age	This is the maximum time (in seconds) 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 printable ASCII characters except [?], [], ['], ["], or [,]) of an MST region.

Table 121 SWITCHING > Spanning Tree Protocol > MSTP > Multiple Spanning Tree Protocol (continued)

LABEL	DESCRIPTION
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	This field displays the ID of an MST instance.
VLAN	This field displays the VID (or VID ranges) to which the MST instance is mapped.
Active Port	This field display the ports configured to participate in the MST instance.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new instance or edit a selected one.
Delete	Click Delete to remove the selected instances.

40.9.1 Add/Edit Multiple Spanning Tree

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SWITCHING > Spanning Tree Protocol > MSTP > Multiple Spanning Tree Protocol** screen to display this screen.

Figure 174 SWITCHING > Spanning Tree Protocol > MSTP > Multiple Spanning Tree Protocol > Add/Edit

Instance

Bridge Priority

VLAN List

Port	Active	Priority	Path Cost
*	☐		
1	☐	128	2
2	☐	128	2
3	☐	128	2
4	☐	128	2
5	☐	128	2
6	☐	128	2
7	☐	128	2

The following table describes the labels in this screen.

Table 122 SWITCHING > Spanning Tree Protocol > MSTP > Multiple Spanning Tree Protocol > Add/Edit

LABEL	DESCRIPTION
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 List	Enter the VLAN ID range. You can specify multiple VLAN ID range separated by (no space) comma (,) or hyphen ("-") for a range. For example, enter "1,3,5-7" for VLANs 1, 3, 5, 6, and 7.
Port	This field displays the port number. * means all ports.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox 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. Note: Set the value to 0 to use the auto path cost you set in the SWITCHING > Spanning Tree Protocol > Spanning Tree Setup 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.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

40.10 Multiple Spanning Tree Protocol Port Setup

Click **SWITCHING > Spanning Tree Protocol > MSTP > MSTP Port Setup** to display the screen as shown next.

Figure 175 SWITCHING > Spanning Tree Protocol > MSTP > MSTP Port Setup

Port	Edge	Root Guard
*	☐	☐
1	☐	☐
2	☐	☐
3	☐	☐
4	☐	☐
5	☐	☐
6	☐	☐
7	☐	☐

Apply Cancel

The following table describes the labels in this screen.

Table 123 SWITCHING > Spanning Tree Protocol > MSTP > MSTP Port Setup

LABEL	DESCRIPTION
Port	This field displays the port number. * means all ports.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Edge	Select this checkbox to configure a port as an edge port when it is directly attached to a computer. An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).
Root Guard	Select this checkbox to enable root guard on this port in order to prevent the switches attached to the port from becoming the root bridge. With root guard enabled, a port is blocked when the Switch receives a superior BPDU on it. The Switch allows traffic to pass through this port again when the switch connected to the port stops to send superior BPDUs.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

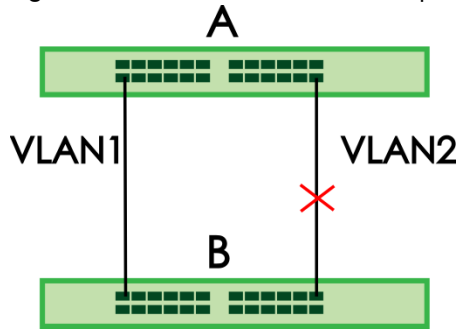
40.11 Technical Reference

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

40.11.1 MSTP Network Example

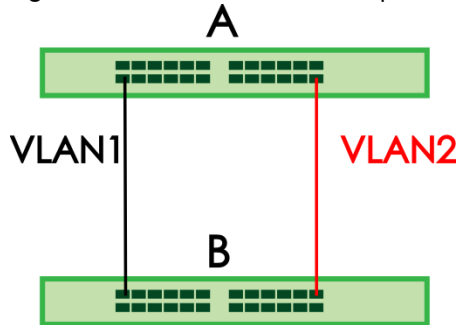
The following figure shows a network example where two VLANs are configured on the two switches. If the switches are using STP or RSTP, the link for VLAN 2 will be blocked as STP and RSTP allow only one link in the network and block the redundant link.

Figure 176 STP/RSTP Network Example



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

Figure 177 MSTP Network Example



40.11.2 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:

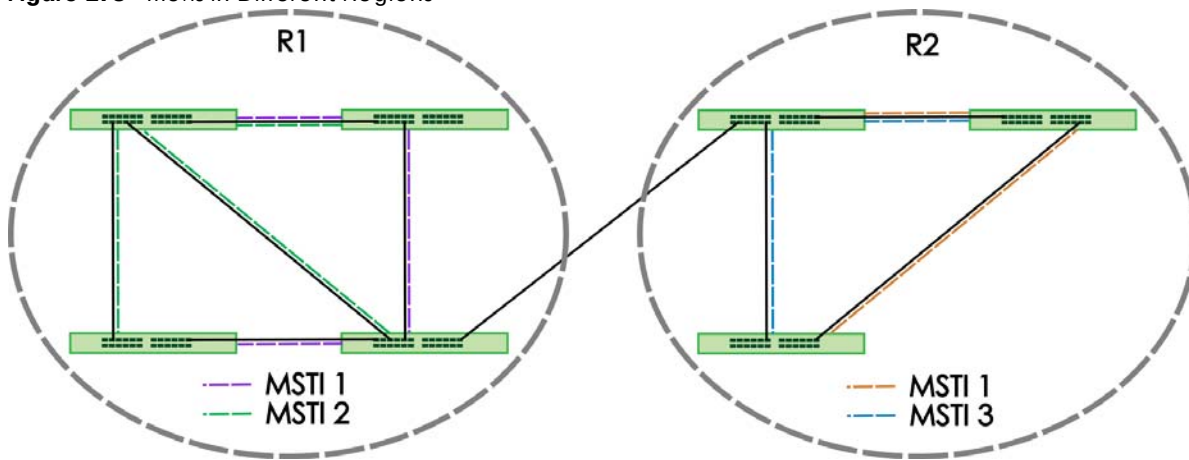
- Name of the MST region
- Revision level as the unique number for the MST region
- VLAN-to-MST Instance mapping

40.11.3 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. Therefore an MSTI does not span across MST regions.

The following figure shows an example where there are two MSTT regions. Regions 1 (**R1**) and 2 (**R2**) have two spanning tree instances. (**MSTI1**, **MSTI2** and **MSTI1**, **MSTI3**). The black connecting lines represent the physical connections.

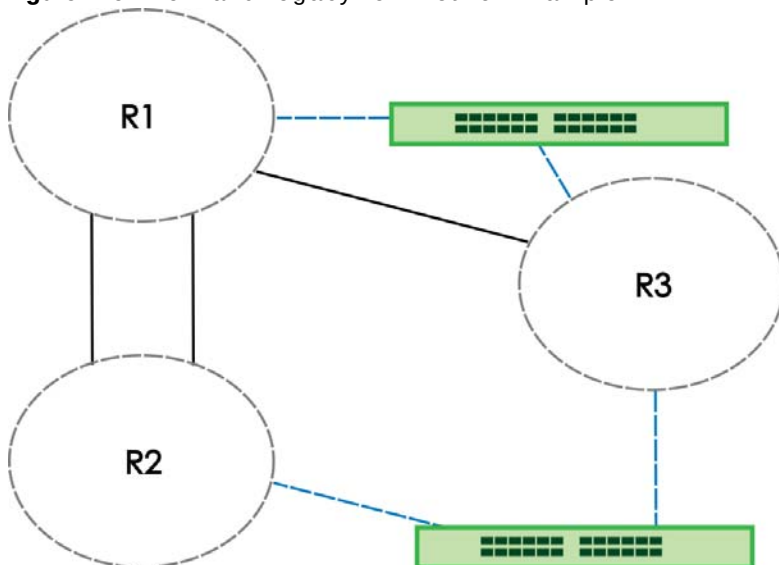
Figure 178 MSTIs in Different Regions



40.11.4 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 (**R1**, **R2**, **R3**) and single spanning tree devices. A network may contain multiple MST regions and other network segments running RSTP. In the figure below, the black connecting lines represent the physical connections. The green connecting lines represent RSTP on the link.

Figure 179 MSTP and Legacy RSTP Network Example



CHAPTER 41

Static MAC Filtering

41.1 Static MAC Filtering Overview

This chapter discusses MAC address port filtering.

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

41.1.1 What You Can Do

Use the **Static MAC Filtering** screen ([Section 41.2 on page 274](#)) to create rules for traffic going through the Switch.

41.2 Configure a Static MAC Filtering Rule

Use this screen to view and configure rules for traffic going through the Switch. Click **SWITCHING > Static MAC Filtering > Static MAC Filtering** in the navigation panel to display the screen as shown next.

Figure 180 SWITCHING > Static MAC Filtering > Static MAC Filtering

Index	Active	Name	MAC Address	VID	Action

The following table describes the related labels in this screen.

Table 124 SWITCHING > Static MAC Filtering > Static MAC Filtering

LABEL	DESCRIPTION
Index	This field displays the index number of the rule.
Active	This field displays whether the rule is activated or not.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
MAC Address	This field displays the source or destination MAC address with the VLAN identification number to which the MAC address belongs.
VID	This field displays the VLAN group identification number.
Action	This field displays Discard source , Discard destination , or Discard both depending on what you configured above.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.

Table 124 SWITCHING > Static MAC Filtering > Static MAC Filtering (continued)

LABEL	DESCRIPTION
Add/Edit	Click Add/Edit to add a new entry or edit a selected one.
Delete	Click Delete to remove the selected entries.

41.2.1 Add/Edit a Static MAC Filtering Rule

Use this screen to create or edit rules for traffic going through the Switch. Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SWITCHING > Static MAC Filtering > Static MAC Filtering** screen to display this screen.

Figure 181 SWITCHING > Static MAC Filtering > Static MAC Filtering > Add/Edit

The following table describes the related labels in this screen.

Table 125 SWITCHING > Static MAC Filtering > Static MAC Filtering > Add/Edit

LABEL	DESCRIPTION
Active	Enable the switch button to activate your rule. You may temporarily deactivate a rule without deleting it by de-selecting this checkbox.
Name	Enter a descriptive name (up to 32 printable ASCII characters excluding [?], [], ['], ["], or [,]) for this rule. This is for identification only.
Action	Select Discard source to drop the frames from the source MAC address (specified in the MAC field). The Switch can still send frames to the MAC address. Select Discard destination to drop the frames to the destination MAC address (specified in the MAC address). The Switch can still receive frames originating from the MAC address. Select Discard source and Discard destination to block traffic to or from the MAC address specified in the MAC field.
MAC	Enter a MAC address in valid MAC address format, that is, six hexadecimal character pairs.
VID	Enter the VLAN group identification number.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

CHAPTER 42

Static MAC Forwarding

42.1 Static MAC Forwarding Overview

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

Use these screens to configure static MAC address forwarding.

42.1.1 What You Can Do

Use the **Static MAC Forwarding** screen ([Section 42.2 on page 276](#)) to assign static MAC addresses for a port.

42.2 Configure Static MAC Forwarding

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

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

Figure 182 SWITCHING > Static MAC Forwarding > Static MAC Forwarding

	Index	Active	Name	MAC Address	VID	Port
☐	1	ON	Example	88:ac:88:ac:88:ac	1	17

The following table describes the labels in this screen.

Table 126 SWITCHING > Static MAC Forwarding > Static MAC Forwarding

LABEL	DESCRIPTION
Index	This is the index number of a static MAC address rule.
Active	This field displays whether this static MAC address forwarding rule is active. 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.

Table 126 SWITCHING > Static MAC Forwarding > Static MAC Forwarding (continued)

LABEL	DESCRIPTION
MAC Address	This field displays the MAC address that will be forwarded and the VLAN identification number to which the MAC address belongs.
VID	This field displays the ID number of the VLAN group.
Port	This field displays the port where the MAC address shown in the next field will be forwarded.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new rule or edit a selected one.
Delete	Click Delete to remove the selected rules.

42.2.1 Add/Edit Static MAC Forwarding Rules

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SWITCHING > Static MAC Forwarding > Static MAC Forwarding** screen to display this screen.

Figure 183 SWITCHING > Static MAC Forwarding > Static MAC Forwarding > Add/Edit

The following table describes the labels in this screen.

Table 127 SWITCHING > Static MAC Forwarding > Static MAC Forwarding > Add/Edit

LABEL	DESCRIPTION
Active	Enable the switch button to activate your rule. You may temporarily deactivate a rule without deleting it by disabling the switch.
Name	Enter a descriptive name for identification purposes for this static MAC address forwarding rule. You can enter up to 32 printable ASCII characters except [?], [], ['], ["], or [.].
MAC Address	Enter the MAC address in valid MAC address format, that is, six hexadecimal character pairs. Note: Static MAC addresses do NOT age out.
VID	Enter the VLAN identification number.
Port	Enter the port where the MAC address entered in the previous field will be automatically forwarded.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

CHAPTER 43

VLAN

43.1 VLAN Overview

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

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

43.1.1 What You Can Do

- Use the **VLAN Status** screen ([Section 43.3 on page 281](#)) to view and search all static VLAN groups.
- Use the **VLAN Status Details** screen ([Section 43.3.1 on page 282](#)) to view detailed port settings and status of the static VLAN group.
- Use the **Private VLAN Status** screen ([Section 43.4 on page 283](#)) to view all private VLANs created on the Switch.
- Use the **Static VLAN Setup** screen ([Section 43.5 on page 284](#)) to configure a static VLAN for the Switch.
- Use the **VLAN Port Setup** screen ([Section 43.6 on page 286](#)) to configure the static VLAN (IEEE 802.1Q) settings on a port.
- Use the **GVRP** screen ([Section 43.7 on page 288](#)) to enable/disable GVRP on each port.
- Use the **Subnet Based VLAN Setup** screen ([Section 43.9 on page 290](#)) to set up VLANs that allow you to group traffic into logical VLANs based on the source IP subnet you specify.
- Use the **Protocol Based VLAN Setup** screen ([Section 43.10 on page 291](#)) to set up VLANs that allow you to group traffic into logical VLANs based on the protocol you specify.
- Use the **MAC Based VLAN Setup** screen ([Section 43.12 on page 294](#)) to set up VLANs that allow you to group untagged packets into logical VLANs based on the source MAC address of the packet. This eliminates the need to reconfigure the Switch when you change ports. The Switch will forward the packets based on the source MAC address you set up previously.

43.1.2 What You Need to Know

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

43.2 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 4 bytes longer than an untagged frame and contains 2 bytes of TPID (Tag Protocol Identifier, residing within the type or length field of the Ethernet frame) and 2 bytes of TCI (Tag Control

Information, starts after the source address field of the Ethernet frame).

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4094.

TPID	User Priority	CFI	VLAN ID
16 Bits	3 Bits	1 Bit	12 Bits

Forwarding Tagged and Untagged Frames

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

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

43.2.0.1 Automatic VLAN Registration

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

GARP

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

GARP Timers

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

GVRP

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

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

Table 128 IEEE 802.1Q VLAN Terminology

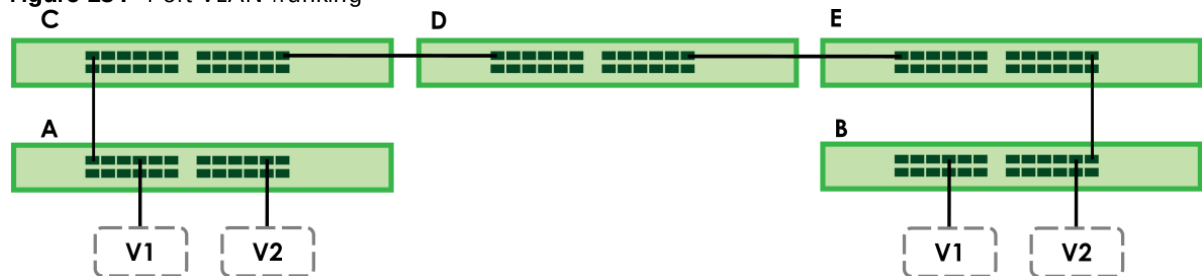
VLAN PARAMETER	TERM	DESCRIPTION
VLAN Type	Permanent VLAN	This is a static VLAN created manually.
	Dynamic VLAN	This is a VLAN configured by a GVRP registration or de-registration process.
VLAN Administrative Control	Registration Fixed	Fixed registration ports are permanent VLAN members.
	Registration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

43.2.0.2 Port VLAN Trunking

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

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

Figure 184 Port VLAN Trunking



43.2.0.3 Select the VLAN Type

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

Figure 185 SYSTEM > Switch Setup: Select VLAN Type

Switch Setup

VLAN Type ☒ 802.1Q ☐ Port Based

Bridge Control Protocol Transparency ☐ OFF

MAC Address Learning

Aging Time seconds

ARP Aging Time

Aging Time seconds

GARP Timer

Join Timer milliseconds

Leave Timer milliseconds

Leave All Timer milliseconds

Apply **Cancel**

802.1Q Static VLAN

Make sure **802.1Q** is selected in the **SYSTEM > Switch Setup > 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.

43.3 VLAN Status

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

Figure 186 SWITCHING > VLAN > VLAN Status

VLAN Status Private VLAN Status

VLAN Search by VID **Search**

The Number of VLAN: 1

Index	VID	Name	Tagged Port	Untagged Port	Elapsed Time	Status
1	1	1	1-56	1-56	9:59:41	Static

Navigation: < Page 1 of 1 >

The following table describes the labels in this screen.

Table 129 SWITCHING > VLAN > VLAN Status

LABEL	DESCRIPTION
VLAN Search by VID	Enter (an) existing VLAN ID numbers (use a comma (,) to separate individual VLANs or a hyphen (-) to indicate a range of VLANs. For example, "3,4" or "3-9") and click Search to display only the specified VLANs in the list below. Leave this field blank and click Search to display all VLANs configured on the Switch.
The Number of VLAN	This is the number of VLANs configured on the Switch.
The Number of Search Results	This is the number of VLANs that match the searching criteria and display in the list below. This field displays only when you use the Search button to look for certain VLANs.
Index	This is the VLAN index number. Click an index number to view more VLAN details.
VID	This is the VLAN identification number that was configured in the corresponding VLAN configuration screen.
Name	This fields shows the descriptive name of the VLAN.
Tagged Port	This field shows the tagged ports that are participating in the VLAN.
Untagged Port	This field shows the untagged ports that are participating in the VLAN.
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the Switch. • Dynamic – using GVRP • Static – manually added as a normal VLAN • Private – manually added as a private VLAN (primary, isolated or community) • MVR – added through Multicast VLAN Registration (MVR)

43.3.1 VLAN Details

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

Figure 187 SWITCHING > VLAN > VLAN Status > VLAN Status Details

VLAN Status Private VLAN Status

VID: 1
Elapsed Time: 0:04:09
Status: Static

Port Number

U:Untagged T:Tagged

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49	51	53	55
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56
U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U
U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U

Private VLAN Status

Page 1 of 0

Primary VLAN	Secondary VLAN	Type	Port List

Page 1 of 0

The following table describes the labels in this screen.

Table 130 SWITCHING > VLAN > VLAN Status > VLAN Status Details

LABEL	DESCRIPTION
VID	This is the VLAN identification number that was configured in the corresponding VLAN configuration screen.
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the Switch. Dynamic – using GVRP Static – manually added as a normal VLAN Private – manually added as a private VLAN (primary, isolated or community) MVR – added through Multicast VLAN Registration (MVR)
Port Number	This section displays the ports that are participating in a VLAN. A tagged port is marked as T, an untagged port is marked as U and ports not participating in a VLAN are marked as “–”.
Private VLAN Status This section show private VLAN information for the selected VLAN.	
Primary VLAN	This field shows the primary VLAN ID in the selected VLAN.
Secondary VLAN	This field shows the secondary VLAN ID in the selected VLAN.
Type	This field shows the type of private VLAN: Primary , Community or Isolated .
Port List	This shows the ports mapped to the private VLAN using the SWITCHING > Private VLAN or SWITCHING > VLAN > VLAN Setup > Static VLAN screen.

43.4 Private VLAN Status

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

Figure 188 SWITCHING > VLAN > VLAN Status > Private VLAN Status

VLAN Status	Private VLAN Status

⏪ < Page 1 of 1 > ⏩			
Primary VLAN	Secondary VLAN	Type	Port List
	2	Community	1-28
⏪ < Page 1 of 1 > ⏩			

The following table describes the labels in this screen.

Table 131 SWITCHING > VLAN > VLAN Status > Private VLAN Status

Label	Description
	These fields show information for the all private VLANs. See also SWITCHING > 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 SWITCHING > Private VLAN or SWITCHING > VLAN > VLAN Setup > Static VLAN screen.

43.5 Configure a Static VLAN

Use this screen to view and configure a static VLAN for the Switch. Click **SWITCHING > VLAN > VLAN Setup > Static VLAN** to display the screen as shown next.

Figure 189 SWITCHING > VLAN > VLAN Setup > Static VLAN

Static VLAN

VLAN Port Setup

GVRP

+

Add/Edit

🗑

Delete

☐	VID	Active	Name
☐	1	ON	1
☐	2	ON	2
☐	3	ON	3
☐	100	ON	VLAN100

The following table describes the related labels in this screen.

Table 132 SWITCHING > VLAN > VLAN Setup > Static VLAN

Label	Description
VID	This field displays the ID number of the VLAN group.
Active	This field indicates whether the VLAN settings are enabled or disabled.
Name	This field displays the descriptive name for this VLAN group.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.

Table 132 SWITCHING > VLAN > VLAN Setup > Static VLAN (continued)

LABEL	DESCRIPTION
Add/Edit	Click Add/Edit to add a new static VLAN or edit a selected one.
Delete	Click Delete to remove the selected static VLAN.

43.5.1 Add/Edit a Static VLAN

Use this screen to configure a static VLAN for the Switch. Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SWITCHING > VLAN > VLAN Setup > Static VLAN** screen to display this screen.

Figure 190 SWITCHING > VLAN > VLAN Setup > Static VLAN > Add/Edit

Active ☐ OFF

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

Apply Clear Cancel

The following table describes the related labels in this screen.

Table 133 SWITCHING > VLAN > VLAN Setup > Static VLAN > Add/Edit

LABEL	DESCRIPTION
Active	Enable the switch button 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 ASCII characters. The string should not contain [?], [], ['], ["], or [,].
VLAN Group ID	Enter the VLAN ID for this static entry; the valid range is between 1 and 4094. Note: Do NOT add a VLAN ID that has been used in the SWITCHING > VLAN > Voice VLAN Setup .
VLAN Type	Select Normal (static) or Private . For Private VLANs, select Primary , Isolated or Community .

Table 133 SWITCHING > VLAN > VLAN Setup > Static VLAN > Add/Edit (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.
Port	The port number identifies the port you are configuring.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Control	Select Normal for the port to dynamically join this VLAN group 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.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

43.6 VLAN Port Setup

Use this screen to configure the static VLAN (IEEE 802.1Q) settings on a port. Click **SWITCHING > VLAN > VLAN Setup > VLAN Port Setup** to display the screen as shown.

Figure 191 SWITCHING > VLAN > VLAN Setup > VLAN Port Setup

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

The following table describes the labels in this screen.

Table 134 SWITCHING > VLAN > VLAN Setup > VLAN Port Setup

LABEL	DESCRIPTION
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Ingress Check	If this checkbox is selected, the Switch discards incoming frames on a port for VLANs that do not include this port in its member set. Clear this checkbox 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.
Acceptable Frame Type	Specify the type of frames allowed on a port. Choices are All, Tag Only and Untag Only. Select All from the drop-down list box to accept all untagged or tagged frames on this port. This is the default setting. Select Tag Only to accept only tagged frames on this port. All untagged frames will be dropped. Select Untag Only to accept only untagged frames on this port. All tagged frames will be dropped.
VLAN Trunking	Enable VLAN Trunking on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the Switch.
Isolation	Select this to allow this port to communicate only with the CPU management port and the ports on which the isolation feature is NOT enabled.

Table 134 SWITCHING > VLAN > VLAN Setup > VLAN Port Setup (continued)

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

43.7 Configure GVRP

Use this screen to configure GVRP settings on a port. Click **SWITCHING > VLAN > VLAN Setup > GVRP** to display the screen as shown.

Figure 192 SWITCHING > VLAN > VLAN Setup > GVRP

Port	GVRP
*	☐
1	☐
2	☐
3	☐
4	☐
5	☐
6	☐
7	☐

The following table describes the labels in this screen.

Table 135 SWITCHING > VLAN > VLAN Setup > GVRP

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. Enable the switch button to permit VLAN groups beyond the local Switch.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
GVRP	Select this checkbox to allow GVRP on this port.

Table 135 SWITCHING > VLAN > VLAN Setup > GVRP (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.

43.8 Subnet Based VLAN

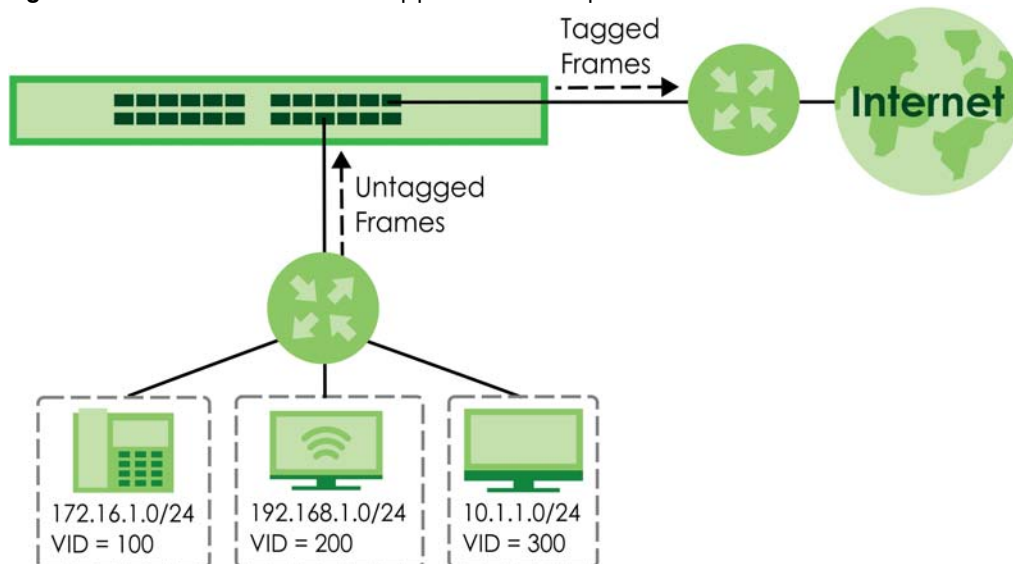
Subnet based VLANs allow you to group traffic into logical VLANs based on the source IP subnet you specify. When a frame is received on a port, the Switch checks if a tag is added already and the IP subnet it came from. The untagged packets from the same IP subnet are then placed in the same subnet based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

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

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

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

Figure 193 Subnet Based VLAN Application Example



43.9 Configuring Subnet Based VLAN

Click the **SWITCHING > VLAN > Subnet Based VLAN Setup > Subnet Based VLAN** link in the navigation panel to display the configuration screen as shown.

Figure 194 SWITCHING > VLAN > Subnet Based VLAN Setup > Subnet Based VLAN

The following table describes the labels in this screen.

Table 136 SWITCHING > VLAN > Subnet Based VLAN Setup > Subnet Based VLAN

LABEL	DESCRIPTION
Active	Enable the switch button 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 through another DHCP server on the subnet based VLAN. Enable the switch button 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.
Cancel	Click Cancel to begin configuring this screen afresh.
Index	This is the index number identifying this 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.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new entry or edit a selected one.
Delete	Click Delete to remove the selected entry.

43.9.1 Add/Edit Subnet Based VLAN

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SWITCHING > VLAN > Subnet Based VLAN Setup > Subnet Based VLAN** screen to display this screen.

Figure 195 SWITCHING > VLAN > Subnet Based VLAN Setup > Subnet Based VLAN > Add/Edit

Active ☐ OFF

Name

IP

Mask-Bits

VLAN

Priority

Apply Clear Cancel

The following table describes the labels in this screen.

Table 137 SWITCHING > VLAN > Subnet Based VLAN Setup > Subnet Based VLAN > Add/Edit

LABEL	DESCRIPTION
Active	Enable the switch button to activate the IP subnet VLAN you are creating or editing.
Name	Enter up to 32 alphanumeric characters to identify this subnet based VLAN. The string should not contain [?], [], ['], ["], or [,].
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).
VLAN	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 SWITCHING > VLAN > VLAN Setup > Static VLAN screen.
Priority	Select the priority level that the Switch assigns to frames belonging to this 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.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

43.10 Protocol Based VLAN

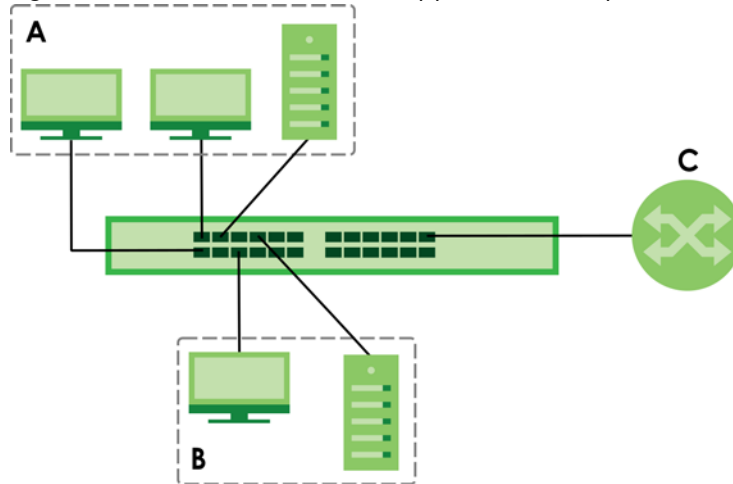
Protocol based VLANs allow you to group traffic into logical VLANs based on the protocol you specify. When an upstream frame is received on a port (configured for a protocol based VLAN), the Switch checks if a tag is added already and its protocol. The untagged packets of the same protocol are then placed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

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

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

upstream ARP traffic from port 1, 2 and 3 will be grouped together, and all upstream Apple Talk traffic from port 6 and 7 will be in another group and have higher priority than ARP traffic, when they go through the uplink port to a backbone switch **C**.

Figure 196 Protocol Based VLAN Application Example



43.11 Configuring Protocol Based VLAN

Click the **SWITCHING > VLAN > Protocol Based VLAN Setup > Protocol Based VLAN** link in the navigation panel to display the configuration screen as shown.

Figure 197 SWITCHING > VLAN > Protocol Based VLAN Setup > Protocol Based VLAN

Protocol Based VLAN

+ Add/Edit
Delete

☐	Index	Active	Port	Name	Ethernet-type	VID	Priority

The following table describes the labels in this screen.

Table 138 SWITCHING > VLAN > Protocol Based VLAN Setup > Protocol Based VLAN

LABEL	DESCRIPTION
Index	This is the index number identifying this protocol based VLAN. Click any of these numbers to edit an existing protocol based VLAN.
Active	This field shows whether the protocol based VLAN is active or not.
Port	This field shows which port belongs to this protocol based VLAN.
Name	This field shows the name of the protocol based VLAN.
Ethernet-type	This field shows which Ethernet protocol is part of this protocol based VLAN.
VID	This field shows the VLAN ID of the port.
Priority	This field shows the priority which is assigned to frames belonging to this protocol based VLAN.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.

Table 138 SWITCHING > VLAN > Protocol Based VLAN Setup > Protocol Based VLAN (continued)

LABEL	DESCRIPTION
Add/Edit	Click Add/Edit to add a new entry or edit a selected one.
Delete	Click Delete to remove the selected entry.

43.11.1 Add/Edit a Protocol Based VLAN

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SWITCHING > VLAN > Protocol Based VLAN Setup > Protocol Based VLAN** screen to display this configuration screen.

Figure 198 SWITCHING > VLAN > Protocol Based VLAN Setup > Protocol Based VLAN > Add/Edit

The screenshot shows the 'Add/Edit' configuration screen for a Protocol Based VLAN. It contains the following elements:

- Active:** A toggle switch currently set to 'OFF'.
- Port:** A text input field.
- Name:** A text input field.
- Ethernet-type:** Two radio buttons. The 'IP' radio button is selected, and it is associated with a dropdown menu. The 'Other' radio button is unselected and is associated with a text input field followed by '(Hex)'.
- VLAN:** A text input field.
- Priority:** A dropdown menu with '0' selected.
- Buttons:** At the bottom, there are three buttons: 'Apply' (green), 'Clear' (grey), and 'Cancel' (grey).

The following table describes the labels in this screen.

Table 139 SWITCHING > VLAN > Protocol Based VLAN Setup > Protocol Based VLAN Setup > Add/Edit

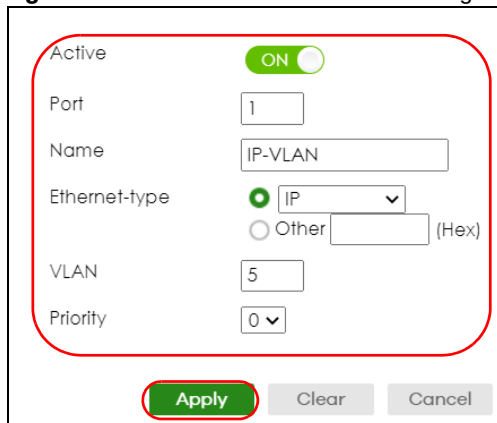
LABEL	DESCRIPTION
Active	Enable the switch button to activate this protocol based VLAN.
Port	Type a port to be included in this protocol based VLAN. This port must belong to a static VLAN in order to participate in a protocol based VLAN.
Name	Enter up to 32 alphanumeric characters to identify this protocol based VLAN. The string should not contain [?], [], ['], ["], or [,].
Ethernet-type	Use the drop down list box to select a predefined protocol to be included in this protocol based VLAN or select Other 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.
VLAN	Enter the ID of a VLAN to which the port belongs. This must be an existing VLAN which you defined in the SWITCHING > VLAN > VLAN Setup > Static VLAN screen.
Priority	Select the priority level that the Switch will assign to frames belonging to this 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.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

43.11.1.1 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 **Apply**.

Figure 199 Protocol Based VLAN Configuration Example



The screenshot shows a configuration window for a Protocol Based VLAN. It includes the following fields and controls:

- Active:** A toggle switch set to **ON**.
- Port:** A text input field containing the value **1**.
- Name:** A text input field containing the value **IP-VLAN**.
- Ethernet-type:** A radio button selection with **IP** selected and **Other** (Hex) as an alternative.
- VLAN:** A text input field containing the value **5**.
- Priority:** A dropdown menu set to **0**.
- Buttons:** **Apply** (highlighted with a red circle), **Clear**, and **Cancel**.

To add more ports to this protocol based VLAN.

- 1 Select the checkbox of this protocol based VLAN. Click **Add/Edit**.
- 2 Change the value in the **Port** field to the next port you want to add.
- 3 Click **Apply**.

43.12 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 **SWITCHING > VLAN > MAC Based VLAN Setup > MAC Based VLAN** to see the following screen.

Figure 200 SWITCHING > VLAN > MAC Based VLAN Setup > MAC Based VLAN

The following table describes the fields in the above screen.

Table 140 SWITCHING > VLAN > MAC Based VLAN Setup > MAC Based VLAN

LABEL	DESCRIPTION
Index	This field displays the index number of the MAC-based VLAN entry.
Name	This field displays the name of the MAC-based VLAN entry.
MAC Address	This field displays the source MAC address that is bind to the MAC-based VLAN entry.
VID	This field displays the VLAN ID of the MAC-based VLAN entry.
Priority	This field displays the priority level which is assigned to frames belonging to this MAC-based VLAN entity.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new entry or edit a selected one.
Delete	Click Delete to remove the selected entry.

43.12.1 Add/Edit a MAC Based VLAN

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SWITCHING > VLAN > MAC Based VLAN Setup > MAC Based VLAN** screen to see this screen.

Figure 201 SWITCHING > VLAN > MAC Based VLAN Setup > MAC Based VLAN > Add/Edit

The following table describes the fields in the above screen.

Table 141 SWITCHING > VLAN > MAC Based VLAN Setup > MAC Based VLAN > Add/Edit

LABEL	DESCRIPTION
Name	Enter a name up to 32 alphanumeric characters except [?], [], ['], ["], or [,] for the MAC-based VLAN entry.
MAC Address	Enter 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	Enter an ID (from 1 to 4094) for the VLAN that is associated with the MAC-based VLAN entry.

Table 141 SWITCHING > VLAN > MAC Based VLAN Setup > MAC Based VLAN > Add/Edit (continued)

LABEL	DESCRIPTION
Priority	Enter a priority (0 to 7) that the Switch assigns to frames belonging to this VLAN. The higher the numeric value you assign, the higher the priority for this MAC-based VLAN entry.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

CHAPTER 44

VLAN Mapping

This chapter shows you how to configure VLAN mapping on the Switch.

44.1 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.

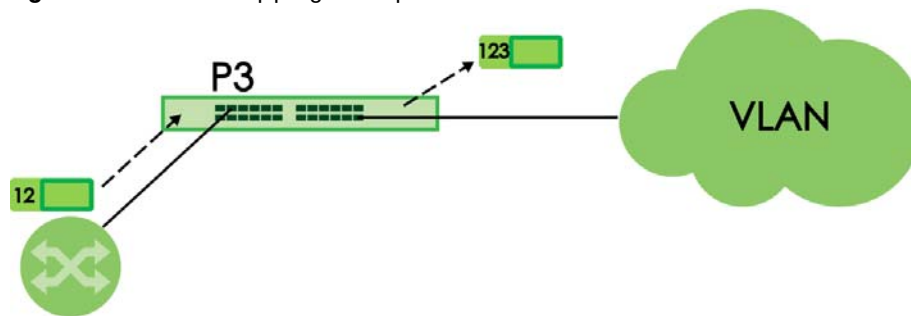
The Switch checks incoming traffic from the switch ports (non-management ports) against the VLAN mapping table first, the MAC learning table and then the VLAN table before forwarding them through the Gigabit uplink port. When VLAN mapping is enabled, the Switch discards the tagged packets that do not 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 cannot enable VLAN mapping and VLAN stacking at the same time.

44.1.1 VLAN Mapping Example

In the following example figure, packets that carry VLAN ID 12 and are received on port 3 (**P3**) 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 (**P3**) will be dropped.

Figure 202 VLAN Mapping Example



44.1.2 What You Can Do

- Use the **VLAN Mapping** screen ([Section 44.2 on page 298](#)) to enable VLAN mapping on the Switch and ports.
- Use the **VLAN Mapping Setup** screen ([Section 44.3 on page 298](#)) to enable and edit the VLAN mapping rules.

44.2 Enable VLAN Mapping

Click **SWITCHING > VLAN Mapping > VLAN Mapping** in the navigation panel to display the screen as shown.

Figure 203 SWITCHING > VLAN Mapping > VLAN Mapping

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

The following table describes the labels in this screen.

Table 142 SWITCHING > VLAN Mapping > VLAN Mapping

LABEL	DESCRIPTION
Active	Enable the switch button to enable VLAN mapping on the Switch.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to enable the VLAN mapping feature on this port. Clear this checkbox to disable the VLAN mapping feature.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

44.3 VLAN Mapping Setup

Click the **SWITCHING > VLAN Mapping > VLAN Mapping Setup** to display the screen as shown. Use this screen to view and configure the VLAN mapping rules.

Figure 204 SWITCHING > VLAN Mapping > VLAN Mapping Setup

The screenshot shows the 'VLAN Mapping Setup' configuration page. At the top, there are two tabs: 'VLAN Mapping' and 'VLAN Mapping Setup' (which is active). Below the tabs, there is a search bar and two buttons: '+ Add/Edit' and 'Delete'. Below these is a table with the following columns: Index, Active, Name, Port, VID, Translated VID, and Priority. The 'Active' column has a checkbox. The 'Index' column has a small square icon.

The following table describes the labels in this screen.

Table 143 SWITCHING > VLAN Mapping > VLAN Mapping Setup

LABEL	DESCRIPTION
Index	This is the number of the VLAN mapping entry in the table.
Active	This shows whether this entry is activated or not.
Name	This is the descriptive name for this rule.
Port	This is the port number to which this rule is applied.
VID	This is the customer VLAN ID in the incoming packets.
Translated VID	This is the VLAN ID that replaces the customer VLAN ID in the tagged packets.
Priority	This is the priority level that replaces the customer priority level in the tagged packets.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new entry or edit a selected one.
Delete	Click Delete to remove the selected entries.

44.3.1 Add/Edit VLAN Mapping

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SWITCHING > VLAN Mapping > VLAN Mapping Setup** to display this screen. Use this screen to enable and edit the VLAN mapping rules.

Figure 205 SWITCHING > VLAN Mapping > VLAN Mapping Setup > Add/Edit

The screenshot shows the 'Add/Edit' configuration page for VLAN Mapping. It contains the following fields: 'Active' with a toggle switch currently set to 'OFF'; 'Name' with a text input field; 'Port' with a text input field; 'VID' with a text input field; 'Translated VID' with a text input field; and 'Priority' with a dropdown menu currently showing '0'. At the bottom, there are three buttons: 'Apply' (green), 'Clear' (grey), and 'Cancel' (grey).

The following table describes the labels in this screen.

Table 144 SWITCHING > VLAN Mapping > VLAN Mapping Setup > Add/Edit

LABEL	DESCRIPTION
Active	Enable the switch button to activate this rule.
Name	Enter a descriptive name (up to 32 printable ASCII characters except [?], [], ['], ["], or [,]) for identification purposes.

Table 144 SWITCHING > VLAN Mapping > VLAN Mapping Setup > Add/Edit (continued)

LABEL	DESCRIPTION
Port	Type a port to be included in this rule.
VID	Enter a VLAN ID from 1 to 4094. This is the VLAN tag carried in the packets and will be translated into the VID you specified in the Translated VID field.
Translated VID	Enter a VLAN ID (from 1 to 4094) into which the customer VID carried in the packets will be translated.
Priority	Select a priority level (from 0 to 7). This is the priority level that replaces the customer priority level in the tagged packets or adds to the untagged packets.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

CHAPTER 45

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 LANs (VLANs).

45.1 VLAN Stacking Overview

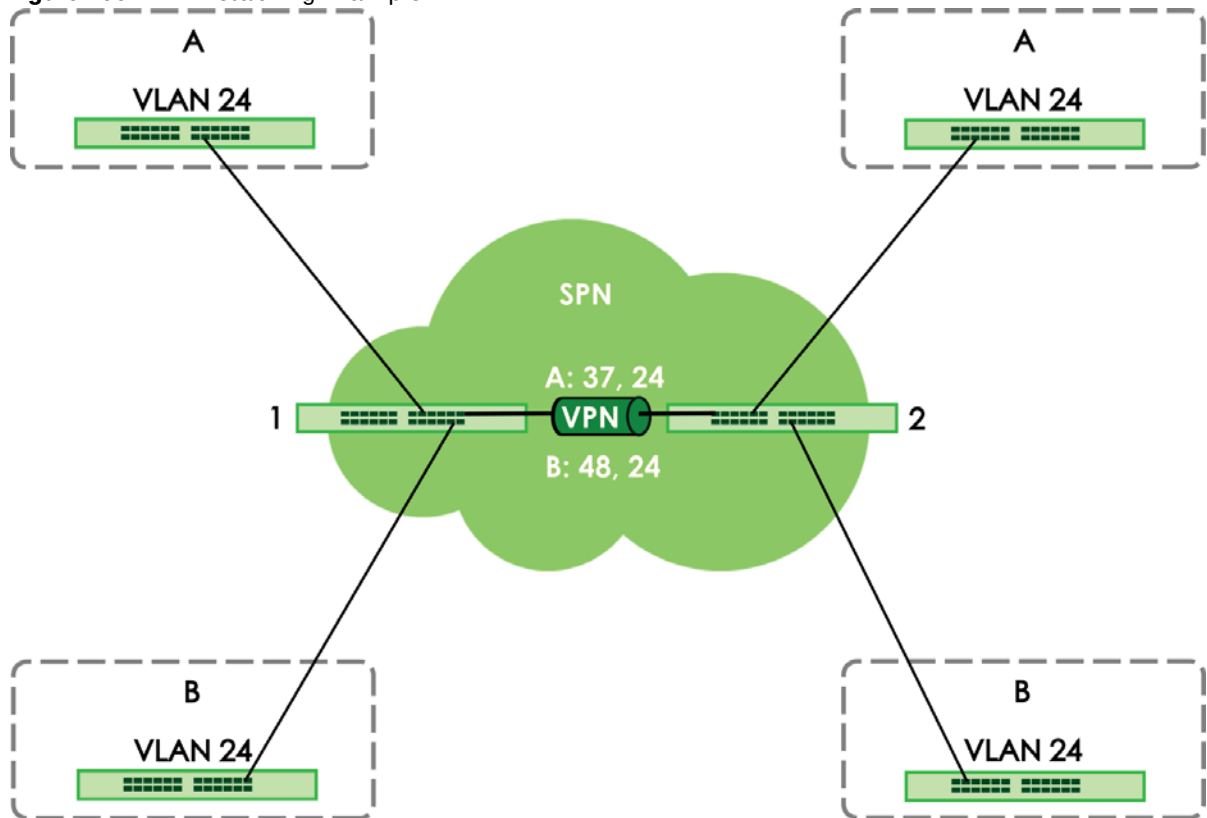
A service provider can use VLAN stacking to allow it to distinguish multiple customers VLANs, even those with the same (customer-assigned) VLAN ID, within its network.

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 4094 VLAN groups with each group containing up to 4094 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.

45.1.1 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 206 VLAN Stacking Example

45.2 VLAN Stacking Port Roles

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

- Select **Normal** for “regular” (non-VLAN stacking) IEEE 802.1Q frame switching.
- Select **Access** 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**.

- Select **Tunnel** (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**.

45.3 VLAN Tag Format

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

Table 145 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 > Port Setup > Port Setup** screen.
- "0" is the lowest priority level and "7" is the highest.

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

45.3.1 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 **SWITCHING > VLAN Stacking** screens.

Table 146 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 147 802.1Q 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

45.4 Configuring VLAN Stacking

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

Figure 207 SWITCHING > VLAN Stacking > VLAN Stacking

Port	Role	Tunnel TPID (Hex)
*	Normal	
1	Normal	8100
2	Normal	8100
3	Normal	8100
4	Normal	8100
5	Normal	8100
6	Normal	8100
7	Normal	8100

The following table describes the labels in this screen.

Table 148 SWITCHING > VLAN Stacking > VLAN Stacking

LABEL	DESCRIPTION
Active	Enable the switch button to enable VLAN stacking on the Switch.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
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 to have the Switch add the SP TPID tag to all incoming frames received on this port. Select Access for ingress ports at the edge of the service provider's network. Select Tunnel (available for Gigabit ports only) for egress ports at the edge of the service provider's network. Select Tunnel to have the Switch add the Tunnel TPID (HEX) 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.

Table 148 SWITCHING > VLAN Stacking > VLAN Stacking (continued)

LABEL	DESCRIPTION
Tunnel TPID (HEX)	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 ports. 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. It is used to identify the customer tag of an incoming frame. 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.

45.5 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 if they have different customer VLAN IDs.

Click **SWITCHING > VLAN Stacking > Port-Based QinQ** to display the screen as shown.

Figure 208 SWITCHING > VLAN Stacking > Port-Based QinQ

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 ▼

The following table describes the labels in this screen.

Table 149 SWITCHING > VLAN Stacking > Port-Based QinQ

LABEL	DESCRIPTION
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
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.
Priority	Select a priority level (from 0 to 7). This is the service provider's priority level that adds to the frames received on this port. "0" is the lowest priority level and "7" is the highest.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

45.6 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 **SWITCHING > VLAN Stacking > Selective QinQ** to display the screen as shown.

Figure 209 SWITCHING > VLAN Stacking > Selective QinQ

The following table describes the labels in this screen.

Table 150 SWITCHING > VLAN Stacking > Selective QinQ

LABEL	DESCRIPTION
Index	This is the number of the selective VLAN stacking rule.
Active	This shows whether this rule is activated or not.
Name	This is the descriptive name for this rule.
Port	This is the port number to which this rule is applied.
CVID	This is the customer VLAN ID in the incoming packets.

Table 150 SWITCHING > VLAN Stacking > Selective QinQ (continued)

LABEL	DESCRIPTION
SPVID	This is the service provider's VLAN ID that adds to the packets from the subscribers.
Priority	This is the service provider's priority level in the packets.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new entry or edit a selected one.
Delete	Click Delete to remove the selected entries.

45.6.1 Add/Edit Selective Q-in-Q

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SWITCHING > VLAN Stacking > Selective QinQ** screen to display this screen.

Figure 210 SWITCHING > VLAN Stacking > Selective QinQ > Add/Edit

The following table describes the labels in this screen.

Table 151 SWITCHING > VLAN Stacking > Selective QinQ > Add/Edit

LABEL	DESCRIPTION
Active	Enable the switch button to activate this rule.
Name	Enter a descriptive name (up to 32 printable ASCII characters except [?], [], ['], ["], or [,]) for identification purposes.
Port	The port number identifies the port you are configuring.
CVID	Enter a customer VLAN ID (the inner VLAN tag) from 1 to 4094. This is the VLAN tag carried in the packets from the subscribers.
SPVID	SPVID is the service provider's VLAN ID (the outer VLAN tag). Enter the service provider ID (from 1 to 4094) for frames received on this port.
Priority	Select a priority level (from 0 to 7). This is the service provider's priority level that adds to the frames received on this port. "0" is the lowest priority level and "7" is the highest.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

CHAPTER 46

WoL Relay

46.1 WoL Relay Overview

Wake On LAN is a feature to remotely turn on a device on the LAN network. A device is turned on by receiving a magic packet. To use this feature the remote hardware (for example the network adapter on a computer) must support Wake On LAN using the “Magic Packet” method.

A magic packet is a UDP broadcast packet. The device that you want to turn on is off, so it cannot respond to a TCP packet. Therefore, it has to be a UDP broadcast packet to turn on a device.

Broadcast packets are generally not routed. A magic packet cannot be routed. This prevents DDoS attacks, but also prohibits you from sending magic packets to other devices in different subnets. The Switch's Wake On LAN relay feature allows you to send magic packets to devices across different subnets.

46.2 WoL Relay

Use this screen to configure settings on Wake On LAN relay. Click **SWITCHING > WoL Relay** to open the following screen.

Figure 211 SWITCHING > WoL Relay

☐	Index	UDP Port	Source VLAN	Destination VLAN
+ Add/Edit Delete				

The following table describes the labels in this screen.

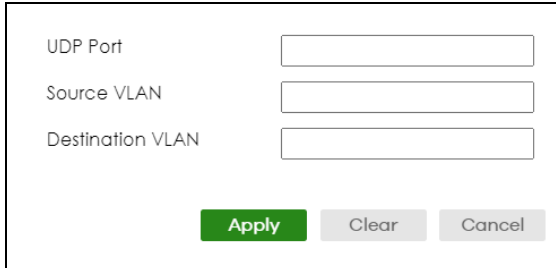
Table 152 SWITCHING > WoL Relay

LABEL	DESCRIPTION
Index	This field displays the index number of the rule.
UDP	This field displays the UDP port of the rule.
Source VLAN	This field displays the source VLAN ID of the rule.
Destination VLAN	This field displays the destination VLAN ID of the rule.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new entry or edit a selected one.
Delete	Click Delete to remove the selected entries.

46.2.1 Add/Edit WoL Relay

Use this screen to add or edit configurations on Wake On LAN relay. Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SWITCHING > WoL Relay** screen to open this screen.

Figure 212 SWITCHING > WoL Relay > Add/Edit



UDP Port

Source VLAN

Destination VLAN

Apply **Clear** **Cancel**

The following table describes the labels in this screen.

Table 153 SWITCHING > WoL Relay > Add/Edit

LABEL	DESCRIPTION
UDP Port	Enter a UDP port number that magic packets are sent through. The most common port for transmission is UDP port 9.
Source VLAN	Enter the source VLAN ID where the magic packet originates from.
Destination VLAN	Enter the destination VLAN ID where the magic packet will be sent to.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

CHAPTER 47

NETWORKING

The following chapters introduces the configurations of the links under the **NETWORKING** navigation panel.

Quick links to chapters:

- [ARP Setup](#)
- [DHCP](#)
- [Static Route](#)

CHAPTER 48

ARP Setup

48.1 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.

48.1.1 What You Can Do

Use the **ARP Learning** screen ([Section 48.2 on page 313](#)) to configure ARP learning mode on a per-port basis.

Use the **Static ARP** screen ([Section 48.3 on page 314](#)) to create static ARP entries that will display in the **MONITOR > ARP Table** screen and will not age out.

48.1.2 What You Need to Know

Read on for concepts on ARP that can help you configure the screen in this chapter.

48.1.2.1 How ARP Works

When an incoming packet destined for a host device on a local area network arrives at the Switch, the Switch looks in the ARP Table and if it finds the address, it sends it to the device.

If no entry is found for the IP address, ARP broadcasts the request to all the devices on the LAN. The Switch fills in its own MAC and IP address in the sender address fields, and puts the known IP address of the target in the target IP address field. In addition, the Switch puts all ones in the target MAC field (FF.FF.FF.FF.FF.FF is the Ethernet broadcast address). The replying device (which is either the IP address of the device being sought or the router that knows the way) replaces the broadcast address with the target's MAC address, swaps the sender and target pairs, and unicasts the answer directly back to the requesting machine. ARP updates the ARP Table for future reference and then sends the packet to the MAC address that replied.

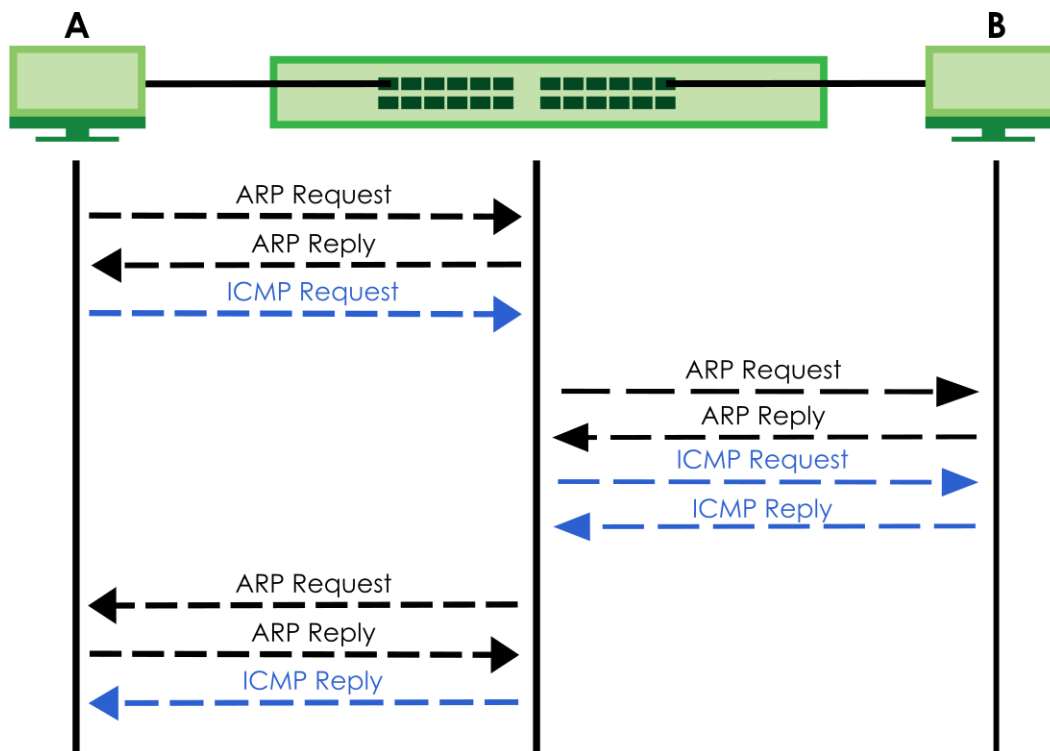
48.1.2.2 ARP Learning Mode

The Switch supports three ARP learning modes: ARP-Reply, Gratuitous-ARP, and ARP-Request.

ARP-Reply

The Switch in ARP-Reply learning mode updates the ARP table only with the ARP replies to the ARP requests sent by the Switch. This can help prevent ARP spoofing.

In the following example, the Switch does not have IP address and MAC address mapping information for hosts **A** and **B** in its ARP table, and host **A** wants to ping host **B**. Host **A** sends an ARP request to the Switch and then sends an ICMP request after getting the ARP reply from the Switch. The Switch finds no matched entry for host **B** in the ARP table and broadcasts the ARP request to all the devices on the LAN. When the Switch receives the ARP reply from host **B**, it updates its ARP table and also forwards host **A**'s ICMP request to host **B**. After the Switch gets the ICMP reply from host **B**, it sends out an ARP request to get host **A**'s MAC address and updates the ARP table with host **A**'s ARP reply. The Switch then can forward host **B**'s ICMP reply to host **A**.



Gratuitous-ARP

A gratuitous ARP is an ARP request in which both the source and destination IP address fields are set to the IP address of the device that sends this request and the destination MAC address field is set to the broadcast address. There will be no reply to a gratuitous ARP request.

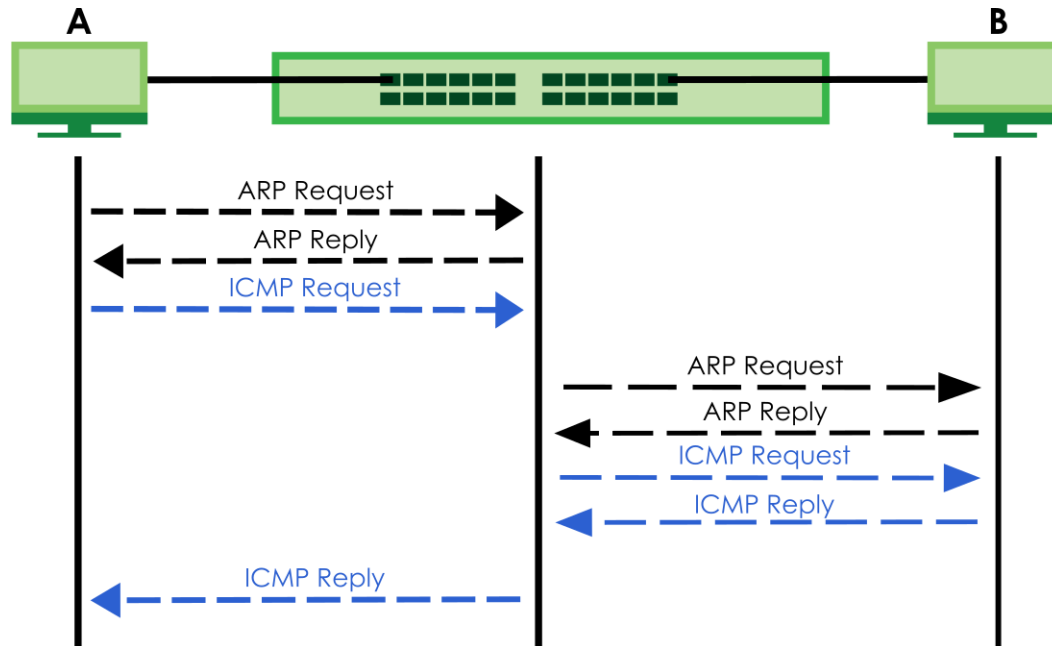
A device may send a gratuitous ARP packet to detect IP collisions. If a device restarts or its MAC address is changed, it can also use gratuitous ARP to inform other devices in the same network to update their ARP table with the new mapping information.

In Gratuitous-ARP learning mode, the Switch updates its ARP table with either an ARP reply or a gratuitous ARP request.

ARP-Request

When the Switch is in ARP-Request learning mode, it updates the ARP table with both ARP replies, gratuitous ARP requests and ARP requests.

Therefore in the following example, the Switch can learn host **A**'s MAC address from the ARP request sent by host **A**. The Switch then forwards host **B**'s ICMP reply to host **A** right after getting host **B**'s MAC address and ICMP reply.



48.2 ARP Learning

Use this screen to configure each port's ARP learning mode. Click **NETWORKING > ARP Setup > ARP Learning > ARP Learning** in the navigation panel to display the screen as shown next.

Figure 213 NETWORKING > ARP Setup > ARP Learning > 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

Apply Cancel

The following table describes the labels in this screen.

Table 154 NETWORKING > ARP Setup > ARP Learning > ARP Learning

LABEL	DESCRIPTION
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
ARP Learning Mode	Select the ARP learning mode the Switch uses on the port. Select ARP-Reply to have the Switch update the ARP table only with the ARP replies to the ARP requests sent by the Switch. Select Gratuitous-ARP to have the Switch update its ARP table with either an ARP reply or a gratuitous ARP request. Select ARP-Request to have the Switch update the ARP table with both ARP replies, gratuitous ARP requests and ARP requests.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

48.3 Static ARP

Use this screen to view and configure static ARP entries that will display in the **MONITOR > ARP Table > ARP Table** screen and will not age out. Click **NETWORKING > ARP Setup > Static ARP > Static ARP** to display the screen as shown.

Figure 214 NETWORKING > ARP Setup > Static ARP > Static ARP

Static ARP

+ Add/Edit Delete

☐	Index	Active	Name	IP Address	MAC Address	VID	Port

The following table describes the related labels in this screen.

Table 155 NETWORKING > ARP Setup > Static ARP > Static ARP

LABEL	DESCRIPTION
Index	This field displays the index number of an entry.
Active	This field displays whether the entry is activated.
Name	This field displays the descriptive name for this entry. This is for identification purposes only.
IP Address	This is the IP address of a device connected to a Switch port with the corresponding MAC address below.
MAC Address	This is the MAC address of the device with the corresponding IP address above.
VID	This field displays the VLAN to which the device belongs.
Port	This field displays the port to which the device connects.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new entry or edit a selected one.
Delete	Click Delete to remove the selected entries.

48.3.1 Add/Edit Static ARP

Use this screen to add/edit static ARP entries. Click **Add/Edit**, or select an entry and click **Add/Edit** in the **NETWORKING > ARP Setup > Static ARP > Static ARP** to display this screen.

Figure 215 NETWORKING > ARP Setup > Static ARP > Static ARP > Add/Edit

Active ☐ OFF

Name

IP Address

MAC Address

VID

Port

Apply Clear Cancel

The following table describes the related labels in this screen.

Table 156 NETWORKING > ARP Setup > Static ARP > Static ARP > Add/Edit

LABEL	DESCRIPTION
Active	Enable the switch button to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this checkbox.
Name	Enter a descriptive name (up to 32 printable ASCII characters except [?], [], ['], ["] or [,]) 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.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

CHAPTER 49

DHCP

49.1 DHCP Overview

This chapter shows you how to configure the DHCP feature.

DHCP (Dynamic Host Configuration Protocol RFC 2131 and RFC 2132) allows individual computers to obtain TCP/IP configuration at start-up from a server. 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 do not 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.

49.1.1 What You Can Do

- Use the **DHCPv4 Relay Status** screen ([Section 49.2 on page 318](#)) to display the relay mode and status.
- Use the **DHCPv4 Option 82 Profile** screen ([Section 49.4 on page 320](#)) to create DHCPv4 option 82 profiles.
- Use the **DHCPv4 Smart Relay** screen ([Section 49.5 on page 322](#)) to configure global DHCPv4 relay. You can also use this screen to apply different DHCP option 82 profile to certain ports on the Switch.
- Use the **DHCPv4 Relay VLAN Setting** screen ([Section 49.6 on page 324](#)) to configure your DHCPv4 settings based on the VLAN domain of the DHCPv4 clients. You can also use this screen to apply a different DHCP option 82 profile to certain ports in a VLAN.
- Use the **DHCPv4 Server Status** screen ([Section 49.7 on page 327](#)) to display the server status.
- Use the **DHCPv4 Server Status Details** screen ([Section 49.7.1 on page 328](#)) to view details regarding DHCP server settings configured on the Switch.
- Use the **DHCPv4 Server Setup** screen ([Section 49.8 on page 329](#)) to configure DHCP server settings on the Switch.
- Use the **DHCP Server Guard** screen ([Section 49.9 on page 332](#)) to specify whether ports are trusted or untrusted ports for DHCP packets.

49.1.2 What You Need to Know

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

DHCP Modes

If there is already a DHCP server on your network, then you can configure the Switch as a DHCP relay agent. When the Switch receives a request from a computer on your network, it contacts the DHCP server for the necessary IP information, and then relays the assigned information back to the computer.

DHCPv4 Configuration Options

The DHCPv4 configuration on the Switch is divided into **Smart Relay** 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:

- **Smart Relay** – The Switch forwards all DHCP requests to the same DHCP server.
- **VLAN** – The Switch is configured on a VLAN by VLAN basis. The Switch can be configured to relay DHCP requests to different DHCP servers for clients in different VLAN.

49.2 DHCPv4 Relay Status

Click **NETWORKING > DHCP > DHCPv4 Relay** in the navigation panel. The **DHCP Relay Status** screen displays.

Figure 216 NETWORKING > DHCP > DHCPv4 Relay > DHCP Relay Status

DHCP Relay Status		DHCP Option 82 Profile	DHCP Smart Relay	DHCP Relay VLAN Setting
Relay Mode	VLAN: 1			
VID	Current Source Address			
1	172.21.40.213			

The following table describes the labels in this screen.

Table 157 NETWORKING > DHCP > DHCPv4 Relay > DHCP Relay Status

LABEL	DESCRIPTION
Relay Mode	This field displays: None – if the Switch is not configured as a DHCP relay agent. Smart – if the Switch is configured as a DHCP relay agent only. VLAN – followed by a VLAN ID or multiple VLAN IDs if it is configured as a relay agent for specific VLANs.
VID	This field displays the ID number of the VLAN for which the Switch acts as a DHCP relay agent.
Current Source Address	This field displays the source IP address of the DHCP requests that the Switch forwards to a DHCP server.

49.3 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.

49.3.1 DHCPv4 Relay Agent Information

The Switch can add information about the source of client DHCP requests that it relays to a DHCP server by adding **Relay Agent Information**. This helps provide authentication about the source of the requests. The DHCP server can then provide an IP address based on this information. Please refer to RFC 3046 for more details.

The DHCP **Relay Agent Information** feature adds an Agent Information field (also known as the **Option 82** field) to DHCP requests. The **Option 82** field is in the DHCP headers of client DHCP request frames that the Switch relays to a DHCP server.

Relay Agent Information can include the **System Name** of the Switch if you select this option. You can change the **System Name** in **SYSTEM > General Setup**.

The following describes the DHCP relay agent information that the Switch sends to the DHCP server:

Table 158 Relay Agent Information

FIELD LABELS	DESCRIPTION
Slot ID	(1 byte) This value is always 0 for stand-alone switches.
Port ID	(1 byte) This is the port that the DHCP client is connected to.
VLAN ID	(2 bytes) This is the VLAN that the port belongs to.
Information	(up to 64 bytes) This optional, read-only field is set according to system name set in SYSTEM > General Setup .

49.3.1.1 DHCPv4 Relay Agent Information Format

A DHCP Relay Agent Information option has the following format.

Table 159 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.

49.3.1.2 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 160 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 161 DHCP Relay Agent Remote ID Sub-option Format

SubOpt Code	Length	Value
2 (1 byte)	N (1 byte)	MAC Address or String

The 1 in the first field identifies this as an Agent Circuit ID sub-option and two identifies this as an Agent Remote ID sub-option. The next field specifies the length of the field.

49.4 DHCPv4 Option 82 Profile

Use this screen to view and configure DHCPv4 option 82 profiles. Click **NETWORKING > DHCP > DHCPv4 Relay > DHCP Option 82 Profile** link to display the screen as shown.

Figure 217 NETWORKING > DHCP > DHCPv4 Relay > DHCP Option 82 Profile

Profile Name	Enable	Circuit-ID	Field	Enable	Remote-ID
default1	ON	slot-port, vlan		OFF	-
default2	ON	slot-port, vlan, hostname		OFF	-

The following table describes the labels in this screen.

Table 162 NETWORKING > DHCP > DHCPv4 Relay > DHCP Option 82 Profile

LABEL	DESCRIPTION
Profile Name	This field displays the descriptive name of the profile.
Circuit-ID	This section displays the Circuit ID sub-option including information that is specific to the relay agent (the Switch).
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	This section displays the Remote ID sub-option including information that identifies the relay agent (the Switch).
Enable	This field displays whether the Remote ID sub-option is added to client DHCP requests.
Field	This field displays the information that is included in the Remote ID sub-option.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new entry or edit a selected one.
Delete	Click Delete to remove the selected entries.

49.4.1 Add/Edit a DHCPv4 Option 82 Profile

Use this screen to create DHCPv4 option 82 profiles. Click **Add/Edit**, or select an entry and click **Add/Edit** in the **NETWORKING > DHCP > DHCPv4 Relay > DHCP Option 82 Profile** link to display this screen.

Figure 218 NETWORKING > DHCP > DHCPv4 Relay > DHCP Option 82 Profile > Add/Edit

The screenshot shows a configuration window for a DHCP Option 82 Profile. The 'Name' field is set to 'default1'. In the 'Circuit-ID' section, the 'Enable' checkbox is checked, and the sub-options 'slot-port', 'vlan', and 'hostname' are also checked. There is an empty 'string' field below these options. In the 'Remote-ID' section, 'Enable' is unchecked, and the 'mac' radio button is selected. There is also an empty 'string' field. At the bottom of the window are three buttons: 'Apply' (highlighted in green), 'Clear', and 'Cancel'.

Note: The string of any field in this screen should not contain [?], [|], ['], ["], or [,].

The following table describes the labels in this screen.

Table 163 NETWORKING > DHCP > DHCPv4 Relay > DHCP Option 82 Profile > Add/Edit

LABEL	DESCRIPTION
Name	Enter a descriptive name for the profile for identification purposes. You can use up to 32 printable ASCII characters.
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 SYSTEM > General Setup > 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 printable ASCII characters that the Switch adds into the client DHCP requests.
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 printable ASCII characters for the remote ID information in this field.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

49.5 Configure a DHCPv4 Smart Relay

Use this screen to configure global DHCPv4 relay. Click **NETWORKING > DHCP > DHCPv4 Relay > DHCP Smart Relay** to display the screen as shown.

Figure 219 NETWORKING > DHCP > DHCPv4 Relay > DHCP Smart Relay

The following table describes the labels in this screen.

Table 164 NETWORKING > DHCP > DHCPv4 Relay > DHCP Smart Relay

LABEL	DESCRIPTION
DHCP Smart Relay	
Active	Select this checkbox to enable DHCPv4 relay.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCPv4 server in dotted decimal notation.
Option 82 Profile	Select a pre-defined DHCPv4 option 82 profile that the Switch applies to all ports. The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Port	
Use this section to apply a different DHCP option 82 profile to certain ports on the Switch.	
Index	This field displays a sequential number for each entry.
Port	This field displays the ports to which the Switch applies the settings.
Profile Name	This field displays the DHCP option 82 profile that the Switch applies to the ports.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new entry or edit a selected one.
Delete	Click Delete to remove the selected entries.

49.5.1 Add/Edit DHCPv4 Global Relay Port

Use this screen to apply a different DHCP option 82 profile to certain ports on the Switch. To open this screen, Click **Add/Edit**, or select an entry and click **Add/Edit** in the **Port** section of the **NETWORKING > DHCP > DHCPv4 Relay > DHCP Smart Relay** screen.

Figure 220 NETWORKING > DHCP > DHCPv4 Relay > DHCP Smart Relay > Add/Edit

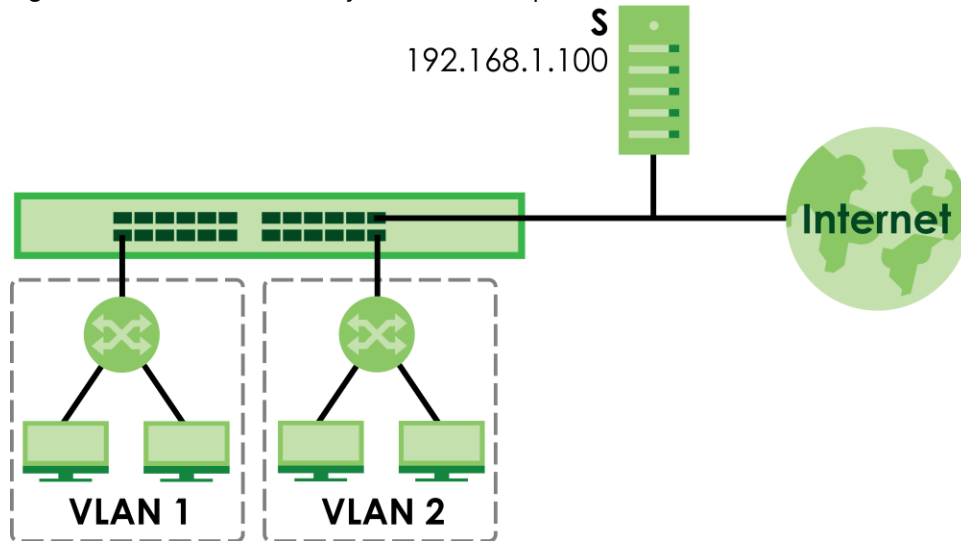
The following table describes the labels in this screen.

Table 165 NETWORKING > DHCP > DHCPv4 Relay > DHCP Smart Relay > Add/Edit

LABEL	DESCRIPTION
Port	Enter the number of ports to which you want to apply the specified DHCP option 82 profile. You can enter multiple ports separated by (no space) comma (,) or hyphen (-). For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to the specified ports. The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server. The profile you select here has priority over the one you select in the NETWORKING > DHCP > DHCPv4 Relay > DHCPv4 Smart Relay 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.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

49.5.2 DHCP Smart 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 (**S**) that services the DHCP clients in both domains.

Figure 221 DHCP Smart Relay Network Example

Configure the **NETWORKING > DHCP > DHCPv4 Relay > DHCP Smart 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. Click **Apply** after you finish the configuration.

Figure 222 DHCP Relay Configuration Example

The screenshot shows the **DHCP Smart Relay** configuration screen. The **Active** toggle is set to **ON**. The **Remote DHCP Server 1** is set to **192.168.1.100**. The **Option 82 Profile** is set to **default1**. The **Apply** button is highlighted.

Port		
	Index	Port
		Profile Name

49.6 DHCPv4 VLAN Setting

Use this screen to configure your DHCP settings based on the VLAN domain of the DHCP clients. Click **NETWORKING > DHCP > DHCPv4 Relay > DHCP Relay VLAN Setting** to display the screen as shown.

Figure 223 NETWORKING > DHCP > DHCPv4 Relay > DHCP Relay VLAN Setting

The following table describes the labels in this screen.

Table 166 NETWORKING > DHCP > DHCPv4 Relay > DHCP Relay VLAN Setting

LABEL	DESCRIPTION
DHCP Relay VLAN Setting	
VID	This field displays the ID number of the VLAN group to which this DHCP settings apply.
Remote DHCP Server	This displays the IP address of a DHCP server in dotted decimal notation.
Source Address	This field displays the source IP address you configured for DHCP requests from clients on this VLAN.
Profile Name	This field displays the DHCP option 82 profile that the Switch applies to this VLAN.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new entry or edit a selected one.
Delete	Click Delete to remove the selected entries.
Port	
Use this section to apply a different DHCP option 82 profile to certain ports in a VLAN.	
Index	This field displays a sequential number for each entry. Click an index number to change the settings.
VID	This field displays the VLAN to which the ports belongs.
Port	This field displays the ports to which the Switch applies the settings.
Profile Name	This field displays the DHCP option 82 profile that the Switch applies to the ports in this VLAN.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new entry or edit a selected one.
Delete	Click Delete to remove the selected entries.

49.6.1 Add/Edit DHCPv4 VLAN Setting

Use this screen to add/edit your DHCP settings based on the VLAN domain of the DHCP clients. Click the **Add/Edit** button in the **DHCP Relay VLAN Setting** section of the **NETWORKING > DHCP > DHCPv4 Relay > DHCP Relay VLAN Setting** screen to access this screen.

Note: You must set up a management IP address for each VLAN that you want to configure DHCP settings for on the Switch.

Figure 224 NETWORKING > DHCP > DHCPv4 Relay > DHCP Relay VLAN Setting > Add/Edit (DHCP Relay VLAN Setting)

The screenshot shows a configuration window with the following fields and buttons:

- VID**: A text input field.
- Remote DHCP Server 1**: A text input field with the value 0.0.0.0.
- Remote DHCP Server 2**: A text input field with the value 0.0.0.0.
- Remote DHCP Server 3**: A text input field with the value 0.0.0.0.
- Source Address**: A text input field with the value 0.0.0.0.
- Option 82 Profile**: A dropdown menu.
- Buttons**: Apply (green), Clear (grey), and Cancel (grey).

The following table describes the labels in this screen.

Table 167 NETWORKING > DHCP > DHCPv4 Relay > DHCP Relay VLAN Setting > Add/Edit (DHCP Relay VLAN Setting)

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN to which these DHCP settings apply.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCP server in dotted decimal notation.
Source Address	Enter the source IP address that the Switch adds to DHCP requests from clients on this VLAN before forwarding them. If you leave this field set to 0.0.0.0 , the Switch automatically sets the source IP address of the DHCP requests to the IP address of the interface on which the packet is received. The source IP address helps DHCP clients obtain an appropriate IP address when you configure multiple routing domains on a VLAN.
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.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

49.6.2 Add/Edit DHCPv4 VLAN Port

Use this screen to apply a different DHCP option 82 profile to certain ports in a VLAN. Click the **Add/Edit** button in the **Port** section of the **NETWORKING > DHCP > DHCPv4 Relay > DHCP Relay VLAN Setting** screen to access this screen.

Figure 225 NETWORKING > DHCP > DHCPv4 Relay > DHCP Relay VLAN Setting > Add/Edit (Port)

VID

Port

Option 82 Profile

Apply Clear Cancel

The following table describes the labels in this screen.

Table 168 NETWORKING > DHCP > DHCPv4 Relay > DHCP Relay VLAN Setting > Add/Edit (Port)

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN you want to configure here.
Port	Enter the number of ports to which you want to apply the specified DHCP option 82 profile. You can enter multiple ports separated by (no space) comma (,) or hyphen (-). For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to the specified ports in this VLAN. The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server. The profile you select here has priority over the one you select in the NETWORKING > DHCP > DHCPv4 Relay > DHCP Relay VLAN Setting (the DHCP Relay VLAN Setting section)> Add/Edit 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.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

49.7 DHCPv4 Server Status

Click **NETWORKING > DHCP > DHCPv4 Server** in the navigation panel. The **DHCP Server Status** screen displays.

Figure 226 NETWORKING > DHCP > DHCPv4 Server > DHCP Server Status

DHCP Server Status			
DHCP Server Setup			
Index	VID	Server Status	IP Pool Size
1	1	172.21.40.32	15

The following table describes the labels in this screen.

Table 169 NETWORKING > DHCP > DHCPv4 Server > DHCP Server Status

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 view the server configuration details.

Table 169 NETWORKING > DHCP > DHCPv4 Server > DHCP Server Status

LABEL	DESCRIPTION
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.

49.7.1 DHCPv4 Server Status Details

Click an existing index number of a DHCP server configuration in the **NETWORKING > DHCP > DHCPv4 Server > DHCPv4 Server Status** screen to display the screen as shown. Use this screen to view details regarding DHCP server settings configured on the Switch.

Figure 227 NETWORKING > DHCP > DHCPv4 Server > DHCP Server Status > Server Status Details

DHCP Server Status

DHCP Server Setup

[Server Status](#)

> Server Status Details

Server Status Details

Start IP Address

172.21.40.22

End IP Address

172.21.40.36

Subnet Mask

255.255.255.0

Default Gateway

172.21.43.55

Primary DNS Server

0.0.0.0

Secondary DNS Server

0.0.0.0

Lease Time

3 day 0 hour 0 minute

Unavailable Lease Time

1 day 0 hour 0 minute

Address Leases

Index	IP Address	Timer	Hardware Address	Hostname

The following table describes the labels in this screen.

Table 170 NETWORKING > DHCP > DHCPv4 Server > DHCP Server Status > Server Status Details

LABEL	DESCRIPTION
Server Status Details	
This section displays the configuration details of this DHCP server. You can change the DHCP server configuration in the NETWORKING > DHCP > DHCPv4 Server > DHCP Server Setup screen.	
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.

Table 170 NETWORKING > DHCP > DHCPv4 Server > DHCP Server Status > Server Status Details

LABEL	DESCRIPTION
Secondary DNS Server	This field displays the secondary DNS server value sent to clients from this DHCP server instance.
Lease Time	This field displays the amount of time that the IP address is valid.
Unavailable Lease Time	This field display the lease time of the unavailable IP addresses occupied by unknown hosts.
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.

49.8 DHCPv4 Server Setup

Use this screen to view and configure the DHCP server settings. The Switch serves as a DHCP server (DHCP server mode) when you add a configuration entry in this screen. Click **NETWORKING > DHCP > DHCPv4 Server > DHCP Server Setup** to display the screen as shown.

Note: You must set up a management IP address for each VLAN that you want to configure DHCP Server settings for on the Switch.

Note: You cannot enable configurations simultaneously in the **NETWORKING > DHCP > DHCPv4 Relay > DHCP Relay VLAN Setting** and **NETWORKING > DHCP > DHCPv4 Server > DHCP Server Setup** screens.

Figure 228 NETWORKING > DHCP > DHCPv4 Server > DHCP Server Setup

The screenshot shows the 'DHCP Server Setup' interface. At the top, there's a header 'DHCP Server Setup'. Below it is a table with three columns: 'VID', 'Starting Address', and 'Size of IP Pool'. A checkbox is located to the left of the 'VID' column. To the right of the table, there are two buttons: a green '+ Add/Edit' button and a red 'Delete' button.

The following table describes the labels in this screen.

Table 171 NETWORKING > DHCP > DHCPv4 Server > DHCP Server Setup

LABEL	DESCRIPTION
VID	This field displays the ID number of the VLAN group to which this DHCP settings apply.
Starting Address	This field displays the starting IP address of the IP address pool configured for the DHCP server.
Size of IP Pool	This field displays the IP address pool size of the DHCP server.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.

Table 171 NETWORKING > DHCP > DHCPv4 Server > DHCP Server Setup (continued)

LABEL	DESCRIPTION
Add/Edit	Click Add/Edit to add a new entry or edit a selected one.
Delete	Click Delete to remove the selected entries.

49.8.1 Add/Edit DHCPv4 Server

Use this screen to configure the DHCP server settings. Click **Add/Edit**, or select an entry and click **Add/Edit** in the **NETWORKING > DHCP > DHCPv4 Server > DHCP Server Setup** to display this screen.

Figure 229 NETWORKING > DHCP > DHCPv4 Server > DHCP Server Setup > Add/Edit

VID

Client IP Pool Starting Address

Size of Client IP Pool

IP Subnet Mask

Default Gateway

Primary DNS Server

Secondary DNS Server

Lease Time
☐ Infinite
☒ Days Hours Minutes

Unavailable Lease Time
 Days Hours Minutes

Apply **Clear** **Cancel**

The following table describes the labels in this screen.

Table 172 NETWORKING > DHCP > DHCPv4 Server > DHCP Server Setup > Add/Edit

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN to which these DHCP settings apply.
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.

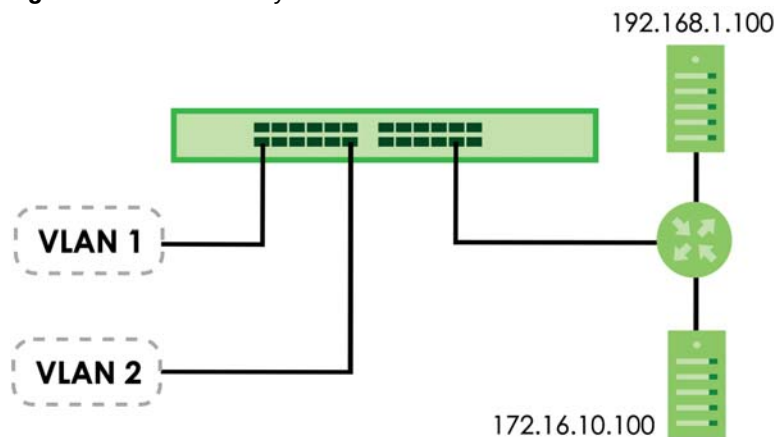
Table 172 NETWORKING > DHCP > DHCPv4 Server > DHCP Server Setup > Add/Edit (continued)

LABEL	DESCRIPTION
Lease Time	Select Infinite to have the binding always valid. Select the second radio button to set up the binding's valid days, hours and minutes.
Unavailable Lease Time	Unavailable lease time is the lease time of an IP address that is distributed by other unknown DHCP servers to other devices. A DHCP client rejects the IP address assigned by the Switch when it discovers the assigned IP is already in use by other devices. When an IP is in use by other devices, the Switch cannot assign this unavailable IP to the Switch's DHCP client. The Switch will mark the IP as an unavailable IP and removes it from the IP address pool. The Switch will not assign the unavailable IP to DHCP clients until Unavailable Lease Time expires. Set up the days, hours, and minutes of unavailable lease time.

49.8.2 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 230 DHCP Relay for Two VLANs



For the example network, add two entries in **DHCP Relay VLAN Setting** section of the **NETWORKING > DHCP > DHCPv4 Relay > DHCP Relay VLAN Setting** screen as shown.

Figure 231 DHCP Relay for Two VLANs Configuration Example

Relay Status DHCP Option 82 Profile DHCP Smart Relay **DHCP Relay VLAN Setting**

DHCP Relay VLAN Setting

[+ Add/Edit](#) [Delete](#)

☐	VID	Remote DHCP Server	Profile Name
☐	1	192.168.1.100	
☐	2	172.16.10.100	

Port

[+ Add/Edit](#) [Delete](#)

☐	Index	VID	Port	Profile Name

49.9 DHCP Server Guard

Use this screen to specify whether ports are trusted or untrusted ports for DHCP packets. Click **NETWORKING > DHCP > DHCP Server Guard > DHCP Server Guard** in the navigation panel to display the screen as shown.

Figure 232 NETWORKING > DHCP > DHCP Server Guard > DHCP Server Guard

DHCP Server Guard

DHCP Server Guard

Active ☐ OFF

Port Setting

Port	Trusted State
*	Untrusted ▼
1	Untrusted ▼
2	Untrusted ▼
3	Untrusted ▼
4	Untrusted ▼
5	Untrusted ▼
6	Untrusted ▼
7	Untrusted ▼

Apply Cancel

The following table describes the labels in this screen.

Table 173 NETWORKING > DHCP > DHCP Server Guard > DHCP Server Guard

LABEL	DESCRIPTION
DHCP Server Guard	
Active	Enable the switch button to enable DHCP Server Guard.
Port Setting	
Port	The port number identifies the port you are configuring.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Trusted State	Select whether this port is a trusted port (Trusted) or an untrusted port (Untrusted). The Switch does not discard DHCP packets on trusted ports for any reason. The Switch discards DHCP packets from untrusted ports when the packet is a DHCP server packet (for example, OFFER, ACK, or NACK).
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to their last saved values.

CHAPTER 50

Static Route

50.1 Static Routing Overview

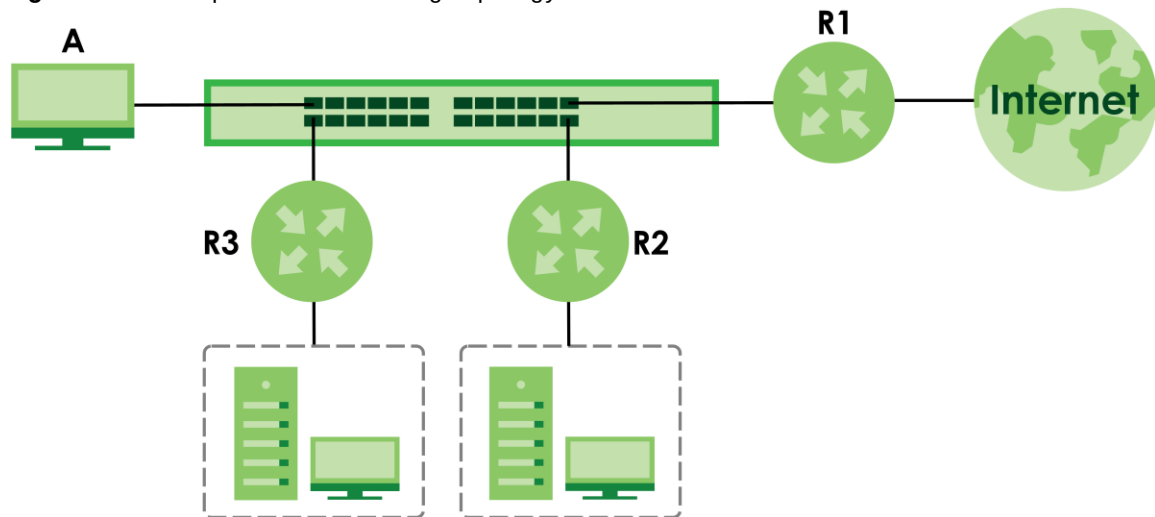
This chapter shows you how to configure static routes.

The Switch uses IP for communication with management computers, for example using HTTP, Telnet, SSH, or SNMP. Use IP static routes to have the Switch respond to remote management stations that are not reachable through the default gateway. The Switch can also use static routes to send data to a server or device that is not reachable through the default gateway, for example when sending SNMP traps or using ping to test IP connectivity.

The Switch usually uses the default gateway to route outbound traffic from computers on the LAN to the Internet. To have the Switch send data to devices not reachable through the default gateway, use static routes.

For example, the next figure shows a computer (**A**) connected to the Switch. The Switch routes most traffic from **A** to the Internet through the Switch's default gateway (**R1**). You create one static route to connect to services offered by your ISP behind router **R2**. You create another static route to communicate with a separate network behind a router **R3** connected to the Switch.

Figure 233 Example of Static Routing Topology



50.1.1 What You Can Do

Use the **IPv4 Static Route** screen ([Section 50.2 on page 335](#)) to configure and enable an IPv4 static route.

50.2 IPv4 Static Route

Click **NETWORKING > Static Routing > IPv4 Static Route > IPv4 Static Route** to display the screen as shown.

Figure 234 NETWORKING > Static Routing > IPv4 Static Route > IPv4 Static Route

The following table describes the related labels you use to create a static route.

Table 174 NETWORKING > Static Routing > IPv4 Static Route > IPv4 Static Route

LABEL	DESCRIPTION
Index	This field displays the index number of the route.
Active	This field displays whether the static route is activated or not.
Name	This field displays the descriptive name for this route. This is for identification purposes only.
Destination Address	This field displays the IP network address of the final destination.
Subnet Mask	This field displays the subnet mask for this destination.
Gateway Address	This field displays the IP address of the gateway. The gateway is an immediate neighbor of your Switch that will forward the packet to the destination.
Metric	This field displays the cost of transmission for routing purposes.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new entry or edit a selected one.
Delete	Click Delete to remove the selected entries.

50.2.1 Add/Edit IPv4 Static Route

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **NETWORKING > Static Routing > IPv4 Static Route > IPv4 Static Route** screen to display this screen.

Figure 235 NETWORKING > Static Routing > IPv4 Static Route > IPv4 Static Route > Add/Edit

The following table describes the related labels you use to create a static route.

Table 175 NETWORKING > Static Routing > IPv4 Static Route > IPv4 Static Route > Add/Edit

LABEL	DESCRIPTION
Active	This field allows you to activate or deactivate this static route.
Name	Enter a descriptive name (up to 10 printable ASCII characters except [?], [], ['], ["], or [,]) for identification purposes.
Destination IP Address	This parameter specifies the IP network address of the final destination.
IP Subnet Mask	Enter the subnet mask for this destination. Routing is always based on network number. If you need to specify a route to a single host, use a subnet mask of 255.255.255.255 in the subnet mask field to force the network number to be identical to the host ID.
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your Switch that will forward the packet to the destination. The gateway must be a router on the same segment as your Switch.
Metric	The metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

CHAPTER 51

SECURITY

The following chapters introduces the configurations of the links under the **SECURITY** navigation panel.

Quick links to chapters:

- [AAA](#)
- [Access Control](#)
- [Classifier](#)
- [Policy Rule](#)
- [Anti-Arpscan](#)
- [BPDU Guard](#)
- [Storm Control](#)
- [Error-Disable](#)
- [IP Source Guard](#)
- [DHCP Snooping](#)
- [ARP Inspection](#)
- [Port Authentication](#)
- [Port Security](#)

CHAPTER 52

AAA

52.1 Authentication, Authorization and Accounting (AAA)

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

The external servers that perform authentication, authorization and accounting functions are known as AAA servers (**S**). The Switch supports RADIUS (Remote Authentication Dial-In User Service) and TACACS+ (Terminal Access Controller Access-Control System Plus) as the external authentication, authorization, and accounting server on clients (**C**).

Figure 236 AAA Server



52.1.1 What You Can Do

- use the **RADIUS Server Setup** screen ([Section 52.2 on page 339](#)) to configure your RADIUS server settings.
- Use the **TACACS+ Server Setup** screen ([Section 52.3 on page 341](#)) to configure your TACACS+ authentication settings.
- Use the **AAA Setup** screen ([Section 52.4 on page 343](#)) to configure authentication, authorization and accounting settings, such as the methods used to authenticate users accessing the Switch and which database the Switch should use first.

52.1.2 What You Need to Know

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

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

Accounting is the process of recording what a user is doing. The Switch can use an external server to

track when users log in, log out, execute commands and so on. Accounting can also record system related actions such as boot up and shut down times of the Switch.

Local User Accounts

By storing user profiles locally on the Switch, your Switch is able to authenticate and authorize users without interacting with a network AAA server. However, there is a limit on the number of users you may authenticate in this way.

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 176 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.

52.2 RADIUS Server Setup

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

Figure 237 SECURITY > AAA > RADIUS Server Setup > RADIUS Server Setup

RADIUS Server Setup

Authentication Server

Mode: ▼

Timeout: seconds

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

Accounting Server

Timeout: seconds

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

Attribute

NAS-IP-Address:

The following table describes the labels in this screen.

Table 177 SECURITY > AAA > RADIUS Server Setup > RADIUS Server Setup

LABEL	DESCRIPTION
Authentication Server Use this section to configure your RADIUS authentication settings.	
Mode	This field is only valid if you configure multiple RADIUS servers. Select index-priority and the Switch tries to authenticate with the first configured RADIUS server, if the RADIUS server does not respond then the Switch tries to authenticate with the second RADIUS server. Select round-robin to alternate between the RADIUS servers that it sends authentication requests to.
Timeout	Specify the amount of time in seconds that the Switch waits for an authentication request response from the RADIUS server. If you are using 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.
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 .
Index	This is a read-only number representing a RADIUS server entry.
IP Address	Enter the IPv4 address of an external RADIUS server.
UDP Port	The default port of a RADIUS server for authentication is 1812 . You need not change this value unless your network administrator instructs you to do so.

Table 177 SECURITY > AAA > RADIUS Server Setup > RADIUS Server Setup (continued)

LABEL	DESCRIPTION
Shared Secret	Specify a password (up to 32 alphanumeric characters except [?], [], ['], ["], [space], or [,]) 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.
Encrypted Shared Secret	This displays the encrypted shared secret in '**' format if you enabled Server Key Encryption in SECURITY > AAA > AAA Setup > AAA Setup. Note: If you forget the key you set, simply reset the key in the Shared Secret field. If a key is encrypted, it will remain in the encrypted format even if you later disable Server Key Encryption in SECURITY > AAA > AAA Setup > AAA Setup. Note: The shared secret displayed in this field does not present the actual length of the shared secret.
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.
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 .
Index	This is a read-only number representing a RADIUS accounting server entry.
IP Address	Enter the IPv4 address of an external RADIUS accounting server.
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 except [?], [], ['], ["], [space], or [,]) 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.
Encrypted Shared Secret	This displays the encrypted shared secret in '**' format if you enabled Server Key Encryption in SECURITY > AAA > AAA Setup > AAA Setup. Note: If you forget the key you set, simply reset the key in the Shared Secret field. If a key is encrypted, it will remain in the encrypted format even if you later disable Server Key Encryption in SECURITY > AAA > AAA Setup > AAA Setup. Note: The shared secret displayed in this field does not present the actual length of the shared secret.
Attribute Use this section to define the RADIUS server attribute for its account.	
NAS-IP-Address	Enter the IP address of the NAS (Network Access Server).
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

52.3 TACACS+ Server Setup

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

Figure 238 SECURITY > AAA > TACACS+ Server Setup > TACACS+ Server Setup

TACACS+ Server Setup

Authentication Server

Mode index-priority ▼
 Timeout 30 seconds

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

Accounting Server

Timeout 30 seconds

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

Apply
Cancel

The following table describes the labels in this screen.

Table 178 SECURITY > AAA > TACACS+ Server Setup > 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.
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 .
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.

Table 178 SECURITY > AAA > TACACS+ Server Setup > TACACS+ Server Setup (continued)

LABEL	DESCRIPTION
Shared Secret	Specify a password (up to 32 alphanumeric characters except [?], [], ['], ["], [space], or [,]) 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.
Encrypted Shared Secret	This displays the encrypted shared secret in '*' format if you enabled Server Key Encryption in SECURITY > AAA > AAA Setup > AAA Setup. Note: If you forget the key you set, simply reset the key in the Shared Secret field. If a key is encrypted, it will remain in the encrypted format even if you later disable Server Key Encryption in SECURITY > AAA > AAA Setup > AAA Setup. Note: The shared secret displayed in this field does not present the actual length of the shared secret.
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.
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 .
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 except [?], [], ['], ["], [space], or [,]) 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.
Encrypted Shared Secret	This displays the encrypted shared secret in '*' format if you enabled Server Key Encryption in SECURITY > AAA > AAA Setup > AAA Setup. Note: If you forget the key you set, simply reset the key in the Shared Secret field. If a key is encrypted, it will remain in the encrypted format even if you later disable Server Key Encryption in SECURITY > AAA > AAA Setup > AAA Setup. Note: The shared secret displayed in this field does not present the actual length of the shared secret.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

52.4 AAA Setup

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

Figure 239 SECURITY > AAA > AAA Setup > AAA Setup

AAA Setup

Server Key Encryption

Active ☐ OFF

Authentication

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

Authorization

Type	Active	Console	Method
Exec	☐ OFF	☐	radius
Dot1x	☐ OFF	-	radius

Accounting

Update Period minutes

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

The following table describes the labels in this screen.

Table 179 SECURITY > AAA > AAA Setup > AAA Setup

LABEL	DESCRIPTION
Server Key Encryption	
Use this section to configure server key encryption settings.	
Active	Enable the switch button to enable server key (shared secret) encryption for RADIUS server and TACACS+ server for security enhancement. The shared secret will be stored on the Switch in an encrypted format and displayed as '*' in the SECURITY > AAA > RADIUS Server Setup > RADIUS Server Setup and SECURITY > AAA > TACACS+ Server Setup > TACACS+ Server Setup screens.

Table 179 SECURITY > AAA > AAA Setup > AAA Setup (continued)

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 through 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 through the external servers.
Login	These fields specify which database the Switch should use (first, second and third) to authenticate administrator accounts (users for Switch management). Configure the local user accounts in the SYSTEM > Logins > 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 SYSTEM > Logins > Logins screen. Select radius to have the Switch check the administrator accounts configured through the RADIUS Server. Select tacacs+ to have the Switch check the administrator accounts configured through the TACACS+ Server.
Authorization	
Use this section to configure authorization settings on the Switch.	
Type	Set whether the Switch provides the following services to a user. • Exec: Allow an administrator which logs into the Switch through Telnet or SSH to have a different access privilege level assigned through the external server. • Dot1x: Allow an IEEE 802.1x client to have different bandwidth limit or VLAN ID assigned through the external server.
Active	Enable the switch button to activate authorization for a specified event type.
Console	Select this to allow an administrator which logs in the Switch through the console port to have different access privilege level assigned through 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.	

Table 179 SECURITY > AAA > AAA Setup > AAA Setup (continued)

LABEL	DESCRIPTION
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 servers: • System – Configure the Switch to send information when the following system events occur: system boots up, system shuts down, system accounting is enabled, system accounting is disabled. • Exec – Configure the Switch to send information when an administrator logs in and logs out through the console port, telnet or SSH. • Dot1x – Configure the Switch to send information when an IEEE 802.1x client begins a session (authenticates through 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	Enable the switch button to activate accounting for a specified event type.
Broadcast	Select this to have the Switch send accounting information to all configured accounting servers at the same time. If you do not select this and you have two accounting servers set up, then the Switch sends information to the first accounting server and if it does not get a response from the accounting server then it tries the second accounting server.
Mode	The Switch supports two modes of recording login events. Select: • start-stop – to have the Switch send information to the accounting server when a user begins a session, during a user's session (if it lasts past the Update Period), and when a user ends a session. • stop-only – to have the Switch send information to the accounting server only when a user ends a session.
Method	Select whether you want to use radius or tacacs+ for accounting of specific types of events. tacacs+ is the only method for recording Commands type of event.
Privilege	This field is only configurable for Commands type of event. Select the threshold command privilege level for which the Switch should send accounting information. The Switch will send accounting information when commands at the level you specify and higher are executed on the Switch.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

52.5 Technical Reference

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

52.5.1 Vendor Specific Attribute

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

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

- Limit bandwidth on incoming or outgoing traffic for the port the user connects to.
- Assign account privilege levels 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 through 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 52.4 on page 343](#)).

Table 180 Supported VSAs

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

52.5.1.1 Tunnel Protocol Attribute

You can configure tunnel protocol attributes on the RADIUS server (refer to your RADIUS server documentation) to assign a port on the Switch to a VLAN based on IEEE 802.1x authentication. The port VLAN settings are fixed and untagged. This will also set the port's VID. The following table describes the values you need to configure. Note that these attributes only work when you enable authorization (see [Section 52.4 on page 343](#)).

Table 181 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.

52.5.2 Supported RADIUS Attributes

Remote Authentication Dial-In User Service (RADIUS) attributes are data used to define specific authentication elements in a user profile, which is stored on the RADIUS server. This 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 functions on the Switch. In cases where the attribute has a specific format associated with it, the format is specified.

52.5.3 Attributes Used for Authentication

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

52.5.3.1 Attributes Used for Authenticating Privilege Access

User-Name

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

User-Password

NAS-Identifier

NAS-IP-Address

52.5.3.2 Attributes Used to Login Users

User-Name

User-Password

NAS-Identifier

NAS-IP-Address

52.5.3.3 Attributes Used by the IEEE 802.1x Authentication

User-Name
 NAS-Identifier
 NAS-IP-Address
 NAS-Port
 NAS-Port-Type
 – This value is set to **Ethernet(15)** on the Switch.
 Calling-Station-Id
 Frame-MTU
 EAP-Message
 State
 Message-Authenticator

52.5.4 Attributes Used for Accounting

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

52.5.4.1 Attributes Used for Accounting System Events

NAS-IP-Address
 NAS-Identifier
 Acct-Status-Type
 Acct-Session-ID
 – The format of Acct-Session-Id is **date+time+8-digit sequential number**, for example, 2007041917210300000001. (date: 2007/04/19, time: 17:21:03, serial number: 00000001)
 Acct-Delay-Time

52.5.4.2 Attributes Used for Accounting Exec Events

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

Table 182 RADIUS Attributes – Exec Events through 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	✓	✓	✓

Table 182 RADIUS Attributes – Exec Events through Console (continued)

ATTRIBUTE	START	INTERIM-UPDATE	STOP
Acct-Session-Time		✓	✓
Acct-Terminate-Cause			✓

Table 183 RADIUS Attributes – Exec Events through 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			✓

52.5.4.3 Attributes Used for Accounting IEEE 802.1x Events

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

Table 184 RADIUS Attributes – Exec Events through 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		✓	✓

Table 184 RADIUS Attributes – Exec Events through Console (continued)

ATTRIBUTE	START	INTERIM-UPDATE	STOP
Acct-Output-Packets		✓	✓
Acct-Terminate-Cause			✓
Acct-Input-Gigawords		✓	✓
Acct-Output-Gigawords		✓	✓

CHAPTER 53

Access Control

53.1 Access Control Overview

This chapter describes how to control access to the Switch.

A console port and FTP are allowed one session each, Telnet and SSH share nine sessions, up to five web sessions (five different user names and passwords) and/or limitless SNMP access control sessions are allowed.

Table 185 Access Control Overview

Console Port	SSH	Telnet	FTP	Web	SNMP
One session	Share up to 9 sessions		One session	Up to 5 accounts	No limit

A console port access control session and Telnet access control session cannot coexist when multi-login is disabled. See the CLI Reference Guide for more information on disabling multi-login.

53.1.1 What You Can Do

- Use the **Service Access Control** screen ([Section 53.2 on page 352](#)) to decide what services you may use to access the Switch.
- Use the **Remote Management** screen ([Section 53.3 on page 353](#)) to specify a group of one or more “trusted computers” from which an administrator may use a service to manage the Switch.
- Use the **Account Security** screen ([Section 53.4 on page 355](#)) to encrypt all passwords configured in the Switch. You can also display the authentication, authorization, external authentication server information (RADIUS or TACACS+), system and SNMP user account information in the configuration file saved.

53.2 Service Access Control

Service Access Control allows you to decide what services you may use to access the Switch. You may also change the default service port and configure “trusted computers” for each service in the **SECURITY > Access Control > Remote Management > Remote Management** screen (see [Section 53.3 on page 353](#) for more information). Click **SECURITY > Access Control > Service Access Control > Service Access Control** to display the following screen.

Figure 240 SECURITY > Access Control > Service Access Control > Service Access Control

Services	Active	Service Port	Timeout	Login Timeout
Console	☐ ON		5 Minutes	
Telnet	☐ OFF	23	5 Minutes	150 Seconds
SSH	☐ ON	22		
FTP	☐ ON	21	5 Minutes	
HTTP	☐ ON	80	5 Minutes	☒ Redirect to HTTPS
HTTPS	☐ ON	443		
ICMP	☐ ON			
SNMP	☐ OFF			

The following table describes the fields in this screen.

Table 186 SECURITY > Access Control > Service Access Control > Service Access Control

LABEL	DESCRIPTION
Services	Services you may use to access the Switch are listed here.
Active	Enable the switch button for the corresponding services that you want to allow to access the Switch.
Service Port	For Telnet, SSH, FTP, HTTP or HTTPS services, you may change the default service port by typing the new port number in the Service Port field. If you change the default port number then you will have to let people (who wish to use the service) know the new port number for that service.
Timeout	Enter how many minutes (from 1 to 255) a management session can be left idle before the session times out. After it times out you have to log in with your password again. Very long idle timeouts may have security risks.
Login Timeout	The Telnet or SSH server do not allow multiple user logins at the same time. Enter how many seconds (from 30 to 300 seconds) a login session times out. After it times out you have to start the login session again. Very long login session timeouts may have security risks. For example, if User A attempts to connect to the Switch (through SSH), but during the login stage, do not enter the user name and/or password, User B cannot connect to the Switch (through SSH) before the Login Timeout for User A expires (default 150 seconds).
Redirect to HTTPS	This option allows your web browser to automatically redirect to a secure page, from HTTP to HTTPS (secure hypertext transfer protocol). SSL (Secure Sockets Layer) in HTTPS encrypts the transferred data by changing plain text to random letters and numbers.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

53.3 Remote Management (IPv4)

Use this screen to specify a group of one or more “trusted computers” from which an administrator may use a service to manage the Switch.

Click **SECURITY > Access Control > Remote Management > Remote Management** to view the screen as shown next.

Figure 241 SECURITY > Access Control > Remote Management > Remote Management IPv4

Remote Management IPv4

Secured Client Setup

Entry	Active	Start Address	End Address	Telnet	FTP	HTTP	ICMP	SNMP	SSH	HTTPS
1	☒ ON	0.0.0.0	0.0.0.0	☒	☒	☒	☒	☒	☒	☒
2	☐ OFF	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
3	☐ OFF	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
4	☐ OFF	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
5	☐ OFF	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
6	☐ OFF	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
7	☐ OFF	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
8	☐ OFF	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
9	☐ OFF	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
10	☐ OFF	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
11	☐ OFF	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
12	☐ OFF	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
13	☐ OFF	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
14	☐ OFF	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
15	☐ OFF	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
16	☐ OFF	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐

Apply **Cancel**

The following table describes the labels in this screen.

Table 187 SECURITY > Access Control > Remote Management > Remote Management IPv4

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	Enable the switch button to activate this secured client set. Clear the checkbox if you wish to temporarily disable the set without deleting it.
Start Address	Configure the IPv4 address range of trusted computers from which you can manage this Switch.
End Address	The Switch checks if the client IPv4 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.

53.4 Account Security

Use this screen to encrypt all passwords configured in the Switch. This setting will affect how the password is shown (as plain text or encrypted text) in the configuration file saved in **MAINTENANCE > Configuration > Save Configuration > Save Configuration**.

Note: Make sure to enable **Password Encryption** to avoid displaying passwords as plain text in the configuration file.

Note: Be careful who can access configuration files with plain text passwords!

Password Encryption encrypts all passwords in the configuration file. However, if you want to show some passwords as plain text in the configuration file, select them as below:

- **Authentication** information configured for **Authentication** in the **SECURITY > AAA > AAA Setup > AAA Setup** screen (**Method 1/2/3** setting in the **Privilege Enable** and **Login** fields).
- **Authorization** information configured for **Authorization** in the **SECURITY > AAA > AAA Setup > AAA Setup** screen (**Active/Console/Method** setting in the **Exec** and **Dot1x** fields).
- **Server** information configured for **Authentication Server** in the **SECURITY > AAA > RADIUS Server Setup > RADIUS Server Setup** screen, and for **Authentication Server** in the **SECURITY > AAA > TACACS+ Server Setup > TACACS+ Server Setup** screen (**Mode/Timeout** fields).
- **System** account information configured in the Switch (admin, user login name, and password).
- **SNMP** user account information configured in the **SYSTEM > SNMP > SNMP User** screen (password for SNMP user authentication in the **Authentication** field, and the password for the encryption method for SNMP communication in the **Privacy** field).

Note: The passwords will appear as encrypted text when **Password Encryption** is **Active**.

Click **SECURITY > Access Control > Account Security > Account Security** to view the screen as shown next.

Figure 242 SECURITY > Access Control > Account Security > Account Security

Account Security

Account Security

Password Encryption ☐ OFF

Apply **Cancel**

Display

☒ **AAA**

☐ Authentication ☐ Authorization ☐ Server

☒ **User**

☐ System ☐ SNMP

Apply **Cancel**

The following table describes the labels in this screen.

Table 188 SECURITY > Access Control > Account Security > Account Security

LABEL	DESCRIPTION
Account Security	
Password Encryption	Click the switch to the right to encrypt all passwords configured on the Switch (default is enabled). This displays the password as encrypted text, in a saved configuration file. Otherwise, the passwords configured on the Switch are displayed in plain text.
Apply	Click Apply to save your changes for Account Security to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring Account Security afresh.
Display	
AAA	Select which specific information to display in plain text, in the saved configuration file. • Authentication • Authorization • Server
User	Select which user account information to display in plain text, in the saved configuration file. • System • SNMP
Apply	Click Apply to save your changes for Display to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring Display afresh.

53.5 Technical Reference

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

53.5.1 SSH Overview

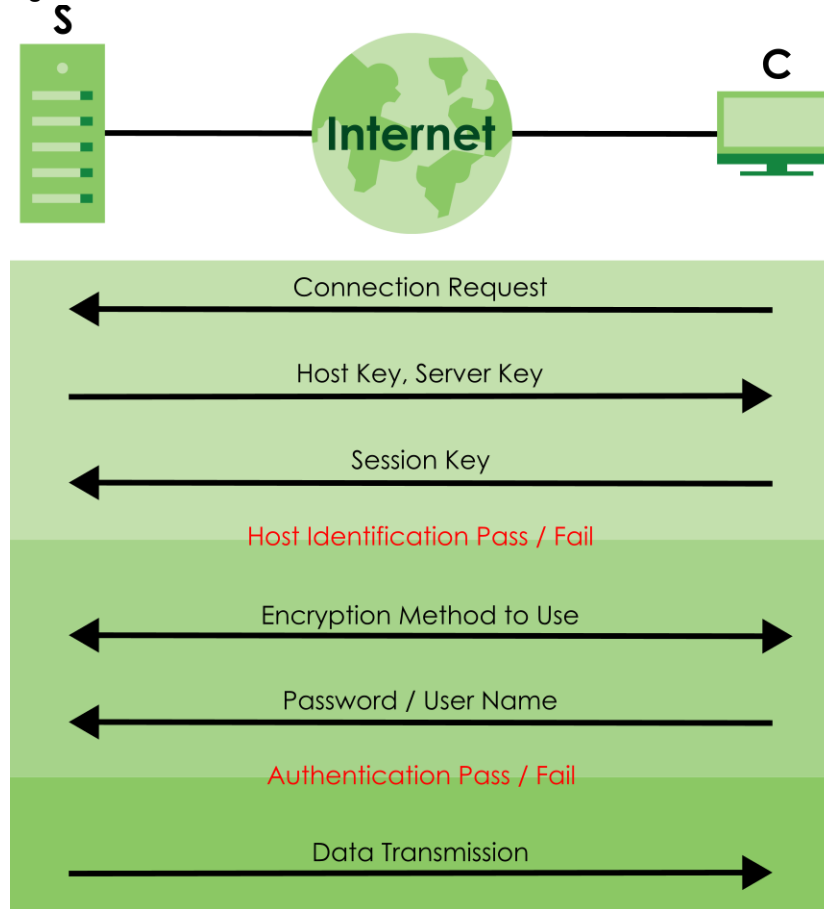
Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication (**SC**) protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

Figure 243 SSH Communication Example



53.5.1.1 How SSH Works

The following table summarizes how a secure connection is established between two remote hosts, SSH server (**S**) and SSH client (**C**).

Figure 244 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.

53.5.1.2 SSH Implementation on the Switch

Your Switch supports SSH version 2 using RSA authentication and the AES encryption method. 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.

53.5.1.3 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the Switch over SSH.

53.5.2 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).

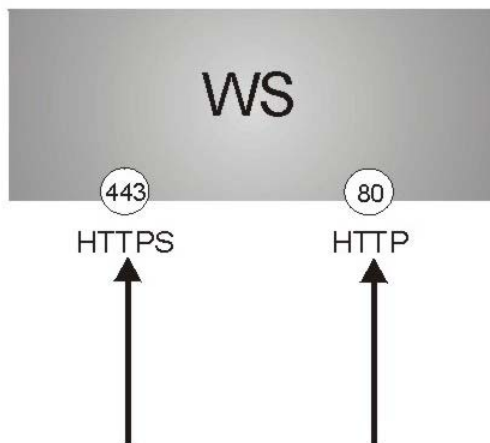
It relies upon certificates, public keys, and private keys.

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 245 HTTPS Implementation



Note: If you disable HTTP in the Service Access Control screen, then the Switch blocks all HTTP connection attempts.

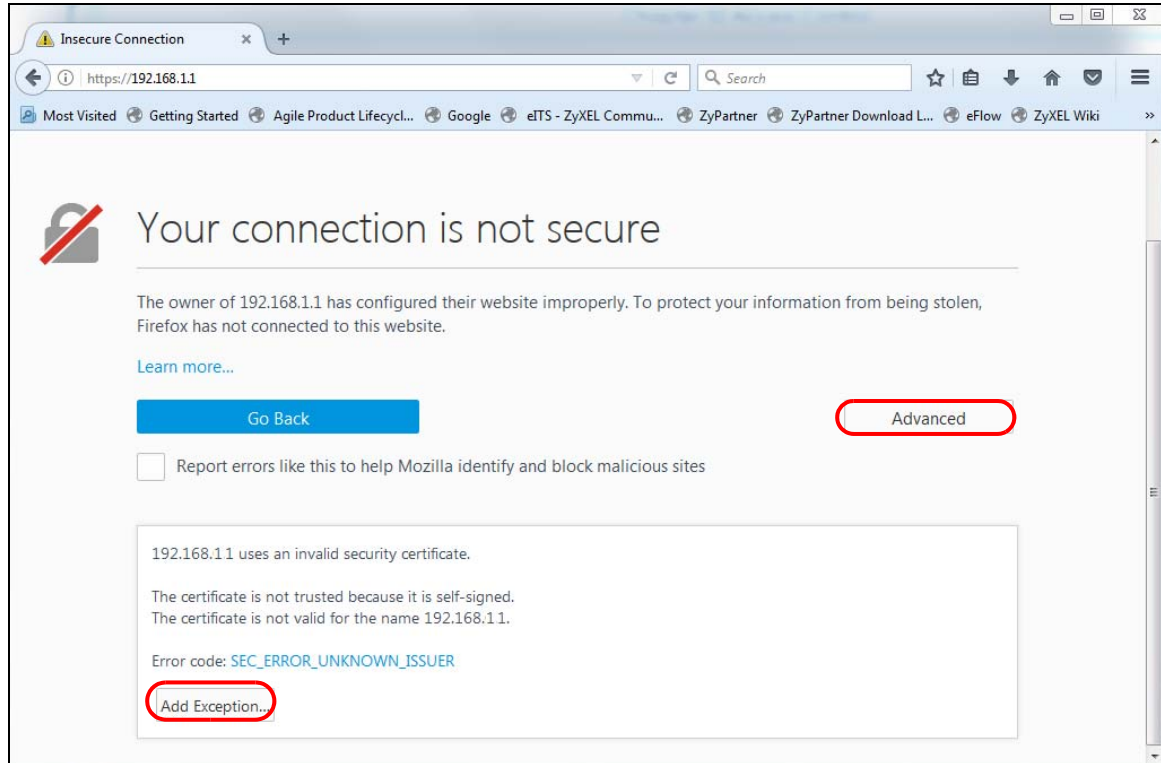
53.5.2.1 HTTPS Example

If you have not changed the default HTTPS port on the Switch, then in your browser enter "https://Switch IP Address/" as the web site address where "Switch IP Address" is the IP address or domain name of the Switch you wish to access.

Mozilla Firefox Warning Messages

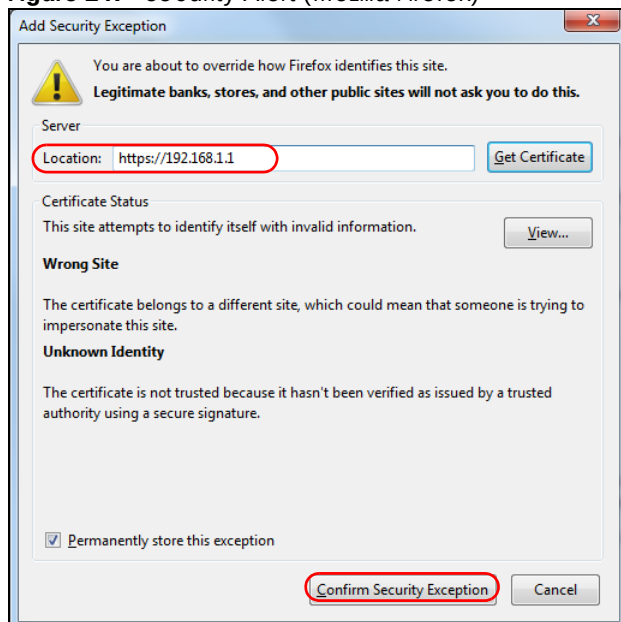
When you attempt to access the Switch HTTPS server, a **Your connection is not secure** screen may display. If that is the case, click **I Understand the Risks** and then the **Add Exception...** button.

Figure 246 Security Alert (Mozilla Firefox)



Confirm the HTTPS server URL matches. Click **Confirm Security Exception** to proceed to the Web Configurator login screen.

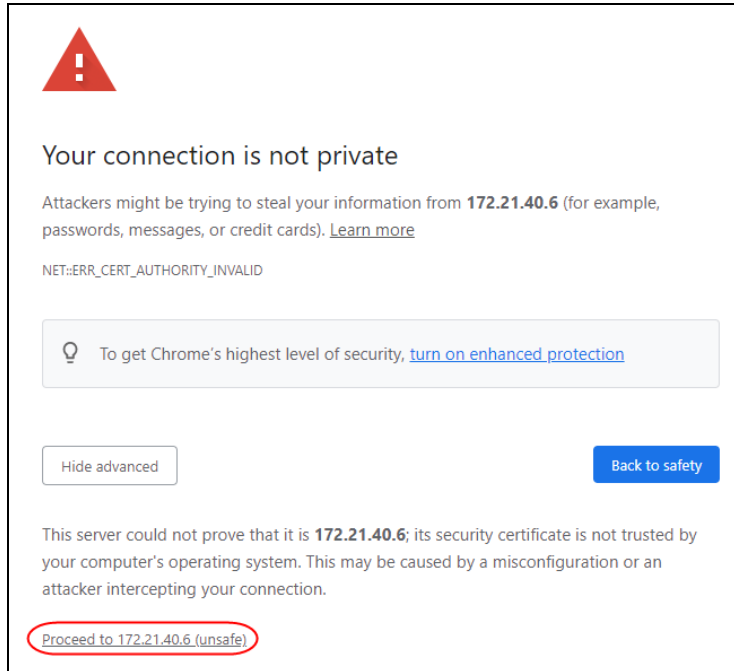
Figure 247 Security Alert (Mozilla Firefox)



53.5.3 Google Chrome Warning Messages

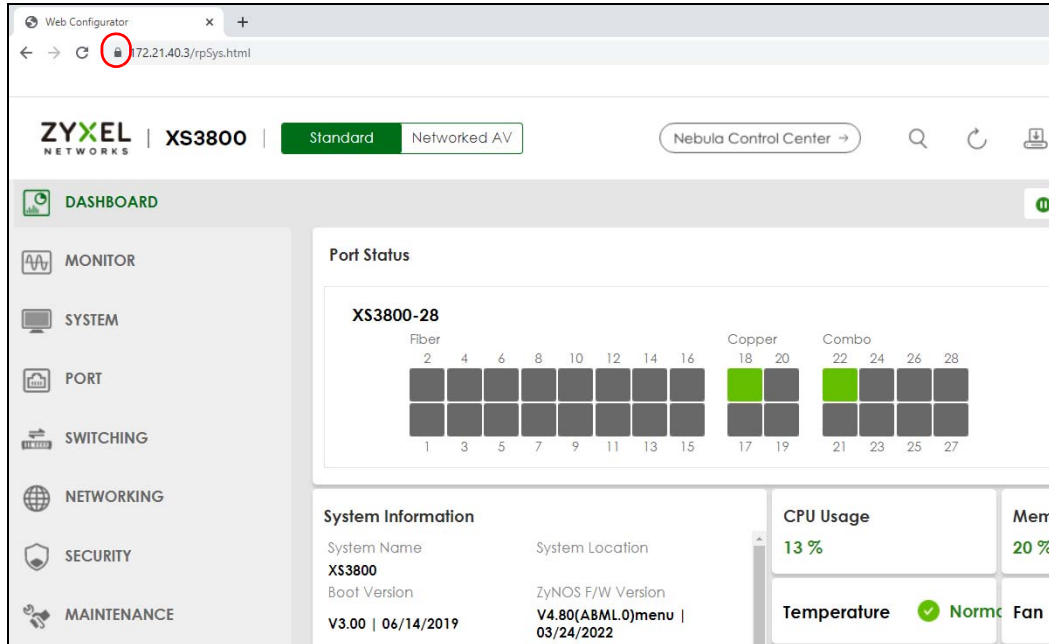
When you attempt to access the Switch HTTPS server, a **Your connection is not private** screen may display. If that is the case, click **Advanced** and then **Proceed to x.x.x.x (unsafe)** to proceed to the Web Configurator login screen.

Figure 248 Security Alert (Google Chrome 99.0.4844.82)



53.5.3.1 Main Settings

After you accept the certificate and enter the login user name and password, the Switch main screen appears. The lock displayed in the bottom right of the browser status bar or next to the website address denotes a secure connection.

Figure 249 Example: Lock Denoting a Secure Connection

CHAPTER 54

Classifier

54.1 Classifier Overview

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

54.1.1 What You Can Do

- Use the **Classifier Status** screen ([Section 54.2 on page 363](#)) to view the classifiers configured on the Switch and how many times the traffic matches the rules.
- Use the **Classifier Setup** screen ([Section 54.3 on page 363](#)) to define the classifiers and view a summary of the classifier configuration. After you define the classifier, you can specify actions (or policy) to act upon the traffic that matches the rules.
- Use the **Classifier Global Setting** screen ([Section 54.4 on page 369](#)) to configure the match order and enable logging on the Switch.

54.1.2 What You Need to Know

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

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

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

- 1 Configure classifiers to sort traffic into different flows.
- 2 Configure policy rules to define actions to be performed on a classified traffic flow (refer to [Chapter 55 on page 372](#) 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.

54.2 Classifier Status

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

Click **SECURITY > ACL > Classifier > Classifier Status** to display the configuration screen as shown.

Figure 250 SECURITY > ACL > Classifier > Classifier Status

The following table describes the labels in this screen.

Table 189 SECURITY > ACL > Classifier > Classifier Status

LABEL	DESCRIPTION
Index	This field displays the index number of the rule.
Active	This field displays whether the rule is activated or not.
Weight	This field displays the rule's weight. This is to indicate a rule's priority when the match order is set to manual in the SECURITY > ACL > Classifier > Classifier Global Setting screen. The higher the number, the higher the rule's priority.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
Match Count	This field displays the number of times a rule is applied. It displays '-' if the rule does not have count enabled.
Rule	This field displays a summary of the classifier rule's settings.
Clear the Classifier	
Any	Select Any , then click Clear to clear the matched count for all classifiers.
Classifier	Select Classifier , enter a classifier rule name and then click Clear to erase the recorded statistical information for that classifier, or select Any to clear statistics for all classifiers.
Clear	Click Clear to erase the recorded statistical information for the classifier.

54.3 Classifier Setup

Use this screen to view and configure the classifiers. After you define the classifier, you can specify actions (or policy) to act upon the traffic that matches the rules.

Click **SECURITY > ACL > Classifier Setup** to display the configuration screen as shown.

Figure 251 SECURITY > ACL > Classifier > Classifier Setup

The following table describes the labels in this screen.

Table 190 SECURITY > ACL > Classifier > Classifier Setup

LABEL	DESCRIPTION
Index	This field displays the index number of the rule.
Active	This field displays Yes when the rule is activated and No when it is deactivated.
Weight	The field displays the priority of the rule when the match order is in manual mode. A higher weight means a higher priority.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
Rule	This field displays a summary of the classifier rule's settings.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new entry or edit a selected one.
Delete	Click Delete to remove the selected entries.

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

Table 191 Common Ethernet Types and Protocol Numbers

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

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

Table 192 Common IP Protocol Types and Protocol Numbers

PROTOCOL TYPE	PROTOCOL NUMBER
ICMP	1
TCP	6
UDP	17

Table 192 Common IP Protocol Types and Protocol Numbers (continued)

PROTOCOL TYPE	PROTOCOL NUMBER
EGP	8
L2TP	115

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

Table 193 Common TCP and UDP Port Numbers

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

54.3.1 Add/Edit a Classifier

Use this 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.

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SECURITY > ACL > Classifier > Classifier Setup** screen to display this screen.

Figure 252 SECURITY > ACL > Classifier > Classifier Setup > Add/Edit

Active ☒ OFF

Name

Weight

Log ☐

Count ☐

Time Range

Packet Format

Ingress Port

Port ☒ Any ☐

Trunk ☒ Any ☐

Layer 2

VLAN ☒ Any ☐

Inner VLAN ☒ Any ☐

Priority ☒ Any ☐

Inner Priority ☒ Any ☐

Ethernet Type ☒ All ☐ Others (Hex)

Source MAC Address ☒ Any ☐ MAC/Mask /

Destination MAC Address ☒ Any ☐ MAC/Mask /

Layer 3

IP Packet Length ☒ Any ☐ to bytes

IPv4 DSCP ☒ Any ☐

IPv6 DSCP ☒ Any ☐

Precedence ☒ Any ☐

ToS ☒ Any ☐

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

IPv6 Next Header ☒ All ☐ Establish Only ☐ Others (Dec)

Source IP Address/Prefix /

Destination IP Address/Prefix /

Layer 4

Source Socket Number ☒ Any ☐ to

Destination Socket Number ☒ Any ☐ to

Apply **Clear** **Cancel**

The following table describes the labels in this screen.

Table 194 SECURITY > ACL > Classifier > Classifier Setup > Add/Edit

LABEL	DESCRIPTION
Active	Enable the switch button to enable this rule.
Name	Enter a descriptive name for this rule for identifying purposes. You can enter up to 32 printable ASCII characters except [?], [], ['], ["], or [,].

Table 194 SECURITY > ACL > Classifier > Classifier Setup > Add/Edit (continued)

LABEL	DESCRIPTION
Weight	Enter a number between 0 and 65535 to specify the rule's weight. When the match order is in manual mode in the Classifier Global Setting screen, a higher weight means a higher priority.
Log	Select this option to have the Switch create a log message when the rule is applied and record the number of matched packets in a particular time interval. Note: Make sure you also enable logging in the Classifier Global Setting screen.
Count	Select this option to have the Switch count how many times the rule is applied.
Time Range	Select the name of the pre-configured schedule that you want to apply to the rule. The rule will be active only at the scheduled date and/or time. If you select None , the rule will be active all the time.
Packet Format	Specify the format of the packet. Choices are All , 802.3 untagged , 802.3 tagged , Ethernet II untagged and Ethernet II tagged . 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.
Ingress Port	
Port	Select Any to apply the rule to all ports. Alternatively, to specify the ports enter the port numbers to which the rule should be applied. You can enter multiple ports separated by (no space) comma (,) or hyphen (-). For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7.
Trunk	Select Any to apply the rule to all trunk groups. Alternatively, to specify multiple trunks, enter the trunk group ID to apply the rule to multiple trunks. You can enter multiple trunks with (t) or (T) then the trunk group ID separated by (no space) comma (,) or hyphen (-). For example, enter "t3-t5" for trunks 3, 4, and 5. Enter "T3,T5,T7" for trunks 3, 5, and 7.
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.
Inner VLAN	Select Any to classify traffic from any inner VLAN (the customer's VLAN) or select the second option and specify the source VLAN ID in the field provided.
Priority	Select Any to classify traffic from any priority level or select the second option and specify a priority level in the field provided.
Inner Priority	Select Any to classify traffic from any inner priority level or select the second option and specify a priority level in the field provided.
Ethernet Type	Select an Ethernet type or select Other and enter the Ethernet type number in hexadecimal value.
Source MAC Address	Select Any to apply the rule to all MAC addresses. To specify a source, select MAC/Mask to enter the source MAC address of the packet in valid MAC address format (six hexadecimal character pairs) and type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified MAC address that the traffic's MAC address should match. Enter "0" for the bits of the matched traffic's MAC address, which can be of any hexadecimal characters. For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria. If you leave the Mask field blank, the Switch automatically sets the mask to ff:ff:ff:ff:ff:ff.

Table 194 SECURITY > ACL > Classifier > Classifier Setup > Add/Edit (continued)

LABEL	DESCRIPTION
Destination MAC Address	Select Any to apply the rule to all MAC addresses. To specify a destination, select MAC/Mask to enter the destination MAC address of the packet in valid MAC address format (six hexadecimal character pairs) and type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified MAC address that the traffic's MAC address should match. Enter "0" for the bits of the matched traffic's MAC address, which can be of any hexadecimal characters. For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria. If you leave the Mask field blank, the Switch automatically sets the mask to ff:ff:ff:ff:ff:ff.
Layer 3 Specify the fields below to configure a layer 3 classifier.	
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.
IPv4/IPv6 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	Select Any to classify traffic from any precedence or select the second option and specify an IP Precedence (the first 3 bits of the 8-bit ToS field) value between 0 and 7 in the field provided.
ToS	Select Any to classify traffic from any ToS or select the second option and specify Type of Service (the last 5 bits of the 8-bit ToS field) value between 0 and 255 in the field provided.
IP Protocol	Select an IPv4 protocol type or select Other and enter the protocol number in decimal value. You may select Establish Only for TCP protocol type. This means that the Switch will pick out the packets that are sent to establish TCP connections.
IPv6 Next Header	Select an IPv6 protocol type or select Other and enter an 8-bit next header in the IPv6 packet. The Next Header field is similar to the IPv4 Protocol field. The IPv6 protocol number ranges from 1 to 255. You may select Establish Only for TCP protocol type. This means that the Switch will identify packets that initiate or acknowledge (establish) TCP connections.
Source IP Address/Prefix	Enter a source IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask. A subnet mask can be represented in a 32-bit notation. For example, the subnet mask "255.255.255.0" can be represented as "11111111.11111111.11111111.00000000", and counting up the number of ones in this case results in 24.
Destination IP Address/Prefix	Enter a destination IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Layer 4 Specify the fields below to configure a layer 4 classifier.	
Source Socket Number	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. Note: You must select either UDP or TCP in the IP Protocol field before you configure the socket numbers.
Destination Socket Number	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. Note: You must select either UDP or TCP in the IP Protocol field before you configure the socket numbers.

Table 194 SECURITY > ACL > Classifier > Classifier Setup > Add/Edit (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.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

54.4 Classifier Global Setting

Use this screen to configure the match order and enable logging on the Switch. Click **SECURITY > ACL > Classifier > Classifier Global Setting** to display the configuration screen as shown.

Figure 253 SECURITY > ACL > Classifier > Classifier Global Setting

The following table describes the labels in this screen.

Table 195 SECURITY > ACL > Classifier > Classifier Global Setting

LABEL	DESCRIPTION
Match Order	Use this field to set the match order for the classifier rules. A traffic flow can only be classified to one classifier. When a traffic flow matches more than one classifier rule, the Switch classifies the traffic based on the Match Order. Select manual to have classifier rules applied according to the weight of each rule you configured in SECURITY > ACL > Classifier > Classifier Setup. If they have the same weight, the Switch will classify the traffic to the classifier with a higher name priority (see Classifier Name Priority). Alternatively, select auto to have classifier rules applied according to the layer of the item configured in the rule. Layer-4 items have the highest priority, and layer-2 items has the lowest priority. For example, you configure a layer-2 item (VLAN ID) in classifier A and configure a layer-3 item (source IP address) in classifier B. When an incoming packet matches both classifier rules, classifier B has priority over classifier A. If both classifiers have the same priority, the Switch will apply the classifier with a higher name priority. Classifier Name Priority The longer the classifier name, the higher the classifier priority. If two classifier names are the same length, the bigger the character, the higher the classifier priority. The lowercase letters (such as a and b) have higher priority than the capitals (such as A and B) in the classifier name. For example, the classifier with the name of class 2, class a or class B takes priority over the classifier with the name of class 1 or class A.
Logging	

Table 195 SECURITY > ACL > Classifier > Classifier Global Setting (continued)

LABEL	DESCRIPTION
Active	Enable the switch button to allow the Switch to create a log when packets match a classifier rule during a defined time interval.
Interval	Set the length of the time period (in seconds) to count matched packets for a classifier rule. Enter an integer from 0 – 65535. 0 means that no logging is done.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

54.5 Classifier Example

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

Figure 254 Classifier: Example

Active	☒ ON ☐	
Name	example	
Weight	32767	
Log	☐	
Count	☐	
Time Range	None ▾	
Packet Format	All ▾	
Ingress Port		
Port	☐ Any	☒ 2
Trunk	☒ Any	☐
Layer 2		
VLAN	☒ Any	☐
Inner VLAN	☒ Any	☐
Priority	☒ Any	☐ 0 ▾
Inner Priority	☒ Any	☐ 0 ▾
EtherType	☒ All ▾	☐ Others (Hex)
Source MAC Address	☐ Any	☒ MAC/Mask 00:50:ba:ad:4f:81 /
Destination MAC Address	☒ Any	☐ MAC/Mask /
Layer 3		
IP Packet Length	☒ Any	☐ to bytes
IPv4 DSCP	☒ Any	☐
IPv6 DSCP	☒ Any	☐
Precedence	☒ Any	☐
ToS	☒ Any	☐
IP Protocol	☒ All ▾ ☐ Establish Only	☐ Others (Dec)
IPv6 Next Header	☒ All ▾ ☐ Establish Only	☐ Others (Dec)
Source IP Address/Prefix	/	
Destination IP Address/Prefix	/	
Layer 4		
Source Socket Number	☒ Any	☐ to
Destination Socket Number	☒ Any	☐ to
<input checked="" type="button"/> Apply Clear Cancel		

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

CHAPTER 55

Policy Rule

55.1 Policy Rules Overview

This chapter shows you how to configure policy rules.

A classifier distinguishes traffic into flows based on the configured criteria (refer to [Chapter 54 on page 362](#) for more information). A policy rule ensures that a traffic flow gets the requested treatment in the network.

55.1.1 What You Can Do

Use the **Policy Rule** screen ([Section 55.2 on page 373](#)) to enable the policy and display the active classifiers you configure in the **Classifier** screen.

55.1.2 DiffServ

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

55.1.3 DSCP and Per-Hop Behavior

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

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

DSCP (6 bits)	Unused (2 bits)

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

55.2 Policy Rules

Click **SECURITY > ACL > Policy Rule** in the navigation panel to display the screen as shown.

Figure 255 SECURITY > ACL > Policy Rule > Policy Rule

Index	Active	Name	Classifier(s)
☐			

The following table describes the labels in this screen.

Table 196 SECURITY > ACL > Policy Rule > Policy Rule

LABEL	DESCRIPTION
Index	This field displays the policy index number.
Active	This field displays whether policy is activated or not.
Name	This field displays the name you have assigned to this policy.
Classifier(s)	This field displays the names of the classifier to which this policy applies.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new entry or edit a selected one.
Delete	Click Delete to remove the selected entries.

55.2.1 Add/Edit a Policy Rule

You must first configure a classifier in the **SECURITY > ACL > Classifier > Classifier Setup** screen.

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SECURITY > ACL > Policy Rule > Policy Rule** screen to display this screen.

Figure 256 SECURITY > ACL > Policy Rule > Policy Rule > Add/Edit

Source & Destination

Active

OFF

Name

Classifier(s)

classifier1

General Parameters

Egress Port

1

Priority

0

DSCP

TOS

0

Metering Parameters

Bandwidth

0

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

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

OFF

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

Apply

Clear

Cancel

The following table describes the labels in this screen.

Table 197 SECURITY > ACL > Policy Rule > Policy Rule > Add/Edit

LABEL	DESCRIPTION
Source & Destination	
Active	Enable the switch button to enable the policy.
Name	Enter a descriptive name for identification purposes. You can enter up to 32 printable ASCII characters except [?], [], ['], ["], or [,].

Table 197 SECURITY > ACL > Policy Rule > Policy Rule > Add/Edit (continued)

LABEL	DESCRIPTION
Classifier(s)	This field displays the active classifiers you configure in the SECURITY > ACL > Classifier > Classifier Setup screen. Select the classifiers to which this policy rule applies. To select more than one classifier, press [SHIFT] and select the choices at the same time.
General Parameters Set the fields below for this policy. You only have to set the fields that is related to the actions you configure in the Action field.	
Egress Port	Enter the number of an outgoing port.
Priority	Specify a priority level.
DSCP	Specify a DSCP (DiffServ Code Point) number between 0 and 63.
TOS	Specify the Type Of Service (TOS) priority level.
Metering Parameters 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 actions the Switch takes on the associated classified traffic flow. Note: You can specify only one action (option) for each category (Forwarding, Priority, Queue, Outgoing) in a policy rule. Note: The Switch only applies one policy rule for each traffic flow. Say you have a traffic flow that matches several classifiers, and you specify a different policy rule for each. The Switch only classifies the traffic flow to the classifier with the highest Match Order. The Switch then applies the policy rule with which the classifier is associated. You can set the classifier Match Order rule (manual or auto) in the ACL > Classifier > Classifier Global settings screen (see Section 54.4 on page 369 for more information). Let's say you set two classifiers (Class 1 and Class 2) and both identify all traffic from MAC address 11:22:33:44:55:66 on port 3. If Policy 1 applies to Class 1 and the action is to drop the packets, Policy 2 applies to Class 2 and the action is to forward the packets to the egress port, the Switch will forward the packets. If Policy 1 applies to Class 1 and the action is to drop the packets, Policy 2 applies to Class 2 and the action is to enable bandwidth limitation, the Switch will discard the packets immediately. If Policy 1 applies to Class 1 and the action is to forward the packets to the egress port, Policy 2 applies to Class 2 and the action is to enable bandwidth limitation, the Switch will forward the packets.	
Forwarding	Select No change to forward the packets. Select Discard the packet to drop the packets. Select Do not drop the matching frame previously marked for dropping to retain the frames that were marked to be dropped before.

Table 197 SECURITY > ACL > Policy Rule > Policy Rule > Add/Edit (continued)

LABEL	DESCRIPTION
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 and put the packets in the designated queue. Select Replace the 802.1p priority field with the IP TOS value to replace the packet's 802.1p priority field with the value you set in the TOS field and put the packets in the designated queue. Select Replace the 802.1p priority field with the inner 802.1p priority value to replace the packet's 802.1p priority field with the existing customer priority level carried in the frames and put the packets in the designated queue.
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 field 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	Enable the switch button to activate bandwidth limitation on the traffic flows then set the actions to be taken on out-of-profile packets.
Out of profile action	Select the actions 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.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

55.3 Policy Example

The figure below shows an example **SECURITY > ACL > Policy Rule** 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 54.5 on page 370](#)).

Figure 257 Policy Example

Source & Destination

Active ☒ ON

Name

Classifier(s)

Example

General Parameters

Egress Port

Priority ▼

DSCP

TOS ▼

Metering Parameters

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

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

☒ ON

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

Apply Clear Cancel

CHAPTER 56

Anti-Arpscan

56.1 Anti-Arpscan Overview

Address Resolution Protocol (ARP), RFC 826, is a protocol used to convert a network-layer IP address to a link-layer MAC address. ARP scan is used to scan the network of a certain interface for alive hosts. It shows the IP address and MAC addresses of all hosts found. Hackers could use ARP scan to find targets in your network. **Anti-arpscan** is used to detect unusual ARP scan activity and block suspicious hosts or ports.

Unusual ARP scan activity is determined by port and host thresholds that you set. A port threshold is determined by the number of packets received per second on the port. If the received packet rate is over the threshold, then the port is put into an **Err-Disable** state. You can recover the normal state of the port manually if this happens and after you identify the cause of the problem.

A host threshold is determined by the number of ARP-request packets received per second. There is a global threshold rate for all hosts. If the rate of a host is over the threshold, then that host is blocked by using a MAC address filter. A blocked host is released automatically after the MAC aging time expires.

Note: A port-based threshold must be larger than the host-based threshold or the host-based threshold will not work.

56.1.1 What You Can Do

- Use the **Anti-Arpscan Status** screen ([Section 56.2 on page 379](#)) to see what ports are trusted and are forwarding traffic or are disabled.
- Use the **Anti-Arpscan Host Status** screen ([Section 56.3 on page 379](#)) to view blocked hosts and clear selected ones.
- Use this **Anti-Arpscan Setup** screen ([Section 56.4 on page 380](#)) to enable anti-arpscan, set port and host thresholds as well as configure ports to be trusted or untrusted.
- Use the **Anti-Arpscan Trust Host** screen ([Section 56.5 on page 382](#)) to create or remove trusted hosts identified by IP address and subnet mask. **Anti-arpscan** is not performed on trusted hosts.

56.1.2 What You Need to Know

- You should set an uplink port as a trusted port before enabling **Anti-arpscan** so as to prevent the port from being shutdown due to receiving too many ARP messages.
- When a port is configured as a trusted port, **Anti-arpscan** is not performed on the port. Both host and port thresholds are ignored for trusted ports. If the received ARP packet rate on a port or the received ARP-requests from a host exceed the thresholds, the trusted port will not be closed.
- If a port on the Switch is closed by **Anti-arpscan**, and you want to recover it, then do one of the following:

- Go to **PORT > Port Setup**. Clear **Active** and click **Apply**. Then select **Active** and click **Apply** again.
- Go to **SECURITY > Errdisable > Errdisable Recovery** and set the interval for **anti-arpscan**. After the interval expires, the closed ports will become active and start receiving packets again.
- Use the command `port no inactive`.
- Refer to the port logs to see when a port was closed.

56.2 Anti-Arpscan Status

Use this screen to see what ports are trusted and are forwarding traffic or are disabled. To open this screen, click **SECURITY > Anti-Arpscan > Anti-Arpscan Status**.

Figure 258 SECURITY > Anti-Arpscan > Anti-Arpscan Status

Anti-Arpscan Status	Anti-Arpscan Host Status	Anti-Arpscan Setup
Anti-Arpscan is Disabled		
Port	Trusted	State
1	OFF	Forwarding
2	OFF	Forwarding
3	OFF	Forwarding
4	OFF	Forwarding
5	OFF	Forwarding
6	OFF	Forwarding
7	OFF	Forwarding

The following table describes the fields in this screen.

Table 198 SECURITY > Anti-Arpscan > Anti-Arpscan Status

LABEL	DESCRIPTION
Anti-Arpscan is....	This shows whether Anti-arpscan is enabled or disabled on the Switch.
Port	This field displays the port number of the Switch.
Trusted	This field displays whether the port is trusted or untrusted. Anti-arpscan is not performed on a trusted port.
State	This field displays whether the port can forward traffic normally (Forwarding) or is disabled (Err-Disable).

56.3 Anti-Arpscan Host Status

Use this screen to view blocked hosts and unblock ones connected to certain ports. To open this screen, click **SECURITY > Anti-Arpscan > Anti-Arpscan Host Status**.

Figure 259 SECURITY > Anti-Arpscan > Anti-Arpscan Host Status

Anti-Arpscan Status	Anti-Arpscan Host Status	Anti-Arpscan Setup	Anti-Arpscan Trust Host		
Clear Filtered Host					
Port List Clear					
Filtered Host					
Index	Host IP	MAC Address	VLAN	Port	State

The following table describes the fields in the above screen.

Table 199 SECURITY > Anti-Arpscan > Anti-Arpscan Host Status

LABEL	DESCRIPTION
Clear Filtered host	A filtered host is a blocked IP address.
Port List	Enter a port number or a series of port numbers separated by commas and spaces, and then click Clear to unblock all hosts connected to these ports.
Filtered host	This table lists information on blocked hosts.
Index	This displays the index number of an IP address (a host) that has been blocked.
Host IP	This displays the IP address of the blocked host.
MAC Address	This displays the MAC address of the blocked host.
VLAN	This displays the VLAN ID that shows which VLAN the blocked host is in.
Port	This displays the port number to which the blocked host is connected.
State	This shows Err-Disable if the ARP-request rate from this host is over the threshold. Forwarding hosts are not displayed.

56.4 Anti-Arpscan Setup

Use this screen to enable **Anti-Arpscan**, set port and host thresholds as well as configure ports to be trusted or untrusted. To open this screen, click **SECURITY > Anti-Arpscan > Anti-Arpscan Setup**.

Figure 260 SECURITY > Anti-Arpscan > Anti-Arpscan Setup

Anti-Arpscan Status Anti-Arpscan Host Status **Anti-Arpscan Setup**

Active ☐ OFF

Port Threshold pps

Host Threshold pps

Port	Trusted State
*	Untrusted ▼
1	Untrusted ▼
2	Untrusted ▼
3	Untrusted ▼
4	Untrusted ▼
5	Untrusted ▼
6	Untrusted ▼
7	Untrusted ▼

Apply Cancel

The following table describes the fields in the above screen.

Table 200 SECURITY > Anti-Arpscan > Anti-Arpscan Setup

LABEL	DESCRIPTION
Active	Enable the switch button to enable Anti-arpscan on the Switch.
Port Threshold	A port threshold is determined by the number of packets received per second on the port. If the received packet rate is over the threshold, then the port is put into an Err-Disable state. Type the maximum number of packets per second allowed on the port before it is blocked. Note: The allowed range is 2 to 255 packets received per second.
Host Threshold	A host threshold is determined by the number of ARP-request packets received per second. This is the global threshold rate for all hosts. If the rate of a host is over the threshold, then that host is blocked by using a MAC address filter. A blocked host is released automatically after the MAC aging time expires. Type the maximum number of ARP-request packets allowed by a host before it is blocked. Note: The allowed range is 2 to 100 ARP-request packets per second. Note: The port-based threshold must be larger than the host-based threshold or the host-based threshold will not be applied.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.

Table 200 SECURITY > Anti-Arpscan > Anti-Arpscan Setup (continued)

LABEL	DESCRIPTION
Trusted State	Select Untrusted or Trusted for the associated port. Anti-arpscan is not performed on trusted hosts.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

56.5 Anti-Arpscan Trust Host

Use this screen to create or remove trusted hosts identified by IP address and subnet mask. **Anti-arpscan** is not performed on trusted hosts. To open this screen, click **SECURITY > Anti-Arpscan > Anti-Arpscan Trust Host**.

Figure 261 SECURITY > Anti-Arpscan > Anti-Arpscan Trust Host

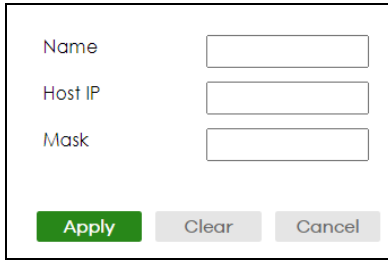
The following table describes the fields in the above screen.

Table 201 SECURITY > Anti-Arpscan > Anti-Arpscan Trust Host

LABEL	DESCRIPTION
Index	This field displays a sequential number for each trusted host.
Name	This field displays the name of the trusted host.
Host IP	This field displays the IP address of the trusted host.
Mask	This field displays the subnet mask of the trusted host.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new entry or edit a selected one.
Delete	Click Delete to remove the selected entries.

56.5.1 Add/Edit Anti-Arpscan Trust Hosts

Use this screen to add/edit trusted hosts identified by IP address and subnet mask. Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SECURITY > Anti-Arpscan > Anti-Arpscan Trust Host** screen to view this screen.

Figure 262 SECURITY > Anti-Arpscan > Anti-Arpscan Trust Host > Add/Edit


The screenshot shows a web form with three text input fields labeled 'Name', 'Host IP', and 'Mask'. Below these fields are three buttons: 'Apply' (highlighted in green), 'Clear', and 'Cancel'.

The following table describes the fields in the above screen.

Table 202 SECURITY > Anti-Arpscan > Anti-Arpscan Trust Host > Add/Edit

LABEL	DESCRIPTION
Name	Type a descriptive name of up to 32 printable ASCII (except [?], [], ['], ["], or [,]) characters to identify this host.
Host IP	Type the IP address of the host.
Mask	A trusted host may consist of a subnet of IP addresses. Type a subnet mask to create a single host or a subnet of hosts.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

CHAPTER 57

BPDU Guard

57.1 BPDU Guard Overview

A BPDU (Bridge Protocol Data Units) is a data frame that contains information about STP. STP-aware switches exchange BPDUs periodically.

The BPDU guard feature allows you to prevent any new STP-aware switch from connecting to an existing network and causing STP topology changes in the network. If there is any BPDU detected on the ports on which BPDU guard is enabled, the Switch disables the ports automatically. You can then enable the ports manually in the **PORT > Port Setup > Port Setup** screen, or use the **SECURITY > Errdisable > Errdisable Recovery** screen (see [Section 59.5 on page 393](#)) to have the ports become active after a certain time interval.

57.1.1 What You Can Do

- Use the **BPDU Guard Status** screen ([Section 57.2 on page 384](#)) to view the BPDU guard status.
- Use the **BPDU Guard Setup** screen ([Section 57.3 on page 385](#)) to enable BPDU guard on the Switch.

57.2 BPDU Guard Status

Use this screen to view whether BPDU guard is enabled on the Switch and the port status. Click **SECURITY > BPDU Guard > BPDU Guard Status** to view the following screen.

Figure 263 SECURITY > BPDU Guard > BPDU Guard Status

BPDU Guard Status		
BPDU Guard Setup		
BPDU guard global setup: Disable		
Port	Active	Status
1	OFF	Forwarding
2	OFF	Forwarding
3	OFF	Forwarding
4	OFF	Forwarding
5	OFF	Forwarding
6	OFF	Forwarding
7	OFF	Forwarding

The following table describes the fields in the above screen.

Table 203 SECURITY > BPDU Guard > BPDU Guard Status

LABEL	DESCRIPTION
BPDU guard global setup	This field displays whether BPDU guard is activated on the Switch.
Port	This field displays the port number.
Active	This shows whether BPDU guard is activated on the port.
Status	This shows whether the port is shut down (Err-disable) or able to transmit packets (Forwarding).

57.3 BPDU Guard Setup

Use this screen to turn on the BPDU guard feature on the Switch and ports.

Click **SECURITY > BPDU Guard > BPDU Guard Setup** to display the configuration screen as shown.

Figure 264 SECURITY > BPDU Guard > BPDU Guard Setup

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

The following table describes the fields in the above screen.

Table 204 SECURITY > BPDU Guard > BPDU Guard Setup

LABEL	DESCRIPTION
Active	Enable the switch button to enable BPDU guard on the Switch.
Port	This field displays the port number.

Table 204 SECURITY > BPDU Guard > BPDU Guard Setup (continued)

LABEL	DESCRIPTION
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to enable the BPDU guard feature on this port. The Switch shuts down this port if there is any BPDU received on the port. Clear this checkbox to disable the BPDU guard feature.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 58

Storm Control

58.1 Storm Control Overview

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

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.

58.1.1 What You Can Do

Use the **Storm Control** screen ([Section 58.2 on page 387](#)) to limit the number of broadcast, multicast and destination lookup failure (DLF) packets the Switch receives per second on the ports.

58.2 Storm Control Setup

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

Figure 265 SECURITY > Storm Control > Storm Control

Storm Control

Active ☐ OFF

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

Apply Cancel

The following table describes the labels in this screen.

Table 205 SECURITY > Storm Control > Storm Control

LABEL	DESCRIPTION
Active	Enable the switch button to enable traffic storm control on the Switch. Disable the switch button to disable this feature.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Broadcast (pkt/s)	Select this option to enable and specify how many broadcast packets the Switch accepts per second on the port. The Switch will generate a trap and/or log when the actual rate is higher than the specified threshold.
Multicast (pkt/s)	Select this option to enable and specify how many multicast packets the Switch accepts per second on the port. The Switch will generate a trap and/or log when the actual rate is higher than the specified threshold.
DLF (pkt/s)	Select this option and specify how many destination lookup failure (DLF) packets the port receives per second.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields.

CHAPTER 59

Error-Disable

59.1 Error-Disable Overview

This chapter shows you how to configure the rate limit for control packets on a port, and set the Switch to take an action (such as to shut down a port or stop sending packets) on a port when the Switch detects a pre-configured error. It also shows you how to configure the Switch to automatically undo the action after the error is gone.

59.1.1 CPU Protection Overview

Switches exchange protocol control packets in a network to get the latest networking information. If a switch receives large numbers of control packets, such as ARP, BPDU or IGMP packets, which are to be processed by the CPU, the CPU may become overloaded and be unable to handle regular tasks properly.

The CPU protection feature allows you to limit the rate of ARP, BPDU and IGMP packets to be delivered to the CPU on a port. This enhances the CPU efficiency and protects against potential DoS attacks or errors from other networks. You then can choose to drop control packets that exceed the specified rate limit or disable a port on which the packets are received.

59.1.2 Error-Disable Recovery Overview

Some features, such as loop guard or CPU protection, allow the Switch to shut down a port or discard specific packets on a port when an error is detected on the port. For example, if the Switch detects that packets sent out the ports loop back to the Switch, the Switch can shut down the ports automatically. After that, you need to enable the ports or allow the packets on a port manually through the Web Configurator or the commands. With error-disable recovery, you can set the disabled ports to become active or start receiving the packets again after the time interval you specify.

59.1.3 What You Can Do

- Use the **Errdisable Status** screen ([Section 59.2 on page 390](#)) to view whether the Switch detected that control packets exceeded the rate limit configured for a port or a port is disabled according to the feature requirements and what action you configure, and related information.
- Use the **CPU Protection** screen ([Section 59.3 on page 391](#)) to limit the maximum number of control packets (ARP, BPDU and/or IGMP) that the Switch can receive or transmit on a port.
- Use the **Errdisable Detect** screen ([Section 59.4 on page 392](#)) to have the Switch detect whether the control packets exceed the rate limit configured for a port and configure the action to take once the limit is exceeded.
- Use the **Errdisable Recovery** screen ([Section 59.5 on page 393](#)) to set the Switch to automatically undo an action after the error is gone.

59.2 Error-Disable Status

Use this screen to view whether the Switch detected that control packets exceeded the rate limit configured for a port or a port is disabled according to the feature requirements and what action you configure, and related information. Click **SECURITY > Errdisable > Errdisable Status** to display the screen as shown.

Figure 266 SECURITY > Errdisable > Errdisable Status

Port	Cause	Active	Mode	Rate	Status	Recovery Time Left (secs)	Total Dropped
1	Loop Guard	OFF	inactive-port	-	Forwarding	-	-
	ARP	OFF	inactive-port	0	Forwarding	-	-
	BPDU	OFF	inactive-port	0	Forwarding	-	-
	IGMP	OFF	inactive-port	0	Forwarding	-	-
2	BPDU Guard	OFF	inactive-port	-	Forwarding	-	-
	Loop Guard	OFF	inactive-port	-	Forwarding	-	-
	ARP	OFF	inactive-port	0	Forwarding	-	-
	IGMP	OFF	inactive-port	0	Forwarding	-	-
3	BPDU Guard	OFF	inactive-port	-	Forwarding	-	-
	Loop Guard	OFF	inactive-port	-	Forwarding	-	-
	ARP	OFF	inactive-port	0	Forwarding	-	-
	IGMP	OFF	inactive-port	0	Forwarding	-	-

The following table describes the labels in this screen.

Table 206 SECURITY > Errdisable > Errdisable Status

LABEL	DESCRIPTION
Inactive-reason mode reset	
Port	Enter the number of the ports (separated by a comma) on which you want to reset inactive-reason status.
Cause	Select the cause of inactive-reason mode you want to reset here.
Reset	Click to reset the specified ports to handle ARP, BPDU or IGMP packets instead of ignoring them, if the ports is in inactive-reason mode.
Errdisable Status	
Port	This is the number of the port on which you want to configure Errdisable Status.
Cause	This displays the type of the control packet received on the port or the feature enabled on the port and causing the Switch to take the specified action.

Table 206 SECURITY > Errdisable > Errdisable Status (continued)

LABEL	DESCRIPTION
Active	This field displays whether the control packets (ARP, BPDU, and/or IGMP) on the port is being detected or not. It also shows whether loop guard, anti-arp scanning, BPDU guard or ZULD is enabled on the port.
Mode	This field shows the action that the Switch takes for the cause. • inactive-port – The Switch disables the port. • inactive-reason – The Switch drops all the specified control packets (such as BPDU) on the port. • rate-limitation – The Switch drops the additional control packets the ports has to handle in every one second.
Rate	This field displays how many control packets this port can receive or transmit per second. It can be adjusted in CPU Protection . 0 means no rate limit.
Status	This field displays the errdisable status. • Forwarding: The Switch is forwarding packets. Rate-limitation mode is always in Forwarding status. • Err-disable: The Switch disables the port on which the control packets are received (inactive-port) or drops specified control packets on the port (inactive-reason).
Recovery Time Left (secs)	This field displays the time (seconds) left before the ports becomes active of Errdisable Recovery.
Total Dropped	This field displays the total packet number dropped by this port where the packet rate exceeds the rate of mode rate-limitation.

59.3 CPU Protection Setup

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 **SECURITY > Errdisable > CPU Protection** 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 **SECURITY > Errdisable > Errdisable Detect** screen.

Figure 267 SECURITY > Errdisable > CPU Protection

Port	Rate Limit (pkt/s)
*	
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0

The following table describes the labels in this screen.

Table 207 SECURITY > Errdisable > CPU Protection

LABEL	DESCRIPTION
Reason	Select the type of control packet you want to configure here.
Port	This field displays the port number.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Changes in this row are copied to all the ports as soon as you make them.
Rate Limit (pkt/s)	Enter a number from 0 to 256 to specify how many control packets this port can receive or transmit per second. 0 means no rate limit. You can configure the action that the Switch takes when the limit is exceeded.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

59.4 Error-Disable Detect Setup

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 **SECURITY > Errdisable > Errdisable Detect** to display the screen as shown.

Figure 268 SECURITY > Errdisable > Errdisable Detect

Errdisable Status	CPU Protection	Errdisable Detect	Errdisable Recovery															
		<table border="1"> <thead> <tr> <th>Cause</th> <th>Active</th> <th>Mode</th> </tr> </thead> <tbody> <tr> <td>*</td> <td>☐</td> <td>inactive-port ▼</td> </tr> <tr> <td>ARP</td> <td>☐</td> <td>inactive-port ▼</td> </tr> <tr> <td>BPDU</td> <td>☐</td> <td>inactive-port ▼</td> </tr> <tr> <td>IGMP</td> <td>☐</td> <td>inactive-port ▼</td> </tr> </tbody> </table>	Cause	Active	Mode	*	☐	inactive-port ▼	ARP	☐	inactive-port ▼	BPDU	☐	inactive-port ▼	IGMP	☐	inactive-port ▼	
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 208 SECURITY > Errdisable > Errdisable Detect

LABEL	DESCRIPTION
Cause	This field displays the types of control packet that may cause CPU overload.
*	Use this row to make the setting the same for all entries. Use this row first and then make adjustments to each entry if necessary. Changes in this row are copied to all the entries as soon as you make them.
Active	Select this option to have the Switch detect if the configured rate limit for a specific control packet is exceeded and take the action selected below.
Mode	Select the action that the Switch takes when the number of control packets exceed the rate limit on a port, set in the SECURITY > Errdisable > CPU Protection screen. inactive-port – The Switch disables the port on which the control packets are received. inactive-reason – The Switch drops all the specified control packets (such as BPDU) on the port. rate-limitation – The Switch drops the additional control packets the ports has to handle in every one second.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

59.5 Error-Disable Recovery Setup

Use this screen to configure the Switch to automatically undo an action after the error is gone. Click **SECURITY > Errdisable > Errdisable Recovery** to display the screen as shown.

Figure 269 SECURITY > Errdisable > Errdisable Recovery

Reason	Time Status	Interval
*	☐	
loopguard	☐	300
ARP	☐	300
BPDU	☐	300
IGMP	☐	300
anti-arpscan	☐	300
bpduguard	☐	300

The following table describes the labels in this screen.

Table 209 SECURITY > Errdisable > Errdisable Recovery

LABEL	DESCRIPTION
Active	Enable the switch button to turn on the error-disable recovery function on the Switch.
Reason	This field displays the supported features that allow the Switch to shut down a port or discard packets on a port according to the feature requirements and what action you configure.
*	Use this row to make the setting the same for all entries. Use this row first and then make adjustments to each entry if necessary. Changes in this row are copied to all the entries as soon as you make them.
Time Status	Select this checkbox to allow the Switch to wait for the specified time interval to activate a port or allow specific packets on a port, after the error was gone. Clear the checkbox to turn off this rule.
Interval	Enter the number of seconds (from 30 to 2592000) for the time interval.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 60

IP Source Guard

60.1 IP Source Guard Overview

IP source guard consists of the following features:

- DHCP snooping. Use this to filter unauthorized DHCP server packets on the network and to build a binding table dynamically.
- ARP inspection. Use this to filter unauthorized ARP packets on the network.
- Static IP bindings. Use this to create static bindings in the binding table.

The Switch builds the binding table by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings).

Binding Table

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

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

The Switch builds the binding table by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings).

DHCP Snooping

The Switch only allows an authorized DHCP server on a trusted port to assign IP addresses. Unauthorized DHCP servers will not be able to assign IP addresses to network clients. When the Switch receives a DHCP server packet from an authorized DHCP server, it inspects the packet and records the DHCP information in a binding table. The binding records are used in ARP inspection to filter unauthorized ARP packets. See [Section 61.1 on page 400](#) for more DHCP snooping information.

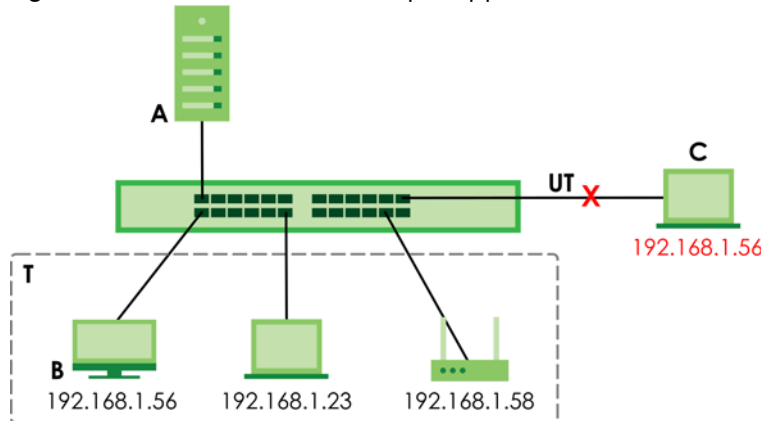
ARP Inspection

When the Switch receives an 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. Otherwise, the Switch discards the packet.

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.

The following figure demonstrates a scenario with DHCP snooping and ARP inspection enabled. In this scenario, we connect an authorized DHCP server (**A**) and the client devices on the ARP trusted ports (**T**). A client device (**B**) is assigned the IP address 192.168.1.56 by the authorized DHCP server (**A**). A malicious host (**C**) on an untrusted port (**UT**) puts a wrong MAC address with the IP address 192.168.1.56 in an ARP reply packet pretending to be client device (**B**) (192.168.1.56). The Switch snoops DHCP packets sent from the authorized DHCP server (**A**) and creates bindings in the binding table. When the Switch receives ARP packets from an untrusted port (**UT**), it compares the IP and MAC addresses with the existing bindings. Since the IP and MAC binding is different from the existing bindings, the Switch blocks the unauthorized ARP packets sent from the malicious host (**C**). The malicious host (**C**) therefore cannot disguise as client device (**B**) to build connections with other client devices on your network.

Figure 270 IP Source Guard Example Application



60.1.1 What You Can Do

- Use the **IP Source Guard** screen ([Section 60.2 on page 396](#)) to look at the current bindings for DHCP snooping and ARP inspection.
- Use the **Static Binding** screen ([Section 60.3 on page 397](#)) to manage static bindings for DHCP snooping and ARP inspection.

60.2 IPv4 Source Guard

Use this screen to look at the current bindings for DHCP snooping and ARP inspection. Bindings are used by ARP inspection to distinguish between authorized and unauthorized ARP packets in the network. The Switch learns the bindings by snooping DHCP packets (dynamic bindings) and from information provided manually by administrators (static bindings).

Figure 271 SECURITY > IPv4 Source Guard > IP Source Guard > IP Source Guard

IP Source Guard						
Static Binding						
Index	IP Address	VID	MAC Address	Port	Lease	Type

The following table describes the labels in this screen.

Table 210 SECURITY > IPv4 Source Guard > IP Source Guard > IP Source Guard

LABEL	DESCRIPTION
Index	This field displays a sequential number for each binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
VID	This field displays the source VLAN ID in the binding.
MAC Address	This field displays the source MAC address in the binding.
Port	This field displays the port number in the binding. If this field is blank, the binding applies to all ports.
Lease	This field displays how many days, hours, minutes, and seconds the binding is valid; for example, 2d3h4m5s means the binding is still valid for 2 days, 3 hours, 4 minutes, and 5 seconds. This field displays infinity if the binding is always valid (for example, a static binding).
Type	This field displays how the Switch learned the binding. static : This binding was learned from information provided manually by an administrator. dhcp-snooping : This binding was learned by snooping DHCP packets.

60.3 IPv4 Source Guard Static Binding

Use this screen to manage static bindings for DHCP snooping and ARP inspection. Static bindings are uniquely identified by the MAC address and VLAN ID. Each MAC address and VLAN ID can only be in one static binding. If you try to create a static binding with the same MAC address and VLAN ID as an existing static binding, the new static binding replaces the original one. To open this screen, click **SECURITY > IPv4 Source Guard > IP Source Guard > Static Binding**.

Figure 272 SECURITY > IPv4 Source Guard > IP Source Guard > Static Binding

The screenshot shows the 'Static Binding' configuration page. At the top, there are tabs for 'IP Source Guard' and 'Static Binding'. Below the tabs, there is a section for 'ARP Freeze' with three radio button options: 'All' (selected), 'Port List', and 'VLAN List'. The 'Port List' and 'VLAN List' options have associated text input fields. Below these options are two buttons: 'ARP Freeze' (green) and 'Cancel' (grey). The main section is titled 'Static Binding' and contains a table with columns: Index, IP Address, VID, MAC Address, Port, Lease, and Type. Above the table, there are two buttons: '+ Add/Edit' (green) and '- Delete' (red). A checkbox is located to the left of the table header.

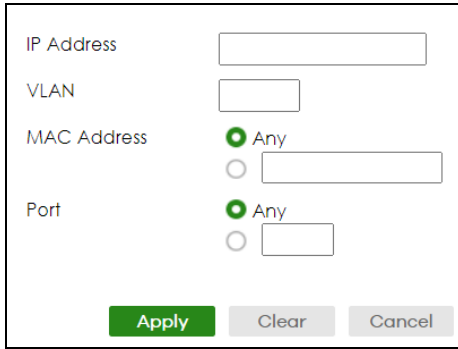
The following table describes the labels in this screen.

Table 211 SECURITY > IPv4 Source Guard > 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 NETWORKING > ARP Setup > ARP Learning screen before you use the ARP Freeze feature.
Condition	All – Select this and click ARP Freeze to have the Switch automatically add all the current ARP entries to the static bindings table. Port List – Select this and enter the number of the ports (separated by a comma). 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. ARP entries learned on the specified ports are added to the static bindings table after you click ARP Freeze. VLAN List – Select this and enter the ID number of the VLANs (separated by a comma). ARP entries for the specified VLANs are added to the static bindings table after you click ARP Freeze.
Static Binding	
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Index	This field displays a sequential number for each binding.
IP Address	This field displays the IP address assigned to the MAC address in the binding.
VID	This field displays the source VLAN ID in the binding.
MAC Address	This field displays the source MAC address in the binding.
Port	This field displays the port number.
Lease	This field displays how long the binding is valid.
Type	This field displays how the Switch learned the binding. Static: This binding was learned from information provided manually by an administrator.
Add/Edit	Click Add/Edit to add a new entry or edit a selected one.
Delete	Click Delete to remove the selected entries.

60.3.1 Add/Edit IPv4 Source Guard Static Binding

Use this screen to manage static bindings for DHCP snooping and ARP inspection. Static bindings are uniquely identified by the MAC address and VLAN ID. Each MAC address and VLAN ID can only be in one static binding. If you try to create a static binding with the same MAC address and VLAN ID as an existing static binding, the new static binding replaces the original one. Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SECURITY > IPv4 Source Guard > IP Source Guard > Static Binding** screen to display this screen.

Figure 273 SECURITY > IPv4 Source Guard > IP Source Guard > Static Binding > Add/Edit


IP Address

VLAN

MAC Address ☒ Any ☐

Port ☒ Any ☐

Apply Clear Cancel

The following table describes the labels in this screen.

Table 212 SECURITY > IPv4 Source Guard > IP Source Guard > Static Binding > Add/Edit

LABEL	DESCRIPTION
IP Address	Enter the IP address assigned to the MAC address in the binding.
VLAN	Enter the source VLAN ID in the binding.
MAC Address	Enter the source MAC address in the binding. If this binding applies to all MAC addresses, select Any .
Port	Specify the ports in the binding. If this binding has one port, select the first radio button and enter the port number in the field to the right. If this binding applies to all ports, select Any .
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

CHAPTER 61

DHCP Snooping

61.1 DHCP Snooping Overview

DHCP snooping filters unauthorized DHCP server packets. The Switch allows only the authorized DHCP server on a trusted port to assign IP addresses. Clients on your network will only receive DHCP packets from the authorized DHCP server.

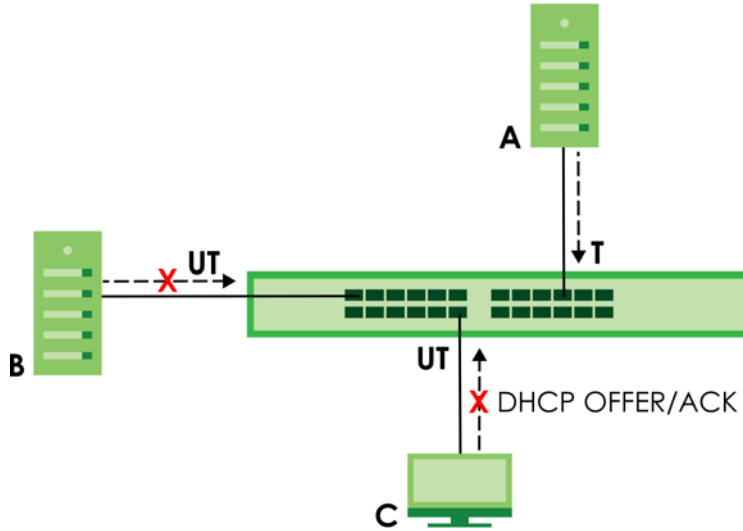
The Switch also builds a DHCP snooping binding table dynamically by snooping DHCP packets (dynamic bindings). A DHCP snooping binding table contains the IP binding information the Switch learns from DHCP packets in your network. A binding contains these key attributes:

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

The following settings demonstrates DHCP snooping on the Switch.

- An authorized DHCP server (**A**) on a snooped VLAN from the trusted port (**T**)
- An unauthorized DHCP server (**B**) on a snooped VLAN from an untrusted port (**UT**)
- DHCP clients (**C**) on the untrusted ports (**UT**).

With DHCP snooping, the Switch blocks all DHCP server packets (**DHCP OFFER/ACK**) coming from the untrusted ports (**UT**). The Switch only forwards the DHCP server packets from the trusted port (**T**). This assures that DHCP clients on your network only receive IP addresses assigned by the authorized DHCP server (**A**).

Figure 274 DHCP Snooping Example Application

61.1.1 What You Can Do

- Use the **DHCP Snooping Status** screen ([Section 61.2 on page 401](#)) to look at various statistics about the DHCP snooping database.
- Use this **DHCP Snooping Setup** screen ([Section 61.3 on page 404](#)) to enable DHCP snooping on the Switch (not on specific VLAN), specify the VLAN where the default DHCP server is located, and configure the DHCP snooping database.
- Use the **DHCP Snooping Port Setup** screen ([Section 61.4 on page 405](#)) to specify whether ports are trusted or untrusted ports for DHCP snooping.
- Use the **DHCP Snooping VLAN Setup** screen ([Section 61.5 on page 407](#)) to enable DHCP snooping on each VLAN and to specify whether or not the Switch adds DHCP relay agent option 82 information to DHCP requests that the Switch relays to a DHCP server for each VLAN.
- Use the **DHCP Snooping VLAN Port Setup** screen ([Section 61.6 on page 408](#)) to apply a different DHCP option 82 profile to certain ports in a VLAN.

61.2 DHCP Snooping Status

Use this screen to look at various statistics about the DHCP snooping database.

To open this screen, click **SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. Status**.

Figure 275 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. Status

DHCP Snp. Status		DHCP Snp. Setup	DHCP Snp. Port Setup	DHCP Snp. VLAN Setup	DHCP Snp. VLAN Port Setup
DHCP Snooping					
Database Status			Database Detail		
Agent URL			First Successful Access		None
Write Delay Timer300			Last Ignored Bindings Counters		
Abort Timer300			Binding Collisions		0
Agent RunningNone			Invalid Interfaces		0
Delay Timer ExpiryNot Running			Parse Failures		0
Abort Timer ExpiryNot Running			Expired Leases		0
Last Succeeded TimeNone			Unsupported VLANs		0
Last Failed TimeNone			Last Ignored Time		None
Last Failed ReasonNo failure recorded			Total Ignored Bindings Counters		
Counters			Binding Collisions		0
Total Attempts0			Invalid Interfaces		0
Startup Failures0			Parse Failures		0
Successful Transfers0			Expired Leases		0
Failed Transfers0			Unsupported VLANs		0
Successful Reads0					
Failed Reads0					
Successful Writes0					
Failed Writes0					

The following table describes the labels in this screen.

Table 213 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. Status

LABEL	DESCRIPTION
Database Status	
This section displays the current settings for the DHCP snooping database. You can configure them in the SECURITY > DHCP Snooping > DHCP Snp. Setup screen.	
Agent URL	This field displays the location of the DHCP snooping database.
Write Delay Timer	This field displays how long (in seconds) the Switch tries to complete a specific update in the DHCP snooping database before it gives up.
Abort Timer	This field displays how long (in seconds) the Switch waits to update the DHCP snooping database after the current bindings change.
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.
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.

Table 213 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. Status (continued)

LABEL	DESCRIPTION
Last Failed Reason	This field displays the reason the Switch updated the DHCP snooping database unsuccessfully.
Counters 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.	
Binding Collisions	This field displays the number of bindings the Switch ignored because the Switch already had a binding with the same MAC address and VLAN ID.
Invalid Interfaces	This field displays the number of bindings the Switch ignored because the port number was a trusted interface or does not exist anymore.
Parse Failures	This field displays the number of bindings the Switch ignored because the Switch was unable to understand the binding in the DHCP binding database.
Expired Leases	This field displays the number of bindings the Switch ignored because the lease time had already expired.
Unsupported VLANs	This field displays the number of bindings the Switch ignored because the VLAN ID does not exist anymore.
Last Ignored Time	This field displays the last time the Switch ignored any bindings for any reason from the DHCP binding database.
Total Ignored Bindings Counters This section displays the reasons the Switch has ignored bindings any time it read bindings from the DHCP binding database. You can clear these counters by restarting the Switch.	
Binding Collisions	This field displays the number of bindings the Switch has ignored because the Switch already had a binding with the same MAC address and VLAN ID.
Invalid Interfaces	This field displays the number of bindings the Switch has ignored because the port number was a trusted interface or does not exist anymore.

Table 213 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. Status (continued)

LABEL	DESCRIPTION
Parse Failures	This field displays the number of bindings the Switch has ignored because the Switch was unable to understand the binding in the DHCP binding database.
Expired Leases	This field displays the number of bindings the Switch has ignored because the lease time had already expired.
Unsupported VLANs	This field displays the number of bindings the Switch has ignored because the VLAN ID does not exist anymore.

61.3 DHCP Snooping Setup

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 **SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. Setup**.

Note: The input string of any field in this screen should not contain [?], [|], ['], ["], or [,].

Figure 276 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. Setup

The following table describes the labels in this screen.

Table 214 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. Setup

LABEL	DESCRIPTION
DHCP Snooping Setup	
Active	Enable the switch button to enable DHCP snooping on the Switch. You still have to enable DHCP snooping on specific VLAN and specify trusted ports. Note: If DHCP is enabled and there are no trusted ports, DHCP requests will not succeed.

Table 214 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. Setup (continued)

LABEL	DESCRIPTION
DHCP VLAN	Select a VLAN ID if you want the Switch to forward DHCP packets to DHCP servers on a specific VLAN. Note: You have to enable DHCP snooping on the DHCP VLAN too. You can enable Option 82 Profile in the SECURITY > DHCP Snooping > DHCP Snp. VLAN Setup screen to help the DHCP servers distinguish between DHCP requests from different VLAN. Select Disable if you do not want the Switch to forward DHCP packets to a specific VLAN.
Database If Timeout Interval is greater than Write Delay Interval, it is possible that the next update is scheduled to occur before the current update has finished successfully or timed out. In this case, the Switch waits to start the next update until it completes the current one.	
Agent URL	Enter the location of the DHCP snooping database. The location should be expressed like this: http://{domain name or IP address}/directory, if applicable/file name ; for example, http://192.168.10.1/database.txt . You can enter up to 256 printable ASCII characters except [?], [], ['], ["], or [,].
Timeout Interval	Enter how long (10 – 65535 seconds) the Switch tries to complete a specific update in the DHCP snooping database before it gives up.
Write Delay Interval	Enter how long (10 – 65535 seconds) the Switch waits to update the DHCP snooping database the first time the current bindings change after an update. Once the next update is scheduled, additional changes in current bindings are automatically included in the next update.
Renew DHCP Snooping URL	Enter the location of a DHCP snooping database, and click Renew if you want the Switch to load it. You can use this to load dynamic bindings from a different DHCP snooping database than the one specified in Agent URL. When the Switch loads dynamic bindings from a DHCP snooping database, it does not discard the current dynamic bindings first. If there is a conflict, the Switch keeps the dynamic binding in volatile memory and updates the Binding Collisions counter in the DHCP Snooping Status screen (Section 61.2 on page 401).
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use 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.

61.4 DHCP Snooping Port Setup

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

Note: If DHCP snooping is enabled but there are no trusted ports, DHCP requests cannot reach the DHCP server.

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 **SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. Port Setup**.

Figure 277 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. Port Setup

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

The following table describes the labels in this screen.

Table 215 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. Port Setup

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

61.5 DHCP Snooping VLAN Setup

Use this screen to enable DHCP snooping on each VLAN and to specify whether or not the Switch adds DHCP relay agent option 82 information to DHCP requests that the Switch relays to a DHCP server for each VLAN.

To open this screen, click **SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. VLAN Setup**.

Figure 278 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. VLAN Setup

Search VLAN by VID **Search**

The Number of VLANs: 1

VID	Enabled	Option 82 Profile
*	No ▾	▾
1	No ▾	▾

Apply **Cancel**

The following table describes the labels in this screen.

Table 216 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. VLAN Setup

LABEL	DESCRIPTION
Search VLAN by VID	Enter the VLAN ID you want to manage. Use a comma (,) to separate individual VLANs or a hyphen (-) to indicates a range of VLANs. For example, "3,4" or "3-9".
Search	Click this to display the specified range of VLANs in the section below.
The Number of VLANs	This displays the number of VLAN search results.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the * VLAN, the settings are applied to all VLANs.
Enabled	Select Yes to enable DHCP snooping on the VLAN. You still have to enable DHCP snooping on the Switch and specify trusted ports. Note: The Switch will drop all DHCP requests if you enable DHCP snooping and there are no trusted ports.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to all ports in the specified VLANs. The Switch adds the information (such as slot number, port number, VLAN ID and/or system name) specified in the profile to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN. You can specify the DHCP VLAN in the SECURITY > DHCP Snooping > DHCP Snp. Setup screen.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values in this screen to their last-saved values.

61.6 DHCP Snooping VLAN Port Setup

Use this screen to apply a different DHCP option 82 profile to certain ports in a VLAN.

To open this screen, click **SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. VLAN Port Setup**.

Figure 279 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. VLAN Port Setup

Index	VID	Port	ProfileName

The following table describes the labels in this screen.

Table 217 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. VLAN Port Setup

LABEL	DESCRIPTION
Index	This field displays a sequential number for each entry.
VID	This field displays the VLAN to which the ports belongs.
Port	This field displays the ports to which the Switch applies the settings.
Profile Name	This field displays the DHCP option 82 profile that the Switch applies to the ports.
Add/Edit	Click Add/Edit to add a new entry or edit a selected one.
Delete	Click Delete to remove the selected entries.

61.6.1 Add/EDIT DHCP Snooping VLAN Ports

Use this screen to apply a different DHCP option 82 profile to certain ports in a VLAN.

Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. VLAN Port Setup** screen to display this screen.

Figure 280 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. VLAN Port Setup > Add/Edit

The following table describes the labels in this screen.

Table 218 SECURITY > IPv4 Source Guard > DHCP Snooping > DHCP Snp. VLAN Port Setup > Add/Edit

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN you want to configure here.
Port	Enter the number of ports to which you want to apply the specified DHCP option 82 profile. You can enter multiple ports separated by (no space) comma (,) or hyphen (-) for a range. For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7.
Option 82 Profile	Select a pre-defined DHCP option 82 profile that the Switch applies to the specified ports in this VLAN. The Switch adds the information (such as slot number, port number, VLAN ID and/or system name) specified in the profile to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN. You can specify the DHCP VLAN in the SECURITY > DHCP Snooping > DHCP Snp. Setup screen. Note: The profile you select here has priority over the one you select in the SECURITY > DHCP Snooping > DHCP Snp. VLAN Setup 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.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

61.7 Technical Reference

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

61.7.1 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.

61.7.1.1 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 or untrusted setting for ARP inspection. You can also specify the maximum number for DHCP packets that each port (trusted or untrusted) can receive each second.

Trusted ports are connected to DHCP servers or other switches. The Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. The Switch learns dynamic bindings from trusted ports.

Note: If DHCP is enabled and there are no trusted ports, DHCP requests will not succeed.

Untrusted ports are connected to subscribers. The Switch discards DHCP packets from untrusted ports in the following situations:

- The packet is a DHCP server packet (for example, OFFER, ACK, or NACK).
- The rate at which DHCP packets arrive is too high.

61.7.1.2 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 281 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.

61.7.1.3 DHCP Relay Option 82 Information

The Switch can add information to DHCP requests that it does not discard. This provides the DHCP server more information about the source of the requests. The Switch can add the following information:

- Slot ID (1 byte), port ID (1 byte), and source VLAN ID (2 bytes)
- System name (up to 32 bytes)

This information is stored in an Agent Information field in the option 82 field of the DHCP headers of client DHCP request frames.

When the DHCP server responds, the Switch removes the information in the Agent Information field before forwarding the response to the original source.

You can configure this setting for each source VLAN. This setting is independent of the DHCP relay settings.

61.7.1.4 Configuring DHCP Snooping

Follow these steps to configure DHCP snooping on the Switch.

- 1 Enable DHCP snooping on the Switch.
- 2 Enable DHCP snooping on each VLAN, and configure DHCP relay option 82.

- 3** Configure trusted and untrusted ports, and specify the maximum number of DHCP packets that each port can receive per second.
- 4** Configure static bindings.

CHAPTER 62

ARP Inspection

62.1 ARP Inspection Status

Use this screen to look at the current list of MAC address filters that were created because the Switch identified an unauthorized ARP packet. When the Switch identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address and source VLAN ID of the unauthorized ARP packet. To open this screen, click **SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. Status**.

Figure 282 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. Status

The following table describes the labels in this screen.

Table 219 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. Status

LABEL	DESCRIPTION
Total Number of Bindings	This field displays the current number of MAC address filters that were created because the Switch identified unauthorized ARP packets.
Index	This field displays a sequential number for each MAC address filter.
MAC Address	This field displays the source MAC address in the MAC address filter.
VID	This field displays the source VLAN ID in the MAC address filter.
Port	This field displays the source port of the discarded ARP packet.
Expiry (sec)	This field displays how long (in seconds) the MAC address filter remains in the Switch. You can also delete the record manually (Delete).
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Delete	Click this to remove the selected entries.
Cancel	Click this to clear the Delete checkboxes above.

62.2 ARP Inspection VLAN Status

Use this screen to look at various statistics about ARP packets in each VLAN. To open this screen, click **SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. VLAN Status**.

Figure 283 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. VLAN Status

The following table describes the labels in this screen.

Table 220 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. VLAN Status

LABEL	DESCRIPTION
Search VLAN by VID	Specify the VLANs you want to view in the section below. Use a comma (,) to separate individual VLANs or a hyphen (-) to indicates a range of VLANs. For example, "3,4" or "3-9".
Search	Click this to display the specified range of VLANs in the section below.
The Number of VLANs	This is the number of VLANs that match the searching criteria and display in the list below. The number displays when you use the Search button to look for certain VLANs. The default value is 0.
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.

62.3 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 **SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. Log Status**.

Figure 284 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. Log Status

ARP Insp. Status ARP Insp. VLAN Status **ARP Insp. Log Status** ARP Insp. Setup ARP Insp. Port Setup

Clearing Log Status Table **Clear**

Total Number of Bindings : 0

Index	Port	VID	Sender MAC	Sender IP	Packet Number	Reason	Time

The following table describes the labels in this screen.

Table 221 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. Log Status

LABEL	DESCRIPTION
Clearing Log Status Table	Click Clear 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 Bindings	This field displays the number of log messages that were generated by ARP packets and that have not been sent to the syslog server yet. If one or more log messages are dropped due to unavailable buffer, there is an entry called overflow with the current number of dropped log messages.
Index	This field displays a sequential number for each log message.
Port	This field displays the source port of the ARP packet.
VID	This field displays the source VLAN ID of the ARP packet.
Sender MAC	This field displays the source MAC address of the ARP packet.
Sender IP	This field displays the source IP address of the ARP packet.
Packet Number	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 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. Setup screen.
Reason	This field displays the reason the log message was generated. dhcp deny: An ARP packet was discarded because it violated a dynamic binding with the same MAC address and VLAN ID. static deny: An ARP packet was discarded because it violated a static binding with the same MAC address and VLAN ID. deny: An ARP packet was discarded because there were no bindings with the same MAC address and VLAN ID. dhcp permit: An ARP packet was forwarded because it matched a dynamic binding. static permit: An ARP packet was forwarded because it matched a static binding. In the SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. VLAN Setup screen, you can configure the Switch to generate log messages when ARP packets are discarded or forwarded based on the VLAN ID of the ARP packet.
Time	This field displays when the log message was generated.

62.4 ARP Inspection Setup

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 **SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. Setup**.

Figure 285 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. Setup

ARP Insp. Status	ARP Insp. VLAN Status	ARP Insp. Log Status	ARP Insp. Setup
ARP Inspection Setup			
Active		☐ OFF	
Filter Aging Time			
Filter Aging Time		300 seconds	
Log Profile			
Log Buffer Size		32 entries	
Syslog Rate		5 entries	
Log Interval		1 seconds	
		Apply Cancel	

The following table describes the labels in this screen.

Table 222 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. Setup

LABEL	DESCRIPTION
ARP Inspection Setup	
Active	Enable the switch button 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 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. Log Status screen to clear the log and reset this counter.
Syslog Rate	Type the maximum number of syslog messages the Switch can send to the syslog server in one batch. This number is expressed as a rate because the batch frequency is determined by the Log Interval. You must configure the syslog server to use this. Enter 0 if you do not want the Switch to send log messages generated by ARP packets to the syslog server. The relationship between Syslog Rate and Log Interval is illustrated in the following examples: - Four invalid ARP packets per second, Syslog Rate is 5, Log Interval is 1: the Switch sends 4 syslog messages every second. - Six invalid ARP packets per second, Syslog Rate is 5, Log Interval is 2: the Switch sends 5 syslog messages every 2 seconds.

Table 222 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. Setup (continued)

LABEL	DESCRIPTION
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.

62.5 ARP Inspection Port Setup

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 **SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. Port Setup**.

Figure 286 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. Port Setup

The screenshot shows the 'ARP Insp. Port Setup' configuration page. At the top, there are navigation tabs: 'p. VLAN Status', 'ARP Insp. Log Status', 'ARP Insp. Setup', and 'ARP Insp. Port Setup' (which is active and highlighted in green). Below the tabs is a table with the following structure:

Port	Trusted State	Limit	
		Rate(pps)	Burst Interval (seconds)
*	Untrusted ▼		
1	Untrusted ▼	15	1
2	Untrusted ▼	15	1
3	Untrusted ▼	15	1
4	Untrusted ▼	15	1
5	Untrusted ▼	15	1
6	Untrusted ▼	15	1
7	Untrusted ▼	15	1

At the bottom of the table, there is a green 'Apply' button and a grey 'Cancel' button.

The following table describes the labels in this screen.

Table 223 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. Port Setup

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

Table 223 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. Port Setup (continued)

LABEL	DESCRIPTION
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.

62.6 ARP Inspection VLAN Setup

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 **SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. VLAN Setup**.

Figure 287 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. VLAN Setup

ARP Insp. Log Status ARP Insp. Setup ARP Insp. Port Setup **ARP Insp. VLAN Setup**

Search VLAN by VID

The Number of VLANs: 1

« < Page 1 of 1 > »

VID	Enabled	Log
*	No	None
1	No	Deny

« < Page 1 of 1 > »

The following table describes the labels in this screen.

Table 224 SECURITY > IPv4 Source Guard > ARP Inspection > ARP Insp. VLAN Setup

LABEL	DESCRIPTION
Search VLAN by VID	Specify the VLANs you want to manage in the section below. Use a comma (,) to separate individual VLANs or a hyphen (-) to indicate a range of VLANs. For example, "3,4" or "3-9".
Search	Click this to display the specified range of VLANs in the section below.
The Number of VLANs	This display the number of ARP inspection VLAN search results.
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.

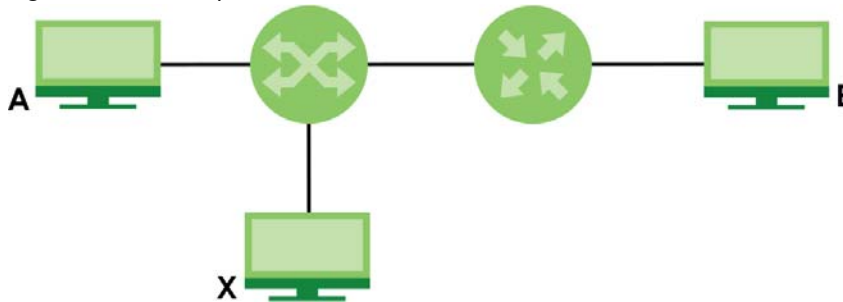
62.7 Technical Reference

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

62.7.1 ARP Inspection Overview

Use ARP inspection to filter unauthorized ARP packets on the network. This can prevent many kinds of man-in-the-middle attacks, such as the one in the following example.

Figure 288 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:

- 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.

62.7.1.1 ARP Inspection and MAC Address Filters

When the Switch identifies an unauthorized ARP packet, it automatically creates a MAC address filter to block traffic from the source MAC address and source VLAN ID of the unauthorized ARP packet. You can configure how long the MAC address filter remains in the Switch.

These MAC address filters are different than regular MAC address filters.

- They are stored only in volatile memory.
- They do not use the same space in memory that regular MAC address filters use.
- They appear only in the **ARP Inspection** screens and commands, not in the **MAC Address Filter** screens and commands.

62.7.1.2 Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for ARP inspection. This setting is independent of the trusted or untrusted setting for DHCP snooping. You can also specify the maximum rate at which the Switch receives ARP packets on untrusted ports.

The Switch does not discard ARP packets on trusted ports for any reason.

The Switch discards ARP packets on untrusted ports in the following situations:

- The sender's information in the ARP packet does not match any of the current bindings.
- The rate at which ARP packets arrive is too high.

62.7.1.3 Syslog

The Switch can send syslog messages to the specified syslog server when it forwards or discards ARP packets. The Switch can consolidate log messages and send log messages in batches to make this mechanism more efficient.

62.7.1.4 Configuring ARP Inspection

Follow these steps to configure ARP inspection on the Switch.

- 1 Configure DHCP snooping.

Note: It is recommended you enable DHCP snooping at least one day before you enable ARP inspection so that the Switch has enough time to build the binding table.

- 2 Enable ARP inspection on each VLAN.
- 3 Configure trusted and untrusted ports, and specify the maximum number of ARP packets that each port can receive per second.

CHAPTER 63

Port Authentication

63.1 Port Authentication Overview

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

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

- **IEEE 802.1x** – An authentication server validates access to a port based on a user name and password provided by the user. A user that fails an authentication server can still access the port, but traffic from the user is forwarded to the guest VLAN port.
- **MAC Authentication** – An authentication server validates access to a port based on the MAC address and password of the client.
- **Guest VLAN** – In either mode, if authentication fails the Switch can still allow the client to access the network on a **Guest VLAN**.
- **Compound Authentication** – An authentication server validates access to a port based on combination of IEEE 802.1x and MAC Authentication. There are two modes:
 - **Loose**: The client authenticates using either IEEE 802.1x authentication or MAC Authentication.
 - **Strict**: The client authenticates using both IEEE 802.1x authentication and MAC Authentication.

Note: All types of authentication use the RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) protocol to validate users. You must configure a RADIUS server before enabling port authentication.

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

Note: IEEE 802.1x is not supported by all user operating systems. For details on compatibility, see your operating system documentation. If your operating system does not support 802.1x, you must install 802.1x client software.

63.1.1 What You Can Do

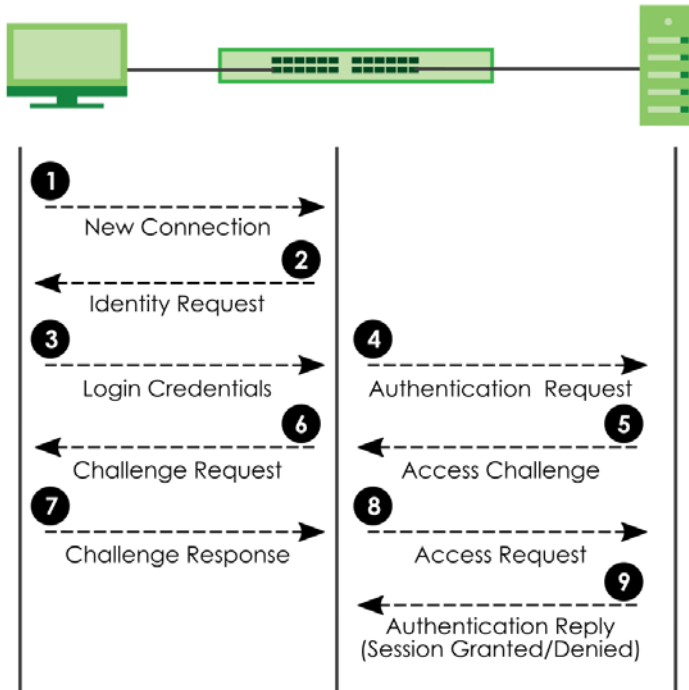
- Use the **802.1x** screen ([Section 63.2 on page 422](#)) to activate IEEE 802.1x security.
- Use the **MAC Authentication** screen ([Section 63.3 on page 423](#)) to activate MAC authentication.
- Use the **Guest VLAN** screen ([Section 63.4 on page 425](#)) to enable and assign a guest VLAN to a port.
- Use the **Compound Authentication** screen ([Section 63.5 on page 427](#)) to allow network access for clients that pass either IEEE 802.1x authentication OR MAC authentication, or pass both IEEE 802.1x authentication AND MAC authentication.

63.1.2 What You Need to Know

IEEE 802.1x Authentication

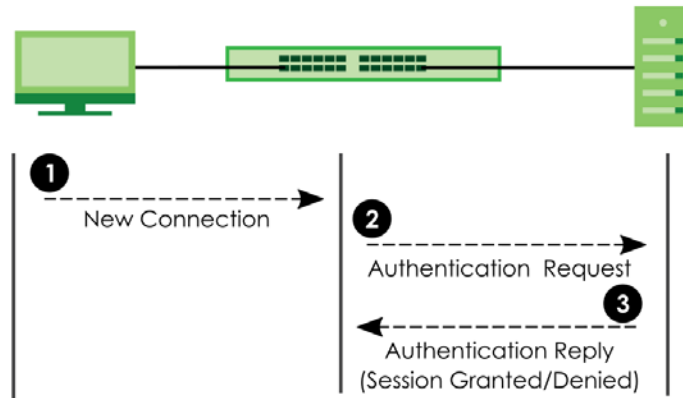
The following figure illustrates how a client connecting to a IEEE 802.1x authentication enabled port goes through a validation process. The Switch prompts the client for login information in the form of a user name and password after the client responds to its identity request. When the client provides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

Figure 289 IEEE 802.1x Authentication Process



63.1.3 MAC Authentication

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

Figure 290 MAC Authentication Process

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

63.2 Activate IEEE 802.1x Security

Use this screen to activate IEEE 802.1x security. Click **SECURITY > Port Authentication > 802.1x > 802.1x** to display the configuration screen as shown.

Figure 291 SECURITY > Port Authentication > 802.1x > 802.1x

802.1x

Active ☐ OFF

EAPOL flood ☐ OFF

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

The following table describes the labels in this screen.

Table 225 SECURITY > Port Authentication > 802.1x > 802.1x

LABEL	DESCRIPTION
Active	Enable the switch button to permit 802.1x authentication on the Switch. Note: You must first enable 802.1x authentication on the Switch before configuring it on each port.
EAPOL flood	Enable the switch button to flood EAPOL packets to all ports in the same VLAN. EAP over LAN (EAPOL) is a port authentication protocol used in IEEE 802.1x. It is used to encapsulate and transmit EAP packets between the supplicant (a client device that requests access to the network resources or services) and authenticator (the Switch) directly over the LAN. Note: EAPOL flood will not take effect when 802.1x authentication is enabled.
Port	This field displays the port number. * means all ports.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this to permit 802.1x authentication on this port. You must first allow 802.1x authentication on the Switch before configuring it on each port.
Max-Req	Specify the number of times the Switch tries to authenticate clients before sending unresponsive ports to the Guest VLAN. This is set to 2 by default. That is, the Switch attempts to authenticate a client twice. If the client does not respond to the first authentication request, the Switch tries again. If the client still does not respond to the second request, the Switch sends the client to the Guest VLAN. The client needs to send a new request to be authenticated by the Switch again.
Reauth	Specify if a subscriber has to periodically re-enter his or her user name and password to stay connected to the port.
Reauth-period secs	Specify the length of time required to pass before a client has to re-enter his or her user name and password to stay connected to the port.
Quiet-period secs	Specify the number of seconds the port remains in the HELD state and rejects further authentication requests from the connected client after a failed authentication exchange.
Tx-period secs	Specify the number of seconds the Switch waits for client's response before re-sending an identity request to the client.
Supp-Timeout secs	Specify the number of seconds the Switch waits for client's response to a challenge request before sending another request.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

63.3 Activate MAC Authentication

Use this screen to activate MAC authentication. Click **SECURITY > Port Authentication > MAC Authentication > MAC Authentication** to display the configuration screen as shown.

Figure 292 SECURITY > Port Authentication > MAC Authentication > MAC Authentication

MAC Authentication

Active: ☐ OFF

Name Prefix:

Delimiter:

Case: ☒ Upper ☐ Lower

Password Type: ☒ Static ☐ MAC Address

Password:

Timeout: seconds

Port	Active	Trusted-VLAN List
*	☐	
1	☐	
2	☐	
3	☐	
4	☐	
5	☐	
6	☐	
7	☐	
8	☐	
9	☐	
10	☐	
11	☐	
12	☐	

Apply Cancel

The following table describes the labels in this screen.

Table 226 SECURITY > Port Authentication > MAC Authentication > MAC Authentication

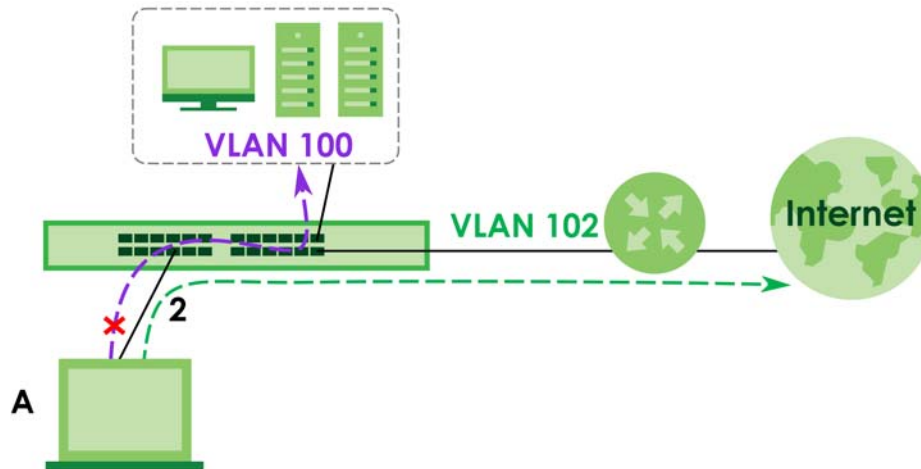
LABEL	DESCRIPTION
Active	Enable the switch button to permit MAC authentication on the Switch. Note: You must first enable MAC authentication on the Switch before configuring it on each port.
Name Prefix	Type the prefix that is appended to all MAC addresses sent to the RADIUS server for authentication. You can enter up to 32 printable ASCII characters except [?], [], ['], ["], [,], [.]. If you leave this field blank, then only the MAC address of the client is forwarded to the RADIUS server.
Delimiter	Select the delimiter the RADIUS server uses to separate the pairs in MAC addresses used as the account user name (and password). You can select Dash (-), Colon (:), or None to use no delimiters at all in the MAC address.
Case	Select the case (Upper or Lower) the RADIUS server requires for letters in MAC addresses used as the account user name (and password).
Password Type	Select Static to have the Switch send the password you specify below or MAC-Address to use the client MAC address as the password.
Password	Type the password the Switch sends along with the MAC address of a client for authentication with the RADIUS server. You can enter up to 32 printable ASCII characters except [?], [], ['], ["], or [,].

Table 226 SECURITY > Port Authentication > MAC Authentication > MAC Authentication (continued)

LABEL	DESCRIPTION
Timeout	Specify the amount of time (in seconds) before the Switch allows a client MAC address that fails authentication to try and authenticate again. Maximum time is 3000 seconds. When a client fails MAC authentication, its MAC address is learned by the MAC address table with a status of denied. The timeout period you specify here is the time the MAC address entry stays in the MAC address table until it is cleared. If you specify 0 for the timeout value, the Switch uses the Aging Time configured in the SYSTEM > Switch Setup > Switch Setup screen. Note: If the Aging Time in the SYSTEM > Switch Setup > Switch Setup screen is set to a lower value, then it supersedes this setting.
Port	This field displays a port number. * means all ports.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to permit MAC authentication on this port. You must first allow MAC authentication on the Switch before configuring it on each port.
Trusted-VLAN List	Enter the ID numbers of the trusted VLANs (separated by a comma). If a client's VLAN ID is specified here, the client can access the port and the connected networks without MAC authentication.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

63.4 Guest VLAN

When 802.1x or MAC Authentication is enabled on the Switch and its ports, clients that do not have the correct credentials are blocked from using the ports. You can configure your Switch to have one VLAN that acts as a guest VLAN. If you enable the guest VLAN (**102** in the example) on a port (**2** in the example), the user (**A** in the example) that is not IEEE 802.1x capable or fails to enter the correct user name 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 access granted to the Guest VLAN depends on how the network administrator configures switches or routers with the guest network feature.

Figure 293 Guest VLAN Example

Use this screen to enable and assign a guest VLAN to a port. Click **SECURITY > Port Authentication > Guest VLAN > Guest VLAN** to display the configuration screen as shown.

Figure 294 SECURITY > Port Authentication > Guest VLAN > Guest VLAN

Guest VLAN

Port	Active	Guest VLAN	Host-mode	Multi-secure Num
*	☐		Multi-Host v	
1	☐	1	Multi-Host v	1
2	☐	1	Multi-Host v	1
3	☐	1	Multi-Host v	1
4	☐	1	Multi-Host v	1
5	☐	1	Multi-Host v	1
6	☐	1	Multi-Host v	1
7	☐	1	Multi-Host v	1

The following table describes the labels in this screen.

Table 227 SECURITY > Port Authentication > Guest VLAN > Guest VLAN

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

Table 227 SECURITY > Port Authentication > Guest VLAN > Guest VLAN (continued)

LABEL	DESCRIPTION
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, the 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.

63.5 Compound Authentication

Use this screen to allow network access for clients that:

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

The authentication modes are:

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

Click **SECURITY > Port Authentication > Compound Authentication Mode > Compound Authentication Mode** to display the configuration screen as shown.

Figure 295 SECURITY > Port Authentication > Compound Authentication Mode > Compound Authentication Mode

Port	Compound Authentication Mode
*	Strict ▼
1	Strict ▼
2	Strict ▼
3	Strict ▼
4	Strict ▼
5	Strict ▼
6	Strict ▼
7	Strict ▼

Apply Cancel

The following table describes the labels in this screen.

Table 228 SECURITY > Port Authentication > Compound Authentication Mode > Compound Authentication Mode

LABEL	DESCRIPTION
Port	This field displays a port number. * means all ports.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Compound Authentication Mode	Specify how the Switch authenticates clients for network access. Select Strict to allow network access to clients only when clients passes IEEE 802.1x authentication AND MAC authentication at the same time. Select Loose to allow network access to clients when clients passes IEEE 802.1x authentication OR MAC authentication.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

63.6 Technical Reference

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

63.6.1 IEEE 802.1x

The IEEE 802.1x is a standard for authentication as well as providing additional accounting and control features. It can be implemented both on wired and wireless networks. It is supported by Windows XP and a number of network devices. Some advantages of IEEE 802.1x are:

- User based identification
- Support for RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) for centralized user profile and accounting management on a network RADIUS server.
- Support for EAP (Extensible Authentication Protocol, RFC 2486) that allows additional authentication methods to be deployed with no changes to the switch or the wired clients.

63.6.2 RADIUS

RADIUS is based on a client-server model that supports authentication, authorization and accounting. The RADIUS server handles the following tasks:

- Authentication

Determines the identity of the users.

- Authorization

Determines the network services available to authenticated users once they are connected to the network.

- Accounting

Keeps track of the actions that are performed on the switch, such as login events.

RADIUS is a simple package exchange in which your switch acts as a message relay between the wired client and the network RADIUS server.

63.6.2.1 Types of RADIUS Messages

The following types of RADIUS messages are exchanged between the switch and the RADIUS server for user authentication:

- Access-Request

Sent by a switch requesting authentication.

- Access-Reject

Sent by a RADIUS server rejecting access.

- Access-Accept

Sent by a RADIUS server allowing access.

- Access-Challenge

Sent by a RADIUS server requesting more information in order to allow access. The switch sends a proper response from the user and then sends another Access-Request message.

The following types of RADIUS messages are exchanged between the switch and the RADIUS server for user accounting:

- Accounting-Request

Sent by the switch requesting accounting.

- Accounting-Response

Sent by the RADIUS server to indicate that it has started or stopped accounting.

The switch and the RADIUS server use a shared secret key, which is a password, they both know to authenticate the communications between them, and ensure network security. A shared key is not sent over the network.

The switch forwards the RADIUS requests of a client to the RADIUS server. The login password information exchanged is sent over the network and encrypted to protect the network from unauthorized access.

63.6.3 EAP (Extensible Authentication Protocol) Authentication

This section discusses some popular authentication types: EAP-MD5, EAP-TLS, EAP-TTLS, PEAP and LEAP. Your wired LAN device may not support all authentication types.

EAP (Extensible Authentication Protocol) is an authentication protocol that runs on top of the IEEE 802.1x transport mechanism in order to support multiple types of user authentication. By using EAP to interact with an EAP-compatible RADIUS server, a switch helps a wired station and a RADIUS server perform authentication.

The type of authentication you use depends on the RADIUS server and an intermediary switch that supports IEEE 802.1x.

For EAP-TLS authentication type, you must first have a wired connection to the network and obtain the certificates from a certificate authority (CA). A certificate (also called digital IDs) can be used to authenticate users and a CA issues certificates and guarantees the identity of each certificate owner.

- EAP-MD5 (Message-Digest Algorithm 5)

MD5 authentication is the simplest one-way authentication method. The authentication server sends a challenge to the wired client. The wired client 'proves' that it knows the password by encrypting the password with the challenge and sends back the information. Password is not sent in plain text.

However, MD5 authentication has some weaknesses. Since the authentication server needs to get the plain text passwords, the passwords must be stored. Thus someone other than the authentication server may access the password file. In addition, it is possible to impersonate an authentication server as MD5 authentication method does not perform mutual authentication. Finally, MD5 authentication method does not support data encryption with dynamic session key. You must configure WEP encryption keys for data encryption.

- EAP-TLS (Transport Layer Security)

With EAP-TLS, digital certifications are needed by both the server and the wired clients for mutual authentication. The server presents a certificate to the client. After validating the identity of the server, the client sends a different certificate to the server. The exchange of certificates is done in the open before a secured tunnel is created. This makes user identity vulnerable to passive attacks. A digital certificate is an electronic ID card that authenticates the sender's identity. However, to implement

EAPTLS, you need a Certificate Authority (CA) to handle certificates, which imposes a management overhead.

- EAP-TTLS (Tunneled Transport Layer Service)

EAP-TTLS is an extension of the EAP-TLS authentication that uses certificates for only the server-side authentications to establish a secure connection. Client authentication is then done by sending user name and password through the secure connection, thus client identity is protected. For client authentication, EAP-TTLS supports EAP methods and legacy authentication methods such as PAP, CHAP, MS-CHAP and MS-CHAP v2.

- PEAP (Protected EAP)

Like EAP-TTLS, server-side certificate authentication is used to establish a secure connection, then use simple user name and password methods through the secured connection to authenticate the clients, thus hiding client identity. However, PEAP only supports EAP methods, such as EAP-MD5, EAP-MSCHAPv2 and EAP-GTC (EAP-Generic Token Card), for client authentication. EAP-GTC is implemented only by Cisco.

- LEAP

LEAP (Lightweight Extensible Authentication Protocol) is a Cisco implementation of IEEE 802.1x.

63.6.4 EAPOL (EAP over LAN)

EAPOL is a port authentication protocol used in IEEE 802.1x. It encapsulates and sends EAP packets from the LAN. EAPOL exchanges the following messages between a wired client and switch.

- EAPOL-Start

A wired client will send this message to a switch to let it know the wired client is ready.

- EAPOL-Key

The switch will send an encryption key to the wired client. It will be allowed access to the network when both of the switch and wired client have the correct encryption keys.

- EAP-Packet

Both of the wired client and the switch will send this message to complete the authentication process.

- EAPOL-Logoff

This message will be sent when the wired client wants to be disconnected from the network.

- EAPOL-Encapsulated-ASF-Alert

This message is sent if the authentication process is not completed yet, and alerts need to be forwarded.

CHAPTER 64

Port Security

64.1 Port Security Overview

This chapter shows you how to set up port security.

64.2 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.

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

64.3 Port Security Setup

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

Figure 296 SECURITY > Port Security > Port Security

Port Security | VLAN MAC Address Limit

MAC Freeze

Port List **MAC Freeze**

Port Security

Active ☐ OFF

Port	Active	Address Learning	Limited Number of Learned MAC Address
*	☐	☐	
1	☐	☒	0
2	☐	☒	0
3	☐	☒	0
4	☐	☒	0
5	☐	☒	0
6	☐	☒	0
7	☐	☒	0

Apply **Cancel**

The following table describes the labels in this screen.

Table 229 SECURITY > Port Security > Port Security

LABEL	DESCRIPTION
MAC Freeze	
Port List	Enter the number of the ports (separated by a comma) on which you want to enable port security and disable MAC address learning. After you click MAC Freeze , all previously learned MAC addresses on the specified ports will become static MAC addresses and display in the SWITCHING > Static MAC Forwarding > Static MAC Forwarding screen.
MAC Freeze	Click MAC Freeze to have the Switch automatically select the Active checkboxes and clear the Address Learning checkboxes only for the ports specified in the Port List .
Port Security	
Active	Enable the switch button to enable port security on the Switch.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some of the settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.

Table 229 SECURITY > Port Security > Port Security (continued)

LABEL	DESCRIPTION
Active	Select this checkbox to enable the port security feature on this port. The Switch forwards packets whose MAC addresses is in the MAC address table on this port. Packets with no matching MAC addresses are dropped. Clear this checkbox to disable the port security feature. The Switch forwards all packets on this port.
Address Learning	MAC address learning reduces outgoing broadcast traffic. For MAC address learning to occur on a port, the port itself must be active with address learning enabled.
Limited Number of Learned MAC Address	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device must wait until one of the five learned MAC addresses ages out. MAC address aging out time can be set in the SYSTEM > Switch Setup screen. The valid range is from "0" to "32K". "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.

64.4 VLAN MAC Address Limit

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

Figure 297 SECURITY > Port Security > VLAN MAC Address Limit

The screenshot shows the 'VLAN MAC Address Limit' configuration screen. At the top, there are tabs for 'Port Security' and 'VLAN MAC Address Limit'. Below the tabs is a table with the following columns: Index, Active, Port, VID, and Limit Number. There are 'Add/Edit' and 'Delete' buttons at the top right of the table.

The following table describes the labels in this screen.

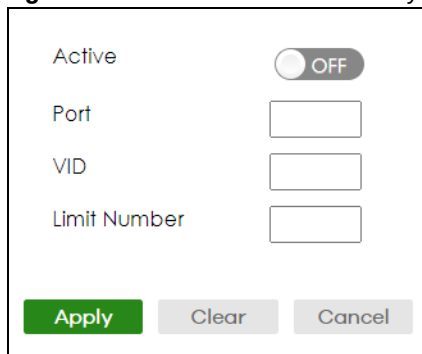
Table 230 SECURITY > Port Security > VLAN MAC Address Limit

LABEL	DESCRIPTION
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Index	This field displays the index number of the rule.
Active	This field displays whether the rule is activated or not.
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.
Add/Edit	Click Add/Edit to add a new entry or edit a selected one.
Delete	Click Delete to remove the selected entries.

64.4.1 VLAN MAC Address Limit

Use this screen to add/edit the MAC address learning limit on per-port and per-VLAN basis. Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SECURITY > Port Security > VLAN MAC Address Limit** screen to display this screen.

Figure 298 SECURITY > Port Security > VLAN MAC Address Limit > Add/Edit



The following table describes the labels in this screen.

Table 231 SECURITY > Port Security > VLAN MAC Address Limit > Add/Edit

LABEL	DESCRIPTION
Port	Enter the number of the port to which this rule is applied.
VID	Enter the VLAN identification number.
Limit Number	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port in a specified VLAN. For example, if you set this field to "5" on port 2, then only the devices with these 5 learned MAC addresses may access port 2 at any one time. A sixth device would have to wait until one of the 5 learned MAC addresses aged out. MAC address aging out time can be set in the SYSTEM > Switch Setup screen. The valid range is from "0" to "32K". "0" means this feature is disabled.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

CHAPTER 65

MAINTENANCE

65.1 Overview

This chapter explains how to configure the screens that let you maintain the firmware and configuration files.

65.1.1 What You Can Do

- Use the **Certificates** screen ([Section 65.2 on page 437](#)) to see the **Certificates** screen and import the Switch's CA-signed certificates.
- Use the **Cluster Management** screens ([Section 65.5 on page 441](#)) to manage the switches within a cluster and view cluster status.
- Use the **Restore Configuration** screen ([Section 65.8 on page 446](#)) to upload a stored device configuration file.
- Use the **Backup Configuration** screen ([Section 65.9 on page 446](#)) to save your configurations for later use.
- Use the **Auto Configuration** screen ([Section 65.10 on page 447](#)) to overwrite the running configuration stored in the Switch's RAM.
- Use the **Erase Running-Configuration** screen ([Section 65.11 on page 449](#)) to reset the configuration to the Zyxel default configuration settings.
- Use the **Save Configuration** screen ([Section 65.12 on page 449](#)) to save the current configuration settings to a specific configuration file on the Switch.
- Use the **Configure Clone** screen ([Section 65.13 on page 450](#)) to copy the basic and advanced settings from a source port to a destination port or ports.
- Use the **Diagnostic** screen ([Section 65.14 on page 452](#)) to ping IP addresses, run a traceroute, perform port tests or show the Switch's location between devices.
- Use the **Firmware Upgrade** screen ([Section 65.15 on page 453](#)) to upload the latest firmware.
- Use the **Reboot System** screen ([Section 65.16 on page 455](#)) to restart the Switch without physically turning the power off and load a specific configuration file.
- Use the **SSH Authorized Keys** screen ([Section 65.17 on page 456](#)) to authenticate secure SSH connections between a client computer and the Switch (also called the server) without needing a password to connect to the Switch.
- Use the **SSH Host Keys** screen ([Section 65.18 on page 463](#)) to regenerate the Switch's SSH host key. You may want to do this to change the factory default SSH host key.
- Use the **Tech-Support** screen ([Section 65.19 on page 463](#)) to create reports for customer support if there are problems with the Switch.

65.2 Certificates

The Switch can use HTTPS certificates that are verified by a third party to create secure HTTPS connections between your computer and the Switch. This way, you may securely access the Switch using the Web Configurator. See [Section 53.5.2 on page 358](#) for more information about HTTPS.

Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

Click **MAINTENANCE > Certificates > Certificates** to open the following screen. Use this screen to import the Switch's CA-signed certificates.

Figure 299 MAINTENANCE > Certificates > Certificates

Service	Subject	Issuer	Valid From	Valid To
☐ HTTPS	/CN=CX4800 f44d5c7c7b14	/CN=CX4800 f44d5c7c7b14	Jun 4 17:07:55 2024 GMT	Aug 28 17:07:55 2084 GMT

The following table describes the labels in this screen.

Table 232 MAINTENANCE > Certificates > Certificates

LABEL	DESCRIPTION
File Path	Click Choose File or Browse to find the certificate file you want to upload.
Password	Enter the certificate file's password that was created when the PKCS #12 file was exported. The password consists of up to 32 printable ASCII characters except [?], [], ['], ["], or [,].
Import	Click this button to save the certificate that you have enrolled from a certification authority from your computer to the Switch.
Service	This field displays the service type that this certificate is for.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires.
	Select an entry's checkbox to select a specific entry.
Delete	Click this button to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

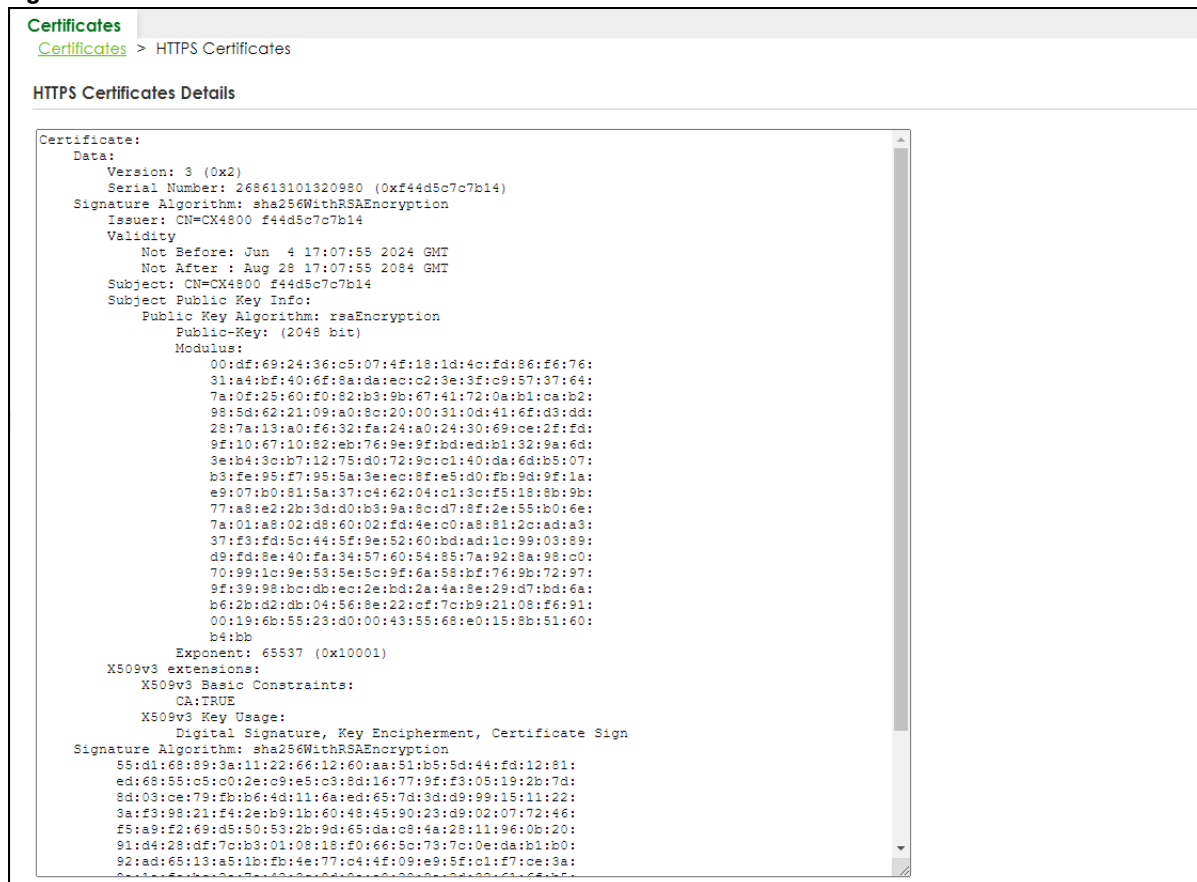
65.2.1 Install Certificates

After buying the certificates from a trusted third-party Certificate Authorities (CA), (for example, DigiCert), install the certificates. See [Importing a Certificate](#) for more information.

65.2.2 HTTPS Certificates

Use this screen to view the HTTPS certificate details. Click a hyperlink in the **Service** column in the **MAINTENANCE > Certificates > Certificates** screen to open the following screen.

Figure 300 MAINTENANCE > Certificates > HTTPS



65.3 Technical Reference

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

65.3.1 FTP Command Line

This section shows some examples of uploading to or downloading files from the Switch using FTP commands. First, understand the filename conventions.

65.3.2 Filename Conventions

The configuration file (also known as the romfile or ROM) contains the Zyxel factory default configuration settings in the screens such as password, Switch setup, IP Setup, and so on. Once you have customized the Switch's settings, they can be saved back to your computer under a filename of your choosing.

FaOS (sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension.

Table 233 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	config1 config2	*.cfg	This is the configuration filename on the Switch. Uploading the config file replaces the specified configuration file system, including your Switch configurations, system-related data (including the default password), the error log and the trace log.
Firmware	ras	*.bin	This is the generic name for the FaOS firmware on the Switch.

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.

65.3.2.1 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's **Firmware 1**.

```
ftp> get config1 config1.cfg
```

This is a sample FTP session saving the Switch's configuration file 1 (**Config1**) to a file called "config1.cfg" on your computer.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the Switch only recognizes "config" and "ras". Be sure you keep unaltered copies of both files for later use.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

65.3.3 FTP Command Line Procedure

- 1 Launch the FTP client on your computer.

- 2 Enter open, followed by a space and the IP address of your Switch.
- 3 Press [ENTER] when prompted for a user name.
- 4 Enter your password as requested (see the back label on the Switch for the default).
- 5 Enter bin to set transfer mode to binary.
- 6 Use put to transfer files from the computer to the Switch, for example, put firmware.bin ras transfers the firmware on your computer (firmware.bin) to the Switch and renames it to "ras". Similarly, put config.cfg config1 transfers the configuration file on your computer (config.cfg) to the Switch and renames it to "config1". Likewise get config1 config config.cfg transfers the configuration file on the Switch to your computer and renames it to "config.cfg".
- 7 Enter quit to exit the ftp prompt.

65.3.4 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 234 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 single-byte printable characters (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

65.3.5 FTP Restrictions

FTP will not work when:

- FTP service is disabled in the **SECURITY > Access Control > Service Access Control > Service Access Control** screen.
- The IP addresses in the **SECURITY > Access Control > Remote Management > Remote Management** screen does not match the client IP address. If it does not match, the Switch will disconnect the FTP session immediately.

65.4 Cluster Management Overview

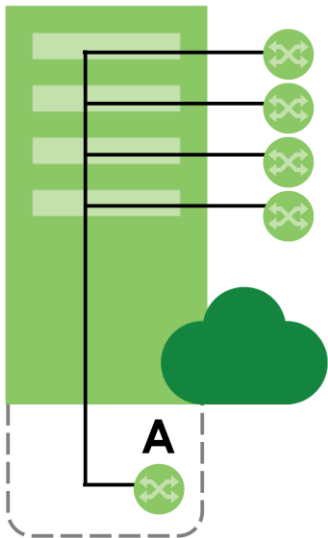
Cluster Management allows you to manage switches through one Switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

Table 235 Zyxel Clustering Management Specifications

Maximum number of cluster members	24
Cluster Member Models	Must be compatible with Zyxel cluster management implementation.
Cluster Manager	The Switch through which you manage the cluster member switches.
Cluster Members	The switches being managed by the cluster manager Switch.

In the following example, switch **A** in the basement is the cluster manager and the other switches on the upper floors of the building are cluster members.

Figure 301 Clustering Application Example



65.4.1 What You Can Do

- Use the **Cluster Management Status** screen ([Section 65.5 on page 441](#)) to view the role of the Switch within the cluster and to access a cluster member Switch's Web Configurator.
- Use the **Cluster Management Setup** screen ([Section 65.6 on page 442](#)) to configure clustering management.

65.5 Cluster Management Status

Use this screen to view the role of the Switch within the cluster and to access a cluster member Switch's Web Configurator.

Click **MAINTENANCE > Cluster Management > Cluster Management Status** in the navigation panel to display the following screen.

Note: A cluster can only have one manager.

Figure 302 MAINTENANCE > Cluster Management > Cluster Management Status

Index	MAC Address	Name	Model	Status
The Number Of Member = 0				

The following table describes the labels in this screen.

Table 236 MAINTENANCE > Cluster Management > Cluster Management Status

LABEL	DESCRIPTION
Status	This field displays the role of this Switch within the cluster. Manager Member (you see this if you access this screen in the cluster member Switch directly and not through 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 through the cluster manager Switch. Each number in the Index column is a hyperlink leading to the cluster member Switch's Web Configurator.
MAC Address	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, and so on) Offline (the Switch is disconnected – Offline shows approximately 1.5 minutes after the link between cluster member and manager goes down)

65.6 Clustering Management Setup

Use this screen to configure clustering management. Click **MAINTENANCE > Cluster Management > Cluster Management Setup** to display the next screen.

Figure 303 MAINTENANCE > Cluster Management > Cluster Management Setup

The following table describes the labels in this screen.

Table 237 MAINTENANCE > Cluster Management > Cluster Management Setup

LABEL	DESCRIPTION
Clustering Manager	The following fields relate to configuring the cluster manager.
Active	Enable the switch button to have this Switch become the cluster manager switch. A cluster can only have one manager. Other (directly connected) switches that are set to be cluster managers will not be visible in the Clustering Candidates list. If a Switch that was previously a cluster member is later set to become a cluster manager, then its Status is displayed as Error in the Cluster Management Status screen and a warning icon (⚠) appears in the member summary list below.
Name	Type a name to identify the Clustering Manager . You may use up to 32 printable ASCII characters except [?], [], ['], ["], or [,]. (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 next summary table shows the information for the clustering members configured.
Add/Edit	Click this button to create or configure a clustering candidate.
Delete	Click this button to remove the clustering candidate.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Index	This is the index number of a cluster member switch.
MAC Address	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.

Click the **Add/Edit** button to open the **Add/Edit** screen. Use this screen to configure a clustering candidate for the Switch.

Figure 304 MAINTENANCE > Cluster Management > Cluster Management Setup > Add/Edit

The following table describes the labels in this screen.

Table 238 MAINTENANCE > Cluster Management > Cluster Management Setup > Add/Edit

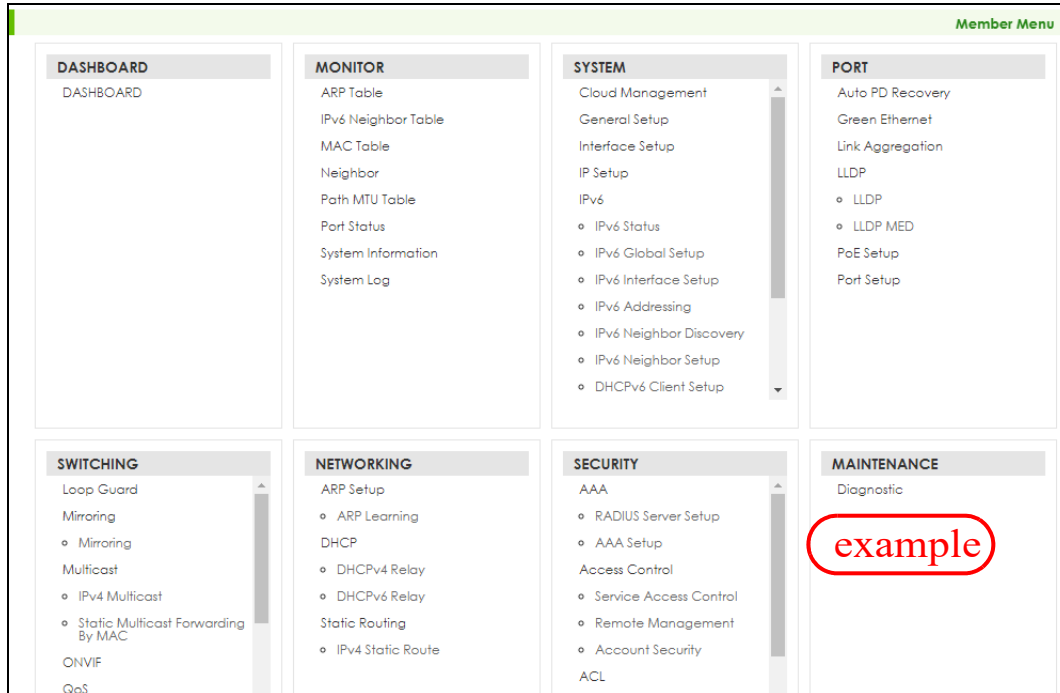
LABEL	DESCRIPTION
List	A list of suitable candidates found by auto-discovery is shown here. The switches must be directly connected. Directly connected switches that are set to be cluster managers will not be visible in the Clustering Candidate list. Switches that are not in the same management VLAN 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. You can enter 4 up to 32 printable ASCII characters except [?], [], ['], ["], or [,]. The default password is on the label on the bottom of 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.
Clear	Click Clear to reset the fields to the factory defaults.
Cancel	Click Cancel to begin configuring this screen afresh.

65.7 Technical Reference

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

65.7.1 Cluster Member Switch Management

Go to the **MAINTENANCE > Cluster Management > Clustering Management Status** screen of the cluster manager switch and then select an **Index** hyperlink from the list of members to go to that cluster member switch's Web Configurator home page. This cluster member Web Configurator home page and the home page that you would see if you accessed it directly are different.

Figure 305 Cluster Management: Cluster Member Web Configurator Screen

65.7.1.1 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 306 Example: Uploading Firmware to a Cluster Member Switch

```
C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 Switch FTP version 1.0 ready at Thu Jan 1 00:58:46 1970
User (192.168.0.1:(none)): admin
331 Enter PASS command
Password:
230 Logged in
ftp> ls
200 Port command okay
150 Opening data connection for LIST
--w--w--w- 1 owner group 3042210 Jul 01 12:00 ras
-rw-rw-rw- 1 owner group 393216 Jul 01 12:00 config
--w--w--w- 1 owner group 0 Jul 01 12:00 fw-00-a0-c5-01-23-46
-rw-rw-rw- 1 owner group 0 Jul 01 12:00 config-00-a0-c5-01-23-46
226 File sent OK
ftp: 297 bytes received in 0.00Seconds 297000.00Kbytes/sec.
ftp> bin
200 Type I OK
ftp> put 470ACAQ0.bin fw-00-a0-c5-01-23-46
200 Port command okay
150 Opening data connection for STOR fw-00-a0-c5-01-23-46
226 File received OK
ftp: 262144 bytes sent in 0.63Seconds 415.44Kbytes/sec.
ftp>
```

The following table explains some of the FTP parameters.

Table 239 FTP Upload to Cluster Member Example

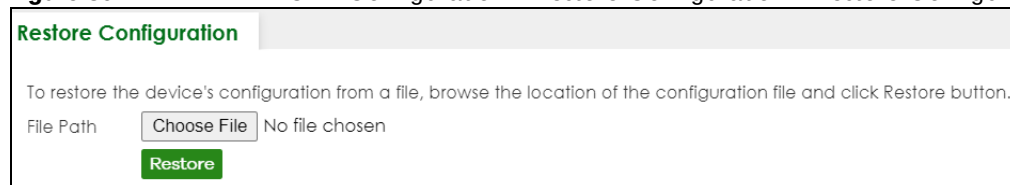
FTP PARAMETER	DESCRIPTION
User	Enter "admin".
Password	The Web Configurator password default is on the back label of the Switch.
ls	Enter this command to list the name of cluster member switch's firmware and configuration file.
470ACAQ0.bin	This is the name of the firmware file you want to upload to the cluster member switch.
fw-00-a0-c5-01-23-46	This is the cluster member switch's firmware name as seen in the cluster manager switch.
config-00-a0-c5-01-23-46	This is the cluster member switch's configuration file name as seen in the cluster manager switch.

65.8 Restore Configuration

Use this screen to restore a previously saved configuration file (See [Section 65.9 on page 446](#) for more information on how to back up a configuration file) from your computer to the Switch.

Click **MAINTENANCE > Configuration > Restore Configuration > Restore Configuration** to access this screen.

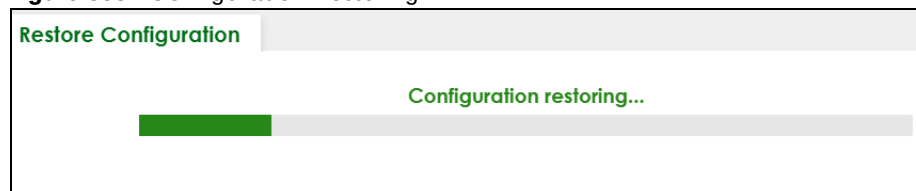
Figure 307 MAINTENANCE > Configuration > Restore Configuration > Restore Configuration



- 1 Click **Choose File** or **Browse** to locate the configuration file you wish to restore.
- 2 After you have specified the file, click **Restore**.

The Switch will run on the restored configuration after the restore process.

Figure 308 Configuration Restoring

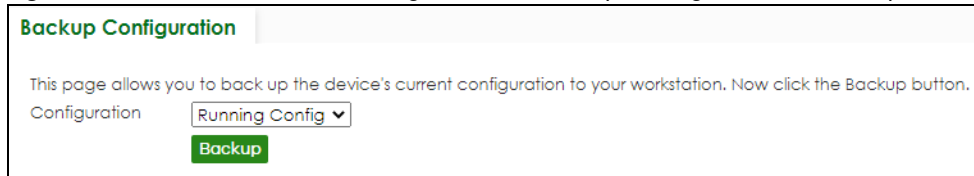


65.9 Backup Configuration

Backing up your Switch configurations allows you to create various "snap shots" of your device from which you may restore at a later date. Use this screen to back up your current Switch configuration to a computer.

To access this screen, click **MAINTENANCE > Configuration > Backup Configuration > Backup Configuration** in the navigation panel.

Figure 309 MAINTENANCE > Configuration > Backup Configuration > Backup Configuration



Follow the steps below to back up the current Switch configuration to your computer in this screen.

- 1 Select which Switch configuration file you want to download to your computer.

Note: **Custom Default** is only available in Standalone mode.

- 2 Click **Backup**.
- 3 If the current configuration file is open and/or downloaded to your computer automatically, you can click **File > Save As** on your computer to save the file to a specific place.
If a dialog box pops up asking whether you want to open or save the file, click **Save** or **Save File** to download it to the default downloads folder on your computer. If a **Save As** screen displays after you click **Save** or **Save File**, choose a location to save the file on your computer from the **Save in** drop-down list box and type a descriptive name for it in the **File name** list box. Click **Save** to save the configuration file to your computer.

65.10 Auto Configuration

The Switch can download a pre-saved auto configuration file automatically when you reboot the Switch using the DHCP or HTTPS mode. This will overwrite the running configuration stored in the Switch's RAM instead of the startup configuration stored in the Switch's flash memory.

To access this screen, click **MAINTENANCE > Configuration > Auto Configuration > Auto Configuration** in the navigation panel.

Figure 310 MAINTENANCE > Configuration > Auto Configuration > Auto Configuration

Auto Configuration

Mode: None
 State: None
 Filename:

Active: ☐ OFF
 Mode:
 DHCP VLAN ID:
 HTTPS URL:

The following table describes the labels in this screen.

Table 240 MAINTENANCE > Configuration > Auto Configuration > Auto Configuration

LABEL	DESCRIPTION
Use this section to view the auto configuration status after you restarted the Switch.	
Mode	This field shows the mode (DHCP or HTTPS) that is used for auto configuration after you enabled auto configuration and restarted the Switch. It shows None if auto configuration was not enabled.
State	This field shows whether auto configuration was executed successfully the last time the Switch rebooted. None – Auto configuration was disabled and not executed. Success – An auto configuration file was downloaded successfully to the Switch. Un-success – An auto configuration file was not downloaded to the Switch.
Filename	This field displays the name of the auto configuration file that was downloaded the last time the Switch rebooted. It shows blank if auto configuration was not enabled or not executed successfully.
Use this section to enable auto configuration and select the mode that you want to use for auto configuration.	
Active	Enable the switch button to enable auto configuration.
Mode	Select DHCP to have the Switch use the TFTP server IP address and auto configuration file name assigned by a DHCP server to download a pre-saved configuration file when the Switch reboots. Note: The Switch should act as a DHCP client to send a DHCP request with DHCP option 60 so that it can get the TFTP server address and configuration file name from the DHCP server. Select HTTPS to have the Switch use the URL you specified in the HTTPS URL field to access a web server and download the auto configuration file using HTTPS.
DHCP VLAN ID	Enter the VLAN ID of the DHCP server that assigns the TFTP server IP address and auto configuration file name to the Switch.

Table 240 MAINTENANCE > Configuration > Auto Configuration > Auto Configuration (continued)

LABEL	DESCRIPTION
HTTPS URL	Enter the URL that can be used to access and download the auto configuration file from a web server using HTTPS. For example, https://webserverIPaddress/configfilename.cfg. Note: You must fill in this field if you select HTTPS in the Mode field. Otherwise, auto configuration will not work.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

65.11 Erase Running-Configuration

Follow the steps below to remove the running configuration on the Switch. Unlike when you reset the Switch to the factory defaults, the user name, password, system logs, memory logs, baud rate and SSH service are not removed.

To access this screen, click **MAINTENANCE > Configuration > Erase Running Configuration > Erase Running Configuration** in the navigation panel.

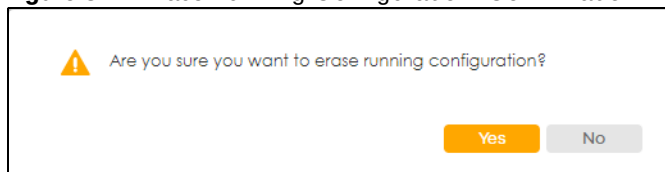
- 1 In the **Erase Running Configuration** screen, click the **Erase** button to clear all Switch configuration information you configured and return to the Zyxel default configuration settings.

Figure 311 MAINTENANCE > Configuration > Erase Running Configuration > Erase Running Configuration



- 2 Click **YES** to remove the running configuration on the Switch.

Figure 312 Erase Running Configuration: Confirmation



- 3 In the Web Configurator, click the **Save** button in the top of the screen to make the changes take effect. If you want to access the Switch Web Configurator again, you may need to change the IP address of your computer to be in the same subnet as that of the default Switch IP address (192.168.1.1 or DHCP-assigned IP).

65.12 Save Configuration

To access this screen, click **MAINTENANCE > Configuration > Save Configuration > Save Configuration** in the navigation panel.

Click **Config 1** to save the current configuration settings permanently to **Configuration 1** on the Switch. These configurations are set up according to your network environment.

Click **Config 2** to save the current configuration settings permanently to **Configuration 2** on the Switch. These configurations are set up according to your network environment.

Click **Custom Default** to save the current configuration settings permanently to a customized default file on the Switch. If configuration changes cause the Switch to behave abnormally, click **Custom Default** (in the **MAINTENANCE > Reboot System > Reboot System** screen) to have the Switch automatically reboot and restore the saved **Custom Default** configuration file.

Note: **Custom Default** is only available in Standalone mode.

Figure 313 MAINTENANCE > Configuration > Save Configuration > Save Configuration



Note: If a customized default file was not saved, clicking **Custom Default** in the **MAINTENANCE > Reboot System > Reboot System** screen loads the factory default configuration on the Switch.

Alternatively, click **Save** on the top right in any screen to save the configuration changes to the current configuration.

Note: Clicking the **Apply** button after making configuration does NOT save the changes permanently. All unsaved changes are erased after you reboot the Switch.

65.13 Configure Clone

Cloning allows you to copy the basic and advanced settings from a source port to a destination port or ports. Click **MAINTENANCE > Configuration > Configure Clone > Configure Clone** to open the following screen.

Figure 314 MAINTENANCE > Configuration > Configure Clone > Configure Clone

Configure Clone

Configure Clone

Source Destination

Port

Port Features

☐ **SYSTEM**

☐ SNMP Trap

☐ **PORT**

☐ Active ☐ BPDU Control ☐ LLDP

☐ Name ☐ Speed / Duplex ☐ FEC

☐ **SWITCHING**

☐ Diffserv ☐ IGMP Filtering ☐ Loop Guard

☐ Mirroring ☐ Multiple Rapid Spanning Tree Protocol ☐ Multiple Spanning Tree Protocol

☐ Port-based VLAN ☐ Protocol-based VLAN ☐ Queuing Method

☐ sFlow ☐ STP ☐ VLAN1q

☐ VLAN Mapping ☐ VLAN1q Member ☐ VLAN Stacking

☐ **NETWORKING**

☐ ARP Learning

☐ **SECURITY**

☐ Anti-Arpscan ☐ ARP Inspection ☐ BPDU Guard

☐ CPU Protection ☐ DHCP Snooping ☐ MAC Authentication

☐ Port Access Authenticator ☐ Port Security ☐ Storm Control

Apply **Cancel**

The following table describes the labels in this screen.

Table 241 MAINTENANCE > Configuration > Configure Clone > Configure Clone

LABEL	DESCRIPTION
Configure Clone	
Source/ Destination	Enter the source port under the Source label. This port's attributes are copied.
Port	Enter the destination port or ports under the Destination label. These are the ports which are going to have the same attributes as the source port. You can enter individual ports separated by a comma or a range of ports by using a dash. Example: 2, 4, 6 indicates that ports 2, 4 and 6 are the destination ports. 2-6 indicates that ports 2 through 6 are the destination ports.
Port Features	
	Select a feature's checkbox to select a specific feature. Otherwise, select the checkbox in the table heading row to select all features for a category.
SYSTEM	Select the system feature (you configured in the SYSTEM menus) to be copied to the destination ports. Otherwise, select the SYSTEM checkbox in the table heading row to select all features for a category.
PORT	Select which port features (you configured in the PORT menus) should be copied to the destination ports. Otherwise, select the PORT checkbox in the table heading row to select all features for a category.

Table 241 MAINTENANCE > Configuration > Configure Clone > Configure Clone (continued)

LABEL	DESCRIPTION
SWITCHING	Select which switching features (you configured in the SWITCHING menus) should be copied to the destination ports. Otherwise, select the SWITCHING checkbox in the table heading row to select all features for a category.
NETWORKING	Select the networking feature (you configured in the NETWORKING menus) to be copied to the destination ports. Otherwise, select the NETWORKING checkbox in the table heading row to select all features for a category.
SECURITY	Select which security features (you configured in the SECURITY menus) should be copied to the destination ports. Otherwise, select the SECURITY checkbox in the table heading row to select all features for a category.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

65.14 Diagnostic

Click **MAINTENANCE > Diagnostic > Diagnostic** in the navigation panel to open this screen. Use this screen to ping IP addresses, run a traceroute, perform port tests or show the Switch's location between devices.

Figure 315 MAINTENANCE > Diagnostic > Diagnostic

Diagnostic

- Info -

Ping Test

☒ IPv4

IP Address/Host Name

Source IP Address

Count

Ping

Trace Route Test

☒ IPv4

IP Address/Host Name

TTL

Wait Time Seconds

Queries

Trace Route

Ethernet Port Test

Port

Port Test

Locator LED

Minutes

Blink **Stop**

The following table describes the labels in this screen.

Table 242 MAINTENANCE > Diagnostic > Diagnostic

LABEL	DESCRIPTION
Ping Test	
IPv4	Select this option if you want to ping an IPv4 address, and select which traffic flow (in-band or out-of-band) the Switch is to send ping frames. If you select in-band, the Switch sends the frames to all ports except the management port (labeled MGMT). If you select out-of-band, the Switch sends the frames to the management port (labeled MGMT). Otherwise, select – to send ping requests to all VLANs on the Switch.
IP Address/Host Name	Type the IP address or host name of a device that you want to ping in order to test a connection. Click Ping to have the Switch ping the IP address.
Source IP Address	Type the source IP address that you want to ping in order to test a connection. Click Ping to have the Switch ping the IP address.
Count	Enter the number of ICMP Echo Request (ping) messages the Switch continuously sends.
Trace Route Test	
IPv4	Select this option if you want to trace the route packets take to a device with an IPv4 address, and select in-band or out-of-band on which the Switch traces the path. Otherwise, select – to trace the path on any VLAN.
IP Address/Host Name	Enter the IP address or host name of a device to which you want to perform a traceroute. Click Trace Route to have the Switch perform the traceroute function. This determines the path a packet takes to the specified device.
TTL	Enter the Time To Live (TTL) value for the ICMP Echo Request packets. This is to set the maximum number of the hops (routers) a packet can travel through. Each router along the path will decrement the TTL value by one and forward the packets. When the TTL value becomes zero and the destination is not found, the router drops the packets and informs the sender.
Wait Time	Specify how many seconds the Switch waits for a response to a probe before running another traceroute.
Queries	Specify how many times the Switch performs the traceroute function.
Ethernet Port Test	
Port	Enter a port number and click Port Test to perform an internal loopback test.
Locator LED	
	Enter a time interval (in minutes) and click Blink to show the actual location of the Switch between several devices in a rack. The default time interval is 30 minutes. Click Stop to have the Switch terminate the blinking locator LED.

65.15 Firmware Upgrade

You can upgrade the Switch's firmware through Web Configurator or NCC.

Firmware Upgrade Through NCC

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

On the NCC web portal, go to **Site-wide > Configure > Firmware management > Firmware management** to schedule the firmware upgrade time.

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

Firmware Upgrade Through the Web Configurator

Use the following screen to upgrade your Switch to the latest firmware. The Switch supports dual firmware images, **Firmware 1** and **Firmware 2**. Use this screen to specify which image is updated when firmware is uploaded using the Web Configurator and to specify which image is loaded when the Switch starts up.

Note: Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.

Click **MAINTENANCE > Firmware Upgrade > Firmware Upgrade** to view the screen as shown next.

Figure 316 MAINTENANCE > Firmware Upgrade > Firmware Upgrade

Firmware Upgrade

Firmware Upgrade

Name	Version
CX4800-56F	Running V1.00(ACJN.0)b9 09/13/2024
	Firmware 1 V1.00(ACJN.0)b9 09/13/2024
	Firmware 2 V1.00(ACJN.0)b8 08/27/2024

Boot Image

Current Boot image: Firmware 1

Config Boot image: Firmware 1

Apply **Cancel**

To upgrade the switch firmware, browse the location of the binary (.BIN) file and click Upgrade button.

Firmware: 1

File Path: **Choose File** No file chosen

Upgrade

The top of the screen shows which firmware version is currently **Running** on the Switch. Click **Choose File** or **Browse** to locate the firmware file you wish to upload to the Switch in the **File Path** field. Click **Upgrade** to load the new firmware. The Switch does not apply the uploaded firmware immediately. Firmware upgrades are only applied after you reboot the Switch using the uploaded firmware.

Click the **Config Boot Image** drop-down list box to select the boot image (**Firmware1** or **Firmware2**) you want the Switch to use when rebooting, click **Apply**. Restart the Switch (manually or using the **MAINTENANCE > Reboot System > Reboot System** screen) to apply the firmware image you selected.

After the process is complete, see the **DASHBOARD** screen to verify your current firmware version number.

Table 243 MAINTENANCE > Firmware Upgrade > Firmware Upgrade

LABEL	DESCRIPTION
Name	This is the name of the Switch that you are configuring.
Version	The Switch has 2 firmware sets, Firmware 1 and Firmware 2, residing in flash. Running shows the version number (and model code) and MM/DD/YYYY creation date of the firmware currently in use on the Switch (Firmware 1 or Firmware 2). The firmware information is also displayed at System Information in Basic Setting. 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.
Boot Image	
Current Boot Image	This displays which firmware is currently in use on the Switch (Firmware 1 or Firmware 2).
Config Boot Image	Select which firmware (Firmware 1 or Firmware 2) should load, click Apply and reboot the Switch to see changes, you will also see changes in the Current Boot Image field above as well.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Firmware	Choose to upload the new firmware to (Firmware) 1 or (Firmware) 2 .
File Path	Click Choose File or Browse to locate the firmware file you wish to upload to the Switch.
Upgrade	Click Upgrade to load the new firmware. Firmwares are only applied after a reboot. To reboot, go to MAINTENANCE > Reboot System > Reboot System and click Config 1 , Config 2 or Factory Default (Config 1 , Config 2 , Factory Default , and Custom Default are the configuration files you want the Switch to use when it restarts).

65.16 Reboot System

Reboot System allows you to restart the Switch without physically turning the power off. It also allows you to load configuration one (**Config 1**), configuration two (**Config 2**), a **Custom Default** or the **Factory Default** configuration when you reboot. Follow the steps below to reboot the Switch.

Note: **Custom Default** is only available in Standalone mode.

Click **MAINTENANCE > Reboot System > Reboot System** to view the screen as shown next.

Figure 317 MAINTENANCE > Reboot System > Reboot System

Reboot System

Current Configuration is Configuration 1

Reboot System with

Config 1

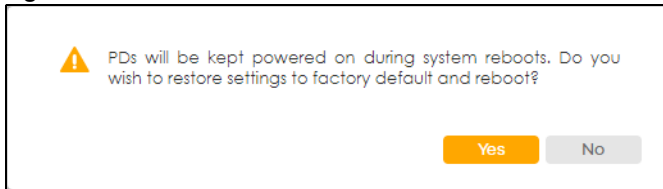
Config 2

Factory Default

Custom Default

- 1 Click the **Config 1**, **Config 2**, **Factory Default**, or **Custom Default** button to reboot and load that configuration file. The confirmation screen displays.

Figure 318 Reboot Confirmation



- 2 Click **YES** and then wait for the Switch to restart. This takes up to 2 minutes.

Click **Config 1** and follow steps 1 to 2 to reboot and load configuration one on the Switch.

Click **Config 2** and follow steps 1 to 2 to reboot and load configuration two on the Switch.

Click **Factory Default** and follow steps 1 to 2 to reboot and load Zyxel factory default configuration settings on the Switch.

Click **Custom Default** and follow steps 1 to 2 to reboot and load a customized default file on the Switch. This will save the custom default configuration settings to both **Configuration 1** and **Configuration 2**.

Note: If a customized default file was not saved, clicking **Custom Default** loads the factory default configuration on the Switch.

65.17 SSH Authorized Keys

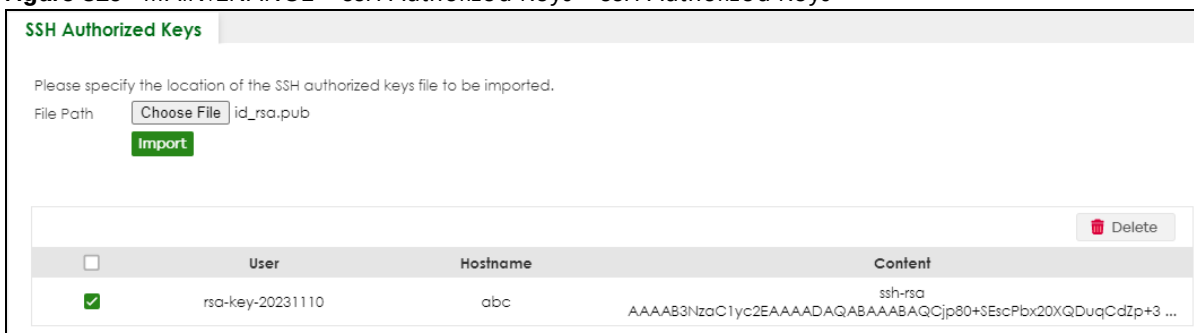
The Switch can use SSH-authorized keys to authenticate secure SSH connections between a client computer and the Switch (also called the server) without needing a password to connect to the Switch. You can use a third-party utility to generate a private and public key for SSH, for example:

- In Windows, use the PuTTY terminal emulator
- In Linux Ubuntu, use the "ssh-keygen" command.

The Switch and the client computer should have a unique set of private and public keys for encryption/decryption. See [Section 53.5.1 on page 356](#) for more information about SSH.

Click **MAINTENANCE > SSH Authorized Keys > SSH Authorized Keys** to open the following screen. Use this screen to import the client computer's public key into the Switch.

Figure 319 MAINTENANCE > SSH Authorized Keys > SSH Authorized Keys



The following table describes the labels in this screen.

Table 244 MAINTENANCE > SSH Authorized Keys > SSH Authorized Keys

LABEL	DESCRIPTION
File Path	Click Choose File or Browse to find the authorized key file you want to upload.
Import	Click this button to save the authorized key file you want to import from your computer to the Switch.
	Select an entry's checkbox to select a specific key.
User	This field displays the user name of the authorized key file (up to 32 characters).
Hostname	This field displays the hostname of the authorized key file (up to 32 characters only).
Content	This field displays the actual encryption key's text string (up to 64 characters).
Delete	After selecting an entry's checkbox, click this button to delete the authorized key file.

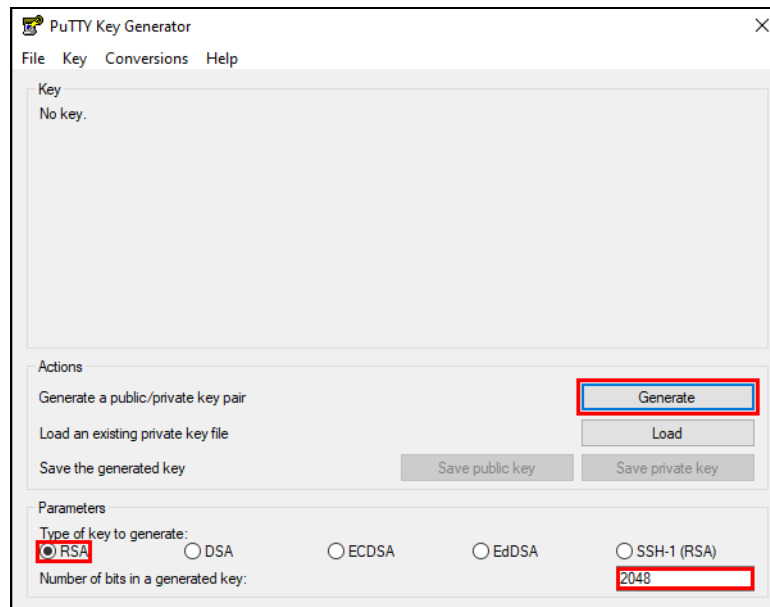
65.17.1 Generate the SSH Authorized Keys

You must install an SSH client program on a client computer (Windows or Linux operating system) to connect to the Switch over SSH.

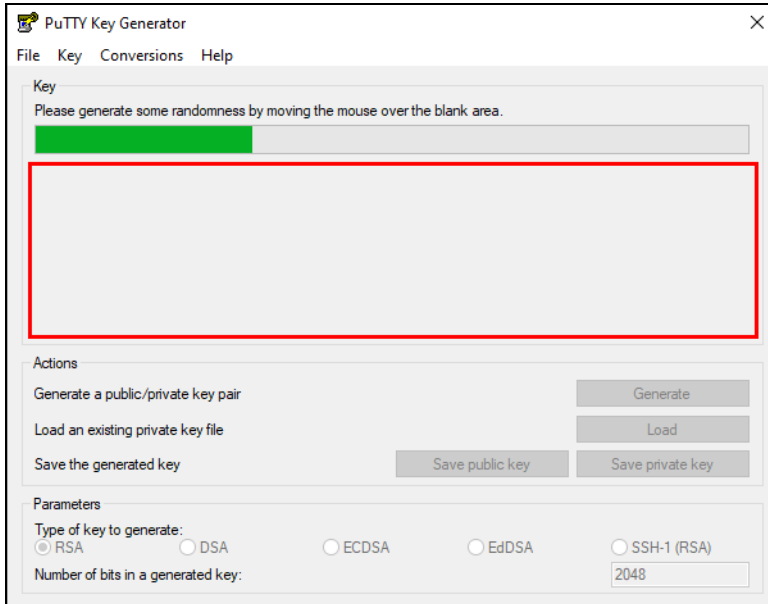
Example – Generate the SSH Authorized Keys on Windows

PuTTY is a free and open-source terminal emulator. It supports the SSH network protocol. To generate the SSH-authorized keys in PuTTY, the following are the steps at the time of writing:

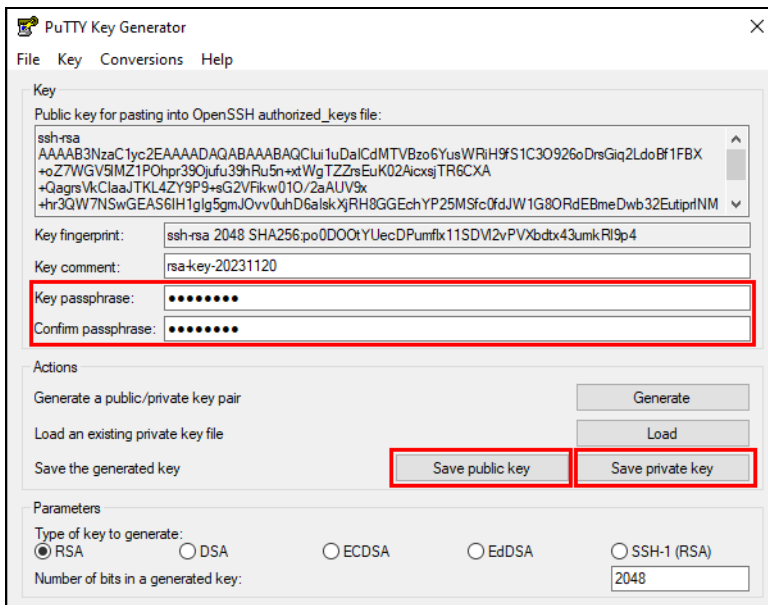
- 1 Run PuTTYgen.



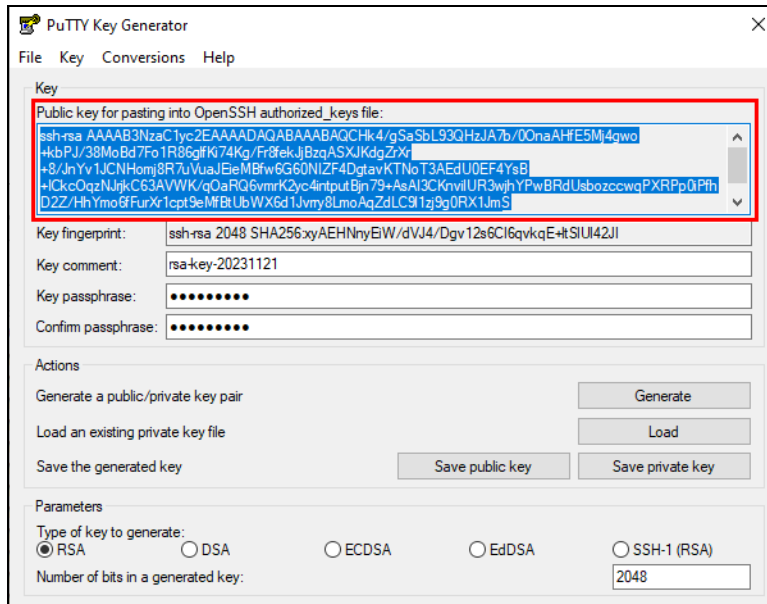
- 2 Select **RSA** in the **Type of key to generate**. RSA (Rivest-Shamir-Adleman) is an asymmetric encryption scheme that generates its keys by multiplying two pseudo-random prime numbers. Enter **2048** in the **Number of bits in a generated key**. SSH keys with encryption lower than 2048 are considered insecure. Then click **Generate**.
- 3 Move the mouse back and forth over the blank area to complete the key generation.



- 4 (Optional) The **Key passphrase** and **Confirm passphrase** fields allow you to set a passphrase for your key. Use the passphrase to encrypt the key on your computer. When set, you need to enter the passphrase to use the key. See step 5 on [Run PuTTY for SSH Connections on Windows](#) for more information.



- 5 Click **Save public key** and **Save private key** to save the generated keys in your computer.
- 6 Copy the text on the generated public key into a text editor app like Notepad.



- At the end of the text string, enter “@(Hostname)”. This will appear in the **Hostname** field in the **MAINTENANCE > SSH Authorized Keys > SSH Authorized Keys** screen. Press **Enter** to add a line break, then save the text file. Import the text file into the Switch using the **SSH Authorized Keys** screen.

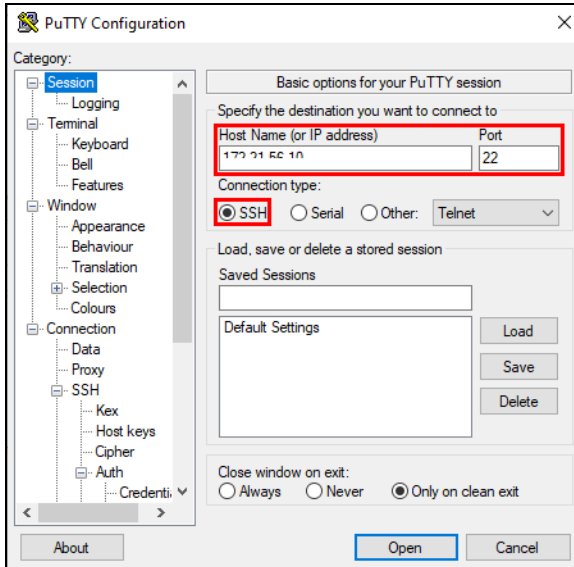


Note: The Switch only supports one SSH-authorized key at a time. Only one client computer can authenticate without entering a password using an SSH connection.

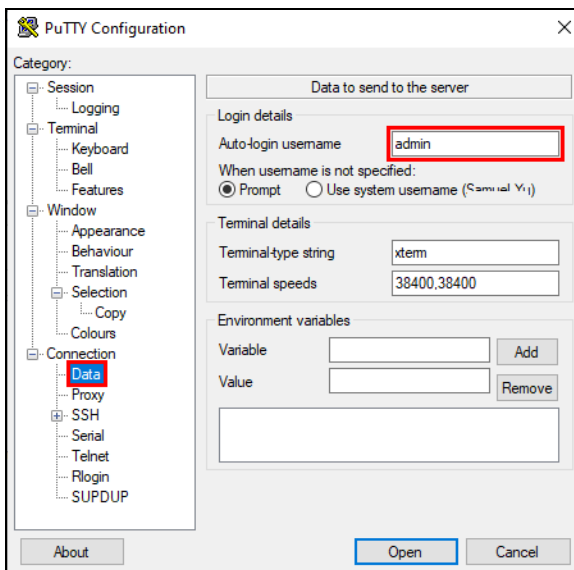
Run PuTTY for SSH Connections on Windows

To use PuTTY to connect to the Switch through SSH, the following are the steps at the time of writing:

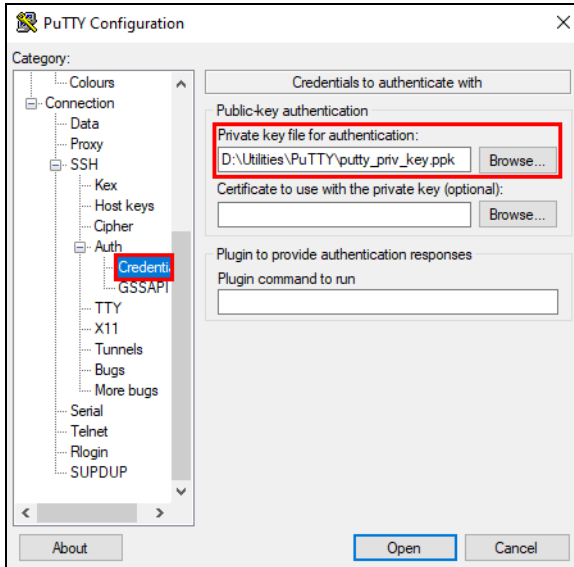
- Run PuTTY. In the **Session** screen, enter the IP address of the Switch and “22” for the **Port**. Select **SSH** for the **Connection type**.



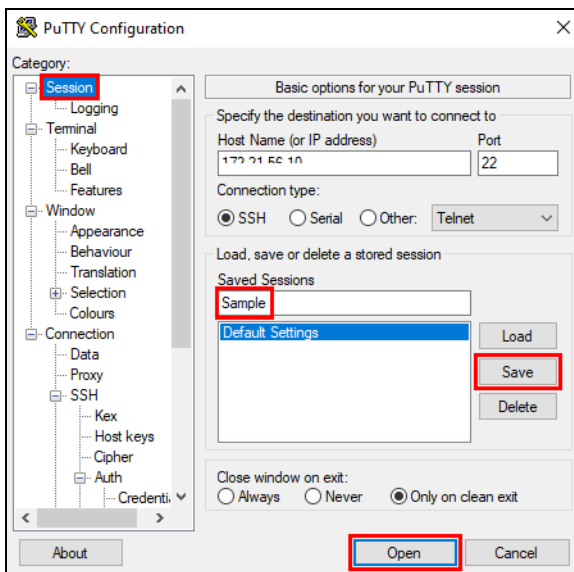
- 2 In the **Data** screen, enter **admin** for **Auto-login username**. The Switch only supports the **admin** login for the SSH-authorized key.



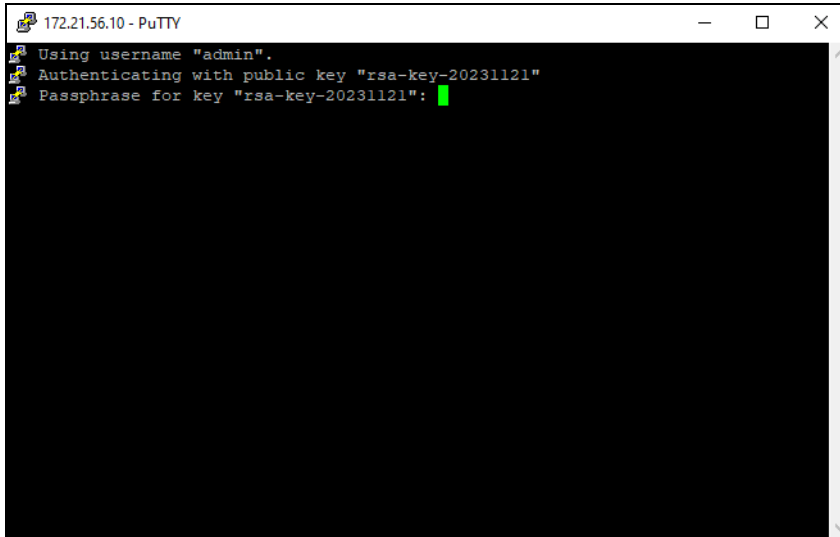
- 3 In the **Credentials** screen, click **Browse** to locate the generated private key.



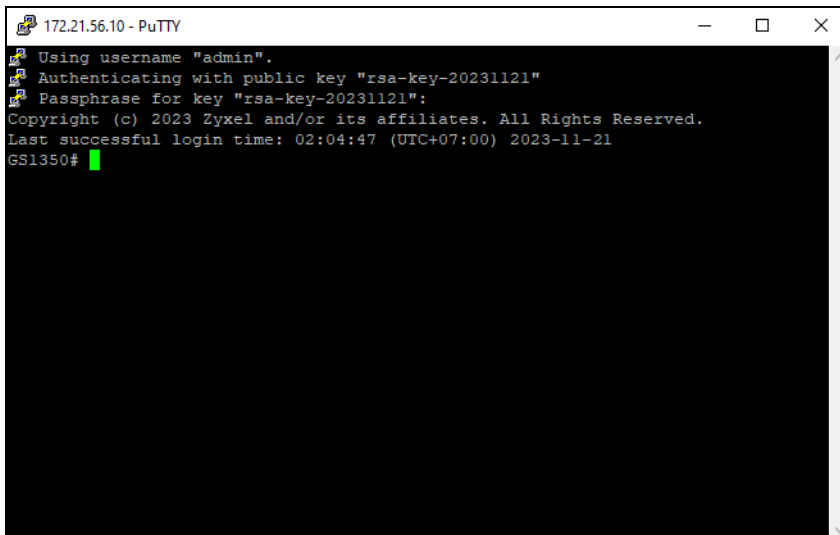
- 4 In the **Session** screen, you can save the PuTTY configuration by entering a name (for example, “Sample”) in the **Saved Sessions**, then click **Save**. Click **Open** to start the SSH connection.



- 5 Enter the **Passphrase for key** if you configured the **Key passphrase** in step 4 of using the PuTTY Key Generator.



You have now logged in to the Switch.



Example – Generate the SSH Authorized Keys on Linux

To generate the SSH-authorized keys in Ubuntu, enter the following commands at the time of writing:

```
UserA@UbuntuClient:~$ ssh-keygen -t rsa -b 2048
.....(enter..)
UserA@UbuntuClient:~$ ls -all .ssh/
.....
-rw-----  1 UserA UserA  1831 Mar 25  09:46 id_rsa
-rw-r--r--  1 UserA UserA   408 Mar 25  09:46 id_rsa.pub
.....
```

“id_rsa” is the private key and “id_rsa.pub” is the public key generated in Ubuntu.

65.18 SSH Host Keys

The Switch uses its SSH host public key (P) to authenticate secure SSH connections from an SSH client (C).

When the Switch receives a connection request from an SSH client, the Switch sends its public key to the SSH client. If it's the first time the SSH client accesses the Switch, the SSH client may receive a warning message prompting it to accept or reject the public key.

After the SSH client accepts the Switch's public key, the SSH client encrypts the SSH client's username and password with the Switch's public key and sends the encrypted credentials to the Switch.

When the Switch gets the encrypted credentials from the SSH client, the Switch uses its private key to decrypt the encrypted credentials from the SSH client. If the credentials are correct, the Switch authenticates the SSH client and the SSH client can log into the Switch using SSH.

Figure 320 SSH Host Keys



Click **MAINTENANCE > SSH Host Keys > SSH Host Keys** to open the following screen. Use this screen to regenerate the Switch's SSH host key. You may want to do this to change the factory default SSH host key.

Figure 321 MAINTENANCE > SSH Host Keys > SSH Host Keys



The following table describes the labels in this screen.

Table 245 MAINTENANCE > SSH Host Keys > SSH Host Keys

LABEL	DESCRIPTION
RSA	At the time of writing, the Switch supports RSA encryption for the SSH host key. See Section 65.17.1 on page 457 for information about the RSA.
Regenerate Key	Click this button to regenerate the Switch's default host key. Note: After the Switch regenerates the host key, the previous authenticated SSH clients may receive a message to replace the old host key with the new one the next time they connect to the Switch.

65.19 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 entering the "Show tech-support" command.

Click **MAINTENANCE > Tech-Support > Tech-Support** to see the following screen.

Figure 322 MAINTENANCE > Tech-Support > Tech-Support

Tech-Support

CPU Threshold % Keep Seconds

Mbuf Threshold %

Apply **Cancel**

All **Download**

Crash **Download**

CPU **Download**

Memory **Download**

Mbuf **Download**

ROM **Download**

L3 **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 246 MAINTENANCE > Tech-Support > Tech-Support

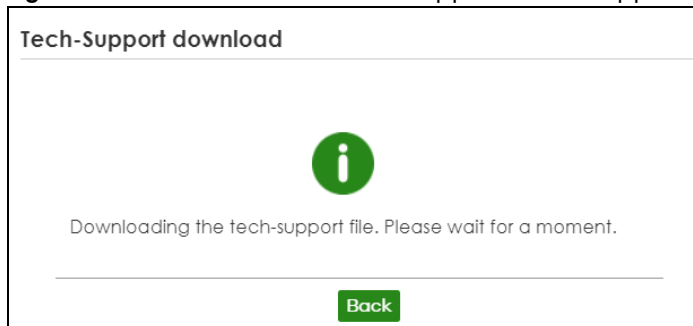
LABEL	DESCRIPTION
CPU	Type a number ranging from 50 to 100 in the CPU threshold box, and type another number ranging from 5 to 60 in the seconds box then click Apply. For example, 80 for CPU threshold and 5 for seconds means a log will be created when CPU utilization reaches over 80% and lasts for 5 seconds. The log report holds 7 days of CPU log data and is stored in volatile memory (RAM). The data is lost if the Switch is turned off or in event of power outage. After 7 days, the logs wrap around and new ones and replace the earliest ones. The higher the CPU threshold number, the fewer logs will be created, and the less data technical support will have to analyze and vice versa.
Mbuf	Type a number ranging from 50 to 100 in the Mbuf (Memory Buffer) threshold box. The Mbuf log report is stored in flash (permanent) memory. For example, Mbuf 50 means a log will be created when the Mbuf utilization is over 50%. The higher the Mbuf threshold number, the fewer logs will be created, and the less data technical support will have to analyze and vice versa.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
All	Click Download to see all the log report and system status. This log report is stored in flash memory. If the All log report is too large, you can download the log reports separately below.
Crash	Click Download to see the crash log report. The log will include information of the last crash and is stored in flash memory.
CPU	Click Download to see the CPU history log report. The 7-days log is stored in RAM and you will need to save it, otherwise it will be lost when the Switch is shutdown or during power outage.

Table 246 MAINTENANCE > Tech-Support > Tech-Support (continued)

LABEL	DESCRIPTION
Memory	Click Download to see the memory section log report. This log report is stored in flash memory.
Mbuf	Click Download to see the Mbuf (Memory Buffer) log report. 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.
L3	Click Download to see the layer-3 Switch log report. The log only applies to the layer-3 Switch models. This report is stored in flash memory.

65.19.1 Tech-Support Download

When you click **Download** to save your current Switch configuration to a computer, the following screen appears. When the log report has downloaded successfully, click **Back** to return to the previous screen.

Figure 323 MAINTENANCE > Tech-Support > Tech-Support: Download

CHAPTER 66

Networked AV Mode

66.1 Overview

Aside from the Web Configurator in Standard mode that has a complete set of configuration for network installation, you can switch to Networked AV mode. Networked AV mode contains just the necessary configurations for setting up and managing audio-video traffic on your network.

AV over IP is the transmission of audio-video data over an IP network.

Use a browser that supports HTML5, such as Microsoft Edge, Mozilla Firefox, or Google Chrome. The recommended minimum screen resolution is 1024 by 768 pixels.

The following sections introduce the configuration and functions of the Web Configurator in Networked AV mode.

Click **Networked AV** at the top left of the Web Configurator to switch between the Web Configurator's **Standard** or **Networked AV** mode.

Figure 324 Web Configurator – Networked AV Mode Switch

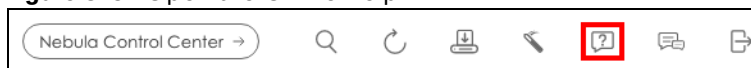


66.2 Help

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

Click the **Help** link from a Web Configurator screen to scan the QR code or click the web link to display the online help.

Figure 325 Open the Online Help



66.3 Summary

Use the **SUMMARY** screen to see the Switch's front panel port status, connected ports information, networked AV information, Nebula Cloud Control status, and a link to go to the **IP Setup** screen ([Section 66.11 on page 476](#)).

The **SUMMARY** screen displays when you log into the Switch in Networked AV mode.

Figure 326 Summary



The following table describes the labels in this screen.

Table 247 SUMMARY

LABEL	DESCRIPTION
Auto Refresh	Click the Pause Auto Refresh or Resume Auto Refresh icon to stop or resume the screen update.
Port Status	This chart displays the status of the Switch's front panel ports with connection (Fiber).
Networked AV Information	
IP Setup	This link takes you to a screen where you can configure the IP address and subnet mask (necessary for Switch management) and set up to 128 IP routing domains.
IGMP-Snooping VLAN	This displays the ID number of the VLAN group upon which the Switch is to perform IGMP snooping.
IGMP-Snooping	This displays Active when IGMP snooping is enabled to forward group multicast traffic only to ports that are members of that group. Otherwise, it is Inactive .
IGMP-Querier	This displays Active when the Switch is allowed to send IGMP General Query messages to the VLANs with the multicast hosts attached. Otherwise, it is Inactive .
IP Interface	This displays the IP address of the Switch for it to be managed over the network.
Unknown Multicast	This displays the action to perform when the Switch receives an unknown multicast frame. It displays Drop when the frames are discarded. It displays Flooding when the frames are sent to all ports. It displays Drop on VLAN when the frames are discarded on the specified VLANs.
Cloud Control Status	This displays the registration and connection status between the Switch and the NCC (Nebula Control Center). Click NCC Discovery or the switch button to go to SYSTEM > Cloud Management > Cloud Management screen.
Port	This displays the port of this Switch.
Port Name	This displays the port description of this Switch.
Link Speed	This displays the speed (either 1G for 1 Gbps, 10G for 10 Gbps, 25G for 25 Gbps, or 100G for 100 Gbps) and the duplex (F for full duplex or H for half). This field displays – (dash) if the port is not connected to any device.
Bandwidth Usage (Tx) Bandwidth Usage (Rx)	These display the percentage of bandwidth usage on this port as a percentage of the Link Speed .
IGMP Leave Mode	This displays Immediate when the Switch receives IGMP leave packets, the Switch will close the multicast stream immediately without any further action. This displays Fast when the Switch will further generate a group specific query packet to all the receivers. This could prevent the traffic being cut if some receivers still want to receive the multicast stream. This displays Normal when the Switch receives an IGMP leave message from a host on a port, it forwards the message to the multicast router. The multicast router then sends out an IGMP Group-Specific Query (GSQ) message to determine whether other hosts connected to the port should remain in the specific multicast group. The Switch forwards the query message to all hosts connected to the port and waits for IGMP reports from hosts to update the forwarding table for this port.

66.4 MONITOR

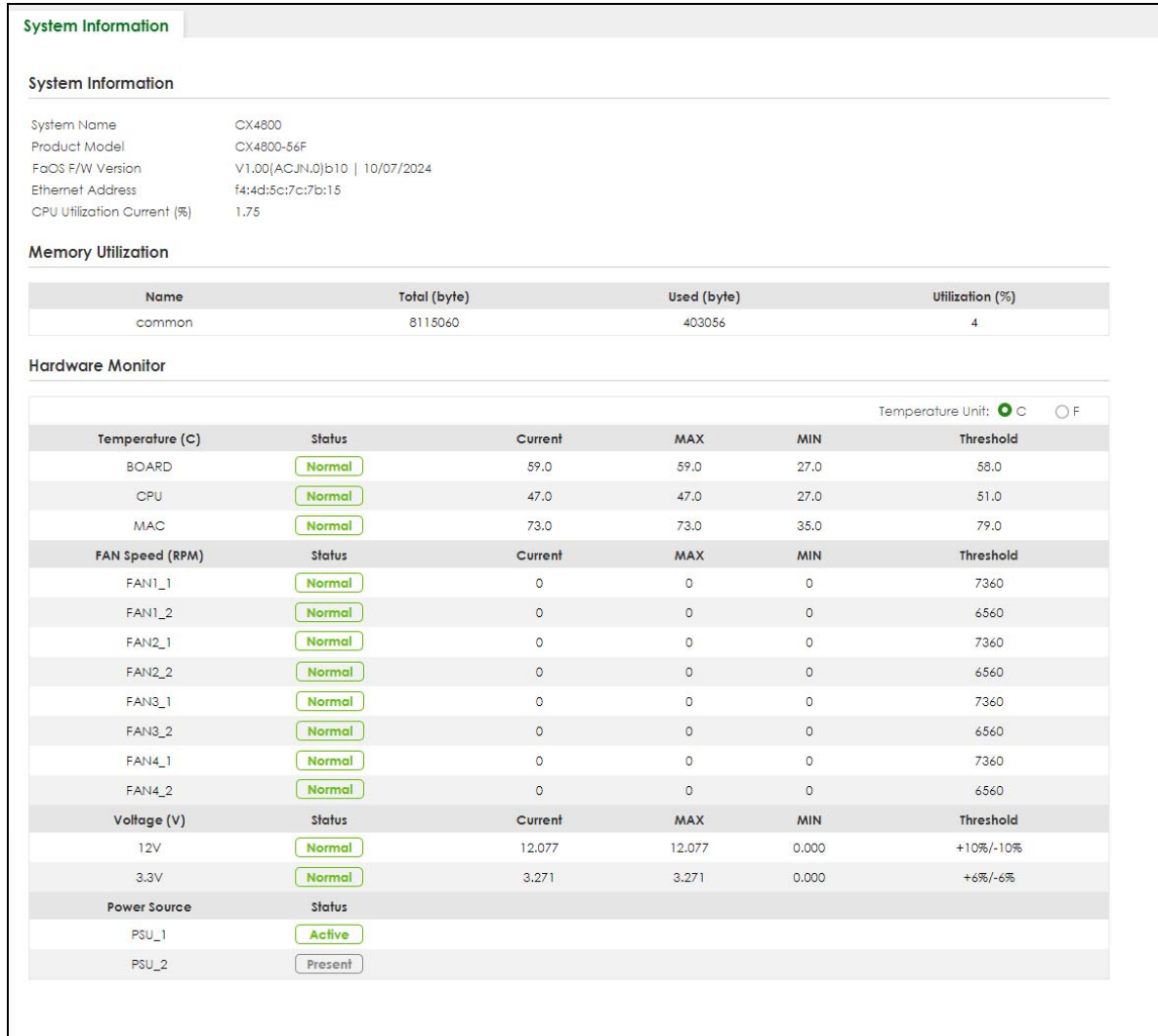
The following sections introduce the **MONITOR** screens.

66.5 What You Can Do

Use the **System Information** screen ([Section 66.6 on page 469](#)) to check the firmware version number and monitor the Switch temperature.

66.6 System Information

In the navigation panel, click **MONITOR > System Information > System Information** to display the screen as shown. Use this screen to view general system information. You can check the firmware version number and monitor the Switch temperature.

Figure 327 MONITOR > System Information > System Information

The following table describes the labels in this screen.

Table 248 MONITOR > System Information > System Information

LABEL	DESCRIPTION
System Information	
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.
FaOS F/W Version	This field displays the version number of the Switch 's current firmware including the creation date.
Ethernet Address	This field refers to the Ethernet MAC (Media Access Control) address of the Switch.
CPU Utilization Current (%)	CPU utilization quantifies how busy the system is. Current (%) displays the current percentage of CPU utilization.
Memory Utilization	
Memory utilization shows how much DRAM memory is available and in use. It also displays the current percentage of memory utilization.	

Table 248 MONITOR > System Information > System Information (continued)

LABEL	DESCRIPTION
Name	This field displays the name of memory pool.
Total (byte)	This field displays the total number of bytes in this memory pool.
Used (byte)	This field displays the number of bytes being used in this memory pool.
Utilization (%)	This field displays the percentage (%) of memory being used in this memory pool.
Hardware Monitor	
Temperature (C/F)	BOARD, CPU/MAC refers to the location of the temperature sensor on the Switch printed circuit board.
Status	This field displays Normal for temperatures below the threshold and Error for those above.
Current	This shows the current temperature at this sensor.
MAX	This field displays the maximum temperature measured at this sensor.
MIN	This field displays the minimum temperature measured at this sensor.
Threshold	This field displays the upper temperature limit at this sensor.
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.
Status	Normal indicates that this fan is functioning above the minimum speed. Error indicates that this fan is functioning below the minimum speed.
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.
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.
Status	Normal indicates that the voltage is within an acceptable operating range at this point; otherwise Error is displayed.
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.
Power Source	This field lists the power supply modules installed in the Switch. PSU_1 is PWR1 , and PSU_2 is PWR2 .
Status	Active indicates the Switch is currently operating from the power source to which the power module is connected. Present is displayed when the power module is connected to the Switch, but is not connected to a power source and there is no available power. Absent is displayed when there is no power module connected to the Switch. Error indicates that this power module is functioning below the power requirement. Or, the fan in this power module is not working.

66.7 SYSTEM

The following sections introduces the **SYSTEM** screens.

66.8 What You Can Do

- Use the **Cloud Management** screen ([Section 66.9 on page 472](#)) to view NCC Connection status and enable/disable NCC Discovery.
- Use the **General Setup** screen ([Section 66.10 on page 474](#)) to configure general settings such as the system name and time.
- Use the **IP Setup** screen ([Section 66.11 on page 476](#)) to configure the default gateway device, the default domain name server and add IP domains.
- Use the **Logins** screen ([Section 66.12 on page 478](#)) to change the system password, configure passwords for up to four users and set their privilege level.
- Use the **SNMP** screen ([Section 66.13 on page 480](#)) to configure your SNMP (Simple Network Management Protocol) settings.
- Use the **SNMP User** screen ([Section 66.14 on page 482](#)) to create SNMP users for authentication with managers using SNMP v3 and associate them to SNMP groups.
- Use the **SNMP Trap Group** screen ([Section 66.15 on page 484](#)) to specify the types of SNMP traps that should be sent to each SNMP manager.
- Use the **SNMP Trap Port** screen ([Section 66.16 on page 485](#)) to set whether a trap received on the ports would be sent to the SNMP manager.

66.9 Cloud Management

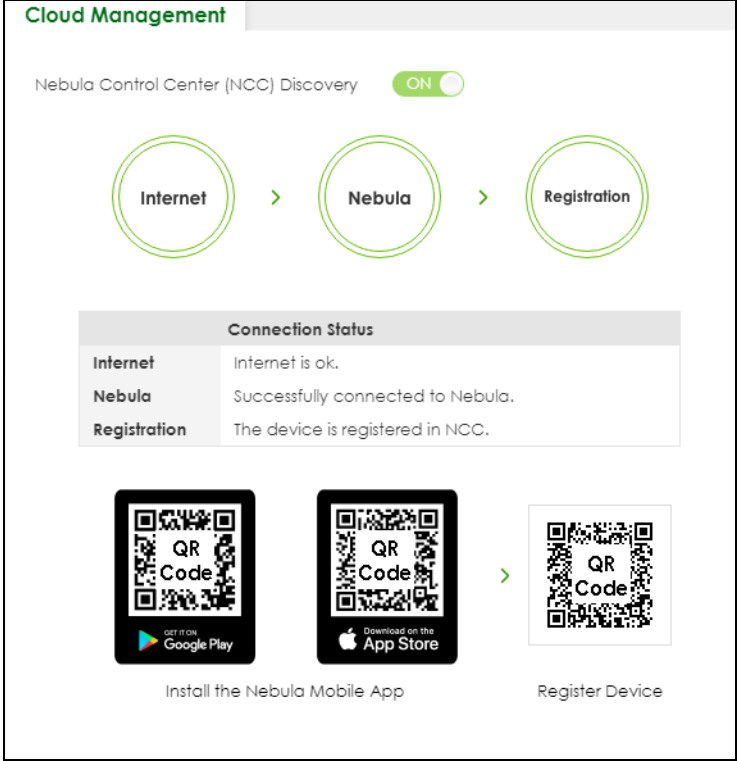
The Zyxel Nebula Control Center (NCC) is a cloud-based network management system that allows you to remotely manage and monitor Zyxel Nebula APs, Ethernet switches, security gateways, security routers, mobile routers, and accessories.

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

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

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

Figure 328 SYSTEM > Cloud Management > Cloud Management



The following table describes the labels in this screen.

Table 249 SYSTEM > Cloud Management > Cloud Management

LABEL	DESCRIPTION
Nebula Control Center (NCC) Discovery	Enable the switch button to turn on Nebula Control Center (NCC) discovery on the Switch. This field displays: • The Switch Internet connection status. • The connection status between the Switch and NCC. • The Switch registration status on NCC. Mouse over the circles to display detailed information. To pass your Switch management to NCC, first make sure your Switch is connected to the Internet. Then go to NCC and register your Switch. 1. Internet Green – The Switch is connected to the Internet. Orange – The Switch is not connected to the Internet. 2. Nebula Green – The Switch is connected to NCC. Orange – The Switch is not connected to NCC. 3. Registration Green – The Switch is registered on NCC. Gray – The Switch is not registered on NCC. Note: All circles will gray out if you disable Nebula Discovery.
Connection Status	This table displays the NCC connection status information. Use the status logs in the Internet, Nebula, and Registration fields for connection troubleshooting.

Enable **Nebula Control Center (NCC) Discovery** to turn on NCC discovery on the Switch. If the Switch has Internet access and has been registered in the NCC, it will go into cloud management mode.

Disable **Nebula Control Center (NCC) Discovery** to turn off NCC discovery on the Switch. The Switch will NOT discover the NCC and remain in standalone mode.

This screen has a QR code containing the Switch's serial number and Registration MAC address for handy NCC registration of the Switch using the Nebula Mobile app. First, download the app from the Google Play store for Android devices or the App Store for iOS devices and create an organization and site. Open the Nebula Mobile app and follow the wizard to scan the **Register Device** QR code to register the Switch on NCC.

66.10 General Setup

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

Figure 329 SYSTEM > General Setup > General Setup

General Setup

System Name: CX4800

Location:

Contact Person's Name:

Use Time Server when Bootup: NTP(RFC-1305) ▼

Time Server 1: pool.ntp.org

Time Server 2: time.google.com

Time Server 3: time.google.com

Time Server Sync Interval: 1440 minutes

Current Time: 11 : 16 : 01 UTC+00:00

New Time (hh:mm:ss): 11 : 16 : 01

Current Date: 2024 - 09 - 26

New Date (yyyy-mm-dd): 2024 - 09 - 26

Time Zone: UTC ▼

Daylight Saving Time: ☐ OFF

Start Date: First ▼ Sunday ▼ of January ▼ at 0:00 ▼

End Date: First ▼ Sunday ▼ of January ▼ at 0:00 ▼

Apply Cancel

Note: The input string of any field in this screen should not contain [?], [|], ['], ["], or [,].

The following table describes the labels in this screen.

Table 250 SYSTEM > General Setup > General Setup

LABEL	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. This name consists of up to 64 printable ASCII characters; spaces are allowed.
Location	Enter the geographic location of your Switch. You can use up to 128 printable ASCII characters; spaces are allowed.
Contact Person's Name	Enter the name of the person in charge of this Switch. You can use up to 32 printable ASCII characters; spaces are allowed.
Use Time Server when Bootup	Enter the time service protocol that your time server uses. Not all time servers support all protocols, so you may have to use trial and error to find a protocol that works. The main differences between them are the time format. When you select the Daytime (RFC-867) format, the Switch displays the day, month, year and time with no time zone adjustment. When you use this format it is recommended that you use a Daytime timeserver within your geographical time zone. Time (RFC-868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 00:00:00. 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 2022-01-01 00:00:00.
Time Server 1 / 2 / 3	Enter the IPv4 address or domain name of your time server. The Switch searches for the first, then the second, then the third time server for around 60 seconds.
Time Server Sync Interval	Enter the period in minutes between each time server synchronization. The Switch checks the time server after every synchronization interval.

Table 250 SYSTEM > General Setup > General Setup (continued)

LABEL	DESCRIPTION
Current Time	This field displays the time you open this menu (or refresh the menu).
New Time (hh:mm:ss)	Enter the new time in hour, minute and second format. The new time then appears in the 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. Enable the switch button if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected Daylight Saving Time . The time is displayed in the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select Second, Sunday, March and 2:00 . Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, March and the last field depends on your time zone. In Germany for instance, you would select 2:00 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected Daylight Saving Time . The time field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select First, Sunday, November and 2:00 . Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, October and the last field depends on your time zone. In Germany for instance, you would select 2:00 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

66.11 IP Setup

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

Note: The Switch allows you to set a static IP interface in the same subnet that already has a DHCP-assigned IP interface on the Switch. The Switch will use the static IP you set and the DHCP-assigned IP will be set to 0.0.0.0.

Figure 330 SYSTEM > IP Setup > IP Setup

IP Setup

Default Gateway

Domain Name Server 1

Domain Name Server 2

Apply **Cancel**

IP Interface

+ Add/Edit **Delete**

☐	Index	IP Address	IP Subnet Mask	VID	Type
☐	1	10.214.35.43	255.255.255.0	1	DHCP

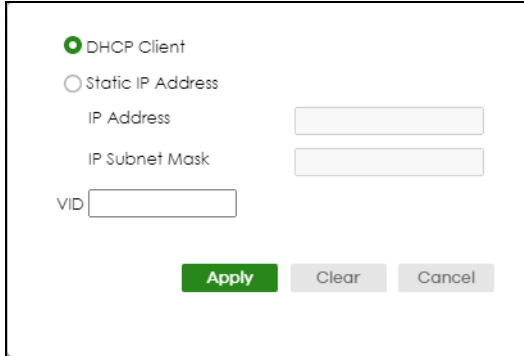
The following table describes the labels in this screen.

Table 251 SYSTEM > IP Setup > IP Setup

LABEL	DESCRIPTION
Default Gateway	Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
Domain Name Server 1/2	Enter a domain name server IPv4 address in order to be able to use a domain name instead of an IP address.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save 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.	
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Index	This is the IP routing domain entry number.
IP Address	This is the IP address of the Switch in an IP routing domain.
IP Subnet Mask	This is the IP subnet mask of an IP routing domain in dotted decimal notation, for example, 255.255.252.0.
VID	Enter the VLAN identification number to which an IP routing domain belongs.
Add/Edit	Click Add/Edit to add a new management port setting or edit a selected one.
Delete	Click Delete to remove the selected entry from the summary table.
	Note: Deleting all IP subnets locks you out of the Switch.

66.11.1 Add/Edit IP Interfaces

Use this screen to add or edit IP interfaces. Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SYSTEM > IP Setup > IP Setup** screen to display this screen.

Figure 331 SYSTEM > IP Setup > IP Setup > Add/Edit


The following table describes the labels in this screen.

Table 252 SYSTEM > IP Setup > IP Setup > Add/Edit

LABEL	DESCRIPTION
DHCP Client	Select this option if you have a DHCP server that can assign the Switch an IP address, subnet mask, a default gateway IP address and a domain name server IP address automatically.
Static IP Address	Select this option if you do not have a DHCP server or if you wish to assign static IP address information to the Switch. You need to fill in the following fields when you select this option.
IP Address	Enter the IP address of your Switch in dotted decimal notation, for example, 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.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

66.12 Logins

Up to five people (one administrator and four non-administrators) may access the Switch through Web Configurator at any one time.

- An administrator is someone who can both view and configure Switch changes. The default user name for the Administrator is **admin**. See the default administrator password on the back label of the Switch.
- A non-administrator (user name is something other than **admin**) is someone who can view and/or configure Switch settings. The configuration right varies depending on the user's privilege level.

Click **SYSTEM > Logins** to view the screen as shown.

Figure 332 SYSTEM > Logins > Logins

Logins

Administrator

User Name:

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				

Apply **Cancel**

The following table describes the labels in this screen.

Table 253 SYSTEM > Logins > Logins

LABEL	DESCRIPTION
Administrator	
This is the default administrator account with the “admin” user name. You cannot change the default administrator user name.	
User Name	Change the default “admin” system user name (up to 32 printable ASCII characters except [?], [], ['], ["], [space], [,], or [:]).
Old Password	Enter the existing system password (see the back label on the Switch for the default password).
Old Password	Enter the existing system password (the default password is found on the label on bottom of the Switch).
New Password	Enter your new system password. The password rules are: • 4 to 32 characters in length • [?], [], ['], ["], [,], [[], []] and space are not allowed
Retype to confirm	Re-enter your new system password for confirmation.
Edit Logins	
You may configure passwords for up to four users. These users can have read-only or read/write access. You can give users higher privileges through the Web Configurator or the CLI. For more information on assigning privileges through the CLI see the Ethernet Switch CLI Reference Guide.	
Login	This is the index of an user account.
User Name	Set a user name (up to 32 printable ASCII characters except [?], [], ['], ["], or [,]).
Password	Enter your new system password. The password rules are: • 4 to 32 characters in length • [?], [], ['], ["], [,], [[], []] and space are not allowed
Retype to confirm	Retype your new system password for confirmation.

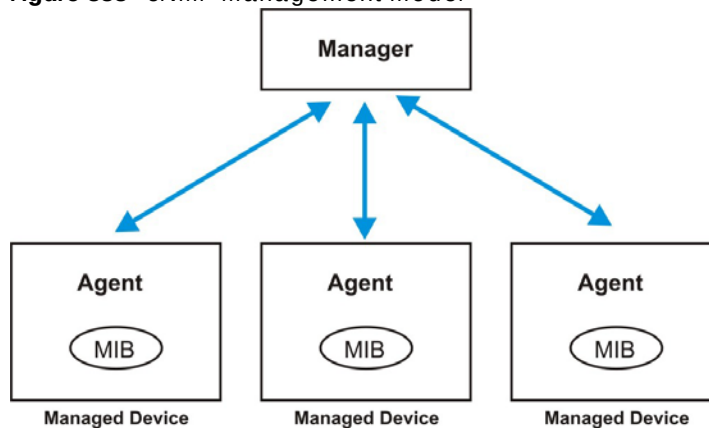
Table 253 SYSTEM > Logins > Logins (continued)

LABEL	DESCRIPTION
Privilege	Enter the privilege level for this user. At the time of writing, users may have a privilege level of 0, 3, 13, or 14 representing different configuration rights as shown below. 0 – Display basic system information. 3 – Display configuration or status. 13 – Configure features except for login accounts, SNMP user accounts, the authentication method sequence and authorization settings, multiple logins, administrator and enable passwords, and configuration information display. 14 – Configure login accounts, SNMP user accounts, the authentication method sequence and authorization settings, multiple logins, and administrator and enable passwords, and display configuration information. Users can run command lines if the session's privilege level is greater than or equal to the command's privilege level. The session privilege initially comes from the privilege of the login account. For example, if the user has a privilege of 5, he or she can run commands that requires privilege level of 5 or less but not more.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

66.13 Configure SNMP

Use this screen to configure your SNMP settings. Simple Network Management Protocol (SNMP) is an application layer protocol used to manage and monitor TCP/IP-based devices. SNMP is used to exchange management information between the network management system (NMS) and a network element (NE). A manager station can manage and monitor the Switch through the network through 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 333 SNMP Management Model



An SNMP managed network consists of two main components: agents and a manager.

An agent is a management software module that resides in a managed Switch (the Switch). An agent translates the local management information from the managed Switch into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

The managed devices contain object variables or managed objects that define each piece of information to be collected about a Switch. Examples of variables include number of packets received, node port status and so on. A Management Information Base (MIB) is a collection of managed objects. SNMP allows a manager and agents to communicate for the purpose of accessing these objects.

SNMP itself is a simple request or response protocol based on the manager or agent model. The manager issues a request and the agent returns responses using the following protocol operations:

Table 254 SNMP Commands

LABEL	DESCRIPTION
Get	Allows the manager to retrieve an object variable from the agent.
GetNext	Allows the manager to retrieve the next object variable from a table or list within an agent. In SNMPv1, when a manager wants to retrieve all elements of a table from an agent, it initiates a Get operation, followed by a series of GetNext operations.
Set	Allows the manager to set values for object variables within an agent.
Trap	Used by the agent to inform the manager of some events.

SNMP v3 and Security

SNMP v3 enhances security for SNMP management. SNMP managers can be required to authenticate with agents before conducting SNMP management sessions.

Security can be further enhanced by encrypting the SNMP messages sent from the managers. Encryption protects the contents of the SNMP messages. When the contents of the SNMP messages are encrypted, only the intended recipients can read them.

Click **SYSTEM > SNMP > SNMP** to view the screen as shown.

Figure 334 SYSTEM > SNMP > SNMP

SNMP SNMP User SNMP Trap Group SNMP Trap Port

General Setting

Version:

Get Community:

Set Community:

Trap Community:

Trap Destination

Index	Version	IP	Port	Username
1	v2c	0.0.0.0	162	
2	v2c	0.0.0.0	162	
3	v2c	0.0.0.0	162	
4	v2c	0.0.0.0	162	

Note: The string of any field in this screen should not contain [?], [|], ['], ["], or [,].

The following table describes the labels in this screen.

Table 255 SYSTEM > SNMP > SNMP

LABEL	DESCRIPTION
General Setting	
Use this section to specify the SNMP version and community (password) values.	
Version	Select the SNMP version for the Switch. The SNMP version on the Switch must match the version on the SNMP manager. Choose SNMP version 2c (v2c), SNMP version 3 (v3) or both (v3v2c). SNMP version 2c is backwards compatible with SNMP version 1.
Get Community	Enter the Get Community string, which is the password for the incoming Get- and GetNext-requests from the management station. The Get Community string is only used by SNMP managers using SNMP version 2c or lower.
Set Community	Enter the Set Community string, which is the password for incoming Set- requests from the management station. The Set Community string is only used by SNMP managers using SNMP version 2c or lower.
Trap Community	Enter the Trap Community string, which is the password sent with each trap to the SNMP manager. The Trap Community string is only used by SNMP managers using SNMP version 2c or lower.
Trap Destination	
Use this section to configure where to send SNMP traps from the Switch.	
Index	This is the index of a trap destination.
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 user name to be sent to the SNMP manager along with the SNMP v3 trap. This user name must match an existing account on the Switch (configured in the SYSTEM > SNMP > SNMP User screen).
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

66.14 Configure SNMP User

Use this 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. Click **SYSTEM > SNMP > SNMP User** to view the screen as shown.

Figure 335 SYSTEM > SNMP > SNMP User

The screenshot shows the 'SNMP User' configuration page. At the top, there are four tabs: 'SNMP', 'SNMP User' (selected), 'SNMP Trap Group', and 'SNMP Trap Port'. Below the tabs is a search bar and two buttons: '+ Add/Edit' and '- Delete'. Below these is a table with the following columns: a checkbox, 'Index', 'Username', 'Security Level', 'Authentication', 'Privacy', and 'Group'.

The following table describes the labels in this screen.

Table 256 SYSTEM > SNMP > SNMP User

LABEL	DESCRIPTION
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Index	This is a read-only number identifying a login account on the Switch.
Username	This field displays the user name of a login account on the Switch.
Security Level	This field displays whether you want to implement authentication and/or encryption for SNMP communication with this user.
Authentication	This field displays the authentication algorithm used for SNMP communication with this user.
Privacy	This field displays the encryption method used for SNMP communication with this user.
Group	This field displays the SNMP group to which this user belongs.
Add/Edit	Click Add/Edit to add a new entry or edit a selected one.
Delete	Click Delete to remove the selected entries.

66.14.1 Add/Edit SNMP User

Use this 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. Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SYSTEM > SNMP > SNMP User** screen to view this screen.

Note: Use the user name and password of the login accounts you specify in this screen to create accounts on the SNMP v3 manager.

Figure 336 SYSTEM > SNMP > SNMP User > Add/Edit

The screenshot shows the 'Add/Edit' form for an SNMP user. It contains the following fields: 'Username' (text input), 'Security Level' (dropdown menu showing 'no auth'), 'Authentication' (dropdown menu showing 'MD5'), 'Privacy' (dropdown menu showing 'DES'), and 'Group' (dropdown menu showing 'admin'). To the right of the 'Authentication' and 'Privacy' dropdowns are 'Password' text input fields. At the bottom right are three buttons: 'Apply' (green), 'Clear' (grey), and 'Cancel' (grey).

The following table describes the labels in this screen.

Table 257 SYSTEM > SNMP > SNMP User > Add/Edit

LABEL	DESCRIPTION
Username	Specify the user name (up to 32 printable ASCII characters) of a login account on the Switch. The string should not contain [?], [], ['], ["], [,], [:], or space.
Security Level	Select whether you want to implement authentication and/or encryption for SNMP communication from this user. Choose: no auth – to use the user name 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 printable ASCII characters (except [?], [], ['], ["], [space], [,], [[], or []]) 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 printable ASCII characters (except [?], [], ['], ["], [space], [,], [[], or []]) 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. read-write – 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. read-only – Members of this group have read rights only, meaning the user can collect information from 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.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

66.15 Configure SNMP Trap Group

Use this screen to specify the types of SNMP traps that should be sent to each SNMP manager. Click **SYSTEM > SNMP > SNMP Trap Group** to view the screen as shown.

Figure 337 SYSTEM > SNMP > SNMP Trap Group

The following table describes the labels in this screen.

Table 258 SYSTEM > SNMP > 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 SYSTEM > SNMP > SNMP screen. Use the rest of the screen to select which traps the Switch sends to that SNMP manager.
	Select the individual SNMP traps that the Switch is to send to the SNMP station. The traps are grouped by category. Selecting a category in the heading row automatically selects all of the SNMP traps under that category. Clear the checkboxes for individual traps that you do not want the Switch to send to the SNMP station. Clearing a category's checkbox automatically clears all of the category's trap checkboxes (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.

66.16 Enable or Disable Sending of SNMP Traps on a Port

Click **SYSTEM > SNMP > SNMP Trap Port** to view the screen as shown. Use this screen to set whether a trap received on the ports would be sent to the SNMP manager.

Figure 338 SYSTEM > SNMP > SNMP Trap Port

SNMP

SNMP User

SNMP Trap Group

SNMP Trap Port

Options

loopguard

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

Apply

Cancel

The following table describes the labels in this screen.

Table 259 SYSTEM > SNMP > SNMP Trap Port

LABEL	DESCRIPTION
Options	Select the trap type you want to configure here.
Port	This field displays a port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some of the settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox to enable the trap type of SNMP traps on this port. The Switch sends the related traps received on this port to the SNMP manager. Clear this checkbox 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.

66.17 PORT

The following sections introduce the **PORT** screens.

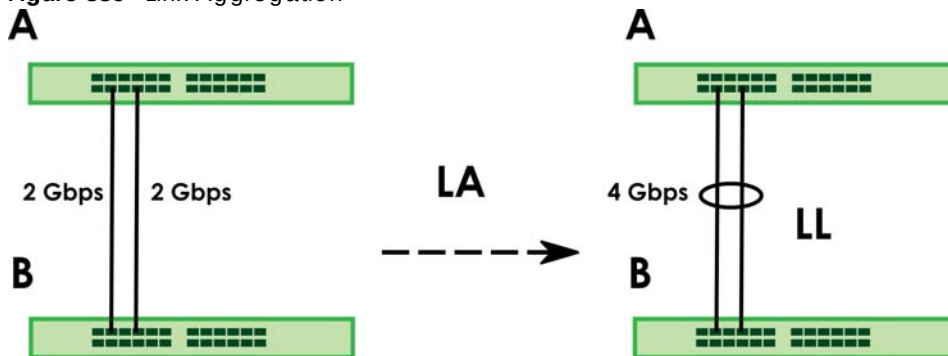
66.18 Link Aggregation

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

Link aggregation (**LA**) (trunking) is the grouping of physical ports into one logical higher-capacity link (**LL**). 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.

Figure 339 Link Aggregation



66.18.1 What You Can Do

- Use the **Link Aggregation Status** screen ([Section 66.19 on page 487](#)) to view ports you have configured to be in the trunk group, ports that are currently transmitting data as one logical link in the trunk group and so on.
- Use the **Link Aggregation Setting** screen ([Section 66.20 on page 489](#)) to configure to enable static link aggregation.
- Use the **Link Aggregation Control Protocol** screen ([Section 66.21 on page 490](#)) to enable Link Aggregation Control Protocol (LACP).

66.19 Link Aggregation Status

Use the **Link Aggregation Status** screen to view ports you have configured to be in the trunk group, ports that are currently transmitting data as one logical link in the trunk group and so on.

Click **PORT > Link Aggregation > Link Aggregation Status** in the navigation panel to display the screen as shown.

Figure 340 PORT > Link Aggregation > Link Aggregation Status

Link Aggregation Status					
Link Aggregation Setting			Link Aggregation Control Protocol		
Group ID	Enabled Ports	Synchronized Ports	Aggregator ID	Criteria	Status
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	-

The following table describes the labels in this screen.

Table 260 PORT > Link Aggregation > Link Aggregation Status

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

66.20 Link Aggregation Setting

Use the **Link Aggregation Setting** screen to enable static link. Link aggregation (trunking) is the grouping of physical ports into one logical higher-capacity link. You may want to trunk ports if for example, it is cheaper to use multiple lower-speed links than to under-utilize a high-speed, but more costly, single-port link. However, the more ports you aggregate then the fewer available ports you have. A trunk group is one logical link containing multiple ports.

Click **PORT > Link Aggregation > Link Aggregation Setting** to display the screen shown next.

Figure 341 PORT > Link Aggregation > Link Aggregation Setting

Group ID	Active	Criteria
T1	☒	src-dst-mac ▼
T2	☐	src-dst-mac ▼
T3	☐	src-dst-mac ▼
T4	☐	src-dst-mac ▼
T5	☐	src-dst-mac ▼
T6	☐	src-dst-mac ▼
T7	☐	src-dst-mac ▼

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

The following table describes the labels in this screen.

Table 261 PORT> Link Aggregation > Link Aggregation Setting

LABEL	DESCRIPTION
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 to activate a trunk group.

Table 261 PORT > Link Aggregation > Link Aggregation Setting (continued)

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

66.21 Link Aggregation Control Protocol

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

Click **PORT > Link Aggregation > Link Aggregation Control Protocol** to display the screen shown next.

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

Figure 342 PORT > Link Aggregation > Link Aggregation Control Protocol

Active ☒ ON

System Priority

Group ID	LACP Active
T1	☐
T2	☐
T3	☐
T4	☐
T5	☐
T6	☐
T7	☐

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

The following table describes the labels in this screen.

Table 262 PORT > Link Aggregation > Link Aggregation Control Protocol

LABEL	DESCRIPTION
Active	Enable the switch button to enable Link Aggregation Control Protocol (LACP).
System Priority	LACP system priority is a number between 1 and 65535. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP “server”. The LACP “server” controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregation Control Protocol (LACP). The smaller the number, the higher the priority level.
Use this section to enable LACP on trunks.	
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.
Use this section to configure LACP timeout on ports.	
Port	This field displays the port number.

Table 262 PORT > Link Aggregation > Link Aggregation Control Protocol (continued)

LABEL	DESCRIPTION
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
LACP Timeout	Timeout is the time interval between the individual port exchanges of LACP packets in order to check that the peer port in the trunk group is still up. If a port does not respond after three tries, then it is deemed to be “down” and is removed from the trunk. Set a short timeout (1 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.

66.22 Port Setup

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

Figure 343 PORT > Port Setup > Port Setup

Port	Active	Name	Speed / Duplex	FEC	802.1p Priority	BPDU Ctrl
*	☐		Auto	Auto	0	Peer
1	☒		Auto	Auto	0	Peer
2	☒		Auto	Auto	0	Peer
3	☒		Auto	Auto	0	Peer
4	☒		Auto	Auto	0	Peer
5	☒		Auto	Auto	0	Peer
6	☒		Auto	Auto	0	Peer
7	☒		Auto	Auto	0	Peer
8	☒		Auto	Auto	0	Peer
9	☒		Auto	Auto	0	Peer

The following table describes the labels in this screen.

Table 263 PORT > Port Setup > Port Setup

LABEL	DESCRIPTION
Port	This is the port index number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this checkbox 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 128 printable ASCII characters except [?], [], ['], or ["]. Note: Due to space limitations, the port name may be truncated in some Web Configurator screens.
Speed/Duplex	Select the speed and the duplex mode of the connection on this port. For an SFP28 fiber port, the choices are Auto, 1G / Full Duplex, 10G / Full Duplex, 25G-an (25G/ auto-negotiation), and 25G / Full Duplex. For a QSFP28 fiber port, the choices are 100G-an (100G/auto-negotiation), and 100G / Full Duplex. 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.
FEC	To minimize signal degradation of data at high transmission speeds (for example, 25 Gbps or 100 Gbps), set the same FEC (Forward Error Correction) type between the Switch and the connected device. Select Auto to allow both connected ports to automatically set the FEC type according to the following rules: - For 10G transceivers, the FEC type on the port will automatically be None. - For 25G transceivers, the FEC type on the port will automatically be CL108. - For 100G transceivers, the FEC type on the port will automatically be None if the transceiver type is 100G LR4/ER4; all other types of transceiver will automatically be CL91. Select CL74 when both connected ports support 25 Gbps speed and require low latency in data transmission. Select CL91 when both connected ports support 25 Gbps and 100 Gbps speeds. Select CL108 when both connected ports support 25 Gbps speed but low latency in data transmission is not required. Alternatively, select None when you do not need to set the FEC type. Make sure to set the correct Speed/Duplex on this screen.
802.1p Priority	This priority value is added to incoming frames without a (802.1p) tag.

Table 263 PORT > Port Setup > Port Setup (continued)

LABEL	DESCRIPTION
BPDU Ctrl	Configure the way to treat BPDUs received on this port. You must activate Bridging Control Protocol Transparency in the SYSTEM > 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.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

66.23 SWITCHING

The following sections introduce the **SWITCHING** screens.

66.24 Differentiated Services

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.

Activate DiffServ to apply marking rules or IEEE 802.1p priority mapping on the selected ports.

Click **SWITCHING > Diffserv > Diffserv** to display the screen as shown.

Figure 344 SWITCHING > Diffserv > Diffserv

Diffserv DSCP Setting

Active ☐ OFF

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

Apply Cancel

The following table describes the labels in this screen.

Table 264 SWITCHING > Diffserv > Diffserv

LABEL	DESCRIPTION
Active	Enable the switch button to enable Diffserv on the Switch.
Port	This field displays the index number of a port on the Switch.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Active	Select Active to enable Diffserv on the port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

66.25 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 265 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

To change the DSCP-IEEE 802.1p mapping click **SWITCHING > Diffserv > DSCP Setting** to display the screen as shown next.

Figure 345 SWITCHING > Diffserv > DSCP Setting

The following table describes the labels in this screen.

Table 266 SWITCHING > 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.

66.26 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.

Click **SWITCHING > Mirroring > 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 346 SWITCHING > Mirroring > Mirroring

Mirroring

Active ☐ OFF

Monitor Port

Port	Mirrored	Direction
*	☐	ingress ▼
1	☐	ingress ▼
2	☐	ingress ▼
3	☐	ingress ▼
4	☐	ingress ▼
5	☐	ingress ▼
6	☐	ingress ▼
7	☐	ingress ▼

Apply Cancel

The following table describes the labels in this screen.

Table 267 SWITCHING > Mirroring > Mirroring

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

66.27 Multicast

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

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

This section shows you how to configure various multicast features.

66.27.1 What You Can Do

- Use the **IPv4 Multicast Status** screen ([Section 66.28 on page 498](#)) to view multicast group information.
- Use the **IGMP Snooping** screen ([Section 66.29 on page 499](#)) to enable IGMP snooping to forward group multicast traffic only to ports that are members of that group.
- Use the **IGMP Snooping VLAN** screen ([Section 66.30 on page 502](#)) to perform IGMP snooping on up to 16 VLANs.
- Use the **IGMP Filtering Profile** screen ([Section 66.31 on page 504](#)) to specify a range of multicast groups that clients connected to the Switch are able to join.

66.28 IPv4 Multicast Status

Click **SWITCHING > Multicast > IPv4 Multicast > IPv4 Multicast Status** to display the screen as shown. This screen shows the IPv4 multicast group information.

Figure 347 SWITCHING > Multicast > IPv4 Multicast > IPv4 Multicast Status

IPv4 Multicast Status			
IGMP Snooping		IGMP Snooping VLAN	
Index	VID	Port	Multicast Group
1	1	18	224.0.0.251
2	1	18	224.0.0.252
3	1	18	239.255.255.250

The following table describes the labels in this screen.

Table 268 SWITCHING > Multicast > IPv4 Multicast > IPv4 Multicast Status

LABEL	DESCRIPTION
Index	This is the index number of the entry.
VID	This field displays the multicast VLAN ID.
Port	This field displays the port number that belongs to the multicast group.
Multicast Group	This field displays IP multicast group addresses.

66.29 IGMP Snooping

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

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

Click **SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping** to display the screen as shown.

Figure 348 SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping

Port	Immediate Leave	Normal Leave	Fast Leave	Group Limited	Max Group Number	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

The following table describes the labels in this screen.

Table 269 SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping

LABEL	DESCRIPTION
Active	Enable the switch button to enable IGMP Snooping to forward group multicast traffic only to ports that are members of that group.
Querier	Select this to allow the Switch to send IGMP General Query messages to the VLANs with the multicast hosts attached.

Table 269 SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping (continued)

LABEL	DESCRIPTION
Querier Version	IGMP snooping query works only when both host and Switch support the same IGMP version. Select v2 to allow the Switch to send IGMPv2 queries only. Select v3 to allow the Switch to send IGMPv3 queries only.
Querier Query Interval	Enter the period in seconds (1 to 65535) between each IGMP snooping query. The Switch sends IGMP General Query messages after every query interval.
Report Proxy	Select this to allow the Switch to act as the IGMP report proxy and leave proxy. It will report group changes to a connected multicast router. The Switch not only checks IGMP packets between multicast routers or switches and multicast hosts to learn the multicast group membership, but also replaces the source MAC address in an IGMP v1/v2 report with its own MAC address before forwarding to the multicast router or switch. When the Switch receives more than one IGMP v1/v2 join report that requests to join the same multicast group, it only sends a new join report with its MAC address. This helps reduce the number of multicast join reports passed to the multicast router or switch. The Switch sends a leave message with its MAC address to the multicast router or switch only when it receives the leave message from the last host in a multicast group.
Host Timeout	Specify the time (from 1 to 16711450) in seconds that elapses before the Switch removes an IGMP group membership entry if it does not receive report messages from the port.
802.1p Priority	Select a priority level (0 – 7) to which the Switch changes the priority in outgoing IGMP control packets. Otherwise, select No-Change to not replace the priority.
IGMP Filtering Active	Enable the switch button to enable IGMP filtering to control which IGMP groups a subscriber on a port can join. If you enable IGMP filtering, you must create and assign IGMP filtering profiles for the ports that you want to allow to join multicast groups.
IGMP Snooping Smart Forward Active	Enable the switch button to enable sending of multicast frame to querier port and IGMP subscriber groups. Otherwise, the querier port forwards the frames only when it receives a join report and it belongs to the IGMP group.
Unknown Multicast Frame	Specify the action to perform when the Switch receives an unknown multicast frame. - Select Flooding to send the frames to all ports. - Select Drop to discard the frames. - Select Drop on VLAN and enter the VLAN ID numbers to discard the frames on the specified VLANs. Use a dash to specify consecutive VLANs and a comma (no spaces) to specify non-consecutive VLANs. For example, 51–53 includes 51, 52 and 53, but 51,53 does not include 52.
Unknown Multicast Frame to Querier Port	Specify the action to perform when Unknown Multicast Frame is set to Drop. - Select Drop to discard the frames. - Select Forwarding to send the frames to all querier ports. - Select Forwarding on VLAN and enter the VLAN ID numbers to send the frames to the ports which are used as an IGMP query port on the specified VLANs. Use a dash to specify consecutive VLANs and a comma (no spaces) to specify non-consecutive VLANs. For example, 51–53 includes 51, 52 and 53, but 51,53 does not include 52.

Table 269 SWITCHING > 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 Flooding to send the frames to all ports. • Select Drop to discard the frames.
Use this section to configure IGMP Snooping on each port.	
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Immediate Leave	Select this option to set the Switch to remove this port from the multicast tree when an IGMP version 2 leave message is received on this port. Select this option if there is only one host connected to this port.
Normal Leave	Enter an IGMP normal leave timeout value (from 200 to 6348800) in 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 6348800) 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 Number	Enter the number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new IGMP join report frames is dropped on this port.

Table 269 SWITCHING > 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 reports received on this port.
IGMP Filtering Profile	Select the name of the IGMP filtering profile to use for this port. Otherwise, select Default to prohibit the port from joining any multicast group. You can create IGMP filtering profiles in the SWITCHING > Multicast > IPv4 Multicast > IGMP Filtering Profile screen.
IGMP Querier Mode	The Switch treats an IGMP query port as being connected to an IGMP multicast router (or server). The Switch forwards IGMP join or leave packets to an IGMP query port. Select Auto to have the Switch use the port as an IGMP query port if the port receives IGMP query packets. Select Fixed to have the Switch always use the port as an IGMP query port. Select this when you connect an IGMP multicast server to the port. Select Edge to stop the Switch from using the port as an IGMP query port. The Switch will not keep any record of an IGMP router being connected to this port. The Switch does not forward IGMP join or leave packets to this port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

66.30 IGMP Snooping VLAN

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

Click **SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping VLAN** to display the screen as shown.

Note: You can perform IGMP snooping on up to 16 VLANs.

Figure 349 SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping VLAN

IGMP Snooping VLAN

Mode ☒ auto ☐ fixed

Apply **Cancel**

VLAN

+ Add/Edit **- Delete**

☐	Index	Name	VID
☐	1	VLAN66	66

The following table describes the labels in this screen.

Table 270 SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping VLAN

LABEL	DESCRIPTION
IGMP Snooping VLAN	
Mode	Select auto to have the Switch learn multicast group membership information of any VLANs automatically. Select fixed to have the Switch only learn multicast group membership information of the VLANs that you specify below. In either auto or fixed mode, the Switch can learn up to 16 VLANs. The Switch drops any IGMP control messages which do not belong to these 16 VLANs. You must also enable IGMP snooping in the SWITCHING > Multicast > IGMP Snooping screen first.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
VLAN	
Use this section of the screen to add VLANs on which the Switch is to perform IGMP snooping.	
Index	This is the index number of the IGMP snooping VLAN entry in the table.
Name	This field displays the descriptive name for this VLAN group.
VID	This field displays the ID number of the VLAN group.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to create a new entry or edit a selected one.
Delete	Click Delete to remove the selected entries.

66.30.1 Add/Edit IGMP Snooping VLANs

This screen allows you to add an IGMP snooping VLAN or edit an existing one.

To access this screen, click the **Add/Edit** button or select an entry from the list and click the **Add/Edit** button.

Figure 350 SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping VLAN > Add/Edit

The following table describes the labels in this screen.

Table 271 SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping VLAN > Add/Edit

LABEL	DESCRIPTION
Name	Enter the descriptive name (up to 32 printable ASCII characters except [?], [], ['], ["], or [,]) of the VLAN for identification purposes.
VID	Enter the ID of a static VLAN; the valid range is between 1 and 4094.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

66.31 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 **SWITCHING > Multicast > IPv4 Multicast > IGMP Snooping** screen). Clients connected to those ports are then able to join the multicast groups specified in the profile. Each port can be assigned a single profile. A profile can be assigned to multiple ports.

Click **SWITCHING > Multicast > IPv4 Multicast > IGMP Filtering Profile** link to display the screen as shown.

Figure 351 SWITCHING > Multicast > IPv4 Multicast > IGMP Filtering Profile

The following table describes the labels in this screen.

Table 272 SWITCHING > Multicast > IPv4 Multicast > IGMP Filtering Profile

LABEL	DESCRIPTION
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.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add Profile	Click this to add a new IGMP filtering profile.
Add Rule	Click Add Rule to add a new rule and specify the profile it belongs to in the Add Rule screen. You can also select a profile entry and click Add Rule to add an additional rule for the selected profile.
Delete	Select a profile and click Delete to remove the selected profile and the accompanying rules. Select a rule from a profile and click Delete to remove the selected rule.

66.31.1 Add IGMP Filtering Profile

To access this screen, click the **Add Profile** button in the **SWITCHING > Multicast > IPv4 Multicast > IGMP Filtering Profile** screen.

Figure 352 SWITCHING > Multicast > IPv4 Multicast > IGMP Filtering Profile > Add Profile

The following table describes the labels in this screen.

Table 273 SWITCHING > Multicast > IPv4 Multicast > IGMP Filtering Profile > Add Profile

LABEL	DESCRIPTION
Profile Name	Enter a descriptive name for the profile for identification purposes. You can enter up to 32 printable ASCII characters except [?], [], ['], ["], or [,].
Start Address	Enter the starting multicast IP address for a range of multicast IP addresses that you want to belong to the IGMP filter profile.
End Address	Enter 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.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

66.31.2 Add IGMP Filtering Rule

Click **Add Rule** in the **SWITCHING > Multicast > IPv4 Multicast > IGMP Filtering Profile** screen to access this screen.

Figure 353 SWITCHING > Multicast > IPv4 Multicast > IGMP Filtering Profile > Add Rule

The following table describes the labels in this screen.

Table 274 SWITCHING > Multicast > IPv4 Multicast > IGMP Filtering Profile > Add Rule

LABEL	DESCRIPTION
Profile Name	Select a profile from the drop-down list to add a additional rule for the existing profile.
Start Address	Enter the starting multicast IP address for a range of multicast IP addresses that you want to belong to the IGMP filter profile.
End Address	Enter 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.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

66.32 Static Multicast Forwarding By MAC

Use this screen to view and configure static multicast MAC addresses for ports to receive the multicast stream. Click **SWITCHING > Multicast > Static Multicast Forwarding By MAC > Static Multicast Forwarding By MAC** to display the screen as shown next.

Figure 354 SWITCHING > Multicast > Static Multicast Forwarding By MAC > Static Multicast Forwarding By MAC

The following table describes the labels in this screen.

Table 275 SWITCHING > Multicast > Static Multicast Forwarding By MAC > Static Multicast Forwarding By MAC

LABEL	DESCRIPTION
Index	This is the index number of the static multicast MAC address rule.
Active	This field displays whether a static multicast MAC address forwarding rule is active or not. You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for a static multicast MAC address-forwarding rule.
MAC Address	This field displays the multicast MAC address that identifies a multicast group.
VID	This field displays the ID number of a VLAN group to which frames containing the specified multicast MAC address will be forwarded.
Port	This field displays the ports within an identified VLAN group to which frames containing the specified multicast MAC address will be forwarded.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new rule or edit a selected one.
Delete	Click Delete to remove the selected rules.

66.33 VLAN

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

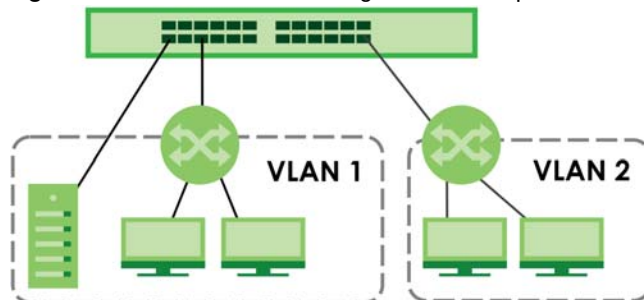
66.33.1 What You Can Do

- Use the **VLAN Status** screen ([Section 66.34 on page 510](#)) to view and search all static VLAN groups.
- Use the **VLAN Detail** screen ([Section 66.34.1 on page 511](#)) to view detailed port settings and status of the static VLAN group.
- Use the **Static VLAN** screen ([Section 66.35 on page 511](#)) to configure a static VLAN for the Switch.
- Use the **VLAN Port Setup** screen ([Section 66.36 on page 514](#)) to configure the static VLAN (IEEE 802.1Q) settings on a port.

66.33.2 What You Need to Know

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

Figure 355 Shared Server Using VLAN Example



IEEE 802.1Q Tagged VLANs

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges – they are not confined to the switch on which they were created. The VLANs can be created statically by hand dynamically through GVRP. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is 4 bytes longer than an untagged frame and contains 2 bytes of TPID (Tag Protocol Identifier, residing within the type or length field of the Ethernet frame) and 2 bytes of TCI (Tag Control Information, starts after the source address field of the Ethernet frame).

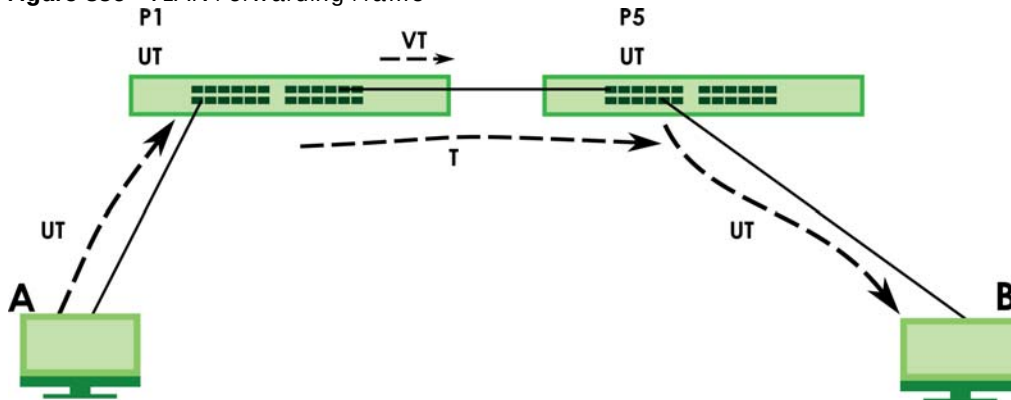
The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum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

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

Forwarding Tagged and Untagged Frames

Each port on the Switch is capable of passing tagged (T) or untagged (UT) 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 (VT). 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 (VT) reflecting the ingress port's default VID. The default PVID is VLAN 1 for all ports, but this can be changed.

Figure 356 VLAN Forwarding Frame



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.

66.33.2.1 Automatic VLAN Registration

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

GARP

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

GARP Timers

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

GVRP

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

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

Table 276 IEEE 802.1Q VLAN Terminology

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

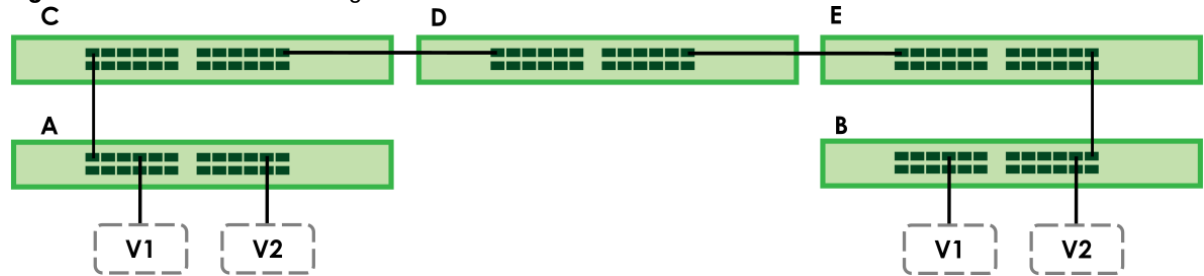
66.33.2.2 Port VLAN Trunking

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

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

unknown to those switches) to pass through their VLAN trunking ports.

Figure 357 Port VLAN Trunking



66.34 VLAN Status

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

Figure 358 SWITCHING > VLAN > VLAN Status

VLAN Status Static VLAN VLAN Port Setup

VLAN Search by VID

The Number of VLAN: 4

Index	VID	Name	Tagged Port	Untagged Port	Elapsed Time	Status
1	1	1		1-54	9:54:59	Static
2	2	2	2		0:51:05	Static
3	3	3			0:50:37	Static
4	100	VLAN100	5		0:50:13	Static

Page 1 of 1

The following table describes the labels in this screen.

Table 277 SWITCHING > VLAN > VLAN Status

LABEL	DESCRIPTION
VLAN Search by VID	Enter (an) existing VLAN ID numbers (use a comma (,) to separate individual VLANs or a hyphen (-) to indicate a range of VLANs. For example, "3,4" or "3-9") and click Search to display only the specified VLANs in the list below. Leave this field blank and click Search to display all VLANs configured on the Switch.
The Number of VLAN	This is the number of VLANs configured on the Switch.
The Number of Search Results	This is the number of VLANs that match the searching criteria and display in the list below. This field displays only when you use the Search button to look for certain VLANs.
Index	This is the VLAN index number. Click an index number to view more VLAN details.
VID	This is the VLAN identification number that was configured in the corresponding VLAN configuration screen.
Name	This fields shows the descriptive name of the VLAN.
Tagged Port	This field shows the tagged ports that are participating in the VLAN.
Untagged Port	This field shows the untagged ports that are participating in the VLAN.

Table 277 SWITCHING > VLAN > VLAN Status (continued)

LABEL	DESCRIPTION
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the Switch. Static: added as a permanent entry.

66.34.1 VLAN Details

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

Figure 359 SWITCHING > VLAN > VLAN Status > VLAN Status Details

VLAN Status Static VLAN VLAN Port Setup

[VLAN Status](#) > VLAN Status Details

VID: 1
Elapsed Time: 6:48:56
Status: Static

Port Number

U:Untagged T:Tagged

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49	51	53	55
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52	54	56
U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	
U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	U	

The following table describes the labels in this screen.

Table 278 SWITCHING > VLAN > VLAN Status > VLAN Status Details

LABEL	DESCRIPTION
VID	This is the VLAN identification number that was configured in the corresponding VLAN configuration screen.
Elapsed Time	This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up.
Status	This field shows how this VLAN was added to the Switch. Static: added as a permanent entry.
Port Number	This section displays the ports that are participating in a VLAN. A tagged port is marked as T , an untagged port is marked as U and ports not participating in a VLAN are marked as — .

66.35 Configure a Static VLAN

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

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

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

Use this screen to view and configure a static VLAN for the Switch. Click **SWITCHING > VLAN > Static VLAN** to display the screen as shown next.

Figure 360 SWITCHING > VLAN > Static VLAN

VLAN Status

Static VLAN

VLAN Port Setup

+ Add/Edit

🗑 Delete

☐	VID	Active	Name
☐	1	ON	1
☐	2	ON	2
☒	3	ON	3
☐	100	ON	VLAN100

The following table describes the related labels in this screen.

Table 279 SWITCHING > VLAN > Static VLAN

LABEL	DESCRIPTION
VID	This field displays the ID number of the VLAN group.
Active	This field indicates whether the VLAN settings are enabled or disabled.
Name	This field displays the descriptive name for this VLAN group.
	Select an entry's checkbox to select a specific entry. Otherwise, select the checkbox in the table heading row to select all entries.
Add/Edit	Click Add/Edit to add a new static VLAN or edit a selected one.
Delete	Click Delete to remove the selected static VLAN.

66.35.1 Add/Edit a Static VLAN

Use this screen to configure a static VLAN for the Switch. Click **Add/Edit**, or select an entry and click **Add/Edit** in the **SWITCHING > VLAN > Static VLAN** screen to display this screen.

Figure 361 SWITCHING > VLAN > Static VLAN > Add/Edit

Active ☐ OFF

Name

VLAN Group ID

VLAN Type ☒ Normal ☐ Private

Association VLAN List

Port	Control	Tagging
*	☐ Normal ☐ Fixed ☐ Forbidden	☒ 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

Apply Clear Cancel

The following table describes the related labels in this screen.

Table 280 SWITCHING > VLAN > Static VLAN > Add/Edit

LABEL	DESCRIPTION
Active	Enable the switch button 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 ASCII characters. The string should not contain [?], [], ['], ["], or [,].
VLAN Group ID	Enter the VLAN ID for this static entry; the valid range is between 1 and 4094.
VLAN Type	Select Normal (static) or Private . For Private VLANs, select Primary , Isolated or Community .
Association VLAN List	Primary private VLANs can associate with several (secondary) Community private VLANs and up to one (secondary) Isolated private VLAN. You only configure VLAN Association List for Primary private VLANs. Use a dash to associate consecutive VLANs and a comma (no spaces) to associate non-consecutive VLANs. For example, 51–53 includes 51, 52 and 53, but 51,53 does not include 52. Secondary private VLANs can only be associated with one primary private VLAN.
Port	The port number identifies the port you are configuring.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.

Table 280 SWITCHING > VLAN > Static VLAN > Add/Edit (continued)

LABEL	DESCRIPTION
Control	Select Normal for the port to dynamically join this VLAN group using GVRP. This is the default selection. Select Fixed for the port to be a permanent member of this VLAN group. Select Forbidden if you want to prohibit the port from joining this VLAN group.
Tagging	Select Tx Tagging if you want the port to tag all outgoing frames transmitted with this VLAN Group ID.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Clear	Click Clear to clear the fields to the factory defaults.
Cancel	Click Cancel to not save the configuration you make and return to the last screen.

66.36 VLAN Port Setup

Use this screen to configure the static VLAN (IEEE 802.1Q) settings on a port. Click **SWITCHING > VLAN > VLAN Port Setup** to display the screen as shown.

Figure 362 SWITCHING > VLAN > VLAN Port Setup

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

The following table describes the labels in this screen.

Table 281 SWITCHING > VLAN > VLAN Port Setup

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

Table 281 SWITCHING > VLAN > VLAN Port Setup (continued)

LABEL	DESCRIPTION
Ingress Check	If this checkbox is selected, the Switch discards incoming frames on a port for VLANs that do not include this port in its member set. Clear this checkbox 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.
Acceptable Frame Type	Specify the type of frames allowed on a port. Choices are All , Tag Only and Untag Only . Select All from the drop-down list box to accept all untagged or tagged frames on this port. This is the default setting. Select Tag Only to accept only tagged frames on this port. All untagged frames will be dropped. Select Untag Only to accept only untagged frames on this port. All tagged frames will be dropped.
VLAN Trunking	Enable VLAN Trunking on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the Switch.
Isolation	Select this to allow this port to communicate only with the CPU management port and the ports on which the isolation feature is NOT enabled.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

66.37 SECURITY

The following sections introduce the **SECURITY** screens.

66.38 Access Control

A console port and FTP are allowed one session each, Telnet and SSH share nine sessions, up to five Web sessions (five different user names and passwords) and/or limitless SNMP access control sessions are allowed.

Table 282 Access Control Overview

Console Port	SSH	Telnet	FTP	Web	SNMP
One session	Share up to 9 sessions		One session	Up to 5 accounts	No limit

A console port access control session and Telnet access control session cannot coexist when multi-login is disabled. See the CLI Reference Guide for more information on disabling multi-login.

This section describes how to control access to the Switch.

66.38.1 What You Can Do

- Use the **Service Access Control** screen (Section 66.39 on page 516) to decide what services you may use to access the Switch.
- Use the **Remote Management** screen (Section 66.40 on page 517) to specify a group of one or more “trusted computers” from which an administrator may use a service to manage the Switch.

66.39 Service Access Control

Service Access Control allows you to decide what services you may use to access the Switch. You may also change the default service port and configure “trusted computers” for each service in the **Remote Management** screen (discussed earlier). Click **SECURITY > Access Control > Service Access Control > Service Access Control** to view the screen as shown.

Figure 363 SECURITY > Access Control > Service Access Control > Service Access Control

Services	Active	Service Port	Timeout	Login Timeout
Console			5 Minutes	
Telnet	OFF	23	5 Minutes	150 Seconds
SSH	ON	22		
FTP	ON	21	5 Minutes	
HTTP	ON	80	55 Minutes	☒ Redirect to HTTPS
HTTPS	ON	443		
ICMP	ON			
SNMP	OFF			

The following table describes the fields in this screen.

Table 283 SECURITY > Access Control > Service Access Control > Service Access Control

LABEL	DESCRIPTION
Services	Services you may use to access the Switch are listed here.
Active	Enable the switch button for the corresponding services that you want to allow to access the Switch.
Service Port	For Telnet, SSH, FTP, HTTP or HTTPS services, you may change the default service port by typing the new port number in the Service Port field. If you change the default port number then you will have to let people (who wish to use the service) know the new port number for that service.
Timeout	Enter how many minutes (from 1 to 255) a management session can be left idle before the session times out. After it times out you have to log in with your password again. Very long idle timeouts may have security risks.

Table 283 SECURITY > Access Control > Service Access Control > Service Access Control (continued)

LABEL	DESCRIPTION
Login Timeout	The Telnet or SSH server do not allow multiple user logins at the same time. Enter how many seconds (from 30 to 300 seconds) a login session times out. After it times out you have to start the login session again. Very long login session timeouts may have security risks. For example, if User A attempts to connect to the Switch (through SSH), but during the login stage, do not enter the user name and/or password, User B cannot connect to the Switch (through SSH) before the Login Timeout for User A expires (default 150 seconds).
Redirect to HTTPS	This option allows your web browser to automatically redirect to a secure page, from HTTP to HTTPS (secure hypertext transfer protocol). SSL (Secure Sockets Layer) in HTTPS encrypts the transferred data by changing plain text to random letters and numbers.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

66.40 Remote Management

Use this screen to specify a group of one or more “trusted computers” from which an administrator may use a service to manage the Switch.

Click **SECURITY > Access Control > Remote Management** to view the screen as shown next.

Figure 364 SECURITY > Access Control > Remote Management > Remote Management IPv4

Remote Management IPv4

Secured Client Setup

Entry	Active	Start Address	End Address	Telnet	FTP	HTTP	ICMP	SNMP	SSH	HTTPS
1	☒	0.0.0.0	0.0.0.0	☒	☒	☒	☒	☒	☒	☒
2	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
3	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
4	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
5	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
6	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
7	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
8	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
9	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
10	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
11	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
12	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
13	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
14	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
15	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
16	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐

Apply **Cancel**

The following table describes the labels in this screen.

Table 284 SECURITY > Access Control > Remote Management > Remote Management IPv4

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	Enable the switch button to activate this secured client set. Clear the checkbox if you wish to temporarily disable the set without deleting it.
Start Address	Configure the IPv4 address range of trusted computers from which you can manage this Switch.
End Address	The Switch checks if the client IPv4 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.

66.41 Storm Control

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 **SECURITY > Storm Control > Storm Control** in the navigation panel to display the screen as shown next.

Figure 365 SECURITY > Storm Control > Storm Control

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

The following table describes the labels in this screen.

Table 285 SECURITY > Storm Control > Storm Control

LABEL	DESCRIPTION
Active	Enable the switch button to enable traffic storm control on the Switch. Disable the switch button to disable this feature.
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Broadcast (pkt/s)	Select this option and specify how many broadcast packets the port receives per second.
Multicast (pkt/s)	Select this option and specify how many multicast packets the port receives per second.
DLF (pkt/s)	Select this option and specify how many destination lookup failure (DLF) packets the port receives per second.

Table 285 SECURITY > Storm Control > Storm Control (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 reset the fields.

66.42 MAINTENANCE

This section explains how to configure the screens that let you maintain the firmware and configuration files.

66.43 What You Can Do

- Use the **Restore Configuration** screen ([Section 66.44 on page 520](#)) to upload a stored device configuration file.
- Use the **Backup Configuration** screen ([Section 66.45 on page 521](#)) to save your configuration for later use.
- Use the **Save Configuration** screen ([Section 66.46 on page 521](#)) to save the current configuration settings to a specific configuration file on the Switch.
- Use the **Firmware Upgrade** screen ([Section 66.47 on page 522](#)) to upload the latest firmware.
- Use the **Reboot System** screen ([Section 66.48 on page 523](#)) to restart the Switch without physically turning the power off and load a specific configuration file.
- Use the **Tech-Support** screen ([Section 66.49 on page 524](#)) to create reports for customer support if there are problems with the Switch.

66.44 Restore Configuration

Use this screen to restore a previously saved configuration file from your computer to the Switch.

Click **MAINTENANCE > Configuration > Restore Configuration > Restore Configuration** to access this screen.

Figure 366 MAINTENANCE > Configuration > Restore Configuration > Restore Configuration

Restore Configuration

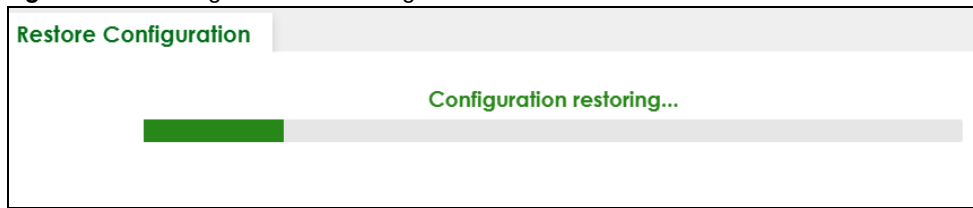
To restore the device's configuration from a file, browse the location of the configuration file and click Restore button.

File Path No file chosen

- 1 Click **Choose File** or **Browse** to locate the configuration file you wish to restore.
- 2 After you have specified the file, click **Restore**.

The Switch will run on the restored configuration after the restore process.

Figure 367 Configuration Restoring

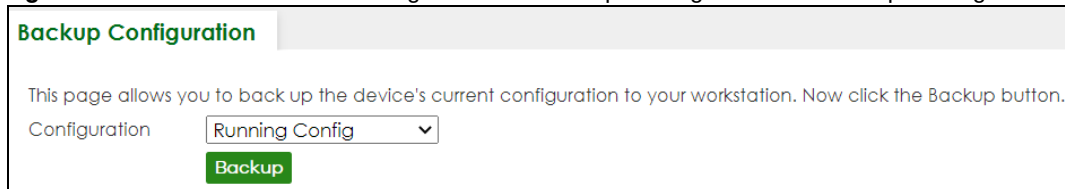


66.45 Backup Configuration

Backing up your Switch configurations allows you to create various “snap shots” of your device from which you may restore at a later date. Use this screen to back up your current Switch configuration to a computer.

To access this screen, click **MAINTENANCE > Configuration > Backup Configuration > Backup Configuration** in the navigation panel.

Figure 368 MAINTENANCE > Configuration > Backup Configuration > Backup Configuration



Follow the steps below to back up the current Switch configuration to your computer in this screen.

- 1 Select which Switch configuration file you want to download to your computer.

Note: **Custom Default** is only available in Standalone mode.

- 2 Click **Backup**.
- 3 If the current configuration file is open and/or downloaded to your computer automatically, you can click **File > Save As** on your computer to save the file to a specific place.
If a dialog box pops up asking whether you want to open or save the file, click **Save** or **Save File** to download it to the default downloads folder on your computer. If a **Save As** screen displays after you click **Save** or **Save File**, choose a location to save the file on your computer from the **Save in** drop-down list box and type a descriptive name for it in the **File name** list box. Click **Save** to save the configuration file to your computer.

66.46 Save Configuration

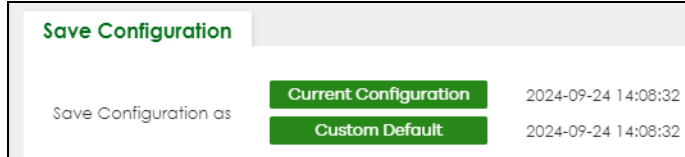
To access this screen, click **MAINTENANCE > Configuration > Save Configuration > Save Configuration** in the navigation panel.

Click **Current Configuration** to save the current configuration settings permanently to the Switch. This configuration is set up according to your network environment.

Click **Custom Default** to save the current configuration settings permanently to a customized default file on the Switch.

Note: **Custom Default** is only available in Standalone mode.

Figure 369 Maintenance > Configuration > Save Configuration



Note: If a customized default file was not saved, clicking **Custom Default** loads the factory default configuration on the Switch.

Alternatively, click **Save** on the top right in any screen to save the configuration changes to the current configuration.

Note: Clicking the **Apply** button after making configuration does NOT save the changes permanently. All unsaved changes are erased after you reboot the Switch.

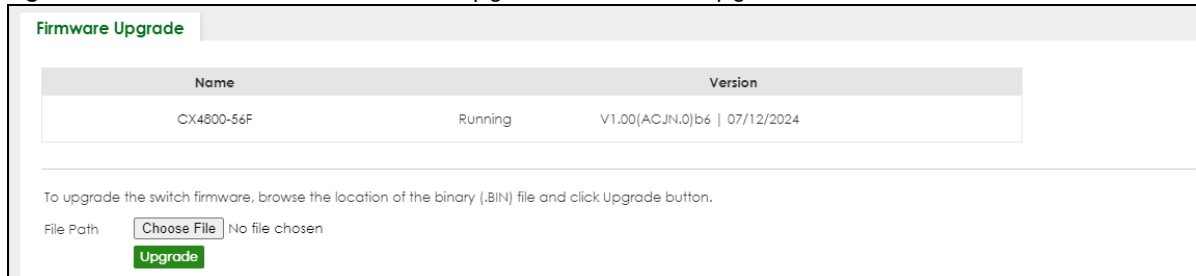
66.47 Firmware Upgrade

Use the following screen to upgrade your Switch to the latest firmware.

Note: Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.

Click **MAINTENANCE > Firmware Upgrade > Firmware Upgrade** to view the screen as shown next.

Figure 370 MAINTENANCE > Firmware Upgrade > Firmware Upgrade



Click **Choose File** or **Browse** to locate the firmware file you wish to upload to the Switch. Firmware upgrades are only applied after a reboot. Click **Upgrade** to load the new firmware.

After the firmware upgrade process is complete, see the **MONITOR > System Information > System Information** screen to verify your current firmware version number.

Table 286 MAINTENANCE > Firmware Upgrade > Firmware Upgrade

LABEL	DESCRIPTION
Name	This is the name of the Switch that you are configuring.
Version	This is the version number (and model code) and MM/DD/YYYY creation date of the firmware currently in use on the Switch. The firmware information is also displayed in MONITOR > System Information > System Information .
File Path	Click Choose File or Browse to locate 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 MAINTENANCE > Reboot System > Reboot System and click Current Configuration , Factory Default , or Custom Default (Current Configuration , Factory Default , and Custom Default are the configuration files you want the Switch to use when it restarts).

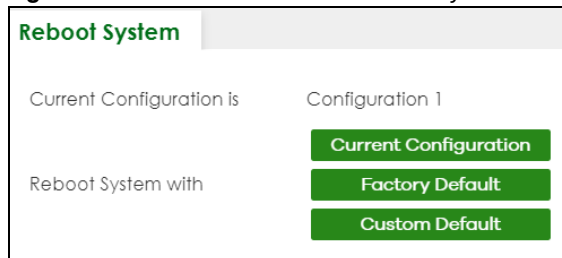
66.48 Reboot System

Reboot System allows you to restart the Switch without physically turning the power off. It also allows you to load the **Current Configuration**, a **Custom Default** or the **Factory Default** configuration when you reboot. Follow the steps below to reboot the Switch.

Note: **Custom Default** is only available in Standalone mode.

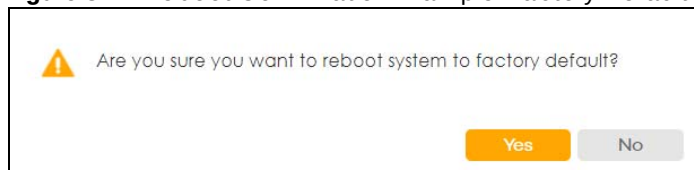
Click **MAINTENANCE > Reboot System > Reboot System** to view the screen as shown next.

Figure 371 MAINTENANCE > Reboot System > Reboot System



- 1 Click the **Current Configuration**, **Factory Default**, or **Custom Default** button to reboot and load that configuration file. The confirmation screen displays.

Figure 372 Reboot Confirmation Example: Factory Default



- 2 Click **YES** and then wait for the Switch to restart. This takes up to 2 minutes.

Click **Current Configuration** and follow steps 1 to 2 to reboot and load configuration one on the Switch.

Click **Factory Default** and follow steps 1 to 2 to reboot and load Zyxel factory default configuration settings on the Switch.

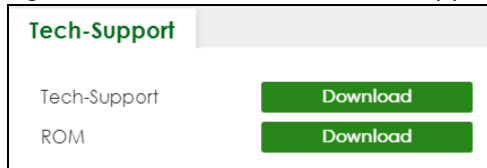
Click **Custom Default** and follow steps 1 to 2 to reboot and load a customized default file on the Switch.

66.49 Tech-Support

The Tech-Support feature is a log enhancement tool that logs useful information such as CPU utilization history, memory and Mbuf (Memory Buffer) log and crash reports for issue analysis by customer support should you have difficulty with your Switch. The Tech Support menu eases your effort in obtaining reports and it is also available in CLI command by typing “Show tech-support” command.

Click **MAINTENANCE > Tech-Support > Tech-Support** to see the following screen.

Figure 373 MAINTENANCE > Tech-Support > Tech-Support



You may need WordPad or similar software to see the log report correctly. The table below describes the fields in the above screen.

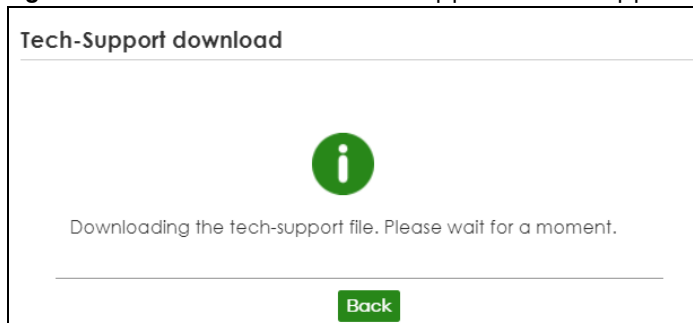
Table 287 MAINTENANCE > Tech-Support > Tech-Support

LABEL	DESCRIPTION
Tech-Support	Click Download to see all the log report and system status. This log report is stored in flash memory. If the All log report is too large, you can download the log reports separately below.
ROM	Click Download to see the Read Only Memory (ROM) log report. This report is stored in flash memory.

66.49.1 Tech-Support Download

When you click **Download** to save your current Switch configuration to a computer, the following screen appears. When the log report has downloaded successfully, click **Back** to return to the previous screen.

Figure 374 MAINTENANCE > Tech-Support > Tech-Support: Download



PART III

Troubleshooting and Appendices

CHAPTER 67

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](#)
- [Nebula Registration](#)

67.1 Power, Hardware Connections, and LEDs

[The Switch does not turn on. None of the LEDs turn on.](#)

- 1 Make sure you are using the power adapter or cord included with the Switch.
- 2 Make sure the power adapter or cord is connected to the Switch and plugged in to an appropriate power source. Make sure the power source is turned on.
- 3 Disconnect and re-connect the power adapter or cord to the Switch.
- 4 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 3.4 on page 46](#).
- 2 Check the hardware connections. See [Section 3.2 on page 37](#).
- 3 Inspect your cables for damage. Contact the vendor to replace any damaged cables.
- 4 Disconnect and re-connect the power adapter or cord to the Switch (in AC models or if the AC power supply is connected in AC/DC models).
- 5 If the problem continues, contact the vendor.

67.2 Switch Access and Login

I can see the **Login** screen, but I cannot log in to the Switch. (I forgot the user name and/or password.)

- 1 Check the Switch's management mode by using the **CLOUD** LED. See [Section 3.4 on page 46](#) for more information on the LED descriptions.
 - If you are in Cloud management mode, use the **Local credentials Password** to log in to the cloud mode – local GUI. The **Local credentials Password** can be found in **Site-wide > Configure > Site settings > Device configuration: Local credentials: Password** in the NCC portal.
 - If you are in standalone management mode, use the default user name **admin** and the default password on the label on the back of the Switch.

Note: Steps 1 and 2 are applicable if you get an invalid administrator password when using some functions in the ZON utility. See [Section 1.4.2 on page 31](#) for more information.

- 3 You may have exceeded the maximum number of concurrent Telnet sessions. Close other Telnet sessions or try connecting again later.

Check that you have enabled logins for HTTP or Telnet. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on access control for details.
- 4 If this does not work, or you are not sure what the Switch's management mode is, you have to reset the device to its factory defaults (Standalone management mode) first. See [Section 4.8 on page 80](#) for more information on resetting the Switch. (Temporarily disconnect the Internet connection to the Switch after the reset process, to prevent the Switch from being managed by NCC again.)

Note: After performing step 4 and you want to use the Cloud management mode, make sure the Switch is registered in your organization and site in the NCC portal. To register the Switch again, scan the QR code using the Zyxel Nebula Mobile app. See the [Section 1.4.1 on page 29](#) for more information on using the app to register the Switch.

I forgot the IP address for the Switch.

- 1 You can use the default IP address **https://DHCP-assigned IP** (when connecting to a DHCP server) or **192.168.1.1**. When in Cloud mode, the DHCP-assigned IP address could be found in the NCC portal, in **Site-wide > Devices > Switches** (The Switch must be registered and added to a site in Nebula in order for it to be managed by Nebula).

Note: When your computer is directly connected to the Switch, you can always use the domain name **setup.zyxel** to access the Web Configurator. This requires your computer to be able to connect to a DNS server.

- 2 If the Switch is removed from a site in Nebula, all the settings in the configuration file are reset to the Nebula factory defaults except for the IP address. If you changed the default dynamic IP address to a static IP address while the Switch was in a site in Nebula, the Switch will retain that static IP address after you remove it from the site in Nebula.
- 3 Use the ZON utility to find the IP address.
- 4 If you are using the console/USB port, use the command line **show ip** to find the IP address.
- 5 If the Switch is removed from a site in Nebula, all the settings in the configuration file are reset to the Nebula factory defaults except for the IP address. If you changed the default dynamic IP address to a static IP address while the Switch was in a site in Nebula, the Switch will retain that static IP address after you remove it from the site in Nebula.
- 6 Use the console port to log in to the Switch.
- 7 Use the **MGMT** port to log in to the Switch, the default IP address of the **MGMT** port is **192.168.0.1**.
- 8 If this does not work, you have to reset the device to its factory defaults. See [Section 4.8 on page 80](#).

I cannot see or access the **Login** screen in the Web Configurator.

- 1 Make sure you are using the correct IP address.
 - The default IP address is <https://DHCP-assigned IP> (when connecting to a DHCP server) or [192.168.1.1](#).
 - If you changed the IP address, use the new IP address.
 - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I forgot the IP address for the Switch](#).
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See [Section 3.4 on page 46](#).
- 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 Switch to its factory defaults, and try to access the Switch with the default IP address. See [Section 4.7 on page 79](#).
- 6 If the problem continues, contact Zyxel technical support, or try the advanced suggestion.

Advanced Suggestion

- Try to access the Switch using another service, such as Telnet. If you can access the Switch, check the remote management settings to find out why the Switch does not respond to HTTP.

[Pop-up Windows, JavaScripts and Java Permissions](#)

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

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

There is unauthorized access to my Switch through telnet, HTTP and SSH.

Go to the **MONITOR > System Log** screen to check for logs of unauthorized access to your Switch. To avoid unauthorized access, configure the secured client setting in the **SECURITY > Access Control > Remote Management** screen for telnet, HTTP and SSH (see [Section 52.5 on page 346](#)). Computers not belonging to the secured client set cannot get permission to access the Switch.

The Switch is already registered with NCC, but it is still in Standalone mode; it cannot connect to the NCC.

- 1 Make sure that NCC Discovery is enabled. Check the three NCC connection status circles on the **DASHBOARD** screen. All status circles display green (normal) when the Switch is connected and managed by NCC. If a circle displays orange (fails), hover a mouse over the circle to see diagnostic messages for troubleshooting. You can also go to the **SYSTEM > Cloud Management** screen to check the diagnostic messages.
- 2 Check your network's firewall or security settings. Make sure the following TCP ports are allowed: 443, 4335, and 6667.
- 3 Make sure your Switch can access the Internet.
- 4 Make sure your Switch does not have to go through network authentication such as a captive portal. If your network uses a captive portal, the network administrator may have to create a new VLAN without this requirement. Change your Switch's management VLAN settings as necessary.

67.3 Switch Configuration

I lost my configuration settings after I restarted the Switch.

Make sure you save your configuration into the Switch's non-volatile memory each time you make changes. Click **Save** at the top right of the Web Configurator to save the configuration permanently. See also [Section 65.12 on page 449](#) for more information about how to save your configuration.



I accidentally unplugged the Switch. I am not sure which configuration file will be loaded.

If you plug the power cable back to the Switch, it will reboot and load the configuration file that was used the last time. For example, if **Config 1** was used on the Switch before you accidentally unplugged the Switch, **Config 1** will be loaded when rebooting.

I want to use a different configuration file on the Switch, what should I do?

- 1 Go to **MAINTENANCE > Configuration > Restore Configuration**.
- 2 Click **Choose File** or **Browse** to locate the configuration file you wish to restore.
- 3 After you have specified the file, click **Restore**. The Switch will run on the restored configuration after the restore process.

I cannot access the NCC portal.

- Check that you are using the correct URL:
 - NCC: <https://nebula.zyxel.com/>
- Make sure your computer's Ethernet card is installed and functioning properly.
- Check that you have Internet access. In your computer, click **Start, (All) Programs, Accessories** and then **Command Prompt**. In the **Command Prompt** window, enter 'ping' followed by a website such as 'zyxel.com'. If you get a reply, try to ping 'nebula.zyxel.com'.
- Make sure you are using the correct web browser that supports HTML5. View the browser in full screen mode to display the NCC portal properly. Browsers supported are:
 - Google Chrome
 - Microsoft Edge
 - Mozilla Firefox

I cannot log into the NCC portal.

- Open your web browser and go to <https://nebula.zyxel.com>. If you do not have a Nebula Zyxel Account, click **Create account** and create an account.
- If you already have an account but cannot login, click **Forgot Password** to reset the password.

Some features I set using the NCC do not work as expected.

- 1 Make sure your Switch can access the Internet.
- 2 Make sure the Switch's **Status** displays "**Online**" in **Site-wide > Devices > Switches** on the NCC portal.
- 3 If the Switch is offline when the settings were changed, wait for ten minutes after the Switch goes back online.
- 4 After changing your Switch settings using the NCC, wait 1 – 2 minutes for the changes to take effect.
- 5 Check the Switch **Configuration status** in **Site-wide > Devices > Switches** on the NCC portal. The status should display "**up to date**".

67.4 Nebula Registration

I cannot register the Switch in Nebula because the previous owner has registered/locked it.

- To register a pre-owned Switch in Nebula, use the Nebula Mobile app to scan the Nebula QR code on the back label of the Switch.
- To register a pre-owned Switch in Nebula locked by the previous owner, inform the previous owner to remove the Switch from the Nebula organization or contact Zyxel technical support.

I no longer want to use Nebula to manage the Switch, what should I do?

- Remove the Switch from the Nebula organization first. See [From Nebula-managed to Standalone Mode on page 31](#) for details. The Switch will reboot and restore its factory-default settings.
- Make sure the **CLOUD** LED is off or blinking green. See [LEDs on page 46](#) for more information on LED behavior. This means the Switch is operating in standalone mode. Nebula Control Center Discovery is disabled in **SYSTEM > Cloud Management > Nebula Control Center Discovery** in the Web Configurator.

APPENDIX A

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the device.

For Zyxel Communications offices, see <https://service-provider.zyxel.com/global/en/contact-us> for the latest information.

For Zyxel Networks offices, see <https://www.zyxel.com/index.shtml> for the latest information.

Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

Taiwan

- Zyxel Communications (Taiwan) Co., Ltd.
- <https://www.zyxel.com>

Asia

China

- Zyxel Communications Corporation–China Office
- <https://www.zyxel.com/cn/sc>

India

- Zyxel Communications Corporation–India Office
- <https://www.zyxel.com/in/en-in>

Kazakhstan

- Zyxel Kazakhstan
- <https://www.zyxel.com/ru/ru>

Korea

- Zyxel Korea Co., Ltd.
- <http://www.zyxel.kr/>

Malaysia

- Zyxel Communications Corp.
- <https://www.zyxel.com/global/en>

Philippines

- Zyxel Communications Corp.
- <https://www.zyxel.com/global/en>

Singapore

- Zyxel Communications Corp.
- <https://www.zyxel.com/global/en>

Taiwan

- Zyxel Communications (Taiwan) Co., Ltd.
- <https://www.zyxel.com/tw/zh>

Thailand

- Zyxel Thailand Co., Ltd.
- <https://www.zyxel.com/th/th>

Vietnam

- Zyxel Communications Corporation–Vietnam Office
- <https://www.zyxel.com/vn/vi>

Europe

Belarus

- Zyxel Communications Corp.
- <https://www.zyxel.com/ru/ru>

Belgium (Netherlands)

- Zyxel Benelux
- <https://www.zyxel.com/nl/nl>
- <https://www.zyxel.com/fr/fr>

Bulgaria

- Zyxel Bulgaria

- <https://www.zyxel.com/bg/bg>

Czech Republic

- Zyxel Communications Czech s.r.o.
- <https://www.zyxel.com/cz/cs>

Denmark

- Zyxel Communications A/S
- <https://www.zyxel.com/dk/da>

Finland

- Zyxel Communications
- <https://www.zyxel.com/fi/fi>

France

- Zyxel France
- <https://www.zyxel.com/fr/fr>

Germany

- Zyxel Deutschland GmbH.
- <https://www.zyxel.com/de/de>

Hungary

- Zyxel Hungary & SEE
- <https://www.zyxel.com/hu/hu>

Italy

- Zyxel Communications Italy S.r.l.
- <https://www.zyxel.com/it/it>

Norway

- Zyxel Communications A/S
- <https://www.zyxel.com/no/no>

Poland

- Zyxel Communications Poland
- <https://www.zyxel.com/pl/pl>

Romania

- Zyxel Romania
- <https://www.zyxel.com/ro/ro>

Russian Federation

- Zyxel Communications Corp.
- <https://www.zyxel.com/ru/ru>

Slovakia

- Zyxel Slovakia
- <https://www.zyxel.com/sk/sk>

Spain

- Zyxel Iberia
- <https://www.zyxel.com/es/es>

Sweden

- Zyxel Communications A/S
- <https://www.zyxel.com/se/sv>

Switzerland

- Studerus AG
- <https://www.zyxel.com/ch/de-ch>
- <https://www.zyxel.com/fr/fr>

Turkey

- Zyxel Turkey A.S.
- <https://www.zyxel.com/tr/tr>

UK

- Zyxel Communications UK Ltd.
- <https://www.zyxel.com/uk/en-gb>

Ukraine

- Zyxel Ukraine
- <https://www.zyxel.com/ua/uk-ua>

South America

Argentina

- Zyxel Communications Corp.
- <https://www.zyxel.com/co/es-co>

Brazil

- Zyxel Communications Brasil Ltda.

- <https://www.zyxel.com/br/pt>

Colombia

- Zyxel Communications Corp.
- <https://www.zyxel.com/co/es-co>

Ecuador

- Zyxel Communications Corp.
- <https://www.zyxel.com/co/es-co>

South America

- Zyxel Communications Corp.
- <https://www.zyxel.com/co/es-co>

Middle East

Israel

- Zyxel Communications Corp.
- <https://il.zyxel.com>

North America

USA

- Zyxel Communications, Inc. – North America Headquarters
- <https://www.zyxel.com/us/en-us>

APPENDIX B

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type or 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 288 Commonly Used Services

NAME	PROTOCOL	PORT(S)	DESCRIPTION
AH (IPSEC_TUNNEL)	User-Defined	51	The IPSEC AH (Authentication Header) tunneling protocol uses this service.
AIM/New-ICQ	TCP	5190	AOL's Internet Messenger service. It is also used as a listening port by ICQ.
AUTH	TCP	113	Authentication protocol used by some servers.
BGP	TCP	179	Border Gateway Protocol.
BOOTP_CLIENT	UDP	68	DHCP Client.
BOOTP_SERVER	UDP	67	DHCP Server.
CU-SEEME	TCP UDP	7648 24032	A popular videoconferencing solution from White Pines Software.
DNS	TCP/UDP	53	Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers.
ESP (IPSEC_TUNNEL)	User-Defined	50	The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service.
FINGER	TCP	79	Finger is a UNIX or Internet related command that can be used to find out if a user is logged on.
FTP	TCP TCP	20 21	File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by email.
H.323	TCP	1720	NetMeeting uses this protocol.
HTTP	TCP	80	Hyper Text Transfer Protocol – a client or server protocol for the world wide web.

Table 288 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System – NFS is a client or server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet Internet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other).
PPTP	TCP	1723	Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel.
PPTP_TUNNEL (GRE)	User-Defined	47	PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel.
RCMD	TCP	512	Remote Command Service.
REAL_AUDIO	TCP	7070	A streaming audio service that enables real time sound over the web.
REXEC	TCP	514	Remote Execution Daemon.
RLOGIN	TCP	513	Remote Login.
RTELNET	TCP	107	Remote Telnet.
RTSP	TCP/UDP	554	The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet.
SFTP	TCP	115	Simple File Transfer Protocol.
SMTP	TCP	25	Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one email server to another.
SNMP	TCP/UDP	161	Simple Network Management Program.
SNMP-TRAPS	TCP/UDP	162	Traps for use with the SNMP (RFC:1215).

Table 288 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
SQL-NET	TCP	1521	Structured Query Language is an interface to access data on many different types of database systems, including mainframes, midrange systems, UNIX systems and network servers.
SSH	TCP/UDP	22	Secure Shell Remote Login Program.
STRM WORKS	UDP	1558	Stream Works Protocol.
SYSLOG	UDP	514	Syslog allows you to send system logs to a UNIX server.
TACACS	UDP	49	Login Host Protocol used for (Terminal Access Controller Access Control System).
TELNET	TCP	23	Telnet is the login and terminal emulation protocol common on the Internet and in UNIX environments. It operates over TCP/IP networks. Its primary function is to allow users to log into remote host systems.
TFTP	UDP	69	Trivial File Transfer Protocol is an Internet file transfer protocol similar to FTP, but uses the UDP (User Datagram Protocol) rather than TCP (Transmission Control Protocol).
VDOLIVE	TCP	7000	Another videoconferencing solution.

APPENDIX C

IPv6

Overview

IPv6 (Internet Protocol version 6), is designed to enhance IP address size and features. The increase in IPv6 address size to 128 bits (from the 32-bit IPv4 address) allows up to 3.4×10^{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 289 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 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 (0:0:0:0:0:1 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 290 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 cannot be assigned to a multicast group.

Table 291 Reserved Multicast Address

MULTICAST ADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses 4 bits for each character (1 – 10, A – F). Each block's 16 bits are then represented by 4 hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

Interface ID

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

EUI-64

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

Table 292

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

Table 293

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

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.

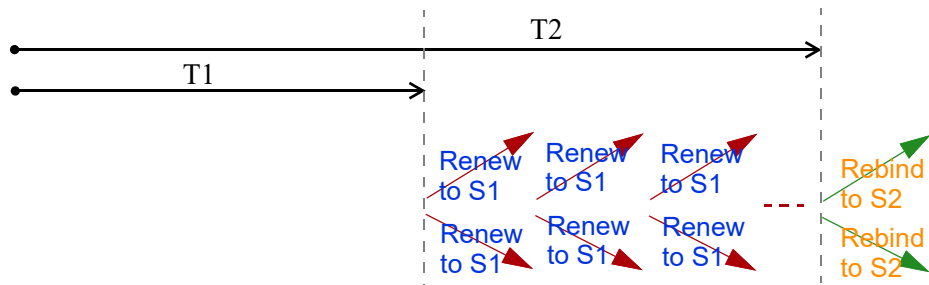
Identity Association

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, 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.

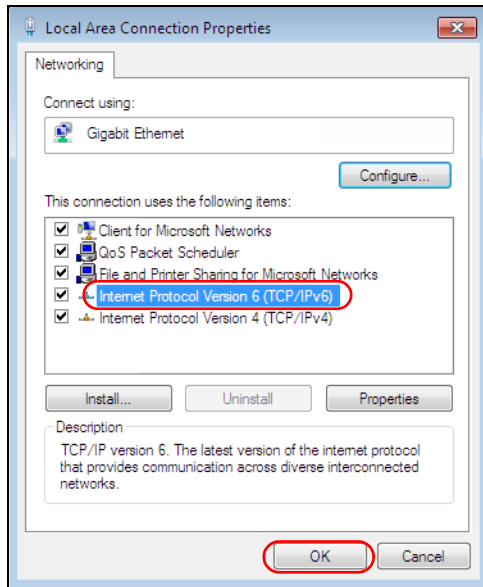
An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

Example – Enabling IPv6 on Windows 7

Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

- 1 Select **Control Panel > Network and Sharing Center > Local Area Connection**.
- 2 Select the **Internet Protocol Version 6 (TCP/IPv6)** check box to enable it.
- 3 Click **OK** to save the change.



- 4 Click **Close** to exit the **Local Area Connection Status** screen.
- 5 Select **Start > All Programs > Accessories > Command Prompt**.
- 6 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

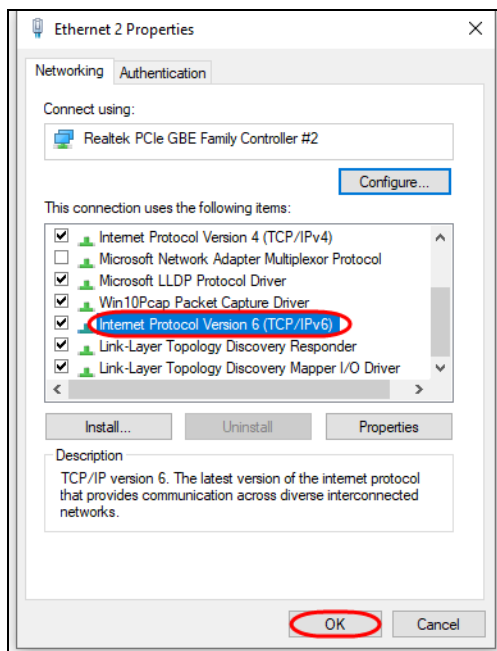
    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:b021:2d::1000
    Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
    IPv4 Address. . . . . : 172.16.100.61
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::213:49ff:feaa:7125%11
                                172.16.100.254
```

Example – Enabling IPv6 on Windows 10

Windows 10 supports IPv6 by default. DHCPv6 is enabled when you enable IPv6 on a Windows 10 PC.

To enable IPv6 in Windows 10:

- 1 Select **Control Panel > Network and Sharing Center**.
- 2 On the left side of the **Network and Sharing Center**, select **Change adapter settings**.
- 3 Right-click your network connection and select **Properties**.
- 4 Select the **Internet Protocol Version 6 (TCP/IPv6)** check box to enable it.
- 5 Click **OK** to save the changes for the selected network adapter.

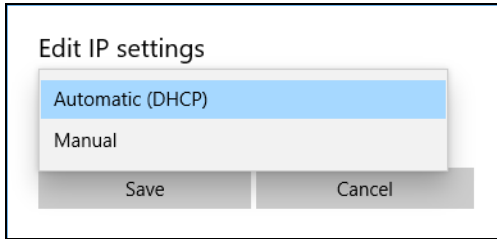


- 6 Click **OK** to exit the selected network adapter **Properties** screen.

Example – Enabling DHCPv6 on Windows 10

Windows 10 supports DHCPv6 by default. To enable DHCPv6 client on your computer:

- 1 Select **Start > Settings > Network & Internet**.
- 2 On the left side of the **Network & Internet**, select **Ethernet**. Then select the Ethernet network you are connected to.
- 3 Under **IP assignment**, select **Edit**.
- 4 Under **Edit IP settings**, select **Automatic (DHCP)** or **Manual**. Then click **Save**.



- When you select **Automatic (DHCP)**, the IP address settings and DNS server address setting are set automatically by your router.
- When you select **Manual**, you can manually set your IP address settings and DNS server address.

Now your computer can obtain an IPv6 address from a DHCPv6 server.

APPENDIX D

Importing a Certificate

When you connect to the Switch Web Configurator using HTTPS, a warning screen “Your connection is not private” may show up. If you see this warning screen, it indicates that your web browser has failed to verify the Secure Sockets Layer (SSL) certificate, which opens an encrypted connection. You can ignore this message and proceed to the website.

This appendix shows you how to import a public key certificate into your web browser to avoid the “Your connection is not private” screen. The web browsers are:

- Google Chrome
- Microsoft Edge
- Mozilla Firefox.

Public key certificates are used by web browsers to ensure that a secure web site is legitimate. When a certificate authority such as VeriSign, Comodo, or Network Solutions, to name a few, receives a certificate request from a website operator, they confirm that the web domain and contact information in the request match those on public record with a domain name registrar. If they match, then the certificate is issued to the website operator, who then places it on the website to be issued to all visiting web browsers to let them know that the website is legitimate.

Many Zyxel products, such as the Switch, issue their own public key certificates. These can be used by web browsers on a LAN or WAN to verify that they are in fact connecting to the legitimate device and not one masquerading as it. However, because the certificates were not issued by one of the several organizations officially recognized by the most common web browsers, you will need to import the Zyxel-created certificate into your web browser and flag that certificate as a trusted authority.

Note: You can see if you are browsing on a secure website if the URL on your web browser’s address bar begins with `https://` or there is a sealed padlock icon () somewhere in the web browser window (not all web browsers show the padlock in the same location).

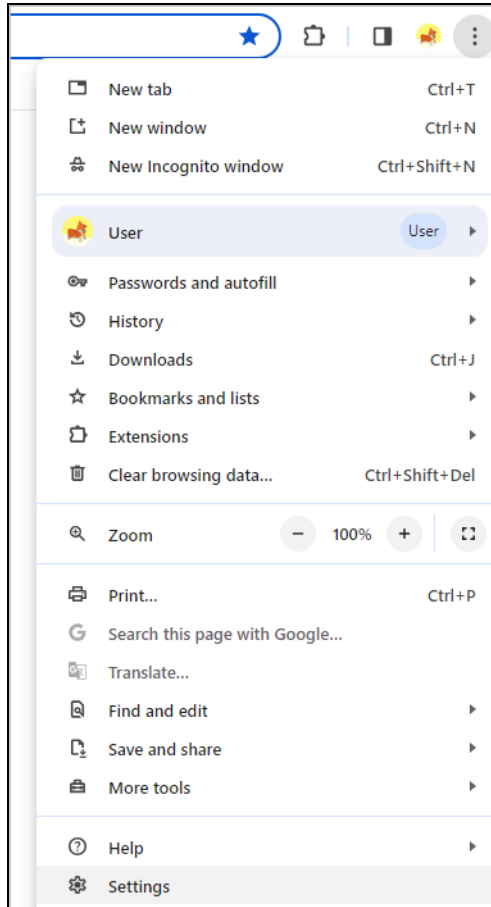
Note: You need a certificate from a trusted Certification Authority (CA) for this Switch.

Importing a Certificate to Google Chrome and Microsoft Edge

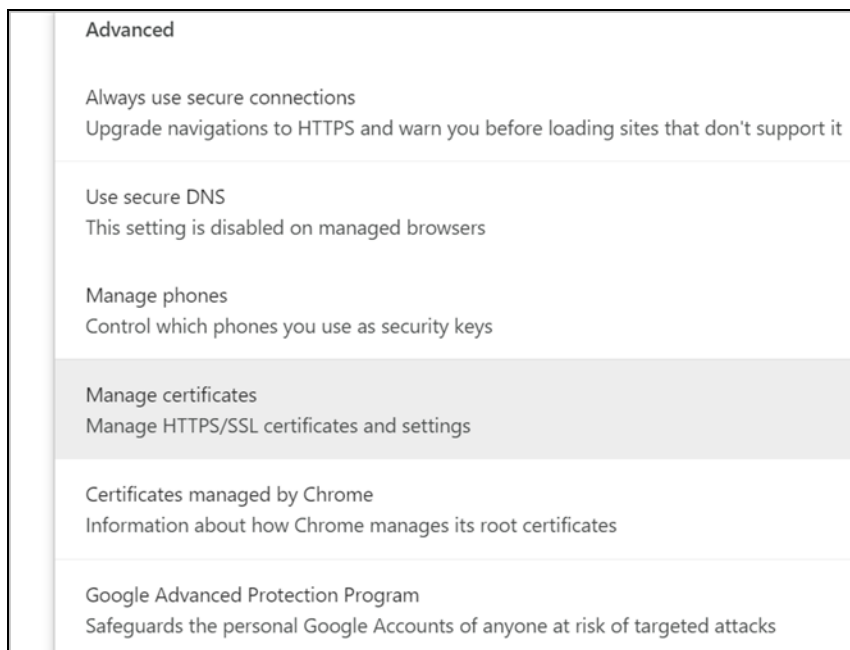
The following example uses Google Chrome on Windows 10. You first have to store the certificate in your computer and then install it as a Trusted Root CA, as shown in the following tutorial.

The Importing process is quite similar between Google Chrome and Microsoft Edge. The following procedures in Google Chrome can apply the same way in Microsoft Edge.

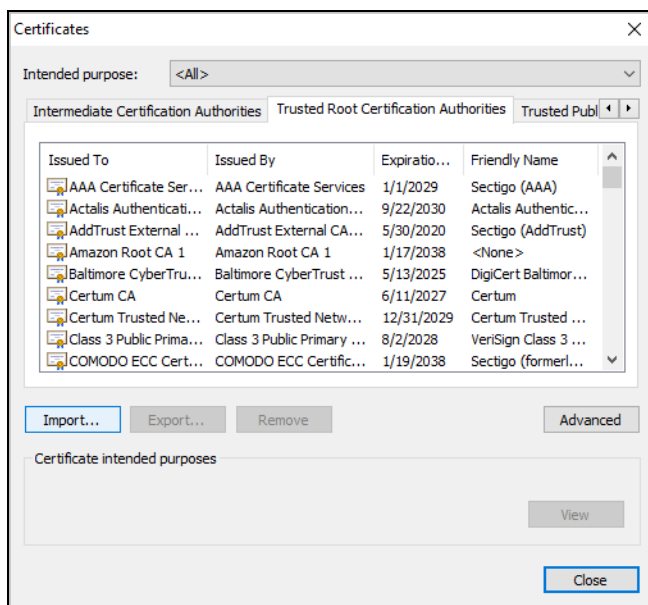
- 1 Open the Google Chrome browser. Click the three dots on the upper right. Then choose **Settings**.



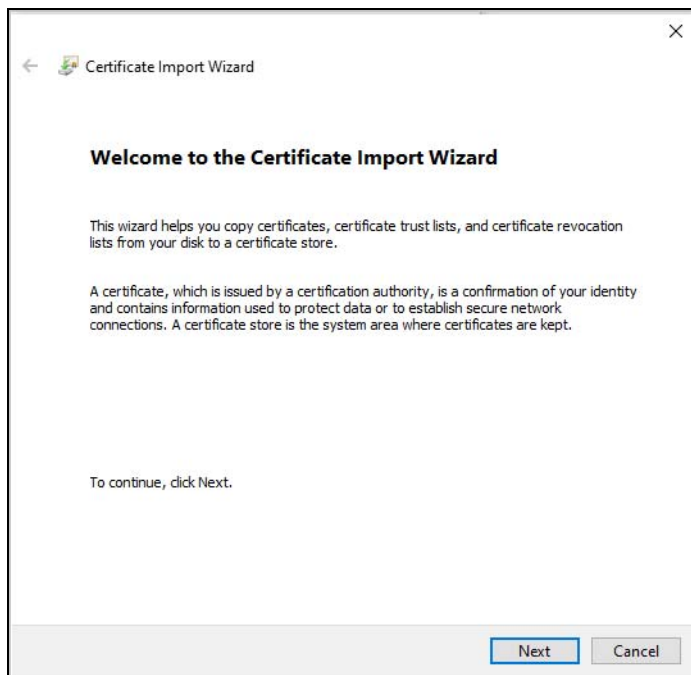
- 2 In Google Chrome, click **Privacy and security** > **Security** > **Manage certificates**.
In Microsoft Edge, click **Privacy, search, and services** > **Manage certificates**.



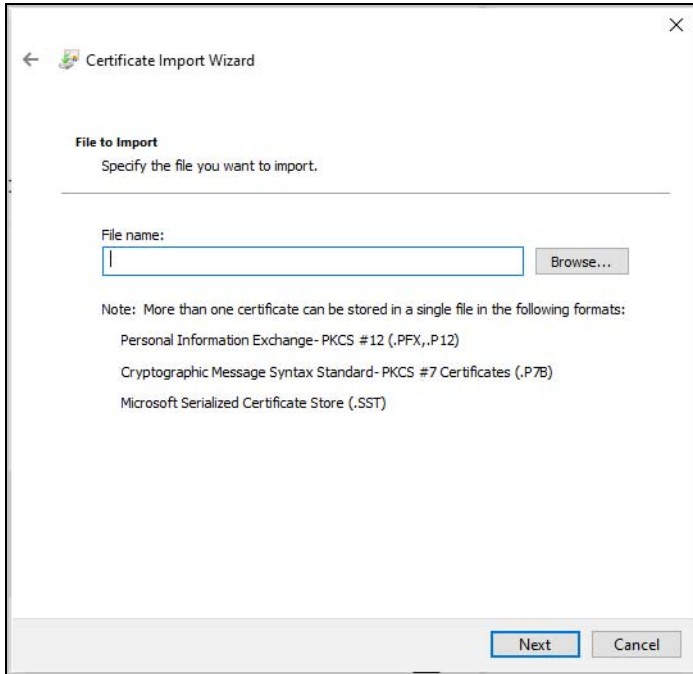
- 3 Select the **Trusted Root Certification Authorities** tab and click **Import**.



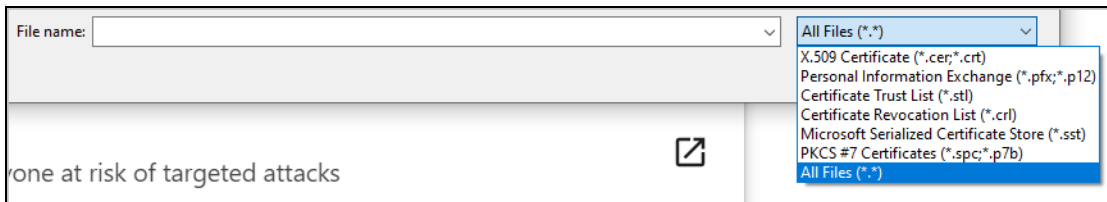
- 4 The **Certificate Import Wizard** screen appears. Click **Next** to continue.



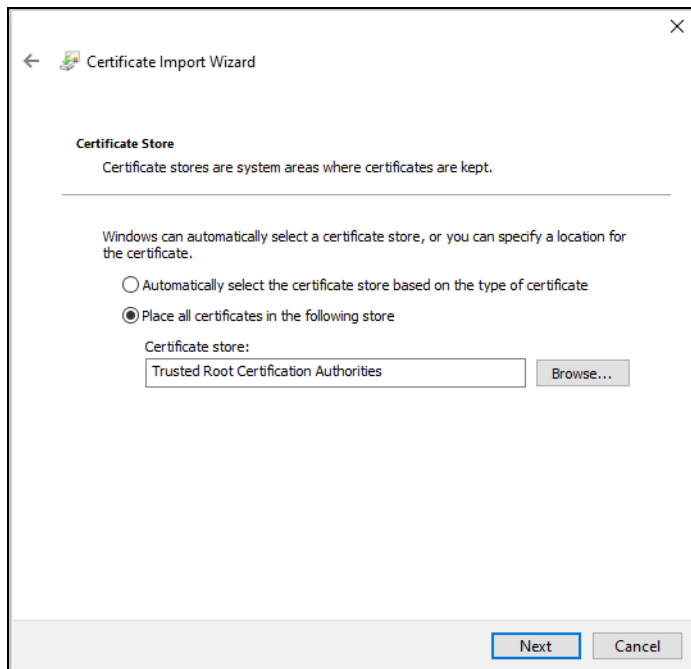
- 5 Click **Browse** to select a certificate already saved in your computer and click **Next** to continue.



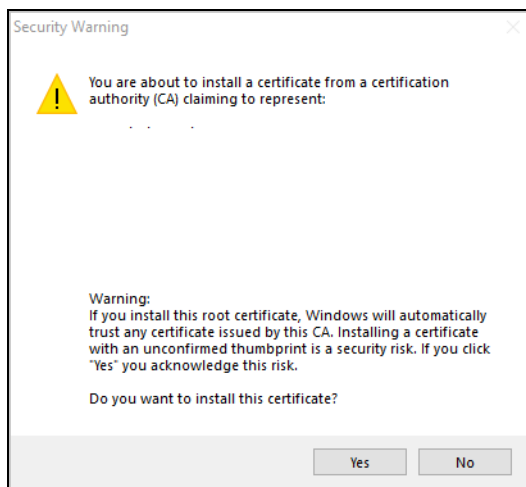
- 6 Select **All Files** to locate the certificate in your computer.



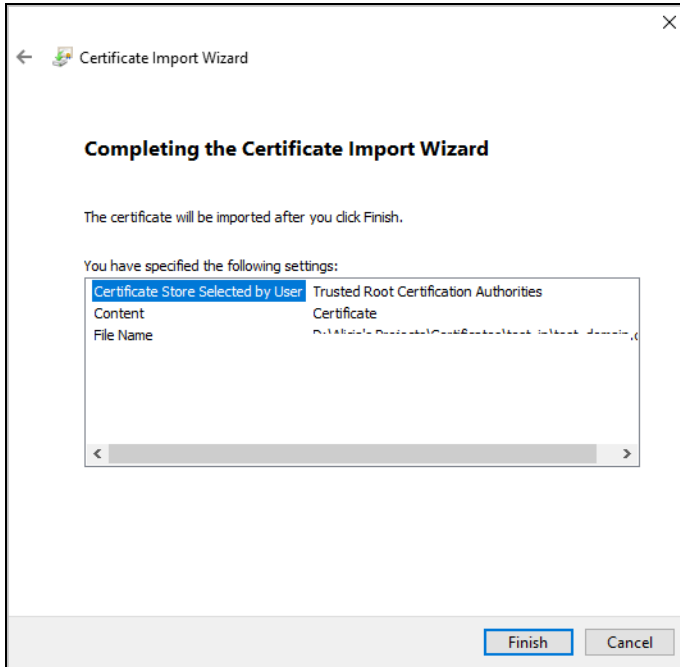
- 7 Two options are available for certificate stores. One is **Automatically select the certificate store based on the type of certificate**. This means the certificate import wizard can identify from the certificate whether it is a CA certificate or a personal certificate, and install it into the appropriate certificate store. The other option is **Place all certificates in the following store**. With this option, you can choose the desired folder for the certificate store. After selection, click **Next**.



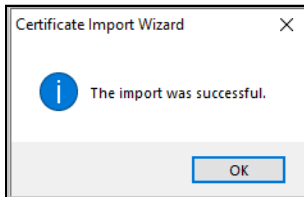
- 8 A security warning message appears, click **Yes** to continue.



- 9 Click **Finish** to exit the wizard.



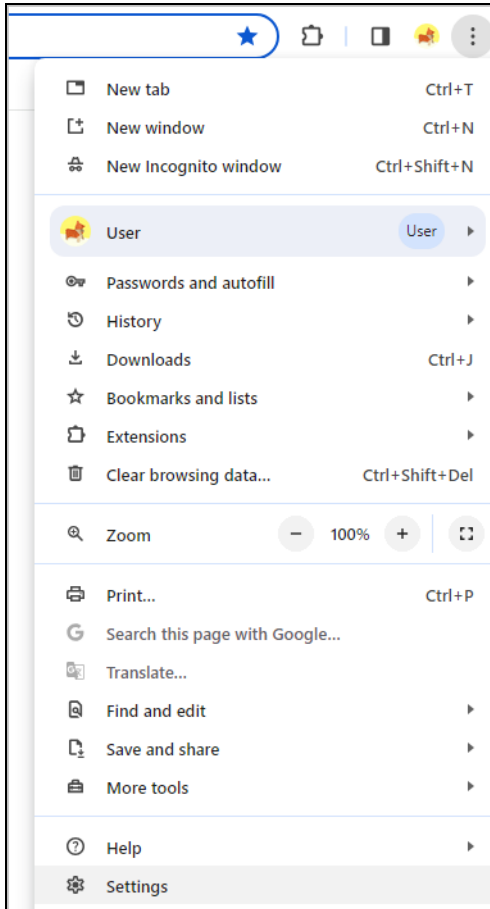
A pop-up screen informs you that the import was successful.



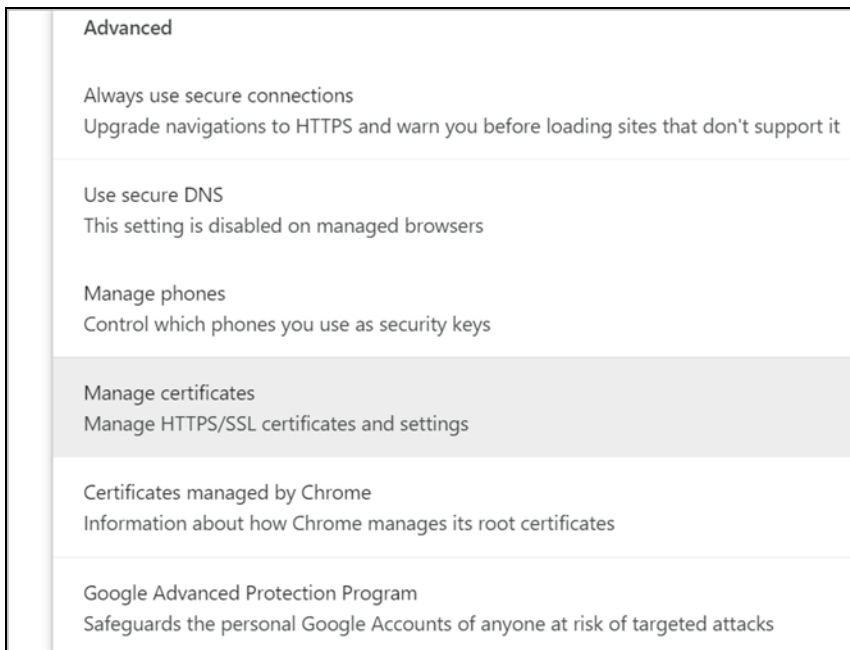
Remove a Certificate in Google Chrome and Microsoft Edge

This section shows you how to remove a public key certificate in Google Chrome and Microsoft Edge on Windows 10.

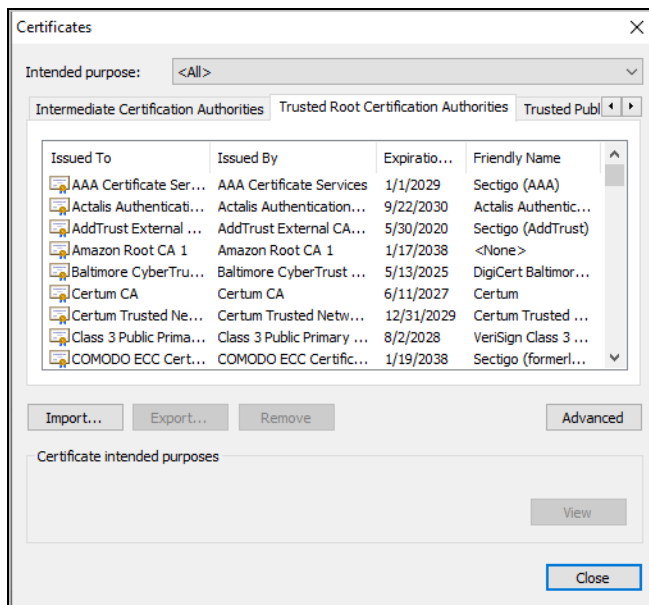
- 1 Open your web browser, click the three dots on the upper right, and click **Settings**.



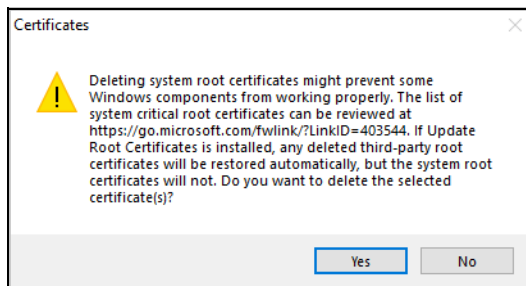
- 2 In Google Chrome, click **Privacy and security** > **Security** > **Manage certificates**.
In Microsoft Edge, click **Privacy, search, and services** > **Manage certificates**.



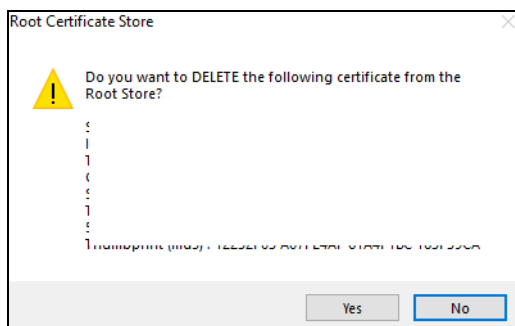
- 3** On the **Certificates** screen, select the **Trusted Root Certification Authorities** tab.



- 4 Select the certificate you want to remove and click **Remove**.
- 5 Click **Yes** when you see the following warning message.



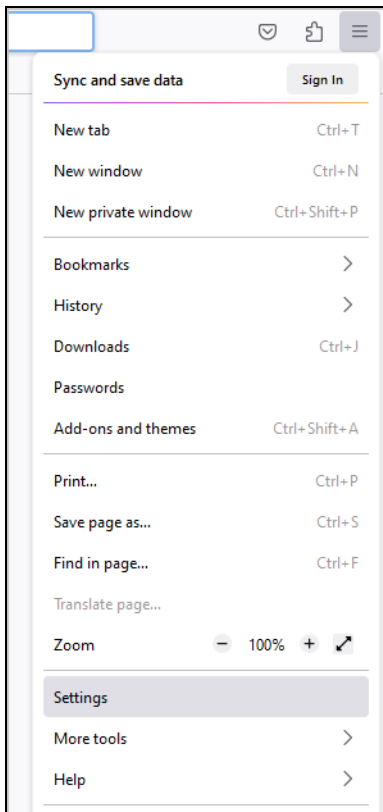
- 6** Confirm the details displayed in the warning message and click **Yes**.



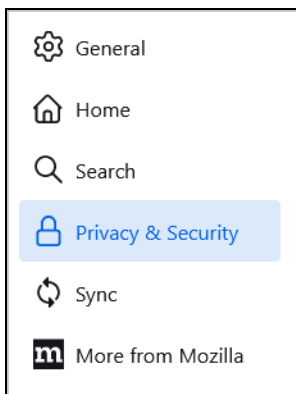
Import a Certificate to Mozilla Firefox

The following example uses Mozilla Firefox on Windows 10. You first have to store the certificate in your computer and then install it as a Trusted Root CA. To import a certificate to the Firefox browser, do the following:

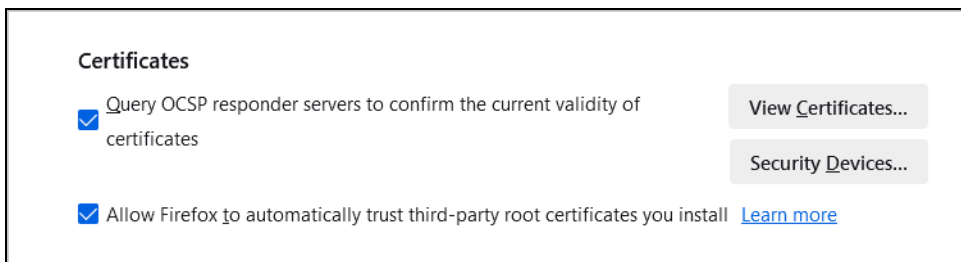
- 1 Open the Firefox browser and click the **Open application menu** icon on the upper right. Then click **Settings**.



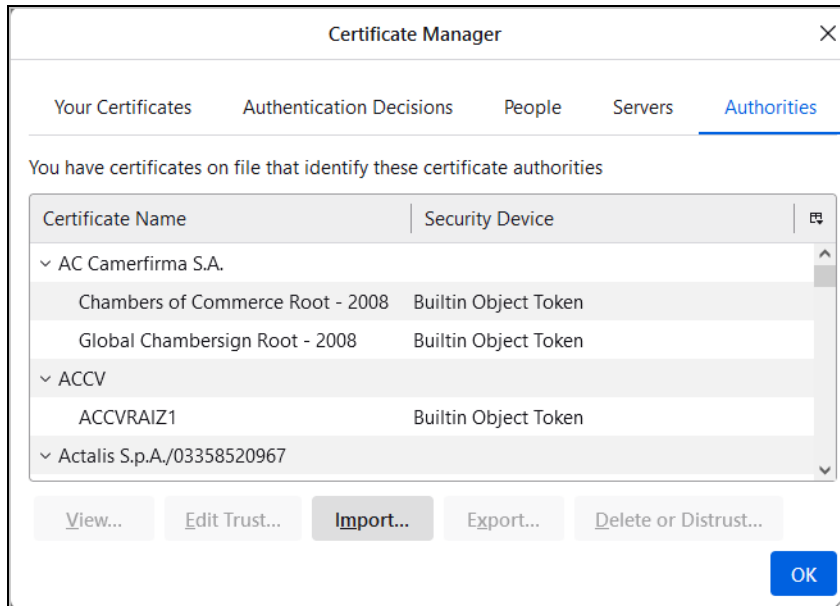
- 2 Click **Privacy & Security**.



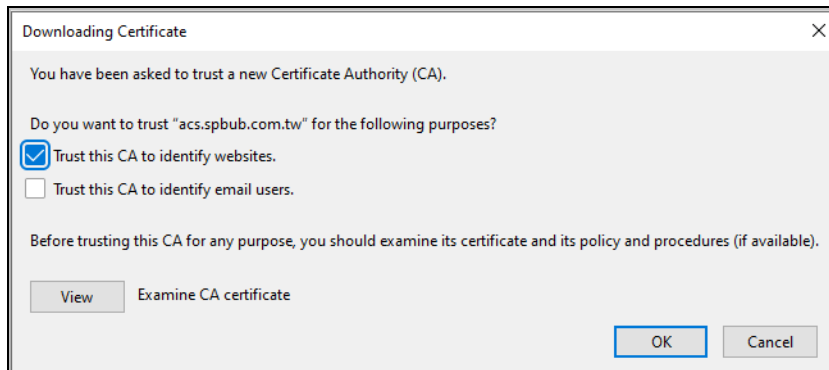
- 3 On the **Privacy & Security** screen, scroll down to locate **Certificates** and click **View Certificates**.



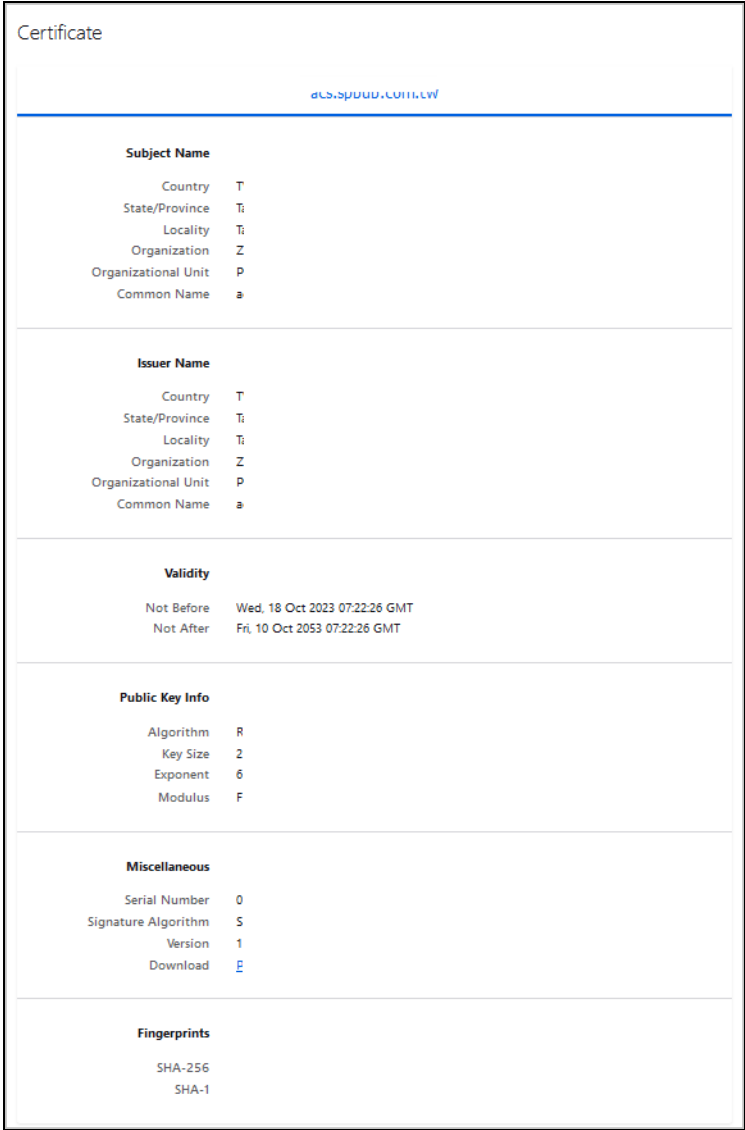
- 4 On the **Certificate Manager** screen, select the **Authorities** tab and click **Import**.



- 5 Open the certificate file in your computer and the **Downloading Certificate** screen appears. Click **Trust this CA to identify websites**. Click **View** to examine the imported CA certificate.

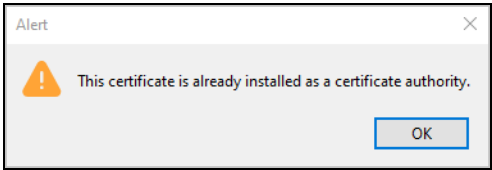


- 6 When the certificate details appear, view the content to confirm the correct organization name. Confirm that the validity period has the correct start and end dates. The **Common Name** can be either an IP address or domain name. Confirm that the client's IP address or domain name aligns with the **Common Name** on the certificate. If all the information on the certificate is correct, close the certificate screen and click **OK**.



The certificate file is now installed in the Firefox browser.

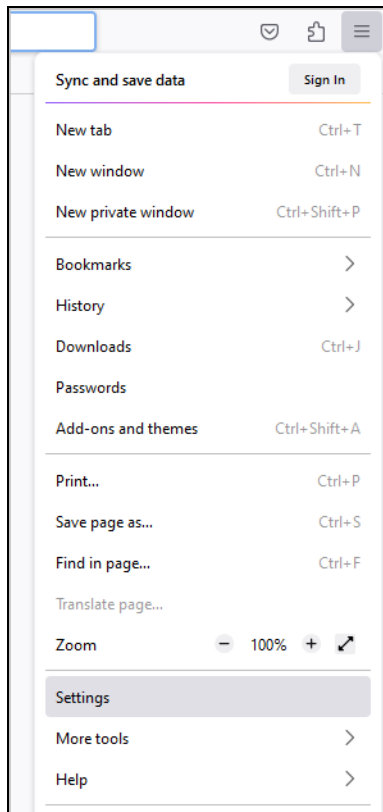
To check if the import is successful, click **Import** to select the same certificate again to see if the alert **This certificate is already installed as a certificate authority** pops up.



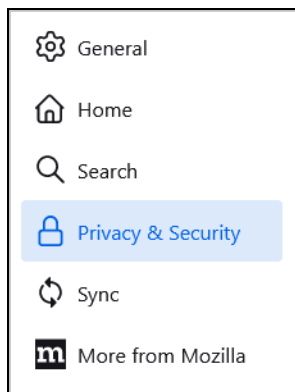
Removing a Certificate in Mozilla Firefox

This section shows you how to remove a public key certificate in Mozilla Firefox.

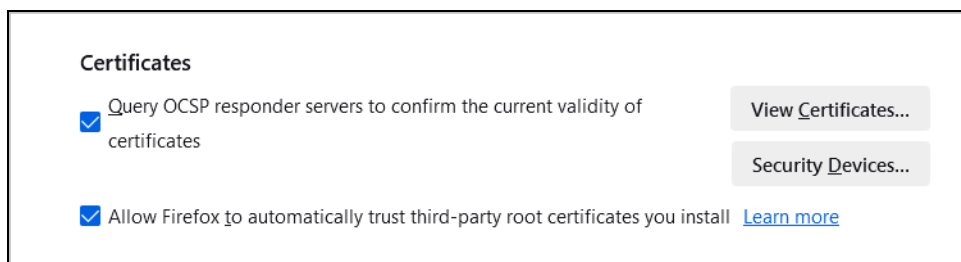
- 1 Open the Firefox browser and click the **Open application menu** icon on the upper right. Then click **Settings**.



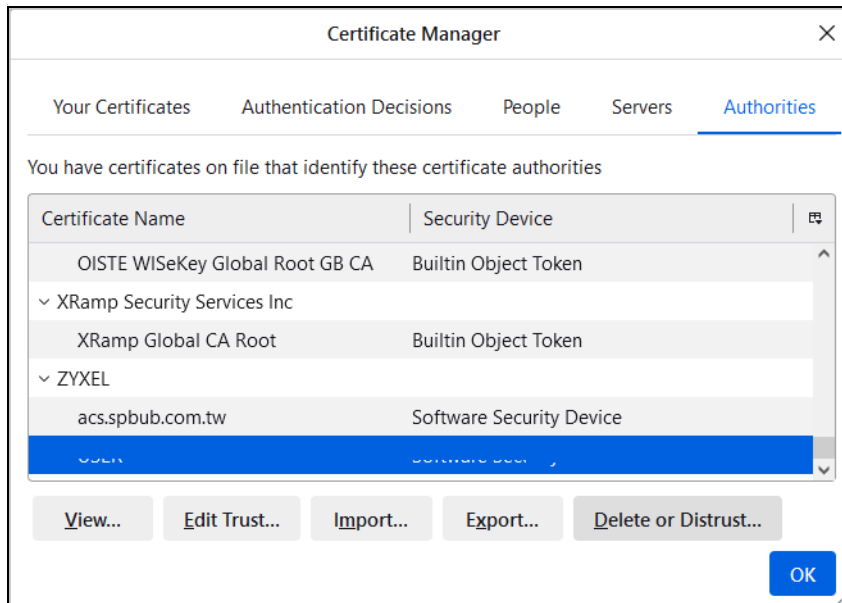
- 2 Click **Privacy & Security**.



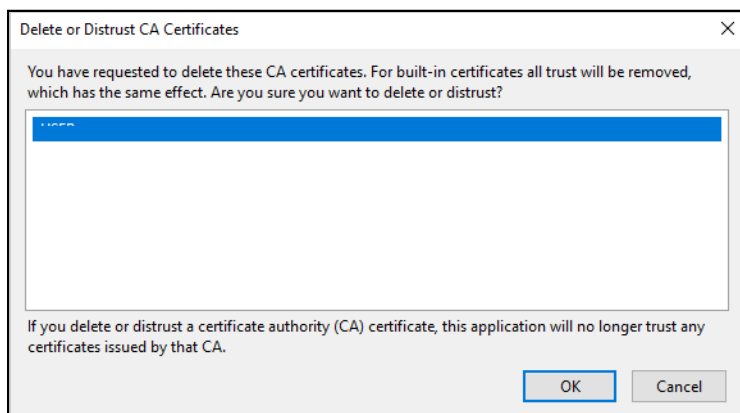
- 3 On the **Privacy & Security** screen, locate **Certificates** and click **View Certificates**.



- 4 In the **Certificate Manager** screen, click the **Authorities** tab and select the certificate you want to remove. Then, click **Delete or Distrust**.



- 5 On the next screen, click **OK**.



The next time you visit the web site with the public key certificate removed, a certification error will appear.

APPENDIX E

Legal Information

Copyright

Copyright © 2025 by Zyxel and/or its affiliates.

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 and/or its affiliates.

Published by Zyxel and/or its affiliates. All rights reserved.

Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Regulatory Notice and Statement

United States of America



The following information applies if you use the product within USA area.

Federal Communications Commission (FCC) EMC Statement

- This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:
 - (1) This device may not cause harmful interference.
 - (2) This device must accept any interference received, including interference that may cause undesired operations.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
- This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canada

The following information applies if you use the product within Canada area.

Innovation, Science and Economic Development Canada ICES statement

CAN ICES (A)/NMB(A)

Europe and the United Kingdom



The following information applies if you use the product within the European Union and United Kingdom.

EMC statement

WARNING: This equipment is compliant with Class A of EN55032. In a residential environment this equipment may cause radio interference.

List of National Codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CZ	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Sweden	SE
Ireland	IE	Switzerland	CH
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- To avoid possible eye injury, do NOT look into an operating fiber-optic module's connector.
- Do NOT use this device near water, for example, in a wet basement or near a swimming pool.
- Do NOT expose your device to dampness, dust or corrosive liquids.
- Do NOT store things on the device.
- Do NOT obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do NOT install or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do NOT open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. Only qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Do NOT remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do NOT allow anything to rest on the power adaptor or cord and do NOT place the device where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/adaptors. Connect it to the right supply voltage (for example, 120V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adaptor or cord is prohibited. Contact your local vendor to order a new one.
- Do NOT use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- CAUTION: RISK OF EXPLOSION IF BATTERY IS REPLACED BY AN INCORRECT TYPE, DISPOSE OF USED BATTERIES ACCORDING TO THE INSTRUCTION. Dispose them at the applicable collection point for the recycling of electrical and electronic device. For detailed information about recycling of this device, please contact your local city office, your household waste disposal service or the store where you purchased the device.
- Use ONLY power wires of the appropriate wire gauge for your device. Connect it to a power supply of the correct voltage.
- Fuse Warning! Replace a fuse only with a fuse of the same type and rating.
- The POE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,
 - For PERMANENTLY CONNECTED DEVICES, a readily accessible disconnect device shall be incorporated external to the device;
 - For PLUGGABLE DEVICES, the socket-outlet shall be installed near the device and shall be easily accessible.
- This device must be grounded by qualified service personnel. Never defeat the ground conductor or operate the device in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.
- If your device has an earthing screw (frame ground), connect the screw to a ground terminal using an appropriate AWG ground wire. Do this before you make other connections.
- If your device has no earthing screw, but has a 3-prong power plug, make sure to connect the plug to a 3-hole earthed socket.
- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:
 - Install the power supply before connecting the power cable to the power supply.
 - Unplug the power cable before removing the power supply.
 - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supply.
- Do not put the device in a place that is humid, dusty or has extreme temperatures as these conditions may harm your device.
- Please refer to the device back label, datasheet, box specifications or catalog information for the power rating of the device and operating temperature.

- Complies with 21 CFR 1040.10 and 1040.11 except for conformance with IEC 60825-1 Ed. 3., as described in Laser Notice No. 56, dated May 8, 2019.
- Conforme à 21 CFR 1040.10 et 1040.11 sauf pour la conformité à la norme CEI 60825-1 Ed. 3., comme décrit dans la notice laser Numéro 56 du 8 mai 2019.
- Ce produit laser est un produit laser de classe 1 conforme à la norme CEI 60825-1: 2014
- CLASS 1 LASER PRODUCT & "IEC 60825-1:2014"
- Caution – Use of controls or adjustments or performance of procedures other than those specified herein may result in hazardous radiation exposure.
- Attention – L'utilisation des commandes ou réglages ou l'exécution des procédures autres que celles spécifiées dans les présents exigences peuvent être la cause d'une exposition à un rayonnement dangereux)

Important Safety Instructions

- 1 Warning! Energy Hazard. Remove all metal jewelry, watches, and so on from your hands and wrists before serving the Switch.

- 2 Caution! The RJ-45 jacks are not used for telephone line connection.

- 3  Hazardous Moving Parts. Keep body parts away from fan blades.

- 4  Hot Surface. Do not touch.

- 1 Avertissement: Risque de choc électrique. Retirer tout bijoux en métal et votre montre de vos mains et poignets avant de manipuler cet appareil.

- 2 Attention: Les câbles RJ-45 ne doivent pas être utilisés pour les connections téléphoniques.

- 3  Mobilité des pièces détachées. S'assurer que les pièces détachées ne sont pas en contact avec les pales du ventilateur.

- 4  Surface brûlante. Ne pas toucher.

Environment Statement

Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.



台灣

以下訊息僅適用於產品銷售至台灣地區

- 這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。
- 為避免電磁干擾，本產品不應安裝或使用於住宅環境。

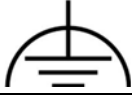
安全警告 – 為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸
 - 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
 - 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請使用隨貨提供或指定的連接線 / 電源線 / 電源變壓器，將其連接到合適的供應電壓（如：台灣供應電壓 110 伏特）。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 設備必須接地，接地導線不允許被破壞或沒有適當安裝接地導線，如果不確定接地方式是否符合要求可聯繫相應的電氣檢驗機構檢驗。
- 如果您提供的系統中有提供熱插拔電源，連接或斷開電源請遵循以下指導原則：
 - 先連接電源線至設備連，再連接電源。
 - 先斷開電源再拔除連接至設備的電源線。
 - 如果系統有多個電源，需拔除所有連接至電源的電源線再關閉設備電源。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
 - 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
 - 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Explanation of the Symbols

SYMBOL	EXPLANATION
	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC is the unidirectional flow or movement of electric charge carriers.
	Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor.
	Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation.

Viewing Certifications

Go to <https://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 <https://www.zyxel.com/global/en/support/warranty-information>.

Registration

Register your product online at www.zyxel.com to receive email notices of firmware upgrades and related information.

Trademarks

The trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Index

Numbers

802.1P priority [203](#), [493](#)

A

AAA [338](#)

accounting [338](#)

authentication [338](#)

authorization [338](#)

AAA (Authentication, Authorization and Accounting) [338](#)

access control

account security [355](#)

limitations [352](#), [515](#)

login account [145](#), [478](#)

overview [352](#), [515](#)

remote management [353](#), [517](#)

service port [352](#), [516](#)

SNMP [153](#)

account security [355](#)

Account Security screen [355](#)

accounting

setup [343](#)

Address Resolution Protocol (ARP) [105](#), [311](#), [450](#), [451](#)

admin [355](#)

administrator password [146](#), [479](#)

age [268](#)

aging time [160](#)

air circulation

for cooling [33](#)

anti-arp scan [378](#)

blocked hosts [379](#)

host threshold [380](#)

status [379](#)

trusted hosts [382](#)

applications

backbone [25](#)

bridging [25](#)

fiber uplink [25](#)

IEEE 802.1Q VLAN [26](#)

switched workgroup [26](#)

ARP

how it works [311](#)

learning mode [311](#)

overview [311](#)

ARP (Address Resolution Protocol) [105](#)

ARP inspection [395](#), [418](#)

and MAC filter [419](#)

configuring [419](#)

syslog messages [419](#)

trusted ports [419](#)

ARP Learning screen [313](#)

ARP scan [378](#)

ARP Setup screen [313](#)

ARP Table screen [105](#)

ARP-Reply [312](#)

ARP-Request [313](#)

ATM (Asynchronous Transmission Mode) [26](#)

authentication

setup [343](#)

authentication, authorization and accounting [338](#)

authorization

privilege levels [346](#)

setup [343](#)

authorized technician

install the Switch [33](#)

automatic VLAN registration [279](#), [508](#)

B

back up

configuration file [446](#), [521](#)

binding table [395](#)

build [400](#)

building [395](#)

BPDU (Bridge Protocol Data Units) [384](#)

BPDU guard [384](#)

and Errdisable Recovery [384](#)

port status [384](#)

BPDUs [252](#)
Bridge Protocol Data Units [384](#)
Bridge Protocol Data Units (BPDUs) [252](#)
broadcast storm control [387](#)

C

Certificates screen [437](#)
certifications
 viewing [565](#)
CFI (Canonical Format Indicator) [279](#), [508](#)
CIST [273](#)
Class of Service [238](#)
classifier [362](#)
 and QoS [362](#)
 example [370](#)
 logging [369](#)
 match order [369](#)
 overview [362](#)
 setup [363](#), [365](#)
 status [363](#)
clearance
 Switch installation [33](#)
cloning a port, see port cloning
Cloud Connection Status [101](#)
cluster management [441](#)
 and switch passwords [444](#)
 cluster manager [441](#), [443](#)
 cluster member [441](#)
 cluster member firmware upgrade [445](#)
 network example [441](#)
 setup [442](#)
 specification [441](#)
 status [441](#)
 switch models [441](#)
 VID [443](#)
 Web Configurator [444](#)
Cluster Management Configuration screen [442](#)
cluster manager [441](#)
CNC
 portal [530](#)
Common and Internal Spanning Tree, see CIST [273](#)
Config 1 [456](#)
Config 2 [456](#)
configuration [334](#)

 back up [32](#)
 change running config [455](#), [523](#)
 saving [79](#)
configuration file
 backup [446](#), [521](#)
 restore [446](#), [520](#)
 save [450](#)
Configure Clone screen [450](#)
contact information [532](#)
copying port settings, see port cloning
copyright [561](#)
CoS [238](#)
CPU protection [389](#)
Current Configuration [523](#)
current date [134](#), [476](#)
current time [134](#), [476](#)
Custom Default [456](#), [524](#)
customer support [532](#)

D

date
 current [134](#), [476](#)
daylight saving time [134](#), [476](#)
DDMI Details screen [120](#)
DDMI screen [119](#)
debug port [40](#)
default gateway [330](#)
default IP address
 management port [40](#)
device back label
 Switch [29](#)
DHCP [317](#)
 client IP pool [330](#)
 configuration options [318](#)
 modes [317](#)
 Relay Agent Information format [319](#)
DHCP (Dynamic Host Configuration Protocol) [317](#)
DHCP Option 82 Profile screen [320](#)
DHCP relay
 configure [91](#)
 tutorial [88](#)
DHCP relay agent [543](#)
DHCP relay option 82 [410](#)

DHCP server
 block [400](#)

DHCP Server Status screen [327](#)

DHCP snooping [395, 400, 409](#)
 configure [410](#)
 DHCP relay option 82 [410](#)
 trusted ports [409](#)
 untrusted ports [409](#)

DHCP snooping database [410](#)

DHCP Status screen [318](#)

DHCP Unique IDentifier (DUID) [542](#)

DHCPv4
 global relay [322](#)
 global relay example [323](#)
 Option 82 [319](#)
 option 82 profiles [320](#)
 Relay Agent Information [319](#)

DHCPv4 relay [318](#)

DHCPv6
 enable in Windows 10 [546](#)

diagnostics
 ping [453](#)

Differentiated Service (DiffServ) [238](#)

DiffServ [238](#)
 activate [239, 494](#)
 DS field [238](#)
 DSCP [238, 494](#)
 network example [239](#)
 PHB [238](#)
 service level [238](#)

DiffServ Code Points [238, 494](#)

Digital Diagnostics Monitoring Interface [119](#)

disclaimer [561](#)

disposal and recycling information
 EU [563](#)

double-tagged frames [301](#)

DS (Differentiated Services) [238](#)

DSCP [238, 494](#)
 what it does [238](#)

dual firmware images [454, 522](#)

dust plug [39](#)

Dynamic Host Configuration Protocol for IPv6
 (DHCPv6) [542](#)

dynamic link aggregation [172](#)

E

electrical inspection authority [42](#)

electrician [42](#)

electrostatic discharge (ESD) [38](#)

EMC statement [561](#)

Environment Statement [563](#)

Errdisable Detect screen [392](#)

Errdisable Recovery screen [393](#)

errdisable status [391](#)

error disable [389](#)
 control packets [391](#)
 CPU protection [391](#)
 detect [392](#)
 recovery [393](#)
 status [390](#)

error-disable recovery [389](#)

Ethernet broadcast address [105, 311](#)

Ethernet MAC [126, 470](#)

external authentication server [339](#)

F

Factory Default [456, 524](#)

FaOS [439](#)

FCC interference statement [561](#)

fiber cable
 connecting [39](#)
 removal [40](#)

file transfer using FTP
 command example [439](#)

filename convention, configuration
 file names [439](#)

filtering [274](#)
 rules [274](#)

filtering database, MAC table [109](#)

Filtering screen [274](#)

firmware [470](#)
 upgrade [445, 454, 522](#)
 ZyNOS [126](#)

Firmware Upgrade screen [454, 522](#)

forwarding
 delay [268](#)

frames

- tagged [287, 515](#)
- untagged [287, 515](#)

- freestanding installation
 - precautions [34](#)

- front panel [37](#)

- FTP [438](#)

- file transfer procedure [439](#)
 - restrictions over WAN [440](#)

G

- GARP (Generic Attribute Registration Protocol) [279, 509](#)

- GARP timer [160, 279, 509](#)

- general setup [133](#)

- General Setup screen [133, 474](#)

- getting help [81](#)

- GMT (Greenwich Mean Time) [134, 476](#)

- gratuitous ARP [312](#)

- grounding
 - for safety [41](#)

- GVRP [509](#)

- GVRP (GARP VLAN Registration Protocol) [279, 509](#)

H

- hardware installation [33](#)

- hardware monitor [127, 471](#)

- hardware overview [37](#)

- hello time [268](#)

- hops [268](#)

- HTTPS [358](#)

- certificates [358](#)
 - implementation [358](#)
 - public keys, private keys [358](#)

- HTTPS Certificates screen [438](#)

- HTTPS example [358](#)

I

- IANA (Internet Assigned Number Authority) [537](#)

- Identity Association (IA) [542](#)

- IEEE 802.1x

- activate [422](#)

- re-authentication [423](#)

- IGMP filtering [214](#)

- profile [222, 223, 504, 505](#)

- profiles [218](#)

- IGMP leave timeout

- fast [220, 501](#)

- normal [220, 501](#)

- IGMP snooping [214](#)

- MVR [215](#)

- IGMP snooping and VLANs [214](#)

- IGMP throttling [220, 502](#)

- initial setup [82](#)

- Innovation, Science and Economic Development
Canada ICES statement [561](#)

- installation

- air circulation [33](#)

- desktop [33](#)

- freestanding [33](#)

- rack-mounting [34](#)

- transceiver [38](#)

- Internet Protocol version 6, see IPv6

- IP

- configuration [140](#)

- interface [137](#)

- routing domain [137](#)

- status [138](#)

- IP address [139](#)

- Switch management [82, 84, 86](#)

- IP Setup screen [137](#)

- IP source guard [395](#)

- ARP inspection [395, 418](#)

- DHCP snooping [395](#)

- static bindings [395](#)

- IP Status Detail screen [138](#)

- IP subnet mask [139](#)

- IP table [107](#)

- how it works [107](#)

- IPv6 [540](#)

- addressing [540](#)

- enable in Windows 10 [546](#)

- enable in Windows 7 [545](#)

- EUI-64 [542](#)

- global address [540](#)

- interface ID [542](#)

- link-local address [540](#)
- Neighbor Discovery Protocol [540](#)
- ping [540](#)
- prefix [540](#)
- prefix length [540](#)
- unspecified address [541](#)

IPv6 cache [544](#)

J

Java permission [49, 529](#)

JavaScript [49, 529](#)

L

LACP [172](#)

- system priority [177, 491](#)
- timeout [178, 492](#)

LED behavior

- CLOUD [29](#)

LED description [29, 46](#)

LEDs [46](#)

limit MAC address learning [434](#)

link aggregation [65, 172](#)

- dynamic [172](#)
- ID information [173](#)
- setup [175, 489](#)
- traffic distribution algorithm [174, 488](#)
- traffic distribution type [176, 490](#)
- trunk group [172](#)

link aggregation (trunking) [489](#)

Link Aggregation Control Protocol (LACP) [172](#)

Link Aggregation Setting screen [489](#)

Link Aggregation Status screen [487](#)

Link Layer Discovery Protocol [180](#)

LLDP [180](#)

- basic TLV [194](#)
- global settings [192](#)
- local port status [184](#)
- organization-specific TLV [195](#)
- status of remote device [188](#)
- TLV [180](#)

LLDP (Link Layer Discovery Protocol) [180](#)

LLDP-MED [181](#)

- classes of endpoint devices [181](#)
- example [181](#)

LLDP-MED Location screen [198](#)

LLDP-MED Setup screen [196](#)

local port mirroring [210](#)

lockout [79](#)

- Switch [79](#)

log message [129](#)

login [49](#)

- privilege level [146, 480](#)

login account

- administrator [145, 478](#)
- non-administrator [145, 478](#)

login accounts [145, 478](#)

- configuring through Web Configurator [145, 478](#)
- multiple [145, 478](#)
- number of [145, 478](#)

login password

- edit [146, 479](#)

login user name

- display [355](#)

Logins screen [145, 478](#)

loop guard [207](#)

- examples [208](#)
- port shut down [208](#)
- setup [208](#)
- vs. STP [207](#)

M

MAC (Media Access Control) [126, 470](#)

MAC address [105, 126, 470](#)

- maximum number per port [434](#)

MAC address learning [160, 434](#)

- specify limit [434](#)

MAC Based VLAN screen [295](#)

MAC filter

- and ARP inspection [419](#)

MAC freeze [433](#)

MAC table [109](#)

- display criteria [111](#)
- how it works [109](#)
- sorting criteria [111](#)
- viewing [110](#)

MAC-based VLAN [294](#)

- maintenance
 - configuration backup [446, 521](#)
 - firmware [454, 522](#)
 - restore configuration [446, 520](#)
- Management Information Base (MIB) [154, 481](#)
- management IP address [82, 84, 86](#)
- management mode [27](#)
- management port [40](#)
 - default IP address [40](#)
- managing the device
 - using the command line interface, see command line interface [27](#)
- managing the Switch
 - cluster management [27](#)
 - good habits [32](#)
 - NCC [27](#)
 - using FTP, see FTP [27](#)
 - using SNMP [27](#)
 - Web Configurator [27](#)
 - ZON Utility [27](#)
- man-in-the-middle attacks [418](#)
- max
 - age [268](#)
 - hops [268](#)
- Mbuf (Memory Buffer) [464](#)
- Media Access Control [126, 470](#)
- Memory Buffer [464](#)
- MGMT (management) port [40](#)
- MIB
 - and SNMP [154, 481](#)
 - supported MIBs [154](#)
- MIB (Management Information Base) [154, 481](#)
- mirroring ports [210](#)
- monitor port [211, 496](#)
- mounting brackets
 - attaching [34](#)
- MST Instance, see MSTI [272](#)
- MST region [272](#)
- MSTI [272](#)
- MSTP
 - bridge ID [266](#)
 - configuration [267](#)
 - configuration digest [266](#)
 - forwarding delay [268](#)
 - Hello Time [266](#)
 - hello time [268](#)
 - Max Age [266](#)

- max age [268](#)
 - max hops [268](#)
 - path cost [270](#)
 - port priority [270](#)
 - revision level [269](#)
 - status [265](#)
- MTU (Multi-Tenant Unit) [159](#)
- multicast
 - 802.1 priority [218](#)
 - IGMP throttling [220, 502](#)
 - IP addresses [213](#)
 - setup [218](#)
- multicast group [222, 223, 504, 505](#)
- multicast IP address [231](#)
- multicast MAC address [231](#)
- Multi-Tenant Unit [159](#)
- MVR [215](#)
 - configuration [225](#)
 - network example [215](#)
- MVR (Multicast VLAN Registration) [215](#)

N

- Nebula Cloud Management [28](#)
 - switching to [29](#)
- Nebula web portal [28, 29](#)
 - access in three ways [29](#)
- Neighbor Details [113](#)
- Neighbor Discovery Protocol (NDP) [543](#)
- Neighbor screen [112](#)
- network applications [24](#)
- network element (NE) [480](#)
- network management system (NMS) [153, 480](#)
- Networked AV mode [32, 466](#)
 - overview [466](#)
- Networked AV screen
 - Wizard [62, 67](#)
- NTP (RFC-1305) [134, 475](#)

O

- Option 82 [319](#)
- organization

- create [29](#)
- Org-specific TLV Setting screen [195](#)
- overheating
 - prevention [33](#)

P

- password
 - administrator [146, 479](#)
 - change [32](#)
 - change through Wizard [61, 66](#)
 - display [355](#)
 - write down [32](#)
- password encryption
 - activate [356](#)
- Per-Hop Behavior [238](#)
- PHB [238](#)
- ping, test connection [453](#)
- policy [308, 309, 373, 374](#)
 - and classifier [308, 309, 373, 374](#)
 - and DiffServ [372](#)
 - configuration [308, 309, 373, 374](#)
 - example [376](#)
 - overview [372](#)
 - rules [372, 373](#)
- port
 - setup [202, 492](#)
 - speed/duplex [203](#)
- port authentication [420](#)
 - guest VLAN [425](#)
 - IEEE802.1x [422](#)
 - MAC authentication [423](#)
 - method [422](#)
- port cloning [450, 451](#)
 - advanced settings [450, 451](#)
 - basic settings [450, 451](#)
- port details [117](#)
- port mirroring [210](#)
- port redundancy [172](#)
- Port screen
 - DHCPv4 Global Relay [323](#)
- port security [432](#)
 - address learning [434](#)
 - limit MAC address learning [434](#)
 - setup [432, 434](#)

- Port Setup screen [202, 492](#)
- port status
 - port details [117](#)
 - port utilization [121](#)
- port utilization [121](#)
- Port VID (PVID) [85](#)
- port VLAN ID, see PVID [287, 515](#)
- port VLAN trunking [280, 509](#)
- ports
 - diagnostics [453](#)
 - mirroring [210](#)
 - speed/duplex [493](#)
 - standby [173](#)
- power
 - voltage [127, 471](#)
- power connections [44](#)
- power connector [44](#)
- power status [127, 471](#)
- prefix delegation [543](#)
- product registration [565](#)
- protocol based VLAN
 - example [294](#)
- PVID [279, 508](#)

Q

- QoS [238](#)
 - and classifier [362](#)
- QR code
 - Switch [29](#)
 - where to find [29](#)
- Quality of Service [238](#)
- queue weight [243](#)
- queuing [242, 243](#)
 - SPQ [242](#)
 - WRR [242](#)
- queuing method [242, 244](#)
- Quick Start Guide
 - steps for registering the Switch [29](#)

R

- rack-mount [37](#)

- rack-mounting [34](#)
 - installation requirements [34](#)
 - precautions [34](#)
- RADIUS [339, 352](#)
 - advantages [339](#)
 - setup [339](#)
- Rapid Spanning Tree Protocol (RSTP) [251](#)
- rear panel [40](#)
- reboot
 - load configuration [455, 523](#)
- reboot system [455, 523](#)
- reflector port [210](#)
- registration
 - product [565](#)
- Registration MAC address [29](#)
- Regulatory Notice and Statement [561](#)
- remote management [353, 517](#)
 - service [354, 518](#)
 - trusted computers [354, 518](#)
- Remote Management screen [517](#)
- remote port mirroring [210](#)
- RESET button [80](#)
- resetting [80, 449](#)
 - to factory default settings [449](#)
- restore
 - configuration [32](#)
- restore configuration [80, 446, 520](#)
- RFC 3164 [162](#)
- RMirror [210](#)
- Round Robin Scheduling [242](#)
- Router Advertisement (RA) [543](#)
- routing domain [137](#)
- RSTP
 - configuration [258](#)
- rubber feet
 - attach [33](#)
- running configuration [449](#)
 - erase [449](#)
 - reset [449](#)

S

- safety precautions
 - using the Switch [33](#)

- safety warnings [562](#)
- save configuration [79, 450](#)
- Save link [79](#)
- schedule
 - type [166](#)
- Secure Shell, see SSH
- serial number
 - Switch [29](#)
- service access control [352, 516](#)
 - service port [353, 516](#)
- Service Access Control screen [516](#)
- Setup Wizard
 - parts [59](#)
- Setup Wizard screen [54](#)
- sFlow [247](#)
 - configuration [247](#)
 - datagram [247](#)
 - overview [247](#)
 - poll interval [248](#)
 - sample rate [248](#)
 - UDP port [250](#)
- sFlow agent [247](#)
- sFlow collector [247](#)
- SFP/SFP+ slot [38](#)
- Simple Network Management Protocol (SNMP) [480](#)
- Simple Network Management Protocol, see SNMP
- site
 - create [29](#)
- Small Form-factor Pluggable (SFP) [38](#)
- SNMP [153](#)
 - agent [153, 480](#)
 - and MIB [154, 481](#)
 - authentication [149, 150, 483, 484](#)
 - communities [148, 482](#)
 - management model [153, 480](#)
 - manager [154, 480](#)
 - MIB [154](#)
 - network components [153, 480](#)
 - object variables [154, 481](#)
 - protocol operations [154, 481](#)
 - security [150, 484](#)
 - security level [149, 483](#)
 - settings [480](#)
 - setup [147, 480](#)
 - traps [151, 484](#)
 - users [149, 150, 482](#)
 - version 3 and security [154, 481](#)

- versions supported [153, 480](#)
- SNMP agent
 - enable through Wizard [61, 66](#)
- SNMP screen [481](#)
- SNMP traps [154](#)
 - supported [155, 156, 158](#)
- SNMP version
 - select [62, 67](#)
- SPQ (Strict Priority Queuing) [242](#)
- SSH
 - encryption methods [357](#)
 - how it works [356](#)
 - implementation [357](#)
- SSH (Secure Shell) [356](#)
- SSH Authorized Keys screen [456](#)
- SSL (Secure Socket Layer) [358](#)
- Standalone mode
 - switch to [31](#)
- standby ports [173](#)
- static bindings [395](#)
- static MAC address [276](#)
- static MAC forwarding [276](#)
- Static MAC Forwarding screen [276, 277](#)
- static multicast forwarding [231](#)
- static route [334](#)
 - enable [336](#)
 - metric [336](#)
 - overview [334](#)
- static VLAN [284, 511](#)
 - control [286, 514](#)
 - tagging [286, 514](#)
- status [70](#)
 - MSTP [265](#)
 - power [127, 471](#)
 - STP [256](#)
 - VLAN [281, 510](#)
- Storm Control screen [519](#)
- STP
 - bridge ID [257, 261](#)
 - bridge priority [259, 263](#)
 - designated bridge [252](#)
 - edge port [260, 264](#)
 - forwarding delay [260](#)
 - Hello BPDU [252](#)
 - Hello Time [257, 259, 261, 263](#)
 - how it works [252](#)

- Max Age [257, 259, 261, 264](#)
- path cost [252, 260, 264](#)
- port priority [260, 264](#)
- port role [258, 262](#)
- port state [252, 258, 262](#)
- root port [252](#)
- status [254, 256](#)
- terminology [252](#)
- vs. loop guard [207](#)
- STP Path Cost [252](#)
- subnet based VLANs [289](#)
- subnet masking [542](#)
- Summary screen [466](#)
- Switch
 - DHCP client [49](#)
 - fanless-type usage precaution [33](#)
 - fan-type usage precaution [33](#)
- switch lockdown [79](#)
- Switch reset [80](#)
- syslog [162, 419](#)
 - protocol [162](#)
 - settings [162](#)
 - setup [162](#)
 - severity levels [162](#)
- Syslog Setup screen [162](#)
- System Info screen [125, 469](#)
- system reboot [455, 523](#)

T

- TACACS+ [339, 352](#)
 - advantages [339](#)
 - setup [341](#)
- tag-based VLAN
 - example [26](#)
- tagged VLAN [278, 508](#)
- Tech-Support [463, 524](#)
 - log enhancement [463, 524](#)
- Tech-Support screen [464, 524](#)
- temperature indicator [127, 471](#)
- time
 - current [134, 476](#)
 - daylight saving [134, 476](#)
 - format [134, 475](#)
- Time (RFC-868) [134, 475](#)

- time server [134, 475](#)
- time service protocol [134, 475](#)
- ToS [238](#)
- trademarks [565](#)
- traffic distribution criteria [173](#)
- transceiver
 - connection interface [38](#)
 - connection speed [38](#)
 - installation [38](#)
 - removal [39](#)
- transceiver MultiSource Agreement (MSA) [38](#)
- transceivers [38](#)
- traps
 - destination [148, 482](#)
- troubleshooting [91](#)
- trunk group [172](#)
- trunking [172](#)
- trusted ports
 - ARP inspection [419](#)
 - DHCP snooping [409](#)
- Type of Service [238](#)
- Type Transfer [111](#)

U

- unregister
 - Switch [31](#)
- untrusted ports
 - ARP inspection [419](#)
 - DHCP snooping [409](#)
- user name [52](#)
 - default [52](#)
- user profiles [339](#)
- UTC (Universal Time Coordinated) [134, 476](#)

V

- Vendor Specific Attribute, see VSA [346](#)
- ventilation holes [33](#)
- VID [143, 282, 283, 303, 477, 478, 510, 511](#)
 - number of possible VIDs [279, 508](#)
 - priority frame [279, 508](#)
- VID (VLAN Identifier) [279, 508](#)

- Virtual Local Area Network [159](#)
- VLAN [159](#)
 - acceptable frame type [287, 515](#)
 - and IGMP snooping [214](#)
 - automatic registration [279, 508](#)
 - creation [84, 89](#)
 - ID [278, 508](#)
 - ingress filtering [287, 515](#)
 - introduction [159, 278, 508](#)
 - number of VLANs [282, 510](#)
 - port number [283, 511](#)
 - port settings [286, 288, 514](#)
 - PVID [287, 515](#)
 - static VLAN [284, 511](#)
 - status [281, 282, 283, 510, 511](#)
 - subnet based [289](#)
 - tagged [278, 508](#)
 - terminology [280, 509](#)
 - trunking [280, 287, 509, 515](#)
 - type [160, 280](#)
- VLAN (Virtual Local Area Network) [159](#)
- VLAN ID [278, 508](#)
- VLAN mapping [297](#)
 - activating [298](#)
 - configuration [298, 299](#)
 - example [297](#)
 - priority level [297](#)
 - tagged [297](#)
 - traffic flow [297](#)
 - untagged [297](#)
 - VLAN ID [297](#)
- VLAN number [139, 143, 477, 478](#)
- VLAN Setting screen
 - DHCPv4 [326, 329](#)
- VLAN stacking [301](#)
 - configuration [304](#)
 - example [301](#)
 - frame format [303](#)
 - port roles [304](#)
 - port-based Q-in-Q [305](#)
 - priority [303](#)
 - selective Q-in-Q [306](#)
- VLAN terminology [280, 509](#)
- VLAN trunking [287, 515](#)
- VLAN-unaware devices [85](#)
- VSA [346](#)

W

- warranty
 - note [565](#)
- Web browser pop-up window [49, 529](#)
- Web Configurator
 - getting help [81](#)
 - home [70](#)
 - login [49](#)
 - logout [81](#)
 - navigating components [70](#)
 - navigation panel [72](#)
 - online help [81](#)
 - usage prerequisite [49](#)
- weight [243](#)
- Wizard
 - link aggregation [65](#)
- WRR (Weighted Round Robin Scheduling) [242](#)

Z

- ZDP [56](#)
- ZON Utility [56](#)
 - compatible OS [56](#)
 - fields description [58](#)
 - icon description [58](#)
 - installation requirements [56](#)
 - introduction [31](#)
 - minimum hardware requirements [56](#)
 - network adapter select [56](#)
 - password prompt [58](#)
 - run [56](#)
 - supported firmware version [59](#)
 - supported models [59](#)
 - Switch IP address [49](#)
- ZON utility
 - use for troubleshooting [528](#)
- Zyxel Account
 - sign up [29](#)
- Zyxel Account information
 - enter [29](#)
- Zyxel AP Configurator (ZAC) [58](#)
- Zyxel Discovery Protocol (ZDP) [56](#)
- Zyxel Nebula Mobile app [29](#)
- Zyxel One Network (ZON) Utility [31](#)