

User's Guide

XS1930 Series

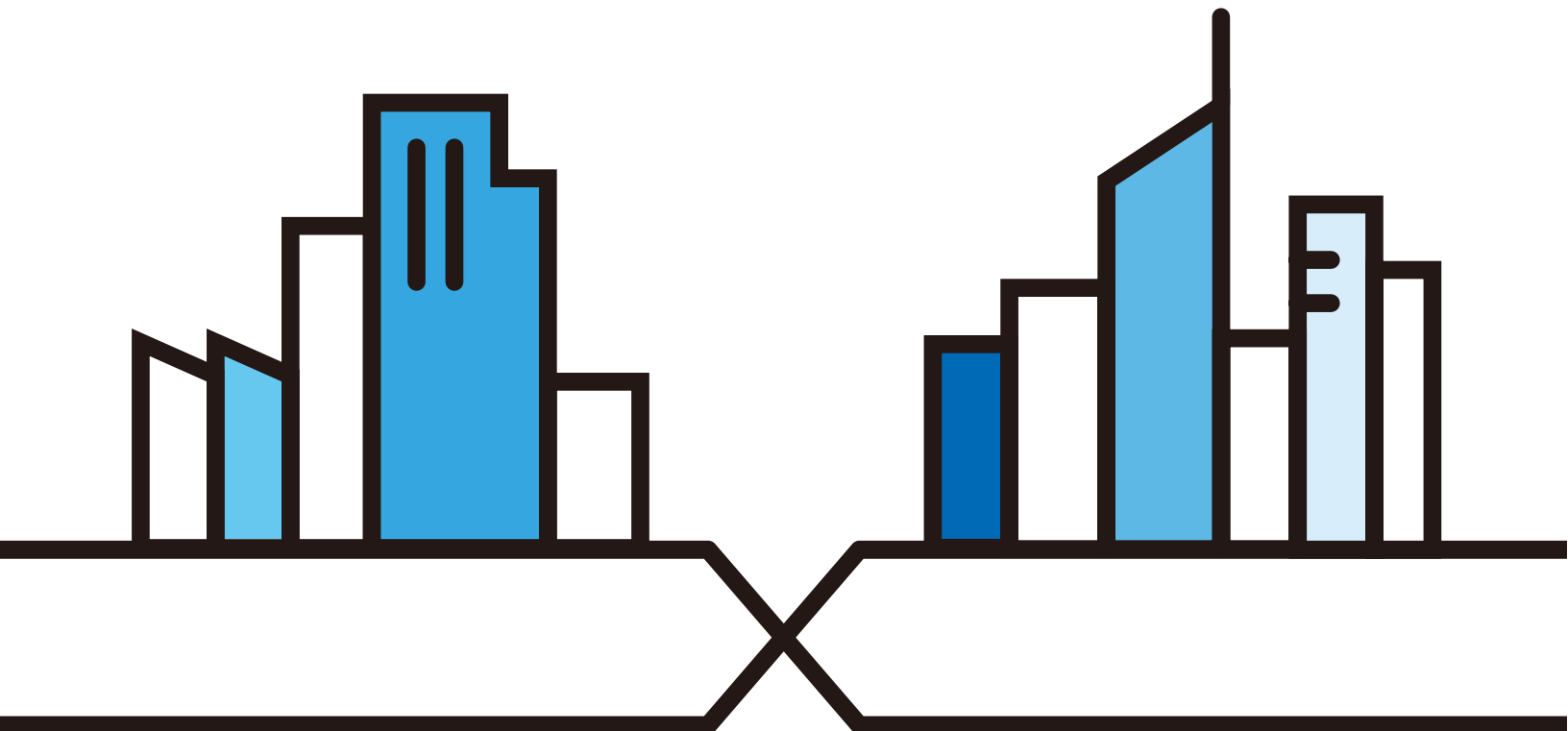
10-port Multi-Gigabit Smart Managed L2 Switch

12-port Multi-Gigabit Smart Managed L2 PoE Switch

Default Login Details

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

Version 4.60 Edition 1, 12/2019



IMPORTANT!

READ CAREFULLY BEFORE USE

KEEP THIS GUIDE FOR FUTURE REFERENCE

This is a User's Guide for a series of products. Not all products support all firmware features. Screenshots and graphics in this book may differ slightly from your product due to differences in your product firmware or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Related Documentation

- Quick Start Guide

The Quick Start Guide shows how to connect the Switch.

- 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://businessforum.zyxel.com> for product discussions.

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



Contents Overview

User's Guide	17
Getting to Know Your Switch	18
Hardware Installation and Connection	27
Hardware Panels	31
Technical Reference	38
The Web Configurator	39
Initial Setup Example	64
DHCP Relay Tutorial	68
Status	73
Basic Setting	79
VLAN	114
Static MAC Forward Setup	129
Static Multicast Forwarding	131
Filtering	135
Spanning Tree Protocol	137
Bandwidth Control	154
Broadcast Storm Control	156
Mirroring	158
Link Aggregation	160
Port Authentication	167
Port Security	175
Time Range	177
Classifier	179
Policy Rule	188
Queuing Method	192
Multicast	195
AAA	203
Loop Guard	211
Layer 2 Protocol Tunneling	214
PPPoE	218
Error Disable	226
Green Ethernet	233
Link Layer Discovery Protocol (LLDP)	235
Static Route	258
DHCP	262
ARP Setup	275
Maintenance	280

Access Control	293
Diagnostic	313
System Log	316
Syslog Setup	317
Cluster Management	320
MAC Table	326
IP Table	329
ARP Table	331
Routing Table	333
Path MTU Table	335
Configure Clone	336
IPv6 Neighbor Table	339
Port Status	341
Troubleshooting	348

Table of Contents

Contents Overview	3
Table of Contents.....	5
 Part I: User's Guide.....	 17
 Chapter 1	
Getting to Know Your Switch	18
1.1 Introduction	18
1.1.1 Multi-Gigabit	18
1.1.2 Management Modes	19
1.1.3 Mode Changing	20
1.1.4 ZON Utility	22
1.1.5 PoE	22
1.2 Example Applications	22
1.2.1 PoE Example Application	22
1.2.2 Backbone Example Application	23
1.2.3 Bridging / Fiber Uplink Example Application	24
1.2.4 High Performance Switching Example	24
1.2.5 IEEE 802.1Q VLAN Application Examples	25
1.3 Ways to Manage the Switch	25
1.4 Good Habits for Managing the Switch	26
 Chapter 2	
Hardware Installation and Connection	27
2.1 Installation Scenarios	27
2.2 Desktop Installation Procedure	27
2.3 Mounting the Switch on a Rack	28
2.3.1 Rack-mounted Installation Requirements	28
2.3.2 Attaching the Mounting Brackets to the Switch	29
2.3.3 Mounting the Switch on a Rack	29
 Chapter 3	
Hardware Panels.....	31
3.1 Front Panel	31
3.1.1 Ethernet Ports	32
3.1.2 PoE (XS1930-12HP)	32
3.1.3 SFP/SFP+ Slots	32

3.2 Rear Panel	34
3.2.1 Grounding	34
3.2.2 Power Connector	35
3.3 LEDs	35
 Part II: Technical Reference	38
 Chapter 4	
The Web Configurator.....	39
4.1 Overview	39
4.2 System Login	39
4.3 Zyxel One Network (ZON) Utility	44
4.3.1 Requirements	44
4.3.2 Run the ZON Utility	44
4.4 Wizard	48
4.4.1 Basic	48
4.4.2 Protection	53
4.4.3 VLAN	55
4.4.4 QoS	56
4.5 The Web Configurator Layout	57
4.5.1 Change Your Password	61
4.6 Saving Your Configuration	62
4.7 Switch Lockout	62
4.8 Resetting the Switch	62
4.8.1 The Restore Button	62
4.9 Logging Out of the Web Configurator	63
4.10 Help	63
 Chapter 5	
Initial Setup Example	64
5.1 Overview	64
5.1.1 Creating a VLAN	64
5.1.2 Setting Port VID	65
5.2 Configuring Switch Management IP Address	66
 Chapter 6	
DHCP Relay Tutorial	68
6.1 Overview	68
6.2 How to Use DHCPv4 Relay on the Switch	68
6.2.1 DHCP Relay Tutorial Introduction	68
6.2.2 Creating a VLAN	68

6.2.3 Configuring DHCPv4 Relay	71
6.2.4 Troubleshooting	72
Chapter 7	
Status.....	73
7.1 Overview	73
7.1.1 What You Can Do	73
7.2 Status	73
7.2.1 Neighbor Screen	75
7.2.2 Neighbor Detail	77
Chapter 8	
Basic Setting	79
8.1 Overview	79
8.1.1 What You Can Do	79
8.2 System Information	79
8.3 General Setup	81
8.4 Introduction to VLANs	83
8.5 Switch Setup	84
8.6 IP Setup	85
8.6.1 Management IP Addresses (IP Interfaces)	85
8.6.2 IP Status Details	86
8.6.3 IP Configuration	87
8.7 Port Setup	89
8.8 PoE Setup	90
8.8.1 PoE Time Range Setup	93
8.8.2 PoE Setup	94
8.9 Interface Setup	97
8.10 IPv6	98
8.10.1 IPv6 Interface Status	98
8.10.2 IPv6 Configuration	100
8.10.3 IPv6 Global Setup	101
8.10.4 IPv6 Interface Setup	102
8.10.5 IPv6 Link-Local Address Setup	103
8.10.6 IPv6 Global Address Setup	104
8.10.7 IPv6 Neighbor Discovery Setup	105
8.10.8 IPv6 Router Discovery Setup	106
8.10.9 IPv6 Prefix Setup	107
8.10.10 IPv6 Neighbor Setup	108
8.10.11 DHCPv6 Client Setup	110
8.11 DNS	111
8.12 Cloud Management	112
8.12.1 Nebula Control Center Discovery	112

8.12.2 Nebula Switch Registration	113
Chapter 9	
VLAN.....	114
9.1 Overview	114
9.1.1 What You Can Do	114
9.1.2 What You Need to Know	114
9.2 VLAN Status	117
9.2.1 VLAN Detail	118
9.3 VLAN Configuration	119
9.4 Configure a Static VLAN	119
9.5 Configure VLAN Port Setting	121
9.6 Voice VLAN Setup	122
9.7 Vendor ID Based VLAN	124
9.8 Port-Based VLAN Setup	126
9.8.1 Configure a Port-Based VLAN	126
Chapter 10	
Static MAC Forward Setup	129
10.1 Overview	129
10.1.1 What You Can Do	129
10.2 Configuring Static MAC Forwarding	129
Chapter 11	
Static Multicast Forwarding	131
11.1 Static Multicast Forward Setup Overview	131
11.1.1 What You Can Do	131
11.1.2 What You Need To Know	131
11.2 Configuring Static Multicast Forwarding	132
Chapter 12	
Filtering	135
12.1 Filtering Overview	135
12.1.1 What You Can Do	135
12.2 Configure a Filtering Rule	135
Chapter 13	
Spanning Tree Protocol	137
13.1 Spanning Tree Protocol Overview	137
13.1.1 What You Can Do	137
13.1.2 What You Need to Know	137
13.2 Spanning Tree Protocol Status Screen	139
13.3 Spanning Tree Configuration	140

13.4 Configure Rapid Spanning Tree Protocol	140
13.5 Rapid Spanning Tree Protocol Status	142
13.6 Configure Multiple Spanning Tree Protocol	144
13.6.1 Multiple Spanning Tree Protocol Port Configuration	147
13.7 Multiple Spanning Tree Protocol Status	148
13.8 Technical Reference	151
13.8.1 MSTP Network Example	151
13.8.2 MST Region	152
13.8.3 MST Instance	152
13.8.4 Common and Internal Spanning Tree (CIST)	152
Chapter 14	
Bandwidth Control	154
14.1 Bandwidth Control Overview	154
14.1.1 What You Can Do	154
14.2 Bandwidth Control Setup	154
Chapter 15	
Broadcast Storm Control	156
15.1 Broadcast Storm Control Overview	156
15.1.1 What You Can Do	156
15.2 Broadcast Storm Control Setup	156
Chapter 16	
Mirroring	158
16.1 Mirroring Overview	158
16.1.1 What You Can Do	158
16.2 Port Mirroring Setup	158
Chapter 17	
Link Aggregation	160
17.1 Link Aggregation Overview	160
17.1.1 What You Can Do	160
17.1.2 What You Need to Know	160
17.2 Link Aggregation Status	161
17.3 Link Aggregation Setting	162
17.3.1 Link Aggregation Control Protocol	164
17.4 Technical Reference	165
17.4.1 Static Trunking Example	165
Chapter 18	
Port Authentication	167
18.1 Port Authentication Overview	167

18.1.1 What You Can Do	167
18.1.2 What You Need to Know	167
18.1.3 MAC Authentication	168
18.2 Port Authentication Configuration	169
18.3 Activate IEEE 802.1x Security	169
18.3.1 Guest VLAN	170
18.4 Activate MAC Authentication	172
Chapter 19	
Port Security	175
19.1 Port Security Overview	175
19.1.1 What You Can Do	175
19.2 Port Security Setup	175
Chapter 20	
Time Range	177
20.1 Time Range Overview	177
20.1.1 What You Can Do	177
20.2 Configuring Time Range	177
Chapter 21	
Classifier	179
21.1 Classifier Overview	179
21.1.1 What You Can Do	179
21.1.2 What You Need to Know	179
21.2 Classifier Status	179
21.3 Classifier Configuration	180
21.3.1 Viewing and Editing Classifier Configuration Summary	184
21.4 Classifier Global Setting Configuration	185
21.5 Classifier Example	186
Chapter 22	
Policy Rule	188
22.1 Policy Rules Overview	188
22.1.1 What You Can Do	188
22.2 Configuring Policy Rules	188
22.3 Policy Example	191
Chapter 23	
Queuing Method	192
23.1 Queuing Method Overview	192
23.1.1 What You Can Do	192
23.1.2 What You Need to Know	192

23.2 Configuring Queuing	193
Chapter 24	
Multicast.....	195
24.1 Multicast Overview	195
24.1.1 What You Can Do	195
24.1.2 What You Need to Know	195
24.2 Multicast Setup	196
24.3 IPv4 Multicast Status	196
24.3.1 IGMP Snooping	197
24.3.2 IGMP Snooping VLAN	200
24.3.3 IGMP Filtering Profile	201
Chapter 25	
AAA	203
25.1 AAA Overview	203
25.1.1 What You Can Do	203
25.1.2 What You Need to Know	204
25.2 AAA Screens	204
25.3 RADIUS Server Setup	204
25.4 AAA Setup	206
25.5 Technical Reference	208
25.5.1 Vendor Specific Attribute	208
25.5.2 Supported RADIUS Attributes	209
25.5.3 Attributes Used for Authentication	209
Chapter 26	
Loop Guard	211
26.1 Loop Guard Overview	211
26.1.1 What You Can Do	211
26.1.2 What You Need to Know	211
26.2 Loop Guard Setup	213
Chapter 27	
Layer 2 Protocol Tunneling	214
27.1 Layer 2 Protocol Tunneling Overview	214
27.1.1 What You Can Do	214
27.1.2 What You Need to Know	214
27.2 Configuring Layer 2 Protocol Tunneling	215
Chapter 28	
PPPoE.....	218
28.1 PPPoE Intermediate Agent Overview	218

28.1.1 What You Can Do	218
28.1.2 What You Need to Know	218
28.2 PPPoE Screen	220
28.3 PPPoE Intermediate Agent	221
28.3.1 PPPoE IA Per-Port	222
28.3.2 PPPoE IA Per-Port Per-VLAN	223
28.3.3 PPPoE IA for VLAN	224
Chapter 29	
Error Disable	226
29.1 Error Disable Overview	226
29.1.1 CPU Protection Overview	226
29.1.2 Error-Disable Recovery Overview	226
29.1.3 What You Can Do	226
29.2 Error Disable Screen	227
29.3 Error-Disable Status	227
29.4 CPU Protection Configuration	229
29.5 Error-Disable Detect Configuration	230
29.6 Error-Disable Recovery Configuration	231
Chapter 30	
Green Ethernet	233
30.1 Green Ethernet Overview	233
30.2 Configuring Green Ethernet	233
Chapter 31	
Link Layer Discovery Protocol (LLDP)	235
31.1 LLDP Overview	235
31.2 LLDP-MED Overview	236
31.3 LLDP Screens	237
31.4 LLDP Local Status	238
31.4.1 LLDP Local Port Status Detail	239
31.5 LLDP Remote Status	242
31.5.1 LLDP Remote Port Status Detail	243
31.6 LLDP Configuration	249
31.6.1 Basic TLV Setting	250
31.6.2 Org-specific TLV Setting	251
31.7 LLDP-MED Configuration	252
31.8 LLDP-MED Network Policy	253
31.9 LLDP-MED Location	254
Chapter 32	
Static Route	258

32.1 Static Routing Overview	258
32.1.1 What You Can Do	258
32.2 Static Routing	259
32.3 IPv4 Static Route	259
32.4 IPv6 Static Route	260
 Chapter 33	
DHCP	262
33.1 DHCP Overview	262
33.1.1 What You Can Do	262
33.1.2 What You Need to Know	262
33.2 DHCP Configuration	263
33.3 DHCPv4 Status	263
33.4 DHCPv4 Relay	264
33.4.1 DHCPv4 Relay Agent Information	264
33.4.2 DHCPv4 Option 82 Profile	265
33.4.3 Configuring DHCPv4 Global Relay	266
33.4.4 DHCPv4 Global Relay Port Configure	267
33.4.5 Global DHCP Relay Configuration Example	268
33.4.6 Configuring DHCP VLAN Settings	269
33.4.7 DHCPv4 VLAN Port Configure	271
33.4.8 Example: DHCP Relay for Two VLANs	272
33.5 DHCPv6 Relay	273
 Chapter 34	
ARP Setup	275
34.1 ARP Overview	275
34.1.1 What You Can Do	275
34.1.2 What You Need to Know	275
34.2 ARP Setup	277
34.2.1 ARP Learning	277
34.2.2 Static ARP	278
 Chapter 35	
Maintenance	280
35.1 Overview	280
35.1.1 What You Can Do	280
35.2 The Maintenance Screen	280
35.3 Erase Running-Configuration	282
35.4 Save Configuration	282
35.5 Reboot System	283
35.5.1 Factory Default	283
35.5.2 Custom Default	284

35.6 Firmware Upgrade	284
35.7 Restore Configuration	286
35.8 Backup Configuration	286
35.9 Tech-Support	287
35.9.1 Tech-Support Download	288
35.10 Certificates	289
35.10.1 HTTPS Certificates	290
35.11 Technical Reference	291
35.11.1 FTP Command Line	291
35.11.2 Filename Conventions	291
35.11.3 FTP Command Line Procedure	291
35.11.4 GUI-based FTP Clients	292
35.11.5 FTP Restrictions	292
Chapter 36	
Access Control.....	293
36.1 Access Control Overview	293
36.1.1 What You Can Do	293
36.2 The Access Control Main Screen	293
36.3 Configuring SNMP	294
36.3.1 Configuring SNMP Trap Group	295
36.3.2 Enabling/Disabling Sending of SNMP Traps on a Port	296
36.3.3 Configuring SNMP User	297
36.4 Logins	299
36.5 Service Access Control	300
36.6 Remote Management	301
36.7 Technical Reference	302
36.7.1 About SNMP	303
36.7.2 SSH Overview	306
36.7.3 Introduction to HTTPS	307
36.7.4 Google Chrome Warning Messages	311
Chapter 37	
Diagnostic.....	313
37.1 Overview	313
37.2 Diagnostic	313
Chapter 38	
System Log.....	316
38.1 Overview	316
38.2 System Log	316
Chapter 39	
Syslog Setup	317

39.1 Syslog Overview	317
39.1.1 What You Can Do	317
39.2 Syslog Setup	317
Chapter 40	
Cluster Management.....	320
40.1 Cluster Management Overview	320
40.1.1 What You Can Do	320
40.2 Cluster Management Status	321
40.3 Clustering Management Configuration	322
40.4 Technical Reference	324
40.4.1 Cluster Member Switch Management	324
Chapter 41	
MAC Table	326
41.1 MAC Table Overview	326
41.1.1 What You Can Do	326
41.1.2 What You Need to Know	326
41.2 Viewing the MAC Table	327
Chapter 42	
IP Table	329
42.1 IP Table Overview	329
42.2 Viewing the IP Table	329
Chapter 43	
ARP Table	331
43.1 ARP Table Overview	331
43.1.1 What You Can Do	331
43.1.2 What You Need to Know	331
43.2 Viewing the ARP Table	331
Chapter 44	
Routing Table	333
44.1 Overview	333
44.2 The Routing Table Main Screen	333
44.3 IPv4 Routing Table	333
44.4 IPv6 Routing Table	334
Chapter 45	
Path MTU Table	335
45.1 Path MTU Overview	335
45.2 Viewing the Path MTU Table	335

Chapter 46	
Configure Clone.....	336
46.1 Overview	336
46.2 Configure Clone	336
Chapter 47	
IPv6 Neighbor Table.....	339
47.1 IPv6 Neighbor Table Overview	339
47.2 Viewing the IPv6 Neighbor Table	339
Chapter 48	
Port Status	341
48.1 Port Status	341
48.1.1 Port Details	342
48.1.2 DDMI	345
48.1.3 DDMI Details	345
48.1.4 Port Utilization	347
Chapter 49	
Troubleshooting.....	348
49.1 Power, Hardware Connections, and LEDs	348
49.2 Switch Access and Login	349
49.3 Switch Configuration	350
Appendix A Customer Support	352
Appendix B Common Services.....	358
Appendix C IPv6.....	361
Appendix D Legal Information	369
Index	373

PART I

User's Guide

CHAPTER 1

Getting to Know Your Switch

1.1 Introduction

This chapter introduces the main features and applications of the Switch. The XS1930 Series consists of the following models:

- XS1930-10
- XS1930-12HP

References to PoE model(s) in this User's Guide only apply to XS1930-12HP.

The Switch is a smart managed switch supporting Multi-Gigabit ports. See [Section 1.1.1 on page 18](#) for more information about Multi-Gigabit. The Switch provides two SFP+ slots for uplink. By integrating static route functions, the Switch performs wire-speed layer-3 routing in addition to layer-2 switching.

The Switch supports NebulaFlex which can set the Switch to operate in either standalone or Nebula cloud management mode. When the Switch is in standalone mode, it can be configured and managed by the web configurator. When the Switch is in Nebula cloud management mode, it can be managed and provisioned by the Zyxel Nebula Control Center (NCC) (see [Section 8.12 on page 112](#)).

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

Table 1 XS1930 Series Comparison Table

FEATURE	XS1930-10	XS1930-12HP
100 Mbps, 1 Gbps, 2.5 Gbps, 5 Gbps, and 10 Gbps RJ-45 Ethernet Ports	8	2
100 Mbps, 1 Gbps, 2.5 Gbps, 5 Gbps, and 10 Gbps PoE Ports	0	8
10 Gbps SFP+ Interface	2	2
FAN	1	2

1.1.1 Multi-Gigabit

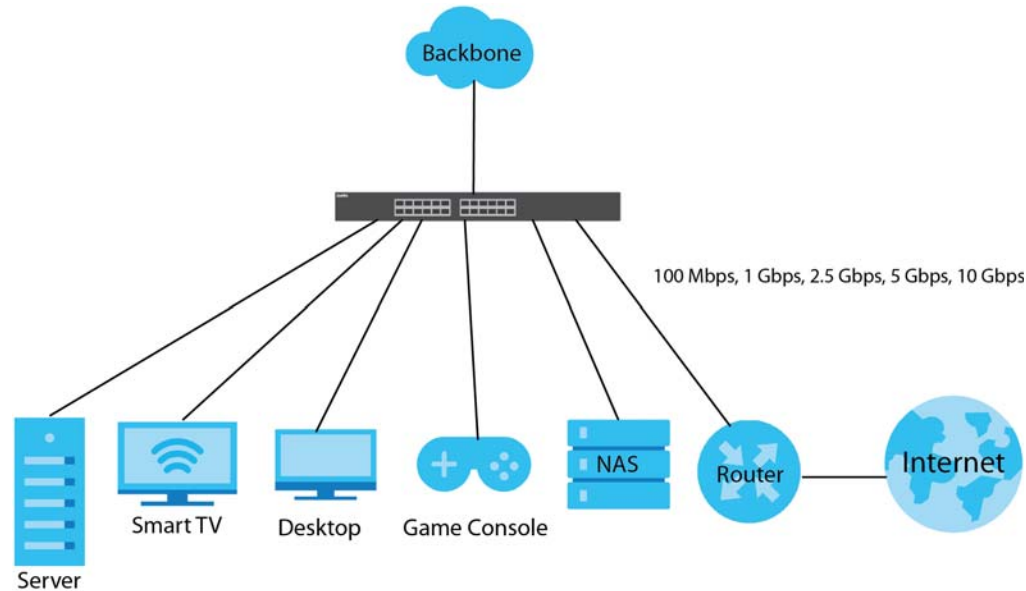
A 10 Gigabit Ethernet port supports speeds of 10 Gbps if the connected device supports 10 Gbps and a Cat 6a (up to 100 m) or Cat 6 cable (up to 50 m) is used.

Some network devices such as gaming computers, servers, network attached storage (NAS) devices, or access points may have network cards that are capable of 2.5 Gbps or 5 Gbps connectivity.

If these devices are connected to a 1 Gbps or 10 Gbps Ethernet port, they can only transmit or receive up to 1 Gbps as speeds of 10 Gbps cannot be attained. Moreover, if network devices with 10 Gbps network cards are connected to a 10 Gbps Ethernet port, you must use Cat 6A or better Ethernet cables to achieve 10 Gbps speeds.

The Multi-Gigabit Ethernet ports on the Switch automatically allow connections up to the speed of the connected network device (100 Mbps, 1 Gbps, 2.5 Gbps or 5 Gbps), and you just need to use a Cat 5e or Cat 6 Ethernet cable.

Figure 1 Multi-Gigabit Application



See the following table for the cables required and distance limitation to attain the corresponding speed.

Table 2 Cable Types

CABLE	TRANSMISSION SPEED	MAXIMUM DISTANCE	BANDWIDTH CAPACITY
Category 5	100 Mbps	100 m	100 MHz
Category 5e	1 Gbps/2.5 Gbps/5 Gbps	100 m	100 MHz
Category 6	5 Gbps/10 Gbps	50 m	250 MHz
Category 6a	10 Gbps	100 m	500 MHz
Category 7	10 Gbps	100 m	650 MHz

Note: Make sure to select the correct speed for the port in **Basic Setting > Port Setup**.

1.1.2 Management Modes

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

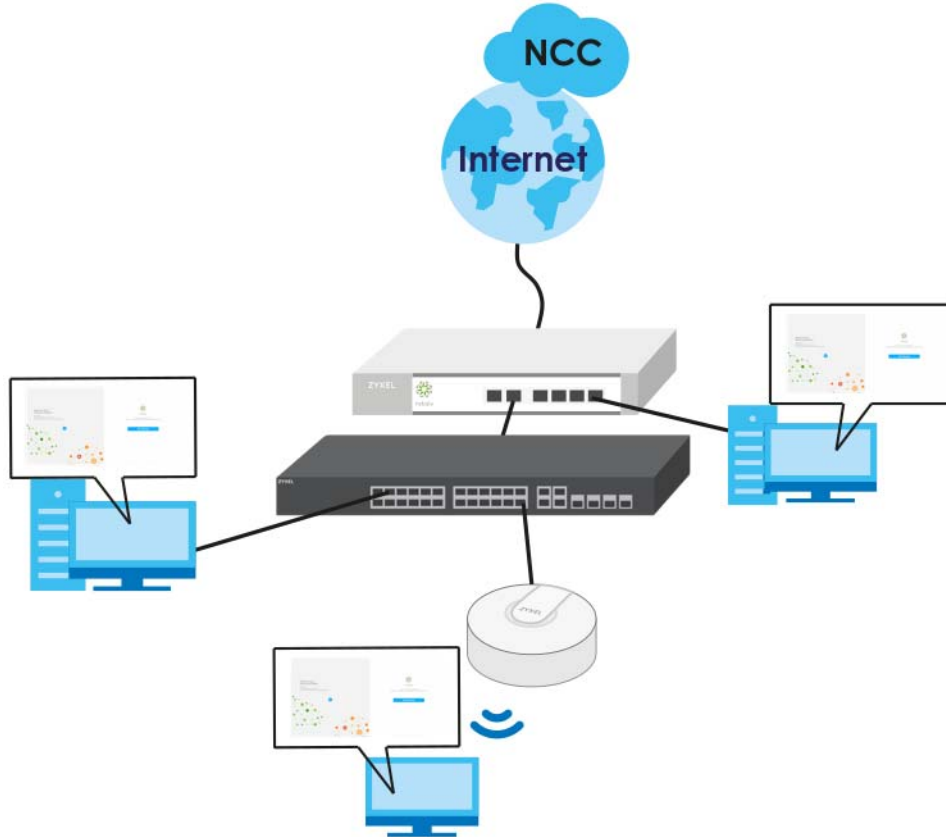
Use the web configurator to configure and manage the Switch directly in standalone mode or use Nebula Control Center (NCC) to configure and manage the Switch in cloud mode. The Nebula Control Center (NCC) is an alternative cloud-based network management system that allows you to remotely manage and monitor the Switch. You may also access a minimized version of the web configurator in cloud mode.

Nebula Cloud Management

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

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

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



1.1.3 Mode Changing

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

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

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

From Standalone to Nebula Cloud Management

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

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

Go to the NCC to Register the Switch

- 1 Go to the Nebula web portal in one of three ways.
 - Type <https://nebula.zyxel.com> in a supported web browser. See the Nebula User's Guide for more information about supported browsers.
 - Click **Nebula Mode** in the Switch's login page.
 - Click the **Nebula** icon in the upper right corner of the Switch's web configurator.
- 2 Click **Login** in the Nebula web portal. Enter your myZyXel account information. You'll be redirected to another screen where you can sign up for a myZyXel account if you don't have one.
- 3 Create an organization and a site or select an existing site.
- 4 Register the Switch by entering its MAC address and serial number and assign it to the site. The serial number and MAC address can be found in the **Status** screen or the device back label on the Switch.

Use the ZyXel Nebula Mobile App to Register the Switch

- 1 Download and open the ZyXel Nebula Mobile app in your mobile device. Click **Sign Up** to create a myZyXel account or enter your existing account information to log in.
- 2 You should already have created an organization and a site.
- 3 Select a site and scan the Switch's QR code to add it to the site. You can find the QR code:
 - On a label on the Switch or
 - On its box or
 - In the web configurator at **Basic Setting > Cloud Management > Nebula Switch Registration**.

See [Section 3.3 on page 35](#) for more information about the **CLOUD LED** or [Section 7.2 on page 73](#) for more information about the **Hybrid Mode** field in the **Status** screen to see if the Switch goes into Nebula cloud management mode successfully.

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

From Nebula-managed to Standalone

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

1.1.4 ZON Utility

You can view, manage, and configure the Switch and its neighboring devices using its built-in web configurator, including the Neighbor Management feature ([Section 4.4 on page 48](#)).

In addition, Zyxel offers a proprietary software program called Zyxel One Network (ZON) Utility. It is a 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 44](#).

1.1.5 PoE

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

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

- IEEE 802.3af Power over Ethernet (PoE)
- IEEE 802.3at Power over Ethernet (PoE) Plus
- IEEE 802.3bt 4PPoE (4-pair PoE)

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

Table 3 Models and PoE Features

POE FEATURES	XS1930-12HP
IEEE 802.3af PoE	Yes
IEEE 802.3at PoE Plus	Yes
IEEE 802.3bt 4PPoE	Yes
Power Management Mode	Consumption Classification
PoE Power Budget	375 W

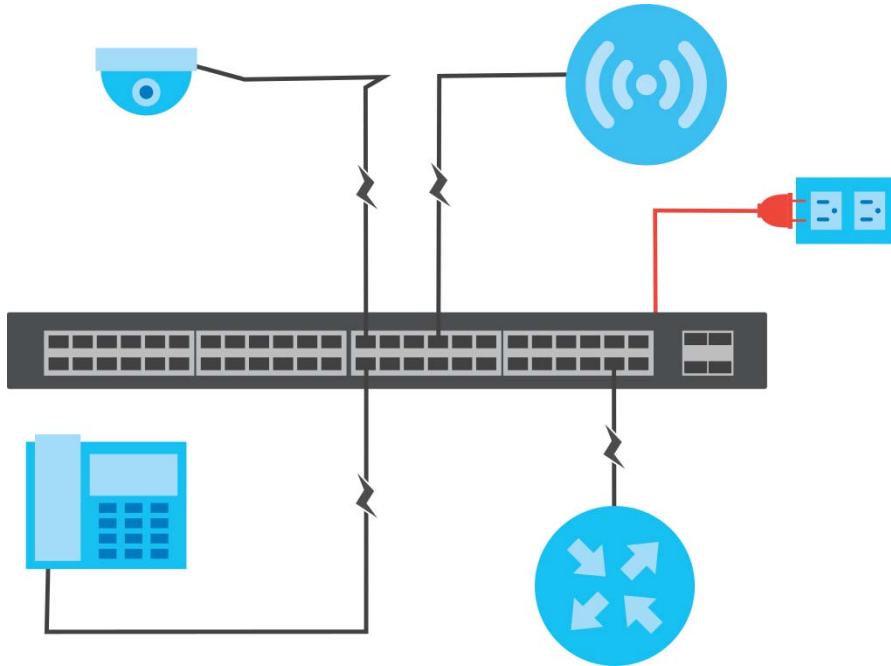
1.2 Example Applications

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

1.2.1 PoE Example Application

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

Figure 2 PoE Example Application

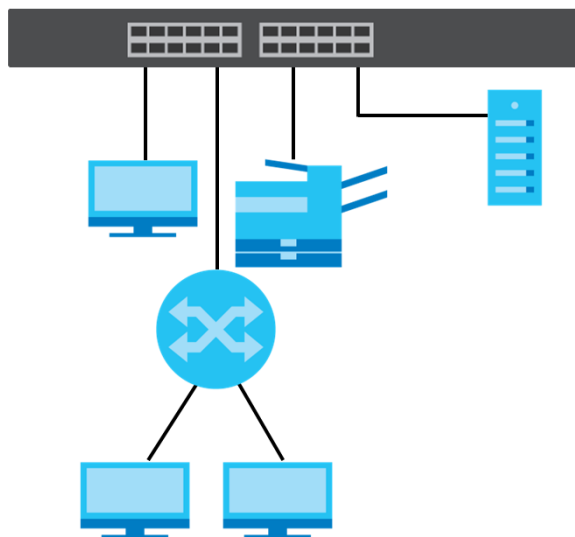


1.2.2 Backbone Example Application

The Switch is an ideal solution for small networks where rapid growth can be expected in the near future. The Switch can be used standalone for a group of heavy traffic users. You can connect computers and servers directly to the Switch's port or connect other switches to the Switch.

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

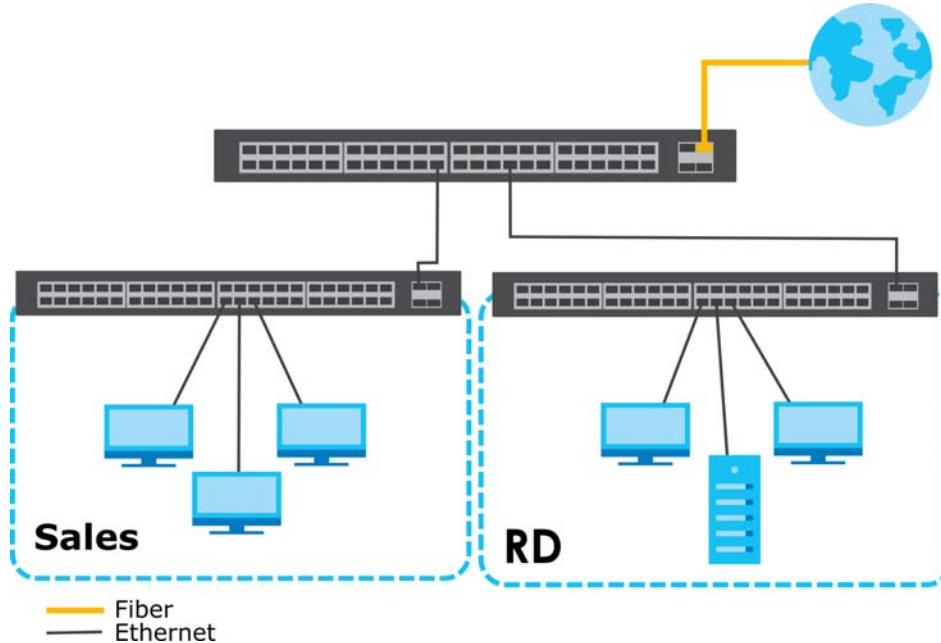
Figure 3 Backbone Application



1.2.3 Bridging / Fiber Uplink Example Application

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

Figure 4 Bridging / Fiber Uplink Example Application

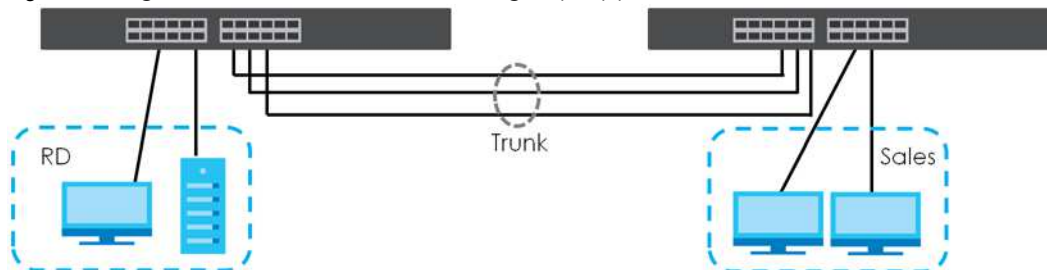


1.2.4 High Performance Switching Example

The Switch is ideal for connecting two networks that need high bandwidth. In the following example, use link aggregation (trunking) to connect these two networks. The Switch can provide high bandwidth at much lower cost while still being able to use existing network adapters and switches. Moreover, the current LAN structure can be retained as all ports can freely communicate with each other.

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

Figure 5 High Performance Switched Workgroup Application



1.2.5 IEEE 802.1Q VLAN Application Examples

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

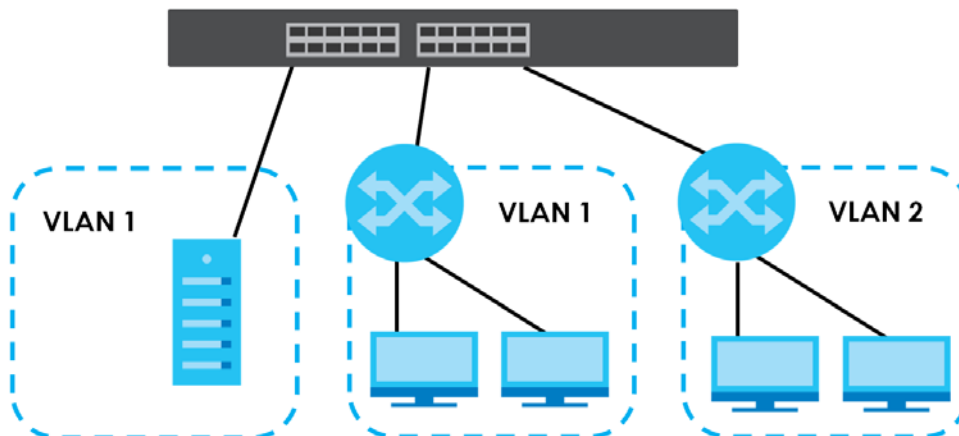
For more information on VLANs, refer to [Chapter 9 on page 114](#).

1.2.5.1 Tag-based VLAN Example

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

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

Figure 6 Shared Server Using VLAN Example



1.3 Ways to Manage the Switch

Use any of the following methods to manage the Switch.

- Web Configurator. This is recommended for everyday management of the Switch using a (supported) web browser. See [Chapter 4 on page 39](#).
- FTP. Use FTP for firmware upgrades and configuration backup/restore. See [Section 35.11.1 on page 291](#).
- SNMP. The Switch can be monitored by an SNMP manager. See [Section 35.8 on page 286](#).
- Cluster Management. Cluster Management allows you to manage multiple switches through one switch, called the cluster manager. See [Chapter 39 on page 317](#).
- 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 44](#).

- NCC (Zyxel Nebula Control Center). With the NCC, you can remotely manage and monitor the Switch through a cloud-based network management system. See [Section 8.12 on page 112](#) or the NCC User's Guide for detailed information about how to access the NCC and manage your Switch via the NCC. See the NCC User's Guide for how to configure Nebula managed devices.

1.4 Good Habits for Managing the Switch

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

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

CHAPTER 2

Hardware Installation and Connection

2.1 Installation Scenarios

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

The Switch can be:

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

Note: Ask an authorized technician to attach the Switch to the rack. See the **Installation Requirements** sections in this chapter to know the types of screws and screw drivers for each mounting method.

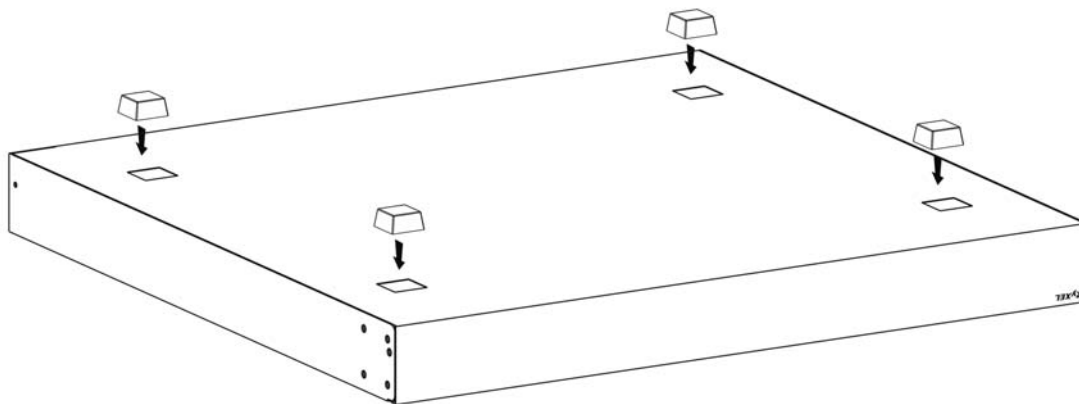
WARNING! Failure to use the proper screws may damage the unit.

WARNING! This Switch is not suitable for use in locations where children are likely to be present.

2.2 Desktop Installation Procedure

- 1 Make sure the Switch is clean and dry.
- 2 Set the Switch on a smooth, level surface strong enough to support the weight of the Switch and the connected cables. Make sure there is a power outlet nearby.
- 3 Make sure there is at least 40 mm of clearance from the bottom to the Switch, and make sure there is enough clearance around the Switch to allow air circulation and the attachment of cables and the power cord. This is especially important for enclosed rack installations.
- 4 Remove the adhesive backing from the rubber feet.
- 5 Attach the rubber feet to each corner on the bottom of the Switch. These rubber feet help protect the Switch from shock or vibration and ensure space between devices when stacking.

Figure 7 Attaching Rubber Feet



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

Note: Do NOT store things on the Switch, and allow clearance next to the ventilation holes to prevent your Switch from overheating. This is especially crucial when your Switch doesn't have fan modules. See [Section Table 1 on page 18](#) to see whether your Switch has fan modules.

Overheating could affect the performance of your Switch, or even damage it.

2.3 Mounting the Switch on a Rack

The Switch can be mounted on an EIA standard size, 17-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 Rack-mounted Installation Requirements

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

Failure to use the proper screws may damage the unit.

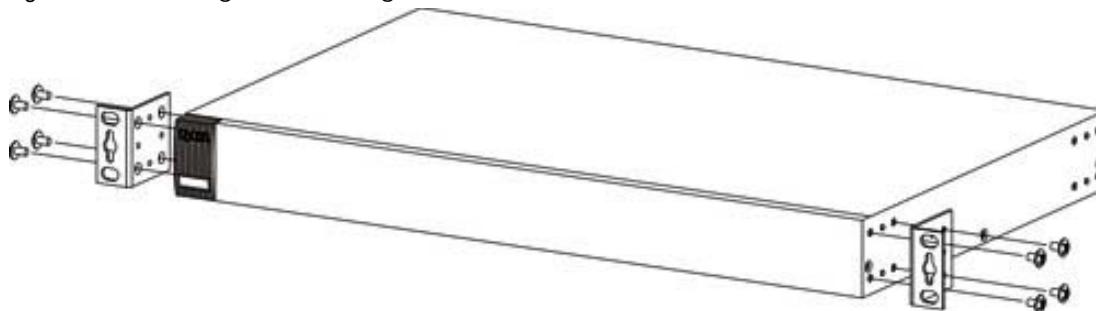
2.3.1.1 Precautions

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

2.3.2 Attaching the Mounting Brackets to the Switch

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

Figure 8 Attaching the Mounting Brackets

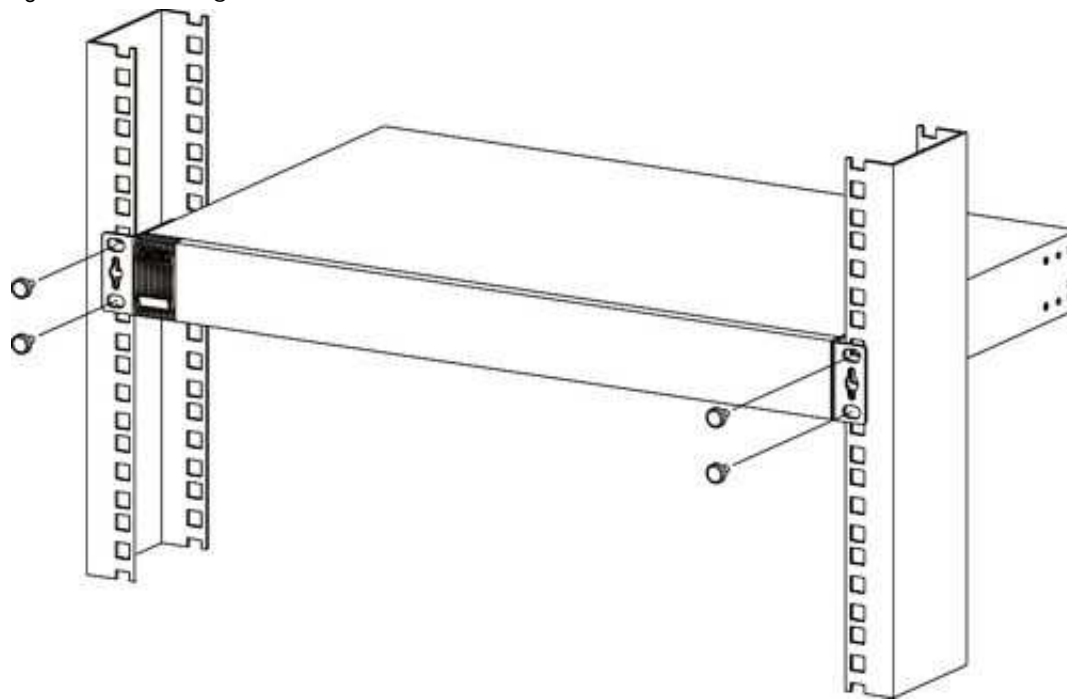


- 2 Using a #2 Philips screwdriver, install the M3 flat head screws through the mounting bracket holes into the Switch.
- 3 Repeat steps 1 and 2 to install the second mounting bracket on the other side of the Switch.
- 4 You may now mount the Switch on a rack. Proceed to the next section.

2.3.3 Mounting the Switch on a Rack

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

Figure 9 Mounting the Switch on a Rack



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

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

CHAPTER 3

Hardware Panels

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

3.1 Front Panel

The following figures show the front panels of the Switch.

Figure 10 Front Panel: XS1930-10

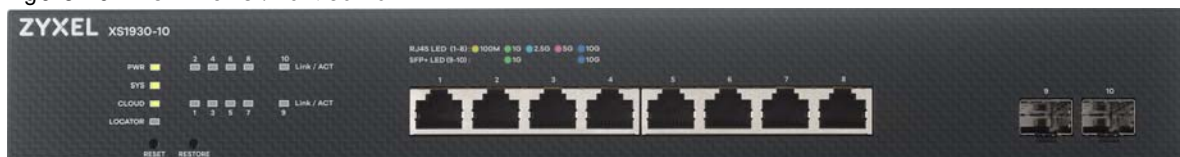
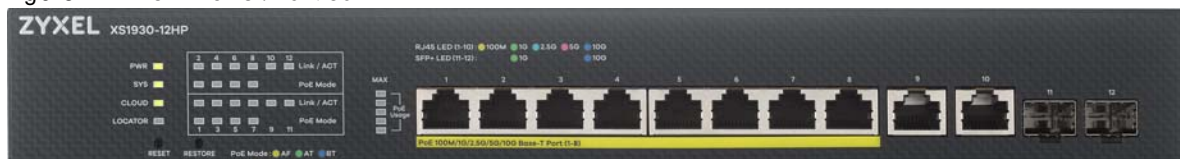


Figure 11 Front Panel: XS1930-12HP



The following table describes the ports.

Table 4 Front Panel Connections

CONNECTOR	DESCRIPTION
2 or 8 100 Mbps, 1 Gbps, 2.5 Gbps, 5 Gbps, and 10 Gbps RJ-45 Ethernet Ports	These are 10GBase-T auto-negotiating and auto-crossover Ethernet ports. Connect these ports to a computer, a hub, a router, or an Ethernet switch.
8 100 Mbps, 1 Gbps, 2.5 Gbps, 5 Gbps, and 10 Gbps RJ-45 PoE Ports	These are 10GBase-T auto-negotiating and auto-crossover Ethernet ports. Connect these ports to a computer, a hub, a router, or an Ethernet switch.
2 10 GbE SFP+ Slots	Use SFP+ transceivers in these ports for high-bandwidth backbone connections. You can also insert an SFP+ Direct Attach Copper (DAC) in the SFP+ slot.
Reset	Press the RESET button to reboot the Switch without turning the power off. See Section 3.3 on page 35 for more information about the LED behavior.
Restore	Press the RESTORE button for three to six seconds to have the Switch automatically reboot and restore the last-saved custom default file. See Section 3.3 on page 35 for more information about the LED behavior. Press the RESTORE button for more than seven seconds to have the Switch automatically reboot and restore the factory default file. See Section 3.3 on page 35 for more information about the LED behavior.

3.1.1 Ethernet Ports

The Switch has 10GBase-T auto-negotiating, auto-crossover Ethernet ports. In Multi-Gigabit Ethernet, the speed can be 100 Mbps, 1 Gbps, 2.5 Gbps, 5 Gbps, or 10 Gbps. See [Section 1.1.1 on page 18](#) for more information about Multi-Gigabit Ethernet. The duplex mode can be full duplex only.

An auto-negotiating port can detect and adjust to the optimum Ethernet speed (100 Mbps, 1 Gbps, 2.5 Gbps, 5 Gbps, and 10 Gbps) and full duplex mode of the connected device.

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

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

3.1.1.1 Default Ethernet Negotiation Settings

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

- Speed: Auto
- Duplex: Auto
- Flow control: Off
- Link Aggregation: Disabled

3.1.1.2 Auto-crossover

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

3.1.2 PoE (XS1930-12HP)

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

3.1.3 SFP/SFP+ Slots

These slots are for Small Form-Factor Pluggable (SFP) or SFP+ transceivers or SFP+ DAC (Direct Attach Copper) cables. The SFP+ (SFP Plus) is an enhanced version of the SFP and supports data rates of 10 Gbps. A transceiver is a single unit that houses a transmitter and a receiver. Use a transceiver or a DAC cable to connect a fiber-optic cable to the Switch. The Switch does not come with transceivers nor DAC cables. You must use transceivers or DAC cables that comply with the Small Form-factor Pluggable (SFP) Transceiver MultiSource Agreement (MSA). See the SFF committee's INF-8074i specification Rev 1.0 for details.

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

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

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

3.1.3.1 Transceiver Installation

Use the following steps to install an SFP/SFP+ transceiver.

- 1 Locate the transmit (Tx) and the receive (Rx) markings on the SFP+ module to identify the top.
- 2 Insert the transceiver into the slot.
- 3 Press the transceiver firmly until it clicks into place.
- 4 The Switch automatically detects the installed transceiver. Check the LEDs to verify that it is functioning properly.
- 5 Close the transceiver's latch (latch styles vary).
- 6 Connect the fiber optic cables to the transceiver.

Figure 12 Transceiver Installation Example

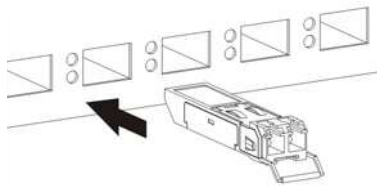
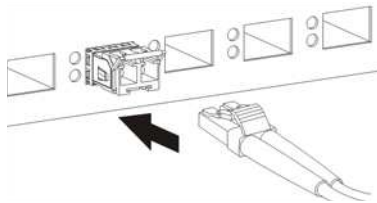


Figure 13 Connecting the Fiber Optic Cables



3.1.3.2 Transceiver Removal

Use the following steps to remove an SFP/SFP+ transceiver.

- 1 Remove the fiber optic cables from the transceiver.
- 2 Open the transceiver's latch (latch styles vary).
- 3 Pull the transceiver out of the slot.

Figure 14 Removing the Fiber Optic Cables

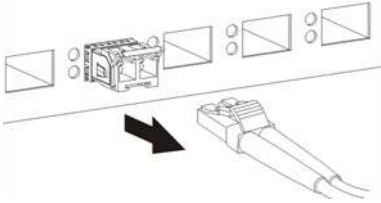


Figure 15 Opening the Transceiver's Latch Example

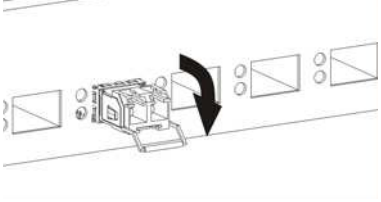
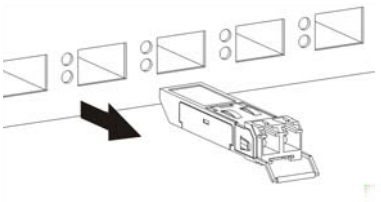


Figure 16 Transceiver Removal Example



3.2 Rear Panel

The following figures show the rear panels of the Switch.

Figure 17 Rear Panel: XS1930-10



Figure 18 Rear Panel: XS1930-12HP



3.2.1 Grounding

Grounding is a safety measure to have unused electricity return to the ground. It prevents damage to the Switch, and protects you from electrocution.

Note: The Switch must be grounded by qualified service personnel.

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

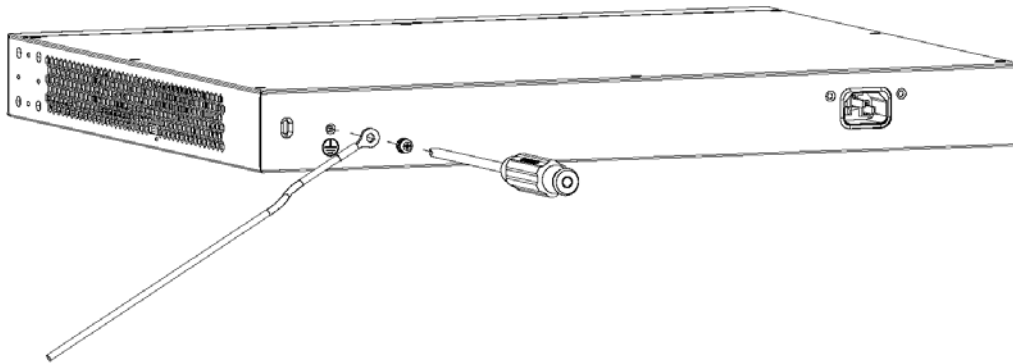
- 2 Secure a green/yellow ground cable (16 AWG or smaller) to the Switch's rear panel using the M4 ground screw.
- 3 Attach the other end of the cable to the ground, either to the same ground electrode as the rack you installed the device on or to the main grounding electrode of the building.

Follow your country's regulations and safety instructions to electrically ground the device properly.

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

Warning! Connect the ground cable before you connect any other cables or wiring.

Figure 19 Grounding



3.2.2 Power Connector

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. Make sure that no objects obstruct the airflow of the fans (located on the side of the unit).

Note: Make sure you are using the correct power source as shown on the panel.

See [Chapter 49 on page 348](#) for information on the Switch's power supply requirements.

3.3 LEDs

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

Table 5 LED Descriptions

LED	COLOR	STATUS	DESCRIPTION
PWR	Green	On	The Switch is receiving power from the power source.
		Blinking	The Switch is returning to the custom default configuration settings.
	Amber	On	The Switch is returning to its factory default configuration settings.
		Off	The Switch is not receiving power from the power source.

Table 5 LED Descriptions (continued)

LED	COLOR	STATUS	DESCRIPTION	
SYS	Green	On	The Switch is on and functioning properly.	
		Blinking	The Switch is rebooting and performing self-diagnostic tests.	
	Red	On	The Switch is functioning abnormally.	
		Off	The power is off or the Switch is not ready/malfunctioning.	
CLOUD	Green	On	The Switch is managed by the NCC (Nebula Control Center).	
		Blinking	The Switch is connected to the NCC, but not registered.	
	Amber	On	The Switch is in Nebula cloud management mode. It was trying to connect to the NCC, but failed.	
		Blinking	The Switch is in standalone mode. It was trying to connect to the NCC, but failed.	
		Off	Nebula cloud management mode is disabled.	
LOCATOR	Blue	On	The Switch is uploading firmware. While the Switch is doing this, don't turn off the power.	
		Blinking	Shows the actual location of the Switch between several devices in a rack. The default timer is 30 minutes when you are configuring the Switch.	
		Off	The locator is not functioning or malfunctioning.	
PoE MAX (XS1930-12HP) Bar1 is the bar at the bottom; bar 5 is the bar at the top.	Green (Bar1-Bar3)	On	Each bar represents 20% of PoE Power consumption.	
			Bar 1: PoE power usage is below 20 percent of the power supplied budget.	
			Bar 2: PoE power usage is below 40 percent of the power supplied budget, but over 20 percent of the power supplied budget.	
				Bar 3: PoE power usage is below 60 percent of the power supplied budget, but over 40 percent of the power supplied budget.
	Yellow (Bar4)	On	PoE power usage is below 80 percent of the power supplied budget, but over 60 percent of the power supplied budget.	
Red (Bar5)	On	PoE power usage is more than 80 percent of the power supplied budget.		
	Blinking	Less than 5 percent of the power supplied budget remains. 5 percent is the default value.		
		Off	PoE power usage is 0 percent of the power supplied budget.	
10GBase-T Ports				
LNK/ACT 1-8 (XS1930-10) 9-10 (XS1930-12HP)	Blue	On	The link to a 10 Gbps Ethernet network is up.	
		Blinking	The Switch is transmitting/receiving to/from a 10 Gbps Ethernet network.	
	Purple	On	The link to a 5 Gbps Ethernet network is up.	
		Blinking	The Switch is transmitting/receiving to/from a 5 Gbps Ethernet network.	
	Sky Blue	On	The link to a 2.5 Gbps Ethernet network is up.	
		Blinking	The Switch is transmitting/receiving to/from a 2.5 Gbps Ethernet network.	
	Green	On	The link to a 1000 Mbps Ethernet network is up.	
		Blinking	The Switch is transmitting/receiving to/from a 1000 Mbps Ethernet network.	
	Amber	On	The link to a 100 Mbps Ethernet network is up.	
		Blinking	The Switch is transmitting/receiving to/from a 100 Mbps Ethernet network.	
		Off	The link to an Ethernet network is down.	
PoE 10GBase-T Ports				

Table 5 LED Descriptions (continued)

LED	COLOR	STATUS	DESCRIPTION
LNK/ACT 1-8 (XS1930-12HP)	Blue	On	The link to a 10 Gbps Ethernet network is up.
		Blinking	The Switch is transmitting/receiving to/from a 10 Gbps Ethernet network.
	Purple	On	The link to a 5 Gbps Ethernet network is up.
		Blinking	The Switch is transmitting/receiving to/from a 5 Gbps Ethernet network.
	Sky Blue	On	The link to a 2.5 Gbps Ethernet network is up.
		Blinking	The Switch is transmitting/receiving to/from a 2.5 Gbps Ethernet network.
	Green	On	The link to a 1000 Mbps Ethernet network is up.
		Blinking	The Switch is transmitting/receiving to/from a 1000 Mbps Ethernet network.
	Amber	On	The link to a 100 Mbps Ethernet network is up.
		Blinking	The Switch is transmitting/receiving to/from a 100 Mbps Ethernet network.
		Off	The link to an Ethernet network is down.
PoE Mode 1-8 (XS1930-12HP)	Blue	On	Power supplied to all PoE Ethernet ports meets the IEEE 802.3bt standard.
	Green	On	Power supplied to all PoE Ethernet ports meets the IEEE 802.3at standard.
	Yellow	On	Power supplied to all PoE Ethernet ports meets the IEEE 802.3af standard.
		Off	There is no power supplied.
1G/10G SFP+ Slots			
LNK/ACT 9-10 (XS1930-10)	Green	On	The port has a successful 1000 Mbps connection.
		Blinking	The port is transmitting or receiving data at 1000 Mbps.
11-12 (XS1930-12HP)	Blue	On	The port has a successful 10 Gbps connection.
		Blinking	The port is transmitting or receiving data at 10 Gbps.
		Off	This link is disconnected.

PART II

Technical Reference

CHAPTER 4

The 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 Switch setup and management via Internet browser. Use Internet Explorer 9.0 and later versions, Mozilla Firefox 21 and later versions, Safari 6.0 and later versions or Google Chrome 26.0 and later versions. The recommended screen resolution is 1024 by 768 pixels.

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

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

Note: The screens are based on the Switch in standalone mode.

4.2 System Login

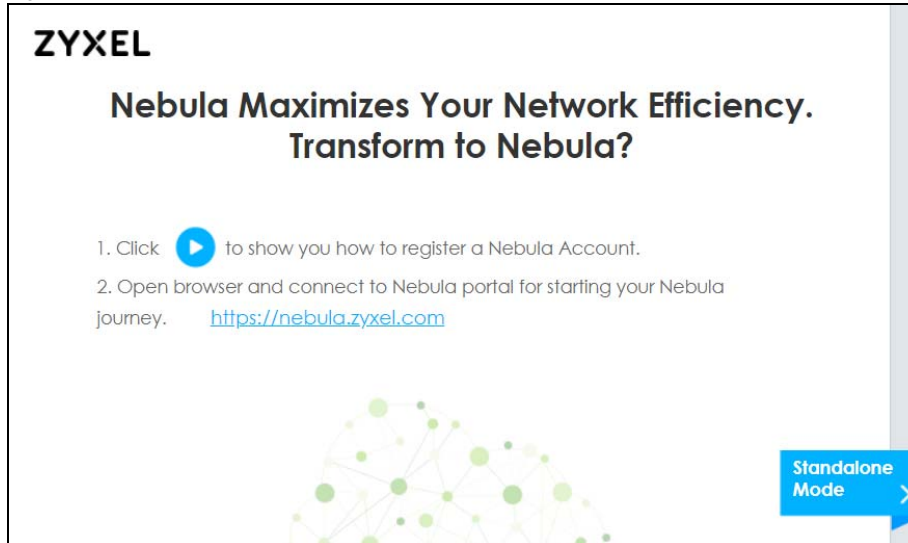
- 1 Start your web browser.
- 2 The Switch is a DHCP client by default. Type "http://DHCP-assigned IP" in the **Location** or **Address** field. Press [ENTER].

If the Switch is not connected to a DHCP server, type "http://" and the static IP address of the Switch (for example, the default management IP address is 192.168.1.1) 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 44](#)).
- 3 The following screen appears.

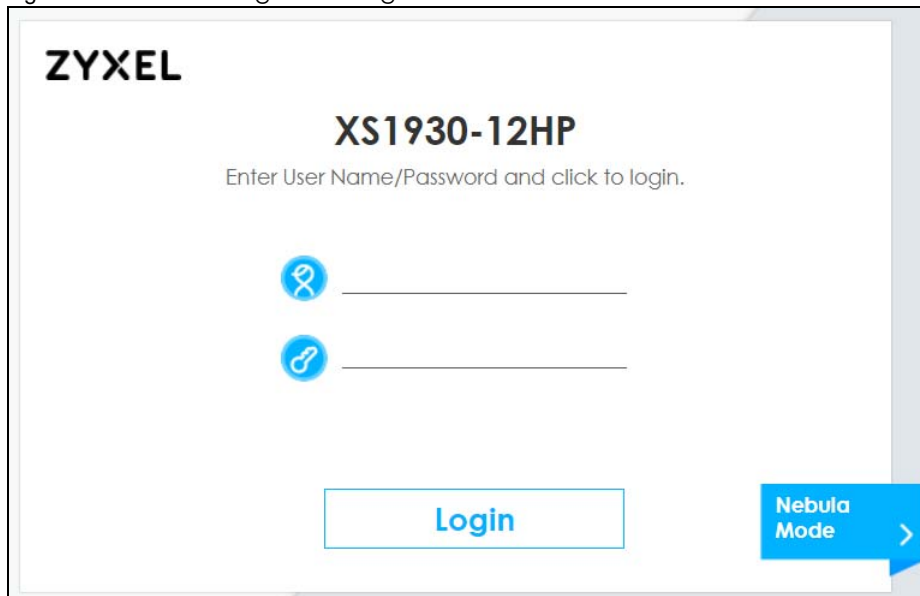
You can click the play icon to watch a tutorial video on how to create an NCC account or click the link to access the NCC portal. The NCC is a cloud-based network management system that allows you to remotely manage and monitor the Switch in Nebula cloud management mode. Click **Standalone Mode** to go back to the login screen and continue with the next step.

Figure 20 Web Configurator > Login: Nebula Mode



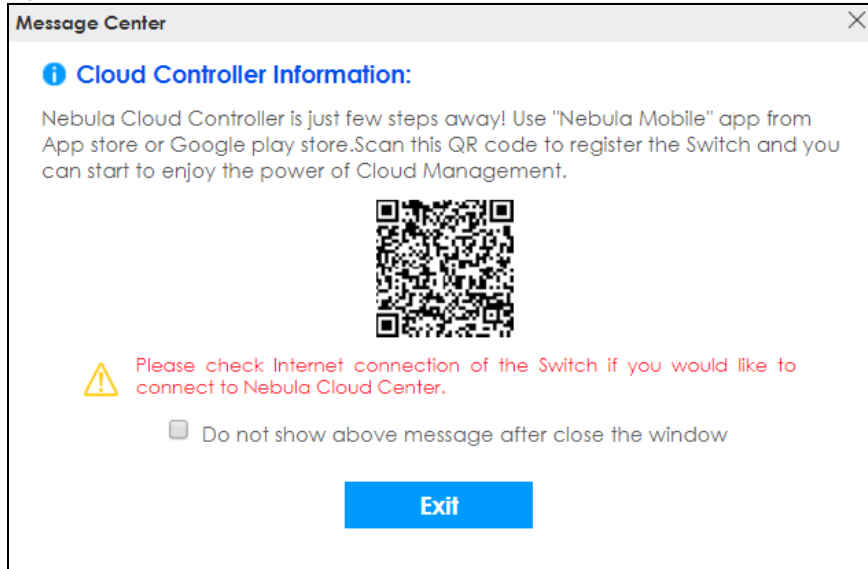
- 4 Click **Login** to log into the web configurator to manage the Switch directly. The default username is admin and associated default password is 1234.

Figure 21 Web Configurator: Login: Standalone Mode



- 5 After you log into the web configurator, you will see the following screen encouraging you to use NCC. The screen has a QR code containing the Switch's serial number and MAC address for 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 at NCC.

Figure 22 Web Configurator: Message



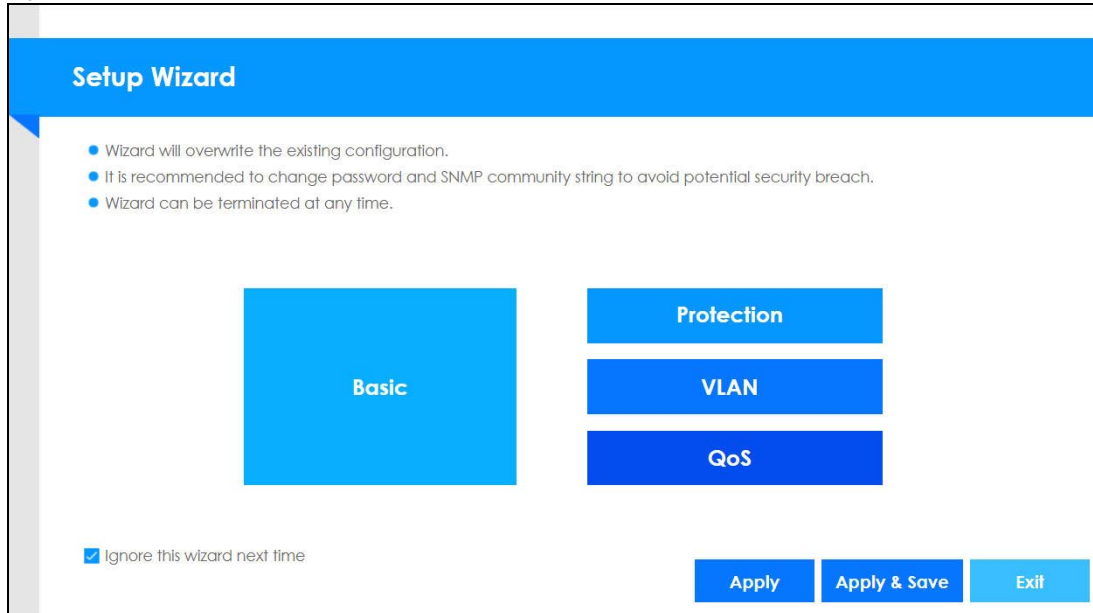
You may also access this screen at **Basic Setting > Cloud Management > Nebula Switch Registration**.

- 6 The Wizard screen will appear after logging into the Switch. You can use the Wizard screen to configure the Switch's IP, login password, SNMP community, link aggregation, and so on. See [Section 4.4 on page 48](#) for more information on the Wizard screen. When you finish configuring the settings, you can click the **Apply** button to make the settings take effect. Check the screens to see if the settings are applied, and click the **Save** button in the top to save your configuration into the Switch's nonvolatile memory. You can also just click the **Apply & Save** button to make the settings takes effect, and save your configuration into the Switch's nonvolatile memory at once.

Note: Once you click the **Apply** or **Apply & Save** button, the settings configured in the Wizard screen will overwrite the existing settings.

Otherwise, click the **Exit** button. You can select the **Ignore this wizard next time** check box and click **Apply** if you don't want the Wizard screen to appear the next time you log in. If you want to open the Wizard screen later, click the Wizard icon in the upper right hand corner of the web configurator.

Figure 23 Web Configurator: Wizard



- 7 If you didn't change the default administrator password and/or SNMP community values, a warning screen displays each time you log into the web configurator. Click **Password / SNMP** to open a screen where you can change the administrator and SNMP passwords simultaneously. Otherwise, click Ignore to close it.

Figure 24 Web Configurator: Warning

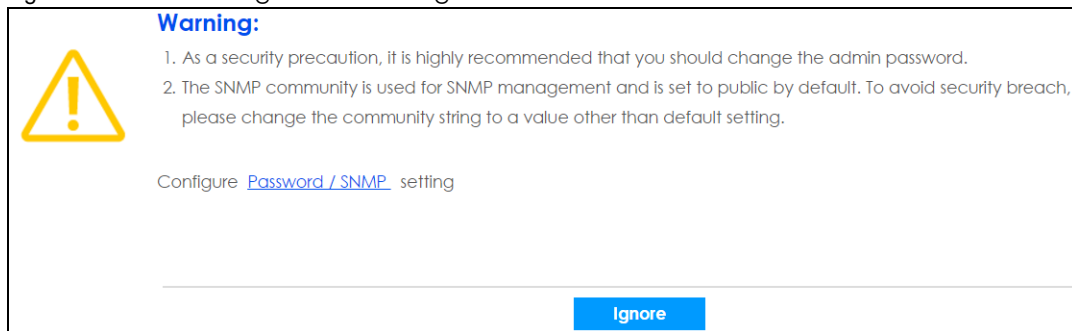


Figure 25 Web Configurator: Password

The screenshot shows two sections of the Web Configurator interface. The top section is titled "Password" and "Administrator". It contains three input fields: "Old Password", "New Password", and "Retype to confirm". The bottom section is titled "SNMP" and "General Setting". It contains a "Version" dropdown menu set to "v2c", and three input fields for "Get Community", "Set Community", and "Trap Community", all of which contain the text "public". At the bottom of the form are "Apply" and "Cancel" buttons.

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

Table 6 Web Configurator: Password/SNMP

LABEL	DESCRIPTION
Administrator	This is the default administrator account with the "admin" user name. You cannot change the default administrator user name.
Old Password	Type the existing system password (1234 is the default password when shipped).
New Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation
General Setting	Use this section to specify the SNMP version and community (password) values.
Version	Select the SNMP version for the Switch. The SNMP version on the Switch must match the version on the SNMP manager. Choose SNMP version 2c (v2c), SNMP version 3 (v3) or both (v3v2c). Note: SNMP version 2c is backwards compatible with SNMP version 1.
Get Community	Enter the Get Community string, which is the password for the incoming Get- and GetNext-requests from the management station. The Get Community string is only used by SNMP managers using SNMP version 2c or lower.
Set Community	Enter the Set Community string, which is the password for the incoming Set- requests from the management station. The Set Community string is only used by SNMP managers using SNMP version 2c or lower.
Trap Community	Enter the Trap Community string, which is the password sent with each trap to the SNMP manager. The Trap Community string is only used by SNMP managers using SNMP version 2c or lower.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

4.3 Zyxel One Network (ZON) Utility

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

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

4.3.1 Requirements

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

Operating System

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

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

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

Note: It is suggested that you install Npcap, the packet capture library for Windows operating systems, and remove WinPcap or any other installed packet capture tools before you install the ZON utility.

Hardware

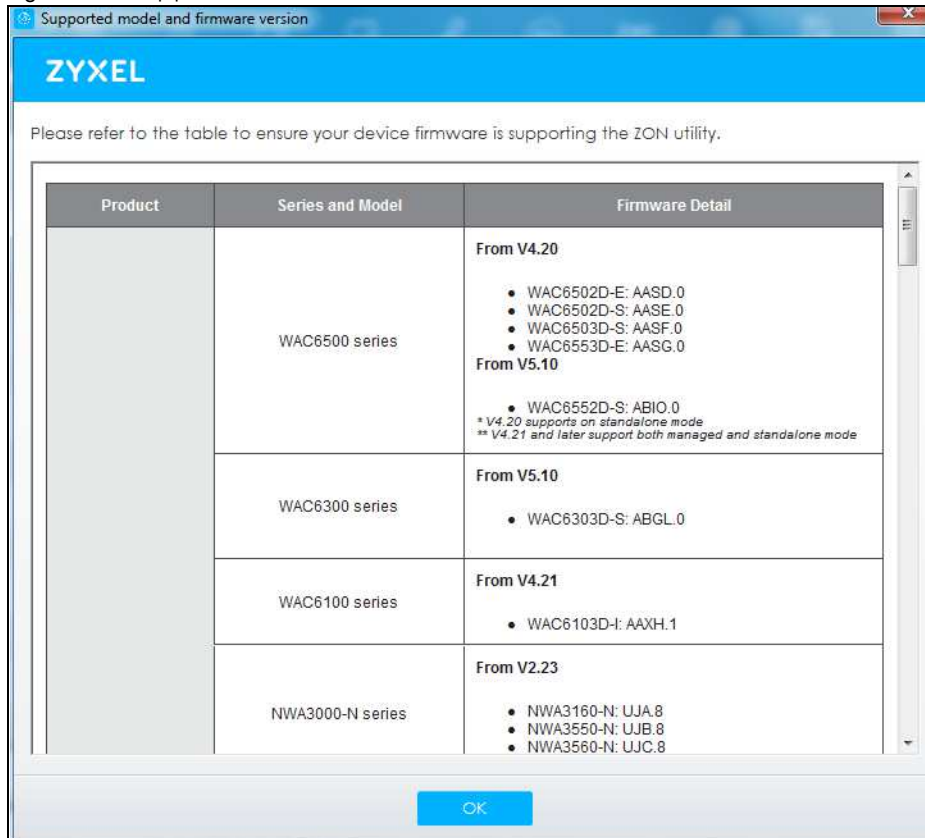
Here are the minimum hardware requirements to use the ZON Utility on your PC.

- Core i3 processor
- 2GB RAM
- 100MB free hard disk
- WXGA (Wide XGA 1280x800)

4.3.2 Run the ZON Utility

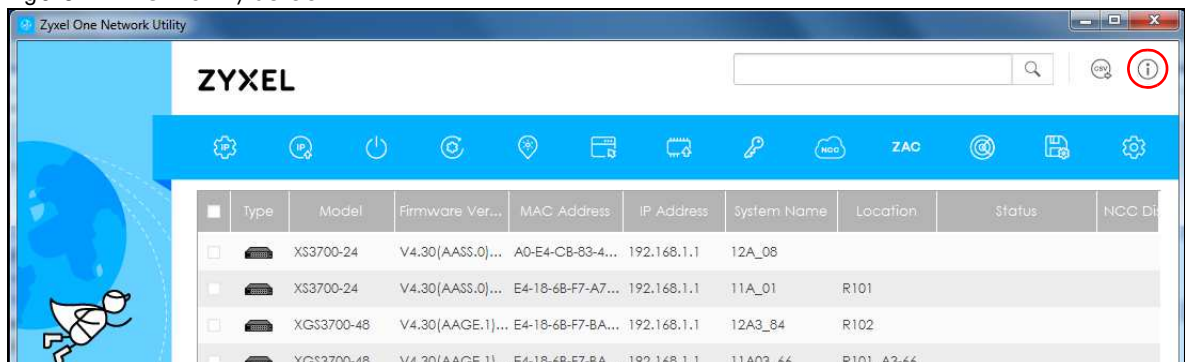
- 1 Double-click the ZON Utility to run it.
- 2 The first time you run the ZON Utility, you will see if your Switch and firmware version support the ZON Utility. Click the OK button to close this screen.

Figure 26 Supported Devices and Versions



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

Figure 27 ZON Utility Screen



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

Figure 28 Network Adapter



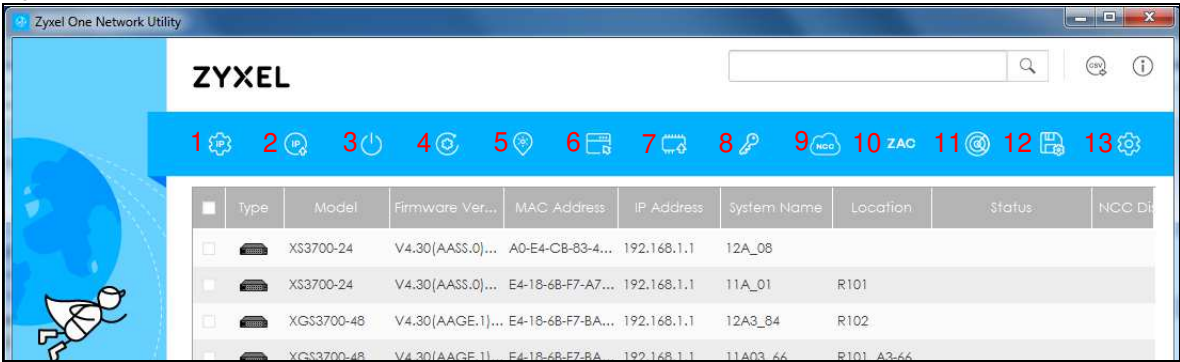
- Click the Go button for the ZON Utility to discover all supported devices in your network.

Figure 29 Discovery



- The ZON Utility screen shows the devices discovered.

Figure 30 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 31 Password Prompt



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

Table 7 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 device(s). 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 username and password to log in.
7 Firmware Upgrade	Use this icon to upgrade new firmware to selected device(s) 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's 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'll 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 adaptor 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 8 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.

Table 8 ZON Utility Fields

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

4.4 Wizard

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

- **Basic** - to configure the Switch IP address, DNS server, system password, SNMP community, and link aggregation (trunking).
- **Protection** - to enable loop guard and broadcast storm on the Switch and its ports.
- **VLAN** - to create a static VLAN, assign ports to the VLAN, and set the ports to tag or untag outgoing frames.
- **QoS** - to determine a port's IEEE 802.1p priority level for QoS.

4.4.1 Basic

In **Basic**, you can set up IP/DNS, set up your password, SNMP community, link aggregation, and view finished results.

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

Figure 32 Wizard > Basic > Step 1 IP

The screenshot shows the 'Setup IP' configuration screen. At the top, there is a progress bar with four steps: 1 IP, 2 Password, 3 Link Aggregation, and 4 Summary. The '1 IP' step is currently active. Below the progress bar, the title 'Setup IP' is displayed. The configuration fields are as follows:

- Host Name: XS1930
- IP Interface: ☒ Static IP Address ☐ DHCP Client
- VID: 1
- IP Address: 192.168.1.1
- IP Subnet Mask: 255.255.255.0
- Default Gateway: 0.0.0.0
- DNS Server: 0.0.0.0

At the bottom right, there are two buttons: 'Next' and 'Cancel'.

Each field is described in the following table.

Table 9 Wizard > Basic > 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 Address when the Switch is NOT connected to a router or you want to assign it a fixed IP address.
VID	This field displays the VLAN ID.
IP Address	The Switch needs an IP address for it to be managed over the network.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address.
Default Gateway	Type the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
DNS Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. Enter a domain name server IP address in order to be able to use a domain name instead of an IP address.
Next	Click Next to show the next screen.
Cancel	Click Cancel to exit this screen without saving.

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

Figure 33 Wizard > Basic > Step 2 Password

Each field is described in the following table.

Table 10 Wizard > Basic > Step 2 Password

LABEL	DESCRIPTION
Administrator's Password	
Current password	Type the existing system password (1234 is the default password when shipped).
New password	Enter your new system password.
Confirm password	Retype your new system password for confirmation
SNMP	
SNMP	Select Enabled to let the Switch act as an SNMP agent, which allows a manager station to manage and monitor the Switch through the network. Select Disabled to turn this feature off.
Version	Select the SNMP version for the Switch. The SNMP version on the Switch must match the version on the SNMP manager. Choose SNMP version 2c (v2c), SNMP version 3 (v3) or both (v3v2c). Note: SNMP version 2c is backwards compatible with SNMP version 1.
Get Community	Enter the Get Community string, which is the password for the incoming Get- and GetNextrequests from the management station. The Get Community string is only used by SNMP managers using SNMP version 2c or lower.
Set Community	Enter the Set Community string, which is the password for the incoming Set- requests from the management station. The Set Community string is only used by SNMP managers using SNMP version 2c or lower.
Trap Community	Enter the Trap Community string, which is the password sent with each trap to the SNMP manager. The Trap Community string is only used by SNMP managers using SNMP version 2c or lower.
Previous	Click Previous to show the previous screen.

Table 10 Wizard > Basic > Step 2 Password

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

After clicking Next, the Link Aggregation screen appears.

Figure 34 Wizard > Basic > Step 3 Link Aggregation

Each field is described in the following table.

Table 11 Wizard > Basic > Step 3 Link Aggregation

LABEL	DESCRIPTION
Link Aggregation	
T1-T5	Click the arrows to add or delete icons located on the left to desired preference. Select Static if the ports are configured as static members of a trunk group. Select LACP if the ports are configured to join a trunk group via LACP.
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 35 Wizard > Basic > Step 4 Summary

Summary

Setup IP

Host Name: XS1930

IP Interface: Static IP Address

VID: 1

IP Address: 192.168.1.1

IP Subnet Mask: 255.255.255.0

Default Gateway: 0.0.0.0

DNS Server:

Change administrator's password and activate SNMP

New password:

SNMP: Enabled

Version: v2c

Get Community: public

Set Community: public

Trap Community: public

Link Aggregation

Group	Type	Member
T1	Static	11,12

Previous Finish Cancel

Each field is described in the following table.

Table 12 Wizard > Basic > 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	The Switch needs an IP address for it to be managed over the network.
IP Subnet Mask	The subnet mask specifies the network number portion of an IP address.
Default Gateway	Type the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
DNS Server	DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and vice versa. Enter a domain name server IP address in order to be able to use a domain name instead of an IP address.
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.
Link Aggregation	
Group	This field displays the group number.
Type	This field displays Static or LACP of this group.
Member	This field displays the members of this group.

Table 12 Wizard > Basic > Step 4 Summary

LABEL	DESCRIPTION
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 Protection

In **Protection**, you can set up loop guard and broadcast storm control.

In order to set up loop guard, please do the following. Click **Wizard > Protection > Step 1 Loop Guard** to access this screen.

Figure 36 Wizard > Protection > Step 1 Loop Guard

Each field is described in the following table.

Table 13 Wizard > Protection > Step 1 Loop Guard

LABEL	DESCRIPTION
Loop Guard	
Select all ports	Select all ports to enable the loop guard feature on all ports. You can select a port by clicking it.
Next	Click Next to show the next screen.
Cancel	Click Cancel to exit this screen without saving.

After clicking **Next**, the **Broadcast Storm Control** screen appears.

Figure 37 Wizard > Protection > Step 2 Broadcast Storm Control

Broadcast Storm Control

Select all ports ☒

Broadcast pkt/s

2 1000	4 1000	6 1000	8 1000	10 1000	12 1000
1 1000	3 1000	5 1000	7 1000	9 1000	11 1000

Unselected Selected

Previous Next Cancel

Each field is described in the following table.

Table 14 Wizard > Protection > Step 2 Broadcast Storm Control

LABEL	DESCRIPTION
Broadcast Storm Control	
Select all ports	Select all ports to apply settings on all ports. You can select a port by clicking it.
Broadcast pkt/s	Specify how many broadcast packets the port receives per second.
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 38 Wizard > Protection > Step 3 Summary

Summary

Loop Guard

2	4	6	8	10	12
☐	☐	☐	☐	☐	☐
1	3	5	7	9	11
☐	☐	☐	☐	☐	☐

Unselected Selected

Broadcast Storm Control

2	4	6	8	10	12
☒	☒	☒	☒	☒	☒
1000	1000	1000	1000	1000	1000
1	3	5	7	9	11
☒	☒	☒	☒	☒	☒
1000	1000	1000	1000	1000	1000

Unselected Selected

Previous Finish Cancel

Each field is described in the following table.

Table 15 Wizard > Protection > Step 3 Summary

LABEL	DESCRIPTION
Summary	
Loop Guard	If the loop guard feature is enabled on a port, the Switch will prevent loops on this port.
Broadcast Storm Control	If the broadcast storm control feature is enabled on a port, the number of broadcast packets the Switch receives per second will be limited on this port.
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.

4.4.3 VLAN

In VLAN, you can create VLAN, and tag VLAN settings.

Click **Wizard > VLAN > VLAN Setting** to access this screen.

Figure 39 Wizard > VLAN > VLAN Setting

VLAN

VLAN Setting

1 Create up to 5 VLANs by entering VLAN ID (2-4094)

Default VLAN 1 / Access Untagged port

port1 port2 port3 port4 port5
port6 port7 port8 port9 port10
port11 port12

Unselected Selected

VLAN member port

VLAN VLAN VLAN VLAN VLAN

Untagged Tagged

2 Select ports and specify VID for VLAN untagged member assignment

3 Select ports to be the Trunk tagged port member for all VLANs

Trunk Tagged port

Unselected Selected

Finish Cancel

Each field is described in the following table.

Table 16 Wizard > VLAN > VLAN Setting

LABEL	DESCRIPTION
VLAN Setting	
Default VLAN 1 / Access Untagged port	After you create a VLAN and select the VLAN ID from the drop-down list box, select ports and use the right arrow to add them as the untagged ports to a VLAN group.
VLAN member port	
VLAN	Type a number between 2 and 4094 to create a VLAN.
Trunk Tagged port	Select ports and use the downward arrow to add them as the tagged ports to the VLAN group(s) you created.
Finish	Review the information and click Finish to create the task.
Cancel	Click Cancel to exit this screen without saving.

4.4.4 QoS

In QoS, you can create QoS settings.

In order to create QoS settings, please do the following. Click **Wizard > QoS > QoS Setting** to access this screen.

Figure 40 Wizard > QoS > QoS Setting

Each field is described in the following table.

Table 17 Wizard > QoS > QoS Setting

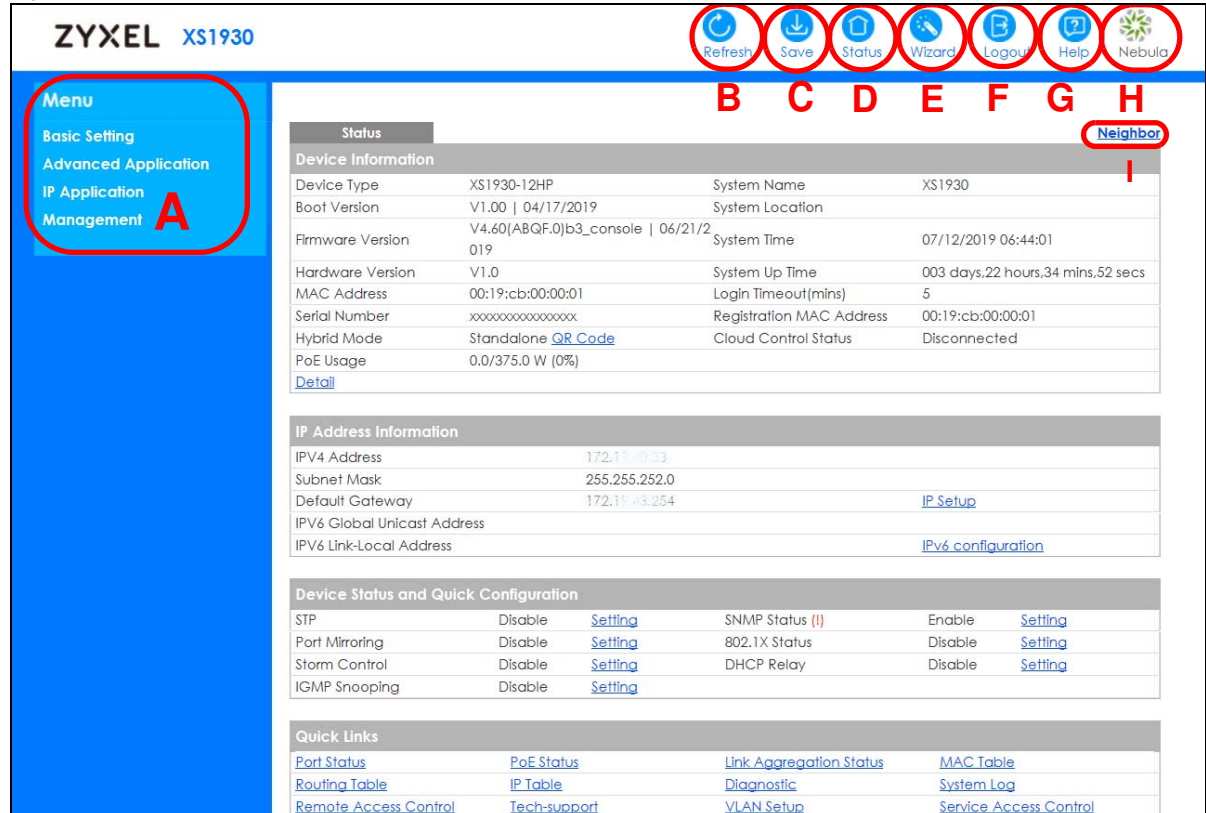
LABEL	DESCRIPTION
QoS Setting	
Select all ports	Select all ports to apply settings on all ports. You can select a port by clicking it.
High	Select ports and click the High button, so they will have high priority. The port's IEEE 802.1p priority level will be set to 5. Use Basic Setting > Port Setup to adjust the value.
Medium	Select ports and click the Medium button and, so they will have medium priority. The port's IEEE 802.1p priority level will be set to 3. Use Basic Setting > Port Setup to adjust the value.
Low	Select ports and click the Low button, so they will have low priority. The port's IEEE 802.1p priority level will be set to 1. Use Basic Setting > Port Setup to adjust the value.
Finish	Review the information and click Finish to create the task.
Cancel	Click Cancel to exit this screen without saving.

4.5 The Web Configurator Layout

This guide uses XS1930-12HP screens as an example. The screen may vary slightly for different models.

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

Figure 41 Web Configurator Layout for PoE model(s)



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

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

B - Click this link to update the information in the screen you are viewing currently.

C - Click this link to save your configuration into the Switch's nonvolatile memory. Nonvolatile memory is the configuration of your Switch that stays the same even if the Switch's power is turned off.

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

E - Click this icon to open the Wizard screen where you can configure the Switch's IP, login password, SNMP community, link aggregation, and so on.

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

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

H - Click this link to go to the NCC (Nebula Control Center) portal website.

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

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

Table 18 Navigation Panel Sub-links Overview

BASIC SETTING	ADVANCED APPLICATION	IP APPLICATION	MANAGEMENT
Menu Basic Setting Advanced Application IP Application Management System Info General Setup Switch Setup IP Setup Port Setup PoE Setup Interface Setup IPv6 DNS Cloud Management	Menu Basic Setting Advanced Application IP Application Management VLAN Static MAC Forwarding Static Multicast Forwarding Filtering Spanning Tree Protocol Bandwidth Control Broadcast Storm Control Mirroring Link Aggregation Port Authentication Port Security Time Range Classifier Policy Rule Queuing Method Multicast AAA Loop Guard Layer 2 Protocol Tunneling PPPoE Erdisable Green Ethernet LLDP	Menu Basic Setting Advanced Application IP Application Management Static Routing DHCP ARP Setup	Menu Basic Setting Advanced Application IP Application Management Maintenance Access Control Diagnostic System Log Syslog Setup Cluster Management MAC Table IP Table ARP Table Routing Table Path MTU Table Configure Clone IPv6 Neighbor Table Port Status

The following table describes the links in the navigation panel.

Table 19 Navigation Panel Links

LINK	DESCRIPTION
Basic Settings	
System Info	This link takes you to a screen that displays general system information.
General Setup	This link takes you to a screen where you can configure general identification information about the Switch.
Switch Setup	This link takes you to a screen where you can set up global Switch parameters such as VLAN type, GARP and priority queues.
IP Setup	This link takes you to a screen where you can configure the IP address and subnet mask (necessary for Switch management) and set up to 32 IP routing domains.
Port Setup	This link takes you to a screen where you can configure settings for individual Switch ports.
PoE Setup	For PoE model(s). This link takes you to a screen where you can set priorities, PoE power-up settings and schedule so that the Switch is able to reserve and allocate power to certain PDs.
Interface Setup	This link takes you to a screen where you can configure settings for individual interface type and ID.
IPv6	This link takes you to a screen where you can view IPv6 status and configure IPv6 settings.
DNS	This link takes you to a screen where you can configure DNS (domain name server) IP addresses.
Cloud Management	This screen displays a link to a screen where you can enable or disable the NCC Discovery feature. If it's enabled, you can have the Switch search for the NCC (Nebula Control Center). Another link takes you to a Nebula Switch Registration screen which has a QR code containing the Switch's serial number and MAC address for handy registration of the Switch at NCC.
Advanced Application	

Table 19 Navigation Panel Links (continued)

LINK	DESCRIPTION
VLAN	This link takes you to screens where you can configure port-based or 802.1Q VLAN (depending on what you configured in the Switch Setup menu). You can also configure a protocol based VLAN or a subnet based VLAN in these screens.
Static MAC Forwarding	This link takes you to a screen where you can configure static MAC addresses for a port. These static MAC addresses do not age out.
Static Multicast Forwarding	This link takes you to a screen where you can configure static multicast MAC addresses for port(s). These static multicast MAC addresses do not age out.
Filtering	This link takes you to a screen to set up filtering rules.
Spanning Tree Protocol	This link takes you to screens where you can configure the RSTP/MRSTP/MSTP to prevent network loops.
Bandwidth Control	This link takes you to a screen where you can configure bandwidth limits on the Switch.
Broadcast Storm Control	This link takes you to a screen to set up broadcast filters.
Mirroring	This link takes you to screens where you can copy traffic from one port or ports to another port in order that you can examine the traffic from the first port without interference.
Link Aggregation	This link takes you to screens where you can logically aggregate physical links to form one logical, higher-bandwidth link.
Port Authentication	This link takes you to a screen where you can configure IEEE 802.1x port authentication for clients communicating via the Switch.
Port Security	This link takes you to screens where you can activate MAC address learning and set the maximum number of MAC addresses to learn on a port.
Time Range	This link takes you to a screen where you can define different schedules.
Classifier	This link takes you to screens where you can configure the Switch to group packets based on the specified criteria.
Policy Rule	This link takes you to a screen where you can configure the Switch to perform special treatment on the grouped packets.
Queuing Method	This link takes you to a screen where you can configure queuing with associated queue weights for each port.
Multicast	This link takes you to screens where you can configure various multicast features, IGMP snooping, MLD snooping-proxy and create multicast VLANs.
AAA	This link takes you to a screen where you can configure authentication, authorization and accounting services via external servers. The external servers can be either RADIUS (Remote Authentication Dial-In User Service).
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.
Layer 2 Protocol Tunneling	This link takes you to a screen where you can configure L2PT (Layer 2 Protocol Tunneling) settings on the Switch.
PPPoE	This link takes you to screens where you can configure intermediate agent settings in port, VLAN, and PPPoE.
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.
Green Ethernet	This link takes you to a screen where you can configure green Ethernet settings in EEE, auto power down, and short reach for each port.
LLDP	This link takes you to screens where you can configure LLDP settings.
IP Application	
Static Routing	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 configuring the TCP/IP parameters manually.
DHCP	This link takes you to screens where you can configure the DHCP settings.

Table 19 Navigation Panel Links (continued)

LINK	DESCRIPTION
ARP Setup	This link takes you to screens where you can configure the ARP learning settings for each port.
Management	
Maintenance	This link takes you to screens where you can perform firmware and configuration file maintenance as well as reboot the system.
Access Control	This link takes you to screens where you can change the system login password and configure SNMP and remote management.
Diagnostic	This link takes you to a screen where you can ping IP addresses, run traceroute, test port(s) and show the Switch's location.
System Log	This link takes you to a screen where you can view system logs.
Syslog Setup	This link takes you to a screen where you can setup system logs and a system log server.
Cluster Management	This link takes you to screens where you can configure clustering management and view its status.
MAC Table	This link takes you to a screen where you can view the MAC addresses (and types) of devices attached to what ports and VLAN IDs.
IP Table	This link takes you to a screen where you can view the IP addresses and VLAN ID of a device attached to a port. You can also view what kind of device it is.
ARP Table	This link takes you to a screen where you can view the MAC addresses – IP address resolution table.
Routing Table	This link takes you to a screen where you can view the routing table.
Path MTU Table	This link takes you to a screen where you can view the path MTU aging time, index, destination address, MTU, and expire settings.
Configure Clone	This link takes you to a screen where you can copy attributes of one port to other ports.
IPv6 Neighbor Table	This link takes you to a screen where you can view the IPv6 neighbor table which includes index, interface, neighbor address, MAC address, status and type.
Port Status	This link takes you to a screen where you can view the port statistics.

4.5.1 Change Your Password

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

Figure 42 Change Administrator Login Password

The screenshot shows the 'Logins' configuration page. At the top, there is a 'Logins' tab and an 'Access Control' link. Below the tab is the 'Administrator' section. A red oval highlights the password change form, which includes three input fields: 'Old Password', 'New Password', and 'Retype to confirm'. Below this form is a warning message: 'Please record your new password whenever you change it. The system will lock you out if you have forgotten your password.' Below the warning is the 'Edit Logins' section, which contains a table with the following columns: 'Login', 'User Name', 'Password', 'Retype to confirm', and 'Privilege'. The table has 4 rows, numbered 1 to 4. At the bottom right of the page are 'Apply' and 'Cancel' buttons.

4.6 Saving Your Configuration

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

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

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

4.7 Switch Lockout

You could block yourself (and all others) from managing the Switch if you do one of the following:

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

Note: Be careful not to lock yourself and others out of the Switch.

4.8 Resetting the Switch

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

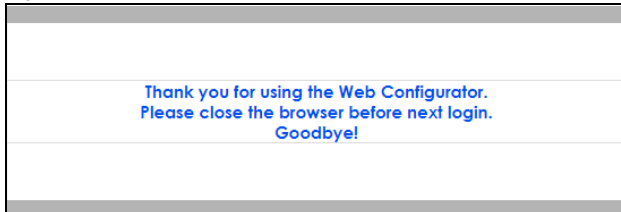
4.8.1 The Restore Button

See [Table 4 on page 31](#) to see how to use the **RESTORE** button to restore the factory default file.

4.9 Logging Out of the Web Configurator

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

Figure 43 Web Configurator: Logout Screen



4.10 Help

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

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

CHAPTER 5

Initial Setup Example

5.1 Overview

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

The following lists the configuration steps for the initial setup:

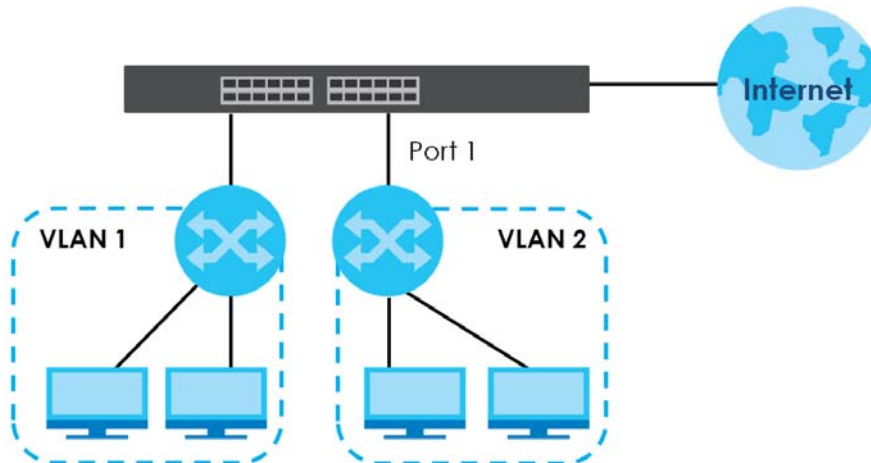
- Create a VLAN
- Set port VLAN ID
- Configure the Switch IP management address

5.1.1 Creating a VLAN

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

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

Figure 44 Initial Setup Network Example: VLAN



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

VLAN Configuration		VLAN Status
Static VLAN Setup	Click Here	
VLAN Port Setup	Click Here	
Voice VLAN Setup	Click Here	
Vendor ID Based VLAN Setup	Click Here	

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

Static VLAN		VLAN Configuration
ACTIVE	☒	
Name	VLAN2	
VLAN Group ID	2	

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

Add Cancel Clear

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

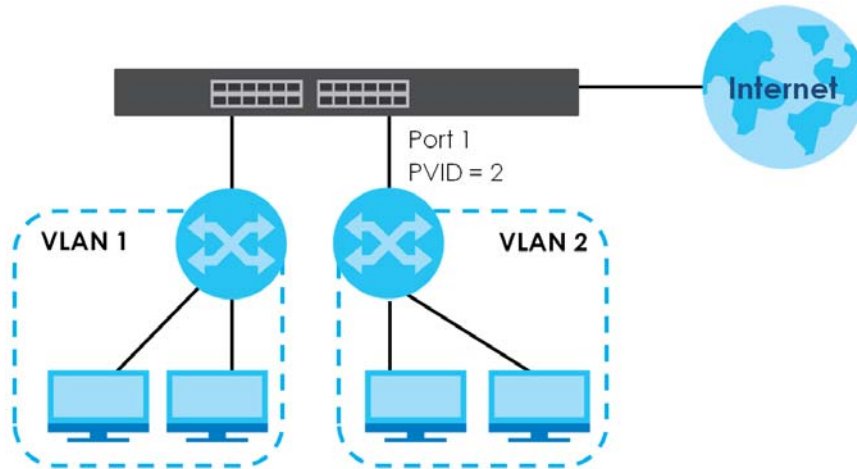
- 3 Since the **VLAN2** network is connected to port 1 on the Switch, select **Fixed** to configure port 1 to be a permanent member of the VLAN only.
- 4 To ensure that VLAN-unaware devices (such as computers and hubs) can receive frames properly, clear the **TX Tagging** check box to set the Switch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

5.1.2 Setting Port VID

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

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

Figure 45 Initial Setup Network Example: Port VID



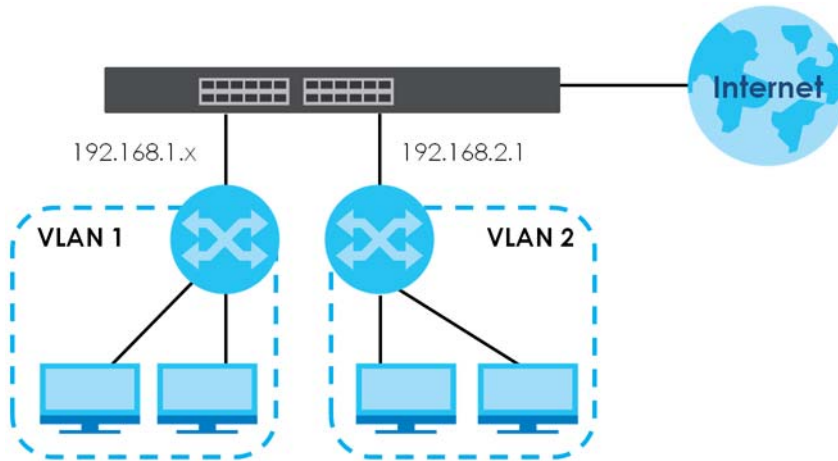
- 1 Click Advanced Applications > VLAN > VLAN Configuration in the navigation panel. Then click the VLAN Port Setup link.
- 2 Enter 2 in the PVID field for port 1 and click Apply to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned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

VLAN Port Setting							VLAN Configuration
GVRP							
Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking	Isolation	
*	☐		☐	All ☐	☐	☐	
1	☐	2	☐	All ☐	☐	☐	
2	☐	1	☐	All ☐	☐	☐	
3	☐	1	☐	All ☐	☐	☐	
4	☐	1	☐	All ☐	☐	☐	
5	☐	1	☐	All ☐	☐	☐	
6	☐	1	☐	All ☐	☐	☐	
7	☐	1	☐	All ☐	☐	☐	
8	☐	1	☐	All ☐	☐	☐	
9	☐	1	☐	All ☐	☐	☐	
10	☐	1	☐	All ☐	☐	☐	
11	☐	1	☐	All ☐	☐	☐	
12	☐	1	☐	All ☐	☐	☐	

5.2 Configuring 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 46 Initial Setup Example: Management IP Address



- 1 Connect your computer to any Ethernet port on the Switch. Make sure your computer is in the same subnet as the Switch.
- 2 Open your web browser and enter 192.168.1.1 (the default IP address) in the address bar to access the web configurator. See [Section 4.2 on page 39](#) for more information.
- 3 Click **Basic Setting > IP Setup > IP Configuration** in the navigation panel.
- 4 Configure the related fields in the IP Configuration screen.
- 5 For the VLAN2 network, enter 192.168.2.1 as the IP address and 255.255.255.0 as the subnet mask.
- 6 In the VID field, enter the ID of the VLAN group to which you want this management IP address to belong. This is the same as the VLAN ID you configure in the **Static VLAN** screen.
- 7 Click **Add** to save your changes back to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

The screenshot shows the 'IP Configuration' web interface. The 'Static IP Address' section is highlighted with a red box. It contains the following fields:

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

Below the form is a table listing configured IP addresses:

Index	IP Address	IP Subnet Mask	VID	Type
1	192.168.1.1	255.255.252.0	1	DHCP
2	192.168.2.1	255.255.255.0	2	Static

CHAPTER 6

DHCP Relay Tutorial

6.1 Overview

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

- [How to Use DHCPv4 Relay on the Switch](#)

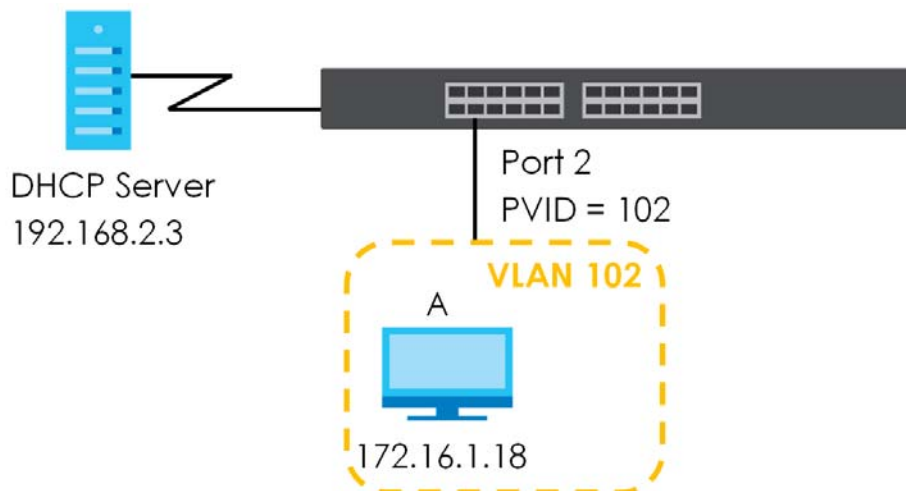
6.2 How to Use DHCPv4 Relay on the Switch

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

6.2.1 DHCP Relay Tutorial Introduction

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

Figure 47 Tutorial: DHCP Relay Scenario



6.2.2 Creating a VLAN

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

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

Figure 48 Tutorial: Set VLAN Type to 802.1Q

The screenshot shows the 'Switch Setup' web interface. The 'VLAN Type' section is highlighted with a red circle, showing two radio buttons: '802.1Q' (selected) and 'Port Based'. Below this, there are several configuration fields:

MAC Address Learning	Aging Time	300	seconds
ARP Aging Time	Aging Time	300	seconds
GARP Timer	Join Timer	200	milliseconds
	Leave Timer	600	milliseconds
	Leave All Timer	10000	milliseconds
Priority Queue Assignment	Priority7	7	
	Priority6	6	
	Priority5	5	
	Priority4	4	
	Priority3	3	
	Priority2	1	
	Priority1	0	
	Priority0	2	

At the bottom of the interface, there are two buttons: 'Apply' and 'Cancel'.

- 3 Click **Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup**.
- 4 In the **Static VLAN** screen, select **ACTIVE**, enter a descriptive name (VLAN 102 for example) in the Name field and enter 102 in the **VLAN Group ID** field. Use the default VLAN type, **Normal**, in the **VLAN Type** field.
- 5 Select **Fixed** to configure port 2 to be a permanent member of this VLAN.
- 6 Clear the **TX Tagging** check box to set the Switch to remove VLAN tags before sending.
- 7 Click **Add** to save the settings to the run-time memory. Settings in the run-time memory are lost when the Switch's power is turned off.

Figure 49 Tutorial: Create a Static VLAN

Static VLAN [VLAN Configuration](#)

ACTIVE ☒

Name

VLAN Group ID

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

[Add](#) [Cancel](#) [Clear](#)

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

Figure 50 Tutorial: Click the VLAN Port Setting Link

VLAN Configuration [VLAN Status](#)

Static VLAN Setup [Click Here](#)

VLAN Port Setup [Click Here](#)

Voice VLAN Setup [Click Here](#)

Vendor ID Based VLAN Setup [Click Here](#)

- 9 Enter 102 in the **PVID** field for port 2 to add a tag to incoming untagged frames received on that port so that the frames are forwarded to the VLAN group that the tag defines.
- 10 Click **Apply** to save your changes back to the run-time memory.

Figure 51 Tutorial: Add Tag for Frames Received on Port 2

VLAN Port Setting [VLAN Configuration](#)

GVRP ☐

Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking	Isolation
*	☐		☐	All ▼	☐	☐
1	☐	1	☐	All ▼	☐	☐
2	☐	102	☐	All ▼	☐	☐
3	☐	1	☐	All ▼	☐	☐
4	☐	1	☐	All ▼	☐	☐
5	☐	1	☐	All ▼	☐	☐
6	☐	1	☐	All ▼	☐	☐
7	☐	1	☐	All ▼	☐	☐
8	☐	1	☐	All ▼	☐	☐
9	☐	1	☐	All ▼	☐	☐
10	☐	1	☐	All ▼	☐	☐
11	☐	1	☐	All ▼	☐	☐
12	☐	1	☐	All ▼	☐	☐

[Apply](#) [Cancel](#)

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

6.2.3 Configuring DHCPv4 Relay

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

- 1 Click IP Application > DHCP > DHCPv4 and then the Global link to open the DHCP Relay screen.
- 2 Select the **Active** check box.
- 3 Enter the DHCP server's IP address (192.168.2.3 in this example) in the **Remote DHCP Server 1** field.
- 4 Select default1 or default2 in the **Option 82 Profile** field.
- 5 Click **Apply** to save your changes back to the run-time memory.

Figure 52 Tutorial: Set DHCP Server and Relay Information

DHCP Relay [Status](#) [Port](#)

Active ☒

Remote DHCP Server 1 192.168.2.3

Remote DHCP Server 2 0.0.0.0

Remote DHCP Server 3 0.0.0.0

Option 82 Profile default1 ▼

[Apply](#) [Cancel](#)

- 6 Click the **Save** link in the upper right corner of the web configurator to save your configuration permanently.
- 7 The DHCP server can then assign a specific IP address based on the DHCP request.

6.2.4 Troubleshooting

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

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

CHAPTER 7

Status

7.1 Overview

This chapter describes the screens for System Status and Neighbor.

7.1.1 What You Can Do

- Use the **Status** screen ([Section 7.2 on page 73](#)) to see the Switch's general device information, system status, and IP addresses. You can also display other status screens for more information.
- Use the **Neighbor** screen ([Section 7.2.1 on page 75](#)) to view and manage Switch's neighbor devices.

7.2 Status

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

Figure 53 Status (for PoE model(s))

Status

Neighbor

Device Information

Device Type

XS1930-12HP

System Name

XS1930

Boot Version

V1.00 | 04/17/2019

System Location

Firmware Version

V4.60(ABQF.0)b3_console | 06/21/2019

System Time

07/12/2019 06:44:01

Hardware Version

V1.0

System Up Time

003 days,22 hours,34 mins,52 secs

MAC Address

00:19:cb:00:00:01

Login Timeout(mins)

5

Serial Number

xxxxxxxxxxxxxx

Registration MAC Address

00:19:cb:00:00:01

Hybrid Mode

Standalone [QR Code](#)

Cloud Control Status

Disconnected

PoE Usage

0.0/375.0 W (0%)

Detail

IP Address Information

IPv4 Address

172.17.43.23

Subnet Mask

255.255.252.0

Default Gateway

172.17.43.254

[IP Setup](#)

IPv6 Global Unicast Address

IPv6 Link-Local Address

[IPv6 configuration](#)

Device Status and Quick Configuration

STP

Disable

[Setting](#)

SNMP Status (I)

Enable

[Setting](#)

Port Mirroring

Disable

[Setting](#)

802.1X Status

Disable

[Setting](#)

Storm Control

Disable

[Setting](#)

DHCP Relay

Disable

[Setting](#)

IGMP Snooping

Disable

[Setting](#)

Quick Links

[Port Status](#)

[PoE Status](#)

[Link Aggregation Status](#)

[MAC Table](#)

[Routing Table](#)

[IP Table](#)

[Diagnostic](#)

[System Log](#)

[Remote Access Control](#)

[Tech-support](#)

[VLAN Setup](#)

[Service Access Control](#)

The following table describes the labels in this screen.

Table 20 Status

LABEL	DESCRIPTION
Device Information	
Device Type	This field displays the model name of this Switch.
System Name	This field displays the name used to identify the Switch on any network.
Boot Version	This field displays the version number and date of the boot module that is currently on the Switch.
System Location	This field displays the geographic location of your Switch. You can change the setting in the Basic Setting > General Setup screen.
Firmware Version	This field displays the version number and date of the firmware the Switch is currently running.
System Time	This field displays the current date and time in the Switch. The format is mm-dd-yyyy hh:mm:ss.
Hardware Version	This field displays the hardware version number of the Switch. The integer is the generation number of the Switch series, and the decimal is the version of the hardware change. For example, V1.0 is a hardware version for the Switch where 1 identifies the first generation of the Switch series, and .0 is the first hardware change.
System Up Time	This field displays how long the Switch has been running since it last restarted or was turned on.
MAC Address	This field displays the MAC addresses of the Switch.
Login Timeout	This field displays how many minutes a management session can be left idle before the session times out. After it times out you have to log in with your password again.

Table 20 Status (continued)

LABEL	DESCRIPTION
Serial Number	This field displays the serial number of this Switch. The serial number is used for device tracking and control.
Registration MAC Address	This field displays the MAC address of the Switch that you must use to register at myZyxel.com or the NCC (Nebula Control Center).
Hybrid Mode	This field is available only when Nebula Control Center Discovery is enabled on the Switch. This field displays whether the Switch is in Standalone mode or Cloud mode. In Standalone mode you can see a link to a QR code to register the Switch to use NCC (Nebula Control Center).
Cloud Control Status	This field is available only when Nebula Control Center Discovery is enabled on the Switch. This field displays the registration and connection status between the Switch and the NCC (Nebula Control Center). See Section 3.3 on page 35 for more information on the Cloud LED. In Standalone mode, the status will display Disconnected or Unregistered . In Cloud mode the status will display Connected or Disconnected . Connected - The Switch is registered with and connected to the NCC. Disconnected - The Switch is not connected to the NCC. Unregistered - The Switch is not registered with the NCC.
PoE Usage	This field displays the amount of power the Switch is currently supplying to the connected PoE-enabled devices and the total power the Switch can provide to the connected PDs. It also shows the percentage of PoE power usage. When PoE usage reaches 100%, the Switch will shut down PDs one-by-one according to the PD priority which you configured in Basic Setting > PoE Setup .
Detail	Click this link to go to the Basic Setting > System Info screen to check other detailed information, such as system resource usage and the Switch temperature, fan speeds or voltage.
IP Address Information	
IPv4 Address	This field displays the Switch's current IPv4 address.
Subnet Mask	This field displays the Switch's subnet mask.
Default Gateway	This field displays the IP address of the Switch's default gateway.
IP Setup	Click the link to go to the Basic Setting > IP Setup screen.
IPv6 Global Unicast Address	This field displays the Switch's IPv6 global unicast address
IPv6 Link-Local Address	This field displays the Switch's IPv6 link-local address.
IPv6 configuration	Click the link to go to the Basic Setting > IPv6 screen.
Device Status and Quick Configuration	This section shows whether a feature is enabled or not on the Switch. You can click a feature's Setting link to go to the configuration screen for the feature. Hover your cursor over a red exclamation mark to display information about the feature.
Quick Links	This section provides the shortcut link to a specific configuration screen.

7.2.1 Neighbor Screen

The neighbor screen allows you to view and manage the Switch's neighboring devices more conveniently. It uses Layer Link Discovery Protocol (LLDP) to discover all neighbor devices connected to the Switch including non-Zyxel devices. You can perform tasks on the neighboring devices like login, reboot (turn the power off and then back on again), and reset to factory default settings in the Neighbor screen. For more information on LLDP, see [Section 31.1 on page 235](#).

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

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

Figure 54 Status > Neighbor

Switch Neighbor								Status	Neighbor Detail
Port	Port Name	Link	PoE Draw (W)	System Name	IP	PWR Cycle	Reset to Default		
1	--	Down	0.0	--	--	Cycle	Reset		
2	--	Down	0.0	--	--	Cycle	Reset		
3	--	Down	0.0	--	--	Cycle	Reset		
4	--	Down	0.0	--	--	Cycle	Reset		
5	--	1G/F	8.5	NWA5123-AC-HD		Cycle	Reset		
6	--	Down	0.0	--	--	Cycle	Reset		
7	--	1G/F	0.0	--	--	Cycle	Reset		
8	--	Down	0.0	--	--	Cycle	Reset		
9	--	Down	0.0	--	--	Cycle	Reset		
10	--	Down	0.0	--	--	Cycle	Reset		
11	--	Down	0.0	--	--	Cycle	Reset		
12	--	Down	0.0	--	--	Cycle	Reset		

Flush

The following table describes the fields in the above screen.

Table 21 Status > Neighbor

LABEL	DESCRIPTION
Port	This shows the port of the Switch, on which the neighboring device is discovered.
Port Name	This shows the port description of the Switch.
Link	This shows the speed (either 100M for 100Mbps, 1G for 1 Gbps, 2.5G for 2.5 Gbps, 5G for 5 Gbps, or 10G for 10 Gbps) and the duplex (F for full duplex or H for half). This field displays Down if the port is not connected to any device.
PoE Draw (W)	This shows the consumption that the neighboring device connected to this port draws from the Switch. This allows you to plan and use within the power budget of the Switch.
System Name	This shows the system name of the neighbor device.
IP	This shows the IP address of the neighbor device. The IP address is a hyper link that you can click to log into and manage the neighbor device through its web configurator.
PWR Cycle	Click the Cycle button to turn OFF the power of the neighboring device and turn it back ON again. A count down button (from 5 to 0) starts. Note: The Cycle button is clickable only when the neighboring device is a powered device (PD) and able to receive power from the Switch.
Reset to Default	Click the Reset button to reset the neighboring device to its factory default settings. A warning message "Are you sure you want to load factory default?" appears, prompting you to confirm the action. After confirming the action a count down button (from 5 to 0) starts. Note: - The Switch must be a Power Sourcing Equipment (PSE) and the neighboring device is a powered device (PD). - If multiple neighboring devices use the same port, the Reset button is not available. - You can only reset Zyxel powered devices that support the ZON utility.

Table 21 Status > Neighbor

LABEL	DESCRIPTION
	Select an entry's check box to select a specific port. Otherwise, select the check box in the table heading row to select all ports.
Flush	Click the Flush button to remove information about neighbors learned on the selected ports.

7.2.2 Neighbor Detail

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

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

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

Figure 55 Status > Neighbor > Neighbor Detail

The screenshot shows the 'Switch Neighbor Detail' screen. It features a table with columns for port details and a 'Switch Neighbor' link. The table lists ports 1 through 12, with columns for Desc., Link, PoE Draw (W), and PWR Cycle. Ports 1-4 and 6-12 show 'Down' link status and 0.0 W power draw. Port 5 shows '1G/F' link status and 7.9 W power draw. A 'Remote' section provides details for a device connected to Port 1, including System Name, Model, Firmware, IP, Port 1 details, and MAC address. A 'Reset' button is visible next to the MAC address.

Switch Neighbor Detail							Switch Neighbor
Local Port 1							
Desc.	--	Link	Down	PoE Draw (W)	0.0	PWR Cycle	☐
Local Port 2							
Desc.	--	Link	Down	PoE Draw (W)	0.0	PWR Cycle	☐
Local Port 3							
Desc.	--	Link	Down	PoE Draw (W)	0.0	PWR Cycle	☐
Local Port 4							
Desc.	--	Link	Down	PoE Draw (W)	0.0	PWR Cycle	☐
Local Port 5							
Desc.	--	Link	1G/F	PoE Draw (W)	7.9	PWR Cycle	☒
Remote							
System Name	NWA5123-AC-HD	Model	NWA5123-AC-HD	Firmware	V5.30(ABIM.0)b4	IP	172.17.4.11
Port 1	Desc. UPLINK	Location	--	MAC	60-31-97-0F-8D-C4	Reset to Default	Reset
Local Port 6							
Desc.	--	Link	Down	PoE Draw (W)	0.0	PWR Cycle	☐
Local Port 7							
Desc.	--	Link	1G/F	PoE Draw (W)	0.0	PWR Cycle	☐
Local Port 8							
Desc.	--	Link	Down	PoE Draw (W)	0.0	PWR Cycle	☐
Local Port 9							
Desc.	--	Link	Down	PoE Draw (W)	0.0	PWR Cycle	☐
Local Port 10							
Desc.	--	Link	Down	PoE Draw (W)	0.0	PWR Cycle	☐
Local Port 11							
Desc.	--	Link	Down	PoE Draw (W)	0.0	PWR Cycle	☐
Local Port 12							
Desc.	--	Link	Down	PoE Draw (W)	0.0	PWR Cycle	☐

The following table describes the fields in the above screen.

Table 22 Status > Neighbor > Neighbor Detail

LABEL	DESCRIPTION
Local Port	This shows the port of the Switch, on which the neighboring device is discovered.
Desc.	This shows the port description of the Switch.
Link	This shows the speed (either 100M for 100Mbps, 1G for 1 Gbps, 2.5G for 2.5 Gbps, 5G for 5 Gbps, or 10G for 10 Gbps) and the duplex (F for full duplex or H for half). This field displays Down if the port is not connected to any device.
PoE Draw (W)	This shows the consumption that the neighboring device connected to this port draws from the Switch. This allows you to plan and use within the power budget of the Switch.

Table 22 Status > Neighbor > Neighbor Detail

LABEL	DESCRIPTION
PWR Cycle	Click the Cycle button to turn OFF the power of the neighboring device and turn it back ON again. A count down button (from 5 to 0) starts. Note: The Cycle button is clickable only when the neighboring device is a powered device (PD) and able to receive power from the Switch.
Remote	
System Name	This shows the system name of the neighbor device.
Model	This shows the model name of the neighbor device. This field will show "--" for devices that do not support the ZON utility.
Firmware	This shows the firmware version of the neighbor device. This field will show "--" for devices that do not support the ZON utility.
IP	This shows the IP address of the neighbor device. The IP address is a hyper link that you can click to log into and manage the neighbor device through its web configurator.
Port	This shows the number of the neighbor device's port which is connected to the Switch.
Desc.	This shows the description of the neighbor device's port which is connected to the Switch.
Location	This shows the geographic location of the neighbor device. This field will show "--" for devices that do not support the ZON utility.
MAC	This shows the MAC address of the neighbor device.
Reset to Default	Click the Reset button to reset the neighboring device to its factory default settings. A warning message "Are you sure you want to load factory default?" appears, prompting you to confirm the action. After confirming the action a count down button (from 5 to 0) starts. Note: • The Switch must be a Power Sourcing Equipment (PSE) and the neighboring device is a powered device (PD). • If multiple neighbor devices use the same port, the Reset button is not available. • You can only reset Zyxel powered devices that support the ZON utility.

CHAPTER 8

Basic Setting

8.1 Overview

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

8.1.1 What You Can Do

- Use the **System Info** screen ([Section 8.2 on page 79](#)) to check the firmware version number and monitor the Switch temperature, fan speeds and voltage.
- Use the **General Setup** screen ([Section 8.3 on page 81](#)) to configure general settings such as the system name and time.
- Use the **Switch Setup** screen ([Section 8.5 on page 84](#)) to choose your VLAN type, set the GARP timers and assign priorities to queues.
- Use the **IP Setup** screen ([Section 8.6 on page 85](#)) to configure the Switch IP address, default gateway device, and the management VLAN ID.
- Use the **Port Setup** screen ([Section 8.7 on page 89](#)) to configure Switch port settings.
- Use the **PoE Setup** screens ([Section 8.8 on page 90](#)) to view the current amount of power that PDs are receiving from the Switch and set the priority levels for the Switch in distributing power to PDs. This screen is available for PoE model(s) only.
- Use the **Interface Setup** screens ([Section 8.9 on page 97](#)) to configure Switch interface type and interface ID settings.
- Use the **IPv6** screens ([Section 8.10 on page 98](#)) to view IPv6 status and IPv6 configuration.
- Use the **DNS** screen ([Section 8.11 on page 111](#)) to configure the default domain name server.
- Use the **Cloud Management** screen ([Section 8.12 on page 112](#)) to display links to **Nebula Control Center Discovery** and **Nebula Switch Registration** screens.

8.2 System Information

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

Figure 56 Basic Setting > System Info

System Info	
System Name	XS1930
Product Model	XS1930-12HP
ZyNOS F/W Version	V4.60[ABQF.0]b3_console 06/21/2019
Ethernet Address	00:19:cb:00:00:01

CPU Utilization	
Current (%)	18.17

Memory Utilization			
Name	Total (byte)	Used (byte)	Utilization (%)
common	68740608	7334512	10

Hardware Monitor					
Temperature Unit C					
Temperature (C)	Current	MAX	MIN	Threshold	Status
MAC	48.0	53.0	0.0	85.0	Normal
BOARD	43.0	48.0	30.0	110.0	Normal
PHY	49.0	54.0	29.0	85.0	Normal
FAN Speed (RPM)	Current	MAX	MIN	Threshold	Status
FAN1	4415	4503	4195	500	Normal
FAN2	4358	4429	4195	500	Normal
Voltage (V)	Current	MAX	MIN	Threshold	Status
3.3V	3.257	3.257	3.257	+6%/-6%	Normal
12V	11.843	11.906	11.781	+10%/-10%	Normal

The following table describes the labels in this screen.

Table 23 Basic Setting > System Info

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

Table 23 Basic Setting > System Info (continued)

LABEL	DESCRIPTION
Current	This shows the current temperature at this sensor.
MAX	This field displays the maximum temperature measured at this sensor.
MIN	This field displays the minimum temperature measured at this sensor.
Threshold	This field displays the upper temperature limit at this sensor.
Status	This field displays Normal for temperatures below the threshold and Error for those above.
FAN Speed (RPM)	A properly functioning fan is an essential component (along with a sufficiently ventilated, cool operating environment) in order for the device to stay within the temperature threshold. Each fan has a sensor that is capable of detecting and reporting if the fan speed falls below the threshold shown.
Current	This field displays this fan's current speed in Revolutions Per Minute (RPM).
MAX	This field displays this fan's maximum speed measured in Revolutions Per Minute (RPM).
MIN	This field displays this fan's minimum speed measured in Revolutions Per Minute (RPM). "<41" is displayed for speeds too small to measure (under 2000 RPM).
Threshold	This field displays the minimum speed at which a normal fan should work.
Status	Normal indicates that this fan is functioning above the minimum speed. Error indicates that this fan is functioning below the minimum speed.
Voltage(V)	The power supply for each voltage has a sensor that is capable of detecting and reporting if the voltage falls out of the tolerance range.
Current	This is the current voltage reading.
MAX	This field displays the maximum voltage measured at this point.
MIN	This field displays the minimum voltage measured at this point.
Threshold	This field displays the percentage tolerance of the voltage with which the Switch still works.
Status	Normal indicates that the voltage is within an acceptable operating range at this point; otherwise Error is displayed.

8.3 General Setup

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

Figure 57 Basic Setting > General Setup

General Setup	
System Name	XS1930
Location	
Contact Person's Name	
Use Time Server when Bootstrap	Daytime(RFC-867) ▼
Time Server IP Address	1.pool.ntp.org
Current Time	09 : 18 : 36 UTC+08:00
New Time (hh:mm:ss)	09 : 18 : 36
Current Date	2019 - 07 - 16
New Date (yyyy-mm-dd)	2019 - 07 - 16
Time Zone	UTC+08:00 ▼
Daylight Saving Time	☐
Start Date	First ▼ Sunday ▼ of January ▼ at 0:00 ▼
End Date	First ▼ Sunday ▼ of January ▼ at 0:00 ▼
It will take 60 seconds if time server is unreachable.	
Apply Cancel	

The following table describes the labels in this screen.

Table 24 Basic Setting > General Setup

LABEL	DESCRIPTION
System Name	Choose a descriptive name for identification purposes. This name consists of up to 64 printable characters; spaces are allowed.
Location	Enter the geographic location of your Switch. You can use up to 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 Bootstrap	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 2016/1/1 at 0:0:0. NTP (RFC-1305) is similar to Time (RFC-868). If you select None, enter the time manually. Each time you turn on the Switch, the time and date will be reset to 2016-1-1 0:0:0.
Time Server IP Address	Enter the IP address or domain name of your timeserver. The Switch searches for the timeserver for up to 60 seconds. If you select a timeserver that is unreachable, then this screen will appear locked for 60 seconds. Please wait.
Current Time	This field displays the time you open this menu (or refresh the menu).
New Time (hh:min:ss)	Enter the new time in hour, minute and second format. The new time then appears in the Current Time field after you click Apply .
Current Date	This field displays the date you open this menu.
New Date (yyyy-mm-dd)	Enter the new date in year, month and day format. The new date then appears in the Current Date field after you click Apply .

Table 24 Basic Setting > General Setup (continued)

LABEL	DESCRIPTION
Time Zone	Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone from the drop-down list box.
Daylight Saving Time	Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time.
Start Date	Configure the day and time when Daylight Saving Time starts if you selected Daylight Saving Time . The time is displayed in the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select Second, Sunday, March and 2:00. Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, March and the last field depends on your time zone. In Germany for instance, you would select 2:00 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
End Date	Configure the day and time when Daylight Saving Time ends if you selected Daylight Saving Time . The time field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the first Sunday of November. Each time zone in the United States stops using Daylight Saving Time at 2 A.M. local time. So in the United States you would select First, Sunday, November and 2:00. Daylight Saving Time ends in the European Union on the last Sunday of October. All of the time zones in the European Union stop using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, October and the last field depends on your time zone. In Germany for instance, you would select 2:00 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1).
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

8.4 Introduction to VLANs

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

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

See [Chapter 9 on page 114](#) for information on port-based and 802.1Q tagged VLANs.

8.5 Switch Setup

Click **Basic Setting > Switch Setup** in the navigation panel to display the screen as shown. The VLAN setup screens change depending on whether you choose **802.1Q** or **Port Based** in the **VLAN Type** field in this screen. Refer to [Chapter 9 on page 114](#) for more information on VLAN.

Figure 58 Basic Setting > Switch Setup

The following table describes the labels in this screen.

Table 25 Basic Setting > Switch Setup

LABEL	DESCRIPTION
VLAN Type	Choose 802.1Q or Port Based . The VLAN Setup screen changes depending on whether you choose 802.1Q VLAN type or Port Based VLAN type in this screen. See Chapter 9 on page 114 for more information.
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.

Table 25 Basic Setting > Switch Setup (continued)

LABEL	DESCRIPTION
Leave Timer	Leave Time sets the duration of the Leave Period timer for GVRP in milliseconds. Each port has a single Leave Period timer. Leave Time must be two times larger than Join Timer ; the default is 600 milliseconds.
Leave All Timer	Leave All Timer sets the duration of the Leave All Period timer for GVRP in milliseconds. Each port has a single Leave All Period timer. Leave All Timer must be larger than Leave Timer.
Priority Queue Assignment IEEE 802.1p defines up to eight separate traffic types by inserting a tag into a MAC-layer frame that contains bits to define class of service. Frames without an explicit priority tag are given the default priority of the ingress port. Use the next fields to configure the priority level-to-physical queue mapping. The Switch has eight physical queues that you can map to the 8 priority levels. On the Switch, traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested. Priority Level (The following descriptions are based on the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).	
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.

8.6 IP Setup

Use the **IP Setup** screen to view the Switch IP address(es) and the management VLAN ID.

8.6.1 Management IP Addresses (IP Interfaces)

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

On the Switch, an IP address is not bound to any physical port. 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 32 IP addresses (domains) which are used to access and manage the Switch from the ports belonging to the pre-defined VLAN(s).

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

Figure 59 Basic Setting > IP Setup

IP Status			IP Configuration			
Index	IP Address	IP Subnet Mask	VID	Type	Renew	Release
1	172.17.4.33	255.255.252.0	1	DHCP	Click	Click
2	192.168.1.1	255.255.255.0	1	Static		

The following table describes the labels in this screen.

Table 26 Basic Setting > IP Setup

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

8.6.2 IP Status Details

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

Figure 60 Basic Setting > IP Setup > IP Status Details: Static

IP Status Detail		IP Status
Type	Static	
VID	1	
IP Address	192.168.1.1	
IP Subnet Mask	255.255.255.0	

The following table describes the labels in this screen.

Table 27 Basic Setting > IP Setup > IP Status Details: Static

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

Figure 61 Basic Setting > IP Setup > IP Status Details: DHCP

IP Status Detail		IP Status
Type	DHCP	
VID	1	
IP Address	172.16.0.33	
IP Subnet Mask	255.255.252.0	
Lease Time	86400 seconds	
Renew Time	43200 seconds	
Rebind Time	75600 seconds	
Lease Time Start	2019-07-16 08:30:41	
Lease Time End	2019-07-17 08:30:41	
Default Gateway	172.16.0.254	
DNS Server	172.16.0.1	
DNS Server	172.16.0.1	

The following table describes the labels in this screen.

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

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

8.6.3 IP Configuration

Use this screen to configure the default gateway device and add IP domains. The default gateway specifies the IP address of the default gateway (next hop) for outgoing traffic.

Figure 62 Basic Setting > IP Setup > IP Configuration

IP Configuration [IP Status](#)

Default Gateway: 0.0.0.0

[Apply](#) [Cancel](#)

IP Interface

IP Address: ☒ DHCP Client ☐ Static IP Address

IP Address: 0.0.0.0

IP Subnet Mask: 0.0.0.0

VID:

[Add](#) [Cancel](#)

Index	IP Address	IP Subnet Mask	VID	Type	
1	192.168.1.1	255.255.252.0	1	DHCP	☐
2	192.168.1.1	255.255.255.0	1	Static	☐

[Delete](#) [Cancel](#)

The following table describes the labels in this screen.

Table 29 Basic Setting > IP Setup > IP Configuration

LABEL	DESCRIPTION
Default Gateway	Type the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
IP Interface	
Use these fields to create or edit IP routing domains on the Switch.	
DHCP Client	Select this option if you have a DHCP server that can assign the Switch an IP address, subnet mask, a default gateway IP address and a domain name server IP address automatically.
Static IP Address	Select this option if you don't have a DHCP server or if you wish to assign static IP address information to the Switch. You need to fill in the following fields when you select this option.
IP Address	Enter the IP address of your Switch in dotted decimal notation, for example, 192.168.1.1. This is the IP address of the Switch in an IP routing domain.
IP Subnet Mask	Enter the IP subnet mask of an IP routing domain in dotted decimal notation, for example, 255.255.255.0.
VID	Enter the VLAN identification number to which an IP routing domain belongs.
Add	Click this to create a new entry. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Index	This field displays the index number of an entry.
IP Address	This field displays IP address of the Switch in the IP domain.
IP Subnet Mask	This field displays the subnet mask of the Switch in the IP domain.
VID	This field displays the VLAN identification number of the IP domain on the Switch.

Table 29 Basic Setting > IP Setup > IP Configuration (continued)

LABEL	DESCRIPTION
Type	This field displays the type of IP address status.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click Delete to remove the selected entry from the summary table. Note: Deleting all IP subnets locks you out of the Switch.
Cancel	Click Cancel to clear the check boxes.

8.7 Port Setup

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

Figure 63 Basic Setting > Port Setup

Port	Active	Name	Speed / Duplex	Flow Control	802.1p Priority	Media Type
*	☐		Auto	☐	0	sfp_plus
1	☒		Auto	☐	0	
2	☒		Auto	☐	0	
3	☒		Auto	☐	0	
4	☒		Auto	☐	0	
5	☒		Auto	☐	0	
6	☒		Auto	☐	0	
7	☒		Auto	☐	0	
8	☒		Auto	☐	0	
9	☒		Auto	☐	0	
10	☒		Auto	☐	0	
11	☒		Auto	☐	0	sfp_plus
12	☒		Auto	☐	0	sfp_plus

Apply Cancel

The following table describes the labels in this screen.

Table 30 Basic Setting > Port Setup

LABEL	DESCRIPTION
Port	This is the port index number. * means all ports.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable a port. The factory default for all ports is enabled. A port must be enabled for data transmission to occur.

Table 30 Basic Setting > Port Setup (continued)

LABEL	DESCRIPTION
Name	Enter a descriptive name that identifies this port. You can enter up to 64 alpha-numerical characters. Note: Due to space limitation, the port name may be truncated in some web configurator screens.
Speed/Duplex	Select the speed and the duplex mode of the Ethernet connection on this port. The choices are Auto, Auto-1G, 2.5G / Full Duplex, 5G / Full Duplex, and 100M / Full Duplex for a 100Base-T connection. 1G / Full Duplex is supported by both 1000Base-T and 1000Base-X connections. 10G / Full Duplex is supported by the 10 Gigabit Ethernet connections on the Switch that has a 10 Gigabit interface. Selecting Auto-1G or 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 autonegotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the Switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect.
Flow Control	A concentration of traffic on a port decreases port bandwidth and overflows buffer memory causing packet discards and frame losses. Flow Control is used to regulate transmission of signals to match the bandwidth of the receiving port. The Switch uses IEEE802.3x flow control in full duplex mode and backpressure flow control in half duplex mode. IEEE802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill. Back Pressure flow control is typically used in half duplex mode to send a "collision" signal to the sending port (mimicking a state of packet collision) causing the sending port to temporarily stop sending signals and resend later. Select Flow Control to enable it.
802.1p Priority	This priority value is added to incoming frames without a (802.1p) priority queue tag. See Priority Queue Assignment in Table 25 on page 84 for more information.
Media Type	On the Switch that has a 10 Gigabit interface, such as the SFP+ slot, you can insert either an SFP+ transceiver or an SFP+ Direct Attach Copper (DAC). An SFP+ Direct Attach Copper (DAC) is an SFP+ housing that has no optical module but uses a fixed-length passive copper cable assembly, which reduces cost and power significantly. Select the media type (sfp_plus or dac 10g) of the SFP+ module that is attached to the 10 Gigabit interface.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

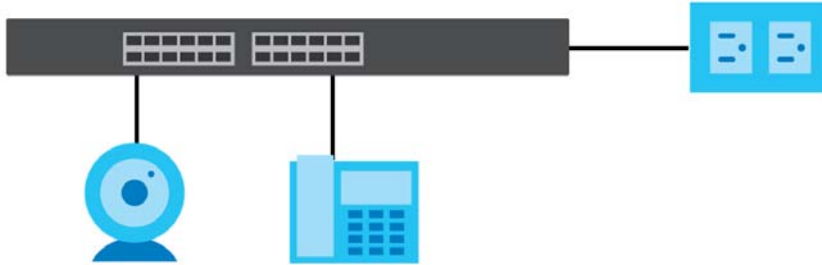
8.8 PoE Setup

Note: The following screens are available for the PoE model(s) only.

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

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

Figure 64 Powered Device Examples



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

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

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

Figure 65 Basic Setting > PoE Setup

PoE Status

[PoE Time Range Setup](#)
[PoE Setup](#)

PoE Mode	Consumption
Total Power (W)	375.0
PoE Usage (%)	2
PoE Usage Threshold (%)	95
Consuming Power (W)	8.6
Allocated Power (W)	NA
Remaining Power (W)	366.4

Port	State	Class	PD Priority	Power-Up	Consuming Power (W)	Max Power (W)	Time-Range State
1	Enable	0	Low	802.3bt	0.0	0.0	-
2	Enable	0	Low	802.3bt	0.0	0.0	-
3	Enable	0	Low	802.3bt	0.0	0.0	-
4	Enable	0	Low	802.3bt	0.0	0.0	-
5	Enable	4	Low	802.3bt	8.6	30.0	-
6	Enable	0	Low	802.3bt	0.0	0.0	-
7	Enable	0	Low	802.3bt	0.0	0.0	-
8	Enable	0	Low	802.3bt	0.0	0.0	-

The following table describes the labels in this screen.

Table 31 Basic Setting > PoE Setup

LABEL	DESCRIPTION
PoE Status	
PoE Mode	This field displays the power management mode used by the Switch, whether it is in Classification or Consumption mode.
Total Power (W)	This field displays the total power the Switch can provide to the connected PoE-enabled devices on the PoE ports.

Table 31 Basic Setting > PoE Setup (continued)

LABEL	DESCRIPTION
PoE Usage (%)	This field displays the amount of power currently being supplied to connected PoE devices (PDs) as a percentage of the total PoE power the Switch can supply. When PoE usage reaches 100%, the Switch will shut down PDs one-by-one according to the PD priority which you configured in Basic Setting > PoE Setup.
PoE Usage Threshold (%)	This field displays the percentage of PoE usage. The Switch will generate a trap and/or a log when the usage exceeds the specified threshold.
Consuming Power (W)	This field displays the amount of power the Switch is currently supplying to the connected PoE-enabled devices.
Allocated Power (W)	This field displays the total amount of power the Switch (in classification mode) has reserved for PoE after negotiating with the connected PoE device(s). It shows NA when the Switch is in consumption mode. Consuming Power (W) can be less than or equal but not more than the Allocated Power (W).
Remaining Power (W)	This field displays the amount of power the Switch can still provide for PoE. Note: The Switch must have at least 16 W of remaining power in order to supply power to a PoE device, even if the PoE device needs less than 16W.
Port	This is the port index number.
State	This field shows which ports can receive power from the Switch. You can set this in Section 8.8.2 on page 94. Disable - The PD connected to this port cannot get power supply. Enable - The PD connected to this port can receive power.
Class	This shows the power classification of the PD. Each PD has a specified maximum power that fall under one of the classes. The Class is a number from 0 to 8, where each value represents the range of power that the Switch provides to the PD. The power ranges in PoE standards are as follows. Class 0 - default: 0.44 W to 15.4 W. Class 1 - default: 0.44 W to 4 W. Class 2 - default: 0.44 W to 7 W. Class 3 - default: 0.44 W to 15.4 W. Class 4 - default: 0.44 W to 30 W. Class 5 - default: 0.44 W to 45 W. Class 6 - default: 0.44 W to 60 W. Class 7 - default: 0.44 W to 60 W. Class 8 - default: 0.44 W to 60 W. Note: You can set a limit on the maximum power the connected PD can use on a port in Basic Setting > PoE Setup > PoE Setup.
PD Priority	When the total power requested by the PDs exceeds the total PoE power budget on the Switch, you can set the PD priority to allow the Switch to provide power to ports with higher priority first. Critical has the highest priority. High has the Switch assign power to the port after all critical priority ports are served. Low has the Switch assign power to the port after all critical and high priority ports are served.
Power-Up	This field displays the PoE standard the Switch uses to provide power on this port.
Consuming Power (W)	This field displays the current amount of power consumed by the PD from the Switch on this port.

Table 31 Basic Setting > PoE Setup (continued)

LABEL	DESCRIPTION
Max Power (W)	This field displays the maximum amount of power the PD could use from the Switch on this port.
Time Range State	This field shows whether or not the port currently receives power from the Switch according to its schedule. - It shows "In" followed by the time range name if PoE is currently enabled on the port. - It shows "Out" if PoE is currently disabled on the port. - It shows "-" if no schedule is applied to the port. PoE is enabled by default.

8.8.1 PoE Time Range Setup

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

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

Figure 66 Basic Setting > PoE Setup > PoE Time Range Setup

PoE Time Range Setup [PoE Status](#)

Port

Time Range

[Apply](#) [Clear](#)

Port	Time Range Profiles	
1	-	☐
2	-	☐
3	-	☐
4	-	☐
5	-	☐
6	-	☐
7	-	☐
8	-	☐

[Delete](#) [Cancel](#)

The following table describes the labels in this screen.

Table 32 Basic Setting > PoE Setup > PoE Time Range Setup

LABEL	DESCRIPTION
Port Time Range Setup	
Port	Enter the number of the port to which you want to apply a schedule.

Table 32 Basic Setting > PoE Setup > PoE Time Range Setup (continued)

LABEL	DESCRIPTION
Time Range	This field displays the name of the schedule that you have created using the Advanced Application > Time Range screen. Select one or more time range profiles that determine when PoE will be enabled in this port. You can configure time range profiles in Advanced Application > Time Range. You can select multiple profiles by holding the Ctrl key before clicking on multiple profiles, or by clicking on one profile and dragging your mouse to select the desired profiles. Note: The schedules you assign to one port must not have any overlap.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, 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 this button to reset the Port and Time Range fields.
Port	This is the number of the port on the Switch. Click this number to configure the PoE time range of this port.
Time Range Profiles	This field displays the name of the schedule(s) applied to the port. If a schedule is assigned to a port, PoE is enabled only at the time/date specified in the time range profile(s). If no schedule is assigned, PoE is enabled by default.
	Select an entry's check box to select a specific port. Otherwise, select the check box in the table heading row to select all ports.
Delete	Click this button to delete the time range profile of the selected port(s).
Cancel	Click this button to clear the selected check box(es).

8.8.2 PoE Setup

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

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

Figure 67 Basic Setting > PoE Setup > PoE Setup

PoE Setup				PoE Status			
PoE Mode	☐ Classification ☒ Consumption						
Pre-Allocate	Active ☒						
Power Up Sequence Delay	Active ☒						
PoE Usage Threshold (%)	95						

Port	PD	PD Priority	Power-Up	Max Power (mW)	Wide Range Detection	LLDP Power Via MDI
*	☐	Critical ▼	802.3af ▼		☐	☐
1	☒	Low ▼	802.3bt ▼		☐	☒
2	☒	Low ▼	802.3bt ▼		☐	☒
3	☒	Low ▼	802.3bt ▼		☐	☒
4	☒	Low ▼	802.3bt ▼		☐	☒
5	☒	Low ▼	802.3bt ▼		☐	☒
6	☒	Low ▼	802.3bt ▼		☐	☒
7	☒	Low ▼	802.3bt ▼		☐	☒
8	☒	Low ▼	802.3bt ▼		☐	☒

The following table describes the labels in this screen.

Table 33 Basic Setting > PoE Setup > PoE Setup

LABEL	DESCRIPTION
PoE Mode	Select the power management mode you want the Switch to use. Classification - Select this if you want the Switch to reserve the maximum power for each PD according to the PD's power class and priority level. If the total power supply runs out, PDs with lower priority do not get power to function. In this mode, the maximum power is reserved based on what you configure in Max Power or the standard power limit for each class. Consumption - Select this if you want the Switch to supply the actual power that the PD needs. The Switch also allocates power based on a port's Max Power and the PD's power class and priority level. The Switch puts a limit on the maximum amount of power the PD can request and use. In this mode, the default maximum power that can be delivered to the PD is 33 W (IEEE 802.3at Class 4) or 22 W (IEEE 802.3af Classes 0 to 3).
Pre-Allocate	Select this to have the Switch pre-allocate power to each port based on the classification of the PD device.
Power Up Sequence Delay	Select this to allow PoE ports to be powered up one-by-one randomly or clear to allow them all to be powered up at the same time.
PoE Usage Threshold (%)	Enter a number ranging from 1 to 99 to set the threshold. The Switch will generate a trap and/or log when the actual PoE usage is higher than the specified threshold.
Port	This is the port index number. * 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.
PD	Select this to provide power to a PD connected to the port. If left unchecked, the PD connected to the port cannot receive power from the Switch.

Table 33 Basic Setting > PoE Setup > PoE Setup (continued)

LABEL	DESCRIPTION
PD Priority	When the total power requested by the PDs exceeds the total PoE power budget on the Switch, you can set the PD priority to allow the Switch to provide power to ports with higher priority. Select Critical to give the highest PD priority on the port. Select High to set the Switch to assign the remaining power to the port after all critical priority ports are served. Select Low to set the Switch to assign the remaining power to the port after all critical and high priority ports are served.
Power-Up	Set how the Switch provides power to a connected PD at power-up. 802.3af - the Switch follows the IEEE 802.3af Power over Ethernet standard to supply power of up to 15.4W per Ethernet port to the connected PDs during power-up. Legacy - the Switch can provide power to the connected PDs that require high inrush currents at power-up. Inrush current is the maximum, instantaneous input current drawn by the PD when first turned on. Pre-802.3at - the Switch initially offers power on the port according to the IEEE 802.3af standard, and then switches to support the IEEE 802.3at standard within 75 milliseconds after a PD is connected to the port. Select this option if the Switch is performing 2-event Layer-1 classification (PoE+ hardware classification) or the connected PD is NOT performing Layer 2 power classification using Link Layer Discovery Protocol (LLDP). 802.3at - the Switch supports the IEEE 802.3at High Power over Ethernet standard and can supply power of up to 33W per Ethernet port. IEEE 802.3at is also known as PoE+ or PoE Plus. An IEEE 802.3at compatible device is referred to as Type 2. Power Class 4 (High Power) can only be used by Type 2 devices. If the connected PD requires a Class 4 current when it is turned on, it will be powered up in this mode. Force-802.3at - the Switch offers power of up to 33W on the port without performing PoE hardware classification. Select this option if the connected PD doesn't comply with any PoE standard and requests power higher than a standard power limit. Pre-802.3bt - the Switch offers power on the port according to the IEEE 802.3bt standard. Select this option if the connected PD was developed before the IEEE 802.3bt standard is implemented but requires power between 33W and 60W. 802.3bt - the Switch supports the IEEE 802.3bt standard and can supply power of up to 60W per Ethernet port to the connected PDs at power-up.
Max Power (mW)	Specify the maximum amount of power the PD could use from the Switch on this port. If you leave this field blank, the Switch refers to the standard or default maximum power for each class. Note: The setting you enter here will not take effect when the power-up mode is set to 802.3bt.
Wide Range Detection	Select this to let the Switch have a wider current detection range for the PD. The Switch detects whether a connected device is a powered device or not before supplying power to the port. For the PD detection, the Switch applies a fixed voltage to the device and then receives returned current. If the returned current is within the IEEE 802.3af/at standard range, the device will be considered as a valid PD by the Switch. However, in real cases, environmental interferences might easily cause the returned current to be out of the standard range.

Table 33 Basic Setting > PoE Setup > PoE Setup (continued)

LABEL	DESCRIPTION
LLDP Power Via MDI	Select this to have the Switch negotiate PoE power with the PD connected to the port by transmitting LLDP Power Via MDI TLV frames. This helps the Switch allocate less power to the PD on this port. The connected PD must be able to request PoE power through LLDP. The Power Via MDI TLV allows PoE devices to advertise and discover the MDI power support capabilities of the sending port on the remote device. • Port Class • MDI Supported • MDI Enabled • Pair Controllable • PSE Power Pairs • Power Class
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

8.9 Interface Setup

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

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

Figure 68 Basic Setting > Interface Setup

The following table describes the labels in this screen.

Table 34 Basic Setting > Interface Setup

LABEL	DESCRIPTION
Interface Type	Select the type of IPv6 interface for which you want to configure. The Switch supports the VLAN interface type for IPv6 at the time of writing.
Interface ID	Specify a unique identification number (from 1 to 4094) for the interface. To have IPv6 function properly, you should configure a static VLAN with the same ID number in the Advanced Application > VLAN screens.

Table 34 Basic Setting > Interface Setup (continued)

LABEL	DESCRIPTION
Add	Click this to create a new entry. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Index	This field displays the index number of an entry.
Interface Type	This field displays the type of interface.
Interface ID	This field displays the identification number of the interface.
Interface	This field displays the interface's descriptive name which is generated automatically by the Switch. The name is from a combination of the interface type and ID number.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the check boxes.

8.10 IPv6

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

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

Figure 69 Basic Setting > IPv6

IPv6 Status		IPv6 Configuration
Index	Interface	Active
1	VLAN123	No

The following table describes the labels in this screen.

Table 35 Basic Setting > IPv6

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

8.10.1 IPv6 Interface Status

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

Figure 70 Basic Setting > IPv6 > IPv6 Interface Status

IPv6 Interface Status [IPv6 Status](#)

Interface: VLAN123

IPv6 Active	disable
MTU Size	
ICMPv6 Rate Limit Bucket Size	
ICMPv6 Rate Limit Error Interval	
Link Local Address	
Global Unicast Address(es)	
Joined Group Address(es)	
ND DAD Active	
Number of DAD Attempts	
NS-Interval (millisecond)	
ND Reachable Time (millisecond)	

DHCPv6 Client Active	No	
Identity Association	IA Type	
	IAID	
	T1	
	T2	
	State	
	SID	
	Address	
	Preferred Lifetime	
	Valid Lifetime	
DNS		
Domain List		

Restart DHCPv6 Client [Click Here](#)

The following table describes the labels in this screen.

Table 36 Basic Setting > IPv6 > IPv6 Interface Status

LABEL	DESCRIPTION
IPv6 Active	This field displays whether the IPv6 interface is activated or not.
MTU Size	This field displays the Maximum Transmission Unit (MTU) size for IPv6 packets on this interface.
ICMPv6 Rate Limit Bucket Size	This field displays the maximum number of ICMPv6 error messages which are allowed to transmit in a given time interval. If the bucket is full, subsequent error messages are suppressed.
ICMPv6 Rate Limit Error Interval	This field displays the time period (in milliseconds) during which ICMPv6 error messages of up to the bucket size can be transmitted. 0 means no limit.
Link Local Address	This field displays the Switch's link-local IP address and prefix generated by the interface. It also shows whether the IP address is preferred, which means it is a valid address and can be used as a sender or receiver address.
Global Unicast Address(es)	This field displays the Switch's global unicast address to identify this interface.
Joined Group Address(es)	This field displays the IPv6 multicast addresses of groups the Switch's interface joins.
ND DAD Active	This field displays whether Neighbor Discovery (ND) Duplicate Address Detection (DAD) is enabled on the interface.

Table 36 Basic Setting > IPv6 > IPv6 Interface Status (continued)

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

8.10.2 IPv6 Configuration

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

Figure 71 Basic Setting > IPv6 > IPv6 Configuration

IPv6 Configuration		IPv6 Status
IPv6 Global Setup		Click Here
IPv6 Interface Setup		Click Here
IPv6 Addressing	IPv6 Link-Local Address Setup	Click Here
	IPv6 Global Address Setup	Click Here
IPv6 Neighbor Discovery	IPv6 Neighbor Discovery Setup	Click Here
	IPv6 Router Discovery Setup	Click Here
	IPv6 Prefix Setup	Click Here
IPv6 Neighbor Setup		Click Here
DHCPv6 Client Setup		Click Here

The following table describes the labels in this screen.

Table 37 Basic Setting > IPv6 > IPv6 Configuration

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

8.10.3 IPv6 Global Setup

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

Figure 72 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Setup

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

The following table describes the labels in this screen.

Table 38 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Setup

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

8.10.4 IPv6 Interface Setup

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

Figure 73 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Interface Setup

IPv6 Interface Setup		IPv6 Configuration
Interface	VLAN123 ▼	
Active	☐	
Apply Cancel Clear		
Index	Interface	Active
1	VLAN123	No

The following table describes the labels in this screen.

Table 39 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Interface Setup

LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
Active	Select this option to enable the interface.

Table 39 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Interface Setup (continued)

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

8.10.5 IPv6 Link-Local Address Setup

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

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

Figure 74 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Link-Local Address Setup

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

The following table describes the labels in this screen.

Table 40 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Link-Local Address Setup

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

Table 40 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Link-Local Address Setup (continued)

LABEL	DESCRIPTION
IPv6 Link-Local Address	This is the static IPv6 link-local address for the interface.
IPv6 Default Gateway	This is the default gateway IPv6 address for the interface.

8.10.6 IPv6 Global Address Setup

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

Figure 75 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Address Setup

The following table describes the labels in this screen.

Table 41 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Address Setup

LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
IPv6 Global Address	Manually configure a static IPv6 global address for the interface.
Prefix Length	Specify an IPv6 prefix length that specifies how many most significant bits (start from the left) in the address compose the network address.
EUI-64	Select this option to have the interface ID be generated automatically using the EUI-64 format.
Add	Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to reset the fields to the factory defaults.
Index	This is the interface index number. Click on an index number to change the settings.
Interface	This is the name of the IPv6 interface you created.
IPv6 Global Address/Prefix Length	This field displays the IPv6 global address and prefix length for the interface.
EUI-64	This shows whether the interface ID of the global address is generated using the EUI-64 format.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.

Table 41 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Address Setup (continued)

LABEL	DESCRIPTION
Delete	Check the entry(ies) that you want to remove and then click Delete to remove the selected entry(ies) from the summary table.
Cancel	Click Cancel to clear the check boxes.

8.10.7 IPv6 Neighbor Discovery Setup

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

Figure 76 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Discovery Setup

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

The following table describes the labels in this screen.

Table 42 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Discovery Setup

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

Table 42 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Discovery Setup (continued)

LABEL	DESCRIPTION
NS Interval	This field displays the time interval (in milliseconds) at which neighbor solicitations are re-sent for this interface.
Reachable Time	This field displays how long (in milliseconds) a neighbor is considered reachable for this interface.

8.10.8 IPv6 Router Discovery Setup

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

Figure 77 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Router Discovery Setup

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

The following table describes the labels in this screen.

Table 43 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Router Discovery Setup

LABEL	DESCRIPTION
Interface	Select the IPv6 interface you want to configure.
Flags	Select the Managed Config Flag option to have the Switch set the "managed address configuration" flag (the M flag) to 1 in IPv6 router advertisements, which means IPv6 hosts use DHCPv6 to obtain IPv6 stateful addresses. Deselect the option to set the flag to 0 and the host will not use DHCPv6 to obtain IPv6 stateful addresses. Select the Other Config Flag option to have the Switch set the "Other stateful configuration" flag (the O flag) to 1 in IPv6 router advertisements, which means IPv6 hosts use DHCPv6 to obtain additional configuration settings, such as DNS information. Deselect the option to set the flag to 0 and the host will not use DHCPv6 to obtain additional configuration settings.
Minimum Interval	Specify the minimum time interval (from 3 to 1350 seconds) at which the Switch sends router advertisements for this interface. Note: The minimum time interval cannot be greater than three-quarters of the maximum time interval.
Maximum Interval	Specify the maximum time interval (from 4 to 1800 seconds) at which the Switch sends router advertisements for this interface.
Lifetime	Specify how long (from 0 to 9000 seconds) the router in router advertisements can be used as a default router for this interface.

Table 43 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Router Discovery Setup (continued)

LABEL	DESCRIPTION
Suppress	Select this option to set the Switch to not send router advertisements and responses to router solicitations on this interface.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to reset the fields to the factory defaults.
Index	This is the interface index number. Click on an index number to change the settings.
Interface	This is the name of the IPv6 interface you created.
Flags	This field displays whether IPv6 hosts use DHCPv6 to obtain IPv6 stateful addresses (M) and/or additional configuration settings (O).
Minimum Interval	This field displays the minimum time interval at which the Switch sends router advertisements for this interface.
Maximum Interval	This field displays the maximum time interval at which the Switch sends router advertisements for this interface.
Lifetime	This field displays how long the router in router advertisements can be used as a default router for this interface.
Suppress	This field displays whether the Switch sends router advertisements and responses to router solicitations on this interface (No) or not (Yes).

8.10.9 IPv6 Prefix Setup

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

Figure 78 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Prefix Setup

IPv6 Prefix Setup [IPv6 Configuration](#)

Interface:

Prefix:

Prefix Length:

Valid Lifetime: seconds

Preferred Lifetime: seconds

Flags:

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

Add **Cancel** **Clear**

Index	Interface	Prefix/Prefix Length	Valid Lifetime	Preferred Lifetime

Delete **Cancel**

The following table describes the labels in this screen.

Table 44 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Prefix Setup

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

8.10.10 IPv6 Neighbor Setup

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

Figure 79 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Setup

The following table describes the labels in this screen.

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

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

8.10.11 DHCPv6 Client Setup

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

Figure 80 Basic Setting > IPv6 > IPv6 Configuration > DHCPv6 Client Setup

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

The following table describes the labels in this screen.

Table 46 Basic Setting > IPv6 > IPv6 Configuration > DHCPv6 Client Setup

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

Table 46 Basic Setting > IPv6 > IPv6 Configuration > DHCPv6 Client Setup

LABEL	DESCRIPTION
Domain-List	This field displays whether the Switch obtains a list of domain names from the DHCP server.
Information Refresh Minimum	This field displays the time interval (in seconds) at which the Switch exchanges other configuration information with a DHCPv6 server again.

8.11 DNS

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

Figure 81 Basic Setting > DNS

DNS

Static Domain Name Server

Preference	Server Address
1	
2	

Apply Cancel

Domain Name Server Table

Index	Server Address	Source
1		DHCPv4

The following table describes the labels in this screen.

Table 47 Basic Setting > DNS

LABEL	DESCRIPTION
Static Domain Name Server	
Preference	This is the priority of the DNS server address.
Server Address	Enter a domain name server IPv6/IPv4 address in order to be able to use a domain name instead of an IP address.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the nonvolatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Domain Name Server Table	
Index	This field displays priority of the DNS server address.
Server Address	This field displays the IP address of the DNS server.
Source	This field displays whether the DNS server address is configured manually (Static) or obtained automatically using DHCPv4 or DHCPv6 .

8.12 Cloud Management

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

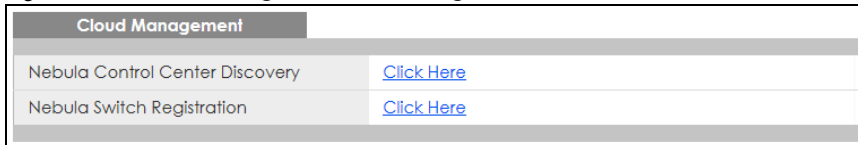
The Switch is managed and provisioned automatically by the NCC (Nebula Control Center) when:

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

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

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

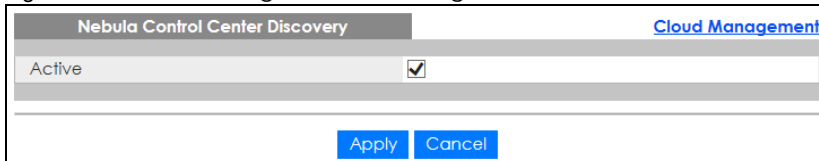
Figure 82 Basic Setting > Cloud Management



8.12.1 Nebula Control Center Discovery

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

Figure 83 Basic Setting > Cloud Management > Nebula Control Center Discovery



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

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

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

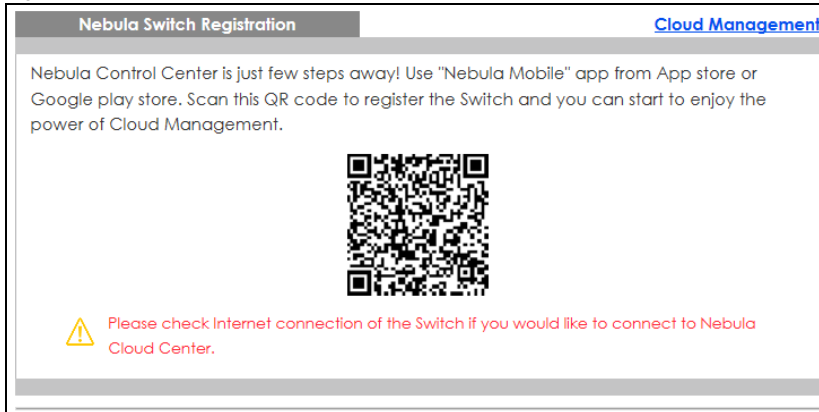
Note: While the Switch is rebooting, don't turn off the power.

Clear **Active** to turn off NCC discovery on the Switch. The Switch will not discover the NCC and remain in standalone mode. See [Section 1.1.2 on page 19](#) for more information.

8.12.2 Nebula Switch Registration

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

Figure 84 Basic Setting > Cloud Management > Nebula Switch Registration



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

CHAPTER 9

VLAN

9.1 Overview

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

9.1.1 What You Can Do

- Use the **VLAN Status** screen ([Section 9.2 on page 117](#)) to view and search all VLAN groups.
- Use the **VLAN Detail** screen ([Section 9.2.1 on page 118](#)) to view detailed port settings and status of the VLAN group.
- Use the **Static VLAN Setup** screen ([Section 9.4 on page 119](#)) to configure and view 802.1Q VLAN parameters for the Switch.
- Use the **VLAN Port Setup** screen ([Section 9.5 on page 121](#)) to configure the static VLAN (IEEE 802.1Q) settings on a port.
- Use the **Voice VLAN Setup** screen ([Section 9.6 on page 122](#)) to set up VLANs that allow you to group voice traffic with defined priority and enable the switch port to carry the voice traffic separately from data traffic to ensure the sound quality does not deteriorate.
- Use the **Vendor ID Based VLAN Setup** screen ([Section 9.7 on page 124](#)) to set up VLANs that allow you to group untagged packets into logical VLANs based on the source MAC address of the packet. You can specify a mask for the MAC address to create a MAC address filter and enter a weight to set the VLAN rule's priority.
- Use the **Port-Based VLAN** screen ([Section 9.8 on page 126](#)) to set up VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

9.1.2 What You Need to Know

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

IEEE 802.1Q Tagged VLANs

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

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4,096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID

(VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4,094.

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

Forwarding Tagged and Untagged Frames

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

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

9.1.2.1 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 48 IEEE 802.1Q VLAN Terminology

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

Table 48 IEEE 802.1Q VLAN Terminology (continued)

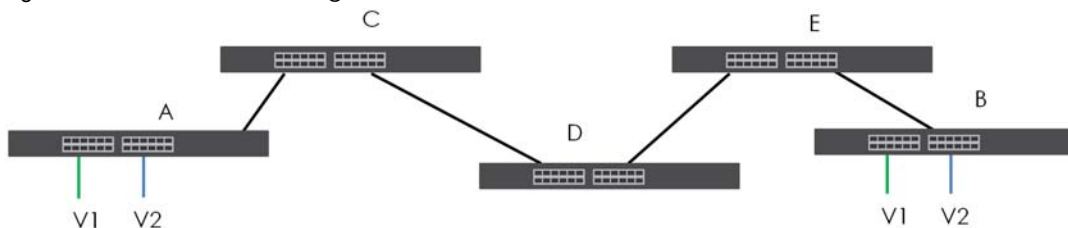
VLAN PARAMETER	TERM	DESCRIPTION
VLAN Administrative Control	Registration Fixed	Fixed registration ports are permanent VLAN members.
	Registration Forbidden	Ports with registration forbidden are forbidden to join the specified VLAN.
	Normal Registration	Ports dynamically join a VLAN using GVRP.
VLAN Tag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

9.1.2.2 Port VLAN Trunking

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

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

Figure 85 Port VLAN Trunking



9.1.2.3 VLAN Priority

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

- 1 Vendor ID Based VLAN
- 2 Voice VLAN

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

9.1.2.4 Select the VLAN Type

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

Figure 86 Switch Setup > Select VLAN Type

Switch Setup			
VLAN Type	☒ 802.1Q	☐ Port Based	
MAC Address Learning	Aging Time	300	seconds
ARP Aging Time	Aging Time	300	seconds

Static VLAN

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

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

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

9.2 VLAN Status

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

Figure 87 Advanced Application > VLAN: VLAN Status

VLAN Status						
VLAN Configuration						
VLAN Search by VID: Search						
The Number of VLAN: 1.						
Index	VID	Name	Tagged Port	Untagged Port	Elapsed Time	Status
1	1	1		1-12	214:36:41	Static

Change Pages: [Previous](#) [Next](#)

The following table describes the labels in this screen.

Table 49 Advanced Application > VLAN: VLAN Status

LABEL	DESCRIPTION
VLAN Search by VID	Enter an existing VLAN ID number(s) (separated by a comma) and click Search to display only the specified VLAN(s) in the list below. Leave this field blank and click Search to display all VLANs configured on the Switch.
The Number of VLAN	This is the number of VLANs configured on the Switch.
The Number of Search Results	This is the number of VLANs that match the searching criteria and display in the list below. This field displays only when you use the Search button to look for certain VLANs.
Index	This is the VLAN index number. Click on an index number to view more VLAN details.
VID	This is the VLAN identification number that was configured in the Static VLAN screen.
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 : added as a permanent entry
Change Pages	Click Previous or Next to show the previous/next screen if all status information cannot be seen in one screen.

9.2.1 VLAN Detail

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

Figure 88 Advanced Application > VLAN > VLAN Detail

VLAN Detail							VLAN Status	
VID	Port Number						Elapsed Time	Status
	2	4	6	8	10	12		
1	U	U	U	U	U	U	214:40:03	Static
	U	U	U	U	U	U		

The following table describes the labels in this screen.

Table 50 Advanced Application > VLAN > VLAN Detail

LABEL	DESCRIPTION
VLAN Status	Click this to go to the VLAN Status screen.
VID	This is the VLAN identification number that was configured in the Static VLAN screen.
Port Number	This column displays the ports that are participating in a VLAN. A tagged port is marked as T, an untagged port is marked as U and ports not participating in a VLAN are marked as "—".

Table 50 Advanced Application > VLAN > VLAN Detail (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. Dynamic: using GVRP Static: added as a permanent entry

9.3 VLAN Configuration

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

Figure 89 Advanced Application > VLAN > VLAN Configuration



VLAN Configuration		VLAN Status
Static VLAN Setup	Click Here	
VLAN Port Setup	Click Here	
Voice VLAN Setup	Click Here	
Vendor ID Based VLAN Setup	Click Here	

The following table describes the labels in the above screen.

Table 51 Advanced Application > VLAN > VLAN Configuration

LABEL	DESCRIPTION
Static VLAN Setup	Click Click Here to configure the Static VLAN for the Switch.
VLAN Port Setup	Click Click Here to configure the VLAN Port for the Switch.
Voice VLAN Setup	Click Click Here to configure the Voice VLAN for the Switch.
Vendor ID Based VLAN Setup	Click Click Here to configure the Vendor ID Based VLAN for the Switch.

9.4 Configure a Static VLAN

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

Figure 90 Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup

Static VLAN

VLAN Configuration

ACTIVE

☐

Name

VLAN Group ID

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

Add

Cancel

Clear

VID	Active	Name	
1	Yes	1	☐

Delete

Cancel

The following table describes the related labels in this screen.

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

LABEL	DESCRIPTION
ACTIVE	Select this check box to activate the VLAN settings.
Name	Enter a descriptive name for the VLAN group for identification purposes. This name consists of up to 64 printable characters. Spaces are allowed.
VLAN Group ID	Enter the VLAN ID for this static entry; the valid range is between 1 and 4094.
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.

Table 52 Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup (continued)

LABEL	DESCRIPTION
Add	Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to change the fields back to their last saved values.
Clear	Click Clear to start configuring the screen again.
VID	This field displays the ID number of the VLAN group. Click the number to edit the VLAN settings.
Active	This field indicates whether the VLAN settings are enabled (Yes) or disabled (No).
Name	This field displays the descriptive name for this VLAN group.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the check boxes.

9.5 Configure VLAN Port Setting

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

Figure 91 Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup

VLAN Port Setting [VLAN Configuration](#)

GVRP ☐

Port	Ingress Check	PVID	GVRP	Acceptable Frame Type	VLAN Trunking	Isolation
*	☐		☐	All ☐	☐	☐
1	☐	1	☐	All ☐	☐	☐
2	☐	1	☐	All ☐	☐	☐
3	☐	1	☐	All ☐	☐	☐
4	☐	1	☐	All ☐	☐	☐
5	☐	1	☐	All ☐	☐	☐
6	☐	1	☐	All ☐	☐	☐
7	☐	1	☐	All ☐	☐	☐
8	☐	1	☐	All ☐	☐	☐
9	☐	1	☐	All ☐	☐	☐
10	☐	1	☐	All ☐	☐	☐
11	☐	1	☐	All ☐	☐	☐
12	☐	1	☐	All ☐	☐	☐

[Apply](#) [Cancel](#)

The following table describes the labels in this screen.

Table 53 Advanced Application > VLAN > VLAN Configuration> VLAN Port Setup

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

9.6 Voice VLAN Setup

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

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

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

Figure 92 Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup

Voice VLAN Setup [VLAN Configuration](#)

Voice VLAN Global Setup

Voice VLAN ☒ Disable ☐

Priority

[Apply](#) [Cancel](#) [Clear](#)

Voice VLAN OUI Setup

OUI address

OUI mask

Description

[Add](#) [Cancel](#)

Index	OUI address	OUI mask	Description

[Delete](#) [Cancel](#)

The following table describes the fields in the above screen.

Table 54 Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup

LABEL	DESCRIPTION
Voice VLAN Global Setup	
Voice VLAN	Click the second radio button if you want to enable the Voice VLAN feature. Type a VLAN ID number in the box next to the radio button that is associated with the Voice VLAN. You also need to create a static VLAN with the same VID in the Static VLAN Setup screen, and then connect the IP phone with the specified OUI MAC address to a port that joins the static VLAN. Click the Disable radio button if you do not want to enable the Voice VLAN feature.
Priority	Select the priority level of the Voice VLAN from 0 to 7. Default setting is 5. The higher the numeric value you assign, the higher the priority for this Voice VLAN.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to reset the fields to default settings.
Voice VLAN OUI Setup	
OUI address	Type the IP Phone manufacturer's OUI MAC address. The first three bytes is the manufacturer identifier, the last three bytes is a unique station ID.
OUI mask	Type the mask for the specified IP Phone manufacturer's OUI MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
Description	Type an description up to 32 characters for the Voice VLAN device. For example: Siemens.

Table 54 Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup

LABEL	DESCRIPTION
Add	Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Index	This field displays the index number of the Voice VLAN.
OUI address	This field displays the OUI address of the Voice VLAN.
OUI mask	This field displays the OUI mask address of the Voice VLAN.
Description	This field displays the description of the Voice VLAN with OUI address.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the check boxes.

9.7 Vendor ID Based VLAN

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

This feature allows users to change ports without having to reconfigure the VLAN. You can assign a 802.1p priority to the vendor ID based VLAN and define a vendor ID to VLAN mapping table by entering a specified source MAC address and mask in the vendor ID based VLAN setup screen. You can also delete a vendor ID based VLAN entry in the same screen.

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

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

Figure 93 Advanced Application > VLAN > VLAN Configuration > Vendor ID Based VLAN Setup

Vendor ID Based VLAN [VLAN Configuration](#)

Name	
MAC address	5c:e2:8c:11:22:33
Mask	ff:ff:ff:00:00:00
VLAN	
Priority	0 ▼
Weight	127

[Add](#) [Cancel](#)

Index	Name	MAC address	Mask	VLAN	Priority	Weight	☐
Delete Cancel							

The following table describes the fields in the above screen.

Table 55 Advanced Application > VLAN > VLAN Configuration > Vendor ID Based VLAN Setup

LABEL	DESCRIPTION
Name	Type a name up to 32 alpha numeric characters for the vendor ID based VLAN entry.
MAC address	Type a MAC address that is bind to the vendor ID-based VLAN entry. This is the source MAC address of the data packet that is looked up when untagged packets arrive at the Switch.
Mask	Type the mask for the specified source MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria.
VLAN	Type an ID (from 1 to 4094) for the VLAN that is associated with the vendor ID based VLAN entry.
Priority	Select the priority level that the Switch assigns to frames belonging to this VLAN. The higher the numeric value you assign, the higher the priority for this vendor ID based VLAN entry.
Weight	Enter a number between 0 and 255 to specify the rule's weight. This is to decide the priority in which the rule is applied. The higher the number, the higher the rule's priority.
Add	Click Add to save the new vendor ID based VLAN entry.
Cancel	Click Cancel to clear the fields in the vendor ID based VLAN entry.
Index	This field displays the index number of the vendor ID based VLAN entry.
Name	This field displays the name of the vendor ID based VLAN entry.
MAC address	This field displays the source MAC address that is bind to the vendor ID based VLAN entry.
Mask	This field displays the mask for the source MAC address that is bind to the vendor ID based VLAN entry.
VLAN	This field displays the VLAN ID of the vendor ID based VLAN entry.
Priority	This field displays the priority level which is assigned to frames belonging to this vendor ID based VLAN.
Weight	This field displays the weight of the vendor ID based VLAN entry.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.

Table 55 Advanced Application > VLAN > VLAN Configuration > Vendor ID Based VLAN Setup

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

9.8 Port-Based VLAN Setup

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

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

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

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

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

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

9.8.1 Configure a Port-Based VLAN

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

Figure 94 Advanced Application > VLAN: Port Based VLAN Setup (All Connected)

Port Based VLAN Setup

Setting Wizard All connected ▼ Apply

Incoming

	1	2	3	4	5	6	7	8	9	10	11	12	
1	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	1
2	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	2
3	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	3
4	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	4
5	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	5
6	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	6
7	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	7
8	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	8
9	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	9
10	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	10
11	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	11
12	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	12
CPU	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	CPU
	1	2	3	4	5	6	7	8	9	10	11	12	

Outgoing

Apply Cancel

Figure 95 Advanced Application > VLAN: Port Based VLAN Setup (Port Isolation)

Port Based VLAN Setup

Setting Wizard Port isolation ▼ Apply

Incoming

	1	2	3	4	5	6	7	8	9	10	11	12	
1	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	1
2	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	2
3	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	☐	3
4	☐	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	☐	4
5	☐	☐	☐	☐	☒	☐	☐	☐	☐	☐	☐	☐	5
6	☐	☐	☐	☐	☐	☒	☐	☐	☐	☐	☐	☐	6
7	☐	☐	☐	☐	☐	☐	☒	☐	☐	☐	☐	☐	7
8	☐	☐	☐	☐	☐	☐	☐	☒	☐	☐	☐	☐	8
9	☐	☐	☐	☐	☐	☐	☐	☐	☒	☐	☐	☐	9
10	☐	☐	☐	☐	☐	☐	☐	☐	☐	☒	☐	☐	10
11	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☒	☐	11
12	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☐	☒	12
CPU	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	☒	CPU
	1	2	3	4	5	6	7	8	9	10	11	12	

Outgoing

Apply Cancel

The following table describes the labels in this screen.

Table 56 Advanced Application > VLAN: Port Based VLAN Setup

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

CHAPTER 10

Static MAC Forward Setup

10.1 Overview

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

Use these screens to configure static MAC address forwarding.

10.1.1 What You Can Do

Use the **Static MAC Forwarding** screen ([Section 10.2 on page 129](#)) to assign static MAC addresses for a port.

10.2 Configuring Static MAC Forwarding

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

Static MAC address forwarding together with port security allow only computers in the MAC address table on a port to access the Switch. See [Chapter 19 on page 175](#) for more information on port security.

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

Figure 96 Advanced Application > Static MAC Forwarding

Static MAC Forwarding						
Active	☐					
Name						
MAC Address						
VID						
Port						
Add Cancel Clear						
Index	Active	Name	MAC Address	VID	Port	
Delete Cancel						

The following table describes the labels in this screen.

Table 57 Advanced Application > Static MAC Forwarding

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Enter a descriptive name for identification purposes for this static MAC address forwarding rule.
MAC Address	Enter the MAC address in valid MAC address format, that is, six hexadecimal character pairs. Note: Static MAC addresses do not age out.
VID	Enter the VLAN identification number.
Port	Enter the port where the MAC address entered in the previous field will be automatically forwarded.
Add	Click Add to save your rule to the Switch's run-time memory. The Switch loses this rule if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to their last saved values.
Clear	Click Clear to begin configuring this screen afresh.
Index	Click an index number to modify a static MAC address rule for a port.
Active	This field displays whether this static MAC address forwarding rule is active (Yes) or not (No). You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for this static MAC address-forwarding rule.
MAC Address	This field displays the MAC address that will be forwarded and the VLAN identification number to which the MAC address belongs.
VID	This field displays the ID number of the VLAN group.
Port	This field displays the port where the MAC address shown in the next field will be forwarded.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the check boxes.

CHAPTER 11

Static Multicast Forwarding

11.1 Static Multicast Forward Setup Overview

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

Use these screens to configure static multicast address forwarding.

11.1.1 What You Can Do

Use the **Static Multicast Forwarding** screen ([Section 11.2 on page 132](#)) to configure rules to forward specific multicast frames, such as streaming or control frames, to specific port(s).

11.1.2 What You Need To Know

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

If a multicast group has no members, then the switch will either flood the multicast frames to all ports or drop them. [Figure 97 on page 131](#) shows such unknown multicast frames flooded to all ports. With static multicast forwarding, you can forward these multicasts to port(s) within a VLAN group. [Figure 98 on page 132](#) shows frames being forwarded to devices connected to port 3. [Figure 99 on page 132](#) shows frames being forwarded to ports 2 and 3 within VLAN group 4.

Figure 97 No Static Multicast Forwarding

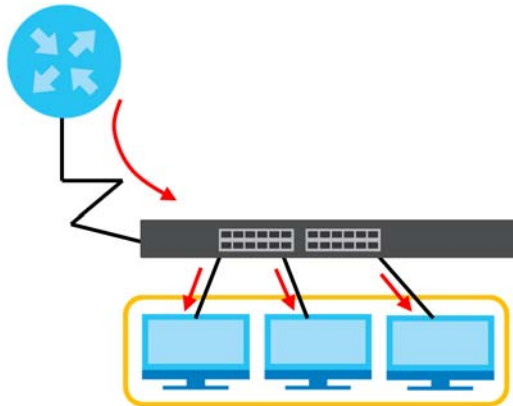


Figure 98 Static Multicast Forwarding to A Single Port

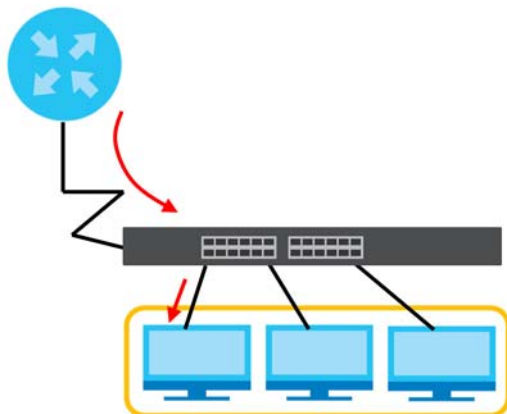
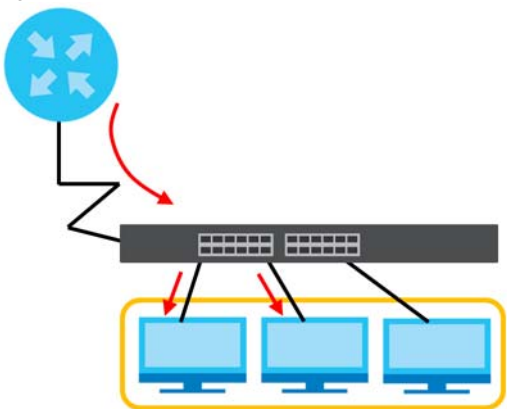


Figure 99 Static Multicast Forwarding to Multiple Ports



11.2 Configuring Static Multicast Forwarding

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

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

Figure 100 Advanced Application > Static Multicast Forwarding

The following table describes the labels in this screen.

Table 58 Advanced Application > Static Multicast Forwarding

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Type a descriptive name (up to 32 printable ASCII characters) for this static multicast MAC address forwarding rule. This is for identification only.
MAC Address	Enter a multicast MAC address which identifies the multicast group. The last binary bit of the first octet pair in a multicast MAC address must be 1. For example, the first octet pair 00000001 is 01 and 00000011 is 03 in hexadecimal, so 01:00:5e:00:00:0A and 03:00:5e:00:00:27 are valid multicast MAC addresses.
VID	You can forward frames with matching destination MAC address to port(s) within a VLAN group. Enter the ID that identifies the VLAN group here. If you don't have a specific target VLAN, enter 1.
Port	Enter the port(s) where frames with destination MAC address that matched the entry above are forwarded. You can enter multiple ports separated by (no space) comma (,) or hyphen (-). For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7.
Add	Click Add to save your rule to the Switch's run-time memory. The Switch loses this rule if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to their last saved values.
Clear	Click Clear to begin configuring this screen afresh.
Index	Click an index number to modify a static multicast MAC address rule for port(s).
Active	This field displays whether a static multicast MAC address forwarding rule is active (Yes) or not (No). You may temporarily deactivate a rule without deleting it.
Name	This field displays the descriptive name for identification purposes for a static multicast MAC address-forwarding rule.
MAC Address	This field displays the multicast MAC address that identifies a multicast group.
VID	This field displays the ID number of a VLAN group to which frames containing the specified multicast MAC address will be forwarded.
Port	This field displays the port(s) within a identified VLAN group to which frames containing the specified multicast MAC address will be forwarded.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.

Table 58 Advanced Application > Static Multicast Forwarding (continued)

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

CHAPTER 12

Filtering

12.1 Filtering Overview

This chapter discusses MAC address port filtering.

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

12.1.1 What You Can Do

Use the Filtering screen ([Section 12.2 on page 135](#)) to create rules for traffic going through the Switch.

12.2 Configure a Filtering Rule

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

Figure 101 Advanced Application > Filtering

Filtering						
Active	☐					
Name						
Action	☐ Discard source ☐ Discard destination					
MAC						
VID						
Add Cancel Clear						
Index	Active	Name	MAC Address	VID	Action	☐
Delete Cancel						

The following table describes the related labels in this screen.

Table 59 Advanced Application > Filtering

LABEL	DESCRIPTION
Active	Make sure to select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by deselecting this check box.
Name	Type a descriptive name (up to 32 printable ASCII characters) for this rule. This is for identification only.
Action	Select Discard source to drop the frames from the source MAC address (specified in the MAC field). The Switch can still send frames to the MAC address. Select Discard destination to drop the frames to the destination MAC address (specified in the MAC address). The Switch can still receive frames originating from the MAC address. Select Discard source and Discard destination to block traffic to/from the MAC address specified in the MAC field.
MAC	Type a MAC address in valid MAC address format, that is, six hexadecimal character pairs.
VID	Type the VLAN group identification number.
Add	Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Clear	Click Clear to clear the fields to the factory defaults.
Index	This field displays the index number of the rule. Click an index number to change the settings.
Active	This field displays Yes when the rule is activated and No when is it deactivated.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
MAC Address	This field displays the source/destination MAC address with the VLAN identification number to which the MAC address belongs.
VID	This field displays the VLAN group identification number.
Action	This field displays Discard source , Discard destination , or Discard both depending on what you configured above.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Check the rule(s) that you want to remove and then click the Delete button.
Cancel	Click Cancel to clear the selected checkbox(es).

CHAPTER 13

Spanning Tree Protocol

13.1 Spanning Tree Protocol Overview

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

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

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

13.1.1 What You Can Do

- Use the **Spanning Tree Protocol Status** screen ([Section 13.2 on page 139](#)) to view the STP status in the different STP modes (RSTP or MSTP) you can configure on the Switch.
- Use the **Spanning Tree Configuration** screen ([Section 13.3 on page 140](#)) to activate one of the STP modes on the Switch.
- Use the **Rapid Spanning Tree Protocol** screen ([Section 13.4 on page 140](#)) to configure RSTP settings.
- Use the **Rapid Spanning Tree Protocol Status** screen ([Section 13.5 on page 142](#)) to view the RSTP status.
- Use the **Multiple Spanning Tree Protocol** screen ([Section 13.6 on page 144](#)) to configure MSTP.
- Use the **Multiple Spanning Tree Protocol Status** screen ([Section 13.7 on page 148](#)) to view the MSTP status.

13.1.2 What You Need to Know

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

(Rapid) Spanning Tree Protocol

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

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

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

STP Terminology

The root bridge is the base of the spanning tree.

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

Table 60 STP Path Costs

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

On each bridge, the 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 61 STP Port States

PORT STATE	DESCRIPTION
Disabled	STP is disabled (default).
Blocking	Only configuration and management BPDUs are received and processed.

Table 61 STP Port States

PORT STATE	DESCRIPTION
Listening	All BPDUs are received and processed. Note: The listening state does not exist in RSTP.
Learning	All BPDUs are received and processed. Information frames are submitted to the learning process but not forwarded.
Forwarding	All BPDUs are received and processed. All information frames are received and forwarded.

Multiple STP

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

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

13.2 Spanning Tree Protocol Status Screen

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

Figure 102 Advanced Application > Spanning Tree Protocol

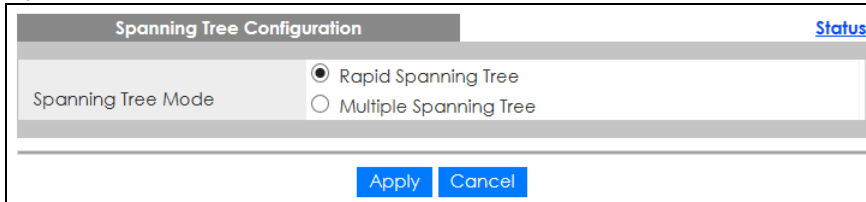
Spanning Tree Protocol Status			Configuration RSTP MSTP		
Spanning Tree Protocol: RSTP					
Bridge	Root	Our Bridge			
Bridge ID	0000-000000000000	0000-000000000000			
Hello Time (second)	0	0			
Max Age (second)	0	0			
Forwarding Delay (second)	0	0			
Cost to Bridge	0				
Port ID	0X0000				
Topology Changed Times	0				
Time Since Last Change	0:00:00				
Port	Port State	Port Role	Designated Bridge ID	Designated Port ID	Designated Cost

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

13.3 Spanning Tree Configuration

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

Figure 103 Advanced Application > Spanning Tree Protocol > Configuration



The following table describes the labels in this screen.

Table 62 Advanced Application > Spanning Tree Protocol > Configuration

LABEL	DESCRIPTION
Spanning Tree Mode	You can activate one of the STP modes on the Switch. Select Rapid Spanning Tree or Multiple Spanning Tree . See Section 13.1 on page 137 for background information on STP.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

13.4 Configure Rapid Spanning Tree Protocol

Use this screen to configure RSTP settings, see [Section 13.1 on page 137](#) for more information on RSTP. Click **RSTP** in the Advanced Application > Spanning Tree Protocol screen.

Figure 104 Advanced Application > Spanning Tree Protocol > RSTP

Rapid Spanning Tree Protocol				Status	
Active	☐				
Bridge Priority	32768 ▼				
Hello Time	2	Seconds			
MAX Age	20	Seconds			
Forwarding Delay	15	Seconds			

Port	Active	Edge	Priority	Path Cost
*	☐	☐		
1	☐	☐	128	2
2	☐	☐	128	2
3	☐	☐	128	2
4	☐	☐	128	2
5	☐	☐	128	2
6	☐	☐	128	2
7	☐	☐	128	2
8	☐	☐	128	2
9	☐	☐	128	2
10	☐	☐	128	2
11	☐	☐	128	2
12	☐	☐	128	2

[Apply](#)
[Cancel](#)

The following table describes the labels in this screen.

Table 63 Advanced Application > Spanning Tree Protocol > RSTP

LABEL	DESCRIPTION
Status	Click Status to display the RSTP Status screen (see Figure 105 on page 143).
Active	Select this check box to activate RSTP. Clear this check box to disable RSTP. Note: You must also activate Rapid Spanning Tree in the Advanced Application > Spanning Tree Protocol > Configuration screen to enable RSTP on the Switch.
Bridge Priority	Bridge priority is used in determining the root switch, root port and designated port. The switch with the highest priority (lowest numeric value) becomes the STP root switch. If all switches have the same priority, the switch with the lowest MAC address will then become the root switch. Select a value from the drop-down list box. The lower the numeric value you assign, the higher the priority for this bridge. Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Max Age	This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.

Table 63 Advanced Application > Spanning Tree Protocol > RSTP (continued)

LABEL	DESCRIPTION
Forwarding Delay	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: Note: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$
Port	This field displays the port number. * means all ports.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to activate RSTP on this port.
Edge	Select this check box to configure a port as an edge port when it is directly attached to a computer. An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost - see Table 60 on page 138 for more information.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

13.5 Rapid Spanning Tree Protocol Status

Click **Advanced Application > Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See [Section 13.1 on page 137](#) for more information on RSTP.

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

Figure 105 Advanced Application > Spanning Tree Protocol > Status: RSTP

Spanning Tree Protocol Status			Configuration	RSTP	MSTP
Spanning Tree Protocol: RSTP					
Bridge	Root	Our Bridge			
Bridge ID	0000-000000000000	0000-000000000000			
Hello Time (second)	0	0			
Max Age (second)	0	0			
Forwarding Delay (second)	0	0			
Cost to Bridge	0				
Port ID	0X0000				
Topology Changed Times	0				
Time Since Last Change	0:00:00				
Port	Port State	Port Role	Designated Bridge ID	Designated Port ID	Designated Cost

The following table describes the labels in this screen.

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

LABEL	DESCRIPTION
Configuration	Click Configuration to specify which STP mode you want to activate.
RSTP	Click RSTP to edit RSTP settings on the Switch.
MSTP	Click MSTP to edit MSTP settings on the Switch.
Bridge	Root refers to the base of the spanning tree (the root bridge). Our Bridge is this switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for Root and Our Bridge if the Switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay.
Max Age (second)	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding). Note: The listening state does not exist in RSTP.
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.
Port	This field displays the number of the port on the Switch.
Port State	This field displays the port state in STP. Discarding - The port does not forward/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 64 Advanced Application > Spanning Tree Protocol > Status: RSTP (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/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.

13.6 Configure Multiple Spanning Tree Protocol

To configure MSTP, click **MSTP** in the Advanced Application > Spanning Tree Protocol screen. See [Multiple STP on page 139](#) for more information on MSTP.

Figure 106 Advanced Application > Spanning Tree Protocol > MSTP

Multiple Spanning Tree Protocol

Status Port

Bridge

Active

☐

Hello Time

2

seconds

MAX Age

20

seconds

Forwarding Delay

15

seconds

Maximum hops

20

Configuration Name

0019cb000001

Revision Number

0

Apply

Cancel

Instance

Instance

Bridge Priority

32768

▼

VLAN Range

Start

End

Add

Remove

Clear

Enabled VLAN(s)

Port	Active	Priority	Path Cost
*	☐		
1	☐	128	2
2	☐	128	2
3	☐	128	2
4	☐	128	2
5	☐	128	2
6	☐	128	2
7	☐	128	2
8	☐	128	2
9	☐	128	2
10	☐	128	2
11	☐	128	2
12	☐	128	2

Add

Cancel

Instance

VLAN

Active Port

☐

0

1-4094

-

Delete

Cancel

The following table describes the labels in this screen.

Table 65 Advanced Application > Spanning Tree Protocol > MSTP

LABEL	DESCRIPTION
Status	Click Status to display the MSTP Status screen (see Figure 108 on page 149).
Port	Click Port to display the MSTP Port screen (see Figure 107 on page 147).
Active	Select this to activate MSTP on the Switch. Clear this to disable MSTP on the Switch. Note: You must also activate Multiple Spanning Tree in the Advanced Application > Spanning Tree Protocol > Configuration screen to enable MSTP on the Switch.

Table 65 Advanced Application > Spanning Tree Protocol > MSTP (continued)

LABEL	DESCRIPTION
Hello Time	This is the time interval in seconds between BPDU (Bridge Protocol Data Units) configuration message generations by the root switch. The allowed range is 1 to 10 seconds.
Max Age	This is the maximum time (in seconds) the Switch can wait without receiving a BPDU before attempting to reconfigure. All Switch ports (except for designated ports) should receive BPDUs at regular intervals. Any port that ages out STP information (provided in the last BPDU) becomes the designated port for the attached LAN. If it is a root port, a new root port is selected from among the Switch ports attached to the network. The allowed range is 6 to 40 seconds.
Forwarding Delay	This is the maximum time (in seconds) the Switch will wait before changing states. This delay is required because every switch must receive information about topology changes before it starts to forward frames. In addition, each port needs time to listen for conflicting information that would make it return to a blocking state; otherwise, temporary data loops might result. The allowed range is 4 to 30 seconds. As a general rule: Note: $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$
Maximum hops	Enter the number of hops (between 1 and 255) in an MSTP region before the BPDU is discarded and the port information is aged.
Configuration Name	Enter a descriptive name (up to 32 characters) of an MST region.
Revision Number	Enter a number to identify a region's configuration. Devices must have the same revision number to belong to the same region.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Instance	Use this section to configure MSTI (Multiple Spanning Tree Instance) settings.
Instance	Enter the number you want to use to identify this MST instance on the Switch. Note: The Switch supports instance numbers 0-16.
Bridge Priority	Set the priority of the Switch for the specific spanning tree instance. The lower the number, the more likely the Switch will be chosen as the root bridge within the spanning tree instance. Enter priority values between 0 and 61440 in increments of 4096 (thus valid values are 4096, 8192, 12288, 16384, 20480, 24576, 28672, 32768, 36864, 40960, 45056, 49152, 53248, 57344 and 61440).
VLAN Range	Enter the start of the VLAN ID range that you want to add or remove from the VLAN range edit area in the Start field. Enter the end of the VLAN ID range that you want to add or remove from the VLAN range edit area in the End field. Next click: Add - to add this range of VLAN(s) to be mapped to the MST instance. Remove - to remove this range of VLAN(s) from being mapped to the MST instance. Clear - to remove all VLAN(s) from being mapped to this MST instance.
Enabled VLAN(s)	This field displays which VLAN(s) are mapped to this MST instance.
Port	This field displays the port number. * means all ports.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to add this port to the MST instance.

Table 65 Advanced Application > Spanning Tree Protocol > MSTP (continued)

LABEL	DESCRIPTION
Priority	Configure the priority for each port here. Priority decides which port should be disabled when more than one port forms a loop in a switch. Ports with a higher priority numeric value are disabled first. The allowed range is between 0 and 255 and the default value is 128.
Path Cost	Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost - see Table 60 on page 138 for more information.
Add	Click Add to save this MST instance to the Switch's run-time memory. The Switch loses this change if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Instance	This field displays the ID of an MST instance. Click this number to modify its settings.
VLAN	This field displays the VID (or VID ranges) to which the MST instance is mapped.
Active Port	This field display the ports configured to participate in the MST instance.
	Select an entry's check box to select a specific entry.
Delete	Check the rule(s) that you want to remove and then click the Delete button.
Cancel	Click Cancel to clear the selected checkbox(es).

13.6.1 Multiple Spanning Tree Protocol Port Configuration

Click **Advanced Application > Spanning Tree Protocol > MSTP > Port** in the navigation panel to display the status screen as shown next. See [Multiple STP on page 139](#) for more information on MSTP.

Figure 107 Advanced Application > Spanning Tree Protocol > MSTP > Port

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

The following table describes the labels in this screen.

Table 66 Advanced Application > Spanning Tree Protocol > MSTP > Port

LABEL	DESCRIPTION
MSTP	Click MSTP to edit MSTP settings on the Switch.
Port	This field displays the port number. * means all ports.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Edge	Select this check box to configure a port as an edge port when it is directly attached to a computer. An edge port changes its initial STP port state from blocking state to forwarding state immediately without going through listening and learning states right after the port is configured as an edge port or when its link status changes. Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

13.7 Multiple Spanning Tree Protocol Status

Click **Advanced Application > Spanning Tree Protocol** in the navigation panel to display the status screen as shown next. See [Multiple STP on page 139](#) for more information on MSTP.

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

Figure 108 Advanced Application > Spanning Tree Protocol > Status: MSTP

Spanning Tree Protocol Status

[Configuration](#)
[RSTP](#)
[MSTP](#)

Spanning Tree Protocol: MSTP
CST

Bridge	Root	Our Bridge
Bridge ID	0000-000000000000	0000-000000000000
Hello Time (second)	0	0
Max Age (second)	0	0
Forwarding Delay (second)	0	0
Cost to Bridge	0	0
Port ID	0x0000	0x0000
Configuration Name	0019cb000001	
Revision Number	0	
Configuration Digest	0	
Topology Changed Times	0	
Time Since Last Change	0:00:00	

Instance

Instance	VLAN
0	1-4094

MSTI 0 ▼

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

Port	Port State	Port Role	Designated Bridge ID	Designated Port ID	Designated Cost

The following table describes the labels in this screen.

Table 67 Advanced Application > Spanning Tree Protocol > Status: MSTP

LABEL	DESCRIPTION
Configuration	Click Configuration to specify which STP mode you want to activate.
RSTP	Click RSTP to edit RSTP settings on the Switch.
MSTP	Click MSTP to edit MSTP settings on the Switch.
CST	This section describes the Common Spanning Tree settings.
Bridge	Root refers to the base of the spanning tree (the root bridge). Our Bridge is this switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for Root and Our Bridge if the Switch is the root switch.
Hello Time (second)	This is the time interval (in seconds) at which the root switch transmits a configuration message. The root bridge determines Hello Time, Max Age and Forwarding Delay.
Max Age (second)	This is the maximum time (in seconds) the Switch can wait without receiving a configuration message before attempting to reconfigure.
Forwarding Delay (second)	This is the time (in seconds) the root switch will wait before changing states (that is, listening to learning to forwarding).
Cost to Bridge	This is the path cost from the root port on this Switch to the root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the Spanning Tree.

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

LABEL	DESCRIPTION
Configuration Name	This field displays the configuration name for this MST region.
Revision Number	This field displays the revision number for this MST region.
Configuration Digest	A configuration digest is generated from the VLAN-MSTI mapping information. This field displays the 16-octet signature that is included in an MSTP BPDU. This field displays the digest when MSTP is activated on the system.
Topology Changed Times	This is the number of times the spanning tree has been reconfigured.
Time Since Last Change	This is the time since the spanning tree was last reconfigured.
Instance	These fields display the MSTI to VLAN mapping. In other words, which VLANs run on each spanning tree instance.
Instance	This field displays the MSTI ID.
VLAN	This field displays which VLANs are mapped to an MSTI.
MSTI	Select the MST instance settings you want to view.
Bridge	Root refers to the base of the MST instance. Our Bridge is this switch. This Switch may also be the root bridge.
Bridge ID	This is the unique identifier for this bridge, consisting of bridge priority plus MAC address. This ID is the same for Root and Our Bridge if the Switch is the root switch.
Internal Cost	This is the path cost from the root port in this MST instance to the regional root switch.
Port ID	This is the priority and number of the port on the Switch through which this Switch must communicate with the root of the MST instance.
Port	This field displays the number of the port on the Switch.
Port State	This field displays the port state in STP. • Discarding - The port does not forward/process received frames or learn MAC addresses, but still listens for BPDUs. • Learning - The port learns MAC addresses and processes BPDUs, but does not forward frames yet. • Forwarding - The port is operating normally. It learns MAC addresses, processes BPDUs and forwards received frames.
Port Role	This field displays the role of the port in STP. • Root - A forwarding port on a non-root bridge, which has the lowest path cost and is the best port from the non-root bridge to the root bridge. A root bridge does not have a root port. • Designated - A forwarding port on the designated bridge for each connected LAN segment. A designated bridge has the lowest path cost to the root bridge among the bridges connected to the LAN segment. All the ports on a root bridge (root switch) are designated ports. • Alternate - A blocked port, which has a best alternate path to the root bridge. This path is different from using the root port. The port moves to the forwarding state when the designated port for the LAN segment fails. • Backup - A blocked port, which has a backup/redundant path to a LAN segment where a designated port is already connected when a switch has two links to the same LAN segment. • Disabled - Not strictly part of STP. The port can be disabled manually.
Designated Bridge ID	This field displays the identifier of the designated bridge to which this port belongs when the port is a designated port. Otherwise, it displays the identifier of the designated bridge for the LAN segment to which this port is connected.

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

LABEL	DESCRIPTION
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.

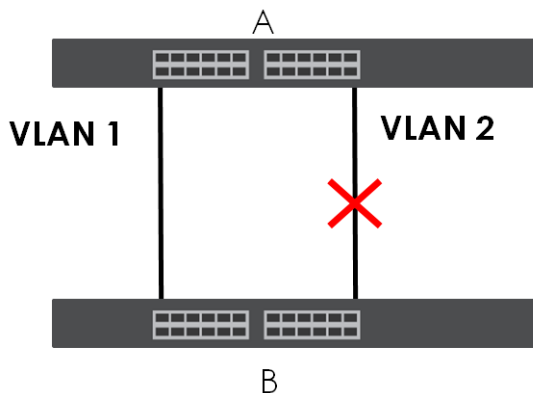
13.8 Technical Reference

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

13.8.1 MSTP Network Example

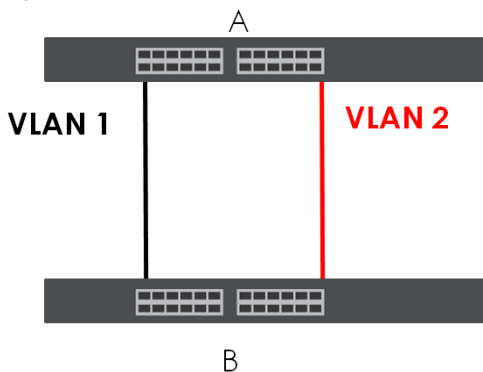
The following figure shows a network example where two VLANs are configured on the two switches. If the switches are using STP or RSTP, the link for VLAN 2 will be blocked as STP and RSTP allow only one link in the network and block the redundant link.

Figure 109 STP/RSTP Network Example



With MSTP, VLANs 1 and 2 are mapped to different spanning trees in the network. Thus traffic from the two VLANs travel on different paths. The following figure shows the network example using MSTP.

Figure 110 MSTP Network Example



13.8.2 MST Region

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

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

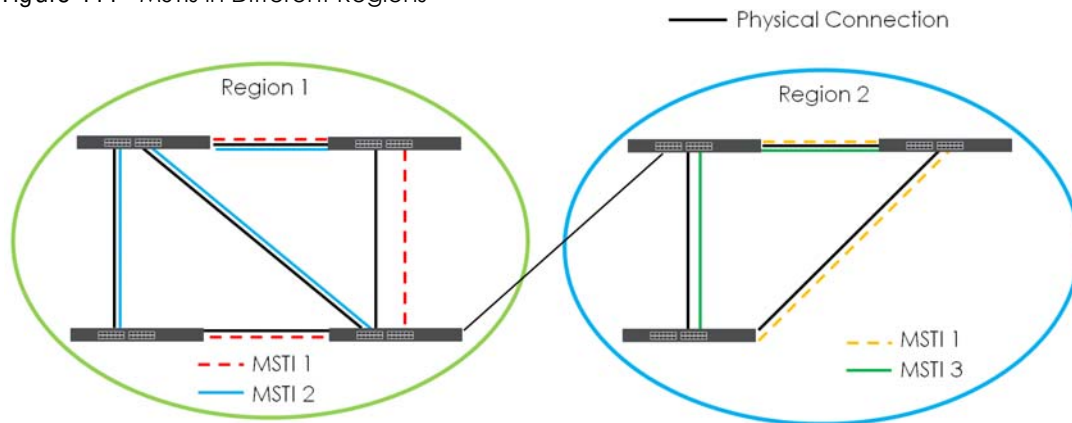
- Name of the MST region
- Revision level as the unique number for the MST region
- VLAN-to-MST Instance mapping

13.8.3 MST Instance

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

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

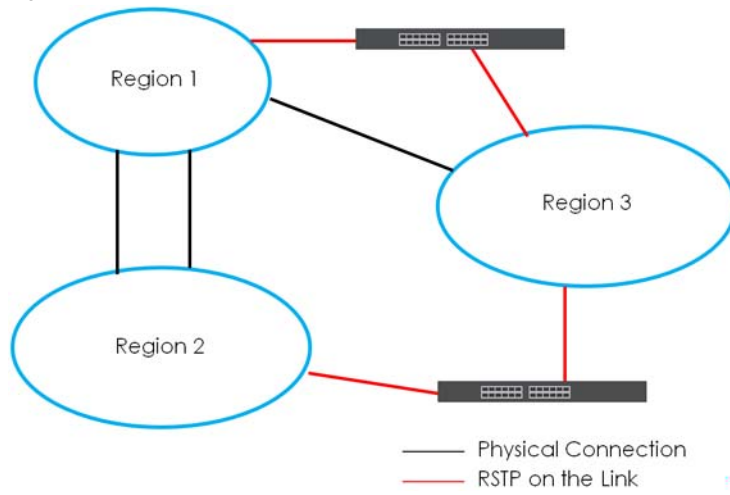
Figure 111 MSTIs in Different Regions



13.8.4 Common and Internal Spanning Tree (CIST)

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

Figure 112 MSTP and Legacy RSTP Network Example



CHAPTER 14

Bandwidth Control

14.1 Bandwidth Control Overview

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

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

14.1.1 What You Can Do

Use the **Bandwidth Control** screen ([Section 14.2 on page 154](#)) to limit the bandwidth for traffic going through the Switch.

14.2 Bandwidth Control Setup

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

Figure 113 Advanced Application > Bandwidth Control

Bandwidth Control						
Active ☐						
Port	Active	Ingress Rate		Active	Egress Rate	
*	☐		kbps	☐		kbps
1	☐	64	kbps	☐	64	kbps
2	☐	64	kbps	☐	64	kbps
3	☐	64	kbps	☐	64	kbps
4	☐	64	kbps	☐	64	kbps
5	☐	64	kbps	☐	64	kbps
6	☐	64	kbps	☐	64	kbps
7	☐	64	kbps	☐	64	kbps
8	☐	64	kbps	☐	64	kbps
9	☐	64	kbps	☐	64	kbps
10	☐	64	kbps	☐	64	kbps
11	☐	64	kbps	☐	64	kbps
12	☐	64	kbps	☐	64	kbps

Apply Cancel

The following table describes the related labels in this screen.

Table 68 Advanced Application > Bandwidth Control

LABEL	DESCRIPTION
Active	Select this check box to enable bandwidth control on the Switch.
Port	This field displays the port number. * means all ports.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to activate ingress rate limits on this port.
Ingress Rate	Specify the maximum bandwidth allowed in kilobits per second (kbps) for the incoming traffic flow on a port. Note: Ingress rate bandwidth control applies to layer 2 traffic only.
Active	Select this check box to activate egress rate limits on this port.
Egress Rate	Specify the maximum bandwidth allowed in kilobits per second (kbps) for the out-going traffic flow on a port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields.

CHAPTER 15

Broadcast Storm Control

15.1 Broadcast Storm Control Overview

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

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

15.1.1 What You Can Do

Use the **Broadcast Storm Control** screen ([Section 15.2 on page 156](#)) to limit the number of broadcast, multicast and destination lookup failure (DLF) packets the Switch receives per second on the ports.

15.2 Broadcast Storm Control Setup

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

Figure 114 Advanced Application > Broadcast Storm Control

Port	Broadcast (pkt/s)	Multicast (pkt/s)	DLF (pkt/s)
*	☐	☐	☐
1	☐ 0	☐ 0	☐ 0
2	☐ 0	☐ 0	☐ 0
3	☐ 0	☐ 0	☐ 0
4	☐ 0	☐ 0	☐ 0
5	☐ 0	☐ 0	☐ 0
6	☐ 0	☐ 0	☐ 0
7	☐ 0	☐ 0	☐ 0
8	☐ 0	☐ 0	☐ 0
9	☐ 0	☐ 0	☐ 0
10	☐ 0	☐ 0	☐ 0
11	☐ 0	☐ 0	☐ 0
12	☐ 0	☐ 0	☐ 0

The following table describes the labels in this screen.

Table 69 Advanced Application > Broadcast Storm Control

LABEL	DESCRIPTION
Active	Select this check box to enable traffic storm control on the Switch. Clear this check box to disable this feature.
Port	This field displays the port number. * 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.
Broadcast (pkt/s)	Select this option and specify how many broadcast packets the port receives per second.
Multicast (pkt/s)	Select this option and specify how many multicast packets the port receives per second.
DLF (pkt/s)	Select this option and specify how many destination lookup failure (DLF) packets the port receives per second.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields.

CHAPTER 16

Mirroring

16.1 Mirroring Overview

This chapter discusses port mirroring setup screens.

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

16.1.1 What You Can Do

Use the Mirroring screen ([Section 16.2 on page 158](#)) to select a monitor port and specify the traffic flow to be copied to the monitor port.

16.2 Port Mirroring Setup

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

Figure 115 Advanced Application > Mirroring

The screenshot shows the 'Mirroring' configuration interface. At the top, there is a title bar labeled 'Mirroring'. Below it, there is an 'Active' checkbox and a 'Monitor Port' dropdown menu. The main part of the screen is a table with three columns: 'Port', 'Mirrored', and 'Direction'. The 'Port' column lists ports from 1 to 12, plus an asterisk (*). The 'Mirrored' column contains checkboxes for each port. The 'Direction' column contains a dropdown menu for each port, all currently set to 'Ingress'. At the bottom of the screen, there are two buttons: 'Apply' and 'Cancel'.

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

The following table describes the labels in this screen.

Table 70 Advanced Application > Mirroring

LABEL	DESCRIPTION
Active	Select this check box to activate port mirroring on the Switch. Clear this check box to disable the feature.
Monitor Port	The monitor port is the port you copy the traffic to in order to examine it in more detail without interfering with the traffic flow on the original port(s). Enter the port number of the monitor port.
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.
Mirrored	Select this option to mirror the traffic on a port.
Direction	Specify the direction of the traffic to mirror by selecting from the drop-down list box. Choices are Egress (outgoing), Ingress (incoming) and Both .
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields.

CHAPTER 17

Link Aggregation

17.1 Link Aggregation Overview

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

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

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

17.1.1 What You Can Do

- Use the **Link Aggregation Status** screen ([Section 17.2 on page 161](#)) to view ports you have configured to be in the trunk group, ports that are currently transmitting data as one logical link in the trunk group and so on.
- Use the **Link Aggregation Setting** screen ([Section 17.3 on page 162](#)) to configure to enable static link aggregation.
- Use the **Link Aggregation Control Protocol** screen ([Section 17.3.1 on page 164](#)) to enable Link Aggregation Control Protocol (LACP).

17.1.2 What You Need to Know

The Switch supports both static and dynamic link aggregation.

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

See [Section 17.4.1 on page 165](#) 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 71 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 72 Link Aggregation ID: Peer Switch

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

17.2 Link Aggregation Status

Click **Advanced Application > Link Aggregation** in the navigation panel. The **Link Aggregation Status** screen displays by default. See [Section 17.1 on page 160](#) for more information.

Figure 116 Advanced Application > Link Aggregation

Link Aggregation Status			Link Aggregation Setting		
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	-

The following table describes the labels in this screen.

Table 73 Advanced Application > Link Aggregation

LABEL	DESCRIPTION
Group ID	This field displays the group ID to identify a trunk group, that is, one logical link containing multiple ports.
Enabled Ports	These are the ports you have configured in the Link Aggregation screen to be in the trunk group. The port number(s) displays only when this trunk group is activated and there is a port belonging to this group.

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

Table 73 Advanced Application > Link Aggregation

LABEL	DESCRIPTION
Synchronized Ports	These are the ports that are currently transmitting data as one logical link in this trunk group.
Aggregator ID	Link Aggregator ID consists of the following: system priority, MAC address, key, port priority and port number. Refer to Link Aggregation ID on page 161 for more information on this field. The ID displays only when there is a port belonging to this trunk group and LACP is also enabled for this group.
Criteria	This shows the outgoing traffic distribution algorithm used in this trunk group. Packets from the same source and/or to the same destination are sent over the same link within the trunk. src-mac means the Switch distributes traffic based on the packet's source MAC address. dst-mac means the Switch distributes traffic based on the packet's destination MAC address. src-dst-mac means the Switch distributes traffic based on a combination of the packet's source and destination MAC addresses. src-ip means the Switch distributes traffic based on the packet's source IP address. dst-ip means the Switch distributes traffic based on the packet's destination IP address. src-dst-ip means the Switch distributes traffic based on a combination of the packet's source and destination IP addresses.
Status	This field displays how these ports were added to the trunk group. It displays: • Static - if the ports are configured as static members of a trunk group. • LACP - if the ports are configured to join a trunk group via LACP.

17.3 Link Aggregation Setting

Click Advanced Application > Link Aggregation > Link Aggregation Setting to display the screen shown next. See [Section 17.1 on page 160](#) for more information on link aggregation.

Figure 117 Advanced Application > Link Aggregation > Link Aggregation Setting

Link Aggregation Setting			Status	LACP
Group ID	Active	Criteria		
T1	☐	src-dst-mac ▼		
T2	☐	src-dst-mac ▼		
T3	☐	src-dst-mac ▼		
T4	☐	src-dst-mac ▼		
T5	☐	src-dst-mac ▼		
T6	☐	src-dst-mac ▼		

Port	Group
1	None ▼
2	None ▼
3	None ▼
4	None ▼
5	None ▼
6	None ▼
7	None ▼
8	None ▼
9	None ▼
10	None ▼
11	None ▼
12	None ▼

The following table describes the labels in this screen.

Table 74 Advanced Application > Link Aggregation > Link Aggregation Setting

LABEL	DESCRIPTION
Link Aggregation Setting	This is the only screen you need to configure to enable static link aggregation.
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports.
Active	Select this option to activate a trunk group.
Criteria	Select the outgoing traffic distribution type. Packets from the same source and/or to the same destination are sent over the same link within the trunk. By default, the Switch uses the src-dst-mac distribution type. If the Switch is behind a router, the packet's destination or source MAC address will be changed. In this case, set the Switch to distribute traffic based on its IP address to make sure port trunking can work properly. Select src-mac to distribute traffic based on the packet's source MAC address. Select dst-mac to distribute traffic based on the packet's destination MAC address. Select src-dst-mac to distribute traffic based on a combination of the packet's source and destination MAC addresses. Select src-ip to distribute traffic based on the packet's source IP address. Select dst-ip to distribute traffic based on the packet's destination IP address. Select src-dst-ip to distribute traffic based on a combination of the packet's source and destination IP addresses.
Port	This field displays the port number.

Table 74 Advanced Application > Link Aggregation > Link Aggregation Setting (continued)

LABEL	DESCRIPTION
Group	Select the trunk group to which a port belongs. Note: When you enable the port security feature on the Switch and configure port security settings for a port, you cannot include the port in an active trunk group.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

17.3.1 Link Aggregation Control Protocol

Click **Advanced Application > Link Aggregation > Link Aggregation Setting > LACP** to display the screen shown next. See [Dynamic Link Aggregation on page 160](#) for more information on dynamic link aggregation.

Figure 118 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP

Link Aggregation Control Protocol

[Link Aggregation Setting](#)

Active

☐

System Priority

65535

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

Port	LACP Timeout
*	30 ▼ seconds
1	30 ▼ seconds
2	30 ▼ seconds
3	30 ▼ seconds
4	30 ▼ seconds
5	30 ▼ seconds
6	30 ▼ seconds
7	30 ▼ seconds
8	30 ▼ seconds
9	30 ▼ seconds
10	30 ▼ seconds
11	30 ▼ seconds
12	30 ▼ seconds

Apply

Cancel

The following table describes the labels in this screen.

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

LABEL	DESCRIPTION
Link Aggregation Control Protocol	Note: Do not configure this screen unless you want to enable dynamic link aggregation.
Active	Select this check box to enable Link Aggregation Control Protocol (LACP).
System Priority	LACP system priority is a number between 1 and 65,535. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP "server". The LACP "server" controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregation Control Protocol (LACP). The smaller the number, the higher the priority level.
Group ID	The field identifies the link aggregation group, that is, one logical link containing multiple ports.
LACP Active	Select this option to enable LACP for a trunk.
Port	This field displays the port number. * 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.
LACP Timeout	Timeout is the time interval between the individual port exchanges of LACP packets in order to check that the peer port in the trunk group is still up. If a port does not respond after three tries, then it is deemed to be "down" and is removed from the trunk. Set a short timeout (one second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible. Select either 1 second or 30 seconds.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

17.4 Technical Reference

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

17.4.1 Static Trunking Example

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

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

Figure 119 Trunking Example - Physical Connections



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

Figure 120 Trunking Example - Configuration Screen

Link Aggregation Setting			Status	LACP
Group ID	Active	Criteria		
T1	☒	src-dst-mac ▼		
T2	☐	src-dst-mac ▼		
T3	☐	src-dst-mac ▼		
T4	☐	src-dst-mac ▼		
T5	☐	src-dst-mac ▼		
T6	☐	src-dst-mac ▼		

Port	Group
1	None ▼
2	T1 ▼
3	T1 ▼
4	T1 ▼
5	T1 ▼
6	None ▼
7	None ▼
8	None ▼
9	None ▼
10	None ▼
11	None ▼
12	None ▼

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

CHAPTER 18

Port Authentication

18.1 Port Authentication Overview

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

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

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

Both types of authentication use the RADIUS (Remote Authentication Dial In User Service, RFC 2138, 2139) protocol to validate users. See [RADIUS on page 204](#) for more information on configuring your RADIUS server settings.

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

18.1.1 What You Can Do

- Use the Port Authentication screen ([Section 18.2 on page 169](#)) to display the links to the configuration screens where you can enable the port authentication methods.
- Use the 802.1x screen ([Section 18.3 on page 169](#)) to activate IEEE 802.1x security.
- Use the MAC Authentication screen ([Section 18.4 on page 172](#)) to activate MAC authentication.

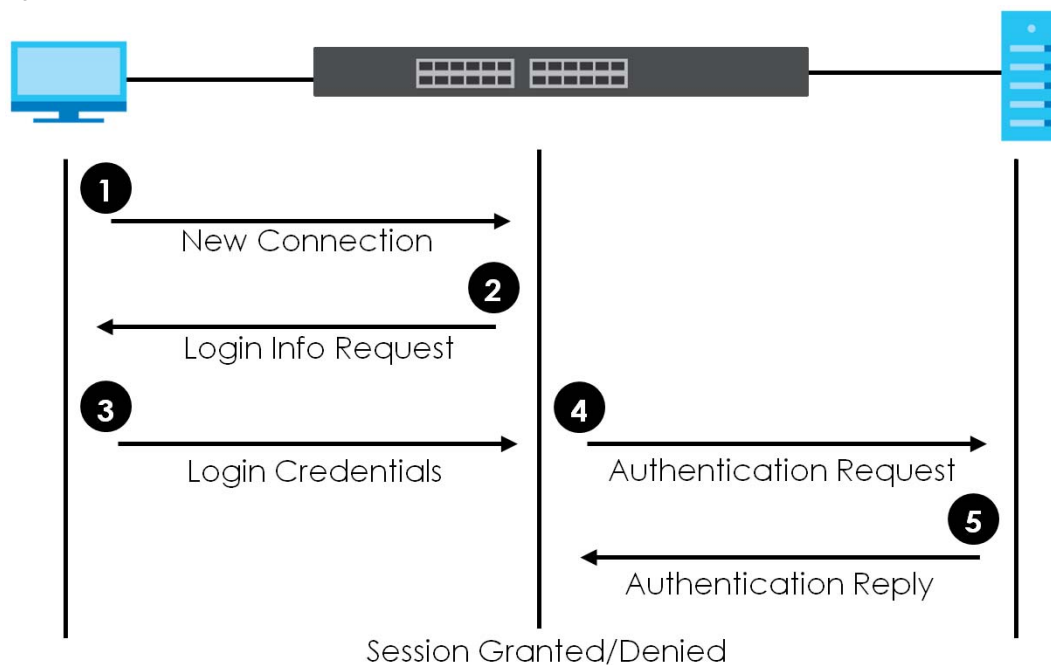
18.1.2 What You Need to Know

IEEE 802.1x Authentication

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

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

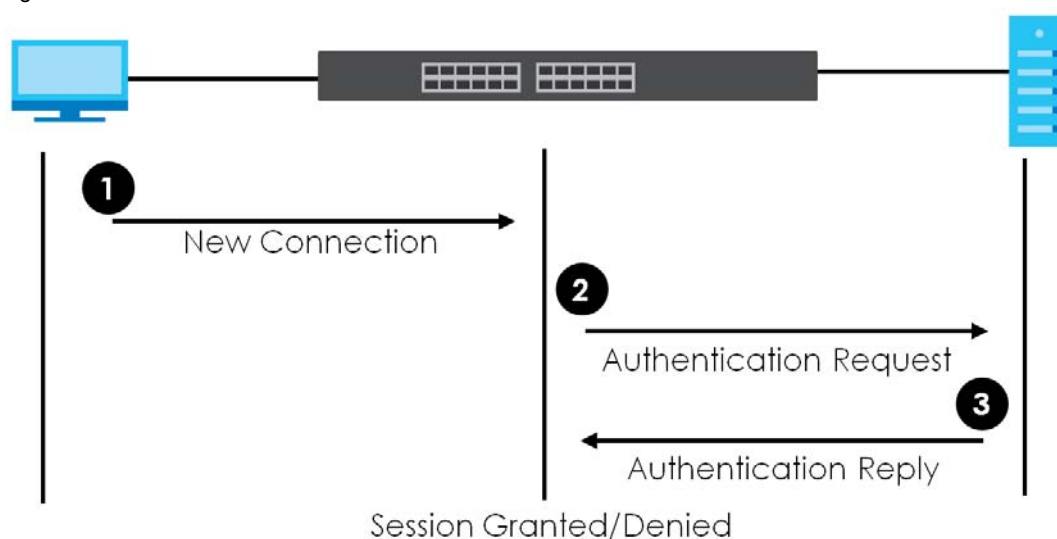
Figure 121 IEEE 802.1x Authentication Process



18.1.3 MAC Authentication

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

Figure 122 MAC Authentication Process



18.2 Port Authentication Configuration

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

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

Figure 123 Advanced Application > Port Authentication

Port Authentication	
802.1x	Click here
MAC Authentication	Click here

18.3 Activate IEEE 802.1x Security

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

Figure 124 Advanced Application > Port Authentication > 802.1x

802.1x										Port Authentication	Guest Vlan
Active	☐										
EAPOL flood	☐										

Port	Active	Max-Req	Reauth	Reauth-period secs	Quiet-period secs	Tx-period secs	Supp-Timeout secs
*	☐		On ▼				
1	☐	2	On ▼	3600	60	30	30
2	☐	2	On ▼	3600	60	30	30
3	☐	2	On ▼	3600	60	30	30
4	☐	2	On ▼	3600	60	30	30
5	☐	2	On ▼	3600	60	30	30
6	☐	2	On ▼	3600	60	30	30
7	☐	2	On ▼	3600	60	30	30
8	☐	2	On ▼	3600	60	30	30
9	☐	2	On ▼	3600	60	30	30
10	☐	2	On ▼	3600	60	30	30
11	☐	2	On ▼	3600	60	30	30
12	☐	2	On ▼	3600	60	30	30

The following table describes the labels in this screen.

Table 76 Advanced Application > Port Authentication > 802.1x

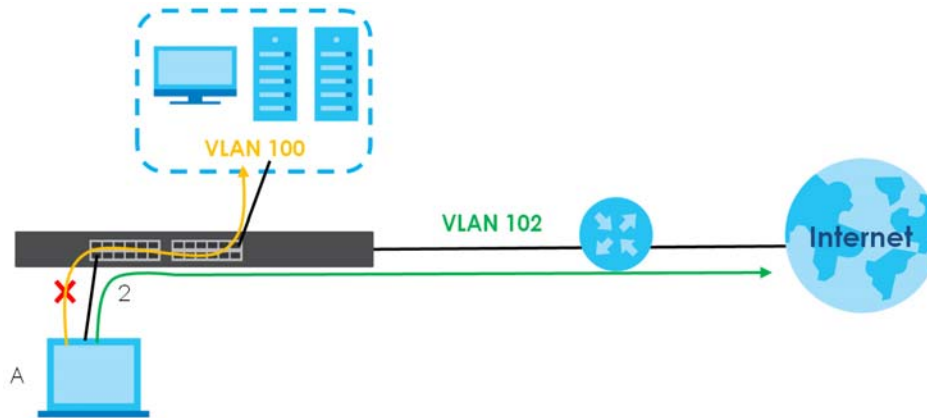
LABEL	DESCRIPTION
Active	Select this check box to permit 802.1x authentication on the Switch. Note: You must first enable 802.1x authentication on the Switch before configuring it on each port.
EAPOL flood	Select this check box to flood EAPoL packets to all ports in the same VLAN. EAP over LAN (EAPOL) is a port authentication protocol used in IEEE 802.1x. It is used to encapsulate and transmit EAP packets between the supplicant (a client device that requests access to the network resources or services) and authenticator (the Switch) directly over the LAN. Note: EAPOL flood will not take effect when 802.1x authentication is enabled.
Port	This field displays the port number. * means all ports.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this to permit 802.1x authentication on this port. You must first allow 802.1x authentication on the Switch before configuring it on each port.
Max-Req	Specify the number of times the Switch tries to authenticate client(s) before sending unresponsive ports to the Guest VLAN. This is set to 2 by default. That is, the Switch attempts to authenticate a client twice. If the client does not respond to the first authentication request, the Switch tries again. If the client still does not respond to the second request, the Switch sends the client to the Guest VLAN. The client needs to send a new request to be authenticated by the Switch again.
Reauth	Specify if a subscriber has to periodically re-enter his or her username and password to stay connected to the port.
Reauth-period secs	Specify the length of time required to pass before a client has to re-enter his or her username and password to stay connected to the port.
Quiet-period secs	Specify the number of seconds the port remains in the HELD state and rejects further authentication requests from the connected client after a failed authentication exchange.
Tx-period secs	Specify the number of seconds the Switch waits for client's response before re-sending an identity request to the client.
Supp-Timeout secs	Specify the number of seconds the Switch waits for client's response to a challenge request before sending another request.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

18.3.1 Guest VLAN

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

VLAN, such as the Internet. The rights granted to the Guest VLAN depends on how the network administrator configures switches or routers with the guest network feature.

Figure 125 Guest VLAN Example



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

Figure 126 Advanced Application > Port Authentication > 802.1x > Guest VLAN

Guest Vlan		802.1x			
Port	Active	Guest Vlan	Host-mode	Multi-Secure Num	
*	☐		Multi-Host ▼		
1	☐	1	Multi-Host ▼	1	
2	☐	1	Multi-Host ▼	1	
3	☐	1	Multi-Host ▼	1	
4	☐	1	Multi-Host ▼	1	
5	☐	1	Multi-Host ▼	1	
6	☐	1	Multi-Host ▼	1	
7	☐	1	Multi-Host ▼	1	
8	☐	1	Multi-Host ▼	1	
9	☐	1	Multi-Host ▼	1	
10	☐	1	Multi-Host ▼	1	
11	☐	1	Multi-Host ▼	1	
12	☐	1	Multi-Host ▼	1	
Apply Cancel					

The following table describes the labels in this screen.

Table 77 Advanced Application > Port Authentication > 802.1x > Guest VLAN

LABEL	DESCRIPTION
Port	This field displays a port number. * means all ports.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable the guest VLAN feature on this port. Clients that fail authentication are placed in the guest VLAN and can receive limited services.

Table 77 Advanced Application > Port Authentication > 802.1x > 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, 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 that the Switch will authenticate on this port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

18.4 Activate MAC Authentication

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

Figure 127 Advanced Application > Port Authentication > MAC Authentication

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

The following table describes the labels in this screen.

Table 78 Advanced Application > Port Authentication > MAC Authentication

LABEL	DESCRIPTION
Active	Select this check box to permit MAC authentication on the Switch. Note: You must first enable MAC authentication on the Switch before configuring it on each port.
Name Prefix	Type the prefix that is appended to all MAC addresses sent to the RADIUS server for authentication. You can enter up to 32 printable ASCII characters. If you leave this field blank, then only the MAC address of the client is forwarded to the RADIUS server.
Delimiter	Select the delimiter the RADIUS server uses to separate the pairs in MAC addresses used as the account username (and password). You can select Dash (-), Colon (:), or None to use no delimiters at all in the MAC address.
Case	Select the case (Upper or Lower) the RADIUS server requires for letters in MAC addresses used as the account username (and password).
Password Type	Select Static to have the Switch send the password you specify below or MAC-Address to use the client MAC address as the password.
Password	Type the password the Switch sends along with the MAC address of a client for authentication with the RADIUS server. You can enter up to 32 printable ASCII characters.

Table 78 Advanced Application > Port Authentication > MAC Authentication (continued)

LABEL	DESCRIPTION
Timeout	Specify the amount of time before the Switch allows a client MAC address that fails authentication to try and authenticate again. Maximum time is 3000 seconds. When a client fails MAC authentication, its MAC address is learned by the MAC address table with a status of denied. The timeout period you specify here is the time the MAC address entry stays in the MAC address table until it is cleared. If you specify 0 for the timeout value, the Switch uses the Aging Time configured in the Switch Setup screen. Note: If the Aging Time in the Switch Setup screen is set to a lower value, then it supersedes this setting. See Section 8.5 on page 84.
Port	This field displays a port number. * means all ports.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to permit MAC authentication on this port. You must first allow MAC authentication on the Switch before configuring it on each port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 19

Port Security

19.1 Port Security Overview

This chapter shows you how to set up port security.

Port security allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the Switch. The Switch can learn up to 16K MAC addresses in total with no limit on individual ports other than the sum cannot exceed 16K.

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

19.1.1 What You Can Do

Use the Port Security screen ([Section 19.2 on page 175](#)) to enable port security and disable MAC address learning. You can also enable the port security feature on a port.

19.2 Port Security Setup

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

Figure 128 Advanced Application > Port Security

Port Security			
Active ☐			
Port	Active	Address Learning	Limited Number of Learned MAC Address
*	☐	☒	
1	☐	☒	0
2	☐	☒	0
3	☐	☒	0
4	☐	☒	0
5	☐	☒	0
6	☐	☒	0
7	☐	☒	0
8	☐	☒	0
9	☐	☒	0
10	☐	☒	0
11	☐	☒	0
12	☐	☒	0
Apply Cancel			

The following table describes the labels in this screen.

Table 79 Advanced Application > Port Security

LABEL	DESCRIPTION
Port Security	
Active	Select this option to enable port security on the Switch.
Port	This field displays the port number. * means all ports.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable the port security feature on this port. The Switch forwards packets whose MAC address(es) is in the MAC address table on this port. Packets with no matching MAC address(es) are dropped. Clear this check box to disable the port security feature. The Switch forwards all packets on this port.
Address Learning	MAC address learning reduces outgoing broadcast traffic. For MAC address learning to occur on a port, the port itself must be active with address learning enabled.
Limited Number of Learned MAC Address	Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device would have to wait until one of the five learned MAC addresses aged out. MAC address aging out time can be set in the Switch Setup screen. The valid range is from "0" to "16K". "0" means this feature is disabled.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 20

Time Range

20.1 Time Range Overview

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

20.1.1 What You Can Do

Use the Time Range screen ([Section 20.2 on page 177](#)) to view or define a schedule on the Switch.

20.2 Configuring Time Range

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

Figure 129 Advanced Application > Time Range

Time Range			
Name			
Type	☒ Absolute ☐ Periodic		
Absolute	Start	1970 ▾ 01 ▾ 01 ▾ 00 ▾ : 00 ▾	
	End	1970 ▾ 01 ▾ 01 ▾ 00 ▾ : 00 ▾	
Periodic	☒ Monday ▾ 00 ▾ : 00 ▾ to Monday ▾ 00 ▾ : 00 ▾		
	☐ Mon ☐ Tue ☐ Wed ☐ Thu ☐ Fri ☐ Sat ☐ Sun ☐ Weekdays ☐ Weekend		
	☐ Daily 00 ▾ : 00 ▾ to 00 ▾ : 00 ▾		
Add Cancel Clear			
Index	Name	Type	Range
Delete Cancel			

The following table describes the labels in this screen.

Table 80 Advanced Application > Time Range

LABEL	DESCRIPTION
Name	Enter a descriptive name for this rule for identifying purposes.
Type	Select Absolute to create a one-time schedule. One-time schedules begin on a specific start date and time and end on a specific stop date and time. One-time schedules are useful for long holidays and vacation periods. Alternatively, select Periodic to create a recurring schedule. Recurring schedules begin at a specific start time and end at a specific stop time on selected days of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday). Recurring schedules are useful for defining the workday and off-work hours.
Absolute	This section is available only when you set Type to Absolute .
Start	Specify the year, month, day, hour and minute when the schedule begins.
End	Specify the year, month, day, hour and minute when the schedule ends.
Periodic	This section is available only when you set Type to Periodic. Select the first option if you want to define a recurring schedule for a consecutive time period. You then select the day of the week, hour and minute when the schedule begins and ends respectively. Select the second option if you want to define a recurring schedule for multiple non-consecutive time periods. You need to select each day of the week the recurring schedule is effective. You also need to specify the hour and minute when the schedule begins and ends each day. The schedule begins and ends in the same day.
Add	Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Clear	Click Clear to clear the fields to the factory defaults.
Index	This field displays the index number of the rule. Click an index number to change the settings.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
Type	This field displays the type of the schedule.
Range	This field displays the time period(s) to which this schedule applies.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Check the rule(s) that you want to remove and then click the Delete button.
Cancel	Click Cancel to clear the selected checkbox(es).

CHAPTER 21

Classifier

21.1 Classifier Overview

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

21.1.1 What You Can Do

- Use the **Classifier Status** screen ([Section 21.2 on page 179](#)) to view the classifiers configured on the Switch and how many times the traffic matches the rules.
- Use the **Classifier Configuration** screen ([Section 21.3 on page 180](#)) to define the classifiers and view a summary of the classifier configuration. After you define the classifier, you can specify actions (or policy) to act upon the traffic that matches the rules.
- Use the **Classifier Global Setting** screen ([Section 21.4 on page 185](#)) to configure the match order and enable logging on the Switch.

21.1.2 What You Need to Know

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

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

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

- 1 Configure classifiers to sort traffic into different flows.
- 2 Configure policy rules to define actions to be performed on a classified traffic flow (refer to [Chapter 22 on page 188](#) to configure policy rules).

21.2 Classifier Status

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

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

Figure 130 Advanced Application > Classifier

Index	Active	Weight	Name	Match Count	Rule
1	Yes	32767	Class1	-	EtherType = IP; log;

☒ Any
☐ Classifier

Clear

The following table describes the labels in this screen.

Table 81 Advanced Application > Classifier

LABEL	DESCRIPTION
Index	This field displays the index number of the rule. Click an index number to edit the rule.
Active	This field displays Yes when the rule is activated and No when it is deactivated.
Weight	This field displays the rule's weight. This is to indicate a rule's priority when the match order is set to manual in the Classifier > Classifier Configuration > Classifier Global Setting screen. The higher the number, the higher the rule's priority.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
Match Count	This field displays the number of times a rule is applied. It displays '-' if the rule does not have count enabled.
Rule	This field displays a summary of the classifier rule's settings.
Clear	Select 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.

21.3 Classifier Configuration

Use the **Classifier Configuration** screen to define the classifiers. After you define the classifier, you can specify actions (or policy) to act upon the traffic that matches the rules. To configure policy rules, refer to [Chapter 22 on page 188](#).

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

Figure 131 Advanced Application > Classifier > Classifier Configuration

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

Index	Active	Weight	Name	Rule
Delete Cancel				

The following table describes the labels in this screen.

Table 82 Advanced Application > Classifier > Classifier Configuration

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

Table 82 Advanced Application > Classifier > Classifier Configuration (continued)

LABEL	DESCRIPTION
Weight	Enter a number between 0 and 65535 to specify the rule's weight. When the match order is in manual mode in the Classifier Global Setting screen, a higher weight means a higher priority.
Log	Select this option to have the Switch create a log message when the rule is applied and record the number of matched packets in a particular time interval. Note: Make sure you also enable logging in the Classifier Global Setting screen.
Count	Select this option to have the Switch count how many times the rule is applied.
Time Range	Select the name of the pre-configured schedule that you want to apply to the rule. The rule will be active only at the scheduled date and/or time. If you select None , the rule will be active all the time.
Ingress Port	
Port	Type the port number to which the rule should be applied. You may choose one port only or all ports (Any).
Trunk	Select Any to apply the rule to all trunk groups. To specify a trunk group, select the second choice and type a trunk group ID.
Layer 2	
Specify the fields below to configure a layer 2 classifier.	
VLAN	
VLAN	Select Any to classify traffic from any VLAN or select the second option and specify the source VLAN ID in the field provided.
Priority	
Priority	Select Any to classify traffic from any priority level or select the second option and specify a priority level in the field provided.
Ethernet Type	Select an Ethernet type or select Other and enter the Ethernet type number in hexadecimal value. Refer to Table 84 on page 184 for information.
Source	
MAC Address	Select Any to apply the rule to all MAC addresses. To specify a source, select MAC/Mask to enter the source MAC address of the packet in valid MAC address format (six hexadecimal character pairs) and type the mask for the specified MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified MAC address that the traffic's MAC address should match. Enter "0" for the bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria. If you leave the Mask field blank, the Switch automatically sets the mask to ff:ff:ff:ff:ff:ff.
Destination	
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 bit(s) of the matched traffic's MAC address, which can be of any hexadecimal character(s). For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria. If you leave the Mask field blank, the Switch automatically sets the mask to ff:ff:ff:ff:ff:ff.
Layer 3	
Specify the fields below to configure a layer 3 classifier.	

Table 82 Advanced Application > Classifier > Classifier Configuration (continued)

LABEL	DESCRIPTION
DSCP IPv4/IPv6	Select Any to classify traffic from any DSCP or select the second option and specify a DSCP (DiffServ Code Point) number between 0 and 63 in the field provided.
Precedence	Select Any to classify traffic from any precedence or select the second option and specify an IP Precedence (the first 3 bits of the 8-bit ToS field) value between 0 and 7 in the field provided.
ToS	Select Any to classify traffic from any ToS or select the second option and specify Type of Service (the last 5 bits of the 8-bit ToS field) value between 0 and 255 in the field provided.
IP Protocol	Select an IPv4 protocol type or select Other and enter the protocol number in decimal value. Refer to Table 85 on page 185 for more information. You may select Establish Only for TCP protocol type. This means that the Switch will pick out the packets that are sent to establish TCP connections.
IPv6 Next Header	Select an IPv6 protocol type or select Other and enter an 8-bit next header in the IPv6 packet. The Next Header field is similar to the IPv4 Protocol field. The IPv6 protocol number ranges from 1 to 255. You may select Establish Only for TCP protocol type. This means that the Switch will identify packets that initiate or acknowledge (establish) TCP connections.
Source	
IP Address/ Address Prefix	Enter a source IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask. A subnet mask can be represented in a 32-bit notation. For example, the subnet mask "255.255.255.0" can be represented as "11111111.11111111.11111111.00000000", and counting up the number of ones in this case results in 24.
Destination	
IP Address/ Address Prefix	Enter a destination IP address in dotted decimal notation. Specify the address prefix by entering the number of ones in the subnet mask.
Layer 4	
Specify the fields below to configure a layer 4 classifier.	
Source	
Socket Number	Note: You must select either UDP or TCP in the IP Protocol field before you configure the socket numbers. Select Any to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number. Refer to Table 86 on page 185 for more information.
Destination	
Socket Number	Note: You must select either UDP or TCP in the IP Protocol field before you configure the socket numbers. Select Any to apply the rule to all TCP/UDP protocol port numbers or select the second option and enter a TCP/UDP protocol port number. Refer to Table 86 on page 185 for more information.
Add	Click Add to insert the entry in the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields back to your previous configuration.
Clear	Click Clear to set the above fields back to the factory defaults.

21.3.1 Viewing and Editing Classifier Configuration Summary

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

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

Figure 132 Advanced Application > Classifier > Classifier Configuration: Summary Table

Index	Active	Weight	Name	Rule	☐
1	Yes	32767	Class1	EtherType = IP; log:	☐
Delete Cancel					

The following table describes the labels in this screen.

Table 83 Advanced Application > Classifier > Classifier Configuration: Summary Table

LABEL	DESCRIPTION
Index	This field displays the index number of the rule. Click an index number to edit the rule.
Active	This field displays Yes when the rule is activated and No when it is deactivated.
Weight	The field displays the priority of the rule when the match order is in manual mode. A higher weight means a higher priority.
Name	This field displays the descriptive name for this rule. This is for identification purpose only.
Rule	This field displays a summary of the classifier rule's settings.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the check boxes.

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

Table 84 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 85 Common IP Protocol Types and Protocol Numbers

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

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

Table 86 Common TCP and UDP Port Numbers

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

See [Appendix B on page 358](#) for information on commonly used port numbers.

21.4 Classifier Global Setting Configuration

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

Figure 133 Advanced Application > Classifier > Classifier Configuration > Classifier Global Setting

Classifier Global Setting		Classifier Configuration
Match Order	auto ▼	
Logging	Active ☐	
	Interval 3600 Second(s)	
Apply Cancel		

The following table describes the labels in this screen.

Table 87 Advanced Application > Classifier > Classifier Configuration > Classifier Global Setting

LABEL	DESCRIPTION
Match Order	Select manual to have classifier rules applied according to the weight of each rule you configured in Advanced Application > Classifier > Classifier Configuration . Alternatively, select auto to have classifier rules applied according to the layer of the item configured in the rule. Layer-4 items have the highest priority, and layer-2 items has the lowest priority. For example, you configure a layer-2 item (VLAN ID) in classifier A and configure a layer-3 item (source IP address) in classifier B. When an incoming packet matches both classifier rules, classifier B has priority over classifier A.
Logging	
Active	Select this to allow the Switch to create a log when packets match a classifier rule during a defined time interval.
Interval	Select the length of the time period (in seconds) to count matched packets for a classifier rule. Enter an integer from 0-65535. 0 means that no logging is done.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

21.5 Classifier Example

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

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

Figure 134 Classifier: Example

Classifier Configuration		Classifier Status Classifier Global Setting		
Active	☒			
Name	Example			
Weight	32767			
Log	☐			
Count	☐			
Time Range	None ▼			
Ingress Port	Port	☐ Any ☒ 2		
	Trunk	☒ Any ☐		
Layer 2	VLAN	☒ Any ☐		
	Priority	☒ Any ☐ 0 ▼		
	Ethernet Type	☒ All ☐ Others (Hex)		
	Source	☐ Any ☒ MAC Address	00:50:ba:ad:4f:81	
Layer 3	Destination	☒ Any ☐ MAC Address ☐ /Mask		
	DSCP	IPv4	☒ Any ☐	
		IPv6	☒ Any ☐	
	Precedence	☒ Any ☐		
	ToS	☒ Any ☐		
	IP Protocol	☒ All ☐ Others (Dec)	Establish Only	
	IPv6 Next Header	☒ All ☐ Others (Dec)	Establish Only	
	Source	IP Address / Address Prefix		
	Destination	IP Address / Address Prefix		
	Layer 4	Source	☒ Any ☐ Socket Number	To
Destination		☒ Any ☐ Socket Number	To	

[Add](#) [Cancel](#) [Clear](#)

Index	Active	Weight	Name	Rule
Delete Cancel				

CHAPTER 22

Policy Rule

22.1 Policy Rules Overview

This chapter shows you how to configure policy rules.

A classifier distinguishes traffic into flows based on the configured criteria (refer to [Chapter 21 on page 179](#) for more information). A policy rule ensures that a traffic flow gets the requested treatment in the network.

22.1.1 What You Can Do

Use the **Policy Rule** screen ([Section 22.2 on page 188](#)) to enable the policy and display the active classifier(s) you configure in the **Classifier** screen.

22.2 Configuring Policy Rules

You must first configure a classifier in the **Classifier** screen. Refer to [Section 21.3 on page 180](#) for more information.

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

Figure 135 Advanced Application > Policy Rule

Policy			
Active	☐		
Name			
Classifier(s)	Class1		
Parameters	General		Rate Limit
	VLAN ID		Bandwidth kbps
	Egress Port	1	
	Priority	0 ▼	
Action	Forwarding		
	☒ No change		
	☐ Discard the packet		
	Priority		
	☒ No change		
	☐ Set the packet's 802.1p priority		
	Outgoing		
	☐ Send the packet to the mirror port ☐ Send the packet to the egress port ☐ Set the packet's VLAN ID		
Rate Limit			
☐ Enable			
Add Cancel Clear			
Index	Active	Name	Classifier(s)
Delete Cancel			

The following table describes the labels in this screen.

Table 88 Advanced Application > Policy Rule

LABEL	DESCRIPTION
Active	Select this option to enable the policy.
Name	Enter a descriptive name for identification purposes.
Classifier(s)	This field displays the active classifier(s) you configure in the Classifier screen. Select the classifier(s) to which this policy rule applies. To select more than one classifier, press [SHIFT] and select the choices at the same time.
Parameters	Set the fields below for this policy. You only have to set the field(s) that is related to the action(s) you configure in the Action field.
General	
VLAN ID	Specify a VLAN ID.
Egress Port	Type the number of an outgoing port.
Priority	Specify a priority level.
Rate Limit	You can configure the desired bandwidth available to a traffic flow. Traffic that exceeds the maximum bandwidth allocated (in cases where the network is congested) is called out-of-profile traffic.
Bandwidth	Specify the bandwidth in kilobit per second (kbps). Enter a number between 1 and 1000000.

Table 88 Advanced Application > Policy Rule (continued)

LABEL	DESCRIPTION
Action Specify the action(s) the Switch takes on the associated classified traffic flow. Note: You can specify only one action (pair) in a policy rule. To have the Switch take multiple actions on the same traffic flow, you need to define multiple classifiers with the same criteria and apply different policy rules. Say you have several classifiers that identify the same traffic flow and you specify a different policy rule for each. If their policy actions conflict (Discard the packet, Send the packet to the egress port and Rate Limit), the Switch only applies the policy rules with the Discard the packet and Send the packet to the egress port actions depending on the classifier names. The longer the classifier name, the higher the classifier priority. If two classifier names are the same length, the bigger the character, the higher the classifier priority. The lowercase letters (such as a and b) have higher priority than the capitals (such as A and B) in the classifier name. For example, the classifier with the name of class 2, class a or class B takes priority over the classifier with the name of class 1 or class A. Let's say you set two classifiers (Class 1 and Class 2) and both identify all traffic from MAC address 11:22:33:44:55:66 on port 3. If Policy 1 applies to Class 1 and the action is to drop the packets, Policy 2 applies to Class 2 and the action is to forward the packets to the egress port, the Switch will forward the packets. If Policy 1 applies to Class 1 and the action is to drop the packets, Policy 2 applies to Class 2 and the action is to enable bandwidth limitation, the Switch will discard the packets immediately. If Policy 1 applies to Class 1 and the action is to forward the packets to the egress port, Policy 2 applies to Class 2 and the action is to enable bandwidth limitation, the Switch will forward the packets.	
Forwarding	Select No change to forward the packets. Select Discard the packet to drop the packets.
Priority	Select No change to keep the priority setting of the frames. Select Set the packet's 802.1p priority to replace the packet's 802.1p priority field with the value you set in the Priority field.
Outgoing	Select Send the packet to the mirror port to send the packet to the mirror port. Select Send the packet to the egress port to send the packet to the egress port. Select Set the packet's VLAN ID to set the packet's VLAN ID.
Rate Limit	Select Enable to activate bandwidth limitation on the traffic flow(s) then set the actions to be taken on out-of-profile packets.
Add	Click Add to inset the entry to the summary table below and save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields back to your previous configuration.
Clear	Click Clear to set the above fields back to the factory defaults.
Index	This field displays the policy index number. Click an index number to edit the policy.
Active	This field displays Yes when policy is activated and No when is it deactivated.
Name	This field displays the name you have assigned to this policy.
Classifier(s)	This field displays the name(s) of the classifier to which this policy applies.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the check boxes.

22.3 Policy Example

The figure below shows an example Policy screen where you configure a policy to limit bandwidth on a traffic flow classified using the **Example** classifier (refer to [Section 21.5 on page 186](#)).

Figure 136 Policy Example

Policy	
Active	☒
Name	Test
Classifier(s)	Example
Parameters	General VLAN ID Egress Port 1 Priority 0
	Forwarding ☒ No change ☐ Discard the packet
	Priority ☒ No change ☐ Set the packet's 802.1p priority
Action	Outgoing ☐ Send the packet to the mirror port ☐ Send the packet to the egress port ☐ Set the packet's VLAN ID
	Rate Limit ☐ Enable
	Bandwidth Rate Limit 10000 kbps

CHAPTER 23

Queuing Method

23.1 Queuing Method Overview

This chapter introduces the queuing methods supported.

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

23.1.1 What You Can Do

Use the **Queuing Method** screen ([Section 23.2 on page 193](#)) set priorities for the queues of the Switch. This distributes bandwidth across the different traffic queues.

23.1.2 What You Need to Know

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

Strictly Priority Queuing

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

Weighted Fair Queuing

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

Weighted Round Robin Scheduling (WRR)

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

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

23.2 Configuring Queuing

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

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

Figure 137 Advanced Application > Queuing Method

Queuing Method										
Port	Method	Q0	Q1	Q2	Q3	Q4	Q5	Q6	Q7	Hybrid-SPQ Lowest-Queue
*	SPQ ▼									None ▼
1	☒ SPQ ☐ WFQ ☐ WRR	1	2	3	4	5	6	7	8	None ▼
2	☒ SPQ ☐ WFQ ☐ WRR	1	2	3	4	5	6	7	8	None ▼
3	☒ SPQ ☐ WFQ ☐ WRR	1	2	3	4	5	6	7	8	None ▼
4	☒ SPQ ☐ WFQ ☐ WRR	1	2	3	4	5	6	7	8	None ▼
5	☒ SPQ ☐ WFQ ☐ WRR	1	2	3	4	5	6	7	8	None ▼
6	☒ SPQ ☐ WFQ ☐ WRR	1	2	3	4	5	6	7	8	None ▼
7	☒ SPQ ☐ WFQ ☐ WRR	1	2	3	4	5	6	7	8	None ▼
12	☒ SPQ ☐ WFQ ☐ WRR	1	2	3	4	5	6	7	8	None ▼

Apply Cancel

The following table describes the labels in this screen.

Table 89 Advanced Application > Queuing Method

LABEL	DESCRIPTION
Port	This label shows the port you are configuring. * 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.
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 queue(s) after and including the specified queue for the port. For example, if you select Q5, the Switch services traffic on Q5, Q6 and Q7 using SPQ. Select None to always use WFQ or WRR for the port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 24

Multicast

24.1 Multicast Overview

This chapter shows you how to configure various multicast features.

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

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

24.1.1 What You Can Do

- Use the **Multicast Setup** screen ([Section 24.2 on page 196](#)) to display the links to the configuration screens where you can configure IPv4 or IPv6 multicast settings.
- Use the **IPv4 Multicast Status** screen ([Section 24.3 on page 196](#)) to view multicast group information.
- Use the **IGMP Snooping** screen ([Section 24.3.1 on page 197](#)) to enable IGMP snooping to forward group multicast traffic only to ports that are members of that group.
- Use the **IGMP Snooping VLAN** screen ([Section 24.3.2 on page 200](#)) to perform IGMP snooping on up to 16 VLANs.
- Use the **IGMP Filtering Profile** ([Section 24.3.3 on page 201](#)) to specify a range of multicast groups that clients connected to the Switch are able to join.

24.1.2 What You Need to Know

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

IP Multicast Addresses

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

IGMP Snooping

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

24.2 Multicast Setup

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

Figure 138 Advanced Application > Multicast Setup



The following table describes the labels in this screen.

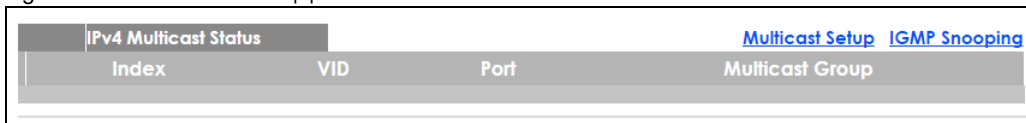
Table 90 Advanced Application > Multicast Setup

LABEL	DESCRIPTION
IPv4 Multicast	Click the link to open screens where you can configure IGMP snooping and IGMP filtering for IPv4.

24.3 IPv4 Multicast Status

Click **Advanced Application > Multicast > IPv4 Multicast** to display the screen as shown. This screen shows the IPv4 multicast group information. See [Section 24.1 on page 195](#) for more information on multicasting.

Figure 139 Advanced Application > Multicast > IPv4 Multicast



The following table describes the labels in this screen.

Table 91 Advanced Application > Multicast > IPv4 Multicast

LABEL	DESCRIPTION
Index	This is the index number of the entry.
VID	This field displays the multicast VLAN ID.
Port	This field displays the port number that belongs to the multicast group.
Multicast Group	This field displays IP multicast group addresses.

24.3.1 IGMP Snooping

Click the IGMP Snooping link in the Advanced Application > Multicast > IPv4 Multicast screen to display the screen as shown. See [Section 24.1 on page 195](#) for more information on multicasting.

Figure 140 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping

IGMP Snooping

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

IGMP Snooping

Active ☐
Querier ☐
Report Proxy ☒
Host Timeout 260
802.1p Priority No-Change ▼

IGMP Filtering

Active ☐
Unknown Multicast Frame ☒ Flooding ☐ Drop
Unknown Multicast Frame to Querier Port ☒ Drop ☐ Forwarding ☐ Forwarding on VLAN
Reserved Multicast Group ☒ Flooding ☐ Drop

Port	Normal Leave	Fast Leave	Group Limited	Max Group Num.	Throttling	IGMP Filtering Profile	IGMP Querier Mode
*	☒	☐	☐		Deny ▼	Default ▼	Auto ▼
1	☒ 4000	☐ 200	☐	0	Deny ▼	Default ▼	Auto ▼
2	☒ 4000	☐ 200	☐	0	Deny ▼	Default ▼	Auto ▼
3	☒ 4000	☐ 200	☐	0	Deny ▼	Default ▼	Auto ▼
4	☒ 4000	☐ 200	☐	0	Deny ▼	Default ▼	Auto ▼
5	☒ 4000	☐ 200	☐	0	Deny ▼	Default ▼	Auto ▼
6	☒ 4000	☐ 200	☐	0	Deny ▼	Default ▼	Auto ▼
7	☒ 4000	☐ 200	☐	0	Deny ▼	Default ▼	Auto ▼
8	☒ 4000	☐ 200	☐	0	Deny ▼	Default ▼	Auto ▼
9	☒ 4000	☐ 200	☐	0	Deny ▼	Default ▼	Auto ▼
10	☒ 4000	☐ 200	☐	0	Deny ▼	Default ▼	Auto ▼
11	☒ 4000	☐ 200	☐	0	Deny ▼	Default ▼	Auto ▼
12	☒ 4000	☐ 200	☐	0	Deny ▼	Default ▼	Auto ▼

Apply

Cancel

The following table describes the labels in this screen.

Table 92 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping

LABEL	DESCRIPTION
IGMP Snooping	Use these settings to configure IGMP snooping.
Active	Select Active to enable IGMP Snooping to forward group multicast traffic only to ports that are members of that group.

Table 92 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping (continued) (continued)

LABEL	DESCRIPTION
Querier	Select this option to allow the Switch to send IGMP General Query messages to the VLANs with the multicast hosts attached.
Report Proxy	Select this option to allow the Switch to act as the IGMP report proxy and leave proxy. It will report group changes to a connected multicast router. The Switch not only checks IGMP packets between multicast routers/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/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/switch. The Switch sends a leave message with its MAC address to the multicast router/switch only when it receives the leave message from the last host in a multicast group.
Host Timeout	Specify the time (from 1 to 16 711 450) in seconds that elapses before the Switch removes an IGMP group membership entry if it does not receive report messages from the port.
802.1p Priority	Select a priority level (0-7) to which the Switch changes the priority in outgoing IGMP control packets. Otherwise, select No-Change to not replace the priority.
IGMP Filtering	Select Active to enable IGMP filtering to control which IGMP groups a subscriber on a port can join. If you enable IGMP filtering, you must create and assign IGMP filtering profiles for the ports that you want to allow to join multicast groups.
Unknown Multicast Frame	Specify the action to perform when the Switch receives an unknown multicast frame. - Select Drop to discard the frame(s). - Select Flooding to send the frame(s) to all ports.
Unknown Multicast Frame to Querier Port	Specify the action to perform when Unknown Multicast Frame is set to Drop. - Select Drop to discard the frame(s). - Select Forwarding to send the frame(s) to all querier ports. - Select Forwarding on VLAN and enter the VLAN ID number(s) to send the frame(s) to the ports which are used as an IGMP query port on the specified VLAN(s). Use a dash to specify consecutive VLANs and a comma (no spaces) to specify non-consecutive VLANs. For example, 51-53 includes 51, 52 and 53, but 51,53 does not include 52.
Reserved Multicast Group	The IP address range of 224.0.0.0 to 224.0.0.255 are reserved for multicasting on the local network only. For example, 224.0.0.1 is for all hosts on a local network segment and 224.0.0.9 is used to send RIP routing information to all RIP v2 routers on the same network segment. A multicast router will not forward a packet with the destination IP address within this range to other networks. See the IANA web site for more information. The layer-2 multicast MAC addresses used by Cisco layer-2 protocols, 01:00:0C:CC:CC:CC and 01:00:0C:CC:CC:CD, are also included in this group. Specify the action to perform when the Switch receives a frame with a reserved multicast address. - Select Drop to discard the frame(s). - Select Flooding to send the frame(s) to all ports.
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. Changes in this row are copied to all the ports as soon as you make them.

Table 92 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping (continued) (continued)

LABEL	DESCRIPTION
Normal Leave	Enter an IGMP normal leave timeout value (from 200 to 6,348,800) in milliseconds. Select this option to have the Switch use this timeout to update the forwarding table for the port. In normal leave mode, when the Switch receives an IGMP leave message from a host on a port, it forwards the message to the multicast router. The multicast router then sends out an IGMP Group-Specific Query (GSQ) message to determine whether other hosts connected to the port should remain in the specific multicast group. The Switch forwards the query message to all hosts connected to the port and waits for IGMP reports from hosts to update the forwarding table. This defines how many seconds the Switch waits for an IGMP report before removing an IGMP snooping membership entry when an IGMP leave message is received on this port from a host.
Fast Leave	Enter an IGMP fast leave timeout value (from 200 to 6,348,800) in milliseconds. Select this option to have the Switch use this timeout to update the forwarding table for the port. In fast leave mode, right after receiving an IGMP leave message from a host on a port, the Switch itself sends out an IGMP Group-Specific Query (GSQ) message to determine whether other hosts connected to the port should remain in the specific multicast group. This helps speed up the leave process. This defines how many seconds the Switch waits for an IGMP report before removing an IGMP snooping membership entry when an IGMP leave message is received on this port from a host.
Group Limited	Select this option to limit the number of multicast groups this port is allowed to join.
Max Group Num.	Enter the number of multicast groups this port is allowed to join. Once a port is registered in the specified number of multicast groups, any new IGMP join report frame(s) is dropped on this port.
Throttling	IGMP throttling controls how the Switch deals with the IGMP reports when the maximum number of the IGMP groups a port can join is reached. Select Deny to drop any new IGMP join report received on this port until an existing multicast forwarding table entry is aged out. Select Replace to replace an existing entry in the multicast forwarding table with the new IGMP report(s) received on this port.
IGMP Filtering Profile	Select the name of the IGMP filtering profile to use for this port. Otherwise, select Default to prohibit the port from joining any multicast group. You can create IGMP filtering profiles in the Multicast > IPv4 Multicast > IGMP Snooping > IGMP Filtering Profile screen.
IGMP Querier Mode	The Switch treats an IGMP query port as being connected to an IGMP multicast router (or server). The Switch forwards IGMP join or leave packets to an IGMP query port. Select Auto to have the Switch use the port as an IGMP query port if the port receives IGMP query packets. Select Fixed to have the Switch always use the port as an IGMP query port. Select this when you connect an IGMP multicast server to the port. Select Edge to stop the Switch from using the port as an IGMP query port. The Switch will not keep any record of an IGMP router being connected to this port. The Switch does not forward IGMP join or leave packets to this port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

24.3.2 IGMP Snooping VLAN

Click **Advanced Application > Multicast > IPv4 Multicast** in the navigation panel. Click the **IGMP Snooping** link and then the **IGMP Snooping VLAN** link to display the screen as shown. See [IGMP Snooping and VLANs on page 196](#) for more information on IGMP Snooping VLAN.

Figure 141 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Snooping VLAN

The screenshot shows the 'IGMP Snooping VLAN' configuration interface. At the top, there's a title bar with 'IGMP Snooping VLAN' and a link to 'IGMP Snooping'. Below the title bar, the 'Mode' is set to 'auto' (selected) with a radio button, and 'fixed' is unselected. There are 'Apply' and 'Cancel' buttons. Below this is a 'VLAN' section with input fields for 'Name' and 'VID', and 'Add', 'Cancel', and 'Clear' buttons. At the bottom, there's a table with columns 'Index', 'Name', and 'VID', and a checkbox. Below the table are 'Delete' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 93 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Snooping VLAN

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

Table 93 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Snooping VLAN

LABEL	DESCRIPTION
Clear	Click Clear to reset the fields to the factory defaults.
Index	This is the index number of the IGMP snooping VLAN entry in the table. Click on an index number to view more details or change the settings.
Name	This field displays the descriptive name for this VLAN group.
VID	This field displays the ID number of the VLAN group.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Check the entry(ies) that you want to remove, then click the Delete button.
Cancel	Click Cancel to clear the check boxes.

24.3.3 IGMP Filtering Profile

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

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

Figure 142 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Filtering Profile

The following table describes the labels in this screen.

Table 94 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Filtering Profile

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

Table 94 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Filtering Profile

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

CHAPTER 25

AAA

25.1 AAA Overview

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

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, and so on. Accounting can also record system related actions such as boot up and shut down times of the Switch.

The external servers that perform authentication, authorization and accounting functions are known as AAA servers. The Switch supports RADIUS (Remote Authentication Dial-In User Service, see [RADIUS on page 204](#)) as the external authentication and authorization server.

Figure 143 AAA Server



25.1.1 What You Can Do

- Use the AAA screen ([Section 25.2 on page 204](#)) to display the links to the screens where you can enable authentication and authorization or both of them on the Switch.
- use the RADIUS Server Setup screen ([Section 25.3 on page 204](#)) to configure your RADIUS server settings.
- Use the AAA Setup screen ([Section 25.4 on page 206](#)) to configure authentication, authorization and accounting settings, such as the methods used to authenticate users accessing the Switch and which database the Switch should use first.

25.1.2 What You Need to Know

Local User Accounts

By storing user profiles locally on the Switch, your Switch is able to authenticate and authorize users without interacting with a network AAA server. However, there is a limit on the number of users you may authenticate in this way (See [Section 36.4 on page 299](#)).

RADIUS

RADIUS is a security protocol 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 authentication allows you to validate an unlimited number of users from a central location.

The following table describes some key features of RADIUS

Table 95 RADIUS

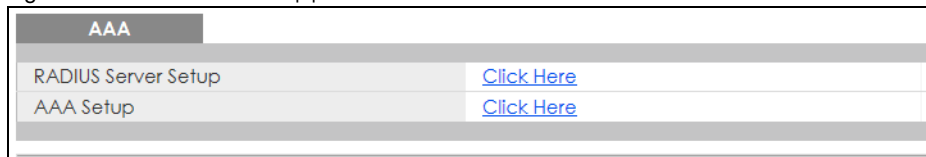
	RADIUS
Transport Protocol	UDP (User Datagram Protocol)
Encryption	Encrypts the password sent for authentication.

25.2 AAA Screens

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

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

Figure 144 Advanced Application > AAA



25.3 RADIUS Server Setup

Use this screen to configure your RADIUS server settings. See [RADIUS on page 204](#) for more information on RADIUS servers and [Section 25.5.2 on page 209](#) for RADIUS attributes utilized by the authentication features on the Switch. Click on the **RADIUS Server Setup** link in the **AAA** screen to view the screen as shown.

Figure 145 Advanced Application > AAA > RADIUS Server Setup

RADIUS Server Setup

[AAA](#)

Authentication Server

Mode

index-priority ▼

Timeout

30

seconds

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

Accounting Server

Timeout

30

seconds

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

Apply

Cancel

The following table describes the labels in this screen.

Table 96 Advanced Application > AAA > RADIUS Server Setup

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

Table 96 Advanced Application > AAA > RADIUS Server Setup (continued)

LABEL	DESCRIPTION
Timeout	Specify the amount of time in seconds that the Switch waits for an accounting request response from the RADIUS accounting server.
Index	This is a read-only number representing a RADIUS accounting server entry.
IP Address	Enter the IP address of an external RADIUS accounting server in dotted decimal notation.
UDP Port	The default port of a RADIUS accounting server for accounting is 1813. You need not change this value unless your network administrator instructs you to do so.
Shared Secret	Specify a password (up to 32 alphanumeric characters) as the key to be shared between the external RADIUS accounting server and the Switch. This key is not sent over the network. This key must be the same on the external RADIUS accounting server and the Switch.
Delete	Check this box if you want to remove an existing RADIUS accounting server entry from the Switch. This entry is deleted when you click Apply .
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

25.4 AAA Setup

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

Figure 146 Advanced Application > AAA > AAA Setup

AAA Setup

AAA

Authentication

Type	Method 1	Method 2
Login	local ▼	- ▼

Authorization

Type	Active	Method
Exec	☐	radius
Dot1x	☐	radius

Accounting

Update Period minutes

Type	Active	Broadcast	Mode	Method
System	☐	☐	-	radius
Dot1x	☐	☐	start-stop ▼	radius

Apply

Cancel

The following table describes the labels in this screen.

Table 97 Advanced Application > AAA > AAA Setup

LABEL	DESCRIPTION
Authentication	Use this section to specify the methods used to authenticate users accessing the Switch.
Login	These fields specify which database the Switch should use (first, second and third) to authenticate administrator accounts (users for Switch management). Configure the local user accounts in the Access Control > Logins screen. The RADIUS is a external server. 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, and finally Method 2). 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 the Method 2 field. Select local to have the Switch check the administrator accounts configured in the Access Control > Logins screen. Select radius to have the Switch check the administrator accounts configured via your RADIUS server.
Authorization	Use this section to configure authorization settings on the Switch.
Type	Set whether the Switch provides the following services to a user. Exec: Allow an administrator which logs into the Switch through Telnet or SSH to have a different access privilege level assigned via the external server. Dot1x: Allow an IEEE 802.1x client to have different bandwidth limit or VLAN ID assigned via the external server.
Active	Select this to activate authorization for a specified event types.
Method	This field displays the authorization protocol used for the corresponding event type.
Accounting	Use this section to configure accounting settings on the Switch.
Update Period	This is the amount of time in minutes before the Switch sends an update to the accounting server. This is only valid if you select the start-stop option for the Exec or Dot1x entries.
Type	The Switch supports the following types of events to be sent to the accounting server(s): System - Configure the Switch to send information when the following system events occur: system boots up, system shuts down, system accounting is enabled, system accounting is disabled Dot1x - Configure the Switch to send information when an IEEE 802.1x client begins a session (authenticates via the Switch), ends a session as well as interim updates of a session.
Active	Select this to activate accounting for a specified event types.
Broadcast	Select this to have the Switch send accounting information to all configured accounting servers at the same time. If you don't select this and you have two accounting servers set up, then the Switch sends information to the first accounting server and if it doesn't get a response from the accounting server then it tries the second accounting server.
Mode	The Switch supports two modes of recording login events. Select: start-stop - to have the Switch send information to the accounting server when a user begins a session, during a user's session (if it lasts past the Update Period), and when a user ends a session. stop-only - to have the Switch send information to the accounting server only when a user ends a session.
Method	This field displays the accounting protocol used for the corresponding event type.

Table 97 Advanced Application > AAA > AAA Setup (continued)

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

25.5 Technical Reference

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

25.5.1 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 via the RADIUS server.

The following table describes the VSAs supported on the Switch.

Table 98 Supported VSAs

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

Table 98 Supported VSAs

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

25.5.1.1 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 the bolded values in the table are fixed values as defined in RFC 3580.

Table 99 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.

25.5.2 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 appendix lists the RADIUS attributes supported by the Switch.

Refer to RFC 2865 for more information about RADIUS attributes used for authentication.

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

25.5.3 Attributes Used for Authentication

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

25.5.3.1 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

25.5.3.2 Attributes Used to Login Users

User-Name

User-Password

NAS-Identifier

NAS-IP-Address

25.5.3.3 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

CHAPTER 26

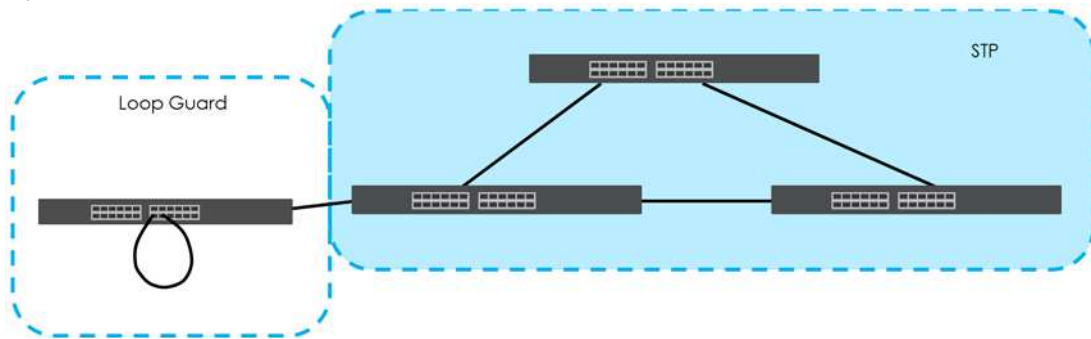
Loop Guard

26.1 Loop Guard Overview

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

Loop guard allows you to configure the Switch to shut down a port if it detects that packets sent out on that port loop back to the Switch. While you can use Spanning Tree Protocol (STP) to prevent loops in the core of your network, STP cannot prevent loops that occur on the edge of your network.

Figure 147 Loop Guard vs. STP



Refer to [Section 26.1.2 on page 211](#) for more information.

26.1.1 What You Can Do

Use the Loop Guard screen ([Section 26.2 on page 213](#)) to enable loop guard on the Switch and in specific ports.

26.1.2 What You Need to Know

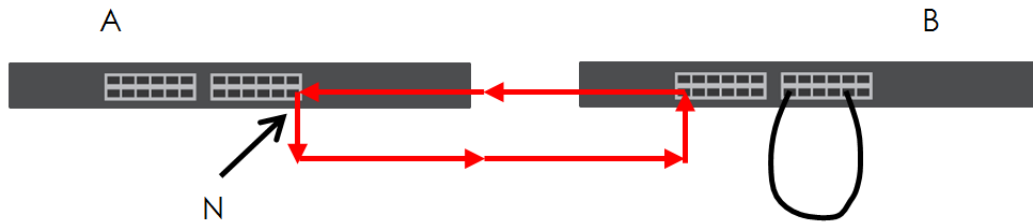
Loop guard is designed to handle loop problems on the edge of your network. This can occur when a port is connected to a Switch that is in a loop state. Loop state occurs as a result of human error. It happens when two ports on a switch are connected with the same cable. When a switch in loop state sends 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:

- It will receive broadcast messages sent out from the switch in loop state.
- It will receive its own broadcast messages that it sends out as they loop back. It will then re-broadcast those messages again.

The following figure shows port N on switch A connected to switch B. Switch B is in loop state. When broadcast or multicast packets leave port N and reach switch B, they are sent back to port N on A as they are rebroadcast from B.

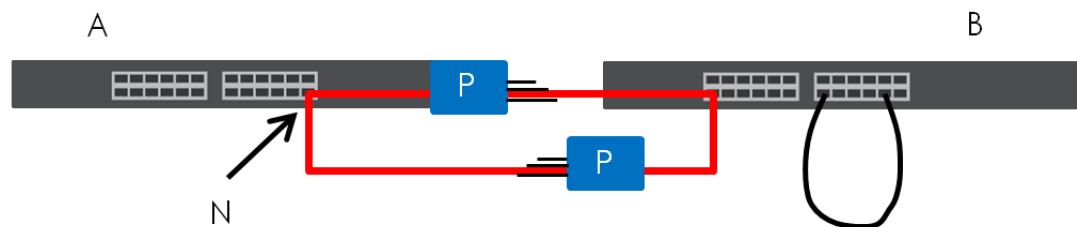
Figure 148 Switch in Loop State



The loop guard feature checks to see if a loop guard enabled port is connected to a switch in loop state. This is accomplished by periodically sending a probe packet and seeing if the packet returns on the same port. If this is the case, the Switch will shut down the port connected to the switch in loop state.

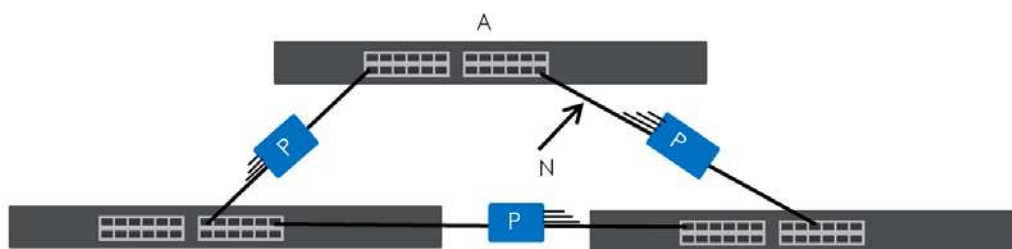
The following figure shows a loop guard enabled port N on switch A sending a probe packet P to switch B. Since switch B is in loop state, the probe packet P returns to port N on A. The Switch then shuts down port N to ensure that the rest of the network is not affected by the switch in loop state.

Figure 149 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 150 Loop Guard - Network Loop



Note: After resolving the loop problem on your network you can re-activate the disabled port via the web configurator (see [Section 8.7 on page 89](#)).

26.2 Loop Guard Setup

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

Note: The loop guard feature can not be enabled on the ports that have Spanning Tree Protocol (RSTP or MSTP) enabled.

Figure 151 Advanced Application > Loop Guard

Loop Guard	
Active	☐
Port	Active
*	☐
1	☐
2	☐
3	☐
4	☐
5	☐
6	☐
7	☐
8	☐
9	☐
10	☐
11	☐
12	☐
Apply Cancel	

The following table describes the labels in this screen.

Table 100 Advanced Application > Loop Guard

LABEL	DESCRIPTION
Active	Select this option to enable loop guard on the Switch. The Switch generates syslog, internal log messages as well as SNMP traps when it shuts down a port via the loop guard feature.
Port	This field displays the port number. * means all ports.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable the loop guard feature on this port. The Switch sends probe packets from this port to check if the switch it is connected to is in loop state. If the switch that this port is connected is in loop state the Switch will shut down this port. Clear this check box to disable the loop guard feature.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 27

Layer 2 Protocol Tunneling

27.1 Layer 2 Protocol Tunneling Overview

This chapter shows you how to configure layer 2 protocol tunneling on the Switch.

27.1.1 What You Can Do

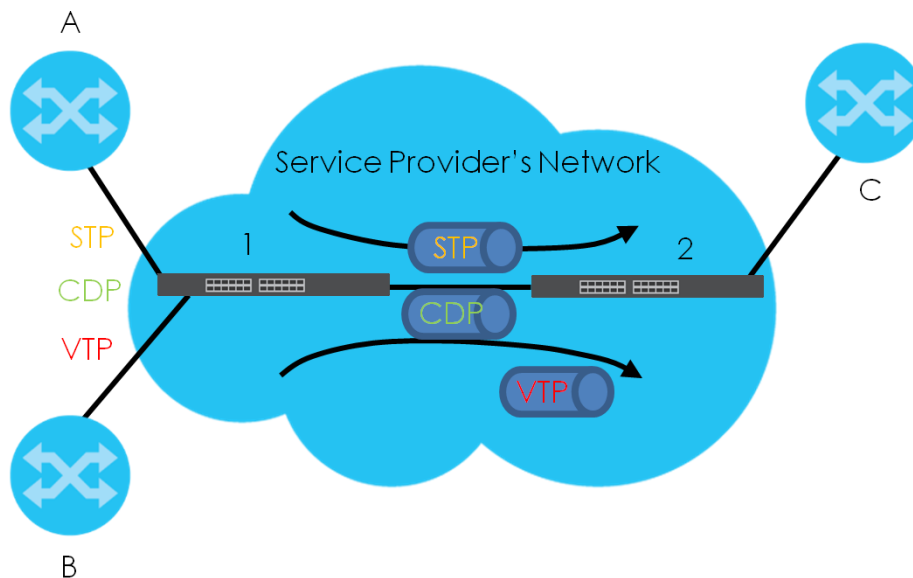
Use the Layer 2 Protocol Tunnel screen ([Section 27.2 on page 215](#)) to enable layer 2 protocol tunneling on the Switch and specify a MAC address with which the Switch uses to encapsulate the layer 2 protocol packets by replacing the destination MAC address in the packets.

27.1.2 What You Need to Know

Layer 2 protocol tunneling (L2PT) is used on the service provider's edge devices.

L2PT allows edge switches (1 and 2 in the following figure) to tunnel layer 2 STP (Spanning Tree Protocol), CDP (Cisco Discovery Protocol) and VTP (VLAN Trunking Protocol) packets between customer switches (A, B and C in the following figure) connected through the service provider's network. The edge switch encapsulates layer 2 protocol packets with a specific MAC address before sending them across the service provider's network to other edge switches.

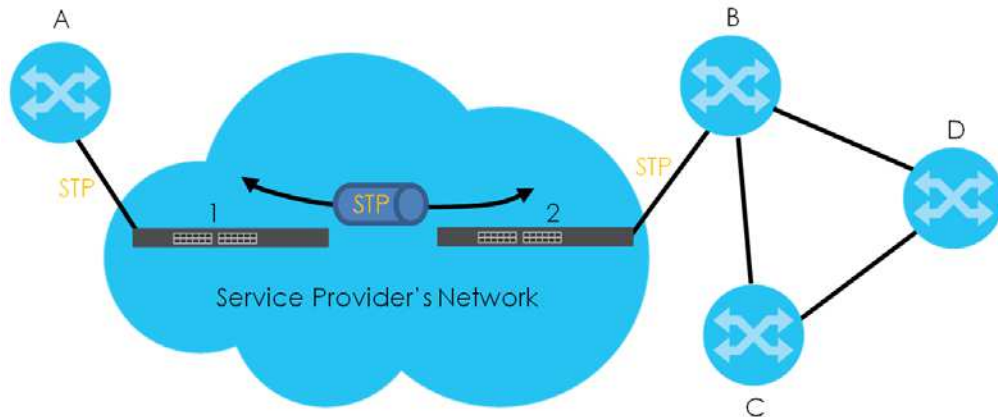
Figure 152 Layer 2 Protocol Tunneling Network Scenario



In the following example, if you enable L2PT for STP, you can have switches A, B, C and D in the same spanning tree, even though switch A is not directly connected to switches B, C and D. Topology change information can be propagated throughout the service provider's network.

To emulate a point-to-point topology between two customer switches at different sites, such as A and B, you can enable protocol tunneling on edge switches 1 and 2 for PAgP (Port Aggregation Protocol), LACP or UDLD (UniDirectional Link Detection).

Figure 153 L2PT Network Example



27.1.2.1 Layer 2 Protocol Tunneling Mode

Each port can have two layer 2 protocol tunneling modes, Access and Tunnel.

- The **Access** port is an ingress port on the service provider's edge device (1 or 2 in [Figure 153 on page 215](#)) and connected to a customer switch (A or B). Incoming layer 2 protocol packets received on an access port are encapsulated and forwarded to the tunnel ports.
- The **Tunnel** port is an egress port at the edge of the service provider's network and connected to another service provider's switch. Incoming encapsulated layer 2 protocol packets received on a tunnel port are decapsulated and sent to an access port.

27.2 Configuring Layer 2 Protocol Tunneling

Click **Advanced Application > Layer 2 Protocol Tunneling** in the navigation panel to display the screen as shown.

Figure 154 Advanced Application > Layer 2 Protocol Tunneling

Layer 2 Protocol Tunnel							
Active	☐						
Destination MAC Address	00:00:00:00:00:00						
Port	CDP	STP	VTP	Point to Point			Mode
				PAGP	LACP	UDLD	
*	☐	☐	☐	☐	☐	☐	Access ▼
1	☐	☐	☐	☐	☐	☐	Access ▼
2	☐	☐	☐	☐	☐	☐	Access ▼
3	☐	☐	☐	☐	☐	☐	Access ▼
4	☐	☐	☐	☐	☐	☐	Access ▼
5	☐	☐	☐	☐	☐	☐	Access ▼
6	☐	☐	☐	☐	☐	☐	Access ▼
7	☐	☐	☐	☐	☐	☐	Access ▼
8	☐	☐	☐	☐	☐	☐	Access ▼
9	☐	☐	☐	☐	☐	☐	Access ▼
10	☐	☐	☐	☐	☐	☐	Access ▼
11	☐	☐	☐	☐	☐	☐	Access ▼
12	☐	☐	☐	☐	☐	☐	Access ▼
Apply Cancel							

The following table describes the labels in this screen.

Table 101 Advanced Application > Layer 2 Protocol Tunneling

LABEL	DESCRIPTION
Active	Select this to enable layer 2 protocol tunneling on the Switch.
Destination MAC Address	Specify a MAC address with which the Switch uses to encapsulate the layer 2 protocol packets by replacing the destination MAC address in the packets. Note: The MAC address can be either a unicast MAC address or multicast MAC address. If you use a unicast MAC address, make sure the MAC address does not exist in the address table of a switch on the service provider's network. Note: All the edge switches in the service provider's network should be set to use the same MAC address for encapsulation.
Port	This field displays the port number. * means all ports.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them.
CDP	Select this option to have the Switch tunnel CDP (Cisco Discovery Protocol) packets so that other Cisco devices can be discovered through the service provider's network.
STP	Select this option to have the Switch tunnel STP (Spanning Tree Protocol) packets so that STP can run properly across the service provider's network and spanning trees can be set up based on bridge information from all (local and remote) networks.
VTP	Select this option to have the Switch tunnel VTP (VLAN Trunking Protocol) packets so that all customer switches can use consistent VLAN configuration through the service provider's network.

Table 101 Advanced Application > Layer 2 Protocol Tunneling (continued)

LABEL	DESCRIPTION
Point to Point	The Switch supports PAGP (Port Aggregation Protocol), LACP (Link Aggregation Control Protocol) and UDLD (UniDirectional Link Detection) tunneling for a point-to-point topology. Both PAGP and UDLD are Cisco's proprietary data link layer protocols. PAGP is similar to LACP and used to set up a logical aggregation of Ethernet ports automatically. UDLD is to determine the link's physical status and detect a unidirectional link.
PAGP	Select this option to have the Switch send PAGP packets to a peer to automatically negotiate and build a logical port aggregation.
LACP	Select this option to have the Switch send LACP packets to a peer to dynamically creates and manages trunk groups.
UDLD	Select this option to have the Switch send UDLD packets to a peer's port it connected to monitor the physical status of a link.
Mode	Select Access to have the Switch encapsulate the incoming layer 2 protocol packets and forward them to the tunnel port(s). Select Access for ingress ports at the edge of the service provider's network. Note: You can enable L2PT services for STP, LACP, VTP, CDP, UDLD, and PAGP on the access port(s) only. Select Tunnel for egress ports at the edge of the service provider's network. The Switch decapsulates the encapsulated layer 2 protocol packets received on a tunnel port by changing the destination MAC address to the original one, and then forward them to an access port. If the service(s) is not enabled on an access port, the protocol packets are dropped.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

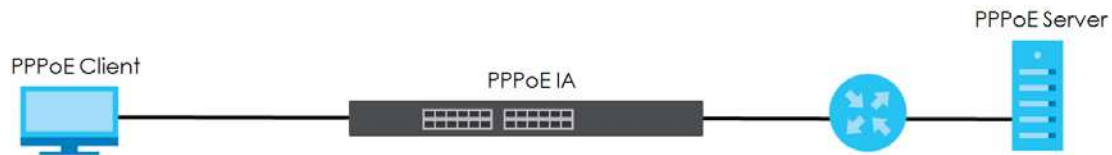
CHAPTER 28

PPPoE

28.1 PPPoE Intermediate Agent Overview

This chapter describes how the Switch gives a PPPoE termination server additional information that the server can use to identify and authenticate a PPPoE client.

A PPPoE Intermediate Agent (PPPoE IA) is deployed between a PPPoE server and PPPoE clients. It helps the PPPoE server identify and authenticate clients by adding subscriber line specific information to PPPoE discovery packets from clients on a per-port or per-port-per-VLAN basis before forwarding them to the PPPoE server.



28.1.1 What You Can Do

- Use the **PPPoE** screen ([Section 28.2 on page 220](#)) to display the main PPPoE screen.
- Use the **Intermediate Agent** screen ([Section 28.3 on page 221](#)) to enable the PPPoE Intermediate Agent on the Switch.
- Use the **PPPoE IA Per-Port** screen ([Section 28.3.1 on page 222](#)) to set the port state and configure PPPoE intermediate agent sub-options on a per-port basis.
- Use the **PPPoE IA Per-Port Per-VLAN** screen ([Section 28.3.2 on page 223](#)) to configure PPPoE IA settings that apply to a specific VLAN on a port.
- Use the **PPPoE IA for VLAN** ([Section 28.3.3 on page 224](#)) to enable the PPPoE Intermediate Agent on a VLAN.

28.1.2 What You Need to Know

Read on for concepts on ARP that can help you configure the screen in this chapter.

28.1.2.1 PPPoE Intermediate Agent Tag Format

If the PPPoE Intermediate Agent is enabled, the Switch adds a vendor-specific tag to PADI (PPPoE Active Discovery Initialization) and PADR (PPPoE Active Discovery Request) packets from PPPoE clients. This tag is defined in RFC 2516 and has the following format for this feature.

Table 102 PPPoE Intermediate Agent Vendor-specific Tag Format

Tag_Type (0x0105)	Tag_Len	Value	i1	i2

The Tag_Type is 0x0105 for vendor-specific tags, as defined in RFC 2516. The Tag_Len indicates the length of Value, i1 and i2. The Value is the 32-bit number 0x00000DE9, which stands for the "ADSL Forum" IANA entry. i1 and i2 are PPPoE intermediate agent sub-options, which contain additional information about the PPPoE client.

28.1.2.2 Sub-Option Format

There are two types of sub-option: "Agent Circuit ID Sub-option" and "Agent Remote ID Sub-option". They have the following formats.

Table 103 PPPoE IA Circuit ID Sub-option Format: User-defined String

SubOpt	Length	Value
0x01 (1 byte)	N (1 byte)	String (63 bytes)

Table 104 PPPoE IA Remote ID Sub-option Format

SubOpt	Length	Value
0x02 (1 byte)	N (1 byte)	MAC Address or String (63 bytes)

The 1 in the first field identifies this as an Agent Circuit ID sub-option and 2 identifies this as an Agent Remote ID sub-option. The next field specifies the length of the field. The Switch takes the Circuit ID string you manually configure for a VLAN on a port as the highest priority and the Circuit ID string for a port as the second priority. In addition, the Switch puts the PPPoE client's MAC address into the Agent Remote ID Sub-option if you do not specify any user-defined string.

Flexible Circuit ID Syntax with Identifier String and Variables

If you do not configure a Circuit ID string for a VLAN on a specific port or for a specific port, the Switch adds the user-defined identifier string and variables into the Agent Circuit ID Sub-option. The variables can be the slot ID of the PPPoE client, the port number of the PPPoE client and/or the VLAN ID on the PPPoE packet.

The identifier-string, slot ID, port number and VLAN ID are separated from each other by a pound key (#), semi-colon (;), period (.), comma (,), forward slash (/) or space. An Agent Circuit ID Sub-option example is "Switch/07/0123" and indicates the PPPoE packets come from a PPPoE client which is connected to the Switch's port 7 and belong to VLAN 123.

Table 105 PPPoE IA Circuit ID Sub-option Format: Using Identifier String and Variables

SubOpt	Length	Value						
0x01 (1 byte)	N (1 byte)	Identifier String (53 bytes)	delimiter (1 byte)	Slot ID (1 byte)	delimiter (1 byte)	Port No (2 bytes)	delimiter (1 byte)	VLAN ID (4 bytes)

WT-101 Default Circuit ID Syntax

If you do not configure a Circuit ID string for a specific VLAN on a port or for a specific port, and disable the flexible Circuit ID syntax in the **PPPoE > Intermediate Agent** screen, the Switch automatically generates a Circuit ID string according to the default Circuit ID syntax which is defined in the DSL Forum

Working Text (WT)-101. The default access node identifier is the host name of the PPPoE intermediate agent and the eth indicates "Ethernet".

Table 106 PPPoE IA Circuit ID Sub-option Format: Defined in WT-101

SubOpt	Length	Value								
0x01 (1 byte)	N (1 byte)	Access Node Identifier (20 byte)	Space (1 byte)	eth (3 byte)	Space (1 byte)	Slot ID (1 byte)	/ (1 byte)	Port No (2 byte)	: (1 byte)	VLAN ID (4 bytes)

28.1.2.3 Port State

Every port is either a trusted port or an untrusted port for the PPPoE intermediate agent. This setting is independent of the trusted/untrusted setting for DHCP snooping or ARP inspection. You can also specify the agent sub-options (circuit ID and remote ID) that the Switch adds to PADI and PADR packets from PPPoE clients.

Trusted ports are connected to PPPoE servers.

- If a PADO (PPPoE Active Discovery Offer), PADS (PPPoE Active Discovery Session-confirmation), or PADT (PPPoE Active Discovery Terminate) packet is sent from a PPPoE server and received on a trusted port, the Switch forwards it to all other ports.
- If a PADI or PADR packet is sent from a PPPoE client but received on a trusted port, the Switch forwards it to other trusted port(s).

Note: The Switch will drop all PPPoE discovery packets if you enable the PPPoE intermediate agent and there are no trusted ports.

Untrusted ports are connected to subscribers.

- If a PADI, PADR, or PADT packet is sent from a PPPoE client and received on an untrusted port, the Switch adds a vendor-specific tag to the packet and then forwards it to the trusted port(s).
- The Switch discards PADO and PADS packets which are sent from a PPPoE server but received on an untrusted port.

28.2 PPPoE Screen

Use this screen to configure the PPPoE Intermediate Agent on the Switch.

Click **Advanced Application > PPPoE** in the navigation panel to display the screen as shown. Click [Click Here](#) to go to the Intermediate Agent screen.

Figure 155 Advanced Application > PPPoE Intermediate Agent



28.3 PPPoE Intermediate Agent

Use this screen to configure the Switch to give a PPPoE termination server additional subscriber information that the server can use to identify and authenticate a PPPoE client.

Click **Advanced Application > PPPoE > Intermediate Agent** in the navigation panel to display the screen as shown.

Figure 156 Advanced Application > PPPoE > Intermediate Agent

The following table describes the labels in this screen.

Table 107 Advanced Application > PPPoE > Intermediate Agent

LABEL	DESCRIPTION
Active	Select this option to enable the PPPoE intermediate agent globally on the Switch.
access-node-identifier	Enter up to 20 ASCII characters to identify the PPPoE intermediate agent. Hyphens (-) and spaces are also allowed. The default is the Switch's host name.
circuit-id	Use this section to configure the Circuit ID field in the PADI and PADR packets. The Circuit ID you configure for a specific port or for a specific VLAN on a port has priority over this. The Circuit ID you configure for a specific port (in the Advanced Application > PPPoE > Intermediate Agent > Port screen) or for a specific VLAN on a port (in the Advanced Application > PPPoE > Intermediate Agent > Port > VLAN screen) has priority over this. That means, if you also want to configure PPPoE IA Per-Port or Per-Port Per-VLAN setting, leave the fields here empty and configure circuit-id and remote-id in the Per-Port or Per-Port Per-VLAN screen.
Active	Select this option to have the Switch add the user-defined identifier string and variables (specified in the option field) to PADI or PADR packets from PPPoE clients. If you leave this option unselected and do not configure any Circuit ID string on the Switch, the Switch will use the string specified in the access-node-identifier field.
identifier-string	Specify a string that the Switch adds in the Agent Circuit ID sub-option. You can enter up to 53 ASCII characters. Spaces are allowed.
option	Select the variables that you want the Switch to generate and add in the Agent Circuit ID sub-option. The variable options include sp , sv , pv and spv which indicate combinations of slot-port, slot-VLAN, port-VLAN and slot-port-VLAN respectively. The Switch enters a zero into the PADI and PADR packets for the slot value.
delimiter	Select a delimiter to separate the identifier-string, slot ID, port number and/or VLAN ID from each other. You can use a pound key (#), semi-colon (;), period (.), comma (,), forward slash (/) or space.

Table 107 Advanced Application > PPPoE > Intermediate Agent (continued)

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

28.3.1 PPPoE IA Per-Port

Use this screen to specify whether individual ports are trusted or untrusted ports and have the Switch add extra information to PPPoE discovery packets from PPPoE clients on a per-port basis.

Note: The Switch will drop all PPPoE packets if you enable the PPPoE Intermediate Agent on the Switch and there are no trusted ports.

Click the **Port** link in the **Intermediate Agent** screen to display the screen as shown.

Figure 157 Advanced Application > PPPoE > Intermediate Agent > Port

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

The following table describes the labels in this screen.

Table 108 Advanced Application > PPPoE > Intermediate Agent > Port

LABEL	DESCRIPTION
Port	This field displays the port number. * means all ports.
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.

Table 108 Advanced Application > PPPoE > Intermediate Agent > Port (continued)

LABEL	DESCRIPTION
Server Trusted State	Select whether this port is a trusted port (Trusted) or an untrusted port (Untrusted). Trusted ports are uplink ports connected to PPPoE servers. If a PADO (PPPoE Active Discovery Offer), PADS (PPPoE Active Discovery Session-confirmation), or PADT (PPPoE Active Discovery Terminate) packet is sent from a PPPoE server and received on a trusted port, the Switch forwards it to all other ports. If a PADI or PADR packet is sent from a PPPoE client but received on a trusted port, the Switch forwards it to other trusted port(s). Untrusted ports are downlink ports connected to subscribers. If a PADI, PADR, or PADT packet is sent from a PPPoE client and received on an untrusted port, the Switch adds a vendor-specific tag to the packet and then forwards it to the trusted port(s). The Switch discards PADO and PADS packets which are sent from a PPPoE server but received on an untrusted port.
Circuit-id	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Circuit ID sub-option for PPPoE discovery packets received on this port. Spaces are allowed. The Circuit ID you configure for a specific VLAN on a port (in the Advanced Application > PPPoE > Intermediate Agent > Port > VLAN screen) has the highest priority.
Remote-id	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Remote ID sub-option for PPPoE discovery packets received on this port. Spaces are allowed. If you do not specify a string here or in the Remote-id field for a VLAN on a port, the Switch automatically uses the PPPoE client's MAC address. The Remote ID you configure for a specific VLAN on a port (in the Advanced Application > PPPoE > Intermediate Agent > Port > VLAN screen) has the highest priority.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

28.3.2 PPPoE IA Per-Port Per-VLAN

Use this screen to configure PPPoE IA settings that apply to a specific VLAN on a port.

Click the **VLAN** link in the **Intermediate Agent > Port** screen to display the screen as shown.

Figure 158 Advanced Application > PPPoE > Intermediate Agent > Port > VLAN

The screenshot displays the configuration interface for PPPoE IA settings per port and VLAN. The top section includes a 'VLAN' tab and a 'Port' dropdown menu currently set to '0'. Below these are input fields for 'Start VID' and 'End VID'. An 'Apply' button is located below the VID fields. The bottom section features a table with three columns: 'VID', 'Circuit-id', and 'Remote-id'. The 'VID' column contains an asterisk (*). At the bottom right of the table, there are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 109 Advanced Application > PPPoE > Intermediate Agent > Port > VLAN

LABEL	DESCRIPTION
Show Port	Enter a port number to show the PPPoE Intermediate Agent settings for the specified VLAN(s) on the port.
Show VLAN	Use this section to specify the VLANs you want to configure in the section below.
Start VID	Enter the lowest VLAN ID you want to configure in the section below.
End VID	Enter the highest VLAN ID you want to configure in the section below.
Apply	Click Apply to display the specified range of VLANs in the section below.
Port	This field displays the port number specified above.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the * VLAN, the settings are applied to all VLANs.
*	Use this row to make the setting the same for all VLANs. Use this row first and then make adjustments on a VLAN-by-VLAN basis. Changes in this row are copied to all the VLANs as soon as you make them.
Circuit-id	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Circuit ID sub-option for this VLAN on the specified port. Spaces are allowed. The Circuit ID you configure here has the highest priority.
Remote-id	Enter a string of up to 63 ASCII characters that the Switch adds into the Agent Remote ID sub-option for this VLAN on the specified port. Spaces are allowed. If you do not specify a string here or in the Remote-id field for a specific port, the Switch automatically uses the PPPoE client's MAC address. The Remote ID you configure here has the highest priority.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

28.3.3 PPPoE IA for VLAN

Use this screen to set whether the PPPoE Intermediate Agent is enabled on a VLAN and whether the Switch appends the Circuit ID and/or Remote ID to PPPoE discovery packets from a specific VLAN.

Click the **VLAN** link in the **Intermediate Agent** screen to display the screen as shown.

Figure 159 Advanced Application > PPPoE > Intermediate Agent > VLAN

The screenshot shows the 'VLAN' configuration interface. At the top, there's a 'VLAN' tab and a link to 'Intermediate Agent'. Below the tab is a 'Show VLAN' section with 'Start VID' and 'End VID' input fields and an 'Apply' button. Underneath is a table with the following structure:

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

At the bottom of the screen are 'Apply' and 'Cancel' buttons.

The following table describes the labels in this screen.

Table 110 Advanced Application > PPPoE > Intermediate Agent > VLAN

LABEL	DESCRIPTION
Show VLAN	Use this section to specify the VLANs you want to configure in the section below.
Start VID	Enter the lowest VLAN ID you want to configure in the section below.
End VID	Enter the highest VLAN ID you want to configure in the section below.
Apply	Click Apply to display the specified range of VLANs in the section below.
VID	This field displays the VLAN ID of each VLAN in the range specified above. If you configure the * VLAN, the settings are applied to all VLANs.
*	Use this row to make the setting the same for all VLANs. Use this row first and then make adjustments on a VLAN-by-VLAN basis. Changes in this row are copied to all the VLANs as soon as you make them.
Enabled	Select this option to turn on the PPPoE Intermediate Agent on a VLAN.
Circuit-id	Select this option to make the Circuit ID settings for a specific VLAN take effect.
Remote-id	Select this option to make the Remote ID settings for a specific VLAN take effect.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 29

Error Disable

29.1 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.

29.1.1 CPU Protection Overview

Switches exchange protocol control packets in a network to get the latest networking information. If a switch receives large numbers of control packets, such as ARP, BPDU or IGMP packets, which are to be processed by the CPU, the CPU may become overloaded and be unable to handle regular tasks properly.

The CPU protection feature allows you to limit the rate of ARP, BPDU and IGMP packets to be delivered to the CPU on a port. This enhances the CPU efficiency and protects against potential DoS attacks or errors from other network(s). You then can choose to drop control packets that exceed the specified rate limit or disable a port on which the packets are received.

29.1.2 Error-Disable Recovery Overview

Some features, such as loop guard or CPU protection, allow the Switch to shut down a port or discard specific packets on a port when an error is detected on the port. For example, if the Switch detects that packets sent out the port(s) loop back to the Switch, the Switch can shut down the port(s) automatically. After that, you need to enable the port(s) or allow the packets on a port manually via the web configurator. With error-disable recovery, you can set the disabled port(s) to become active or start receiving the packets again after the time interval you specify.

29.1.3 What You Can Do

- Use the **Error Disable Status** screen ([Section 29.3 on page 227](#)) 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 29.4 on page 229](#)) 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 **Error Disable Detect** screen ([Section 29.5 on page 230](#)) 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 **Error Disable Recovery** screen ([Section 29.6 on page 231](#)) to set the Switch to automatically undo an action after the error is gone.

29.2 Error Disable Screen

Use this screen to go to the screens where you can configure error disable related settings. Click **Advanced Application > Errdisable** in the navigation panel to open the following screen.

Figure 160 Advanced Application > Errdisable

Errdisable	
Errdisable Status	Click here
CPU protection	Click here
Errdisable Detect	Click here
Errdisable Recovery	Click here

The following table describes the labels in this screen.

Table 111 Advanced Application > Errdisable

LABEL	DESCRIPTION
Errdisable Status	Click this link to view whether the Switch detected that control packets exceeded the rate limit configured for a port or a port is disabled according to the feature requirements and what action you configure, and related information.
CPU protection	Click this link to limit the maximum number of control packets (ARP, BPDU and/or IGMP) that the Switch can receive or transmit on a port.
Errdisable Detect	Click this link to have the Switch detect whether the control packets exceed the rate limit configured for a port and configure the action to take once the limit is exceeded.
Errdisable Recovery	Click this link to set the Switch to automatically undo an action after the error is gone.

29.3 Error-Disable Status

Use this screen to view whether the Switch detected that control packets exceeded the rate limit configured for a port or a port is disabled according to the feature requirements and what action you configure, and related information. Click the **Click here** link next to **Errdisable Status** in the **Advanced Application > Errdisable** screen to display the screen as shown.

Figure 161 Advanced Application > Errdisable > Errdisable Status

Errdisable Status

Errdisable

Inactive-reason mode reset

Port List

Cause

ARP

Reset

Errdisable Status

Port	Cause	Active	Mode	Rate	Status	Recovery Time Left (secs)	Total Dropped
1	Loop Guard	NO	inactive-port	-	Forwarding	-	-
	ARP	NO	inactive-port	0	Forwarding	-	-
	BPDU	NO	inactive-port	0	Forwarding	-	-
	IGMP	NO	inactive-port	0	Forwarding	-	-
2	Loop Guard	NO	inactive-port	-	Forwarding	-	-
	ARP	NO	inactive-port	0	Forwarding	-	-
	BPDU	NO	inactive-port	0	Forwarding	-	-
	IGMP	NO	inactive-port	0	Forwarding	-	-
3	Loop Guard	NO	inactive-port	-	Forwarding	-	-
	ARP	NO	inactive-port	0	Forwarding	-	-
	BPDU	NO	inactive-port	0	Forwarding	-	-
	IGMP	NO	inactive-port	0	Forwarding	-	-
4	Loop Guard	NO	inactive-port	-	Forwarding	-	-
	ARP	NO	inactive-port	0	Forwarding	-	-
	BPDU	NO	inactive-port	0	Forwarding	-	-
	IGMP	NO	inactive-port	0	Forwarding	-	-
5	Loop Guard	NO	inactive-port	-	Forwarding	-	-
	ARP	NO	inactive-port	0	Forwarding	-	-
	BPDU	NO	inactive-port	0	Forwarding	-	-
	IGMP	NO	inactive-port	0	Forwarding	-	-
	Loop Guard	NO	inactive-port	-	Forwarding	-	-
	ARP	NO	inactive-port	0	Forwarding	-	-
	BPDU	NO	inactive-port	0	Forwarding	-	-
	IGMP	NO	inactive-port	0	Forwarding	-	-

The following table describes the labels in this screen.

Table 112 Advanced Application > Errdisable > Errdisable Status

LABEL	DESCRIPTION
Inactive-reason mode reset	
Port List	Enter the number of the port(s) (separated by a comma) on which you want to reset inactive-reason status.
Cause	Select the cause of inactive-reason mode you want to reset here.
Reset	Press to reset the specified port(s) to handle ARP, BPDU or IGMP packets instead of ignoring them, if the port(s) is in inactive-reason mode.
Errdisable Status	
Port	This is the number of the port on which you want to configure Errdisable Status.
Cause	This displays the type of the control packet received on the port or the feature enabled on the port and causing the Switch to take the specified action.
Active	This field displays whether the control packets (ARP, BPDU, and/or IGMP) on the port is being detected or not. It also shows whether loop guard is enabled on the port.

Table 112 Advanced Application > Errdisable > Errdisable Status (continued)

LABEL	DESCRIPTION
Mode	This field shows the action that the Switch takes for the cause. inactive-port - The Switch disables the port. inactive-reason - The Switch drops all the specified control packets (such as BPDU) on the port. rate-limitation - The Switch drops the additional control packets the port(s) has to handle in every one second.
Rate	This field displays how many control packets this port can receive or transmit per second. It can be adjusted in CPU Protection . 0 means no rate limit.
Status	This field displays the errdisable status Forwarding: The Switch is forwarding packets. Rate-limitation mode is always in Forwarding status. Err-disable: The Switch disables the port on which the control packets are received (inactive-port) or drops specified control packets on the port (inactive-reason)
Recovery Time Left (secs)	This field displays the time (seconds) left before the port(s) becomes active of Errdisable Recovery.
Total Dropped	This field displays the total packet number dropped by this port where the packet rate exceeds the rate of mode rate-limitation.

29.4 CPU Protection Configuration

Use this screen to limit the maximum number of control packets (ARP, BPDU and/or IGMP) that the Switch can receive or transmit on a port. Click the [Click Here](#) link next to **CPU protection** in the **Advanced Application > Errdisable** screen to display the screen as shown.

Note: After you configure this screen, make sure you also enable error detection for the specific control packets in the **Advanced Application > Errdisable > Errdisable Detect** screen.

Figure 162 Advanced Application > Errdisable > CPU protection

CPU protection [Errdisable](#)

Reason: ARP

Port	Rate Limit (pkt/s)
*	
1	0
2	0
3	0
4	0
5	0
6	0
7	0
8	0
9	0
10	0
11	0
12	0

[Apply](#) [Cancel](#)

The following table describes the labels in this screen.

Table 113 Advanced Application > Errdisable > CPU protection

LABEL	DESCRIPTION
Reason	Select the type of control packet you want to configure here.
Port	This field displays the port number. * 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.
Rate Limit (pkt/s)	Enter a number from 0 to 256 to specify how many control packets this port can receive or transmit per second. 0 means no rate limit. You can configure the action that the Switch takes when the limit is exceeded. See Section 29.5 on page 230 for detailed information.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

29.5 Error-Disable Detect Configuration

Use this screen to have the Switch detect whether the control packets exceed the rate limit configured for a port and configure the action to take once the limit is exceeded. Click the [Click Here](#) link next to [Errdisable Detect](#) link in the [Advanced Application > Errdisable](#) screen to display the screen as shown.

Figure 163 Advanced Application > Errdisable > Errdisable Detect

Errdisable Detect		Errdisable
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 114 Advanced Application > Errdisable > Errdisable Detect

LABEL	DESCRIPTION
Cause	This field displays the types of control packet that may cause CPU overload.
*	Use this row to make the setting the same for all entries. Use this row first and then make adjustments to each entry if necessary. Changes in this row are copied to all the entries as soon as you make them.
Active	Select this option to have the Switch detect if the configured rate limit for a specific control packet is exceeded and take the action selected below.
Mode	Select the action that the Switch takes when the number of control packets exceed the rate limit on a port, set in the Advanced Application > Errdisable > CPU protection screen. inactive-port - The Switch disables the port on which the control packets are received. inactive-reason - The Switch drops all the specified control packets (such as BPDU) on the port. rate-limitation - The Switch drops the additional control packets the port(s) 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.

29.6 Error-Disable Recovery Configuration

Use this screen to configure the Switch to automatically undo an action after the error is gone. Click the [Click Here](#) link next to **Errdisable Recovery** in the **Advanced Application > Errdisable** screen to display the screen as shown.

Figure 164 Advanced Application > Errdisable > Errdisable Recovery

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

The following table describes the labels in this screen.

Table 115 Advanced Application > Errdisable > Errdisable Recovery

LABEL	DESCRIPTION
Active	Select this option to turn on the error-disable recovery function on the Switch.
Reason	This field displays the supported features that allow the Switch to shut down a port or discard packets on a port according to the feature requirements and what action you configure.
*	Use this row to make the setting the same for all entries. Use this row first and then make adjustments to each entry if necessary. Changes in this row are copied to all the entries as soon as you make them.
Timer Status	Select this option to allow the Switch to wait for the specified time interval to activate a port or allow specific packets on a port, after the error was gone. Deselect this option to turn off this rule.
Interval	Enter the number of seconds (from 30 to 2592000) for the time interval.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 30

Green Ethernet

This chapter shows you how to configure the Switch to reduce the power consumed by switch ports.

30.1 Green Ethernet Overview

Green Ethernet reduces switch port power consumption in the following ways.

IEEE 802.3az Energy Efficient Ethernet (EEE)

If EEE is enabled, both sides of a link support EEE and there is no traffic, the port enters Low Power Idle (LPI) mode. LPI mode turns off some functions of the physical layer (becomes quiet) to save power. Periodically the port transmits a REFRESH signal to allow the link partner to keep the link alive. When there is traffic to be sent, a WAKE signal is sent to the link partner to return the link to active mode.

Auto Power Down

Auto Power Down turns off almost all functions of the port's physical layer functions when the link is down, so the port only uses power to check for a link up pulse from the link partner. After the link up pulse is detected, the port wakes up from Auto Power Down and operates normally.

Short Reach

Traditional Ethernet transmits all data with enough power to reach the maximum cable length. Shorter cables lose less power, so Short Reach saves power by adjusting the transmit power of each port according to the length of cable attached to that port.

30.2 Configuring Green Ethernet

Click Advanced Application > Green Ethernet in the navigation panel to display the screen as shown.

Note: EEE, Auto Power Down and Short Reach are not supported on an uplink port.

Figure 165 Advanced Application > Green Ethernet

Green Ethernet			
EEE	☐		
Auto Power Down	☐		
Short Reach	☐		

Port	EEE	Auto Power Down	Short Reach
*	☐	☐	☐
1	☐	☐	☐
2	☐	☐	☐
3	☐	☐	☐
4	☐	☐	☐
5	☐	☐	☐
6	☐	☐	☐
7	☐	☐	☐
8	☐	☐	☐
9	☐	☐	☐
10	☐	☐	☐
11	☐	☐	☐
12	☐	☐	☐

The following table describes the labels in this screen.

Table 116 Advanced Application > Green Ethernet

LABEL	DESCRIPTION
EEE	Select this to activate Energy Efficient Ethernet globally.
Auto Power Down	Select this to activate Auto Power Down globally.
Short Reach	Select this to activate Short Reach globally.
Port	This field displays the port number. * 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.
EEE	Select this to activate Energy Efficient Ethernet on this port.
Auto Power Down	Select this to activate Auto Power Down on this port.
Short Reach	Select this to activate Short Reach on this port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 31

Link Layer Discovery Protocol (LLDP)

31.1 LLDP Overview

The LLDP (Link Layer Discovery Protocol) is a layer 2 protocol. It allows a network device to advertise its identity and capabilities on the local network. It also allows the device to maintain and store information from adjacent devices which are directly connected to the network device. This helps an administrator discover network changes and perform necessary network reconfiguration and management. The device information is encapsulated in the LLDPDUs (LLDP data units) in the form of TLV (Type, Length, Value). Device information carried in the received LLDPDUs is stored in the standard MIB.

The Switch supports these basic management TLVs.

- End of LLDPDU (mandatory)
- Chassis ID (mandatory)
- Port ID (mandatory)
- Time to Live (mandatory)
- Port Description (optional)
- System Name (optional)
- System Description (optional)
- System Capabilities (optional)
- Management Address (optional)

The Switch also supports the IEEE 802.1 and IEEE 802.3 organizationally-specific TLVs.

IEEE 802.1 specific TLVs:

- Port VLAN ID TLV (optional)
- Port and Protocol VLAN ID TLV (optional)

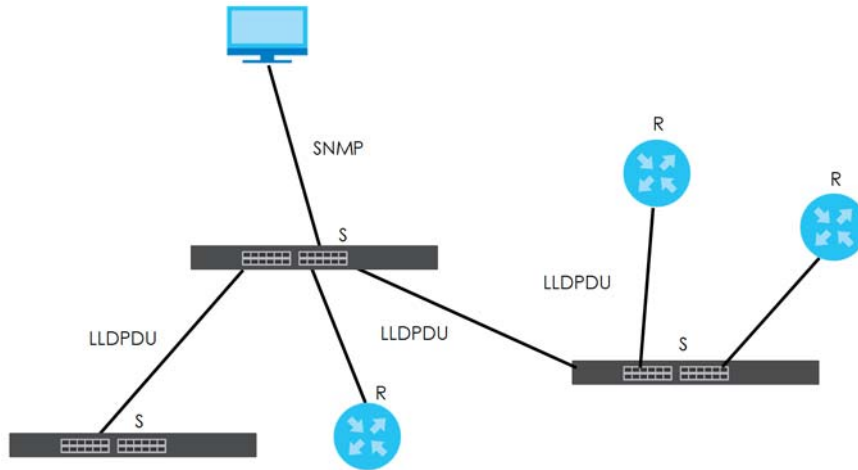
IEEE 802.3 specific TLVs:

- MAC/PHY Configuration/Status TLV (optional)
- Power via MDI TLV (optional, For PoE models only)
- Link Aggregation TLV (optional)
- Maximum Frame Size TLV (optional)

The optional TLVs are inserted between the Time To Live TLV and the End of LLDPDU TLV.

The next figure demonstrates that the network devices Switches and Routers (S and R) transmit and receive device information via LLDPDU and the network manager can query the information using Simple Network Management Protocol (SNMP).

Figure 166 LLDP Overview



31.2 LLDP-MED Overview

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

Class I: IP Communications Controllers or other communication related servers

Class II: Voice Gateways, Conference Bridges or Media Servers

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

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

31.3 LLDP Screens

Figure 168 Advanced Application > LLDP

LLDP		
LLDP	LLDP Local Status	Click here
	LLDP Remote Status	Click here
	LLDP Configuration	Click here
LLDP-MED	LLDP-MED Configuration	Click here
	LLDP-MED Network Policy	Click here
	LLDP-MED Location	Click here

Table 117 Advanced Application > LLDP

LABEL	DESCRIPTION
LLDP	
LLDP Local Status	Click here to show a screen with the Switch's LLDP information.
LLDP Remote Status	Click here to show a screen with LLDP information from the neighboring devices.
LLDP Configuration	Click here to show a screen to configure LLDP parameters.
LLDP-MED	
LLDP-MED Configuration	Click here to show a screen to configure LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) parameters.

Table 117 Advanced Application > LLDP (continued)

LABEL	DESCRIPTION
LLDP-MED Network Policy	Click here to show a screen to configure LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) network policy parameters.
LLDP-MED Location	Click here to show a screen to configure LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) location parameters.

31.4 LLDP Local Status

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

Figure 169 Advanced Application > LLDP > LLDP Local Status

LLDP Local Status

LLDP System Information

Basic TLV

Chassis ID TLV	Chassis ID Subtype	mac-address
	Chassis ID	00:19:cb:00:00:01
System Name TLV	System Name	XS1930
System Description TLV	System Description	V4.60(ABQF.0)b3_console 06/21/2019
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	
		12	

The following table describes the labels in this screen.

Table 118 Advanced Application > LLDP > LLDP Local Status

LABEL	DESCRIPTION
Basic TLV	
Chassis ID TLV	This displays the chassis ID of the local Switch, that is the Switch you're configuring. The chassis ID is identified by the chassis ID subtype. Chassis ID Subtype - this displays how the chassis of the Switch is identified. Chassis ID - This displays the chassis ID of the local Switch.
System Name TLV	This shows the host name of the Switch.
System Description TLV	This shows the firmware version of the Switch.
System Capabilities TLV	This shows the System Capabilities enabled and supported on the local Switch. • System Capabilities Supported - Bridge • System Capabilities Enabled - Bridge
Management Address TLV	The Management Address TLV identifies an address associated with the local LLDP agent that may be used to reach higher layer entities to assist discovery by network management. The TLV may also include the system interface number and an object identifier (OID) that are associated with this management address This field displays the Management Address settings on the specified port(s). • Management Address Subtype - ipv4 / all-802 • Interface Number Subtype - unknown • Interface Number - 0 (not supported) • Object Identifier - 0 (not supported)
LLDP Port Information	This displays the local port information.
Local Port	This displays the number of the Switch port which receives the LLDPDU from the remote device. Click a port number to view the detailed LLDP status on this port at LLDP Local Port Status Detail screen.
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.

31.4.1 LLDP Local Port Status Detail

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

Figure 170 Advanced Application > LLDP > LLDP Local Status > LLDP Local Port Status Detail (Basic TLV)

LLDP Local Port Status Detail			LLDP Local Status
Local Port: 1			
Basic TLV			
Port ID TLV	Port ID Subtype	local-assigned	
	Port ID	1	
Port Description TLV	Port Description		
Dot1 TLV			
Port VLAN ID TLV	Port VLAN ID	1	
Dot3 TLV			
MAC PHY Configuration & Status TLV	AN Supported	Yes	
	AN Enabled	Yes	
	AN Advertised Capability	100baseTX 100baseTXFD 1000baseTFD	
	Oper MAU Type	30	
Link Aggregation TLV	Aggregation Capability	Yes	
	Aggregation Status	No	
	Aggregated Port ID	0	
Max Frame Size TLV	Max Frame Size	1518	

Figure 171 Advanced Application > LLDP > LLDP Local Status > LLDP Local Port Status Detail (MED TLV)

MED TLV		
Capabilities TLV	Network Policy	Yes
	Location	Yes
	Extend Power via MDI PSE	No
	Extend Power via MDI PD	No
	Inventory Management	No
Device Type TLV	Device Type	Network Connectivity
Network Policy TLV	Voice	
	Voice-Signaling	
	Guest-Voice	
	Guest-Voice-Signaling	
	Softphone-Voice	
	Video-Conferencing	
	Streaming-Video	
	Video-Signaling	
Location Identification TLV	Coordinate-base LCI	
	Civic LCI	
	ELIN	

The following table describes the labels in this screen.

Table 119 Advanced Application > LLDP > LLDP Local Status > LLDP Local Port Status Detail

LABEL	DESCRIPTION
Basic TLV	These are the Basic TLV flags
Port ID TLV	The port ID TLV identifies the specific port that transmitted the LLDP frame. - Port ID Subtype: This shows how the port is identified. - Port ID: This is the ID of the port.
Port Description TLV	This displays the local port description.
Dot1 TLV	
Port VLAN ID TLV	This displays the VLAN ID sent by the IEEE 802.1 Port VLAN ID TLV.
Dot3 TLV	
MAC PHY Configuration & Status TLV	The MAC/PHY Configuration/Status TLV advertises the bit-rate and duplex capability of the sending 802.3 node. It also advertises the current duplex and bit-rating of the sending node. Lastly, it advertises whether these setting were the result of auto-negotiation during link initiation or manual override. - AN Supported - Displays if the port supports or does not support auto-negotiation. - AN Enabled - The current auto-negotiation status of the port. - AN Advertised Capability - The auto-negotiation capabilities of the port. - Oper MAU Type - The current Medium Attachment Unit (MAU) type of the port
Link Aggregation TLV	The Link Aggregation TLV indicates whether the link is capable of being aggregated, whether the link is currently in an aggregation, and if in an aggregation, the port identification of the aggregation. - Aggregation Capability — The current aggregation capability of the port. - Aggregation Status — The current aggregation status of the port. - Aggregation Port ID — The aggregation ID of the current port.
Max Frame Size TLV	This displays the maximum supported frame size in octets.
MED TLV	LLDP Media Endpoint Discovery (MED) is an extension of LLDP that provides additional capabilities to support media endpoint devices. MED enables advertisement and discovery of network policies, device location discovery to allow creation of location databases, and information for troubleshooting.
Capabilities TLV	This field displays which LLDP-MED TLV are capable to transmit on the Switch. - Network Policy - Location - Extend Power via MDI PSE - Extend Power via MDI PD - Inventory Management
Device Type TLV	This is the LLDP-MED device class. The Zyxel Switch device type is: Network Connectivity

Table 119 Advanced Application > LLDP > LLDP Local Status > LLDP Local Port Status Detail

LABEL	DESCRIPTION
Network Policy TLV	This displays a network policy for the specified application. - Voice - Voice-Signaling - Guest-Voice - Guest-Voice-Signaling - Softphone-Voice - Video-Conferencing - Streaming-Video - Video-Signaling
Location Identification TLV	This shows the location information of a caller by its ELIN (Emergency Location Identifier Number) or the IETF Geopriv Civic Address based Location Configuration Information (Civic Address LCI). - Coordinate-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)

31.5 LLDP Remote Status

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

Figure 172 Advanced Application > LLDP > LLDP Remote Status

LLDP Remote Status							LLDP
Index	Local Port	Chassis ID	Port ID	Port Description	System Name	Management Address	
1	5	60:31:97:0f:8d:c4	1	UPLINK	NWA5123-AC-HD	172.21.10.11	

The following table describes the labels in this screen.

Table 120 Advanced Application > LLDP > LLDP Remote Status

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

31.5.1 LLDP Remote Port Status Detail

This screen displays detailed LLDP status of the remote device connected to the Switch. Click **Advanced Application > LLDP > LLDP Remote Status (Click Here)** and then click an index number, for example 1, in the **Index** column in the **LLDP Remote Status** screen to display the screen as shown next.

Figure 173 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Basic TLV)

LLDP Remote Port Status Detail			LLDP Remote Status
Local Port: 26			
Basic TLV			
Chassis ID TLV	Chassis ID Subtype	mac-address	
	Chassis ID	00:19:cb:01:01:02	
Port ID TLV	Port ID Subtype	local-assigned	
	Port ID	2	
Time To Live TLV	Time To Live	120	
Port Description TLV	Port Description		
System Name TLV	System Name	G53700	
System Description TLV	System Description	V4.30(AAGE.1)_20170802 08/02/2017	
System Capabilities TLV	System Capabilities Supported	bridge	
	System Capabilities Enabled	bridge	
Management Address TLV	Management Address Subtype	ipv4	
	Management Address	172.16.1.100	
	Interface Number Subtype	unknown	
	Interface Number	0	
	Object Identifier		

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

Table 121 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Basic TLV)

LABEL	DESCRIPTION
Local Port	This displays the number of the Switch's port to which the remote device is connected.
Basic TLV	
Chassis ID TLV	Chassis ID Subtype - this displays how the chassis of the remote device is identified. Chassis ID - this displays the chassis ID of the remote device. The chassis ID is identified by the chassis ID subtype.
Port ID TLV	Port ID Subtype - this displays how the port of the remote device is identified. Port ID - this displays the port ID of the remote device. The port ID is identified by the port ID subtype.

Table 121 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Basic TLV)

LABEL	DESCRIPTION
Time To Live TLV	This displays the time-to-live (TTL) multiplier of LLDP frames. The device information on the neighboring devices ages out and is discarded when its corresponding TTL expires. The TTL value is to multiply the TTL multiplier by the LLDP frames transmitting interval.
Port Description TLV	This displays the remote port description.
System Name TLV	This displays the system name of the remote device.
System Description TLV	This displays the system description of the remote device.
System Capabilities TLV	This displays whether the system capabilities are enabled and supported on the remote device. • System Capabilities Supported • System Capabilities Enabled
Management Address TLV	This displays the following management address parameters of the remote device. • Management Address Subtype • Management Address • Interface Number Subtype • Interface Number • Object Identifier

Figure 174 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail> (Dot 1 and Dot3 TLV)

Dot1 TLV		
Port VLAN ID TLV	Port VLAN ID	1
Port-Protocol VLAN ID TLV	Port-Protocol VLAN ID	1
	Port-Protocol VLAN ID Supported	Yes
	Port-Protocol VLAN ID Enabled	Yes
Vlan Name TLV	VLAN ID	
	VLAN Name	
Protocol Identity TLV	Protocol ID	
Dot3 TLV		
MAC PHY Configuration & Status TLV	AN Supported	Yes
	AN Enabled	Yes
	AN Advertised Capability	10baseT 10baseTFD 100baseTX 100baseTXFD 1000baseTFD
	Oper MAU type	30
Link Aggregation TLV	Aggregation Capability	Yes
	Aggregation Status	No
	Aggregated Port ID	2
Power Via MDI TLV	Port Class	PSE
	MDI Supported	Yes
	MDI Enabled	Yes
	Pair Controlable	No
	PSE Power Pairs	1
	Power Class	1
Max Frame Size TLV	Max Frame Size	1518

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

Table 122 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Dot1 and Dot3 TLV)

LABEL	DESCRIPTION
Dot1 TLV	
Port VLAN ID TLV	This displays the VLAN ID of this port on the remote device.
Port-Protocol VLAN ID TLV	This displays the IEEE 802.1 Port Protocol VLAN ID TLV, which indicates whether the VLAN ID and whether it is enabled and supported on the port of remote Switch which sent the LLDPDU. - Port-Protocol VLAN ID - Port-Protocol VLAN ID Supported - Port-Protocol VLAN ID Enabled

Table 122 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Dot1 and Dot3 TLV)

LABEL	DESCRIPTION
Vlan Name TLV	This shows the VLAN ID and name for remote device port. - VLAN ID - VLAN Name
Protocol Identity TLV	The Protocol Identity TLV allows the Switch to advertise the particular protocols that are accessible through its port.
Dot3 TLV	
MAC PHY Configuration & Status TLV	The MAC/PHY Configuration/Status TLV advertises the bit-rate and duplex capability of the sending 802.3 node. It also advertises the current duplex and bit-rating of the sending node. Lastly, it advertises whether these setting were the result of auto-negotiation during link initiation or manual override. - AN Supported - Displays if the port supports or does not support auto-negotiation. - AN Enabled - The current auto-negotiation status of the port. - AN Advertised Capability - The auto-negotiation capabilities of the port. - Oper MAU Type - The current Medium Attachment Unit (MAU) type of the port
Link Aggregation TLV	The Link Aggregation TLV indicates whether the link is capable of being aggregated, whether the link is currently in an aggregation, and if in an aggregation, the port identification of the aggregation. - Aggregation Capability — The current aggregation capability of the port. - Aggregation Status — The current aggregation status of the port. - Aggregation Port ID — The aggregation ID of the current port.
Power Via MDI TLV	The Power Via MDI TLV allows PoE devices to advertise and discover the MDI power support capabilities of the sending port on the remote device. - Port Class - MDI Supported - MDI Enabled - Pair Controllable - PSE Power Pairs - Power Class
Max Frame Size TLV	This displays the maximum supported frame size in octets.

Figure 175 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (MED TLV)

MED TLV		
Capabilities TLV	Network Policy	Yes
	Location	Yes
	Extend Power via MDI PSE	No
	Extend Power via MDI PD	No
	Inventory Management	No
Device Type TLV	Device Type	Network Connectivity
Network Policy TLV	Voice	VLAN ID 10, tagged, known, L2-priority 7, DSCP 63
	Voice-Signaling	VLAN ID 100, tagged, known, L2-priority 2, DSCP 10
	Guest-Voice	VLAN ID 20, tagged, known, L2-priority 3, DSCP 12
	Guest-Voice-Signaling	VLAN ID 0, untagged, known, L2-priority 0, DSCP 0
	Softphone-Voice	VLAN ID 200, tagged, known, L2-priority 1, DSCP 1
	Video-Conferencing	VLAN ID 0, untagged, known, L2-priority 0, DSCP 0
	Streaming-Video	VLAN ID 300, tagged, known, L2-priority 4, DSCP 20
	Video-Signaling	VLAN ID 400, tagged, known, L2-priority 6, DSCP 55
Location Identification TLV	Coordinate-base LCI	latitude north 0.0 longitude east 0.9995 altitude meters 0.0 datum NAD83-MLLW
	Civic LCI	country TW city HSINCHU building ZYXEL
	ELIN	1234567890
Inventory TLV	Hardware Revision	V20131114 11/14/2013
	Software Revision	V4.10(AAOA.0) 11/15/2013
	Firmware Revision	V4.10(AAOA.0) 11/15/2013
	Model Name	GS3700-HP
	Manufacturer	123456789
	Serial Number	123456789
	Asset ID	123456789
Extended Power via MDI TLV	Power Type	PSE Device
	Power Source	PSE
	Power Priority	High
	Power Value	Available power 130.0 Watts

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

Table 123 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (MED TLV)

LABEL	DESCRIPTION
MED TLV	LLDP Media Endpoint Discovery (MED) is an extension of LLDP that provides additional capabilities to support media endpoint devices. MED enables advertisement and discovery of network policies, device location discovery to allow creation of location databases, and information for troubleshooting.
Capabilities TLV	This displays the MED capabilities the remote port supports. • Network Policy • Location • Extend Power via MDI PSE • Extend Power via MDI PD • Inventory Management
Device Type TLV	LLDP-MED endpoint device classes: • Endpoint Class I • Endpoint Class II • Endpoint Class III • Network Connectivity
Network Policy TLV	This displays a network policy for the specified application. • Voice • Voice-Signaling • Guest-Voice • Guest-Voice-Signaling • Softphone-Voice • Video-Conferencing • Streaming-Video • Video-Signaling
Location Identification TLV	This shows the location information of a caller by its: • Coordinate-base LCI - latitude and longitude coordinates of the Location Configuration Information (LCI) • Civic LCI - IETF Geopriv Civic Address based Location Configuration Information • EIJN - (Emergency Location Identifier Number)
Inventory TLV	The majority of IP Phones lack support of management protocols such as SNMP, so LLDP-MED inventory TLVs are used to provide their inventory information to the Network Connectivity Devices such as the Switch. The Inventory TLV may contain the following information. • Hardware Revision • Software Revision • Firmware Revision • Model Name • Manufacturer • Serial Number • Asset ID
Extended Power via MDI TLV	Extended Power Via MDI Discovery enables detailed power information to be advertised by Media Endpoints, such as IP phones and Network Connectivity Devices such as the Switch. • Power Type - whether it is currently operating from primary power or is on backup power (backup power may indicate to the Endpoint Device that it should move to a power conservation mode). • Power Source - whether or not the Endpoint is currently operating from an external power source. • Power Priority - the Endpoint Device's power priority (which the Network Connectivity Device may use to prioritize which devices will remain in service during power shortages) • Power Value - power requirement, in fractions of Watts, in current configuration

31.6 LLDP Configuration

Use this screen to configure global LLDP settings on the Switch. Click **Advanced Application > LLDP > LLDP Configuration** (Click Here) to display the screen as shown next.

Figure 176 Advanced Application > LLDP > LLDP Configuration

LLDP Configuration		
Active	☒	
Transmit Interval	30	seconds
Transmit Hold	4	times
Transmit Delay	2	seconds
Reinitialize Delay	2	seconds
Apply Cancel		
Port	Admin Status	Notification
*	Disable ▼	☐
1	Tx-Rx ▼	☐
2	Tx-Rx ▼	☐
3	Tx-Rx ▼	☐
4	Tx-Rx ▼	☐
5	Tx-Rx ▼	☐
6	Tx-Rx ▼	☐
7	Tx-Rx ▼	☐
8	Tx-Rx ▼	☐
9	Tx-Rx ▼	☐
10	Tx-Rx ▼	☐
11	Tx-Rx ▼	☐
12	Tx-Rx ▼	☐
Apply Cancel		

The following table describes the labels in this screen.

Table 124 Advanced Application > LLDP > LLDP Configuration

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

Table 124 Advanced Application > LLDP > LLDP Configuration

LABEL	DESCRIPTION
*	Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Changes in this row are copied to all the ports as soon as you make them.
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.

31.6.1 Basic TLV Setting

Use this screen to configure Basic TLV settings. Click **Advanced Application > LLDP > LLDP Configuration (Click Here) > Basic TLV Setting** to display the screen as shown next.

Figure 177 Advanced Application > LLDP > LLDP Configuration > Basic TLV Setting

Basic TLV Setting				LLDP Configuration		
Port	Management Address	Port Description	System Capabilities	System Description	System Name	
*	☐	☐	☐	☐	☐	☐
1	☒	☒	☒	☒	☒	☒
2	☒	☒	☒	☒	☒	☒
3	☒	☒	☒	☒	☒	☒
4	☒	☒	☒	☒	☒	☒
5	☒	☒	☒	☒	☒	☒
6	☒	☒	☒	☒	☒	☒
7	☒	☒	☒	☒	☒	☒
8	☒	☒	☒	☒	☒	☒
9	☒	☒	☒	☒	☒	☒
10	☒	☒	☒	☒	☒	☒
11	☒	☒	☒	☒	☒	☒
12	☒	☒	☒	☒	☒	☒
Apply Cancel						

The following table describes the labels in this screen.

Table 125 Advanced Application > LLDP > LLDP Configuration > Basic TLV Setting

LABEL	DESCRIPTION
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.
Management Address	Select the check box(es) to enable or disable the sending of Management Address TLVs on the port(s).
Port Description	Select the check box(es) to enable or disable the sending of Port Description TLVs on the port(s).

Table 125 Advanced Application > LLDP > LLDP Configuration > Basic TLV Setting

LABEL	DESCRIPTION
System Capabilities	Select the check box(es) to enable or to disable the sending of System Capabilities TLVs on the port(s).
System Description	Select the check box(es) to enable or to disable the sending of System Description TLVs on the port(s).
System Name	Select the check box(es) to enable or to disable the sending of System Name TLVs on the port(s).
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

31.6.2 Org-specific TLV Setting

Use this screen to configure organization-specific TLV settings. Click **Advanced Application > LLDP > LLDP Configuration (Click Here) > Org-specific TLV Setting** to display the screen as shown next.

Figure 178 Advanced Application > LLDP > LLDP Configuration> Org-specific TLV Setting

Port	Dot1 TLV Port VLAN ID	Link Aggregation	Dot3 TLV MAC/PHY	Max Frame Size
*	☐	☐	☐	☐
1	☒	☐	☒	☐
2	☒	☐	☒	☐
3	☒	☐	☒	☐
4	☒	☐	☒	☐
5	☒	☐	☒	☐
6	☒	☐	☒	☐
7	☒	☐	☒	☐
8	☒	☐	☒	☐
9	☒	☐	☒	☐
10	☒	☐	☒	☐
11	☒	☐	☒	☐
12	☒	☐	☒	☐

The following table describes the labels in this screen.

Table 126 Advanced Application > LLDP > LLDP Configuration > Org-specific TLV Setting

LABEL	DESCRIPTION
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.
Dot1 TLV	
Port VLAN ID	Select the check box(es) to enable or disable the sending of IEEE 802.1 Port VLAN ID TLVs on the port(s). All check boxes in this column are enabled by default.
Dot3 TLV	
Link Aggregation	Select the check box(es) to enable or disable the sending of IEEE 802.3 Link Aggregation TLVs on the port(s).

Table 126 Advanced Application > LLDP > LLDP Configuration > Org-specific TLV Setting

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

31.7 LLDP-MED Configuration

Click **Advanced Application > LLDP > LLDP-MED Configuration** to display the screen as shown next.

Figure 179 Advanced Application > LLDP > LLDP-MED Configuration

Port	Notification Topology Change	MED TLV Setting Location	Network Policy
*	☐	☐	☐
1	☐	☐	☐
2	☐	☐	☐
3	☐	☐	☐
4	☐	☐	☐
5	☐	☐	☐
6	☐	☐	☐
7	☐	☐	☐
8	☐	☐	☐
9	☐	☐	☐
10	☐	☐	☐
11	☐	☐	☐
12	☐	☐	☐

The following table describes the labels in this screen.

Table 127 Advanced Application > LLDP > LLDP-MED Configuration

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

Table 127 Advanced Application > LLDP > LLDP-MED Configuration

LABEL	DESCRIPTION
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.

31.8 LLDP-MED Network Policy

Click **Advanced Application > LLDP > LLDP-MED Network Policy (Click Here)** to display the screen as shown next.

Figure 180 Advanced Application > LLDP > LLDP-MED Network Policy

The following table describes the labels in this screen.

Table 128 Advanced Application > LLDP > LLDP-MED Network Policy

LABEL	DESCRIPTION
Port	Enter the port number to set up the LLDP-MED network policy.
Application Type	Select the type of application used in the network policy. • voice • voice-signaling • guest-voice • guest-voice-signaling • softphone-voice • video-conferencing • streaming-video • video-signaling
Tag	Select to tag or untag in the network policy. • tagged • untagged
VLAN	Enter the VLAN ID number. It should be from 1 to 4094. For priority tagged frames, enter "0".

Table 128 Advanced Application > LLDP > LLDP-MED Network Policy

LABEL	DESCRIPTION
DSCP	Enter the DSCP value of the network policy. The value is defined from 0 through 63 with the 0 representing use of the default DSCP value.
Priority	Enter the priority value for the network policy.
Add	Click Add after finish entering the network policy information. A summary table will list all the Switch you've added.
Cancel	Click Cancel to begin entering the information afresh.
Index	This field displays the of index number of the network policy. Click an index number to edit the rule.
Port	This field displays the port number of the network policy.
Application Type	This field displays the application type of the network policy.
Tag	This field displays the Tag Status of the network policy.
VLAN	This field displays the VLANID of the network policy.
Priority	This field displays the priority value of the network policy.
DSCP	This field displays the DSCP value of the network policy.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Check the rules that you want to remove, then click the Delete button.
Cancel	Click Cancel to clear the selected check boxes.

31.9 LLDP-MED Location

Click **Advanced Application > LLDP > LLDP-MED Location (Click Here)** to display the screen as shown next.

Figure 181 Advanced Application > LLDP > LLDP-MED Location

LLDP-MED Location					LLDP
Port					
Location Coordinates	Latitude		north ▼		
	Longitude		west ▼		
	Altitude		meters ▼		
	Datum	WGS84 ▼			
Civic Address	Country		State		
	County		City		
	Division		Neighbor		
	Street		Leading-Street-Direction		
	Street-Suffix		Trailing-Street-Suffix		
	House-Number		House-Number-Suffix		
	Landmark		Additional-Location		
	Name		Zip-Code		
	Building		Unit		
	Floor		Room-Number		
	Place-Type		Postal-Community-Name		
	Post-Office-Box		Additional-Code		
	ELIN Number				
	Add Cancel				
Index	Port	Location Coordinates	Civic Address	ELIN Number	☐
Delete Cancel					

The following table describes the labels in this screen.

Table 129 Advanced Application > LLDP > LLDP-MED Location

LABEL	DESCRIPTION
Port	Enter the port number you want to set up the location within the LLDP-MED network.
Location Coordinates	The LLDP-MED uses geographical coordinates and Civic Address to set the location information of the remote device. Geographical based coordinates includes latitude, longitude, altitude and datum. Civic Address includes Country, State, County, City, Street and other related information.
Latitude	Enter the latitude information. The value should be from 0° to 90°. The negative value represents the South. • north • south
Longitude	Enter the longitude information. The value should be from 0° to 180°. The negative value represents the West. • west • east

Table 129 Advanced Application > LLDP > LLDP-MED Location

LABEL	DESCRIPTION
Altitude	Enter the altitude information. The value should be from -2097151 to 2097151 in meters or in floors. • meters • floor
Datum	Select the appropriate geodetic datum used by GPS. • WGS84 • NAD83-NAVD88 • NAD83-MLLW
Civic Address	Enter the Civic Address by providing information such as Country, State, County, City, Street, Number, ZIP code and other additional information. Enter at least two field in this configuration including the Country. The valid length of the Country field is 2 characters and all other fields are up to 32 characters. • Country • State • County • City • Division • Neighbor • Street • Leading-Street-Direction • Street-Suffix • Trailing-Street-Suffix • House-Number • House-Number-Suffix • Landmark • Additional-Location • Name • Zip-Code • Building • Unit • Floor • Room-Number • Place-Type • Postal-Community-Name • Post-Office-Box • Additional-Code
ELIN Number	Enter a numerical digit string, corresponding to the ELIN identifier which is used during emergency call setup to a traditional CAMA or ISDN trunk-based PSAP. The valid length is from 10 to 25 characters.
Add	Click Add after finish entering the location information.
Cancel	Click Cancel to begin entering the location information afresh.
Index	This lists the index number of the location configuration. Click an index number to view or edit the location.
Port	This lists the port number of the location configuration.
Location Coordinates	This field displays the location configuration information based on geographical coordinates that includes longitude, latitude, altitude and datum.
Civic Address	This field displays the Civic Address for the remote device using information such as Country, State, County, City, Street, Number, ZIP code and additional information.
ELIN Number	This field shows the Emergency Location Identification Number (ELIN), which is used to identify endpoint devices when they issue emergency call services. The valid length is form 10 to 25 characters.

Table 129 Advanced Application > LLDP > LLDP-MED Location

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

CHAPTER 32

Static Route

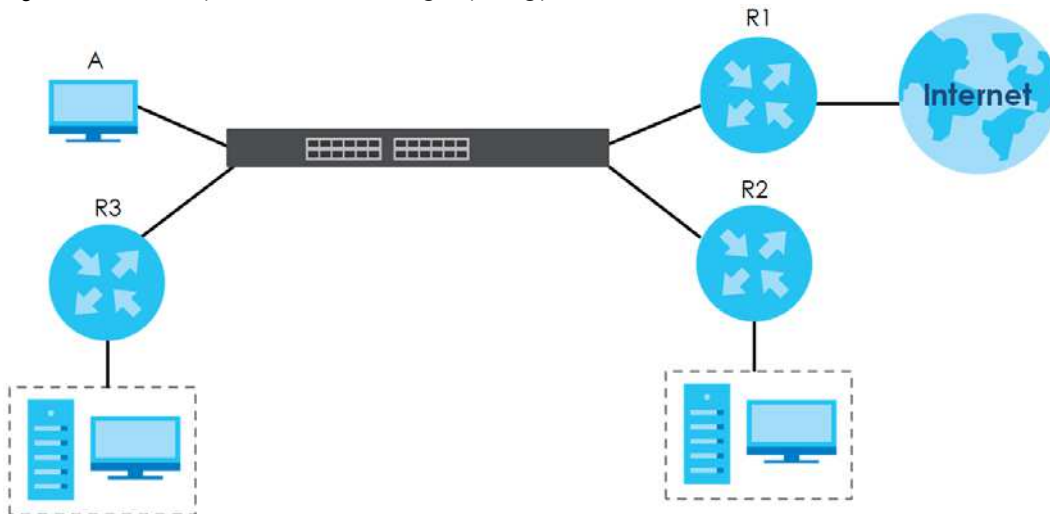
32.1 Static Routing Overview

This chapter shows you how to configure static routes.

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 182 Example of Static Routing Topology



32.1.1 What You Can Do

- Use the **Static Routing** screen ([Section 32.2 on page 259](#)) to display the link to the **IPv4 Static Route** screen.
- Use the **IPv4 Static Route** screen ([Section 32.3 on page 259](#)) to configure and enable an IPv4 static route.
- Use the **IPv6 Static Route** screen ([Section 32.4 on page 260](#)) to configure and enable an IPv6 static route.

32.2 Static Routing

Click IP Application > **Static Routing** in the navigation panel to display the screen as shown. Click the link next to **IPv4 Static Route** to open a screen where you can create IPv4 static routing rules. Click the link next to **IPv6 Static Route** to open a screen where you can create IPv6 static routing rules.

Figure 183 IP Application > Static Routing

Static Routing	
IPv4 Static Route	Click Here
IPv6 Static Route	Click Here

32.3 IPv4 Static Route

Click the link next to **IPv4 Static Route** in the IP Application > **Static Routing** screen to display the screen as shown.

Figure 184 IP Application > Static Routing > IPv4 Static Route

IPv4 Static Route Static Routing

Active ☐

Name

Destination IP Address

IP Subnet Mask

Gateway IP Address

Metric

Add Cancel Clear

Index	Active	Name	Destination Address	Subnet Mask	Gateway Address	Metric	
Delete Cancel							

The following table describes the related labels you use to create a static route.

Table 130 IP Application > Static Routing > IPv4 Static Route

LABEL	DESCRIPTION
Active	This field allows you to activate/deactivate this static route.
Name	Enter a descriptive name (up to 10 printable ASCII characters) for identification purposes.
Destination IP Address	This parameter specifies the IP network address of the final destination.
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.

Table 130 IP Application > Static Routing > IPv4 Static Route (continued)

LABEL	DESCRIPTION
Gateway IP Address	Enter the IP address of the gateway. The gateway is an immediate neighbor of your Switch that will forward the packet to the destination. The gateway must be a router on the same segment as your Switch.
Metric	The metric represents the "cost" of transmission for routing purposes. IP routing uses hop count as the measurement of cost, with a minimum of 1 for directly connected networks. Enter a number that approximates the cost for this link. The number need not be precise, but it must be between 1 and 15. In practice, 2 or 3 is usually a good number.
Add	Click Add to insert a new static route to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the above fields to your previous configuration.
Clear	Click Clear to set the above fields back to the factory defaults.
Index	This field displays the index number of the route. Click a number to edit the static route entry.
Active	This field displays Yes when the static route is activated and NO when it is deactivated.
Name	This field displays the descriptive name for this route. This is for identification purposes only.
Destination Address	This field displays the IP network address of the final destination.
Subnet Mask	This field displays the subnet mask for this destination.
Gateway Address	This field displays the IP address of the gateway. The gateway is an immediate neighbor of your Switch that will forward the packet to the destination.
Metric	This field displays the cost of transmission for routing purposes.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the check boxes.

32.4 IPv6 Static Route

Click the link next to **IPv6 Static Route** in the **IP Application > Static Routing** screen to display the screen as shown.

Figure 185 IP Application > Static Routing > IPv6 Static Route

The screenshot shows the 'IPv6 Static Route' configuration interface. It includes a header with the title 'IPv6 Static Route' and a link 'Static Routing'. The main area contains several input fields: 'Route Destination', 'Prefix Length', 'Next Hop', 'Interface Type' (which has a dropdown menu currently showing 'VLAN'), and 'Interface ID'. Below these fields are two buttons: 'Add' and 'Cancel'. At the bottom of the interface is a table with the following columns: 'Index', 'Interface', 'Route Destination/Prefix Length', 'Next Hop', and a checkbox. Below the table are two more buttons: 'Delete' and 'Cancel'.

The following table describes the related labels you use to create a static route.

Table 131 IP Application > Static Routing > IPv6 Static Route

LABEL	DESCRIPTION
Route Destination	Enter the IPv6 address of the final destination.
Prefix Length	Enter the prefix length number of up to 64 for this destination.
Next Hop	Enter the IPv6 address of the next-hop router.
Interface Type	Select the type of the IPv6 interface through which the IPv6 packets are forwarded. The Switch supports only the VLAN interface type at the time of writing.
Interface ID	Enter the ID number of the IPv6 interface through which the IPv6 packets are forwarded.
Add	Click Add to insert a new static route to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Index	This field displays the index number of the route. Click a number to edit the static route entry.
Interface	This field displays the descriptive name of the interface that is used to forward the packets to the destination.
Route Destination/Prefix Length	This field displays the IPv6 subnet prefix and prefix length of the final destination.
Next Hop	This field displays the IPv6 address of the gateway that helps forward the packet to the destination.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the check boxes.

CHAPTER 33

DHCP

33.1 DHCP Overview

This chapter shows you how to configure the DHCP feature.

DHCP (Dynamic Host Configuration Protocol RFC 2131 and RFC 2132) allows individual computers to obtain TCP/IP configuration at start-up from a server. If you configure the Switch as a DHCP relay agent, then the Switch forwards DHCP requests to DHCP server on your network. If you don't configure the Switch as a DHCP relay agent then you must have a DHCP server in the broadcast domain of the client computers or else the client computers must be configured manually.

33.1.1 What You Can Do

- Use the DHCPv4 **Status** screen ([Section 33.3 on page 263](#)) to display the relay mode.
- Use the DHCPv4 **Relay** screen ([Section 33.4 on page 264](#)) to enable and configure global DHCPv4 relay.
- Use the VLAN **Setting** screen ([Section 33.4.6 on page 269](#)) to configure your DHCPv4 settings based on the VLAN domain of the DHCPv4 clients.
- Use the DHCPv6 **Relay** screen ([Section 33.5 on page 273](#)) to enable and configure DHCPv6 relay.

33.1.2 What You Need to Know

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

DHCP Modes

If there is already a DHCP server on your network, then you can configure the Switch as a DHCP relay agent. When the Switch receives a request from a computer on your network, it contacts the DHCP server for the necessary IP information, and then relays the assigned information back to the computer.

DHCPv4 Configuration Options

The DHCPv4 configuration on the Switch is divided into **Global** and **VLAN** screens. The screen you should use for configuration depends on the DHCP services you want to offer the DHCP clients on your network. Choose the configuration screen based on the following criteria:

- **Global** - The Switch forwards all DHCP requests to the same DHCP server.
- **VLAN** - The Switch is configured on a VLAN by VLAN basis. The Switch can be configured to relay DHCP requests to different DHCP servers for clients in different VLAN.

33.2 DHCP Configuration

Click IP Application > DHCP in the navigation panel to display the screen as shown. Click the link next to DHCPv4 to open screens where you can enable and configure DHCPv4 relay settings and create option 82 profiles. Click the link next to DHCPv6 to open a screen where you can configure DHCPv6 relay settings.

Figure 186 IP Application > DHCP

DHCP	
DHCPv4	Click Here
DHCPv6	Click Here

33.3 DHCPv4 Status

Click IP Application > DHCP > DHCPv4 in the navigation panel. The DHCP Status screen displays.

Figure 187 IP Application > DHCP > DHCPv4

DHCP Status		DHCP	Option 82 Profile	Global	VLAN
Relay Status					
Relay Mode	None				
VID		Current Source Address			

The following table describes the labels in this screen.

Table 132 IP Application > DHCP > DHCPv4

LABEL	DESCRIPTION
Relay Status	This section displays configuration settings related to the Switch's DHCP relay mode.
Relay Mode	This field displays: None - if the Switch is not configured as a DHCP relay agent. Global - if the Switch is configured as a DHCP relay agent only. VLAN - followed by a VLAN ID or multiple VLAN IDs if it is configured as a relay agent for specific VLAN(s).
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.

33.4 DHCPv4 Relay

Configure DHCP relay on the Switch if the DHCP clients and the DHCP server are not in the same broadcast domain. During the initial IP address leasing, the Switch helps to relay network information (such as the IP address and subnet mask) between a DHCP client and a DHCP server. Once the DHCP client obtains an IP address and can connect to the network, network information renewal is done between the DHCP client and the DHCP server without the help of the Switch.

The Switch can be configured as a global DHCP relay. This means that the Switch forwards all DHCP requests from all domains to the same DHCP server. You can also configure the Switch to relay DHCP information based on the VLAN membership of the DHCP clients.

33.4.1 DHCPv4 Relay Agent Information

The Switch can add information about the source of client DHCP requests that it relays to a DHCP server by adding **Relay Agent Information**. This helps provide authentication about the source of the requests. The DHCP server can then provide an IP address based on this information. Please refer to RFC 3046 for more details.

The DHCP **Relay Agent Information** feature adds an Agent Information field (also known as the **Option 82** field) to DHCP requests. The **Option 82** field is in the DHCP headers of client DHCP request frames that the Switch relays to a DHCP server.

Relay Agent Information can include the **System Name** of the Switch if you select this option. You can change the **System Name** in **Basic Settings > General Setup**.

The following describes the DHCP relay agent information that the Switch sends to the DHCP server:

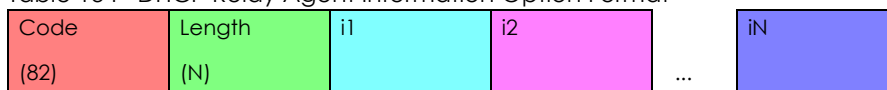
Table 133 Relay Agent Information

FIELD LABELS	DESCRIPTION
Slot ID	(1 byte) This value is always 0 for stand-alone switches.
Port ID	(1 byte) This is the port that the DHCP client is connected to.
VLAN ID	(2 bytes) This is the VLAN that the port belongs to.
Information	(up to 64 bytes) This optional, read-only field is set according to system name set in Basic Settings > General Setup .

33.4.1.1 DHCPv4 Relay Agent Information Format

A DHCP Relay Agent Information option has the following format.

Table 134 DHCP Relay Agent Information Option Format



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.

33.4.1.2 Sub-Option Format

There are two types of sub-option: "Agent Circuit ID Sub-option" and "Agent Remote ID Sub-option". They have the following formats.

Table 135 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 136 DHCP Relay Agent Remote ID Sub-option Format

SubOpt Code	Length	Value
2 (1 byte)	N (1 byte)	MAC Address or String

The 1 in the first field identifies this as an Agent Circuit ID sub-option and 2 identifies this as an Agent Remote ID sub-option. The next field specifies the length of the field.

33.4.2 DHCPv4 Option 82 Profile

Use this screen to create DHCPv4 option 82 profiles. Click IP Application > DHCP > DHCPv4 in the navigation panel and click the Option 82 Profile link to display the screen as shown.

Figure 188 IP Application > DHCP > DHCPv4 > Option 82 Profile

DHCP Option 82 Profile [DHCP Setting](#)

Profile Setup

Name:

Circuit-ID: ☐ Enable
☐ slot-port ☐ vlan ☐ hostname
 string:

Remote-ID: ☐ Enable
☐ mac
 string:

[Add](#) [Cancel](#)

Profile Name	Circuit-ID Enable	Circuit-ID Field	Remote-ID Enable	Remote-ID Field	
default1	Yes	slot-port, vlan	No	-	☐
default2	Yes	slot-port, vlan, hostname	No	-	☐

[Delete](#) [Cancel](#)

The following table describes the labels in this screen.

Table 137 IP Application > DHCP > DHCPv4 > Option 82 Profile

LABEL	DESCRIPTION
Name	Enter a descriptive name for the profile for identification purposes. You can use up to 32 ASCII characters. Spaces are allowed.
Circuit-ID	Use this section to configure the Circuit ID sub-option to include information that is specific to the relay agent (the Switch).
Enable	Select this option to have the Switch add the Circuit ID sub-option to client DHCP requests that it relays to a DHCP server.
slot-port	Select this option to have the Switch add the number of port that the DHCP client is connected to.
vlan	Select this option to have the Switch add the ID of VLAN which the port belongs to.
hostname	This is the system name you configure in the Basic Setting > General Setup screen. Select this option for the Switch to add the system name to the client DHCP requests that it relays to a DHCP server.
string	Enter a string of up to 64 ASCII characters that the Switch adds into the client DHCP requests. Spaces are allowed.
Remote-ID	Use this section to configure the Remote ID sub-option to include information that identifies the relay agent (the Switch).
Enable	Select this option to have the Switch append the Remote ID sub-option to the option 82 field of DHCP requests.
mac	Select this option to have the Switch add its MAC address to the client DHCP requests that it relays to a DHCP server.
string	Enter a string of up to 64 ASCII characters for the remote ID information in this field. Spaces are allowed.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to their last saved values.
Profile Name	This field displays the descriptive name of the profile. Click the name to change the settings.
Circuit-ID	
Enable	This field displays whether the Circuit ID sub-option is added to client DHCP requests.
Field	This field displays the information that is included in the Circuit ID sub-option.
Remote-ID	
Enable	This field displays whether the Remote ID sub-option is added to client DHCP requests.
Field	This field displays the information that is included in the Remote ID sub-option.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Check the entry(ies) that you want to remove and then click the Delete button.
Cancel	Click Cancel to clear the selected check box(es).

33.4.3 Configuring DHCPv4 Global Relay

Use this screen to configure global DHCPv4 relay. Click **IP Application > DHCP > DHCPv4** in the navigation panel and click the **Global** link to display the screen as shown.

Figure 189 IP Application > DHCP > DHCPv4 > Global

DHCP Relay		Status	Port
Active	☐		
Remote DHCP Server 1	0.0.0.0		
Remote DHCP Server 2	0.0.0.0		
Remote DHCP Server 3	0.0.0.0		
Option 82 Profile			

[Apply](#) [Cancel](#)

The following table describes the labels in this screen.

Table 138 IP Application > DHCP > DHCPv4 > Global

LABEL	DESCRIPTION
Active	Select this check box to enable DHCPv4 relay.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCPv4 server in dotted decimal notation.
Option 82 Profile	Select a pre-defined DHCPv4 option 82 profile that the Switch applies to all ports. The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

33.4.4 DHCPv4 Global Relay Port Configure

Use this screen to apply a different DHCP option 82 profile to certain ports on the Switch. To open this screen, click IP Application > DHCP > DHCPv4 > Global > Port.

Figure 190 IP Application > DHCP > DHCPv4 > Global > Port

Port		DHCP relay
Port		
Option 82 Profile		

[Add](#) [Cancel](#) [Clear](#)

Index	Port	Profile Name	☐

[Delete](#) [Cancel](#)

The following table describes the labels in this screen.

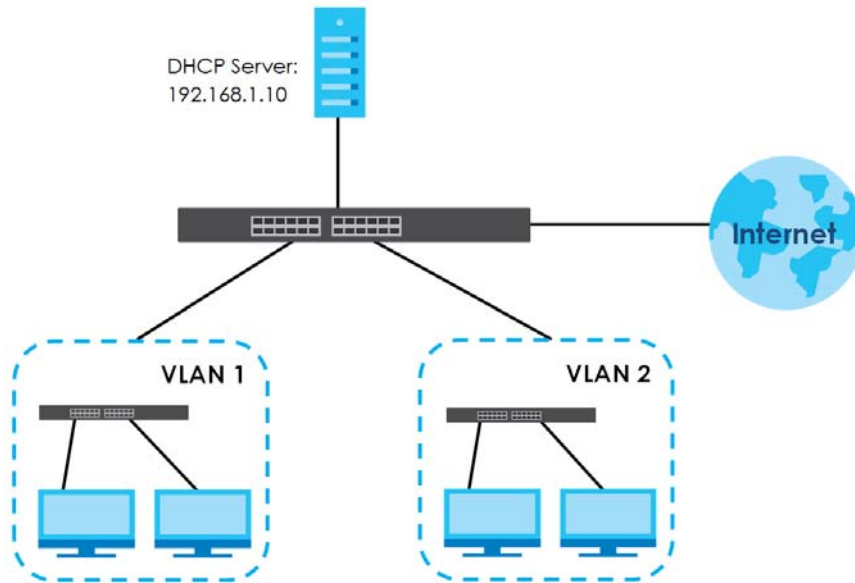
Table 139 IP Application > DHCP > DHCPv4 > Global > Port

LABEL	DESCRIPTION
Port	Enter the number of port(s) to which you want to apply the specified DHCP option 82 profile. You can enter multiple ports separated by (no space) comma (,) or hyphen (-). For 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 port(s). The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server. The profile you select here has priority over the one you select in the DHCP > DHCPv4 > Global screen.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values above based on the last selected entry or, if not applicable, to clear the fields above.
Clear	Click Clear to reset the fields to the factory defaults.
Index	This field displays a sequential number for each entry. Click an index number to change the settings.
Port	This field displays the port(s) to which the Switch applies the settings.
Profile Name	This field displays the DHCP option 82 profile that the Switch applies to the port(s).
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Select the entry(ies) that you want to remove, then click the Delete button to remove the selected entry(ies) from the table.
Cancel	Click this to clear the check boxes above.

33.4.5 Global DHCP Relay Configuration Example

The follow figure shows a network example where the Switch is used to relay DHCP requests for the VLAN1 and VLAN2 domains. There is only one DHCP server that services the DHCP clients in both domains.

Figure 191 Global DHCP Relay Network Example



Configure the **DHCP Relay** screen as shown. Make sure you select a DHCP option 82 profile (default1 in this example) to set the Switch to send additional information (such as the VLAN ID) together with the DHCP requests to the DHCP server. This allows the DHCP server to assign the appropriate IP address according to the VLAN ID.

Figure 192 DHCP Relay Configuration Example

DHCP Relay		Status	Port
Active	☒		
Remote DHCP Server 1	192.168.1.100		
Remote DHCP Server 2	0.0.0.0		
Remote DHCP Server 3	0.0.0.0		
Option 82 Profile	default1 ▼		

[Apply](#) [Cancel](#)
EXAMPLE

33.4.6 Configuring DHCP VLAN Settings

Use this screen to configure your DHCP settings based on the VLAN domain of the DHCP clients. Click **IP Application > DHCP > DHCPv4** in the navigation panel, then click the **VLAN** link in the **DHCP Status** screen that displays.

Note: You must set up a management IP address for each VLAN that you want to configure DHCP settings for on the Switch. See [Section 5.2 on page 66](#) for information on how to do this.

Figure 193 IP Application > DHCP > DHCPv4 > VLAN

VLAN Setting [Status](#) [Port](#)

VID:

Relay:

Remote DHCP Server 1:

Remote DHCP Server 2:

Remote DHCP Server 3:

Source Address:

Option 82 Profile:

[Add](#) [Cancel](#) [Clear](#)

VID	Type	DHCP Status	Source Address

[Delete](#) [Cancel](#)

The following table describes the labels in this screen.

Table 140 IP Application > DHCP > DHCPv4 > VLAN

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN to which these DHCP settings apply.
Relay	Use this section if you want to configure the Switch to function as a DHCP relay for this VLAN.
Remote DHCP Server 1 .. 3	Enter the IP address of a DHCP server in dotted decimal notation.
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.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to reset the fields to the factory defaults.
VID	This field displays the ID number of the VLAN group to which this DHCP settings apply.
Type	This field displays Relay for the DHCP mode.
DHCP Status	For DHCP server configuration, this field displays the starting IP address and the size of the IP address pool. For DHCP relay configuration, this field displays the first remote DHCP server IP address.
Source Address	This field displays the source IP address you configured for DHCP requests from clients on this VLAN.

Table 140 IP Application > DHCP > DHCPv4 > VLAN (continued)

LABEL	DESCRIPTION
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Select the configuration entries you want to remove and click Delete to remove them.
Cancel	Click Cancel to clear the check boxes.

33.4.7 DHCPv4 VLAN Port Configure

Use this screen to apply a different DHCP option 82 profile to certain ports in a VLAN. To open this screen, click IP Application > DHCP > DHCPv4 > VLAN > Port.

Figure 194 IP Application > DHCP > DHCPv4 > VLAN > Port

The following table describes the labels in this screen.

Table 141 IP Application > DHCP > DHCPv4 > VLAN > Port

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN you want to configure here.
Port	Enter the number of port(s) to which you want to apply the specified DHCP option 82 profile. You can enter multiple ports separated by (no space) comma (,) or hyphen (-). For 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 port(s) in this VLAN. The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server. The profile you select here has priority over the one you select in the DHCP > DHCPv4 > VLAN screen.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click this to reset the values above based on the last selected entry or, if not applicable, to clear the fields above.
Clear	Click Clear to reset the fields to the factory defaults.
Index	This field displays a sequential number for each entry. Click an index number to change the settings.
VID	This field displays the VLAN to which the port(s) belongs.

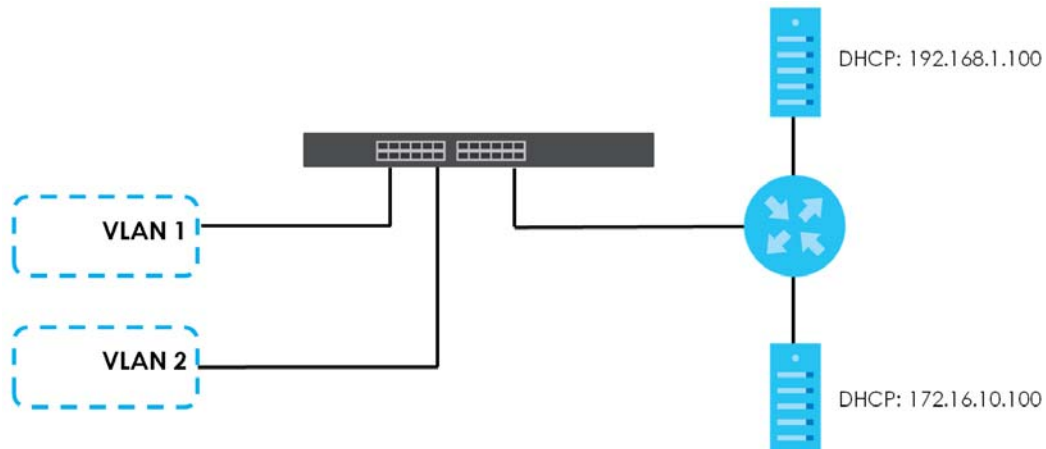
Table 141 IP Application > DHCP > DHCPv4 > VLAN > Port (continued)

LABEL	DESCRIPTION
Port	This field displays the port(s) to which the Switch applies the settings.
Profile Name	This field displays the DHCP option 82 profile that the Switch applies to the port(s) in this VLAN.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Select the entry(ies) that you want to remove, then click the Delete button to remove the selected entry(ies) from the table.
Cancel	Click this to clear the check boxes above.

33.4.8 Example: DHCP Relay for Two VLANs

The following example displays two VLANs (VIDs 1 and 2) for a campus network. Two DHCP servers are installed to serve each VLAN. The system is set up to forward DHCP requests from the dormitory rooms (VLAN 1) to the DHCP server with an IP address of 192.168.1.100. Requests from the academic buildings (VLAN 2) are sent to the other DHCP server with an IP address of 172.16.10.100.

Figure 195 DHCP Relay for Two VLANs



For the example network, configure the **VLAN Setting** screen as shown.

Figure 196 DHCP Relay for Two VLANs Configuration Example

VLAN Setting		Status	Port
VID	2		
Relay			
Remote DHCP Server 1	172.16.10.100		
Remote DHCP Server 2	0.0.0.0		
Remote DHCP Server 3	0.0.0.0		
Source Address	0.0.0.0		
Option 82 Profile			
Add Cancel Clear EXAMPLE			
VID	Type	DHCP Status	Source Address
Delete Cancel			

33.5 DHCPv6 Relay

A DHCPv6 relay agent is on the same network as the DHCPv6 clients and helps forward messages between the DHCPv6 server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCPv6 server on its network, it then needs a DHCPv6 relay agent to send a message to a DHCPv6 server that is not attached to the same network.

The DHCPv6 relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCPv6 server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Use this screen to configure DHCPv6 relay settings for a specific VLAN on the Switch. Click **IP Application > DHCP > DHCPv6** in the navigation panel to display the screen as shown.

Figure 197 IP Application > DHCP > DHCPv6

The following table describes the labels in this screen.

Table 142 IP Application > DHCP > DHCPv6

LABEL	DESCRIPTION
VID	Enter the ID number of the VLAN you want to configure here.
Helper Address	Enter the remote DHCPv6 server address for the specified VLAN.
Options	
Interface ID	Select this option to have the Switch add the interface-ID option in the DHCPv6 requests from the clients in the specified VLAN before the Switch forwards them to a DHCPv6 server.
Remote ID	Enter a string of up to 64 printable characters to be carried in the remote-ID option. The Switch adds the remote-ID option in the DHCPv6 requests from the clients in the specified VLAN before the Switch forwards them to a DHCPv6 server.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to their last saved values.

Table 142 IP Application > DHCP > DHCPv6 (continued)

LABEL	DESCRIPTION
Clear	Click Clear to reset the fields to the factory defaults.
VID	This field displays the VLAN ID number. Click the VLAN ID to change the settings.
Helper Address	This field displays the IPv6 address of the remote DHCPv6 server for this VLAN.
Interface ID	This field displays whether the interface-ID option is added to DHCPv6 requests from clients in this VLAN.
Remote ID	This field displays whether the remote-ID option is added to DHCPv6 requests from clients in this VLAN.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Check the entry(ies) that you want to remove and then click the Delete button.
Cancel	Click Cancel to clear the selected check boxes.

CHAPTER 34

ARP Setup

34.1 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.

34.1.1 What You Can Do

- Use the **ARP Learning** screen ([Section 34.2.1 on page 277](#)) to configure ARP learning mode on a per-port basis.
- Use the **Static ARP** screen ([Section 34.2.2 on page 278](#)) to create static ARP entries on the Switch.

34.1.2 What You Need to Know

Read on for concepts on ARP that can help you configure the screen in this chapter.

34.1.2.1 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.

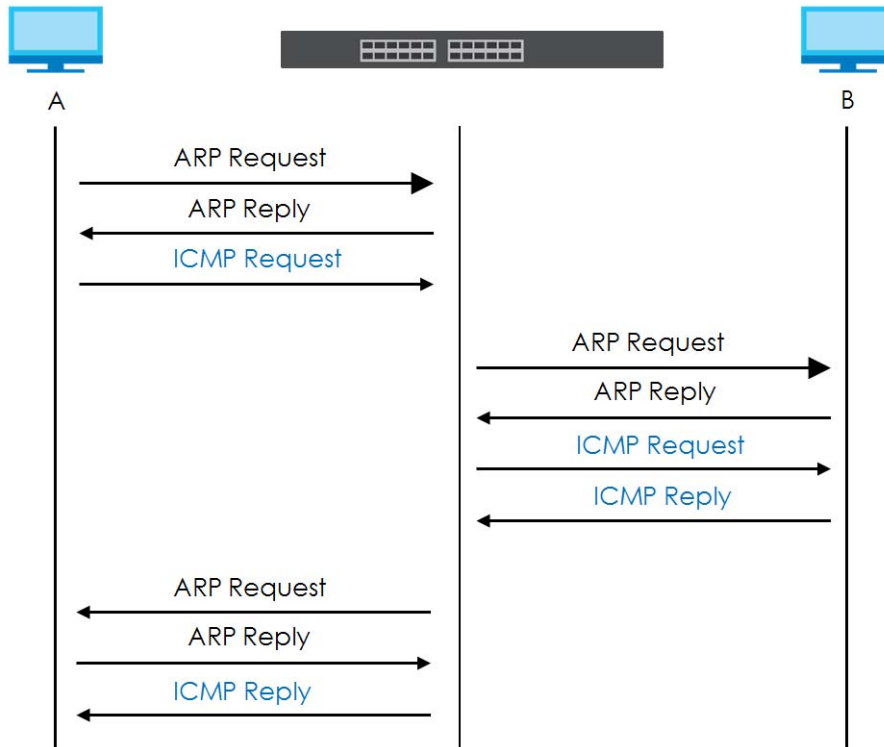
34.1.2.2 ARP Learning Mode

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.

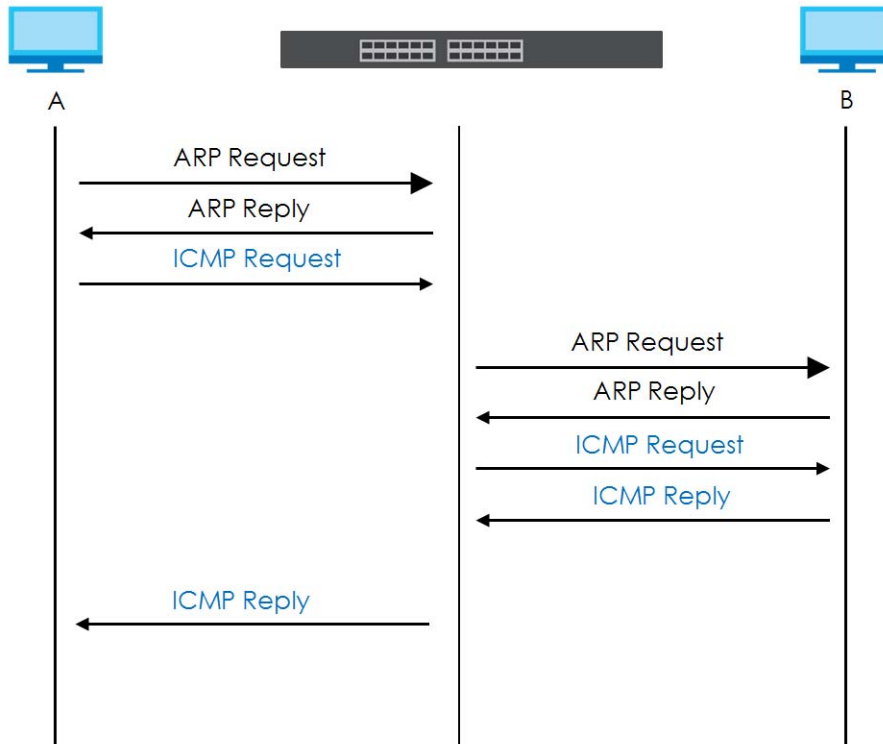
A device may send a gratuitous ARP packet to detect IP collisions. If a device restarts or its MAC address is changed, it can also use gratuitous ARP to inform other devices in the same network to update their ARP table with the new mapping information.

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.

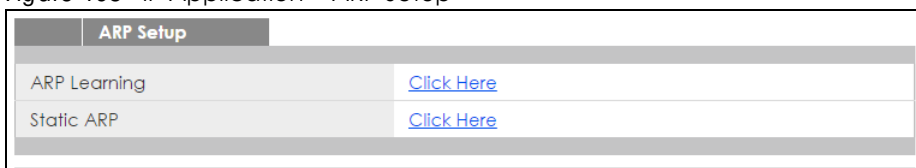
Therefore in the following example, the Switch can learn host A's MAC address from the ARP request sent by host A. The Switch then forwards host B's ICMP reply to host A right after getting host B's MAC address and ICMP reply.



34.2 ARP Setup

Click **IP Application > ARP Setup** in the navigation panel to display the screen as shown. Click the link next to **ARP Learning** to open a screen where you can set the ARP learning mode for each port. Click the link next to **Static ARP** to open a screen where you can create static ARP entries on the Switch.

Figure 198 IP Application > ARP Setup



34.2.1 ARP Learning

Use this screen to configure each port's ARP learning mode. Click the link next to **ARP Learning** in the **IP Application > ARP Setup** screen to display the screen as shown next.

Figure 199 IP Application > ARP Setup > ARP Learning

Port	ARP Learning Mode
*	ARP-Reply ▼
1	ARP-Reply ▼
2	ARP-Reply ▼
3	ARP-Reply ▼
4	ARP-Reply ▼
5	ARP-Reply ▼
6	ARP-Reply ▼
7	ARP-Reply ▼
8	ARP-Reply ▼
9	ARP-Reply ▼
10	ARP-Reply ▼
11	ARP-Reply ▼
12	ARP-Reply ▼

Apply Cancel

The following table describes the labels in this screen.

Table 143 IP Application > ARP Setup > ARP Learning

LABEL	DESCRIPTION
Port	This field displays the port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
ARP Learning Mode	Select the ARP learning mode the Switch uses on the port. Select ARP-Reply to have the Switch update the ARP table only with the ARP replies to the ARP requests sent by the Switch. Select Gratuitous-ARP to have the Switch update its ARP table with either an ARP reply or a gratuitous ARP request. Select ARP-Request to have the Switch update the ARP table with both ARP replies, gratuitous ARP requests and ARP requests.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

34.2.2 Static ARP

Use this screen to create static ARP entries that will display in the **Management > ARP Table** screen and will not age out. Click the link next to **Static ARP** in the **IP Application > ARP Setup** screen to display the screen as shown.

Figure 200 IP Application > ARP Setup > Static ARP

The screenshot shows the 'Static ARP' configuration interface. At the top, there's a header 'Static ARP' and a link 'ARP Setup'. The main form includes an 'Active' checkbox and input fields for 'Name', 'IP Address', 'MAC Address', 'VID', and 'Port'. Below these fields are three buttons: 'Add', 'Cancel', and 'Clear'. At the bottom of the screen, there is a table with columns: 'Index', 'Active', 'Name', 'IP Address', 'MAC Address', 'VID', 'Port', and a checkbox. Below the table are two buttons: 'Delete' and 'Cancel'.

The following table describes the related labels in this screen.

Table 144 IP Application > ARP Setup > Static ARP

LABEL	DESCRIPTION
Active	Select this check box to activate your rule. You may temporarily deactivate a rule without deleting it by clearing this check box.
Name	Enter a descriptive name (up to 32 printable ASCII characters) for identification purposes.
IP Address	Enter the IP address of a device connected to a Switch port with the corresponding MAC address below.
MAC Address	Enter the MAC address of the device with the corresponding IP address above.
VID	Enter the ID number of VLAN to which the device belongs.
Port	Enter the number of port to which the device connects.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to set the above fields back to the factory defaults.
Index	This field displays the index number of an entry. Click an index number to change the settings.
Active	This field displays Yes when the entry is activated and NO when it is deactivated.
Name	This field displays the descriptive name for this entry. This is for identification purposes only.
IP Address	This is the IP address of a device connected to a Switch port with the corresponding MAC address below.
MAC Address	This is the MAC address of the device with the corresponding IP address above.
VID	This field displays the VLAN to which the device belongs.
Port	This field displays the port to which the device connects.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to clear the check boxes.

CHAPTER 35

Maintenance

35.1 Overview

This chapter explains how to configure the screens that let you maintain the firmware and configuration files.

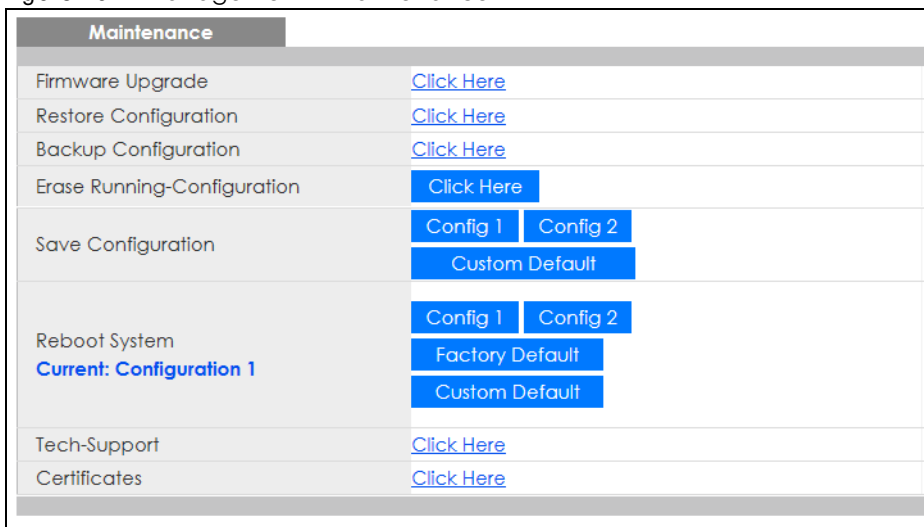
35.1.1 What You Can Do

- Use the Maintenance screen ([Section 35.2 on page 280](#)) to erase running configuration, save a configuration file or restart the Switch.
- Use the Firmware Upgrade screen ([Section 35.6 on page 284](#)) to upload the latest firmware.
- Use the Restore Configuration screen ([Section 35.7 on page 286](#)) to upload a stored device configuration file.
- Use the Backup Configuration screen ([Section 35.8 on page 286](#)) to save your configurations for later use.
- Use the Erase Running-Configuration screen ([Section 35.3 on page 282](#)) to reset the configuration to the Zyxel default configuration settings.
- Use the Save Configuration screen ([Section 35.4 on page 282](#)) to save the current configuration settings to a specific configuration file on the Switch.
- Use the Reboot System screen ([Section 35.5 on page 283](#)) to restart the Switch without physically turning the power off and load a specific configuration file.
- Use the Tech-Support screen ([Section 35.9 on page 287](#)) to create reports for customer support if there are problems with the Switch.
- Use the Certificates screen ([Section 35.10 on page 289](#)) to import the Switch's CA-signed certificates.

35.2 The Maintenance Screen

Use this screen to manage firmware and your configuration files. Click **Management > Maintenance** in the navigation panel to open the following screen.

Figure 201 Management > Maintenance



The following table describes the labels in this screen.

Table 145 Management > Maintenance

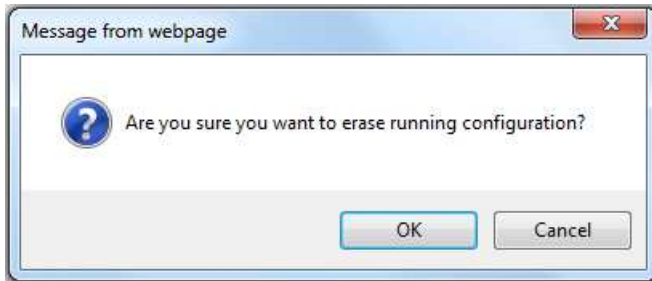
LABEL	DESCRIPTION
Firmware Upgrade	Click Click Here to go to the Firmware Upgrade screen.
Restore Configuration	Click Click Here to go to the Restore Configuration screen.
Backup Configuration	Click Click Here to go to the Backup Configuration screen.
Erase Running-Configuration	Click Click Here to reset the current configuration of the Switch. Note that this will not reset the configuration to the factory default settings.
Save Configuration	Click Config 1 to save the current configuration settings to Configuration 1 on the Switch. Click Config 2 to save the current configuration settings to Configuration 2 on the Switch. Click Custom Default to save the current configuration settings to a custom default file on the Switch.
Reboot System	Click Config 1 to reboot the system and load Configuration 1 on the Switch. Click Config 2 to reboot the system and load Configuration 2 on the Switch. Click Factory Default to reboot the system and load the default configuration settings on the Switch. Click Custom Default to reboot the system and load a saved custom default file on the Switch. This will save the custom default configuration settings to both Configuration 1 and Configuration 2 . If a custom default file was not saved, clicking Custom Default loads the factory default configuration on the Switch. Note: Make sure to click the Save button in any screen to save your settings to the current configuration on the Switch.
Current	This field displays which configuration (Configuration 1 or Configuration 2) is currently operating on the Switch.
Tech-Support	Click Click Here to see the Tech-Support screen. You can set CPU and memory thresholds for log reports and download related log reports for issue analysis. Log reports include CPU history and utilization, crash and memory.
Certificates	Click Click Here to see the Certificates screen and import the Switch's CA-signed certificates.

35.3 Erase Running-Configuration

Follow the steps below to clear current configuration on the Switch. Note that this will NOT reset the Switch back to its factory defaults. If you want to change the Switch to its factory default mode, click the **Factory Default** button in **Reboot System**.

- 1 In the **Maintenance** screen, click the **Click Here** button next to **Erase Running-Configuration** to clear all Switch configuration information you configured on the Switch.
- 2 Click **OK** to remove the running configuration on the Switch.

Figure 202 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).

35.4 Save Configuration

Click **Config 1** to save the current configuration settings permanently to configuration one on the Switch.

Click **Config 2** to save the current configuration settings permanently to configuration two on the Switch.

Click **Custom Default** to save the current configuration settings permanently to a custom default file on the Switch. If configuration changes cause the Switch to behave abnormally, click **Custom Default** (next to **Reboot System**) to have the Switch automatically reboot and restore the saved **Custom Default** configuration file.

Alternatively, click **Save** on the top right-hand corner in any screen to save the configuration changes to the current configuration.

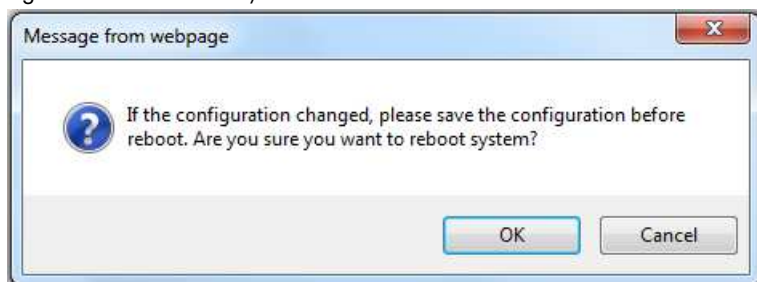
Note: Clicking the **Apply** or **Add** button does NOT save the changes permanently. All unsaved changes are erased after you reboot the Switch.

35.5 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 **Factory Default** when you reboot. Follow the steps below to reboot the Switch.

- 1 In the **Maintenance** screen, click a configuration button next to **Reboot System** to reboot and load that configuration file. The following screen displays.

Figure 203 Reboot System: Confirmation



- 2 Click **OK** again and then wait for the Switch to restart. This takes up to two minutes. This does not affect the Switch's configuration.

Click **Config 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 default configuration settings on the Switch.

Click **Custom Default** and follow steps 1 to 2 to reboot and load **Custom Default** configuration settings on the Switch. This will save the custom default configuration settings to both **Configuration 1** and **Configuration 2**.

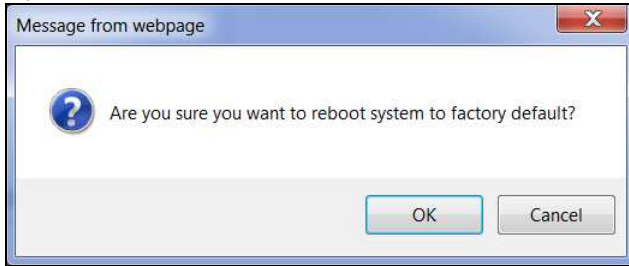
Note: If a customized default file was not saved, clicking **Custom Default** loads the factory default configuration on the Switch.

35.5.1 Factory Default

Follow the steps below to reset the Switch back to the factory defaults.

- 1 Click the **Factory Default** button.
- 2 Click **OK** to continue or **Cancel** to abort.

Figure 204 Load Factory Default: Confirmation



If you want to access the Switch web configurator again, you may need to change the IP address of your computer to be in the same subnet as that of the default Switch IP address (192.168.1.1 or DHCP-assigned IP).

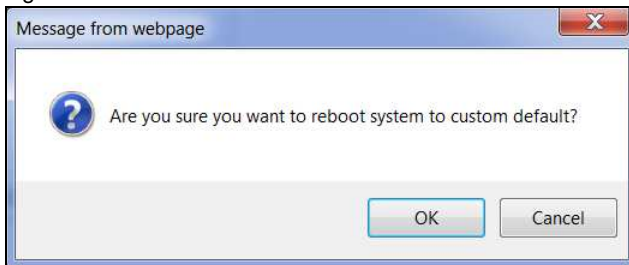
35.5.2 Custom Default

Follow the steps below to reset the Switch back to the Custom Default configuration file you created. This will save the custom default configuration settings to both Configuration 1 and Configuration 2.

- 1 Click the Custom Default button.
- 2 Click OK to continue or Cancel to abort.

Note: If you did not save a custom default file in the web configurator, then the factory default file is restored after you press click **Custom Default** (next to **Reboot System**) on the Switch. You will then have to make all your configurations again on the Switch.

Figure 205 Load Custom Default: Confirmation



35.6 Firmware Upgrade

The Switch supports dual firmware images, **Firmware 1** and **Firmware 2**. Use this screen to specify which image is updated when firmware is uploaded using the web configurator and to specify which image is loaded when the Switch starts up.

Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

Click **Management > Maintenance > Firmware Upgrade** to view the screen as shown next.

Figure 206 Management > Maintenance > Firmware Upgrade

Firmware Upgrade		Maintenance
Name	Version	
XS1930-12HP	Running	V4.60(ABQF.0)b4 07/09/2019
	Firmware 1	V4.60(ABQF.0)b4 07/09/2019
	Firmware 2	V4.60(ABQF.0)b3_console 06/21/2019

Current Boot Image	Firmware 1
Config Boot Image	Firmware 1 ▼

[Apply](#) [Cancel](#)

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

Firmware	1 ▼	File Path		Browse...

[Upgrade](#)

The top of firmware upgrade screen shows which firmware version is currently running on the Switch. Type the path and file name of the firmware file you wish to upload to the Switch in the **File Path** text box or click **Choose File** or **Browse** to locate it (Firmware upgrades are only applied after a reboot). Click **Upgrade** to load the new firmware.

After the firmware upgrade process is complete, see the **System Info** screen to verify your current firmware version number.

Table 146 Management > Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
Name	This is the name of the Switch that you're configuring.
Version	The Switch has two firmware sets, Firmware 1 and Firmware 2, residing in flash. Running shows the version number (and model code) and MM/DD/YYYY creation date of the firmware currently in use on the Switch (Firmware 1 or Firmware 2). The firmware information is also displayed at System Information in Basic Settings. Firmware 1 shows its version number (and model code) and MM/DD/YYYY creation date. Firmware 2 shows its version number (and model code) and MM/DD/YYYY creation date.
Current Boot Image	This displays which firmware is currently in use on the Switch (Firmware 1 or Firmware 2).
Config Boot Image	Select which firmware (Firmware 1 or Firmware 2) should load, 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 to (Firmware) 1 or (Firmware) 2.

Table 146 Management > Maintenance > Firmware Upgrade

LABEL	DESCRIPTION
File Path	Type the path and file name of the firmware file you wish to upload to the Switch in the File Path text box or click Choose File or Browse to locate it.
Upgrade	Click Upgrade to load the new firmware. Firmware upgrades are only applied after a reboot. To reboot, go to Management > Maintenance > Reboot System and click Config 1 , Config 2 or Factory Default (Config 1 , Config 2 and Factory Default are the configuration files you want the Switch to use when it restarts).

35.7 Restore Configuration

Use this screen to restore a previously saved configuration from your computer to the Switch.

Figure 207 Management > Maintenance > Restore Configuration

Type the path and file name of the configuration file you wish to restore in the **File Path** text box or click **Choose File** or **Browse** to locate it. After you have specified the file, click **Restore**. "config" is the name of the configuration file on the Switch, so your backup configuration file is automatically renamed when you restore using this screen.

35.8 Backup Configuration

Backing up your Switch configurations allows you to create various "snap shots" of your device from which you may restore at a later date.

Back up your current Switch configuration to a computer using the **Backup Configuration** screen.

Figure 208 Management > Maintenance > Backup Configuration

Follow the steps below to back up the current Switch configuration to your computer in this screen.

- 1 Select which Switch configuration file you want to download to your computer.
- 2 Click **Backup**.

- 3 If the current configuration file is open and/or downloaded to your computer automatically, you can click **File > Save As** to save the file to a specific place.

If a dialog box pops up asking whether you want to open or save the file, click **Save** or **Save File** to download it to the default downloads folder on your computer. If a **Save As** screen displays after you click **Save** or **Save File**, choose a location to save the file on your computer from the **Save in** drop-down list box and type a descriptive name for it in the **File name** list box. Click **Save** to save the configuration file to your computer.

35.9 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.

Click **Management > Maintenance > Tech-Support** to see the following screen.

Figure 209 Management > Maintenance > Tech-Support

Tech-Support		Maintenance
CPU	threshold 100 keep 5 seconds	
Mbuf	threshold 50 %	

[Apply](#)
[Cancel](#)

All	Download
Crash	Download
CPU history	Download
Memory section	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 147 Management > Maintenance > Tech-Support

LABEL	DESCRIPTION
CPU	Type a number ranging from 50 to 100 in the CPU threshold box, and type another number ranging from 5 to 60 in the seconds box then click Apply. For example, 80 for CPU threshold and 5 for seconds means a log will be created when CPU utilization reaches over 80% and lasts for 5 seconds. The log report holds 7 days of CPU log data and is stored in volatile memory (RAM). The data is lost if the Switch is turned off or in event of power outage. After 7 days, the logs wrap around and new ones and replace the earliest ones. The higher the CPU threshold number, the fewer logs will be created, and the less data technical support will have to analyze and vice versa.
Mbuf	Type a number ranging from 50 to 100 in the Mbuf (Memory Buffer) threshold box. The Mbuf log report is stored in flash (permanent) memory. For example, Mbuf 50 means a log will be created when the Mbuf utilization is over 50%. The higher the Mbuf threshold number, the fewer logs will be created, and the less data technical support will have to analyze and vice versa.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
All	Click Download to see all the log report and system status. This log report is stored in flash memory. If the All log report is too large, you can download the log reports separately below.
Crash	Click Download to see the crash log report. The log will include information of the last crash and is stored in flash memory.
CPU history	Click Download to see the CPU history log report. The 7-days log is stored in RAM and you will need to save it, otherwise it will be lost when the Switch is shutdown or during power outage.
Memory Section	Click Download to see the memory section log report. This log report is stored in flash memory.
Mbuf	Click Download to see the Mbuf log report. The log includes Mbuf over threshold information. This log report is stored in flash memory.
ROM	Click Download to see the Read Only Memory (ROM) log report. This report is stored in flash memory.
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.

35.9.1 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 210 Management > Maintenance > Tech-Support: Download

Tech-Support download

Downloading the tech-support file. Please wait for a moment.

[Back](#)

35.10 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 36.7.3 on page 307](#) for more information about HTTPS.

Certificates are based on public-private key pairs. A certificate contains the certificate owner's identity and public key. Certificates provide a way to exchange public keys for use in authentication.

Click **Management > Maintenance > Certificates** to open the following screen. Use this screen to import the Switch's CA-signed certificates.

Figure 211 Management > Maintenance > Certificates

Certificates [Maintenance](#)

Please specify the location of the HTTPS certificate file to be imported. The certificate file must be the Binary PKCS#12 format.

File Path [Browse...](#)

Password

[Import](#)

Service	Subject	Issuer	Valid From	Valid To	☐
HTTPS	/CN=XS1930 0019cb000001	/CN=XS1930 0019cb000001	Jan 1 00:00:56 2016 GMT	Mar 26 00:00:56 2076 GMT	☐

[Delete](#)

The following table describes the labels in this screen.

Table 148 Management > Maintenance > Certificates

LABEL	DESCRIPTION
File Path	Click Choose File or Browse to find the certificate file you want to upload.
Password	Type the certificate file's password that was created when the PKCS #12 file was exported. The password consists of up to 32 ASCII characters.
Import	Click this button to save the certificate that you have enrolled from a certification authority from your computer to the Switch.
Service	This field displays the service type that this certificate is for.
Subject	This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information.

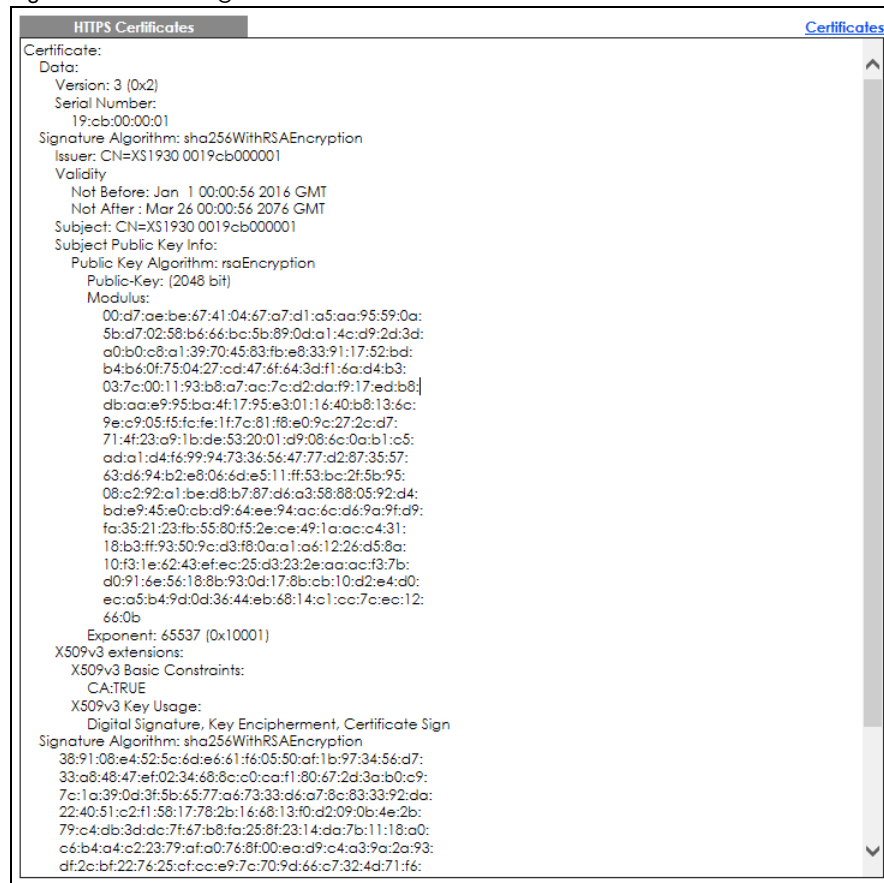
Table 148 Management > Maintenance > Certificates

LABEL	DESCRIPTION
Issuer	This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country.
Valid From	This field displays the date that the certificate becomes applicable.
Valid To	This field displays the date that the certificate expires.
	Select an entry's check box to select a specific entry.
Delete	Click this button to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use.

35.10.1 HTTPS Certificates

Use this screen to view the HTTPS certificate details. Click a hyperlink in the **Service** column in the **Management > Maintenance > Certificates** screen to open the following screen.

Figure 212 Management > Maintenance > Certificates > HTTPS



35.11 Technical Reference

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

35.11.1 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.

35.11.2 Filename Conventions

The configuration file (also known as the romfile or ROM) contains the factory default settings in the screens such as password, Switch setup, IP Setup, and so on. Once you have custom the Switch's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (Zyxel Network Operating System sometimes referred to as the "ras" file) is the system firmware and has a "bin" filename extension.

Table 149 Filename Conventions

FILE TYPE	INTERNAL NAME	EXTERNAL NAME	DESCRIPTION
Configuration File	config	*.cfg	This is the configuration filename on the Switch. Uploading the config file replaces the specified configuration file system, including your Switch configurations, system-related data (including the default password), the error log and the trace log.
Firmware	ras	*.bin	This is the generic name for the ZyNOS firmware on the Switch.

35.11.2.1 Example FTP Commands

```
ftp> put firmware.bin ras
```

This is a sample FTP session showing the transfer of the computer file "firmware.bin" to the Switch.

```
ftp> get config config.cfg
```

This is a sample FTP session saving the current configuration to a file called "config.cfg" on your computer.

If your (T)FTP client does not allow you to have a destination filename different than the source, you will need to rename them as the Switch only recognizes "config" and "ras". Be sure you keep unaltered copies of both files for later use.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

35.11.3 FTP Command Line Procedure

- 1 Launch the FTP client on your computer.
- 2 Enter open, followed by a space and the IP address of your Switch.

- 3 Press [ENTER] when prompted for a username.
- 4 Enter your password as requested (the default is "1234").
- 5 Enter `bin` to set transfer mode to binary.
- 6 Use `put` to transfer files from the computer to the Switch, for example, `put firmware.bin ras` transfers the firmware on your computer (`firmware.bin`) to the Switch and renames it to "ras". Similarly, `put config.cfg config` transfers the configuration file on your computer (`config.cfg`) to the Switch and renames it to "config". Likewise `get config config` transfers the configuration file on the Switch to your computer and renames it to "config.cfg". See [Table 149 on page 291](#) for more information on filename conventions.
- 7 Enter `quit` to exit the ftp prompt.

35.11.4 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

General Commands for GUI-based FTP Clients

COMMAND	DESCRIPTION
Host Address	Enter the address of the host server.
Login Type	Anonymous. This is when a user I.D. and password is automatically supplied to the server for anonymous access. Anonymous logins will work only if your ISP or service administrator has enabled this option. Normal. The server requires a unique User ID and Password to login.
Transfer Type	Transfer files in either ASCII (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode.
Initial Remote Directory	Specify the default remote directory (path).
Initial Local Directory	Specify the default local directory (path).

35.11.5 FTP Restrictions

FTP will not work when:

- FTP service is disabled in the **Service Access Control** screen.
- The IP address(es) in the **Remote Management** screen does not match the client IP address. If it does not match, the Switch will disconnect the FTP session immediately.

CHAPTER 36

Access Control

36.1 Access Control Overview

This chapter describes how to control access to the Switch.

FTP is allowed one session. 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 150 Access Control Overview

SSH	Telnet	FTP	Web	SNMP
Share up to nine sessions		One session	Up to five accounts	No limit

36.1.1 What You Can Do

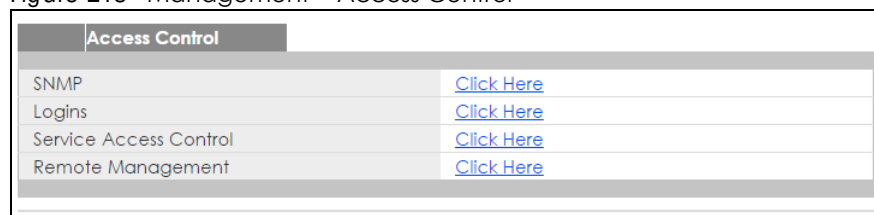
- Use the **Access Control** screen ([Section 36.2 on page 293](#)) to display the main screen.
- Use the **SNMP** screen ([Section 36.3 on page 294](#)) to configure your SNMP settings.
- Use the **Trap Group** screen ([Section 36.3.1 on page 295](#)) to specify the types of SNMP traps that should be sent to each SNMP manager.
- Use the **User Information** screen ([Section 36.3.3 on page 297](#)) to create SNMP users for authentication with managers using SNMP v3 and associate them to SNMP groups.
- Use the **Logins** screens ([Section 36.4 on page 299](#)) to assign which users can access the Switch via web configurator at any one time.
- Use the **Service Access Control** screen ([Section 36.5 on page 300](#)) to decide what services you may use to access the Switch.
- Use the **Remote Management** screen ([Section 36.6 on page 301](#)) to specify a group of one or more "trusted computers" from which an administrator may use a service to manage the Switch.

36.2 The Access Control Main Screen

Use this screen to display the main screen.

Click **Management > Access Control** in the navigation panel to display the main screen as shown.

Figure 213 Management > Access Control



Access Control	
SNMP	Click Here
Logins	Click Here
Service Access Control	Click Here
Remote Management	Click Here

The following table describes the labels in this screen.

Table 151 Management > Access Control

LABEL	DESCRIPTION
SNMP	Click this link to configure your SNMP settings.
Logins	Click this link to assign which users can access the Switch via web configurator at any one time.
Service Access Control	Click this link to decide what services you may use to access the Switch.
Remote Management	Click this link to specify a group of one or more "trusted computers" from which an administrator may use a service to manage the Switch.

36.3 Configuring SNMP

Use this screen to configure your SNMP settings.

Click **Management > Access Control > SNMP** to view the screen as shown.

Figure 214 Management > Access Control > SNMP

SNMP [Access Control](#) [Trap Group](#) [User](#)

General Setting

Version	v2c ▼
Get Community	public
Set Community	public
Trap Community	public

Trap Destination

Version	IP	Port	Username
v2c ▼	0.0.0.0	162	
v2c ▼	0.0.0.0	162	
v2c ▼	0.0.0.0	162	
v2c ▼	0.0.0.0	162	

[Apply](#) [Cancel](#)

The following table describes the labels in this screen.

Table 152 Management > Access Control > SNMP

LABEL	DESCRIPTION
General Setting	Use this section to specify the SNMP version and community (password) values.
Version	Select the SNMP version for the Switch. The SNMP version on the Switch must match the version on the SNMP manager. Choose SNMP version 2c (v2c), SNMP version 3 (v3) or both (v3v2c). SNMP version 2c is backwards compatible with SNMP version 1.

Table 152 Management > Access Control > SNMP (continued)

LABEL	DESCRIPTION
Get Community	Enter the Get Community string, which is the password for the incoming Get- and GetNext-requests from the management station. The Get Community string is only used by SNMP managers using SNMP version 2c or lower.
Set Community	Enter the Set Community , which is the password for incoming Set- requests from the management station. The Set Community string is only used by SNMP managers using SNMP version 2c or lower.
Trap Community	Enter the Trap Community string, which is the password sent with each trap to the SNMP manager. The Trap Community string is only used by SNMP managers using SNMP version 2c or lower.
Trap Destination	Use this section to configure where to send SNMP traps from the Switch.
Version	Specify the version of the SNMP trap messages.
IP	Enter the IP addresses of up to four managers to send your SNMP traps to.
Port	Enter the port number upon which the manager listens for SNMP traps.
Username	Enter the username to be sent to the SNMP manager along with the SNMP v3 trap. This username must match an existing account on the Switch (configured in Management > Access Control > Logins 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.

36.3.1 Configuring SNMP Trap Group

From the **SNMP** screen, click **Trap Group** to view the screen as shown. Use the **Trap Group** screen to specify the types of SNMP traps that should be sent to each SNMP manager.

Figure 215 Management > Access Control > SNMP > Trap Group

Type	Options
System	☐ * ☐ coldstart ☐ warmstart ☐ poe ☐ custom-ca
Interface	☐ * ☐ linkup ☐ linkdown ☐ lldp
AAA	☐ * ☐ authentication
IP	☐ * ☐ ping ☐ traceroute
Switch	☐ * ☐ stp ☐ rmon

The following table describes the labels in this screen.

Table 153 Management > Access Control > SNMP > Trap Group

LABEL	DESCRIPTION
Trap Destination IP	Select one of your configured trap destination IP addresses. These are the IP addresses of the SNMP managers. You must first configure a trap destination IP address in the SNMP Setting screen. Use the rest of the screen to select which traps the Switch sends to that SNMP manager.
Type	Select the categories of SNMP traps that the Switch is to send to the SNMP manager.
Options	Select the individual SNMP traps that the Switch is to send to the SNMP station. See SNMP Traps on page 304 for individual trap descriptions. The traps are grouped by category. Selecting a category automatically selects all of the category's traps. Clear the check boxes for individual traps that you do not want the Switch to send to the SNMP station. Clearing a category's check box automatically clears all of the category's trap check boxes (the Switch only sends traps from selected categories).
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

36.3.2 Enabling/Disabling Sending of SNMP Traps on a Port

From the **SNMP > Trap Group** screen, click **Port** to view the screen as shown. Use this screen to set whether a trap received on the port(s) would be sent to the SNMP manager.

Figure 216 Management > Access Control > SNMP > Trap Group > Port

Port [Trap Group](#)

Option: poe ▼

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

Apply
Cancel

The following table describes the labels in this screen.

Table 154 Management > Access Control > SNMP > Trap Group > Port

LABEL	DESCRIPTION
Option	Select the trap type you want to configure here.
Port	This field displays a port number.
*	Settings in this row apply to all ports. Use this row only if you want to make some of the settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them.
Active	Select this check box to enable the trap type of SNMP traps on this port. Clear this check box to disable the sending of SNMP traps on this port.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

36.3.3 Configuring SNMP User

From the **SNMP** screen, click **User** to view the screen as shown. Use the **User** screen to create SNMP users for authentication with managers using SNMP v3 and associate them to SNMP groups. An SNMP user is an SNMP manager.

Figure 217 Management > Access Control > SNMP > User

The following table describes the labels in this screen.

Table 155 Management > Access Control > SNMP > User

LABEL	DESCRIPTION
User Information	Note: Use the username and password of the login accounts you specify in this screen to create accounts on the SNMP v3 manager.
Username	Specify the username of a login account on the Switch.

Table 155 Management > Access Control > SNMP > User (continued)

LABEL	DESCRIPTION
Security Level	Select whether you want to implement authentication and/or encryption for SNMP communication from this user. Choose: noauth -to use the username as the password string to send to the SNMP manager. This is equivalent to the Get, Set and Trap Community in SNMP v2c. This is the lowest security level. auth - to implement an authentication algorithm for SNMP messages sent by this user. priv - to implement authentication and encryption for SNMP messages sent by this user. This is the highest security level. Note: The settings on the SNMP manager must be set at the same security level or higher than the security level settings on the Switch.
Authentication	Select an authentication algorithm. MD5 (Message Digest 5) and SHA (Secure Hash Algorithm) are hash algorithms used to authenticate SNMP data. SHA authentication is generally considered stronger than MD5, but is slower.
Password	Enter the password of up to 32 ASCII characters for SNMP user authentication.
Privacy	Specify the encryption method for SNMP communication from this user. You can choose one of the following: DES - Data Encryption Standard is a widely used (but breakable) method of data encryption. It applies a 56-bit key to each 64-bit block of data. AES - Advanced Encryption Standard is another method for data encryption that also uses a secret key. AES applies a 128-bit key to 128-bit blocks of data.
Password	Enter the password of up to 32 ASCII characters for encrypting SNMP packets.
Group	SNMP v3 adopts the concept of View-based Access Control Model (VACM) group. SNMP managers in one group are assigned common access rights to MIBs. Specify in which SNMP group this user is. admin - Members of this group can perform all types of system configuration, including the management of administrator accounts. readwrite - Members of this group have read and write rights, meaning that the user can create and edit the MIBs on the Switch, except the user account and AAA configuration. readonly - Members of this group have read rights only, meaning the user can collect information from the Switch.
Add	Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to reset the fields to your previous configuration.
Clear	Click Clear to reset the fields to the factory defaults.
Index	This is a read-only number identifying a login account on the Switch. Click on an index number to view more details and edit an existing account.
Username	This field displays the username of a login account on the Switch.
Security Level	This field displays whether you want to implement authentication and/or encryption for SNMP communication with this user.
Authentication	This field displays the authentication algorithm used for SNMP communication with this user.
Privacy	This field displays the encryption method used for SNMP communication with this user.
Group	This field displays the SNMP group to which this user belongs.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click Delete to remove the selected entry from the summary table.
Cancel	Click Cancel to begin configuring this screen afresh.

36.4 Logins

Up to five people (one administrator and four non-administrators) may access the Switch via web configurator at any one time.

- An administrator is someone who can both view and configure Switch changes. The username for the Administrator is always admin. The default administrator password is 1234.

Note: It is highly recommended that you change the default administrator password (1234).

- A non-administrator (username is something other than admin) is someone who can view and/or configure Switch settings. The configuration right varies depending on the user's privilege level.

Click **Management > Access Control > Logins** to view the screen as shown.

Figure 218 Management > Access Control > Logins

Logins [Access Control](#)

Administrator

Old Password		
New Password		
Retype to confirm		

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

Edit Logins

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

Apply **Cancel**

The following table describes the labels in this screen.

Table 156 Management > Access Control > Logins

LABEL	DESCRIPTION
Administrator	This is the default administrator account with the "admin" user name. You cannot change the default administrator user name.
Old Password	Type the existing system password (1234 is the default password when shipped).
New Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation.
Edit Logins	You may configure passwords for up to four users. These users can have read-only or read/write access. You can give users higher privileges via the web configurator.

Table 156 Management > Access Control > Logins (continued)

LABEL	DESCRIPTION
User Name	Set a user name (up to 32 ASCII characters long).
Password	Enter your new system password.
Retype to confirm	Retype your new system password for confirmation.
Privilege	Type the privilege level for this user. At the time of writing, users may have a privilege level of 0, 3, 13, or 14 representing different configuration rights as shown below. 0 - Display basic system information. 3 - Display configuration or status. 13 - Configure features except for login accounts, SNMP user accounts, the authentication method sequence and authorization settings, multiple logins, administrator and enable passwords, and configuration information display. 14 - Configure login accounts, SNMP user accounts, the authentication method sequence and authorization settings, multiple logins, and administrator and enable passwords, and display configuration information. Users can run command lines if the session's privilege level is greater than or equal to the command's privilege level. The session privilege initially comes from the privilege of the login account. For example, if the user has a privilege of 5, he/she can run commands that requires privilege level of 5 or less but not more.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

36.5 Service Access Control

Service Access Control allows you to decide what services you may use to access the Switch. You may also change the default service port and configure "trusted computer(s)" for each service in the **Remote Management** screen (discussed later). Click **Access Control** to go back to the main **Access Control** screen.

Figure 219 Management > Access Control > Service Access Control

Service Access Control				Access Control	
Services	Active	Service Port	Timeout		Login Timeout
Telnet	☒	23	5	Minutes	150 Seconds
SSH	☒	22			
FTP	☒	21	5	Minutes	
HTTP	☒	80	5	Minutes	
HTTPS	☒	443			
ICMP	☒				
SNMP	☒				

Apply Cancel

The following table describes the fields in this screen.

Table 157 Management > Access Control > Service Access Control

LABEL	DESCRIPTION
Services	Services you may use to access the Switch are listed here.
Active	Select this option for the corresponding services that you want to allow to access the Switch.
Service Port	For Telnet, SSH, FTP, HTTP or HTTPS services, you may change the default service port by typing the new port number in the Service Port field. If you change the default port number then you will have to let people (who wish to use the service) know the new port number for that service.
Timeout	Type how many minutes (from 1 to 255) a management session can be left idle before the session times out. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. Note: The timeout period you specified for Telnet sessions also applies to SSH sessions. Likewise, the HTTP and HTTPS sessions are set to use the same timeout value.
Login Timeout	Type how many seconds (from 30 to 300) the Switch waits before stopping a "trusted" computer's failed attempt to log in and access the Switch. Note: The login timeout period you specified for Telnet sessions also applies to SSH sessions.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

36.6 Remote Management

Use this screen to specify a group of one or more "trusted computers" from which an administrator may use a service to manage the Switch.

Click **Management > Access Control > Remote Management** to view the screen as shown next.

You can specify a group of one or more "trusted computers" from which an administrator may use a service to manage the Switch. Click **Access Control** to return to the **Access Control** screen.

Figure 220 Management > Access Control > Remote Management

Entry	Active	Start Address	End Address	Telnet	FTP	HTTP	ICMP	SNMP	SSH	HTTPS
1	☒	0.0.0.0	0.0.0.0	☒	☒	☒	☒	☒	☒	☒
2	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
3	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
4	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
5	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
6	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
7	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
8	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
9	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
10	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
11	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
12	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
13	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
14	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
15	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐
16	☐	0.0.0.0	0.0.0.0	☐	☐	☐	☐	☐	☐	☐

Apply Cancel

The following table describes the labels in this screen.

Table 158 Management > Access Control > Remote Management

LABEL	DESCRIPTION
Entry	This is the client set index number. A "client set" is a group of one or more "trusted computers" from which an administrator may use a service to manage the Switch.
Active	Select this check box to activate this secured client set. Clear the check box if you wish to temporarily disable the set without deleting it.
Start Address	Configure the IP address range of trusted computers from which you can manage this Switch.
End Address	The Switch checks if the client IP address of a computer requesting a service or protocol matches the range set here. The Switch immediately disconnects the session if it does not match.
Telnet/FTP/HTTP/ICMP/SNMP/SSH/HTTPS	Select services that may be used for managing the Switch from the specified trusted computers.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

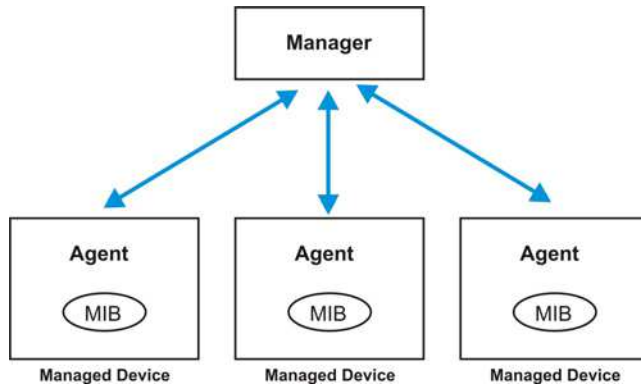
36.7 Technical Reference

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

36.7.1 About SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol used to manage and monitor TCP/IP-based devices. SNMP is used to exchange management information between the network management system (NMS) and a network element (NE). A manager station can manage and monitor the Switch through the network via SNMP version 1 (SNMPv1), SNMP version 2c or SNMP version 3. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 221 SNMP Management Model



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

An agent is a management software module that resides in a managed Switch (the Switch). An agent translates the local management information from the managed Switch into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

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

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

Table 159 SNMP Commands

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

SNMP v3 and Security

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

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

Supported MIBs

MIBs let administrators collect statistics and monitor status and performance.

The Switch supports the following MIBs:

- SNMP MIB II (RFC 1213)
- RFC 1157 SNMP v1
- RFC 1493 Bridge MIBs
- RFC 1643 Ethernet MIBs
- RFC 1155 SMI
- RFC 2674 SNMPv2, SNMPv2c
- RFC 1757 RMON
- SNMPv2, SNMPv2c or later version, compliant with RFC 2011 SNMPv2 MIB for IP, RFC 2012 SNMPv2 MIB for TCP, RFC 2013 SNMPv2 MIB for UDP

SNMP Traps

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

Table 160 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.
poe (For PoE models only)	pethPsePortOnOffNotification	1.3.6.1.2.1.105.0.1	This trap is sent when the PoE port delivers power or delivers no power to a PD.
	pethMainPowerUsageOnNotification	1.3.6.1.2.1.105.0.2	This trap is sent when the usage power is above the usage indication threshold.
	pethMainPowerUsageOffNotification	1.3.6.1.2.1.105.0.3	This trap is sent when the usage power is below the usage indication threshold.

Table 161 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.

Table 161 SNMP Interface Traps (continued)

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
linkdown	linkDown	1.3.6.1.6.3.1.1.5.3	This trap is sent when the Ethernet link is down.
lldp	lldpRemTablesChange	1.0.8802.1.1.2.0.0.1	The trap is sent when entries in the remote database have any updates. Link Layer Discovery Protocol (LLDP), defined as IEEE 802.1ab, enables LAN devices that support LLDP to exchange their configured settings. This helps eliminate configuration mismatch issues.

Table 162 SNMP AAA Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
authentication	authenticationFailure	1.3.6.1.6.3.1.1.5.5	This trap is sent when authentication fails due to incorrect user name and/or password.

Table 163 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 164 SNMP Switch Traps

OPTION	OBJECT LABEL	OBJECT ID	DESCRIPTION
stp	STPNewRoot	1.3.6.1.2.1.17.0.1	This trap is sent when the STP root switch changes.
	STPTopologyChange	1.3.6.1.2.1.17.0.2	This trap is sent when the STP topology changes.
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.

36.7.2 SSH Overview

Unlike Telnet or FTP, which transmit data in clear text, SSH (Secure Shell) is a secure communication protocol that combines authentication and data encryption to provide secure encrypted communication between two hosts over an unsecured network.

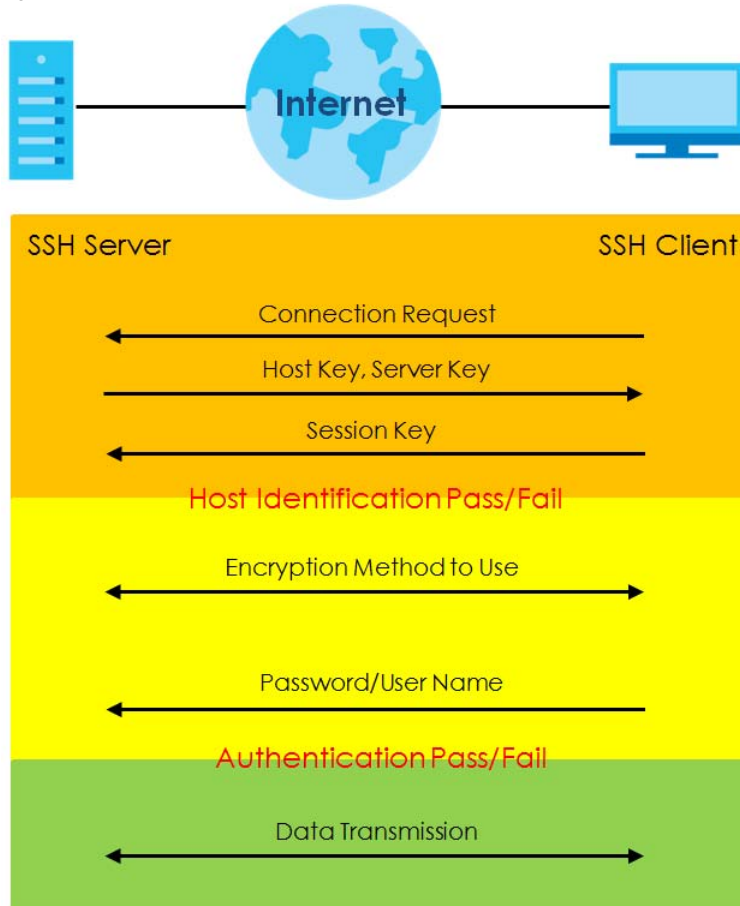
Figure 222 SSH Communication Example



36.7.2.1 How SSH works

The following table summarizes how a secure connection is established between two remote hosts.

Figure 223 How SSH Works



1 Host Identification

The SSH client sends a connection request to the SSH server. The server identifies itself with a host key. The client encrypts a randomly generated session key with the host key and server key and sends the result back to the server.

The client automatically saves any new server public keys. In subsequent connections, the server public key is checked against the saved version on the client computer.

2 Encryption Method

Once the identification is verified, both the client and server must agree on the type of encryption method to use.

3 Authentication and Data Transmission

After the identification is verified and data encryption activated, a secure tunnel is established between the client and the server. The client then sends its authentication information (user name and password) to the server to log in to the server.

36.7.2.2 SSH Implementation on the Switch

Your Switch supports SSH version 2 using RSA authentication and three encryption methods (DES, 3DES and Blowfish). The SSH server is implemented on the Switch for remote management and file transfer on port 22. Only one SSH connection is allowed at a time.

36.7.2.3 Requirements for Using SSH

You must install an SSH client program on a client computer (Windows or Linux operating system) that is used to connect to the Switch over SSH.

36.7.3 Introduction to HTTPS

HTTPS (HyperText Transfer Protocol over Secure Socket Layer, or HTTP over SSL) is a web protocol that encrypts and decrypts web pages. Secure Socket Layer (SSL) is an application-level protocol that enables secure transactions of data by ensuring confidentiality (an unauthorized party cannot read the transferred data), authentication (one party can identify the other party) and data integrity (you know if data has been changed).

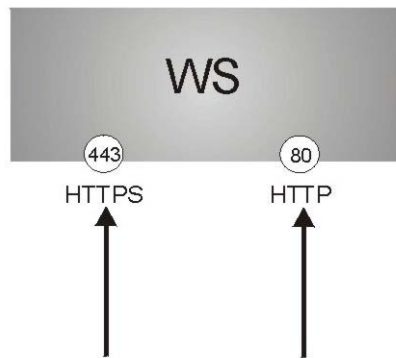
It relies upon certificates, public keys, and private keys.

HTTPS on the Switch is used so that you may securely access the Switch using the web configurator. The SSL protocol specifies that the SSL server (the Switch) must always authenticate itself to the SSL client (the computer which requests the HTTPS connection with the Switch), whereas the SSL client only should authenticate itself when the SSL server requires it to do so. Authenticating client certificates is optional and if selected means the SSL-client must send the Switch a certificate. You must apply for a certificate for the browser from a Certificate Authority (CA) that is a trusted CA on the Switch.

Please refer to the following figure.

- 1** HTTPS connection requests from an SSL-aware web browser go to port 443 (by default) on the Switch's WS (web server).
- 2** HTTP connection requests from a web browser go to port 80 (by default) on the Switch's WS (web server).

Figure 224 HTTPS Implementation



Note: If you disable HTTP in the Service Access Control screen, then the Switch blocks all HTTP connection attempts.

36.7.3.1 HTTPS Example

If you haven't changed the default HTTPS port on the Switch, then in your browser enter "https://Switch IP Address/" as the web site address where "Switch IP Address" is the IP address or domain name of the Switch you wish to access.

Internet Explorer Warning Messages

Internet Explorer 6

When you attempt to access the Switch HTTPS server, a Windows dialog box pops up asking if you trust the server certificate.

You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the web configurator login screen; if you select **No**, then web configurator access is blocked.

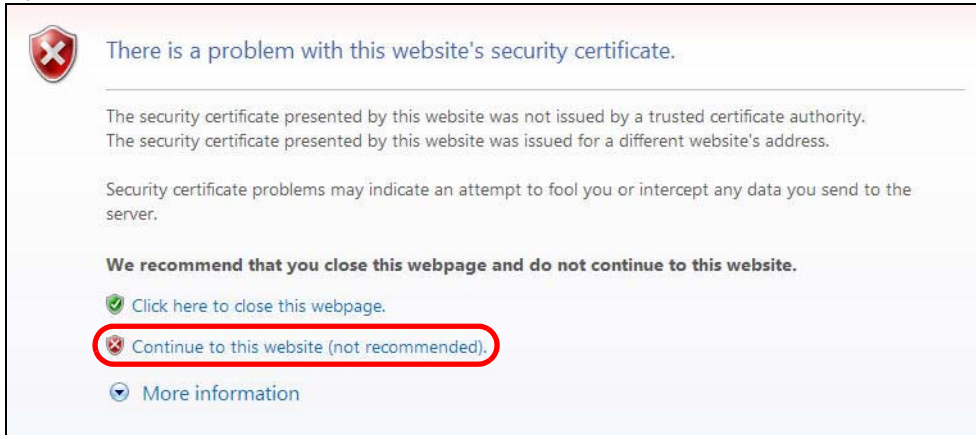
Figure 225 Security Alert Dialog Box (Internet Explorer 6)



Internet Explorer 7 later version

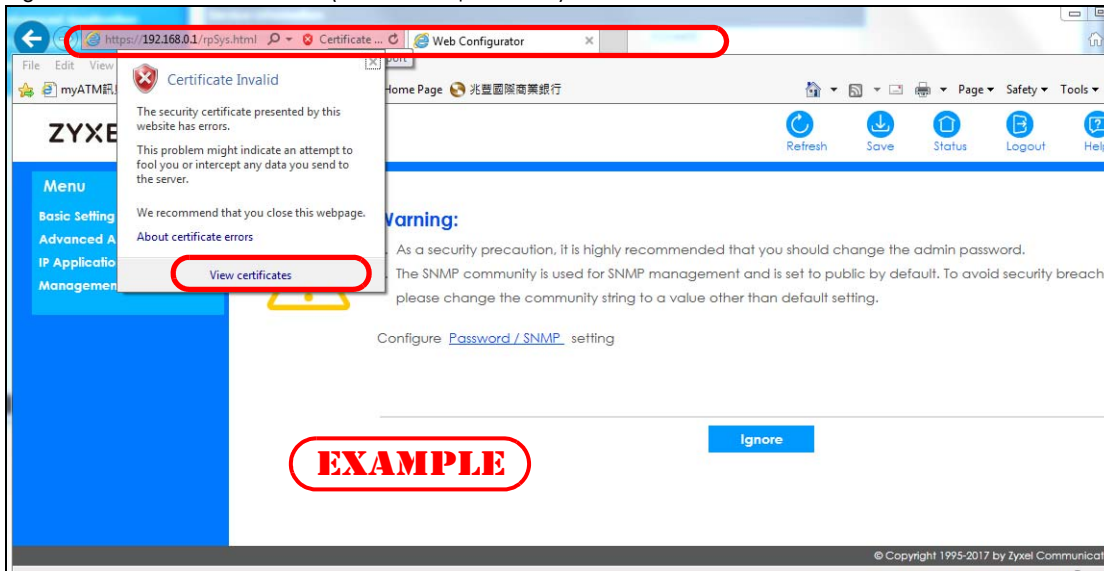
When you attempt to access the Switch HTTPS server, a screen with the message "There is a problem with this website's security certificate." may display. If that is the case, click **Continue to this website** (not recommended) to proceed to the web configurator login screen.

Figure 226 Security Certificate Warning (Internet Explorer 11)



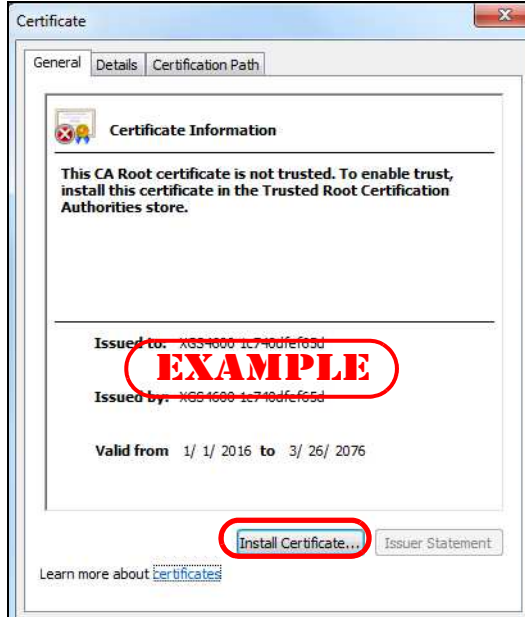
After you log in, you will see the red address bar with the message **Certificate Error**. Click on **Certificate Error** next to the address bar and click **View certificates**.

Figure 227 Certificate Error (Internet Explorer 11)



Click **Install Certificate...** and follow the on-screen instructions to install the certificate in your browser.

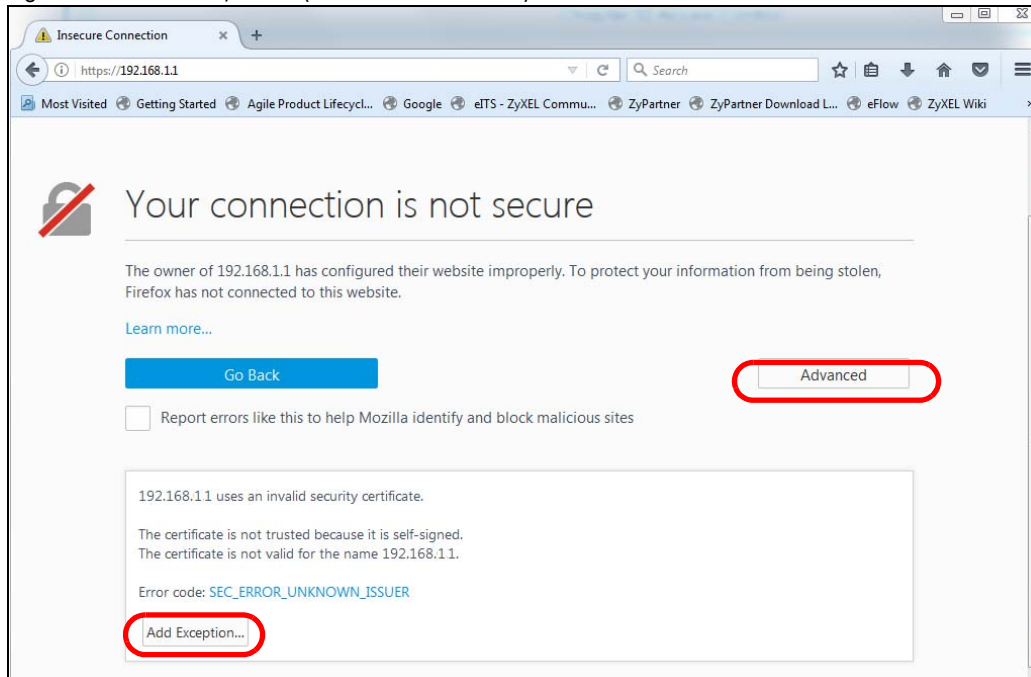
Figure 228 Certificate (Internet Explorer 11)



Mozilla Firefox Warning Messages

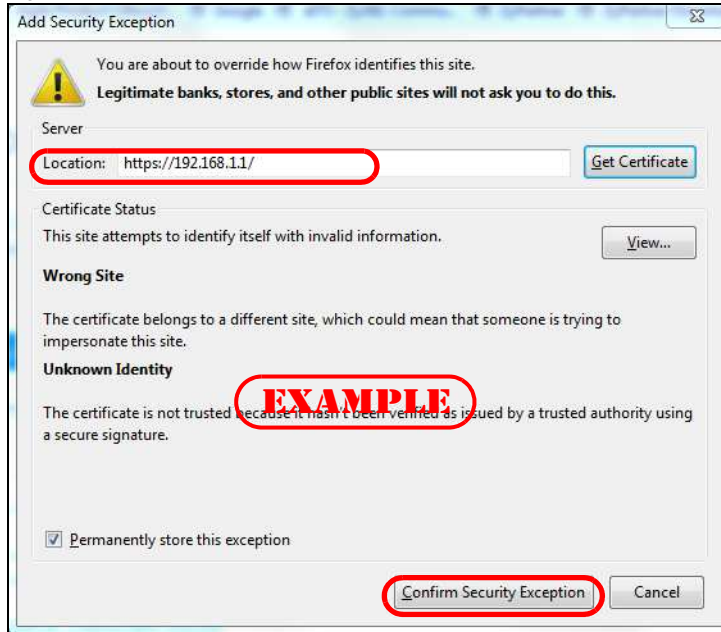
When you attempt to access the Switch HTTPS server, a **This Connection is Unstructured** or **Your connection is not secure** screen may display. If that is the case, click **I Understand the Risks** or **Advanced** and then the **Add Exception...** button.

Figure 229 Security Alert (Mozilla Firefox 53.0)



Confirm the HTTPS server URL matches. Click **Confirm Security Exception** to proceed to the web configurator login screen.

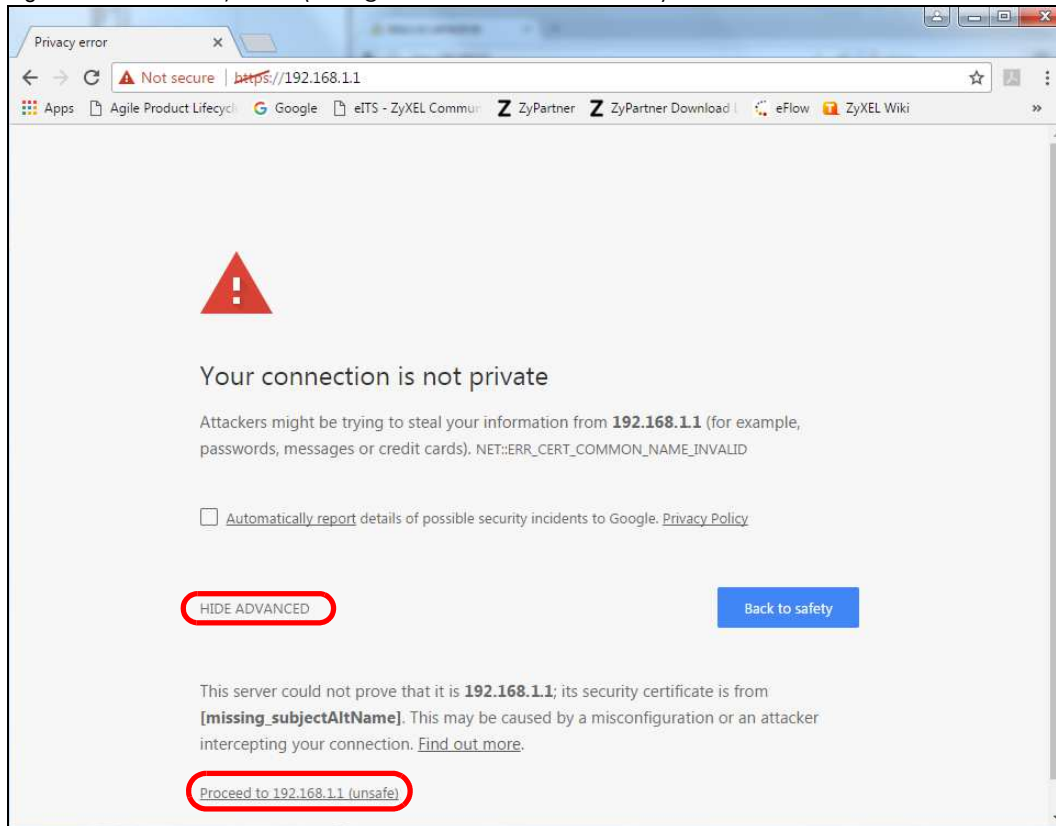
Figure 230 Security Alert (Mozilla Firefox 53.0)



36.7.4 Google Chrome Warning Messages

When you attempt to access the Switch HTTPS server, a Your connection is not private screen may display. If that is the case, click **Advanced** and then **Proceed to x.x.x.x (unsafe)** to proceed to the web configurator login screen.

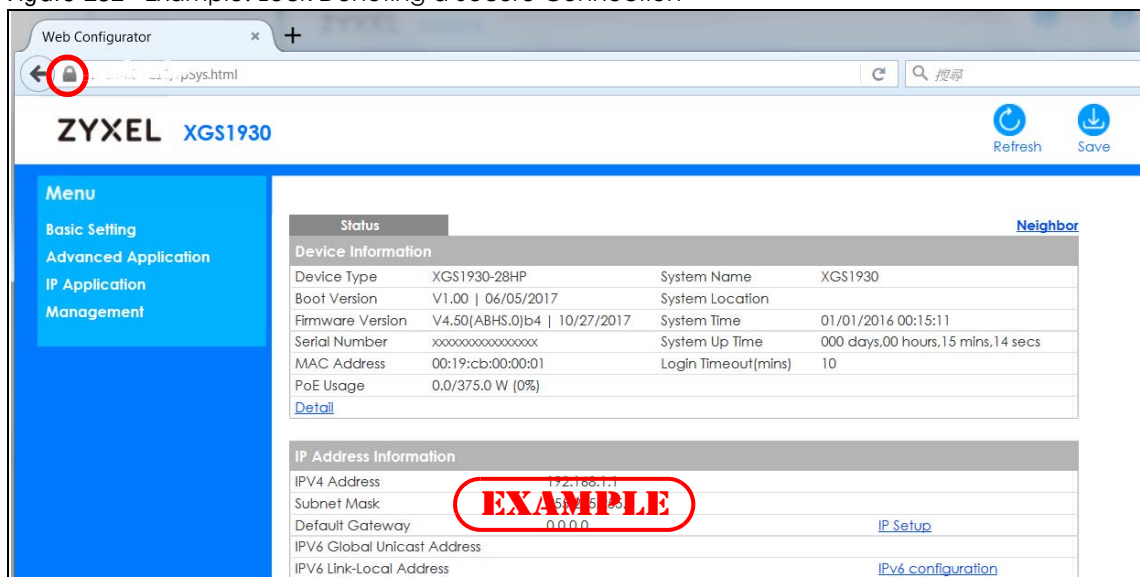
Figure 231 Security Alert (Google Chrome 58.0.3029.110)



36.7.4.1 The Main Screen

After you accept the certificate and enter the login username and password, the Switch main screen appears. The lock displayed in the bottom right of the browser status bar or next to the website address denotes a secure connection.

Figure 232 Example: Lock Denoting a Secure Connection



CHAPTER 37

Diagnostic

37.1 Overview

This chapter explains the **Diagnostic** screen. You can use this screen to help you identify problems.

37.2 Diagnostic

Click **Management > Diagnostic** in the navigation panel to open this screen. Use this screen to ping IP addresses, run a traceroute, perform port tests or show the Switch's location between devices.

Figure 233 Management > Diagnostic

The screenshot shows the 'Diagnostic' screen with a tab labeled 'Diagnostic' and a sub-tab '- Info -'. Below this, there are five test sections:

- Ping Test:** Includes radio buttons for IPv4 (selected) and IPv6, a dropdown menu, a text input for 'IP Address/Host Name', a text input for 'Source IP Address', and a numeric input for 'Count' (set to 3). A blue 'Ping' button is on the right.
- Trace Route Test:** Includes radio buttons for IPv4 (selected) and IPv6, a text input for 'IP Address/Host Name', a numeric input for 'TTL' (set to 30), a numeric input for 'Wait Time' (set to 2) with 'Seconds' next to it, and a numeric input for 'Queries' (set to 3). A blue 'Trace Route' button is on the right.
- Ethernet Port Test:** Includes a text input for 'Port' and a blue 'Port Test' button.
- Cable Diagnostics:** Includes a text input for 'Port' and a blue 'Diagnose' button.
- Locator LED:** Includes a numeric input for '30' and the text 'Minutes'. It has two blue buttons: 'Blink' and 'Stop'.

The following table describes the labels in this screen.

Table 165 Management > Diagnostic

LABEL	DESCRIPTION
Ping Test	
IPv4	Select this option if you want to ping an IPv4 address. Select - to send ping requests to all VLANs on the Switch.
IPv6	Select this option if you want to ping an IPv6 address. You can also select vlan and specify the ID number of the VLAN to which the Switch is to send ping requests. Otherwise, select - to send ping requests to all VLANs on the Switch.
IP Address/Host Name	Type the IP address or host name of a device that you want to ping in order to test a connection. Click Ping to have the Switch ping the IP address.
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. Select - to trace the path on any VLAN. Note: The device to which you want to run a traceroute must belong to the VLAN you specify here.
IPv6	Select this option if you want to trace the route packets take to a device with an IPv6 address.
IP Address/Host Name	Enter the IP address or host name of a device to which you want to perform a traceroute. Click Trace Route to have the Switch perform the traceroute function. This determines the path a packet takes to the specified device.
TTL	Enter the Time To Live (TTL) value for the ICMP Echo Request packets. This is to set the maximum number of the hops (routers) a packet can travel through. Each router along the path will decrement the TTL value by one and forward the packets. When the TTL value becomes zero and the destination is not found, the router drops the packets and informs the sender.
Wait Time	Specify how many seconds the Switch waits for a response to a probe before running another traceroute.
Queries	Specify how many times the Switch performs the traceroute function.
Ethernet Port Test	Enter a port number and click Port Test to perform an internal loopback test.
Cable Diagnostics	Enter an Ethernet port number and click Diagnose to perform a physical wire-pair test of the Ethernet connections on the specified port(s). The following fields display in the Diagnostic field when you diagnose a port. This field is available only on the Switch that has one or more copper Ethernet ports (except the MGMTport). Note: The Switch measures the cable length by sending an electric signal through the cable and reading the signal that is reflected back. To prevent possible interference from a connected device, it's suggested that you disconnect the other end of the Ethernet cable which is connected to the specified port.
Port	This is the number of the physical Ethernet port on the Switch.
Channel	An Ethernet cable usually has four pairs of wires. A 10BASE-T or 100BASE-TX port only use and test two pairs, while a 1000BASE-T port requires all four pairs. This displays the descriptive name of the wire-pair in the cable.

Table 165 Management > Diagnostic (continued)

LABEL	DESCRIPTION
Pair status	Ok: The physical connection between the wire-pair is okay. Open: There is no physical connection (an open circuit detected) between the wire-pair. Short: There is an short circuit detected between the wire-pair. Unknown: The Switch failed to run cable diagnostics on the cable connected this port. Unsupported: The port is a fiber port or it is not active.
Cable length	This displays the total length of the Ethernet cable that is connected to the port when the Pair status is Ok and the Switch chipset supports this feature. This shows N/A if the Pair status is Open or Short. Check the Distance to fault. This shows Unsupported if the Switch chipset does not support to show the cable length.
Distance to fault	This displays the distance between the port and the location where the cable is open or shorted. This shows N/A if the Pair status is Ok. This shows Unsupported if the Switch chipset does not support to show the distance.
Locator LED	Enter a time interval (in minutes) and click Blink to show the actual location of the Switch between several devices in a rack. The default time interval is 30 minutes. Click Stop to have the Switch terminate the blinking locator LED.

CHAPTER 38

System Log

38.1 Overview

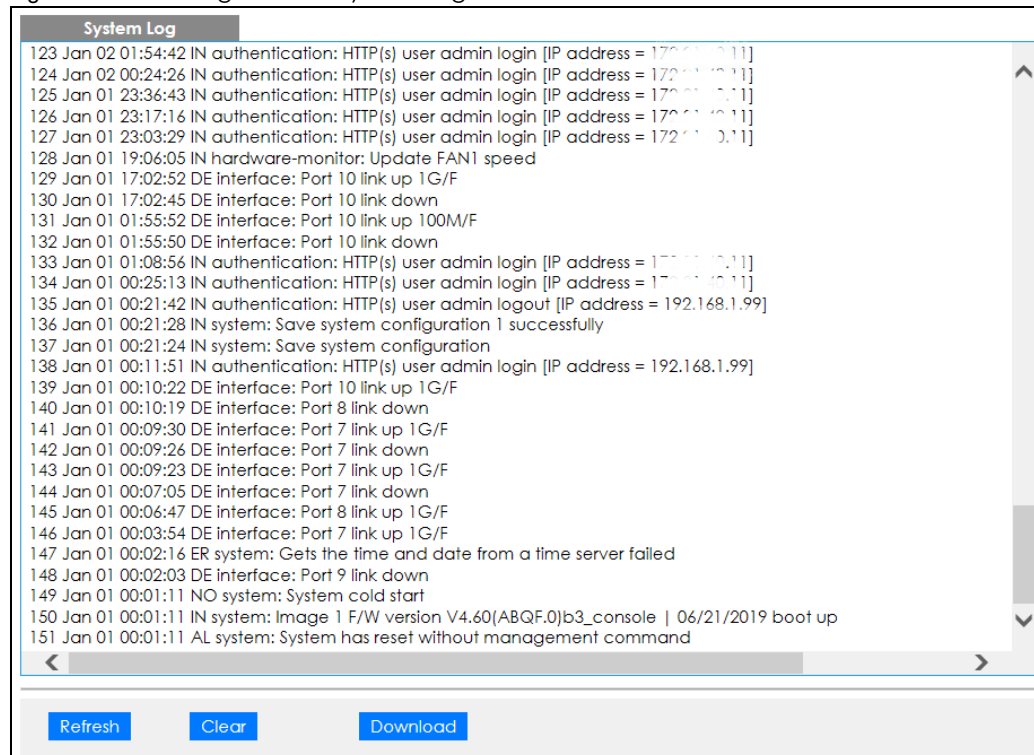
A log message stores the information for viewing.

38.2 System Log

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

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

Figure 234 Management > System Log



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

CHAPTER 39

Syslog Setup

39.1 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 166 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.

39.1.1 What You Can Do

Use the **Syslog Setup** screen ([Section 39.2 on page 317](#)) to configure the device's system logging settings and configure a list of external syslog servers.

39.2 Syslog Setup

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

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

Figure 235 Management > Syslog Setup

Syslog Setup

Syslog ☐ Active

Logging type	Active	Facility
System	☐	local use 0 ▼
Interface	☐	local use 0 ▼
Switch	☐	local use 0 ▼
AAA	☐	local use 0 ▼
IP	☐	local use 0 ▼

[Apply](#) [Cancel](#)

Syslog Server Setup

Active ☐

Server Address

UDP Port

Log Level

[Add](#) [Cancel](#) [Clear](#)

Index	Active	IP Address	UDP Port	Log Level	
					☐

[Delete](#) [Cancel](#)

The following table describes the labels in this screen.

Table 167 Management > Syslog Setup

LABEL	DESCRIPTION
Syslog	Select Active to turn on syslog (system logging) and then configure the syslog setting
Logging Type	This column displays the names of the categories of logs that the device can generate.
Active	Select this option to set the device to generate logs for the corresponding category.
Facility	The log facility allows you to send logs to different files in the syslog server. Refer to the documentation of your syslog program for more details.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Syslog Server Setup	
Active	Select this check box to have the device send logs to this syslog server. Clear the check box if you want to create a syslog server entry but not have the device send logs to it (you can edit the entry later).
Server Address	Enter the IPv4 or IPv6 address of the syslog server.
UDP Port	The default syslog server port is 514. If your syslog server uses a different port, configure the one it uses here.
Log Level	Select the severity level(s) of the logs that you want the device to send to this syslog server. The lower the number, the more critical the logs are.

Table 167 Management > Syslog Setup

LABEL	DESCRIPTION
Add	Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clear	Click Clear to return the fields to the factory defaults.
Index	This is the index number of a syslog server entry. Click this number to edit the entry.
Active	This field displays Yes if the device is to send logs to the syslog server. No displays if the device is not to send logs to the syslog server.
IP Address	This field displays the IP address of the syslog server.
UDP Port	This field displays the port of the syslog server.
Log Level	This field displays the severity level of the logs that the device is to send to this syslog server.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Delete	Click Delete to remove the selected entry(ies).
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 40

Cluster Management

40.1 Cluster Management Overview

This chapter introduces cluster management.

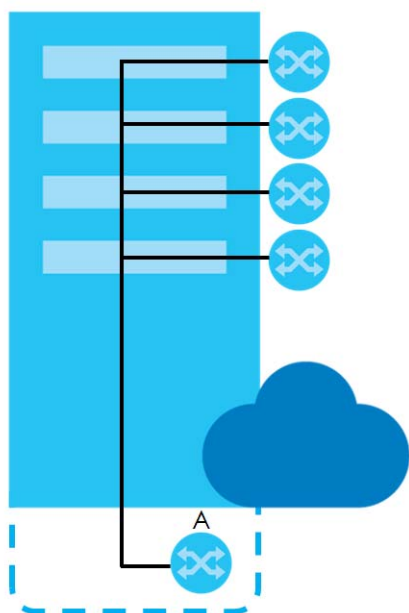
Cluster Management allows you to manage switches through one Switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

Table 168 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 236 Clustering Application Example



40.1.1 What You Can Do

- Use the Cluster Management screen ([Section 40.2 on page 321](#)) to view the role of the Switch within the cluster and to access a cluster member switch's web configurator.

- Use the Clustering Management Configuration screen ([Section 40.1 on page 320](#)) to configure clustering management.

40.2 Cluster Management Status

Use this screen to view the role of the Switch within the cluster and to access a cluster member switch's web configurator.

Click **Management > Cluster Management** in the navigation panel to display the following screen.

Note: A cluster can only have one manager.

Figure 237 Management > Cluster Management: Status

Clustering Management Status		Configuration		
Status	None			
Manager	00:00:00:00:00:00			
The Number Of Member = 0				
Index	MacAddr	Name	Model	Status

The following table describes the labels in this screen.

Table 169 Management > Cluster Management: Status

LABEL	DESCRIPTION
Status	This field displays the role of this Switch within the cluster. Manager Member (you see this if you access this screen in the cluster member switch directly and not via the cluster manager) None (neither a manager nor a member of a cluster)
Manager	This field displays the cluster manager switch's hardware MAC address.
The Number of Member	This field displays the number of switches that make up this cluster. The following fields describe the cluster member switches.
Index	You can manage cluster member switches via the cluster manager switch. Each number in the Index column is a hyperlink leading to the cluster member switch's web configurator (see Figure 239 on page 324).
MacAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's System Name .

Table 169 Management > Cluster Management: Status (continued)

LABEL	DESCRIPTION
Model	This field displays the model name.
Status	This field displays: Online (the cluster member switch is accessible) Error (for example the cluster member switch password was changed or the switch was set as the manager and so left the member list, etc.) Offline (the switch is disconnected - Offline shows approximately 1.5 minutes after the link between cluster member and manager goes down)

40.3 Clustering Management Configuration

Use this screen to configure clustering management. Click **Management > Cluster Management > Configuration** to display the next screen.

Figure 238 Management > Cluster Management > Configuration

Clustering Management Configuration [Status](#)

Clustering Manager

Active ☐

Name

VID

[Apply](#) [Cancel](#)

Clustering Candidate

List

Password

[Add](#) [Cancel](#) [Refresh](#)

Index	MacAddr	Name	Model

[Remove](#) [Cancel](#)

The following table describes the labels in this screen.

Table 170 Management > Cluster Management > Configuration

LABEL	DESCRIPTION
Clustering Manager	
Active	Select Active to have this Switch become the cluster manager switch. A cluster can only have one manager. Other (directly connected) switches that are set to be cluster managers will not be visible in the Clustering Candidates list. If a switch that was previously a cluster member is later set to become a cluster manager, then its Status is displayed as Error in the Cluster Management Status screen and a warning icon () appears in the member summary list below.
Name	Type a name to identify the Clustering Manager . You may use up to 32 printable characters (spaces are allowed).
VID	This is the VLAN ID and is only applicable if the Switch is set to 802.1Q VLAN. All switches must be directly connected and in the same VLAN group to belong to the same cluster. Switches that are not in the same VLAN group are not visible in the Clustering Candidates list. This field is ignored if the Clustering Manager is using Port-based VLAN.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Clustering Candidate	The following fields relate to the switches that are potential cluster members.
List	A list of suitable candidates found by auto-discovery is shown here. The switches must be directly connected. Directly connected switches that are set to be cluster managers will not be visible in the Clustering Candidate list. Switches that are not in the same management VLAN group will not be visible in the Clustering Candidate list.
Password	Each cluster member's password is its web configurator password. Select a member in the Clustering Candidate list and then enter its web configurator password. If that switch administrator changes the web configurator password afterwards, then it cannot be managed from the Cluster Manager . Its Status is displayed as Error in the Cluster Management Status screen. If multiple devices have the same password then hold [SHIFT] and click those switches to select them. Then enter their common web configurator password.
Add	Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.
Refresh	Click Refresh to perform auto-discovery again to list potential cluster members.
The next summary table shows the information for the clustering members configured.	
Index	This is the index number of a cluster member switch.
MacAddr	This is the cluster member switch's hardware MAC address.
Name	This is the cluster member switch's System Name .
Model	This is the cluster member switch's model name.
	Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries.
Remove	Click the Remove button to remove the selected cluster member switch(es) from the cluster.
Cancel	Click Cancel to begin configuring this screen afresh.

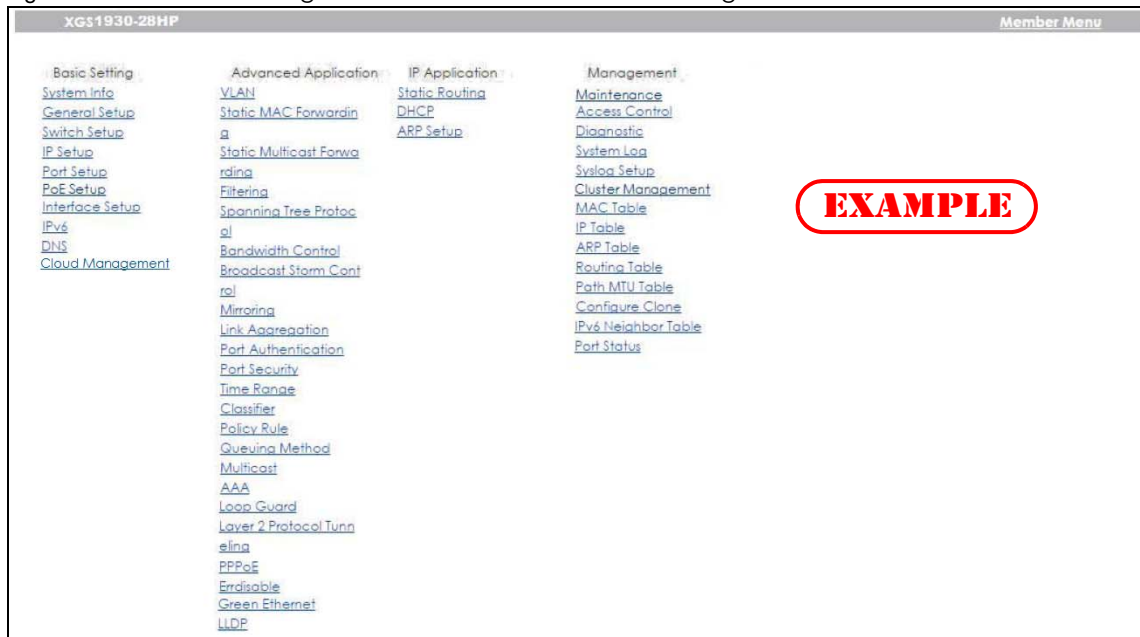
40.4 Technical Reference

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

40.4.1 Cluster Member Switch Management

Go to the Clustering Management Status screen of the cluster manager switch and then select an Index hyperlink from the list of members to go to that cluster member switch's web configurator home page. This cluster member web configurator home page and the home page that you'd see if you accessed it directly are different.

Figure 239 Cluster Management: Cluster Member Web Configurator Screen



40.4.1.1 Uploading Firmware to a Cluster Member Switch

You can use FTP to upload firmware to a cluster member switch through the cluster manager switch as shown in the following example.

Figure 240 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 460ABQF0.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 171 FTP Upload to Cluster Member Example

FTP PARAMETER	DESCRIPTION
User	Enter "admin".
Password	The web configurator password default is 1234.
ls	Enter this command to list the name of cluster member switch's firmware and configuration file.
460ABQF0.bin	This is the name of the firmware file you want to upload to the cluster member switch.
fw-00-a0-c5-01-23-46	This is the cluster member switch's firmware name as seen in the cluster manager switch.
config-00-a0-c5-01-23-46	This is the cluster member switch's configuration file name as seen in the cluster manager switch.

CHAPTER 41

MAC Table

41.1 MAC Table Overview

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

The **MAC Table** screen (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the Switch's ports. It shows what device MAC address, belonging to what VLAN group (if any) is forwarded to which port(s) and whether the MAC address is dynamic (learned by the Switch) or static (manually entered in the **Static MAC Forwarding** screen).

41.1.1 What You Can Do

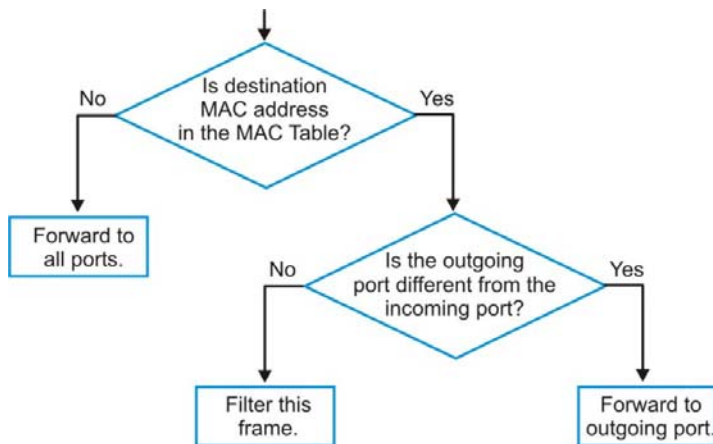
Use the **MAC Table** screen ([Section 41.2 on page 327](#)) to check whether the MAC address is dynamic or static.

41.1.2 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.
 - 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 241 MAC Table Flowchart



41.2 Viewing the MAC Table

Use this screen to check whether the MAC address is dynamic or static.

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

Figure 242 Management > MAC Table

MAC table

Condition

☐ All
☒ Static
☐ MAC
☐ VID
☐ Port
☐ Trunk

Sort by

MAC ▼

Transfer Type

☒ Dynamic to MAC forwarding
☐ Dynamic to MAC filtering

Search

Transfer

Cancel

Index	MAC Address	VID	Port	Type
11	00:19:cb:00:00:01	1	CPU	Static

The following table describes the labels in this screen.

Table 172 Management > MAC Table

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

CHAPTER 42

IP Table

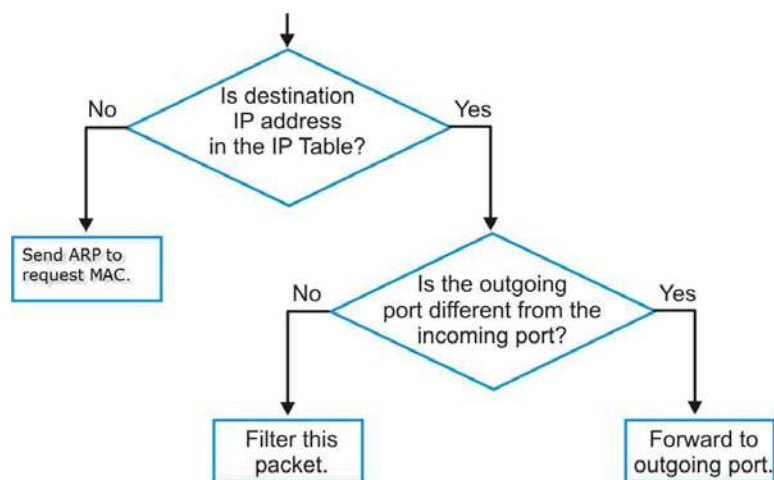
42.1 IP Table Overview

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 243 IP Table Flowchart



42.2 Viewing the IP Table

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

Figure 244 Management > IP Table

IP Table				
Sort by				
IP VID Port				
Index	IP Address	VID	Port	Type
1	172.31.42.12	1	7	dynamic
2	172.31.42.23	1	CPU	static
3	172.31.42.24	1	7	dynamic
4	192.168.1.1	1	CPU	static

The following table describes the labels in this screen.

Table 173 Management > IP Table

LABEL	DESCRIPTION
Sort by	Click one of the following buttons to display and arrange the data according to that button type. The information is then displayed in the summary table below.
IP	Click this button to display and arrange the data according to IP address.
VID	Click this button to display and arrange the data according to VLAN group.
Port	Click this button to display and arrange the data according to port number.
Index	This field displays the index number.
IP Address	This is the IP address of the device from which the incoming packets came.
VID	This is the VLAN group to which the packet belongs.
Port	This is the port from which the above IP address was learned. This field displays CPU to indicate the IP address belongs to the Switch.
Type	This shows whether the IP address is dynamic (learned by the Switch) or static (belonging to the Switch).

CHAPTER 43

ARP Table

43.1 ARP Table Overview

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

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

43.1.1 What You Can Do

Use the ARP Table screen ([Section 43.2 on page 331](#)) to view IP-to-MAC address mapping(s).

43.1.2 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.

43.2 Viewing the ARP Table

Use the ARP table to view IP-to-MAC address mapping(s) and remove specific dynamic ARP entries.

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

Figure 245 Management > ARP Table

Index	IP Address	MAC Address	VID	Port	Age(s)	Type
1	192.168.1.1	00:19:cb:00:01:02	1	CPU	0	static
2	192.168.1.1	dc:4a:3e:40:ec:67	1	44	205	dynamic
3	192.168.1.1	00:19:cb:00:01:02	1	CPU	0	static

The following table describes the labels in this screen.

Table 174 Management > ARP Table

LABEL	DESCRIPTION
Condition	Specify how you want the Switch to remove ARP entries when you click Flush . Select All to remove all of the dynamic entries from the ARP table. Select IP Address and enter an IP address to remove the dynamic entries learned with the specified IP address. Select Port and enter a port number to remove the dynamic entries learned on the specified port.
Flush	Click Flush to remove the ARP entries according to the condition you specified.
Cancel	Click Cancel to return the fields to the factory defaults.
Index	This is the ARP table entry number.
IP Address	This is the IP address of a device connected to a Switch port with the corresponding MAC address below.
MAC Address	This is the MAC address of the device with the corresponding IP address above.
VID	This field displays the VLAN to which the device belongs.
Port	This field displays the port to which the device connects. CPU means this IP address is the Switch's management IP address.
Age(s)	This field displays how long (in seconds) an entry can still remain in the ARP table before it ages out and needs to be relearned. This shows 0 for a static entry.
Type	This shows whether the IP address is dynamic (learned by the Switch) or static (manually configured in the Basic Setting > IP Setup or IP Application > ARP Setup > Static ARP screen).

CHAPTER 44

Routing Table

44.1 Overview

The routing table contains the route information to the network(s) that the Switch can reach.

44.2 The Routing Table Main Screen

Click **Management > Routing Table** in the navigation panel to display the main screen as shown. Click the link next to **IPv4 Routing Table** to open a screen where you can view the IPv4 routing table information. Click the link next to **IPv6 Routing Table** to open a screen where you can view the IPv6 routing table information.

Figure 246 Management > Routing Table

Routing Table	
IPv4 Routing Table	Click Here
IPv6 Routing Table	Click Here

44.3 IPv4 Routing Table

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

Figure 247 Management > Routing Table > IPv4 Routing Table

IPv4 Routing Table						Routing Table
Index	Destination	Gateway	Interface	Metric	Type	Uptime
1	192.168.1.0/24	192.168.1.1	192.168.1.1	1	LOCAL	120:58:29
2	172.31.10.0/24	172.31.10.254	172.31.10.254	1	LOCAL	120:58:12
3	127.0.0.0/16	127.0.0.1	127.0.0.1	1	LOCAL	120:58:37
4	default	172.31.10.254	172.31.10.254	2	STATIC	120:58:12

The following table describes the labels in this screen.

Table 175 Management > 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.

Table 175 Management > Routing Table > IPv4 Routing Table (continued)

LABEL	DESCRIPTION
Interface	This field displays the IP address of the Interface.
Metric	This field displays the cost of the route.
Type	This field displays the method used to learn the route. STATIC - added as a static entry. LOCAL - added as a local 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.

44.4 IPv6 Routing Table

Use this screen to view IPv6 routing table information. Click **Management > Routing Table > IPv6 Routing Table** in the navigation panel to display the screen as shown.

Figure 248 Management > Routing Table > IPv6 Routing Table

IPv6 Routing Table					Routing Table
Index	Route Destination / Prefix Length	Next Hop	Interface	Metric	Type

The following table describes the labels in this screen.

Table 176 Management > Routing Table > IPv6 Routing Table

LABEL	DESCRIPTION
Index	This field displays the index number.
Route Destination/ Prefix Length	This field displays the IPv6 subnet prefix and prefix length of the final destination.
Next Hop	This field displays the IPv6 address of the gateway that helps forward the packet to the destination.
Interface	This field displays the descriptive name of the IPv6 interface that is used to forward the packets to the destination.
Metric	This field displays the cost of the route.
Type	This field displays the method used to learn the route. STATIC - added as a static entry. Connect - added as a local interface entry.

CHAPTER 45

Path MTU Table

45.1 Path MTU Overview

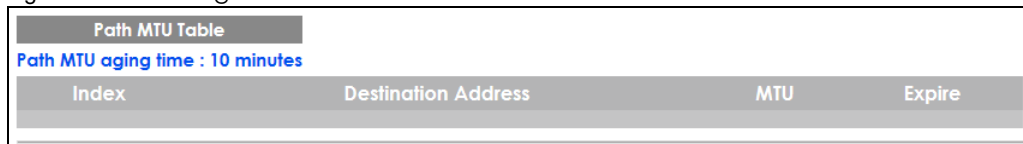
This chapter introduces the IPv6 Path MTU table.

The largest size (in bytes) of a packet that can be transferred over a data link is called the maximum transmission unit (MTU). The Switch uses Path MTU Discovery to discover Path MTU (PMTU), that is, the minimum link MTU of all the links in a path to the destination. If the Switch receives an ICMPv6 Packet Too Big error message after sending a packet, it fragments the next packet according to the suggested MTU in the error message.

45.2 Viewing the Path MTU Table

Use this screen to view IPv6 path MTU information on the Switch. Click **Management > Path MTU Table** in the navigation panel to display the screen as shown.

Figure 249 Management > Path MTU Table



Index	Destination Address	MTU	Expire

The following table describes the labels in this screen.

Table 177 Management > Path MTU Table

LABEL	DESCRIPTION
Path MTU aging time	This field displays how long an entry remains in the Path MTU table before it ages out and needs to be relearned.
Index	This field displays the index number of each entry in the table.
Destination Address	This field displays the destination IPv6 address of each path/entry.
MTU	This field displays the maximum transmission unit of the links in the path.
Expire	This field displays how long (in minutes) an entry can still remain in the Path MTU table before it ages out and needs to be relearned.

CHAPTER 46

Configure Clone

46.1 Overview

This chapter shows you how you can copy the settings of one port onto other ports.

46.2 Configure Clone

Cloning allows you to copy the basic and advanced settings from a source port to a destination port or ports. Click **Management > Configure Clone** to open the following screen.

Figure 250 Management > Configure Clone

Configure Clone

Source **Destination**

☒ Port

Port Features

	☐ *
Basic Setting	☐ Active
	☐ Name
	☐ Speed / Duplex
	☐ Flow Control
	☐ VLAN1q
Advanced Application	☐ VLAN1q Member
	☐ Bandwidth Control
	☐ Port Security
	☐ Broadcast Storm Control
	☐ Mirroring
	☐ Port Authentication
	☐ Queuing Method
	☐ IGMP Filtering
	☐ Spanning Tree Protocol
	☐ Port-based VLAN
	☐ MAC Authentication
	☐ Loop Guard
	☐ Layer 2 Protocol Tunneling
	☐ LLDP
	☐ PPPoE IA
	☐ ARP Learning
	☐ CPUProtection
	☐ Multiple Spanning Tree Protocol
	☐ Power over Ethernet
	☐ SNMP Trap
☐ Green Ethernet	

Apply **Cancel**

The following table describes the labels in this screen.

Table 178 Management > Configure Clone

LABEL	DESCRIPTION
Source/ Destination 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 hyphen. For example, 2, 4, 6 indicates that ports 2, 4 and 6 are the destination ports. 2-6 indicates that ports 2 through 6 are the destination ports.
*	Select this check box to select all port settings.
Basic Setting	Select which port settings (you configured in the Basic Setting menus) should be copied to the destination port(s).

Table 178 Management > Configure Clone (continued)

LABEL	DESCRIPTION
Advanced Application	Select which port settings (you configured in the Advanced Application menus) should be copied to the destination ports.
Apply	Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.
Cancel	Click Cancel to begin configuring this screen afresh.

CHAPTER 47

IPv6 Neighbor Table

47.1 IPv6 Neighbor Table Overview

This chapter introduces the IPv6 neighbor table.

An IPv6 host is required to have a neighbor table. If there is an address to be resolved or verified, the Switch sends out a neighbor solicitation message. When the Switch receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor table. You can also manually create a static IPv6 neighbor entry using the **Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Setup** screen.

When the Switch needs to send a packet, it first consults other table to determine the next hop. Once the next hop IPv6 address is known, the Switch looks into the neighbor table to get the link-layer address and sends the packet when the neighbor is reachable. If the Switch cannot find an entry in the neighbor table or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

47.2 Viewing the IPv6 Neighbor Table

Use this screen to view IPv6 neighbor information on the Switch. Click **Management > IPv6 Neighbor Table** in the navigation panel to display the screen as shown.

Figure 251 Management > IPv6 Neighbor Table

IPv6 Neighbor Table					
Sort by:	Address	MAC	Interface		
Index	Address	MAC	Status	Type	Interface

The following table describes the labels in this screen.

Table 179 Management > IPv6 Neighbor Table

LABEL	DESCRIPTION
Sort by	Select this to display and arrange the data according to IPv6 address (Address), MAC address (MAC) or IPv6 interface (Interface). The information is then displayed in the summary table below.
Index	This field displays the index number of each entry in the table.
Address	This field displays the IPv6 address of the Switch or a neighboring device.
MAC	This field displays the MAC address of the IPv6 interface on which the IPv6 address is configured or the MAC address of the neighboring device.

Table 179 Management > IPv6 Neighbor Table (continued)

LABEL	DESCRIPTION
Status	This field displays whether the neighbor IPv6 interface is reachable. In IPv6, "reachable" means an IPv6 packet can be correctly forwarded to a neighbor node (host or router) and the neighbor can successfully receive and handle the packet. The available options in this field are: • reachable (R): The interface of the neighboring device is reachable. (The Switch has received a response to the initial request.) • stale (S): The last reachable time has expired and the Switch is waiting for a response to another initial request. The field displays this also when the Switch receives an unrequested response from the neighbor's interface. • delay (D): The neighboring interface is no longer known to be reachable, and traffic has been sent to the neighbor recently. The Switch delays sending request packets for a short to give upper-layer protocols a chance to determine reachability. • probe (P): The Switch is sending request packets and waiting for the neighbor's response. • invalid (IV): The neighbor address is with an invalid IPv6 address. • unknown (?): The status of the neighboring interface can not be determined for some reason. • incomplete (I): Address resolution is in progress and the link-layer address of the neighbor has not yet been determined. The interface of the neighboring device did not give a complete response.
Type	This field displays the type of an address mapping to a neighbor interface. The available options in this field are: • other (O): none of the following type. • local (L): A Switch interface is using the address. • dynamic (D): The IP address to MAC address can be successfully resolved using IPv6 Neighbor Discovery protocol. Is it similar as IPv4 ARP (Address Resolution protocol). • static (S): The interface address is statically configured.
Interface	This field displays the ID number of the IPv6 interface on which the IPv6 address is created or through which the neighboring device can be reached.

CHAPTER 48

Port Status

This chapter introduces the port status screens.

48.1 Port Status

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

Figure 252 Port Status (for PoE model(s))

Port Status											DDMI Utilization
Port	Name	Link	State	PD	LACP	TxPkts	RxPkts	Errors	Tx kB/s	Rx kB/s	Up Time
1		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
2		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
3		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
4		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
5		Down	STOP	Off	Disabled	1891243	181027	0	0.0	0.0	0:00:00
6		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
7	1G/F	FORWARDING	FORWARDING	Off	Disabled	177968	2044916	0	0.0	0.340	121:56:23
8		Down	STOP	Off	Disabled	0	0	0	0.0	0.0	0:00:00
9		Down	STOP	-	Disabled	0	0	0	0.0	0.0	0:00:00
10		Down	STOP	-	Disabled	0	0	0	0.0	0.0	0:00:00
11		Down	STOP	-	Disabled	0	0	0	0.0	0.0	0:00:00
12		Down	STOP	-	Disabled	0	0	0	0.0	0.0	0:00:00

☒ Any
 ☐ Port

The following table describes the labels in this screen.

Table 180 Port Status

LABEL	DESCRIPTION
Port	This identifies the Ethernet port. Click a port number to display the Port Details screen (refer to Figure 253 on page 343).
Name	This is the name you assigned to this port in the Basic Setting > Port Setup screen.
Link	This field displays the speed (either 100M for 100Mbps, 1G for 1 Gbps, 2.5G for 2.5 Gbps, 5G for 5 Gbps, or 10G for 10 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.
State	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port. See page 138 for more information. If STP is disabled, this field displays FORWARDING if the link is up, otherwise, it displays STOP. When LACP (Link Aggregation Control Protocol), STP, and dot1x are in blocking state, it displays Blocking.

Table 180 Port Status (continued)

LABEL	DESCRIPTION
PD	For PoE model(s) only. This field displays whether or not a powered device (PD) is allowed to receive power from the Switch on this port.
LACP	This fields displays whether LACP (Link Aggregation Control Protocol) has been enabled on the port.
TxPkts	This field shows the number of transmitted frames on this port.
RxPkts	This field shows the number of received frames on this port.
Errors	This field shows the number of received errors on this port.
Tx kB/s	This field shows the number of kilobytes per second transmitted on this port.
Rx kB/s	This field shows the number of kilobytes per second received on this port.
Up Time	This field shows the total amount of time in hours, minutes and seconds the port has been up.
Clear Counter	Select Port , enter a port number and then click Clear Counter to erase the recorded statistical information for that port, or select Any to clear statistics for all ports.

48.1.1 Port Details

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

Figure 253 Port Status > Port Details

Port Details		Port Status
Port Info	Port NO.	1
	Name	
	Link	Down
	State	STOP
	LACP	Disabled
	TxPkts	0
	RxPkts	0
	Errors	0
	Tx kB/s	0.0
	Tx Utilization%	0.0
	Rx kB/s	0.0
	Rx Utilization%	0.0
	Up Time	0:00:00
TX Packet	Unicast	0
	Multicast	0
	Broadcast	0
	Pause	0
RX Packet	Unicast	0
	Multicast	0
	Broadcast	0
	Pause	0
TX Collision	Single	0
	Multiple	0
	Excessive	0
	Late	0
Error Packet	RX CRC	0
	Length	0
	Runt	0
Distribution	64	0
	65 to 127	0
	128 to 255	0
	256 to 511	0
	512 to 1023	0
	1024 to 1518	0
	Giant	0

The following table describes the labels in this screen.

Table 181 Port Status: Port Details

LABEL	DESCRIPTION
Port Info	
Port NO.	This field displays the port number you are viewing.
Name	This field displays the name of the port.
Link	This field displays the speed (either 100M for 100Mbps, 1G for 1 Gbps, 2.5G for 2.5 Gbps, 5G for 5 Gbps, or 10G for 10 Gbps) and the duplex (F for full duplex or H for half duplex). This field displays Down if the port is not connected to any device.
State	If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port. See page 138 for more information. 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

Table 181 Port Status: Port Details (continued)

LABEL	DESCRIPTION
Errors	This field shows the number of received errors on this port.
Tx kB/s	This field shows the number of kilobytes per second transmitted on this port.
Tx Utilization%	This field shows the percentage of actual transmitted frames on this port as a percentage of the Link speed.
Rx kB/s	This field shows the number of kilobytes per second received on this port.
Rx Utilization%	This field shows the percentage of actual received frames on this port as a percentage of the Link speed.
Up Time	This field shows the total amount of time the connection has been up.
Tx Packet	
The following fields display detailed information about packets transmitted.	
Unicast	This field shows the number of good unicast packets transmitted.
Multicast	This field shows the number of good multicast packets transmitted.
Broadcast	This field shows the number of good broadcast packets transmitted.
Pause	This field shows the number of 802.3x Pause packets transmitted.
Rx Packet	
The following fields display detailed information about packets received.	
Unicast	This field shows the number of good unicast packets received.
Multicast	This field shows the number of good multicast packets received.
Broadcast	This field shows the number of good broadcast packets received.
Pause	This field shows the number of 802.3x Pause packets received.
TX Collision	
The following fields display information on collisions while transmitting.	
Single	This is a count of successfully transmitted packets for which transmission is inhibited by exactly one collision.
Multiple	This is a count of successfully transmitted packets for which transmission was inhibited by more than one collision.
Excessive	This is a count of packets for which transmission failed due to excessive collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset.
Late	This is the number of times a late collision is detected, that is, after 512 bits of the packets have already been transmitted.
Error Packet	
The following fields display detailed information about packets received that were in error.	
RX CRC	This field shows the number of packets received with CRC (Cyclic Redundant Check) error(s).
Length	This field shows the number of packets received with a length that was out of range.
Runt	This field shows the number of packets received that were too short (shorter than 64 octets), including the ones with CRC errors.
Distribution	
64	This field shows the number of packets (including bad packets) received that were 64 octets in length.
65-127	This field shows the number of packets (including bad packets) received that were between 65 and 127 octets in length.
128-255	This field shows the number of packets (including bad packets) received that were between 128 and 255 octets in length.
256-511	This field shows the number of packets (including bad packets) received that were between 256 and 511 octets in length.

Table 181 Port Status: Port Details (continued)

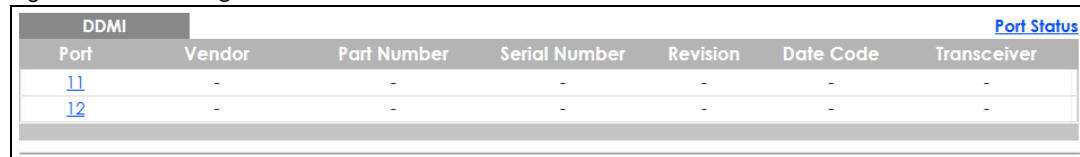
LABEL	DESCRIPTION
512-1023	This field shows the number of packets (including bad packets) received that were between 512 and 1023 octets in length.
1024-1518	This field shows the number of packets (including bad packets) received that were between 1024 and 1518 octets in length.
Giant	This field shows the number of packets (including bad packets) received that were between 1519 octets and the maximum frame size. The maximum frame size varies depending on your switch model.

48.1.2 DDMI

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

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

Figure 254 Management > Port Status > DDMI



DDMI						Port Status
Port	Vendor	Part Number	Serial Number	Revision	Date Code	Transceiver
11	-	-	-	-	-	-
12	-	-	-	-	-	-

The following table describes the labels in this screen.

Table 182 Management > Port Status > DDMI

LABEL	DESCRIPTION
Port	This identifies the SFP port.
Vendor	This displays the vendor name of the optical transceiver.
Part Number	This displays the part number of the optical transceiver.
Serial Number	This displays the serial number of the optical transceiver.
Revision	This displays the revision number of the optical transceiver.
Date Code	This displays the date when the optical transceiver was manufactured.
Transceiver	This displays whether the connection to the optical network is up or down.

48.1.3 DDMI Details

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

Click a number in the **Port** column in the DDMI screen to view current transceivers' status.

Figure 255 Management > Port Status > DDMI > DDMI Details

DDMI Details						DDMI
Transceiver Information						
Port No:	11					
Connector Type	-					
Vendor	-					
Part Number	-					
Serial Number	-					
Revision	-					
Date Code	-					
Transceiver	-					
DDMI Information						
Type	Current	High Alarm Threshold	High Warn Threshold	Low Warn Threshold	Low Alarm Threshold	
Temperature(C)	-	-	-	-	-	
Voltage(V)	-	-	-	-	-	
TX Bias(mA)	-	-	-	-	-	
TX Power(dbm)	-	-	-	-	-	
RX Power(dbm)	-	-	-	-	-	

The following table describes the labels in this screen.

Table 183 Management > Port Status > DDMI > DDMI Details

LABEL	DESCRIPTION
Transceiver Information	
Port No	This identifies the SFP port.
Connector Type	This displays the connector type of the optical transceiver.
Vendor	This displays the vendor name of the optical transceiver.
Part Number	This displays the part number of the optical transceiver.
Serial Number	This displays the serial number of the optical transceiver.
Revision	This displays the revision number of the optical transceiver.
Date Code	This displays the date when the optical transceiver was manufactured.
Transceiver	This displays details about the type of transceiver installed in the SFP slot.
Calibration	This field is available only when an SFP transceiver is inserted into the SFP slot. Internal displays if the measurement values are calibrated by the transceiver. External displays if the measurement values are raw data which the Switch calibrates.
DDMI Information	
Type	This displays the DDMI parameter.
Temperature (C)	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 optic 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.

Table 183 Management > Port Status > DDMI > DDMI Details (continued)

LABEL	DESCRIPTION
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.

48.1.4 Port Utilization

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

Figure 256 Management > Port Status > Utilization

Port Utilization				Port Status	
Port	Link	Tx kB/s	Tx Utilization%	Rx kB/s	Rx Utilization%
1	Down	0.0	0.0	0.0	0.0
2	Down	0.0	0.0	0.0	0.0
3	Down	0.0	0.0	0.0	0.0
4	Down	0.0	0.0	0.0	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
8	Down	0.0	0.0	0.0	0.0
9	Down	0.0	0.0	0.0	0.0
10	1G/F	0.320	0.0	0.987	0.0
11	Down	0.0	0.0	0.0	0.0
12	Down	0.0	0.0	0.0	0.0

The following table describes the labels in this screen.

Table 184 Port Status > Utilization

LABEL	DESCRIPTION
Port	This identifies the Ethernet port.
Link	This field displays the speed (either 100M for 100Mbps, 1G for 1 Gbps, 2.5G for 2.5 Gbps, 5G for 5 Gbps, or 10G for 10 Gbps) and the duplex (F for full duplex). This field displays Down if the port is not connected to any device.
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 49

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](#)

49.1 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 3.3 on page 35](#).
- 2 Check the hardware connections. See [Section 49.1 on page 348](#).
- 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.
- 5 If the problem continues, contact the vendor.

49.2 Switch Access and Login

I forgot the IP address for the Switch.

- 1 The default IP address is [http://DHCP-assigned IP](#) or 192.168.1.1.
- 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 NCC, the ZON utility, or the console port to find the IP address. The Switch must be registered and added to a site in Nebula in order for it to be managed using Nebula.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 4.8 on page 62](#).

I forgot the username and/or password.

- 1 The default username is admin and the default password is 1234.
- 2 If this does not work, you have to reset the device to its factory defaults. See [Section 4.8 on page 62](#).

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 [http://DHCP-assigned IP](#) or 192.168.1.1.
 - If you changed the IP address, use the new IP address.
 - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I forgot the IP address for the Switch](#).
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See [Section 3.3 on page 35](#).
- 3 Make sure your Internet browser does not block pop-up windows and has JavaScripts and Java enabled.
- 4 Make sure your computer is in the same subnet as the Switch. (If you know that there are routers between your computer and the Switch, skip this step.)
- 5 Reset the device to its factory defaults, and try to access the Switch with the default IP address. See [Section 4.8 on page 62](#).
- 6 If the problem continues, contact the vendor, or try one of the advanced suggestions.

Advanced Suggestions

- Try to access the Switch using another service, such as Telnet. If you can access the Switch, check the remote management settings to find out why the Switch does not respond to HTTP.

I can see the [Login screen](#), but I cannot log in to the Switch.

- 1 Make sure you have entered the user name and password correctly. The default user name is **admin**, and the default password is **1234**. These fields are case-sensitive, so make sure [Caps Lock] is not on.
- 2 You may have exceeded the maximum number of concurrent Telnet sessions. Close other Telnet session(s) or try connecting again later.

Check that you have enabled logins for HTTP or Telnet. If you have configured a secured client IP address, your computer's IP address must match it. Refer to the chapter on access control for details.
- 3 Disconnect and re-connect the cord to the Switch.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 4.8 on page 62](#).

Pop-up Windows, JavaScripts and Java Permissions

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

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

There is [unauthorized access to my Switch via telnet, HTTP and SSH](#).

To avoid unauthorized access, configure the secured client setting in the **Management > Access Control > Remote Management** screen for telnet, HTTP and SSH (see [Section 36.6 on page 301](#)). Computers not belonging to the secured client set cannot get permission to access the Switch.

49.3 Switch Configuration

I lost my configuration settings after I restart the Switch.

Make sure you save your configuration into the Switch's nonvolatile memory each time you make changes. Click



Save at the top right corner of the web configurator to save the configuration permanently. See also [Section 35.8 on page 286](#) for more information about how to save your configuration.

APPENDIX A

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the device.

See <https://www.zyxel.com/homepage.shtml> and also https://www.zyxel.com/about_zyxel/zyxel_worldwide.shtml for the latest information.

Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

Taiwan

- Zyxel Communications Corporation
- <http://www.zyxel.com>

Asia

China

- Zyxel Communications (Shanghai) Corp.
- Zyxel Communications (Beijing) Corp.
- Zyxel Communications (Tianjin) Corp.
- <https://www.zyxel.com/cn/zh/>

India

- Zyxel Technology India Pvt Ltd
- <https://www.zyxel.com/in/en/>

Kazakhstan

- Zyxel Kazakhstan
- <https://www.zyxel.kz>

Korea

- Zyxel Korea Corp.
- <http://www.zyxel.kr>

Malaysia

- Zyxel Malaysia Sdn Bhd.
- <http://www.zyxel.com.my>

Pakistan

- Zyxel Pakistan (Pvt.) Ltd.
- <http://www.zyxel.com.pk>

Philippines

- Zyxel Philippines
- <http://www.zyxel.com.ph>

Singapore

- Zyxel Singapore Pte Ltd.
- <http://www.zyxel.com.sg>

Taiwan

- Zyxel Communications Corporation
- <https://www.zyxel.com/tw/zh/>

Thailand

- Zyxel Thailand Co., Ltd
- <https://www.zyxel.com/th/th/>

Vietnam

- Zyxel Communications Corporation-Vietnam Office
- <https://www.zyxel.com/vn/vi>

Europe

Belarus

- Zyxel BY
- <https://www.zyxel.by>

Belgium

- Zyxel Communications B.V.
- <https://www.zyxel.com/be/nl/>

- <https://www.zyxel.com/be/fr/>

Bulgaria

- Zyxel България
- <https://www.zyxel.com/bg/bg/>

Czech Republic

- Zyxel Communications Czech s.r.o
- <https://www.zyxel.com/cz/cs/>

Denmark

- Zyxel Communications A/S
- <https://www.zyxel.com/dk/da/>

Estonia

- Zyxel Estonia
- <https://www.zyxel.com/ee/et/>

Finland

- Zyxel Communications
- <https://www.zyxel.com/fi/fi/>

France

- Zyxel France
- <https://www.zyxel.fr>

Germany

- Zyxel Deutschland GmbH
- <https://www.zyxel.com/de/de/>

Hungary

- Zyxel Hungary & SEE
- <https://www.zyxel.com/hu/hu/>

Italy

- Zyxel Communications Italy
- <https://www.zyxel.com/it/it/>

Latvia

- Zyxel Latvia
- <https://www.zyxel.com/lv/lv/>

Lithuania

- Zyxel Lithuania
- <https://www.zyxel.com/lt/lt/>

Netherlands

- Zyxel Benelux
- <https://www.zyxel.com/nl/nl/>

Norway

- Zyxel Communications
- <https://www.zyxel.com/no/no/>

Poland

- Zyxel Communications Poland
- <https://www.zyxel.com/pl/pl/>

Romania

- Zyxel Romania
- <https://www.zyxel.com/ro/ro/>

Russia

- Zyxel Russia
- <https://www.zyxel.com/ru/ru/>

Slovakia

- Zyxel Communications Czech s.r.o. organizacna zlozka
- <https://www.zyxel.com/sk/sk/>

Spain

- Zyxel Communications ES Ltd
- <https://www.zyxel.com/es/es/>

Sweden

- Zyxel Communications
- <https://www.zyxel.com/se/sv/>

Switzerland

- Studerus AG
- <https://www.zyxel.ch/de>
- <https://www.zyxel.ch/fr>

Turkey

- Zyxel Turkey A.S.
- <https://www.zyxel.com/tr/tr/>

UK

- Zyxel Communications UK Ltd.
- <https://www.zyxel.com/uk/en/>

Ukraine

- Zyxel Ukraine
- <http://www.ua.zyxel.com>

South America

Argentina

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

Brazil

- Zyxel Communications Brasil Ltda.
- <https://www.zyxel.com/br/pt/>

Colombia

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

Ecuador

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

South America

- Zyxel Communications Corporation
- <https://www.zyxel.com/co/es/>

Middle East

Israel

- Zyxel Communications Corporation
- <http://il.zyxel.com/>

Middle East

- Zyxel Communications Corporation
- <https://www.zyxel.com/me/en/>

North America

USA

- Zyxel Communications, Inc. - North America Headquarters
- <https://www.zyxel.com/us/en/>

Oceania

Australia

- Zyxel Communications Corporation
- <https://www.zyxel.com/au/en/>

Africa

South Africa

- Nology (Pty) Ltd.
- <https://www.zyxel.com/za/en/>

APPENDIX B

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type/code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name:** This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol:** This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **User-Defined**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s):** This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
 - If the **Protocol** is **TCP**, **UDP**, or **TCP/UDP**, this is the IP port number.
 - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description:** This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 185 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/server protocol for the world wide web.

Table 185 Commonly Used Services (continued)

NAME	PROTOCOL	PORT(S)	DESCRIPTION
HTTPS	TCP	443	HTTPS is a secured http session often used in e-commerce.
ICMP	User-Defined	1	Internet Control Message Protocol is often used for diagnostic or routing purposes.
ICQ	UDP	4000	This is a popular Internet chat program.
IGMP (MULTICAST)	User-Defined	2	Internet Group Multicast Protocol is used when sending packets to a specific group of hosts.
IKE	UDP	500	The Internet Key Exchange algorithm is used for key distribution and management.
IRC	TCP/UDP	6667	This is another popular Internet chat program.
MSN Messenger	TCP	1863	Microsoft Networks' messenger service uses this protocol.
NEW-ICQ	TCP	5190	An Internet chat program.
NEWS	TCP	144	A protocol for news groups.
NFS	UDP	2049	Network File System - NFS is a client/server distributed file service that provides transparent file sharing for network environments.
NNTP	TCP	119	Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service.
PING	User-Defined	1	Packet Internet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable.
POP3	TCP	110	Post Office Protocol version 3 lets a client computer get email 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 185 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 186 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 187 Predefined Multicast Address

MULTICASTADDRESS	DESCRIPTION
FF01:0:0:0:0:0:1	All hosts on a local node.
FF01:0:0:0:0:0:2	All routers on a local node.
FF02:0:0:0:0:0:1	All hosts on a local connected link.
FF02:0:0:0:0:0:2	All routers on a local connected link.
FF05:0:0:0:0:0:2	All routers on a local site.
FF05:0:0:0:0:0:1:3	All DHCP servers on a local site.

The following table describes the multicast addresses which are reserved and can not be assigned to a multicast group.

Table 188 Reserved Multicast Address

MULTICASTADDRESS
FF00:0:0:0:0:0:0:0
FF01:0:0:0:0:0:0:0
FF02:0:0:0:0:0:0:0
FF03:0:0:0:0:0:0:0
FF04:0:0:0:0:0:0:0
FF05:0:0:0:0:0:0:0
FF06:0:0:0:0:0:0:0
FF07:0:0:0:0:0:0:0
FF08:0:0:0:0:0:0:0
FF09:0:0:0:0:0:0:0
FF0A:0:0:0:0:0:0:0
FF0B:0:0:0:0:0:0:0
FF0C:0:0:0:0:0:0:0
FF0D:0:0:0:0:0:0:0
FF0E:0:0:0:0:0:0:0
FF0F:0:0:0:0:0:0:0

Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses four bits for each character (1 ~ 10, A ~ F). Each block's 16 bits are then represented by four hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

EUI-64

The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits fffe between the third and fourth bytes of the MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.

Table 189

MAC	00	:	13	:	49	:	12	:	34	:	56

Table 190

EUI-64	02	:	13	:	49	:	FF	:	FE	:	12	:	34	:	56

Stateless Autoconfiguration

With stateless autoconfiguration in IPv6, addresses can be uniquely and automatically generated. Unlike DHCPv6 (Dynamic Host Configuration Protocol version six) which is used in IPv6 stateful autoconfiguration, the owner and status of addresses don't need to be maintained by a DHCP server. Every IPv6 device is able to generate its own and unique IP address automatically when IPv6 is initiated on its interface. It combines the prefix and the interface ID (generated from its own Ethernet MAC address, see [Interface ID](#) and [EUI-64](#)) to form a complete IPv6 address.

When IPv6 is enabled on a device, its interface automatically generates a link-local address (beginning with fe80).

When the interface is connected to a network with a router and the Switch is set to automatically obtain an IPv6 network prefix from the router for the interface, it generates ³another address which combines its interface ID and global and subnet information advertised from the router. This is a routable global IP address.

DHCPv6

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 3315) is a server-client protocol that allows a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients. DHCPv6 servers and clients exchange DHCP messages using UDP.

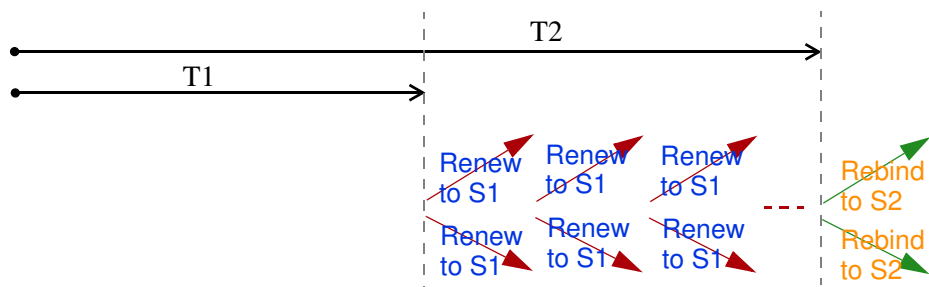
3. In IPv6, all network interfaces can be associated with several addresses.

Each DHCP client and server has a unique DHCP Unique Identifier (DUID), which is used for identification when they are exchanging DHCPv6 messages. The DUID is generated from the MAC address, time, vendor assigned ID and/or the vendor's private enterprise number registered with the IANA. It should not change over time even after you reboot the device.

Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.

The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses. An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (S1) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (S2). For an IA_TA, the client may send a Renew or Rebind message at the client's discretion.



DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The Switch uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the Switch passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor's reachability in a network. An IPv6 device uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor's link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being "reachable" means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.
- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and forward packets.
- Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The Switch maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the Switch configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the Switch also sends out a neighbor solicitation message. When the Switch receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the Switch uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The Switch creates an entry in the default router list cache if the router can be used as a default router.

When the Switch needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the Switch uses the prefix list to determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is onlink, the address is considered as the next hop. Otherwise, the Switch determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the Switch looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the Switch cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

Example - Enabling IPv6 on Windows XP/ 2003/ Vista

By default, Windows XP and Windows 2003 support IPv6. This example shows you how to use the `ipv6 install` command on Windows XP/2003 to enable IPv6. This also displays how to use the `ipconfig` command to see auto-generated IP addresses.

```
C:\>ipv6 install
Installing...
Succeeded.

C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IP Address. . . . . : 10.1.1.46
    Subnet Mask . . . . . : 255.255.255.0
    IP Address. . . . . : fe80::2d0:59ff:feb8:103c%4
    Default Gateway . . . . . : 10.1.1.254
```

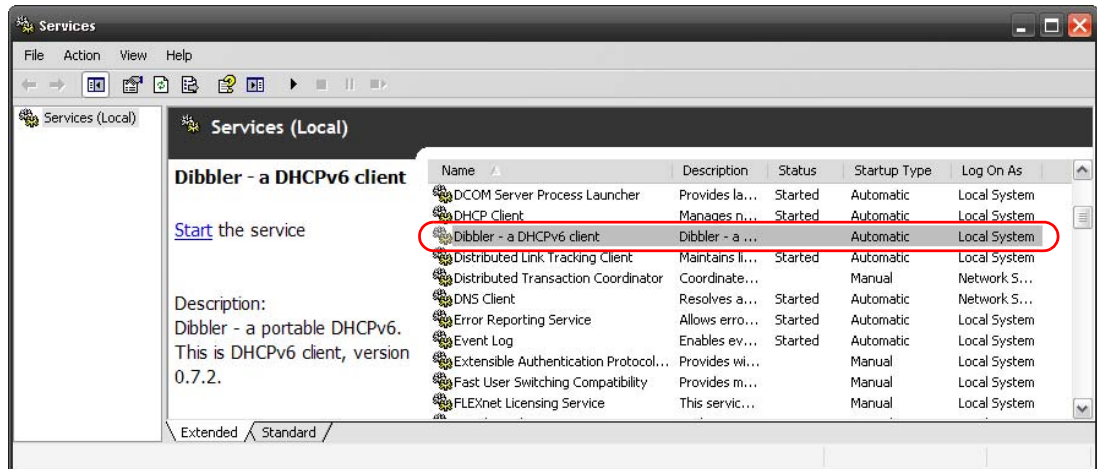
IPv6 is installed and enabled by default in Windows Vista. Use the `ipconfig` command to check your automatic configured IPv6 address as well. You should see at least one IPv6 address available for the interface on your computer.

Example - Enabling DHCPv6 on Windows XP

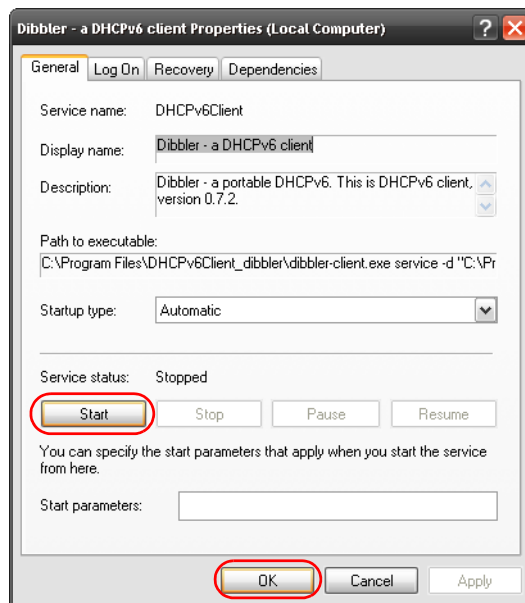
Windows XP does not support DHCPv6. If your network uses DHCPv6 for IP address assignment, you have to additionally install a DHCPv6 client software on your Windows XP. (Note: If you use static IP addresses or Router Advertisement for IPv6 address assignment in your network, ignore this section.)

This example uses Dibbler as the DHCPv6 client. To enable DHCPv6 client on your computer:

- 1 Install Dibbler and select the DHCPv6 client option on your computer.
- 2 After the installation is complete, select **Start > All Programs > Dibbler-DHCPv6 > Client Install as service**.
- 3 Select **Start > Control Panel > Administrative Tools > Services**.
- 4 Double click Dibbler - a DHCPv6 client.



- Click **Start** and then **OK**.



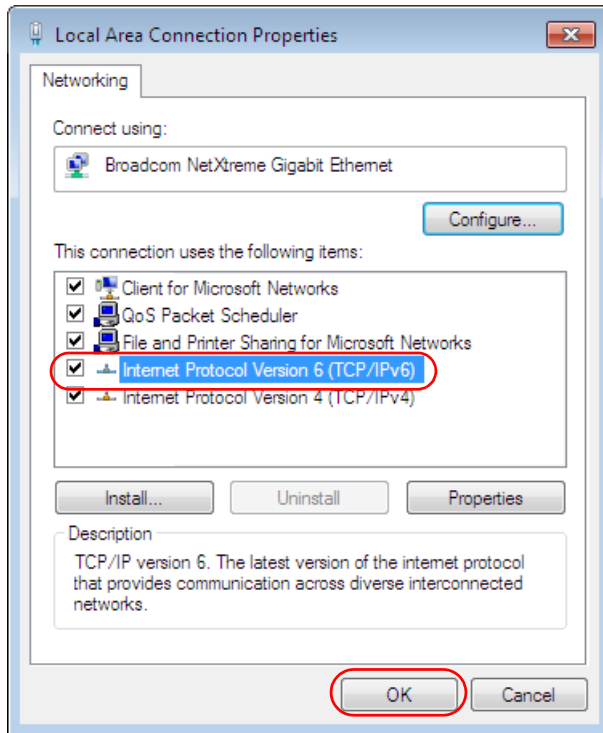
- Now your computer can obtain an IPv6 address from a DHCPv6 server.

Example - Enabling IPv6 on Windows 7

Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

- Select **Control Panel > Network and Sharing Center > Local Area Connection**.
- Select the **Internet Protocol Version 6 (TCP/IPv6)** checkbox to enable it.
- Click **OK** to save the change.



- 4 Click Close to exit the Local Area Connection Status screen.
- 5 Select Start > All Programs > Accessories > Command Prompt.
- 6 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

    Connection-specific DNS Suffix  . : 
    IPv6 Address. . . . . : 2001:b021:2d::1000
    Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
    IPv4 Address. . . . . : 172.16.100.61
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::213:49ff:feaa:7125%11
                                172.16.100.254
```

APPENDIX D

Legal Information

Copyright

Copyright © 2019 by Zyxel Communications Corporation.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel Communications Corporation.

Published by Zyxel Communications Corporation. All rights reserved.

Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Regulatory Notice and Statement

United States of America



The following information applies if you use the product within USA area.

Federal Communications Commission (FCC) EMC Statement

- This device complies with Part 15 of FCC rules. Operation is subject to the following two conditions:
 - (1) This device may not cause harmful interference.
 - (2) This device must accept any interference received, including interference that may cause undesired operations.
- Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
- This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canada

The following information applies if you use the product within Canada area.

Innovation, Science and Economic Development Canada ICES statement

CAN ICES-3 (A)/NMB-3(A)

European Union



The following information applies if you use the product within the European Union.

CE EMC statement

WARNING: This equipment is compliant with Class A of EN55032. In a residential environment this equipment may cause radio interference.

List of National Codes

COUNTRY	ISO 3166 2 LETTER CODE	COUNTRY	ISO 3166 2 LETTER CODE
Austria	AT	Liechtenstein	LI
Belgium	BE	Lithuania	LT
Bulgaria	BG	Luxembourg	LU
Croatia	HR	Malta	MT
Cyprus	CY	Netherlands	NL
Czech Republic	CR	Norway	NO
Denmark	DK	Poland	PL
Estonia	EE	Portugal	PT
Finland	FI	Romania	RO
France	FR	Serbia	RS
Germany	DE	Slovakia	SK
Greece	GR	Slovenia	SI
Hungary	HU	Spain	ES
Iceland	IS	Sweden	SE
Ireland	IE	Switzerland	CH
Italy	IT	Turkey	TR
Latvia	LV	United Kingdom	GB

Safety Warnings

- To avoid possible eye injury, do NOT look into an operating fiber-optic module's connector.
- Do not use this product near water, for example, in a wet basement or near a swimming pool.
- Do not expose your device to dampness, dust or corrosive liquids.
- Do not store things on the device.
- Do not obstruct the device ventilation slots as insufficient airflow may harm your device. For example, do not place the device in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do not install, use, or service this device during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the device.
- Do not open the device or unit. Opening or removing covers can expose you to dangerous high voltage points or other risks. Only qualified service personnel should service or disassemble this device. Please contact your vendor for further information.
- Make sure to connect the cables to the correct ports.
- Place connecting cables carefully so that no one will step on them or stumble over them.
- Always disconnect all cables from this device before servicing or disassembling.
- Do not remove the plug and connect it to a power outlet by itself; always attach the plug to the power adaptor first before connecting it to a power outlet.
- Do not allow anything to rest on the power adaptor or cord and do NOT place the product where anyone can walk on the power adaptor or cord.
- Please use the provided or designated connection cables/power cables/ adaptors. Connect it to the right supply voltage (for example, 110V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the device and the power source, repairing the power adapter or cord is prohibited. Contact your local vendor to order a new one.
- Do not use the device outside, and make sure all the connections are indoors. There is a remote risk of electric shock from lightning.
- Caution: Risk of explosion if battery is replaced by an incorrect type, dispose of used batteries according to the instruction. Dispose them at the applicable collection point for the recycling of electrical and electronic device. For detailed information about recycling of this product, please contact your local city office, your household waste disposal service or the store where you purchased the product.
- Use ONLY power wires of the appropriate wire gauge for your device. Connect it to a power supply of the correct voltage.
- Fuse Warning! Replace a fuse only with a fuse of the same type and rating.
- The POE (Power over Ethernet) devices that supply or receive power and their connected Ethernet cables must all be completely indoors.
- The following warning statements apply, where the disconnect device is not incorporated in the device or where the plug on the power supply cord is intended to serve as the disconnect device,
 - For permanently connected devices, a readily accessible disconnect device shall be incorporated external to the device;
 - For pluggable devices, the socket-outlet shall be installed near the device and shall be easily accessible.
- This device must be grounded by qualified service personnel. Never defeat the ground conductor or operate the device in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.
- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:
 - Install the power supply before connecting the power cable to the power supply.
 - Unplug the power cable before removing the power supply.
 - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supply.
- CLASS 1 LASER PRODUCT (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products).
- PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11. (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products)
- APPAREIL À LASER DE CLASS 1 (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products).

- PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11. (for products with mini-GBIC slots or laser products, such as fiber-optic transceiver and GPON products)

Environment Statement

European Union - Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.



台灣

警告使用者：

- 這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。」

安全警告 - 為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸
 - 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
 - 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝，使用或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請插在正確的電壓供給插座（如：北美 / 台灣電壓 110V AC，歐洲是 230V AC）。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。

- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 設備必須接地，接地導線不允許被破壞或沒有適當安裝接地導線，如果不確定接地方式是否符合要求可聯繫相應的電氣檢驗機構檢驗。
- 如果您提供的系統中有提供熱插拔電源，連接或斷開電源請遵循以下指導原則
 - 先連接電源線至設備連，再連接電源。
 - 先斷開電源再拔除連接至設備的電源線。
 - 如果系統有多個電源，需拔除所有連接至電源的電源線再關閉設備電源。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
 - 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
 - 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Explanation of the Symbols

SYMBOL	EXPLANATION
	Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction.
	Direct current (DC): DC 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 <http://www.zyxel.com> to view this product's documentation and certifications.

Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, Zyxel will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Zyxel shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive email notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Trademarks

ZyNOS (Zyxel Network Operating System) and ZON (Zyxel One Network) are registered trademarks of Zyxel Communications, Inc. Other trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Index

Numerics

802.1P priority [90](#)

A

AAA [203](#)

- accounting [203](#)
- authentication [203](#)
- authorization [203](#)
- external server [203](#)
- RADIUS [203](#)

AAA (Authentication, Authorization and Accounting) [204](#)

- access control
 - limitations [293](#)
 - login account [299](#)
 - remote management [301](#)
 - service port [300](#)
 - SNMP [303](#)

- accounting
 - setup [206](#)

Address Resolution Protocol (ARP) [275](#), [331](#), [336](#), [337](#)

administrator password [43](#), [299](#)

aging time [84](#)

- applications
 - backbone [23](#)
 - bridging [24](#)
 - fiber uplink [24](#)
 - IEEE 802.1Q VLAN [25](#)
 - PoE [22](#)
 - switched workgroup [24](#)

ARP

- how it works [275](#)
- learning mode [275](#)
- overview [275](#)
- setup [277](#)

ARP (Address Resolution Protocol) [331](#)

ARP-Reply [275](#)

ARP-Request [276](#)

authentication

- setup [206](#)

authentication, authorization and accounting [203](#)

Authentication, Authorization and Accounting, see AAA [204](#)

authorization

- setup [206](#)

auto-crossover [32](#)

automatic VLAN registration [115](#)

B

bandwidth control [154](#)

- egress rate [155](#)
- ingress rate [155](#)
- setup [154](#)

basic settings [79](#)

basic setup tutorial [68](#)

BPDUs [138](#)

Bridge Protocol Data Units (BPDUs) [138](#)

broadcast storm control [156](#)

C

cable diagnostics [314](#)

CDP [216](#)

certifications

- viewing [372](#)

CFI [114](#)

CFI (Canonical Format Indicator) [114](#)

changing the password [61](#)

Cisco Discovery Protocol, see CDP

CIST [152](#)

classifier [179](#)

- and QoS [179](#)
- editing [184](#)
- example [186](#)
- logging [185](#)

- match order [185](#)
- overview [179](#)
- setup [180](#), [184](#)
- status [179](#)
- viewing [184](#)
- cloning a port See port cloning
- cluster management [320](#)
 - and switch passwords [323](#)
 - cluster manager [320](#), [323](#)
 - cluster member [320](#), [323](#)
 - cluster member firmware upgrade [324](#)
 - network example [320](#)
 - setup [322](#)
 - specification [320](#)
 - status [321](#)
 - switch models [320](#)
 - VID [323](#)
 - web configurator [324](#)
- cluster manager [320](#)
- cluster member [320](#)
- Common and Internal Spanning Tree, See CIST [152](#)
- configuration [258](#)
 - change running config [283](#)
 - saving [62](#)
- configuration file
 - restore [286](#)
 - saving [282](#)
- contact information [352](#)
- copying port settings, See port cloning
- copyright [369](#)
- CPU management port [126](#)
- CPU protection [226](#)
- current date [82](#)
- current time [82](#)
- customer support [352](#)

D

- daylight saving time [83](#)
- default Ethernet settings [32](#)
- DHCP

- configuration options [262](#)
 - Dynamic Host Configuration Protocol [262](#)
 - modes [262](#)
 - Relay Agent Information format [264](#)

- setup [263](#)
- DHCPv4
 - global relay [266](#)
 - global relay example [268](#)
 - Option 82 [264](#)
 - option 82 profiles [265](#)
 - Relay Agent Information [264](#)
- DHCPv4 relay [264](#)
- DHCPv6 relay [273](#)
 - interface-ID [273](#)
 - remote-ID [273](#)
- diagnostics [313](#)
 - Ethernet port test [314](#)
 - ping [314](#)
- disclaimer [369](#)
- DNS [111](#)
- DNS (Domain Name System) [111](#)
- Domain Name System [111](#)
- dual firmware images [284](#)
- dynamic link aggregation [160](#)

E

- egress port [128](#)
- egress rate, and bandwidth control [155](#)
- errdisable status [229](#)
- error disable [226](#)
 - control packets [228](#)
 - CPU protection [229](#)
 - detect [230](#)
 - recovery [231](#)
 - status [227](#)
- error-disable recovery [226](#)
- Ethernet broadcast address [275](#), [331](#)
- Ethernet MAC [80](#)
- Ethernet port test [314](#)
- external authentication server [204](#)

F

- FCC interference statement [369](#)
- file transfer using FTP
 - command example [291](#)

- filename convention, configuration
 - configuration
 - file names [291](#)
- filtering [135](#)
 - rules [135](#)
- filtering database, MAC table [326](#)
- firmware [80](#)
 - upgrade [284](#), [324](#)
- flow control
 - back pressure [90](#)
 - IEEE802.3x [90](#)
- forwarding
 - delay [146](#)
- frames
 - tagged [122](#)
 - untagged [122](#)
- front panel [31](#)
- FTP [291](#)
 - file transfer procedure [291](#)
 - restrictions over WAN [292](#)

G

- GARP [115](#)
- GARP (Generic Attribute Registration Protocol) [115](#)
- GARP timer [84](#), [115](#)
- general setup [81](#)
- getting help [63](#)
- Gigabit ports [32](#)
- GMT (Greenwich Mean Time) [83](#)
- gratuitous ARP [276](#)
- green Ethernet [233](#)
 - and uplink port [233](#)
 - auto power down [233](#)
 - EEE [233](#)
 - short reach [233](#)
- GVRP [115](#), [122](#)
 - and port assignment [122](#)
- GVRP (GARP VLAN Registration Protocol) [115](#)

H

- hardware installation [27](#)

- hardware monitor [80](#)
- hardware overview [31](#)
- hello time [146](#)
- HTTPS [307](#)
 - certificates [307](#)
 - implementation [307](#)
 - public keys, private keys [307](#)
- HTTPS example [308](#)

I

- IEEE 802.1x
 - activate [169](#)
 - port authentication [167](#)
 - reauthentication [170](#)
- IEEE 802.3af [22](#)
- IEEE 802.3at [22](#)
- IEEE 802.3az [233](#)
- IEEE 802.3bt [22](#)
- IGMP filtering
 - profile [201](#)
- IGMP leave timeout
 - fast [199](#)
 - normal [199](#)
- IGMP snooping [195](#)
- IGMP throttling [199](#)
- ingress port [128](#)
- ingress rate, and bandwidth control [155](#)
- initial setup [64](#)
- installation
 - desktop [27](#)
 - precautions [28](#)
 - rack-mounting [28](#)
 - transceivers [33](#)
- installation scenarios [27](#)
- Internet Protocol version 6, see IPv6
- IP
 - interface [86](#), [87](#)
- IP address [86](#), [87](#)
- IP setup [85](#)
- IP subnet mask [86](#), [87](#)
- IP table [329](#)
 - how it works [329](#)
- IPv6 [361](#)

- addressing [361](#)
 - EUI-64 [363](#)
 - global address [361](#)
 - interface ID [363](#)
 - link-local address [361](#)
 - Neighbor Discovery Protocol [361](#)
 - neighbor table [339](#)
 - ping [361](#)
 - prefix [361](#)
 - prefix length [361](#)
 - stateless autoconfiguration [363](#)
 - unspecified address [362](#)
 - IPv6 interface [97](#)
 - DHCPv6 client [110](#)
 - enable [102](#)
 - global address [104](#)
 - global unicast address [99](#)
 - link-local address [103](#)
 - link-local IP [99](#)
 - neighbor discovery [105](#)
 - neighbor table [108](#)
 - stateless autoconfiguration [102](#)
 - status [98](#)
 - IPv6 neighbor table [339](#)
 - IPv6 static route
 - configuration [260](#)
- ## L
- L2PT [214](#)
 - access port [215](#)
 - CDP [214](#)
 - configuration [215](#)
 - encapsulation [214](#)
 - example [214](#)
 - LACP [215](#)
 - MAC address [214](#), [216](#)
 - mode [215](#)
 - overview [214](#)
 - PAgP [215](#)
 - point to point [215](#)
 - STP [214](#)
 - tunnel port [215](#)
 - UDLD [215](#)
 - VTP [214](#)
 - LACP [160](#), [217](#)
 - system priority [165](#)
 - timeout [165](#)
 - Layer 2 protocol tunneling, see L2PT
 - LEDs [35](#)
 - link aggregation [160](#)
 - dynamic [160](#)
 - ID information [161](#)
 - setup [162](#)
 - traffic distribution algorithm [162](#)
 - traffic distribution type [163](#)
 - trunk group [160](#)
 - Link Aggregation Control Protocol (LACP) [160](#)
 - Link Layer Discovery Protocol [235](#)
 - LLDP [235](#)
 - Basic TLV [250](#)
 - global settings [249](#)
 - local port status [239](#)
 - organization-specific TLV [251](#)
 - status of remote device [243](#)
 - TLV [235](#)
 - LLDP (Link Layer Discovery Protocol) [235](#)
 - LLDP-MED [236](#)
 - classes of endpoint devices [236](#)
 - example [236](#)
 - lockout [62](#)
 - log message [316](#)
 - login [39](#)
 - password [61](#)
 - login account
 - Administrator [299](#)
 - non-administrator [299](#)
 - login accounts [299](#)
 - configuring via web configurator [299](#)
 - multiple [299](#)
 - number of [299](#)
 - login password [299](#)
 - loop guard [211](#)
 - examples [212](#)
 - port shut down [212](#)
 - setup [213](#)
 - vs. STP [211](#)
- ## M
- MAC [80](#)
 - MAC (Media Access Control) [80](#)

- MAC address [80](#), [331](#)
 - maximum number per port [176](#)
 - MAC address learning [84](#), [176](#)
 - specify limit [176](#)
 - MAC table [326](#)
 - display criteria [328](#)
 - how it works [326](#)
 - sorting criteria [328](#)
 - transfer type [328](#)
 - viewing [327](#)
 - maintenance
 - firmware [284](#)
 - restoring configuration [286](#)
 - maintenance [280](#)
 - current configuration [281](#)
 - main screen [281](#)
 - Management Information Base (MIB) [303](#)
 - management IP address [85](#)
 - management port [128](#)
 - managing the device
 - good habits [26](#)
 - using FTP. See FTP. [25](#)
 - maximum transmission unit [335](#)
 - Mbuf [288](#)
 - Mbuf (Memory Buffer) [288](#)
 - MDIX (Media Dependent Interface Crossover) [32](#)
 - Media Access Control [80](#)
 - Memory Buffer [288](#)
 - MIB
 - and SNMP [303](#)
 - supported MIBs [304](#)
 - MIB (Management Information Base) [303](#)
 - mirroring ports [158](#)
 - monitor port [158](#)
 - mounting brackets [29](#)
 - MST Instance, See MSTI [152](#)
 - MST region [152](#)
 - MSTI [146](#), [152](#)
 - MSTI (Multiple Spanning Tree Instance) [146](#)
 - MSTP [137](#), [139](#)
 - bridge ID [149](#)
 - configuration digest [150](#)
 - forwarding delay [146](#)
 - Hello Time [149](#)
 - hello time [146](#)
 - Max Age [146](#), [149](#)
 - maximum hops [146](#)
 - revision level [146](#)
 - status [148](#)
 - MTU [335](#)
 - MTU (Multi-Tenant Unit) [83](#)
 - multicast
 - IGMP throttling [199](#)
 - IP addresses [195](#)
 - setup [196](#)
 - multicast group [201](#)
 - multicast MAC address [131](#)
 - Multiple Spanning Tree Protocol, See MSTP [137](#), [139](#)
 - Multiple STP [139](#)
 - Multi-Tenant Unit [83](#)
- ## N
- network applications [22](#)
 - network management system (NMS) [303](#)
 - NTP (RFC-1305) [82](#)
- ## O
- one-time schedule [177](#)
 - Option 82 [264](#)
- ## P
- PAGP [217](#)
 - password [61](#)
 - administrator [43](#), [299](#)
 - Path MTU [335](#)
 - Path MTU Discovery [335](#)
 - ping, test connection [314](#)
 - PoE
 - PD priority [96](#)
 - power management mode [95](#)
 - power-up mode [94](#)
 - PoE standard [22](#)
 - policy [188](#)
 - and classifier [188](#)

- and DiffServ [188](#)
 - configuration [188](#)
 - example [191](#)
 - overview [188](#)
 - rules [188](#)
 - Port Aggregation Protocol, see PAgP
 - port authentication [167](#)
 - guest VLAN [170](#)
 - IEEE802.1x [169](#)
 - MAC authentication [172](#)
 - method [169](#)
 - port cloning [336, 337](#)
 - advanced settings [336, 337](#)
 - basic settings [336, 337](#)
 - port details [342](#)
 - port mirroring [158](#)
 - port redundancy [160](#)
 - port security [175](#)
 - limit MAC address learning [176](#)
 - MAC address learning [175](#)
 - overview [175](#)
 - setup [175](#)
 - port setup [89](#)
 - port status [341](#)
 - port details [342](#)
 - port utilization [347](#)
 - port utilization [347](#)
 - port VLAN ID, see PVID [122](#)
 - port VLAN trunking [116](#)
 - port-based VLAN [126](#)
 - all connected [128](#)
 - port isolation [128](#)
 - settings wizard [128](#)
 - ports
 - diagnostics [314, 315](#)
 - mirroring [158](#)
 - speed/duplex [90](#)
 - standby [160](#)
 - power
 - voltage [81](#)
 - power connector [35](#)
 - power status [81](#)
 - PPPoE IA [218](#)
 - agent sub-options [220](#)
 - configuration [220](#)
 - drop PPPoE packets [222](#)
 - port state [220](#)
 - sub-option format [219](#)
 - tag format [218](#)
 - trusted ports [220](#)
 - untrusted ports [220](#)
 - VLAN [224](#)
 - PPPoE Intermediate Agent [218](#)
 - priority level [85](#)
 - priority queue assignment [85](#)
 - product registration [372](#)
 - PVID [115](#)
- ## Q
- QoS
 - and classifier [179](#)
 - queue weight [193](#)
 - queuing [192](#)
 - SPQ [192](#)
 - WRR [192](#)
 - queuing method [192, 194](#)
- ## R
- rack-mounting [28](#)
 - RADIUS [204](#)
 - advantages [204](#)
 - and tunnel protocol attribute [209](#)
 - setup [204](#)
 - Rapid Spanning Tree Protocol, See RSTP. [137](#)
 - rear panel connections [35](#)
 - reboot
 - load configuration [283](#)
 - reboot system [283](#)
 - recurring schedule [177](#)
 - registration
 - product [372](#)
 - remote management [301](#)
 - service [302](#)
 - trusted computers [302](#)
 - resetting [62, 282, 283, 284](#)
 - to custom default settings [284](#)
 - to factory default settings [282, 283](#)
 - restoring configuration [62, 286](#)

RFC 3164 [317](#)
Round Robin Scheduling [192](#)
routing table [333](#)
RSTP [137](#)
 configuration [140](#)
 status [142](#)
rubber feet [27](#)
running configuration [282](#)
 erase [282](#)
 reset [282](#)

S

save configuration [62](#), [282](#)
schedule
 one-time [177](#)
 recurring [177](#)
 type [178](#)
Secure Shell See SSH
service access control [300](#)
 service port [301](#)
Simple Network Management Protocol, see SNMP
Small Form-factor Pluggable (SFP) [32](#)
SNMP [303](#)
 agent [303](#)
 and MIB [303](#)
 authentication [298](#)
 communities [43](#), [295](#)
 management model [303](#)
 manager [303](#)
 MIB [304](#)
 network components [303](#)
 object variables [303](#)
 protocol operations [303](#)
 security [298](#)
 setup [294](#)
 traps [295](#)
 users [297](#)
 version 3 and security [303](#)
 versions supported [303](#)
SNMP traps [304](#)
 supported [304](#), [305](#)
Spanning Tree Protocol, See STP. [137](#)
SPQ (Strict Priority Queuing) [192](#)
SSH
 encryption methods [307](#)
 how it works [306](#)
 implementation [307](#)
SSH (Secure Shell) [306](#)
SSL (Secure Socket Layer) [307](#)
standby ports [160](#)
static MAC address [129](#)
static MAC forwarding [129](#)
static multicast address [131](#)
static multicast forwarding [131](#)
static route
 enable [259](#)
 metric [260](#)
 overview [258](#)
static routes [258](#)
static VLAN [119](#)
 control [120](#)
 tagging [120](#)
status [57](#), [73](#)
 MSTP [148](#)
 port [341](#)
 power [81](#)
 RSTP [142](#)
 VLAN [117](#)
STP [137](#), [216](#)
 bridge ID [143](#)
 bridge priority [141](#)
 designated bridge [138](#)
 edge port [142](#)
 forwarding delay [142](#)
 Hello BPDU [138](#)
 Hello Time [141](#), [143](#)
 how it works [138](#)
 Max Age [141](#), [143](#)
 path cost [138](#), [142](#)
 port priority [142](#)
 port role [144](#)
 port state [138](#), [143](#)
 root port [138](#)
 status [139](#)
 terminology [138](#)
 vs. loop guard [211](#)
switch lockout [62](#)
switch reset [62](#)
switch setup [84](#)
syslog [317](#)
 protocol [317](#)
 settings [317](#)

- setup [317](#)
- severity levels [317](#)
- system information [79](#)
- system reboot [283](#)

T

- TACACS+
 - advantages [204](#)
- tagged VLAN [114](#)
- Tech-Support [287](#)
 - log enhancement [287](#)
- temperature indicator [80](#)
- time
 - current [82](#)
- Time (RFC-868) [82](#)
- time range [177](#)
- time server [82](#)
- time service protocol [82](#)
 - format [82](#)
- trademarks [372](#)
- transceiver MultiSource Agreement (MSA) [32](#)
- transceivers [32](#)
 - installation [33](#)
 - removal [33](#)
- traps
 - destination [295](#)
- trunk group [160](#)
- trunking [160](#)
- trusted ports
 - PPPoE IA [220](#)
- tunnel protocol attribute
 - and RADIUS [209](#)
- tutorials [68](#)

U

- UDLD [217](#)
- UniDirectional Link Detection, see UDLD
- untrusted ports
 - PPPoE IA [220](#)
- user name [40](#)
 - default [40](#)

- user profiles [204](#)

V

- Vendor Specific Attribute, See VSA [208](#)
- ventilation holes [28](#)
- VID [88](#), [118](#)
 - number of possible VIDs [115](#)
 - priority frame [115](#)
- VID (VLAN Identifier) [114](#)
- Virtual Local Area Network [83](#)
- VLAN [83](#)
 - acceptable frame type [122](#)
 - automatic registration [115](#)
 - ID [114](#)
 - ingress filtering [122](#)
 - introduction [83](#), [114](#)
 - number of VLANs [118](#)
 - port number [118](#)
 - port settings [121](#)
 - port-based VLAN [126](#)
 - port-based, all connected [128](#)
 - port-based, isolation [128](#)
 - port-based, wizard [128](#)
 - PVID [122](#)
 - static VLAN [119](#)
 - status [117](#), [118](#), [119](#)
 - tagged [114](#)
 - terminology [115](#)
 - trunking [116](#), [122](#)
 - type [84](#), [117](#)
- VLAN (Virtual Local Area Network) [83](#)
- VLAN ID [114](#)
- VLAN number [86](#), [87](#), [88](#)
- VLAN terminology [115](#)
- VLAN trunking [122](#)
- VLAN Trunking Protocol, see VTP
- Voice VLAN [122](#)
- VSA [208](#)
- VTP [216](#)

W

- warranty [372](#)

- note [372](#)
- web configurator
 - getting help [63](#)
 - home [57](#)
 - login [39](#)
 - logout [63](#)
 - navigation panel [58](#)
- weight, queuing [193](#)
- Weighted Round Robin Scheduling (WRR) [193](#)
- WRR (Weighted Round Robin Scheduling) [192](#)

Z

- ZDP [44](#)
- ZON Utility [44](#)
- ZyNOS (ZyXEL Network Operating System) [291](#)
- ZyXEL Discovery Protocol [44](#)