

User's Guide

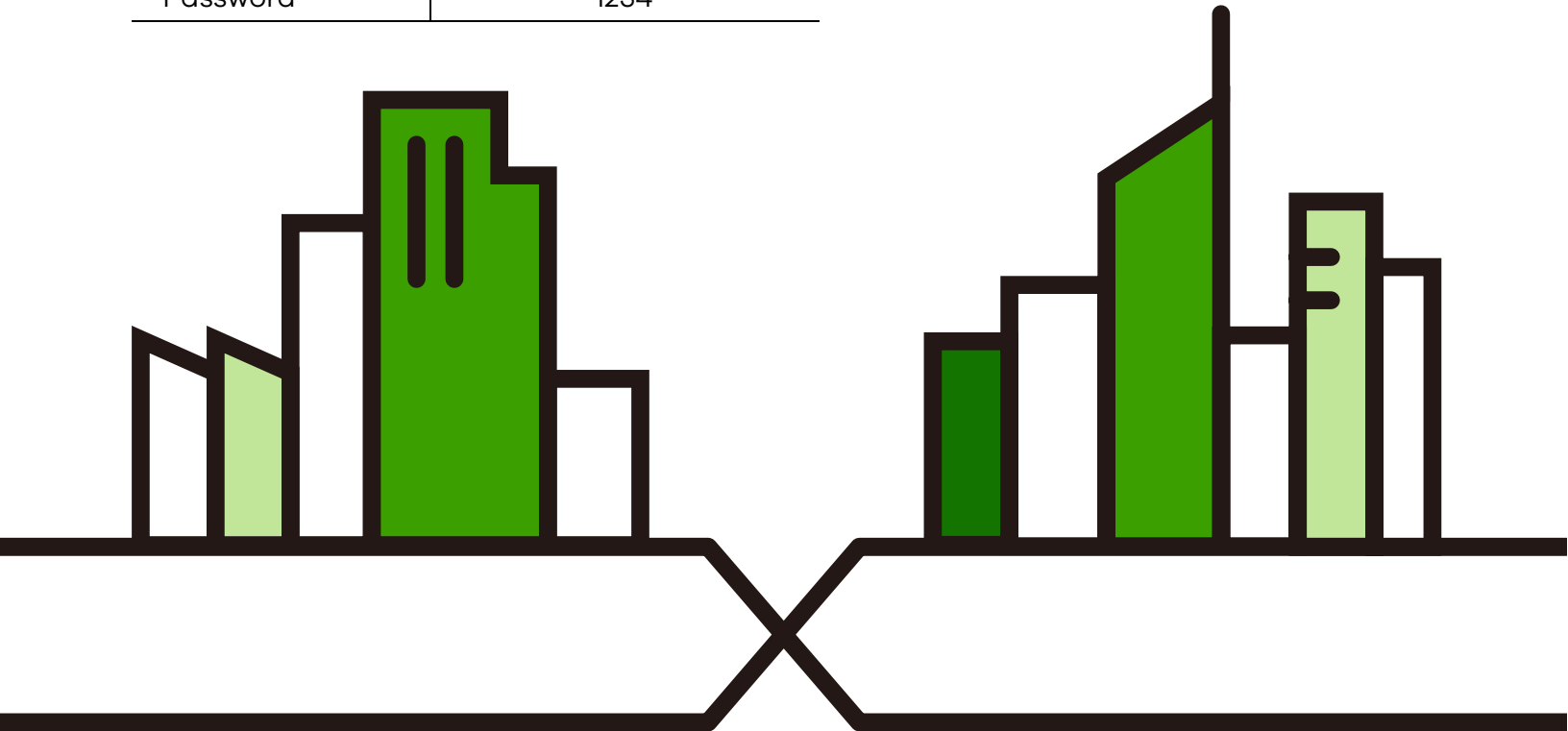
GS1915 Series

8/24-port Gigabit Smart Managed Layer-2 Switch

Default Login Details

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

Version 4.70 Edition 5, 12/2024



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.
- Web Configurator Online Help
Click the help link for a description of the fields in the Switch menus.
- Nebula Control Center (NCC) User's Guide
Go to nebula.zyxel.com or support.zyxel.com to get this User's Guide on how to configure the Switch using Nebula.
- More Information
Go to <https://community.zyxel.com/en> for product discussions.
Go to support.zyxel.com to find other information on the Switch.



Document Conventions

Warnings and Notes

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

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











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

Syntax Conventions

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

Icons Used in Figures

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

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

Contents Overview

| | |
|--|-----------|
| User's Guide | 17 |
| Getting to Know Your Switch | 18 |
| Hardware Installation and Connection | 27 |
| Hardware Panels | 33 |
| Technical Reference | 39 |
| Web Configurator | 40 |
| Initial Setup Example | 65 |
| Tutorials | 70 |
| Status | 78 |
| Basic Setting | 85 |
| VLAN | 118 |
| Static MAC Forwarding | 133 |
| Static Multicast Forwarding | 135 |
| Filtering | 138 |
| Spanning Tree Protocol | 140 |
| Bandwidth Control | 146 |
| Broadcast Storm Control | 148 |
| Mirroring | 150 |
| Link Aggregation | 152 |
| Port Security | 159 |
| Time Range | 162 |
| Queuing Method | 164 |
| Multicast | 167 |
| AAA | 173 |
| DHCP Snooping | 181 |
| Loop Guard | 192 |
| Error-Disable | 195 |
| Green Ethernet | 202 |
| Link Layer Discovery Protocol (LLDP) | 204 |
| Differentiated Services | 226 |
| DHCP | 230 |
| ARP Setup | 242 |
| Maintenance | 246 |
| Access Control | 259 |
| Diagnostic | 281 |
| System Log | 284 |
| Syslog Setup | 285 |

| | |
|---|------------|
| Cluster Management | 288 |
| MAC Table | 294 |
| ARP Table | 297 |
| Path MTU Table | 299 |
| Configure Clone | 300 |
| IPv6 Neighbor Table | 302 |
| Port Status | 304 |
| Troubleshooting and Appendices | 309 |
| Troubleshooting | 310 |

Table of Contents

| | |
|---|-----------|
| Document Conventions | 3 |
| Contents Overview | 4 |
| Table of Contents | 6 |
| | |
| Part I: User's Guide..... | 17 |
| | |
| Chapter 1 | |
| Getting to Know Your Switch | 18 |
| 1.1 Introduction | 18 |
| 1.1.1 Management Modes | 19 |
| 1.1.2 Mode Changing | 20 |
| 1.1.3 ZON Utility | 21 |
| 1.1.4 PoE | 22 |
| 1.2 Example Applications | 22 |
| 1.2.1 PoE Example Application | 23 |
| 1.2.2 Backbone Example Application | 23 |
| 1.2.3 Bridging Example | 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 | 26 |
| 1.4 Good Habits for Managing the Switch | 26 |
| | |
| Chapter 2 | |
| Hardware Installation and Connection | 27 |
| 2.1 Installation Scenarios | 27 |
| 2.2 Safety Precautions | 27 |
| 2.3 Desktop Installation Procedure | 27 |
| 2.4 Wall Mounting | 28 |
| 2.4.1 Installation Requirements | 28 |
| 2.5 Mounting the Switch on a Rack | 30 |
| 2.5.1 Installation Requirements | 30 |
| 2.5.2 Precautions | 31 |
| 2.5.3 Attaching the Mounting Brackets to the Switch | 31 |
| 2.5.4 Mounting the Switch on a Rack | 31 |
| | |
| Chapter 3 | |
| Hardware Panels..... | 33 |

| | |
|--|----|
| 3.1 Front Panel Connections | 33 |
| 3.1.1 Gigabit Ethernet Ports | 34 |
| 3.1.2 PoE (GS1915-8EP / GS1915-24EP) | 34 |
| 3.2 Rear Panel | 35 |
| 3.2.1 Grounding | 35 |
| 3.2.2 Power Connection | 37 |
| 3.3 LEDs | 37 |

Part II: Technical Reference..... 39

**Chapter 4
Web Configurator.....40**

| | |
|---|----|
| 4.1 Overview | 40 |
| 4.2 System Login | 40 |
| 4.3 Zyxel One Network (ZON) Utility | 44 |
| 4.3.1 Requirements | 44 |
| 4.3.2 Run the ZON Utility | 45 |
| 4.4 Wizard | 48 |
| 4.4.1 Basic | 49 |
| 4.4.2 Protection | 53 |
| 4.4.3 VLAN | 56 |
| 4.4.4 QoS | 57 |
| 4.5 Web Configurator Layout | 58 |
| 4.5.1 Change Your Password | 62 |
| 4.6 Save Your Configuration | 63 |
| 4.7 Switch Lockout | 63 |
| 4.8 Reset the Switch | 64 |
| 4.8.1 Restore/Reset Button | 64 |
| 4.9 Log Out of the Web Configurator | 64 |
| 4.10 Help | 64 |

**Chapter 5
Initial Setup Example.....65**

| | |
|--|----|
| 5.1 Overview | 65 |
| 5.1.1 Create a VLAN | 65 |
| 5.1.2 Set Port VID | 66 |
| 5.1.3 Configure Switch Management IP Address | 67 |

**Chapter 6
Tutorials.....70**

| | |
|--------------------|----|
| 6.1 Overview | 70 |
|--------------------|----|

| | |
|--|-----------|
| 6.2 How to Use DHCPv4 Snooping on the Switch | 70 |
| 6.3 How to Use DHCPv4 Relay on the Switch | 73 |
| 6.3.1 DHCP Relay Tutorial Introduction | 73 |
| 6.3.2 Create a VLAN | 74 |
| 6.3.3 Configure DHCPv4 Relay | 76 |
| 6.3.4 Troubleshooting | 76 |
| Chapter 7 | |
| Status..... | 78 |
| 7.1 Overview | 78 |
| 7.1.1 What You Can Do | 78 |
| 7.2 Status | 78 |
| 7.2.1 Neighbor Screen | 81 |
| 7.2.2 Neighbor Detail | 82 |
| Chapter 8 | |
| Basic Setting | 85 |
| 8.1 Overview | 85 |
| 8.1.1 What You Can Do | 85 |
| 8.2 System Information | 85 |
| 8.3 General Setup | 86 |
| 8.4 Switch Setup | 88 |
| 8.4.1 Introduction to VLANs | 88 |
| 8.4.2 Setting up | 89 |
| 8.5 IP Setup | 90 |
| 8.5.1 IP Interfaces | 90 |
| 8.5.2 IP Status | 91 |
| 8.5.3 IP Status Details | 91 |
| 8.5.4 IP Configuration | 93 |
| 8.5.5 Network Proxy Configuration | 95 |
| 8.6 Port Setup | 96 |
| 8.7 PoE Status | 97 |
| 8.7.1 PoE Time Range Setup | 99 |
| 8.7.2 PoE Setup | 100 |
| 8.8 Interface Setup | 103 |
| 8.9 IPv6 | 104 |
| 8.9.1 IPv6 Status | 104 |
| 8.9.2 IPv6 Interface Status | 105 |
| 8.9.3 IPv6 Configuration | 107 |
| 8.9.4 IPv6 Global Setup | 108 |
| 8.9.5 IPv6 Interface Setup | 109 |
| 8.9.6 IPv6 Link-Local Address Setup | 110 |
| 8.9.7 IPv6 Global Address Setup | 111 |

| | |
|--|------------|
| 8.9.8 IPv6 Neighbor Discovery Setup | 112 |
| 8.9.9 IPv6 Neighbor Setup | 113 |
| 8.9.10 DHCPv6 Client Setup | 114 |
| 8.10 Cloud Management | 115 |
| 8.10.1 Nebula Center Control Discovery | 117 |
| Chapter 9 | |
| VLAN..... | 118 |
| 9.1 Overview | 118 |
| 9.1.1 What You Can Do | 118 |
| 9.1.2 What You Need to Know | 118 |
| 9.2 Introduction to IEEE 802.1Q Tagged VLANs | 118 |
| 9.3 VLAN Status | 120 |
| 9.3.1 VLAN Details | 121 |
| 9.4 VLAN Configuration | 122 |
| 9.5 Configure a Static VLAN | 123 |
| 9.6 Configure VLAN Port Settings | 124 |
| 9.7 Voice VLAN | 125 |
| 9.8 MAC Based VLAN | 127 |
| 9.9 Vendor ID Based VLAN | 128 |
| 9.10 Port-Based VLAN Setup | 130 |
| 9.10.1 Configure a Port-Based VLAN | 130 |
| Chapter 10 | |
| Static MAC Forwarding..... | 133 |
| 10.1 Overview | 133 |
| 10.1.1 What You Can Do | 133 |
| 10.2 Configure Static MAC Forwarding | 133 |
| Chapter 11 | |
| Static Multicast Forwarding..... | 135 |
| 11.1 Static Multicast Forwarding Overview | 135 |
| 11.1.1 What You Can Do | 135 |
| 11.1.2 What You Need To Know | 135 |
| 11.2 Static Multicast Forwarding Configuration | 136 |
| Chapter 12 | |
| Filtering..... | 138 |
| 12.1 Filtering Overview | 138 |
| 12.1.1 What You Can Do | 138 |
| 12.2 Configure a Filtering Rule | 138 |
| Chapter 13 | |
| Spanning Tree Protocol | 140 |

| | |
|---|------------|
| 13.1 Spanning Tree Protocol Overview | 140 |
| 13.1.1 What You Can Do | 140 |
| 13.1.2 What You Need to Know | 140 |
| 13.2 Rapid Spanning Tree Protocol Status | 142 |
| 13.3 Configure Rapid Spanning Tree Protocol | 143 |
| Chapter 14 | |
| Bandwidth Control | 146 |
| 14.1 Bandwidth Control Overview | 146 |
| 14.1.1 What You Can Do | 146 |
| 14.2 Bandwidth Control Setup | 146 |
| Chapter 15 | |
| Broadcast Storm Control | 148 |
| 15.1 Broadcast Storm Control Overview | 148 |
| 15.1.1 What You Can Do | 148 |
| 15.2 Broadcast Storm Control Setup | 148 |
| Chapter 16 | |
| Mirroring | 150 |
| 16.1 Mirroring Overview | 150 |
| 16.2 Port Mirroring Setup | 150 |
| Chapter 17 | |
| Link Aggregation | 152 |
| 17.1 Link Aggregation Overview | 152 |
| 17.1.1 What You Can Do | 152 |
| 17.1.2 What You Need to Know | 152 |
| 17.2 Link Aggregation Status | 153 |
| 17.3 Link Aggregation Setting | 154 |
| 17.3.1 Link Aggregation Control Protocol | 156 |
| 17.4 Technical Reference | 157 |
| 17.4.1 Static Trunking Example | 157 |
| Chapter 18 | |
| Port Security | 159 |
| 18.1 Port Security Overview | 159 |
| 18.2 About Port Security | 159 |
| 18.3 Port Security Setup | 159 |
| Chapter 19 | |
| Time Range | 162 |
| 19.1 Time Range Overview | 162 |

| | |
|---|------------|
| 19.1.1 What You Can Do | 162 |
| 19.2 Configuring Time Range | 162 |
| Chapter 20 | |
| Queuing Method..... | 164 |
| 20.1 Queuing Method Overview | 164 |
| 20.1.1 What You Can Do | 164 |
| 20.1.2 What You Need to Know | 164 |
| 20.2 Configuring Queuing | 165 |
| Chapter 21 | |
| Multicast..... | 167 |
| 21.1 Multicast Overview | 167 |
| 21.1.1 What You Can Do | 167 |
| 21.1.2 What You Need to Know | 167 |
| 21.2 Multicast Setup | 168 |
| 21.3 IPv4 Multicast Status | 168 |
| 21.3.1 IGMP Snooping | 169 |
| 21.3.2 IGMP Snooping VLAN | 171 |
| Chapter 22 | |
| AAA..... | 173 |
| 22.1 Authentication, Authorization and Accounting (AAA) | 173 |
| 22.1.1 What You Can Do | 173 |
| 22.1.2 What You Need to Know | 173 |
| 22.2 AAA Screens | 174 |
| 22.3 RADIUS Server Setup | 174 |
| 22.4 AAA Setup | 176 |
| 22.5 Technical Reference | 178 |
| 22.5.1 Vendor Specific Attribute | 178 |
| 22.5.2 Supported RADIUS Attributes | 179 |
| 22.5.3 Attributes Used for Authentication | 180 |
| Chapter 23 | |
| DHCP Snooping..... | 181 |
| 23.1 DHCP Snooping Overview | 181 |
| 23.1.1 What You Can Do | 181 |
| 23.2 DHCP Snooping | 181 |
| 23.3 DHCP Snooping Configure | 184 |
| 23.3.1 DHCP Snooping Port Configure | 186 |
| 23.3.2 DHCP Snooping VLAN Configure | 187 |
| 23.3.3 DHCP Snooping VLAN Port Configure | 188 |
| 23.4 Technical Reference | 189 |

| | |
|--|------------|
| 23.4.1 DHCP Snooping Overview | 189 |
| Chapter 24 | |
| Loop Guard | 192 |
| 24.1 Loop Guard Overview | 192 |
| 24.1.1 What You Can Do | 192 |
| 24.1.2 What You Need to Know | 192 |
| 24.2 Loop Guard Setup | 194 |
| Chapter 25 | |
| Error-Disable | 195 |
| 25.1 Error-Disable Overview | 195 |
| 25.1.1 CPU Protection Overview | 195 |
| 25.1.2 Error-Disable Recovery Overview | 195 |
| 25.1.3 What You Can Do | 195 |
| 25.2 Error-Disable Settings | 196 |
| 25.3 Error-Disable Status | 196 |
| 25.4 CPU Protection Configuration | 198 |
| 25.5 Error-Disable Detect Configuration | 199 |
| 25.6 Error-Disable Recovery Configuration | 200 |
| Chapter 26 | |
| Green Ethernet | 202 |
| 26.1 Green Ethernet Overview | 202 |
| 26.2 Configuring Green Ethernet | 202 |
| Chapter 27 | |
| Link Layer Discovery Protocol (LLDP) | 204 |
| 27.1 LLDP Overview | 204 |
| 27.2 LLDP-MED Overview | 205 |
| 27.3 LLDP Settings | 206 |
| 27.4 LLDP Local Status | 207 |
| 27.4.1 LLDP Local Port Status Detail | 208 |
| 27.5 LLDP Remote Status | 211 |
| 27.5.1 LLDP Remote Port Status Detail | 212 |
| 27.6 LLDP Configuration | 218 |
| 27.6.1 LLDP Configuration Basic TLV Setting | 219 |
| 27.6.2 LLDP Configuration Org-specific TLV Setting | 220 |
| 27.7 LLDP-MED Configuration | 221 |
| 27.8 LLDP-MED Network Policy | 221 |
| 27.9 LLDP-MED Location | 223 |
| Chapter 28 | |
| Differentiated Services | 226 |

| | |
|--|------------|
| 28.1 DiffServ Overview | 226 |
| 28.1.1 What You Need to Know | 226 |
| 28.2 Activating DiffServ | 227 |
| 28.3 DSCP-to-IEEE 802.1p Priority Settings | 228 |
| 28.3.1 Configuring DSCP Settings | 229 |
| Chapter 29 | |
| DHCP | 230 |
| 29.1 DHCP Overview | 230 |
| 29.1.1 What You Can Do | 230 |
| 29.1.2 What You Need to Know | 230 |
| 29.2 DHCP Configuration | 231 |
| 29.3 DHCPv4 Status | 231 |
| 29.4 DHCPv4 Relay | 231 |
| 29.4.1 DHCPv4 Relay Agent Information | 232 |
| 29.4.2 DHCPv4 Option 82 Profile | 233 |
| 29.4.3 Configuring DHCPv4 Global Relay | 234 |
| 29.4.4 Configure DHCPv4 Global Relay Port | 235 |
| 29.4.5 Global DHCP Relay Configuration Example | 236 |
| 29.4.6 DHCPv4 VLAN Setting | 237 |
| 29.4.7 Configure DHCPv4 VLAN Port | 238 |
| 29.4.8 Example: DHCP Relay for Two VLANs | 239 |
| 29.5 DHCPv6 Relay | 240 |
| Chapter 30 | |
| ARP Setup..... | 242 |
| 30.1 ARP Overview | 242 |
| 30.1.1 What You Can Do | 242 |
| 30.1.2 What You Need to Know | 242 |
| 30.2 ARP Setup | 244 |
| 30.2.1 ARP Learning | 244 |
| Chapter 31 | |
| Maintenance..... | 246 |
| 31.1 Overview | 246 |
| 31.1.1 What You Can Do | 246 |
| 31.2 Maintenance Settings | 246 |
| 31.2.1 Erase Running-Configuration | 248 |
| 31.2.2 Save Configuration | 248 |
| 31.2.3 Reboot System | 248 |
| 31.2.4 Factory Default | 249 |
| 31.2.5 Custom Default | 249 |
| 31.3 Firmware Upgrade | 250 |

| | |
|--|------------|
| 31.4 Restore Configuration | 251 |
| 31.5 Backup Configuration | 252 |
| 31.6 Tech-Support | 252 |
| 31.6.1 Tech-Support Download | 254 |
| 31.7 Certificates | 254 |
| 31.7.1 HTTPS Certificates | 255 |
| 31.8 Technical Reference | 256 |
| 31.8.1 FTP Command Line | 256 |
| 31.8.2 Filename Conventions | 256 |
| 31.8.3 FTP Command Line Procedure | 257 |
| 31.8.4 GUI-based FTP Clients | 258 |
| 31.8.5 FTP Restrictions | 258 |
| Chapter 32 | |
| Access Control..... | 259 |
| 32.1 Access Control Overview | 259 |
| 32.1.1 What You Can Do | 259 |
| 32.2 Access Control Main Settings | 259 |
| 32.3 Configure SNMP | 260 |
| 32.3.1 Configure SNMP Trap Group | 261 |
| 32.3.2 Enable or Disable Sending of SNMP Traps on a Port | 262 |
| 32.3.3 Configure SNMP User | 263 |
| 32.4 Set Up Login Accounts | 265 |
| 32.5 Service Access Control | 266 |
| 32.6 Remote Management | 267 |
| 32.7 Account Security | 268 |
| 32.8 Technical Reference | 270 |
| 32.8.1 About SNMP | 270 |
| 32.8.2 SSH Overview | 273 |
| 32.8.3 Introduction to HTTPS | 275 |
| 32.8.4 Google Chrome Warning Messages | 279 |
| Chapter 33 | |
| Diagnostic..... | 281 |
| 33.1 Overview | 281 |
| 33.2 Diagnostic | 281 |
| Chapter 34 | |
| System Log..... | 284 |
| 34.1 Overview | 284 |
| 34.2 System Log | 284 |
| Chapter 35 | |
| Syslog Setup | 285 |

| | |
|--|------------|
| 35.1 Syslog Overview | 285 |
| 35.1.1 What You Can Do | 285 |
| 35.2 Syslog Setup | 285 |
| Chapter 36 | |
| Cluster Management..... | 288 |
| 36.1 Cluster Management Overview | 288 |
| 36.1.1 What You Can Do | 288 |
| 36.2 Cluster Management Status | 289 |
| 36.3 Clustering Management Configuration | 290 |
| 36.4 Technical Reference | 291 |
| 36.4.1 Cluster Member Switch Management | 291 |
| Chapter 37 | |
| MAC Table..... | 294 |
| 37.1 MAC Table Overview | 294 |
| 37.1.1 What You Can Do | 294 |
| 37.1.2 What You Need to Know | 294 |
| 37.2 Viewing the MAC Table | 295 |
| Chapter 38 | |
| ARP Table..... | 297 |
| 38.1 Overview | 297 |
| 38.1.1 What You Can Do | 297 |
| 38.1.2 What You Need to Know | 297 |
| 38.2 Viewing the ARP Table | 297 |
| Chapter 39 | |
| Path MTU Table | 299 |
| 39.1 Path MTU Overview | 299 |
| 39.2 Viewing the Path MTU Table | 299 |
| Chapter 40 | |
| Configure Clone..... | 300 |
| 40.1 Overview | 300 |
| 40.2 Configure Clone | 300 |
| Chapter 41 | |
| IPv6 Neighbor Table..... | 302 |
| 41.1 IPv6 Neighbor Table Overview | 302 |
| 41.2 Viewing the IPv6 Neighbor Table | 302 |
| Chapter 42 | |
| Port Status | 304 |

| | |
|--|------------|
| 42.1 Overview | 304 |
| 42.2 Port Status | 304 |
| 42.2.1 Port Details | 305 |
| 42.2.2 Port Utilization | 308 |
| | |
| Part III: Troubleshooting and Appendices..... | 309 |
| | |
| Chapter 43 | |
| Troubleshooting..... | 310 |
| 43.1 Power, Hardware Connections, and LEDs | 310 |
| 43.2 Switch Access and Login | 311 |
| 43.3 Switch Configuration | 313 |
| | |
| Appendix A Customer Support | 314 |
| | |
| Appendix B Common Services..... | 319 |
| | |
| Appendix C IPv6..... | 322 |
| | |
| Appendix D Legal Information | 330 |
| | |
| Index | 335 |

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 GS1915 Series consists of the following models:

- GS1915-8
- GS1915-8EP
- GS1915-24E
- GS1915-24EP

References to PoE models in this User's Guide only apply to GS1915-8EP and GS1915-24EP.

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

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

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

Table 1 GS1915 Series Comparison Table

| FEATURES | GS1915-8 | GS1915-8EP | GS1915-24E | GS1915-24EP |
|---|----------|------------|------------|-------------|
| Number of 10/100/1000 Mbps Ethernet ports | 8 | 8 | 24 | 24 |
| Number of 10/100/1000 Mbps PoE ports | 0 | 8 | 0 | 12 |
| Total system ports | 8 | 8 | 24 | 24 |
| Auto-Fan | Fanless | Fanless | Fanless | Yes |
| Rubber feet for desktop placement | Yes | Yes | Yes | Yes |
| Wall-mount | Yes | Yes | Yes | Yes |
| Rack-mount | No | No | Yes | Yes |
| Reboot Function | Yes* | Yes* | Yes* | Yes** |
| Note: * Press the RESTORE button for 3 to 6 seconds. ** Press the RESET button for 1 second. | | | | |
| Reset to Factory Default Function | Yes | Yes | Yes | Yes |
| Note: Press the RESTORE button for more than 6 seconds. | | | | |

1.1.1 Management Modes

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

Use the DHCP-assigned IP address to access the Web Configurator. To know the IP address, use the NCC, the ZON utility, or the console port if available. You can also use the domain name "setup.zyxel" to access the Web Configurator when you are directly connected to the Switch. Make sure your PC can connect to a DNS server via the switch.

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

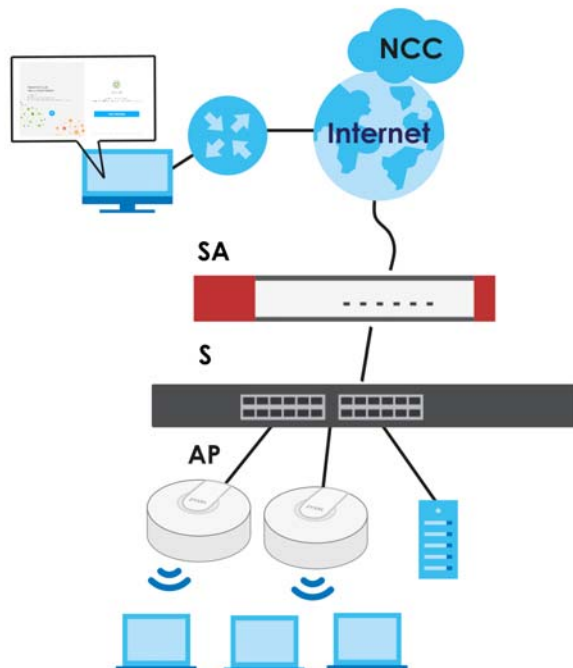
Nebula Cloud Management

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** in the Switch Web Configurator.

Note: See the Switch's datasheet for the feature differences between Nebula cloud and standalone 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.

Figure 1 NCC Example Network Topology



1.1.2 Mode Changing

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

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

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

From Standalone to Nebula Cloud Management

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

See the following steps or the Switch Quick Start Guide for 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.
 - Enter <https://nebula.zyxel.com> in a supported web browser. See the Nebula User's Guide for more information about supported browsers.
 - Click **Visit Nebula** in the Switch's login page.
 - Click the **Nebula** icon in the upper right of the Switch's Web Configurator.
- 2 Click **Get Started** in the Nebula web portal. Enter your myZyxel account information. You will be redirected to another screen where you can sign up for a myZyxel account if you do not have one.
- 3 Create an organization and a site (using the Nebula setup wizard) or select an existing organization.
- 4 Register the Switch by entering its Registration 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 **Start** on the first page. Click **Create account** to create a myZyxel account or enter your existing account information to log in.
- 2 Create an organization and site, or select an existing organization using the Zyxel Nebula Mobile app.
- 3 Select a site and scan the Switch's QR code or manually enter the information to add it to the site. You can find the QR code:
 - On a label on the Switch or
 - On its box or
 - In the Web Configurator at **Basic Setting > Cloud Management**.

See [Section 3.3 on page 37](#) for more information about the **CLOUD** LED or [Section 7.2 on page 78](#) for more information about the **Hybrid Mode** field in the **Status** screen to see if the Switch goes into Nebula cloud management mode successfully.

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. To access the Web Configurator when the Switch is in Cloud mode, use the Local credentials password to login.

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

Table 2 Management Method Comparison

| MODE | ACCESS | LOGIN USER NAME | LOGIN PASSWORD | LOGIN IP ADDRESS/URL |
|-----------------|------------------------------------|----------------------|----------------------------|---|
| Cloud mode | NCC (Nebula Control Center) portal | myZyxel account name | myZyxel account password | https://nebula.zyxel.com |
| | Web Configurator (Local GUI) * | admin | Local credentials password | http://setup.zyxel OR http://DHCP-assigned IP OR a configured static IP address |
| Standalone mode | Web Configurator | admin | 1234 | http://setup.zyxel OR http://DHCP-assigned IP OR http://192.168.1.1 |

* The Web Configurator (Local GUI) of Cloud mode supports limited features for troubleshooting use only.

From Nebula-managed to Standalone

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

To unregister the Switch:

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

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

1.1.3 ZON Utility

With its built-in Web Configurator, including the Neighbor Management feature ([Section 7.2.1 on page 81](#)), viewing, managing and configuring the Switch and its neighboring devices is simplified.

In addition, Zyxel offers a proprietary software program called Zyxel One Network (ZON) Utility, it is a utility tool that assists you to set up and maintain network devices in a more simple and efficient way.

You can download the ZON Utility at www.zyxel.com and install it on a PC (Windows operation system). For more information on ZON Utility see [Section 4.3 on page 44](#).

1.1.4 PoE

The Switch is a Power Sourcing Equipment (PSE) because it provides a source of power through 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) +

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

Table 3 GS1915 Series Models and PoE Features

| POE FEATURES | GS1915-8EP | GS1915-24EP |
|-----------------------|--|--|
| IEEE 802.3af PoE | Yes | Yes |
| IEEE 802.3at PoE+ | Yes | Yes |
| Power Management Mode | Consumption mode (default) / Classification mode | Consumption mode (default) / Classification mode |
| PoE Power Budget | 60 W | 130 W |

Table 4 PoE Standards

| POE FEATURES | PoE | PoE+ |
|------------------------|----------------|----------------|
| IEEE Standard | IEEE 802.3af | IEEE 802.3at |
| PoE Type | Type 1 | Type 2 |
| Switch Port Power | | |
| Maximum Power Per Port | 15.4 W | 30 W |
| Port Voltage Range | 44 – 57 V | 50 – 57 V |
| Cables | | |
| Twisted Pairs Used | 2-pair | 2-pair |
| Supported Cables | Cat3 or better | Cat5 or better |

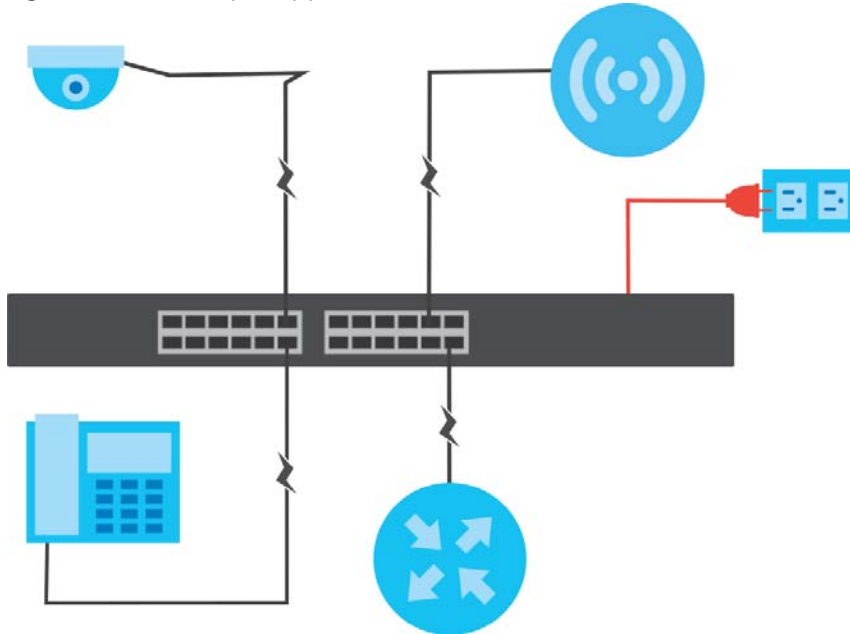
1.2 Example Applications

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

1.2.1 PoE Example Application

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

Figure 2 PoE Example Application

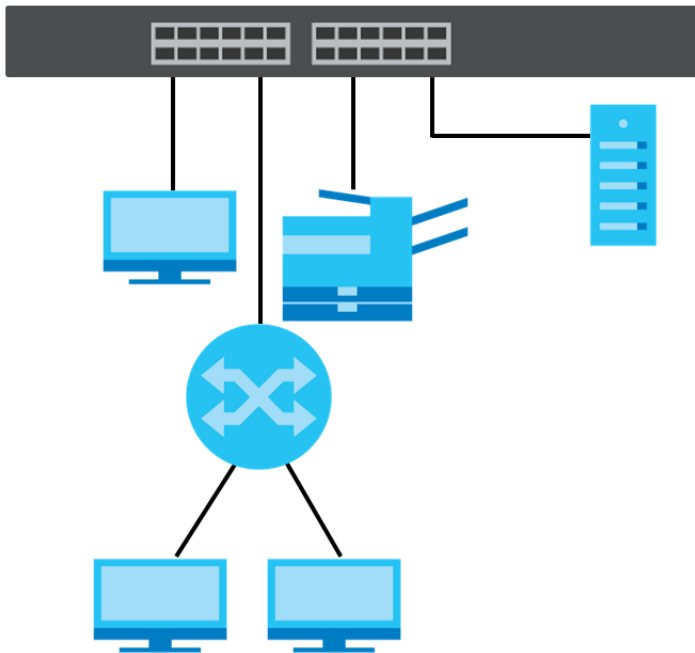


1.2.2 Backbone Example Application

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

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

Figure 3 Backbone Application

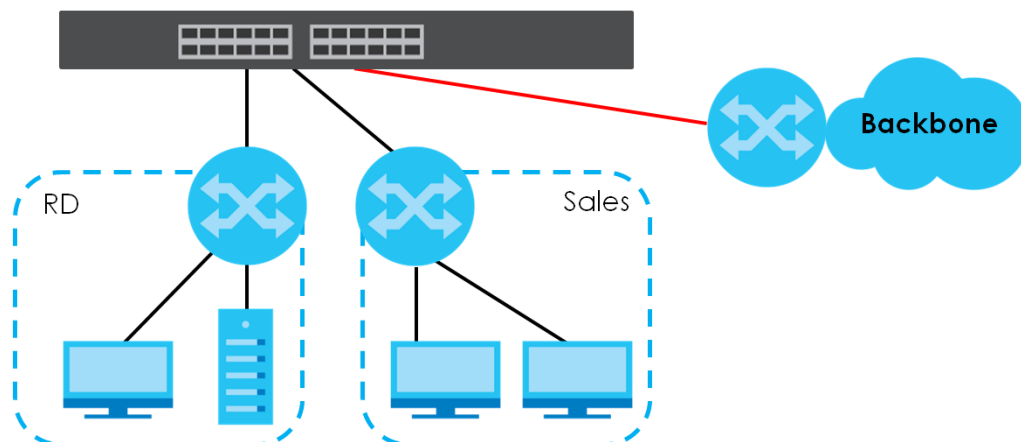


1.2.3 Bridging Example

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

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

Figure 4 Bridging Application



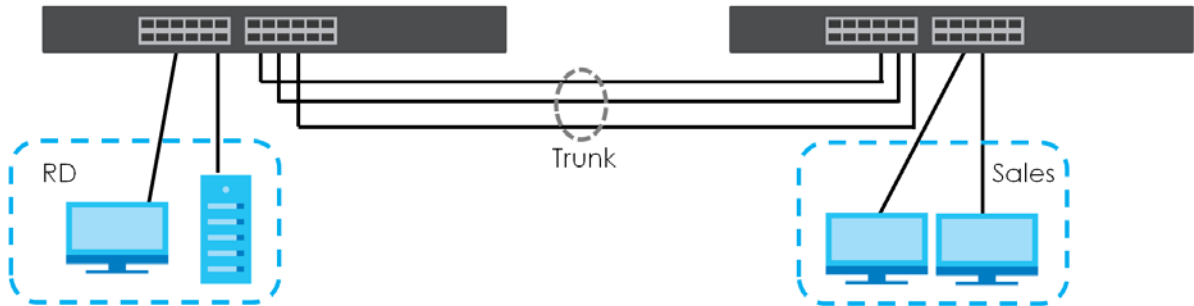
1.2.4 High Performance Switching Example

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

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

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

Figure 5 High Performance Switched Workgroup Application



1.2.5 IEEE 802.1Q VLAN Application Examples

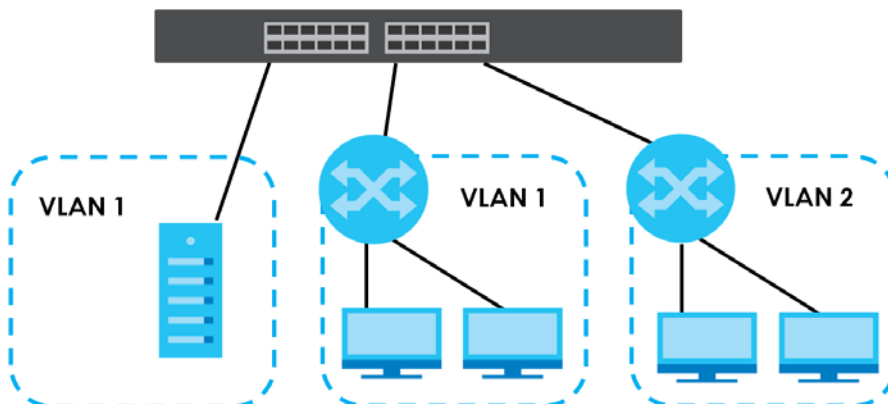
A VLAN (Virtual Local Area Network) allows a physical network to be partitioned into multiple logical networks. Stations on a logical network belong to one or more groups. With VLAN, a station cannot directly talk to or hear from stations that are not in the same groups unless such traffic first goes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

1.2.5.1 Tag-based VLAN Example

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

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

Figure 6 Shared Server Using VLAN Example



1.3 Ways to Manage the Switch

Use any of the following methods to manage the Switch.

- NCC (Zyxel Nebula Control Center). With the NCC, you can remotely manage and monitor the Switch through a cloud-based network management system. See the NCC User's Guide for detailed information about how to access the NCC and manage your Switch through the NCC. See the NCC User's Guide for how to configure Nebula managed devices.
- Web Configurator. This is recommended for everyday management of the Switch using a (supported) web browser. See [Chapter 4 on page 40](#).
- FTP. Use File Transfer Protocol for firmware upgrades and configuration backup or restore. See [Section 31.8.1 on page 256](#).
- SNMP. The Switch can be monitored and/or managed by an SNMP manager. See [Section 32.8.1 on page 270](#).
- Cluster Management. Cluster Management allows you to manage multiple switches through one switch, called the cluster manager. See [Chapter 36 on page 288](#).
- 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](#).

1.4 Good Habits for Managing the Switch

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

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

CHAPTER 2

Hardware Installation and Connection

2.1 Installation Scenarios

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

The Switch can be:

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

2.2 Safety Precautions

Please observe the following before using the Switch:

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

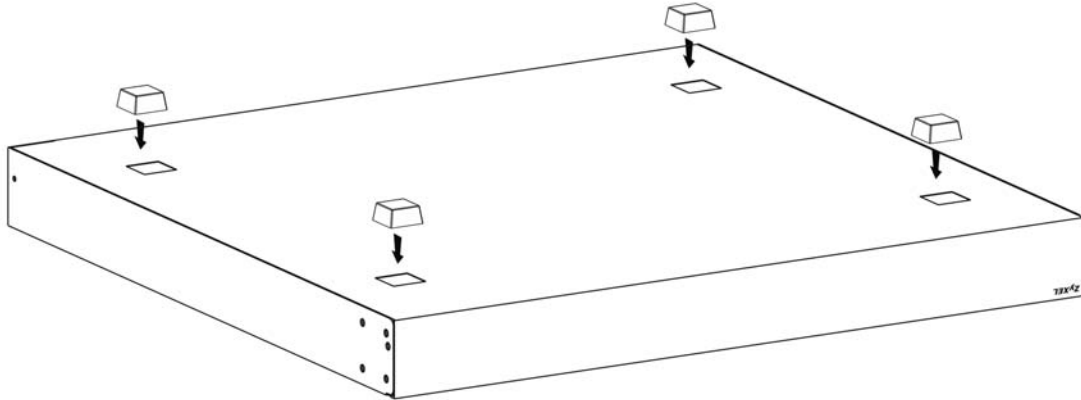
To start using the Switch, simply connect the power cables to turn it on.

2.3 Desktop Installation Procedure

- 1 Make sure the Switch is clean and dry.
- 2 Remove the adhesive backing from the rubber feet.

- 3 Attach the rubber feet to each corner on the bottom of the Switch. These rubber feet help protect the Switch from shock or vibration and ensure space between devices when stacking.

Figure 7 Attaching Rubber Feet



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

Cautions:

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

2.4 Wall Mounting

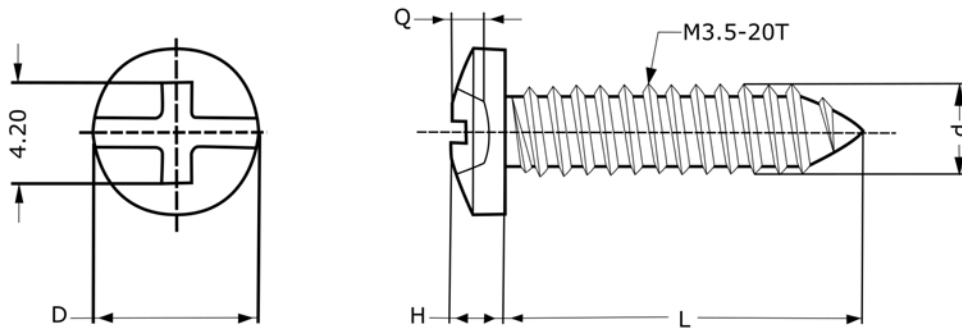
The Switch can be mounted on a wall. You may need screw anchors if mounting on a concrete or brick wall.

2.4.1 Installation Requirements

- Use screws with 6 mm – 8 mm (0.24" – 0.31") wide heads.
- The distance between the screws: 176 mm.

The following figure shows the screw specifications used for wall mounting.

- D = 7.00 mm
- H = 2.00 mm
- L = 15.50 mm
- d = 3.50 mm



Do the following to attach your Switch to a wall.

- 1 Select a position free of obstructions on a wall strong enough to hold the weight of the Switch.
- 2 Mark two holes on the wall at the appropriate distance apart for the screws.

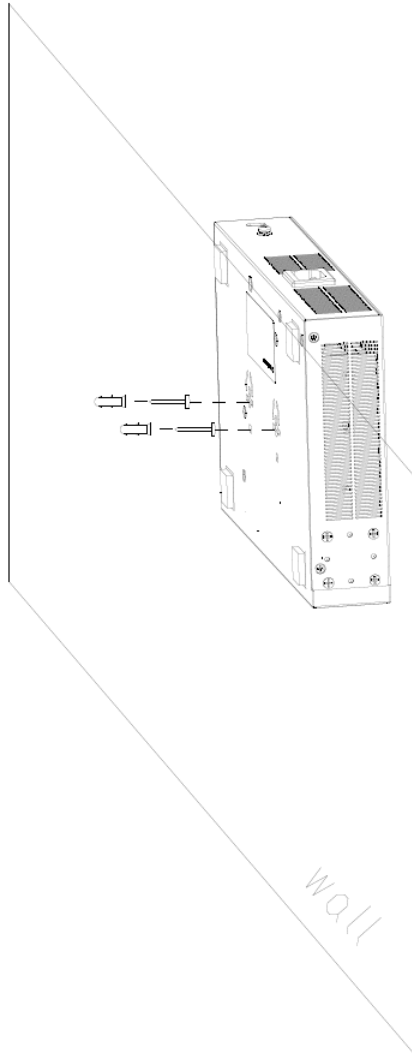
WARNING! Be careful to avoid damaging pipes or cables located inside the wall when drilling holes for the screws.

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

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

- 4 Make sure the screws are fastened well enough to hold the weight of the Switch with the connection cables.
- 5 Align the holes on the back of the Switch with the screws on the wall. Hang the Switch on the screws.

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



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

2.5 Mounting the Switch on a Rack

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

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

2.5.1 Installation Requirements

- Two mounting brackets.

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

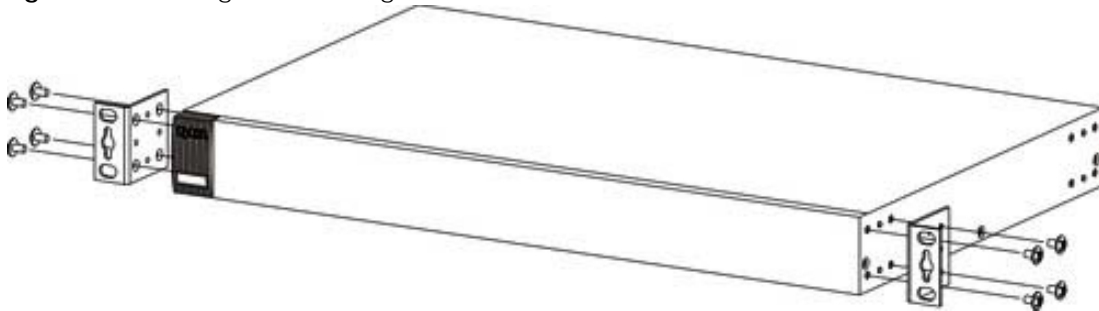
2.5.2 Precautions

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

2.5.3 Attaching the Mounting Brackets to the Switch

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

Figure 8 Attaching the Mounting Brackets

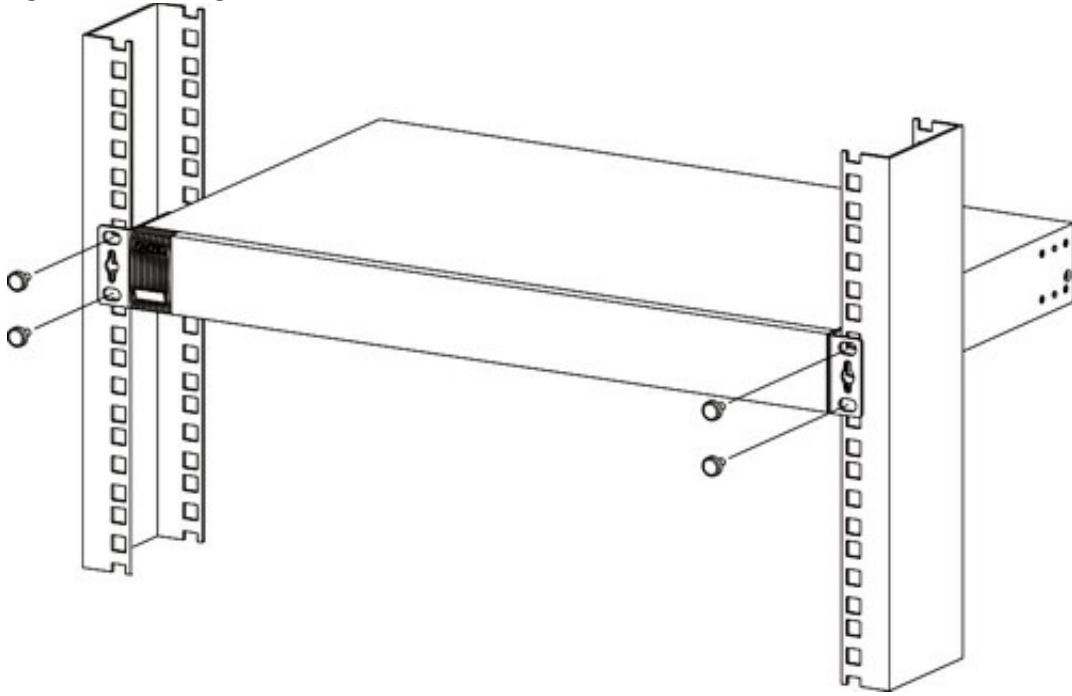


- 2 Using a #2 Philips screwdriver, install the M3 flat head screws through the mounting bracket holes into the Switch.
- 3 Repeat steps 1 and 2 to install the second mounting bracket on the other side of the Switch.
- 4 You may now mount the Switch on a rack. Proceed to the next section.

2.5.4 Mounting the Switch on a Rack

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

Figure 9 Mounting the Switch on a Rack



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

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

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

CHAPTER 3

Hardware Panels

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

3.1 Front Panel Connections

The following figures show the front panels of the Switch.

Figure 10 Front Panel: GS1915-8



Figure 11 Front Panel: GS1915-8EP



Figure 12 Front Panel: GS1915-24E



Figure 13 Front Panel: GS1915-24EP



The following table describes the ports.

Table 5 Panel Connections

| CONNECTOR | DESCRIPTION |
|--------------------------------------|--|
| 8/24 1000Base-T RJ-45 Ethernet Ports | These are 10/100/1000Base-T auto-negotiating and auto-crossover Ethernet ports. Connect these ports to a computer, a hub, a router, or an Ethernet switch. |
| 8/12 1000Base-T RJ-45 PoE Ports | These are 10/100/1000Base-T auto-negotiating and auto-crossover Ethernet ports. A PoE port is an Ethernet port that can supply power to a connected device. Connect these ports to a PoE-enabled IP camera / IP phone / AP, or an Ethernet switch. |

Table 5 Panel Connections (continued)

| CONNECTOR | DESCRIPTION |
|---|--|
| Restore | <p>Press the RESTORE button for 3 to 6 seconds to have the Switch automatically reboot. See Section 3.3 on page 37 for more information about the LED behavior.</p> <p>Press the RESTORE button for more than 6 seconds to have the Switch restore the factory default file. See Section 3.3 on page 37 for more information about the LED behavior.</p> |
| Reset (only available for GS1915-24EP) | <p>Press the RESET button to reboot the Switch without turning the power off. See Section 3.3 on page 37 for more information about the LED behavior.</p> |

3.1.1 Gigabit Ethernet Ports

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

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

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

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 using 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, thereby 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 or hubs.

3.1.2 PoE (GS1915-8EP / GS1915-24EP)

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

3.2 Rear Panel

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

Figure 14 Rear Panel: GS1915-8



Figure 15 Rear Panel: GS1915-8EP



Figure 16 Rear Panel: GS1915-24E



Figure 17 Rear Panel: GS1915-24EP



3.2.1 Grounding

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

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

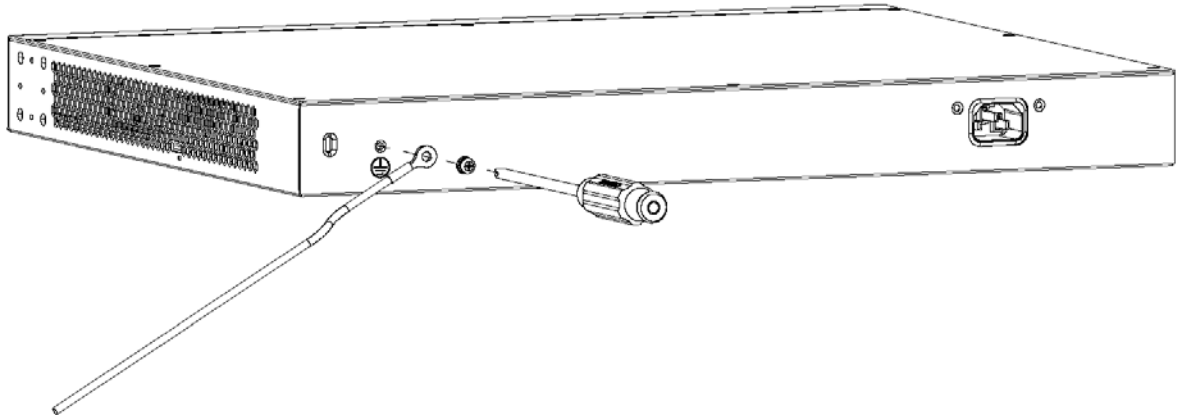
Installation of Ethernet cables must be separate from AC power lines. To avoid electric surge and electromagnetic interference, use a different electrical conduit or raceway (tube/trough or enclosed conduit for protecting electric wiring) that is 15 cm apart, or as specified by your country's electrical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

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

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

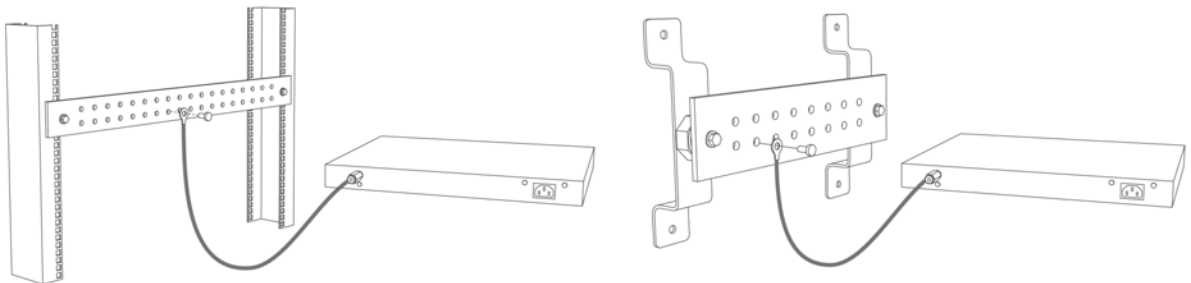
- 1 Remove the M4 ground screw from the Switch's rear panel.
- 2 Secure a green or yellow ground cable (16 AWG or smaller) to the Switch's rear panel using the M4 ground screw.

Figure 18 Grounding



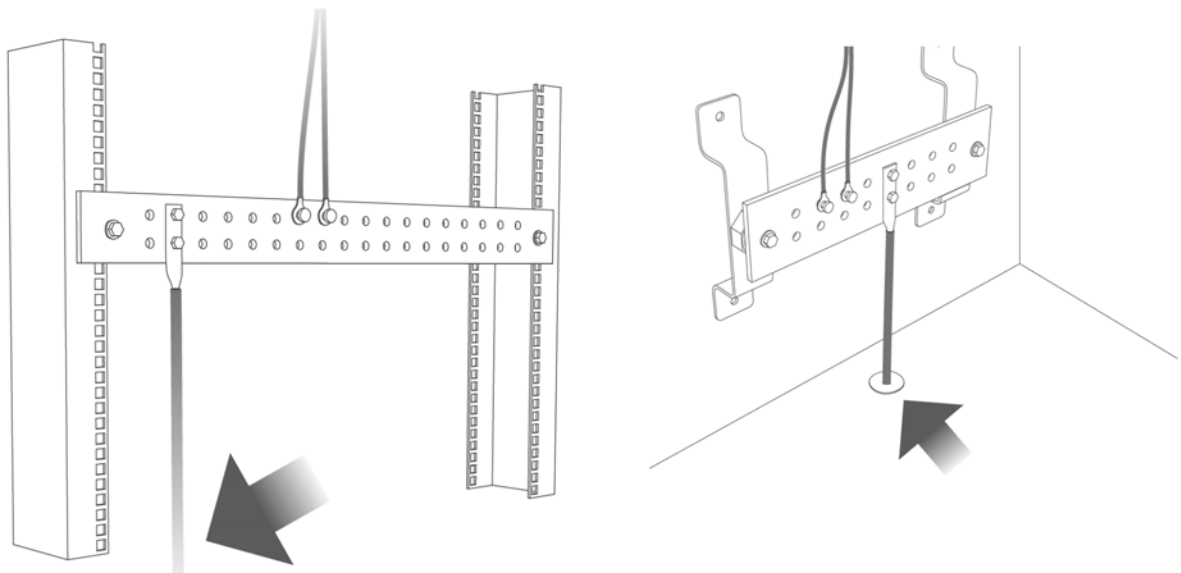
- 3 Attach the other end of the ground cable to a grounding bar located on the rack where you install the Switch or to an on-site grounding terminal.

Figure 19 Attach Ground Cable to Grounding Bar or On-site Grounding Terminal



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

Figure 20 Connecting to the Building's Main Grounding Electrode



If you are uncertain that suitable grounding is available, contact the appropriate electrical inspection

authority or an electrician.

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

3.2.2 Power Connection

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

Rear Panel Power Connection

Connect one end of the supplied power cord or power adapter to the power receptacle on the back of the Switch and the other end to the appropriate power source.

Connecting the Power

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

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

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

Disconnecting the Power

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

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

3.3 LEDs

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 6 LED Descriptions

| LED | COLOR | STATUS | DESCRIPTION |
|---------|-------|----------|--|
| PWR/SYS | Green | On | The Switch is receiving power from the power module in the power slot. |
| | | Blinking | The Switch is rebooting or reloading factory default file. |
| | | Off | The Switch is not receiving power from the power module in the power slot. |

Table 6 LED Descriptions (continued)

| LED | COLOR | STATUS | DESCRIPTION |
|---|-------|----------|---|
| CLOUD | Green | On | The Switch has successfully connected to the NCC (Nebula Control Center). |
| | | Blinking | The Switch cannot connect to the NCC because it is not registered or due to the Internet connection and other possible problems. |
| | | Off | The Switch is operating in standalone mode. Nebula Control Center Discovery is disabled in Basic Setting > Cloud Management in the Switch Web Configurator. |
| Ethernet Ports and PoE | | | |
| LNK/ACT | Green | On | The link to an Ethernet network is up. |
| | | Blinking | The Switch is transmitting or receiving to or from an Ethernet network. |
| | | Off | The link to an Ethernet network is down. |
| PoE Mode (GS1915-8EP / GS1915-24EP) | Green | On | Power is supplied through the Ethernet port. |
| | | Off | There is no power supplied. Note: If the PD is receiving power from an AC power source when connected to the Switch, the LED is off |

PART II

Technical Reference

CHAPTER 4

Web Configurator

4.1 Overview

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

The Web Configurator is an HTML-based management interface that allows easy system setup and management through Internet browser. Use a browser that supports HTML5, such as Microsoft Edge, Internet Explorer 11, Mozilla Firefox, or Google Chrome. The recommended minimum screen resolution is 1024 by 768 pixels.

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

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

4.2 System Login

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

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

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

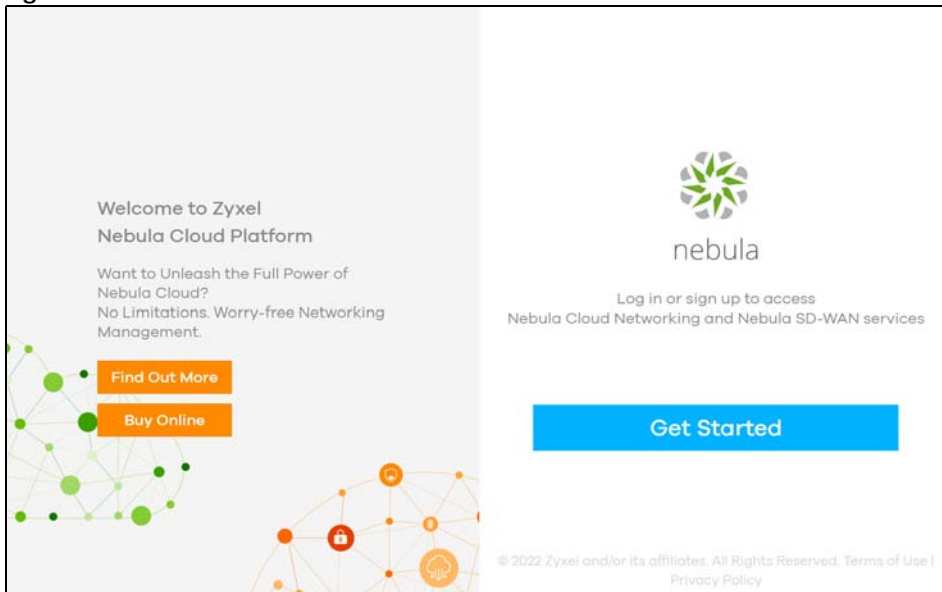
Also, you can use the ZON Utility to check your Switch's IP address. See [Section 4.3 on page 44](#) for more information on the ZON utility.

- 3 The following screen appears.

Figure 21 Web Configurator: Login and Visit Nebula

- 4 Click the **Visit Nebula** button if you want to open the Zyxel Nebula Control Center (NCC) login page in a new tab or window. The NCC is a cloud-based network management system that allows you to remotely manage and monitor the Switch. See the [Section on page 20](#) for information on changing your Switch to Nebula Cloud management.

Figure 22 Visit Nebula



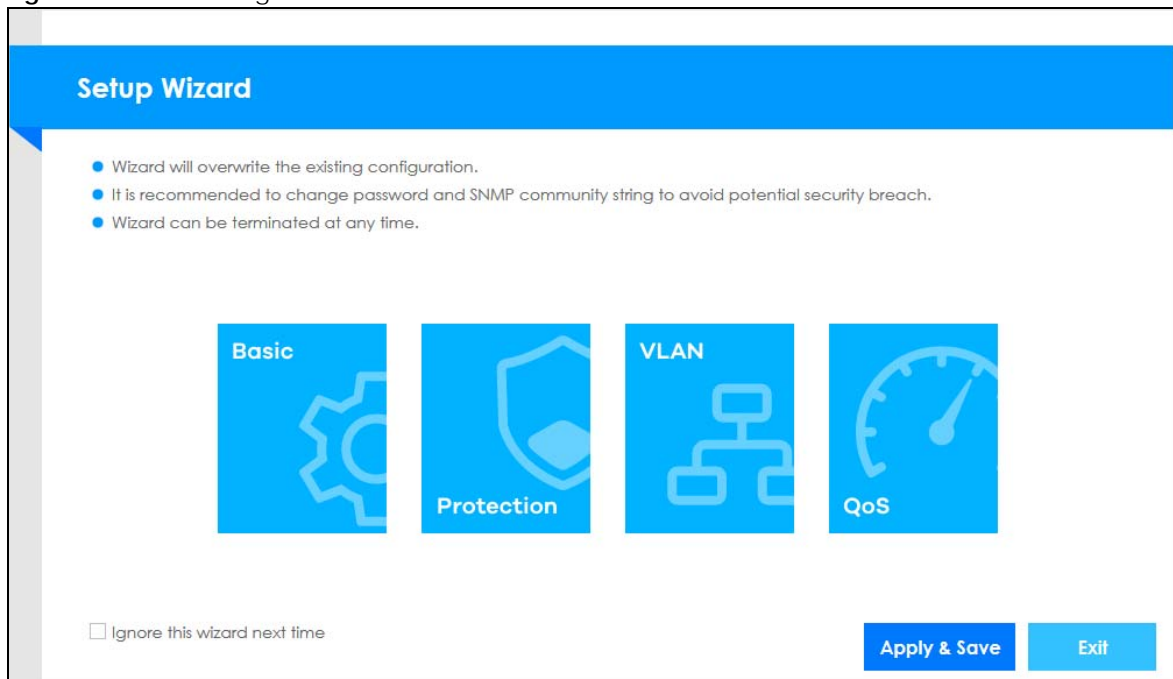
- 5 Alternatively, click **Login** to log into the Web Configurator to manage the Switch directly. The default user name is **admin** and associated default password is **1234**.

- The **Setup Wizard** screen will appear. You can use the **Setup Wizard** screen to configure the Switch's IP, login password, SNMP community, link aggregation, and view a summary of the settings. When you finish configuring the settings, you can click the **Apply & Save** button to make the settings take effect, and save your configuration into the Switch's non-volatile memory at once. Check the screens to see if the settings are applied.

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

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

Figure 23 Web Configurator: Wizard



- If you did not change the default administrator password and/or SNMP community values, a warning screen displays each time you log into the Web Configurator and select **Standard Mode**. Click **Password / SNMP** to open a screen where you can change the administrator password and SNMP community string simultaneously. Otherwise, click **Ignore** to close it.

Password/SNMP Setting

Figure 24 Web Configurator: Warning

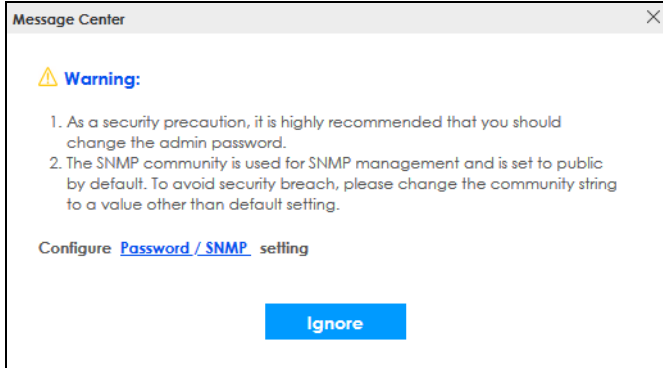


Figure 25 Web Configurator: Password

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

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

Table 7 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 | Enter the existing system password (1234 is the default password when shipped). |
| New Password | Enter your new system password. Up to 32 characters are allowed for the new password except [?], [], ['], ["], [space], or [,]. |
| Retype to confirm | Re-enter 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. |

Table 7 Web Configurator: Password/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 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 through Zyxel Discovery Protocol (ZDP) and in response to the query, the device responds back with basic information including IP address, firmware version, location, system and model name in the same broadcast domain. The information is then displayed in the ZON Utility screen and you can perform tasks like basic configuration of the devices and batch firmware upgrade in it. You can download the ZON Utility at www.zyxel.com and install it in a computer (Windows operating system).

4.3.1 Requirements

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

Operating System

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

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

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

Hardware

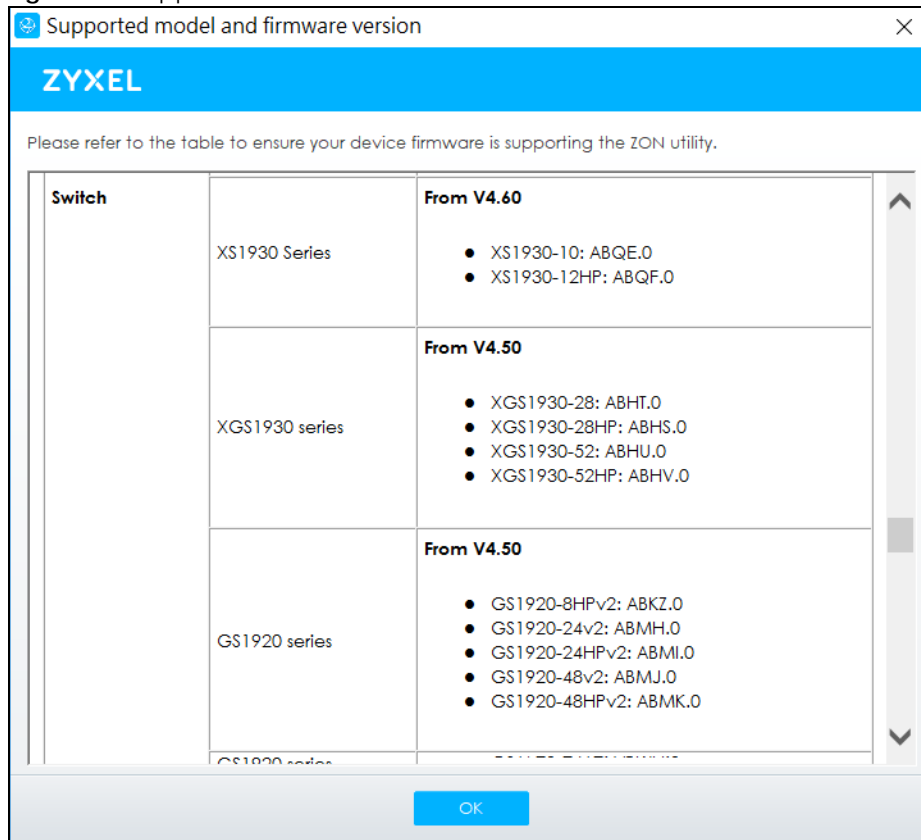
Here are the minimum hardware requirements to use the ZON Utility on your computer.

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

4.3.2 Run the ZON Utility

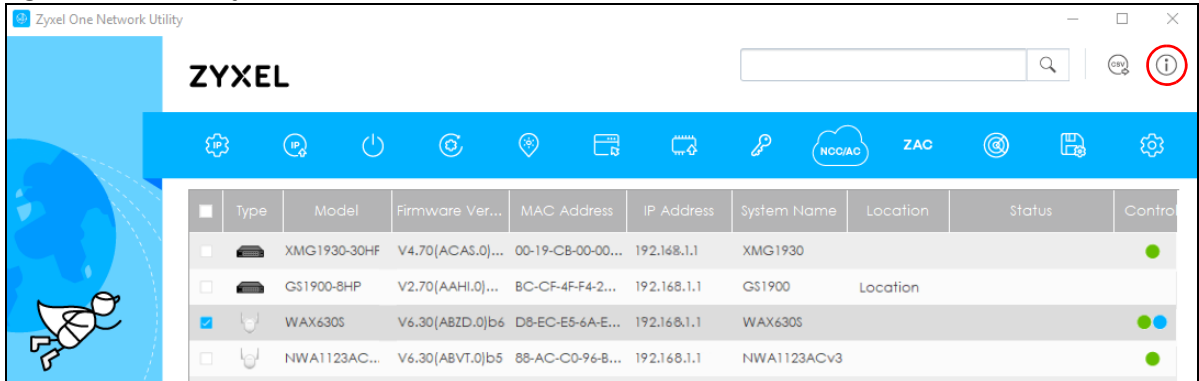
- 1 Double-click the ZON Utility to run it.
- 2 The first time you run the ZON Utility, you will see if your device and firmware version support the ZON Utility. Click the **OK** button to close this screen.

Figure 26 Supported Devices and Versions



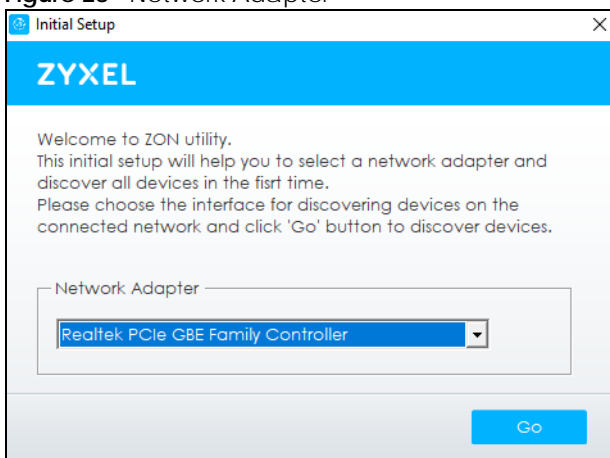
If you want to check the supported models and firmware versions later, you can click the **Show information about ZON** icon in the upper right of the screen. Then select the **Supported model and firmware version** link. If your device is not listed here, see the device release notes for ZON Utility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

Figure 27 ZON Utility Screen



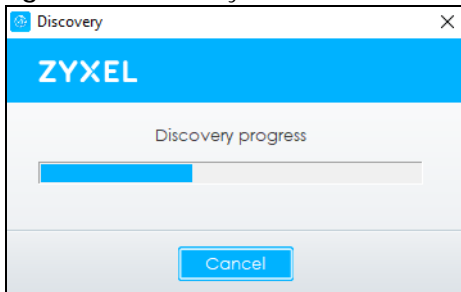
- 3 Select a network adapter to which your supported devices are connected.

Figure 28 Network Adapter



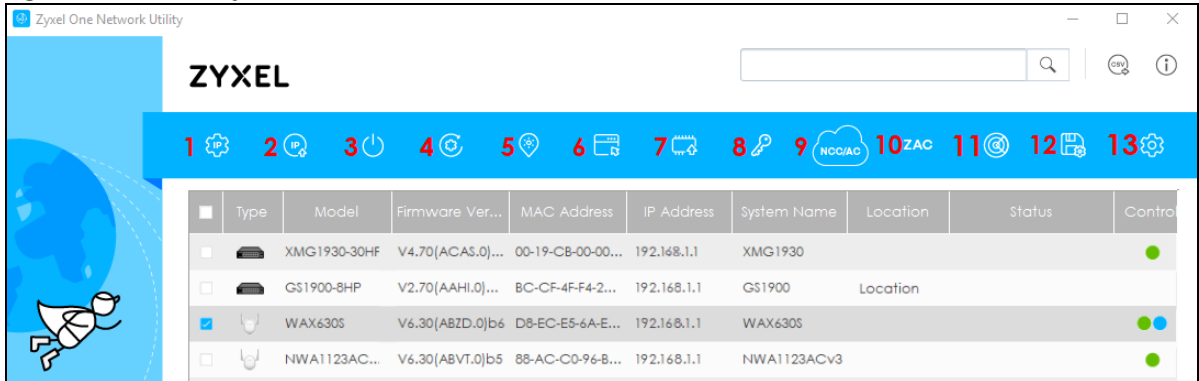
- 4 Click the **Go** button for the ZON Utility to discover all supported devices in your network.

Figure 29 Discovery



- 5 The ZON Utility screen shows the devices discovered.

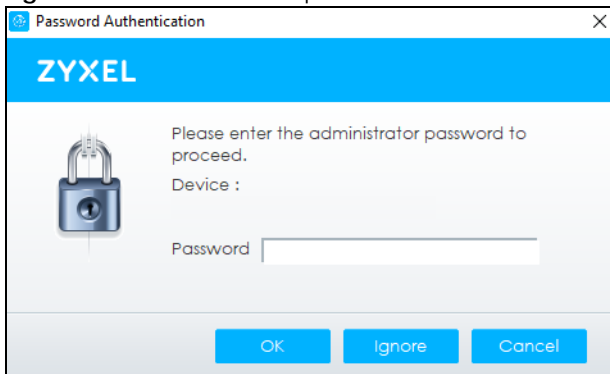
Figure 30 ZON Utility Screen



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

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

Figure 31 Password Prompt



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

Table 8 ZON Utility Icons

| ICON | DESCRIPTION |
|----------------------------------|---|
| 1 IP Configuration | Change the selected device's IP address. |
| 2 Renew IP Address | Update a DHCP-assigned dynamic IP address. |
| 3 Reboot Device | Use this icon to restart the selected devices. This may be useful when troubleshooting or upgrading new firmware. |
| 4 Reset Configuration to Default | Use this icon to reload the factory-default configuration file. This means that you will lose all previous configurations. |
| 5 Locator LED | Use this icon to locate the selected device by causing its Locator LED to blink. |
| 6 Web GUI | Use this to access the selected device Web Configurator from your browser. You will need a user name and password to log in. |
| 7 Firmware Upgrade | Use this icon to upgrade new firmware to selected devices of the same model. Make sure you have downloaded the firmware from the Zyxel website to your computer and unzipped it in advance. |
| 8 Change Password | Use this icon to change the admin password of the selected device. You must know the current admin password before changing to a new one. |

Table 8 ZON Utility Icons (continued)

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

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

Table 9 ZON Utility Fields

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

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 control 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 blue navigation bar with four steps: 1 IP, 2 Password, 3 Link Aggregation, and 4 Summary. The '1 IP' step is highlighted. Below the navigation bar, the title 'Setup IP' is displayed. The form contains the following fields:

- Host Name: GS1915
- IP Interface: Static IP Address DHCP Client
- VID: 1
- IP Address: 172.16.0.22
- IP Subnet Mask: 255.255.255.0
- Default Gateway: 172.16.0.254
- DNS Server: 172.16.0.1

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

Each field is described in the following table.

Table 10 Wizard > Basic > Step 1 IP

| LABEL | DESCRIPTION |
|-----------------|---|
| Host Name | This field displays a host name. Enter a string to set a new host name. The host name should not contain [?], [], ['], ["], or [,]. |
| IP Interface | Select DHCP Client if the Switch is connected to a router with the DHCP server enabled. You then need to check the router for the IP address assigned to the Switch in order to access the Switch's Web Configurator again. Select Static IP 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 | Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 192.168.1.254. |

Table 10 Wizard > Basic > Step 1 IP

| LABEL | DESCRIPTION |
|------------|--|
| DNS Server | DNS (Domain Name System) is for mapping a domain name to its corresponding IP address and so forth. Enter a domain name server IP address in order to be able to use a domain name instead of an IP address. |
| 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

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

Each field is described in the following table.

Table 11 Wizard > Basic > Step 2 Password

| LABEL | DESCRIPTION |
|--------------------------|---|
| Administrator's Password | |
| Current password | Enter the existing system password (1234 is the default password when shipped). |
| New password | Enter your new system password. Up to 32 characters are allowed for the new password except [?], [], ['], ["], [space], or [,]. |
| Confirm password | Reenter your new system password for confirmation. |
| SNMP | |
| SNMP | Select Enabled to let the Switch act as an SNMP agent, which allows a manager station to manage and monitor the Switch through the network. Select Disabled to turn this feature off. |

Table 11 Wizard > Basic > Step 2 Password (continued)

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

After clicking **Next**, the **Link Aggregation** screen appears.

Figure 34 Wizard > Basic > Step 3 Link Aggregation

The screenshot shows the 'Link Aggregation' configuration screen. At the top, a blue progress bar indicates the current step is '3 Link Aggregation'. Below this, the title 'Link Aggregation' is centered. On the left side, there are eight port icons labeled 'port1' through 'port8'. A legend at the bottom indicates that a light blue icon represents 'Unselected' and a dark blue icon represents 'Selected'. In the center, there is a dropdown menu labeled 'T1' with a right arrow button below it and a left arrow button below that. On the right side, there are four columns labeled 'T1', 'T2', 'T3', and 'T4'. Each column has a 'Static' dropdown menu at the top. At the bottom right, there are three buttons: 'Previous', 'Next', and 'Cancel'.

Each field is described in the following table.

Table 12 Wizard > Basic > Step 3 Link Aggregation

| LABEL | DESCRIPTION |
|------------------|--|
| Link Aggregation | |
| T1-Tx | 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 through 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: GS1915
 IP Interface: DHCP Client
 VID: 1
 IP Address: 172.21.40.8
 IP Subnet Mask: 255.255.252.0
 Default Gateway: 172.21.43.254
 DNS Server: 172.21.10.1

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 |
|-------|------|--------|
|-------|------|--------|

Previous Finish Cancel

Each field is described in the following table.

Table 13 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. |

Table 13 Wizard > Basic > Step 4 Summary (continued)

| LABEL | DESCRIPTION |
|---|--|
| Default Gateway | Enter 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. |
| 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 14 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

Each field is described in the following table.

Table 15 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

Each field is described in the following table.

Table 16 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

Each field is described in the following table.

Table 17 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 | Enter 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 groups 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 18 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 the Basic Setting > Port Setup screen 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 the Basic Setting > Port Setup screen 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 the Basic Setting > Port Setup screen to adjust the value. |
| Finish | Review the information and click Finish to create the task. |
| Cancel | Click Cancel to exit this screen without saving. |

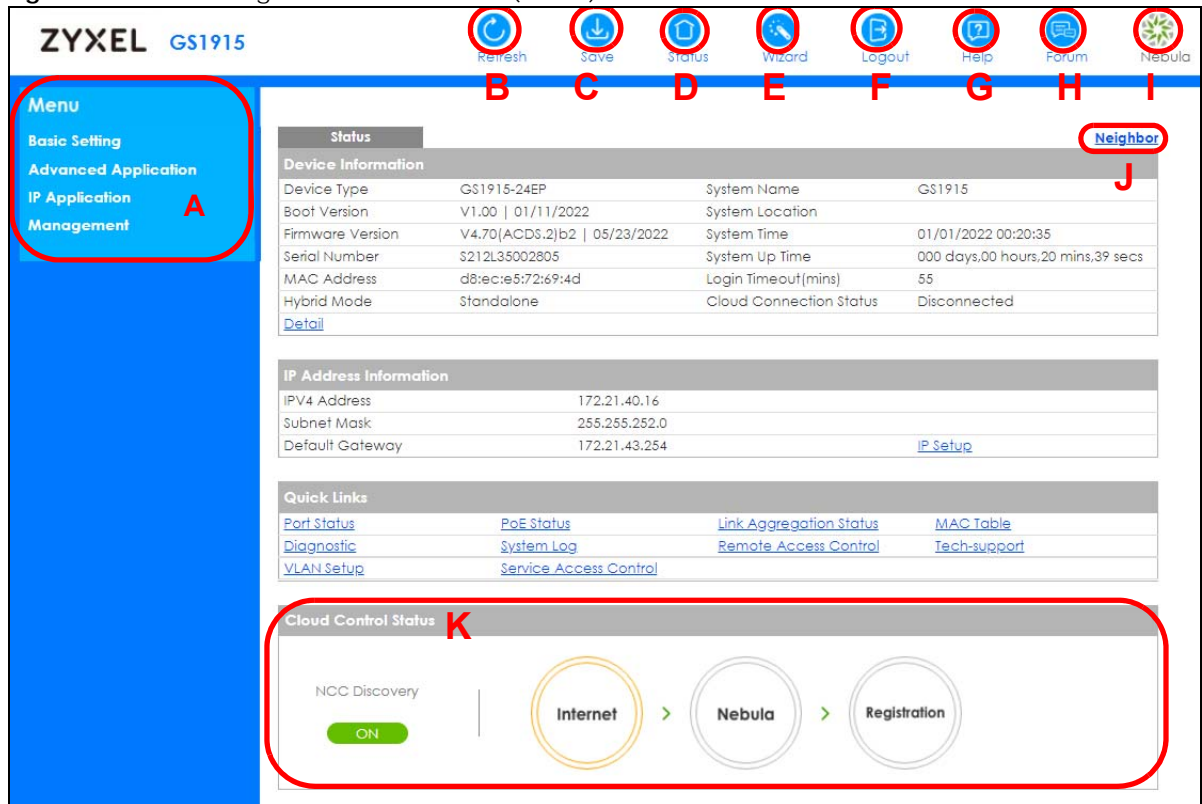
4.5 Web Configurator Layout

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

This guide uses GS1915-8EP screens as an example. The screens may vary slightly for different models.

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

Figure 41 Web Configurator Home Screen (Status)



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

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

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

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

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

E – Click this 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 configuration screens.

H – Click this link to go to the Zyxel Community Biz Forum.

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

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

K - This displays the Nebula Cloud Control Status. The ON/OFF switch displays if **NCC Discovery** is enabled. If a status circle turns Orange, it means the Switch is unable to connect to NCC. Hover the mouse over the status circle to check the diagnostic message. You can also click the ON/OFF switch to go to the **Basic Setting > Cloud Management** screen and check the diagnostic messages. See [Table 22 on page 79](#) for more information.

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

Table 19 Navigation Panel Sub-links Overview

| BASIC SETTING | ADVANCED APPLICATION | IP APPLICATION | MANAGEMENT |
|--|--|---|--|
| Menu Basic Setting Advanced Application IP Application Management <hr/> System Info General Setup Switch Setup IP Setup Port Setup PoE Setup Interface Setup IPv6 Cloud Management | Menu Basic Setting Advanced Application IP Application Management <hr/> VLAN Static MAC Forwarding Static Multicast Forwarding Filtering Spanning Tree Protocol Bandwidth Control Broadcast Storm Control Mirroring Link Aggregation Port Security Time Range Queuing Method Multicast AAA DHCP Snooping Loop Guard Errdisable Green Ethernet LLDP | Menu Basic Setting Advanced Application IP Application Management <hr/> DiffServ DHCP ARP Setup | Menu Basic Setting Advanced Application IP Application Management <hr/> Maintenance Access Control Diagnostic System Log Syslog Setup Cluster Management MAC Table ARP Table Path MTU Table Configure Clone IPv6 Neighbor Table Port Status |

The following table describes the links in the navigation panel.

Table 20 Navigation Panel Links

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

Table 20 Navigation Panel Links (continued)

| LINK | DESCRIPTION |
|-----------------------------|--|
| PoE Setup | For PoE models. This link takes you to a screen where you can set priorities, PoE power-up settings and schedule so that the Switch is able to reserve and allocate power to certain PDs. |
| Interface Setup | This link takes you to a screen where you can configure settings for individual interface type and ID. |
| IPv6 | This link takes you to a screen where you can view IPv6 status and configure IPv6 settings. |
| Cloud Management | This link takes you to a screen where you can enable or disable the Nebula Control Center (NCC) Discovery feature and view the NCC connection status. If Nebula Control Center (NCC) Discovery is enabled, you can have the Switch search for the NCC. The screen also displays a QR code containing the Switch's serial number and MAC address for handy registration of the Switch at NCC. |
| Advanced Application | |
| VLAN | This link takes you to screens where you can configure port-based or 802.1Q VLAN (depending on what you configured in the Switch Setup menu). You can also configure a voice VLAN, a MAC based VLAN or a vendor ID based VLAN in these screens. |
| Static MAC Forwarding | This link takes you to a screen where you can configure static MAC addresses for a port. These static MAC addresses do not age out. |
| Static Multicast Forwarding | This link takes you to a screen where you can configure static multicast MAC addresses for ports. These static multicast MAC addresses do not age out. |
| Filtering | This link takes you to a screen to set up filtering rules. |
| Spanning Tree Protocol | This link takes you to screens where you can configure the RSTP to prevent network loops. |
| Bandwidth Control | This link takes you to a screen where you can configure bandwidth limits on the Switch. |
| Broadcast Storm Control | This link takes you to a screen to set up broadcast filters. |
| Mirroring | This link takes you to screens where you can copy traffic from one port or ports to another port in order that you can examine the traffic from the first port without interference. |
| Link Aggregation | This link takes you to screens where you can logically aggregate physical links to form one logical, higher-bandwidth link. |
| Port Security | This link takes you to a screen where you can activate MAC address learning and set the maximum number of MAC addresses to learn on a port. |
| Time Range | This link takes you to a screen where you can define different schedules. |
| Queuing Method | This link takes you to a screen where you can configure queuing with associated queue weights for each port. |
| Multicast | This link takes you to screens where you can configure various multicast features and IGMP snooping. |
| AAA | This link takes you to a screen where you can configure authentication, authorization and accounting services through external servers. The external servers should be RADIUS (Remote Authentication Dial-In User Service). |
| DHCP Snooping | This link takes you to screens where you can configure filtering of unauthorized DHCP packets in your network. |
| Loop Guard | This link takes you to a screen where you can configure protection against network loops that occur on the edge of your network. |
| 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. |

Table 20 Navigation Panel Links (continued)

| LINK | DESCRIPTION |
|---------------------|---|
| IP Application | |
| DiffServ | This link takes you to screens where you can enable DiffServ, configure marking rules and set DSCP-to-IEEE802.1p mappings. |
| DHCP | This link takes you to screens where you can configure the DHCP settings. |
| ARP Setup | This link takes you to screens where you can configure the ARP learning settings for each port. |
| Management | |
| Maintenance | This link takes you to screens where you can perform firmware and configuration file maintenance as well as reboot the system. |
| Access Control | This link takes you to screens where you can change the system login password and configure SNMP and remote management. |
| Diagnostic | This link takes you to a screen where you can ping IP addresses, run traceroute, test ports and show the Switch's location. |
| System Log | This link takes you to a screen where you can view system logs. |
| Syslog Setup | This link takes you to a screen where you can setup system logs and a system log server. |
| Cluster Management | This link takes you to screens where you can configure clustering management and view its status. |
| MAC Table | This link takes you to a screen where you can view the MAC addresses (and types) of devices attached to what ports and VLAN IDs. |
| ARP Table | This link takes you to a screen where you can view the MAC addresses – IP address resolution table. |
| Path MTU Table | This link takes you to a screen where you can view the path MTU aging time, index, destination address, MTU, and expire settings. |
| Configure Clone | This link takes you to a screen where you can copy attributes of one port to other ports. |
| IPv6 Neighbor Table | This link takes you to a screen where you can view the IPv6 neighbor table which includes index, interface, neighbor address, MAC address, status and type. |
| Port Status | This link takes you to a screen where you can view the port statistics. |

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 are tabs for 'Logins' and 'Access Control'. The 'Administrator' section contains three input fields: 'Old Password', 'New Password', and 'Retype to confirm'. A red oval highlights these three fields. Below the 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.' Underneath is an 'Edit Logins' table with columns for Login, User Name, Password, Retype to confirm, and Privilege. At the bottom are 'Apply' and 'Cancel' buttons.

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

4.6 Save Your Configuration

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

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

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

4.7 Switch Lockout

You could block yourself (and all others) from 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.

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

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

4.8 Reset the Switch

If you lock yourself (and others) from the Switch, or you forget your password, or cannot access the Web Configurator, you will need to reload the factory-default configuration file.

4.8.1 Restore/Reset Button

Press the **RESTORE** button for 3 to 6 seconds or the **RESET** button for one second to have the Switch automatically reboot. See [Table 1 on page 18](#) to know which button is supported on your model.

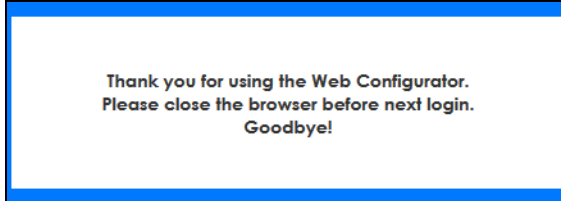
Press the **RESTORE** button for more than 6 seconds to have the Switch restore the factory default file.

See [Section 3.3 on page 37](#) for more information about the LED behavior.

4.9 Log Out of the Web Configurator

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

Figure 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:

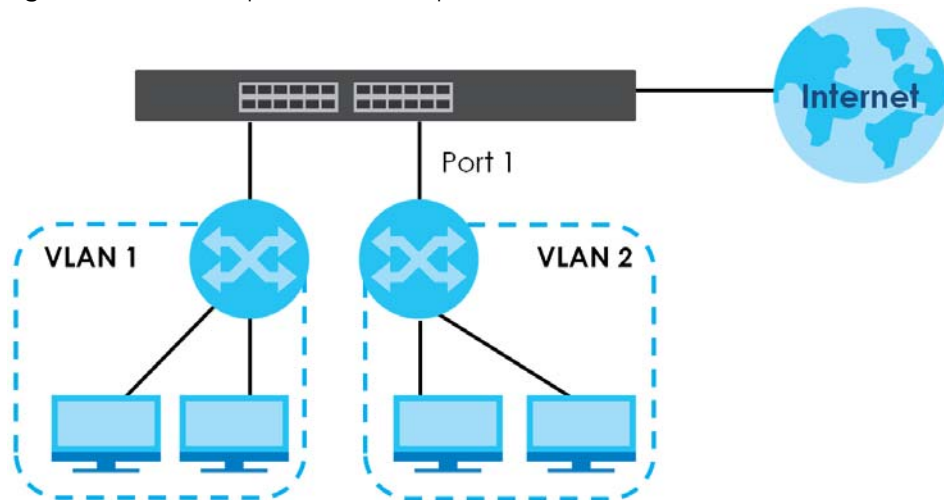
- [Create a VLAN](#)
- [Set Port VID](#)
- [Configure Switch Management IP Address](#)

5.1.1 Create a VLAN

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

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

Figure 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 | |
| MAC Based VLAN Setup | Click Here | |
| Vendor ID Based VLAN Setup | Click Here | |

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

| Static VLAN | | VLAN Configuration |
|---|---|--|
| ACTIVE | <input checked="" type="checkbox"/> | |
| Name | EXAMPLE | |
| VLAN Group ID | 2 | |
| Port | Control | Tagging |
| * | Normal | <input checked="" type="checkbox"/> Tx Tagging |
| 1 | <input type="radio"/> Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden | <input type="checkbox"/> Tx Tagging |
| 2 | <input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden | <input checked="" type="checkbox"/> Tx Tagging |
| 3 | <input type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden | <input checked="" type="checkbox"/> Tx Tagging |
| 4 | <input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden | <input checked="" type="checkbox"/> Tx Tagging |
| 5 | <input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden | <input checked="" type="checkbox"/> Tx Tagging |
| 6 | <input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden | <input checked="" type="checkbox"/> Tx Tagging |
| 7 | <input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden | <input checked="" type="checkbox"/> Tx Tagging |
| 8 | <input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden | <input checked="" type="checkbox"/> Tx Tagging |
| <input type="button" value="Add"/> <input type="button" value="Cancel"/> <input type="button" value="Clear"/> | | |
| VID | Active | Name |
| 1 | Yes | 1 |
| <input type="button" value="Delete"/> <input type="button" value="Cancel"/> | | |

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

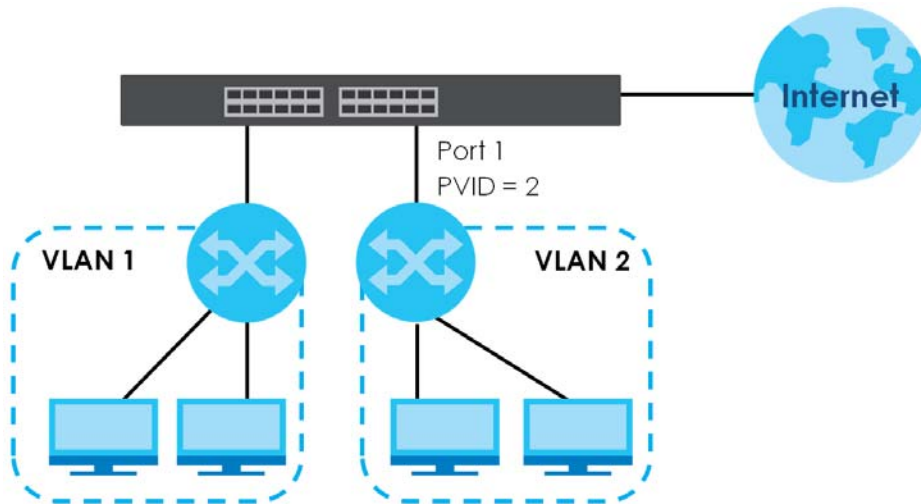
- Since the **VLAN2** network is connected to port 1 on the Switch, select **Fixed** to configure port 1 to be a permanent member of the VLAN only.
- To ensure that VLAN-unaware devices (such as computers and hubs) can receive frames properly, clear the **TX Tagging** check box to set the Switch to remove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

5.1.2 Set Port VID

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

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

Figure 45 Initial Setup Network Example: Port VID



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

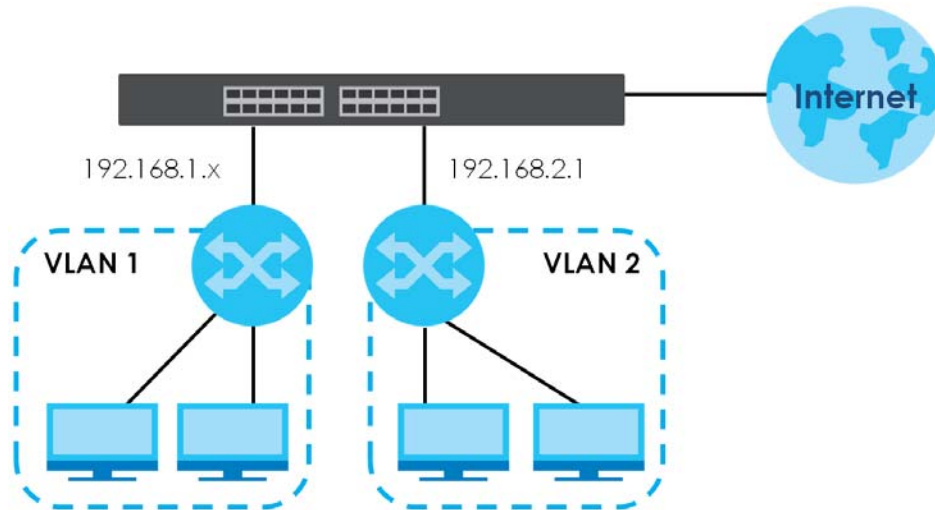
| VLAN Port Setting | | | VLAN Configuration | | |
|-------------------|--------------------------|------|--------------------------------------|--------------------------|--------------------------|
| Port | Ingress Check | PVID | Acceptable Frame Type | VLAN Trunking | Isolation |
| * | <input type="checkbox"/> | | All <input type="button" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 1 | <input type="checkbox"/> | 2 | All <input type="button" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2 | <input type="checkbox"/> | 1 | All <input type="button" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3 | <input type="checkbox"/> | 1 | All <input type="button" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4 | <input type="checkbox"/> | 1 | All <input type="button" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 5 | <input type="checkbox"/> | 1 | All <input type="button" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 6 | <input type="checkbox"/> | 1 | All <input type="button" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 7 | <input type="checkbox"/> | 1 | All <input type="button" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 8 | <input type="checkbox"/> | 1 | All <input type="button" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |

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

5.1.3 Configure Switch Management IP Address

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

Figure 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 40](#) for more information.
- 3 Click **Basic Setting** > **IP Setup** > **IP Configuration** in the navigation panel.

The screenshot shows the IP Setup configuration page. The page has a header with "IP Setup" and links for "IP Status" and "Network Proxy Configuration". Below the header, there are fields for "Domain Name Server 1" and "Domain Name Server 2". The "Default Management IP Address" section has two options: "DHCP Client" (selected) and "Static IP Address". The "DHCP Client" option has fields for "Option-60" (checked), "Class-ID" (Zyxel Corporator), "IP Address" (172.21.40.07), "IP Subnet Mask" (255.255.252.0), and "Default Gateway" (172.21.40.254). The "Static IP Address" option has fields for "IP Address", "IP Subnet Mask", and "Default Gateway". The "VID" field is set to 1. Below the "Default Management IP Address" section, there are "Apply" and "Cancel" buttons. The "Management IP Addresses" section is highlighted with a red box and contains a table with the following data:

| IP Address | 192.168.2.1 |
|-----------------|---------------|
| IP Subnet Mask | 255.255.255.0 |
| VID | 2 |
| Default Gateway | 0.0.0.0 |

Below the table, there are "Add" and "Cancel" buttons. At the bottom of the page, there is a table with the following data:

| Index | IP Address | IP Subnet Mask | VID | Default Gateway | |
|-------|------------|----------------|-----|-----------------|--------------------------|
| | | | | | <input type="checkbox"/> |

Below the table, there are "Delete" and "Cancel" buttons.

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

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

CHAPTER 6

Tutorials

6.1 Overview

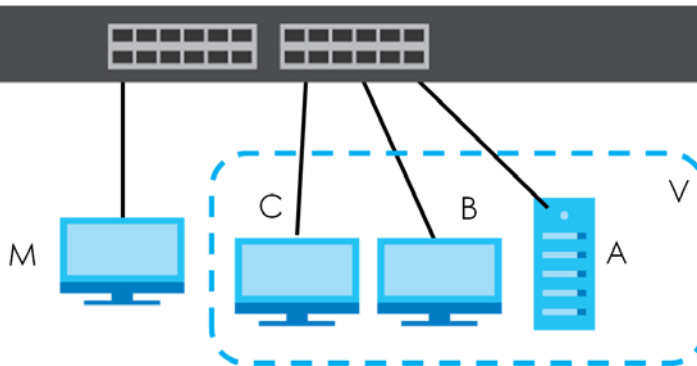
This chapter provides some examples of using the Web Configurator to set up and use the Switch. The tutorials include:

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

6.2 How to Use DHCPv4 Snooping on the Switch

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

Figure 47 Tutorial: DHCP Snooping Tutorial Overview



The settings in this tutorial are as the following.

Table 21 Tutorial: Settings in this Tutorial

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

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

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

Figure 48 Tutorial: Create a VLAN and Add Ports to It

Static VLAN VLAN Configuration

ACTIVE

Name

VLAN Group ID

| Port | Control | Tagging |
|------|---|--|
| * | Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden <input type="radio"/> | <input checked="" type="checkbox"/> Tx Tagging |
| 1 | Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden <input type="radio"/> | <input checked="" type="checkbox"/> Tx Tagging |
| 2 | Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden <input type="radio"/> | <input checked="" type="checkbox"/> Tx Tagging |
| 3 | Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden <input type="radio"/> | <input checked="" type="checkbox"/> Tx Tagging |
| 4 | Normal <input type="radio"/> Fixed <input checked="" type="radio"/> Forbidden <input type="radio"/> | <input type="checkbox"/> Tx Tagging |
| 5 | Normal <input type="radio"/> Fixed <input checked="" type="radio"/> Forbidden <input type="radio"/> | <input type="checkbox"/> Tx Tagging |
| 6 | Normal <input type="radio"/> Fixed <input checked="" type="radio"/> Forbidden <input type="radio"/> | <input type="checkbox"/> Tx Tagging |
| 7 | Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden <input type="radio"/> | <input checked="" type="checkbox"/> Tx Tagging |
| 8 | Normal <input checked="" type="radio"/> Fixed <input type="radio"/> Forbidden <input type="radio"/> | <input checked="" type="checkbox"/> Tx Tagging |

| VID | Active | Name |
|-----|--------|------|
| 1 | Yes | 1 |

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

Figure 49 Tutorial: Tag Untagged Frames

VLAN Port Setting VLAN Configuration

| Port | Ingress Check | PVID | Acceptable Frame Type | VLAN Trunking | Isolation |
|------|--------------------------|------|--------------------------------------|--------------------------|--------------------------|
| * | <input type="checkbox"/> | | All <input type="text" value="All"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 1 | <input type="checkbox"/> | 1 | All <input type="text" value="All"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2 | <input type="checkbox"/> | 1 | All <input type="text" value="All"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3 | <input type="checkbox"/> | 1 | All <input type="text" value="All"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4 | <input type="checkbox"/> | 100 | All <input type="text" value="All"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 5 | <input type="checkbox"/> | 100 | All <input type="text" value="All"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 6 | <input type="checkbox"/> | 100 | All <input type="text" value="All"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 7 | <input type="checkbox"/> | 1 | All <input type="text" value="All"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 8 | <input type="checkbox"/> | 1 | All <input type="text" value="All"/> | <input type="checkbox"/> | <input type="checkbox"/> |

- Go to **Advanced Application > DHCP Snooping > Configure**, activate and specify VLAN 100 as the DHCP VLAN as shown. Click **Apply**.

Figure 50 Tutorial: Specify DHCP VLAN

The screenshot shows the 'DHCP Snooping Configure' page. At the top right, there are links for 'DHCP Snooping', 'Port', and 'VLAN'. The 'Active' checkbox is checked, and the 'DHCP Vlan' dropdown menu is set to '100'. Below this is a 'Database' section with fields for 'Agent URL', 'Timeout interval' (300 seconds), and 'Write delay interval' (300 seconds). At the bottom, there is a 'Renew DHCP Snooping URL' field and a 'Renew' button. The 'Apply' button is circled in red.

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

Figure 51 Tutorial: Set the DHCP Server Port to Trusted

The screenshot shows the 'DHCP Snooping Port Configure' page. It features a table with columns for 'Port', 'Server Trusted state', and 'Rate (pps)'. The 'Server Trusted state' dropdown for port 4 is set to 'Trusted'. The 'Apply' button is circled in red.

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

- 7 Go to **Advanced Application > DHCP Snooping > Configure > VLAN**, show VLAN 100 by entering 100 in the **VLAN Search by VID** field and click **Search**.

Then select **Yes** in the **Enabled** field of the VLAN 100 entry shown at the bottom section of the screen. Click **Apply**.

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

Figure 52 Tutorial: Enable DHCP Snooping on this VLAN

DHCP Snooping VLAN Configure Configure Port

VLAN Search by VID:

The Number of Search Results: 1

| VID | Enabled | Option 82 Profile |
|-----|---------|-------------------|
| * | No ▾ | ▾ |
| 100 | Yes ▾ | ▾ |

Change Pages:

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



- 9 Connect your DHCP server to port 4 and a computer (as DHCP client) to either port 5 or 6. The computer should be able to get an IP address from the DHCP server. If you put the DHCP server on port 5 or 6, the computer will NOT be able to get an IP address.
- 10 To check if DHCP snooping works, connect to the Switch through Telnet. Use the command “show dhcp snooping binding” to see the DHCP snooping binding table as shown next.

```

sysname# show dhcp snooping binding
-----
MacAddress      IpAddress      Lease          Type           VLAN   Port
-----
00:02:00:00:00:1c  10.10.1.16    6d23h59m20s  dhcp-snooping  100    5
Total number of bindings: 1

```

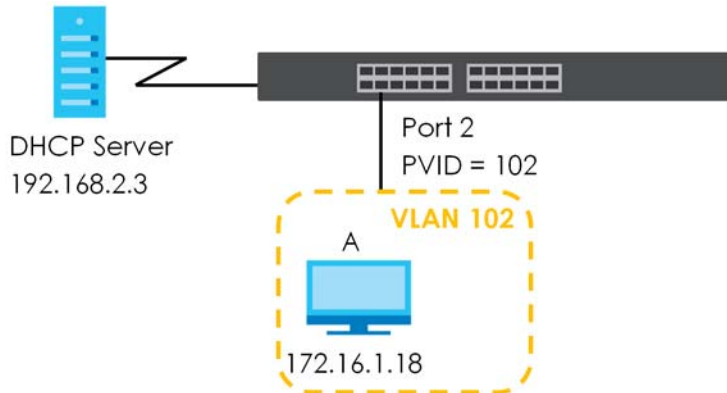
6.3 How to Use DHCPv4 Relay on the Switch

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

6.3.1 DHCP Relay Tutorial Introduction

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

Figure 53 Tutorial: DHCP Relay Scenario



6.3.2 Create a VLAN

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

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

Figure 54 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' (unselected). Below this are several configuration options:

| | | | |
|---------------------------|------------|-----|---------|
| MAC Address Learning | Aging Time | 300 | seconds |
| ARP Aging Time | Aging Time | 300 | seconds |
| 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.
- 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 55 Tutorial: Create a Static VLAN

Static VLAN [VLAN Configuration](#)

ACTIVE

Name VLAN 102

VLAN Group ID 102

| Port | Control | | | Tagging |
|------|---|--|---------------------------------|--|
| * | Normal | | | <input checked="" type="checkbox"/> Tx Tagging |
| 1 | <input checked="" type="radio"/> Normal | <input type="radio"/> Fixed | <input type="radio"/> Forbidden | <input checked="" type="checkbox"/> Tx Tagging |
| 2 | <input type="radio"/> Normal | <input checked="" type="radio"/> Fixed | <input type="radio"/> Forbidden | <input type="checkbox"/> Tx Tagging |
| 3 | <input checked="" type="radio"/> Normal | <input type="radio"/> Fixed | <input type="radio"/> Forbidden | <input checked="" type="checkbox"/> Tx Tagging |
| 4 | <input checked="" type="radio"/> Normal | <input type="radio"/> Fixed | <input type="radio"/> Forbidden | <input checked="" type="checkbox"/> Tx Tagging |
| 5 | <input checked="" type="radio"/> Normal | <input type="radio"/> Fixed | <input type="radio"/> Forbidden | <input checked="" type="checkbox"/> Tx Tagging |
| 6 | <input type="radio"/> Normal | <input type="radio"/> Fixed | <input type="radio"/> Forbidden | <input checked="" type="checkbox"/> Tx Tagging |
| 7 | <input checked="" type="radio"/> Normal | <input type="radio"/> Fixed | <input type="radio"/> Forbidden | <input checked="" type="checkbox"/> Tx Tagging |
| 8 | <input checked="" type="radio"/> Normal | <input type="radio"/> Fixed | <input type="radio"/> Forbidden | <input checked="" type="checkbox"/> Tx Tagging |

| VID | Active | Name | |
|-----|--------|------|--------------------------|
| 1 | Yes | 1 | <input type="checkbox"/> |

- 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 56 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 |
| MAC Based 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 57 Tutorial: Add Tag for Frames Received on Port 2

| VLAN Port Setting | | | VLAN Configuration | | |
|-------------------|--------------------------|------|--------------------------------------|--------------------------|--------------------------|
| Port | Ingress Check | PVID | Acceptable Frame Type | VLAN Trunking | Isolation |
| * | <input type="checkbox"/> | | All <input type="button" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 1 | <input type="checkbox"/> | 1 | All <input type="button" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2 | <input type="checkbox"/> | 102 | All <input type="button" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3 | <input type="checkbox"/> | 1 | All <input type="button" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4 | <input type="checkbox"/> | 1 | All <input type="button" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 5 | <input type="checkbox"/> | 1 | All <input type="button" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 6 | <input type="checkbox"/> | 1 | All <input type="button" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 7 | <input type="checkbox"/> | 1 | All <input type="button" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 8 | <input type="checkbox"/> | 1 | All <input type="button" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |

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

6.3.3 Configure DHCPv4 Relay

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

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

Figure 58 Tutorial: Set DHCP Server and Relay Information

| DHCP Relay | | Status | Port |
|----------------------|---|------------------------|----------------------|
| Active | <input checked="" type="checkbox"/> | | |
| 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 <input type="button" value="v"/> | | |

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

6.3.4 Troubleshooting

Check 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 Details.

7.1.1 What You Can Do

- Use the **Status** screen ([Section 7.2 on page 78](#)) 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 81](#)) to view a summary and manage Switch's neighbor devices.
- Use the **Neighbor Detail** screen ([Section 7.2.2 on page 82](#)) to view more detailed information on the Switch's neighbor devices.

7.2 Status

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

Figure 59 Status (for PoE models)

The following table describes the labels in this screen.

Table 22 Status

| LABEL | DESCRIPTION |
|---------------------|--|
| Device Information | |
| Device Type | This field displays the model name of this Switch. |
| System Name | This field displays the name used to identify the Switch on any network. |
| Boot Version | This field displays the version number and date of the boot module that is currently on the Switch. |
| System Location | This field displays the geographic location of your Switch. You can change the setting in the Basic Setting > General Setup screen. |
| Firmware Version | This field displays the version number and date of the firmware the Switch is currently running. |
| System Time | This field displays the current date and time in the UAG. The format is mm-dd-yyyy hh:mm:ss. |
| Serial Number | This field displays the serial number of this Switch. The serial number is used for device tracking and control. |
| System Up Time | This field displays how long the Switch has been running since it last restarted or was turned on. |
| MAC Address | This field displays the MAC addresses of the Switch. |
| Login Timeout(mins) | This field displays how many minutes a management session can be left idle before the session times out. After it times out you have to log in with your password again. |
| Hybrid Mode | This field displays whether the Switch is in Standalone mode or Cloud mode. |

Table 22 Status (continued)

| LABEL | DESCRIPTION |
|-------------------------|--|
| Cloud Connection Status | <p>This field displays the registration and connection status between the Switch and the NCC (Nebula Control Center).</p> <p>In Standalone mode, the status will display Disconnected or Unregistered. In cloud mode the status will display Connected or Disconnected.</p> <p>Connected – The Switch is registered with and connected to the NCC.</p> <p>Disconnected – The Switch is not connected to the NCC.</p> <p>Unregistered – The Switch is not registered with the NCC.</p> |
| Detail | Click this link to go to the Basic Setting > System Info screen to check other detailed information, such as system resource usage. |
| System Information | |
| System Name | This field displays the name used to identify the Switch on any network. |
| 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 and date of the firmware the Switch is currently running. |
| 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 the 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. |
| IP Address Information | |
| IPv4 Address | This field displays the current IPv4 address of the Switch. |
| Subnet Mask | This field displays the subnet mask of the Switch. |
| Default Gateway | This field displays the IP address of the default gateway of the Switch. |
| IP Setup | Click the link to go to the Basic Setting > IP Setup > IP Configuration screen. |
| Quick Links | This section provides the shortcut link to a specific configuration screen. |

Table 22 Status (continued)

| LABEL | DESCRIPTION |
|----------------------|--|
| Cloud Control Status | <p>This field displays:</p> <ul style="list-style-type: none"> The Switch Internet connection status. The connection status between the Switch and NCC. The Switch registration status on NCC. <p>Mouse over the circles to display detailed information.</p> <p>To pass your Switch management to NCC, first make sure your Switch is connected to the Internet. Then go to NCC and register your Switch.</p> <p>Click NCC Discovery or the switch button to go to the Basic Setting > Cloud Management screen. You can enable/disable NCC Discovery or view the NCC connection status in the Cloud Management screen.</p> <p>1. Internet</p> <p>Green – The Switch is connected to the Internet.</p> <p>Orange – The Switch is not connected to the Internet.</p> <p>2. Nebula</p> <p>Green – The Switch is connected to NCC.</p> <p>Orange – The Switch is not connected to NCC.</p> <p>3. Registration</p> <p>Green – The Switch is registered on NCC.</p> <p>Gray – The Switch is not registered on NCC.</p> <p>Note: All circles will gray out if you disable Nebula Discovery.</p> <p>Note: If a circle displays orange or gray, hover the mouse over the circle to check the diagnostic message.</p> |
| NCC Discovery | <p>This displays ON if NCC discovery is enabled on the Switch. The Switch will connect to NCC and change to the NCC management mode if it:</p> <ul style="list-style-type: none"> is connected to the Internet. has been registered on NCC. |

7.2.1 Neighbor Screen

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 60 Status > Neighbor

| Switch Neighbor | | | | | | | | Status Neighbor Detail | | |
|-----------------|-----------|------|--------------|-------------|---------|------|-----------|--|--------------------------|--|
| Port | Port Name | Link | PoE Draw (W) | System Name | IPv4 | IPv6 | PWR Cycle | Reset to Default | <input type="checkbox"/> | |
| 1 | -- | Down | 0.0 | -- | -- | -- | Cycle | Reset | <input type="checkbox"/> | |
| 2 | -- | 1G/F | 0.0 | -- | -- | -- | Cycle | Reset | <input type="checkbox"/> | |
| 3 | -- | Down | 0.0 | -- | -- | -- | Cycle | Reset | <input type="checkbox"/> | |
| 4 | -- | Down | 0.0 | -- | -- | -- | Cycle | Reset | <input type="checkbox"/> | |
| 5 | -- | Down | 0.0 | -- | -- | -- | Cycle | Reset | <input type="checkbox"/> | |
| 6 | -- | 1G/F | 0.0 | 12A3_84 | 0.0.0.0 | -- | Cycle | Reset | <input type="checkbox"/> | |
| 7 | -- | Down | 0.0 | -- | -- | -- | Cycle | Reset | <input type="checkbox"/> | |
| 8 | -- | Down | 0.0 | -- | -- | -- | Cycle | Reset | <input type="checkbox"/> | |

[Flush](#)

The following table describes the fields in the above screen.

Table 23 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 10M for 10 Mbps, 100M for 100 Mbps, 1G for 1 Gbps) and the duplex (F for full duplex or H for half). This field displays Down if the port is not connected to any device. |
| PoE Draw (W) | This shows the consumption that the neighboring device connected to this port draws from the Switch. This allows you to plan and use within the power budget of the Switch. |
| System Name | This shows the system name of the neighbor device. |
| IPv4 | This shows the IPv4 address of the neighbor device. The IPv4 address is a hyper link that you can click to log into and manage the neighbor device through its Web Configurator. |
| IPv6 | This shows the IPv6 address of the neighbor device. The IPv6 address is a hyper link that you can click to log into and manage the neighbor device through its Web Configurator. |
| PWR Cycle | Click the Cycle button to turn OFF the power of the neighbor device and turn it back ON again. A count down button (from 5 to 0) starts. Note: The Switch must support power sourcing (PSE) or the network device is a powered device (PD). |
| 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: <ul style="list-style-type: none"> The Switch must support power sourcing (PSE) or the network device is a powered device (PD). If multiple neighbor devices use the same port, the Reset button is not available. You can only reset Zyxel powered devices that support the ZON utility. |
| | Select an entry's check box to select a specific port. Otherwise, select the check box in the table heading row to select all ports. |
| Flush | Click the Flush button to remove information about neighbors learned on the selected ports. |

7.2.2 Neighbor Detail

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

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

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

Figure 61 Status > Neighbor > Neighbor Detail

| Switch Neighbor Detail | | | | Switch Neighbor | |
|------------------------|-------------------------|-------|------------|-----------------|--|
| Local Port 1 | | | | | |
| Desc. | -- | Link | Down | PoE Draw (W) | 0.0 |
| | | | | PWR Cycle | Cycle |
| Local Port 2 | | | | | |
| Desc. | -- | Link | 1G/F | PoE Draw (W) | 0.0 |
| | | | | PWR Cycle | Cycle |
| Remote | | | | | |
| System Name | -- | Model | -- | Firmware | -- |
| MAC | c0:3f:d5:b6:78:44 | | | | |
| IPv4 | -- | | | | |
| Port | c0:3f:d5:b6:78:44 | Desc. | -- | Location | -- |
| | | | | | Reset to Default Reset |
| Local Port 3 | | | | | |
| Desc. | -- | Link | Down | PoE Draw (W) | 0.0 |
| | | | | PWR Cycle | Cycle |
| Local Port 4 | | | | | |
| Desc. | -- | Link | Down | PoE Draw (W) | 0.0 |
| | | | | PWR Cycle | Cycle |
| Local Port 5 | | | | | |
| Desc. | -- | Link | Down | PoE Draw (W) | 0.0 |
| | | | | PWR Cycle | Cycle |
| Local Port 6 | | | | | |
| Desc. | -- | Link | 1G/F | PoE Draw (W) | 0.0 |
| | | | | PWR Cycle | Cycle |
| Remote | | | | | |
| System Name | 12A3_84 | Model | XGS3700-48 | Firmware | V4.30(AAGE.2)_20200930 09/30 |
| MAC | E4-18-68-F7-8A-0D | | | | |
| IPv4 | 0.0.0.0 | | | | |
| IPv6 | -- | | | | |
| Port | 37 | Desc. | HQ2_R102 | Location | -- |
| | | | | | Reset to Default Reset |
| Local Port 7 | | | | | |
| Desc. | -- | Link | Down | PoE Draw (W) | 0.0 |
| | | | | PWR Cycle | Cycle |
| Local Port 8 | | | | | |
| Desc. | -- | Link | Down | PoE Draw (W) | 0.0 |
| | | | | PWR Cycle | Cycle |

The following table describes the fields in the above screen.

Table 24 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 10M for 10 Mbps, 100M for 100 Mbps, 1G for 1 Gbps) and the duplex (F for full duplex or H for half). This field displays Down if the port is not connected to any device. |
| PoE Draw (W) | This shows the consumption that the neighboring device connected to this port draws from the Switch. This allows you to plan and use within the power budget of the Switch. |
| PWR Cycle | Click the Cycle button to turn OFF the power of the neighbor device and turn it back ON again. A count down button (from 5 to 0) starts. Note: The Switch must support power sourcing (PSE) or the network device is a powered device (PD). |
| Remote | |
| System Name | This shows the system name of the neighbor device. |
| Model | This shows the model name of the neighbor device. This field will show "--" for devices that do not support the ZON utility. |
| Firmware | This shows the firmware version of the neighbor device. This field will show "--" for devices that do not support the ZON utility. |
| MAC | This shows the MAC address of the neighbor device. |
| IPv4 | This shows the IPv4 address of the neighbor device. The IPv4 address is a hyper link that you can click to log into and manage the neighbor device through its Web Configurator. |
| IPv6 | This shows the IPv6 address of the neighbor device. The IPv6 address is a hyper link that you can click to log into and manage the neighbor device through its Web Configurator. |
| Port | This show the number of the neighbor device's port which is connected to the Switch. |
| Desc. | This shows the description of the neighbor device's port which is connected to the Switch. |

Table 24 Status > Neighbor > Neighbor Detail (continued)

| LABEL | DESCRIPTION |
|------------------|--|
| Location | This shows the geographic location of the neighbor device. This field will show “-” for devices that do not support the ZON utility. |
| Reset to Default | <p>Click the Reset button to reset the neighbor device to its factory default settings. A warning message “Are you sure you want to load factory default?” appears prompting you to confirm the action. After confirming the action a count down button (from 5 to 0) starts.</p> <p>Note:</p> <ul style="list-style-type: none">• The Switch must support power sourcing (PSE) or the network device is a powered device (PD).• If multiple neighbor devices use the same port, the Reset button is not available.• You can only reset Zyxel powered devices that support the ZON utility. |

CHAPTER 8

Basic Setting

8.1 Overview

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

8.1.1 What You Can Do

- Use the **System Info** screen ([Section 8.2 on page 85](#)) to check the firmware version number and system resource usage.
- Use the **General Setup** screen ([Section 8.3 on page 86](#)) to configure general settings such as the system name and time.
- Use the **Switch Setup** screen ([Section 8.4 on page 88](#)) to choose your VLAN type and assign priorities to queues.
- Use the **IP Setup** screen ([Section 8.5 on page 90](#)) to configure the Switch IP address, default gateway device, management VLAN ID, and proxy server.
- Use the **Port Setup** screen ([Section 8.6 on page 96](#)) to configure Switch port settings.
- Use the **PoE Setup** screens ([Section 8.7 on page 97](#)) to view the current amount of power that PDs are receiving from the Switch and set the priority levels for the Switch in distributing power to PDs. This screen is available for PoE models only.
- Use the **Interface Setup** screens ([Section 8.8 on page 103](#)) to configure Switch interface type and interface ID settings.
- Use the **IPv6** screens ([Section 8.9 on page 104](#)) to view IPv6 status and IPv6 configuration.
- Use the **Cloud Management** screen ([Section 8.10 on page 115](#)) to allow remote management of the Switch using Nebula.

8.2 System Information

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

Figure 62 Basic Setting > System Info

| System Info | | | |
|--------------------|------------------------------|-------------|-----------------|
| System Name | GS1915 | | |
| Product Model | GS1915-8EP | | |
| ZyNOS F/W Version | V4.70(ACAG.0)b1 09/06/2021 | | |
| Ethernet Address | 00:19:cb:00:00:01 | | |
| | | | |
| CPU Utilization | | | |
| Current (%) | 5.23 | | |
| | | | |
| Memory Utilization | | | |
| Name | Total (byte) | Used (byte) | Utilization (%) |
| common | 35381248 | 3795680 | 10 |

The following table describes the labels in this screen.

Table 25 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 the 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. |

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 63 Basic Setting > General Setup

| General Setup | |
|--|---|
| System Name | <input type="text"/> |
| Location | <input type="text"/> |
| Contact Person's Name | <input type="text"/> |
| | |
| Use Time Server when Bootup | NTP(RFC-1305) <input type="button" value="v"/> |
| Time Server IP Address | <input type="text" value="1.pool.ntp.org"/> |
| Time Server Sync Interval | 1440 minutes |
| Current Time | 11 : 00 : 46 UTC+00:00 |
| New Time (hh:mm:ss) | 11 : 00 : 46 |
| Current Date | 2016 - 01 - 01 |
| New Date (yyyy-mm-dd) | 2016 - 01 - 01 |
| Time Zone | UTC <input type="button" value="v"/> |
| Daylight Saving Time | <input type="checkbox"/> |
| Start Date | First <input type="button" value="v"/> Sunday <input type="button" value="v"/> of January <input type="button" value="v"/> at 0:00 <input type="button" value="v"/> |
| End Date | First <input type="button" value="v"/> Sunday <input type="button" value="v"/> of January <input type="button" value="v"/> at 0:00 <input type="button" value="v"/> |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

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

The following table describes the labels in this screen.

Table 26 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 single-byte printable 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 single-byte printable characters; spaces are allowed. |
| Use Time Server when Bootup | <p>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.</p> <p>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.</p> <p>Time (RFC-868) format displays a 4-byte integer giving the total number of seconds since 1970/1/1 at 0:0:0.</p> <p>NTP (RFC-1305) is similar to Time (RFC-868).</p> <p>None is the default value. Enter the time manually. Each time you turn on the Switch, the time and date will be reset to 2020-01-01 0:0:0.</p> |
| Time Server IP Address | Enter the IP address or domain name of your timeserver. The Switch searches for the timeserver for up to 60 seconds. |
| Time Server Sync Interval | Enter the period in minutes between each time server synchronization. The Switch checks the time server after every synchronization interval. |
| Current Time | This field displays the time you open this menu (or refresh the menu). |
| New Time (hh:mm:ss) | Enter the new time in hour, minute and second format. The new time then appears in the Current Time field after you click Apply . |

Table 26 Basic Setting > General Setup (continued)

| LABEL | DESCRIPTION |
|-----------------------|---|
| Current Date | This field displays the date you open this menu. |
| New Date (yyyy-mm-dd) | Enter the new date in year, month and day format. The new date then appears in the Current Date field after you click Apply . |
| Time Zone | Select the time difference between UTC (Universal Time Coordinated, formerly known as GMT, Greenwich Mean Time) and your time zone from the drop-down list box. |
| Daylight Saving Time | Daylight saving is a period from late spring to early fall when many countries set their clocks ahead of normal local time by one hour to give more daytime light in the evening. Select this option if you use Daylight Saving Time. |
| Start Date | Configure the day and time when Daylight Saving Time starts if you selected Daylight Saving Time . The time is displayed in the 24 hour format. Here are a couple of examples: Daylight Saving Time starts in most parts of the United States on the second Sunday of March. Each time zone in the United States starts using Daylight Saving Time at 2 A.M. local time. So in the United States you would select Second, Sunday, March and 2:00 . Daylight Saving Time starts in the European Union on the last Sunday of March. All of the time zones in the European Union start using Daylight Saving Time at the same moment (1 A.M. GMT or UTC). So in the European Union you would select Last, Sunday, March and the last field depends on your time zone. In Germany for instance, you would select 2:00 because Germany's time zone is one hour ahead of GMT or UTC (GMT+1). |
| End Date | Configure the day and time when Daylight Saving Time ends if you selected Daylight Saving Time . The time field uses the 24 hour format. Here are a couple of examples: Daylight Saving Time ends in the United States on the 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 Switch Setup

Use this to choose the VLAN (Virtual Local Area Network) type, map the priority queue, and configure other settings.

8.4.1 Introduction to VLANs

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

In MTU (Multi-Tenant Unit) applications, VLAN is vital in providing isolation and security among the subscribers. When properly configured, VLAN prevents one subscriber from accessing the network

resources of another on the same LAN, thus a user will NOT see the printers and hard disks of another user in the same building.

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

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

8.4.2 Setting up

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

Figure 64 Basic Setting > Switch Setup

| Switch Setup | | | |
|---------------------------|---|-------|---------|
| VLAN Type | <input type="radio"/> 802.1Q <input checked="" type="radio"/> Port Based | | |
| MAC Address Learning | Aging Time | 300 | seconds |
| ARP Aging Time | Aging Time | 300 | seconds |
| Priority Queue Assignment | Priority7 | 7 | ▼ |
| | Priority6 | 6 | ▼ |
| | Priority5 | 5 | ▼ |
| | Priority4 | 4 | ▼ |
| | Priority3 | 3 | ▼ |
| | Priority2 | 1 | ▼ |
| | Priority1 | 0 | ▼ |
| | Priority0 | 2 | ▼ |
| | | Apply | Cancel |

The following table describes the labels in this screen.

Table 27 Basic Setting > Switch Setup

| LABEL | DESCRIPTION |
|----------------------|--|
| VLAN Type | Choose 802.1Q or Port Based . The Advanced Application > VLAN Setup screen changes depending on whether you choose 802.1Q VLAN type or Port Based VLAN type in this screen. |
| MAC Address Learning | MAC address learning reduces outgoing traffic broadcasts. For MAC address learning to occur on a port, the port must be active. |
| Aging Time | Enter a time from 10 to 1000000 seconds. This is how long all dynamically learned MAC addresses remain in the MAC address table before they age out (and must be relearned). |
| ARP Aging Time | 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 . |

Table 27 Basic Setting > Switch Setup (continued)

| LABEL | DESCRIPTION |
|------------|--|
| | <p>Priority Queue Assignment</p> <p>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.</p> <p>The Switch has eight physical queues that you can map to the eight priority levels. On the Switch, traffic assigned to higher index queues gets through faster while traffic in lower index queues is dropped if the network is congested.</p> |
| | <p>Priority Level (The following descriptions are based on the traffic types defined in the IEEE 802.1d standard (which incorporates the 802.1p).</p> <p>To map a priority level to a physical queue, select a physical queue from the drop-down menu on the right.</p> |
| Priority 7 | Typically used for network control traffic such as router configuration messages. |
| Priority 6 | Typically used for voice traffic that is especially sensitive to jitter (jitter is the variations in delay). |
| Priority 5 | Typically used for video that consumes high bandwidth and is sensitive to jitter. |
| Priority 4 | Typically used for controlled load, latency-sensitive traffic such as SNA (Systems Network Architecture) transactions. |
| Priority 3 | Typically used for "excellent effort" or better than best effort and would include important business traffic that can tolerate some delay. |
| Priority 2 | This is for "spare bandwidth". |
| Priority 1 | This is typically used for non-critical "background" traffic such as bulk transfers that are allowed but that should not affect other applications and users. |
| Priority 0 | Typically used for best-effort traffic. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

8.5 IP Setup

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

8.5.1 IP Interfaces

The Switch needs an IP address for it to be managed over the network. When the Switch (in Standalone mode) 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 ports. Since each IP address on the Switch must be in a separate subnet, the configured IP address is also known as IP interface (or routing domain). In addition, this allows routing between subnets based on the IP address without additional routers.

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

You can configure up to 64 IP domains which are used to access and manage the Switch from the ports belonging to the pre-defined VLANs.

Note: You must configure a VLAN first. Each VLAN can only have one management IP address.

8.5.2 IP Status

Figure 65 Basic Setting > IP Setup: IP Status

| IP Status | | | | IP Configuration | |
|---------------------|--------------|----------------|-----|----------------------------------|---|
| Domain Name Server | | Source | | | |
| 172.21.10.1 | | DHCPv4 | | | |
| 8.8.8.8 | | Backup | | | |
| IP Interface | | | | | |
| Index | IP Address | IP Subnet Mask | VID | Type | Action |
| 1 | 172.21.40.19 | 255.255.252.0 | 1 | DHCP | <input type="button" value="Renew"/> <input type="button" value="Release"/> |

The following table describes the labels in this screen.

Table 28 Basic Setting > IP Setup: IP Status

| LABEL | DESCRIPTION |
|--------------------|---|
| IP Status | |
| Domain Name Server | This field displays the IP address of the DNS server. |
| Source | This field displays whether the DNS server address is configured manually (Static) or obtained automatically using DHCPv4 . Note: If DNS server is not configured or configuration is deleted, the system automatically uses the default Backup server. |
| IP Interface | |
| Index | This field displays the index number of an entry. |
| IP Address | This field displays the IP address of the Switch in the IP domain. |
| IP Subnet Mask | This field displays the subnet mask of the Switch in the IP domain. |
| VID | This field displays the VLAN identification number of the IP domain on the Switch. |
| Type | This shows whether this IP address is dynamically assigned from a DHCP server or manually assigned (Static). |
| Renew | Click this to renew the dynamic IP address. |
| Release | Click this to release the dynamic IP address. |

8.5.3 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 66 Basic Setting > IP Setup > IP Status Details: Static

| IP Status Detail | | IP Status |
|------------------|---------------|---------------------------|
| Type | Static | |
| VID | 1 | |
| IP Address | 172.21.40.3 | |
| IP Subnet Mask | 255.255.252.0 | |

The following table describes the labels in this screen.

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

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

Figure 67 Basic Setting > IP Setup > IP Status Details: DHCP

| IP Status Detail | | IP Status |
|------------------|---------------------|---------------------------|
| Type | DHCP | |
| VID | 1 | |
| IP Address | 172.21.40.5 | |
| IP Subnet Mask | 255.255.252.0 | |
| Lease Time | 86400 seconds | |
| Renew Time | 43200 seconds | |
| Rebind Time | 75600 seconds | |
| Lease Time Start | 2020-01-01 00:01:24 | |
| Lease Time End | 2020-01-02 00:01:24 | |
| Default Gateway | 172.21.43.254 | |
| DNS Server | 172.21.10.1 | |
| DNS Server | 172.21.5.1 | |

The following table describes the labels in this screen.

Table 30 Basic Setting > IP Setup > IP Status Details: DHCP

| LABEL | DESCRIPTION |
|------------------|---|
| Type | This shows the IP address is dynamically assigned from a DHCP server (DHCP). |
| VID | This is the VLAN identification number to which an IP routing domain belongs. |
| IP Address | This is the IP address of your Switch in dotted decimal notation for example 192.168.1.1. |
| IP Subnet Mask | This is the IP subnet mask of your Switch in dotted decimal notation for example 255.255.255.0. |
| Lease Time | This displays the length of time in seconds that this interface can use the current dynamic IP address from the DHCP server. |
| Renew Time | This displays the length of time from the lease start that the Switch will request to renew its current dynamic IP address from the DHCP server. |
| Rebind Time | This displays the length of time from the lease start that the Switch will request to get any dynamic IP address from the DHCP server. |
| Lease Time Start | This displays the date and time that the current dynamic IP address assignment from the DHCP server began. You should configure date and time in Basic Setting > General Setup . |
| Lease Time End | This displays the date and time that the current dynamic IP address assignment from the DHCP server will end. You should configure date and time in Basic Setting > General Setup . |

Table 30 Basic Setting > IP Setup > IP Status Details: DHCP (continued)

| LABEL | DESCRIPTION |
|-----------------|---|
| 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. |

8.5.4 IP Configuration

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

Figure 68 Basic Setting > IP Setup > IP Configuration

The following table describes the labels in this screen.

Table 31 Basic Setting > IP Setup > IP Configuration

| LABEL | DESCRIPTION |
|-------------------------------|---|
| Domain Name Server 1/2 | Enter a domain name server IPv4 address in order to be able to use a domain name instead of an IP address. |
| Default Management IP Address | Use these fields to create or edit IP routing domains on the Switch. |
| DHCP Client | Select this option if you have a DHCP server that can assign the Switch an IP address, subnet mask, a default gateway IP address and a domain name server IP address automatically. |

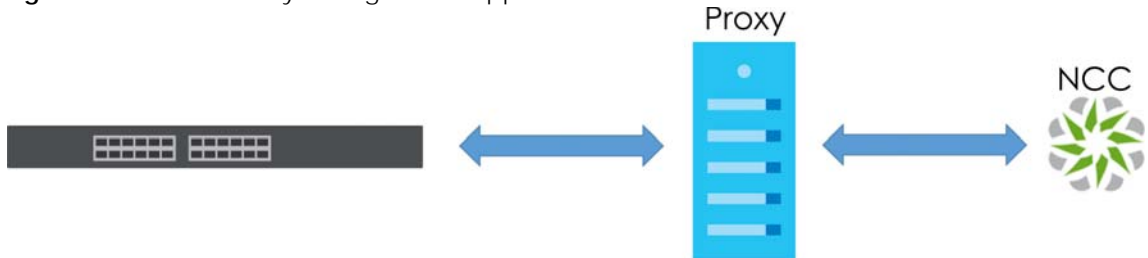
Table 31 Basic Setting > IP Setup > IP Configuration (continued)

| LABEL | DESCRIPTION |
|---|---|
| Option-60 | DHCP Option 60 is used by the Switch for identification to the DHCP server using the VCI (Vendor Class Identifier) on the DHCP server. The Switch adds it in the initial DHCP discovery message that a DHCP client broadcasts in search of an IP address. The DHCP server can assign different IP addresses or options to clients with the specific VCI or reject the request from clients without the specific VCI. Select this and enter the device identity you want the Switch to add in the DHCP discovery frames that go to the DHCP server. This allows the Switch to identify itself to the DHCP server. |
| Class-ID | Enter a string of up to 32 characters to identify this Switch to the DHCP server. For example, Zyxel-TW. |
| Static IP Address | Select this option if you do not have a DHCP server or if you wish to assign static IP address information to the Switch. You need to fill in the following fields when you select this option. |
| IP Address | Enter the IP address of your Switch in dotted decimal notation, for example, 172.21.40.x. This is the IP address of the Switch in an IP routing domain. |
| IP Subnet Mask | Enter the IP subnet mask of an IP routing domain in dotted decimal notation, for example, 255.255.252.0. |
| Default Gateway | Enter the IP address of the default outgoing gateway in dotted decimal notation, for example 172.21.43.254. |
| VID | Enter the VLAN identification number to which an IP routing domain belongs. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to reset the fields to your previous configuration. |
| Management IP Address | |
| Use these fields to set the settings for the management port. | |
| IP Address | Enter the IP address for managing the Switch by the members of the VLAN specified in the VID field below. |
| IP Subnet Mask | Enter the IP subnet mask of your Switch in dotted decimal notation, for example, 255.255.255.0. |
| VID | Enter the VLAN identification number to which an IP routing domain belongs. |
| Default Gateway | Enter the IP address of the default outgoing gateway in dotted decimal notation, for example, 192.168.0.254. |
| Add | Click this to create a new entry. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to reset the fields to your previous configuration. |
| Index | This field displays the index number of an entry. |
| IP Address | This field displays IP address of the Switch in the IP domain. |
| IP Subnet Mask | This field displays the subnet mask of the Switch in the IP domain. |
| VID | This field displays the VLAN identification number of the IP domain on the Switch. |
| Default Gateway | This field displays the IP address of the default outgoing gateway in dotted decimal notation. |
| | Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries. |
| Delete | Click Delete to remove the selected entry from the summary table. Note: Deleting all IP subnets locks you out of the Switch. |
| Cancel | Click Cancel to clear the check boxes. |

8.5.5 Network Proxy Configuration

The proxy server of an organization may prohibit communication between the Switch and NCC (Nebula Control Center)(Section 8.10 on page 115). Use this screen to enable communication between the Switch and NCC through the proxy server.

Figure 69 Network Proxy Configuration Application



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

Figure 70 Basic Setting > IP Setup > IP Configuration > Network Proxy Configuration

The following table describes the labels in this screen.

Table 32 Basic Setting > IP Setup > IP Configuration > Network Proxy Configuration

| LABEL | DESCRIPTION |
|----------------|--|
| Active | Select this option to enable communication between the Switch and NCC through a proxy server. |
| Server | Enter the IP address (dotted decimal notation) or host name of the proxy server. When entering the host name, up to 128 alphanumeric characters are allowed for the Server except [?], [], ['], or ["]. |
| Port | Enter the port number of the proxy server (1 – 65535). |
| Authentication | Select this option to enable proxy server authentication using a Username and Password . |
| Username | Enter a login user name from the proxy server administrator. Up to 32 alphanumeric characters are allowed for the Username . The string should not contain [?], [], ['], ["], [.], [:], or space. |
| Password | Enter a login password from the proxy server administrator. Up to 32 alphanumeric characters are allowed for the Password except [?], [], ['], or ["]. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to reset the fields to your previous configuration. |

8.6 Port Setup

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

Figure 71 Basic Setting > Port Setup

| Port | Active | Name | Speed / Duplex | Flow Control | 802.1p Priority |
|------|-------------------------------------|------|----------------|--------------------------|-----------------|
| * | <input type="checkbox"/> | | Auto | <input type="checkbox"/> | 0 |
| 1 | <input checked="" type="checkbox"/> | | Auto | <input type="checkbox"/> | 0 |
| 2 | <input checked="" type="checkbox"/> | | Auto | <input type="checkbox"/> | 0 |
| 3 | <input checked="" type="checkbox"/> | | Auto | <input type="checkbox"/> | 0 |
| 4 | <input checked="" type="checkbox"/> | | Auto | <input type="checkbox"/> | 0 |
| 5 | <input checked="" type="checkbox"/> | | Auto | <input type="checkbox"/> | 0 |
| 6 | <input checked="" type="checkbox"/> | | Auto | <input type="checkbox"/> | 0 |
| 7 | <input checked="" type="checkbox"/> | | Auto | <input type="checkbox"/> | 0 |
| 8 | <input checked="" type="checkbox"/> | | Auto | <input type="checkbox"/> | 0 |

The following table describes the labels in this screen.

Table 33 Basic Setting > Port Setup

| LABEL | DESCRIPTION |
|--------------|---|
| Port | This is the port index number. |
| * | Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them. |
| Active | Select this check box to enable a port. The factory default for all ports is enabled. A port must be enabled for data transmission to occur. |
| Name | Enter a descriptive name that identifies this port. You can enter up to 128 single-byte printable characters except [?], [], ['] or ["]. Note: Due to space limitations, the port name may be truncated in some Web Configurator screens. |
| Speed/Duplex | Select the speed and the duplex mode of the Ethernet connection on this port. Choices are Auto , 10-an (10M/auto-negotiation), 10M/Half Duplex , 10M/Full Duplex , 100-an (100M/auto-negotiation), 100M/Half Duplex , 100M/Full Duplex , and 1G/Full Duplex . Selecting Auto (auto-negotiation) allows one port to negotiate with a peer port automatically to obtain the connection speed and duplex mode that both ends support. When auto-negotiation is turned on, a port on the Switch negotiates with the peer automatically to determine the connection speed and duplex mode. If the peer port does not support auto-negotiation or turns off this feature, the Switch determines the connection speed by detecting the signal on the cable and using half duplex mode. When the Switch's auto-negotiation is turned off, a port uses the pre-configured speed and duplex mode when making a connection, thus requiring you to make sure that the settings of the peer port are the same in order to connect. |

Table 33 Basic Setting > Port Setup (continued)

| LABEL | DESCRIPTION |
|-----------------|--|
| Flow Control | <p>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.</p> <p>The Switch uses IEEE 802.3x flow control in full duplex mode and backpressure flow control in half duplex mode.</p> <p>IEEE 802.3x flow control is used in full duplex mode to send a pause signal to the sending port, causing it to temporarily stop sending signals when the receiving port memory buffers fill.</p> <p>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.</p> |
| 802.1p Priority | This priority value is added to incoming frames without a (802.1p) priority queue tag. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

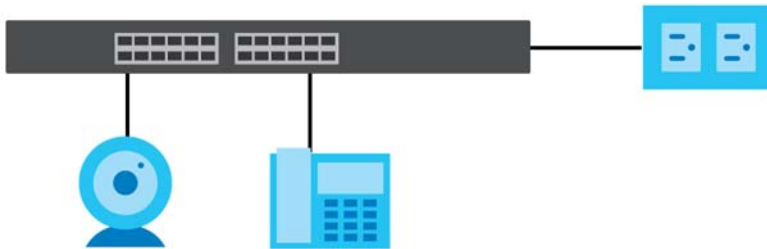
8.7 PoE Status

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

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

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

Figure 72 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 73 Basic Setting > PoE Setup: PoE Status

| PoE Status | | PoE Time Range Setup PoE Setup |
|-------------------------|-------------|--|
| PoE Mode | Consumption | |
| Total Power (W) | 60.0 | |
| PoE Usage (%) | 0 | |
| PoE Usage Threshold (%) | 95 | |
| Consuming Power (W) | 0.0 | |
| Allocated Power (W) | NA | |
| Remaining Power (W) | 60.0 | |

| Port | State | Class | Priority | Power-Up | Consuming Power (W) | Max Power (W) | Time-Range State |
|------|--------|-------|----------|----------|---------------------|---------------|------------------|
| 1 | Enable | 0 | Low | 802.3at | 0.0 | 23.4 | - |
| 2 | Enable | 0 | Low | 802.3at | 0.0 | - | - |
| 3 | Enable | 0 | Low | 802.3at | 0.0 | - | - |
| 4 | Enable | 0 | Low | 802.3at | 0.0 | 7.9 | - |
| 5 | Enable | 0 | Low | 802.3at | 0.0 | - | - |
| 6 | Enable | 0 | Low | 802.3at | 0.0 | - | - |
| 7 | Enable | 0 | Low | 802.3at | 0.0 | - | - |
| 8 | Enable | 0 | Low | 802.3at | 0.0 | 15.4 | - |

The following table describes the labels in this screen.

Table 34 Basic Setting > PoE Setup: PoE Status

| LABEL | DESCRIPTION |
|-------------------------|--|
| PoE Mode | This field displays the power management mode used by the Switch, whether it is in Classification or Consumption mode. |
| Total Power (W) | This field displays the total power the Switch can provide to the connected PoE-enabled devices on the PoE ports. |
| PoE Usage (%) | This field displays the amount of power currently being supplied to connected PoE devices (PDs) as a percentage of the total PoE power the Switch can supply. When PoE usage reaches 100%, the Switch will shut down PDs one-by-one according to the PD priority which you configured in Basic Setting > PoE Setup > PoE Setup . |
| PoE Usage Threshold (%) | This field displays the percentage of PoE usage. The Switch will generate a trap and/or a log when the usage exceeds the specified threshold. |
| Consuming Power (W) | This field displays the amount of power the Switch is currently supplying to the connected PoE-enabled devices. |
| Allocated Power (W) | This field displays the total amount of power the Switch (in classification mode) has reserved for PoE after negotiating with the connected PoE devices. It shows NA when the Switch is in consumption mode. Consuming Power (W) can be less than or equal but not more than the Allocated Power (W) . |
| Remaining Power (W) | This field displays the amount of power the Switch can still provide for PoE. |
| Port | This is the port index number. |
| State | This field shows which ports can receive power from the Switch. <ul style="list-style-type: none"> Disable – The PD connected to this port cannot get power supply. Enable – The PD connected to this port can receive power. |

Table 34 Basic Setting > PoE Setup: PoE Status (continued)

| LABEL | DESCRIPTION |
|---------------------|---|
| Class | <p>This shows the power classification of the PD. Each PD has a specified maximum power that fall under one of the classes.</p> <p>The Class is a number from 0 to 4, where each value represents the range of power that the Switch provides to the PD. The power ranges in PoE standards are as follows.</p> <ul style="list-style-type: none"> • 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. <p>Note: You can extend or set a limit on the maximum power the connected PD can use on a port in Basic Setting > PoE Setup > PoE Setup.</p> |
| Priority | <p>When the total power requested by the PDs exceeds the total PoE power budget on the Switch, you can set the priority to allow the Switch to provide power to ports with higher priority first.</p> <ul style="list-style-type: none"> • Critical has the highest priority. • High has the Switch assign power to the port after all critical priority ports are served. • Low has the Switch assign power to the port after all critical and high priority ports are served. |
| Power-Up | This field displays the PoE standard the Switch uses to provide power on this port. |
| Consuming Power (W) | This field displays the current amount of power consumed by the PD from the Switch on this port. |
| Max Power (W) | This field displays the maximum amount of power the PD could use from the Switch on this port. This field displays “–” if the maximum power is not specified in Basic Setting > PoE Setup > PoE Setup . |
| Time-Range State | <p>This field shows whether or not the port currently receives power from the Switch according to its schedule.</p> <ul style="list-style-type: none"> • 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. |

8.7.1 PoE Time Range Setup

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

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

Figure 74 Basic Setting > PoE Setup > PoE Time Range Setup

| Port | Time Range Profiles | <input type="checkbox"/> |
|------|---------------------|--------------------------|
| 1 | - | <input type="checkbox"/> |
| 2 | - | <input type="checkbox"/> |
| 3 | - | <input type="checkbox"/> |
| 4 | - | <input type="checkbox"/> |
| 5 | - | <input type="checkbox"/> |
| 6 | - | <input type="checkbox"/> |
| 7 | - | <input type="checkbox"/> |
| 8 | - | <input type="checkbox"/> |

The following table describes the labels in this screen.

Table 35 Basic Setting > PoE Setup > PoE Time Range Setup

| LABEL | DESCRIPTION |
|---------------------|---|
| Port | Enter the number of the port to which you want to apply a schedule. |
| Time Range | This field displays the name of the schedule that you have created using the Advanced Application > Time Range screen. Select a pre-defined schedule to control when the Switch enables PoE to provide power on the port. To select more than one schedule, press [SHIFT] and select the choices at the same time. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Clear | Click Clear to clear the fields to the factory defaults. |
| Port | This field displays the index number of the port. Click a port number to change the schedule settings. |
| Time Range Profiles | This field displays the name of the schedule which is applied to the port. PoE is enabled at the specified time or date. |
| | Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries. |
| Delete | Check the rules that you want to remove and then click the Delete button. |
| Cancel | Click Cancel to clear the selected check boxes. |

8.7.2 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 75 Basic Setting > PoE Setup > PoE Setup

PoE Setup
[PoE Status](#)

| | |
|-------------------------|---|
| PoE Mode | <input type="radio"/> Classification <input checked="" type="radio"/> Consumption |
| MIB Trap | Active <input type="checkbox"/> |
| PoE Usage Threshold (%) | <input type="text" value="95"/> |

| Port | Active | Priority | Power-Up | Max Power (mW) | LLDP Power Via MDI |
|------|-------------------------------------|------------|-----------|----------------------|-------------------------------------|
| * | <input type="checkbox"/> | Critical ▼ | 802.3af ▼ | <input type="text"/> | <input type="checkbox"/> |
| 1 | <input checked="" type="checkbox"/> | Low ▼ | 802.3af ▼ | <input type="text"/> | <input checked="" type="checkbox"/> |
| 2 | <input checked="" type="checkbox"/> | Low ▼ | 802.3af ▼ | <input type="text"/> | <input checked="" type="checkbox"/> |
| 3 | <input checked="" type="checkbox"/> | Low ▼ | 802.3af ▼ | <input type="text"/> | <input checked="" type="checkbox"/> |
| 4 | <input checked="" type="checkbox"/> | Low ▼ | 802.3af ▼ | <input type="text"/> | <input checked="" type="checkbox"/> |
| 5 | <input checked="" type="checkbox"/> | Low ▼ | 802.3af ▼ | <input type="text"/> | <input checked="" type="checkbox"/> |
| 6 | <input checked="" type="checkbox"/> | Low ▼ | 802.3af ▼ | <input type="text"/> | <input checked="" type="checkbox"/> |
| 7 | <input checked="" type="checkbox"/> | Low ▼ | 802.3af ▼ | <input type="text"/> | <input checked="" type="checkbox"/> |
| 8 | <input checked="" type="checkbox"/> | Low ▼ | 802.3af ▼ | <input type="text"/> | <input checked="" type="checkbox"/> |
| 9 | <input checked="" type="checkbox"/> | Low ▼ | 802.3af ▼ | <input type="text"/> | <input checked="" type="checkbox"/> |
| 10 | <input checked="" type="checkbox"/> | Low ▼ | 802.3af ▼ | <input type="text"/> | <input checked="" type="checkbox"/> |
| 11 | <input checked="" type="checkbox"/> | Low ▼ | 802.3af ▼ | <input type="text"/> | <input checked="" type="checkbox"/> |
| 12 | <input checked="" type="checkbox"/> | Low ▼ | 802.3af ▼ | <input type="text"/> | <input checked="" type="checkbox"/> |

The following table describes the labels in this screen.

Table 36 Basic Setting > PoE Setup > PoE Setup

| LABEL | DESCRIPTION |
|-------------------------|--|
| PoE Mode | <p>Select the power management mode you want the Switch to use.</p> <ul style="list-style-type: none"> • 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 30 W (IEEE 802.3at Class 4) or 22 W (IEEE 802.3af Classes 0 to 3). |
| MIB Trap | <p>The Switch sends traps (monitoring event notification) to an SNMP (Simple Network Management Protocol) manager when an event occurs. See Section 32.3 on page 260 for more information on SNMP, MIB (Management Information Base), and SNMP traps.</p> <p>Select ON to allow sending of MIB Trap when the following situations occur:</p> <ul style="list-style-type: none"> • Situation 1- Trap sent whenever a PoE port status change occurs (PoE port delivers power or delivers no power to a PD (powered device)) • Situation 2- Trap sent in cases where the total power usage exceeds the PoE usage threshold • Situation 3- Trap sent if total usage power decreases below the PoE usage threshold (only if previous total power usage exceeded the PoE usage threshold and a trap was sent). <p>Note: If the MIB Trap is ON, you must also configure:</p> <ul style="list-style-type: none"> • SNMP trap destination (Management > Access Control > SNMP), SNMP trap group (Management > Access Control > SNMP > Trap Group) and SNMP trap port (Management > Access Control > SNMP > Trap Group > Port) for Situation 1. • SNMP trap destination and SNMP trap group for Situation 2 and Situation 3. <p>See Section 32.3 on page 260 for more information on configuring SNMP.</p> |
| PoE Usage Threshold (%) | <p>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.</p> |
| Port | <p>This is the port index number.</p> |
| * | <p>Settings in this row apply to all ports.</p> <p>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.</p> <p>Changes in this row are copied to all the ports as soon as you make them.</p> |
| Active | <p>Select this to provide power to a PD connected to the port.</p> <p>If left unchecked, the PD connected to the port cannot receive power from the Switch.</p> |
| Priority | <p>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.</p> <p>Select Critical to give the highest PD priority on the port.</p> <p>Select High to set the Switch to assign the remaining power to the port after all critical priority ports are served.</p> <p>Select Low to set the Switch to assign the remaining power to the port after all critical and high priority ports are served.</p> |

Table 36 Basic Setting > PoE Setup > PoE Setup (continued)

| LABEL | DESCRIPTION |
|--------------------|---|
| Power-Up | <p>Set how the Switch provides power to a connected PD at power-up.</p> <p>802.3af – the Switch follows the IEEE 802.3af Power over Ethernet standard to supply power to the connected PDs during power-up.</p> <p>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.</p> <p>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).</p> <p>802.3at – the Switch supports the IEEE 802.3at High Power over Ethernet standard and can supply power of up to 30 W per Ethernet port. IEEE 802.3at is also known as PoE+ or PoE Plus. An IEEE 802.3at compatible device is referred to as Type 2. Power Class 4 (High Power) can only be used by Type 2 devices. If the connected PD requires a Class 4 current when it is turned on, it will be powered up in this mode.</p> <p>Force-802.3at – the Switch offers power of up to 30 W on the port without performing PoE hardware classification. Select this option if the connected PD does not comply with any PoE standard and requests power higher than a standard power limit.</p> |
| Max Power (mW) | Specify the maximum amount of power the PD could use from the Switch on this port. |
| LLDP Power Via MDI | <p>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.</p> <p>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.</p> <ul style="list-style-type: none"> • 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. |

8.8 Interface Setup

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

Use this screen to set IPv6 interfaces on which you can configure an IPv6 address to access and manage the Switch.

Click **Basic Setting** > **Interface Setup** in the navigation panel to display the configuration screen.

Figure 76 Basic Setting > Interface Setup

The following table describes the labels in this screen.

Table 37 Basic Setting > Interface Setup

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

8.9 IPv6

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

8.9.1 IPv6 Status

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

Figure 77 Basic Setting > IPv6

The screenshot shows the IPv6 configuration page. At the top, there is a header 'IPv6 Status' and a link 'IPv6 Configuration'. Below this, there are two input fields: 'Domain Name Server' and 'Source'. Further down, there is a section titled 'IPv6 Table' which contains a table with three columns: 'Index', 'Interface', and 'Active'. The table has one row with the values '1', 'VLAN1', and 'Yes' respectively.

| IPv6 Status | | IPv6 Configuration |
|--------------------|-----------|------------------------------------|
| Domain Name Server | Source | |
| | | |
| IPv6 Table | | |
| Index | Interface | Active |
| 1 | VLAN1 | Yes |

The following table describes the labels in this screen.

Table 38 Basic Setting > IPv6

| LABEL | DESCRIPTION |
|--------------------|---|
| IPv6 Status | |
| Domain Name Server | This field displays the IP address of the DNS server. |
| Source | This field displays whether the DNS server address is configured manually (Static) or obtained automatically using DHCPv6 . |
| IPv6 Table | |
| Index | This field displays the index number of an IPv6 interface. Click on an index number to view more interface details. |
| Interface | This is the name of the IPv6 interface you created. |
| Active | This field displays whether the IPv6 interface is activated or not. |

8.9.2 IPv6 Interface Status

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

Figure 78 Basic Setting > IPv6 > IPv6 Interface Status

| IPv6 Interface Status | | IPv6 Status |
|----------------------------------|--------------------------------------|-----------------------------|
| Interface: VLAN1 | | |
| IPv6 Active | enable | |
| MTU Size | 1500 | |
| ICMPv6 Rate Limit Bucket Size | 100 | |
| ICMPv6 Rate Limit Error Interval | 1000 | |
| Stateless Address Autoconfig | enable | |
| Link Local Address | fe80::219:cbff:fe00:1/64 [preferred] | |
| Global Unicast Address(es) | | |
| Joined Group Address(es) | #01::1 #02::1 #02::1:ff00:1 | |
| ND DAD Active | enable | |
| Number of DAD Attempts | 1 | |
| NS-Interval (millisecond) | 1000 | |
| ND Reachable Time (millisecond) | 30000 | |
| | | |
| DHCPv6 Client Active | Yes | |
| | IA Type | IA-NA |
| | IAID | 11 |
| | T1 | 0 |
| | T2 | 0 |
| Identity Association | State | |
| | SID | |
| | Address | |
| | Preferred Lifetime | 0 |
| | Valid Lifetime | 0 |
| DNS | | |
| Domain List | | |
| | | |
| Restart DHCPv6 Client | | Click Here |

The following table describes the labels in this screen.

Table 39 Basic Setting > IPv6 > IPv6 Interface Status

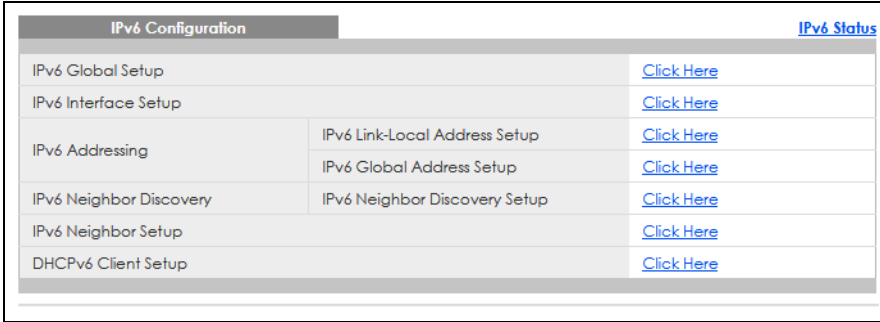
| LABEL | DESCRIPTION |
|----------------------------------|---|
| IPv6 Active | This field displays whether the IPv6 interface is activated or not. |
| MTU Size | This field displays the Maximum Transmission Unit (MTU) size for IPv6 packets on this interface. |
| ICMPv6 Rate Limit Bucket Size | This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

Table 39 Basic Setting > IPv6 > IPv6 Interface Status (continued)

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

8.9.3 IPv6 Configuration

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

Figure 79 Basic Setting > IPv6 > IPv6 Configuration

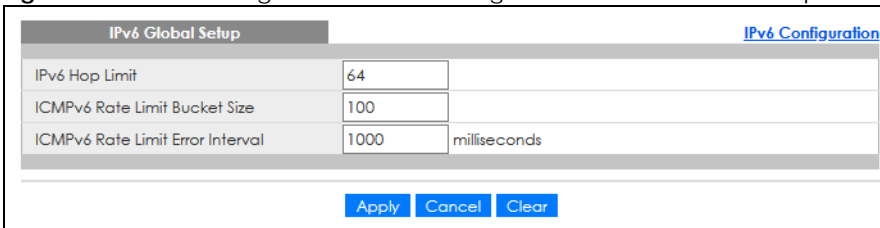
The following table describes the labels in this screen.

Table 40 Basic Setting > IPv6 > IPv6 Configuration

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

8.9.4 IPv6 Global Setup

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

Figure 80 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Setup

The following table describes the labels in this screen.

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

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

8.9.5 IPv6 Interface Setup

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

Figure 81 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Interface Setup

| Index | Interface | Active | Address Autoconfig |
|-------|-----------|--------|--------------------|
| 1 | VLAN1 | Yes | Yes |

The following table describes the labels in this screen.

Table 42 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Interface Setup

| LABEL | DESCRIPTION |
|--------------------|--|
| Interface | Select the IPv6 interface you want to configure. |
| Active | Select this option to enable the interface. |
| Address Autoconfig | Select this option to allow the interface to automatically generate a link-local address through stateless auto-configuration. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |
| Clear | Click Clear to reset the fields to the factory defaults. |
| Index | This is the interface index number. Click on an index number to change the settings. |
| Interface | This is the name of the IPv6 interface you created. |

Table 42 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Interface Setup (continued)

| LABEL | DESCRIPTION |
|--------------------|---|
| Active | This field displays whether the IPv6 interface is activated or not. |
| Address Autoconfig | This field displays whether stateless auto-configuration is enabled on the interface. |

8.9.6 IPv6 Link-Local Address Setup

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

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

Figure 82 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Link-Local Address Setup

| Index | Interface | IPv6 Link-Local Address | IPv6 Default Gateway |
|-------|-----------|-------------------------|----------------------|
| 1 | VLAN1 | | |

The following table describes the labels in this screen.

Table 43 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 non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |
| Clear | Click Clear to reset the fields to the factory defaults. |
| Index | This is the interface index number. Click an index number to change the settings. |
| Interface | This is the name of the IPv6 interface you created. |
| IPv6 Link-Local Address | This is the static IPv6 link-local address for the interface. |
| IPv6 Default Gateway | This is the default gateway IPv6 address for the interface. |

8.9.7 IPv6 Global Address Setup

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

Figure 83 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Address Setup

The following table describes the labels in this screen.

Table 44 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Address Setup

| LABEL | DESCRIPTION |
|-----------------------------------|---|
| Domain Name Server 1/2 | Enter a domain name server IPv6 address in order to be able to use a domain name instead of an IP address. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click this to reset the Domain Name Server values in this screen to their last-saved values. |
| Interface | Select the IPv6 interface you want to configure. |
| IPv6 Global Address | Manually configure a static IPv6 global address for the interface. |
| Prefix Length | Specify an IPv6 prefix length that specifies how many most significant bits (start from the left) in the address compose the network address. |
| EUI-64 | Select this option to have the interface ID be generated automatically using the EUI-64 format. |
| Add | Click this to create a new entry. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |
| Clear | Click Clear to reset the fields to the factory defaults. |
| Index | This is the interface index number. Click 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. |

Table 44 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Global Address Setup (continued)

| LABEL | DESCRIPTION |
|--------|---|
| EUI-64 | This shows whether the interface ID of the global address is generated using the EUI-64 format. |
| | Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries. |
| Delete | Check the entries that you want to remove and then click Delete to remove the selected entries from the summary table. |
| Cancel | Click Cancel to clear the check boxes. |

8.9.8 IPv6 Neighbor Discovery Setup

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

Figure 84 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Discovery Setup

| Index | Interface | DAD Attempts | NS Interval | Reachable Time |
|-------|-----------|--------------|-------------|----------------|
| 1 | VLAN1 | 1 | 1000 | 30000 |

The following table describes the labels in this screen.

Table 45 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. Specify the number of consecutive neighbor solicitations (from 0 to 600) the Switch sends for this interface. Enter 0 to turn off DAD. |
| NS Interval | Specify the time interval (from 1000 to 3600000 milliseconds) at which neighbor solicitations are re-sent for this interface. |
| Reachable Time | Specify how long (from 1000 to 3600000 milliseconds) a neighbor is considered reachable for this interface. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |
| Clear | Click Clear to reset the fields to the factory defaults. |
| Index | This is the interface index number. Click on an index number to change the settings. |
| Interface | This is the name of the IPv6 interface you created. |
| DAD Attempts | This field displays the number of consecutive neighbor solicitations the Switch sends for this interface. |

Table 45 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. |

8.9.9 IPv6 Neighbor Setup

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

Figure 85 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Setup

The following table describes the labels in this screen.

Table 46 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Setup

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

Table 46 Basic Setting > IPv6 > IPv6 Configuration > IPv6 Neighbor Setup (continued)

| LABEL | DESCRIPTION |
|------------------|---|
| Interface | This is the name of the IPv6 interface you created. |
| Neighbor Address | This field displays the IPv6 address of the neighboring device which can be reached through the interface. |
| MAC | This field displays the MAC address of the neighboring device which can be reached through the interface. |
| | Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries. |
| Delete | Check the entries that you want to remove and then click Delete to remove the selected entries from the summary table. |
| Cancel | Click Cancel to clear the check boxes. |

8.9.10 DHCPv6 Client Setup

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

Figure 86 Basic Setting > IPv6 > IPv6 Configuration > DHCPv6 Client Setup

| Index | Interface | IA-NA | Rapid-Commit | DNS | Domain-List | Information Refresh Minimum |
|-------|-----------|-------|--------------|-----|-------------|-----------------------------|
| 1 | VLAN1 | No | No | No | No | 86400 |

The following table describes the labels in this screen.

Table 47 Basic Setting > IPv6 > IPv6 Configuration > DHCPv6 Client Setup

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

Table 47 Basic Setting > IPv6 > IPv6 Configuration > DHCPv6 Client Setup (continued)

| LABEL | DESCRIPTION |
|-----------------------------|--|
| 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 an index number to change the settings. |
| Interface | This is the name of the IPv6 interface you created. |
| IA-NA | This field displays whether the Switch obtains a non-temporary IP address from the DHCPv6 server. |
| Rapid-Commit | This field displays whether the Switch obtains information from the DHCPv6 server by a rapid two-message exchange. |
| DNS | This field displays whether the Switch obtains DNS server IPv6 addresses from the DHCPv6 server. |
| Domain-List | This field displays whether the Switch obtains a list of domain names from the DHCP server. |
| Information Refresh Minimum | This field displays the time interval (in seconds) at which the Switch exchanges other configuration information with a DHCPv6 server again. |

8.10 Cloud Management

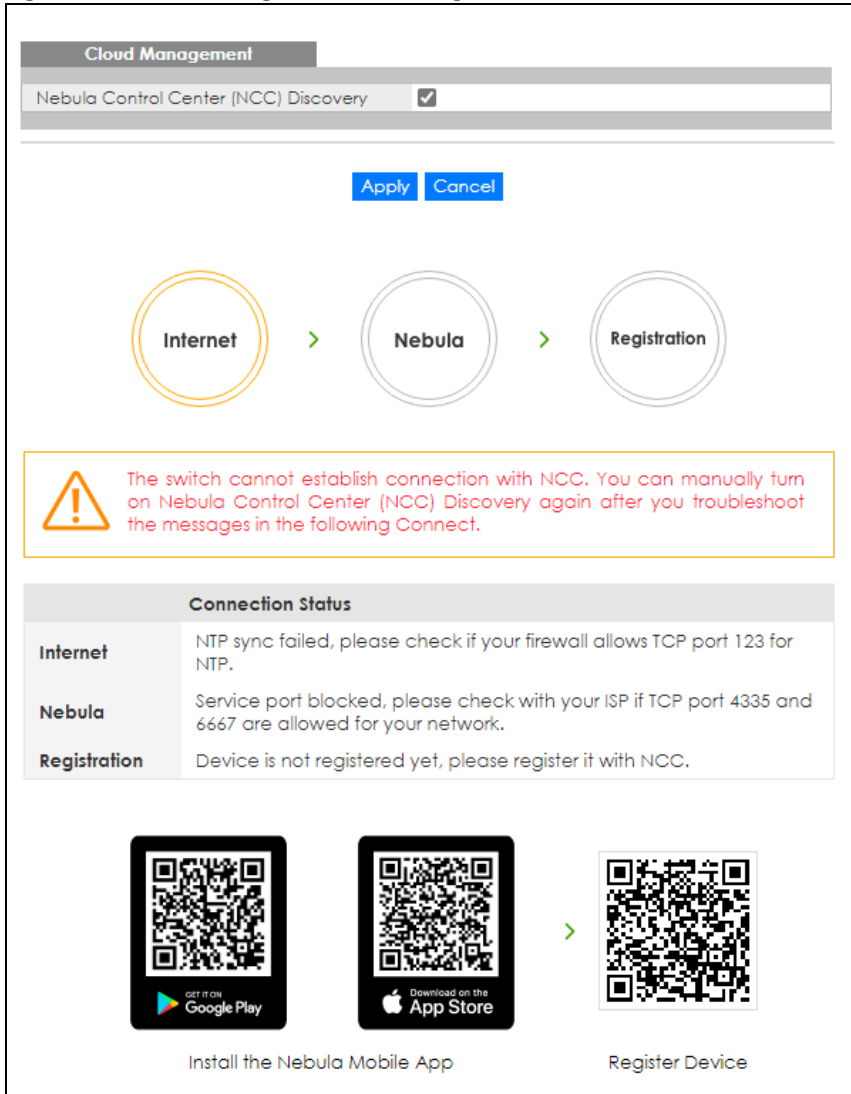
The Zyxel Nebula Control Center (NCC) is a cloud-based network management system that allows you to remotely manage and monitor Zyxel Nebula APs, Ethernet switches and security gateways.

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.

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

Figure 87 Basic Setting > Cloud Management



The following table describes the labels in this screen.

Table 48 Basic Setting > Cloud Management

| LABEL | DESCRIPTION |
|---------------------------------------|--|
| Nebula Control Center (NCC) Discovery | Select this to turn on NCC discovery on the Switch. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |

Table 48 Basic Setting > Cloud Management

| LABEL | DESCRIPTION |
|-------------------|--|
| Cancel | Click Cancel to begin configuring this screen afresh. |
| Connection Status | <p>This field displays:</p> <ul style="list-style-type: none"> • The Switch Internet connection status. • The connection status between the Switch and NCC. • The Switch registration status on NCC. <p>To Pass your Switch management to NCC, first make sure your Switch is connected to the Internet. Then go to NCC and register your Switch.</p> <p>1. Internet</p> <p>Green - The Switch is connected to the Internet.</p> <p>Orange - The Switch is not connected to the Internet.</p> <p>2. Nebula</p> <p>Green - The Switch is connected to NCC.</p> <p>Orange - The Switch is not connected to NCC.</p> <p>3. Registration</p> <p>Green - The Switch is registered on NCC.</p> <p>Gray - The Switch is not registered on NCC.</p> <p>Note: All circles will gray out if you disable Nebula Discovery.</p> <p>This table displays the NCC connection status information.</p> <p>Use the status logs in the Internet, Nebula, and Registration fields for connection troubleshooting.</p> |

8.10.1 Nebula Center Control Discovery

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

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

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

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

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

CHAPTER 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** screen ([Section 9.3 on page 120](#)) to view and search all static VLAN groups.
- Use the **VLAN Detail** screen ([Section 9.3.1 on page 121](#)) to view detailed port settings and status of the static VLAN group.
- Use the **Static VLAN Setup** screen ([Section 9.5 on page 123](#)) to configure a static VLAN for the Switch.
- Use the **VLAN Port Setup** screen ([Section 9.6 on page 124](#)) to configure the static VLAN (IEEE 802.1Q) settings on a port.
- Use the **Voice VLAN Setup** screen ([Section 9.7 on page 125](#)) to set up VLANs that allow you to group voice traffic with defined priority and enable the Switch port to carry the voice traffic separately from data traffic to ensure the sound quality does NOT deteriorate.
- Use the **MAC Based VLAN Setup** screen ([Section 9.8 on page 127](#)) to set up VLANs that allow you to group untagged packets into logical VLANs based on the source MAC address of the packet. This eliminates the need to reconfigure the Switch when you change ports. The Switch will forward the packets based on the source MAC address you set up previously.
- Use the **Vendor ID Based VLAN Setup** screen ([Section 9.9 on page 128](#)) to set up VLANs that allow you to group untagged packets into logical VLANs based on the source MAC address of the packet. You can specify a mask for the MAC address to create a MAC address filter and enter a weight to set the VLAN rule's priority.
- Use the **Port-Based VLAN Setup** screen ([Section 9.10 on page 130](#)) to set up VLANs where the packet forwarding decision is based on the destination MAC address and its associated port.

9.1.2 What You Need to Know

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

9.2 Introduction to IEEE 802.1Q Tagged VLANs

A tagged VLAN uses an explicit tag (VLAN ID) in the MAC header to identify the VLAN membership of a frame across bridges – they are not confined to the switch on which they were created. The VLANs can be created statically by hand. The VLAN ID associates a frame with a specific VLAN and provides the information that switches need to process the frame across the network. A tagged frame is 4 bytes longer than an untagged frame and contains 2 bytes (16 Bits) of TPID (Tag Protocol Identifier, residing within the type or length field of the Ethernet frame) and 2 bytes (16 Bits) of TCI (Tag Control Information,

starts after the source address field of the Ethernet frame). The TCI field consists of three fields: User Priority, CFI (Canonical Format Indicator), and VLAN ID.

The CFI (Canonical Format Indicator) is a single-bit flag, always set to zero for Ethernet switches. If a frame received at an Ethernet port has a CFI set to 1, then that frame should not be forwarded as it is to an untagged port. The remaining twelve bits define the VLAN ID, giving a possible maximum number of 4096 VLANs. Note that user priority and VLAN ID are independent of each other. A frame with VID (VLAN Identifier) of null (0) is called a priority frame, meaning that only the priority level is significant and the default VID of the ingress port is given as the VID of the frame. Of the 4096 possible VIDs, a VID of 0 is used to identify priority frames and value 4095 (FFF) is reserved, so the maximum possible VLAN configurations are 4094.

| TPID | User Priority | CFI | VLAN ID |
|---------|---------------|-------|---------|
| 16 Bits | 3 Bits | 1 Bit | 12 Bits |

Forwarding Tagged and Untagged Frames

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

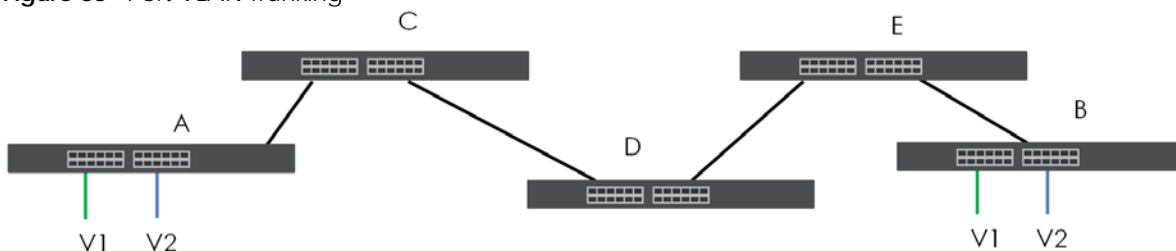
A broadcast frame (or a multicast frame for a multicast group that is known by the system) is duplicated only on ports that are members of the VID (except the ingress port itself), thus confining the broadcast to a specific domain.

9.2.0.1 Port VLAN Trunking

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

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

Figure 88 Port VLAN Trunking



At the time of writing, you can create static VLANs, Voice VLANs, MAC-based 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
- 3 MAC Based VLAN

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

9.2.0.2 Select the VLAN Type

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

Figure 89 Basic Setting > Switch Setup > Select VLAN Type

| Switch Setup | | | |
|--|---|-----|---------|
| VLAN Type | <input checked="" type="radio"/> 802.1Q <input type="radio"/> Port Based | | |
| MAC Address Learning | Aging Time | 300 | seconds |
| ARP Aging Time | Aging Time | 300 | seconds |
| Priority Queue Assignment | Priority7 | 7 | ▼ |
| | Priority6 | 6 | ▼ |
| | Priority5 | 5 | ▼ |
| | Priority4 | 4 | ▼ |
| | Priority3 | 3 | ▼ |
| | Priority2 | 1 | ▼ |
| | Priority1 | 0 | ▼ |
| | Priority0 | 2 | ▼ |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | | | |

802.1Q Static VLAN

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

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

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

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

9.3 VLAN Status

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

Figure 90 Advanced Application > VLAN: VLAN Status

The screenshot shows the 'VLAN Status' page. At the top, there is a search bar labeled 'VLAN Search by VID' with a 'Search' button. Below the search bar, it says 'The Number of VLAN: 2.' A table lists two VLANs:

| Index | VID | Name | Tagged Port | Untagged Port | Elapsed Time | Status |
|-------|-----|---------|-------------|---------------|--------------|--------|
| 1 | 1 | 1 | | 1-6 | 98:24:33 | Static |
| 2 | 123 | VLAN123 | | | 67:30:19 | Static |

At the bottom, there are 'Change Pages' buttons for 'Previous' and '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 numbers (use a comma (,) to separate individual VLANs or a dash (-) to indicate a range of VLANs. For example, "3,4" or "3-9") and click Search to display only the specified VLANs in the list below. Leave this field blank and click Search to display all VLANs configured on the Switch. |
| The Number of VLAN | This is the number of VLANs configured on the Switch. |
| The Number of Search Results | This is the number of VLANs that match the searching criteria and display in the list below. This field displays only when you use the Search button to look for certain VLANs. |
| Index | This is the VLAN index number. Click an index number to view more VLAN details. |
| VID | This is the VLAN identification number that was configured in the corresponding VLAN configuration screen. |
| Name | This fields shows the descriptive name of the VLAN. |
| Tagged Port | This field shows the tagged ports that are participating in the VLAN. |
| Untagged Port | This field shows the untagged ports that are participating in the VLAN. |
| Elapsed Time | This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up. |
| Status | This field shows how this VLAN was added to the Switch. Static: added as a permanent entry. |
| Change Pages | Click Previous or Next to show the previous or next screen if all status information cannot be seen in one screen. |

9.3.1 VLAN Details

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

Figure 91 Advanced Application > VLAN > VLAN Detail

| VLAN Detail | | | | | VLAN Status | |
|-------------|-------------|---|---|---|-----------------------------|--------|
| VID | Port Number | | | | Elapsed Time | Status |
| | 2 | 4 | 6 | 8 | | |
| | 1 | 3 | 5 | 7 | | |
| 1 | U | U | U | U | 6:51:24 | Static |
| | 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 corresponding VLAN configuration screen. |
| Port Number | This column displays the ports that are participating in a VLAN. A tagged port is marked as T , an untagged port is marked as U and ports not participating in a VLAN are marked as - . |
| Elapsed Time | This field shows how long it has been since a normal VLAN was registered or a static VLAN was set up. |
| Status | This field shows how this VLAN was added to the Switch. Static: added as a permanent entry. |

9.4 VLAN Configuration

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

Figure 92 Advanced Application > VLAN > VLAN Configuration

| VLAN Configuration | | VLAN Status |
|----------------------------|----------------------------|-----------------------------|
| Static VLAN Setup | Click Here | |
| VLAN Port Setup | Click Here | |
| Voice VLAN Setup | Click Here | |
| MAC Based 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. |
| MAC Based VLAN Setup | Click Click Here to configure the MAC Based VLAN for the Switch. |
| Vendor ID Based VLAN Setup | Click Click Here to configure the Vendor ID Based VLAN for the Switch. |

9.5 Configure a Static VLAN

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

Figure 93 Advanced Application > VLAN > VLAN Configuration > Static VLAN Setup

The screenshot shows the 'Static VLAN' configuration interface. At the top, there is a header 'Static VLAN' and a link 'VLAN Configuration'. Below this is an 'ACTIVE' checkbox. There are two input fields: 'Name' and 'VLAN Group ID'. The main part of the screen is a table with three columns: 'Port', 'Control', and 'Tagging'. The 'Port' column lists ports from 1 to 8, plus a '*' row for all ports. The 'Control' column has radio buttons for 'Normal', 'Fixed', and 'Forbidden'. The 'Tagging' column has a checked 'Tx Tagging' checkbox. Below the table are 'Add', 'Cancel', and 'Clear' buttons. At the bottom, there is a table with columns 'VID', 'Active', and 'Name', and 'Delete' and 'Cancel' buttons.

| Port | Control | Tagging |
|------|---|--|
| * | Normal | <input checked="" type="checkbox"/> Tx Tagging |
| 1 | <input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden | <input checked="" type="checkbox"/> Tx Tagging |
| 2 | <input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden | <input checked="" type="checkbox"/> Tx Tagging |
| 3 | <input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden | <input checked="" type="checkbox"/> Tx Tagging |
| 4 | <input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden | <input checked="" type="checkbox"/> Tx Tagging |
| 5 | <input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden | <input checked="" type="checkbox"/> Tx Tagging |
| 6 | <input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden | <input checked="" type="checkbox"/> Tx Tagging |
| 7 | <input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden | <input checked="" type="checkbox"/> Tx Tagging |
| 8 | <input checked="" type="radio"/> Normal <input type="radio"/> Fixed <input type="radio"/> Forbidden | <input checked="" type="checkbox"/> Tx Tagging |

| VID | Active | Name |
|-----|--------|------|
| 1 | Yes | 1 |

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. The string should not contain [?], [], ['], ["] or [,]. |
| VLAN Group ID | Enter the VLAN ID for this static entry; the valid range is between 1 and 4094. Note: Do NOT add a VLAN ID that has been used in the Voice VLAN Setup . |
| Port | The port number identifies the port you are configuring. |
| * | Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them. |
| Control | Select Normal to exclude the port from VLAN. 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. |

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

| LABEL | DESCRIPTION |
|---------|---|
| Tagging | Select TX Tagging if you want outgoing traffic to contain this VLAN tag. Otherwise, to ensure that VLAN-unaware devices (such as computers and hubs) can receive frames properly, clear the TX Tagging check box to set the Switch to remove VLAN tags before sending. |
| Add | Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |
| Clear | Click Clear to start configuring the screen again. |
| VID | This field displays the ID number of the VLAN group. Click the number to edit the VLAN settings. |
| Active | This field indicates whether the VLAN settings are enabled (Yes) or disabled (No). |
| Name | This field displays the descriptive name for this VLAN group. |
| | Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries. |
| Delete | Click Delete to remove the selected entry from the summary table. |
| Cancel | Click Cancel to clear the check boxes. |

9.6 Configure VLAN Port Settings

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

Figure 94 Advanced Application > VLAN > VLAN Configuration > VLAN Port Setup

| VLAN Port Setting | | | | VLAN Configuration | |
|-------------------|--------------------------|------|------------------------------------|------------------------------------|--------------------------|
| Port | Ingress Check | PVID | Acceptable Frame Type | VLAN Trunking | Isolation |
| * | <input type="checkbox"/> | | All <input type="text" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 1 | <input type="checkbox"/> | 1 | All <input type="text" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2 | <input type="checkbox"/> | 1 | All <input type="text" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3 | <input type="checkbox"/> | 1 | All <input type="text" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4 | <input type="checkbox"/> | 1 | All <input type="text" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 5 | <input type="checkbox"/> | 1 | All <input type="text" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 6 | <input type="checkbox"/> | 1 | All <input type="text" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 7 | <input type="checkbox"/> | 1 | All <input type="text" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 8 | <input type="checkbox"/> | 1 | All <input type="text" value="v"/> | <input type="checkbox"/> | <input type="checkbox"/> |

The following table describes the labels in this screen.

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

| LABEL | DESCRIPTION |
|-----------------------|--|
| Port | This field displays the port number. |
| * | Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them. |
| Ingress Check | If this 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. |
| Acceptable Frame Type | Specify the type of frames allowed on a port. Choices are All , Tag Only and Untag Only . Select All from the drop-down list box to accept all untagged or tagged frames on this port. This is the default setting. Select Tag Only to accept only tagged frames on this port. All untagged frames will be dropped. Select Untag Only to accept only untagged frames on this port. All tagged frames will be dropped. |
| VLAN Trunking | Enable VLAN Trunking on ports connected to other switches or routers (but not ports directly connected to end users) to allow frames belonging to unknown VLAN groups to pass through the Switch. |
| Isolation | Select this to allow this port to communicate only with the CPU management port and the ports on which the isolation feature is NOT enabled. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

9.7 Voice VLAN

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

The Switch can determine whether a received packet is

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

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

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

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

Figure 95 Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup

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. Enter a VLAN ID number that is associated with the Voice VLAN. Click the Disable radio button if you do not want to enable the Voice VLAN feature. |
| Priority | Select the priority level of the voice traffic from 0 to 7. Default setting is 5. The higher the numeric value you assign, the higher the priority for this voice traffic. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this section afresh. |
| Clear | Click Clear to reset the fields to default settings. |
| Voice VLAN OUI Setup | |
| OUI address | Enter the IP phone manufacturer's OUI MAC address. The first 3 bytes is the manufacturer identifier, the last 3 bytes is a unique station ID. |
| OUI mask | Enter the mask for the specified IP phone manufacturer's OUI MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified MAC address that the traffic's MAC address should match. Enter "0" for the bits of the matched traffic's MAC address, which can be of any hexadecimal characters. For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria. |

Table 54 Advanced Application > VLAN > VLAN Configuration > Voice VLAN Setup (continued)

| LABEL | DESCRIPTION |
|-------------|--|
| Description | Enter a description up to 32 characters excluding [?], [], ['], or ["] for the Voice VLAN device. For example: Siemens. |
| Add | Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this section afresh. |
| Index | This field displays the index number of the Voice VLAN. |
| OUI address | This field displays the OUI address of the Voice VLAN. |
| OUI mask | This field displays the OUI mask address of the Voice VLAN. |
| Description | This field displays the description of the Voice VLAN with OUI address. |
| | Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries. |
| Delete | Click Delete to remove the selected entry from the summary table. |
| Cancel | Click Cancel to clear the check boxes. |

9.8 MAC Based VLAN

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

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

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

Figure 96 Advanced Application > VLAN > VLAN Configuration > MAC Based VLAN Setup

The screenshot shows the 'MAC Based VLAN' configuration interface. At the top, there is a header 'MAC Based VLAN' and a link 'VLAN Configuration'. Below the header, there are four input fields: 'Name', 'MAC Address', 'VID', and 'Priority'. Below these fields are two buttons: 'Add' and 'Cancel'. Below the buttons is a table with columns: 'Index', 'Name', 'MAC Address', 'VID', 'Priority', and a checkbox. Below the table are two buttons: 'Delete' and 'Cancel'.

The following table describes the fields in the above screen.

Table 55 Advanced Application > VLAN > VLAN Configuration > MAC Based VLAN Setup

| LABEL | DESCRIPTION |
|-------------|---|
| Name | Enter a name up to 32 alphanumeric characters excluding [?], [], ['], ["] or [.] for the MAC-based VLAN entry. |
| MAC Address | Enter a MAC address that is bind to the MAC-based VLAN entry. This is the source MAC address of the data packet that is looked up when untagged packets arrive at the Switch. |
| VID | Enter an ID (from 1 to 4094) for the VLAN that is associated with the MAC-based VLAN entry. |
| Priority | Enter a priority (0 to 7) that the Switch assigns to frames belonging to this VLAN. The higher the numeric value you assign, the higher the priority for this MAC-based VLAN entry. |
| Add | Click Add to save the new MAC-based VLAN entry. |
| Cancel | Click Cancel to clear the fields in the MAC-based VLAN entry. |
| Index | This field displays the index number of the MAC-based VLAN entry. |
| Name | This field displays the name of the MAC-based VLAN entry. |
| MAC Address | This field displays the source MAC address that is bind to the MAC-based VLAN entry. |
| VID | This field displays the VLAN ID of the MAC-based VLAN entry. |
| Priority | This field displays the priority level which is assigned to frames belonging to this MAC-based VLAN entity. |
| | Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries. |
| Delete | Click Delete to remove the selected entry from the summary table. |
| Cancel | Click Cancel to clear the check boxes. |

9.9 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 97 Advanced Application > VLAN > VLAN Configuration > Vendor ID Based VLAN Setup

The following table describes the fields in the above screen.

Table 56 Advanced Application > VLAN > VLAN Configuration > Vendor ID Based VLAN Setup

| LABEL | DESCRIPTION |
|-------------|---|
| Name | Enter a name up to 32 alphanumeric characters excluding [?], [], ['], or ["] for the vendor ID based VLAN entry. |
| MAC Address | Enter 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 | Enter the mask for the specified source MAC address to determine which bits a packet's MAC address should match. Enter "f" for each bit of the specified MAC address that the traffic's MAC address should match. Enter "0" for the bits of the matched traffic's MAC address, which can be of any hexadecimal characters. For example, if you set the MAC address to 00:13:49:00:00:00 and the mask to ff:ff:ff:00:00:00, a packet with a MAC address of 00:13:49:12:34:56 matches this criteria. |
| VLAN | Enter 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 56 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. |

9.10 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.

9.10.1 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 98 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 | | |
| Outgoing | 1 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 1 |
| | 2 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 2 |
| | 3 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 3 |
| | 4 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 4 |
| | 5 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 5 |
| | 6 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 6 |
| | 7 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 7 |
| | 8 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | 8 |
| | CPU | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | CPU |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | | |

Apply Cancel

Figure 99 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 | | |
| Outgoing | 1 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 1 |
| | 2 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 2 |
| | 3 | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 3 |
| | 4 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 4 |
| | 5 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 5 |
| | 6 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | 6 |
| | 7 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | 7 |
| | 8 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 8 |
| | CPU | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | CPU |
| | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | | |

Apply Cancel

The following table describes the labels in this screen.

Table 57 Advanced Application > VLAN: Port Based VLAN Setup

| LABEL | DESCRIPTION |
|----------------|---|
| Setting Wizard | <p>Choose All connected or Port isolation.</p> <p>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.</p> <p>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.</p> <p>After you make your selection, click Apply (top right of screen) to display the screens as mentioned above. You can still customize these settings by adding or deleting incoming or outgoing ports, but you must also click Apply at the bottom of the screen.</p> |
| Incoming | <p>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.</p> |
| Outgoing | <p>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.</p> |
| Apply | <p>Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring.</p> |
| Cancel | <p>Click Cancel to begin configuring this screen afresh.</p> |

CHAPTER 10

Static MAC Forwarding

10.1 Overview

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

Use these screens to configure static MAC address forwarding.

10.1.1 What You Can Do

Use the **Static MAC Forwarding** screen ([Section 10.2 on page 133](#)) to assign static MAC addresses for a port.

10.2 Configure Static MAC Forwarding

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

Static MAC address forwarding together with port security allow only computers in the MAC address table on a port to access the Switch.

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

Figure 100 Advanced Application > Static MAC Forwarding

| Index | Active | Name | MAC Address | VID | Port | |
|-------|--------|------|-------------|-----|------|--|
|-------|--------|------|-------------|-----|------|--|

The following table describes the labels in this screen.

Table 58 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. The string should not contain [?], [], ['], ["] or [,]. |
| MAC Address | Enter the MAC address in valid MAC address format, that is, six hexadecimal character pairs. Note: Static MAC addresses do NOT age out. |
| VID | Enter the VLAN identification number. |
| Port | Enter the port where the MAC address entered in the previous field will be automatically forwarded. |
| Add | Click this to create a new entry or to update an existing one. This saves your rule to the Switch's run-time memory. The Switch loses this rule if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to reset the fields to their last saved values. |
| Clear | Click Clear to begin configuring this screen afresh. |
| Index | Click an index number to modify a static MAC address rule for a port. |
| Active | This field displays whether this static MAC address forwarding rule is active (Yes) or not (No). You may temporarily deactivate a rule without deleting it. |
| Name | This field displays the descriptive name for identification purposes for this static MAC address-forwarding rule. |
| MAC Address | This field displays the MAC address that will be forwarded and the VLAN identification number to which the MAC address belongs. |
| VID | This field displays the ID number of the VLAN group. |
| Port | This field displays the port where the MAC address shown in the next field will be forwarded. |
| | Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries. |
| Delete | Click Delete to remove the selected entry from the summary table. |
| Cancel | Click Cancel to clear the check boxes. |

CHAPTER 11

Static Multicast Forwarding

11.1 Static Multicast Forwarding Overview

This chapter discusses how to configure static multicast forwarding rules based on multicast MAC addresses or multicast IPv4 addresses.

11.1.1 What You Can Do

Use the **Static Multicast Forwarding** screen ([Section 11.2 on page 136](#)) to configure rules to forward specific multicast frames, such as streaming or control frames, to specific ports.

11.1.2 What You Need To Know

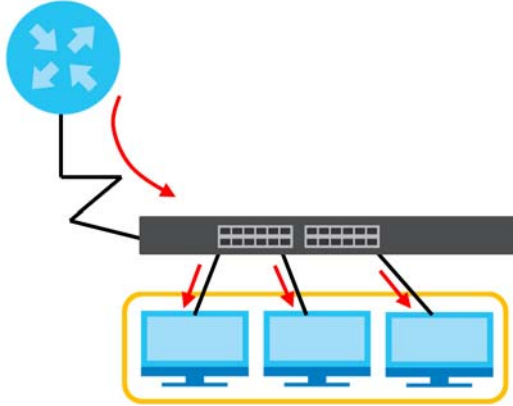
A multicast MAC address or multicast IP address is the MAC address or IP address of a multicast group.

A static multicast address is a multicast MAC address or multicast IPv4 address that has been manually entered in the multicast table. This identifies the destination of the multicast content. Multicast IPv4 addresses use the Class D IP address range 224.0.0.0 to 239.255.255.255. Multicast MAC addresses have a "1" as the last binary bit of the first octet pair (for example, 01:00:5e:00:00:0A). Static multicast addresses do not age out. See [IP Multicast Addresses on page 167](#) for more information on IP multicast addresses.

Note: Static (manual) multicast forwarding allows you (the administrator) to forward multicast frames to a member without the member having to join the group first.

If a multicast group has no members, then the Switch cannot forward to specific ports unless you configure static (manual) multicast entries. The Switch will either flood the multicast frames to all ports (default) or drop them. [Figure 101 on page 136](#) shows such unknown multicast frames flooded to all ports. With static multicast forwarding, you can forward these multicasts to ports within a VLAN group.

Figure 101 No Multicast Forwarding



11.2 Static Multicast Forwarding Configuration

Click **Advanced Application > Static Multicast Forwarding** to see the following screen.

Figure 102 Advanced Application > Static Multicast Forwarding

The following table describes the labels in this screen.

Table 59 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 | Enter a descriptive name (up to 32 single-byte printable characters except [?], [], ['], ["] or [, ,]) for this static multicast MAC address forwarding rule. This is for identification only. |
| MAC Address | Enter a multicast MAC address which identifies the multicast group. The last binary bit of the first octet pair in a multicast MAC address must be 1. For example, the first octet pair 00000001 is 01 in hexadecimal, so 01:00:5e:00:00:0A and 01:00:5e:00:00:27 are valid multicast MAC addresses. |
| VID | You can forward frames with matching destination multicast MAC address to ports within a VLAN group. Enter the ID that identifies the VLAN group here. If you do NOT have a specific target VLAN, enter 1. |

Table 59 Advanced Application > Static Multicast Forwarding (continued)

| LABEL | DESCRIPTION |
|-------------|---|
| Port | Enter the ports where frames with destination multicast MAC address that matched the entry above are forwarded. You can enter multiple ports separated by (no space) comma (,) or hyphen (-). For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7. |
| Add | Click this to create a new entry or to update an existing one. This saves your rule to the Switch's run-time memory. The Switch loses this rule if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to reset the fields to their last saved values. |
| Clear | Click Clear to begin configuring this screen afresh. |
| Index | Click an index number to modify a static multicast MAC address rule for ports. |
| Active | This field displays whether a static multicast MAC address forwarding rule is active (Yes) or not (No). You may temporarily deactivate a rule without deleting it. |
| Name | This field displays the descriptive name for identification purposes for a static multicast MAC address-forwarding rule. |
| MAC Address | This field displays the multicast MAC address that identifies a multicast group. |
| VID | This field displays the ID number of a VLAN group to which frames containing the specified multicast MAC address will be forwarded. |
| Port | This field displays the ports within an 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. |
| 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 138](#)) 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 103 Advanced Application > Filtering

| Index | Active | Name | MAC Address | VID | Action | <input type="checkbox"/> |
|-------|--------|------|-------------|-----|--------|--------------------------|
|-------|--------|------|-------------|-----|--------|--------------------------|

The following table describes the related labels in this screen.

Table 60 Advanced Application > Filtering

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

CHAPTER 13

Spanning Tree Protocol

13.1 Spanning Tree Protocol Overview

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

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

13.1.1 What You Can Do

- Use the **Rapid Spanning Tree Protocol Status** screen ([Section 13.2 on page 142](#)) to view the RSTP status.
- Use the **Rapid Spanning Tree Protocol** screen ([Section 13.3 on page 143](#)) to configure RSTP settings.

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 61 STP Path Costs

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

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

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

How STP Works

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

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

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

STP Port States

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

Table 62 STP Port States

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

13.2 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 140](#) for more information on RSTP.

Figure 104 Advanced Application > Spanning Tree Protocol

| Spanning Tree Protocol Status | | | RSTP | | |
|-------------------------------|-------------------|-------------------|----------------------|--|--|
| Spanning Tree Protocol: RSTP | | | | | |
| Bridge | Root | Our Bridge | | | |
| Bridge ID | 8000-0019cb000001 | 8000-0019cb000001 | | | |
| Hello Time (second) | 2 | 2 | | | |
| Max Age (second) | 20 | 20 | | | |
| Forwarding Delay (second) | 15 | 15 | | | |
| Cost to Bridge | 0 | | | | |
| Port ID | 0X0000 | | | | |
| Topology Changed Times | 3 | | | | |
| Time Since Last Change | 0:00:15 | | | | |

| Port | Port State | Port Role | Designated Bridge ID | Designated Port ID | Designated Cost |
|------|------------|------------|----------------------|--------------------|-----------------|
| 1 | FORWARDING | Designated | 8000-0019cb000001 | 0x8001 | 0 |
| 2 | DISCARDING | Disabled | 0000-000000000000 | 0x0000 | 0 |
| 3 | FORWARDING | Designated | 8000-0019cb000001 | 0x8003 | 0 |
| 4 | FORWARDING | Designated | 8000-0019cb000001 | 0x8004 | 0 |
| 5 | DISCARDING | Disabled | 0000-000000000000 | 0x0000 | 0 |
| 6 | DISCARDING | Disabled | 0000-000000000000 | 0x0000 | 0 |

The following table describes the labels in this screen.

Table 63 Advanced Application > Spanning Tree Protocol

| LABEL | DESCRIPTION |
|---------------------------|--|
| RSTP | Click RSTP to edit RSTP settings on the Switch. |
| Bridge | Root refers to the base of the spanning tree (the root bridge). Our Bridge is this Switch. This Switch may also be the root bridge. |
| Bridge ID | This is the unique identifier for this bridge, consisting of 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. |

Table 63 Advanced Application > Spanning Tree Protocol (continued)

| LABEL | DESCRIPTION |
|----------------------|---|
| Port | This field displays the number of the port on the Switch. |
| Port State | <p>This field displays the port state in STP.</p> <ul style="list-style-type: none"> • Discarding – The port does not forward or process received frames or learn MAC addresses, but still listens for BPDUs. • Learning – The port learns MAC addresses and processes BPDUs, but does NOT forward frames yet. • Forwarding – The port is operating normally. It learns MAC addresses, processes BPDUs and forwards received frames. |
| Port Role | <p>This field displays the role of the port in STP.</p> <ul style="list-style-type: none"> • Root – A forwarding port on a non-root bridge, which has the lowest path cost and is the best port from the non-root bridge to the root bridge. A root bridge does NOT have a root port. • Designated – A forwarding port on the designated bridge for each connected LAN segment. A designated bridge has the lowest path cost to the root bridge among the bridges connected to the LAN segment. All the ports on a root bridge (root switch) are designated ports. • Alternate – A blocked port, which has a best alternate path to the root bridge. This path is different from using the root port. The port moves to the forwarding state when the designated port for the LAN segment fails. • Backup – A blocked port, which has a backup or redundant path to a LAN segment where a designated port is already connected when a switch has two links to the same LAN segment. • Disabled – Not strictly part of STP. The port can be disabled manually. |
| Designated Bridge ID | This field displays the identifier of the designated bridge to which this port belongs when the port is a designated port. Otherwise, it displays the identifier of the designated bridge for the LAN segment to which this port is connected. |
| Designated Port ID | This field displays the priority and number of the bridge port (on the designated bridge), through which the designated bridge transmits the stored configuration messages. |
| Designated Cost | This field displays the path cost to the LAN segment to which the port is connected when the port is a designated port. Otherwise, it displays the path cost to the root bridge from the designated port for the LAN segment to which this port is connected. |

13.3 Configure Rapid Spanning Tree Protocol

Use this screen to configure RSTP settings, see [Section 13.1 on page 140](#) for more information on RSTP. Click **RSTP** in the **Advanced Application > Spanning Tree Protocol** screen.

Figure 105 Advanced Application > Spanning Tree Protocol > RSTP

| Rapid Spanning Tree Protocol | | Status |
|------------------------------|--------------------------|------------------------|
| Active | <input type="checkbox"/> | |
| Bridge Priority | 32768 ▼ | |
| Hello Time | 2 Seconds | |
| MAX Age | 20 Seconds | |
| Forwarding Delay | 15 Seconds | |

| Port | Active | Edge | Priority | Path Cost |
|------|--------------------------|--------------------------|----------|-----------|
| * | <input type="checkbox"/> | <input type="checkbox"/> | | |
| 1 | <input type="checkbox"/> | <input type="checkbox"/> | 128 | 4 |
| 2 | <input type="checkbox"/> | <input type="checkbox"/> | 128 | 4 |
| 3 | <input type="checkbox"/> | <input type="checkbox"/> | 128 | 4 |
| 4 | <input type="checkbox"/> | <input type="checkbox"/> | 128 | 4 |
| 5 | <input type="checkbox"/> | <input type="checkbox"/> | 128 | 4 |

The following table describes the labels in this screen.

Table 64 Advanced Application > Spanning Tree Protocol > RSTP

| LABEL | DESCRIPTION |
|------------------|---|
| Status | Click Status to display the RSTP Status screen. |
| Active | Select this check box to activate RSTP. Clear this check box to disable RSTP. |
| Bridge Priority | <p>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.</p> <p>The lower the numeric value you assign, the higher the priority for this bridge.</p> <p>Bridge Priority determines the root bridge, which in turn determines Hello Time, Max Age and Forwarding Delay.</p> |
| 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 | <p>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.</p> <p>As a general rule:</p> $2 * (\text{Forward Delay} - 1) \geq \text{Max Age} \geq 2 * (\text{Hello Time} + 1)$ |
| Port | This field displays the port number. |

Table 64 Advanced Application > Spanning Tree Protocol > RSTP (continued)

| LABEL | DESCRIPTION |
|-----------|---|
| * | <p>Settings in this row apply to all ports.</p> <p>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.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p> |
| Active | Select this check box to activate RSTP on this port. |
| Edge | <p>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.</p> <p>Note: An edge port becomes a non-edge port as soon as it receives a Bridge Protocol Data Unit (BPDU).</p> |
| Priority | <p>Configure the priority for each port here.</p> <p>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.</p> |
| Path Cost | Path cost is the cost of transmitting a frame on to a LAN through that port. It is recommended to assign this value according to the speed of the bridge. The slower the media, the higher the cost. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

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 146](#)) 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 106 Advanced Application > Bandwidth Control

| Bandwidth Control | | | | | | |
|---------------------------------|--------------------------|--------------|------|--------------------------|-------------|------|
| Active <input type="checkbox"/> | | | | | | |
| Port | Active | Ingress Rate | | Active | Egress Rate | |
| * | <input type="checkbox"/> | | kbps | <input type="checkbox"/> | | kbps |
| 1 | <input type="checkbox"/> | 64 | kbps | <input type="checkbox"/> | 64 | kbps |
| 2 | <input type="checkbox"/> | 64 | kbps | <input type="checkbox"/> | 64 | kbps |
| 3 | <input type="checkbox"/> | 64 | kbps | <input type="checkbox"/> | 64 | kbps |
| 4 | <input type="checkbox"/> | 64 | kbps | <input type="checkbox"/> | 64 | kbps |
| 5 | <input type="checkbox"/> | 64 | kbps | <input type="checkbox"/> | 64 | kbps |
| 6 | <input type="checkbox"/> | 64 | kbps | <input type="checkbox"/> | 64 | kbps |
| 7 | <input type="checkbox"/> | 64 | kbps | <input type="checkbox"/> | 64 | kbps |
| 8 | <input type="checkbox"/> | 64 | kbps | <input type="checkbox"/> | 64 | kbps |

Apply Cancel

The following table describes the related labels in this screen.

Table 65 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. |
| * | <p>Settings in this row apply to all ports.</p> <p>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.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p> |
| Active | Select this check box to activate ingress rate limits on this port. |
| Ingress Rate | <p>Specify the maximum bandwidth allowed in kilobits per second (Kbps) for the incoming traffic flow on a port.</p> <p>Note: Ingress rate bandwidth control applies to layer 2 traffic only.</p> |
| 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 148](#)) 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 107 Advanced Application > Broadcast Storm Control

| Broadcast Storm Control | | | | | | | |
|---------------------------------|--------------------------|---|--------------------------|---|--------------------------|---|--|
| Active <input type="checkbox"/> | | | | | | | |
| Port | Broadcast (pkt/s) | | Multicast (pkt/s) | | DLF (pkt/s) | | |
| * | <input type="checkbox"/> | | <input type="checkbox"/> | | <input type="checkbox"/> | | |
| 1 | <input type="checkbox"/> | 0 | <input type="checkbox"/> | 0 | <input type="checkbox"/> | 0 | |
| 2 | <input type="checkbox"/> | 0 | <input type="checkbox"/> | 0 | <input type="checkbox"/> | 0 | |
| 3 | <input type="checkbox"/> | 0 | <input type="checkbox"/> | 0 | <input type="checkbox"/> | 0 | |
| 4 | <input type="checkbox"/> | 0 | <input type="checkbox"/> | 0 | <input type="checkbox"/> | 0 | |
| 5 | <input type="checkbox"/> | 0 | <input type="checkbox"/> | 0 | <input type="checkbox"/> | 0 | |
| 6 | <input type="checkbox"/> | 0 | <input type="checkbox"/> | 0 | <input type="checkbox"/> | 0 | |
| 7 | <input type="checkbox"/> | 0 | <input type="checkbox"/> | 0 | <input type="checkbox"/> | 0 | |
| 8 | <input type="checkbox"/> | 0 | <input type="checkbox"/> | 0 | <input type="checkbox"/> | 0 | |

The following table describes the labels in this screen.

Table 66 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. |
| * | <p>Settings in this row apply to all ports.</p> <p>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.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p> |
| Broadcast (pkt/s) | Select this option and specify how many broadcast packets the port receives per second. |
| Multicast (pkt/s) | Select this option and specify how many multicast packets the port receives per second. |
| DLF (pkt/s) | Select this option and specify how many destination lookup failure (DLF) packets the port receives per second. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to reset the fields. |

CHAPTER 16

Mirroring

16.1 Mirroring Overview

This chapter discusses port mirroring setup screens.

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

16.2 Port Mirroring Setup

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

Figure 108 Advanced Application > Mirroring

| Mirroring | | |
|--------------|--------------------------|-----------|
| Active | <input type="checkbox"/> | |
| Monitor Port | <input type="text"/> | |
| Port | Mirrored | Direction |
| * | <input type="checkbox"/> | Ingress ▾ |
| 1 | <input type="checkbox"/> | Ingress ▾ |
| 2 | <input type="checkbox"/> | Ingress ▾ |
| 3 | <input type="checkbox"/> | Ingress ▾ |
| 4 | <input type="checkbox"/> | Ingress ▾ |
| 5 | <input type="checkbox"/> | Ingress ▾ |
| 6 | <input type="checkbox"/> | Ingress ▾ |
| 7 | <input type="checkbox"/> | Ingress ▾ |
| 8 | <input type="checkbox"/> | Ingress ▾ |

The following table describes the labels in this screen.

Table 67 Advanced Application > Mirroring

| LABEL | DESCRIPTION |
|--------------|--|
| Active | Select this check box to activate port mirroring on the Switch. Clear this check box to disable the feature. |
| Monitor Port | The monitor port is the port you copy the traffic to in order to examine it in more detail without interfering with the traffic flow on the original ports. Enter the port number of the monitor port. |
| Port | This field displays the port number. |
| * | <p>Settings in this row apply to all ports.</p> <p>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.</p> <p>Note: Changes in this row are copied to all the ports as soon as you make them.</p> |
| 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 153](#)) 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 154](#)) to configure static link aggregation.
- Use the **Link Aggregation Control Protocol** screen ([Section 17.3.1 on page 156](#)) 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 157](#) 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 68 Link Aggregation ID: Local Switch

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

Table 69 Link Aggregation ID: Peer Switch

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

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 152](#) for more information.

Figure 109 Advanced Application > Link Aggregation Status

| 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 | - |

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

The following table describes the labels in this screen.

Table 70 Advanced Application > Link Aggregation Status

| LABEL | DESCRIPTION |
|--------------------|--|
| Group ID | This field displays the group ID to identify a trunk group, that is, one logical link containing multiple ports. |
| Enabled Ports | These are the ports you have configured in the Link Aggregation screen to be in the trunk group. The port numbers displays only when this trunk group is activated and there is a port belonging to this group. |
| Synchronized Ports | These are the ports that are currently transmitting data as one logical link in this trunk group. |
| Aggregator ID | Link Aggregator ID consists of the following: system priority, MAC address, key, port priority and port number. The ID displays only when there is a port belonging to this trunk group and LACP is also enabled for this group. |
| Criteria | This shows the outgoing traffic distribution algorithm used in this trunk group. Packets from the same source and/or to the same destination are sent over the same link within the trunk. src-mac means the Switch distributes traffic based on the packet's source MAC address. dst-mac means the Switch distributes traffic based on the packet's destination MAC address. src-dst-mac means the Switch distributes traffic based on a combination of the packet's source and destination MAC addresses. src-ip means the Switch distributes traffic based on the packet's source IP address. dst-ip means the Switch distributes traffic based on the packet's destination IP address. src-dst-ip means the Switch distributes traffic based on a combination of the packet's source and destination IP addresses. |
| Status | This field displays how these ports were added to the trunk group. It displays: <ul style="list-style-type: none"> • Static – if the ports are configured as static members of a trunk group. • LACP – if the ports are configured to join a trunk group through LACP. |

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 152](#) for more information on link aggregation.

Figure 110 Advanced Application > Link Aggregation > Link Aggregation Setting

| Link Aggregation Setting | | Status | LACP |
|--------------------------|--------------------------|---------------|------|
| Group ID | Active | Criteria | |
| T1 | <input type="checkbox"/> | src-dst-mac ▾ | |
| T2 | <input type="checkbox"/> | src-dst-mac ▾ | |
| T3 | <input type="checkbox"/> | src-dst-mac ▾ | |
| T4 | <input type="checkbox"/> | src-dst-mac ▾ | |

| Port | Group |
|------|--------|
| 1 | None ▾ |
| 2 | None ▾ |
| 3 | None ▾ |
| 4 | None ▾ |
| 5 | None ▾ |
| 6 | None ▾ |
| 7 | None ▾ |
| 8 | None ▾ |

The following table describes the labels in this screen.

Table 71 Advanced Application > Link Aggregation > Link Aggregation Setting

| LABEL | DESCRIPTION |
|--------------------------|--|
| Link Aggregation Setting | This is the only screen you need to configure to enable static link aggregation. |
| Group ID | The field identifies the link aggregation group, that is, one logical link containing multiple ports. |
| Active | Select this option to activate a trunk group. |
| Criteria | <p>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.</p> <p>Select src-mac to distribute traffic based on the packet's source MAC address.</p> <p>Select dst-mac to distribute traffic based on the packet's destination MAC address.</p> <p>Select src-dst-mac to distribute traffic based on a combination of the packet's source and destination MAC addresses.</p> <p>Select src-ip to distribute traffic based on the packet's source IP address.</p> <p>Select dst-ip to distribute traffic based on the packet's destination IP address.</p> <p>Select src-dst-ip to distribute traffic based on a combination of the packet's source and destination IP addresses.</p> |
| Port | This field displays the port number. |
| Group | <p>Select the trunk group to which a port belongs.</p> <p>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.</p> |

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

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

17.3.1 Link Aggregation Control Protocol

Click **Advanced Application > Link Aggregation > Link Aggregation Setting > LACP** to display the screen shown next. See [Dynamic Link Aggregation on page 152](#) for more information on dynamic link aggregation.

Figure 111 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP

The following table describes the labels in this screen.

Table 72 Advanced Application > Link Aggregation > Link Aggregation Setting > LACP

| LABEL | DESCRIPTION |
|-----------------------------------|--|
| Link Aggregation Control Protocol | Note: Do NOT configure this screen unless you want to enable dynamic link aggregation. |
| Active | Select this check box to enable Link Aggregation Control Protocol (LACP). |

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

| LABEL | DESCRIPTION |
|-----------------|--|
| System Priority | LACP system priority is a number between 1 and 65535. The switch with the lowest system priority (and lowest port number if system priority is the same) becomes the LACP "server". The LACP "server" controls the operation of LACP setup. Enter a number to set the priority of an active port using Link Aggregation Control Protocol (LACP). The smaller the number, the higher the priority level. |
| Group ID | The field identifies the link aggregation group, that is, one logical link containing multiple ports. |
| LACP Active | Select this option to enable LACP for a trunk. |
| Port | This field displays the port number. |
| * | Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them. |
| LACP Timeout | Timeout is the time interval between the individual port exchanges of LACP packets in order to check that the peer port in the trunk group is still up. If a port does not respond after three tries, then it is deemed to be "down" and is removed from the trunk. Set a short timeout (1 second) for busy trunked links to ensure that disabled ports are removed from the trunk group as soon as possible. Select either 1 second or 30 seconds. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

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 112 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 113 Trunking Example – Configuration Screen

| Link Aggregation Setting | | | Status | LACP |
|--------------------------|-------------------------------------|---------------|--------|------|
| Group ID | Active | Criteria | | |
| T1 | <input checked="" type="checkbox"/> | src-dst-mac ▾ | | |
| T2 | <input type="checkbox"/> | src-dst-mac ▾ | | |
| T3 | <input type="checkbox"/> | src-dst-mac ▾ | | |
| T4 | <input type="checkbox"/> | src-dst-mac ▾ | | |

| Port | Group |
|------|--------|
| 1 | None ▾ |
| 2 | T1 ▾ |
| 3 | T1 ▾ |
| 4 | T1 ▾ |
| 5 | T1 ▾ |
| 6 | None ▾ |
| 7 | None ▾ |
| 8 | None ▾ |

Apply **Cancel**

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

CHAPTER 18

Port Security

18.1 Port Security Overview

This chapter shows you how to set up port security.

18.2 About Port Security

Port security allows only packets with dynamically learned MAC addresses and/or configured static MAC addresses to pass through a port on the Switch. The Switch can learn up to 8k MAC addresses in total with no limit on individual ports other than the sum cannot exceed 8k.

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

18.3 Port Security Setup

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

Figure 114 Advanced Application > Port Security

| Port | Active | Address Learning | Limited Number of Learned MAC Address |
|------|--------------------------|-------------------------------------|---------------------------------------|
| * | <input type="checkbox"/> | <input checked="" type="checkbox"/> | |
| 1 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 0 |
| 2 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 0 |
| 3 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 0 |
| 4 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 0 |
| 5 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 0 |
| 6 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 0 |
| 7 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 0 |
| 8 | <input type="checkbox"/> | <input checked="" type="checkbox"/> | 0 |

The following table describes the labels in this screen.

Table 73 Advanced Application > Port Security

| LABEL | DESCRIPTION |
|---------------------------------------|---|
| Port List | Enter the number of the ports (separated by a comma) on which you want to enable port security and disable MAC address learning. After you click MAC freeze , all previously learned MAC addresses on the specified ports will become static MAC addresses and display in the Static MAC Forwarding screen. |
| MAC freeze | Click MAC freeze to have the Switch automatically select the Active check boxes and clear the Address Learning check boxes only for the ports specified in the Port List . |
| Active | Select this option to enable port security on the Switch. |
| Port | This field displays the port number. |
| * | Settings in this row apply to all ports. Use this row only if you want to make some of the settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them. |
| Active | Select this check box to enable the port security feature on this port. The Switch forwards packets whose MAC addresses is in the MAC address table on this port. Packets with no matching MAC addresses are dropped. Clear this check box to disable the port security feature. The Switch forwards all packets on this port. |
| Address Learning | MAC address learning reduces outgoing broadcast traffic. For MAC address learning to occur on a port, the port itself must be active with address learning enabled. |
| Limited Number of Learned MAC Address | Use this field to limit the number of (dynamic) MAC addresses that may be learned on a port. For example, if you set this field to "5" on port 2, then only the devices with these five learned MAC addresses may access port 2 at any one time. A sixth device must wait until one of the five learned MAC addresses ages out. MAC address aging out time can be set in the Switch Setup screen. The valid range is from "0" to "8K". "0" means this feature is disabled. |

Table 73 Advanced Application > Port Security (continued)

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

CHAPTER 19

Time Range

19.1 Time Range Overview

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

19.1.1 What You Can Do

Use the **Time Range** screen ([Section 19.2 on page 162](#)) to view or define a schedule on the Switch.

19.2 Configuring Time Range

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

Figure 115 Advanced Application > Time Range

| Index | Name | Type | Range |
|-------|------|------|-------|
| | | | |

The following table describes the labels in this screen.

Table 74 Advanced Application > Time Range

| LABEL | DESCRIPTION |
|----------|--|
| Name | Enter a descriptive name for this rule for identifying purposes. The string should not contain [?], [], ['], ["] or [,]. |
| Type | Select Absolute to create a one-time schedule. One-time schedules begin on a specific start date and time and end on a specific stop date and time. One-time schedules are useful for long holidays and vacation periods. Alternatively, select Periodic to create a recurring schedule. Recurring schedules begin at a specific start time and end at a specific stop time on selected days of the week (Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday). Recurring schedules are useful for defining the workday and off-work hours. |
| Absolute | This section is available only when you set Type to Absolute . |
| Start | Specify the year, month, day, hour and minute when the schedule begins. |
| End | Specify the year, month, day, hour and minute when the schedule ends. |
| Periodic | This section is available only when you set Type to Periodic . Select the first option if you want to define a recurring schedule for a consecutive time period. You then select the day of the week, hour and minute when the schedule begins and ends respectively. Select the second option if you want to define a recurring schedule for multiple non-consecutive time periods. You need to select each day of the week the recurring schedule is effective. You also need to specify the hour and minute when the schedule begins and ends each day. The schedule begins and ends in the same day. |
| Add | Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to reset the fields to your previous configuration. |
| Clear | Click Clear to clear the fields to the factory defaults. |
| Index | This field displays the index number of the rule. Click an index number to change the settings. |
| Name | This field displays the descriptive name for this rule. This is for identification purpose only. |
| Type | This field displays the type of the schedule. |
| Range | This field displays the time periods to which this schedule applies. |
| | Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries. |
| Delete | Check the rules that you want to remove and then click the Delete button. |
| Cancel | Click Cancel to clear the selected check boxes. |

CHAPTER 20

Queuing Method

20.1 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.

20.1.1 What You Can Do

Use the **Queuing Method** screen ([Section 20.2 on page 165](#)) to set priorities for the queues of the Switch. This distributes bandwidth across the different traffic queues.

20.1.2 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.

20.2 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 116 Advanced Application > Queuing Method

| Queuing Method | | | | | | | | | | |
|----------------|--|--------|----|----|----|----|----|----|----|----------------------------|
| Port | Method | Weight | | | | | | | | Hybrid-SPQ Lowest-Queue |
| | | Q0 | Q1 | Q2 | Q3 | Q4 | Q5 | Q6 | Q7 | |
| * | SPQ | | | | | | | | | None |
| 1 | <input checked="" type="radio"/> SPQ <input type="radio"/> WFQ <input type="radio"/> WRR | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | None |
| 2 | <input checked="" type="radio"/> SPQ <input type="radio"/> WFQ <input type="radio"/> WRR | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | None |
| 3 | <input checked="" type="radio"/> SPQ <input type="radio"/> WFQ <input type="radio"/> WRR | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | None |
| 4 | <input checked="" type="radio"/> SPQ <input type="radio"/> WFQ <input type="radio"/> WRR | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | None |
| 5 | <input checked="" type="radio"/> SPQ <input type="radio"/> WFQ <input type="radio"/> WRR | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | None |
| 6 | <input checked="" type="radio"/> SPQ <input type="radio"/> WFQ <input type="radio"/> WRR | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | None |
| 7 | <input checked="" type="radio"/> SPQ <input type="radio"/> WFQ <input type="radio"/> WRR | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | None |
| 8 | <input checked="" type="radio"/> SPQ <input type="radio"/> WFQ <input type="radio"/> WRR | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | None |

The following table describes the labels in this screen.

Table 75 Advanced Application > Queuing Method

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

Table 75 Advanced Application > Queuing Method (continued)

| LABEL | DESCRIPTION |
|--------------------------------|---|
| Method | <p>Select SPQ (Strictly Priority Queuing), WFQ (Weighted Fair Queuing) or WRR (Weighted Round Robin).</p> <p>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.</p> <p>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.</p> <p>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.</p> |
| 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 | <p>This field is applicable only when you select WFQ or WRR.</p> <p>Select a queue (Q0 to Q7) to have the Switch use SPQ to service the subsequent queues after and including the specified queue for the port. For example, if you select Q5, the Switch services traffic on Q5, Q6 and Q7 using SPQ.</p> <p>Select None to always use WFQ or WRR for the port.</p> |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

CHAPTER 21

Multicast

21.1 Multicast Overview

This chapter shows you how to configure various multicast features.

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

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

21.1.1 What You Can Do

- Use the **Multicast Setup** screen ([Section 21.2 on page 168](#)) to display the links to the configuration screens where you can configure IPv4 multicast settings.
- Use the **IPv4 Multicast Status** screen ([Section 21.3 on page 168](#)) to view IPv4 multicast group information.
- Use the **IGMP Snooping** screen ([Section 21.3.1 on page 169](#)) 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 21.3.2 on page 171](#)) to perform IGMP snooping on VLANs.

21.1.2 What You Need to Know

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

IP Multicast Addresses

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

IGMP Snooping

A Switch can passively snoop on IGMP packets transferred between IP multicast routers or switches and IP multicast hosts to learn the IP multicast group membership. It checks IGMP packets passing through it, picks out the group registration information, and configures multicasting accordingly. IGMP snooping

allows the Switch to learn multicast groups without you having to manually configure them.

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

IGMP Snooping and VLANs

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

21.2 Multicast Setup

Use this screen to configure IGMP for IPv4. Click **Advanced Application > Multicast** in the navigation panel.

Figure 117 Advanced Application > Multicast Setup



The following table describes the labels in this screen.

Table 76 Advanced Application > Multicast Setup

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

21.3 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 21.1 on page 167](#) for more information on multicasting.

Figure 118 Advanced Application > Multicast > IPv4 Multicast

| IPv4 Multicast Status | | | Multicast Setup | IGMP Snooping |
|-----------------------|-----|------|---------------------------------|-------------------------------|
| Index | VID | Port | Multicast Group | |
| 1 | 1 | 6 | 224.0.0.251 | |
| 2 | 1 | 6 | 224.0.0.252 | |
| 3 | 1 | 6 | 239.255.255.250 | |

The following table describes the labels in this screen.

Table 77 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. |

21.3.1 IGMP Snooping

Click the **IGMP Snooping** link in the **Advanced Application > Multicast > IPv4 Multicast** screen to display the screen as shown. See [Section 21.1 on page 167](#) for more information on multicasting.

Figure 119 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping

The screenshot shows the IGMP Snooping configuration interface. At the top, there are links for "IPv4 Multicast Status" and "IGMP Snooping VLAN". The main configuration area includes the following settings:

- Active:
- Querier:
- Report Proxy:
- Host Timeout: 260
- 802.1p Priority: No-Change
- Unknown Multicast Frame: Flooding, Drop
- Reserved Multicast Group: Flooding, Drop

Below the settings is a table for port configurations:

| Port | Normal Leave | Fast Leave | IGMP Querier Mode |
|------|----------------------------------|-----------------------|-------------------|
| * | <input checked="" type="radio"/> | <input type="radio"/> | Auto |
| 1 | <input checked="" type="radio"/> | <input type="radio"/> | Auto |
| 2 | <input checked="" type="radio"/> | <input type="radio"/> | Auto |
| 3 | <input checked="" type="radio"/> | <input type="radio"/> | Auto |
| 4 | <input checked="" type="radio"/> | <input type="radio"/> | Auto |
| 5 | <input checked="" type="radio"/> | <input type="radio"/> | Auto |
| 6 | <input checked="" type="radio"/> | <input type="radio"/> | Auto |
| 7 | <input checked="" type="radio"/> | <input type="radio"/> | Auto |
| 8 | <input checked="" type="radio"/> | <input type="radio"/> | Auto |

At the bottom of the screen are "Apply" and "Cancel" buttons.

The following table describes the labels in this screen.

Table 78 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping

| LABEL | DESCRIPTION |
|---------------|---|
| IGMP Snooping | Use these settings to configure IGMP snooping. |
| Active | Select Active to enable IGMP Snooping to forward group multicast traffic only to ports that are members of that group. |
| Querier | Select this option to allow the Switch to send IGMP General Query messages to the VLANs with the multicast hosts attached. |

Table 78 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping (continued)

| LABEL | DESCRIPTION |
|--------------------------|--|
| Report Proxy | <p>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.</p> <p>The Switch not only checks IGMP packets between multicast routers or switches and multicast hosts to learn the multicast group membership, but also replaces the source MAC address in an IGMP v1/v2 report with its own MAC address before forwarding to the multicast router or switch. When the Switch receives more than one IGMP v1/v2 join report that requests to join the same multicast group, it only sends a new join report with its MAC address. This helps reduce the number of multicast join reports passed to the multicast router or switch.</p> <p>The Switch sends a leave message with its MAC address to the multicast router or switch only when it receives the leave message from the last host in a multicast group.</p> |
| Host Timeout | Specify the time (from 1 to 16711450) in seconds that elapses before the Switch removes an IGMP group membership entry if it does not receive report messages from the port. |
| 802.1p Priority | Select a priority level (0 – 7) to which the Switch changes the priority in outgoing IGMP control packets. Otherwise, select No-Change to not replace the priority. |
| Unknown Multicast Frame | Specify the action to perform when the Switch receives an unknown multicast frame. Select Drop to discard the frames. Select Flooding to send the frames to all ports. |
| Reserved Multicast Group | <p>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.</p> <p>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.</p> <p>Specify the action to perform when the Switch receives a frame with a reserved multicast address.</p> <ul style="list-style-type: none"> • Select Drop to discard the frames. • Select Flooding to send the frames to all ports. |
| Port | This field displays the port number. |
| * | <p>Settings in this row apply to all ports.</p> <p>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.</p> <p>Changes in this row are copied to all the ports as soon as you make them.</p> |
| Normal Leave | <p>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.</p> <p>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.</p> |
| Fast Leave | <p>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.</p> <p>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.</p> |

Table 78 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping (continued)

| LABEL | DESCRIPTION |
|-------------------|---|
| IGMP Querier Mode | <p>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.</p> <p>Select Auto to have the Switch use the port as an IGMP query port if the port receives IGMP query packets.</p> <p>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.</p> <p>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.</p> |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

21.3.2 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 168](#) for more information on IGMP Snooping VLAN.

Figure 120 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Snooping VLAN

The screenshot shows the configuration interface for IGMP Snooping VLAN. It includes a title bar, a mode selection section with radio buttons for 'auto' and 'fixed', a set of 'Apply' and 'Cancel' buttons, a 'VLAN' section with input fields for 'Name' and 'VID' and 'Add', 'Cancel', and 'Clear' buttons, and 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 79 Advanced Application > Multicast > IPv4 Multicast > IGMP Snooping > IGMP Snooping VLAN

| LABEL | DESCRIPTION |
|--------|--|
| Mode | <p>Select auto to have the Switch learn multicast group membership information of any VLANs automatically.</p> <p>Select fixed to have the Switch only learn multicast group membership information of the VLANs that you specify below.</p> <p>In either auto or fixed mode, the Switch can learn up to 16 VLANs.</p> <p>The Switch drops any IGMP control messages which do not belong to these 16 VLANs.</p> <p>You must also enable IGMP snooping in the Multicast > IPv4 Multicast > IGMP Snooping screen first.</p> |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |
| VLAN | Use this section of the screen to add VLANs on which the Switch is to perform IGMP snooping. |
| Name | Enter the descriptive name of the VLAN for identification purposes. The string should not contain [?], [], ['], ["] or [,]. |
| VID | Enter the ID of a static VLAN; the valid range is between 1 and 4094. |
| Add | <p>Click this to create a new entry or to update an existing one.</p> <p>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.</p> |
| Cancel | Click Cancel to reset the fields to your previous configuration. |
| Clear | Click Clear to reset the fields to the factory defaults. |
| Index | This is the index number of the IGMP snooping VLAN entry in the table. Click an index number to view more details or change the settings. |
| Name | This field displays the descriptive name for this VLAN group. |
| VID | This field displays the ID number of the VLAN group. |
| | Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries. |
| Delete | Check the entries that you want to remove, then click the Delete button. |
| Cancel | Click Cancel to clear the check boxes. |

CHAPTER 22

AAA

22.1 Authentication, Authorization and Accounting (AAA)

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

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

Figure 121 AAA Server



22.1.1 What You Can Do

- Use the **AAA** screen ([Section 22.2 on page 174](#)) 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 22.3 on page 174](#)) to configure your RADIUS server settings.
- Use the **AAA Setup** screen ([Section 22.4 on page 176](#)) 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.

22.1.2 What You Need to Know

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

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

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

Local User Accounts

By storing user profiles locally on the Switch, your Switch is able to authenticate and authorize users without interacting with a network AAA server. However, there is a limit on the number of users you may authenticate in this way.

RADIUS

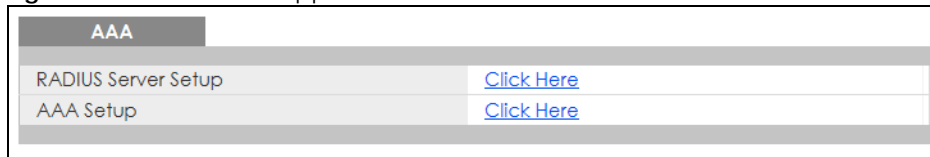
RADIUS is a security protocol used to authenticate users by means of an external server instead of (or in addition to) an internal device user database that is limited to the memory capacity of the device. In essence, RADIUS authentication allows you to validate an unlimited number of users from a central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

22.2 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 and then set up the authentication priority, activate authorization.

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

Figure 122 Advanced Application > AAA



22.3 RADIUS Server Setup

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

Figure 123 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 | | <input type="checkbox"/> |
| 2 | 0.0.0.0 | 1812 | | <input type="checkbox"/> |

Accounting Server

| | | |
|---------|----|---------|
| Timeout | 30 | seconds |
|---------|----|---------|

| Index | IP Address | UDP Port | Shared Secret | Delete |
|-------|------------|----------|---------------|--------------------------|
| 1 | 0.0.0.0 | 1813 | | <input type="checkbox"/> |
| 2 | 0.0.0.0 | 1813 | | <input type="checkbox"/> |

Attribute

| | |
|----------------|---------|
| NAS-IP-Address | 0.0.0.0 |
|----------------|---------|

Apply
Cancel

The following table describes the labels in this screen.

Table 80 Advanced Application > AAA > RADIUS Server Setup

| LABEL | DESCRIPTION |
|-----------------------|---|
| Authentication Server | Use this section to configure your RADIUS authentication settings. |
| Mode | <p>This field is only valid if you configure multiple RADIUS servers.</p> <p>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.</p> <p>Select round-robin to alternate between the RADIUS servers that it sends authentication requests to.</p> |
| Timeout | <p>Specify the amount of time in seconds that the Switch waits for an authentication request response from the RADIUS server.</p> <p>If you are using two RADIUS servers then the timeout value is divided between the two RADIUS servers. For example, if you set the timeout value to 30 seconds, then the Switch waits for a response from the first RADIUS server for 15 seconds and then tries the second RADIUS server.</p> |
| Index | This is a read-only number representing a RADIUS server entry. |
| IP Address | Enter the IP address of an external RADIUS server in dotted decimal notation. |
| UDP Port | The default port of a RADIUS server for authentication is 1812 . You need not change this value unless your network administrator instructs you to do so. |

Table 80 Advanced Application > AAA > RADIUS Server Setup (continued)

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

22.4 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 124 Advanced Application > AAA > AAA Setup

AAA Setup [AAA](#)

Authentication

| Type | Method 1 | Method 2 |
|-------|----------|----------|
| Login | local | - |

Authorization

| Type | Active | Method |
|------|--------------------------|--------|
| Exec | <input type="checkbox"/> | radius |

Accounting

| Type | Active | Broadcast | Mode | Method |
|--------|--------------------------|--------------------------|------|--------|
| System | <input type="checkbox"/> | <input type="checkbox"/> | - | radius |

The following table describes the labels in this screen.

Table 81 Advanced Application > AAA > AAA Setup

| LABEL | DESCRIPTION |
|----------------|---|
| Authentication | Use this section to specify the methods used to authenticate users accessing the Switch. |
| Login | <p>These fields specify which database the Switch should use (first and second) to authenticate administrator accounts (users for Switch management).</p> <p>Configure the local user accounts in the Access Control > Logins screen. The RADIUS is an external server. Before you specify the priority, make sure you have set up the corresponding database correctly first.</p> <p>You can specify up to two methods for the Switch to authenticate administrator accounts. The Switch checks the methods in the order you configure them (first Method 1, and then Method 2). You must configure the settings in the Method 1 field. If you want the Switch to check another source for administrator accounts, specify them in the Method 2 field.</p> <p>Select local to have the Switch check the administrator accounts configured in the Access Control > Logins screen.</p> <p>Select radius to have the Switch check the administrator accounts configured through your RADIUS server.</p> |
| Authorization | Use this section to configure authorization settings on the Switch. |
| Type | <p>Set whether the Switch provides the following services to a user.</p> <ul style="list-style-type: none"> Exec: Allow an administrator which logs into the Switch through Telnet or SSH to have a different access privilege level assigned through the external server. |
| Active | Select this to activate authorization for a specified event type. |
| Method | RADIUS is the only method for authorization of the Exec type of service. |
| Accounting | Use this section to configure accounting settings on the Switch. |
| Type | <p>The Switch supports the following types of events to be sent to the accounting servers:</p> <ul style="list-style-type: none"> 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. |
| Active | Select this to activate accounting for a specified event type. |

Table 81 Advanced Application > AAA > AAA Setup (continued)

| LABEL | DESCRIPTION |
|-----------|--|
| Broadcast | Select this to have the Switch send accounting information to all configured accounting servers at the same time. If you do not select this and you have two accounting servers set up, then the Switch sends information to the first accounting server and if it does not get a response from the accounting server then it tries the second accounting server. |
| Mode | This should show '-' by default. |
| Method | RADIUS is the only method for recording System or Exec type of event. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

22.5 Technical Reference

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

22.5.1 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 (See the CLI Reference Guide for more information on account privilege levels) for the authenticated user.

The VSAs are composed of the following:

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

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

The following table describes the VSAs supported on the Switch.

Table 82 Supported VSAs

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

22.5.1.1 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. 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 83 Supported Tunnel Protocol Attribute

| FUNCTION | ATTRIBUTE |
|-----------------|---|
| VLAN Assignment | Tunnel-Type = VLAN(13) Tunnel-Medium-Type = 802(6) Tunnel-Private-Group-ID = VLAN ID Note: You must also create a VLAN with the specified VID on the Switch. Note: The bolded values in this table are fixed values as defined in RFC 3580. |

22.5.2 Supported RADIUS Attributes

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

Refer to RFC 2865 for more information about RADIUS attributes used for authentication.

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.

22.5.3 Attributes Used for Authentication

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

22.5.3.1 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

22.5.3.2 Attributes Used to Login Users

User-Name

User-Password

NAS-Identifier

NAS-IP-Address

22.5.3.3 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 23

DHCP Snooping

23.1 DHCP Snooping Overview

With DHCP snooping, the Switch can build the binding table dynamically by snooping DHCP packets (dynamic bindings) and filter unauthorized DHCP packets in your network.

The Switch uses a binding table to distinguish between authorized and unauthorized DHCP packets in your network. A binding contains these key attributes:

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

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

With DHCP snooping, the Switch can block a DHCP server on a snooped VLAN that comes from an untrusted port in your network.

23.1.1 What You Can Do

- Use the **DHCP Snooping** screen ([Section 23.2 on page 181](#)) to look at various statistics about the DHCP snooping database.
- Use this **DHCP Snooping Configure** screen ([Section 23.3 on page 184](#)) to enable DHCP snooping on the Switch (not on specific VLAN), specify the VLAN where the default DHCP server is located, and configure the DHCP snooping database.
- Use the **DHCP Snooping Port Configure** screen ([Section 23.3.1 on page 186](#)) to specify whether ports are trusted or untrusted ports for DHCP snooping.
- Use the **DHCP Snooping VLAN Configure** screen ([Section 23.3.2 on page 187](#)) to enable DHCP snooping on each VLAN and to specify whether or not the Switch adds DHCP relay agent option 82 information to DHCP requests that the Switch relays to a DHCP server for each VLAN.
- Use the **DHCP Snooping VLAN Port Configure** screen ([Section 23.3.3 on page 188](#)) to apply a different DHCP option 82 profile to certain ports in a VLAN.

23.2 DHCP Snooping

Use this screen to look at various statistics about the DHCP snooping database.

To open this screen, click **Advanced Application > DHCP Snooping**.

Figure 125 Advanced Application > DHCP Snooping

| DHCP Snooping | | Configure |
|--|---------------------|---------------------------|
| Database Status | | |
| Description | Status | |
| Agent URL | | |
| Write delay timer | 300 | seconds |
| Abort timer | 300 | seconds |
| Agent running | | |
| Agent running | None | |
| Delay timer expiry | Not Running | |
| Abort timer expiry | Not Running | |
| Last succeeded time | | |
| Last succeeded time | None | |
| Last failed time | | |
| Last failed time | None | |
| Last failed reason | | |
| Last failed reason | No failure recorded | |
| Times | | |
| Total attempts | 0 | |
| Startup failures | 0 | |
| Successful transfers | 0 | |
| Failed transfers | 0 | |
| Successful reads | 0 | |
| Failed reads | 0 | |
| Successful writes | 0 | |
| Failed writes | 0 | |
| Database detail | | |
| Description | Status | |
| First successful access | None | |
| Last ignored bindings counters | | |
| Binding collisions | 0 | |
| Invalid interfaces | 0 | |
| Parse failures | 0 | |
| Expired leases | 0 | |
| Unsupported vlans | 0 | |
| Last ignored time | None | |
| Total ignored bindings counters | | |
| Binding collisions | 0 | |
| Invalid interfaces | 0 | |
| Parse failures | 0 | |
| Expired leases | 0 | |
| Unsupported vlans | 0 | |

The following table describes the labels in this screen.

Table 84 Advanced Application > DHCP Snooping

| LABEL | DESCRIPTION |
|-----------------|---|
| Database Status | This section displays the current settings for the DHCP snooping database. You can configure them in the DHCP Snooping Configure screen. |
| Agent URL | This field displays the location of the DHCP snooping database. |

Table 84 Advanced Application > DHCP Snooping (continued)

| LABEL | DESCRIPTION |
|-------------------------|---|
| Write delay timer | This field displays how long (in seconds) the Switch tries to complete a specific update in the DHCP snooping database before it gives up. |
| Abort timer | This field displays how long (in seconds) the Switch waits to update the DHCP snooping database after the current bindings change. |
| | This section displays information about the current update and the next update of the DHCP snooping database. |
| Agent running | This field displays the status of the current update or access of the DHCP snooping database. None: The Switch is not accessing the DHCP snooping database. Read: The Switch is loading dynamic bindings from the DHCP snooping database. Write: The Switch is updating the DHCP snooping database. |
| Delay timer expiry | This field displays how much longer (in seconds) the Switch tries to complete the current update before it gives up. It displays Not Running if the Switch is not updating the DHCP snooping database right now. |
| Abort timer expiry | This field displays when (in seconds) the Switch is going to update the DHCP snooping database again. It displays Not Running if the current bindings have not changed since the last update. |
| | This section displays information about the last time the Switch updated the DHCP snooping database. |
| Last succeeded time | This field displays the last time the Switch updated the DHCP snooping database successfully. |
| Last failed time | This field displays the last time the Switch updated the DHCP snooping database unsuccessfully. |
| Last failed reason | This field displays the reason the Switch updated the DHCP snooping database unsuccessfully. |
| | This section displays historical information about the number of times the Switch successfully or unsuccessfully read or updated the DHCP snooping database. |
| Total attempts | This field displays the number of times the Switch has tried to access the DHCP snooping database for any reason. |
| Startup failures | This field displays the number of times the Switch could not create or read the DHCP snooping database when the Switch started up or a new URL is configured for the DHCP snooping database. |
| Successful transfers | This field displays the number of times the Switch read bindings from or updated the bindings in the DHCP snooping database successfully. |
| Failed transfers | This field displays the number of times the Switch was unable to read bindings from or update the bindings in the DHCP snooping database. |
| Successful reads | This field displays the number of times the Switch read bindings from the DHCP snooping database successfully. |
| Failed reads | This field displays the number of times the Switch was unable to read bindings from the DHCP snooping database. |
| Successful writes | This field displays the number of times the Switch updated the bindings in the DHCP snooping database successfully. |
| Failed writes | This field displays the number of times the Switch was unable to update the bindings in the DHCP snooping database. |
| Database detail | |
| First successful access | This field displays the first time the Switch accessed the DHCP snooping database for any reason. |

Table 84 Advanced Application > DHCP Snooping (continued)

| LABEL | DESCRIPTION |
|---------------------------------|--|
| Last ignored bindings counters | This section displays the number of times and the reasons the Switch ignored bindings the last time it read bindings from the DHCP binding database. You can clear these counters by restarting the Switch or using CLI commands. See the CLI Reference Guide. |
| Binding collisions | This field displays the number of bindings the Switch ignored because the Switch already had a binding with the same MAC address and VLAN ID. |
| Invalid interfaces | This field displays the number of bindings the Switch ignored because the port number was a trusted interface or does not exist anymore. |
| Parse failures | This field displays the number of bindings the Switch ignored because the Switch was unable to understand the binding in the DHCP binding database. |
| Expired leases | This field displays the number of bindings the Switch ignored because the lease time had already expired. |
| Unsupported vlans | This field displays the number of bindings the Switch ignored because the VLAN ID does not exist anymore. |
| Last ignored time | This field displays the last time the Switch ignored any bindings for any reason from the DHCP binding database. |
| Total ignored bindings counters | This section displays the reasons the Switch has ignored bindings any time it read bindings from the DHCP binding database. You can clear these counters by restarting the Switch or using CLI commands. See the CLI Reference Guide. |
| Binding collisions | This field displays the number of bindings the Switch has ignored because the Switch already had a binding with the same MAC address and VLAN ID. |
| Invalid interfaces | This field displays the number of bindings the Switch has ignored because the port number was a trusted interface or does not exist anymore. |
| Parse failures | This field displays the number of bindings the Switch has ignored because the Switch was unable to understand the binding in the DHCP binding database. |
| Expired leases | This field displays the number of bindings the Switch has ignored because the lease time had already expired. |
| Unsupported vlans | This field displays the number of bindings the Switch has ignored because the VLAN ID does not exist anymore. |

23.3 DHCP Snooping Configure

Use this screen to enable DHCP snooping on the Switch (not on specific VLAN), specify the VLAN where the default DHCP server is located, and configure the DHCP snooping database. The DHCP snooping database stores the current bindings on a secure, external TFTP server so that they are still available after a restart.

To open this screen, click **Advanced Application > DHCP Snooping > Configure**.

Figure 126 Advanced Application > DHCP Snooping > Configure

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

The following table describes the labels in this screen.

Table 85 Advanced Application > DHCP Snooping > Configure

| LABEL | DESCRIPTION |
|----------------------|--|
| Active | Select this to enable DHCP snooping on the Switch. You still have to enable DHCP snooping on specific VLAN and specify trusted ports. Note: If DHCP is enabled and there are no trusted ports, DHCP requests will not succeed. |
| DHCP Vlan | Select a VLAN ID if you want the Switch to forward DHCP packets to DHCP servers on a specific VLAN. Note: You have to enable DHCP snooping on the DHCP VLAN too. You can enable Option82 in the DHCP Snooping VLAN Configure screen to help the DHCP servers distinguish between DHCP requests from different VLAN. Select Disable if you do not want the Switch to forward DHCP packets to a specific VLAN. |
| Database | If Timeout interval is greater than Write delay interval , it is possible that the next update is scheduled to occur before the current update has finished successfully or timed out. In this case, the Switch waits to start the next update until it completes the current one. |
| Agent URL | Enter the location of the DHCP snooping database. The location should be expressed like this: tftp://{domain name or IP address}/directory, if applicable/file name ; for example, tftp://192.168.10.1/database.txt . |
| Timeout interval | Enter how long (10 – 65535 seconds) the Switch tries to complete a specific update in the DHCP snooping database before it gives up. |
| Write delay interval | Enter how long (10 – 65535 seconds) the Switch waits to update the DHCP snooping database the first time the current bindings change after an update. Once the next update is scheduled, additional changes in current bindings are automatically included in the next update. |

Table 85 Advanced Application > DHCP Snooping > Configure (continued)

| LABEL | DESCRIPTION |
|-------------------------|--|
| Renew DHCP Snooping URL | Enter the location of a DHCP snooping database, and click Renew if you want the Switch to load it. You can use this to load dynamic bindings from a different DHCP snooping database than the one specified in Agent URL . When the Switch loads dynamic bindings from a DHCP snooping database, it does not discard the current dynamic bindings first. If there is a conflict, the Switch keeps the dynamic binding in volatile memory and updates the Binding collisions counter in the DHCP Snooping screen (Section 23.2 on page 181). |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click this to reset the values in this screen to their last-saved values. |

23.3.1 DHCP Snooping Port Configure

Use this screen to specify whether ports are trusted or untrusted ports for DHCP snooping.

Note: If DHCP snooping is enabled but there are no trusted ports, DHCP requests cannot reach the DHCP server.

You can also specify the maximum number for DHCP packets that each port (trusted or untrusted) can receive each second.

To open this screen, click **Advanced Application > DHCP Snooping > Configure > Port**.

Figure 127 Advanced Application > DHCP Snooping > Configure > Port

| DHCP Snooping Port Configure | | Configure |
|------------------------------|----------------------|------------|
| Port | Server Trusted state | Rate (pps) |
| * | Untrusted ▼ | |
| 1 | Untrusted ▼ | 0 |
| 2 | Untrusted ▼ | 0 |
| 3 | Trusted ▼ | 0 |
| 4 | Untrusted ▼ | 0 |
| 5 | Untrusted ▼ | 0 |

Apply Cancel

The following table describes the labels in this screen.

Table 86 Advanced Application > DHCP Snooping > Configure > Port

| LABEL | DESCRIPTION |
|----------------------|---|
| Port | This field displays the port number. If you configure the * port, the settings are applied to all of the 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. |
| Server Trusted state | Select whether this port is a trusted port (Trusted) or an untrusted port (Untrusted). Trusted ports are connected to DHCP servers or other switches, and the Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. Untrusted ports are connected to subscribers, and the Switch discards DHCP packets from untrusted ports in the following situations: <ul style="list-style-type: none"> • The packet is a DHCP server packet (for example, OFFER, ACK, or NACK). • The source MAC address and source IP address in the packet do not match any of the current bindings. • The packet is a RELEASE or DECLINE packet, and the source MAC address and source port do not match any of the current bindings. • The rate at which DHCP packets arrive is too high. |
| Rate (pps) | Specify the maximum number for DHCP packets (1 – 256) that the Switch receives from each port each second. The Switch discards any additional DHCP packets. Enter 0 to disable this limit, which is recommended for trusted ports. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click this to reset the values in this screen to their last-saved values. |

23.3.2 DHCP Snooping VLAN Configure

Use this screen to enable DHCP snooping on each VLAN and to specify whether or not the Switch adds DHCP relay agent option 82 information to DHCP requests that the Switch relays to a DHCP server for each VLAN.

To open this screen, click **Advanced Application > DHCP Snooping > Configure > VLAN**.

Figure 128 Advanced Application > DHCP Snooping > Configure > VLAN

The following table describes the labels in this screen.

Table 87 Advanced Application > DHCP Snooping > Configure > VLAN

| LABEL | DESCRIPTION |
|--------------------|---|
| VLAN Search by VID | Specify the VLANs you want to manage in the section below. Use a comma (,) to separate individual VLANs or a dash (-) to indicate a range of VLANs. For example, "3,4" or "3-9". |
| Search | Click this to display the specified range of VLANs in the section below. |
| VID | This field displays the VLAN ID of each VLAN in the range specified above. If you configure the * VLAN, the settings are applied to all VLANs. |
| Enabled | Select Yes to enable DHCP snooping on the VLAN. You still have to enable DHCP snooping on the Switch and specify trusted ports. Note: If DHCP is enabled and there are no trusted ports, DHCP requests will not succeed. |
| Option 82 Profile | Select a pre-defined DHCP option 82 profile that the Switch applies to all ports in the specified VLANs. The Switch adds the information (such as slot number, port number, VLAN ID and/or system name) specified in the profile to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN. You can specify the DHCP VLAN in the DHCP Snooping Configure screen. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click this to reset the values in this screen to their last-saved values. |
| Change Pages | Click Previous or Next to show the previous/next screen if all status information cannot be seen in one screen. |

23.3.3 DHCP Snooping VLAN Port Configure

Use this screen to apply a different DHCP option 82 profile to certain ports in a VLAN.

To open this screen, click **Advanced Application > DHCP Snooping > Configure > VLAN > Port**.

Figure 129 Advanced Application > DHCP Snooping > Configure > VLAN > Port

The screenshot shows the 'DHCP Snooping VLAN Configure' interface. At the top, there is a 'Port' header and a link to 'DHCP Snooping VLAN Configure'. Below this, there are three input fields: 'VID', 'Port', and 'Option 82 Profile'. Underneath these fields are three buttons: 'Add', 'Cancel', and 'Clear'. At the bottom of the screen, there is a table with the following columns: 'Index', 'VID', 'Port', 'Profile Name', and 'Delete'. Below the table are two buttons: 'Delete' and 'Cancel'.

The following table describes the labels in this screen.

Table 88 Advanced Application > DHCP Snooping > Configure > VLAN > Port

| LABEL | DESCRIPTION |
|-------------------|--|
| VID | Enter the ID number of the VLAN you want to configure here. |
| Port | Enter the number of ports to which you want to apply the specified DHCP option 82 profile. You can enter multiple ports separated by (no space) comma (,) or hyphen (-). For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7. |
| Option 82 Profile | Select a pre-defined DHCP option 82 profile that the Switch applies to the specified ports in this VLAN. The Switch adds the information (such as slot number, port number, VLAN ID and/or system name) specified in the profile to DHCP requests that it broadcasts to the DHCP VLAN, if specified, or VLAN. You can specify the DHCP VLAN in the DHCP Snooping Configure screen. The profile you select here has priority over the one you select in the DHCP Snooping > Configure > VLAN screen. |
| Add | Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click this to reset the values above based on the last selected entry or, if not applicable, to clear the fields above. |
| Clear | Click Clear to reset the fields to the factory defaults. |
| Index | This field displays a sequential number for each entry. Click an index number to change the settings. |
| VID | This field displays the VLAN to which the ports belong. |
| Port | This field displays the ports to which the Switch applies the settings. |
| Profile Name | This field displays the DHCP option 82 profile that the Switch applies to the ports. |
| Delete | Select the entries that you want to remove in the Delete column, then click the Delete button to remove the selected entries from the table. |
| Cancel | Click this to clear the Delete check boxes above. |

23.4 Technical Reference

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

23.4.1 DHCP Snooping Overview

Use DHCP snooping to filter unauthorized DHCP packets on the network and to build the binding table dynamically. This can prevent clients from getting IP addresses from unauthorized DHCP servers.

23.4.1.1 Trusted vs. Untrusted Ports

Every port is either a trusted port or an untrusted port for DHCP snooping. This setting is independent of the trusted or untrusted setting for ARP inspection. You can also specify the maximum number for DHCP packets that each port (trusted or untrusted) can receive each second.

Trusted ports are connected to DHCP servers or other switches. The Switch discards DHCP packets from trusted ports only if the rate at which DHCP packets arrive is too high. The Switch learns dynamic bindings from trusted ports.

Note: If DHCP is enabled and there are no trusted ports, DHCP requests will not succeed.

Untrusted ports are connected to subscribers. The Switch discards DHCP packets from untrusted ports in the following situations:

- The packet is a DHCP server packet (for example, OFFER, ACK, or NACK).
- The source MAC address and source IP address in the packet do not match any of the current bindings.
- The packet is a RELEASE or DECLINE packet, and the source MAC address and source port do not match any of the current bindings.
- The rate at which DHCP packets arrive is too high.

23.4.1.2 DHCP Snooping Database

The Switch stores the binding table in volatile memory. If the Switch restarts, it loads static bindings from permanent memory but loses the dynamic bindings, in which case the devices in the network have to send DHCP requests again. As a result, it is recommended you configure the DHCP snooping database.

The DHCP snooping database maintains the dynamic bindings for DHCP snooping and ARP inspection in a file on an external TFTP server. If you set up the DHCP snooping database, the Switch can reload the dynamic bindings from the DHCP snooping database after the Switch restarts.

You can configure the name and location of the file on the external TFTP server. The file has the following format:

Figure 130 DHCP Snooping Database File Format

```
<initial-checksum>
TYPE DHCP-SNOOPING
VERSION 1
BEGIN
<binding-1> <checksum-1>
<binding-2> <checksum-1-2>
...
...
<binding-n> <checksum-1-2-..-n>
END
```

The <initial-checksum> helps distinguish between the bindings in the latest update and the bindings from previous updates. Each binding consists of 72 bytes, a space, and another checksum that is used to validate the binding when it is read. If the calculated checksum is not equal to the checksum in the file, that binding and all others after it are ignored.

23.4.1.3 DHCP Relay Option 82 Information

The Switch can add information to DHCP requests that it does not discard. This provides the DHCP server more information about the source of the requests. The Switch can add the following information:

- Slot ID (1 byte), port ID (1 byte), and source VLAN ID (2 bytes)
- System name (up to 32 bytes)

This information is stored in an Agent Information field in the option 82 field of the DHCP headers of client DHCP request frames.

When the DHCP server responds, the Switch removes the information in the Agent Information field before forwarding the response to the original source.

You can configure this setting for each source VLAN. This setting is independent of the DHCP relay settings.

23.4.1.4 Configuring DHCP Snooping

Follow these steps to configure DHCP snooping on the Switch.

- 1** Enable DHCP snooping on the Switch.
- 2** Enable DHCP snooping on each VLAN, and configure DHCP relay option 82.
- 3** Configure trusted and untrusted ports, and specify the maximum number of DHCP packets that each port can receive per second.
- 4** Configure static bindings.

CHAPTER 24

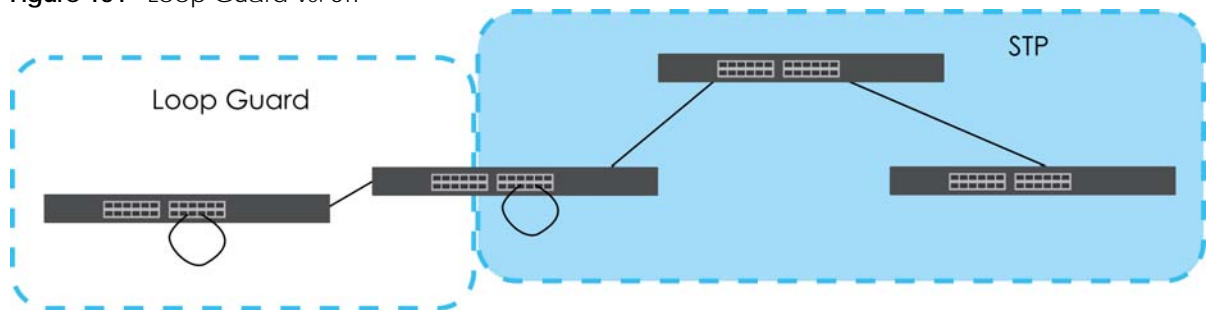
Loop Guard

24.1 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 131 Loop Guard vs. STP



Refer to [Section 24.1.2 on page 192](#) for more information.

24.1.1 What You Can Do

Use the **Loop Guard** screen ([Section 24.2 on page 194](#)) to enable loop guard on the Switch and in specific ports.

24.1.2 What You Need to Know

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

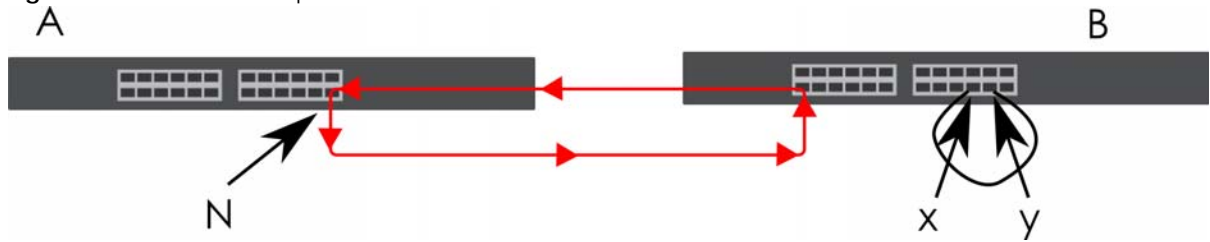
If a switch (not in loop state) connects to a switch in loop state, then it will be affected by the switch in loop state in the following way:

- The switch (not in loop state) will receive broadcast messages sent out from the switch in loop state.
- The switch (not in loop state) will receive its own broadcast messages that it sends out as they loop back. It will then re-broadcast those messages again.

The following figure shows port **N** on switch **A** connected to switch **B**. Switch **B** has two ports, **x** and **y**, mistakenly connected to each other. It forms a loop. When broadcast or multicast packets leave port **N**

and reach switch **B**, they are sent back to port **N** on **A** as they are rebroadcast from **B**.

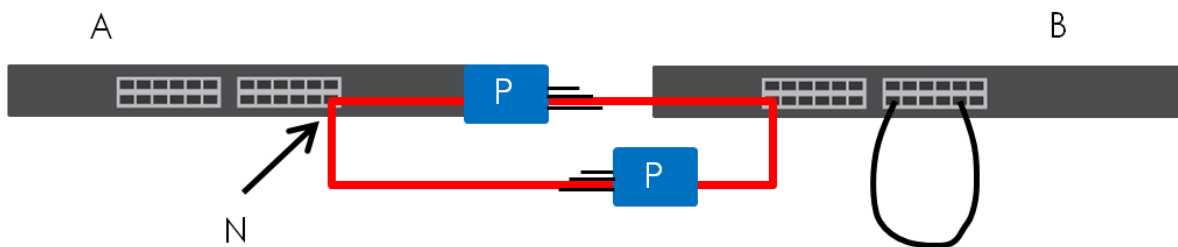
Figure 132 Switch in Loop State



The loop guard feature checks to see if a loop guard enabled port is connected to a Switch in loop state. This is accomplished by periodically sending a probe packet and seeing if the packet returns on the same port. If this is the case, the Switch will shut down the port connected to the switch in loop state.

Loop guard can be enabled on both Ethernet ports. The following figure shows a loop guard enabled port **N** on switch **A** sending a probe packet **P** to switch **B**. Since switch **B** is in loop state, the probe packet **P** returns to port **N** on **A**. The Switch then shuts down port **N** to ensure that the rest of the network is not affected by the switch in loop state.

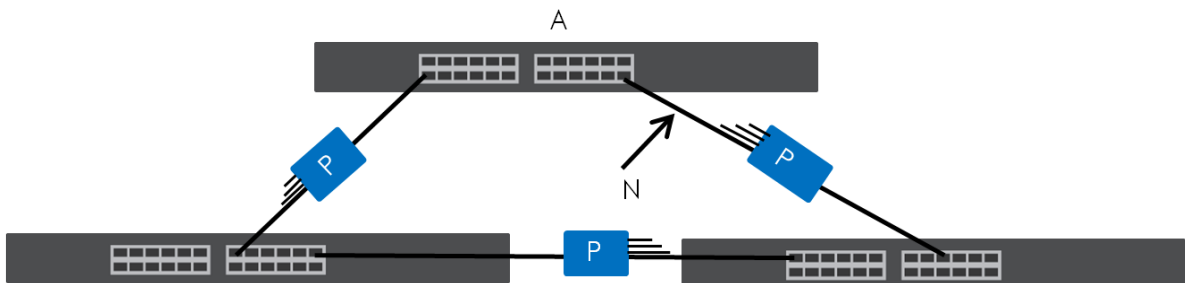
Figure 133 Loop Guard – Probe Packet



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 134 Loop Guard – Network Loop



Note: After resolving the loop problem on your network you can re-activate the disabled port through the Web Configurator or through commands (See the CLI Reference Guide).

24.2 Loop Guard Setup

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

Note: The loop guard feature cannot be enabled on the ports that have Spanning Tree Protocol (RSTP) enabled.

Figure 135 Advanced Application > Loop Guard

| Loop Guard | |
|--|--------------------------|
| Active | <input type="checkbox"/> |
| Port | Active |
| * | <input type="checkbox"/> |
| 1 | <input type="checkbox"/> |
| 2 | <input type="checkbox"/> |
| 3 | <input type="checkbox"/> |
| 4 | <input type="checkbox"/> |
| 5 | <input type="checkbox"/> |
| 6 | <input type="checkbox"/> |
| 7 | <input type="checkbox"/> |
| 8 | <input type="checkbox"/> |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

The following table describes the labels in this screen.

Table 89 Advanced Application > Loop Guard

| LABEL | DESCRIPTION |
|--------|---|
| Active | Select this option to enable loop guard on the Switch. The Switch generates syslog, internal log messages as well as SNMP traps when it shuts down a port through the loop guard feature. |
| Port | This field displays the port number. |
| * | Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Note: Changes in this row are copied to all the ports as soon as you make them. |
| Active | Select this check box to enable the loop guard feature on this port. The Switch sends broadcast and multicast probe packets from this port to check if the switch it is connected to is in loop state. If the switch that this port is connected is in loop state the Switch will shut down this port. Clear this check box to disable the loop guard feature. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

CHAPTER 25

Error-Disable

25.1 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.

25.1.1 CPU Protection Overview

Switches exchange protocol control packets in a network to get the latest networking information. If a switch receives large numbers of control packets, such as ARP, BPDU or IGMP packets, which are to be processed by the CPU, the CPU may become overloaded and be unable to handle regular tasks properly.

The CPU protection feature allows you to limit the rate of ARP, BPDU and IGMP packets to be delivered to the CPU on a port. This enhances the CPU efficiency and protects against potential DoS attacks or errors from other networks. You then can choose to drop control packets that exceed the specified rate limit or disable a port on which the packets are received.

25.1.2 Error-Disable Recovery Overview

Some features, such as loop guard or CPU protection, allow the Switch to shut down a port or discard specific packets on a port when an error is detected on the port. For example, if the Switch detects that packets sent out the ports loop back to the Switch, the Switch can shut down the ports automatically. After that, you need to enable the ports or allow the packets on a port manually through the Web Configurator or the commands. With error-disable recovery, you can set the disabled ports to become active or start receiving the packets again after the time interval you specify.


25.1.3 What You Can Do

- Use the **Errdisable Status** screen ([Section 25.3 on page 196](#)) 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 25.4 on page 198](#)) to limit the maximum number of control packets (ARP, BPDU and/or IGMP) that the Switch can receive or transmit on a port.
- Use the **Errdisable Detect** screen ([Section 25.5 on page 199](#)) to have the Switch detect whether the control packets exceed the rate limit configured for a port and configure the action to take once the limit is exceeded.
- Use the **Errdisable Recovery** screen ([Section 25.6 on page 200](#)) to set the Switch to automatically undo an action after the error is gone.

25.2 Error-Disable Settings

Use this screen to go to the screens where you can configure error disable related settings. Click **Advanced Application > Errdisable** in the navigation panel to open the following screen.

Figure 136 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 90 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. |

25.3 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 137 Advanced Application > Errdisable > Errdisable Status

| Errdisable Status Errdisable | | | | | | | |
|---|------------|----------------------|---------------|-------|------------|---------------------------|---------------|
| Inactive-reason mode reset | | | | | | | |
| Port List | | <input type="text"/> | 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 91 Advanced Application > Errdisable > Errdisable Status

| LABEL | DESCRIPTION |
|----------------------------|---|
| Inactive-reason mode reset | |
| Port List | Enter the number of the ports (separated by a comma) on which you want to reset inactive-reason status. |
| Cause | Select the cause of inactive-reason mode you want to reset here. |
| Reset | Press to reset the specified ports to handle ARP, BPDU or IGMP packets instead of ignoring them, if the ports is in inactive-reason mode. |
| Errdisable Status | |
| Port | This is the number of the port on which you want to configure Errdisable Status. |
| Cause | This displays the type of the control packet received on the port or the feature enabled on the port and causing the Switch to take the specified action. |
| Active | This field displays whether the control packets (ARP, BPDU, and/or IGMP) detecting are enabled or not. It also shows whether loop guard is enabled on the port. You can configure these settings under Advanced Application > Errdisable > Errdisable Detect and Advanced Application > Loop Guard screen. |

Table 91 Advanced Application > Errdisable > Errdisable Status (continued)

| LABEL | DESCRIPTION |
|---------------------------|---|
| Mode | This field shows the action that the Switch takes for the cause. <ul style="list-style-type: none"> • inactive-port – The Switch disables the port. • inactive-reason – The Switch drops all the specified control packets (such as BPDU) on the port. • rate-limitation – The Switch drops the additional control packets the ports has to handle in every one second. |
| Rate | This field displays how many control packets this port can receive or transmit per second. It can be adjusted in CPU Protection . 0 means no rate limit. |
| Status | This field displays the errdisable status <ul style="list-style-type: none"> • Forwarding: The Switch is forwarding packets. Rate-limitation mode is always in Forwarding status. • Err-disable: The Switch disables the port on which the control packets are received (inactive-port) or drops specified control packets on the port (inactive-reason). |
| Recovery Time Left (secs) | This field displays the time (seconds) left before the ports becomes active of Errdisable Recovery. |
| Total Dropped | This field displays the total packet number dropped by this port where the packet rate exceeds the rate of mode rate-limitation. |

25.4 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 138 Advanced Application > Errdisable > CPU protection

The screenshot shows the 'CPU protection' configuration interface. At the top, there is a header 'CPU protection' and a blue link 'Errdisable'. Below this, a 'Reason:' dropdown menu is set to 'ARP'. The main part of the screen is a table with two columns: 'Port' and 'Rate Limit (pkt/s)'. The table has 9 rows, with the first row containing an asterisk (*) and the subsequent rows numbered 1 through 8. Each row has a text input field for the rate limit, all of which are currently set to '0'. At the bottom of the screen, there are two buttons: 'Apply' and 'Cancel'.

| Port | Rate Limit (pkt/s) |
|------|--------------------|
| * | |
| 1 | 0 |
| 2 | 0 |
| 3 | 0 |
| 4 | 0 |
| 5 | 0 |
| 6 | 0 |
| 7 | 0 |
| 8 | 0 |

The following table describes the labels in this screen.

Table 92 Advanced Application > Errdisable > CPU protection

| LABEL | DESCRIPTION |
|--------------------|--|
| Reason | Select the type of control packet you want to configure here. |
| Port | This field displays the port number. |
| * | Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Changes in this row are copied to all the ports as soon as you make them. |
| Rate Limit (pkt/s) | Enter a number from 0 to 256 to specify how many control packets this port can receive or transmit per second. 0 means no rate limit. You can configure the action that the Switch takes when the limit is exceeded. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

25.5 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 139 Advanced Application > Errdisable > Errdisable Detect

| Errdisable Detect | | Errdisable |
|-------------------|--------------------------|----------------------------|
| Cause | Active | Mode |
| * | <input type="checkbox"/> | inactive-port ▾ |
| ARP | <input type="checkbox"/> | inactive-port ▾ |
| BPDU | <input type="checkbox"/> | inactive-port ▾ |
| IGMP | <input type="checkbox"/> | inactive-port ▾ |

The following table describes the labels in this screen.

Table 93 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. |

Table 93 Advanced Application > Errdisable > Errdisable Detect (continued)

| LABEL | DESCRIPTION |
|--------|---|
| 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. <ul style="list-style-type: none"> inactive-port – The Switch disables the port on which the control packets are received. inactive-reason – The Switch drops all the specified control packets (such as BPDU) on the port. rate-limitation – The Switch drops the additional control packets the ports has to handle in every one second. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

25.6 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 140 Advanced Application > Errdisable > Errdisable Recovery

| Reason | Timer Status | Interval |
|-----------|--------------------------|----------|
| * | <input type="checkbox"/> | |
| loopguard | <input type="checkbox"/> | 300 |
| ARP | <input type="checkbox"/> | 300 |
| BPDU | <input type="checkbox"/> | 300 |
| IGMP | <input type="checkbox"/> | 300 |

The following table describes the labels in this screen.

Table 94 Advanced Application > Errdisable > Errdisable Recovery

| LABEL | DESCRIPTION |
|--------------|--|
| Active | Select this option to turn on the error-disable recovery function on the Switch. |
| Reason | This field displays the supported features that allow the Switch to shut down a port or discard packets on a port according to the feature requirements and what action you configure. |
| * | Use this row to make the setting the same for all entries. Use this row first and then make adjustments to each entry if necessary. Changes in this row are copied to all the entries as soon as you make them. |
| Timer Status | Select this check box to allow the Switch to wait for the specified time interval to activate a port or allow specific packets on a port, after the error was gone. Clear the check box to turn off this rule. |

Table 94 Advanced Application > Errdisable > Errdisable Recovery (continued)

| LABEL | DESCRIPTION |
|----------|--|
| 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 26

Green Ethernet

This chapter shows you how to configure the Switch to reduce the power consumed by switch ports.

26.1 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.

26.2 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 141 Advanced Application > Green Ethernet

| Green Ethernet | | | |
|--|--------------------------|--------------------------|--------------------------|
| EEE | <input type="checkbox"/> | | |
| Auto Power Down | <input type="checkbox"/> | | |
| Short Reach | <input type="checkbox"/> | | |
| Port | EEE | Auto Power Down | Short Reach |
| * | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 1 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 5 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 6 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 7 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 8 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | | | |

The following table describes the labels in this screen.

Table 95 Advanced Application > Green Ethernet

| LABEL | DESCRIPTION |
|-----------------|--|
| EEE | Select this to activate Energy Efficient Ethernet globally. |
| Auto Power Down | Select this to activate Auto Power Down globally. |
| Short Reach | Select this to activate Short Reach globally. |
| Port | This field displays the port number. |
| * | Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Changes in this row are copied to all the ports as soon as you make them. |
| EEE | Select this to activate Energy Efficient Ethernet on this port. |
| Auto Power Down | Select this to activate Auto Power Down on this port. |
| Short Reach | Select this to activate Short Reach on this port. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

Link Layer Discovery Protocol (LLDP)

27.1 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:

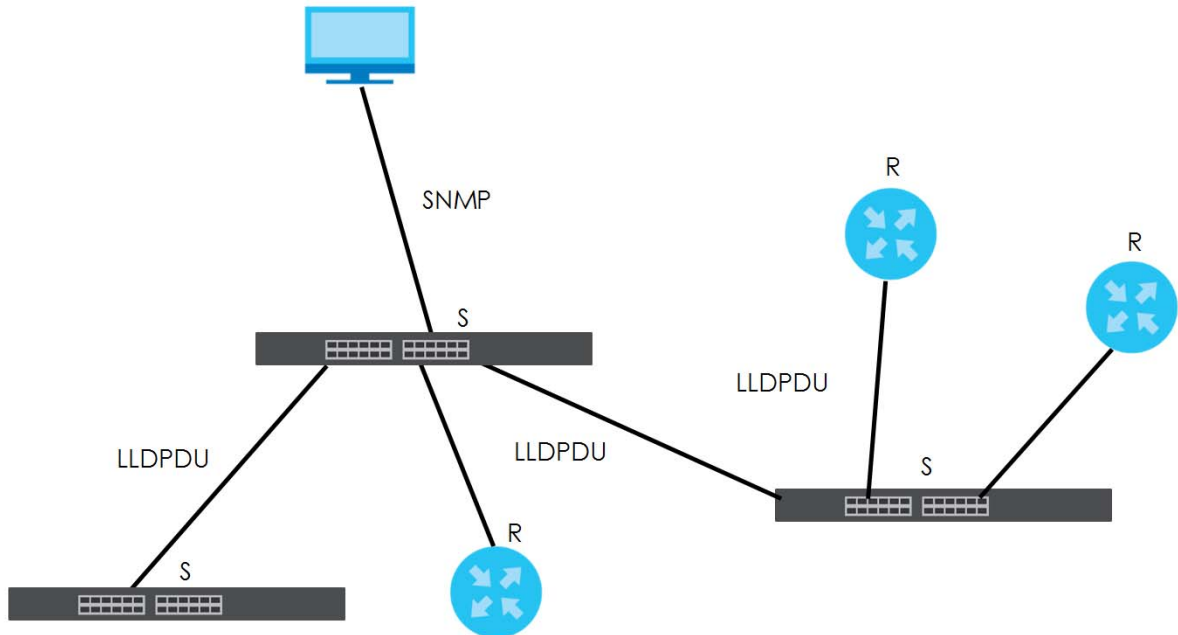
- MAC/PHY Configuration/Status TLV (optional)
- Power via MDI TLV (optional, For PoE models only)
- Link Aggregation TLV (optional)
- Maximum Frame Size TLV (optional)

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 through LLDPDU and the network manager can query the information using Simple Network Management Protocol (SNMP).

Figure 142 LLDP Overview



27.2 LLDP-MED Overview

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

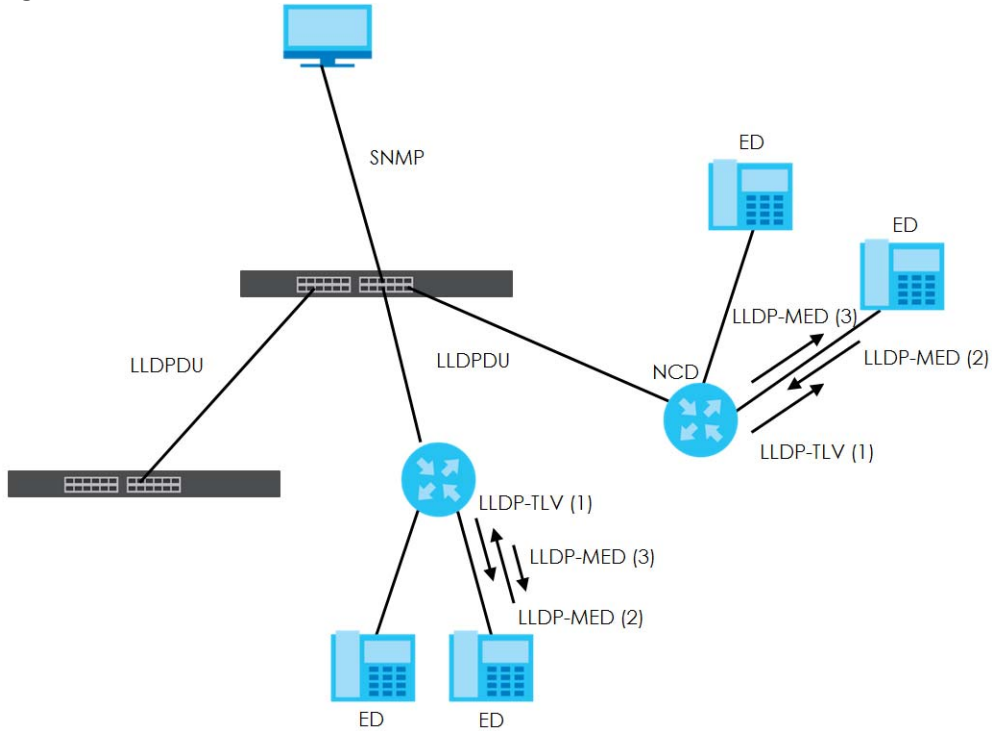
Class I: IP Communications Controllers or other communication related servers

Class II: Voice Gateways, Conference Bridges or Media Servers

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

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

Figure 143 LLDP-MED Overview



27.3 LLDP Settings

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

Figure 144 Advanced Application > LLDP

| LLDP | | |
|----------|-------------------------|----------------------------|
| LLDP | LLDP Local Status | Click here |
| | LLDP Remote Status | Click here |
| | LLDP Configuration | Click here |
| LLDP-MED | LLDP-MED Configuration | Click here |
| | LLDP-MED Network Policy | Click here |
| | LLDP-MED Location | Click here |

The following table describes the labels in this screen.

Table 96 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. |

Table 96 Advanced Application > LLDP (continued)

| LABEL | DESCRIPTION |
|-------------------------|---|
| LLDP-MED | |
| LLDP-MED Configuration | Click here to show a screen to configure LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) parameters. |
| LLDP-MED Network Policy | Click here to show a screen to configure LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) network policy parameters. |
| LLDP-MED Location | Click here to show a screen to configure LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) location parameters. |

27.4 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 145 Advanced Application > LLDP > LLDP Local Status

| LLDP Local Status | | | LLDP |
|--------------------------------|-------------------------------|------------------------------|------------------|
| 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 | GS1915 | |
| System Description TLV | System Description | V4.70(ACAQ.0)b1 09/06/2021 | |
| System Capabilities TLV | System Capabilities Supported | Bridge | |
| | System Capabilities Enabled | Bridge | |
| Management Address TLV | Management Address Subtype | ipv4 / all-802 | |
| | Interface Number Subtype | unknown | |
| | Interface Number | 0 | |
| | Object Identifier | 0 | |
| LLDP Port Information | | | |
| Local Port | Port ID Subtype | Port ID | Port Description |
| 1 | local-assigned | 1 | |
| 2 | local-assigned | 2 | |
| 3 | local-assigned | 3 | |
| 4 | local-assigned | 4 | |
| 5 | local-assigned | 5 | |
| 6 | local-assigned | 6 | |
| 7 | local-assigned | 7 | |
| 8 | local-assigned | 8 | |

The following table describes the labels in this screen.

Table 97 Advanced Application > LLDP > LLDP Local Status

| LABEL | DESCRIPTION |
|-------------------------|--|
| Basic TLV | |
| Chassis ID TLV | This displays the chassis ID of the local Switch, that is the Switch you are configuring. The chassis ID is identified by the chassis ID subtype. Chassis ID Subtype – this displays how the chassis of the Switch is identified. Chassis ID – This displays the chassis ID of the local Switch. |
| System Name TLV | This shows the host name of the Switch. |
| System Description TLV | This shows the firmware version of the Switch. |
| System Capabilities TLV | This shows the System Capabilities enabled and supported on the local Switch. <ul style="list-style-type: none"> • System Capabilities Supported – Bridge • System Capabilities Enabled – Bridge |
| Management Address TLV | The Management Address TLV identifies an address associated with the local LLDP agent that may be used to reach higher layer entities to assist discovery by network management. The TLV may also include the system interface number and an object identifier (OID) that are associated with this management address. This field displays the Management Address settings on the specified ports. <ul style="list-style-type: none"> • Management Address Subtype – ipv4 or all-802 • Interface Number Subtype – unknown • Interface Number – 0 (not supported) • Object Identifier – 0 (not supported) |
| LLDP Port Information | This displays the local port information. |
| Local Port | This displays the number of the Switch port which receives the LLDPDU from the remote device. Click a port number to view the detailed LLDP status on this port in the LLDP Local Port Status Detail screen. |
| Port ID Subtype | This indicates how the port ID field is identified. |
| Port ID | This is an alpha-numeric string that contains the specific identifier for the port from which this LLDPDU was transmitted. |
| Port Description | This shows the port description that the Switch will advertise from this port. |

27.4.1 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 146 Advanced Application > LLDP > LLDP Local Status > LLDP Local Port Status Detail

| LLDP Local Port Status Detail | | LLDP Local Status |
|------------------------------------|--------------------------|---|
| Local Port: 1 | | |
| Basic TLV | | |
| Port ID TLV | Port ID Subtype | local-assigned |
| | Port ID | 1 |
| Port Description TLV | Port Description | port1 |
| Dot1 TLV | | |
| Port VLAN ID TLV | Port VLAN ID | 1 |
| Dot3 TLV | | |
| MAC PHY Configuration & Status TLV | AN Supported | Yes |
| | AN Enabled | Yes |
| | AN Advertised Capability | 10baseT 10baseTFD 100baseTX 100baseTXFD 1000baseTFD |
| | Oper MAU Type | 30 |
| Link Aggregation TLV | Aggregation Capability | Yes |
| | Aggregation Status | No |
| | Aggregated Port ID | 0 |
| Max Frame Size TLV | Max Frame Size | 1518 |
| MED TLV | | |
| Capabilities TLV | Network Policy | Yes |
| | Location | Yes |
| | Extend Power via MDI PSE | No |
| | Extend Power via MDI PD | No |
| | Inventory Management | No |
| Device Type TLV | Device Type | Network Connectivity |
| Network Policy TLV | Voice | |
| | Voice-Signaling | |
| | Guest-Voice | |
| | Guest-Voice-Signaling | |
| | Softphone-Voice | |
| | Video-Conferencing | |
| | Streaming-Video | |
| | Video-Signaling | |
| Location Identification TLV | Coordinate-base LCI | |
| | Civic LCI | |
| | ELIN | |

The following table describes the labels in this screen.

Table 98 Advanced Application > LLDP > LLDP Local Status > LLDP Local Port Status Detail

| LABEL | DESCRIPTION |
|------------------------------------|---|
| Local Port | This displays the number of the Switch's port. |
| Basic TLV | These are the Basic TLV flags |
| Port ID TLV | The port ID TLV identifies the specific port that transmitted the LLDP frame. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • Network Connectivity |

Table 98 Advanced Application > LLDP > LLDP Local Status > LLDP Local Port Status Detail (continued)

| LABEL | DESCRIPTION |
|-----------------------------|---|
| Network Policy TLV | This displays a network policy for the specified application. <ul style="list-style-type: none"> • 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). <ul style="list-style-type: none"> • 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) |

27.5 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 147 Advanced Application > LLDP > LLDP Remote Status

| Index | Local Port | Chassis ID | Port ID | Port Description | System Name | Management Address |
|-------|------------|-------------------|-----------------------|------------------|-------------|--------------------|
| 1 | 1 | 08:26:97:c4:cc:a2 | 08:26:97:c4:c c:a2 | | | |
| 2 | 1 | 0a:26:97:c4:cc:a4 | 08:26:97:c4:c c:a2 | | | |
| 3 | 3 | dc:4a:3e:40:ec:5f | dc:4a:3e:40:e c:5f | | | |
| 4 | 5 | e4:18:6b:f7:ba:0d | 39 | | 12A3_84 | e4:18:6b:f7:ba:0d |

The following table describes the labels in this screen.

Table 99 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. |

27.5.1 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 148 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Basic TLV)

| LLDP Remote Port Status Detail | | LLDP Remote Status |
|--------------------------------|-------------------------------|-------------------------------------|
| Local Port: 5 | | |
| Basic TLV | | |
| Chassis ID TLV | Chassis ID Subtype | mac-address |
| | Chassis ID | e4:18:6b:f7:ba:0d |
| Port ID TLV | Port ID Subtype | local-assigned |
| | Port ID | 37 |
| Time To Live TLV | Time To Live | 120 |
| Port Description TLV | Port Description | |
| System Name TLV | System Name | 12A3_84 |
| System Description TLV | System Description | V4.30(AAGE.2)_20200930 09/30/2020 |
| System Capabilities TLV | System Capabilities Supported | bridge |
| | System Capabilities Enabled | bridge |
| Management Address TLV | Management Address Subtype | ALL_802 |
| | Management Address | e4:18:6b:f7:ba:0d |
| | Interface Number Subtype | unknown |
| | Interface Number | 0 |
| | Object Identifier | |

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

Table 100 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 | <ul style="list-style-type: none"> 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 | <ul style="list-style-type: none"> Port ID Subtype – this displays how the port of the remote device is identified. Port ID – this displays the port ID of the remote device. The port ID is identified by the port ID subtype. |
| Time To Live TLV | This displays the time-to-live (TTL) multiplier of LLDP frames. The device information on the neighboring devices ages out and is discarded when its corresponding TTL expires. The TTL value is to multiply the TTL multiplier by the LLDP frames transmitting interval. |

Table 100 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Basic TLV) (continued)

| LABEL | DESCRIPTION |
|-------------------------|---|
| 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. <ul style="list-style-type: none">• System Capabilities Supported• System Capabilities Enabled |
| Management Address TLV | This displays the management address (IPv4 and IPv6) of the remote device. <ul style="list-style-type: none">• Management Address Subtype• Management Address• Interface Number Subtype• Interface Number• Object Identifier |

Figure 149 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Dot1 and Dot3 TLV)

| Dot1 TLV | | |
|------------------------------------|---------------------------------|-----|
| Port VLAN ID TLV | Port VLAN ID | |
| Port-Protocol VLAN ID TLV | Port-Protocol VLAN ID | |
| | Port-Protocol VLAN ID Supported | |
| | Port-Protocol VLAN ID Enabled | |
| Vlan Name TLV | VLAN ID | |
| | VLAN Name | |
| Protocol Identity TLV | Protocol ID | |
| Dot3 TLV | | |
| MAC PHY Configuration & Status TLV | AN Supported | No |
| | AN Enabled | No |
| | AN Advertised Capability | |
| | Oper MAU type | 0 |
| Link Aggregation TLV | Aggregation Capability | Yes |
| | Aggregation Status | No |
| | Aggregated Port ID | 0 |
| Power Via MDI TLV | Port Class | |
| | MDI Supported | |
| | MDI Enabled | |
| | Pair Controlable | |
| | PSE Power Pairs | |
| | Power Class | |
| Max Frame Size TLV | Max Frame Size | |

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

Table 101 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. <ul style="list-style-type: none"> • Port-Protocol VLAN ID • Port-Protocol VLAN ID Supported • Port-Protocol VLAN ID Enabled |

Table 101 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (Dot1 and Dot3 TLV) (continued)

| LABEL | DESCRIPTION |
|------------------------------------|--|
| Vlan Name TLV | <p>This shows the VLAN ID and name for remote device port.</p> <ul style="list-style-type: none"> • VLAN ID • VLAN Name |
| Protocol Identity TLV | <p>The Protocol Identity TLV allows the Switch to advertise the particular protocols that are accessible through its port.</p> |
| Dot3 TLV | |
| MAC PHY Configuration & Status TLV | <p>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.</p> <ul style="list-style-type: none"> • 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 | <p>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.</p> <ul style="list-style-type: none"> • 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 | <p>The Power Via MDI TLV allows network management to advertise and discover the MDI power support capabilities of the sending port on the remote device.</p> <ul style="list-style-type: none"> • Port Class • MDI Supported • MDI Enabled • Pair Controllable • PSE Power Pairs • Power Class |
| Max Frame Size TLV | <p>This displays the maximum supported frame size in octets.</p> |

Figure 150 Advanced Application > LLDP > LLDP Remote Status > LLDP Remote Port Status Detail (MED TLV)

| MED TLV | |
|-----------------------------|--------------------------|
| Capabilities TLV | Network Policy |
| | Location |
| | Extend Power via MDI PSE |
| | Extend Power via MDI PD |
| | Inventory Management |
| Device Type TLV | Device Type |
| 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 |
| Inventory TLV | Hardware Revision |
| | Software Revision |
| | Firmware Revision |
| | Model Name |
| | Manufacturer |
| | Serial Number |
| Extended Power via MDI TLV | Asset ID |
| | Power Type |
| | Power Source |
| | Power Priority |
| | Power Value |

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

Table 102 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 | <p>This displays the MED capabilities the remote port supports.</p> <ul style="list-style-type: none"> • Network Policy • Location • Extend Power via MDI PSE • Extend Power via MDI PD • Inventory Management |
| Device Type TLV | <p>LLDP-MED endpoint device classes:</p> <ul style="list-style-type: none"> • Endpoint Class I • Endpoint Class II • Endpoint Class III • Network Connectivity |
| Network Policy TLV | <p>This displays a network policy for the specified application.</p> <ul style="list-style-type: none"> • Voice • Voice-Signaling • Guest-Voice • Guest-Voice-Signaling • Softphone-Voice • Video-Conferencing • Streaming-Video • Video-Signaling |
| Location Identification TLV | <p>This shows the location information of a caller by its:</p> <ul style="list-style-type: none"> • Coordinate-base LCI – latitude and longitude coordinates of the Location Configuration Information (LCI) • Civic LCI – IETF Geopriv Civic Address based Location Configuration Information • ELIN – (Emergency Location Identifier Number) |
| Inventory TLV | <p>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.</p> <ul style="list-style-type: none"> • Hardware Revision • Software Revision • Firmware Revision • Model Name • Manufacturer • Serial Number • Asset ID |
| Extended Power via MDI TLV | <p>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.</p> <ul style="list-style-type: none"> • 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. |

27.6 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 151 Advanced Application > LLDP > LLDP Configuration

| LLDP Configuration | | LLDP | Basic TLV Setting | Org-specific TLV Setting |
|--|-------------------------------------|--------------------------|-------------------|--------------------------|
| Active | <input checked="" type="checkbox"/> | | | |
| Transmit Interval | 30 | seconds | | |
| Transmit Hold | 4 | times | | |
| Transmit Delay | 2 | seconds | | |
| Reinitialize Delay | 2 | seconds | | |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | | | | |
| Port | Admin Status | Notification | | |
| * | Disable ▾ | <input type="checkbox"/> | | |
| 1 | Tx-Rx ▾ | <input type="checkbox"/> | | |
| 2 | Tx-Rx ▾ | <input type="checkbox"/> | | |
| 3 | Tx-Rx ▾ | <input type="checkbox"/> | | |
| 4 | Tx-Rx ▾ | <input type="checkbox"/> | | |
| 5 | Tx-Rx ▾ | <input type="checkbox"/> | | |
| 6 | Tx-Rx ▾ | <input type="checkbox"/> | | |
| 7 | Tx-Rx ▾ | <input type="checkbox"/> | | |
| 8 | Tx-Rx ▾ | <input type="checkbox"/> | | |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | | | | |

The following table describes the labels in this screen.

Table 103 Advanced Application > LLDP > LLDP Configuration

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

Table 103 Advanced Application > LLDP > LLDP Configuration (continued)

| LABEL | DESCRIPTION |
|--------------|---|
| Admin Status | Select whether LLDP transmission and/or reception is allowed on this port. <ul style="list-style-type: none"> • 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. |

27.6.1 LLDP Configuration Basic TLV Setting

Use this screen to configure Basic TLV settings. Click **Advanced Application > LLDP > LLDP Configuration (Click Here) > Basic TLV Setting** to display the screen as shown next.

Figure 152 Advanced Application > LLDP > LLDP Configuration > Basic TLV Setting

| Basic TLV Setting | | LLDP Configuration | | | |
|-------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|
| Port | Management Address | Port Description | System Capabilities | System Description | System Name |
| * | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 1 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 2 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 3 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 4 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 5 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 6 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 7 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |
| 8 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> |

The following table describes the labels in this screen.

Table 104 Advanced Application > LLDP > LLDP Configuration > Basic TLV Setting

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

Table 104 Advanced Application > LLDP > LLDP Configuration > Basic TLV Setting (continued)

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

27.6.2 LLDP Configuration Org-specific TLV Setting

Use this screen to configure organization-specific TLV settings. Click **Advanced Application > LLDP > LLDP Configuration (Click Here) > Org-specific TLV Setting** to display the screen as shown next.

Figure 153 Advanced Application > LLDP > LLDP Configuration > Org-specific TLV Setting

| Org-specific TLV Setting | | | | | LLDP Configuration |
|--------------------------|-------------------------------------|--------------------------|-------------------------------------|--------------------------|------------------------------------|
| Port | Dot1 TLV Port VLAN ID | Link Aggregation | Dot3 TLV MAC/PHY | Max Frame Size | |
| * | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| 1 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 2 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 3 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 4 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |
| 5 | <input checked="" type="checkbox"/> | <input type="checkbox"/> | <input checked="" type="checkbox"/> | <input type="checkbox"/> | |

The following table describes the labels in this screen.

Table 105 Advanced Application > LLDP > LLDP Configuration > Org-specific TLV Setting

| LABEL | DESCRIPTION |
|------------------|--|
| Port | This displays the Switch's port number. |
| * | Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Changes in this row are copied to all the ports as soon as you make them. |
| Dot1 TLV | |
| Port VLAN ID | Select the check boxes to enable or disable the sending of IEEE 802.1 Port VLAN ID TLVs on the ports. All check boxes in this column are enabled by default. |
| Dot3 TLV | |
| Link Aggregation | Select the check boxes to enable or disable the sending of IEEE 802.3 Link Aggregation TLVs on the ports. |
| MAC/PHY | Select the check boxes to enable or disable the sending of IEEE 802.3 MAC/PHY Configuration/Status TLVs on the ports. All check boxes in this column are enabled by default. |
| Max Frame Size | Select the check boxes to enable or disable the sending of IEEE 802.3 Max Frame Size TLVs on the ports. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

27.7 LLDP-MED Configuration

Click **Advanced Application > LLDP > LLDP-MED Configuration** to display the screen as shown next.

Figure 154 Advanced Application > LLDP > LLDP-MED Configuration

| LLDP-MED Configuration | | | |
|------------------------|------------------------------|--------------------------|--------------------------|
| Port | MED TLV Setting | | |
| | Notification Topology Change | Location | Network Policy |
| * | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 1 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 2 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 3 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 4 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 5 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 6 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 7 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |
| 8 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> |

The following table describes the labels in this screen.

Table 106 Advanced Application > LLDP > LLDP-MED Configuration

| LABEL | DESCRIPTION |
|-----------------|--|
| Port | This displays the Switch's port number. Select * to configure all ports simultaneously. |
| * | Use this row to make the setting the same for all ports. Use this row first and then make adjustments to each port if necessary. Changes in this row are copied to all the ports as soon as you make them. |
| Notification | |
| Topology Change | Select to enable LLDP-MED topology change traps on this port. |
| MED TLV Setting | |
| Location | Select to enable transmitting LLDP-MED location TLV. |
| Network Policy | Select to enable transmitting LLDP-MED Network Policy TLV. |
| Apply | Click Apply to save the changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

27.8 LLDP-MED Network Policy

Click **Advanced Application > LLDP > LLDP-MED Network Policy (Click Here)** to display the screen as shown next.

Figure 155 Advanced Application > LLDP > LLDP-MED Network Policy

The following table describes the labels in this screen.

Table 107 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. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • tagged • untagged |
| VLAN | Enter the VLAN ID number. It should be from 1 to 4094. For priority tagged frames, enter "0". |
| DSCP | Enter the DSCP value of the network policy. The value is defined from 0 through 63 with the 0 representing use of the default DSCP value. |
| Priority | Enter the priority value for the network policy. |
| Add | Click Add after finish entering the network policy information. A summary table will list all the Switch you have added. |
| Cancel | Click Cancel to begin entering the information afresh. |
| Index | This field displays the of index number of the network policy. Click an index number to edit the rule. |
| Port | This field displays the port number of the network policy. |
| Application Type | This field displays the application type of the network policy. |
| Tag | This field displays the Tag Status of the network policy. |
| VLAN | This field displays the VLAN ID 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. |

Table 107 Advanced Application > LLDP > LLDP-MED Network Policy (continued)

| LABEL | DESCRIPTION |
|--------|---|
| Delete | Check the rules that you want to remove, then click the Delete button. |
| Cancel | Click Cancel to clear the selected check boxes. |

27.9 LLDP-MED Location

Click **Advanced Application > LLDP > LLDP-MED Location (Click Here)** to display the screen as shown next.

Figure 156 Advanced Application > LLDP > LLDP-MED Location

The following table describes the labels in this screen.

Table 108 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. <ul style="list-style-type: none"> • north • south |

Table 108 Advanced Application > LLDP > LLDP-MED Location (continued)

| LABEL | DESCRIPTION |
|----------------------|---|
| Longitude | Enter the longitude information. The value should be from 0° to 180°. The negative value represents the West. <ul style="list-style-type: none"> • west • east |
| Altitude | Enter the altitude information. The value should be from -2097151 to 2097151 in meters or in floors. <ul style="list-style-type: none"> • meters • floor |
| Datum | Select the appropriate geodetic datum used by GPS. <ul style="list-style-type: none"> • WGS84 • NAD83-NAVD88 • NAD83-MLLW |
| Civic Address | Enter the Civic Address by providing information such as Country, State, County, City, Street, Number, ZIP code and other additional information. Enter at least 2 fields in this configuration including the Country. The valid length of the Country field is 2 characters and all other fields are up to 32 characters. <ul style="list-style-type: none"> • 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. |

Table 108 Advanced Application > LLDP > LLDP-MED Location (continued)

| LABEL | DESCRIPTION |
|---------------|---|
| Civic Address | This field displays the Civic Address for the remote device using information such as Country, State, County, City, Street, Number, ZIP code and additional information. |
| ELIN Number | This field shows the Emergency Location Identification Number (ELIN), which is used to identify endpoint devices when they issue emergency call services. The valid length is form 10 to 25 characters. |
| | Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries. |
| Delete | Check the locations that you want to remove, then click the Delete button. |
| Cancel | Click Cancel to clear the selected check boxes. |

CHAPTER 28

Differentiated Services

28.1 DiffServ Overview

This chapter shows you how to configure Differentiated Services (DiffServ) on the Switch.

Quality of Service (QoS) is used to prioritize source-to-destination traffic flows. All packets in the flow are given the same priority. You can use CoS (class of service) to give different priorities to different packet types.

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

- Use the **DiffServ** screen ([Section 28.2 on page 227](#)) to activate DiffServ to apply marking rules or IEEE 802.1p priority mapping on the Switch.
- Use the **DSCP Setting** screen ([Section 28.3.1 on page 229](#)) to change the DSCP-IEEE 802.1p mapping.

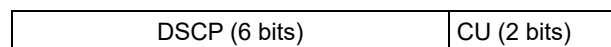
28.1.1 What You Need to Know

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

DSCP and Per-Hop Behavior

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

Figure 157 DiffServ: Differentiated Service Field



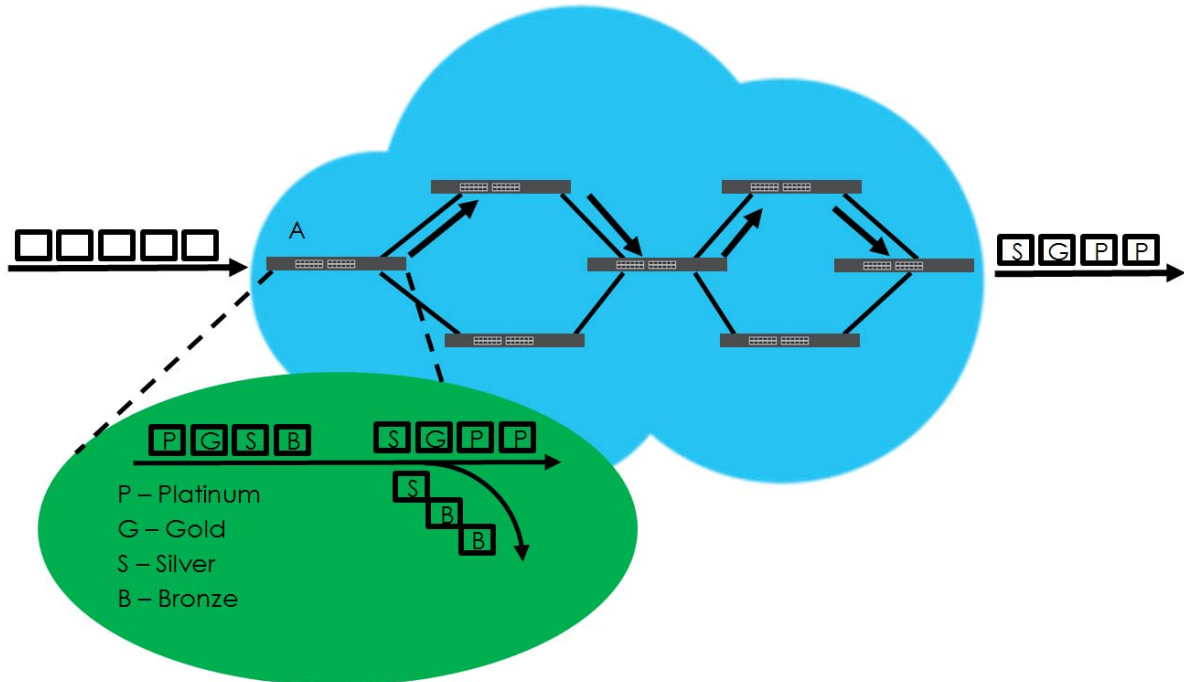
DSCP is backward compatible with the three precedence bits in the ToS octet so that non-DiffServ compliant, ToS-enabled network device will not conflict with the DSCP mapping.

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

DiffServ Network Example

The following figure depicts a DiffServ network consisting of a group of directly connected DiffServ-compliant network devices. The boundary node (**A** in Figure 158) in a DiffServ network classifies (marks with a DSCP value) the incoming packets into different traffic flows (**Platinum, Gold, Silver, Bronze**) based on the configured marking rules. A network administrator can then apply various traffic policies to the traffic flows. An example traffic policy, is to give higher drop precedence to one traffic flow over others. In our example, packets in the **Bronze** traffic flow are more likely to be dropped when congestion occurs than the packets in the **Platinum** traffic flow as they move across the DiffServ network.

Figure 158 DiffServ Network



28.2 Activating DiffServ

Activate DiffServ to apply marking rules or IEEE 802.1p priority mapping on the selected ports.

Click **IP Application** > **DiffServ** in the navigation panel to display the screen as shown.

Figure 159 IP Application > DiffServ

| Diffserv | | DSCP Setting |
|--|--------------------------|------------------------------|
| Active | <input type="checkbox"/> | |
| Port | Active | |
| * | <input type="checkbox"/> | |
| 1 | <input type="checkbox"/> | |
| 2 | <input type="checkbox"/> | |
| 3 | <input type="checkbox"/> | |
| 4 | <input type="checkbox"/> | |
| 5 | <input type="checkbox"/> | |
| 6 | <input type="checkbox"/> | |
| 7 | <input type="checkbox"/> | |
| 8 | <input type="checkbox"/> | |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | | |

The following table describes the labels in this screen.

Table 109 IP Application > DiffServ

| LABEL | DESCRIPTION |
|--------|---|
| Active | Select this option to enable DiffServ on the Switch. |
| Port | This field displays the index number of a port on the Switch. |
| * | Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them. |
| Active | Select Active to enable Diffserv on the port. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

28.3 DSCP-to-IEEE 802.1p Priority Settings

You can configure the DSCP to IEEE 802.1p mapping to allow the Switch to prioritize all traffic based on the incoming DSCP value according to the DiffServ to IEEE 802.1p mapping table.

The following table shows the default DSCP-to-IEEE802.1p mapping.

Table 110 Default DSCP-IEEE 802.1p Mapping

| | | | | | | | | |
|-------------|-------|--------|---------|---------|---------|---------|---------|---------|
| DSCP VALUE | 0 – 7 | 8 – 15 | 16 – 23 | 24 – 31 | 32 – 39 | 40 – 47 | 48 – 55 | 56 – 63 |
| IEEE 802.1p | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

28.3.1 Configuring DSCP Settings

To change the DSCP-IEEE 802.1p mapping click the **DSCP Setting** link in the **DiffServ** screen to display the screen as shown next.

Figure 160 IP Application > DiffServ > DSCP Setting

| DSCP Setting | | | | | | | | Diffserv | | | | | | | |
|------------------------|---|----|---|----|---|----|---|----------|---|----|---|----|---|----|---|
| DSCP to 802.1p Mapping | | | | | | | | | | | | | | | |
| 0 | 0 | 1 | 0 | 2 | 0 | 3 | 0 | 4 | 0 | 5 | 0 | 6 | 0 | 7 | 0 |
| 8 | 1 | 9 | 1 | 10 | 1 | 11 | 1 | 12 | 1 | 13 | 1 | 14 | 1 | 15 | 1 |
| 16 | 2 | 17 | 2 | 18 | 2 | 19 | 2 | 20 | 2 | 21 | 2 | 22 | 2 | 23 | 2 |
| 24 | 3 | 25 | 3 | 26 | 3 | 27 | 3 | 28 | 3 | 29 | 3 | 30 | 3 | 31 | 3 |
| 32 | 4 | 33 | 4 | 34 | 4 | 35 | 4 | 36 | 4 | 37 | 4 | 38 | 4 | 39 | 4 |
| 40 | 5 | 41 | 5 | 42 | 5 | 43 | 5 | 44 | 5 | 45 | 5 | 46 | 5 | 47 | 5 |
| 48 | 6 | 49 | 6 | 50 | 6 | 51 | 6 | 52 | 6 | 53 | 6 | 54 | 6 | 55 | 6 |
| 56 | 7 | 57 | 7 | 58 | 7 | 59 | 7 | 60 | 7 | 61 | 7 | 62 | 7 | 63 | 7 |

Apply Cancel

The following table describes the labels in this screen.

Table 111 IP Application > DiffServ > DSCP Setting

| LABEL | DESCRIPTION |
|----------|--|
| 0 ... 63 | This is the DSCP classification identification number. To set the IEEE 802.1p priority mapping, select the priority level from the drop-down list box. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

29.1 DHCP Overview

This chapter shows you how to configure the DHCP feature.

DHCP (Dynamic Host Configuration Protocol RFC 2131 and RFC 2132) allows individual computers to obtain TCP/IP configuration at start-up from a server. If you configure the Switch as a DHCP relay agent, then the Switch forwards DHCP requests to DHCP server on your network. If you do not configure the Switch as a DHCP relay agent then you must have a DHCP server in the broadcast domain of the client computers or else the client computers must be configured manually.

29.1.1 What You Can Do

- Use the **DHCPv4 Status** screen ([Section 29.3 on page 231](#)) to display the relay mode.
- Use the **DHCPv4 Option 82 Profile** screen ([Section 29.4.2 on page 233](#)) to create DHCPv4 option 82 profiles.
- Use the **DHCPv4 Global Relay** screen ([Section 29.4.3 on page 234](#)) to configure global DHCPv4 relay.
- Use the **DHCPv4 Global Relay Port** screen ([Section 29.4.4 on page 235](#)) to apply a different DHCP option 82 profile to certain ports on the Switch.
- Use the **VLAN Setting** screen ([Section 29.4.6 on page 237](#)) to configure your DHCPv4 settings based on the VLAN domain of the DHCPv4 clients.
- Use the **DHCPv4 VLAN Port** screen ([Section 29.4.7 on page 238](#)) to apply a different DHCP option 82 profile to certain ports in a VLAN.
- Use the **DHCPv6 Relay** screen ([Section 29.5 on page 240](#)) to enable and configure DHCPv6 relay.

29.1.2 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.

29.2 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.

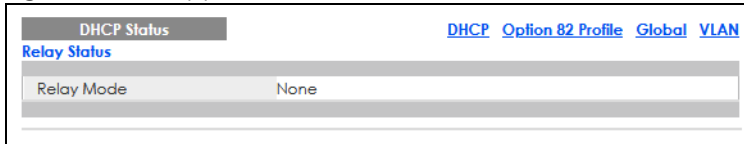
Figure 161 IP Application > DHCP



29.3 DHCPv4 Status

Click **IP Application** > **DHCP** > **DHCPv4** in the navigation panel. The **DHCP Status** screen displays.

Figure 162 IP Application > DHCP > DHCPv4



The following table describes the labels in this screen.

Table 112 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: <ul style="list-style-type: none"> None – if the Switch is not configured as a DHCP relay agent. Global – if the Switch is configured as a DHCP relay agent only. VLAN – followed by a VLAN ID or multiple VLAN IDs if it is configured as a relay agent for specific VLANs. |

29.4 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.

29.4.1 DHCPv4 Relay Agent Information

The Switch can add information about the source of client DHCP requests that it relays to a DHCP server by adding **Relay Agent Information**. This helps provide authentication about the source of the requests. The DHCP server can then provide an IP address based on this information. Please refer to RFC 3046 for more details.

The DHCP **Relay Agent Information** feature adds an Agent Information field (also known as the **Option 82** field) to DHCP requests. The **Option 82** field is in the DHCP headers of client DHCP request frames that the Switch relays to a DHCP server.

Relay Agent Information can include the **System Name** of the Switch if you select this option. You can change the **System Name** in **Basic Setting > General Setup**.

The following describes the DHCP relay agent information that the Switch sends to the DHCP server:

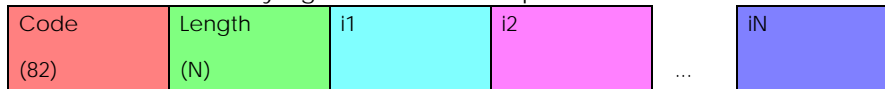
Table 113 Relay Agent Information

| 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 Setting > General Setup . |

29.4.1.1 DHCPv4 Relay Agent Information Format

A DHCP Relay Agent Information option has the following format.

Table 114 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.

29.4.1.2 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 115 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 116 DHCP Relay Agent Remote ID Sub-option Format

| SubOpt Code | Length | Value |
|---------------|---------------|-----------------------|
| 2 (1 byte) | N (1 byte) | MAC Address or String |

The 1 in the first field identifies this as an Agent Circuit ID sub-option and two identifies this as an Agent Remote ID sub-option. The next field specifies the length of the field.

29.4.2 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 163 IP Application > DHCP > DHCPv4 > Option 82 Profile

| Profile Name | Enable | Circuit-ID Field | Remote-ID Enable | Remote-ID Field | |
|--------------------------|--------|---------------------------|------------------|-----------------|--------------------------|
| default1 | Yes | slot-port, vlan | No | - | <input type="checkbox"/> |
| default2 | Yes | slot-port, vlan, hostname | No | - | <input type="checkbox"/> |

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

The following table describes the labels in this screen.

Table 117 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 single-byte printable characters. |
| Circuit-ID | Use this section to configure the Circuit ID sub-option to include information that is specific to the relay agent (the Switch). |
| Enable | Select this option to have the Switch add the Circuit ID sub-option to client DHCP requests that it relays to a DHCP server. |
| slot-port | Select this option to have the Switch add the number of port that the DHCP client is connected to. |
| vlan | Select this option to have the Switch add the ID of VLAN which the port belongs to. |
| hostname | This is the system name you configure in the 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 single-byte printable characters that the Switch adds into the client DHCP requests. |
| Remote-ID | Use this section to configure the Remote ID sub-option to include information that identifies the relay agent (the Switch). |
| Enable | Select this option to have the Switch append the Remote ID sub-option to the option 82 field of DHCP requests. |
| mac | Select this option to have the Switch add its MAC address to the client DHCP requests that it relays to a DHCP server. |
| string | Enter a string of up to 64 single-byte printable characters for the remote ID information in this field. |

Table 117 IP Application > DHCP > DHCPv4 > Option 82 Profile (continued)

| LABEL | DESCRIPTION |
|--------------|--|
| Add | Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to reset the fields to their last saved values. |
| Profile Name | This field displays the descriptive name of the profile. Click the name to change the settings. |
| Circuit-ID | This section displays the Circuit ID sub-option including information that is specific to the relay agent (the Switch). |
| Enable | This field displays whether the Circuit ID sub-option is added to client DHCP requests. |
| Field | This field displays the information that is included in the Circuit ID sub-option. |
| Remote-ID | This section displays the Remote ID sub-option including information that identifies the relay agent (the Switch). |
| Enable | This field displays whether the Remote ID sub-option is added to client DHCP requests. |
| Field | This field displays the information that is included in the Remote ID sub-option. |
| | Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries. |
| Delete | Check the entries that you want to remove and then click the Delete button. |
| Cancel | Click Cancel to clear the selected check boxes. |

29.4.3 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 164 IP Application > DHCP > DHCPv4 > Global

The following table describes the labels in this screen.

Table 118 IP Application > DHCP > DHCPv4 > Global

| LABEL | DESCRIPTION |
|---------------------------|--|
| Active | Select this check box to enable DHCPv4 relay. |
| Remote DHCP Server 1 .. 3 | Enter the IP address of a DHCPv4 server in dotted decimal notation. |
| Option 82 Profile | Select a pre-defined DHCPv4 option 82 profile that the Switch applies to all ports. The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server. |

Table 118 IP Application > DHCP > DHCPv4 > Global (continued)

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

29.4.4 Configure DHCPv4 Global Relay Port

Use this screen to apply a different DHCP option 82 profile to certain ports on the Switch. To open this screen, click **IP Application > DHCP > DHCPv4 > Global > Port**.

Figure 165 IP Application > DHCP > DHCPv4 > Global > Port

The following table describes the labels in this screen.

Table 119 IP Application > DHCP > DHCPv4 > Global > Port

| LABEL | DESCRIPTION |
|-------------------|---|
| Port | Enter the number of ports to which you want to apply the specified DHCP option 82 profile. You can enter multiple ports separated by (no space) comma (,) or hyphen (-). For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7. |
| Option 82 Profile | Select a pre-defined DHCP option 82 profile that the Switch applies to the specified ports. The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server. The profile you select here has priority over the one you select in the DHCP > DHCPv4 > Global screen. |
| Add | Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click this to reset the values above based on the last selected entry or, if not applicable, to clear the fields above. |
| Clear | Click Clear to reset the fields to the factory defaults. |
| Index | This field displays a sequential number for each entry. Click an index number to change the settings. |
| Port | This field displays the ports to which the Switch applies the settings. |
| Profile Name | This field displays the DHCP option 82 profile that the Switch applies to the ports. |
| | Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries. |

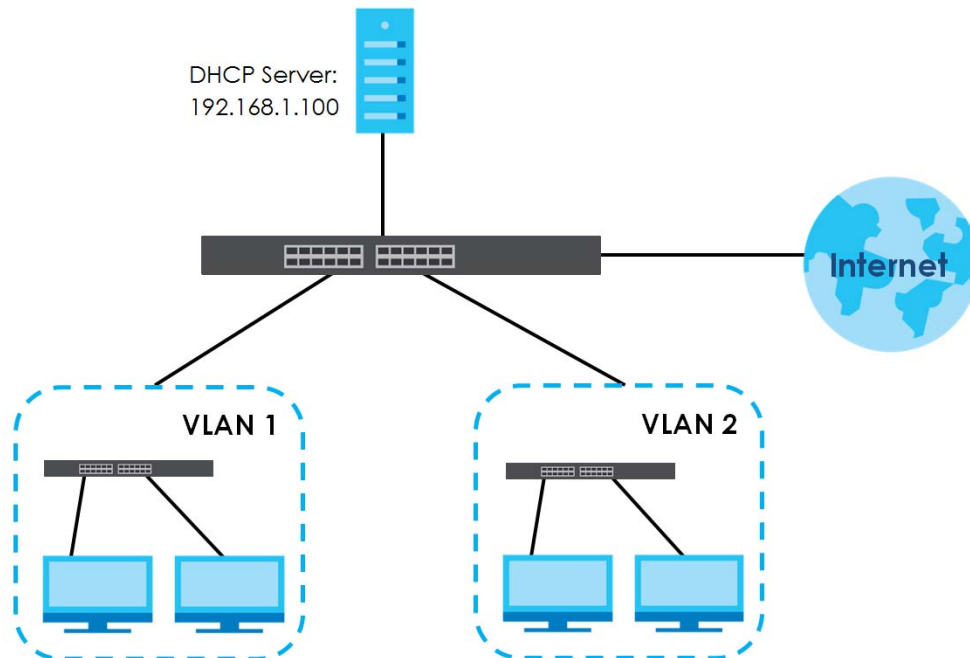
Table 119 IP Application > DHCP > DHCPv4 > Global > Port (continued)

| LABEL | DESCRIPTION |
|--------|--|
| Delete | Select the entries that you want to remove, then click the Delete button to remove the selected entries from the table. |
| Cancel | Click this to clear the check boxes above. |

29.4.5 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 166 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 167 DHCP Relay Configuration Example

| DHCP Relay | | Status | Port |
|----------------------|-------------------------------------|--------|------|
| Active | <input checked="" type="checkbox"/> | | |
| 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 | | |

EXAMPLE

Apply Cancel

29.4.6 DHCPv4 VLAN Setting

Use this screen to configure your DHCP settings based on the VLAN domain of the DHCP clients. Click **IP Application > DHCP > DHCPv4** in the navigation panel, then click the **VLAN** link in the **DHCP Status** screen that displays.

Note: You must set up a management IP address for each VLAN that you want to configure DHCP settings for on the Switch.

Figure 168 IP Application > DHCP > DHCPv4 > VLAN

The following table describes the labels in this screen.

Table 120 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. |
| Option 82 Profile | Select a pre-defined DHCP option 82 profile that the Switch applies to all ports in this VLAN. The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server. |
| Add | Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |
| Clear | Click Clear to reset the fields to the factory defaults. |
| VID | This field displays the ID number of the VLAN group to which this DHCP settings apply. |
| Type | This field displays Relay for the DHCP mode. |
| DHCP Status | For DHCP server configuration, this field displays the starting IP address and the size of the IP address pool. For DHCP relay configuration, this field displays the first remote DHCP server IP address. |
| | Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries. |

Table 120 IP Application > DHCP > DHCPv4 > VLAN (continued)

| LABEL | DESCRIPTION |
|--------|---|
| Delete | Select the configuration entries you want to remove and click Delete to remove them. |
| Cancel | Click Cancel to clear the check boxes. |

29.4.7 Configure DHCPv4 VLAN Port

Use this screen to apply a different DHCP option 82 profile to certain ports in a VLAN. To open this screen, click **IP Application > DHCP > DHCPv4 > VLAN > Port**.

Figure 169 IP Application > DHCP > DHCPv4 > VLAN > Port

The following table describes the labels in this screen.

Table 121 IP Application > DHCP > DHCPv4 > VLAN > Port

| LABEL | DESCRIPTION |
|-------------------|--|
| VID | Enter the ID number of the VLAN you want to configure here. |
| Port | Enter the number of ports to which you want to apply the specified DHCP option 82 profile. You can enter multiple ports separated by (no space) comma (,) or hyphen (-). For example, enter "3-5" for ports 3, 4, and 5. Enter "3,5,7" for ports 3, 5, and 7. |
| Option 82 Profile | Select a pre-defined DHCP option 82 profile that the Switch applies to the specified ports in this VLAN. The Switch adds the Circuit ID sub-option and/or Remote ID sub-option specified in the profile to DHCP requests that it relays to a DHCP server. The profile you select here has priority over the one you select in the DHCP > DHCPv4 > VLAN screen. |
| Add | Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click this to reset the values above based on the last selected entry or, if not applicable, to clear the fields above. |
| Clear | Click Clear to reset the fields to the factory defaults. |
| Index | This field displays a sequential number for each entry. Click an index number to change the settings. |
| VID | This field displays the VLAN to which the ports belongs. |
| Port | This field displays the ports to which the Switch applies the settings. |
| Profile Name | This field displays the DHCP option 82 profile that the Switch applies to the ports in this VLAN. |

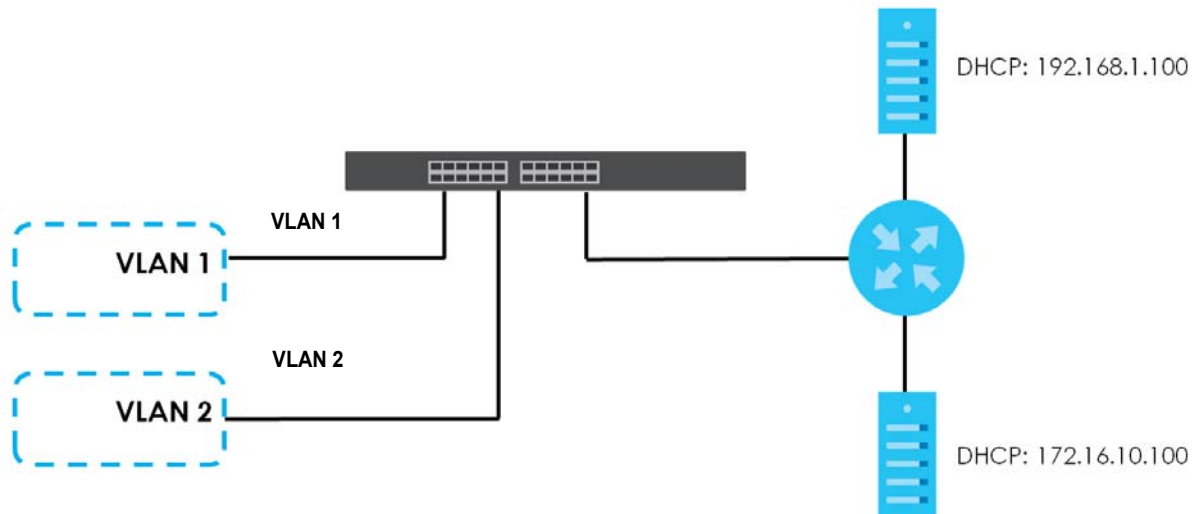
Table 121 IP Application > DHCP > DHCPv4 > VLAN > Port (continued)

| 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 entries that you want to remove, then click the Delete button to remove the selected entries from the table. |
| Cancel | Click this to clear the check boxes above. |

29.4.8 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 170 DHCP Relay for Two VLANs



For the example network, configure the **VLAN Setting** screen as shown.

Figure 171 DHCP Relay for Two VLANs Configuration Example

| VLAN Setting | | Status | Port |
|--|--------------------------------------|----------------------|--------------------------|
| VID | <input type="text"/> | | |
| Relay | <input type="text"/> | | |
| Remote DHCP Server 1 | <input type="text" value="0.0.0.0"/> | <input type="text"/> | |
| Remote DHCP Server 2 | <input type="text" value="0.0.0.0"/> | <input type="text"/> | |
| Remote DHCP Server 3 | <input type="text" value="0.0.0.0"/> | <input type="text"/> | |
| Option 82 Profile | <input type="text"/> | | |
| <input type="button" value="Add"/> <input type="button" value="Cancel"/> <input type="button" value="Clear"/> | | | |
| <div style="border: 2px solid red; border-radius: 15px; padding: 5px; display: inline-block; color: red; font-weight: bold; font-size: 1.2em;">EXAMPLE</div> | | | |
| VID | Type | DHCP Status | |
| 1 | Relay | 192.168.1.100 | <input type="checkbox"/> |
| <input type="button" value="Delete"/> <input type="button" value="Cancel"/> | | | |

29.5 DHCPv6 Relay

A DHCPv6 relay agent is on the same network as the DHCPv6 clients and helps forward messages between the DHCPv6 server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCPv6 server on its network, it then needs a DHCPv6 relay agent to send a message to a DHCPv6 server that is not attached to the same network.

The DHCPv6 relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCPv6 server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Use this screen to configure DHCPv6 relay settings for a specific VLAN on the Switch. Click **IP Application > DHCP > DHCPv6 > DHCPv6 Relay** in the navigation panel to display the screen as shown.

Figure 172 IP Application > DHCP > DHCPv6 Relay

| VID | Helper Address | Interface ID | Remote ID | |
|-----|----------------|--------------|-----------|--------------------------|
| 100 | 1888::200 | disable | disable | <input type="checkbox"/> |

The following table describes the labels in this screen.

Table 122 IP Application > DHCP > DHCPv6 Relay

| 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 string should not contain [?], [], ['], or ["]. The Switch adds the remote-ID option in the DHCPv6 requests from the clients in the specified VLAN before the Switch forwards them to a DHCPv6 server. |
| Add | Click this to create a new entry or to update an existing one. This saves your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to reset the fields to their last saved values. |
| Clear | Click Clear to reset the fields to the factory defaults. |
| VID | This field displays the VLAN ID number. Click the VLAN ID to change the settings. |
| Helper Address | This field displays the IPv6 address of the remote DHCPv6 server for this VLAN. |
| Interface ID | This field displays whether the interface-ID option is added to DHCPv6 requests from clients in this VLAN. |
| Remote ID | This field displays whether the remote-ID option is added to DHCPv6 requests from clients in this VLAN. |
| | Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries. |
| Delete | Check the entries that you want to remove and then click the Delete button. |
| Cancel | Click Cancel to clear the selected check boxes. |

30.1 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.

30.1.1 What You Can Do

Use the **ARP Learning** screen ([Section 30.2.1 on page 244](#)) to configure ARP learning mode on a per-port basis.

30.1.2 What You Need to Know

Read on for concepts on ARP that can help you configure the screen in this chapter.

30.1.2.1 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.

30.1.2.2 ARP Learning Mode

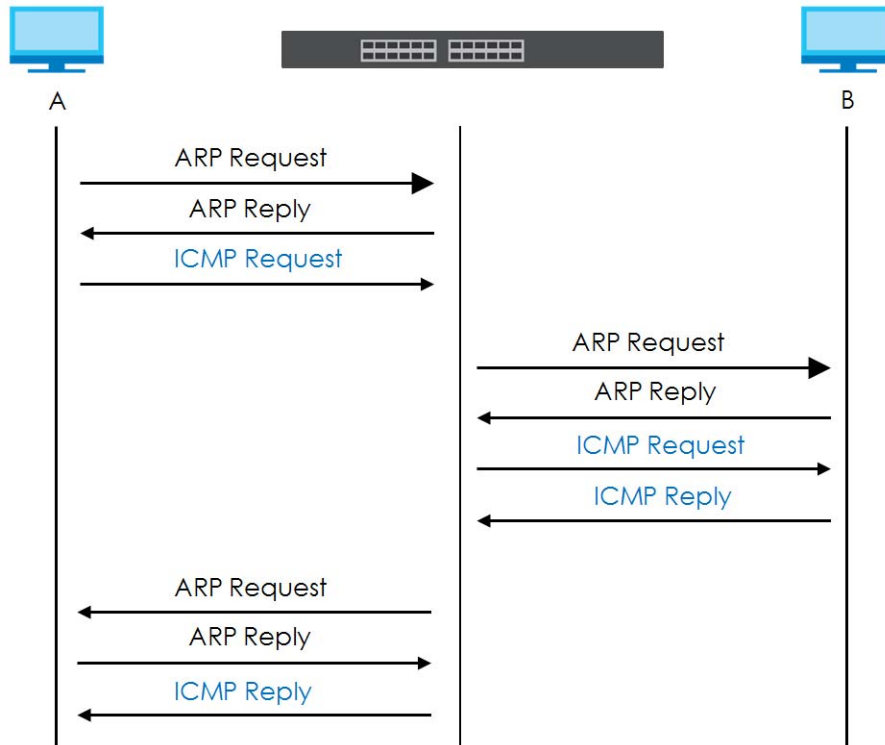
The Switch supports three ARP learning modes: ARP-Reply, Gratuitous-ARP, and ARP-Request.

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.

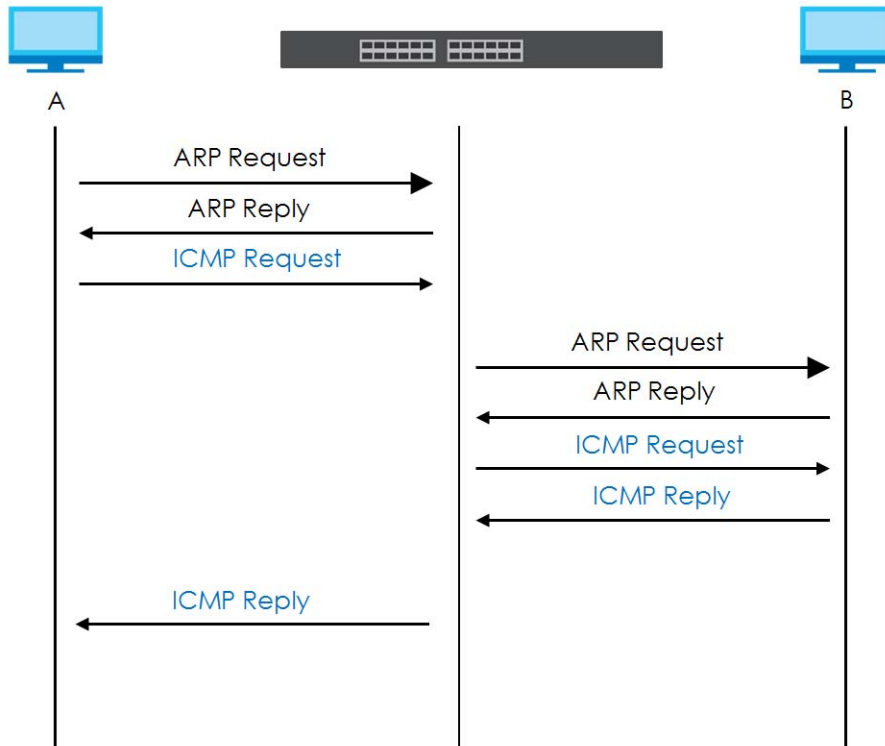
A device may send a gratuitous ARP packet to detect IP collisions. If a device restarts or its MAC address is changed, it can also use gratuitous ARP to inform other devices in the same network to update their ARP table with the new mapping information.

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.

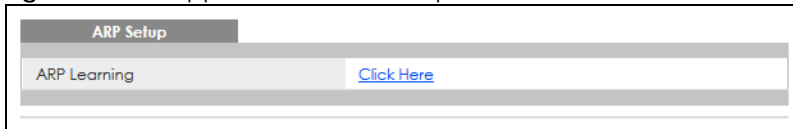
Therefore in the following example, the Switch can learn host **A**'s MAC address from the ARP request sent by host **A**. The Switch then forwards host **B**'s ICMP reply to host **A** right after getting host **B**'s MAC address and ICMP reply.



30.2 ARP Setup

Click **IP Application** > **ARP Setup** in the navigation panel to display the screen as shown. Click the link next to **ARP Learning** to open a screen where you can set the ARP learning mode for each port.

Figure 173 IP Application > ARP Setup



30.2.1 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 174 IP Application > ARP Setup > ARP Learning

| ARP Learning | | ARP Setup |
|--------------|-------------------|---------------------------|
| 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 | ▼ |

The following table describes the labels in this screen.

Table 123 IP Application > ARP Setup > ARP Learning

| LABEL | DESCRIPTION |
|-------------------|--|
| Port | This field displays the port number. |
| * | Settings in this row apply to all ports. Use this row only if you want to make some settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them. |
| ARP Learning Mode | Select the ARP learning mode the Switch uses on the port. Select ARP-Reply to have the Switch update the ARP table only with the ARP replies to the ARP requests sent by the Switch. Select Gratuitous-ARP to have the Switch update its ARP table with either an ARP reply or a gratuitous ARP request. Select ARP-Request to have the Switch update the ARP table with both ARP replies, gratuitous ARP requests and ARP requests. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

CHAPTER 31

Maintenance

31.1 Overview

This chapter explains how to configure the screens that let you maintain the firmware and configuration files.

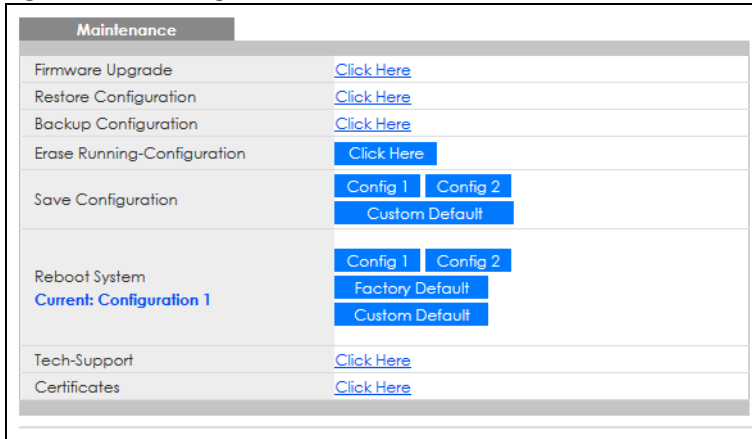
31.1.1 What You Can Do

- Use the **Maintenance** screen ([Section 31.2 on page 246](#)) to manage firmware and your configuration files.
- Use the **Firmware Upgrade** screen ([Section 31.3 on page 250](#)) to upload the latest firmware.
- Use the **Restore Configuration** screen ([Section 31.4 on page 251](#)) to upload a stored device configuration file.
- Use the **Backup Configuration** screen ([Section 31.5 on page 252](#)) to save your configurations for later use.
- Use the **Erase Running-Configuration** screen ([Section 31.2.1 on page 248](#)) to reset the configuration to the Zyxel default configuration settings.
- Use the **Save Configuration** screen ([Section 31.2.2 on page 248](#)) to save the current configuration settings to a specific configuration file on the Switch.
- Use the **Reboot System** screen ([Section 31.2.3 on page 248](#)) to restart the Switch without physically turning the power off and load a specific configuration file.
- Use the **Tech-Support** screen ([Section 31.6 on page 252](#)) to create reports for customer support if there are problems with the Switch.
- Use the **Certificates** screen ([Section 31.7 on page 254](#)) to see the **Certificate** screen and import the Switch's CA-signed certificates.

31.2 Maintenance Settings

Use this screen to manage firmware and your configuration files. Click **Management > Maintenance** in the navigation panel to open the following screen.

Figure 175 Management > Maintenance



The following table describes the labels in this screen.

Table 124 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 configuration to the Zyxel default configuration settings. 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 customized default file on the Switch. This file can be used instead of the Zyxel factory default configuration file. |
| Reboot System | Click Config 1 to reboot the Switch and load Configuration 1 on the Switch. Click Config 2 to reboot the Switch and load Configuration 2 on the Switch. Click Factory Default to reboot the Switch and load the Zyxel factory default configuration settings on the Switch. Click Custom Default to reboot the system and load a saved Custom Default configuration file on the Switch. This will save the custom default configuration settings to both Config 1 and Config 2 . If a Custom Default configuration 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 Certificate screen and import the Switch's CA-signed certificates. |

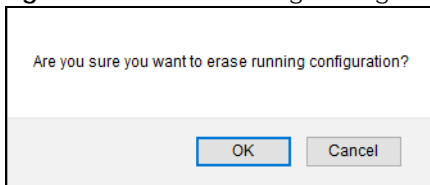
31.2.1 Erase Running-Configuration

Follow the steps below to reset the Switch back to the Zyxel default configuration settings.

Follow the steps below to remove the running configuration on the Switch. Unlike when you reset the Switch to the factory defaults, the user name, password, system logs, memory logs, baud rate and SSH service are not removed.

- 1 In the **Maintenance** screen, click the **Click Here** button next to **Erase Running-Configuration** to clear all Switch configuration information you configured and return to the Zyxel default configuration settings.
- 2 Click **OK** to reset all Switch configurations to the Zyxel default configuration settings.

Figure 176 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).

31.2.2 Save Configuration

Click **Config 1** to save the current configuration settings permanently to **Configuration 1** on the Switch. These configurations are set up according to your network environment.

Click **Config 2** to save the current configuration settings permanently to **Configuration 2** on the Switch. These configurations are set up according to your network environment.

Click **Custom Default** to save the current configuration settings permanently to a customized default file on the Switch. If configuration changes cause the Switch to behave abnormally, click **Custom Default** (next to **Reboot System**) to have the Switch automatically reboot and restore the saved **Custom Default** configuration file.

Note: If a customized default file was not saved, clicking **Custom Default** loads the factory default configuration on the Switch.

Alternatively, click **Save** on the top right 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.

31.2.3 Reboot System

Reboot System allows you to restart the Switch without physically turning the power off. It also allows you to load configuration one (**Config 1**), configuration two (**Config 2**), a **Custom Default** or the **Factory Default** configuration when you reboot. Follow the steps below to reboot the Switch.

- 1 In the **Maintenance** screen, click a configuration button next to **Reboot System** to reboot and load that configuration file. The confirmation screen displays.
- 2 Click **OK** again and then wait for the Switch to restart. This takes up to 2 minutes. This does not affect the Switch's configuration.

Click **Config 1** and follow steps 1 to 2 to reboot and load configuration one on the Switch.

Click **Config 2** and follow steps 1 to 2 to reboot and load configuration two on the Switch.

Click **Factory Default** and follow steps 1 to 2 to reboot and load Zyxel factory default configuration settings on the Switch.

Click **Custom Default** and follow steps 1 to 2 to reboot and load a customized default file on the Switch. This will save the custom default configuration settings to both **Configuration 1** and **Configuration 2**.

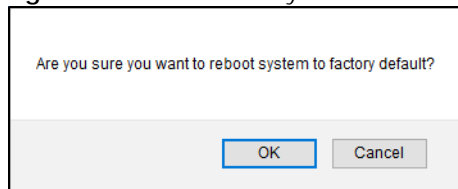
Note: If a customized default file was not saved, clicking **Custom Default** loads the factory default configuration on the Switch.

31.2.4 Factory Default

Follow the steps below to reset the Switch back to the factory defaults.

- 1 Click the **Factory Default** button.
- 2 Click **OK** to continue or **Cancel** to abort.

Figure 177 Load Factory Default: Confirmation



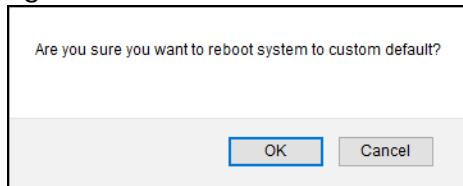
If you want to access the Switch Web Configurator again, you may need to change the IP address of your computer to be in the same subnet as that of the default Switch IP address (192.168.1.1 or DHCP-assigned IP).

31.2.5 Custom Default

Follow the steps below to reset the Switch back to the **Custom Default** configuration file you created. This will save the custom default configuration settings to both **Configuration 1** and **Configuration 2**.

- 1 Click the **Custom Default** button.
- 2 Click **OK** to continue or **Cancel** to abort.

Note: If you did not save a custom default file in the Web Configurator, then the factory default file is restored after you press click **Custom Default** (next to **Reboot System**) on the Switch. You will then have to make all your configurations again on the Switch.

Figure 178 Load Custom Default: Confirmation

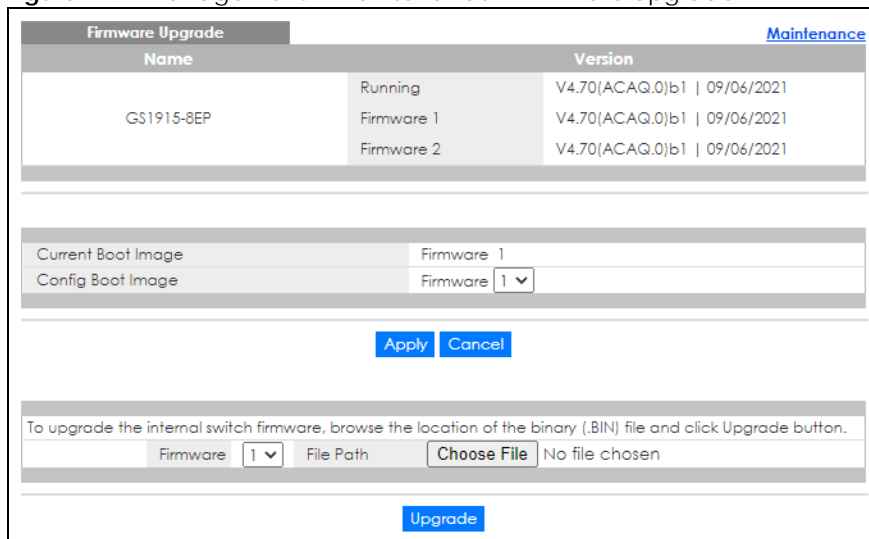
31.3 Firmware Upgrade

Use the following screen to upgrade your Switch to the latest firmware. The Switch supports dual firmware images, **Firmware 1** and **Firmware 2**. Use this screen to specify which image is updated when firmware is uploaded using the Web Configurator and to specify which image is loaded when the Switch starts up.

Make sure you have downloaded (and unzipped) the correct model firmware and version to your computer before uploading to the device.

Be sure to upload the correct model firmware as uploading the wrong model firmware may damage your device.

Click **Management > Maintenance > Firmware Upgrade** to view the screen as shown next.

Figure 179 Management > Maintenance > Firmware Upgrade

The top of firmware upgrade screen shows which firmware version is currently running on the Switch. Enter the path and file name of the firmware file you wish to upload to the Switch in the **File Path** text box or click **Choose File** or **Browse** to locate it. Firmware upgrades are only applied after a reboot. Click **Upgrade** to load the new firmware. Select the **Config Boot Image** drop-down list box if you want to reboot the Switch and click **Apply** to apply the new firmware immediately. Click **Upgrade** to load the new firmware.

After the process is complete, see the **System Info** screen to verify your current firmware version number.

Table 125 Management > Maintenance > Firmware Upgrade

| LABEL | DESCRIPTION |
|--------------------|--|
| Name | This is the name of the Switch that you are configuring. |
| Version | The Switch has 2 firmware sets, Firmware 1 and Firmware 2 , residing in flash. <ul style="list-style-type: none"> Running shows the version number (and model code) and MM/DD/YYYY creation date of the firmware currently in use on the Switch (Firmware 1 or Firmware 2). The firmware information is also displayed at System Information in Basic Setting. Firmware 1 shows its version number (and model code) and MM/DD/YYYY creation date. Firmware 2 shows its version number (and model code) and MM/DD/YYYY creation date. |
| Current Boot Image | This displays which firmware is currently in use on the Switch (Firmware 1 or Firmware 2). |
| Config Boot Image | Select which firmware (Firmware 1 or Firmware 2) should load, click Apply and reboot the Switch to see changes, you will also see changes in the Current Boot Image field above as well. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |
| Firmware | Choose to upload the new firmware to (Firmware) 1 or (Firmware) 2 . |
| File Path | Type the path and file name of the firmware file you wish to upload to the Switch in the File Path text box or click Choose File or Browse to locate it. |
| Upgrade | Click Upgrade to load the new firmware. s are only applied after a reboot. To reboot, go to Management > Maintenance > Reboot System and click Config 1 , Config 2 or Factory Default (Config 1 , Config 2 and Factory Default are the configuration files you want the Switch to use when it restarts). |

31.4 Restore Configuration

Use this screen to restore a previously saved configuration from your computer to the Switch.

Figure 180 Management > Maintenance > Restore Configuration

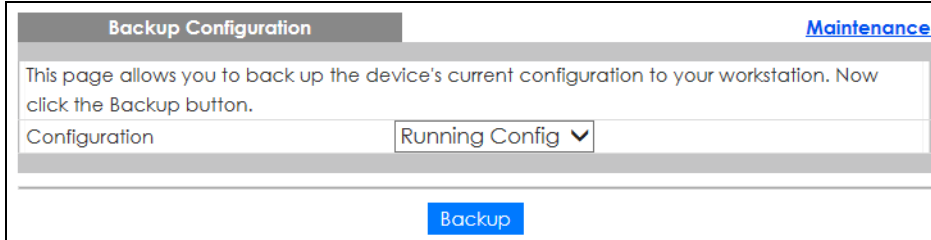
Enter the path and file name of the configuration file you wish to restore in the **File Path** text box or click **Choose File** or **Browse** to locate it. After you have specified the file, click **Restore**. "config" is the name of the configuration file on the Switch, so your backup configuration file is automatically renamed when you restore using this screen.

31.5 Backup Configuration

Backing up your Switch configurations allows you to create various “snap shots” of your device from which you may restore at a later date.

Back up your current Switch configuration to a computer using the **Backup Configuration** screen.

Figure 181 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.

31.6 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 182 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 | | |

You may need WordPad or similar software to see the log report correctly. The table below describes the fields in the above screen.

Table 126 Management > Maintenance > Tech-Support

| LABEL | DESCRIPTION |
|----------------|---|
| CPU | <p>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.</p> <p>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.</p> <p>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.</p> <p>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.</p> |
| Mbuf | <p>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.</p> <p>For example, Mbuf 50 means a log will be created when the Mbuf utilization is over 50%.</p> <p>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.</p> |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |
| All | Click Download to see all the log report and system status. This log report is stored in flash memory. If the All log report is too large, you can download the log reports separately below. |
| Crash | Click Download to see the crash log report. The log will include information of the last crash and is stored in flash memory. |
| CPU history | Click Download to see the CPU history log report. The 7-days log is stored in RAM and you will need to save it, otherwise it will be lost when the Switch is shutdown or during power outage. |
| Memory section | Click Download to see the memory section log report. This log report is stored in flash memory. |

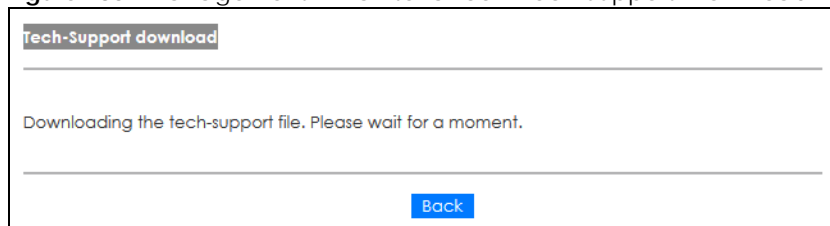
Table 126 Management > Maintenance > Tech-Support (continued)

| LABEL | DESCRIPTION |
|-------|--|
| Mbuf | Click Download to see the Mbuf log report. The log includes Mbuf over threshold information. This log report is stored in flash memory. |
| ROM | Click Download to see the Read Only Memory (ROM) log report. This report is stored in flash memory. |

31.6.1 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 183 Management > Maintenance > Tech-Support: Download



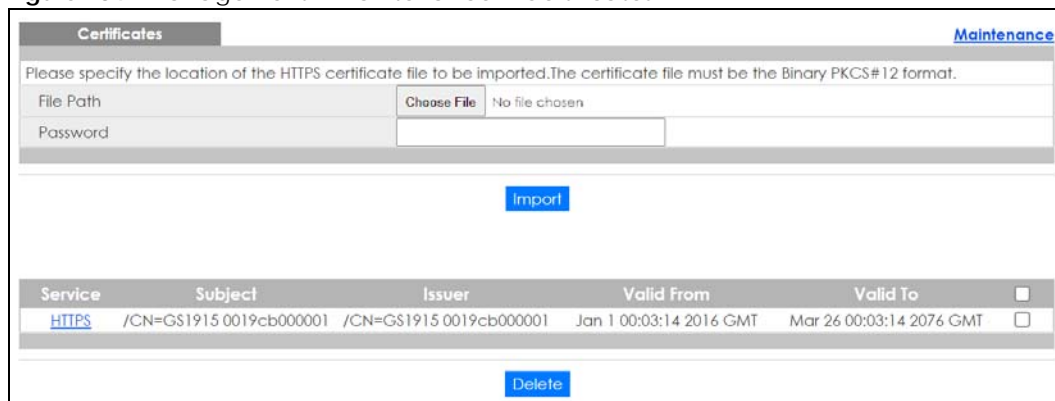
31.7 Certificates

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 32.8.3 on page 275](#) 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 184 Management > Maintenance > Certificates



The following table describes the labels in this screen.

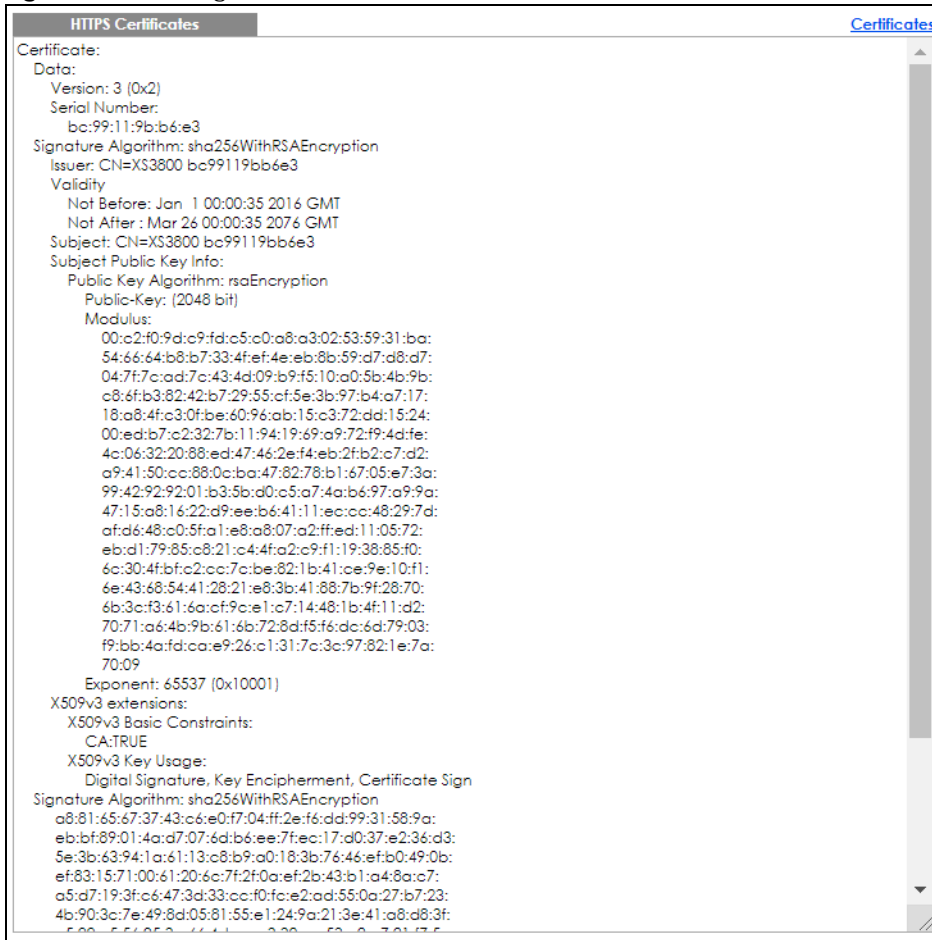
Table 127 Management > Maintenance > Certificates

| LABEL | DESCRIPTION |
|------------|--|
| File Path | Click Choose File or Browse to find the certificate file you want to upload. |
| Password | Enter the certificate file's password that was created when the PKCS #12 file was exported. The password consists of up to 32 single-byte printable characters. |
| Import | Click this button to save the certificate that you have enrolled from a certification authority from your computer to the Switch. |
| Service | This field displays the service type that this certificate is for. |
| Subject | This field displays identifying information about the certificate's owner, such as CN (Common Name), OU (Organizational Unit or department), O (Organization or company) and C (Country). It is recommended that each certificate have unique subject information. |
| Issuer | This field displays identifying information about the certificate's issuing certification authority, such as a common name, organizational unit or department, organization or company and country. |
| Valid From | This field displays the date that the certificate becomes applicable. |
| Valid To | This field displays the date that the certificate expires. |
| | Select an entry's check box to select a specific entry. |
| Delete | Click this button to delete the certificate (or certification request). You cannot delete a certificate that one or more features is configured to use. |

31.7.1 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 185 Management > Maintenance > Certificates > HTTPS



31.8 Technical Reference

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

31.8.1 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.

31.8.2 Filename Conventions

The configuration file (also known as the romfile or ROM) contains the Zyxel factory default configuration settings in the screens such as password, Switch setup, IP Setup, and so on. Once you have customized the Switch's settings, they can be saved back to your computer under a filename of your choosing.

ZyNOS (Zyxel Network Operating System sometimes referred to as the "ras" file) is the system firmware

and has a "bin" filename extension.

Table 128 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. |

31.8.2.1 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.

31.8.3 FTP Command Line Procedure

- 1 Launch the FTP client on your computer.
- 2 Enter `open`, followed by a space and the IP address of your Switch.
- 3 Press [ENTER] when prompted for a user name.
- 4 Enter your password as requested (the default is "1234").
- 5 Enter `bin` to set transfer mode to binary.
- 6 Use `put` to transfer files from the computer to the Switch, for example, `put firmware.bin ras` transfers the firmware on your computer (firmware.bin) to the Switch and renames it to "ras". Similarly, `put config.cfg config` transfers the configuration file on your computer (config.cfg) to the Switch and renames it to "config". Likewise `get config config.cfg` transfers the configuration file on the Switch to your computer and renames it to "config.cfg". See [Table 128 on page 257](#) for more information on filename conventions.
- 7 Enter `quit` to exit the ftp prompt.

31.8.4 GUI-based FTP Clients

The following table describes some of the commands that you may see in GUI-based FTP clients.

Table 129 General Commands for GUI-based FTP Clients

| COMMAND | DESCRIPTION |
|--------------------------|--|
| Host Address | Enter the address of the host server. |
| Login Type | <p>Anonymous.</p> <p>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.</p> <p>Normal.</p> <p>The server requires a unique User ID and Password to login.</p> |
| Transfer Type | Transfer files in either single-byte printable characters (plain text format) or in binary mode. Configuration and firmware files should be transferred in binary mode. |
| Initial Remote Directory | Specify the default remote directory (path). |
| Initial Local Directory | Specify the default local directory (path). |

31.8.5 FTP Restrictions

FTP will not work when:

- FTP service is disabled in the **Management > Access Control > Service Access Control** screen.
- The IP addresses in the **Management > Access Control > Remote Management** screen does not match the client IP address. If it does not match, the Switch will disconnect the FTP session immediately.

CHAPTER 32

Access Control

32.1 Access Control Overview

This chapter describes how to control access to the Switch.

A console port and FTP are allowed one session each, Telnet and SSH share nine sessions, up to five web sessions (five different user names and passwords) and/or limitless SNMP access control sessions are allowed.

Table 130 Access Control Overview

| Console Port | SSH | Telnet | FTP | Web | SNMP |
|--------------|------------------------|--------|-------------|------------------|----------|
| One session | Share up to 9 sessions | | One session | Up to 5 accounts | No limit |

A console port access control session and Telnet access control session cannot coexist when multi-login is disabled.

32.1.1 What You Can Do

- Use the **Access Control** screen ([Section 32.2 on page 259](#)) to display the main screen.
- Use the **SNMP** screen ([Section 32.3 on page 260](#)) to configure your SNMP settings.
- Use the **Trap Group** screen ([Section 32.3.1 on page 261](#)) to specify the types of SNMP traps that should be sent to each SNMP manager.
- Use the **User Information** screen ([Section 32.3.3 on page 263](#)) to create SNMP users for authentication with managers using SNMP v3 and associate them to SNMP groups.
- Use the **Logins** screens ([Section 32.4 on page 265](#)) to assign which users can access the Switch through Web Configurator at any one time.
- Use the **Service Access Control** screen ([Section 32.5 on page 266](#)) to decide what services you may use to access the Switch.
- Use the **Remote Management** screen ([Section 32.6 on page 267](#)) to specify a group of one or more "trusted computers" from which an administrator may use a service to manage the Switch.
- Use the **Account Security** screen ([Section 32.7 on page 268](#)) to encrypt all passwords configured in the Switch. You can also display the authentication, authorization, external authentication server information (RADIUS), system and SNMP user account information in the configuration file saved.

32.2 Access Control Main Settings

Use this screen to display the main screen.

Click **Management > Access Control** in the navigation panel to display the main screen as shown.

Figure 186 Management > Access Control

| Access Control | |
|------------------------|----------------------------|
| SNMP | Click Here |
| Logins | Click Here |
| Service Access Control | Click Here |
| Remote Management | Click Here |
| Account Security | Click Here |

The following table describes the labels in this screen.

Table 131 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 through 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. |
| Account Security | Click this link to encrypt all passwords configured in the Switch. You can also display the authentication, authorization, external authentication server information (RADIUS), system and SNMP user account information in the configuration file saved. |

32.3 Configure SNMP

Use this screen to configure your SNMP settings.

Click **Management > Access Control > SNMP** to view the screen as shown.

Figure 187 Management > Access Control > SNMP

| SNMP | | Access Control | Trap Group | User |
|--|---------------|--------------------------------|----------------------------|----------------------|
| General Setting | | | | |
| Version | v2c | | | |
| Get Community | public | | | |
| Set Community | private | | | |
| Trap Community | public123 | | | |
| Trap Destination | | | | |
| Version | IP | Port | Username | |
| v2c | 192.168.1.223 | 162 | | |
| v2c | 0.0.0.0 | 162 | | |
| v2c | 0.0.0.0 | 162 | | |
| v2c | 0.0.0.0 | 162 | | |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | | | | |

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

The following table describes the labels in this screen.

Table 132 Management > Access Control > SNMP

| LABEL | DESCRIPTION |
|------------------|--|
| General Setting | Use this section to specify the SNMP version and community (password) values. |
| Version | Select the SNMP version for the Switch. The SNMP version on the Switch must match the version on the SNMP manager. Choose SNMP version 2c (v2c), SNMP version 3 (v3) or both (v3v2c). SNMP version 2c is backwards compatible with SNMP version 1. |
| Get Community | Enter the Get Community string, which is the password for the incoming Get- and GetNext-requests from the management station. The Get Community string is only used by SNMP managers using SNMP version 2c or lower. |
| Set Community | Enter the Set Community string, which is the password for incoming Set- requests from the management station. The Set Community string is only used by SNMP managers using SNMP version 2c or lower. |
| Trap Community | Enter the Trap Community string, which is the password sent with each trap to the SNMP manager. The Trap Community string is only used by SNMP managers using SNMP version 2c or lower. |
| Trap Destination | Use this section to configure where to send SNMP traps from the Switch. |
| Version | Specify the version of the SNMP trap messages. |
| IP | Enter the IP addresses of up to four managers to send your SNMP traps to. |
| Port | Enter the port number upon which the manager listens for SNMP traps. |
| Username | Enter the user name to be sent to the SNMP manager along with the SNMP v3 trap. The string should not contain [?], [], ['], ["], [,], [:], or space. This user name must match an existing account on the Switch (configured in the Management > Access Control > SNMP > User screen). |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

32.3.1 Configure SNMP Trap Group

From the **SNMP** screen, click **Trap Group** to view the screen as shown. Use the **Trap Group** screen to specify the types of SNMP traps that should be sent to each SNMP manager.

Figure 188 Management > Access Control > SNMP > Trap Group

The screenshot shows the 'Trap Group' configuration interface. At the top, there is a 'Trap Destination IP' dropdown menu. Below this is a table with two columns: 'Type' and 'Options'. The 'Type' column lists various system components: System, Interface, AAA, IP, and Switch. The 'Options' column lists specific trap types: coldstart, linkup, authentication, ping, stp, warmstart, linkdown, traceroute, poe, and lldp. Each option is accompanied by a checkbox. At the bottom of the screen, there are two buttons: 'Apply' and 'Cancel'.

The following table describes the labels in this screen.

Table 133 Management > Access Control > SNMP > Trap Group

| LABEL | DESCRIPTION |
|---------------------|--|
| Trap Destination IP | Select one of your configured trap destination IP addresses. These are the IP addresses of the SNMP managers. You must first configure a trap destination IP address in the SNMP Setting screen. Use the rest of the screen to select which traps the Switch sends to that SNMP manager. |
| Type | Select the categories of SNMP traps that the Switch is to send to the SNMP manager. |
| Options | Select the individual SNMP traps that the Switch is to send to the SNMP station. The traps are grouped by category. Selecting a category automatically selects all of the category's traps. Clear the check boxes for individual traps that you do not want the Switch to send to the SNMP station. Clearing a category's check box automatically clears all of the category's trap check boxes (the Switch only sends traps from selected categories). |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

32.3.2 Enable or Disable Sending of SNMP Traps on a Port

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

Figure 189 Management > Access Control > SNMP > Trap Group > Port

| Port | Active |
|------|-------------------------------------|
| * | <input type="checkbox"/> |
| 1 | <input checked="" type="checkbox"/> |
| 2 | <input checked="" type="checkbox"/> |
| 3 | <input checked="" type="checkbox"/> |
| 4 | <input checked="" type="checkbox"/> |
| 5 | <input checked="" type="checkbox"/> |
| 6 | <input checked="" type="checkbox"/> |
| 7 | <input checked="" type="checkbox"/> |
| 8 | <input checked="" type="checkbox"/> |

The following table describes the labels in this screen.

Table 134 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. |

Table 134 Management > Access Control > SNMP > Trap Group > Port (continued)

| LABEL | DESCRIPTION |
|--------|--|
| * | Settings in this row apply to all ports. Use this row only if you want to make some of the settings the same for all ports. Use this row first to set the common settings and then make adjustments on a port-by-port basis. Changes in this row are copied to all the ports as soon as you make them. |
| Active | Select this check box to enable the trap type of SNMP traps on this port. The Switch sends the related traps received on this port to the SNMP manager. Clear this check box to disable the sending of SNMP traps on this port. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

32.3.3 Configure SNMP User

From the **SNMP** screen, click **User** to view the screen as shown. Use the **User** screen to create SNMP users for authentication with managers using SNMP v3 and associate them to SNMP groups. An SNMP user is an SNMP manager.

Figure 190 Management > Access Control > SNMP > User

The following table describes the labels in this screen.

Table 135 Management > Access Control > SNMP > User

| LABEL | DESCRIPTION |
|------------------|---|
| User Information | Note: Use the user name and password of the login accounts you specify in this screen to create accounts on the SNMP v3 manager. |
| Username | Specify the user name of a login account on the Switch. The string should not contain [?], [], ['], ["], [.], [:], or space. |

Table 135 Management > Access Control > SNMP > User (continued)

| LABEL | DESCRIPTION |
|----------------|---|
| Security Level | <p>Select whether you want to implement authentication and/or encryption for SNMP communication from this user. Choose:</p> <ul style="list-style-type: none"> noauth – to use the user name as the password string to send to the SNMP manager. This is equivalent to the Get, Set and Trap Community in SNMP v2c. This is the lowest security level. auth – to implement an authentication algorithm for SNMP messages sent by this user. priv – to implement authentication and encryption for SNMP messages sent by this user. This is the highest security level. <p>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.</p> |
| 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 single-byte printable characters (except [?], [], ['], ["] or [,]) for SNMP user authentication. |
| Privacy | Specify the encryption method for SNMP communication from this user. You can choose one of the following: <ul style="list-style-type: none"> 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 single-byte printable characters (except [?], [], ['], ["] or [,]) for encrypting SNMP packets. |
| Group | <p>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.</p> <p>admin – Members of this group can perform all types of system configuration, including the management of administrator accounts.</p> <p>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.</p> <p>readonly – Members of this group have read rights only, meaning the user can collect information from the Switch.</p> |
| Add | <p>Click this to create a new entry or to update an existing one.</p> <p>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.</p> |
| 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 user name of a login account on the Switch. |
| Security Level | This field displays whether you want to implement authentication and/or encryption for SNMP communication with this user. |
| Authentication | This field displays the authentication algorithm used for SNMP communication with this user. |
| Privacy | This field displays the encryption method used for SNMP communication with this user. |
| Group | This field displays the SNMP group to which this user belongs. |
| | Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries. |

Table 135 Management > Access Control > SNMP > User (continued)

| LABEL | DESCRIPTION |
|--------|--|
| Delete | Click Delete to remove the selected entry from the summary table. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

32.4 Set Up Login Accounts

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

- An administrator is someone who can both view and configure Switch changes. The user name 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 (user name is something other than **admin**) is someone who can view and/or configure Switch settings. The configuration right varies depending on the user's privilege level.

Click **Management > Access Control > Logins** to view the screen as shown.

Figure 191 Management > Access Control > Logins

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

The following table describes the labels in this screen.

Table 136 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. |

Table 136 Management > Access Control > Logins (continued)

| LABEL | DESCRIPTION |
|-------------------|---|
| Retype to confirm | Retype your new system password for confirmation. |
| User Name | Set a user name (up to 32 single-byte printable characters long). The string should not contain [?], [], ['], ["], [.], [:], or space. |
| Password | Enter your new system password. |
| Retype to confirm | Retype your new system password for confirmation. |
| Privilege | <p>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.</p> <ul style="list-style-type: none"> 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. <p>Users can run command lines if the session's privilege level is greater than or equal to the command's privilege level. The session privilege initially comes from the privilege of the login account. For example, if the user has a privilege of 5, he or she can run commands that requires privilege level of 5 or less but not more.</p> |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

32.5 Service Access Control

Service Access Control allows you to decide what services you may use to access the Switch. You may also change the default service port and configure "trusted computers" for each service in the **Remote Management** screen (discussed later). Click **Access Control** to go back to the main **Access Control** screen.

Figure 192 Management > Access Control > Service Access Control

| Service Access Control | | | | Access Control | |
|------------------------|-------------------------------------|--------------|---------|--------------------------------|---------------|
| Services | Active | Service Port | Timeout | | Login Timeout |
| Telnet | <input checked="" type="checkbox"/> | 23 | 5 | Minutes | 150 Seconds |
| SSH | <input checked="" type="checkbox"/> | 22 | | | |
| FTP | <input checked="" type="checkbox"/> | 21 | 5 | Minutes | |
| HTTP | <input checked="" type="checkbox"/> | 80 | 55 | Minutes | |
| HTTPS | <input checked="" type="checkbox"/> | 443 | | | |
| ICMP | <input checked="" type="checkbox"/> | | | | |
| SNMP | <input checked="" type="checkbox"/> | | | | |

The following table describes the fields in this screen.

Table 137 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 | Enter how many minutes (from 1 to 255) a management session can be left idle before the session times out. After it times out you have to log in with your password again. Very long idle timeouts may have security risks. |
| Login Timeout | The Telnet or SSH server do not allow multiple user logins at the same time. Enter how many seconds (from 30 to 300 seconds) a login session times out. After it times out you have to start the login session again. Very long login session timeouts may have security risks. For example, if User A attempts to connect to the Switch (through SSH), but during the login stage, do not enter the user name and/or password, User B cannot connect to the Switch (through SSH) before the Login Timeout for User A expires (default 150 seconds). |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

32.6 Remote Management

Use this screen to specify a group of one or more "trusted computers" from which an administrator may use a service to manage the Switch.

Click **Management > Access Control > Remote Management** to view the screen as shown next.

Click **Access Control** to return to the **Access Control** screen.

Figure 193 Management > Access Control > Remote Management

| Remote Management | | | | Access Control | | | | | | | |
|----------------------|-------------------------------------|---------------|-------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|-------------------------------------|--|
| Secured Client Setup | | | | | | | | | | | |
| Entry | Active | Start Address | End Address | Telnet | FTP | HTTP | ICMP | SNMP | SSH | HTTPS | |
| 1 | <input checked="" type="checkbox"/> | 0.0.0.0 | 0.0.0.0 | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | <input checked="" type="checkbox"/> | |
| 2 | <input type="checkbox"/> | 0.0.0.0 | 0.0.0.0 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| 3 | <input type="checkbox"/> | 0.0.0.0 | 0.0.0.0 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| 4 | <input type="checkbox"/> | 0.0.0.0 | 0.0.0.0 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| 5 | <input type="checkbox"/> | 0.0.0.0 | 0.0.0.0 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| 6 | <input type="checkbox"/> | 0.0.0.0 | 0.0.0.0 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| 7 | <input type="checkbox"/> | 0.0.0.0 | 0.0.0.0 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| 8 | <input type="checkbox"/> | 0.0.0.0 | 0.0.0.0 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| 9 | <input type="checkbox"/> | 0.0.0.0 | 0.0.0.0 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| 10 | <input type="checkbox"/> | 0.0.0.0 | 0.0.0.0 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| 11 | <input type="checkbox"/> | 0.0.0.0 | 0.0.0.0 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| 12 | <input type="checkbox"/> | 0.0.0.0 | 0.0.0.0 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| 13 | <input type="checkbox"/> | 0.0.0.0 | 0.0.0.0 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| 14 | <input type="checkbox"/> | 0.0.0.0 | 0.0.0.0 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| 15 | <input type="checkbox"/> | 0.0.0.0 | 0.0.0.0 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |
| 16 | <input type="checkbox"/> | 0.0.0.0 | 0.0.0.0 | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | <input type="checkbox"/> | |

The following table describes the labels in this screen.

Table 138 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. |

32.7 Account Security

Use this screen to encrypt all passwords configured in the Switch. This setting will affect how the password is shown (as plain text or encrypted text) in the configuration file saved in **Management > Maintenance > Save Configuration**.

Note: Make sure to enable **Password Encryption** to avoid displaying passwords as plain text in the configuration file.

Password Encryption encrypts all passwords in the configuration file. However, if you want to show some passwords as plain text in the configuration file, select them as below.

Note: Be careful who can access configuration files with plain text passwords!

- **Authentication** information configured for **Authentication** in the **Advanced Application > AAA > AAA Setup** screen (**Method 1/2/3** setting in the **Privilege Enable** and **Login** fields).
- **Authorization** information configured for **Authorization** in the **Advanced Application > AAA > AAA Setup** screen (**Active/Console/Method** setting in the **Exec** and **Dot1x** fields).
- **Server** information configured for **Authentication Server** in the **Advanced Application > AAA > RADIUS Server Setup** screen (**Mode/Timeout** fields).
- **System** account information configured in the Switch (admin, user login name, and password).
- **SNMP** user account information configured in the **Management > Access Control > SNMP > User** screen (password for SNMP user authentication in the **Authentication** field, and the password for the encryption method for SNMP communication in the **Privacy** field).

Note: The passwords will appear as encrypted text when **Password Encryption** is **Active**.

Click **Management > Access Control > Account Security** to view the screen as shown next.

Click **Access Control** to return to the **Access Control** screen.

Figure 194 Management > Access Control > Account Security

The following table describes the labels in this screen.

Table 139 Management > Access Control > Account Security

| LABEL | DESCRIPTION |
|---------------------|--|
| Account Security | |
| Password Encryption | Select this check box to encrypt all passwords configured on the Switch. This displays the password as encrypted text, in a saved configuration file. Otherwise, the passwords configured on the Switch are displayed in plain text. |
| Apply | Click Apply to save your changes for Account Security to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring Account Security afresh. |
| Display | |

Table 139 Management > Access Control > Account Security (continued)

| LABEL | DESCRIPTION |
|---------|---|
| Display | Select which specific information to display in plain text, in the saved configuration file. <ul style="list-style-type: none"> • Authentication • Authorization • Server |
| User | Select which user account information to display in plain text, in the saved configuration file. <ul style="list-style-type: none"> • System • SNMP |
| Apply | Click Apply to save your changes for Display to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring Display afresh. |

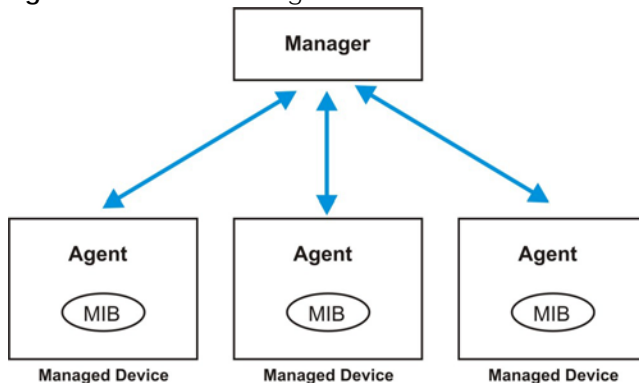
32.8 Technical Reference

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

32.8.1 About SNMP

Simple Network Management Protocol (SNMP) is an application layer protocol used to manage and monitor TCP/IP-based devices. SNMP is used to exchange management information between the network management system (NMS) and a network element (NE). A manager station can manage and monitor the Switch through the network through SNMP version 1 (SNMPv1), SNMP version 2c or SNMP version 3. The next figure illustrates an SNMP management operation. SNMP is only available if TCP/IP is configured.

Figure 195 SNMP Management Model



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

An agent is a management software module that resides in a managed Switch (the Switch). An agent translates the local management information from the managed Switch into a form compatible with SNMP. The manager is the console through which network administrators perform network management functions. It executes applications that control and monitor managed devices.

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

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

Table 140 SNMP Commands

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

SNMP v3 and Security

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

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

Supported MIBs

A MIB is a collection of managed objects that is organized according to hierarchy. The objects define the attributes of the managed device, which includes the names, status, access rights, and data types. Each object can be addressed through an object identifier (OID).

MIBs let administrators collect statistics and monitor status and performance. The Switch uses standard public (RFC-defined) MIBs for standard functionality.

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

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

SNMP Traps

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

Table 141 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 142 SNMP Interface Traps

| OPTION | OBJECT LABEL | OBJECT ID | DESCRIPTION |
|----------|---------------------|----------------------|---|
| linkup | linkUp | 1.3.6.1.6.3.1.1.5.4 | This trap is sent when the Ethernet link is up. |
| linkdown | linkDown | 1.3.6.1.6.3.1.1.5.3 | This trap is sent when the Ethernet link is down. |
| 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 143 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 144 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 145 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. |

32.8.2 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.

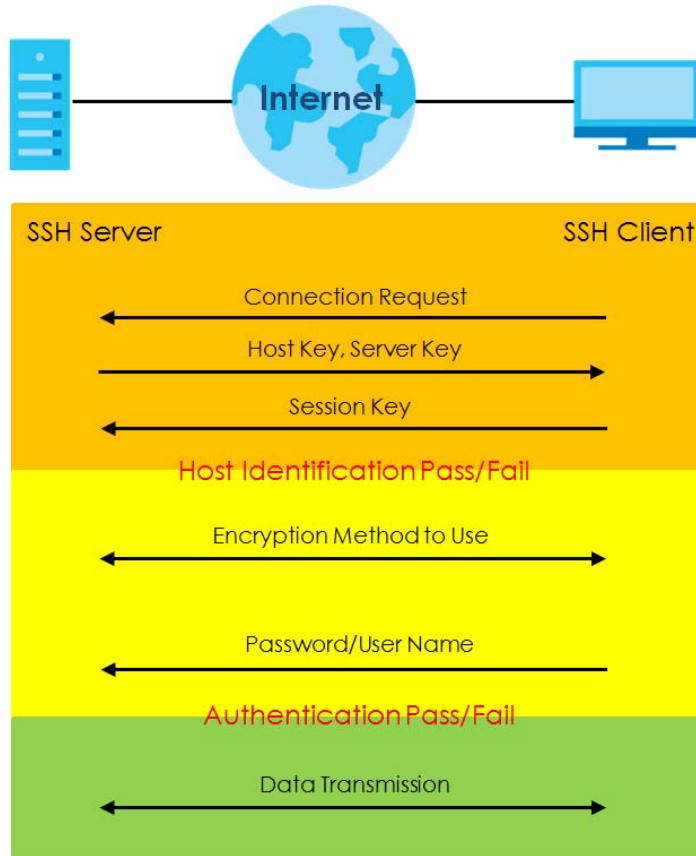
Figure 196 SSH Communication Example



32.8.2.1 How SSH Works

The following table summarizes how a secure connection is established between two remote hosts.

Figure 197 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.

32.8.2.2 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.

32.8.2.3 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.

32.8.3 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).

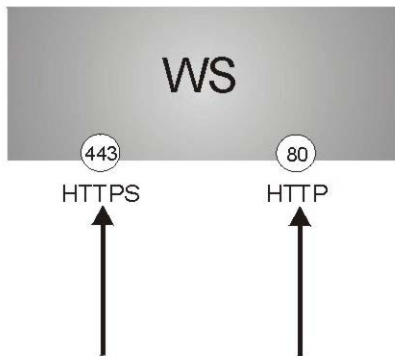
It relies upon certificates, public keys, and private keys.

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 198 HTTPS Implementation



Note: If you disable HTTP in the Service Access Control screen, then the Switch blocks all HTTP connection attempts.

32.8.3.1 HTTPS Example

If you have not changed the default HTTPS port on the Switch, then in your browser enter "https://Switch IP Address/" as the web site address where "Switch IP Address" is the IP address or domain name of the Switch you wish to access.

Internet Explorer Warning Messages

Internet Explorer 6

When you attempt to access the Switch HTTPS server, a Windows dialog box pops up asking if you trust the server certificate.

You see the following **Security Alert** screen in Internet Explorer. Select **Yes** to proceed to the Web Configurator login screen; if you select **No**, then Web Configurator access is blocked.

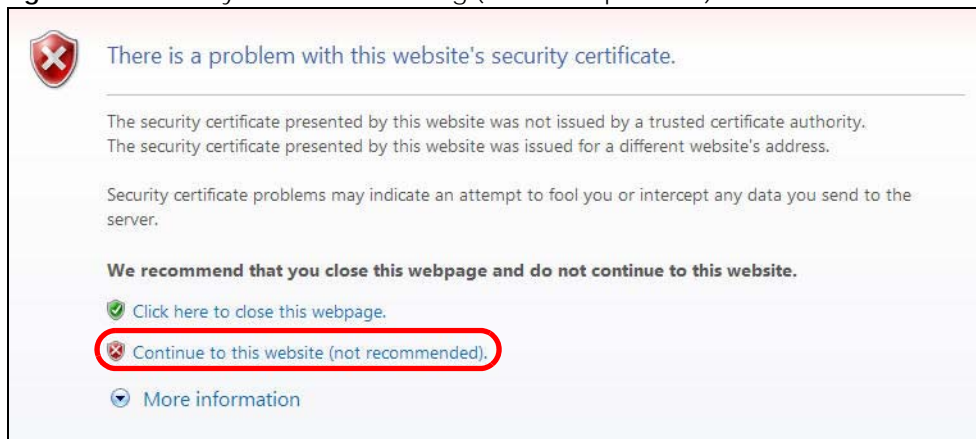
Figure 199 Security Alert Dialog Box (Internet Explorer 6)



Internet Explorer 7 later version

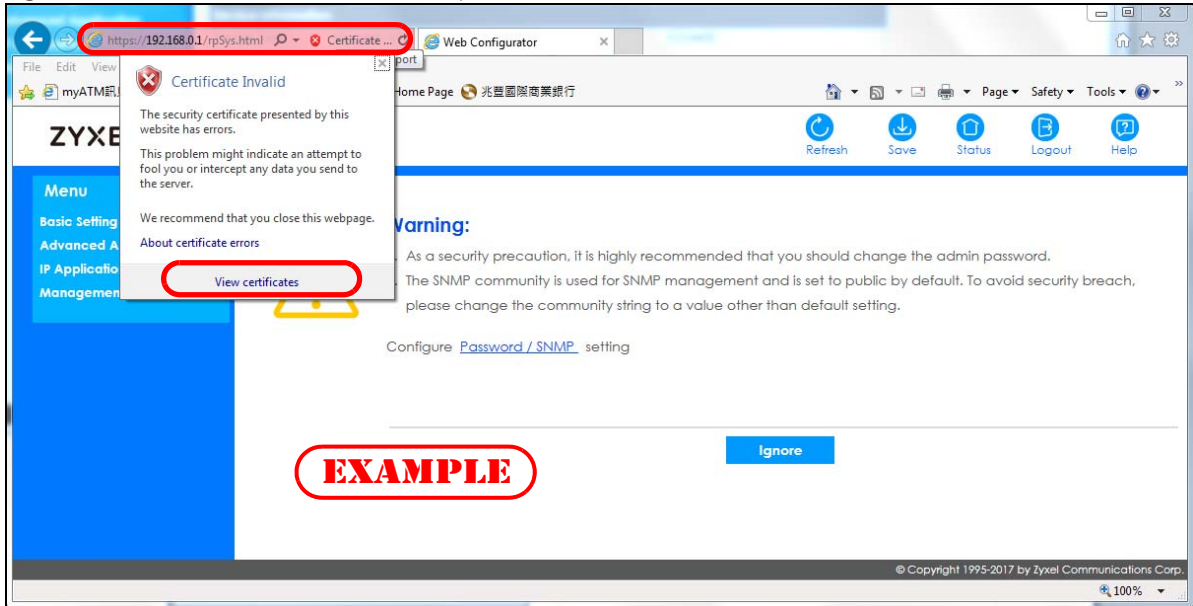
When you attempt to access the Switch HTTPS server, a screen with the message "There is a problem with this website's security certificate." may display. If that is the case, click **Continue to this website (not recommended)** to proceed to the Web Configurator login screen.

Figure 200 Security Certificate Warning (Internet Explorer 11)



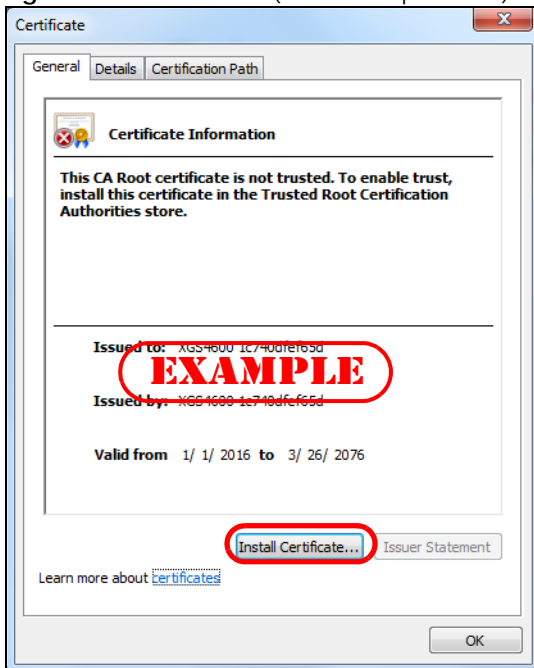
After you log in, you will see the red address bar with the message **Certificate Error**. Click on **Certificate Error** next to the address bar and click **View certificates**.

Figure 201 Certificate Error (Internet Explorer 11)



Click **Install Certificate...** and follow the on-screen instructions to install the certificate in your browser.

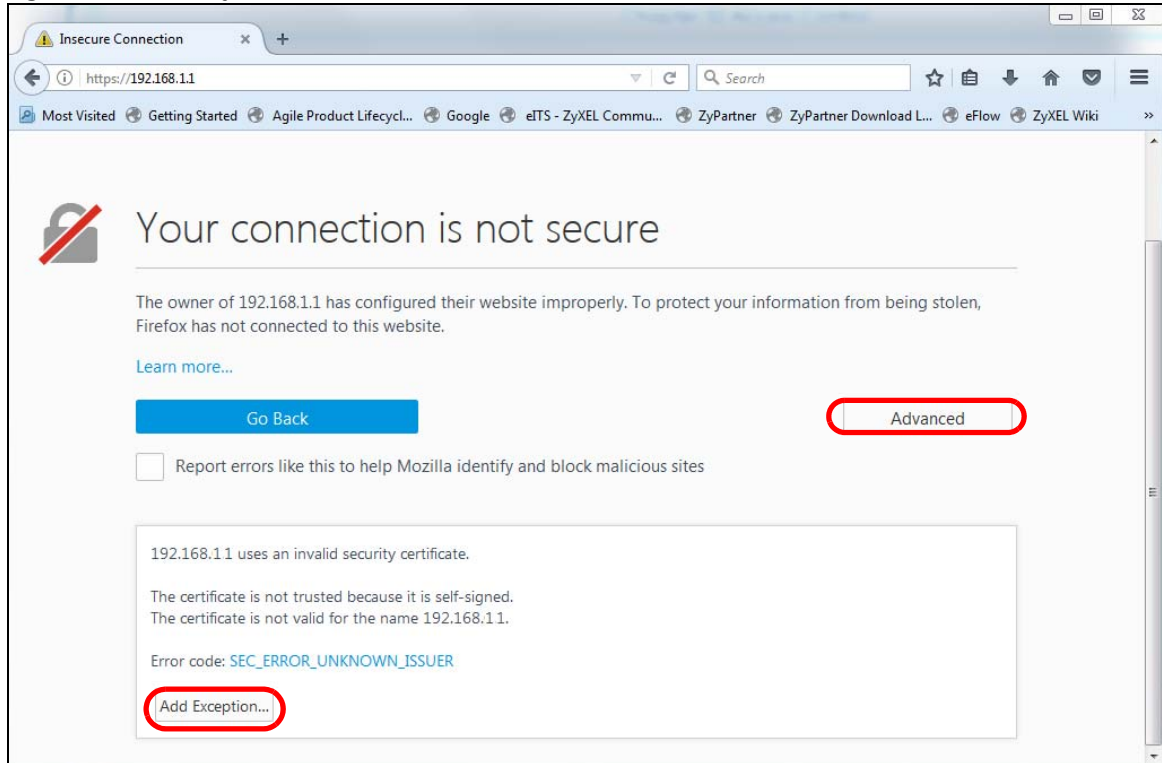
Figure 202 Certificate (Internet Explorer 11)



Mozilla Firefox Warning Messages

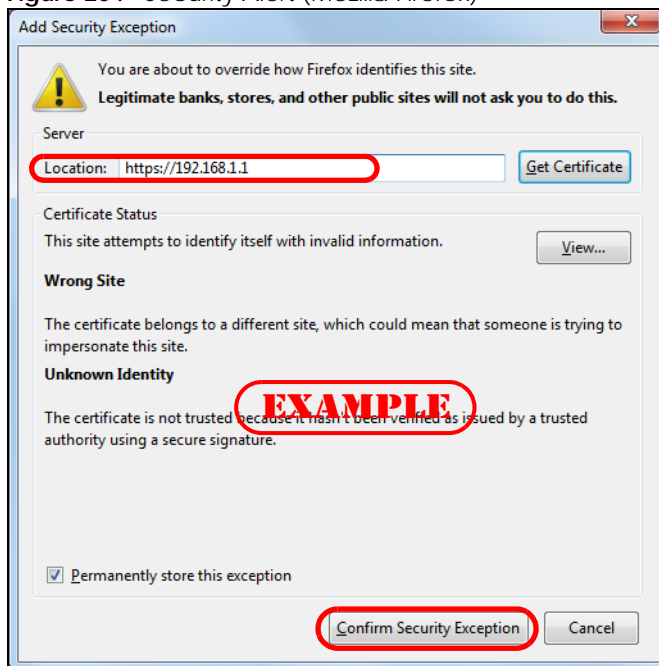
When you attempt to access the Switch HTTPS server, a **Your connection is not secure** screen may display. If that is the case, click **I Understand the Risks** and then the **Add Exception...** button.

Figure 203 Security Alert (Mozilla Firefox)



Confirm the HTTPS server URL matches. Click **Confirm Security Exception** to proceed to the Web Configurator login screen.

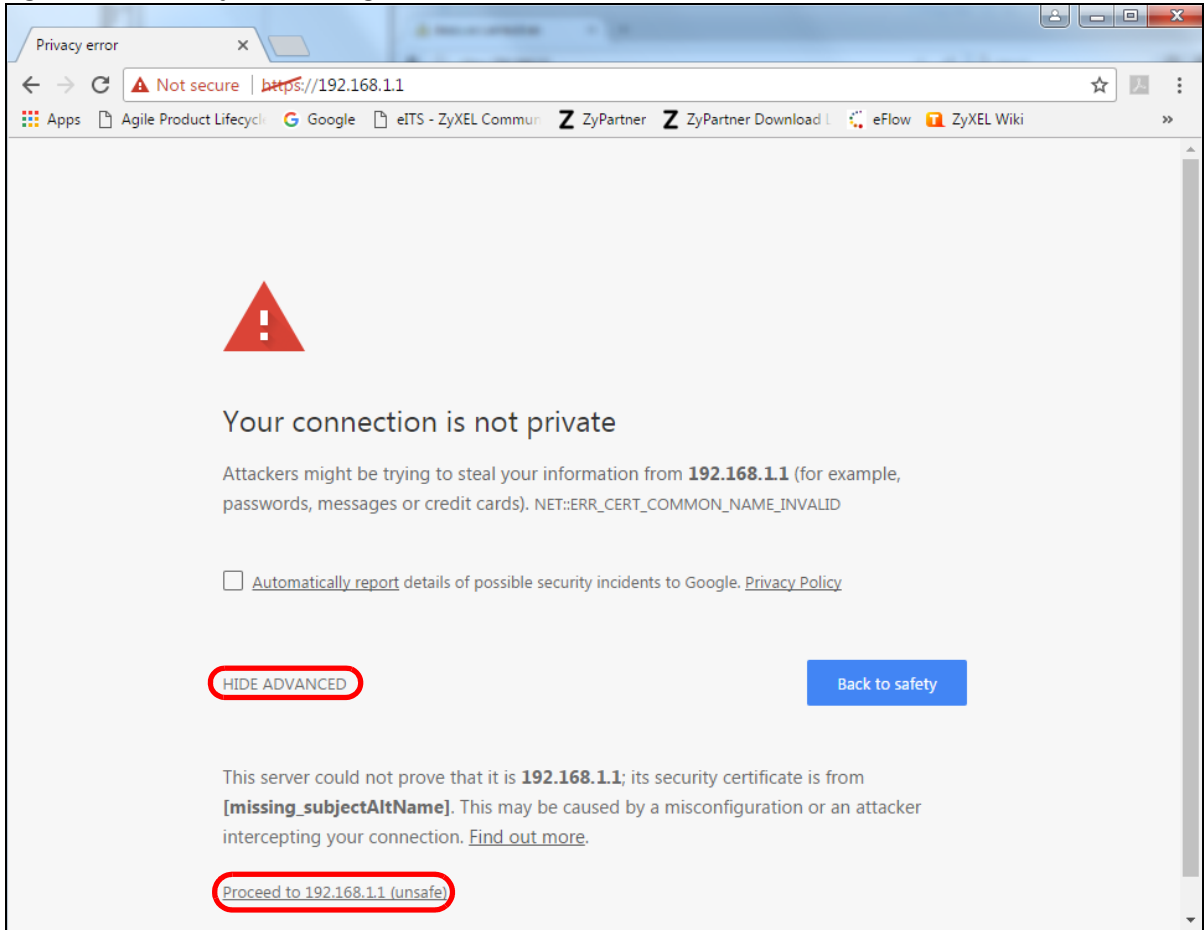
Figure 204 Security Alert (Mozilla Firefox)



32.8.4 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.

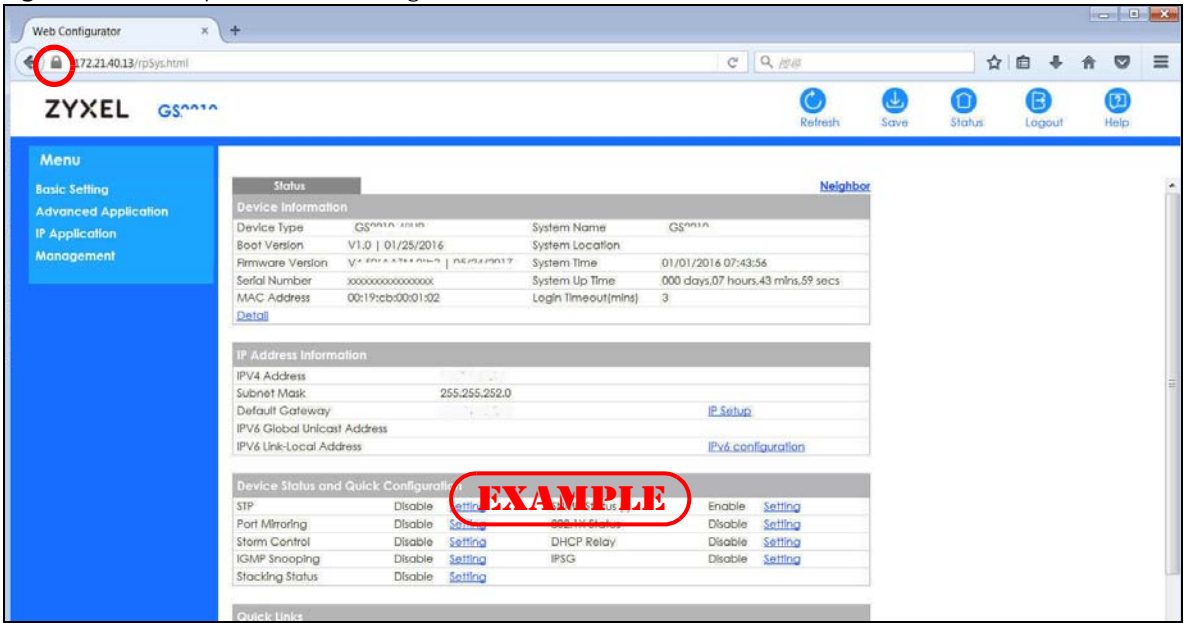
Figure 205 Security Alert (Google Chrome 58.0.3029.110)



32.8.4.1 Main Settings

After you accept the certificate and enter the login user name and password, the Switch main screen appears. The lock displayed in the bottom right of the browser status bar or next to the website address denotes a secure connection.

Figure 206 Example: Lock Denoting a Secure Connection



CHAPTER 33

Diagnostic

33.1 Overview

This chapter explains the **Diagnostic** screen. You can use this screen to help you identify problems.

33.2 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 207 Management > Diagnostic

The screenshot shows the 'Diagnostic' screen with a header bar and a main content area. The main content area is divided into several sections:

- Diagnostic** (Header)
- Info -** (Placeholder for information)
- Ping Test**: Includes radio buttons for IPv4 (selected) and IPv6, dropdown menus for protocol selection, a text input for 'IP Address/Host Name', a numeric input for 'Count' (set to 3), and a blue 'Ping' button.
- Trace Route Test**: Includes radio buttons for IPv4 (selected) and IPv6, dropdown menus for protocol selection, 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' label, a numeric input for 'Queries' (set to 3), and a blue 'Trace Route' button.
- Ethernet Port Test**: Includes a text input for 'Port' and a blue 'Port Test' button.
- Cable Diagnostics** (with an information icon): Includes a text input for 'Port' and a blue 'Diagnose' button.

The following table describes the labels in this screen.

Table 146 Management > Diagnostic

| LABEL | DESCRIPTION |
|----------------------|---|
| Ping Test | |
| IPv4 | Select this option if you want to ping an IPv4 address. Otherwise, select – to send ping requests to all VLANs on the Switch. |
| IPv6 | Select this option if you want to ping an IPv6 address. You can also select vlan and specify the ID number of the VLAN to which the Switch is to send ping requests. Otherwise, select – to send ping requests to all VLANs on the Switch. |
| IP Address/Host Name | Type the IP address or host name of a device that you want to ping in order to test a connection. Click Ping to have the Switch ping the IP address. |
| Count | Enter the number of ICMP Echo Request (ping) messages the Switch continuously sends. |
| Trace Route Test | |
| IPv4 | Select this option if you want to trace the route packets taken to a device with an IPv4 address. Otherwise, select – to trace the path on any VLAN. Note: The device to which you want to run a traceroute must belong to the VLAN you specify here. |
| IPv6 | Select this option if you want to trace the route packets taken to a device with an IPv6 address. |
| IP Address/Host Name | Enter the IP address or host name of a device to which you want to perform a traceroute. Click Trace Route to have the Switch perform the traceroute function. This determines the path a packet takes to the specified device. |
| TTL | Enter the Time To Live (TTL) value for the ICMP Echo Request packets. This is to set the maximum number of the hops (routers) a packet can travel through. Each router along the path will decrement the TTL value by one and forward the packets. When the TTL value becomes zero and the destination is not found, the router drops the packets and informs the sender. |
| Wait Time | Specify how many seconds the Switch waits for a response to a probe before running another traceroute. |
| Queries | Specify how many times the Switch performs the traceroute function. |
| Ethernet Port Test | Enter a port number and click Port Test to perform an internal loopback test. |
| Port | This is the number of the physical Ethernet port on the Switch. |
| Cable Diagnostics | Enter a port number and click Diagnose to perform a physical wire-pair test of the Ethernet connections on the specified ports. The following fields display when you diagnose a port. Note: This feature is limited to within 100 meters only. |
| Port | This is the number of the physical Ethernet port on the Switch. |
| Channel | An Ethernet cable usually has four pairs of wires. A 10BASE-T or 100BASE-TX port only use and test two pairs, while a 1000BASE-T port requires all four pairs. This displays the descriptive name of the wire-pair in the cable. |
| Pair status | Ok: The physical connection between the wire-pair is okay. Open: There is no physical connection (an open circuit detected) between the wire-pair. Short: There is an short circuit detected between the wire-pair. Unknown: The Switch failed to run cable diagnostics on the cable connected this port. Unsupported: The port is a fiber port or it is not active. |

Table 146 Management > Diagnostic (continued)

| LABEL | DESCRIPTION |
|-------------------|---|
| Cable length | <p>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.</p> <p>This shows N/A if the Pair status is Open or Short. Check the Distance to fault.</p> <p>This shows Unsupported if the Switch chipset does not support to show the cable length.</p> |
| Distance to fault | <p>This displays the distance between the port and the location where the cable is open or shorted.</p> <p>This shows N/A if the Pair status is Ok.</p> <p>This shows Unsupported if the Switch chipset does not support to show the distance.</p> |

CHAPTER 34

System Log

34.1 Overview

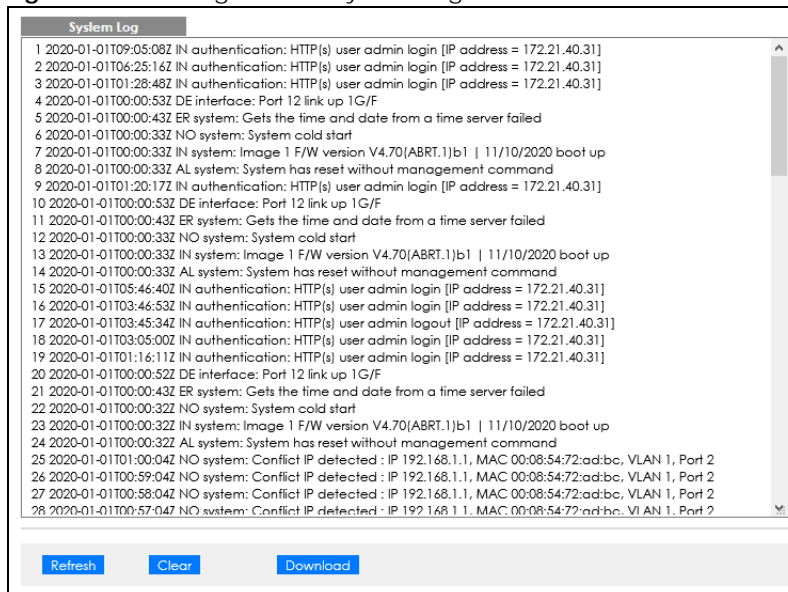
A log message stores the information for viewing.

34.2 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 208 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 35

Syslog Setup

35.1 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 147 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. |

35.1.1 What You Can Do

Use the **Syslog Setup** screen ([Section 35.2 on page 285](#)) to configure the device's system logging settings and configure a list of external syslog servers.

35.2 Syslog Setup

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

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

Figure 209 Management > Syslog Setup

The following table describes the labels in this screen.

Table 148 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 levels of the logs that you want the device to send to this syslog server. The lower the number, the more critical the logs are. |

Table 148 Management > Syslog Setup (continued)

| LABEL | DESCRIPTION |
|------------|--|
| Add | Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |
| Clear | Click Clear to return the fields to the factory defaults. |
| Index | This is the index number of a syslog server entry. Click this number to edit the entry. |
| Active | This field displays Yes if the device is to send logs to the syslog server. No displays if the device is not to send logs to the syslog server. |
| IP Address | This field displays the IP address of the syslog server. |
| UDP Port | This field displays the port of the syslog server. |
| Log Level | This field displays the severity level of the logs that the device is to send to this syslog server. |
| | Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries. |
| Delete | Click Delete to remove the selected entries. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

CHAPTER 36

Cluster Management

36.1 Cluster Management Overview

This chapter introduces cluster management.

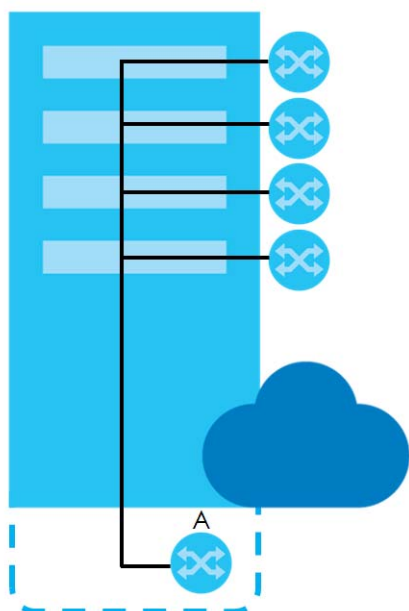
Cluster Management allows you to manage switches through one Switch, called the cluster manager. The switches must be directly connected and be in the same VLAN group so as to be able to communicate with one another.

Table 149 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 210 Clustering Application Example



36.1.1 What You Can Do

- Use the **Cluster Management Status** screen ([Section 36.2 on page 289](#)) 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 36.3 on page 290) to configure clustering management.

36.2 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 211 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 150 Management > Cluster Management Status

| LABEL | DESCRIPTION |
|----------------------|--|
| Status | This field displays the role of this Switch within the cluster. Manager Member (you see this if you access this screen in the cluster member Switch directly and not through the cluster manager) None (neither a manager nor a member of a cluster) |
| Manager | This field displays the cluster manager Switch's hardware MAC address. |
| The Number of Member | This field displays the number of switches that make up this cluster. The following fields describe the cluster member switches. |
| Index | You can manage cluster member switches through the cluster manager Switch. Each number in the Index column is a hyperlink leading to the cluster member Switch's Web Configurator. |
| MacAddr | This is the cluster member Switch's hardware MAC address. |
| Name | This is the cluster member Switch's System Name . |
| Model | This field displays the model name. |
| Status | This field displays: Online (the cluster member Switch is accessible) Error (for example the cluster member Switch password was changed or the Switch was set as the manager and so left the member list, and so on) Offline (the Switch is disconnected – Offline shows approximately 1.5 minutes after the link between cluster member and manager goes down) |

36.3 Clustering Management Configuration

Use this screen to configure clustering management. Click **Management > Cluster Management > Configuration** to display the next screen.

Figure 212 Management > Cluster Management > Configuration

The following table describes the labels in this screen.

Table 151 Management > Cluster Management > Configuration


| LABEL | DESCRIPTION |
|----------------------|---|
| Clustering Manager | The following fields relate to configuring the cluster manager. |
| Active | Select Active to have this Switch become the cluster manager switch. A cluster can only have one manager. Other (directly connected) switches that are set to be cluster managers will not be visible in the Clustering Candidates list. If a Switch that was previously a cluster member is later set to become a cluster manager, then its Status is displayed as Error in the Cluster Management Status screen and a warning icon () appears in the member summary list below. |
| Name | Type a name to identify the Clustering Manager . You may use up to 32 printable characters (spaces are allowed). |
| VID | This is the VLAN ID and is only applicable if the Switch is set to 802.1Q VLAN. All switches must be directly connected and in the same VLAN group to belong to the same cluster. Switches that are not in the same VLAN group are not visible in the Clustering Candidates list. This field is ignored if the Clustering Manager is using Port-based VLAN. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |
| Clustering Candidate | The following fields relate to the switches that are potential cluster members. |

Table 151 Management > Cluster Management > Configuration (continued)

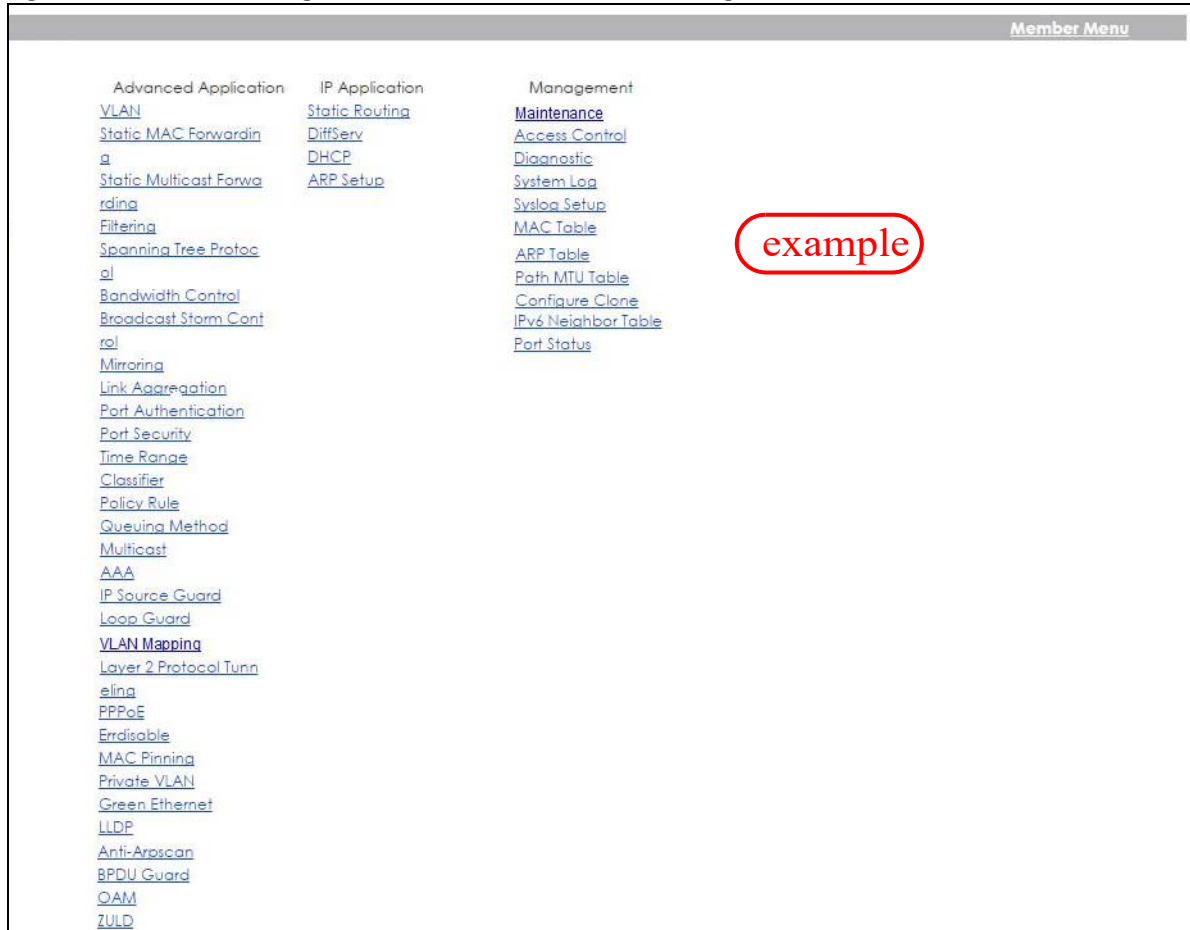
| LABEL | DESCRIPTION |
|---|--|
| List | A list of suitable candidates found by auto-discovery is shown here. The switches must be directly connected. Directly connected switches that are set to be cluster managers will not be visible in the Clustering Candidate list. Switches that are not in the same management VLAN group will not be visible in the Clustering Candidate list. |
| Password | Each cluster member's password is its Web Configurator password. Select a member in the Clustering Candidate list and then enter its Web Configurator password. If that switch administrator changes the Web Configurator password afterwards, then it cannot be managed from the Cluster Manager . Its Status is displayed as Error in the Cluster Management Status screen. If multiple devices have the same password then hold [SHIFT] and click those switches to select them. Then enter their common Web Configurator password. |
| Add | Click Add to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |
| Refresh | Click Refresh to perform auto-discovery again to list potential cluster members. |
| The next summary table shows the information for the clustering members configured. | |
| Index | This is the index number of a cluster member switch. |
| MacAddr | This is the cluster member switch's hardware MAC address. |
| Name | This is the cluster member switch's System Name . |
| Model | This is the cluster member switch's model name. |
| | Select an entry's check box to select a specific entry. Otherwise, select the check box in the table heading row to select all entries. |
| Remove | Click the Remove button to remove the selected cluster member switches from the cluster. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

36.4 Technical Reference

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

36.4.1 Cluster Member Switch Management

Go to the **Clustering Management Status** screen of the cluster manager switch and then select an **Index** hyperlink from the list of members to go to that cluster member switch's Web Configurator home page. This cluster member Web Configurator home page and the home page that you would see if you accessed it directly are different.

Figure 213 Cluster Management: Cluster Member Web Configurator Screen

36.4.1.1 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 214 Example: Uploading Firmware to a Cluster Member Switch

```

C:\>ftp 192.168.1.1
Connected to 192.168.1.1.
220 Switch FTP version 1.0 ready at Thu Jan  1 00:58:46 1970
User (192.168.0.1:(none)): admin
331 Enter PASS command
Password:
230 Logged in
ftp> ls
200 Port command okay
150 Opening data connection for LIST
--w--w--w-  1 owner   group      3042210 Jul  01 12:00 ras
-rw-rw-rw-  1 owner   group      393216  Jul  01 12:00 config
--w--w--w-  1 owner   group           0 Jul  01 12:00 fw-00-a0-c5-01-23-46
-rw-rw-rw-  1 owner   group           0 Jul  01 12:00 config-00-a0-c5-01-23-46
226 File sent OK
ftp: 297 bytes received in 0.00Seconds 297000.00Kbytes/sec.
ftp> bin
200 Type I OK
ftp> put 470ACAQ0.bin fw-00-a0-c5-01-23-46
200 Port command okay
150 Opening data connection for STOR fw-00-a0-c5-01-23-46
226 File received OK
ftp: 262144 bytes sent in 0.63Seconds 415.44Kbytes/sec.
ftp>

```

The following table explains some of the FTP parameters.

Table 152 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. |
| 470ACAQ0.bin | This is the name of the firmware file you want to upload to the cluster member switch. |
| fw-00-a0-c5-01-23-46 | This is the cluster member switch's firmware name as seen in the cluster manager switch. |
| config-00-a0-c5-01-23-46 | This is the cluster member switch's configuration file name as seen in the cluster manager switch. |

CHAPTER 37

MAC Table

37.1 MAC Table Overview

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

The **MAC Table** screen (a MAC table is also known as a filtering database) shows how frames are forwarded or filtered across the Switch's ports. It shows what device MAC address, belonging to what VLAN group (if any) is forwarded to which ports and whether the MAC address is dynamic (learned by the Switch) or static (manually entered in the **Static MAC Forwarding** screen).

37.1.1 What You Can Do

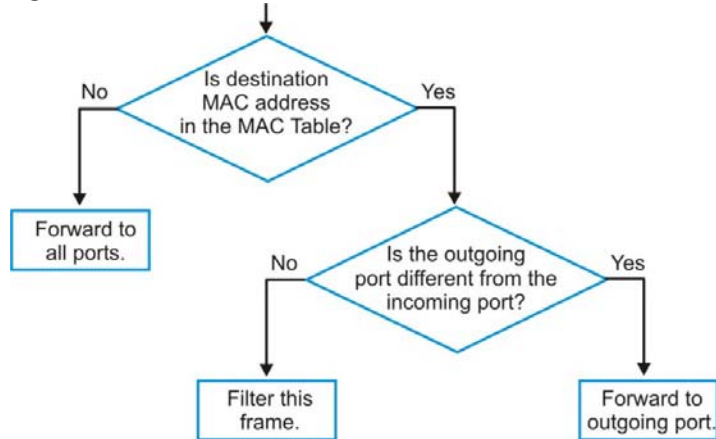
Use the **MAC Table** screen ([Section 37.2 on page 295](#)) to check whether the MAC address is dynamic or static.

37.1.2 What You Need to Know

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

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

Figure 215 MAC Table Flowchart



37.2 Viewing the MAC Table

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

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

Figure 216 Management > MAC Table

MAC table

Condition

Sort by

Transfer Type

All

Static

MAC

VID

Port

Trunk

MAC

Dynamic to MAC forwarding

Dynamic to MAC filtering

| Index | MAC Address | VID | Port | Type |
|-------|-------------------|-----|------|---------|
| 1 | 00:00:5e:00:01:02 | 1 | 3 | Dynamic |
| 2 | 00:03:21:10:be:00 | 1 | 3 | Dynamic |
| 3 | 00:03:21:10:f7:7c | 1 | 3 | Dynamic |
| 4 | 00:03:21:10:f7:7d | 1 | 3 | Dynamic |
| 5 | 00:03:21:11:02:a1 | 1 | 3 | Dynamic |
| 6 | 00:08:54:72:ad:bc | 1 | 3 | Dynamic |
| 7 | 00:0e:e3:00:3d:0d | 1 | 3 | Dynamic |
| 8 | 00:0e:e3:00:3d:48 | 1 | 3 | Dynamic |
| 9 | 00:0e:e3:01:75:e2 | 1 | 3 | Dynamic |
| 10 | 00:0e:e3:03:e5:e6 | 1 | 3 | Dynamic |

The following table describes the labels in this screen.

Table 153 Management > MAC Table

| LABEL | DESCRIPTION |
|---------------|---|
| Condition | <p>Select one of the buttons and click Search to only display the data which matches the criteria you specified.</p> <p>Select All to display any entry in the MAC table of the Switch.</p> <p>Select Static to display the MAC entries manually configured on the Switch.</p> <p>Select MAC and enter a MAC address in the field provided to display a specified MAC entry.</p> <p>Select VID and enter a VLAN ID in the field provided to display the MAC entries belonging to the specified VLAN.</p> <p>Select Port and enter a port number in the field provided to display the MAC addresses which are forwarded on the specified port.</p> <p>Select Trunk and type the ID of a trunk group to display all MAC addresses learned from the ports in the trunk group.</p> |
| Sort by | <p>Define how the Switch displays and arranges the data in the summary table below.</p> <p>Select MAC to display and arrange the data according to MAC address.</p> <p>Select VID to display and arrange the data according to VLAN group.</p> <p>Select PORT to display and arrange the data according to port number.</p> |
| Transfer Type | <p>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 Advanced Application > Static MAC Forwarding screen.</p> <p>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 Advanced Application > Filtering screen and the default filtering action is Discard source.</p> |
| 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 Advanced Application > Static MAC Forwarding screen). |

CHAPTER 38

ARP Table

38.1 Overview

This chapter introduces ARP Table.

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

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

38.1.1 What You Can Do

Use the **ARP Table** screen ([Section 38.2 on page 297](#)) to view IP-to-MAC address mappings.

38.1.2 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.

38.2 Viewing the ARP Table

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

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

Figure 217 Management > ARP Table

| Index | IP Address | MAC Address | VID | Port | Age(s) | Type |
|-------|---------------|-------------------|-----|------|--------|---------|
| 1 | 172.21.40.6 | 58:8b:f3:ff:ee:71 | 1 | CPU | 0 | static |
| 2 | 172.21.40.14 | dc:4a:3e:40:ec:5f | 1 | 8 | 100 | dynamic |
| 3 | 172.21.40.37 | 94:57:a5:e8:4f:77 | 1 | 6 | 35 | dynamic |
| 4 | 172.21.43.254 | 00:00:5e:00:01:02 | 1 | 6 | 265 | dynamic |

The following table describes the labels in this screen.

Table 154 Management > ARP Table

| LABEL | DESCRIPTION |
|-------------|---|
| Condition | Specify how you want the Switch to remove ARP entries when you click Flush . Select All to remove all of the dynamic entries from the ARP table. Select IP Address and enter an IP address to remove the dynamic entries learned with the specified IP address. Select Port and enter a port number to remove the dynamic entries learned on the specified port. |
| Flush | Click Flush to remove the ARP entries according to the condition you specified. |
| Cancel | Click Cancel to return the fields to the factory defaults. |
| Index | This is the ARP table entry number. |
| IP Address | This is the IP address of a device connected to a Switch port with the corresponding MAC address below. |
| MAC Address | This is the MAC address of the device with the corresponding IP address above. |
| VID | This field displays the VLAN to which the device belongs. |
| Port | This field displays the port to which the device connects. CPU means this IP address is the Switch's management IP address. |
| Age(s) | This field displays how long (in seconds) an entry can still remain in the ARP table before it ages out and needs to be relearned. This shows 0 for a static entry. |
| Type | This shows the IP address is dynamic (learned by the Switch). |

CHAPTER 39

Path MTU Table

39.1 Path MTU Overview

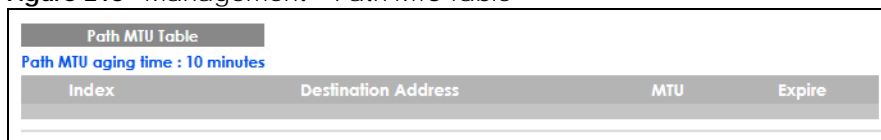
This chapter introduces the IPv6 Path MTU table.

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.

39.2 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 218 Management > Path MTU Table



| Index | Destination Address | MTU | Expire |
|-------|---------------------|-----|--------|
|-------|---------------------|-----|--------|

The following table describes the labels in this screen.

Table 155 Management > Path MTU Table

| LABEL | DESCRIPTION |
|---------------------|---|
| Path MTU aging time | This field displays how long an entry remains in the Path MTU table before it ages out and needs to be relearned. |
| Index | This field displays the index number of each entry in the table. |
| Destination Address | This field displays the destination IPv6 address of each path or entry. |
| MTU | This field displays the maximum transmission unit of the links in the path. |
| Expire | This field displays how long (in minutes) an entry can still remain in the Path MTU table before it ages out and needs to be relearned. |

CHAPTER 40

Configure Clone

40.1 Overview

This chapter shows you how you can copy the settings of one port onto other ports.

40.2 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 219 Management > Configure Clone

| Configure Clone | |
|--|---|
| Source | Destination |
| <input checked="" type="radio"/> Port <input type="text"/> | <input type="text"/> |
| Port Features | |
| Basic Setting | <input type="checkbox"/> • <input type="checkbox"/> Active <input type="checkbox"/> Name <input type="checkbox"/> Speed / Duplex <input type="checkbox"/> Flow Control |
| Advanced Application | <input type="checkbox"/> VLAN1q <input type="checkbox"/> VLAN1q Member <input type="checkbox"/> Bandwidth Control <input type="checkbox"/> Port Security <input type="checkbox"/> Broadcast Storm Control <input type="checkbox"/> Mirroring <input type="checkbox"/> Queuing Method <input type="checkbox"/> Spanning Tree Protocol <input type="checkbox"/> Port-based VLAN <input type="checkbox"/> Loop Guard <input type="checkbox"/> DHCP Snooping <input type="checkbox"/> LLDP <input type="checkbox"/> ARP Learning <input type="checkbox"/> CPU Protection <input type="checkbox"/> Power over Ethernet <input type="checkbox"/> SNMP Trap <input type="checkbox"/> Green Ethernet <input type="checkbox"/> Diffserv |
| <input type="button" value="Apply"/> <input type="button" value="Cancel"/> | |

The following table describes the labels in this screen.

Table 156 Management > Configure Clone

| LABEL | DESCRIPTION |
|------------------------------------|---|
| Source/ Destination Port | <p>Enter the source port under the Source label. This port's attributes are copied.</p> <p>Enter the destination port or ports under the Destination label. These are the ports which are going to have the same attributes as the source port. You can enter individual ports separated by a comma or a range of ports by using a dash.</p> <p>Example:</p> <p>2, 4, 6 indicates that ports 2, 4 and 6 are the destination ports.</p> <p>2-6 indicates that ports 2 through 6 are the destination ports.</p> |
| * | Select * to apply all settings to the port. Use this first to select the common settings and then remove the settings you do not want copied. |
| Basic Setting | Select which port settings (you configured in the Basic Setting menus) should be copied to the destination ports. |
| Advanced Application | Select which port settings (you configured in the Advanced Application menus) should be copied to the destination ports. |
| Apply | Click Apply to save your changes to the Switch's run-time memory. The Switch loses these changes if it is turned off or loses power, so use the Save link on the top navigation panel to save your changes to the non-volatile memory when you are done configuring. |
| Cancel | Click Cancel to begin configuring this screen afresh. |

CHAPTER 41

IPv6 Neighbor Table

41.1 IPv6 Neighbor Table Overview

This chapter introduces the IPv6 neighbor table.

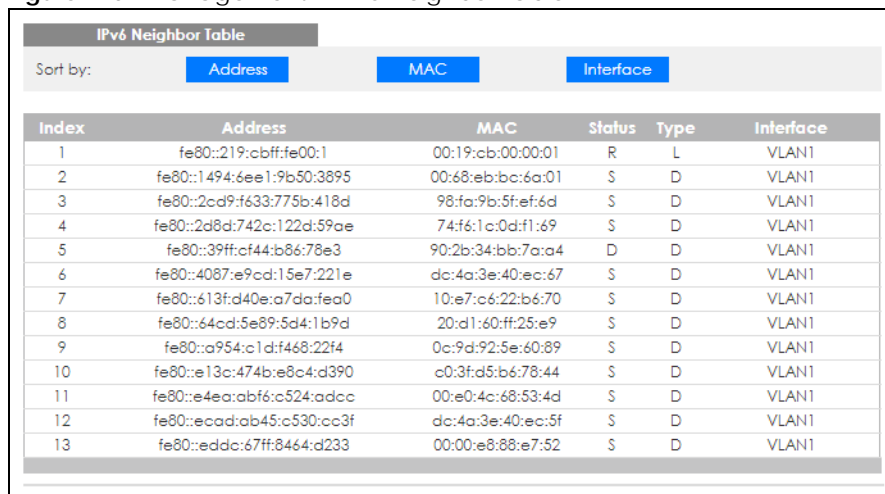
An IPv6 host is required to have a neighbor table. If there is an address to be resolved or verified, the Switch sends out a neighbor solicitation message. When the Switch receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor table. You can also manually 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.

41.2 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 220 Management > IPv6 Neighbor Table



| Index | Address | MAC | Status | Type | Interface |
|-------|---------------------------|-------------------|--------|------|-----------|
| 1 | fe80::219:cbff:fe00:1 | 00:19:cb:00:00:01 | R | L | VLAN1 |
| 2 | fe80::1494:6ee1:9b50:3895 | 00:68:eb:bc:6a:01 | S | D | VLAN1 |
| 3 | fe80::2cd9:f633:775b:418d | 98:fa:9b:5f:ef:6d | S | D | VLAN1 |
| 4 | fe80::2d8d:742c:122d:59ae | 74:f6:1c:0d:f1:69 | S | D | VLAN1 |
| 5 | fe80::39ff:cf44:b86:78e3 | 90:2b:34:bb:7a:a4 | D | D | VLAN1 |
| 6 | fe80::4087:e9cd:15e7:221e | dc:4a:3e:40:ec:67 | S | D | VLAN1 |
| 7 | fe80::613f:d40e:a7da:fea0 | 10:e7:c6:22:b6:70 | S | D | VLAN1 |
| 8 | fe80::64cd:5e89:5d4:1b9d | 20:d1:60:ff:25:e9 | S | D | VLAN1 |
| 9 | fe80::a954:c1d:f468:22f4 | 0c:9d:92:5e:60:89 | S | D | VLAN1 |
| 10 | fe80::e13c:474b:e8c4:d390 | c0:3f:d5:b6:78:44 | S | D | VLAN1 |
| 11 | fe80::e4ea:abf6:c524:adcc | 00:e0:4c:68:53:4d | S | D | VLAN1 |
| 12 | fe80::eccd:ab45:c530:cc3f | dc:4a:3e:40:ec:5f | S | D | VLAN1 |
| 13 | fe80::eddc:67ff:8464:d233 | 00:00:e8:88:e7:52 | S | D | VLAN1 |

The following table describes the labels in this screen.

Table 157 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. |
| Status | <p>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:</p> <ul style="list-style-type: none"> • reachable (R): The interface of the neighboring device is reachable. (The Switch has received a response to the initial request.) • stale (S): The last reachable time has expired and the Switch is waiting for a response to another initial request. The field displays this also when the Switch receives an unrequested response from the neighbor's interface. • delay (D): The neighboring interface is no longer known to be reachable, and traffic has been sent to the neighbor recently. The Switch delays sending request packets for a short to give upper-layer protocols a chance to determine reachability. • probe (P): The Switch is sending request packets and waiting for the neighbor's response. • invalid (IV): The neighbor address is with an invalid IPv6 address. • unknown (?): The status of the neighboring interface cannot be determined for some reason. • incomplete (I): Address resolution is in progress and the link-layer address of the neighbor has not yet been determined. The interface of the neighboring device did not give a complete response. |
| Type | <p>This field displays the type of an address mapping to a neighbor interface. The available options in this field are:</p> <ul style="list-style-type: none"> • 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 42

Port Status

42.1 Overview

This chapter introduces the port status screens.

42.2 Port Status

This screen displays a port statistical summary with links to each port showing statistical details. To view the port statistics, click **Status** in all Web Configurator screens and then the **Port Status** link in the **Quick Links** section of the **Status** screen to display the **Port Status** screen as shown next. You can also click **Management > Port Status** to see the following screen.

Figure 221 Management > Port Status

| Port Status | | | | | | | | | | | Utilization |
|-------------------|------|------|------------|-----|----------|---------|---------|--------|---------|---------|-------------|
| Port | Name | Link | State | PD | LACP | TxPkts | RxPkts | Errors | Tx kB/s | Rx kB/s | Up Time |
| 1 | | 1G/F | FORWARDING | Off | Disabled | 1578014 | 517385 | 0 | 44.738 | 6.523 | 0:45:55 |
| 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 | | 1G/F | FORWARDING | Off | Disabled | 486084 | 1563478 | 0 | 0.564 | 0.561 | 15:48:01 |
| 6 | | Down | STOP | Off | Disabled | 12350 | 21234 | 0 | 0.0 | 0.0 | 0:00:00 |
| 7 | | Down | STOP | Off | Disabled | 0 | 0 | 0 | 0.0 | 0.0 | 0:00:00 |
| 8 | | Down | STOP | Off | Disabled | 6448 | 3414 | 0 | 0.0 | 0.0 | 0:00:00 |

Any
 Port [Clear Counter](#)

The following table describes the labels in this screen.

Table 158 Management > Port Status

| LABEL | DESCRIPTION |
|-------|---|
| Port | This identifies the Ethernet port. Click a port number to display the Port Details screen. |
| Name | This is the name you assigned to this port in the Basic Setting > Port Setup screen. |
| Link | This field displays the speed (either 10M for 10 Mbps, 100M for 100 Mbps, or 1G for 1 Gbps) and the duplex (F for full duplex or H for half). This field displays Down if the port is not connected to any device. |
| State | If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port. If STP is disabled, this field displays FORWARDING if the link is up, otherwise, it displays STOP . When LACP (Link Aggregation Control Protocol) and STP are in blocking state, it displays Blocking . |

Table 158 Management > Port Status (continued)

| LABEL | DESCRIPTION |
|---------------|---|
| PD | For PoE models only. This field displays whether or not a powered device (PD) is allowed to receive power from the Switch on this port. |
| LACP | This 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. |

42.2.1 Port Details

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

Figure 222 Management > 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 159 Management > Port Status > Port Details

| LABEL | DESCRIPTION |
|-----------|---|
| Port Info | |
| Port NO. | This field displays the port number you are viewing. |
| Name | This field displays the name of the port. |
| Link | This field displays the speed (either 10M for 10 Mbps, 100M for 100 Mbps, or 1G for 1 Gbps) and the duplex (F for full duplex or H for half duplex). This field displays Down if the port is not connected to any device. |
| State | If STP (Spanning Tree Protocol) is enabled, this field displays the STP state of the port. If STP is disabled, this field displays FORWARDING if the link is up, otherwise, it displays STOP . When LACP (Link Aggregation Control Protocol) and STP are in blocking state, it displays Blocking . |
| LACP | This field shows if LACP is enabled on this port or not. |
| TxPkts | This field shows the number of transmitted frames on this port. |
| RxPkts | This field shows the number of received frames on this port. |
| Errors | This field shows the number of received errors on this port. |
| Tx kB/s | This field shows the number of kilobytes per second transmitted on this port. |

Table 159 Management > Port Status > Port Details (continued)

| LABEL | DESCRIPTION |
|--|--|
| Tx Utilization% | This field shows the percentage of actual transmitted frames on this port as a percentage of the Link speed. |
| Rx kB/s | This field shows the number of kilobytes per second received on this port. |
| Rx Utilization% | This field shows the percentage of actual received frames on this port as a percentage of the Link speed. |
| Up Time | This field shows the total amount of time the connection has been up. |
| Tx Packet | |
| The following fields display detailed information about packets transmitted. | |
| Unicast | This field shows the number of good unicast packets transmitted. |
| Multicast | This field shows the number of good multicast packets transmitted. |
| Broadcast | This field shows the number of good broadcast packets transmitted. |
| Pause | This field shows the number of 802.3x pause packets transmitted. |
| Rx Packet | |
| The following fields display detailed information about packets received. | |
| Unicast | This field shows the number of good unicast packets received. |
| Multicast | This field shows the number of good multicast packets received. |
| Broadcast | This field shows the number of good broadcast packets received. |
| Pause | This field shows the number of 802.3x pause packets received. |
| TX Collision | |
| The following fields display information on collisions while transmitting. | |
| Single | This is a count of successfully transmitted packets for which transmission is inhibited by exactly one collision. |
| Multiple | This is a count of successfully transmitted packets for which transmission was inhibited by more than one collision. |
| Excessive | This is a count of packets for which transmission failed due to excessive collisions. Excessive collision is defined as the number of maximum collisions before the retransmission count is reset. |
| Late | This is the number of times a late collision is detected, that is, after 512 bits of the packets have already been transmitted. |
| Error Packet | |
| The following fields display detailed information about packets received that were in error. | |
| RX CRC | This field shows the number of packets received with CRC (Cyclic Redundant Check) errors. |
| Length | This field shows the number of packets received with a length that was out of range. |
| Runt | This field shows the number of packets received that were too short (shorter than 64 octets), including the ones with CRC errors. |
| Distribution | |
| 64 | This field shows the number of packets (including bad packets) received that were 64 octets in length. |
| 65 to 127 | This field shows the number of packets (including bad packets) received that were between 65 and 127 octets in length. |
| 128 to 255 | This field shows the number of packets (including bad packets) received that were between 128 and 255 octets in length. |
| 256 to 511 | This field shows the number of packets (including bad packets) received that were between 256 and 511 octets in length. |
| 512 to 1023 | This field shows the number of packets (including bad packets) received that were between 512 and 1023 octets in length. |

Table 159 Management > Port Status > Port Details (continued)

| LABEL | DESCRIPTION |
|--------------|--|
| 1024 to 1518 | This field shows the number of packets (including bad packets) received that were between 1024 and 1518 octets in length. |
| Giant | This field shows the number of packets (including bad packets) received that were between 1519 octets and the maximum frame size. The maximum frame size varies depending on your switch model. |

42.2.2 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 223 Management > Port Status > Utilization

| Port Utilization | | | | | Port Status |
|------------------|------|---------|-----------------|---------|-----------------|
| Port | Link | Tx kB/s | Tx Utilization% | Rx kB/s | Rx Utilization% |
| 1 | 1G/F | 0.128 | 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 | 1G/F | 0.0 | 0.0 | 0.128 | 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 |

The following table describes the labels in this screen.

Table 160 Management > Port Status > Utilization

| LABEL | DESCRIPTION |
|-----------------|--|
| Port | This identifies the Ethernet port. |
| Link | This field displays the speed (either 10M for 10 Mbps, 100M for 100 Mbps, or 1G for 1 Gbps) and the duplex (F for full duplex). 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. |

PART III

Troubleshooting and Appendices

CHAPTER 43

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](#)

43.1 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 37](#).
- 2 Check the hardware connections. See [Section 3.1 on page 33](#).
- 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.

43.2 Switch Access and Login

I can see the **Login** screen, but I cannot log in to the Switch. (I forgot the user name and/or password.)

- 1 Check the Switch's management mode by using the **CLOUD** LED.
 - If you are in Cloud management mode, use the **Local credentials Password** to log in to the cloud mode – local GUI. The **Local credentials Password** can be found in **Site-wide > Configure > General settings > Device configuration: Local credentials: Password** in the NCC portal.
 - If you are in standalone management mode, use the default user name **admin** and the default password **1234**.
- 2 Depending on your Switch's management mode, make sure you have entered the correct user name and password. These fields are case-sensitive, please make sure [Caps Lock] is not on.
- 3 If this does not work, or you are not sure what the Switch's management mode is, you have to reset the device to its factory defaults (standalone management mode) first. See [Section 4.8 on page 64](#) for more information on resetting the Switch. (Temporarily disconnect the Internet connection to the Switch after the reset process, to prevent the Switch from being managed by NCC again.)

Note: After performing step 3 and you want to use the Cloud management mode, make sure the Switch is registered in your organization and site in the NCC portal. To register the Switch again, scan the QR code using the Zyxel Nebula Mobile app. See the [Section on page 20](#) for more information on using the app to register the Switch.

I forgot the IP address for the Switch.

- 1 The default IP address is **http://DHCP-assigned IP** (when connecting to a DHCP server) or **192.168.1.1**.
- 2 Use the NCC (Nebula Control Center) or the ZON utility 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.

Note: When your PC is directly connected to the Switch, you can always use the domain name "setup.zyxel" to access the Web Configurator. This requires your PC to be able to connect to a DNS server via the Switch.

- 3 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.
- 4 If this does not work, you have to reset the device to its factory defaults. See [Section 4.8 on page 64](#).

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](#) (when connecting to a DHCP server) or [192.168.1.1](#).
 - If you changed the IP address, use the new IP address.
 - If you changed the IP address and have forgotten it, see the troubleshooting suggestions for [I forgot the IP address for the Switch](#).
- 2 Check the hardware connections, and make sure the LEDs are behaving as expected. See [Section 3.3 on page 37](#).
- 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 64](#).
- 6 If the problem continues, contact the vendor, or try the advanced suggestion.

Advanced Suggestion

- Try to access the Switch using another service, such as Telnet. If you can access the Switch, check the remote management settings to find out why the Switch does not respond to HTTP.

[Pop-up Windows, JavaScripts and Java Permissions](#)

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

- Web browser pop-up windows from your device.
- JavaScripts (enabled by default).
- Java permissions (enabled by default).

[There is unauthorized access to my Switch through telnet, HTTP and SSH.](#)

Click the **Display** button in the **System Log** field in the **Management > Diagnostic** screen to check for unauthorized access to your Switch. To avoid unauthorized access, configure the secured client setting in the **Management > Access Control > Remote Management** screen for telnet, HTTP and SSH (see [Section 32.6 on page 267](#)). Computers not belonging to the secured client set cannot get permission to access the Switch.

43.3 Switch Configuration

I lost my configuration settings after I restart the Switch.

Make sure you save your configuration into the Switch's non-volatile memory each time you make changes. Click **Save** at the top right of the Web Configurator to save the configuration permanently. See also [Section 31.2.2 on page 248](#) for more information about how to save your configuration.



I accidentally unplugged the Switch. I am not sure which configuration file will be loaded.

If you plug the power cable back to the Switch, it will reboot and load the configuration file that was used the last time. For example, if **Config 1** was used on the Switch before you accidentally unplugged the Switch, **Config 1** will be loaded when rebooting.

APPENDIX A

Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the device.

For Zyxel Communications offices, see <https://service-provider.zyxel.com/global/en/contact-us> for the latest information.

For Zyxel Networks offices, see <https://www.zyxel.com/index.shtml> for the latest information.

Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

Taiwan

- Zyxel Communications (Taiwan) Co., Ltd.
- <https://www.zyxel.com>

Asia

China

- Zyxel Communications Corporation–China Office
- <https://www.zyxel.com/cn/sc>

India

- Zyxel Communications Corporation–India Office
- <https://www.zyxel.com/in/en-in>

Kazakhstan

- Zyxel Kazakhstan
- <https://www.zyxel.com/ru/ru>

Korea

- Zyxel Korea Co., Ltd.
- <http://www.zyxel.kr/>

Malaysia

- Zyxel Communications Corp.
- <https://www.zyxel.com/global/en>

Philippines

- Zyxel Communications Corp.
- <https://www.zyxel.com/global/en>

Singapore

- Zyxel Communications Corp.
- <https://www.zyxel.com/global/en>

Taiwan

- Zyxel Communications (Taiwan) Co., Ltd.
- <https://www.zyxel.com/tw/zh>

Thailand

- Zyxel Thailand Co., Ltd.
- <https://www.zyxel.com/th/th>

Vietnam

- Zyxel Communications Corporation–Vietnam Office
- <https://www.zyxel.com/vn/vi>

Europe

Belarus

- Zyxel Communications Corp.
- <https://www.zyxel.com/ru/ru>

Belgium (Netherlands)

- Zyxel Benelux
- <https://www.zyxel.com/nl/nl>
- <https://www.zyxel.com/fr/fr>

Bulgaria

- Zyxel Bulgaria

- <https://www.zyxel.com/bg/bg>

Czech Republic

- Zyxel Communications Czech s.r.o.
- <https://www.zyxel.com/cz/cs>

Denmark

- Zyxel Communications A/S
- <https://www.zyxel.com/dk/da>

Finland

- Zyxel Communications
- <https://www.zyxel.com/fi/fi>

France

- Zyxel France
- <https://www.zyxel.com/fr/fr>

Germany

- Zyxel Deutschland GmbH.
- <https://www.zyxel.com/de/de>

Hungary

- Zyxel Hungary & SEE
- <https://www.zyxel.com/hu/hu>

Italy

- Zyxel Communications Italy S.r.l.
- <https://www.zyxel.com/it/it>

Norway

- Zyxel Communications A/S
- <https://www.zyxel.com/no/no>

Poland

- Zyxel Communications Poland
- <https://www.zyxel.com/pl/pl>

Romania

- Zyxel Romania
- <https://www.zyxel.com/ro/ro>

Russian Federation

- Zyxel Communications Corp.
- <https://www.zyxel.com/ru/ru>

Slovakia

- Zyxel Slovakia
- <https://www.zyxel.com/sk/sk>

Spain

- Zyxel Iberia
- <https://www.zyxel.com/es/es>

Sweden

- Zyxel Communications A/S
- <https://www.zyxel.com/se/sv>

Switzerland

- Studerus AG
- <https://www.zyxel.com/ch/de-ch>
- <https://www.zyxel.com/fr/fr>

Turkey

- Zyxel Turkey A.S.
- <https://www.zyxel.com/tr/tr>

UK

- Zyxel Communications UK Ltd.
- <https://www.zyxel.com/uk/en-gb>

Ukraine

- Zyxel Ukraine
- <https://www.zyxel.com/ua/uk-ua>

South America

Argentina

- Zyxel Communications Corp.
- <https://www.zyxel.com/co/es-co>

Brazil

- Zyxel Communications Brasil Ltda.

- <https://www.zyxel.com/br/pt>

Colombia

- Zyxel Communications Corp.
- <https://www.zyxel.com/co/es-co>

Ecuador

- Zyxel Communications Corp.
- <https://www.zyxel.com/co/es-co>

South America

- Zyxel Communications Corp.
- <https://www.zyxel.com/co/es-co>

Middle East

Israel

- Zyxel Communications Corp.
- <https://il.zyxel.com>

North America

USA

- Zyxel Communications, Inc. – North America Headquarters
- <https://www.zyxel.com/us/en-us>

APPENDIX B

Common Services

The following table lists some commonly-used services and their associated protocols and port numbers. For a comprehensive list of port numbers, ICMP type or code numbers and services, visit the IANA (Internet Assigned Number Authority) web site.

- **Name:** This is a short, descriptive name for the service. You can use this one or create a different one, if you like.
- **Protocol:** This is the type of IP protocol used by the service. If this is **TCP/UDP**, then the service uses the same port number with TCP and UDP. If this is **User-Defined**, the **Port(s)** is the IP protocol number, not the port number.
- **Port(s):** This value depends on the **Protocol**. Please refer to RFC 1700 for further information about port numbers.
 - If the **Protocol** is **TCP, UDP, or TCP/UDP**, this is the IP port number.
 - If the **Protocol** is **USER**, this is the IP protocol number.
- **Description:** This is a brief explanation of the applications that use this service or the situations in which this service is used.

Table 161 Commonly Used Services

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|--------------------|--------------|---------------|---|
| AH (IPSEC_TUNNEL) | User-Defined | 51 | The IPSEC AH (Authentication Header) tunneling protocol uses this service. |
| AIM/New-ICQ | TCP | 5190 | AOL's Internet Messenger service. It is also used as a listening port by ICQ. |
| AUTH | TCP | 113 | Authentication protocol used by some servers. |
| BGP | TCP | 179 | Border Gateway Protocol. |
| BOOTP_CLIENT | UDP | 68 | DHCP Client. |
| BOOTP_SERVER | UDP | 67 | DHCP Server. |
| CU-SEEME | TCP UDP | 7648 24032 | A popular videoconferencing solution from White Pines Software. |
| DNS | TCP/UDP | 53 | Domain Name Server, a service that matches web names (for example www.zyxel.com) to IP numbers. |
| ESP (IPSEC_TUNNEL) | User-Defined | 50 | The IPSEC ESP (Encapsulation Security Protocol) tunneling protocol uses this service. |
| FINGER | TCP | 79 | Finger is a UNIX or Internet related command that can be used to find out if a user is logged on. |
| FTP | TCP TCP | 20 21 | File Transfer Program, a program to enable fast transfer of files, including large files that may not be possible by email. |
| H.323 | TCP | 1720 | NetMeeting uses this protocol. |
| HTTP | TCP | 80 | Hyper Text Transfer Protocol – a client or server protocol for the world wide web. |

Table 161 Commonly Used Services (continued)

| NAME | PROTOCOL | PORT(S) | DESCRIPTION |
|-------------------|--------------|---------|--|
| HTTPS | TCP | 443 | HTTPS is a secured http session often used in e-commerce. |
| ICMP | User-Defined | 1 | Internet Control Message Protocol is often used for diagnostic or routing purposes. |
| ICQ | UDP | 4000 | This is a popular Internet chat program. |
| IGMP (MULTICAST) | User-Defined | 2 | Internet Group Multicast Protocol is used when sending packets to a specific group of hosts. |
| IKE | UDP | 500 | The Internet Key Exchange algorithm is used for key distribution and management. |
| IRC | TCP/UDP | 6667 | This is another popular Internet chat program. |
| MSN Messenger | TCP | 1863 | Microsoft Networks' messenger service uses this protocol. |
| NEW-ICQ | TCP | 5190 | An Internet chat program. |
| NEWS | TCP | 144 | A protocol for news groups. |
| NFS | UDP | 2049 | Network File System – NFS is a client or server distributed file service that provides transparent file sharing for network environments. |
| NNTP | TCP | 119 | Network News Transport Protocol is the delivery mechanism for the USENET newsgroup service. |
| PING | User-Defined | 1 | Packet Internet Groper is a protocol that sends out ICMP echo requests to test whether or not a remote host is reachable. |
| POP3 | TCP | 110 | Post Office Protocol version 3 lets a client computer get e-mail from a POP3 server through a temporary connection (TCP/IP or other). |
| PPTP | TCP | 1723 | Point-to-Point Tunneling Protocol enables secure transfer of data over public networks. This is the control channel. |
| PPTP_TUNNEL (GRE) | User-Defined | 47 | PPTP (Point-to-Point Tunneling Protocol) enables secure transfer of data over public networks. This is the data channel. |
| RCMD | TCP | 512 | Remote Command Service. |
| REAL_AUDIO | TCP | 7070 | A streaming audio service that enables real time sound over the web. |
| REXEC | TCP | 514 | Remote Execution Daemon. |
| RLOGIN | TCP | 513 | Remote Login. |
| RTELNET | TCP | 107 | Remote Telnet. |
| RTSP | TCP/UDP | 554 | The Real Time Streaming (media control) Protocol (RTSP) is a remote control for multimedia on the Internet. |
| SFTP | TCP | 115 | Simple File Transfer Protocol. |
| SMTP | TCP | 25 | Simple Mail Transfer Protocol is the message-exchange standard for the Internet. SMTP enables you to move messages from one email server to another. |
| SNMP | TCP/UDP | 161 | Simple Network Management Program. |
| SNMP-TRAPS | TCP/UDP | 162 | Traps for use with the SNMP (RFC:1215). |

Table 161 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 162 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 163 Predefined Multicast Address

| MULTICAST ADDRESS | 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 cannot be assigned to a multicast group.

Table 164 Reserved Multicast Address

| MULTICAST ADDRESS |
|--------------------|
| FF00:0:0:0:0:0:0:0 |
| FF01:0:0:0:0:0:0:0 |
| FF02:0:0:0:0:0:0:0 |
| FF03:0:0:0:0:0:0:0 |
| FF04:0:0:0:0:0:0:0 |
| FF05:0:0:0:0:0:0:0 |
| FF06:0:0:0:0:0:0:0 |
| FF07:0:0:0:0:0:0:0 |
| FF08:0:0:0:0:0:0:0 |
| FF09:0:0:0:0:0:0:0 |
| FF0A:0:0:0:0:0:0:0 |
| FF0B:0:0:0:0:0:0:0 |
| FF0C:0:0:0:0:0:0:0 |
| FF0D:0:0:0:0:0:0:0 |
| FF0E:0:0:0:0:0:0:0 |
| FF0F:0:0:0:0:0:0:0 |

Subnet Masking

Both an IPv6 address and IPv6 subnet mask compose of 128-bit binary digits, which are divided into eight 16-bit blocks and written in hexadecimal notation. Hexadecimal uses 4 bits for each character (1 – 10, A – F). Each block's 16 bits are then represented by 4 hexadecimal characters. For example, FFFF:FFFF:FFFF:FFFF:FC00:0000:0000:0000.

Interface ID

In IPv6, an interface ID is a 64-bit identifier. It identifies a physical interface (for example, an Ethernet port) or a virtual interface (for example, the management IP address for a VLAN). One interface should have a unique interface ID.

EUI-64

The EUI-64 (Extended Unique Identifier) defined by the IEEE (Institute of Electrical and Electronics Engineers) is an interface ID format designed to adapt with IPv6. It is derived from the 48-bit (6-byte) Ethernet MAC address as shown next. EUI-64 inserts the hex digits fffe between the third and fourth bytes of the MAC address and complements the seventh bit of the first byte of the MAC address. See the following example.

Table 165

| | | | | | | | | | | | |
|------------|----|---|----|---|----|---|----|---|----|---|----|
| MAC | 00 | : | 13 | : | 49 | : | 12 | : | 34 | : | 56 |
|------------|----|---|----|---|----|---|----|---|----|---|----|

Table 166

| | | | | | | | | | | | | | | | |
|---------------|----|---|----|---|----|---|----|---|----|---|----|---|----|---|----|
| EUI-64 | 02 | : | 13 | : | 49 | : | FF | : | FE | : | 12 | : | 34 | : | 56 |
|---------------|----|---|----|---|----|---|----|---|----|---|----|---|----|---|----|

DHCPv6

The Dynamic Host Configuration Protocol for IPv6 (DHCPv6, RFC 3315) is a server-client protocol that allows a DHCP server to assign and pass IPv6 network addresses, prefixes and other configuration information to DHCP clients. DHCPv6 servers and clients exchange DHCP messages using UDP.

Each DHCP client and server has a unique DHCP Unique Identifier (DUID), which is used for identification when they are exchanging DHCPv6 messages. The DUID is generated from the MAC address, time, vendor assigned ID and/or the vendor's private enterprise number registered with the IANA. It should not change over time even after you reboot the device.

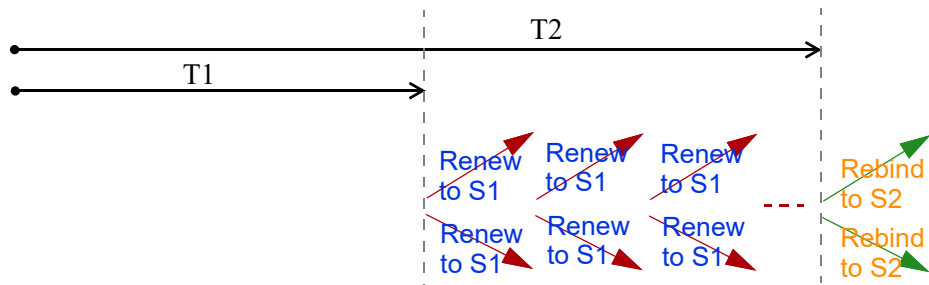
Identity Association

An Identity Association (IA) is a collection of addresses assigned to a DHCP client, through which the server and client can manage a set of related IP addresses. Each IA must be associated with exactly one interface. The DHCP client uses the IA assigned to an interface to obtain configuration from a DHCP server for that interface. Each IA consists of a unique IAID and associated IP information.

The IA type is the type of address in the IA. Each IA holds one type of address. IA_NA means an identity association for non-temporary addresses and IA_TA is an identity association for temporary addresses.

An IA_NA option contains the T1 and T2 fields, but an IA_TA option does not. The DHCPv6 server uses T1 and T2 to control the time at which the client contacts with the server to extend the lifetimes on any addresses in the IA_NA before the lifetimes expire. After T1, the client sends the server (**S1**) (from which the addresses in the IA_NA were obtained) a Renew message. If the time T2 is reached and the server does not respond, the client sends a Rebind message to any available server (**S2**). For an IA_TA, the

client may send a Renew or Rebind message at the client's discretion.



DHCP Relay Agent

A DHCP relay agent is on the same network as the DHCP clients and helps forward messages between the DHCP server and clients. When a client cannot use its link-local address and a well-known multicast address to locate a DHCP server on its network, it then needs a DHCP relay agent to send a message to a DHCP server that is not attached to the same network.

The DHCP relay agent can add the remote identification (remote-ID) option and the interface-ID option to the Relay-Forward DHCPv6 messages. The remote-ID option carries a user-defined string, such as the system name. The interface-ID option provides slot number, port information and the VLAN ID to the DHCPv6 server. The remote-ID option (if any) is stripped from the Relay-Reply messages before the relay agent sends the packets to the clients. The DHCP server copies the interface-ID option from the Relay-Forward message into the Relay-Reply message and sends it to the relay agent. The interface-ID should not change even after the relay agent restarts.

Prefix Delegation

Prefix delegation enables an IPv6 router to use the IPv6 prefix (network address) received from the ISP (or a connected uplink router) for its LAN. The Switch uses the received IPv6 prefix (for example, 2001:db2::/48) to generate its LAN IP address. Through sending Router Advertisements (RAs) regularly by multicast, the Switch passes the IPv6 prefix information to its LAN hosts. The hosts then can use the prefix to generate their IPv6 addresses.

ICMPv6

Internet Control Message Protocol for IPv6 (ICMPv6 or ICMP for IPv6) is defined in RFC 4443. ICMPv6 has a preceding Next Header value of 58, which is different from the value used to identify ICMP for IPv4. ICMPv6 is an integral part of IPv6. IPv6 nodes use ICMPv6 to report errors encountered in packet processing and perform other diagnostic functions, such as "ping".

Neighbor Discovery Protocol (NDP)

The Neighbor Discovery Protocol (NDP) is a protocol used to discover other IPv6 devices and track neighbor's reachability in a network. An IPv6 device uses the following ICMPv6 messages types:

- Neighbor solicitation: A request from a host to determine a neighbor's link-layer address (MAC address) and detect if the neighbor is still reachable. A neighbor being "reachable" means it responds to a neighbor solicitation message (from the host) with a neighbor advertisement message.
- Neighbor advertisement: A response from a node to announce its link-layer address.
- Router solicitation: A request from a host to locate a router that can act as the default router and

forward packets.

- Router advertisement: A response to a router solicitation or a periodical multicast advertisement from a router to advertise its presence and other parameters.

IPv6 Cache

An IPv6 host is required to have a neighbor cache, destination cache, prefix list and default router list. The Switch maintains and updates its IPv6 caches constantly using the information from response messages. In IPv6, the Switch configures a link-local address automatically, and then sends a neighbor solicitation message to check if the address is unique. If there is an address to be resolved or verified, the Switch also sends out a neighbor solicitation message. When the Switch receives a neighbor advertisement in response, it stores the neighbor's link-layer address in the neighbor cache. When the Switch uses a router solicitation message to query for a router and receives a router advertisement message, it adds the router's information to the neighbor cache, prefix list and destination cache. The Switch creates an entry in the default router list cache if the router can be used as a default router.

When the Switch needs to send a packet, it first consults the destination cache to determine the next hop. If there is no matching entry in the destination cache, the Switch uses the prefix list to determine whether the destination address is on-link and can be reached directly without passing through a router. If the address is onlink, the address is considered as the next hop. Otherwise, the Switch determines the next-hop from the default router list or routing table. Once the next hop IP address is known, the Switch looks into the neighbor cache to get the link-layer address and sends the packet when the neighbor is reachable. If the Switch cannot find an entry in the neighbor cache or the state for the neighbor is not reachable, it starts the address resolution process. This helps reduce the number of IPv6 solicitation and advertisement messages.

Multicast Listener Discovery

The Multicast Listener Discovery (MLD) protocol (defined in RFC 2710) is derived from IPv4's Internet Group Management Protocol version 2 (IGMPv2). MLD uses ICMPv6 message types, rather than IGMP message types. MLDv1 is equivalent to IGMPv2 and MLDv2 is equivalent to IGMPv3.

MLD allows an IPv6 switch or router to discover the presence of MLD listeners who wish to receive multicast packets and the IP addresses of multicast groups the hosts want to join on its network.

MLD snooping and MLD proxy are analogous to IGMP snooping and IGMP proxy in IPv4.

MLD filtering controls which multicast groups a port can join.

MLD Messages

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

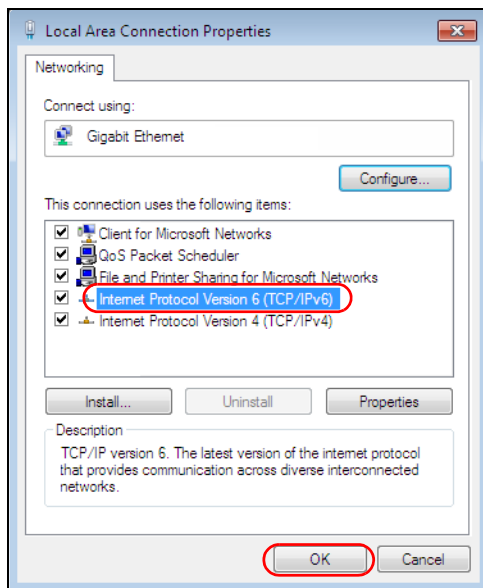
An MLD Done message is equivalent to an IGMP Leave message. When an MLD host wants to leave a multicast group, it can send a Done message to the router or switch. The router or switch then sends a group-specific query to the port on which the Done message is received to determine if other devices connected to this port should remain in the group.

Example – Enabling IPv6 on Windows 7

Windows 7 supports IPv6 by default. DHCPv6 is also enabled when you enable IPv6 on a Windows 7 computer.

To enable IPv6 in Windows 7:

- 1 Select **Control Panel > Network and Sharing Center > Local Area Connection**.
- 2 Select the **Internet Protocol Version 6 (TCP/IPv6)** check box to enable it.
- 3 Click **OK** to save the change.



- 4 Click **Close** to exit the **Local Area Connection Status** screen.
- 5 Select **Start > All Programs > Accessories > Command Prompt**.
- 6 Use the `ipconfig` command to check your dynamic IPv6 address. This example shows a global address (2001:b021:2d::1000) obtained from a DHCP server.

```
C:\>ipconfig

Windows IP Configuration

Ethernet adapter Local Area Connection:

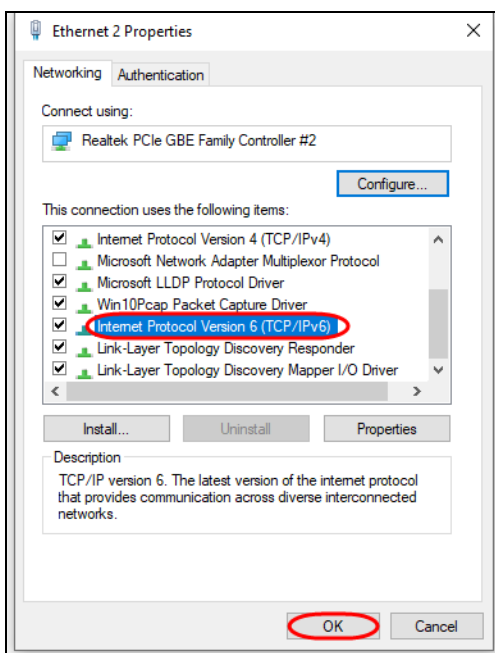
    Connection-specific DNS Suffix  . :
    IPv6 Address. . . . . : 2001:b021:2d::1000
    Link-local IPv6 Address . . . . . : fe80::25d8:dcab:c80a:5189%11
    IPv4 Address. . . . . : 172.16.100.61
    Subnet Mask . . . . . : 255.255.255.0
    Default Gateway . . . . . : fe80::213:49ff:feaa:7125%11
                                172.16.100.254
```

Example – Enabling IPv6 on Windows 10

Windows 10 supports IPv6 by default. DHCPv6 is enabled when you enable IPv6 on a Windows 10 PC.

To enable IPv6 in Windows 10:

- 1 Select **Control Panel > Network and Sharing Center**.
- 2 On the left side of the **Network and Sharing Center**, select **Change adapter settings**.
- 3 Right-click your network connection and select **Properties**.
- 4 Select the **Internet Protocol Version 6 (TCP/IPv6)** check box to enable it.
- 5 Click **OK** to save the changes for the selected network adapter.

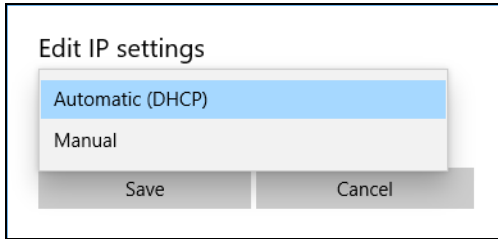


- 6 Click **OK** to exit the selected network adapter **Properties** screen.

Example – Enabling DHCPv6 on Windows 10

Windows 10 supports DHCPv6 by default. To enable DHCPv6 client on your computer:

- 1 Select **Start > Settings > Network & Internet**.
- 2 On the left side of the **Network & Internet**, select **Ethernet**. Then select the Ethernet network you are connected to.
- 3 Under **IP assignment**, select **Edit**.
- 4 Under **Edit IP settings**, select **Automatic (DHCP)** or **Manual**. Then click **Save**.



- When you select **Automatic (DHCP)**, the IP address settings and DNS server address setting are set automatically by your router.
- When you select **Manual**, you can manually set your IP address settings and DNS server address.

Now your computer can obtain an IPv6 address from a DHCPv6 server.

APPENDIX D

Legal Information

Copyright

Copyright © 2024 by Zyxel and/or its affiliates.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel and/or its affiliates.

Published by Zyxel and/or its affiliates. All rights reserved.

Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Regulatory Notice and Statement

United States of America



The following information applies if you use the product within USA area.

US Importer: Zyxel Communications, Inc, 1130 North Miller Street Anaheim, CA92806-2001, <https://www.zyxel.com/us/en/>

Federal Communications Commission (FCC) EMC Statement

- This Switch complies with Part 15 of FCC rules. Operation is subject to the following two conditions:
 - (1) This Switch may not cause harmful interference.
 - (2) This Switch 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 Switch, 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 and United Kingdom



The following information applies if you use the product within the European Union and United Kingdom.

EMC statement

WARNING: This equipment is compliant with Class A of EN55032. In a residential environment this equipment may cause radio interference.

List of National Codes

| COUNTRY | ISO 3166 2 LETTER CODE | COUNTRY | ISO 3166 2 LETTER CODE |
|----------------|------------------------|----------------|------------------------|
| Austria | AT | Liechtenstein | LI |
| Belgium | BE | Lithuania | LT |
| Bulgaria | BG | Luxembourg | LU |
| Croatia | HR | Malta | MT |
| Cyprus | CY | Netherlands | NL |
| Czech Republic | 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 Switch to dampness, dust or corrosive liquids.
- Do NOT store things on the Switch.
- Do NOT obstruct the Switch ventilation slots as insufficient airflow may harm your Switch. For example, do not place the Switch in an enclosed space such as a box or on a very soft surface such as a bed or sofa.
- Do NOT install or service this Switch during a thunderstorm. There is a remote risk of electric shock from lightning.
- Connect ONLY suitable accessories to the Switch.
- Do NOT open the Switch 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 Switch. 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 Switch 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, 120V AC in North America or 230V AC in Europe). If the power adaptor or cord is damaged, it might cause electrocution. Remove it from the Switch 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 Switch 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 Switch. 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 Switch. 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) Switches that supply or receive power and their connected Ethernet cables must all be completely indoors.
- The following warning statements apply, where the disconnect Switch is not incorporated in the Switch or where the plug on the power supply cord is intended to serve as the disconnect Switch,
 - For PERMANENTLY CONNECTED SWITCHES, a readily accessible disconnect Switch shall be incorporated external to the Switch;
 - For PLUGGABLE SWITCHES, the socket-outlet shall be installed near the Switch and shall be easily accessible.
- This Switch must be grounded by qualified service personnel. Never defeat the ground conductor or operate the Switch in the absence of a suitably installed ground conductor. Contact the appropriate electrical inspection authority or an electrician if you are uncertain that suitable grounding is available.
- If your Switch has an earthing screw (frame ground), connect the screw to a ground terminal using an appropriate AWG ground wire. Do this before you make other connections.
- If your Switch has no earthing screw, but has a 3-prong power plug, make sure to connect the plug to a 3-hole earthed socket.
- When connecting or disconnecting power to hot-pluggable power supplies, if offered with your system, observe the following guidelines:
 - Install the power supply before connecting the power cable to the power supply.
 - Unplug the power cable before removing the power supply.
 - If the system has multiple sources of power, disconnect power from the system by unplugging all power cables from the power supply.
- CLASS 1 LASER PRODUCT
- APPAREIL À LASER DE CLASS 1

- PRODUCT COMPLIES WITH 21 CFR 1040.10 AND 1040.11.
- PRODUIT CONFORME SELON 21 CFR 1040.10 ET 1040.11.

Important Safety Instructions


- 1 Warning! Energy Hazard. Remove all metal jewelry, watches, and so on from your hands and wrists before serving this Switch.
- 2 Caution! The RJ-45 jacks are not used for telephone line connection.

- 3  Hazardous Moving Parts. Keep body parts away from fan blades.

- 4  Hot Surface. Do not touch.

- 1 Avertissement: Risque de choc électrique. Retirer tout bijoux en métal et votre montre de vos mains et poignets avant de manipuler cet appareil.

- 2 Attention: Les câbles RJ-45 ne doivent pas être utilisés pour les connections téléphoniques.

- 3  Mobilité des pièces détachées. S'assurer que les pièces détachées ne sont pas en contact avec les pales du ventilateur.

- 4  Surface brûlante. Ne pas toucher.

Environment Statement

Disposal and Recycling Information

The symbol below means that according to local regulations your product and/or its battery shall be disposed of separately from domestic waste. If this product is end of life, take it to a recycling station designated by local authorities. At the time of disposal, the separate collection of your product and/or its battery will help save natural resources and ensure that the environment is sustainable development.

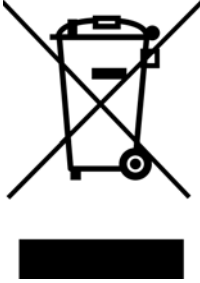
Die folgende Symbol bedeutet, dass Ihr Produkt und/oder seine Batterie gemäß den örtlichen Bestimmungen getrennt vom Hausmüll entsorgt werden muss. Wenden Sie sich an eine Recyclingstation, wenn dieses Produkt das Ende seiner Lebensdauer erreicht hat. Zum Zeitpunkt der Entsorgung wird die getrennte Sammlung von Produkt und/oder seiner Batterie dazu beitragen, natürliche Ressourcen zu sparen und die Umwelt und die menschliche Gesundheit zu schützen.

El símbolo de abajo indica que según las regulaciones locales, su producto y/o su batería deberán depositarse como basura separada de la doméstica. Cuando este producto alcance el final de su vida útil, llévelo a un punto limpio. Cuando llegue el momento de desechar el producto, la recogida por separado éste y/o su batería ayudará a salvar los recursos naturales y a proteger la salud humana y medioambiental.

Le symbole ci-dessous signifie que selon les réglementations locales votre produit et/ou sa batterie doivent être éliminés séparément des ordures ménagères. Lorsque ce produit atteint sa fin de vie, amenez-le à un centre de recyclage. Au moment de la mise au rebut, la collecte séparée de votre produit et/ou de sa batterie aidera à économiser les ressources naturelles et protéger l'environnement et la santé humaine.

Il simbolo sotto significa che secondo i regolamenti locali il vostro prodotto e/o batteria deve essere smaltito separatamente dai rifiuti domestici. Quando questo prodotto raggiunge la fine della vita di servizio portarlo a una stazione di riciclaggio. Al momento dello smaltimento, la raccolta separata del vostro prodotto e/o della sua batteria aiuta a risparmiare risorse naturali e a proteggere l'ambiente e la salute umana.

Symbolen innebär att enligt lokal lagstiftning ska produkten och/eller dess batteri kastas separat från hushållsavfallet. När den här produkten når slutet av sin livslängd ska du ta den till en återvinningsstation. Vid tiden för kasseringen bidrar du till en bättre miljö och mänsklig hälsa genom att göra dig av med den på ett återvinningsställe.



台灣

以下訊息僅適用於產品銷售至台灣地區

- 這是甲類的資訊產品，在居住的環境中使用時，可能會造成射頻干擾，在這種情況下，使用者會被要求採取某些適當的對策。
- 為避免電磁干擾，本產品不應安裝或使用於住宅環境。


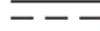


安全警告 – 為了您的安全，請先閱讀以下警告及指示：

- 請勿將此產品接近水、火焰或放置在高溫的環境。
- 避免設備接觸
 - 任何液體 - 切勿讓設備接觸水、雨水、高濕度、污水腐蝕性的液體或其他水份。
 - 灰塵及污物 - 切勿接觸灰塵、污物、沙土、食物或其他不合適的材料。
- 雷雨天氣時，不要安裝或維修此設備。有遭受電擊的風險。
- 切勿重摔或撞擊設備，並勿使用不正確的電源變壓器。
- 若接上不正確的電源變壓器會有爆炸的風險。
- 請勿隨意更換產品內的電池。
- 如果更換不正確之電池型式，會有爆炸的風險，請依製造商說明書處理使用過之電池。
- 請將廢電池丟棄在適當的電器或電子設備回收處。
- 請勿將設備解體。
- 請勿阻礙設備的散熱孔，空氣對流不足將會造成設備損害。
- 請使用隨貨提供或指定的連接線 / 電源線 / 電源變壓器，將其連接到合適的供應電壓 (如：台灣供應電壓 110 伏特)。
- 假若電源變壓器或電源變壓器的纜線損壞，請從插座拔除，若您還繼續插電使用，會有觸電死亡的風險。
- 請勿試圖修理電源變壓器或電源變壓器的纜線，若有毀損，請直接聯絡您購買的店家，購買一個新的電源變壓器。
- 請勿將此設備安裝於室外，此設備僅適合放置於室內。
- 請勿隨一般垃圾丟棄。
- 請參閱產品背貼上的設備額定功率。
- 請參考產品型錄或是彩盒上的作業溫度。
- 設備必須接地，接地導線不允許被破壞或沒有適當安裝接地導線，如果不確定接地方式是否符合要求可聯繫相應的電氣檢驗機構檢驗。
- 如果您提供的系統中有提供熱插拔電源，連接或斷開電源請遵循以下指導原則：
 - 先連接電源線至設備連，再連接電源。
 - 先斷開電源再拔除連接至設備的電源線。
 - 如果系統有多個電源，需拔除所有連接至電源的電源線再關閉設備電源。
- 產品沒有斷電裝置或者採用電源線的插頭視為斷電裝置的一部分，以下警語將適用：
 - 對永久連接之設備，在設備外部須安裝可觸及之斷電裝置；
 - 對插接式之設備，插座必須接近安裝之地點而且是易於觸及的。

About the Symbols

Various symbols are used in this product to ensure correct usage, to prevent danger to the user and others, and to prevent property damage. The meaning of these symbols are described below. It is important that you read these descriptions thoroughly and fully understand the contents.

Explanation of the Symbols

| SYMBOL | EXPLANATION |
|---|--|
|  | Alternating current (AC): AC is an electric current in which the flow of electric charge periodically reverses direction. |
|  | Direct current (DC): DC is the unidirectional flow or movement of electric charge carriers. |
|  | Earth; ground: A wiring terminal intended for connection of a Protective Earthing Conductor. |
|  | Class II equipment: The method of protection against electric shock in the case of class II equipment is either double insulation or reinforced insulation. |

Viewing Certifications

Go to <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 Switch at http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online at www.zyxel.com to receive email notices of firmware upgrades and related information.

Trademarks

The trademarks mentioned in this publication are used for identification purposes only and may be properties of their respective owners.

Numbers

802.1P priority [97](#)

A

AAA [173](#)

- accounting [173](#)
- authentication [173](#)
- authorization [173](#)
- external server [173](#)
- RADIUS [173](#)

AAA (Authentication, Authorization and Accounting) [173](#)

access control

- account security [268](#)
- limitations [259](#)
- login account [265](#)
- overview [259](#)
- remote management [267](#)
- service port [266](#)
- SNMP [270](#)

Access Control screen [259](#)

account security [268](#)

Account Security screen [269](#)

accounting

- setup [176](#)

Address Resolution Protocol (ARP) [242](#), [297](#), [300](#), [301](#)

admin [269](#)

administrator password [43](#), [265](#)

aging time [89](#)

air circulation

- for cooling [27](#)

All connected

- Setting Wizard [132](#)

applications

- backbone [23](#)
- bridging [24](#)
- IEEE 802.1Q VLAN [25](#)
- PoE [23](#)

switched workgroup [24](#)

ARP

- how it works [242](#)
- learning mode [242](#)
- overview [242](#)
- setup [244](#)

ARP (Address Resolution Protocol) [297](#)

ARP Learning screen [244](#)

ARP Setup screen [244](#)

ARP Table screen [297](#)

ARP-Reply [242](#)

ARP-Request [243](#)

ATM (Asynchronous Transmission Mode) [25](#)

authentication

- setup [176](#)

authentication, authorization and accounting [173](#)

authorization

- setup [176](#)

authorized technician

- install the Switch [27](#)

auto-crossover port [34](#)

auto-fan [18](#)

auto-MDIX port [34](#)

B

back up

- configuration file [252](#)

Backup Configuration screen [252](#)

bandwidth control [146](#), [147](#)

- egress rate [147](#)
- ingress rate [147](#)
- setup [146](#)

Bandwidth Control screen [146](#)

basic settings [85](#)

basic setup tutorial [70](#)

Basic TLV Setting screen [219](#)

binding table

- building [181](#)

BPDUs [141](#)
 Bridge Protocol Data Units (BPDUs) [141](#)
 bridging application [24](#)
 broadcast storm control [148](#)
 Wizard [53](#)

C

cables
 supported [22](#)
 Certificates screen [254](#)
 certifications
 viewing [334](#)
 CFI (Canonical Format Indicator) [119](#)
 changing the password [62](#)
 Class of Service [226](#)
 clearance
 Switch installation [27](#)
 cloning a port, see port cloning
 Cloud Connection Status [81](#)
 cluster management [288](#)
 and switch passwords [291](#)
 cluster manager [288](#), [290](#)
 cluster member [288](#), [290](#)
 cluster member firmware upgrade [292](#)
 network example [288](#)
 setup [290](#)
 specification [288](#)
 status [289](#)
 switch models [288](#)
 VID [290](#)
 Web Configurator [291](#)
 Cluster Management Configuration screen [290](#)
 cluster manager [288](#)
 configuration
 back up [26](#)
 change running config [248](#)
 saving [63](#)
 configuration file
 backup [252](#)
 restore [251](#)
 save [248](#)
 Configure Clone screen [300](#)
 contact information [314](#)
 copying port settings, see port cloning

copyright [330](#)
 CoS [226](#)
 CPU management port [130](#)
 CPU protection [195](#)
 crossover Ethernet cable [34](#)
 current date [88](#)
 current time [87](#)
 customer support [314](#)

D

date
 current [88](#)
 daylight saving time [88](#)
 DHCP
 configuration options [230](#)
 Dynamic Host Configuration Protocol [230](#)
 modes [230](#)
 Relay Agent Information format [232](#)
 setup [231](#)
 DHCP Option 82 Profile screen [233](#)
 DHCP relay
 configure [76](#)
 tutorial [73](#)
 DHCP relay agent [325](#)
 DHCP relay option 82 [190](#)
 DHCP Relay screen [234](#), [236](#)
 DHCP screen [231](#)
 DHCP server
 block [181](#)
 DHCP snooping [70](#), [189](#)
 configure [191](#)
 DHCP relay option 82 [190](#)
 trusted ports [189](#)
 untrusted ports [190](#)
 DHCP Snooping Configure screen [185](#)
 DHCP snooping database [190](#)
 DHCP Snooping Port Configure screen [72](#), [186](#)
 DHCP Snooping screen [182](#)
 DHCP Snooping VLAN Configure screen [187](#)
 DHCP Status screen [231](#)
 DHCP Unique IDentifier (DUID) [324](#)
 DHCP-assigned IP [311](#)
 DHCPv4

- global relay [234](#)
- global relay example [236](#)
- Option 82 [232](#)
- option 82 profiles [233](#)
- Relay Agent Information [232](#)
- DHCPv4 relay [231](#)
- DHCPv6
 - enable in Windows 10 [328](#)
- DHCPv6 Client Setup screen [114](#)
- DHCPv6 relay [240](#)
 - interface-ID [240](#)
 - remote-ID [240](#)
- DHCPv6 Relay screen [240](#)
- diagnostics [281](#)
 - Ethernet port test [282](#)
 - ping [282](#)
- Differentiated Service (DiffServ) [226](#)
- DiffServ [226](#)
 - activate [227](#)
 - DS field [226](#)
 - DSCP [226](#)
 - network example [227](#)
 - PHB [226](#)
 - service level [226](#)
- DiffServ Code Points [226](#)
- disclaimer [330](#)
- disposal and recycling information
 - EU [332](#)
- DS (Differentiated Services) [226](#)
- DSCP [226](#)
 - what it does [226](#)
- dual firmware images [250](#)
- duplex mode [34](#)
- Dynamic Host Configuration Protocol for IPv6 (DHCPv6) [324](#)
- dynamic link aggregation [152](#)

E

- egress port [132](#)
- egress rate [147](#)
- electrical inspection authority [36](#)
- electrician [37](#)
- EMC statement [330](#)
- Environment Statement [332](#)

- Errdisable Detect screen [199](#)
- Errdisable Recovery screen [200](#)
- Errdisable screen [196](#)
- errdisable status [198](#)
- error disable [195](#)
 - control packets [197](#)
 - CPU protection [198](#)
 - detect [199](#)
 - recovery [200](#)
 - status [196](#)
- error-disable recovery [195](#)
- Ethernet broadcast address [242, 297](#)
- Ethernet MAC [86](#)
- Ethernet port
 - auto-crossover [34](#)
 - auto-negotiating [34](#)
- Ethernet port test [282](#)
- Ethernet ports
 - number of [18](#)
- Ethernet settings
 - default [34](#)
- external authentication server [174](#)

F

- FCC interference statement [330](#)
- file transfer using FTP
 - command example [257](#)
- filename convention, configuration
 - file names [256](#)
- filtering [138](#)
 - rules [138](#)
- filtering database, MAC table [294](#)
- Filtering screen [138](#)
- firmware
 - upgrade [250, 292](#)
 - ZyNOS [86](#)
- Firmware Upgrade screen [250](#)
- flow control [97](#)
 - back pressure [97](#)
 - IEEE802.3x [97](#)
- frames
 - tagged [125](#)
 - untagged [125](#)

freestanding installation

precautions [28](#)

front panel [33](#)

FTP [256](#)

file transfer procedure [257](#)

restrictions over WAN [258](#)

full duplex

Ethernet port [34](#)

G

general setup [86](#)

General Setup screen [86](#)

getting help [64](#)

GMT (Greenwich Mean Time) [88](#)

gratuitous ARP [243](#)

green Ethernet [202](#)

and uplink port [202](#)

auto power down [202](#)

EEE [202](#)

short reach [202](#)

grounding

for safety [35](#)

GS1350 Series

comparison table [18](#)

models [18](#)

H

half duplex

Ethernet port [34](#)

hardware features [18](#)

hardware installation [27](#)

hardware overview [33](#)

HTTPS [275](#)

certificates [275](#)

implementation [275](#)

public keys, private keys [275](#)

HTTPS Certificates screen [255](#)

HTTPS example [275](#)

I

IANA (Internet Assigned Number Authority) [319](#)

Identity Association (IA) [324](#)

IEEE 802.3af [22](#)

IEEE 802.3at [22](#)

IEEE 802.3az [202](#)

IEEE standard [22](#)

IGMP leave timeout

fast [170](#)

IGMP snooping [167](#)

IGMP snooping and VLANs [168](#)

ingress port [132](#)

ingress rate [147](#)

initial setup [65](#)

Innovation, Science and Economic Development

Canada ICES statement [330](#)

installation

air circulation [27](#)

desktop [27](#)

freestanding [27](#)

rack-mounting [30](#)

wall mounting [28](#)

installation requirements

wall mounting [28](#)

installation scenarios [27](#)

Interface Setup screen [103](#)

Internet Protocol version 6, see IPv6

IP

configuration [93](#)

interface [90](#)

routing domain [90](#)

status [91](#)

IP address [92](#)

Switch management [67](#)

IP Setup screen [68, 90](#)

IP Status Detail screen [91](#)

IP subnet mask [92](#)

IPv6 [322](#)

addressing [322](#)

enable in Windows 10 [328](#)

enable in Windows 7 [327](#)

EUI-64 [324](#)

global address [322](#)

interface ID [324](#)

link-local address [322](#)

- Neighbor Discovery Protocol [322](#)
 - neighbor table [302](#)
 - ping [322](#)
 - prefix [322](#)
 - prefix length [322](#)
 - unspecified address [323](#)
 - IPv6 cache [326](#)
 - IPv6 Configuration screen [107](#)
 - IPv6 Global Address Setup screen [111](#)
 - IPv6 Global Setup screen [108](#)
 - IPv6 interface [103](#)
 - DHCPv6 client [114](#)
 - enable [109](#)
 - global address [111](#)
 - global unicast address [106](#)
 - link-local address [110](#)
 - link-local IP [106](#)
 - neighbor discovery [112](#)
 - neighbor table [113](#)
 - status [105](#)
 - IPv6 Interface Setup screen [109](#)
 - IPv6 Interface Status screen [106](#)
 - IPv6 Link-Local Address Setup screen [110](#)
 - IPv6 Neighbor Setup screen [113](#)
 - IPv6 Neighbor Table screen [302](#)
 - IPv6 screen [104](#)
- J**
- Java permission [40, 312](#)
 - JavaScript [40, 312](#)
- L**
- LACP [152](#)
 - system priority [157](#)
 - timeout [157](#)
 - LEDs [37](#)
 - limit MAC address learning [160](#)
 - link aggregation [52, 152](#)
 - dynamic [152](#)
 - ID information [153](#)
 - setup [154](#)
 - traffic distribution algorithm [154](#)
 - traffic distribution type [155](#)
 - trunk group [152](#)
 - link aggregation (trunking)
 - example [24](#)
 - Link Aggregation Control Protocol (LACP) [152](#)
 - Link Aggregation screen
 - Wizard [51](#)
 - Link Layer Discovery Protocol [204](#)
 - LLDP [204](#)
 - basic TLV [219](#)
 - global settings [218](#)
 - local port status [208](#)
 - organization-specific TLV [220](#)
 - status of remote device [212](#)
 - TLV [204](#)
 - LLDP (Link Layer Discovery Protocol) [204](#)
 - LLDP screen [206](#)
 - LLDP-MED [205](#)
 - classes of endpoint devices [205](#)
 - example [205](#)
 - LLDP-MED Configuration screen [221](#)
 - LLDP-MED Location screen [223](#)
 - lockout [63](#)
 - Switch [63](#)
 - log message [284](#)
 - login [40](#)
 - password [62](#)
 - privilege level [266](#)
 - login account
 - administrator [265](#)
 - non-administrator [265](#)
 - login accounts [265](#)
 - configuring through Web Configurator [265](#)
 - multiple [265](#)
 - number of [265](#)
 - login user name
 - display [269](#)
 - Logins screen [265](#)
 - loop guard [192](#)
 - examples [193](#)
 - port shut down [193](#)
 - setup [194](#)
 - vs. STP [192](#)
 - Wizard [53](#)

M

MAC (Media Access Control) [86](#)

MAC address [86](#), [297](#)

- maximum number per port [160](#)

MAC address learning [89](#), [160](#)

- specify limit [160](#)

MAC Based VLAN screen [127](#)

MAC freeze [160](#)

MAC table [294](#)

- display criteria [296](#)
- how it works [294](#)
- sorting criteria [296](#)
- transfer type [296](#)
- viewing [295](#)

MAC-based VLAN [127](#)

maintenance [246](#)

- configuration backup [252](#)
- current configuration [247](#)
- firmware [250](#)
- main screen [247](#)
- restore configuration [251](#)

Maintenance screen [246](#)

Management Information Base (MIB) [271](#)

management IP address [67](#)

management mode [19](#)

- change [20](#)

management port [132](#)

managing the Switch

- cluster management [26](#)
- good habits [26](#)
- NCC [26](#)
- using FTP, see FTP [26](#)
- using SNMP [26](#)
- Web Configurator [26](#)
- ZON Utility [26](#)

maximum transmission unit [299](#)

Maximum Transmission Unit (MTU) [106](#)

Mbuf (Memory Buffer) [253](#)

MDIX (Media Dependent Interface Crossover) [34](#)

Media Access Control [86](#)

Memory Buffer [253](#)

MIB

- and SNMP [271](#)
- supported MIBs [271](#)

MIB (Management Information Base) [271](#)

mirroring ports [150](#)

monitor port [150](#)

mounting brackets

- attaching [31](#)

MTU [299](#)

MTU (Multi-Tenant Unit) [88](#)

multicast

- IP addresses [167](#)
- setup [168](#)

multicast IP address [135](#)

multicast MAC address [135](#)

multi-gigabit ports [34](#)

Multi-Tenant Unit [88](#)

myZyxel account [20](#)

N

navigation panel [60](#)

NCC registration [20](#)

Nebula Cloud Management [19](#)

Nebula setup wizard

- select site [20](#)

Nebula web portal [19](#)

Neighbor Detail screen [82](#)

Neighbor Discovery Protocol (NDP) [325](#)

network applications [22](#)

network management system (NMS) [270](#)

NTP (RFC-1305) [87](#)

O

one-time schedule [162](#)

Option 82 [232](#)

Organizationally Unique Identifiers (OUI) [126](#)

Org-specific TLV Setting screen [220](#)

overheating

- prevention [27](#)

P

password [62](#)

- administrator [43, 265](#)
 - change [26](#)
 - change through Wizard [50](#)
 - display [269](#)
 - write down [26](#)
 - password change
 - through Password / SNMP link [42](#)
 - password encryption
 - activate [269](#)
 - Path MTU Discovery [299](#)
 - Path MTU Table screen [299](#)
 - Per-Hop Behavior [226](#)
 - PHB [226](#)
 - ping, test connection [282](#)
 - PoE
 - PD priority [102](#)
 - power management mode [102](#)
 - power-up mode [100](#)
 - PoE (Power over Ethernet) [97](#)
 - PoE features
 - by model [22](#)
 - PoE ports
 - number of [18](#)
 - PoE Setup screen [100](#)
 - PoE standards [22](#)
 - PoE Status screen [98](#)
 - PoE Time Range Setup screen [100](#)
 - PoE type [22](#)
 - port
 - maximum power [22](#)
 - setup [96](#)
 - voltage range [22](#)
 - port cloning [300, 301](#)
 - advanced settings [300, 301](#)
 - basic settings [300, 301](#)
 - port details [305](#)
 - port isolation
 - Setting Wizard [132](#)
 - port mirroring [150](#)
 - port redundancy [152](#)
 - Port screen
 - DHCP snooping [188](#)
 - DHCPv4 Global Relay [235](#)
 - DHCPv4 VLAN [238](#)
 - port security [159](#)
 - address learning [160](#)
 - limit MAC address learning [160](#)
 - setup [159](#)
 - Port Setup screen [96](#)
 - port status [304](#)
 - port details [305](#)
 - port utilization [308](#)
 - port utilization [308](#)
 - Port VID (PVID) [66](#)
 - port VLAN ID, see PVID [125](#)
 - port VLAN trunking [119](#)
 - port-based VLAN [130](#)
 - all connected [132](#)
 - configure [130](#)
 - port isolation [132](#)
 - settings wizard [132](#)
 - ports
 - diagnostics [282](#)
 - mirroring [150](#)
 - speed/duplex [96](#)
 - standby [153](#)
 - power
 - maximum per port [22](#)
 - Power Budget
 - PoE [22](#)
 - power connection [37](#)
 - power management mode
 - PoE [22](#)
 - power module
 - disconnecting [37](#)
 - Power Sourcing Equipment (PSE) [22](#)
 - powered device (PD) [22, 97](#)
 - prefix delegation [325](#)
 - priority level
 - queue assignment [90](#)
 - priority queue assignment [90](#)
 - product registration [334](#)
 - PVID [119](#)
- ## Q
- QoS [226](#)
 - priority setting [58](#)
 - QoS setting [57](#)
 - Quality of Service [226](#)

queue weight [165](#)
 queuing [164, 165](#)
 SPQ [164](#)
 WRR [164](#)
 queuing method [164, 166](#)

R

rack-mount [18](#)
 rack-mounting [30](#)
 installation requirements [30](#)
 precautions [31](#)
 RADIUS [174, 259](#)
 advantages [174](#)
 and tunnel protocol attribute [179](#)
 setup [174](#)
 Rapid Spanning Tree Protocol (RSTP) [140](#)
 rear panel [35](#)
 reboot
 load configuration [248](#)
 reboot system [248](#)
 recurring schedule [162](#)
 registration
 product [334](#)
 Regulatory Notice and Statement [330](#)
 remote management [267](#)
 service [268](#)
 trusted computers [268](#)
 resetting [64, 248, 249](#)
 to custom default settings [249](#)
 to factory default settings [248, 249](#)
 restore
 configuration [26](#)
 RESTORE button [64](#)
 restore configuration [64, 251](#)
 RFC 3164 [285](#)
 Round Robin Scheduling [164](#)
 Router Advertisement (RA) [325](#)
 routing domain [90](#)
 RSTP
 configuration [143](#)
 rubber feet [18](#)
 attach [28](#)
 running configuration [248](#)

erase [248](#)
 reset [248](#)

S

safety precautions
 using the Switch [27](#)
 safety warnings [331](#)
 save configuration [63, 248](#)
 Save link [63](#)
 schedule
 one-time [162](#)
 recurring [162](#)
 type [163](#)
 screw anchors
 using [29](#)
 screw specification
 for wall mounting [28](#)
 Secure Shell, see SSH
 service access control [266](#)
 service port [267](#)
 Setup Wizard
 parts [48](#)
 Setup Wizard screen [42](#)
 SFP/SFP+ slot [35](#)
 Simple Network Management Protocol, see SNMP
 SNMP [270](#)
 agent [270](#)
 and MIB [271](#)
 authentication [264](#)
 communities [44, 261](#)
 management model [270](#)
 manager [270](#)
 MIB [271](#)
 network components [270](#)
 object variables [271](#)
 protocol operations [271](#)
 security [264](#)
 security level [264](#)
 setup [260](#)
 traps [261](#)
 users [263](#)
 version 3 and security [271](#)
 versions supported [270](#)
 SNMP agent
 enable through Wizard [50](#)

- SNMP traps [271](#)
 - supported [272, 273](#)
 - SNMP version
 - select [51](#)
 - SPQ (Strict Priority Queuing) [164](#)
 - SSH
 - encryption methods [274](#)
 - how it works [273](#)
 - implementation [274](#)
 - SSH (Secure Shell) [273](#)
 - SSL (Secure Socket Layer) [275](#)
 - standby ports [153](#)
 - static MAC address [133](#)
 - static MAC forwarding [133](#)
 - Static MAC Forwarding screen [133](#)
 - static multicast forwarding [135](#)
 - Static Multicast Forwarding screen [136](#)
 - static VLAN [123](#)
 - control [123](#)
 - tagging [124](#)
 - Static VLAN screen [66](#)
 - status [58, 78](#)
 - port [304](#)
 - STP [142](#)
 - VLAN [120](#)
 - Status screen [78](#)
 - STP
 - bridge ID [142](#)
 - bridge priority [144](#)
 - designated bridge [141](#)
 - edge port [145](#)
 - forwarding delay [144](#)
 - Hello BPDU [141](#)
 - Hello Time [142, 144](#)
 - how it works [141](#)
 - Max Age [142, 144](#)
 - path cost [140, 145](#)
 - port priority [145](#)
 - port role [143](#)
 - port state [141, 143](#)
 - root port [141](#)
 - status [142](#)
 - terminology [140](#)
 - vs. loop guard [192](#)
 - STP Path Cost [141](#)
 - straight-through Ethernet cable [34](#)
 - subnet masking [324](#)
 - Switch
 - DHCP client [40](#)
 - fanless-type usage precaution [27](#)
 - fan-type usage precaution [27](#)
 - switch lockout [63](#)
 - Switch reset [64](#)
 - Switch Setup screen [88](#)
 - Switch's QR code [20](#)
 - syslog [285](#)
 - protocol [285](#)
 - settings [285](#)
 - setup [285](#)
 - severity levels [285](#)
 - Syslog Setup screen [285](#)
 - System Info screen [85](#)
 - system reboot [248](#)
- ## T
- tag-based VLAN
 - example [25](#)
 - tagged VLAN [118](#)
 - Tech-Support [252](#)
 - log enhancement [252](#)
 - Tech-Support screen [252](#)
 - time
 - current [87](#)
 - daylight saving [88](#)
 - format [87](#)
 - Time (RFC-868) [87](#)
 - time range [162](#)
 - time server [87](#)
 - time service protocol [87](#)
 - ToS [226](#)
 - trademarks [334](#)
 - Trap Group screen [261](#)
 - traps
 - destination [261](#)
 - troubleshooting [76](#)
 - trunk group [152](#)
 - Trunk Tagged port [57](#)
 - trunking [152](#)
 - trusted ports
 - DHCP snooping [189](#)

tunnel protocol attribute
and RADIUS [179](#)

tutorial
basic setup [70](#)
DHCP snooping [70](#)

twisted pair
used [22](#)

Type of Service [226](#)

U

untrusted ports
DHCP snooping [190](#)

uplink connection
super-fast [24](#)

User Information screen
SNMP [263](#)

user name [41](#)
default [41](#)

user profiles [174](#)

UTC (Universal Time Coordinated) [88](#)

V

Vendor ID Based VLAN screen [128](#)

Vendor Specific Attribute, see VSA [178](#)

ventilation holes [27](#)

VID [94](#), [121](#), [122](#)
number of possible VIDs [119](#)
priority frame [119](#)

VID (VLAN Identifier) [119](#)

Virtual Local Area Network [88](#)

VLAN [88](#)
acceptable frame type [125](#)
and IGMP snooping [168](#)
creation [65](#), [74](#)
ID [118](#)
ingress filtering [125](#)
introduction [88](#), [118](#)
number of VLANs [121](#)
port number [122](#)
port settings [124](#)
port-based [132](#)
port-based VLAN [130](#)

port-based, isolation [132](#)
port-based, wizard [132](#)
PVID [125](#)
static VLAN [123](#)
status [120](#), [121](#), [122](#)
tagged [118](#)
trunking [119](#), [125](#)
type [89](#), [120](#)

VLAN (Virtual Local Area Network) [88](#)

VLAN ID [118](#)

VLAN member port [57](#)

VLAN number [92](#), [94](#)

VLAN setting
Wizard [56](#)

VLAN Setting screen [239](#)
DHCPv4 [237](#)

VLAN trunking [125](#)

VLAN-unaware devices [66](#)

voice VLAN [125](#)

Voice VLAN Setup screen [126](#)

voltage range
port [22](#)

VSA [178](#)

W

wall mounting [28](#)

wall-mount [18](#)

warranty
note [334](#)

Web browser pop-up window [40](#), [312](#)

Web Configurator
getting help [64](#)
home [58](#)
home screen [59](#)
login [40](#)
logout [64](#)
navigating components [59](#)
navigation panel [60](#)
online help [64](#)
usage prerequisite [40](#)

weight [165](#)

Windows OS version
check [44](#)

WRR (Weighted Round Robin Scheduling) [164](#)

Z

ZDP [44](#)

ZON Utility [44](#)

compatible OS [44](#)

fields description [48](#)

icon description [47](#)

installation requirements [44](#)

introduction [22](#)

minimum hardware requirements [45](#)

network adapter select [46](#)

password prompt [47](#)

run [45](#)

supported firmware version [45](#)

supported models [45](#)

Switch IP address [40](#)

ZON utility

use for troubleshooting [311](#)

ZyNOS (Zyxel Network Operating System) [256](#)

Zyxel AP Configurator (ZAC) [48](#)

Zyxel Discovery Protocol (ZDP) [44](#)

Zyxel Nebula Mobile App

register the Switch [20](#)

Zyxel One Network (ZON) Utility [21](#)