EtherWAN



Hardened Managed Ethernet Switch
Firmware 5.0

User's Guide

FastFind Links

Computer Setup

Setting the initial IP address

All Rights Reserved

Dissemination or reproduction of this document, or its contents, is not authorized except where expressly permitted. Violators are liable for damages. All rights reserved, for the purposes of patent application or trademark registration.

Disclaimer of Liability

The information contained in this document is subject to change without notice. EtherWAN is not liable for any errors or omissions contained herein or for resulting damage in connection with the information provided in this manual.

Registered Trademarks

The following words and phrases are registered Trademarks of EtherWAN Systems Inc.

EtherWAN

All other Trademarks are property of their respective owners.

Warranty

For details on the EtherWAN warranty replacement policy, please visit our web site at: www.etherwan.com

Contact EtherWAN Systems

Corporate Headquarters
EtherWAN Systems Inc.
2301 E Winston Rd Anaheim
Anaheim, CA 92806
Tel: (714) 779 3800
Fax: (714) 779 3806
Email: support@etherwan.com

Table of Contents

Preface xvii

Applicable Models xvii
NOTE ON GRAPHICAL USER INTERFACE xviii
Safety and Warnings xviii
Typographic Conventions xviii

Computer Setup 19

Management Methods and Protocols 19
Default IP 19
Login Process and Default Credentials 20

Setting the initial IP address 21

Simple IP Addressing 21

CLI Command Usage 22

Navigating the CLI Hierarchy 23
CLI Keyboard Shortcuts 23
Command Syntax 24
Variable Placeholders 24
CLI Command modes 24
Global Configuration Mode 24
MSTP Configuration Mode 25
Interface Configuration Mode 25
VLAN Database Configuration Mode 26
Router Configuration Mode 26
Saving a Configuration from the CLI 26
Command Help 26

System Menu (web interface) 27

System Information 27
System Name/Password 28
System Name/Password using the CLI 29
Show Switch Model/Serial Number using the CLI 30
IP Address 31
Static IP 31
DHCP Client 31
Default Gateway 31
DNS Server 31
IP Address - Configuration using the CLI 32

Set the IP Address 32
Set the Default Gateway 33
Set the Domain Name Server (DNS) 34
Enable/Disable DHCP Client on a VLAN 35
Enable/Disable Static IP on a VLAN 35
Set the IPv6 Address of an Interface 36
Set the IPv6 Address through DHCP 36
Enable/Disable DHCP Server for IPv6 37
Configure DHCPv6 server settings 37
IPv6 Address 37
IP Address - Configuration using the CLI 38
Set the IPv6 Address 38
Configure IPv6 Neighbor Discovery 38
Management Interface 38
HTTPS 39
Login Failure Lock 39
Session Time Out 39
Telnet 40
SSH (Secure Shell) 40
SSL (Secure Socket Layer) 41
Management Interface Configuration using the CLI 42
Enabling/Disabling Telnet 42
Enabling/Disabling SSH 43
Enabling/Disabling HTTP and/or HTTPS 44
Save Configuration Page 45
Backup Configuration to server 45
Load Configuration from server 46
Save Configuration 46
Restore Default 46
Restore Configuration from USB 47
Auto Save 47
Reset Button Setting 48
Save Configuration Page using the CLI 48
Saving a Configuration 48
Restore Default Settings 48
Load Configuration from an SCP, SFTP or TFTP Server 49
Enable the USB port privilege 49
Load Configuration from USB 49
Save Configuration to an SCP, SFTP or TFTP Server 50
Auto Save Configuration 50
Auto USB Backup & Restore Operation 50
Automatic Backup to USB Configuration 51
Automatic Restore from USB Configuration 52

Firmware Upgrade 52
Firmware Update using the CLI 54
Booting From Alternate (Backup) Firmware 54
Reboot 55
Reboot using the CLI 55
Logout 55
Logout from the CLI 55
User Account Page 56
Changing the User Mode 56
Creating a New User 57
Changing an Existing User Account 57
User Privilege Configuration 58
User Account Settings using the CLI 60
Multi-User Mode 60
Single User Mode 60
Creating a New User 61
Permissions 61

Diagnostics 62

Utilization 62
System Log 62
System Log using CLI commands 64
Remote Logging 66
Remote Logging using CLI commands 69
Enable/Disable Remote Logging 69
Add/Delete a Remote Logging Host 69
ARP Table 70
ARP Table using CLI Commands 70
Route Table 71
Route Table Using CLI Commands 71
Alarm Setting 71
Alarm Setting Using CLI Commands 72
Setting EEE (Energy-Efficient Ethernet) 73
Email Alert 74
Digital IO-Setting 75
Digital IO Setting Using CLI Commands 76
Direct DO Trigger 77

Port 78

Configuration 78
Port Status 80
Rate Control 81
RMON Statistics 83

Per Port VLAN Activities 84
Port Security 86
Port Configuration Examples Using CLI Commands 88
Setting the Port Description 88
Enable or Disable a Port 88
Setting the Port Speed 89
Setting Port Duplex 89
Enable or Disable Port Flow Control 89
Display Port Status 90
Setting a Port's Rate Control 90
Display a Port's RMON Statistics 90
Display a Port's VLAN Activities 90
Setting MAC Port Security 91

Switching 94

Bridging 94
Aging Time 95
Threshold Level 95
Storm Control Type 95
Loopback Detect 96
Loopback Detection (Global) 97
Loopback Detect Action 97
Loopback Detect Recovery Time 97
Polling Interval 97
Loopback Detection (Per Port) 98
Storm Detect 99
Enable/Disable Storm Detection 99
Static MAC Entry 100
Adding a Static MAC Address to a Port 101
Removing a Static MAC Address from a Port 102
Adding a MAC to the Static-MAC-Entry Discard Table 102
Removing a MAC address from the Static-MAC-Entry Discard Table 103
Port Mirroring 103
Link State Tracking 105
Enable/Disable Link State Tracking 105
Port Settings 105
PoE (Power over Ethernet) - System and Port Settings 106
PoE System Setting 106
PoE Port Setting 107
PoE Scheduling 109
PoE Watchdog 110
PoE Action 111
Update PoE Firmware 113

Switch Configuration Examples Using CLI Commands 115
Setting the Aging Time Value 115
Enabling Port Isolation 115
Setting Storm Control 115
Enabling Loopback Detect (Global) 116
Setting the Loopback Detect Action 116
Setting the Loopback Detect Recovery Time 116
Setting the Loopback Detect Polling Interval 116
Enabling Loopback Detect (Port) 117
Configuring Storm-Detect 117
Adding a MAC Address for Static-MAC-Entry Forwarding 120
Discard a Static MAC Entry 121
Configuring Port Mirroring 121
Enabling a Link State Tracking Group 121
Assigning a Port to a Link State Tracking Group 122
Setting PoE Power Budget 122
PoE Port Settings 122
Fixed Power Limit 124
Power-priority 126
PoE Scheduling 126
PoE Watchdog 128
PoE 4-Pair Delivery 128
Extended PoE 129
PoE Action 129

Trunking 130

Overview 130
Static Channel Trunking 130
Link Aggregation Control Protocol 131
Port Trunking 131
LACP Trunking 133
Trunking Configuration Using CLI Commands 135
Adding an Interface to a Static Trunk 135
Adding an Interface to a LACP Trunk 135
Setting the LACP Port Priority 135
Setting the LACP Timeout 136

STP/Ring Page – Overview 136

Choosing the Spanning Tree Protocols 136
Spanning Tree Protocol (STP) 136
Rapid Spanning Tree protocol (RSTP) 137
Multiple Spanning Tree Protocol (MSTP) 137

STP/Ring Page - Configuring RSTP 137

Global Configuration Page 137
Enabling the RSTP Protocol 137
Additional Global Configuration page settings 137
The Root Bridge & Backup Root Bridge 139
Setting the MAX Age, Forward Delay and Hello Timer 140
RSTP Port Setting Page 141
Spanning Tree Port Roles 141
Path Cost & Port Priority 142
Point to Point Link 144
Edge Port 145
RSTP Configuration Using CLI Commands 145
Enabling the Spanning Tree Protocol 145
Bridge Priority, Max Age, Forward Delay, and Hello Time 145
Modifying the Port Priority and Path Cost 146
Manually Setting a Port to be a Shared or Point to Point Link 146
Enabling/Disabling a port to be an Edge Port 147
Enabling/Disabling automatic edge detection 147

STP/Ring Page - Configuring MSTP 148

Global Configuration Page 148
Enabling the MSTP Protocol 148
The CIST Root Bridge & Backup CIST Root Bridge 149
Setting Bridge Priority 150
Configuring the CST Network Diameter 151
MSTP Properties Page 152
Configuring an MSTP Region 152
Configuring the IST Network Diameter 153
MSTP Instance Setting Page 154
Setting an MSTP Instance 154
Modifying MSTP parameters for load balancing 155
MSTP Port Setting page 157
Adjusting the blocking port in a MSTP network 157
MSTI Instance Port Membership 158
MSTP Configuration Using CLI Commands 159
Enabling Spanning Tree for MSTP 159
Bridge Priority, Max Age, Forward Delay, and Hello Time 160
Configure IST MAX Hops 160
MSTP Regional Configuration Name and the Revision Level 161
Creating an MSTI Instance 161
Setting MSTI Priority 161
Modifying CIST Port Priority and Port Path Cost 162
Adding a Port to an MSTI Instance 163

STP/Ring Page - Alpha Ring 163
Alpha Ring Setting Page 163
EtherWAN Alpha-Ring Technology 163
Implementing a Simple Alpha-Ring 164
Alpha-Ring V2 164
Connecting two Alpha-Ring Networks together (Ring Coupling) 165
Connecting Additional Rings (Redundancy Pairs) 166
Configuring Alpha Ring using CLI commands 169
Enable Alpha Ring and Alpha Ring V2 Protocols 169
Set the Ring Ports 170
Show Ring, Port and All States 170
Define a Ring's Blocked Port 171
Set Delay Time for Restoration of a Failed Port 171
Enable Ring Coupling 171
Set Ring Coupling Ports 171
Enable Redundancy Pairs 172
Show Ring Coupling, Port Coupling, and Redundancy Pair States 172

STP/Ring Page – Alpha Chain 173
The Alpha Chain Protocol 173
General Overview 173
Alpha Chain Settings 173
Global Settings 174
Configuring the Alpha Chain Ports 175
Alpha Chain Pass-Through Ports 175
Configuring Alpha Chain using CLI commands 176
Storm Control 176
Configuring Chain Ports 177
Configuring Chain Pass-Through Ports 177

STP/Ring Page - Advanced Setting 178
Advanced Bridge Configuration 178
Advanced Per Port Configuration 179
Configuring Spanning Tree Advanced Settings using CLI commands 180
Enabling BPDU Guard Globally 180
Enabling BPDU Guard on a Port 181
Enabling BPDU Guard Error Disable-timeout 181
Enabling the Loop Guard Feature 181

VLAN 183
Configuring VLANs 183
Add and delete VLANs 183
Port Setting 184

Tag Based VLAN Configuration Using CLI Commands 185
Configuring a 802.1Q VLAN 185
Configuring an IP Address for a Management VLAN 186
Removing an IP Address from a Management VLAN 186
Configuring an Access Port 186
Configuring a Trunk Port 187
Add an IP to the Management VLAN 187

QoS 188

Global Configuration Page 189
Web GUI Interface 189
QoS Global Configuration using the CLI Interface 192
Enable/Disable QoS Trust 192
Configuring the Egress Expedite Queue 193
802.1p Priority Page 194
Web GUI Interface 194
802.1p Priority Submenu – CLI Interface 195
DSCP Page – HTTP Interface 196
DSCP Submenu – CLI Interface 197
QoS Interface Commands – CLI Interface 197
ACL Information 198
ACL Configuration 198
ACL Configuration Using CLI Commands 199
Creating a Standard IP Access List 199
Creating an Extended IP Access List 199
Creating a MAC Access List 200
Creating an ACL Class Map with Layer 4 Access List 200
Creating a ACL Class Map with an IP or MAC Access List 201
Creating an ACL Policy Map 202
Appling an Existing ACL Policy to a Port 203
Deleting an ACL Class 203
Deleting an ACL Policy 204

IP ACL (Access Control List) 204

Configuring IP ACL 204
Port ACL Settings 206
Creating a Standard IP Access List using CLI 206

SNMP 207

SNMP General Settings 208
Configuring SNMP v1 & v2 Community Groups 211
Configuring SNMP v3 Users 212
Adding SNMP v3 Users to the switch 212

Deleting SNMP v3 Users from the switch....214
Create SNMPv3 Group and View....215
SNMP Configuration Using CLI Commands....216
Enabling SNMP and configuring general settings....216
Configuring SNMP Traps....217
Configuring SNMP v1 & v2 Community Groups....218
Adding SNMP v3 Users....218
Configuring a New SNMP Group....219
Create or Update a View Entry....220

AAA....220

Configuring Radius from the GUI....221
Enabling Radius....221
Adding a Radius Server....221
Port Authentication....223
Configuring TACACS+ from the GUI....224
Enabling TACACS+....224
Adding a TACACS+ Server....225
Configuring DoS (Denial of Service) from the GUI....225
AAA Configuration Using the CLI....227
View RADIUS Status....227
Enable RADIUS Globally....227
Configure RADIUS on Ports....228
Configure MAC-Based Authentication....228
TACACS+ Authentication and Authorization....228
Configure TACACS+ Server....229

LLDP....229

LLDP General Settings....230
Enable/Disable LLDP....230
Holdtime Multiplier....230
Global TLV Setting....231
LLDP Ports Settings....232
Enabling LLDP transmission for a specific Port....232
Enabling LLDP Reception for a specific Port....232
Enabling Notifications....233
LLDP Neighbors....234
LLDP Statistics....235
LLDP MED Network Policy....236
LLDP MED Location ID....237
LLDP MED Port Settings....239
LLDP Configuration Using CLI Commands....240
Enable/Disable LLDP....240

LLDP Holdtime Multiplier....240
LLDP Transmit Interval....241
Enable/Disable Global LLDP TLVs....242
Enabling LLDP Transmit on a Port....242
Enabling LLDP Receive on a Port....243
Enabling LLDP Notify....243
Enabling Transmission of the Management IP....244
Enabling Specific TLV's on a Port....244
Enabling LLDP MED TLV's on a Port....244
Set LLDP-MED location information....245

Routing....245

Static Route Configuration....245
Creating a Static Route....246
Routing Table....246
Route Map....247
Proxy ARP....248
Static Routing with CLI Commands....249
Create or Delete Static Route....249
Show Existing IP Routes....249
Create or Delete Access List....250
Configure Route Map....250
Enable Proxy ARP....250
VRRP....251
VRRP with CLI Commands....253
Enable or Disable VRRP....253
Enable or Disable Virtual MAC feature....253
Set the Virtual IP Address for the VRRP Session....253
Specify the Interface for Virtual Routing....253
Configure VRRP Router Priority....254
Enable/Disable Preempt Mode....254
Set the Advertisement Interval....254
Enable the VRRP Session....254
Configure Circuit Failover....255

OSPF....255

OSPF Configuration....255
Stub Area Configuration....256
NSSA Configuration....257
OSPF Network....258
OSPF Interface....259
OSPF Virtual Link....260
OSPF Redistribute....261

OSPF Area Range 262
OSPF Neighbor 263
OSPF Route 263
OSPF Configuration with CLI Commands 263
Enable or Disable OSPF 263
Show OSPF Configuration and Settings 264
Enable authentication for an OSPF area 264
Specify a cost for the default summary route 264
Configure a filter to advertise summary routes 264
Summarize OSPF routes at an area boundary 265
Set an area as a Not-So-Stubby-Area (NSSA) 265
Configure the short-cutting mode of an area 265
Define an area as a stub area 266
Configure a link between two separated backbone areas 266
Control how OSPF calculates the default metric for the interface 266
Enable / disable RFC 2328 compatibility 267
Create a default external route into an OSPF routing domain 267
Set OSPF administrative distances 267
Configure a stub host entry belonging to a particular area 268
Limit number of Database Descriptors (DD) that can be processed concurrently 268
Set maximum number of OSPF areas 268
Specify and configure neighbor routers 268
Enable OSPF routing with a specified area 269
Set an OSPF Area Border Router (ABR) type 269
Specify a router ID for the OSPF process 269
Set maximum number of LSAs that can be supported 269
Suppress sending Hello packets 270
Redistribute routes into an OSPF routing table 270
Summarize or suppress external routes 270
Adjust route-calculation timers 270
Set OSPF authentication method on an interface 271
Specify OSPF authentication password for neighboring routers 271
Specify the cost of the link-state metric in a router-LSA 271
Turn on LSA database-filter 271
Set interval after which a neighbor is declared dead 272
Disable OSPF on an interface 272
Set Hello packet interval 272
Register an MD5 key for OSPF authentication 272
Set MTU size for OSPF to construct packets 273
Ignore MTU in DBD packets 273
Set the OSPF network type 273
Set designated router priority 273

Set time between retransmitting lost link state advertisements....273
Set the link state transmit delay....274
Configure a distribution list....274

RIP....274

RIP General Settings....274
RIP Port Settings....275
RIP Route....276
RIP Network....277
RIP Neighbor....277
Add or Delete RIP Passive Interface....278
RIP Redistribute....278
RIP Configuration with CLI Commands....279
Enable or Disable RIP....279
Enable RIP Routing on a Specific Network....279
Show RIP Routing Table....279
Define RIP Neighbor....280
Set Interface to Passive....280
RIP Default Metric....280
RIP Send Version....280
Redistribute....280
RIP Default Route....281
Define RIP Administrative Distance....281
Define RIP Timers....281
RIP Authentication....282

Other Protocols....283

IGMP Snooping....283
General Overview....283
Enabling the IGMP Snooping Modes....284
Configuring IGMP Snooping General properties....284
Configuring IGMP Passive Mode Specific properties....285
Configuring IGMP Querier Mode Specific properties....286
Configuring IGMP Unknown Multicast Forwarding....287
Monitoring Registered Multicast Groups....291
IGMP Configuration Examples Using CLI Commands....292
GVRP....298
General Overview....299
Enabling the GVRP Protocol at the Global Level....300
Enabling the GVRP Protocol at the Port Level....302
GVRP Configuration Examples Using CLI Commands....303
GMRP....306
General Overview....306

GMRP Normal mode....306
GMRP Fixed mode....306
GMRP Forbidden mode....307
GMRP Forward All mode....307
GMRP Disabled mode....307
Enabling the GMRP Feature Globally on the Switch....307
Configuring the GMRP Feature Per Port....308
GMRP Configuration Examples Using CLI Commands....310
Network Time Protocol (NTP)....312
Setting RTC Time....312
Enabling NTP....313
Setting the NTP Server IP Address....313
Setting the Time Zone....313
Setting the Polling Period....313
Manually Syncing Time....313
Daylight Savings Time - Weekday Mode....314
Daylight Savings Time – Date Mode....315
Network Time Protocol Configuration Examples Using CLI Commands....316
Prosition Time Protocol (PTP)....319
General Overview....319
Configuring the PTP feature....319
PTP Configuration of CLI Commands....321
DHCP Server....324
General Overview....324
Configuring the DHCP Server....324
DHCP Configuration Examples Using CLI Commands....326
Configuring DHCPv6 Server....328
DHCPv6 Configuration Examples CLI Commands....328
DHCP Relay....329
General Overview....329
Configuring the DHCP Relay....329
DHCP Relay Configuration of CLI Commands....331
DHCP Snooping....332
General Overview....333
Configuring the DHCP Snooping....333
DHCP Snooping Configuration of CLI Commands....334
Dynamic ARP Inspection (DAI)....336
General Overview....336
Configuring the Dynamic ARP Inspection....336
DAI Configuration of CLI Commands....338
IP Source Guard (IPSG)....340
General Overview....340
Configuring the IP Source Guard....340

IPSG Configuration of CLI Commands 341
Modbus TCP 343
Functional Description 343
Data Format and Function code 344
Configuring the MODBUS Function features 346
Modbus Configuration of CLI Commands 347
Register table 348
RESTful API 350
API Command List 350

Cyber Security Index 353

Security Context 353
General Description of the Product/System 353
Intended Use Cases Description 353
Location in Intended Use Environment 354
Site Operations and Control 355
Site IND Engineer Work 356
Security Requirements 358
Switch Security Features 358
Port Security 359
SNMP (SNMPv3) 359
DoS Protection 359
Firmware Upgrade Security 359
Auditable events 359
Security Function Verification 362

Contact Information 364

PREFACE

Audience

This guide is designed for the person who installs, configures, deploys, and maintains the Ethernet network. This document assumes the reader has moderate hardware, computer, and Internet skills.

Document Revision Level

This section provides a history of the revision changes to this document.

Revision	Document Version	Date	Description
A	Version 1	12/26/2019	Initial release for Firmware version 5.0
A	Version 2	08/25/2020	Minor changes
B	Version 1	10/7/2020	New GUI images, Added SFTP option, Added PoE Action function, Added DDM information
B	Version 2	01/14/2021	Removed redundancy pairs CLI comand
B	Version 3	04/06/2021	Added instructions for updating PoE firmware, and new CLI commands [no] poe extend-mode auto-10m. Added support for IEEE 802.3bt PoE.
C	Version 1	05/24/2021	Revised for version 5.00.4.x.
C	Version 2	06/17/2021	Minor changes to saving configuration description.
C	Version 3	06/29/2021	Added voltage requirement information for Extend Mode when running PoE IEEE 802.3 BT firmware ver. 3.5.2.
C	Version 4	12/02/2021	Updated for firmware version 5.01.0.4
C	Version 5	12/21/2021	Fixed incorrect 100Mbps references and interface changes
D	Version 1	10/25/2023	Updated for firmware version 5.02.2.2
E	Version 1	02/15/2024	Updated for firmware version 5.03.0.3
F	Version 1	05/16/2024	Updated for firmware version 5.04.1.4
G	Version 1	06/28/2024	Updated for firmware version 5.05.0.2

Applicable Models

This user manual corresponds to the following model series:

EX78900E, EX78900X, EX78900H, EX73900E, EX73900X, EX75900, IG5 & IG5 L Series

All Applicable Models are fulfilled the definition of Device categories in of IEC 62443-4-2: 2019 annex A.3 Device category: Network device/ A.3.1 Switch.

NOTE ON GRAPHICAL USER INTERFACE

The GUI images shown in this manual represent the latest 5.00.x firmware. Devices running older 5.xx firmware versions will still show the older interface. Document Conventions

This guide uses the following conventions to draw your attention to certain information.

Safety and Warnings

This guide uses the following symbols to draw your attention to certain information.

Symbol	Meaning	Description
	Note	Notes emphasize or supplement important points of the main text.
	Tip	Tips provide helpful information, guidelines, or suggestions for performing tasks more effectively.
	Warning	Warnings indicate that failure to take a specified action could result in damage to the device or could result in serious bodily injury.
	Electric Shock Hazard	This symbol warns users of electric shock hazard. Failure to take appropriate precautions such as not opening or touching hazardous areas of the equipment could result in injury or death.

Typographic Conventions

This guide also uses the following typographic conventions.

Convention	Description
Bold	Indicates text on a window, other than the window title, including menus, menu options, buttons, fields, and labels.
Italic	Indicates a variable, which is a placeholder for actual text provided by the user or system. Angled brackets (< >) are also used to indicate variables.
`screen/code`	Indicates text that is displayed on screen or entered by the user.
< > angled brackets	Indicates a variable, which is a placeholder for actual text provided by the user or system. Italic font is also used to indicate variables.
[ ] square brackets	Indicates optional values.
{ } braces	Indicates required or expected values.
| vertical bar	Indicates that you have a choice between two or more options or arguments.

COMPUTER SETUP

The end user's management computer may need to be reconfigured prior to connecting to the switch in order to access the switch's web interface through its default IP address (See Default IP 錯誤! 找不到參照來源。).

Management Methods and Protocols

There are several methods that can be used to manage the switch. This manual will show the details of configuring the switch using a web browser. Each section will be followed by the CLI (Command Line Interface) commands needed to achieve the same results as described in that section.

The methods available to manage the switch include:

- **SSH** - Secure Shell CLI that is accessible over TCP/IP networks which and is generally regarded as the most secure method of remotely accessing a device.
- **Telnet** - is like SSH in that it allows a CLI to be established across a TCP/IP network, but it does not encrypt the data stream. This type of connection requires a terminal, or a computer running a terminal emulation application (such as HyperTerminal or Putty).
- **HTTP** (Hypertext Transfer Protocol) is the most popular switch management protocol involving the use of a web browser.
- **RS-232** – The switch is equipped with a RS-232 serial port that can be used to access the switch's CLI. The Serial port is DCE DB9F. A straight through serial cable is used to connect to a typical computer serial port (Also requires terminal emulation application).

Default IP

The switch's default IP address is 192.168.1.10. The management computer must be set up so that it is on the same network as the switch. For example, the IP address of the management computer can be set to 192.168.1.100 with a subnet mask of 255.255.255.0.

Login Process and Default Credentials

Once a compatible IP address has been assigned to the management computer, the user is ready to log in to the switch. To log in, type the URL http://192.168.1.10/ into the address field of the browser and hit return. The following will appear in the browser window (See Figure 1)

- The Default Login is **root** (case sensitive)
- There is no password by default
- Enter the login name and click the Login button



Figure 1: Login screen

Note: When logging into the GUI or the CLI for the first time, the switch will prompt you to change the default password to a new one. The new password must meet the following complexity requirements:

- Minimum 8 characters and maximum 35 characters in password length without leading or trailing blanks.
- The password must contain characters from the following categories:

  1. Uppercase English letters, (A to Z)

  2. Lowercase English letters, (a to z)

  3. Numbers, (0 to 9)

4. Non-alphanumeric characters (e.g. @,#,$), but not including (”, ?, !)

The password will be displayed in encrypted form in the configuration file, and the User Account authentication process is obscured.

User account will be locked after 10 (configurable) password attempts and will stay locked for 5 minutes.

SETTING THE INITIAL IP ADDRESS

Once logged in the user can now configure the switch per the network requirements. The two major addressing options are:

- Simple IP addressing
- Multiple VLAN addressing (See Add an IP to the Management VLAN on page 187).

Simple IP Addressing

A new IP address can now be assigned to the switch. From the System Information screen, go to the left-hand navigation menu.

1. Click on the **+** next to **System**
2. Click on **IP address**
3. Enter the desired IP address and subnet mask in the **IP Address/Subnet Mask** fields associated with VLAN 1
4. Click the **Apply & Save** button (See Figure 2)

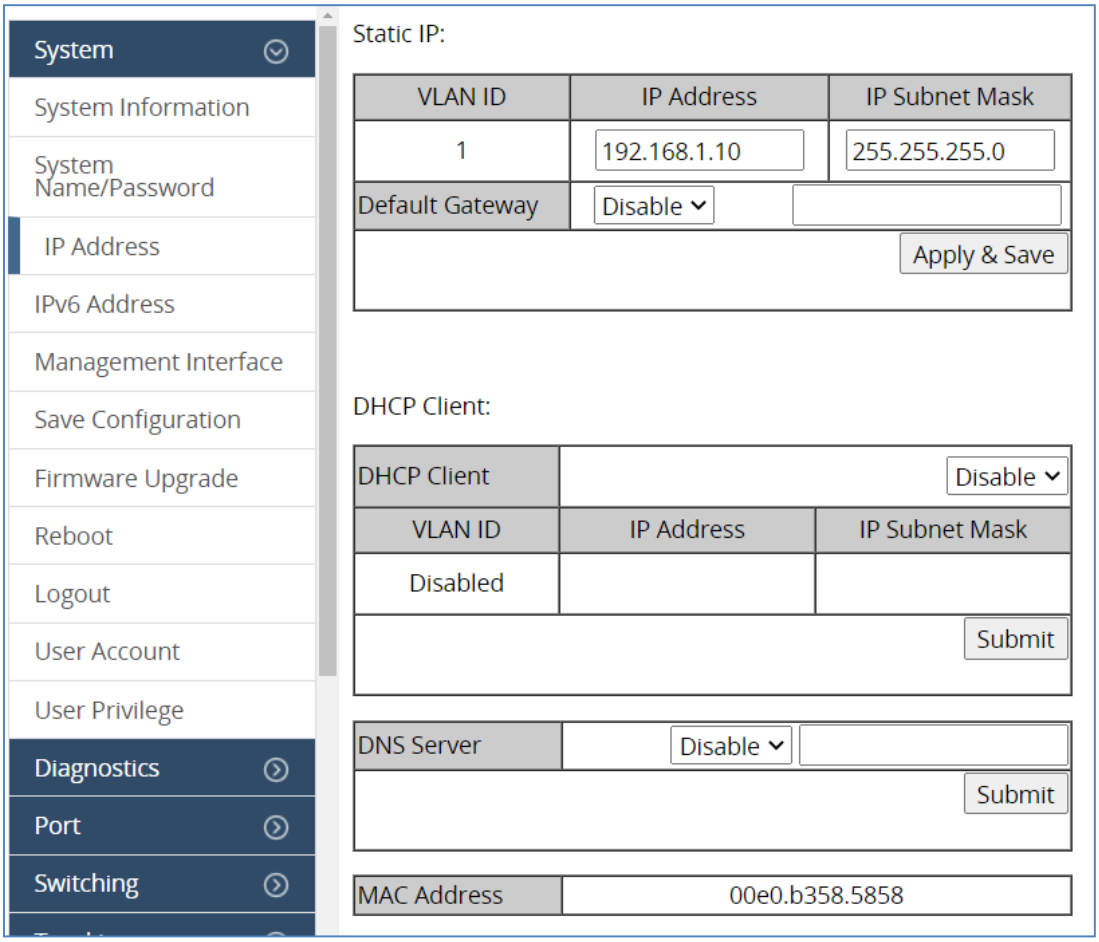


Figure 2: Assigning an IP address

CLI COMMAND USAGE

This chapter describes accessing the switch by using Telnet, SSH, or serial ports to configure the switch, navigating the Command Line Interface (CLI), typing keyboard shortcuts, and moving between the levels. This chapter assumes the user has a working understanding of Telnet, SSH and Terminal emulation applications.

Note: For a serial port connection use a standard DB9F to DB9M Modem Cable. The default Serial port parameters are Baud rate: 115,200bps, Data bits: 8, Parity: none, Stop bit: 1, Flow control: none.

Navigating the CLI Hierarchy

The CLI is organized into a hierarchy of command modes. The basic modes are User exec mode, Privileged exec mode, and Global configuration mode. There are also other modes, specific to certain configurations. Each mode has its own group of commands for a specific purpose. Below are the CLI commands needed to enter a specific mode:

```
switch_a> ← User exec mode
switch_a>enable
switch_a# ← Privileged exec mode
switch_a#configure terminal
switch_a(config) ← Global configuration mode
switch_a(config) spanning-tree mst configuration
switch_a(config-mst)# ← MSTP configuration mode

switch_a(config)#line console 0
switch_a(config-line) ← Line configuration mode

switch_a(config)# interface ge1
switch_a(config-if)# ← Interface configuration mode

switch_a(config)#vlan database
switch_a(config-vlan)# ← VLAN database configuration mode
```

CLI Keyboard Shortcuts

Ctrl + a: place cursor at the beginning of a line

Ctrl + b: backspace one character

Ctrl + d: delete one character

Ctrl + e: place cursor at the end of the line

Ctrl + f: move cursor forward one character

Ctrl + k: delete from the current position to the end of the line

Ctrl + l: redraw the command line

Ctrl + n: display the next line in the history

Ctrl + p: display the previous line in the history

Ctrl + u: delete entire line and place cursor at start of prompt

Ctrl + w: delete one word back

Command Syntax

The following symbols are used to describe the values and arguments for command entries in the CLI.

- **<angle brackets>** : Variable or value that must be specified.
- **[square brackets]** : Optional parameters or arguments.
- **optionA | optionB** : Vertical bar. Separates multiple exclusive items in a list of options.
- **{braces} :** Indicate optional values or arguments, where one must be selected
- **(parentheses) :** Indicates at least one or more of the values or arguments in the receding syntax enclosed by braces must be specified.

Variable Placeholders

The command syntax uses the following tokens to represent command line variables for which you supply a value:

- `WORD` : A contiguous text string (excluding spaces), such as IFNAME for the name of an interface.
- `LINE` : A text string, including spaces; no other parameters can follow this parameter.
- `A.B.C.D` : IPv4 address
- `A.B.C.D/M` : IPv4 address and mask/prefix.
- `HH:MM:SS` : Time format
- `AA:NN` : BGP community value
- `XX:XX:XX:XX:XX:XX` : MAC address
- `<1-65535>` : Numeric Range

CLI Command modes

Throughout this manual, each section that has CLI commands relevant to that section requires that the CLI be in a specific configuration mode. This section shows the main CLI commands to needed to enter a specific mode.

Global Configuration Mode

To set the switch to Global Configuration Mode, run the following commands from the CLI:

1. enable
2. configure terminal

Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#
```

MSTP Configuration Mode

To set the switch to General MSTP configuration mode, run the following commands from the CLI:

1. enable
2. configure terminal
3. spanning-tree mst configuration

Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#spanning-tree mst configuration
switch_a(config-mst)#
```

Interface Configuration Mode

Interface mode on the switch is used to configure the Ethernet ports and VLAN information. Valid interfaces are:

- **xe<port #>** - 10 gigabit ports use xe followed by the port number. Example: **xe1**
- **ge<*port #*>** - Gigabit ports use ge followed by the port number. Example: **ge1**
- **vlan1.<vlan#>** - VLAN's use vlan. Followed by the VLAN ID. Example: **vlan1.10**

Example 1

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface ge1
switch_a(config-if)
```

Example 2 configures VLAN ID 9

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface vlan1.9
switch_a(config-if)
```

VLAN Database Configuration Mode

VLAN Database Configuration Mode on the switch is used to configure the VLAN settings.

Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#vlan database
switch_a(config-vlan)#
```

Router Configuration Mode

Used for RIP and OSPF configuration

Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#router rip
switch_a(config-router)#
```

Saving a Configuration from the CLI

Example:

```
switch_a>enable
switch_a#write memory
Building configuration.....
[OK]
switch_a#>
```

Command Help

Help information is available from the command line by entering the following commands:

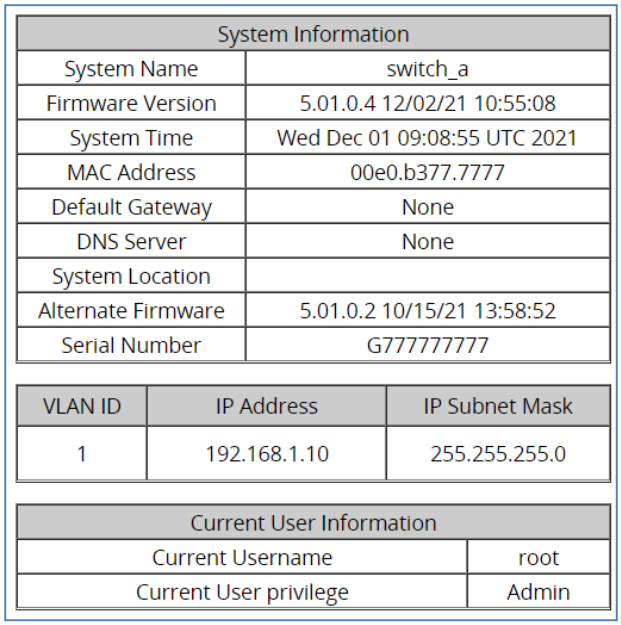
- Use "**?**" to query the commands and descriptions available at the current level.
- Using "**Command_name ?**" will display a list of available parameters under the command.

SYSTEM MENU (WEB INTERFACE)

System Information

The System information link on the Left menu of the Web Configuration page takes you to a page that shows the following (see Figure 3):

- **System Name**
    - The System name is typically used by network administrators. If SNMP is enabled on the switch, the system name can be found using MIB II (RFC1213) in the sysName property.
- **Firmware Version**
    - If SNMP is enabled on the switch, the Firmware version can be found using MIB II in the sysDesc property
- **System Time**
    - System time can be changed using NTP
- **MAC Address**
    - The hardware (MAC) address of the Management interface
- **Default Gateway**
    - The IP address of your networks Gateway (Typically a Router on your network)
- **DNS Server**
    - The Dynamic Name Server (DNS) for your network
- **System Location**
    - SNMP location information
- **VLAN ID**
    - One or more listings depending on the number of VLANs defined on the switch
    - Lists VLAN ID, IP address, and subnet mask of the VLAN Interface(s)
- **Current User Information**
    - Lists the current the currently logged in user and their user privileges



System Information	
System Name	switch_a
Firmware Version	5.01.0.4 12/02/21 10:55:08
System Time	Wed Dec 01 09:08:55 UTC 2021
MAC Address	00e0.b377.7777
Default Gateway	None
DNS Server	None
System Location	
Alternate Firmware	5.01.0.2 10/15/21 13:58:52
Serial Number	G777777777

VLAN ID	IP Address	IP Subnet Mask
1	192.168.1.10	255.255.255.0

Current User Information	
Current Username	root
Current User privilege	Admin

Figure 3: System Information

System Name/Password

The System name is typically used by network administrators to make it easier to document a networks infrastructure and locate equipment on large networks. If SNMP is enabled on the switch, the system name can be found using MIB II (RFC1213) in the sysName property. To change the system name:

1. Click on the **+** next to **System**.
2. Click on **System Name/Password** (see Figure 4).
3. Use your mouse to place the cursor in the **System Name** text box.
4. Replace the existing name with the name you want to assign to the switch.
5. Click on the **Update Setting** button.

By default, there is no password assigned to the switch. To add or change a password:

1. Click on the **+** next to **System**.
2. Click on **System Name/Password** (see Figure 4).
3. Use your mouse to place the cursor in the **Password** text box.
4. Enter the new password.
5. Retype the password in the **Retype Password** text box.

6. Click on the **Update Setting** button below the **Retype Password** text box.

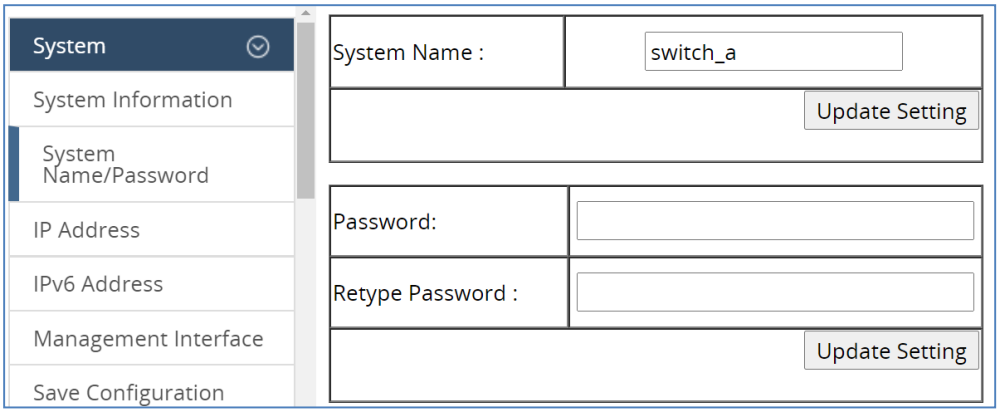


Figure 4: System Name/Password

Note: To reboot the switch, press and hold the **reset button** for **less** than **10 seconds**.

To reset the switch to the default password, **press and hold** the reset button for **more** than **10 seconds.**

System Name/Password using the CLI

For more information on CLI command usage see CLI Command Usage.

System Name
To set the system name on a switch, use the following CLI commands (Hostname must not contain spaces. Use the dash and underscore characters):

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
hostname *<name>*
no hostname

Usage Example 1: Setting a Hostname

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#hostname switch_a
switch_a(config)#write memory
```

Usage Example 2: Removing a Hostname

```
switch_a>enable
```

```
switch_a#configure terminal
switch_a(config)#no hostname
switch_a(config)#write memory
```

Password
To enable a password on a switch, use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
enable password <*password*>

Usage Example
```
switch_a>enable
switch_a#configure terminal
switch_a(config)#enable password mypassword
switch_a(config)#write memory
```

Show Switch Model/Serial Number using the CLI

For more information on CLI command usage see CLI Command Usage.

System Name
To see the model number of a switch, use the following CLI command:

CLI Command Mode: **User Exec Mode** or **Privileged Exec Mode**

CLI Command Syntax:
show integrate product series

Usage Example 1:
```
switch_a>enable
switch_a# show integrate product series
EX78000 series
```

Serial Number
To see the serial number of a switch, use the following CLI command:

CLI Command Mode: **User Exec Mode** or **Privileged Exec Mode**

CLI Command Syntax:
show serial number

IP Address

To navigate to the **IP Address** page:

1. Click on the **+** next to **System**
2. Click on **IP Address** (see Figure 5)

There are 4 settings on this page:

Static IP (see Simple IP Addressing)

DHCP Client

Use this to enable or disable DHCP on a VLAN.
To enable the DHCP Client:

1. Use the drop-down box to enable the DHCP client on the desired VLAN
2. Click the **Submit** Button

Default Gateway

If DHCP is enabled, the gateway setting is controlled by the DHCP server. The setting will be grayed out and the gateway supplied by the DHCP server will be displayed. The default gateway setting can be used when using a Static IP address. To enable the default gateway:

1. Use the dropdown box to enable the default gateway.
2. Type in the default gateway in the **Default Gateway** text box.
3. Click on the **Apply & Save** button.

DNS Server

If DHCP is enabled, the DNS Server setting is controlled by the DHCP server. The setting will be grayed out and the DNS Server supplied by the DHCP server will be displayed. The DNS Server setting can be used when using a Static IP address. To enable the DNS Server:

1. Use the dropdown box to enable the DNS Server.
2. Type in the default gateway in the **Default Gateway** text box.
3. Click on the **Submit** button.

Note: After making changes to settings in the IP address section, the configuration needs to be saved using the **System/Save configuration** page (See Save Configuration)

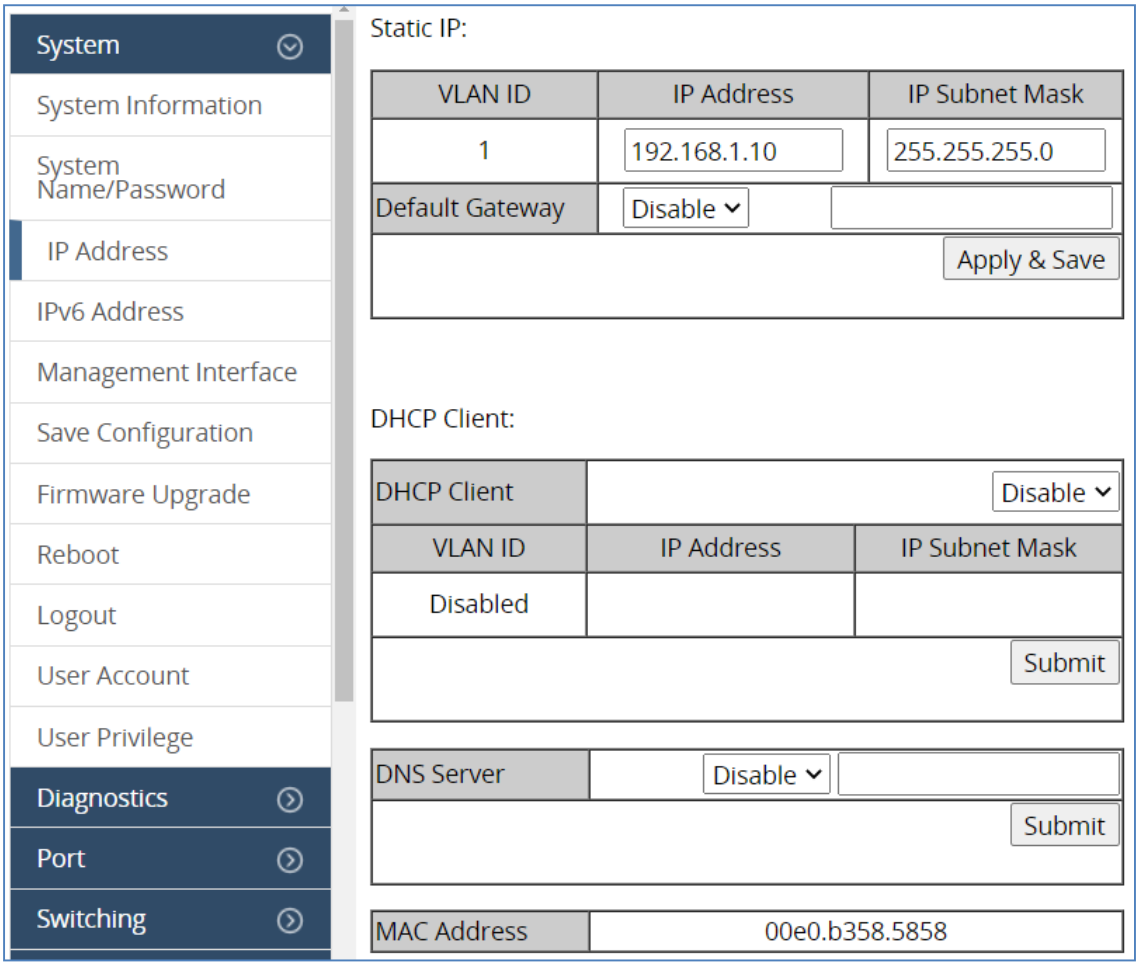


Figure 5: IP Address

IP Address - Configuration using the CLI

For more information on CLI command usage see CLI Command Usage.

Set the IP Address

CLI Command Mode: **Global Configuration** and **Interface Configuration**

CLI Command Syntax:
ip address <*A.B.C.D/M*> (IP Address/Mask e.g. 10.0.0.1/8)
no ip address

Note: The Subnet Mask is defined as a **Network Prefix** instead of the common **dotted decimal** (ex. 255.255.255.0).
The most commonly used Network Prefixes are:

- **/8** – Known as Class A. Also known in dotted decimal as 255.0.0.0
- **/16**– Known as Class B. Also known in dotted decimal as 255.255.0.0
- **/24**– Known as Class C. Also known in dotted decimal as 255.255.255.0

Usage Example 1: Assigning an IP address

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#ip address 192.168.1.1/24
switch_a(config)#q
switch_a#write memory
Building configuration.....
[OK]
switch_a#q
switch_a#
```

Usage Example 2: Removing an IP address

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#no ip address
switch_a(config)#q
switch_a#write memory
Building configuration.....
[OK]
switch_a#q
switch_a#
```

Set the Default Gateway

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
ip default-gateway <*A.B.C.D*>
no ip default gateway

Usage Example 1: Setting the Gateway

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#ip default-gateway 192.168.1.254
switch_a(config)#q
```

```
switch_a#write memory
Building configuration.....
[OK]
switch_a#q
switch_a#
```

Usage Example 2: Removing the Gateway

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#no ip default-gateway
switch_a(config)#q
switch_a#write memory
Building configuration.....
[OK]
switch_a#q
switch_a#
```

Set the Domain Name Server (DNS)

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
ip dns <*A.B.C.D*>
no ip dns

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#ip dns 192.168.1.253
switch_a(config)#q
switch_a#write memory
Building configuration.....
[OK]
switch_a#q
switch_a#
```

Usage Example 2: Remove a DNS IP Address

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#no ip dns
switch_a(config)#q
switch_a#write memory
Building configuration.....
[OK]
```

```
switch_a#q
switch_a#
```

Enable/Disable DHCP Client on a VLAN

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
get ip dhcp enable
no get ip dhcp enable

Usage Example – Enable DHCP Client on VLAN2:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface vlan1.2
switch_a(config-if)#get ip dhcp enable
switch_a(config-if)#q
switch_a(config)#q
switch_a#write memory
Building configuration.....
[OK]
switch_a#q
switch_a#
```

Enable/Disable Static IP on a VLAN

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
ip address <*A.B.C.D*>
no ip address <*A.B.C.D*>

Usage Example 1 – Enable Static IP on VLAN2:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface vlan1.2
switch_a(config-if)#ip address 192.168.1.11
switch_a(config-if)#q
switch_a(config)#q
switch_a#write memory
Building configuration.....
[OK]
switch_a#q
switch_a#
```

Usage Example 2 – Disable Static IP on VLAN2:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface vlan1.2
switch_a(config-if)#no ip address 192.168.1.11
switch_a(config-if)#q
switch_a(config)#q
switch_a#write memory
Building configuration.....
[OK]
switch_a#q
switch_a#
```

Set the IPv6 Address of an Interface

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
ipv6 address X:X::X:X/M

no ipv6 address (X:X::X:X/M |)

Usage Example 1 – Set IPv6 address on VLAN1:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface vlan1.1
switch_a(config-if)#ipv6 address 3ffe:506::1/48
switch_a(config-if)#q
switch_a(config)#q
switch_a#write memory
```

Set the IPv6 Address through DHCP

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
get ipv6 dhcpv6 enable

no get ipv6 dhcpv6 enable

Usage Example –

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface vlan1.2
switch_a(config-if)# get ipv6 dhcpv6 enable
```

```
switch_a(config-if)#q
switch_a(config)#q
switch_a#write memory
```

Enable/Disable DHCP Server for IPv6

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
dhcpv6-server enable

no dhcpv6-server enable

Usage Example –

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface vlan1.2
switch_a(config-if)# dhcpv6-server enable
switch_a(config-if)#q
switch_a(config)#q
switch_a#write memory
```

Configure DHCPv6 server settings

CLI Command Mode: **Configuration Mode**

CLI Command Syntax:
dhcpv6-server lease-time <0-864000>

dhcpv6-server range <A:B :C:D>

Usage Example –

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# dhcpv6-server lease-time 5000
switch_a(config)#q
switch_a#write memory
```

IPv6 Address

To navigate to the **IPv6 Address** page:

1. Click on the **+** next to **System**
2. Click on **IPv6 Address**

Use the drop-down menu to select the VLAN ID. The select a radio button **Static IP** or **DHCP**. If Static IP is selected, enter the IPv6 address and prefix length in the corresponding field below. Then click **Apply & Save**.

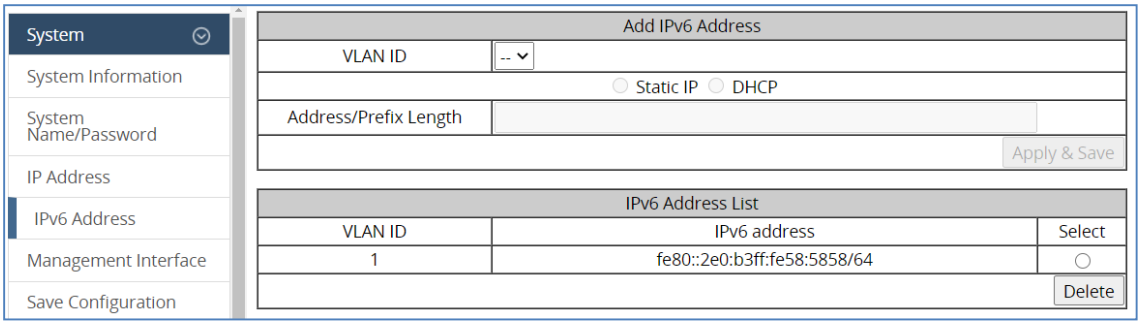


Figure 6: Set IPv6 address

IP Address - Configuration using the CLI

Set the IPv6 Address

CLI Command Mode: **Interface Configuration**

CLI Command Syntax:
ipv6 address < *X:X::X:X/M*>
no ipv6 address

Configure IPv6 Neighbor Discovery

CLI Command Mode: **Interface Configuration**

CLI Command Syntax:
ipv6 nd managed-config-flag
ipv6 nd other-config-flag
ipv6 nd prefix
ipv6 nd ra-interval
ipv6 nd ra-lifetime
ipv6 nd reachable time
ipv6 nd suppress-ra

Management Interface

To navigate to the **Management Interface** page:

1. Click on the **+** next to **System**
2. Click on **Management Interface**

The Management Interface configuration page has three settings that allow the user to configure the methods available to manage the switch.

HTTPS

HTTPS (Hypertext Transfer Protocol Secure) allows the user to determine what method, if any, is used to configure the switch. The default is encrypted HTTPS (see Figure 7). Test procedure please HTTPS function verification.

To disable the Web interface:

1. Select Web Agent drop-down menu to **None.**
2. Click on the **Update setting** button.

Warning: Once the Submit button is pressed, the Web console will no longer function. As a safety precaution, the configuration is not saved by default. Rebooting the switch will restore the Web Console. To save the configuration, connect via Telnet or SSH and save the configuration.

To enable the Web Interface:

1. Check **Http** or **Https** (default)
2. Click on the **Update Setting** button.
3. Save the Configuration (see Save Configuration)

Login Failure Lock

By default, a user account will be locked after 10 failed attempts to log in, and will stay locked for 5 minutes. To disable this feature, click the **disable** radio button and then click **Update Setting**.

Session Time Out

In the Web Auto-logout session, the period of WEB page idle without operation exceed value can be setted from 0~120 minute, counter will be force log out automatically, and requires re-login to ensure administrative security.

To set the WEB agent timeout period:

1. Set the **Expire Time** by minute. (default value is 5 min)
2. Click on the **Update Setting** button.
3. Save the Configuration (see Save Configuration)
4. Press Logout & re-login to assume the setting.

Timeout Count feature provide option for CLI configurable setting, and logout after countdown as sample below:
Commands to DUT to change the telnet exec-timeout value to 5 minutes:

```
switch_a> en
switch_a# config t
switch_a(config)# line vty 0 4
switch_a(config-line)# exec-timeout 5 0
```

Warning: Any unused login service is recommended to be manually terminated at any time by the local organization or by the user who initiated the remote session.

Telnet

Telnet is a network protocol that allows a remote computer to log into the to access its CLI (Command Line Interface). The CLI can be access using Telnet, SSH and the serial port on the switch. The secure method of accessing the CLI over a network is SSH.

To enable or disable Telnet:

1. Click the **Enable** or **Disable** radio button in the Telnet section on the Management Interface page (see Figure 7 below)
2. Click on the **Update Setting** button
3. Save the Configuration (see Save Configuration)

Note: Telnet is Disabled on the switch by default. To change that Telnet be enabled, modify that the “Enable” radio button is checked in the TELNET section on this screen.

SSH (Secure Shell)

Secure Shell or SSH is a network protocol that allows data to be exchanged using a secure channel between two networked devices such as a computer and the switch. SSH is disabled by default on the switch.

To enable or disable SSH:

1. Use the drop-down menu in the SSH section on the Management Interface page to select Disable, SSHv1/SSHv2, SSHv1, or SSHv2. (see Figure 7)
2. Click on the Update Setting button
3. Save the Configuration (see Save Configuration)

To verify that SSH is enabled, navigate to this screen and check the value displayed in the drop-down field. The field displays the current SSH status.

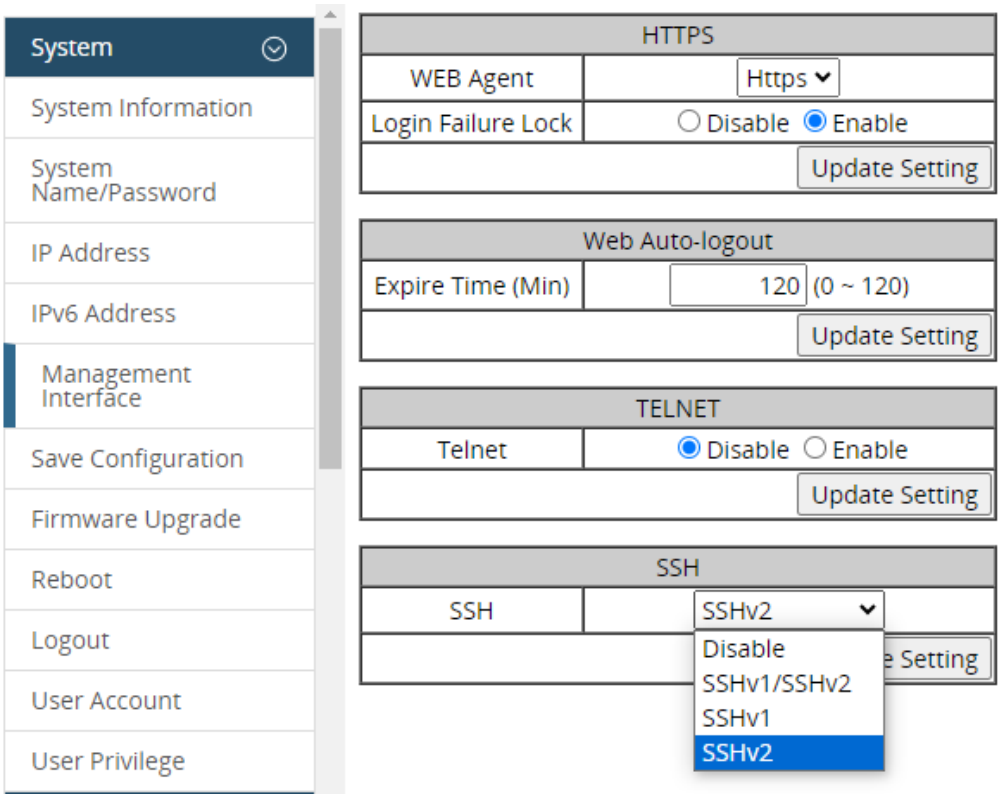


Figure 7: Management Interface

Use an external program such as “Tera Term” to set SSH service for connection to the switch.

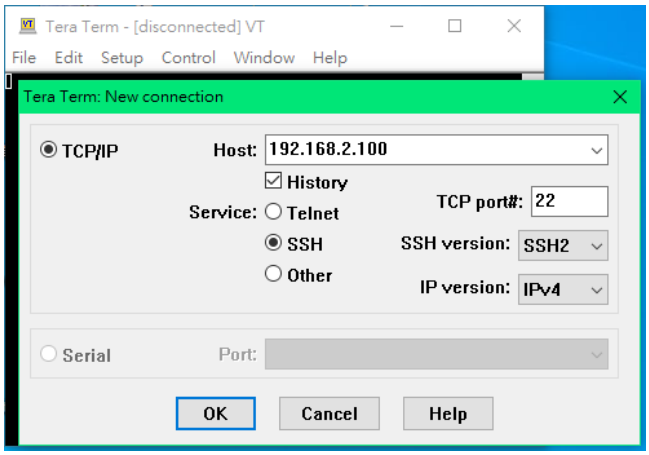


Figure 8: Console Connection Interface

SSL (Secure Socket Layer)

Secure Socket Layer provides security to data exchanged between a web browser and a server. It encrypts the link between web server and browser, preventing data from being stolen, modified, or spoofed.

To set up SSL environment for the switch, please enable HTTPS first:

1. Click the HTTPS check box in the HTTPS section on the Management Interface page (see Figure 7).
2. Click the **Update Setting** button.
3. Save the configuration (see Save Configuration).

Secondly, close the current web browser and open a new browser window. To log in again, type the URL **https://192.168.1.10/** into the address field of the browser and hit return. If the browser window login screen appears, it means SSL connection is provided for the browser access. Otherwise, login screen will not display.

Management Interface Configuration using the CLI

Enabling/Disabling Telnet

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
ip telnet
no ip telnet

Usage Example 1: Enabling Telnet:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#ip telnet
switch_a(config)#q
switch_a#write memory
Building configuration.....
[OK]
switch_a#q
switch_a#
```

Usage Example 2: Disabling Telnet:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#no ip telnet
switch_a(config)#q
switch_a#write memory
Building configuration.....
```

```
[OK]
switch_a#q
```

Note: If using Telnet to run the CLI Commands that disable Telnet you will lose your connection. To Disable Telnet using the CLI, use SSH or the RS-232 Console port on the switch.

Enabling/Disabling SSH

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
ip ssh
no ip ssh

Usage Example 1: Enabling SSH:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#ip ssh
switch_a(config)#q
switch_a#write memory
Building configuration.....
[OK]
switch_a#q
switch_a#
```

Usage Example 2: Disabling SSH:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#no ip ssh
switch_a(config)#q
switch_a#write memory
Building configuration.....
[OK]
switch_a#q
```

Note: If using SSH to run the CLI Commands that disable SSH you will lose your connection. To Disable SSH using the CLI, use Telnet or the RS-232 Console port on the switch.

Enabling/Disabling HTTP and/or HTTPS

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
ip http server
ip http secure-server
no ip http server
no ip http secure-server

Usage Example 1: Enabling HTTP:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#ip http server
switch_a(config)#q
switch_a#write memory
Building configuration.....
[OK]
switch_a#q
switch_a#
```

Usage Example 2: Disabling HTTP:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#no ip http server
switch_a(config)#q
switch_a#write memory
Building configuration.....
[OK]
switch_a#q
```

Usage Example 3: Enabling HTTPS:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#ip http secure-server
switch_a(config)#q
switch_a#write memory
Building configuration.....
[OK]
switch_a#q
switch_a#
```

Usage Example 4: Disabling HTTPS:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#no ip http secure-server
switch_a(config)#q
switch_a#write memory
Building configuration.....
[OK]
switch_a#q
```

Save Configuration Page

Navigate to the **Save Configuration** page:

1. Click on the **+** next to **System**
2. Click on **Save Configuration**

The Save Configuration page contains the following configuration methods (see Figure 9). Select **TFTP** (Trivial File Transfer Protocol), **SFTP** (SSH File Transfer Protocol) or **SCP** (Secure Copy Protocol) to save or load a configuration. Once you have saved the configuration to a disk or server, you can copy this file to a USB flash drive to restore saved settings or apply them to other deployments.

Backup Configuration to server

This function is used to back up the current configuration of the switch to specific SCP, SFTP or TFTP server.

To back up a configuration:

1. Enter the IP address of target server in the **Server IP** text box.
2. Enter the name of the configuration file in the **FILE** text box.
3. Enter the username and password for the SCP or SFTP server.
4. Click on the **Submit** button.
5. If the backup is successful the following message will be shown:
   `tftp <filename> to ip <ip address> success!!`

Load Configuration from server

This function is used to load a previously saved configuration file through the access from SCP, SFTP or TFTP server.

To load a configuration:

1. Enter the IP address of your SCP, SFTP or TFTP server in the **Server IP** field.
2. Enter the name of the configuration file in the **FILE** field.
3. If using SCP or SFTP, enter the username and password for the corresponding server.
4. Click on the **Submit** button.
5. If the file is successfully loaded the following message will be shown:
   `Success! System reboot is required!`

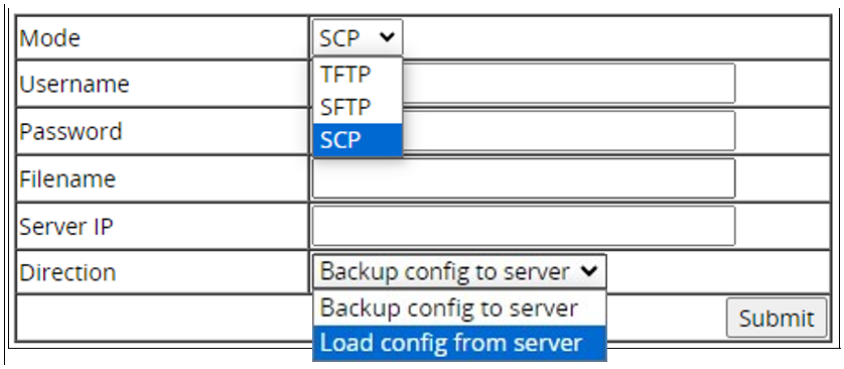


Figure 8: Load Configuration Page

Save Configuration

To save the currently running configuration to the flash memory on the switch:

1. Click the **Save Configuration** button
2. If the save is successful you will see the message:
   `Building configuration….. [OK]`

Restore Default

To restore the switch to factory defaults:

1. Click on the **Restore Default** button.
2. Confirm the execution from the system message.
3. The system will reboot to restore original factory settings.

Restore Configuration from USB

To restore a switch configuration from USB storage:

1. Click on the **Restore Configuration (USB)** button.

While the **Restore Configuration (USB)** button is pressed, the restore configuration process will take place. Once the retore process is completed, a message “The restore configuration is completed now” will display. If an error occurs during the restore process, the message “The restore process is in error” will display.

Auto Save

The Auto Save function is used to set the switch to automatically save the configuration to flash. If the saved configuration is the same as the running configuration then a save is not made. The Auto Save interval is used to determine how often the running configuration is checked for changes.

To set the Auto Save function:

1. Click the dropdown box next to **Auto Save.**
2. Set the Auto Save interval (5~65535 sec)

Note: If a Firewall is running on the PC that is running the SCP, SFTP or TFTP server, it may need to be temporarily disabled.

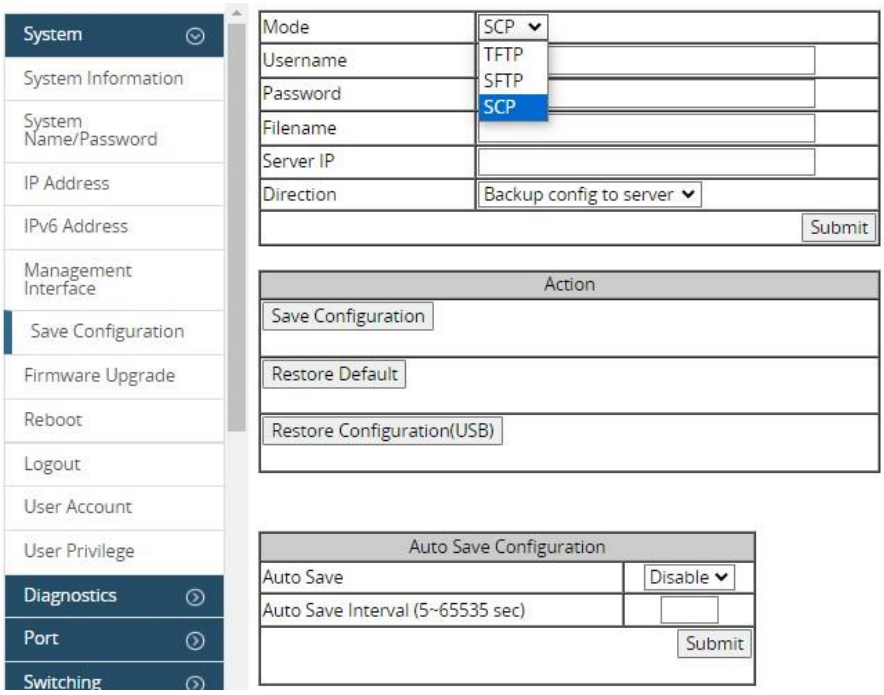


Figure 9: Save Configuration Page

Reset Button Setting

You can define the behavior of the switch's physical reset button, to either just reset the switch to the default password, or reset everything to the default configuration. Select the desired option from the drop-down menu and click **Submit**.

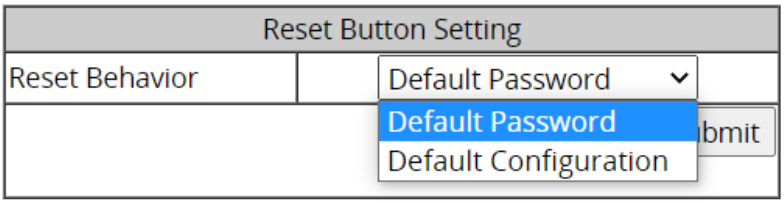


Figure 10: Reset Button Setting

Save Configuration Page using the CLI

For more information on CLI command usage see CLI Command Usage.

Saving a Configuration

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
write memory

Usage Example 1: Saving a Configuration

```
switch_a>enable
switch_a#write memory
Building configuration.....
[OK]
switch_a#q
switch_a#
```

Restore Default Settings

CLI Command Mode: **Privileged Exec Mode**

CLI Command Syntax:
restore default

Usage Example 1: Restoring Defaults

```
switch_a>enable
switch_a#restore default
switch_a#q
switch_a#
```

Load Configuration from an SCP, SFTP or TFTP Server

CLI Command Mode: **Privileged Exec Mode**

CLI Command Syntax:
install config-file <*tftpserver_ipaddress*> <*filename*>

install [image|config-file] sftp <username> <password> <ipaddress> <filename>

Usage Example: Loading a Configuration

```
switch_a>enable
switch_a#install config-file 192.168.1.100 file_name.txt
switch_a#q
switch_a#
```

Enable the USB port privilege

Enable the USB port privilege, global CLI setting to enable/disable USB port as blow.

CLI Command Mode: **Global Mode**

CLI Command Syntax:
//Enable USB port

usb-enable

//Disable USB port

no usb-enable

Load Configuration from USB

CLI Command Mode: **Privileged Exec Mode**

CLI Command Syntax:
install config-file *usb*

Usage Example: Loading a Configuration

```
switch_a>enable
switch_a#install config-file usb
switch_a#q
```

Save Configuration to an SCP, SFTP or TFTP Server

CLI Command Mode: **Privileged Exec Mode**

CLI Command Syntax:
write config-file <*tftpserver_ipaddress*> <*filename*>

write config-file sftp <username> <password> <*sftpserver_ipaddress*> <*filename*>

Usage Example: Saving a Configuration

```
switch_a>enable
switch_a#write config-file 192.168.1.100 flash.tgz
switch_a#q
switch_a>
```

Auto Save Configuration

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
service auto-config enable
no service auto-config enable
service auto-config interval <*number*>

Usage Example 1: Enabling Auto Save and setting the interval

```
switch_a>enable
switch_a#service auto-config enable
switch_a#service auto-config interval 10
switch_a#q
switch_a>
```

Usage Example 2: Disabling Auto Save

```
switch_a>enable
switch_a#no service auto-config enable
switch_a#q
switch_a>
```

Auto USB Backup & Restore Operation

The auto USB backup and restore provide fast and effortless system backup and restoration on managed switches. An automatic backup and restore function can be activated, allowing the running switch's configuration settings will be saved automatically to a connected USB or configuration saved on a connected USB to be automatically loaded onto the switch when the switch is rebooted or power cycled. This greatly cuts down on system downtime in the event of

a switch failure, because a failed switch can be quickly replaced with a new one running the same configuration.

Note: This feature runs when the auto backup to / restore from the USB function is enabled. The USB flash drive format is recommended to be **FAT32**. Please confirm the USB port privilege **enabled** in advance.

Automatic Backup to USB Configuration

When the switch has finished booting and is running, plug in the USB and the reset function will be disabled automatically due to USB presence. Then press and hold the "**reset**" bottom for more than **5** seconds to startup auto backup to the USB. The switch's configuration settings will be automatically saved to the USB flash and the file will be named "model name.conf" (e.g. EX73900X.conf). If there is already a file named "model name.conf", the switch compares whether the file is identical from the switch and do backup if they are not identical. After saving configuration completion, the alarm LED will flash for **10** seconds and then turn off. By this time, the USB can be operated further on the same switch or removed.

To enable Auto backup to the USB on switch using the CLI:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
service auto-usb-backup-config enable
no service auto-usb-backup-config enable

Usage Example 1: Enable Auto USB Backup

```
switch_a>enable
switch_a#configure terminal
switch_a#service auto-usb-backup-config enable
switch_a#q
switch_a>
```

Usage Example 2: Disable Auto USB Backup

```
switch_a>enable
switch_a#configure terminal
switch_a#no service auto-usb-backup-config enable
switch_a#q
switch_a>
```

Automatic Restore from USB Configuration

Power off the switch first, and then plug in the USB. Then power on the switch. Or plug in the USB before rebooting. When the switch has finished booting and is running, the reset function will be disabled automatically due to USB presence. Then press and hold the "**reset**" bottom for more than **5** seconds to startup auto restore from the USB. The switch will check if there is a file named "model name.conf" in the USB folder, and then this feature will compare the configuration data on the switch with the data stored on the USB. If the files are not identical, the configuration currently saved on the USB flash will automatically be loaded onto the switch. Once the restore process is complete, the alarm LED will flash for **10** seconds and then turn off. It will then automatically reboot. By this time, the USB can be removed or continue to be used.

To enable Auto Restore from the USB on switch using the CLI:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
service auto-usb-restore-config enable
no service auto-usb-restore-config enable

Usage Example 1: Enable Auto USB Restore

```
switch_a>enable
switch_a#configure terminal
switch_a#service auto-usb-restore-config enable
switch_a#q
switch_a>
```

Usage Example 2: Disable Auto USB Restore

```
switch_a>enable
switch_a#configure terminal
switch_a#no service auto-usb-restore-config enable
switch_a#q
switch_a>
```

Firmware Upgrade

To navigate to the **Firmware Upgrade** page:

1. Click on the **+** next to **System**
2. Click on **Firmware Upgrade**

To upgrade the firmware on the switch, an SFTP or TFTP server is required, or a USB Flash drive with the new firmware file. The firmware file is in a .TGZ or .IMG format. This is a compressed file; however, it should not be decompressed before updating the switch.

To update the firmware on the switch via SFTP or TFTP:

1. Copy the firmware file to the correct directory for your SFTP or TFTP server. The correct directory depends on your server settings
2. Enter the filename of the firmware in the **Filename** text box.
3. Enter the IP Address of your SFTP or TFTP server in the **Server IP** text box.
4. Click on the **Upgrade** button.
5. During the firmware upgrade you will see the following messages. Do not reboot or unplug the switch until the final message is received.
    a. `Downloading now, please wait...`
    b. `tftp <filename>.img from ip <ip address> success!! Install now. This may take several minutes, please wait...`
    c. `Firmware upgrade success!`

Note: If a Firewall is running on the PC that is running the SFTP or TFTP server it may need to be temporarily disabled.

To upgrade firmware via USB, insert USB Flash drive into the USP port on the switch, and select **USB** as the mode on the firmware upgrade page. Enter the firmware filename (i.e. flash759-5.03.0.2.tgz) in the **Filename** field, then click the **Upgrade** button.

Firmware has protection mechanism; unauthorized firmware will be blocked during the download process. Please download the latest firmware from website.(www.etherwan.com)

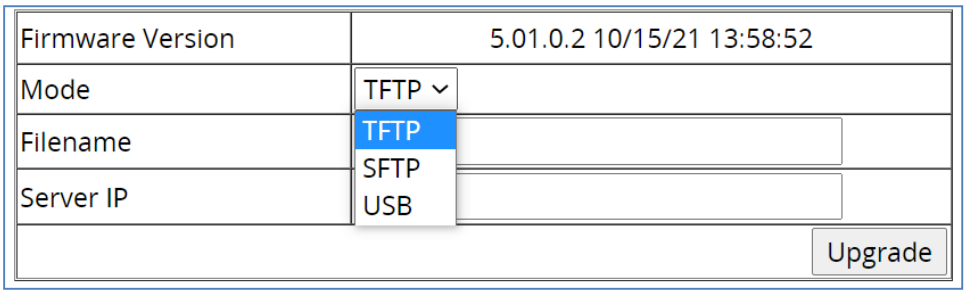


Figure 8: Firmware Upgrade Page

Firmware can also be updated through the web browser. Select the firmware file with the **Choose File** button, then click **Upload file**.

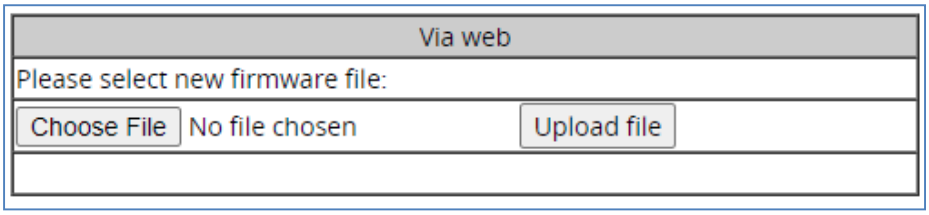


Figure 11: Web Firmware select Page

Firmware Update using the CLI

CLI Command Mode: **Privileged Exec Mode**

CLI Command Syntax:
install image <*tftpserver_ipaddress*> <*filename*>

install image sftp <username> <password> <*sftpserver_ipaddress*> <*filename*>

Usage Example:

```
switch_a>enable
switch_a#install image 192.168.1.100 flash.tgz
switch_a#q
```

To upgrade firmware via USB, use the CLI commands below:

CLI Command Syntax: **install image usb filename**

Usage Example:

```
switch_a>enable
switch_a#install image usb flash.tgz
switch_a#q
```

Note: Depending on the firmware being loaded, the extension may not be .tgz. The switch does not use the extension to validate firmware.

Booting From Alternate (Backup) Firmware

Under certain circumstances, such as when there is a loss of power during an upgrade, the firmware build on the switch can become unstable. To prevent the switch from becoming unbootable in this situation, there are two firmware images stored on the switch: primary and backup. If the primary firmware image becomes unstable, the switch will detect it automatically and boot from the backup image on the next boot.

You can also manually boot from the backup firmware image. To do so, follow these steps:

1. Connect to the switch's RS-232 port with a terminal emulator.
2. Power cycle the switch (turn the power off and then on).
3. While the switch is rebooting, hold down **Ctrl + C**. This will cause the switch to enter CFE mode. The prompt should look like this:

```
CFE_1.5>
```

4. Use the command **boot_image0** and **boot_image1** to manually boot from the primary and alternate firmware images respectively. Future boots will be from the image selected with this command.

When a loss of power occurs during an upgrade the system configuration will keep the last configuration unchanged; therefore, booting from the primary firmware image or booting from the backup image can achieve regular operation without any missing information.

Reboot

To navigate to the **Reboot** page:

1. Click on the **+** next to **System**
2. Click on **Reboot**

To reboot the switch:

1. Click on the **Reboot** button.
2. Click OK on the popup message.

Reboot using the CLI

CLI Command Mode: **Privileged Exec Mode**

CLI Command Syntax:
reload

Usage Example:

```
switch_a>enable
switch_a#reload
Reboot now, please wait...
```

Logout

To logout of the Web Configuration Console:

1. Click on the **+** next to **System**
2. Click on **Logout**

Logout from the CLI

CLI Command Mode: **User Exec mode or Privileged Exec Mode**

CLI Command Syntax:
logout

User Account Page

To navigate to the **User Account** page:

1. Click on the **+** next to **System**
2. Click on **User Account**

From the **User Account** page, multiple users can be setup with different access privileges to the switch. There are two modes that can be used, **Single-User** or **Multi-User**.

Changing the User Mode

To set the user mode (see Figure 9):

1. Select **Single-User**, **Multi-User**, **Radius-User**, **Radius-User Local**, **TACACS**, or **TACACS Local** in the dropdown box in the Multi-User Mode section.
2. Click on the **Update Setting** button.
3. Click OK on the Popup message that appears.

Note: Changing the user mode saves the configuration and reboots the switch.

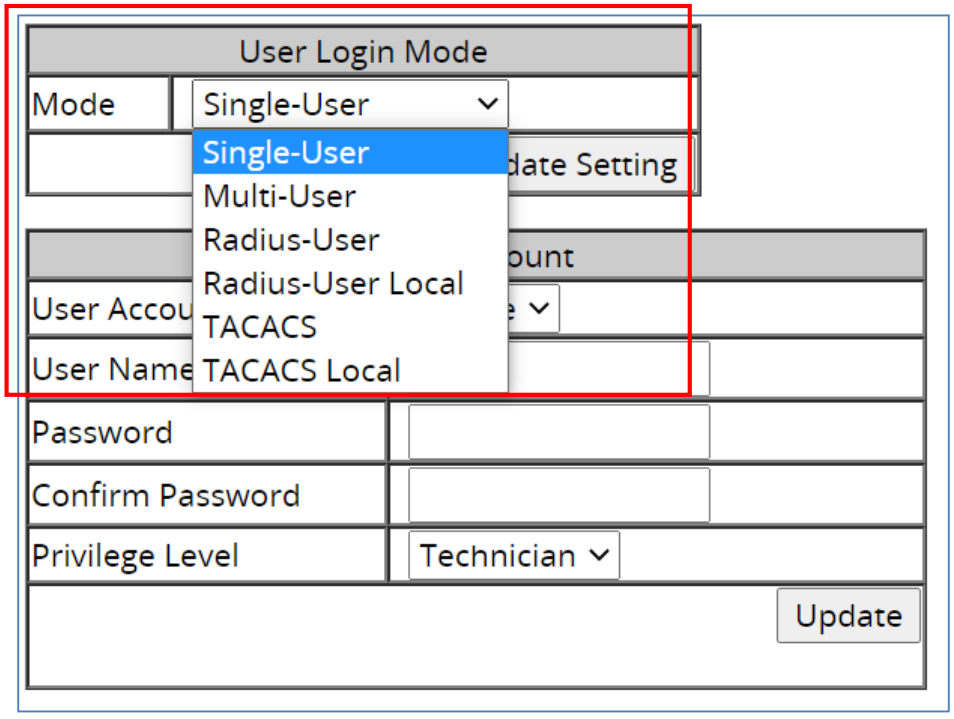


Figure 9: User Mode

Creating a New User

To create a new user (see Figure 10):

1. Choose the **Create** option from the dropdown list next to the **User Account** row heading.
2. Enter a User Name (case sensitive) for the new user in the **User Name** text box.
3. Enter a Password for the new user in the **Password** text box.
4. Re-enter the Password in the **Confirm Password** text box.
5. Select a Privilege Level from the dropdown list next to the **Privilege Level** row heading. For more information on Privilege levels see the User Privilege Configuration.
6. Click on the **Update** button.
7. Save the configuration (See the Save Configuration Page)

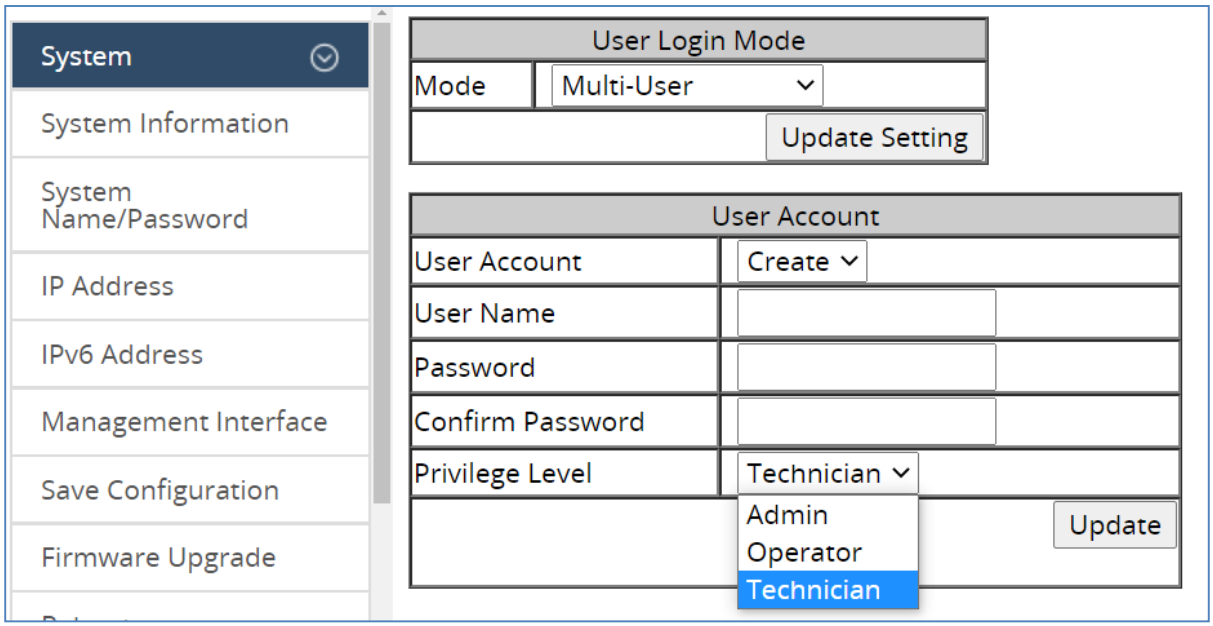


Figure 10: Creating Users

Changing an Existing User Account

To make modifications to an existing user account:

1. Choose an existing user from the dropdown list next to the **User Account** row heading (see Figure 11).
2. Change the password and/or access level following the steps in Creating a New User.
3. To delete an existing user, select the user as in step 1 and then click on the **Delete** button (see Figure 12).

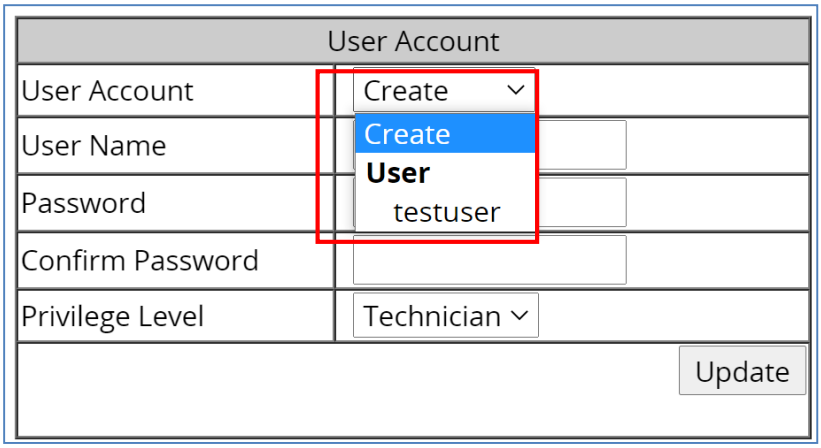


Figure 11: Selecting an Existing User Account

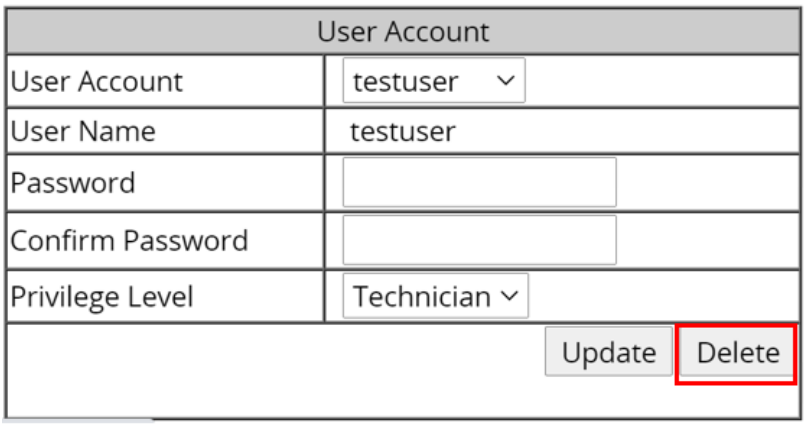


Figure 12: Deleting a User Account

User Privilege Configuration

To navigate to the **User Privilege** page:

1. Click on the **+** next to **System.**
2. Click on **User Privilege**. (see Figure 16)

There are 3 different Privilege levels on the switch.

- **Admin** – Has access to all configuration and administration of the switch.
- **Technician** – Configurable by Admin – By default no configuration ability is given.
- **Operator** – Configurable by Admin – By default no configuration ability is given.

The User Privilege Configuration page allows specific configuration and/or administration levels to be assigned or removed from the Technician and Operator user roles.

Note: For each function, an operator's privilege cannot be higher than a technician's

To configure the privileges for each user access level, follow the below steps:

1. For each of the configuration options listed under **Web function \ User Privilege** (see Figure 13), select the proper privilege from the drop-down list under the appropriate user access level (**Technician** or **Operator**). The valid options are:
    a. **Show, Hidden, Read-Only, Read-Write**
2. Click on the **Update** button at the bottom of the page.
3. Save the configuration (see Save Configuration)

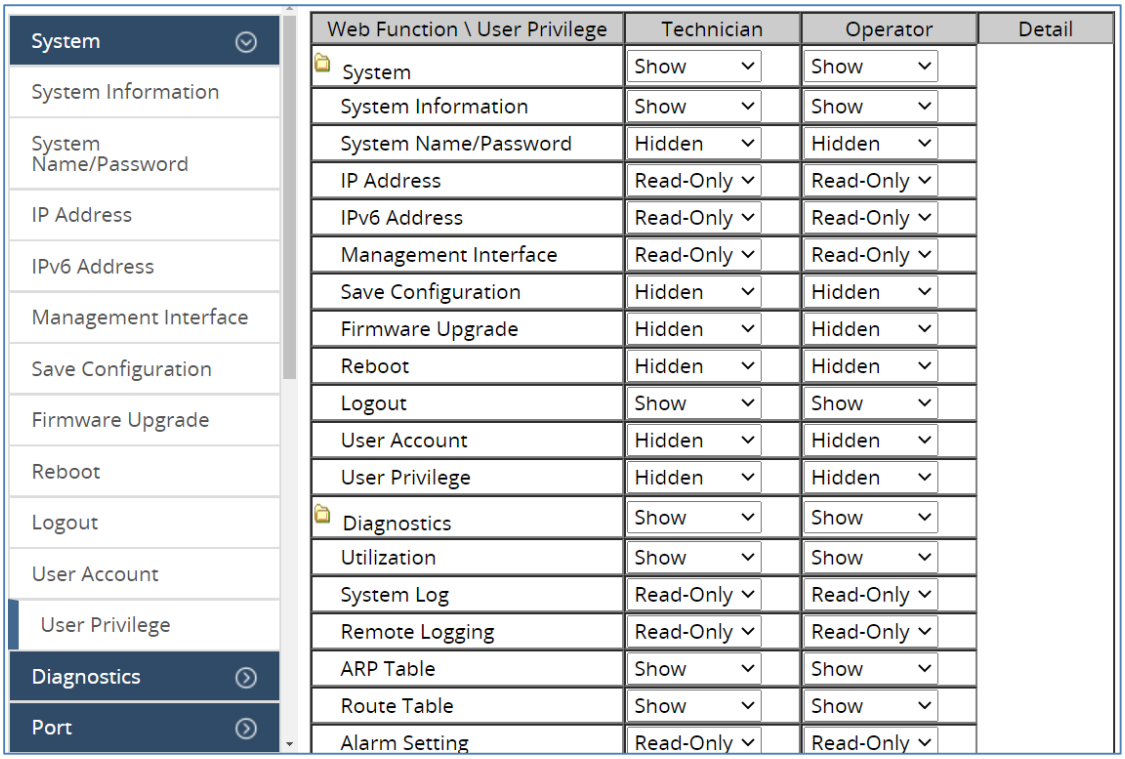


Figure 13: User Privilege Page

User Account Settings using the CLI

Multi-User Mode

To enable the multi-user feature, use the following CLI commands:

CLI Command Mode: **Line Configuration Mode**

CLI Command Syntax: **login local**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#line console 0
switch_a(config-line)#login local
% Switching Single/Multi/Radius-User mode need to reboot the
switch to take effect!
switch_a(config-line)#q
switch_a(config)#q
switch_a#
```

Single User Mode

To enable the single-user feature, use the following CLI commands:

CLI Command Mode: **Line Configuration Mode**

CLI Command Syntax: **login**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#line console 0
switch_a(config-line)#login
% Switching Single/Multi/Radius-User mode need to reboot the
switch to take effect!
switch_a(config-line)#q
switch_a(config)#q
switch_a#
```

Creating a New User

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
username ***<user name-4 to 16 characters>*** **privilege** ***<admin|operator|technician>*** **password** ***< 8|blank> <password-1 to 35 characters>***

Note: The optional **<8>** CLI command after the CLI command **password** is used to specify that the password will be displayed in encrypted form in the configuration file, and the User Account authentication process is obscured.

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#username user1 privilege operator password 1234
switch_a(config)#username user1 privilege operator password 8 1234
switch_a(config)#username user2 privilege technician password 4321
switch_a(config)#username user2 privilege technician password 8 4321
switch_a(config)#username user3 privilege admin password 5678
switch_a(config)#username user3 privilege admin password 8 5678
switch_a(config)#q
switch_a#
```

Permissions

Permissions must be set using the Web GUI. See User Privilege Configuration.

DIAGNOSTICS

Utilization

To navigate to the **Utilization** page:

1. Click on the **+** next to **Diagnostics**.
2. Click on **Utilization**.

The **Utilization** page shows (see Figure 14):

- **CPU Utilization** – Current and Max Utilization
- **Memory Utilization** – Total, Used and Free Memory

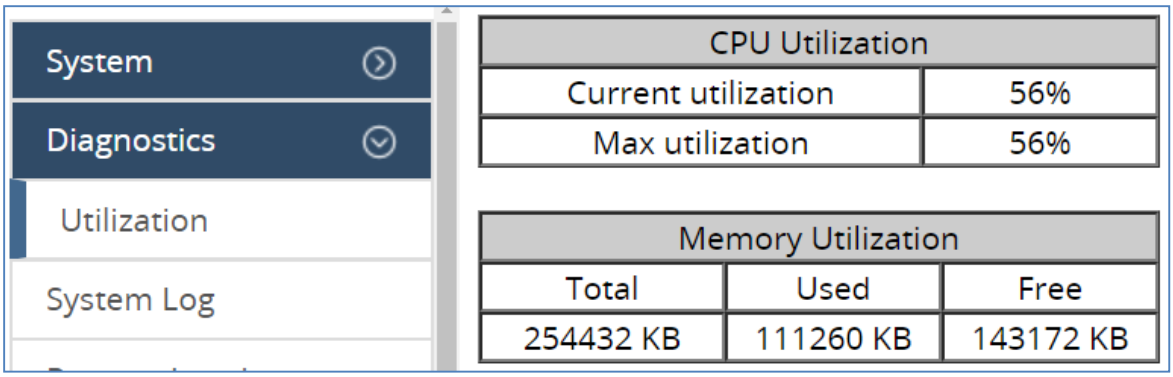


Figure 14: Utilization Page

System Log

To navigate to the **System Log** page:

1. Click on the **+** next to **Diagnostics**.
2. Click on **System Log**.

In addition to saving the system logging messages in the memory (RAM) of the switch, messages can be also saved into the switch's non-volatile memory (flash). Messages saved on the flash memory persist even when the switch is rebooted.

Log Severity Levels

Each log message contains a Severity field that indicates the severity of the event that caused the log message. For each log destination, you can define a severity level threshold.

This switch will filter log messages based on severity level. A message will be logged to permanent memory (Flash) or the RAM when a message's severity level is less than or equal to this setting. This change will take effect immediately. Each of the RAM and the Flash has its own severity setting.

Examples:

Set the level to value 3. All messages with severity level from 0 (Emergency) to 3 (Error) will be saved to the flash.

Set the level to value 7. All messages with severity level from 0(Emergency) to 7(Debug) will be saved to the flash.

To configure system log settings (see Figure 19):

1. Select a **Severity Level** from 0 to 7 for messages saved to RAM or Flash memory. A message will be logged to permanent memory (Flash) or the RAM when a message's severity level is less than or equal to this setting.
2. Click a radio button next to either Flash or Memory to view the logs on that medium.
3. Select **Enable** or **Disable** for **Auto Refresh**, and select the maximim number of messages to be viewed on one page.
4. Click **Update Setting**.

Click the Export Logs button to export logs to a USB flash drive. The filenames will contain the switch model number at the beginning:

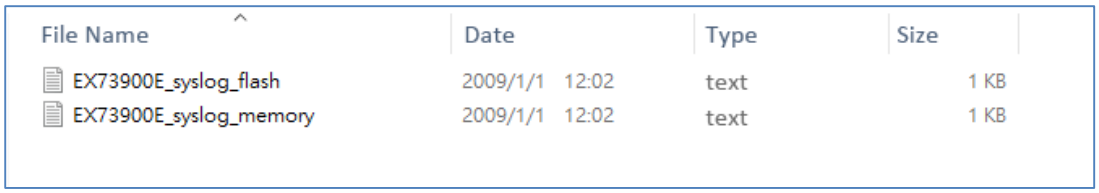


Figure 15: File export

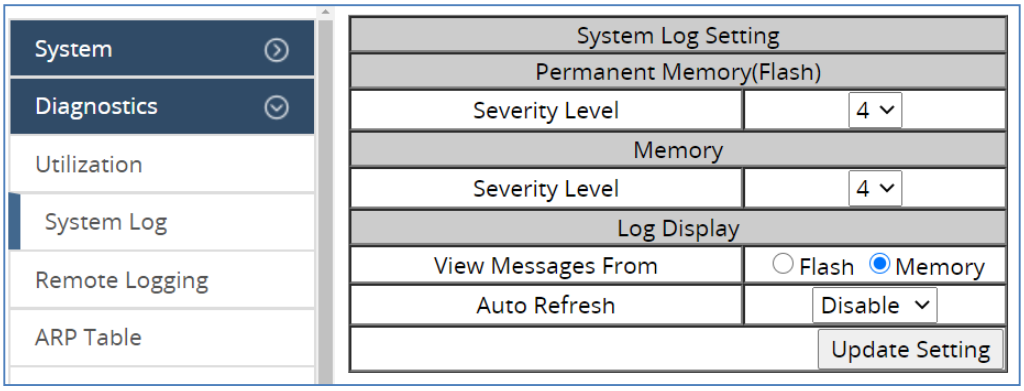


Figure 19: System Log Setting

At the bottom of the screen, the System Log shows the logs for either Permanent Memory (Flash) or Memory (RAM), depending on the System Log Settings (above). Use the **Clear Log** button to clear the System Log for the selecred medium.

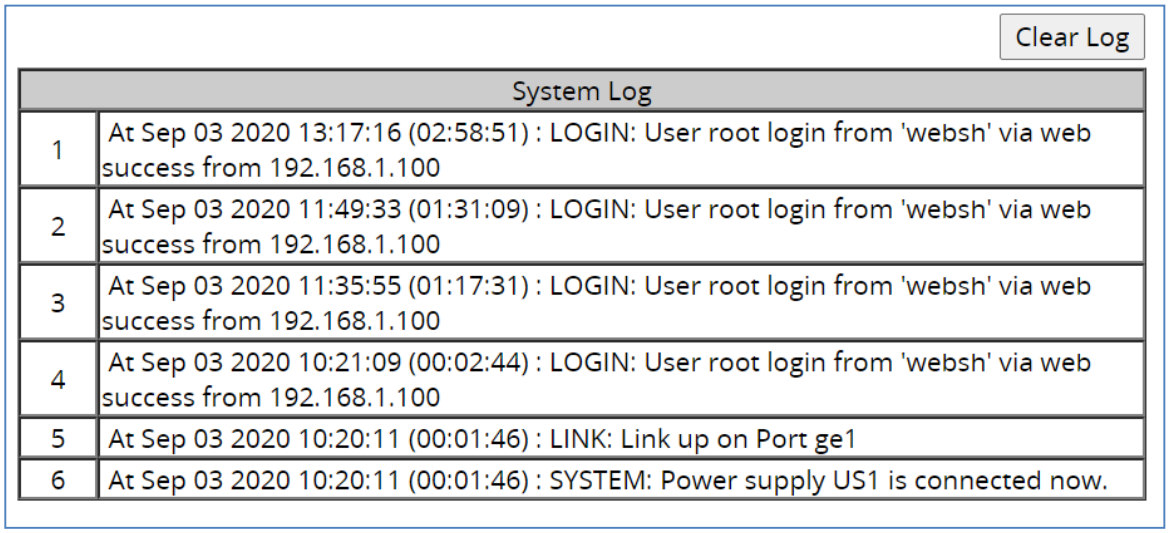


Figure 16: System Log

System Log using CLI commands

Configure the message view in the GUI.

CLI Command Mode: **Global config**

CLI Command Syntax:
system-log display permanent
system-log display memory

Usage Example:

```
switch_a(config)# system-log display memory
```

System Log general configuration – set severity for saved logs. Storage location: Flash (permanent memory). This command will take effect immediately.

CLI Command Mode: **Global config**

CLI Command Syntax:
switch_a(config)# system-log severity permanent <0-7>

Usage Example:

```
switch_a(config)# system-log severity permanent 5
```

Set severity for saved logs - Storage location: Memory (RAM). This command will take effect immediately.

CLI Command Mode: **Global config**

CLI Command Syntax:
switch_a(config)# system-log severity memory <0-7>

Usage Example:

```
switch_a(config)# system-log severity memory 5
```

Configure Auto Refresh on the WebUI (in number of minutes). The messages on the web page will be refreshed automatically, at the specified interval. However, this command applies to the first page of messages only.

CLI Command Mode: **Global config**

CLI Command Syntax:
system-log page refresh (disable | 1 | 2 | 5 | 10)

Usage Example:

```
switch_a(config)# system-log page refresh 10
```

Configuring Page Size. Specify the maximum number of messages to be displayed with each SHOW command. This command applies to flash view only.

CLI Command Mode: **Global config**

CLI Command Syntax:
system-log page size (50 | 100 | 200 | 1000)

Usage Example:

```
switch_a(config)# system-log page size 50
```

Clear the Log. Clear all messages in flash or memory.

CLI Command Mode: **Global config**

CLI Command Syntax:
Flash
system-log permanent clear
Memory
system-log clear

Usage Example:

```
switch_a(config)# system-log clear
```

Show commands. Display messages stored in the flash (permanent memory) or in memory (RAM).

CLI Command Mode: **Exec Mode or Privileged Exec Mode**

CLI Command Syntax:
Flash
show system-log permanent (first | next | prev)
Memory

show system-log

Usage Example:

```
switch_a(config)# show system-log
```

Export system logs to USB.

CLI Command Mode: **Exec Mode or Privileged Exec Mode**

CLI Command Syntax:
Flash
export logs flash
export logs memory

Remote Logging

To navigate to the **Remote Logging** page:

1. Click on the **+** next to **Diagnostics**.

2. Click on **Remote Logging**.

Remote Logging to a Syslog server allows administrators to log important system and debugging information. The Remote Logging configuration page allows reporting to a Syslog server to be enabled or disabled as well as management of a list of Syslog servers to report to (see Figure 17).

To configure the Remote Logging on the switch:

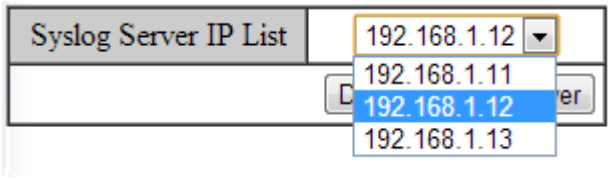
1. Click on the **Enable** or **Disable** radio button under Remote Logging.
2. Click on the **Update Setting** button.

To add a Syslog server:

1. Enter the IP Address and the port of the Syslog Server in the **Syslog Server IP** text box.
2. Click on the **Add Syslog Server** button.

To delete a Syslog server from the list of servers currently on the switch:

1. Select the Syslog server from the Drop down box



2. Click on the **Delete Syslog Server** button



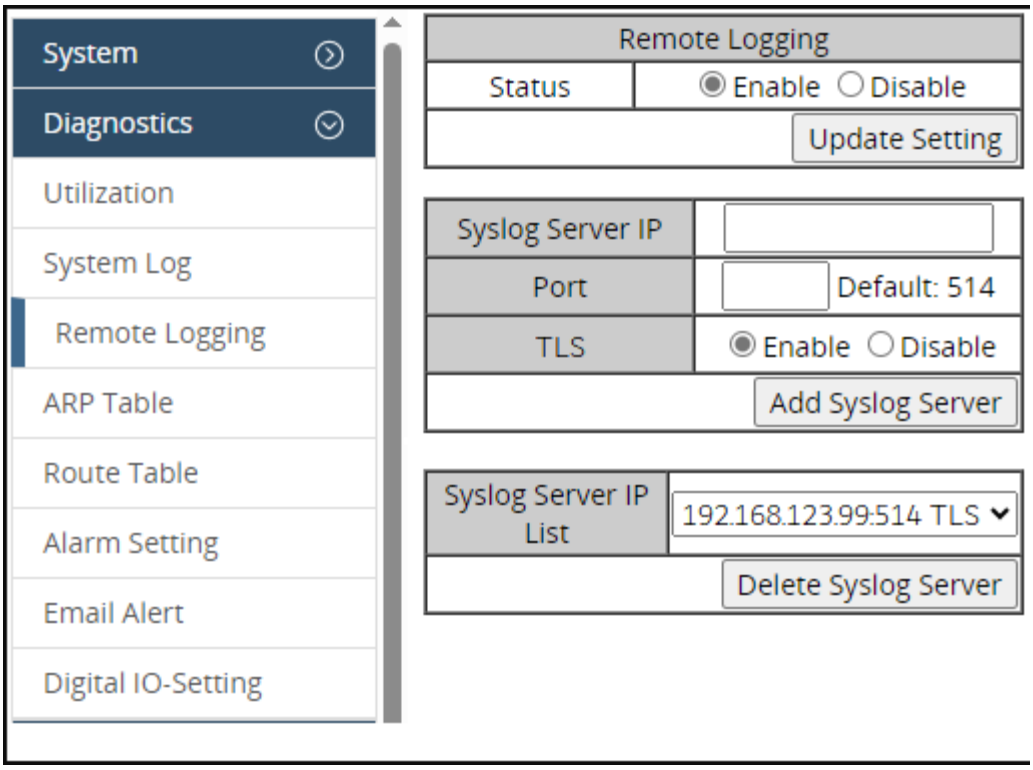


Figure 17: Remote Logging Page

Remote Logging using CLI commands

Enable/Disable Remote Logging

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
remote-log enable
no remote-log enable

Usage Example 1: Enable Remote Logging

```
switch_a>enable
switch_a#remote-log enable
switch_a#q
switch_a#
```

Usage Example 2: Disable Remote Logging

```
switch_a>enable
switch_a#no remote-log enable
switch_a#q
switch_a#
```

Add/Delete a Remote Logging Host

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
remote-log add *<ip_address>* *<port>*
remote-log del *<ip_address>*
remote-log add A.B.C.D (<0-65535>|) tls
remote-log del A.B.C.D (<0-65535>|)
remote-log del all

Usage Example 1: Add a Remote Logging Host

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# int ge1
switch_a(config)-if#remote-log add 192.168.1.100 1524
switch_a#q
switch_a#
```

Usage Example 2: Delete a Remote Logging Host

```
switch_a(config)-if#remote-log del 192.168.1.100
switch_a#q
```

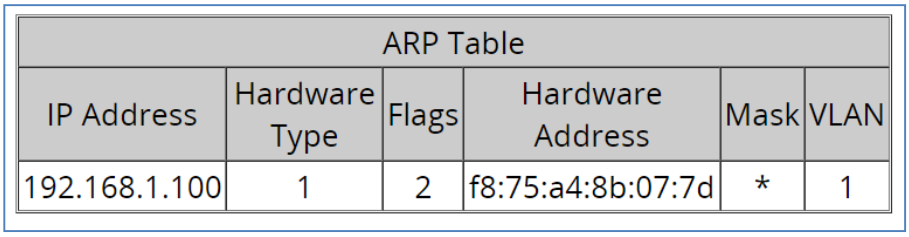
ARP Table

To navigate to the **ARP Table** page:

1. Click on the **+** next to **Diagnostics**.
2. Click on **ARP Table**.

The ARP Table page shows ARP (Address Resolution Protocol) entries that are stored in the Switches ARP Table. This is useful for System Administrators for troubleshooting purposes. The information shown is:

- **IP Address** of the listed device
- **Hardware Type** – For Ethernet devices this will always be **1**.
- **Flags**
  - **2** = Device responded to ARP Request
  - **0** = No response to ARP Request
- **Hardware Address** – MAC Address of the listed device
- **VLAN** – The VLAN that the listed device is on



ARP Table

IP Address	Hardware Type	Flags	Hardware Address	Mask	VLAN
192.168.1.100	1	2	f8:75:a4:8b:07:7d	*	1

Figure 18: ARP Table

ARP Table using CLI Commands

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
show arp-table

Usage Example:

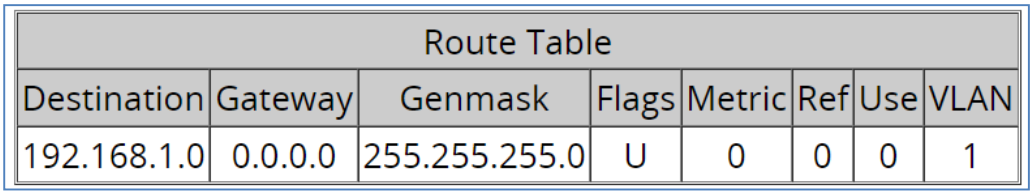
```
switch_a>enable
switch_a#show arp-table
IP address      HW type  Flags  HW address              Mask    VLAN
10.58.7.130     1        2      00:50:B6:65:2A:22       *       1
switch_a#q
```

Route Table

To navigate to the **Route Table** page:

1. Click on the **+** next to **Diagnostics**.
2. Click on **Route Table**.

The Route Table lists the routes to network destinations and metrics (distances) that are associated with those routes. The Route Table contains information about the topology of the network around it.



Route Table							
Destination	Gateway	Genmask	Flags	Metric	Ref	Use	VLAN
192.168.1.0	0.0.0.0	255.255.255.0	U	0	0	0	1

Figure 19: Route Table

Route Table Using CLI Commands

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
show route-table

Usage Example:

```
switch_a>enable
switch_a#show route-table
Destination     Gateway         Genmask         Flags Metric Ref   Use   VLAN
10.58.7.0       0.0.0.0         255.255.255.0   U     0      0     0     1
switch_a#q
switch_a#
```

Alarm Setting

This setting applies only to Switch models that have a hardware relay.

To navigate to the **Alarm Setting** page:

1. Click on the **+** next to **Diagnostics**.
2. Click on **Alarm Setting**.

The Alarm Setting page allows users to define Ethernet port **Link-down** and Power failure alarms for triggering an alarm using the relay on the switch.
To configure an Ethernet port or Power input:

1. Select an Ethernet port or Power input from the dropdown box (see Figure 20).

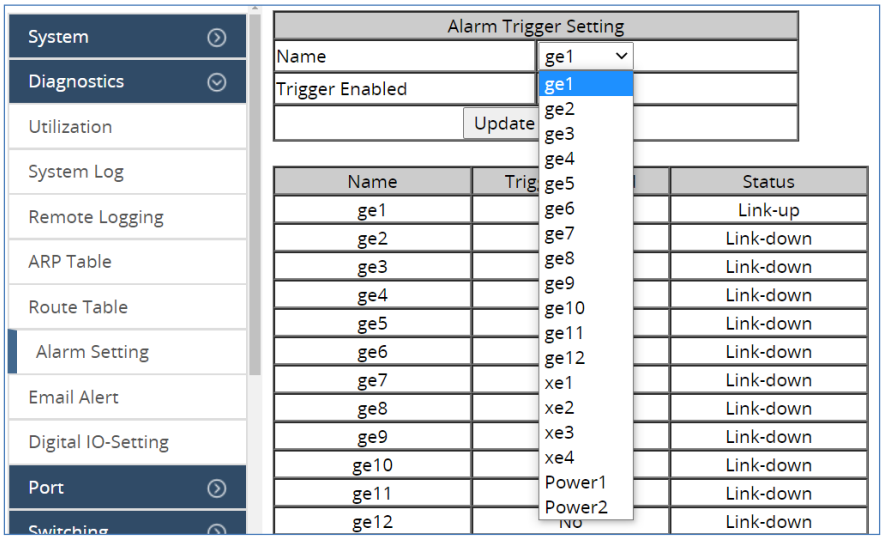


Figure 20: Alarm Trigger

3. Select **YES** or **NO** from the dropdown box next to Trigger Enabled (see Figure 21).
4. Click **Update Setting** to save any changes made.

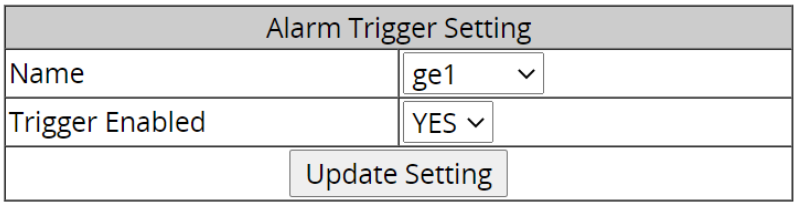


Figure 21: Trigger Enable

Alarm Setting Using CLI Commands

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
alarm-trigger if <interface> | power <1 - 3>
no alarm-trigger if <interface> | power <1 - 3>

Usage Example:
Enable alarm on interface ge1

```
switch_a>enable
switch_a#conf t
switch_a(config)alarm-trigger if ge1
switch_a(config)#q
switch_a#
```

Enable alarm on input power 2

```
switch_a>enable
switch_a#conf t
switch_a(config)alarm-trigger power 2
switch_a(config)#q
switch_a#
```

Dying Gasp

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
dying primary (snmp-trap, syslog)

Setting EEE (Energy-Efficient Ethernet)

Energy-Efficient Ethernet (EEE) reduces the switch's power consumption during periods of low activity. Use the **show eee** command in Privileged Exec mode to view the EEE status of all ports. EEE is disabled by default.

For more information on CLI command usage see CLI Command Usage.

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
eee enable
no eee enable

Usage Example:
Enable alarm on interface ge1

```
switch_a>enable
switch_a#conf t
switch_a#int ge5
switch_a(config-if)eee enable
```

Email Alert

To navigate to the **Email Alert** page:

1. Click on the **+** next to **Diagnostics**.
2. Click on **Email Alert**.

The switch can send email alerts to up to five recipients when a digital input or environmental alarm is triggered. The Email Alert settings page allows users to configure the email server and recipient list.

To enable email notifications:

1. Choose **Enable** from the drop down menu in the **SMTP Server** field.
2. Click on the **Update Setting** button under the field.

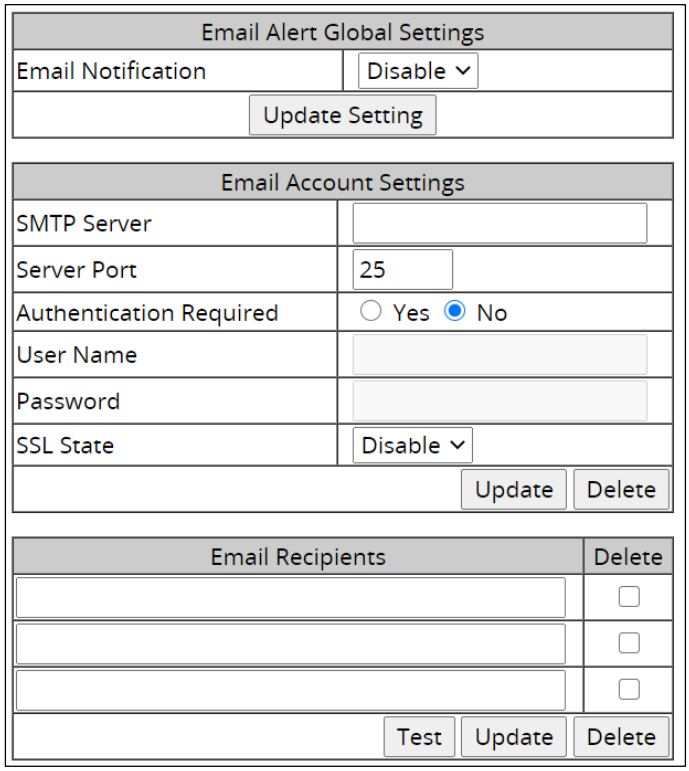


Figure 22: Email ALERT Settings

To configure mail server and recipient email addresses:

1. Enter the name of the SMTP server to be used in the corresponding field.
2. Enter the email address of the sending account.

3. Enter the password for the email account being used, and select **Enable** or **Disable** for SSL (Secure Sockets Layer).
4. Click the Update button.

Note: If SSL is disabled, port 25 will be used to send email. If SSL is enabled, port 465 will be used.

You can view, add, and delete email recipients in the fields at the bottom of the page. Only one email address can be added at a time.

Digital IO-Setting

To navigate to the **Digital IO-Setting** page:

1. Click on the **+** next to **Diagnostics**.
2. Click on **Digital IO-Setting**.

The Digital IO-Setting page allows for quick configuration and enabling of digital input and environmental alarms.

To enable digital input alarms globally:

1. Choose **Enable** from the drop down menu in the **Digital Input/Sensor Monitoring** field, then enter a monitoring interval in the corresponding field.

2. Click on the **Update Setting** button to the right of the field.

To enable specific digital input alarms:

1. Enter a name or description of the alarm in the **Description** field. This will display in any emails sent if the alarm is triggered.

2. In the **Alert** field, choose **Enable/High** from the drop-down menu if you want the alarm to trigger in an occurrence of high voltage (wet contact), or Open state (dry contact). Choose **Enable/Low** if you want the alarm to trigger in an occurrence of low voltage (wet contact), or Closed to ground state (dry contact).

3. Set the Min Interval in seconds.This is the set minimum period between successive traps, range from 0 to 3600 seconds.

4. Click on the **Update Setting** button at the bottom right to put the new settings into effect. **Then navigate to the Email configuration page.**

5. Set the alert conditions for Digital Outputs (DO) 1 and 2 at the bottom of the page from the drop-down menu next to each. Digital output alert can be triggered by system events or digital-inputs (DI).

If DI 1 is selected from DO 1, DI 1 will generate a DI event and trigger DO 1.

If DI 1 AND DI 2 are selected from DO 1, DI 1 and DI 2 must both generate DI events to trigger DO 1.

If DI 1 OR DI 2 are selected from DO 1, either DI 1 or DI 2 will trigger DO 1 when an event in generated.

The logic above is the same for setting DO2.

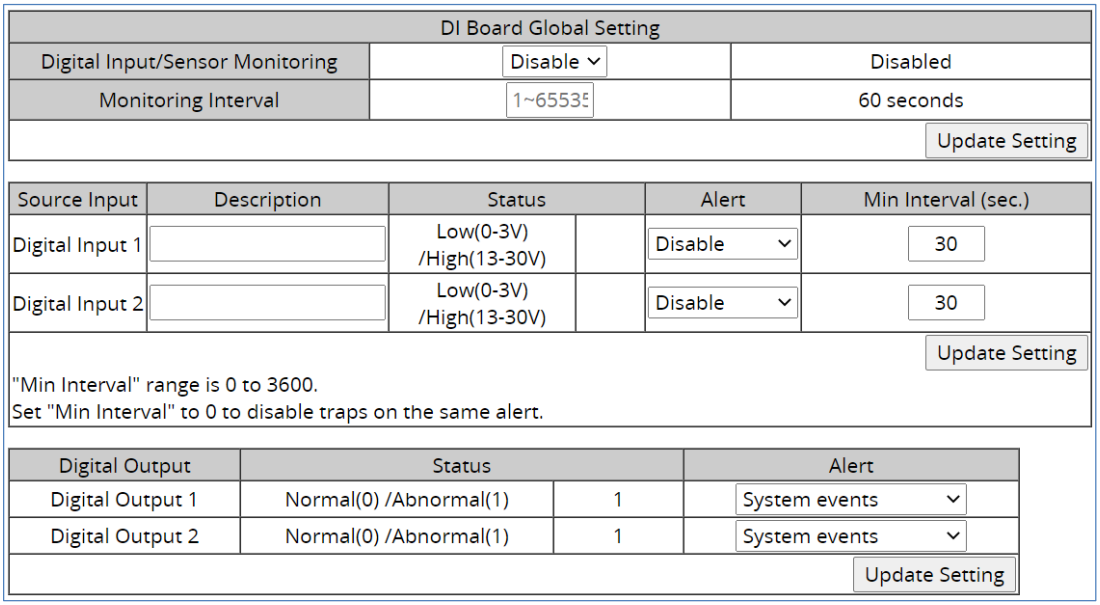


Figure 23: Digital IO Setting

Digital IO Setting Using CLI Commands

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:

[no] digital-input enable
digital-input polling-interval <1-65535>
digital-input <1-2> alarm {high | low | disable}
digital-input <1-2> description WORD
digital-input <1-2> min-interval <0-3600>
digital-outputs <1-2> trigger-type {system-event |digital-input (PIN combination)}

Usage Example:
Enable alarm on interface ge1

```
switch_a>enable
switch_a#conf t
switch_a(config)digital-input enable
switch_a(config) digital-input 1 alarm high
switch_a(config) digital-outputs 1 trigger-type digital-input 1
or 2
```

Direct DO Trigger

Manually open/close and Target IP Watchdog control options in Digital output

1. Added the Manually open/close option in the Alert field to manually control the status of the output side (including CLI commands and web operation screens and SNMP control).

2. In the event that the settings need to be changed manually, the user can switch the setting to Manually open to actively cut off the corresponding output connection. When the event ends, the user can change the setting back to Manually close to restore the corresponding output connection.

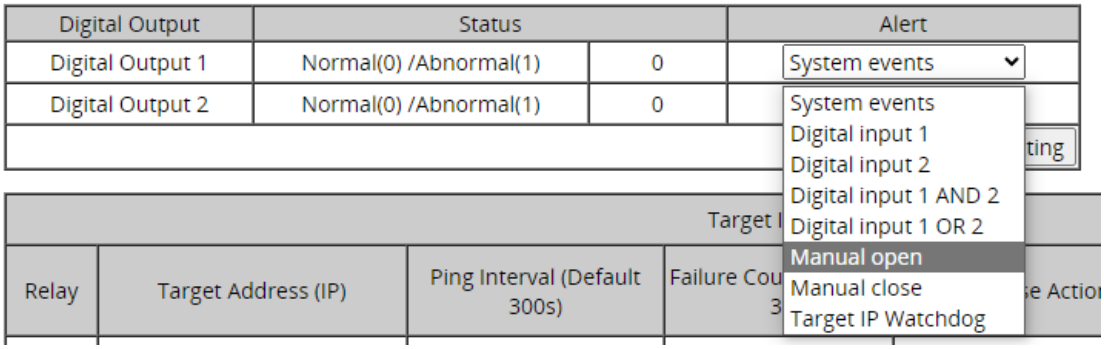


Figure 24: Digital Output Trigger menu

Target IP Watchdog Config

1. Added Target IP Watchdog Config to enable the device to Auto detect and open/close DO (including CLI commands, web operation screen and SNMP control).

2. Added a new detection mode that allows users to set the system to automatically open/close DO connections when the connected device has no response action.

Usage Example:

1. Click on Diagnostics -> Digital IO-Setting.
2. Set Digital Output 1/2 Alert as "Target IP Watchdog".
3. Set "Target IP Watchdog Config" as below.

Target Address (IP): DO1 (1.1.1.1), DO2 (2.2.2.2)
Ping Interval: 30
Failure Count: 1
No Response Action: DO1 (Relay Open), DO2 (Relay Close)
Startup Delay: 30

4. While the switch executes the startup delay time and ping fail occured (about 60s) to trigger the relay function and the current status were displayed. (DO1: Relay Open/ DO2: Relay Close).

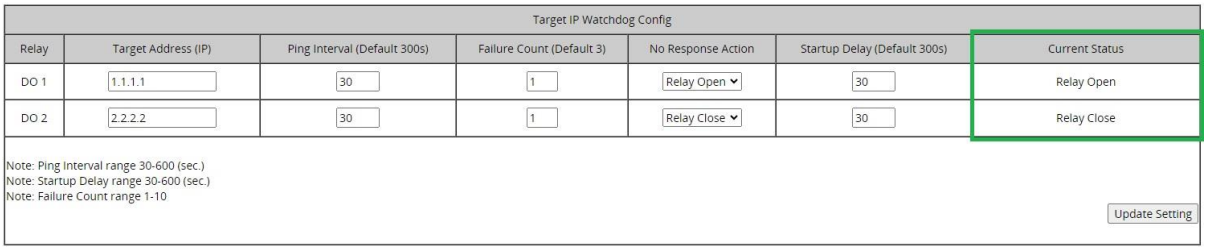


Figure 25: Digital Output status

PORT

Configuration

To navigate to the **Configuration** page:

1. Click on the **+** next to **Port**.
2. Click on **Configuration**.

Port configuration contains such useful features as flow control, port speed, and duplex settings. Some users will find these settings very valuable such as when the switch is connected to a latency-critical device such as a VOIP phone or IP camera or video multiplexor. In these cases and others, the ability to alter the port settings can make the difference between a poorly responding device and one that functions without loss of data or clarity.

The **Configuration** page shows (see Figure 26):

- **Port Number** – xe(n) for 10Gb ports and ge(n) for 1 Gb
- **Link Status** – Operational State of the Port's Link (Read-Only)
- **Port Description** – User-supplied Port Description
- **Admin Setting** – Administratively Enable or Disable the Port.

- **Speed** – Speed and Duplex Settings for Port.
- **Flow Control** – State of Flow Control for the Port.

To provide a description to a port on the switch:

1. Click in the **Description** text box for the appropriate port.
2. Type in the description of the port.
3. Click on the **Submit** button.

To enable or disable a port on the switch:

1. Click on the drop-down box under Admin Setting and select either **Link Up** or **Link Down**.
2. Click on the **Submit** button.

Ports that have been disabled in this way will display “Link Down” when this screen is navigated to.

To set the Port Speed and/or Port Duplex Settings on the switch:

1. Click on the drop-down box under **Speed** and select the desired port speed / duplex settings for that port. Please note, not all port types will have the same options. 10/100/1Gb ports will have five options for speed/duplex while 1/10Gb ports will have three.
2. Click on the **Submit** button.

To enable or disable a port’s Flow Control settings on the switch:

1. Click on the drop-down box under Flow Control and select either **Enable** or **Disable**. Flow Control is disabled by default.
2. Click on the **Submit** button.

Port	Link Status	Port Description	Port type	IP address (A.B.C.D/M)	Admin Setting	Speed	EEE	Flow Control
ge1	Running		Switch port		Link Up	Auto	Disable	Disable
ge2	Down		Switch port		Link Up	Auto	Disable	Disable
ge3	Down		Switch port		Link Up	Auto	Disable	Disable
ge4	Down		Switch port		Link Up	Auto	Disable	Disable
ge5	Down		Switch port		Link Up	Auto	Disable	Disable
ge6	Down		Switch port		Link Up	Auto	Disable	Disable
ge7	Down		Switch port		Link Up	Auto	Disable	Disable
ge8	Down		Switch port		Link Up	Auto	Disable	Disable
ge9	Down		Switch port		Link Up	Auto	Disable	Disable
ge10	Down		Switch port		Link Up	Auto	Disable	Disable
ge11	Down		Switch port		Link Up	Auto	Disable	Disable
ge12	Down		Switch port		Link Up	Auto	Disable	Disable
xe1	Down		Switch port		Link Up	Auto DDM	Disable	Disable
xe2	Down		Switch port		Link Up	Auto DDM	Disable	Disable
xe3	Down		Switch port		Link Up	Auto DDM	Disable	Disable
xe4	Down		Switch port		Link Up	Auto DDM	Disable	Disable

Figure 26: Port Configuration

Port Status

To navigate to the **Port Status** page:

1. Click on the **+** next to **Port**.
2. Click on **Port Status**.

This page is a read-only page that lists the settings described in the previous section. It is useful if all the user intends to do is read the values of the port settings, not modify the port settings. .The Port Status page shows (see Figure 27):

- **Port Number** – xe(n) for 10Gb ports and ge(n) for 1Gb
- **Link Status** – Operational State of the Port's Link
- **Port Description** – User-supplied Port Description
- **Port Type** – Denotes the port type
- **IP Address** – Shows the defined IP address for the port, if defined
- **Speed** – Speed Settings for Port ("Auto" option is still under development)
- **Duplex** – Duplex status
- **EEE** – Shows whether EEE (Energy-Efficient Ethernet) is enabled or disabled for the port
- **Flow Control** – State of Flow Control for the port, enabled or disabled

Port	Link Status	Port Description	Port type	IP address	Speed	Duplex	EEE	Flow Control
ge1	Running		Switch port	-	1000M	Auto	Disable	Disable
ge2	Down		Switch port	-	1000M	Auto	Disable	Disable
ge3	Down		Switch port	-	1000M	Auto	Disable	Disable
ge4	Down		Switch port	-	1000M	Auto	Disable	Disable
ge5	Down		Switch port	-	1000M	Auto	Disable	Disable
ge6	Down		Switch port	-	1000M	Auto	Disable	Disable
ge7	Down		Switch port	-	1000M	Auto	Disable	Disable
ge8	Down		Switch port	-	1000M	Auto	Disable	Disable
ge9	Down		Switch port	-	1000M	Auto	Disable	Disable
ge10	Down		Switch port	-	1000M	Auto	Disable	Disable
ge11	Down		Switch port	-	1000M	Auto	Disable	Disable
ge12	Down		Switch port	-	1000M	Auto	Disable	Disable
xe1	Down		Switch port	-	10G	Full	Disable	Disable
xe2	Down		Switch port	-	10G	Full	Disable	Disable
xe3	Down		Switch port	-	10G	Full	Disable	Disable
xe4	Down		Switch port	-	10G	Full	Disable	Disable

Figure 27: Port Status

Digital Diagnostics Monitoring (DDM)

Digital Diagnostics Monitoring (DDM) and Digital Optical Monitoring (DOM) allow a user to easily monitor and troubleshoot fiber-optic connectivity issues. The SFP paramters displayed are Connector Type, Bit Rate, Mode, Wave Length, Link Length, Temperature, Vcc, Tx Bias, Tx Power, and Rx Power.

SFP Port

Port	Connector Type	Bit Rate	Mode	Wave Length(nm)	Link Length(m)	Temperature(C)	Vcc(V)	Tx Bias(mA)	Tx Pow(dbm)	Rx Pow(dbm)
ge13	None	None	None	None	None	None	None	None	None	None
Port	Connector Type	Bit Rate	Mode	Wave Length(nm)	Link Length(m)	Temperature(C)	Vcc(V)	Tx Bias(mA)	Tx Pow(dbm)	Rx Pow(dbm)
ge14	None	None	None	None	None	None	None	None	None	None
Port	Connector Type	Bit Rate	Mode	Wave Length(nm)	Link Length(m)	Temperature(C)	Vcc(V)	Tx Bias(mA)	Tx Pow(dbm)	Rx Pow(dbm)
ge15	None	None	None	None	None	None	None	None	None	None
Port	Connector Type	Bit Rate	Mode	Wave Length(nm)	Link Length(m)	Temperature(C)	Vcc(V)	Tx Bias(mA)	Tx Pow(dbm)	Rx Pow(dbm)
ge16	None	None	None	None	None	None	None	None	None	None

Figure 28: SFP Port Status

Rate Control

To navigate to the **Rate Control** page:

1. Click on the **+** next to **Port**.
2. Click on **Rate Control**.

The Rate Control page allows the user to set the maximum throughput on a port or ports on both packets entering the port (from the connected device) or packets leaving the port.

The **Ingress** text box controls the rate of data traveling into the port while the **Egress** text box controls the rate of data leaving the port.

Note: Entries will be rounded down to the nearest acceptable rate value. If the value entered is below the lowest acceptable value, then the lowest acceptable value will be used.

The Rate Control page is shown below (see Figure 29):

To provide either an ingress or egress rate control for a port on the switch:

1. Click in the Ingress or Egress Text Box for the appropriate port.
2. Type in the ingress/egress rate for the port according to the values listed above.
3. Click on the **Update Setting** button.

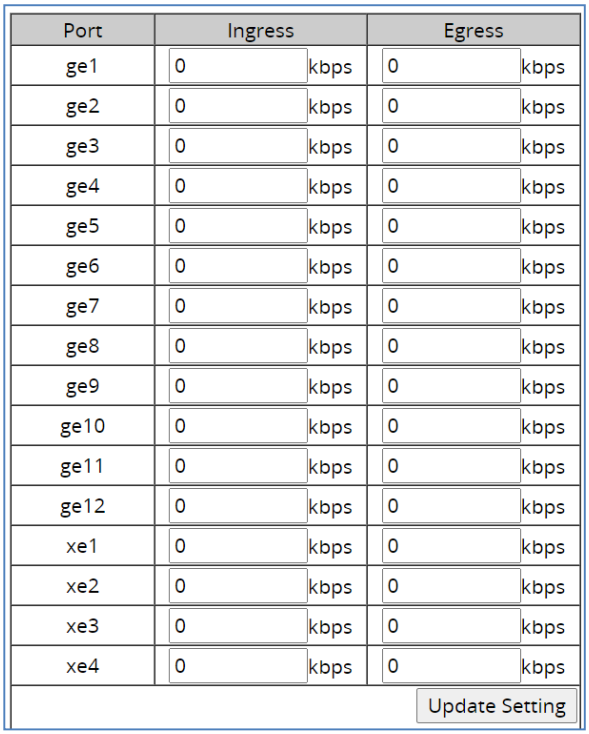


Figure 29: Rate Control

RMON Statistics

To navigate to the **RMON Statistics** page:

1. Click on the **+** next to **Port**.
2. Click on **RMON Statistics**.

RMON Statistics gives a detailed listing of the types and quantity of packets that a particular port has seen since the last reboot of the switch (see Figure 30).

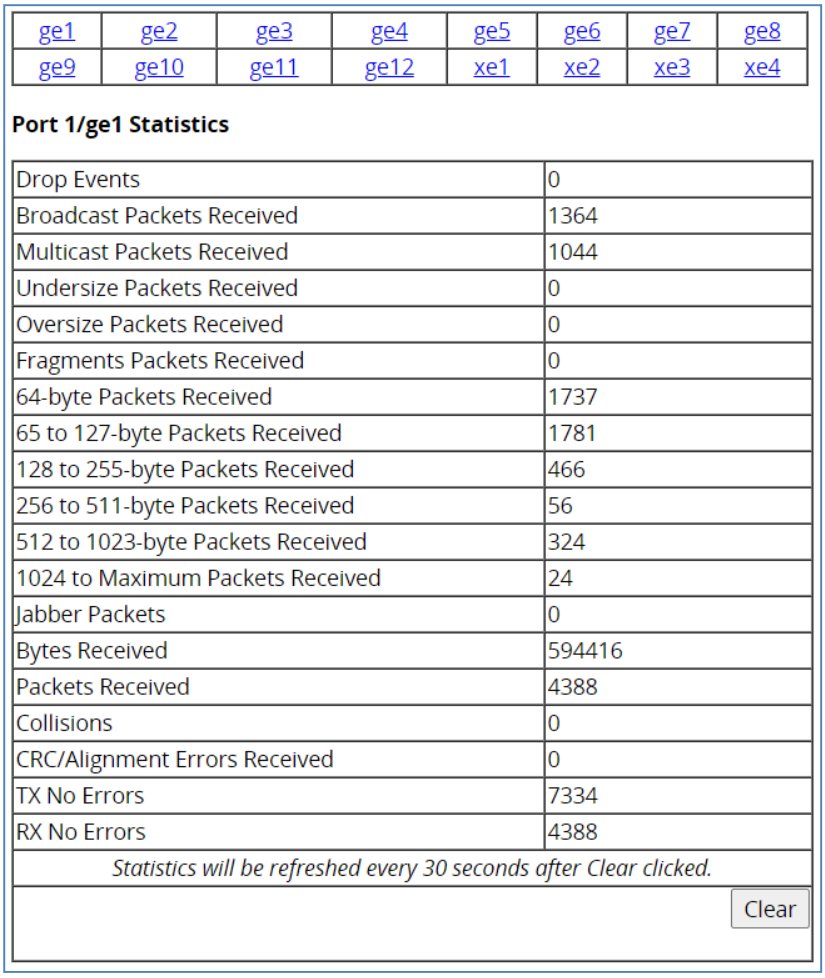
To view the RMON statistics for a specific port on the switch:

1. Click on the link to the port at the top of the RMON Statistics page.

To clear the RMON statistics for a specific port on the switch:

1. Click on the link to the port at the top of the RMON Statistics page.
2. Click on the **Clear** button at the bottom of the page.
3. The statistics for the port will update every ten seconds.

 Pay close attention to the values for CRC/Alignment errors and collisions. Nonzero values for these fields can indicate that a port speed or duplex mismatch exists on the port.



ge1	ge2	ge3	ge4	ge5	ge6	ge7	ge8
ge9	ge10	ge11	ge12	xe1	xe2	xe3	xe4

Port 1/ge1 Statistics

Drop Events	0
Broadcast Packets Received	1364
Multicast Packets Received	1044
Undersize Packets Received	0
Oversize Packets Received	0
Fragments Packets Received	0
64-byte Packets Received	1737
65 to 127-byte Packets Received	1781
128 to 255-byte Packets Received	466
256 to 511-byte Packets Received	56
512 to 1023-byte Packets Received	324
1024 to Maximum Packets Received	24
Jabber Packets	0
Bytes Received	594416
Packets Received	4388
Collisions	0
CRC/Alignment Errors Received	0
TX No Errors	7334
RX No Errors	4388
Statistics will be refreshed every 30 seconds after Clear clicked.	
Clear	

Figure 30: RMON Page

Per Port VLAN Activities

To navigate to the **Per Port VLAN Activities** page:

1. Click on the **+** next to **Port**.
2. Click on **Per Port VLAN Activities**.

This is a read-only page that will allow the user to see what devices are connected to a specific port and the vlan associated with that device and port.

To clear the MAC addresses for a specific port on the switch (see Figure 31):

1. Click on the link to the port at the top of the Per Port VLAN Activities page.
2. Click on the **Clear MAC** button at the bottom of the page.
3. The statistics for the port will update every ten seconds.

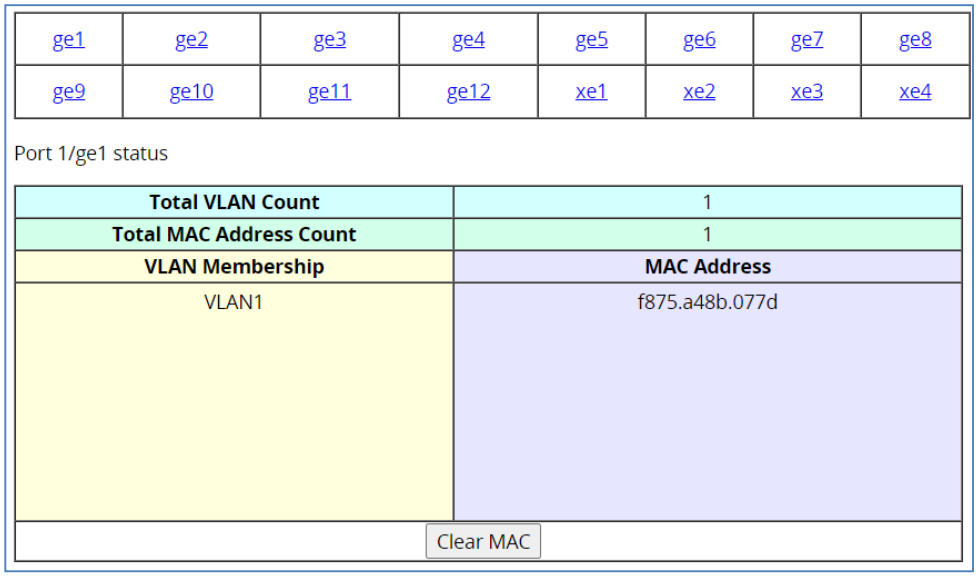


Figure 31: Port VLAN Activities

Port Security

To navigate to the **Port Security** page:

1. Click on the **+** next to **Port**.
2. Click on **Port Security**.(see Figure 36)

One way for an attacker to gain unauthorized access to a network is by connecting to an available port on an unsecured switch. By default, there is no limit to the number of MAC addresses that can be accessed by a port, and no prohibited MAC addresses. The Port Security feature can be used to prevent this kind of unauthorized network access.

Port Security uses dynamically or statically learned MAC addresses to restrict ingress traffic by limiting the MAC address that are allowed to send traffic to the port. Port Security is disabled by default.

There are two options for configuring Port Security:

Enable mode is for manual entry of static MAC addresses for a port. This is the most common method but can often require a lot of effort and time. The maximum number of static MAC addresses that can be set is 10 per port.

Sticky mode allows an interface to dynamically (learn automatically) the MAC address of the connected device, and afterwards will only accept packets from that MAC address. Only one MAC address is set for each port in this mode.

To add a static MAC address to a port (See figure below)

1. Select **Enable** from the **Mode** column for the port you want to configure.

2. **In the Add MAC Address** field, enter the source MAC address of the device to be allowed to connect to the port.

3. Click the **Update Setting** button. Repeat this process for the MAC addresses of all connecting devices.

To set a port to dynamically learn MAC addresses from connected devices:

1. Select **Sticky** from the **Mode** column for the port you want to configure.

2. Click the **Update Setting** button.

The first MAC address learned dynamically from the connected port will be shown in the **Add MAC address** field if the page is reloaded. Existing static MAC addresses (set from enable mode) for the port will not be converted to sticky MAC addresses for the port.

To remove a static MAC address from a port:

1. Select the MAC address from the dropdown list in the **Delete MAC address** column next to the port that you want to configure.

2. Click the **Update Setting** button.

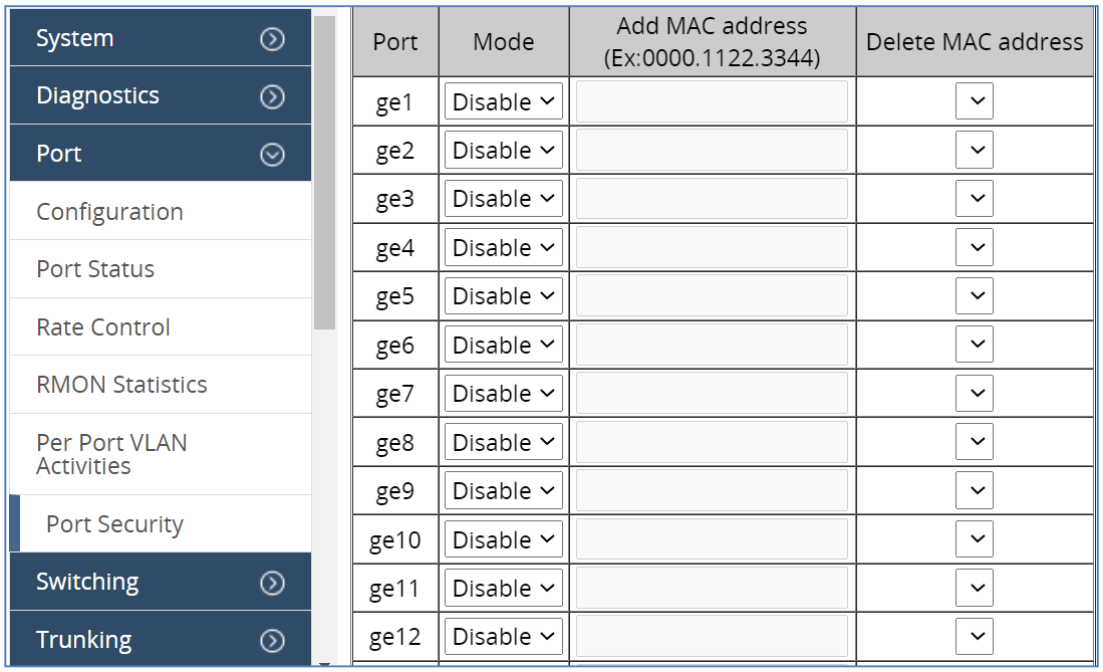


Figure 32: Port Security settings

Port Configuration Examples Using CLI Commands

Setting the Port Description

To provide a description of a port use the CLI commands below:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **description <*description text*>**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#int ge1
switch_a(config-if)#description A_Port_Description
switch_a(config-if)#q
switch_a(config)#
```

Enable or Disable a Port

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:

shutdown
no shutdown

Usage Example 1: Disabling a port:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#int ge1
switch_a(config-if)#shutdown
switch_a(config-if)#q
switch_a(config)#
```

Usage Example 2: Enabling a port:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#int ge1
switch_a(config-if)#no shutdown
switch_a(config-if)#q
switch_a(config)#
```

Setting the Port Speed

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **bandwidth *<1-10000000000 bits>*** (usable units: k, m, g)

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#int ge1
switch_a(config-if)#bandwidth 100m
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Setting Port Duplex

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **duplex *<full* | *half* | *auto>***

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#int ge1
switch_a(config-if)#duplex full
switch_a(config-if)#q
switch_a(config)#
```

Enable or Disable Port Flow Control

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **flowcontrol on**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#int ge1
switch_a(config-if)#flowcontrol on
switch_a(config-if)#q
switch_a(config)#
```

Display Port Status

CLI Command Mode: **Privileged Exec Mode**

CLI Command Syntax: **show interface <*ifname*>**

Usage Example:

```
switch_a>enable
switch_a#show interface ge1
```

Setting a Port's Rate Control

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **rate-control <*ingress* | *egress*> value <*value in kbps*>**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#int ge1
switch_a(config-if)#rate-control ingress value 100000
switch_a(config-if)#q
switch_a(config)#
```

Display a Port's RMON Statistics

CLI Command Mode: **Privileged Exec Mode**

CLI Command Syntax: **show interface statistics <*interface name*>**

Usage Example:

```
switch_a>enable
switch_a#show interface statistics ge1
```

Display a Port's VLAN Activities

To display a port's VLAN activities use the CLI commands below:

CLI Command Mode: **Privileged Exec Mode**

CLI Command Syntax: **show bridge interface <*interface name*>**

Usage Example:

```
switch_a>enable
switch_a#show bridge interface ge1
```

Setting MAC Port Security

To enable MAC port security, use the CLI commands below:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **port-security enable**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#int ge1
switch_a(config-if)#port-security enable
switch_a(config-if)#q
switch_a(config)#
```

To disable MAC port security, use the CLI command below. Note that this command will clear all MAC address that have been created, both statically and dynamically.

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **no port-security enable**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#int ge1
switch_a(config-if)#no port-security enable
switch_a(config-if)#q
switch_a(config)#
```

To set allowed MAC addresses (maximum 10 per port), use the CLI commands below:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **port-security allowed-address <value>** (hex format, e.g. 00aa.0062.c609)

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#int ge1
switch_a(config-if)#port-security allowed-address 00aa.0062.c609
switch_a(config-if)#q
switch_a(config)#
```

To delete an allowed MAC address use the CLI commands below:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **no port-security allowed-address <value>** (hex format, e.g. 00aa.0062.c609)

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#int ge1
switch_a(config-if)#no port-security allowed-address
00aa.0062.c609
switch_a(config-if)#q
switch_a(config)#
```

To set sticky mode, use the CLI command below:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **port-security mac-address sticky**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#int ge1
switch_a(config-if)#port-security mac-address sticky
switch_a(config-if)#q
switch_a(config)#
```

To disable sticky mode, use the CLI commands below:

This command will clear MAC addresses previously acquired via sticky mode.

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **no port-security mac-address sticky**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#int ge1
switch_a(config-if)#no port-security mac-address sticky
switch_a(config-if)#q
```

To display the Port Security MAC addresses from all ports, use this CLI command:

CLI Command Mode: **Privileged Exec Mode**

CLI Command Syntax: **show port-security address**

Usage Example:

```
switch_a>enable
switch_a# show port-security address
```

SWITCHING

Bridging

To learn MAC addresses, a switch reads all packets that it detects on the LAN or on the local VLAN, looking for MAC addresses of sending nodes. It places these addresses into its Ethernet Switching table, along with the interface on which the traffic was received and the time when the address was learned. When the switch receives traffic on an interface, it searches the Ethernet switching table for the MAC address of the destination. If the MAC address is not found, the traffic is flooded out all of the other interfaces associated with the VLAN. If traffic is received on an interface that is associated with VLAN 1 and there is no entry in the Ethernet switching table for VLAN 1, then the traffic is flooded to all access and trunk interfaces that are members of VLAN 1.

Flooding allows the switch to learn about destinations that are not yet in its Ethernet switching table. If a certain destination MAC address is not in the Ethernet switching table, the switch floods the traffic to all interfaces except the interface on which it was received. When the destination node receives the flooded traffic, it sends an acknowledgment packet back to the switch, allowing the switch to learn the MAC address of the node and to add the address to its Ethernet switching table.

The switch uses a process called aging to keep the Ethernet switching table current. For each MAC address in the Ethernet switching table, the switch records a timestamp of when the information about the network node was learned. Each time the switch detects traffic from a MAC address that is in its Ethernet switching table, it updates the timestamp of that MAC address. A timer on the switch periodically checks the timestamp, and if it is older than the value set for **mac-table-aging-time**, the switch removes the node's MAC address from the Ethernet switching table. This aging process ensures that the switch tracks only active MAC addresses on the network and that it is able to flush out from the Ethernet switching table MAC addresses that are no longer available.

The user can configure:

- How long MAC addresses remain in the Ethernet switching table
- Add a MAC address permanently to the switching table
- Prevent a MAC address from ever being registered in the switching table.

To navigate to the **Bridging** page:

1. Click on the **+** next to **Switching**.
2. Click on **Bridging.**

Aging Time

The Aging Time value is a global value and represents the time that a networked device's MAC address will live in the switch's memory before being removed. The default value is 300s (5 minutes) (see Figure 33).

To update the Aging Time value on the switch:

1. Click in the Error Disable Recovery text box at the top of the Port Security Dynamic-MAC page.
2. Type in the desired value. Values can be from **0 to 65535 seconds**. A value of **0** indicates that the port is not to return to normal operating condition until an administrator resets the port or the switch is restarted.
3. Click on the **Update Setting** button.

Threshold Level

The **Threshold Level** setting is a **per port value**. A traffic *storm* occurs when packets flood the LAN, creating excessive traffic and degrading network performance. The traffic *storm control* feature prevents LAN ports from being disrupted by a broadcast or multicast traffic *storm* on physical interfaces. A Threshold is set to determine when the switch will react to Broadcasts and/or Multicasts.

To set the Threshold level per port:

1. Type in the desired value. Values can be from **0.1 to 100**. This value is a percentage of allowable broadcast traffic for this port. Once this percentage of traffic is exceeded, all broadcast traffic beyond this percentage is dropped.
2. Click on the **Update Setting** button.

Storm Control Type

The **Storm Control Enabled Type** setting is a per port value. The Storm Control Enabled Type allows users to determine the type of storm control to be used by the switch.

To set the Storm Control Enabled Type:

1. Select the check box next to **Broadcast** and/or **DLF-Multicast** for the port that needs to be changed
2. Click on the **Update Setting** button.

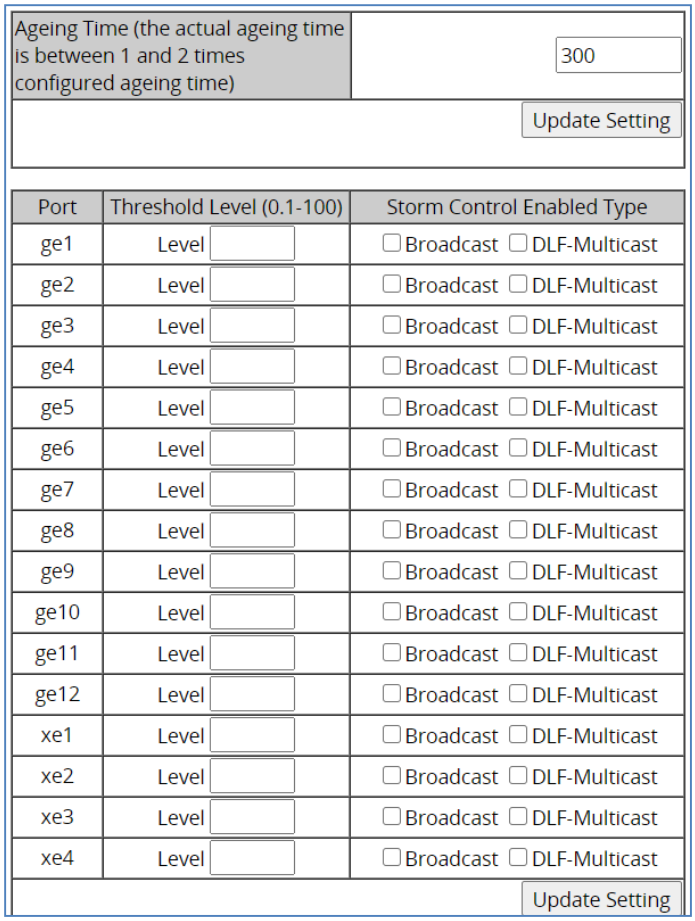


Figure 33: Bridging

Existing Storm Control types and Threshhold levels for each port can be verified later by returning to this screen.

Loopback Detect

Loopback detection is quite simply the ability of the switch to detect when a port on the switch has been connected directly (or “looped back”) to another port on the switch. This configuration would likely lead to a broadcast storm on the switch which would cause network performance to suffer. Loopback detection offers the ability of the switch to detect this condition and shutdown the loop-backed port before any disruption of network traffic occurs.

To navigate to the **Loopback Detect** page:

1. Click on the **+** next to **Switching**.
2. Click on **Loopback Detect.**

Loopback Detection (Global)

To globally enable the **Loopback Detect** feature of the switch (see Figure 34):

1. Click on the **Loopback Detect** drop-down box.
2. Select **Enable** from the drop down list.
3. Click on the **Update Setting** button.

Loopback Detect Action

To change the action that the switch takes when a loopback condition is detected (see Figure 34):

1. Choose an action from the **Loopback Detect Action** dropdown list. The available options are **None** and **Error Disable**.
2. Click on the **Update Setting** button.

Loopback Detect Recovery Time

To change the length of time that the **Loopback Detect Action** will stay in effect (see Figure 34):

1. Enter a value in the text box next to **Error Disable Recovery**. Valid values range from **0 to 65535 seconds**.
2. Click on the **Update Setting** button.

Polling Interval

To change the polling interval of the Loopback Detect function (see Figure 34):

1. Enter a value in the text box next to **Interval**. Valid values range from **1 to 65535** seconds.
2. Click on the **Update Setting** button.

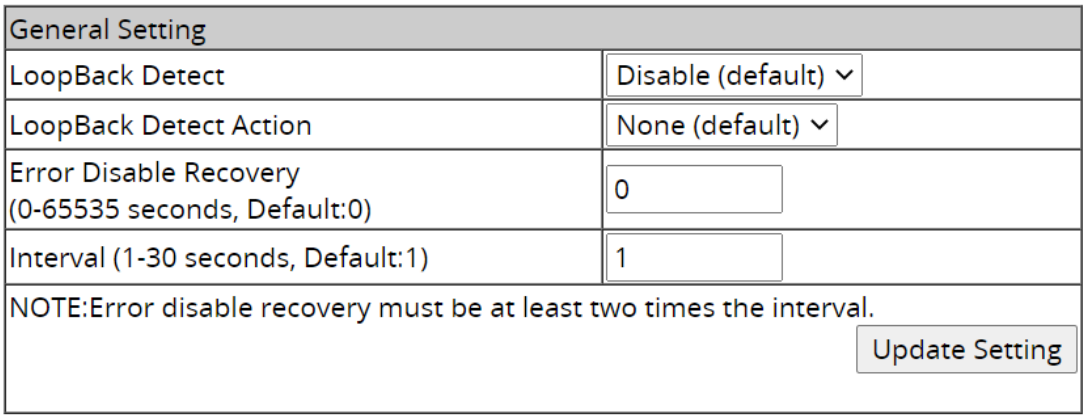


Figure 34: Loopback Detection

Loopback Detection (Per Port)

To enable **Loopback Detection** for a particular port or ports on the switch (see Figure 35):

1. Select the value **Enable** from the **Mode** drop down list for a port on the Loopback Detect page.
2. Click on the **Update Setting** button.

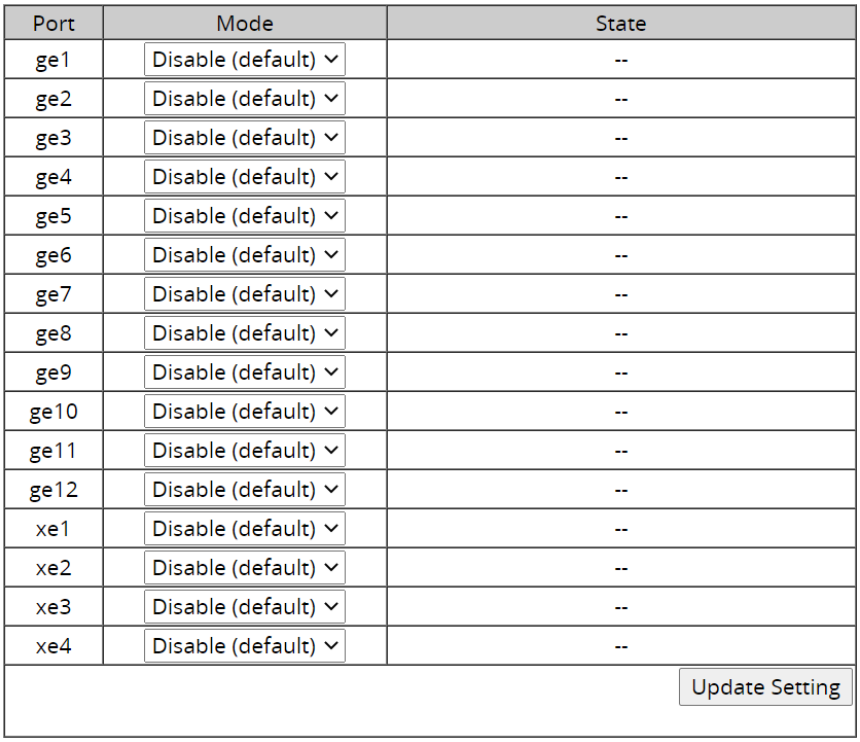


Figure 35: Loopback Detection (port)

Storm Detect

The **Storm Detect** feature allows the switch to be configured to disable a port that is receiving a large number of Broadcast and/or Multicast packets. The switch can monitor for packets and take action based on percentage of bandwidth utilization or number of packets per second.

To navigate to the **Storm Detect** page:

1. Click on the **+** next to **Switching**.
2. Click on **Storm Detect.**

Enable/Disable Storm Detection

1. **Enable** or **Disable** Storm Detection by Clicking on the drop down box in the **Storm-Detect Configuration** box (see Figure 36).
2. Set the **Storm Detect interval** to a number between **2 and 65535** seconds. The Default value is 10 seconds.
3. Set the **Storm-Detect errdisable-recovery time** to value between **0 and 65535 seconds**. The Default is 0 (disabled). This value determines if the switch should re-enable the port after the specified value or leave the port disabled.

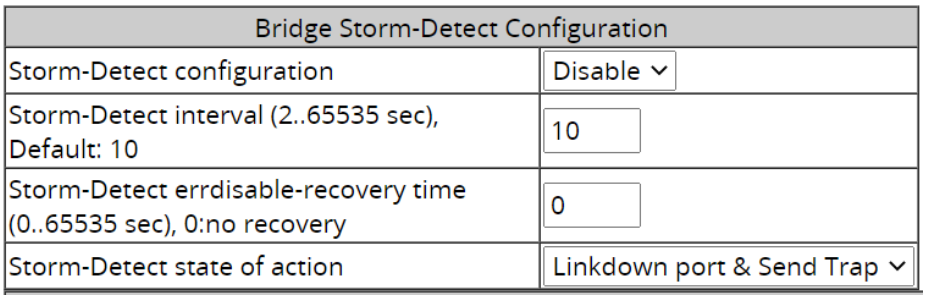


Figure 36: Storm Detect – Global

4. Set the **By Utilization(%)** for each port in the **Storm-Detect Per Port Configuration** box (see Figure 37). The default is 0 (not limited). Setting this to a value between 1 and 100 will cause the port to be disabled when the defined percentage of bandwidth is reached.
5. Set the type of packet to be monitored in the Dropdown box under **By Broadcast / Multicast+Broadcast Packets Per Second**. Set the value to **BC** to monitor Broadcast packets and **BC-MC** to monitor both Broadcast and Multicast packets.
6. Set the number of **packets per second** to a value between 0 and 1000000 packets. The default is 0 (not limited).

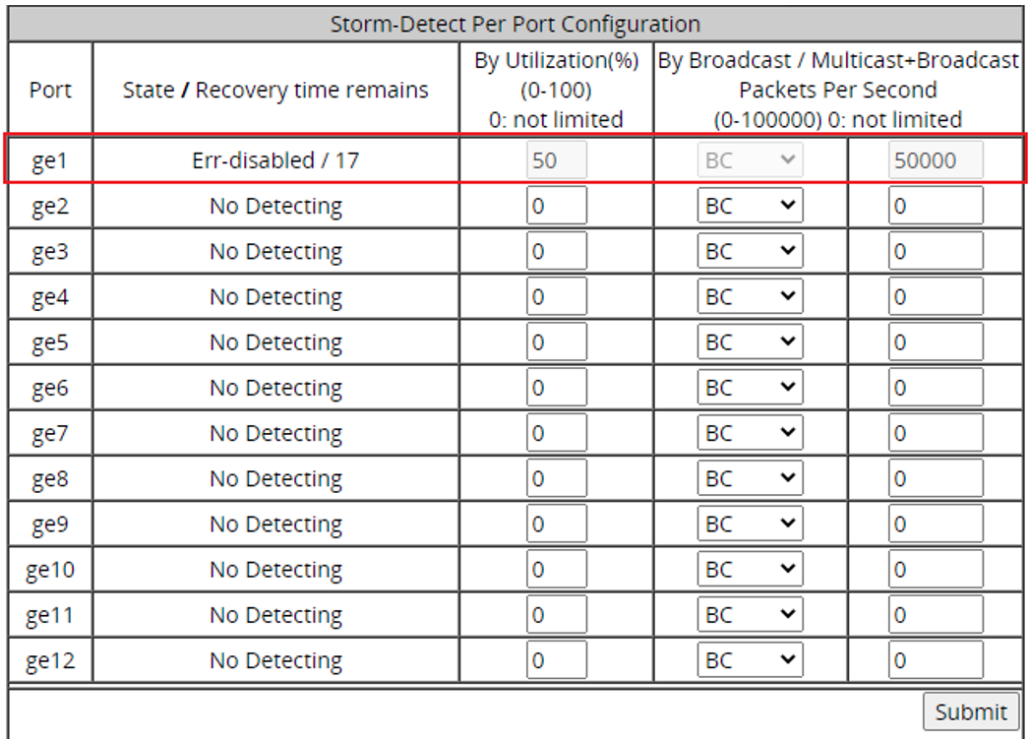


Figure 37: Storm Detect – Per Port

Static MAC Entry

Occasionally, it may be useful to specify a MAC address on a specific port and VLAN rather than adjusting the ageing time for the entire switch. Alternatively, it is also possible and even desirable to prevent a MAC address from ever being registered with a switch. These features are offered under the **Static MAC Entry** menu.

To navigate to the **Static MAC Entry** menu:

1. Click on the **+** next to **Switching**.
2. Click on **Static MAC Entry.**

Adding a Static MAC Address to a Port

To add a static MAC entry for a specific port (see Figure 38):

1. Enter the MAC address for end the corresponding port's text box. The format of the MAC address should be in the form **aaaa:bbbb:cccc**).
2. Select the VLAN that this MAC address is associated with from the **VLAN ID** drop down list for the port.
3. Click on the **Submit** button.

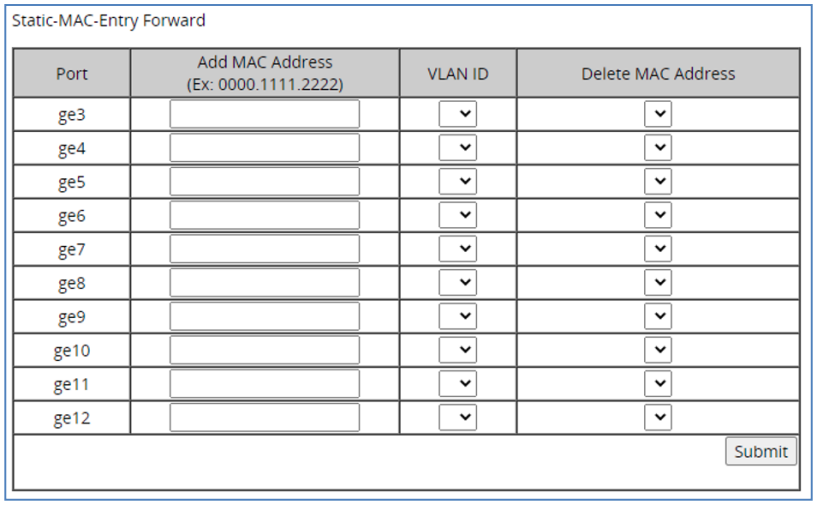


Figure 38: MAC Static Entry

To confirm existing static MAC addresses for a port, navigate to **Port → Per Port VLAN Activities**, and click on the corresponding port number link at the top of the screen. In the example below, ge1 is set to only forward these five MAC addresses:

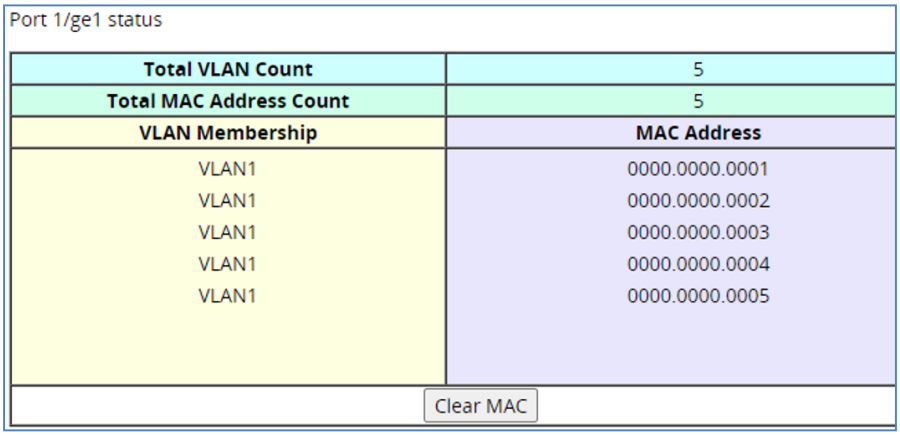


Figure 39: Example of Port forwarding MAC List

Removing a Static MAC Address from a Port

To remove a static MAC entry for a specific port (see Figure 40):

1. For a specific port, select the MAC address to be deleted from the **Delete MAC Address** drop down box.
2. Click on the **Submit** button.

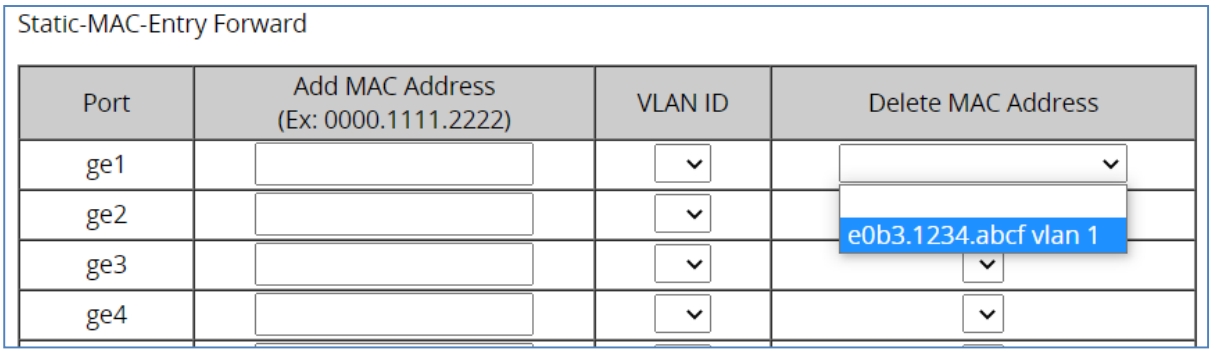


Figure 40: Removing a Static MAC Address

Adding a MAC to the Static-MAC-Entry Discard Table

To add a MAC address to the **Static-MAC-Entry Discard** table (see Figure 41):

1. Enter a MAC address in the form “0000.1234.abdc” in the **Add MAC Address** text box of the **Static-MAC-Entry-Discard** section.
2. Select the VLAN associated with the MAC address.
3. It should be noted that while static MAC address for forwarding are associated with the switch on a per-port basis. Static MAC discards are associated with the switch for all ports.
4. Click on the **Submit** button.

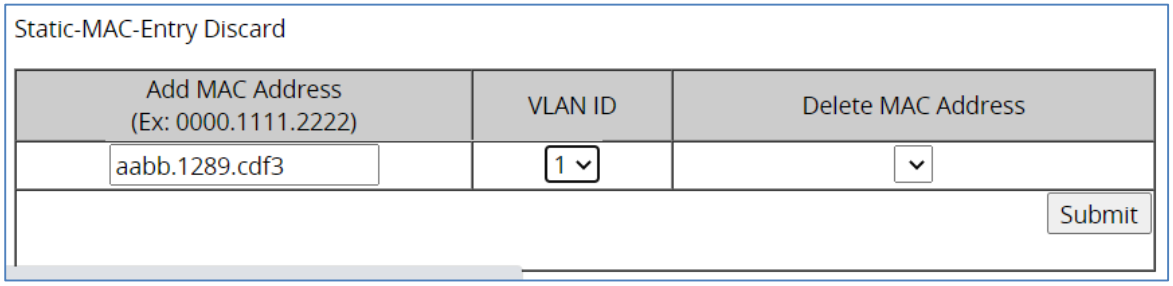


Figure 41: Adding a MAC – Static-MAC-Entry Table

Removing a MAC address from the Static-MAC-Entry Discard Table

To remove a MAC address from the **Static-MAC-Entry Discard** table (see Figure 42):

1. From the drop-down box underneath **Delete MAC Address**, select the MAC address to be deleted.
2. Click on the **Submit** button.

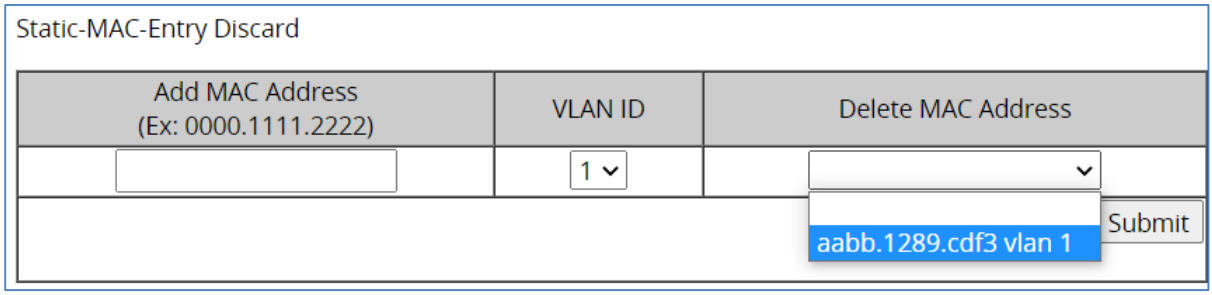


Figure 42: Deleting a MAC – Static-MAC-Entry Table

Port Mirroring

Port mirroring allows network traffic from one port to be copied or mirrored to another port. This is a very useful troubleshooting feature in that all data from one port is sent to another port which is attached to a computer or other network device that is configured to capture packets. This enables a network administrator or technician to see the traffic that is entering or leaving a specific port without disrupting normal network operations on the port that is being mirrored.

To navigate to the **Port Mirroring** menu:

1. Click on the **+** next to **Switching**.
2. Click on **Port Mirroring.**

To configure port mirroring for a port or ports on the switch (see Figure 43):

1. Select the port or ports that traffic is to be mirrored from under the **Mirror From** column.
2. Select the destination port under the **Mirror To** drop down box.
3. Select the type of traffic that should be mirrored from the **Mirror Mode** drop down box. The available options are:
    a. TX – transmit only
    b. RX – Receive Only

c. TX/RX – Transmit and Receive.

4. Click on the **Submit** button.

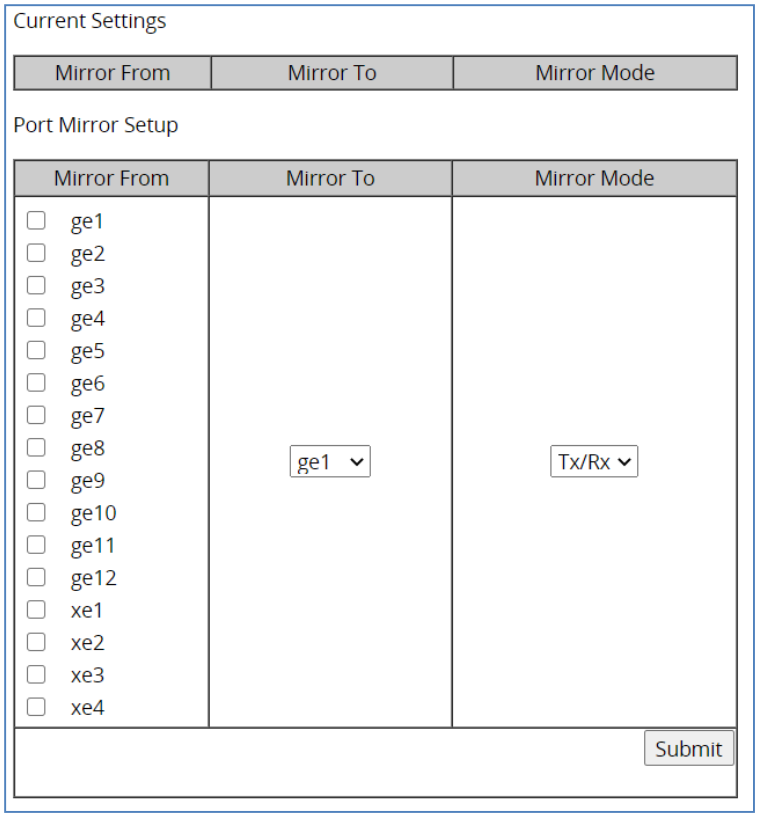
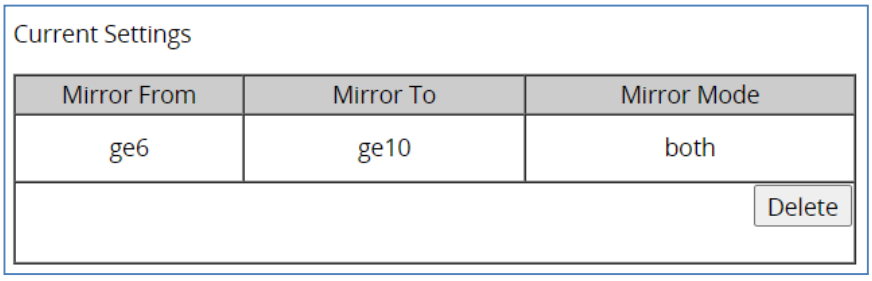


Figure 43: Port Mirroring

To disable port mirroring for a port or ports on the switch (see Figure 44):

1. Under the **Current Settings** section, the current port mirroring configuration should be displayed.
2. Click on the **Delete** button.



.

Figure 44: Disabling Port Mirroring

Link State Tracking

Link-state tracking binds the link state of multiple interfaces. Link-state tracking provides redundancy in the network when used with server network interface card (NIC) adapter teaming or bonding. When the server network adapters are configured in a primary or secondary relationship known as teaming and the link is lost on the primary interface, connectivity transparently changes to the secondary interface.

To navigate to the **Link State Tracking** menu:

1. Click on the **+** next to **Switching**.
2. Click on **Link State Tracking.**

Enable/Disable Link State Tracking

To enable Link State Tracking for a specific group on the switch (see Figure 45):

1. Under **Group Setting**, click the check box of the Link State groups that are to be enabled (or disabled).
2. Click on **Update Setting.**

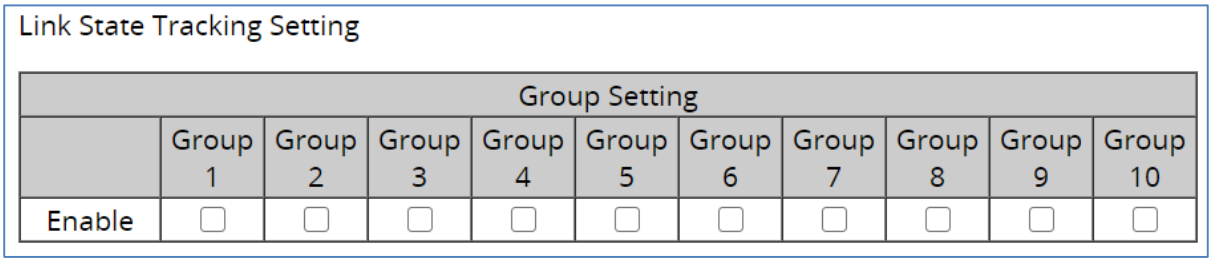


Figure 45: Link State Tracking

Port Settings

To configure individual ports for a Link State group on the switch (see Figure 46):

1. Under **Port Setting**, select the Link State Group that the port will belong to from the Group drop down box
2. Select if the port is upstream or downstream from the Up/Down Stream) drop down box.
3. Click on **Update Setting.**

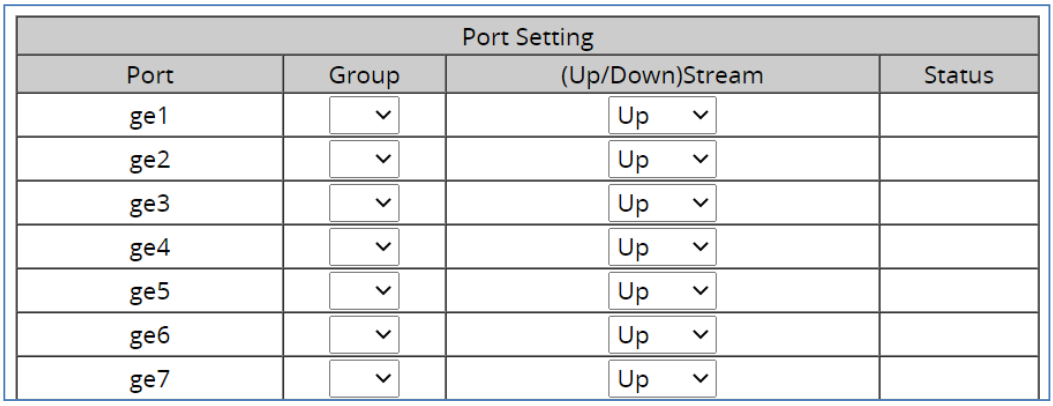


Figure 46: Link State Tracking – Port Settings

PoE (Power over Ethernet) - System and Port Settings

This section only applies to Managed EtherWAN Switches with support for PoE.

To navigate to the **PoE page**:

1. Click on the **+** next to **Switching**.
2. Click on **PoE.**

PoE System Setting

The PoE Page provides access to **PoE System Setting** information and configuration. The information provided is (See Figure 47):

1. **Main Supply Voltage**
2. **System Temperature**
3. **Power Allocation** – Actual wattage supplied to attached PoE device(s)
4. **System Power Budget** – The maximum and default values are 240W for the EX78900E series, 360W for EX78934X, and 720W for the EX75900 series.

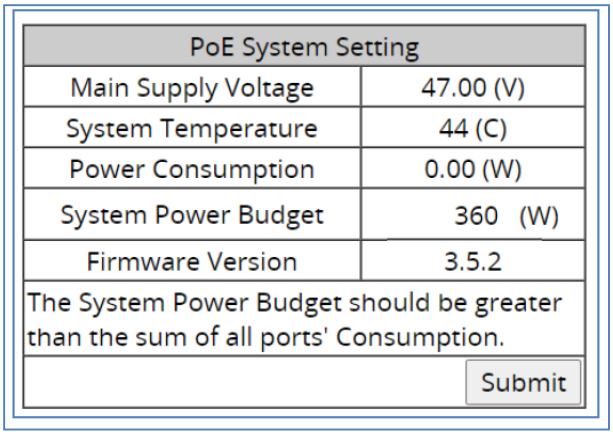


Figure 47: PoE System Setting

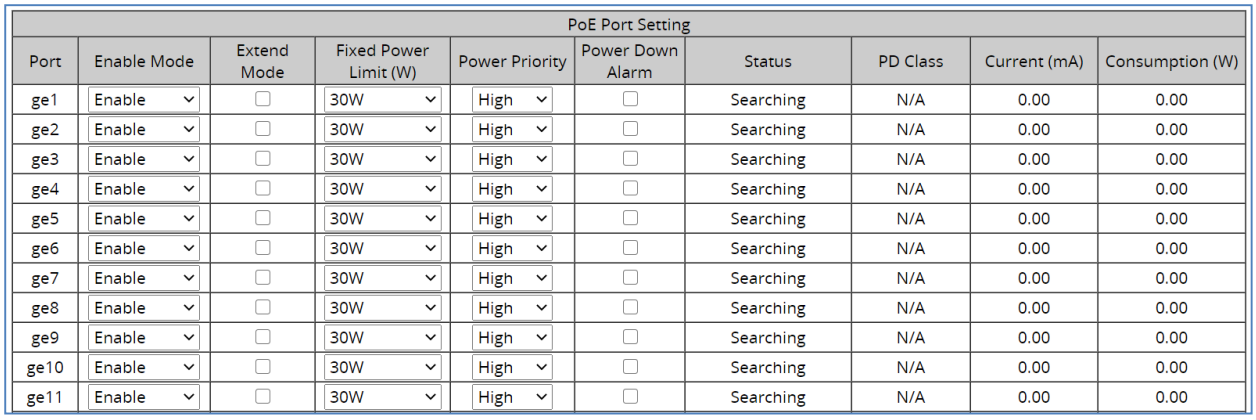
PoE Port Setting

The PoE Port Setting section provides the following configurable settings and information:

1. **Enable Mode**– Set the PoE Enable Mode by selecting one of the following settings in the drop-down box under PoE Mode (see Figure 48)
    - **Enable** – Enable PoE on a specific port
    - **Disable** – Disable PoE on a specific port
    - **Scheduling** – Schedule time of day that PoE will be enabled per port
2. **Extend Mode** – This allows the port to deliver PoE power up to 250 meters at a speed of 10Mbps.

    Note: It is suggested to pre-test the function before deployment. The maximum available transmission distance of PoE depends on the negotiation result of PD and PSE. Some PDs using EtherWAN PoE/PSE switches may only support a standard distance of 100 meters. Contact EtherWAN if assistance is needed. When the PoE IEEE 802.3 BT firmware ver. 3.5.2 has been installed, the input power voltage from the switch must be at least 57 volts in order to make PoE Extend Mode work.
3. **Fixed Power Limit** – Provides a fixed maximum Wattage to the attached PoE (PD) device.
4. **Power Priority** – Use the Drop-Down box in the *Power Priority* column to set the priority to High, Medium or Low.
5. **Power Down Alarm** – This setting only applies to EtherWAN Switches that have a relay. If this box is checked, losing PoE power on a port triggers the relay on the switch.
6. **Status** – Informational only. Provides the status of the PoE port

7. **PD Class** - Informational only. Provides the PoE Classification of the PoE (PD) device attached to the PoE port
8. **Current (mA)** – Informational only. Shows the current draw from the attached PoE (PD) device.
9. **Consumption (W)** - Informational only. Shows the power consumption of the attached PoE (PD) device.



PoE Port Setting

Port	Enable Mode	Extend Mode	Fixed Power Limit (W)	Power Priority	Power Down Alarm	Status	PD Class	Current (mA)	Consumption (W)
ge1	Enable		30W	High		Searching	N/A	0.00	0.00
ge2	Enable		30W	High		Searching	N/A	0.00	0.00
ge3	Enable		30W	High		Searching	N/A	0.00	0.00
ge4	Enable		30W	High		Searching	N/A	0.00	0.00
ge5	Enable		30W	High		Searching	N/A	0.00	0.00
ge6	Enable		30W	High		Searching	N/A	0.00	0.00
ge7	Enable		30W	High		Searching	N/A	0.00	0.00
ge8	Enable		30W	High		Searching	N/A	0.00	0.00
ge9	Enable		30W	High		Searching	N/A	0.00	0.00
ge10	Enable		30W	High		Searching	N/A	0.00	0.00
ge11	Enable		30W	High		Searching	N/A	0.00	0.00

Figure 48: PoE Port Settings for PoE Models

Note: The sum of all **Fixed Power Limit** values must be equal to or less than the power budget for the device.

Before setting a port power limit to 60 Watts, the sum of the other ports must be at least 60 Watts less than the maximum.

All entries for **Fixed Power Limit** must be whole numbers.

Fixed power limit settings:

- For PD compliance with IEEE 802.3bt, select “15W / 30W / 60W” on Fixed Power Limit
- For PD compliance with IEEE 802.3af / IEEE 802.3at, select “15W (2 pair) / 30W (2 pair)” on Fixed Power Limit
- For non-standard 60W PoE PD, select “60W Pre-BT” on Fixed Power Limit

PoE Scheduling

PoE Scheduling allows PoE ports to have their power up time scheduled by hour of the day and day of the week. In order for a port to follow a schedule defined here, the port must be set to **Scheduling** on the **PoE settings** page (see PoE Port Setting)

To navigate to the **PoE Scheduling** page:

1. Click on the **+** next to **Switching**.
2. Click on **PoE Scheduling.**

Each PoE port on the switch can be schedule to power up and down automatically. To configure a port:

1. Select the port from the drop-down list (See Figure 49)

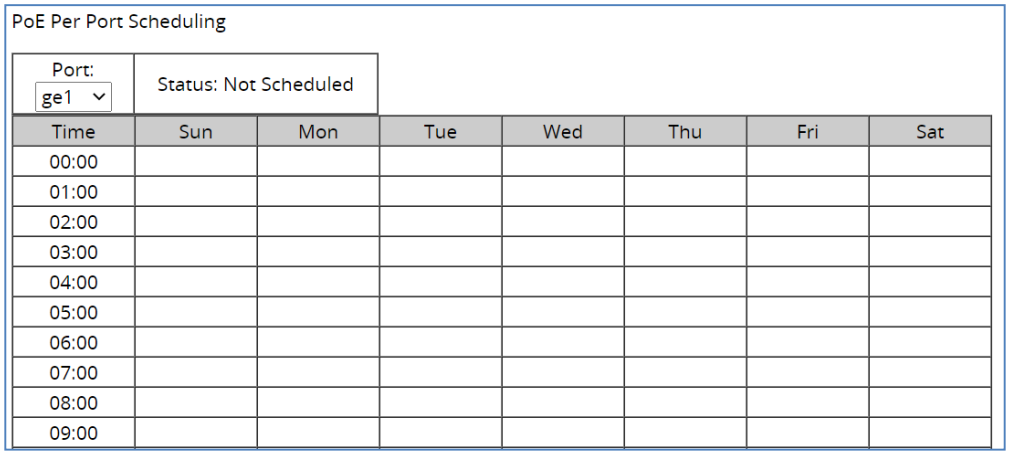


Figure 49: Selecting a Port

2. Select the hour(s) of day for each day of the week (see Figure 50).
3. Click on the **Submit** button.

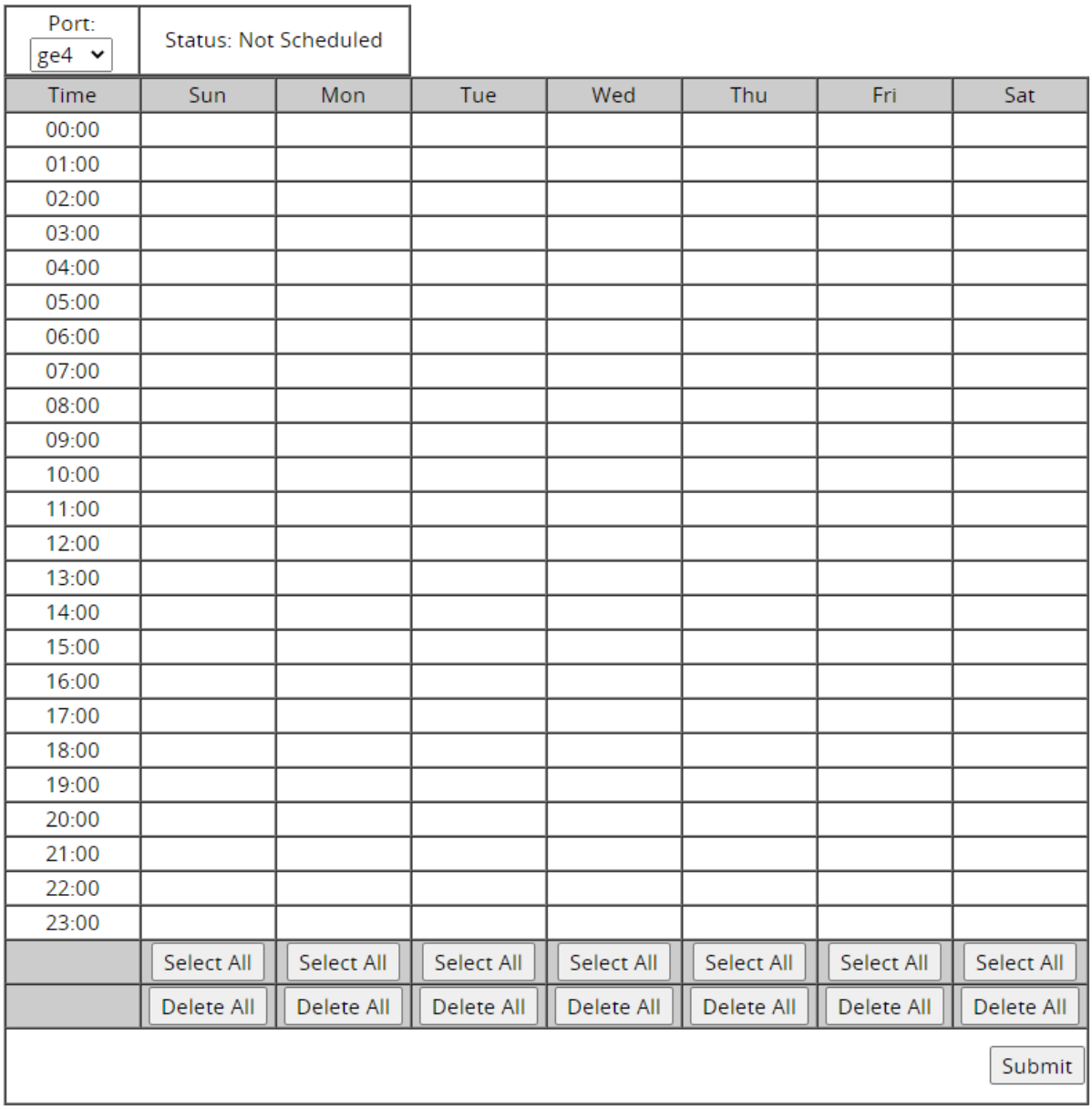


Figure 50: PoE Power Scheduling

PoE Watchdog

PoE Watchdog is a management feature to help system administrators monitor and manage critical PoE powered devices. PD Watchdog is only supported on PoE enabled ports. Once enabled, the system will continuously ping a user specified IP address across the port. If the system does not receive a reply within a specified interval, it can automatically power down or power cycle the powered device.

To navigate to the **PoE Watchdog** page:

1. Click on the **+** next to **Switching**.
2. Click on **PoE Watchdog.**

To enable PoE Watchdog on a port, select **enable** from the drop-down menu, and then enter the IP address to which the device is connected. Set the ping interval and failure count, and choose the response action (**No action**, **Power off PD**, or **Reboot PD**). The **StartUp Delay** is the initial time delay before the system sends out the first ICMP echo request on the port Range: 30 - 600 sec). Click **Submit** when finished.

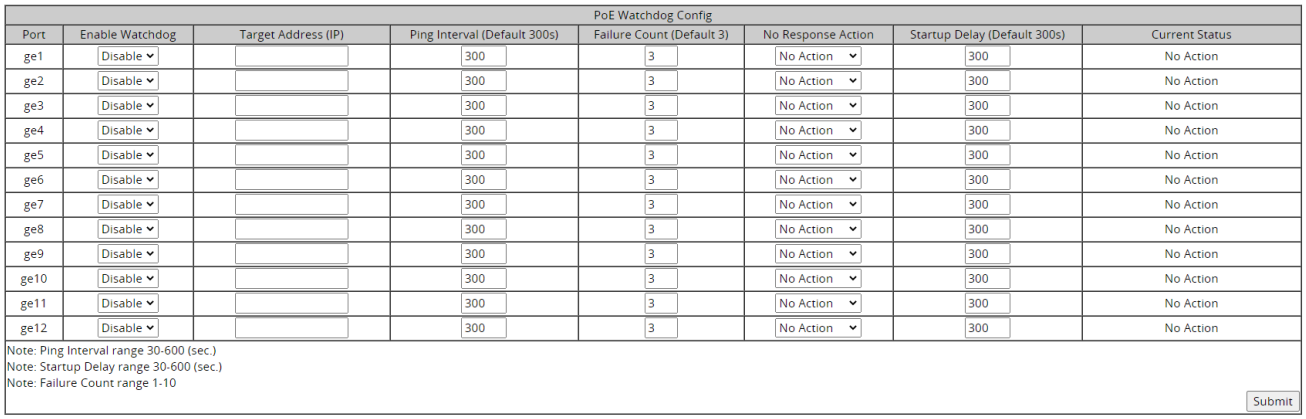


Figure 51: PoE Watchdog

PoE Action

PoE Action allows a PoE port to be activated in response to a digital input.

To navigate to the **PoE Action** page:

1. Click on the **+** next to **Switching**.
2. Click on **PoE Action.**

To enable the PoE Action feature, select **enable** from the drop-down menu at the top of the screen, and then click **Update Setting**. Once PoE Action has been enabled, set it up for the desired ports by selecting a trigger (either DI1 or DI2), the number of ON and off seconds for the action, and the number of times it is to repeat. Then click the Submit button.

Note: The DI global setting should be enabled before selecting DI1 or DI2 trigger. Refer to Digital I/O setting.

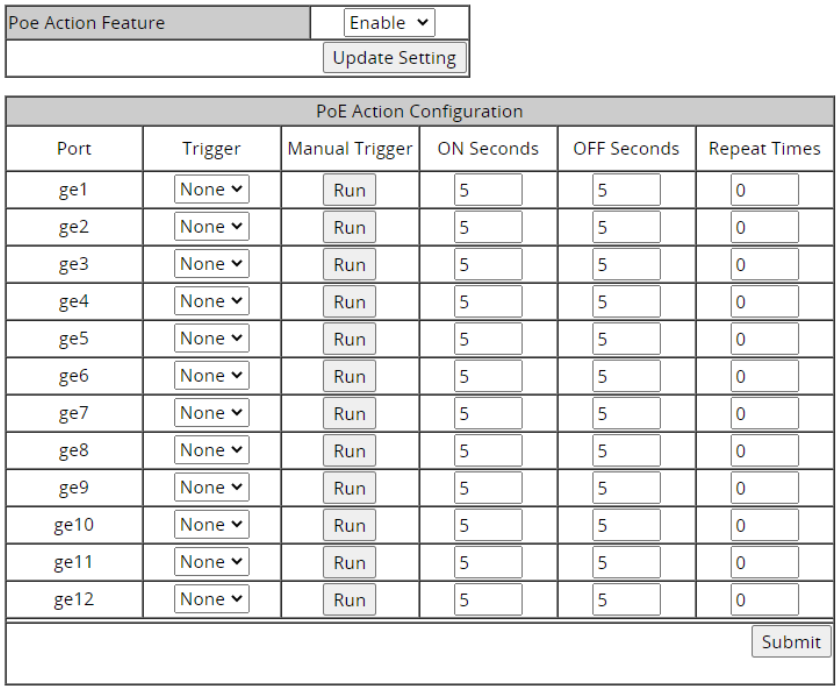


Figure 52: PoE Action

Update PoE Firmware

In order to cope with the compatibility expansion of some non-standard PD devices and provide power budget limited operation, the system firmware after V5.02.1.0 provides the function of adjusting PoE firmware to support corresponding PSE settings between IEEE 802.3at or bt modes.

If the device PoE firmware is version 2.1.1 or 2.2.4 (IEEE 802.3af/at supported), it can be updated to PoE firmware version 3.5.2 or 3.5.5 (IEEE 802.3bt supported).

PoE FW Ver. 2.11(at) ↔ 3.52(bt)

Ver. 2.24(at) ↔ 3.55(bt)

Click the **Upgrade to ver 3.5.2 (or 3.5.5) (BT supported)** button to upgrade the PoE firmware.

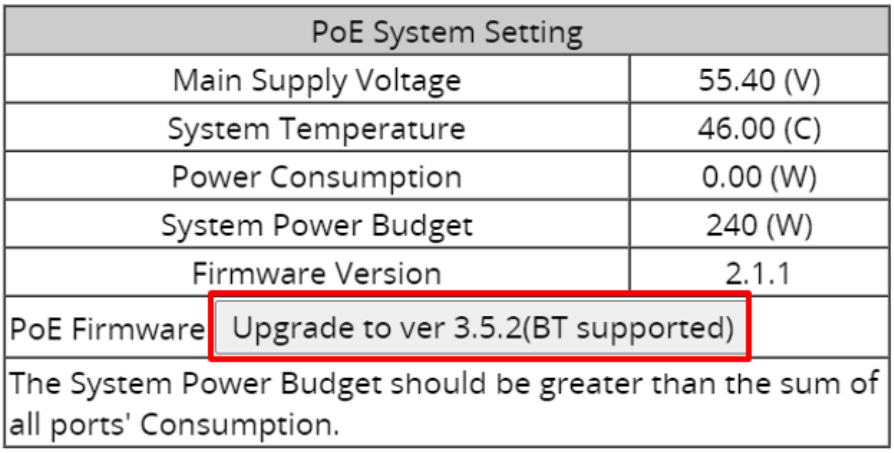


Figure 53: Upgrade of PoE firmware

And the following dialogue window will pop up,

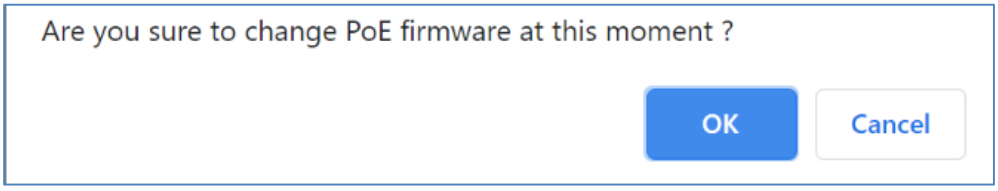


Figure 54: PoE upgrade action dialogue message

Once you click "**OK**", the PoE firmware will update. It will take approximately **8** minutes for the update and reboot of the device. When the processing completed, the PoE Firmware will become version 3.5.2

While the PoE BT firmware ver.3.5.2 was installed, the Fixed Power Limit for specific devices will be changed as table below:

Models	Port	15W	30W	60W	90W	15W (2 Pairs)	30W (2 Pairs)	60W Pre-bt
EX78934E	1~4 Port	N	N	N	N	Y	Y	N
	5~8 Port	Y	Y	Y	N	Y	Y	Y
	9~12 Port	N	N	N	N	Y	Y	N
EX78924E	1~4 Port	N	N	N	N	Y	Y	N
	5~8 Port	Y	Y	Y	N	Y	Y	Y
EX78922E	1~4 Port	N	N	N	N	Y	Y	N
	5~8 Port	Y	Y	Y	N	Y	Y	Y
EX75960	All Ports	Y	Y	Y	N	Y	Y	Y
EX75964	All Ports	Y	Y	Y	N	Y	Y	Y
EX78900X	All Ports	Y	Y	Y	Y	N	N	N
EX78934H	All Ports	Y	Y	Y	Y	N	N	N
EX78924H	All Ports	Y	Y	Y	Y	N	N	N
EX78922H	All Ports	Y	Y	Y	Y	N	N	N

Figure 55: Fixed Power Limit of bt mode

Additionally, PoE Extend mode 10M will be available to support more camera brands (i.e. Axis camera… etc). from auto-negotiation mode. Use the following CLI commands to enable 10M auto-negotiation mode or full-duplex mode:

#poe extend-mode auto-10m

10M auto-negotiation mode

#no poe extend-mode auto-10m

full-duplex mode

Using the GUI, when PoE extend mode is enabled from the CLI, the GUI will display the speed and EEE as “disabled” status (i.e. ge2 and ge3 as shown below), until PoE extend mode setting is removed through either GUI or CLI command.

Port	Link Status	Port Description	Port type	IP address (A.B.C.D/M)	Admin Setting	Speed	EEE	Flow Control
ge1	Running		Switch port		Link Up	Auto	Disable	Disable
ge2	Down		Switch port		Link Up	PoE Extend	Disable	Disable
ge3	Down		Switch port		Link Up	PoE Extend	Disable	Disable
ge4	Down		Switch port		Link Up	Auto	Disable	Disable
ge5	Down		Switch port		Link Up	Auto	Disable	Disable

Figure 60: Display of PoE port status

Switch Configuration Examples Using CLI Commands

Setting the Aging Time Value

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **bridge 1 ageing-time** (time in ms)

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#bridge 1 ageing time 300
switch_a(config)#q
switch_a#
```

Enabling Port Isolation

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **port-isolation enable**
port-isolation disable

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface ge1
switch_a(config-if)#port-isolation enable
switch_a(config-if)#q
switch_a(config)#
```

Setting Storm Control

To set the value for the **Broadcast and or DLF-Multicast Storm Control** value of a port on the switch, use the CLI commands below:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **stormcontrol <*broadcast* | *dlf-multicast*> <*level*>**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a#configure interface ge1
switch_a(config-if)#storm-control broadcast 20
```

```
switch_a(config-if)#q
switch_a(config)#
```

Enabling Loopback Detect (Global)

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: bridge 1 loopback-detect <enable | disable>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#bridge 1 loopback-detect enable
switch_a(config)#q
switch_a#
```

Setting the Loopback Detect Action

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: bridge 1 loopback-detect action <err-disable | none>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#bridge 1 loopback-detect action err-disable
switch_a(config)#q
switch_a#
```

Setting the Loopback Detect Recovery Time

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **bridge 1 loopback-detect errdisable-recovery <*0-65535*>**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#bridge 1 loopback-detect errdisable-recovery 30
switch_a(config)#q
switch_a#
```

Setting the Loopback Detect Polling Interval

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **bridge 1 loopback-detect interval <*1-65535*>**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#bridge 1 loopback-detect interval 5
switch_a(config)#q
switch_a#
```

Enabling Loopback Detect (Port)

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **loopback-detect enable**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a#interface ge1
switch_a(config)# loopback-detect enable
switch_a(config)#q
switch_a#
```

Configuring Storm-Detect

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
bridge 1 storm-detect errdisable

no bridge 1 storm-detect errdisable

Default: **Disabled**

Usage Example – Enabling storm detect:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# bridge 1 storm-detect errdisable
switch_a(config)#q
switch_a#
```

Usage Example – Disabling storm detect:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# no bridge 1 storm-detect errdisable
switch_a(config)#q
switch_a#
```

To set the storm-detect interval use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **bridge 1 storm-detect interval *<2-65535>***

Default: **10**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# bridge 1 storm-detect interval 10
switch_a(config)#q
switch_a#
```

To set the storm-detect recovery time use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **bridge 1 storm-detect errdisable-recovery *<0-65535>***

Default: **0** No errdisable recovery.

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# bridge 1 storm-detect errdisable-recovery 60
switch_a(config)#q
switch_a#
```

Storm Detect Packet Type

Enable this port's storm detect by detect number of broadcast or broadcast plus multicast packets per second. Unit is packets per second. Set to 0 to disable this feature.

To set the storm-detect packet type use the following CLI commands:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **storm-detect (bc | mc-bc) pps <*0-100000*>**
bc = broadcast only
mc-bc = count broadcast & multicast packets together.

Default: **0** (Disabled)

Usage Example 1 – Enabling Multicast + Broadcast:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# interface ge1
switch_a(config-if)#storm-detect mc-bc pps 50000
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Usage Example 2 – Enabling Multicast + Broadcast:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# interface ge1
switch_a(config-if)#storm-detect bc pps 50000
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

To set the storm-detect utilization use the following CLI commands:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **storm-detect utilization <*0-100*>**

Default: **0** (Disabled)

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# interface ge1
switch_a(config-if)#storm-detect utilization 80
switch_a(config-if)#q
```

```
switch_a(config)#q
switch_a#
```

To disable storm-detect on a port use the following CLI commands:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **no storm-detect port enable**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# interface ge1
switch_a(config-if)#no storm-detect port enable
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

To disable storm-detect on a port use the following CLI commands:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **no storm-detect port enable**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# interface ge1
switch_a(config-if)#no storm-detect port enable
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Adding a MAC Address for Static-MAC-Entry Forwarding

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
bridge 1 address <*mac address*> forward <*interface*> vlan <*vlan id*>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# bridge 1 address 00e0.abcd.1245 forward ge1 vlan 1
switch_a(config)#q
switch_a#
```

Discard a Static MAC Entry

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **bridge 1 address <*mac address*> discard vlan <*vlan id*>**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# bridge 1 address 00e0.abcd.1245 discard vlan 1
switch_a(config)#q
switch_a#
```

Configuring Port Mirroring

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **mirror interface <*interface*> direction <*both* | *tx* | *rx*>**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a#interface ge1
switch_a(config-if)# mirror interface ge1 direction both
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Enabling a Link State Tracking Group

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **link state track <*group #*>**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# link state track 4
switch_a(config)#q
switch_a#
```

Assigning a Port to a Link State Tracking Group

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **link state group <*group* #> <*upstream* | *downstream*>**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface ge1
switch_a(config-if)# link state group 4 downstream
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Setting PoE Power Budget

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **poe system-power-budget <*value*>**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# poe system-power-budget 144.14
switch_a(config)#q
switch_a#
```

PoE Port Settings

The following commands are used to set PoE functions related directly to individual PoE ports:

CLI Command (click link for syntax)	**Function**
Enable	Enables PoE on a port
Fixed Power Limit	Sets a fixed wattage for a PoE port
Power-classification	Sets a port to negotiate power-classification
Power-down-alarm	Turns on alarm by relay on PoE power down
Power-priority	Sets priority of power distribution to ports
Scheduling	Enable Scheduling
Schedule-time	Sets schedule time to power PoE ports
Schedule-time-hour	Schedule time (hour)

Figure 61: CLI commend syntax

Enable

To enable or disable PoE on a port use the following CLI commands

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
poe enable
no poe enable

Usage Example 1 – Enabling PoE on a port:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# interface ge1
switch_a(config-if)# poe enable
switch_a(config-if)#q
switch_a(config)#q
```

Usage Example 2 – Disabling PoE on a port:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# interface ge1
switch_a(config-if)# no poe enable
switch_a(config-if)#q
switch_a(config)#q
```

Fixed Power Limit

The fixed-power-limit CLI command sets the maximum wattage that a switch port will provide to the attached PoE device. To set a fixed power limit on a port **Power Limit by Classification** must be disabled on the port first (see Power-classification).

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **poe fixed-power-limit <*level*>**
Level = 0-15.4 (802.3af) / 30 (802.3at) / 60 (W)

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# interface ge1
switch_a(config-if)# poe fixed-power-limit 7.5
switch_a(config-if)#q
switch_a(config)#q
```

Power-classification

This setting tells the switch to negotiate with the attached PoE device to determine the Watts that will be provided by the switch. To change this setting, check (enable) or uncheck (disable) the check box located in the *Power Limit by Classification* column. The default is checked (Enabled). This is a per port setting.

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
poe power-classification enable
no poe power-classification enable

Usage Example 1 – Enabling PoE Power Classification on a port:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# interface ge1
switch_a(config-if)# poe power-classification enable
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Usage Example 2 – Disabling PoE Power Classification on a port:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# interface ge1
switch_a(config-if)# no poe power-classification enable
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Power-down-alarm

This setting only applies to EtherWAN Switches that have a relay. If this setting is enabled, losing PoE power on a port triggers the relay on the switch.

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
poe power-down-alarm enable
no poe power-down-alarm enable

Usage Example 1 – Enabling PoE power down alarm on a port:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# interface ge1
switch_a(config-if)# poe power-down-alarm enable
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Usage Example 2 – Disabling PoE power down alarm on a port:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# interface ge1
switch_a(config-if)# no poe power-down-alarm enable
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Power-priority

Use this setting to set the priority to High, Medium or Low.
To set the PoE power priority, use the following CLI command:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **poe power-priority *<high | medium | low>***

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# interface ge1
switch_a(config-if)# poe power-priority medium
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

PoE Scheduling

PoE Scheduling allows PoE ports to have their power up time scheduled by hour of the day and day of the week.

Scheduling

To enable PoE Power Scheduling on a port, use the following CLI command:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **poe scheduling enable**

To disable PoE scheduling on a port use the *no poe* *Enable* command

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# interface ge1
switch_a(config-if)# poe scheduling enable
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Schedule-time

To enable PoE Power Scheduling on a port, use the following CLI command:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **poe schedule-time *<day> <hour(s)>***
Day = 0 (Sunday) to 6 (Saturday)
Hour = 1 to 23. Multiple hours can be defined using a dash (ex. 1-23)

To disable PoE scheduling on a port use the *no poe* Enable command

Usage Example 1:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# interface ge1
switch_a(config-if)# poe schedule-time 0 10
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Usage Example 2 – Multiple hours:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# interface ge1
switch_a(config-if)# poe schedule-time 0 10-14
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Schedule-time-hour

To enable PoE Power Scheduling on a pse the following CLI command:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **poe schedule-time *<day> <hour>***
Day = 0 (Sunday) to 6 (Saturday)
Hour = 1 to 23

To disable PoE scheduling on a port use the *no poe* Enable command.

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# interface ge1
switch_a(config-if)# poe schedule-time 0 10
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

PoE Watchdog

PoE Watchdog is a management feature to help system administrators monitor and manage critical PoE powered devices. PD Watchdog is only supported on PoE enabled ports. Once enabled, the system will continuously ping a user specified IP address across the port. If the system does not receive a reply within a specified interval, it can automatically power down or power cycle the powered device. To configure PoE Watchdog use the following CLI commands

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **poe watchdog check-address AAA.BBB.CCC.DDD**
poe watchdog enable
poe watchdog failure-action < noaction | powercycle | poweroff >
poe watchdog failure-count <1-10>
poe watchdog ping-interval <30-600>
poe watchdog startup delay <30-600>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface ge1
switch_a(config-if)#poe watchdog enable
switch_a(config-if)#poe watchdog check-address 10.10.10.120
switch_a(config-if)# poe watchdog startup-delay 45
switch_a(config-if)# poe watchdog ping interval 60
switch_a(config-if)# poe watchdog failure-action <powercycle>
switch_a(config-if)#q
switch_a(config-)#
```

PoE 4-Pair Delivery

This feature is not available on all models.

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **poe 4-pair-power enable**

Usage Example:

```
switch_a(config-if)#poe 4-pair-power enable
```

Extended PoE

PoE can be extended to 250m with 10Mbps transfer speed.This feature is not available on all models. Note that if PoE extend mode is enabled, EEE and auto-negotiation will be disabled. Only 10Mbps speed is available if this feature is enabled.

CLI Command Mode: **Interface Configuration Mode**
CLI Command Syntax: **poe extend-mode enable**

Usage Example:

```
switch_a(config-if)#poe extend-mode enable
```

Note: When PoE extended mode is enabled, please also set the end device to "force-10Mbps full duplex" to cooperate with the switch.

Note: It is suggested to pre-test the function before deployment. The maximum available transmission distance of PoE depends on the negotiation result of PD and PSE. Some PDs using EtherWAN PoE/PSE switches may only support a standard distance of 100 meters. Contact EtherWAN if assistance is needed.

PoE Action

PoE Action provides the option to turn on or turn off the PoE port for a specific amount of seconds. This "on/off" cycle can be repeated for a specific amount of times.

CLI Command Mode: **Privileged Exec Mode**
CLI Command Syntax: **show poe action**

Usage Example:

```
switch_a>#show poe action
```

Enable/disable PoE Action

CLI Command Mode: **Global Config Mode**
CLI Command Syntax: **[no] poe action enable**

Select a trigger source of a specific port.

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **[no] poe action trigger <1-2>**

Set the duration and times to repeat of the PoE action cycle.

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **poe action on <3-60> off <3-60> repeat <0-50>**

Trigger the PoE action on the port

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **poe action run**

TRUNKING

Overview

Port Trunking refers to the use of multiple network connections in parallel to increase the link speed beyond the limits of any one single cable or port. This is commonly called link aggregation. These aggregated links may be used to interconnect switches or to connect high-capacity servers to a network.

The switch supports up to four trunk groups. Each trunk can be composed of up to eight 1Gbps ports while each SFP trunk can support up to two gigabit or 10Gb ports.

There are two popular types of port trunking, static and link aggregation control protocol (LACP).

Static Channel Trunking

Originally specified in the IEEE802.3AD specification and now in the IEEE 802.1AX2008 specification, this type of trunking is the most basic and easiest to understand. It simply is the aggregation of two or more Ethernet links to form a virtual link equivalent in bandwidth to the sum of its individual links. For example, if one had four 1Gbps Ethernet links composing a single static channel, the overall bandwidth of the static channel would be 4Gbps.

The aggregation feature allows up to eight ports to be grouped together as a single-link connection between two switch devices. The increases the effective bandwidth thought a link and provides redundancy. It allows up to 4 aggregation groups which depends on your available port counts. Ports within an aggregation group must be of the same linked speed. By performing a dynamic hashing algorithm on the MAC address, each packet destined for the aggregation is forwarded to one of the valid ports within the aggregation group. By dynamically performing this function, the traffic patterns can be more balanced across the ports within an aggregation. In addition, the MAC-based algorithm provides dynamic failover. If a port within an

aggregation group fails, the other ports within the aggregation automatically assume all traffic designated for the aggregation.

Link Aggregation Control Protocol

Within the IEEE specification, the Link Aggregation Control Protocol (LACP) provides a method to control the bundling of several physical ports together to form a single logical channel. LACP allows a network device to negotiate an automatic bundling of links by sending LACP packets to the peer (directly connected device that also implements LACP). This means that both sides of the LACP channel must be configured for LACP which implies both devices must support it.

LACP also has a couple of very important advantages over static channel:

- Failover when a link fails and there is (for example) a media converter between the devices which means that the peer will not see the link down. With static link aggregation the peer would continue sending traffic down the link causing it to be lost.
- The device can confirm that the configuration at the other end can handle link aggregation. With Static link aggregation a cabling or configuration mistake could go undetected and cause undesirable network behavior.

NOTE: Before configuring a port trunk, disable or disconnect all of the ports that you want to use with this trunk. When the trunk has been (re)configured, enable or reconnect the ports.

Port Trunking

To navigate to the **Port Trunking** menu:

1. Click on the **+** next to **Trunking**.
2. Click on **Port Trunking.**

There are 2 interfaces for Port Trunking supported, depending on the model of EtherWAN Managed switch.

Interface 1 (see Figure 56)

To create a trunk:

1. Click on the checkbox for each desired port in the radio button selected **Static Channel** or **LACP** Group. A port cannot be in the Static Channel Group and the LACP Group at the same time

2. Click on the **Submit** button.

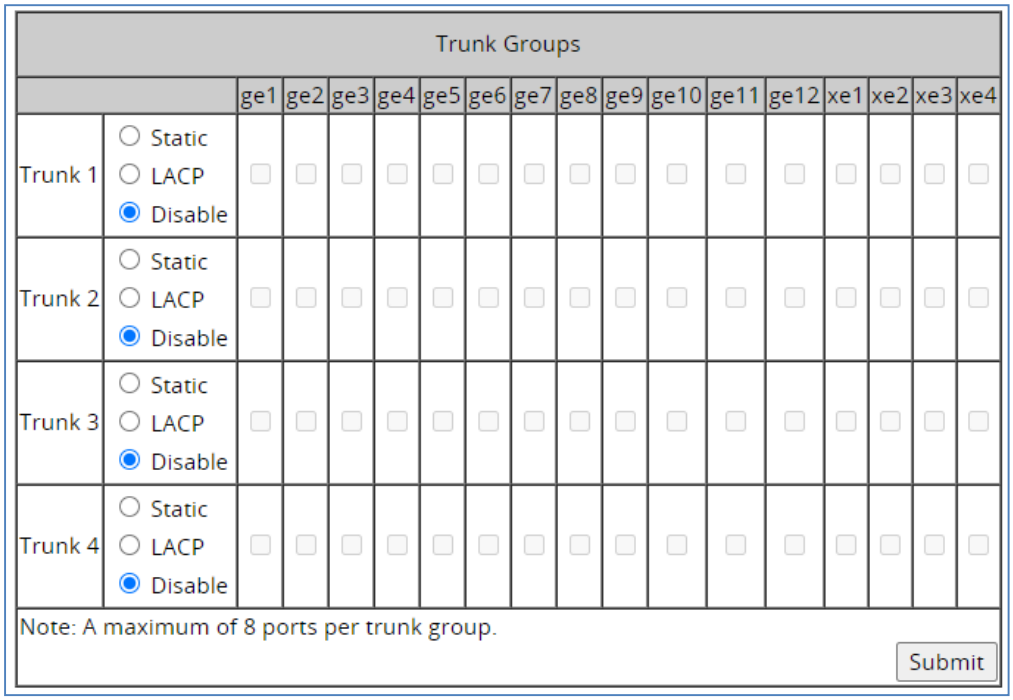


Figure 56: Port Trunking – Interface 1

Version 2 (see Figure 57)

To create a static trunk consisting of 10Gbps ports:

1. Click on the checkbox for each desired port in a specific trunk.
2. Click on the **Submit** button.

To create a static trunk consisting of 1000Mbps ports (see Figure 57):

1. In the **XE Trunking** section, click on the checkbox for each desired port in a specific trunk.
2. Click on the **Submit** button.

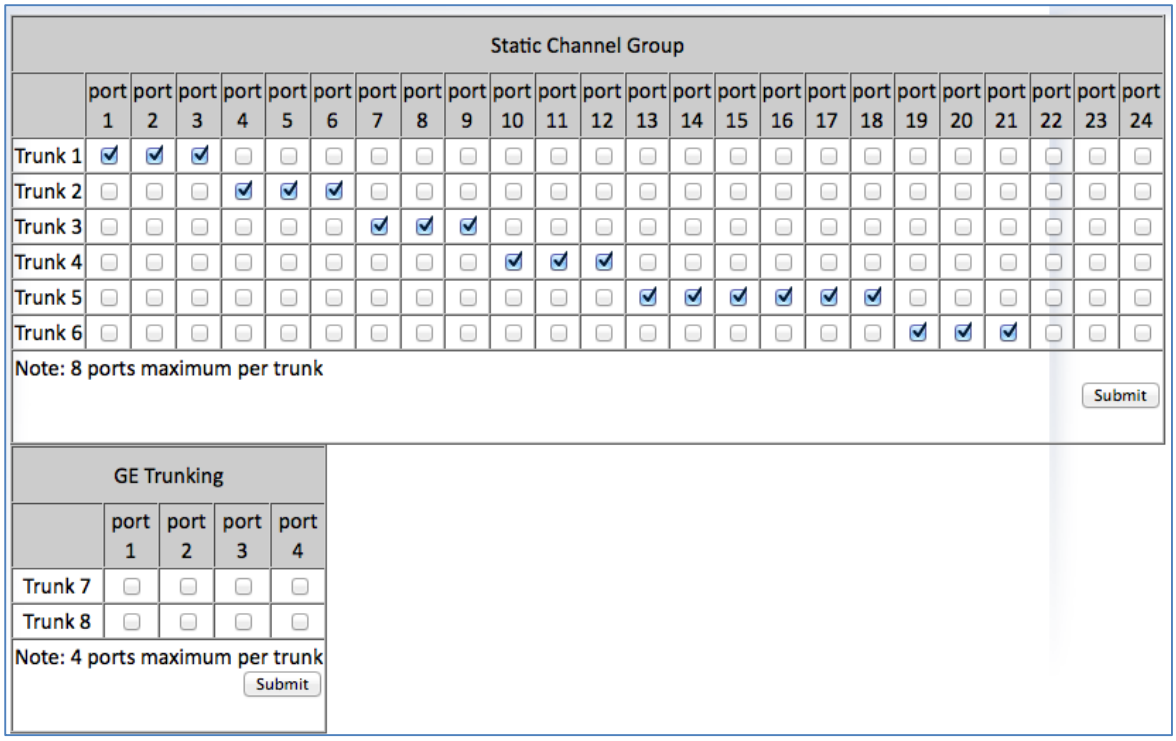


Figure 57: Port Trunking – Interface 2

LACP Trunking

To navigate to the **LACP Trunking** menu:

1. Click on the **+** next to **Trunking**.
2. Click on **LACP Trunking.**

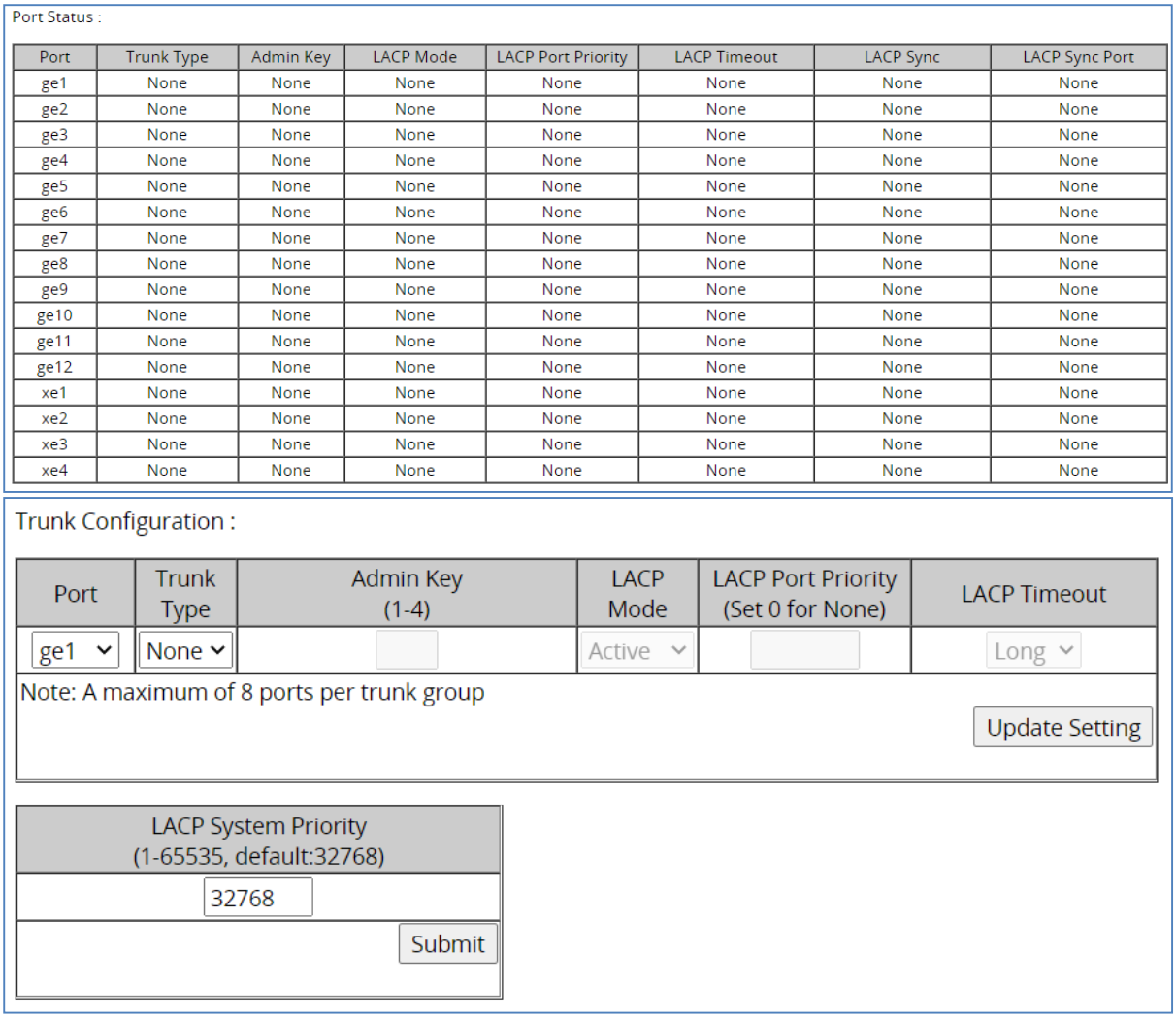
To create a LACP trunk (see Figure 58):

1. In the **Trunk Configuration** section, select a port in the LACP trunk.
2. Select **LACP** from the Trunk Type dropdown box for this port.
3. Enter an admin key for this port in the **Admin Key** textbox. 10Gb ports admin keys must be **1** and 1Gbps ports must be **3**.
4. Select the LACP Mode to either **Active** or **Passive**.
5. Enter a value in the **Port Priority** textbox.
6. Select a Timeout value of **Short** or **Long**.
7. Click on the **Submit** button.

8. Repeat steps 1-7 for each additional port that is to be used in the trunk.

To set the LACP System Priority

1. Enter a value between 1 and 65535. The default value is 32768.
2. Click on the **Submit** button.



Port Status :

Port	Trunk Type	Admin Key	LACP Mode	LACP Port Priority	LACP Timeout	LACP Sync	LACP Sync Port
ge1	None	None	None	None	None	None	None
ge2	None	None	None	None	None	None	None
ge3	None	None	None	None	None	None	None
ge4	None	None	None	None	None	None	None
ge5	None	None	None	None	None	None	None
ge6	None	None	None	None	None	None	None
ge7	None	None	None	None	None	None	None
ge8	None	None	None	None	None	None	None
ge9	None	None	None	None	None	None	None
ge10	None	None	None	None	None	None	None
ge11	None	None	None	None	None	None	None
ge12	None	None	None	None	None	None	None
xe1	None	None	None	None	None	None	None
xe2	None	None	None	None	None	None	None
xe3	None	None	None	None	None	None	None
xe4	None	None	None	None	None	None	None

Trunk Configuration :

Port	Trunk Type	Admin Key (1-4)	LACP Mode	LACP Port Priority (Set 0 for None)	LACP Timeout
ge1	None		Active		Long

Note: A maximum of 8 ports per trunk group

Update Setting

LACP System Priority (1-65535, default:32768)
32768
Submit

Figure 58: LACP Trunking Interface

Trunking Configuration Using CLI Commands

Adding an Interface to a Static Trunk

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
static-channel-group <*static channel*> (1-6 for 100Mbps, 7-8 for 1Gbps ports)

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface ge1
switch_a(config-if)#static-channel-group 1
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Adding an Interface to a LACP Trunk

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
channel-group <*LACP Channel*> mode <*active* | *passive*>
(LACP Channel is 1-6 for 100Mbps, 7-8 for 1Gbps ports)

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface ge1
switch_a(config-if)# channel-group 2 mode passive
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Setting the LACP Port Priority

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **lacp port-priority <1 - 65535>**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface ge1
```

```
switch_a(config)# lacp port-priority 1
switch_a(config)#q
switch_a(config)#q
switch_a#
```

Setting the LACP Timeout

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **lacp timeout *<long* | *short>***

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface ge1
switch_a(config-if)# lacp timeout long
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

STP/RING PAGE – OVERVIEW

Choosing the Spanning Tree Protocols

The Spanning Tree algorithm works by designating a single switch (The Root Bridge) in the network, as the root or the parent to all the switches. All the switches in the network will use the same algorithm to form unique paths all the way back to the Root Bridge. Some switches establish a blocking point (a port on a switch) somewhere along the path to prevent a loop. There are 3 versions of the Spanning Tree protocol, STP, RSTP, MSTP, and they are all backwards compatible with each other.

Spanning Tree Protocol (STP)

This is the original Spanning Tree protocol, and it has been superseded by both the RSTP and MSTP protocol. It is based on a network with a maximum diameter of no more than 17 switches. It uses timers to synchronize any changes in the network topology, and this could take minutes. It is not recommended that you use this version of the Spanning Tree protocol.

Rapid Spanning Tree protocol (RSTP)

The RSTP protocol is the new enhanced version of the original STP protocol. It uses an enhanced negotiation mechanism to directly synchronize any topology changes between switches; it no longer uses timers as in the original STP protocol, which results in a faster re-convergence time. The maximum allowed network diameter for the RSTP protocol is 40 switches.

Multiple Spanning Tree Protocol (MSTP)

The MSTP protocol extends the RSTP protocol by simultaneously running multiple instances of the Spanning Tree Protocol and mapping different VLANs to each instance, thus providing load balance across multiple switches. The MSTP protocol accomplishes this by creating new extended sections within the RSTP protocol, called Regions. Each region runs its own instance of the Spanning Tree Protocol. Within each Region, the MSTP protocol can accommodate a network diameter of up to 40 switches. There can be a maximum of 40 Regions in a single MSTP network.

STP/RING PAGE - CONFIGURING RSTP

Global Configuration Page

To navigate to the **STP/Ring Global Configuration** page:

1. Click on the **+** next to **STP/Ring**.
2. Click on **Global Configuration**.

Enabling the RSTP Protocol

RSTP is enabled by Default. If RSTP has been disabled and you wish to enable it (see Figure 59):

1. Click the dropdown box next to **Spanning Tree** Protocol and choose **Enable**.
2. Click on the dropdown box next to **STP Version** and select **RSTP**.
3. Click on the **Update Setting** button.

Additional Global Configuration page settings

- **Bridge Priority** – Bridge Priority is used to set the Root and backup Root Bridge. For more details see The Root Bridge & Backup Root Bridge.

- Default is 32768. Range is 0 to 61440.

- **Hello Time** – This tells how often a BPDU (Bridge Protocol Data Unit) is sent (see Bridge Protocol Data Units). Default is 2 seconds. Range is 1 to 10 seconds.
- **Max Age** – Default is 20. Hop count limit for BPDU packets (see Setting the MAX Age, Forward Delay and Hello Timer),
- **Forward Delay -** Default is 15 sec.

Note: Bridge Protocol Data Units (BPDUs) are frames that contain information about the Spanning tree protocol (STP). Switches send BPDUs using a unique MAC address from its origin port and a multicast address as destination MAC (01:80:C2:00:00:00). There are three kinds of BPDUs:

- Configuration BPDU, used by Spanning Tree Protocol to provide information to all switches.
- TCN (Topology change), tells about changes in the topology.
- TCA (Topology change Acknowledgment), confirm the reception of the TCN.

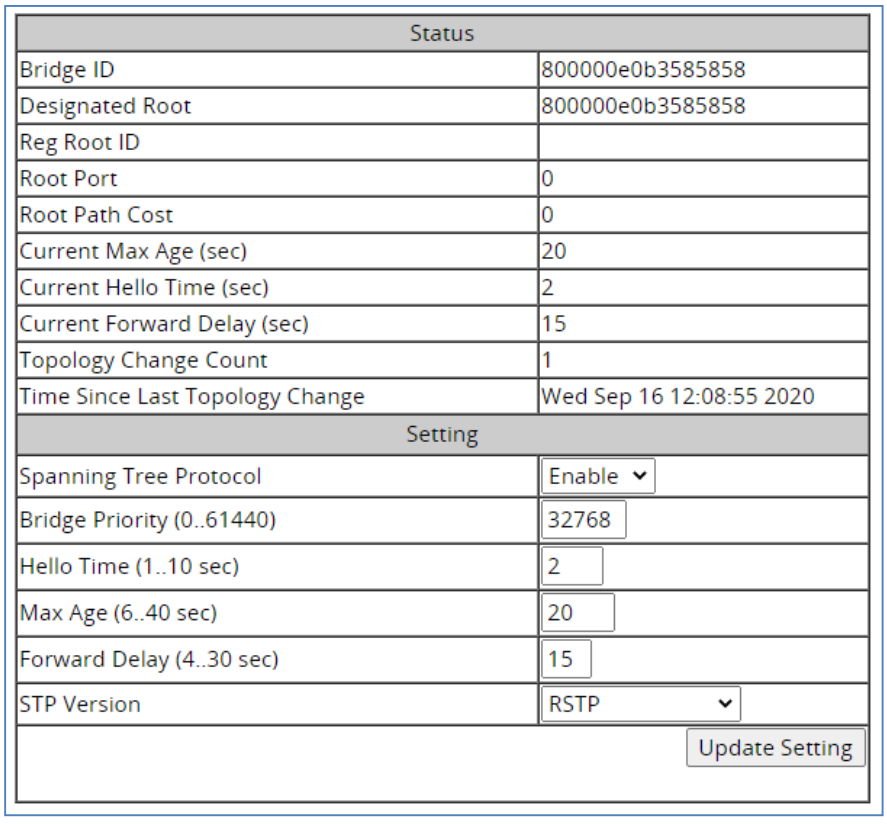


Figure 59: STP/Ring Global Configuration

The Root Bridge & Backup Root Bridge

To configure the Spanning Tree protocol on your network, you will need to setup a Root Bridge and Backup Root Bridge. In order to configure a switch to be the Root Bridge of a Spanning Tree network, you have to make sure that the Bridge Priority (which is the most significant 4 bits of the Bridge ID) of the switch is the lowest among any of the switches on the network. Similarly for the Backup Root Bridge, it must have the next lowest Bridge Priority of all the switches.

Note: Since the **Bridge Priority** is the most significant 4 bit of the Bridge ID, the lowest **Bridge Priority** will always be the Root Bridge and the second lowest **Bridge Priority** will be the Backup Root Bridge. If all switches have the same **Bridge Priority**, then The 12 bit System ID or MAC Address (if the system ID's are the same) will be used to determine the Root and Backup Root Bridge (See Figure 66).

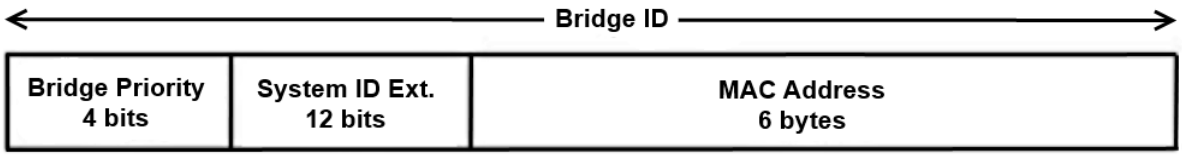


Figure 60: Bridge ID

Bridge ID is a concatenation of 3 values: a 4-bit Bridge Priority (most significant), a 12 bit System ID (less significant), and the 48 bit MAC address of the local switch (least significant).

Setting the Root Bridge and Backup Root Bridge

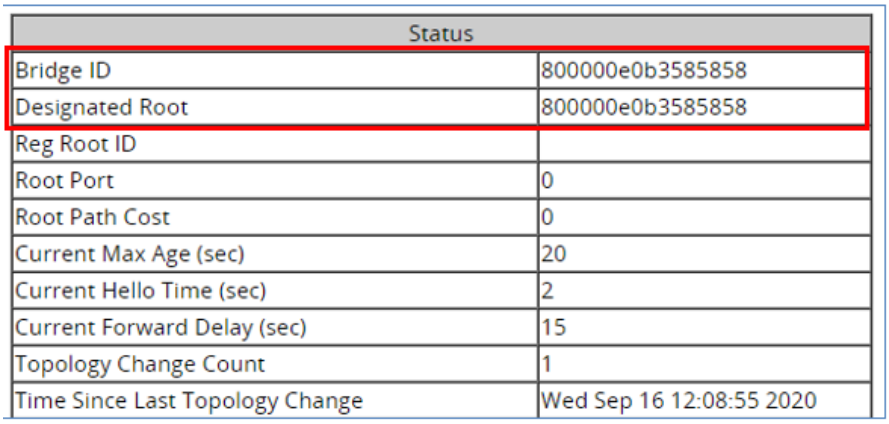
To navigate to the **STP/Ring Global Configuration** page:

1. Click on the **+** next to **STP/Ring**.
2. Click on **Global Configuration**.

To set the Bridge Priority:

1. Enter the **Bridge Priority ID** in the text box to the right of **Bridge Priority (0..61440)**
2. Click on the **Update Setting** button.

Note: The valid values for this parameter are from 0 to 61440, in increments of 4096; you will see this value reflected in the first hexadecimal digit of the **Bridge ID** field after you click the **Update Setting** button (See Figure 61). Set this value to be less than any other switch on the network, in order to make this switch the Root Switch. To set a **Backup Root Bridge** set the **Bridge ID** to be between the **Root Bridge** and the rest of the network switches.



Status	
Bridge ID	800000e0b3585858
Designated Root	800000e0b3585858
Reg Root ID	
Root Port	0
Root Path Cost	0
Current Max Age (sec)	20
Current Hello Time (sec)	2
Current Forward Delay (sec)	15
Topology Change Count	1
Time Since Last Topology Change	Wed Sep 16 12:08:55 2020

Figure 61: Bridge ID Display

Setting the MAX Age, Forward Delay and Hello Timer

To navigate to the **STP/Ring Global Configuration** page:

1. Click on the **+** next to **STP/Ring**.
2. Click on **Global Configuration**.

The Network Diameter

The Diameter of a network depends on the type of topology your network uses. In a ring topology, the Network Diameter is the total number of switches in a network minus the Root Bridge. In a star topology, the Network Diameter is the maximum number of hops to get from Root Bridge to the switch that is the most hops away. In the RSTP protocol, the **Max Age** parameter is used as a hop count limit on how far the Spanning Tree protocol packet can propagate throughout the network topology, therefore, it must be configured with a value that is greater than the network diameter.

Relationship between Max Age, Forward Delay and Hello Time

The following rules must be followed when setting the **Max Age**, **Forward Delay** and **Hello Timer**:

- Max Age >= 2 × (Hello Time + 1.0 second)
- 2 × (Forward Delay – 1.0 second) >= Max Age

To change the **Max Age**, **Forward Delay** and **Hello Timer** (see Figure 62):

1. Enter the **Max Age** in the text box to the right of Max Age (6..40 sec) label.

2. Enter the **Hello Time** in the text box to the right of the Hello Time (1..10 sec) label.
3. Enter the **Forward Delay** in the text box to the right of the Forward Delay (4..30 sec) label.
4. Click on the **Update Setting** button.
5. Save the configuration (see the Save Configuration Page)

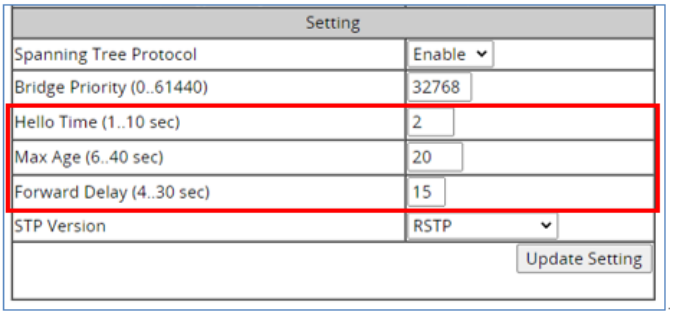


Figure 62: Max Age, Hello Timer & Forward Delay

RSTP Port Setting Page

To navigate to the **STP/Ring RSTP Port Setting** page:

1. Click on the **+** next to **STP/Ring**.
2. Click on **RSTP Port Setting.**

Spanning Tree Port Roles

In a stable RSTP topology, each port on a switch can function in any one of 4 different Spanning Tree port roles. These Spanning Tree port roles are (see Figure 63):

- Root Port
- Designated Port
- Alternate Port
- Backup Port

Port	Port Status	Priority	Path Cost	Point to Point Link	Edge Port
ge1	Designated(Forwarding)	128	20000	Point to Point	Conf. Disabled / Curr. Edge off
ge2	Disabled(Discarding)	128	20000	Shared	Conf. Disabled / Curr. Edge off
ge3	Disabled(Discarding)	128	20000	Shared	Conf. Disabled / Curr. Edge off
ge4	Disabled(Discarding)	128	20000	Shared	Conf. Disabled / Curr. Edge off
ge5	Disabled(Discarding)	128	20000	Shared	Conf. Disabled / Curr. Edge off
ge6	Disabled(Discarding)	128	20000	Shared	Conf. Disabled / Curr. Edge off
ge7	Disabled(Discarding)	128	20000	Shared	Conf. Disabled / Curr. Edge off
ge8	Disabled(Discarding)	128	20000	Shared	Conf. Disabled / Curr. Edge off
ge9	Disabled(Discarding)	128	20000	Shared	Conf. Disabled / Curr. Edge off
ge10	Disabled(Discarding)	128	20000	Shared	Conf. Disabled / Curr. Edge off
ge11	Disabled(Discarding)	128	20000	Shared	Conf. Disabled / Curr. Edge off
ge12	Disabled(Discarding)	128	20000	Shared	Conf. Disabled / Curr. Edge off
xe1	Disabled(Discarding)	128	2000	Shared	Conf. Disabled / Curr. Edge off
xe2	Disabled(Discarding)	128	2000	Shared	Conf. Disabled / Curr. Edge off
xe3	Disabled(Discarding)	128	2000	Shared	Conf. Disabled / Curr. Edge off
xe4	Disabled(Discarding)	128	2000	Shared	Conf. Disabled / Curr. Edge off

Figure 63: Spanning Tree Port Roles

Path Cost & Port Priority

By default, each port on a Spanning Tree switch will be assigned a **Path Cost** based on the port's transmission speed according to the IEEE standard below:

Link speed	**Recommended value**
Less than or equal 100Kb/s	200,000,000
1 Mb/s	20,000,000
10 Mb/s	2,000,000
100 Mb/s	200,000
1 Gb/s	20,000
10 Gb/s	2,000
100 Gb/s	200
1 Tb/s	20
10 Tb/s	2

By default, each port on a Spanning Tree switch will be assigned a Port Priority of 128, according to the IEEE standard. This Port Priority is part of the Port ID, which is a concatenation of 2 values: Port Priority (4 bits) + Interface ID (12 bits) (see Figure 64)

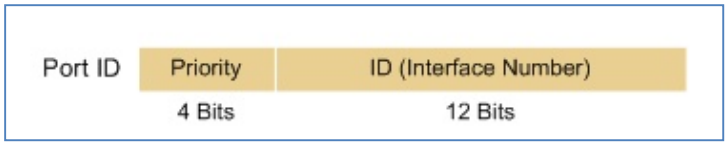


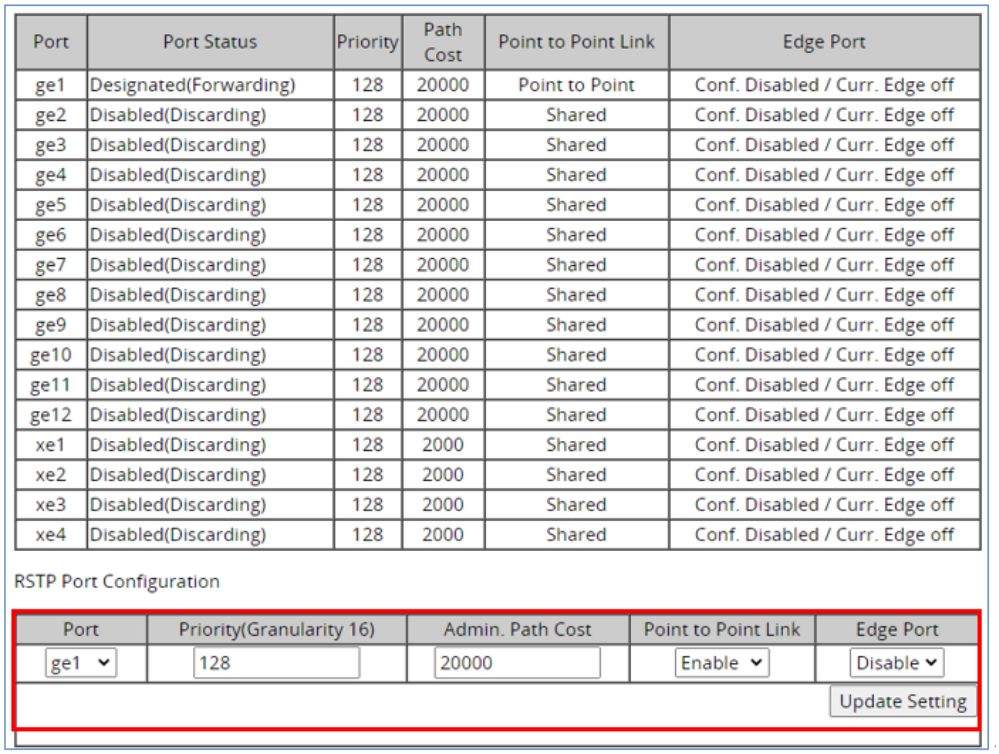
Figure 65: Port ID

Port Priority is part of the Port ID, which is a concatenation of 2 values: Port Priority (4 bits) + Interface ID (12 bits).

The default values will work fine in most scenarios; however, there are times when you may need to adjust these values manually in order to influence the location of the Alternate Port, the Root Port or the Backup Port.

To adjust the Port Priority value or the Path Cost value on a port:

1. Choose the correct port from the drop-down list under **Port** (see Figure 66)
2. Enter the proper value under the **Priority (Granularity 16)**
    a. The Port Priority range is between 0 and 240 in multiples of 16.
3. Enter the proper value under the **Admin. Path Cost** entry field.
    a. The Path Cost range is between 1 and 200,000,000.
4. Click on the **Update Setting** button
5. Save your configuration (see the Save Configuration Page).



Port	Port Status	Priority	Path Cost	Point to Point Link	Edge Port
ge1	Designated(Forwarding)	128	20000	Point to Point	Conf. Disabled / Curr. Edge off
ge2	Disabled(Discarding)	128	20000	Shared	Conf. Disabled / Curr. Edge off
ge3	Disabled(Discarding)	128	20000	Shared	Conf. Disabled / Curr. Edge off
ge4	Disabled(Discarding)	128	20000	Shared	Conf. Disabled / Curr. Edge off
ge5	Disabled(Discarding)	128	20000	Shared	Conf. Disabled / Curr. Edge off
ge6	Disabled(Discarding)	128	20000	Shared	Conf. Disabled / Curr. Edge off
ge7	Disabled(Discarding)	128	20000	Shared	Conf. Disabled / Curr. Edge off
ge8	Disabled(Discarding)	128	20000	Shared	Conf. Disabled / Curr. Edge off
ge9	Disabled(Discarding)	128	20000	Shared	Conf. Disabled / Curr. Edge off
ge10	Disabled(Discarding)	128	20000	Shared	Conf. Disabled / Curr. Edge off
ge11	Disabled(Discarding)	128	20000	Shared	Conf. Disabled / Curr. Edge off
ge12	Disabled(Discarding)	128	20000	Shared	Conf. Disabled / Curr. Edge off
xe1	Disabled(Discarding)	128	2000	Shared	Conf. Disabled / Curr. Edge off
xe2	Disabled(Discarding)	128	2000	Shared	Conf. Disabled / Curr. Edge off
xe3	Disabled(Discarding)	128	2000	Shared	Conf. Disabled / Curr. Edge off
xe4	Disabled(Discarding)	128	2000	Shared	Conf. Disabled / Curr. Edge off

RSTP Port Configuration

Port	Priority(Granularity 16)	Admin. Path Cost	Point to Point Link	Edge Port
ge1	128	20000	Enable	Disable

Update Setting

Figure 66: Port Priority and Path Cost

Point to Point Link

By default, RSTP will assume any full-duplex link as a **Point to Point Link**, but if the switch detects that the neighbor switch is not running the RSTP protocol, it will assume the port to be a **Shared Port**. You can force a port to be a **Shared Port**, if you know in advance that there will be more than one switch connecting to this link (through an unmanaged switch, for example), or if you know in advance that the other switch on this link will be running the older STP protocol.

To manually force a port to be a **Shared Port** or a **Point to Point Link:**

1. Choose the correct port from the drop down list under **Port**, and choose **Enable** or **Disable** under **Point to Point Link** (see Figure 66).
2. Click on the **Update Setting** button.
3. Save the configuration (see the Save Configuration Page)

Edge Port

By enabling the **Edge Port** feature on a port, the switch will stop reacting to any linkup event on this port and will not send out any Topology Change notification to the neighbor bridges.

1. Choose the correct port from the drop down list under **Port**, and choose **Enable** or **Disable** under **Edge Port** (see Figure 66).
2. Click on the **Update Setting** button.
3. Save the configuration (see the Save Configuration Page)

RSTP Configuration Using CLI Commands

Enabling the Spanning Tree Protocol

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
no bridge shutdown 1
bridge 1 protocol rstp vlan-bridge

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#no bridge shutdown 1
switch_a(config)#bridge 1 protocol rstp vlan-bridge
switch_a(config)#q
switch_a#
```

Bridge Priority, Max Age, Forward Delay, and Hello Time

To configure the Bridge Priority, Max Age, Forward Delay, and Hello Time of a Spanning Tree Bridge, use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
bridge 1 priority *<0-61440>*
bridge 1 max-age *<6-40>*
bridge 1 forward-time *<4-30>*
bridge 1 hello-time *<1-10>*

Usage Example:

```
switch_a>enable
```

```
switch_a#configure terminal
switch_a(config)#bridge 1 priority 4096
switch_a(config)#bridge 1 max-age 20
switch_a(config)#bridge 1 forward-time 15
switch_a(config)#bridge 1 hello-time 2
switch_a(config)#q
switch_a#
```

Modifying the Port Priority and Path Cost

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
bridge-group 1 path-cost <*1-200000000*>
bridge-group 1 priority <*0-240*>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface ge1
switch_a(config-if)#bridge-group 1 path-cost 200000
switch_a(config-if)#bridge-group 1 priority 128
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Manually Setting a Port to be a Shared or Point to Point Link

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
spanning-tree link-type point-to-point
spanning-tree link-type shared

Usage Example 1: Setting port 1 to be point-to-point:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface ge1
switch_a(config-if)#spanning-tree link-type point-to-point
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Usage Example 2: Setting port 1 to be shared:

```
switch_a>enable
```

```
switch_a#configure terminal
switch_a(config)#interface ge1
switch_a(config-if)#spanning-tree link-type shared
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Enabling/Disabling a port to be an Edge Port

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
spanning-tree edgeport
no spanning-tree edgeport

Usage Example 1: Enabling edge port on port 1:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface ge1
switch_a(config-if)#spanning-tree edgeport
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Usage Example 2: Disabling edge port on port 1:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface ge1
switch_a(config-if)#no spanning-tree edgeport
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Enabling/Disabling automatic edge detection

CLI Command Mode: **Interface Configuration Mode**

Automatic edge detection is disabled by default.

CLI Command Syntax:
spanning-tree autoedge
no spanning-tree autoedge

STP/RING PAGE - CONFIGURING MSTP

The MSTP protocol adds a new concept called a **Region** to the Spanning Tree algorithm. Unlike RSTP and STP, inside each MSTP Region, there can be more than one instance of Spanning Tree Protocol running simultaneously. The MSTP protocol can then map multiple VLANs to each instance of Spanning Tree protocol to provide load balancing among the switches. Between Regions, the MSTP runs a single instance of Spanning Tree similar to, and is backward compatible with, the RSTP protocol.

Global Configuration Page

Enabling the MSTP Protocol

Navigate to the **STP/Ring Global Configuration** page:

1. Click on the **+** next to **STP/Ring**.
2. Click on **Global Configuration**.
3. Verify that the Spanning Tree Protocol is enabled (see Figure 67), if not, choose **Enabled** from the **Spanning Tree Protocol** drop down list.
4. Choose **MSTP** in the **STP Version** drop down list.
5. Click on the **Update Setting** button.
6. Save the configuration (see the Save Configuration Page).

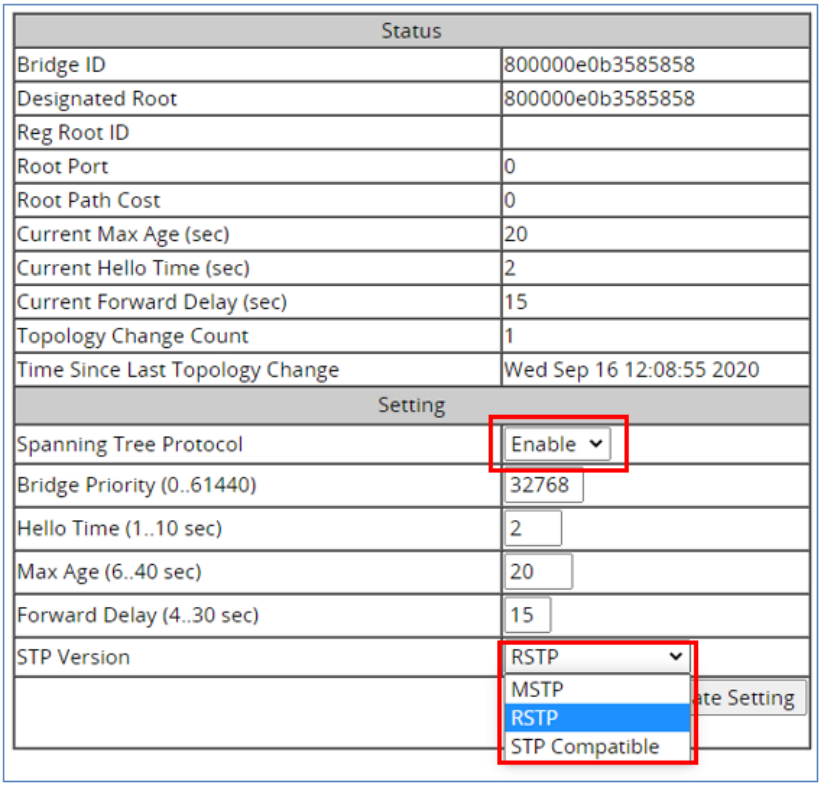


Figure 67: Enabling MSTP

The CIST Root Bridge & Backup CIST Root Bridge

In order to configure a switch to be the CIST Root Bridge of a Spanning Tree network, you just have to make sure that the Bridge Priority (which is the most significant 4 bits of the Bridge ID) of the switch is the lowest among any of the switches on the network. Similarly for the Backup CIST Root Bridge, it must have the next lowest Bridge Priority of all the switches. This Bridge ID is a concatenation of 3 values: a 4 bit Bridge Priority (most significant), a 12 bit System ID (less significant), and the 48 bit MAC address of the local switch (least significant) (see Figure 61).

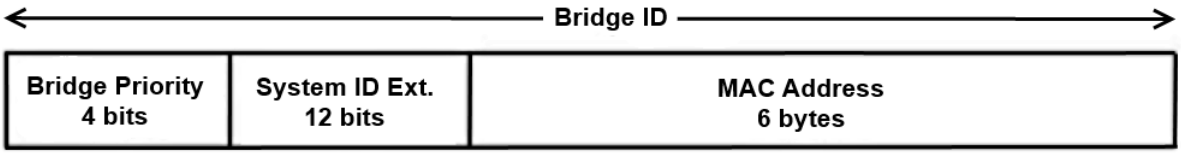


Figure 68: Bridge ID

Setting Bridge Priority

To set the Bridge Priority:

1. Enter the **Bridge Priority ID** in the text box to the right of **Bridge Priority (0..61440)**
2. Click on the **Update Setting** button.

Note: The valid values for this parameter are from 0 to 61440, in increments of 4096; you will see this value reflected in the first hexadecimal digit of the **Bridge ID** field after you click the **Update Setting** button (See Figure 69). Set this value to be less than any other switch on the network, in order to make this switch the Root Switch. To set a **Backup Root Bridge** set the **Bridge ID** to be between the **Root Bridge** and the rest of the network switches.

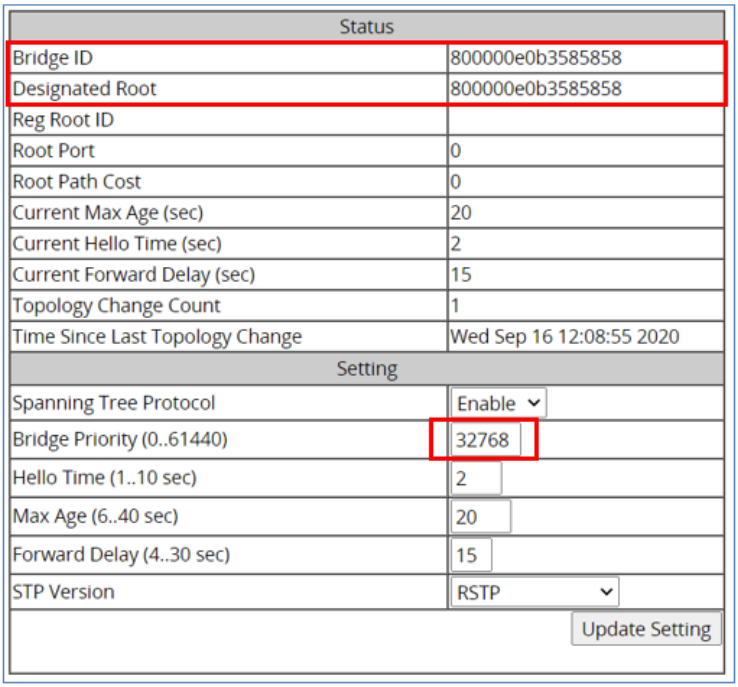


Figure 69: Bridge ID Display

Configuring the CST Network Diameter

When using MSTP, the **Max Age** parameter is used for the CST (Common Spanning Tree) topology simply as a hop count limit on how far the Spanning Tree protocol packet can propagate throughout the CST topology, therefore, the Max Age must be configured with a value that is greater than the network diameter of the CST topology. The Max Age parameter will need to be configured correctly on both the CIST Root Bridge as well as on the Backup CIST Root Bridge (in the event when the CIST Root Bridge fails).

Setting the MAX Age, Forward Delay and Hello Timer

Navigate to the **STP/Ring Global Configuration** page:

1. Click on the **+** next to **STP/Ring**.
2. Click on **Global Configuration**.

Relationship between Max Age, Forward Delay and Hello Time

The following rules must be followed when setting the **Max Age**, **Forward Delay** and **Hello Timer**:

- Max Age >= 2 × (Hello Time + 1.0 second)
- 2 × (Forward Delay – 1.0 second) >= Max Age

To change the **Max Age**, **Forward Delay** and **Hello Timer** (see Figure 70):

1. Enter the **Max Age** in the text box to the right of Max Age (6..40 sec) label.
2. Enter the **Hello Time** in the text box to the right of the Hello Time (1..10 sec) label.
3. Enter the **Forward Delay** in the text box to the right of the Forward Delay (4..30 sec) label.
4. Click on the **Update Setting** button.
5. Save the configuration (see the Save Configuration Page)

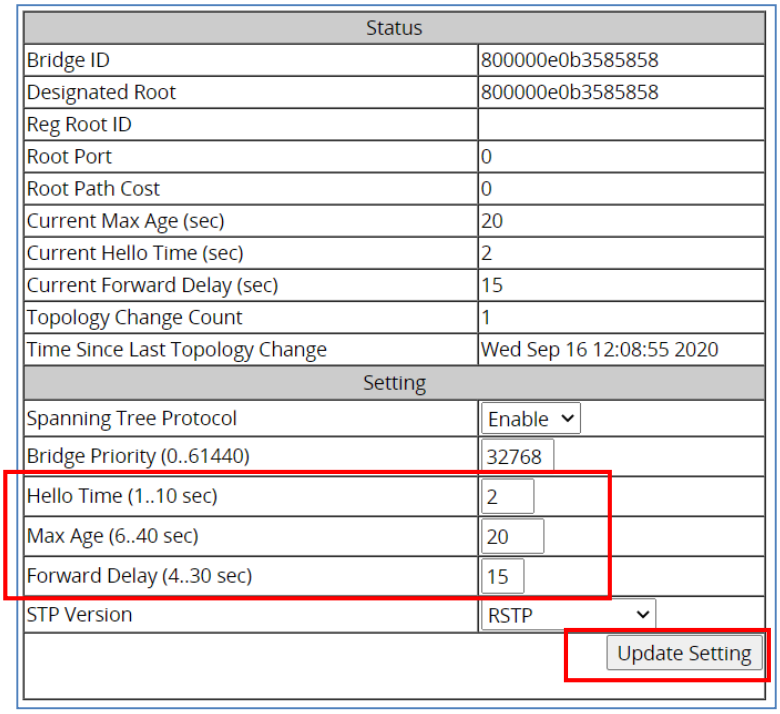


Figure 70: Max Age, Hello Timer & Forward Delay

MSTP Properties Page

Configuring an MSTP Region

In order to form a MSTP Region, the switches that will be connected together to form the MSTP Region must have the same values for the configuration parameters listed below. Two of the parameters can be configured directly, the third parameter (Configuration Digest) will be automatically calculated by the switch based on the **VLAN** to **MSTI (Multiple Spanning Tree Instance)** mapping. The **VLAN** to **MSTI** instance mapping must be the same for all the switches within the same **MSTP Region** (see MSTP Instance Setting Page).

- Region name
- Revision level
- Configuration Digest

To navigate to the **STP/Ring MSTP Properties** page:

1. Click on the **+** next to **STP/Ring**.
2. Click on **MSTP Properties.**

To configure both the MSTP Regional Configuration Name and the Revision Level for each of the switches located in the same MSTP Region (see Figure 76):

1. Enter the **Region Name** of the Region that the switch will belong to in the **Region Name** entry field,
2. Enter the **Revision Level** value for the corresponding Region in the **Revision Level** entry field,
3. Click on the **Update Setting** button.
4. Save the configuration (see the Save Configuration Page)

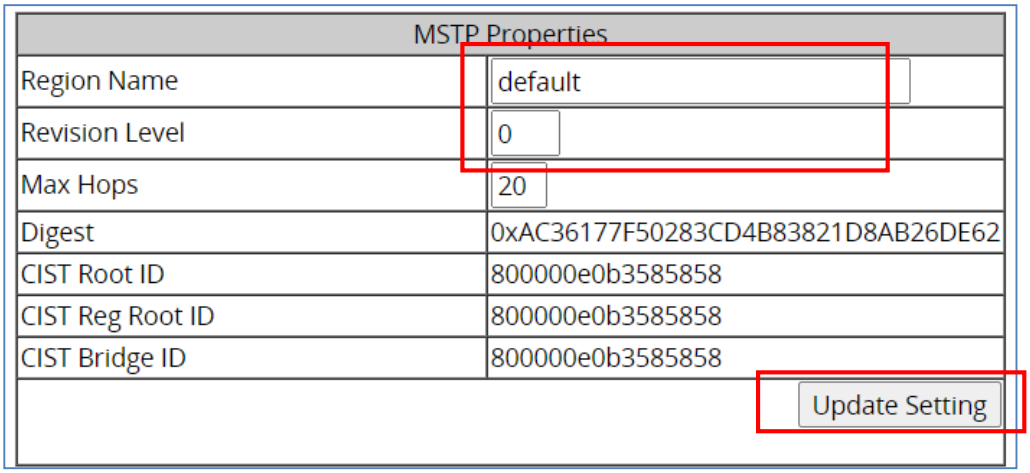


Figure 71: MSTP Region and Revision Level

Configuring the IST Network Diameter

To navigate to the **STP/Ring MSTP Properties** page:

1. Click on the **+** next to **STP/Ring**.
2. Click on **MSTP Properties.**

In the MSTP protocol, the **Max Hops** parameter is used for the **IST** (Internal Spanning Tree) and the **MSTI** (Multiple Spanning Tree Instance) topology as a hop count limit on how far the Spanning Tree protocol packet can propagate inside of a MSTP Region, therefore, it must be configured with a value that is greater than the network diameter of the **IST/MSTI** topology. The **Max Hops** parameters should be configured correctly on the CIST Root and the Backup CIST Root switch and on all the Boundary switches of a MSTP Region (if there are multiple Regions within your MSTP network).

Follow the steps below to configure the **Max Hops** parameter:

1. Enter the desired hop count in the entry field next to **Max Hops**
2. Click on the **Update Setting** button (see Figure 77).
3. Save the configuration (see the Save Configuration Page)

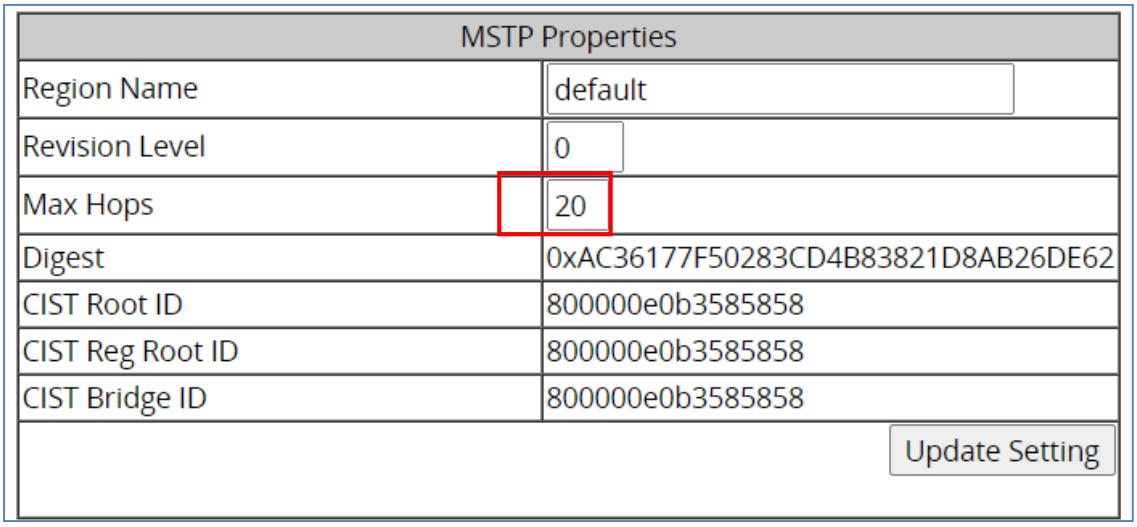


Figure 72: MSTP Properties – Max Hops

MSTP Instance Setting Page

Setting an MSTP Instance

Navigate to the **STP/Ring MSTP Instance Setting** page:

1. Click on the **+** next to **STP/Ring**.
2. Click on **MSTP Instance Setting.**

To create the Spanning Tree instances to be run inside a MSTP Region and its VLAN mappings, follow the below steps.

1. Click on the **VLAN Instance Configuration** button (see Figure 73),
2. Choose the **VLAN** that you want to map to a MSTI instance from the **VLAN ID** drop down box (see Figure 74).
3. Enter the **Instance ID** that you want the VLAN to map to In the entry field next to **Instance ID (1..15)**.
4. Click on the **Update Settings** button.

5. Save the configuration (see the Save Configuration Page)

Note: You can enter a new instance number here, which is how a new MSTI instance is created. You can use an existing MSTI instance if it has already been created on another switch.

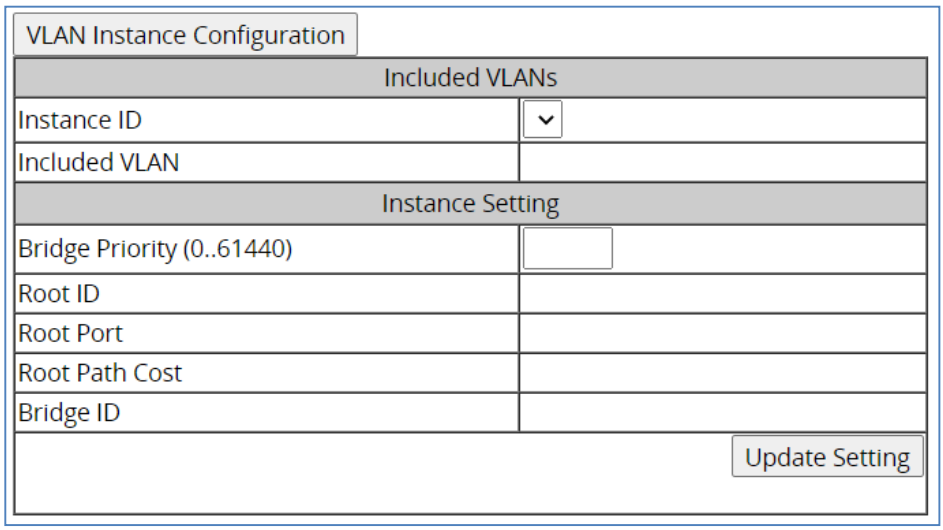


Figure 73: VLAN Instance Configuration

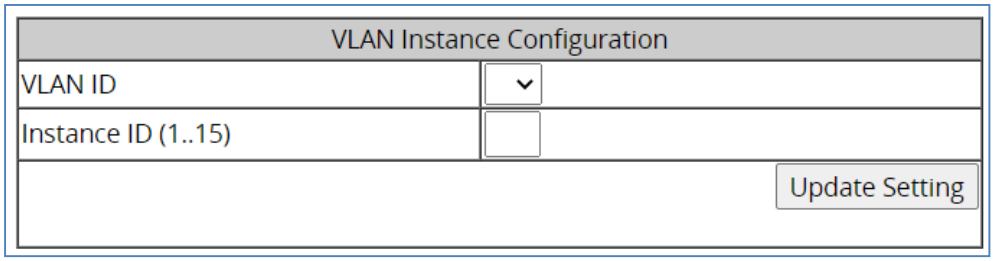


Figure 74: VLAN Instance ID

Modifying MSTP parameters for load balancing

To navigate to the **STP/Ring MSTP Instance Setting** page:

1. Click on the **+** next to **STP/Ring**.
2. Click on **MSTP Instance Setting.**

To load balance switches within a MSTP Region, set different switches within the MSTP Region to be the Root Bridge for different MSTI instances. A Root Bridge in a specific MSTI instance is called a MSTI Regional Root Bridge.

To designate a specific switch in a MSTP Region to be the Root Bridge in a specific MSTI instance, the bridge priority must be set to be the lowest number of all the switches in a specific MSTI instance.

To set the bridge priority on the switch for a specific MSTI Instance (see Figure 75):

1. Choose the specific instance in the **Instance ID** drop down list for which the switch will be a MSTI Regional Root Bridge;
2. Enter the desired value in the **Bridge Priority** text box
3. Click on the **Update Setting** button. The valid values for this parameter are from 0 to 61440, in increments of 4096.
4. Save the configuration (see the Save Configuration Page)

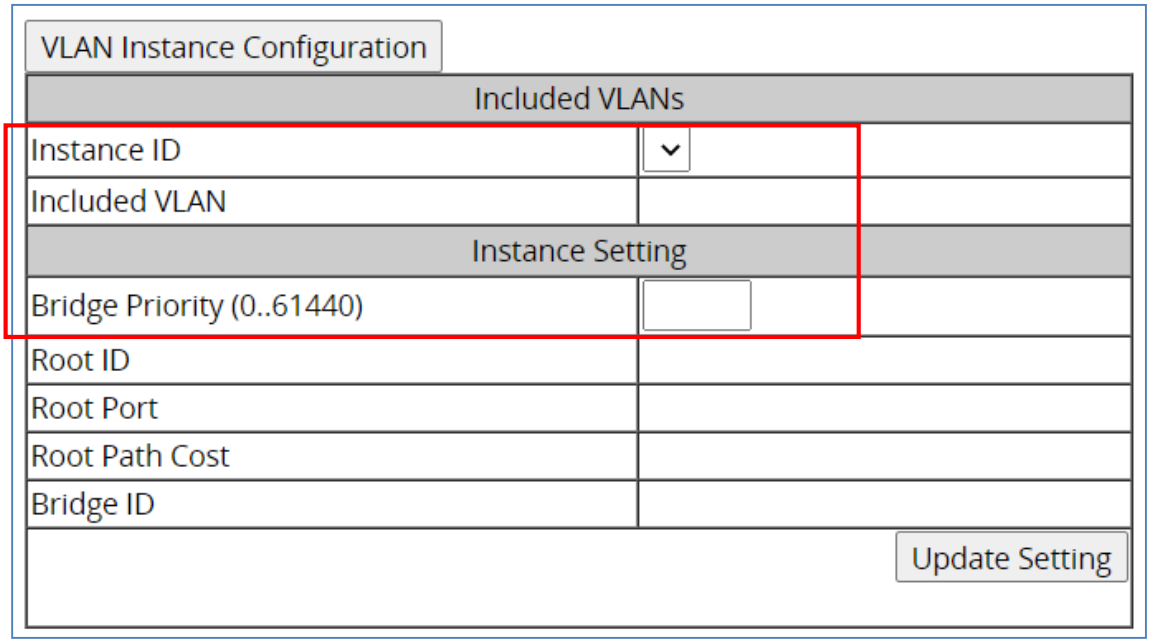


Figure 75: Setting the MSTI Regional Root Bridge

MSTP Port Setting page

Adjusting the blocking port in a MSTP network

To navigate to the **STP/Ring MSTP Port Setting** page:

1. Click on the **+** next to **STP/Ring**.
2. Click on **MSTP Port Setting.**

You can adjust the location of the blocking port in a MSTP network by modifying the **Port Priority** and the **Path Cost** of the ports on the switch. Modifying the **Port Priority** adjusts the blocking port between two switches. Modify the **Port Cost** adjusts the location of the blocking port in a MSTP loop.

To modify the Port Priority and the Path Cost of the ports on a MSTP switch for the MSTI instance only, follow these steps:

1. Choose the correct MSTI Spanning Tree instance from the drop-down list under **Instance ID** (see Figure 76).
2. Choose the correct port number from the drop-down list under **Port**, and enter the proper value under the **Priority** and the **Admin. Path Cost** text box,
3. Click on the **Update Setting** button (see Figure 76).
4. Save the configuration (see the Save Configuration Page)

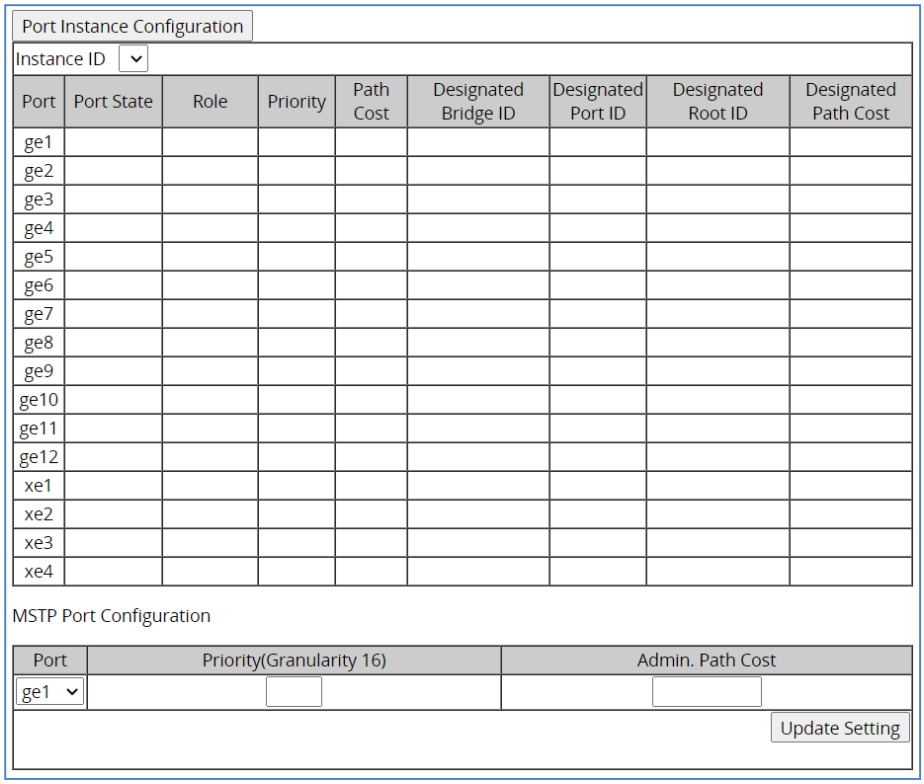


Figure 76: Port Cost & Priority

MSTI Instance Port Membership

To navigate to the **STP/Ring MSTP Port Settings** page:

1. Click on the **+** next to **STP/Ring**.
2. Click on **MSTP Port Setting.**

If changes have been made to the port membership of a VLAN, you must also reconfigure the MSTI port membership for the MSTI instance that the VLAN maps to.

To reconfigure the MSTI instance port membership:

1. Click on the **Port Instance Configuration** button (see Figure 77)
2. Choose the correct MSTI instance from the drop down list next to **Instance ID** (see Figure 78).
3. Check the box next to all the ports that should be part of this instance
4. Click on the **Update Setting** button.
5. Save the configuration (see the Save Configuration Page)

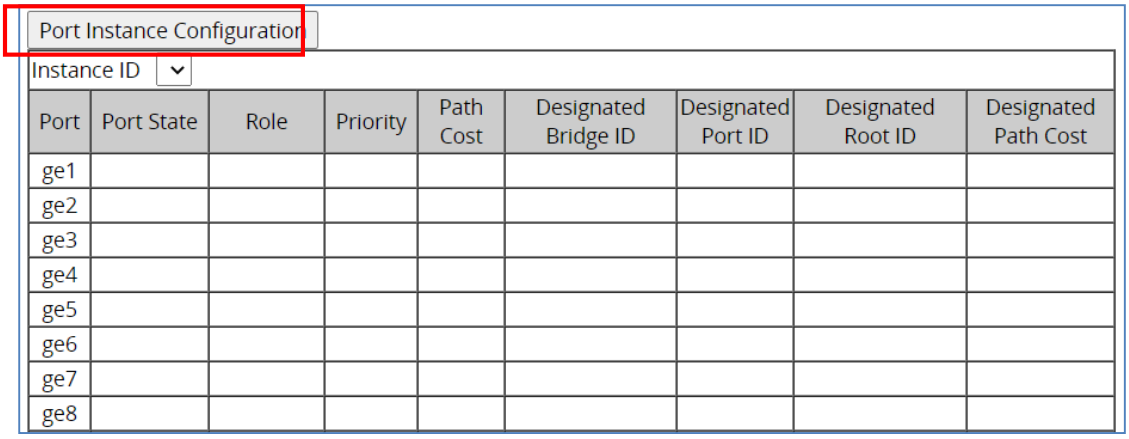


Figure 77: Port Instance Configuration

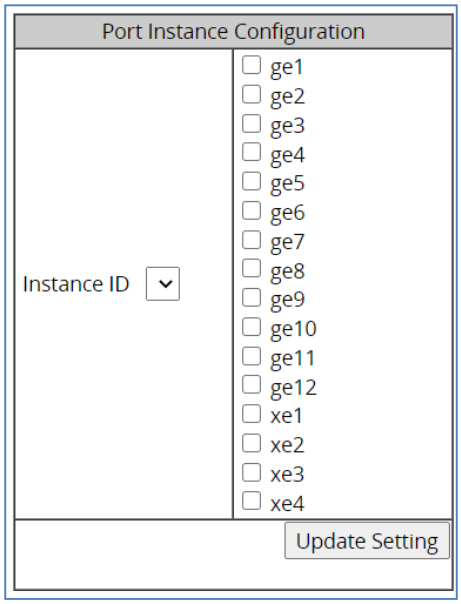


Figure 78: Port Instance - Adding Ports

MSTP Configuration Using CLI Commands

Enabling Spanning Tree for MSTP

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
no bridge shutdown 1
bridge 1 protocol mstp

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#no bridge shutdown 1
switch_a(config)#bridge 1 protocol mstp
switch_a(config)#q
switch_a#
```

Bridge Priority, Max Age, Forward Delay, and Hello Time

To configure the CIST Bridge Priority, Max Age, Forward Delay, and Hello Time of a Spanning Tree Bridge, use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
bridge 1 priority *<0-61440>*
bridge 1 max-age *<6-40>*
bridge 1 forward-time *<4-30>*
bridge 1 hello-time <*1-10*>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#bridge 1 priority 4096
switch_a(config)#bridge 1 max-age 20
switch_a(config)#bridge 1 forward-time 15
switch_a(config)#bridge 1 hello-time 2
switch_a(config)#q
switch_a#
```

Configure IST MAX Hops

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **bridge 1 max-hops *<1-40>***

Usage Example:

```
switch_a>enable
switch_a#configure terminal
```

```
switch_a(config)#bridge 1 max-hops 20
switch_a(config)#q
switch_a#
```

MSTP Regional Configuration Name and the Revision Level

CLI Command Mode: **MSTP Configuration Mode**

CLI Command Syntax:
bridge 1 region <*region_name*>
bridge 1 revision <*revision_number*>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#spanning-tree mst configuration
switch_a(config-mst)#bridge 1 region R1
switch_a(config-mst)#bridge 1 revision 0
switch_a(config-mst)#q
switch_a(config)#q
switch_a#
```

Creating an MSTI Instance

To create a MSTI instance and map it to a VLAN, use the following CLI commands:

CLI Command Mode: **MSTP Configuration Mode**

CLI Command Syntax: **bridge 1 instance <*1-15*> vlan <*vlan_ID*>**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#spanning-tree mst configuration
switch_a(config-mst)#bridge 1 instance 1 vlan 10
switch_a(config-mst)#q
switch_a(config)#q
switch_a#
```

Setting MSTI Priority

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **bridge 1 instance <*1-15*> priority <*0-61440*>**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#bridge 1 instance 1 priority 0
switch_a(config)#q
switch_a#
```

Modifying CIST Port Priority and Port Path Cost

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
bridge-group 1 path-cost <*1-200000000*>;
bridge-group 1 priority <*0-240*>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface ge1
switch_a(config-if)#bridge-group 1 path-cost 200000
switch_a(config-if)#bridge-group 1 priority 128
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

To modify the MSTI Port Priority and MSTI Port Path Cost for an Instance on a switch, use the below CLI commands:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
bridge-group 1 instance <*1-15*> path-cost <*1-200000000*>
bridge-group 1 instance <*1-15*> priority <*0-240*>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface ge1
switch_a(config-if)# bridge-group 1 instance 1 path-cost 20000
```

```
switch_a(config-if)# bridge-group 1 instance 1 priority 128
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Adding a Port to an MSTI Instance

To add a port to a MSTI instance (this port must be a member port of the VLAN that is mapped to the MSTI instance), use these CLI commands:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **bridge-group 1 instance <*1-15*>**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface ge1
switch_a(config-if)#bridge-group 1 instance 1
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

STP/RING PAGE - ALPHA RING

Alpha Ring Setting Page

To navigate to the **STP/Ring Alpha-Ring Settings** page:

1. Click on the **+** next to **STP/Ring**.
2. Click on **Alpha-Ring Setting.**

EtherWAN Alpha-Ring Technology

The Alpha-Ring protocol was designed and developed by EtherWAN to overcome traditional STP and RSTP's inability to provide fast network recovery and minimize packet loss caused by link failure. Among the advantages of Alpha-Ring are:

- **Flexibility for Network Deployment** – Coexistence with STP, RSTP and MSTP

- **Ring Coupling** – Smaller rings coupled together through a single switch to increase network efficiency

Implementing a Simple Alpha-Ring

1. Change the **Ring State** to **Enabled**
2. Click on the **Update Setting** button.

Next, the ports that will be used to connect this switch to the Alpha-Ring need to be assigned to provide the connection redundancy (see Figure 79).

1. Change **Ring Port 1** to the port you will be using for the first ring connection
2. Change **Ring Port 2** to the port you will be using for the second ring connection.
3. Click on the **Update Setting** button.
4. Save the configuration (see the Save Configuration Page)

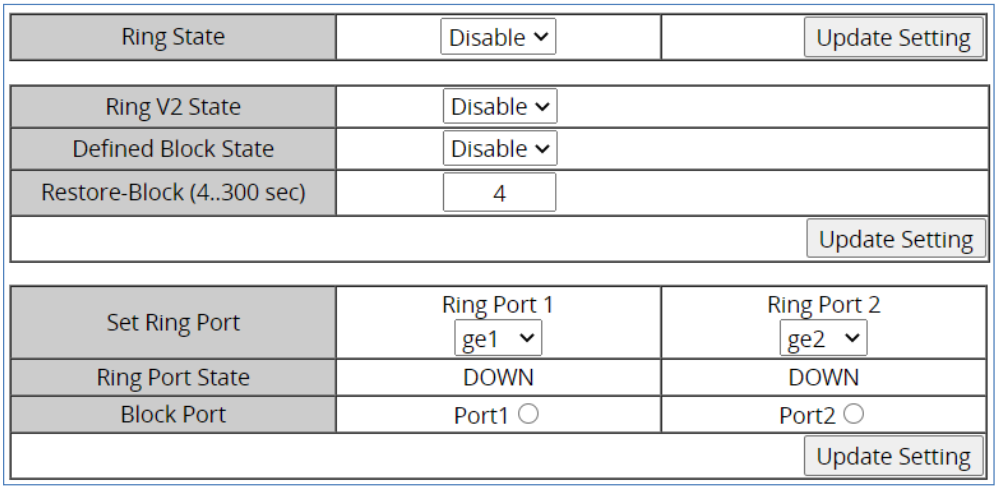


Figure 79: Alpha-Ring Settings

Alpha-Ring V2

The Alpha-ring protocol will automatically set the last connected link to BLOCK status. However, sometimes you may need to keep a specific link in a FOWARD state. An example would be where a port was connected to a high capacity fiber link – overall network performance would benefit by keeping that link running. Alpha-ring V2 allows you to manually define the port in the ring topology that will be set to BLOCK state. If a link in the ring fails, the pre-defined blocked port will be set to a forward state. When the failed link is restored, the pre-defined block port will return to a BLOCK state in the time defined by the **Restore-Block** variable.

To pre-define the block port (See Figure 85):

1. Set the Ring V2 State to **Enable**.
2. Set the **Defined Block State** to **Enable**.
3. Enter **Restore-Block** time in seconds**.**
4. Click **Update Setting**
5. Select the Ring port that you want to block by clicking the radio button underneath that port. Then click the corresponding **Update Setting** button.

The Alpha-Ring V2 protocol must be enabled on all switches in ring. However, the **Defined Block State** should only be enabled on the switch that has the port you want to set as blocked.

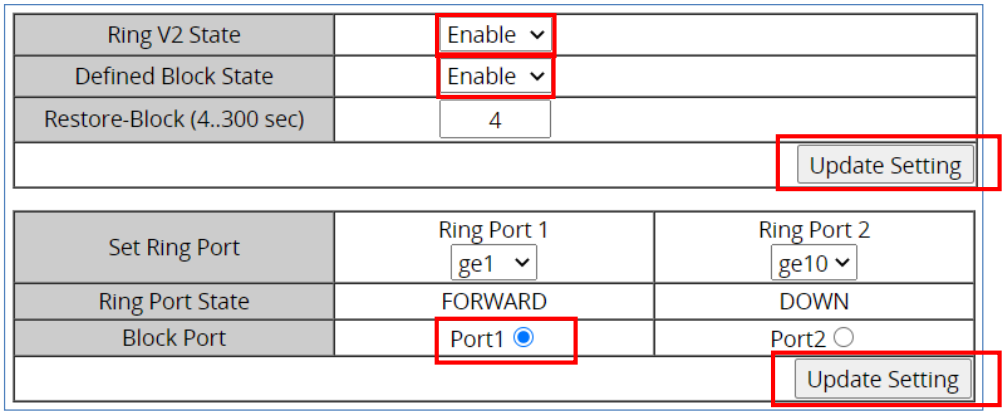


Figure 80: Pre-defining a Block Port with Alpha-Ring V2 Settings

Connecting two Alpha-Ring Networks together (Ring Coupling)

To navigate to the **STP/Ring Alpha-Ring Settings** page:

1. Click on the **+** next to **STP/Ring**.
2. Click on **Alpha-Ring Setting.**

As additional switches are added to a network, it may become necessary to connect multiple Alpha-Ring networks together. This is called **Ring-coupling** and uses two additional Ethernet ports on the switch. To setup Ring-coupling (see Figure 82):

1. Change the **Ring-coupling** state to **Enable.**
2. Click on the **Update Setting** button next to the Ring-coupling state.
3. Choose the desired port from the dropdown list under **Ring Coupling Port 1**
4. Choose the desired port from the dropdown list under **Ring Coupling Port 2**

5. Click on the **Update Setting** button.
6. Save the configuration (see the Save Configuration Page)

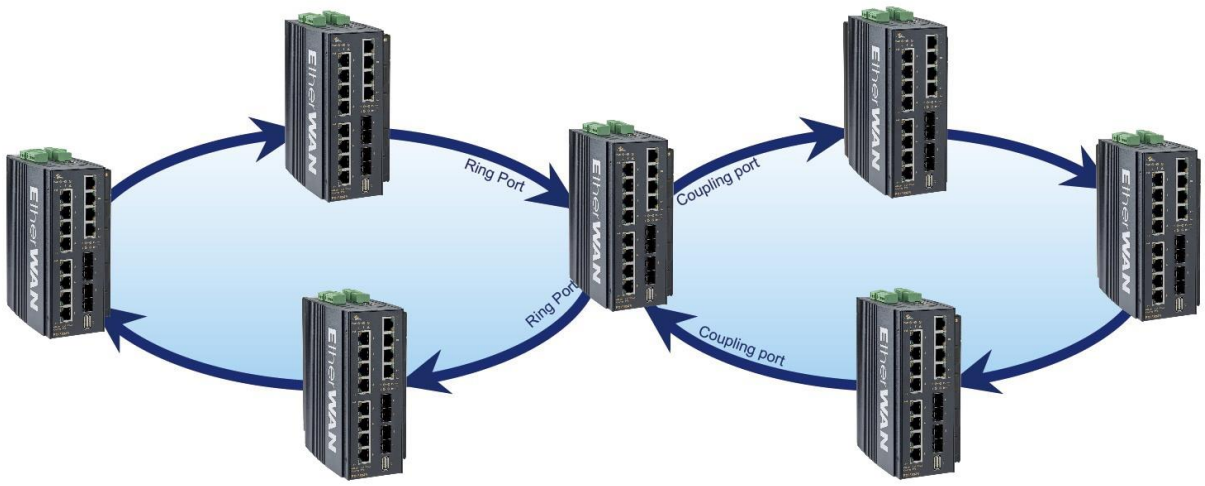


Figure 81: Ring Coupling Example

Ring Coupling State	Enable	Update Setting
Set Coupling Port	Coupling Port 1 ge3	Coupling Port 2 ge4
Port State	DOWN	DOWN
		Update Setting

Figure 82: Ring Coupling

Connecting Additional Rings (Redundancy Pairs)

Only two rings can be connected through Ring Coupling. To connect additional rings, you will need to use **Redundant Port Pairs**. Below are some topology examples for using redundancy pairs to connect two or more rings.

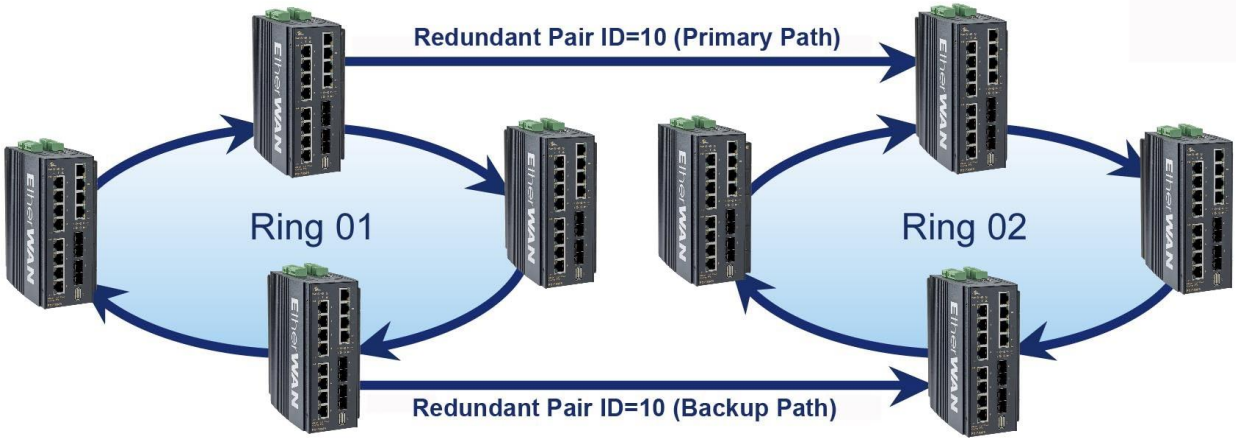


Figure 83: Redundant Pair Example 1

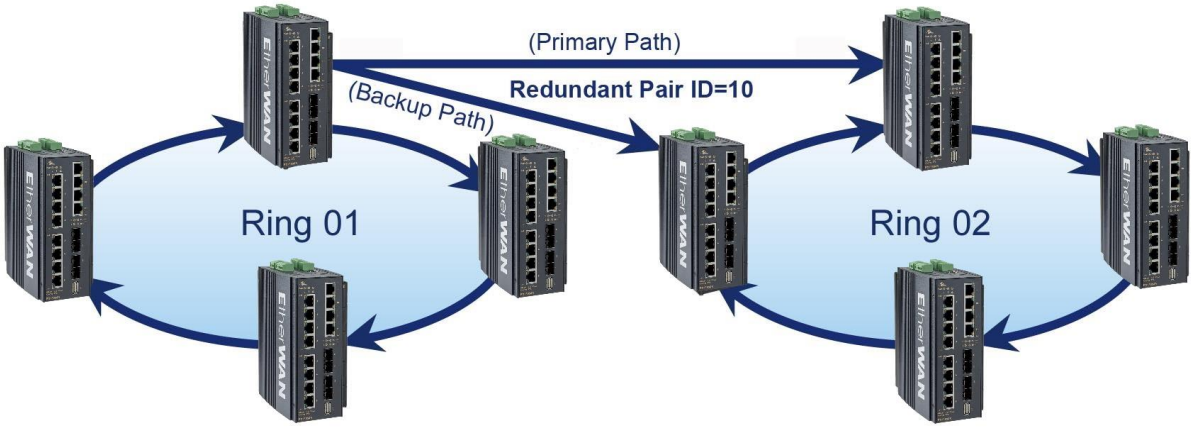


Figure 84: Redundant Pair Example 2

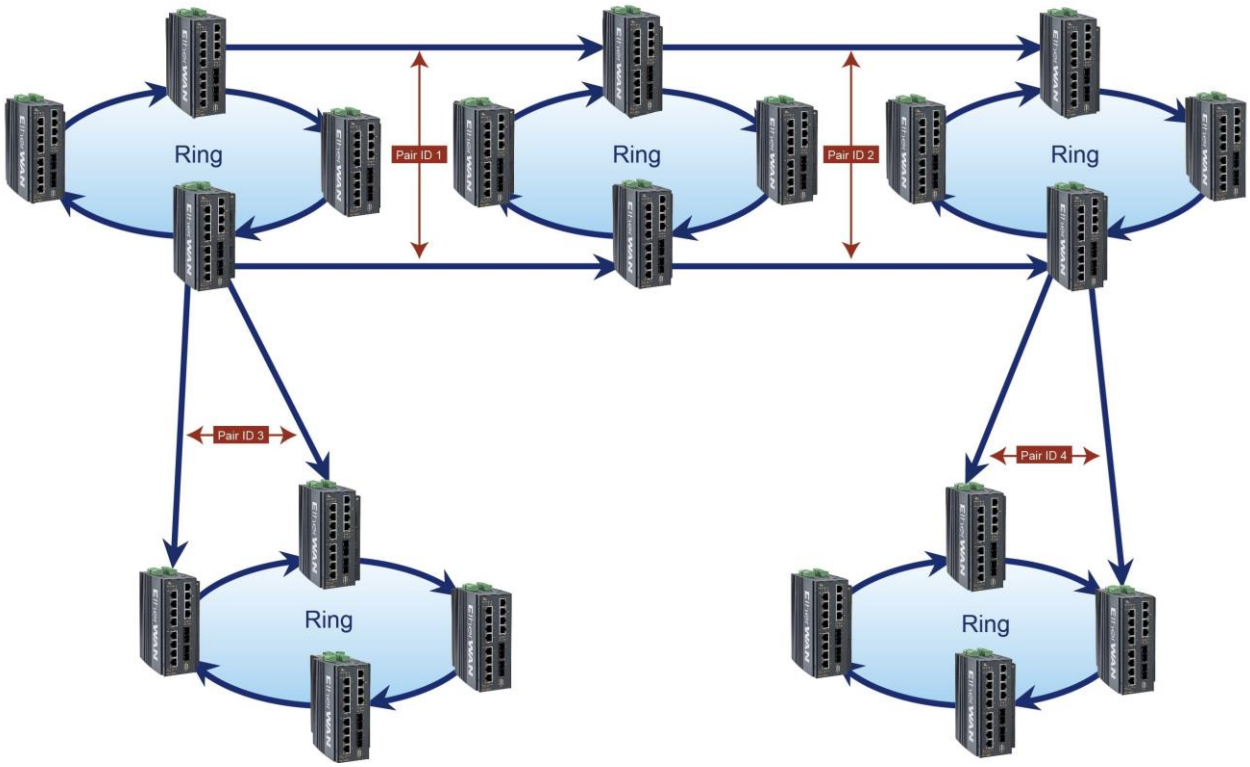


Figure 85 Redundant Pair Example 3

To setup Redundant Pairs:

1. Change the **Redundancy State** to **Enable.**
2. Click on the **Update Setting** button next to the Redundancy State
3. Select the port that will act as a Redundant Port and choose “Normal” or “Slave” with the radio buttons. (“Normal” means “Master” in this context.)
4. Choose a Pair ID for the port.
5. Click on the **Update Setting** button.

To delete an existing Redundant Port, select it by clicking the check box at the right and then clicking **Update Setting**.

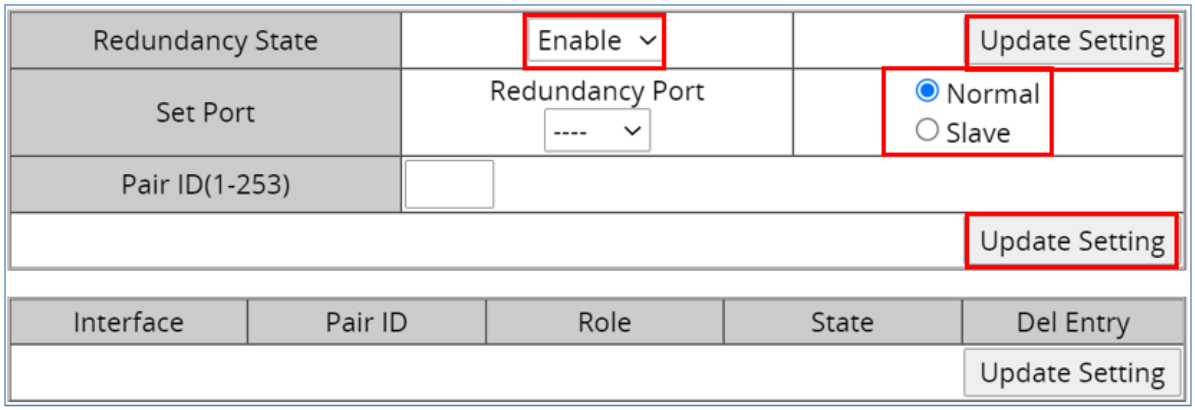


Figure 86: Redundancy Pairs Configuration

Configuring Alpha Ring using CLI commands

Enable Alpha Ring and Alpha Ring V2 Protocols

To enable the Alpha Ring and Alpha Ring V2 protocols, use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **bridge 1 ring enable/disable**

(no) ring v2 enable

Usage Example 1: Enabling alpha ring

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# bridge 1 ring enable
switch_a(config)#q
switch_a#
```

Usage Example 2: Enabling alpha V2 ring

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ring v2 enable
switch_a(config)#q
switch_a#
```

Set the Ring Ports

To configure the ports used in the ring, use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **ring set-port <interface1> <interface2>**

(**interface1** and **interface2** will be set as **ring-port 1** and **ring-port 2**)

Usage Example 1:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ring set-port ge2 ge3
switch_a(config)#q
switch_a#
```

Show Ring, Port and All States

There are three CLI commands for viewing Alpha Ring statuses:

CLI Command Mode: **Privileged Exec Mode**

CLI Commands: **show ring state** -- Shows ring service state as enable or disabled.

show ring port-state -- Shows whether ring ports are in BLOCK or FORWARD mode.

show ring all -- Shows all Alpha and Alpha Ring V2 information.

Usage Example 1:

```
switch_a>enable
switch_a#show ring state
switch_a(config)#
ring enable
switch_a(config)#show ring port-state
ring-port 1 ge2 BLOCK
ring-port 2 ge3 FORWARD
switch_a#show ring all
Ring protocol: Enable
Ring frame type V2: Enable
Ring Defined-Block state: Enable
Ring Restore-Block seconds: 4
Ring coupling protocol: Disable
Port                    Interface       Role                    State
-------------------------------------------------------------------
Ring port 1              ge2            defined-block          Block
Ring port 2              ge3                                  Forward
Coupling port 1          ge3                                  Forward
Coupling port 2          ge4                                     Down
```

Define a Ring's Blocked Port

To define a specific port to be set to BLOCK state, use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **ring set-defined-block <1-2>**

Usage Example 1:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ring set-defined-block 1
switch_a(config)#q
switch_a#
```

Set Delay Time for Restoration of a Failed Port

To set the delay in seconds for the restoration of a failed port, use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **ring restore-block <4-300>**

Enable Ring Coupling

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **(no) ring-coupling enable**

Usage Example 1:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ring-coupling enable
switch_a(config)#q
switch_a#
```

Set Ring Coupling Ports

To define the ports that will be used for ring coupling, use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **ring set-coupling-port <interface1> <interface2>**

Usage Example 1: Set ports ge7 and ge8 as coupling ports for connection to another ring

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ring set-coupling-port ge7 ge8
switch_a(config)#q
switch_a#
```

Enable Redundancy Pairs

To enable the ring to be coupled to another ring using redundant port pairs, use the following CLI commands:

CLI Command Mode: **Privileged Exec Mode**

CLI Command Syntax: **(no) redundancy pair enable**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# redundancy pair enable
switch_a(config)#q
switch_a#
```

Show Ring Coupling, Port Coupling, and Redundancy Pair States

To view the statuses of ring couplings and rings connected by redundancy pair, use the following CLI commands:

CLI Command Mode: **Privileged Exec Mode**

CLI Command Syntax: **show ring-coupling state**
show ring-coupling port-state
show redundancy pair

Usage Example 1:

```
switch_a>enable
switch_a# show ring-coupling state
ring-coupling enable
switch_a(config)# show ring-coupling port-state
ring-coupling-port 1 ge7 DOWN
ring-coupling-port 2 ge8 DOWN
```

```
switch_a(config)#q
switch_a#
```

STP/RING PAGE – ALPHA CHAIN

The Alpha Chain Protocol

Although the Spanning Tree Protocols are very versatile in forming all possible redundant topologies, its re-convergence time is too slow for most mission critical applications. The EtherWAN Alpha Ring protocols can be used in mission critical applications to recover from a link failure quickly. However, with the Alpha Ring protocols (Alpha Ring, Alpha Ring-Coupling), the redundant topologies that these protocols can be applied to will be limited to at the most two Rings per switch. Alpha Chain protocol can be used independently, or in conjunction with the Alpha Ring protocols, to form almost limitless redundant topologies, all with the recovering time from a link failure in less than a second. With the Alpha Chain protocol, a redundant network segment can be created anywhere that a single path of daisy-chained switches exists.

General Overview

To ensure that the Alpha Chain protocol will function properly on your network, please follow the minimum configuration guidelines listed below for the two types of Alpha Chain switches (Chain Port switch, Chain-pass-through switch).

There are two types of port configurations used in the Alpha Chain setup. The flexibility of Alpha Chain allows for many different types of topologies to be created.

- **Alpha Chain Port** – Alpha Chain Ports make up the Beginning and End of an Alpha Chain. Each Alpha Chain segment contains a Master and a Slave port. The Master and Slave ports can be on one switch or they can be on two different switches.
- **Chain Pass-Through Port** – Every port that is part of the chain that **is not** a Master or Slave **Alpha Chain** port must be configured as a Chain Pass-Through port.

Alpha Chain Settings

To navigate to the **STP/Ring Alpha-Chain Settings** page:

1. Click on the **+** next to **STP/Ring**.
2. Click on **Alpha-Chain Setting.**

Global Settings

To configure Alpha Chain use the instructions below:

1. **VLAN (91-4096, default: 1) -** In the text entry, enter the VLAN number of a VLAN that is supported on all the switches in the Alpha Chain segment (see Figure 87).
2. **Priority (0-255, default:128) -** The Chain Port switch(es) at the ends of an Alpha Chain segment will automatically determine which Chain Port switch should be forwarding and which should be blocking. However, if you should have a preference as to which Chain Port switch should be forwarding on the Alpha Chain segment, then you can enter a priority number in the range of **0-255**, in the entry field, to control if the local switch will be forwarding or blocking.
    a. Enter a number that is lower than the partner Chain Port switch's Priority setting, if you want the local switch to be the forwarding Chain Port switch.
    b. Enter a number that is higher than the partner Chain Port switch's Priority setting, if you want the partner Chain Port switch to be the forwarding switch.
3. **Timeout Count (3-255, default:5) -** Enter the number PDUs (protocol data units) that a Chain Port is allowed to miss into the entry field.
    a. The Alpha Chain protocol works by sending PDUs between two Chain Ports to determine the forwarding and blocking status of each the two Chain Ports at the end points of an Alpha Chain Segment. One PDU is sent every 200 milliseconds. You can configure the number PDUs that a Chain Port can miss, before the port determines a link failure has occurred.
4. **Storm Control (broadcast and multicast) -** Choose **Disable** or **Enable** from the dropdown list.

    Warning: When this option is enabled, all the ports on the switch will have the Storm Control feature automatically enabled.
5. Click on the **Submit** button to load the changes into the running configuration.

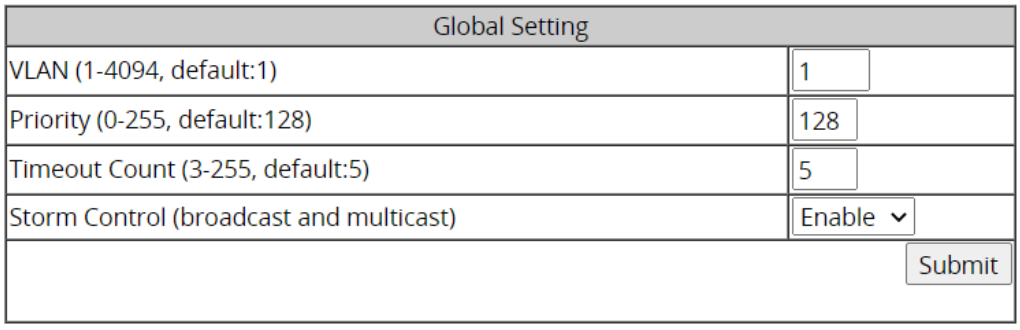
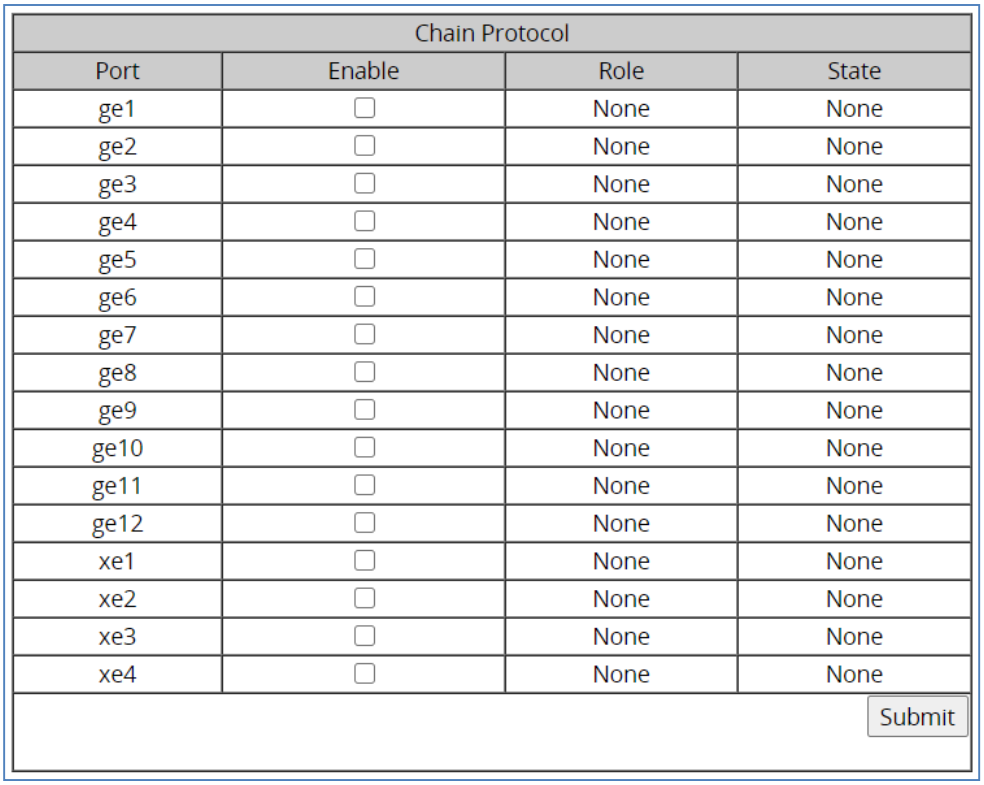


Figure 87: Alpha Chain Setting

Configuring the Alpha Chain Ports

1. Check the check box next to the port number of the ports that you want to be configured as a Chain Port (see Figure 88).
2. Click on the **Submit** button to load the changes into the running configuration.



Chain Protocol			
Port	Enable	Role	State
ge1	☐	None	None
ge2	☐	None	None
ge3	☐	None	None
ge4	☐	None	None
ge5	☐	None	None
ge6	☐	None	None
ge7	☐	None	None
ge8	☐	None	None
ge9	☐	None	None
ge10	☐	None	None
ge11	☐	None	None
ge12	☐	None	None
xe1	☐	None	None
xe2	☐	None	None
xe3	☐	None	None
xe4	☐	None	None
			Submit

Figure 88: Chain Ports – Master and Slave on One Switch

Alpha Chain Pass-Through Ports

To navigate to the **Chain Pass-Through Setting** page:

1. Click on the **+** next to **STP/Ring**.
2. Click on **Chain Pass-Through Setting.**

To configure the Alpha Chain Pass-Through ports:

1. From the drop-down list below the **Chain Pass-Through Port 1** heading, choose one of the daisy chained ports on the switch to be the Chain Pass-Through Port #1 for the switch.

2. Next, from the drop-down list below the **Chain Pass-Through Port 2** heading choose the remaining daisy chained port on the switch to be the Chain Pass-Through Port #2 for the switch.
3. To change the port number for either of the Chain pass-through ports on the switch, you must first click on the **Disable** button to clear the settings for both Chain Pass-Through ports. Repeat the previous steps to set the new port numbers to be Chain Pass-Through.
4. Click on the **Submit** button to load the changes into the running configuration.

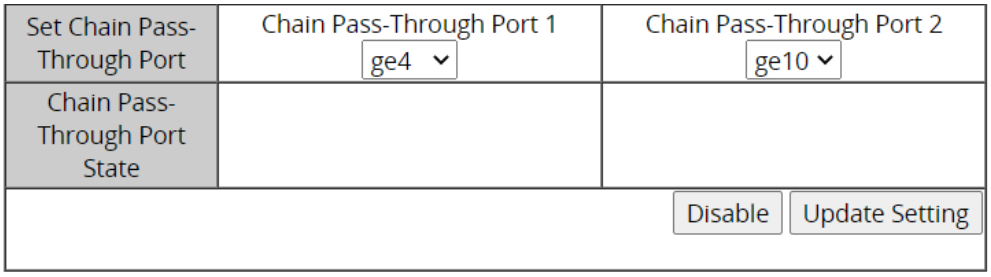


Figure 89: Chain Pass-through Ports

Configuring Alpha Chain using CLI commands

Storm Control

To disable the automatic enabling of Storm Control feature on all the ports, use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **no bridge 1 chain-storm**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# no bridge 1 chain-storm
switch_a(config)#q
switch_a#
```

Configuring Chain Ports

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
chain port enable
no chain port

Usage Example 1: Enabling a chain port

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#in ge6
switch_a(config-if)#chain port enable
switch_a(config-if)#q
switch_a(config)#q
```

Usage Example 2: Disabling a chain port

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#in ge6
switch_a(config-if)#no chain port
switch_a(config-if)#q
switch_a(config)#q
```

Configuring Chain Pass-Through Ports

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
chain pass-through <*port #1 port #2*>
no chain pass-through

Usage Example 1: Enabling chain pass-through

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# chain pass-through ge3 ge4
switch_a(config)#q
switch_a#
```

Usage Example 2: Disabling chain port pass-through

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# no chain pass-through
switch_a(config)#q
switch_a#
```

STP/RING PAGE - ADVANCED SETTING

To navigate to the **STP/Ring Advanced Setting** page:

1. Click on the **+** next to **STP/Ring**.
2. Click on **Advanced Setting.**

Advanced Bridge Configuration

The Advanced Setting Page contain several settings to determine how the switch will handle BPDU packets.

- **Bridge bpdu-guard configuration -** When the BPDU Guard feature is set for a bridge, all portfast-enabled ports of the bridge that have **bpdu-guard** set to default shut down the port on receiving a BPDU. In this case, the BPDU is not processed.
- **Error disable timeout configuration –** Enabling this allows a Disabled port to re-enable itself automatically after the specified Interval.
- **Interval –** Default is 300 seconds. This is the length of time a port will remain disabled after shutting down due to the **bpdu-guard**.

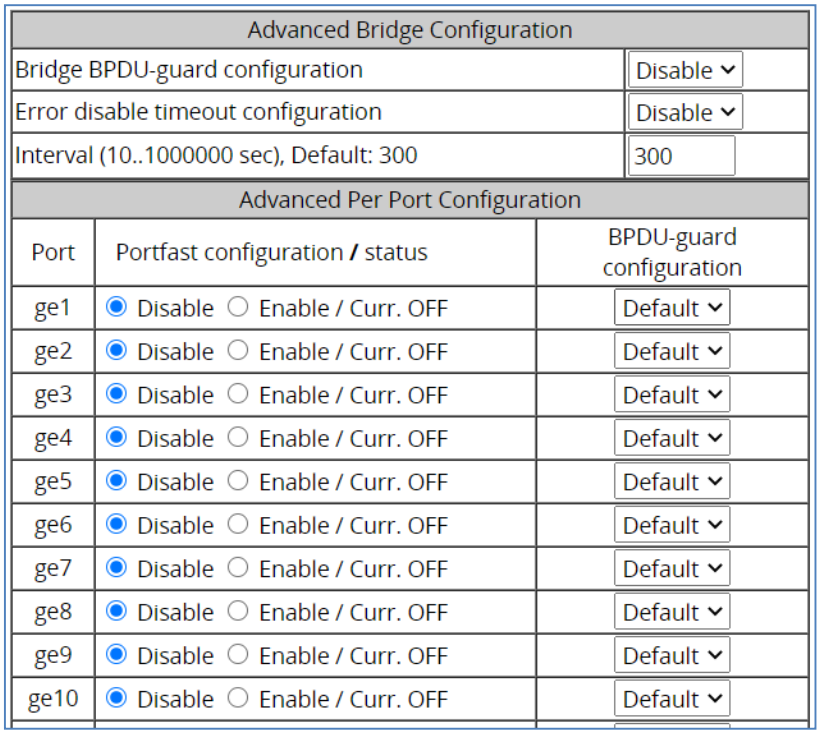


Figure 90: Advanced Bridge Configuration

Advanced Per Port Configuration

- **Portfast Configuration / status –** Enabling this for Edge ports (ports connecting to an end device as opposed to another switch) allows the port to enter the forwarding state immediately, bypassing the listening and learning states to achieve -

    1. Reduced Delay: By avoiding the listening and learning states, PortFast minimizes the time it takes for devices to come online. This is especially important for applications like DHCP, DNS, and boot services.

    2. Avoiding Network Loops: Although PortFast is safe for end stations, it's essential to avoid enabling it on ports connected to other Layer 2 devices (e.g., switches) to prevent network loops.

- **BPDU-Guard Configuration –** When set to **Default** the port will default to the Advanced Bridge Configuration settings. **Enable** or **Disable** to override the Bridge BPDU-Guard

Note: Do not use PortFast on switch ports that are connected to other switches, hubs, or routers. These wires can cause physical loops, and in these cases the spanning tree must complete a complete initialization process. Spanning tree directory loops may cause network

outages. If PortFast is turned on for a port that is part of a physical loop, there may be a window of time during which packets are continuously forwarded (perhaps even doubled) to the point where the network cannot recover.

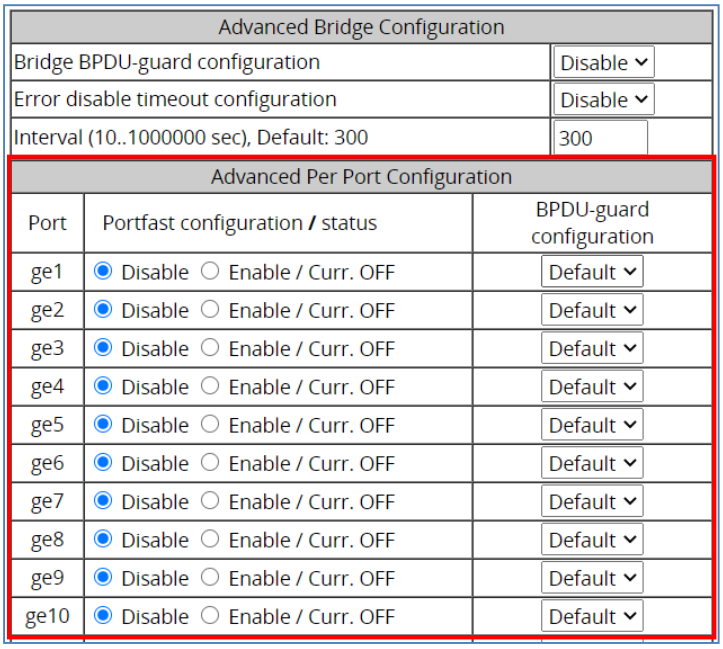


Figure 91: Advanced Per Port Configuration

Configuring Spanning Tree Advanced Settings using CLI commands

Enabling BPDU Guard Globally

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **bridge 1 spanning-tree portfast bpdu-guard**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# bridge 1 spanning-tree portfast bpdu-guard
switch_a(config)#q
switch_a#
```

Enabling BPDU Guard on a Port

To enable the BPDU Guard feature on an **individual** switch port, use the CLI commands below:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
spanning-tree portfast;
spanning-tree portfast bpdu-guard enable

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface ge1
switch_a(config-if)#spanning-tree portfast
switch_a(config-if)#spanning-tree portfast bpdu-guard enable
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Enabling BPDU Guard Error Disable-timeout

To enable the BPDU Guard Error Disable-timeout feature on a switch port, and set the timeout interval, use the CLI commands below:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
bridge 1 spanning-tree errdisable-timeout enable
bridge 1 spanning-tree errdisable-timeout interval 300

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#bridge 1 spanning-tree errdisable-timeout enable
switch_a(config)#bridge 1 spanning-tree errdisable-timeout interval 300
switch_a(config)#q
switch_a#
```

Enabling the Loop Guard Feature

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **spanning-tree guard loop**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface ge1
switch_a(config-if)# spanning-tree guard loop
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

VLAN

Configuring VLANs

Add and delete VLANs

To navigate to the **VLAN Setting** page:

1. Click on the **+** next to **VLAN**.
2. Click on **VLAN Setting.**

Add and delete VLANs from this screen.

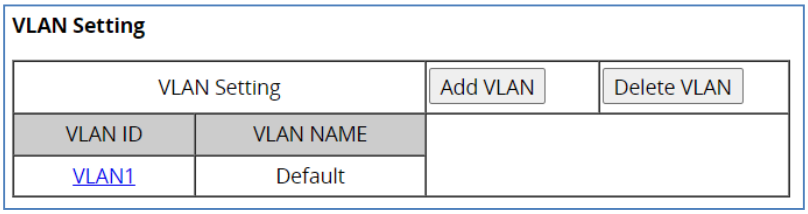


Figure 92: VLAN Setting

Clicking the Add VLAN button takes you to the screen shown below. Assign a VLAN number and name and select **Attach** or **Detach** to the CPU port. Select which ports are to be members of the VLAN and choose **tagged** or **untagged** for each port. Then click **Submit**.

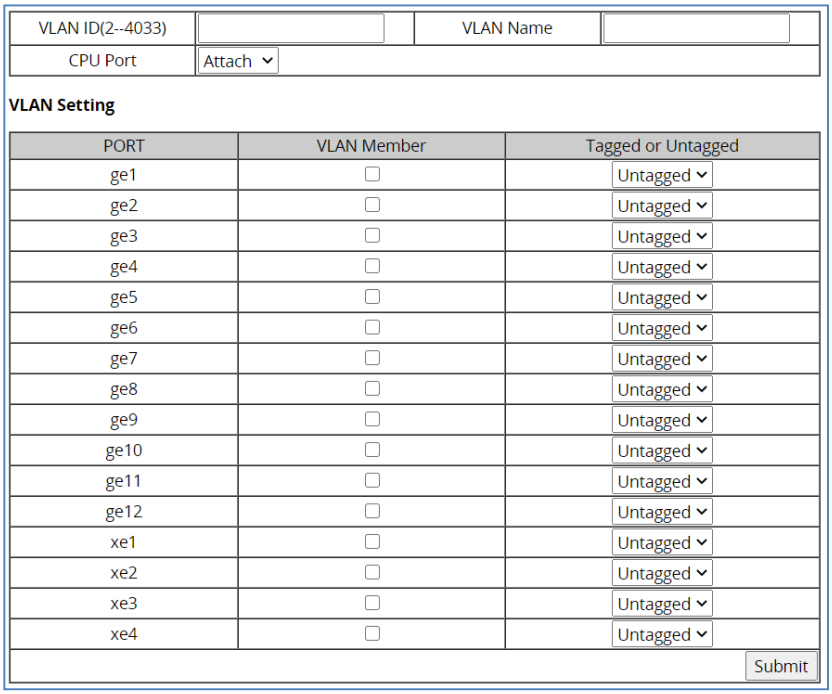


Figure 93: Add VLAN

Port Setting

All ports on the switch can be configured with different Port Types that have different tagging restrictions as defined below.

- **Access Port** - If a port is configured to be an Access Port, then this port can only be a member of a single VLAN based on the Access Port's **PVID VLAN** setting, and this port's outgoing packets cannot be modified to contain a VLAN Tag.
- **Trunk Port** - If a port is configured to be a Trunk Port, then this port can be a member of multiple VLANs. This port's outgoing packets will be automatically modified to contain a VLAN tag of the VLAN that the packet belongs to, with the exception of the PVID VLAN on that port. The PVID VLAN on a Trunk Port will not be automatically modified to contain a VLAN tag of the PVID VLAN.
- **Hybrid Port** - A Hybrid Port has no restriction on it. If a port is configured to be a Hybrid Port, then this port can be a member of multiple VLANs, and this port's outgoing packets can be configured to be either with or without a VLAN tag of the VLAN that the packet belongs to, including the PVID VLAN of the Hybrid Port.

For all three types of ports above, if an incoming packet contains a VLAN tag, then the packet's VLAN association rule will be based on the VLAN Tag.

To configure the proper port type and the PVID setting for each switch port:

1. Choose the port type for each port in the drop-down list.
2. Enter the **PVID VLAN** for each port (see below).
3. Enter the **Priority Level** (optional).
4. Click on the **Update Setting** button.
5. Save the configuration (see the Save Configuration Page)

 **Warning:** Modifying the Port Type using the Web GUI will cause that switch port to lose all its current VLAN membership and become a member port for the PVID VLAN only. You will lose your current connection to the switch, should you choose to modify the PVID of the port that connects your Computer to the switch.

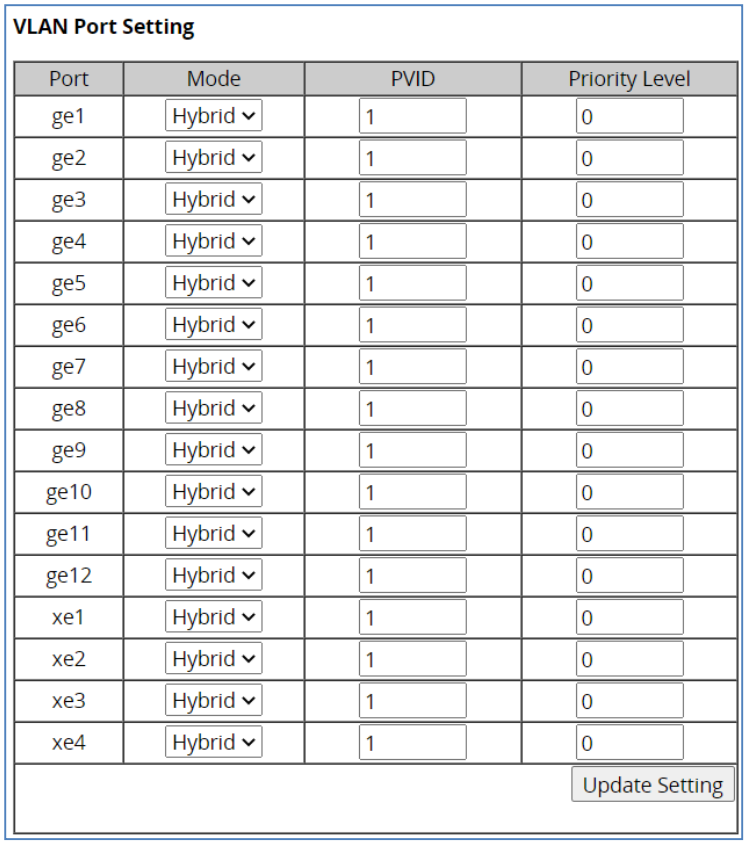


Figure 94: Port Setting

Tag Based VLAN Configuration Using CLI Commands

Configuring a 802.1Q VLAN

To configure an 802.1Q VLAN on a switch use the following CLI commands:

CLI Command Mode: **VLAN Database Configuration Mode**

CLI Command Syntax: **vlan NUMBER bridge 1 name NAME state enable**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#vlan database
switch_a(config-vlan)#vlan 100 bridge 1 name Management state enable
switch_a(config-vlan)#vlan 200 bridge 1 name Accounting state enable
switch_a(config-vlan)#vlan 300 bridge 1 name Sales state enable
```

```
switch_a(config-vlan)#q
switch_a(config)#q
switch_a#
```

Configuring an IP Address for a Management VLAN

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **ip address IP_ADDRESS/PREFIX [e.g. 10.0.0.1/24]**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface vlan1.100
switch_a(config-if)#ip address 192.168.100.10/24
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Removing an IP Address from a Management VLAN

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **no ip address**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface vlan1.100
switch_a(config-if)#no ip address
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Configuring an Access Port

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **switchport mode access**

CLI Command Syntax: **switchport access vlan <1 – 4094>**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface ge1
switch_a(config-if)#switchport mode access
switch_a(config-if)#switchport access vlan 100
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Configuring a Trunk Port

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **switchport mode trunk**

CLI Command Syntax: **switchport trunk allowed vlan [add | all | except | none | remove] VLAN_ID**

CLI Command Syntax: **switchport trunk native vlan <1-4033>**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface ge7
switch_a(config-if)#switchport mode trunk
switch_a(config-if)#switchport trunk allowed vlan add 100,200,300
switch_a(config-if)#switchport trunk native vlan 1
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Add an IP to the Management VLAN

To navigate to the **System/IP Address** page:

1. Click on the **+** next to **System**.
2. Click on **IP Address.**

To add an IP for a Management VLAN:

1. Enter the **IP address** and **subnet mask** for the management VLAN
2. Click on the **Submit** button (see Figure 100).
3. Save the configuration (see the Save Configuration Page)

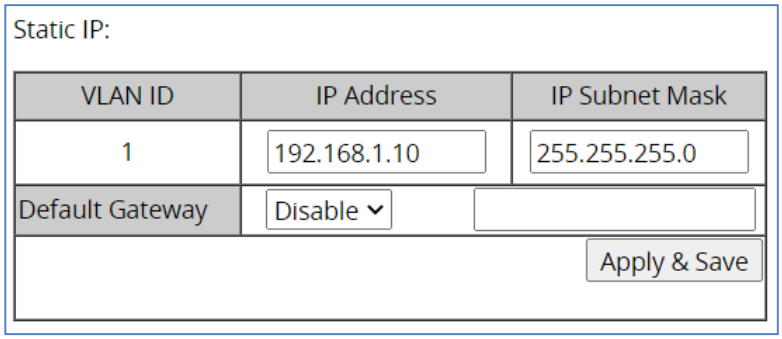


Figure 95: Management VLAN IP Address

To delete an IP from a VLAN (the default VLAN, for an example):

1. Delete the IP and the subnet mask of the default VLAN and leave it as blank
2. Click on the **Submit** button.

Warning: Before completing the steps above, make sure that you have already set up another management IP on another VLAN, and have set up a port properly for accessing that VLAN.

QOS

QoS (Quality of Service) refers to several related aspects of computer networks that allow the transport of traffic with special requirements. In particular, technology has been developed to allow computer networks to become as useful as telephone networks for audio conversations, as well as supporting new applications with even stricter service demands. Beyond the audio applications that QoS was originally intended, data traffic such as video or real-time information can benefit from QoS.

QoS as it pertains to the switch can be broken down into two types, CoS and DCSP. CoS or **Class of Service** operates at Layer 2 and was developed by an IEEE working group in the 1990s. CoS uses a 3-bit field called the **Priority Code Point** (PCP) within an Ethernet frame header when using VLAN tagged frames as defined by IEEE 802.1Q. It specifies a priority value between 0 and 7, inclusive that can be used by QoS disciplines to differentiate

traffic. Although this technique is commonly referred to as IEEE 802.1p, there is no standard or amendment by that name published by the IEEE. Rather the technique is incorporated into the IEEE 802.1Q standard which specifies the tag inserted into an Ethernet frame.

Eight different classes of service are available as expressed through the 3-bit PCP field in an IEEE 802.1Q header added to the frame. The way traffic is treated when assigned to any particular class is undefined and left to the implementation. The IEEE however has made some broad recommendations:

PCP	Priority	Acronym	Traffic Types
1	0 (lowest)	BK	Background
1	1	BE	Best Effort
2	2	EE	Excellent Effort
3	3	CA	Critical Applications
4	4	VI	Video, < 100 ms latency and jitter
5	5	VO	Voice, < 10 ms latency and jitter
6	6	IC	Internetwork Control
7	7 (highest)	NC	Network Control

Figure 96: 802.1p Priority submenu

The above recommendations are implemented in the **802.1p Priority** submenu.

DSPC or **Diffserv Code Point** uses the first 6 bits in the ToS field of the IP(v4) packet header. This type of QoS is primarily useful if the QoS needs to pass through a router or routers. We will touch on DSPC briefly later in this section.

Global Configuration Page

Web GUI Interface

To navigate to the **QoS Global Configuration** page (see Figure 102):

1. Click on the **+** next to **QoS**.
2. Click on **Global Configuration**.

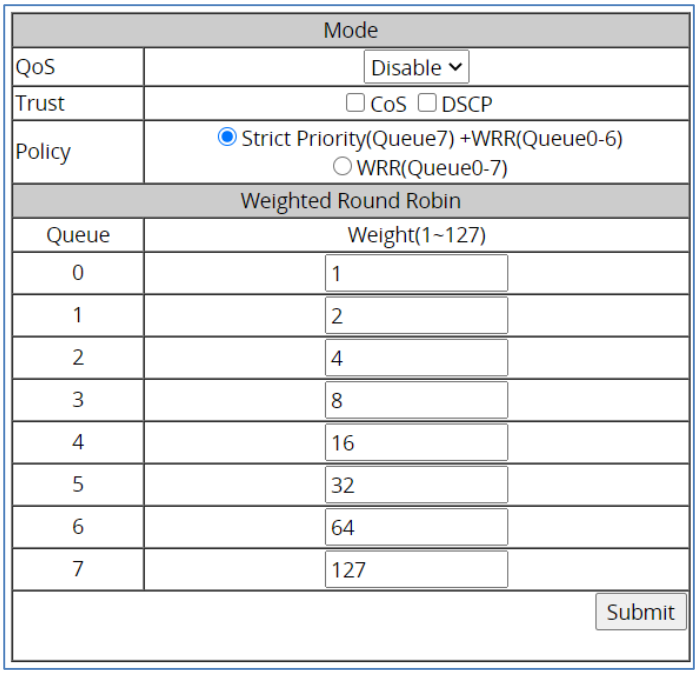


Figure 97: QoS Global Configuration

To Enable the QoS settings:

1. Enable QoS, by selecting the drop-down box to the right of the QoS option.
2. Choose CoS and/or DSCP next to the Trust option.
3. Select the desired option next to Policy:
    a. **Strict Priority (Queue0-3)** – **Note:** Not all switches support this mode. Packets must be emptied from the queues in order. Starting with queue 3 and ending with queue 0, the packets in each queue must be completely emptied before the next queue's packets are considered for transmission.
    b. **Strict Priority (Queue3) +WRR(Queue0-2)** – Packets must be emptied from queue 3 first and the three remaining queues are emptied according the WRR weights in the Weighted Round Robin section (see below).
    c. **WRR (Queue 0 – 3)** – each queue is allowed to discharge a certain number of packets (according to the WRR weights in the Weighted Round Robin section) before moving to the next queue.
4. Enter the **Weight** for each queue in the Weight Round Robin section
5. Click on the **Submit** button.
6. Save the configuration (see the Save Configuration Page)

Note: Weighted Round Robin – There are four text fields, one for each queue (0 – 3). A number from 1 to 20 can be assigned for each queue. This number is used with **WRR** policy and is the value of the number of packets that must be emptied from the queue before the next queue is considered.

By default, these values are:

Queue	Weight
0	1
1	2
2	4
3	8

Figure 102: Weight of Queue

QoS Global Configuration using the CLI Interface

This section gives information on Command line commands related to QoS and assumes the user has a working knowledge of connecting to the switch using Telnet, SSH or the Serial port. Telnet is enabled by default. To enable or disable Telnet or SSH see the Management Interface section.

Enabling/Disabling QoS

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
mls qos enable
no mls qos

Usage Example – Enabling QoS:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#int ge1
switch_a(config-if)# mls qos enable
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Usage Example – Disabling QoS:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#int ge1
switch_a(config-if)# no mls qos
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Enable/Disable QoS Trust

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
mls qos trust <*cos/dscp*>
no qos trust

Usage Example – Enable QoS Trust:

```
switch_a>enable
switch_a#configure terminal
```

```
switch_a(config)# mls qos trust cos
switch_a(config)#q
switch_a#
```

Usage Example – Disable QoS Trust:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# no mls qos trust
switch_a(config)#q
switch_a#
```

Configuring the Egress Expedite Queue

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
priority-queue strict
priority-queue out
no priority-queue out
mls qos <*WRR_WTS*> (4 values separated by spaces. Range is 1-20 (See the Usage Example).

Usage Example – Enable QoS Strict Priority (Queue 0-3):

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# priority-queue strict
switch_a(config)#q
switch_a#
```

Usage Example – Enable QoS Strict Priority (Queue 3) + WWR (Queue 0-2):

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# priority-queue out
switch_a(config)#q
switch_a#
```

Usage Example – Disable QoS Strict Priority:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# no priority-queue out
switch_a(config)#q
switch_a#
```

Usage Example – The following example specifies the bandwidth ratios of the four transmit queues, starting with queue 0, on the switch. WRR_WTS Weighted Round Robin (WRR) weights for the 4 queues (4 values separated by spaces). Range is 1-20.

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#mls qos 1 2 4 8
switch_a(config)#q
switch_a#
```

802.1p Priority Page

Web GUI Interface

To navigate to the **QoS 802.1p Priority** page (see Figure 98):

1. Click on the **+** next to **QoS**.
2. Click on **802.1p Priority**.

The 802.1p Priority page allows a user to assign the queues to VLAN priorities (see Global Configuration Page for more information on queues).

Each VLAN priority is expressed as the three-bit PCP field in the 802.1Q header discussed previously. The values shown above are the default values with the higher VLAN priorities corresponding to the higher priority queues.

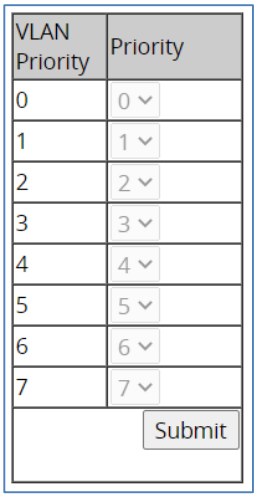


Figure 98: 802.1p Priority

Note: Remember to enable QOS in Global Configuration section in order to configure the priority.

By default, the higher priority queue 3 are assigned to VLAN priorities 6 and 7, queue 2 assigned to VLAN priorities 4 and 5; queue 1 assigned to VLAN priorities 2 and 3; and finally, queue 0 assigned to VLAN priorities 0 and 1.

After making any changes on the page, click on the **Submit** button to ensure that the changes are stored.

802.1p Priority Submenu – CLI Interface

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
wrr-queue cos-map <*QUEUE_ID*> <*COS_VALUE*>

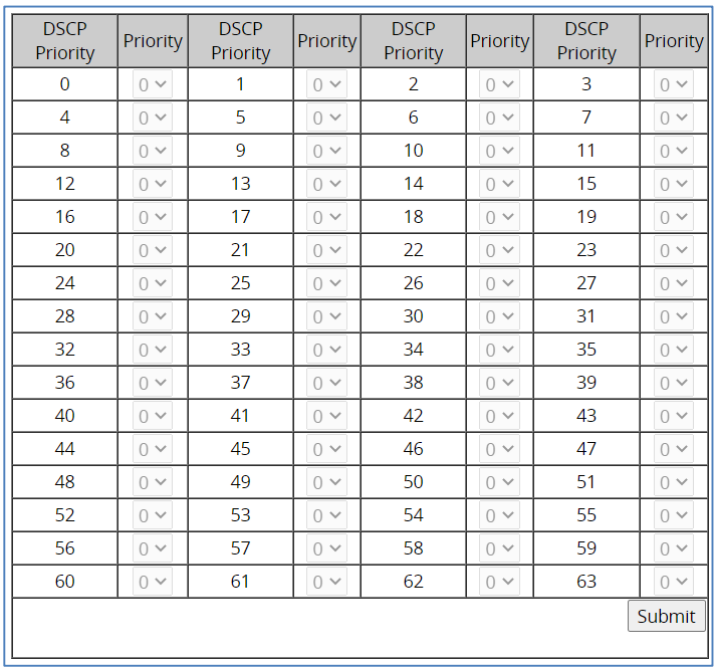
Queue ID. Range is 0-3.
COS_VALUE CoS values. Up to 8 values (separated by spaces).

Usage Example The following example shows mapping CoS values 0 and 1 to queue 1 on the switch:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#wrr-queue cos-map 1 0 1
switch_a(config)#q
switch_a#
```

DSCP Page – HTTP Interface

The DSCP submenu is much like the 802.1p submenu except there are many more DSCP priorities to choose from and they are all assigned to the lowest-priority queue, 0. For each DSCP priority, the user can change the value of the queue to between 0 and 3. See Figure 3 for more information:



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

Submit

Figure 99: DSCP

Note: Remember to enable QOS in Global Configuration section in order to configure the priority.

After changing any values on this page, click on the **Submit** button to allow them to take effect.

DSCP Submenu – CLI Interface

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
mls qos map dscp-queue <dscp_value> to <queue_ID>
dscp_value: Up to 8 values (separated by spaces). Range is 0-63.
queue_ID: Range is 0-3.

Usage Example The following example shows mapping DSCP values 0 to 3 to queue 1 on the switch:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# mls qos map dscp-queue 0 1 2 3 to 1
switch_a(config)#q
switch_a#
```

QoS Interface Commands – CLI Interface

To assign a VLAN Priority to an Interface:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **user-priority <*0-7*>**

Usage Example The following example shows mapping DSCP values 0 to 3 to queue 1 on the switch:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface ge1
switch_a(config-if) user-priority 4
switch_a(config-if)#q
switch_a(config)#
```

ACL Information

To navigate to the **ACL Information** page:

1. Click on the **+** next to **QoS**.
2. Click on **ACL Information**.

This page shows the ACL information for the selected interface.

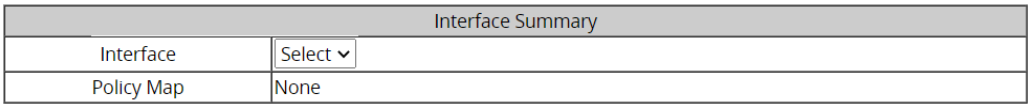


Figure 100: ACL Interface

ACL Configuration

To navigate to the **ACL Configuration** page:

1. Click on the **+** next to **QoS**.
2. Click on **ACL Configuration**.

QoS must be enabled globally before a policy map can be created. Enter a policy map name and a class name, then the information and burst rates. Then create the IP access list below and click **submit**.

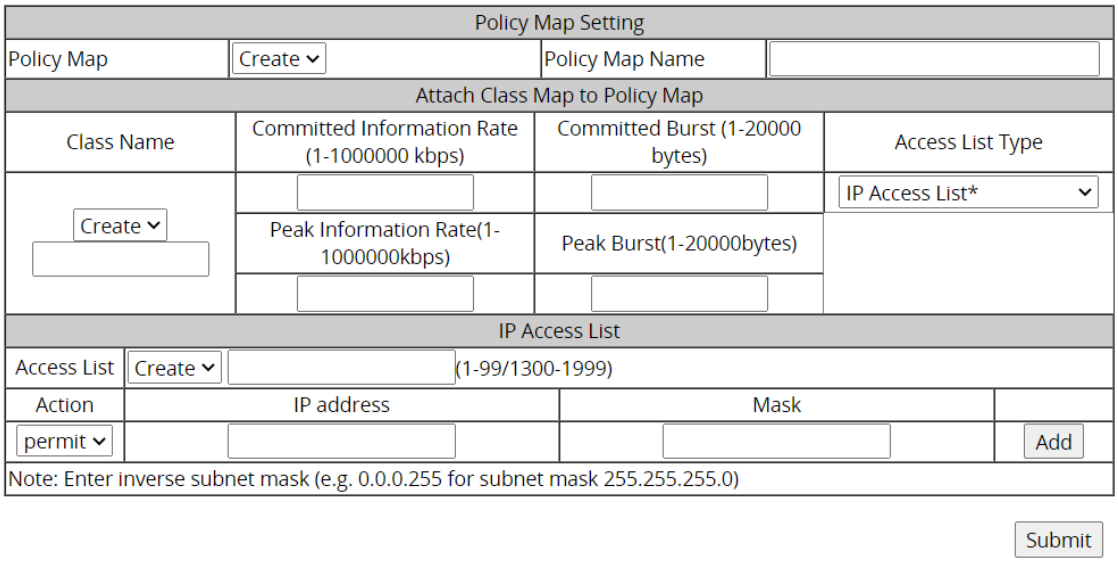


Figure 101: ACL setting page

ACL Configuration Using CLI Commands

Creating a Standard IP Access List

To create a new Standard IP Access List to allow or deny an IP address/range access to the switch, use the following CLI commands with the Access list ID in the range from 1 – 99, or from 1300 – 1999:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
ip-access-list *<1-99, 1300-1999>* permit *<source IP> <source bit mask>*
ip-access-list *<1-99, 1300-1999>* deny *<source IP> <source bit mask>*
ip-access-list *<1-99, 1300-1999>* deny any

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ip-access-list 1 permit 192.168.1.224 0.0.0.31
switch_a(config)# ip-access-list 1 deny 192.168.1.224 0.0.0.31
switch_a(config)# ip-access-list 1 deny any
switch_a(config)#q
switch_a#
```

Creating an Extended IP Access List

To create a new Extended IP Access List to allow or deny an source IP address/range and destination IP address/range pair access to the switch, use the following CLI commands with the Access list ID in the range from 100 – 199, or from 2000 – 2699:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
ip-access-list *<100-199, 2000-2699>* permit ip *<source IP> <source bit mask> <destination IP> <destination bit mask>*
ip-access-list *<100-199, 2000-2699>* deny ip *<source IP> <source bit mask> <destination IP> <destination bit mask>*
ip-access-list *<100-199, 2000-2699>* deny ip any any

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#ip-access-list 100 permit ip 192.168.1.224 0.0.0.31
192.168.1.224 0.0.0.31
switch_a(config)#ip-access-list 100 deny ip 192.168.1.224 0.0.0.31
```

```
192.168.1.224 0.0.0.31
switch_a(config)#ip-access-list 100 deny ip any any
switch_a(config)#q
switch_a#
```

Creating a MAC Access List

To create a new MAC Access List to allow or deny a source and destination Ethernet address pair access to the switch, use the CLI commands below with the Access list ID in the range from 100 – 199, or from 2000 – 2699.:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
mac-access-list *<2000-2699>* permit *<source MAC address> <source bit mask> <destination MAC address> <destination bit mask> <encapsulation format: 1=Ethernet II, 2=SNAP, 4=802.3, 8=LLC>* ether-type *<EtherType> < EtherType bit mask>*
mac-access-list *<2000-2699>* deny *<source MAC address> <source bit mask> <destination MAC address> <destination bit mask> <encapsulation format: 1=Ethernet II, 2=SNAP, 4=802.3, 8=LLC>* ether-type *<EtherType> < EtherType bit mask>*
mac-access-list *<2000-2699>* deny any *any <encapsulation format: 1=Ethernet II, 2=SNAP, 4=802.3, 8=LLC>* ether-type *<EtherType> < EtherType bit mask>*

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#mac-access-list 2000 permit 00e0.b321.03de
0000.0000.0000 00e0.b321.03df 0000.0000.0000 1 ether-type 800 0000
switch_a(config)#mac-access-list 2000 deny 00e0.b321.03de
0000.0000.0000 00e0.b321.03df 0000.0000.0000 1 ether-type 800 0000
switch_a(config)#mac-access-list 2000 deny any any 1 ether-type 800
0000
switch_a(config)#q
switch_a#
```

Creating an ACL Class Map with Layer 4 Access List

In order to create a Layer 4 Access List you must create it within an ACL Class Map. Use the CLI commands below to create an ACL Class Map together with the Layer 4 Access List. The Layer 4 Access List only classifies the ingress packets for the ACL Policy Map that it is

associated with; therefore, all packets will be allowed entry to the switch with the Layer 4 Access List. You will have to use this Access List in conjunction with another type of Access List, if you wish to filter any packet that did not match the classification rules from this Access List.

Note: The bandwidth policing capabilities of the ACL Class cannot be configured here; it can only be configured during the ACL Policy Map creation or modification:

CLI Command Mode:
Global Configuration Mode
Class Map Configuration Mode

CLI Command Syntax:
class-map <*Class Map Name*>
match layer4 source-port <*TCP/UDP Port number*>
match layer4 destination-port <*TCP/UDP Port number*>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#class-map FTP
switch_a(config-cmap)#match layer4 destination-port 21
switch_a(config-cmap)#q
switch_a(config)#
switch_a(config)#class-map FTP_Download
switch_a(config-cmap)#match layer4 source-port 20
switch_a(config-cmap)#q
switch_a(config)#q
switch_a#
```

Creating a ACL Class Map with an IP or MAC Access List

To create a new ACL Class Map with a Standard/Extended IP Access List or a MAC Access List, you must have first created a Standard/Extended IP Access List or MAC Access List already. You can then use the CLI commands below to create a new ACL Class Map and assign one (you can only assign one Access List per Class Map) existing Standard/Extended IP Access List, or MAC Access List, to the ACL Class Map by referencing its Access list ID.

Note: The bandwidth policing capabilities of the ACL Class cannot be configured here; it can only be configured during the ACL Policy Map creation or modification:

CLI Command Mode:
Global Configuration Mode
Class Map Configuration Mode

CLI Command Syntax:
class-map *<ACL Class Name>*
match access-group *<Access List ID>*

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#class-map Layer_2-3_Class
switch_a(config-cmap)#match access-group 1
switch_a(config-cmap)#q
switch_a(config)#q
switch_a#
```

Creating an ACL Policy Map

To create a new ACL Policy Map you must have first created the ACL Class Maps that you want to assign to the ACL Policy Map. You can then use the CLI commands below to create the new ACL Policy Map and assign one or multiple existing ACL Class Maps to the ACL Policy Map by referencing its ACL Class Map name. You can also complete or modify the bandwidth policing capabilities of the ACL Class Maps used during the ACL Policy Map creation process

CLI Command Mode:
Global Configuration Mode
Policy Map Configuration Mode
Policy Map Class Configuration Mode

CLI Command Syntax:
policy-map *<ACL Policy Name>*
class *<ACL Class Name>*
police *<1-1000000>* *<1-20000>* exceed-action drop

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#policy-map IP_Policy_1
switch_a(config-pmap)#class IP_Class_1
switch_a(config-pmap-c)#police 50000 5000 exceed-action drop
switch_a(config-pmap-c)#q
```

```
switch_a(config-pmap)#class IP_Class_2
switch_a(config-pmap-c)#police 50000 5000 exceed-action drop
switch_a(config-pmap-c)#q
switch_a(config-pmap)#class IP_Class_3
switch_a(config-pmap-c)#police 50000 5000 exceed-action drop
switch_a(config-pmap-c)#q
switch_a(config-pmap)#q
switch_a(config)#q
switch_a#
```

Appling an Existing ACL Policy to a Port

To apply the ACL packet filtering features on a port, you must have first created an ACL Policy already. You can then use the CLI commands below to apply the existing ACL Policy to a port.

CLI Command Mode:
Global Configuration Mode
Interface Configuration Mode

CLI Command Syntax:
interface <Interface Name>
service-policy input <ACL Policy Name>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface ge1
switch_a(config-if)#service-policy input IP_Policy_1
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Deleting an ACL Class

You can use the CLI commands below to delete an existing ACL Class.

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **no class-map *<ACL Class Name>***

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#no class-map IP_Class_1
switch_a(config)#q
switch_a#
```

Deleting an ACL Policy

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **no policy-map <*ACL Policy Name*>**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#no policy-map IP_Policy_1
switch_a(config)#q
switch_a#
```

IP ACL (ACCESS CONTROL LIST)

The settings in the ACL feature of the EtherWAN switch can be used to control which packets are allowed to enter the switch (Packet Filtering), as well as to control the amount of bandwidth that can be allocated for those packets (Bandwidth Policing).

Configuring IP ACL

To navigate to the **ACL/ACL Configuration** page:

1. Click on the **+** next to **ACL**.
2. Click on **IP ACL**

To configure an IP Access List (See below figure):

1. Enter a number for the ACL, and then select **deny** or **permit**.
2. Select the type **standard** or **exended**.

3. Enter the **source address** and the **source wildcard mask**.
4. Enter source port (or select **any**), and (**eq**, **gt**, **lt**, **neq**). (eq = equal to, gt = greater than, lt= less than, neq = not equal)
5. For the destination, select **Address**, **Any** or **Host**.
6. If Address was selected, **Destination Address**, and the **Destination Wildcard Mask**.
7. Enter the **Destination Port** and the **Destination Port (Maximum)**.
8. Select the IP Protocol and then click **Add**.

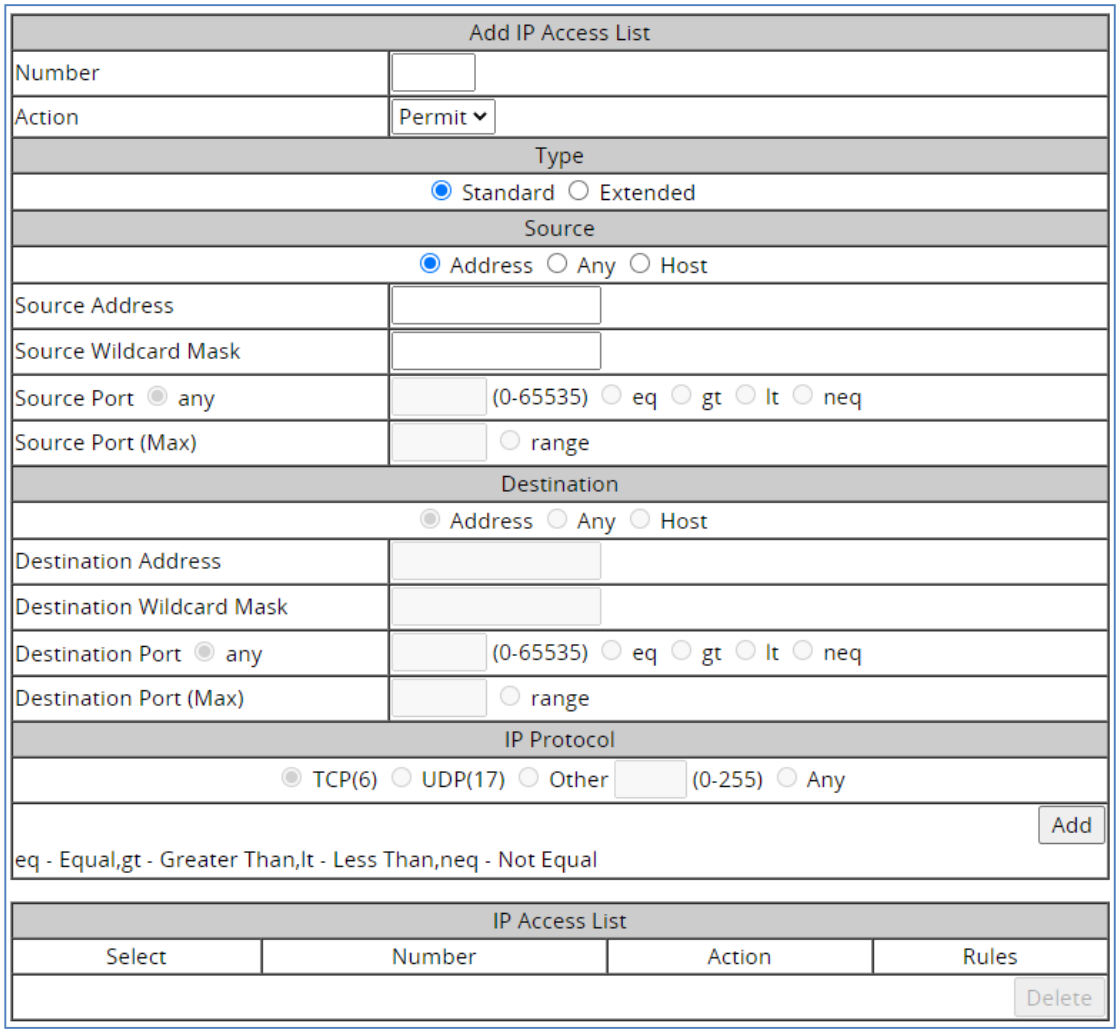


Figure 102: IP ACL Configuration

Created IP ACLs will be displayed at the bottom of the page, where they can be be verified and/or deleted.

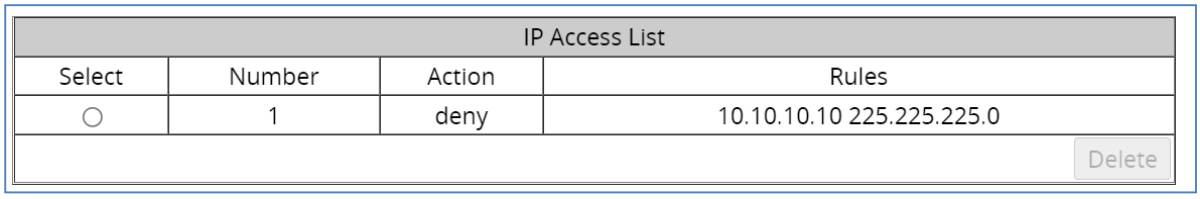


Figure 103: IP ACL List

Port ACL Settings

To navigate to the **Port ACL Settings** page:

1. Click on the **+** next to **ACL**.
2. Click on **Porrt ACL Settings**

To configure a port with an ACL, simply select the exisiting ACL, and the port number with which you want to associate it. Then click **Update Setting.**

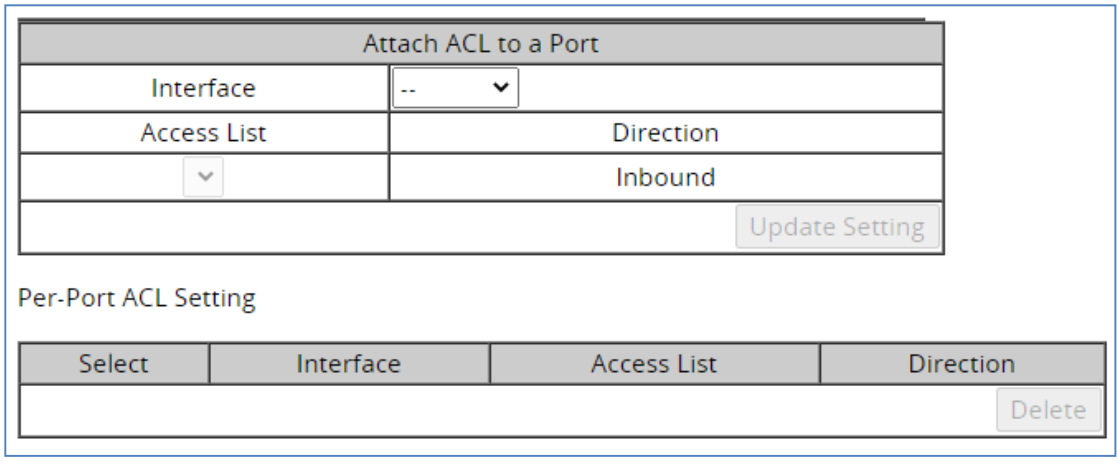


Figure 104: Port ACL Settings

Creating a Standard IP Access List using CLI

To create a new Standard IP Access List to allow or deny an IP address/range access to the switch, use the following CLI commands with the Access list ID in the range from 1 – 99, or from 1300 – 1999:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
access-list <*1-99, 1300-1999*> permit <*source IP*> <*source bit mask*>
access-list <*1-99, 1300-1999*> deny <*source IP*> <*source bit mask*>
access-list <*1-99, 1300-1999*> deny any

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# access-list 1 permit 192.168.1.224 0.0.0.31
switch_a(config)# access-list 1 deny 192.168.1.224 0.0.0.31
switch_a(config)# access-list 1 deny any
switch_a(config)#q
switch_a#
```

Creating an Extended IP Access List

To create a new Extended IP Access List to allow or deny an source IP address/range and destination IP address/range pair access to the switch, use the following CLI commands with the Access list ID in the range from 100 – 199, or from 2000 – 2699:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:

access-list <100-199, 2000-2699> permit ip <source IP> <source bit mask> <destination IP> <destination bit mask>
access-list <100-199, 2000-2699> deny ip <source IP> <source bit mask> <destination IP> <destination bit mask>
access-list <100-199, 2000-2699> deny ip any any

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#access-list 100 permit ip 192.168.1.224 0.0.0.31
192.168.1.224 0.0.0.31
switch_a(config)#access-list 100 deny ip 192.168.1.224 0.0.0.31
192.168.1.224 0.0.0.31
switch_a(config)#access-list 100 deny ip any any
switch_a(config)#q
switch_a#
```

SNMP

SNMP is a TCP/IP application layer network management protocol that allows any TCP/IP device to be managed across a TCP/IP network. It is based on the client-server paradigm. The

server (called a SNMP Agent) runs a process on the managed device that listens for a client's (a network management software running on a computer, usually called a NMS, short for Network Management Station) polling requests to fetch or to set a data item on the managed device. The SNMP Agent can also send alert messages (called Traps) to a NMS automatically, based on the occurrence of certain events on the device that the Agent resides. Note that SNMP is enabled by default.

SNMP General Settings

To navigate to the **SNMP General Settings** page:

1. Click on the **+** next to **SNMP**.
2. Click on **SNMP General Settings**.

To configure the general settings for the SNMP feature (see Figure 105):

1. The SNMP server on the switch can be enabled or disabled by selecting the appropriate choice from the dropdown list next to SNMP Status.
2. The description field displays the switch model and port configuration by default. If needed, enter a short description (up to 256 characters) into this field.
3. Enter a name into the entry field next to Location, for the purpose of identifying the location of the switch.
4. Enter a name (up to 256 characters) into the entry field next to Contact, to identify the entity that is responsible for this switch.
5. Enter a trap community name (up to 256 characters) into the entry field next to any one of the 5 Trap community name entry boxes from Trap Community Name 1 to Trap Community Name 5.
    a. Community names identify the SNMP Trap community group that the traps on this switch should be sending to. The identical Trap community names should also be set on the NMS hosts that will be receiving the traps. Each name defined corresponds with the **Trap host IP address** entry box with the same number. For example, **Trap Community Name 1** corresponds with **Trap Host 1 IP Address**.
6. Enter an IP address, for the NMS host(s) that should be receiving traps from this switch, into the entry field next to any one of the 5 Trap host IP address entry boxes from **Trap Host 1 IP Address to Trap Host 5 IP Address**
7. Enable or disable the link down trap by selecting the appropriate choice from the drop-down list next to **Link Down Trap**. This will allow or stop the switch from sending a trap to the identified trap community groups when any port on the switch moves from the link up state to the link down state.

8. Enable or disable the link up trap by selecting the appropriate choice from the drop-down list next **Link Up Trap**. This will allow or stop the switch from sending a trap to the identified trap community groups when any port on the switch moves from the link down state to the link up state.

9. Enable or disable the power down trap by selecting the appropriate choice from the drop-down list next **Power Down Trap**. This will allow or stop the switch from sending a trap to the identified trap community groups when one of the redundant power sources goes down (This feature is not on EX75000 and EX74000, and models with a single power input).

10. Enable or disable the power up trap by selecting the appropriate choice from the drop-down list next **Power Up Trap**. This will allow or stop the switch from sending a trap to the identified trap community groups when one of the redundant power sources powers up (This feature is not on EX75000 and EX74000, and models with a single power input).

11. Enable or disable the MAC notification trap by selecting the appropriate choice from the drop-down list next to **MAC Notification Trap**. This will allow or stop the switch from sending a trap to the identified trap community groups anytime there is a change in the MAC table on certain selected ports of the switch.

12. Set the interval between the MAC notification traps that you want the switch to send by entering the interval (in number of seconds from 1 to 65535) into the entry field next to **MAC Notification Interval (1 to 65535 seconds)**.

13. Set the size of the MAC notification history table by entering the total number of records (from 1 to 500) that the switch will keep for user to review at any one time into the entry field next to **MAC Notification History Size (1 to 500)**.

14. Select which ports on the switch for which traps should be sent when there is a new MAC address added to the MAC table for the port, by checking the appropriate check boxes for these ports in the **MAC Notification Added** section.

15. Select which ports on the switch for which traps should be sent when there is a MAC address being removed from the MAC table for the port, by checking the appropriate check boxes for these ports in the **MAC Notification Removed** section.

16. Click on the **Update** button after you have finished the configuration of the SNMP Server (Agent) General Settings.

17. Save the configuration (see the Save Configuration Page)

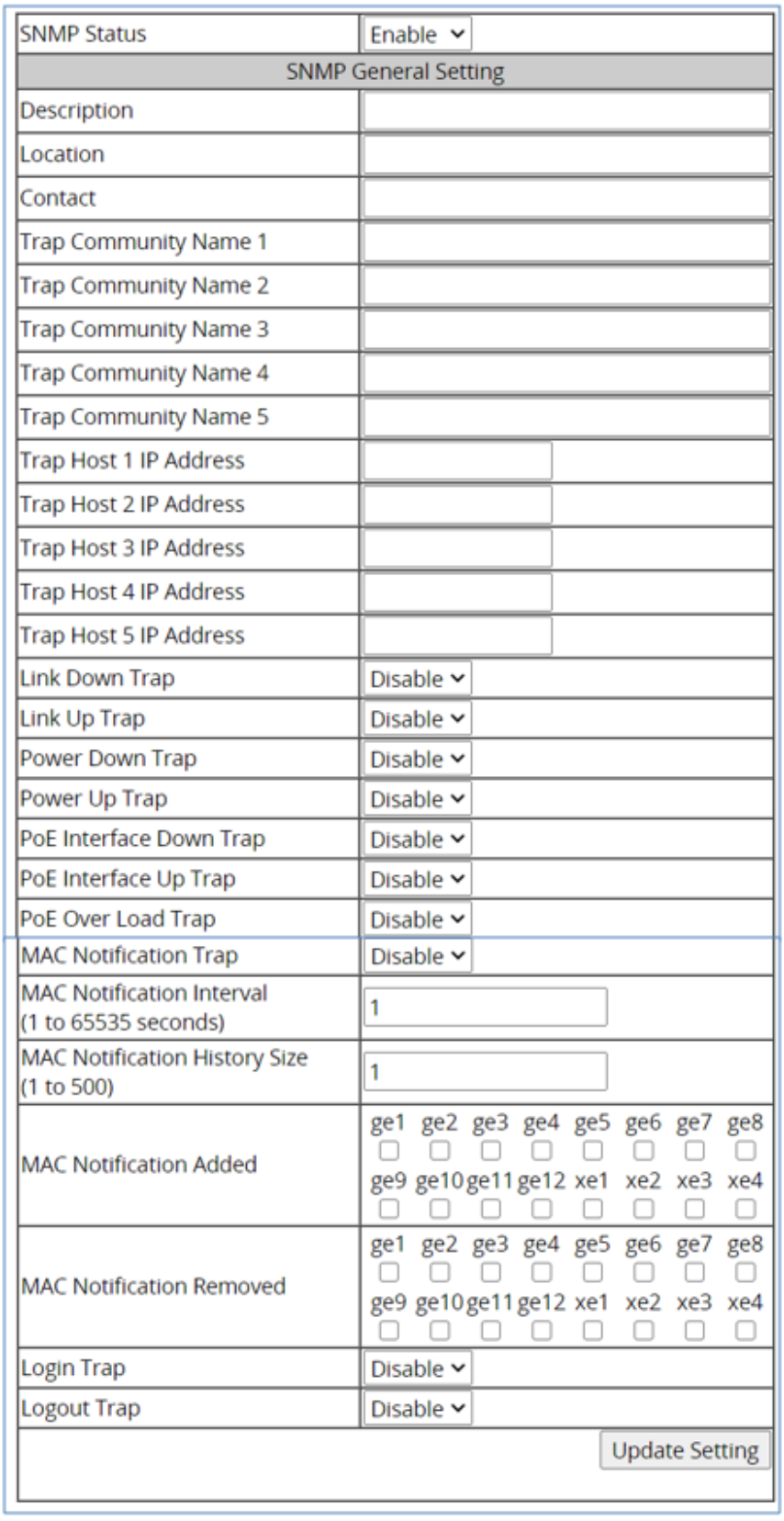


Figure 105: SNMP General Settings

Configuring SNMP v1 & v2 Community Groups

To navigate to the **SNMP v1/v2** page:

1. Click on the **+** next to **SNMP**.
2. Click on **SNMP v1/v2**.

To configure the SNMP v1 & v2 community groups (see Figure 106):

1. Enter the SNMP community name into the entry field next to **Get Community Name** (the default value is “Public”). This will allow the NMS to poll status information from the switch (read only).
2. Enter the SNMP community name, into the entry field next to **Set Community Name**. This will allow a NMS to change the status of a data item in the switch.
3. Click on the **Update Setting** button after you have finished the configuration.
4. Save the configuration (see the Save Configuration Page)

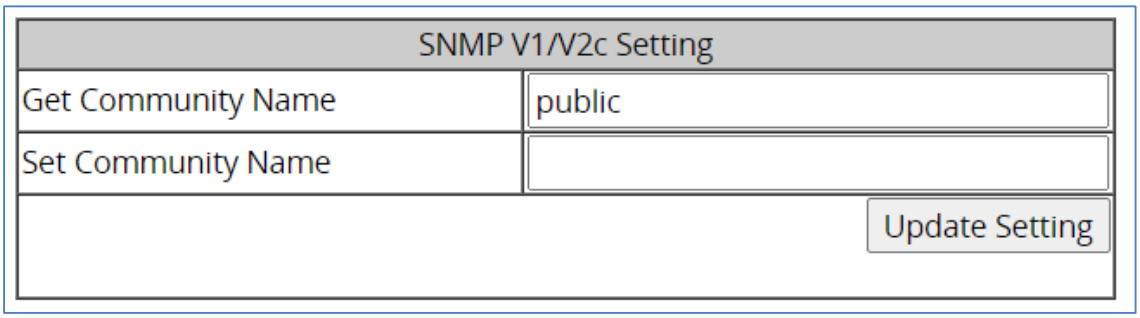


Figure 106: Community Name V1/V2c

Configuring SNMP v3 Users

To navigate to the **SNMP v3** page:

1. Click on the **+** next to **SNMP**.
2. Click on **SNMP v3**.

Adding SNMP v3 Users to the switch

1. Click on the **Add User** button.

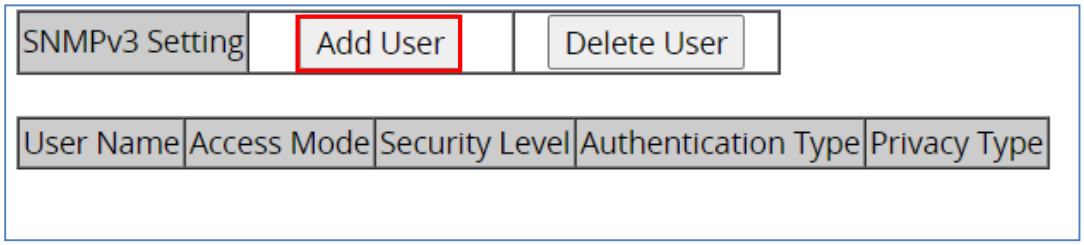


Figure 107: SNMP V3 User setting

2. Next, select the desired **authentication/ privacy protocols** from the drop-down list next to “NMP Version, according to the chart below (also see Figure 108):
    a. **SNMPv3 No-Auth** = Only user name match is required for SNMP access to the switch. No user authentication or data encryption will be used.
    b. **SNMPv3 Auth-MD5** = User authentication will be required using the MD5 hashing algorithm, but no data encryption will be used.
    c. **SNMPv3 Auth-SHA** = User authentication will be required using the SHA-1 hashing algorithm, but no data encryption will be used.
    d. **SNMPv3 Priv Auth-MD5** = User authentication will be required using the MD5 hashing Algorithm, and in addition, all data in protocol message will be encrypted using 128 to 256-bit encryption algorithm.
    e. **SNMPv3 Priv Auth-SHA** = User authentication will be required using the SHA-1 hashing Algorithm, and in addition, all data in protocol message will be encrypted using 128 to 256-bit encryption algorithm.

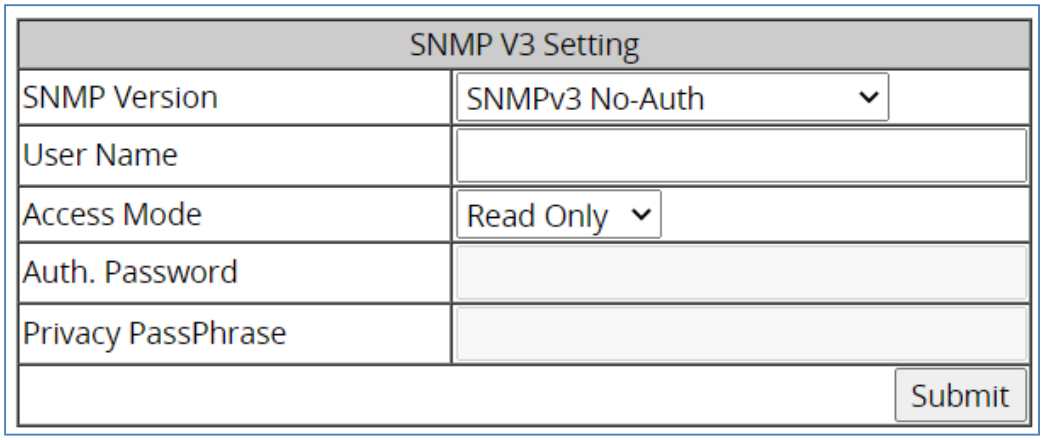


Figure 108: SNMP v3 Settings

3. Next, enter the desired username in the entry field next to **User Name**.
4. Next, select the desired access authorization for the user from the drop-down list next to **Access Mode**. See Figure 109.
5.

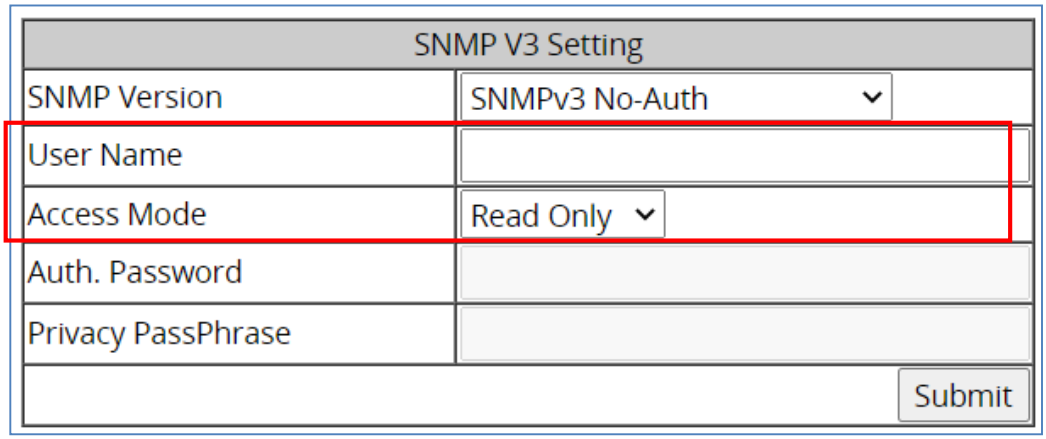


Figure 109: User name & Access Mode

6. Next, if authentication is required for this user, and you have chosen an authentication protocol, then the entry field next to **Auth. Password** will have been enabled. Enter a password for this user inside this entry field. See Figure 110.

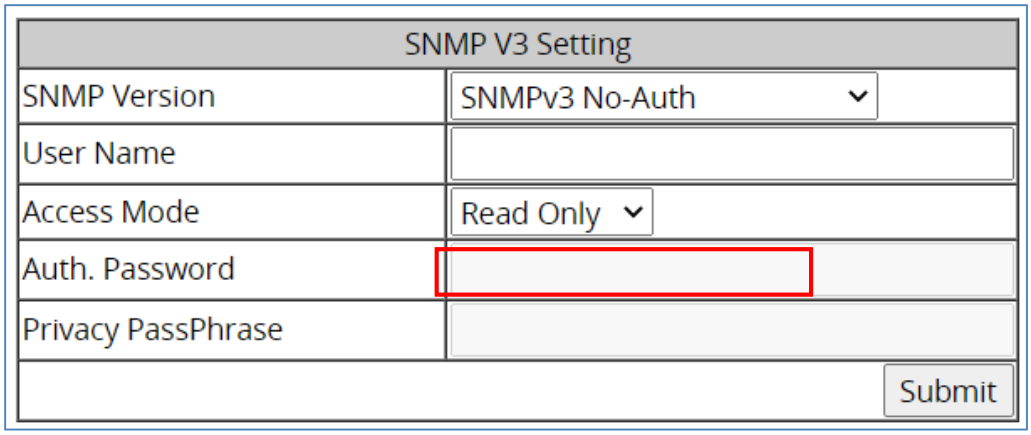


Figure 110: Auth Password

7. Next, if both authentication and privacy are required for this user, and you have chosen both an authentication and privacy protocol, then the entry field next to **Privacy PassPhrase** will have been enabled. Enter a pass phrase inside this entry field, as part of the key used to encrypt the protocol message for this user. (See Figure 111)

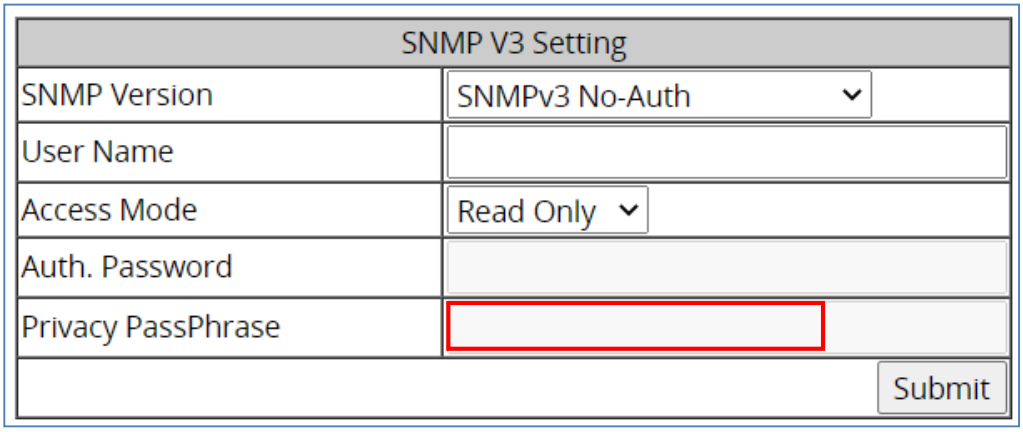


Figure 111: Privacy PassPhrase

Deleting SNMP v3 Users from the switch

1. Go to SNMP → SNMP v3, you should see a list of previously configured users. Next, click on the **Delete User** button. (See Figure116).

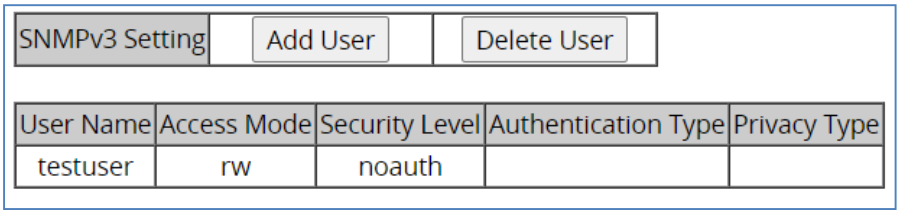


Figure 112: Delete User

2. Next, select the user that you wish to delete from the drop-down list next to **Select User Name**.
3. Click on the **Submit** button.

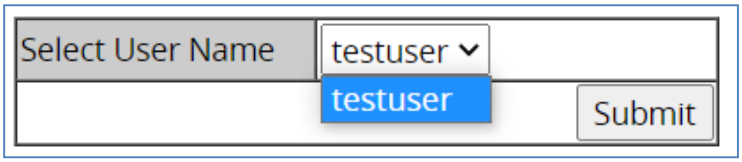


Figure 113: Select User

Create SNMPv3 Group and View

To create SNMPv3 Group and View, first, click on SNMP v3 from the left panel of Web GUI.

Click “Add User” and follow the steps described under Adding SNMP v3 Users.

To provide SNMPv3 View & Group, first finish the SNMPv3 View setup, and input View Name and OID. For OID, select Included or Excluded.

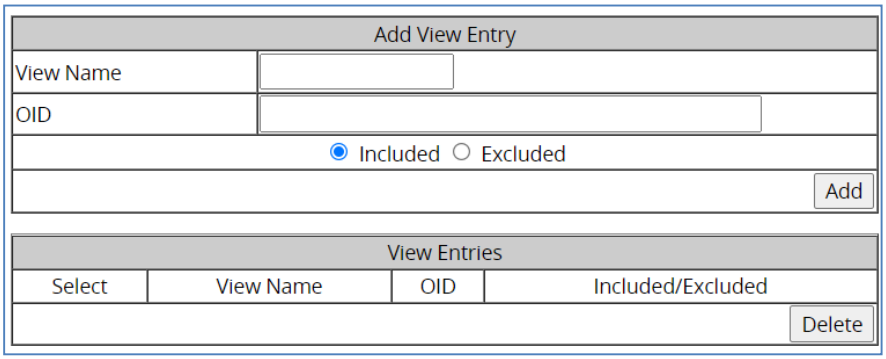


Figure 114: SNMPv3 View setup

After View is created, set up Group Name Entry
Create Group Name according to its Read or Write View attributes.

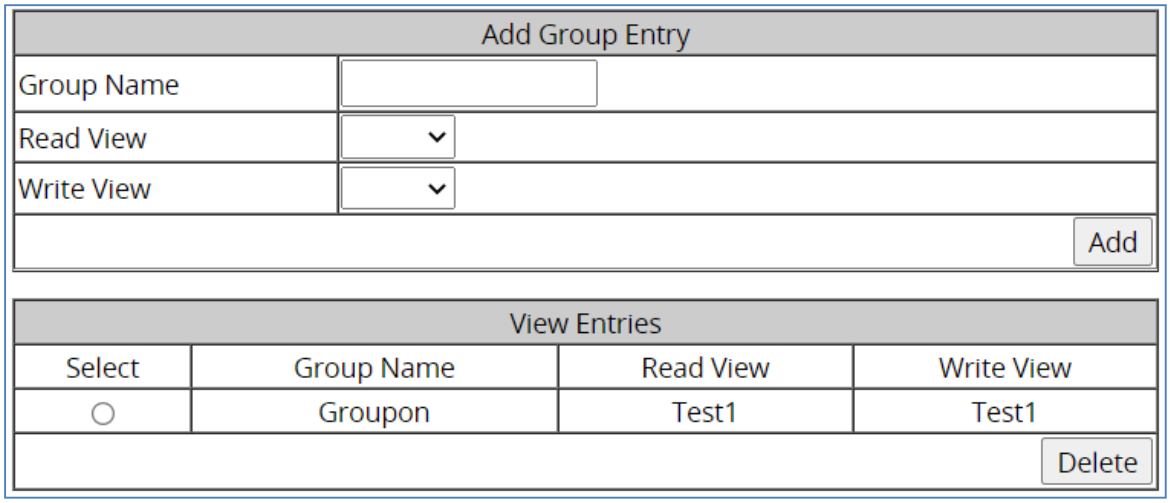


Figure 115: SNMPv3 Group setup

SNMP Configuration Using CLI Commands

Enabling SNMP and configuring general settings

To enable the SNMP feature of the switch, and configure its general settings (Description, Location, and Contact information), use these CLI commands.:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
snmp-server enable
snmp-server description *<1 -256 characters>*
snmp-server location *<1 -256 characters>*
snmp-server contact *<1 -256 characters>*

Usage Example:

```
switch_a> enable
switch_a#configure terminal
switch_a(config)# snmp-server enable
switch_a(config)# snmp-server description Hub_Switch_1
switch_a(config)# snmp-server location First_Floor_Closet
switch_a(config)# snmp-server contact Administrator
```

```
switch_a(config)#q
switch_a#
```

Configuring SNMP Traps

To configure the Trap features of the SNMP protocol on the switch, you use the following CLI commands:

CLI Command Mode:
Global Configuration Mode
Interface Configuration Mode

CLI Command Syntax:
snmp-server trap-community 1 *<1 -256 characters >*
snmp-server trap-community 2 *<1 -256 characters >*
snmp-server trap-community 3 *<1 -256 characters >*
snmp-server trap-community 4 *<1 -256 characters >*
snmp-server trap-community 5 *<1 -256 characters >*
snmp-server trap-ipaddress 1 *<IP Address>*
snmp-server trap-ipaddress 2 *<IP Address>*
snmp-server trap-ipaddress 3 *<IP Address>*
snmp-server trap-ipaddress 4 *<IP Address>*
snmp-server trap-ipaddress 5 *<IP Address>*
snmp-server trap-type enable linkDown
snmp-server trap-type enable linkup
snmp-server trap-type enable mac-notification
snmp-server mac-notification interval *<1 to 65535 seconds>*
snmp-server mac-notification history-size *<1 to 500 entries>*
snmp-server trap mac-notification added
snmp-server trap mac-notification removed

Usage Example:

```
switch_a> enable
switch_a#configure terminal
switch_a(config)# snmp-server trap-community 1 Trap_Group_1
switch_a(config)# snmp-server trap-community 2 Trap_Group_2
switch_a(config)# snmp-server trap-community 3 Trap_Group_3
switch_a(config)# snmp-server trap-community 4 Trap_Group_4
switch_a(config)# snmp-server trap-community 5 Trap_Group_5
switch_a(config)# snmp-server trap-ipaddress 1 192.168.1.100
switch_a(config)# snmp-server trap-ipaddress 2 192.168.2.100
switch_a(config)# snmp-server trap-ipaddress 3 192.168.3.100
```

```
switch_a(config)# snmp-server trap-ipaddress 4 192.168.4.100
switch_a(config)# snmp-server trap-ipaddress 5 192.168.5.100
switch_a(config)# snmp-server trap-type enable linkDown
switch_a(config)# snmp-server trap-type enable linkup
switch_a(config)# snmp-server trap-type enable mac-notification
switch_a(config)# snmp-server mac-notification interval 60
switch_a(config)# snmp-server mac-notification history-size 100
switch_a(config)#interface ge1
switch_a(config-if)#snmp-server trap mac-notification added
switch_a(config-if)#snmp-server trap mac-notification removed
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

Configuring SNMP v1 & v2 Community Groups

To configure the SNMP v1 & v2 community groups to make the SNMP feature more secure, use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
snmp-server enable
snmp-server community get *<1 -256 characters>*
snmp-server community set *<1 -256 characters>*

Usage Example:

```
switch_a> enable
switch_a#configure terminal
switch_a(config)# snmp-server community get public
switch_a(config)# snmp-server community set private
switch_a(config)#q
switch_a#
```

Adding SNMP v3 Users

To add SNMP v3 Users to the switch and maximize the security for the SNMP feature, you must use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
snmp-server v3-user <username> <ro|rw> noauth
snmp-server v3-user <username> <ro|rw> auth <md5|sha> <password>
snmp-server v3-user <username> <ro|rw> priv <md5|sha> <password> des <pass_phrase>

Usage Example:

```
switch_a> enable
switch_a#configure terminal
switch_a(config)# snmp-server v3-user SNMP_User_1 ro noauth
switch_a(config)# snmp-server v3-user SNMP_User_2 ro auth md5 User2
switch_a(config)# snmp-server v3-user SNMP_User_3 rw priv md5 User3 des
Private_User
switch_a(config)#q
switch_a#
```

Configuring a New SNMP Group

The SNMP Group feature is only for SNMPv3. As long as any SNMP command is executed, the SNMP service will be restarted. Up to five SNMP groups can be set. When creating a Group, the user must select **Read View**, **Write View**, or **both**. When a Group is created with a write view, users in this Group will be able to read and write the SNMP OIDs defined in the write view.

CLI Command Mode: **Global Configuration Mode**
CLI Command Syntax:
snmp-server group <group-name> [read read-view] [write write-view]
no snmp-server group <group-name>

Syntax Description:

group-name	Name of the group. String of a maximum of 32 characters.
read	(Optional) Specifies a read view for the SNMP group. This view enables you to view only the contents of the agent.
read-view	(Optional) String of a maximum of 32 characters that is the name of the view. The default is that the read-view is assumed to be every object belonging to the Internet object identifier (OID) space (1.3.6.1), unless the read option is used to override this state.
write	(Optional) Specifies a write view for the SNMP group. This view enables you to enter data and configure the contents of the agent.
write-view	(Optional) String of a maximum of 32 characters that is the name of the view.

Create or Update a View Entry

To create or update a view entry, use the **snmp-server view** command in global configuration mode. To remove the specified Simple Network Management Protocol (SNMP) server view entry, use the **no** form of this command.

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
snmp-server view view-name oid-tree {included | excluded}
no snmp-server view view-name

Syntax Description:

group-name	Name of the group. String of a maximum of 32 characters.
Oid-tree	Object identifier of the ASN.1 subtree to be included or excluded from the view. To identify the subtree, specify a text string consisting of numbers, such as 1.3.6.2.4. Replace a single sub-identifier with the asterisk (*) wildcard to specify a subtree family; for example 1.3.*.4.
Included	Configures the OID (and subtree OIDs) specified in oid-tree argument to be included in the SNMP view.
excluded	Configures the OID (and subtree OIDs) specified in oid-tree argument to be explicitly excluded from the SNMP view.

AAA

EtherWAN switches support the IEEE 802.1X protocol to provide port-based security on a switch port against unauthorized access. RADIUS and TACACS+ protocols are supported.

An EAP (Extensible Authentication Protocol) compatible RADIUS or TACACS+ server is required, as well as 802.1X client software (known as the “Supplicant” software) on the end device to communicate with the server for the purposes of authenticating the end device that is trying to gain access to the network through the switch port.

When an end device is initially connected to a port on the EtherWAN switch where the 802.1X protocol is enabled on the port, the switch will only pass 802.1X authentication traffic (known as EAPOL traffic) on that port between the Supplicant on the end device and the server, and will not allow any other traffic to pass. After the initial connection, the switch will request authentication credentials from the Supplicant in the end device that has just connected to the port. After the switch receives the proper authentication credentials from the Supplicant in the end device, the switch will send the credentials to the EAP compatible. If the end device is successfully authenticated by the server, the server will send a message to the switch.

Configuring Radius from the GUI

To navigate to the **Radius Configuration** page:

1. Click on the **+** next to **802.1X**
2. Click on **Radius Configuration**

Enabling Radius

By default, the 802.1X function is globally disabled on the EtherWAN switch. To use the 802.1X port-based security on a port, you must enable it globally on the switch first, and then enable it on a per port basis.

To enable the 802.1X function globally on the switch:

1. Select **Dot1x Enable** or **Mac-auth Enable** from the drop-down list next to **Radius Status**.
2. Click on the **Update Setting** button. (See Figure 116)

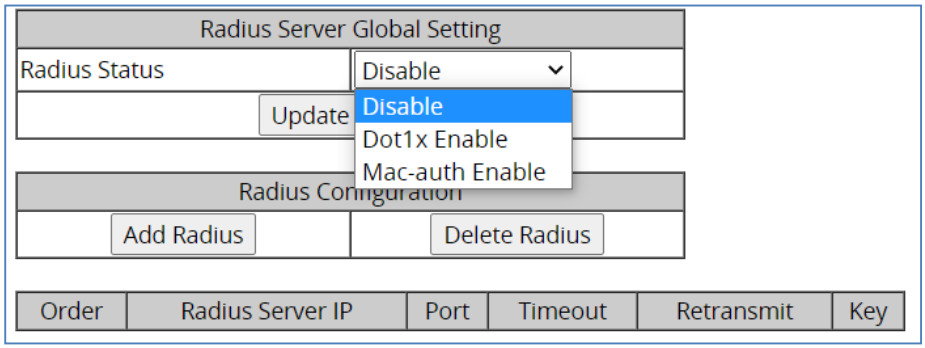


Figure 116: Enable Radius

Adding a Radius Server

Next, you will need to configure the settings that the switch will need in order to connect to a RADIUS server.

1. Click on the **Add Radius** button (See Figure 116).
2. Next, enter the IP address of the RADIUS server that the switch will use in order to authenticate in the entry field next to **Radius Server IP** (see Figure 117).
3. Enter the password for RADIUS server in the entry field next to **Secret Key**.

4. Optionally, the UDP port number for the RADIUS server (if it is different from the standard default 1812) can be changed. To do this, enter the port number in the entry field next to **Radius Server Port**.

5. Next, you can choose to configure the minimum time that the switch must wait, before it is allowed to retransmit a message to the RADIUS server due to no response. To do this, enter the number of seconds that the switch must wait (between 1 and 1000 seconds) into the entry field next to **Timeout <1-1000>**.

6. Next, you can choose to configure the maximum number of times that the switch can attempt to retransmit a message to the RADIUS server. To do this, enter a number (from 1 to 100) into the entry field next to **Retransmit**.

7. Click on the **Submit** button.

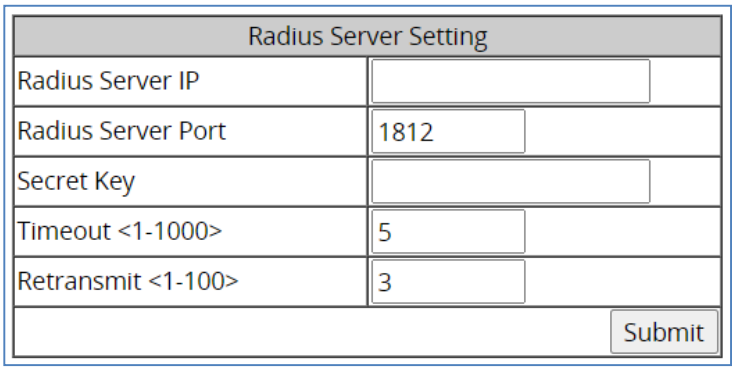


Figure 117: Radius Setup

After a Radius server has been added and configured, verify the existing setup on the same screen.

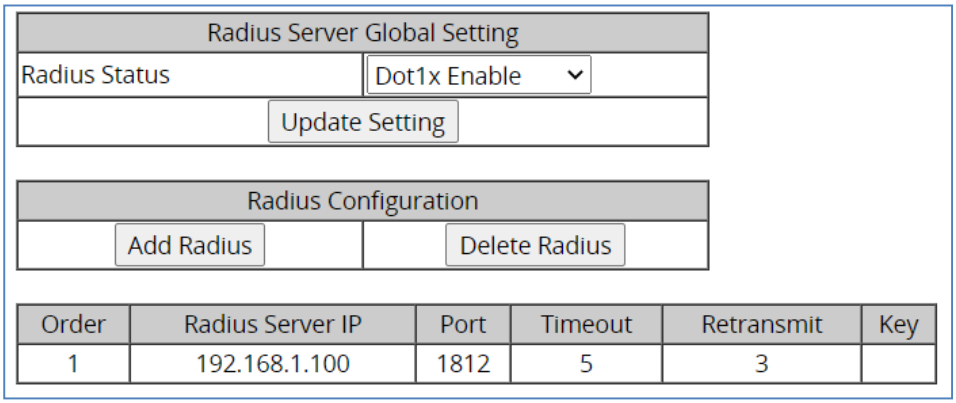


Figure 118: Resulting Radius Server Setup

Port Authentication

After the 802.1X port-based security is enabled globally, you must enable it locally on the port.

To navigate to the **802.1X / Port Authentication** page:

1. Click on the **+** next to **802.1X**
2. Click on **Port Authentication**

To enable 802.1X on a port (see Figure 119):

1. Choose the desired port from the drop-down list next to **Interface**, to have the 802.1X feature applied to that port.
2. Next, make sure **Enabled** is selected from the drop-down list next to **Authentication State**, this will enable the 802.1X function on the previously selected port.
3. Next, make sure that the choice **Auto** is selected in the drop-down list next to **Port Control**; this will allow the port to use 802.1X to authenticate the end station.
    a. If you choose to have the port to be always unauthorized or to be always authorized, you can choose the appropriate choice in the drop-down list.
4. Next, you can choose to have the end station to be re-authenticated periodically. To do this, choose **Enabled** in the drop-down list next to **Periodic Re-authentication**.
5. After you have enabled periodic re-authentication, you must also configure the time period interval for the re-authentication of the end station. To do this, enter the number of seconds (1-4294967295), into the entry field next to **Re-authentication Period**.
6. Next, **Update Setting** button in order to activate all the configured settings (see the below screenshot)

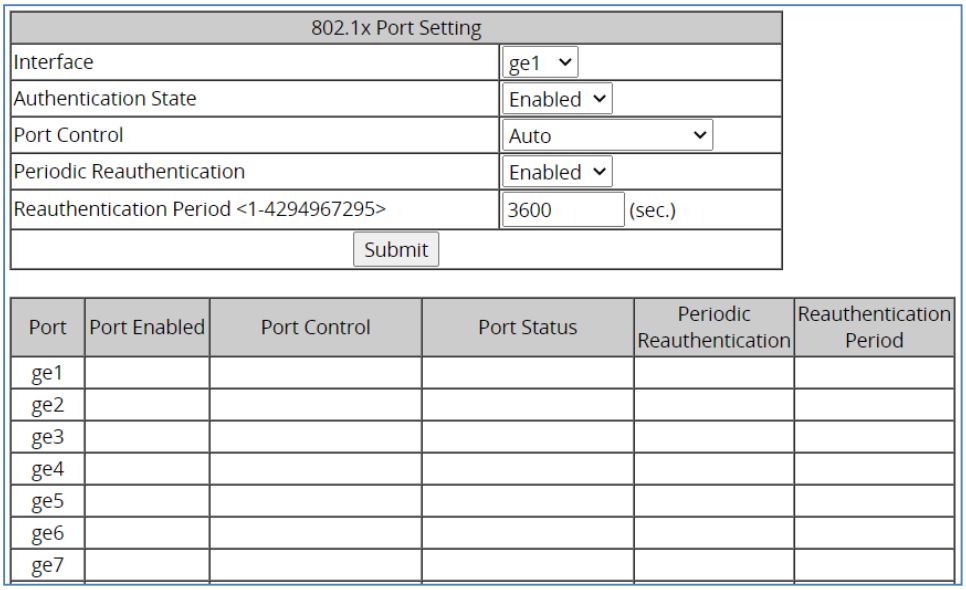


Figure 119: Enabling 802.1X on a Port

Configuring TACACS+ from the GUI

To navigate to the **AAA / TACACS+ Configuration** page:

1. Click on the **+** next to **AAA**
2. Click on **TACACS+**

Enabling TACACS+

To enable TACACS+, click the corresponding check boxes next to **Console**, **VTY**, and **Web**, and click **Update Setting**.

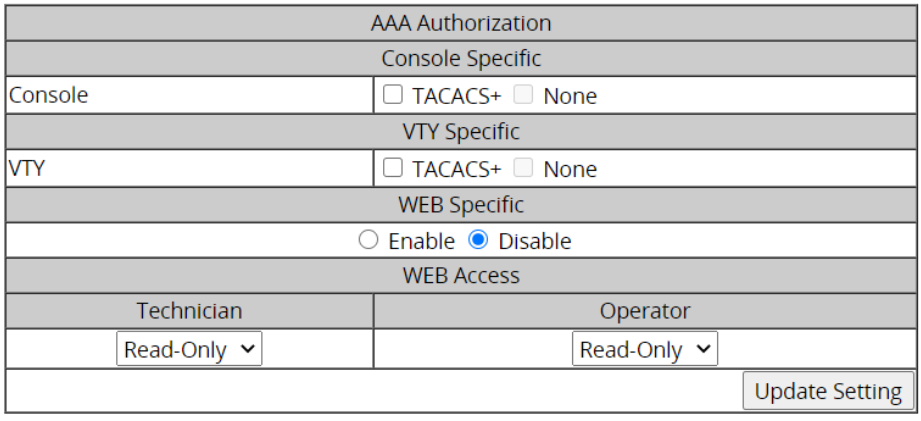


Figure 120: Enabling TACACS+

Adding a TACACS+ Server

Next, you will need to configure the switch to connect to a TACACS+ server. Setting a TACACS+ server to “primary” means that it will be the first server contacted when the switch tries to create a TACACS+ session. Only one server can be set to primary. Setting a TACACS+ server to “inactive” will disable it. A maximum of 3 servers can be added to a switch.

1. In the **TACACS** Account button, select **Create**, or choose an existing server to modify.
2. Enter the IP address of the TACACS server.
3. Enter the server port.
4. Enter the timeout value in seconds.
5. Enter the secret key that will authenticate the switch to the TACAS server.
6. Select **Primary** or **Inactive** for the server state. Inactive in this sense means “secondary,” or “backup.”
7. Click on the **Update** button.

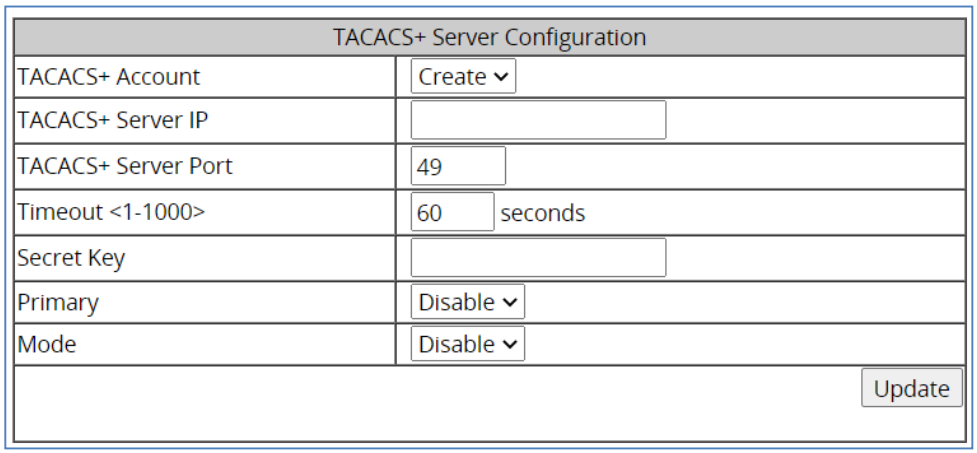


Figure 121: TACACS+ Setup

Configuring DoS (Denial of Service) from the GUI

To navigate to the **AAA / DoS Configuration** page:

1. Click on the **+** next to **AAA**
2. Click on **DoS**

There are 11 functions for protection against Denial of Service or distributed Denial of Service attacks. Enable the desired functions using the dropdown menus on the right, then click **Submit**.

Source IP address == Destination IP address: Source IP address = Destination IP address (SIP = DIP) DoS protection. If packets ingress with SIP = DIP, the packets will be dropped when this mode is enabled.

TCP Flag SYN = 0: TCP Flag DoS protections. If packets ingress with TCP Flag SYN set and a source port less than 1024, or have TCP Control Flags set to 0 and TCP Sequence Number set to 0, or have TCP Flags FIN, URG, and PSH set and TCP Sequence Number set to 0, or have TCP Flags SYN and FIN both set, the packets will be dropped

TCP Control Flags = 0 and TCP Sequence Number = 0: TCP Flag and Sequence DoS protections. If packets ingress with TCP Flag SYN set and a source port less than 1024, or have TCP Control Flags set to 0 and TCP Sequence Number set to 0, or have TCP Flags FIN, URG, and PSH set and TCP Sequence Number set to 0, or have TCP Flags SYN and FIN both set, the packets will be dropped.

TCP Flags (FIN, URG, PSH set, TCP Seq. Num.) = 0: TCP FIN and URG and PSH and SEQ = 0 checking DoS protections. If packets ingress with TCP FIN, URG, and PSH all set and TCP Sequence Number set to 0, the packets will be dropped

TCP Flag SYN and FIN set: TCP SYN and FIN DoS protection. If packets ingress with TCP flags SYN and FIN set, the packets will be dropped.

Source TCP Port = Destination TCP Port: TCP source = destination port number (Source TCP Port = Destination TCP Port) DoS protection. If packets ingress with Source TCP Port = Destination TCP Port, the packets will be dropped.

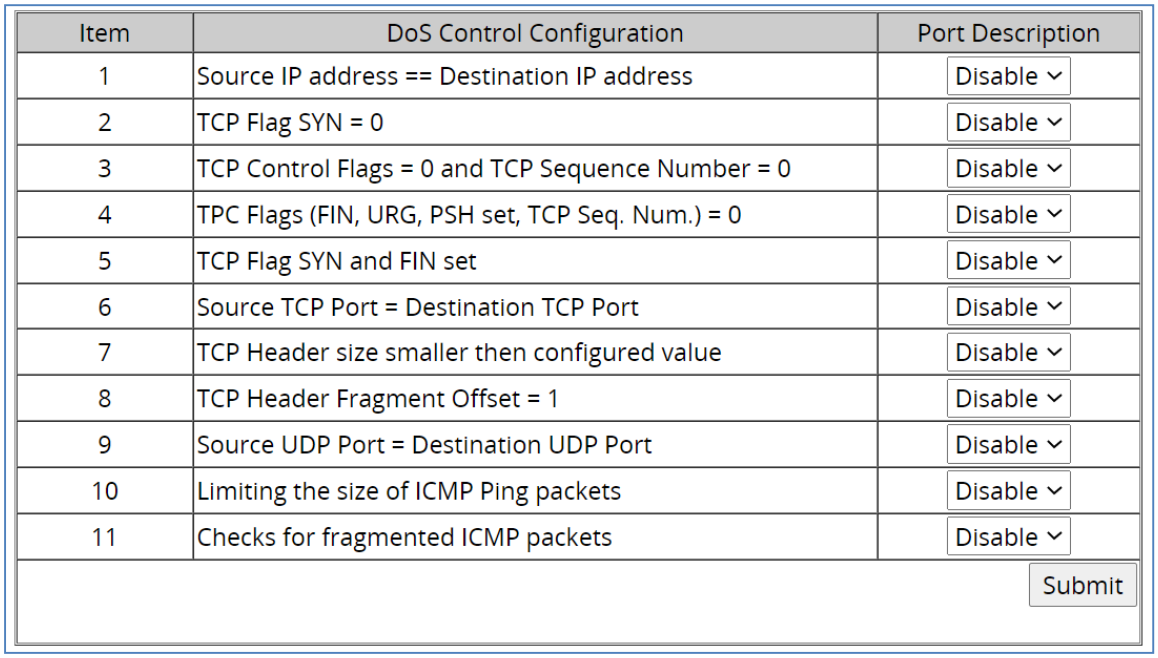
TCP Header size smaller then configured value: Minimum TCP Header Size DoS protection. If packets ingress with a TCP Header Size smaller then the configured value, the packets will be dropped.

TCP Header Fragment Offset = 1: TCP Fragment DoS protection. If packets ingress with IP Fragment Offset equal to one (1), the packets will be dropped.

Source UDP Port = Destination UDP Port: Source UDP Port = Destination UDP Port number DoS protection. If packets ingress with Source UDP Port = Destination UDP Port, the packets will be dropped.

Limiting the size of ICMP Ping packets: Maximum ICMP Packet Size DoS protections. If ICMP Echo Request (PING) packets ingress with a size greater than the configured value, the packets will be dropped.

Checks for fragmented ICMP packets: ICMP Fragment DoS protection. If packets ingress with fragmented ICMP packets, the packets will be dropped.



Item	DoS Control Configuration	Port Description
1	Source IP address == Destination IP address	Disable
2	TCP Flag SYN = 0	Disable
3	TCP Control Flags = 0 and TCP Sequence Number = 0	Disable
4	TPC Flags (FIN, URG, PSH set, TCP Seq. Num.) = 0	Disable
5	TCP Flag SYN and FIN set	Disable
6	Source TCP Port = Destination TCP Port	Disable
7	TCP Header size smaller then configured value	Disable
8	TCP Header Fragment Offset = 1	Disable
9	Source UDP Port = Destination UDP Port	Disable
10	Limiting the size of ICMP Ping packets	Disable
11	Checks for fragmented ICMP packets	Disable
		Submit

Figure 122: DoS Configuration

AAA Configuration Using the CLI

View RADIUS Status

Use the CLI commands below to view RADIUS statuses:

CLI Command Mode: **User Exec Mode**
CLI Command Syntax:
show dot1x
show dot1x all
show dot1x diagnostics interface <ifname>
show dot1x interface <ifname>
show dot1x sessionstatistics interface <ifname>
show dot1x statistics interface <ifname>

Enable RADIUS Globally

CLI Command Mode: **Global Configuration Mode**
CLI Command Syntax:
dot1x system-auth-ctrl
dot1x system-auth-ctrl disable

Configure RADIUS on Ports

CLI Command Mode: **Interface Configuration Mode**
CLI Command Syntax:
dot1x keytxenabled <enable | disable>
dot1x max-req <1-10>
dot1x port-control <force-unauthorized | force-authorized | auto>
dot1x port-control dir <in | both>
dot1x protocol-version <1-2>
dot1x quiet-period <1-65535>
dot1x reauthMax <1-10>
dot1x reauthentication
dot1x timeout re-authperiod <1-4294967295>
dot1x timeout server-timeout <1-65535>
dot1x timeout supp-timeout <1-65535>
dot1x timeout tx-period <1-65535>

Usage Example – Enabling and configuring RADIUS with host 10.1.1.100 and key “textkey.” Authentication is automatic:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#dot1x system-auth-ctrl
switch_a(config)#radius-server host 10.1.1.100 key textkey
switch_a(config)#interface ge1
switch_a(config-if)#dot1x port-control auto
switch_a(config-if)#q
switch_(config)
```

Configure MAC-Based Authentication

MAC authentication uses the MAC address of the host for authentication. The RADIUS server has a dedicated host database that contains only allowed MAC addresses.

Use the CLI commands below to set up a mac-based authentication:

CLI Command Mode: **Global Configuration Mode**
CLI Command Syntax:
auth-mac <system-auth-control, username-format uppercase>

CLI Command Mode: **Interface Configuration Mode**
CLI Command Syntax:
auth-mac <enable, disable>

TACACS+ Authentication and Authorization

Use the CLI commands below to enable/disable TACACS+ for authentication:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
(no) aaa authentication login tacplus

Use the CLI commands below to enable/disable TACACS+ for authorization:

CLI Command Mode: **Global Configuration Mode**
CLI Command Syntax:
(no) aaa authorization command tacplus

Configure TACACS+ Server

Setting a TACACS+ server to “primary” means that it will be the first server contacted when the switch tries to create a TACACS+ session. Only one server can be set to primary. Setting a TACACS+ server to “inactive” will disable it. A maximum of 3 servers can be added to a switch.

Use the CLI commands below to set up a TACACS+ server:

CLI Command Mode: **Global Configuration Mode**
CLI Command Syntax:
(no) tacplus-server host *hostname* | *IP address* <key *string*> <timeout 1-1000> <port *portnumber*> <primary | inactive>

Usage Example – Setting up a primary TACACS+ server with IP address 192.168.200.1 and secret key of “password1234” and a timeout of 3 minutes (180 seconds):

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#aaa authentication login tacplus
switch_a(config)# tacplus-server host 192.168.200.1 key
password1234 timeout 180 primary
switch_a(config)
```

LLDP

LLDP is a network discovery protocol that defines a method for network access devices using Ethernet connectivity to advertise information about devices to peer devices on the same physical LAN and store information about the network. It allows a device to learn higher layer management reachability and connection endpoint information from adjacent devices.

Using LLDP, a device is able to advertise its own identification information, its capabilities and media-specific configuration information, as well as learn the same information from the devices connected to it. LLDP advertises this information over Logical Link-Layer Control frames and the information received from other agents in IEEE-defined Management Information Bases (MIB) modules.

LLDP significantly aids in the deployment of any network device that supports the protocol. As a media independent protocol intended to be run on all IEEE 802 devices, LLDP may be used to discover routers, bridges, repeaters, WLAN APs, IP telephones, network camera or any LLDP-enabled device, regardless of manufacturer. Since LLDP runs over the data-link layer only, a switch running one network layer protocol can discover and learn about an access device running a different network layer protocol.

LLDP General Settings

To navigate to the **LLDP General Settings** page:

1. Click on the **+** next to **LLDP**.
2. Click on **General Settings.**

Enable/Disable LLDP

To enable LLDP on the switch:

1. Select Enable or Disable from the Drop Down box in the **LLDP** field of the LLDP Transmit Settings box (see Figure 123)
2. Click on the **Update Settings** button.
3. Save the configuration (see the Save Configuration Page)

LLDP is enabled by default.

Holdtime Multiplier

The Holdtime multiplier for transmit TTL is used to compute the actual time-to-live (TTL) value used in an LLDP frame. The TTL value is the length of time the receiving device should maintain the information in its MIB. To compute the TTL value, the system multiplies the LLDP transmit (TX) interval by the holdtime multiplier. For example, if the LLDP transmit (TX) interval is 30 and the holdtime multiplier for TTL is 4, then the value 120 is encoded in the TTL field in the LLDP header.

To adjust the Holdtime multiplier:

1. Enter a numeric value between 2 and 10 (default is 4) in the Holdtime Multiplier text box.
2. Click on the **Update Settings** button.

The TX Interval setting adjusts the time that LLDP information is transmitted by the switch. Values can range from 5 to 32768 seconds (default is 30 seconds).

To adjust the TX Interval setting (see Figure 123):

1. Enter a numeric value between 5 and 32768 (default is 30) in the TX Interval text box.
2. Click on the **Update Settings** button.
3. Save the configuration (see the Save Configuration Page)

Global TLV Setting

The global TLV (Time – Length – Value) settings are advertised by the switch to other LLDP devices. The TLVs supported by the switch are (see Figure 123):

- Port Description
- System Name
- System Description
- System Capabilities
- Management Address
- Port VLAN ID
- MAC/PHY Configuration/Status
- Port And Protocol VLAN ID
- VLAN Name
- Protocol Identity
- Power Via MDI
- Link Aggregation
- Maximum Frame Size

To enable specific TLVs for the switch:

1. Select the check box for each TLV that is to be enabled or select the checkbox for the **All** option which will enable all TLVs for the switch.
2. Click on the **Update Settings** button.
3. Save the configuration (see the Save Configuration Page)

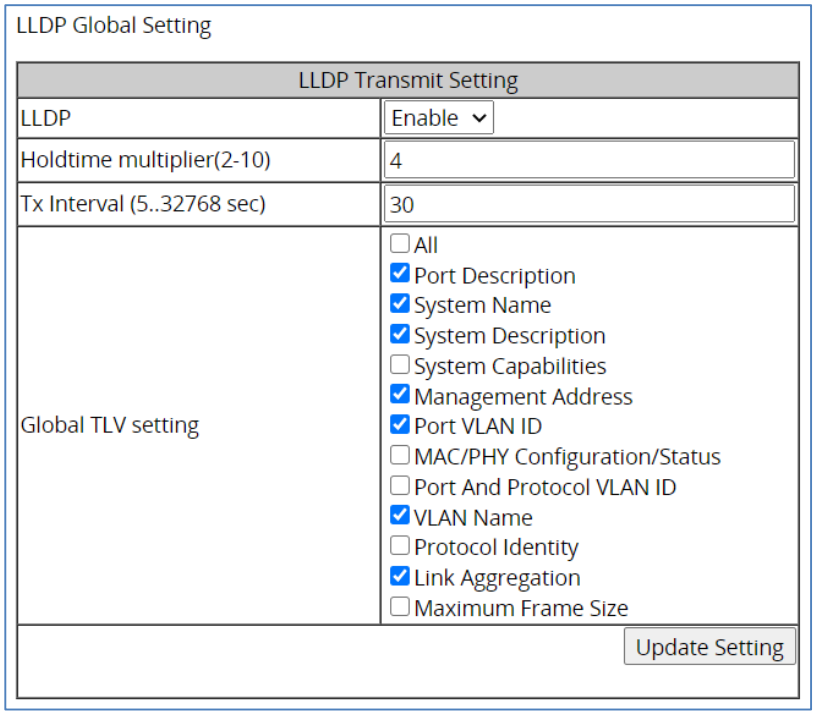


Figure 123: LLDP Global Settings

LLDP Ports Settings

LLDP Ports Settings allows the individual ports on the switch to be configured for LLDP independently of one another. Each port can be configured to transmit LLDP information, receive LLDP information, and notify (via SNMP or Syslog) if there are changes in the LLDP information received from neighboring devices.

To navigate to the **LLDP Port Settings** page:

1. Click on the **+** next to **LLDP**.
4. Click on **LLDP Ports Settings** (see Figure 124)

Enabling LLDP transmission for a specific Port

To enable the transmission of LLDP information for a specific port:

1. Select Enable from the Drop-Down box under the Transmit field for each port for which the transmission of LLDP information should be enabled.
2. Click on the **Submit** button.

Enabling LLDP Reception for a specific Port

To enable the reception of LLDP information for a specific port:

1. Select Enable from the Drop-Down box under the Receive field for each port for which the reception of LLDP information should be enabled.
2. Click on the **Submit** button.

Enabling Notifications

To enable notification whenever a port receives changed LLDP information:

1. Select Enable from the Drop-Down box under the Notify field for each port that should send a notification whenever received LLDP information changes.
2. Click on the **Submit** button
3. Save the configuration (see the Save Configuration Page) after making changes shown on this page.

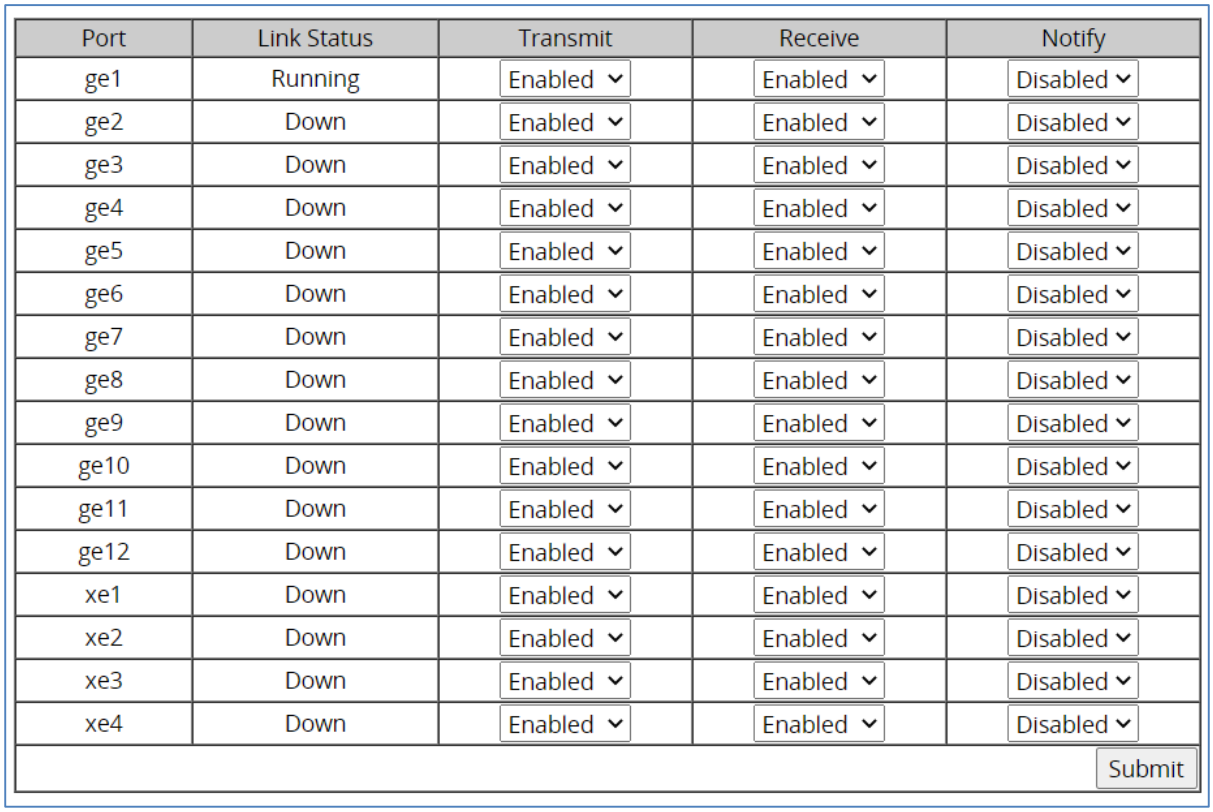
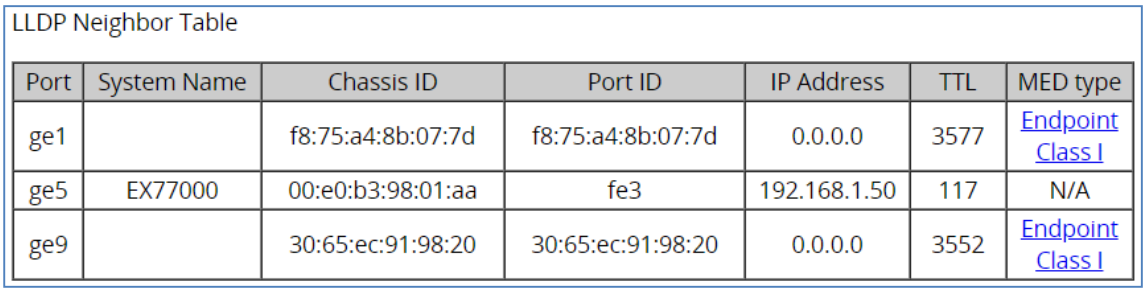


Figure 124: LLDP Ports Settings

LLDP Neighbors

LLDP Neighbors is a read-only page (see Figure 125) that will display all the LLDP capable devices detected by the switch. The following information about connected LLDP-enabled devices is displayed in a tabular format. The columns displayed are:

- **Port** – The local switch port to which the remote device is connected.
- **Chassis ID** – The MAC address of the remote device.
- **Port ID** – The port number of the remote device.
- **IP Address** – The management IP address of the remote device.
- **TTL** – Time to Live, the amount time remaining before the remote device's LLDP is aged-out from the switch.
- **MED type** – Media endpoint discovery information



LLDP Neighbor Table

Port	System Name	Chassis ID	Port ID	IP Address	TTL	MED type
ge1		f8:75:a4:8b:07:7d	f8:75:a4:8b:07:7d	0.0.0.0	3577	Endpoint Class I
ge5	EX77000	00:e0:b3:98:01:aa	fe3	192.168.1.50	117	N/A
ge9		30:65:ec:91:98:20	30:65:ec:91:98:20	0.0.0.0	3552	Endpoint Class I

Figure 125: LLDP Neighbors

Shown above: switch with LLDP enabled connected to port ge5, PC connected to ports ge1 and ge9. "Endpoint Class I" indicates the PC connected to this port, and therefore may not provide its IP Address.

LLDP Statistics

This is a read-only page (see Figure 126) that displays LLDP device statistics and LLDP statistics on a per-port basis. The information collected on this page includes:

- Port – switch port number.
- TX Total – Total LLDP packets sent.
- RX Total – Total LLDP packets received.
- Discards – Number of LLDP packets discarded.
- Errors – LLDP errors.
- Ageout – LLDP information that has been aged out by the switch.
- TLV Discards – TLV information discarded
- TLV Unknown – TLV information that is unknown

LLDP Device Statistics	
Last Update	04:54:47
Total Inserts	2
Total Deletes	1
Total Drops	0
Total Ageouts	1

Port	Tx Total	Rx Total	Discards	Errors	Ageout	TLV Discards	TLV Unknowns
ge1	737	27	0	0	1	0	0
ge2	0	0	0	0	0	0	0
ge3	0	0	0	0	0	0	0
ge4	0	0	0	0	0	0	0
ge5	0	0	0	0	0	0	0
ge6	0	0	0	0	0	0	0
ge7	0	0	0	0	0	0	0
ge8	0	0	0	0	0	0	0
ge9	0	0	0	0	0	0	0
ge10	0	0	0	0	0	0	0
ge11	0	0	0	0	0	0	0
ge12	0	0	0	0	0	0	0
xe1	0	0	0	0	0	0	0
xe2	0	0	0	0	0	0	0
xe3	0	0	0	0	0	0	0
xe4	0	0	0	0	0	0	0

Figure 126: LLDP Statistics

LLDP MED Network Policy

Link Layer Discovery Protocol-Media Endpoint Discovery (LLDP-MED), improves information sharing between endpoints and network infrastructure devices. LLDP-MED network policies let endpoints and devices on the network to advertise the VLAN, priority levels, and DSCP values used by a voice or video application. Ports are assigned a network policy on the **LLDP MED Port Settings** page.

To create an LLDP Network Policy, enter the policy number (1 – 64), and select the application type:

guest-voice: Used when there is a separate voice network for visitors (guest users).
guest-voice-signaling: For when the network requires a separate policy for guest voice signaling and guest voice media.
softphone-voice: For softphone voice applications
streaming-video: For multicast video or other streaming video services that require a specific network policy
videoconferencing: For video conferencing applications.
video-signaling: Used to separate video signaling than for the video media. Do not use this application type if both the same network policies apply to both video and video signaling traffic.
voice: if the services, IP telephones, and other appliances support interactive voice services. This is the default application type.
voice-signaling: When there is a different policy for voice signaling than for voice media. Do not use this application type if both the same network policies apply to both voice and voice signaling traffic.

Enter the **VLAN Type**, the **VLAN ID**, **L2 Priority**, and **DSCP** value. Then click **Update Setting**.

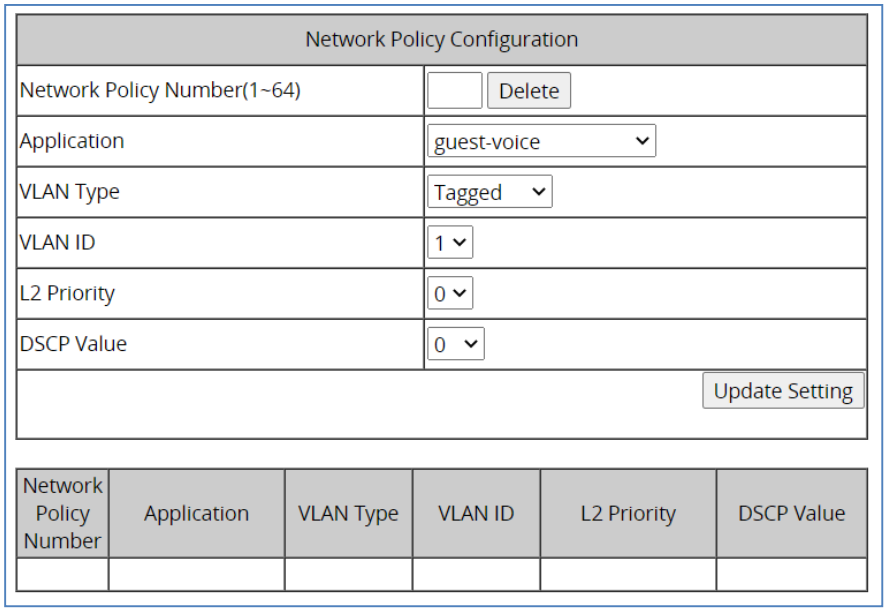


Figure 127: LLDP MED Network Policy

LLDP MED Location ID

A wide array of location information can be configured for each port, and advertised to remote devices. This includes geographical coordinates, ELIN (emergency location identifier number) location, and physical address parameters. This information can be transmitted in calls, a feature especially important for calls to emergency services. All ports may be configured with the location of the switch, or each port may set up to read the location of the remote voice device connected to it.

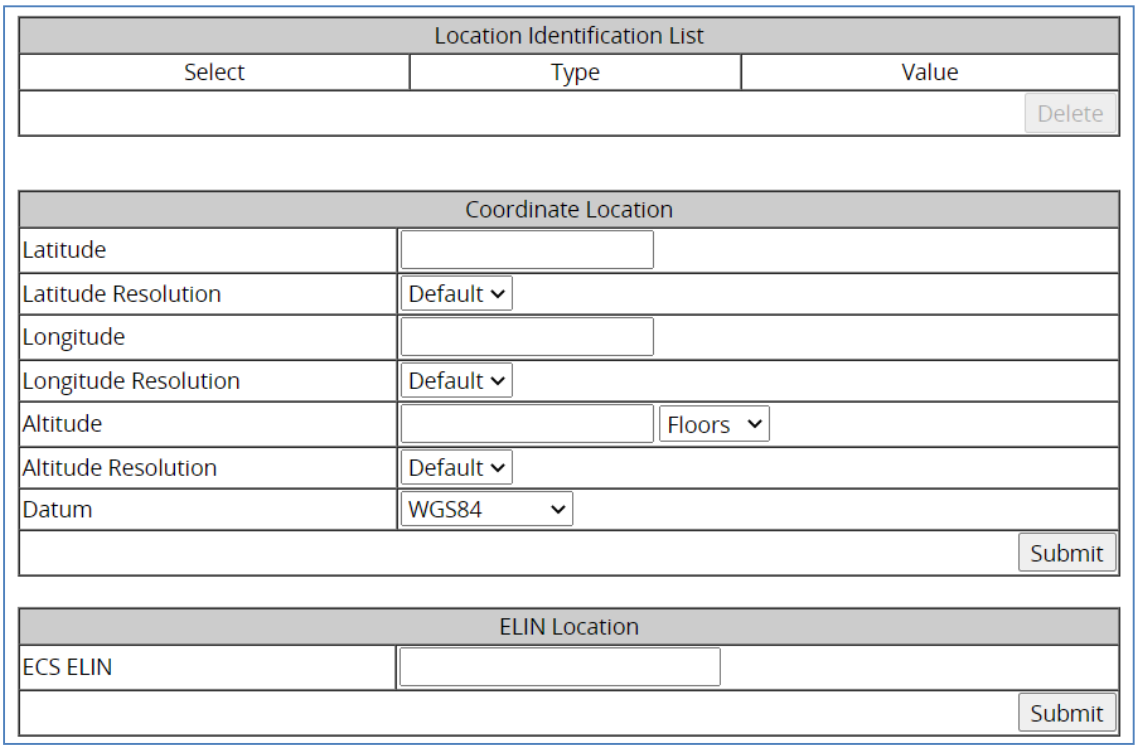


Figure 128: LLDP MED Location ID

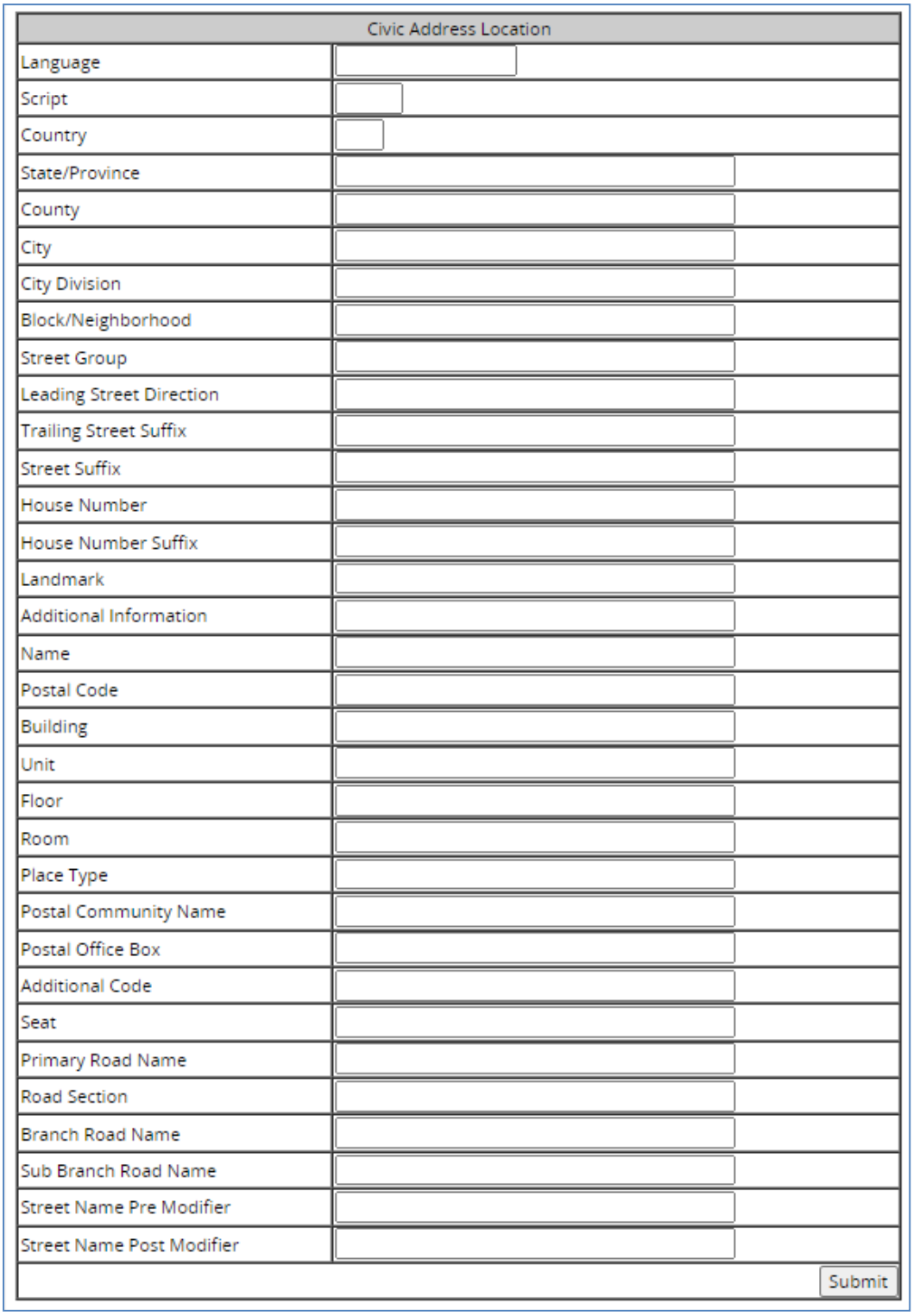
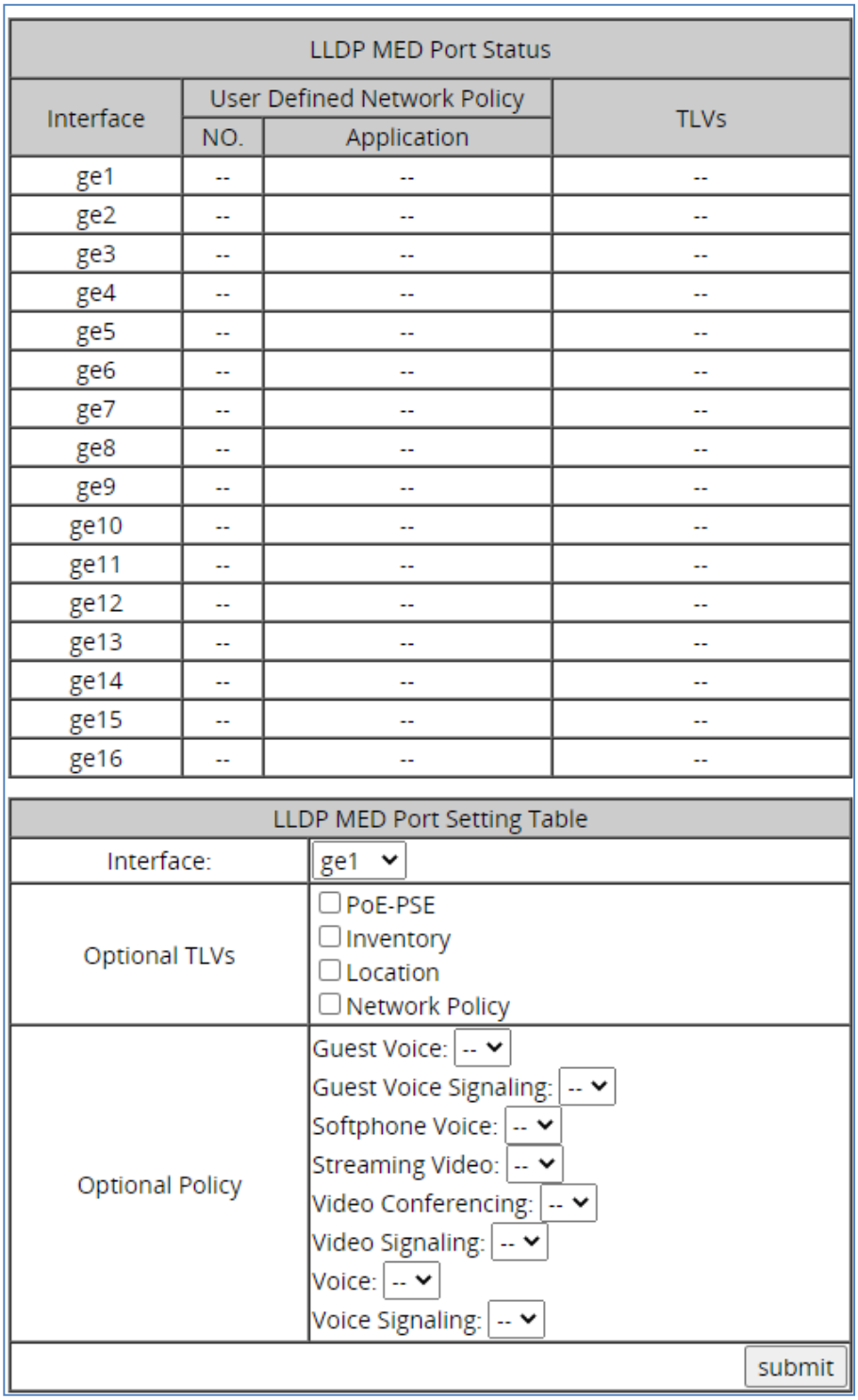


Figure 129: LLDP MED Location ID

LLDP MED Port Settings

On this page you can assign which LLDP TLVs a specific port will use, and assign an optional policy.



LLDP MED Port Status

Interface	User Defined Network Policy		TLVs
	NO.	Application	
ge1	--	--	--
ge2	--	--	--
ge3	--	--	--
ge4	--	--	--
ge5	--	--	--
ge6	--	--	--
ge7	--	--	--
ge8	--	--	--
ge9	--	--	--
ge10	--	--	--
ge11	--	--	--
ge12	--	--	--
ge13	--	--	--
ge14	--	--	--
ge15	--	--	--
ge16	--	--	--

Figure 130: LLDP MED port settings

LLDP Configuration Using CLI Commands

Enable/Disable LLDP

To enable or disable LLDP on the switch use the CLI commands below:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
lldp enable
no lldp enable

Usage Example – Enabling LLDP:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#lldp enable
switch_a(config)#q
switch_a#
```

Usage Example – Disabling LLDP:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#no lldp enable
switch_a(config)#q
switch_a#
```

LLDP Holdtime Multiplier

To modify LLDP holdtime multiplier use the CLI commands below:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **lldp holdtime multiplier <*1-10*>**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#lldp holdtime multiplier 4
switch_a(config)#q
switch_a#
```

LLDP Transmit Interval

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **lldp txinterval <*5-32768*>**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# lldp txinterval 30
switch_a(config)#q
switch_a#
```

Enable/Disable Global LLDP TLVs

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **lldp tlv-global <*TLV*>**

TLV Parameters

TLV Parameters	Description
port-descr	Port Description
sys-name	System Name TLV
sys-descr	System Description TLV
sys-cap	System Capabilities
mgmt-addrs	Management Address
port-vlan-id	Port VLAN ID
mac-phy	MAC/PHY Configuration/Status
port-and-protocol	Port And Protocol VLAN ID
vlan-name	VLAN Name
protocol-identity	Protocol Identity
link-aggregation	(Link Aggregation
max-frame	Maximum Frame Size

Figure 135: TLV Parameters

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# lldp tlv-global mgmt-addrs
switch_a(config)#q
switch_a#
```

Enabling LLDP Transmit on a Port

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **lldp tx-pkt**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a#interface ge1
switch_a(config)# lldp tx-pkt
switch_a(config)#q
switch_a#
```

Enabling LLDP Receive on a Port

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **lldp rcv-pkt**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a#interface ge1
switch_a(config)# lldp rcv-pkt
switch_a(config)#q
switch_a#
```

Enabling LLDP Notify

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **lldp notification**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a#interface ge1
switch_a(config)# lldp notification
switch_a(config)#q
switch_a#
```

Enabling Transmission of the Management IP

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **lldp mgmt-ip vlan <*vlan id*>**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a#interface ge1
switch_a(config)# lldp mgmt-ip vlan 1
switch_a(config)#q
switch_a(config)#q
switch_a#
```

Enabling Specific TLV's on a Port

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **lldp tlv-select <TLV ID>** (see TLV Parameters)

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a#interface ge1
switch_a(config)# lldp tlv-select mgmt-addrs
switch_a(config)#q
switch_a#
```

Enabling LLDP MED TLV's on a Port

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **[no] lldp med-tlv-select <extended-power-via-mdi, inventory, location, network-policy>**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a#interface ge1
switch_a(config)# lldp med-tlv-select location
switch_a(config)#q
switch_a#
```

Set LLDP-MED location information

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **[no] location civic-address [country-subdivision, county, city, city-division, country, block, street, leading-street-direction, trailing-street-suffix, street-suffix, number, number-suffix, landmark, location-information, name, zip, building, unit, floor, room, place-type, postal-community-name, post-box, additional-code, seat]**

[no] location coordinate [latitude, longitude, altitude, alters, datum]

[no] location ecs-elin

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# location civic address Fryeburg
switch_a(config)#q
switch_a#
```

ROUTING

Static Route Configuration

A static route is a predefined path for the flow of network information. In networks with multiple layer three switches and VLANs, or switches with routers, you will need to enable static or dynamic routing.

To navigate to the **Static Route** page:

1. Click on the **+** next to **Routing**.
2. Click on **Static Route**.

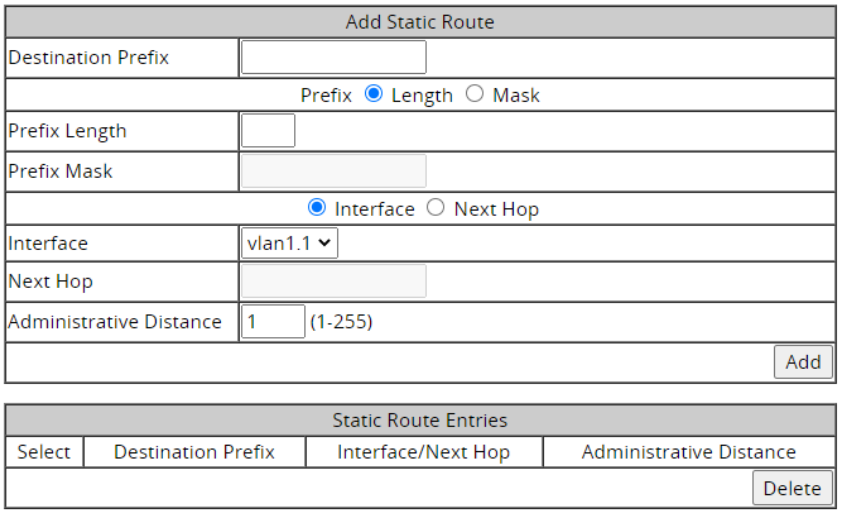


Figure 131: Add Static Route

Creating a Static Route

1. In the Destination field, enter the IP address of the final destination.
2. Choose either Prefix **Length** or **Mask**, and enter the corresponding number in the field below.
3. Select **Interface** or **Next Hop**. For interface, choose the switch VLAN port to be used for the static route. For Next Hop, enter the IP address of the closest router or switch to be used.
4. Enter the Administrative Distance.
5. Click Add to create the static route.

You can delete existing static routes by selecting an entry and clicking the Delete button.

Routing Table

The routing table is a read-only page that shows existing routes. The Routing Table shows:

- **Route Code** – (R)ip, (K)ernel, (C)onnected, (S)tatic, * Default
- **Destination** – Destination IP address
- **Distance/Metric** – Administrative distance/metric.
- **Next Hop** – Next closest router or Layer 3 switch on the route
- **Interface** – Interface used by defined route
- **Up Time** – Length of time the route is active

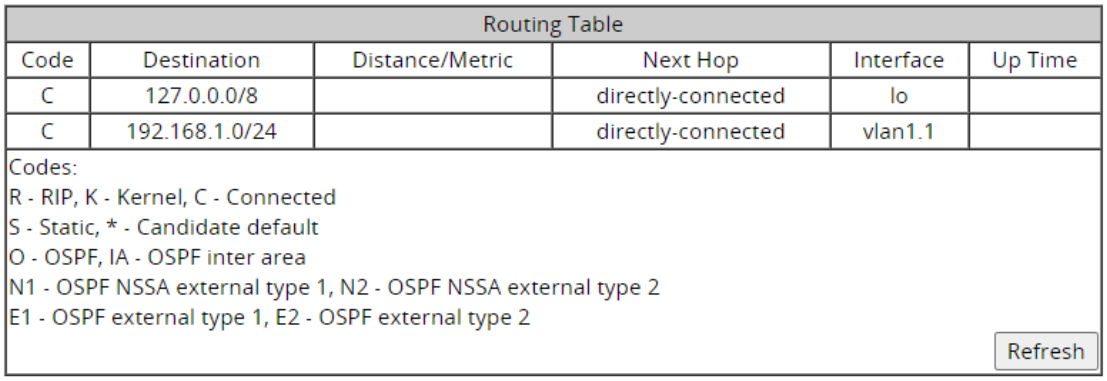


Figure 132: Routing Table

Route Map

Route Maps can be used for both redistribution and policy routing, and thus give you more control over the way packets move around the network.

To navigate to the **Route Map** page:

1. Click on the **+** next to **Routing**.
2. Click on **Route Map**.

To create a new Route Map:

1. Enter a descriptive name in the Name field.
2. Select the type of Route Map – **Permit** or **Deny**.
3. Under Match Clause, choose the data item that the map will match for the route to take effect: **Interface**, **Metric**, **IP address**, or **None**.
4. Select the destination network or next hop router address to match an ACL, in an ACL is to be used.
5. Select the Set Clause data type, and enter the metric or next hop results.
6. Click **Add** to create the Route Map.

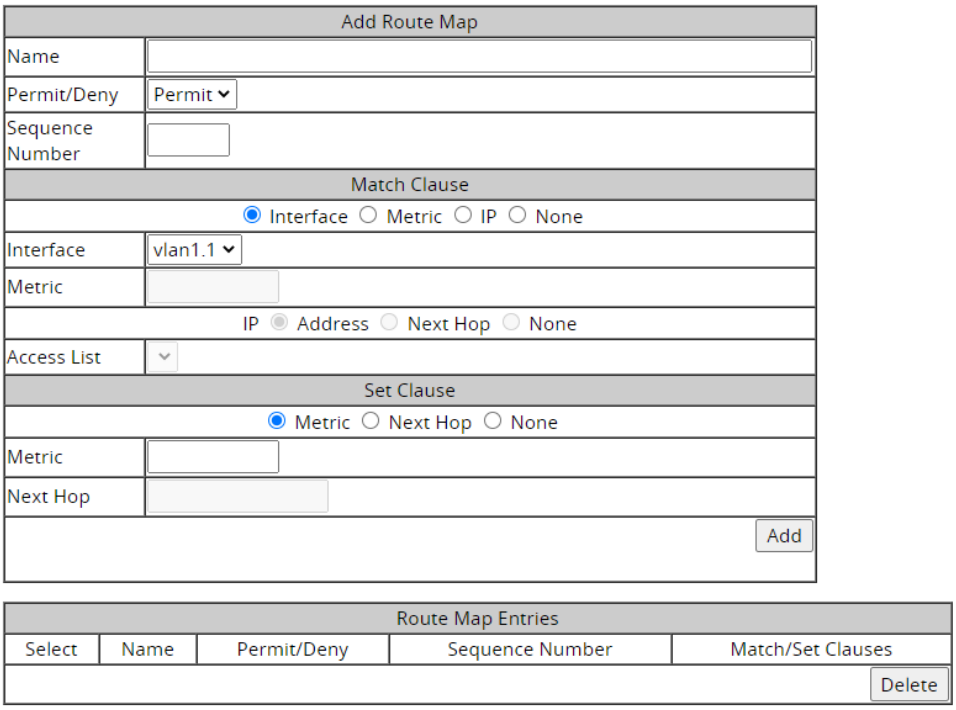


Figure 133: Create/Delete Route Map

Proxy ARP

Proxy ARP allows the switch to answer ARP queries for a network address that is not on that network. The ARP Proxy is aware of the location of the traffic's destination, and offers its own MAC address as the (seemingly) final destination. The "captured" traffic is then typically routed by the Proxy to the intended destination via another interface or via a tunnel. Proxy ARP should be used on networks where IP hosts are not configured with a default gateway.

To navigate to the **Proxy ARP** page:

1. Click on the **+** next to **Routing**.
2. Click on **Proxy ARP**.

To enable Proxy ARP on the switch:

1. Select the VLAN or layer 3 interface on which you want to enable Proxy ARP.
2. Select “enable” from the dropdown menu.
3. Click **Update Setting**.

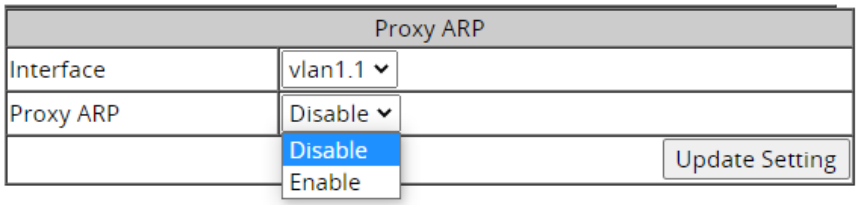


Figure 134: Enable Proxy ARP on an interface

Static Routing with CLI Commands

Create or Delete Static Route

To create (or delete) a static route, use the CLI commands below:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
ip route <destination_network>/<prefix-length> <next-hop_address or exit interface> [<admin_distance>]

no ip route <destination_network>/<prefix-length> <next-hop_address or exit interface> [<admin_distance>]

Usage Example: Set a route to remote network 172.16.3.0 with mask /24 where 192.168.2.4 is the next hop and administrative distance is 150.

```
switch_a(config)#ip route 172.16.3.0/24 192.168.2.4 150
```

Show Existing IP Routes

To show all current IP routes, use the CLI commands below:

CLI Command Mode: **Privileged Exec Mode**

CLI Command Syntax:
show ip route

Usage example:

```
switch_a#show ip route

Codes: K - kernel, C - connected, S - static, R - RIP
       * - candidate default

S       1.111.111.0/24 [1/0] via 172.16.0.200, ge1
S       2.111.111.0/24 [1/0] via 172.16.0.200, ge1
C       127.0.0.0/8 is directly connected, lo
```

```
C       172.16.0.0/24 is directly connected, ge1
C       192.168.2.0/24 is directly connected, ge8
R       192.168.3.0/24 [120/2] via 172.16.0.200, ge1, 00:03:33
R       192.168.4.0/24 [120/12] via 172.16.0.200, ge1, 00:03:23
R       192.168.5.0/24 [120/12] via 172.16.0.200, ge1, 00:03:23
```

Create or Delete Access List

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
access-list <number> <permit or **deny> <host_address> <mask>**

no access-list <number> <permit or **deny> <host_address> <mask>**

Usage Example 1: Deny packets from host 172.16.30.2

```
switch_a(config)#access-list 10 deny host 172.16.30.2
```

Usage Example 2: Deny packets from hosts with IP address 172.16.30.x, where x = any number

```
switch_a(config)#access-list 10 deny host 172.16.30.2 0.0.0.255
```

Configure Route Map

CLI Command Mode: **Global Configuration Mode, Route-Map Configuration Mode**

CLI Command Syntax:
route-map name <permit or deny> <sequence_number>

match ip address access_list <acl_id]

Usage Example:

```
switch_a(config)#route-map FIRST_MAP permit 12
switch_a(config-route-map)#match ip address 12
switch_a(config-route-map)#Set ip next-hop 10.1.2.1
```

Enable Proxy ARP

To enable Proxy ARP on an interface, use the CLI commands below:

CLI Command Mode: **Interface Configuration Mode**

CLI Command syntax:

ip proxy arp

no ip proxy arp

Usage Example:

```
switch_a(config)#vlan database
switch_a(config-vlan)#int vlan1.1
switch_a(config-if)#ip proxy-arp
```

VRRP

VRRP (Virtual Router Redundancy Protocol) is a distance-vector routing protocol that uses hop count as a routing metric. VRRP eliminates the risk of a single point of failure inherent in a static default routing environment. It specifies an election protocol that dynamically assigns responsibility for a virtual router to one of the VRRP routers on a LAN. One of the major advantages of VRRP is that it makes default path available without requiring configuration of dynamic routing on every end-host.

To navigate to the **VRRP** page:

1. Click on the **+** next to **Routing**.
2. Click on **VRRP**.

To configure VRRP:

1. Enter a Virtual Router Identifier (VRID), from 1 – 255.
2. Select the physical interface or VLAN that will be used for virtual routing.
3. Set the preempt mode to specify that the router with the highest priority will function as a backup to the **Master** router when master is unavailable.
4. Configure the priority. If you are configuring the master router, set this value to 255. For other VRRP routers, use a value from from 1 - 254. If the master router fails, the router with the highest priority will become the new master.
5. Set the **Advertisement Interval** (the rate at which the Master router sends advertisement packets to all members of the VRRP group) in seconds. Range is from 1 – 10. These packets indicate that the master router is still operational.
6. Set the Role to either **Master** or **Backup**.
7. Enter the virtual IP address for the VRRP session.
8. Set **Authentication Type** to either **None** or **Text**. This determines whether VRRP protocol exchanges are to be authenticated by a clear text password.
9. If the **Authentication Type** is set to **Text**, then enter the password to be used in the **Authentication Data** field (1 – 16 characters).

10. Select the Circuit Failover Interface from the dropdown menu.
11. Enter the Delta Priority. This is the time in seconds for the master to send VRRP advertisements.
12. Set the **Status** field to **Enable**.
13. Click the **Add** button.

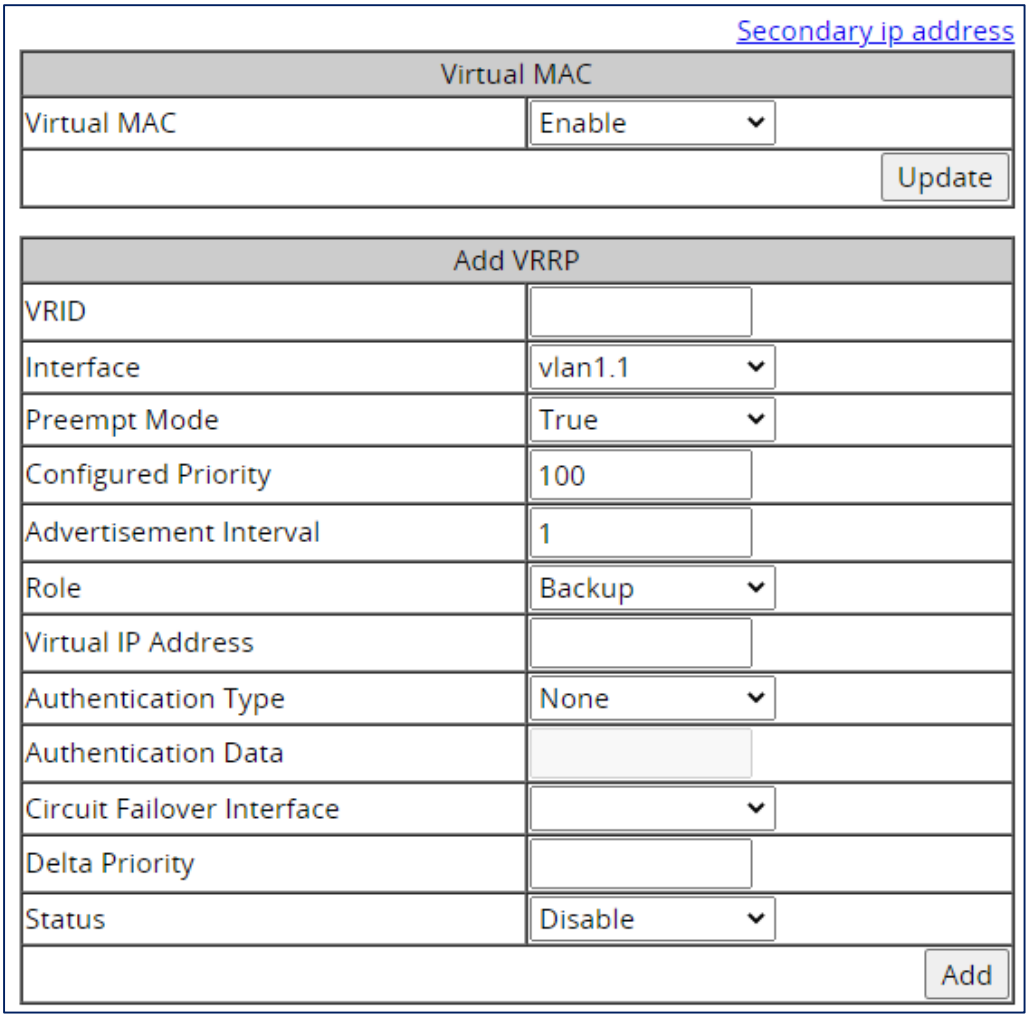


Figure 135: Configure VRRP

VRRP with CLI Commands

Enable or Disable VRRP

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
router vrrp <1-255>

no router vrrp <1-255>

Usage Example: Enable VRRP with VRID (Virtual Router Identifier) of 1

```
switch_a(config)#router vrrp 1
```

Enable or Disable Virtual MAC feature

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
vrrp vmac <enable | disablee>

Usage Example: Enable VRRP with VRID (Virtual Router Identifier) of 1

```
switch_a(config)#vrrp vmac enable
```

Set the Virtual IP Address for the VRRP Session

Use the CLI commands below to set the virtual IP address and the default state (master or backup) of the VRRP router

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
virtual-ip <ip_address/mask> [e.g. 10.10.10.50/24] <master/slave>

Usage Example: Set the virtual IP address to 10.10.10.50, and set the state to **Master**.

```
switch_a(config-router)#virtual-ip 10.10.10.50
master
```

Specify the Interface for Virtual Routing

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
interface <interface name>

Usage Example: Set the interface for VRRP to ge1

```
switch_a(config-router)#interface ge1
```

Configure VRRP Router Priority

The VRRP router that owns the IP address(es) associated with the virtual router must have a priority of 255. VRRP backup routers must have a priority value from 1 to 254.

Use the CLI command below to set the priority.

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
priority <1-255>

Usage Example: Set the priority for the master router to 255

```
switch_a(config-router)#priority 255
```

Enable/Disable Preempt Mode

Set the preempt mode for the VRRP session to specify that the highest priority will function as a backup to master when master is unavailable.

Use the CLI command below.

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
preempt <true/false>

Set the Advertisement Interval

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
advertisement interval <1-10>

Usage Example: Set the advertisement interval to 5 seconds

```
switch_a(config-router)#advertisement-interval 5
```

Enable the VRRP Session

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
enable

Configure Circuit Failover

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
circuit-failover IFNAME <1-253>

<1-253> is the Priority Delta

OSPF

OSPF (Open Shortest Path First) is a link state routing protocol. It is a classless protocol with support for VLSM and CIDR, manual route summarization, incremental updates, and equal cost load balancing. OSPF uses only the interface cost as its metric. The administrative distance default value is 110. OSPF uses multicast addresses 224.0.0.5 and 224.0.0.6 for routing updates.

Devices running OSPF establish neighbor relationships, and then exchange routes. Instead of exchanging routing tables, devices exchange information about known network topologies. Each OSFP enabled device then calculates best routes and adds them to the routing table.

OSPF Configuration

To navigate to the **Configuration** page:

1. Click on the **+** next to **OSPF**.
2. Click on **OSPF Configuration**

To configure OSPF on the managed switch (create an OSPF instance):

1. Enter an **OSPF Process ID** in a range of 1 to 65,535. The Process ID is only used locally, when multiple OSPF instances (with distinct Process IDs) are run on the same device. The Process ID does not need to match that of other devices.
2. Set **Router ID** (A.B.C.D).
3. Select **enable** or **disable** for RFC 1583 Compatibility. Setting this to enable will make the instance compatible with OSPFv2.
4. Set the Delay Time (0~2147483647). Default is 5 seconds.
5. Set the Hold Time (0~2147483647). Default is 10 seconds.
6. Set the Default Metric (0~16777214). Default is 0.

7. Enter the Auto-Cost Reference-Bandwidth (1~4294967). This is the cost in Mbps of an interface that a device advertises to its OSPF neighbors.
8. Click **Add** to create the OSPF instance.

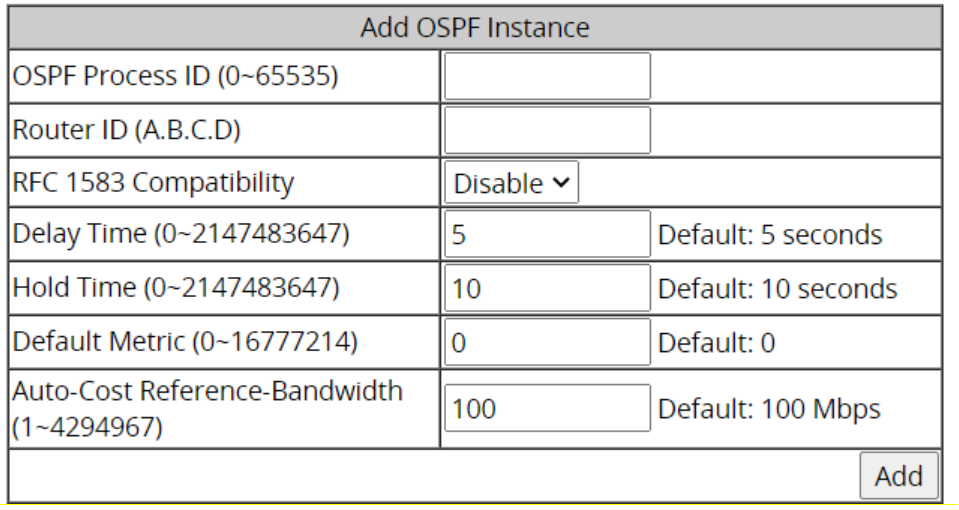


Figure 136: OSPF Configuration

Stub Area Configuration

To navigate to the **Configuration** page:

1. Click on the **+** next to **OSPF**.
2. Click on **Stub area configuration**

External link state advertisements are not flooded to an OSPF Stub Area. Only routing information for destinations within the same stub area and for destinations in other areas within the OSPF domain are sent to the Stub Area. Default routes are used for destinations outside the OSPF domain.

To configure an OSPF Stub Area:

1. Select the OSPF Process ID.
2. Enter the Area ID (0~4294967295 in decimal, A.B.C.D in IP address format)
3. Select **enable** or **disable** for Import Summary LSAs.
4. Set the Default Cost (0~16777215).
5. Click the **Add** button when finished.

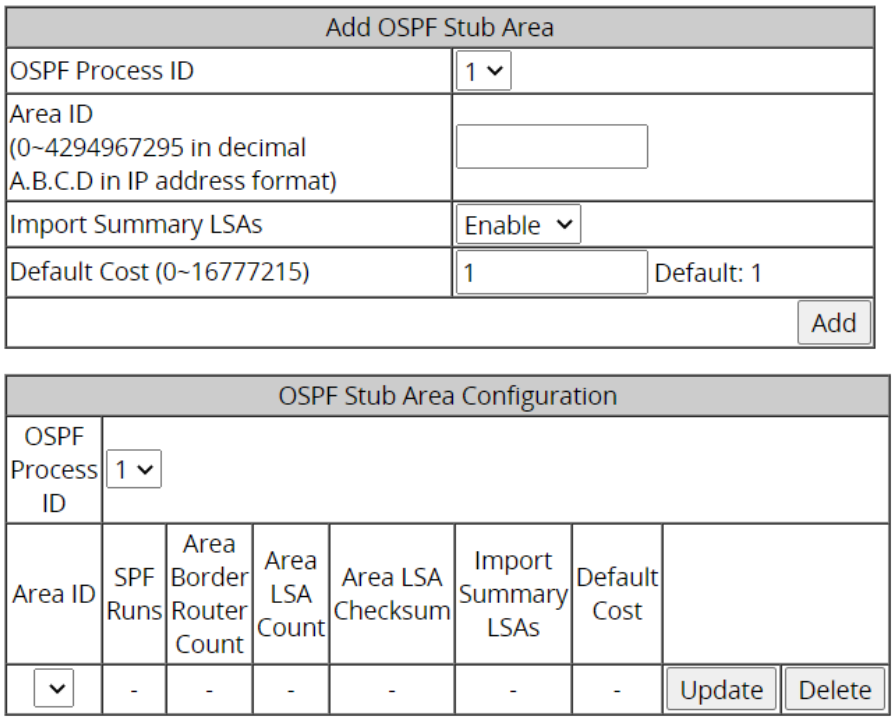


Figure 137: OSPF Stub Area

NSSA Configuration

To navigate to the **NSSA Configuration** page:

1. Click on the **+** next to **OSPF**.
2. Click on **NSSA Configuration.**

An NSSA (Not So Stubby Area) (NSSA) is an OSPF stub area that can also import external route information. External routes from other areas are not flooded into an NSSA, but route information from the NSSA is translated and flooded into other areas (like the backbone).

To configure an NSSA:

1. Select the OSPF Process ID.
2. Enter the Area ID (0~4294967295 in decimal, A.B.C.D in IP address format)
3. Set **Import Summary LSAs** to Yes or No.
4. **Default Information Originate** has three fields: Admin Mode (enable or disable), Metric Value (0~16777214), and Metric Type (1 or 2).
5. Select the **Translator Role** to Never, Candidate, or Always.

6. Set the **Redistribute Mode** to enable or disable
7. Click the **Add** button when finished.

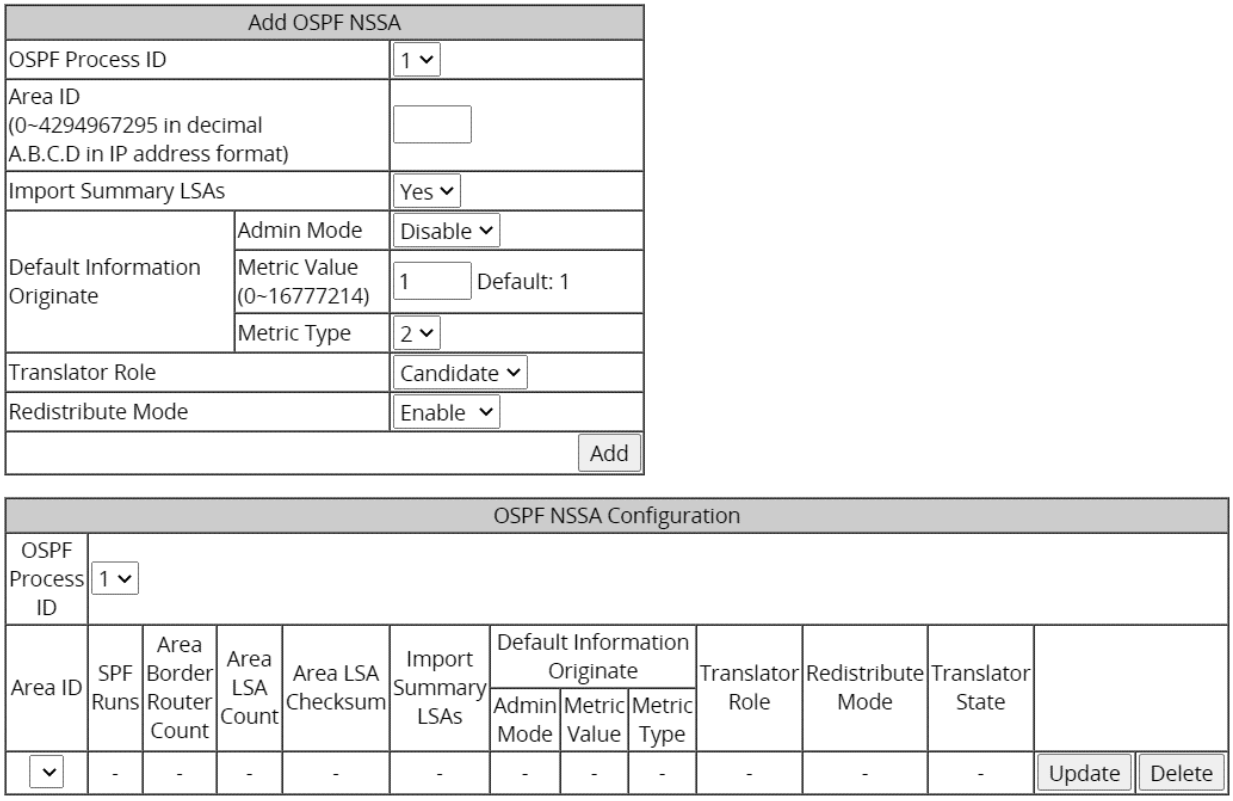


Figure 138: Add an NSSA

OSPF Network

To navigate to the **OSPF Network** page:

1. Click on the **+** next to **OSPF**.
2. Click on **OSPF Network.**

Enable OSPF routing with a specified area ID on interfaces with IP addresses that match the specified network address.

To add an OSPF network:

1. Select the **OSPF Process ID**.
2. Enter the **Area ID**.
3. Enter the Network Prefix in A.B.C.D/X format.

4. Click **Add**.

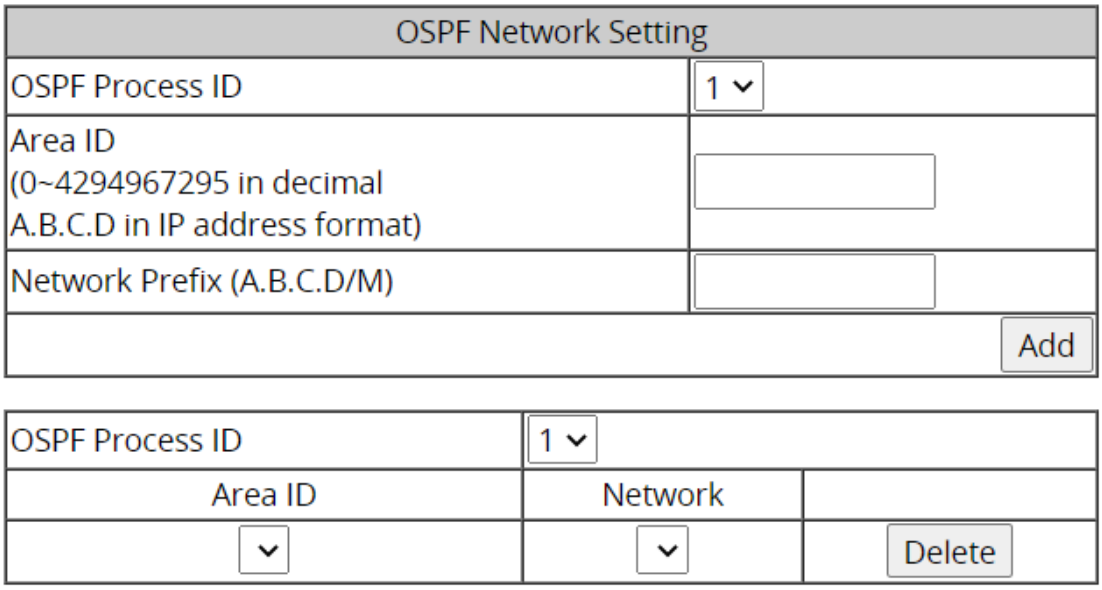


Figure 139: OSPF Network Setting

OSPF Interface

To navigate to the **OSPF Interface** page:

1. Click on the **+** next to **OSPF**.
2. Click on **OSPF Interface.**

OSPF must be enabled on at least one interface in order to be activated on a network. Select the interface from the drop-down menu at the top, and fill out the following fields:

IP Address: (A.B.C.D format)

Router Priority: (0~255) (Default is 1)

Retransmission Interval: (1~65535) (Default is 5 seconds)

Hello Interval: (1~65535) (Default is 10 seconds)

Dead Interval: (1~65535) (Default is 40 seconds)

Transmit Delay: (1~65535) (Default is 1 second)

MTU: (Maximum transmission unit) Ignore (enable or disable)

MTU: Default is 9216

Authentication Type: (None, Simple or MD5)

Authentication Key: (1~8 characters)

MD5 Key ID: (1~255)

MD5 Password: (1~16 characters)

Cost: (1~65535) (Default is 10)

Click the **Update** button when finished.

Configure OSPF Interface	
Interface	
IP Address (A.B.C.D)	
Router Priority (0~255)	1 Default: 1
Retransmission Interval (1~65535)	5 Default: 5 seconds
Hello Interval (1~65535)	10 Default: 10 seconds
Dead Interval (1~65535)	40 Default: 40 seconds
Transmit Delay (1~65535)	1 Default: 1 second
MTU Ignore	Disable
MTU	9216 Default: 9216
Authentication Type	None
Authentication Key (1~8 characters)	
MD5 Key ID (1~255)	
MD5 Password (1~16 characters)	
Cost (1~65535)	10 Default: 10
	Update

Figure 140: Configure OSPF Interface

OSPF Virtual Link

To navigate to the **OSPF Virtual Link** page:

1. Click on the **+** next to **OSPF**.
2. Click on **OSPF Virtual Link.**

All OSPF areas must be connected to the backbone area 0. If this is not physically possible, a Virtual Link can be used. A virtual link is connecting through another area that is connected to area 0.

To create a Virtual Link:

1. Select the **Process ID** for the link.
2. Select the **Area ID**.
3. Enter the **Neighbor Router ID.**

1. Enter the, **Hello** and **Dead Intervals**, and **Transmit Delay**.
4. Enter the Retransmit Interval.

5. Select the **Authentication Type**, and enter the corresponding keys/password in the fields below.

6. Click **Update Setting**. The newly added Virtual Link will be displayed in the table at the bottom of the screen.

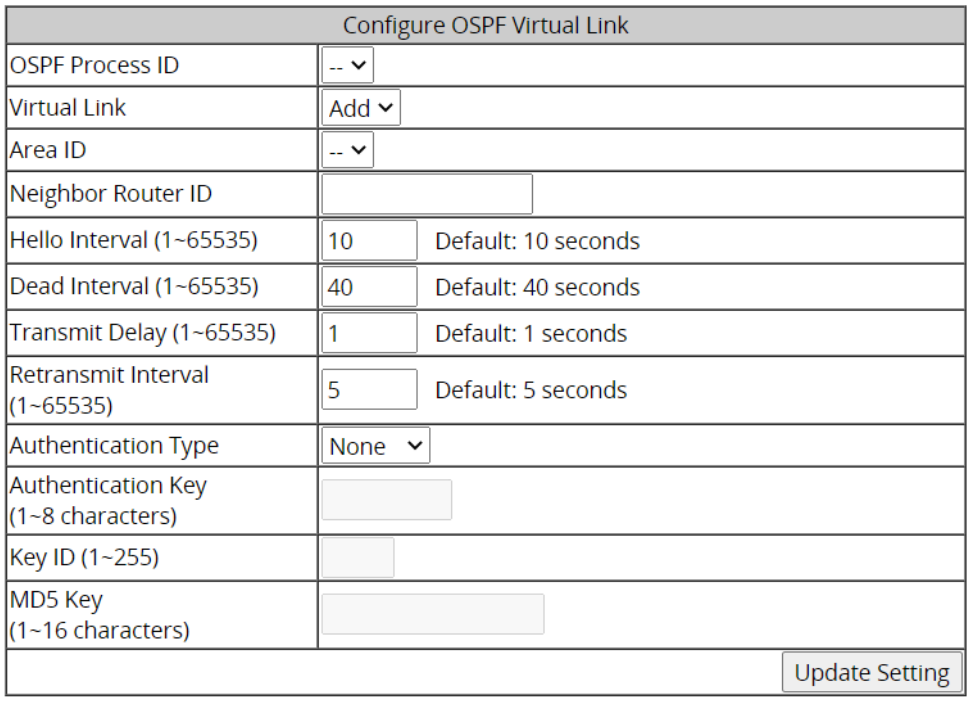


Figure 141: Configure OSPF Virtual Link

OSPF Redistribute

To navigate to the **OSPF Redistribute** page:

1. Click on the **+** next to **OSPF**.
2. Click on **OSPF Redistribute.**

This screen is for redistributing routes from a routing protocol, static route, and kernel route into an OSPF routing table.

1. Select the **Process ID.**
2. Select the protocol type to be redistributed (Connected, Static, RIP).
3. Select the **Route Map.**
4. Enter the **Metric** and **Metric Type**.
5. Enter the **Tag** to be used for fltering, if applicable.
6. Click **Add**. The entry will display in the Redistribute List below.

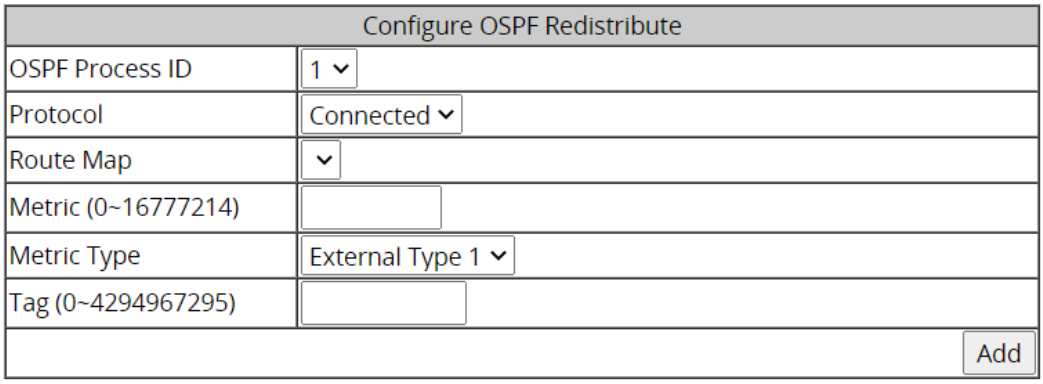


Figure 142: Configure OSPF Redistribute

OSPF Area Range

To navigate to the **OSPF Area Range** page:

1. Click on the **+** next to **OSPF**.
2. Click on **OSPF Area Range.**

Use area range command to consolidate or summarize area routes. Enter the OSPF Process ID, Area ID, and Network Prefix, and set **Advertise** to **enable**. Then click the Add button.

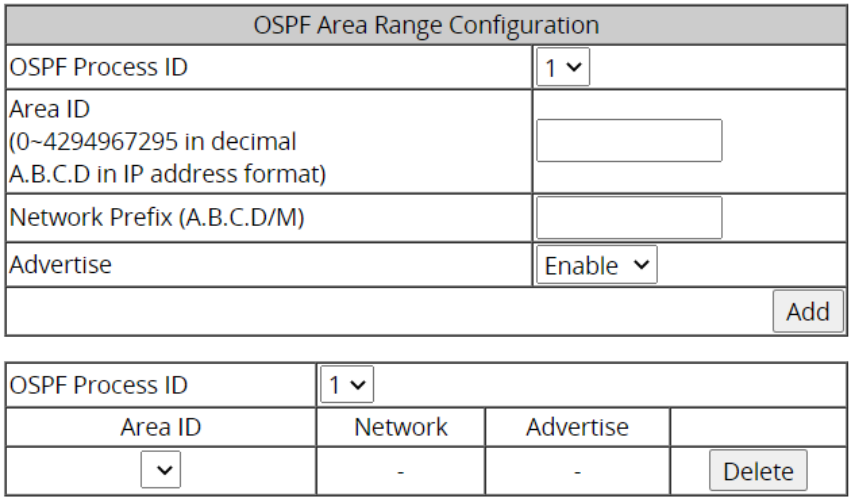


Figure 143: OSPF Area Range

OSPF Neighbor

To navigate to the **OSPF Neighbor** page:

1. Click on the **+** next to **OSPF**.
2. Click on **OSPF Neighbor.**

This is a read only page that shows current OSPF neighbors.

OSPF Route

To navigate to the **OSPF Route** page:

1. Click on the **+** next to **OSPF**.
2. Click on **OSPF Route.**

This is a read only page that shows the OSPF routing table.

OSPF Configuration with CLI Commands

Enable or Disable OSPF

To enable OSPF on the switch, use the CLI commands below

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
[no] router ospf <1-65535>

Parameters <1-65535>: Process ID; unique for each routing process.

Usage Example:

```
switch_a(config)#router ospf 100
switch_a(config-router)#
```

Show OSPF Configuration and Settings

CLI Command Mode: **Privileged Exec Mode**

CLI Command Syntax:
show ip ospf
show ip ospf border-routers
show ip ospf database
show ip ospf interface
show ip ospf neighbor
show ip ospf route
show ip ospf virtual-links

Usage Example:

```
switch_a#show ip ospf neighbor
```

Enable authentication for an OSPF area

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
[no] area (A.B.C.D | <0-4294967295>) authentication

area (A.B.C.D | <0-4294967295>) authentication message-digest

Usage Example:

```
switch_a(config-router)#area 1 authentication message-digest
```

Specify a cost for the default summary route

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
area (A.B.C.D | <0-4294967295>) default-cost <0-16777215>

no area (A.B.C.D | <0-4294967295>) default-cost

Usage Example:

```
switch_a(config-router)#area 1 default-cost 10
```

Configure a filter to advertise summary routes

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
[no] area (A.B.C.D | <0-4294967295>) filter-list access WORD (in | out)

Usage Example:

```
switch_a(config-router)#area 1 filter-list access 1 in
```

Summarize OSPF routes at an area boundary

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
area (A.B.C.D | <0-4294967295>) range A.B.C.D/M

area (A.B.C.D | <0-4294967295>) range A.B.C.D/M advertise

area (A.B.C.D | <0-4294967295>) range A.B.C.D/M not-advertise

no area (A.B.C.D | <0-4294967295>) range A.B.C.D/M

no area (A.B.C.D | <0-4294967295>) range A.B.C.D/M (advertise | not-advertise)

Usage Example:

```
switch_a(config-router)#area 1 range 192.16.0.0/24
```

Set an area as a Not-So-Stubby-Area (NSSA)

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
[no] area (A.B.C.D | <0-4294967295>) nssa

area (A.B.C.D | <0-4294967295>) nssa (translate-candidate | translate-always)

area (A.B.C.D | <0-4294967295>) nssa {translator-role (candidate | always) | stabilityinterval <0-2147483647> | no-redistribution | default-information-originate (metric <0-16777214> | metric-type <1-2> | metric <0-16777214> metric-type <1-2> | metric-type <1-2> metric <0-16777214> |) | no-summary}

no area (A.B.C.D | <0-4294967295>) nssa {translator-role | no-redistribution | defaultinformation-originate | no-summary}

Usage Example:

```
switch_a(config-router)#area 3 nssa translator-role candidate
noredistribution
```

Configure the short-cutting mode of an area

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
area (A.B.C.D | <0-4294967295>) shortcut (default | enable | disable)

no area (A.B.C.D | <0-4294967295>) shortcut

no area (A.B.C.D | <0-4294967295>) shortcut (enable | disable)

Usage Example:
```
switch_a(config-router)# area 1 shortcut default
```

Define an area as a stub area

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
area (A.B.C.D | <0-4294967295>) stub

area (A.B.C.D | <0-4294967295>) stub no-summary

no area (A.B.C.D | <0-4294967295>) stub

no area (A.B.C.D | <0-4294967295>) stub no-summary

Usage Example:
```
switch_a(config-router)# area 1 stub no-summary
```

Configure a link between two separated backbone areas

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
[no] area (A.B.C.D | <0-4294967295>) virtual-link A.B.C.D

area (A.B.C.D | <0-4294967295>) virtual-link A.B.C.D {authentication (messagedigest | null|) | authentication-key LINE | message-digest-key <1-255> md5 LINE | deadinterval <1-65535> | hello-interval <1-65535> | retransmit-interval <1-3600> | transmit-delay <1-3600>}

[no] area (A.B.C.D | <0-4294967295>) virtual-link A.B.C.D {fall-over bfd}

no area (A.B.C.D |<0-4294967295>) virtual-link A.B.C.D {dead-interval | hellointerval | retransmit-interval | transmit-delay | authentication | authenticationkey | message-digest-key <1-255>}

Usage Example:
```
switch_a(config-router)#area 1 virtual-link 10.10.11.50 hello 5 dead
10
```

Control how OSPF calculates the default metric for the interface

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
auto-cost reference-bandwidth <1-4294967>

no auto-cost reference-bandwidth

Usage Example:
```
switch_a(config-router)#auto-cost reference-bandwidth 50
```

Enable / disable RFC 2328 compatibility

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
[no] compatible rfc1583

Usage Example:
```
switch_a(config-router)#compatible rfc1583
```

Create a default external route into an OSPF routing domain

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
default-information originate

default-information originate {metric <0-16777214> | metric-type (1 | 2) | {route-map WORD | always}

no default-information originate

no default-information originate {metric | metric-type | {route-map | always}

Usage Example:
```
switch_a(config-router)#default-information originate always metric 23
metrictype 2 route-map myinfo
```

Set OSPF administrative distances

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
[no] distance <1-255>

[no] distance ospf [external | inter-area | intra-area] <1-255>

Usage Example:
```
switch_a(config-router)#distance 255
```

Configure a stub host entry belonging to a particular area

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
host A.B.C.D area (A.B.C.D | <0-4294967295>)

host A.B.C.D area (A.B.C.D | <0-4294967295>) cost <0-65535>

no host A.B.C.D area (A.B.C.D | <0-4294967295>)

no host A.B.C.D area (A.B.C.D | <0-4294967295>) cost (<0-65535> |)

Usage Example:

```
switch_a(config-router)# host 172.16.10.101 area 2 cost 10
```

Limit number of Database Descriptors (DD) that can be processed concurrently

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
max-concurrent-dd <1-65535>

no max-concurrent-dd

Usage Example:

```
switch_a(config-router)# max-concurrent-dd 4
```

Set maximum number of OSPF areas

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
maximum-area <1-4294967294>

no maximum-area

Usage Example:

```
switch_a(config-router)# maximum-area 5000
```

Specify and configure neighbor routers

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
[no] neighbor A.B.C.D

[no] neighbor A.B.C.D (priority <0-255> | poll-interval <1-2147483647> | cost <1-65535>)

[no] neighbor A.B.C.D (cost <1-65535>)

Usage Example:

```
switch_a(config-router)#neighbor 1.2.3.4 priority 1
```

Enable OSPF routing with a specified area

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
Network address defined using the prefix length:

[no] network A.B.C.D/M area (A.B.C.D | <0-4294967295>) (instance-id <0-255> |)

Network address defined using subnet mask:

[no] network A.B.C.D A.B.C.D area (A.B.C.D | <0-4294967295>) (instance-id <0-255> |)

Usage Example:

```
switch_a(config-router)#network 10.0.0.0/8 area 1.1.1.1
```

Set an OSPF Area Border Router (ABR) type

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
[no] ospf abr-type (cisco | ibm | standard | shortcut |)

Usage Example:

```
switch_a(config-router)#ospf abr-type ibm
```

Specify a router ID for the OSPF process

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
[no] ospf router-id A.B.C.D

Usage Example:

```
switch_a(config-router)#ospf router-id 2.3.4.5
```

Set maximum number of LSAs that can be supported

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
overflow database (<0-4294967294> | asbr-summary | external | network | router | summary) <0-2147483647> <0-65535>

Parameters: <0-2147483647> Maximum number of LSAs

<0-65535> Time to recover (0 not recover)

Usage Example:

```
switch_a(config-router)#overflow database 100
```

Suppress sending Hello packets

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
[no] passive-interface IFNAME

[no] passive-interface (IFNAME | A.B.C.D)

Usage Example:
```
switch_a(config-router)#passive-interface ge10
```

Redistribute routes into an OSPF routing table

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
redistribute (connected | static | rip) (<1-65535> |)) {metric <0-16777214> | metric-type (1 | 2) | route-map WORD | tag <0-4294967295>}

no redistribute (connected | static | rip (<1-65535> |)) {metric | metric-type | route-map | tag}

Usage Example:
```
switch_a(config-router)#redistribute bgp metric 12
```

Summarize or suppress external routes

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
[no] summary-address A.B.C.D/M (not-advertise | tag <0-4294967295>|)

no summary-address A.B.C.D/M

Usage Example:
```
switch_a(config-router)#summary-address 10.10.10.0/24 not-advertise
```

Adjust route-calculation timers

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
timers spf <0-2147483647> <0-2147483647>

no timers spf

Usage Example:
```
switch_a(config-router)#timers spf exp 10000 25000
```

Set OSPF authentication method on an interface

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
ip ospf authentication (null | message-digest |)

ip ospf A.B.C.D authentication (null | message-digest |)

no ip ospf (A.B.C.D |) authentication

Usage Example:

```
switch_a(config-if)#ip ospf authentication null
```

Specify OSPF authentication password for neighboring routers

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
ip ospf (A.B.C.D|) authentication-key LINE

no ip ospf (A.B.C.D|) authentication-key

Usage Example:

```
switch_a#configure terminal
switch_a(config)#router ospf 100
switch_a(config-router)#network 10.10.10.0/24 area 0
switch_a(config-router)#area 0 authentication
switch_a(config-router)#exit
switch_a(config)#interface ge24
switch_a(config-if)#ip ospf 12.10.10.2 authentication-key testkey
```

Specify the cost of the link-state metric in a router-LSA

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
ip ospf (A.B.C.D |) cost <1-65535>

no ip ospf (A.B.C.D |) cost

Usage Example:

```
switch_a(config-if)# ip ospf 10.10.12.12 cost 200
```

Turn on LSA database-filter

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
ip ospf (A.B.C.D|) database-filter all out

no ip ospf (A.B.C.D|) database-filter

Usage Example:
```
switch_a(config-if)# ip ospf database-filter all out
```

Set interval after which a neighbor is declared dead

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
ip ospf (A.B.C.D |) dead-interval <1-65535>

no ip ospf (A.B.C.D |) dead-interval

Usage Example:
```
switch_a(config-if)# ip ospf dead-interval 100
```

Disable OSPF on an interface

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
[no] ip ospf disable all

Usage Example:
```
switch_a(config-if)# ip ospf disable all
```

Set Hello packet interval

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
ip ospf (A.B.C.D |) hello-interval <1-65535>

no ip ospf (A.B.C.D |) hello-interval

Usage Example:
```
switch_a(config-if)# ip ospf hello-interval 10
```

Register an MD5 key for OSPF authentication

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
ip ospf (A.B.C.D |) message-digest-key <1-255> md5 LINE

no ip ospf (A.B.C.D |) message-digest-key <1-255>

Usage Example:
```
switch_a(config-if)#ip ospf authentication message-digest
switch_a(config-if)#ip ospf message-digest-key 1 md5 passwordsample
```

Set MTU size for OSPF to construct packets

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
ip ospf mtu <576-65535>

no ip ospf mtu

Usage Example:
```
switch_a(config-if)# ip ospf mtu 10000
```

Ignore MTU in DBD packets

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
ip ospf (A.B.C.D|) mtu-ignore

no ip ospf (A.B.C.D|) mtu-ignore

Usage Example:
```
switch_a(config-if)# ip ospf mtu-ignore
```

Set the OSPF network type

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
ip ospf network (broadcast | non-broadcast | point-to-multipoint | point-to-point)

ip ospf network point-to-multipoint non-broadcast

no ip ospf network

Usage Example:
```
switch_a(config-if)# ip ospf network point-to-point
```

Set designated router priority

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
ip ospf (A.B.C.D|) priority <0-255>

no ip ospf (A.B.C.D|) priority

Usage Example:
```
switch_a(config-if)# ip ospf priority 20
```

Set time between retransmitting lost link state advertisements

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
ip ospf (A.B.C.D |) retransmit-interval <5-65535>

no ip ospf (A.B.C.D |) retransmit-interval

Usage Example:
`switch_a(config-if)#` **`ip ospf retransmit-interval 20`**

Set the link state transmit delay

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
ip ospf (A.B.C.D |) transmit-delay <1-65535>

no ip ospf (A.B.C.D |) transmit-delay

Usage Example:
`switch_a(config-if)#` **`ip ospf transmit-delay 5`**

Configure a distribution list

CLI Command Mode: **Router Configuration Mode**

CLI Command Syntax:
distribute-list <list> <in/out>

Usage Example:
`switch_a(config-router)#` **`distribute-list 1300 in`**

RIP

The Routing Information Protocol (RIP) is a distance-vector routing protocol that uses hop count as a routing metric. RIP prevents routing loops by setting a limit on the number of hops allowed in a path from source to destination.

RIP General Settings

To navigate to the **General Settings** page:

1. Click on the **+** next to **RIP**.
2. Click on **RIP General Settings**

To enable and configure RIP on the managed switch:

1. Set the Router RIP field to Enable.

2. Choose RIP version 1 or 2.
3. Set the Default Metric value in the range of 1 to 16.
4. Set the Distance from 1 to 255 (Default value is **120**)
5. Set the timings for the Routing Table Update Timer, the Routing Information Timeout Timer, and the Garbage Collection Timer (Default values are 30, 180, and 120 seconds respectively).
6. Click Update Setting to start RIP with the set values.

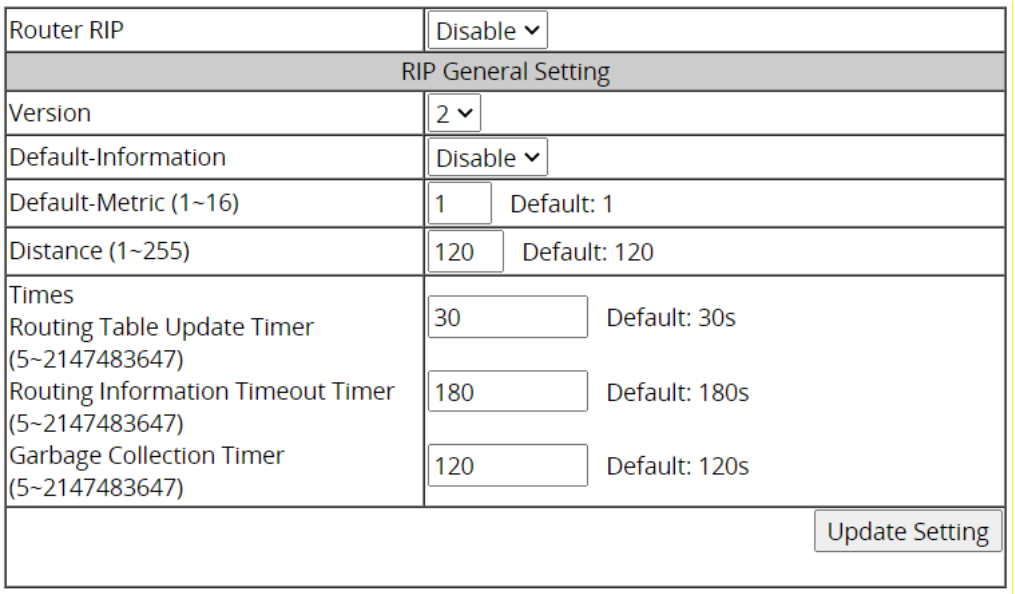


Figure 144: RIP General Settings

RIP Port Settings

To configure RIP port settings:

1. Select the interface.
2. Set the RIP receive version (1, 2, or both)
3. Set Receive packets to enable or disable
4. Set the Send Version to 1, 2, 1-compatible, or both.
5. Set Send Packet to Enable or Disable.
6. For the Split Horizon Field, select enable, disable, or poison reverse.

7. Set the Authentication Mode to disable, MD5, or simple password.
8. If the Authentication Mode is MD5 or Simple Password, set the Authentication Key (1 – 16 characters).
9. Click **Update Setting**

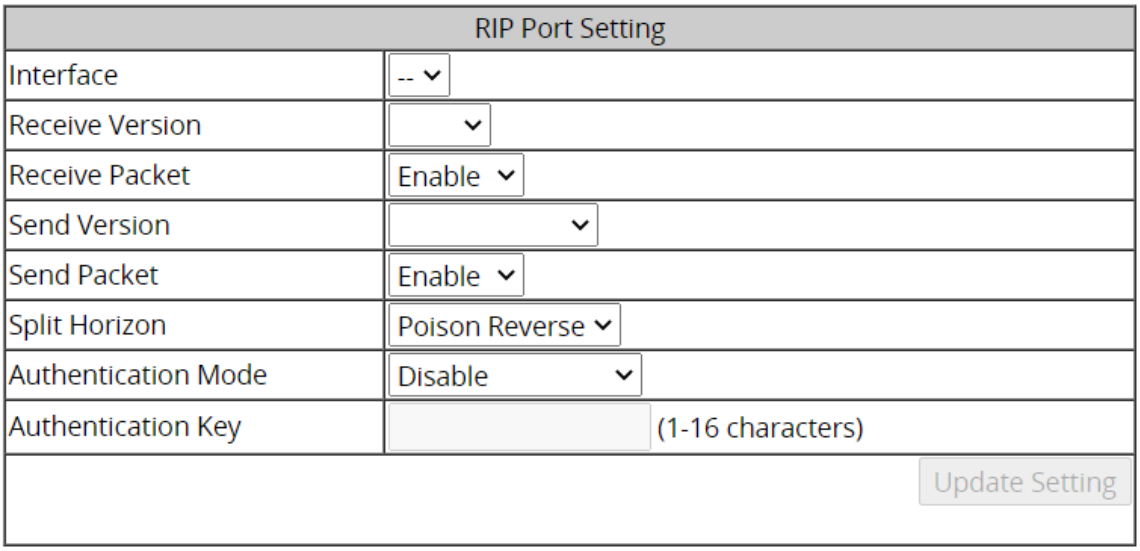


Figure 145: RIP Port Settings

RIP Route

The RIP route table is a read-only page that shows existing RIP routes. The Routing Table fields are:

- **Route Code** – (R)ip, (K)ernel, (C)onnected, (S)tatic
- **Network** – IP address of destination network
- **Next Hop** – Next closest router or Layer 3 switch towards destination
- **Metric** – Number of hops
- **From** – IP address of source router
- **I/F** – Interface
- **Time** – Duration of time since last update

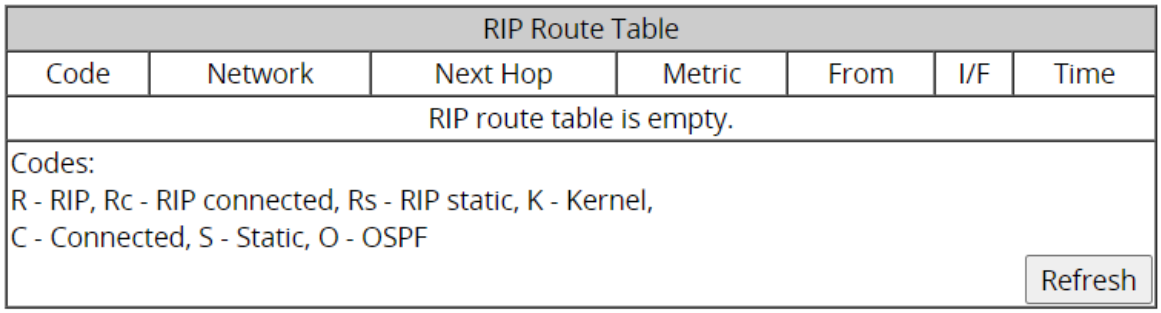


Figure 146: RIP Route Table

RIP Network

On the RIP Network screen, you can add or delete subnet addresses and interfaces to be advertised by RIP.

To navigate to the **RIP Network** page:

1. Click on the **+** next to **RIP**.
2. Click on **RIP Network**

To add subnets or interfaces:

1. Enter the subnet address and prefix length, or choose the interface from the drop-down menu.
2. Click Add button.

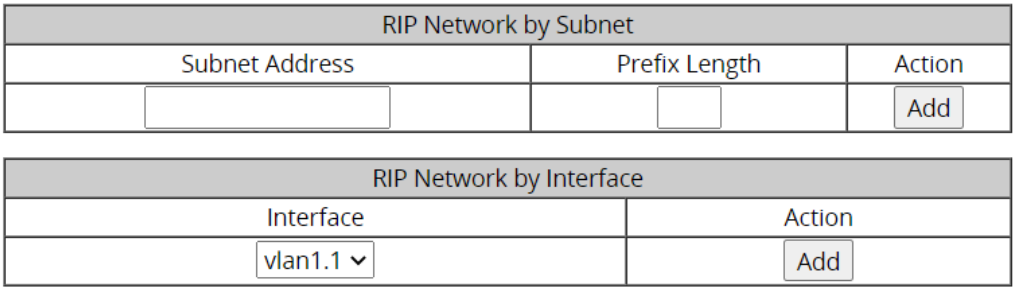


Figure 147: RIP Network Additions and Deletions

RIP Neighbor

The RIP Neighbor screen is used to add/delete RIP neighbor IP addresses. Add the IP address of neighboring routers and layer 3 switches, and click Add. Select existing neighbors from the list at the bottom and click Delete to remove them.

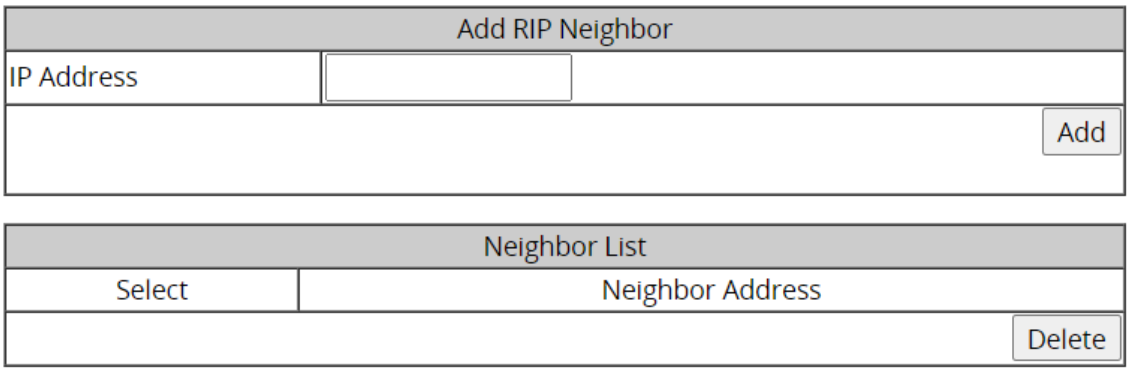


Figure 148: RIP Neighbor Addition and Deletion

Add or Delete RIP Passive Interface

On the RIP Passive screen, you can select an interface to be “passive,” that is, to prevent the RIP routing process from sending multicast/broadcast updates on that interface. Select the desired interface from the drop-down menu and click Add to make that interface passive. You can select and delete passive interfaces from the Passive Interface List at the bottom. Doing so will return them to send multicast/broadcast updates normally.

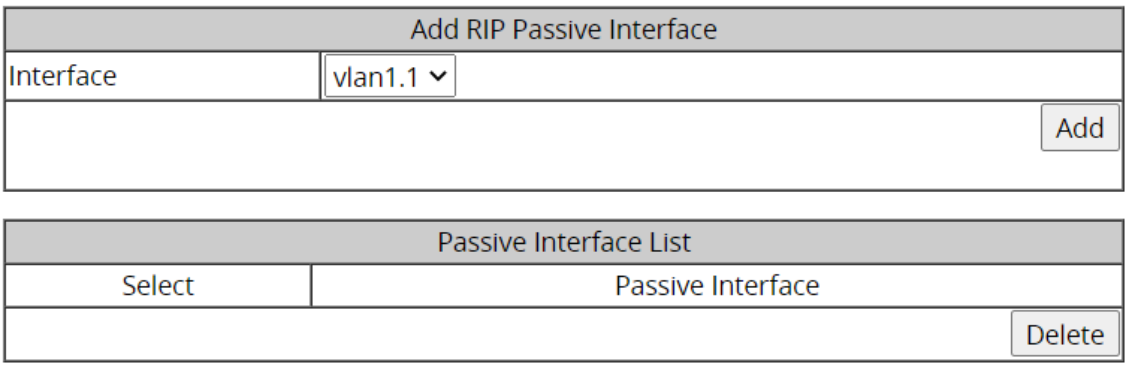


Figure 149: Set and Delete Passive RIP interfaces

RIP Redistribute

Redistribution is using a routing protocol to advertise routes that have been learned by another routing protocol, static routes, or directly connected routes. To add an item to the redistribute list, select the protocol (**connected** or **static**), a route map that has been previously defined, and the desired metric, then click the Add button.

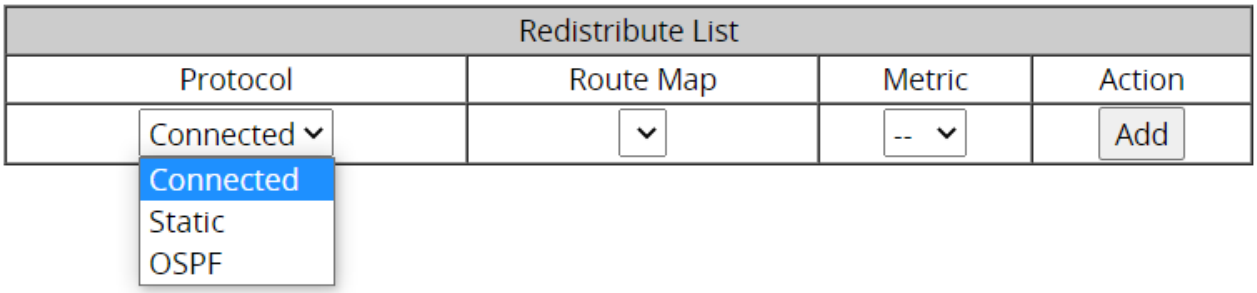


Figure 150: Add or Delete Items to Redistribute List

RIP Configuration with CLI Commands

Enable or Disable RIP

CLI Command Mode: **Global Configuration Mode, Router Configuration**

CLI Command Syntax:
router rip

Version 2

No router rip

Usage Example: Enable RIP version 2

```
switch_a(config)#router rip
switch_a(config-router)#version 2
```

Enable RIP Routing on a Specific Network

CLI Command Mode: **Router Configuration**

CLI Command Syntax:
network <submask>

Usage Example: Enable RIP on 2.2.2.0 255.255.255. 0 and 192.168.20.0 255.255.255.0

```
switch_a(config-router)#network 2.2.2.0/24
switch_a(config-router)#network 192.168.20.0/24
```

Show RIP Routing Table

CLI Command Mode: **Privileged Exec Mode**

CLI Command Syntax:
show ip rip

show ip interface brief

Define RIP Neighbor

CLI Command Mode: **Router Configuration**

CLI Command Syntax:
neighbor <ip address>

no neighbor <ip address>

Set Interface to Passive

Set an interface to passive, use the CLI commands below:

CLI Command Mode: **Router Configuration**

CLI Command Syntax:
passive-interface <interface>

no passive-interface <interface>

RIP Default Metric

To create a default RIP metric for redistributed routes, use the CLI commands below:

CLI Command Mode: **Router Configuration**

CLI Command Syntax:

default-metric <value>

no default-metric

RIP Send Version

To specify a RIP version on an interface basis, use the CLI commands below:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:

ip rip send version <1,2>

no ip rip send version <1,2>

Redistribute

To redistribute routes from one routing domain to another, use the CLI commands below:

CLI Command Mode: **Router Configuration**

CLI Command Syntax:
redistribute (connected | static) [metric <0-16>] [route-map map_name]

Usage Example:

```
switch_a(config-router)#redistribute static metric 10
```

RIP Default Route

To generate a default route into the local RIP domain:

CLI Command Mode: **Router Configuration**

CLI Command Syntax:
default-information originate

no default-information originate

Define RIP Administrative Distance

To define the administrative distance assigned to routes by RIP, use the CLI commands below:

CLI Command Mode: **Router Configuration**

CLI Command Syntax:
distance <admin-distance value>

no distance

Define RIP Timers

To define the RIP network timers, use the CLI commands below:

CLI Command Mode: **Router Configuration**

CLI Command Syntax:
timers basic <update> <invalid> <flush>

no timers basic

Description of parameters:

- **Update**: Rate (in seconds) at which updates are sent. Default is 30 seconds.
- **Invalid**: Interval (in seconds) after which a route is declared invalid. The interval should be at least three times the value of update time. Default is 180 seconds.
- **Flush**: Number of seconds that must pass before route is removed from routing table. Default is 240 seconds.

Usage Example:

```
switch_a(config-router)#timers basic 30 180 120
```

RIP Authentication

To configure text or MD5 authentication for RIP:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
ip rip authentication mode <md5 | text>

Usage Example:

```
switch_a(config-if)#ip rip authentication mode md5
```

OTHER PROTOCOLS

IGMP Snooping

The settings in the IGMP Snooping feature of the EtherWAN switch controls how the switch forwards multicast packets.

General Overview

The switch has been outfitted with the IGMP Snooping function in three modes:

- **Disabled:**
    - The switch will forward all multicast packets according to the **Forced Forwarding Port** setting based on the following rule:
        - All multicast packets will be forwarded to only the port specified by either the **PassiveForwardMode** or the **ForcedForwardMode** function.
- **Passive mode:**
    - The switch will forward any multicast packets that have known receivers to the known multicast receiver ports only.
    - The switch will forward any unknown multicast packets (multicast packets without any known receivers) according to the **Forced Forwarding Port** setting based on the following rule:
        - When there is no Querier Port (a port that receives IGMP queries) present all unknown multicast packets will be forwarded to the port specified by either the **PassiveForwardMode** function or the **ForcedForwardMode** function.
        - When there is a Querier port present, the switch will forward all unknown multicast packets to the Querier port. In addition, all unknown multicast packets will be forwarded to the port specified by the **ForcedForwardMode** function as well.
- **Querier mode:**
    - The switch will forward any multicast packets that have known receivers to the known multicast receiver ports only.
    - The switch will forward any unknown multicast packets according to the **Forced Forwarding Port** setting based on the following rule:
        - All unknown multicast packets will be sent to only the port specified by the **ForcedForwardMode** function.

- The switch will also transmit IGMP Queries to the specified VLAN and according to the specified IGMP Query parameters.

Enabling the IGMP Snooping Modes

To navigate to the **IGMP Snooping** page:

1. Click on the **+** next to **Other Protocols**.
2. Click on **IGMP Snooping**.

To put the IGMP Snooping feature in the correct Mode, follow the steps below:

- Choose the appropriate choice from the dropdown list next to **IGMP mode**
- Click on the **Update Setting** button (See Figure 156)

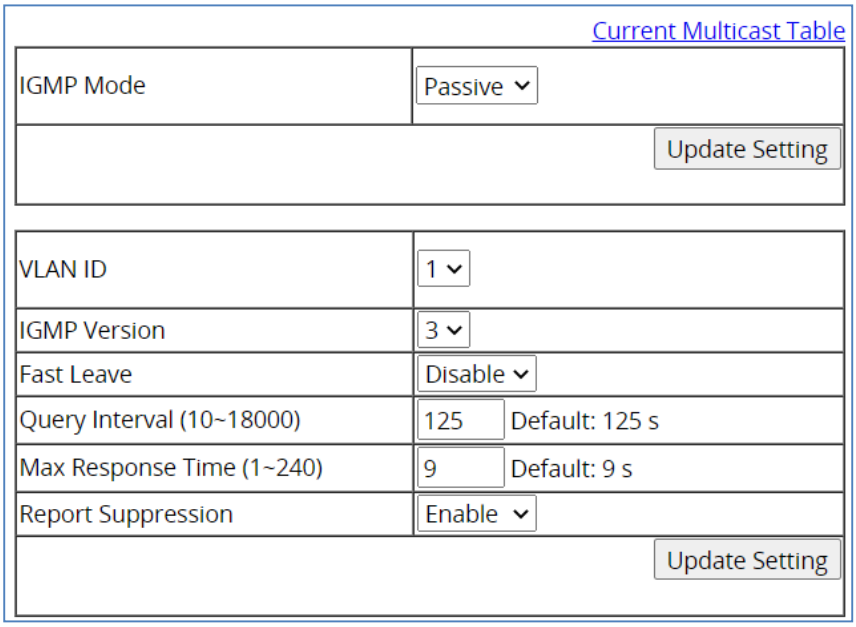


Figure 156: IGMP Mode

Configuring IGMP Snooping General properties

To navigate to the **IGMP Snooping** page:

1. Click on the **+** next to **Other Protocols**.
2. Click on **IGMP Snooping**.

To configure the general features for IGMP Snooping in either the **Passive** or **Querier** mode, follow the steps below (see Figure 157):

1. From the dropdown list next to **VLAN ID**, choose the VLAN that you want the IGMP Snooping process to run on.
2. From the dropdown list next to **IGMP Version**, choose the correct IGMP version to be run on this VLAN. This setting must match the IGMP version being used by the IGMP querier and the IGMP client on the network.
3. Choosing the appropriate choice (Enable or Disable) from the dropdown list next to **Fast Leave**.
    - If this feature is enabled on the switch, and the switch receives a request to leave a multicast stream on a port, then the switch will drop this multicast stream on that port without checking to see if there are any other multicast clients on that port that might still be interested in receiving this multicast stream. This allows the multicast stream to disappear from a port much faster.
2. Next, click on the **Update Setting** button

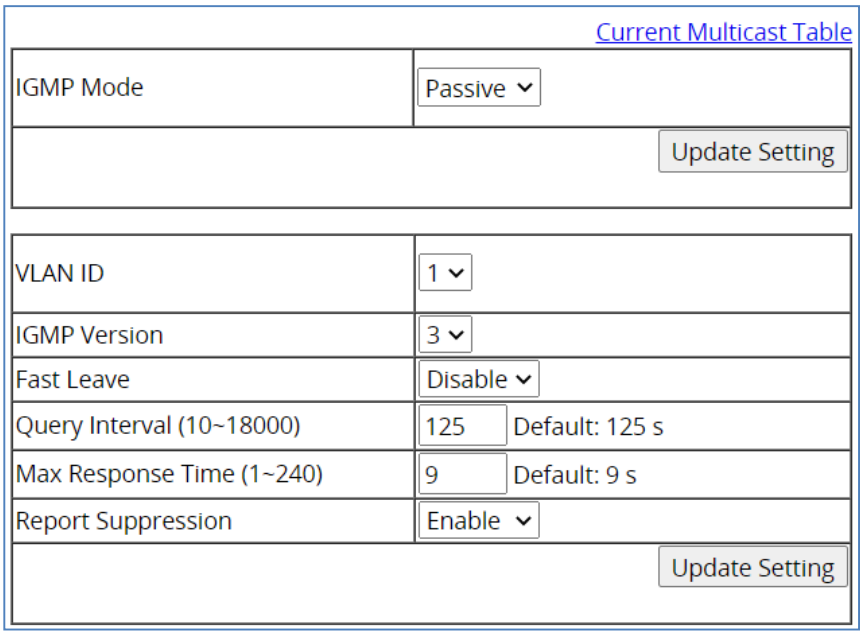


Figure 151: IGMP General Properties

Configuring IGMP Passive Mode Specific properties

To navigate to the **IGMP Snooping** page:

1. Click on the **+** next to **Other Protocols**.
2. Click on **IGMP Snooping**.

To configure specific properties for IGMP Passive Mode, follow the steps below.

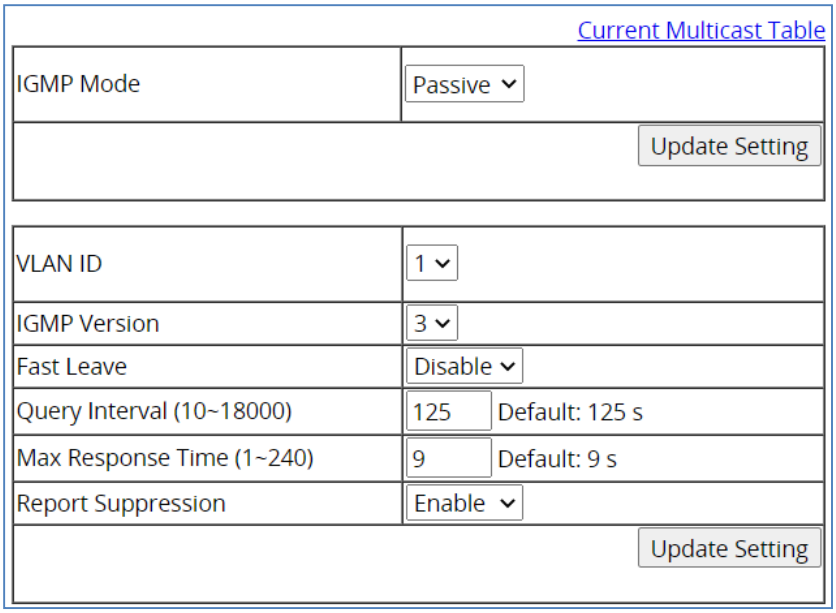


Figure 152: IGMP Passive Mode

1. From the dropdown list next to **VLAN ID**, choose the VLAN for which you wish to configure the Report Suppression feature.
2. Choose **Enable** or **Disable** in the dropdown list next to **Report Suppression**. (**Note**: if the switch is not in **Passive** mode, then this feature will have no effect.)

Note: If you are using IGMP version 1 or 2, the **Query Interval**, and the **Max Response Time** setting must be configured even if you are not configuring IGMP Querier mode. For IGMP version 1 and 2, the membership registration timer (used to time out the membership status on each port) is based on these two parameters on the local switch. These two parameters should configure to match that of the current active IGMP Querier. The formula for the membership registration timer is: 2 X query-interval + max-response-time = Timeout period.

Configuring IGMP Querier Mode Specific properties

To navigate to the **IGMP Snooping** page:

1. Click on the **+** next to **Other Protocols**.
2. Click on **IGMP Snooping**.

To configure specific properties for IGMP Querier Mode, follow the steps below (see Figure 159):

1. In the text box next to **Query Interval,** enter a value between 10 and 18000

- This value will represent the time interval, in seconds, between any two queries that the switch scents on to the network. It is recommended that you use the default setting of 125 seconds that are according to the IGMP standard.

2. In the text box next to **Max Response Time**, enter a value between 1 and 240.
    - This value represents the maximum time in seconds that a multicast client will have to respond to an IGMP query. Any response received after this time will not be accepted by the Querier. It is recommended that you use the default setting of 10 seconds according to the IGMP standard.

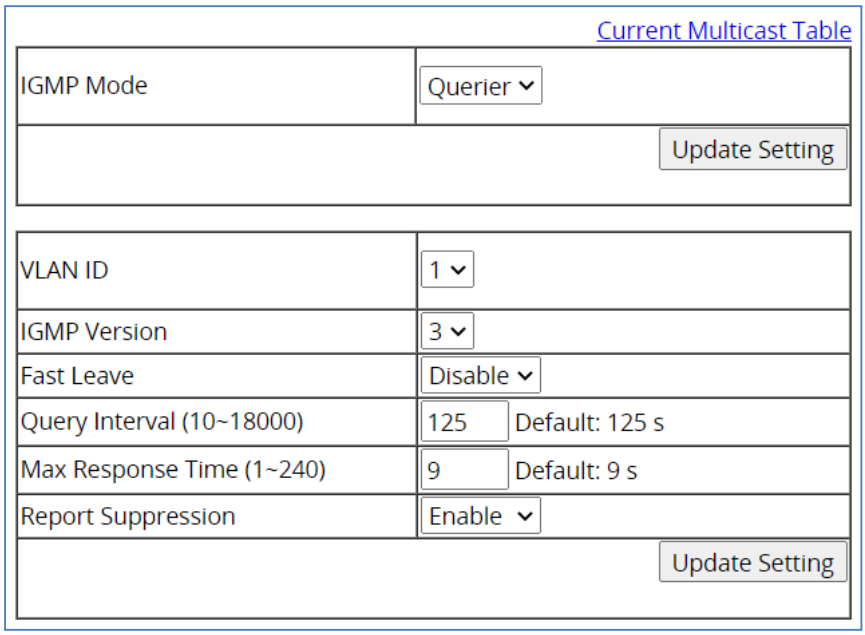


Figure 153: Querier Mode Properties

Configuring IGMP Unknown Multicast Forwarding

To navigate to the **IGMP Snooping** page:

1. Click on the **+** next to **Other Protocols**.
2. Click on **IGMP Snooping**.

With IGMP enabled, the EtherWAN switch will transmit all multicast packets to their only multicast receiver ports. However, some multicast packets will not have any known multicast receiver ports either due to IGMP Snooping being disabled on the switch, or because no multicast receiver has sent IGMP requests for these multicast packets. The multicast packets in these scenarios are referred to as **unknown multicast packets**. You can use the **Passive Mode Forwarding Port** section of the IGMP Snooping configuration page to control how the

switch will forward these unknown multicast packets under different IGMP Snooping modes of the switch (see Figure 160).

Disabled Mode Forwarding Port Configuration

When IGMP is in Disabled Mode, all multicast packets are unknown multicast packets, and by default all unknown multicast packets are forwarded to all the ports of the switch. To modify the default behavior and to control how the switch will forward unknown multicast packets when the switch is in **IGMP Snooping Disabled mode**:

1. Select either the **PassiveForwardMode** or the **ForceForwardMode** radio button.
2. Make sure that only the ports that you would like to have the **unknown multicast packets** to be forwarded to, have a check mark next to it.
3. Then click on the **Update Setting** button.

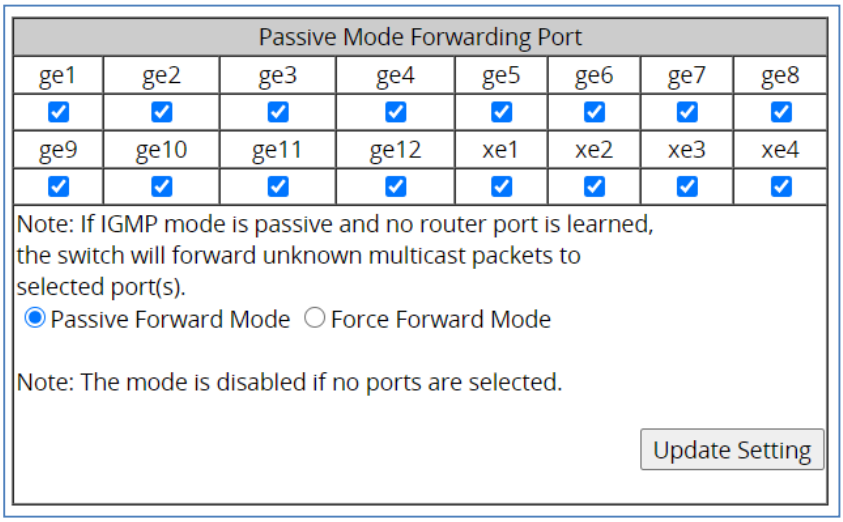


Figure 154: Disabled Mode Forwarding Port

Passive Mode Forwarding Port Configuration

You can control how the switch forwards unknown multicast packets under **IGMP Passive mode** in two different conditions:

- When there is no IGMP Querier port (a port that receives IGMP queries) present.
- When an IGMP Querier port is present **or** when no IGMP Querier port is present.

To configure how the switch forwards unknown multicast packets when the switch is in IGMP Passive mode, follow the steps below:

No IGMP Querier port present

1. Under the **Passive Mode Forwarding Port** section, select the **PassiveForwardMode** radio button.
2. Select the checkbox under the ports that you would like to have the **unknown multicast packets** forwarded to.
3. Click on the “Update Setting” button.

Note: The presence of an IGMP Querier port will make the settings provided by the **PassiveForwardMode** to have no effect, and all unknown multicast packets will be forwarded to the IGMP Querier port only.

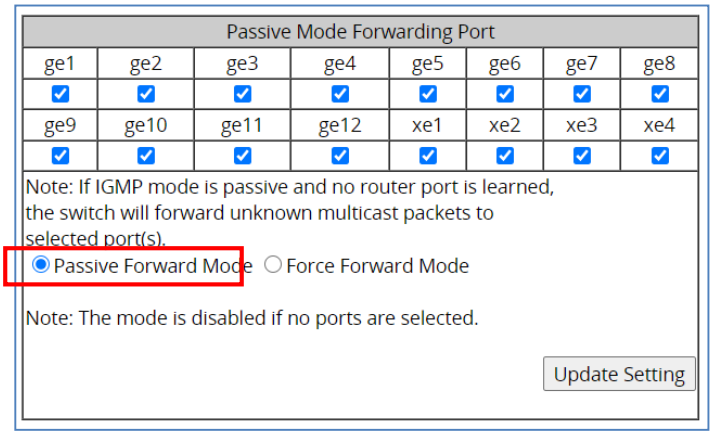


Figure 155: PassiveForwardMode

IGMP Querier port present or no IGMP Querier port present

1. Under the **Passive Mode Forwarding Port** section, select the **ForceForwardMode** radio button
2. Select the checkbox under the ports that you would like to have the **unknown multicast packets** forwarded to.
3. Click on the **Update Setting** button.

Note: The settings according to the **ForceForwardMode** will always be in effect both with and without the presence of an IGMP Querier port. In addition, when an IGMP Querier port is present, all unknown multicast packets will also be forwarded to the IGMP Querier port as well, in addition to the settings in the **ForceForwardMode** function.

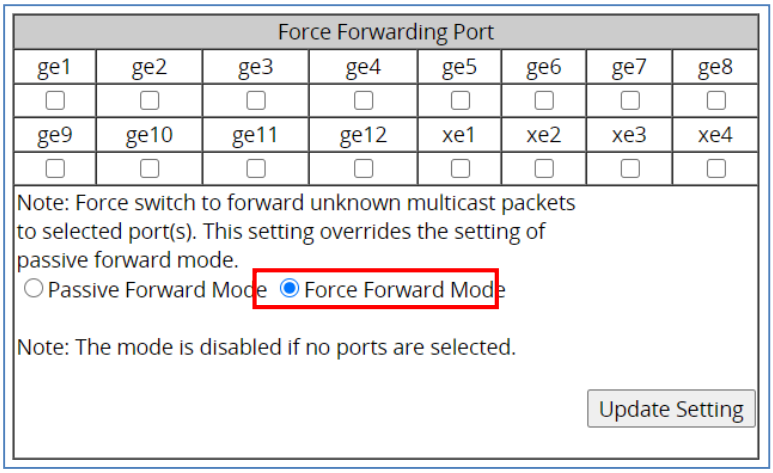


Figure 156: ForceForwardMode

IGMP Querier Mode Forwarding Port Configuration

To configure how the switch forwards unknown multicast packets when the switch is in IGMP Querier mode, follow the below instructions:

1. Under the **Passive Mode Forwarding Port** section, select the **ForceForwardMode** radio button
2. Select the checkbox under the ports that you would like to have the **unknown multicast packets** forwarded to.
3. Click on the **Update Setting** button.

Note: When the switch is in **IGMP Snooping Querier mode**, there will not be an IGMP Querier port present, and the settings according to the **ForceForwardMode** will always be in effect.

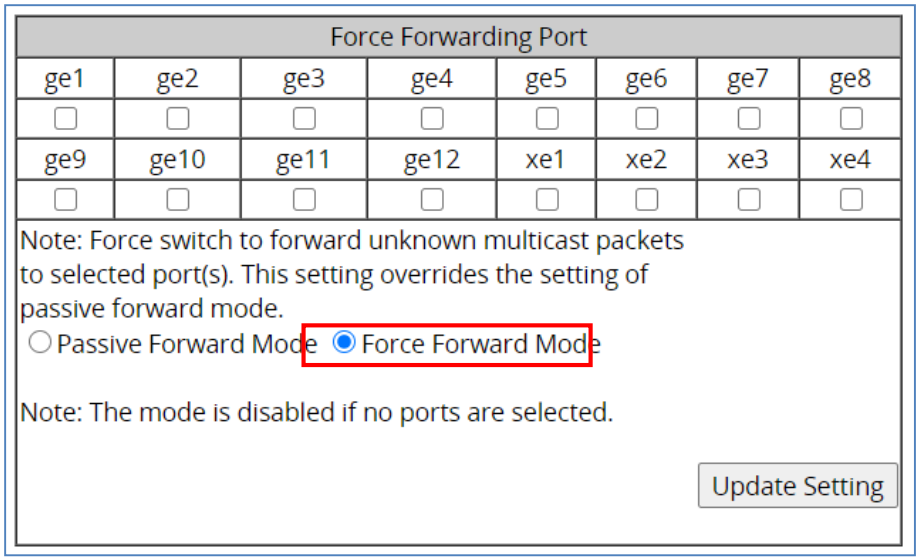


Figure 157: IGMP Querier Mode Forwarding

Monitoring Registered Multicast Groups

To navigate to the **Multicast Current Table** page:

1. Click on the **+** next to **Other Protocols**.
2. Click on **IGMP Snooping**.
3. Click on the **Multicast Current Table** link at the top of the page.

When the switch is in IGMP Passive **or** IGMP Querier mode, registered Multicast Groups can be monitored on each port, as well as the location of the IGMP Querier port (see Figure 142).

- All the registered multicast Groups will be listed in the **Group Address** column.
- The port where each registered Group ID was received can be found in the **Membership** column in each registered Groups corresponding row.

Note: when an IGMP Querier port is present, all registered multicast group IDs will show up in the **Membership** column as a checked box for the IGMP Querier port, even if an **IGMP Join** was never received for that Group ID on the Querier port.

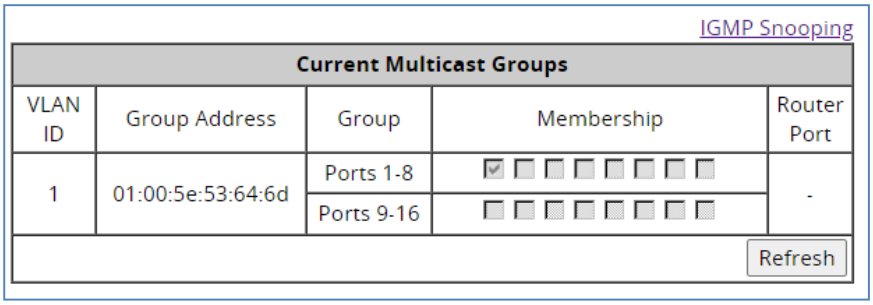


Figure 164: Current Multicast Groups

IGMP Configuration Examples Using CLI Commands

For more information on CLI command usage see CLI Command Usage.

To put the IGMP Snooping feature in **Disabled Mode** use the CLI commands below:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **no ip igmp snooping**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#no ip igmp snooping
switch_a(config)#q
switch_a#
```

To put the IGMP Snooping feature in **Passive Mode** use the CLI commands below:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
ip igmp snooping enable
no ip igmp snooping querier

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#ip igmp snooping enable
switch_a(config)#no ip igmp snooping querier
switch_a(config)#q
switch_a#
```

To put the IGMP Snooping feature in **Querier Mode** use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
ip igmp snooping enable
ip igmp snooping querier

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#ip igmp snooping enable
switch_a(config)#ip igmp snooping querier
switch_a(config)#q
switch_a#
```

To set the IGMP version per VLAN, use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **ip igmp version <1-3>**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface vlan1.1
switch_a(config-if)#ip igmp version 2
switch_a(config-if)#q
switch_a(config)#
```

To enable or disable the IGMP **fast-leave** feature on a VLAN, use the CLI commands below:

CLI Command Mode: **VLAN Interface Configuration Mode**

CLI Command Syntax:
ip igmp snooping fast-leave
no ip igmp snooping fast-leave

Usage Example - **Enabling** the IGMP **fast-leave** feature:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface vlan1.1
switch_a(config-if)#ip igmp snooping fast-leave
switch_a(config-if)#q
switch_a(config)#
```

Usage Example - **Disabling** the IGMP **fast-leave** feature:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface vlan1.1
switch_a(config-if)#no ip igmp snooping fast-leave
switch_a(config-if)#q
switch_a(config)#
```

To enable or disable the IGMP **Report Suppression** feature on a VLAN, use the CLI commands below:

CLI Command Mode: **VLAN Interface Configuration Mode**

CLI Command Syntax:
ip igmp snooping report-suppression
no ip igmp snooping report-suppression

Usage Example - **Enabling** the IGMP **Report Suppression** feature:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface vlan1.1
switch_a(config-if)# ip igmp snooping report-suppression
switch_a(config-if)#q
switch_a(config)#
```

Usage Example - **Disabling** the IGMP **Report Suppression** feature:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface vlan1.1
switch_a(config-if)#no ip igmp snooping report-suppression
switch_a(config-if)#q
switch_a(config)#
```

To configure the IGMP **query-interval**, and the **max-response-time** settings per VLAN, use the CLI commands below:

CLI Command Mode: **VLAN Interface Configuration Mode**

CLI Command Syntax:
ip igmp query-interval <10-18000>
ip igmp query-max-response-time <1-240>

Usage Example - Configuring the IGMP **query-interval** parameter:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface vlan1.1
switch_a(config-if)# ip igmp query-interval 125
switch_a(config-if)#q
switch_a(config)#
```

Usage Example - Configuring the IGMP **max-response-time** parameter:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#interface vlan1.1
switch_a(config-if)# ip igmp query-max-response-time 10
switch_a(config-if)#q
switch_a(config)#
```

To control how the switch forwards unknown multicast packets when the switch is in IGMP Disabled mode, follow the instructions below:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
ip igmp snooping passive-forward all
ip igmp snooping passive-forward none
ip igmp snooping passive-forward *<ifname>,<ifname>,<ifname>*

Usage Example - Flood all unknown multicast packets:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ip igmp snooping passive-forward all
switch_a(config)#q
```

Usage Example - Drop all unknown multicast packets:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ip igmp snooping passive-forward none
switch_a(config)#q
```

Usage Example - Forward unknown multicast packets to the specified ports only:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ip igmp snooping passive-forward ge1,ge2,ge3
switch_a(config)#q
```

To only control how the switch will forward unknown multicast packets when the switch is in IGMP Passive mode and also without a Querier Port present, follow the below instructions:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
ip igmp snooping passive-forward all
ip igmp snooping passive-forward none
ip igmp snooping passive-forward *<ifname>,<ifname>,<ifname>*

Usage Example - Flood all unknown multicast packets:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ip igmp snooping passive-forward all
switch_a(config)#q
switch_a#
```

Usage Example - Drop all unknown multicast packets:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ip igmp snooping passive-forward none
switch_a(config)#q
switch_a#
```

Usage Example - Forward unknown multicast packets to the specified ports only:

```
switch_a>enable
switch_a#configure terminal
```

```
switch_a(config)# ip igmp snooping passive-forward ge1,ge2,ge3
switch_a(config)#q
switch_a#
```

To control how the switch will forward unknown multicast packets when the switch is in IGMP Passive mode, both with or without a Querier Port present, follow the instructions below:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
ip igmp snooping force-forward all
ip igmp snooping force-forward none
ip igmp snooping force-forward *<ifname>,<ifname>,<ifname>*

Usage Example - Flood all unknown multicast packets:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ip igmp snooping force-forward all
switch_a(config)#q
switch_a#
```

Usage Example - Drop all unknown multicast packets:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ip igmp snooping force-forward none
switch_a(config)#q
switch_a#
```

Usage Example - Forward unknown multicast packets to the specified ports only:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ip igmp snooping force-forward ge1,ge2,ge3
switch_a(config)#q
switch_a#
```

To control how the switch will forward unknown multicast packets when the switch is in IGMP Querier mode, follow the below instructions:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
ip igmp snooping force-forward all
ip igmp snooping force-forward none
ip igmp snooping force-forward *<ifname>,<ifname>,<ifname>*

Usage Example - Flood all unknown multicast packets:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ip igmp snooping force-forward all
switch_a(config)#q
switch_a#
```

Usage Example - Drop all unknown multicast packets:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ip igmp snooping force-forward none
switch_a(config)#q
switch_a#
```

Usage Example - Forward unknown multicast packets to the specified ports only:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# ip igmp snooping force-forward ge1,ge2,ge3
switch_a(config)#q
switch_a#
```

GVRP

Defined in IEEE 802.1Q, GVRP is a protocol used to dynamically create VLANs on a switch. Any IEEE 802.1Q compliant switch must implement this protocol.

To navigate to the **Other Protocols / GVRP** page (see Figure 165):

1. Click on the **+** next to **Other Protocols**.
2. Click on **GVRP**.

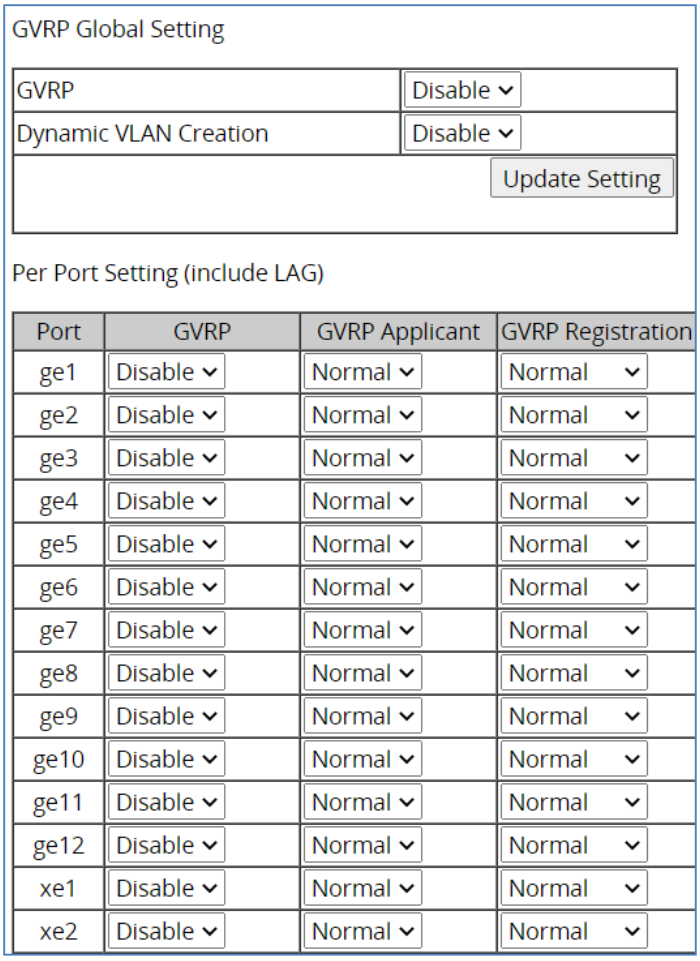


Figure 158: GVRP

General Overview

To enable the GVRP protocol on your network, you must make sure that the switches in your network are configured with the minimum requirements for each type of switches listed below:

For the **Access Switches** at the edge of the network, below are the minimum requirements:

- All of the user VLANs have been created in the VLAN Database.
- The IP address for the Management VLAN has been configured.
- The appropriate Port Type (Access or Trunk) and the PVID have been configured for all the ports of the switch.
- All the member Trunk ports for all the user VLANs have been configured.
- The GVRP protocol has been globally enabled, and GVRP is locally enabled on the Trunk Ports as well.

For the **Distribution Switches** in the core of the network, below are the minimum requirements:

- The Management VLAN has been created in the VLAN Database.
- The IP address for the Management VLAN has been configured.
- The appropriate Port Type (Access or Trunk) and the PVID have been configured for all the ports of the switch.
- The GVRP protocol has been globally enabled and GVRP is locally enabled on the Trunk Ports as well.
- The Dynamic VLAN Creation feature has been enabled.

Enabling the GVRP Protocol at the Global Level

To enable the GVRP protocol globally on a distribution switch (see Figure 166):

1. Under **GVRP Global Setting**, choose the **Enable** option from the drop-down list next to **GVRP**.
2. Choose the **Enable** option from the drop-down list next to **Dynamic VLAN Creation**.
3. Click on the **Update Setting** button.

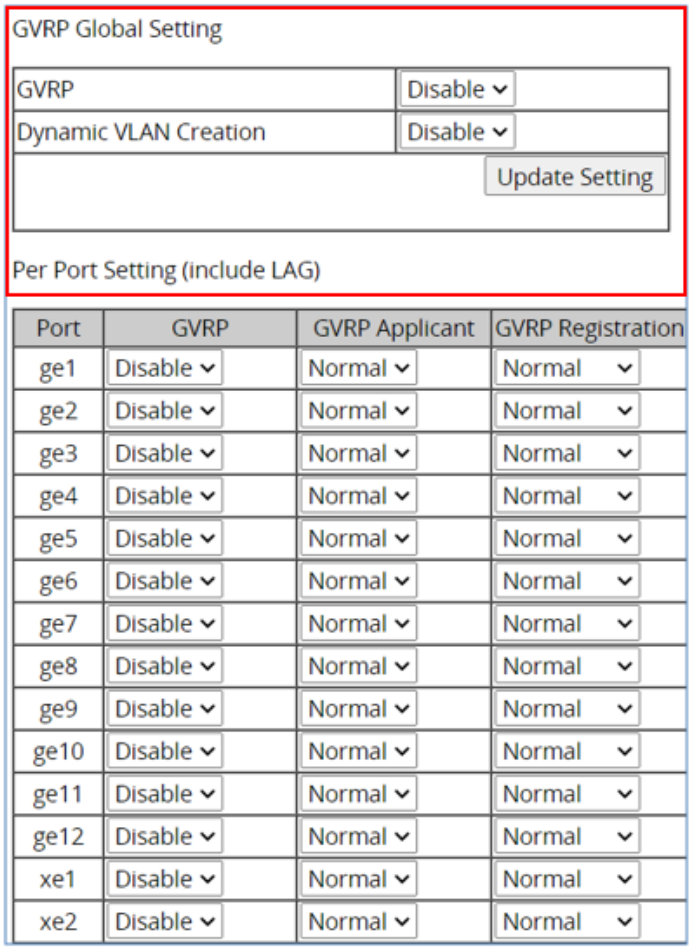


Figure 159: GVRP Configuration Distribution Switch

To enable the GVRP protocol globally on an **Access Switch** (see Figure 167):

1. Under **GVRP Global Setting**, choose the **Enable** option from the drop-down list next to **GVRP**.
2. Click on the **Update Setting** button.

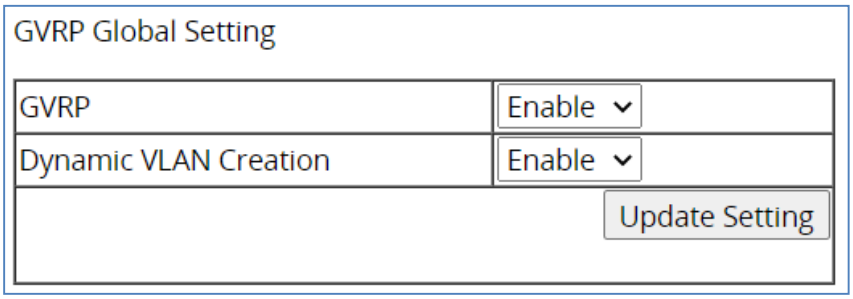


Figure 160: GVRP Configuration Access Switch

Enabling the GVRP Protocol at the Port Level

To navigate to the **Other Protocols / GVRP** page (see Figure167):

1. Click on the **+** next to **Other Protocols**.
2. Click on **GVRP**.

To enable the GVRP protocol locally at the port level, for both the Access switch and the Distribution switch, apply the following procedures to all the Trunk Ports of the switch:

1. For all the Trunk Ports under the **Per Port Setting (include LAG)** section, choose the **Enable** option from the drop-down list under the **GVRP** column.
2. For all the Trunk Ports under the **Per Port Setting (include LAG)** section, choose the **Active** or **Normal** option from the drop-down list under the **GVRP Applicant** column.
    - **Active** - Use this option if you want to run the GVRP protocol on that Trunk Port even if it is blocked by the STP protocol.
    - **Normal** – Use this option if you do not wish to run the GVRP protocol on a Trunk Port when it is being blocked by the STP protocol.
3. For all the Trunk Ports under the **Per Port Setting (include LAG)** section, choose **Normal, Fixed,** or **Forbidden** from the drop-down list under the **GVRP Registration** column.
4. Click on the **Update Setting** button.
5. Save the configuration (see the Save Configuration Page)

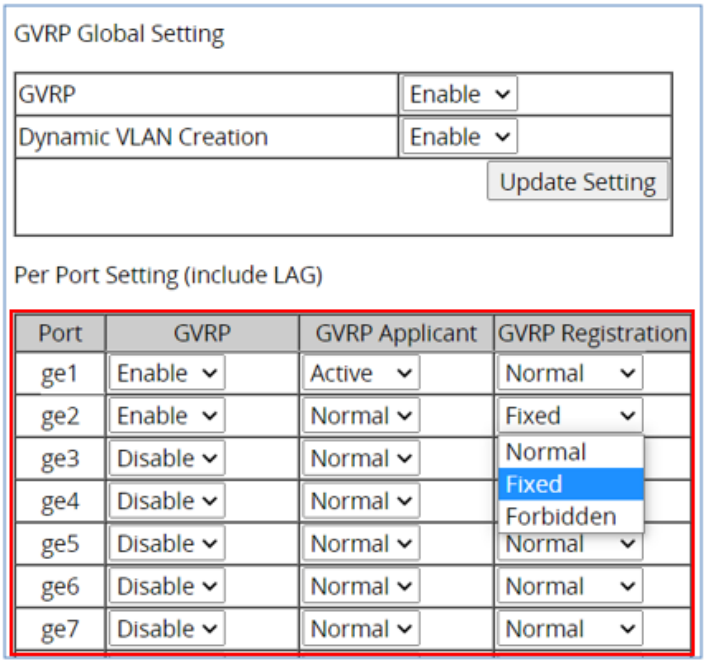


Figure 161: GVRP Per Port Settings

GVRP Configuration Examples Using CLI Commands

For more information on CLI command usage see CLI Command Usage.

To enable or disable GVRP globally on the EtherWAN switch, use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
set gvrp enable bridge 1
set gvrp disable bridge 1

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# set gvrp enable bridge 1
switch_a(config)# set gvrp disable bridge 1
switch_a(config)#q
switch_a#
```

To enable the dynamic VLAN creation feature of GVRP on the EtherWAN switch, you must use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **set gvrp dynamic-vlan-creation disable bridge 1**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# set gvrp dynamic-vlan-creation disable bridge 1
switch_a(config)#q
switch_a#
```

To enable or disable GVRP locally on a port on the EtherWAN switch, you must use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
set port gvrp enable <port id>
set port gvrp disable <port id>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# set port gvrp enable ge1
switch_a(config)# set port gvrp disable ge1
switch_a(config)#q
switch_a#
```

By default, when GVRP is enabled on a port the **Applicant** runs in Normal mode, which means that the GVRP protocol will not send out any PDUs from a port if the port is being blocked by STP. When you enable the GVRP Applicant to run in Active mode on a port, the GVRP protocol will continue to send PDUs from a port even if the port is being blocked by STP.

The GVRP **Applicant** can be set to run in Normal or Active mode on a port by issuing the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
set gvrp applicant state normal <port id>
set gvrp applicant state active <port id>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# set gvrp applicant state normal ge1
switch_a(config)# set gvrp applicant state active ge1
switch_a(config)#q
switch_a#
```

When you enable GVRP on a port, the **Registrar** is enabled on the port by default. You can enable or disable the GVRP **Registrar** on a port by issuing the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
set gvrp registration normal <port id>

set gvrp registration forbidden <port id>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# set gvrp registration normal ge1
switch_a(config)# set gvrp registration forbidden ge1
switch_a(config)#q
switch_a#
```

GMRP

The settings in the GMRP feature controls how the switch automates the process of multicast packet forwarding, both within a single switch as wells as between switches in a bridged network. With the GMRP feature enabled, when the switch receives any GMRP multicast group registration requests from either a multicast client or a neighbor switch, the switch will register these multicast groups on these ports and will only transmit the multicast packets that belong to these groups to these ports. The switch will also automatically propagate these multicast group registrations onto the neighbor switches to allow the neighbor switches to forward the multicast packets that belong to these groups to the local switch.

To navigate to the **Other Protocols / GMRP** page:

1. Click on the **+** next to **Other Protocols**.
2. Click on **GMRP**.

General Overview

The ports on the EtherWAN switch can be configured with the GMRP feature in five modes:

- Disabled
- Normal
- Fixed
- Forbidden
- Forward All.

GMRP Normal mode

When a port is put in GMRP **Normal** mode, that port can accept both multicast group registration and multicast group deregistration from the multicast client or the neighbor switch that is residing on that port. Also, the switch will propagate all the registered multicast groups on the switch to the neighbor switch residing on that port.

GMRP Fixed mode

When a port is put in GMRP **Fixed** mode, that port can accept group registration but will not accept any group deregistration from multicast clients or neighbor switches that reside on that port. Also, the switch will be propagating all the registered multicast groups on the switch to the neighbor switch residing on that port.

GMRP Forbidden mode

When a port is put in GMRP **Forbidden** mode, all multicast groups will be deregistered on that port and that port will not be accepting any further multicast group registrations. However, the switch will still be propagating all the registered multicast groups on the switch to the neighbor switch residing on that port.

GMRP Forward All mode

When a port is put in GMRP **Forward All** mode, all the registered multicast groups on the switch will automatically be registered to this port, so the switch will be forwarding all the multicast packets that belong to these groups to this port and this port will also be propagating all the registered multicast groups on the switch to the neighbor switch residing on that port.

GMRP Disabled mode

When a port is put in GMRP **disabled** mode that port will not participate in any GMRP activities.

Enabling the GMRP Feature Globally on the Switch

To navigate to the **Other Protocols / GMRP** page:

1. Click on the **+** next to **Other Protocols**.
2. Click on **GMRP**.

To enable the GMRP function in the switch, follow the procedure below:

1. Choose the **Enable** option from the dropdown list next to **GMRP**
2. Click on the **Update Setting** button. (See Figure169)

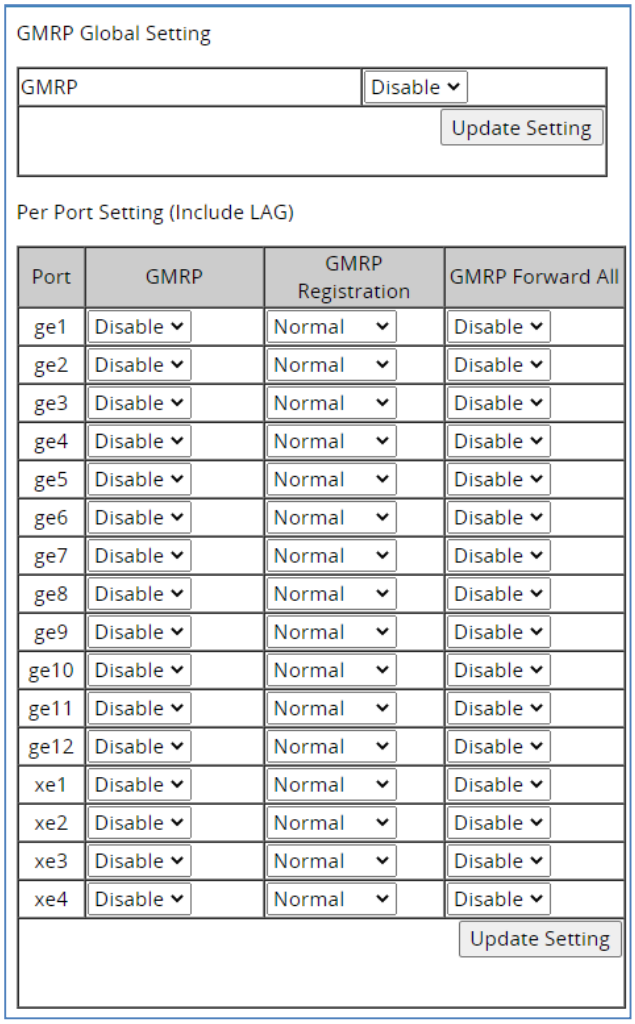


Figure 162: GMRP Global Setting

Configuring the GMRP Feature Per Port

To navigate to the **Other Protocols / GMRP** page:

1. Click on the **+** next to **Other Protocols**.
2. Click on **GMRP**.

GMRP should be enabled on all the ports that could be a potential source of multicast traffic, and on the ports that are connected to multicast clients. You can also further configure each GMRP enabled port with the specific application modes described in the below configuration.

To allow a port to dynamically receive GMRP multicast group registrations and dynamically transmit the multicast packets that belong to these multicast groups on this port configure the items listed below:

- For each port that you wish to apply this application, select the **Enable** option from the drop-down list under the GMRP column.
- For each port that you wish to apply this application, select the **Normal** option from the drop-down list under the GMRP Registration column.
- For each port that you wish to apply this application, select the **Disable** option from the drop-down list under the GMRP Forward All column.
- Click on the **Update Setting** button.

To allow a port to dynamically receive GMRP multicast group registrations and then make the multicast packets that belong to these multicast groups constantly available on this port, configure the items listed below:

- For each port that you wish to apply this application, select the **Enable** option from the drop-down list under the GMRP column.
- For each port that you wish to apply this application, select the **Fixed** option from the drop-down list under the GMRP Registration column.
- For each port that you wish to apply this application, select the **Disable** option from the drop-down list under the GMRP Forward All column.
- Click on the **Update Setting** button.

If you do not wish to transmit any multicast packets on a port based on the received GMRP multicast group registrations on that port, but would like to receive multicast packets that belong to the currently registered multicast groups on the switch on that port, configure the items listed below:

- For each port that you wish to apply this application, select the **Enable** option from the drop-down list under the GMRP column.
- For each port that you wish to apply this application, select the **Forbidden** option from the drop-down list under the GMRP Registration column.
- For each port that you wish to apply this application, select the **Disable** option from the drop-down list under the GMRP Forward All column.
- Click on the **Update Setting** button.

If you wish to transmit all the multicast packets that belong to all the currently registered multicast groups on the switch on a port, configure the items listed below:

- For each port that you wish to apply this application, select the “**Enable**” option from the drop-down list under the GMRP column.

- For each port that you wish to apply this application, select the appropriate option from the drop-down list under the GMRP Registration column, according to the previous instructions.
- For each port that you wish to apply this application, select the **Enable** option from the drop-down list under the GMRP Forward All column.
- Click on the **Update Setting** button.

If you do not want a port to participate in the GMRP protocol, configure the items listed below:

- For each port that you wish to apply this application, select the **Disable** option from the drop-down list under the GMRP column.
- Click on the **Update Setting** button.

GMRP Configuration Examples Using CLI Commands

For more information on CLI command usage see CLI Command Usage.

To enable or disable GMRP globally on the EtherWAN switch, use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
set gmrp enable bridge 1
set gmrp disable bridge 1

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# set gmrp enable bridge 1
switch_a(config)# set gmrp disable bridge 1
switch_a(config)#q
switch_a#
```

To enable GMRP locally on a port on the EtherWAN switch, you must use the below CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
set port gmrp enable <port id>
set port gmrp enable <port id>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# set port gmrp enable ge1
switch_a(config)# set port gmrp disable ge1
switch_a(config)#q
switch_a#
```

When you enable GMRP on a port, the **Registrar** is in **Normal** mode by default.
The GMRP **Registrar** on a port can be configured in 3 different modes by issuing the following CLI commands

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
set gmrp registration normal <port id>
set gmrp registration fixed ge1 <port id>
set gmrp registration forbidden <port id>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#set gmrp registration normal ge1
switch_a(config)#set gmrp registration fixed ge1
switch_a(config)#set gmrp registration forbidden ge1
switch_a(config)#q
switch_a#
```

By default when you enable GVRP on a port this feature is disabled
To enable or disable the **Forward All** feature on a port, use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
set gmrp fwdall enable <port id>
set gmrp fwdall disable <port id>

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#set gmrp fwdall enable ge1
switch_a(config)#set gmrp fwdall disable ge1
switch_a(config)#q
switch_a#
```

Network Time Protocol (NTP)

NTP or Network Time Protocol is a useful tool designed to update your switch with the most accurate time available from a user specified time source. This is useful for the end user in that the switch logging is noted with the actual time rather than the default switch time (begins on Jan 1st, 2010) as it can aid debugging switching related problems by showing an accurate time an event occurred.

To navigate to the **NTP** page:

1. Click on the **+** next to **Other Protocols**.
2. Click on **NTP**

Setting RTC Time

(Only applicable to certain models) At the top of this screen, there are fields in which you can enter the current year, date, and time. When done, click Update Setting to make the time change take effect. (See figure below) Note that the time will reset whenever the switch is rebooted, or restarted after a power loss.

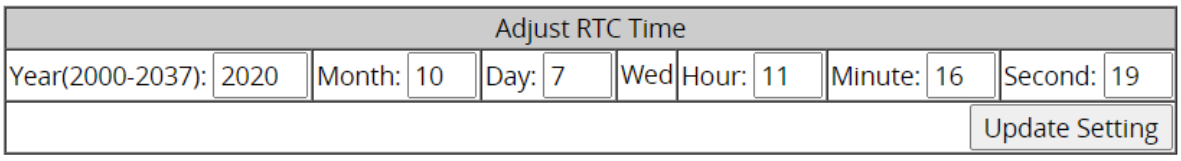


Figure 170: RTC Time setting

To manually set the time using the CLI:

CLI Command Mode: **Privileged exec mode**

CLI Command Syntax: **set clock <2000-2037> <1-12> <1-31> <0-23> <0-59> <0-59>**

Usage Example:

```
switch_a>enable
switch_a# set clock 2020 10 27 17 24 30
```

Enabling NTP

To enable the NTP client, follow the steps below (see Figure 163):

1. Choose Enable from the dropdown list next to **NTP Status**
2. Click on the **Update Setting** button

Setting the NTP Server IP Address

To provide a time source for the NTP client, follow the steps below:

1. Enter an IP address or host name in the **NTP Server** text box.
2. Click on the **Update Setting** button

Setting the Time Zone

To change the time zone of the switch, follow the steps below:

1. Select the proper time zone from the dropdown list next to **Time Zone.**
2. Click on the **Update Setting** button

Setting the Polling Period

To alter the polling period (how often the NTP client checks the server for the correct time), follow the steps below:

1. Enter the new polling period in the Polling Interval textbox**.**
2. Click on the **Update Setting** button

Manually Syncing Time

To set the time immediately using an NTP server, follow the steps below:

1. Enter the new polling period in the Polling Interval textbox**.**
2. Click on the **Sync Time** button in the **NTP Server** field

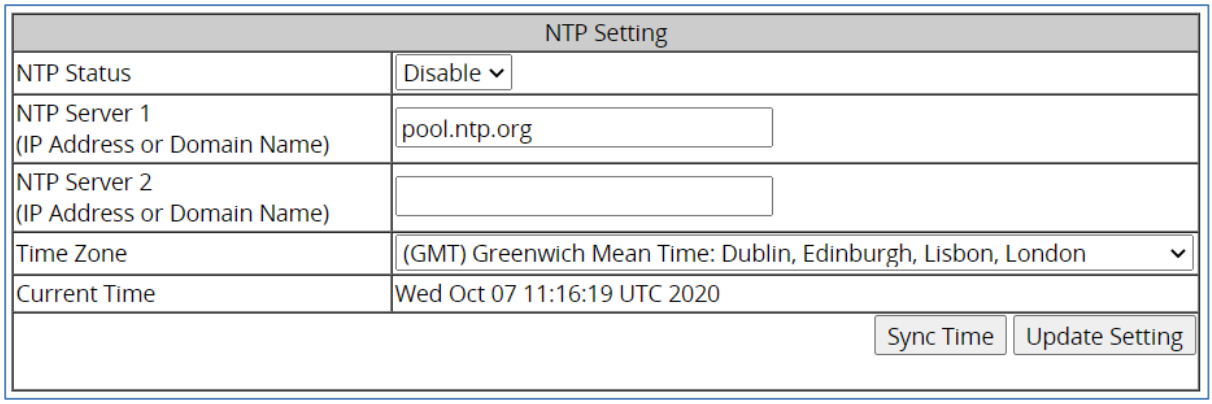


Figure 163: NTP Settings

Daylight Savings Time - Weekday Mode

To adjust the switch's clock for Daylight Savings Time using the weekday mode, follow the steps below:

1. Select the option **Weekday** from the **Daylight-Saving Mode** dropdown box.
2. Enter the value for the time offset in the **Time Set Offset** textbox.
3. Enter the name of the **Daylight-Saving Time Zone**.
4. In the **Weekday Box**, select the month, week, day, hour, and minute for both the from and to fields. For example, if Daylight Saving Time begins on the second Sunday in March at 2:00AM and ends on the first Sunday in November at 2:00AM, then select the values as shown in Figure 164.
5. Click on the **Update Setting** button

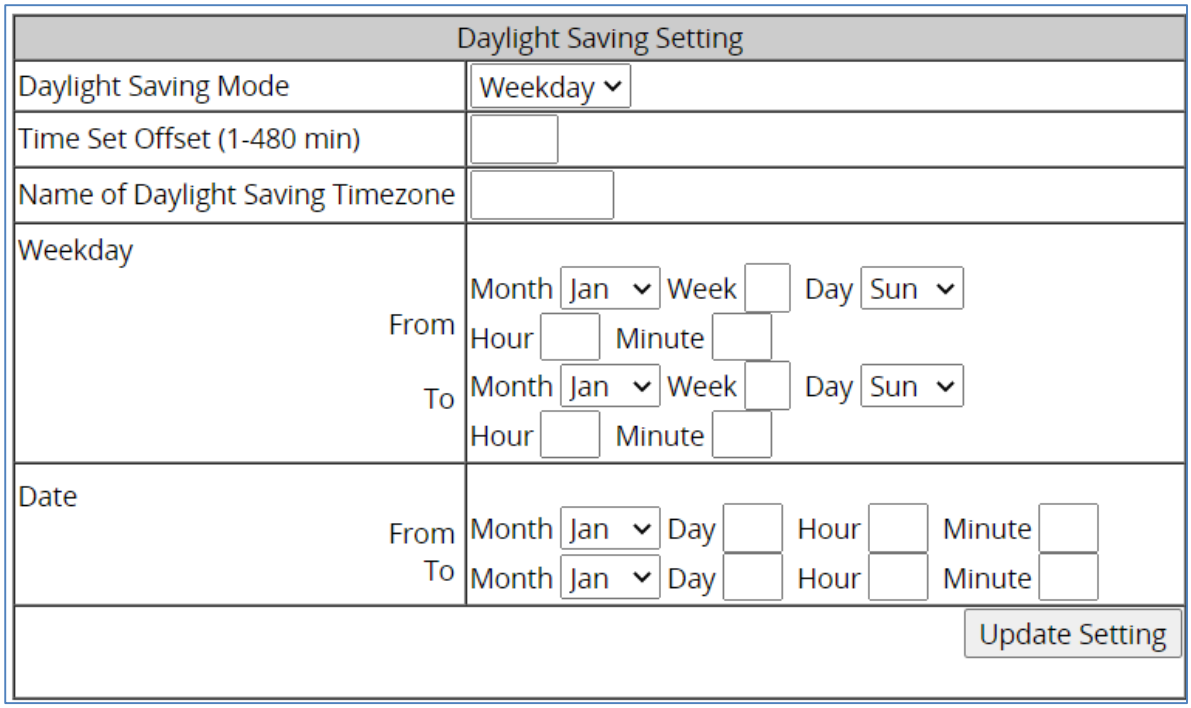


Figure 164: Daylight Savings – Weekday Mode

Daylight Savings Time – Date Mode

To adjust the switch's clock for Daylight Savings Time using the date mode, follow the steps below:

1. Select the option **Date** from the **Daylight-Saving Mode** dropdown box.
2. Enter the value for the time offset in the **Time Set Offset** textbox.
3. Enter the name of the **Daylight-Saving Time Zone**.
4. In the **Date section**, select the month and enter the date, hour, and minute for both the from and to fields. For example, if Daylight Saving Time begins on March 9th at 2:00AM and ends on November 2nd at 2:00AM, then select the values as shown in Figure 165.
5. Click on the **Update Setting** button

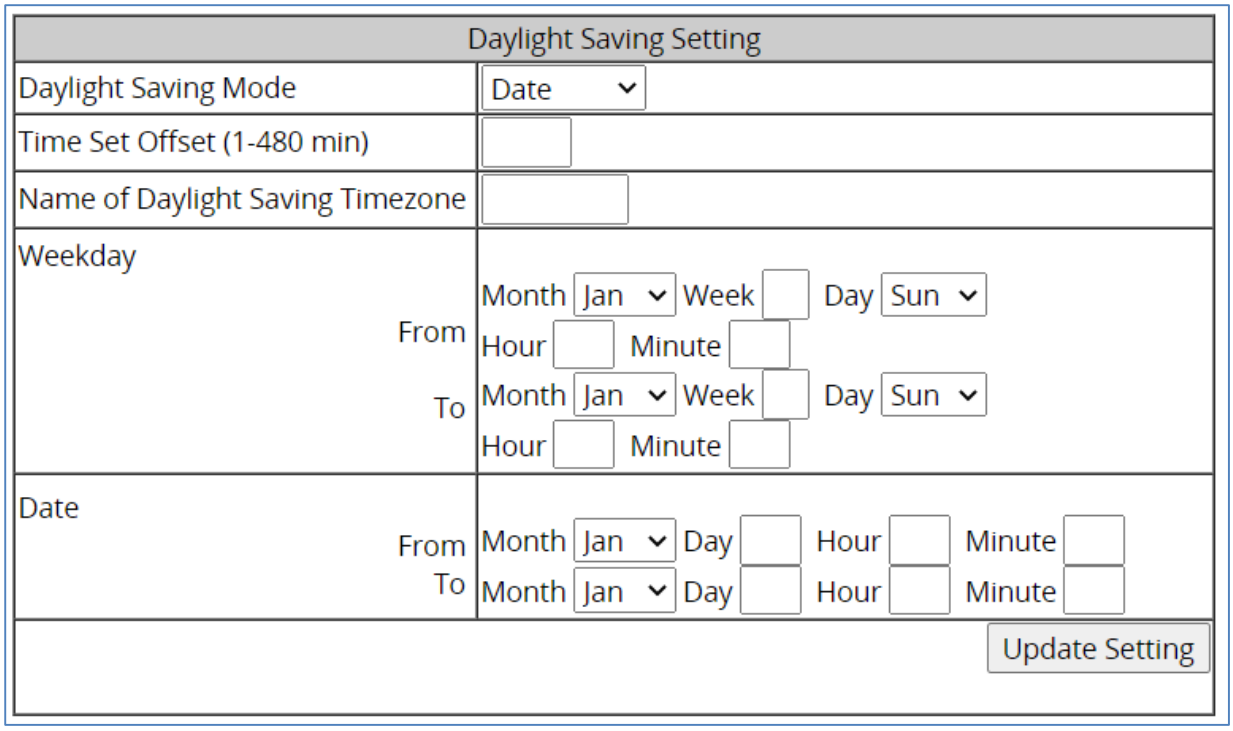


Figure 165: Daylight Savings – Date Mode

Network Time Protocol Configuration Examples Using CLI Commands

For more information on CLI command usage see CLI Command Usage.

To enable NTP on the switch, use the CLI commands below:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **ntp enable**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#ntp enable
switch_a(config)#q
```

To set the NTP server on the switch, use the CLI commands below:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **ntp server *<IP Address or Host Name of NTP Server>***

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#ntp server 192.168.1.126
switch_a(config)#q
switch_a#
```

To set the NTP polling interval on the switch, use the CLI commands below:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **ntp polling-interval *<time in minutes, 1-10080>***

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#ntp polling-interval 180
switch_a(config)#q
switch_a#
```

To have the NTP client sync the clock immediately on the switch, use the CLI commands below:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **ntp sync-time**

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#ntp sync-time
switch_a(config)#q
switch_a#
```

To set the current time zone for the switch, use the CLI commands below:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
clock timezone *<Name of Time Zone> <UTC Offset in hh:mm format>*

Usage Example:

```
switch_a>enable
switch_a#configure terminal
```

```
switch_a(config)#clock timezone CDT -6:00
switch_a(config)#q
switch_a#
```

To set the Daylight Savings Time settings using weekday mode for the switch, use the CLI commands below:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
clock summer-time *<Name of Time Zone>* weekday *<start week number> <start day> <start month> <start hour> <start minute> <end week number> <end day> <end hour> <end minute> <time offset in minutes>*

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# clock summer-time CDT weekday 2 Sun March 2 0 1
Sun November 2 0 60
switch_a(config)#q
switch_a#
```

To set the Daylight Savings Time settings using date mode for the switch, use the CLI commands below:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
clock summer-time *<Name of Time Zone>* date *<start date> <start month> <start hour> <start minute> <end date> <end month> <end hour> <end minute> <time offset in minutes>*

Usage Example:

```
switch_a>enable
switch_a#configure terminal
switch_a(config)# clock summer-time CDT date 9 March 2 0 2 November 2 0
60
switch_a(config)#q
switch_a#
```

Prosition Time Protocol (PTP)

Precision Time Protocol(PTP) is a time synchronization protocol for nodes distributed across a network, which specifies how real-time PTP clocks in the system synchronize with each other. Through the hardware timestamp feature provides greater accuracy than other time synchronization protocols such as Network Time Protocol (NTP).

A PTP domain system consist of a combination of ordinary clocks, boundary clocks, and transparent devices combined with network switches, routers, and other infrastructure devices organized into a master-slave synchronization hierarchy with the grandmaster clock, the members using exchanging PTP timing messages to adjust their clocks to follow the time of master in the hierarchy.

General Overview

The EtherWAN switch forwards all PTP messages, measures the residence time of a packet in the switch and the link delay of the ingress port for the packet. Support two kinds of transparent clocks by models:

- **End-to-End transparent clock** (for all Firmware 5.0 product series)

  Measures the residence time of a PTP message and accumulates the times in the correction field of the PTP message or an associated follow-up message.

- **Peer-to-Peer transparent clock** (available for specific product series)

  Measures the residence time of a PTP message and computes the link delay between each port and a similarly equipped port on another node that shares the link. For a packet, this incoming link delay is added to the residence time in the correction field of the PTP message or an associated follow-up message.

Configuring the PTP feature

To navigate to the **PTP** page:

1. Click on the **+** next to **Other Protocols**
2. Click on **PTP** (see Figure 174)

To set the PTP Mode function features:

1. Select the **PTP setting** item for settings
2. Select “Mode of synchronization” from the dropdown menu of **PTP Mode** item.
   - **Disable** (default)
   - **E2E 1-step**

   Option item will be displayed on **P2P** mode available models
   - **P2P 1-step / P2P 2-step**

3. To set **PTP domin** number. **(0~255)**
4. To set **Pdelay req interval** in 2^n sec. **(-3~5)**
5. Click **Update Setting**.

To enable the PTP Interface configuration:

1. Select the target port shown in **Status**.
2. Select "**Enable**" from the dropdown menu.
3. Set the **VLAN ID** as require. **(0~4094)**
4. Click **Update Setting**.

Note: The "**P2P Mode**" corresponding ports will be displayed and configurable in "**Status** and **VLAN**" item.

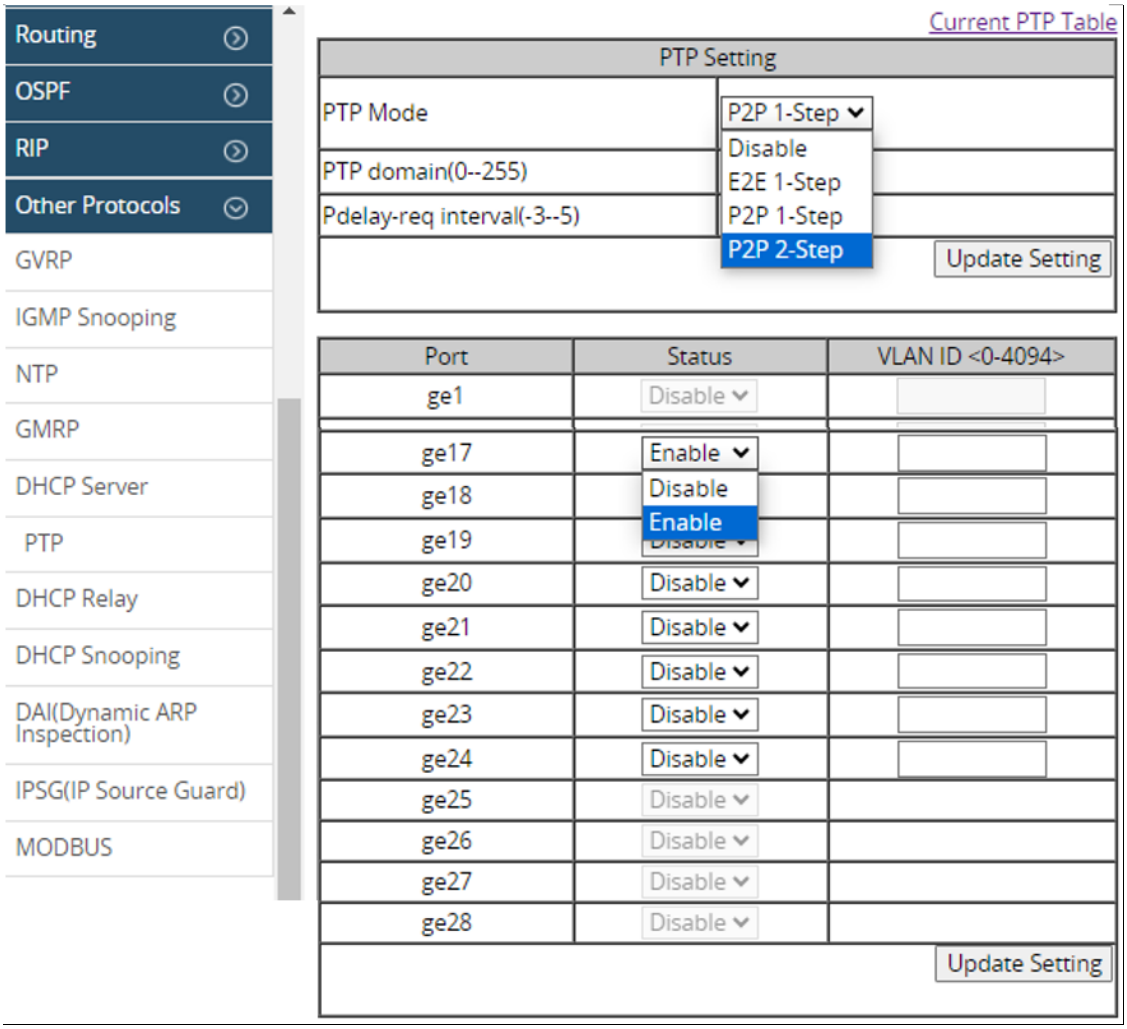
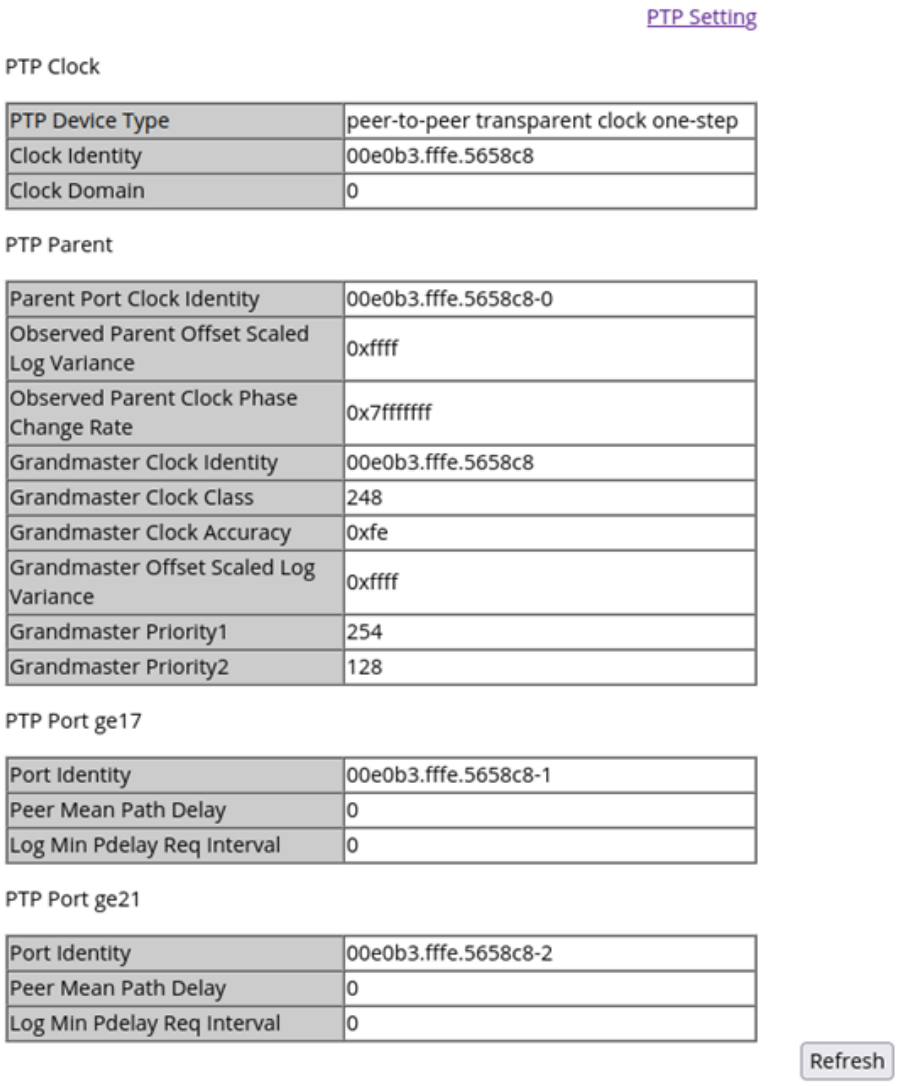


Figure 174 PTP settings

To check PTP Domain & PTP Parent information of interface connection status:

1. Click on the **Current PTP Table** link.
2. The PTP related connection and synchronization status information were being shown in table. (see Figure175).



PTP Setting

PTP Clock

PTP Device Type	peer-to-peer transparent clock one-step
Clock Identity	00e0b3.fffe.5658c8
Clock Domain	0

PTP Parent

Parent Port Clock Identity	00e0b3.fffe.5658c8-0
Observed Parent Offset Scaled Log Variance	0xffff
Observed Parent Clock Phase Change Rate	0x7fffffff
Grandmaster Clock Identity	00e0b3.fffe.5658c8
Grandmaster Clock Class	248
Grandmaster Clock Accuracy	0xfe
Grandmaster Offset Scaled Log Variance	0xffff
Grandmaster Priority1	254
Grandmaster Priority2	128

PTP Port ge17

Port Identity	00e0b3.fffe.5658c8-1
Peer Mean Path Delay	0
Log Min Pdelay Req Interval	0

PTP Port ge21

Port Identity	00e0b3.fffe.5658c8-2
Peer Mean Path Delay	0
Log Min Pdelay Req Interval	0

Refresh

Figure 166: PTP Table

PTP Configuration of CLI Commands

To set the **PTP Mode** function features:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
ptp mode {e2e | p2p {1step | 2step}}
no ptp mode (default)

To set **PTP domain** configuration:
(Option item for p2p mode available product series)

CLI Command Syntax:
ptp domain <domain-number> (0~255)
no ptp domain (0) (default)

To set **Pdelay-req interval** configuration: (2^n sec)
(Option item for p2p mode available product series)

CLI Command Syntax:
ptp pdelay-req interval <n> (-3~5)
no ptp pdelay-req interval (0) (default)

To set the **PTP Interface** configuration:

CLI Command Syntax:
ptp enable
no ptp enable (default)

To set the **PTP VLAN tagging** configuration:
(Option item for p2p mode available product series)

CLI Command Syntax:
ptp vlan <vlan-id> (0~4094)
no ptp vlan (default)

To set the **check PTP information** configuration:

CLI Command Syntax:
show ptp clock
show ptp port
show ptp parent
no ptp enable (default)

Usage Example 1: Set P2P 1-step configuration on ge17 and ge18.

```
switch_a(config)# ptp mode p2p 1step
switch_a(config)# interface ge17
switch_a(config-if)# no ptp enable
switch_a(config-if)# ptp enable
switch_a(config-if)#exit
switch_a(config)# interface ge18
```

```
switch_a(config-if)# no ptp enable
switch_a(config-if)# ptp enable
switch_a(config-if)#exit
```

Usage Example 2: Set PTP domain.

```
switch_a(config)#ptp domain 0
```

Usage Example 3: Check PTP clock information.

```
switch_a#show ptp clock
PTP Clock Information
  PTP Device Type: peer-to-peer transparent clock two-step
  Clock Identity: 0xa27cd9fffe3144c7
  Clock Domain: 254
switch_a#
```

Usage Example 4: Check PTP parent information.

```
switch_a#Show ptp parent
PTP Parent Information
  Parent Clock Identity: 0xc6d299fffe8eae76
  Observed Parent Offset Scaled Log Variance: 0xffff
  Observed Parent Clock Phase Change Rate: 0x7fffffff
  Grandmaster Clock Identity: 0xc6d299fffe8eae76
  Grandmaster Clock Class: 248
  Grandmaster Clock Accuracy: 0xfe
  Grandmaster Offset Scaled Log Variance: 0xffff
  Grandmaster Priority1: 128
  Grandmaster Priority2: 128
switch_a#
```

Usage Example 5: Check PTP Port status and synchronized information.

```
switch_a#Show ptp port
PTP Port Information: ge17
  Port Identity: 00e0b3.fffe.772716-1
  Peer Mean Path Delay: 393
  Log Min Pdelay Req Interval: 0
PTP Port Information: ge18
  Port Identity: 00e0b3.fffe.772716-2
  Peer Mean Path Delay: 390
  Log Min Pdelay Req Interval: 0
PTP Port Information: ge19
  Port Identity: 00e0b3.fffe.772716-3
  Peer Mean Path Delay: 391
  Log Min Pdelay Req Interval: 0
PTP Port Information: ge20
  Port Identity: 00e0b3.fffe.772716-4
  Peer Mean Path Delay: 392
  Log Min Pdelay Req Interval: 0
switch_a#
```

DHCP Server

DHCP is a TCP/IP application protocol that allows any TCP/IP device to dynamically obtain its initial TCP/IP configurations through the TCP/IP protocol itself (in this case, through the UDP protocol). It is based on the client-server paradigm. The EtherWAN switch can be set up as a DHCP server to allow any DHCP client to dynamically obtain its IP address, default router, and DNS servers.

General Overview

The EtherWAN switch can function as a DHCP server for a single VLAN (it can be any VLAN) on the switch. When functioning as a DHCP server, the EtherWAN switch can be configured with a range of IP addresses, default gateway and DNS servers, which will allow the switch to use the dynamic configuration function of the DHCP protocol to provide any TCP/IP device that is a DHCP client, to dynamically obtain an IP address, default router, and DNS servers. The EtherWAN DHCP server can also be configured with a lease period that the DHCP clients are allowed the use of their assigned IP address. In this simple implementation, both the DHCP Client and the DHCP Server must be on the same network (same VLAN).

Configuring the DHCP Server

To navigate to the **DHCP Server** page:

1. Click on the **+** next to **Other Protocols**
2. Click on **DHCP Server** (see Figure 167)

You can use the GUI to set the following DHCP server parameters:

- DHCP Server Enable
- DHCP VLAN.
- DHCP Client Parameters
    - IP Address range
    - Subnet Mask
    - Default gateway
    - Primary and Secondary DNS.
- DHCP Client lease time

To set the DHCP server parameters:

1. From the drop-down list next to **DHCP Server Status,** select the VLAN that will get the DHCP provided TCP/IP Parameters.

2. Enter the starting and ending IP addresses for the DHCP Client IP address range, in the text boxes next to **Start IP** and **End IP**.
3. Enter the Subnet Mask in the text box next to **Subnet Mask.**
4. Enter the IP address for the DHCP Client default router in the entry field next to **Gateway**.
5. Enter the IP addresses for the DHCP Client primary and secondary DNS servers, in the entry field next to **Primary DNS** and **Secondary DNS**.
6. Enter the lease period in seconds, which the DHCP clients are allowed the use of their leased IP addresses, in the entry field next to **Lease Time**.
7. Click on the **Update Setting** button.

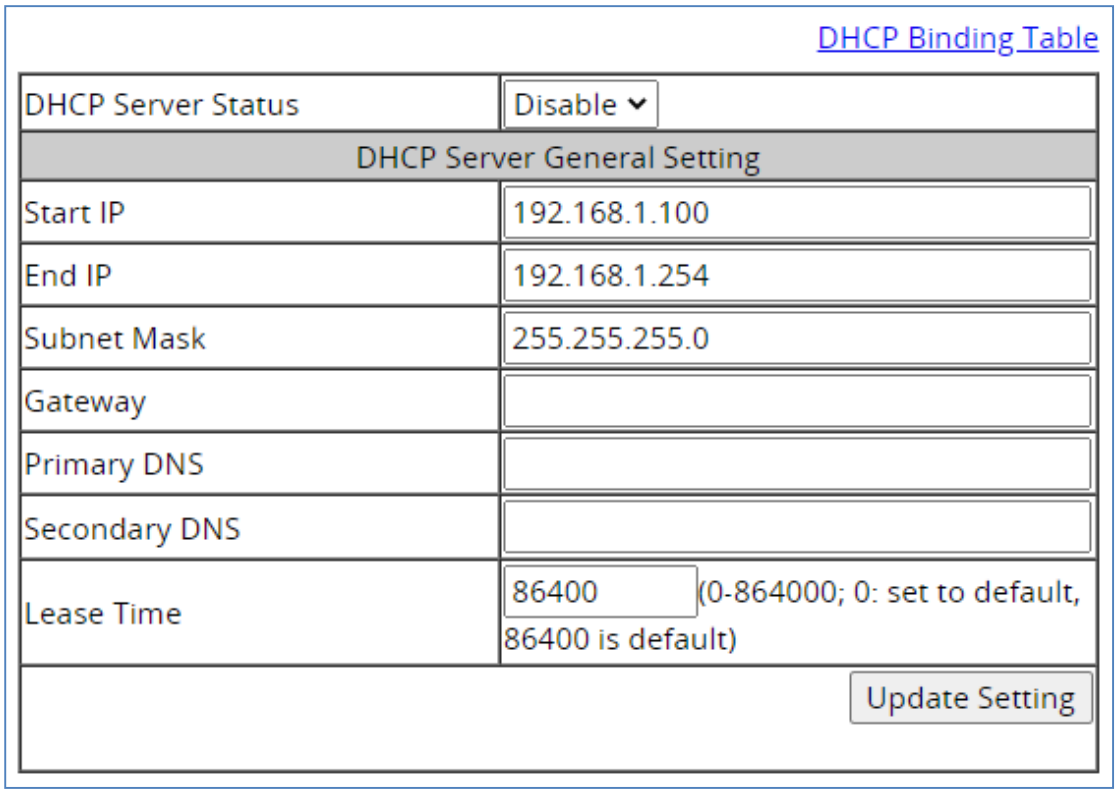


Figure 167: DHCP Server

To check what IP addresses has been allocated to which DHCP clients:

3. Click on the **DHCP Binding Table** link.
4. Click on the DHCP General Setting link to get back to the previous DHCP configuration Web GUI page (see Figure 168).

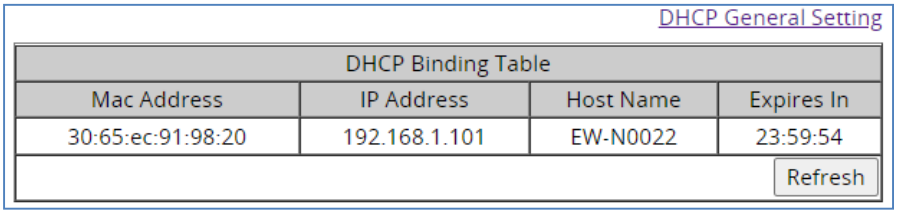


Figure 168: DHCP Binding Table

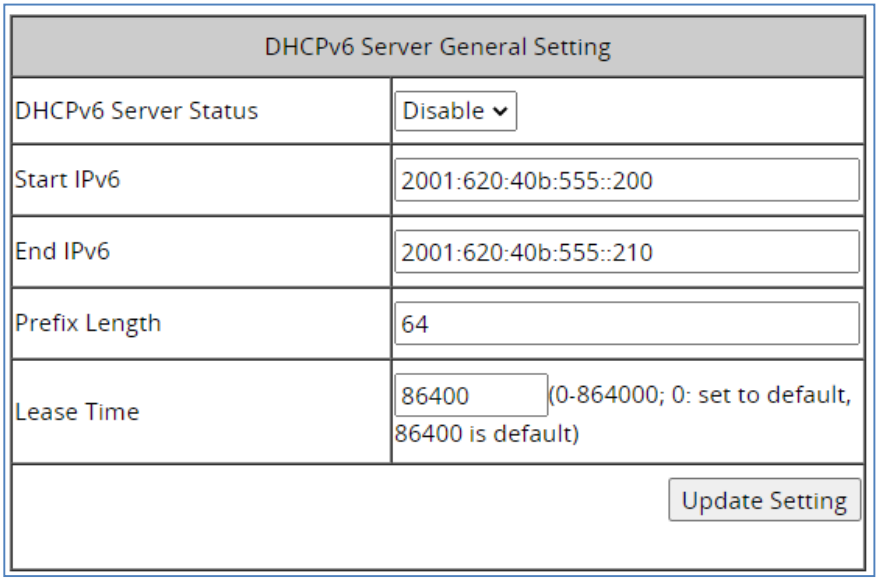


Figure 169: DHCPv6 Server Settings

DHCP Configuration Examples Using CLI Commands

For more information on CLI command usage see CLI Command Usage.

To set the DHCP server parameters:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
dhcp-server range *<start IP> <end IP>*
dhcp-server subnet-mask *<subnet mask in doted decimal notation>*
dhcp-server gateway *<IP address>*
dhcp-server dns 1 *<IP address>*
dhcp-server dns 2 *<IP address>*

dhcp-server lease-time <*0-864000*>

Usage Example:

```
switch_a> enable
switch_a#configure terminal
switch_a(config)#dhcp-server range 192.168.7.100 192.168.7.107
switch_a(config)#dhcp-server subnet-mask 255.255.255.0
switch_a(config)#dhcp-server gateway 192.168.7.1
switch_a(config)#dhcp-server dns 1 1.2.3.4
switch_a(config)#dhcp-server dns 2 5.6.7.8
switch_a(config)#dhcp-server lease-time 86400
switch_a(config)#q
switch_a#
```

To enable the DHCP server and set the DHCP VLAN:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **dhcp-server enable; no dhcp-server enable**

Usage Example:

```
switch_a> enable
switch_a#configure terminal
switch_a(config)#interface vlan1.100
switch_a(config-if)#dhcp-server enable
switch_a(config-if)#no dhcp-server enable
switch_a(config-if)#q
switch_a(config)#q
switch_a#
```

To check what IP addresses has been allocated:

CLI Command Mode: **Privileged Exec Mode**

CLI Command Syntax: **show dhcp-server binding**

Usage Example:

```
switch_a> enable
switch_a#show dhcp-server binding
Mac Address       IP-Address      Expires in
a4:ba:db:de:d6:2f 192.168.7.100   23 hours, 57 minutes, 15
seconds
```

```
switch_a#
```

Configuring DHCPv6 Server

To set the DHCPv6 server parameters:

1. Select enable from the drop down menu.
2. Enter the starting and ending IP addresses for the DHCPv6 Client IP address range, in the text boxes next to **Start IPv6** and **End IPv6**.
3. Enter the Prefix Length in the text box next to **Prefix Length.**
4. Enter the lease period in seconds, which the DHCP clients are allowed the use of their leased IP addresses, in the entry field next to **Lease Time**.
5. Click on the **Update Setting** button.

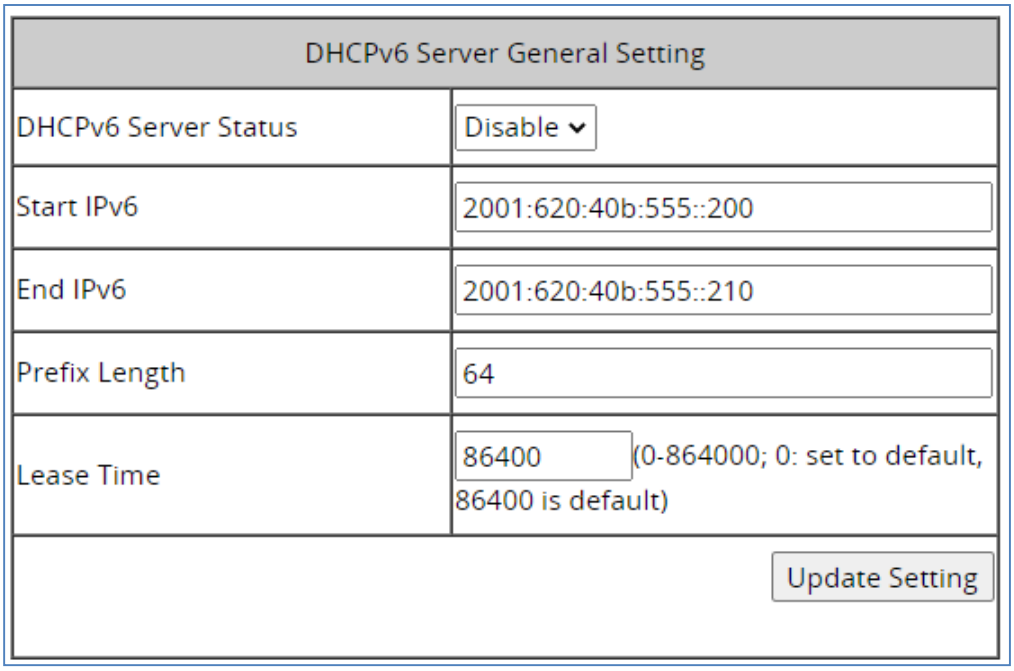


Figure 170: DHCPv6 Server

DHCPv6 Configuration Examples CLI Commands

To set the DHCPv6 server parameters:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
dhcpv6-server range A:B::C:D A:B::C:D
dhcpv6-server lease-time <0-864000>

Usage Example:

```
switch_a> enable
switch_a#configure terminal
switch_a(config)#dhcpv6-server range
fda8:06c3:ce53:a890:0000:0000:0000:0001
fda8:06c3:ce53:a890:0000:0000:0000:1001
switch_a(config)#dhcpv6-server lease-time 86400
switch_a(config)#q
switch_a#
```

DHCP Relay

DHCP relay function is used to forward requests and replies between clients and servers while they are not on the same physical subnet, all the subnets can share the same DHCP server. Saving the need of server transmit different subnets' DHCP packets.

General Overview

EtherWAN DHCP relay agents receive DHCP messages and then generate a new DHCP message to send out on another interface. The relay agent sets the gateway address (giaddr field of the DHCP packet) and, if configured, adds the relay agent information option (option82) in the packet and forwards it to the DHCP server. The reply from the server is forwarded back to the client after removing option 82.

To configure a DHCP relay, first enter the IP address of a DHCP relay server. Then select the ports, and enable Option 82 (for added security) and domain-wide status (if required).

Configuring the DHCP Relay

To navigate to the **DHCP Relay** page:

1. Click on the **+** next to **Other Protocols**
2. Click on **DHCP Relay** (see **Figure 180**)

To enable the DHCP Relay function features:

1. Select the **Global** item for settings
2. Select “Enable” from the dropdown menu of **Enable** item.
3. Select “Enable” from the dropdown menu of **Option 82** item if required.
4. Click **Update Setting**.
5. Click **Restart** for setting initial

To add or delete DHCP Relay Server IP Address:

1. Select the **Add or Delete Server IP Address** item for settings
2. Input “IP Address” in the blank menu of add or delete Server IP Address.
3. Click “add” then the input IP were bing added
4. The added IP Address were bing shown to Relay Server IP List

To set the DHCP Relay interface domain and status:

1. Select the **DHCP Relay Interface** for setting.
2. Select “VLAN” from the dropdown menu.
3. Select “**Enable**” or “**Disable**” for Relay status.
4. Click **Update Setting**.

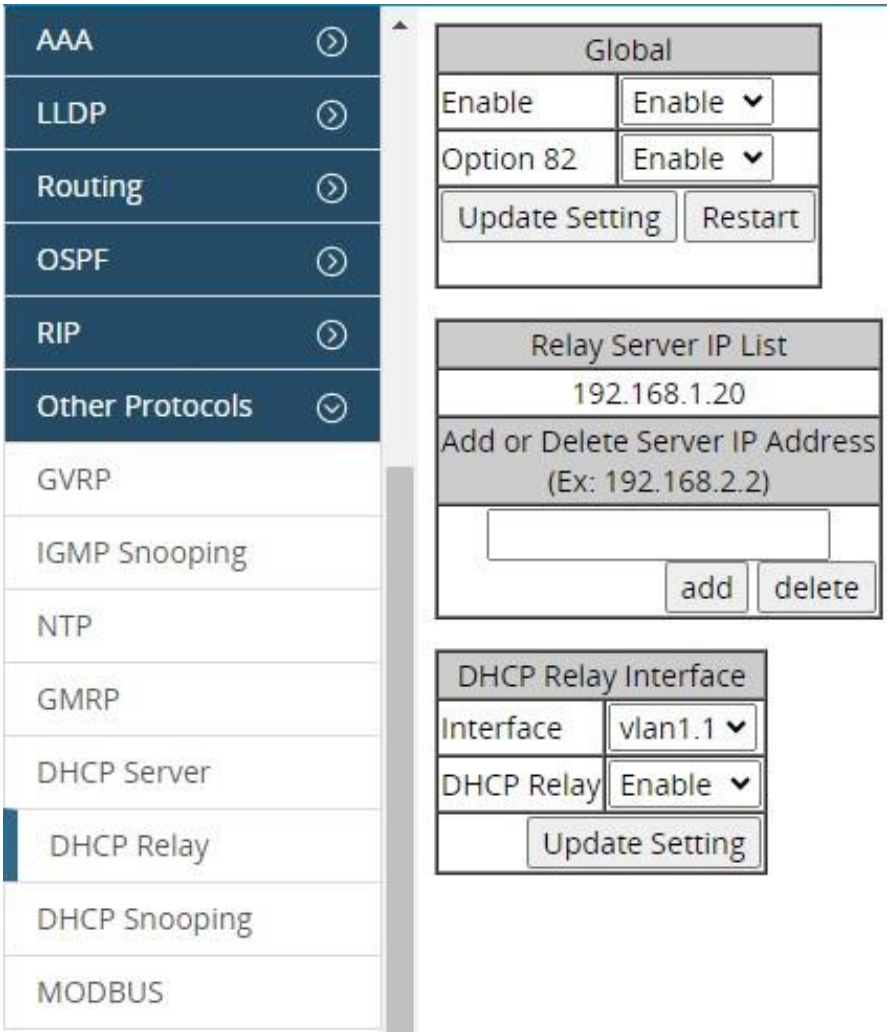


Figure 180: DHCP Relay settings

DHCP Relay Configuration of CLI Commands

To set the DHCP Relay function features:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
dhcprelay enable
no dhcprelay enable (default)

To add DHCP server IP configuration:

CLI Command Syntax:
dhcprelay serverip <A.B.C.D>
no dhcprelay serverip <A.B.C.D>

To enable DHCP Relay **Option 82** configuration:

CLI Command Syntax:
dhcprelay information-option
no dhcprelay information-option

To enable DHCP Relay **Interface** configuration:

CLI Command Syntax:
dhcprelay Interface enable
no dhcprelay Interface enable

To Restart DHCP Relay configuration:

CLI Command Syntax:
dhcprelay restart

Usage Example 1: Set DHCP Relay status.

```
switch_a#configure terminal
switch_a(config)# dhcprelay enable
switch_a(config-if)#exit
```

Usage Example 2: Set DHCP Relay server ip 192.168.10.53

```
switch_a(config)#dhcp-snooping enable
switch_a(config)#dhcprelay serverip 192.168.10.53
```

Usage Example 3: Enable DHCP Relay on vlan1.1 and set server ip 192.168.1.253 with option 82 then restart status.

```
switch_a(config)#int vlan1.1
switch_a(config-if)#dhcprelay interface enable
switch_a(config-if)#exit
switch_a(config)#dhcprelay serverip 192.168.1.253
switch_a(config)#dhcprelay information-option
switch_a(config)#dhcprelay enable
switch_a(config)#dhcprelay restart
```

DHCP Snooping

DHCP Snooping is a security feature of DHCP (Dynamic Host Configuration Protocol). It is used to ensure that the DHCP client obtains an IP address from a legal DHCP server and

records the DHCP client IP address and MAC address. The correspondence between parameters is used to resist various attacks on DHCP on the network, providing users with a safer network environment and more stable network services.

General Overview

The EtherWAN switch administrators can specify the switch ports through the DHCP Snooping trust function. By control the source of DHCP server response messages to prevent possible DHCP Server counterfeiters in the network from allocating IP addresses and other configuration information to DHCP clients.

The DHCP Snooping binding table has bindings that are learned by DHCP snooping or are manually configured (static DHCP Snooping bindings). An entry in this table has an IP address, its associated MAC address, and its associated VLAN number.

The switch performs the following verification through DHCP snooping binding types:

- **Static:** configure a static ARP access control list for a static IP address.
- **Dynamic:** Reference to DHCP snooping binding table for DHCP assigned IP addresses.
- **All:** Refer to both configured ARP access control list & DHCP snooping binding table.

Configuring the DHCP Snooping

To navigate to the **DHCP Snooping** page:

1. Click on the **+** next to **Other Protocols**
2. Click on **DHCP Snooping** (see **Figure 181**)

To enable **DHCP Snooping** on the switch:

1. Select “**Enable**” from the dropdown menu of Mode item.
2. Click **Update Setting**.

To configure trust port settings:

1. Select the set target port.
2. Select “**Enable**” from the dropdown menu.
3. Click **Update Setting**.

To configure Binding Type settings:

1. Select the DHCP Snooping Binding Type item.
2. Select type of binding from the dropdown menu.

- Static / Dynamic / All

3. Click **Update Setting**.

To configure a Static IP address Binding settings:

1. Select the “DHCP Snooping Binding Table” item.
2. Configure a static binding with **MAC / IP address / VLAN** for corresponding ports.
3. Click **Update Setting**.

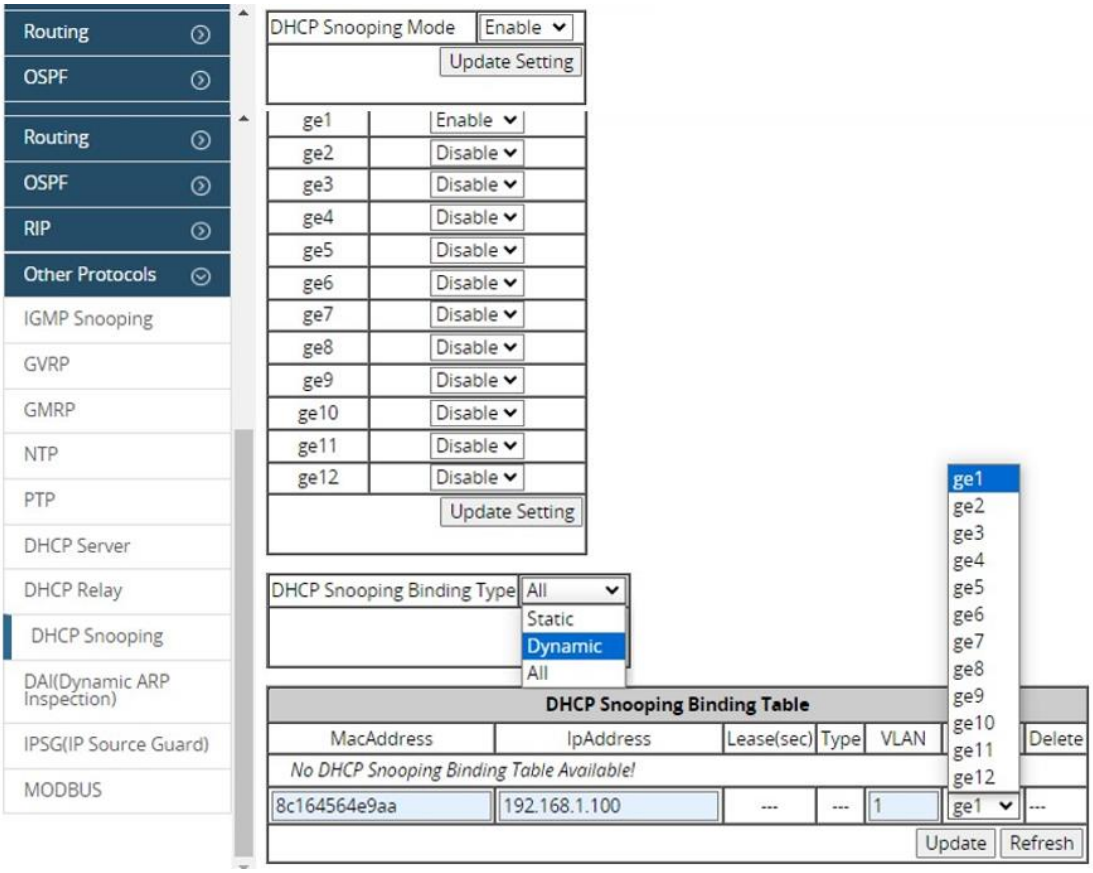


Figure 171: DHCP Snooping

DHCP Snooping Configuration of CLI Commands

To set the DHCP Snooping function features:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:

dhcp-snooping enable

no dhcp-snooping enable (default)

dhcp-snooping binding <mac-address> vlan <vlan-id> <ip-address> interface <if-name>

Add static binding

no dhcp-snooping binding <mac-address>

Delete static binding

To set the Interface configuration:

CLI Command Syntax:

dhcp-snooping trust

Set the port as DHCP Snooping trusted port

no dhcp-snooping trust

Set the port as DHCP Snooping untrusted port (default)

show dhcp-snooping binding

Check dhcp-snooping binding

Usage Example 1: Set dhcp-snooping enable on ge1.

```
switch_a>enable
switch_a#configure terminal
switch_a(config)#dhcp-snooping enable
switch_a(config)#int ge1
switch_a(config)#dhcp-snooping trust
switch_a(config-if)#exit
```

Usage Example 2: Set dhcp-snooping binding.

```
switch_a(config)#dhcp-snooping enable
switch_a(config)#dhcp-snooping binding aaaa.bbbb.cccc vlan 1
10.10.1.3 interface ge1
```

Usage Example 3: Set dhcp-snooping binding.

```
switch_a(config)#dhcp-snooping enable
switch_a(config)#dhcp-snooping binding aaaa.bbbb.cccc vlan 1
10.10.1.3 interface ge1
```

Usage Example 4: Check DHCP Snooping Binding status.

```
switch_a#show dhcp-snooping binding

MacAddress          IpAddress        Lease(sec)  Type           VLAN  Interface
------------------  ---------------  ----------  -------------  ----  ---------
0001.2222.3333      192.168.1.111    infinite    static         1     ge1
0001.2222.3334      192.168.1.112    infinite    static         1     ge2
00e0.b3aa.5664      192.168.1.14     5933        dynamic        1     ge12
```

Dynamic ARP Inspection (DAI)

Dynamic ARP Inspection (DAI) is a security feature that protects networks against man-in-the-middle ARP spoofing attacks. DAI filtering is applied to the traffic ingress ports, performs verification by intercepting each ARP packet and comparing its MAC and IP address information to the MAC-IP binding contained in the DHCP snooping table.

Any ARP packets that are inconsistent with the information contained in the DHCP snooping table will be discarded.

General Overview

The EtherWAN switch administrators can specify the switch ports as trusted and untrusted ports by using DAI:

- **Trust port settings**- Trusted ports can forward any ARP information.
- **Untrust port settings**- ARP messages on untrusted ports must be verified by ARP inspection.

Configuring the Dynamic ARP Inspection

Before the configuration, please confirm that the **DHCP snooping** setting has been **enabled** and the necessary filling of the binding table has been completed.

To navigate to the **Dynamic ARP Inspection** page:

1. Click on the **+** next to **Other Protocols**
2. Click on **Dynamic ARP Inspection** (see Figure 182)

To enable Dynamic ARP Inspection on the switch:

1. Select “**Enable**” from the dropdown menu of Mode.
2. Click **Update Setting**.

To configure trust port settings:

1. Select the set target port.
2. Select “**Enable**” from the dropdown menu.
3. Click **Update Setting**.

Warning: Once the **DAI** mode is enabled, be sure set the corresponding port connecting to the WEB GUI interface to **trust enabled** to avoid access denial of control.

Observe the Inspection results -

The statistical of inspection results can be observed from the DAI count table in below, the number of forwarded and discarded ARP messages also the counter can be reset by click "**Clear**".

Note: 1. Configuring ports as untrusted when they should be trusted can result in a loss of connectivity, including Web/Telnet/SSH to the switch itself.

2. The trunk interface of the switch cascade must be configured as a trusted port.
3. Even if there is no DHCP server, configuration of DHCP snooping is still need.

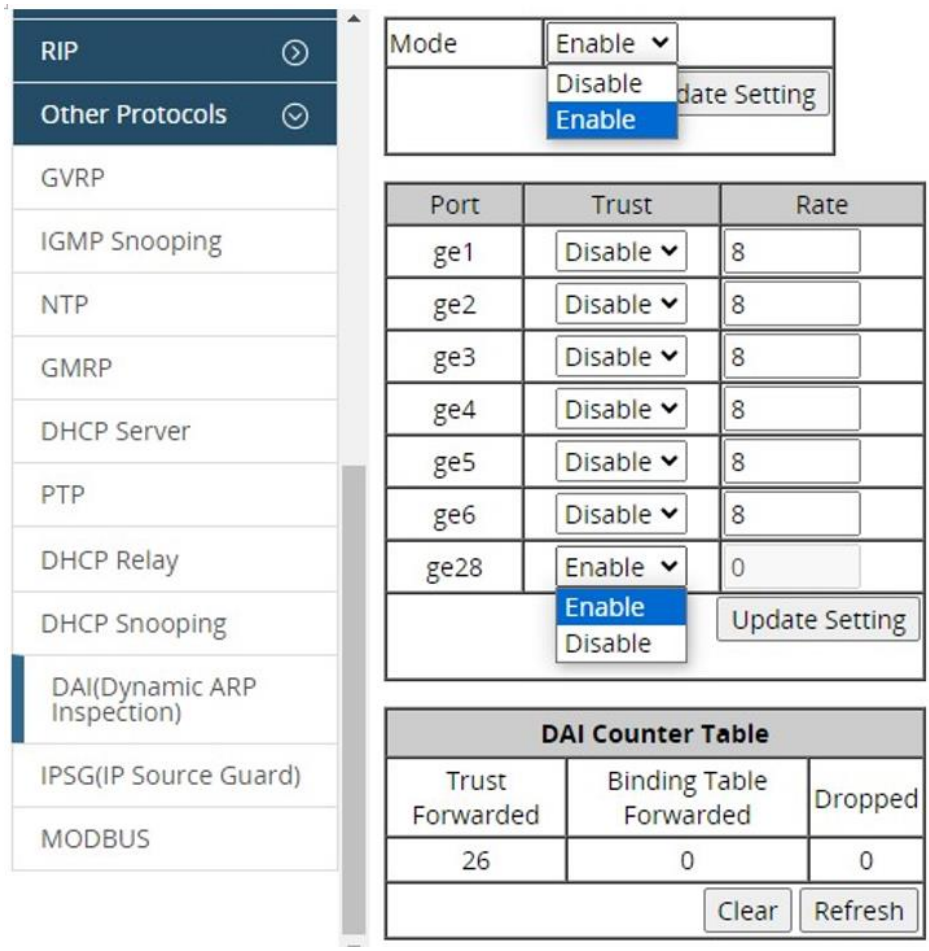


Figure 172: Dynamic ARP Inspection

DAI Configuration of CLI Commands

To set the DAI function features:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:

ip arp inspection
no ip arp inspection

To set the Interface configuration:

CLI Command Syntax:

ip arp inspection trust

Set the port as DAI trusted port, no rate limit.

no ip arp inspection trust

Set the port as DAI untrusted port (default), rate limit is 8 kbps.

clear ip arp inspection statistics
show ip arp inspection interfaces
show ip arp inspection statistics

Usage Example 1: Set DAI port configuration on ge1.

```
switch_a(config)#int ge1
switch_a(config-if)#dhcp-snooping trust
switch_a(config-if)#exit
switch_a(config)#ip arp inspection
switch_a(config)#int ge1
switch_a(config-if)#ip arp inspection trust
switch_a(config)# exit
switch_a#
```

Usage Example 2: Show DAI interface.

```
switch_a(config)#show ip arp inspection interfaces

   Interface  Trust State   Rate(kbps)
   -----------------------------------
        ge1      Trusted   infinite
        ge2    Untrusted   8
        ge3    Untrusted   8
        ge4    Untrusted   8
        ge5    Untrusted   8
        ge6    Untrusted   8
        ge7    Untrusted   8
        ge8    Untrusted   8
        ge9      Trusted   infinite
       ge10    Untrusted   8
       ge11    Untrusted   8
       ge12    Untrusted   8
```

Usage Example 3: Show DAI statistics.

```
switch_a(config)#show ip arp inspection statistics

   Trust Forwarded  Binding Table Forwarded  Dropped
   --------------  ----------------------  --------
                11                       4        22
```

Usage Example 4: Clear DAI counters.

```
switch_a#clear ip arp inspection statistics
```

IP Source Guard (IPSG)

IP Source Guard provides source IP address filtering on a Layer 2 port to prevent a malicious host from impersonating a legitimate host by assuming the legitimate host's IP address. The feature uses dynamic DHCP snooping and static IP source binding to match IP addresses to hosts on untrusted Layer 2 access ports.

All IP traffic on the protected port is blocked except Initially for DHCP packets. After a client receives an IP address from the DHCP server, or after static IP source binding is configured by the administrator, all traffic with that IP source address is permitted from that client. Traffic from other hosts is denied.

This filtering limits a host's ability to attack the network by claiming a neighbor host's IP address. IP Source Guard is a port-based feature that automatically creates an implicit port access control list (PACL).

General Overview

EtherWAN switches provide source-specific inspection of ingress ports by configuring switch ports via IPSG to use source IP address and/or source MAC address filtering:

- **Source IP Address Filtering**- The switch forwards IP traffic when the source IP address matches a DHCP Snooping binding.
- **Source IP and Source MAC Address Filtering**- The switch forwards traffic only when the source IP address and the source MAC address match a DHCP Snooping binding.

Configuring the IP Source Guard

Before the configuration, please confirm that the **DHCP snooping** setting has been **enabled** and the necessary filling of the binding table has been completed.

To navigate to the **IP Source Guard** page:

3. Click on the **+** next to **Other Protocols**
4. Click on **IP Source Guard** (see **Figure 183**)

To enable IP Source Guard on the switch ports with **source IP filtering**:

5. Select the target port for settings
6. Select "**Enable**" from the dropdown menu of Mode item.
7. Click **Update Setting**.

To enable IP Source Guard on the switch ports with **source IP & source MAC filtering**:

1. Select the target port for settings
2. Select "**Enable**" from the dropdown menu of Mode item.

3. Select “**Enable**” from the dropdown menu of MAC check item.
4. Click **Update Setting**.

Note: 1. DHCP Snooping should be enabled simultaneously when setting up IPSG for the corresponding ports, otherwise the Web/Telnet/SSH connection to the switch itself may be lost.

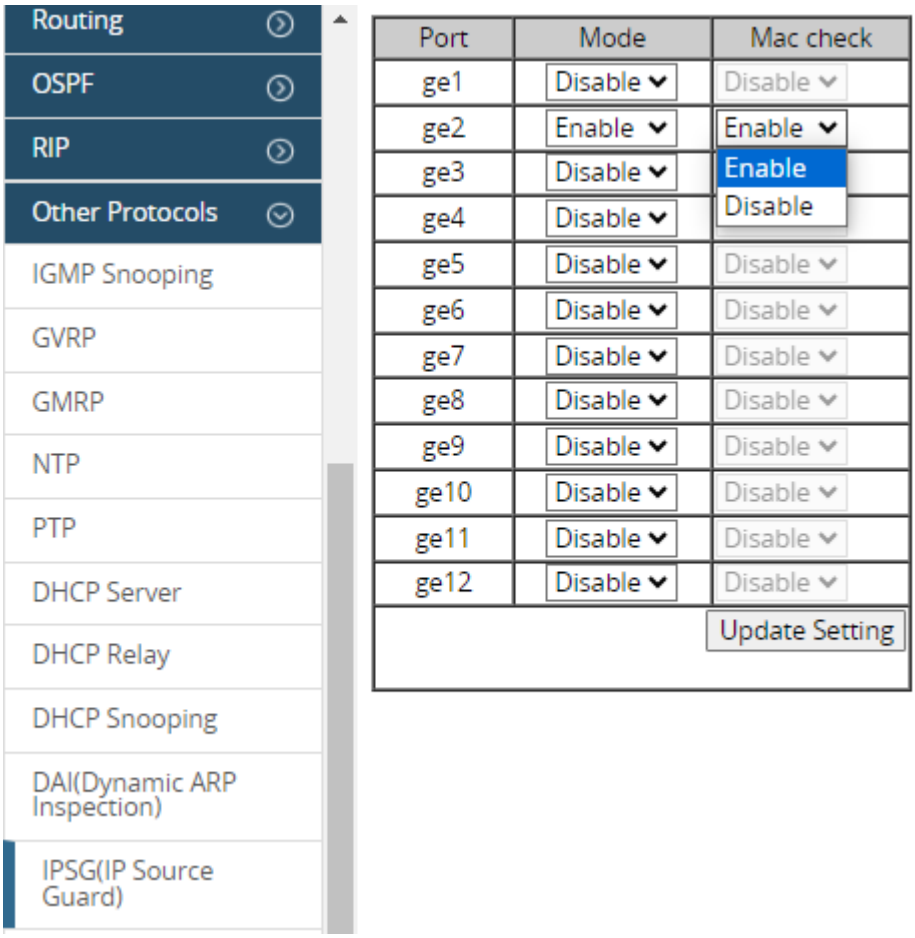


Figure 173: IP Source Guard

IPSG Configuration of CLI Commands

To set the **IPSG** Interface configuration:

CLI Command Mode: **Global Configuration Mode**
CLI Command Syntax:
ip verify source [mac-check]
Enable IPSG with source IP filtering and optional source MAC filtering

no ip verify source

Disable IPSG (default)

show ip verify source statistics

show ip verify source binding statistics [vlan <vlan-id>]

Usage Example 1: Set IPSG configuration on ge2.

```
switch_a(config)#int ge2
switch_a(config-if)# ip verify source mac-check
switch_a(config)#exit
switch_a#
```

Usage Example 2: Show ip verify source statistics.

```
switch_a(config)#show ip verify source statistics

MacAddress          IpAddress        Type           VLAN  Interface  Forward
------------------  ---------------  -------------  ----  ---------  -------
0001.2222.3333      192.168.1.111    static         1        ge1        0
0001.2222.3334      192.168.1.112    static         1        ge2        0
00e0.b3aa.5664      192.168.1.14     static         1        ge12       3
```

Usage Example 3: Show ip verify source binding statistics.

```
switch_a(config)#show ip verify source binding statistics

   Interface  Drop
   ---------  ------------
   ge1        0
   ge2        0
   ge3        0
   ge4        0
   ge5        0
   ge6        0
   ge7        0
   ge8        0
   ge9        15
   ge10       0
   ge11       0
   ge12       2
   ge13       0
   ge14       0
   ge15       0
   ge16       0
```

Modbus TCP

Modbus is a serial communications protocol for client-server communication between a switch (server) and a device in the network running Modbus client software (client). User can access through Modbus protocol to connect a computer to a remote terminal unit (RTU) in supervisory control and data acquisition (SCADA) systems. It is also a vendor-neutral communication protocol used to monitor and control industrial automation equipment such as PLCs, sensors, and meters.

Functional Description

Modbus transaction

The MODBUS protocol defines a simple protocol data unit (PDU) independent of the underlying communication layers. The mapping of MODBUS protocol on specific buses or network can introduce some additional fields on the application data unit (ADU).

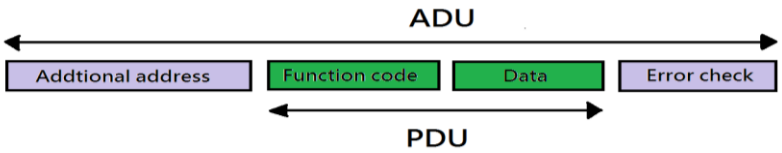


Figure 174: Modbus protocol defination

The switch encapsulates a request or response message in a MODBUS TCP application data unit (ADU). A client sends a message to a TCP port on the switch. The default port number is **502**

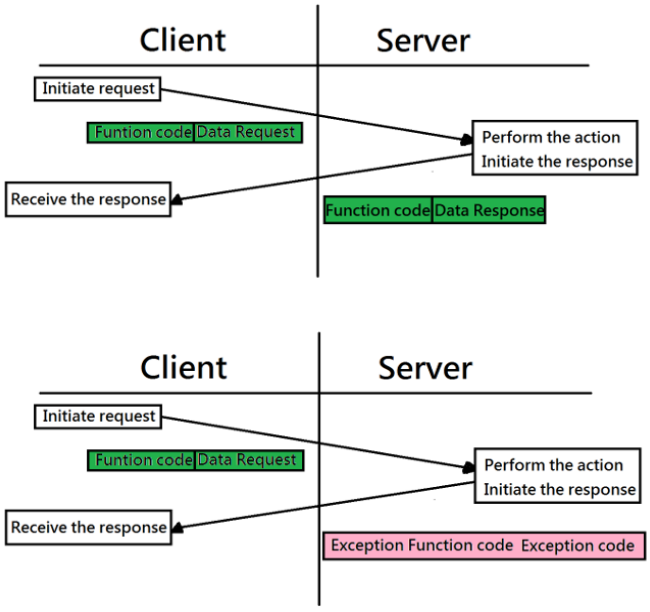


Figure 175: Modbus transaction

Data Format and Function code

Modbus TCP supports different types of data format for reading.

EtherWAN switches support Function Code 3 and Code 6.

Data Access Type		Function Code	Function name
Bit access	Physical Discrete Inputs	2	Read Discrete Inputs
	Internal Bits or Physical Coils	1	Read Coils
16 bits access	Physical Input Registers	4	Read Input Registers
	Physical Output Registers	**3**	Read Multiple Holding Registers
		6	Write Single Holding Register

Figure 176: Modbus function code

Function code 03(0x03) Read Holding Registers

This function code is used to read the contents of a contiguous block of holding registers in a remote device. The Request PDU specifies the starting register address and the number of registers.

The register data in the response message are packed as two bytes per register, with the binary contents right justified within each byte. For each register, the first byte contains the high order bits and the second contains the low order bits.

Request

Function code	1 Byte	0x03
Starting Address	2 Bytes	0x0000 to 0xFFFF
Quantity of Registers	2 Bytes	1 to 125 (0x7D)

Response

Function code	1 Byte	0x03
Byte count	2 Bytes	2 * N

Register value	N *2 Bytes	

Error

Error code	1 Byte	0x83
Exception code	1 Byte	01 or 02 or 04

Here is an example of a request to read registers 108 – 110:

Request		Response	
Field Name	(Hex)	Field Name	(Hex)
Function	03	Function	03
Starting Address Hi	00	Byte Count	06
Starting Address Lo	6B	Register value Hi (108)	02
No. of Registers Hi	00	Register value Lo (108)	2B
No. of Registers Lo	03	Register value Hi (109)	00
		Register value Lo (109)	00
		Register value Hi (110)	00
		Register value Lo (110)	64

Figure 177: Function code 03 Registers

Function code 06(0x06) Read Holding Registers

This function code is used to write a single holding register in a remote device. The Request PDU specifies the address of the register to be written. Registers are addressed starting at zero. Therefore register numbered 1 is addressed as 0. The normal response is an echo of the request, returned after the register contents have been written.

Request

Function code	1 Byte	0x06
Register Address	2 Bytes	0x0000 to 0xFFFF
Register Value	2 Bytes	0x0000 to 0xFFFF

Response

Function code	1 Byte	0x06
Register Address	2 Bytes	0x0000 to 0xFFFF
Register Value	2 Bytes	0x0000 to 0xFFFF

Error

Error code	1 Byte	0x86
Exception code	1 Byte	01 or 02 or 04

Here is an example of a request to write register 2 with value 0x0003:

Request		Response	
Field Name	(Hex)	Field Name	(Hex)
Function	06	Function	06
Register Address Hi	00	Register Address Hi	00
Register Address Lo	01	Register Address Lo	01
Register Value Hi	00	Register Value Hi	00
Register Value Lo	03	Register Value Lo	03

Figure 178: Function code 06 Registers

Configuring the MODBUS Function features

To navigate to the Modbus page:

1. Click on the **+** next to **Other Protocols**
2. Click on **MODBUS** (see **Figure 189**)

To enable Modbus on the switch:

1. Select the **Modbus Server Golbol Setting** item.
2. Select "**Enable**" from the dropdown menu of Modbus state item.
3. Click **Update Setting**.

To set Modbus Configuration:

1. Select the **Modbus Configuration** item.

2. Fill the modbus tcp port from <**1~65535>** in the blank of port number. (default port number is **502)**
3. Set modbus tcp server connection number <**1~5**>
4. Click **Update Setting**.

Then the result of connected Modbus server IP & Port information were shown in the table below.

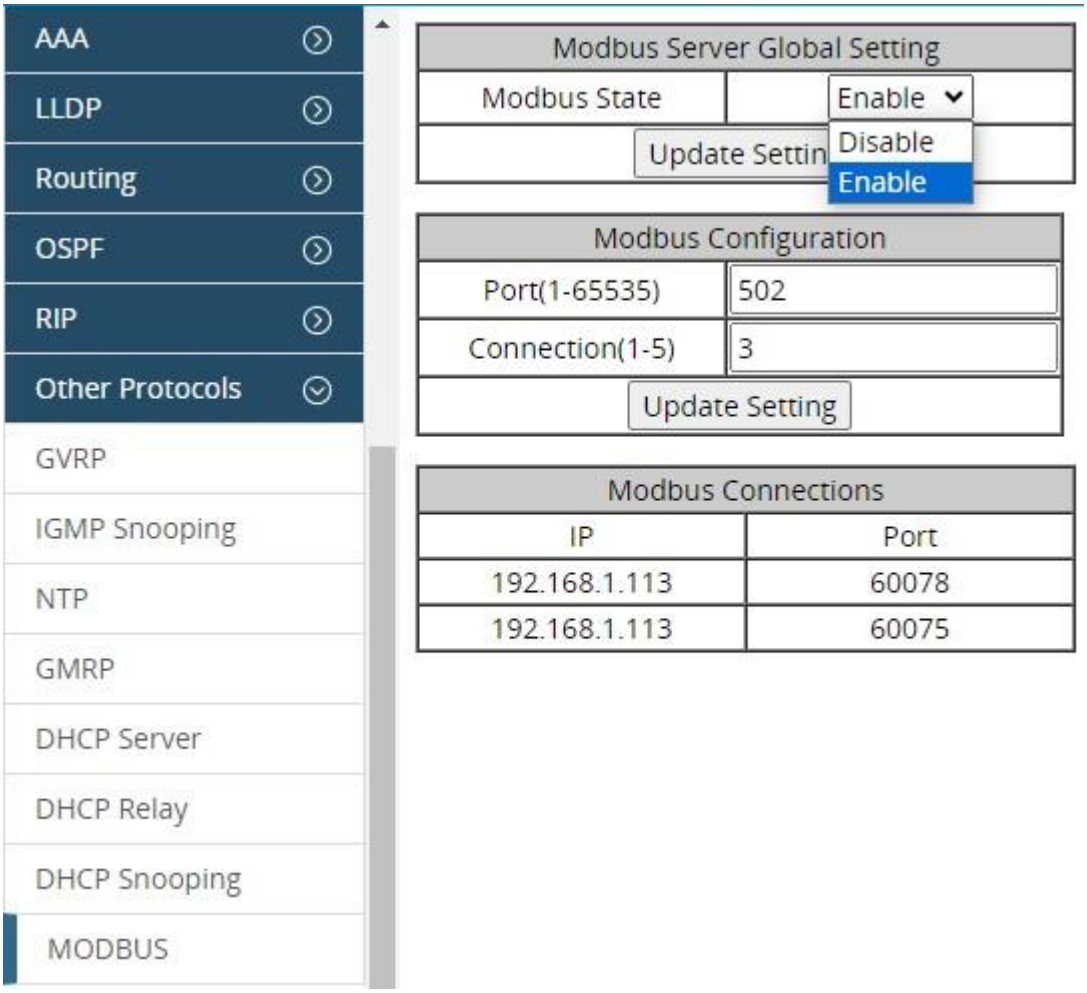


Figure 189 Modbus settings

Modbus Configuration of CLI Commands

To set the Modbus register parameters:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:

scada modbus tcp server

Enable modbus server service.

no scada modbus tcp server

Disable modbus server service.

scada modbus tcp server port {default | <1-65535>}

Set modbus tcp port which default port is **502**.

scada modbus tcp server connection <1-5>

Set modbus tcp server connection number

Usage Example 1: Enable modbus server service

```
switch_a(config)#scada modbus tcp server
switch_a(config)#exit
switch_a#
```

Register table

The EtherWAN Switch Modbus Registers –

	Address	Quantity	Min	Max	Interpretation	Description	Read/Write
System Information	0x0002	1 word			HEX	**Unit ID (Ethernet = 1)**	Read Only
	0x0006 to 0x000B	6 words			ASCII	**Product Serial Number**	Read Only
	0x0031 to 0x0045	21 words			ASCII	**Product Name**	Read Only
	0x0052	1 word			HEX	**Firmware Version**	Read Only
	0x0053 to 0x0054	2 words	0x0000	0xFFFF	HEX	**System Uptime**	Read Only
	0x0056 to 0x0058	3 words	0x000000000000	0xFFFFFFFFFFFF	HEX	**Ethernet MAC Address**	Read Only
System Diagnostics	0x0059	1 word	0x0000	0x0001	HEX	**Power 1**	Read Only
	0x005A	1 word	0x0000	0x0001	HEX	**Power 2**	Read Only
	0x0061	1 word	0x0000	0x0101	HEX	**Alarm Contact Status**	Read Only
	0x0062 to 0x0064	3 words	0x0000	0x010101	HEX	**Alarm Contact Events**	Read Only
	0x0073	1 word	0x0000	0x6464	HEX	**CPU utilization**	Read Only

Port Status	0x00D1 to 0x0110	1 word	0x0000	0xFFFF	HEX	Port **Status** (Port 1 to 64)	Read Only
	0x0111 to 0x0150	1 word	0x0000	0xFFFF	HEX	Port **Speed** (Ports 1 to 64)	Read Only
	0x0151 to 0x0190	1 word	0x0000	0xFFFF	HEX	Port **Flow Ctrl** (Ports 1 to 64)	Read Only
Port Diagnostics	0x0301	1 word	0x0000	0x0001	HEX	**All Ports - Reset All Port Statistics**	**Read/Write**
	0x0801, 0x0833, … , 0x144F	1 word	0	4294967295	32-bit unsigned long	Port (1 - 64) - Number of **broadcast frames received**	Read Only
	0x0803, 0x0835, … , 0x1451	1 word	0	4294967295	32-bit unsigned long	Port (1 - 64) - Number of **multicast frames received**	Read Only
	0x0805, 0x0837, … , 0x1453	1 word	0	4294967295	32-bit unsigned long	Port (1 - 64) - Number of **frames with CRC error**	Read Only
	0x0807, 0x0839, … , 0x1455	1 word	0	4294967295	32-bit unsigned long	Port (1 - 64) - Number of **oversized frames received**	Read Only
	0x080B, 0x083D, … , 0x1459	1 word	0	4294967295	32-bit unsigned long	Port (1 - 64) - Number of **jabber frames received**	Read Only
	0x080D, 0x083F, … , 0x145B	1 word	0	4294967295	32-bit unsigned long	Port (1 - 64) - Number of **collisions occurred**	Read Only
	0x080F, 0x0841, … , 0x145D	1 word	0	4294967295	32-bit unsigned long	Port (1 - 64) - Number of **64-byte frames received/sent**	Read Only
	0x081B, 0x084D, … , 0x1469	1 word	0	4294967295	32-bit unsigned long	Port (1 - 64) - Number of **dropped received packets**	Read Only
Redundancy Information	0x0501 to 0x0540	1 word	0x0000	0xFFFF	HEX	**R/STP Role** (Ports 1 - 64) 0x0000 = Default 0x0001 = Disabled 0x0002 = Root 0x0003 = Designated 0x0004 = Blocking / Backup 0x0005 = Alternate 0xFFFF = No Port	Read Only

	0x0541	1 word	0x0000	0x4040	HEX	**Ring Ports** Hi byte = Ring Port 1 Lo byte = Ring Port 2	Read Only
	0x0543	1 word	0x0000	0x4040	HEX	**Ring-coupling Ports** Hi byte = Ring Port 1 Lo byte = Ring Port 2	Read Only

Figure 190 Modbus Register table

RESTful API

The EtherWAN switch provides an application programming interface (API) follow the REST principles architectural style for web services. Through the the defination of parameters whthin the switch, assist developers to implement applications can communicate with their applications programmatically enables integration with other software systems.

API Command List

API Auth. Header Parameters for EtherWAN Router SOW

Required Header Field	Value	Comments
x-request-key	ewapi	
authorization	Bearer {{user-token}}	1. get user-token by login api 2. set this value after login

Figure 191 API Auth. Header Parameters

API Auth. Parameters for EtherWAN Router SOW

Section	Required Device Information	API Call (POST)	Request Body
Login			
	user	/api/auth/login	`{ "user": "user", "password": "password" }`
Logout			
		/api/auth/logout	

Figure 192 API Auth. Header Parameters

API Read Parameters for EtherWAN Router SOW

Section	Required Device Information	API Call (Get)	Comments
Device Info			
	sysName	/api/device/basic	Single entry
	firmwareVersion	/api/device/basic	Single entry
	macAddress	/api/device/basic	Single entry
	productSeries	/api/device/basic	Single entry
IP Address			
	ip	/api/device/netaddess	List
	netmask	/api/device/netaddess	List
	defaultGateWay	/api/device/netaddess	Single Entry
Switch Ports			
	Interfaces	/api/interfaces	Get Interface list, Return the Interface ID list
	interfaceId	/api/interfaces/INTERFACE_ID	List
	interfaceDescript	/api/interfaces/INTERFACE_ID	List
	interfaceStatus	/api/interfaces/INTERFACE_ID	List
	speed	/api/interfaces/INTERFACE_ID	List
	stpPortState	/api/interfaces/INTERFACE_ID	List
VLAN			
	vlanID	/api/vlans	List
	vlanName	/api/vlans	List
	vlanStaticPortMap	/api/vlans	List
	vlanUntaggedPortMap	/api/vlans	List
LLDP Neighbors			
	chassisIdSubtype	/api/lldp	Single entry
	chassisId	/api/lldp	Single entry
	localInterfaces/interfaceId	/api/lldp	List - localInterfaces
	localInterfaces/interfaceDescr	/api/lldp	List - localInterfaces
	remote/lldpRemLocalPortNum	/api/lldp	List - remote
	remote/lldpRemChassisIdSubtype	/api/lldp	List - remote
	remote/lldpRemChassisId	/api/lldp	List - remote
	remote/lldpRemPortId	/api/lldp	List - remote
	remote/remoteIp	/api/lldp	List - remote
Statistics			
	interfaceId	/api/interfaces/INTERFACE_ID/stats	List
	speed	/api/interfaces/INTERFACE_ID/stats	List
	inOctets	/api/interfaces/INTERFACE_ID/stats	List

	outOctets	/api/interfaces/INTERFACE_ID/stats	List
	inUcastPkts	/api/interfaces/INTERFACE_ID/stats	List
	outUcastPkts	/api/interfaces/INTERFACE_ID/stats	List

Figure 193 API Read Parameters

API Write Parameters for EtherWAN Router SOW

Section	Required Device Information	API Call (POST)	Comments
Switch Ports			
	Port Enable	/api/interfaces/INTERFACE_ID/enable	
	Port Disable	/api/interfaces/INTERFACE_ID/disable	
Remote Control			
	System Reboot	/api/device/reboot	

Figure 194 API Write Parameters

CYBER SECURITY INDEX

Security Context

The product series with possible intended use cases and the deployment environment outline recommend examples as below:

General Description of the Product/System

This product allows users to transmit common industrial protocols for manufacturing applications based on Ethernet or Internet architecture, forward and collect various automation applications, instructions, and records, including control, safety, synchronization, motion, status, configuration, and information.

As a reliable device for implementing internal/external communication protocols in the system, it integrates a variety of message transmission functions to ensure that this product under the normal operating procedures of wired transmission system operation within the DMZ range is not easily damaged by external interference to change its original functions or affect the entire environment.

Intended Use Cases Description

According to functional requirements, there are 3 intended use cases of configuration to be straight-liner, redundant backup, and ring connection as shown in the figure below-

a. Cell/Area Zone Linear Topology L1/L2 switch in manufacturing area

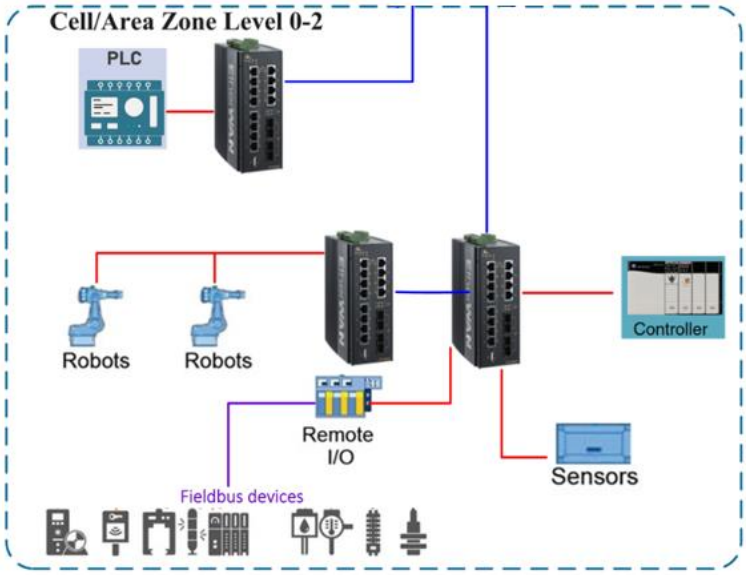


Figure 195: The linear use case of Product-Model_ EX78900x series (stand-alone mode)

b. Cell/Area Zone Redundant Topology L1/L2 switch in manufacturing area

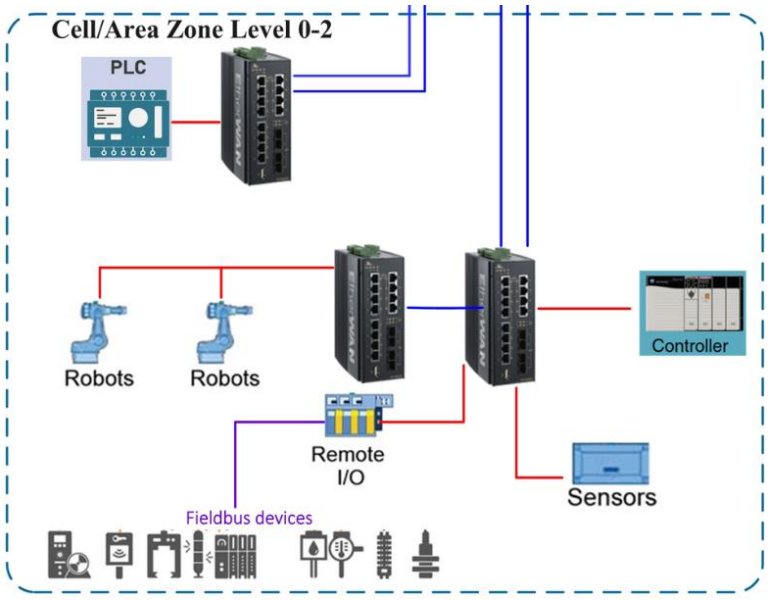


Figure 196: The redundant use case of Product-Model_ EX78900x series (stand-alone mode)

c. Cell/Area Zone Ring Topology L1/L2 switch in manufacturing area

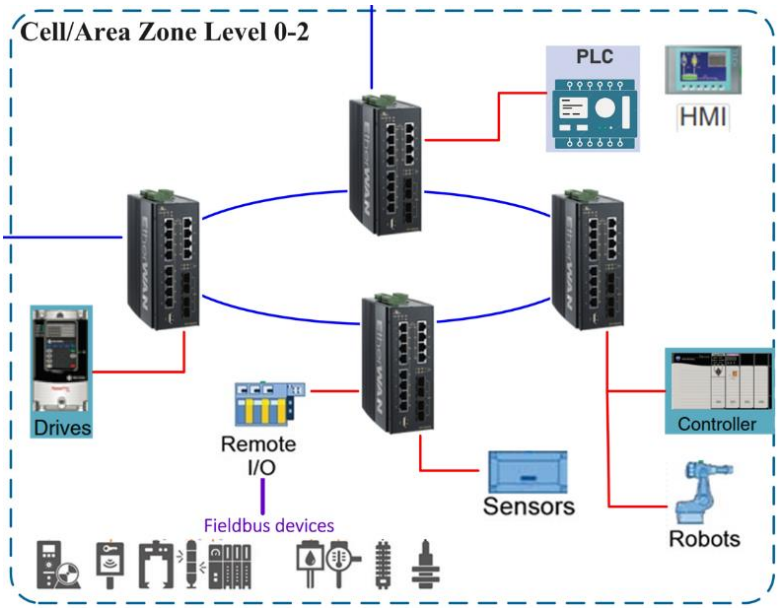


Figure 197: The ring use case of Product-Model_ EX78900E series (stand-alone mode)

Location in Intended Use Environment

The series of industrial switches are specifically applied in smart energy, urban rail, integrated pipeline, intelligent transportation, smart city, mining and metallurgical industry,

crude oil petrochemical industries, new energy technology, smart factories, ship, military, building security, and various infrastructure system constructions.

Site Operations and Control

The following figure provides two examples of network application construction structures - the switch device is within the scope of the IDMZ and is used to transmit common industrial protocols or manufacturing applications built with Ethernet or Internet architecture to communicate, forward and collect various automation application data flows. Through the operation level control division level and gateway facilities conduct the remote or on-site path to various control, security, synchronization, motion, configuration, and information transmission through the possible access path based on the switch device.

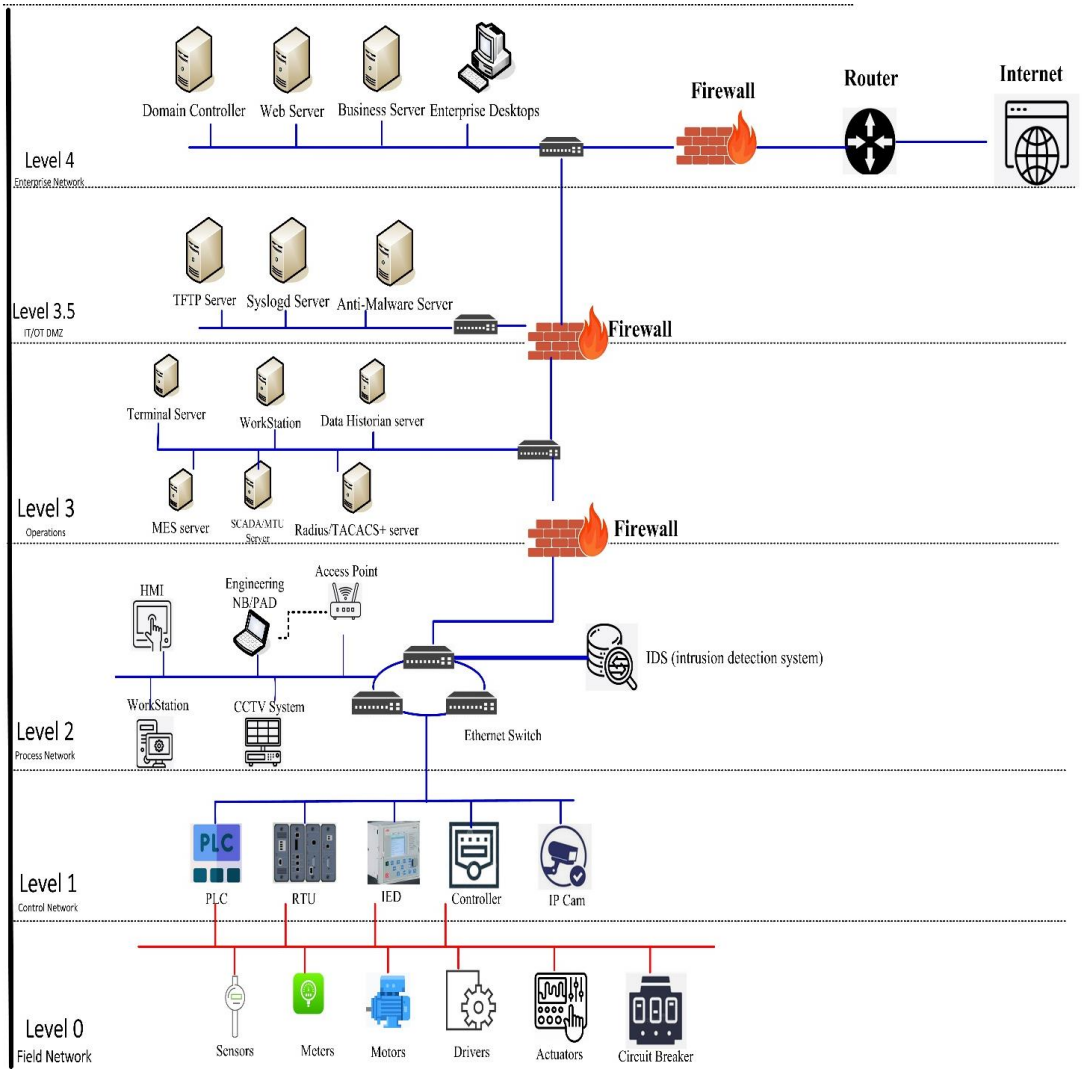


Figure 198: Location in Intended Environment for Site Operations and Control
(Case 1 - Operation Layer with Firewall)

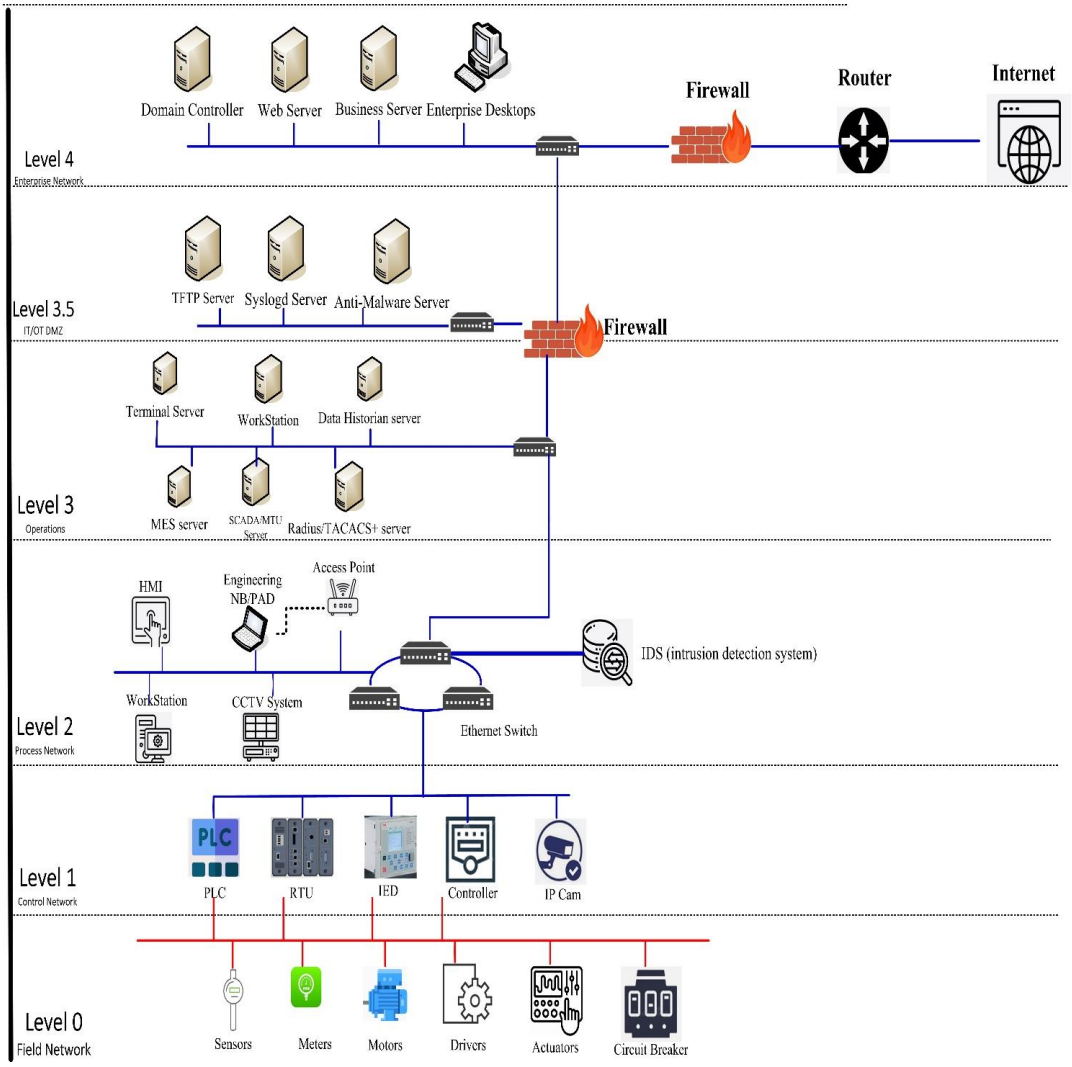


Figure 199: Location in Intended Environment for Site Operations and Control
(Case 2 - Operation Layer without Firewall)

Site IND Engineer Work

As shown in the figure below - the possible access paths of On-site IND engineer/ engineering maintainer based on job requirements in the network architecture application scope defined by the industrial application environment.

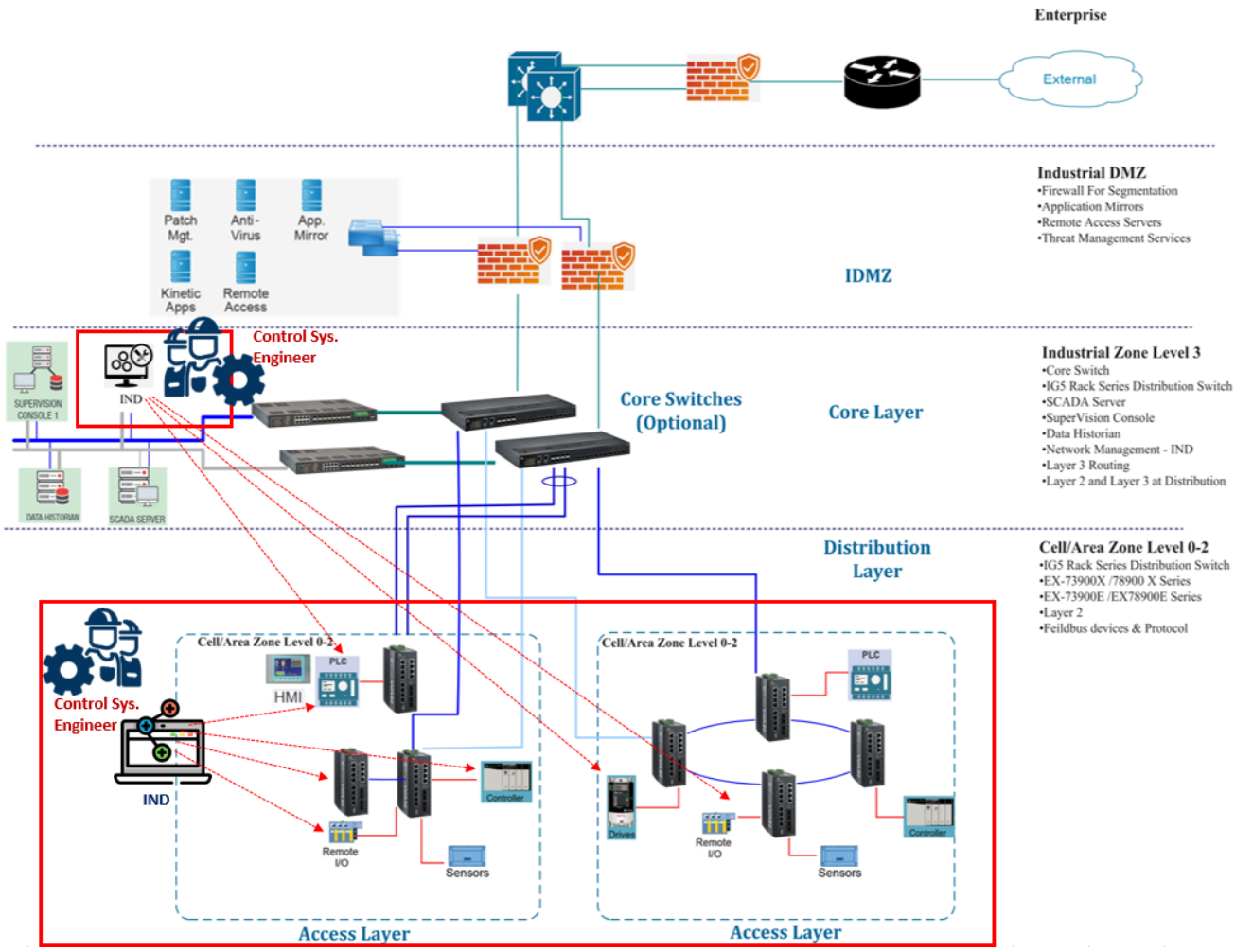


Figure 200: Location in Intended Environment for Site IND Engineer Work

Security Requirements

In order to meet IEC 62443 requirements, EtherWAN switch products has included the switch security features listed in the following table, as well as additional Port Security, SNMPv3, and DoS Protection related security features based on security concerns, to achieve derived from the system security levels defined in IEC 62443-3-3.

Switch Security Features

Feature	IEC-Secure Required	Details
MAC Address filtering	Yes	Block or allow specific MAC addresses for a port. Static MAC entry
Enable/Disable Port	Yes	Enable or disable network ports of the switch. Enable or disable a port
Storm control (broadcast and multicast)	Yes	Monitor traffic levels and drop packets when a specified is exceeded. Storm control
IEEE 802.1x LAN access control	Yes	Set authentication for users and devices. AAA authentication
Remote authentication through RADIUS	Yes	Allows remote access through a central server. RADIUS Authentication and Add RADIUS User
SSH for CLI and Telnet security	Yes	Encrypted communications through secure shell. SSH configuration
SSL for Web security	Yes	Establishes secured links. Secure Socket Layer
System log (remote/local)	Yes	Logs events and severity. System log and Remote logging
ACL	Yes	Create lists to selectively admit or reject inbound traffic. IP ACL (Access Control List)

Figure 201: Security Feature List

Switch operation with the above security features and the commands or procedures will not affect other industrial automation and control processes during its normal operation.

Port Security

Port security options include both **enabled** and **sticky** modes. Refer to Page 88, Port Security.

SNMP (SNMPv3)

SNMPv3 provides authentication and data encryption to meet privacy and security needs. Refer to Page 215, Configuring SNMP v3 Users.

DoS Protection

Choose from eleven functions to provide flexible and robust protection from Denial of Service attacks. Refer to Page 228, Configuring DoS (Denial of Service) from the GUI.

Firmware Upgrade Security

The system configuration when the loss of power occurs during an upgrade will keep the last configuration unchanged; therefore, booting from the primary firmware image or booting from the backup image can achieve regular operation without any missing information except caused by the hardware failure.

If users require a higher level of security than these security features mentioned above, we recommend installing additional security equipment such as a firewall to protect critical infrastructure.

Auditable events

The features and functions (refer to WEB GUI) which related to system security needs to be logged.

Log format:
At <Date> <System Time> (<Uptime>): User <username> <log description> via <interface>.

Date: month date year
System Time: hour: minute: second
Uptime: hour: minute: second
Username: the username of the user who performed the action.
Log description: A textual record of the performed action.
Interface: The interface the user uses to perform actions, as HTTP, TELNET, SSH, CONSOLE, SNMP

Example for output log:
At May 31 2022 08:13:10(05:18:10): User test123 saved configuration via HTTP.
At May 31 2022 08:12:40(05:18:40): User test123 created a user account testabc via TELNET.

At May 31 2022 08:12:10(05:18:10): User test123 failed to create user account via SSH.
At May 31 2022 08:11:40(05:18:40): User test123 changed NTP setting via CONSOLE.
At May 31 2022 08:11:10(05:18:10): User test123 changed NTP setting via SNMP.

The following is log description of each function:

System Name/Password

Success: changed System name/password setting.
Fail: failed to change System name/password setting

IP address

Success: changed IP address setting
Fail: failed to change IP address setting

IPv6 address

Success: changed IPv6 address setting
Fail: failed to change IPv6 address setting

Management Interface

Web Agent

Success: changed Web Agent setting (https enabled/disabled)
changed Web Agent setting (http enabled/disabled)
changed Web Agent setting (Login Failure Lock enabled/disabled)
Fail: failed to change Web Agent setting

Telnet

Success: changed Telnet setting (enabled/disabled)
Fail: failed to change Telnet setting

SSH

Success: changed SSH setting (enabled/disabled)
Fail: failed to change SSH setting

Save Configuration

Backup configuration file

Success: backup configuration file to <server ip>
Fail: fail to backup configuration file to <server ip>

Load configuration file

Success: load configuration file from <server ip>
Fail: fail to load configuration file from <server ip>

Save configuration file

Success: save configuration file
Fail: fail to save configuration file

Restore configuration file

Success: restore configuration file |from USB
Fail: fail to restore configuration file |from USB

Auto Save

Success: changed Auto Save setting
Fail: fail to change Auto Save setting

EB-232 Functionality

Success: changed EB-232 setting.
Fail: fail to change EB-232 setting.

Reset Button Setting

Success: changed Reset Button setting.

Fail: fail to change Reset Button setting.

Firmware Upgrade
Success: upgrade firmware successfully from <server ip>
Fail: fail to upgrade frimware from <server ip>

Reboot
Success: reboot the system
Fail: fail to reboot the system

User Account

User Login Mode
Success: changed the User Login Mode to <Single-User/Multi-User/Radius-User/ Radius-User Local/TACACS/TACACS Local>
Fail: fail to change the User Login Mode
User Account
Success: created|changed a <Admin/Operator/Technician> account <username>
Fail: fail to create|change user account.
User Privilege
Success: changed User Privilege setting
Fail: fail to change User Privilege setting

System Log

System Log Setting
Success: changed System Log setting
Fail: fail to change System Log setting
Clear Log
Success: cleared System Log
Fail: fail to clear System Log
Remote Logging
Success: changed Remote Logging setting
Fail: fail to change Remote Logging setting

Alarm Setting
Success: changed Alarm setting
Fail: fail to change Alarm setting

Email Alert
Success: changed Email Alert setting
Fail: fail to change Email Alert setting

Port Security
Success: changed Port Security setting on Port <port name>
Fail: fail to change Port Security setting on Port <port name>

Static MAC Entry
Success: changed Static MAC Entry setting
Fail: fail to change Static MAC Entry setting

Port Mirroring
Success: changed Port Mirroring setting

Fail: fail to change Port Mirroring setting

QoS
Success: changed QoS setting
Fail: fail to change QoS setting

ACL
Success: changed ACL setting
Fail: fail to change ACL setting

SNMP
SNMP General Setting
Success: changed SNMP General Setting
Fail: fail to change SNMP General Setting
SNMP v1/v2
Success: changed SNMP v1/v2 <get|set> community name
Fail: fail to change SNMP v1/v2 <get|set> community name
SNMP v3
Success: added a SNMPv3 user <username>
Fail: fail to add SNMPv3 user

Radius Configuration
Success: changed Radius Configuration
Fail: fail to change Radius Configuration

Port Authentication
Success: changed Port Authentication on Port <port name>
Fail: fail to change Port Authentication on Port <port name>

TACACS
Success: changed TACACS setting
Fail: fail to change TACACS setting

DoS
Success: changed DoS setting
Fail: fail to change DoS setting

NTP
Success: changed NTP setting
Fail: fail to change NTP setting

DHCP Server
Success: changed DHCP Server setting
Fail: fail to change DHCP Server setting

Security Function Verification

HTTPS

Success: Type the URL https://192.168.1.10/ into the address field of the browser and hit return. If the browser window login screen appears, it means SSL connection is provided for the browser access.
Fail: fail to connect Login page, and no display on browser.

TELNET

Success: “enable” button checked from setting screen. Remote server can reach through “telnet 192.168.1.10” of the browser, and response command Parameters.
Fail: The remote server is unreachable and no response as default and meet security requirement.

SSH

Success: Use an external program e.g. “Tera Term”, “Putty” to set SSH service for connection to the switch and Program UI displays the current SSH information & status.
Fail: fail to Login and no connection establisted.

ACL

Success: The created IP ACLs from source address and the source wildcard mask will be displayed at the bottom of the ACL setting page, and they can be the access or reject and be recorded by system logs.
Fail: the source address and wildcard mask link access without any rules or restrict to be follow.

Port Security

Success: Port Security uses dynamically or statically learned MAC addresses to restrict ingress traffic by limiting the MAC address allowed to send traffic to the port and prevent unauthorized network access.
Fail: Port no access limit and no prohibited MAC addresses, and can be access from unauthorized network.

CONTACT INFORMATION

EtherWAN Systems, Inc.

www.etherwan.com

USA Office

5 Jenner, Irvine, CA 92618
Tel: +1-714-779-3800
E-mail: info@etherwan.com

Pacific Rim Office

8F., No.2, Alley 6, Lane 235, Baoqiao Rd.
Xindian District, New Taipei City 231
Taiwan
Tel: +886 -2- 6629-8986
E-mail: info@etherwan.com.tw

For additional help and training, visit EtherWAN Academy – Your one-stop training resource:
https://academy.etherwan.com

EtherWAN has made a good faith effort to ensure the accuracy of the information in this document and disclaims the implied warranties of merchantability and fitness for a particular purpose, and makes no express warranties, except as may be stated in its written agreement with and for its customers.

EtherWAN shall not be held liable to anyone for any indirect, special or consequential damages due to omissions or errors. The information and specifications in this document are subject to change without notice.

Copyright 2024. All Rights Reserved.
All trademarks and registered trademarks are the property of their respective owners

July 1, 2024