EtherWAN EX77900 Series Hardened Managed Switch

User's Guide

FastFind Links

All Rights Reserved

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.
EtherOS™
Ethernet to the World™

All other Trademarks are property of their respective owners.

Warranty

For details on the EtherWAN warranty replacement policy, please visit our web site at:
https://kb.etherwan.com/index.php?CategoryID=13

Products Supported by this Manual:

E77900 Series Hardened Managed Switch with firmware version 2.01

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

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 2	5/12/2016	Firmware version 2.0.1

Document Conventions

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

Typographic Conventions

This guide 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.
| vertical bar	Indicates that you have a choice between two or more options or arguments.

UNPACKING AND INSTALLATION

This chapter describes how to unpack and install the EtherWAN Managed Switch

The topics covered in this chapter are:

Package Contents

When you unpack the product package, you will find the items listed below. Please inspect the contents, and report any apparent damage or missing items immediately to your authorized reseller.

- Managed Switch
- Product CD
- Quick Installation Guide
- External power adapter/Cable (depending on model)
- Console cable (depending on model)

Unpacking

Follow these steps to unpack the EtherWAN Managed Switch and prepare it for operation:

1. Open the carton and carefully remove the contents.
2. Return all packing materials to the carton. If possible, save the carton and packing material in case you need to ship or store the switch in the future.
3. Confirm that all items listed in the "Package Contents" section are included in the shipment. Check each item for damage. If any item is damaged or missing, notify your authorized EtherWAN representative.

Connecting power

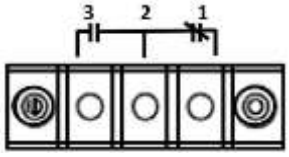
Terminal Block

If your EX77900 comes with power cables, connect the cables into the power modules at the back of the switch. If your switch comes with a terminal block (no cable), then connect the switch to a suitable power supply using 12 to 24 AWG wire.

Redundant power supply is supported. However, only one power input is required to operate the switch.

Relay Output Alarm

The switch provides relay output contacts for signaling of a user-defined power or port failure. The relay output can be connected to an alarm signaling device. Current is 1A at 240VAC.



Normal state: 3 & 2 open, 2 & 1 closed

Alarm state: 3 & 2 closed, 2 & 1 open

Required Equipment and Software (Web Interface)

- **Computer with an Ethernet Interface (RJ-45)**

  Managing the switch requires a personal computer (PC) or notebook computer equipped with a 10/100base-TX Ethernet interface and a physical RJ-45 connection. The preferred operating system for the computer is Microsoft Windows 7/8/8.1/10. It is possible to use Apple OSX or Linux systems as well, but, for the sake of brevity, all web configurations in this manual will be shown using Windows 7 as the underlying operating system.

- **Cat 5+ Ethernet Cables**

  An Ethernet cable of at least Category 5 rating is required to connect your computer to the switch. The cable can be configured as “straight-through” or crossover.

- **TFTP Server Software**

Trivial file transfer protocol (TFTP) server software is needed to update the switch firmware and to upload/download configuration files to the switch. Users not performing these tasks do not need TFTP software installed. Several good TFTP servers are available for free online. The server that will be used in this manual is TFTPD32 by Philippe Jounin.

- **Web Browser Software**

  The end user can employ any of the following web browsers during switch configuration: Internet Explorer, Firefox, or Chrome. Internet Explorer is the preferred browser for EtherWAN switch configuration. If there is trouble with other browsers while attempting to program the switch, Internet Explorer should be used.

COMPUTER SETUP

The 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).

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 EtherWAN Managed 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.

- **HTTPS** (Hypertext Transfer Protocol) HTTP with encryption.
- **RS-232** – The EtherWAN Managed Switch is equipped with a RS-232 serial port that can be used to access the switch CLI. The Serial port is DC-E DB-9F. 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. (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

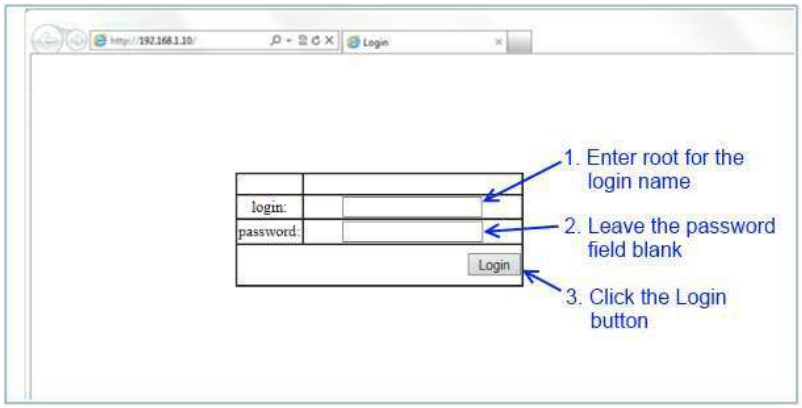


Figure 1: Login screen

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 108).

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)

Note: You will need to log in to the switch again after changing the IP address.

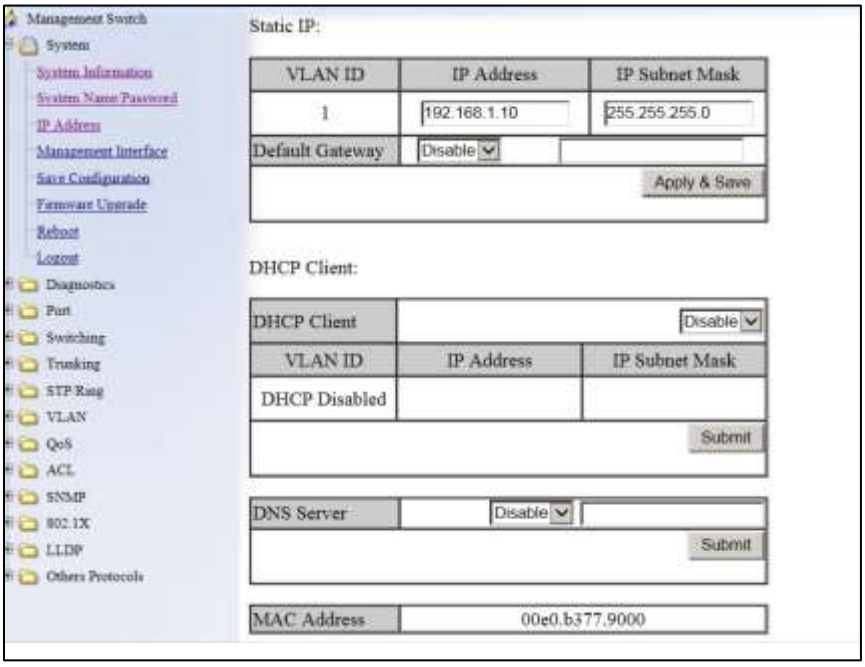


Figure 2: Assigning an IP address

CLI COMMAND USAGE

This chapter describes accessing the EtherWAN Managed 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 DB-9F to DB-9M 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)# interface fe1
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

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**
    - This displays the primary firmware version and date of last update
- **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

- **Alternate Firmware**
    - This shows the backup firmware version mirrored on the switch. If the switch becomes unbootable from the primary firmware image, it will boot to this version on the next boot.
- **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)

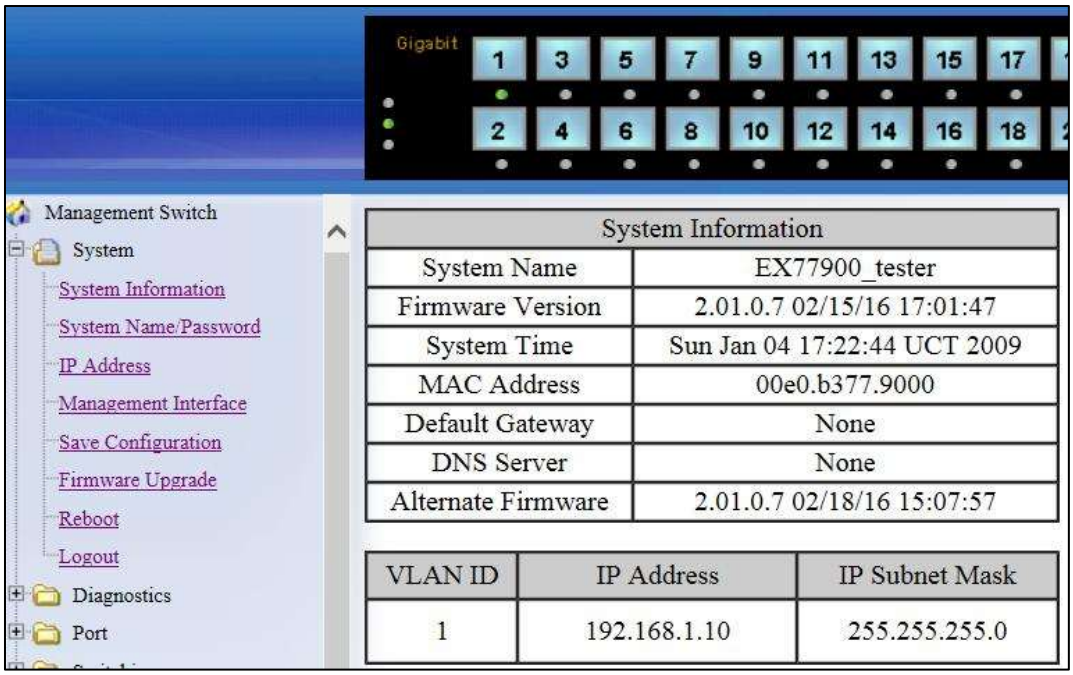


Figure 3: System Information

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.

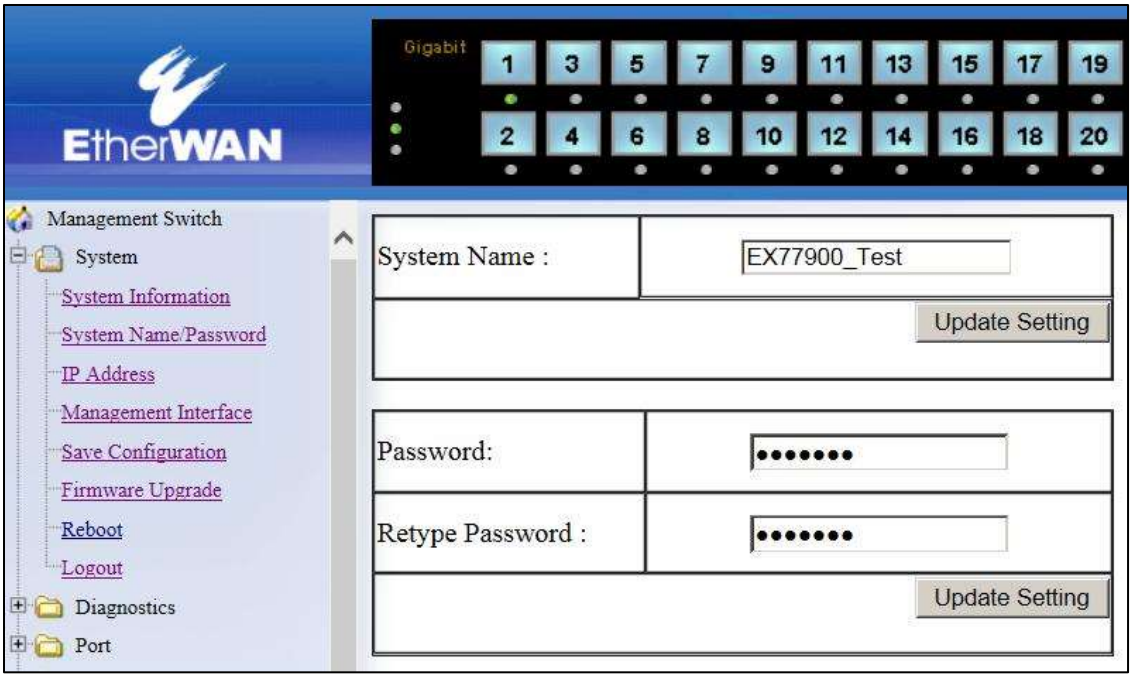


Figure 4: System Name/Password

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:

CLI Command Mode: **Global Configuration Mode**

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

Usage Example 1: Setting a Hostname to “switch_a”

```
switch_a(config)#hostname switch_a
```

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: Setting switch password to “mypassword”

```
switch_a(config)#enable password mypassword
```

In Case of Lost/Forgotten Password

1. If the switch cannot be accessed because the password is not known, then the switch must be reset. This must be done by connecting to the switch through the RS-232 serial port.
2. Connect to the switch’s RS-232 port with a terminal emulator.
3. Power cycle the switch (turn the power off and then on).
4. While the switch is rebooting, hold down **Ctrl + C**. This will cause the switch to enter CFE (Common Firmware Environment) mode. The prompt should look like this:

   ```
   CFE_1.5>
   ```

5. Enter the command **reset_default**. This will reset the switch to its factory default settings.

NOTE: Restoring the switch to factory defaults will reset all data and settings.

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 a particular 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)

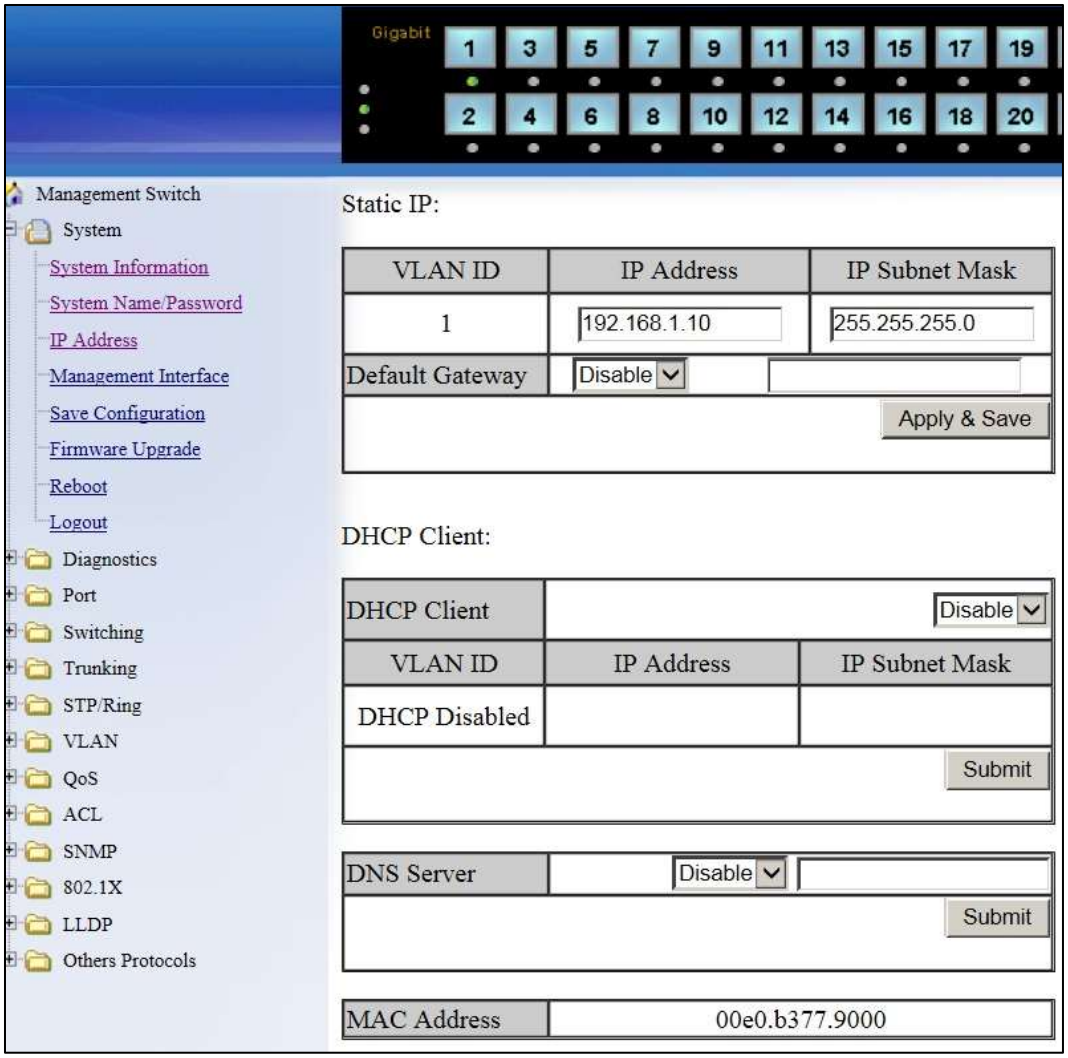


Figure 5: IP Address

IP Address - Configuration using the CLI

IP Address

To set the IP address, use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

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 of 192.168.1.1 with subnet mask of 255.255.255.0

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

Usage Example 2: Removing an IP address

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

Default Gateway

To set the Default Gateway, use the following CLI commands:

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 default gateway to 192.168.1.254

```
switch_a(config)#ip default-gateway 192.168.1.254
switch_a(config)#q
switch_a#write memory
Building configuration.....
[OK]
```

Usage Example 2: Removing the Gateway

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

Domain Name Server (DNS)

To set the DNS, use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

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

Usage Example: Set Domain name server to 192.168.1.253

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

Usage Example 2: Remove a DNS IP Address

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

Enable/Disable DHCP Client on a VLAN

To enable the DHCP client on a VLAN, use the following CLI commands:

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(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]
```

Enable/Disable Static IP on a VLAN

To set the IP address, use the following CLI commands:

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 of 192.168.1.11 with subnet mask 255.255.255.0 on VLAN2:

```
switch_a(config)#interface vlan1.2
switch_a(config-if)#ip address 192.168.1.11/24
switch_a(config-if)#q
switch_a(config)#q
switch_a#write memory
Building configuration.....
[OK]
```

Usage Example 2 – Disable Static IP on VLAN2:

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

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 EtherWAN Managed Switch.

HTTPS

HTTPS (Hypertext Transfer Protocol Secure) allows the user to determine what method, if any, is used to configure the EtherWAN Managed Switch. The default is unencrypted HTTP (see Figure 6).

To disable the Web interface:

1. Uncheck **Http** and **Https.**
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 EtherWAN Managed Switch will restore the Web Console. To save the configuration, connect using the new IP address.

To enable the Web Interface:

1. Check **HTTP**, **HTTPS** or both
2. Click on the **Update Setting** button.
3. Save the Configuration (see Save Configuration)

Telnet

Telnet is a network protocol that allows a remote computer to log into the EtherWAN Managed Switch to access its CLI (Command Line Interface). The CLI can be access using Telnet, SSH and the serial port on the EtherWAN Managed 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 6 below)
2. Click on the **Update Setting** button
3. Save the Configuration (see Save Configuration)

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 EtherWAN Managed Switch. SSH is disabled by default on the V1.94.2 EtherWAN Managed Switch.

To enable or disable SSH:

1. Click the **Enable** or **Disable** radio button in the SSH section on the Management Interface page (see Figure 6)

2. Click on the **Update Setting** button
3. Save the Configuration (see Save Configuration)

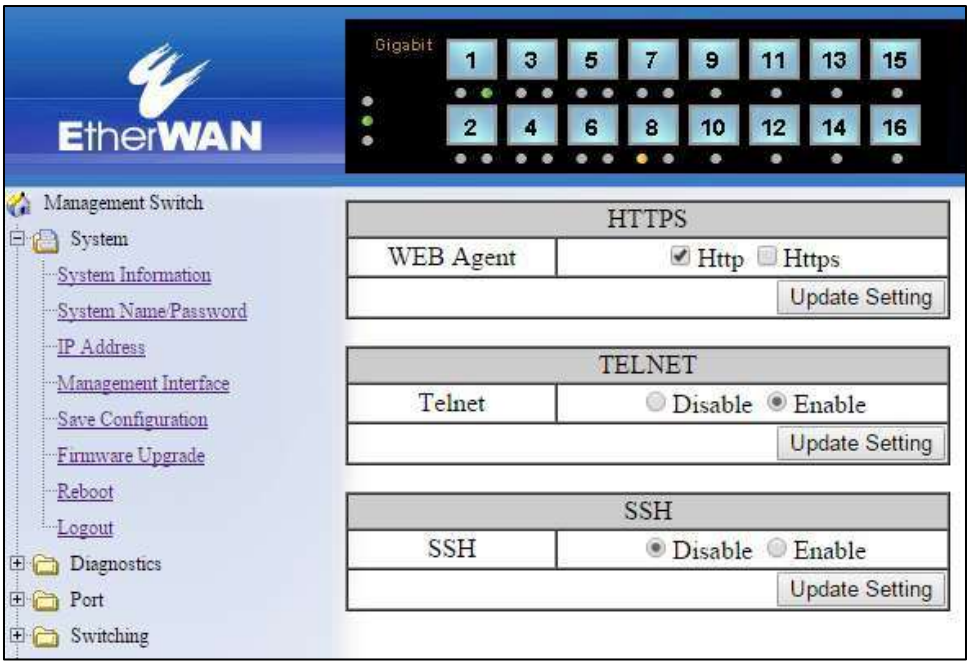


Figure 6: Management Interface

Management Interface Configuration using the CLI

Enabling/Disabling Telnet

To enable or disable telnet, use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
ip telnet
no ip telnet

Usage Example: Enabling Telnet:

```
switch_a(config)#ip telnet
```

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

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

To enable or disable SSH, use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
ip ssh
no ip ssh

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

To enable or disable HTTP or HTTPS, use the following CLI commands:

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

Save Configuration Page

To 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 functions (see Figure 7):

Save Configuration

To save the currently running configuration to the flash memory on the EtherWAN Managed Switch:

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

Load Configuration

This function is used to load a previously saved configuration. Backing up and loading a configuration is usually achieved using a TFTP server.

To load a configuration:

1. Enter the IP address of your TFTP server in the **TFTP Server** text box
2. Enter the name of the configuration file in the **FILE** text box
3. Click on the **Backup** button
4. If the file is successfully loaded the following message will be shown:
   `Success! System reboot is required!`

Backup Configuration

This function is used to back up the current switch configuration. Backing up the configuration is usually achieved using a TFTP server such as TFTPD32.

To back up a configuration:

1. Enter the IP address of your TFTP server in the **TFTP Server** text box
2. Enter the name of the configuration file in the **FILE** text box
3. Click on the **Backup** button
4. If the backup is successful the following message will be shown:
   `tftp <filename> to ip <ip address> success!!`

Restore Default

To restore the switch to factory defaults:

1. Click on the **Restore Default** button.
2. The switch will ask for confirmation, then reboot.

NOTE: Restoring the switch to factory defaults will reset all data, including user accounts and passwords.

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 TFTP server it may need to be temporarily disabled.

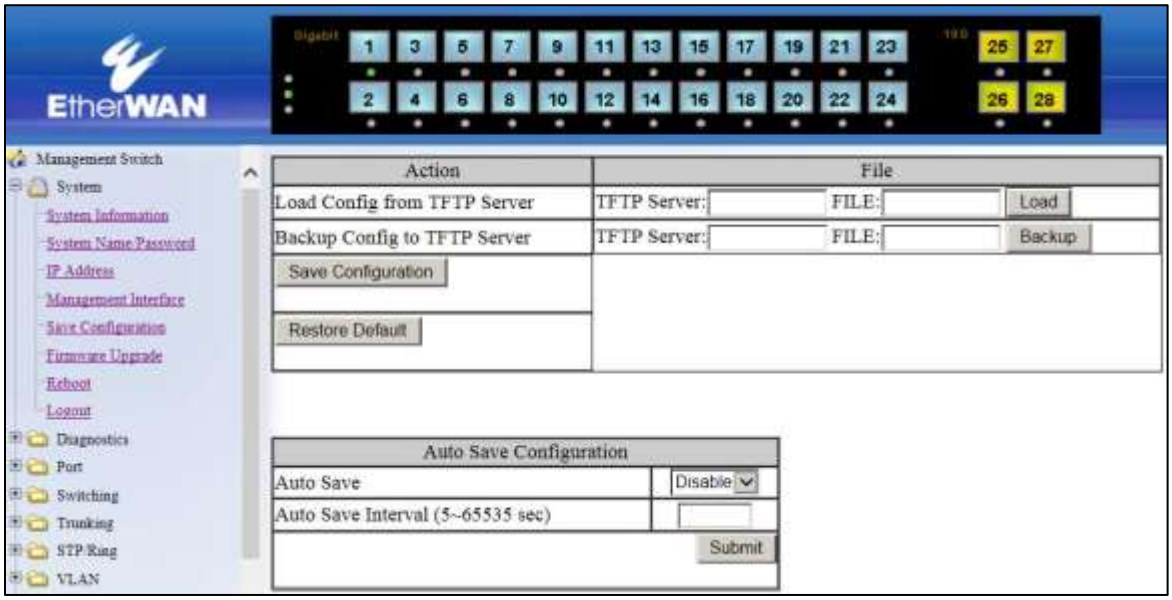


Figure 7: Save Configuration Page

Save Configuration Page using the CLI

Saving a Configuration

To save a running configuration, use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
write memory

Usage Example: Saving a Configuration

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

Restore Default Settings

To restore the switch to its default settings, use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
restore default

Usage Example: Restoring a Configuration

```
switch_a#restore default
```

Load Configuration from a TFTP Server

To Load a Configuration from a TFTP server, use the following CLI commands:

CLI Command Mode: **Privileged Exec Mode**

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

Usage Example: Loading a Configuration from TFTP server on 192.168.1.100, where configuration file is file_name.tgz

```
switch_a#install config-file 192.168.1.100 file_name.tgz
```

Save Configuration to a TFTP Server

To Save a Configuration to a TFTP server, use the following CLI commands:

CLI Command Mode: **Privileged Exec Mode**

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

Usage Example: Saving a Configuration to TFTP server on 192.168.1.100, where configuration file is named flash.tgz

```
switch_a#write config-file 192.168.1.100 flash.tgz
```

Auto Save Configuration

To set the Auto Save Configuration, use the following CLI commands:

CLI Command Mode: **Configure Mode**

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

Usage Example 1: Enabling Auto Save with interval of 10 seconds

```
switch_a(config)#service auto-config enable
switch_a(config)#service auto-config interval 10
```

Usage Example 2: Disabling Auto Save

```
switch_a(config)#no service auto-config enable
```

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, a TFTP server is required. The firmware file for the switch 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 EtherWAN Managed Switch (see Figure 8):

1. Copy the firmware file to the correct directory for your TFTP server. The correct directory depends on your TFTP server settings
2. Enter the filename of the firmware in the **Filename** text box.
3. Enter the IP Address of your TFTP server in the **TFTP 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 TFTP server it may need to be temporarily disabled.

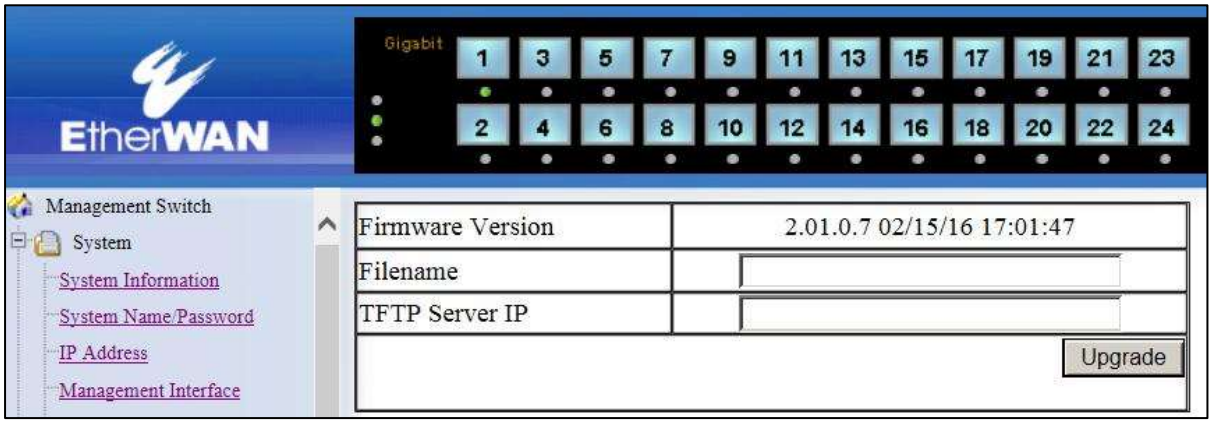


Figure 8: Firmware Upgrade Page

Firmware Update using the CLI

To display the current primary and alternate firmware versions:

CLI Command Mode: **Privileged Exec Mode**

CLI Command Syntax:
show firmware

To update firmware from a TFTP server:

CLI Command Mode: **Privileged Exec Mode**

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

Usage Example: Loading new firmware from TFTP server on 192.168.1.100, where filename is file_name.tgz

```
switch_a#install image 192.168.1.100 flash.tgz
```

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.

Reboot

To navigate to the **Reboot** page:

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

To reboot the EtherWAN Managed 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

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: **Exec mode or Privileged Exec Mode**

CLI Command Syntax:
logout

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 9):

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

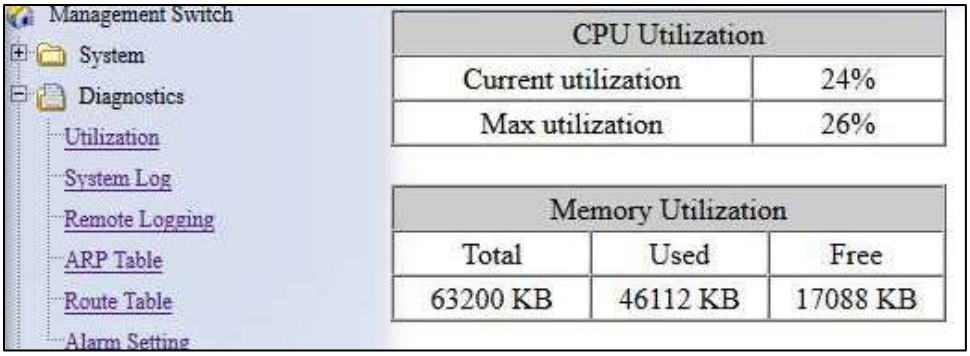


Figure 9: Utilization Page

System Log

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

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

The System Log shows the data and time of port links going up or down (see Figure 10)

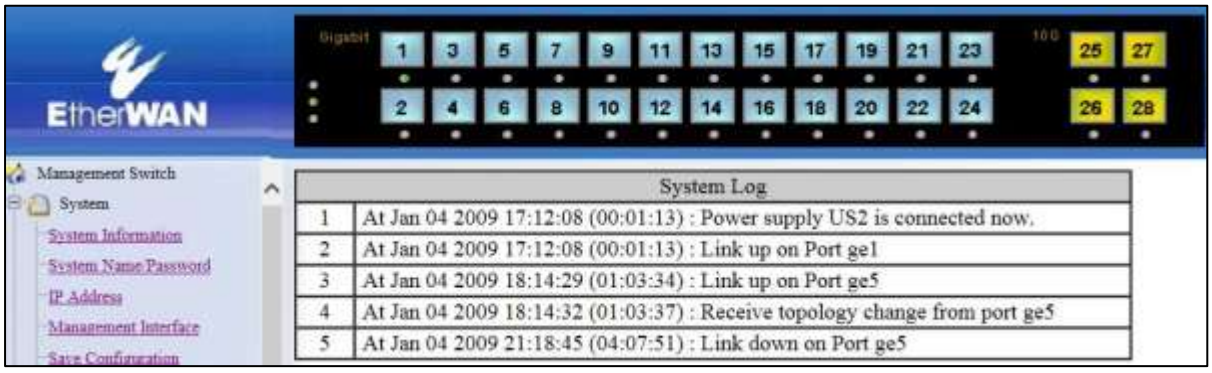


Figure 10: System Log

System log using CLI command

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

CLI Command Syntax:
show system-log

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 11).

To configure the Remote Logging on the EtherWAN Managed Switch:

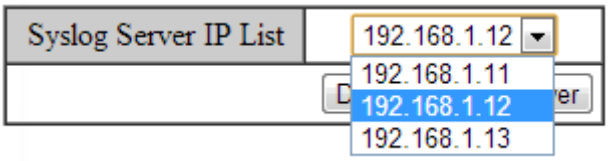
1. Click on the **Enable** or **Disable** radio button under Remote Logging.
2. Click on the **Update Setting** button.

To add a Syslog server:

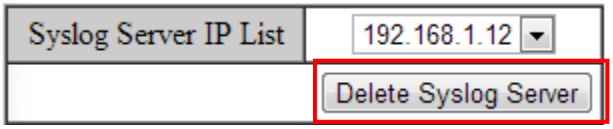
1. Enter the IP Address of the Syslog Server in the **Syslog Server IP** text box.
2. Click on the **Add Syslog Server** button.

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



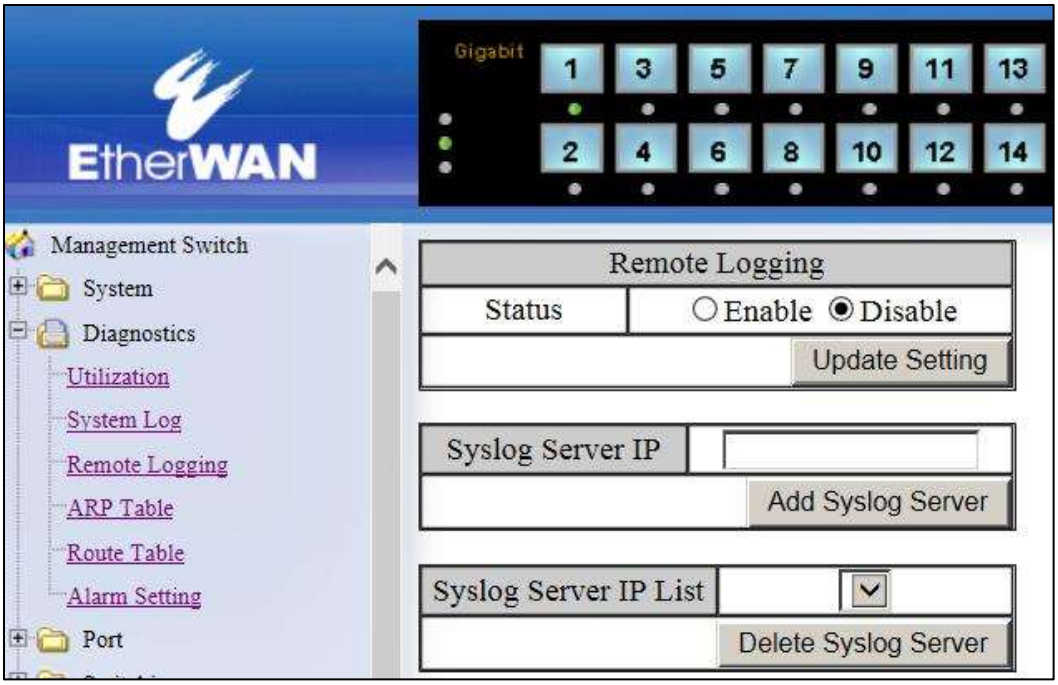


Figure 11: Remote Logging Page

Remote Logging using CLI commands

Enable/Disable Remote Logging

CLI Command Mode: **Global Config Mode**

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

Usage Example 1: Enable Remote Logging

```
switch_a(config)#remote-log enable
```

Add/Delete a Remote Logging Host

CLI Command Mode: **Global Config Mode**

CLI Command Syntax:
remote-log add *<ip_address>*
remote-log del *<ip_address>*
remote-log del all

Usage Example 1: Add a Remote Logging Host at 192.168.1.100

```
switch_a(config)#remote-log add 192.168.1.100
```

Usage Example 2: Delete a Remote Logging Host at 192.168.1.100

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

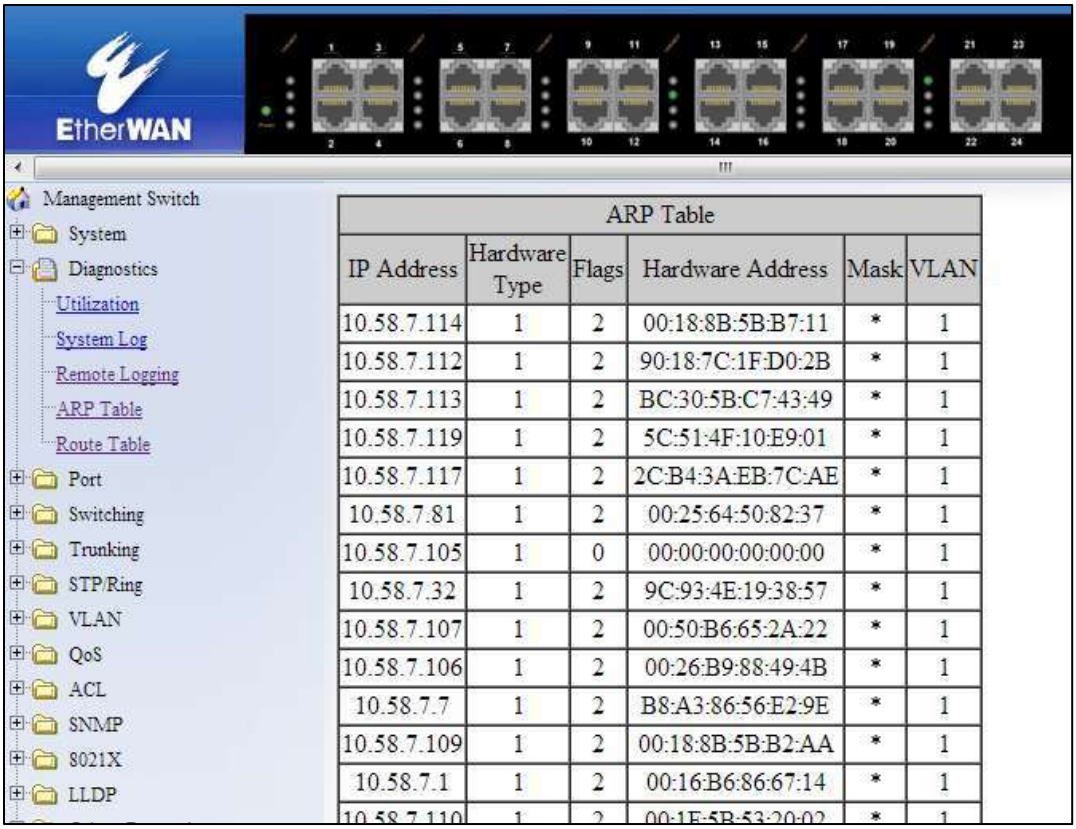
ARP Table

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 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
10.58.7.114	1	2	00:18:8B:5B:B7:11	*	1
10.58.7.112	1	2	90:18:7C:1F:D0:2B	*	1
10.58.7.113	1	2	BC:30:5B:C7:43:49	*	1
10.58.7.119	1	2	5C:51:4F:10:E9:01	*	1
10.58.7.117	1	2	2C:B4:3A:EB:7C:AE	*	1
10.58.7.81	1	2	00:25:64:50:82:37	*	1
10.58.7.105	1	0	00:00:00:00:00:00	*	1
10.58.7.32	1	2	9C:93:4E:19:38:57	*	1
10.58.7.107	1	2	00:50:B6:65:2A:22	*	1
10.58.7.106	1	2	00:26:B9:88:49:4B	*	1
10.58.7.7	1	2	B8:A3:86:56:E2:9E	*	1
10.58.7.109	1	2	00:18:8B:5B:B2:AA	*	1
10.58.7.1	1	2	00:16:B6:86:67:14	*	1
10.58.7.110	1	2	00:1F:5B:53:20:02	*	1

Figure 12: ARP Table

ARP Table using CLI Commands

CLI Command Mode: **Global Configuration Mode**

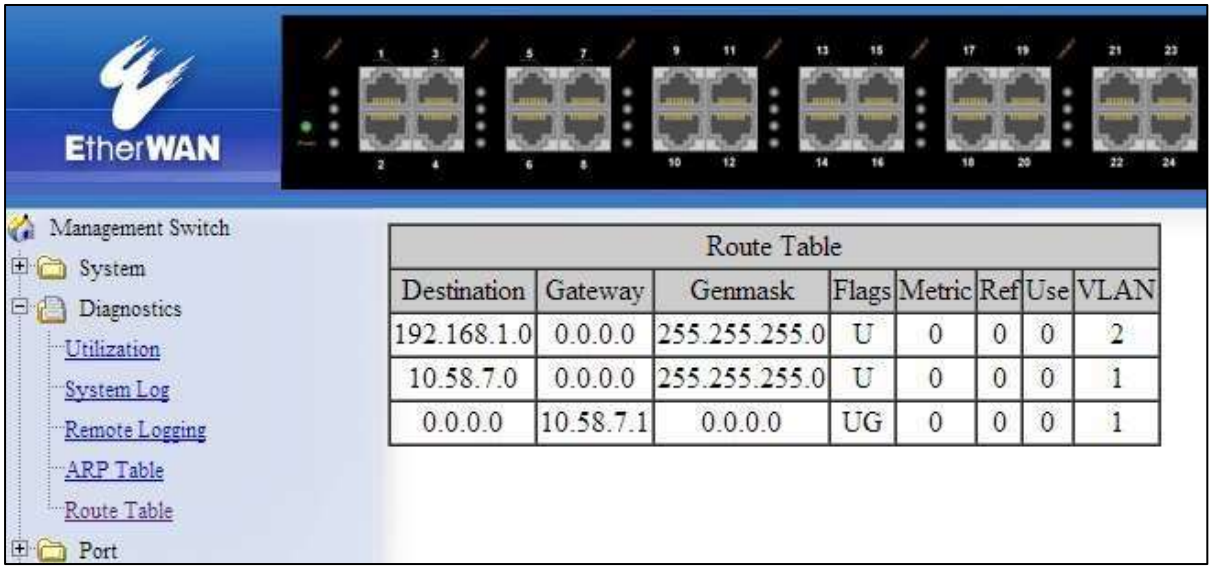
CLI Command Syntax:
show arp-table

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	2
10.58.7.0	0.0.0.0	255.255.255.0	U	0	0	0	1
0.0.0.0	10.58.7.1	0.0.0.0	UG	0	0	0	1

Figure 13: Route Table

Route Table Using CLI Commands

CLI Command Mode: **Privileged Exec Mode**

CLI Command Syntax:
show route-table

Usage Example:

```
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
```

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 14).

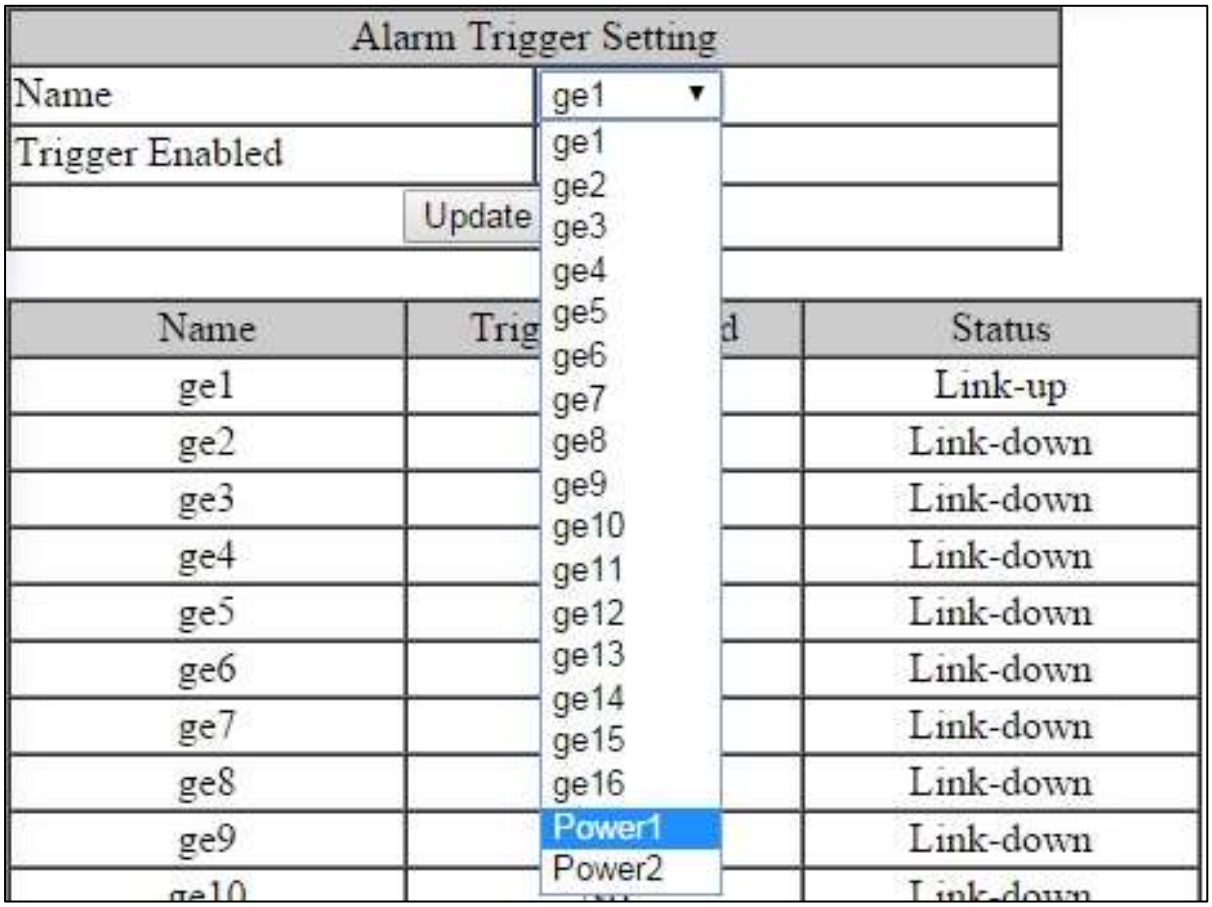


Figure 14: Alarm Trigger

3. Select **YES** or **NO** from the dropdown box next to Trigger Enabled (see Figure 15).
4. Click **Update Setting** to save any changes made.

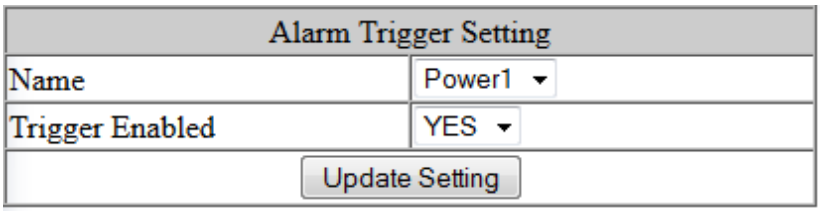


Figure 15: Trigger Enable

Dying Gasp

The dying gasp function allows the switch to send a message to a syslog or SNMP server if power to the switch is lost.

To set the notifications for Dying Gasp:

1. Select the Primary and Secondary notifications, either SNMP Trap or Syslog.
2. Click the **Update Setting** button.

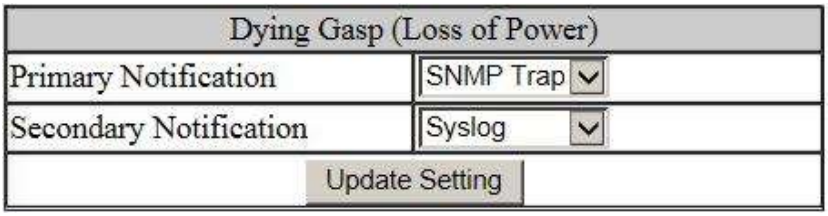


Figure 16: Dying Gasp

Dying Grasp Using CLI Commands

Show current primary and secondary Dying Gasp settings

CLI Command Mode: **Privileged Exec Mode**

CLI Command Syntax:
show dying-gasp status

Set primary and secondary Dying Gasp messages

CLI Command Mode: **Global Config Mode**

CLI Command Syntax:
dying-gasp primary <*delivery_method*> **secondary** <*delivery_method*>

PORT

Configuration

To navigate to the **Configuration** page:

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

Port configuration contains features as flow control, port speed, and duplex settings. These settings can be very useful when the switch is connected to a latency-critical device such as a VOIP phone, IP camera, or video multiplexor. The ability to alter 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 17):

- **Port Number** – fe(n) for 100mb ports and ge(n) for Gigabit ports
- **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 EtherWAN Managed 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 EtherWAN Managed 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.

To set the Port Speed and/or Port Duplex Settings on the EtherWAN Managed 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. For example, 100Mb fiber ports will typically be limited to a single option of 100M/FD (100Mbps and Full Duplex) while running 1Gb UTP ports will have six options for speed/duplex.
2. Click on the **Submit** button.

To enable or disable a port's Flow Control settings on the EtherWAN Managed Switch:

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

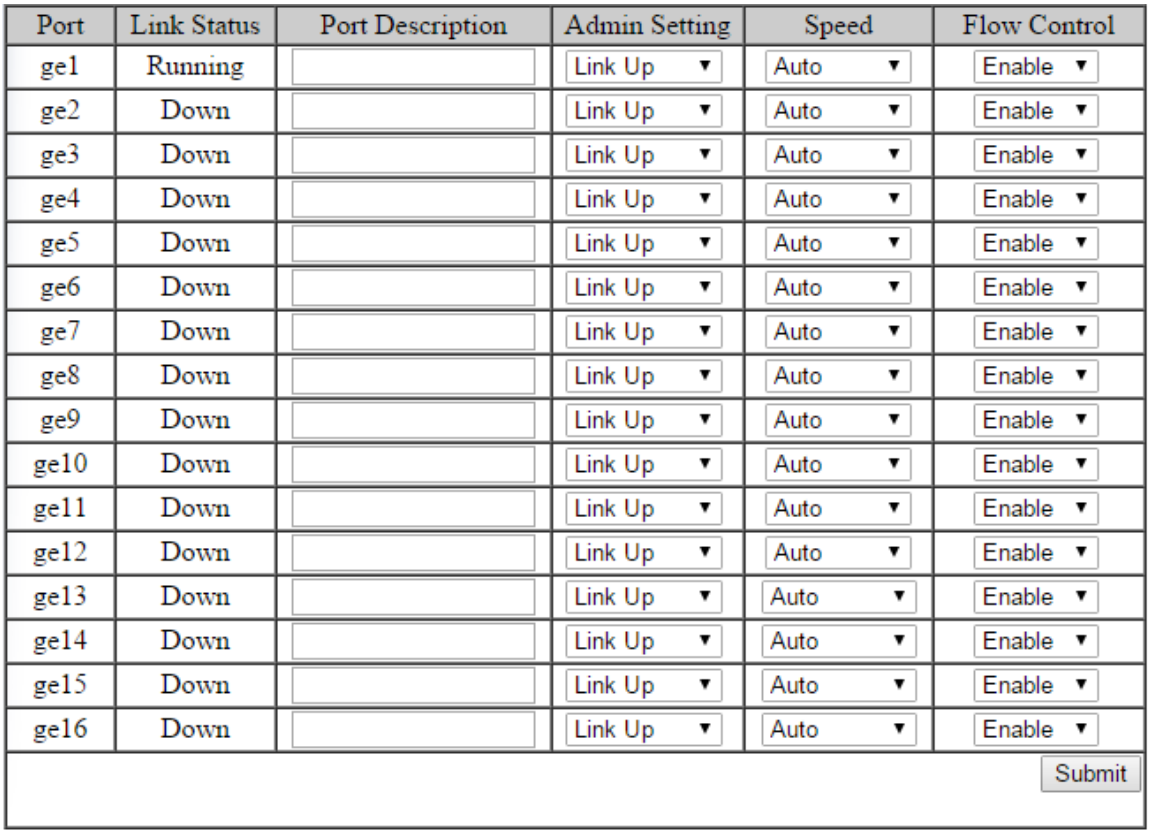


Figure 17: Port Configuration

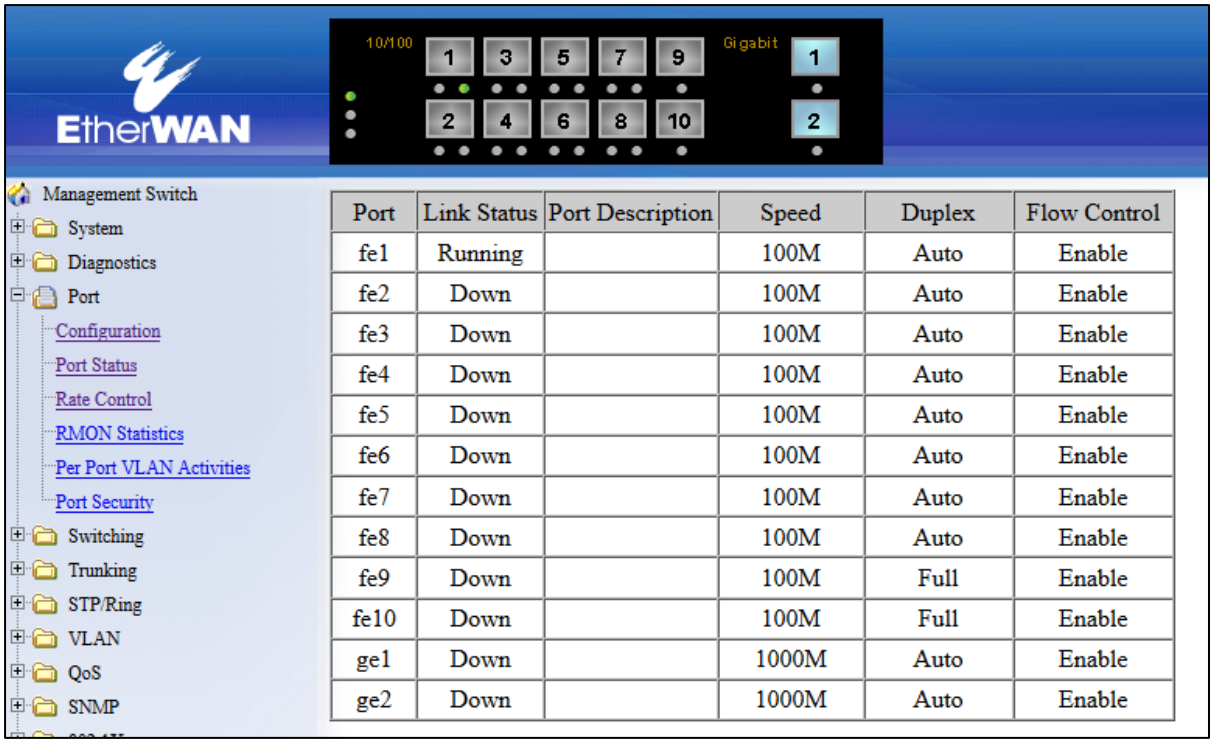
Port Status

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 18):

- **Port Number** – fe(n) for 100mb ports and ge(n) for Gigabit ports
- **Link Status** – Operational State of the Port's Link.
- **Port Description** – User-supplied Port Description
- **Admin Setting** – Administratively State of the Port.
- **Speed** – Speed and Duplex Settings for Port.
- **Flow Control** – State of Flow Control for the Port.



Port	Link Status	Port Description	Speed	Duplex	Flow Control
fe1	Running		100M	Auto	Enable
fe2	Down		100M	Auto	Enable
fe3	Down		100M	Auto	Enable
fe4	Down		100M	Auto	Enable
fe5	Down		100M	Auto	Enable
fe6	Down		100M	Auto	Enable
fe7	Down		100M	Auto	Enable
fe8	Down		100M	Auto	Enable
fe9	Down		100M	Full	Enable
fe10	Down		100M	Full	Enable
ge1	Down		1000M	Auto	Enable
ge2	Down		1000M	Auto	Enable

Figure 18: 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 19):

To provide either an ingress or egress rate control for a port on the EtherWAN Managed 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 19: 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 20).

To view the RMON statistics for a particular port on the EtherWAN Managed Switch:

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

To clear the RMON statistics for a particular port on the EtherWAN Managed 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 particular 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.

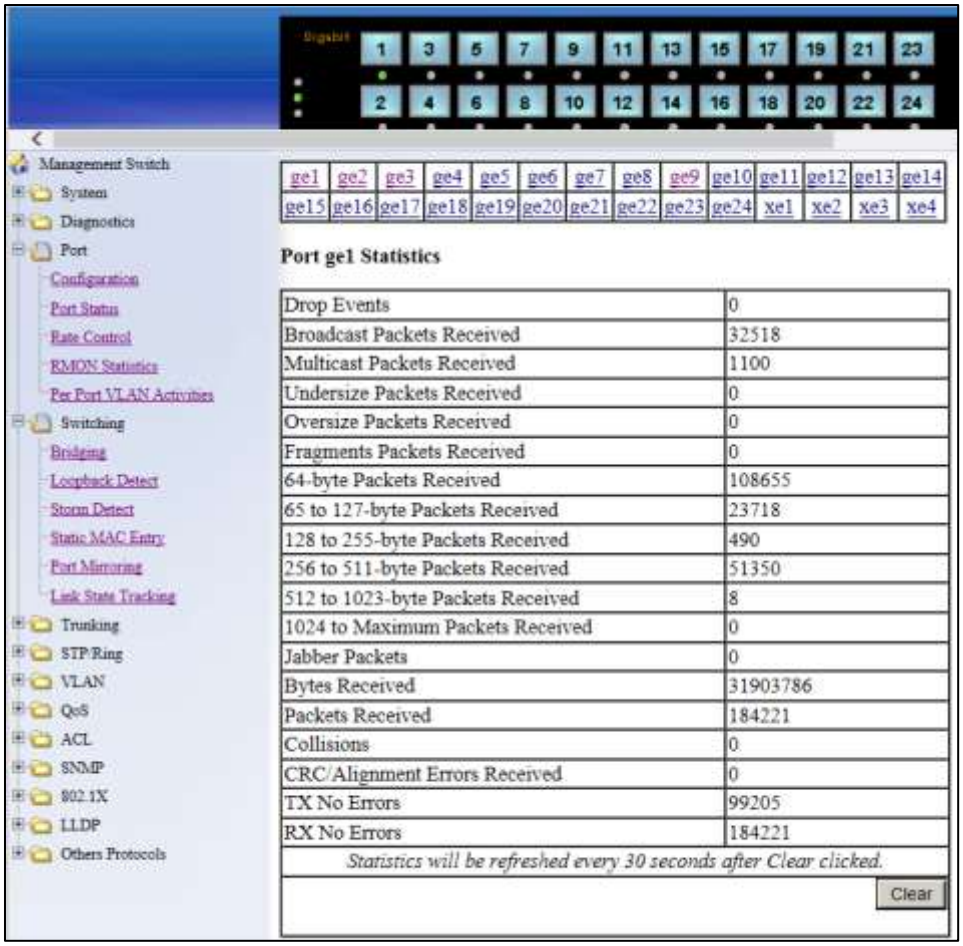


Figure 20: RMON Page

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 particular port and the vlan associated with that device and port.

To clear the MAC addresses for a particular port on the EtherWAN Managed Switch (see Figure 21):

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.

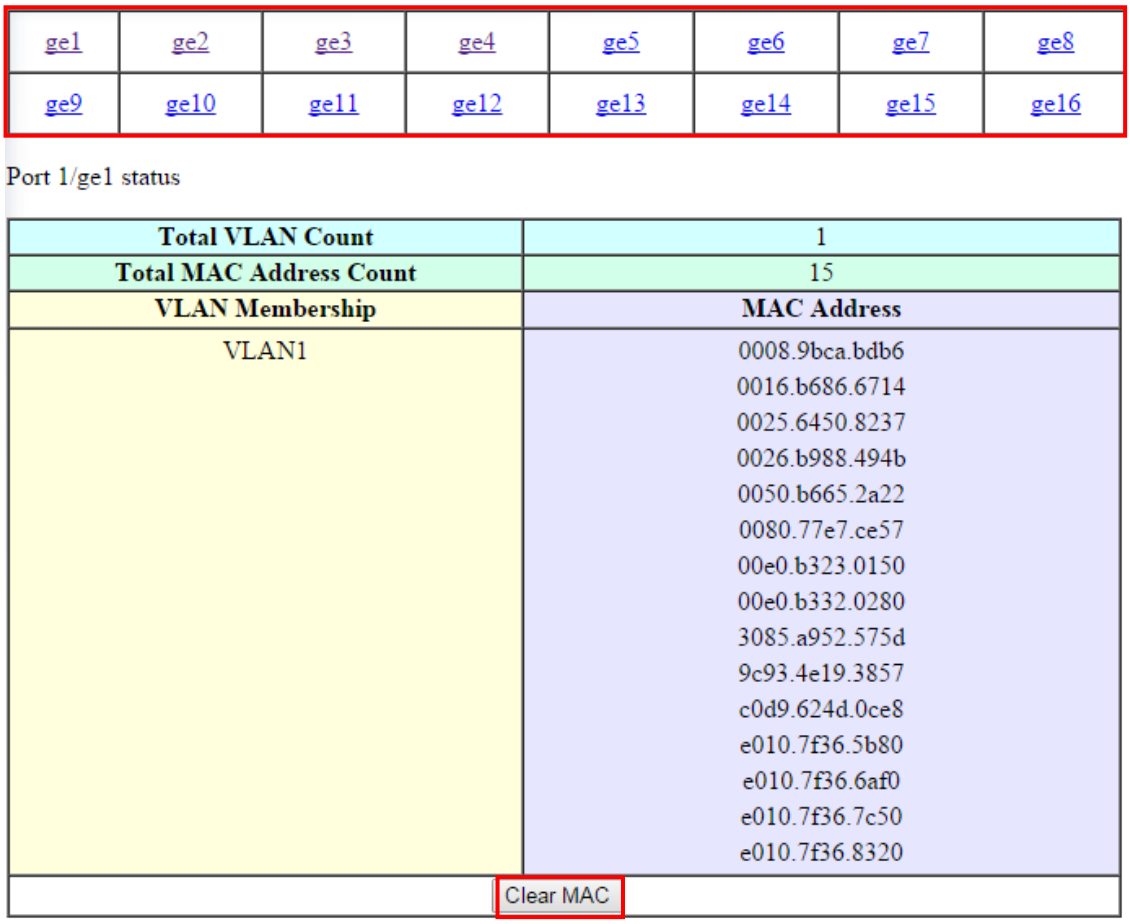


Figure 21: Port VLAN Activities

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(config-if)#description A_Port_Description
```

Enable or Disable a Port

To administratively enable or disable a port use the CLI commands below:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax:
shutdown
no shutdown

Setting the Port Speed

To set the port speed for a port use the CLI commands below:

CLI Command Mode: **Interface Configuration Mode**

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

Usage Example:

```
switch_a(config-if)#bandwidth 100m
```

Setting Port Duplex

To set the duplex for a port use the CLI commands below:

CLI Command Mode: **Interface Configuration Mode**

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

Usage Example:

```
switch_a(config-if)#duplex full
```

Enable or Disable Port Flow Control

To enable or disable flow control for a port use the CLI commands below:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **flowcontrol on**

Usage Example:

```
switch_a(config-if)#flowcontrol on
```

Display Port Status

To display the port status for a port use the CLI commands below:

CLI Command Mode: **Privileged Exec Mode**

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

Usage Example:

```
switch_a#show interface fe1
```

Setting a Ports Rate Control

To set a ports rate control use the CLI commands below:

CLI Command Mode: **Interface Configuration Mode**

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

Usage Example:

```
switch_a(config-if)#rate-control ingress value 100000
```

Display a Ports RMON Statistics

To display a ports RMON statistics use the CLI commands below:

CLI Command Mode: **Privileged Exec Mode**

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

Usage Example:

```
switch_a#show interface statistics fe1
```

Display a Ports 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#show bridge interface fe1
```

SWITCHING

Bridging

To navigate to the **Bridging** page:

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

Ageing Time

The Ageing 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 300 seconds (5 minutes) (see Figure 22).

To update the Ageing Time value:

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 **DFL-Multicast** for the port that needs to be changed
2. Click on the **Update Setting** button.

Figure 22: Bridging

Loopback Detect

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 EtherWAN Managed Switch (see Figure 23):

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 23):

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 23):

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 23):

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.

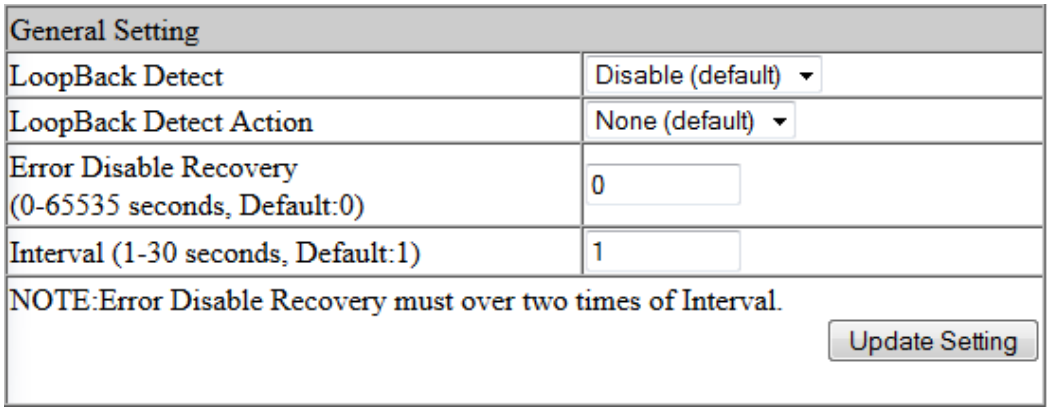


Figure 23: Loopback Detection

Loopback Detection (Per Port)

To enable **Loopback Detection** for a particular port or ports on the EtherWAN Managed Switch (see Figure 24):

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.

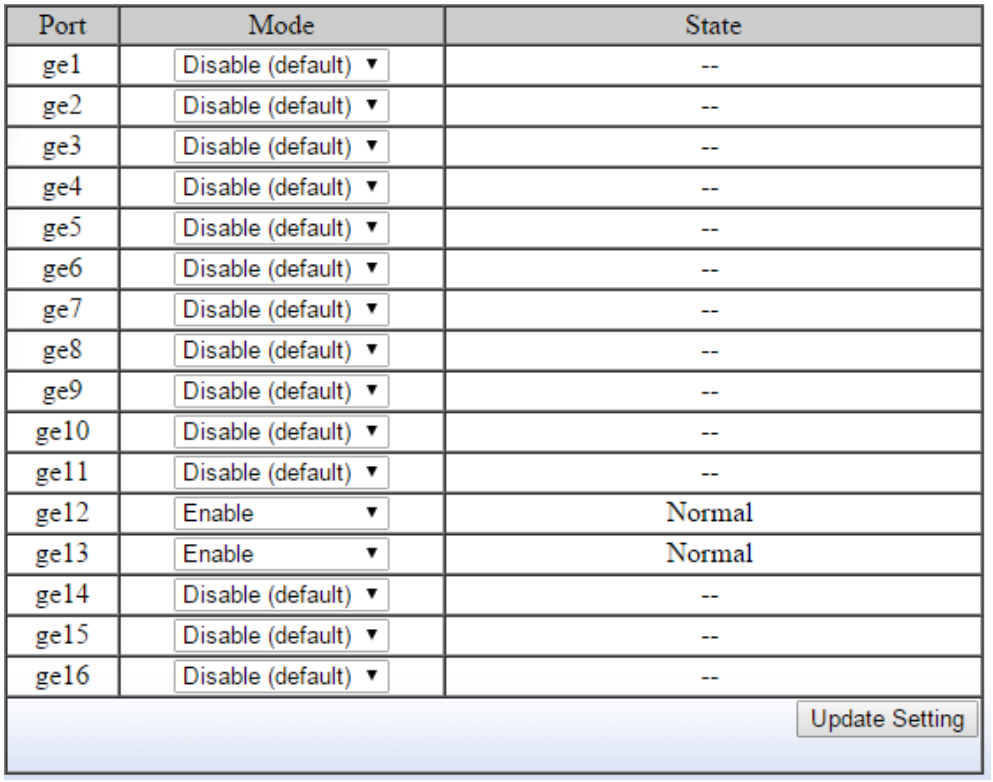


Figure 24: Loopback Detection (port)

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.

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 24).
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.

Bridge Storm-Detect Configuration	
Storm-Detect configuration	Enable
Storm-Detect interval (2..65535 sec), Default: 10	10
Storm-Detect errdisable-recovery time (0..65535 sec), 0:no recovery	0
Storm-Detect state of action	Errdisable

Figure 25: Storm Detect — Global

4. Set the **By Utilization**(%) for each port in the **Storm-Detect Per Port Configuration** box (see Figure 25). 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 Drop-down 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.

Storm-Detect Per Port Configuration				
Port	State / Recovery time remains	By Utilization(%) (0-100) 0: not limited	By Broadcast / Multicast+Broadcast Packets Per Second (0-100000) 0: not limited	
ge1	Normal / NA	50	MC-BC	50
ge2	No Detecting	0	BC	0
ge3	No Detecting	0	BC	0
ge4	No Detecting	0	BC	0
ge5	No Detecting	0	BC	0
ge6	No Detecting	0	BC	0
ge7	No Detecting	0	BC	0
ge8	No Detecting	0	BC	0
ge9	No Detecting	0	BC	0
ge10	No Detecting	0	BC	0
ge11	No Detecting	0	BC	0
ge12	No Detecting	0	BC	0
ge13	No Detecting	0	BC	0
ge14	No Detecting	0	BC	0
ge15	No Detecting	0	BC	0

Figure 26: Storm Detect — Per Port

Static MAC Entry

Occasionally, it may be useful to specify a MAC address on a particular 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 particular port (see Figure 27):

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.

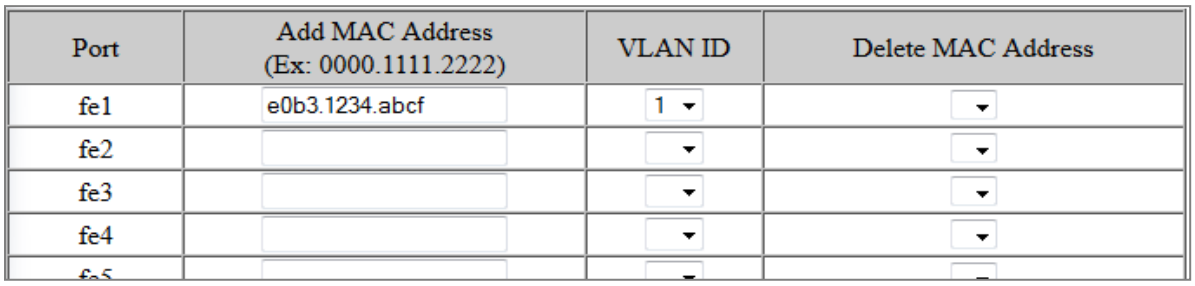


Figure 27: MAC Static Entry

Removing a Static MAC Address from a Port

To remove a static MAC entry for a particular port (see Figure 28):

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

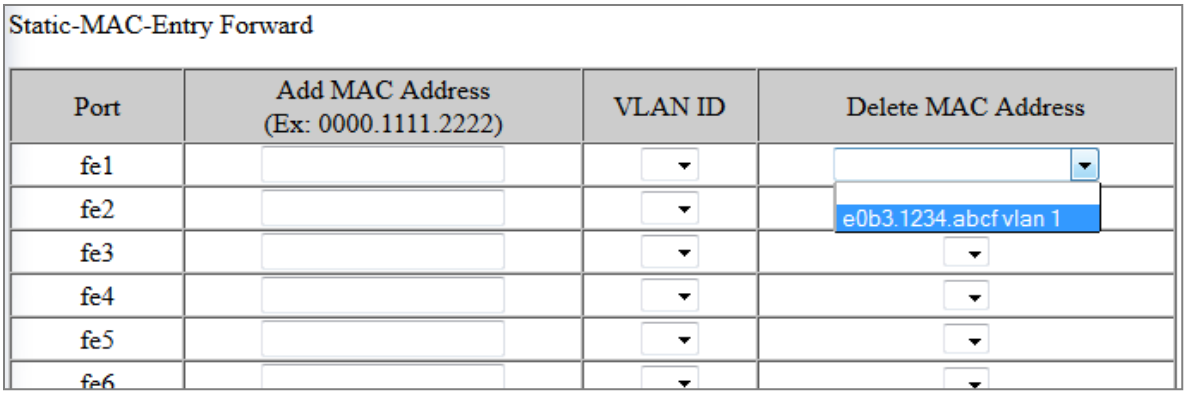


Figure 28: Removing a Static MAC Address

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

To add a MAC address to the **Static-MAC-Entry Discard** table (see Figure 29):

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.

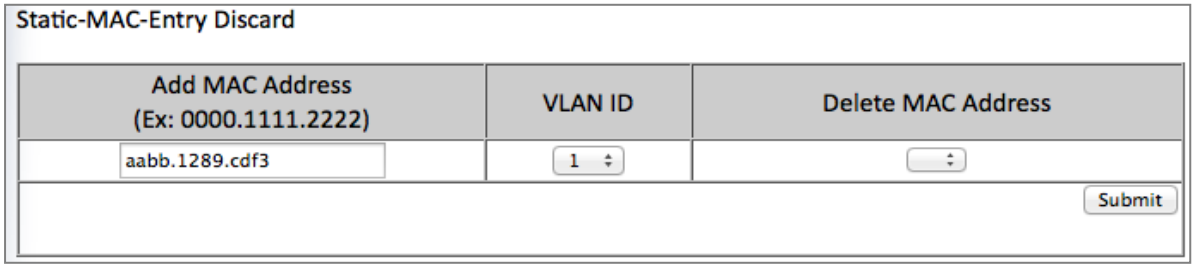


Figure 29: Adding a MAC – Static-MAC-Entry Table

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 30):

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

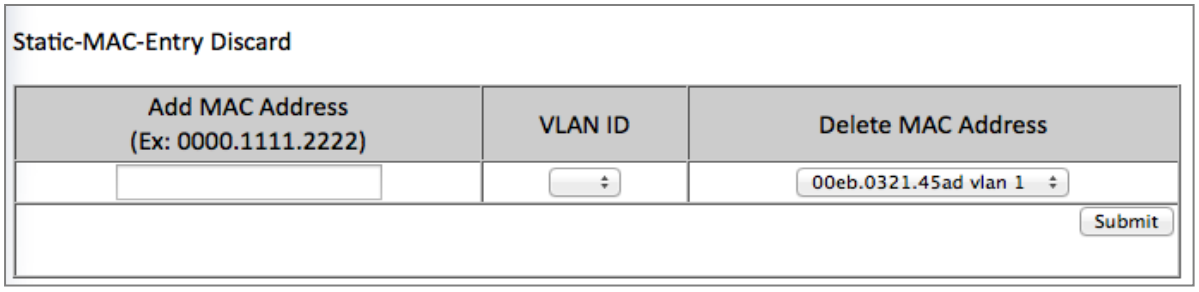


Figure 30: Deleting a MAC Address – Static-MAC-Entry Table

Port Mirroring

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 EtherWAN Managed Switch (see Figure 31):

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.

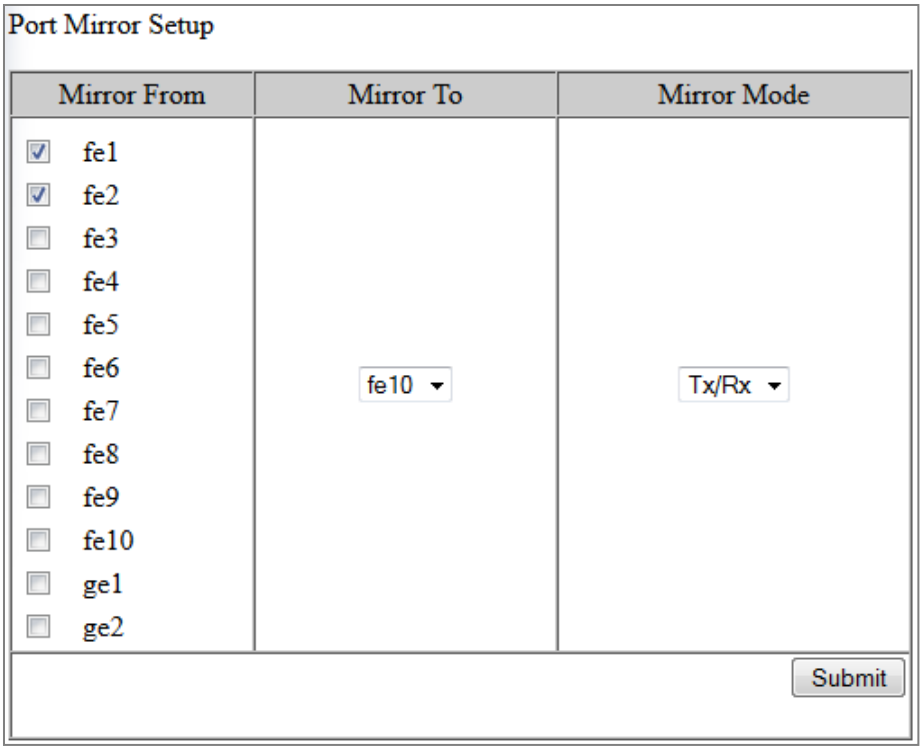


Figure 31: Port Mirroring

To disable port mirroring for a port or ports on the EtherWAN Managed Switch (see Figure 32):

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

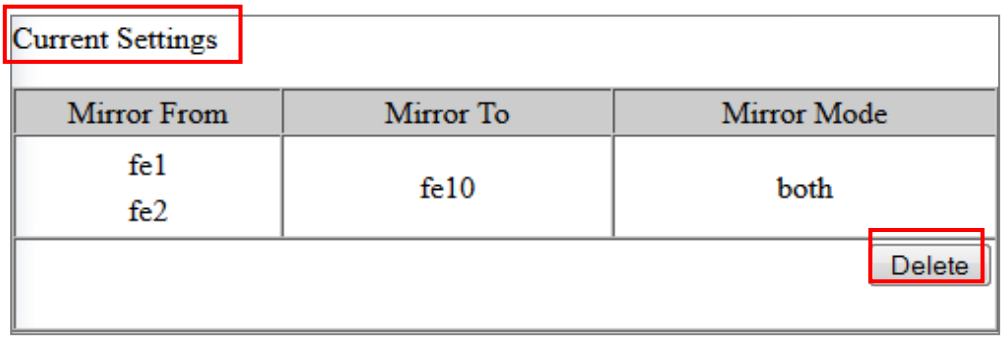


Figure 32: Disabling Port Mirroring

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 particular group on the EtherWAN Managed Switch (see Figure 33):

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.**

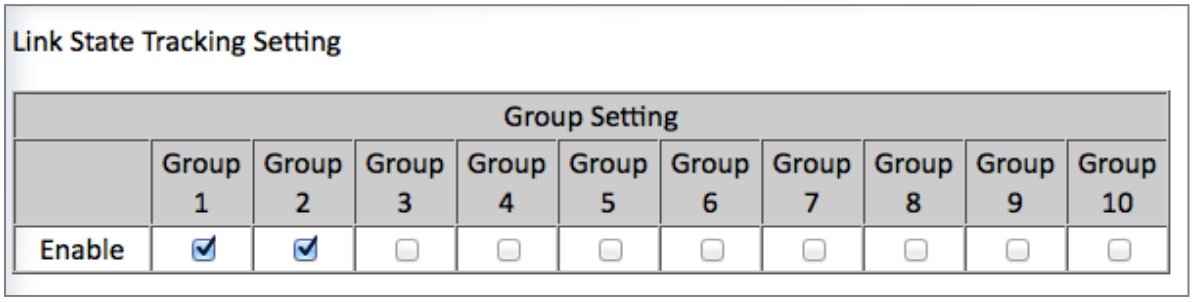


Figure 33: Link State Tracking

Port Settings

To configure individual ports for a Link State group on the EtherWAN Managed Switch (see Figure 34):

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.**

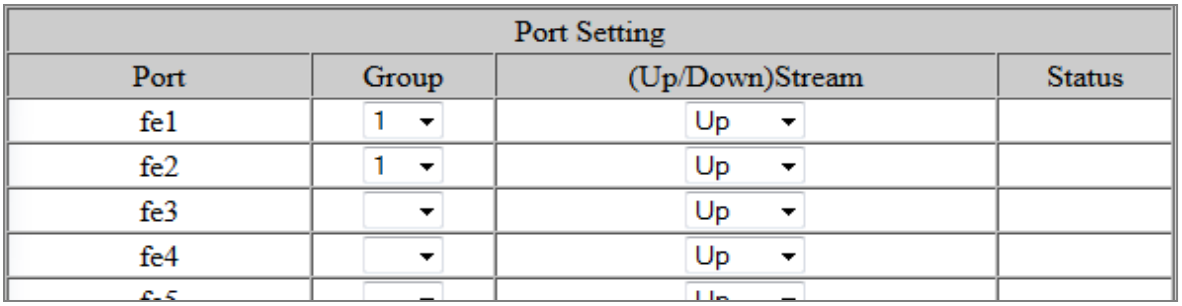


Figure 34: Link State Tracking – Port Settings

Switch Configuration Examples Using CLI Commands

Setting the Ageing Time Value

To update the **Ageing Time** value on the EtherWAN Managed Switch, use the CLI commands below:

CLI Command Mode: **Global Configuration Mode**

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

Usage Example: Set ageing time to 300ms

```
switch_a(config)#bridge 1 ageing time 300
```

Enabling Port Isolation

To enable **Port Isolation**, use the CLI commands below:

CLI Command Mode: **Interface Configuration Mode**

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

Enabling Block Multicast

To enable **Block Multicast**, use the CLI commands below:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **switchport block multicast**

Setting Storm Control

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

CLI Command Mode: **Interface Configuration Mode**

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

Usage Example:

```
switch_a(config-if)#storm-control broadcast enable
switch_a(config-if)#storm-control level 20
```

Enabling Loopback Detect (Global)

To enable **Loopback Detect** on the EtherWAN Managed Switch, use the CLI commands below:

CLI Command Mode: Global Configuration Mode

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

Usage Example:

```
switch_a(config)#bridge 1 loopback-detect enable
```

Setting the Loopback Detect Action

To set the action for **Loopback Detect** on the EtherWAN Managed Switch, use the CLI commands below:

CLI Command Mode: Global Configuration Mode

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

Usage Example:

```
switch_a(config)#bridge 1 loopback-detect action errdisable
```

Setting the Loopback Detect Recovery Time

To set the recovery time for **Loopback Detect** on the EtherWAN Managed Switch, use the CLI commands below:

CLI Command Mode: **Global Configuration Mode**

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

Usage Example:

```
switch_a(config)#bridge 1 loopback-detect errdisable-recovery 30
```

Setting the Loopback Detect Polling Interval

To set the polling interval for **Loopback Detect** on the EtherWAN Managed Switch, use the CLI commands below:

CLI Command Mode: **Global Configuration Mode**

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

Usage Example:

```
switch_a(config)#bridge 1 loopback-detect interval 5
```

Enabling Loopback Detect (Port)

To enable **Loopback Detection** on a port on the EtherWAN Managed Switch, use the CLI commands below:

CLI Command Mode: **Interface Configuration Mode**

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

Configuring Storm-Detect

To Enable or Disable Storm-Detect use the CLI command Below:

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(config)# bridge 1 storm-detect errdisable
```

Usage Example – Disabling storm detect:

```
switch_a(config)# no bridge 1 storm-detect errdisable
```

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(config)# bridge 1 storm-detect interval 10
```

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(config)# bridge 1 storm-detect errdisable-recovery 60
```

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 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(config-if)#storm-detect mc-bc pps 50000
```

Usage Example 2 – Enabling Multicast + Broadcast:

```
switch_a(config-if)#storm-detect bc pps 50000
```

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

CLI Command Mode: **Interface Mode**

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

Default: **0** (Disabled)

Usage Example:

```
switch_a(config-if)#storm-detect utilization 80
```

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

CLI Command Mode: **Interface Mode**

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

Adding a MAC Address for Static-MAC-Entry Forwarding

To add a MAC address for **Static-MAC-Entry Forwarding** for a port on the EtherWAN Managed Switch, use the CLI commands below:

CLI Command Mode: **Global Configuration Mode**

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

Usage Example:

```
switch_a(config)# bridge 1 address 00e0.abcd.1245 forward fe1 vlan 1
```

Adding a MAC Address for Static-MAC-Entry Discarding

To add a MAC address for **Static-MAC-Entry Discarding** for a port on the EtherWAN Managed Switch, use the CLI commands below:

CLI Command Mode: **Global Configuration Mode**

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

Usage Example:

```
switch_a(config)# bridge 1 address 00e0.abcd.1245 discard vlan 1
```

Configuring Port Mirroring

To configure a port for Port Mirroring on the EtherWAN Managed Switch, use the CLI commands below:

CLI Command Mode: **Interface Configuration Mode**

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

Usage Example:

```
switch_a(config-if)#mirror interface fe2 direction both
```

Enabling a Link State Tracking Group

To enable a **Link State Tracking** Group on the EtherWAN Managed Switch, use the CLI commands below:

CLI Command Mode: **Global Configuration Mode**

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

Usage Example:

```
switch_a(config)# link state track 4
```

Assigning a Port to a Link State Tracking Group

To assign a port to a Link State Tracking group on the EtherWAN Managed Switch, use the following CLI commands:

CLI Command Mode: **Interface Configuration Mode**

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

Usage Example:

```
switch_a(config-if)# link state group 4 downstream
```

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.

There are two popular types of port trunking, static and link aggregation control protocol (LACP). We will take a minute to discuss both types of trunking and why one would want to use them.

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 100Mbps Ethernet links composing a single static channel, the overall bandwidth of the static channel would be 400Mbps.

Prioritization of data through the channel is simple as well. When one of the links of the channel becomes saturated the excess data spills over into the remaining channels. For example, if one were sending a constant stream of data at 250Mbps through a static channel composed of 4 individual 100Mbps links, the first two links of the channel would be completely saturated while the half of the third channel would be utilized and none of the forth channel would be used.

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.

Port Trunking

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

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

To create a trunk consisting of 1000Mbps ports:

1. Select **Static, LACP,** or **Disable** for each trunk that is being configured.
2. Click on the corresponding checkbox for each desired port to be included in the **Trunk Group**.
3. Click on the **Submit** button.

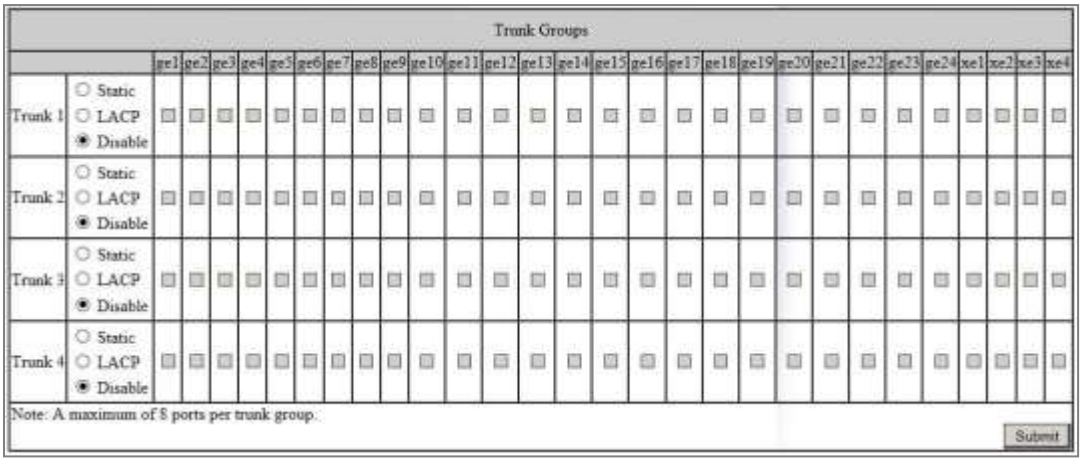


Figure 35: Port Trunking – Version 1

LACP Trunking

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

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

There are 2 versions of Port Trunking supported, depending on the model of managed switch.

To create a LACP trunk:

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. 100Mbps 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.

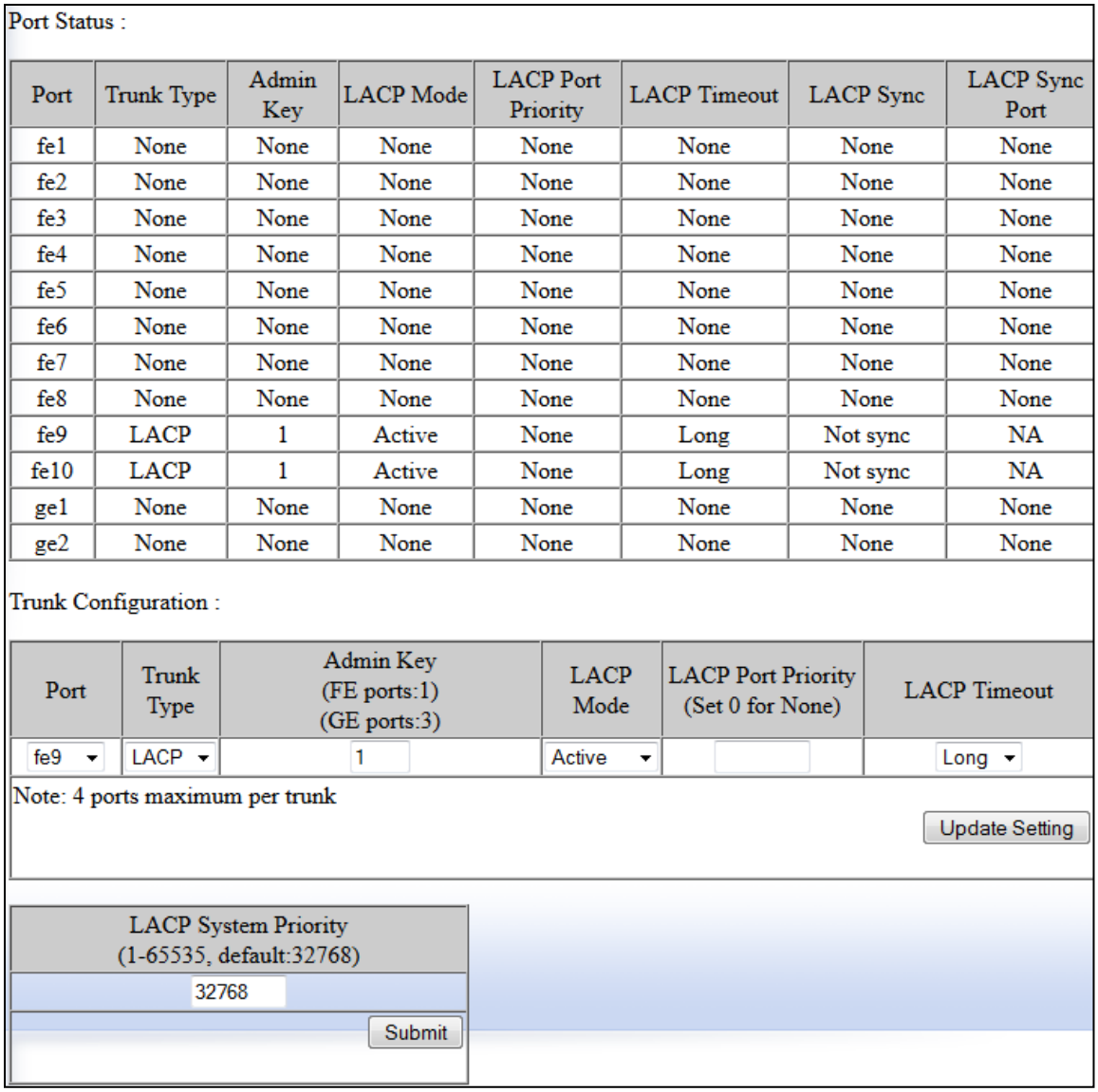


Figure 36: LACP Trunking

Trunking Configuration Examples Using CLI Commands

Adding an Interface to a Static Trunk

To add an interface to a static trunk, use the CLI commands below:

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(config-if)#static-channel-group 1
```

Adding an Interface to a LACP Trunk

To add an interface to a LACP trunk on the EtherWAN Managed Switch, use the CLI commands below:

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(config-if)#channel-group 2 mode passive
switch_a(config-if)#q
```

Setting the LACP Port Priority

To set the port priority for an interface attached to a LACP trunk on the EtherWAN Managed Switch, use the CLI commands below:

CLI Command Mode: **Interface Configuration Mode**

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

Usage Example:

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

Setting the LACP Timeout

To set the timeout for an interface attached to a LACP trunk on the EtherWAN Managed Switch, use the CLI commands below:

CLI Command Mode: **Interface Configuration Mode**

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

Usage Example:

```
switch_a(config-if)#lacp timeout long
```

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 supersede 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 37):

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.

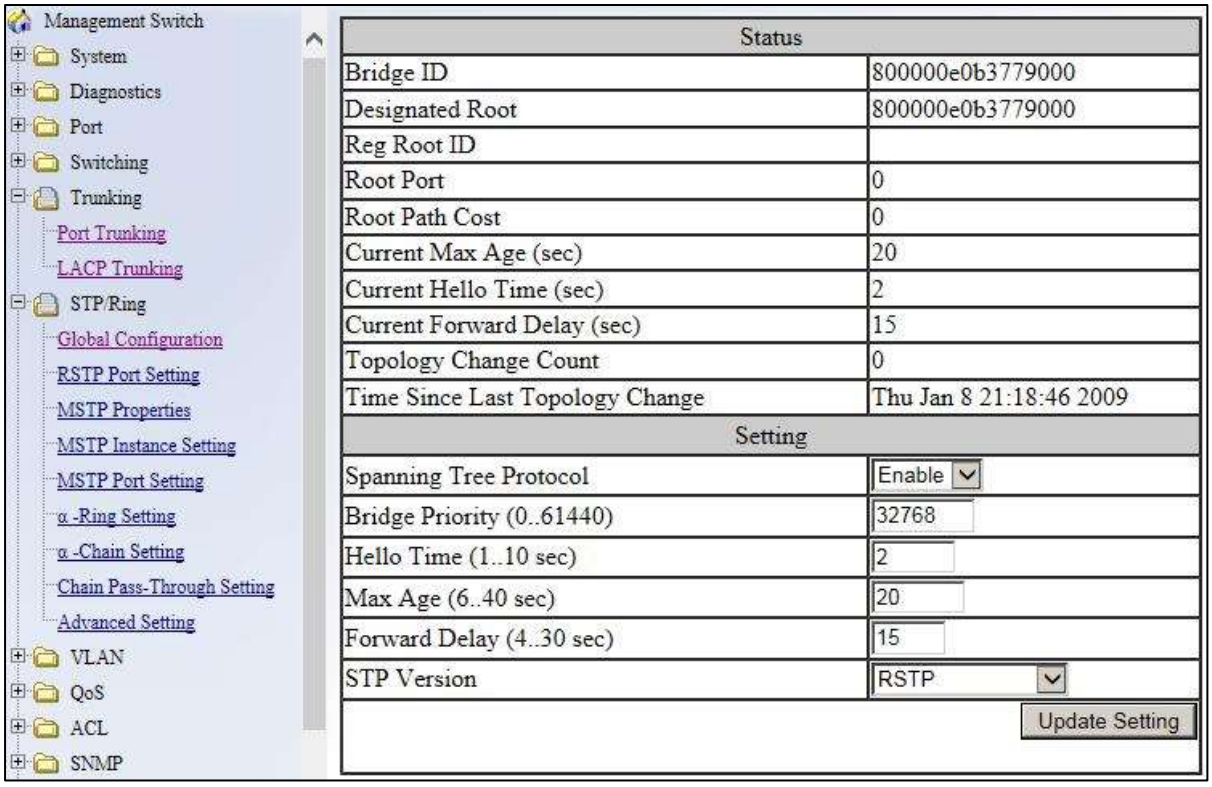


Figure 37: STP/Ring Global Configuration

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 below).

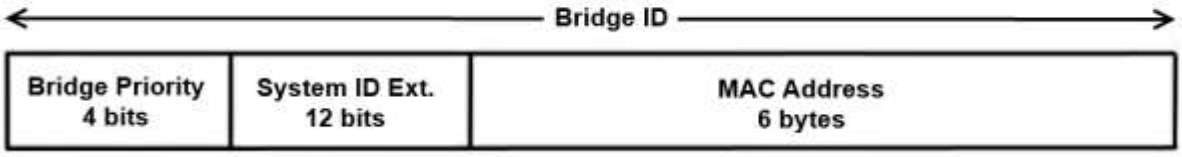


Figure 38: Bridge ID

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 39). 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.

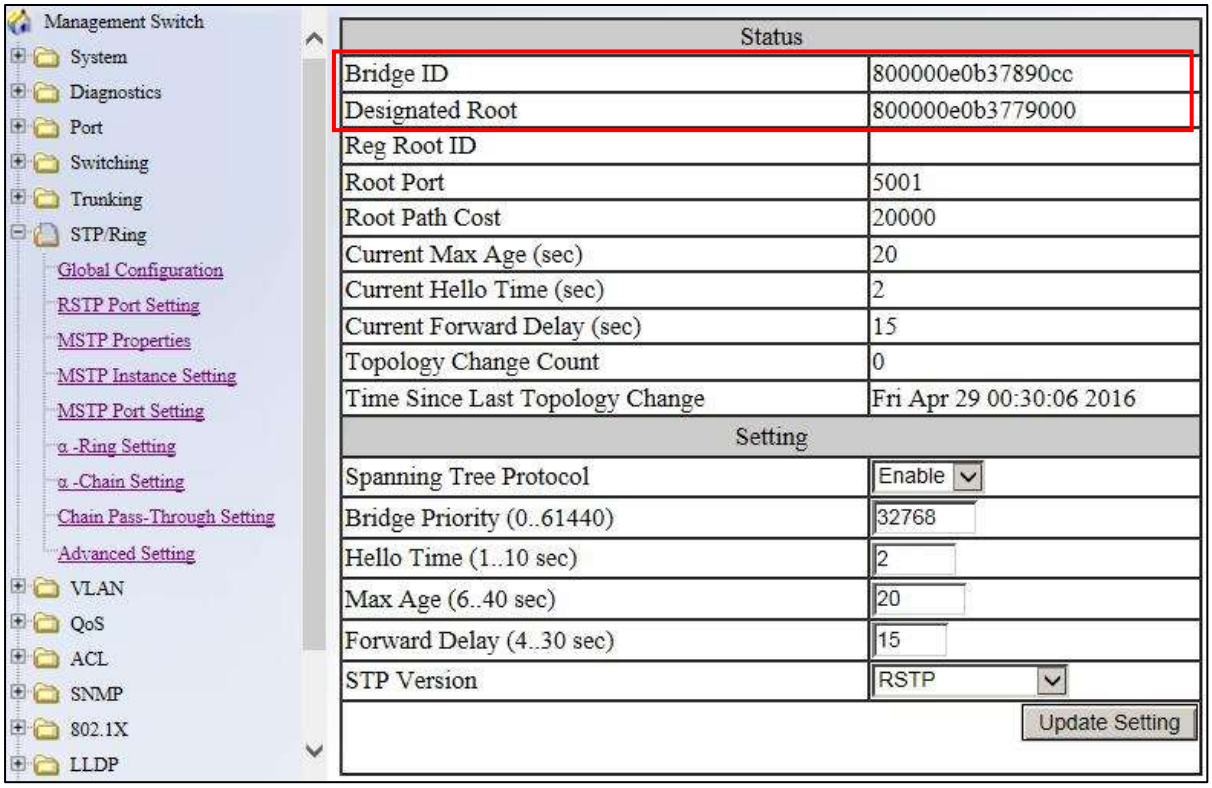


Figure 39: Bridge ID Display

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. the 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 40):

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)

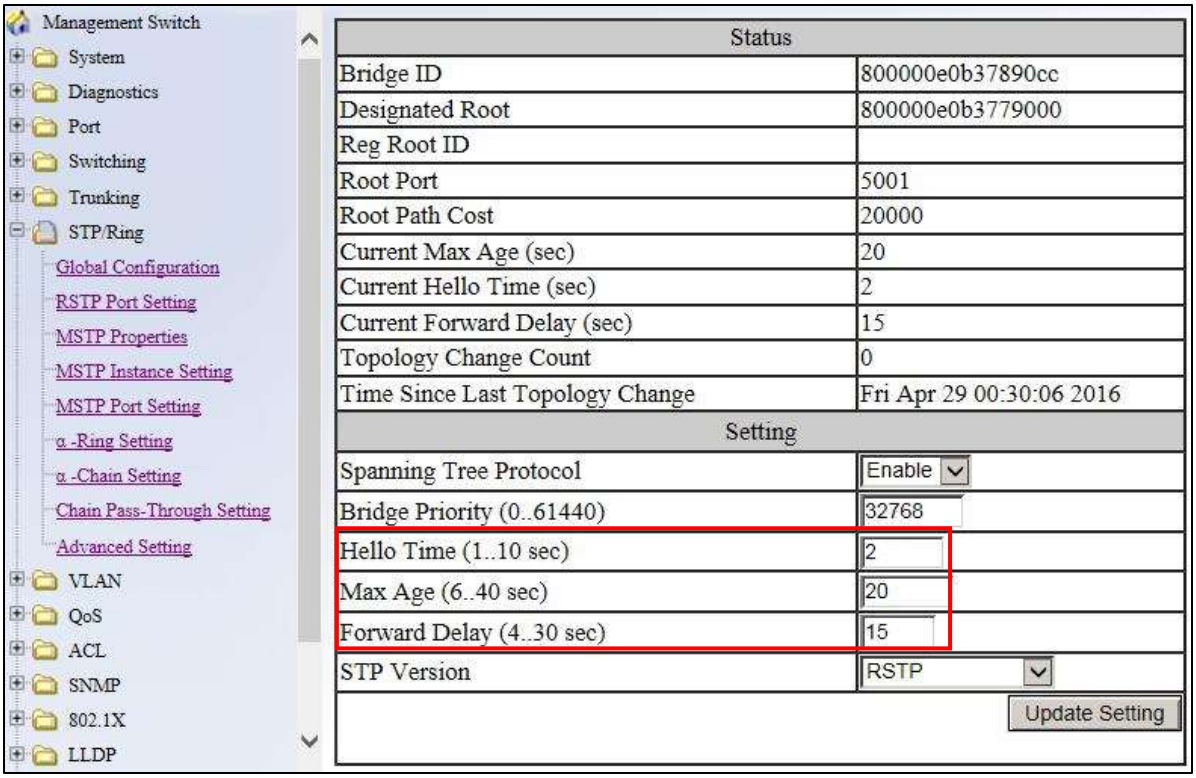


Figure 40: Max Age, Hello Timer & Forward Delay

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 41):

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

Port	Port Status	Priority	Path Cost	Point to Point Link	Edge Port
ge1	Rootport(Forwarding)	128	20000	Point to Point	Conf. Auto / Curr. Edge off
ge2	Disabled(Discarding)	128	20000000	Shared	Conf. Auto / Curr. Edge off
ge3	Disabled(Discarding)	128	20000000	Shared	Conf. Auto / Curr. Edge off
ge4	Disabled(Discarding)	128	20000000	Shared	Conf. Auto / Curr. Edge off
ge5	Disabled(Discarding)	128	20000000	Shared	Conf. Auto / Curr. Edge off
ge6	Disabled(Discarding)	128	20000000	Shared	Conf. Auto / Curr. Edge off
ge7	Disabled(Discarding)	128	20000000	Shared	Conf. Auto / Curr. Edge off
ge8	Disabled(Discarding)	128	20000000	Shared	Conf. Auto / Curr. Edge off
ge9	Disabled(Discarding)	128	20000000	Shared	Conf. Auto / Curr. Edge off
ge10	Disabled(Discarding)	128	20000000	Shared	Conf. Auto / Curr. Edge off
ge11	Disabled(Discarding)	128	20000000	Shared	Conf. Auto / Curr. Edge off
ge12	Disabled(Discarding)	128	20000000	Shared	Conf. Auto / Curr. Edge off
ge13	Disabled(Discarding)	128	20000000	Shared	Conf. Auto / Curr. Edge off
ge14	Disabled(Discarding)	128	20000000	Shared	Conf. Auto / Curr. Edge off
ge15	Disabled(Discarding)	128	20000000	Shared	Conf. Auto / Curr. Edge off
ge16	Disabled(Discarding)	128	20000000	Shared	Conf. Auto / Curr. Edge off

Figure 41: 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 below)

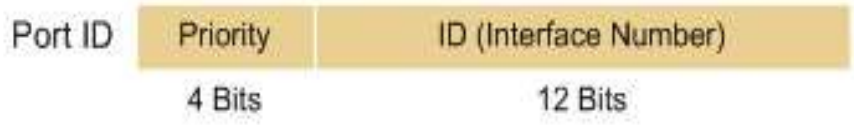


Figure 42: Port ID

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 below)
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** text entry box.
    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).

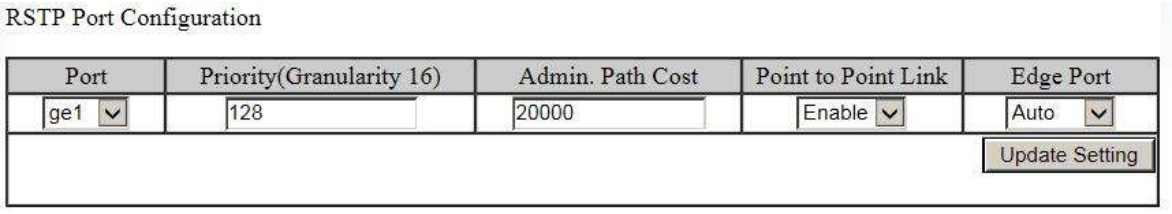


Figure 43: Port Priority and Path Cost

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 43).
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 43).
2. Click on the **Update Setting** button.
3. Save the configuration (see the Save Configuration Page)

RSTP Configuration Examples Using CLI Commands

Enabling the Spanning Tree Protocol

To enable the Spanning Tree function on a switch, use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

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

Usage Example:

```
switch_a(config)#no bridge shutdown 1
switch_a(config)#bridge 1 protocol rstp vlan-bridge
```

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, please 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(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
```

Modifying the Port Priority and Path Cost

To modify the Port Priority and Path Cost on a switch, use the below CLI commands:

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(config-if)#bridge-group 1 path-cost 200000
switch_a(config-if)#bridge-group 1 priority 128
```

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

To manually force a port to be a **shared** link or **Point-to-point** link, use the below CLI commands:

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(config-if)#spanning-tree link-type point-to-point
```

Usage Example 2: Setting port 1 to be shared:

```
switch_a(config-if)#spanning-tree link-type shared
```

Enabling/Disabling a port to be an Edge Port

To manually enable or disable a port to be an **Edge Port**, use the following CLI commands:

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(config-if)#spanning-tree edgeport
```

Usage Example 2: Disabling edge port on port 1:

```
switch_a(config-if)#no spanning-tree edgeport
```

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 44), 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).

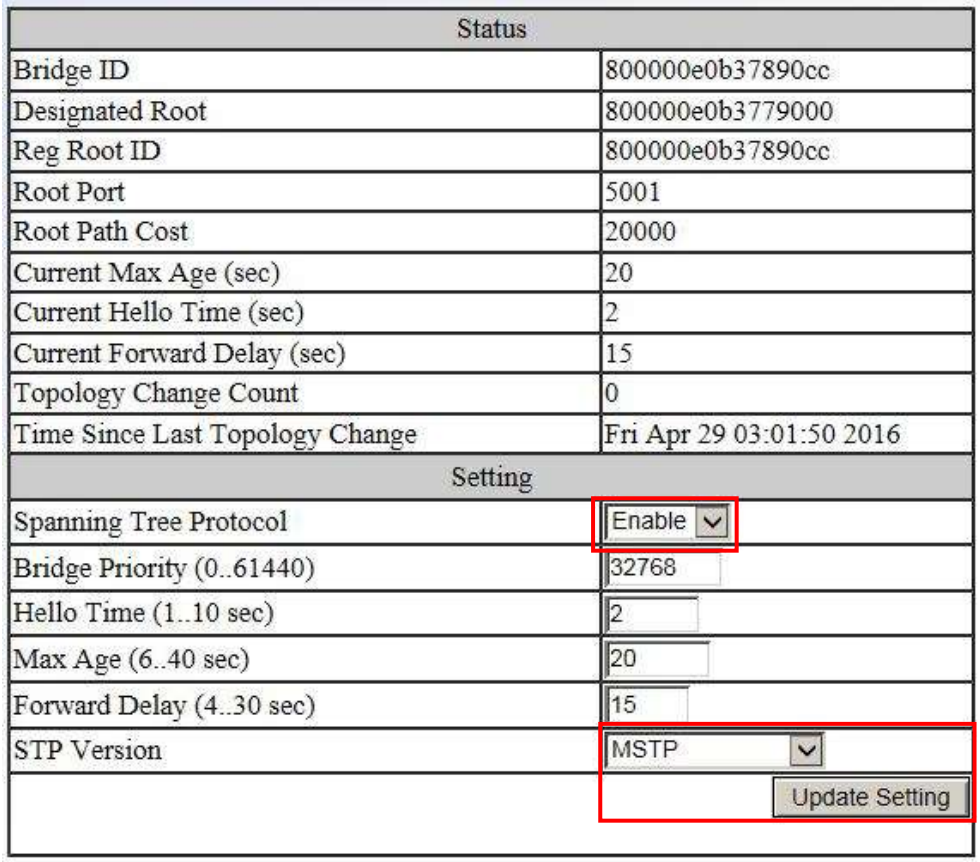


Figure 44: Enabling MSTP on STP/Ring Global Configuration Page

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 below).

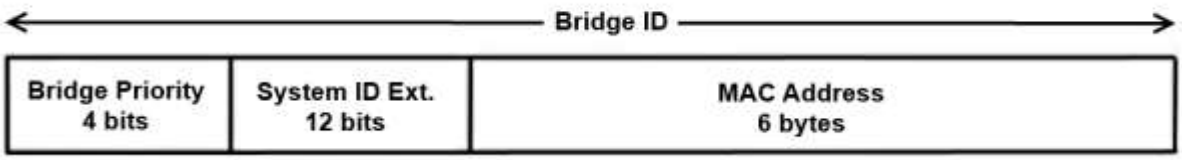


Figure 45: Bridge ID

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 46). 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.

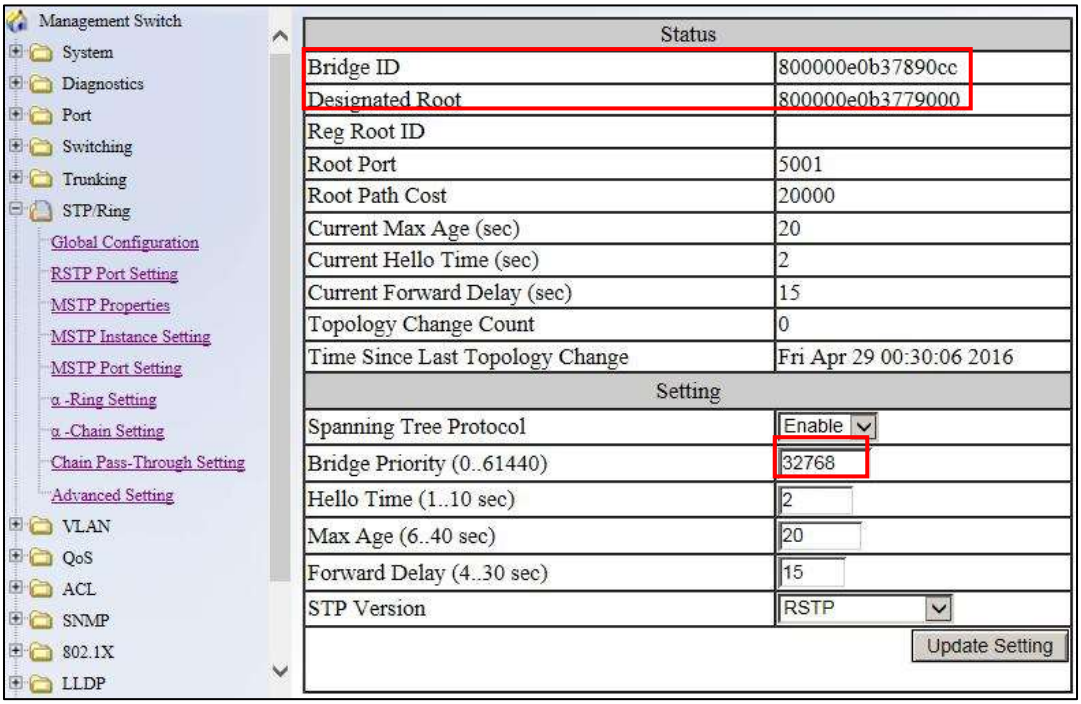


Figure 46: Bridge ID Display

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 47):

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)

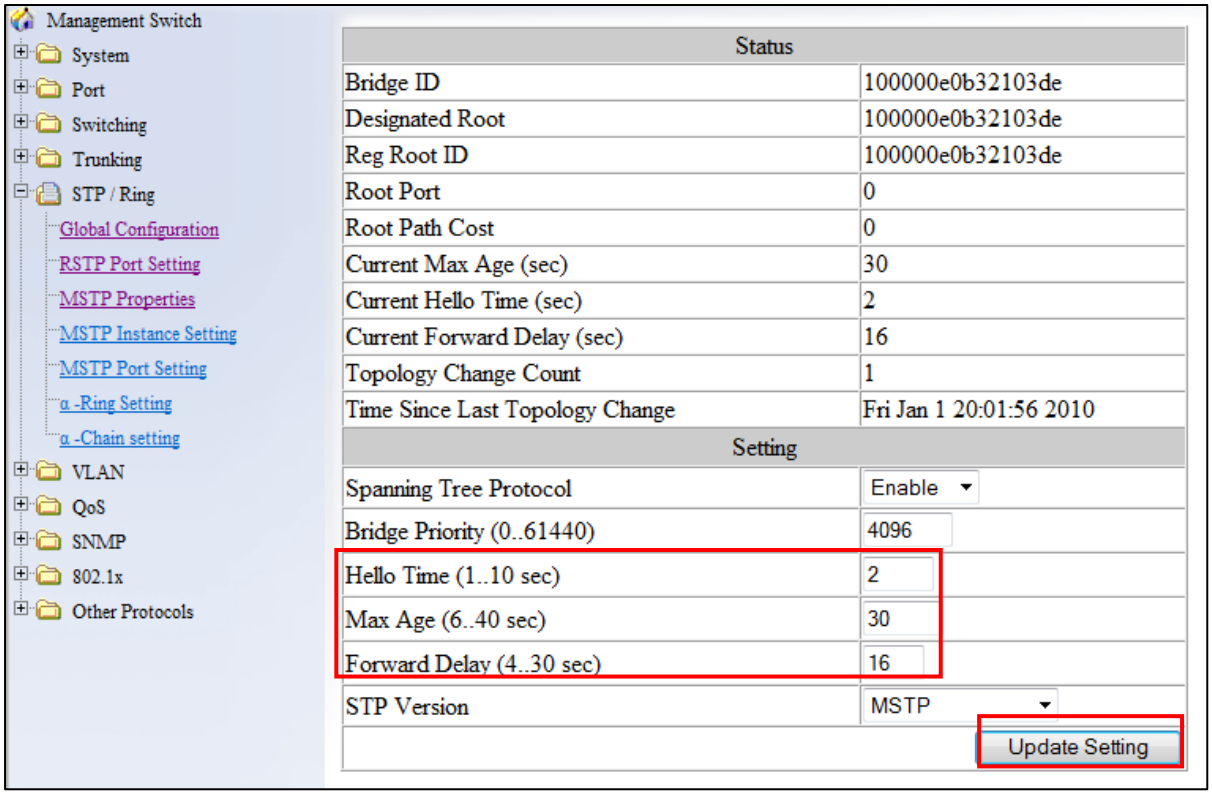


Figure 47: Max Age, Hello Timer & Forward Delay

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 below):

1. Enter the **Region Name** of the Region that the switch will belong to in the **Region Name** text entry box,
2. Enter the **Revision Level** value for the corresponding Region in the **Revision Level** text entry box,
3. Click on the **Update Setting** button.
4. Save the configuration (see the Save Configuration Page)

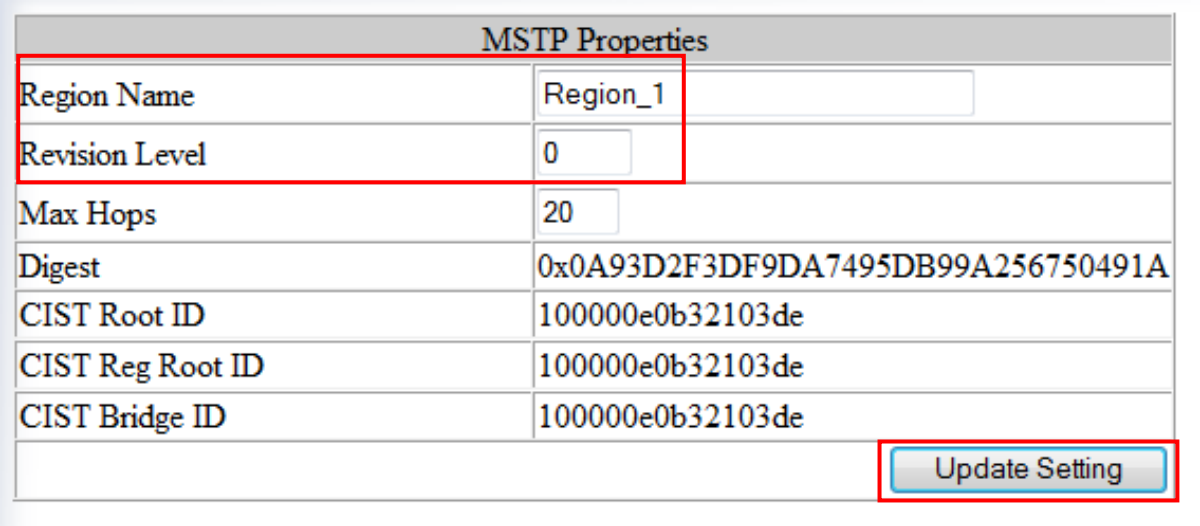


Figure 48: MSTP Region and Revision Level

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 of 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 text entry box next to **Max Hops**
2. Click on the **Update Setting** button (see below).
3. Save the configuration (see the Save Configuration Page)

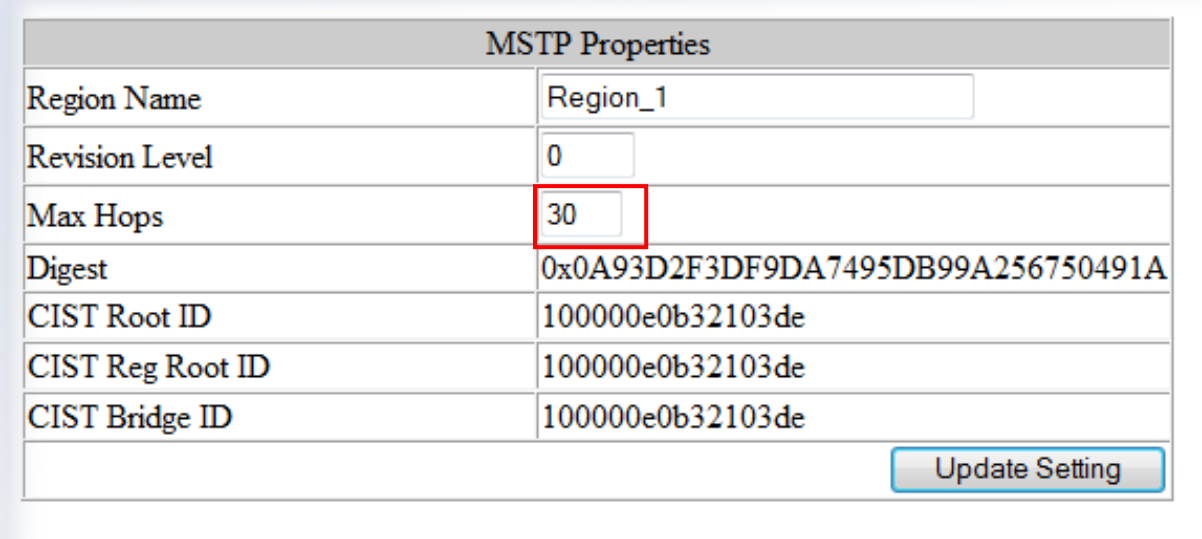


Figure 49: MSTP Properties – Max Hops

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 50),
2. Choose the **VLAN** that you want to map to a MSTI instance from the **VLAN ID** drop down box (see Figure 51).
3. Enter the **Instance ID** that you want the VLAN to map to In the text entry box 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.

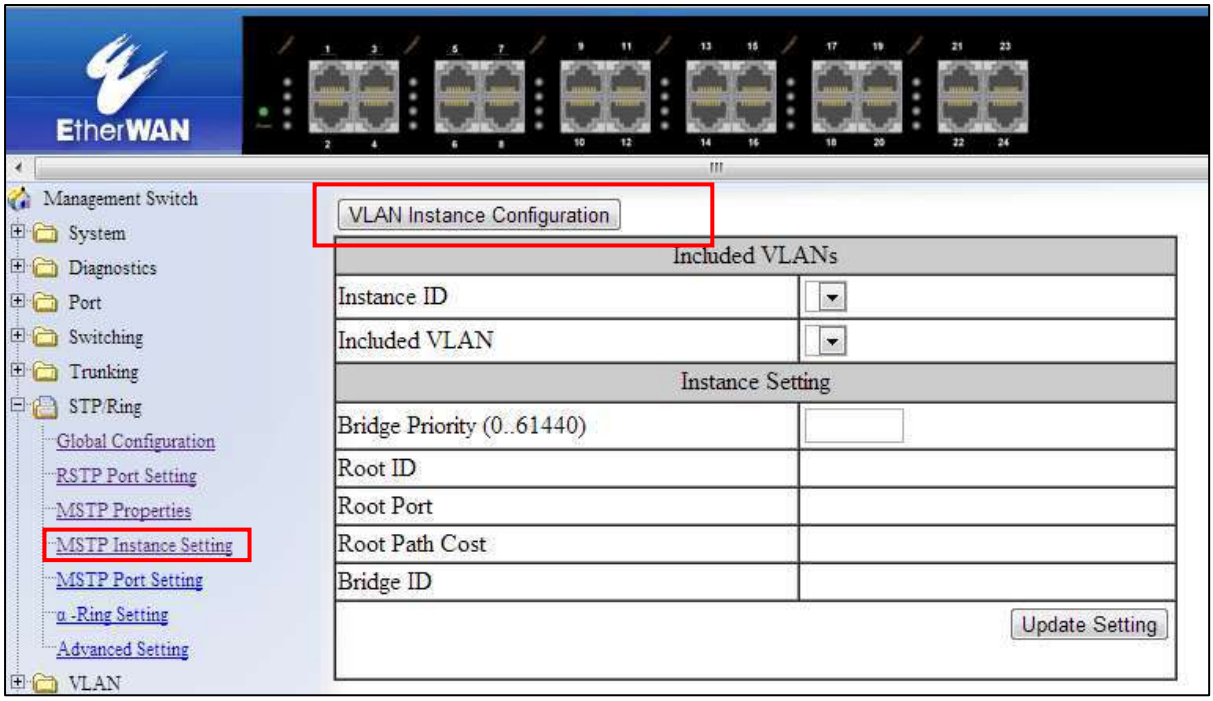


Figure 50: VLAN Instance Configuration

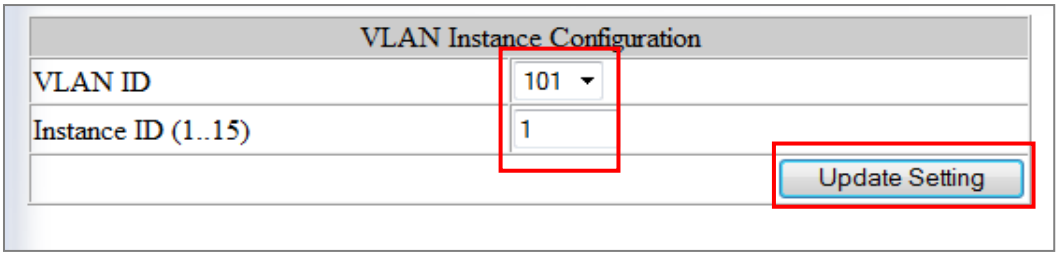


Figure 51: VLAN Instance ID

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 particular 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 particular MSTI instance.

To set the bridge priority on the switch for a specific MSTI Instance (see Figure 52):

1. Choose the particular 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)

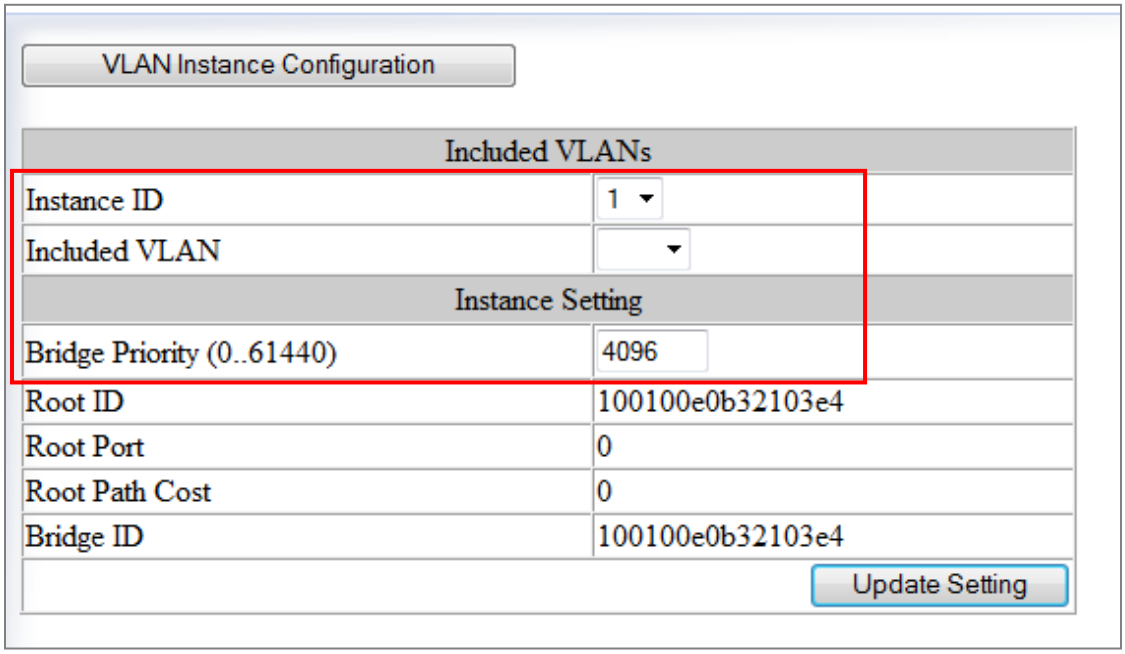


Figure 52: Setting the MSTI Regional Root Bridge

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, please follow the below steps:

1. Choose the correct MSTI Spanning Tree instance from the drop down list under **Instance ID** (see Figure 53).
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 53).
4. Save the configuration (see the Save Configuration Page)

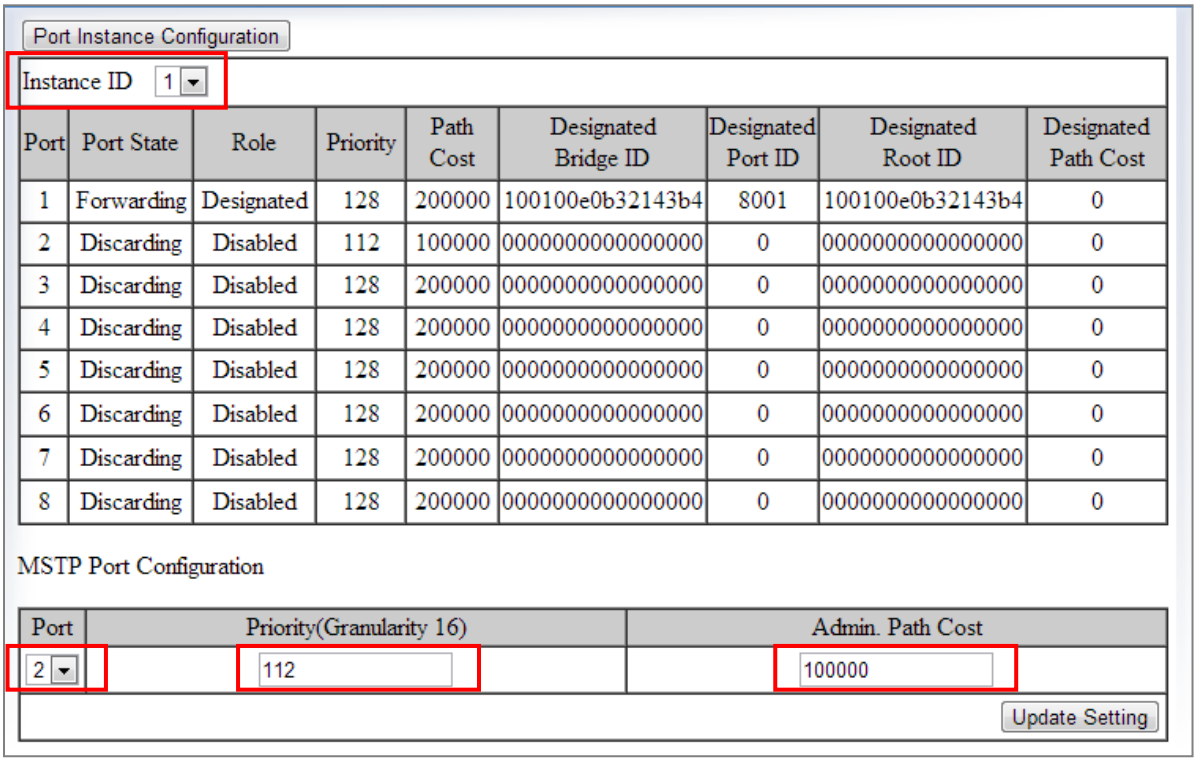


Figure 53: Port Cost & Priority

MSTP 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 MSTP port membership for the MSTP instance that the VLAN maps to.

To reconfigure the MSTP instance port membership:

1. Click on the **Port Instance Configuration** button (see Figure 54)
2. Choose the correct MSTP instance from the drop down list next to **Instance ID** (see Figure 55).
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 54: Port Instance Configuration

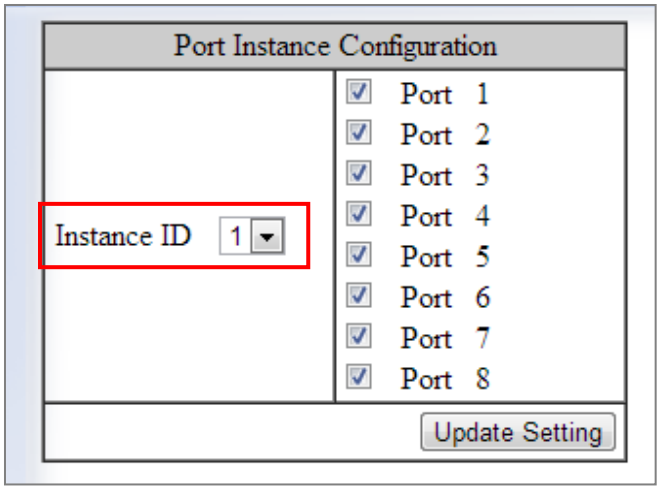


Figure 55: Port Instance - Adding Ports

MSTP Configuration Examples Using CLI Commands

Enabling Spanning Tree for MSTP

To enable the Spanning Tree function on a switch use the below CLI commands.:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
no bridge shutdown 1
bridge 1 protocol mstp

Usage Example:

```
switch_a(config)#no bridge shutdown 1
switch_a(config)#bridge 1 protocol mstp
```

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(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
```

IST MAX Hops

To configure the IST Max Hops parameter on a switch, use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **bridge 1 max-hops *<1-40>***

Usage Example:

```
switch_a(config)#bridge 1 max-hops 20
```

MSTP Regional Configuration Name and the Revision Level

To configure both the MSTP Regional Configuration Name and the Revision Level on a switch, use the following CLI commands:

CLI Command Mode: **MSTP Configuration Mode**

CLI Command Syntax:
bridge 1 region *<region_name>*
bridge 1 revision *<revision_number>*

Usage Example:

```
switch_a(config)#spanning-tree mst configuration
switch_a(config-mst)#bridge 1 region R1
switch_a(config-mst)#bridge 1 revision 0
```

Creating an MSTP Instance

To create a MSTP 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(config)#spanning-tree mst configuration
switch_a(config-mst)#bridge 1 instance 1 vlan 10
```

Setting MSTP Priority

To set the MSTI priority of a switch in a MSTP Region, use the following CLI commands:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **bridge 1 instance <*1-15*> priority <*0-61440*>**

Usage Example:

```
switch_a(config)#bridge 1 instance 1 priority 0
```

Modifying CIST Port Priority and Port Path Cost

To modify the CIST Port Priority and CIST Port Path Cost on a switch, use the below CLI commands:

CLI Command Mode: **Interface Configuration Mode (port)**

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

Usage Example:

```
switch_a(config-if)#bridge-group 1 path-cost 200000
switch_a(config-if)#bridge-group 1 priority 128
```

To modify the MSTP Port Priority and MSTP Port Path Cost for an Instance on a switch, please 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(config-if)# bridge-group 1 instance 1 path-cost 20000
switch_a(config-if)# bridge-group 1 instance 1 priority 128
```

Adding a Port to an MSTP Instance

To add a port to a MSTP instance (this port must be a member port of the VLAN that is mapped to the MSTP instance), please use the below CLI commands:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **bridge-group 1 instance *<1-15>***

Usage Example:

```
switch_a(config-if)#bridge-group 1 instance 1
```

STP/RING PAGE - ALPHA RING

Alpha Ring Setting Page

To navigate to the STP/Ring **α-Ring Settings** page:

1. Click on the **+** next to **STP/Ring**.
2. Click on **α-Ring Setting.**

EtherWAN α-Ring Technology

The α-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 α-Ring are:

- **High-speed Recovery** – Less than 15 milliseconds
- **Flexibility for Network Deployment** – Coexistence with STP, RSTP, and MSTP
- **Ring Coupling** – Smaller rings coupled together to increase network efficiency

Implementing a Simple α-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 α-Ring need to be assigned to provide the connection redundancy.

1. Change **Ring Port 1** to the port you will be using for the first redundant connection
2. Change **Ring Port 2** to the port you will be using for the second redundant connection.
3. Click on the Update Setting button.
4. Save the configuration

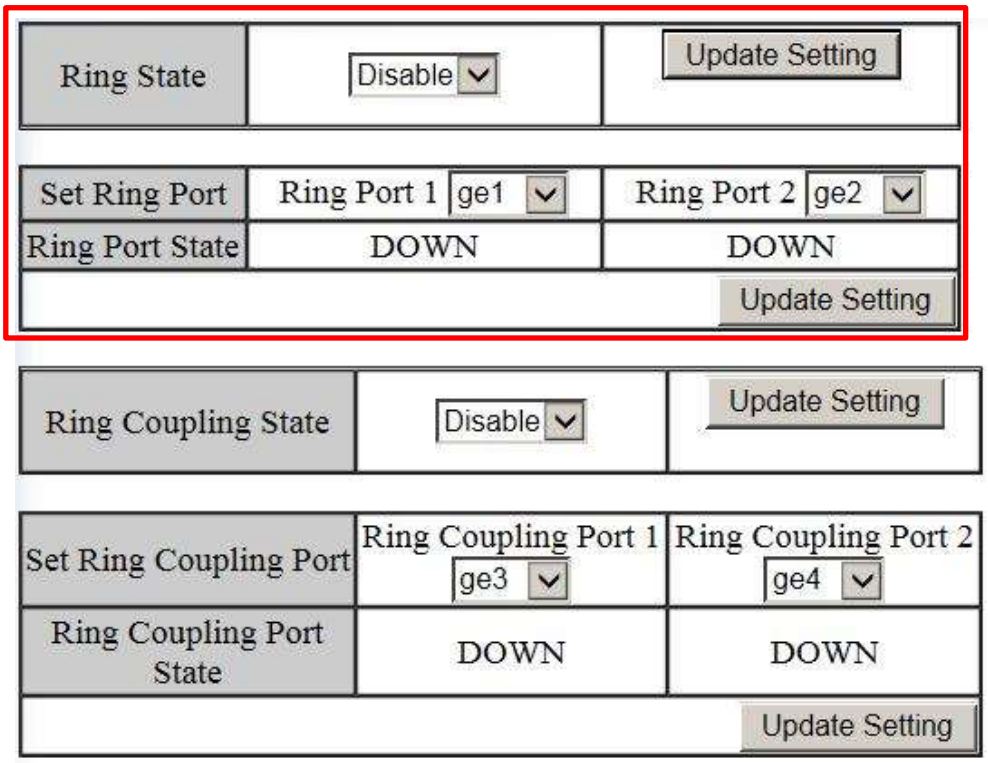


Figure 56: α-Ring Settings

Connecting two α-Ring Networks together

To navigate to the **STP/Ring α-Ring Settings** page:

1. Click on the + next to **STP/Ring**.
2. Click on **α-Ring Setting**.

As additional switches are added to a network, it may become necessary to connect multiple α-Ring networks together. This is called **Ring-coupling** and uses two additional Ethernet ports on the switch. To setup Ring-coupling (see Figure below):

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 drop-down list under **Ring Coupling Port 1**
4. Choose the desired port from the drop-down list under **Ring Coupling Port 2**
5. Click on the **Update Setting** button.
6. Save the configuration.

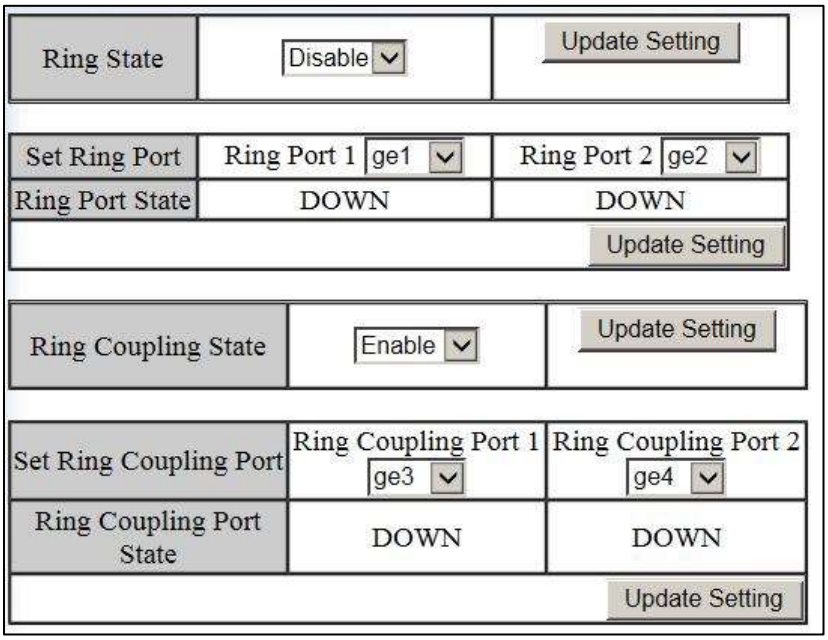


Figure 57: Ring Coupling

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**.

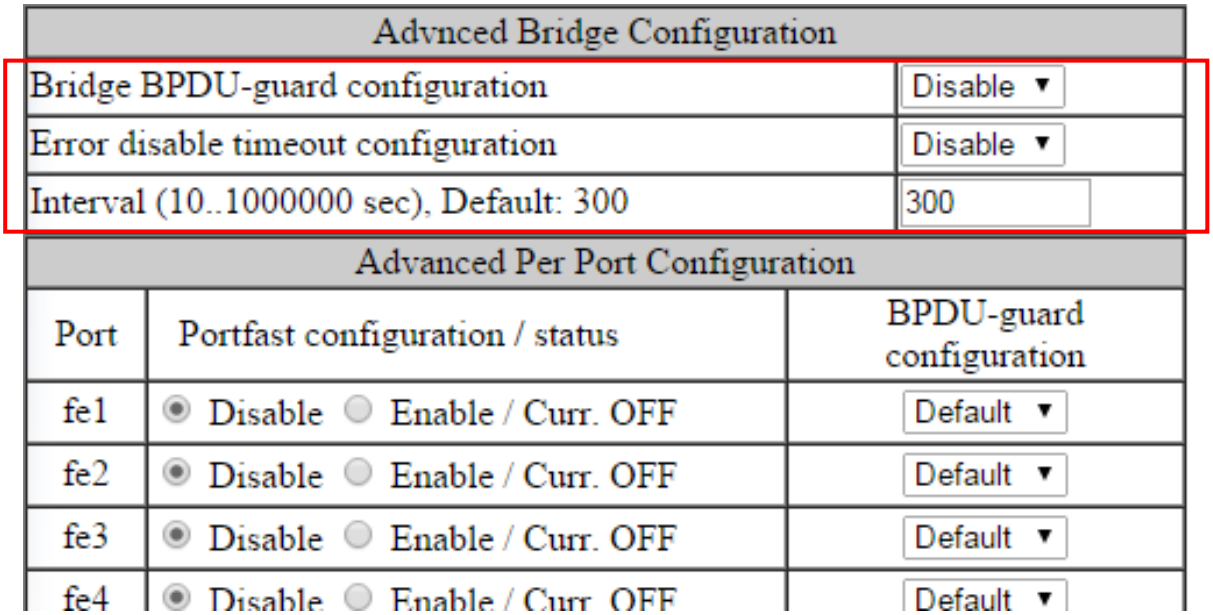


Figure 58: Advanced Bridge Configuration

Advanced Per Port Configuration

- **Portfast Configuration / status –** Enabling this for Edge ports (ports connecting to an end device as opposed to another switch) protect the

- **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

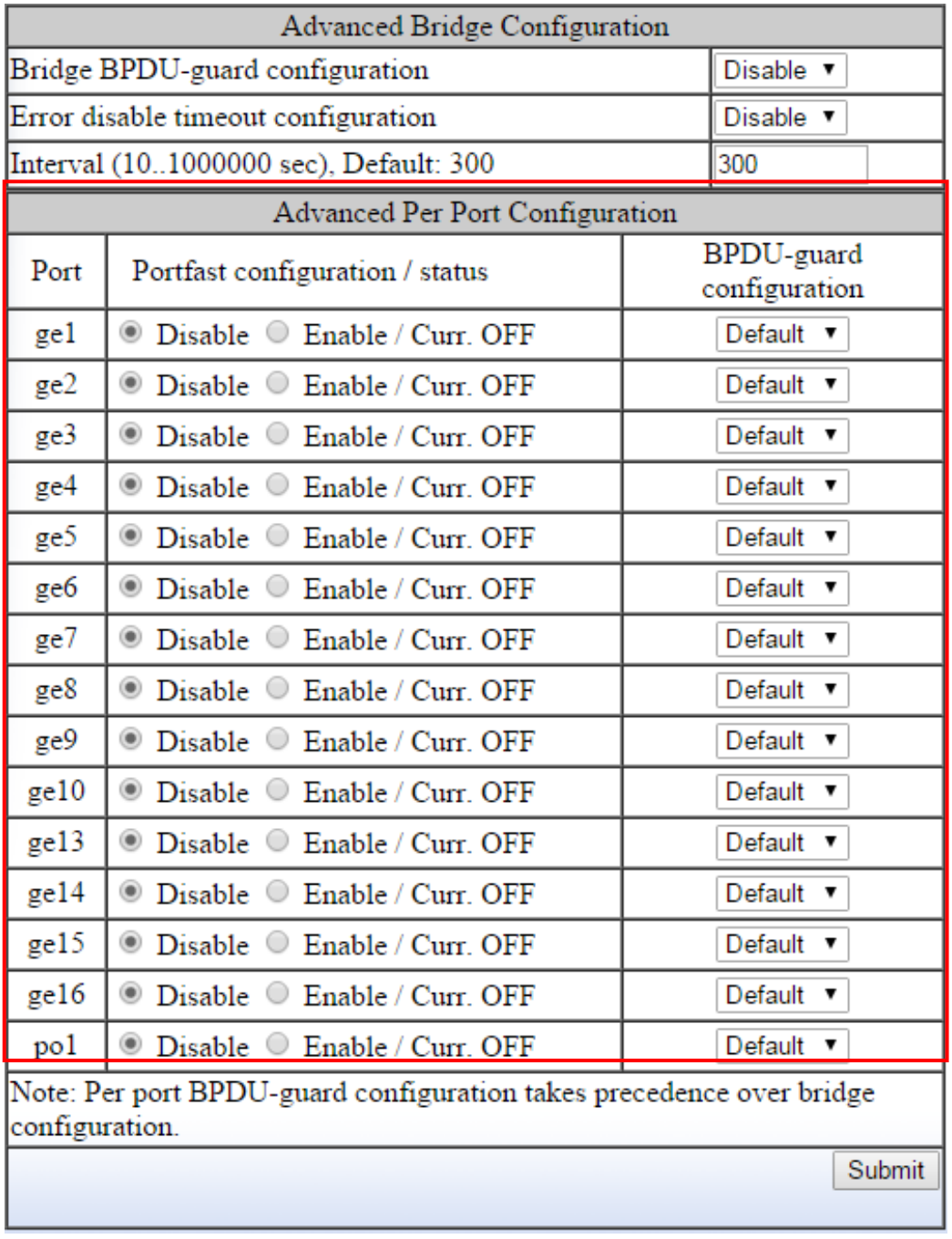


Figure 59: Advanced Per Port Configuration

Configuring Spanning Tree Advanced Settings using CLI commands

Enabling BPDU Guard Globally

To enable the BPDU Guard feature **globally** on the switch use the below CLI commands

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **bridge 1 spanning-tree portfast bpdu-guard**

Usage Example:

```
switch_a(config)# bridge 1 spanning-tree portfast bpdu-guard
```

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: **Switch-Port Interface Configuration Mode**

CLI Command Syntax:
spanning-tree portfast;
spanning-tree portfast bpdu-guard enable

Usage Example:

```
switch_a(config-if)#spanning-tree portfast
switch_a(config-if)#spanning-tree portfast bpdu-guard enable
```

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(config)#bridge 1 spanning-tree errdisable-timeout enable
switch_a(config)#bridge 1 spanning-tree errdisable-timeout interval
300
```

VLAN

Port Based VLAN vs. Tagged Based VLAN

The EtherWAN Managed Switch can be configured to operate in one of two VLAN modes: Port based VLAN mode or Tagged based VLAN mode. In Port based VLAN mode, packets from different VLANs can only be segregated from one another while within a single switch, but not when the packets travel to other switches in the network. The VLAN association rule for all incoming packets in Port based VLAN mode is determined only by the VLAN ID that is associated with the port when a packet enters the switch.

In Tagged based VLAN mode, traffic from different VLANs can be segregated from one another even after it travels to another switch. This is done by “tagging” (inserting information inside a packet) a packet with the VLAN ID that the packet belongs to when the packet exits the switch. The VLAN association rule for incoming packets in Tag based VLAN mode can either be based on the VLAN ID that is assigned to the port (PVID) when a packet enters the switch (in the event when the packet does not contain a VLAN ID), or it can be determined from the packet itself (when the packet does contains a VLAN ID).

VLAN Configuration in 802.1Q Tag Based VLAN Mode

General Overview

802.1Q VLAN configuration consists of the following four elements:

1. Creating all VLANs in the VLAN database.
2. Configuring an incoming untagged packet’s VLAN association rule: this is accomplished by configuring the PVID setting on each individual port.
3. Configuring the ports that are associated with a VLAN to allow the packets that belong to that VLAN to exit and enter the switch through that port.

4. Configuring the tag action on the outgoing packets for each VLAN, that is to say, deciding on whether or not an outgoing packet will be tagged with the VLAN number that the packet belongs to.

All ports on the EtherWAN Managed 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.

Configuring 802.1Q VLAN Database

To navigate to the **802.1Q VLAN Setting** page:

1. Click on the **+** next to **VLAN**.
2. Click on **802.1Q VLAN Setting.**

To configure the 802.1Q VLAN Database, please do the following:

1. Click on the **Add VLAN** button (see Figure 60).

Figure 60: Add VLAN

2. Enter the **VLAN ID**.
3. Enter the **VLAN Name**.
4. Select **Attach** or **Detach** for the **CPU Port.**
    a. Attaching the CPU to a VLAN is typically done on the Management VLAN.
5. Select the ports to be a member of the VLAN (see Configuring the VLAN Egress (outgoing) Member Ports)
6. Click on **Submit** button.
7. Repeat for all the VLANs that are needed.
8. Save the configuration (see the Save Configuration Page)

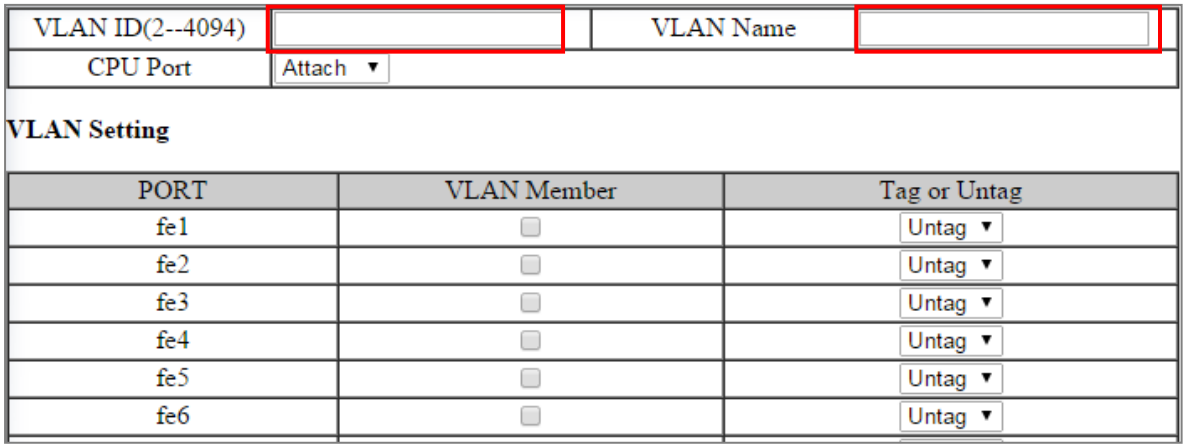


Figure 61: Add VLAN Page

802.1Q Tag Based VLAN Configuration Examples Using CLI Commands

Configuring a 802.1Q VLAN

To configure a 802.1Q VLAN on a switch use the following CLI commands

CLI Command Mode: **VLAN Database Configuration Mode**

CLI Command Syntax: **switchport portbase add vlan <1 – 16> vlan <1 – 4094> bridge 1 name VLAN NAME state enable**

Usage Example:

```
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
```

Configuring an IP Address for a Management VLAN

To configure the IP address for the management VLAN use the following CLI commands

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(config)#interface vlan1.100
switch_a(config-if)#ip address 192.168.100.10/24
```

Removing an IP Address from a Management VLAN

To remove an IP address from a management VLAN use the following CLI commands

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **no ip address**

Usage Example:

```
switch_a(config)#interface vlan1.100
switch_a(config-if)#no ip address
```

Configuring an Access Port

To configure an Access Port use the following CLI commands:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **switchport mode access**

CLI Command Syntax: **switchport access vlan <1 – 4094>**

Usage Example:

```
switch_a(config-if)#switchport mode access
switch_a(config-if)#switchport access vlan 100
```

Configuring a Trunk Port

To configure a Trunk Port use the following CLI commands:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **switchport mode trunk**

CLI Command Syntax: **switchport trunk allowed vlan add 100,200,300**

CLI Command Syntax: **switchport trunk native vlan 1**

Usage Example:

```
switch_a(config)#interface fe7
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
```

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 below).
3. Save the configuration (see the Save Configuration Page)

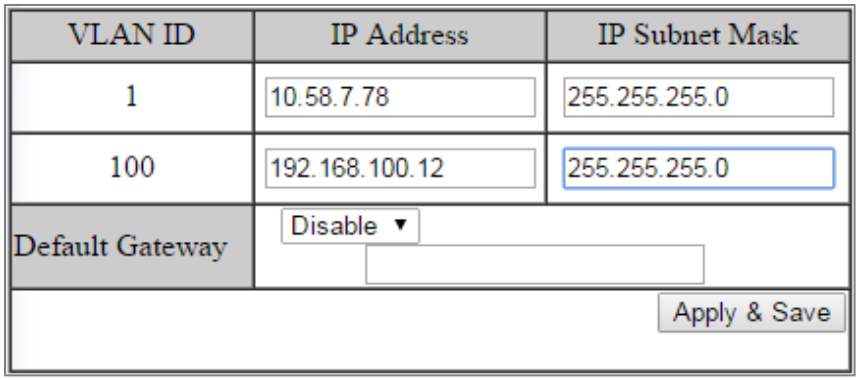


Figure 62: Management VLAN IP Address

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.

Configuring the Port Type and the PVID setting

To navigate to the **802.1Q Port Setting** page:

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

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 (see General Overview for port type details).
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.

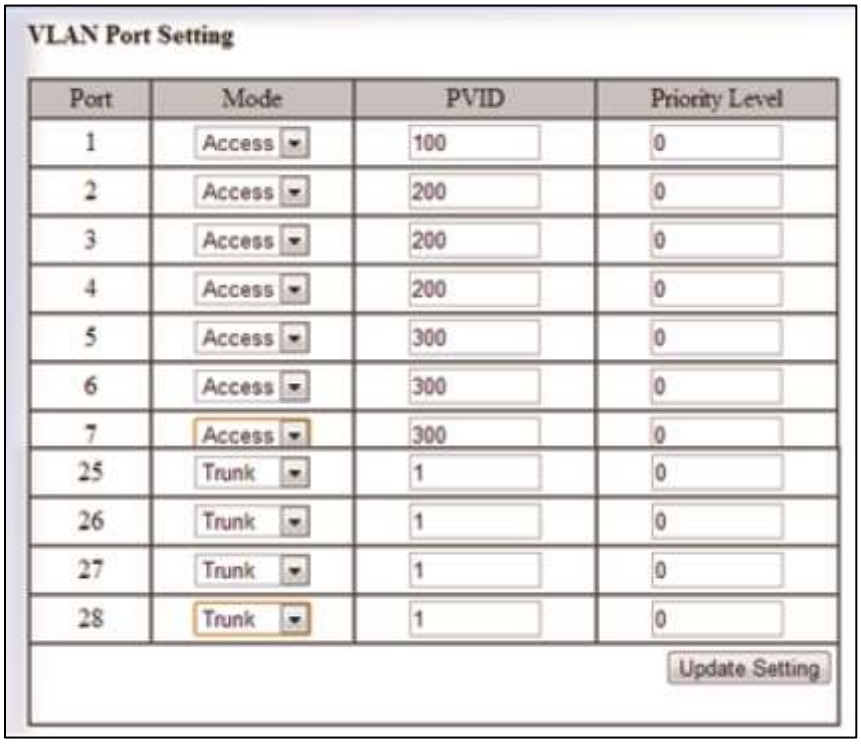


Figure 63: VLAN Port Setting

Configuring the VLAN Egress (outgoing) Member Ports

To navigate to the **802.1Q VLAN Setting** page:

1. Click on the **+** next to **VLAN**.
2. Click on **802.1Q VLAN Setting.**

To configure the egress member ports for each VLAN:

1. Click on the VLAN link that you want to configure (see below).

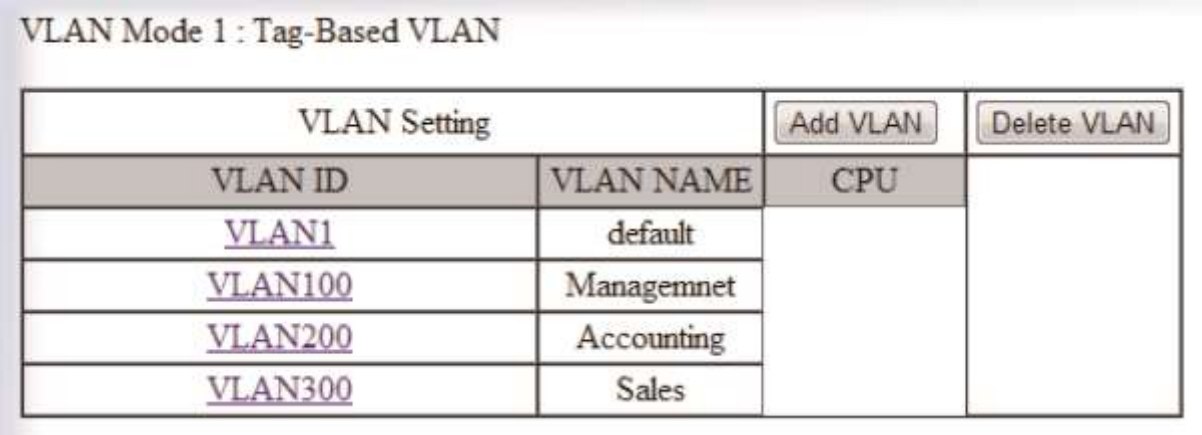


Figure 64: VLAN Links

2. Check the check box next to the port number that should be the egress member port for this VLAN
3. Click on the **Submit** button (see Figure 65).

Note: If an egress member port for a VLAN has the PVID set on that port to be the same as the VLAN, then that port will automatically be configured as an egress member port for the VLAN by the switch. If a check box is not checked and is grayed out, it is because that port is an Access Port with the PVID set to be a different VLAN than the current VLAN.

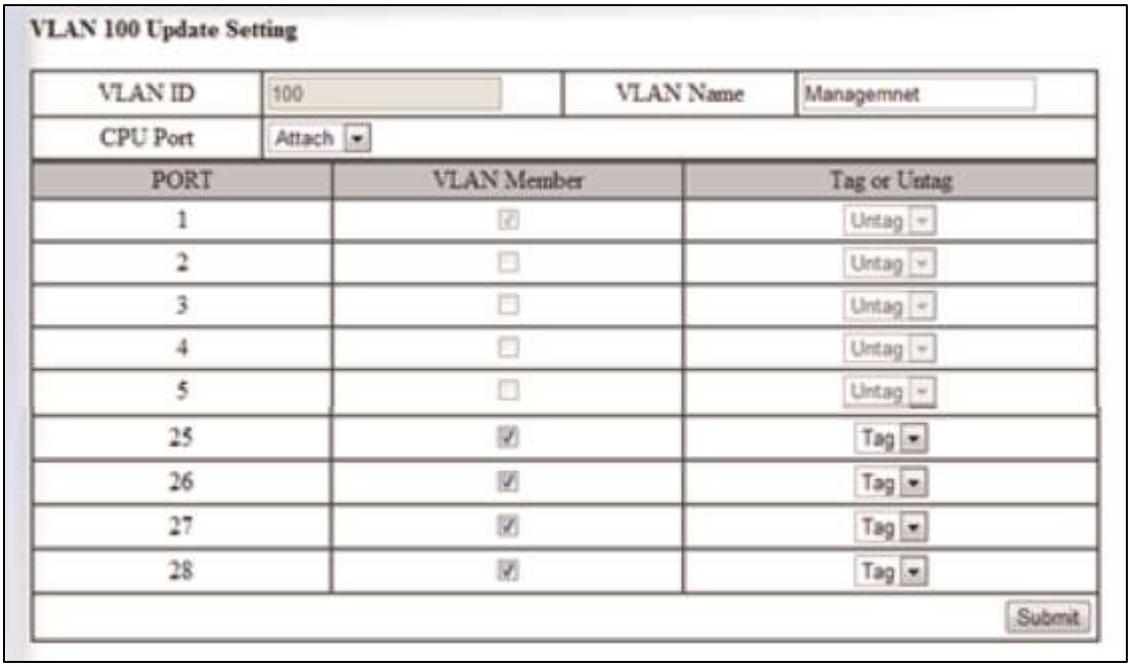


Figure 65: VLAN Ports

If any of the egress member ports are Hybrid ports, you must also configure the Tag action on this port (see Figure 66).

4. Select the correct **Tag** option in the drop down list under **Tag or Untag** for this port.
5. Click on the **Submit** button.

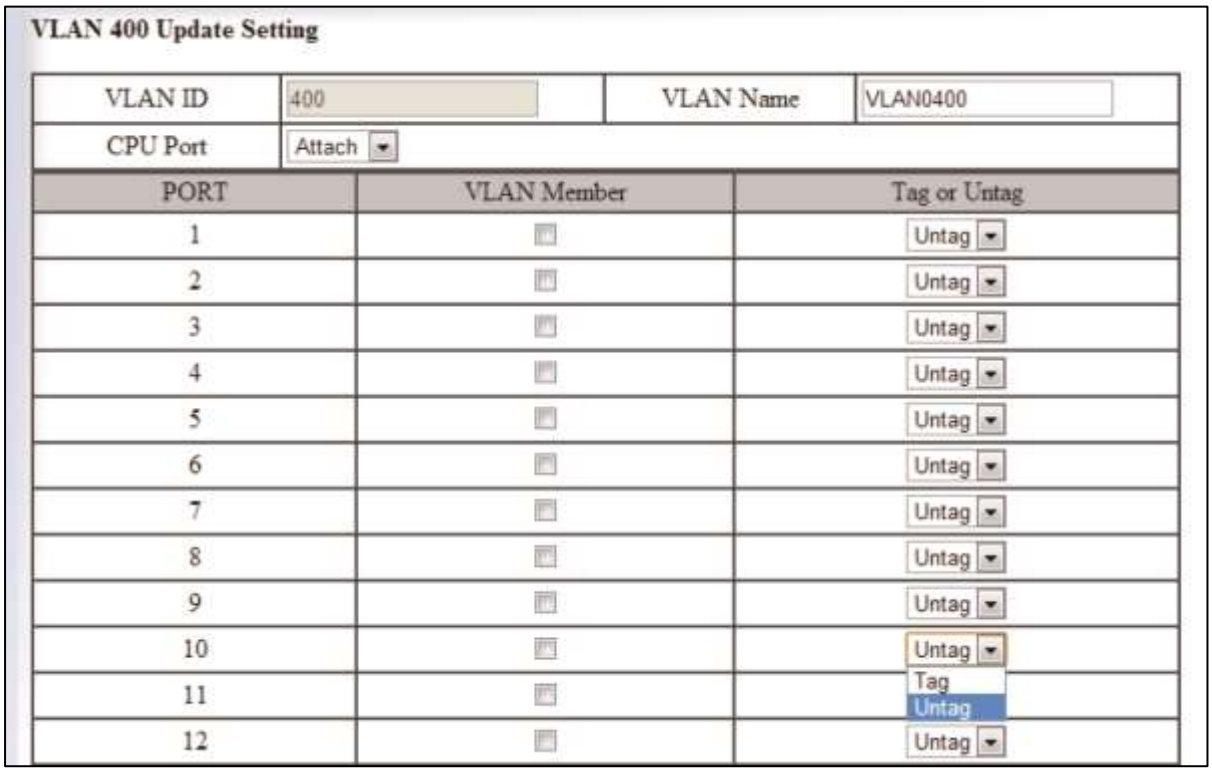


Figure 66: Tag or Untag ports

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 EtherWAN Managed 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

The above recommendations are implemented in the V1.94.2 EtherWAN Managed Switch's 802.1p 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 below):

1. Click on the **+** next to **QoS**.
2. Click on **Global Configuration**.

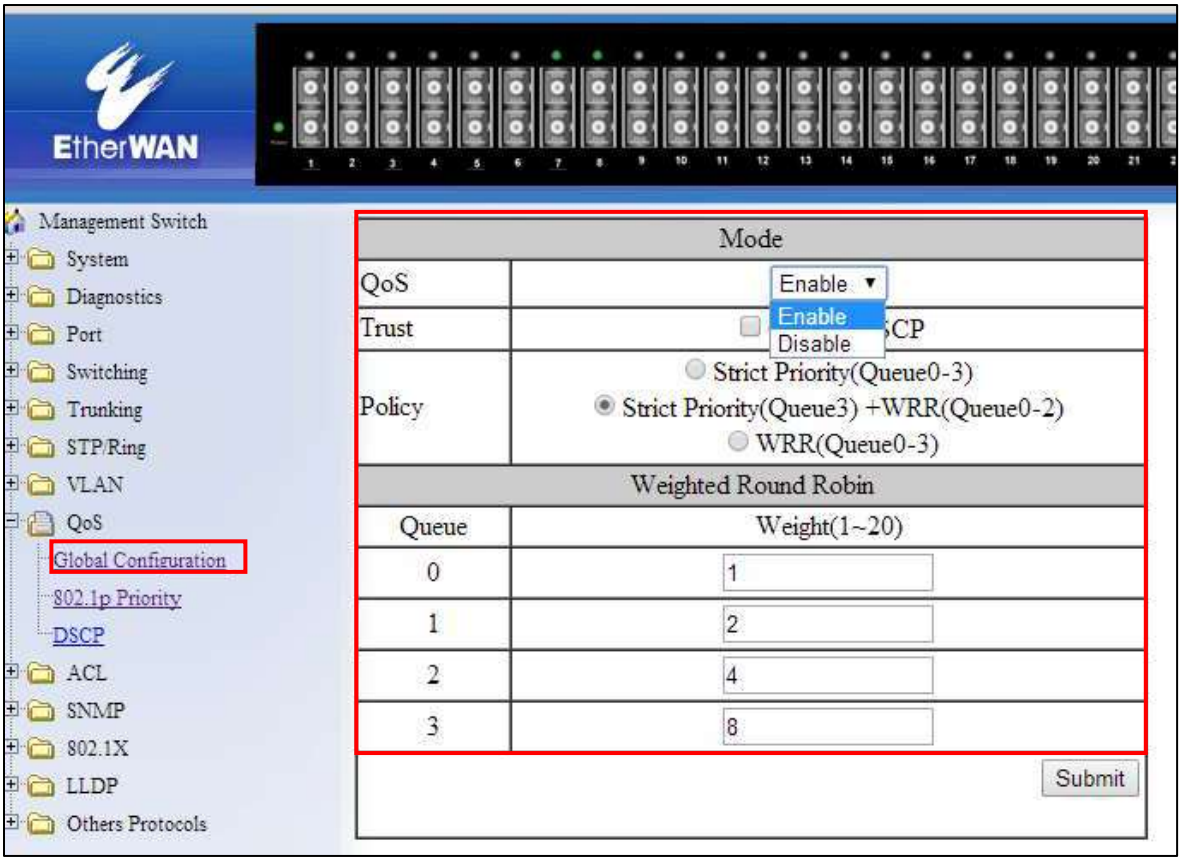


Figure 67: Enabling QoS

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(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).
    b. **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

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

To get to the CLI level to configure QoS:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
mls qos enable
no mls qos

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(config)# mls qos trust cos
```

Usage Example – Disable QoS Trust:

```
switch_a(config)# no mls qos trust
```

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 3) + WWR (Queue 0-2):

```
switch_a(config)# priority-queue out
```

Usage Example – Disable QoS Strict Priority:

```
switch_a(config)# no priority-queue
```

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(config)# wrr-queue bandwidth 1 2 4 8
```

802.1p Priority Page

Web GUI Interface

To navigate to the **QoS 802.1p Priority** page (see Figure 68):

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.

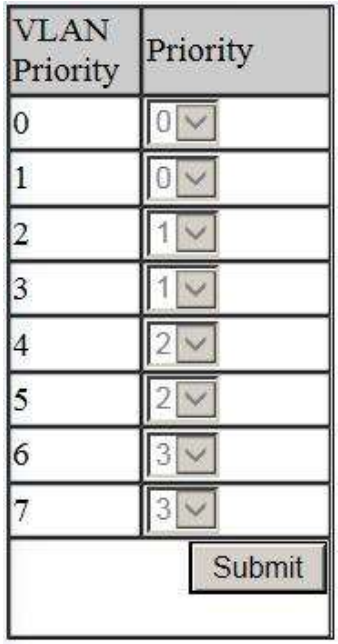


Figure 68: 802.1p Priority

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(config)#wrr-queue cos-map 1 0 1
```

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:

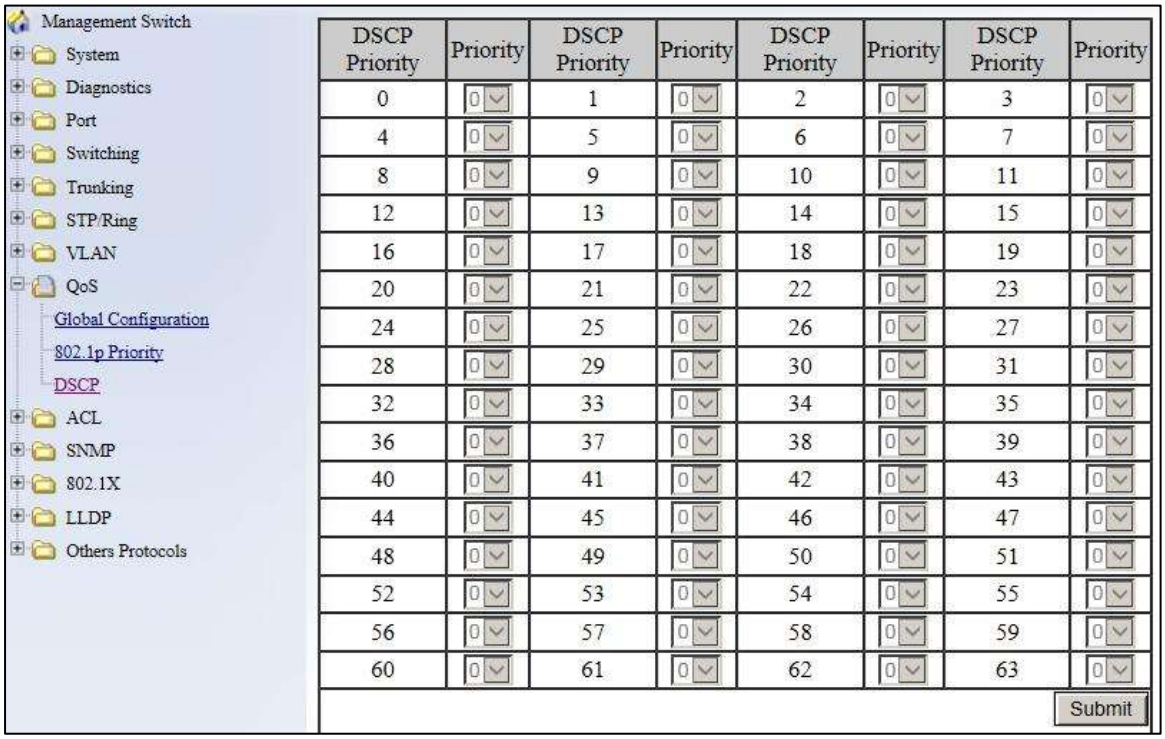


Figure 69: DSCP

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(config)# mls qos map dscp-queue 0 1 2 3 to 1
```

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>***

ACL (ACCESS CONTROL LIST)

This section applies only to specific models of EtherWAN Switches.

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).

General Overview

The ACL feature on the EtherWAN Managed Switch filters packets through access control lists. Any combination of 4 different types of access control lists (called Access Lists) can be used for this purpose. These four different types of access control lists are explained below:

IP Access List:
This Access List can be used to filter IP packets based on the packet's source IP address only.

IP Access List (Extended):
This Access List can be used to filter IP packets based on the packet's source and destination IP addresses, as well as the packet's source and destination transport layer protocol port numbers.

MAC Access List:
This Access List can be used to filter Ethernet packets based on the packet's source and destination Ethernet addresses as well as the packet's Ethernet payload protocol number (EtherType).

Layer 4:
This Access List, if it is used by itself, can only be used to classify IP packets based

only on the IP packet's source and destination transport layer protocol port numbers. Use this Access List in conjunction with another type of Access List mentioned above, if you wish to filter any packet from entry to the switch that did not match the classification rules from this Access Lists, otherwise all packets that did not match the classification rules of this Access List will also be allowed entry into the switch.

Note: You can use any combination of the above four types of Access Lists to filter packets through the ACL feature, the switch will apply these Access Lists in the order that they were configured. Since Access List filters allow packets through, there must be at least one catch all deny rule that can deny all types of packets from entry to the switch in the very last Access List, This will ensure that only packets specified in the access list will be allowed.

Configuring ACL

To navigate to the **ACL/ACL Configuration** page:

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

In order to enable the ACL feature on the EtherWAN switch, the QoS feature must be enabled on the switch as well. In order to apply the ACL packet filtering features on a port, you must:

1. Create and configure an ACL Access List first.
2. Next, you will need to create and configure an ACL Class Map,
3. Associate the previously created ACL Access Lists to this ACL Class Map.
4. Next, create and configure an ACL Policy Map
5. Associate all the appropriate and necessary ACL Classes into this ACL Policy Map.
6. Then apply this ACL Policy Map (and all the Access Lists that it contains) to a specific port.

To enable the ACL feature on the EtherWAN switch first enable the QoS feature using the steps below (see Figure 70).

1. From the drop-down list next to **QoS**, choose the **Enable** option
2. Click on the **Submit** button. For more details see QoS.

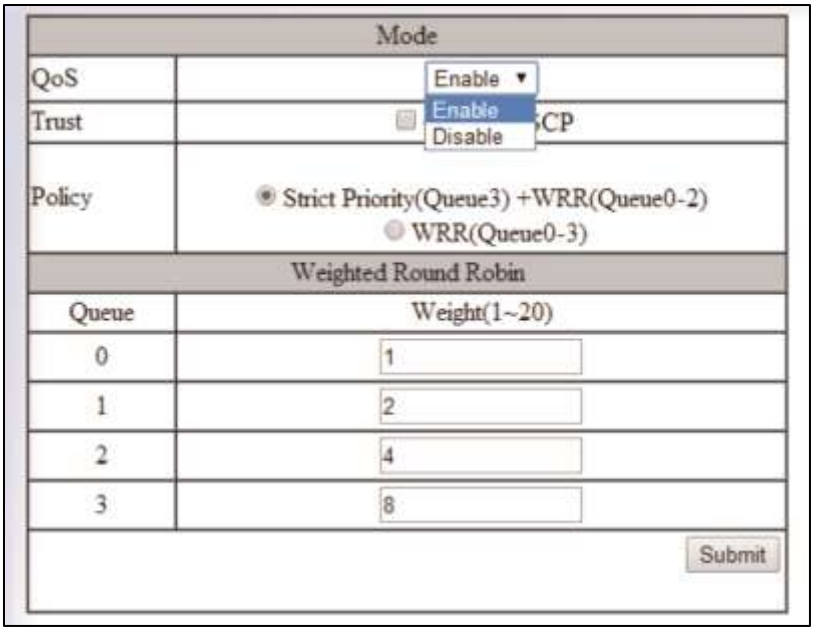


Figure 70: Enabling QoS

ACL Policy Map

To create a new ACL Policy Map, follow the instructions below.

1. Make sure that the **Create** option is selected from the drop-down list next to **Policy Map** (see below)
2. Next, make sure that the **Create** option is selected from the drop-down list under **Class Name** (see below).

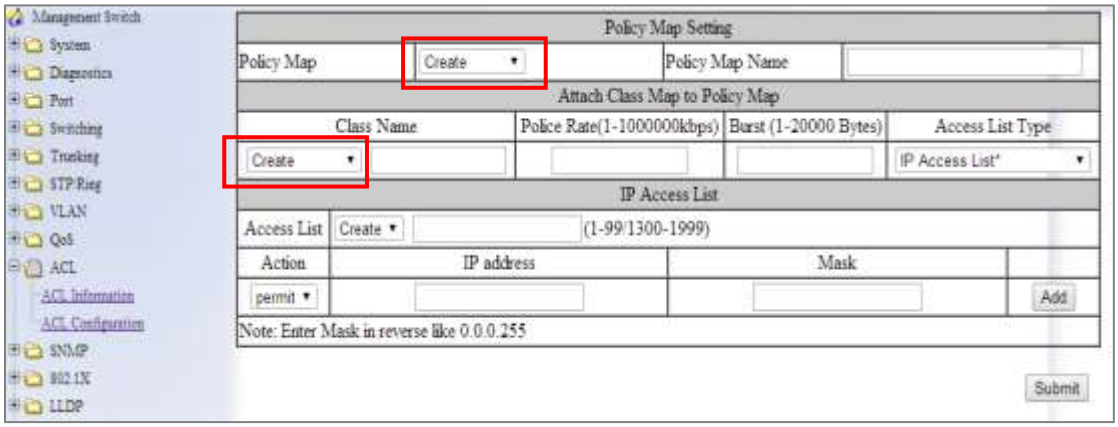


Figure 71: Policy Map

Next, you will be creating a new ACL Access List which is necessary to create an ACL Class Map. From the information listed below you will find the configuration steps necessary for all of the four available ACL Access Lists. You can choose one Access List from the below list and follow the steps there to complete the configuration for that Access List. One Access List can be created during the initial ACL Policy Map creation process. After you have chosen just one Access List from below and have finished all the configuration steps for it, please continue onto step #3.

IP Access List

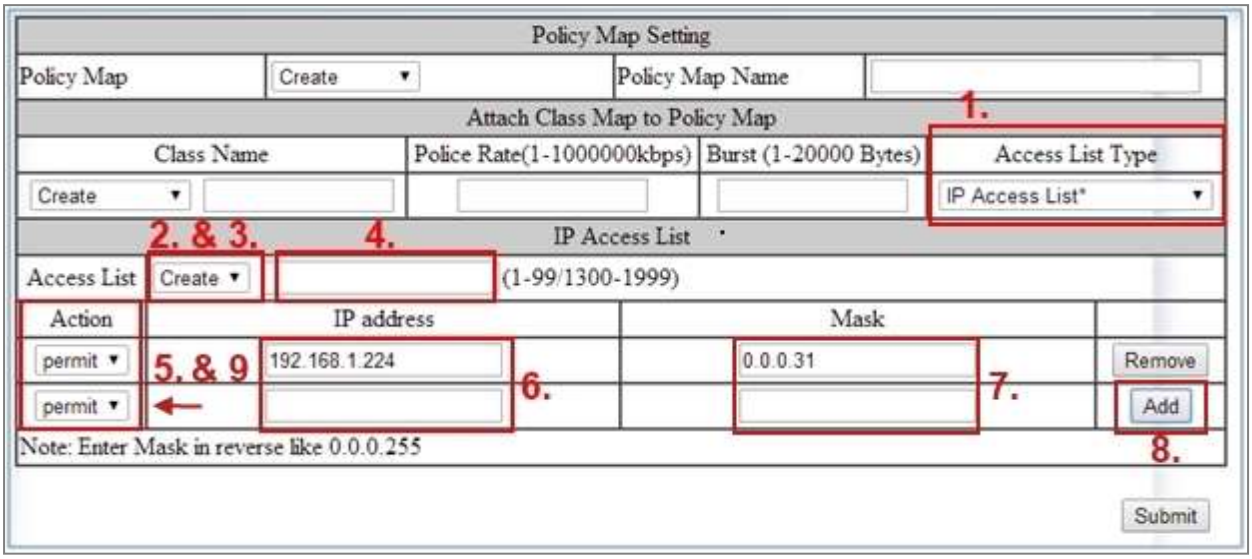


Figure 72: IP Access List

To configure an IP Access List (See Figure 72 above):

1. Select the **IP Access List** option from the drop-down list below **Access List Type**.
2. If you have already created an IP Access List previously and would like to apply it to the new ACL Class, then select the Access List number from the drop-down list next to **Access List**.
3. If you want to create a new IP Access List, make sure that the **Create** option is selected from the drop-down list next to **Access List**.
4. To give the new IP access list an ID, enter a number in the range from 1 – 99, or from 1300 – 1999, into the text entry box next to the “Create” option drop-down list.

5. You can enter a source IP address to allow an IP packet with that source IP to gain entry into the switch. To do this, choose the permit option from the drop-down list under the **Action** column.

6. Next, enter the source IP address into the text entry box from the **IP address** column.

7. Next, enter the Comparison Mask for the source IP address in reverse logic, into the text entry box from the **Mask** column. In reverse logic, 255.255.255.0 would be 0.0.0.255.

8. Next, click on the **Add** button.

9. You can enter a source IP address in order to deny an IP packet with that source IP to gain entry into the switch. To do so, you must choose the **deny** option from the drop-down list under the **Action** column. Next, enter the IP address and mask as described in step 6 and 7.

    a. You can also use the **any** wild card in lieu of entering a source IP address in the text entry box from the **IP address** column. You will need to do this if you wish to deny any additional IP packet from entry to the switch that did not match any of the previous rules from all the previous access control lists, otherwise these additional IP packets will also be allowed entry into the switch.

IP Access List (Extended)

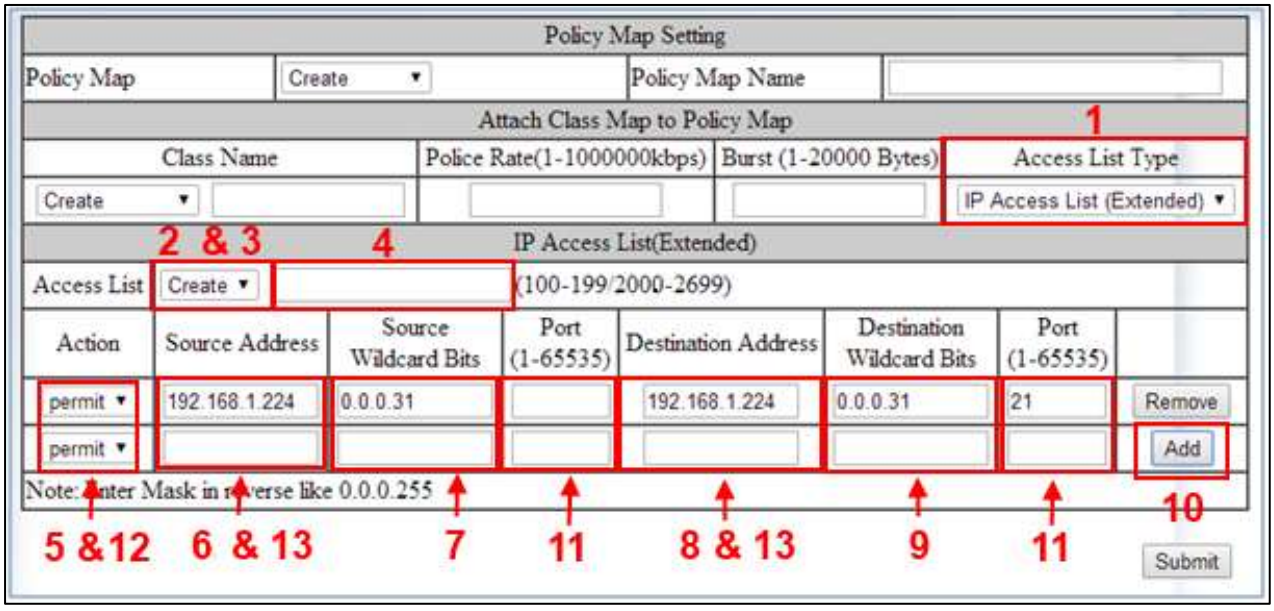


Figure 73: Access List Extended

1. Select the **IP Access List (Extended)** option from the drop-down list below **Access List Type** (see Figure 73)

2. To apply an existing **Extended IP Access** to the new ACL Class, then select the Access List number for the previously configured **Extended IP Access** List from the drop-down list next to **Access List**.

3. if you want to create a new Extended IP Access List, verify that the **Create** option is selected from the drop-down list next to **Access List**.

4. To give this particular Extended IP access list an ID, enter a number in the range from 100 – 199, or from 2000 – 2699, into the text entry box next to the **Create** option drop-down list.

5. You can enter a source and a destination IP address to allow an IP packet with these pair of IP addresses to gain entry into the switch. To do this, choose the **permit** option from the drop-down list under the **Action** column.

6. Next, enter the source IP address of the IP packet into the text entry box under the **Source Address** column.

7. Next, enter the comparison Mask for the source IP address in reverse logic (a binary “0” in the mask means “this bit position needs to checked”, whereas a binary “1” in the mask means “this bit position does not need to be checked”) into the text entry box from the **Source Wildcard Bits** column. In reverse logic, 255.255.255.0 is listed as 0.0.0.255.

8. Next, enter the destination IP address of the IP packet into the text entry box under the **Destination Address** column.

9. Next, enter the comparison Mask for the destination IP address in reverse logic into the text entry box from the **Destination Wildcard Bits** column.

10. Next, click on the **Add** button.

11. You can also filter the IP packet using the packet’s source and destination Transport Layer protocol port numbers in addition to the source and destination IP addresses. Just enter the source Transport Layer protocol port number into the text entry box under the **port (1-65535)** column following the source IP address comparison mask column. Next, enter the destination Transport Layer protocol port number into the text entry box under the **port (1-65535)** column following the destination IP address comparison mask column.

12. To enter an extended IP access list entry in order to deny the entry of an IP packet into the switch, you must choose the **deny** option from the drop-down list under the

Action column. Next, enter the IP addresses and Transport Layer protocol port numbers using the same steps as in the previous two bullets.

13. You can also use the **any** wild card in lieu of entering an IP address in the text entry box from both the **Source Address** and **Destination Address** column. You will need to do this if you wish to deny any additional IP packet from entry to the switch that did not match any of the previous rules from all the previous access control lists, otherwise these additional IP packets will also be allowed entry into the switch.

Mac Access List

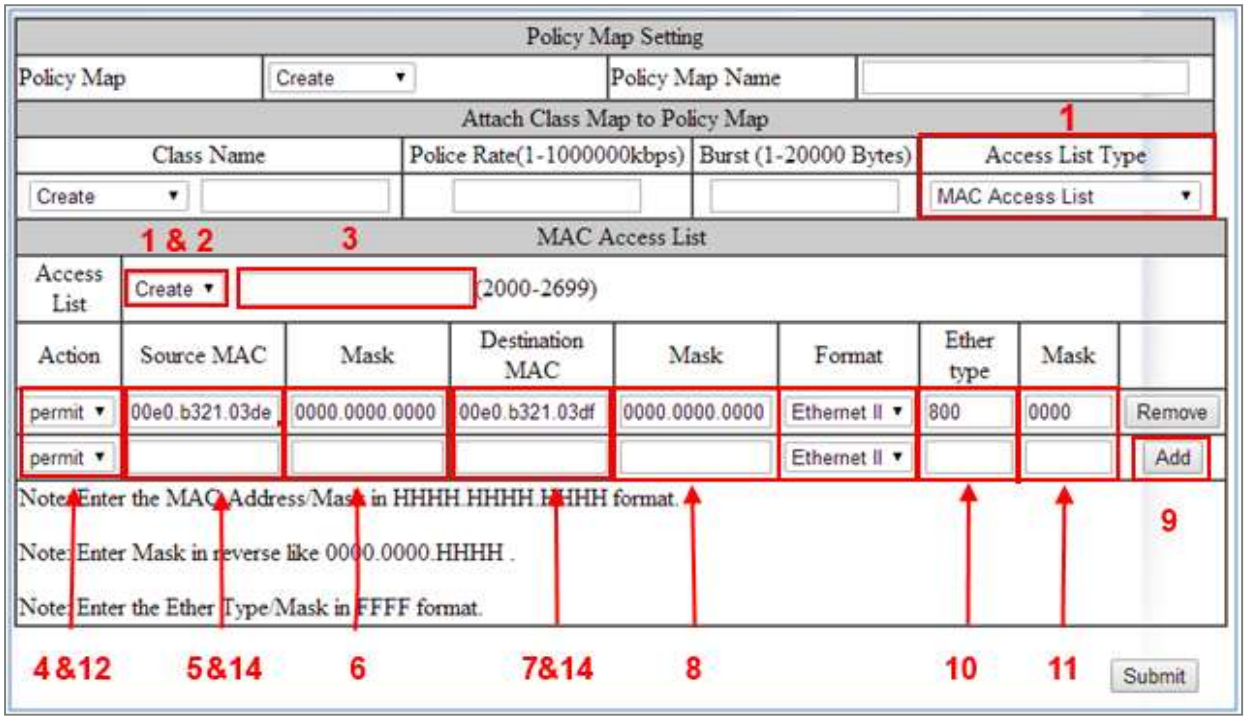


Figure 74: MAC Access list

1. To configure a MAC access list, select the **MAC Access List** option from the drop-down list below **Access List Type** (see Figure 74).
2. If a MAC Access List was previously created and you would like to apply it to the new ACL Class, then select the **Access List number** for the previously configured MAC Access List from the drop-down list next to **Access List**. If you want to create a new MAC Access List, insure that the **Create** option is selected from the drop-down list next to **Access List**.

3. To give this particular MAC Access List an ID, enter a number in the range from 2000 – 2699, into the text entry box next to the **Create** option drop-down list.

4. You can enter a source and a destination Ethernet address to allow a specific Ethernet packet entry into the switch. To do so, you must choose the **permit** option from the drop-down list under the **Action** column.

5. Next, enter the source Ethernet address of the Ethernet packet into the text entry box under the **Source MAC** column.

6. Next, enter the **Comparison Mask** for the source Ethernet address in reverse logic (Ex. 255.255.255.0 is 0.0.0.255 in reverse logic) into the text entry box from the **Mask** column following the **Source MAC** column.

7. Next, enter the destination Ethernet address of the Ethernet packet into the text entry box under the **Destination MAC** column.

8. Next, enter the comparison Mask for the destination Ethernet address in reverse logic into the text entry box from the **Mask** column following the **Destination MAC** column. Next, choose the appropriate encapsulation format of the Ethernet packet that you want to allow entry into the switch from the drop-down list under the **Format** column.

9. Next, click on the **Add** button.

10. You can also filter the Ethernet packet using the Ethernet packet payload's **EtherType number** in addition to the source and destination Ethernet addresses. Just enter the **EtherType number** of the Ethernet packet into the text entry box under the **Ether type** column.

11. Next, you can also enter a **comparison mask** for the EtherType number into the text entry box under the **Mask** column next to the **Ether type** column.

12. To enter a MAC Access List entry in order to deny the entry of an Ethernet packet into the switch, you must choose the **deny** option from the drop-down list under the **Action** column.

13. Next, enter the Ethernet addresses and the EtherType number using the same steps as in steps 11 and 12.

14. You can also use the **any** wild card in lieu of entering an Ethernet address in the text entry box from both the **Source MAC** and **Destination MAC** column. You will need to do this if at any time this Access List should become the very last Access List rule in a ACL Policy Map to serve as the catch all deny rule in order to deny any and all types of packets from entry into the switch that did not match any of the previous rules from all the previous access control lists.

Layer 4

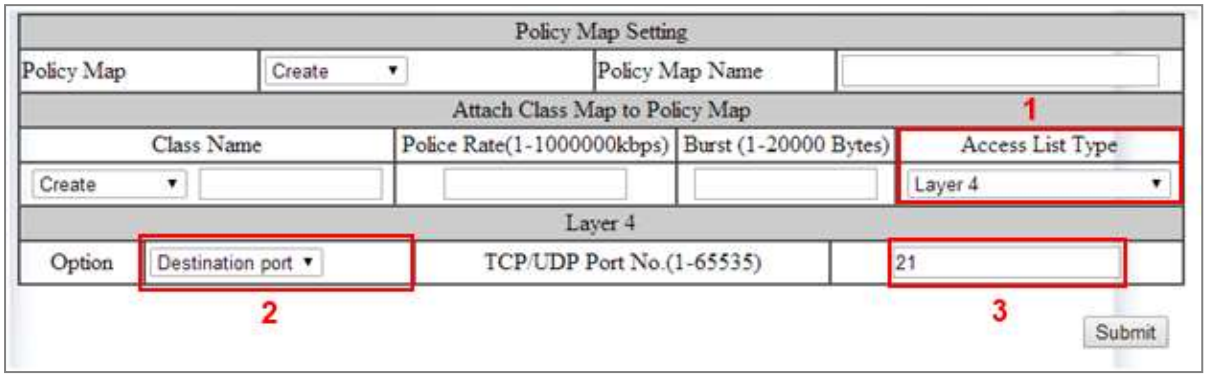


Figure 75: Layer 4

1. To use the Layer 4 access list feature and apply it to the new ACL Class, select the **Layer 4** option from the drop-down list below **Access List Type** (see Figure 75).
2. You can enter a source or destination Transport Layer protocol port number to allow any IP packet with this port number to gain entry into the switch. To do this, choose the appropriate port number type (Source port or Destination port) from the drop-down list next to **Option**.
3. Next, enter the correct port number into the text entry box next to “TCP/UDP Port No.(1-65535)”.
4. After you have finished configuring just one ACL Access List from the previous step, you must now create a name for the new ACL Class Map that will be associated with this Access List. To do this, just enter a name for the new ACL Class Map into the text box under **Class Name** (see Figure 76).

Note: Since this particular Access List type does not contain any deny rules, this Access List will have to be used in conjunction with another type of Access List, if you wish to filter any packet from entry to the switch that did not match the classification rules from this Access Lists. Otherwise all packets that did not match the classification rules of this Access List will also be allowed entry into the switch.

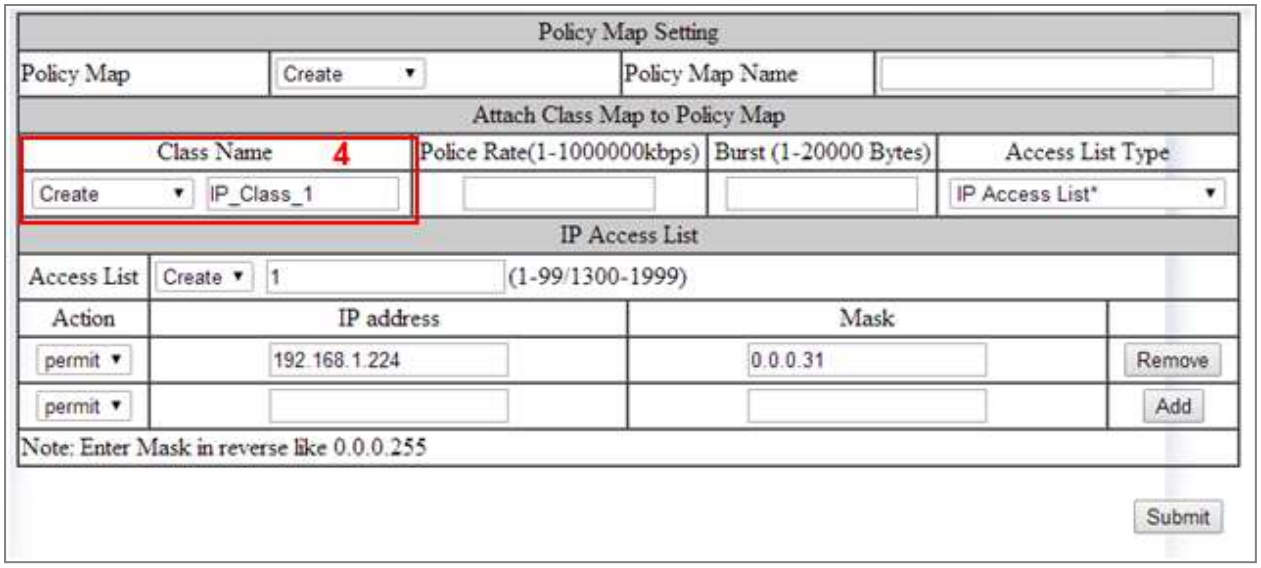


Figure 76: IP Access List Name

Bandwidth Limiting

1. The amount of bandwidth that is being allocated for the traffic that is being allowed under this new ACL Class can also be limited. To do this, enter the bandwidth amount that you want to allocate for the traffic in the text entry boxes in the Attach Class Map to Policy Map section (see Figure 77).

   Update the following text entries:

   - Committed Information Rate (1-1000000 kbps)
   - Peak Information Rate(1-1000000kbps)
   - Committed Burst (1-20000 bytes)
   - Peak Burst (1-20000bytes)

Note: The Peak rates must be higher than the Committed Rate. Current firmware discards any packets that exceed the Committed Rate

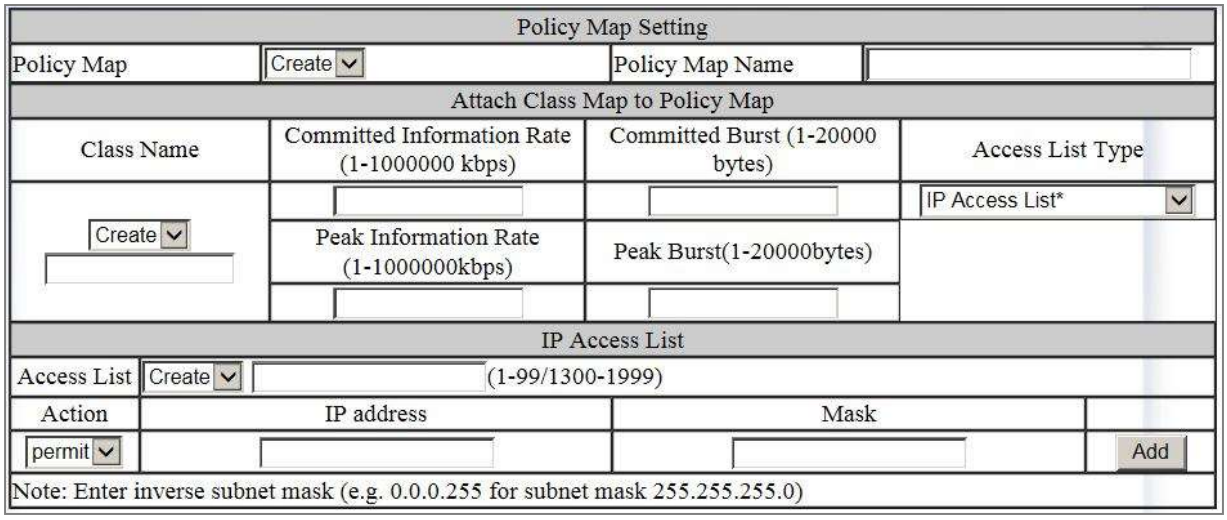


Figure 77: ACL Configuration

2. Next, please enter a name in the text entry box next to “Policy Map Name” for the new ACL “Policy Map” that you are currently creating, and click on the submit button (see Figure 78).

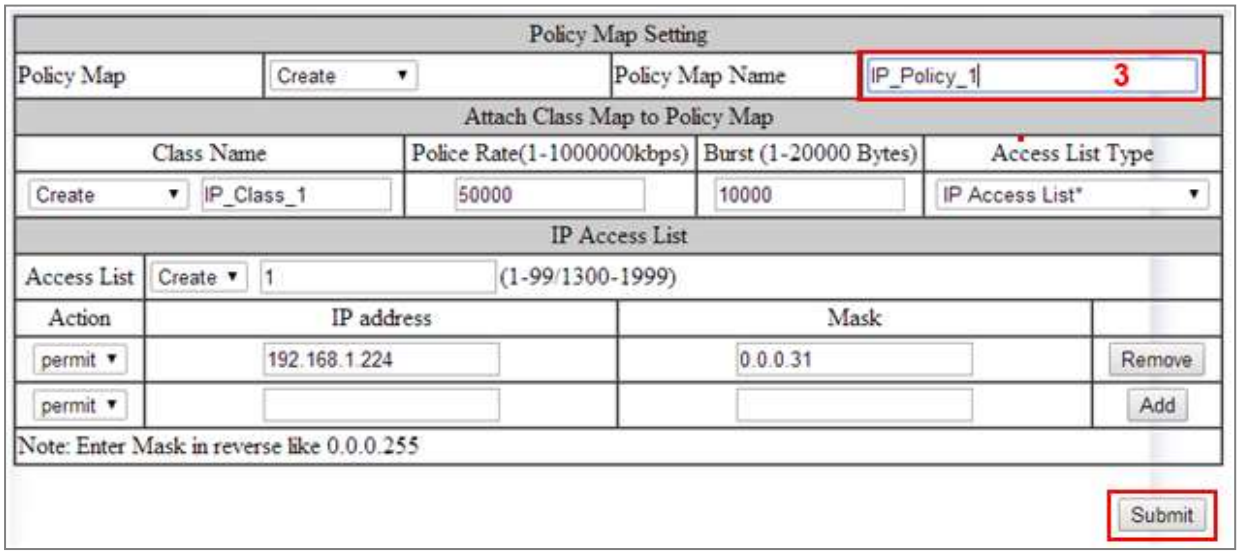


Figure 78: Policy Map Name

Applying a Policy Map to a Port

To apply an ACL **Policy Map** to a port:

1. Select the correct ACL **Policy Map** from the drop-down list next to **Policy Map** (see Figure 79).
2. Next, check the boxes below **Attach Class Map to Policy Map** next to all the ports that you would like to apply this Policy Map to.
3. Click on the **Attach** button.

Figure 79: Applying a Policy Map to a Port

Modifying/Adding an Existing Policy Map

To modify or add to an existing ACL **Policy Map**, just follow the instructions below.

1. Select the correct ACL **Policy Map** from the drop-down list next to **Policy Map** (see Figure 80)
2. Next, detach the Policy Map from all the ports by deselecting the check boxes below **Attach Class Map to Policy Map** for the ports you would like to remove the policy map.
3. Click on the **Attach** button.

Figure 80: Modifying a Policy Map

Adding a New ACL Class to an Existing Policy Map

If you would like to create a new ACL Class and add it to this ACL Policy Map follow the steps below

1. Make sure that the **Create** option is selected from the drop-down list under **Class Name** (see Figure 81)

2. ACL Policy Map Next, follow the instructions on how to create a new on page 121.

3. Next, click on the **Submit** button.

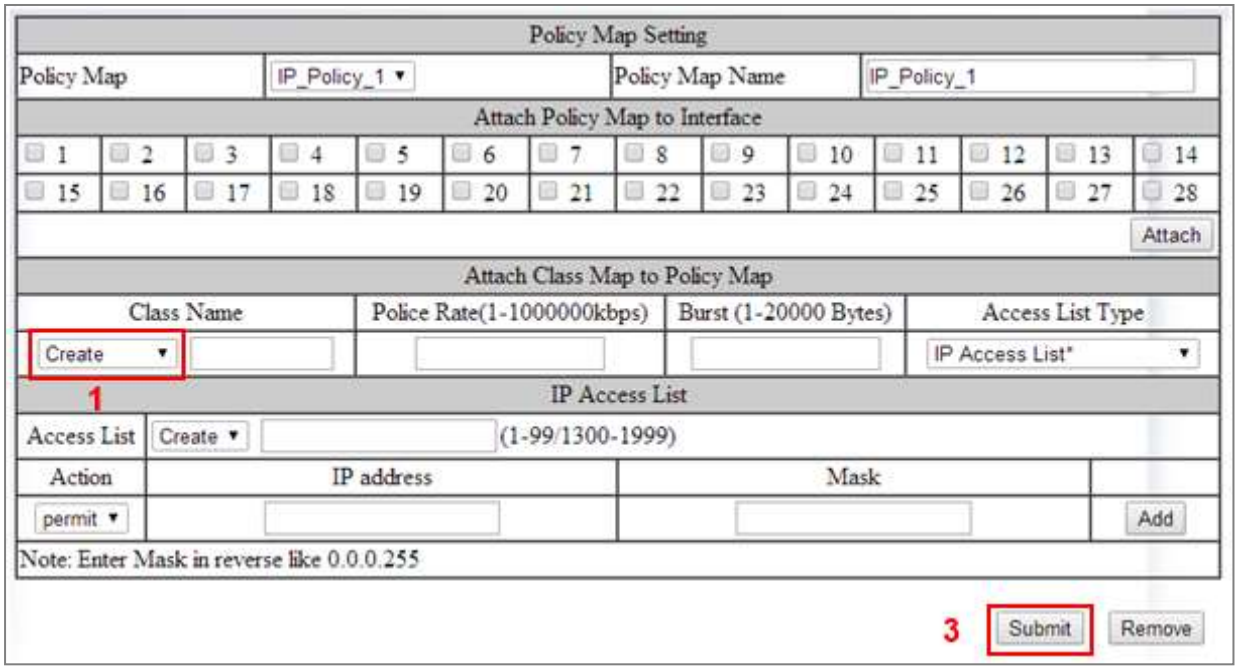


Figure 81: Adding a New ACL Class to an Existing Policy Map

Adding an Existing ACL Class to an Existing Policy Map

If you would like to add an existing ACL Class to this ACL Policy Map (see Figure 82):

1. Select the correct ACL Class from the drop-down list under **Class Name**, and then wait for the GUI to update itself.
2. Click on the **Submit** button.

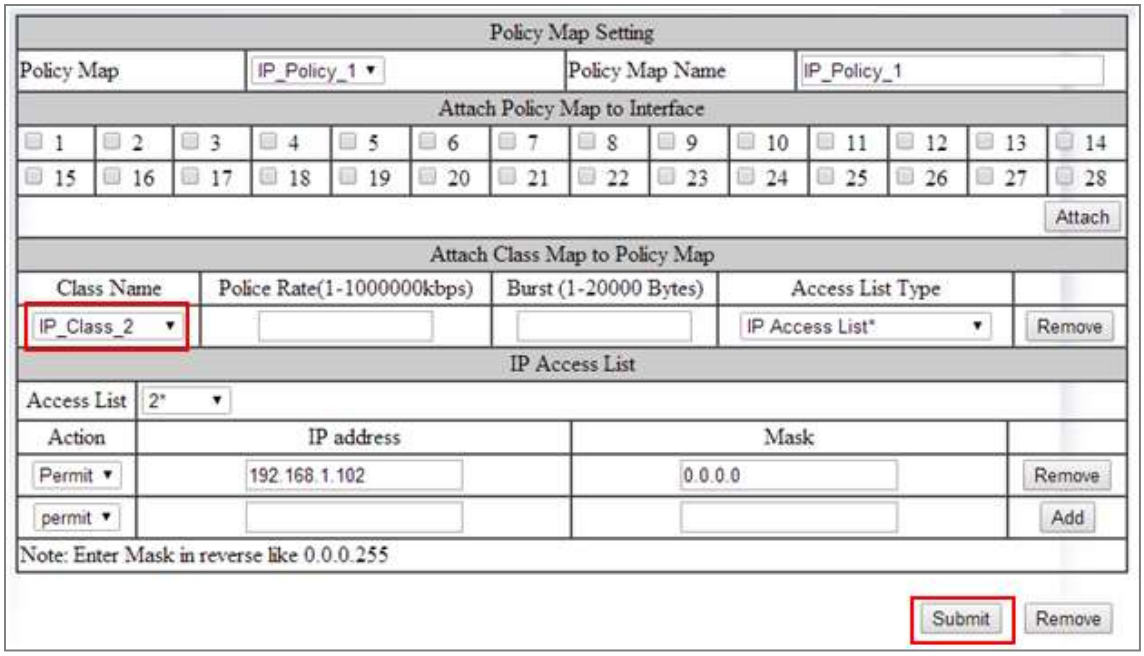


Figure 82: Policy Map Setting – Class Name

3. You can confirm that the ACL Class has been added correctly to this Policy Map by checking the dropdown list under “Class Name”. If you see the newly added ACL Class in the list above the dash line, then it has been added properly (see below).

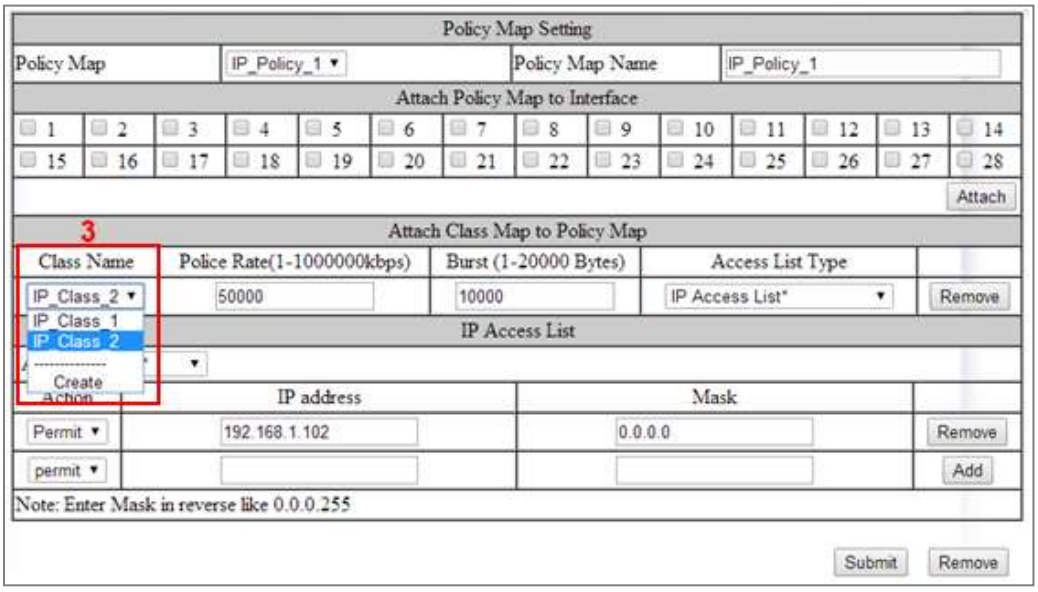


Figure 83: Policy Map Setting

Removing an ACL Class

If you would like to remove an ACL Class from this ACL Policy Map:

1. Make sure to select the correct ACL Class that is above the dash line from the drop-down list under **Class Name** (see Figure 84).

2. Next, click on the **Remove** button under **Attach Class Map to Policy Map**.

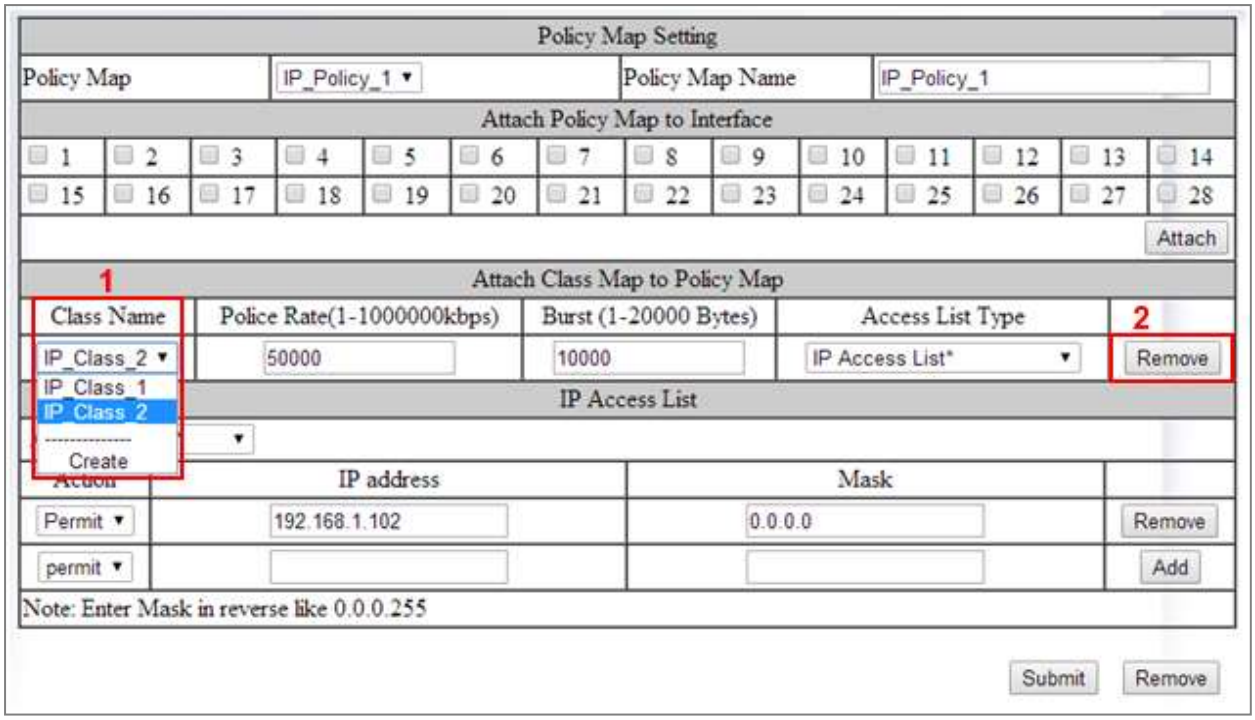


Figure 84: Removing an ACL Class

3. You can confirm that the ACL Class has been removed from this Policy Map by checking the dropdown list under **Class Name**. If you do not see the ACL Class in the list above the dash line, but see it below the dash line, then it means it has been removed from this Policy Map (see Figure 85).

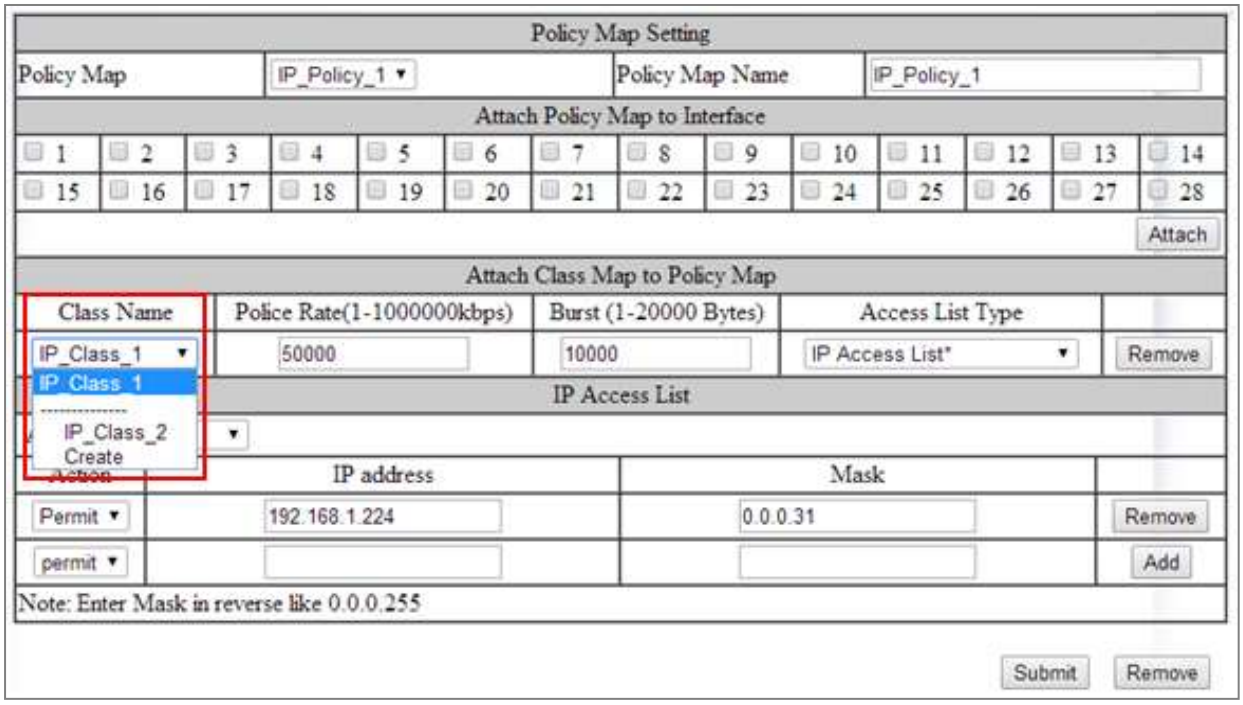


Figure 85: Verifying ACL Class Removal

To remove an existing ACL Policy Map entirely, follow the instructions below:

1. Select the correct ACL **Policy Map** that you want to remove entirely, from the drop-down list next to **Policy Map** (see Figure 86)
2. Next, detach the Policy Map from all the ports by deselecting all the check boxes below **Attach Class Map to Policy Map** for all the selected ports,
3. Click on the **Attach** button.
4. Next, click on the **Remove** button.

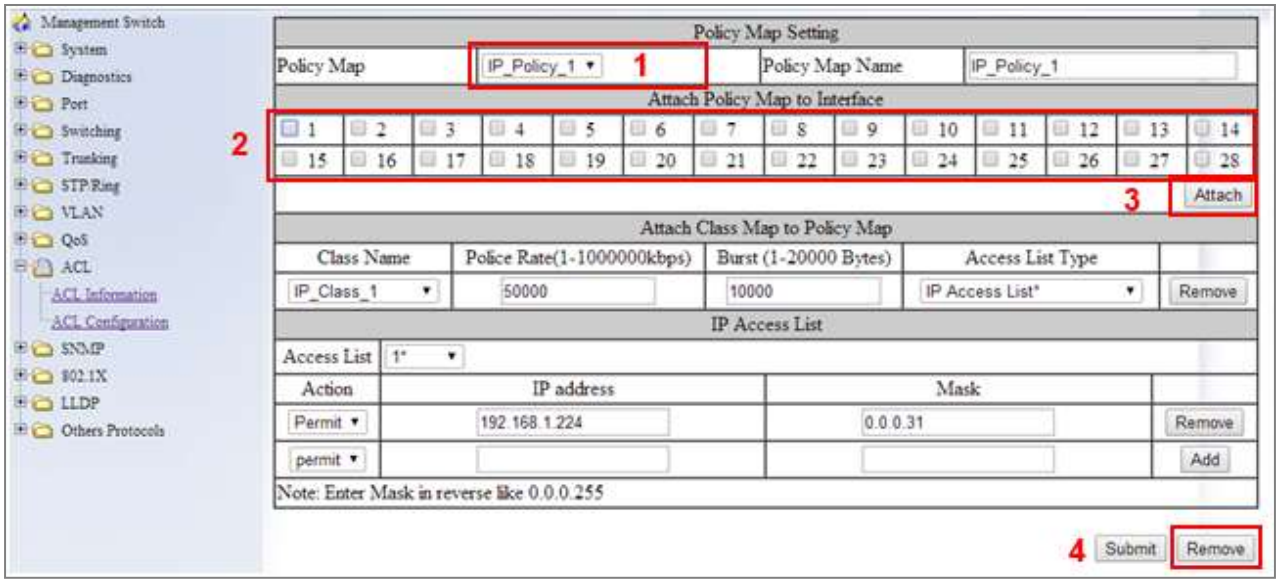


Figure 86: Removing a Policy Map

To remove an existing ACL Class entirely, follow the instructions below.

1. Make sure that the ACL **Class** is not associated with any ACL Policy Map. If it is, you must remove it from that Policy Map first (see Modifying/Adding an Existing Policy Map).
2. Next, make sure that the **Create** option is selected from the drop-down list next to **Policy Map** (see Figure 87).
3. Next, select the correct ACL Class from the drop-down list under **Class Name**, and then wait for the GUI to update itself.
4. Next, click on the **Remove** button under **Attach Class Map to Policy Map**

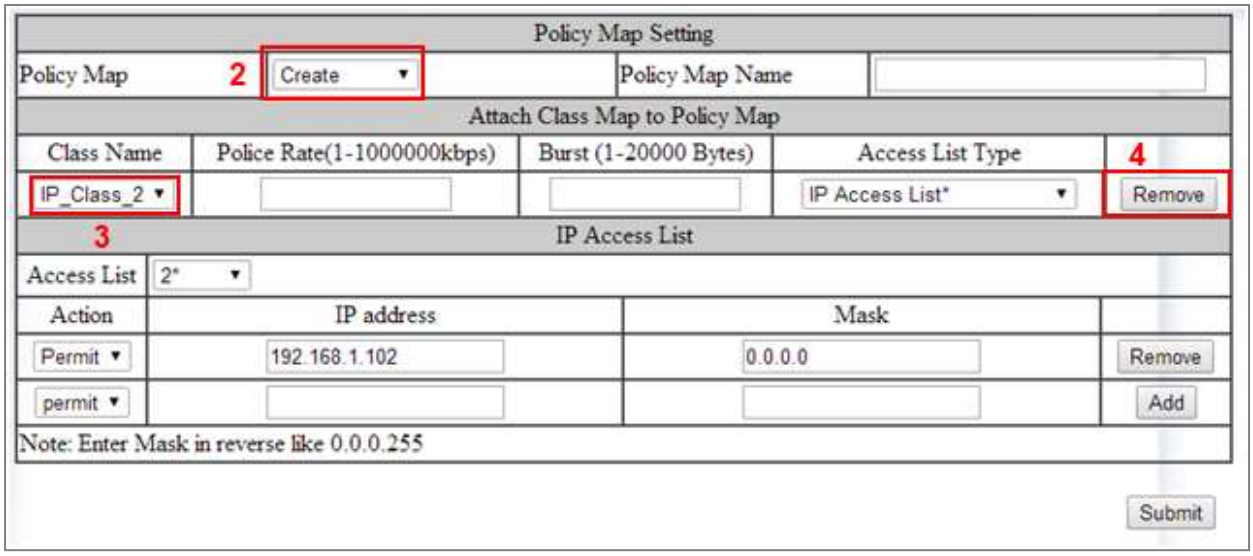


Figure 87: Policy Map 2

5. You can confirm that this ACL Class has been removed completely by checking the drop-down list under “Class Name”. If you do not see the ACL Class in the list then it means it has been completely removed (see below).

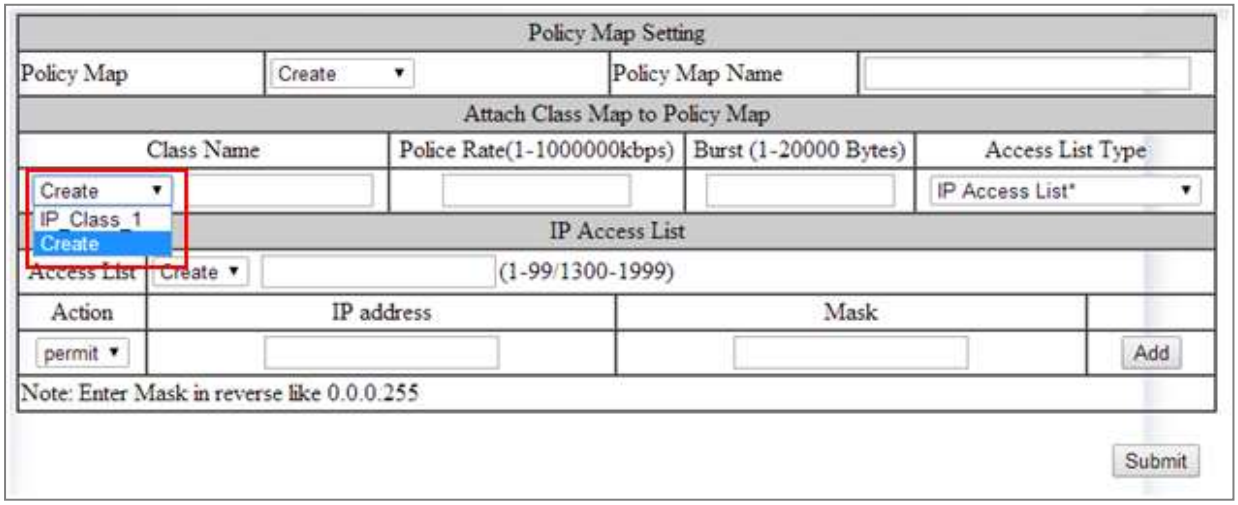


Figure 88: Policy Map 3

ACL Configuration Examples Using CLI Commands

Enabling QoS

To enable the ACL feature on the EtherWAN switch by enabling the QoS feature on the switch, just follow the steps below:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **mls qos enable**

Usage Example:

```
switch_a(config)# mls qos enable
```

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(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
```

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(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
```

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(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
```

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(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
```

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(config)#class-map Layer_2-3_Class
switch_a(config-cmap)#match access-group 1
```

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) #class IP_Class_1
switch_a(config-cmap)#policy-map IP_Policy_1
switch_a(config-pmap)#class IP_Class_1
switch_a(config-pmap-c)# police 50000 5000 5000 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 5000 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 5000 5000 exceed-
action drop
```

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(config)#interface fe1
switch_a(config-if)#service-policy input IP_Policy_1
```

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(config)#no class-map IP_Class_1
```

Deleting an ACL Policy

You can use the below CLI commands to delete an existing ACL Policy:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **no policy-map <*ACL Policy Name*>**

Usage Example:

```
switch_a(config)#no policy-map IP_Policy_1
```

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.

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 89):

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. Enter a short description (up to 256 characters) into the text entry box next to Description, for the purpose of switch identification.

3. Enter a name into the text entry box next to Location, for the purpose of identifying the location of the switch.
4. Enter a name (up to 256 characters) into the text entry box 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 text entry box 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 text entry box 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 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.
10. 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 text entry box next to **MAC Notification Interval (1 to 65535 seconds)**.
11. 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 text entry box next to **MAC Notification History Size (1 to 500)**.
12. 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.

13. 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.

14. Click on the **Update** button after you have finished the configuration of the SNMP Server (Agent) General Settings.

15. Save the configuration (see the Save Configuration Page)

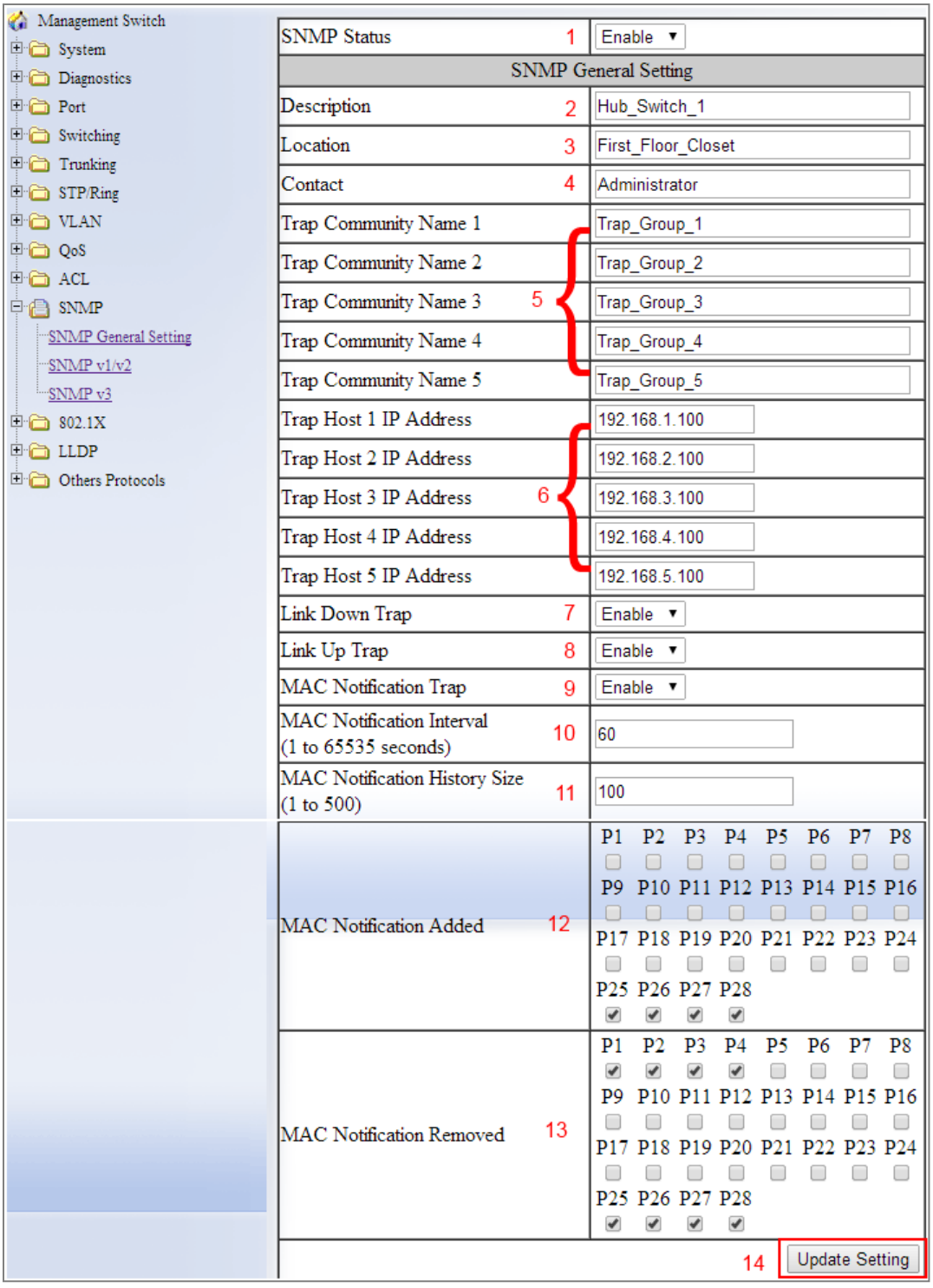


Figure 89: SNMP General Settings

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 90):

1. Enter the SNMP community name into the text entry box next to **Get Community Name**. This will allow the NMS to poll status information from the switch (read only).
2. Enter the SNMP community name, into the text entry box 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)

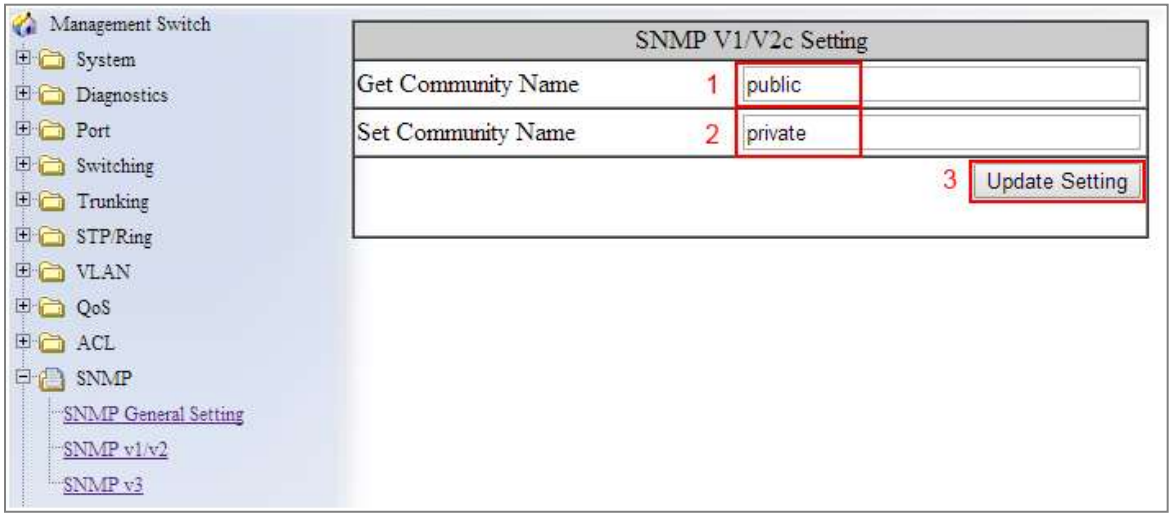


Figure 90: Community Name V1/V2c

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. See below.

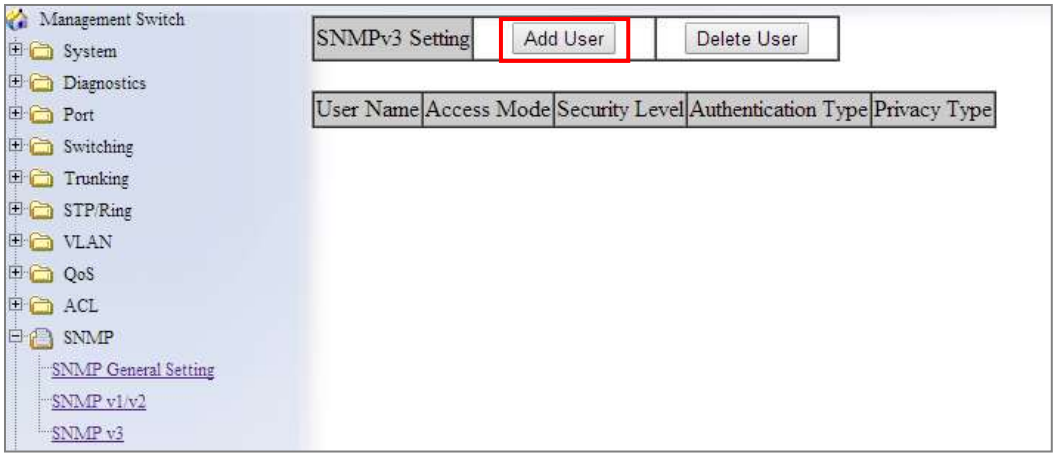


Figure 91: Add User

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 92):

   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 56-bit DES 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 56-bit DES encryption algorithm.

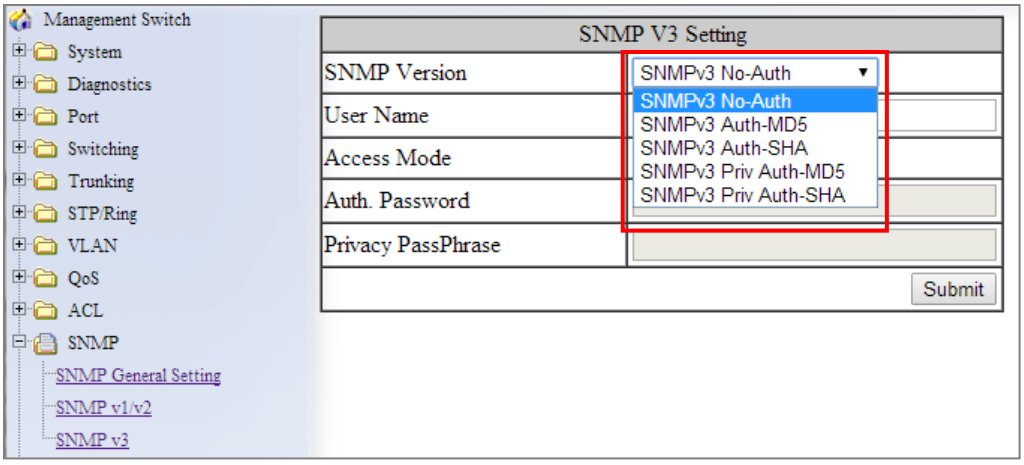


Figure 92: SNMP v3 Settings

3. Next, enter the desired username in the text entry box next to **User Name**.
4. Next, please select the desired access authorization for the user from the drop-down list next to **Access Mode**. See Figure 93.

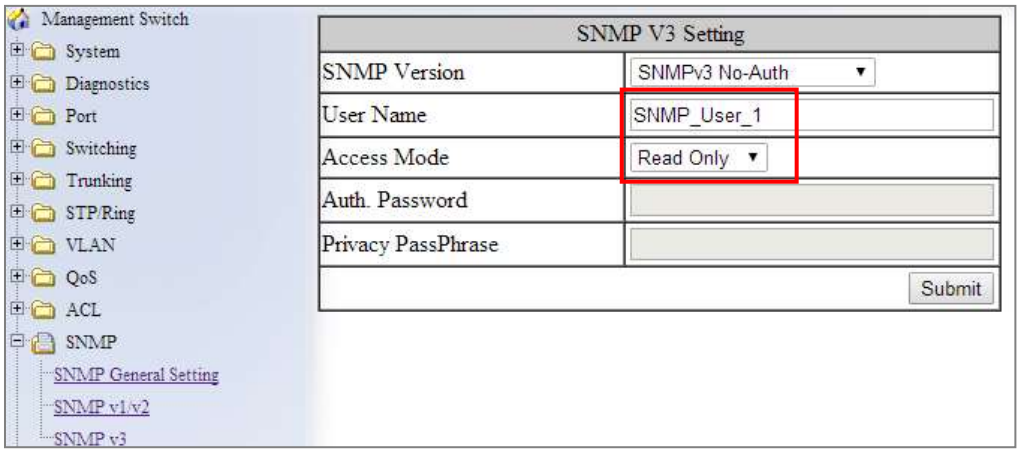


Figure 93: User name & Access Mode

5. Next, if authentication is required for this user, and you have chosen an authentication protocol, then the text entry box next to **Auth. Password** will have been enabled. Enter a password for this user inside this text entry box. See Figure 94.

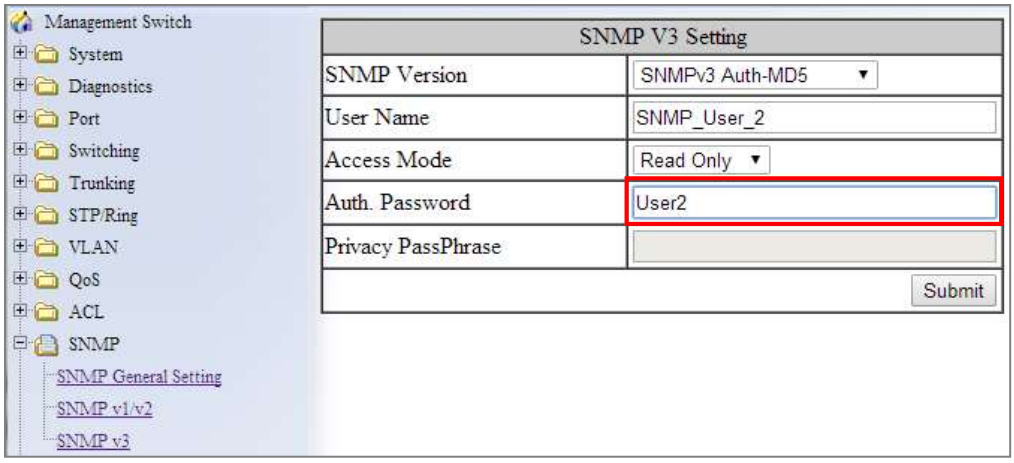


Figure 94: Auth Password

6. Next, if both authentication and privacy are required for this user, and you have chosen both an authentication and privacy protocol, then the text entry box next to **Privacy PassPhrase** will have been enabled. Enter a pass phrase inside this text entry box, as part of the key used to encrypt the protocol message for this user. See Figure 95.

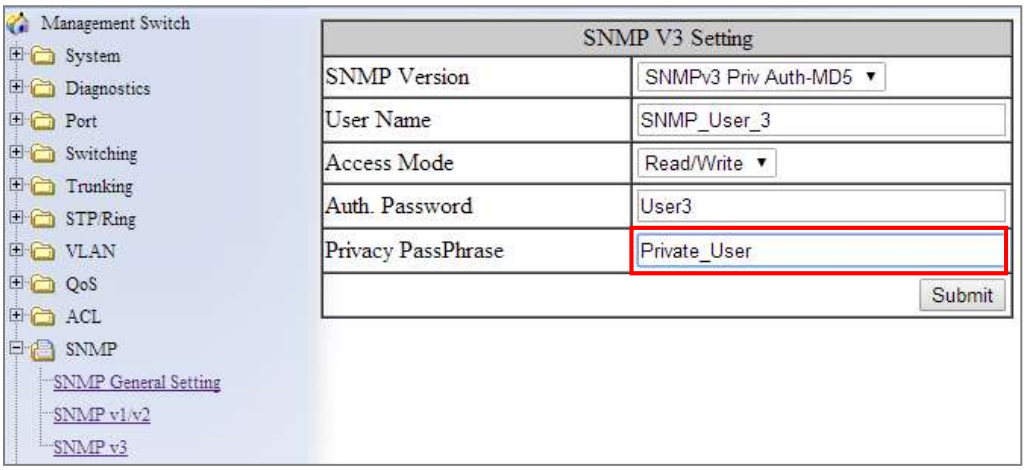


Figure 95: Privacy PassPhrase

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 below.

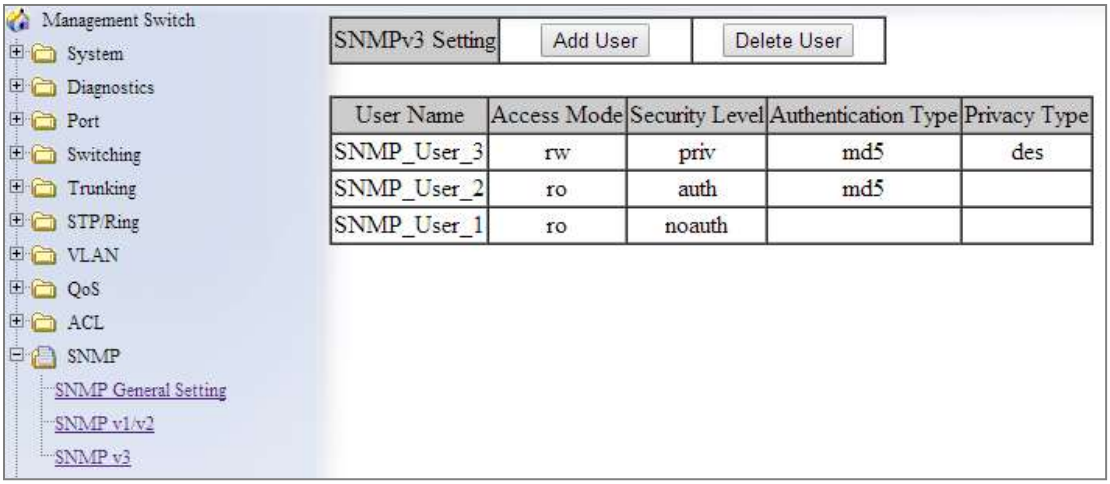


Figure 96: Delete User

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. See below.

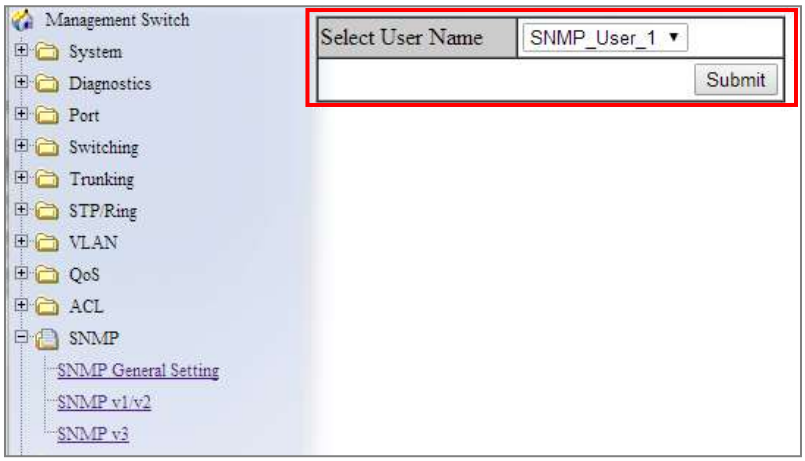


Figure 97: Select User

SNMP Configuration Examples 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), you must use the below 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(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
```

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(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 fe1
switch_a(config-if)#snmp-server trap mac-notification added
switch_a(config-if)#snmp-server trap mac-notification removed
```

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(config)# snmp-server community get public
switch_a(config)# snmp-server community set private
```

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(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
```

IEEE 802.1X

EtherWAN switches support the IEEE 802.1X protocol to provide port based security on a switch port against unauthorized access. In order for this protocol to work, two additional components are required; an EAP (Extensible Authentication Protocol) compatible RADIUS server to authenticate a client station that is trying to gain access to the network through a port on the switch, and an 802.1X client software (known as the “Supplicant” software) used on the end device to communicate with the RADIUS 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 RADIUS server, and will not allow any other traffic to pass. After the initial connection, the EtherWAN 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 sent the credentials to the EAP compatible RADIUS server that’s configured in the switch for the purpose of authenticating the end device. If the end device is successfully authenticated by the RADIUS server, the RADIUS server will sent an “Access-Accept” message to the switch; at this point

the EtherWAN switch will inform the Supplicant in the end device of the successful authentication and open up the port for all network traffic to pass.

Configuring 802.1X from the Web Interface

To navigate to the **802.1X / 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. If you want 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. Choose **enable** from the drop down list next to **Radius Status**
2. Click on the **Update Setting** button. (See Figure 98)

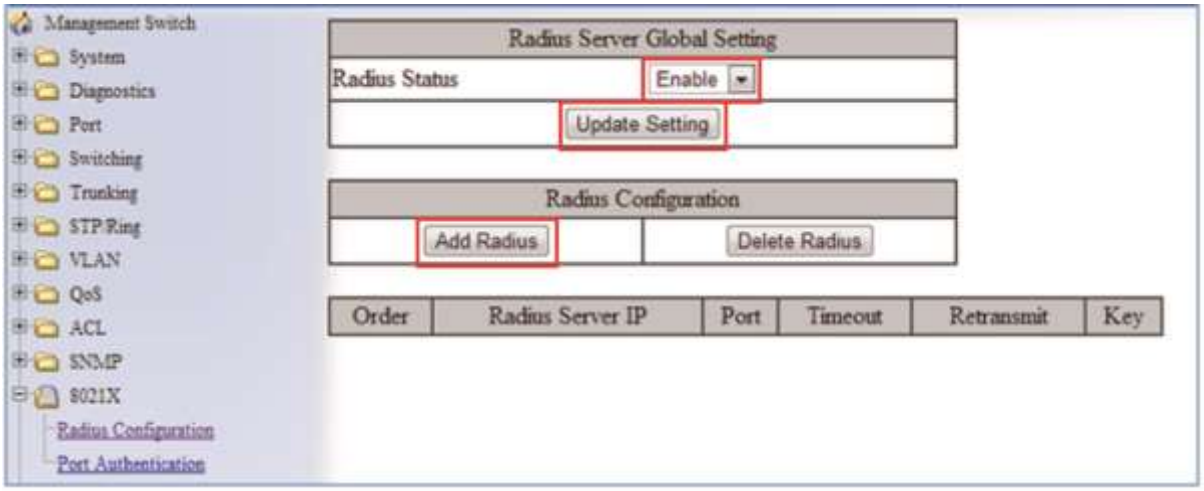


Figure 98: Enable Radius

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 above).

2. Next, enter the IP address of the RADIUS server that the switch will use in order to authenticate in the text entry box next to **Radius Server IP** (see Figure 99).

3. Enter the password for RADIUS server in the text entry box 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 text entry box 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 text entry box 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, please enter a number (from 1 to 100) into the text entry box next to **Retransmit**.

7. Click on the **Submit** button.

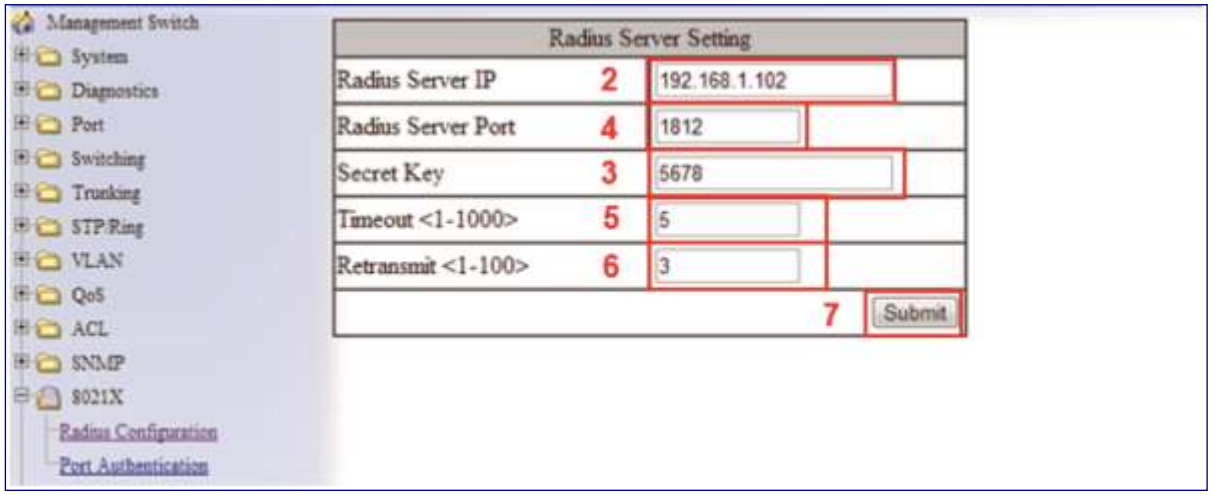


Figure 99: Radius Setup

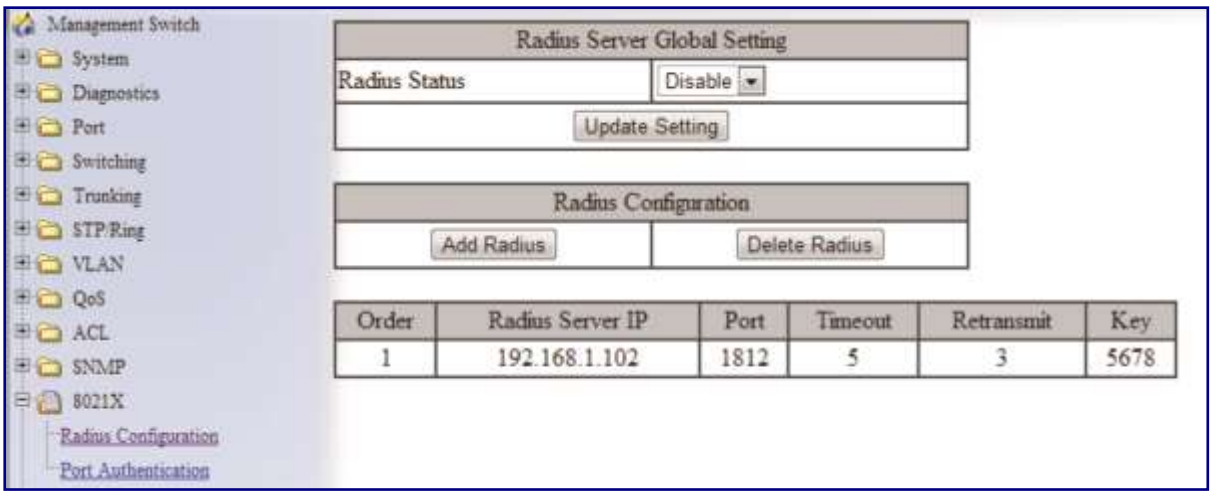


Figure 100: Resulting Radius Server Setup

Enabling 802.1X on a Port

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 101):

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 authentic 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), in to the text entry box next to **Re-authentication Period**.

6. Next, **Update Setting** button in order to activate all the configured settings (see the below screenshot)

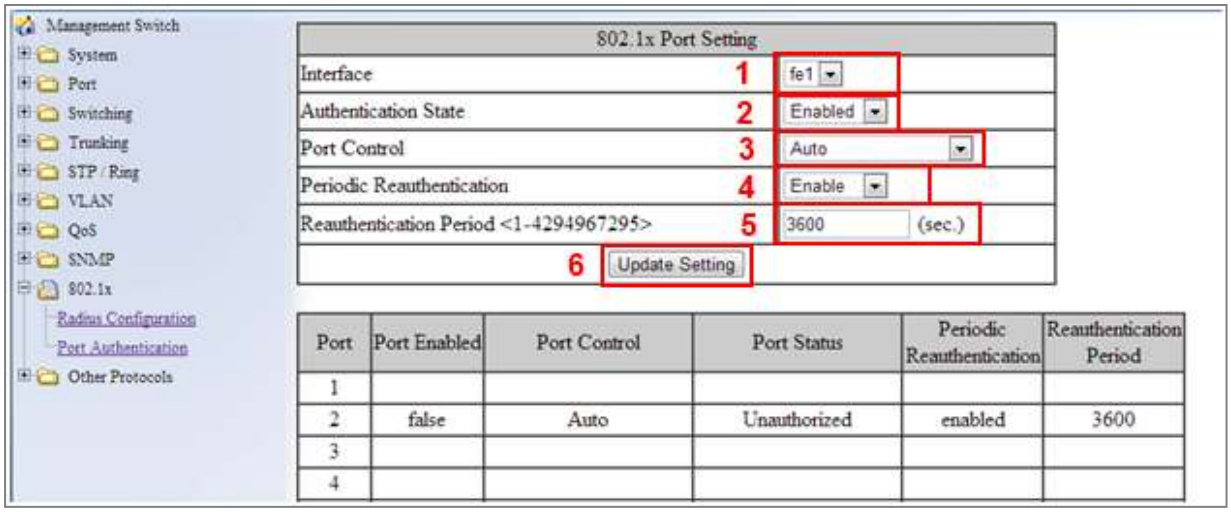


Figure 101: Enabling 802.1X on a Port

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 EtherWAN Managed Switch:

1. Select Enable or Disable from the Drop Down box in the **LLDP** field of the LLDP Transmit Settings box (see Figure 102)
2. Click on the **Update Settings** button.
3. Save the configuration (see the Save Configuration Page)

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 102):

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 EtherWAN Managed Switch are (see Figure 102):

- 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 EtherWAN Managed 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)

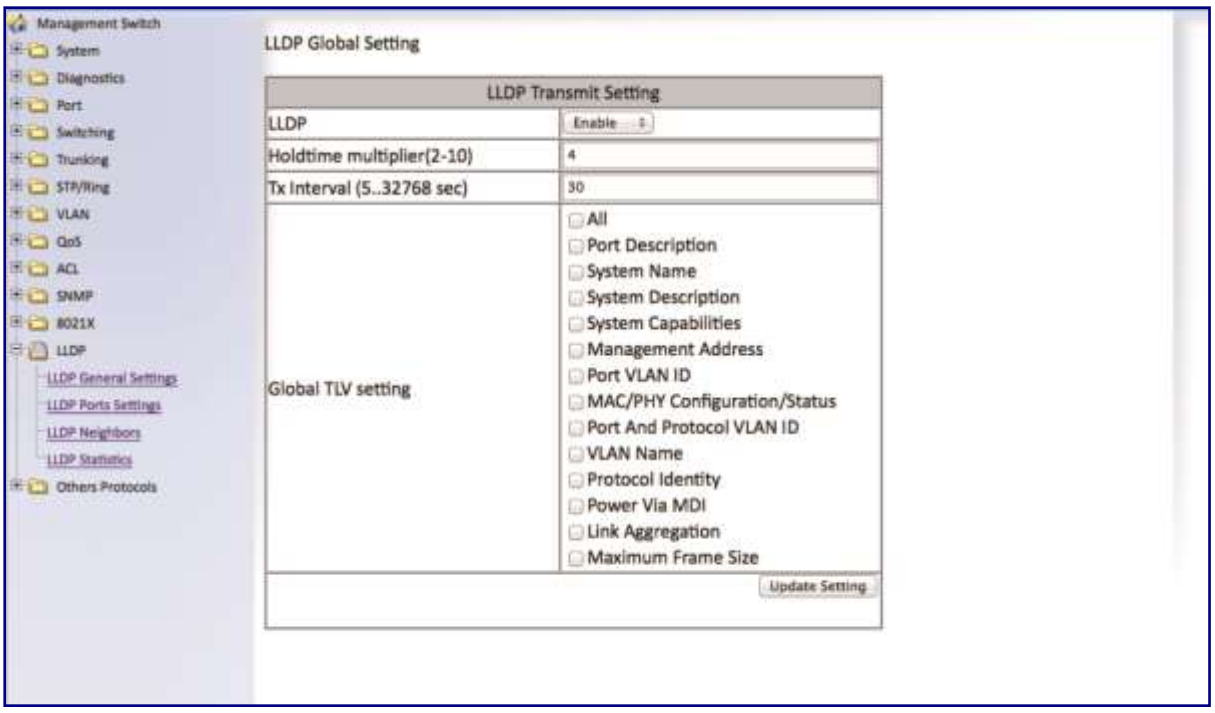


Figure 102: LLDP Global Settings

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 103)

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

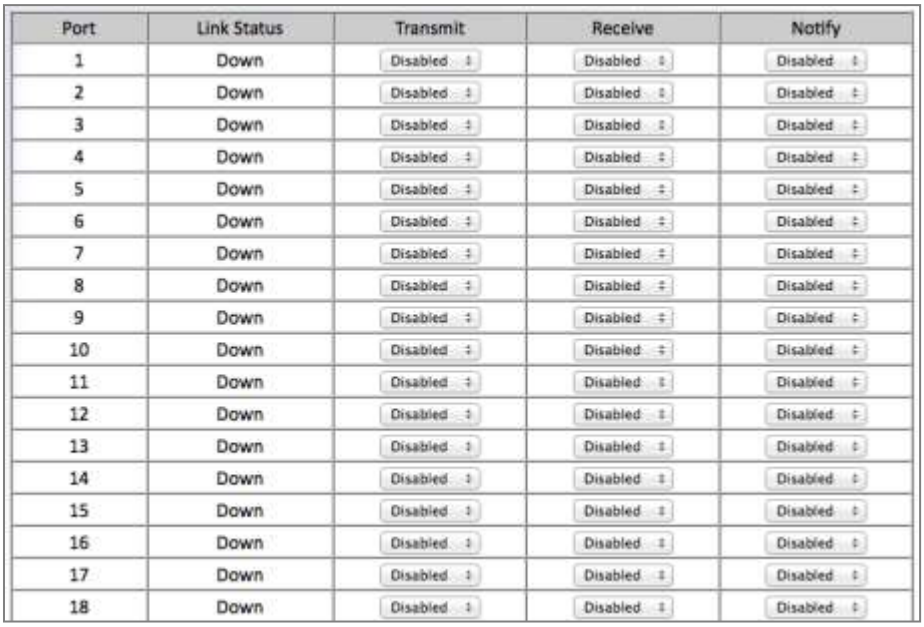
To enable the reception of LLDP information for a specific port:

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.



Port	Link Status	Transmit	Receive	Notify
1	Down	Disabled	Disabled	Disabled
2	Down	Disabled	Disabled	Disabled
3	Down	Disabled	Disabled	Disabled
4	Down	Disabled	Disabled	Disabled
5	Down	Disabled	Disabled	Disabled
6	Down	Disabled	Disabled	Disabled
7	Down	Disabled	Disabled	Disabled
8	Down	Disabled	Disabled	Disabled
9	Down	Disabled	Disabled	Disabled
10	Down	Disabled	Disabled	Disabled
11	Down	Disabled	Disabled	Disabled
12	Down	Disabled	Disabled	Disabled
13	Down	Disabled	Disabled	Disabled
14	Down	Disabled	Disabled	Disabled
15	Down	Disabled	Disabled	Disabled
16	Down	Disabled	Disabled	Disabled
17	Down	Disabled	Disabled	Disabled
18	Down	Disabled	Disabled	Disabled

Figure 103: LLDP Ports Settings

LLDP Neighbors

LLDP Neighbors is a read-only page (see Figure 104) 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.

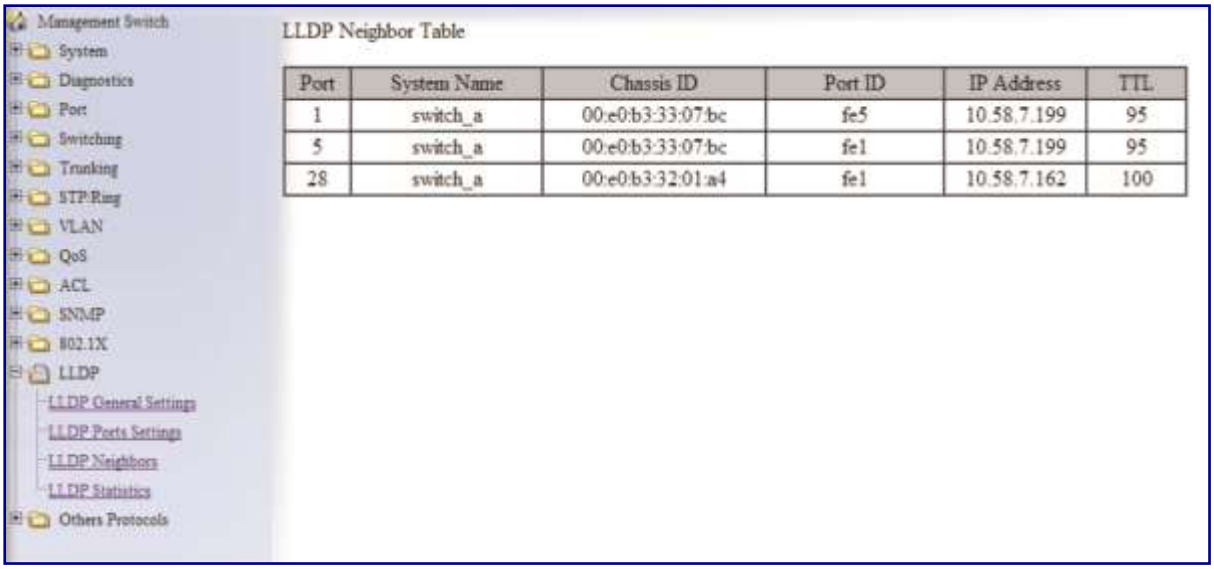


Figure 104: LLDP Neighbors

LLDP Statistics

This is a read-only page (see Figure 105) 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

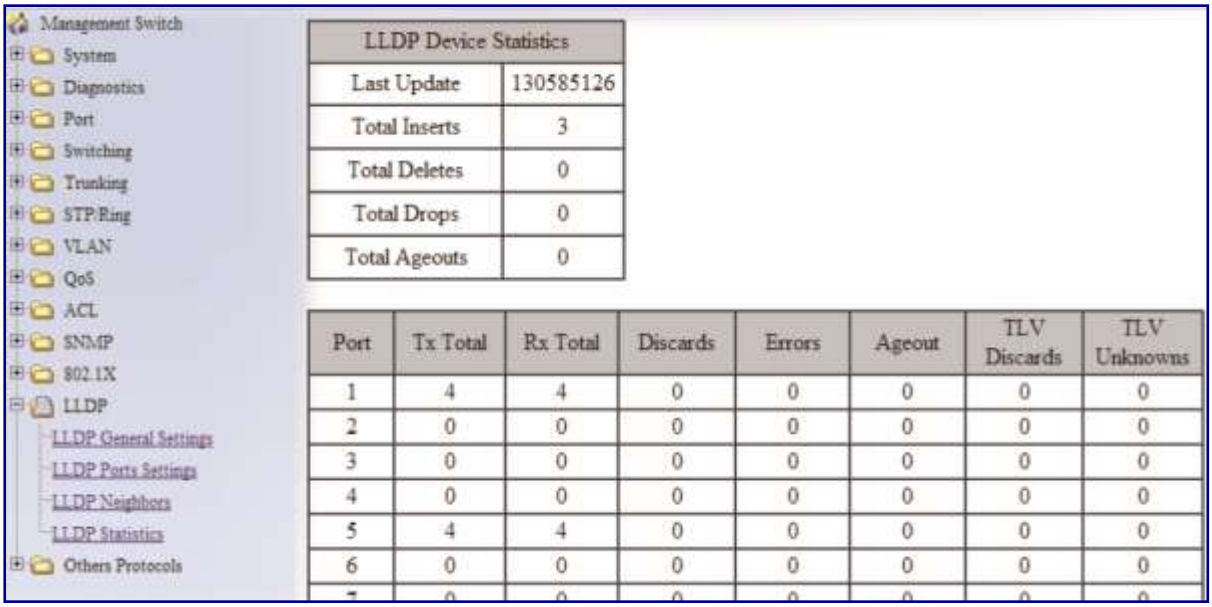


Figure 105: LLDP Statistics

LLDP Configuration Examples Using CLI Commands

Enable/Disable LLDP

To enable or disable LLDP on the EtherWAN Managed Switch use the CLI commands below:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax:
lldp enable
no lldp enable

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(config)#lldp holdtime multiplier 4
```

LLDP Transmit Interval

To modify LLDP Transmit Interval use the CLI commands below:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **lldp txinterval <*5-32768*>**

Usage Example: Set LLDP Transmit interval to 30 seconds

```
switch_a(config)# lldp txinterval 30
```

Enable/Disable Global LLDP TLVs

To enable or disable global LLDP TLVs use the CLI commands below:

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

Usage Example:

```
switch_a(config)# lldp tlv-global mgmt-addrs
```

Enabling LLDP Transmit on a Port

To enable LLDP Transmit for a port use the CLI commands below:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **lldp tx-pkt**

Usage Example:

```
switch_a(config)# lldp tx-pkt
```

Enabling LLDP Receive on a Port

To enable LLDP Receive for a port use the CLI commands below:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **lldp rcv-pkt**

Usage Example:

```
switch_a#interface fe1
switch_a(config)# lldp rcv-pkt
```

Enabling LLDP Notify

To enable LLDP Notify for a port use the CLI commands below:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **lldp notification**

Enabling Transmission of the Management IP

To enable the transmission of the management IP address through a port use the CLI commands below:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **lldp mgmt-ip vlan <*vlan id*>**

Usage Example:

```
switch_a(config)# lldp mgmt-ip vlan 1
```

Enabling Specific TLV's on a Port

To enable specific TLVs on a port use the CLI commands below:

CLI Command Mode: **Interface Configuration Mode**

CLI Command Syntax: **lldp tlv-select <TLV ID>** (see **TLV Parameters** on page 165)

Usage Example:

```
switch_a(config)# lldp tlv-select mgmt-addrs
```

OTHER PROTOCOLS

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 106):

1. Click on the **+** next to **Other Protocols**.
2. Click on **GVRP**.

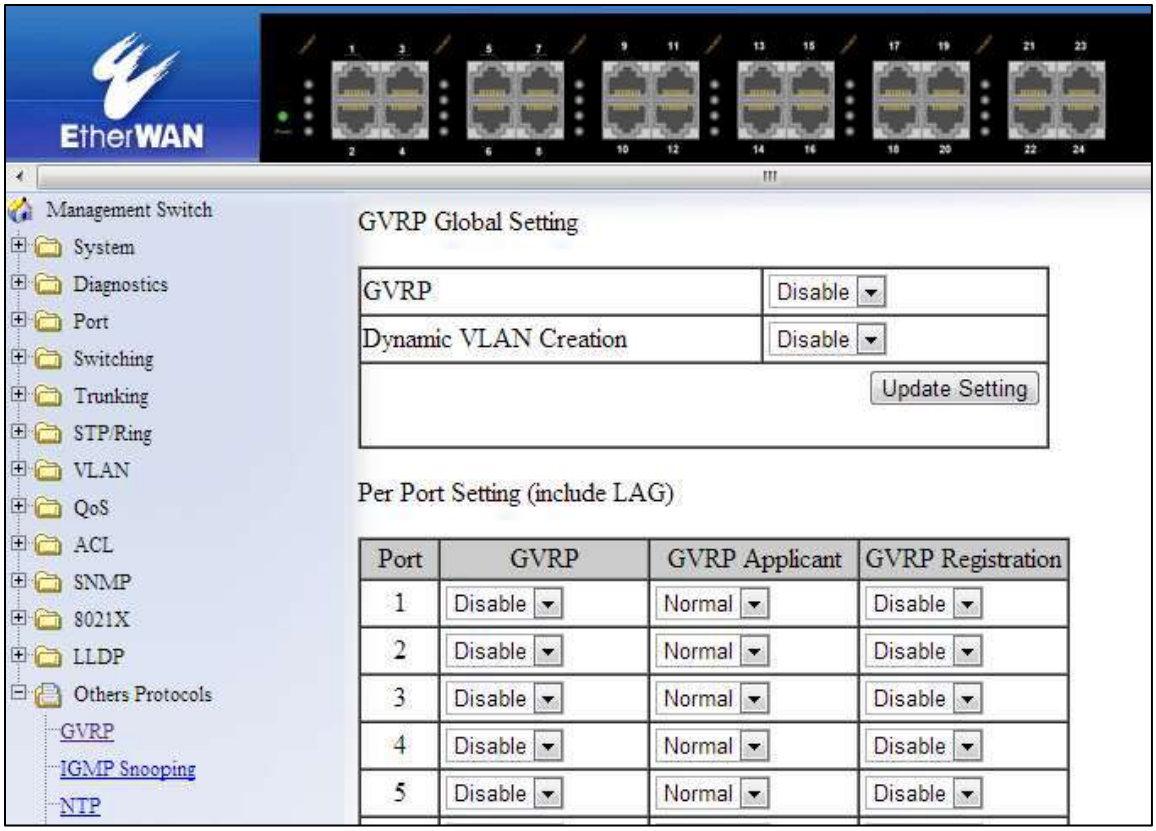


Figure 106: GVRP

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 107):

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.

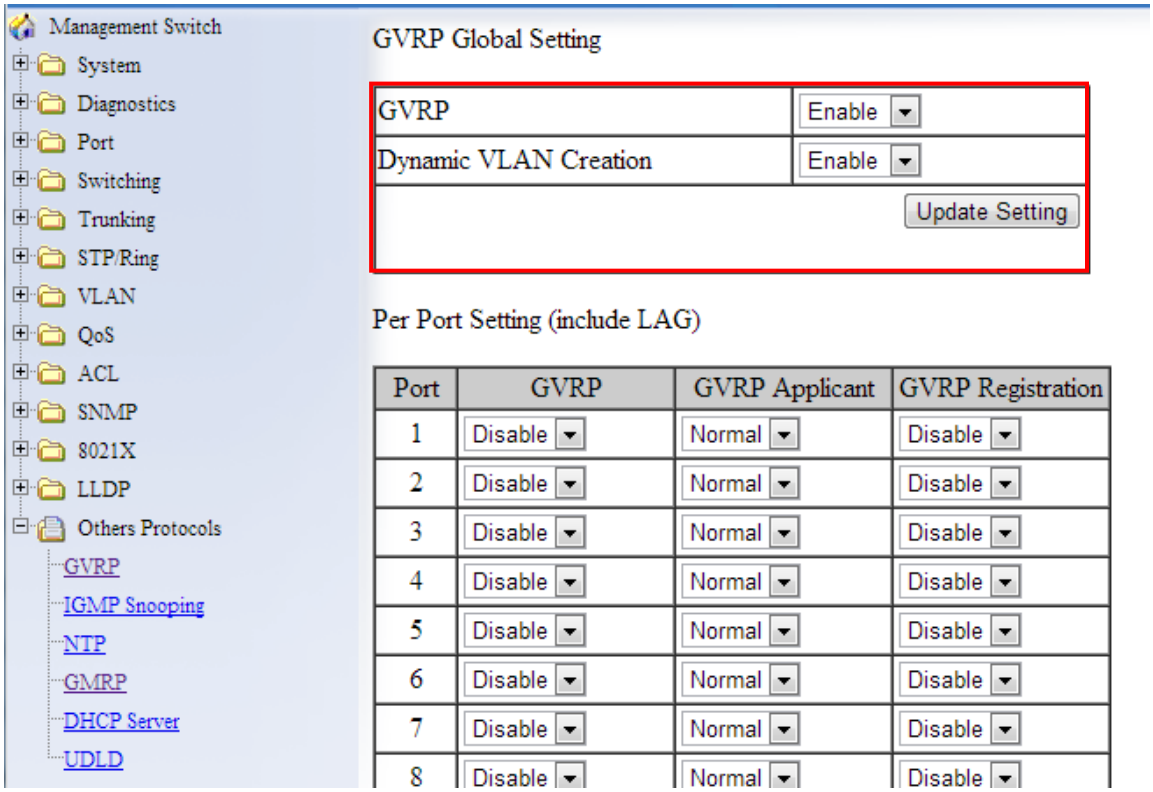


Figure 107: GVRP Configuration Distribution Switch

To enable the GVRP protocol globally on an **Access Switch** (see Figure 108):

1. Under **GVRP Global Setting**, choose the **Enable** option from the drop-down list next to **GVRP**.

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

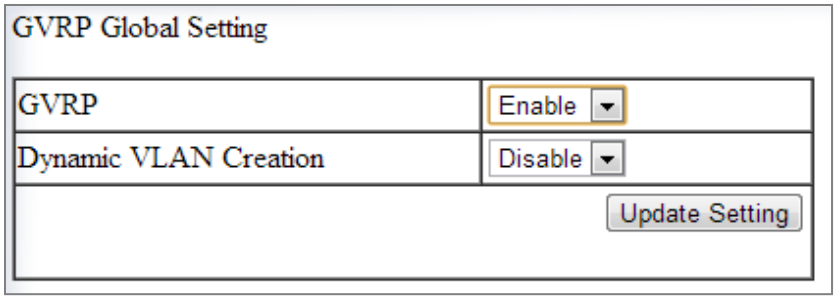


Figure 108: GVRP Configuration Access Switch

Enabling the GVRP Protocol at the Port Level

To navigate to the **Other Protocols / GVRP** page (see Figure 106):

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 the **Enable** option 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)

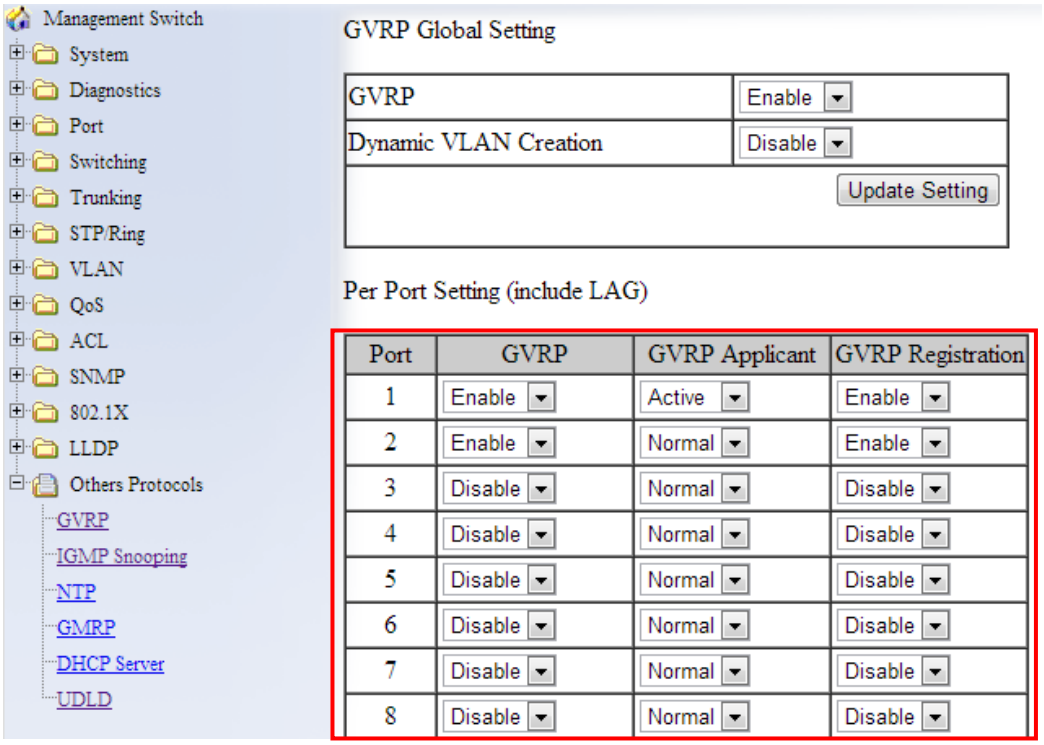


Figure 109: GVRP Per Port Settings

GVRP Configuration Examples Using CLI Commands

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 Examples:

```
switch_a(config)# set gvrp enable bridge 1
switch_a(config)# set gvrp disable bridge 1
```

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(config)# set gvrp dynamic-vlan-creation disable bridge 1
```

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 Examples:

```
switch_a(config)# set port gvrp enable fe1
switch_a(config)# set port gvrp disable fe1
```

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 Examples:

```
switch_a(config)# set gvrp applicant state normal fe1
switch_a(config)# set gvrp applicant state active fe1
```

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 Examples:

```
switch_a(config)# set gvrp registration normal fe1
switch_a(config)# set gvrp registration forbidden fe1
```

IGMP Snooping

The settings in the IGMP Snooping feature of the EtherWAN switch controls how the switch forwards multicast packets.

General Overview

The EtherWAN Managed 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 below)

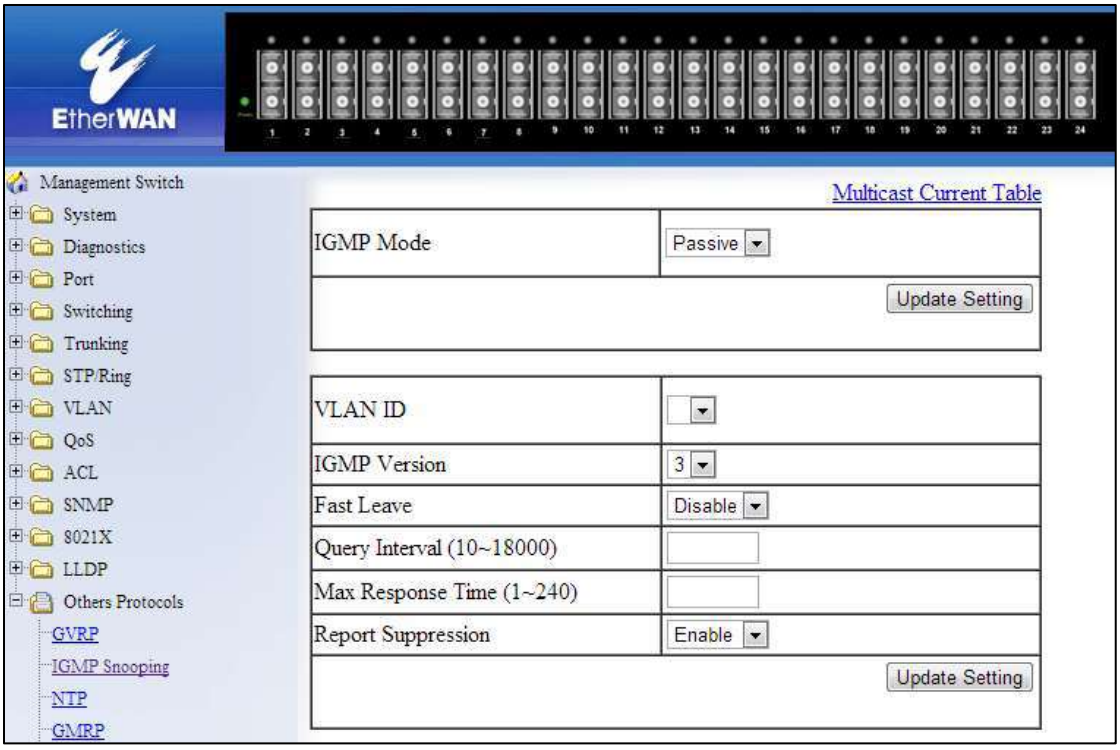


Figure 110: IGMP Mode

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 111):

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

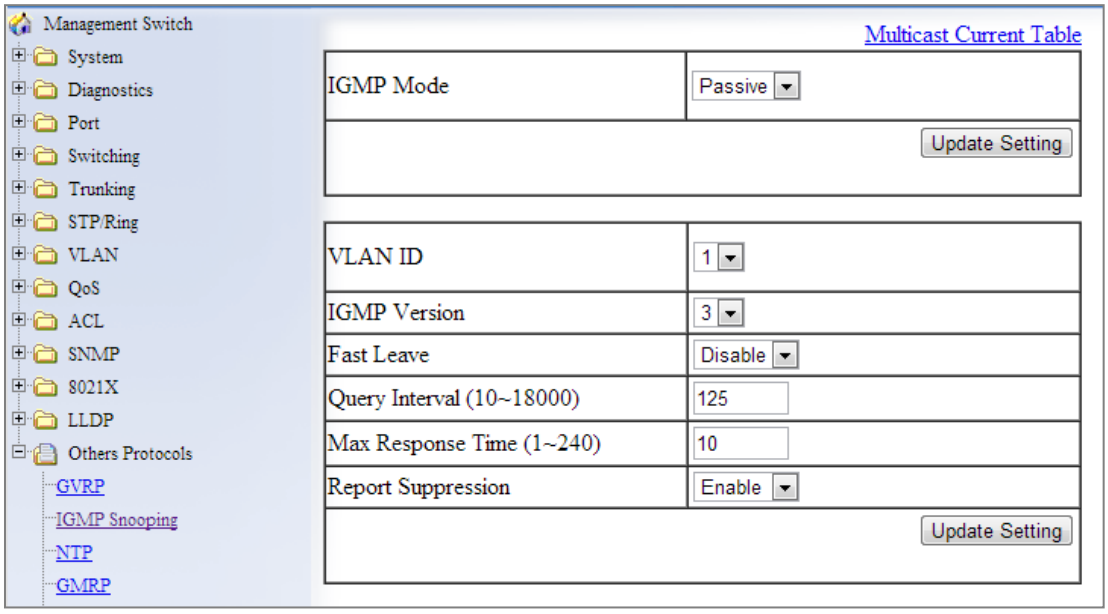


Figure 111: IGMP General Properties

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, please follow the steps below.

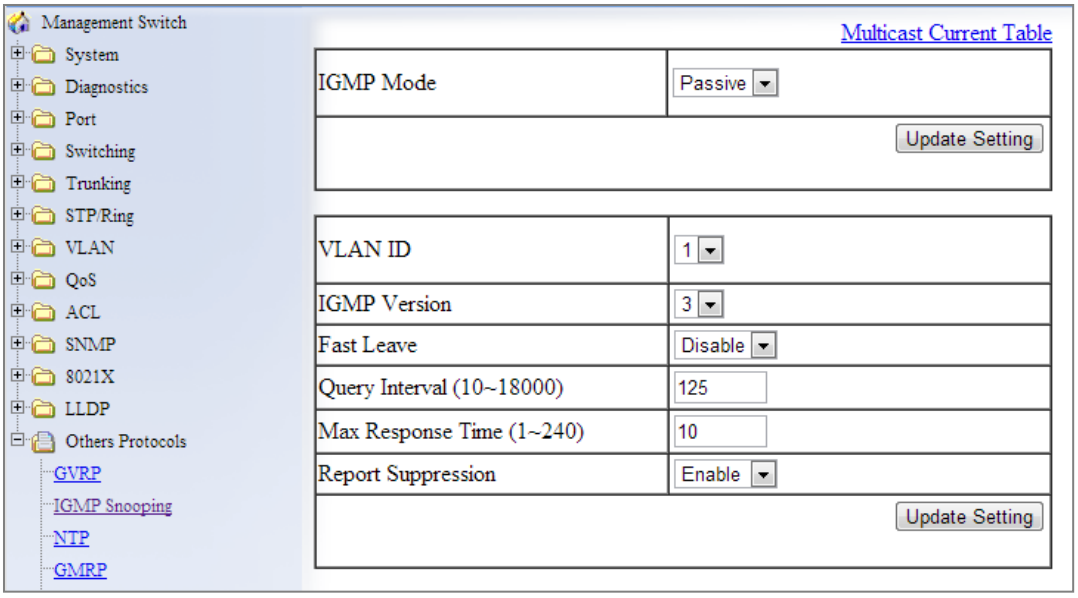


Figure 112: IGMP Passive Mode

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 113):

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.

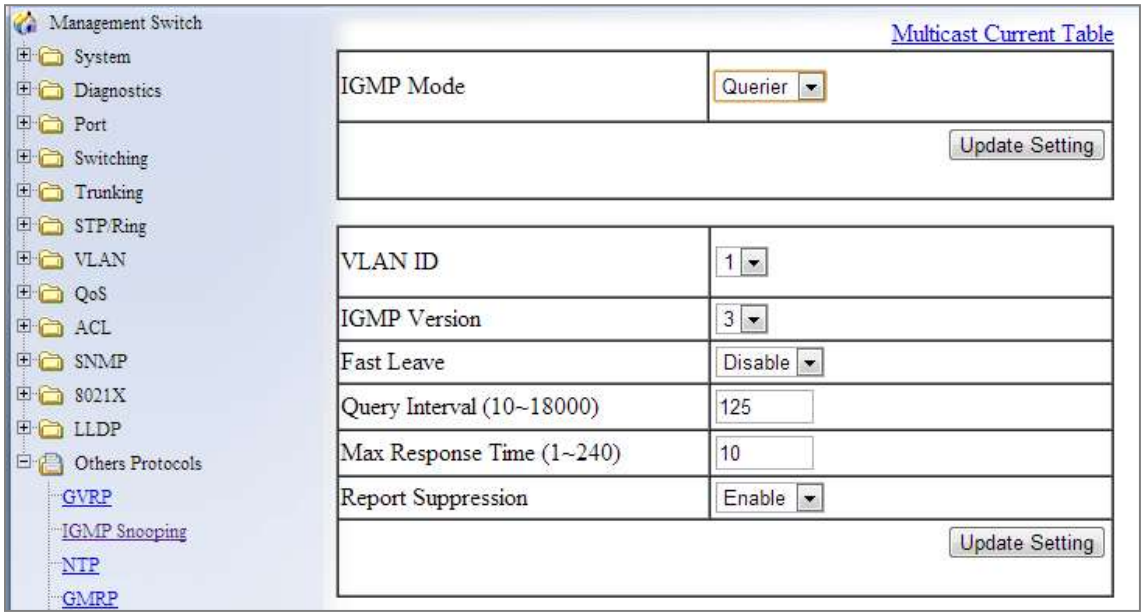


Figure 113: Querier Mode Properties

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 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 114).

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. Click on the **Update Setting** button.

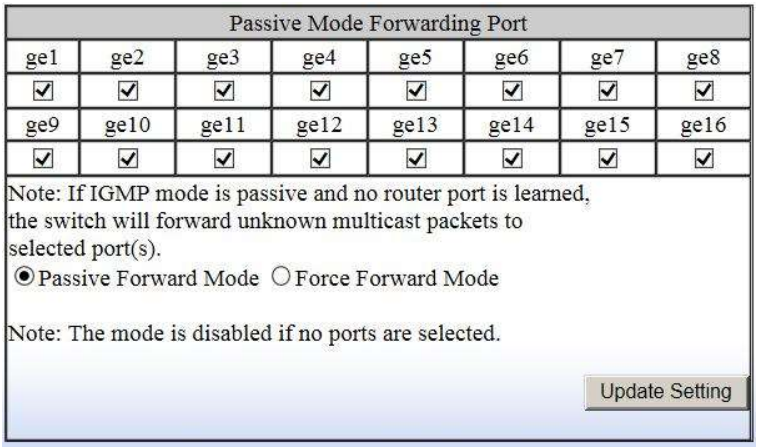


Figure 114: Disabled Mode Forwarding Port

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.

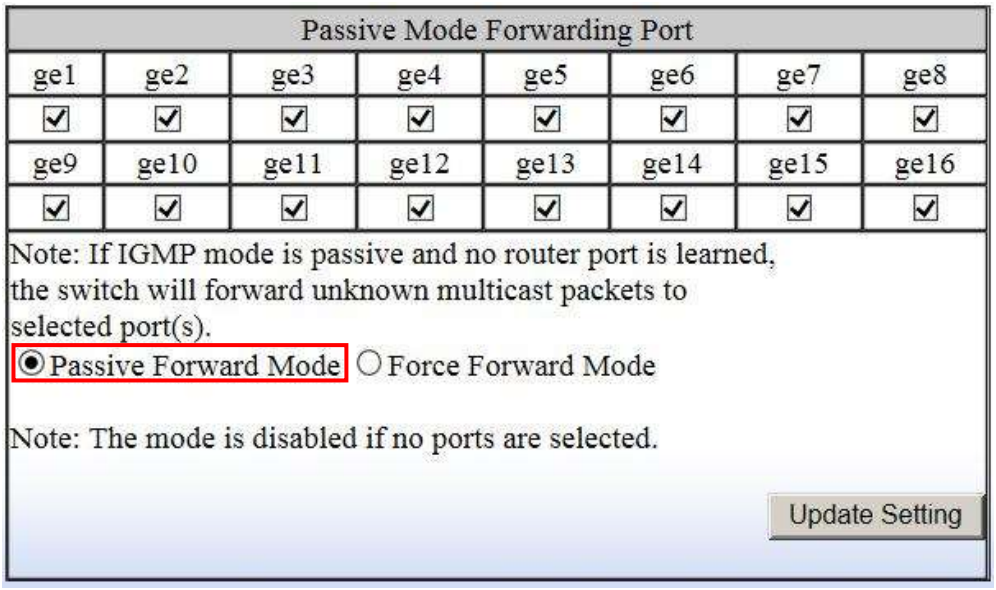


Figure 115: PassiveForwardMode

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.

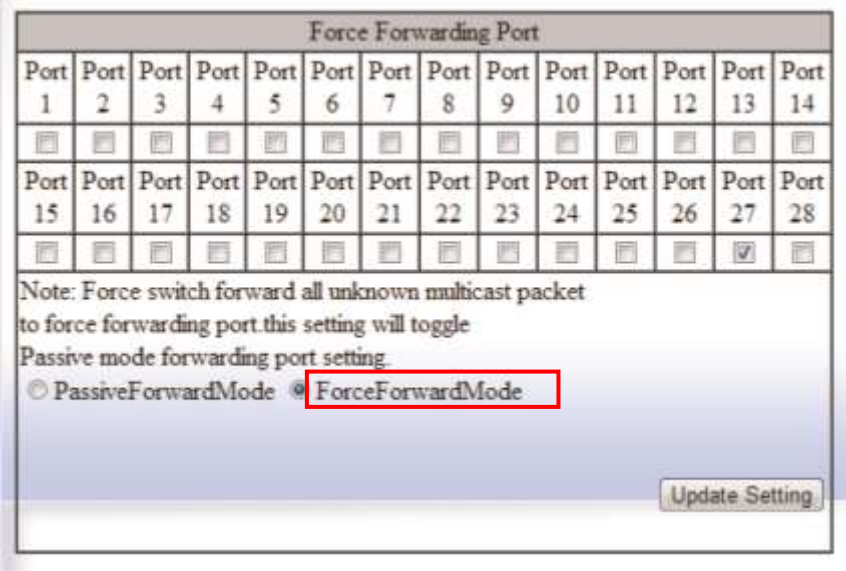


Figure 116: ForceForwardMode

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.

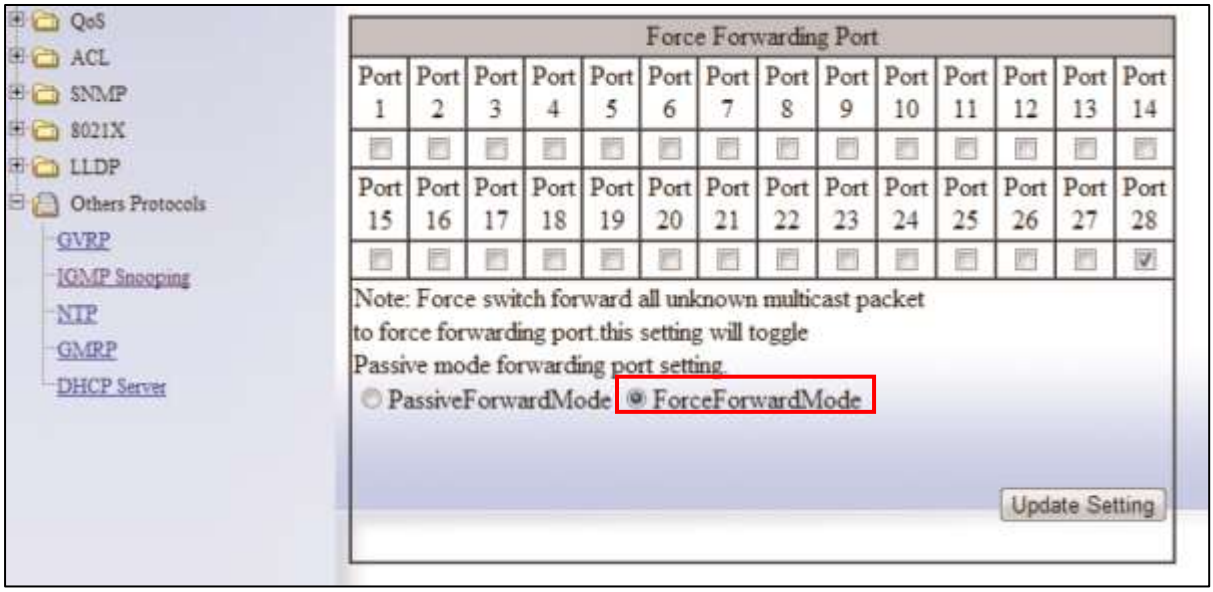


Figure 117: IGMP Querier Mode Forwarding

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 118).

- 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.

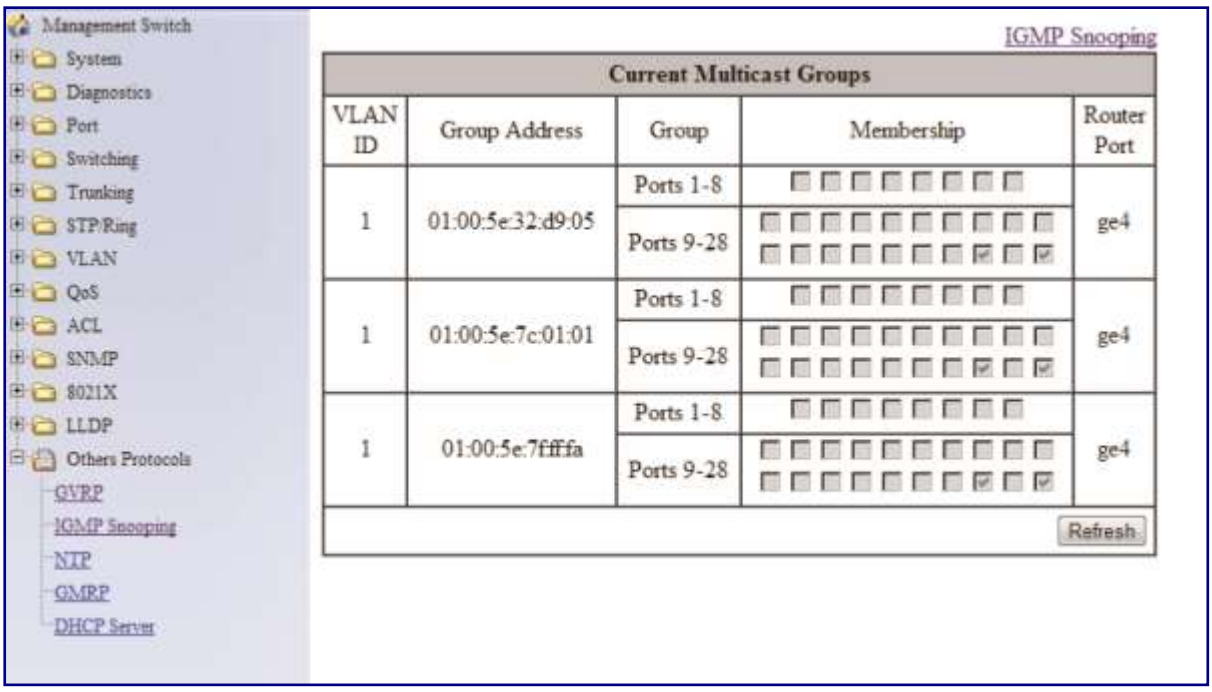


Figure 118: Current Multicast Groups

IGMP Configuration Examples Using CLI Commands

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**

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(config)#ip igmp snooping enable
switch_a(config)#no ip igmp snooping querier
```

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(config)#ip igmp snooping enable
switch_a(config)#ip igmp snooping querier
```

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(config)#interface vlan1.1
switch_a(config-if)#ip igmp version 2
```

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(config)#interface vlan1.1
switch_a(config-if)#ip igmp snooping fast-leave
```

Usage Example - **Disabling** the IGMP **fast-leave** feature:

```
switch_a(config)#interface vlan1.1
switch_a(config-if)#no ip igmp snooping fast-leave
```

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(config)#interface vlan1.1
switch_a(config-if)# ip igmp snooping report-suppression
```

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(config-if)# ip igmp query-interval 125
```

Usage Example - Configuring the IGMP **max-response-time** parameter:

```
switch_a(config-if)# ip igmp query-max-response-time 10
```

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(config)# ip igmp snooping passive-forward all
```

Usage Example - Drop all unknown multicast packets:

```
switch_a(config)# ip igmp snooping passive-forward none
```

Usage Example - Forward unknown multicast packets to the specified ports only:

```
switch_a(config)# ip igmp snooping passive-forward fe1,fe2,fe3
```

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(config)# ip igmp snooping passive-forward all
```

Usage Example - Drop all unknown multicast packets:

```
switch_a(config)# ip igmp snooping passive-forward none
```

Usage Example - Forward unknown multicast packets to the specified ports only:

```
switch_a(config)# ip igmp snooping passive-forward fe1,fe2,fe3
```

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(config)# ip igmp snooping force-forward all
```

Usage Example - Drop all unknown multicast packets:

```
switch_a(config)# ip igmp snooping force-forward none
```

Usage Example - Forward unknown multicast packets to the specified ports only:

```
switch_a(config)# ip igmp snooping force-forward fe1,fe2,fe3
```

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(config)# ip igmp snooping force-forward all
```

Usage Example - Drop all unknown multicast packets:

```
switch_a(config)# ip igmp snooping force-forward none
```

Usage Example - Forward unknown multicast packets to the specified ports only:

```
switch_a(config)# ip igmp snooping force-forward fe1,fe2,fe3
```

Network Time Protocol

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**

Enabling NTP

To enable the NTP client, follow the steps below (see Figure 119):

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

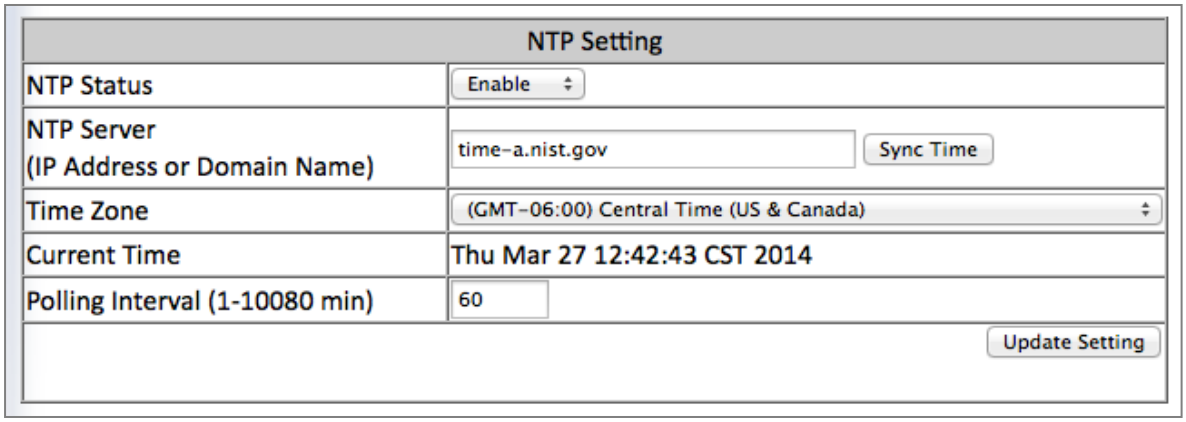


Figure 119: NTP Settings

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 120.
5. Click on the **Update Setting** button

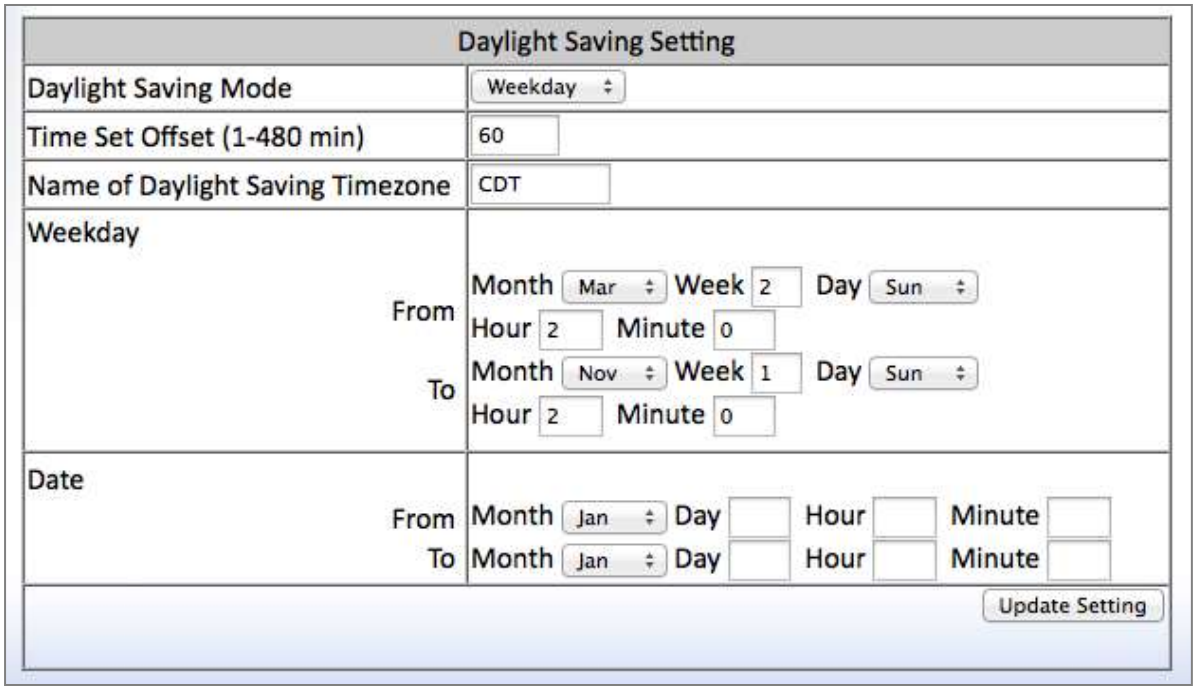


Figure 120: Daylight Savings – Weekday Mode

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 121.
5. Click on the **Update Setting** button

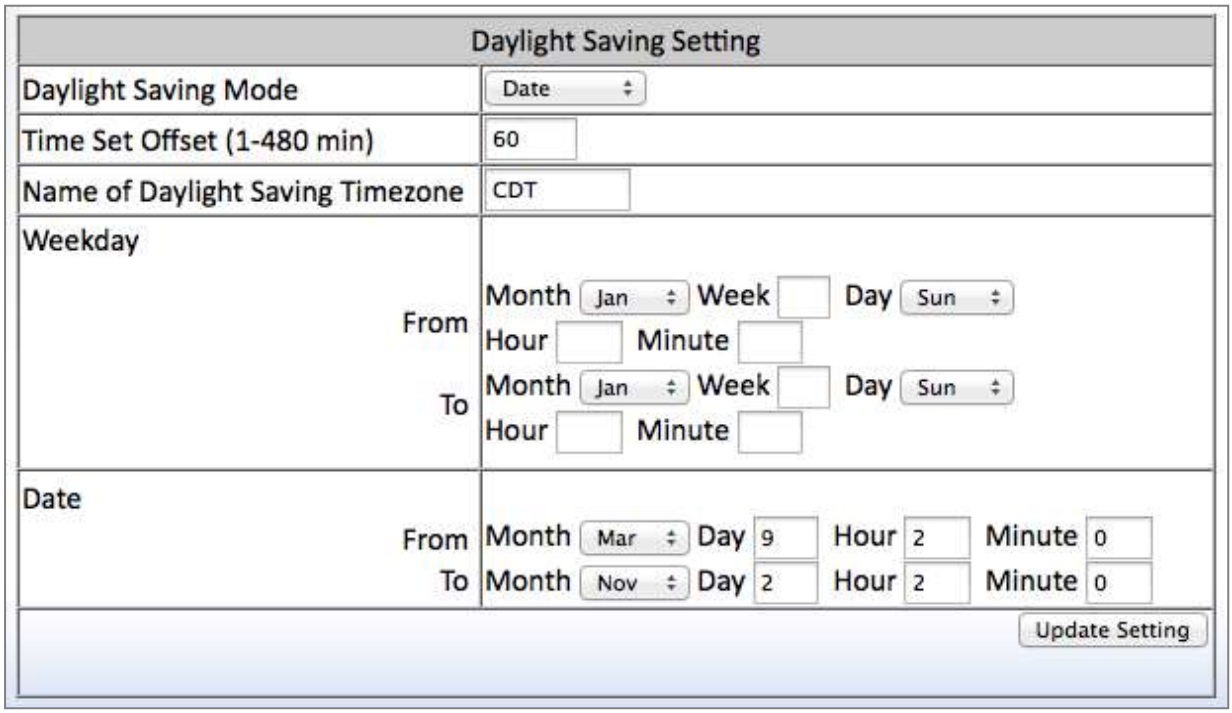


Figure 121: Daylight Savings – Date Mode

Network Time Protocol Configuration Examples Using CLI Commands

To enable NTP on the EtherWAN Managed Switch, use the CLI commands below:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **ntp enable**

To set the NTP server on the EtherWAN Managed 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(config)#ntp server 192.168.1.126
```

To set the NTP polling interval on the EtherWAN Managed 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(config)#ntp polling-interval 180
```

To have the NTP client sync the clock immediately on the EtherWAN Managed Switch, use the CLI commands below:

CLI Command Mode: **Global Configuration Mode**

CLI Command Syntax: **ntp sync-time**

Usage Example:

```
switch_a(config)#ntp sync-time
```

To set the current time zone for the EtherWAN Managed 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(config)#clock timezone CDT -6:00
```

To set the Daylight Savings Time settings using weekday mode for the EtherWAN Managed 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(config)# clock summer-time CDT weekday 2 Sun March 2
0 1 Sun November 2 0 60
```

To set the Daylight Savings Time settings using date mode for the EtherWAN Managed 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(config)# clock summer-time CDT date 9 March 2 0 2 November 2
0 60
```

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 Figure 122)

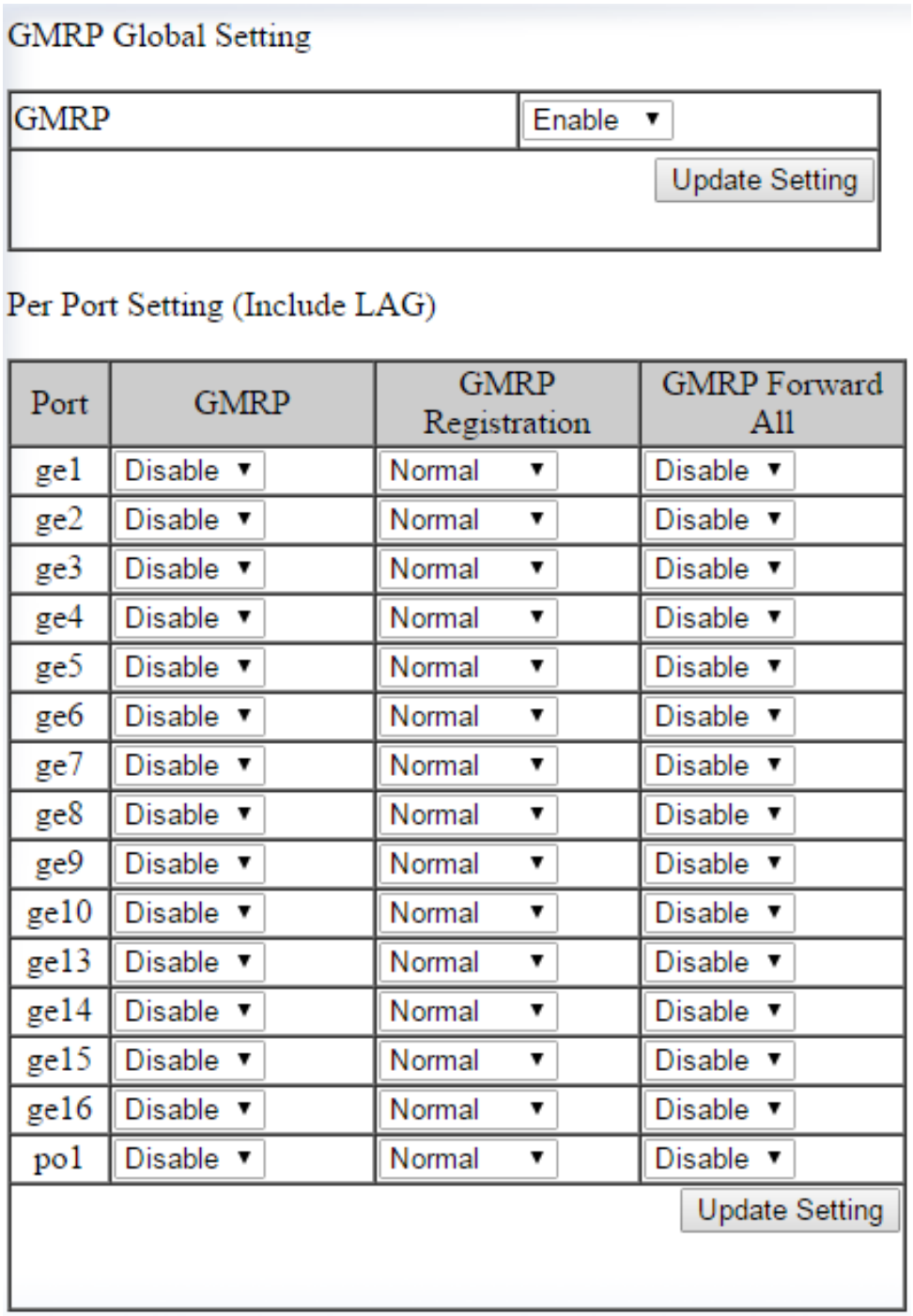


Figure 122: GMRP Global Setting

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 particular 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

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 Examples:

```
switch_a(config)# set gmrp enable bridge 1
switch_a(config)# set gmrp disable bridge 1
```

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 Examples:

```
switch_a(config)# set port gmrp enable fe1
switch_a(config)# set port gmrp disable fe1
```

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 fe1 <port id>
set gmrp registration forbidden <port id>

Usage Examples:

```
switch_a(config)#set gmrp registration normal fe1
switch_a(config)#set gmrp registration fixed fe1
switch_a(config)#set gmrp registration forbidden fe1
```

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 Examples:

```
switch_a(config)#set gmrp fwdall enable fe1
switch_a(config)#set gmrp fwdall disable fe1
```

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 setup 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 123)

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 text entry box next to **Gateway**.
5. Enter the IP addresses for the DHCP Client primary and secondary DNS servers, in the text entry box 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 text entry box next to **Lease Time**.
7. Click on the **Update Setting** button.

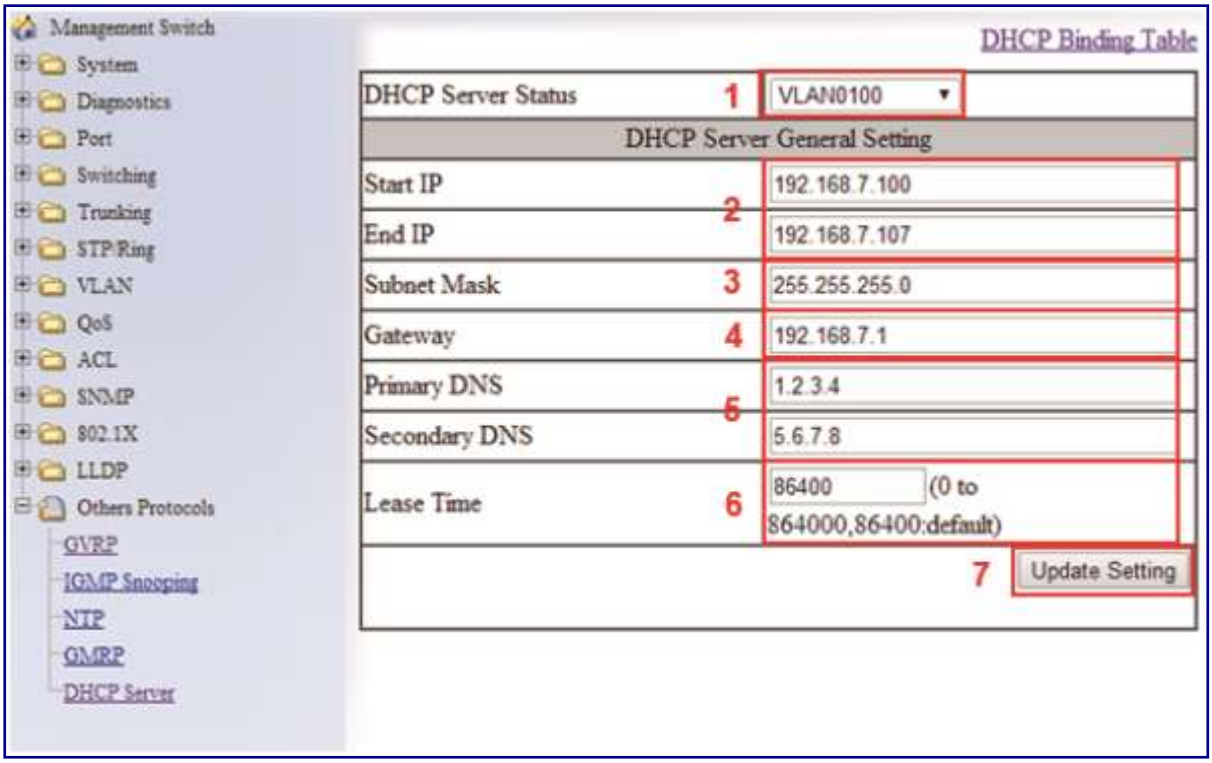


Figure 123: DHCP Server

To check what IP addresses has been allocated to which DHCP clients:

1. Click on the **DHCP Binding Table** link (see Figure 124)
2. Click on the DHCP General Setting link to get back to the previous DHCP configuration Web GUI page (see Figure 125).

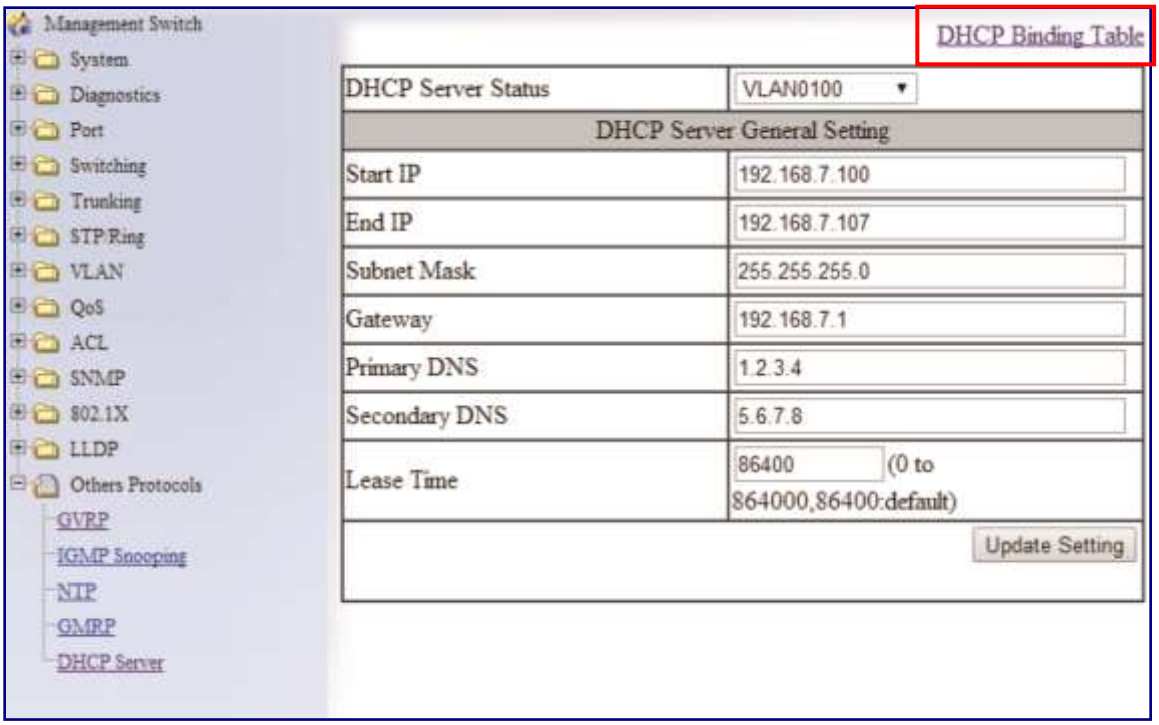


Figure 124: DHCP Bindings

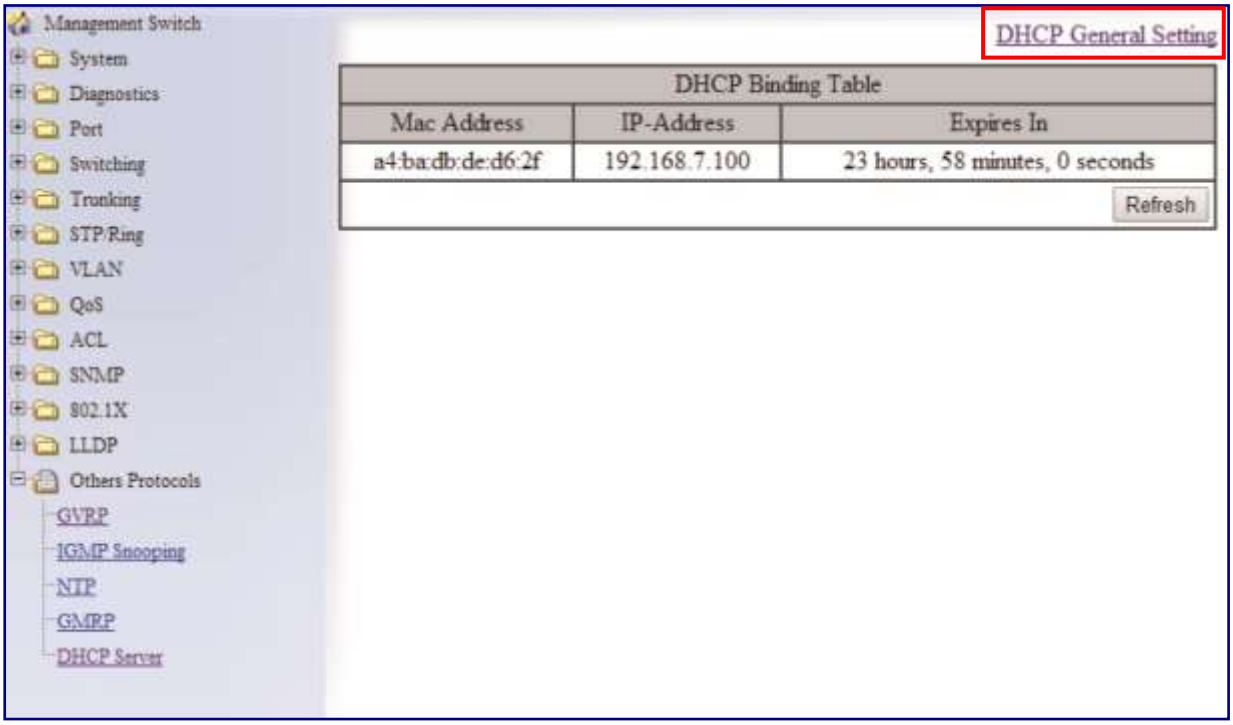


Figure 125: DHCP Binding Table

DHCP Configuration Examples Using CLI Commands

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(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
```

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**

To restart DHCP server:

CLI Command Syntax: **dhcp-server restart**

Usage Examples:

```
switch_a(config)#interface vlan1.100
switch_a(config-if)#dhcp-server enable
switch_a(config-if)#no dhcp-server enable
```

To check what IP addresses has been allocated:

CLI Command Mode: **enable**

CLI Command Syntax: **show dhcp-server binding**

Usage Example:

```
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
```

EtherWAN Corporation
No. 4, 8F, Alley 235, Baoqiao Road
Xindian District
New Taipei City 231
Taiwan
www.EtherWAN.com

EtherWAN Managed Switch User Manual

May 12, 2016