



# THOR200-PE20

2U Half Ruggedized Switch



**User's Manual**

Revision Date: Aug. 26. 2025

## Safety Information

### Electrical safety

- To prevent electrical shock hazard, disconnect the power cable from the electrical outlet before relocating the system.
- When adding or removing devices to or from the system, ensure that the power cables for the devices are unplugged before the signal cables are connected. If possible, disconnect all power cables from the existing system before you add a device.
- Before connecting or removing signal cables from the motherboard, ensure that all power cables are unplugged.
- Seek professional assistance before using an adapter or extension cord. These devices could interrupt the grounding circuit.
- Make sure that your power supply is set to the correct voltage in your area.
- If you are not sure about the voltage of the electrical outlet you are using, contact your local power company.
- If the power supply is broken, do not try to fix it by yourself. Contact a qualified service technician or your local distributor.

### Operation safety

- Before installing the motherboard and adding devices on it, carefully read all the manuals that came with the package.
- Before using the product, make sure all cables are correctly connected and the power cables are not damaged. If you detect any damage, contact your dealer immediately.
- To avoid short circuits, keep paper clips, screws, and staples away from connectors, slots, sockets and circuitry.
- Avoid dust, humidity, and temperature extremes. Do not place the product in any area where it may become wet.
- Place the product on a stable surface.
- If you encounter any technical problems with the product, contact your local distributor

### Statement

- All rights reserved. No part of this publication may be reproduced in any form or by any means, without prior written permission from the publisher.
- All trademarks are the properties of the respective owners.
- All product specifications are subject to change without prior notice

# THOR200-PE20 User's Manual



Revision Date: Aug. 27. 2025



## Revision History

| Revision    | Date (yyyy/mm/dd) | Changes         |
|-------------|-------------------|-----------------|
| Version 1.0 | 2025/08/26        | Initial release |

## Packing list

|   |                                 |
|---|---------------------------------|
|  | THOR200-PE Rugged Switch System |
|  | Power Cable                     |

## Ordering information

| Model Number | Description  |
|--------------|--|
| THOR200-PE20 | 20-port Full Gigabit Ethernet ports Rugged Switch<br>8-port IEEE 802.3at/af compliant PoE, up to 30W/port<br>4-port SFP<br>12V to 30V DC-in, Operating Temp. -40 to 70°C |



If any of the above items is damaged or missing, please contact your local distributor.

## Table of Content

|  |           |
|--|-----------|
| <b>Chapter 1: Product Introduction</b>             | <b>6</b>  |
| <b>1.1 Key Features</b>                            | <b>6</b>  |
| <b>1.2 Dimensions (2D)</b>                         | <b>6</b>  |
| <b>1.3 Panel Component</b>                         | <b>7</b>  |
| <b>1.4 LED Indication</b>                          | <b>8</b>  |
| <b>Chapter 2: JUMPERS AND CONNECTORS LOCATIONS</b> | <b>9</b>  |
| <b>2.1 1 x RS232 in RJ45</b>                       | <b>9</b>  |
| <b>2.2 2 x DI, 2 x DO</b>                          | <b>9</b>  |
| <b>2.3 1 x DC-IN power with D38999 connector</b>   | <b>10</b> |
| <b>2.4 PoE</b>                                     | <b>11</b> |
| <b>Chapter 3: WEB MANAGEMENT CONFIGURATION</b>     | <b>15</b> |
| <b>3.1 System</b>                                  | <b>17</b> |
| <b>3.1.1 INFORMATION</b>                           | <b>17</b> |
| <b>3.1.2 USER ACCOUNT</b>                          | <b>18</b> |
| <b>3.1.2.1 LOCAL USER</b>                          | <b>18</b> |
| <b>3.1.2.2 RADIUS SERVER</b>                       | <b>20</b> |
| <b>3.1.2.3 TACACS+</b>                             | <b>21</b> |
| <b>3.1.3 IP SETTING</b>                            | <b>23</b> |
| <b>3.1.3.1 IPv4</b>                                | <b>23</b> |
| <b>3.1.3.2 IPv6</b>                                | <b>24</b> |
| <b>3.1.4 DATE AND TIME</b>                         | <b>25</b> |
| <b>3.1.4.1 DATE AND TIME SETTING</b>               | <b>25</b> |
| <b>3.1.4.2 PTP SETTING</b>                         | <b>27</b> |
| <b>3.1.5 DHCP SERVER</b>                           | <b>28</b> |
| <b>3.1.5.1 DHCP Server Setting</b>                 | <b>28</b> |
| <b>3.1.5.2 DHCP Option 82</b>                      | <b>33</b> |
| <b>3.1.5.3 DHCP Leased Entries</b>                 | <b>35</b> |
| <b>3.2 ETHERNET PORT</b>                           | <b>36</b> |
| <b>3.2.1 PORT SETTING</b>                          | <b>36</b> |
| <b>3.2.2 PORT STATUS</b>                           | <b>37</b> |
| <b>3.2.3 PORT TRUNK</b>                            | <b>38</b> |
| <b>3.2.4 RATE CONTROL</b>                          | <b>41</b> |
| <b>3.2.5 STORM CONTROL</b>                         | <b>42</b> |
| <b>3.2.6 JUMBO FRAME</b>                           | <b>43</b> |
| <b>3.2.7 CFM SETTING</b>                           | <b>43</b> |

|                |                                     |    |
|----------------|-------------------------------------|----|
| <b>3.3</b>     | <b>REDUNDANCY</b>                   | 47 |
| <b>3.3.1</b>   | <b>RSTP SETTINGS</b>                | 47 |
| <b>3.3.2</b>   | <b>MSTP SETTINGS</b>                | 51 |
| <b>3.3.3</b>   | <b>ERPS SETTINGS</b>                | 54 |
| <b>3.3.3.1</b> | <b>ERPS SETTINGS</b>                | 54 |
| <b>3.3.3.2</b> | <b>ERPS STATUS</b>                  | 57 |
| <b>3.3.4</b>   | <b>LOOP PROTECTION</b>              | 59 |
| <b>3.4</b>     | <b>VLAN</b>                         | 62 |
| <b>3.4.1</b>   | <b>VLAN SETTING</b>                 | 62 |
| <b>3.4.2</b>   | <b>VLAN PORT SETTING</b>            | 64 |
| <b>3.4.3</b>   | <b>VLAN STATUS</b>                  | 66 |
| <b>3.4.4</b>   | <b>PVLAN SETTING</b>                | 66 |
| <b>3.4.5</b>   | <b>PVLAN PORT SETTING</b>           | 67 |
| <b>3.4.6</b>   | <b>PVLAN STATUS</b>                 | 69 |
| <b>3.4.7</b>   | <b>GVRP SETTING</b>                 | 69 |
| <b>3.5</b>     | <b>QUALITY of SERVICE (QoS)</b>     | 71 |
| <b>3.5.1</b>   | <b>QoS SETTING</b>                  | 71 |
| <b>3.5.2</b>   | <b>CoS MAPPING</b>                  | 72 |
| <b>3.5.3</b>   | <b>DSCP MAPPING</b>                 | 73 |
| <b>3.6</b>     | <b>MULTICAST</b>                    | 74 |
| <b>3.6.1</b>   | <b>IGMP QUERY</b>                   | 74 |
| <b>3.6.2</b>   | <b>IGMP SNOOPING</b>                | 75 |
| <b>3.6.3</b>   | <b>GMRP SETTING</b>                 | 76 |
| <b>3.7</b>     | <b>SNMP</b>                         | 77 |
| <b>3.7.1</b>   | <b>SNMP V1/V2c SETTING</b>          | 77 |
| <b>3.7.2</b>   | <b>SNMP V3</b>                      | 77 |
| <b>3.7.3</b>   | <b>SNMP TRAP</b>                    | 78 |
| <b>3.8</b>     | <b>SECURITY</b>                     | 80 |
| <b>3.8.1</b>   | <b>FILTER</b>                       | 80 |
| <b>3.8.2</b>   | <b>IEEE 802.1X</b>                  | 84 |
| <b>3.8.3</b>   | <b>DHCP Snooping</b>                | 88 |
| <b>3.8.4</b>   | <b>IP Source Guard</b>              | 90 |
| <b>3.8.5</b>   | <b>DAI (Dynamic ARP Inspection)</b> | 91 |
| <b>3.9</b>     | <b>WARNING</b>                      | 95 |
| <b>3.9.1</b>   | <b>RELAY OUTPUT</b>                 | 95 |
| <b>3.9.2</b>   | <b>EVENT TYPE</b>                   | 96 |
| <b>3.9.3</b>   | <b>SYSLOG SETTING</b>               | 97 |
| <b>3.9.4</b>   | <b>EMAIL ALERT</b>                  | 98 |

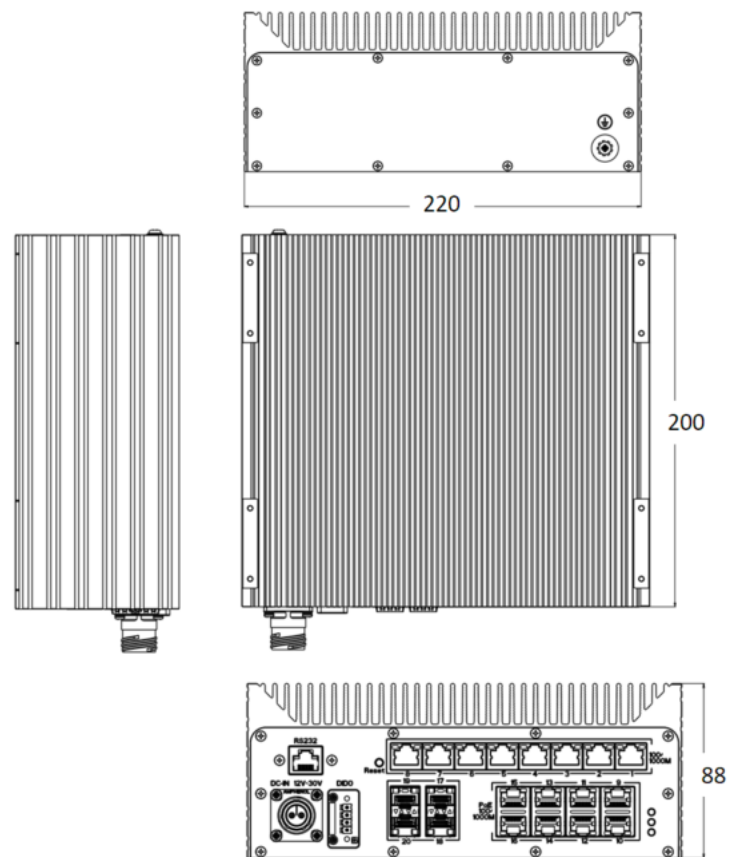
|               |                                |     |
|---------------|--------------------------------|-----|
| <b>3.10</b>   | <b>DIAGNOSTICS</b>             | 99  |
| <b>3.10.1</b> | <b>LLDP SETTING</b>            | 99  |
| <b>3.10.2</b> | <b>MAC TABLE</b>               | 100 |
| <b>3.10.3</b> | <b>PORT STATISTICS</b>         | 101 |
| <b>3.10.4</b> | <b>PORT MIRROR</b>             | 102 |
| <b>3.10.5</b> | <b>EVENT LOGS</b>              | 103 |
| <b>3.10.6</b> | <b>PING</b>                    | 103 |
| <b>3.11</b>   | <b>INDUSTRIAL</b>              | 104 |
| <b>3.12</b>   | <b>PoE</b>                     | 116 |
| <b>3.12.1</b> | <b>PoE STATUS</b>              | 116 |
| <b>3.12.2</b> | <b>PoE SYSTEM/PORT SETTING</b> | 117 |
| <b>3.12.3</b> | <b>PoE SCHEDULING</b>          | 119 |
| <b>3.12.4</b> | <b>PD ALIVE CHECK</b>          | 119 |
| <b>3.12.5</b> | <b>PoE EVENT</b>               | 120 |
| <b>3.13</b>   | <b>BACKUP AND RESTORE</b>      | 121 |
| <b>3.14</b>   | <b>FIRMWARE UPGRADE</b>        | 122 |
| <b>3.15</b>   | <b>RESET TO DEFAULTS</b>       | 123 |
| <b>3.16</b>   | <b>SAVE</b>                    | 124 |
| <b>3.17</b>   | <b>LOGOUT</b>                  | 124 |
| <b>3.18</b>   | <b>REBOOT</b>                  | 124 |
| <b>3.19</b>   | <b>FRONT PANEL</b>             | 125 |

## Chapter 1: Product Introduction

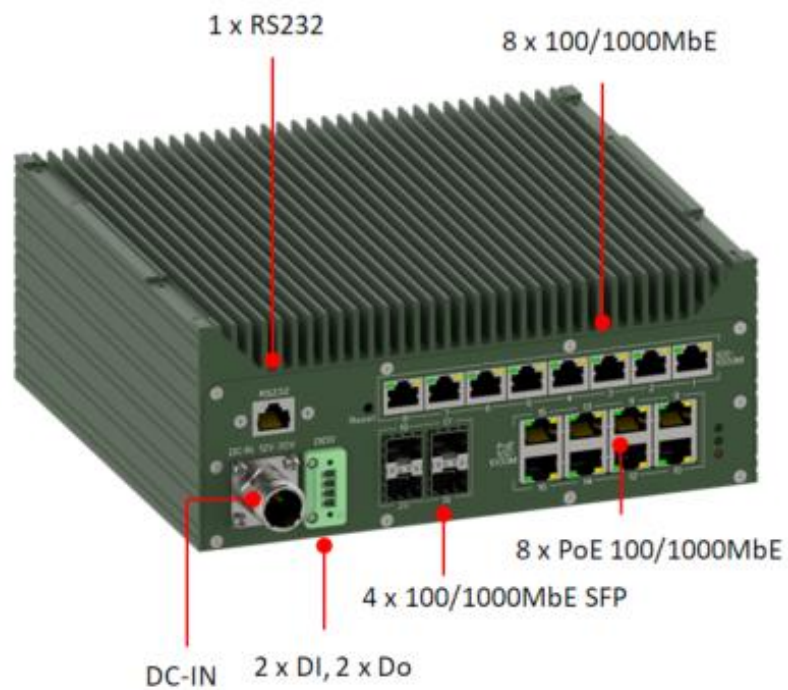
### 1.1 Key Features

| System   |  |
|--|--|
| Processor  | 1.2GHz ARM Cortex-A9 processor           |
| Front I/O  |  |
| Ground Screw   | 1  |
| X1   | 1 x RS232 in RJ45                        |
| X2   | 8 x 100/1000Base-T RJ45                  |
| X3   | 8 x 100/1000Base-T RJ45 PoE (802.3at/af) |
| X4   | 4 x 100/1000M SFP                        |
| X5   | 2 x DI, 2 x DO                           |
| X6   | 1 x DC-IN with D38999                    |
| Mechanical & Environment                             |  |
| Construction   | Aluminum chassis with fanless design     |
| Power requirement                                    | 12V ~ 30V DC-IN                          |
| Dimension  | 220 x 200 x 88 mm(W x D x H)             |
| Operating Temp.                                      | -40 to 70°C (ambient with air flow)      |
| Storage Temp   | -40 to 85°C                              |
| Relative Humidity                                    | 0% to 95%, non-condensing                |
| *Specification are subject to change without notice. |  |

### 1.2 Dimensions (2D)



## 1.3 Panel Component





|   |  |
|---|--|
| 1 | 1 x RS232 in RJ45                                    |
| 2 | 8 x 100/1000Base-T RJ45 (port 1-8)                   |
| 3 | 8 x 100/1000Base-T RJ45 PoE (802.3at/af) (port 9-16) |
| 4 | 4 x 100/1000M SFP (port 17-20)                       |
| 5 | 2 x DI, 2 x DO                                       |
| 6 | 1 x DC-IN  |

## 1.4 LED Indication

| LED           | Status   | Description   |
|---------------|----------|---|
| PWR           | Green On | DC-IN Power is On   |
|               | Off      | No Power in DC-IN   |
| Alarm<br>(DO) | Red On   | Any failures in port link, ping, power, DO and DI State by SW control |
|               | Off      | No failure occurs   |

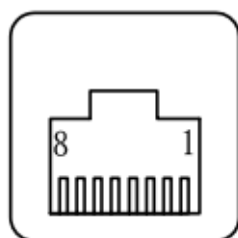
| LED                           | Status         | Description   |
|-------------------------------|----------------|---|
| RJ45 PoE Ports<br>(Port 9-16) | Green On       | Links established                                     |
|                               | Green Blinking | Packets transmitting/receiving                        |
|                               | Green Off      | Link is inactive                                      |
|                               | Amber On       | PoE power feeding(PoE)/<br>Speed 1000Mbps(non-PoE)    |
|                               | Amber Off      | PoE power not feeding(PoE)/<br>Speed 100Mbps(non-PoE) |
| SFP Ports<br>(Port 17-20)     | Green On       | Links established                                     |
|                               | Green Blinking | Packets transmitting/receiving                        |
|                               | Green Off      | Link is inactive                                      |
|                               | Amber On       | 1000M Speed   |
|                               | Amber Off      | 100M Speed  |

## Chapter 2: JUMPERS AND CONNECTORS LOCATIONS

### 2.1 1x RS232 in RJ45

The Console pin Define in RJ45: 3: TxD, 6:RxD, 5:GND

Below is an example of the wiring table of the console cable.

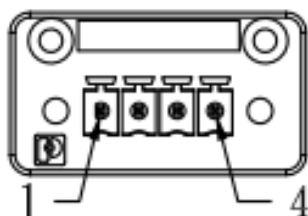


RJ45-female

| RJ45 CONSOLE |   |              |
|--------------|---|--------------|
|              |   | WIRE COLOR   |
|              | 1 | WHITE/ORANGE |
|              | 2 | ORANGE       |
| TXD          | 3 | WHITE/GREEN  |
|              | 4 | BLUE         |
| GND          | 5 | WHITE/BLUE   |
| RXD          | 6 | GREEN        |
|              | 7 | WHITE/BROWN  |
|              | 8 | BROWN        |

### 2.2 2x DI, 2x DO

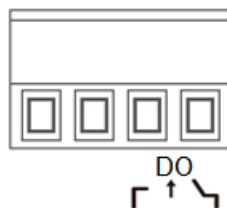
PHOENIX CONTECT  
DFK-MC 1, 5 4-GF-3, 81



| DFK-MC 1, 5 4-GF-3, 81 |   |
|------------------------|---|
|                        |   |
| DI+                    | 1 |
| DI-                    | 2 |
| DO+                    | 3 |
| DO-                    | 4 |

#### 1. WIRING THE ALARM RELAY OUTPUT (DO)

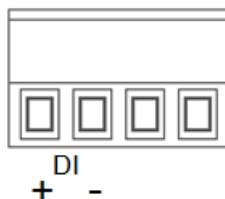
The relay output contacts are located on the front panel of the switch. The relay output consists of the 2-pin terminal block connector that used to detect user-configured events. The two wires attached to the fault contacts form a close circuit when a user-configured event is triggered. If a user-configured event does not occur, the fault circuit remains opened. The fault conditions such as power failure, Ethernet port link break or other pre-defined events which can be configured in the switch. Screw the DO wire tightly after digital output wire is connected.



**NOTE:** The relay contact only supports 0.5 A current, DC 24V. Do not apply voltage and current higher than the specifications.

## 2. WIRING THE DIGITAL INPUT (DI)

The Digital Input accepts one external DC type signal input that consists of two contacts on the terminal block connector on the switch's top panel. And can be configured to send alert message through Ethernet when the signal is changed. The signal may trigger and generated by external power switch, such as door open trigger switch for control cabinet. The switch's Digital Input accepts DC signal and can receive Digital High Level input DC 11V~30V and Digital Low Level input DC 0V~10V.



Here are the steps to wire the Digital Input:

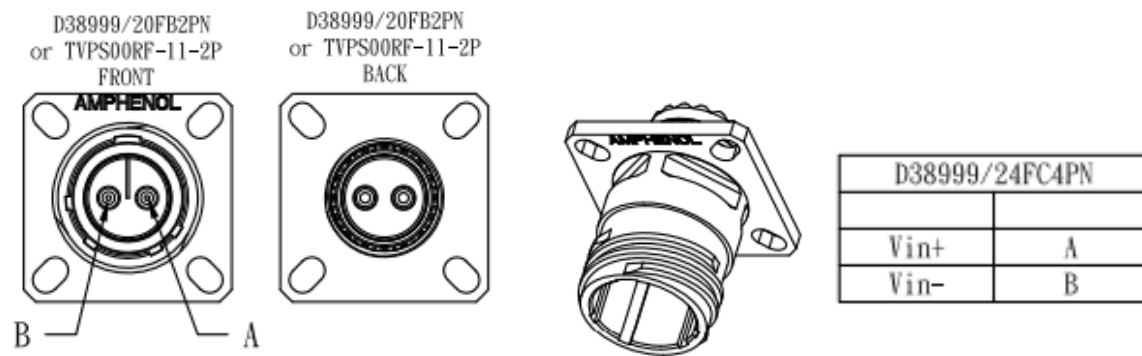
**STEP 1:** Insert the negative and positive wires into the -/+ terminals, respectively.

**STEP 2:** To keep the wires from pulling loose, tighten the wire-clamp screws on the front of the terminal block connector.

**STEP 3:** Insert the terminal block connector prongs into the terminal block receptor, which is located on the switch's top panel.

## 2.3 1 x DC-IN power with D38999 connector

- Connector pin define



## 2.4 PoE

### 1. Power Input

THOR200-PE20 (8 x PoE): Ruggedized 20-port Full Gigabit L2+ Managed PoE+ Switch, including 8 x 100/1000M copper ports, 8 x 100/1000M 802.3at/af PoE+ RJ45 ports and 4 x 100/1000M SFP Fiber ports, Max. 120W PoE output at 24VDC input.

The default setting of PoE system and ports is disabled, please enabled the PoE System, add the PoE budget (depends on the max. output budget of your switch) and then enabled the PoE ports.

THOR200-PE20 (8 x PoE) support 8-port 802.3at/af PoE+, it ranges from port 9-16. It supports **Booster PoE** design, which means it can support 24V low voltage input to 54V PoE power output.

#### Booster PoE

Booster PoE: With the Booster PoE design, the router can support low voltage input and still deliver 54VDC output to the power device (PD). The router support typical 24VDC input, range from 19.2V-30VDC. The compliant power budget of the 24V input, ensure that the power budget is enough before installing. For better power efficiency, we recommend higher voltage input.

|             |                                  |
|-------------|----------------------------------|
| Power Input | 24 (19.2-30)V $\Rightarrow$ 7.2A |
| PoE Output  | 54V $\Rightarrow$ 120W           |

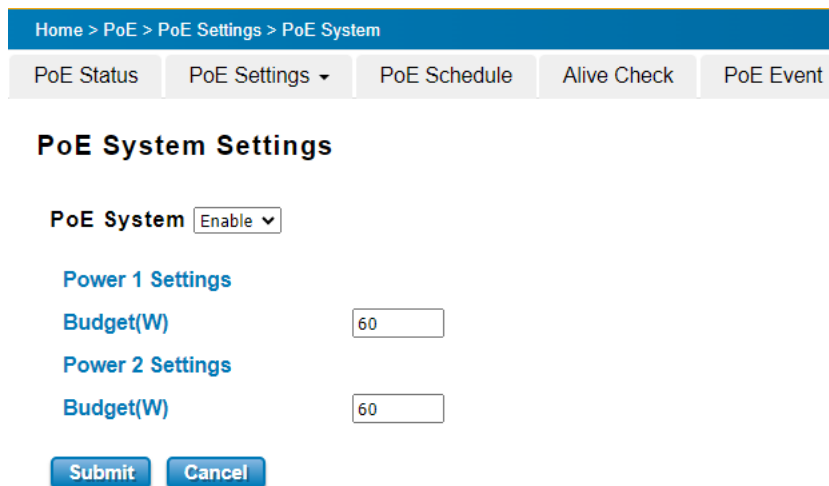
For low voltage (24V) input PoE application, it may generate higher input current, we recommend you connect dual power input to the same power source, the load can be shared and the input current of each power input is reduced. The inner components' temperature can be reduced and has better lifetime as well.

In dual power source installation, they may have different power budget and input voltage. The higher voltage power source will be main source, the other is backup source. In dual power input, we also recommend you connect the dual power input to the same power supply.

### 2. PoE POWER OUTPUT

## PoE Budget

**Port Budget Plan in PoE switch system:** Every PoE device has the restriction of delivering PoE power. The switch supports **maximum 120W while 24V (19.2V-30V) input**. Make sure the power budget is enough for the power request of the Power Devices in the beginning. Type the budget limit while enabled the PoE system. [Below is the figure of the PoE System Setting for PoE On/OFF & Budget configuration:](#)



Select "Enable" and configure the PoE Budget for Power 1 and 2 to 60W.

**WARNING: If the power budget is insufficient, the fuse of the system or PoE components will be damaged. Type the correct budget limit while enabled the PoE system is important.**

**Port Budget Plan in PoE port:** The PoE port budget is compliant with IEEE 802.3at/af standard. The maximum available current in 802.3at is 600mA, the maximum available current in 802.3af is 350mA. The maximum PoE budget of the PoE port can be configured in Web GUI is 33W for 802.3at and 17W for 802.3af in our PoE Switch. [Below is the figure of the PoE Port Setting for PoE Port Enable\(On\)/Disable\(OFF\), powering mode \(802.3at or 802.3af\).](#) For Budget Mode, you can remain "Auto" or select "Manual" to configure maximum budget for each port.

Home > PoE > PoE Settings > PoE Port

PoE Status

PoE Settings ▾

PoE Schedule

Alive Check

PoE Event

## PoE Port Settings

| Port | Mode     | Powering Mode      | Budget Mode | Budget(W)            |
|------|----------|--------------------|-------------|----------------------|
| 9    | Enable ▾ | 802.3at(2-Event) ▾ | Auto ▾      | <input type="text"/> |
| 10   | Enable ▾ | 802.3at(2-Event) ▾ | Auto ▾      | <input type="text"/> |
| 11   | Enable ▾ | 802.3at(2-Event) ▾ | Auto ▾      | <input type="text"/> |
| 12   | Enable ▾ | 802.3at(2-Event) ▾ | Auto ▾      | <input type="text"/> |
| 13   | Enable ▾ | 802.3at(2-Event) ▾ | Auto ▾      | <input type="text"/> |
| 14   | Enable ▾ | 802.3at(2-Event) ▾ | Auto ▾      | <input type="text"/> |
| 15   | Enable ▾ | 802.3at(2-Event) ▾ | Auto ▾      | <input type="text"/> |
| 16   | Enable ▾ | 802.3at(2-Event) ▾ | Auto ▾      | <input type="text"/> |

Submit

Cancel

## PoE Status:

Home > PoE > PoE Status

PoE Status

PoE Settings ▾

PoE Schedule

Alive Check

PoE Event

## PoE Status

Power 1

Budget 60 W

Power 2

Budget 60 W

Total Power Budget

120 W

Total Output Power

5.31 W

Utilization

4 %

Event

Normal

| Port | Mode    | Status   | Class  | Budget(w) | Consumption(W) | Voltage(V) | Current(mA) |
|------|---------|----------|--------|-----------|----------------|------------|-------------|
| 9    | Enable  | Powering | Class2 | 7.00      | 2.52           | 53.8       | 47          |
| 10   | Enable  | Powering | Class3 | 17.00     | 2.79           | 53.8       | 52          |
| 11   | Disable | Off      | ---    | ---       | 0.00           | 0.0        | 0           |
| 12   | Disable | Off      | ---    | ---       | 0.00           | 0.0        | 0           |
| 13   | Disable | Off      | ---    | ---       | 0.00           | 0.0        | 0           |
| 14   | Disable | Off      | ---    | ---       | 0.00           | 0.0        | 0           |
| 15   | Disable | Off      | ---    | ---       | 0.00           | 0.0        | 0           |
| 16   | Disable | Off      | ---    | ---       | 0.00           | 0.0        | 0           |

Reload

**PoE Priority:** If the system PoE consumption is over the system budget control, the PoE system will turn off low priority port PoE function, until the consumption is becomes smaller than the system budget. In THOR200-PE20, the PoE priority is depended on port number; the small port number has higher priority than high port number. It means port 9 (1st PoE port) always has highest priority, then the port 10, 11... and port 16 is the lowest priority port.

The priority setting is pre-configured in the system. There is no Web GUI and you don't need to configure it

**WARNING:**

During the PoE operating, the surface will accumulate heat and caused surface temperature becomes higher than ambient temperature. Do remember don't touch device surface during PoE operating.


## Chapter 3: WEB MANAGEMENT CONFIGURATION

To access the management interface, there has several ways access mode through a network; they are web management, console management and telnet management. Web interface management is the most common way and the easiest way to manage a network, through web interface management, a switch interface offering status information and a subset of switch commands through a standard web browser. If the network is down, another alternative to access the management interface can be used. The alternative way is by using console and telnet management which is offer configuration way through CLI Interface. We also provide excellent alternative by configure the switch via RS232 console cable if user doesn't attach user admin PC to the network, or if user loses network connection to Managed Switch. This manual describes the procedures for Web Interface and how to configure and monitor the managed switch only. For the CLI management interface please refers to the *CLI Command User Manual*.

### PREPARATION FOR WEB INTERFACE MANAGEMENT

Web interface management that allows user through standard web-browser such as Microsoft Internet Explorer, or Mozilla, or Google Chrome, to access and configure the switch management on the network.

1. Plug the DC power to the switch and connect switch to computer.
2. Make sure that the switch default IP address is **192.168.10.1**.
3. Check that PC has an IP address on the same subnet as the switch. For example, the PC and the switch are on the same subnet if they both have addresses that start 192.168.10.x (Ex: **192.168.10.2**). The subnet mask is 255.255.255.0.
4. Open command prompt and ping **192.168.10.1** to verify that the switch is reachable.
5. Launch the web browser (Internet Explorer or Mozilla Firefox or Google Chrome) on the PC.
6. Type <http://192.168.10.1> (or the IP address of the switch). And then press **Enter** and the login page will appear.
7. For security concern, the system will ask you enter New User **Name, Privilege, New Password and Confirm Password** at first Login, please follow the indication to enter new username, Privilege and password. You must add New User Name with **Privilege 15 (Administrator privilege)** at first login.
8. Type New user name and the password, then click **Login**.



The image displays two side-by-side web interface windows. The left window, titled '(Model Name)', contains a login form with two input fields: the first contains 'admin' and the second contains six dots. Below these fields is a blue 'Login' button. The right window, titled 'Please change the password!', contains a form for creating a new user. It has four labeled input fields: 'Name' (containing 'admin'), 'Privilege' (a dropdown menu showing '15'), 'New Password', and 'Confirm Password'. At the bottom of this form are two buttons: 'Submit' and 'Cancel'.



In this Web management for Featured Configuration, user will see all Switch's various configuration menus at the left side from the interface. Through this web management interface user can configure, monitoring, and set the administration functions. The whole information used web management interface to introduce the featured functions. User can use all of the standard web-browser to configure and access the switch on the network.

After the setting is changed on the configuration page/tab, user clicks on the "Submit" button at the bottom of the page to active the new settings. To save the changed settings permanently, user must click on "Save" at the top of the configuration page and click "Yes" to save all the submitted changes. Without "Save", the settings will be discarded if the switch is rebooted.



Following topics are covered in this chapter:

- 3.1 System
- 3.2 Ethernet Port
- 3.3 Redundancy
- 3.4 VLAN
- 3.5 QoS
- 3.6 Multicast
- 3.7 SNMP
- 3.8 Security
- 3.9 Warning
- 3.10 Diagnostics
- 3.11 Industrial
- 3.12 PoE
- 3.13 Backup / Restore
- 3.14 Firmware Upgrade
- 3.15 Reset to Defaults
- 3.16 Save
- 3.17 Logout
- 3.18 Reboot
- 3.19 Front Panel

Note 1: Most of the Web GUI configuration pages are the same for our Layer 2 and Layer 3 switch. The number of the interface may be not the same; however, you can still refer to the features' configuration steps.

## 3.1 System

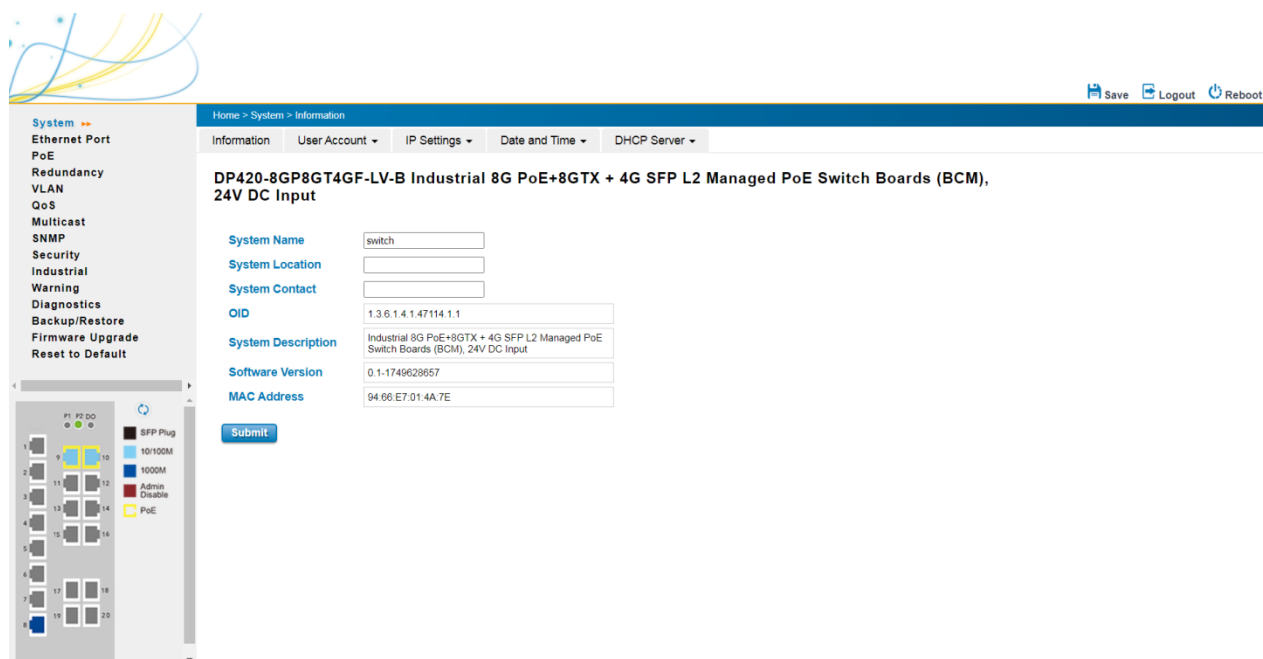
When the user login to the switch, user will see the system section appear. This section provides all the basic setting and information or common setting from the switch that can be configured by the administrator.

Following topics is included:

- Information
- User Account
- IP Setting
- Date and Time
- DHCP Server

### 3.1.1 INFORMATION

Information section, this section shows the basic information from the switch to make it easier to identify different switches that are connected to User network. The figure below shows the interface of the Information section.



| TERMS           | Description  |
|-----------------|--|
| System Name     | <b>Default: switch</b><br>Set up a name to the switch device.  |
| System Location | <b>Default: Blank</b><br>User can specify the switch's physical location.                                  |
| System Contact  | <b>Default: Blank</b><br>User can specify the contact person here. User can type the name, mail address or |

|                           |   |
|---------------------------|---|
|                           | other information of the administrator.                                 |
| <b>OID</b>                | Indicates the Object ID of the switch.                                  |
| <b>System Description</b> | Display the name of the product.  |
| <b>Software Version</b>   | Display the firmware latest version that installed in the device.       |
| <b>MAC Address</b>        | Display the hardware's MAC addresses that assigned by the manufacturer. |

**NOTE:** For any kind of changes in configuration settings always remember to click on Save to save the settings. Otherwise, all of settings User has made will be lost when the switch is powered off or restarted.

After finish the configuration, click on Submit to apply User settings.

## 3.1.2 USER ACCOUNT

Switch supports the management accounts; with the Name default setting is **admin** and the authority allow user to configure all of configuration parameters. Below is the **User Account** section that consists of two interfaces, Local User and Radius Interface.

**NOTE:** For security consideration, please change the password after first log in

### 3.1.2.1 LOCAL USER

Home > System > Local User

Information
User Account
Network Settings
Date and Time
DHCP Server

### Local User

Name
Privilege
New Password
Confirm Password

Submit
Cancel

### Local User List

| Select                   | User   | Privilege |
|--------------------------|--------|-----------|
| <input type="checkbox"/> | admin  | 15        |
| <input type="checkbox"/> | admin2 | 15        |
| <input type="checkbox"/> | guest  | 0         |

Remove Selected
Cancel

### Authentication Order

Order
Local

Submit

The Local User interface describes how to configure the system user name, privilege and password for the web management login. To change the Name, privilege and Password, user just needs to input a new Name, select the Privilege and New Password then confirm the new password in this Local User section. After finished, click **Submit** to apply the changes. Don't forget to **Save** the settings. Try to re-login with the new User Name and Password.

**Privilege:** The privilege 15 represent for administrator privilege, user can read and configure the new settings. The privilege 0 represent for Read-Only privilege. **You must have at least one User Name with Privilege 15 (Administrator privilege) in local user list, otherwise you can't change the switch setting any more.**

Once you try change the new setting with "0" privilege, the system will prompt error message as below:

Your permission is not enough to perform the action!

OK

**Remove the user:** you can Select the checkbox of the user, click "Remove Selected" to apply the change. You will see the below prompt message.

**The settings were successfully changed!**

OK

**Authentication Order:** Select the order of the authentication types. Click "Submit" to apply the change.

**Authentication Order**

Order

- Local
- RADIUS -> Local
- TACACS+ -> Local

The description of the Local User interface is as below:

| TERMS            | Description  |
|------------------|--|
| Name             | <b>Default: admin</b><br>Key in new user name here.  |
| Privilege        | <b>15:</b> Administrator, Read and Write the new configuration<br><b>0:</b> Guest, Read-Only |
| New Password     | <b>Default: admin</b><br>Key in new password here.   |
| Confirm Password | Re-type the new password again to confirm it.  |

After finished setting up the User Name and Password, click on **Submit** to apply the configuration.

### 3.1.2.2 RADIUS SERVER

The Remote Authentication Dial In User Service (RADIUS) mechanism is a centralized "AAA" (Authentication, Authorization and Accounting) system for connecting to network services. The fundamental purpose of RADIUS is to provide an efficient and secure mechanism for user account management. RADIUS server system allows you to access the switch through secure networks against unauthorized access.

Home > System > RADIUS Server

Information
User Account
IP Setting
Date and Time
DHCP Server

### RADIUS Authentication

**RADIUS Server 1**

RADIUS Server IP

Shared Key

Server Port

**RADIUS Server 2**

RADIUS Server IP

Shared Key

Server Port

Submit

How to set up a RADIUS server:

- Enter the IP address of the RADIUS server in **Server IP Address**
- Enter the **Shared Secret** of the RADIUS server
- Enter the **Server port** if necessary, by default RADIUS server listens to port 1812
- Click **Submit**

The description of the RADIUS Authentication interface is as below:

| TERMS                   | Description   |
|-------------------------|---|
| <b>RADIUS Server IP</b> | Radius Server IP Address  |
| <b>Shared Key</b>       | Shared key are used to verify that RADIUS messages, with the exception of the Access-Request message, are sent by a RADIUS-enabled device that is configured with the same shared key. Shared key also verify that the RADIUS message has not been modified in transit (message integrity). |
| <b>Server Port</b>      | Set communication port of an external RADIUS server as the authentication database.<br>The general value is 1812  |

### 3.1.2.3 TACACS+

The Terminal Access Controller Access Control System (TACACS+) security protocol is a recent protocol developed by Cisco. It provides detailed accounting information and flexible administrative control over the authentication and authorization processes. TACACS+ allows for a single access control server (the TACACS+ daemon) to provide authentication, authorization, and accounting services independently. Below TACAS+ server setting allows you to configure TACAS+ Server settings.

Information
User Account
IP Settings
Date and Time
DHCP Server

### TACACS+ Settings

**TACACS+ Server 1**

TACACS+ Server IP

Shared Key

Server Port

**TACACS+ Server 2**

TACACS+ Server IP

Shared Key

Server Port

**TACACS+ Settings**

Authentication Type

Server timeout(s)

**Submit**

How to set up a TACACS+ server:

- Select the **Authentication Type**.
- Enter the **Authentication Timeout** in seconds.
- Enter the IP address of the TACACS+ server in **Server IP Address**.
- Enter the **Shared Secret** of the TACACS+ server.
- Enter the **Server port** if necessary, by default TACACS+ server listens to port 49.
- Click **Submit**

The description of the TACAS+ interface is as below:

| TERMS                      | Description   |
|----------------------------|---|
| <b>TACAS+ Server IP</b>    | TACACS+ Server IP Address.<br>The system allows 2 TACAS+ servers  |
| <b>Share Key</b>           | Specifies the shared key for TACACS+ communications between the device and the TACACS+ server. The shared key must match the encryption used on the TACACS+ server. |
| <b>Server Port</b>         | Set communication port of an external TACACS+ server as the authentication database.<br>The general value is 49   |
| <b>Authentication Type</b> | <b>Type:</b> PAP, ASCII, CHAP<br>Select the authentication type to authenticate to the server.  |
| <b>Server Timeout</b>      | <b>Default:</b> 5   |

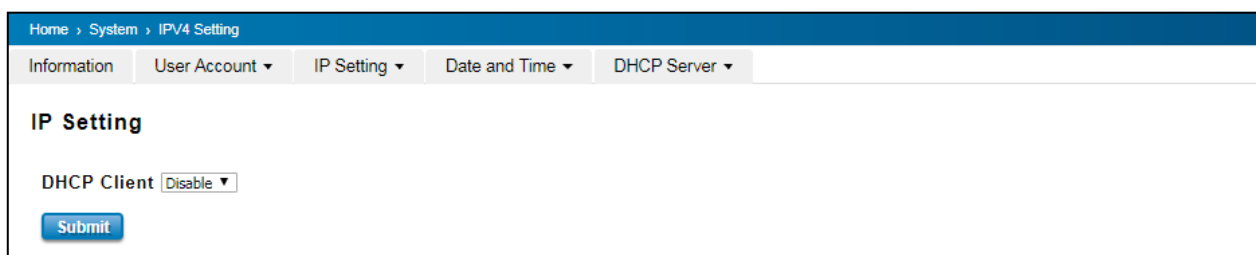
|  |  |
|--|--|
|  | The maximum number of seconds allowed establishing a TCP connection between the device and the TACACS+ server. |
|--|--|

## 3.1.3 IP SETTING

IP Setting section allows users to configure both IPv4 and IPv6 values for management access over the network. Switch supports both IPv4 and IPv6, and can be managed through either of these address types.

### 3.1.3.1 IPv4

#### DHCP Client



When DHCP Client function is enabled, an IP address will be assigned to the switch from the network's DHCP server. In this mode, the default IP address will be replaced by the one assigned by DHCP server. If DHCP Client is disabled, the configured IP settings will be used. The DHCP client will announce the configured System Name as hostname to provide DNS lookup. The description of the columns is as below:

| TERMS       | Description   |
|-------------|---|
| DHCP Client | Select to <b>Enable</b> or <b>Disable</b> to activate or deactivate the DHCP Client function. |

#### IPv4 Configuration



The IPv4 Configuration includes the switch's IP address and subnet mask, as well as the IP address of the default gateway. In addition, input cells are provided for the IP addresses of a 1st and 2nd DNS server. Configure the managed switch's IP settings. The figure below shows the user interface of IPv4 Configuration.

The description of the columns is as below:

| TERMS      | Description           |
|------------|-----------------------|
| IP Address | Default: 192.168.10.1 |



|                                   |  |
|-----------------------------------|--|
|                                   | Set up the IP address reserved by User network for User switch. If DHCP Client function is enabled, no need to assign an IP address to switch as it will be overwritten by DHCP server and shown here. |
| <b>Subnet Mask</b>                | <b>Default: 255.255.255.0</b><br>Assign the subnet mask for the IP address here. If DHCP Client function is enabled, no needs to assign the subnet mask.   |
| <b>Default Gateway</b>            | Assign the gateway for the switch here.  |
| <b>DNS Server 1, DNS Server 2</b> | Specifies the IP address of the DNS server 1 and 2 that used in user network.  |

## 3.1.3.2 IPv6

### IPv6 Setting

#### IPv6 Setting

IPv6 Address

Prefix Length

Add

IPv6 Default Gateway

Submit

☐ IPv6 Address
 

☐ fe80::9666:e7ff:fe12:933/64

Remove

Reload

An Ipv6 address is represented as eight groups of four hexadecimal digits, each group representing 16 bits (two octets). The groups are separated by colons (the length of Ipv6 address is 128bits). An example of an Ipv6 address is: fe80::212:77ff:feff:1acb/64.

The description of the columns is as below:

| TERMS                       | Description   |
|-----------------------------|---|
| <b>Ipv6 Address</b>         | Add the IPv6 address. The network portion of the address can be configured by specifying the Prefix and using a EUI-64 interface ID in the low order 64 bits. The host portion of the address is automatically generated using the modified EUI-64 form of the interface identifier (Switch's MAC address). |
| <b>Prefix Length</b>        | The size of subnet or network, and it equivalent to the subnetmask, but written in different. Then click <b>Add</b> to apply new address to the system.   |
| <b>Ipv6 Default Gateway</b> | The prefix value must be formatted according to the RFC 2373 "IPv6 Addressing Architecture," using 8 colon-separated 16-bit hexadecimal values. One double colon may be used in the address to indicate the appropriate number of zeros required to fill  |

|                     |   |
|---------------------|---|
|                     | the undefined fields.   |
| <b>Ipv6 Address</b> | <b>The default IP address of the Switch: fe80::212:77ff:feff:1acb/64</b><br>Select existed Ipv6 address and click <b>Remove</b> to delete IP address. Click <b>Reload</b> to refresh and reload list. |

## Neighbor Cache

The IPv6 neighbor table includes the neighboring node's IPv6 address, Interface, MAC Address, and the current state of the entry.

**Neighbor Cache**

| IPv6 Address         | Interface            | Link Layer (MAC) Address | State                |
|----------------------|----------------------|--------------------------|----------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/>     | <input type="text"/> |

Reload

The description of the columns is as below:

| TERMS                 | Description  |
|-----------------------|--|
| <b>Neighbor Cache</b> | The system will update Neighbor Cache automatically, and user also can click <b>Reload</b> to refresh the table. |

## 3.1.4 DATE AND TIME

### 3.1.4.1 DATE AND TIME SETTING

The switch has a time calibration function based on information from an NTP server or user specified time and date, allowing functions such as automatic warning emails to include a time and date stamp.

**NOTE:** The switch does not have a real-time clock. The user must update the Current Time to set the initial time for the switch after each reboot, especially when there is no NTP server on the LAN or Internet connection.

**Date and Time**

Current Time

Yr 2017 Mon 01 Day 1 Hr 05 Mn 34 Sec 28

Get PC Time

Time Zone

(GMT) Greenwich Mean Time: Dublin, Edinburgh, Lisbon, London ▼

NTP

☐ Enable NTP client update

1st Time Server

N/A

2st Time server

N/A

Daylight saving Time

Disable ▼

Daylight Saving Start

1st ▼ Sun ▼ in Jan ▼ at 00 ▼ 00 ▼

Daylight Saving End

1st ▼ Sun ▼ in Jan ▼ at 00 ▼ 00 ▼

Submit

Cancel

The description of the columns is as below:

| TERMS  | Description   |
|--|---|
| <b>Current Time</b>                                    | User can configure time by input it manually. User also can click the <b>Get Time from PC</b> to get PC's time setting.   |
| <b>Time Zone</b>                                       | Choose the Time Zone section to adjust the time zone based on the user area.  |
| <b>NTP</b>   | <b>Enable NTP Client update</b> by checking this box. The system will send request packet to acquire current time from the NTP server that assigned.<br><b>*Make sure that the switch also has the internet connection.</b> |
| <b>1st Time Server &amp; 2nd Time Server</b>           | Choose from NTP Server List, to adjust User system time.  |
| <b>Daylight Saving Time</b>                            | Enable the Daylight Saving Function and the setting of function start and end time or disable it.   |
| <b>Daylight Saving Start &amp; Daylight Saving End</b> | Allows user to sets the Start and End time individually.  |

After finished configuring, click on **Submit** to activate the configuration.

## IEEE 1588 PTP

### IEEE 1588

IEEE 1588 was published in 2002, expands the performance capabilities of Ethernet networks to control systems that operate over a communication network. In recent years an increasing number of electrical power systems have been using a more distributed architecture with network technologies that have less stringent timing specifications. IEEE 1588 generates a master-slave relationship between the clocks, and enforces the specific timing requirements in such power systems. All devices ultimately get their time from a clock known as the grandmaster clock. In its basic form, the

protocol is intended to be administration free.”

## How Does an Ethernet Switch Affect 1588 Synchronization?

An Ethernet switch potentially introduces multi-microsecond fluctuations in the latency between the 1588 grandmaster clock and a 1588 slave clock. When these fluctuations are incorrect, it will cause synchronization errors. The magnitude of these fluctuations depends on the design of the Ethernet switch and the details of the communication traffic. Experiments with prototype implementations of IEEE 1588 indicate that with suitable care the effect of these fluctuations can be successfully managed. For example, use of appropriate statistics in the 1588 devices to recognize significant fluctuations and use suitable averaging techniques in the algorithms controlling the correction of the local 1588 clock will be good design means to achieve the highest time accuracy.

## Can Ethernet switches be designed to avoid the effects of these fluctuations?

A switch can be designed to support IEEE 1588 while avoiding the effects of queuing. In this case two modifications to the usual design of an Ethernet switch are necessary:

1. The **Boundary Clock and Transparent Clock** functionalities defined by IEEE 1588 must be implemented in the switch.
2. The switch must be configured so that it does not pass IEEE 1588 message traffic using the normal communication mechanisms of the switch.

Such an Ethernet switch will synchronize clocks directly connected to one of its ports to the highest possible accuracy.

The main function of IEEE 1588 is to synchronize the clocks of different end devices over a network at speeds faster than one Micro-second. After time synchronized, the system time will display the correct time of the PTP server.

### 3.1.4.2 PTP SETTING

The PTP can be set in this PTP Setting webpage in which the user can configure PTP. The top part of this figure allows the users to enable or disable the PTP function. To enable PTP on the managed switch, please choose Enable. Note that the PTP functions will not active if the Operation is disabled. Please see description of PTP Setting in table description. Note that after setting the desired PTP Setting, please click Apply button to allow the configuration take effect.

**PTP Setting**

|                                |              |
|--------------------------------|--------------|
| Operation                      | Disable ▾    |
| Operation Mode                 | Auto Elect ▾ |
| Synchronization Interval       | 0(1s) ▾      |
| Announce Interval              | 1(2s) ▾      |
| Announce Receipt Timeout       | 6            |
| Minimum Delay Request Interval | 1(2s) ▾      |
| Domain Number                  | 0            |
| Priority 1                     | 128          |
| Priority 2                     | 128          |
| Delay Mechanism                | E2E ▾        |

Apply

The description of the columns is as below:

| TERMS                                 | Description   |
|---------------------------------------|---|
| <b>Operation</b>                      | <b>Default: Disable</b><br>Enable/Disable the PTP function. This is the main option that needs to be enabled so that the PTP function will work   |
| <b>Operation Mode</b>                 | <b>Default: Auto Elect</b><br>Choose Mode (Auto Elect, Preferred Master Clock or Slave)   |
| <b>Synchronization Interval</b>       | <b>Default: 0 (1s)</b><br>Set the interval of the sync packet transmitted time. Small interval causes too frequent sync, which will cause more load to the device and network.  |
| <b>Announce Interval</b>              | <b>Default: 1 (2s)</b><br>Sets the announce message interval  |
| <b>Announce Receipt Timeout</b>       | <b>Default: 6</b><br>The multiple of announce message receipt timeout by the announce message interval.   |
| <b>Minimum Delay Request Interval</b> | <b>Default: 1 (2s)</b><br>Minimal delay request message interval  |
| <b>Domain Number</b>                  | Subdomain name (IEEE 1588-2002) or the domain Number (IEEE 1588-2008) fields in PTP messages  |
| <b>Priority 1</b>                     | <b>Default: 128</b><br>Set the clock priority 1 (PTP version 2). The lower values take precedence to be selected as the master clock in the best master clock algorithm, 0 = highest priority, 255 = lowest priority.                             |
| <b>Priority 2</b>                     | <b>Default: 128</b><br>Set the clock priority 2 (PTP version 2). The lower values take precedence to be selected as the master clock in the best master clock algorithm (BMCA), 0 = highest priority, 255 = lowest priority.                      |
| <b>Delay Mechanism</b>                | <b>Default: E2E</b><br>Configures the delay mechanism in boundary clock mode.<br><b>E2E</b> - The delay request or response mechanism used in the boundary clock mode.<br><b>P2P</b> - The peer-to-peer mechanism used in the boundary clock mode |

## 3.1.5 DHCP SERVER

### 3.1.5.1 DHCP Server Setting

Switch has DHCP Server Function that will provide a new IP address to DHCP Client. After enable DHCP Server function, set up the Network IP address for the DHCP server IP address, Subnet Mask, Default Gateway address and Lease Time for client. Below is the DHCP Server Setting interface

Home > System > DHCP Server Settings

Information
User Account
Network Settings
Date and Time
DHCP Server

### DHCP Server Settings

**Global Settings** Enable

Submit

**Create Address Pool**

**Activated Subnet** 192.168.10.0/24

Add

**Address Pool List**

|                                  | Subnet          | Leased Network | Default Gateway | Leased Time | Primary DNS | Secondary DNS |
|----------------------------------|-----------------|----------------|-----------------|-------------|-------------|---------------|
| <input checked="" type="radio"/> | 192.168.10.0/24 | 0.0.0.0/0      | 0.0.0.0         | 604800      | 0.0.0.0     | 0.0.0.0       |

Delete

**Address Pool Settings**

**Subnet** 192.168.10.0/24

**Leased Network** 0.0.0.0

**Mask** 0.0.0.0

**Default Gateway** 0.0.0.0

**Primary DNS Server** 0.0.0.0

**Secondary DNS Server** 0.0.0.0

**Lease Time(s)** 604800  
(60~31536000 seconds)

Submit

The description of the columns is as below:

| TERMS                    | Description  |
|--------------------------|--|
| <b>Global Setting</b>    | Select to <b>Enable</b> or <b>Disable</b> to activate and deactivate DHCP Server function.   |
| <b>Address Pool Add</b>  | Add address pool to local DHCP Server.<br>Select the IP address/mask in <b>Activated Subnet</b> and Click " <b>Add</b> ".<br>After applied, you can see the new Pool in Address Pool List. |
| <b>Address Pool List</b> | Choose the address pool setting that has been entered.<br>You can "Delete" it in the list.   |
| <b>Pool Name</b>         | Add address pool name to local DHCP Server   |
| <b>Network</b>           | Enter the starting IP addresses for the DHCP server's IP assignment.   |
| <b>Mask</b>              | Assign the subnet mask for the IP address here.  |
| <b>Default Gateway</b>   | Enter the ending IP addresses for the DHCP server's IP assignment.   |

|                   |  |
|-------------------|--|
| <b>DNS Server</b> | Type the Primary, Secondary DNS Server's IP address.   |
| <b>Lease Time</b> | The maximum length of time for the IP address lease. Enter the Lease time in minutes.<br>(Lease Time range: 60-31536000 seconds) |

The DHCP Server will automatically assign an IP address to the computers on the LAN/private network. Be sure to set user computers to be DHCP clients by setting their TCP/IP settings to "Obtain an IP Address Automatically." When user turns the computers on, they will automatically load the proper TCP/IP settings provided by the switch. If User manually assigns IP addresses to User computers or devices, make sure the IP addresses are outside of this range or User may have an IP conflict. After finished configuring, click on **Submit** to activate the configuration.

## Excluded Address List

The figure below shows the **Excluded Address List**, the IP address that is listed in the **Excluded Address List** table will not be assigned to the network devices.

**Excluded Address List**

Excluded IP

**Add**

| Index                      | IP Address                                 |
|----------------------------|--|
| <input type="checkbox"/> 1 | <input type="text" value="192.168.10.10"/> |

**Remove** **Reload**

The description of the columns is as below:

| TERMS                        | Description   |
|------------------------------|---|
| <b>Excluded Address List</b> | Type a specific address into the <b>Excluded IP</b> field for the DHCP server reserved IP address. Then click <b>Add</b> , to remove an IP address from the list click <b>Remove</b> . To refresh the list, click <b>Reload</b> . |

## Static Port/IP Binding List

The figure below is the web interface for **Static Port/IP Binding List**.

**Static Port/IP Binding List**

Port

IP Address

**Add**

| Index                      | Port                           | IP Address                                 |
|----------------------------|--------------------------------|--|
| <input type="checkbox"/> 1 | <input type="text" value="5"/> | <input type="text" value="192.168.10.15"/> |

**Remove** **Reload**

Type the specific Port and IP address, and then click **Add** to add a new Port & IP address binding rule for a specific client. The description of the columns is as below:

| TERMS      | Description   |
|------------|---|
| Port       | The port that wishes binding.   |
| IP Address | The IP address that will assign to the device with the Binding MAC address. |

To remove from the binding list, select the index and click **Remove**. To refresh the list, click **Reload**.

## Static MAC/IP Binding List

The figure below is the web interface for **Static MAC/IP Binding List**.



Static MAC/IP Binding List

MAC Address

IP Address

**Add**

| Index                      | MAC Address                                 | IP Address                                 |
|----------------------------|---|--|
| <input type="checkbox"/> 1 | <input type="text" value="000f.fe4d.9196"/> | <input type="text" value="192.168.10.20"/> |

**Remove** **Reload**

Type the specific MAC and IP address, and then click **Add** to add a new MAC & IP address binding rule for a specific client.

The description of the columns is as below:

| TERMS       | Description   |
|-------------|---|
| MAC Address | The MAC address of the device that wishes binding.                          |
| IP Address  | The IP address that will assign to the device with the Binding MAC address. |

To remove from the binding list, select the index and click **Remove**. To refresh the list, click **Reload**.

## Option 82/IP Binding List

The figure below is the web interface for **Option 82/IP Binding List**.



Option82/IP Binding List

Circuit ID

Remote ID

IP Address

**Add**

| Index                      | Circuit ID                            | Remote ID                             | IP Address                                |
|----------------------------|---------------------------------------|---------------------------------------|---|
| <input type="checkbox"/> 1 | <input type="text" value="01000101"/> | <input type="text" value="COA87FFD"/> | <input type="text" value="192.168.10.9"/> |

**Remove** **Reload**

Type the specific Circuit ID, Remote ID and IP address, and then click **Add** to add a new binding rule for a specific client.

The description of the columns is as below:

| TERMS             | Description   |
|-------------------|---|
| <b>Circuit ID</b> | The Circuit ID of the device that wishes binding.                           |
| <b>Remote ID</b>  | The Remote ID of the device that wishes binding.                            |
| <b>IP Address</b> | The IP address that will assign to the device with the Binding MAC address. |

To remove from the binding list, select the index and click **Remove**. To refresh the list, click **Reload**.

## Option 82/IP Binding List

The figure below is the web interface for **Option 82/IP Binding List**.

Option82/IP Binding List

Circuit ID

Remote ID

IP Address

**Add**

| Index                      | Circuit ID                            | Remote ID                             | IP Address                                |
|----------------------------|---------------------------------------|---------------------------------------|---|
| <input type="checkbox"/> 1 | <input type="text" value="01000101"/> | <input type="text" value="COA87FFD"/> | <input type="text" value="192.168.10.9"/> |

**Remove** **Reload**

Type the specific Circuit ID, Remote ID and IP address, and then click **Add** to add a new binding rule for a specific client.

The description of the columns is as below:

| TERMS             | Description   |
|-------------------|---|
| <b>Circuit ID</b> | The Circuit ID of the device that wishes binding.                           |
| <b>Remote ID</b>  | The Remote ID of the device that wishes binding.                            |
| <b>IP Address</b> | The IP address that will assign to the device with the Binding MAC address. |

To remove from the binding list, select the index and click **Remove**. To refresh the list, click **Reload**.

## 3.1.5.2 DHCP Option 82

The DHCP Relay Agent (or DHCP Option 82) makes it possible for DHCP broadcast messages to be sent over routers. The DHCP Relay Agent enables DHCP clients to obtain IP addresses from a DHCP server on a remote subnet, or those that are not located on the local subnet.

**DHCP Option 82** is used by the relay agent to insert additional information into the client's DHCP request. The Relay Agent Information option is inserted by the DHCP relay agent when forwarding client-originated DHCP packets to a DHCP server. Servers can recognize the Relay Agent Information option and use the information to implement IP addresses to Clients.

When DHCP Option 82 is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address). Multiple hosts on the subscriber LAN can be connected to the same port on the access switch and are uniquely identified.

The Option 82 information contains 2 sub-options, Circuit ID and Remote ID, which define the relationship between the end device IP and the DHCP Option 82 server. The **Circuit ID** is a 4-byte number generated by the Ethernet switch—a combination of physical port number and VLAN ID.

### DHCP Option 82

DHCP Relay Agent Enable ▼

Submit

Helper Address

Helper Address

Add

|                          |                  |  |
|--------------------------|------------------|--|
| <input type="checkbox"/> | Helper Address 1 | <input type="text" value="192.168.10.19"/> |
| <input type="checkbox"/> | Helper Address 2 | <input type="text"/>                       |
| <input type="checkbox"/> | Helper Address 3 | <input type="text"/>                       |
| <input type="checkbox"/> | Helper Address 4 | <input type="text"/>                       |

Remove

The description of the columns is as below:

| TERMS                 | Description  |
|-----------------------|--|
| <b>DHCP Option 82</b> | Select to <b>Enable</b> or <b>Disable</b> to activate or deactivate DHCP relay agent function, and then select the modification type of option 82. |
| <b>Helper Address</b> | There are 4 fields for the DHCP server's IP address. Fill the field with preferred IP address of DHCP Server.                                      |

And click **Submit** to activate the DHCP relay agent function. All the DHCP packets from client will be modified by the

policy and forwarded to DHCP server through the gateway port. When **Option 82** is enabled on the switch, a subscriber device is identified by the switch port through which it connects to the network (in addition to its MAC address).

## Relay Policy

**Replace** - Replaces the existing option 82 field and adds new option 82 field. (This is the default setting).

**Keep** - Keeps the original option 82 field and forwards to server.

**Drop** - Drops the option 82 field and do not add any option 82 field.

**Relay Policy**

☒ Replace
 ☐ Keep
 ☐ Drop

Submit

## Circuit ID & Remote ID

The DHCP Option 82 information also contains 2 sub-options, **Circuit ID** and **Remote ID**, which define the relationship between the end device IP and the DHCP Option 82 server. The Circuit ID is a 4-byte number generated by the Ethernet switch. To activate this section, please make sure that DHCP Relay Agent is enabled.

**Circuit ID**

Port 1

☐ Default (VLAN/Port)
 ☐ User Defined

Submit

| Port | Circuit ID | HEX value |
|------|------------|-----------|
| 1    | 00010001   | 00010001  |
| 2    | 00010002   | 00010002  |
| 3    | 00010003   | 00010003  |
| 4    | 00010004   | 00010004  |
| 5    | 00010005   | 00010005  |
| 6    | 00010006   | 00010006  |
| 7    | 00010007   | 00010007  |
| 8    | 00010008   | 00010008  |
| 9    | 00010009   | 00010009  |
| 10   | 0001000a   | 0001000a  |

The format of the **Circuit ID** is shown above: 00-01-00-01, this is where the first byte is "00", the second and the third byte "01-00" is formed by the port VLAN ID, and the last byte "01" is formed by the port number. For example: 00-01-00-01 is the **Circuit ID** of port number 1 with port VLAN ID 1.



**Remote ID**  
☐ Default (MAC Address)  
☐ IP Address  
☐ User Defined

| Remote ID                                      | HEX value                                 |
|--|---|
| <input type="text" value="94:66:e7:9f:98:34"/> | <input type="text" value="9466e79f9834"/> |

The **Remote ID** identifies the relay agent itself and can be one of the following:

1. The IP address of the relay agent.
2. The MAC address of the relay agent.
3. A combination of IP address and MAC address of the relay agent.
4. A user-defined string.

### 3.1.5.3 DHCP Leased Entries

The figure below shows the **DHCP Leased Entries**. It will show the MAC and IP address that was assigned by switch.

**DHCP Leased Entries**

| Index                          | IP Address                                | MAC Address                                 | Leased Time Remains             |
|--------------------------------|---|---|---------------------------------|
| <input type="text" value="1"/> | <input type="text" value="192.168.10.3"/> | <input type="text" value="ac22.0b70.cd13"/> | <input type="text" value="55"/> |

Click the **Reload** button to refresh the list.

The description of the columns is as below:

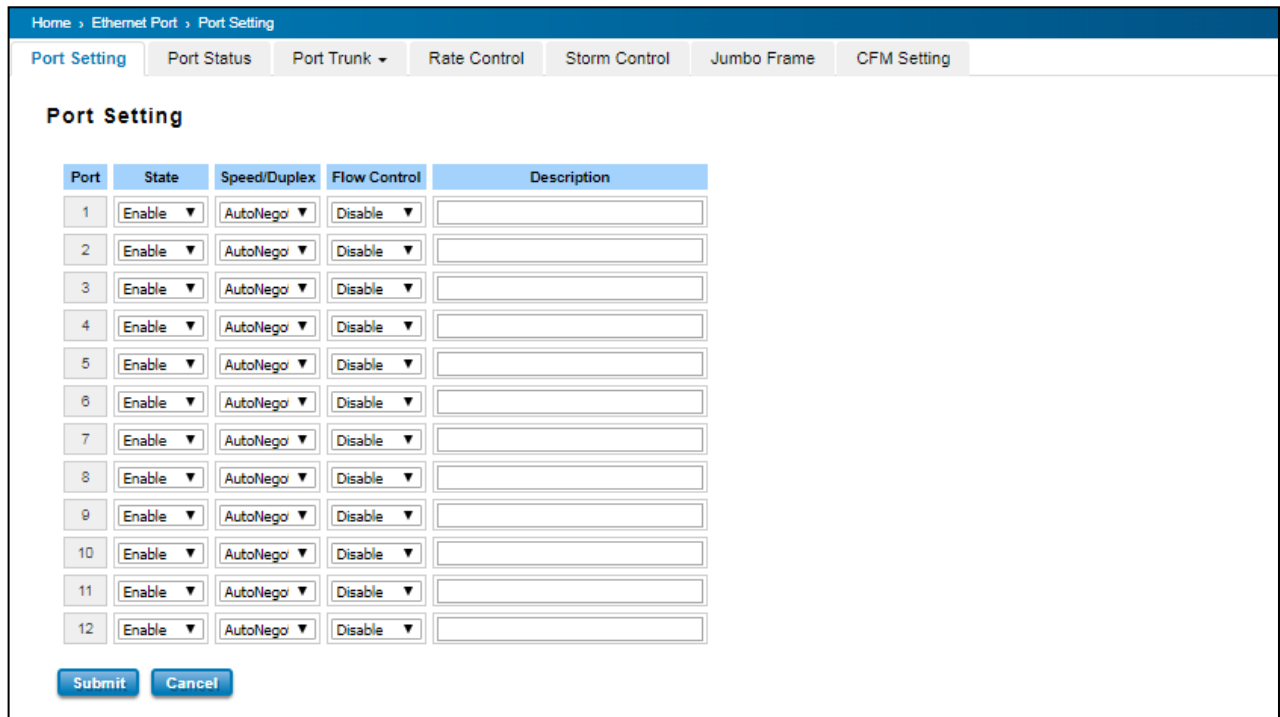
| TERMS               | Description                              |
|---------------------|--|
| IP Address          | IP address that was assigned by switch.  |
| MAC Address         | MAC address that was assigned by switch. |
| Leased Time Remains | Remains time for the IP address leased   |

## 3.2 ETHERNET PORT

Ethernet Port section is used to access the port configuration and rate limit control. It also allows User to view port status and port trunk information.

### 3.2.1 PORT SETTING

Port Settings section allows users to enable or disable each port function; state the speed/duplex of each port; and enable or disable the flow control of the port.



The description of the columns is as below:

| TERMS        | Description   |
|--------------|---|
| Port         | Shows port number   |
| State        | <b>Default: Enable</b><br>Enable or disable a port  |
| Speed/Duplex | <b>Default: AutoNegotiation</b><br>Users can set the bandwidth of each port as Auto-negotiation, 100 full,100 half,10 full,10 half mode for <b>Giga Ethernet Port 1~8 (ge1~ge8)</b> .<br>For <b>Gigabit Ethernet Fiber Port 9~12: (ge9~ge12)</b> , it can be set up to 100M Full Duplex(100 Full) only. |
| Flow Control | <b>Default: Disable</b><br><b>Enable</b> means that User need to activate the flow control function in order to let the flow control of that corresponding port on the switch to work. <b>Disable</b> means that User doesn't need to activate the flow control function, as the flow control of that   |

|             |  |
|-------------|--|
|             | corresponding port on the switch will work anyway. |
| Description | The description of interface.                      |

After finished configuring the settings, click on **Submit** to save the configuration.

## 3.2.2 PORT STATUS

Port Status provides current port status.

| Home > Ethernet Port > Port Status  |      |        |              |              |            |            |          |
|---|------|--------|--------------|--------------|------------|------------|----------|
| <div> Port Setting Port Status Port Trunk Rate Control Storm Control Jumbo Frame CFM Setting </div> |      |        |              |              |            |            |          |
| <b>Port Status</b>  |      |        |              |              |            |            |          |
| Port  | Link | State  | Speed/Duplex | Flow Control | SFP Vendor | Wavelength | Distance |
| 1   | Up   | Enable | 1000 Full    | Disable      | ---        | ---        | ---      |
| 2   | Down | Enable | ---          | Disable      | ---        | ---        | ---      |
| 3   | Down | Enable | ---          | Disable      | ---        | ---        | ---      |
| 4   | Down | Enable | ---          | Disable      | ---        | ---        | ---      |
| 5   | Down | Enable | ---          | Disable      | ---        | ---        | ---      |
| 6   | Down | Enable | ---          | Disable      | ---        | ---        | ---      |
| 7   | Down | Enable | ---          | Disable      | ---        | ---        | ---      |
| 8   | Down | Enable | ---          | Disable      | ---        | ---        | ---      |
| 9   | Down | Enable | ---          | Disable      | ---        | ---        | ---      |
| 10  | Down | Enable | ---          | Disable      | ---        | ---        | ---      |
| 11  | Down | Enable | ---          | Disable      | ---        | ---        | ---      |
| 12  | Down | Enable | ---          | Disable      | ---        | ---        | ---      |

## SFP DDM

Switch supports the SFP module with digital diagnostics monitoring (DDM) function. This technology allows the user to monitor real-time parameters of the fiber optic transceivers, like optical input/output power, temperature, and transceiver supply voltage of an SFP module via SFP DDM section. This section shows and configures the operational status, such as Scan/Eject the SFP, Enable/Disable SFP DDM, Temperature degree, Tx Power statistics, Rx Power Statistics in real time.

| SFP DDM                                      |                |         |                      |                |                |              |                |              |
|--|----------------|---------|----------------------|----------------|----------------|--------------|----------------|--------------|
| Port   | SFP Scan/Eject | SFP DDM | Temperature (degree) |                | Tx Power (dBm) |              | Rx Power (dBm) |              |
|  |                |         | Current              | Range          | Current        | Range        | Current        | Range        |
| 9  | ---            | Enat    | 34.00                | -10.00 - 80.00 | -5.3           | -9.0 - -1.5  | -0.9           | -24.1 - -3.0 |
| 10   | ---            | Enat    | 28.00                | -10.00 - 80.00 | -6.4           | -9.0 - -1.5  | -0.9           | -24.1 - -3.0 |
| 11   | ---            | Enat    | 39.00                | -45.00 - 90.00 | -6.5           | -10.0 - -1.0 | -8.9           | -26.0 - -2.0 |
| 12   | ---            | Enat    | 39.00                | -45.00 - 90.00 | -5.1           | -10.0 - -1.0 | -2.4           | -26.0 - -2.0 |
| <div> Reload Apply Scan All Eject All </div> |                |         |                      |                |                |              |                |              |

From the figure above, the real-time diagnostic parameters can be monitored to alert the system when the transceiver's

specified operating limits are exceeded and compliance cannot be ensured. Basically the SFP DDM has its own specification, as we can see from the table it is showed the temperature, Tx Power and Rx Power range. If all of the current values are higher or lower than the available range or does not meet the SFP vendor specification, there would be a problem for the fiber connection.

The description of the Port Status and SFP DDM columns is as below:

| TERMS          | Description   |
|----------------|---|
| SFP Scan/Eject | Scan the SFP module or Eject the SFP module.  |
| SFP DDM        | Enable/Disable the DDM function.  |
| Temperature    | The specific temperature range and current temperature detected of DDM SFP transceiver. |
| Tx Power (dBm) | The range and current transmit power of DDM SFP transceiver.                            |
| Rx Power (dBm) | The range and current received power of DDM SFP transceiver.                            |

Click **Reload** to reload the all port information, click **Scan All** to scan the SFP transceiver module and display the statistics. **Eject All** to eject the SFP transceiver that User has selected or plugged. User can eject one port or eject all by click the **Eject All** button. Click **Apply** to apply the configuration that just made.

### 3.2.3 PORT TRUNK

**Port Trunk**, also called “Link Aggregation”, is a method of combining multiple network connections in parallel to increase throughput beyond what a single connection could sustain. The aggregated ports can be viewed as one physical port so that the bandwidth is higher than merely one single Ethernet port. The member ports of the same trunk group can balance the loading and backup for each other. Managed switches support 2 types of Port Trunk. One is LACP (dynamic) and the other is Static. Link Aggregation Control Protocol (LACP), which is a protocol running on layer 2, provides a standardized means in accordance with IEEE 802.3ad to bundle several physical ports together to form a single logical channel. LACP mode is more flexible, and it can change modes, either trunk or single port. Dynamic Port Trunk also provides a redundancy function, in case one of the links fails. If one of the trunk members has failed, it will still work well in LACP mode, but it will link down if using static mode. All the ports within the logical channel or so-called logical aggregator work at the same connection speed and LACP operation requires full-duplex mode. Static mode is still necessary, because some devices only support static trunk.

#### Port Trunk Concept

Port trunking protocol that provides the following benefits:

- Flexibility in setting up User network connections, since the bandwidth of a link can be doubled, tripled, or quadrupled.
- Redundancy—if one link is broken, the remaining trunked ports share the traffic within this trunk group.
- Load sharing—MAC client traffic can be distributed across multiple links.

To avoid broadcast storms or loops in User network while configuring a trunk, first disable or disconnect all ports that User want to add to the trunk or remove from the trunk. After User finish configuring the trunk, enable or re-connect

the ports.

If all ports on both switch units are configured as 100BaseTX and they are operating in full duplex mode, this means that users can double, triple, or quadruple the bandwidth of the connection by port trunk between two switches.

When User activates port trunk, certain settings on each port will be reset to factory default values or disabled:

- Communication redundancy will be reset.
- 802.1Q VLAN will be reset.
- Multicast Filtering will be reset.
- Port Lock will be reset and disabled.
- Set Device IP will be reset.
- Mirror will be reset.

After port trunk has been activated, User can configure these items again for each trunk port.

## Port Trunk Setting



| Port | Group ID | Trunk Type |
|------|----------|------------|
| 1    | 0        | Static     |
| 2    | 0        | Static     |
| 3    | 0        | Static     |
| 4    | 0        | Static     |
| 5    | 0        | Static     |
| 6    | 0        | Static     |
| 7    | 0        | Static     |
| 8    | 0        | Static     |
| 9    | 0        | Static     |
| 10   | 0        | Static     |
| 11   | 0        | Static     |
| 12   | 0        | Static     |

The switch can support up to 8 trunk groups with 2 trunk members. Since the member ports should use same speed/duplex, max trunk members would be 8 for 100Mbps, and 2 members for Gigabit.

The description of the columns is as below:

| TERMS          | Description   |
|----------------|---|
| SFP Scan/Eject | <b>Group ID</b><br>Group ID is the ID for the port trunk group. Ports with same group ID are in the same group. |
| SFP DDM        | <b>Default: Blank</b>   |



|  |   |
|--|---|
|  | <b>Static</b> and <b>LACP</b> . Each Trunk Group can only support Static or LACP. Choose the type User need here. |
|--|---|

Click on **Submit** to apply the configuration, and **Reload** to refresh the table.

## Load Balance Setting

Load Balance Setting

| Group ID | Type          |
|----------|---------------|
| 1        | src-dst-mac ▼ |
| 2        | src-dst-mac ▼ |
| 3        | src-dst-mac ▼ |
| 4        | src-dst-mac ▼ |
| 5        | src-dst-mac ▼ |
| 6        | src-dst-mac ▼ |
| 7        | src-dst-mac ▼ |
| 8        | src-dst-mac ▼ |

**Load Balance Type:** Each Trunk Group can support several Load Balance types that can be seen from the table below:

| TERMS       | Description  |
|-------------|--|
| src-mac     | load distribution is based on the source MAC address                 |
| dst-mac     | load distribution is based on the destination-MAC address            |
| src-dst-mac | load distribution is based on the source and destination MAC address |
| src-ip      | load distribution is based on the source IP address                  |
| dst-ip      | load distribution is based on the destination IP address             |
| src-dst-ip  | load distribution is based on the source and destination IP address  |

Click **Submit** to apply your settings.

## Port Trunk Status

This page shows the status of port aggregation. Once the aggregation ports are negotiated well, User will see following status. The figure below is the Port Trunk Status interface.

Home > Ethernet Port > Port Trunk Status

Port Setting
Port Status
Rate Control
Port Trunk

### Port Trunk Status

| Group ID | Type   | Aggregated Ports | Individual Ports | Link Down Ports |
|----------|--------|------------------|------------------|-----------------|
| 1        | Static | 1                |                  | 2               |
| 2        | N/A    |                  |                  |                 |
| 3        | N/A    |                  |                  |                 |
| 4        | N/A    |                  |                  |                 |
| 5        | N/A    |                  |                  |                 |
| 6        | N/A    |                  |                  |                 |
| 7        | N/A    |                  |                  |                 |
| 8        | N/A    |                  |                  |                 |

Reload

The description of the columns is as below:

| TERMS                   | Description   |
|-------------------------|---|
| <b>Group ID</b>         | Display Trunk 1 to Trunk 5 setup in Aggregation Setting.  |
| <b>Type</b>             | Static or LACP setup in Aggregation Setting.  |
| <b>Aggregated Ports</b> | When LACP links well, User can see the member ports in aggregated column.   |
| <b>Individual Ports</b> | When LACP is enabled, member ports of LACP group which are not connected to correct LACP member ports will be displayed in the Individual column. |
| <b>Link Down</b>        | When LACP is enabled, member ports of LACP group which are not linked up will be displayed in the Link Down column.                               |

To refresh the list, click **Reload**.

## 3.2.4 RATE CONTROL

Rate control is a form of flow control used to enforce a strict bandwidth limit at a port. User can program separate transmit (Egress Rule) and receive (Ingress Rule) rate limits at each port, and even apply the limit to certain packet types.

Home > Ethernet Port > Rate Control

Port Setting
Port Status
Port Trunk
Rate Control
Storm Control
Jumbo Frame
CFM Setting

| Port | Ingress Rule(Kbps) | Egress Rule(Kbps) |
|------|--------------------|-------------------|
| 1    | 0                  | 0                 |
| 2    | 0                  | 0                 |
| 3    | 0                  | 0                 |
| 4    | 0                  | 0                 |
| 5    | 0                  | 0                 |
| 6    | 0                  | 0                 |
| 7    | 0                  | 0                 |
| 8    | 0                  | 0                 |
| 9    | 0                  | 0                 |
| 10   | 0                  | 0                 |
| 11   | 0                  | 0                 |
| 12   | 0                  | 0                 |

Submit

The description of the columns is as below:

| TERMS                              | Description   |
|------------------------------------|---|
| <b>Packet Type</b>                 | Select the packet type that wanted to filter.   |
| <b>Ingress</b>                     | The packet types of the Ingress Rule listed here include <b>Broadcast Only / Broadcast and multicast / Broadcast, Multicast and Unknown Unicast</b> or <b>All</b> .   |
| <b>Egress</b>                      | The packet types of the Egress Rule (outgoing) only support <b>all</b> packet types.  |
| <b>Rate (Ingress &amp; Egress)</b> | <b>Default value Ingress:0 Kbps</b><br><b>Default value Egress: 0 Kbps</b> (0 stands for disabling the rate control for the port.)<br>The step of the rate is 64kbps. |

Click on **Submit** to apply the configuration.

## 3.2.5 STORM CONTROL

A LAN storm appears when packets flood the LAN, creating excessive traffic and degrading network performance. Errors in the implementation, mistakes in network configuration, or users issuing a denial-of-service attack can cause a storm. Storm control prevents traffic on a LAN from being disrupted by a broadcast, DLF, or multicast storm on a port. In this page, user can configure the storm control for each port.

Home > Ethernet Port > Storm Control

Port Setting
Port Status
Port Trunk
Rate Control
**Storm Control**
Jumbo Frame
CFM Setting

| Port | Broadcast | Rate(packet/sec) | DLF     | Rate(packet/sec) | Multicast | Rate(packet/sec) |
|------|-----------|------------------|---------|------------------|-----------|------------------|
| 1    | Disable   | 0                | Disable | 0                | Disable   | 0                |
| 2    | Disable   | 0                | Disable | 0                | Disable   | 0                |
| 3    | Disable   | 0                | Disable | 0                | Disable   | 0                |
| 4    | Disable   | 0                | Disable | 0                | Disable   | 0                |
| 5    | Disable   | 0                | Disable | 0                | Disable   | 0                |
| 6    | Disable   | 0                | Disable | 0                | Disable   | 0                |
| 7    | Disable   | 0                | Disable | 0                | Disable   | 0                |
| 8    | Disable   | 0                | Disable | 0                | Disable   | 0                |
| 9    | Disable   | 0                | Disable | 0                | Disable   | 0                |
| 10   | Disable   | 0                | Disable | 0                | Disable   | 0                |
| 11   | Disable   | 0                | Disable | 0                | Disable   | 0                |
| 12   | Disable   | 0                | Disable | 0                | Disable   | 0                |

Submit

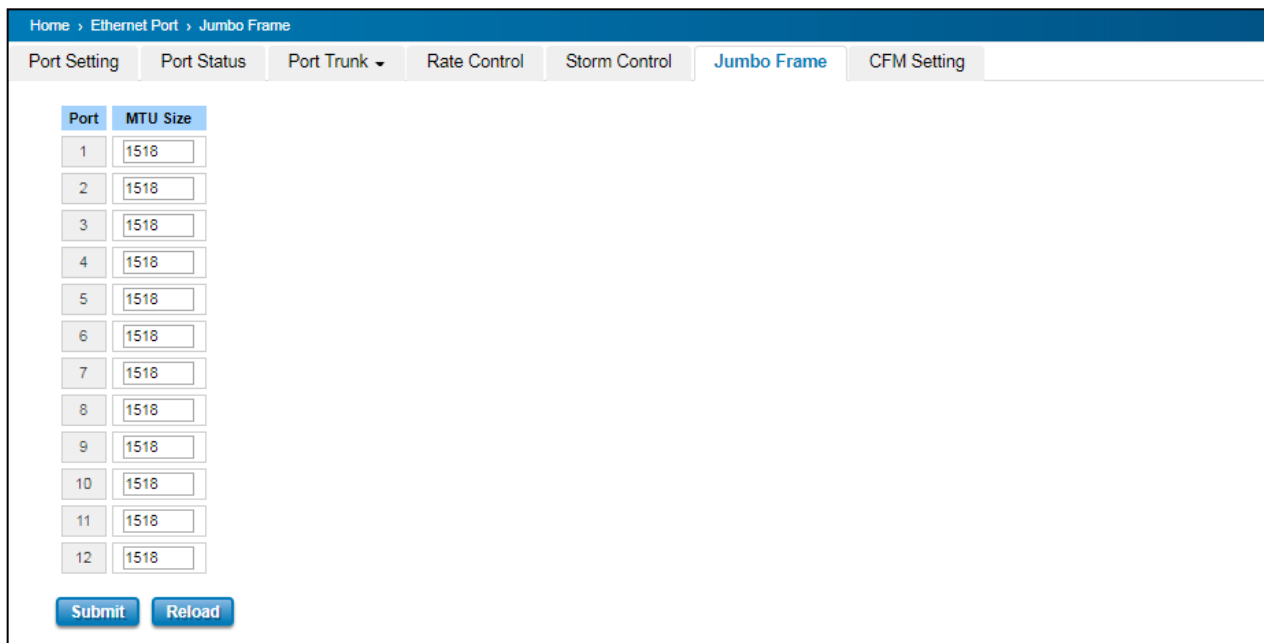
Click Submit to apply the configuration.

| TERMS            | Description  |
|------------------|--|
| <b>Broadcast</b> | Default: Disable<br>Set enable to control Broadcast Packets                  |
| <b>DLF</b>       | Default: Disable<br>Set enable to control Destination Lookup Failure packets |
| <b>Multicast</b> | Default: Disable   |

|                  |   |
|------------------|---|
|                  | Set enable to control Multicast Packets |
| Rate(Packet/Sec) | Rate limit value 0~262142 packet/sec    |

## 3.2.6 JUMBO FRAME

The switch allows user to configure the size of the Maximum Transmission Unit. The default value is 1,518bytes. The maximum Jumbo Frame size is 9,216 bytes.



Home > Ethernet Port > Jumbo Frame

Port Setting Port Status Port Trunk ▾ Rate Control Storm Control **Jumbo Frame** CFM Setting

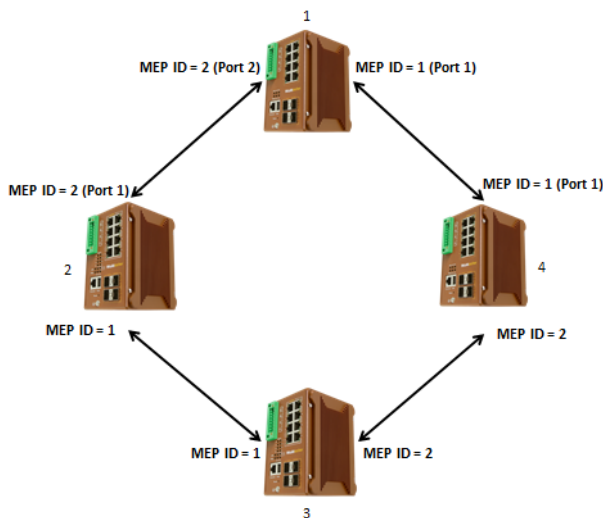
| Port | MTU Size |
|------|----------|
| 1    | 1518     |
| 2    | 1518     |
| 3    | 1518     |
| 4    | 1518     |
| 5    | 1518     |
| 6    | 1518     |
| 7    | 1518     |
| 8    | 1518     |
| 9    | 1518     |
| 10   | 1518     |
| 11   | 1518     |
| 12   | 1518     |

Submit Reload

## 3.2.7 CFM SETTING

Ethernet Connectivity Fault Management (CFM, IEEE 802.1ag) is an end-to-end Ethernet OAM that can cross multiple domains to monitor the health of the entire service instance. A service instance can be a native Ethernet VLAN. CFM is a connectivity checking mechanism that uses its own Ethernet frames (its Ethertype is 0x8902 and it has its own MAC address) to validate the health of the service instance.

Continuity Check Protocol (CCP): "Heartbeating" messages for CFM. The Continuity Check Message (CCM) provides a means to detect connectivity failures in an MA. CCMs are multicast messages. CCMs are confined to a domain (MD). These messages are unidirectional and do not solicit a response. Each MEP transmits a periodic multicast Continuity Check Message inward towards the other MEPs. The switch support Hardware CCM transition. The transition/receiving interval can up to 3.3ms to support detection Gigabit Ethernet cooper interface in 10ms.



The MEP ID in a link connection should be the same. For the example above the ERPS Ring, the port 1 from device one, the MEP ID is 1 and the port 1 from device 4, the MEP ID is also 1. In one device the MEP ID cannot be the same, it can be used only for a port. Below is the CFM CCP configuration page. In this page user may configure the Maintenance Domain, Maintenance Association and the Maintenance association End Point setting.

## Add Domain



Add the Domain name and the MD level then click **Add**.

| TERMS              | Description  |
|--------------------|--|
| <b>MD Level</b>    | Select the MD Level from 0~7<br>The eight levels range from 0 to 7. A hierarchical relationship exists between domains based on levels. The larger the domain, the higher the level value.<br>Recommended values of levels are as follows:<br>Customer Domain: Largest (e.g., 7)<br>Provider Domain: In between (e.g., 3)<br>Operator Domain: Smallest (e.g., 1) |
| <b>Domain Name</b> | Enter a new Domain Name. Domain name, maximum of 43 characters   |

## Add Association

Add Association

Domain Name

Association Name

VLAN

VLAN 1

Transmit Interval (ms)

3

Add

Choose the Domain Name from the list that has been added up then add a new Association Name for the Maintenance Association. After that choose the VLAN, Please create VLAN first, and each port set to be “tagged”

Add the Domain association name, end point type, port number and the MEP ID then click **Add**.

| TERMS            | Description  |
|------------------|--|
| Domain Name      | Choose the Domain Name that has been added                             |
| Association Name | Enter the Association Name. Association name, maximum of 45 characters |
| VLAN             | Choose VLAN that has been assigned                                     |
| Domain Name      | Enter a new Domain Name. Domain name, maximum of 43 characters         |

## Add Endpoint

Add Endpoint

Domain Association Name

Endpoint Type

Local Endpoint

Port

Port 1

MEP ID

1

Add

Points at the edge of the domain, define the boundary for the domain. A MEP sends and receives CFM frames through the relay function, drops all CFM frames of its level or lower that come from the wire side.

All of the configuration above will directly appear at the three tables below, Domain Table, Association Table and the Endpoint Table.

| TERMS                   | Description   |
|-------------------------|---|
| Domain Association Name | Choose the Domain Association Name that has been added  |
| Endpoint Type           | <b>Default: Local Endpoint</b><br>Choose between Local Endpoint and Remote Endpoint<br>Local Endpoint: Set the port as the Continuity Check Message (CCM) sender. |

|               |   |
|---------------|---|
|               | Remote Endpoint: Set the port as the Continuity Check Message (CCM) receiver. |
| <b>Port</b>   | <b>Default: Port 1</b><br>Choose port that need to be assigned                |
| <b>MEP ID</b> | <b>Default: 1</b><br>Choose the MEP ID. One MEP refer to one MEP ID           |

## Domain Table

**Domain Table**

|                          | Domain Name | MD Level |
|--------------------------|-------------|----------|
| <input type="checkbox"/> | 1           | 0        |

Remove Selected
Cancel

This section shows the Domain entry. User may delete the list, by select the list and click **Remove Selected**

## Association Table

**Association Table**

|                          | Domain Name | MD Level | Association Name | VLAN | Transmit Interval (ms) |
|--------------------------|-------------|----------|------------------|------|------------------------|
| <input type="checkbox"/> | 1           | 0        | 1                | 2    | 3 ▼                    |

Submit
Remove Selected
Cancel

This section shows the Association entry. In this table, user can configure the Configure Continuity Check Message transmit interval (default 3 ms), and after that click Submit to apply the setting. User may delete the list, by select the list and click **Remove Selected**

## Endpoint Table

This section shows the Endpoint entry. User may delete the list, by select the list and click **Remove Selected**

**Endpoint Table**

|                          | Domain Name | MD Level | Association Name | Port | Endpoint Type | MEP ID |
|--------------------------|-------------|----------|------------------|------|---------------|--------|
| <input type="checkbox"/> | 1           | 0        | 1                | 1    | Remote        | 1      |

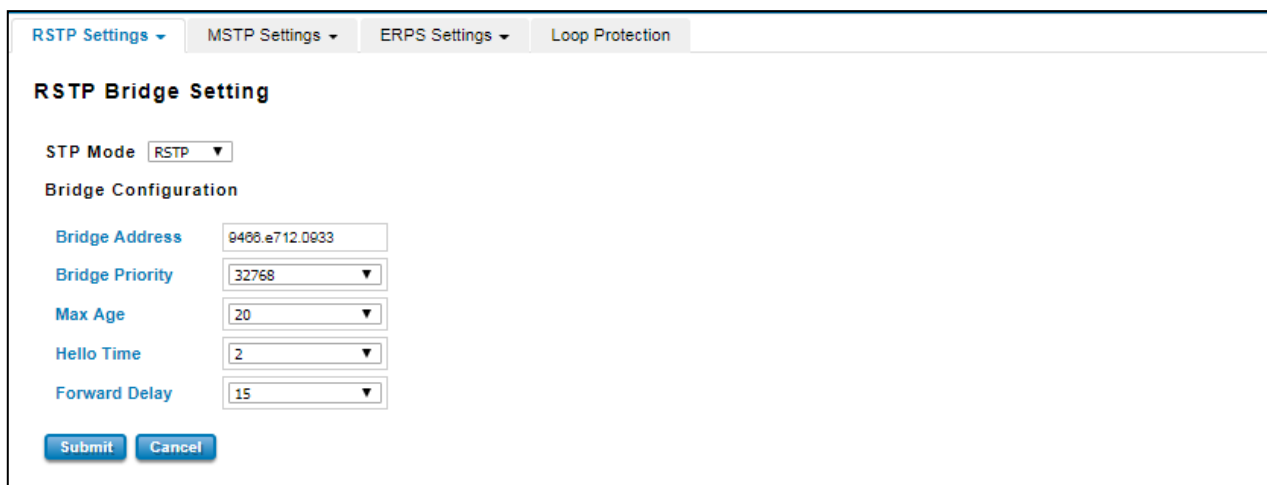
Remove Selected
Cancel

## 3.3 REDUNDANCY

Redundancy role on the network is to help protect critical links against failure, protects against network loops, and keeps network downtime at a minimum. Sustainable, uninterrupted data communication network is critical for industrial applications. Network Redundancy allows user to set up redundant loops in the network to provide a backup data transmission route in the event that a cable is inadvertently disconnected or damaged. This switch supports Rapid Spanning Tree Protocol (RSTP)/Multiple Spanning Tree Protocol (MSTP) and ITU-T G.8032 v1/v2 Ethernet Ring Protection Switching (ERPS). ERPS (Ethernet Ring Protection Switching) or ITU-T G.8032 is a loop resolution protocol, just like STP. Convergence time is much quicker in ERPS. Unlike in STP, most of the ERPS parameters are management configured – which link to block in the start etc. Normally ERPS is implemented with-in the same administrator domain, there by having control on the nodes participating in the Ring. This technology provides sub-50ms protection and recovery switching for Ethernet traffic. This is a particularly important feature for industrial applications, since it could take several minutes to locate the disconnected or severed cable.

### 3.3.1 RSTP SETTINGS

This page allows select the RSTP mode and configuring the global RSTP Bridge Configuration.



**RSTP Bridge Setting**

STP Mode: RSTP

Bridge Configuration

Bridge Address: 0408.e712.0933

Bridge Priority: 32768

Max Age: 20

Hello Time: 2

Forward Delay: 15

Submit Cancel

The STP mode includes the **STP**, **RSTP**, **MSTP** and **Disable**. User can select the STP mode for user system first. The default mode is RSTP enabled. After user selects the STP or RSTP mode; user should continue to configure the global Bridge parameters for STP and RSTP. If user selects the MSTP mode, user need go to MSTP Configuration page.

#### **Spanning Tree Protocol (STP)**

STP is a Layer 2 link management protocol that provides path redundancy while preventing loops in the network. For a Layer 2 Ethernet network to function properly, only one active path can exist between any two stations. Spanning-tree operation is transparent to end stations, which cannot detect whether they are connected to a single LAN segment or a switched LAN of multiple segments

If the destination from a switch is more than one path, it will lead to looping condition that can generate broadcast



storms in a network. The spanning tree was created to combat the negative effects of message loops in switched networks. A spanning tree algorithm is used to automatically sense whether a switch has more than one way to communicate with a node. It will then select the best path, and block the other path. Spanning Tree Protocol (STP) introduced a standard method to accomplish this. Rapid Spanning Tree Protocol (RSTP) was adopted and represents the evolution of STP, providing much faster spanning tree convergence after a topology change.

## ***MSTP (Multiple Spanning Tree Protocol)***

MSTP is a direct extension of RSTP that can provide an independent spanning tree for different VLANs. It simplifies network management by limiting the size of each region, and prevents VLAN members from being segmented from the group. MSTP can provide multiple forwarding paths and enable load balancing. By understand the architecture, allow you effectively maintain and operate the correct spanning tree. One VLAN can be mapped to an instance. The maximum Instance of the switch is 16, with the range is from 0-15. The MSTP builds a separate Multiple Spanning Tree (MST) for each instance to maintain connectivity among each of the assigned VLAN groups. An Internal Spanning Tree (IST) is used to connect all the MSTP switches within an MST region. An MST Region may contain multiple MSTP Instances.

MSTP connects all bridges and LAN segments with a single Common and Internal Spanning Tree that is formed as a result of the running spanning tree algorithm between switches that support the STP, RSTP, MSTP protocols.

To configure the MSTP setting, the STP Mode of the RSTP Settings page should be changed to MSTP mode first. After enabled MSTP mode, user can go to the MSTP Settings page

## **Bridge Configuration**

**Bridge Address:** This shows the switch's MAC address.

**Priority (0-61440):** RSTP uses bridge ID to determine the root bridge, the bridge with the highest bridge ID becomes the root bridge. The bridge ID is composed of bridge priority and bridge MAC address. So that the bridge with the highest priority becomes the highest bridge ID. If all the bridge ID has the same priority, the bridge with the lowest MAC address will then become the root bridge.

### **NOTE:**

1. The bridge priority value must be in multiples of 4096. A device with a lower number has a higher bridge priority.
2. The Web GUI allows user selects the priority number directly. This is the convenient of the GUI design. When user configures the value through the CLI or SNMP, user may need to type the value directly. Please follow the  $n \times 4096$  rules for the Bridge Priority.

**Max Age (6-40):** Enter a value from 6 to 40 seconds here. This value represents the time that a bridge will wait without receiving Spanning Tree Protocol configuration messages before attempting to reconfigure.

**Hello Time (1-10):** Enter a value from 1 to 10 seconds here. This is a periodic timer that drives the switch to send out BPDU (Bridge Protocol Data Unit) packet to check current STP status. The root bridge of the spanning tree topology

periodically sends out a **hello** message to other devices on the network to check if the topology is normal. The **hello time** is the amount of time the root has waited during sending hello messages.

**Forward Delay Time (4-30):** Enter a value between 4 and 30 seconds. This value is the time that a port waits before changing from Spanning Tree Protocol learning and listening states to forwarding state.

Once user has completed user configuration, click on **Submit** to apply user settings.

**NOTE:** User must follow the rule to configure Hello Time, Forwarding Delay, and Max Age parameters.

$$2 \times (\text{Forward Delay Time} - 1 \text{ sec}) \geq \text{Max Age Time} \geq 2 \times (\text{Hello Time value} + 1 \text{ sec})$$

## RSTP Port Settings

Select the port user wants to configure and user will be able to view current setting and status of the port.

RSTP Settings ▾
MSTP Settings ▾
ERPS Settings ▾
Loop Protection

### RSTP Port Setting

| Port | STP State | Path Cost | Port Priority | Link Type | Edge Port |
|------|-----------|-----------|---------------|-----------|-----------|
| 1    | Enable ▾  | 200000    | 128 ▾         | Auto ▾    | Enable ▾  |
| 2    | Enable ▾  | 200000    | 128 ▾         | Auto ▾    | Enable ▾  |
| 3    | Enable ▾  | 200000    | 128 ▾         | Auto ▾    | Enable ▾  |
| 4    | Enable ▾  | 200000    | 128 ▾         | Auto ▾    | Enable ▾  |
| 5    | Enable ▾  | 200000    | 128 ▾         | Auto ▾    | Enable ▾  |
| 6    | Enable ▾  | 200000    | 128 ▾         | Auto ▾    | Enable ▾  |
| 7    | Enable ▾  | 200000    | 128 ▾         | Auto ▾    | Enable ▾  |
| 8    | Enable ▾  | 200000    | 128 ▾         | Auto ▾    | Enable ▾  |
| 9    | Enable ▾  | 200000    | 128 ▾         | Auto ▾    | Enable ▾  |
| 10   | Enable ▾  | 200000    | 128 ▾         | Auto ▾    | Enable ▾  |

Submit
Cancel

The description of the columns is as below:

| TERMS            | Description   |
|------------------|---|
| <b>STP State</b> | <b>Default: Enable</b><br>To enable or disable STP function.  |
| <b>Path Cost</b> | Enter a number between 1 and 200,000,000. This value represents the “ <b>cost</b> ” of the path to the other bridge from the transmitting bridge at the specified port.   |
| <b>Priority</b>  | Enter a value between 0 and 240, using multiples of 16. This is the value that decides which port should be blocked by priority in a LAN.   |
| <b>Link Type</b> | There are 3 types for user selects <b>Auto</b> , <b>P2P</b> and <b>Share</b> . Some of the rapid state transitions that are possible within RSTP depend upon whether the port of concern can only be connected to another bridge (i.e. it is served by a point-to-point LAN segment), |

|                  |   |
|------------------|---|
|                  | <p>or if it can be connected to two or more bridges (i.e. it is served by a shared-medium LAN segment). This function allows link status of the link to be manipulated administratively. <b>Auto</b> - means to auto select P2P or Share mode.</p> <p><b>P2P</b> - means P2P is enabled; the 2 ends work in full duplex mode.</p> <p><b>Share</b> - means P2P is disabled; the 2 ends may connect through a share media and work in half duplex mode.</p> |
| <b>Edge Port</b> | <p>A port directly connected to the end stations cannot create a bridging loop in the network. To configure this port as an edge port, set the port to the <b>Enable</b> state. When the non-bridge device connects an admin edge port, this port will be in blocking state and turn to forwarding state in 4 seconds.</p>  |

Once user finished user configuration, click on **Submit** to save user settings.

## RSTP Status

This page allows user to see the information of the root switch and port status.

RSTP Settings ▾
MSTP Settings ▾
ERPS Settings ▾
Loop Protection

### RSTP Status

**Root Status**

|                |                |
|----------------|----------------|
| Root Address   | 9486.e712.0933 |
| Root Priority  | 32768          |
| Root Port      | N/A            |
| Root Path Cost | 0              |
| Max Age        | 20 second(s)   |
| Hello Time     | 2 second(s)    |
| Forward Delay  | 15 second(s)   |

**Root Status:** User can see root Bridge ID, Root Priority, Root Port, Root Path Cost and the Max Age, Hello Time and Forward Delay of BPDU sent from the root switch.

| Port Status |          |            |           |               |           |           |                     |
|-------------|----------|------------|-----------|---------------|-----------|-----------|---------------------|
| Port        | Role     | Port State | Path Cost | Port Priority | Link Type | Edge Port | Aggregated(ID/Type) |
| 1           | Disabled | Disabled   | 200000    | 128           | P2P       | Edge      | /                   |
| 2           | Disabled | Blocking   | 200000    | 128           | P2P       | Edge      | /                   |
| 3           | Disabled | Blocking   | 200000    | 128           | P2P       | Edge      | /                   |
| 4           | Disabled | Disabled   | 200000    | 128           | P2P       | Edge      | /                   |
| 5           | Disabled | Disabled   | 200000    | 128           | P2P       | Edge      | /                   |
| 6           | Disabled | Disabled   | 200000    | 128           | P2P       | Edge      | /                   |
| 7           | Disabled | Disabled   | 200000    | 128           | P2P       | Edge      | /                   |
| 8           | Disabled | Disabled   | 200000    | 128           | P2P       | Edge      | /                   |
| 9           | Disabled | Disabled   | 20000     | 128           | P2P       | Edge      | /                   |
| 10          | Disabled | Disabled   | 20000     | 128           | P2P       | Edge      | /                   |

Reload

**Port Status:** User can see port Role, Port State, Path Cost, Port Priority, Oper P2P mode, Oper edge port mode and

Aggregated (ID/Type).

## 3.3.2 MSTP SETTINGS

### MSTP Region Configuration

MSTP Setting

MSTP Region Configuration

Region Name

Revision

Submit

Cancel

This page allows configure the Region Name and its Revision, mapping the VLAN to Instance and check current MST Instance configuration. The network can be divided virtually to different Regions. The switches within the Region should have the same Region and Revision level.

| TERMS       | Description  |
|-------------|--|
| Region Name | The name for the Region. Maximum length: 32 characters.          |
| Revision    | <b>Default: 0</b><br>The revision for the Region. Range: 0-65535 |

Once user finished user configuration, click on **Submit** to apply user settings.

### Add MSTP Instance

Add MSTP Instance

Instance ID

VLAN Group

Instance Priority

Add

This page allows mapping the VLAN to Instance and assign priority to the instance. Before mapping VLAN to Instance, user should create VLAN and assign the member ports first. Please refer to the VLAN setting page. **After** finish the configuration, click on **Add** to apply user settings.

| TERMS             | Description   |
|-------------------|---|
| Instance ID       | Select the Instance ID, the available number is 1-15.     |
| VLAN Group        | Type the VLAN ID that user wants mapping to the instance. |
| Instance Priority | Assign the priority to the instance. (0-61440)            |

### MST Instance Configuration

This page allows user to see the current MST Instance Configuration user added. Click on **Submit** to apply the setting.

User can **Remove** the instance in this page.

**MSTP Instance Configuration**

| Instance ID                | VLAN Group                     | Instance Priority                  |
|----------------------------|--------------------------------|------------------------------------|
| <input type="checkbox"/> 1 | <input type="text" value="1"/> | <input type="text" value="32768"/> |

## MSTP Port Setting

This page allows configure the Port settings. Choose the Instance ID user wants to configure. The MSTP enabled and linked up ports within the instance will be listed in this table. Note that the ports not belonged to the Instance, or the ports not MSTP activated will not display. The meaning of the Path Cost, Priority, Link Type and Edge Port is the same as the definition of RSTP.

RSTP Settings ▾
MSTP Settings ▾
ERPS Settings ▾
Loop Protection

Instance ID

| Port | Path Cost                           | Port Priority                    | Link Type                         | Edge Port                           |
|------|-------------------------------------|----------------------------------|-----------------------------------|-------------------------------------|
| 1    | <input type="text" value="200000"/> | <input type="text" value="128"/> | <input type="text" value="Auto"/> | <input type="text" value="Enable"/> |
| 2    | <input type="text" value="200000"/> | <input type="text" value="128"/> | <input type="text" value="Auto"/> | <input type="text" value="Enable"/> |
| 3    | <input type="text" value="200000"/> | <input type="text" value="128"/> | <input type="text" value="Auto"/> | <input type="text" value="Enable"/> |
| 4    | <input type="text" value="200000"/> | <input type="text" value="128"/> | <input type="text" value="Auto"/> | <input type="text" value="Enable"/> |
| 5    | <input type="text" value="200000"/> | <input type="text" value="128"/> | <input type="text" value="Auto"/> | <input type="text" value="Enable"/> |
| 6    | <input type="text" value="200000"/> | <input type="text" value="128"/> | <input type="text" value="Auto"/> | <input type="text" value="Enable"/> |
| 7    | <input type="text" value="200000"/> | <input type="text" value="128"/> | <input type="text" value="Auto"/> | <input type="text" value="Enable"/> |
| 8    | <input type="text" value="200000"/> | <input type="text" value="128"/> | <input type="text" value="Auto"/> | <input type="text" value="Enable"/> |
| 9    | <input type="text" value="20000"/>  | <input type="text" value="128"/> | <input type="text" value="Auto"/> | <input type="text" value="Enable"/> |
| 10   | <input type="text" value="20000"/>  | <input type="text" value="128"/> | <input type="text" value="Auto"/> | <input type="text" value="Enable"/> |

The description of the columns is as below:

| TERMS                | Description   |
|----------------------|---|
| <b>Path Cost</b>     | Enter a number between 1 and 200,000,000. This value represents the cost of the path to the other bridge from the transmitting bridge at the specified port. Path cost value is derived from the media speed of an interface. If a loop occurs, the MSTP uses cost when selecting an interface to put in the forwarding state. Lower cost values can be assigned to interfaces that selected first and higher cost values that selected last. If all interfaces have the same cost value, the MSTP puts the interface with the lowest interface number in the forwarding state and blocks the other interfaces. |
| <b>Port Priority</b> | Enter a value between 0 and 240. This is the value that decides which port should be blocked by priority in a LAN.  |

|                  |   |
|------------------|---|
| <b>Link Type</b> | <p>There are 3 types for user selects <b>Auto</b>, <b>P2P</b> and <b>Share</b>. Some of the rapid state transitions that are possible within RSTP depend upon whether the port of concern can only be connected to another bridge (i.e. it is served by a point-to-point LAN segment), or if it can be connected to two or more bridges (i.e. it is served by a shared-medium LAN segment). This function allows link status of the link to be manipulated administratively. <b>Auto</b> - means to auto select P2P or Share mode.</p> <p><b>P2P</b> - means P2P is enabled; the 2 ends work in full duplex mode.</p> <p><b>Share</b> - means P2P is disabled; the 2 ends may connect through a share media and work in half duplex mode.</p> |
| <b>Edge Port</b> | <p>A port directly connected to the end stations cannot create a bridging loop in the network. To configure this port as an edge port, set the port to the <b>Enable</b> state. When the non-bridge device connects an admin edge port, this port will be in blocking state and turn to forwarding state in 4 seconds.</p>  |

Once user finished user configuration, click on **Submit** to save user settings.

## MSTP Status

This page allows user to see the current MSTP status. Choose the **Instance ID** first. If the instance is not added, the information remains blank. The **Root Information** shows the setting of the Root switch.

**MSTP Status**

Instance ID 0 ▼

**Root Status**

|                |                |
|----------------|----------------|
| Root Address   | 9466.e712.0933 |
| Root Priority  | 32768          |
| Root Port      | N/A            |
| Root Path Cost | 0              |
| Max Age        | 20             |
| Hello Time     | 2              |
| Forward Delay  | 15             |

**Root Status:** User can see Root Address, Root Priority, Root Port, Root Path Cost and the Max Age, Hello Time and Forward Delay of BPDU sent from the root switch based on the Instance ID.

**Port Status**

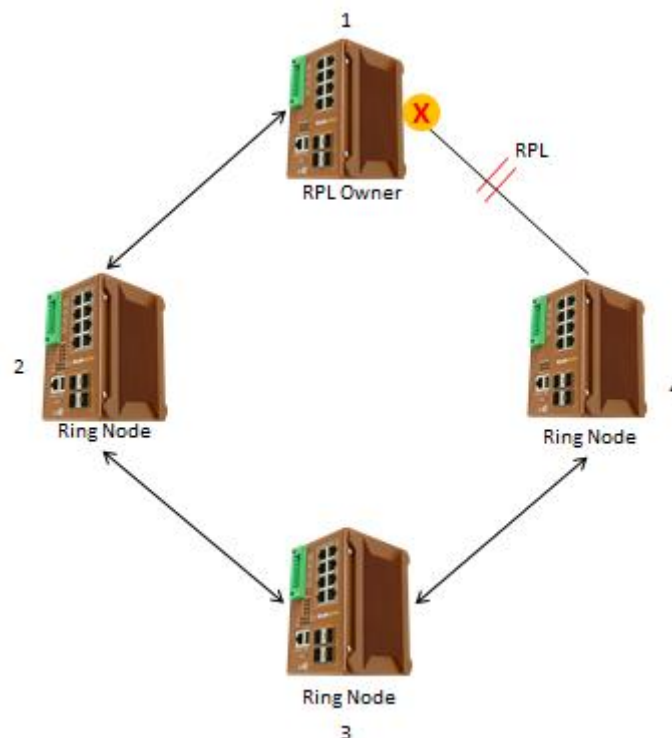
| Port | Role       | Port State | Path Cost | Port Priority | Link Type | Edge Port |
|------|------------|------------|-----------|---------------|-----------|-----------|
| 1    | Disabled   | Blocking   | 200000    | 128           | P2P       | Edge      |
| 2    | Designated | Forwarding | 200000    | 128           | P2P       | Edge      |
| 3    | Designated | Forwarding | 200000    | 128           | P2P       | Edge      |
| 4    | Disabled   | Blocking   | 200000    | 128           | P2P       | Edge      |
| 5    | Designated | Forwarding | 200000    | 128           | P2P       | Edge      |
| 6    | Disabled   | Blocking   | 200000    | 128           | P2P       | Edge      |
| 7    | Designated | Forwarding | 200000    | 128           | P2P       | Edge      |
| 8    | Disabled   | Blocking   | 200000    | 128           | P2P       | Edge      |
| 9    | Disabled   | Blocking   | 20000     | 128           | P2P       | Edge      |
| 10   | Disabled   | Blocking   | 20000     | 128           | P2P       | Edge      |

Reload

**ort Status:** User can see port Role, Port State, Path Cost, Port Priority, Link Type and the Edge Port within the instance.  
Click **Reload** to refresh the information display.

### 3.3.3 ERPS SETTINGS

Ethernet Ring Protection Switching (ERPS) is a protocol for Ethernet layer network rings. The protocol specifies the protection mechanism for sub-50ms delay time. The ring topology provides multipoint connectivity economically by reducing the number of links. ERPS provides highly reliable and stable protection in the ring topology, and it never forms loops, which can affect network operation and service availability.



The figure above shows that each Ethernet Ring Node is connected to other Ethernet Ring Nodes that participating in the same Ethernet Ring using two independent links. In the Ethernet ring, loops can be avoided by guaranteeing that traffic may flow on all but one of the ring links at any time. This particular link is called Ring Protection Link (RPL). A control message called Ring Automatic Protection Switch (R-APS) coordinates the activities of switching on/off the RPL. Under normal conditions, this link is blocked by the Owner Node. Thus, loops can be avoided by this mechanism. In case an Ethernet ring failure occurs, one designated Ethernet Ring Node called the RPL Owner Node will be responsible for unblocking its end of the RPL to allow RPL to be used as a backup link. The RPL is the backup link when one link failure occurs.

Managed switches provide a number of Ethernet ring protocol. The ERPS/Ring section is subdivided into two menus, which are: ERPS Setting and ERPS Status.

#### 3.3.3.1 ERPS SETTINGS

##### ERPS Setting

**ERPS Setting**

**Add ERPS Instance**

Instance ID

VLAN group

0 ▼

Add

**ERPS Instance Setting**

Instance ID

VLAN group

1

1

Submit

Remove Selected

Cancel

**Add ERPS Instance** is a section for mapping the VLAN to Instance. Before mapping VLAN to Instance, user should create VLAN and assign the member ports first. Please refer to the VLAN setting page.

After click the **Add** button, the Instance ID and the VLAN group information will directly display in the **ERPS Instance Setting** section.

| TERMS       | Description   |
|-------------|---|
| Instance ID | Select the Instance ID, the available number is 1-15.     |
| VLAN Group  | Type the VLAN ID that user wants mapping to the instance. |

## Add ERPS Ring

**Add ERPS Ring**

Ring ID

0 ▼

Add

**ERPS Ring Setting**

| Ring ID | Version | Ring State | Node Role   | Control Channel | Sub Ring without Virtual Channel | Virtual Channel of Sub Ring | Ring Port 0 | Ring Port 1 | RPL port | Revertive Mode | Instance | Manual Switch | Force Switch |
|---------|---------|------------|-------------|-----------------|----------------------------------|-----------------------------|-------------|-------------|----------|----------------|----------|---------------|--------------|
| 1       | v2 ▼    | Enable ▼   | Ring Node ▼ | 1 ▼             | False ▼                          | 1 ▼                         | 2 ▼         | 3 ▼         | 1 ▼      | Revertive ▼    | 1 ▼      | None ▼        | None ▼       |

Submit

Remove Selected

Clear Selected

Cancel

**Add ERPS Ring** is a section to add the Ring ID of the created Protection group; it must be an integer value between 0 and 31. The maximum numbers of ERPS Protection Groups that can be created are 32. Click the ID of a Protection group to enter the configuration page. After click Add button, one line will be directly created in the **ERPS Ring Setting** section. The ERPS Ring Setting section is a table that used to set up the ERPS Ring configuration.



Below is the description table.

| TERMS                            | Description   |
|----------------------------------|---|
| Ring ID                          | Display the Ring ID   |
| Version                          | ERPS Protocol Version - v1 or v2.   |
| Ring State                       | <b>Default: Disable</b><br>Enable - Ring Status is enable<br>Disable - Ring Status is disable   |
| Node Role                        | It can be either RPL owner or RPL Neighbor or Ring Node.  |
| Control Channel                  | <b>Default: 1</b><br>Control channel is implemented using a VLAN. Each ERP instance uses a tag-based VLAN for sending and receiving R-APS messages. (1-4094)  |
| Sub Ring without Virtual Channel | <b>Default: False</b><br><b>True</b> – if doesn't have a virtual channel<br><b>False</b> – if have any virtual channel  |
| Virtual Channel of Sub Ring      | <b>Default: 1</b><br>Sub-rings can have a virtual channel on the interconnected node. Choose the number based on the VLANs Range (1-4094)   |
| Ring Port 0                      | This will create a Port 0 of the switch in the Ring. Choose the port number that belongs to Ring port 0   |
| Ring Port 1                      | This will create Port 1 of the switch in the Ring. As interconnected sub-ring will have only one ring port, "Port 1" is configured as "0" for interconnected sub-ring. "0" in this field indicates that no "Port 1" is associated with this instance. Choose the port number that belongs to Ring port 1.   |
| Ring Port 0 RMEP ID              | <b>Default: None</b><br>The remote MEP id that CFM monitored of ERPS ring port detection. (Range 1 -8191). Please check the CFM Setting (MEP ID)  |
| Ring Port 1 RMEP ID              | <b>Default: None</b><br>The remote MEP id that CFM monitored of ERPS ring port detection. (Range 1 -8191). Please Check the CFM Setting (MEP ID).   |
| RPL Port                         | This allows you to select the Ring Port 0 or Ring Port 1 as the RPL block.  |
| Revertive Mode                   | <b>Default: Revertive</b><br><b>Revertive mode</b> , after the conditions causing a protection switch has cleared; the traffic channel is restored to the working transport entity that is blocked on the RPL. In <b>Non-Revertive mode</b> , the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared. |
| Instance                         | Select the Instance ID, the available number is 1-15.   |
| Manual Switch                    | <b>Default: None</b>  |

|                     |  |
|---------------------|--|
|                     | <p>In the absence of a failure or FS, Manual Switch command forces a block on the ring port where the command is issued.</p> <p>Choose 0 or 1, refers to Ring Port 0 or Ring Port 1.</p> |
| <b>Force Switch</b> | <p><b>Default: None</b></p> <p>Forced Switch command forces a block on the ring port where the command is issued.</p> <p>Choose 0 or 1, refers to Ring Port 0 or Ring Port 1.</p>        |

## ERPS Timer Setting

**ERPS Timer Setting**

| Ring ID | Guard Timer(ms) | WTR Timer(m) |
|---------|-----------------|--------------|
| 1       | 100 ▼           | 5 ▼          |

| TERMS                   | Description  |
|-------------------------|--|
| <b>Guard Timer (ms)</b> | Guard timeout value to be used to prevent ring nodes from receiving outdated R-APS messages. The period of the guard timer can be configured in 10 ms steps between 10 ms and 2000 ms, with a default value of 100 ms. |
| <b>WTR Timer (m)</b>    | The Wait To Restore timing value to be used in revertive switching. The period of the WTR time can be configured by the operator in 1 minute steps between 1 and 12 minutes with a default value of 5 minutes.         |

## 3.3.3.2 ERPS STATUS

In this section, user can check the ERPS Status, Timer Status and Statistics from the Ring.

**ERPS Status**

| Ring ID | Version | Ring State | Ring Type  | Node State | Node Role | Control Channel | Sub Ring without Virtual Channel | Virtual Channel of Sub Ring | Ring Port 0          | Ring Port 1        | Ring Port 0 RMEP ID | Ring Port 1 RMEP ID | RPL Port | Revertive Mode | Manual Switch | Forced Switch |
|---------|---------|------------|------------|------------|-----------|-----------------|----------------------------------|-----------------------------|----------------------|--------------------|---------------------|---------------------|----------|----------------|---------------|---------------|
| 0       | v2      | Enabled    | Major Ring | Idle       | RPL Owner | 1               | False                            | 2                           | Link Up / Forwarding | Link Up / Blocking | None                | None                | 1        | Revertive      |               |               |

| TERMS             | Description  |
|-------------------|--|
| <b>Ring ID</b>    | Display the Ring ID  |
| <b>Version</b>    | ERPS Protocol Version - v1 or v2.  |
| <b>Ring State</b> | <p><b>Default: Disable</b></p> <p>Enabled - Ring Status is enable</p> <p>Disabled - Ring Status is disable</p> |

|   |  |
|---|--|
| <b>Node State</b>                       | Status from the <b>Ring is Idle, Protection, Manual Switch, Force Switch</b> or <b>Pending</b> .   |
| <b>Node Role</b>                        | It can be either <b>RPL owner</b> or <b>RPL Neighbor</b> or <b>Ring Node</b> .   |
| <b>Control Channel</b>                  | Control Channel is referred to the VLANs number (1-4094)   |
| <b>Sub Ring without Virtual Channel</b> | <b>Default: False</b><br><b>True</b> – if have a virtual channel<br><b>False</b> – if doesn't have any virtual channel   |
| <b>Virtual Channel of Sub Ring</b>      | <b>Default: 1</b><br>Sub-rings can have a virtual channel on the interconnected node. Choose the number based on the VLANs Range (1-4094)  |
| <b>Ring Port 0</b>                      | The status from the port Link up/link down and Forwarding/Blocking   |
| <b>Ring Port 1</b>                      | The status from the port Link up/link down and Forwarding/Blocking   |
| <b>Ring Port 0 RMEP ID</b>              | Show the remote MEP id that CFM monitored of ERPS ring port detection.   |
| <b>Ring Port 1 RMEP ID</b>              | Show the remote MEP id that CFM monitored of ERPS ring port detection.   |
| <b>RPL Port</b>                         | The port status as the RPL block.  |
| <b>Revertive Mode</b>                   | <b>Default: Revertive</b><br><b>Revertive mode</b> , after the conditions causing a protection switch has cleared; the traffic channel is restored to the working transport entity that is, blocked on the RPL. In <b>Non-Revertive mode</b> , the traffic channel continues to use the RPL, if it is not failed, after a protection switch condition has cleared. |
| <b>Manual Switch</b>                    | Status from the Ring Port 0 and 1 or None  |
| <b>Force Switch</b>                     | Status from the Ring Port 0 and 1 or None  |

## Timer Status

| Timer Status |                 |                          |                      |                 |                      |                      |                   |                        |                        |
|--------------|-----------------|--------------------------|----------------------|-----------------|----------------------|----------------------|-------------------|------------------------|------------------------|
| Ring ID      | WTR Timer State | WTR Timer Period(minute) | WTR Timer Remain(ms) | WTB Timer State | WTB Timer Period(ms) | WTB Timer Remain(ms) | Guard Timer State | Guard Timer Period(ms) | Guard Timer Remain(ms) |
| 1            | not running     | 5                        | 0                    | not running     | 5100                 | 0                    | not running       | 100                    | 0                      |

| TERMS                            | Description                            |
|----------------------------------|--|
| <b>Ring ID</b>                   | Display the Ring ID                    |
| <b>WTR Timer State</b>           | Running or not Running status          |
| <b>WTR Timer Period (minute)</b> | WTR timeout in milliseconds.           |
| <b>WTR Timer Remain (ms)</b>     | Remaining WTR timeout in milliseconds. |
| <b>WTB Timer State</b>           | Running or not Running status          |
| <b>WTB Timer Period (ms)</b>     | WTB timeout in milliseconds.           |
| <b>WTB Timer Remain (ms)</b>     | Remaining WTB timeout in milliseconds. |

|                                |  |
|--------------------------------|--|
| <b>Guard Timer State</b>       | Running or not Running status                  |
| <b>Guard Timer Period (ms)</b> | Guard Timer timeout in milliseconds.           |
| <b>Guard Timer Remain (ms)</b> | Remaining Guard Timer timeout in milliseconds. |

## Statistics

| Ring ID | R-APS(FS) Tx | R-APS(FS) Rx | R-APS(SF) Tx | R-APS(SF) Rx | R-APS(MS) Tx | R-APS(MS) Rx | R-APS(NR,RB) Tx | R-APS(NR,RB) Rx | R-APS(NR) Tx | R-APS(NR) Rx | Node State Transition Count |
|---------|--------------|--------------|--------------|--------------|--------------|--------------|-----------------|-----------------|--------------|--------------|-----------------------------|
| 1       | 0            | 0            | 15           | 12           | 0            | 0            | 0               | 8432            | 22           | 72           | 10                          |

Reload

| TERMS                              | Description   |
|------------------------------------|---|
| <b>Ring ID</b>                     | Display the Ring ID.  |
| <b>R-APS(FS) Tx</b>                | The number of R-APS messages with Forced Switch (FS) being sent.                    |
| <b>R-APS(FS) Rx</b>                | The number of R-APS messages with Forced Switch (FS) being received.                |
| <b>R-APS(SF) Tx</b>                | The number of R-APS messages with Signal Fail (SF) being sent.                      |
| <b>R-APS(SF) Rx</b>                | The number of R-APS messages with Signal Fail (SF) being received.                  |
| <b>R-APS(MS) Tx</b>                | The number of R-APS messages with Manual Switch (MS) being sent.                    |
| <b>R-APS(MS) Rx</b>                | The number of R-APS messages with Manual Switch (MS) being received.                |
| <b>R-APS(NR, RB) Tx</b>            | The number of R-APS messages with a No Request, RPL Blocked (NR,RB) being sent.     |
| <b>R-APS(NR, RB) Rx</b>            | The number of R-APS messages with a No Request, RPL Blocked (NR,RB) being received. |
| <b>R-APS(NR) Tx</b>                | The number of R-APS messages with a No Request (NR) being sent.                     |
| <b>R-APS(NR) Rx</b>                | The number of R-APS messages with a No Request (NR) being received.                 |
| <b>Node State Transition Count</b> | The number of state transition that detected in the Ring.                           |

## 3.3.4 LOOP PROTECTION

Loop Protection is the feature to protect your port/network out of looping. After enabled the loop protection in specific ports, the router/switch detects and avoids the formation of loop on the Ethernet ports of the connected device. The Router/Switch transmits the loop protection packet every loop-protect interval time, if the same packet send and received on the same Ethernet port, then the loop-protect port will be disabled.

While the Loop Protection port is detected, it is better to unplug the port first and clarified the root cause. The root cause may be Ethernet cable broken, incorrect cable assembly, connected NIC(Network Interface Card) failure, unknown software generated the same source/destination address traffic...etc. To protect your network, we request you manually reactivate the loop-protected enabled port in management interface after the problem is resolved. You must login by administrator account and manually reactive the port by "Enable" its **Port State** in Port Settings page.

### Loop Protection

**Transmit Interval (secs)**

10

| Port | Loop Protection | Status                     |
|------|-----------------|----------------------------|
| 1    | Enable          | Loop Detected and Disabled |
| 2    | Enable          | Loop Detected and Disabled |
| 3    | Disable         | --                         |
| 4    | Disable         | --                         |
| 5    | Disable         | --                         |
| 6    | Disable         | --                         |
| 7    | Disable         | --                         |
| 8    | Disable         | --                         |
| 9    | Disable         | --                         |
| 10   | Disable         | --                         |
| 11   | Disable         | --                         |
| 12   | Disable         | --                         |

Submit

Cancel

The description of the columns is as below:

| TERMS                    | Description   |
|--------------------------|---|
| <b>Transmit Interval</b> | <b>Range from 1~10s, Default=0 (for disable)</b><br>The Router/Switch transmits the loop protection packet every loop-protect interval time.  |
| <b>Loop Protection</b>   | To enable the Loop Protection at the port. Select "Enable" to enable loop protection port. Default is disable.  |
| <b>Status</b>            | It shows the current status of the Loop Protect ports.<br>An example in above figure, while the system detects the loop, the port is disabled and shows "Loop Protected and Disabled" in the Status.<br>The recovered status will update while the port is reactivated and Link Up. |

Click on **Submit** to apply the settings.

## How to reactivate the disable port?

Connect to the management interface of the Router/Switch, login by administrator account.

Go to the Port Settings pages, you will see the Port State of the Loop-Protect port is "Disable". You can manually change the Port State from "Disable" to "Enable", and "Submit" the setting to reactive them.

Below figure shows the example, the Port 7 and 8 are Loop-Protect ports and disabled while Loop detected. The port state of the port 7 and 8 in “Port Settings” page are “Disable”. You can manually select “enable” of the port to reactivate it.

Home > Ethernet Port > Port Settings

Port Settings
Port Status
Port Trunk
Rate Control
Traffic Control
Storm Control
Jumbo Frame

CFM Settings

### Port Settings

| Port | State   | Speed/Duplex    | Flow Control | Description |
|------|---------|-----------------|--------------|-------------|
| 1    | Enable  | AutoNegotiation | Disable      |             |
| 2    | Enable  | AutoNegotiation | Disable      |             |
| 3    | Enable  | AutoNegotiation | Disable      |             |
| 4    | Enable  | AutoNegotiation | Disable      |             |
| 5    | Enable  | AutoNegotiation | Disable      |             |
| 6    | Enable  | AutoNegotiation | Disable      |             |
| 7    | Disable | AutoNegotiation | Disable      |             |
| 8    | Disable | AutoNegotiation | Disable      |             |
| wan1 | Enable  | AutoNegotiation | Disable      |             |
| wan2 | Enable  | AutoNegotiation | Disable      |             |

Submit
Cancel

Click on **Submit** to apply the settings

## 3.4 VLAN

A VLAN is a group of devices that can be located anywhere on a network, but which communicate as if they are on the same physical segment. With VLANs, User can segment User network without being restricted by physical connections—a limitation of traditional network design. With VLANs User can segment User network into:

- **Departmental groups**—User could have one VLAN for the marketing department, another for the finance department, and another for the product development department.
- **Hierarchical groups**—User could have one VLAN for directors, another for managers, and another for general staff.
- **Usage groups**—User could have one VLAN for email users and another for multimedia users.

### Benefits of VLANs

The main benefit of VLANs is that they provide a network segmentation system that is far more flexible than traditional networks. Using VLANs also provides User with three other benefits:

- **VLANs ease the relocation of devices on networks:** With a VLAN setup, if a host originally on the Marketing VLAN, is moved to a port on another part of the network, and retains its original subnet membership, User only needs to specify that the new port is on the Marketing VLAN. User does not need to do any re-cabling.
- **VLANs provide extra security:** Devices within each VLAN can only communicate with other devices on the same VLAN. If a device on the Marketing VLAN needs to communicate with devices on the Finance VLAN, the traffic must pass through a routing device or Layer 3 switch.
- **VLANs help control traffic:** VLANs increase the efficiency of User network because each VLAN can be set up to contain only those devices that need to communicate with each other.

This switch also has **private VLAN** functions; it helps to resolve the primary VLAN ID shortage, client ports' isolation and network security issues. A private VLAN partitions the Layer 2 broadcast domain of a VLAN into subdomains, allowing User to isolate the ports on the switch from each other. A subdomain consists of a primary VLAN and one or more secondary VLANs. All VLANs in a private VLAN domain share the same primary VLAN. The secondary VLAN ID differentiates one subdomain from another. The secondary VLANs may either be isolated VLANs or community VLANs. A host on an isolated VLAN can only communicate with the associated promiscuous port in its primary VLAN. Hosts on community VLANs can communicate among themselves and with their associated promiscuous port but not with ports in other community VLANs. The Private VLAN provides **primary** and **secondary VLAN** within a single switch.

| TERMS                 | Description   |
|-----------------------|---|
| <b>Primary VLAN</b>   | The uplink port is usually the primary VLAN. A primary VLAN contains promiscuous ports that can communicate with the Secondary VLANs. |
| <b>Secondary VLAN</b> | The client ports are usually defined within secondary VLAN. The secondary VLAN includes Isolated VLAN and Community VLAN.             |

### 3.4.1 VLAN SETTING

To configure 802.1Q VLAN and port-based VLANs on the switch, use the VLAN Settings page to configure the ports. , User can assign Management VLAN, create the static VLAN, and assigns the Egress rule for the member ports of the VLAN.

### VLAN Setting

Management VLAN ID

#### Static VLAN

| VLAN ID              | NAME                 |
|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> |

The description of the columns is as below:

| TERMS                     | Description   |
|---------------------------|---|
| <b>Management VLAN ID</b> | <b>Default : 1.</b><br>The switch supports management VLAN. The management VLAN ID is the VLAN ID of the CPU interface so that only member ports of the management VLAN can ping and access the switch.                                     |
| <b>Static VLAN</b>        | User can assign a VLAN ID and VLAN Name for new VLAN here.  |
| <b>VLAN ID</b>            | <b>Default: 1</b><br>Used by the switch to identify different VLANs. Valid VLAN ID is between 1 and 4094.   |
| <b>Name</b>               | A reference for network administrator to identify different VLANs. The available character is 12 for User to input. If User don't input VLAN name, the system will automatically assign VLAN name for the VLAN. The rule is VLAN (VLAN ID). |

The steps to create a new VLAN: Type in VLAN ID and NAME, and press **Add** to create a new VLAN. Then User can see the new VLAN in the Static VLAN Configuration table. After created the VLAN, the status of the VLAN will remain in Unused until User adds ports to the VLAN.

#### NOTE:

- Before User changed the management VLAN ID by Web and Telnet, remember that the port attached by the administrator should be the member port of the management VLAN; otherwise the administrator can't access the switch via the network.
- Switch supports max 256 groups VLAN.

### Static VLAN Configuration



Static VLAN Configuration table is presented on the figure below. User can see the created VLANs and specify the egress (outgoing) port rule to be **Untagged** or **Tagged** here.

**Static VLAN Setting**

| VLAN ID                    | Name  | 1    | 2    | 3   | 4   | 5    | 6    | 7    | 8    | 9    | 10   | 11   | 12   |
|----------------------------|-------|------|------|-----|-----|------|------|------|------|------|------|------|------|
| <input type="checkbox"/> 1 | VLAN1 | U ▼  | U ▼  | U ▼ | U ▼ | U ▼  | U ▼  | U ▼  | U ▼  | U ▼  | U ▼  | U ▼  | U ▼  |
| <input type="checkbox"/> 2 | VLAN2 | -- ▼ | -- ▼ | T ▼ | T ▼ | -- ▼ | -- ▼ | -- ▼ | -- ▼ | -- ▼ | -- ▼ | -- ▼ | -- ▼ |

The description of the columns is as below:

| TERMS   | Description  |
|---------|--|
| --      | Not available  |
| U/Untag | Indicates that egress/outgoing frames are not VLAN tagged.   |
| T/Tag   | Indicates that egress/outgoing frames are to be VLAN tagged. |

### Steps to configure Egress rules :

Select the VLAN ID. Entry of the selected VLAN turns to light blue. Assign Egress rule of the ports to **U** or **T**. Press **Submit** to apply the setting. If User wants to remove one VLAN, select the VLAN entry. Then press **Remove** button.

## 3.4.2 VLAN PORT SETTING

VLAN Port Setting allows User to setup VLAN port parameters to specific port

## VLAN Port Settings

| Port | PVID | Tunnel Mode | EtherType | Accept Frame Type | Ingress Filtering |
|------|------|-------------|-----------|-------------------|-------------------|
| 1    | 1    | None ▼      | 0x8100    | Admit , ▼         | Disable ▼         |
| 2    | 1    | None ▼      | 0x8100    | Admit , ▼         | Disable ▼         |
| 3    | 1    | None ▼      | 0x8100    | Admit , ▼         | Disable ▼         |
| 4    | 1    | None ▼      | 0x8100    | Admit , ▼         | Disable ▼         |
| 5    | 1    | None ▼      | 0x8100    | Admit , ▼         | Disable ▼         |
| 6    | 1    | None ▼      | 0x8100    | Admit , ▼         | Disable ▼         |
| 7    | 1    | None ▼      | 0x8100    | Admit , ▼         | Disable ▼         |
| 8    | 1    | None ▼      | 0x8100    | Admit , ▼         | Disable ▼         |
| 9    | 1    | None ▼      | 0x8100    | Admit , ▼         | Disable ▼         |
| 10   | 1    | None ▼      | 0x8100    | Admit , ▼         | Disable ▼         |
| 11   | 1    | None ▼      | 0x8100    | Admit , ▼         | Disable ▼         |
| 12   | 1    | None ▼      | 0x8100    | Admit , ▼         | Disable ▼         |

Submit

The description of the columns is as below:

| TERMS              | Description   |
|--------------------|---|
| <b>PVID</b>        | The abbreviation of the <b>Port VLAN ID</b> . PVID allows the switches to identify which port belongs to which VLAN. To keep things simple, it is recommended that PVID is equivalent to VLAN IDs. The values of PVIDs are from 0 to 4095. But, 0 and 4095 are reserved. User can't input these 2 PVIDs. 1 is the default value. 2 to 4094 are valid and available in this column.  |
| <b>Tunnel Mode</b> | <b>Default: None</b><br><b>None</b> : This is Port that no using Q in Q<br><b>802.1Q Tunnel</b> : As the Ingress port, is connected to the client port. Configures Q in Q tunneling for a client access port to segregate and preserve customer VLAN IDs for traffic crossing the service provider network.<br><b>802.1Q Tunnel Uplink</b> : As the egress port, that is, the middle switch port. Configures Q in Q tunneling for an uplink port to another device within the service provider network.<br><b>802.1Q Tunnel Uplink-Add-PVID</b> : Assign second VLAN tag for specify VLANs. |
| <b>Ether Type</b>  | <b>Default: 0x8100</b>  |

|                          |  |
|--------------------------|--|
|                          | It is used to indicate which <a href="#">protocol</a> is <a href="#">encapsulated</a> in the payload of the frame.   |
| <b>Accept Frame Type</b> | This column defines the accepted frame type of the port. There are 2 modes User can select, <b>Admit All</b> and <b>Tag Only</b> . Admit All mode means that the port can accept both tagged and untagged packets. <b>Tag Only</b> mode means that the port can only accept tagged packets.  |
| <b>Ingress Filtering</b> | Ingress filtering helps VLAN engine to filter out undesired traffic on a port. When Ingress Filtering is enabled, the port checks whether the incoming frames belong to the VLAN they claimed or not. Then the port determines if the frames can be processed or not. For example, if a tagged frame from Engineer VLAN is received, and Ingress Filtering is enabled, the switch will determine if the port is on the Engineer VLAN's Egress list. If it is, the frame can be processed. If it's not, the frame would be dropped. |

### 3.4.3 VLAN STATUS

This table shows User current status of User VLAN, including VLAN ID, Name, Status, and Egress rule of the ports.

### VLAN Status

| VLAN ID | Name  | Status | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |
|---------|-------|--------|---|---|---|---|---|---|---|---|---|----|----|----|
| 1       | VLAN1 | Static | U | U | U | U | U | U | U | U | U | U  | U  | U  |
| 2       | VLAN2 | Static | - | - | T | T | - | - | - | - | - | -  | -  | -  |

Reload

The description of the columns is as below:

| TERMS          | Description  |
|----------------|--|
| <b>VLAN ID</b> | ID of the VLAN.  |
| <b>Name</b>    | Name of the VLAN.  |
| <b>Status</b>  | <b>Static</b> shows this is a manually configured static VLAN. This VLAN is not workable yet.<br><b>Dynamic</b> means this VLAN is learnt by GVRP. |

After created the VLAN, the status of this VLAN will remain in unused status until User adds ports to the VLAN.

### 3.4.4 PVLAN SETTING

| PVLAN Setting |                   |
|---------------|-------------------|
| VLAN ID       | Private VLAN Type |
| 2             | Primary ▼         |
| 3             | Isolated ▼        |
| 4             | Community ▼       |
| 5             | Community ▼       |

[Submit](#)

The figure above is PVLAN Setting interface. PVLAN Configuration allows User to assign Private VLAN type. After created VLAN in VLAN Configuration page, the available VLAN ID will display here. Choose the Private VLAN types for each VLAN User wants configure.

The description of the columns is as below:

| TERMS            | Description   |
|------------------|---|
| <b>None</b>      | The VLAN is not included in Private VLAN.   |
| <b>Primary</b>   | The VLAN is the Primary VLAN. The member ports can communicate with secondary ports.          |
| <b>Isolated</b>  | The VLAN is the Isolated VLAN. The member ports of the VLAN are isolated.                     |
| <b>Community</b> | The VLAN is the Community VLAN. The member ports of the VLAN can communicate with each other. |

## 3.4.5 PVLAN PORT SETTING

PVLAN Port Setting page allows configure Port Configuration and Private VLAN Association.

### PVLAN Port Configuration

### PVLAN Port Settings

#### Port Configuration

| Port | PVLAN Port Type | VLAN ID |
|------|-----------------|---------|
| 1    | Normal          | None    |
| 2    | Normal          | None    |
| 3    | Normal          | None    |
| 4    | Normal          | None    |
| 5    | Normal          | None    |
| 6    | Normal          | None    |
| 7    | Normal          | None    |
| 8    | Normal          | None    |
| 9    | Normal          | None    |
| 10   | Normal          | None    |
| 11   | Normal          | None    |
| 12   | Normal          | None    |

The description of the columns is as below:

| TERMS                  | Description   |
|------------------------|---|
| <b>PVLAN Port Type</b> | <b>Normal:</b> The Normal port is None PVLAN ports; it remains its original VLAN setting. |

|                |  |
|----------------|--|
|                | <b>Host:</b> The Host type ports can be mapped to the Secondary VLAN.<br><b>Promiscuous:</b> The promiscuous port can be associated to the Primary VLAN. |
| <b>VLAN ID</b> | After assigned the port type, the web UI display the available VLAN ID the port can associate to.  |

## Private VLAN Association (PVLAN)

**Secondary VLAN:** Secondary VLAN is included Isolated and Community VLAN Type that assigned in Private VLAN Configuration section. User can select the Secondary VLAN ID here.

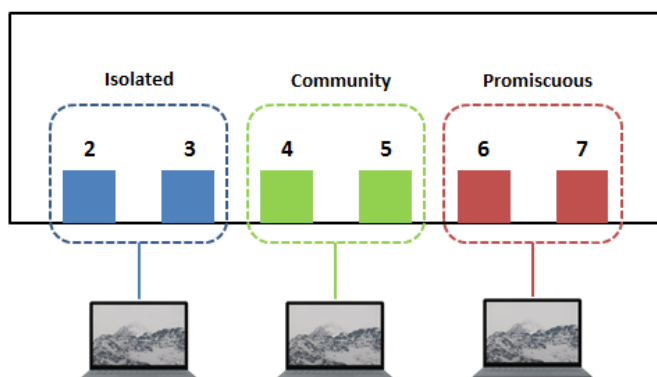
**Primary VLAN:** Primary VLAN is included the Primary VLAN Type that assigned in Private VLAN Configuration section. User can select the Primary VLAN ID here.

**Private VLAN Association**

| Secondary VLAN | Primary VLAN |
|----------------|--------------|
| 2              | 4 ▼          |
| 3              | 4 ▼          |

Before configuring PVLAN port type, the Private VLAN Association should be done first.

For example:



### 1. Create VLAN and Assign the Private VLAN Type:

The very first thing that user need to do is create the VLAN and make sure that the ports are assigned to specific VLAN. After created VLAN, assign the Private VLAN type for each VLAN, for example: VLAN 2 -> Isolated (Secondary VLAN), VLAN 3 -> Community (Secondary VLAN) and VLAN 4 -> Primary.

### 2. Associate the Secondary VLAN to Primary VLAN:

After create the VLAN and assign the Private VLAN Type, then associate the secondary VLAN, VLAN 2 and 3 to VLAN 4 as the Primary VLAN in Private VLAN Association section..

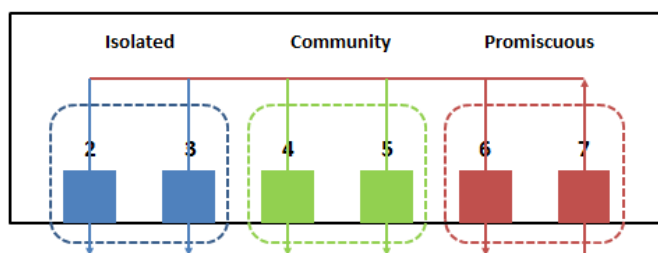
### 3. Configure the Private VLAN Port:

- VLAN 4 – **Primary** -> The member port of VLAN 4 is Promiscuous port. (Port 6 and 7)

- VLAN 2 – **Isolated** -> Map the Host port to VLAN 2. (Port 2 and 3)
- VLAN 3 – **Community** -> Map the Host port to VLAN 3. (Port 4 and 5)

## 5. Result (See 3.5.6 PVLAN Status):

- VLAN 4 -> VLAN 2 and 3; member ports (6 & 7) can communicate with ports in secondary VLAN.
- VLAN 2 -> VLAN 4; member ports (2 & 3) are isolated and cannot communicate each other, but they can communicate with Primary VLAN ports.
- VLAN 3 -> VLAN 4; member ports (4 & 5) within the community can communicate with each other and communicate with Primary VLAN ports.



## 3.4.6 PVLAN STATUS

This page allows User to see the Private VLAN status information.

### PVLAN Status

| Primary VLAN | Secondary VLAN | Secondary VLAN Type | Port    |
|--------------|----------------|---------------------|---------|
| 4            | 2              | Isolated            | 6,7,2,3 |
| 4            | 3              | Community           | 6,7,4,5 |

[Reload](#)

## 3.4.7 GVRP SETTING

### GVRP Setting

GVRP Protocol Disable ▾

| Port | State                  | Join Timer                      | Leave Timer                     | Leave All Timer                   |
|------|------------------------|---------------------------------|---------------------------------|-----------------------------------|
| 1    | <span>Disable ▾</span> | <input type="text" value="20"/> | <input type="text" value="60"/> | <input type="text" value="1000"/> |
| 2    | <span>Disable ▾</span> | <input type="text" value="20"/> | <input type="text" value="60"/> | <input type="text" value="1000"/> |
| 3    | <span>Disable ▾</span> | <input type="text" value="20"/> | <input type="text" value="60"/> | <input type="text" value="1000"/> |
| 4    | <span>Disable ▾</span> | <input type="text" value="20"/> | <input type="text" value="60"/> | <input type="text" value="1000"/> |
| 5    | <span>Disable ▾</span> | <input type="text" value="20"/> | <input type="text" value="60"/> | <input type="text" value="1000"/> |
| 6    | <span>Disable ▾</span> | <input type="text" value="20"/> | <input type="text" value="60"/> | <input type="text" value="1000"/> |
| 7    | <span>Disable ▾</span> | <input type="text" value="20"/> | <input type="text" value="60"/> | <input type="text" value="1000"/> |
| 8    | <span>Disable ▾</span> | <input type="text" value="20"/> | <input type="text" value="60"/> | <input type="text" value="1000"/> |
| 9    | <span>Disable ▾</span> | <input type="text" value="20"/> | <input type="text" value="60"/> | <input type="text" value="1000"/> |
| 10   | <span>Disable ▾</span> | <input type="text" value="20"/> | <input type="text" value="60"/> | <input type="text" value="1000"/> |

GVRP (GARP VLAN Registration Protocol) is a protocol that facilitates control of virtual local area networks (VLANs) within a larger network. GVRP conforms to the IEEE 802.1Q specification, which defines a method of tagging frames with VLAN configuration data. This allows network devices to dynamically exchange VLAN configuration information with other devices. GVRP allows users to set-up VLANs automatically rather than manual configuration on every port of every switch in the network. The description of the columns is as below:

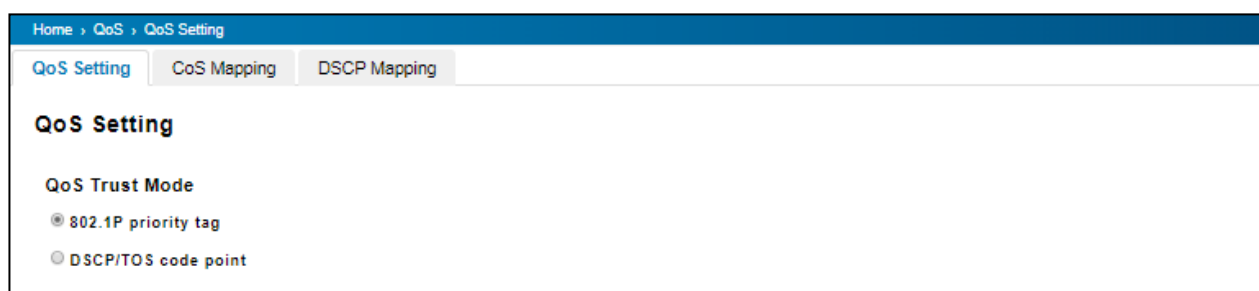
| TERMS                   | Description  |
|-------------------------|--|
| <b>GVRP Protocol</b>    | <b>Default: Disable</b><br>Allow user to enable / disable GVRP function globally.  |
| <b>State</b>            | <b>Default: Disable</b><br>After enable GVRP globally, here still can enable/disable GVRP by port.   |
| <b>Join Timer</b>       | <b>Default: 20</b><br>Controls the interval of sending the GVRP Join BPDU. An instance of this timer is required on a per-Port, per-GARP Participant basis   |
| <b>Leave Timer</b>      | <b>Default: 60</b><br>Control the time to release the GVRP reservation after received the GVRP Leave BPDU.<br>An instance of the timer is required for each state machine that is in the LV state. |
| <b>Leave All Timers</b> | <b>Default: 1000</b><br>Controls the period to initiate the garbage collection of registered VLAN. The timer is required on a per-Port, per-GARP Participant basis                                 |

## 3.5 QUALITY of SERVICE (QoS)

Quality of Service (QoS) is the ability from the switch to provide different priority to different applications, users or data flows, or to guarantee a certain level of performance to a data flow. QoS guarantees are important if the network capacity is insufficient, especially for real-time streaming multimedia applications. QoS can also help to reduce traffic problems and control the traffic by deliver the high priority first. This section allows User to configure Quality of Service settings for each port by configure the priorities in order to provide a smooth data traffic.

### 3.5.1 QoS SETTING

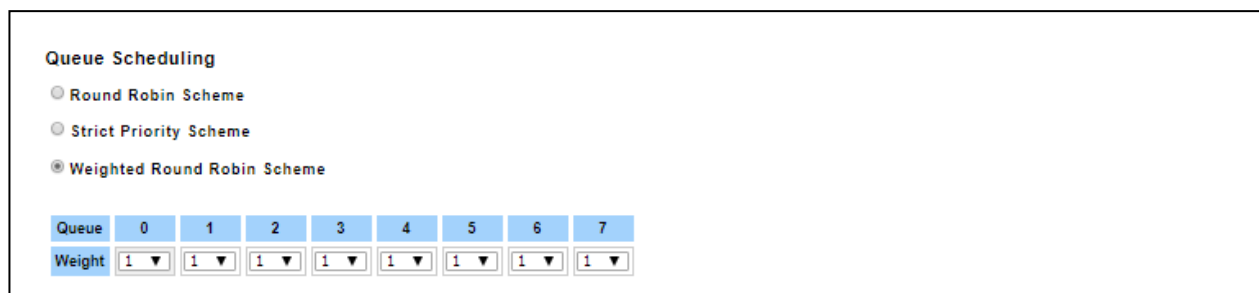
The figure below shows QoS Setting.



#### QoS Trust Mode

**802.1P Priority Tag:** If 802.1P is selected the switch relies on a packet's CoS information to determine priority. This is related to the settings in the CoS-Queue Mapping page

**DSCP/TOS Code Point:** If DSCP/TOS is selected the switch relies on a packets differentiated services code point information to determine the priority. This is related to the settings in the DSCP-Priority Mapping page.



| Queue  | 0   | 1   | 2   | 3   | 4   | 5   | 6   | 7   |
|--------|-----|-----|-----|-----|-----|-----|-----|-----|
| Weight | 1 ▼ | 1 ▼ | 1 ▼ | 1 ▼ | 1 ▼ | 1 ▼ | 1 ▼ | 1 ▼ |

#### Queue Scheduling

User may select the Queue Scheduling rule:

- **Use Round Robin Scheme:** The Round Robin scheme means all the priority has the same privilege, the traffic is forward cyclic from highest to lowest.
- **Use strict priority scheme:** The priority here always the higher queue will be processed first, except the higher queue is empty.
- **Use Weighted Round Robin scheme.** This scheme allows users to assign new weight ratio from 1 to 10 for each class where 10 is the highest ratio.



## Port Setting

Port Setting

| Port | Priority |
|------|----------|
| 1    | 0 ▼      |
| 2    | 0 ▼      |
| 3    | 0 ▼      |
| 4    | 0 ▼      |
| 5    | 0 ▼      |
| 6    | 0 ▼      |
| 7    | 0 ▼      |
| 8    | 0 ▼      |
| 9    | 0 ▼      |
| 10   | 0 ▼      |
| 11   | 0 ▼      |
| 12   | 0 ▼      |

Submit
Cancel

Choose the Queue value of each port, the port then has its default priority. The Queue 7 is the highest port-based queue, 0 is the lowest queue. The traffic injected to the port follows the queue level to be forwarded, but the outgoing traffic does not bring the queue level to next switch. Click the **Submit** button to apply the configuration changes.

## 3.5.2 CoS MAPPING

This section allows user to change CoS values to Physical Queue mapping table. In switch, users can freely assign the mapping table or follow the suggestion of the 802.1p standard. Below is the interface.

Home > QoS > CoS Mapping

QoS Setting
CoS Mapping
DSCP Mapping

CoS Mapping

| CoS   | 0   | 1   | 2   | 3   | 4   | 5   | 6   | 7   |
|-------|-----|-----|-----|-----|-----|-----|-----|-----|
| Queue | 0 ▼ | 1 ▼ | 2 ▼ | 3 ▼ | 4 ▼ | 5 ▼ | 6 ▼ | 7 ▼ |

Submit
Cancel

The service classes (CoS) are assigned to the queues as default as follows:

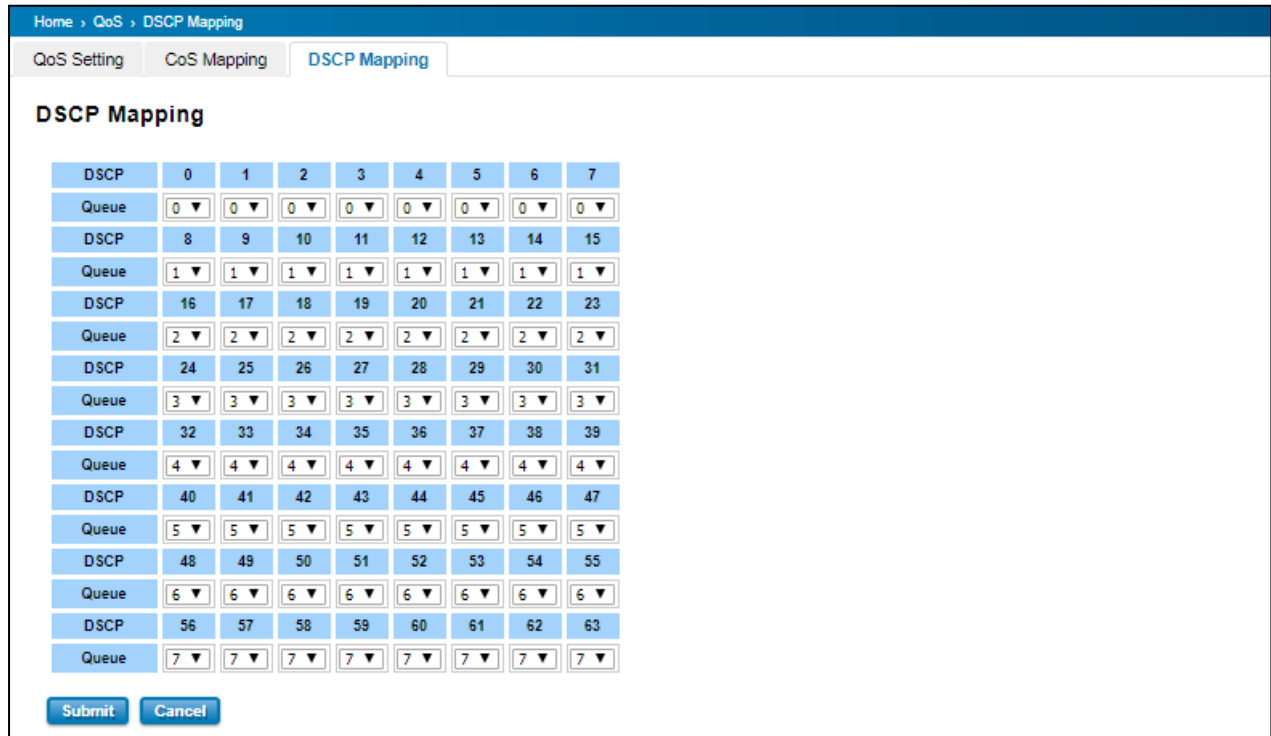
- COS 0 → Queue 0
- COS 1 → Queue 1
- COS 2 → Queue 2
- COS 3 → Queue 3
- COS 4 → Queue 4
- COS 5 → Queue 5
- COS 6 → Queue 6
- COS 7 → Queue 7

For the step in configuration

1. For each value in the **CoS** column, select the queue from the **Queue** drop-down list.
2. Click the **Submit** button.

### 3.5.3 DSCP MAPPING

This page is to change DSCP values to Physical Queue mapping table. Users should therefore assign how to map DSCP value to the level of the physical queue. Users can freely change the mapping table to follow the upper layer 3 switch or routers' DSCP setting.



Home > QoS > DSCP Mapping

QoS Setting CoS Mapping **DSCP Mapping**

#### DSCP Mapping

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

**Submit** **Cancel**

After configuration, press **Submit** to enable the settings.

| DSCP Value and Priority<br>Queues Setting | Description  | Factory Default |
|---|--|-----------------|
| 0 to 7                                    | Maps different TOS values to one of 8 different egress queues. | 0               |
| 8 to 15                                   |  | 1               |
| 16 to 23                                  |  | 2               |
| 24 to 31                                  |  | 3               |
| 32 to 39                                  |  | 4               |
| 40 to 47                                  |  | 5               |
| 48 to 55                                  |  | 6               |
| 56 to 63                                  |  | 7               |

## 3.6 MULTICAST

Multicasts are similar to broadcasts, they are sent to all end stations on a LAN or VLAN that belong to the multicast group. Multicast filtering is the function, which end stations can receive the multicast traffic if the connected ports had been included in the specific multicast groups. With multicast filtering, network devices only forward multicast traffic to the ports that are connected to the registered end stations. For multicast filtering, Switch uses IGMP Snooping technology. IGMP Snooping provides the ability to prune multicast traffic so that it travels only to those end destinations that require that traffic, thereby reducing the amount of traffic on the Ethernet LAN. In effect, it manages multicast traffic by making use of switches, routers, and hosts that support IGMP.

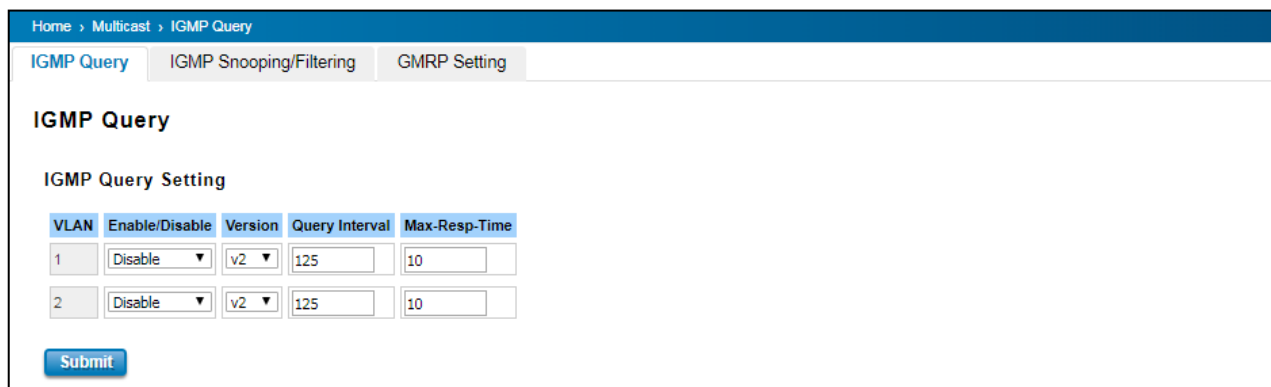
Following sections are included in this group:

- IGMP Query
- IGMP Snooping
- GMRP Setting

### 3.6.1 IGMP QUERY

This page allows users to configure **IGMP Query** feature. Since the device can only be configured by member ports of the management VLAN, IGMP Query can only be enabled on the management VLAN. If User wants to run IGMP Snooping feature in several VLANs, User should notice that whether each VLAN has its own IGMP Querier first.

The IGMP querier periodically sends query packets to all end-stations on the LANs or VLANs that are connected to it.



| VLAN | Enable/Disable | Version | Query Interval | Max-Resp-Time |
|------|----------------|---------|----------------|---------------|
| 1    | Disable        | v2      | 125            | 10            |
| 2    | Disable        | v2      | 125            | 10            |

For networks with more than one IGMP querier, a switch with the lowest IP address becomes the IGMP querier.

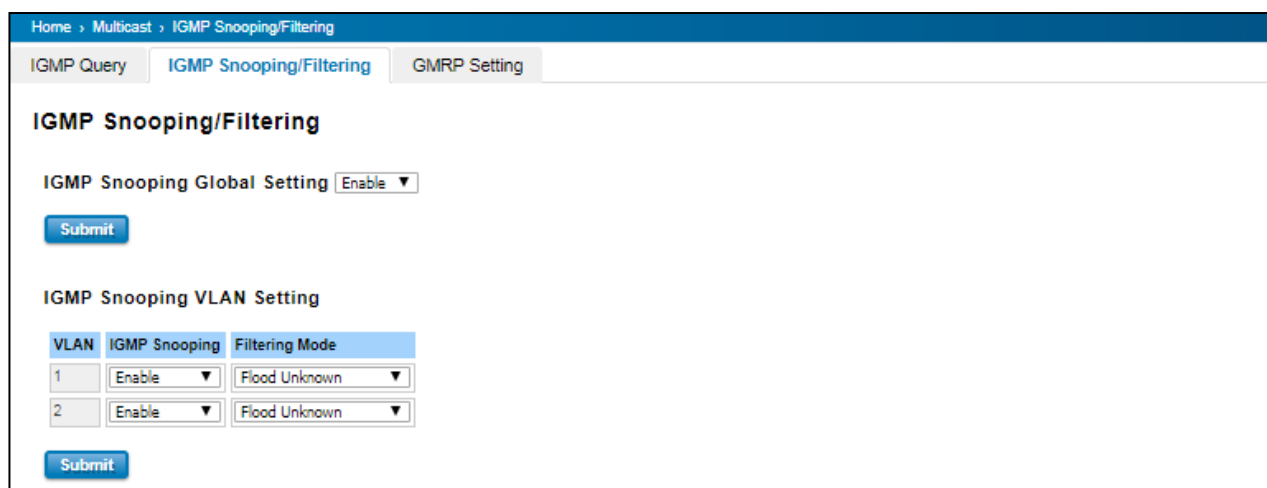
| TERMS                         | Description   |
|-------------------------------|---|
| <b>Enable</b>                 | <b>Default: Disable</b><br>Enable the IGMP Query function   |
| <b>Version</b>                | <b>Default: V2</b><br><b>V1</b> means IGMP V1 General Query<br><b>V2</b> means IGMP V2 General Query. |
| <b>Query Interval(s)</b>      | The interval period of querier to send the query.   |
| <b>Query Maximum Response</b> | The response time for querier detects to confirm there are no more directly connected                 |

|          |                         |
|----------|-------------------------|
| Time (s) | group members on a LAN. |
|----------|-------------------------|

Once User finished configuring the settings, click on **Submit** to apply User configuration.

## 3.6.2 IGMP SNOOPING

This page is to enable IGMP Snooping feature. After enable the feature, user may assign IGMP Snooping function to specific VLAN, and the IGMP Snooping table will show the specific multicast group from dynamic learnt or manual input. By enabling IGMP Snooping allows the ports to detect IGMP queries, report packets, and manage multicast traffic through the switch.



| TERMS                               | Description  |
|-------------------------------------|--|
| <b>IGMP Snooping Global Setting</b> | User can select <b>Enable</b> or <b>Disable</b> this function here. After enabling IGMP Snooping, User can then enable IGMP Snooping for specific VLAN.  |
| <b>IGMP Snooping</b>                | Select the <b>Enable</b> to activate the IGMP Snooping. In the same way, User can also <b>Disable</b> IGMP Snooping for certain VLANs.   |
| <b>Filtering Mode</b>               | It allows the switch to filter the unknown-multicast data flow. Multicast Filtering Mode is Flood unknown, discard unknown and source only learning. <ul style="list-style-type: none"> <li>- Flood Unknown: The switch would filter the unknown packets that transmit through the network and the packets will be flooded to the member ports of the same VLAN.</li> <li>- Discard Unknown: Non-member ports will not receive the unknown packets because the filter discards the unknown multicast.</li> <li>- Source Only Learning: The switch learns the IP multicast group from the IP multicast data stream and only forwards traffic to the multicast ports.</li> </ul> |

**IGMP Snooping Table:** User can see several information such as multicast IP address, VLAN ID from the multicast group, and the interface member ports of the multicast group (256 multicast groups)

## IGMP Snooping Table

| Multicast Address | VLAN ID | Interface |
|-------------------|---------|-----------|
| 224.0.0.251       | 1       | ge5,      |
| 224.0.0.252       | 1       | ge5,      |
| 239.255.255.250   | 1       | ge5,ge7,  |

[Reload](#)

### 3.6.3 GMRP SETTING

GARP Multicast Registration Protocol (GMRP) is a Generic Attribute Registration Protocol (GARP) application that provides a constrained multicast flooding facility similar to IGMP snooping. GMRP and GARP are industry-standard protocols defined by the IEEE 802.1P. The GMRP Setting allows bridges and end stations to dynamically register group membership information with the MAC bridges attached to the same LAN segment and for that information to be disseminated across all bridges in the Bridged LAN that supports extended filtering services.

[Home](#) > [Multicast](#) > [GMRP Setting](#)

[IGMP Query](#)
[IGMP Snooping/Filtering](#)
[GMRP Setting](#)

### GMRP Setting

GMRP Global Setting Disable ▼

[Submit](#)

GMRP Port Setting

| Port | State   |
|------|---------|
| 1    | Disable |
| 2    | Disable |
| 3    | Disable |
| 4    | Disable |
| 5    | Disable |
| 6    | Disable |
| 7    | Disable |
| 8    | Disable |
| 9    | Disable |
| 10   | Disable |
| 11   | Disable |
| 12   | Disable |

[Submit](#)

## 3.7 SNMP

SNMP is a standard TCP/IP protocol for network management. Network administrators use SNMP to monitor and map network availability, performance, and error rates. System management software uses SNMP to allow administrators to remotely monitor and manage thousands of systems on a network, often by presenting the data gathered from monitored devices in a snapshot or dashboard view. Managed Switch supports SNMP v1 and v2c and V3.

SNMP managed network consists of two main components: agents and a manager. An agent is a management software module that resides in a managed switch. An agent translates the local management information from the managed device into a SNMP compatible format. The manager is the console through the network.

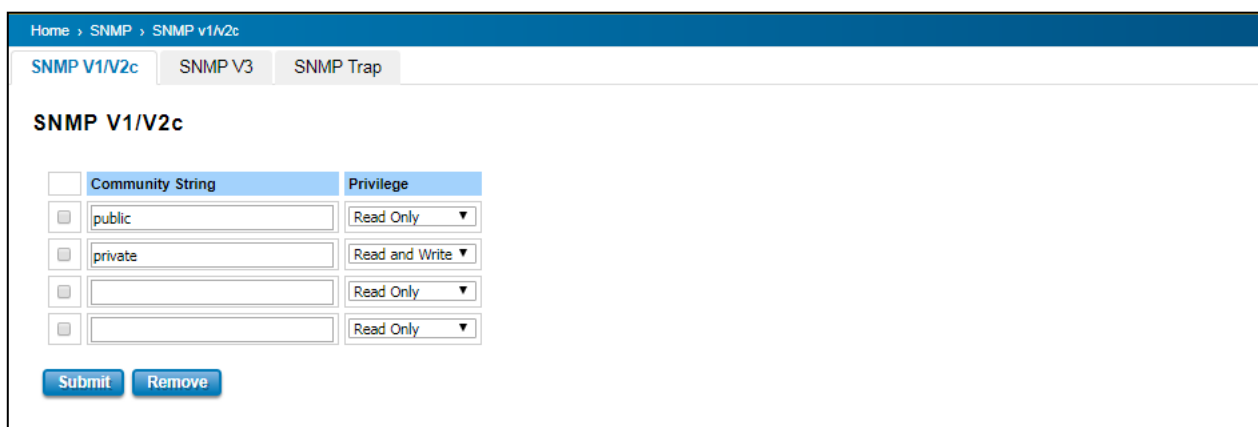
### 3.7.1 SNMP V1/V2c SETTING

In this page allows users to define the new community string set and remove the unwanted community string. The community string can be viewed as the password because SNMP V1/V2c doesn't request User to enter password before User tries to access SNMP agent. The community includes 2 privileges, Read Only and Read and Write.

| PRIVILEGE      | Description   |
|----------------|---|
| Read Only      | User only has the ability to read the values of MIB tables. Default community string is Public.     |
| Read and Write | User has the ability to read and set the values of MIB tables. Default community string is Private. |

Managed Switch allows users to assign 4 community strings. Type the community string and select the privilege. Then press **Submit**.

**NOTE:** When User first installs the device in User network, we highly recommend user to change the community string. Since most SNMP management application uses Public and Private as their default community name, this might be the leakage of the network security.



Home > SNMP > SNMP v1/v2c

SNMP V1/V2c    SNMP V3    SNMP Trap

### SNMP V1/V2c

| Community String                 | Privilege      |
|----------------------------------|----------------|
| <input type="checkbox"/> public  | Read Only      |
| <input type="checkbox"/> private | Read and Write |
| <input type="checkbox"/>         | Read Only      |
| <input type="checkbox"/>         | Read Only      |

### 3.7.2 SNMP V3

SNMPv3 provides network monitoring and control through SNMP protocol that provides secure access to devices by a combination of authenticating (MD5 & SHA) and encrypting packets over the network to ensure the secure communication. The security model that is used by SNMPv3 is an authentication strategy that is set up for a user and user group. A security level is the permitted level of security within a security model. A combination of a security model and a security level determines which security mechanism is used for an SNMP packet.

Home > SNMP > SNMP V3

SNMP V1/V2c
SNMP V3
SNMP Trap

### SNMP V3

SNMP V3

User Name

Security Level

Authentication Level

Authentication Password

DES Password

**Add**

SNMP V3 Users

| <input type="checkbox"/> | User Name            | Security Level       | Authentication Protocol | Authentication Password | Privacy Protocol     | Privacy Password     |
|--------------------------|----------------------|----------------------|-------------------------|-------------------------|----------------------|----------------------|
| <input type="checkbox"/> | <input type="text"/> | <input type="text"/> | <input type="text"/>    | <input type="text"/>    | <input type="text"/> | <input type="text"/> |

**Remove** **Reload**

| TERMS                   | Description  |
|-------------------------|--|
| User Name               | Set up the user name.  |
| Security Level          | <b>Default: None</b><br>Here the user can select the following levels of security: None, User Authentication, and Authentication with privacy.   |
| Authentication Level    | <b>Default: MD5</b><br>MD5 (Message-Digest algorithm 5) is a widely used cryptographic hash function with a 128-bit hash value. SHA (Secure Hash Algorithm) hash functions refer to five Federal Information Processing Standard-approved algorithms for computing a condensed digital representation. |
| Authentication Password | Here the user enters the SNMP v3 user authentication password.   |
| DES Password            | Here the user enters the password for SNMP v3 user DES Encryption.   |

### 3.7.3 SNMP TRAP

SNMP Trap is the notification feature defined by SNMP protocol. All the SNMP management applications can understand such trap messages generated by the switch. If no trap manager is defined, no traps will be issued. To



define a management station as a trap manager, assign an IP address, enter the SNMP community strings, and select the SNMP trap version. Below is the SNMP Trap Interface.

A screenshot of the "SNMP Trap" configuration page in a web interface. The page has a blue header with navigation links: "Home", "SNMP", and "SNMP Trap". Below the header, there are three tabs: "SNMP V1/V2c", "SNMP V3", and "SNMP Trap", with the third tab being active. The main content area is titled "SNMP Trap" and contains several sections. The first section, "SNMP Trap", has a dropdown menu set to "Disable" and a "Submit" button. The second section, "SNMP Trap Server", has input fields for "Server IP", "Community", and a "Version" dropdown set to "V1", along with an "Add" button. The third section, "Trap Server Profile", has a table with columns "Server IP", "Version", and "Community", and buttons "Remove" and "Reload" at the bottom.

| TERMS     | Description   |
|-----------|---|
| SNMP Trap | <b>Default: Disable</b><br>Enable / Disable SNMP Trap |
| Server IP | Enter the IP address of the trap manager.             |
| Community | Enter the community string for the trap station.      |
| Version   | Select the SNMP trap version type—v1 or v2c.          |

After configuration, Click **Add** then User can see the change of the SNMP pre-defined standard traps.



## 3.8 SECURITY

Switch provides several security features for User to secure access to its management functions and it can be remotely managed (monitored and configured).

Following topics are included in this section:

- Filter
- IEEE 802.1X

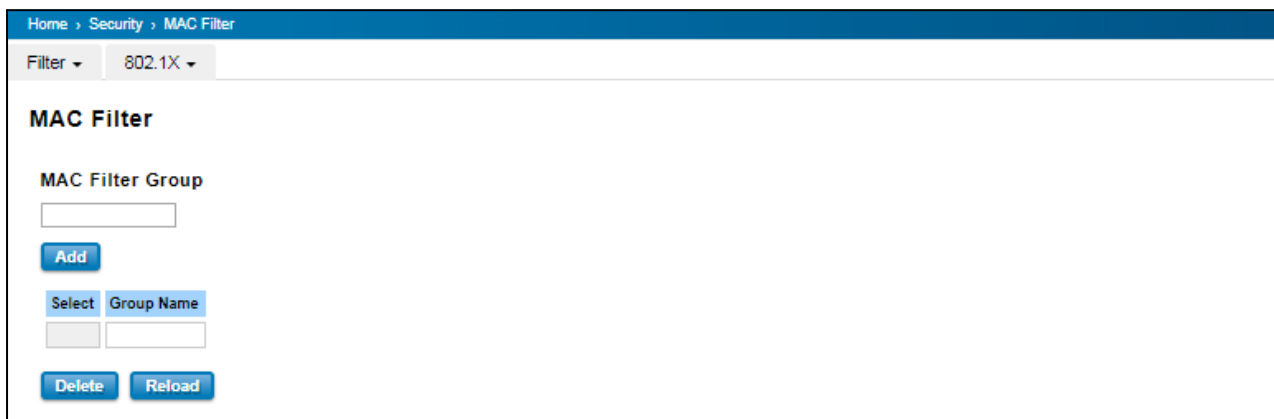
### 3.8.1 FILTER

Filter is known as Access Control List feature. There are 2 major types; one is MAC Filter that allows user to define the access rule based on the MAC address flexibility. Another one is IP Filter. It includes the IP security, IP Standard access list and advanced IP based access lists.

#### MAC Filter

Network security can be increased by limiting access on a specific port only to users with specific MAC addresses. Mac Filter feature allows User to stop the MAC address learning for specific port. After stopping MAC learning, only the MAC address listed in the list can access the switch and transmit/receive traffic. This is a simple way to secure User network environment and not to be accessed by hackers.

#### MAC Filter Group



The screenshot shows a web interface for configuring MAC Filter Groups. At the top, there is a breadcrumb trail: "Home > Security > MAC Filter". Below this, there are two dropdown menus: "Filter" and "802.1X". The main heading is "MAC Filter". Underneath, there is a section titled "MAC Filter Group" with a text input field for the group name. Below the input field is a blue "Add" button. Further down, there is a table with two columns: "Select" and "Group Name". The "Select" column contains a checkbox, and the "Group Name" column contains a text input field. At the bottom of the section, there are two blue buttons: "Delete" and "Reload".

Create a group of MAC Filters by entering a name and clicking the **Add** button to create a new Filter Group. The MAC Filter Group table provides the following information. **Select** the entry and click the **Delete** button then the Filter Group is deleted. Click the **Reload** button to reload the MAC Filter Group table.

#### MAC Filter Setting

**MAC Filter Setting**

Group Name

Source MAC

Source Wildcard

Destination MAC

Destination Wildcard

Egress Port

Action

▼

any ▼

any ▼

-- ▼

☐ Permit ☐ Deny

Add

**MAC Filter Table**

| Select                   | Group Name | Source MAC | Source Wildcard | Destination MAC | Destination Wildcard | Action | Egress Port |
|--------------------------|------------|------------|-----------------|-----------------|----------------------|--------|-------------|
| <input type="checkbox"/> |            |            |                 |                 |                      |        |             |

Delete

In this form user may configure the MAC Filter Setting. The description of the columns is as below:

| TERMS                | Description  |
|----------------------|--|
| Group Name           | This is the name of the MAC Filter Group.  |
| Source MAC           | This is the source MAC Address of the packet.  |
| Source Wildcard      | This is the mask of the MAC Address.   |
| Destination MAC      | This is the destination MAC Address of the packet.   |
| Destination Wildcard | This is the mask of the MAC Address.   |
| Egress Port          | This is the outgoing (exiting) port number.  |
| Action               | <div>This is the filter action, which is to deny or permit the packet.</div> <div><b>Permit:</b> to permit traffic from specified sources.</div> <div><b>Deny:</b> to deny traffic from those sources.</div> |

Once User finishes configuring the settings, click on **Submit/Add** to apply User configuration.

IP Filter

Home > Security > IP Filter

Filter 802.1X

## IP Filter

**IP Filter Group**

(1~99) IP Standard Access List  
 (100~199) IP Extended Access List  
 (1300~1999) IP Standard Access List (expanded range)  
 (2000~2699) IP Extended Access List (expanded range)

**Add**

| Select                   | Group Number         | Type                 |
|--------------------------|----------------------|----------------------|
| <input type="checkbox"/> | <input type="text"/> | <input type="text"/> |

**Delete** **Reload**

User can create a group of IP Filters with following numbers.

1 - 99: IP Standard Access List

100 – 199: IP Extended Access List

1300 – 1999: IP Standard Access List (expanded range)

2000 – 2699: IP Extended Access List (expanded range)

After entering the IP Filter Group number, click the **Add** to create the new Filter Group.

### IP Filter Setting

**Group Number**

**Protocol**

**Source IP**

**Source Wildcard**

**Source Port**

**Destination IP**

**Destination Wildcard**

**Destination Port**

**Egress Port**

**Action** ☐ Permit ☐ Deny

**Add**

**IP Filter List**

| Select                   | Group Number         | Type                 | Protocol             | Source IP            | Source Wildcard      | Source Port          | Destination IP       | Destination Wildcard | Destination Port     | Action               | Egress Port          |
|--------------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|----------------------|
| <input type="checkbox"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

**Delete**

IP Filter Setting

| TERMS                       | Description   |
|-----------------------------|---|
| <b>Group Number</b>         | Number of the Filter Group.   |
| <b>Protocol</b>             | This is the L4 protocol (IP/TCP/UDP/ICMP).  |
| <b>Source IP</b>            | This is the source IP address of the packet.  |
| <b>Source Wildcard</b>      | This is the mask of the IP address.   |
| <b>Source Port</b>          | This is the source port of L4 protocol (TCP/UDP)  |
| <b>Destination IP</b>       | This is the destination IP address of the packet.   |
| <b>Destination Wildcard</b> | This is the mask of the IP address.   |
| <b>Destination Port</b>     | This is the destination port of L4 protocol (TCP/UDP).  |
| <b>Egress Port</b>          | This is the outgoing (exiting) port number.   |
| <b>Action</b>               | This is the filter action, which is to deny or permit the packet.<br><br><b>Permit:</b> to permit traffic from specified sources.<br><br><b>Deny:</b> to deny traffic from those sources. |

## IP Filter List

| TERMS                       | Description   |
|-----------------------------|---|
| <b>Select</b>               | Selected the entry for delete.  |
| <b>Group Number</b>         | Number of the Filter Group.   |
| <b>Type</b>                 | This is the filter group type (standard or extended).   |
| <b>Protocol</b>             | This is the L4 protocol (IP/TCP/UDP/ICMP).  |
| <b>Source IP</b>            | This is the source IP address of the packet.  |
| <b>Source Wildcard</b>      | This is the mask of the IP address.   |
| <b>Source Port</b>          | This is the source port of L4 protocol (TCP/UDP)  |
| <b>Destination IP</b>       | This is the destination IP address of the packet.   |
| <b>Destination Wildcard</b> | This is the mask of the IP address.   |
| <b>Destination Port</b>     | This is the destination port of L4 protocol (TCP/UDP).  |
| <b>Action</b>               | This is the filter action, which is to deny or permit the packet. Click the <b>Delete</b> button to remove the Filter that has been selected. |
| <b>Egress Port</b>          | This is the outgoing (exiting) port number.   |

## Filter Attach

This page allows you to attach filters created on the IP Filter and MAC Filter pages to ports on the switch.

Home > Security > Filter Attach

Filter ▾ 802.1X ▾

### Filter Attach

Filter Attach

Port

MAC Filter

IP Filter

| TERMS      | Description   |
|------------|---|
| Port       | Select the port that needs to be attached the filter.         |
| MAC Filter | Select a MAC address based filter to attach to the interface. |
| IP Filter  | Select an IP address based filter to attach to the interface. |

Click the **Submit** button to apply the configurations.

## Filter Attach List

This table displays what filters are currently attached to each port.

| TERMS      | Description                     |
|------------|---------------------------------|
| Port       | The port number.                |
| MAC Filter | The filter attached MAC address |
| IP Filter  | The filter attached IP address  |

## 3.8.2 IEEE 802.1X

802.1X is an IEEE Standard for Port-based Network Access Control that provides an authentication mechanism to devices that wish to attach to a LAN or WLAN. Port-based network access control protocol contains 3 parts, supplicant, authenticator, and authentication server. With 802.1X authentication, a username can be linked with an IP address, MAC address, and port. This provides greater visibility into the network. 802.1X also provides more security because it only allows traffic transmitting on authenticated ports or MAC addresses.

## RADIUS

RADIUS is used in the authentication process. Database of authorized users is maintained on a RADIUS server. There is an authenticator, our switch enabling 802.1X, to forward the authentication requests between authentication (RADIUS) server and client. Allowing or denying the requests decides if the client can connect to a LAN/WAN or not.

## 802.1X Setting

IEEE 802.1X is the protocol that performing authentication to obtain access to IEEE 802 LANs. It is port-base network

access control. With the function, switch could control which connection is available or not.

### 802.1X Setting

System Auth Control Disable ▾

Authentication Method RADIUS ▾

Submit

#### RADIUS Server

RADIUS Server IP

Shared Key

Server Port

Accounting Port

#### Secondary RADIUS Server

RADIUS Server IP

Shared Key

Server Port

Accounting Port

Submit

#### Local RADIUS User

| User Name            | Password             | VID                  |
|----------------------|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> |

Submit

#### Local RADIUS User List

| User                 | Name                 | Password             | VID                  |
|----------------------|----------------------|----------------------|----------------------|
| <input type="text"/> | <input type="text"/> | <input type="text"/> | <input type="text"/> |

Delete

The description of the columns is as below:

| TERMS                             | Description  |
|-----------------------------------|--|
| <b>System Auth Control</b>        | To enable or disable the 802.1X authentication.  |
| <b>Authentication Method</b>      | Radius is an authentication server that provide key for authentication, with this method, user must connect switch to server. If user selects Local for the authentication method, switch use the local user data base which can be created in this page for authentication. |
| <b>Radius Server IP</b>           | The IP address of Radius server  |
| <b>Shared Key</b>                 | It is the password for communicate between switch and Radius Server.   |
| <b>Server Port</b>                | UDP port of Radius server.   |
| <b>Accounting Port</b>            | Port for packets that contain the information of account login or logout.  |
| <b>Secondary Radius Server IP</b> | Secondary Radius Server could be set in case of the primary radius server down.  |
| <b>802.1X Local User</b>          | Here User can add Account/Password for local authentication.   |
| <b>802.1X Local User List</b>     | This is a list shows the account information; User also can remove selected account.   |

## 802.1X Port Setting

After the configuration of Radius Server or Local user list, user also need configure the authentication mode, authentication behavior, applied VLAN for each port and permitted communication. The following information will explain the port configuration.

Home > Security > 802.1X Port Setting

Filter ▾ 802.1X ▾

### 802.1X Port Setting

| Port                        | Port Control       | Re-authentication | Max Request | Guest VLAN | Host Mode | Admin Control Direction |
|-----------------------------|--------------------|-------------------|-------------|------------|-----------|-------------------------|
| <input type="checkbox"/> 1  | Force Authorized ▾ | Disable ▾         | 2           | 0          | Single ▾  | Both ▾                  |
| <input type="checkbox"/> 2  | Force Authorized ▾ | Disable ▾         | 2           | 0          | Single ▾  | Both ▾                  |
| <input type="checkbox"/> 3  | Force Authorized ▾ | Disable ▾         | 2           | 0          | Single ▾  | Both ▾                  |
| <input type="checkbox"/> 4  | Force Authorized ▾ | Disable ▾         | 2           | 0          | Single ▾  | Both ▾                  |
| <input type="checkbox"/> 5  | Force Authorized ▾ | Disable ▾         | 2           | 0          | Single ▾  | Both ▾                  |
| <input type="checkbox"/> 6  | Force Authorized ▾ | Disable ▾         | 2           | 0          | Single ▾  | Both ▾                  |
| <input type="checkbox"/> 7  | Force Authorized ▾ | Disable ▾         | 2           | 0          | Single ▾  | Both ▾                  |
| <input type="checkbox"/> 8  | Force Authorized ▾ | Disable ▾         | 2           | 0          | Single ▾  | Both ▾                  |
| <input type="checkbox"/> 9  | Force Authorized ▾ | Disable ▾         | 2           | 0          | Single ▾  | Both ▾                  |
| <input type="checkbox"/> 10 | Force Authorized ▾ | Disable ▾         | 2           | 0          | Single ▾  | Both ▾                  |
| <input type="checkbox"/> 11 | Force Authorized ▾ | Disable ▾         | 2           | 0          | Single ▾  | Both ▾                  |
| <input type="checkbox"/> 12 | Force Authorized ▾ | Disable ▾         | 2           | 0          | Single ▾  | Both ▾                  |

### 802.1X Timeout Configuration

| Port | Re-Auth Period(s) | Quiet Period(s) | Tx period(s) | Supplicant Timeout(s) | Server Timeout(s) |
|------|-------------------|-----------------|--------------|-----------------------|-------------------|
| 1    | 3600              | 60              | 30           | 30                    | 30                |
| 2    | 3600              | 60              | 30           | 30                    | 30                |
| 3    | 3600              | 60              | 30           | 30                    | 30                |
| 4    | 3600              | 60              | 30           | 30                    | 30                |
| 5    | 3600              | 60              | 30           | 30                    | 30                |
| 6    | 3600              | 60              | 30           | 30                    | 30                |
| 7    | 3600              | 60              | 30           | 30                    | 30                |
| 8    | 3600              | 60              | 30           | 30                    | 30                |
| 9    | 3600              | 60              | 30           | 30                    | 30                |
| 10   | 3600              | 60              | 30           | 30                    | 30                |

Submit

The description of the columns is as below:

| TERMS        | Description  |
|--------------|--|
| Port control | Force Authorized means this port is authorized; the data is free to in/out. Force unauthorized just opposite, the port is blocked. If users want to control this port with Radius Server, please select Auto for port control. |

|                                |   |
|--------------------------------|---|
| <b>Re-authentication</b>       | <b>Default: 3600 seconds</b><br>If enable this field, switch will ask client to re-authenticate.  |
| <b>Max Request</b>             | The maximum times that the switch allow client request.   |
| <b>Guest VLAN</b>              | 0 to 4094 is available for this field. If this field is set to 0, that means the port is blocked after authentication fail. Otherwise, the port will be set to Guest VLAN.  |
| <b>Host Mode</b>               | If there are more than one device connected to this port, set the Host Mode to single means only the first PC authenticate success can access this port. If this port is set to multi, all the devices can access this port once any one of them pass the authentication. |
| <b>Admin Control Direction</b> | Determined devices can end data out only or both send and receive.  |
| <b>Re-Auth Period</b>          | Control the Re-authentication time interval, 1~65535 are available.   |
| <b>Quiet Period</b>            | When authentication failed, Switch will wait for a period and try to communicate with radius server again.  |
| <b>Tx period</b>               | The time interval of authentication request.  |
| <b>Supplicant Timeout</b>      | The timeout for the client authenticating   |
| <b>Sever Timeout</b>           | The timeout for server response for authenticating.   |

Once User finishes configuring the settings, click on **Submit** to apply User configuration.

Click **Initialize Selected** to set the authorize state of selected port to initialize status.

Click **Re-authenticate Selected** to send EAP Request to supplicant to request re-authentication.

Click **Default Selected** to reset the configurable 802.1X parameters of selected port to the default values.

## 802.1X Port Status

User can observe the port status for Port control, Authorized Status, Authorized Supplicant and Open Control Direction from each port.



Home > Security > 802.1X Port Status

Filter 802.1X

### 802.1X Port Status

| Port | Port Control     | Authorized Status | Authorized Supplicant | Oper Control Direction |
|------|------------------|-------------------|-----------------------|------------------------|
| 1    | Force Authorized | AUTHORIZED        | NONE                  | Both                   |
| 2    | Force Authorized | AUTHORIZED        | NONE                  | Both                   |
| 3    | Force Authorized | AUTHORIZED        | NONE                  | Both                   |
| 4    | Force Authorized | AUTHORIZED        | NONE                  | Both                   |
| 5    | Force Authorized | AUTHORIZED        | NONE                  | Both                   |
| 6    | Force Authorized | AUTHORIZED        | NONE                  | Both                   |
| 7    | Force Authorized | AUTHORIZED        | NONE                  | Both                   |
| 8    | Force Authorized | AUTHORIZED        | NONE                  | Both                   |
| 9    | Force Authorized | AUTHORIZED        | NONE                  | Both                   |
| 10   | Force Authorized | AUTHORIZED        | NONE                  | Both                   |
| 11   | Force Authorized | AUTHORIZED        | NONE                  | Both                   |
| 12   | Force Authorized | AUTHORIZED        | NONE                  | Both                   |

Reload

### 3.8.3 DHCP Snooping

DHCP snooping is a security feature of DHCP and is mainly applied to switches.

The purpose of DHCP Snooping is to block illegal DHCP servers in the access network. That is, after the DHCP Snooping function is enabled, clients on the network can only obtain IP addresses from the DHCP server specified by the administrator. Due to the lack of authentication mechanism in DHCP protocol, if there is an illegal DHCP server in the network, the administrator will not be able to guarantee that the client obtains a legal address and the client may obtain the wrong IP address from the illegal DHCP server.

[Save](#) [Logout](#) [Reboot](#)

[Home](#) > [Security](#) > [DHCP Snooping](#)

Filter ▾   802.1X ▾   DHCP Snooping ▾   IP Source Guard   DAI ▾

### DHCP Snooping

**DHCP Snooping** Enable ▾

**MAC Verify** Enable ▾

[Submit](#)

### DHCP Snooping VLAN Settings

| VLAN ID | DHCP Snooping         |
|---------|-----------------------|
| 1       | <span>Enable ▾</span> |

Note: DHCP Snooping should be enabled first to set VLAN DHCP Snooping.

[Submit](#)

### DHCP Snooping Statistics

| Drop Type                           | Drop Packets |
|-------------------------------------|--------------|
| Total received                      | 0            |
| Dropped (MAC verification failed)   | 0            |
| Dropped (Interface invalid)         | 0            |
| Dropped (Binding not matched)       | 0            |
| Dropped (Relay Agent address error) | 0            |
| Dropped (Total dropped)             | 0            |

[Clear](#)   [Reload](#)

The description of the column is as below:

| TERMS                             | Description   |
|-----------------------------------|---|
| <b>DHCP Snooping</b>              | Enable the DHCP Snooping function.  |
| <b>MAC Verify</b>                 | Enable MAC Verify to start checking.  |
| <b>DHCP Snooping VLAN Setting</b> | Enable DHCP Snooping for specific VLAN interface.<br>DHCP Snooping should be enabled first then it's available to Enable the DHCP Snooping for specific VLAN. |
| <b>DHCP Snooping Statistics</b>   | The column shows the Drop Type and Drop Packets. It can help you check the status of your environment.  |

## DHCP Snooping Binding

The Static Entry in DHCP Snooping Binding table allows to add tracking the specific IP Address and MAC Address for specific VLAN ID and LAN port. The DHCP Snooping Binding List table includes the client MAC address, IP address, DHCP lease time, binding type, VLAN number, and interface information on untrusted switch ports. The Trust/Untrust port setting can be configured in IP Source Guard page.

### DHCP Snooping Binding

**Add Static Entry**

IP Address

192.168.10.253

MAC Address

9466.E700.0002

VLAN

1 ▾

Interface

Port 8 ▾

Submit

**DHCP Snooping Binding List**

| Select                   | MAC Address    | IP Address     | Lease Time | VLAN | Interface | Type   |
|--------------------------|----------------|----------------|------------|------|-----------|--------|
| <input type="checkbox"/> | 9466.e700.0002 | 192.168.10.253 | 0          | 1    | Port 8    | static |

Remove Selected

Reload

**DHCP Snooping Write Interval**

Interval

300 (secs)

Submit

The description of the column is as below:

| TERMS                        | Description   |
|------------------------------|---|
| IP Address                   | Type the IP address to bind the MAC Address of selected server.                                 |
| MAC Address                  | Type the MAC address of the selected IP Address.<br>The format should be like '0060.b312.3456'. |
| VLAN                         | Select the VLAN you'd like to apply.  |
| Interface                    | Select the Port (LAN port) you'd like to apply.   |
| DHCP Snooping Write Interval | Default: 300 secs   |

### 3.8.4 IP Source Guard

IP source guard can prevent the illegal use of IP by others, which is also a headache for many network managers. IP Source Guard is a security feature that restricts IP/IP-MAC traffic on untrusted L2 LAN ports by filtering traffic based on the DHCP snooping binding database.

Home > Security > IP Source Guard

Filter 802.1X DHCP Snooping IP Source Guard DAI

### IP Source Guard

IP Source Guard Settings

| Port | Trust   | IP Source Guard | Packet-discarded |
|------|---------|-----------------|------------------|
| 1    | Trust   | IP-MAC          | 0                |
| 2    | Untrust | Disable         | 0                |
| 3    | Trust   | Disable         | 0                |
| 4    | Trust   | Disable         | 0                |
| 5    | Trust   | Disable         | 0                |
| 6    | Trust   | Disable         | 0                |
| 7    | Trust   | Disable         | 0                |
| 8    | Trust   | Disable         | 0                |
| 9    | Trust   | Disable         | 0                |
| 10   | Trust   | Disable         | 0                |
| 11   | Trust   | Disable         | 0                |
| 12   | Trust   | Disable         | 0                |

Submit Clear Packet-discarded Reload

Statistics Checking Period

Check period 3 (mins)

Submit

The description of the column is as below:

| TERMS                             | Description  |
|-----------------------------------|--|
| <b>Trust</b>                      | Select Trust/Untrust for each LAN port.  |
| <b>IP Source Guard</b>            | Select the Filter Type of IP or IP-MAC traffic.  |
| <b>Packet-discarded</b>           | The entry shows the discarded packet count of the port.<br>You can manually click “Reload” to update the count. Or the system will update it based on the time of Statistic Checking Period. |
| <b>Statistics Checking Period</b> | It’s the time to update the count of discarded traffic.  |

### 3.8.5 DAI (Dynamic ARP Inspection)

DAI (Dynamic ARP Inspection) provides IP address and MAC address binding on the switch and dynamically establishes a binding relationship. DAI is based on the DHCP Snooping binding table. For individual machines that do not use DHCP, you can use statically added ARP access-list. The DAI configuration is for VLANs. For interfaces in the same VLAN, DAI can be enabled or disabled. DAI can control the number of ARP request packets on a certain port. With this configuration, the problem of ARP attacks can be solved, and network security and stability can be better improved.

Home > Security > Dynamic ARP Inspection

Filter ▾ 802.1X ▾ DHCP Snooping ▾ IP Source Guard ▾ DAI ▾

### Dynamic ARP Inspection

#### VLAN Configuration

| VLAN | Configuration | Operation | Gateway Verify | Gateway IP   | ACL-Match |
|------|---------------|-----------|----------------|--------------|-----------|
| 1    | Enable ▾      | Inactive  | Enable ▾       | 192.168.10.1 | ▾         |

Submit

Interface Configuration

Statistics Checking Period

| Port | Trust     | Rate |
|------|-----------|------|
| 1    | Trust ▾   | 15   |
| 2    | Untrust ▾ | 15   |
| 3    | Untrust ▾ | 15   |
| 4    | Untrust ▾ | 15   |
| 5    | Untrust ▾ | 15   |
| 6    | Untrust ▾ | 15   |
| 7    | Untrust ▾ | 15   |
| 8    | Untrust ▾ | 15   |

Check period 1 (mins)

Submit

Submit

The description of the column is as below:

| TERMS                        | Description   |           |                |              |                |            |           |   |          |        |          |              |   |   |           |          |           |         |      |
|------------------------------|---|-----------|----------------|--------------|----------------|------------|-----------|---|----------|--------|----------|--------------|---|---|-----------|----------|-----------|---------|------|
| VLAN                         | Display the VLAN ID.  |           |                |              |                |            |           |   |          |        |          |              |   |   |           |          |           |         |      |
| Configuration                | Enable or Disable the DAI of the VLAN   |           |                |              |                |            |           |   |          |        |          |              |   |   |           |          |           |         |      |
| Operation                    | Display the DAI operation state of the VLAN   |           |                |              |                |            |           |   |          |        |          |              |   |   |           |          |           |         |      |
| Gateway Verify               | Enable/Disable verify the Gateway   |           |                |              |                |            |           |   |          |        |          |              |   |   |           |          |           |         |      |
| Gateway IP                   | Assign the target IP of Gateway Verify  |           |                |              |                |            |           |   |          |        |          |              |   |   |           |          |           |         |      |
| ACL-Match                    | Select the target ARP filter rule. Need to set the rule in ARP Filter. <div><table><tr><th>VLAN</th><th>Configuration</th><th>Operation</th><th>Gateway Verify</th><th>Gateway IP</th><th>ACL-Match</th></tr><tr><td>1</td><td>Enable ▾</td><td>Active</td><td>Enable ▾</td><td>192.168.10.1</td><td>▾</td></tr><tr><td>2</td><td>Disable ▾</td><td>Inactive</td><td>Disable ▾</td><td>0.0.0.0</td><td>test</td></tr></table></div> | VLAN      | Configuration  | Operation    | Gateway Verify | Gateway IP | ACL-Match | 1 | Enable ▾ | Active | Enable ▾ | 192.168.10.1 | ▾ | 2 | Disable ▾ | Inactive | Disable ▾ | 0.0.0.0 | test |
| VLAN                         | Configuration   | Operation | Gateway Verify | Gateway IP   | ACL-Match      |            |           |   |          |        |          |              |   |   |           |          |           |         |      |
| 1                            | Enable ▾  | Active    | Enable ▾       | 192.168.10.1 | ▾              |            |           |   |          |        |          |              |   |   |           |          |           |         |      |
| 2                            | Disable ▾   | Inactive  | Disable ▾      | 0.0.0.0      | test           |            |           |   |          |        |          |              |   |   |           |          |           |         |      |
| Interface Configuration Port | The LAN Port ID   |           |                |              |                |            |           |   |          |        |          |              |   |   |           |          |           |         |      |
| Trust                        | Select Trust/Untrust for each LAN port.   |           |                |              |                |            |           |   |          |        |          |              |   |   |           |          |           |         |      |
| Rate                         | Configure the DAI rate limit of incoming ARP packets  |           |                |              |                |            |           |   |          |        |          |              |   |   |           |          |           |         |      |
| Statistic Checking Period    | It's the time to update the count of DAI Statistics.  |           |                |              |                |            |           |   |          |        |          |              |   |   |           |          |           |         |      |

## ARP Filter

Add the ARP Filter Name and then apply the ARP Filter Rule for it. Then you can see the Name/Rules in ARP Filter List table.

### ARP Filter

**ARP Filter Group**

Filter

**ARP Filter Group**

| Select                   | Filter |
|--------------------------|--------|
| <input type="checkbox"/> | test   |

### ARP Filter Rule Settings

Filter

Action

Source IP

Source MAC

Destination IP

Destination MAC

Egress Port

Note: Leave the field as blank for setting "any".

### ARP Filter List

| Select                   | Filter | Action | Source IP      | Source MAC | Destination IP | Destination MAC | Egress Port      |
|--------------------------|--------|--------|----------------|------------|----------------|-----------------|------------------|
| <input type="checkbox"/> | test   | permit | 192.168.10.111 | any        | any            | any             | gigabitethernet3 |

The description of the column is as below:

| TERMS                                 | Description  |
|---------------------------------------|--|
| <b>ARP Filter Group/Filter</b>        | Type "Name" of ARP Filter and click "Add".<br>The entry can be added in ARP Filter Group.    |
| <b>ARP Filter Rule Setting/Filter</b> | Select the ARP Filter Entry then assign the parameters in below columns.                     |
| <b>Action</b>                         | Permit or Deny   |
| <b>Source IP</b>                      | Configure specific IP Address for the rule.<br>Blank/Any: All the coming source IP address.  |
| <b>Source MAC</b>                     | Configure specific MAC Address for the rule.<br>Blank/Any: All the coming source IP address. |
| <b>Destination IP</b>                 | Configure specific IP Address for the rule.<br>Blank/Any: All the coming source IP address.  |
| <b>Destination MAC</b>                | Configure specific MAC Address for the rule.<br>Blank/Any: All the coming source IP address. |
| <b>Egress Port</b>                    | Select the target Egress Port for the ARP Filter Entry.                                      |

## Dynamic ARP Inspection Statistics

Below figures display the statistics of the Interface and VLAN for your reference. With the info, it can help you identify the overall status of the connected port and VLAN, this is used for network security diagnostic.

## Dynamic ARP Inspection Statistics

### Interface Statistics

| Port | Received | Forwarded | Dropped | Invalid IP | Mismatch MAC | DHCP Dropped | Invalid GW IP | Invalid Opcode | Mismatch Src Port | No Dst Port | ACL Dropped |
|------|----------|-----------|---------|------------|--------------|--------------|---------------|----------------|-------------------|-------------|-------------|
| 1    | 386      | 0         | 386     | 0          | 0            | 0            | 0             | 0              | 0                 | 0           | 386         |
| 2    | 0        | 0         | 0       | 0          | 0            | 0            | 0             | 0              | 0                 | 0           | 0           |
| 3    | 0        | 0         | 0       | 0          | 0            | 0            | 0             | 0              | 0                 | 0           | 0           |
| 4    | 0        | 0         | 0       | 0          | 0            | 0            | 0             | 0              | 0                 | 0           | 0           |
| 5    | 0        | 0         | 0       | 0          | 0            | 0            | 0             | 0              | 0                 | 0           | 0           |
| 6    | 0        | 0         | 0       | 0          | 0            | 0            | 0             | 0              | 0                 | 0           | 0           |
| 7    | 0        | 0         | 0       | 0          | 0            | 0            | 0             | 0              | 0                 | 0           | 0           |
| 8    | 0        | 0         | 0       | 0          | 0            | 0            | 0             | 0              | 0                 | 0           | 0           |

Clear Statistics

Reload

### VLAN Statistics

| VLAN | Forwarded | Dropped | DHCP Dropped | ACL Dropped | DHCP Permits | ACL Permits | Source MAC Dropped | Source MAC Dropped | Destination MAC Dropped | Invalid IP |
|------|-----------|---------|--------------|-------------|--------------|-------------|--------------------|--------------------|-------------------------|------------|
| 1    | 0         | 386     | 0            | 386         | 0            | 0           | 0                  | 0                  | 0                       | 0          |
| 2    | 0         | 0       | 0            | 0           | 0            | 0           | 0                  | 0                  | 0                       | 0          |
| 3    | 0         | 0       | 0            | 0           | 0            | 0           | 0                  | 0                  | 0                       | 0          |

Clear Statistics

Reload

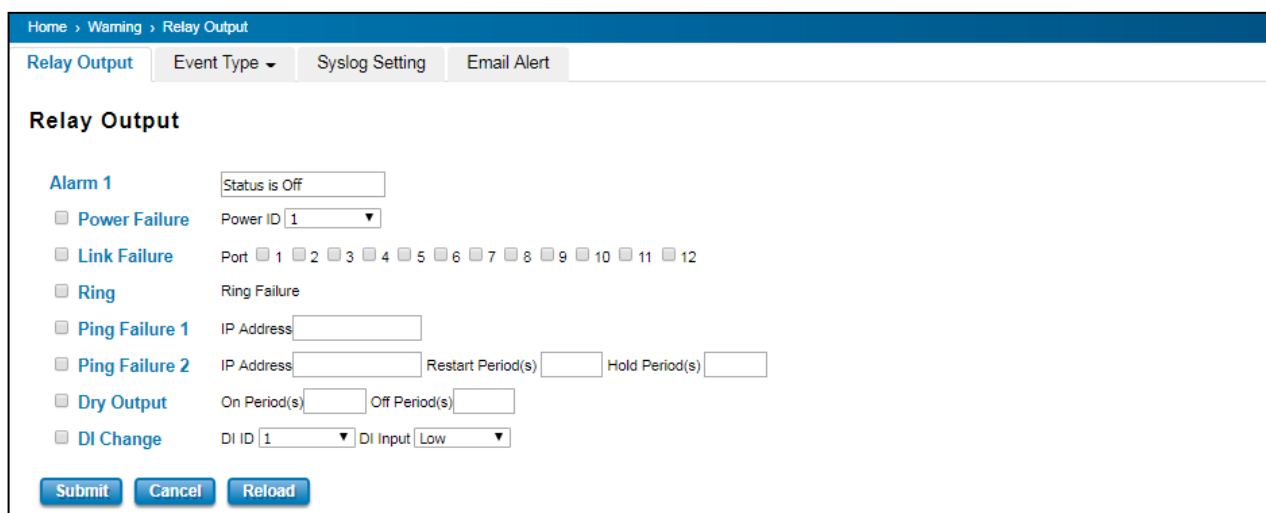
## 3.9 WARNING

The switch provides several types of Warning feature for remote monitoring of end devices status or network changes.

### 3.9.1 RELAY OUTPUT

Switch provides 1 alarm relay output, also known as Digital Output. These settings in Relay Output section control the events that will trigger the alarm output. The OK discrete output is on during normal conditions and turned off in the event of an alarm condition. The relay output supports multiple event relay binding function.

The Relay Output configuration interface has shown as below:



The condition or term described as following table.

| TERMS                 | Condition  | Description  |
|-----------------------|--|--|
| <b>Power Failure</b>  | Power ID 1<br>Power ID 2<br>Any  | Detect power input status. If one of condition occurred, relay triggered.  |
| <b>Link Failure</b>   | Port number  | Monitoring port link down event  |
| <b>Ring</b>           | Ring failure   | If ring topology changed   |
| <b>Ping Failure 1</b> | <b>IP Address:</b> remote device's IP address.   | If target IP does not reply ping request, then relay active.   |
| <b>Ping Failure 2</b> | <b>IP address:</b> remote device's address<br><b>Restart Period:</b> duration of output open.<br><b>Hold Period:</b> duration of Ping hold time. | Ping target device and trigger relay to emulate power reset for remote device, if remote system crash.<br>Note: once perform Ping Restart; the relay output will form a short circuit. |
| <b>Dry Output</b>     | <b>On period:</b> duration of relay output short (close).<br><b>Off period:</b> duration of relay output open.                                   | Relay continuous perform On/Off behavior with different duration.  |



|                  |   |  |
|------------------|---|--|
| <b>DI Change</b> | DI number<br>(the switch supports 1 DI) | Relay trigger when DI states change to Hi or Low |
|------------------|---|--|

The relay supports multiple event trigger function; click and select type of event and setting the detail information, and then clicks **Submit** to activate the relay alarm function.

## 3.9.2 EVENT TYPE

Event Types can be divided into two basic groups: System Event and Port Event. System Event are related to the overall function of the switch, whereas Port Event related to the activity of specific ports

Once User finishes configuring the settings, click on Submit to apply User configuration.

Home > Warning > System Event

Relay Output   Event Type ▾   Syslog Setting   Email Alert

### System Event

- ☒ Device Cold Start
- ☒ Device Warm Start
- ☒ Authentication Failure
- ☒ Time Synchronization Failure
- ☒ Power 1 Failure
- ☒ Power 2 Failure
- ☒ Relay Output 1
- ☒ DI 1 Change
- ☒ Ring Event
- ☒ SFP Event

Submit   Cancel

### Ethernet Port Event

| Port | Link State |
|------|------------|
| 1    | Disable ▾  |
| 2    | Disable ▾  |
| 3    | Disable ▾  |
| 4    | Disable ▾  |
| 5    | Disable ▾  |
| 6    | Disable ▾  |
| 7    | Disable ▾  |
| 8    | Disable ▾  |
| 9    | Disable ▾  |
| 10   | Disable ▾  |
| 11   | Disable ▾  |
| 12   | Disable ▾  |

Submit   Cancel

The description of the columns is as below:

| System Event Selection   | Warning Event is sent when.....                          |
|--------------------------|--|
| Device Cold Start        | Power is cut off and then reconnected.                   |
| Device Warm Start        | Reboot the device by CLI or Web UI.                      |
| Authentication failure   | An incorrect password, SNMP Community String is entered. |
| Time Synchronize Failure | Accessing to NTP Server is failure.                      |
| Power 1/ 2 Failure       | The power input is failure.                              |
| Relay Output 1           | The Digital Output is on.                                |
| DI 1 Change              | The Digital Input change                                 |
| Ring Event               | Ring Status has changed or backup path is activated.     |
| SFP Event                | The SFP transceiver's state is abnormal.                 |

| Port Event | Warning Event is sent when.....   |
|------------|---|
| Up         | The port is connected to another device   |
| Down       | The port is disconnected (e.g. the cable is pulled out, or the opposing devices turns down) |
| Both       | The link status changed.  |

### 3.9.3 SYSLOG SETTING

System Log can provide the switch events history by locally or remotely monitor. There are 3 System Log modes provided by the switch, local mode, remote mode and both.

**Syslog Setting**

Syslog Mode

Disable ▾

Remote IP Address

Note: When enabled Local and Both mode, you can monitor the system logs in the Diagnostics/Event Logs page.

Submit

Cancel

**Local Mode:** In this mode, the device will print the selected events in the Event Selection page to System Log table of the switch.

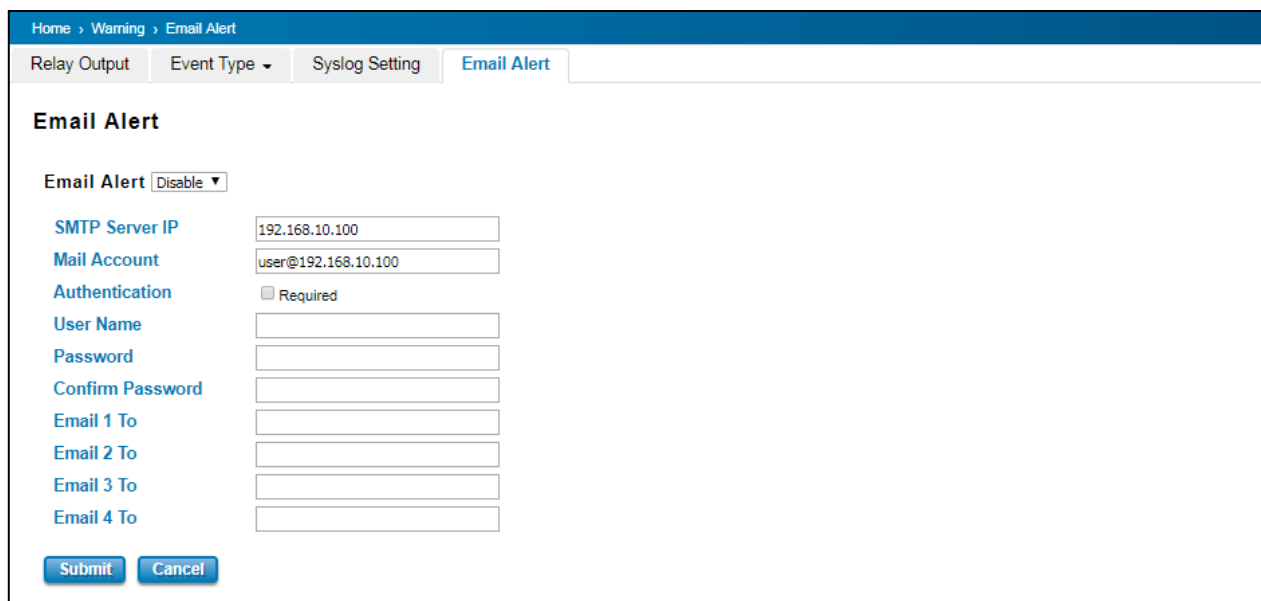
**Remote Mode:** In this mode, User should assign the IP address of the System Log server. Then the selected occurred events will be sent to System Log server User assigned.

**Both:** Above 2 modes can be enabled at the same time.

Once User finishes configuring the settings, click on **Submit** to apply User configuration.

## 3.9.4 EMAIL ALERT

Switch provides the option of automatically sending an e-mail if an alarm event occurs (for example to the network administrator). The e-mail contains the identification of the sending device, a description of the cause of the alarm in plain language, and a time stamp. This allows centralized network monitoring to be set up for networks with few nodes based on an e-mail system. On this page, you can configure SMTP servers and the four corresponding e-mail addresses.



The description of the columns is as below:

| TERMS   | Description  |
|---|--|
| Email Alert   | Enable or Disable the Email Alert function.  |
| SMTP Server IP  | Enter the IP address of the email Server   |
| Mail Account  | Enter the email Server address   |
| Authentication  | Click on check box to enable password  |
| User Name   | Enter email Account name (Max.40 characters)   |
| Password  | Enter the password of the email account  |
| Confirm Password  | Re-type the password of the email account  |
| User can set up to 4 email addresses to receive email alarm from the switch |  |
| Email 1 To  | The first email address to receive email alert from the switch (Max. 40 characters)  |
| Email 2 To  | The second email address to receive email alert from the switch (Max. 40 characters) |
| Email 3 To  | The third email address to receive email alert from the switch (Max. 40 characters)  |
| Email 4 To  | The fourth email address to receive email alert from the switch (Max. 40 characters) |

Once User finishes configuring the settings, click on **Submit** to apply User configuration.

## 3.10 DIAGNOSTICS

Switch provides several types of features for User to monitor the status of the switch or diagnostic for User to check the problem when encountering problems related to the switch.

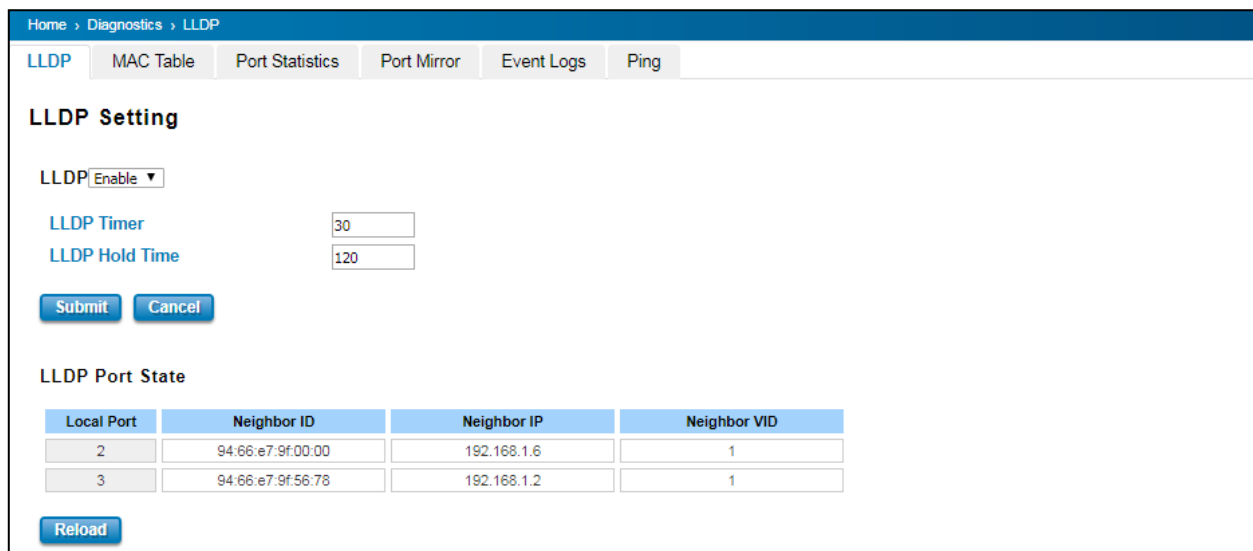
Following commands are included in this group:

- LLDP Setting
- MAC Table
- Port Statistics
- Port Mirror
- Event Log
- Ping

### 3.10.1 LLDP SETTING

LLDP is an OSI Layer 2 protocol defined by IEEE 802.11AB. LLDP standardizes the self-identification advertisement method, and allows each networking device, such as a managed switch, to periodically send its system and configuration information to its neighbors. Because of this, all LLDP devices are kept informed of each other's status and configuration, and with SNMP. From the switch's web interface, User can enable or disable LLDP, and User can view each switch's neighbor-list, which is reported by its network neighbors. Most importantly, enabling the LLDP function allows to automatically display the neighbor ID and IP learnt from the connected devices.

The configuration and settings explain as following.



| Local Port | Neighbor ID       | Neighbor IP | Neighbor VID |
|------------|-------------------|-------------|--------------|
| 2          | 94:66:e7:9f:00:00 | 192.168.1.6 | 1            |
| 3          | 94:66:e7:9f:56:78 | 192.168.1.2 | 1            |

| TERMS      | Description                             |
|------------|---|
| LLDP       | Select to enable/disable LLDP function. |
| LLDP Timer | Default: 30 seconds                     |

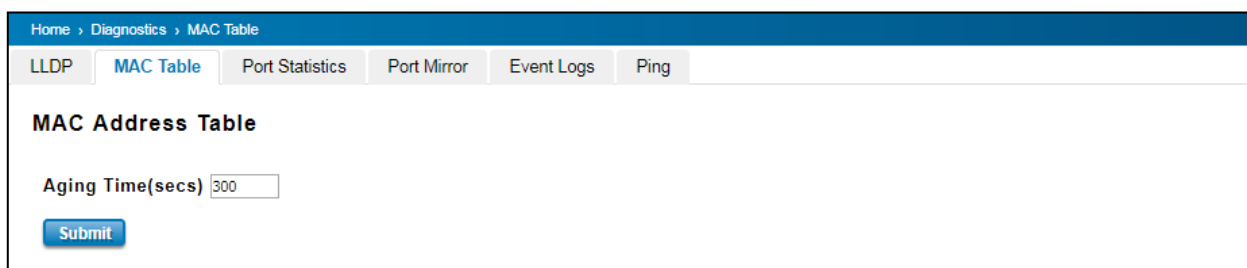
|                       |   |
|-----------------------|---|
|                       | The interval time of each LLDP and counts in second; the valid number is from 5 to 254.   |
| <b>LLDP Hold time</b> | <b>Default: 120 seconds</b><br>The TTL (Time To Live) timer. The LLDP state will be expired once the LLDP is not received by the hold time. |
| <b>Local port</b>     | The current port number that linked with neighbor network device.   |
| <b>Neighbor ID</b>    | The MAC address of neighbor device on the same network segment.   |
| <b>Neighbor IP</b>    | The IP address of neighbor device on the same network segment.  |
| <b>Neighbor VID</b>   | The VLAN ID of neighbor device on the same network segment.   |

## 3.10.2 MAC TABLE

In this page, users can change the Aging time, add Static Unicast MAC Address, monitor the MAC address or sort them by different packet types and ports. Click on **Submit** to change the value.

### Aging Time (Sec)

Each switch Fabric has limit size to write the learnt MAC address. To save more entries for new MAC address, the switch Fabric will age out non-used MAC address entry per Aging Time timeout. The default Aging Time is 300 seconds. The Aging Time can be modified in this page.



### Static Unicast MAC Address

In some applications, users may need to type in the static Unicast MAC address to its MAC address table. In this page, User can type MAC Address (format: xxxx.xxxx.xxxx), select its VID and Port ID, and then click on **Add** to add it to MAC Address table.



### MAC Address Table

At this table, all the MAC Addresses learnt by the switch will be shown here. Use the MAC address table to ensure the

port security. The MAC Address Table can be displayed based on the MAC Address Type and based on the Port.

**MAC Address Table** All

| MAC Address                             | Address Type      | VID | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|-------------------|-----|---|---|---|---|---|---|---|---|---|----|
| <input type="checkbox"/> 708b.cd03.b567 | Dynamic Unicast   | 1   | V |   |   |   |   |   |   |   |   |    |
| <input type="checkbox"/> 0100.5e00.00fb | Dynamic Multicast | 1   | V |   |   |   |   |   |   |   |   |    |
| <input type="checkbox"/> 0100.5e00.00fc | Dynamic Multicast | 1   | V |   |   |   |   |   |   |   |   |    |
| <input type="checkbox"/> 0100.5e7f.ffa  | Dynamic Multicast | 1   | V |   |   |   |   |   |   |   |   |    |

Remove
Reload

Click on **Remove** to remove the selected static Unicast/Multicast MAC address. Click on **Reload** to refresh the table. New learnt Unicast/Multicast MAC address will be updated to MAC address table.

### 3.10.3 PORT STATISTICS

This page displays the number of error packets that is received and sent from the port. This level of detail is not available from the Dashboard graphs. The number of error packets can mean a duplex mismatch, incompatibilities with the port and its attached device, or faulty cables or attached devices. Any of these problems can cause slow network performance, data loss, or lack of connectivity. The statistics that can be viewed include Link Type, Link State, Rx Good, Rx Bad, Rx Abort, Tx Good, Tx Bad and Collision.

Home > Diagnostics > Port Statistics

LLDP
MAC Table
**Port Statistics**
Port Mirror
Event Logs
Ping

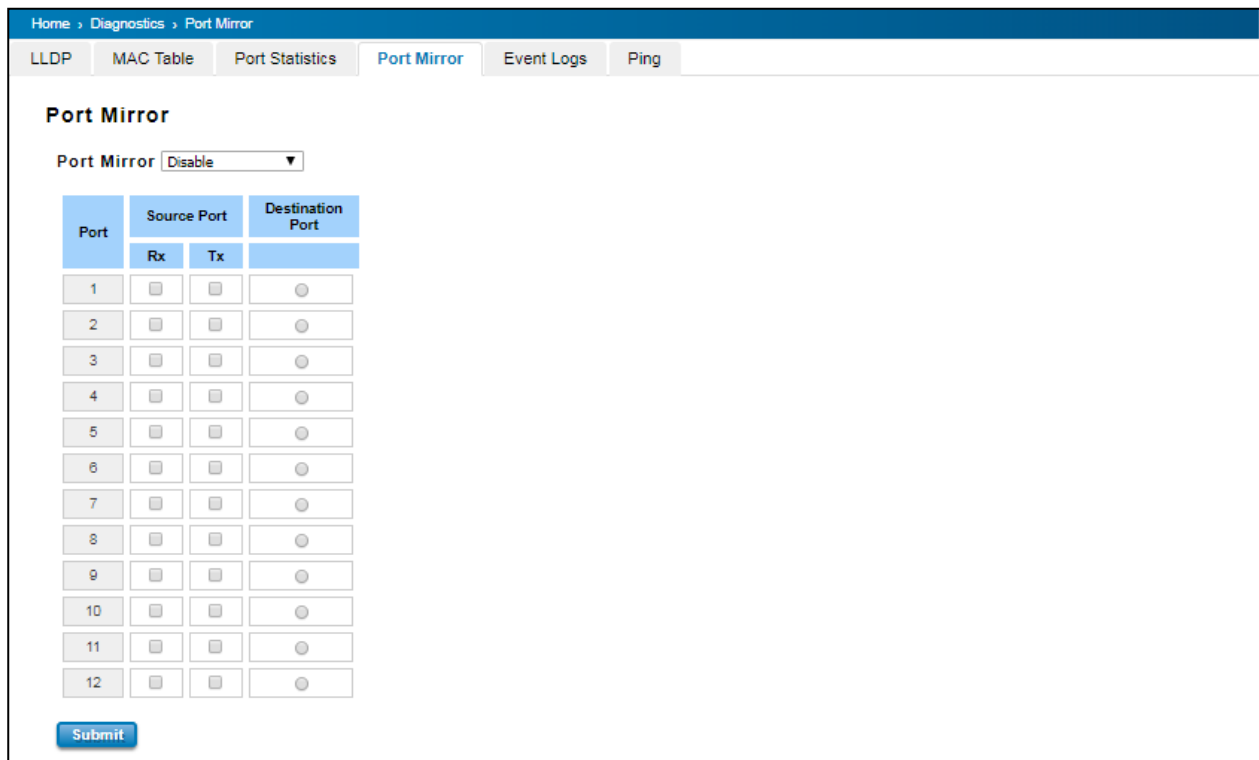
| Port                        | Type | Link         | State  | Rx Good   | Rx Bad | Rx Abort | Tx Good    | Tx Bad | Collision |
|-----------------------------|------|--------------|--------|-----------|--------|----------|------------|--------|-----------|
| <input type="checkbox"/> 1  | 100  | Connected    | Enable | 155947    | 0      | 94       | 1628434    | 0      | 0         |
| <input type="checkbox"/> 2  | 100  | Connected    | Enable | 2598107   | 0      | 52       | 1740950061 | 0      | 0         |
| <input type="checkbox"/> 3  | 0    | Disconnected | Enable | 151722118 | 0      | 3841     | 22607856   | 1      | 0         |
| <input type="checkbox"/> 4  | 1000 | Connected    | Enable | 849857338 | 0      | 8        | 857672721  | 4      | 0         |
| <input type="checkbox"/> 5  | 0    | Disconnected | Enable | 0         | 0      | 0        | 0          | 0      | 0         |
| <input type="checkbox"/> 6  | 0    | Disconnected | Enable | 984       | 0      | 0        | 192        | 0      | 0         |
| <input type="checkbox"/> 7  | 0    | Disconnected | Enable | 0         | 0      | 0        | 0          | 0      | 0         |
| <input type="checkbox"/> 8  | 0    | Disconnected | Enable | 867764923 | 0      | 8        | 868123192  | 0      | 0         |
| <input type="checkbox"/> 9  | 0    | Disconnected | Enable | 0         | 0      | 0        | 0          | 0      | 0         |
| <input type="checkbox"/> 10 | 0    | Disconnected | Enable | 0         | 0      | 0        | 0          | 0      | 0         |
| <input type="checkbox"/> 11 | 0    | Disconnected | Enable | 0         | 0      | 0        | 0          | 0      | 0         |
| <input type="checkbox"/> 12 | 0    | Disconnected | Enable | 0         | 0      | 0        | 0          | 0      | 0         |

Clear Selected
Clear All
Reload

Click on **Clear Selected** to reinitialize the counts of the selected ports, and **Clear All** to reinitialize the counts of all ports. Click on **Reload** to refresh the counts.

## 3.10.4 PORT MIRROR

Port mirroring is a tool that allows User to monitor data that being transmitted through a specific port. User can use this feature for diagnostics, debugging, and any kind of analysis. This is done by setting up another port (the mirror port) to receive the same data being transmitted from, or both to and from, the port under observation. Using a mirror port allows the network administrator to sniff the observed port to keep tabs on network activity. Any traffic will be duplicated at the Destination Port. All of the traffics at the Destination port can be analyzed using a monitoring tool.



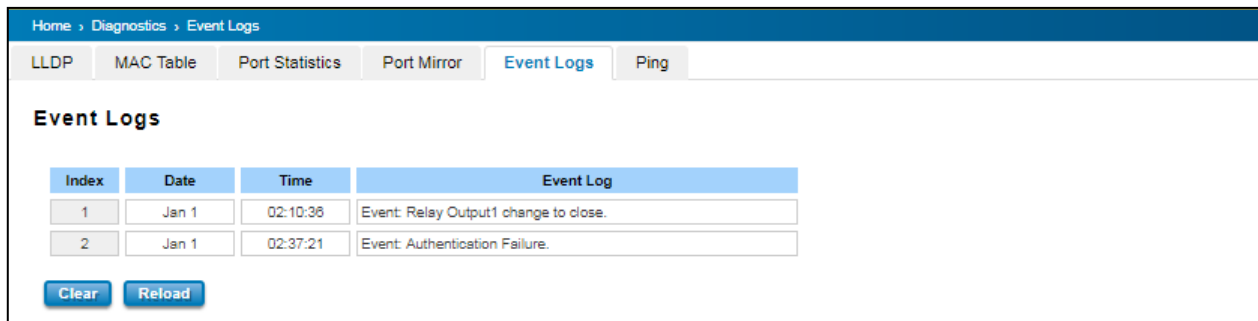
The configuration and settings explain as following.

| TERMS                   | Description   |
|-------------------------|---|
| <b>Port Mirror</b>      | Select Enable/Disable to enable/disable Port Mirror.  |
| <b>Source Port</b>      | These are the ports that User wants to monitor. The traffic of all source ports will be duplicated to destination ports. User can choose a single port, or multiple ports. Click on checkbox of the Port ID, RX, Tx or Both to select the source ports. |
| <b>Destination Port</b> | User can analyze the traffic of all the monitored ports at this port without affecting the flow of traffic on the port being monitored. Only one RX/TX of the destination port can be selected.   |

Once User finishes configuring the settings, click on **Submit** to apply the settings.

## 3.10.5 EVENT LOGS

This event logs page will show and record the system events log.



| Index | Date  | Time     | Event Log                             |
|-------|-------|----------|---------------------------------------|
| 1     | Jan 1 | 02:10:36 | Event: Relay Output1 change to close. |
| 2     | Jan 1 | 02:37:21 | Event: Authentication Failure.        |

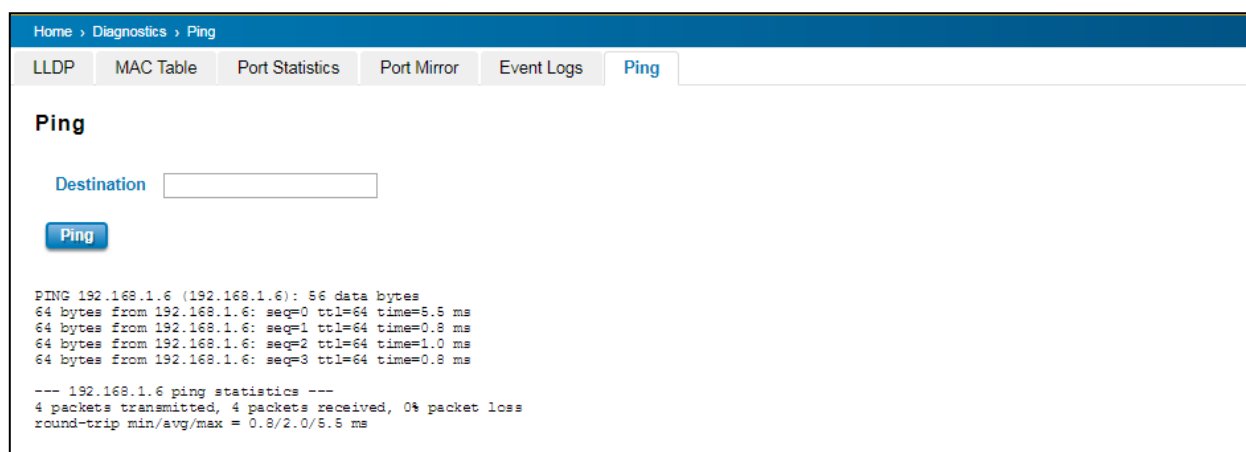
Click on **Clear** to clear the entries. Click on **Reload** to refresh the table.

The description of the columns is as below:

| TERMS     | Description   |
|-----------|---|
| Index     | Event index assigned to identify the event sequence.                                |
| Date      | The date is updated based on how the current date is set in the Basic Setting page. |
| Time      | The time is updated based on how the current time is set in the Basic Setting page. |
| Event Log | The occurred events.  |

## 3.10.6 PING

The function is to give users a simple but powerful tool for troubleshooting network problems and check that the remote device is still alive or not. Type **Destination** IP address of the target device and click on **Ping** to start the ping.



Destination

**Ping**

```

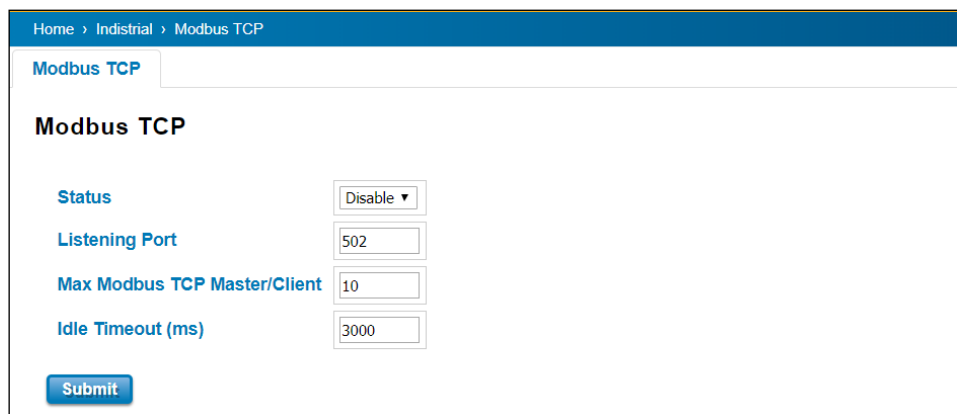
PING 192.168.1.6 (192.168.1.6): 56 data bytes
64 bytes from 192.168.1.6: seq=0 ttl=64 time=5.5 ms
64 bytes from 192.168.1.6: seq=1 ttl=64 time=0.8 ms
64 bytes from 192.168.1.6: seq=2 ttl=64 time=1.0 ms
64 bytes from 192.168.1.6: seq=3 ttl=64 time=0.8 ms

--- 192.168.1.6 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.8/2.0/5.5 ms
    
```



## 3.11 INDUSTRIAL

Switch's latest firmware provides Industrial Modbus features for User to monitor the status of the switch by Modbus TCP protocol. For example user can add the switch to their HMI dashboard and monitor the status by Modbus Read register.



The description of the columns is as below:

| TERMS                        | Description   |
|------------------------------|---|
| Status                       | Select Enable/Disable to enable/disable Modbus TCP.   |
| Listening Port               | Set the TCP port for listening Modbus TCP message. The range of the number is 1 to 65535. The default is <b>502</b> . |
| Max Modbus TCP Master/Client | Set the maximum Modbus TCP Master/Client connection. The default is <b>10</b> .                                       |
| Idle Timeout(ms)             | Set the Idle Timeout for the Modbus TCP connection. The default= <b>3000ms</b>  |

**Note:** The value of Modbus TCP table in below is for reference example, different model may have different product name, description, system name...etc. Some of the new settings may be updated without earlier notice.

Run Modbus TCP poll tool to see the latest values or contact our technical window for up to date info.

The following table shows the Modbus TCP table Example:

| Word Address              | Data Type | Description  |
|---------------------------|-----------|--|
| <b>System Information</b> |           |  |
| 0x0000                    | 32 words  | Product Name = "DRS610" (*Depends on product name)<br>Word 0 Hi byte = 'D'<br>Word 0 Lo byte = 'R'<br>Word 1 Hi byte = 'S'<br>Word 1 Lo byte = '6' |

|                  |           |   |
|------------------|-----------|---|
|                  |           | Word 2 Hi byte = '1'<br>Word 2 Lo byte = '0'<br>....<br>(other words = 0)   |
| 0x0020           | 256 words | Product Description = " Industrial Managed Ethernet Switch" (*Depends on product description)<br>Word 0 Hi byte = 'I'<br>Word 0 Lo byte = 'n'<br>Word 1 Hi byte = 'd'<br>Word 1 Lo byte = 'u'<br>Word 2 Hi byte = 's'<br>Word 2 Lo byte = 't'<br>Word 3 Hi byte = 'r'<br>Word 3 Lo byte = 'i'<br>Word 4 Lo byte = 'a'<br>Word 4 Hi byte = 'l'<br>.....<br>Word 14 Lo byte = 'S'<br>Word 14 Hi byte = 'w'<br>Word 15 Lo byte = 'i'<br>Word 15 Hi byte = 't'<br>Word 16 Lo byte = 'c'<br>Word 16 Hi byte = 'h'<br>Word 17 Lo byte = '\0'<br>(other words = 0) |
| 0x0120           | 128 words | SNMP system name (string)   |
| 0x01A0           | 128 words | SNMP system location (string)   |
| 0x0220           | 128 words | SNMP system contact (string)  |
| 0x02A0           | 32 words  | SNMP system OID (string)  |
| 0x02C0           | 2 words   | System uptime (unsigned long)   |
| 0x02C2 to 0x02FF | 62 words  | Reserved address space  |
| 0x0300           | 2 words   | Boot loader version<br>Word 0 Hi byte = first number of version<br>Word 0 Lo byte = second number of version<br>Word 1 Hi byte = third number of version<br>Word 1 Lo byte = fourth number of version<br>Version = v1.0.3.0   |

|                 |           |   |
|-----------------|-----------|---|
|                 |           | <p>Word 0 Hi byte = 0x1</p> <p>Word 0 Lo byte = 0x0</p> <p>Word 1 Hi byte = 0x3</p> <p>Word 1 Lo byte = 0x0</p>   |
| 0x0302          | 2 words   | <p>Firmware Version</p> <p>Word 0 Hi byte = first number of version</p> <p>Word 0 Lo byte = second number of version</p> <p>Word 1 Hi byte = third number of version</p> <p>Word 1 Lo byte = fourth number of version</p> <p>Ex: Version = v1.2</p> <p>Word 0 Hi byte = 0x1</p> <p>Word 0 Lo byte = 0x2</p> <p>Word 1 Hi byte = 0x0</p> <p>Word 1 Lo byte = 0x0</p> <p>Version = v1.2.3</p> <p>Word 0 Hi byte = 0x1</p> <p>Word 0 Lo byte = 0x2</p> <p>Word 1 Hi byte = 0x3</p> <p>Word 1 Lo byte = 0x0</p> <p>Version = v1.2.3.4</p> <p>Word 0 Hi byte = 0x1</p> <p>Word 0 Lo byte = 0x2</p> <p>Word 1 Hi byte = 0x3</p> <p>Word 1 Lo byte = 0x4</p> |
| 0x0304          | 2 words   | <p>Firmware Release Date</p> <p>Firmware was released on 2018-08-11 at 09 o'clock</p> <p>Word 0 = 0x0B09</p> <p>Word 1 = 0x1208</p>   |
| 0x0306          | 3 words   | <p>Ethernet MAC Address</p> <p>Ex: MAC = 01-02-03-04-05-06</p> <p>Word 0 Hi byte = 0x01</p> <p>Word 0 Lo byte = 0x02</p> <p>Word 1 Hi byte = 0x03</p> <p>Word 1 Lo byte = 0x04</p> <p>Word 2 Hi byte = 0x05</p> <p>Word 2 Lo byte = 0x06</p>  |
| 0x0309 to 0x3FF | 247 words | Reserved address space  |

# THOR200-PE20 User's Manual

Revision Date: Aug. 27. 2025



|                  |           |   |
|------------------|-----------|---|
| 0x0400           | 2 words   | IP address<br>Ex: IP = 192.168.10.1<br>Word 0 Hi byte = 0xC0<br>Word 0 Lo byte = 0xA8<br>Word 1 Hi byte = 0x0A<br>Word 1 Lo byte = 0x01 |
| 0x0402           | 2 words   | Subnet Mask   |
| 0x0404           | 2 words   | Default Gateway   |
| 0x0406           | 2 words   | DNS Server  |
| 0x0408 to 0x04FF | 248 words | Reserved address space (IPv6 or others)   |
| 0x0500           | 1 word    | Power1<br>0x0000:Off<br>0x0001:On<br>0xFFFF: unavailable  |
| 0x0501           | 1 word    | Power2<br>0x0000:Off<br>0x0001:On<br>0xFFFF: unavailable  |
| 0x0502           | 1 word    | Power3<br>0x0000:Off<br>0x0001:On<br>0xFFFF: unavailable  |
| 0x0503           | 1 word    | Power4<br>0x0000:Off<br>0x0001:On<br>0xFFFF: unavailable  |
| 0x0504 to 0x050F | 12 words  | Reserved address space  |
| 0x0510           | 1 word    | DI1<br>0x0000:Off<br>0x0001:On<br>0xFFFF: unavailable   |
| 0x0511           | 1 word    | DI2<br>0x0000:Off<br>0x0001:On<br>0xFFFF: unavailable   |
| 0x0512           | 1 word    | DO1<br>0x0000:Off   |

|                                    |            |  |
|------------------------------------|------------|--|
|                                    |            | 0x0001:On<br>0xFFFF: unavailable   |
| 0x0513                             | 1 word     | DO2<br>0x0000:Off<br>0x0001:On<br>0xFFFF: unavailable  |
| 0x0514 to 0x051F                   | 12 words   | Reserved address space   |
| 0x0520                             | 1 word     | SYS LED (Green light)<br>0x0000:Off<br>0x0001:On<br>0x0002: blinking<br>0x0003: blinking fast<br>0xFFFF: unavailable   |
| 0x0521                             | 1 word     | SYS LED(Yellow light)<br>0x0000:Off<br>0x0001:On<br>0x0002: blinking<br>0x0003: blinking fast<br>0xFFFF: unavailable   |
| 0x0522                             | 1 word     | R.S. LED (Green light)<br>0x0000:Off<br>0x0001:On<br>0x0002: blinking<br>0x0003: blinking fast<br>0xFFFF: unavailable  |
| 0x0523                             | 1 word     | R.S. LED (Yellow light)<br>0x0000:Off<br>0x0001:On<br>0x0002: blinking<br>0x0003: blinking fast<br>0xFFFF: unavailable |
| 0x0524 to<br>0x0BFF                | 1756 words | Reserved address space   |
| <b>Port Information (32 Ports)</b> |            |  |
| 0x1000 to<br>0x101F                | 1 word     | Operating Status<br>0x0000: Link down<br>0x0001: Link up   |

|                                      |          |   |
|--------------------------------------|----------|---|
|                                      |          | 0x0002: Disable<br>0xFFFF: No port  |
| 0x1020 to<br>0x103F                  | 1 word   | Speed/Duplex<br>0x0000: 10M-Half<br>0x0001: 10M-Full<br>0x0002: 100M-Half<br>0x0003: 100M-Full<br>0x0004: 1000M-Half<br>0x0005: 1000M-Full<br>0xFFFF: No port |
| 0x1040 to<br>0x105F                  | 1 word   | Flow Control<br>0x0000: off<br>0x0001: on<br>0xFFFF: No port  |
| 0x1060 to<br>0x107F                  | 1 word   | MDI/MDIX<br>0x0000: MDI<br>0x0001: MDIX<br>0xFFFF: No port  |
| 0x1080 to<br>0x109F                  | 1 word   | Medium mode<br>0x0000: copper<br>0x0001: fiber<br>0x0002: none<br>0xFFFF: No port   |
| 0x10A0 to<br>0x10BF                  | 1 word   | STP Status<br>0x0000: disabled<br>0x0001: blocking<br>0x0002: listening<br>0x0003: learning<br>0x0004: forwarding<br>0xFFFF: No port                          |
| 0x10C0 to 0x14BF                     | 32 words | Port Description  |
| <b>Packet information (32 Ports)</b> |          |   |
| 0x2000 to<br>0x203F                  | 2 words  | Tx Packets<br>Ex: port 1 Tx Packet Amount = 44332211 Received MODBUS response:<br>0x44332211<br>Word 0 = 4433<br>Word 1 = 2211                                |

|                                       |            |   |
|---------------------------------------|------------|---|
| 0x2040 to<br>0x207F                   | 2 words    | Rx Packets<br>Ex: port 1 Rx Packet Amount = 44332211 Received MODBUS response:<br>0x44332211<br>Word 0 = 4433<br>Word 1 = 2211                                    |
| 0x2080 to<br>0x20BF                   | 2 words    | Tx Error Packets<br>Ex: port 1 Tx Packet Amount = 44332211 Received MODBUS response:<br>0x44332211<br>Word 0 = 4433<br>Word 1 = 2211                              |
| 0x20C0 to<br>0x20FF                   | 2 words    | Rx Error Packets<br>Ex: port 1 Rx Packet Amount = 44332211 Received MODBUS response:<br>0x44332211<br>Word 0 = 4433<br>Word 1 = 2211                              |
| 0x2100 to<br>0x2BFF                   | 2816 words | Reserved address space  |
| 0x2C00                                | 1 words    | Clear ROMN by bitmap of port 1 to 16<br>Write to clear<br>Read to return 0x0000<br>To clear port 1<br>Word = 0x0001<br>To clear port 1 and 2<br>Word = 0x0003     |
| 0x2C01                                | 1 words    | Clear ROMN by bitmap of port 17 to 32<br>Write to clear<br>Read to return 0x0000<br>To clear port 17<br>Word = 0x0001<br>To clear port 17 and 18<br>Word = 0x0003 |
| <b>Network Redundancy Information</b> |            |   |
| 0x3000                                | 1 word     | Ring 0's Status<br>0x0000: none<br>0x0001: Disable<br>0x0002: Enable<br>0xFFFF: unavailable   |

|        |         |  |
|--------|---------|--|
| 0x3001 | 1 word  | Ring 0's Version<br>0x0000: none<br>0x0001: v1<br>0x0002: v2<br>0xFFFF: unavailable  |
| 0x3002 | 1 word  | Ring 0's Node State<br>0x0000: Disabled<br>0x0001: Initial<br>0x0002: Idle<br>0x0003: Protection<br>0x0004: Manual Switch<br>0x0005: Forced Switch<br>0x0006: Pending<br>0xFFFF: unavailable |
| 0x3003 | 1 word  | Ring 0's Ring Type<br>0x0000: none<br>0x0001: Major Ring<br>0x0002: Sub Ring<br>0xFFFF: unavailable  |
| 0x3004 | 1 word  | Ring 0's Node Role<br>0x0000: none<br>0x0001: Ring node<br>0x0002: RPL Owner<br>0x0003: RPL Neighbor<br>0xFFFF: unavailable  |
| 0x3005 | 1 word  | Ring 0's Control Channel   |
| 0x3006 | 1 words | Ring 0's Sub Ring without Virtual Channel<br>0x0000: none<br>0x0001: True<br>0x0002: False<br>0xFFFF: unavailable  |
| 0x3007 | 1 word  | Ring 0's Virtual Channel of Sub Ring   |
| 0x3008 | 1 word  | Ring 0's Ring Port 0<br>0x0000: none<br>0x0001: port 1   |



|        |        |  |
|--------|--------|--|
|        |        | 0x0002: port 2<br>...<br>0x001C: port 28<br>0xFFFF: unavailable  |
| 0x3009 | 1 word | Ring 0's Ring Port 1<br>0x0000: none<br>0x0001: port 1<br>0x0002: port 2<br>...<br>0x001C: port 28<br>0xFFFF: unavailable                          |
| 0x300A | 1 word | Ring 0's Ring Port 0 state<br>0x0000: disabled<br>0x0001: blocking<br>0x0002: listening<br>0x0003: learning<br>0x0004: forwarding                  |
| 0x300B | 1 word | Ring 0's Ring Port 1 state<br>0x0000: disabled<br>0x0001: blocking<br>0x0002: listening<br>0x0003: learning<br>0x0004: forwarding                  |
| 0x300C | 1 word | Ring 0's Ring Port 0 RMEP ID<br>0x0000: none<br>0x0001: RMEP ID = 1<br>0x0002: RMEP ID = 2<br>...<br>0x1FFF: RMEP ID = 8191<br>0xFFFF: unavailable |
| 0x300D | 1 word | Ring 0's Ring Port 1 RMEP ID<br>0x0000: none<br>0x0001: RMEP ID = 1<br>0x0002: RMEP ID = 2<br>...<br>0x1FFF: RMEP ID = 8191<br>0xFFFF: unavailable |

|                     |          |  |
|---------------------|----------|--|
| 0x300E              | 1 word   | Ring 0's RPL port<br>0x0000: RPL port = Ring port 0<br>0x0001: RPL port = Ring port 1<br>0xFFFF: unavailable   |
| 0x300F              | 1 word   | Ring 0's Revertive Mode<br>0x0000: Revertive<br>0x0001: non-Revertive<br>0xFFFF: unavailable   |
| 0x3010              | 1 word   | Ring 0's Instance  |
| 0x3011              | 1 word   | Ring 0's Manual Switch<br>0x0000: Manual Switch port = Ring port 0<br>0x0001: Manual Switch port = Ring port 1<br>0x0001: Manual Switch port = none<br>0xFFFF: unavailable |
| 0x3012              | 1 word   | Ring 0's Force Switch<br>0x0000: Force Switch port = Ring port 0<br>0x0001: Force Switch port = Ring port 1<br>0x0001: Force Switch port = none<br>0xFFFF: unavailable     |
| 0x3013 to<br>0x301F | 13 words | Reserved address space   |
| 0x3020 to<br>0x303F |          | ERPS Ring 1's Information  |
| 0x3040 to<br>0x305F |          | ERPS Ring 2's Information  |
| 0x3060 to<br>0x307F |          | ERPS Ring 3's Information  |
| 0x3080 to<br>0x309F |          | ERPS ERPS Ring 4's Information   |
| 0x30A0 to<br>0x30BF |          | ERPS Ring 5's Information  |
| 0x30C0 to<br>0x30DF |          | ERPS Ring 6's Information  |
| 0x30E0 to<br>0x30FF |          | ERPS Ring 7's Information  |
| 0x3100 to           |          | ERPS Ring 8's Information  |

# THOR200-PE20 User's Manual

Revision Date: Aug. 27, 2025



|                     |  |                            |
|---------------------|--|----------------------------|
| 0x311F              |  |                            |
| 0x3120 to<br>0x313F |  | ERPS Ring 9's Information  |
| 0x3140 to<br>0x315F |  | ERPS Ring 10's Information |
| 0x3160 to<br>0x317F |  | ERPS Ring 11's Information |
| 0x3180 to<br>0x319F |  | ERPS Ring 12's Information |
| 0x31A0 to<br>0x31BF |  | ERPS Ring 13's Information |
| 0x31C0 to<br>0x31DF |  | ERPS Ring 14's Information |
| 0x31E0 to<br>0x31FF |  | ERPS Ring 15's Information |
| 0x3200 to<br>0x321F |  | ERPS Ring 16's Information |
| 0x3220 to<br>0x323F |  | ERPS Ring 17's Information |
| 0x3240 to<br>0x325F |  | ERPS Ring 18's Information |
| 0x3260 to<br>0x327F |  | ERPS Ring 19's Information |
| 0x3280 to<br>0x329F |  | ERPS Ring 20's Information |
| 0x32A0 to<br>0x32BF |  | ERPS Ring 21's Information |
| 0x32C0 to<br>0x32DF |  | ERPS Ring 22's Information |
| 0x32E0 to<br>0x32FF |  | ERPS Ring 23's Information |
| 0x3300 to<br>0x331F |  | ERPS Ring 24's Information |
| 0x3320 to<br>0x333F |  | ERPS Ring 25's Information |
| 0x3340 to<br>0x335F |  | ERPS Ring 26's Information |

# THOR200-PE20 User's Manual

Revision Date: Aug. 27. 2025



|                     |  |                            |
|---------------------|--|----------------------------|
| 0x3360 to<br>0x337F |  | ERPS Ring 27's Information |
| 0x3380 to<br>0x339F |  | ERPS Ring 28's Information |
| 0x33A0 to<br>0x33BF |  | ERPS Ring 29's Information |
| 0x33C0 to<br>0x33DF |  | ERPS Ring 30's Information |
| 0x33E0 to<br>0x33FF |  | ERPS Ring 31's Information |

## 3.12 PoE

Power over Ethernet has become increasingly popular due in large part to the reliability provided by PoE Ethernet switches that supply the necessary power to Powered Devices (PD) when AC power is not readily available or cost-prohibitive to provide locally. DIN Rail PoE Switch compliant with IEEE 802.3af and IEEE 802.3at.

Power over Ethernet can be used with:

- Surveillance cameras
- Security I/O sensors
- Industrial wireless access points
- Emergency IP phones

### 3.12.1 PoE STATUS

The PoE Status page shows the system PoE status and the operating status of each PoE Port. The system information includes power budget & utilization, the port information includes PoE port mode, operation status, PD class, power budget and PoE output power consumption, voltage and current. Click “Reload” can refresh the status.

Home > PoE > PoE Status

PoE StatusPoE Settings ▾PoE ScheduleAlive CheckPoE Event

PoE Status

Power 1

Budget 120 W

Power 2

Budget 120 W

Total Power Budget

120 W

Total Output Power

62.92 W

Utilization

52 %

Event

Normal

| Port | Mode   | Status   | Class  | Budget(w) | Consumption(W) | Voltage(V) | Current(mA) |
|------|--------|----------|--------|-----------|----------------|------------|-------------|
| 5    | Enable | Powering | Class4 | 33.00     | 0.76           | 54.5       | 14          |
| 6    | Enable | Powering | Class4 | 33.00     | 0.60           | 54.7       | 11          |
| 7    | Enable | Powering | Class4 | 33.00     | 0.60           | 54.7       | 11          |
| 8    | Enable | Powering | Class4 | 33.00     | 15.67          | 54.6       | 287         |
| 9    | Enable | Powering | Class4 | 17.00     | 14.96          | 54.6       | 274         |
| 10   | Enable | Powering | Class4 | 17.00     | 14.16          | 54.6       | 259         |
| 11   | Enable | Powering | Class4 | 17.00     | 14.21          | 54.6       | 260         |
| 12   | Enable | Powering | Class4 | 17.00     | 1.96           | 54.5       | 36          |

Reload

Example of PoE Port Status in the figure above, the Port 8 is enabled and is supplying power to a Class 4 Powered Device (PD) indicated under the Classification column. The PD device is rated at 54.6V and 287mA. The total power consumption for this PD is 15.67W with Budget 33W(802.3at mode). To check the status of the PoE port, please click on the Reload button.

The description of the columns is as below:

| TERMS           | Description   |
|-----------------|---|
| Mode            | Enable/Disable/Schedule Indicates the PoE port status   |
| Status          | <b>Default: Off</b><br>PoE status is included Off, Powering, and Searching.<br>Off – PoE is inactive.<br>Powering – PoE is enabled and powering the PD.<br>Searching – Searching the PD which need the power. |
| Class           | Indicates the PD included in which PoE class.   |
| Budget(W)       | The Budget you manually configured while Power mode is in Force Mode.<br>Step: Force Mode -> Manual -> Budget   |
| Consumption (W) | Indicates the actual Power consumed value for PoE port  |
| Voltage (V)     | Indicates the actual Voltage consumed value for PoE port  |
| Current (mA)    | Indicates the actual Current consumed value for PoE port  |

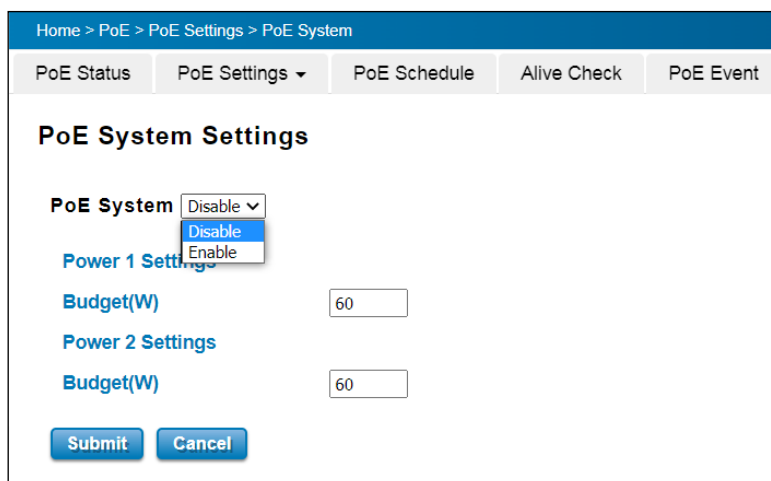
### 3.12.2 PoE SYSTEM/PORT SETTING

The PoE setting includes 3 parts, **PoE System Setting**, **PoE Port setting** and **PD status detection** (depends on model).

The following section will introduce the function.

#### PoE Setting – PoE System

**Non Pre-configured Budget Model: (Ex: DC Model)**



The figure above is **System Setting** interface. In this section, user can enable or disable the PoE function.

The description of the columns is as below:

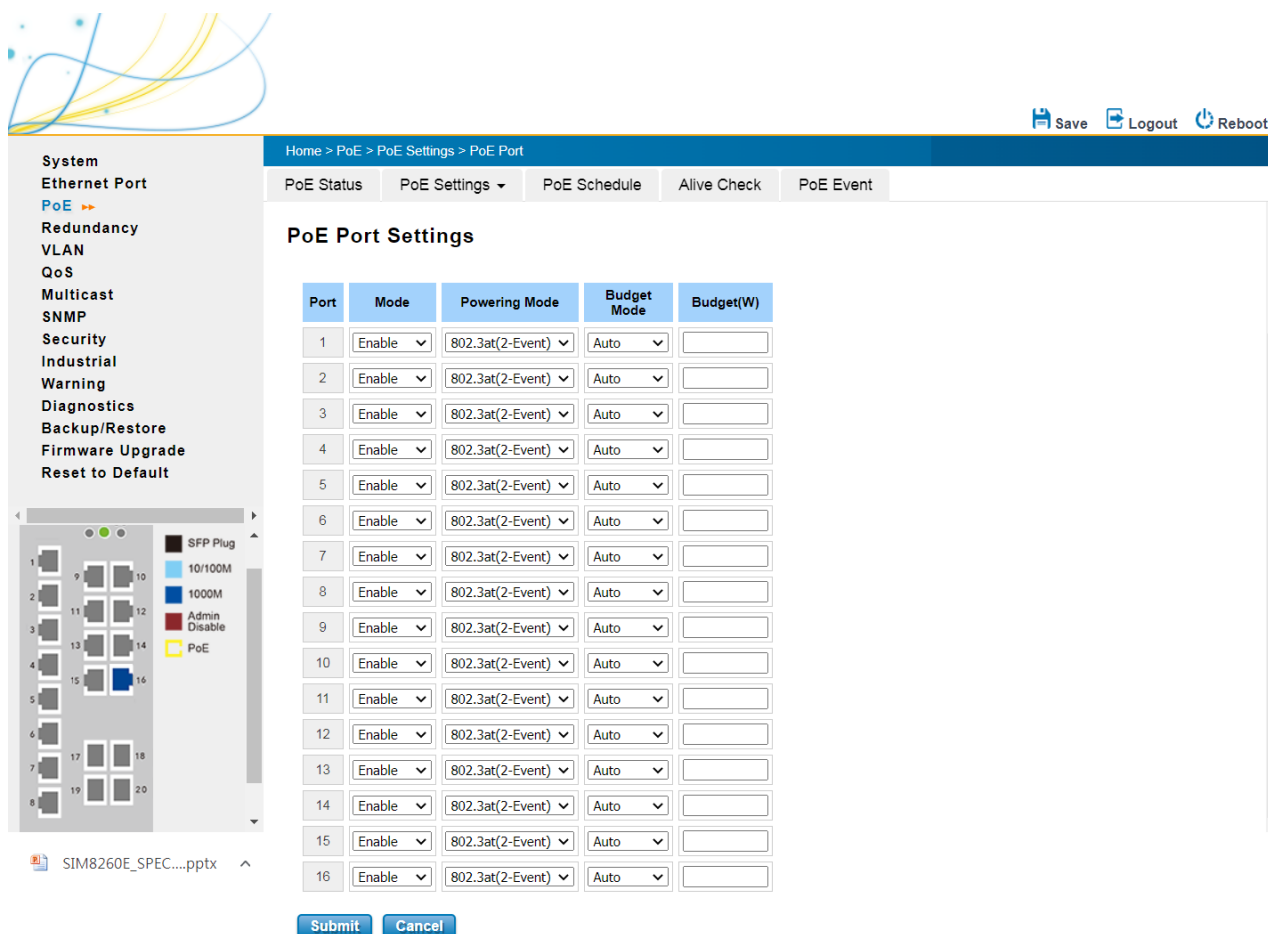
| TERMS      | Description  |
|------------|--|
| PoE System | Default: <b>Disable</b><br>Enable or disable system's PoE function.  |
| Budget (W) | Default: <b>0W</b><br>The power supply maximum output budget. "0" means no power for PoE even you enabled PoE system setting. Some models do not support this setting. |

After finished configuring the settings, click on Submit to save the configuration.

**WARNING:** You must assign correct power budget for each power source, especially for the low voltage booster PoE switch. If the power budget is insufficient, the fuse of the system or PoE components will be damaged. Type the correct budget limit while enabled the PoE system is important.

## PoE Setting – PoE Port

The PoE ports of the THOR200-PE20 is range from port 9-16. After configured the PoE System settings, move to the "PoE Port" mode to configure PoE Ports' setting.



Home > PoE > PoE Settings > PoE Port

PoE Status PoE Settings PoE Schedule Alive Check PoE Event

### PoE Port Settings

| Port | Mode   | Powering Mode    | Budget Mode | Budget(W) |
|------|--------|------------------|-------------|-----------|
| 1    | Enable | 802.3at(2-Event) | Auto        |           |
| 2    | Enable | 802.3at(2-Event) | Auto        |           |
| 3    | Enable | 802.3at(2-Event) | Auto        |           |
| 4    | Enable | 802.3at(2-Event) | Auto        |           |
| 5    | Enable | 802.3at(2-Event) | Auto        |           |
| 6    | Enable | 802.3at(2-Event) | Auto        |           |
| 7    | Enable | 802.3at(2-Event) | Auto        |           |
| 8    | Enable | 802.3at(2-Event) | Auto        |           |
| 9    | Enable | 802.3at(2-Event) | Auto        |           |
| 10   | Enable | 802.3at(2-Event) | Auto        |           |
| 11   | Enable | 802.3at(2-Event) | Auto        |           |
| 12   | Enable | 802.3at(2-Event) | Auto        |           |
| 13   | Enable | 802.3at(2-Event) | Auto        |           |
| 14   | Enable | 802.3at(2-Event) | Auto        |           |
| 15   | Enable | 802.3at(2-Event) | Auto        |           |
| 16   | Enable | 802.3at(2-Event) | Auto        |           |

Submit Cancel

The description of the columns is as below:

| TERMS                | Description  |
|----------------------|--|
| <b>Mode</b>          | Enable/Disable/Schedule port's PoE function.   |
| <b>Powering Mode</b> | <b>802.3af, 802.3at (LLDP), 802.3at (2-event) and Forced mode.</b><br><b>*Forced mode will ignore the classification behaviors and apply power onto the RJ-45, uses the forced mode must be carefully.</b>                               |
| <b>Budget Mode</b>   | Choose budget mode as <b>Auto</b> or <b>Manual</b> .<br>If user chooses Auto, the budget would be delivered automatically based on the end device requirement. If user chooses Manual, user can input the number at the budget text box. |
| <b>Budget (W)</b>    | Input the budget.  |

After finished configuring the settings, click on **Submit** to save the configuration.

**Note:** If the system PoE consumption is over the system budget control, the PoE system will turn off low priority port PoE function, until the consumption is becomes smaller than the system budget. In THOR200-PE20, the PoE priority is depended on port number, the small port number has higher priority than high port number. It means port 9 always has highest priority, then the port 10, 11... and port 16 is the lowest priority port.

The priority setting is pre-configured in the system. There is no Web GUI and you don't need to configure it.

### 3.12.3 PoE SCHEDULING

For energy saving or power recycle powered devices, the PoE managed switch's **PoE scheduling** interface allows users to appoint any date and time to enable or disable PoE functions for each PoE port. User need to configure **PoE Scheduling** and select a target port manually to enable this function. The figure below is PoE Schedule interface.

### 3.12.4 PD ALIVE CHECK

The switch supports a useful function that help user to maintain the PD's status and help use to saving the maintenance time and money. Once user defined this function, the PoE Switch will send Ping Request to the PD system every Ping Interval time and turn-off PoE power if the PD system does not echo the request.



## PD Alive Check

☐ Enable PD Alive Check

| PD | IP Address     | Ping Interval | Delete                   |
|----|----------------|---------------|--------------------------|
| 1  | 192.168.10.101 | 120           | <input type="checkbox"/> |
| 2  | 192.168.10.102 | 120           | <input type="checkbox"/> |
| 3  | 192.168.10.103 | 120           | <input type="checkbox"/> |
| 4  | 192.168.10.104 | 120           | <input type="checkbox"/> |
| 5  | 192.168.10.105 | 120           | <input type="checkbox"/> |
| 6  | 192.168.10.106 | 120           | <input type="checkbox"/> |
| 7  | 192.168.10.107 | 120           | <input type="checkbox"/> |
| 8  | 192.168.10.108 | 120           | <input type="checkbox"/> |

Submit

Cancel

The description of the columns is as below:

| TERMS                 | Description  |
|-----------------------|--|
| Enable PD Alive Check | Select "Enable..." box to enable the function.<br>Make sure you have correct target IP address of the connected PD(IP Cam) before enable the function. |
| IP address            | PD's IP-address that installed on the port.  |
| Ping Interval         | The system will ping the target IP address you configured every the Ping Interval time.  |
| Delete                | Delete PD's IP-address that has been selected.   |

After finished configuring the settings, click on **Submit** to save the configuration.

### 3.12.5 PoE EVENT

In this section, user is allowed to configure the PoE Event, the value is Enable and Disable.

After enabled, the event will be generated while the PoE ON/OFF status is changed.

## PoE Event

### PoE Event Selection

| Port | Event             |
|------|-------------------|
| 5    | Disable           |
| 6    | Disable<br>Enable |
| 7    | Disable           |
| 8    | Disable           |
| 9    | Disable           |
| 10   | Disable           |
| 11   | Disable           |
| 12   | Disable           |

Submit

Cancel

## 3.13 BACKUP AND RESTORE

User can use Backup and Restore configuration to save and load configuration through the switch. There are 3 modes for users to backup/restore the configuration file.

WEB

TFTP

WEB Backup and Restore

Restore Settings

Choose File

No file chosen

Upload

Backup Settings

Save...

**Web** mode: In this mode, the switch acts as the file server. Users can browse the target folder and then type the file name to back-up the configuration. Browse the target folder and select existed configuration file to restore the configuration back to the switch. This mode is only provided by Web UI while CLI is not supported.

WEB

TFTP

TFTP Backup and Restore

TFTP Server IP

File Name

DP412-9466E7ABCDEF.conf

Action

☒ Load
 ☐ Save

Submit

**TFTP Server** mode: In this mode, the switch acts as TFTP client. Before do so, make sure that TFTP server is ready. Then please type the IP address of TFTP Server and Backup configuration file name. This mode can be used in both CLI and Web UI.

The description of the columns is as below:

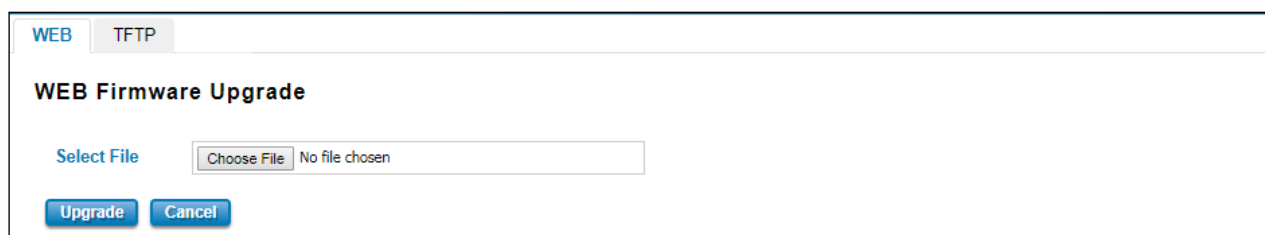
| TERMS                      | Description  |
|----------------------------|--|
| TFTP Server IP             | User needs to key in the IP address of TFTP Server here.   |
| File Name                  | Type the correct file name of the configuration file.  |
| Configuration File (.conf) | The configuration file of the switch is a pure text file. User can open it by word/txt read file. User can also modify the file, add/remove the configuration settings, and then restore back to the switch. |
| Action                     | User can choose to Load or Save configuration  |

## 3.14 FIRMWARE UPGRADE

The new firmware may include new features, bug fixes or other software changes. The release notes for the update as well. For technical viewpoint, it suggests user uses the latest firmware before installing the switch to the customer site.

**NOTE:** Note that the system will be automatically rebooted after User finished upgrading the new firmware. Please remind the attached network users before User performs this function.

There are 3 modes for users to backup/restore the configuration file, Local File mode, USB and TFTP Server mode.



**Web** mode: The switch acts as the file server. Users can browse the target folder and then type the file name to back-up the configuration. Users also can browse the target folder and select the existed upgrade file. This mode is only provided by Web UI while CLI is not supported.



**TFTP Server** mode: In this mode, the switch acts as the TFTP client. Before do so, make sure that TFTP server is ready. Then please type the IP address of TFTP Server and Backup configuration file name. This mode can be used in both CLI and Web UI.

The description of the columns is as below:

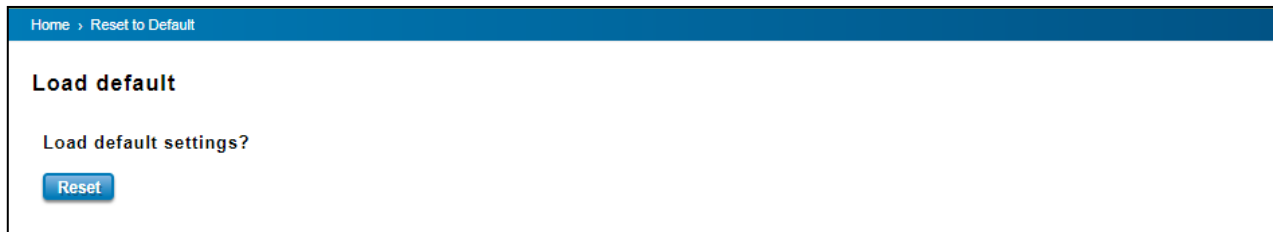
| TERMS     | Description   |
|-----------|---|
| IP        | User need to key in the IP address of TFTP Server here. |
| File Name | Type the correct file name of the configuration file.   |

The UI also shows User the current firmware version and built date of current firmware upgrade. Please check the version number after the switch is rebooted. Input the TFTP Server IP Address and the specific File Name. Then click on **Upgrade** to start the process. After finishing transmitting the firmware, the system will copy the firmware file and replace the firmware in the flash.

## 3.15 RESET TO DEFAULTS

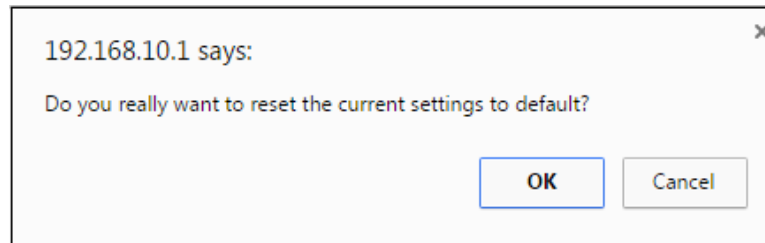
This function provides users with a quick way of restoring the switch's configuration to factory defaults. The function is available in the serial, Telnet, and web consoles.

### Factory Default main screen



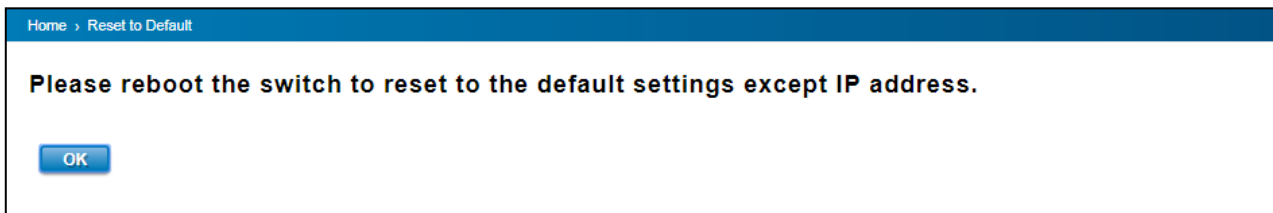
The screenshot shows the 'Factory Default main screen' of the web console. At the top, there is a blue header bar with the text 'Home > Reset to Default'. Below the header, the main content area has the title 'Load default' in bold. Underneath, it says 'Load default settings?' followed by a blue button labeled 'Reset'.

Pop-up message screen to show User that have done the command. Click on **OK** to close the screen.



The screenshot shows a pop-up message screen. It has a light gray background and a thin border. In the top right corner, there is a small 'x' icon to close the window. The text inside reads: '192.168.10.1 says:' followed by 'Do you really want to reset the current settings to default?'. At the bottom right, there are two buttons: 'OK' and 'Cancel'.

Then please go to **Reboot** page to reboot the switch. Click **OK**. The system will auto reboot the device.



The screenshot shows the 'Reboot confirmation screen' of the web console. It has a blue header bar with the text 'Home > Reset to Default'. Below the header, the main content area has the text 'Please reboot the switch to reset to the default settings except IP address.' in bold. At the bottom left, there is a blue button labeled 'OK'.

## 3.16 SAVE

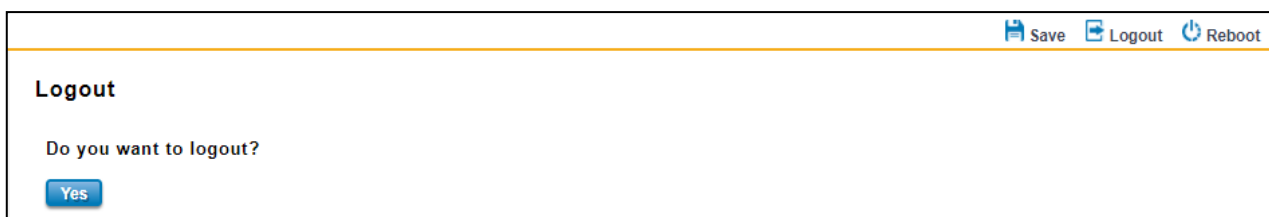
**Save** option allows user to save any configuration. Powering off the switch without clicking on **Save** will cause loss of new settings. After selecting **Save**, click on **Yes** to save new configuration.



The screenshot shows a web interface with a top navigation bar containing 'Save', 'Logout', and 'Reboot' buttons. The main content area is titled 'Save' and contains the text 'Do you want to save all submitted changes?' followed by a 'Yes' button.

## 3.17 LOGOUT

There are 2 logout methods. If user doesn't input any command within 30 seconds, the web connection will be logged out. The Logout command allows user to manually logout the web connection. Click on **Yes** to logout.



The screenshot shows a web interface with a top navigation bar containing 'Save', 'Logout', and 'Reboot' buttons. The main content area is titled 'Logout' and contains the text 'Do you want to logout?' followed by a 'Yes' button.

## 3.18 REBOOT

System Reboot allows user to reboot the device. Some of the feature changes require user to reboot the system. Click on **Reboot** to reboot device.

**NOTE:** Remember to click on Save button to save configuration settings. Otherwise, the settings user made will be gone when the switch is powered off.


Reboot main screen, to do confirmation request. Click **Yes**, then the switch will reboot immediately.

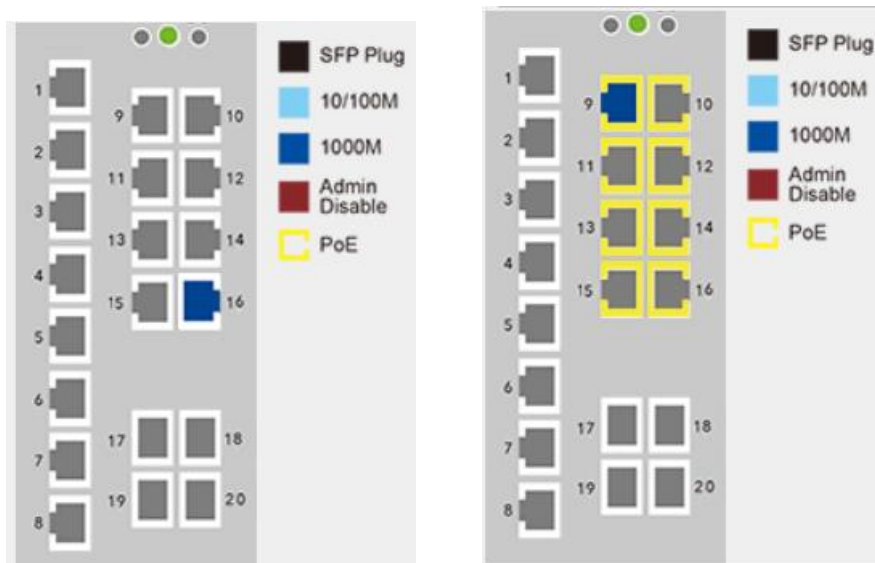


The screenshot shows a web interface with a top navigation bar containing 'Save', 'Logout', and 'Reboot' buttons. The main content area is titled 'Reboot' and contains the text 'Do you want to reboot?' followed by a 'Yes' button.

## 3.19 FRONT PANEL

Front Panel commands allow user to see LED status of the switch. User can see LED and link status of the Power, DO and Port Status. Front panel interface, can be seen on the web consoles. Shown as below.

Click  button to refresh and update the latest status.



(PoE Enabled)

The description of the Front Panel is as below:

| Feature              | LED On  | LED off                                |
|----------------------|---|--|
| <b>P1/P2</b>         | Green on: Power is on   | No power                               |
| <b>DO/ALM</b>        | Red on: alarm relay active and contacts is short.   | Red off: relay output contact is open. |
| <b>10/100M</b>       | Light Blue on: Port is linked   | Port link is down                      |
| <b>1000M</b>         | Dark Blue on: The port is linked at 1000Mbps speed.                                       | Not available                          |
| <b>PoE</b>           | Yellow On: PoE Setting is Enabled and PD is connected, or the PoE Port set to Forced mode | PoE Setting is Disabled                |
| <b>Admin Disable</b> | Maroon on: Port disable   | Not available                          |