Smarter. Greener. Together.

## Industrial Automation Headquarters

**Delta Electronics, Inc.**
Taoyuan Technology Center
No.18, Xinglong Rd., Taoyuan City,
Taoyuan County 33068, Taiwan
TEL: 886-3-362-6301 / FAX: 886-3-371-6301

## Asia

**Delta Electronics (Jiangsu) Ltd.**
Wujiang Plant 3
1688 Jiangxing East Road,
Wujiang Economic Development Zone
Wujiang City, Jiang Su Province, P.R.C. 215200
TEL: 86-512-6340-3008 / FAX: 86-769-6340-7290

**Delta Greentech (China) Co., Ltd.**
238 Min-Xia Road, Pudong District,
ShangHai, P.R.C. 201209
TEL: 86-21-58635678 / FAX: 86-21-58630003

**Delta Electronics (Japan), Inc.**
Tokyo Office
2-1-14 Minato-ku Shibadaimon,
Tokyo 105-0012, Japan
TEL: 81-3-5733-1111 / FAX: 81-3-5733-1211

**Delta Electronics (Korea), Inc.**
1511, Byucksan Digital Valley 6-cha, Gasan-dong,
Geumcheon-gu, Seoul, Korea, 153-704
TEL: 82-2-515-5303 / FAX: 82-2-515-5302

**Delta Electronics Int'l (S) Pte Ltd.**
4 Kaki Bukit Ave 1, #05-05, Singapore 417939
TEL: 65-6747-5155 / FAX: 65-6744-9228

**Delta Electronics (India) Pvt. Ltd.**
Plot No 43 Sector 35, HSIIDC
Gurgaon, PIN 122001, Haryana, India
TEL : 91-124-4874900 / FAX : 91-124-4874945

## Americas

**Delta Products Corporation (USA)**
Raleigh Office
P.O. Box 12173,5101 Davis Drive,
Research Triangle Park, NC 27709, U.S.A.
TEL: 1-919-767-3800 / FAX: 1-919-767-8080

**Delta Greentech (Brasil) S.A.**
Sao Paulo Office
Rua Itapeva, 26 - 3° andar Edificio Itapeva One-Bela Vista
01332-000-São Paulo-SP-Brazil
TEL: 55 11 3568-3855 / FAX: 55 11 3568-3865

## Europe

**Delta Electronics (Netherlands) B.V.**
Eindhoven Office
De Witbogt 20, 5652 AG Eindhoven, The Netherlands
TEL : +31 (0)40-8003800 / FAX : +31 (0)40-8003898

2016-10-19




# DVS-G512 Series Gigabit PoE+ Managed Industrial Ethernet Switch User Manual

www.deltaww.com

Smarter. Greener. Together.

# DVS PoE Managed Industrial

# Ethernet Switch User Manual

## Table of Contents

# Chapter 1 Introduction

## Table of Contents

## FCC Interference Statement

This equipment has been tested and found to comply with the limits for a class A digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation.
This equipment generates radio frequency signal and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
---Reorient or relocate the receiving antenna.
---Increase the separation between the equipment and receiver.
---Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
---Consult the dealer or an experienced radio/TV technician for help.

## CE Declaration of Conformity

The DVS series switches are CE certificated products. They could be used in any kind of the environments under CE environment specification. For keeping more safe application, we strongly suggest to use the CE-compliant industrial enclosure products.

# 1.1 Feature

Thank you for purchasing the DVS PoE Managed Industrial Ethernet Switches. The DVS PoE series switches including Unmanaged and Managed PoE switches. The DVS PoE Managed switch support Power over Ethernet, a system to transmit electrical power up to 30 watts per port, and allow the wide range of operating temperature (-40 to 70℃). The DVS PoE series switches are designed to support the application in any rugged environment and comply with CE and FCC standards.

### 1.1.1 High Performance Network Technology

- 10/100/1000Base-T(X) Ethernet PoE Ports
- 100/1000Base-SFP Fiber
- Auto negotiation speed
- Auto MDI/MDI-X

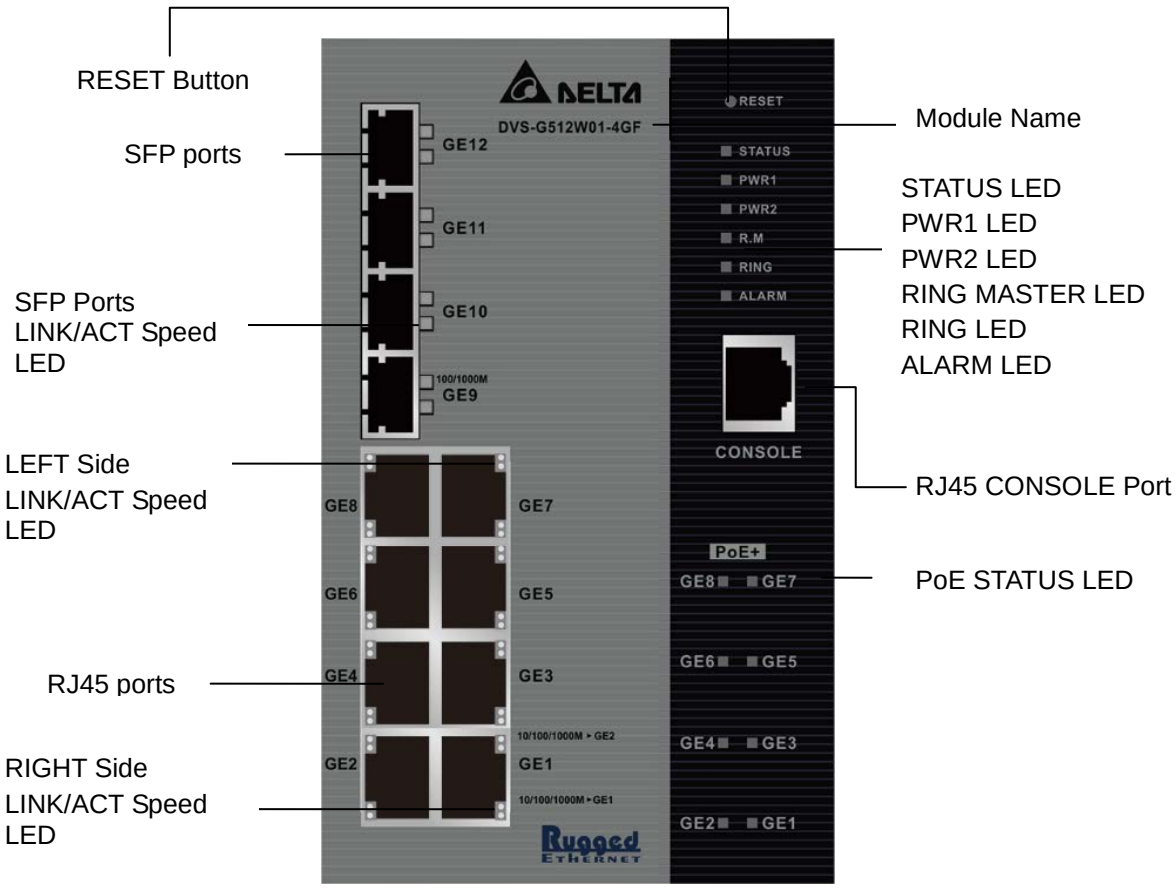
### 1.1.2 Industrial Grade Reliability

- Redundant dual DC power inputs
- 1 set of Relay Alarm

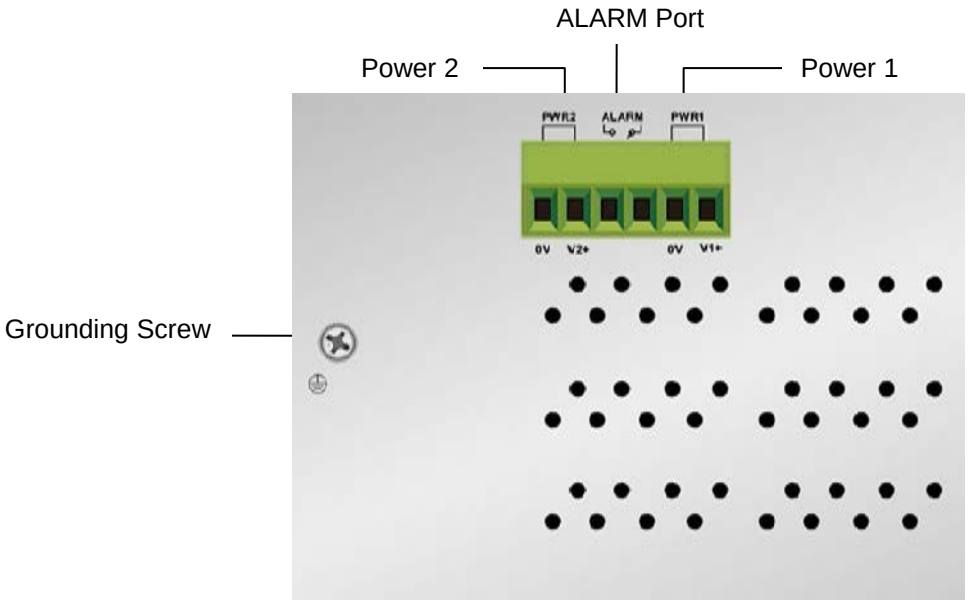
### 1.1.3 Robust Design

- Operating temperature: -40~70℃
- Storage temperature: -40~85 ℃
- Humidity: 5%~95% (non-condensing)
- Protection: IP30

## 1.1.4 Front Panel Ports and LEDs




## 1.1.5 Bottom Panel



## 1.2 SFP Module Installation

**Insert:**
Insert SFP Module into the SFP combo port.

**Remove:**
Pull the tab on the module, and then pull out it.

**Note:**
Delta has LCP-155 and LCP-1250 series SFP module. DVS switch can promise 100% compatible with Delta SFP module.

**Note:**
The actual link distance of a particular fiber optic link given the optical budget, the number of connectors and splices, and cabling quantity. Please measure and verify the actual link loss values once the link is established to identify any potential performance issues.

## 1.3 Package Checklist

- Delta DVS series PoE+ Managed Ethernet Switch
- Protective Caps for unused RJ45 ports and fiber ports
- Flat Screw (M3)
- RS232 to RJ45 console cable
- 6-pin terminal block
- Wall mounting kits and DIN-Rail kits
- User manual and software CD
- Instruction sheet

## 1.4 MTBF (Mean Time Between Failures)

More than 250,000 hours.

**MEMO**

# Chapter 2 User Interface Introduction

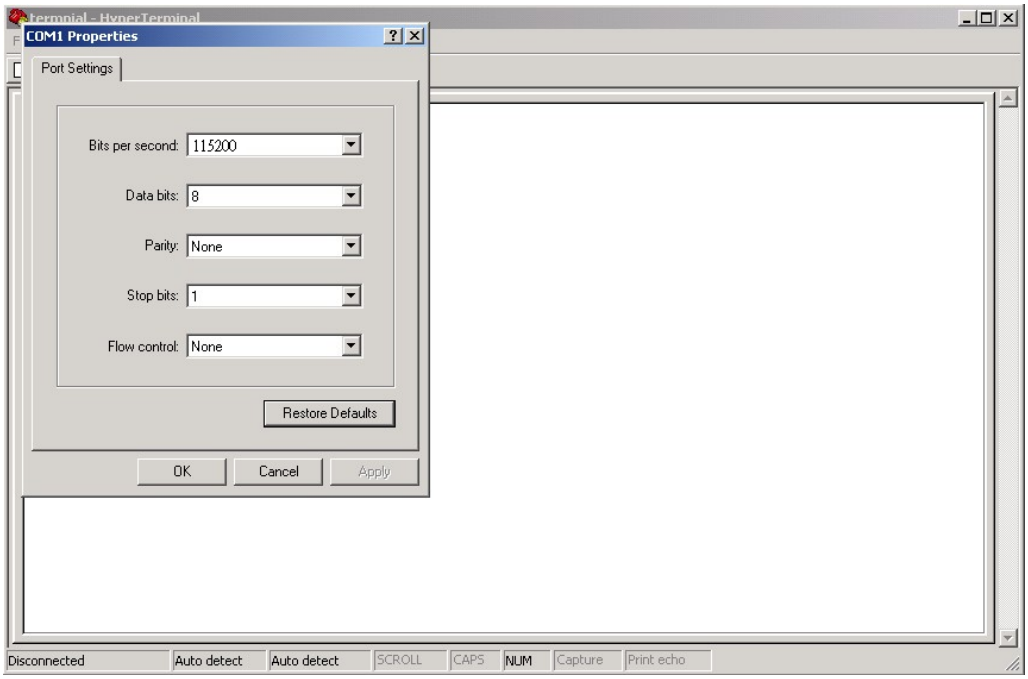
**Table of Contents**

## 2.1 RJ45 Console Configuration

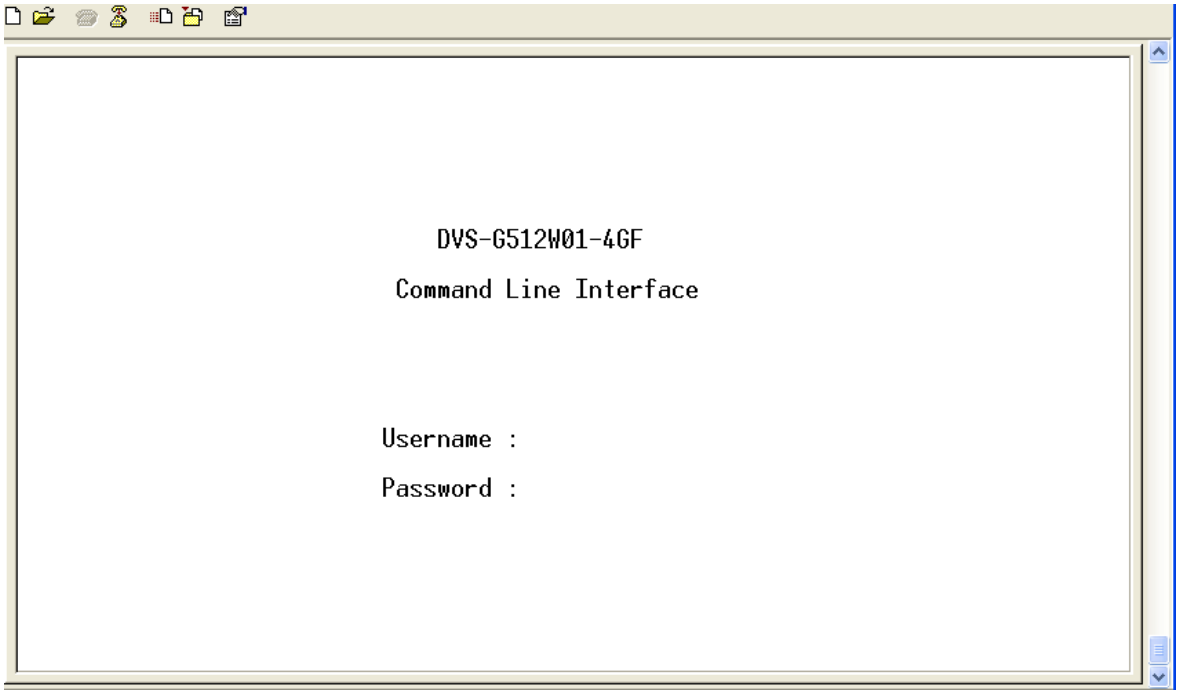
A Delta PoE managed switch supports configuration using the CLI interface, available on the RS232 port to RJ45 interface. You can use the terminal software to connect to a Delta PoE managed switch.

1. Open the terminal software, and select an appropriate COM port for **Console Connection**, **115200** for **Baud Rate**, **8** for **Data Bits**, **None** for **Parity**, and **1** for **Stop Bits, None** for **Flow Control**.

   **Note:**
   The Windows 7 system does not support Hyper Terminal. If you need it, you can download the terminal software to use it.




2. The user name and the password are the same as Web Browser. The default user name is “admin”, and the password is blank.



You can use “?” to list the commands.

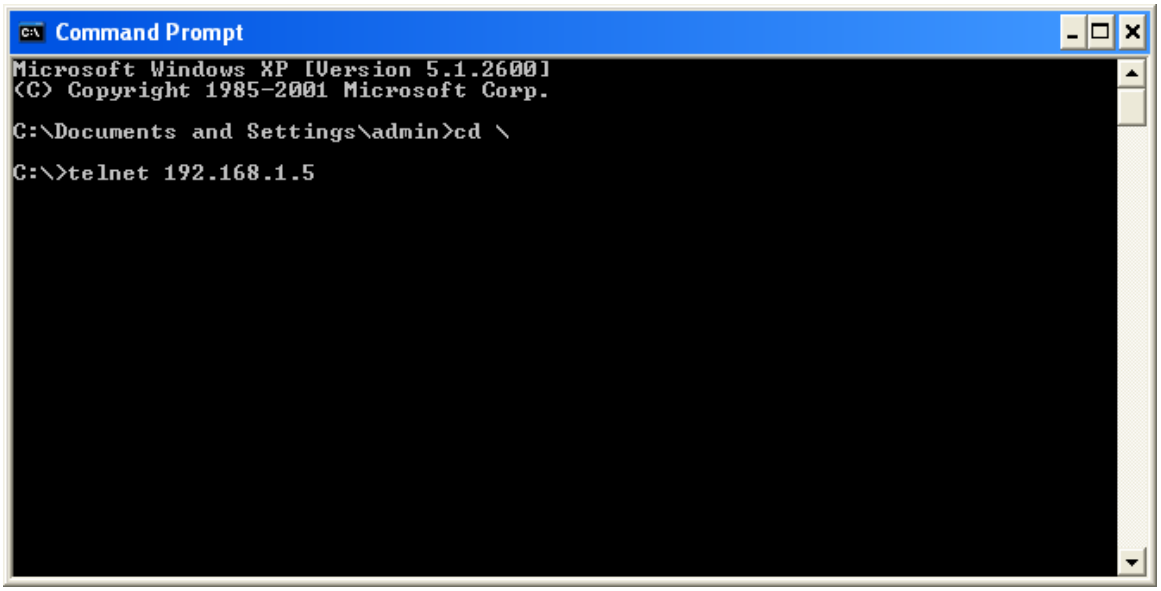
```
Welcome to DVS-G512W01-4GF Command Line Interface.
Type 'help' or '?' to get help.

>?
General Commands:
-----------------
Help/?: Get help on a group or a specific command
Up    : Move one command level up
Logout: Exit CLI

Command Groups:
---------------
System       : System settings and reset options
IP           : IP configuration and
Port         : Port management
MAC          : MAC address table
VLAN         : Virtual LAN
PVLAN        : Private VLAN
Security     : Security management
STP          : Spanning Tree Protocol
Aggr         : Link Aggregation
LACP         : Link Aggregation Control Protocol
LLDP         : Link Layer Discovery Protocol
PoE          : Power Over Ethernet
QoS          : Quality of Service
Mirror       : Port mirroring
```

```
Config       : Load/Save of configuration via TFTP
Firmware     : Download of firmware via TFTP
PTP          : IEEE1588 Precision Time Protocol
Loop Protect : Loop Protection
IPMC         : MLD/IGMP Snooping
Fault        : Fault Alarm Configuration
Event        : Event Selection
DHCPServer   : DHCP Server Configuration
Ring         : Ring Configuration
Chain        : Chain Configuration
Open-Ring    : Open-Ring Configuration
RCS          : Remote Control Security
Fastrecovery : Fast-Recovery Configuration
SFP          : SFP Monitor Configuration
DeviceBinding: Device Binding Configuration
MRP          : MRP Configuration
Modbus       : Modebus TCP Configuration
```

## 2.2 Telnet Console Configuration

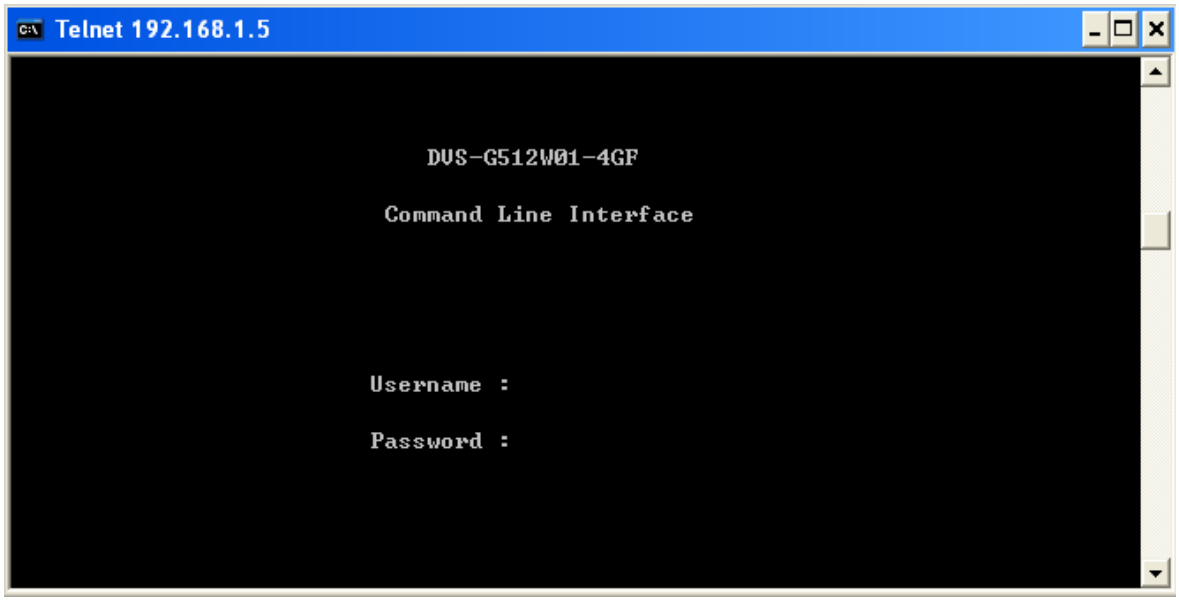
A Delta PoE managed switch supports the telnet server function; it can be globally enabled or disabled. The user can use all CLI commands over a telnet session. The maximum number of inbound telnet sessions allowed on the switch can be configured to 0-5. The inactivity timeout value for the incoming Telnet sessions for the switch can be configured to 1-160 minutes. The login authentication supports the local user method or the remote user method which is configured. When the login authentication is the remote user method, it supports RADIUS and TACACS+.

1. Open a Command Prompt window and input “telnet 192.168.1.X” to login to a Delta switch.




2. After entering a user name and a password, you can use the CLI command to control the switch.

**Note:**
1. The IP Address by default is 192.168.1.5
2. The default user name is “admin” and the password is blank.



## 2.3 Web Browser Configuration

A Delta PoE managed switch supports a friendly GUI for normal users to configure the switch. You can monitor the port status of a Delta PoE managed switch, and configure the settings of each function via the web interface.

1. Open a web browser and connect to the default IP address 192.168.1.5. Enter a user name and a password. (The default user name is “admin” and the password is blank.)

**Note:**

1. The default user name “admin” is in the lowercase not uppercase.
2. By default, IE5.0 or later version does not allow Java Applets to open sockets.
You need to explicitly modify the browser setting in order to enable Java Applets to use network ports.


2. You can use the menu tree in the left side frame to find the function you want to configure. And configure the detailed settings in the right side frame.


3. The port status and the LED status on the switch can be monitored in the top frame.

**MEMO**

# Chapter 3 Featured Functions

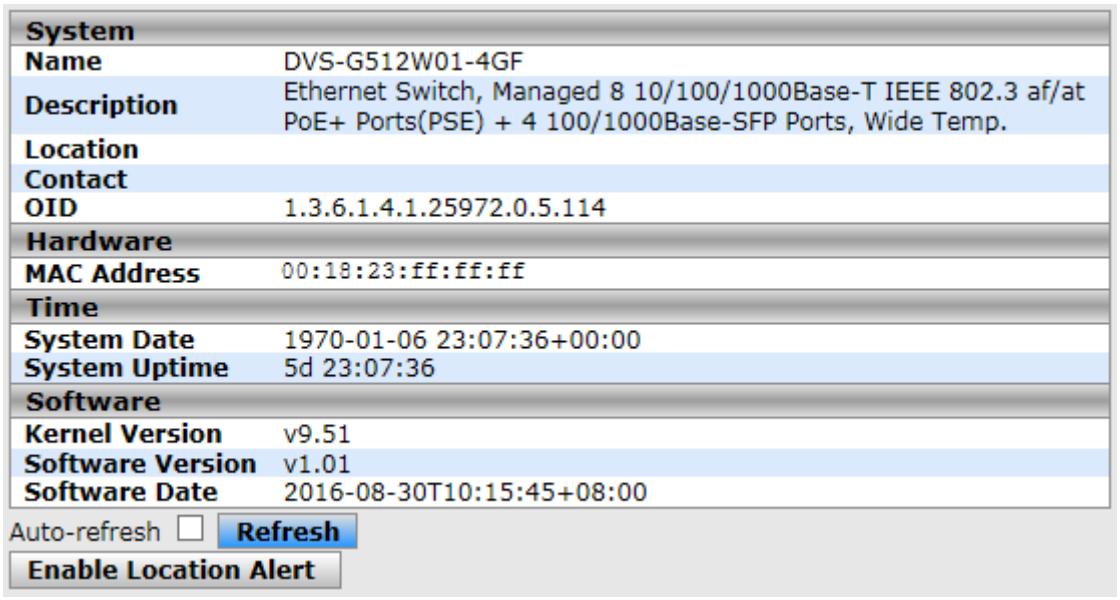
## Table of Contents

# 3.1 Basic Setting

The basic setting group includes the most common settings, and an administrator can maintain the control of the Delta switch in this group.

## 3.1.1 System Information

System Information includes the basic switch status items and the version .It also displayed in the banner of the GUI. These informations can help the administrator identify the switch in the network.




**System**

| Description | Factory default |
|---|---|
| **Name** | |
| The system name of the switch. | Fixed |
| **Description** | |
| The device description of the switch. | Fixed |
| **Location** | |
| The system location of the switch. | Fixed |
| **Contact** | |
| The system contact of the switch. | Fixed |
| **OID** | |
| The based object ID for the Management Information Base (MIB) of the switch. | Fixed |

**Hardware**

| Description | Factory default |
|---|---|
| **MAC Address** | |
| The MAC address of the switch. | Fixed |

**Time**

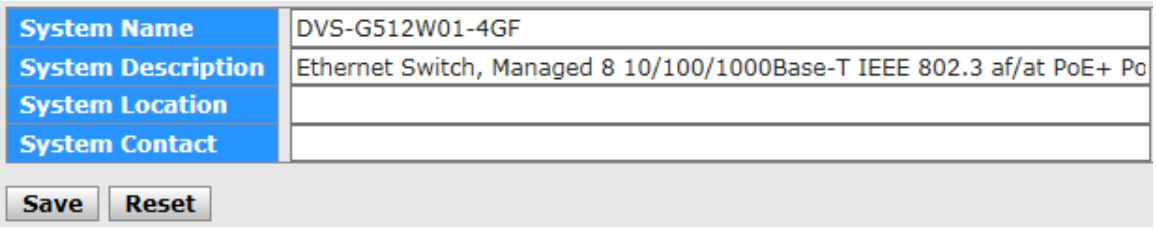
| Description | Factory default |
|---|---|
| **System Date** | |
| The current date and time. | Fixed |
| **System Up Time** | |
| The time of hours, minutes, and seconds since the switch was last started. | Fixed |

**Software**

| Description | Factory default |
|---|---|
| **Kernel Version** | |
| The kernel version of the switch. | Model Name |
| **Software Version** | |
| The software version of the switch. | Boot Version |
| **Software Date** | |
| The software version released date of the switch. | Software Version |

### 3.1.2 Basic Setting

The Basic Setting will help you customerizing the system information.These informations will display in the System Information when you change it.




**Basic Setting**

| Description | Factory default |
|---|---|
| **System Name** | |
| The system name of the switch. | Product Name |
| **System Description** | |
| The device description of the switch. | Product Description |
| **System Location** | |
| The system location of the switch. | None |
| **System Contact** | |
| The system contact of the switch. | None |

### 3.1.3 Admin Password

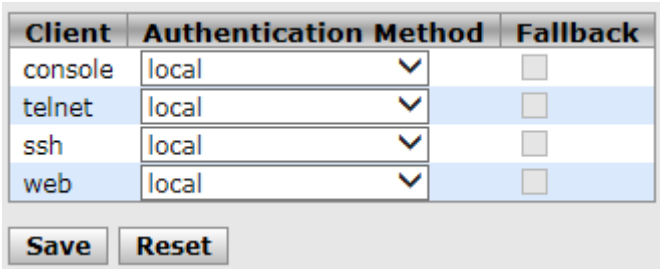
Only the admin of the Delta switch can modify system username and password.


**Admin Password**

| Description | Factory default |
|---|---|
| **Username** | |
| The system username of the switch. | admin |
| **Old Password** | |
| The current password of the switch.The default password is blank. | None |
| **New Password** | |
| Enter the desired new password.Keep it blank if you don't want to any password. Passwords are 1–20 alphanumeric characters in length and are case sensitive. | None |
| Confirm New Password | |
| Enter the same password that you entered in the Password field. | None |

### 3.1.4 Auth Method

A Delta PoE switch provides three authentication methods: Local, RADIUS, and TACACS+. If there is no RADIUS or TACACS+ server in your network environment, you can use the local authentication method for the login authentication




3

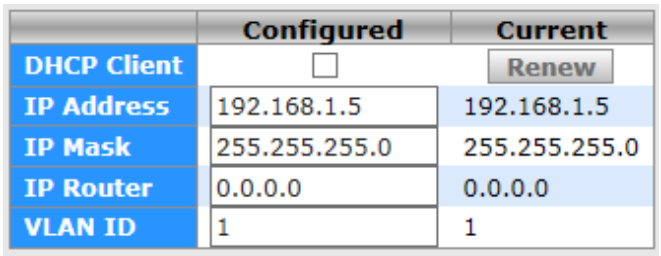
**Auth Method**

| Description | Factory default |
|---|---|
| **Client** | |
| The management client for which the configuration below applies. | Fixed |
| **Authentication Method** | |
| Specify the login authentication method:<br>• **None:** Authentication is disabled and login is not possible.<br>• **Local:** A locally stored user ID and a password are used for the authentication. This is the default setting. You need to set up a user account on the Local User Management page.<br>• **RADIUS:** The user ID and the password are authenticated through a RADIUS server.<br>• **TACACS+:** The user ID and the password are authenticated through a TACACS+ server. | Local |
| **Fallback** | |
| If there is not any confiugured authentication server consist, the local user database is used for authentication.<br>**Note:**<br>This is only possible if the Authentication Method is set to a value other than 'none' or 'local'. | None |

### 3.1.5 IP Setting

You can configure a static IP address, a subnet mask and a default gateway for the switch. Or you can enable DHCP mode for receiving a dynamic IP address, a subnet mask and a default gateway.

**Note:**
The default Current Network Configuration Protocol is None. And the default IP address is **192.168.1.5**.

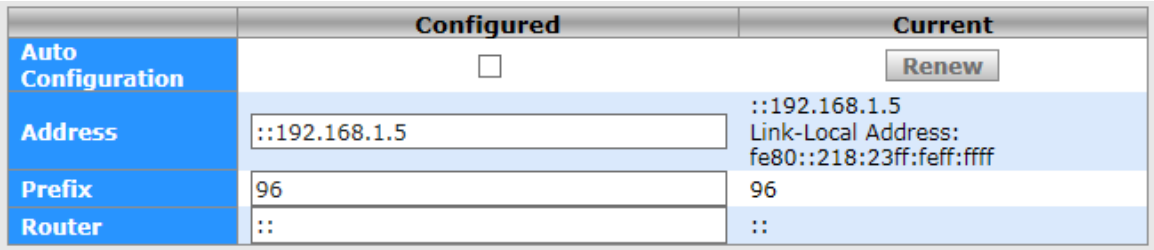


**IP Setting**

| Description | Factory default |
|---|---|
| **DHCP Client** | |
| The IP information of the switch is assigned by a Dynamic Host Configuration Protocol (DHCP) server on the network. | Unchecked |
| **IP Address** | |
| Input the IP address of the IPv4 network interface.<br>**Note:**<br>After you change the IP address and clicking Apply, we suggest you to login again, and making sure the URL is the latest IP address. | 192.168.1.5 |
| **IP Mask** | |
| Input the default gateway of the IPv4 network interface. | 255.255.255.0 |
| **IP Router** | |
| Input the default gateway of the IPv4 network interface. | 0.0.0.0 |
| **VLAN ID** | |
| Input the management VLAN ID in the range from 1 to 4094. | 1 |

## 3.1.6 IPv6 Network Configuration

If you need to configure a global IPv6 address, please follow the standard format: “IPv6 Prefix/Prefix Length”. Example: “1001:2002:3003::7007:8008/64”



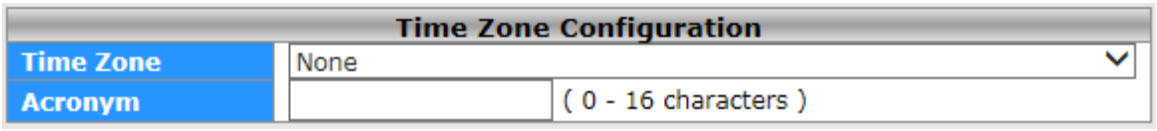

**IPv6 Network Configuration**

| Description | Factory default |
|---|---|
| **Auto Configuration** | |
| If system cannot obtain the stateless address in time, the configured IPv6 settings will be used. The router may delay responding to a router solicitation for a few seconds, the total time needed to complete auto-configuration can be significantly longer. | Disable |
| **Address** | |
| Enter the IPv6 address followed by a slash and then the prefix length of the network interface. | IPv6 address |
| **Prefix** | |
| Input the IPv6 Prefix of this switch. The allowed range is 1 to 128. | 96 |
| **Router** | |
| Input the IPv6 address of the IPv6 gateway. | None |

## 3.1.7 Daylight Saving Time

The Delta switch support Daylight Saving Time.It can used to automatically set the Delta switch’s forward according to national standards.

- **Time Zone Configuration**

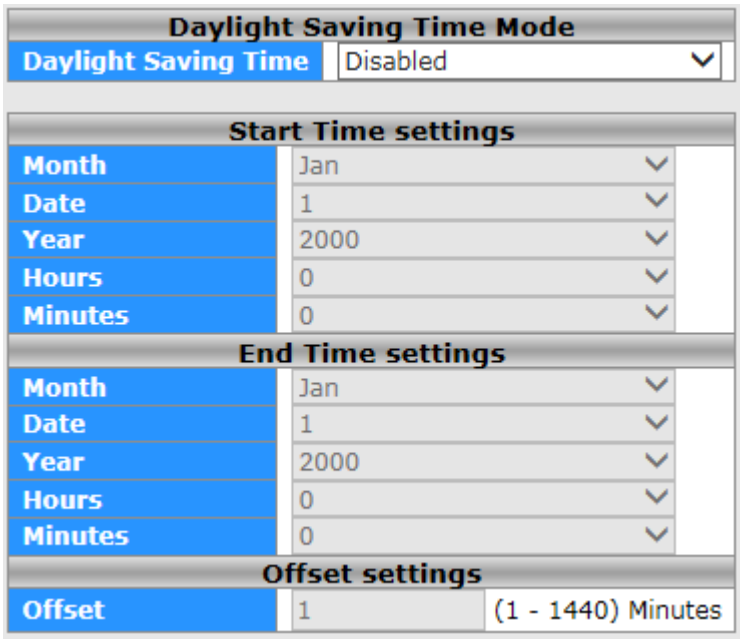



**Time Zone Configuration**

| Description | Factory default |
|---|---|
| **Time Zone** | |
| Lists various Time Zones world wide. Select appropriate Time Zone from the drop down and click Save to set. | None |
| **Acronym** | |
| User can set the acronym of the time zone. This is a User configurable acronym to identify the time zone. ( Range : Up to 16 alpha-numeric characters and can contain '-', '_' or '.') | None |



- **Daylight Saving Time Mode**




**Daylight Saving Time Mode**

| Description | Factory default |
|---|---|
| **Daylight Saving Time Mode** | |
| Specify the clock forward or backward according to the configurations set below for a defined Daylight Saving Time duration.<br>• **Disable**: Disable the Daylight Saving Time configuration.<br>• **Recurring**: Configure the Daylight Saving Time duration to repeat the configuration every year<br>• **Non-Recurring: C**onfigure the Daylight Saving Time duration for single time configuration. | Disable |
| **Start Time Settings** | |
| Enter the daylight saving time (DST) start time.<br>• **Week**: Select the starting week number.<br>• **Day**: Select the starting day.<br>• **Month**: Select the starting month.<br>• **Hours**: Select the starting hour.<br>• **Minutes**: Select the starting minute. | Fixed |

| Description | Factory default |
|---|---|
| **Note:**<br>If you select the daylight saving mode as “Disable”, the configuration will also be disabled. | |
| **End Time settings** | |
| Enter the daylight saving time (DST) end time.<br>• **Week**: Select the starting week number.<br>• **Day**: Select the starting day.<br>• **Month**: Select the starting month.<br>• **Hours**: Select the starting hour.<br>• **Minutes**: Select the starting minute.<br>**Note:**<br>If you select the daylight saving mode as “Disable”, the configuration will also be disabled. | fixed |
| **Offset settings** | |
| Enter the daylight saving time (DST) end time.<br>• **Week**: Select the starting week number.<br>• **Day**: Select the starting day.<br>• **Month**: Select the starting month.<br>• **Hours**: Select the starting hour.<br>• **Minutes**: Select the starting minute.<br>**Note:**<br>If you select the daylight saving mode as “Disable”, the configurations will also be disabled. | fixed |

### 3.1.8 HTTPS

Hypertext Transfer Protocol Secure (HTTPS) is a protocol for secure communication. It enables the transmission of HTTP over an encrypted Secure Sockets Layer (SSL) or Transport Layer Security (TLS) connection. So HTTPS can help protect the communication between a computer and a switch from eavesdroppers and man-in-the-middle (MITM) attacks.
If you want to configure the switch to access an HTTPS connection from a computer, the switch needs a public key certificate. You can configure the switch to generate a key or download it to the switch.


**HTTPS Configuration**

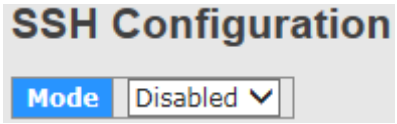
| Description | Factory default |
|---|---|
| **Mode** | |
| Specify whether the web management interface can be accessed from a web browser over an HTTPS connection.<br>• **Disable**: The web management interface can not be accessed over an HTTPS connection. You need to use a Telnet, SSH, or console connection to access the switch.<br>• **Enable**: The web management interface can be accessed over an HTTPS connection.<br>**Notice:**<br>If you want to enable the HTTPS Admin mode, you need to use Generate Key, then apply Generate Certificate, please refer to **Certificate Management**. | Disable |

After you enable the HTTPS connection, you can type **https://Delta switch’s IP address** into the web browser to establish an HTTPS connection.

For example, if a switch’s IP address is 192.168.1.5, the complete address is https://192.168.1.5.

### 3.1.9 SSH

You can configure an SSH configuration on this page.




**SSH Configuration**

| Description | Factory default |
|---|---|
| **SSH Admin Mode** | |
| Specify the status of SSH.<br>• **Disable**: SSH is disabled. This is the default setting.<br>• **Enable**: SSH is enabled. | Disable |

### 3.1.10 LLDP

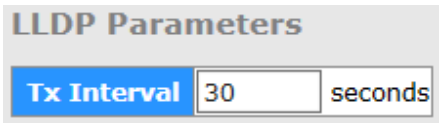
LLDP (Link Layer Discover Protocol) provides a method for switches, routers and access points to advertise their identification, configuration and capabilities to the neighboring devices that store the data in a MIB, and to learn information about the neighboring devices.
LLDP-MED (Link Layer Discovery Protocol for Media Endpoint Devices) is an extension of LLDP in that it operates between endpoint devices such as IP phones or switches.
LLDP-Media Endpoint Discovery (LLDP-MED) is an enhancement of LLDP with the following features:

- **Auto Discovery:** Autodiscovery of LAN policies (such as VLAN, Layer 2 priority, and DiffServ settings) and capability to enable a plug and play networking
- **Device Location:** Device location discovery for the creation of location databases
- **Power Management:** Extended and automated power management of Power over Ethernet (PoE) endpoints
- **Inventory Management:** Inventory management, which lets network administrators track network devices and determine their characteristics such as the manufacturer, the software and hardware versions, and the serial and asset numbers

#### 3.1.10.1 Configuration

This page allows the user to inspect and configure the current LLDP port settings.

- **LLDP Parameter**

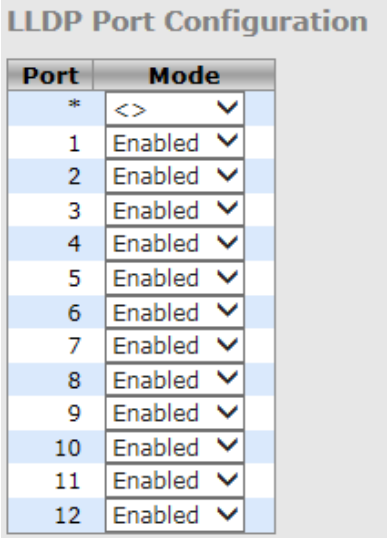



**LLDP Parameter**

| Description | Factory default |
|---|---|
| **Tx Interval** | |
| Entering the transmit interval of LLDP message in seconds. The values are 5 to 32678. | Disable |

- **LLDP Port Configuration**

The default of the LLDP status is enabling. If you want to configure other settings, please refer to the following table.

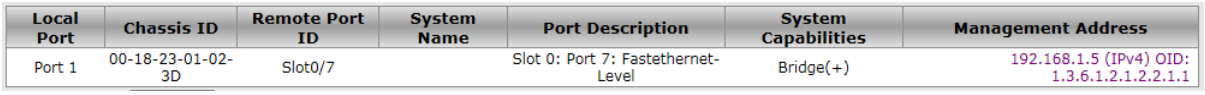



**LLDP Port Configuration**

| Description | Factory default |
|---|---|
| **Port** | |
| This field displays the interface number. | *interface number* |
| **Mode** | |
| Specify the status of LLDP on the switch:<br>• **Enabled:** LLDP is enabled. You can configure LLDP, and the settings take effect after you have applied them.<br>• **Disabled:** LLDP is disabled. You can still configure LLDP, but the settings do not take effect after you have applied them. | Enabled |

### 3.1.10.2 LLDP Neighbours

You can view the LLDP neighbor statistics for an individual interface or all interfaces.




**LLDP Neighbour Information**

| Item | Description |
|---|---|
| **Local Port** | The interface on the switch that receives the LLDP information from the remote neighbor. |
| **Chassis ID** | The chassis ID of the remote neighbor. |
| **Remote Port ID** | The Remote Port ID is the identification of the neighbor port. |
| **System Name** | System Name is the name advertised by the neighbor unit. |
| **Port Description** | Port Description is the port description advertised by the neighbor unit. |
| **System Capabilities** | The fields can display the following information: Router, Bridge, Telephone, DOCSIS Cable Device, WLAN Access Point, Repeater, Station Only, Reserved or Other.<br>Notice:<br>When a capability is enabled, the capability is followed by (+). If the capability is disabled, the capability is followed by (-). |
| **Management Address** | Management Address is the neighbor unit's address that is used for higher layer entities to assist the discovery by the network management. This could for instance hold the neighbor's IP address. |

### 3.1.10.3 Port Statistics

You can view the LLDP neighbor statistics for an individual interface or all interfaces.

- **LLDP Global Counters:** These statistics are total quantities of LLDP traffic for the switch.

| Global Counters | |
|---|---|
| Neighbour entries were last changed | 1970-01-13 05:22:03+00:00 (165901 secs. ago) |
| Total Neighbours Entries Added | 11 |
| Total Neighbours Entries Deleted | 10 |
| Total Neighbours Entries Dropped | 0 |
| Total Neighbours Entries Aged Out | 2 |

**LLDP Global Counters**

| Item | Description |
|---|---|
| **Neighbour entries were last changed** | Shows the time when the last entry was deleted or added. |
| **Total Neighbours Entries Added** | Shows the number of new entries added since switch reboot |
| **Total Neighbours Entries Deleted** | Shows the number of new entries deleted since switch reboot |
| **Total Neighbours Entries Dropped** | Shows the number of LLDP frames dropped due to full entry table |
| **Total Neighbours Entries Aged Out** | Shows the number of entries deleted due to expired time-to-live |

- **LLDP Statistics Local Counters:** The statistics of the fields are for each individual interface.

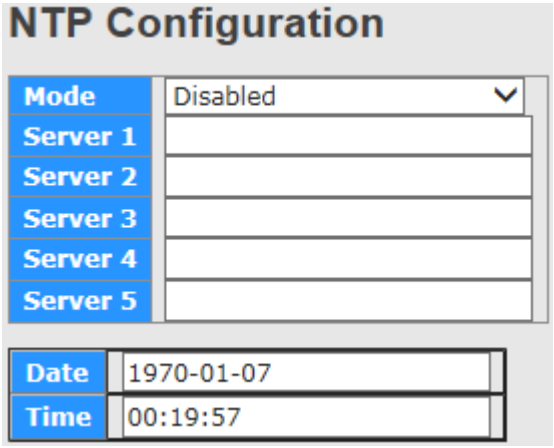
| Local Port | Tx Frames | Rx Frames | Rx Errors | Frames Discarded | TLVs Discarded | TLVs Unrecognized | Org. Discarded | Age-Outs |
|---|---|---|---|---|---|---|---|---|
| 1 | 8859 | 5992 | 0 | 0 | 0 | 0 | 5992 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 22842 | 3086 | 0 | 0 | 0 | 0 | 3086 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 512 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 14982 | 68 | 0 | 0 | 0 | 0 | 68 | 2 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

**LLDP Statistics Local Counters**

| Item | Description |
|---|---|
| **Local Port** | The interface on the switch that receives the LLDP information from the remote neighbor. |
| **Tx Frames** | The number of LLDP frames transmitted on the port. |
| **Rx Frames** | The number of LLDP frames received on the port |
| **Rx Errors** | The number of received LLDP frames containing errors |
| **Framed Discarded** | If a port receives an LLDP frame, and the switch's internal table is full, the LLDP frame will be counted and discarded. |
| **TLVs Discarded** | Each LLDP frame containing multiple pieces of information, known as TLVs (Type Length Value). If a TLV is malformed, it will be counted and discarded. |
| **TLVs Unrecognized** | The number of well-formed TLVs, but with an unknown type value. |
| **Org. Discarded** | The number of organizationally TLVs received |
| **Ages Out** | If no new LLDP frame is received during the age-out time, the LLDP information will be removed, and the value of the age-out counter will be incremented. |

### 3.1.11 NTP

NTP Configuration lets a user configure the time of the switch which can be gotten from the NTP server. And it also can be configured manually.

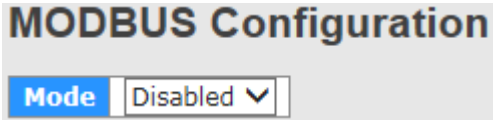



**NTP Configuration**

| Description | Factory default |
|---|---|
| **Mode** | |
| Specify whether the switch works as a SNTP client or a SNTP server.<br>• **Disable**: The switch does not operat in NTP mode.<br>• **Client**: The switch works as an SNTP client mode.<br>• **Server**: The switch works as an SNTP Server mode. | Disable |
| **Server** | |
| Specify a type of SNTP server IP address. | None |
| **Date** | |
| The date parameter format is DD/MM/YYYY.<br>When an SNTP client is disabled, you can manually set the date. When an SNTP client is enabled, the field is grayed out. | YYYY-MM-DD |
| **Time** | |
| The time parameter format is HH:MM:SS. When an SNTP client is disabled, you can manually set the time. When an SNTP client is enabled, the field is grayed out. | HH:MM:SS |

### 3.1.12 MODBUS TCP

The module status of MODBUSMODBUS TCP is used to enable/disable the MODBUSMODBUS TCP feature. If you need to set parameters, please refer to Appendix B MODBUSMODBUS TCP Map.

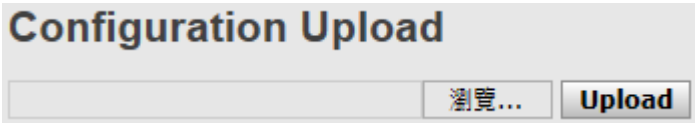



### 3.1.13 Backup

The Delta switch supports uploading the configuration to a local host.

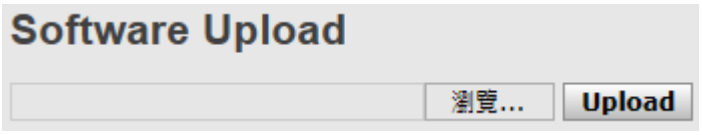
### 3.1.14 Restore

The Delta switch supports downloading the configuration from a local host.




### 3.1.15 Upgrade Firmware

The Delta switch supports uploading the firmware from a local host to the Delta switch.

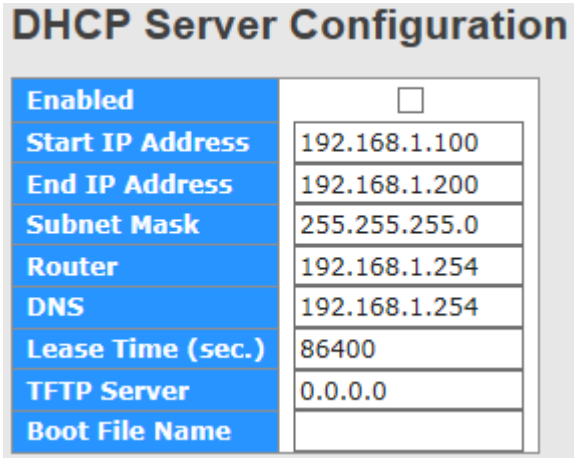



## 3.2 DHCP Server / Relay

The Delta switch can function as a DHCP server, DHCP relay and DHCP L2 relay. If there is no DHCP server in your network, then you can enable a DHCP server function on the Delta switch. If there is a DHCP server in your network, then you can configure the Delta switch as a DHCP relay. If there is already a DHCP server and a DHCP relay in your network, or there are L2 devices between DHCP clients and relay agents, then you can configure the Delta switch as a DHCP L2 relay in this network.

### 3.2.1 Settings

If the DHCP server is enabled on the switch, it can assign an IP address which is in the same network as the switch to the client.




**DHCP Server Configuration**

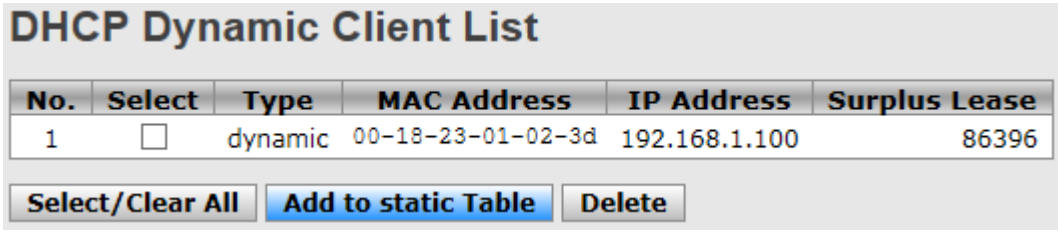
| Description | Factory default |
|---|---|
| **Enabled** | |
| Specify the status of the DHCP server on the switch:<br>• **Unchecked**: The DHCP server is disabled.<br>• **Checked**: The DHCP server is enabled. | Unchecked |
| **Start IP Address** | |
| Enter the start IP address of the DHCP server pool. | 192.168.1.100 |

| Description | Factory default |
|---|---|
| **End IP Address** | |
| Enter the end IP address of the DHCP server pool. | 192.168.1.200 |
| **Subnet mask** | |
| Enter the IP subnet mask for the DHCP pool. | 255.255.255.0 |
| **Router** | |
| Specify the default gateway IP address. The information will be included in the DHCP offer packet. | 192.168.1.254 |
| **DNS** | |
| Specify the DNS server IP address. The information will be included in the DHCP offer packet. | 192.168.1.254 |
| **Lease Time** | |
| Enter the duration by entering the seconds. | 86400 |
| **TFTP Server** | |
| Enter the TFTP server address. | 0.0.0.0 |
| **Boot File Name** | |
| Specify the boot file name. | None |



### 3.2.2 DHCP Dynamic Client List

If the DHCP server function is activated, you can see the DHCP client's information which is get the IP address from the DHCP server on this page.



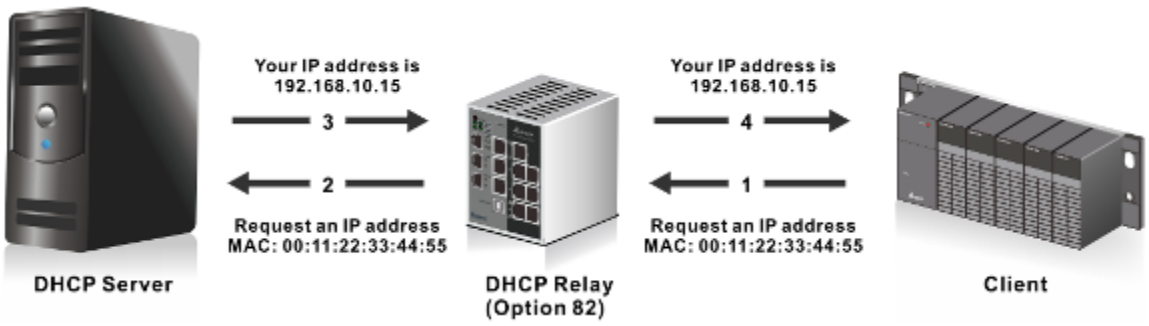

### 3.2.3 DHCP Client List

A Delta PoE managed switch supports the specific IP address which is in the assigned dynamic IP range to the specific port.


If you select a dynamic client from the DHCP Dynamic Client List to add to static Table, then it will appear in the DHCP Client List.

### 3.2.4 DHCP Relay Agent

A DHCP Relay can make broadcast messages to be sent over routers. And a DHCP relay can receive a DHCP broadcast request packet and forward it to a specified server. The operating theory is shown in the figure below.

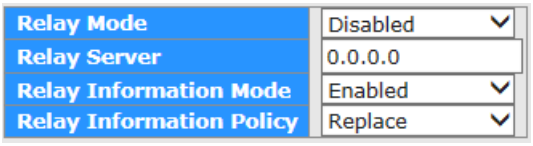



**Notice:**
When a DHCP request packet comes, the DHCP relay receives it and then sends it to all VLANs. But according to RFC 2131, when a unicast DHCP request packet renews, it will be sent to a DHCP server directly without passing a DHCP relay, so it is recommended to make sure that the DHCP client can ping the server after getting an IP address.

3

### 3.2.4.1 Relay

The DHCP relay sends a unicast DHCP packet to the specified server(s). You can enable or disable a DHCP relay function, and configure the parameters on the switch.

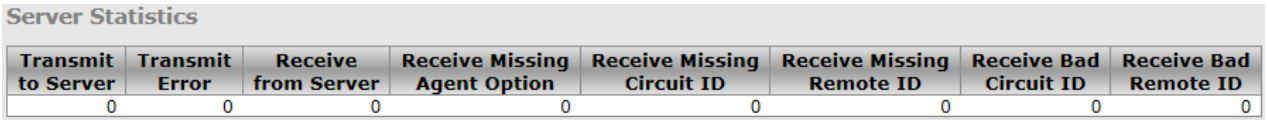



**DHCP Relay Configuration**

| Description | Factory default |
|---|---|
| **Relay Mode** | |
| Specify the status of the DHCP relay on the switch:<br>• **Disable**: The DHCP relay is disabled. This is the default setting.<br>• **Enable**: The DHCP relay is enabled. | Disable |
| **Relay Server** | |
| Specify the DHCP relay server IP address. | 0.0.0.0 |
| **Relay Information Mode** | |
| Specify the DHCP relay information mode option operation.<br>• **Disable**: Enable DHCP relay information mode operation.<br>• **Enable**: Disable DHCP relay information mode operation. | Enabled |
| **Relay Information Policy** | |
| Specify the DHCP relay information option policy.<br>• **Replace**: Replace the original relay information when a DHCP message that already contains it is received.<br>• **Keep**: Keep the original relay information when a DHCP message that already contains it is received.<br>• **Drop**: Drop the package when a DHCP message that already contains relay information is received. | Replace |

### 3.2.4.2 Relay Statistics

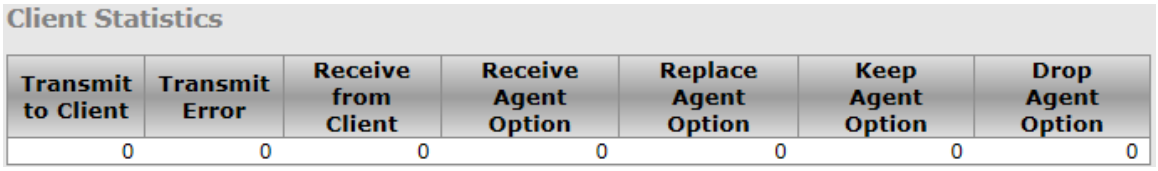
- **Server Statistics**



**Server Statistics**

| Item | Description |
|---|---|
| **Transmit to Server** | The number of packets that are relayed from client to server. |
| **Transmit Error** | The number of packets that resulted in errors while being sent to clients. |
| **Receive from Server** | The number of packets received from server. |
| **Receive Missing Agent Option** | The number of packets received without agent information options. |
| **Receive Missing Circuit ID** | The number of packets received with the Circuit ID option missing. |
| **Receive Missing Remote ID** | The number of packets received with the Remote ID option missing. |
| **Receive Bad Circuit ID** | The number of packets whose Circuit ID option did not match known circuit ID. |
| **Receive Bad Remote ID** | The number of packets whose Remote ID option did not match known Remote ID. |

- **Client Statistics**




**Client Statistics**

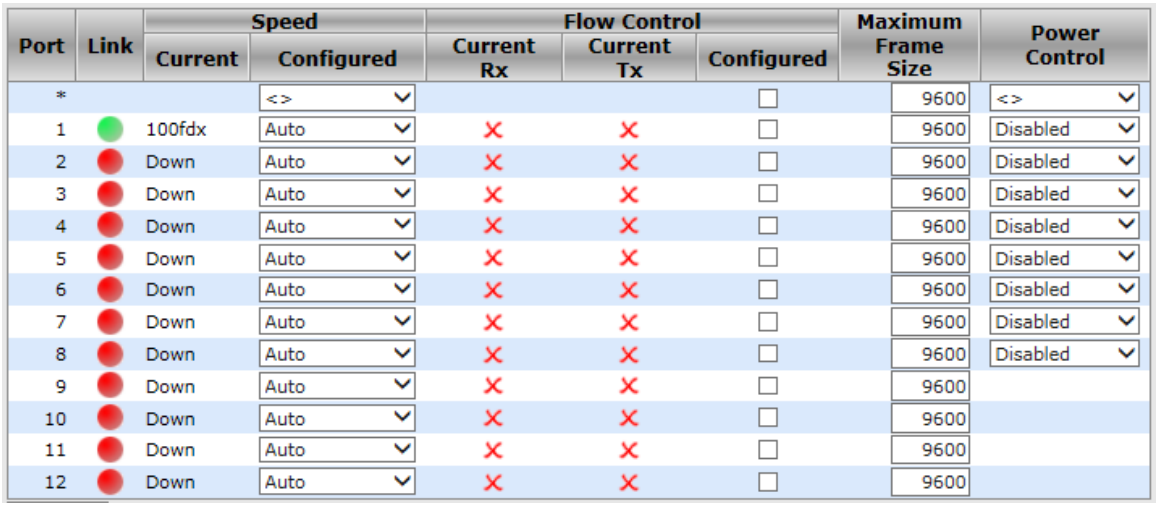
| Item | Description |
|---|---|
| **Transmit to Client** | The number of relayed packets from server to client. |
| **Transmit Error** | The number of packets that resulted in error while being sent to servers. |
| **Receive from Client** | The number of received packets from server. |
| **Receive Agent Option** | The number of received packets with relay agent information option. |
| **Replace Agent Option** | The number of packets which were replaced with relay agent information option. |
| **Keep Agent Option** | The number of packets whose relay agent information was retained. |
| **Drop Agent Option** | The number of packets that were dropped which were received with relay agent information. |

## 3.3 Port Setting

You can configure the basic port settings and LAG settings of a Delta switch in the Port Settings group.

### 3.3.1 Port Control

You can configure and monitor the port status on this page.



| Port | Link | Speed | | Flow Control | | | Maximum Frame Size | Power Control |
|---|---|---|---|---|---|---|---|---|
| | | Current | Configured | Current Rx | Current Tx | Configured | | |
| * | | | <> | | | ☐ | 9600 | <> |
| 1 | | 100fdx | Auto | ✗ | ✗ | ☐ | 9600 | Disabled |
| 2 | | Down | Auto | ✗ | ✗ | ☐ | 9600 | Disabled |
| 3 | | Down | Auto | ✗ | ✗ | ☐ | 9600 | Disabled |
| 4 | | Down | Auto | ✗ | ✗ | ☐ | 9600 | Disabled |
| 5 | | Down | Auto | ✗ | ✗ | ☐ | 9600 | Disabled |
| 6 | | Down | Auto | ✗ | ✗ | ☐ | 9600 | Disabled |
| 7 | | Down | Auto | ✗ | ✗ | ☐ | 9600 | Disabled |
| 8 | | Down | Auto | ✗ | ✗ | ☐ | 9600 | Disabled |
| 9 | | Down | Auto | ✗ | ✗ | ☐ | 9600 | |
| 10 | | Down | Auto | ✗ | ✗ | ☐ | 9600 | |
| 11 | | Down | Auto | ✗ | ✗ | ☐ | 9600 | |
| 12 | | Down | Auto | ✗ | ✗ | ☐ | 9600 | |

**Port Control**

| Description | Factory default |
|---|---|
| **Port** | |
| This field displays the interface number. | *interface number* |
| **Link** | |
| This field displays the connection of the interface graphically.<br>• **Green**: There is a network device connecting to the interface.<br>• **Red**: No network device is connecting to the interface. | Link down |
| **Speed** | |
| This field displays the actual port speed capability and configured the port capability.<br>• **Current**: This field displays the actual port speed and the duplex mode.<br>• **Configured**: Specify the speed capability of each interface.<br>**Note:**<br>1. When you configure the Port "*" to Auto, 100 Mbps HDX, 100 Mbps FDX and 1G Mbps FDX, it meaning configure to all interface the same speed.<br>2. If you select the “Disable”, it will disable the switch port operation. | Current: None<br>Configured: Auto |
| **Flow Control** | |
| This field displays whether the flow control is enabled for the port:<br>• **Current Rx**: Indicates whether pause frames on the port are obeyed.<br>• **Current Tx**: Indicates whether pause frames on the port are transmitted.<br>• **Configured**: Specify the flow control is enabled or not. | Unchecked |
| **Maximum Frame** | |
| The field displays whether the maximum frame is configured for the port. The allowed range is 1518 bytes to 9600 bytes. | 9600 |
| **Power Control** | |
| Specify the speed capability of each interface:<br>• **Disabled**: All power savings mechanisms disabled.<br>• **ActiPHY**: Link down power savings enabled.<br>• **Perfect Reach**: Link up power savings enabled.<br>• **Enabled**: Both link up and link down power saving enabled. | None |

### 3.3.2 Port Alias

You can create an alias on a physical interface. It will help you to manage the network topology more easily.

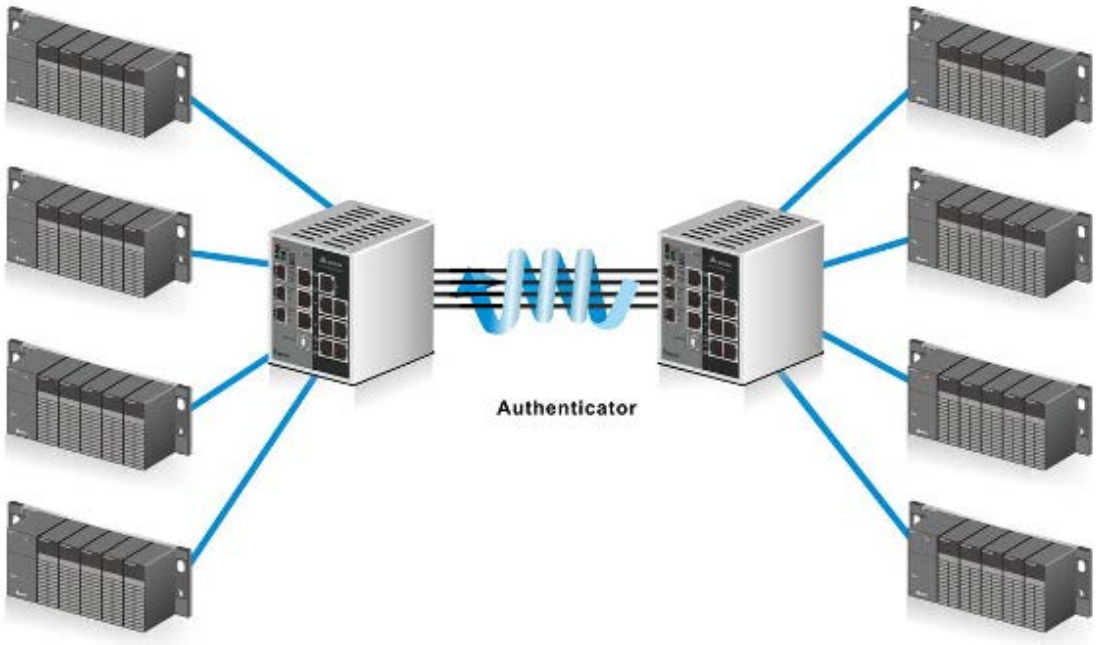
| Port | Port Alias |
|---|---|
| 1 | |
| 2 | |
| 3 | |
| 4 | |
| 5 | |
| 6 | |
| 7 | |
| 8 | |
| 9 | |
| 10 | |
| 11 | |
| 12 | |

**Port Control**

| Description | Factory default |
|---|---|
| **Port** | |
| This field displays the interface number. | *interface number* |
| **Port Alias** | |
| Specify an alias for the port to help administrator differentiate between difference ports. | None |

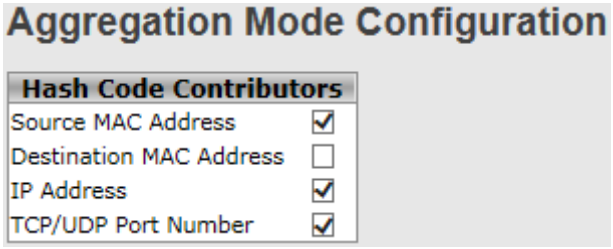
### 3.3.3 Port Trunk

Port Trunking can help you aggregate more links to form one link group.If there are 4 ports in a trunk group, and one port fails, then the other seven ports will provide backups and share the traffic automatically. If all ports on these two switches are configured as 100BaseTX and full duplex, then the potential bandwidth of the connection can be 400Mbps.The function theory is shown in the figure below.



### 3.3.3.1 Configuration

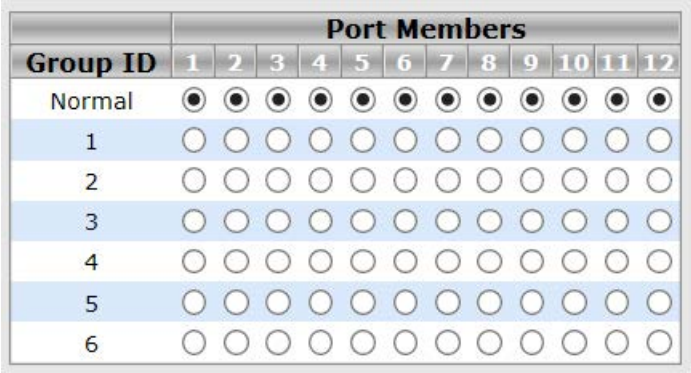
- **Aggregation Mode Configuration**




**Aggregation Mode Configuration**

| Description | Factory default |
|---|---|
| **Source MAC Address** | |
| Specify the Source MAC Address to calculate the source port for the frame.<br>• **Checked**: Enabled the use of the Source MAC address.<br>• **Unchecked**: Disabled the use of the Source MAC address. | Checked |
| **Destination MAC Address** | |
| Specify the Source MAC Address to calculate the destination port for the frame.<br>• **Checked**: Enabled the use of the Destination MAC address.<br>• **Unchecked**: Disabled the use of the Destination MAC address. | Unchecked |
| **IP Address** | |
| Specify the IP Address to calculate the destination port for the frame.<br>• **Checked**: Enabled the use of the IP address.<br>• **Unchecked**: Disabled the use of the IP address. | Checked |
| **TCP/UDP Port Number** | |
| Specify the TCP/UDP port number to calculate the destination port for the frame.<br>• **Checked**: Enabled the use of the TCP/UDP port number.<br>• **Unchecked**: Disabled the use of the TCP/UDP port number. | Checked |

- **Aggregation Group Configuration**

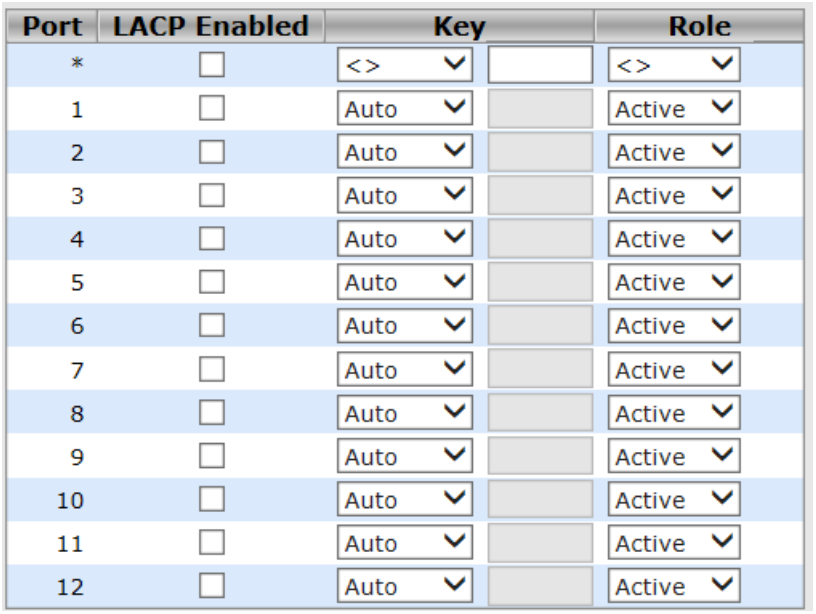



**Aggregation Group Configuration**

| Description | Factory default |
|---|---|
| **Group ID** | |
| This field displays the group ID number. The Group ID "Normal" indicates there is no aggregation. Only one group ID is valid per port. | *Group number* |
| **Port Members** | |
| Select one or more interfaces by clicking the square. | Normal |

### 3.3.3.2 LACP Configuration

Link aggregation groups (LAGs) let you combine multiple full-duplex Ethernet links into a single logical link. LAG increases fault tolerance and provide traffic sharing. You can assign LAG VLAN membership after you have added interfaces as members of a LAG.
After you have added interfaces to a LAG and enabled the LAG, Link Aggregation Control Protocol (LACP) can automatically configure a port channel link between the switch and another device.




**LACP Port Configuration**

| Description | Factory default |
|---|---|
| **Port** | |
| This field displays the interface number. | *Interface number* |
| **LACP Enabled** | |
| Specify whether the static mode of the LAG ID is enabled. | Unchecked |
| **Key** | |
| Specify whether the key of the LACP mode.<br>• **Auto**: Enabled the key as appropriate by the physical link speed, 10Mb = 1, 100Mb = 2, 1Gb = 3<br>• Specific: User-defined value can be entered. | Auto |
| **Role** | |
| Specify the role of the LACP activity status.<br>• **Activ**e: It will transmit LACP packets in per second<br>• Passive: It will wait for a LACP packet from a partner (speak if spoken to). | Active |

### 3.3.3.3 System Status

The System Status is displayed on this page

**System Status**

| Item | Description |
|---|---|
| **Aggr ID** | The Aggregation ID associated with this aggregation instance. For LLAG the id is shown as 'isid:aggr-id' and for GLAGs as 'aggr-id' |
| **Partner System ID** | The system ID (MAC address) of the aggregation partner. |
| **Partner Key** | The Key that the partner has assigned to this aggregation ID. |
| **Last Changed** | The time since this aggregation changed. |
| **Local Ports** | Shows which ports are a part of this aggregation for this switch/stack. The format is: "Switch ID:Port". |

### 3.3.3.4 Port Status

The Port Status is displayed on this page.

| Port | LACP | Key | Aggr ID | Partner System ID | Partner Port |
|---|---|---|---|---|---|
| 1 | No | - | - | - | - |
| 2 | No | - | - | - | - |
| 3 | No | - | - | - | - |
| 4 | No | - | - | - | - |
| 5 | No | - | - | - | - |
| 6 | No | - | - | - | - |
| 7 | No | - | - | - | - |
| 8 | No | - | - | - | - |
| 9 | No | - | - | - | - |
| 10 | No | - | - | - | - |
| 11 | No | - | - | - | - |
| 12 | No | - | - | - | - |

**Port Status**

| Item | Description |
|---|---|
| **Port** | This field displays the interface number. |
| **LACP** | The system ID (MAC address) of the aggregation partner. |
| **Key** | The Key that the partner has assigned to this aggregation ID. |
| **Aggr ID** | The time since this aggregation changed. |
| **Partner System ID** | Shows which ports are a part of this aggregation for this switch/stack. The format is: "Switch ID:Port". |
| **Partner Port** | The partner port number connected to this port. |

### 3.3.3.5 Port Statistics

The Port Statistics is displayed on this page.

| Port | LACP Received | LACP Transmitted | Discarded | |
|---|---|---|---|---|
| | | | Unknown | Illegal |
| 1 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 |
| 3 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 |
| 11 | 0 | 0 | 0 | 0 |
| 12 | 0 | 0 | 0 | 0 |

**Port Statistics**

| Item | Description |
|---|---|
| **Port** | This field displays the interface number. |
| **LACP Transmitted** | This field displays how many LACP frames have been sent from each port. |
| **LACP Received** | This field displays how many LACP frames have been received at each port. |
| **Discarded** | This field displays how many unknown or illegal LACP frames have been discarded at each port. |

## 3.3.4 Loopback-Detection

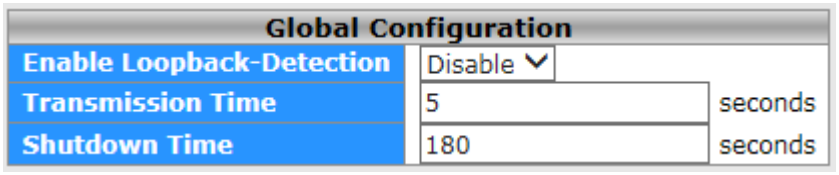
A loopback error occurs when the keep-alive packet is looped back to the port that sent the keep-alive packet.A Delta managed switch provide the Loopback-Detection function to detect the error in the network environment.

**Notice:**
We suggest that the Loopback-Detection function and redundancy protocol should not enable at the same time because the operating theory of these two functions are conflict.

### 3.3.4.1 Configuration

- **Global Configuration**

The module status of Loopback- Detection Global Configuration is used to enable/disable the Loopback-Detection feature.



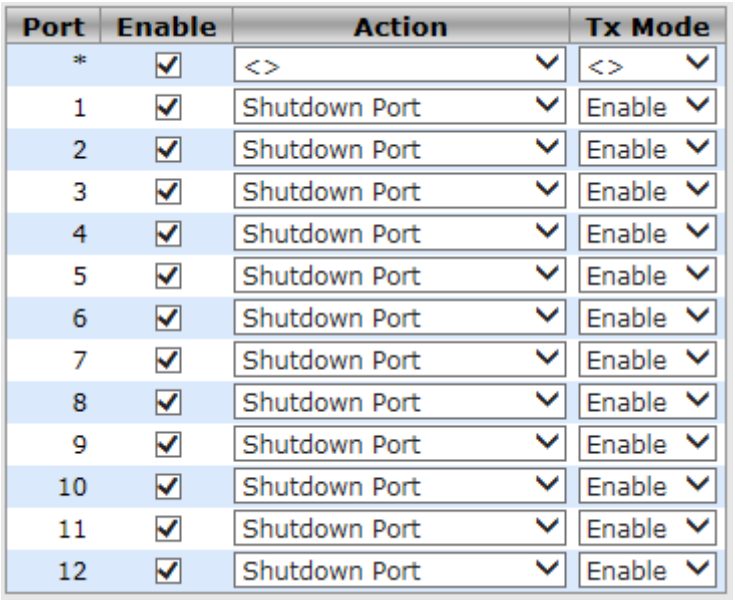

**Global Configuration**

| Description | Factory default |
|---|---|
| **Enable Loopback-Detection** | |
| Specify whether the status in global configuration is activated or not. | Disable |
| **Transmission Time** | |
| The interval between each loop protection PDU sent on each port valid values are 1 to 10 seconds. | 5 |
| **Shutdown Time** | |
| The period (in seconds) for which a port will be kept disabled in the event of a loop is detected (and the port action shuts down the port). Valid values are 0 to 604800 seconds (7 days). A value of zero will keep a port disabled (until next device restart). | 180 |

- **Port Configuration**

The parameters of Loopback-Detection should be set for each port.

**Notice:**
If you need to configure Loopback-Detection Port Configuration, you must enable the Loopback-Detection Global mode.



| Port | Enable | Action | Tx Mode |
|---|---|---|---|
| * | ☑ | <> | <> |
| 1 | ☑ | Shutdown Port | Enable |
| 2 | ☑ | Shutdown Port | Enable |
| 3 | ☑ | Shutdown Port | Enable |
| 4 | ☑ | Shutdown Port | Enable |
| 5 | ☑ | Shutdown Port | Enable |
| 6 | ☑ | Shutdown Port | Enable |
| 7 | ☑ | Shutdown Port | Enable |
| 8 | ☑ | Shutdown Port | Enable |
| 9 | ☑ | Shutdown Port | Enable |
| 10 | ☑ | Shutdown Port | Enable |
| 11 | ☑ | Shutdown Port | Enable |
| 12 | ☑ | Shutdown Port | Enable |

**Port Configuration**

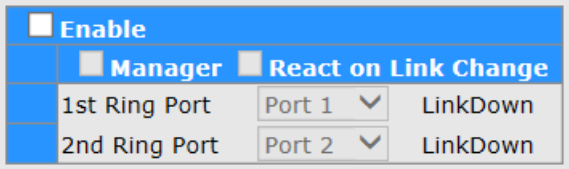
| Description | Factory default |
|---|---|
| **Port** | |
| The interface number. | *interface number* |
| **Enable** | |
| Enable/Disable the Loopback-Detection feature on the port. | Checked |
| **Action** | |
| Specify the action performed when a loop is detected on a port.<br>• Shutdown Port:<br>• Shutdown Port and Log:<br>• Log Only: | Shutdown Port |
| **Tx Mode** | |
| Specify whether the port is actively generating loop protection PDU's, or whether it is just passively looking for looped PDU's | Enable |

## 3.4 Redundancy

In some network environments, users need to set up redundant loops in the network to provide a backup path for disconnection or a network device breakdown. But if there are many network devices in the network, then each host needs to spend more time and cross many network devices to associate with each other. And sometimes the disconnection happens in a busy network, so the network must recover in a short time. Setting up redundancy on your network helps protect critical links against failure, protects against network loops, and keeps network downtime at a minimum. For example, if the Delta switch is used as a key communication component of a production line, several minutes of downtime may cause a big loss in production and revenue.

### 3.4.1 MRP

MRP (Media Redundancy Protocol) Ring (IEC 62439) of up to 50 devices typically transforms back to a line structure within 80 ms (adjustable to max. 200 ms/500 ms).

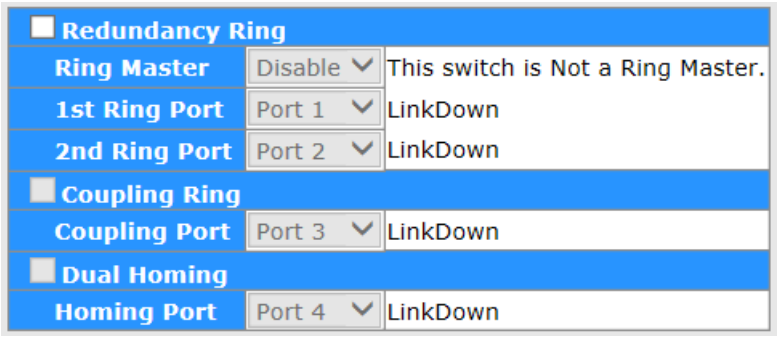



**MRP**

| Description | Factory default |
|---|---|
| **Enable** | |
| Specify whether the status in global configuration is activated or not. | Unchecked |
| **Manager** | |
| The manager node manages the MRP network, and there can only be one manager node in a MRP network. | Unchecked |
| **React on Link Change** | |
| Faster mode, if user enable this function , MRP network will more faster convergence, this function only can setting in MRP Manager Switch. | Unchecked |
| **1st Ring Port** | |
| Choosing the port which connecting to the MRP ring. | Port 1 |
| **2nd Ring Port** | |
| Choosing the port which connecting to the MRP ring. | Port 2 |

## 3.4.2 Redundancy Ring

The Redundany Ring topology consists of nodes having two ports participating in Redundancy Ring.
It can reduce unexpected damage caused by network topology change. It supports three of ring topology: Ring, Coupling Ring and Dual Homing.




**Redundancy Ring**

| Description | Factory default |
|---|---|
| **Redundancy Ring** | |
| Specify whether the Redundancy Ring mode is enabled or not. | Unchecked |
| **Ring Master** | |
| The master node manages the ring network, and there can only be one master node in a ring network. | Disable |
| **1st Ring Port** | |
| On the master node, it is the primary port. | Port1 |
| **2nd Ring Port** | |
| On the master node, it is the backup port. | Port2 |
| **Coupling Ring** | |
| Specify whether the Coupling Ring mode is enabled or not. | Disable |
| **Coupling Port** | |
| Select the specific port as a Coupling Port. | Port1 |

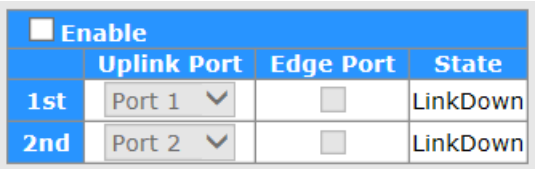
| Description | Factory default |
|---|---|
| **Dual Homing** | |
| Specify whether the Dual Homing mode is enabled or not. | Disable |
| **Homing Port** | |
| Select the specific port as a Homing Port. | Port1 |

**Notice:**
We don't suggest you to set one switch as a Ring Master and a Coupling Ring at the same time due to heavy load.

### 3.4.3 Redundancy Chain



The Redundany Chain topology consists of nodes having two ports participating in Redundancy Chain.
It can reduce unexpected damage caused by network topology change, and allows multiple redundant network rings of different redundancy protocols to join and function as a larger and more robust compound network topology.

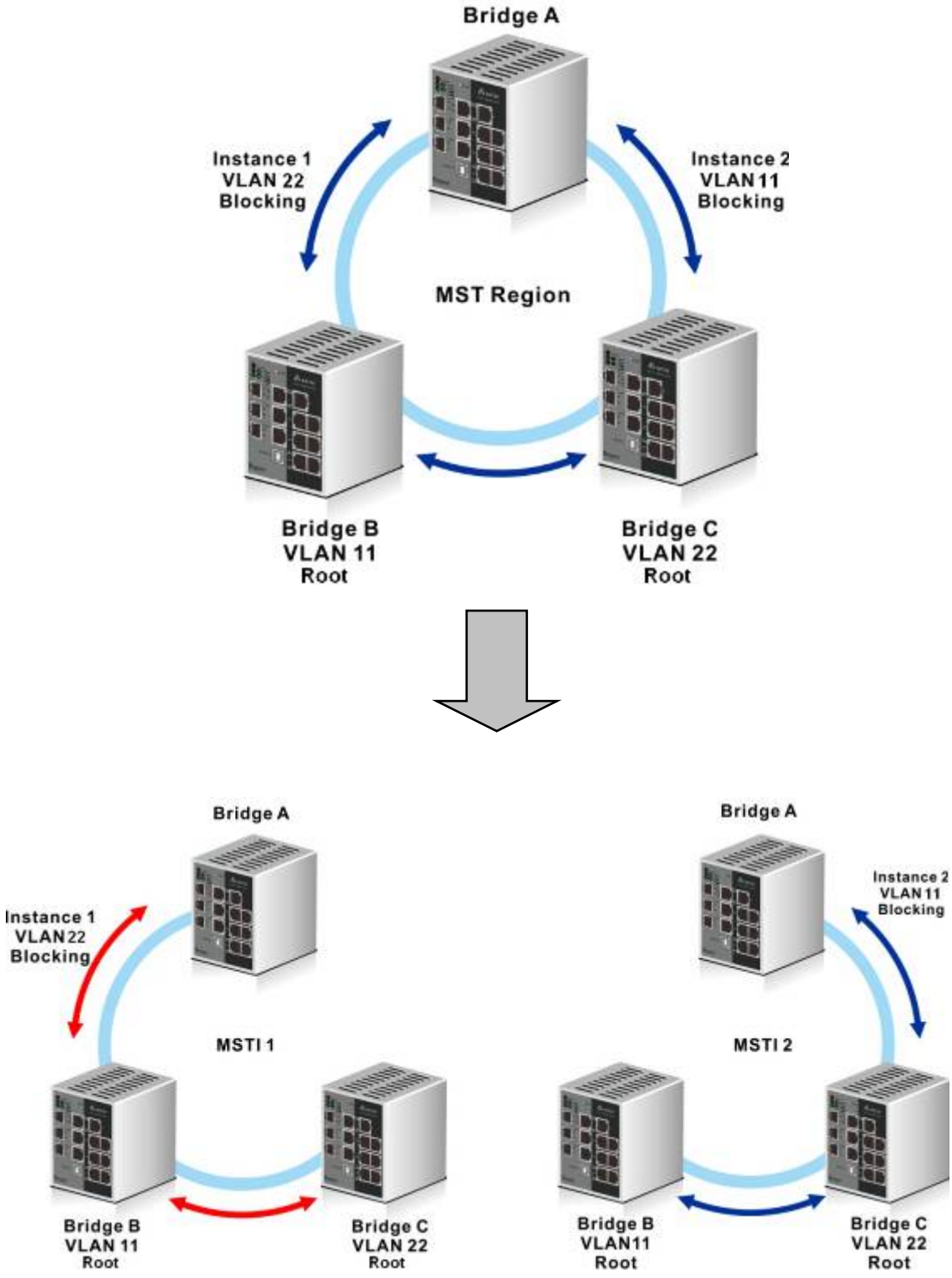



**Redundancy Chain**

| Description | Factory default |
|---|---|
| **Enable** | |
| Specify whether the Redundancy Chain mode is enabled or not. | Unchecked |
| **Uplink Port** | |
| Specify the priority of the specific port as an Uplink Port. | Port1 |
| **Edge Port** | |
| The edge port status of the interface:<br>• Checked: The interface is an edge port.<br>• Unchecked: The interface is not an edge port. | Unchecked |

### 3.4.4 MSTP

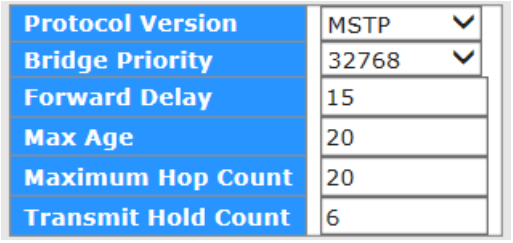
Multiple Spanning Tree Protocol (MSTP) is an extension protocol of RSTP. It can provide an independent spanning tree for different VLANs. MSTP builds a separate Multiple Spanning Tree (MST) for each instance. And MST Region may include multiple MSTP instances. The operating theory is shown in the figure below.




### 3.4.4.1 Bridge Settings

This page allows you to configure RSTP system settings. The settings are used by all RSTP Bridge instances in the Switch Stack.

- **Basic Settings**



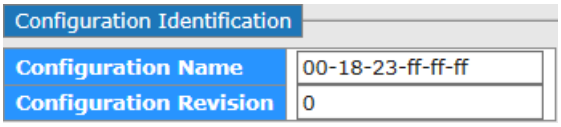

**Basic Settings**

| Description | Factory default |
|---|---|
| **Protocol Version** | |
| Specify the version of the STP protocol:<br>• **STP:** Spanning Tree Protocol.<br>• **RSTP:** Rapid Spanning Tree Protocol.<br>• **MSTP:** Multiple Spanning Tree Protocol. | MSTP |
| **Bridge Priority** | |
| Enter the bridge priority. Enter a number between 0 and 61440. | 32768 |
| **Forward Delay** | |
| Enter the switch forward delay time which the range of 4 to 30 seconds,and considering that the period needs to be greater than or equal to (Bridge Max Age / 2) + 1. | 15 |
| **Max Age** | |
| The timer that controls the maximum time that passes before an STP bridge port saves its configuration BPDU. | 20 |
| **Maximum Hop Count** | |
| Enter the maximum number of bridge hops; the information for a CST instance can travel before being discarded. Enter a number in the range of 6 to 40. | 20 |
| **Transmit Hold Count** | |
| The number of BPDU's a bridge port can send per second. When exceeded, transmission of the next BPDU will be delayed. Valid values are in the range 1 to 10 BPDU's per second. | 6 |

### 3.4.4.2 MSTI Mapping

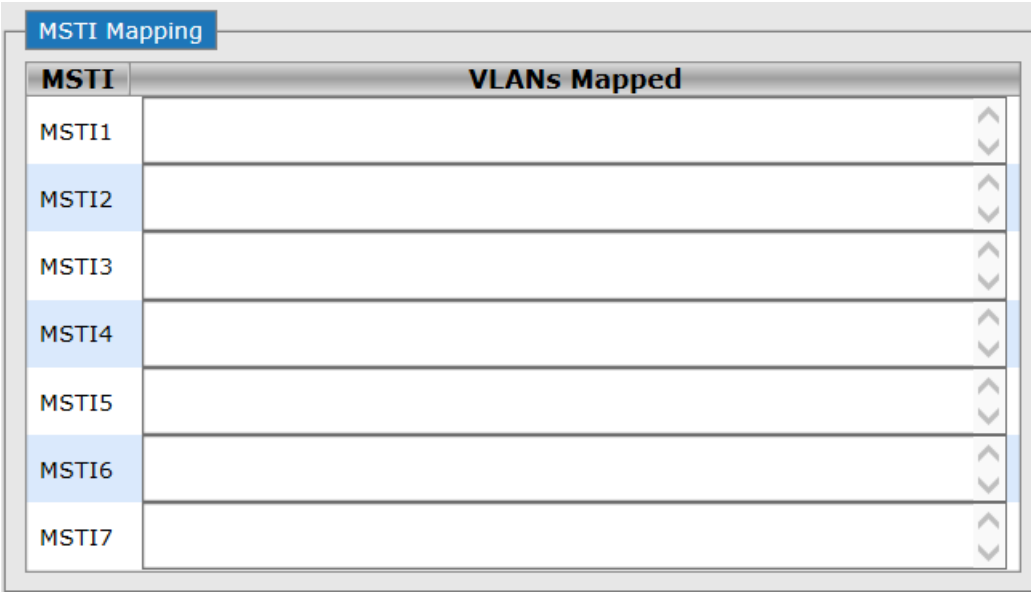
This page allows the user to inspect the current STP MSTI bridge instance priority configurations, and possibly change them as well.

- **Configuration Identification**




**Configuration Identification**

| Description | Factory default |
|---|---|
| **Configuration Name:** | |
| Specify the name identifiying the VLAN to MSTI mapping. The name is at most 32 characters. | *MAC address* |
| **Configuration Revision** | |
| Specify the revision of the MSTI configuration named above. This must be an integer between 0 and 65535. | 0 |

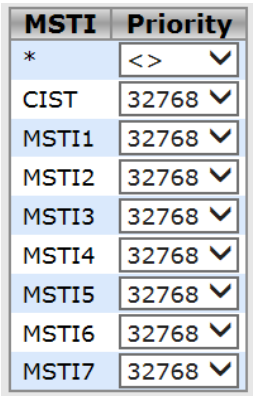



**MSTI Mapping**

| Description | Factory default |
|---|---|
| **MSTI** | |
| The bridge instance. The CIST is not available for explicit mapping, as it will receive the VLANs not explicitly mapped. | *Instance number* |
| **VLANs Mapping** | |
| The list of VLAN's mapped to the MSTI. One VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. | 0 |

### 3.4.4.3 MSTI Priorities

This page allows the user to inspect the current bridge instance priority configurations, and possibly change them as well.

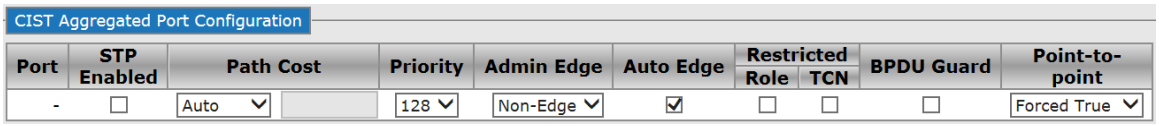



**MSTI Priorities**

| Description | Factory default |
|---|---|
| **MSTI** | |
| The bridge instance. The CIST is the default instance, which is always active. | *Instance number* |
| **Priority** | |
| The list of VLAN's mapped to the MSTI. One VLAN can only be mapped to one MSTI. An unused MSTI should just be left empty. | 0 |

### 3.4.4.4 CIST Ports

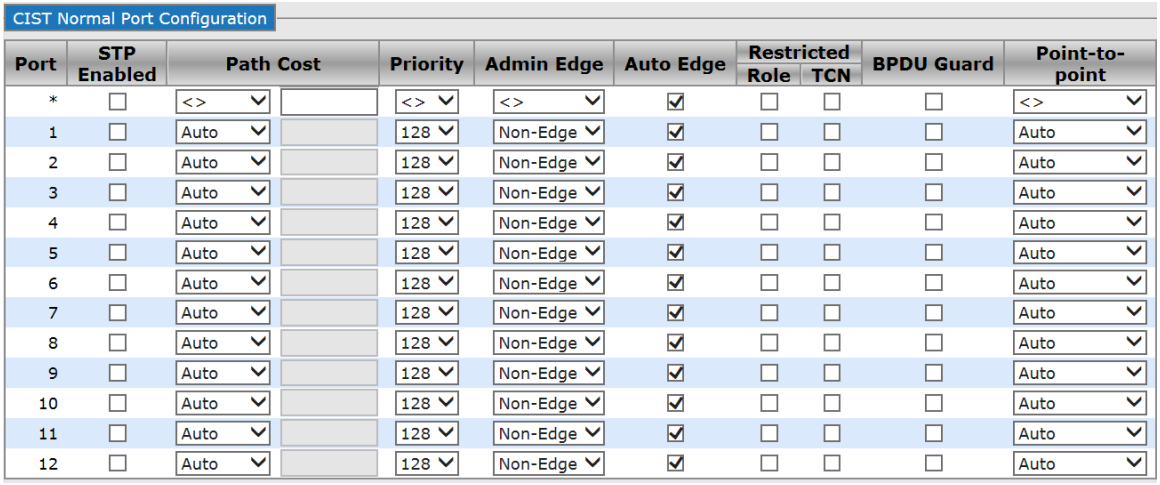
- **CIST Aggrgated Port Configuration**




**CIST Aggrgated Port Configuration**

| Description | Factory default |
|---|---|
| **Port** | |
| The switch port number of the logical STP port. | *None* |
| **STP Enabled** | |
| Specify whether the STP mode is enabled or not.<br>• **Checked:** STP is enabled.<br>• **Unchecked:** STP is disabled. | Unchecked |
| **Path Cost** | |
| Leave the existing path cost, or enters a new path cost that is used for the interface in the CIST.<br>• Auto: It will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values<br>• Specific: Enter a number in the range of 1 to 200,000,000. Enter a blank (that is, remove the number and make sure that there is no space character in the field) to reset the path cost. | Auto |
| **Priority** | |
| Enter the priority for the interface in the CIST. Enter a value between 0 and 240 that is a multiple of 16. The default priority is 128. | 128 |
| **Admin Edge** | |
| Controls whether the operEdge flag should start as beeing set or cleared. (The initial operEdge state when a port is initialized). | Non-Edge |
| **Auto Edge** | |
| Controls whether the bridge should enable automatic edge detection on the bridge port. | Checked |
| **Restricted** | |
| Specify whether the restricted role or TCN guard restricted is enabled or not. | Unchecked |
| **BPDU Guard** | |
| Specify whether the BPDU guard is enabled or not. | Unchecked |
| **Point-to-point** | |
| Specify the point-to-point status of the interface in the CIST:<br>• **ForceTrue:** The interface has a point-to-point connection to a switch, bridge, or end node, irrespective of the actual connection.<br>• **ForceFalse:** The interface does not have a point-to-point connection to a switch, bridge, or end node, irrespective of the actual connection.<br>• **Auto:** The type of connection is automatically detected. | Auto |

- **CIST Normal Port Configuration**



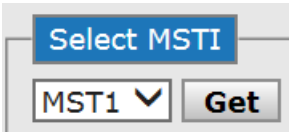

**CIST Normal Port Configuration**

| Description | Factory default |
|---|---|
| **Port** | |
| The switch port number of the logical STP port. | *None* |
| **STP Enabled** | |
| Specify whether the STP mode is enabled or not.<br>• **Checked:** STP is enabled.<br>• **Unchecked:** STP is disabled. | Unchecked |
| **Path Cost** | |
| Leave the existing path cost, or enters a new path cost that is used for the interface in the CIST.<br>• Auto: It will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values<br>• Specific: Enter a number in the range of 1 to 200,000,000. Enter a blank (that is, remove the number and make sure that there is no space character in the field) to reset the path cost. | Auto |
| **Priority** | |
| Enter the priority for the interface in the CIST. Enter a value between 0 and 240 that is a multiple of 16. The default priority is 128. | 128 |
| **Admin Edge** | |
| Controls whether the operEdge flag should start as beeing set or cleared. (The initial operEdge state when a port is initialized). | Non-Edge |
| **Auto Edge** | |
| Controls whether the bridge should enable automatic edge detection on the bridge port. | Checked |
| **Restricted** | |
| Specify whether the restricted role or TCN guard restricted is enabled or not. | Unchecked |
| **BPDU Guard** | |
| Specify whether the BPDU guard is enabled or not. | Unchecked |
| **Point-to-point** | |
| Specify the point-to-point status of the interface in the CIST:<br>• **ForceTrue:** The interface has a point-to-point connection to a switch, bridge, or end node, irrespective of the actual connection.<br>• **ForceFalse:** The interface does not have a point-to-point connection to a switch, bridge, or end node, irrespective of the actual connection.<br>• **Auto:** The type of connection is automatically detected. | Auto |

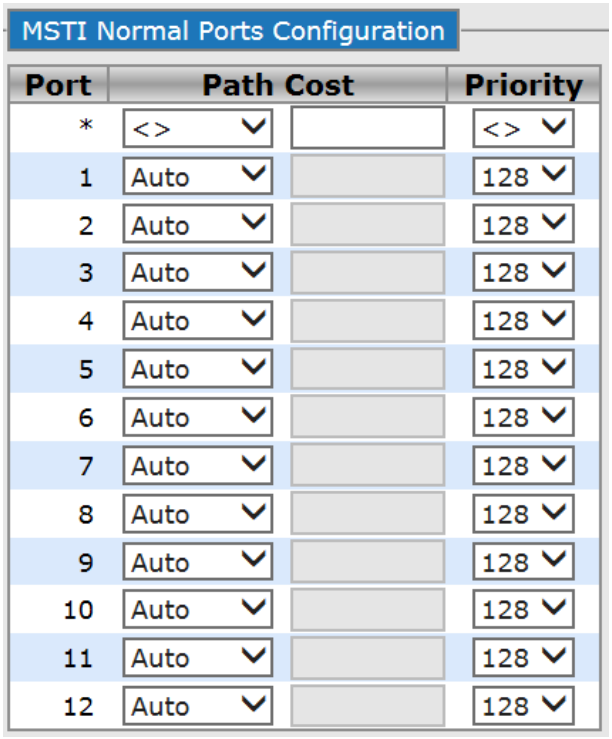
### 3.4.4.5 MSTI Ports

- **Select MSTI**

You can select the MSTI instance number from the drop-down list then click “Get” to go the MSTI Normal Ports Configuration




- **MSTI Normal Ports Configuration**




**MSTI Normal Port Configuration**

| Description | Factory default |
|---|---|
| **Port** | |
| This field displays the interface number or port channel number. | *interface number* |
| **Path Cost** | |
| Leave the existing path cost, or enters a new path cost that is used for the interface in the CIST.<br>• Auto: It will set the path cost as appropriate by the physical link speed, using the 802.1D recommended values<br>• Specific: Enter a number in the range of 1 to 200,000,000. Enter a blank (that is, remove the number and make sure that there is no space character in the field) to reset the path cost. | Auto |
| **Priority** | |
| Enter the priority for the interface in the CIST. Enter a value between 0 and 240 that is a multiple of 16. The default priority is 128. | 128 |

### 3.4.4.6 Bridge Status

| MSTI | Bridge ID | Root | | | Topology Flag | Topology Change Last |
|---|---|---|---|---|---|---|
| | | ID | Port | Cost | | |
| CIST | 32768.00-18-23-FF-FF-FF | 32768.00-18-23-FF-FF-FF | - | 0 | Steady | - |

**Bridge Status**

| Item | Description |
|---|---|
| MSTI | The Bridge Instance. This is also a link to the STP Detailed Bridge Status. |
| Bridge ID | The Bridge ID of this Bridge instance. |
| Root ID | The Bridge ID of the currently elected root bridge. |
| Root Port | The switch port currently assigned the root port role. |
| Root Cost | Root Path Cost. For the Root Bridge this is zero. For all other Bridges, it is the sum of the Port Path Costs on the least cost path to the Root Bridge. |
| Topology Flag | The current state of the Topology Change Flag for this Bridge instance. |
| Topology Change Last | The time since last Topology Change occurred. |

### 3.4.4.7 Port Status

| Port | CIST Role | CIST State | Uptime |
|---|---|---|---|
| 1 | Non-STP | Forwarding | - |
| 2 | Non-STP | Forwarding | - |
| 3 | Non-STP | Forwarding | - |
| 4 | Non-STP | Forwarding | - |
| 5 | Non-STP | Forwarding | - |
| 6 | Non-STP | Forwarding | - |
| 7 | Non-STP | Forwarding | - |
| 8 | Non-STP | Forwarding | - |
| 9 | Non-STP | Forwarding | - |
| 10 | Non-STP | Forwarding | - |
| 11 | Non-STP | Forwarding | - |
| 12 | Non-STP | Forwarding | - |

**Port Status**

| Item | Description |
|---|---|
| **Port** | This field shows the interface number. |
| **CIST Role** | The current STP port role of the CIST port. The port role can be one of the following values: AlternatePort BackupPort RootPort DesignatedPort. |
| **CIST State** | The current STP port state of the CIST port. The port state can be one of the following values: Blocking Learning Forwarding. |
| **Uptime** | The time since the bridge port was last initialized. |

### 3.4.4.8 Port Statistics

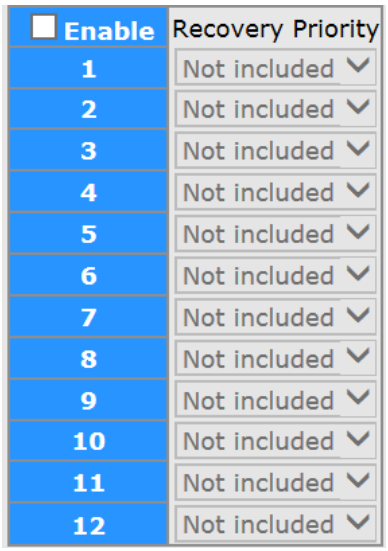
| Port | Transmitted | | | | Received | | | | Discarded | |
|---|---|---|---|---|---|---|---|---|---|---|
| | MSTP | RSTP | STP | TCN | MSTP | RSTP | STP | TCN | Unknown | Illegal |
| No ports enabled | | | | | | | | | | |

**Port Statistics**

| Item | Description |
|---|---|
| **Port** | This field shows the interface number. |
| **Transmitted** | This field shows the number of MSTP/RSTP/STP/TCN configuration BPDU's transmitted on the port. |
| **Received** | This field shows the number of MSTP/RSTP/STP/TCN configuration BPDU's received on the port. |
| **Discarded** | The number of unknown/illegal Spanning Tree BPDU's received (and discarded) on the port. |

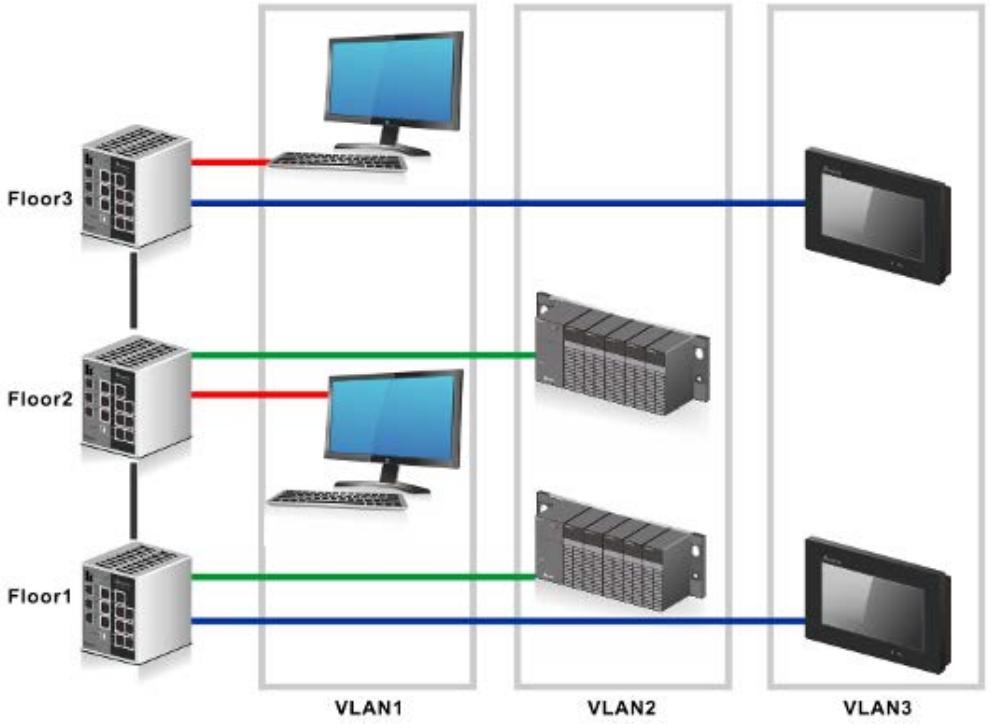
### 3.4.5 Fast Recovery mode

The Fast Recovery Mode can be set to connect multiple ports to one or more switches. The DVS PoE managed switch with its fast recovery mode will provide redundant links.
Fast Recovery mode supports 12 priorities, only the first priority will be the act port, the other ports configured with other priority will be the backup ports.




## 3.5 Virtual LANs

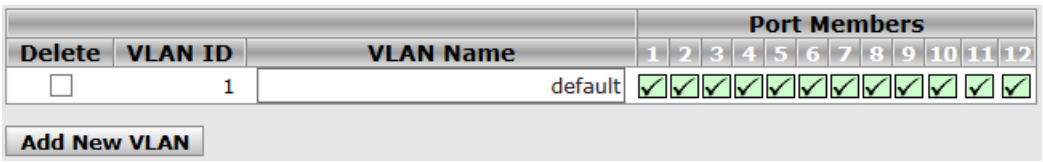
Virtual LAN (VLAN) is a logical group network. VLANs electronically separate interfaces on the same switch into different broadcast domains so that broadcast packets are not sent to all the interfaces on a single switch. VLAN allows the switch manager to isolate network traffic so that only members of the VLAN can receive traffic from the same VLAN members. VLAN also allows a user to access the network from a different place or switch. So VLAN provide security and flexibility.
For example: Configure department A, B, C to VLAN 1, 2, 3. Users can only access the resource which belongs to their department, so the resource in their department can be protected. And they can access the resource in a different floor, even though in a different place. So they do not need to stay in a fixed place to access the resource which belongs to their department.




## 3.5.1 VLAN Membership

VLAN Membership is used to define VLAN groups and the VLAN information will be stored in the VLAN membership table. A Delta PoE switch supports up to 64 VLANs. VLAN 1 is the default VLAN, and all interfaces are untagged members by the default setting.

**Note:**
If you need to access the switch via the port, we suggest that you make sure that the port you use is the untagged port of VLAN 1 (the default VLAN).



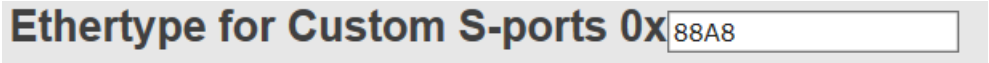

**VLAN Membership**

| Description | Factory default |
|---|---|
| **Delete** | |
| Check to delete the entry. It will be deleted during the next save | Unchecked |
| **VLAN ID** | |
| Enter the identifier for the new VLAN. The range can be set in the range of 1 to 4094. | 1 |
| **VLAN Name** | |
| Enter a name for the VLAN. The name can be up to 32 alphanumeric characters long, including blanks. | None |
| **Port Members** | |
| If the interface is not a member of VLAN, the square must keep blank. The port currently is not the static member of the VLAN, but it can be added dynamically by other protocols, for example by GVRP. | Checked |

**Add New VLAN**
Enter the identifier and a name for the VLAN, and the range of VLAN ID is from 1 to 4095. You can add and configure all interfaces as members to the specific VLAN

### 3.5.2 Ports

- **Ethertype for Custom S-ports**




**Ethertype for Custom S-ports**

| Description | Factory default |
|---|---|
| **Entertype for Custom S-ports** | |
| Specify the ether type used for Custom S-ports. This is a global setting for all the Custom S-ports. | 0x88A8 |

- **Ports Configuration**

Ports Configuration is used to defined all interface with three difference type:

- Unware: It can be used for 802.1 QinQ, and the TPID of frame will be set to 0x8100.
- C-port: The TPID of frame will be set to 0x8100.
- S-port: The TPID of frame will be set to 0x88A8
- S-custom-port: The TPID of received frame will be set to 0x88A8, and the transceived frame will be set to a customize value which from the Ethertype for Custom S-port.

| Port | Port Type | Ingress Filtering | Frame Type | Port VLAN Mode | Port VLAN ID | Tx Tag |
|---|---|---|---|---|---|---|
| * | <> | ☐ | <> | <> | 1 | <> |
| 1 | Unaware | ☐ | All | Specific | 1 | Untag_pvid |
| 2 | Unaware | ☐ | All | Specific | 1 | Untag_pvid |
| 3 | Unaware | ☐ | All | Specific | 1 | Untag_pvid |
| 4 | Unaware | ☐ | All | Specific | 1 | Untag_pvid |
| 5 | Unaware | ☐ | All | Specific | 1 | Untag_pvid |
| 6 | Unaware | ☐ | All | Specific | 1 | Untag_pvid |
| 7 | Unaware | ☐ | All | Specific | 1 | Untag_pvid |
| 8 | Unaware | ☐ | All | Specific | 1 | Untag_pvid |
| 9 | Unaware | ☐ | All | Specific | 1 | Untag_pvid |
| 10 | Unaware | ☐ | All | Specific | 1 | Untag_pvid |
| 11 | Unaware | ☐ | All | Specific | 1 | Untag_pvid |
| 12 | Unaware | ☐ | All | Specific | 1 | Untag_pvid |

**Ports Configuration**

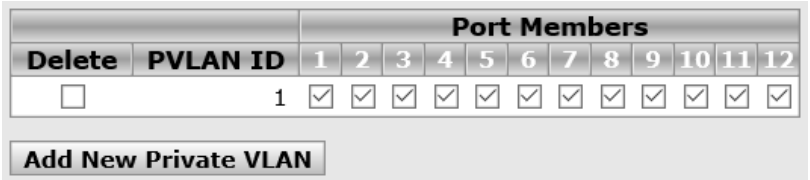
| Description | Factory default |
|---|---|
| **Port** | |
| This field displays the interface number or port channel number | *interface number* |
| **Port Typa** | |
| Specify the interface type:<br>• **Unware:** All frames are classified to the Port VLAN ID and tags are not removed.<br>• **C-port:** Customer Port<br>• **S-port:** Service Port<br>• **S-custom-port:** Custom Service port. | Unware |
| **Ingress Filtering** | |
| Specify whether the ingress filtering is applied:<br>• **Checked:** The ingress filtering is enabled for the interface.<br>• **Unchecked:** The ingress filtering is disabled for the interface. All frames are forwarded. | Unchecked |

| Description | Factory default |
|---|---|
| **Frame Type** | |
| Specify whether the port accepts all frames or only tagged/untagged frames.<br>• **All:** The port accepts all frames.<br>• **Tagged**: The port only accepts tagged frame, and the untagged will be discarded.<br>• **Untagged:** The port only accepts untagged frame. | All |
| **Port VLAN_Mode** | |
| Specify the mode of the interface.<br>• **None:** This mode is normally used for ports connected to VLAN aware switches. Tx tag should be set to Untag_pvid when this mode is used.<br>• **Specific:** If Specific (the default value) is selected, a Port VLAN ID can be configured. | Specific |
| **Port VLAN_ID** | |
| Specify the the VLAN identifier for the port.<br>**Note:**<br>If you want to change the default PVID of an interface, create VLAN and then includes the interface as a member. | 1 |
| **Tx Tag** | |
| Specify the egress tagging rule of a port.<br>• **Untag_pvid**: All VLANs except the configured PVID will be tagged.<br>• **Tag_all**: All VLANs are tagged.<br>• **Untag_all:** All VLANs are untagged. | Untag_pvid |

### 3.5.3 Private VLAN

The Private VLAN membership configurations for the switch can be monitored and modified here. Private VLANs can be added or deleted here. Port members of each Private VLAN can be added or removed here. Private VLANs are based on the source port mask, and there are no connections to VLANs. This means that VLAN IDs and Private VLAN IDs can be identical.
A port must be a member of both a VLAN and a Private VLAN to be able to forward packets. By default, all ports are VLAN unaware and members of VLAN 1 and Private VLAN 1.
A VLAN unaware port can only be a member of one VLAN, but it can be a member of multiple Private VLANs.

#### 3.5.3.1 PVLAN Membership

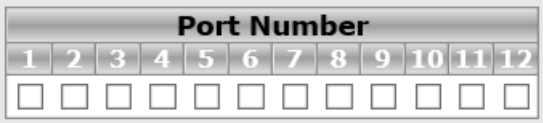



**Private VLAN Membership**

| Description | Factory default |
|---|---|
| **Delete** | |
| Check to delete the entry. It will be deleted during the next save. | Unchecked |
| **PVLAN ID** | |
| Enter the identifier for the new Private VLAN | 1 |
| **Port Members** | |
| If the interface is not a member of VLAN, the square must keep blank. The port currently is not the static member of the VLAN, but it can be added dynamically by other protocols, for example by GVRP. | Checked |

**Add New Private VLAN**
Enter the identifier and a name for the Private VLAN, and the range is from 1 to 4095. You can add and configure all interfaces as members to the specific Private VLAN.

#### 3.5.3.2 Port Isolation




**Port Isolation**

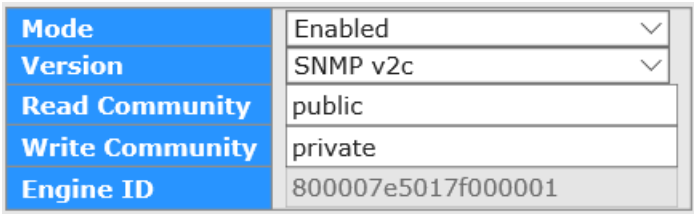
| Description | Factory default |
|---|---|
| **Port Number** | |
| Specify whether the interface is enabled or not.<br>• **Checked:** The interface is enabled.<br>• **Unchecked:** The interface is disabled. | Unchecked |

## 3.6 SNMP

Simple Network Management Protocol (SNMP) is an application protocol used for exchanging management information between network devices. SNMP is a member of the TCP/IP protocol suite. SNMP V1, V2 and V3 are supported on the Delta switch, and it is enabled by default.
A Delta switch supports standard public MIBs for standard functionality and private MIBs that provide additional functionality. You can use SNMP to enable or disable authentication traps, cold-start and warm-start functionality traps, link up and link down traps, Spanning Tree Protocol (STP) traps, SFP traps, and password and IP address change traps.

### 3.6.1 System

- **System Configuration**

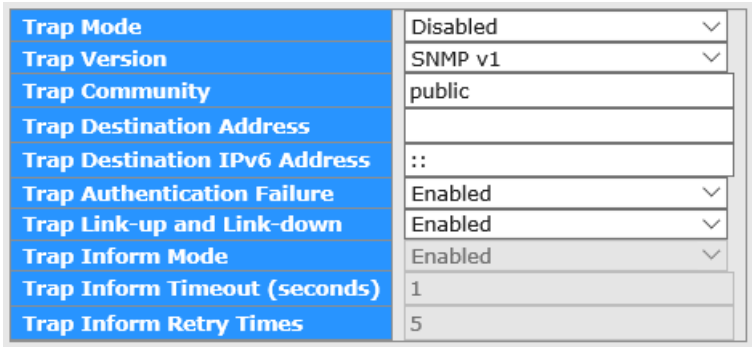



**System Configuration**

| Description | Factory default |
|---|---|
| **Mode** | |
| Specify whether the SNMP mode is enabled or not.<br>• **Enabled:** SNMP is enabled.<br>• **Disabled:** SNMP is disabled. | Enabled |
| **Version** | |
| Specify the SNMP version that is used for the trap community:<br>• **SNMP v1**: Uses SNMPv1 to send traps to the trap community.<br>• **SNMP v2c**: Uses SNMPv2c to send traps to the trap community.<br>• **SNMP v3**: Uses SNMPv3 to send traps to the trap community. | SNMP v2c |
| **Read Community** | |
| Entering the community read access string to permit access to SNMP agent. The string length is 0 to 255, and the content is the ASCII characters from 33 to 126. | public |
| **Write Commnunity** | |
| Entering the community read access string to permit access to SNMP agent. The string length is 0 to 255, and the content is the ASCII characters from 33 to 126. | private |
| **Engine ID** | |
| Entering the SNMPv3 engine ID. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users. | Fixed |

- **Trap Configuration**

If network engineers need to get information from an SNMP agent (network device), they usually use the SNMP software to poll information and get a response from an agent. But the SNMP Trap is the unsolicited trap which sends from the agent to the NMS (Network Management System).The operating theory is shown in the figure below.




**Trap Configuration**

| Description | Factory default |
|---|---|
| **Trap Mode** | |
| Specify whether the Trap mode is enabled or not.<br>• **Enabled:** Trap mode is enabled.<br>• **Disabled:** Trap mode is disabled. | Disabled |
| **Trap Version** | |
| Specify the SNMP Trap version that is used for the trap community.<br>• **SNMP v1**: Uses SNMPv1 to send traps to the trap community.<br>• **SNMP v2c**: Uses SNMPv2c to send traps to the trap community.<br>• **SNMP v3**: Uses SNMPv3 to send traps to the trap community. | SNMP v1 |
| **Trap Community** | |
| Specify the community access string when send SNMP trap packet. The allowed string length is 0 to 255, and the allowed content is the ASCII characters from 33 to 126. | public |
| **Trap Destination Address** | |
| Entering the SNMP trap destination address in IPv6 format. | None |
| **Trap Destination IPv6 Address** | |
| Entering the SNMP trap destination address in IPv6 format. | None |
| **Trap Authentication Failure** | |
| Specify whether the Trap Authentication Failure is enabled or not.<br>• Enabled: Enable SNMP trap authentication failure.<br>• Disabled: Disable SNMP trap authentication failure | Enabled |
| **Trap Link-up and Link-down** | |
| Specify whether the Trap Link-up and Link-down is enabled or not.<br>• Enabled: Enable Trap Link-up and Link-down.<br>• Disabled: Disable Trap Link-up and Link-down. | Enabled |
| **Trap Inform Mode** | |
| Specify whether the Trap Link-up and Link-down is enabled or not.<br>• Enabled: Enable T Trap Inform Mode.<br>• Disabled: Disable Trap Inform Mode.<br>**Note:**<br>It's only be activated the configuration when you select the Trap version to SNMPv2c. | Enabled |
| **Trap Inform Timeout (seconds)** | |
| Entering the Trap Inform Timeout. The range is 0 to 2047.<br>**Note:**<br>It's only be activated the configuration when you select the Trap version to SNMPv2c. | 1 |

| Description | Factory default |
|---|---|
| **Trap Inform Retry Times** | |
| Entering the Trap Inform Retry Times. The range is 0 to 255.<br>**Note:**<br>It's only be activated the configuration when you select the Trap version to SNMPv2c. | 5 |

### 3.6.2 Communities

Configure SNMPv3 communities table on this page. The entry index key is Community.

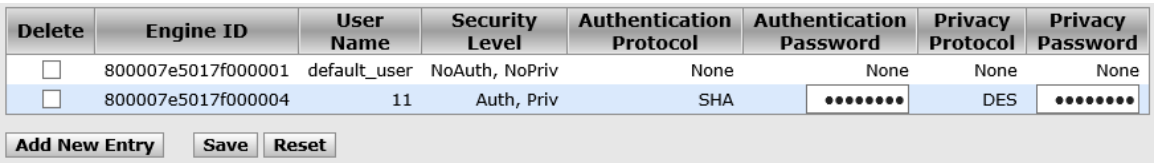
Click " Add New Entry" to add a new communities.


**Communities**

| Description | Factory default |
|---|---|
| **Delete** | |
| Check to delete the entry. It will be deleted during the next save. | Unchecked |
| **Community** | |
| Entering the community access string to permit access to SNMPv3 agent. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126. | None |
| **Source IP** | |
| Entering the SNMP access source address. | 0.0.0.0 |
| **Source Mask** | |
| Entering the SNMP access source address mask. | 0.0.0.0 |

### 3.6.3 Users

Configure SNMPv3 users table on this page. The entry index keys are Engine ID and User Name.




**Users**

| Description | Factory default |
|---|---|
| **Delete** | |
| Check to delete the entry. It will be deleted during the next save. | Unchecked |
| **Engine ID** | |
| Entering the SNMPv3 engine ID. The string must contain an even number between 10 and 64 hexadecimal digits, but all-zeros and all-'F's are not allowed. Change of the Engine ID will clear all original local users. | None |
| **User Name** | |
| A string identifying the user name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126. | None |
| **Security Level** | |
| Specify the security level that this entry should belong to.<br>• NoAuth, NoPriv: None authentication and none privacy. | NoAuth, NoPriv |

| | |
|---|---|
| • Auth, NoPriv: Authentication and none privacy.<br>• Auth, Priv: Authentication and privacy.<br>**Note:**<br>The value of security level cannot be modified if entry already exists. | |
| **Authentication Protocol** | |
| Specify the authentication protocol.<br>• None: None authentication protocol<br>• MD5: An optional flag to indicate that this user is using MD5 authentication protocol.<br>• SHA: An optional flag to indicate that this user is using SHA authentication protocol.<br>**Note:**<br>The value of security level cannot be modified if entry already exists. | None |
| **Authentication Password** | |
| Entering the password for new entry authentication protocol with ASCII character, and the length is 33 to 126. The MD5 Protocol is 8 to 32, and the SHA protocol is 8 to 40. | None |
| **Privacy Protocol** | |
| Specify the privacy protocol.<br>• None: None privacy protocol.<br>• DES: An optional flag to indicate that this user using DES authentication protocol. | None |
| **Privacy Password** | |
| Entering the password for Privacy protocol with ASCII character, and the length is 33 to 126. | None |

## 3.6.4 Groups

| Delete | Security Model | Security Name | Group Name |
|---|---|---|---|
| ☐ | v1 | public | default_ro_group |
| ☐ | v1 | private | default_rw_group |
| ☐ | v2c | public | default_ro_group |
| ☐ | v2c | private | default_rw_group |
| ☐ | usm | default_user | default_rw_group |

**Groups**

| Description | Factory default |
|---|---|
| **Delete** | |
| Check to delete the entry. It will be deleted during the next save. | Unchecked |
| **Security Model** | |
| Specify the security model.<br>• v1: Reserved for SNMPv1.<br>• v2c: Reserved for SNMPv2c.<br>• usm: User-based Security Model (USM). | v1 |
| **Security Name** | |
| A string identifying the security name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126. | None |
| **Group Name** | |
| A string identifying the group name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126. | None |

## 3.6.5 Views

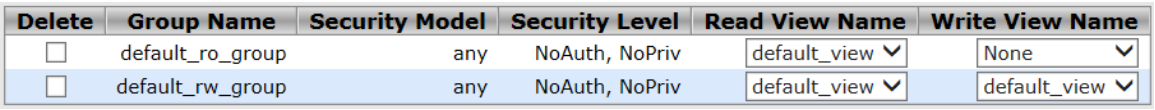
Configure SNMPv3 views table on this page. The entry index keys are View Name and OID Subtree.


**Views**

| Description | Factory default |
|---|---|
| **Delete** | |
| Check to delete the entry. It will be deleted during the next save. | Unchecked |
| **View Name** | |
| A string identifying the view name that this entry should belong to. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126. | None |
| **View Type** | |
| Specify the view type that this entry should belong to.<br>• included: An optional flag to indicate that this view subtree should be included.<br>• excluded: An optional flag to indicate that this view subtree should be excluded.<br>General, if a view entry's view type is 'excluded', it should be exist another view entry which view type is 'included' and it's OID subtree overstep the 'excluded' view entry. | None |
| **OID Subtree** | |
| The OID defining the root of the subtree to add to the named view. The allowed OID length is 1 to 128. The allowed string content is digital number or asterisk(*). | None |

## 3.6.6 Access

Configure SNMPv3 accesses table on this page. The entry index keys are Group Name, Security Model and Security Level.




**Access**

| Description | Factory default |
|---|---|
| **Delete** | |
| Check to delete the entry. It will be deleted during the next save. | Unchecked |
| **Group Name** | |
| Specify the group name.<br>**Note:**<br>If you want to add another group name, you could add the name in "Groups" configuration. | None |
| **Security Model** | |
| Specify the security model.<br>• any: Accepted any security model.<br>• v1: Reserved for SNMPv1.<br>• v2c: Reserved for SNMPv2c.<br>• usm: User-based Security Model (USM). | any |
| **Security Level** | |
| Specify the security level that this entry should belong to.<br>• NoAuth, NoPriv: None authentication and none privacy.<br>• Auth, NoPriv: Authentication and none privacy.<br>• Auth, Priv: Authentication and privacy.<br>**Note:**<br>The value of security level cannot be modified if entry already exists. | NoAuth, NoPriv |
| **Read View Name** | |
| The name of the MIB view which defining the MIB objects for which this request may request the current values. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126. | None |

| Description | Factory default |
|---|---|
| **Write View Name** | |
| The name of the MIB view which defining the MIB objects for which this request may potentially SET new values. The allowed string length is 1 to 32, and the allowed content is the ASCII characters from 33 to 126. | None |

## 3.7 Traffic Prioritization

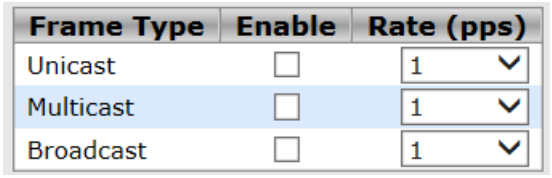
The traffic prioritization allows you to make sure that the time-sensitive and system-critical data can be transferred with the minimal delay. It uses four queues that are present in UI from the high priority to the low priority.
A Delta switch supports the DSCP trust mode, the 802.1p trust mode, the queue scheduling (Support Weighted Round Robin and Strict-Priority) and 4 level priority queues. The traffic prioritization depends on 2 methods:

- **IEEE 802.1P:** a layer 2 marking scheme.
- **Differentiated Services (DiffServ):** a layer 3 marking scheme.



### 3.7.1 Storm Control

A traffic storm occurs when incoming packets flood the LAN, which causes the decreasing of the network performance. The storm control can prevent flooding packets from affecting the network performance. A Delta switch allows you to configure both storm control for each interface and rate limiting of each interface for incoming and outgoing traffic.

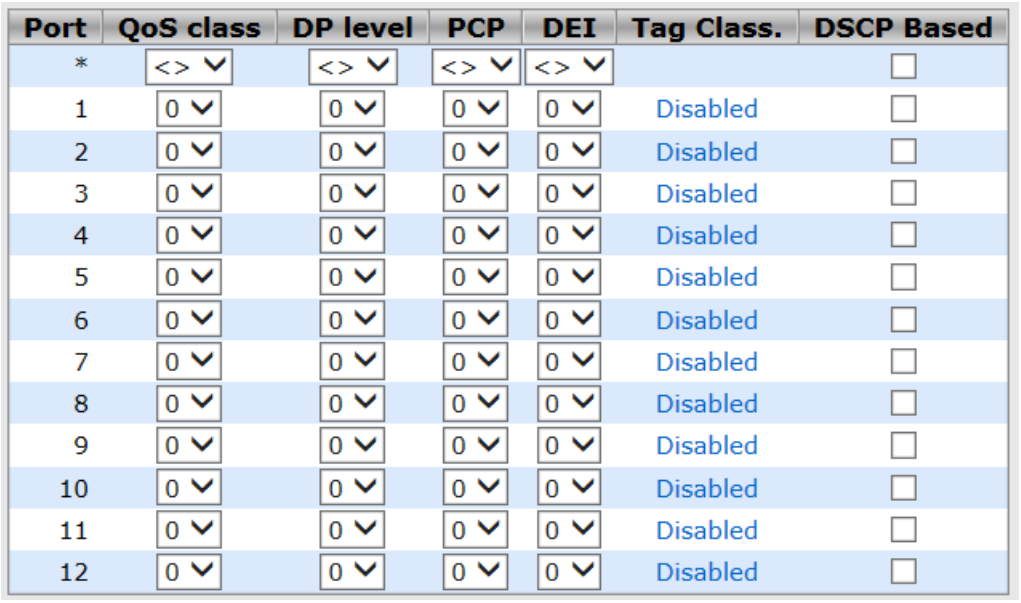



**Storm Control**

| Description | Factory default |
|---|---|
| **Frame Type** | |
| The settings in a particular row apply to the frame type listed here: unicast, multicast, or broadcast. | Fixed |
| **Enable** | |
| Specify whether the frame type is enabled or not.<br>• **Checked:** Enable the storm control of the frame type.<br>• **Unchecked:** Disable the storm control of the frame type. | Unchecked |
| **Rate** | |
| The rate unit is packet per second (pps), configure the rate as 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K.<br>The 1 kpps is actually 1002.1 pps. | 1K |

### 3.7.2 Port Classfication

Quality of Service (QoS) provides a traffic prioritization for you to alleviate the congestion problem, and ensure that high-priority traffic is delivered first. If the bandwidth of the network is limited, you can use QoS to schedule the priority of a different service packet flow.

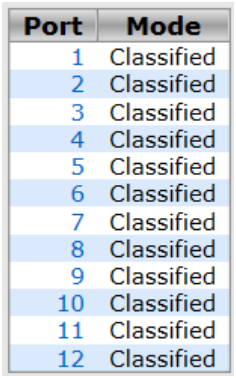


| Port | QoS class | DP level | PCP | DEI | Tag Class. | DSCP Based |
|---|---|---|---|---|---|---|
| * | <> | <> | <> | <> | | |
| 1 | 0 | 0 | 0 | 0 | Disabled | |
| 2 | 0 | 0 | 0 | 0 | Disabled | |
| 3 | 0 | 0 | 0 | 0 | Disabled | |
| 4 | 0 | 0 | 0 | 0 | Disabled | |
| 5 | 0 | 0 | 0 | 0 | Disabled | |
| 6 | 0 | 0 | 0 | 0 | Disabled | |
| 7 | 0 | 0 | 0 | 0 | Disabled | |
| 8 | 0 | 0 | 0 | 0 | Disabled | |
| 9 | 0 | 0 | 0 | 0 | Disabled | |
| 10 | 0 | 0 | 0 | 0 | Disabled | |
| 11 | 0 | 0 | 0 | 0 | Disabled | |
| 12 | 0 | 0 | 0 | 0 | Disabled | |

**Port Classification**

| Description | Factory default |
|---|---|
| **Port** | |
| The interface number. | *interface number* |
| **QoS class** | |
| Specify the default QoS class.<br>• **PCP value:** 0 1 2 3 4 5 6 7<br>• **QoS class:** 1 0 2 3 4 5 6 7 | 0 |
| **DP level** | |
| Specif the default Drop Precedence Level. All frames are classified to a DP level.<br>If the port is VLAN aware and the frame is tagged, then the frame is classified to a DP level that is equal to the DEI value in the tag. Otherwise the frame is classified to the default DP level.<br>If the port is VLAN aware, the frame is tagged and Tag Class is enabled, then the frame is classified to a DP level that is mapped from the PCP and DEI value in the tag. Otherwise the frame is classified to the default DP level.<br>The classified DP level can be overruled by a QCL entry. | 0 |
| **PCP** | |
| Specify the default PCP value. All frames are classified to a PCP value.<br>If the port is VLAN aware and the frame is tagged, then the frame is classified to the PCP value in the tag. Otherwise the frame is classified to the default PCP value | 0 |
| **DEI** | |
| Specify the default DEI value. All frames are classified to a DEI value.<br>If the port is VLAN aware and the frame is tagged, then the frame is classified to the DEI value in the tag. Otherwise the frame is classified to the default DEI value. | 0 |
| **Tag Class** | |
| Specify the classification mode for tagged frames on this port.<br>Disabled: Use default QoS class and DP level for tagged frames.<br>• **Unchecked:** Use default QoS class and DP level for tagged frames.<br>• **Checked:** Use mapped versions of PCP and DEI for tagged frames.<br>**Note:**<br>This setting has no effect if the port is VLAN unaware. Tagged frames received on VLAN unaware ports are always classified to the default QoS class and DP level. | interface number |

### 3.7.3 Port Tag Remarking

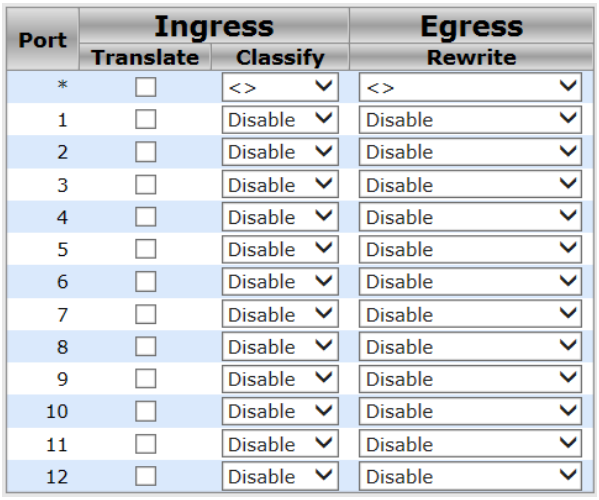


| Port | Mode |
|---|---|
| 1 | Classified |
| 2 | Classified |
| 3 | Classified |
| 4 | Classified |
| 5 | Classified |
| 6 | Classified |
| 7 | Classified |
| 8 | Classified |
| 9 | Classified |
| 10 | Classified |
| 11 | Classified |
| 12 | Classified |

**Port Tag Remarking**

| Item | Description |
|---|---|
| **Port** | The interface number. |
| **Mode** | The field displays the tag remarking mode for this port.<br>• Classified: Use classified PCP/DEI values.<br>• Default: Use default PCP/DEI values.<br>• Mapped: Use mapped versions of QoS class and DP level. |

### 3.7.4 Port DSCP



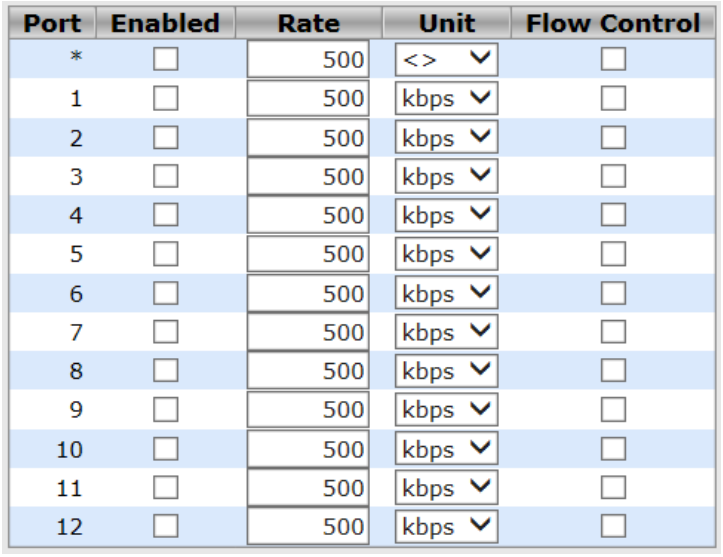
| Port | Ingress | | Egress |
|---|---|---|---|
| | Translate | Classify | Rewrite |
| * | ☐ | <> | <> |
| 1 | ☐ | Disable | Disable |
| 2 | ☐ | Disable | Disable |
| 3 | ☐ | Disable | Disable |
| 4 | ☐ | Disable | Disable |
| 5 | ☐ | Disable | Disable |
| 6 | ☐ | Disable | Disable |
| 7 | ☐ | Disable | Disable |
| 8 | ☐ | Disable | Disable |
| 9 | ☐ | Disable | Disable |
| 10 | ☐ | Disable | Disable |
| 11 | ☐ | Disable | Disable |
| 12 | ☐ | Disable | Disable |

**Port DSCP**

| Description | Factory default |
|---|---|
| **Port** | |
| The interface number | *interface number* |
| **Ingress_Translate** | |
| Specify whether the Ingress Translation is enabled or not.<br>• Checked: Enabled the Translate function.<br>• Unchecked: Disablede the Translate function. | Unchecked |
| **Ingress_Classify** | |
| Specify the Ingress classify function is enabled or not.<br>• Disable: No Ingress DSCP Classification.<br>• DSCP=0: Classify if incoming (or translated if enabled) DSCP is 0.<br>• Selected: Classify only selected DSCP for which classification is enabled as specified in DSCP Translation window for the specific DSCP.<br>• All: Classify all DSCP. | Disable |

| Description | Factory default |
|---|---|
| **Egress_Rewrite** | |
| Specify the Engress rewrite function is enabled or not.<br>• Disable: No Engress rewrite.<br>• Enable: Rewrite enabled without remapping.<br>• Remap DP Unaware: The remapped DSCP value is always taken from the 'DSCP Translation->Egress Remap DP0' table.<br>• Remap DP Aware: the remapped DSCP value is either taken from the 'DSCP Translation->Egress Remap DP0' table or from the 'DSCP Translation->Egress Remap DP1' table. | Disable |

### 3.7.5 Port Policing



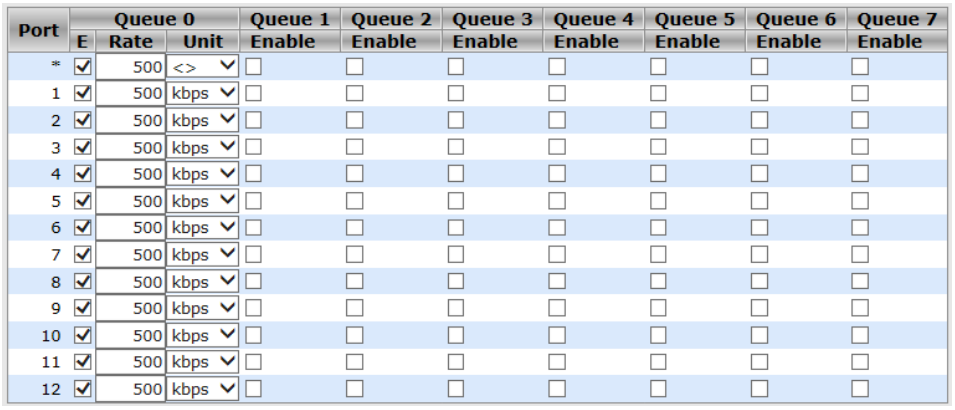
| Port | Enabled | Rate | Unit | Flow Control |
|---|---|---|---|---|
| * | ☐ | 500 | <> | ☐ |
| 1 | ☐ | 500 | kbps | ☐ |
| 2 | ☐ | 500 | kbps | ☐ |
| 3 | ☐ | 500 | kbps | ☐ |
| 4 | ☐ | 500 | kbps | ☐ |
| 5 | ☐ | 500 | kbps | ☐ |
| 6 | ☐ | 500 | kbps | ☐ |
| 7 | ☐ | 500 | kbps | ☐ |
| 8 | ☐ | 500 | kbps | ☐ |
| 9 | ☐ | 500 | kbps | ☐ |
| 10 | ☐ | 500 | kbps | ☐ |
| 11 | ☐ | 500 | kbps | ☐ |
| 12 | ☐ | 500 | kbps | ☐ |

**Port Policing**

| Description | Factory default |
|---|---|
| **Port** | |
| The interface number | *interface number* |
| **Enabled** | |
| Specify whether the QoS ingress port policer is enabled or not.<br>• **Checked**: Enabled the QoS ingress port policer.<br>• **Unchecked**: Disablede the QoS ingress port policer. | Unchecked |
| **Rate** | |
| Specify the rate of the QoS ingress port policer. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-3300 when the "Unit" is "Mbps" or "kfps". | 500 |
| **Unit** | |
| Specify the unit of measure for the policer rate as kbps, Mbps, fps or kfps . The default value is "kbps". | kbps |
| **Flow Control** | |
| This field displays whether the flow control is enabled for the port:<br>• **Checked**: The flow control is enabled. If the port buffers become full, the switch sends pause packets.<br>• **Unchecked**: The flow control is disabled. If the port buffers become full, the switch does not send pause packets. | Unchecked |

### 3.7.6 Queue Policing

It must be enabled the Queue number first, and then you could configure this feature.



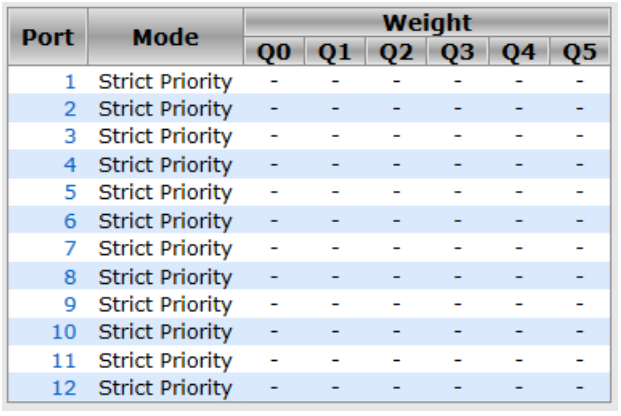
| Port | Queue 0 | | | Queue 1 | Queue 2 | Queue 3 | Queue 4 | Queue 5 | Queue 6 | Queue 7 |
|---|---|---|---|---|---|---|---|---|---|---|
| | E | Rate | Unit | Enable | Enable | Enable | Enable | Enable | Enable | Enable |
| * | ☑ | 500 | <> | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 1 | ☑ | 500 | kbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 2 | ☑ | 500 | kbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 3 | ☑ | 500 | kbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 4 | ☑ | 500 | kbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 5 | ☑ | 500 | kbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 6 | ☑ | 500 | kbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 7 | ☑ | 500 | kbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 8 | ☑ | 500 | kbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 9 | ☑ | 500 | kbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 10 | ☑ | 500 | kbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 11 | ☑ | 500 | kbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |
| 12 | ☑ | 500 | kbps | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ | ☐ |

**Queue Policing**

| Description | Factory default |
|---|---|
| **Port** | |
| The interface number | *interface number* |
| **Queue_0-7** | |
| The Queue policer number. | *Queue number* |
| **Enable** | |
| Specify whether the Queue policer is enabled or not. | Unchecked |
| **E** | |
| Specify whether the interface is participates in the specific Queue policer or not. | kbps |
| **Rate** | |
| Specify the rate of the QoS ingress port policer. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-3300 when the "Unit" is "Mbps" or "kfps". | 500 |
| **Unit** | |
| Specify the unit of measure for the policer rate as kbps, Mbps, fps or kfps . The default value is "kbps". | kbps |

### 3.7.7 Port Scheduler

This feature allows you to configure the Scheduler and Shapers for the specific port.



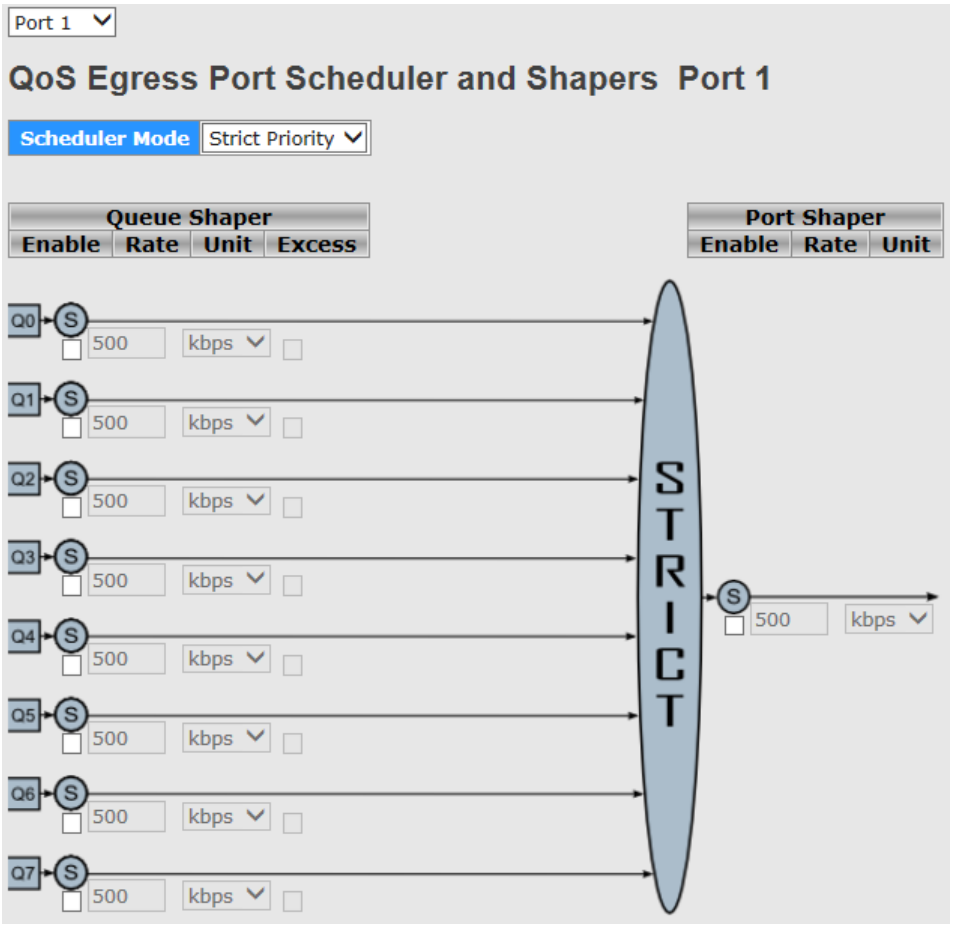
| Port | Mode | Weight | | | | | |
|---|---|---|---|---|---|---|---|
| | | Q0 | Q1 | Q2 | Q3 | Q4 | Q5 |
| 1 | Strict Priority | - | - | - | - | - | - |
| 2 | Strict Priority | - | - | - | - | - | - |
| 3 | Strict Priority | - | - | - | - | - | - |
| 4 | Strict Priority | - | - | - | - | - | - |
| 5 | Strict Priority | - | - | - | - | - | - |
| 6 | Strict Priority | - | - | - | - | - | - |
| 7 | Strict Priority | - | - | - | - | - | - |
| 8 | Strict Priority | - | - | - | - | - | - |
| 9 | Strict Priority | - | - | - | - | - | - |
| 10 | Strict Priority | - | - | - | - | - | - |
| 11 | Strict Priority | - | - | - | - | - | - |
| 12 | Strict Priority | - | - | - | - | - | - |

**Port Scheduler**

| Item | Description |
|---|---|
| **Port** | The interface number. |
| **Mode** | The field displays the scheduler mode for this port. |

If you click on the port number, it will display the information of the specific port scheduler and shapers. And you could also configure the scheduler mode here.

- **Scheduler Mode: Strict Priority**

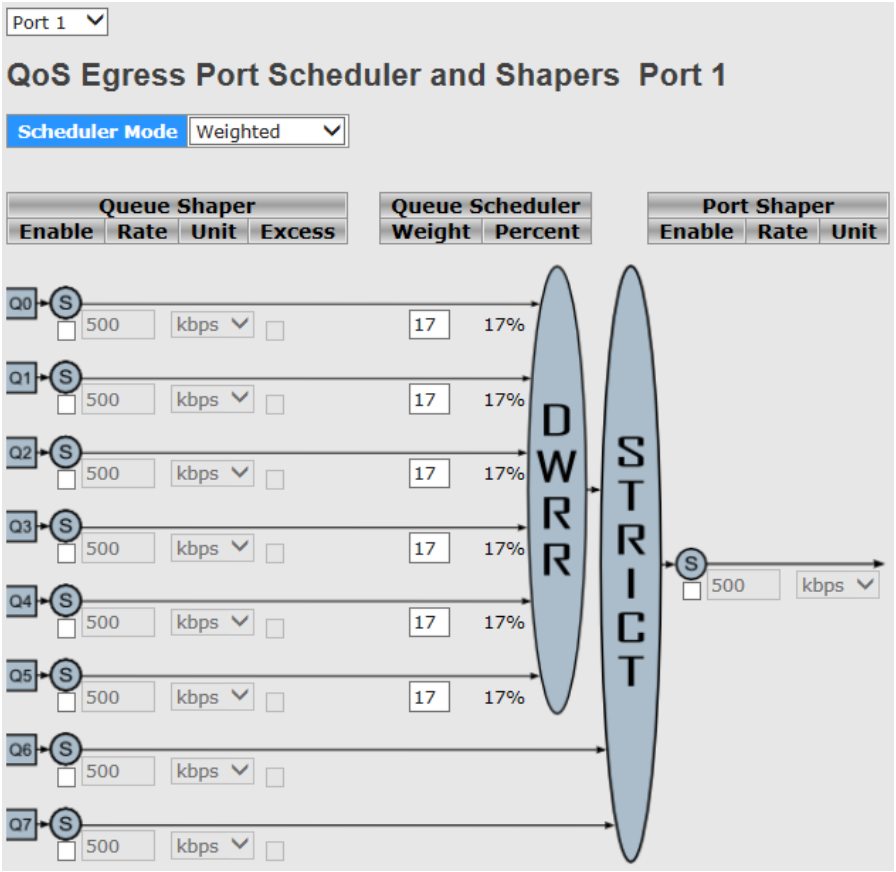



**Scheduler Mode: Strict Priority**

| Description | Factory default |
|---|---|
| **Scheduler Mode** | |
| Specify whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port. | Strict Priority |
| **QueueShaper_Enable** | |
| Controls whether the queue shaper is enabled for this queue on this switch port. | Unchecked |
| **QueueShaper_Rate** | |
| Specify the rate of the queue shaper. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-3300 when the "Unit" is "Mbps" or "kfps". | 500 |
| **QueueShaper_Unit** | |
| Specify the unit of measure for the queue shaper rate as kbps, Mbps, fps or kfps. | kbps |
| **QueueShaper_Excess** | |
| Specify whether the queue is allowed to use excess bandwidth. | Unchecked |

| Description | Factory default |
|---|---|
| **Port Shaper_Enable** | |
| Controls whether the port shaper is enabled or not. | Unchecked |
| **Port Shaper_Rate** | |
| Specify the rate of the port shaper. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-3300 when the "Unit" is "Mbps" or "kfps". | 500 |
| **Port shaper _Unit** | |
| Specify the unit of measure for the port shaper rate as kbps, Mbps, fps or kfps. | kbps |

- **Scheduler Mode: Weighted**




**Scheduler Mode: Weighted**

| Description | Factory default |
|---|---|
| **Scheduler Mode** | |
| Specify whether the scheduler mode is "Strict Priority" or "Weighted" on this switch port. | Strict Priority |
| **QueueShaper_Enable** | |
| Controls whether the queue shaper is enabled for this queue on this switch port. | Unchecked |
| **QueueShaper_Rate** | |
| Specify the rate of the queue shaper. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-3300 when the "Unit" is "Mbps" or "kfps". | 500 |
| **QueueShaper_Unit** | |
| Specify the unit of measure for the queue shaper rate as kbps, Mbps, fps or kfps. | kbps |
| **QueueShaper_Excess** | |
| Specify whether the queue is allowed to use excess bandwidth. | Unchecked |

| Description | Factory default |
|---|---|
| **QueueScheduler_Weight** | |
| Specify the weight for this queue. This value is restricted to 1-100. This parameter is only shown if "Scheduler Mode" is set to "Weighted". | 17 |
| **QueueScheduler_Percent** | |
| This field dispaythe weight in percent for this queue. This parameter is only shown if "Scheduler Mode" is set to "Weighted". | fixed |
| **Port Shaper_Enable** | |
| Specify whether the port shaper is enabled or not. | Unchecked |
| **Port Shaper_Rate** | |
| Specify the rate of the port shaper. This value is restricted to 100-1000000 when the "Unit" is "kbps" or "fps", and it is restricted to 1-3300 when the "Unit" is "Mbps" or "kfps". | 500 |
| **Port shaper _Unit** | |
| Specify the unit of measure for the port shaper rate as kbps, Mbps, fps or kfps. The default value is "kbps". | kbps |



## 3.7.8 Port Shaping

| Port | Shapers | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | Q0 | Q1 | Q2 | Q3 | Q4 | Q5 | Q6 | Q7 | Port |
| 1 | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled |
| 2 | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled |
| 3 | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled |
| 4 | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled |
| 5 | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled |
| 6 | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled |
| 7 | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled |
| 8 | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled |
| 9 | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled |
| 10 | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled |
| 11 | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled |
| 12 | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled | disabled |

**Port Shaping**

| Item | Description |
|---|---|
| Port | The interface number. You could click the port number to configure the shapers. |
| Shapers | The field displays the "disabled" or actual queue shaper rate. |

## 3.7.9 DSCP-Based QoS

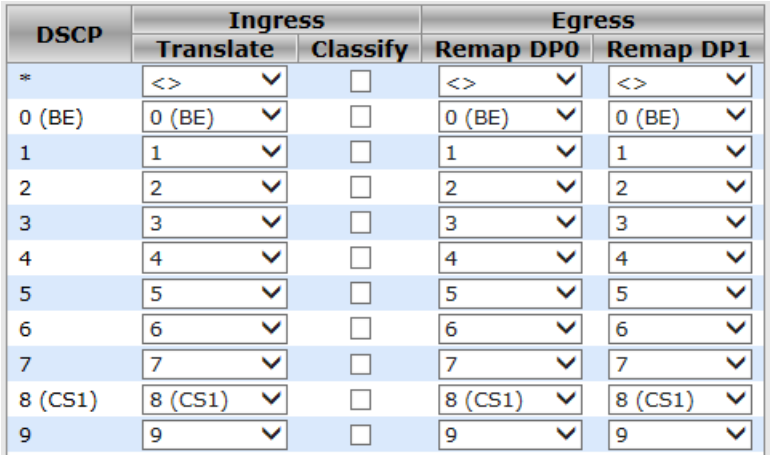
| DSCP | Trust | QoS Class | DPL |
|---|---|---|---|
| * | ☐ | 0 | <> |
| 0 (BE) | ☐ | 0 | 0 |
| 1 | ☐ | 0 | 0 |
| 2 | ☐ | 0 | 0 |
| 3 | ☐ | 0 | 0 |
| 4 | ☐ | 0 | 0 |
| 5 | ☐ | 0 | 0 |
| 6 | ☐ | 0 | 0 |
| 7 | ☐ | 0 | 0 |

**DSCP-Based QoS**

| Description | Factory default |
|---|---|
| **DSCP** | |
| The DSCP number and the maximum value is 64. | interface number |
| **Description** | **Factory default** |
| **Trust** | |
| Specify whether a specific DSCP value is trusted or not.<br>• **Checked**: The trust mode is enabled.<br>• **Unchecked**: The trust mode is disabled. | Unchecked |
| **QoS Class** | |
| Specify the QoS Class.The values are from 0 to 7 | 0 |
| **DPL** | |
| Specify the Drop Percedence Level is 0 or 1. | 0 |



## 3.7.10 DSCP Translation




**DSCP Translation**

| Description | Factory default |
|---|---|
| **DSCP** | |
| The DSCP number and the maximum values are 64. | interface number |
| **Ingress_Translate** | |
| DSCP at Ingress side can be translated to any of (0-63) DSCP values. | interface number |
| **Ingress_Classify** | |
| Specify whether the classification is enabled or not.<br>• **Checked**: The classification is enabled.<br>• **Unchecked**: The classification is disabled. | Unchecked |
| **Egress_Remap DP0** | |
| Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63. | interface number |
| **Egress_Remap DP1** | |
| Select the DSCP value from select menu to which you want to remap. DSCP value ranges from 0 to 63. | interface number |

## 3.7.11 DSCP Classification

This page allows you to configure the mapping of QoS class and Drop Precedence Level to DSCP value.

| QoS Class | DPL | DSCP |
|---|---|---|
| * | * | <> |
| 0 | 0 | 0 (BE) |
| 0 | 1 | 0 (BE) |
| 1 | 0 | 0 (BE) |
| 1 | 1 | 0 (BE) |
| 2 | 0 | 0 (BE) |
| 2 | 1 | 0 (BE) |
| 3 | 0 | 0 (BE) |
| 3 | 1 | 0 (BE) |
| 4 | 0 | 0 (BE) |
| 4 | 1 | 0 (BE) |
| 5 | 0 | 0 (BE) |
| 5 | 1 | 0 (BE) |
| 6 | 0 | 0 (BE) |
| 6 | 1 | 0 (BE) |
| 7 | 0 | 0 (BE) |
| 7 | 1 | 0 (BE) |

**DSCP Classification**

| Description | Factory default |
|---|---|
| **QoS Class** | |
| The QoS class number. | class number |
| **DPL** | |
| Actual Drop Precedence Level. | fixed |
| **DSCP** | |
| Select the classified DSCP value (0-63). | 0 (BE) |

## 3.7.12 QoS Control List

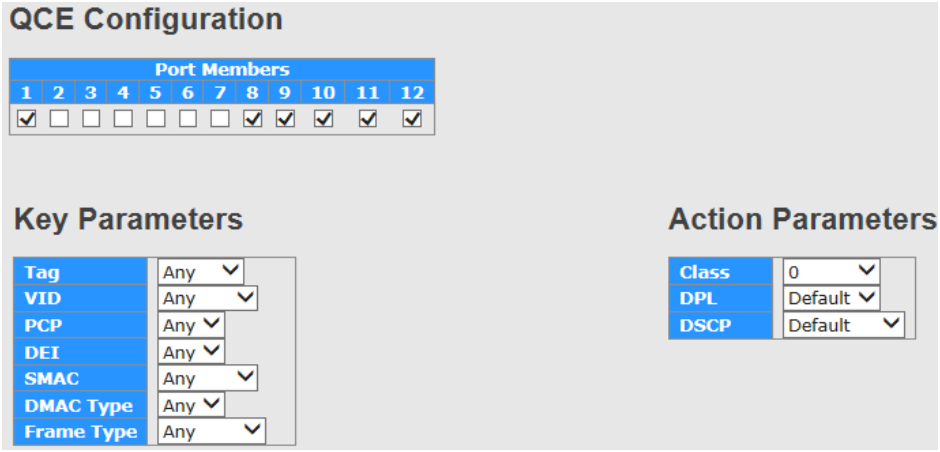
This feature allows you edit or insert a single QoS Control Entry at a time. A QCE consists of several parameters. These parameters vary according to the frame type that you select.

- **QoS Control List**

| QCE# | Port | Frame Type | SMAC | DMAC | VID | PCP | DEI | Action | | |
|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | | | | Class | DPL | DSCP |

You can click the icon to add a QCE, and it will display in the QoS Control List.

- **QoS Control List**



**QCE Configuration**

| Description | Factory default |
|---|---|
| **Port Members** | |
| Select the port to add in the QCL entry.<br>• **Checked**: The port is including in the QCL entry.<br>• **Unchecked**: The port is not including in the QCL entry. | Checked |

**Key Parameters**

| Description | Factory default |
|---|---|
| **Tag** | |
| Specify the Tag mode: 'Any', 'Untag' or 'Tag'. | Any |
| **VID** | |
| Specify the Valid value of VLAN ID in the range 1-4095 or 'Any'; Or you can enter either a specific value or a range of VIDs. | Any |
| **PCP** | |
| Specify the Priority Code Point range.Valid value PCP are specific (0, 1, 2, 3, 4, 5, 6, 7) or in a range (0-1, 2-3, 4-5, 6-7, 0-3, 4-7) or 'Any'. | Any |
| **DEI** | |
| Specify the Drop Eligible Indicator mode. The valid value of DEI can be any of values between 0, 1 or 'Any'. | Any |
| **SMAC** | |
| Source MAC address: 24 MS bits (OUI) or 'Any'. | Any |
| **DMAC type** | |
| Specify the Destination MAC type.<br>• **UC**: In unicast format<br>• **MC**: In multicast format.<br>• **BC**: In broadcast format<br>• **Any**: In any format. | Any |
| **Frame Type** | |
| Specify the frame type as below:<br>• **Any**: Allow all types of frames.<br>• **Ethernet**: Ethernet Type Valid ethernet type can have a value within 0x600-0xFFFF or 'Any' but excluding 0x800(IPv4) and 0x86DD(IPv6)<br>• **LLC**: Include SSAP address, DSAP address and Control Valid.<br>• **SNAP**<br>• **IPv4**<br>• **IPv6** | Any |

**Key Parameter**

| Description | Factory default |
|---|---|
| **Class** | |
| Specify the QoS class range from 0 to 7. | 0 |
| **DPL** | |
| Specify the DPL and the range can be 0 or 1. | Default |
| **DSCP** | |
| Specify the DSCP value. | Default |

## 3.7.13 QoS Statistics

| Port | Q0 | | Q1 | | Q2 | | Q3 | | Q4 | | Q5 | | Q6 | | Q7 | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx | Rx | Tx |
| 1 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 29725 | 15246 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 14143 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 16325 | 9233 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 614 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

You can click on the Port number to check the details.

**QoS Statistics**

| Item | Description |
|---|---|
| **Port** | The interface number. |
| **Queue number** | There are 8 QoS queues per port. Q0 is the lowest priority queue. |
| **Rx** | The number of received packets per queue. |
| **Tx** | The number of transmittd packets per queue. |

## 3.7.14 QCL Status

This page shows the QCL status by different QCL users. Each row describes the QCE that is defined. It is a conflict if a specific QCE is not applied to the hardware due to hardware limitations. The maximum number of QCEs is 256 on each switch.

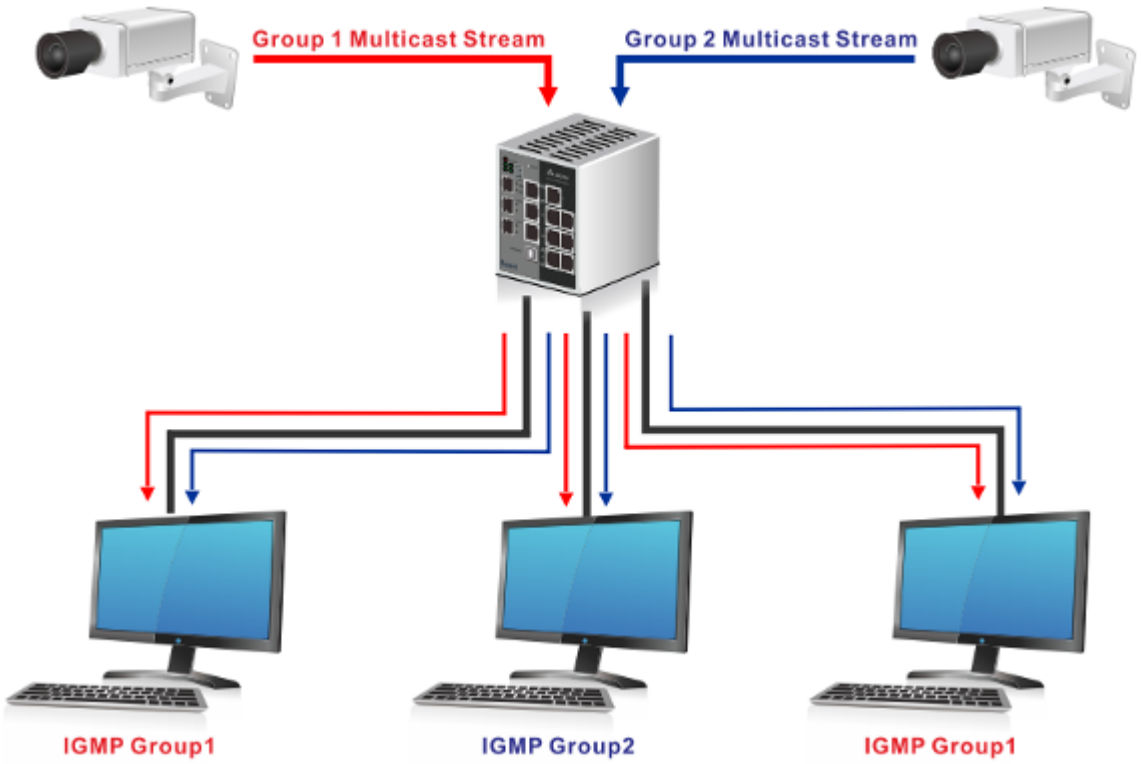

**QCL Status**

| Item | Description |
|---|---|
| **User** | The QCL user name. |
| **QCE#** | The index of QCE |
| **Frame Type** | The type of frame type. |
| **Port** | The port list of the QCE entry. |
| **Action** | The classification action taken on ingress frame if parameters configured are matched with the frame's content.<br>• **Class**: Classified QoS class; if a frame matches the QCE it will be put in the queue.<br>• **DPL**: Drop Precedence Level; if a frame matches the QCE then DP level will set to value displayed under DPL column.<br>• **DSCP**: If a frame matches the QCE then DSCP will be classified with the value displayed under DSCP column. |
| **Conflict** | Displays Conflict status of QCL entries. As H/W resources are shared by multiple applications. It may happen that resources required to add a QCE may not be available, in that case it shows conflict status as 'Yes', otherwise it is always 'No'. Please note that conflict can be resolved by releasing the H/W resources required to add QCL entry on pressing 'Resolve Conflict' button. |

## 3.8 Multicast

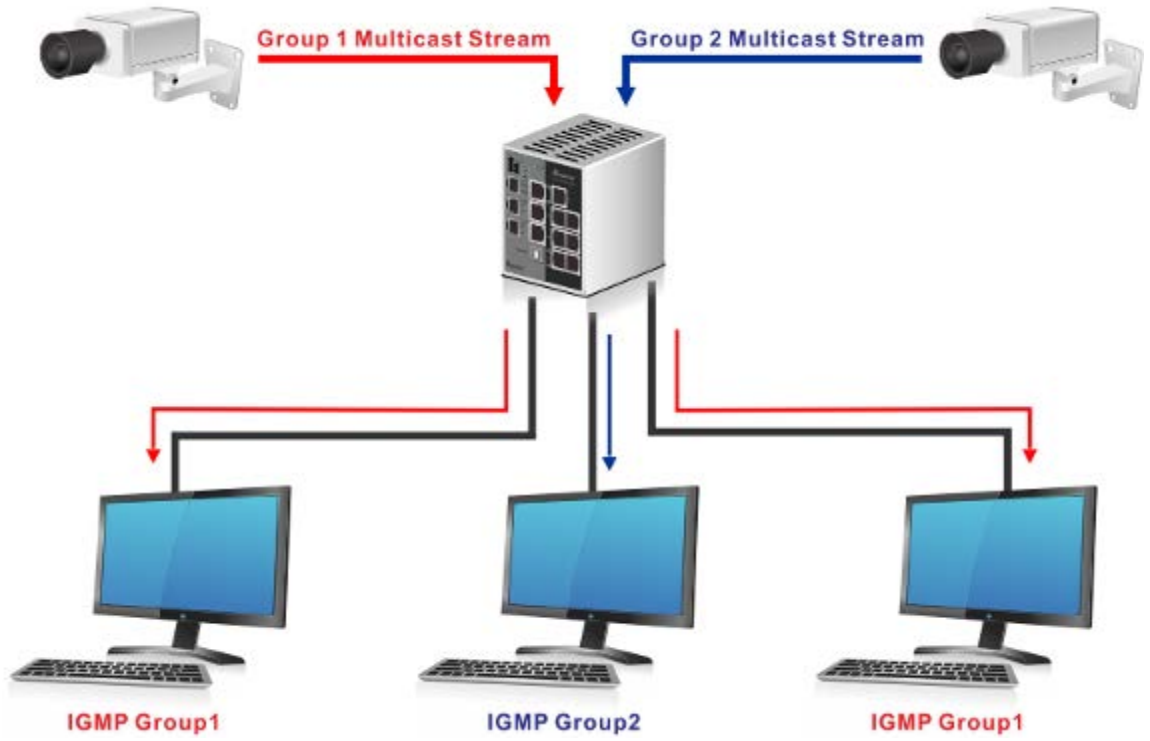
Multicast IP traffic is traffic that is assigned to a host group. Host groups are identified by class D IP addresses, which range from 224.0.0.0 to 239.255.255.255. A multicast IP packet is only sent by one host to multiple hosts. Only those hosts that belong to a specific multicast group will receive the multicast. The Internet Group Management Protocol (IGMP) snooping enables the switch to forward multicast traffic intelligently to only the interface that requests the multicast traffic. So the network resource is not wasted too much.
If there is a network without the multicast filtering, and a host needs to send data to many hosts, then it needs to produce several copies in the network. It wastes too much network bandwidth. If there is a network with the multicast filtering, then it reduces the load of resources (ex. a server) and makes the network bandwidth efficient. The figures below show the difference between the network without Multicast Filtering and the network with Multicast Filtering.

**Network without Multicast Filtering:**




**(All hosts receive the multicast traffic.)**

**Network with Multicast Filtering:**




**(Only the host which belongs to the group can receive the traffic.)**

IGMP Snooping manages multicast traffic by making use of switches, routers, and hosts that support IGMP. Enabling IGMP Snooping allows the ports to detect the IGMP queries, report packets, and manage multicast traffic through the switch. IGMP has three fundamental types of messages, as shown below:

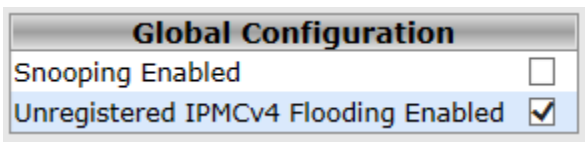
| Item | Description |
|---|---|
| **Query** | A message is sent from the querier (an IGMP router or a switch) which asks for a response from each host that belongs to the multicast group. |
| **Report** | A message is sent by a host to the querier to indicate that the host wants to be or is a member of a given group indicated in the report message. |
| **Leave Group** | A message is sent by a host to the querier to indicate that the host has quit as a member of a specific multicast group. |

## 3.8.1 IGMP Snooping

On this page, you can enable or disable IGMP Snooping. And it displays the VLAN which enables the IGMP Snooping function.

### 3.8.1.1 Basic Configuration

- **Global Configuration**



**Global Configuration**

| Description | Factory default |
|---|---|
| **Snooping Enabled** | |
| Specify the status of IGMP Snooping:<br>• **Unchecked:** The IGMP Snooping is disabled. The IGMP setting still can be configured, but the settings do not take effect after you have applied them.<br>• **Checked:** The IGMP Snooping is enabled. The switch snoop all the IGMP packets it receives to determine which segments should receive the packets directed to the group address. | Unchecked |
| **Unregistered IPMCv4 Flooding Enabled** | |
| Specify the status of unregistered IPMC traffic flooding:<br>• **Unchecked:** The unregistered IPMC traffic flooding is disabled.<br>• **Checked:** The unregistered IPMC traffic flooding is enabled. | Checked |

- **Port Related Configuration**

| Port | Router Port | Fast Leave |
|---|---|---|
| * | ☐ | ☐ |
| 1 | ☐ | ☐ |
| 2 | ☐ | ☐ |
| 3 | ☐ | ☐ |
| 4 | ☐ | ☐ |
| 5 | ☐ | ☐ |
| 6 | ☐ | ☐ |
| 7 | ☐ | ☐ |
| 8 | ☐ | ☐ |
| 9 | ☐ | ☐ |
| 10 | ☐ | ☐ |
| 11 | ☐ | ☐ |
| 12 | ☐ | ☐ |

**Port Related Configuration**

| Description | Factory default |
|---|---|
| **Port** | |
| The port number. | *port number* |
| **Router Port** | |
| Specify which ports act as router ports. A router port is a port on the Ethernet switch that leads towards the Layer 3 multicast device or IGMP querier.<br>If an aggregation member port is selected as a router port, the whole aggregation will act as a router port.<br>• **Unchecked:** The port doesn't act as router port.<br>• **Checked:** The port act as router port. | Unchecked |
| **Fast Leave** | |
| Specify the status of the port.<br>• **Unchecked:** The port is disabled.<br>• **Checked:** The port is enabled. | Unchecked |

### 3.8.1.2 VLAN Configuration

You can use "Add new IGMP VLAN" to create a new IGMP VLAN entry.

| Delete | VLAN ID | Snooping Enabled | IGMP Querier |
|---|---|---|---|
| Delete | | ☐ | ☑ |

Add New IGMP VLAN

**VLAN Configuration**

| Description | Factory default |
|---|---|
| **VLAN ID** | |
| Enter a VLAN ID for which you want to create an IGMP snooping configuration. | None |
| **Snooping Enabled** | |
| Specify the status of per-VLAN IGMP Snooping. Up to 32 VLANs can be selected for IGMP Snooping.<br>• **Unchecked:** The status is disabled.<br>• **Checked:** The status is enabled. | Unchecked |
| **IGMP Querier** | |
| Specify the status of IGMP Querier in the VLAN.<br>• **Unchecked:** The status is disabled.<br>• **Checked:** The status is enabled. | Checked |

3

### 3.8.1.3 Status

- **Statistics**

| VLAN ID | Querier Version | Host Version | Querier Status | Queries Transmitted | Queries Received | V1 Reports Received | V2 Reports Received | V3 Reports Received | V2 Leaves Received |
|---|---|---|---|---|---|---|---|---|---|

**Statistics**

| Item | Description |
|---|---|
| **VLAN ID** | The VLAN ID of the entry. |
| **Querier Version** | Working Querier Version currently. |
| **Host Version** | Working Host Version currently. |
| **Querier Status** | Show the Querier status is "ACTIVE" or "IDLE". |
| **Querier Receive** | The number of Transmitted Querier. |
| **V1 Reports Receive** | The number of Received V1 Reports. |
| **V2 Reports Receive** | The number of Received V2 Reports. |
| **V3 Reports Receive** | The number of Received V3 Reports. |
| **V2 Leave Receive** | The number of Received V2 Leave. |

- **Router Port**

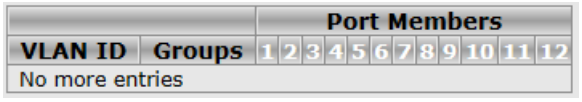
| Port | Status |
|---|---|
| 1 | - |
| 2 | - |
| 3 | - |
| 4 | - |
| 5 | - |
| 6 | - |
| 7 | - |
| 8 | - |
| 9 | - |
| 10 | - |
| 11 | - |
| 12 | - |

**Statistics**

| Item | Description |
|---|---|
| **Port** | The port number. |
| **Status** | Indicate whether specific port is a router port or not. |

#### 3.8.1.4 Group Information

Entries in the IGMP Group Table are shown on this page. The IGMP Group Table is sorted first by VLAN ID, and then by group.




**Group Information**

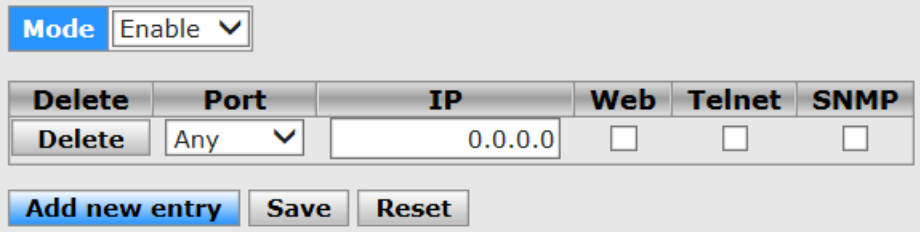
| Item | Description |
|---|---|
| **VLAN ID** | VLAN ID of the group. |
| **Groups** | Group address of the group displayed. |
| **Port Members** | Ports under this group. |

## 3.9 Security

This group allows you to configure a MAC address, an IP address or the Port authentication to reach the security purpose.

### 3.9.1 Remote Control Security

Remote Control Security allows you limit the remote access of management interface. When enabled, the request of client which is not in the allow list will be rejected.
You can enable the mode first, and then click"Add new entry" to add a new role.




**Remote Control Security**

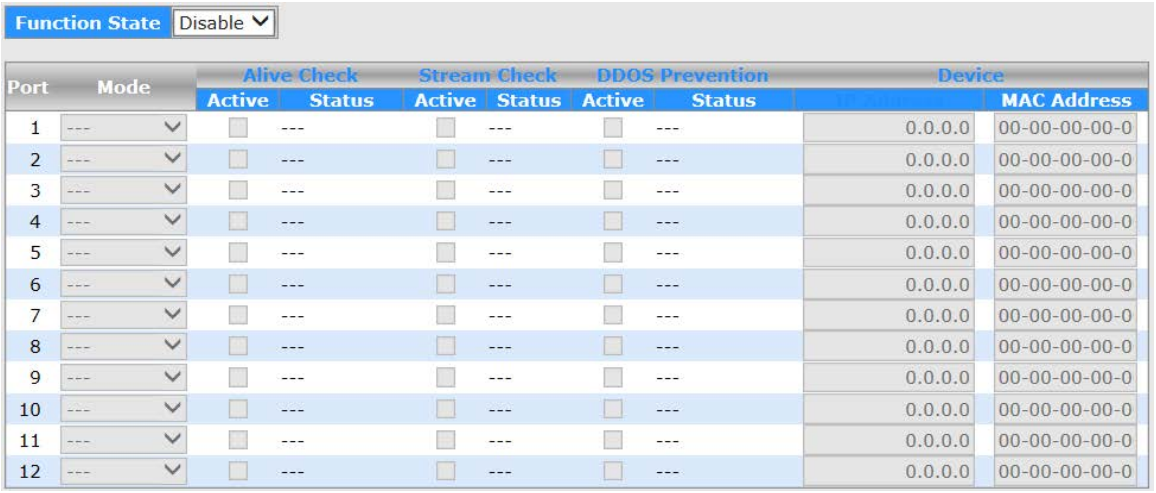
| Description | Factory default |
|---|---|
| **Port** | |
| Port number of remote client. | Any |
| **IP** | |
| IP address of remote client. Keeps this field "0.0.0.0" means "Any IP". | Unchecked |
| **Web** | |
| Specify the status of web management interface<br>• **Unchecked:** The status is disabled.<br>• **Checked:** The status is enabled. | Unchecked |
| **Telnet** | |
| Specify the status of telnet management interface.<br>• **Unchecked:** The status is disabled.<br>• **Checked:** The status is enabled. | Unchecked |
| **SNMP** | |
| Specify the status of SNMP management interface.<br>• **Unchecked:** The status is disabled.<br>• **Checked:** The status is enabled. | Unchecked |

### 3.9.2 Device Binding

This group provides Device Binding related configuration. Device Binding is an powerful monitor for devices and network security.

#### 3.9.2.1 Configuration

The configuration will be activated after the Function State enabled.




**Configuration**

| Description | Factory default |
|---|---|
| **Mode** | |
| Specify the Device Binding operatin mode of the specific port.<br>• **Scan:** Scan IP/MAC automatically, but no binding function.<br>• **Binding**: Any IP/MAC doesn't match the entry will not be allowed to access the network<br>• **Shutdown**: Shutdown the port (No Link) | None |
| **Alive Check_Active** | |
| Specify the status of Alive Check.<br>• **Unchecked:** The status is disabled.<br>• **Checked:** The status is enabled.<br>**Note:**<br>It only can specify when the Device Binding mode is “Binding” mode. | Unchecked |
| **Alive Check_Status** | |
| Display the Alive Check status.<br>• **---**: Disable.<br>• Got Reply: Got ping reply from device, that means the device is still alive.<br>• Lost Reply: Lost ping reply from device, that means the device might have been hanged | --- |
| **Stream Check_Active** | |
| Specify the status of Stream Check.<br>• **Unchecked:** The status is disabled.<br>• **Checked:** The status is enabled.<br>**Note:**<br>It only can specify when the Device Binding mode is “Binding” mode. | Unchecked |
| **Alive Check_Status** | |
| Display the Stream Check status.<br>• **---**: Disable. | --- |

| Description | Factory default |
|---|---|
| • Normal: The stream is normal.<br>• Low: The stream is getting low. | |
| **DDOS Prevention_Active** | |
| Specify the status of DDOS Prevention.<br>• **Unchecked:** The status is disabled.<br>• **Checked:** The status is enabled.<br>**Note:**<br>It only can specify when the Device Binding mode is “Binding” mode. | Unchecked |
| **DDOS Prevention _Status** | |
| Display the DDOS Prevention status.<br>• **---**: Disable.<br>• Analysing: Analysing the packet throughput for initialization.<br>• Running: Function ready.<br>• Attacked: DDOS attack happened. | --- |
| **IP Address** | |
| Specify the IP Address of device. | 0.0.0.0 |
| **MAC Address** | |
| Specify the MAC Address of device. | 00:00:00:00:00:00 |

### 3.9.2.2 Advanced Configuration

- **Alias IP Address**

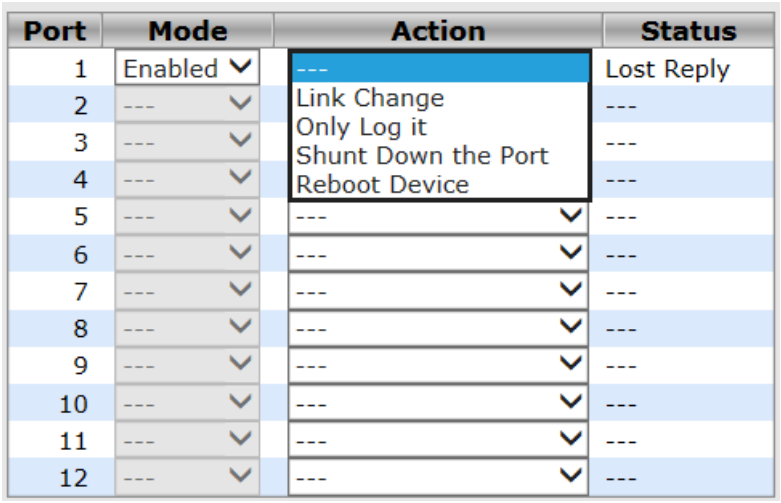
| Port | Alias IP Address |
|---|---|
| 1 | 0.0.0.0 |
| 2 | 0.0.0.0 |
| 3 | 0.0.0.0 |
| 4 | 0.0.0.0 |
| 5 | 0.0.0.0 |
| 6 | 0.0.0.0 |
| 7 | 0.0.0.0 |
| 8 | 0.0.0.0 |
| 9 | 0.0.0.0 |
| 10 | 0.0.0.0 |
| 11 | 0.0.0.0 |
| 12 | 0.0.0.0 |

**Alias IP Address**

| Description | Factory default |
|---|---|
| **Port** | |
| The interface number | *interface number* |
| **Alias IP Address** | |
| Specify Alias IP address. Keeps "0.0.0.0", if the device doesn't have alias IP address. | 0.0.0.0 |

- **Alive Check**

The information will relate with the Device Binding Configuration.



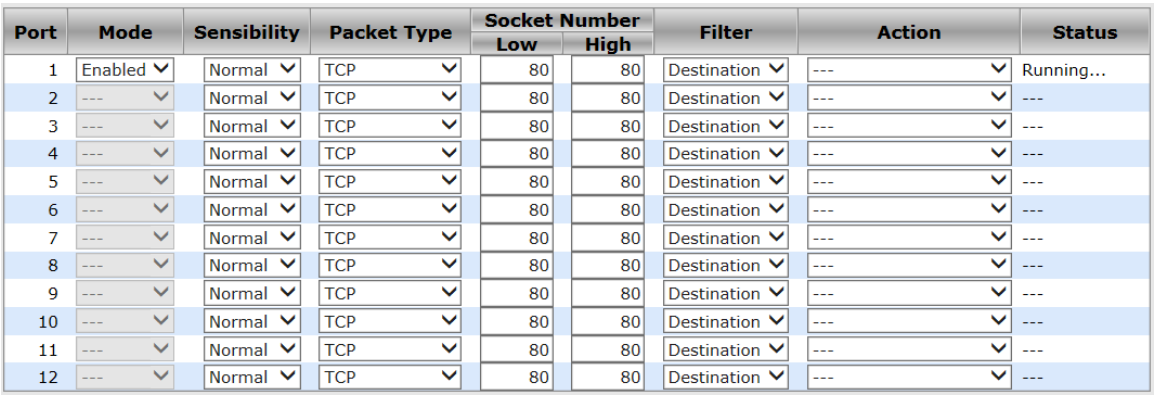

3

**Alive Check**

| Description | Factory default |
|---|---|
| **Port** | |
| The interface number | *interface number* |
| **Mode** | |
| This field displays the status of Alive Check in Device Binding Configuration. | Fixed |
| **Action** | |
| Specify the action of Alive check.<br>• **Link Change**: Disable and enable port<br>• **Only Log it**: Only sent log to log server.<br>• **Shut Down the Port**: Disable this port.<br>• **Reboot Device**: Disable and Enable P.o.E Power | --- |
| **Status** | |
| This field displays the Alive Check Status. | Fixed |

- **DDOS Prevention**

The information will relate with the Device Binding Configuration.




**DDOS Prevention**

| Description | Factory default |
|---|---|
| **Port** | |
| The interface number | *interface number* |
| **Mode** | |
| This field displays the status of Alive Check in Device Binding Configuration. | Fixed |

| Description | Factory default |
|---|---|
| **Sensibility** | |
| Specify the level of DDOS detection.<br>• **Low**: Low sensibility.<br>• **Normal**: Normal sensibility.<br>• **Medium**: Medium sensibility.<br>• **High**: High sensibility. | Normal |
| **Packet Type** | |
| Specify the packet of DDOS monitor.<br>• **RX Total**: Total ingress packets.<br>• **RX Unicast**: Unicast ingress packets.<br>• **RX Multicast**: Multicast ingress packets<br>• **RX Broadcast**: Broadcast ingress packets.<br>• **TCP**: TCP ingress packets.<br>• **UDP**: UDP ingress packets. | TCP |
| **Socket Number** | |
| If packet type is UDP or TCP, please specify the socket number here. The socket number could be a range, from low to high. If the socket number is only one, please fill the same number in low field and high field. | Low:80<br>High:80 |
| **Filter** | |
| If packet type is UDP or TCP, please choose the socket direction (Destination/Source). | Destination |
| **Action** | |
| Specify the action when DDOS attack happened.<br>• **---**: Do nothing.<br>• **Blocking 1 minute**: To block the forwarding for 1 mintue, and log the event.<br>• **Blocking 10 minute**: To block the forwarding for 10 mintues, and log the event.<br>• **Blocking**: Just blocking, and log the event<br>• **Shunt Down the Port**: Shut down the port(No Link), and log the event.<br>• **Only Log it**: Just log the event.<br>• **Reboot Device**: If PoE supported, the device could be rebooted. And log the event. | --- |
| **Status** | |
| This field displays the status of DDOS Prevention.<br>• **---**: Disable.<br>• **Analysing**: Analysing the packet throughput for initialization.<br>• **Running**: Function ready.<br>• **Attacked**: DDOS attack happened. | Fixed |

- **Device Description**

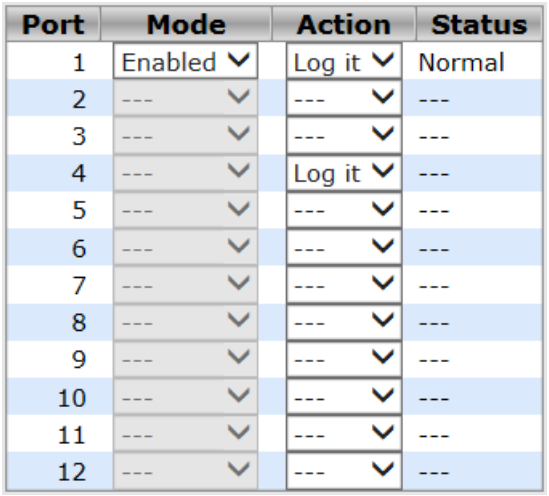
| Port | Device | | |
|---|---|---|---|
| | Type | Location Address | Description |
| 1 | --- | | |
| 2 | --- | | |
| 3 | --- | | |
| 4 | --- | | |
| 5 | --- | | |
| 6 | --- | | |
| 7 | --- | | |
| 8 | --- | | |
| 9 | --- | | |
| 10 | --- | | |
| 11 | --- | | |
| 12 | --- | | |

**Device Description**

| Description | Factory default |
|---|---|
| **Port** | |
| The interface number | *interface number* |
| **Type** | |
| Specify the type of device. | --- |
| **Location Address** | |
| Entering the Location information of device, this information could be used for Google Mapping. | None |
| **Description** | |
| Entering the Device description. | None |

3

- **Stream Check**




**Stream Check**

| Description | Factory default |
|---|---|
| **Port** | |
| The interface number | *interface number* |
| **Mode** | |
| This field displays the status of Alive Check in Device Binding Configuration. | Fixed |
| **Action** | |
| Specify the action of Alive check.<br>• **---**: Do nothing.<br>• **Log it**: Just log the event. | --- |
| **Status** | |
| This field displays the Stream Check status. | Fixed |

### 3.9.3 ACL

Access control lists (ACLs) can make sure that only authorized devices have access to specific resources when any unauthorized devices which are blocked attempt to access network resources. ACLs provide security for the network, traffic flow control, and determine which types of traffic can be forwarded or blocked.
A Delta switch supports ACLs based on the MAC addresses of the source and destination devices (MAC ACLs).

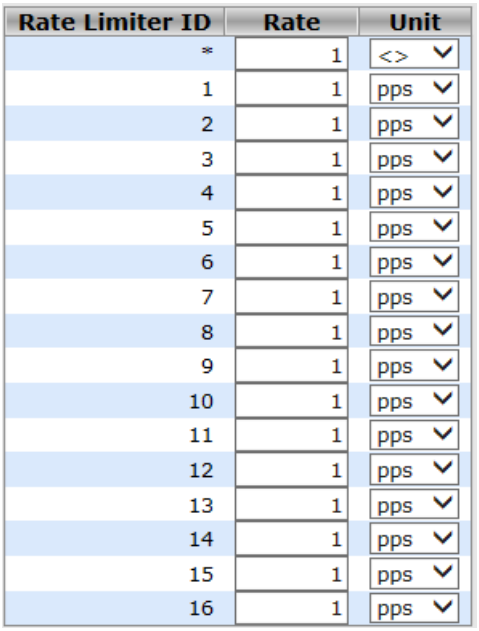
### 3.9.3.1 Ports

| Port | Policy ID | Action | Rate Limiter ID | Port Redirect | Mirror | Logging | Shutdown | State | Counter |
|---|---|---|---|---|---|---|---|---|---|
| * | 0 | <> | <> | Disabled / Port 1 / Port 2 | <> | <> | <> | <> | * |
| 1 | 0 | Permit | Disabled | Disabled / Port 1 / Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |
| 2 | 0 | Permit | Disabled | Disabled / Port 1 / Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |
| 3 | 0 | Permit | Disabled | Disabled / Port 1 / Port 2 | Disabled | Disabled | Disabled | Enabled | 41707 |
| 4 | 0 | Permit | Disabled | Disabled / Port 1 / Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |
| 5 | 0 | Permit | Disabled | Disabled / Port 1 / Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |
| 6 | 0 | Permit | Disabled | Disabled / Port 1 / Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |
| 7 | 0 | Permit | Disabled | Disabled / Port 1 / Port 2 | Disabled | Disabled | Disabled | Enabled | 16325 |
| 8 | 0 | Permit | Disabled | Disabled / Port 1 / Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |
| 9 | 0 | Permit | Disabled | Disabled / Port 1 / Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |
| 10 | 0 | Permit | Disabled | Disabled / Port 1 / Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |
| 11 | 0 | Permit | Disabled | Disabled / Port 1 / Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |
| 12 | 0 | Permit | Disabled | Disabled / Port 1 / Port 2 | Disabled | Disabled | Disabled | Enabled | 0 |

**Ports Configuration**

| Description | Factory default |
|---|---|
| **Port** | |
| The interface number. | *interface number* |
| **Policy ID** | |
| Entering the policy to apply to this port. The allowed values are 1 through 8. The default value is 1. | 0 |
| **Action** | |
| Specify the forwarding rule as Permit or Deny. | Permit |
| **Rate Limiter ID** | |
| Specify which rate limiter to apply to this port. The values 1 through 15. | Disabled |
| **Port Redirect** | |
| Specify the port to redirect. The range is from Port1 to Port 12. | Disabled |
| **Mirror** | |
| Specify the destination port or the monitored interface. | Disabled |
| **Logging** | |
| Specify the logging operation of this port.<br>• **Enabled**: Frames received on the port are stored in the System Log.<br>• **Disabled:** Frames received on the port are not logged. | Disabled |
| **Shutdown** | |
| Specify the logging operation of this port.<br>• **Enabled**: If a frame is received on the port, the port will be disabled.<br>• **Disabled:** Port shut down is disabled. | Disabled |

### 3.9.3.2 Rate Limit



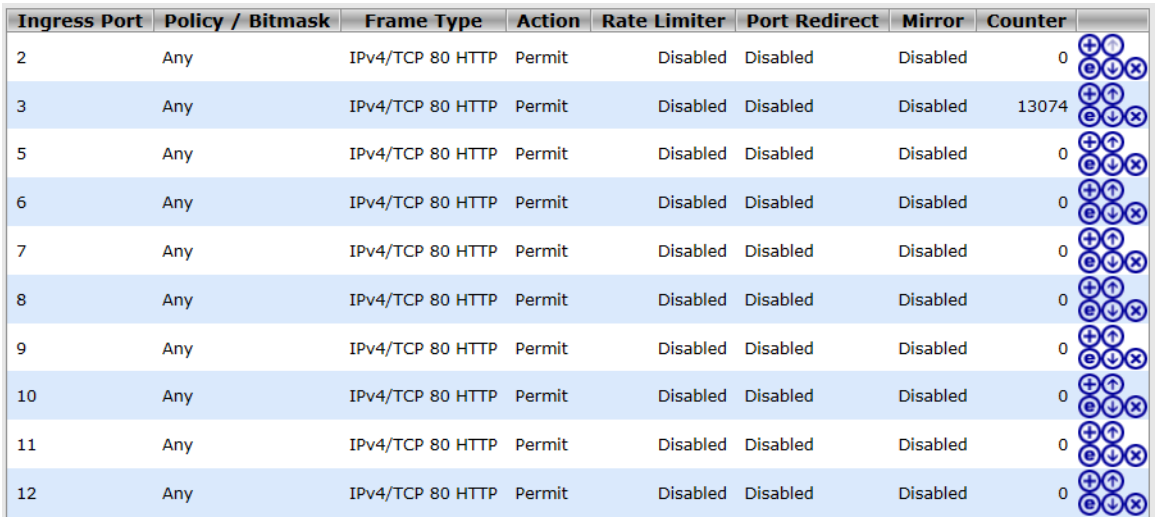
| Rate Limiter ID | Rate | Unit |
|---|---|---|
| * | 1 | <> |
| 1 | 1 | pps |
| 2 | 1 | pps |
| 3 | 1 | pps |
| 4 | 1 | pps |
| 5 | 1 | pps |
| 6 | 1 | pps |
| 7 | 1 | pps |
| 8 | 1 | pps |
| 9 | 1 | pps |
| 10 | 1 | pps |
| 11 | 1 | pps |
| 12 | 1 | pps |
| 13 | 1 | pps |
| 14 | 1 | pps |
| 15 | 1 | pps |
| 16 | 1 | pps |

**Rate Limit**

| Description | Factory default |
|---|---|
| **Rate Limiter ID** | |
| The Rate Limiter ID number. | *ID number* |
| **Rate** | |
| The rate unit is packet per second (pps), configure the rate as 1, 2, 4, 8, 16, 32, 64, 128, 256, 512, 1K, 2K, 4K, 8K, 16K, 32K, 64K, 128K, 256K, 512K, or 1024K. | 1 |
| **Unit** | |
| Specify the unit of measure for the rate limit as pps or kbps. | pps |

### 3.9.3.3 Access Control List

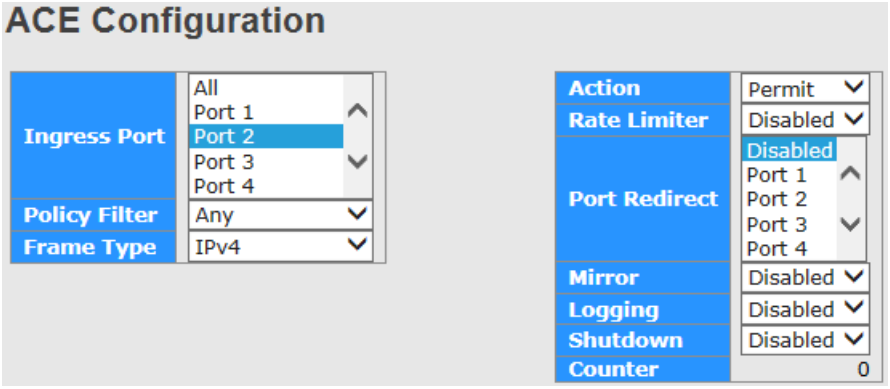
This feature displays the Access Control List, and you can click the edit icon to configure the parameters to the specific ingress port.



| Ingress Port | Policy / Bitmask | Frame Type | Action | Rate Limiter | Port Redirect | Mirror | Counter | |
|---|---|---|---|---|---|---|---|---|
| 2 | Any | IPv4/TCP 80 HTTP | Permit | Disabled | Disabled | Disabled | 0 | |
| 3 | Any | IPv4/TCP 80 HTTP | Permit | Disabled | Disabled | Disabled | 13074 | |
| 5 | Any | IPv4/TCP 80 HTTP | Permit | Disabled | Disabled | Disabled | 0 | |
| 6 | Any | IPv4/TCP 80 HTTP | Permit | Disabled | Disabled | Disabled | 0 | |
| 7 | Any | IPv4/TCP 80 HTTP | Permit | Disabled | Disabled | Disabled | 0 | |
| 8 | Any | IPv4/TCP 80 HTTP | Permit | Disabled | Disabled | Disabled | 0 | |
| 9 | Any | IPv4/TCP 80 HTTP | Permit | Disabled | Disabled | Disabled | 0 | |
| 10 | Any | IPv4/TCP 80 HTTP | Permit | Disabled | Disabled | Disabled | 0 | |
| 11 | Any | IPv4/TCP 80 HTTP | Permit | Disabled | Disabled | Disabled | 0 | |
| 12 | Any | IPv4/TCP 80 HTTP | Permit | Disabled | Disabled | Disabled | 0 | |

- **ACE Configuration**

An ACE consists of several parameters. These parameters vary according to the frame type that you select. First select the ingress port for the ACE, and then select the frame type. Different parameter options are displayed depending on the frame type that you selected. A frame that hits this ACE matches the configuration that is defined here.




**ACE Configuration**

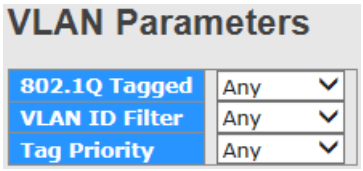
| Description | Factory default |
|---|---|
| **Ingress Port** | |
| Specify the ingress port for which this ACE applies.<br>• **All**: The ACE applies to any port.<br>• **Port number**: The ACE applies to the specific port number. | None |
| **Policy Filter** | |
| Specify the policy filter. | Any |
| **Frame Type** | |
| Specify the frame type for this ACE.<br>• **Any**: Any frame can match this ACE.<br>• **Ethernet Type**: Only Ethernet Type frames can match this ACE.<br>• **ARP**: Only ARP frames can match this ACE.<br>• **IPv4**: Only IPv4 frames can match this ACE. | IPv4 |
| **Action** | |
| Specify the action to take with a frame that hits this ACE.<br>• **Permit**: The frame that hits this ACE is granted permission for the ACE operation.<br>• **Deny**: The frame that hits this ACE is dropped. | Permit |
| **Rate Limiter** | |
| Specify the rate limiter in number of base units. The allowed range is 1 to 15. Disabled indicates that the rate limiter operation is disabled. | Disabled |
| **Port Redirect** | |
| Specify the port to redirect. The range is from Port1 to Port 12. | Disabled |
| **Mirror** | |
| Specify the destination port or the monitored interface. | Disabled |
| **Logging** | |
| Specify the logging operation of this port.<br>• **Enabled**: Frames received on the port are stored in the System Log.<br>• **Disabled:** Frames received on the port are not logged. | Disabled |
| **Shutdown** | |
| Specify the logging operation of this port.<br>• **Enabled**: If a frame is received on the port, the port will be disabled.<br>• **Disabled:** Port shut down is disabled. | Disabled |
| **Counter** | |
| Display the number of times the ACE was hit by a frame. | Fixed |

- **MAC Parameters**


**MAC Parameters**

| Description | Factory default |
|---|---|
| **DMAC filter** | |
| Specify the Destination MAC filter type.<br>• **Any**: In any format.<br>• **MC**: In multicast format.<br>• **BC**: In broadcast format<br>• **UC**: In unicast format | Any |

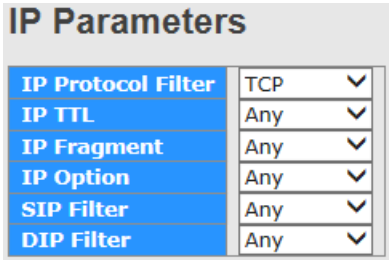
- **VLAN Parameters**




**VLAN Parameters**

| Description | Factory default |
|---|---|
| **802.1Q Tagged** | |
| Specify the 802.1Q status.<br>• **Any**: In any format.<br>• **Disabled**: Disabled the 802.1Q tagged function.<br>• **Enabled**: Enabled the 802.1Q tagged function. | Any |
| **VLAN ID Filter** | |
| Specify the VLAN ID filter for this ACE.<br>• **Any**: No VLAN ID filter is specified. (VLAN ID filter status is "don't-care".)<br>• **Specific**: If you want to filter a specific VLAN ID with this ACE, choose this value. A field for entering a VLAN ID number appears. | Any |
| **Tag Priority** | |
| Specify the tag priority for this ACE. A frame that hits this ACE matches this tag priority. The allowed number range is 0 to 7. The value Any means that no tag priority is specified (tag priority is "don't-care".) | Any |

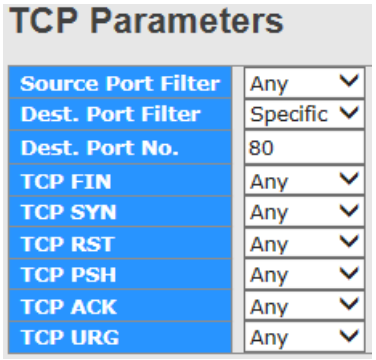
- **IP Parameters**



**IP Parameters**

| Description | Factory default |
|---|---|
| **IP Protocol Filter** | |
| Specify the IP protocol filter for this ACE.<br>• **Any**: No IP protocol filter is specified ("don't-care").<br>• **Specific**: A field for entering an IP protocol filter appears<br>• **ICMP**: Select ICMP to filter IPv4 ICMP protocol frames.<br>• **UDP**: Select UDP to filter IPv4 UDP protocol frames.<br>• **TCP**: Select TCP to filter IPv4 TCP protocol frames. | TCP |
| **IP TTL** | |
| Specify the Time-to-Live settings for this ACE.<br>• **Any**: Any value is allowed ("don't-care").<br>• **Zero**: IPv4 frames with a Time-to-Live field greater than zero must not be able to match this entry.<br>• **non-zero**: IPv4 frames with a Time-to-Live field greater than zero must be able to match this entry. | Any |
| **IP Fragment** | |
| Specify the fragment offset settings for this ACE. This involves the settings for the More Fragments (MF) bit and the Fragment Offset (FRAG OFFSET) field for an IPv4 frame.<br>• **Any**: Any value is allowed ("don't-care").<br>• **Yes**: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must be able to match this entry.<br>• **No**: IPv4 frames where the MF bit is set or the FRAG OFFSET field is greater than zero must not be able to match this entry. | Any |
| **IP Option** | |
| Specify the options flag setting for this ACE.<br>• **Any**: Any value is allowed ("don't-care").<br>• **Yes**: IPv4 frames where the options flag is set must be able to match this entry.<br>• **No**: IPv4 frames where the options flag is set must not be able to match this entry. | Any |
| **SIP Filter** | |
| Specify the source IP filter for this ACE.<br>• **Any**: No source IP filter is specified. (Source IP filter is "don't-care".).<br>• **Host**: Source IP filter is set to Host. Specify the source IP address in the SIP Address field that appears.<br>• **Network**: Source IP filter is set to Network. Specify the source IP address and source IP mask in the SIP Address and SIP Mask fields that appear. | Any |

- **TCP Parameters**



**TCP Parameters**

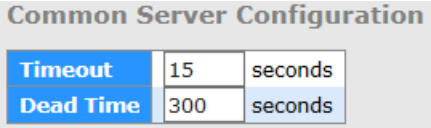
| Description | Factory default |
|---|---|
| **Source Port Filter** | |
| Specify the TCP source filter for this ACE.<br>• **Any**: No TCP/UDP source filter is specified (TCP source filter status is "don't-care").<br>• **Specific**: A field for entering a TCP source value.<br>• **Range**: A field for entering a range of TCP source value. | Any |
| **Dest.Port Filter** | |
| Specify the TCP destination filter for this ACE.<br>• **Any**: No TCP/UDP source filter is specified (TCP source filter status is "don't-care").<br>• **Specific**: A field for entering a TCP source value.<br>• **Range**: A field for entering a range of TCP source value. | Specific |
| **Dest. Port No.** | |
| Enter a specific TCP/UDP destination value. The allowed range is 0 to 65535. A frame that hits this ACE matches this TCP destination value. | 80 |
| **TCP FIN** | |
| Specify the TCP "No more data from sender" (FIN) value for this ACE.<br>• **Any**: Any value is allowed ("don't-care").<br>• **0**: TCP frames where the FIN field is set must not be able to match this entry.<br>• **1**: TCP frames where the FIN field is set must be able to match this entry. | Any |
| **TCP SYN** | |
| Specify the TCP "Synchronize sequence numbers" (SYN) value for this ACE.<br>• **Any**: Any value is allowed ("don't-care").<br>• **0**: TCP frames where the SYN field is set must not be able to match this entry.<br>• **1**: TCP frames where the SYN field is set must be able to match this entry. | Any |
| **TCP PSH** | |
| Specify the TCP "Push Function" (PSH) value for this ACE.<br>• **Any**: Any value is allowed ("don't-care").<br>• **0**: TCP frames where the PSH field is set must not be able to match this entry.<br>• **1**: TCP frames where the PSH field is set must be able to match this entry. | Any |
| **TCP ACK** | |
| Specify the TCP Acknowledgment field significant" (ACK) value for this ACE.<br>• **Any**: Any value is allowed ("don't-care").<br>• **0**: TCP frames where the ACK field is set must not be able to match this entry.<br>• **1**: TCP frames where the ACK field is set must be able to match this entry. | Any |
| **TCP URG** | |
| Specify the TCP Urgent Pointer field significant" (URG) value for this ACE.<br>• **Any**: Any value is allowed ("don't-care").<br>• **0**: TCP frames where the URG field is set must not be able to match this entry.<br>• **1**: TCP frames where the URG field is set must be able to match this entry. | Any |

### 3.9.4 AAA

RADIUS (Remote Authentication Dial In User Service) is a networking protocol that provides the centralized Authentication, Authorization, and Accounting (AAA) management for computers to connect and use a network service. The system implements the RADIUS client and provides the authentication functionality. RADIUS uses UDP port 1812 by default.

### 3.9.4.1 AAA

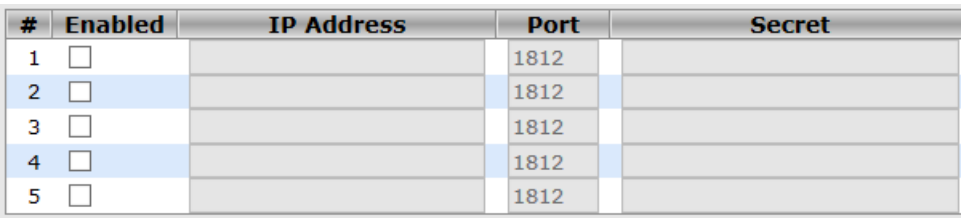
- **Common Server Configuration**




**Common Server Configuration**

| Description | Factory default |
|---|---|
| **Timeout** | |
| Entering the timeout value and the range is 3 to 3600 seconds. | Any |
| **Dead Time** | |
| Entering the timeout value and the range is 3 to 3600 seconds, is the period during which the switch will not send new requests to a server that has failed to respond to a previous request. This will stop the switch from continually trying to contact a server that it has already determined as dead.<br>Setting the Dead Time to a value greater than 0 (zero) will enable this feature, but only if more than one server has been configured. | 300 |

- **RADIUS Authentication / Accounting / TACACS+ Authentication Server Configuration**




**RADIUS Authentication / Accounting / TACACS+ Authentication Server Configuration**

| Description | Factory default |
|---|---|
| # | |
| The server number for which the configuration below applies. | Any |
| **Enabled** | |
| Specify the status of the RADIUS server.<br>• **Unchecked**: Disable the status of RADIUS server.<br>• **Checked**: Enable the status of RADIUS server. | Unchecked |
| **IP Address** | |
| The IP address or hostname of the RADIUS Server. IP address is expressed in dotted decimal notation. | None |
| **Port** | |
| The UDP port to use on the RADIUS Authentication Server. If the port is set to 0 (zero), the default port (1812) is used on the RADIUS Authentication Server. | 1812 |
| **Secret** | |
| Up to 29 characters long - shared between the RADIUS Authentication Server and the switch stack. | None |

### 3.9.4.2 RADIUS Overview

- **RADIUS Authentication / Accounting Server Configuration**

You can click the number to edit the parameter for AAA features.

| # | IP Address | Status |
|---|---|---|
| 1 | 0.0.0.0:1813 | Disabled |
| 2 | 0.0.0.0:1813 | Disabled |
| 3 | 0.0.0.0:1813 | Disabled |
| 4 | 0.0.0.0:1813 | Disabled |
| 5 | 0.0.0.0:1813 | Disabled |

**RADIUS Authentication / Accounting Server Configuration**

| Item | Description |
|---|---|
| # | The RADIUS server number. Click to navigate to detailed statistics for this server. |
| IP Address | The IP address and UDP port number (in <IP Address>:<UDP Port> notation) of this server. |
| **Status** | The current status of the server.<br>• **Disabled**: The server is disabled.<br>• **Not Ready**: The server is enabled, but IP communication is not up and running.<br>• **Ready**: The server is enabled, IP communication is up and running.<br>• **Dead**: Access attempts were made to this server, but it did not reply within the configured timeout. The server has temporarily been disabled, but will get re-enabled when the dead-time expires. The number of seconds left before this occurs is displayed in parentheses. This state is only reachable when more than one server is enabled. |

### 3.9.4.3 RADIUS Details

- **RADIUS Authentication Statistics for Server.**

There are seven receive and four transmit counters.This section contains information about the state of the server and the latest round-trip time.

- **RADIUS Accounting Statistics for Server**

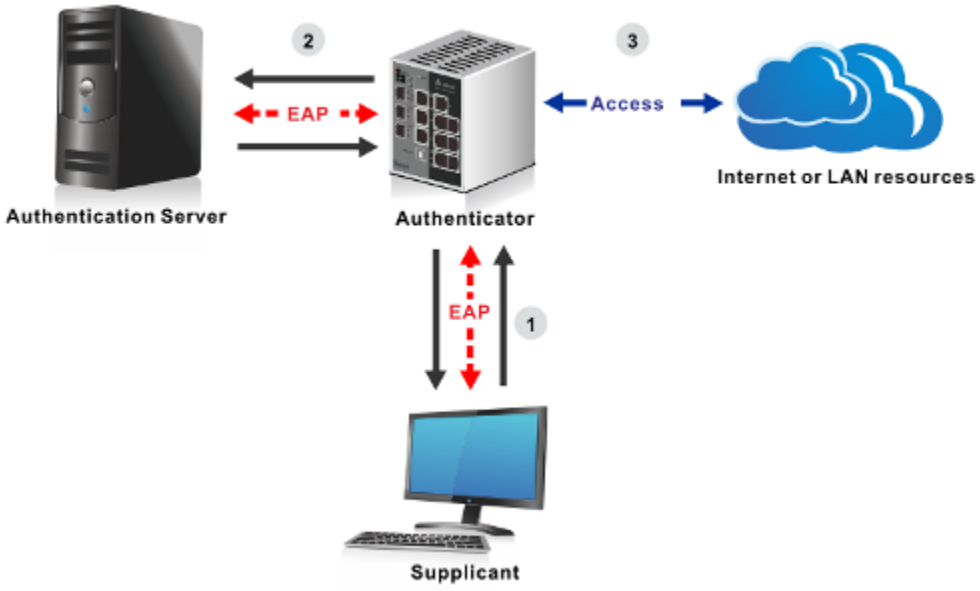
| Receive Packets | | Transmit Packets | |
|---|---|---|---|
| Responses | 0 | Requests | 0 |
| Malformed Responses | 0 | Retransmissions | 0 |
| Bad Authenticators | 0 | Pending Requests | 0 |
| Unknown Types | 0 | Timeouts | 0 |
| Packets Dropped | 0 | | |
| **Other Info** | | | |
| IP Address | | | 0.0.0.0:1813 |
| State | | | Disabled |
| Round-Trip Time | | | 0 ms |

**RADIUS Accounting Statistics for Server**

| Item | Description |
|---|---|
| **Receive Packets** | RADIUS accounting server receive packet counter. There are five receive counters. |
| **Transmit Packets** | RADIUS accounting server transceiver packet counter. There are four transmit counters. |
| **Other Info** | This section contains information about the state of the server and the latest |

### 3.9.5 NAS(802.1X)

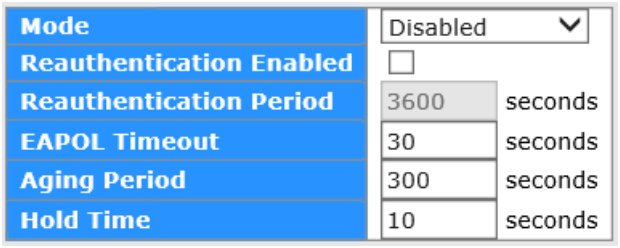
A Delta switch can act as an authenticator in the 802.1X environment. You can either use an external authentication server, or implement the authentication server in the Delta switch by using a Local User Database.
There are three components used to create a port-based authentication mechanism based on 802.1X:
**Supplicant:** The end of the station that requests the access to the LAN resource and switch services.
**Authentication Server:** The external server that performs the actual authentication of the supplicant, for example, a RADIUS server. It performs the authentication to indicate whether the user is authorized to access services.
**Authenticator:** It acts as a proxy between the supplicant and the authentication server. This kind of role is usually the edge switch or the wireless AP. It requests identity information from the supplicant, verifies the information with the authentication server, and relay a response to the supplicant.
The function theory is shown in the figure below.




#### 3.9.5.1 Configuration

You can specify the status of System configuration and the port configuration

- **System Configuration**



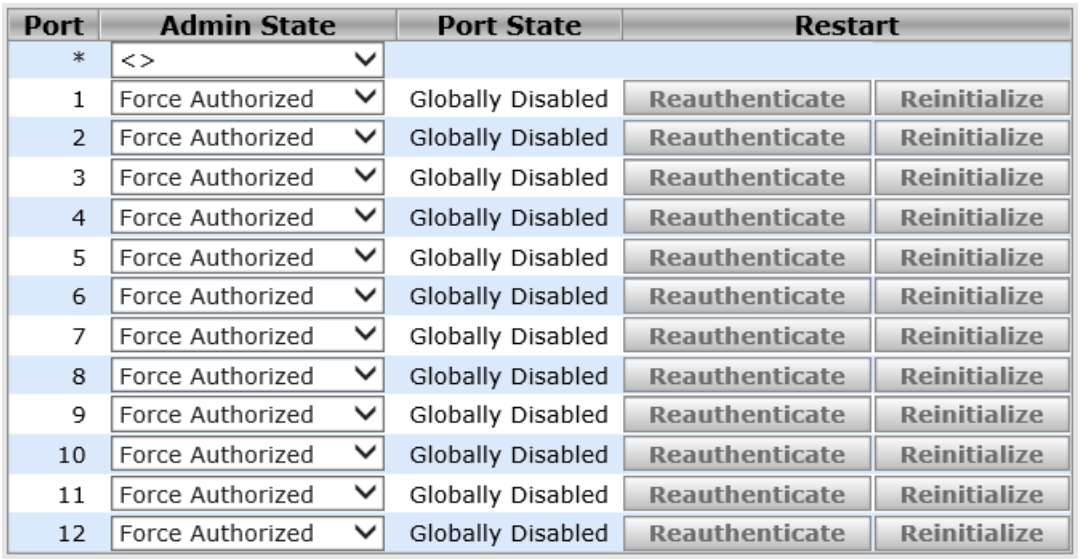

**System Configuration**

| Description | Factory default |
|---|---|
| **Mode** | |
| Specify the status of the system configuration.<br>• **Unchecked**: Disable the status of system configuration.<br>• **Checked**: Enable the status of system configuration. | Disabled |

| Description | Factory default |
|---|---|
| **Reauthentication Enabled** | |
| Specify the status of the Reauthentication.<br>• **Unchecked**: Disable the status of Reauthentication.<br>• **Checked**: Enable the status of Reauthentication. | Unchecked |
| **Reauthentication Period** | |
| Entering the period, in seconds, and this is only active if the Reauthentication Enabled checkbox is checked. Valid values are in the range 1 to 3600 seconds. | 3600 |
| **EAPOL Timeout** | |
| Entering the time for retansmission of Request Identity EAPOL frames, and values are in the range 1 to 65535 seconds. | 30 |
| **Aging Period** | |
| Entering the period for the Aging Period, and can be set to a number between 10 and 1000000 seconds. | 300 |
| **Hold Time** | |
| Entering the period for the Hold Time, and can be set to a number between 10 and 1000000 seconds. | 10 |



- **Port Configuration**




**Port Configuration**

| Description | Factory default |
|---|---|
| **Port** | |
| The interface number. | *interface number* |
| **Admin State** | |
| Specify the status of the Admin State.<br>• **Force Authorized:** Places the interface in the authorized state. The interface sends and receives normal traffic without the client port-based authentication.<br>• **Force Unauthorized**: Places the interface in the unauthorized state. The switch can not provide authentication services for a client through the interface.<br>• **Port-based 802.1X**: The maximum number of supplicants that can be attached to a port can be limited using the Port Security Limit Control functionality.<br>• **MAC-based authentication**: The maximum number of clients that can be attached to a port can be limited using the Port Security Limit Control functionality. | Force Authorized |
| **Port State** | |
| Display the status of the port. | Fixed |

| | |
|---|---|
| • **Globally Disabled:** NAS is globally disabled.<br>• **Link Down**: NAS is globally enabled, but there is no link on the port.<br>• **Authorized**: The port is in Force Authorized or a single-supplicant mode and the supplicant is authorized.<br>• **Unauthorized**: The port is in Force Unauthorized or a single-supplicant mode and the supplicant is not successfully authorized by the RADIUS server.<br>• **X Auth/Y Unauth:** The port is in a multi-supplicant mode. Currently X clients are authorized and Y is unauthorized. | |
| **Restart** | |
| Specify what kind of the restart type.<br>• **Reauthenticate:** Schedules a reauthentication whenever the quiet-period of the port runs out (EAPOL-based authentication).<br>• **Reinitialize**: Forces a reinitialization of the clients on the port and thereby a reauthentication immediately. The clients will transfer to the unauthorized state while the reauthentication is in progress. | None |



### 3.9.5.2 Switch

| Port | Admin State | Port State | Last Source | Last ID |
|---|---|---|---|---|
| 1 | Force Authorized | Globally Disabled | | |
| 2 | Force Authorized | Globally Disabled | | |
| 3 | Force Authorized | Globally Disabled | | |
| 4 | Force Authorized | Globally Disabled | | |
| 5 | Force Authorized | Globally Disabled | | |
| 6 | Force Authorized | Globally Disabled | | |
| 7 | Force Authorized | Globally Disabled | | |
| 8 | Force Authorized | Globally Disabled | | |
| 9 | Force Authorized | Globally Disabled | | |
| 10 | Force Authorized | Globally Disabled | | |
| 11 | Force Authorized | Globally Disabled | | |
| 12 | Force Authorized | Globally Disabled | | |

**Switch Status**

| Item | Description |
|---|---|
| **Port** | The switch port number. Click to navigate to detailed 802.1X statistics for this port. |
| **Admin State** | The port's current administrative state. Refer to NAS Admin State for a description of possible values. |
| **Port State** | The current state of the port. Refer to NAS Port State for a description of the individual states. |
| **Last Source** | The source MAC address carried in the most recently received EAPOL frame for EAPOL-based authentication, and the most recently received frame from a new client for MAC-based authentication. |
| **Last ID** | The user name (supplicant identity) carried in the most recently received Response Identity EAPOL frame for EAPOL-based authentication, and the source MAC address from the most recently received frame from a new client for MAC-based authentication. |

### 3.9.5.3 Port

| | |
|---|---|
| **Admin State** | Force Authorized |
| **Port State** | Globally Disabled |

**Port**

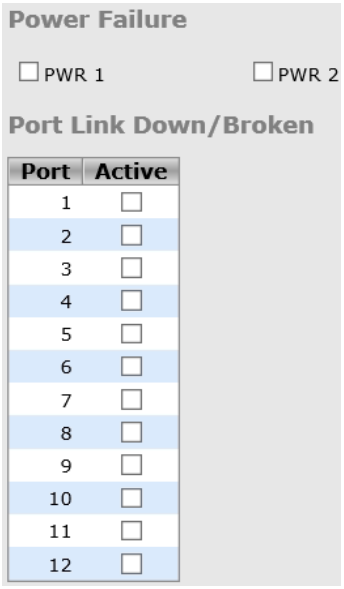
| Item | Description |
|---|---|
| **Admin State** | The port's current administrative state. Refer to NAS Admin State for a description of possible values. |
| **Port State** | The current state of the port. Refer to NAS Port State for a description of the individual states. |

## 3.10 Warning

Industrial Ethernet devices in an industrial environment are very important. These devices usually need to work for a long time and are usually located at the end of the system. So if the devices which connect to the industrial Ethernet switch need to be maintained, the switch must provide some messages for the maintainer. Even when the maintainers or the engineers do not stay in the control room, they still need to be informed of the status of the devices. A Delta switch provides different approaches that can warn engineers automatically. In this section, you can get the information about a relay alarm.

### 3.10.1 Fault Alarm

You can configure the power and the port active to notice related engineers.



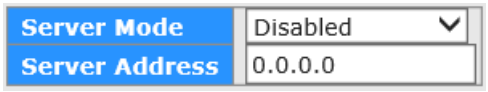

**Fault Alarm**

| Description | Factory default |
|---|---|
| **Power Failure** | |
| Specify the power event status:<br>• **Unchecked**: Disable PWR-1 or PWR2 or both.<br>• **Checked**: Enable PWR-1 or PWR2 or both. | Unchecked |
| **Port Link Down/Broken_Port** | |
| Specify the interface number. | *Port number* |
| **Port Link Down/Broken_Active** | |
| Specify the port link event status.<br>• **Unchecked**: Disable the port link event alarm.<br>• **Checked**: Enable the port link event alarm | Unchecked |

## 3.10.2 System Warning

The System Warning function allows you to monitor the switch. When faults, errors, configuration changes or specified events happen, this function can generate messages, store the messages locally or forward the messages to one syslog server or more syslog servers. You can choose the severity level to filter the message according to your requirement.

### 3.10.2.1 SYSLOG Setting

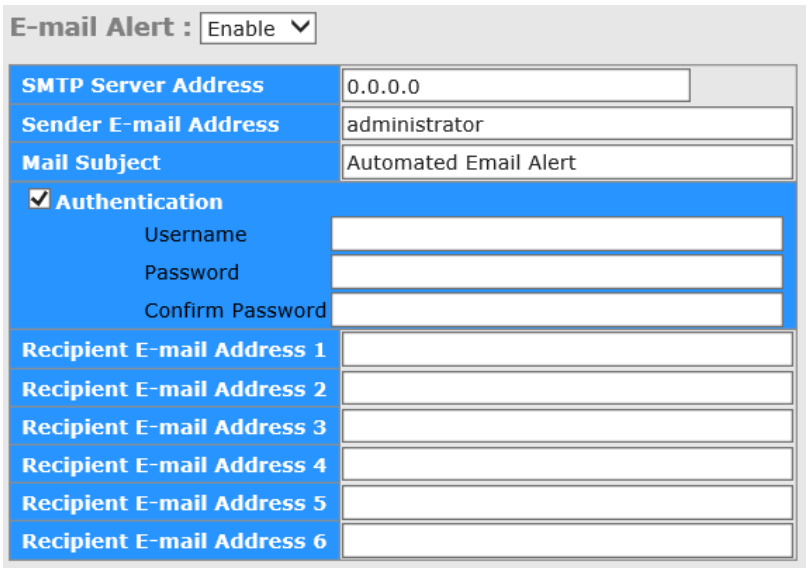



**Fault Alarm**

| Description | Factory default |
|---|---|
| **Server Mode** | |
| Specify the the server mode operation mode:<br>• **Disable**: Disable server mode operation.<br>• **Enabled**: Enable server mode operation. | Unchecked |
| **Server Address** | |
| Specify the Server IP address. | Port number |

### 3.10.2.2 SMTP Setting

E-mail Server Configuration allows you to monitor the switch when you can not stay in front of the computer. For example, when the alarm event happens, you can use a smart phone to get an alarm event email anywhere. And then you can contact a related maintainer or engineer to check the device and solve the problem.




**SMTP Setting**

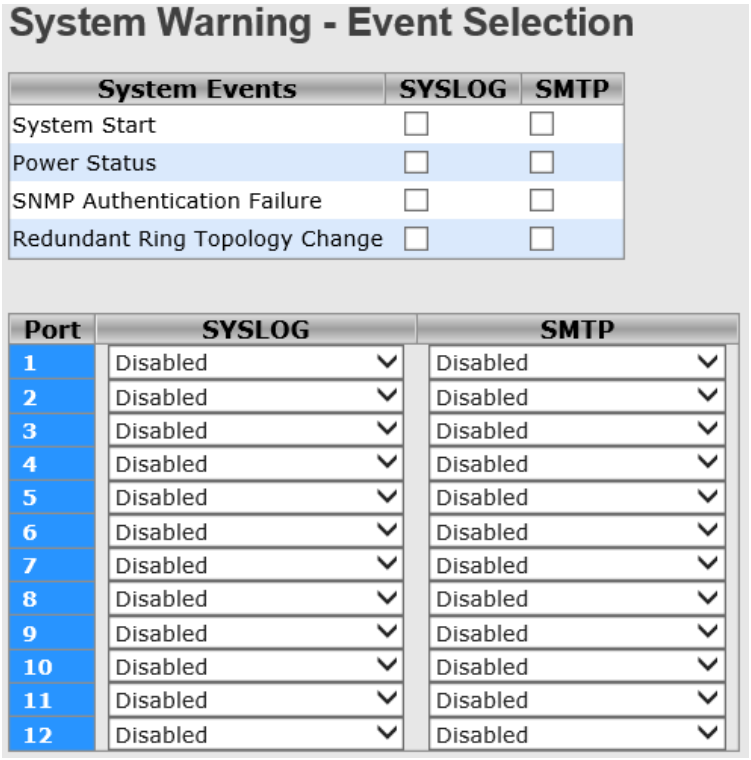
| Description | Factory default |
|---|---|
| **E-mail Alert** | |
| Sepcify the status of email Alert | Disable |
| **SMTP Server Address** | |
| Enter the IP address of the mail server. | 0.0.0.0 |
| **Sender E-mail Address** | |
| Specify the email address of send the email alarm. | Administrator |
| **Mail Object** | |

| Description | Factory default |
|---|---|
| Specify the object of the email alarm. | None |
| **Authentication** | |
| Specify whether the mail server needs the authentication. If the box is selected, please enter the account name of the email. | None |
| **Recipient E-mail Address** | |
| Specify the email address for the email alarm. You can specify 1 to 6 email addresses. | None |

### 3.10.2.3 Event Selecting



The Event Selecting page allows you to get an email message when the event you configured happened.




**Event Selecting**

| Description | Factory default |
|---|---|
| **Switch Start** | |
| Specify whether to send an alarm email or save logs when switch cold starts. | Unchecked |
| **Power Status** | |
| Specify whether to send an alarm email or save logs when there is a transition in power from Off to On or from On to Off. | Unchecked |
| **SNMP Authentication Failure** | |
| Specify whether to send an alarm email or save logs when there is a failure in SNMP Authentication. | Unchecked |
| **Redundant Ring Topology Change** | |
| Specify whether to send alarm email or save logs when the redundancy has changed. | Unchecked |
| **Authentication Failure** | |
| Specify whether to send an alarm email or save logs when there is authentication failure. | Checked |

| Description | Factory default |
|---|---|
| **Port** | |
| This field displays the interface number. | *interface number* |
| **SYSLOG** | |
| Specify whether to save logs when the port event happened.<br>• **Disable**: Disabled to save logs.<br>• **Link Up**: Specify whether to save logs when the Link is up.<br>• **Link Down**: Specify whether to save logs when the Link is down.<br>• **Link Up and down:** Specify whether to save logs when the Link is up or down. | Disabled |
| **SMTP** | |
| Specify whether to send an alarm email when the port event happened.<br>• **Disable**: Disabled to send an alarm email.<br>• **Link Up**: Specify whether to send an alarm email when the Link is up.<br>• **Link Down**: Specify whether to send an alarm email when the Link is down.<br>• **Link Up and down:** Specify whether to send an alarm email when the Link is up or down. | Disabled |



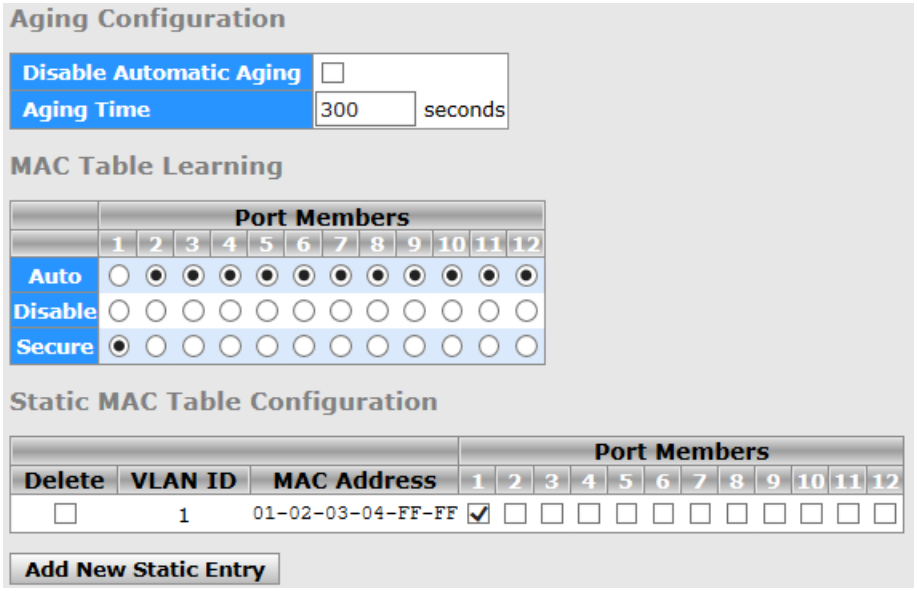
## 3.11 Monitor and Diag

You can monitor the status of the Delta switch in real time via the functions in this group.

### 3.11.1 MAC Table

The MAC address table displays the MAC address which is learned and manually added. There is a search function which can be used to display the information about the entry in the table.

#### 3.11.1.1 MAC Address Table Configuration




**Aging Configuration**

| Description | Factory default |
|---|---|
| **Disable Automatic Aging** | |
| Specify whether the status of Disable Automatic Aging.<br>• **Unchecked**: Disable the Disable Automatic Aging operation mode.<br>• **Checked**: Enable the Disable Automatic Aging operation mode. | Unchecked |
| **Aging Time** | |
| Enter the period in seconds. If a learned MAC address has not been updated during | 300 |

| Description | Factory default |
|---|---|
| the address aging time, then it will be removed from the address table automatically. Enter a period in the range of 10 to 1000000 seconds. | |

**MAC Table Learning**

| Description | Factory default |
|---|---|
| **Port Members** | |
| This field displays the port number. | *port number* |
| **Auto** | |
| Learning is done automatically as soon as a frame with unknown SMAC is received. | Checked |
| **Disable** | |
| No learning is done. | Unchecked |
| **Secure** | |
| Only static MAC entries are learned, all other frames are dropped. Make sure that the link used for managing the switch is added to the Static Mac Table before changing to secure learning mode, otherwise the management link is lost and can only be restored by using another non-secure port or by connecting to the switch via the serial interface. | Unchecked |

**Static MACTable Configuration**

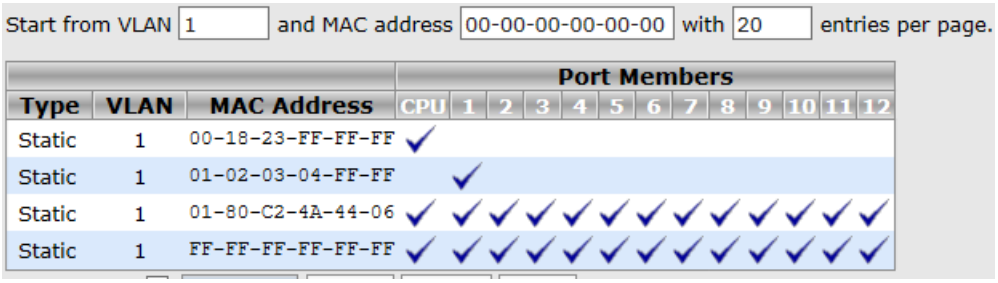
| Description | Factory default |
|---|---|
| **Port Members** | |
| Checkmarks indicate which ports are members of the entry. Check or uncheck as needed to modify the entry. | Unchecked |
| **Delete** | |
| Check to delete the entry. It will be deleted during the next save. | None |
| **VLAN ID** | |
| The VLAN ID for the entry. | Unchecked |
| **MAC Address** | |
| The MAC address for the entry. | Fixed |
| **Add New Static Entry** | |
| Adding a new entry to the static MAC table. Specify the VLAN ID, MAC address, and port members for the new entry. Click "Save". | None |

The static entries in the MAC table are shown in this table. The static MAC table can contain 64 entries. The maximum of 64 entries is for the whole stack, and not per switch.

The MAC table is sorted first by VLAN ID and then by MAC address.

### 3.11.1.2 MAC Address Table

Each page shows up to 999 entries from the MAC table, default being 20, selected through the "entries per page" input field. When first visited, the web page will show the first 20 entries from the beginning of the MAC Table. The first displayed will be the one with the lowest VLAN ID and the lowest MAC address found in the MAC Table.



**MAC Address Table**

| Item | Description |
|---|---|
| **Type** | The status of this entry:.<br>• **Dynamic:** The MAC address was learned through incoming traffic and is being used.<br>• **Static:** The MAC address was manually added and can not be relearned. |
| **VLAN** | The VLAN ID that is associated with the MAC address |
| **MAC Address** | The dynamically learned or manually added MAC address for which the switch has forwarded or filtered information, or both |
| **Port Members** | This field displays the interface which was learned or added manually. It also means the interface through which the MAC address can be reached. |

## 3.11.2 Port Statistics

You can monitor the statistics of each interface of the Delta switch on this page.

**Note:**
Make sure that the port you want to monitor is connected to another device.

### 3.11.2.1 Traffic Overview

| Port | Packets | | Bytes | | Errors | | Drops | | Filtered |
|---|---|---|---|---|---|---|---|---|---|
| | Received | Transmitted | Received | Transmitted | Received | Transmitted | Received | Transmitted | Received |
| 1 | 155711 | 90594 | 19377230 | 16086358 | 0 | 0 | 0 | 0 | 1 |
| 2 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 3 | 320534 | 132756 | 35032521 | 30578708 | 5 | 0 | 0 | 0 | 5344 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 16325 | 186121 | 1219432 | 18846977 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 9 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 10 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 11 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 12 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |

**Traffic Overview**

| Item | Description |
|---|---|
| **Port** | This field displays the port number. |
| **Packets** | The number of received and transmitted packets per port. |
| **Bytes** | The number of received and transmitted bytes per port. |
| **Errors** | The number of frames received in error and the number of incomplete transmissions per port. |
| **Drops** | The number of frames discarded due to ingress or egress congestion. |
| **Filtered** | The number of received frames filtered by the forwarding process. |

### 3.11.2.2 Detail Stastistics

Port 1

| Receive Total | |
|---|---|
| Rx Packets | 157826 |
| Rx Octets | 19691009 |
| Rx Unicast | 88156 |
| Rx Multicast | 10311 |
| Rx Broadcast | 59359 |
| Rx Pause | 0 |
| **Receive Size Counters** | |
| Rx 64 Bytes | 114073 |
| Rx 65-127 Bytes | 9896 |
| Rx 128-255 Bytes | 4106 |
| Rx 256-511 Bytes | 29743 |
| Rx 512-1023 Bytes | 4 |
| Rx 1024-1526 Bytes | 4 |
| Rx 1527- Bytes | 0 |
| **Receive Queue Counters** | |
| Rx Q0 | 157826 |
| Rx Q1 | 0 |
| Rx Q2 | 0 |
| Rx Q3 | 0 |
| Rx Q4 | 0 |
| Rx Q5 | 0 |
| Rx Q6 | 0 |
| Rx Q7 | 0 |
| **Receive Error Counters** | |
| Rx Drops | 0 |
| Rx CRC/Alignment | 0 |
| Rx Undersize | 0 |
| Rx Oversize | 0 |
| Rx Fragments | 0 |
| Rx Jabber | 0 |
| Rx Filtered | 1 |

| Transmit Total | |
|---|---|
| Tx Packets | 91293 |
| Tx Octets | 16231217 |
| Tx Unicast | 59760 |
| Tx Multicast | 31251 |
| Tx Broadcast | 282 |
| Tx Pause | 0 |
| **Transmit Size Counters** | |
| Tx 64 Bytes | 29388 |
| Tx 65-127 Bytes | 418 |
| Tx 128-255 Bytes | 60044 |
| Tx 256-511 Bytes | 711 |
| Tx 512-1023 Bytes | 112 |
| Tx 1024-1526 Bytes | 620 |
| Tx 1527- Bytes | 0 |
| **Transmit Queue Counters** | |
| Tx Q0 | 28404 |
| Tx Q1 | 0 |
| Tx Q2 | 0 |
| Tx Q3 | 0 |
| Tx Q4 | 0 |
| Tx Q5 | 0 |
| Tx Q6 | 0 |
| Tx Q7 | 62889 |
| **Transmit Error Counters** | |
| Tx Drops | 0 |
| Tx Late/Exc. Coll. | 0 |

**Traffic Overview**

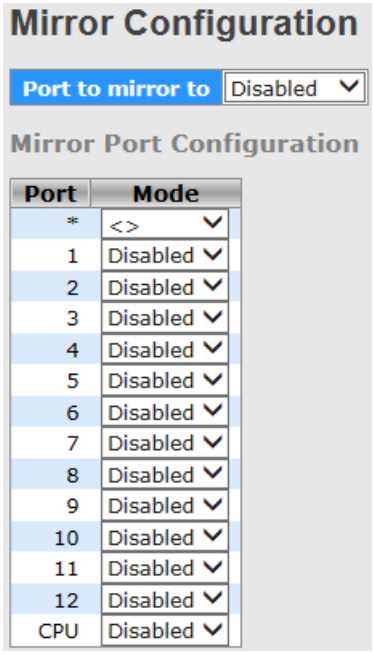
| Item | Description |
|---|---|
| **Rx and Tx Packets** | The number of received and transmitted (good and bad) packets. |
| **Rx and Tx Octets** | The number of received and transmitted (good and bad) bytes. Includes FCS, but excludes framing bits. |
| **Rx and Tx Unicast** | The number of received and transmitted (good and bad) unicast packets. |
| **Rx and Tx Multicast** | The number of received and transmitted (good and bad) multicast packets. |

| Item | Description |
|---|---|
| **Rx and Tx Broadcast** | The number of received and transmitted (good and bad) broadcast packets. |
| **Rx and Tx Pause** | A count of the MAC Control frames received or transmitted on this port that have an opcode indicating a PAUSE operation. |
| **Rx Drops** | The number of frames dropped due to lack of receives buffers or egress congestion. |
| **Rx CRC/Alignment** | The number of frames received with CRC or alignment errors. |
| **Rx Undersize** | The number of short 1 frames received with valid CRC. |
| **Rx Oversize** | The number of long 2 frames received with valid CRC. |
| **Rx Fragments** | The number of short 1 frames received with invalid CRC. |
| **Rx Jabber** | The number of long 2 frames received with invalid CRC. |
| **Rx Filtered** | The number of received frames filtered by the forwarding process. |
| **Tx Drops** | The number of frames dropped due to output buffer congestion. |
| **Tx Late / Exc.Coll.** | The number of frames dropped due to excessive or late collisions. |



### 3.11.3 Port Monitoring

Port Monitoring is used for mirroring the network traffic of the source port by the analyzer.

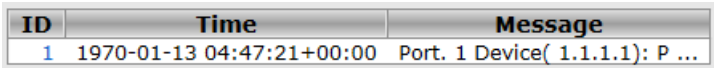



**Port Monitoring**

| Description | Factory default |
|---|---|
| **Port to mirror** | |
| Specify the port which is the mirror port. | Disabled |
| **Port** | |
| This field displays the port number. | *port number* |
| **Mode** | |
| Specify the direction in which the port mirroring occurs:<br>• **Disabled:** Neither frames transmitted nor frames received are mirrored.<br>• **Rx Only:** Only incoming traffic is mirrored.<br>• **Tx Only:** Only outgoing traffic is mirrored.<br>• **Enabled:** Both outgoing traffic and incoming traffic are mirrored. | Disabled |

## 3.11.4 System Log Information

The System Log function allows you to monitor the switch. When faults, errors, configuration changes or specified events happen, this function can generate messages, store the messages locally or forward the messages to one syslog server or more syslog servers. You can choose the severity level to filter the message according to your requirement.



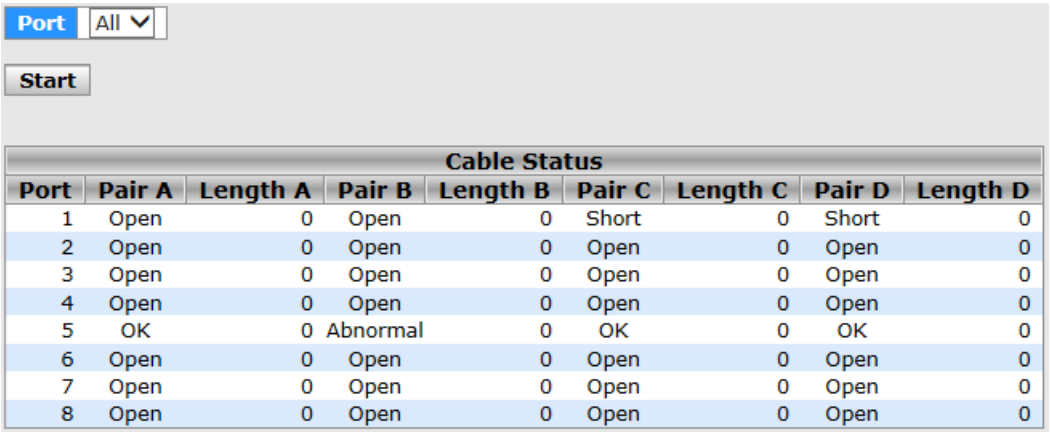
| ID | Time | Message |
|---|---|---|
| 1 | 1970-01-13 04:47:21+00:00 | Port. 1 Device( 1.1.1.1): P ... |

**System Log Information**

| Item | Description |
|---|---|
| **ID** | The ID (>= 1) of the system log entry. |
| **Time** | The time of the system log entry. |
| **Message** | The IP Address of this switch. |

## 3.11.5 VeriPHY Cable Diagnostics

The Delta switch provides administrator the Cable Diagnostic function to detect whether the cable link status of the port is normal or not. The Cable status will show the cable link status of the port which you select.




| Port | Pair A | Length A | Pair B | Length B | Pair C | Length C | Pair D | Length D |
|---|---|---|---|---|---|---|---|---|
| 1 | Open | 0 | Open | 0 | Short | 0 | Short | 0 |
| 2 | Open | 0 | Open | 0 | Open | 0 | Open | 0 |
| 3 | Open | 0 | Open | 0 | Open | 0 | Open | 0 |
| 4 | Open | 0 | Open | 0 | Open | 0 | Open | 0 |
| 5 | OK | 0 | Abnormal | 0 | OK | 0 | OK | 0 |
| 6 | Open | 0 | Open | 0 | Open | 0 | Open | 0 |
| 7 | Open | 0 | Open | 0 | Open | 0 | Open | 0 |
| 8 | Open | 0 | Open | 0 | Open | 0 | Open | 0 |

**VeriPHY Cable Diagnostics**

| Description | Factory default |
|---|---|
| **Port** | |
| The port where you are requesting VeriPHY Cable Diagnostics. | All |

**Cable Status**

| Item | Description |
|---|---|
| **Port** | This field displays the port number. |
| **Cable Status** | This field displays the cable link status.<br>• Port: Port number.<br>• Pair: The status of the cable pair.<br>• Length: The length (in meters) of the cable pair. |

### 3.11.6 SFP Monitor

You can monitor the status of each SFP (small form-factor pluggable) port on this page.

| Port No. | Temperature (°C) | Vcc (V) | TX Bias (mA) | TX Power (mW) | (dBm) | RX Power (mW) | (dBm) |
|---|---|---|---|---|---|---|---|
| 9 | N/A | N/A | N/A | N/A | N/A | N/A | N/A |
| 10 | N/A | N/A | N/A | N/A | N/A | N/A | N/A |
| 11 | N/A | N/A | N/A | N/A | N/A | N/A | N/A |
| 12 | N/A | N/A | N/A | N/A | N/A | N/A | N/A |

**Note:**
Before you use the SFP DDM function, please make sure the SFP module you used are support SFP DDM function.



### 3.11.7 Traffic Monitor

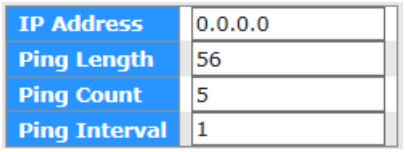
This page can help you monitor about selecting monitor-Counter, and record or notice syslog information immediately.

| Port | Monitor-Counter | Time-Interval | Increasing-Quantity |
|---|---|---|---|
| 1 | Disable | 3 | 1000 |
| 2 | Disable | 3 | 1000 |
| 3 | Disable | 3 | 1000 |
| 4 | Disable | 3 | 1000 |
| 5 | Disable | 3 | 1000 |
| 6 | Disable | 3 | 1000 |
| 7 | Disable | 3 | 1000 |
| 8 | Disable | 3 | 1000 |
| 9 | Disable | 3 | 1000 |
| 10 | Disable | 3 | 1000 |
| 11 | Disable | 3 | 1000 |
| 12 | Disable | 3 | 1000 |

**Traffic Monitor**

| Description | Factory default |
|---|---|
| **Port** | |
| This field displays the port number. | *port number* |
| **Monitor-Counter** | |
| Specify the mode of the Monitor-Counter mode.<br>• **Disable**: Select the Disable mode.<br>• **RxOctet**: Select the Rx Octet mode.<br>• **RxBroadcast**: Select the Rx Broadcast mode.<br>• **RxMulticast**: Select the Rx Multicast mode.<br>• **RxUnicast** : Select the Rx Unicast mode. | Disable |
| **Time-Interval** | |
| Entering values for monitor interval, Time-Interval values between 1 and 300. | 3 |
| **Increasing-Quantity** | |
| Set values for Traffic restrictions,Increasing-Quantity values between 1 and 2147483647, | 1000 |

### 3.11.8 Ping



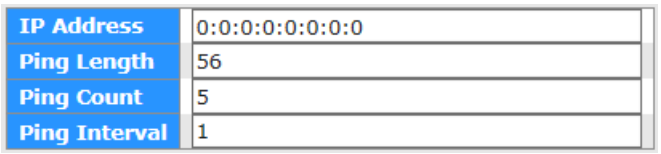

**Ping**

| Description | Factory default |
|---|---|
| **IP Address** | |
| Specify the IP address that you want to ping. Enter an IPv4 address. | 0.0.0.0 |
| **Ping Length** | |
| Specify the size of the ping packet in bytes. Enter a payload size between 0 and 2080 bytes. | 56 |
| **Ping Count** | |
| Specify the number of echo requests to be sent. Enter a number between 1 and 10. | 5 |
| **Ping Interval** | |
| Specify the interval between ping packets in seconds. Enter a number between 1 and 100 seconds. | 1 |

- An unsuccessful ping is displayed in the way described below:
  PING server <ipv4 address>, 56 bytes of data.
  recvfrom: Operation timed out
  recvfrom: Operation timed out
  recvfrom: Operation timed out
  Sent<count> packets, received 0 OK, 0 bad
- A successful ping is displayed in the way described below:
  PING server <ipv4 address>, 56 bytes of data.
  64 bytes from <ipv4 address>: icmp_seq=0, time=10ms
  64 bytes from <ipv4 address>: icmp_seq=1, time=0ms
  64 bytes from <ipv4 address>: icmp_seq=2, time=0ms
  Sent 5<count> packets, received 5 OK, 0 bad

**Note:**
Make sure that the IP Address/Hostname you want to ping really exists and normally works in the same segment as the switch.

### 3.11.9 IPv6 Ping




**IPv6 Ping**

| Description | Factory default |
|---|---|
| **IP Address** | |
| Specify the IP address that you want to ping. Enter an IPv6 address or a host name. | 0:0:0:0:0:0:0:0 |
| **Ping Length** | |
| Specify the size of the ping packet in bytes. Enter a payload size between 0 and 2080 bytes. | 56 |
| **Ping Count** | |
| Specify the number of echo requests to be sent. Enter a number between 1 and 10. | 5 |
| **Ping Interval** | |
| Specify the interval between ping packets in seconds. Enter a number between 1 and 100 seconds. | 1 |

- An unsuccessful ping is displayed in the way described below:
  PING server <ipv6 address>, 56 bytes of data.
  recvfrom: Operation timed out
  recvfrom: Operation timed out
  recvfrom: Operation timed out
  Sent<count> packets, received 0 OK, 0 bad
- A successful ping is displayed in the way described below:
  PING server <ipv6 address>, 56 bytes of data.
  64 bytes from <ipv6 address>: icmp_seq=0, time=10ms
  64 bytes from <ipv6 address>: icmp_seq=1, time=0ms
  64 bytes from <ipv6 address>: icmp_seq=2, time=0ms
  Sent 5<count> packets, received 5 OK, 0 bad

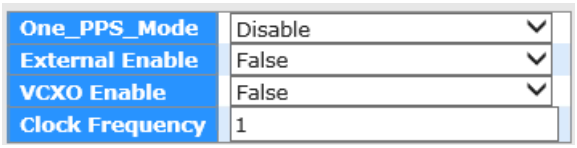
**Note:**
Make sure that the IP Address/Hostname you want to ping really exists and normally works in the same segment as the switch.

## 3.12 Synchronization

This page allows the user to configure and inspect the current PTP clock settings.

### 3.12.1 PTP

- **PTP External Clock Mode**

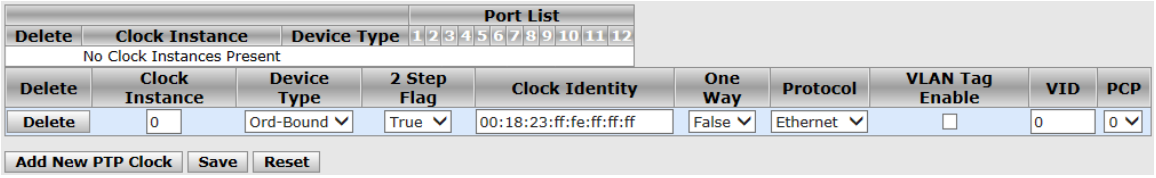



**PTP External Clock Mode**

| Description | Factory default |
|---|---|
| **One_PPS_Mode** | |
| Specify the status of One_PPS_Mode.<br>• **Disable**: Disable the 1 pps clock in/out-put.<br>• **Output**: Enable the 1 pps clock output.<br>• **Input**: Enable the 1 pps clock input. | Disable |
| **External Enable** | |
| Specify the status of the External Clock output.<br>• **False**: Disable the external clock output.<br>• **True**: Enable the external clock output. | False |
| **VCXO Enable** | |
| Specify the status of the External VCXO rate adjustment.<br>• **False**: Disable the VCXO rate adjustment<br>• **True**: Enable the VCXO rate adjustment | False |
| **Clock Frequency** | |
| Entering the Clock Frequency.The possible range of values are 1 - 25000000 (1 - 25MHz) | 1 |

- **PTP Clock Configuration**

You can click “Add New PTP Clock” to add a new PTP clock.




**PTP Clock Configuration**

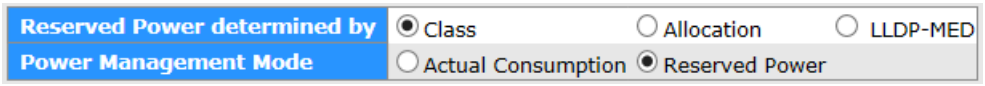
| Description | Factory default |
|---|---|
| **Delete** | |
| Check this box and click on 'Save' to delete the clock instance. | Unchecked |
| **Clock Instance** | |
| Indicates the Instance of a particular Clock Instance [0.3].<br>Click on the Clock Instance number to edit the Clock details. | 0 |
| **Device Type** | |
| Specify whether the Device Type of the PTP Clock.<br>• **Ord-Bound**: Clock's Device Type is Ordinary-Boundary Clock.<br>• **P2p Transp**: Clock's Device Type is Peer to Peer Transparent Clock.<br>• **E2e Transp**: Clock's Device Type is End to End Transparent Clock.<br>• **Master Only**: Clock's Device Type is Master Only.<br>• **Slave Only**: Clock's Device Type is Slave Only. | Ord-Bound |
| **Port List** | |
| Specify the port configured for this Clock Instance. | None |
| **2 Step Flag** | |
| Static member: defined by the system, true if two-step Sync events and Pdelay_Resp events are used. | True |
| **Clock Identity** | |
| It shows unique clock identifier. | None |
| **One Way** | |
| Specify whether the mode is enabled or not.This parameter applies only to a slave. | False |
| **Protocol** | |
| Transport protocol used by the PTP protocol engine<br>• **Ethernet**: PTP over Ethernet multicast.<br>• **IP4Multi**: PTP over IPv4 multicast.<br>• **IPv4Uni**: PTP over IPv4 unicast. | Ethernet |
| **VLAN Tag Enable** | |
| Specify the status of VLAN Tag.<br>• **Unchecked**: Disable the VLAN Tag.<br>• **Checked**: Enable VLAN Tag. | Unchecked |
| **VID** | |
| Specify the VLAN Identifier used for tagging the PTP frames. | 0 |
| **PCP** | |
| Specify the Priority Code Point value used for PTP frames. | 0 |

## 3.13 PoE

PoE is an acronym for Power Over Ethernet. It is used to transmit electrical power, to remote devices over standard Ethernet cable. It could for example be used for powering IP telephones, wireless LAN access points and other equipment, where it would be difficult or expensive to connect the equipment to main power supply.

### 3.13.1 PoE Configuration

The MAC address table displays the MAC address which is learned and manually added. There is a search function which can be used to display the information about the entry in the table.




**PoE Configuration**

| Description | Factory default |
|---|---|
| **Reserved Power determined by** | |
| Specify how the ports/PDs may reserve power.<br>• **Class**: In this mode each port automatically determines how much power to reserve according to the class the connected PD belongs to, and reserves the power accordingly. Four different port classes exist and one for 4, 7, 15.4 or 30 Watts.<br>• **Allocation**: In this mode the user allocates the amount of power that each port may reserve.<br>• **LLDP-MED**: This mode is similar to the Class mode expect that each port determine the amount power it reserves by exchanging PoE information using the LLDP protocol and reserves power accordingly. If no LLDP information is available for a port, the port will reserve power using the class mode. | Class |
| **Power Managed Mode** | |
| Specify the status of Power Managed:<br>• **Actual Consumption**: In this mode the ports are shutted down when the actual power consumption for all ports exceed the amount of power that the power supply can deliver or if the actual power consumption for a given port exceeds the reserved power for that port. The ports are shut down according to the ports priority. If two ports have the same priority the port with the highest port number is shutted down.<br>• **Reserved Power**: In this mode the ports are shutted down when total reserved powered exceeds the amount of power that the power supply can deliver. In this mode the port power is not turned on if the PD requests more power than available from the power supply. | Reserved Power |

### 3.13.2 PoE Status

You can monitor the status of each PoE (Power over Ethernet) port on this page.

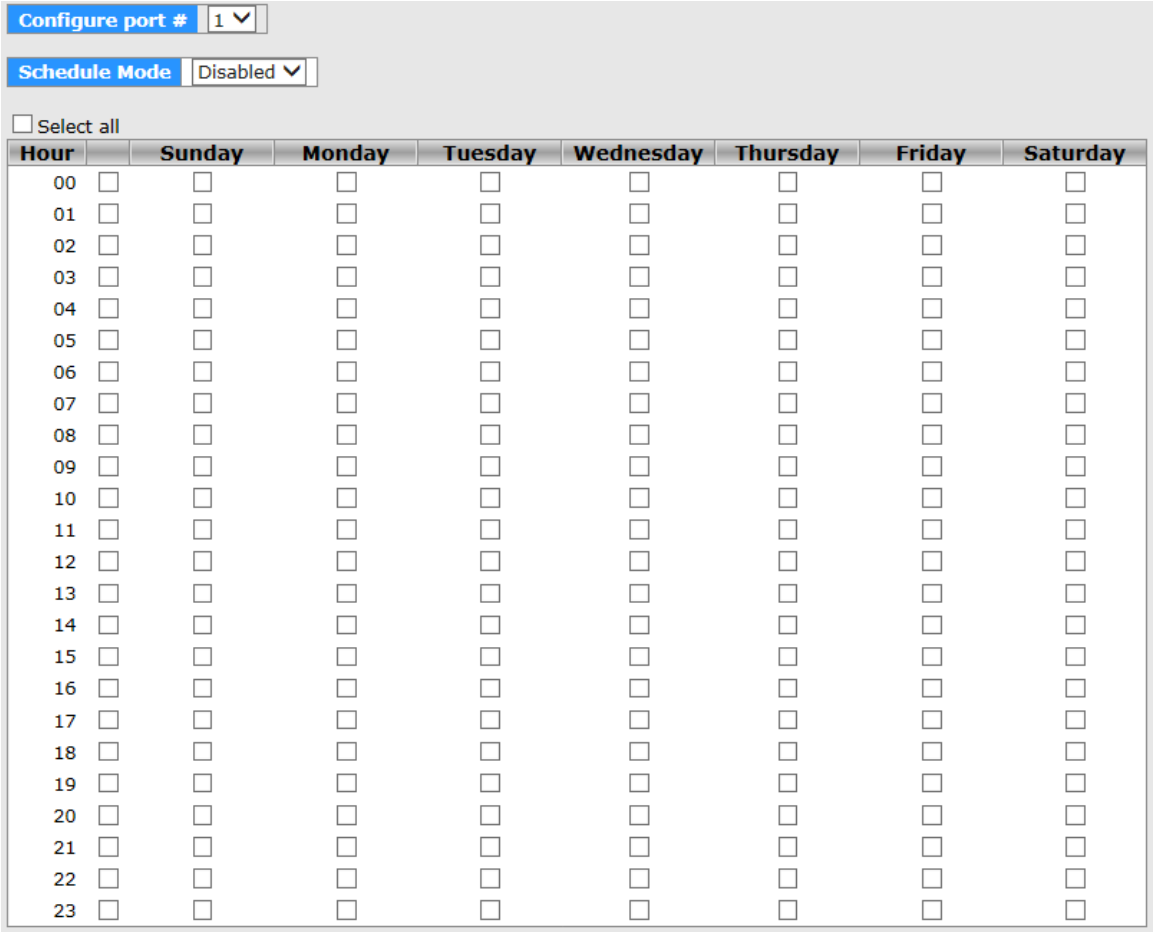
| Local Port | PD class | Power Requested | Power Allocated | Power Used | Current Used | Priority | Port Status |
|---|---|---|---|---|---|---|---|
| 1 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 2 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 3 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 4 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 5 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 6 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| 7 | 4 | 30 [W] | 30 [W] | 1 [W] | 21 [mA] | Low | PoE turned ON |
| 8 | - | 0 [W] | 0 [W] | 0 [W] | 0 [mA] | Low | No PD detected |
| Total | | 30 [W] | 30 [W] | 1 [W] | 21 [mA] | | |

**PoE Status**

| Item | Description |
|---|---|
| **Local Port** | This field displays the PoE port number. |
| **PD Class** | Each PD is classified according to a class that defines the maximum power the PD will use. There are five classes defined:<br>• Class 0: Max. power 15.4 W<br>• Class 1: Max. power 4.0 W<br>• Class 2: Max. power 7.0 W<br>• Class 3: Max. power 15.4 W<br>• Class 4: Max. power 30.0 W |
| **Power Requested** | The Power Requested shows the requested amount of power the PD wants to be reserved. |
| **Power Allocated** | The Power Allocated shows the amount of power the switch has allocated for the PD. |
| **Power used** | The Power Used shows how much power the PD currently is using. |
| **Current used** | The Power Used shows how much current the PD currently is using. |
| **Priority** | The Priority shows the port's priority configured by the user. |
| **Port Status** | The Port Status shows the port's status. The status can be one of the following values:<br>• PoE not available - No PoE chip found: PoE not supported for the port.<br>• PoE turned OFF - PoE disabled: PoE is disabled by user.<br>• PoE turned OFF - Power budget exceede: The total requested or used power by the PDs exceeds the maximum power the Power Supply can deliver, and port(s) with the lowest priority is/are powered down.<br>• No PD detected: No PD detected for the port.<br>• PoE turned OFF - PD overload: The PD has requested or used more power than the port can deliver, and is powered down.<br>• PoE turned OFF - PD is off.<br>• Invalid PD: PD detected, but is not working correctly. |

### 3.13.3 PoE Schedule

Configure port number of the switch supplying power around the clock on this page. The users can set the desired power policy accordingly.

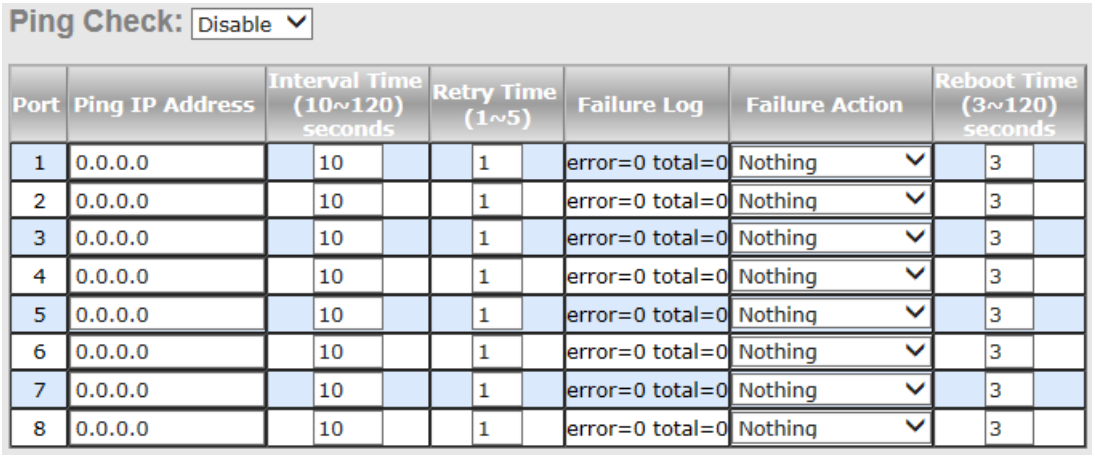



**PTP Clock Configuration**

| Description | Factory default |
|---|---|
| **Configure port** | |
| Select the port number of the switch to configure. | 1 |
| **Schedule Mode** | |
| Select status of the PoE Schedule operation:<br>• **Disable**: Disable the PoE Schedule configuration<br>• **Enable**: Enable the PoE Schedule configuration | Disable |
| **Select all** | |
| Check this box to select all checkbox. | Unchecked |
| **Daily Schedule form** | |
| Check Hours and Week checkbox to set port working times. | Unchecked |

## 3.13.4 PoE Auto Ping

PoE Auto Ping can monitor the real-time status of connected power devices.
Switch could send alive-checking packets to assure the connected devices are in working state.
If the connected devices fail to response, switch could reactivate the connected devives to assure the reliability of the network.

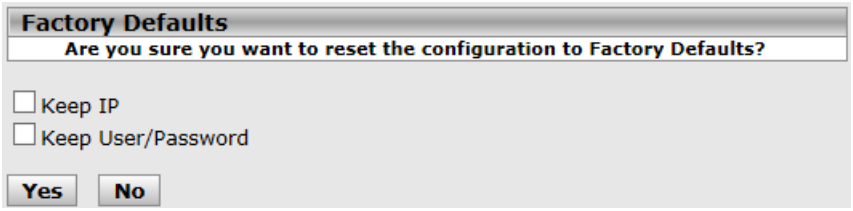



**PoE Auto Ping**

| Description | Factory default |
|---|---|
| **Ping Check** | |
| Specify the status of PoE Auto Ping.<br>• **Disable**: Disable the PoE Auto Ping.<br>• **Enable**: Enable the PoE Auto Ping, | Disable |
| **Port** | |
| This field displays the interface number. | *interface number* |
| **Ping IP Address** | |
| Entering the IP Address of the power device. | 0.0.0.0 |
| **Interval Time** | |
| Entering the Interval time to control switch sending alive-checking packets-, and the range is 10 second to 120 second. | 10 |
| **RetryTime** | |
| Specify the retry time if there is any connected device fail to response. | 1 |

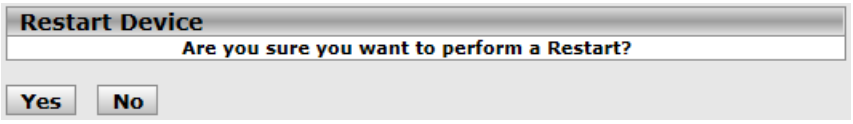
## 3.14 Factory Default

After you click the **Yes** button, the Delta PoE switch will be reset to the factory default values. You can select to keep IP address or login information (username/password).




## 3.15 System Reboot

After you click the **Yes** button, GUI will not be available until the switch completes the boot cycle. After the switch is reset, you need to re-login again.



**MEMO**

# Chapter 4 IEXplorer Utility Introduction

**Table of Contents**

Delta has many kinds of industrial products and network devices. If you have many Delta products, the IEXplorer utility can help you search them via one interface. The IEXplorer utility can search for IES series products, DVP series products and some Delta products which have extension communication cards. It can help you know the IP address of a device, modify the configuration, and upgrade the firmware.

The IEXplorer utility supports the following models:

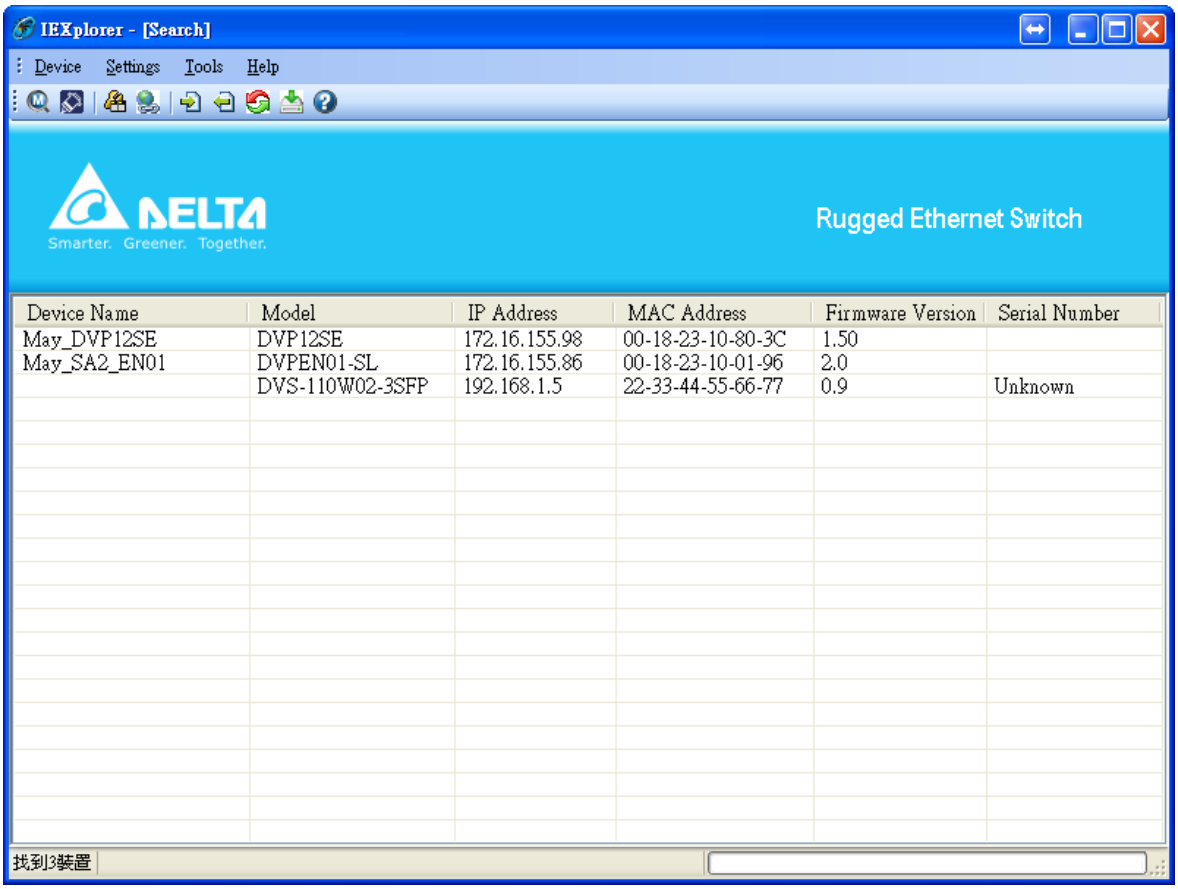
- DVS-108W02-2SFP
- DVS-109W02-1GE
- DVS-110W02-3SFP
- DVW-W02W2-E2
- IFD9506
- IFD9507
- RTU-EN01
- DVPEN01-SL
- DVP12SE
- DVP-FEN01
- DVPSCM12-SL
- DVPSCM52-SL
- ASDA-M
- CMC-MOD01
- CMC-EIP01
- DVS-G512W01-4GF

More models are coming soon.
Please download the new version from Delta official website (www.deltaww.com)
Compatible OS: Windows XP SP2, or Windows 7 (32/64 bits)

## 4.1 Starting the Configuration

After you finish the installation, you can find the IEXplorer icon on the desktop. Double-click the icon to run the program.


After double-clicking the icon, you can see the IEXplorer interface shown below:

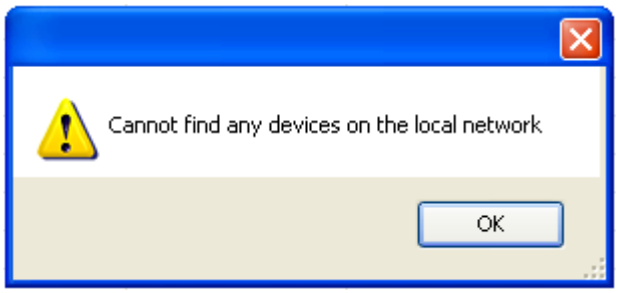



## 4.2 Device

There are three items on the **Devices** menu: Search, Virtual COM and Exit.


### 4.2.1 Search

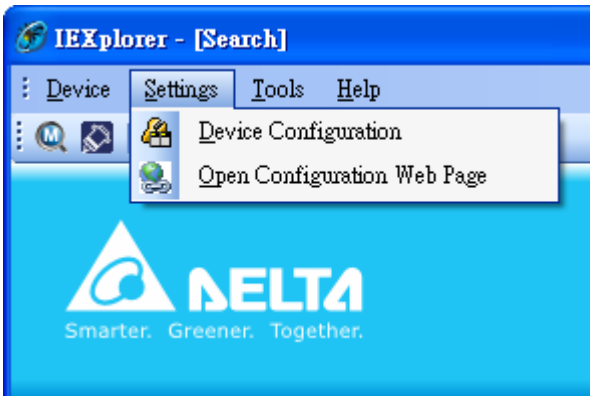
If the utility can not find any devices, the message box will pop up.




The automatic search function performs every 1 minute. If the device does not exist anymore, it will be moved from the list view.

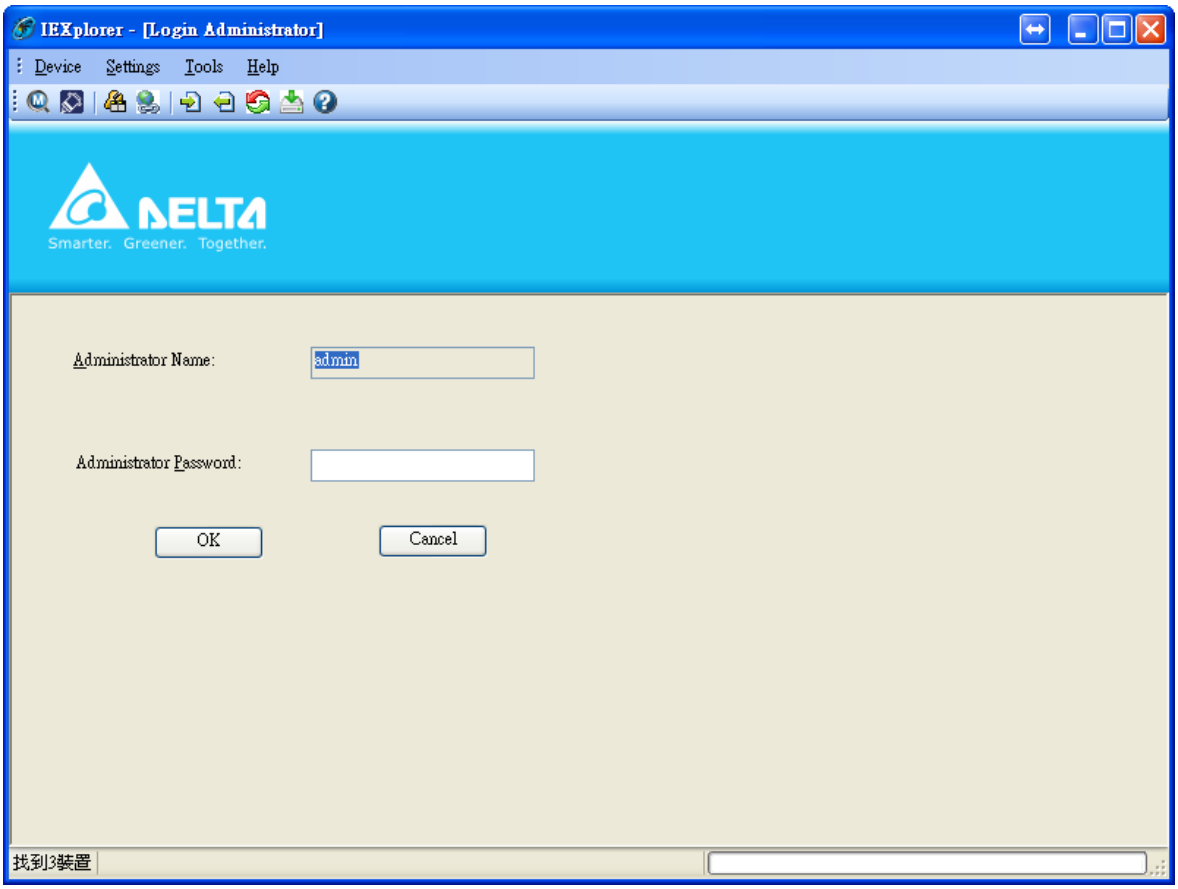
## 4.3 Settings

The IEXplorer utility provides two ways for users to configure the devices. You can configure the basic settings via **Device Configuration** or configure completely settings via **Open Configuration Web Page**. The **Settings** menu can be clicked only when you select DVS or DVW series products in the list view.

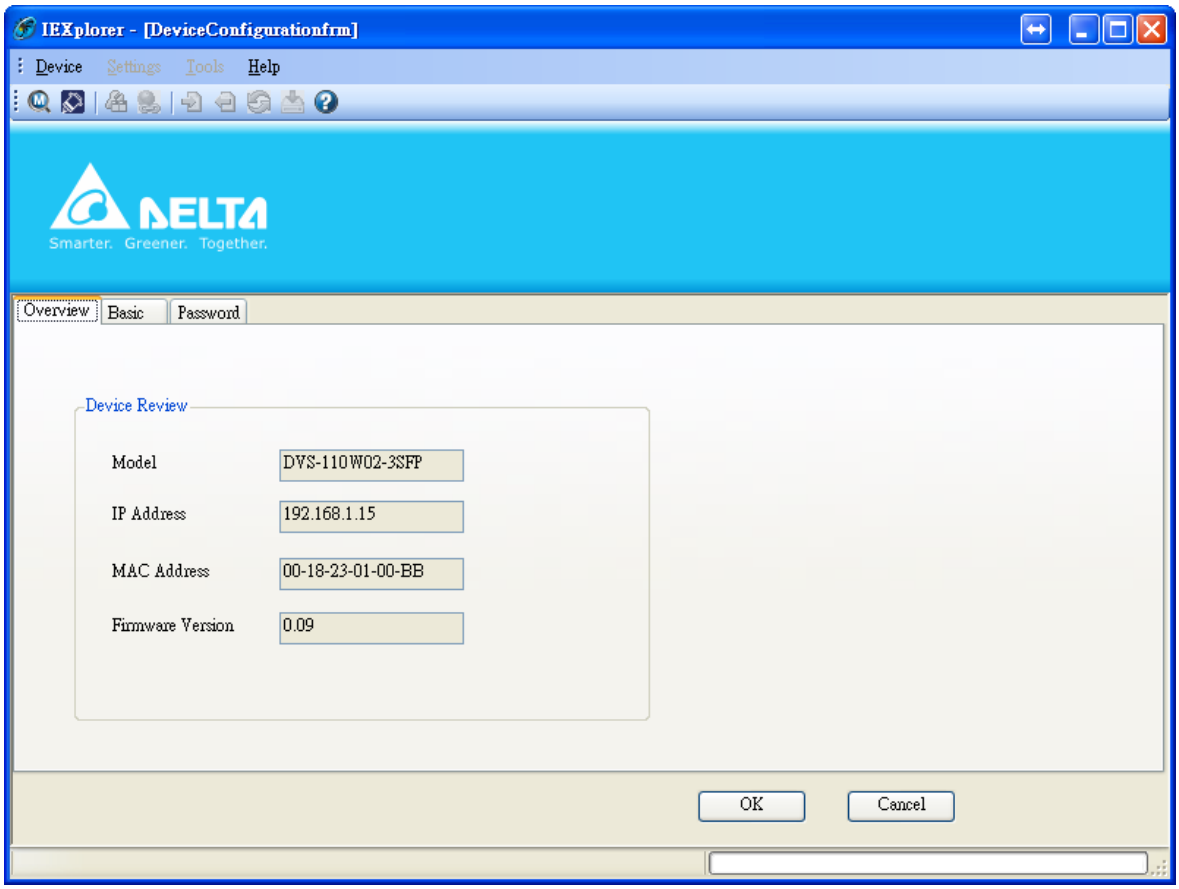



### 4.3.1 Device Configuration

The login ID and the password are the same as the web interface.




After the authentication progresses, the basic setting interface will display information, as shown below:

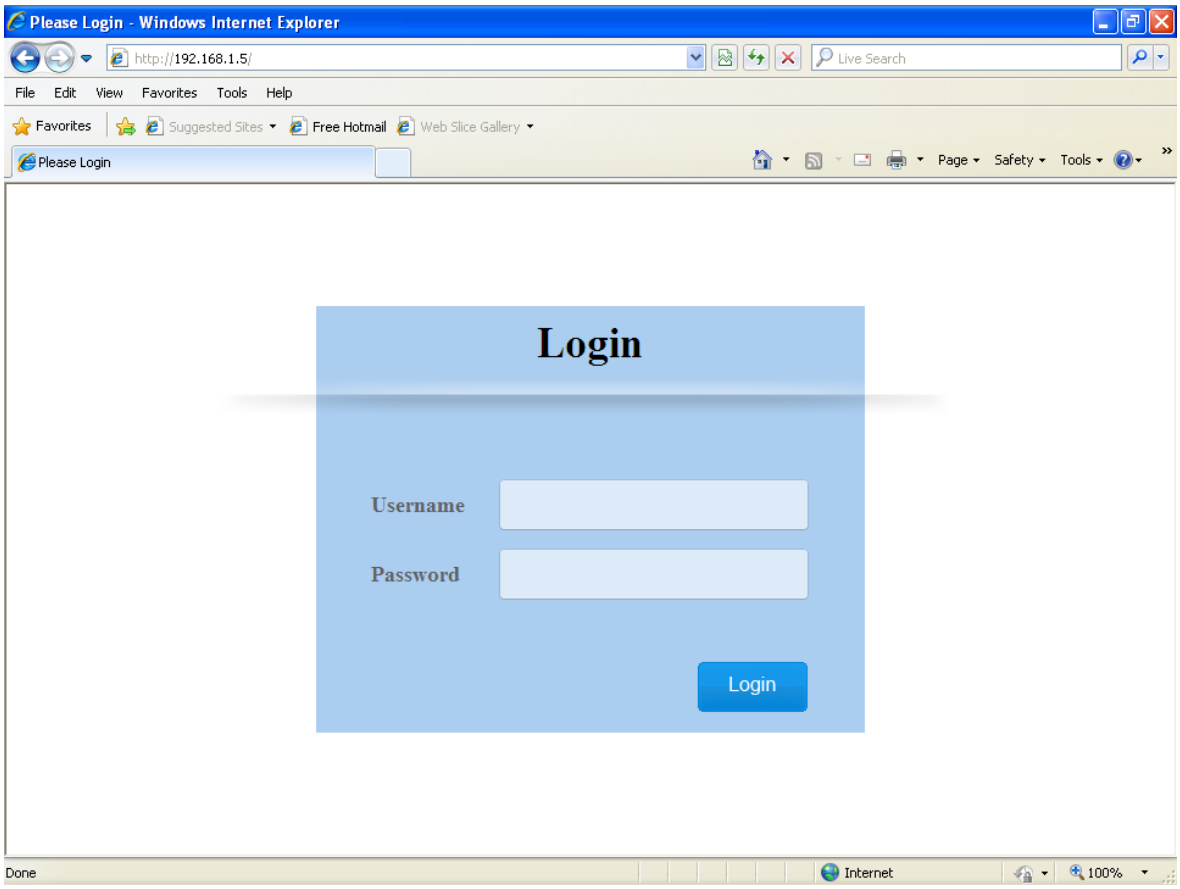



4

You can configure the device name and the IP information, modify the password, and reset the password to the factory default setting in this interface.

### 4.3.2 Configuration Web Page

If you click **Open Configuration Web Page**, the web interface will be displayed.



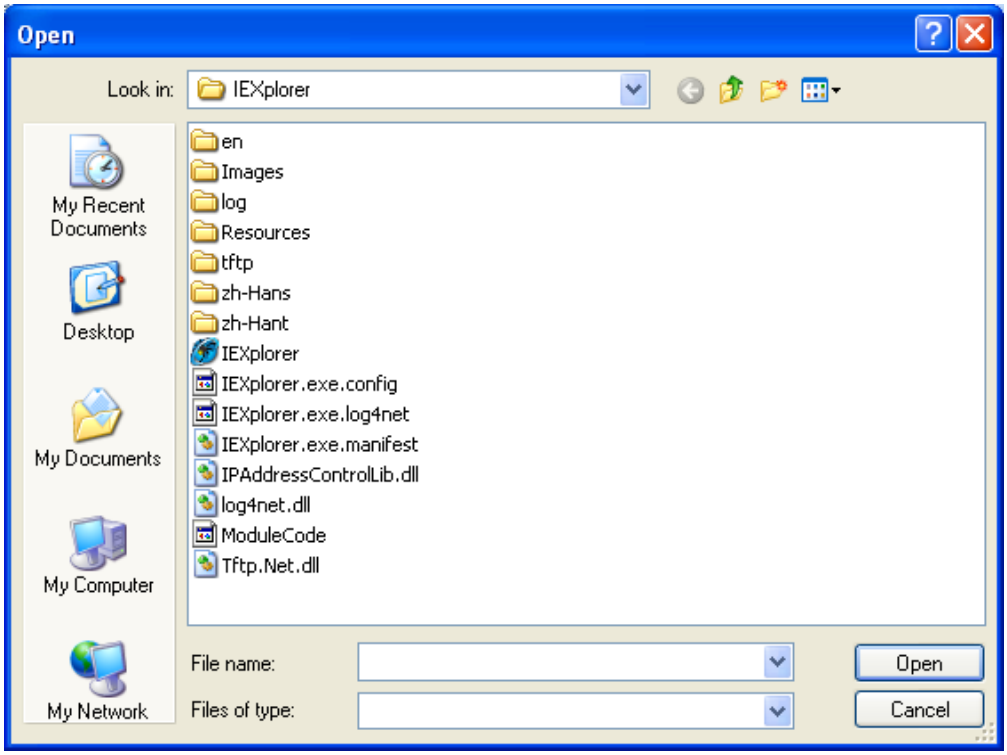

**Note:**
You can double-click the device in the list view to open the configuration web page. If the device which you select is not a DVS or DVW series device, the utility will start **DCISoft** for you to configure the device.

## 4.4 Tools

Please select the device before using the functions on the **Tools** menu.

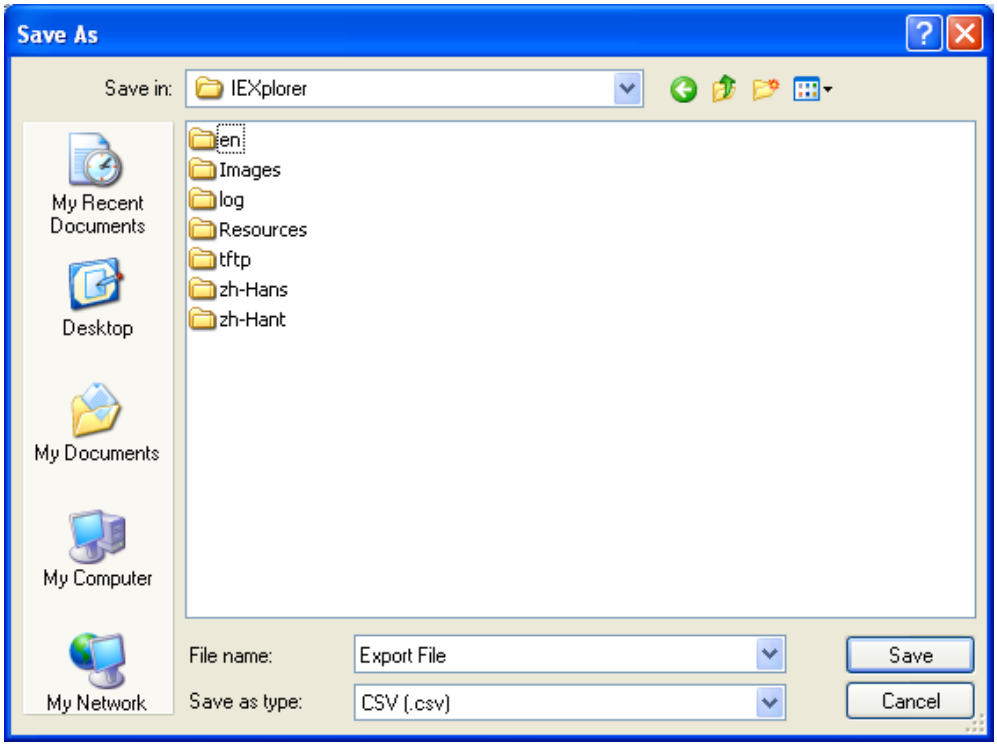
### 4.4.1 Parameter Import

After **Parameter Import** is clicked, a window will pop up for you to select a file imported to the device. Importing a file to multiple devices is supported.




### 4.4.2 Parameter Export

After **Parameter Export** is clicked, a window will pop up for you to select the path to export the file.

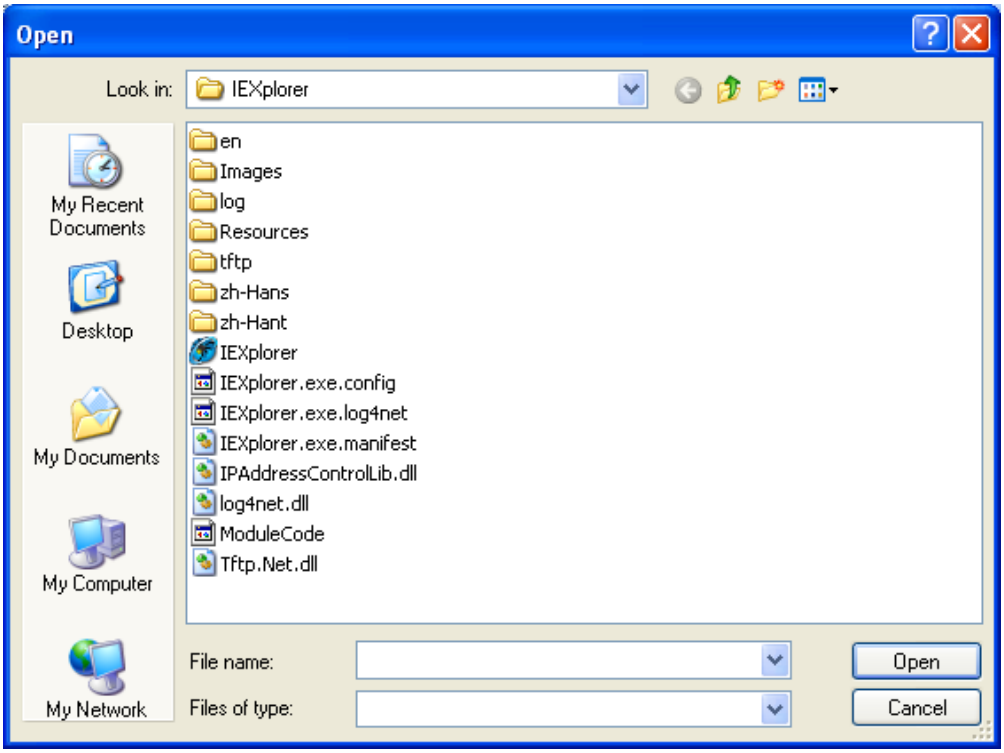


### 4.4.3 Device Reboot

IEXplorer allows you to reboot the device via the utility.

### 4.4.4 Update Firmware

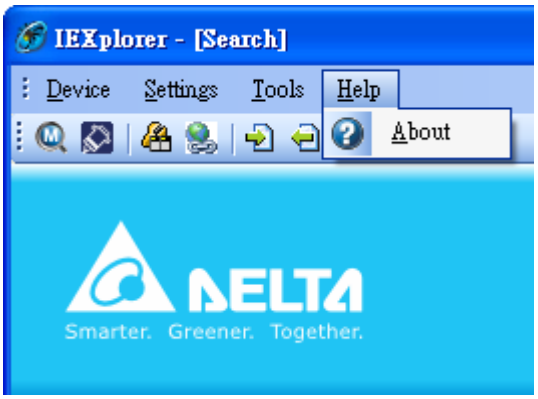
After you click **Update Firmware**, a window will pop up for you to select the firmware file.

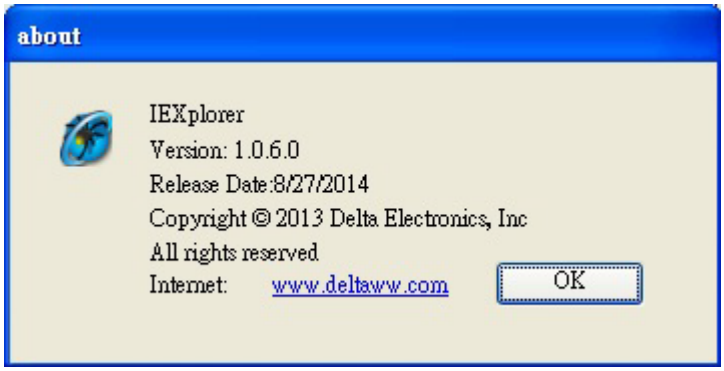



**Note:**
Before you click **Update Firmware**, you should choose the device that you want to update. If it is updated successfully, please wait for 3 minutes to log in again.

## 4.5 Help

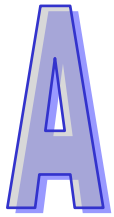
After **About** on the **Help** menu is clicked, an information message window of IEXplorer will pop up.




about
IEXplorer
Version: 1.0.6.0
Release Date:8/27/2014
Copyright © 2013 Delta Electronics, Inc
All rights reserved
Internet: www.deltaww.com
OK

4

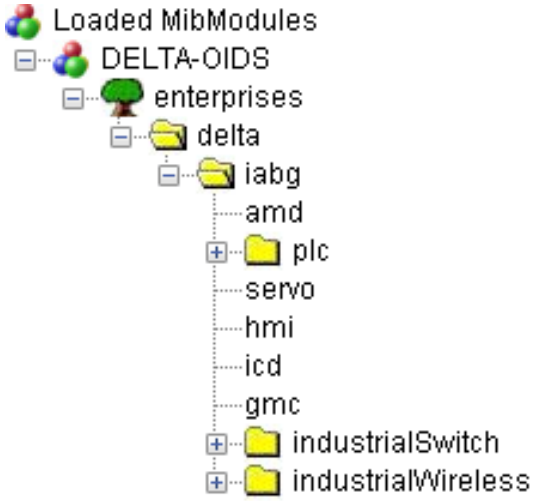
# Appendix A Private MIB Group



## Table of Contents

## A.1 Private MIB Group

Delta switch not only supports standard MIBs, but also provides private MIBs. You can use the SNMP tool to configure or monitor the switch's configuration. The private MIBs are the same as standard MIBs. It is displayed like a web tree. It's easily to be understood and used, so you don't need to learn or find where the OIDs of the commands are.
A private MIB can be found in the product CD if you need to use it.




We also support standard MIB Groups. For example, Interfaces Group, IP Group, TCP Group, UDP Group, and SNMP Group.

# Appendix B MODBUS TCP Map

## Table of Contents



## B.1 MODBUS TCP Map

| Address Offset | Data Type | Description |
|---|---|---|
| **System Information** | | |
| 0x0000 | 1 word | Reserved |
| 0x0001 | 1 word | Reserved |
| 0x0002 | 1 word | Reserved |
| 0x0051 | 1 word | Firmware Version<br>Hi byte = major<br>Lo byte = minor |
| 0x0010 | 20 words | Vendor Name = "Delta Electronics, Inc."<br>Word 0 Hi byte = 'D'<br>Word 0 Lo byte = 'e'<br>Word 1 Hi byte = 'l'<br>Word 1 Lo byte = 't'<br>Word 2 Hi byte = 'a'<br>Word 2 Lo byte = ' '<br>Word 3 Hi byte = 'E'<br>Word 3 Lo byte = 'l'<br>Word 4 Hi byte = 'e'<br>Word 4 Lo byte = 'c'<br>Word 5 Hi byte = 't'<br>Word 5 Lo byte = 'r'<br>Word 6 Hi byte = 'o'<br>Word 6 Lo byte = 'n'<br>Word 7 Hi byte = 'i'<br>Word 7 Lo byte = 'c'<br>Word 8 Hi byte = 's'<br>Word 8 Lo byte = ', '<br>Word 9 Hi byte = ' '<br>Word 9 Lo byte = 'l'<br>Word 10 Hi byte = 'n'<br>Word 10 Lo byte = 'c'<br>Word 11 Hi byte = '.'<br>Word 11 Lo byte = '\0' |
| 0x0030 | 20 words | Product Name = "DVS-G512W01-4GF"<br>Word 0 Hi byte = 'D'<br>Word 0 Lo byte = 'V'<br>Word 1 Hi byte = 'S'<br>Word 1 Lo byte = '-'<br>Word 2 Hi byte = 'G'<br>Word 2 Lo byte = '5'<br>Word 3 Hi byte = '1'<br>Word 3 Lo byte = '2'<br>Word 4 Hi byte = 'W'<br>Word 4 Lo byte = '0'<br>Word 5 Hi byte = '1'<br>Word 5 Lo byte = '-'<br>Word 6 Hi byte = '4'<br>Word 6 Lo byte = 'G'<br>Word 7 Hi byte = 'F' |
| 0x0055 | 3 words | Ethernet MAC Address<br>Ex: MAC = 00:11:22:33:44:55<br>Word 0 Hi byte = 0x00 |

| Address Offset | Data Type | Description |
|---|---|---|
| | | Word 0 Lo byte = '0x11<br>Word 1 Hi byte = 0x22<br>Word 1 Lo byte = 0x33<br>Word 2 Hi byte = 0x44<br>Word 2 Lo byte = '0x55 |
| **Port Information** | | |
| 0x1000 ~ 0x1007 | 1 word | Port 1 to 8 Status<br>0x0000: Link down<br>0x0001: Link up<br>0x0002: Disable |
| 0x1100 ~ 0x1107 | 1 word | Port 1 to 8 Communication Format<br>0x0000: 10M,Half<br>0x0001: 10M,Full<br>0x0002: 100M,Half<br>0x0003: 100M,Full<br>0x0004: 1G,Full |
| 0x1200 ~ 0x1207 | 1 word | Port 1 to 8 Flow Control<br>0x0000: OFF<br>0x0001: ON |
| 0x1400 ~ 0x148B | 20 words | Port 1 to 8 Description<br>EX: 10/100/1000TX,RJ45<br>Word 0 Hi byte = '1'<br>Word 0 Lo byte = '0'<br>Word 1 Hi byte = '/'<br>Word 1 Lo byte = '1'<br>Word 2 Hi byte = '0'<br>Word 2 Lo byte = '0'<br>Word 3 Hi byte = '/'<br>Word 3 Lo byte = '1'<br>Word 4 Hi byte = '0'<br>Word 4 Lo byte = '0'<br>Word 5 Hi byte = '0'<br>Word 5 Lo byte = 'T'<br>Word 6 Hi byte = 'X'<br>Word 6 Lo byte = ','<br>Word 7 Hi byte = 'R'<br>Word 7 Lo byte = 'J'<br>Word 8 Hi byte = '4'<br>Word 8 Lo byte = '5'<br>Word 9 Hi byte = '\0'<br>Word 9 Lo byte = '\0' |