3onedata

Make network communication more reliable

# TNS5500 & TNS5500D Series

# M12 Managed Industrial Ethernet Switch

# User Manual

**Version 1.0.0, Aug. 2017**

**www.3onedata.com**

# TNS5500 &TNS5500D series user manual

# Statement

Copyright Notice



Models covered by this manual:

- TNS5500-4GT-8T
- TNS5500-4GT-8POE
- TNS5500D-4GT-8T
- TNS5500D-4GT-8POE (This document takes this model as an example.)

Trademarks Notice



Agreement

As the product version upgrades or other reasons, this document is subject to change without notice. Unless other agreement, this document only as a guide to use. All statement, information and suggestion in this document, without warranty of any kind, either expressed or implied.

Revision History

| Version No. | Date | Reason |
|---|---|---|
| V1.0.0 | August, 2017 | Creating Documents |
| | | |

Notes

In reading this manual, please pay attention to the following symbols,

 Information necessary to explain

 Special attention

# Content

Chapter 1 Summarize ..... 1
1.1 Introduction ..... 1
1.2 Features ..... 1
Chapter 2 Hardware Description ..... 2
2.1 Panel Design ..... 2
2.2 Power Input ..... 4
2.3 Relay connection ..... 4
2.4 Console port ..... 5
2.5 Communication port ..... 6
2.6 LED Indicator ..... 7
2.7 Installation ..... 7
Chapter 3 Appearance and Dimension ..... 10
3.1 Appearance ..... 10
3.2 Dimension ..... 10
Chapter 4 Packing List ..... 12
Chapter 5 Network Configuration ..... 13
5.1 Configure PC's IP Address ..... 13
Chapter 6 WEB Management ..... 14
6.1 Configuration preparing ..... 14
6.2 System status ..... 15
6.3 Port Configuration ..... 16
6.3.1 Port Settings ..... 16
6.3.2 PoE Setting ..... 18
6.3.3 Bandwidth Management ..... 19
6.3.4 Storm Suppression ..... 20
6.4 L2 Features ..... 21
6.4.1 VLAN ..... 21
6.4.2 IGMP snooping ..... 25
6.4.3 Static Multicast ..... 26
6.5 QOS ..... 27
6.5.1 QOS Classification ..... 27
6.5.2 COS ..... 28
6.5.3 DSCP ..... 29
6.6 Redundancy ..... 31
6.6.1 Port Trunking ..... 31
6.6.2 Rapid Ring ..... 32
6.6.3 RSTP ..... 36

6.7 LLDP ..... 38
6.7.1 Parameter Configuration ..... 38
6.7.2 Neighbor Information ..... 39
6.8 Access Control ..... 39
6.8.1 User password ..... 39
6.8.2 DHCP Server ..... 41
6.8.3 MAC port lock ..... 41
6.9 Remote monitoring ..... 42
6.9.1 SNMP management ..... 42
6.9.2 Email Warning ..... 44
6.9.3 Relay Alarm ..... 45
6.10 Port Statistics ..... 47
6.10.1 RX frame statistics ..... 47
6.10.2 TX frame statistics ..... 48
6.10.3 Traffic Statistics ..... 48
6.10.4 MAC address table ..... 49
6.11 Diagnosis ..... 51
6.11.1 Mirror ..... 51
6.11.2 Ping ..... 52
6.12 Basic settings ..... 52
6.12.1 Logo information ..... 52
6.12.2 SNTP ..... 53
6.12.3 Device address ..... 54
6.12.4 System identification ..... 55
6.12.5 System File Upgrade ..... 56
6.12.6 Logout ..... 58

Chapter 7 Repair and Service ..... 59

7.1 Internet Service ..... 59
7.2 Make a call to our technical office ..... 59
7.3 Repair or Replace ..... 59

Appendix 1 Glossary table ..... 60

Appendix 2 Treatment of common problem ..... 62

# Chapter 1 Summarize

## 1.1 Introduction

TNS5500 & TNS5500D series are a high-end, high-performance and cost-effective M12 managed industrial Ethernet switch. The devices provide with 8 10/100Base-T(X) M12 ports (POE function is optional) and 4 10/100/1000Base-T(X) M12 ports. The Gigabit Ethernet interfaces with an optional bypass relay function. The switch supports Wall and 1U rack mount optional. The switches use M12 connectors to ensure tight, robust connections, and guarantee reliable operation against environmental disturbances, such as vibration and shock. The switch is designed for railway applications, such as rolling stock, and wayside installations. It comes with advanced management functions, such as SW-Ring, VLAN, Trunking, Quality of Service, Rate Control, LLDP, Port Mirroring, Fault Alarm, and Online Firmware Update. The unique SW-Ring$^{TM}$ redundant network patented technology brings you a smart redundancy for Ethernet.

Accorded with FCC, CE standards and industrial design requirements, it provides high-performance and high quality solutions for the construction of smart substation. Provided with one power supply input, one relay alarm output and -40~65℃ (POE) working temperature, it can satisfy all kinds of industrial network environment and can be widely applied in such areas as electric power, PIS (Passenger Information System), VSCS(video surveillance & control system) and CTCS (Chinese Train Control System).

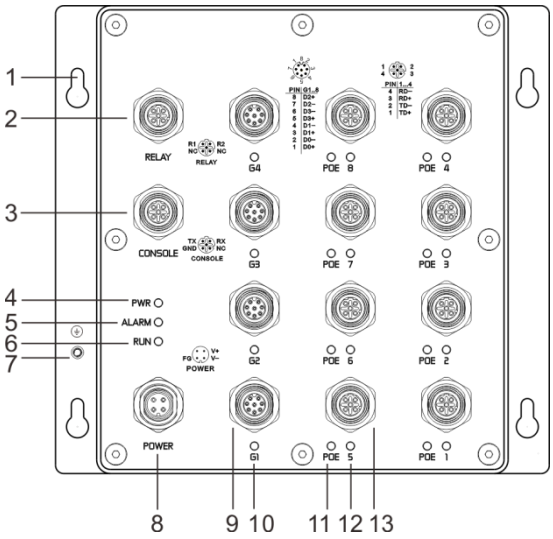
## 1.2 Features

- Supports IEEE802.3, IEEE802.3u, IEEE802.3x, IEEE802.3ab, IEEE802.1p, IEEE802.1Q, IEEE802.1D/W, IEEE802.3ad, IEEE802.3af/at
- Supports 8 10/100Base-T(X) M12 ports (POE function is optional), 4 10/100/1000BaseT(X) M12 ports with bypass
- Support SW-Ring$^{TM}$ ring network patent technology (Fault recovery time<20ms)
- Supports STP/RSTP for network redundancy
- Supports static multicast, IGMP Snooping and LLDP
- Supports Port based VLAN and IEEE802.1Q VLAN
- Supports QOS absolutely and opposite priority
- Supports WEB, SNMP and Telnet configuration
- Supports port Trunking, port mirroring and port frame statistics
- Supports one 110VDC（70-160VDC） input, and one relay alarm output
- 19” rack-mounted or Wall mounted

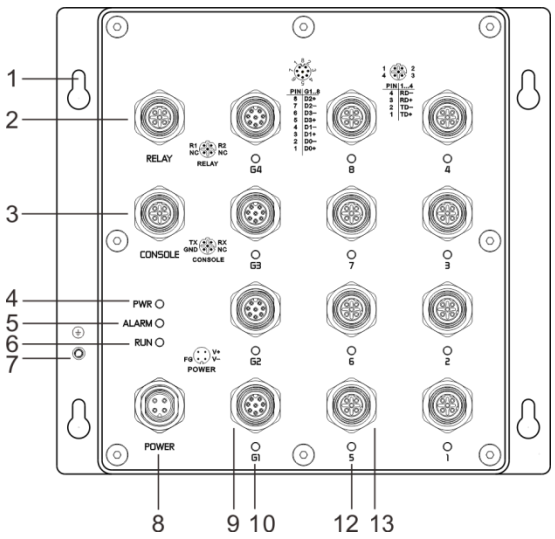
# Chapter 2 Hardware Description

## 2.1 Panel Design

**TNS5500D-4GT-8POE**

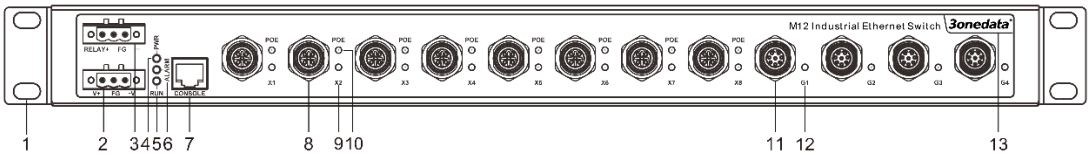



**TNS5500D-4GT-8T**




1. Screw holes for panel mounting kit
2. Relay output port
3. Console port
4. Power input indicator
5. Relay alarm indicator
6. System running indicator
7. Grounding screw
8. Power input port (male 4-pin M12 connector)
9. 10/100/1000Base-T(X) port (female 8-pin M12 connector with bypass function, 1-2, 3-4)
10. Gigabit Ethernet Link/ACT indicator (G1~G4)
11. PoE port Link indicator
12. Fast Ethernet Link/ACT indicator (1~8)
13. 10/100Base-T(X) port (female 4-pin M12 connector)

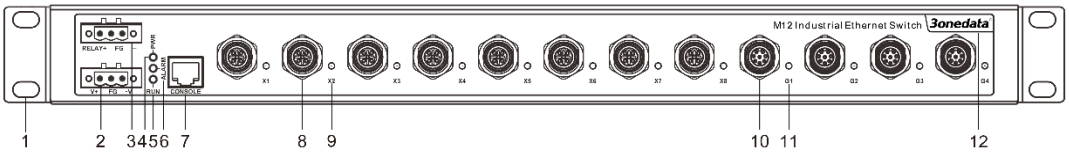
**TNS5500-4GT-8POE**




1. Rackmount ears
2. 3 bit terminal block for power input
3. 3 bit terminal block for relay output
4. Power indicator
5. System running LED

6. Relay alarm LED
7. Console port
8. 10/100Base-T(X) M12 Ethernet port
9. Fast Ethernet LINK/ACT LEDs
10. POE LEDs
11. 10/100/1000Base-T(X) M12 Ethernet port
12. Gigabit Ethernet LINK/ACT LEDs
13. 3onedata product identification

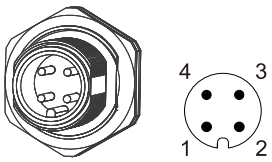
### TNS5500-4GT-8T




1. Rackmount ears
2. 3-pin terminal block for power input
3. 3-pin terminal block for relay output
4. Power indicator
5. System running LED
6. Relay alarm LED
7. Console port
8. 10/100Base-T(X) M12 Ethernet port
9. Fast Ethernet LINK/ACT LEDs
10. 10/100/1000Base-T(X) M12 Ethernet port
11. Gigabit Ethernet LINK/ACT LEDs
12. 3onedata product identification

## 2.2 Power Input

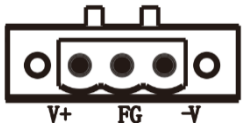
Wall mounting: (TNS5500D series)




| NO. | Signal | Description |
|---|---|---|
| 1 | FG | Shell ground |
| 2 | V- | Power input negative (-) |
| 3 | V+ | Power input positive (+) |
| 4 | NC | Reserved |

The product top panel provided power supply input M12 4-pin male a-coded connector, support DC input. Voltage input range is 110VDC（70-160VDC） (terminal block defined as: 1/FG, 2/V-, 3/V+).

1U Rack mounting: (TNS5500 series)




The product top panel provided 3 bit power supply input terminal block, support DC input. Voltage input range is 110VDC（70-160VDC） (terminal block defined as: V+, FG, and V-).

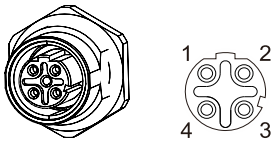
Important notice:

1. Power ON operation: first of all, insert power cable's terminal block into device's power port, then insert power supply plug into power source.

2. Power OFF operation: first of all, unpin power plug, then strike the terminal block, please take care of operation sequence.

## 2.3 Relay connection

Wall mounting: (TNS5500D series)




| NO. | Signal | Description |
|---|---|---|
| 1 | R1 | Relay output terminal R1 |
| 2 | R2 | Relay output terminal R2 |
| 3 | NC | Reserved |
| 4 | NC | Reserved |

Relay adopt M12 4-pin female d-coded connector in the top panel of the device. Between the two pin relay, as an open circuit state in normal non alarm state, when there is power alarm information to the closed state. The M12 two pin connector is used to detect network anomaly. The two wires attached to the fault

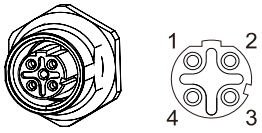
contacts form a closed circuit when the device port connection disconnect. The user can connect the relay to the lamp indicate or buzzer alarm to remind the relevant staff.

1U Rack mounting: (TNS5500 series)


Relay access terminals in the top panel of the device. Between the two terminals block relay, as an open circuit state in normal non alarm state, when there is power alarm information to the closed state. The two terminals block connector is used to detect network anomaly. The two wires attached to the fault contacts form a closed circuit when the device port connection disconnect. The user can connect the relay to the lamp indicate or buzzer alarm to remind the relevant staff.

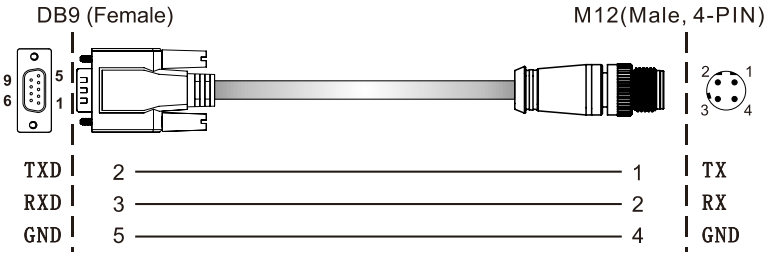
## 2.4 Console port

The Wall mounting series product provided 1pcs procedure test port based in serial port. It adopts RJ45 interface, located in top panel, can configure related command through RJ45 to DB9 female cable.

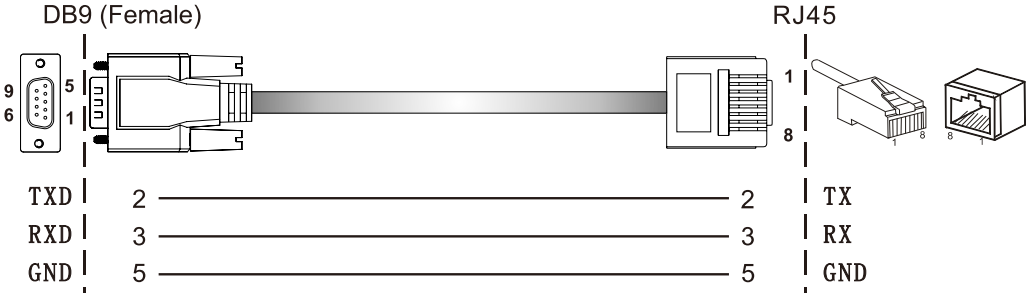



| NO. | Signal | Description |
|---|---|---|
| 1 | TX | Transmitted data |
| 2 | RX | Received data |
| 3 | NC | Reserved |
| 4 | GND | Signal ground |

M12 to DB9:



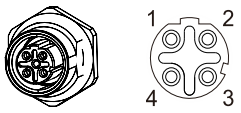

The rackmount series product provided 1pcs procedure test port based in serial port. It adopts M12 interface, located in top panel, can configure related command through M12 to DB9 female cable.



## 2.5 Communication port

### 10/100BaseT(X) Ethernet port

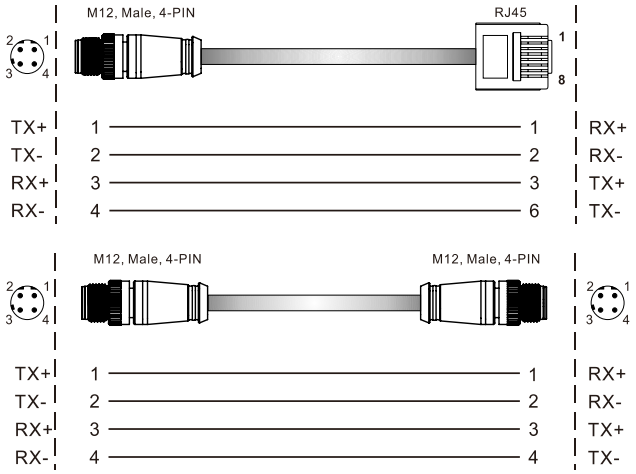
10/100Base-T(X) Ethernet port is used with M12 connectors that guarantee reliable operation against environmental disturbance, such as vibration and shock. M12 support automatic MDI/MDI-X operation that makes switch easy to user for customers without considering type of network cable. It can automatically configure itself to work in 10M or 100M state, full or half duplex mode.



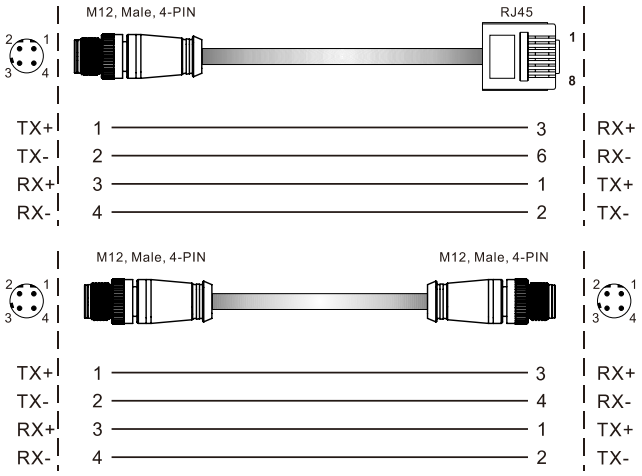

| NO. | Signal | Description |
|---|---|---|
| 1 | TD+ | Fast Ethernet Transmit Data+ |
| 2 | TD- | Fast Ethernet Transmit Data- |
| 3 | RD+ | Fast Ethernet Receive Data+ |
| 4 | RD- | Fast Ethernet Receive Data- |

You can user an M12-M12 or M12-RJ45 cable to connect the port for communication.

### 10/100Base-T(X) MDI (straight-through cable)

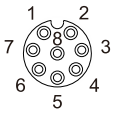



### 10/100Base-T(X) MDI-X (Cross over cable)



**10/100/1000BaseT(X) Ethernet port**

10/100/1000Base-T(X) Ethernet port is used with M12 connectors that guarantee reliable operation against environmental disturbance, such as vibration and shock. M12 support automatic MDI/MDI-X operation that makes switch easy to user for customers without considering type of network cable. It can automatically configure itself to work in 10M, 100M or 1000M state, full or half duplex mode.


| NO. | Signal | Description |
|---|---|---|
| 1 | BI_D0+ | Gigabit Ethernet Bidirectional Data 0+ |
| 2 | BI_D0- | Gigabit Ethernet Bidirectional Data 0- |
| 3 | BI_D1+ | Gigabit Ethernet Bidirectional Data 1+ |
| 4 | BI_D1- | Gigabit Ethernet Bidirectional Data 1- |
| 5 | BI_D3+ | Gigabit Ethernet Bidirectional Data 3+ |
| 6 | BI_D3- | Gigabit Ethernet Bidirectional Data 3- |
| 7 | BI_D2- | Gigabit Ethernet Bidirectional Data 2- |
| 8 | BI_D2+ | Gigabit Ethernet Bidirectional Data 2+ |

## 2.6 LED Indicator

LED indictor light on the front panel of product, the function of each LED is described in the table as below.

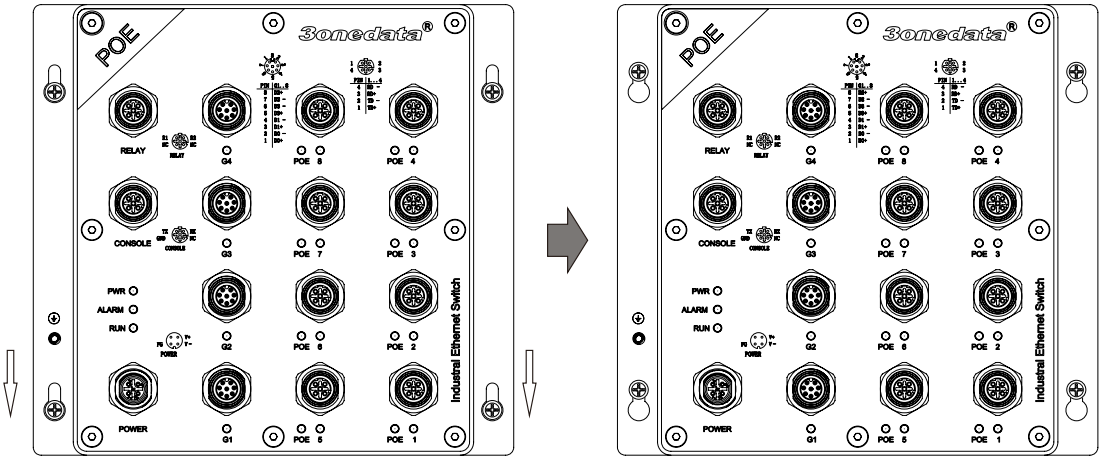
| **System indication LED** | | |
|---|---|---|
| **LED** | **State** | **Description** |
| **PWR** | ON | Power is being supplied to power input PWR input |
| | OFF | Power is not being supplied to power input PWR input |
| **RUN** | ON/OFF | System is not running well |
| | Blinking | System is running well |
| **ALM** | ON | When the alarm is enabled, the port's link is inactive. |
| | OFF | The port's link is active, the alarm is disabled. |
| **Link/ACT** (1~8/G1~G4) | ON | Port connection is active |
| | OFF | Port connection is not active |
| | Blinking | Data transmitted |
| **POE** (1~8) | ON | The PoE device is connected by IEEE802.3af/at standard |
| | OFF | No PoE power output or no PoE connected PoE devices |

## 2.7 Installation

Before installation, confirm that the work environment meet the installation require, including the power needs and abundant space. Whether it is close to the connection equipment and other equipment are prepared or not.

1. Avoid in the sunshine, keep away from the heat fountainhead or the area where in intense EMI.
2. Examine the cables and plugs that installation requirements.
3. Examine whether the cables be seemly or not (less than 100m) according to reasonable scheme.

4. Power: 110VDC（70-160VDC）power input
5. Environment: Working temperature: -40～75℃(POE: -40～65℃)
   Storage Temperature: -40～85℃
   Relative humidity: 5%～95%




**Wall Installation**

1. Mounting the TNS series to a wall requires 4 screws. Use the TNS series switch as a guide to mark the correct positions of the 4 screws.
2. Use the 4 screws in the panel mounting kit.
3. Do not screw the screws in all the way—leave a space of about 2 mm to allow room for sliding the TNS series switch between the wall and the screws.
4. Before tightening the screws into the wall, make sure the screw head and shaft size are suitable by inserting the screw through one of the keyhole-shaped apertures of the TNS series switch.
5. Once the screws are fixed in the wall, hang the TNS series switch on the 4 screws through the large opening of the keyhole-shaped apertures, and then slide the switch downwards. Tighten the four screws for added stability.

**Rack mount installation**

In most of industrial application, it is convenience to use rack mount installation, the step of installation is as follows:

1. Check if have rack mount installation tools and components (The package provided parts of components)
2. Check installation place strong or not, have the place to install the device or not.
3. Put the device into rack, aim at the screw hole of device and rack, fixed it in strong screw. Easy and convenience to operation.

**Wiring Requirements**

Cable laying need to meet the following requirements,

1. It is needed to check whether the type, quantity and specification of cable match the requirement before cable laying;
2. It is needed to check the cable is damaged or not, factory records and quality assurance booklet before cable laying;
3. The required cable specification, quantity, direction and laying position need to match

construction requirements, and cable length depends on actual position;

4. All the cable cannot have break-down and terminal in the middle;
5. Cables should be straight in the hallways and turning;
6. Cable should be straight in the groove, and cannot beyond the groove in case of holding back the inlet and outlet holes. Cables should be banded and fixed when they are out of the groove;
7. User cable should be separated from the power lines. Cables, power lines and grounding lines cannot be overlapped and mixed when they are in the same groove road. When cable is too long, it cannot hold down other cable, but structure in the middle of alignment rack;
8. Pigtail cannot be tied and swerved as less as possible. Swerving radius cannot be too small (small swerving causes terrible loss of link). Its banding should be moderate, not too tight, and should be separated from other cables;
9. It should have corresponding simple signal at both sides of the cable for maintaining.

# Chapter 3 Appearance and Dimension

## 3.1 Appearance

TNS5500D-4GT-8POE

TNS5500D-4GT-8T

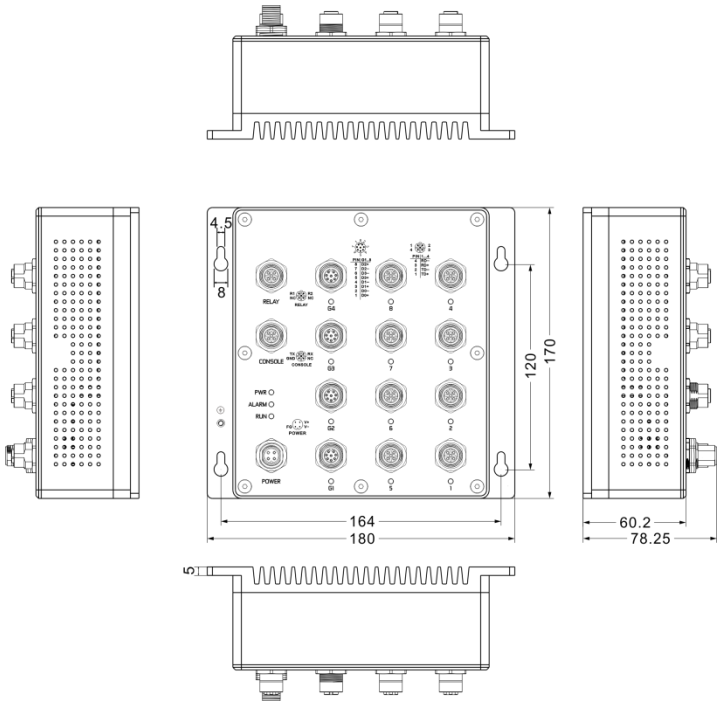
TNS5500-4GT-8POE

TNS5500-4GT-8T

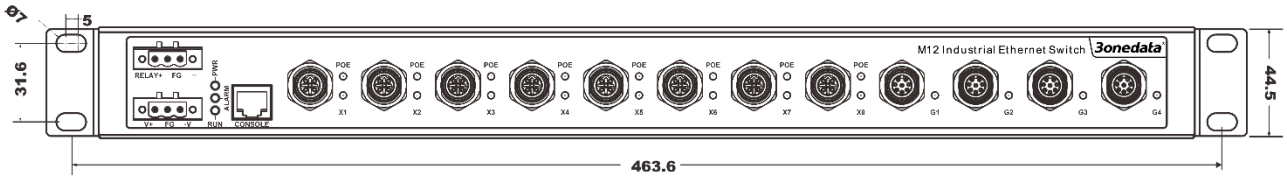
## 3.2 Dimension

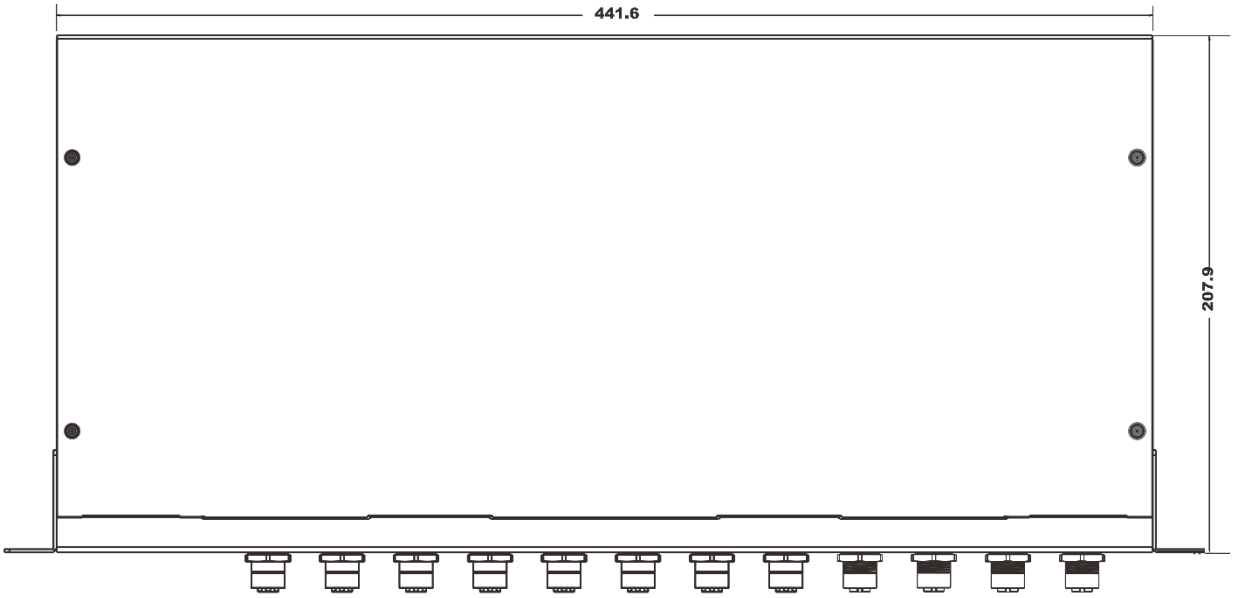
Unit (mm)

Wall mounting



1U rack mounting



# Chapter 4 Packing List

Please check the packaging and accessories by your first using. Please inform us or our distributor if your equipment have been damaged or lost any accessories, we will try our best to satisfy you.

| Description | Quantity |
|---|---|
| Industrial (PoE) switch | 1 |
| User manual | 1 |
| Documentation and software CD | 1 |
| Rackmount ears (1U rackmount switch) | 2 |
| Certificate of quality | 1 |
| Warranty card | 1 |

# Chapter 5 Network Configuration

The switch can access, configuration and management through WEB, the user manual will introduce the operations step by step.

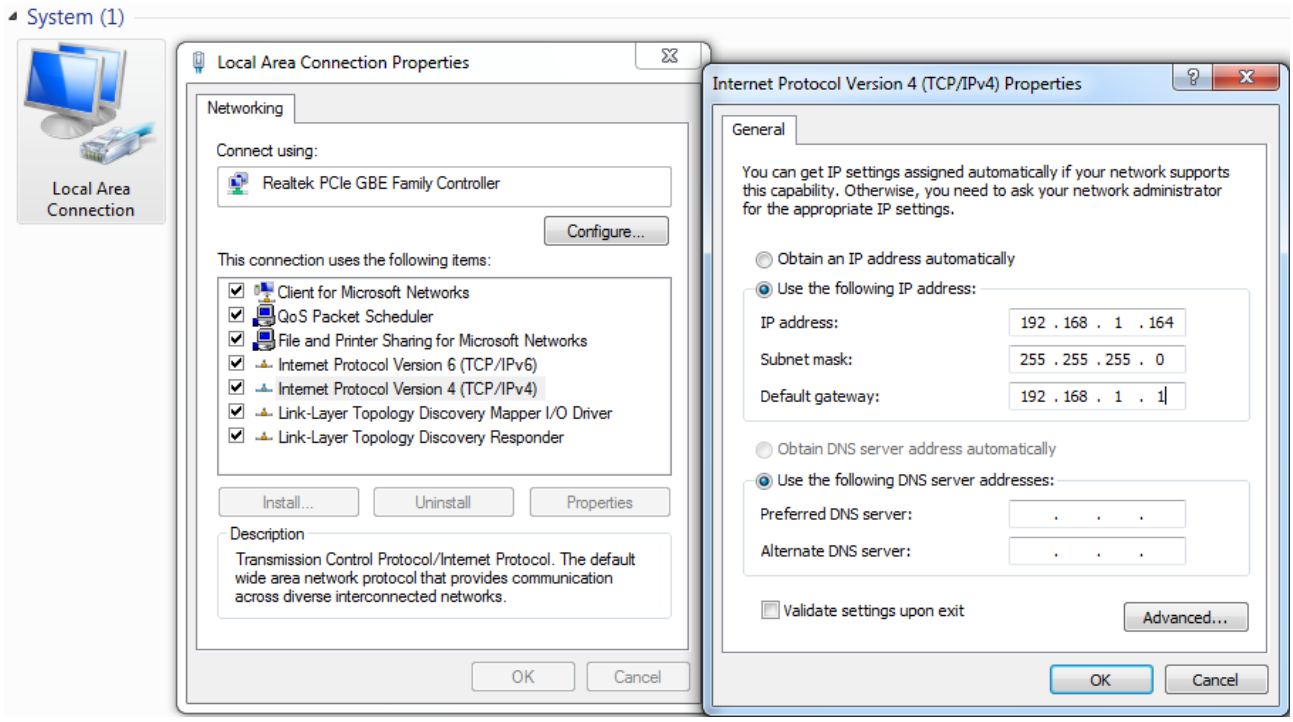
## 5.1 Configure PC's IP Address

The switch default address is: 192.168.1.254, subnet mask is: 255.255.255.0. When entering into switch Web interface through internet explorer, the IP address of switch and PC must be in the same Local Area Network.

You can modify PC's or switch's IP address to make sure that they are in the same Local Area Network. Operating process can follow method 1 or method 2 as below,

Method 1: Modify PC's IP address

- Click Start->Control panel->network connections->Local area Connection->Properties->Internet Protocol (TCP/IP) Setting PC's IP address: 192.168.1.X (X is less than 254, from 2 to 253).
- Click "OK", IP address modifies successfully




Method 2: Modify switch IP address through network manager software.

- Install manager software on the PC.
- Enter into network management interface; click "Search" to search the device.
- After searching the device, move mouse to the device, click right key, modify the device's IP address, Please make sure the device and PC in the same Local Area Network.

This configuration example does not use the Advanced button in the last picture. In one and the same network card allows the use of multiple IP pseudo-address when use the advanced configuration of the IP address, at which does not change the original address can still access the switch device. But in the IGMP polling and IEEE 802.1x polling windows system cannot handle correctly, Unix-like system does not have this problem. The advanced users have to pay attention to this issue.

# Chapter 6 WEB Management

The switch have WEB server inside, can manage and maintenance the device very intuitive through WEB interface.

## 6.1 Configuration preparing

1. The lowest requirement for user's computer is as below:

- Install operating system (Windows XP/2000,etc)
- Install Ethernet card
- Install Web explorer (IE6.0 or higher version)
- Install and start TCP/IP protocol

2. The default management IP address of the switch: 192.168.1.254, subnet mask as: 255.255.255.0. Before access to the configuration interface, the computer's IP address and the switch must be configured in the same subnet (IP address configuration, please refer to "5.1") if need local configuration; Computers and switches must be routed reach if for remote configuration.

**How to log on to Web Server**

Please type in the default IP of switch on the browser's address bar, and then will pop-up a window by clicking the "enter" key which shows you have to enter your user name and password. The default username and password is "admin". You can enter your username and password 3 times if you found the username and password is incorrect. If the 3 input error, the browser will display a "401 Unauthorized" error message. Refresh the page and then enter the correct user name and password, log on to the Web Server, it will recommend to modify the user name and password. Please contact our customer service center if you have more questions.


(Figure 6.1.1)

The default username and password is [admin],case sensitive for this series. The default password is with administrator privileges.

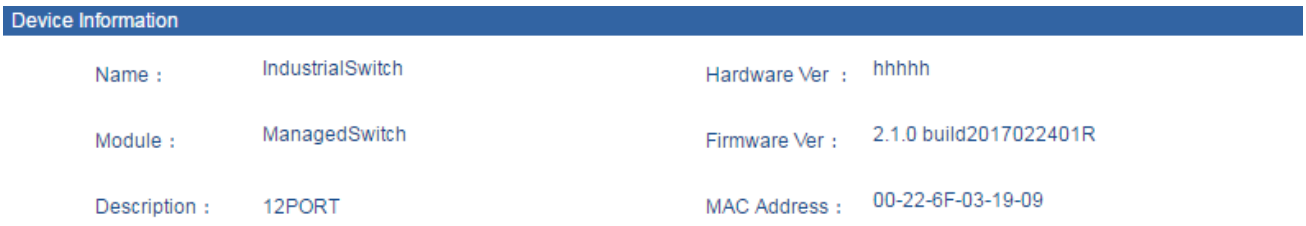
**Web Timeout Treatment**

The system timeout will cancel the login if the user did not login for a long time (The configuration of this login will be remained in the Web interface).

If user doesn't operate the Web interface for a long time, The system will be canceled this login.(but configuration change made in this login will be saved in Web configuration interface.). If the user wants to do any operating on Web configuration interface again, the system will remind user and returns to the login dialog box. Users need to log in again if operating is needed. The timeout time is 300s.

## 6.2 System status

### Device information




(Figure 6.2.1)

| Configuration Items | Description |
|---|---|
| Name | Network mark of the device. It is convenient for management tools to judge. |
| Serial No. | Serial number of the device. It is convenient for device management. |
| Description | Description of the product features. |
| Contact Information | Contact information of the operator for device maintenance. |
| MAC address | Hardware address of the device. It is a unique address which is made up of hexadecimal number with 48 bits (6 bytes) in length. |
| Hardware Version | Current hardware version. |
| Firmware Version | Current firmware version. |
| Current Time | Current time of the device. |
| Run Time | Run time after the device is powered on. When the device reboots, the time need to recalculate. |

**Time display**


(Figure 6.2.2)

**Port information**

Port Informatio

| Port Number | Link Status | Port Status | Speed | Interface Type |
|---|---|---|---|---|
| 1 | LOS | HALF | 10M | TX |
| 2 | LINK | FULL | 100M | TX |
| 3 | LOS | HALF | 10M | TX |
| 4 | LOS | HALF | 10M | TX |
| 5 | LOS | HALF | 10M | TX |
| 6 | LOS | HALF | 10M | TX |
| 7 | LOS | HALF | 10M | TX |
| 8 | LOS | HALF | 10M | TX |
| G1 | LOS | HALF | 10M | TX |
| G2 | LOS | HALF | 10M | TX |
| G3 | LOS | HALF | 10M | TX |
| G4 | LOS | HALF | 10M | TX |

(Figure 6.2.3)

If the port is connected properly the status should be LINK, no connection status will be LOS.

## 6.3 Port Configuration

### 6.3.1 Port Settings

The port configuration interface mainly include port type (Electric port or optical port), setup speed mode and duplex mode, flow control. Only when the port is enabled for the port speed, duplex, flow control will work. Select auto-negotiation, speed, duplex auto-negotiation.

Port Setting

| Port | Type | Speed | Duplex | Enable | Flow Control | MDI/MDIX |
|---|---|---|---|---|---|---|
| * | ---- | < > | < > | ☐ | ☐ | * |
| 1 | TX | Auto | Full Duplex | ☑ | ☐ | Auto |
| 2 | TX | Auto | Full Duplex | ☑ | ☐ | Auto |
| 3 | TX | Auto | Full Duplex | ☑ | ☐ | Auto |
| 4 | TX | Auto | Full Duplex | ☑ | ☐ | Auto |
| 5 | TX | Auto | Full Duplex | ☑ | ☐ | Auto |
| 6 | TX | Auto | Full Duplex | ☑ | ☐ | Auto |
| 7 | TX | Auto | Full Duplex | ☑ | ☐ | Auto |
| 8 | TX | Auto | Full Duplex | ☑ | ☐ | Auto |

(Figure 6.3.1)

| Configuration Items | Description |
|---|---|
| Port | Port name, corresponding to mark in panel. |
| Type | Display port type (TX or FX). |
| Speed | Display configurable speed of port or auto-negotiation mode. |

| Configuration Items | Description |
|---|---|
| Duplex | Auto-negotiation (AUTO), full duplex (FULL), half duplex (HALF) optional, default mode is auto-negotiation mode. |
| Enable | Configurable ports enable or disable. Selecting square frame is for enable the corresponding port. It cannot transmit data if any port disable. The default is “Enable”. |
| Flow Control | Whether selecting flow control to the port. Only can selecting flow control when the port enable. The default is off. |

The described Electric port is the common network device RJ-45 port, commonly known as "crystal head", it's is a twisted-pair Ethernet interface type. This interface can be used in 10Base-T, 100Base-Tx and 1000Base-Tx Ethernet, transmission media is twisted pair, but according to different bandwidth media have different requirements, in particular, 1000Base-Tx Gigabit Ethernet connection, at least to use cat5e.

**Port Speed**

Port speed shows the connecting speed of the port. It includes 3 kinds of speed: 10M, 100M and auto-negotiation.

10M uses 10base-T standard and UTP cable for connection. When the port is in 10M speed, Link/Act indicator will blink continuously while data transmitting and status indicator of 10M/100Mbps will stay OFF.

100M uses 100Base-TX standard and UTP/STP cable for connection. When the port is in 100M speed, Link/Act indicator will blink continuously while data transmitting. 100M fiber port uses 100Base-FX standard and single/multi-mode fiber for connection. Main fiber of 100Base-FX standard includes: 62.5nm multi-mode fiber and 50nm multi-mode fiber. Auto-negotiation includes 2 kinds of speed according the capability of the other end: 10M and 100M.

**Port Enable**

This item provides a device to enable/disable the port. When choosing disable, the device would cut off power supply of this port. Even if other device is connected to this port, all status indicators of this port are OFF. Only enable this port, all settings about this port will be valid. This item provides a kind of safety mechanism to protect the port from illegal use. It is not allowed to disable all the ports.

**Duplex Mode**

Full duplex of the switch means switch can transmit and receive data at the same time. Half duplex of the switch means switch can transmit or receive data in a certain time. Generally the speed will choose auto-negotiation so that the port can automatically judge the connection type of the device connected to it and automatically adjust the connection type to ensure the maximum compatibility.

**Flow Control**

Flow control is used to prevent the frames from discard while port is blocked. This method is to send back the blocking signal to its original address while sending or receiving buffer area start to overflow. It limits the abnormal flows into a certain range. Flow control can be effective in preventing large amounts of data in the network instant impact on the network to ensure the efficient and stable user network running.

**Two types of flow control:**

1. In the half duplex mode, flow control is through back pressure. It is to send a jamming signal to the transmission source to reduce transmission speed.

2. In the full duplex mode, flow control generally follow IEEE 802.3x standard. Switch sends "pause" to information source to pause its sending information.

Use flow control to control the data flow between the sending and receiving nodes, can prevent packet loss.

**Polarity (MDI/MDIX auto-negotiation)**

MDI-II (Medium Dependent Interface- II mode), is a kind of standard built by IEEE for RJ-45 UTP cable of fast Ethernet 100BASE-T. II stands for parallel configuration. MDI-X (Media Dependent Interface-x mode) and MDI- II is a kind of standard built by IEEE for RJ-45 UTP cable of fast Ethernet 100BASE-T. X stands for crossover configuration.

### 6.3.2 PoE Setting

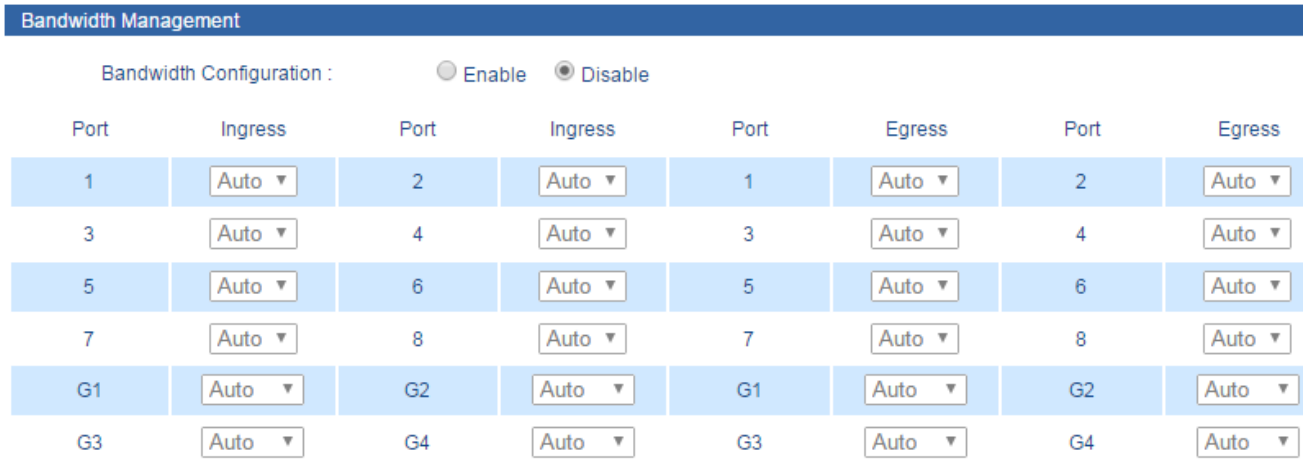
This setting is not supported for non-POE products.

PoE setting, also known as PoE management, can be through the web interface of PoE port function of corresponding operation and view port status, current value, voltage, power, but also can set the maximum power, PoE total power (1-240W) and port corresponding to the power value is: 10W, 15W, 30W. Each port output maximum power is 30W. Off / POE port function is enabled, and set port PoE priority (in limiting the total power allocation by priority power. If there is no priority setting, in the setting of the total power set value must be greater than enabled the sum of the port are arranged corresponding to the maximum power, set PoE total power should be set larger than enabled PoE port setting maximum power sum of 3 - 5W, PoE power restore factory settings default PoE can enable)


(Figure 6.3.2)

### 6.3.3 Bandwidth Management

The device provides port based speed limitation, including ingress and egress limitation. User can limits communication flow of each port and quits the flow limitation of the port. User can choose a settled speed, the range is: 64Kbps ~ 100Mbps. The type of port limitation includes all unicast, multicast and broadcast. When the port speed reaches the appointed speed, the device will enable or disable flow to limit the transmitting speed or receiving speed by flow control or discard the message.




(Figure 6.3.3)

The device provides both ingress and egress speed limitation. The ingress speed refers to the actual speed from PC and other devices to the switch. The egress speed refers to the actual speed from the switch to other devices. If ingress and egress speed of the connecting port between two devices are limited at the same time, the actual speed will be the smaller value.

For example, Port 1 limits the ingress speed only, the maximum speed of this port is 20M, Port 5 limits both egress and ingress speed, the maximum speed of this port is 50M

1. Please enable flow control when using port speed limitation.
2. When using speed limitation, it will not discard the packet unless the flow control disable.
3. Port speed limitation need cables with high quality, otherwise it will cause a lot of conflict packets and incomplete packets.

### 6.3.4 Storm Suppression

Broadcast storm is the accumulation of broadcast and multicast traffic on a computer network. Extreme amounts of broadcast traffic constitute a broadcast storm. A broadcast storm can consume sufficient network resources so as to render the network unable to transport normal traffic.

Storm Suppression

| Port | Broadcast (*62.5 kbps) | Un-multicast (*62.5 kbps) | Un-unicast (*62.5 kbps) | Enable |
|---|---|---|---|---|
| 1 | 160 | 160 | 160 | ☑ |
| 2 | 160 | 160 | 160 | ☑ |
| 3 | 160 | 160 | 160 | ☑ |
| 4 | 160 | 160 | 160 | ☑ |
| 5 | 160 | 160 | 160 | ☑ |
| 6 | 160 | 160 | 160 | ☑ |
| 7 | 160 | 160 | 160 | ☑ |
| 8 | 160 | 160 | 160 | ☑ |

（Figure 6.3.4）

There are many reasons to cause broadcast storm. For example: a redundant or incorrect connect among switches.

If enable storm suppression, it can stop the attack. Our device can detect 3 kinds of broadcast messages according to the type of broadcast storm.

Broadcast packets: data frame of the destination address of FF-FF-FF-FF-FF-FF

Multicast packets: destination address is XX-XX-XX-XX-XX-XX data frames, second x is odd numbers such as 1, 3, 5, 7, 9, b, d, and f, x represents any digit.

Unicast: unicast is the term used to describe communication where a piece of information is sent from one point to another point. In this case there is just one sender, and one receiver.

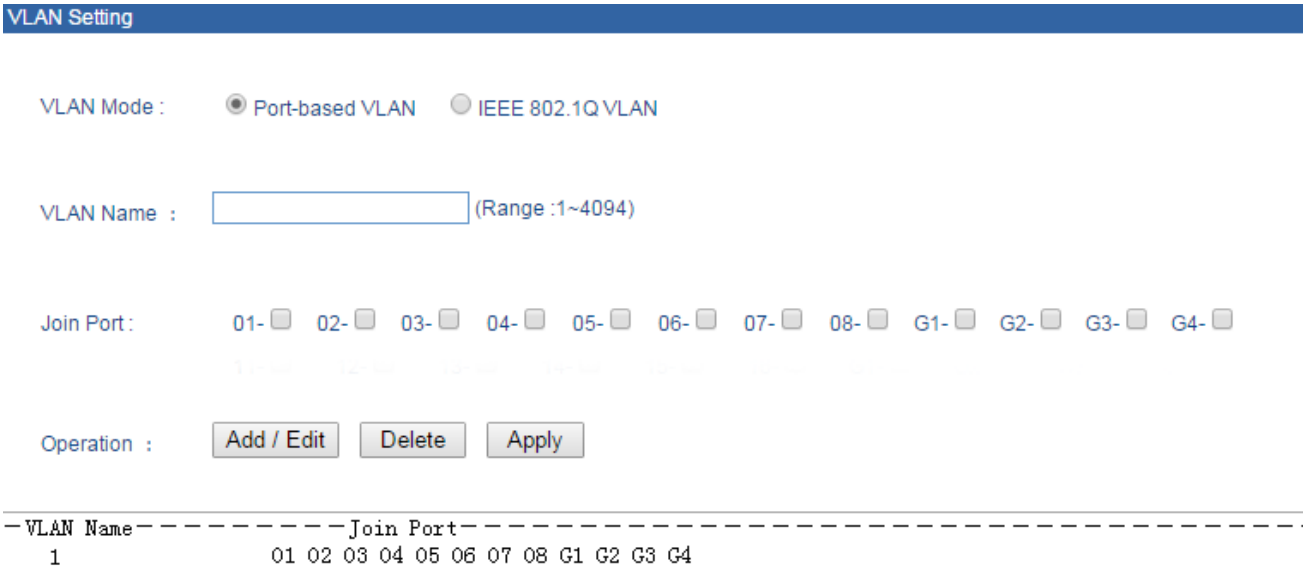
Destination lookup failure frame: the MAC address of this data frame doesn't exist in inside index. It needs to transmit to all the ports, including unicast and multicast flow.

1. The maximum length of Ethernet data frames is 1518 bytes, and each 64Kb of data communication includes about 6 Ethernet data frames with 1518-byte.
2. The minimum length of Ethernet data frames is 64 bytes. Each 64 Kb of data communication includes about 128 Ethernet data frames with 64-byte.
3. In the network the broadcast packets are more than 800packet/s, the network delay is obvious.
4. The recommended setting is 3% based on the above theory.
5. Please be caution to use MAC control frame and destination lookup failure frame, disabling IGMP Snooping will have impact on the transmission of the multicast.

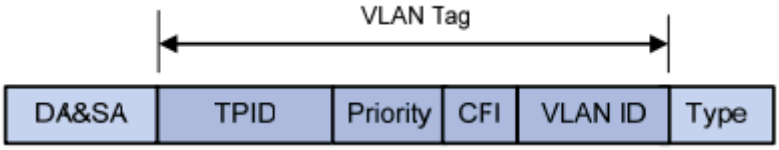
## 6.4 L2 Features

### 6.4.1 VLAN

The switch supports based on 802.1Q VLAN. It deals with messages based on Tag of recognized message (including 802.1p priority and VLAN ID, etc.).




Frames with 802.1q add 4 byte Tag based on Ethernet frames, including 2 byte TPID, 3 byte Priority, 1 byte CFI and 12 byte VLAN ID.




**TPID:** a 16-bit field set to a value of 0x8100 in order to identify the frame as an IEEE 802.1Q-tagged frame.

**Priority:** It indicates the frame priority level. Values are from 0 (best effort) to 7 (highest); 1 represents the lowest priority.

**CFI:** a 1-bit field. If the value of this field is 1, the MAC address is in non-canonical format. If the value is 0, the MAC address is in canonical format.

**VLAN ID:** a 12-bit field specifying the VLAN to which the frame belongs. The hexadecimal values of 0x000 and 0xFFF are reserved. All other values may be used as VLAN identifiers, allowing up to 4,094 VLAN.

**1. The type of port's Line**

The switch support 2 type port line:

**Access:** Port belongs to 1 VLAN, normally, it used for connecting user device, default all port is access port.

**Trunk:** Port belongs to some VLAN, can transmit and receive some VLAN message, normally, it used for connection of network device.

**2.** Deal with transmit and receive message

| Type | Receive message | |
|---|---|---|
| | Message did not take Tag | Message take Tag |
| Access | Put the VLAN tag point to Port default VLAN ID for message | Put the VLAN tag point to Port default VLAN ID for message |
| Trunk | Put the VLAN tag point to Port default VLAN ID for message | Keep up VLAN ID, no need replace |

| Type | Transmit message |
|---|---|
| Unmodify | Did not modify when transmit, the data packet is the same as enter into switch |
| Untagged | Did not take the mark when transmit |
| Tagged | Take the mark when transmit |

**Unmodify:** No need to modify original VLAN mark

**Untagged:** It is a normal Ethernet message

**Tagged:** Added a 4 bytes VLAN information after original MAC address and destination MAC address

**3. Parameter item description**

| Item | Description |
|---|---|
| PVID | Port's LAN ID, value range : 1～4095 |
| VID | VLAN ID number, value range: 1～4095 |
| Power type | Include Access and Trunk |
| Member type | Unmodify, Untagged, Tagged |
| Modify all | Quickly modify the type of all members at the same time |
| Add | Add the configurated VLAN into VLAN table |
| Delete | Choice one VLAN in the table, knock<Delete>, delete VLAN |

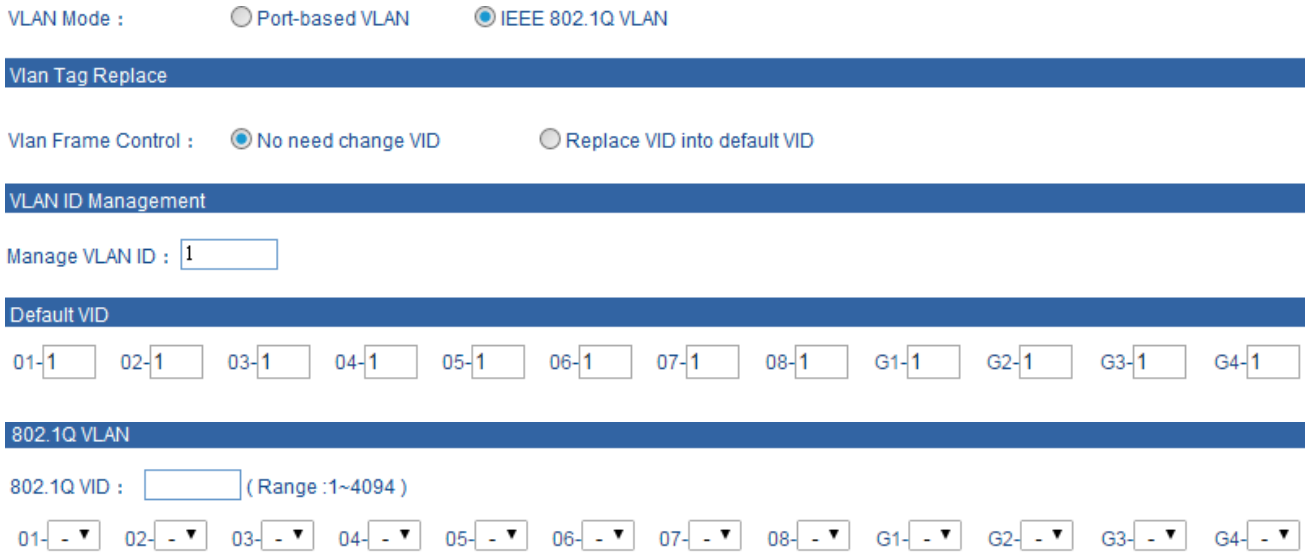
The default VLAN, all port are Access, PVID: 1, all belong to the members of VLAN1

**4. Create VLAN**

The step is as follows:

1. Enter into VLAN configuration interface, firstly select port type, Access or Trunk;
2. Input the default PVID of the port in [PVID] text box;
3. Input appointed VLAN into [VID] text box;
4. Set up members' type of each port: Unmodified, Untagged, Tagged
5. Click [Add] button, add VLAN items into the table and click [Apply] and reboot the device. Then creating new VLAN is finished.

As follow figure 6.4.1, create VLAN1, port type: Access, member type: Untagged, member included CPU port and port 1~4. Create VLAN2, type of port 5, 6: Access, member type: Untagged,type of port 7, 8: Trunk, member type: Tagged.



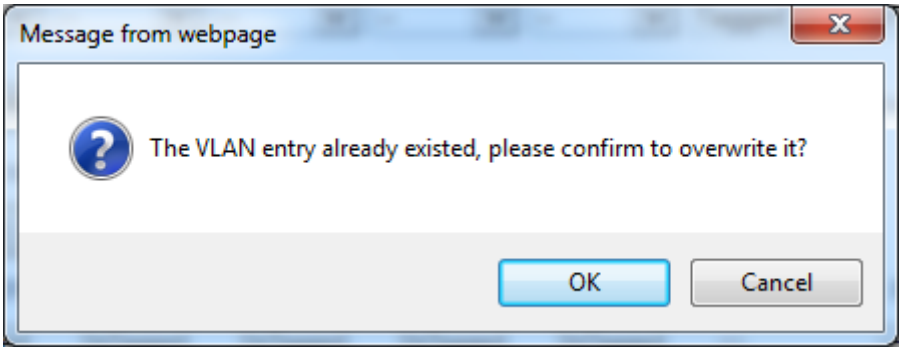

(Figure 6.4.1)

We can know the type of port 7, 8 is Trunk, can allow the data of VLAN 1 and VLAN 2 pass.

**5. Modify VLAN**

It can re-configure existing VLAN including modifying member's type and quantity of the port. Steps are as follows:

1. Enter into VLAN configuration interface, firstly select VLAN items which need to modify in VLAN item table, like as VLAN 1.
2. Member's type of VLAN1 shows in current VLAN item setting and set up member's type of the port according to the steps for creating new VLAN.
3. Click [Add] button, select [OK] when reminds whether overwrite it as shown in Figure 6.4.2. Add new VLAN items into table and click [Apply] and reboot the device. Modify VLAN finished.

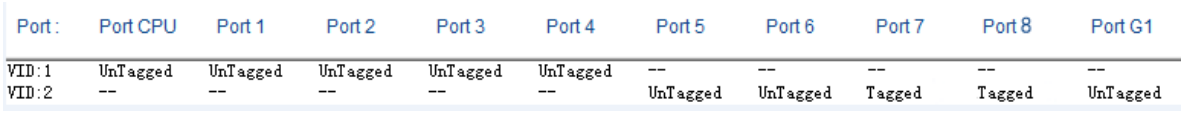



(Figure 6.4.2)

### 6. Delete VLAN

Steps of remove VLAN are as follows:

1. Firstly select VLAN items which need to remove, like as VLAN2;
2. After selected, click [Delete], then [Apply]. As shown in Figure 6.4.3:

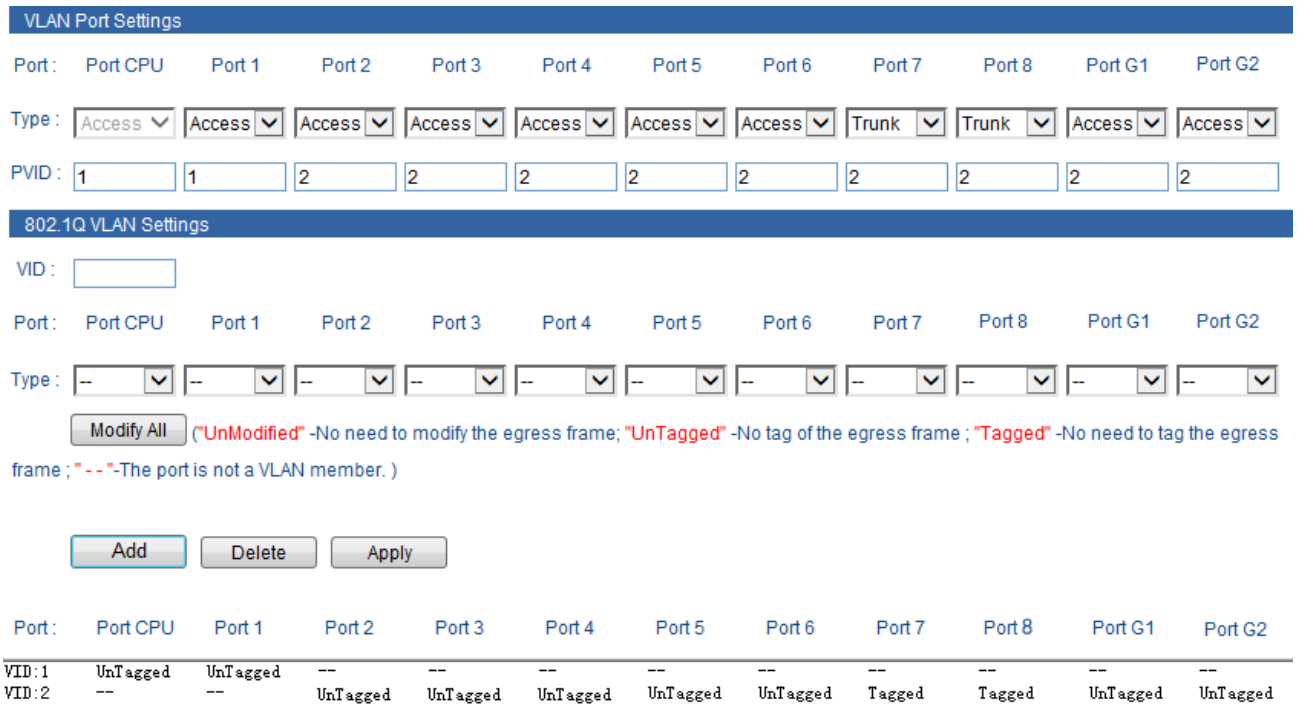



(Figure 6.4.3)

### 7. VLAN Configuration of Single Ring

1. Need to set one port as managed port, managed port and CPU port must in a same VLAN, figure as 6.4.4, port 1 is managed port.

2. The port that already set in ring network port, the VLAN port type must Trunk and take Tag, figure as 6.4.4.




(Figure 6.4.4)

### 8. Typical VLAN Configuration

Suppose switch's port 3, 4, 5 satisfied to the requirements as follows: port 3 can intercommunicate with Port 5, Port 4 can intercommunicate with Port 5, Port 3 can's intercommunicate with Port 4, How to set VLAN? (Not consider the configuration of other VLAN)

Let's analyse at first, port 3 can intercommunicate with Port 5, the port must belong to a same member of VLAN, the same, Port 4 can intercommunicate with Port 5, the port must belong to a same member of VLA, port 3 and port 4 belongs to different VLAN, figure as 6.4.5

1. Port 3's PVID: 2, Port 4's PVID: 3, Port 5's PVID: 4, port type are both Access.
2. Add VLAN2, VLAN3, VLAN4, the member is 3 and 5, 4 and 5, 3,4 and 5. Port type is Untagged.


(Figure 6.4.5)

:

The switch VLAN maximum support 64 VLAN item, VID value range:1~4095

Manged port is the port that manage and configure switch, it must in a same VLAN as CPU port

## 6.4.2 IGMP snooping

IP host applies to join (or leave) multicast group to the neighboring router through IGMP (Internet Group Management Protocol) protocol. IGMP Snooping is multicast constraining mechanism. It manages and controls multicast group by snooping and analysis of the IGMP messages between the host and the multicast device.

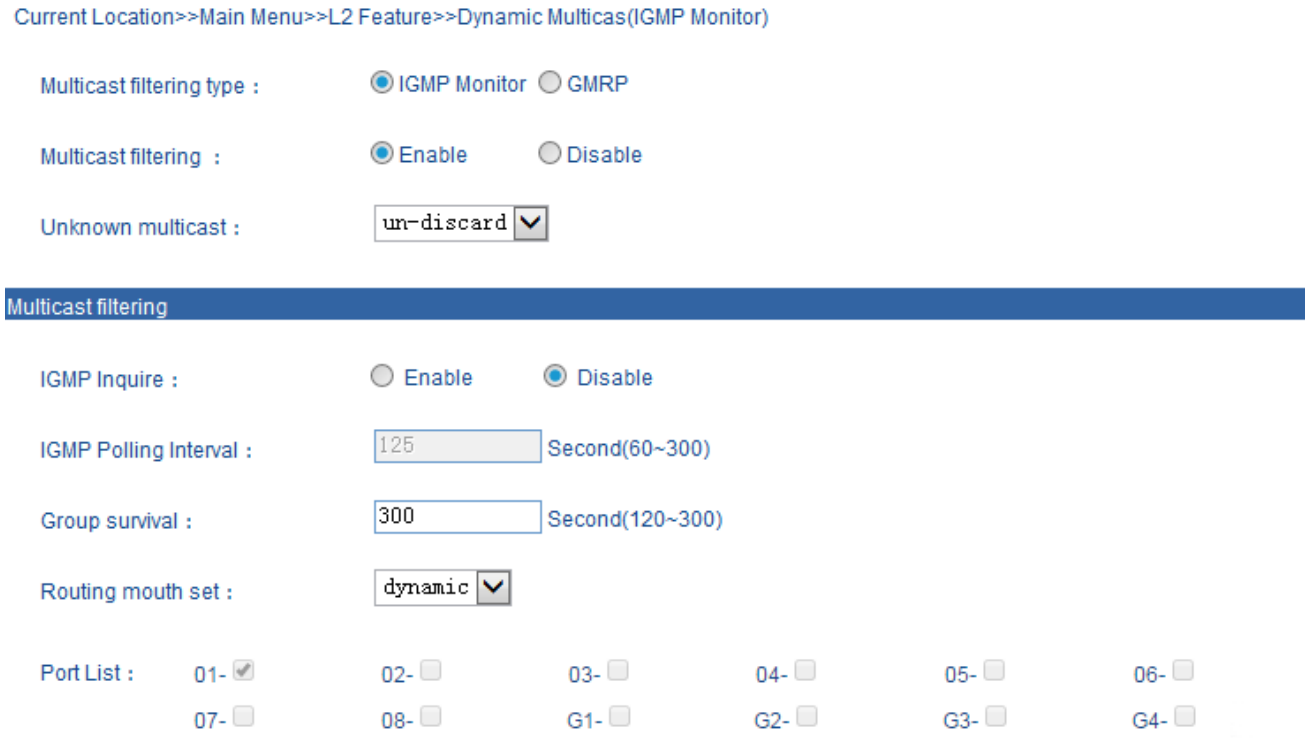
Work process of IGMP Snooping: the switch snoops messages between the host computer and the router and tracks multicast information and the port applied for. When the switch snoops IGMP Report message sent from the host computer to the router, the switch would add this port to multicast forwarding list; when the switch snoops IGMP Leave message sent by the host computer, the router will send Group-Specific Query message of this port. If other hosts need this multicast, then the rely IGMP Report message. If the router doesn't get any reply from the hosts, the switch would delete this port from the multicast forwarding list. The router will send IGMP Query message regularly, the switch will deletes the port from the multicast forwarding list if it doesn't get the IGMP Report message from the host.

**IGMP Snooping:** Enable or disable IGMP snooping function

**IGMP Query:** Enable or disable IGMP query function

**IGMP Query Interval:** after enabling IGMP Query, the interval to check existing multicast members.

**MAX Age:** the maximum existing time of the members

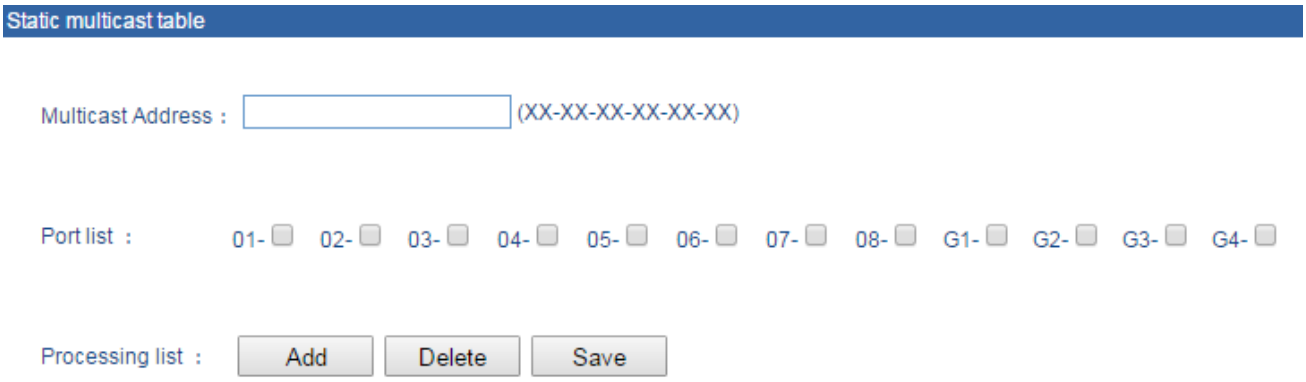



(Figure 6.4.6)

1. Must configure the VLAN of 802.1q at first, then open IGMP Snooping function
2. Please do not open more IGMP snooping, waste source.

### 6.4.3 Static Multicast

The device provides the function of static MAC address forwarding. The destination address includes the data packets with static MAC address which will be transferred to the appointed port. Embedded forwarding address list in the switch chip can learn and support 2,000 MAC addresses and 16 multicast forwarding ports list. Static MAC address carry out transmit function, it did not accept the arrangement of aging.




(Figure 6.4.7)

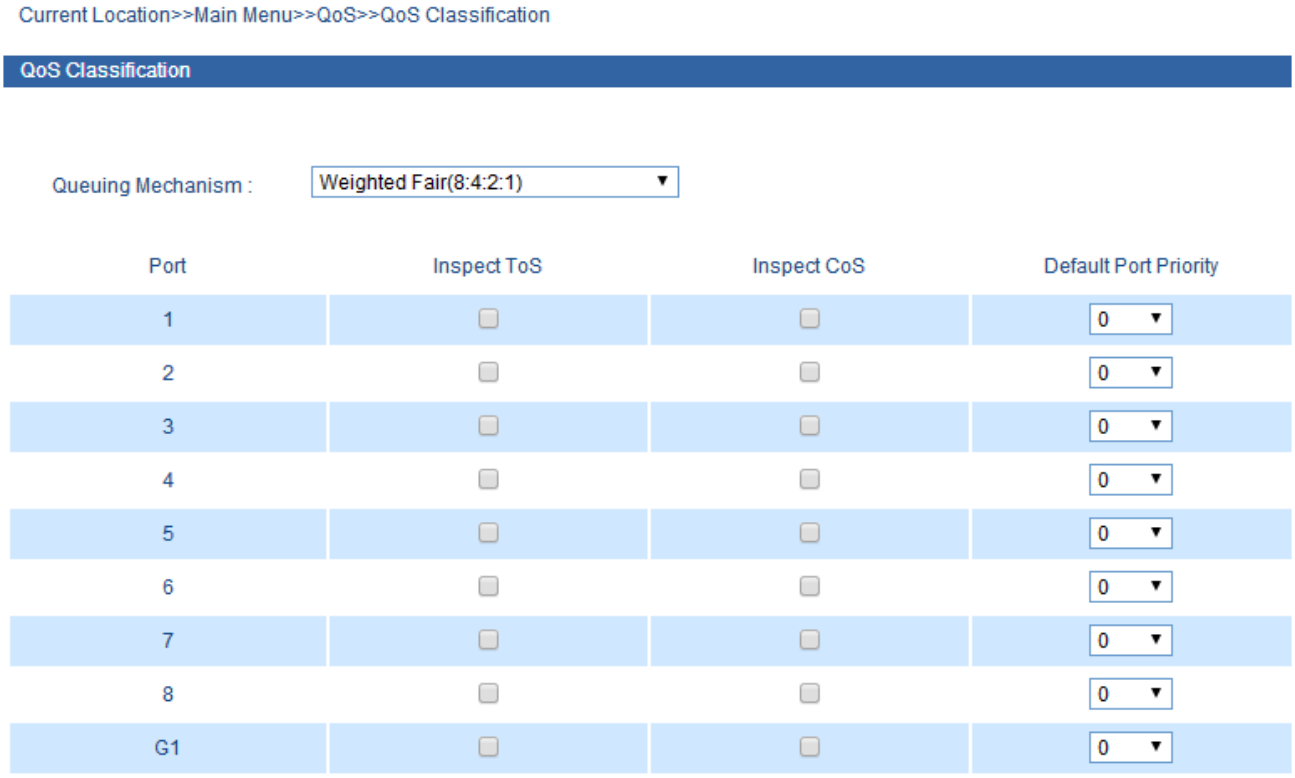
Button [Add/Edit], [Delete] were used for add/delete static Multicast MAC address. Join port is used to choice the transmit port of static MAC address, can point to 1 or more transmit port. Knock [Add], [Delete], static MAC address will be updated. For example, add MAC address “01-00-00-00-01-01” member is port 1, 2, 3, 4. Multicast MAC address is 1 of highest byte’s low byte. All none multicast address did not allow to add in this table and the format must according to XX-XX-XX-XX-XX-XX, did not have space or other illegal character, otherwise, will be display warning information.

1. This function has great impact on forwarding multicast, unless you can make sure the address is no problem, otherwise, please use it with caution.
2. The following multicast addresses are reserved for the device or protocol, please don't use them: 0180C20000xx, 01005E0000xx.
3. IGMP dynamic learning will not update the multicast address, static multicast forwarding is a kind of safety mechanism.

## 6.5 QOS

### 6.5.1 QOS Classification

QoS provides four internal queues, each queue supports four different levels of traffic, shorter persistence time of high-priority data packets in the switch, supports lower latency for certain delay-sensitive traffic. According to port ID, MAC address, 802.1p priority tags, DiONetServ and IP TOS, equipment can be able to put the packets to an appropriate level.




(Figure 6.5.1)

Users can select the QOS priority queue mechanism, the queue mechanism in two ways: weighted Fair mode and strict mode.

### 6.5.2 COS

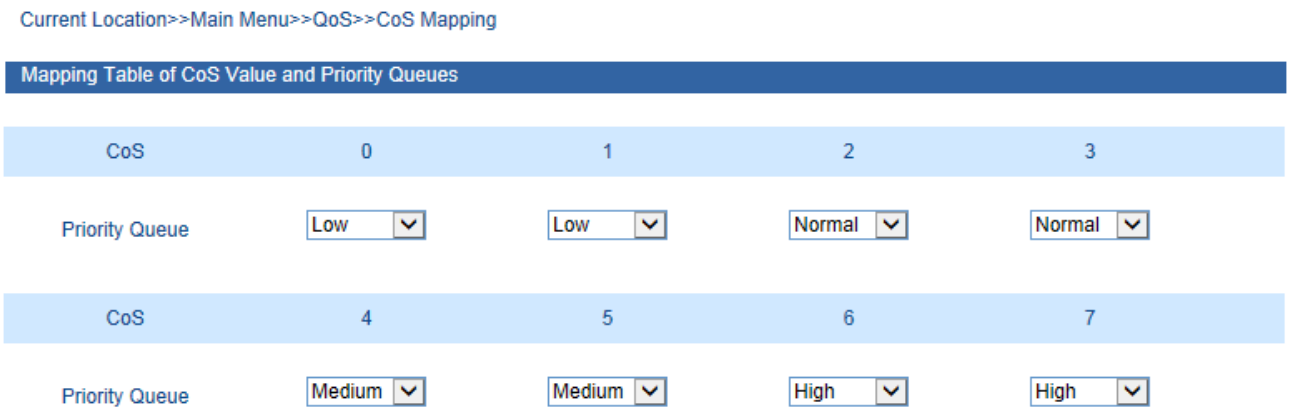
IEEE P802.1p is the name of a task group active during 1995–98 responsible for adding traffic class expediting and dynamic multicast filtering to the IEEE 802.1D standard. Essentially, they provided a mechanism for implementing Quality of Service (QoS) at the media access control (MAC) level. The group's work with the new priority classes and Generic Attribute Registration Protocol (GARP) was not published separately but was incorporated into a major revision of the standard, IEEE 802.1D-1998. It also required a short amendment extending the frame size of the Ethernet standard by four bytes which was published as IEEE 802.3ac in 1998.

The QoS technique developed by the working group, also known as class of service (CoS), is a 3-bit field called the Priority Code Point (PCP) within an Ethernet frame header when using VLAN tagged frames as defined by IEEE 802.1Q. It specifies a priority value of between 0 and 7 inclusive that can be used by QoS disciplines to differentiate traffic. Although this technique is commonly referred to as *IEEE 802.1p*, there is no standard or amendment by that name published by the IEEE. Rather the technique is incorporated into IEEE 802.1Q standard which specifies the tag inserted into an Ethernet frame.

### Priority levels

Eight different classes of service are available as expressed through the 3-bit PCP field in an IEEE 802.1Q header added to the frame. The way traffic is treated when assigned to any particular class is undefined and left to the implementation. The IEEE however has made some broad recommendations:

| PCP | Priority | Acronym | Traffic Types |
|---|---|---|---|
| 1 | 0 (lowest) | BK | Background |
| 0 | 1 | BE | Best Effort |
| 2 | 2 | EE | Excellent Effort |
| 3 | 3 | CA | Critical Applications |
| 4 | 4 | VI | Video, < 100 ms latency and jitter |
| 5 | 5 | VO | Voice, < 10 ms latency and jitter |
| 6 | 6 | IC | Internetwork Control |
| 7 | 7 (highest) | NC | Network Control |




(Figure 6.5.2)

### 6.5.3 DSCP

DiffServ architecture provides each transport packets in the network are classified into different categories, classified information is contained in the IP packet header, DiffServ architecture using the first 6 bits of IP packet header TOS( Type of Service) to carry the packets' classified information. This definition is only for the lower 6 bits, one number does not exceed 63. This definition supports both IPv4 (ToS field) and IPv6 (Traffic Class field). DSCP has 64 priority values (0-63), the lowest priority 0 and the highest priority 63. In fact, the DSCP field is a superset of the IP precedence field, DSCP field definition is backward-compatible with IP precedence field.

So far, the defined DSCP with default DSCP, the value is 0; class selector DSCP defined as the backward-compatible with IP precedence, the value(8,16,24,32,40,48,56); Expedited Forwarding (EF), generally used for low latency service, the recommended value is 46 (101110); identified by forwarding

(AF) defines four service levels, each service level has 3 down process, so spent 12 DSCP values ((10,12,14), (18,20,22), (26,28,30), (34,36,38)).

The priority value of the device (1-16) is defined as the lowest priority, as the first queue. Priority value (17-32) is defined as the second queue, the priority value (33-48) is defined as the third queue, the priority value (49-64 is defined as the fastest queue, the highest priority.

Current Location>>Main Menu>>QoS>>ToS/DiffServ Mapping

Mapping Table of ToS (DSCP) Value and Priority Queues

| ToS(DSCP) | Level | ToS(DSCP) | Level | ToS(DSCP) | Level | ToS(DSCP) | Level |
|---|---|---|---|---|---|---|---|
| 0x00(01) | Low | 0x04(02) | Low | 0x08(03) | Low | 0x0C(04) | Low |
| 0x10(05) | Low | 0x14(06) | Low | 0x18(07) | Low | 0x1C(08) | Low |
| 0x20(09) | Low | 0x24(10) | Low | 0x28(11) | Low | 0x2C(12) | Low |
| 0x30(13) | Low | 0x34(14) | Low | 0x38(15) | Low | 0x3C(16) | Low |
| 0x40(17) | Normal | 0x44(18) | Normal | 0x48(19) | Normal | 0x4C(20) | Normal |
| 0x50(21) | Normal | 0x54(22) | Normal | 0x58(23) | Normal | 0x5C(24) | Normal |
| 0x60(25) | Normal | 0x64(26) | Normal | 0x68(27) | Normal | 0x6C(28) | Normal |
| 0x70(29) | Normal | 0x74(30) | Normal | 0x78(31) | Normal | 0x7C(32) | Normal |
| 0x80(33) | Medium | 0x84(34) | Medium | 0x88(35) | Medium | 0x8C(36) | Medium |
| 0x90(37) | Medium | 0x94(38) | Medium | 0x98(39) | Medium | 0x9C(40) | Medium |
| 0xA0(41) | Medium | 0xA4(42) | Medium | 0xA8(43) | Medium | 0xAC(44) | Medium |
| 0xB0(45) | Medium | 0xB4(46) | Medium | 0xB8(47) | Medium | 0xBC(48) | Medium |
| 0xC0(49) | High | 0xC4(50) | High | 0xC8(51) | High | 0xCC(52) | High |
| 0xD0(53) | High | 0xD4(54) | High | 0xD8(55) | High | 0xDC(56) | High |
| 0xE0(57) | High | 0xE4(58) | High | 0xE8(59) | High | 0xEC(60) | High |
| 0xF0(61) | High | 0xF4(62) | High | 0xF8(63) | High | 0xFC(64) | High |

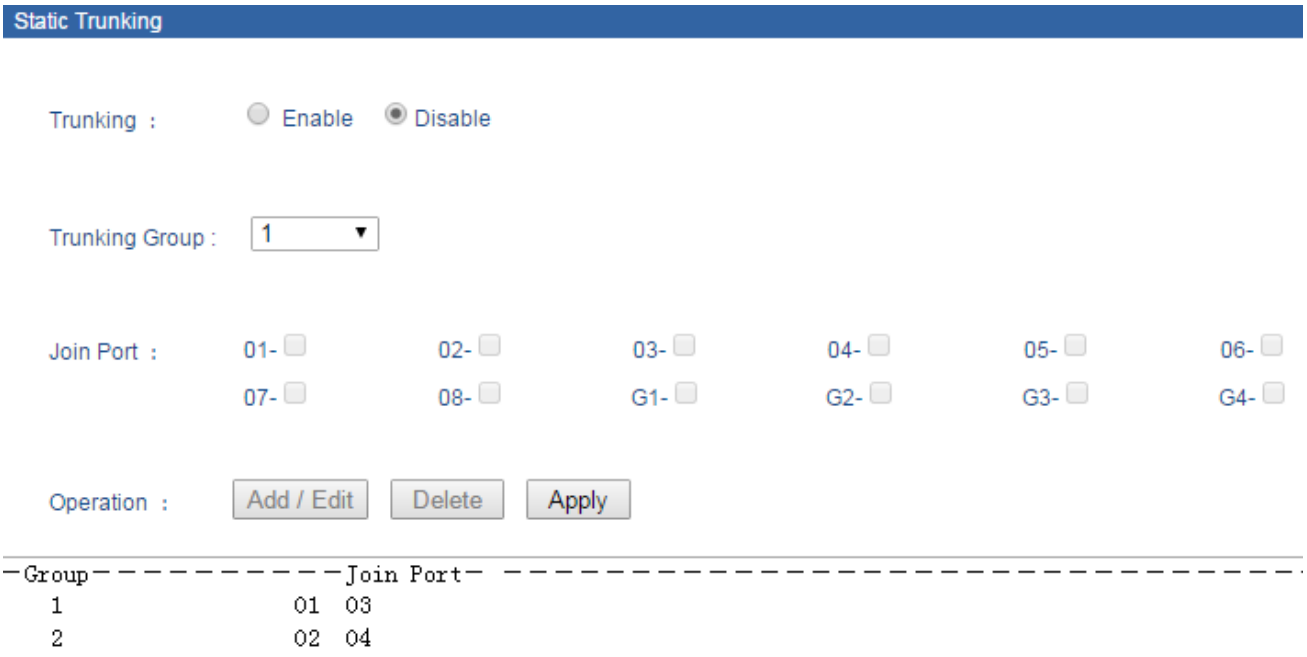
(Figure 6.5.3)

1. Port priority is the highest level, don't need to check other QoS attributes is discharged into the highest priority queue if you set the port priority as 1.
2. DSCP priority comes second, unless we do not set DSCP, therefore will check 802.1p priority, otherwise it will line up according to the DSCP settings.
3. As above, the three priority can be used alone, can also be used at the same time, queuing according to the above rules.

## 6.6 Redundancy

### 6.6.1 Port Trunking

In telecommunications, trunking is a method for a system to provide network access to many clients by sharing a set of lines or frequencies instead of providing them individually. This is analogous to the structure of a tree with one trunk and many branches. Trunking, is set by the configuration software, the two or more physical ports get together into a logical path to increase the bandwidth between the switch and the network node. Trunking is a packaging technology, it is a peer to peer link, both ends of the link are switches, it can be a switch and a router, and also can be a host, switch or router. Based on port trunking function that allows between two or more ports between switches, switches and routers, hosts the switch or router connected in parallel to provide for the simultaneous transmission of higher bandwidth and greater throughput, significantly entire network capacity. Trunking is more economical to increase the bandwidth between the switch and network device, such as servers, routers, workstations, or other switches. Trunking function is to integrate more than one physical port (typically 2-4) to a logical channel.




(Figure 6.6.1)

Device supported 2 trunking group, operate method: choice apply, choice the port need to trunking the port list, Choice setting, available after reboot. If the port already set to Ring port, it cannot set to trunking port. Each trunking group at least have 2 port member, at more 4. 1 port cannot exist in 2 trunking group.

1. The trunking groups require all the attributes can be the same, including speed, duplex, STP state etc.
2.If you do not confirm the STP state, please disable RSTP function, or close others, leaving only one STP channel.
3. Port 1 as the system reserved, cannot be used as trunking.
4. The ports of having been set to the port aggregation that cannot be set to ring ports.

### 6.6.2 Rapid Ring

**SW-Ring™** technology provides auto-recovery and reconnection mechanism for broken network. When network is broken, it has link redundancy and self-recovery capability and self-recovery time is less than 20ms. SW-Ring is the patented technology of 3onedata Co., Ltd. designed for industrial control network requiring high reliability.

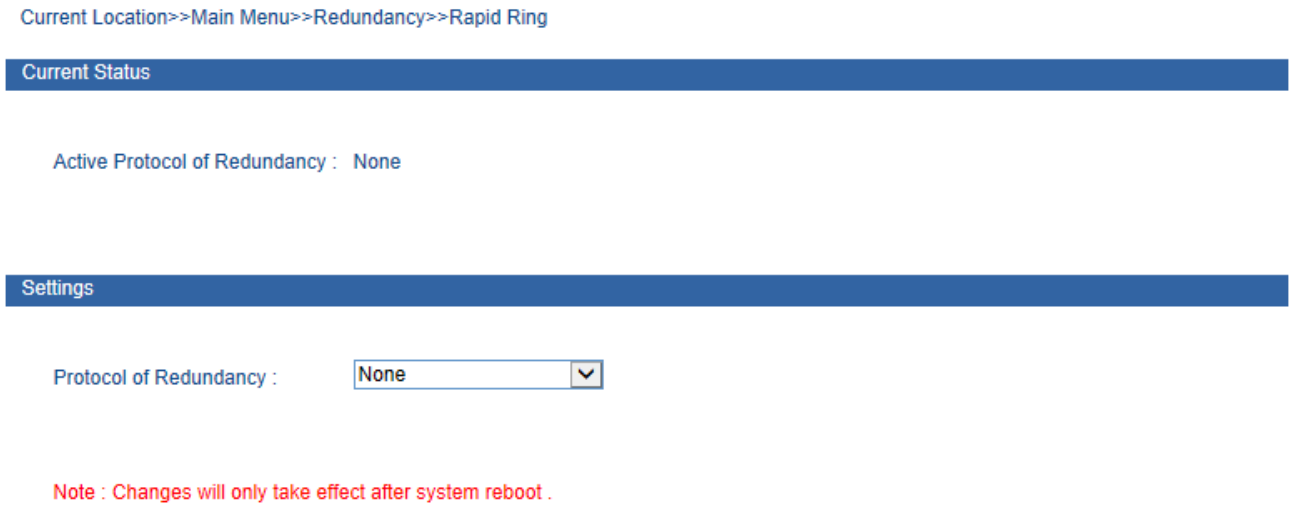
**SW-Ring™** technology support maximum 250 pieces switches, in which the **SW-Ring™** its self-recovery time is <20ms.

Each port of the switch can be Ring Port to connect other switches. When network is broken, relay for failure alarm will be activated. Redundant organization of **SW-Ring™** enable backup link to recover network instantly.

Self-developed patented technology for SW-Ring network can realize the intelligent redundancy for industrial Ethernet switch, which can make you easily and conveniently establish redundant Ethernet, and can facilitate the quick recovery of any network section of automatic system disconnected from the network. The switch supports maximum 4 ring groups. Each group set up 2 ports as Ring Port and a port cannot belong to several rings.

Hello_time setting is time interval of sending detecting packet to network at regular time. The unit is ms. Its main purpose is to detect network connection. It sends a detecting packet to next door devices by CPU. If they receive it, then reply a confirm packet to ensure network connection is active. If this setting will influence self-recovery time, we suggest advanced users can use it.

Basic interface of Rapid Ring as shown in figure 6.6.2:

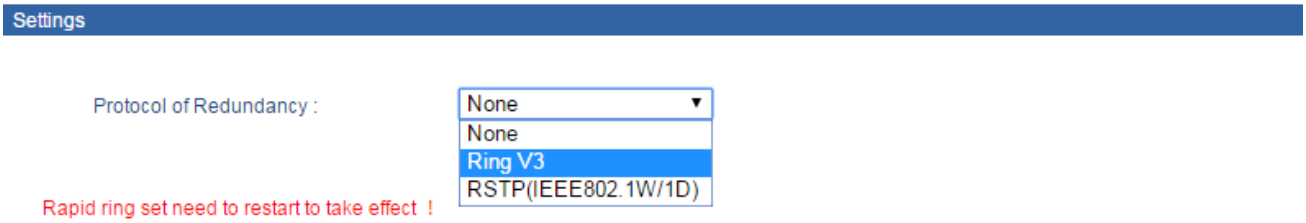



(Figure 6.6.2)

Initial interface display redundancy protocol is none, can configure it through [Settings]. Ring V3 Single ring, coupling ring, chain ring and Dual_homing.

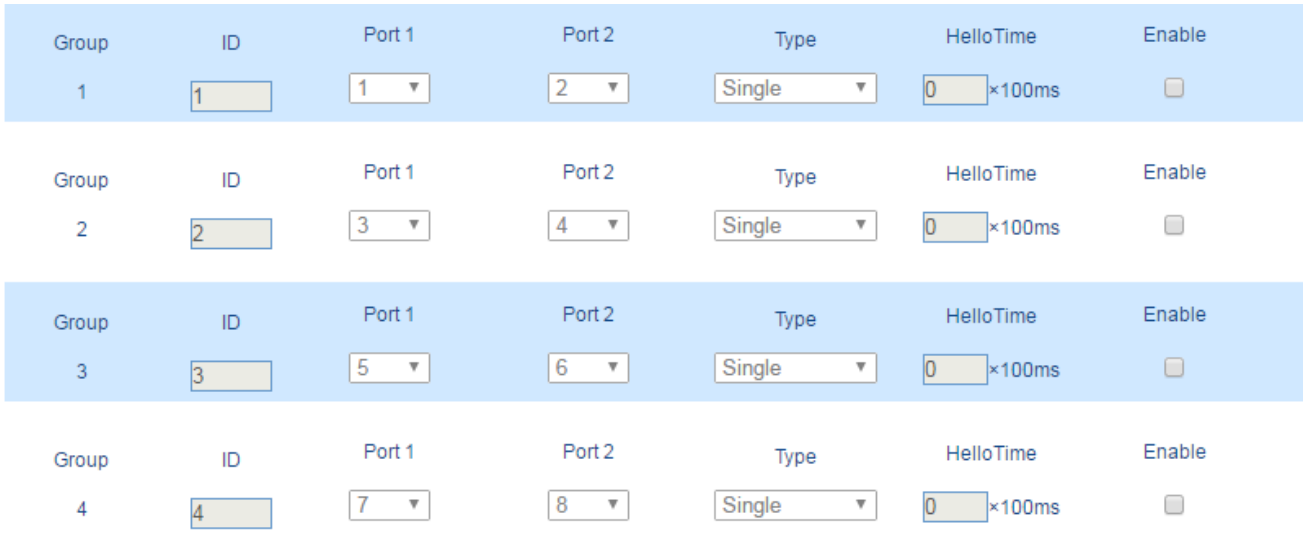
**Method to enable Ring V3**

1. Enable Ring V3,Select Ring V3 in [Settings] drop-down menu, figure as 6.6.3




(Figure 6.6.3)

2. After select Ring V3, Configuration interface is as figure 6.6.4, we can see Ring V3 support 4 different ring group: Single, Coupling, Chain and Dual_homing.




(Figure 6.6.4)

3. Enable Ring Group 1(or Group 2), and enter into Network ID(support 0-255 number only).Select Ring Port between Port 1 and Port 2.

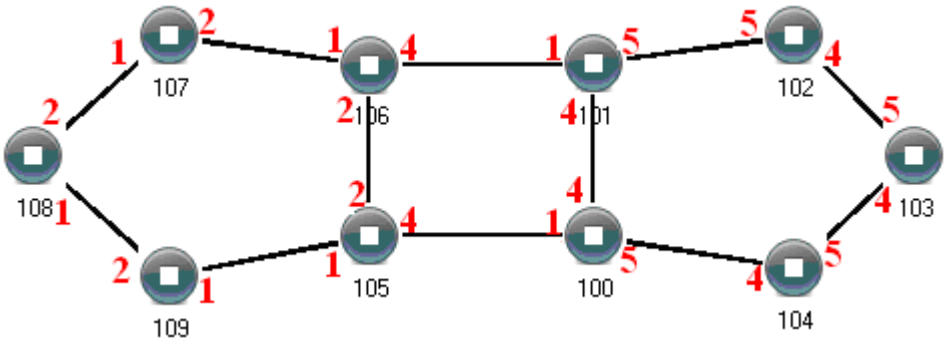
"Chain" refers to strengthen user's capability of making any type of redundant topological structure with flexibility by taking an advanced software technology. In fact, Chain is to cascade several switches already set up to Ring and both sides of chain access to network.

"Dual Homing" refers to a fact that two Rings connect the same switch. This type of configuration is ideal choice for centralized management of several Rings.

Method to enable Chain and Dual Homing is similar to that to enable Single Ring and Coupling Ring. It only needs to select corresponding items in [Type].

**1. Method to enable Ring V3 coupling ring**

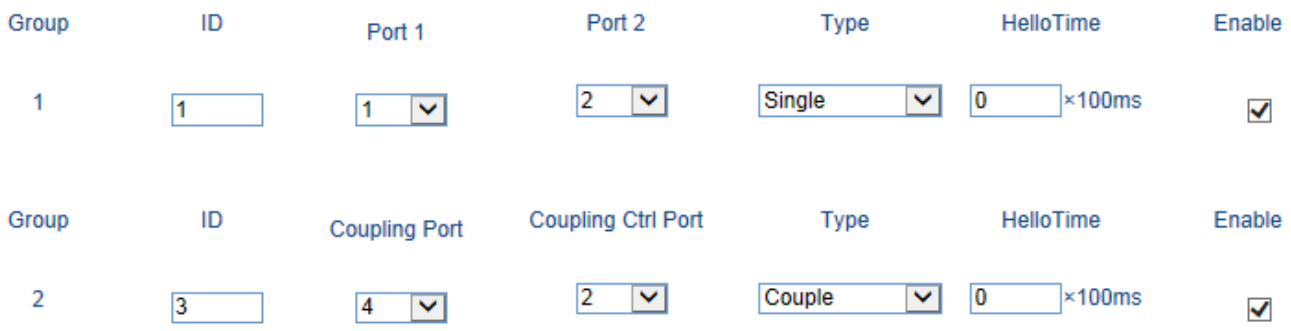
The architecture of coupling ring as figure 6.6.5




Coupling(Figure 6.6.5)

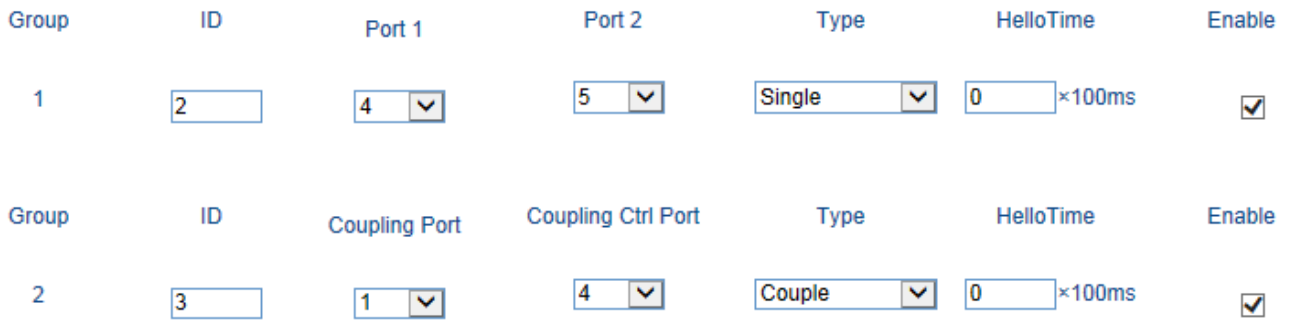
**Operation method:**

1. Select Ring V3, enable ring group 1 and 2. (Hello_time can be disable, if enable, time of sending Hello packet could not be very fast, it will influence CPU operate speed)；
2. Set 105, 106 device's ring port as port 1 and port 2 in ring group 1, network ID: 1, type: single ring. Set ring port as port 4 in ring group 2, Coupling ctrl port: 2, network ID: 3, type: coupling ring, figure as 6.6.6.




(Figure 6.6.6)

3. Set 100, 101 device's ring port as port 4 and port 5 in ring group 1, network ID: 2, type: single ring. Set ring port as port 1 in ring group 2, Coupling ctrl port: 4, network ID: 3, type: coupling ring, figure as 6.6.7.

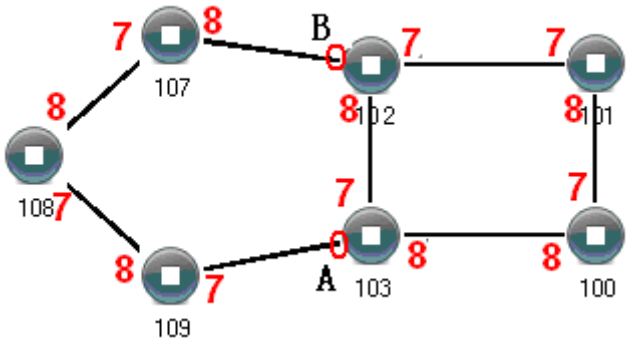



(Figure 6.6.7)

4. Set 107, 108, 109 device's ring port as port 1 and port 2 in ring group 1, network ID: 1, type: single ring. Set 102, 103, 104 device's ring port as port 4 and port 5 in group 1, network ID: 2, type: single ring.
5. Connect 100-104 device's port 4 and port 5 with network cable. Connect 105-109 device's port 1 and port 2 with network cable, Connect 101 device's port 1 to 106 device's port 4 with network cable, Connect 100 device's port 1 to 105 device's port 4 with network cable.

**2. Method to enable Ring V3 Chain ring**

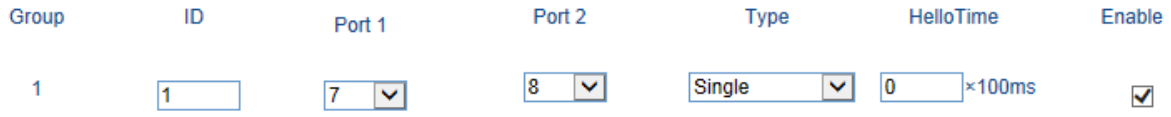
The structure of Chain ring as figure 6.6.15



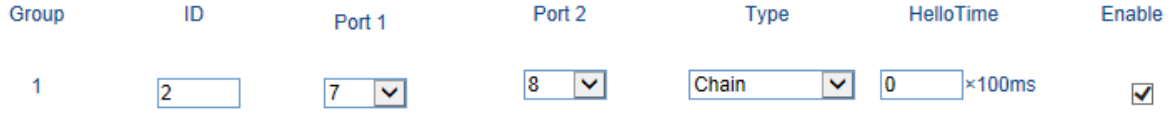

Chain (Figure 6.6.8)

**Operating method:**

1. Enable Ring Group 1: Hello time can be disable too, if it enable, time of sending Hello packet could not be very fast, or it will influence CPU dealing speed.
2. Set up Port 7 and 8 of Device 100, 101, 102 and 103 to be Ring Port in Ring Group 1, Network ID is1, Ring Type is Single; as shown in figure 6.6.9. Set up Port 7 and 8 of Device 107, 108 and 109 to be Ring Ports in Ring Group 2, Network ID is 2. Ring Type is Chain; as shown in figure 6.6.10.




(Figure 6.6.9)




(Figure 6.6.10)

3. Use a wire to connect Port 7 and 8 of Device 107-109 in turn to make a chain. Use a wire to connect Port 7 and 8 of Device 100-103 in turn to make a Single Ring, Then use a wire to connect Port 8 of Device 107 and Port 7 of Device 109 to normal port of Device 102 and 103. Chain is finished.

1. Port can not be trunking setting when it is already Ring port.
2. In the same single ring, identity must be consistent, otherwise it will not built a ring and can not communicate.
3. All ring ports in the VLAN settings must be TRUNK tagged VLAN member, otherwise can not communicate.
4. To form tangent ring or other complex rings, should pay attention to the ring identity whether is it consistent, different single ring identification must be different.

### 6.6.3 RSTP

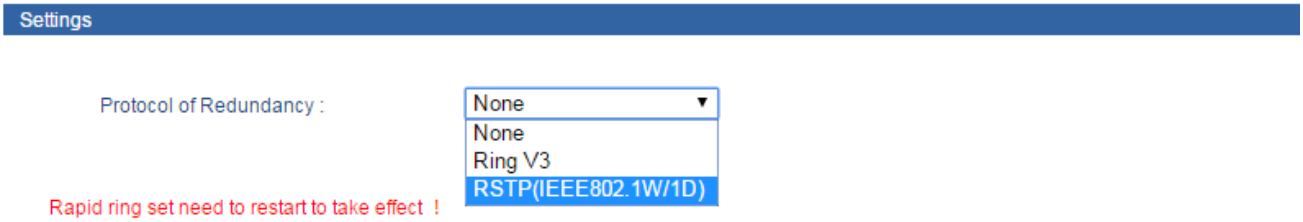
The first spanning tree protocol was invented in 1985 at the Digital Equipment Corporation by Radia Perlman. In 1990, the IEEE published the first standard for the protocol as 802.1D, based on the algorithm designed by Perlman. Subsequent versions were published in 1998 and 2004, incorporating various extensions.

Although the purpose of a standard is to promote interworking of equipment from different vendors, different implementations of a standard are not guaranteed to work, due for example to differences in default timer settings. The IEEE encourages vendors to provide a "Protocol Implementation Conformance Statement", declaring which capabilities and options have been implemented, to help users determine whether different implementations will interwork correctly.

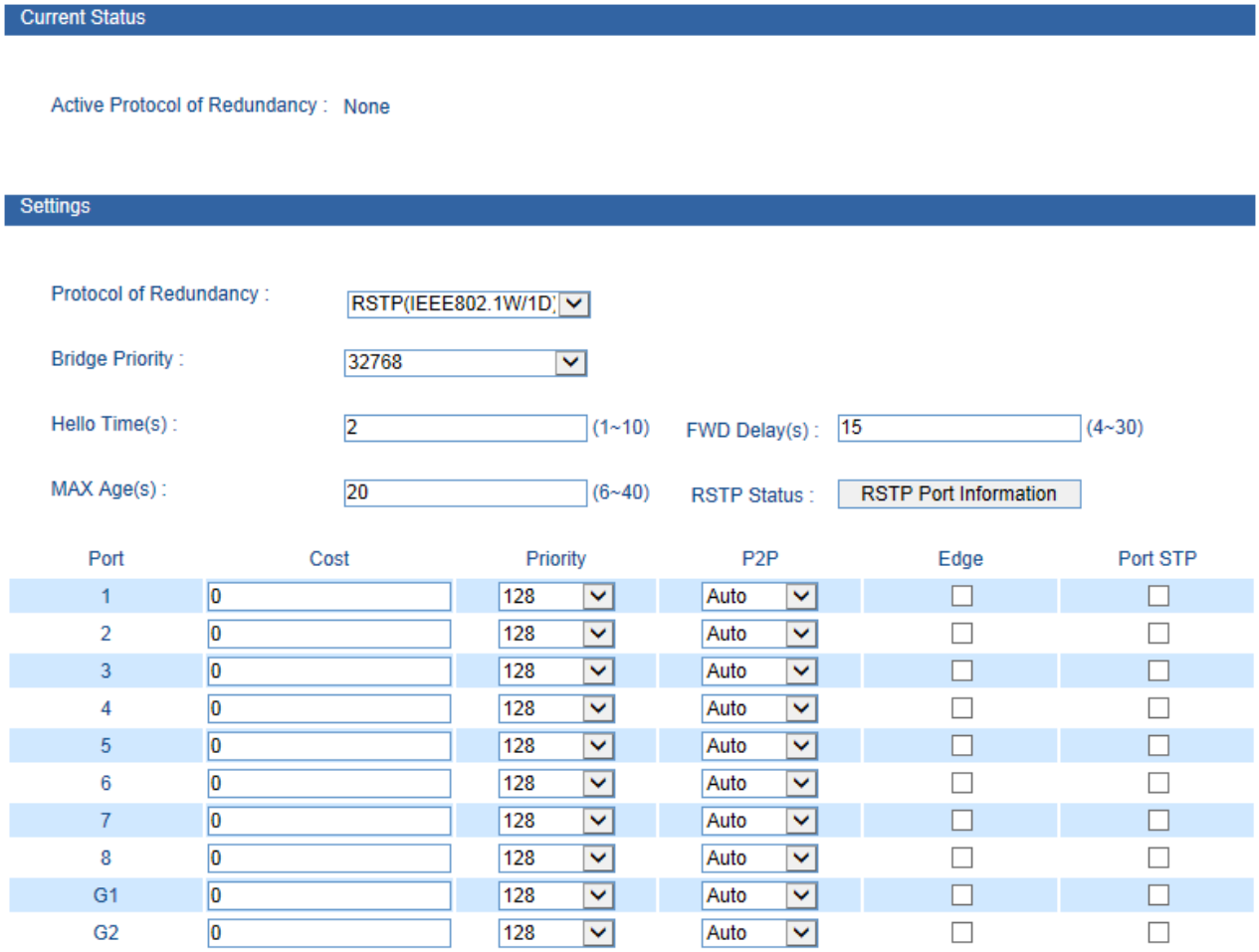
Also, the original Perlman-inspired Spanning Tree Protocol, called DEC STP, is not a standard and differs from the IEEE version in message format as well as timer settings. Some bridges implement both the IEEE and the DEC versions of the Spanning Tree Protocol, but their interworking can create issues for the network administrator, as illustrated by the problem discussed in an on-line Cisco document.

### Rapid Spanning Tree Protocol

In 2001, the IEEE introduced Rapid Spanning Tree Protocol (RSTP) as 802.1w. RSTP provides significantly faster spanning tree convergence after a topology change, introducing new convergence behaviors and bridge port roles to do this. RSTP was designed to be backwards-compatible with standard STP. While STP can take 30 to 50 seconds to respond to a topology change, RSTP is typically able to respond to changes within 3 × Hello times (default: 3 times 2 seconds) or within a few milliseconds of a physical link failure. The so-called Hello time is an important and configurable time interval that is used by RSTP for several purposes; its default value is 2 seconds. Standard IEEE 802.1D-2004 incorporates RSTP and obsoletes the original STP standard Select RSTP function in rapid ring network interface as follows:




(Figure 6.6.11)




(Figure 6.6.12)

**Rapid Spanning Tree of concepts:**

**Switch priority:** As the bridge priority,the bridge priority and bridge MAC address combine bridge ID,the smallest ID bridge will become the root bridge on the network.

**Polling interval:** how often send BPDU packet at one time.

**Forwarding delay:** the port state of switch remain a forward delay time over the listening and learning.

**The maximum aging time**: after one switch receive a packet from other switches , how long the packet is valid

**The port concepts of RSTP:**

**Port path overhead:** port link cost compared with port priority and port ID .

**Port priority:** port priority among the net bridge compared with port priority and port ID.

**Point to point network connection:** directly connect with switches port each other ,the port is P2P,which adopted negotiation mechanism, RSTP can achieve port state rapid conversion RSTP.

**Directly connect terminal:** connect the edge of network switch with terminal devices with configuration Edge port,which can achieve port state rapid conversion without the processing Discarding,Learning,Forwarding.

**Don't join RST structure:** Don't participate in RSTP running.

### RSTP switch port states:

1. **Blocking**- A port that would cause a switching loop if it were active. No user data is sent or received over a blocking port, but it may go into forwarding mode if the other links in use fail and the spanning tree algorithm determines the port may transition to the forwarding state. BPDU data is still received in blocking state. Prevents the use of looped paths.
2. **Listening**- The switch processes BPDUs and awaits possible new information that would cause it to return to the blocking state. It does not populate the MAC address table and it does not forward frames.
3. **Learning**- While the port does not yet forward frames it does learn source addresses from frames received and adds them to the filtering database (switching database). It populates the MAC Address table, but does not forward frames.
4. **Forwarding**- A port receiving and sending data, normal operation. RSTP still monitors incoming BPDUs that would indicate it should return to the blocking state to prevent a loop.

The example of Configuration: The priority of network bridge is "32768",If there did not have network ID less than itself, itself is root network bridge. There did not have same network ID in network. Every 2 seconds, the network bridge will transmit BPDU message to all appoint port. If did not receive BPDU message more than 20 seconds, it realized port invalid, will calculate the status of network bridge again. Each status exchange for each other if need to transmit, need to wait 15 seconds

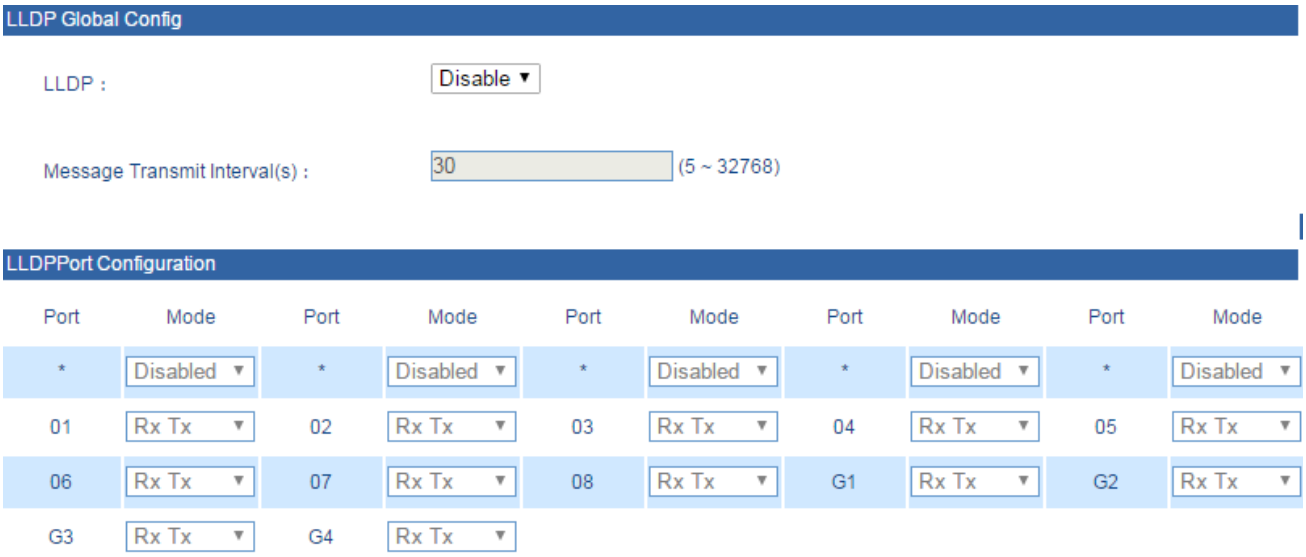
## 6.7 LLDP

### 6.7.1 Parameter Configuration

LLDP is a second layer topology discovery protocol, the basic principle is: network equipment to the adjacent equipment issued its notice of state information, and each port of all equipment are stored with their own information, if a local device state changes, also can with its directly connected neighbor devices to send updated information to that neighbor devices will be the information stored in the standard SNMP-MIB library. Network management system can query from the SNMP-MIB Library of the current second layer connection. It should be noted that LLDP is only a remote device status information discovery protocol, it can't complete the network device configuration and port control and other functions.

| Configuration item | meaning |
|---|---|
| **Disable** | The switch will not send the LLDP message, and will reduce the LLDP message received from the neighbor. |

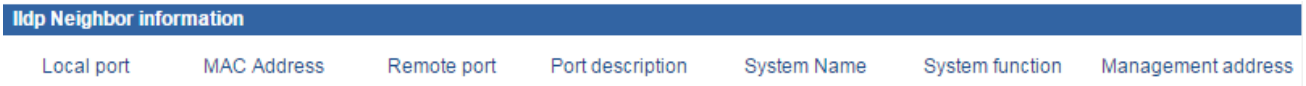
| | |
|---|---|
| **Enable** | The switch will send the LLDP message, which will analyze the LLDP message received from the neighbor. |
| **TX interval** | The switch status is not changed, the device periodically to the neighbor nodes to send LLDP packets, the interval time is called to send LLDP message **interval**. |
| **RX** | Switch will not send out the LLDP information, but the information from the vicinity of the unit LLDP analysis. |
| **TX** | Will reduce the LLDP information received from the neighbors, but will send LLDP information. |




(Figure 6.7.1)

### 6.7.2 Neighbor Information

LLDP management address is the address of the network management system identification and management. Management address can clearly identify a device, it is conducive to the network topology, network management, network management. The management address is encapsulated in the Management Address TLV field of the LLDP message and is sent to the neighbor node.




(Figure 6.7.2)

## 6.8 Access Control

### 6.8.1 User password

Enterprise usually required two different person to monitor device and manage system/ network. The authority need to separate. Monitor person was in charge of monitor work, system/network person was in charge of system/work management. The switch provided classification management: Administrator

authority and Observer authority. Observer just had authority to check the status of switch. Administrator had the authority to configure the parameters of the switch.

**Index**

User index indicates which group of users. There are three user indexes in drop-down list.

**Access level:**

administrator: have the right to check and configure all settings

observer: have the right to check all settings merely

**Login name**

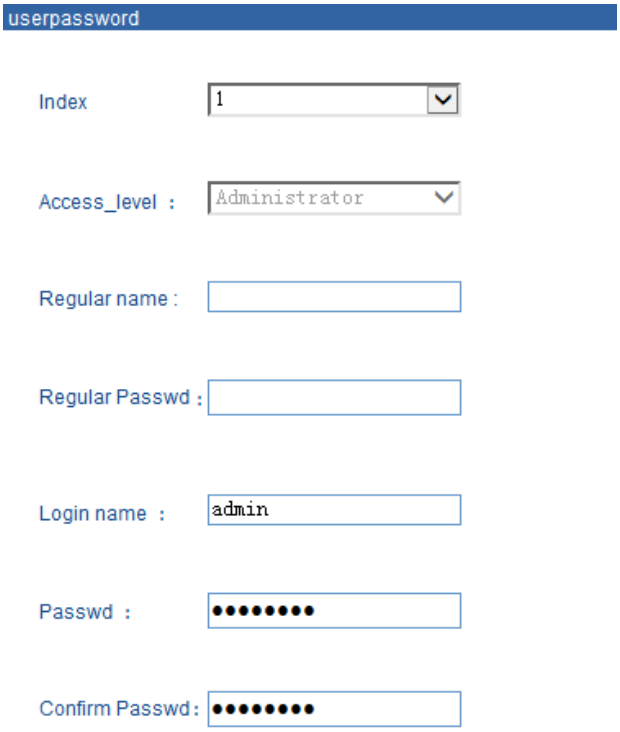
The identity of visitor with the letter combination is no more than 16 bytes

**Password:**

Visitor use password, user authority allows the letter combination no more than 16 bytes

**Confirm password**

Make sure the last time input password is correct.

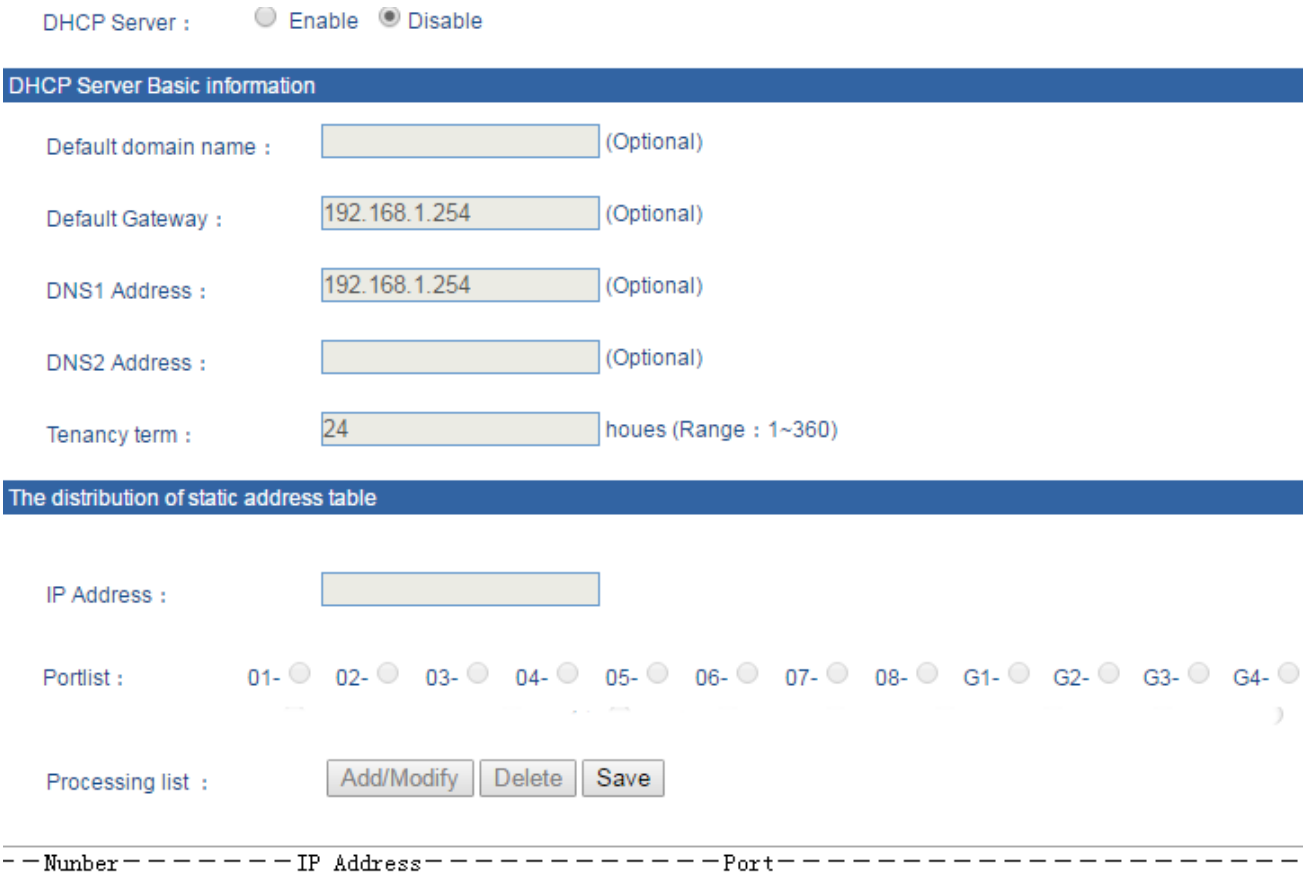



(Figure 6.8.1)

1. User must remember user name and password after modified. If forget it, please use DIP switch to make default factory. The default user name and password: admin.
2. Set same user mane, the front settings of user name/password will be available.

### 6.8.2 DHCP Server

The DHCP Server function is enabled, is to use this equipment as a DHCP server, by setting the static address table realization, this equipment is able to assign IP addresses to other devices connected to this equipment. For example: If the device is a turn on DHCP Server functionality, 2 sets the static address table: 192.168.1.19 corresponds to port 1; 192.168.1.20 port 2. Unit b opens automatically obtain an IP address feature, if the device is connected to a port 1 device-b, device b to automatically obtain IP addresses 192.168.1.19; if the device is connected to port 2 and an equipment b equipment b able to automatically obtain an IP address 192.168.1.20.




（Figure 6.8.2）

Fill out basic information about the DHCP Server, the DHCP client can automatically access to the information.

**Default domain name:** DHCP client can automatically access to the domain name;

**Default gateway:** DHCP client can automatically access to the gateway;

**DNS address:** DHCP clients to automatically obtain DNS address;

**Lease:** DHCP clients to automatically obtain the address to a valid time. Range from 1-360 hours

### 6.8.3 MAC port lock

**Static MAC address table**

Static MAC address is different from dynamic MAC address. Once the static address is added, the address will remain in effect before deleting it, cannot be limited by the maximum aging time. Static address list records the static address of ports. In the static address list, one MAC address corresponds to one port, if try to configuration, all data sent to this address will only be forwarded to the port. And also become he MAC address binding.

Static MAC address list is designed to limit the movement of the computer, any computer's MAC and port binding, this computer inserts to the other port cannot communicate with another computer, over this interface can still communicate with other computers. Port security is designed to protect the port and the corresponding port security, the port will forward the data when the specified MAC make a connection with this port, it is assumed that to set port security and with one MAC binding, then this PC can communicate with other ports, but other computers connected to this port cannot communicate. Button [Add/Edit] and [Delete] for adding, removing the static MAC address. Static MAC address requests a valid input from the user, will display warning messages if you enter an invalid MAC address. Port field is used to select a static MAC address forwarding ports; you can specify one or more forward ports. Click [Add/Edit] and [Delete] will trigger the static MAC address forwarding table updates.


（Figure 6.8.3）

This function is a security mechanism, be careful to confirm the setting, otherwise be used with caution.

Do not use a multicast address as the input address.

Do not enter the reserved MAC address, such as the device's MAC address.

## 6.9 Remote monitoring

### 6.9.1 SNMP management

**1. Introduction of SNMP**

SNMP (Simple Network Management Protocol) is an internet-standard protocol for managing devices on IP networks. It is used mostly in network management systems to monitor network-attached devices for conditions that warrant administrative attention.

**2. Work Mechanism of SNMP**

SNMP includes 2 parts: NMS and Agent:

NMS: Network Management Station. Software runs on the manager. The common management platforms are "Quid View", "Sun Net Manager" and "IBM Net View". Agent is the software of the server running in the network device.

NMS can send "Get Request", "Get Next Request" and "Set Request" message to Agent. After Agent gets those messages, it will read or write according to the message type to create Response message and send the Response message back to NMS. Agent will also send Trap message to NMS when the device is abnormal.

**3. SNMP Version**

Currently SNMP Agent of the device supports SNMP V3 and it is also compatible with SNMP V1and SNMP V2C. It is authenticated by user name and password in SNMP V3.

SNMP V1 and SNMP V2C adopt authentication of Community Name. The SNMP message of the community name which is not authenticated will be discarded. SNMP community name defines the relationship of SNMP NMS and SNMP Agent. User can choose the following one or more features related to community name.

1. Defines MIB view of community name.

2. Setup visit privilege of MIB objective is Write or Read. Community name with Read privilege can check the device information only. Community name with Write privilege can configure the device.

3. Setup appointed basic visit control list of the community name.

The switch supports SNMP V1/V2c. Both SNMP V1 and V2c use public character strings for match authentication.

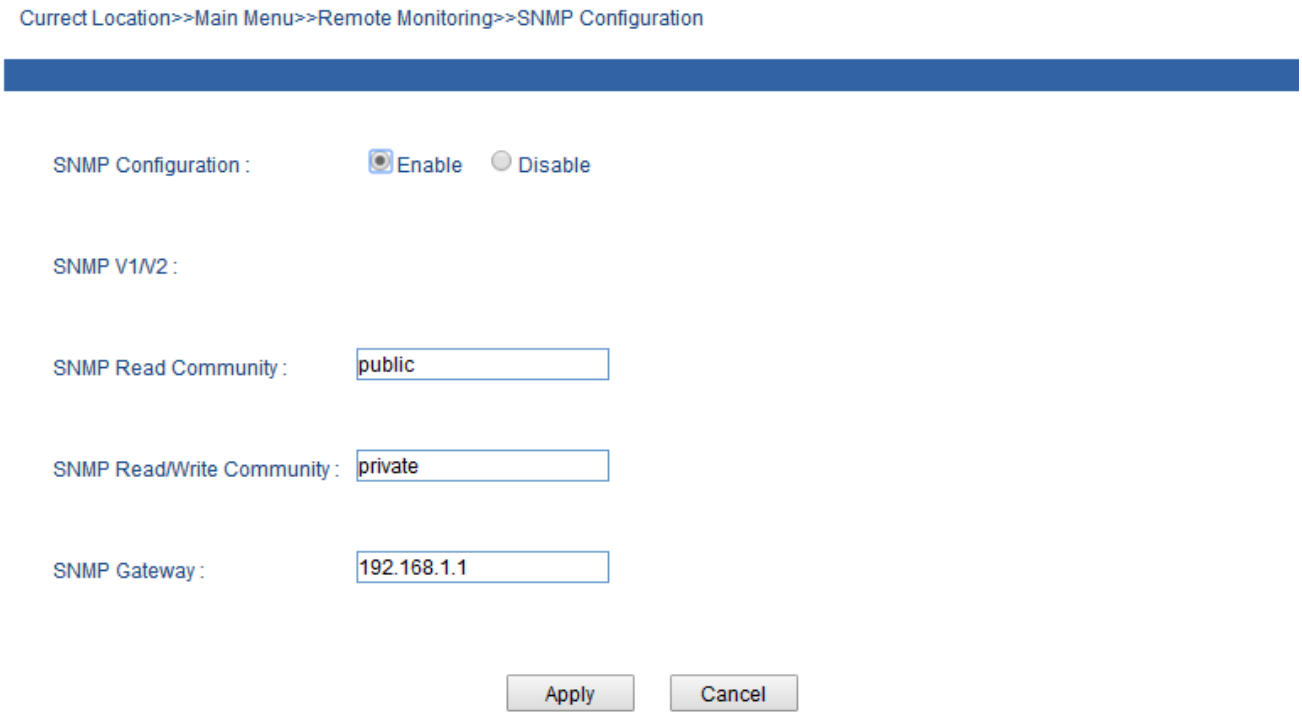
SNMP usually uses UDP Port 161(SNMP) and 162 (SNMP-traps) based on TCP/IP protocol. SNMP protocol agent is existed in network device. MIB (information specific to the device) is uses as device connector. These network devices can be monitored or controlled through the agent. When trap event happens, a message is transmitted by SNMP Trap, an available trap receiver can get this trap information.

SNMP supports 3 kinds of basic operating in total:

**Get:** Manager can use this to get some variable value of Agent.

**Set:** Manager can use this to set up some variable value of Agent.

**Trap:** Agent uses this to send an alarm to manager.




(Figure 6.9.1)

**Read Community**

Use a character string to name a SNMP community. This community only has Get privilege.

**Read/Write Community**

Use a character string to name a SNMP community. This community has Get and Set privilege.

**SNMP TRAP Gateway**

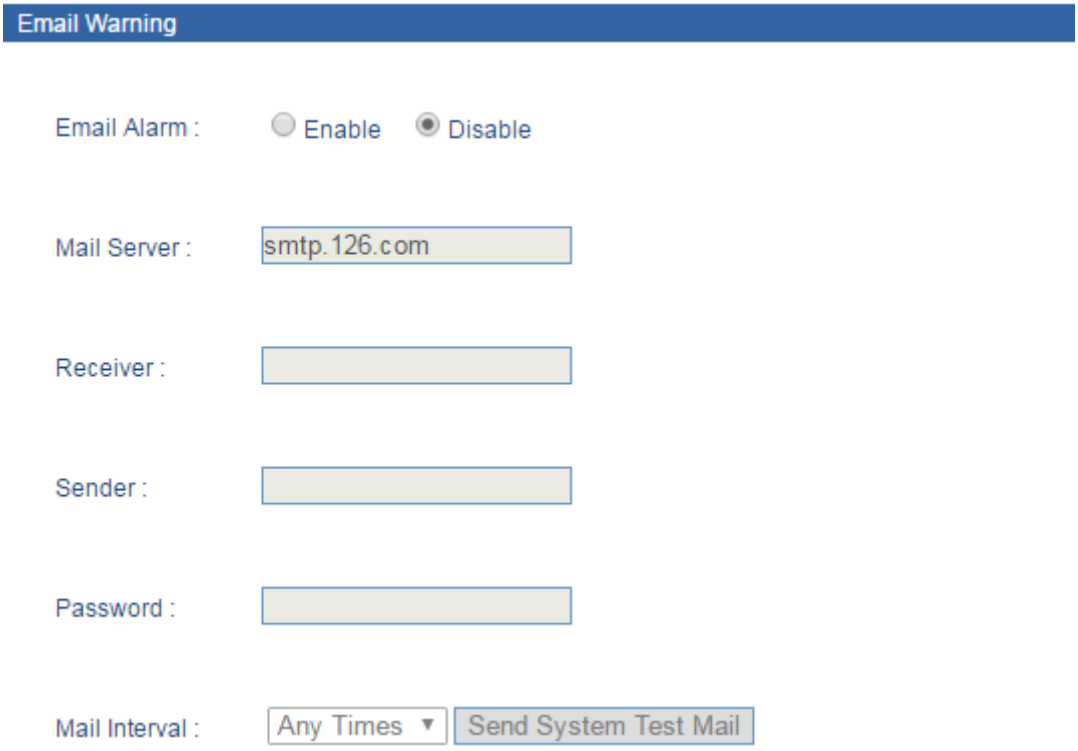
IP address of the receiver of the alarm information sent Agent

The device supports warm start of Trap. If existed IP address in Trap gateway, click "Apply", the Trap receiver can get the trap information. If the trap receiver cannot get trap information, please check network setting and connecting. Please pay attention to the privilege of Read and Write in SNMP Explorer.

### 6.9.2 Email Warning

Please make sure the switch can access internet regularly if use Email Warning. The gateway of the switch and local area network must identical.

Email warning function will send the warn information immediately by Email if these things happen: NTP information, connection statue changed, login information, broadcast storm information, operating record, and other system log.




（Figure 6.9.2）

**Mail server**

Please provide the host IP of POP3 mail delivery service or the host name to our device

**Sender**

E-mail account is used to login to e-mail server.

**Password**

E-mail password.

**Receiver**

Recipient to solve the problem of abnormal events hoping to find a contact e-mail address

**Mail Interval**

Regularly send log interval time

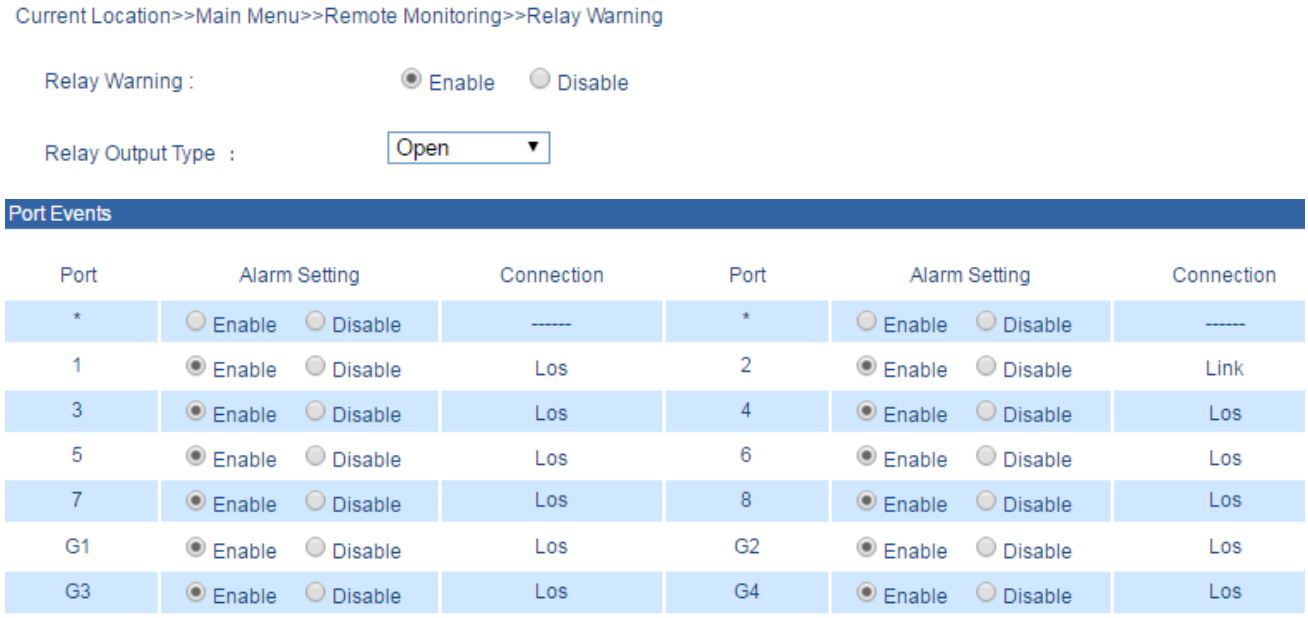
### 6.9.3 Relay Alarm

Warning have port alarm. Main function: once the devices were in unusual status, can inform administrator in time and repair the status of device quickly, can avoid more lose

Relay warning input type: Close/Open. Once select Close, the light will be bright when have alarm. Relay will be in open status.

### Port Alarm

Alarm when port disconnect. Enable port alarm, if port was in unusual status(Connect or disconnect), device will output a signal, inform the device work unusual.




| Port | Alarm Setting | Connection | Port | Alarm Setting | Connection |
|---|---|---|---|---|---|
| * | Enable Disable | ------ | * | Enable Disable | ------ |
| 1 | Enable Disable | Los | 2 | Enable Disable | Link |
| 3 | Enable Disable | Los | 4 | Enable Disable | Los |
| 5 | Enable Disable | Los | 6 | Enable Disable | Los |
| 7 | Enable Disable | Los | 8 | Enable Disable | Los |
| G1 | Enable Disable | Los | G2 | Enable Disable | Los |
| G3 | Enable Disable | Los | G4 | Enable Disable | Los |

(Figure 6.9.3)

In default status, the type of relay output is open, the alarm light is OFF, have no alarm, relay alway open.
When the device have alarm, the light is ON, relay close

## 6.10 Port Statistics

The function of traffic Statistics is to calculate the data packets in a fixed time, included transmit and receive data packets.

Operate method: Start to calculate after select clear

### 6.10.1 RX frame statistics

| Frame Name | Description |
|---|---|
| InUnicasts | Valid Unicast Data Frames |
| InBroadcasts | Valid Broadcast Data Frames |
| InPause | Number of Valid Flow Control Pause frames |
| InMulticasts | Valid multicast excluding InBroadcasts |
| InFCSErr | Number of FCS checkout error frames (completed data) |
| AlignErr | Number of FCS checkout error frames (uncompleted data) |
| InGoodOctets | Number of valid received data byte (including FCS) |
| InbadOctets | Number of invalid received data byte (including FCS) |
| Undersize | Number of valid data frames less than 64 bytes |
| Fragments | Fragments (less than 64 bytes, invalid FCS) |
| In64Octets | Number of frames with 64 bytes (including invalid frames) |
| In127Octets | Number of frames between 65 and 127 bytes (including invalid frames) |
| In255Octets | Number of frames between128 and 255 bytes (including invalid frames) |
| In511Octets | Number of frames between 256 and 511 bytes (including invalid frames) |
| In1023Octets | Number of frames between 512 and 1023 bytes (including invalid frames) |
| InMaxOctets | Number of 1024-1518 or 1522 bytes(802.1Q)(including invalid frames) |
| Jabber | Invalid oversized frames received (more than 1518 or 1522) |
| Oversize | Valid oversized frames received (more than 1518 or 1522) |
| InDiscards | Number of Valid discarded frames (because of cache, flow control, etc.) |
| InFiltered | Valid frames filtered (because of VLAN and so on) |

### 6.10.2 TX frame statistics

| | |
|---|---|
| OutUnicasts | unicast data frames output |
| OutBroadcasts | Broadcast data frames output |
| OutPause | Number of output flow control pause frames |
| OutMulticasts | Multicast data frames output |
| OutFCSErr | Invalid FCS frames output |
| OutOctets | Number of output bytes(including FCS) |
| Out64Octets | Number of output frames with 64 bytes |
| Out127Octets | Number of output frames between 65 and 127 bytes |
| Out255Octets | Number of output frames between 128 and 255 bytes |
| Out511Octets | Number of output frames between 256 and 511 bytes |
| Out1023Octets | Number of output frames between 512 and 1023 bytes |
| OutMaxOctets | Number of output frames between 1024 and 1518 or 1522 bytes(802.1Q) |
| Collisions | Number of collision in output |
| Late | Number of collision after frames output 64 bytes |
| Excessive | Number of unsuccessful output frames(trying more than 16 times with half duplex flow control ) |
| Multiple | Number of successful output frames(collision more than 1 time) |
| Single | Number of successful output frames(collision happens in 1 time only ) |
| Deferred | Number of successful output frames(the receiver is busy, but It sends successfully after a delay) |
| OutFiltered | Filtered frames output |
| OutDiscards | Discarded frames output(because of cache, flow control, etc.) |

### 6.10.3 Traffic Statistics

Traffic Statistics

| Port | Tx | Rx | Unicast | Multicast | Broadcast | Error |
|---|---|---|---|---|---|---|
| 1 | 0 | 0 | 0 | 0 | 0 | 0 |
| 2 | 3571352 | 8244712 | 7857 | 33256 | 18490 | 0 |
| 3 | 0 | 0 | 0 | 0 | 0 | 0 |
| 4 | 0 | 0 | 0 | 0 | 0 | 0 |
| 5 | 0 | 0 | 0 | 0 | 0 | 0 |
| 6 | 0 | 0 | 0 | 0 | 0 | 0 |
| 7 | 0 | 0 | 0 | 0 | 0 | 0 |
| 8 | 0 | 0 | 0 | 0 | 0 | 0 |

（Figure 6.10.1）

**Tx**

Number of bytes of all data packets sent by the port

**Rx**

Number of bytes of all data packets received by the port

**Unicast**

Number of unicast data packets sent and received by the port

**Multicast**

Number of multicast data packets sent and received by the port

**Broadcast**

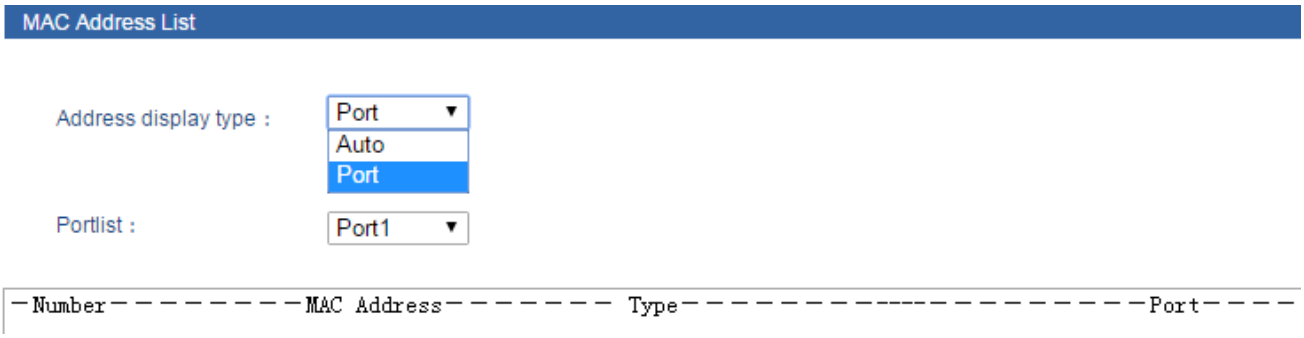
Number of broadcast data packets sent and received by the port

**Error**

Number of error packets because of some reasons sent and received by the port

### 6.10.4 MAC address table

MAC（Media Access Control）address is the network device hardware identification, the switch to forward packets based on MAC addresses. The MAC address is unique, which ensures correct packet forwarding. Each switch maintains a MAC address table. In this table, MAC addresses and switches port one-to-one correspondence. When the switches received a data frame, according to the MAC address table to determine the filter or forward the data frame corresponding to the switch port. MAC address table is the basis and premise of the switch to achieve fast forwarding.




（Figure 6.10.2）

MAC address classify into three types in device address MAC address list:

**1. Dynamic MAC address**

Dynamic MAC address of the switches in the network through the data frame to learn, when the arrival of aging time will be deleted. When the device is connected to the switch port to change the MAC address table and port corresponding relationship will change accordingly. Dynamic MAC address of the switch is powered restart will disappear, the need to re-learn.

**2. Static certification (solidify) MAC address**

Static authentication MAC address by configuring IEEE 802.1x authentication, the switch will not be aging. Regardless of the device is connected to the switch port happen to the MAC address table MAC address and port corresponding relationship always will not change, the relationship is completely controlled by the IEEE 802.1X authentication server. Static MAC address after the switch is powered restart will disappear.

**3. Permanent static MAC addresses**

permanent MAC address generated through configuration will not be aging, regardless of the device is connected switches of the change of the port, the MAC address table of MAC address and port of

corresponding relation is always does not change, permanent MAC address does not disappear after the switch is restart

MAC address table can specify the sort type, can choose "auto" and "MAC" two sort types, MAC address and related forwarding port will be showed in this table. if the status bar displays "certification"，shows MAC address static certification that is not aging treatment, if displays “static” means that MAC address is a permanent static address that is not aging treatment.

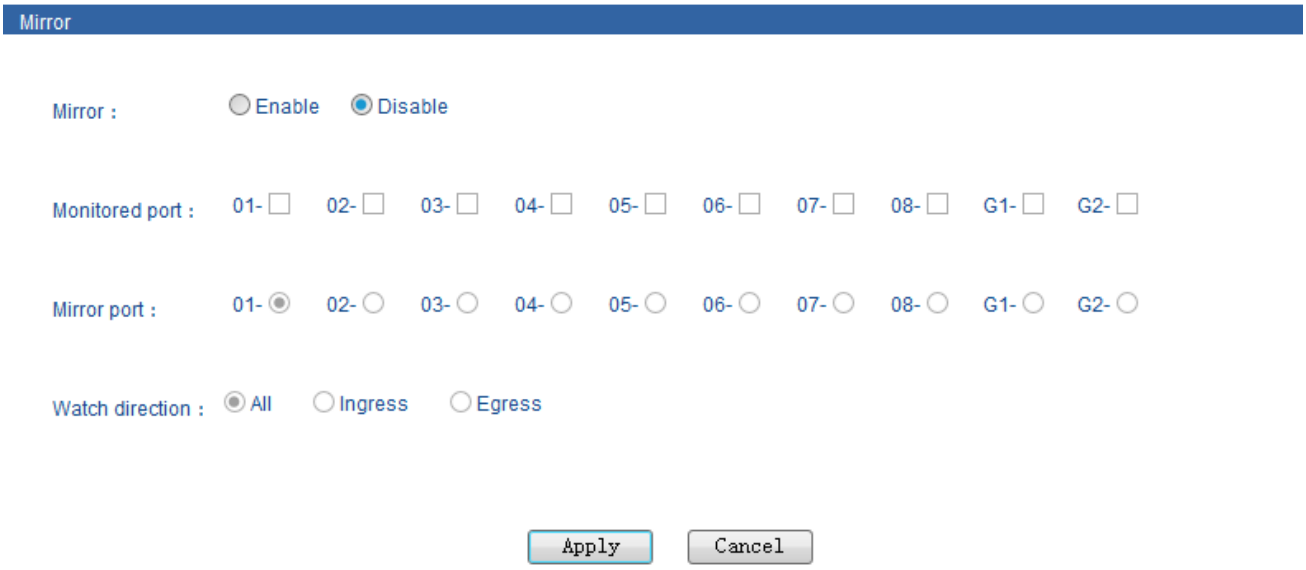
1. The address of the device index according to switch's address, so all MAC address displayed VLAN value is 0.
2. Permanent static address configured in the previous static MAC address port list, need to modify the corresponding item when port changed.
3. Multicast address list displays the IGMP snooping item, in the address list here all unicast address.
4. MAC address aging time is 300 seconds, the port is disconnected our parent program to clear all the corresponding port items.

# 6.11 Diagnosis

## 6.11.1 Mirror

Port mirroring refers to copy data from the port which need to be monitored to appointed monitoring port for analysis and monitoring. Ethernet switch supports many-for-one mirror which means messages from several ports can be copied to a monitored port. User can appoint the direction of monitored message, such as only monitoring of transmitted messages of appointed port. The device configures port mirroring function through port mirroring group. Each group includes a monitored port and a group of mirror ports. Total bandwidth of mirroring is not more than that of monitored port. It is good to monitor and manage its internal network data when using port mirroring in a company. It is also good to locate the failure when network is cut up.

Example as figure: Port 3 collect all of the data from port 1 and port 2




(Figure 6.11.1)

**Mirror Port**

It defines a group of ports which are needed to be monitored. The device collects data from these ports.

**Monitored Port**

It defines a group of ports which are used to monitor other ports. The device outputs the data through these ports.

**Watch direction**

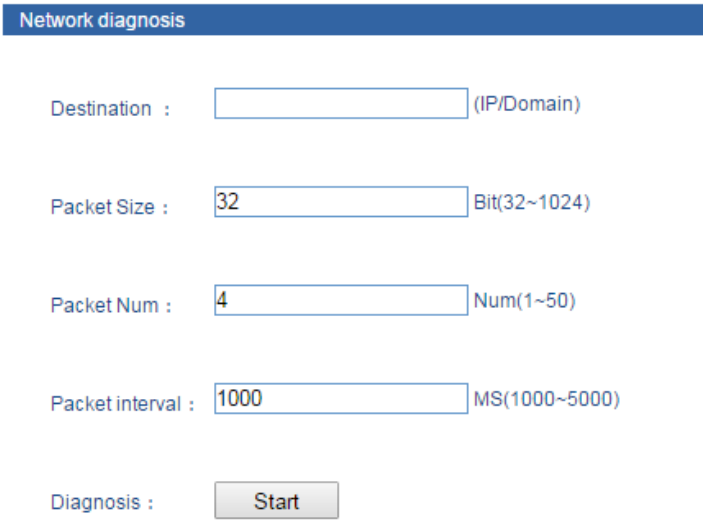
This parameter indicates the direction of the data. It includes 3 kinds of choices: "All", "Ingress" and "Egress".

1. This function is not often used. Otherwise other port-based higher management function like RSTP,IGMP Snooping
2. Port mirroring function can only deal with the normal FCS packets. It cannot deal with error data frames.

### 6.11.2 Ping

Ping is used to check whether the network is open or network connection speed of the order. As a life on the network administrator or a hacker, the ping command is first must master the DOS commands, it uses the principle of is this: the uniqueness on the network IP address of the machine and to target IP address to send a data packet, and then ask to return a similarly sized packets to determine two network machine is connected and communicated, check the size of the delay.

In the menu bar in order to click on the "main menu", "system configuration", "diagnostic ", "Ping", enter the Ping interface.

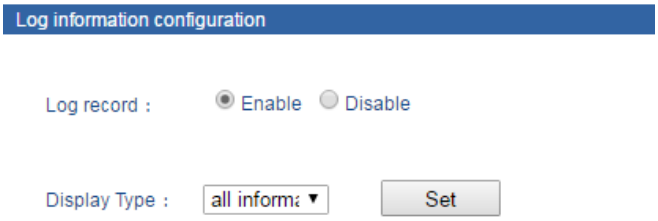



（Figure 6.11.2）

## 6.12 Basic settings

### 6.12.1 Log information

The device provides system log for user's reference of troubles. When enabling this function, the following events will be recorded:
The all information, boot information, handing information, linkage information.




（Figure 6.12.1）

### 6.12.2 SNTP

NTP (Network Time Protocol) is a protocol and software implementation for synchronizing the clocks of computer systems over packet-switched data network. It provides coordinated universal time including scheduled adjustments. No information about time zones or daylight saving time is transmitted; this information is outside its scope and it must be obtained separately.


（Figure 6.12.2）

**Local Time**

To configure the time by hand to undated the time of the device

**Enable NTP**

To update the time of the device by using NTP protocol

**Time Zone**

Standard time zones could be defined by geometrically subdividing the Earth's spheroid into 24 lines. The local time in neighboring zones would differ by one hour. And the variation in the position of the sun from one end of the zone to the other (east vs. west) would be at most 1/24 of the sky. Most of the 25 nautical time zones (specifically UTC−11 to UTC+11) are indeed defined this way, and are 15° of longitude wide. An hourly zone in the central Pacific Ocean is split into two 7.5°-wide zones (UTC±12) by the 180th meridian, part of which coincide with the International Date Line.

**NTP Server**

It provides host name or IP address of NTP timing.

**System Time**

Device time

**PC Time**

Visitor's own PC, display and switch itself does not matter.

1. NTP server can be empty, the device using the own server update, but must use the correct DNS and gateway.
2. NTP server must have a valid host name or a valid IP address.
3. Only the Administrators have permission to manually configure the device time.
4. Time zones must be configured; either uses the "local time" or "NTP time.
5. The configuration of the NTP server or PC can cause the display is not normal, you can change the time display format to adjust the display.

### 6.12.3 Device address

Device configuration support two modes, DHCP and static IP address, can get the device's IP address via client when the DHCP function is running, if you need NTP that need to connect internet, please enter the available and correct gateway and DNS address.

**IP Address**

IP address is a address of 32 bits length which is assigned to the device on the internet. The IP address consists of two fields: the network number field (net-id) and the Host ID field (host-id). For can conveniently manage IP address, IP addresses are divided into five categories. As blow:

| Network type | Address range | Available IP network range |
|---|---|---|
| A | 0.0.0.0～126.255.255.255 | 1.0.0.0～126.0.0.0 |
| B | 128.0.0.0～191.255.255.255 | 128.0.0.0～191.254.0.0 |
| C | 192.0.0.0～223.255.255.255 | 192.0.0.0～223.255.254.0 |
| D | 224.0.0.0～239.255.255.255 | Non |
| E | 240.0.0.0～246.255.255.255 | Non |
| Others | 255.255.255.255 | 255.255.255.255 |

A, B, C class address is unicast address; D class address is multicast address; E class address is reserved to prepare for the future for special purposes.

IP address using dotted decimal. Each IP address is represented as four decimal integers separated by decimal points, each integer corresponds to a byte, such as, 10.110.50.101.

**Subnet Mask**

Mask is corresponding 32 bits number of IP address. Some are 1, the others are 0. These 1 and 0 can be combined arbitrary in principle, but the first continuous bits are 1 when designing subnet mask. IP address can be divided into 2 parts by subnet mask: subnet address and host address. 1 in IP address and subnet corresponds to subnet address, other bits are host address. A type of address corresponding mask is 255.0.0.0; mask of B type address is 255.255.0.0; mask of C type address is 255.255.255.0.

**Default Gateway**

Default gateway in the host PC is generally called default route. Default route refer to a kind of router that destination address of IP data packet will choose when it don't find other existing route. All data packets of destination address which don't exist in the list of router will choose default route.

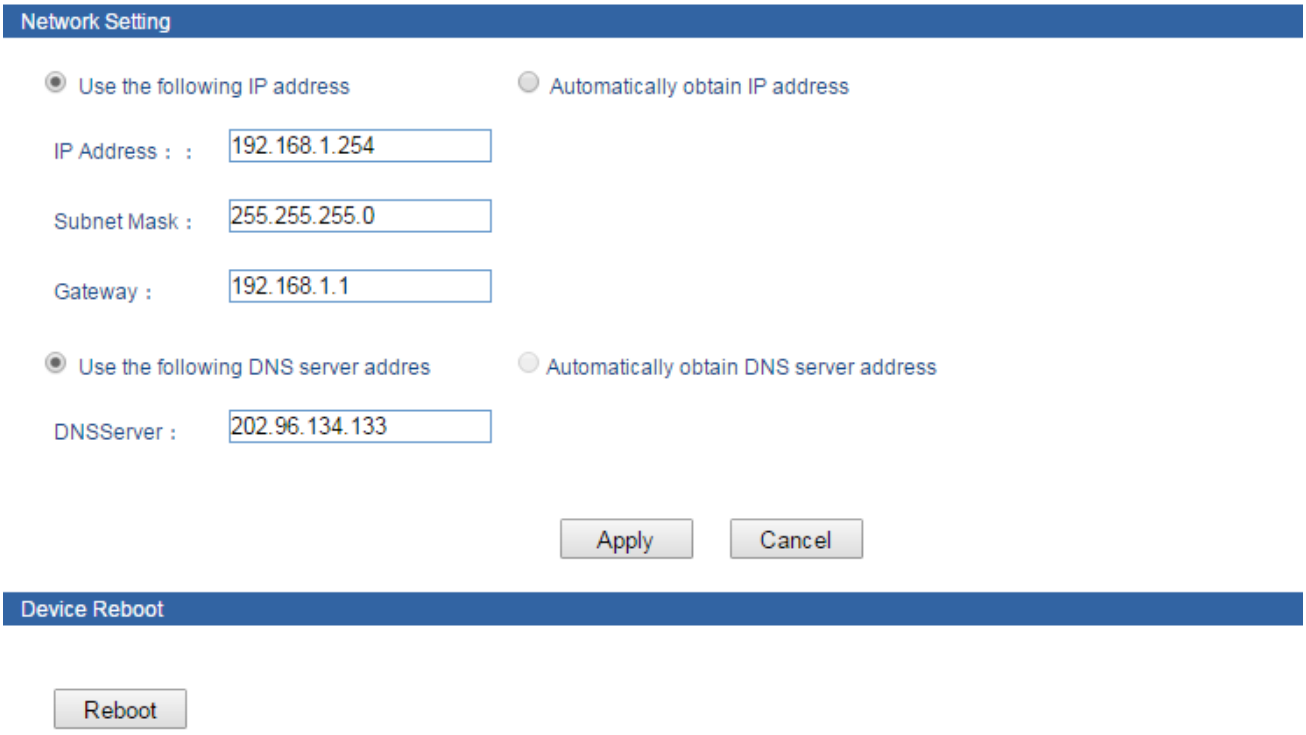
**DNS Address**

DNS (Domain Name Server) is for us to analyze domain to IP address of the Internet. If our equipment needs to access a host, you need to use this server to resolve an IP address.

**Device reboot**

Can reboot the switch remote. Knock [Basic settings/Network&reboot] menu, Enter into reboot interface, Figure as 6.12.3.

Knock<Reboot> button, after confirmation, device will be reboot. After 20 seconds, know menu bar and back to WEB manged login interface.

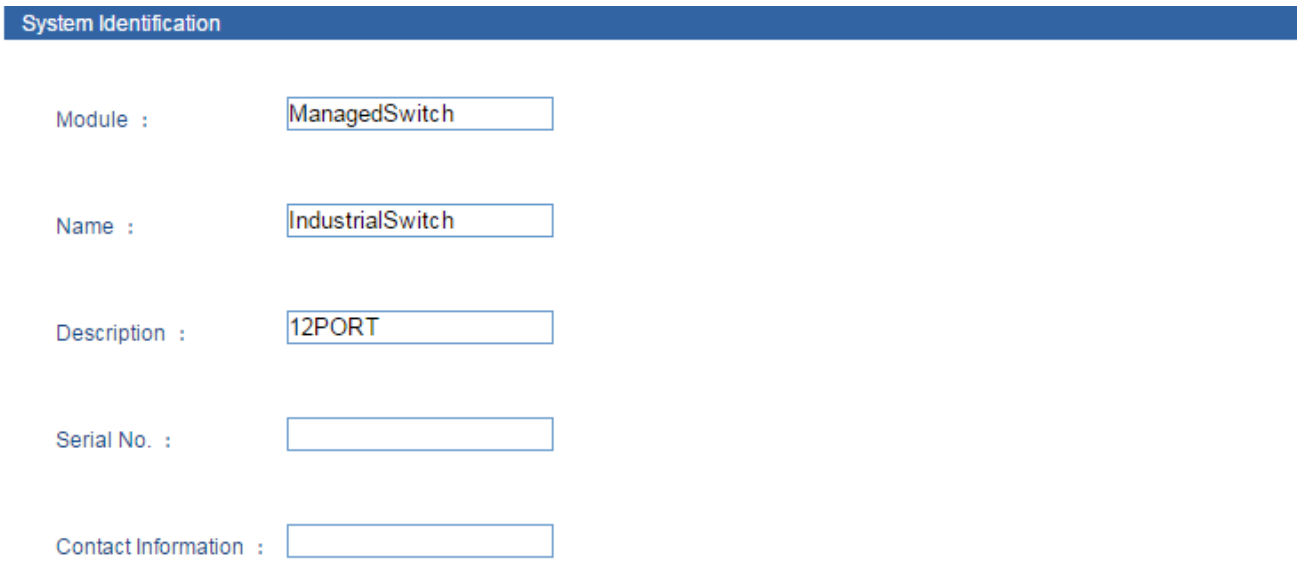



(Figure 6.12.3)

Before reboot, please save all configurations. Otherwise, all configuration will be lost

## 6.12.4 System identification

In System Identification interface we can see Model, Name, Description, Serial NO., and Contact Information. We can modify these above items by this function. It will take effect after system reboot. Figure 6.12.3 is initial device settings of the switch.




(Figure 6.12.4)

**Name**

To give a name to each device, length is not more than 16 bytes.

**Description**

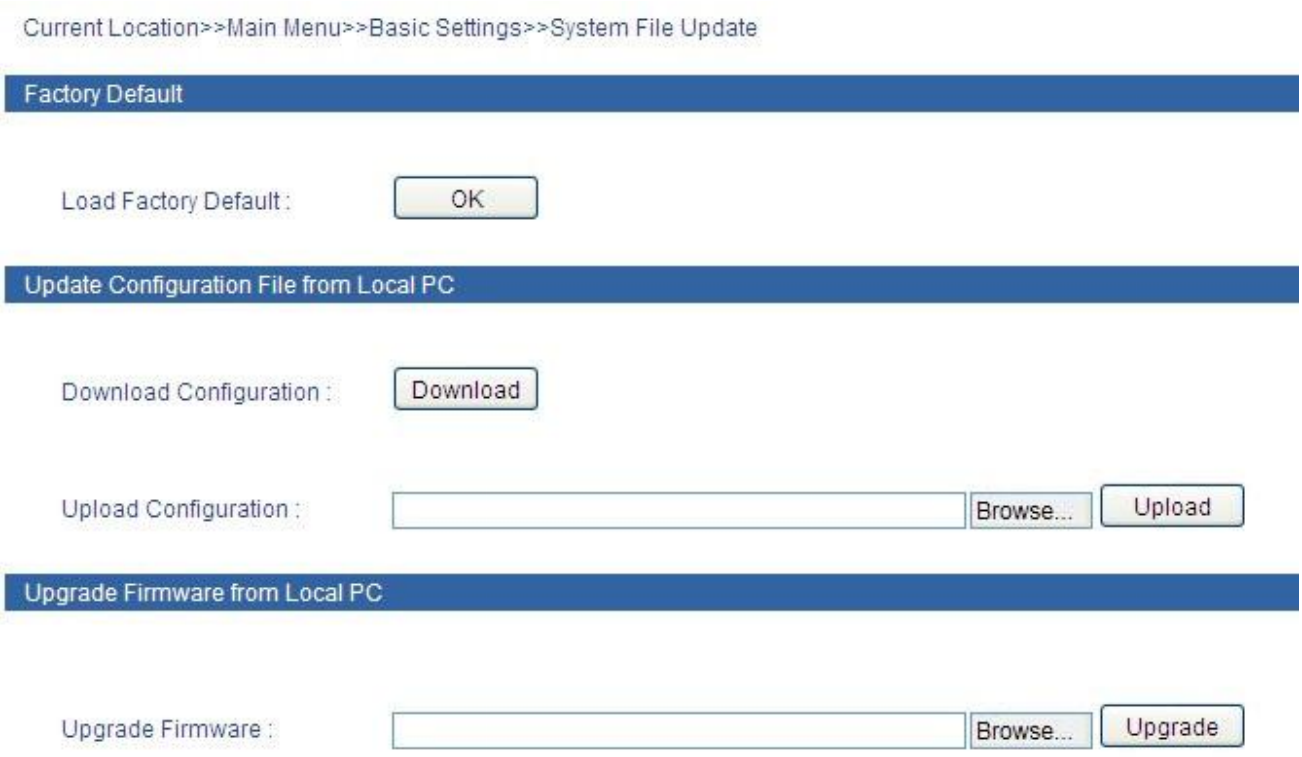
A brief description to a device, the length is not more than 16 bytes.

**Serial No.**

Display Installation Location of the device, the length is not more than 30 bytes.

### 6.12.5 System File Upgrade

The menu included 5 functions: Factory default, Download Configuration, up load configuration, upgrade firmware.




(Figure 6.12.5)

**1. Factory Default**

If you know the IP address of the device, user name and password:

Use IE to login Web interface.

Click "System Management"

Click "System File Update"

Choose "Factory Default"

Click "OK"

Notice: the IP address will be "192.168.1.254".

Open a new interface, input "192.168.1.254" to make a new configuration.

**2. Download Configuration**

If you know the IP address of the device, user name and password:

Use IE to login Web interface.

Click "System Management"

Click "System File Update"

Choose "Download Configuration"

Click "Download"

Choose the name of the file and the place to save.

**3. Upload Configuration**

If you know the IP address of the device, user name and password:

Use IE to login Web interface.

Click "System Management"

Click "System File Update"

Choose "Upload Configuration"

Click "Upload"

**4. Upgrade Firmware**

If you know the IP address of the device, user name and password:

Use IE to login Web interface.

Click "System Management"

Click "System File Update"

Choose "Upgrade Firmware"

Click "Browse" and find the place of uploading the file.

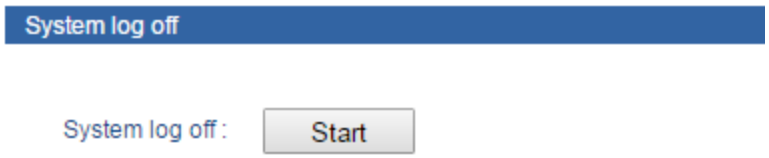
Click "Upgrade"

A suggestion" interruption of power is not allowed during uploading" , confirm it.

1. Load factory default will result in all status be in factory default settings, the IP could be static IP address "192.168.1.254".
2. Upload the configuration file, in the new configuration if static IP is not in the same network segment, the website will not be opened.
3. Use dynamic IP settings, but there is no DHCP server on the network segment, that will result in the relevant part of the IP will not be updated in the new configuration when upload configuration.

### 6.12.6 Logout

As shown in figure 6.12.6, logout functionality for the system interfaces.




（Figure 6.12.6）

**System Logout**

Click the <OK> button, the interface would be returned to the login screen, configuration does not have to be changed.

# Chapter 7 Repair and Service

The company provides a five-year product warranty, from the date of shipment. According to the product specifications, during the warranty period, the company will be free to repair or replace the product if the product has any failure or operation fails. However, these commitments do not cover damage caused by improper use, accident, natural disaster, improper operation or incorrect installation.

To ensure that consumers benefit from our managed series switches, try to get help in the following ways:

Internet service.

Make a call to our technical office.

Return or replace product.

## 7.1 Internet Service

Please visit http://www.3onedata.com

## 7.2 Make a call to our technical office

You can call our technical support office, the company has professional technical engineers to answer your questions and help you resolve your problems at the first time. Free Service Hotline: 400-600-4496

## 7.3 Repair or Replace

Please to confirm with our technical staff if your product need to repair, replace or return, and then contact our sales man to get a deal with the problem. The above should be in accordance with the company's handler to negotiate for treatment with our technical and salesman to complete the repair, replacement or return.

# Appendix 1 Glossary table

| | Glossary | Description |
|---|---|---|
| A | ARP (Address Resolution Protocol) | An IP address to physical address protocol |
| | Auto-Negotiation | Switches at both ends of the device in accordance with the maximum performance to auto-negotiate the speed and duplex mode |
| B | Broadcast Storm | A port send excessive broadcast frame meantime on the network, accumulate the respond to send messages on the network , consume too much network resources or cause the network timeout |
| | Broadcasting | A forwarding way send data to all branch of network |
| C | CoS(Class of Service) | namely 802.1p priority program, CoS offer a way for data packets to join priority tag, classify packets into 8 level with the value 0~7 range |
| D | DHCP (Dynamic Host Configuration Protocol) | Information for the network to assign dynamically IP address, subnet mask and gateway |
| | DSCP(DiffServe Code Point) | Packaged in IP packet header of 6 bit domain, can classify packets into 64 level with the value 0~63 range |
| E | Ethernet | Ethernet uses a bus or star-shaped topology and supports transmission rates up to 10Mbps orders of magnitude. A new version called fast Ethernet speeds of up to 100Mbps |
| F | Flow Control | Flow control allows low-rate devices communicate with high-rate, the flow control can match high rate port contracting speed with low rate port reception speed according to the way of high rate port pause contract |
| | Frame | Packets contain the header and tail message of physical media layer |
| | Full-Duplex | Receive and send data in progress at one moment meantime on IEEE802.3x standard |
| H | Half-Duplex | Receive or send data in one direction at one moment in progress on Backpressure standard. |
| I | IGMP (Internet Group Management Protocol) | Define the mechanism among hosts and three layers multicast device to establish and maintain the relationship between multicast group members. |
| | IEEE 802.1p | Add the priority network traffic on MAC sub layer of data link layer. |
| | IEEE 802.1q | Define the VLAN bridge operation。To manage ,define and operate VLAN on the bridge LAN |

| | | |
|---|---|---|
| **Q** | QoS (Quality of Service) | A technology to resolve the network delay and block problems and so on. |
| **T** | Trunking | To make an aggregated group tied up a group of ports together to increase bandwidth and improve the connection reliability. |
| | ToS (Type of Service) | Packaged in IP packet header of 8 bit domain to perform the different priority packets |
| **U** | UDP (User Datagram Protocol) | Face to disconnected unreliable transmission layer protocol |
| | UTP(Unshielded Twisted Pair) | Not shielded media out of twisted pair |

# Appendix 2 Treatment of common problem

**1. Why the page is not normal when configured by a web browser?**

Before the access to WEB interface, please clear the IE cache and cookies. Otherwise, the WEB interface may be not normal.

**2. How to do if you forgot password?**

You can load factory default to get the initial password if forgot the password, the exact method you can search in Network management software. The initial user name and password is “admin”.

**3. Whether the effects are equivalent that make the configuration via web and network management software?**

Configuration of both is the same, are not in conflict.

**4. What kind of alarms will be informed to technical except displayed in network management software?**

The computer buzzer of monitoring host will continue to make alarm sound when got alarm information.

**5. Why cannot increase the bandwidth after configured trunking?**

Check the Trunking Port's properties are coincident, including rate, duplex mode, VLAN etc.

**6. How to deal the problem that some of ports cannot access?**

When some of ports can no access, that may be line fault, network card failure and switch port failure, by the following test to find faults:

1. Only change a new Ethernet cable.
2. Use the same Ethernet cable and switch port, to replace the computer.
3. Use the same Ethernet cable and computer, to access other ports.
4. If have confirmed switch fault, please contact manufacture to repair.

**7. What about the order of port adaptive status detection?**

Port to detect the status in the following order: 100Mbps full duplex, 100Mbps half duplex, 10Mbps full-duplex, 10Mbps half duplex, in descending order to detect and automatically connect with the highest speed.