3onedata
Make network communication more reliable

IES615-2DI series
Managed Industrial Ethernet switch
User manual

Version 1.0.0, Aug. 2017

www.3onedata.com

IES615-2DI series user manual

Statement

Copyright Notice

Information in this document is reserved by 3onedata Co., Ltd. Reproduction and extract without permission is prohibited.

Trademarks Notice

3onedata, 3onedata® and 3One data® is registered trademarks of 3onedata Co., Ltd. All other trademarks or registered marks in this manual belong to their respective manufacturers.

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 supply input 3
2.3 Relay connection 3
2.4 DIP switch 3
2.5 Communication port 3
2.6 Serial port connection 5
2.7 LED Indicator 6
2.8 Installation 6
Chapter 3 Appearance and Dimension 8
3.1 Appearance 8
3.2 Dimension 8
CHAPTER 4 PACKLING LIST 9
CHAPTER 5 Network Configuration 10
5.1 Modify IP address 10
5.2 Login Web Server 11
5.3 Introduction configure interface 11
5.3.1 Main menu 12
5.4 System Status 13
5.4.1 System information 13
5.4.2 Port information 14
5.5 Serial Server 14
5.5.1 COM Settings 14
5.5.2 Configure working mode 17
5.5.3 COM Information 20
5.6 Port Configuration 20
5.6.1 Port Settings 20
5.6.2 Bandwidth Management 22
5.7 L2 Features 23
5.7.1 VLAN 23
5.7.2 IGMP snooping 27
5.7.3 Static Multicast 27
5.8 QOS 28
5.8.1 QOS Classification 28
5.8.2 COS 29
5.8.3 TOS (DSCP) 30
5.9 Redundancy 31
5.9.1 Port Trunking 31
5.9.2 Rapid Ring 32
5.9.2.1 Ring V3 single ring configuration. 34
5.9.2.2 Ring V3 dual ring configuration 35
5.9.2.3 Ring V3 Coupling Configuration 35
5.9.2.4 Ring V3 Chain Configuration 36
5.9.2.5 Ring V3 Dual_homing Configuration 37
5.9.3 Rapid Spanning Tree Protocol (RSTP) 39
5.10 Access Profile 41
5.10.1 Login Settings 41

5.11 Remote monitoring 42
5.11.1 SNMP management 42
5.11.2 Relay Alarm 44
5.12 Traffic Statistics 45
5.12.1 RX frame statistics 45
5.12.2 TX frame statistics 46
5.13 Diagnosis 46
5.13.1 Mirror 46
5.14 Basic settings 47
5.14.1 Device address 47
5.14.2 System identification 49
5.14.3 System File Upgrade 50
5.14.4 Logout 51
Appendix 1 Glossary table 52
Appendix 2 Default factory 54
Appendix 3 Treatment of common problem 55

CHAPTER 1 SUMMARIZE

1.1 Introduction

The IES615-2DI (3IN1) series is a managed industrial Ethernet switch that provides 5 Fast Ethernet ports, 2 three-in-one RS-232/485/422 serial ports. The electrical port supports 10 / 100M adaptive, MDI / MDI-X adaptive. Power supply supports 12 ~ 48VDC input.

The -40~75℃ operating temperature range to adapt to the harsh working environment. Rail mounting features to meet the needs of industrial sites, the user's Ethernet equipment to provide a reliable, fast solution.

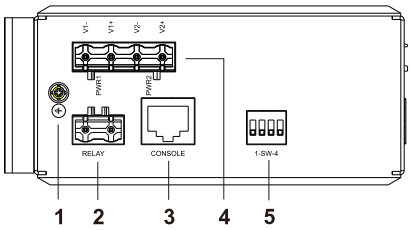
1.2 Features

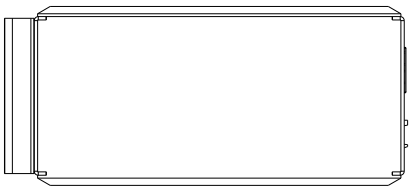
- Supports IEEE802.3, IEEE802.3u, IEEE 802.3x, IEEE802.1Q, IEEE802.1p, IEEE802.1D, IEEE802.1W
- Supports 5-port Fast Ethernet, copper ports and optical fiber ports optional
- Supports 2-Port optical isolation of the three-in-one (RS-232/485/422) serial server
- Support based on socket application access
- Supports TCP Server, TCP Client, and UDP based mode; TCP Server and UDP advanced mode
- SW-Ring ring network patent technology (Fault recovery time<20ms)
- Support RSTP, way exchange time<1s
- Supports static multicast, QoS function
- Supports Port based VLAN and IEEE 802.1Q VLAN
- Industrial grade design, -40~75°C work temperature
- IP40 protection grade, DIN-Rail mounting
- No fan design

CHAPTER 2 HARDWARE DESCRIPTION

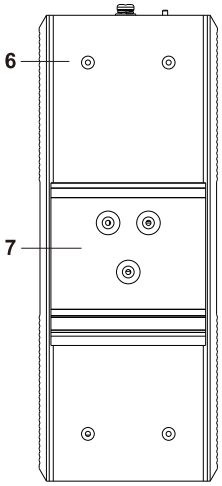
2.1 Panel design

Vertical view and Bottom view

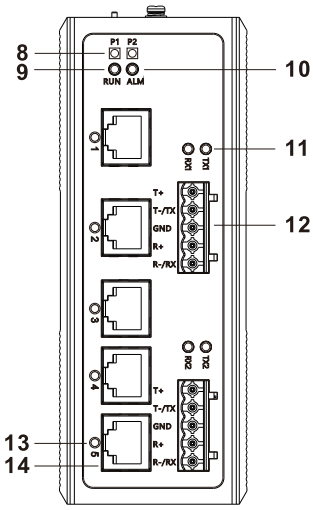




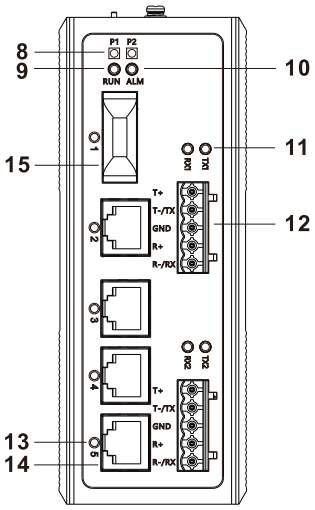
Rear view



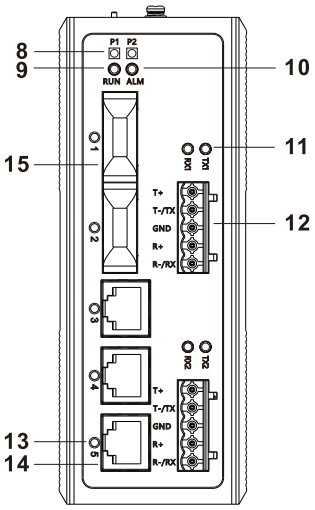
Front view



IES615-2DI (3IN1)



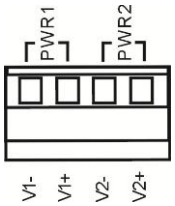
IES615-1F-2DI (3IN1)



IES615-2F-2D (3IN1)

1. Ground screw
2. 2-pin terminal block for relay output
3. Console port
4. 4-pin terminal block for power input
5. DIP switches for default factory
6. Screw holes for wall mounting kit
7. DIN-Rail mounting kit
8. Power LEDs (PWR1, PWE2)
9. System running LED
10. Relay alarm LED
11. Serial port transmits and receives data LEDs
12. RS-232/485/422 serial ports
13. Ethernet port Link/ACT LEDs
14. 10/100Base-T(X) Ethernet ports
15. 100Base-FX fiber ports

2.2 Power supply input



The switch have redundant power input, provides one terminal block (4 bits) for PWR1 and PWR2 input. The redundant power can be used single and used two self-governed power to supply to the system, PWR1 and PWR2 input at the same time, when neither of these two power fails, the other power acts as a backup, and automatically supplies power needs, ensure running Ethernet reassuring. Voltage input range is 12～48VDC (terminal block defined as: V1-、V1+、V2-、V2+).

2.3 Relay connection



The relay owns two contacts of the terminal block on the top panel of the Switch series. It is used to detect both power failure and port failure. The open circuit state in normal non alarm state, when there is any alarm information to the closed state. The relay can external alarm lights or alarm buzzer or external switch signal acquisition device in order to timely notify operators when an alarm occurs.

2.4 DIP switch

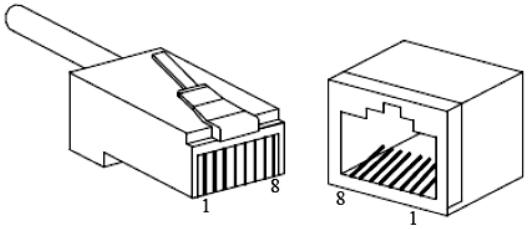


Top panel provided 4 bits DIP switch to do function configure (OFF is default factory). 1 and 4 are reserved. 2 is recovery default factory. 3 is upgrade. Please power off and power on when you change the status of DIP switch.

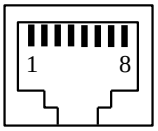
2.5 Communication port

10Base-T /100Base-TX Ethernet port

10Base-T/100Base-TX Ethernet port is located on front panel and the type is RJ45. The pinout of RJ45 port connects to UTP or STP. The distance is not more than 100m. 100Mbps Ethernet connector takes 120Ωof UTP 5, 10Mbps Ethernet connector takes 120Ω of UTP 3, 4, 5.



RJ45 port supports automatically MDI/MDI-X connection. It can connect PC, Server, Converter and HUB .Corresponding connection of Pin 1,2,3,6 is like this: 1→3, 2→6, 3→1, 6→2. The definition of Pin is displayed as below.

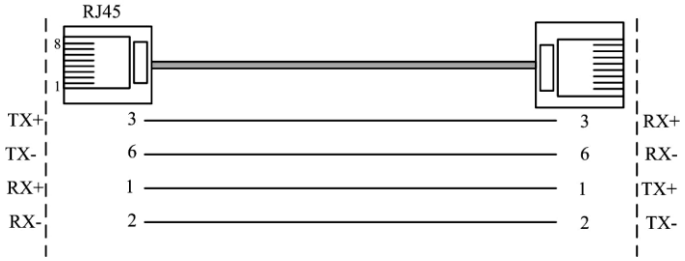


PIN	MDI	MDI-X
1	TX+	RX+
2	TX-	RX-
3	RX+	TX+
6	RX-	TX-
4, 5, 7, 8	—	—

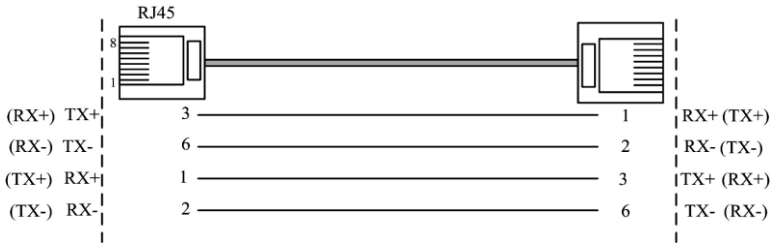
Information necessary to explain:

Note: “TX±”Transmitting data±, “RX±”receiving data±, “—”no use

MDI(**straight-through cable**):



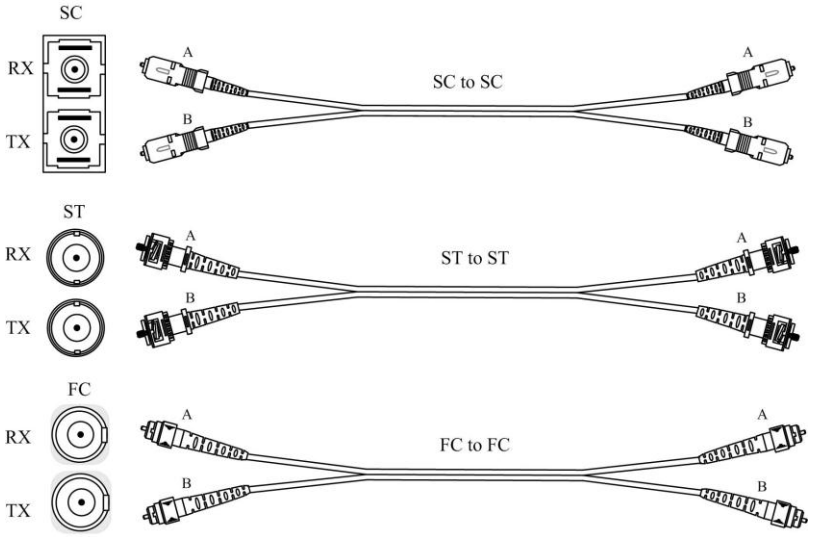
MDI-X(**Cross over cable**):



100Base-FX fiber port

100Base-FX port works with full-duplex, SM or MM SC/ST/FC optional. The fiber port must be used in pair, TX (transmitting) port connects remote switch’s RX (receive) port; RX (receiving) port connect remote switch’s TX (transmitting) port.

Suppose: If you make your own cable, we advise to label the two sides of the cable with the same letter (A-to-A and B-to-B, shown as below, or A1-to-A2 and B1-to-B2).



2.6 Serial port connection

Serial port:

The RS-232/485/422 serial port uses 5-pin terminal block as shown below.



PIN	RS-232	RS-485	RS-422
1	-	D+	T+
2	TX	D-	T-
3	GNS	GND	GND
4	-	-	R+
5	RX	-	R-

2.7 LED Indicator

System Indication LED		
Led	**State**	**Description**
P1	ON	PWR1 is connected and operates properly.
	OFF	PWR1 is not connected or operates abnormally.
P2	ON	PWR2 is connected and operates properly.
	OFF	PWR2 is not connected or operates abnormally.
RUN	ON/OFF	The system is running abnormally.
	Blinking	The system is running properly.
ALM	ON	When the alarm is enabled, power or the port's link is inactive.
	OFF	Power and the port's link is active, the alarm is disabled.
1~5	ON	The Ethernet port is connected properly.
	Blinking	The Ethernet port is connected and data is being transmitted.
	OFF	The Ethernet port is not connected properly.
TX(1~2)	Blinking	The serial port is transmitting data
	OFF	No serial data transmission
RX(1~2)	Blinking	The serial port is receiving data
	OFF	No serial data received

2.8 Installation

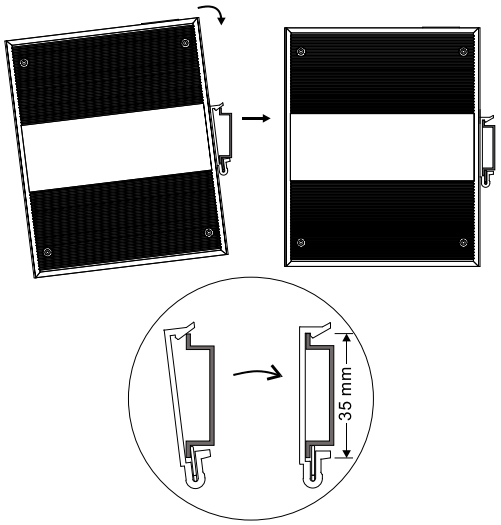
Before installation, confirm that the work environment meet the installation require, including the power needs and abundant space. Whether it is close to the connection equipment and other equipment are prepared or not.

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: Redundant, dual 12-48VDC power input
5. Environment: working temperature: -40～75℃
   Storage Temperature: -40～85℃
   Relative humidity 5%～95%

DIN Rail Installation

In order to use in industrial environments expediently, the switch adopt 35mm DIN-Rail installation, the installation steps as below:

1. Examine the DIN-Rail attachment
2. Examine DIN-Rail whether be firm and the position is suitability or not.
3. Insert the top of the DIN-Rail into the slot just below the stiff metal spring.
4. The DIN-Rail attachment unit will snap into place as shown below.



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

IES615-2DI(3IN1)



IES615-1F-2DI(3IN1)

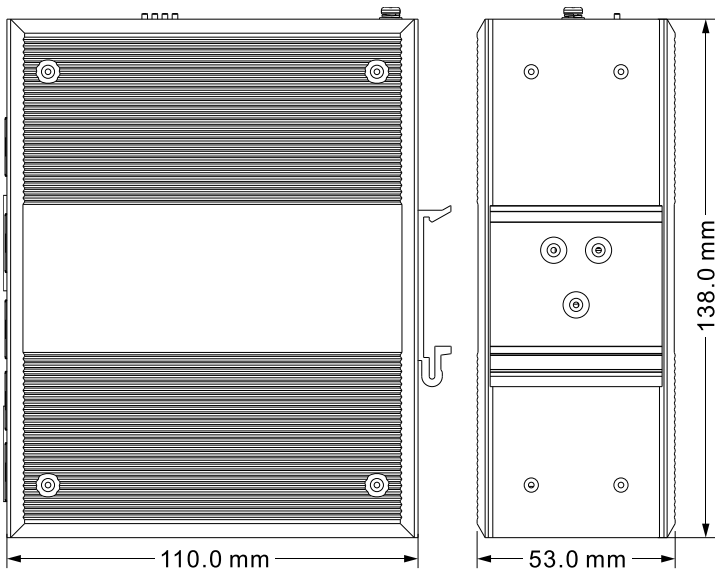


IES615-2F-2DI(3IN1)



3.2 Dimension

The series of products are the same size, but their types of interfaces are different. Unit (mm)



Chapter 4 Packing List

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

Description	Quantity
Industrial Ethernet switch	1
User manual	1
Documentation and software CD	1
Warranty card	1
Certificate of quality	1
DIN-Rail mounting kit	1

Chapter 5 Network Configuration

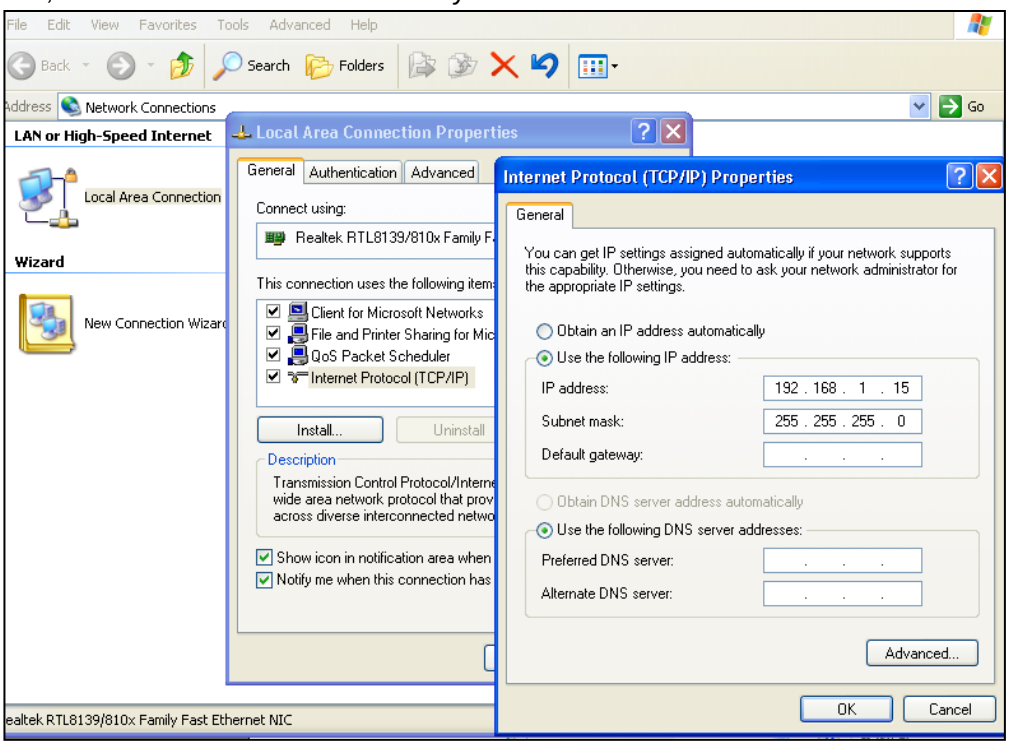
5.1 Modify IP address

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

You can modify PC's or the 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.



(Figure 5.1.1)

Method 2: Modify the switch's IP address through Blue_eyes manager software.

- Install Blue_eyes manager software on the PC.
- Enter into Blue_eyes 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.

Configuration preparing

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

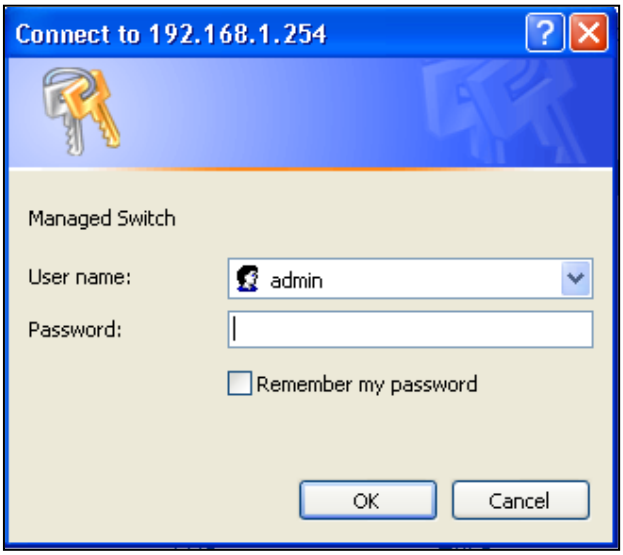
- Install operating system (Windows XP/2000/7/8,etc)
- Install Ethernet card
- Install Web explorer (IE6.0 or higher version)
- Install and start TCP/IP protocol

2. Establish the correct network configuration

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.

5.2 Login 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 "Access denied" 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 5.2.1)

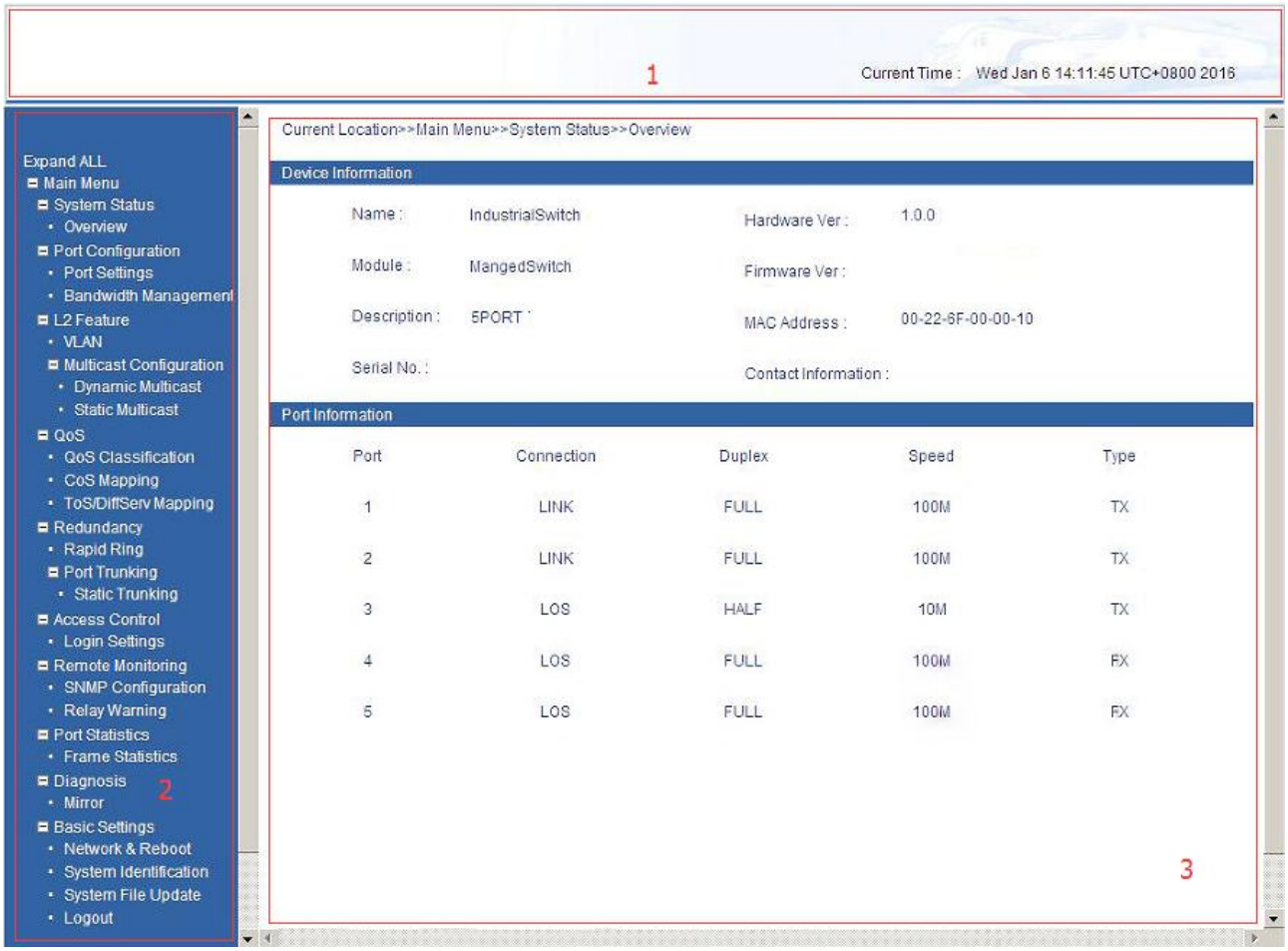
The default username and password is [admin], case sensitive for this series. The default password is with administrator privileges.

:

Before entering the switch Web Server, you must delete temporary IE files, and clear IE history, or perhaps because IE cookies due to an unknown error.
The user name and password are case sensitive. Such as unclear devices IP address, can be obtained through the Blue_eyes management software search. (attached)

5.3 Introduction configure interface

The Web configuration page is divided into: 1 title, 2 main menu, 3 configuration menu bar area three parts. Click the menu item in the menu bar, you can enter the corresponding configuration interface, display device state information and data configuration. As shown in Figure 5.3.1.



(Figure 5.3.1)

5.3.1 Main menu

Menu Introduction:

Main Menu	Tag	Function
System Status	System information	Display device information and port information such as software version, IP address, etc.
Serial Server	COM Settings	Serial parameter and Working mode configuration
	COM Information	Display incorrect data statistics and connection information that send by serial port.
Port Configuration	Port settings	Display and configure information of each port: such as connection status, configuration modes, flow status etc.
	Bandwidth management	Set the maximum rate of the input/output packets for port.
L2 feature	VLAN	Displays the current list of 802.1Q VLAN, configure and manage 802.1Q VLAN.
	IGMP snooping	Display port-based VLAN list, and to configure and manage port-based VLAN.
	Static Multicast	Configure the static multicast MAC address and its corresponding port.
QOS	QoS classification	Configure the QOS queue mode, QOS implementation and port default priority.

Main Menu	Tag	Function
	Cos Mapping	Configure the meaning of COS value.
	ToS/DiffServ Mapping	Configure the DSCP priority.
Redundancy	Port Trunking	Configure port trunking group.
	Rapid Ring	Configure the rapid ring network port and type.
	RSTP	Configure the parameters of RSTP.
Access control	Login Settings	Configure different permissions for the user name and password.
Remote Monitoring	SNMP	Set up a simple configuration
	Relay Warning	Set relay alarm type
Port Statistics	Frame statistics	
Diagnosis	Mirror	Configure the mirror port and mirrored port.
Basic Settings	Network & Reboot	Device IP, gateway, DNS and Device reboot
	System Identification	Model, Name, Description and Contact information.
	System Log	Log information.
	System File update	Software upgrade, acquire, preserve or restore the switch configuration.

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.

5.4 System Status

Enter the correct user name and password that the normal the switch WEB interface display information about the state of the system, including: the main menu, equipment information, port information, and displayed in the upper left corner of the page's 3onedata Technology Co., Ltd. the registered trademark, the upper right corner of display is the current time, as shown in figure 5.4 show:



(Figure 5.4)

5.4.1 System information

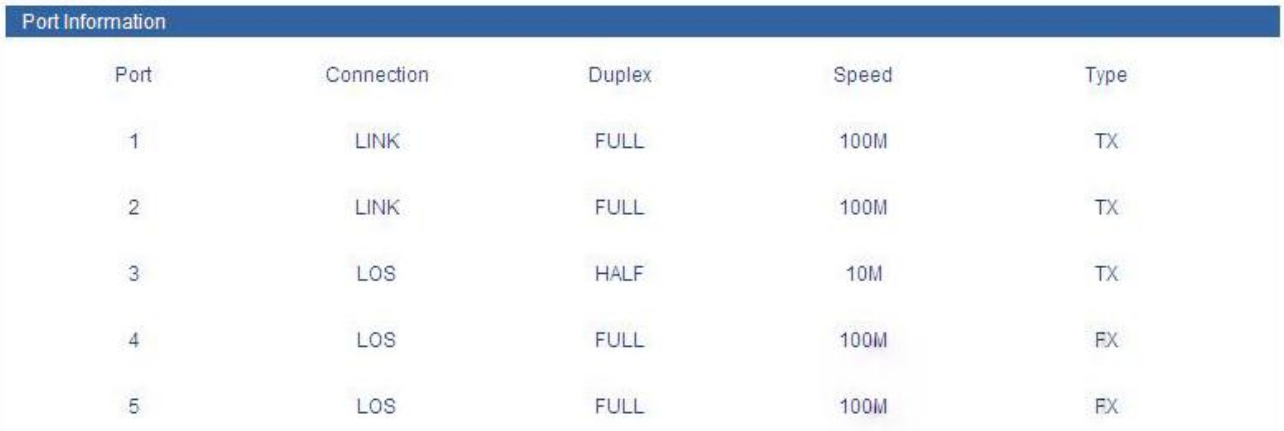
Equipment information mainly display basic information, the switch include: equipment name, description of the equipment, hardware version number, firmware version, the switch of MAC address. As shown in figure 5.4.1



(Figure 5.4.1)

5.4.2 Port information

The switch a total of 5 ports, ports can confirm whether the port with the equipment complies with the information bar. Equipment at work, via the port status of the port information in the status view, for example in the figure below you can see port 3 is LINK and port connection status as FULL, speed is 100M and port type for the TX(RJ45). As shown in Figure 5.4.2.
LINK:Indicates that the port is in a connected state;
LOS:Indicates that the port is not connected;
FULL:Indicates that the port State is full duplex;
HALF:Indicates that the port State is half-duplex (if the ports are not connected, the port status is HALF);



(Figure 5.4.2)

5.5 Serial Server

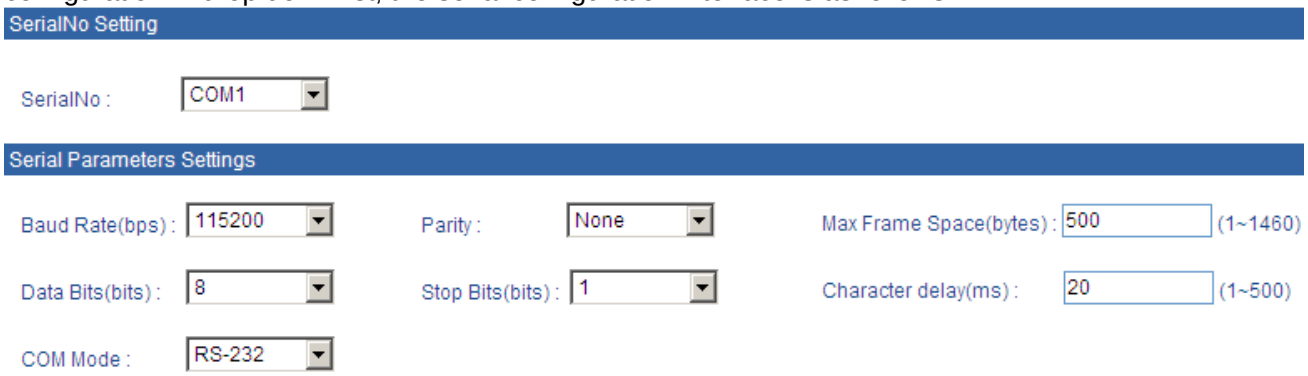
5.5.1 COM Settings

Server configuration includes the serial port configuration and mode of operation of the configuration parameters

Serial port configuration menu	Optional data	Description
Serial port working mode	RS-232 full duplex/RS-422 full duplex/RS-485 half duplex	Serial work mode
Baud rate(bps)	300-115200(10pcs band rate optional)	Baud rate choice
Parity	None, Even, Odd, Mark, Space	Checkout choice
Data bits(bits)	5,6,7,8	The parameter of serial

Stop bits (bits)	1,1.5,2	The last of the data package
Max frame space(bytes)	1-1460	The length of frame from serial data to Ethernet data.
Character delay(ms)	1-500	The time space from serial data to Ethernet data

Enter into the switch WEB interface, knock [Serial Server/COM settings]; please choice necessary configuration in drop down list, the serial configuration interface is as follows:



(Figure 5.5.1)

Configuration option: [Baud rate], [Parity], [Data Bits], [Stop Bits], [Max Frame Space], [Character Delay] and [COM mode], the explaining is as follows:

[Baud rate]

It is a parameter to check the communication speed. It shows to transfer how many bits in 1 second. For example, 300 baud rate means have 300 bits transferred in 1 second.

[Parity]

Parity bits: It is a simple method to checkout fault in serial communication, have 4 types: Even, Odd, Mark, Space

[Data Bits]

It is a parameter to check the actual data bits in communication.
When PC send a Packet, actual data is not 8 bits, the standard is 5, 6, 7, 8.

[Stop Bits]

The last bit of the single Packet. Typical value is 1, 1.5 and 2 bit.
When a data bit is 5, stop bit 1.5 and 1 option. When a data bit is 6, 7, 8, stop bit 1 and 2 option.

[Max frame space]

The frame length that serial interface data convert into Ethernet data, within the range of setting time, it forward when data is equal to or longer than the setting frames.
Available setting value ranged from1 to 1460.

[Character Delay]

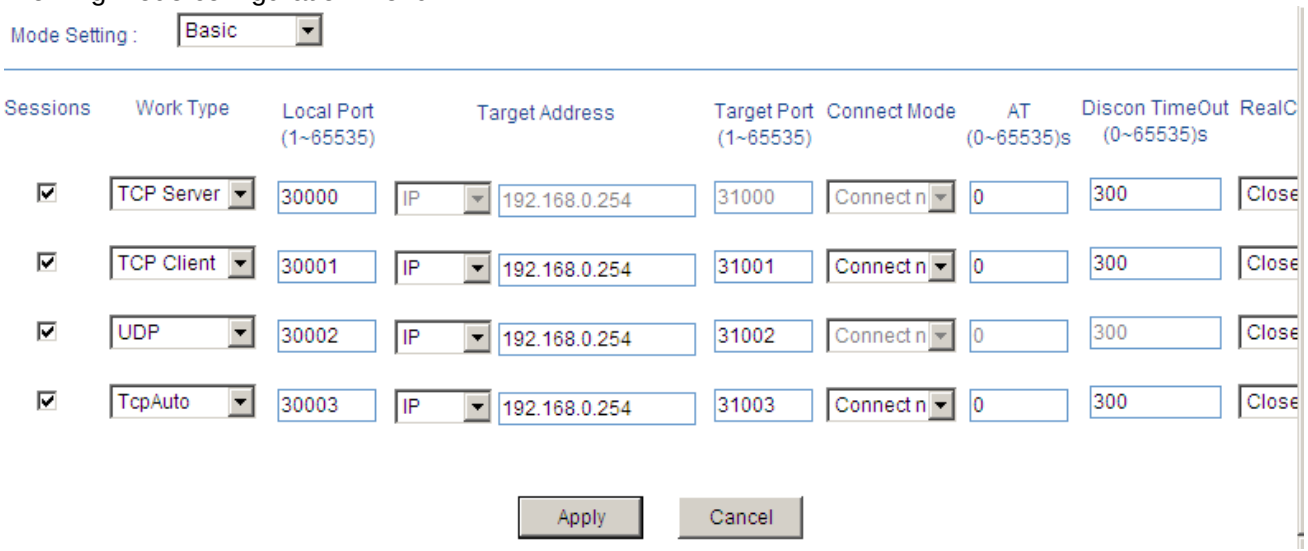
The wait time when serial interface send data do not 1 data frames. If up to this time and do not have data, then send automatic. Can configure 1-500.

[COM mode]

RS-232, RS-485, RS-422 serial port Optional.

5.5.2 Configure working mode

Working mode configuration menu



(Figure 5.5.2.1)

[Sessions]

Each serial port of serial device servers can support 1-4 sessions. It means serial port of serial device server send the received data to Ethernet through socket. More than one of the sessions means serial port of serial device server sends the received data to Ethernet through more than one socket. Sessions enable to use by checking the corresponding box.

Basic mode

1. TCP Client

As TCP Client side, serial device server will connect forwardly to TCP/IP network equipment, such as PC. It need to setup to tell serial device server to connect which network address and TCP port number when conditions is matched. After creating socket, serial device server will sent the data received from each serial port through socket On the contrary, the data received from socket will be sent to the corresponding serial port.

TCP Client setting option: [Destination address], [Destination port] and [Connect mode]

The explanation of these setting is as follows

[Local port]

The configuration is the same TCP server, default is 1~65535.

[Destination address]

The IP address or domain name address that device will connect, both of them can correspond the host computer address on the Internet

[Destination port]

The port that device will be connected, default is 1~65535.

[Connect mode]

Connection mode has 2 types: Immediately and Data trigger

Immediately: When the switches have power supply, it will connect immediately, if connection cut off,

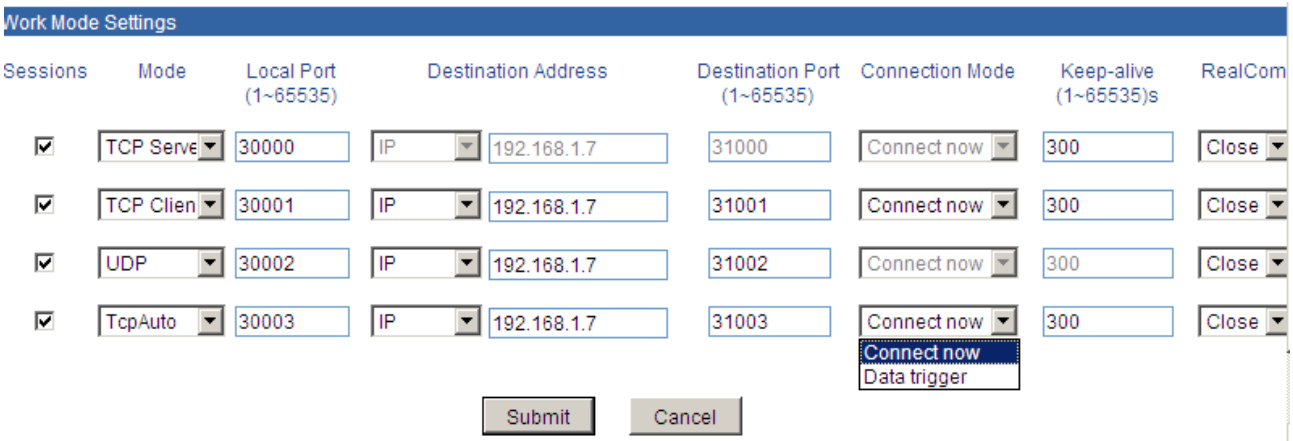
it will connect immediately.

Data trigger: Once the switch receive the data, it will connect immediately.

[Keep-alive]

Setting the vacancy time for connection cut off automatic; if there do not have data transfer, the connection will cut off. If set “0”, means do not care how much time vacancy, the switch do not cut off voluntary. The range is 1-65535s. Default is 300s

The figure below is the configuration interface of TCP Client Mode. Session 2 is setting to local address available for router. “192.168.1.7”, the “Destination Port” connected to serial port is host computer 192.168.1.7” 31001 port, Connection mode is Immediately, Disconnect Keep-alive time is 300 seconds, click “Submit’, setting successful. Please pay attention to pure TCP Client, TCP Server, UDP or TcpAuto mode.



(Figure 5.5.2.2)

2. TCP server

TCP Server, Passive connect, one pivotal parameter is [Local port], have relationship with other setting, need combine setting

[Local port]

The switch provided TCP port can be connect by other TCP/IP node, the TCP port have the relationship with the switch’s relevant serial interface. The figure as follows is TCP Server setting interface, Session 1 set local port is 30000, external TCP port connect switch through this port. Connection keep-alive time is 300 second. Click “Submit”, setting successful as figure 5.5.2.2.

3. UDP

Under the UDP work mode. The switch is server and also client, the relevant setting is “Local port”, “Target address” and “Target port”. It can support point to point and multicast UDP, setting method is the same as TCP.

4. TCP Auto

In this Mode, serial device server can act as server or client. Before setting this Mode, please ensure related parameters are correct when you turn on the server mode, client mode is automatically disconnected.

5. RealCom

RealCom support TCP Server and TcpAuto, can choice open and close function in RealCom, figure 5.5.2.2.

When device open the RealCOM function, can cooperate with VSP Management Software create virtual COM port to communication, now, device’s work mode is server, the virtual COM port is client,

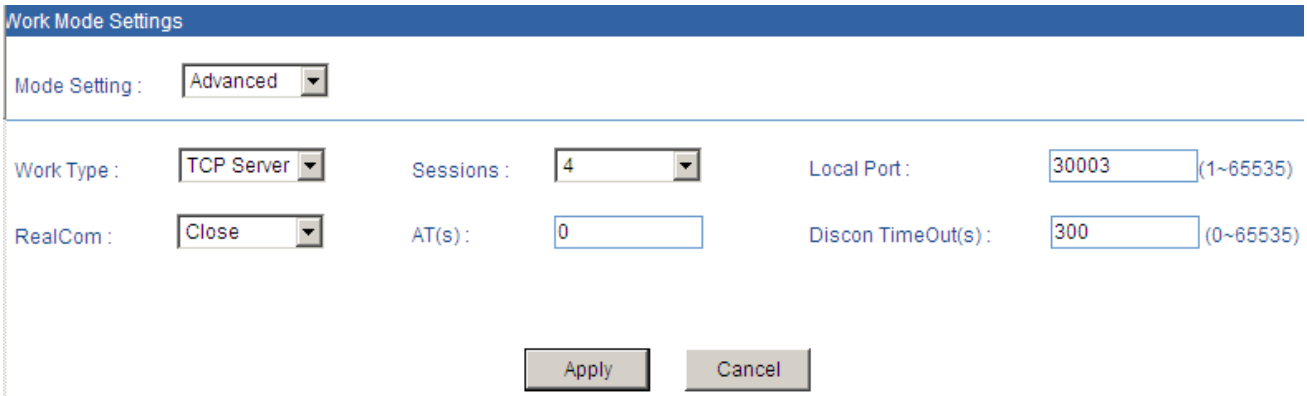
how to create the Virtual COM port, please the VSP Management Software user manual.

1. Address pool just support Type A and type B address
2. Start address and end address must in the network segment.
3. Start address value must less than or equal to end address.

Advanced mode

1. TCP server

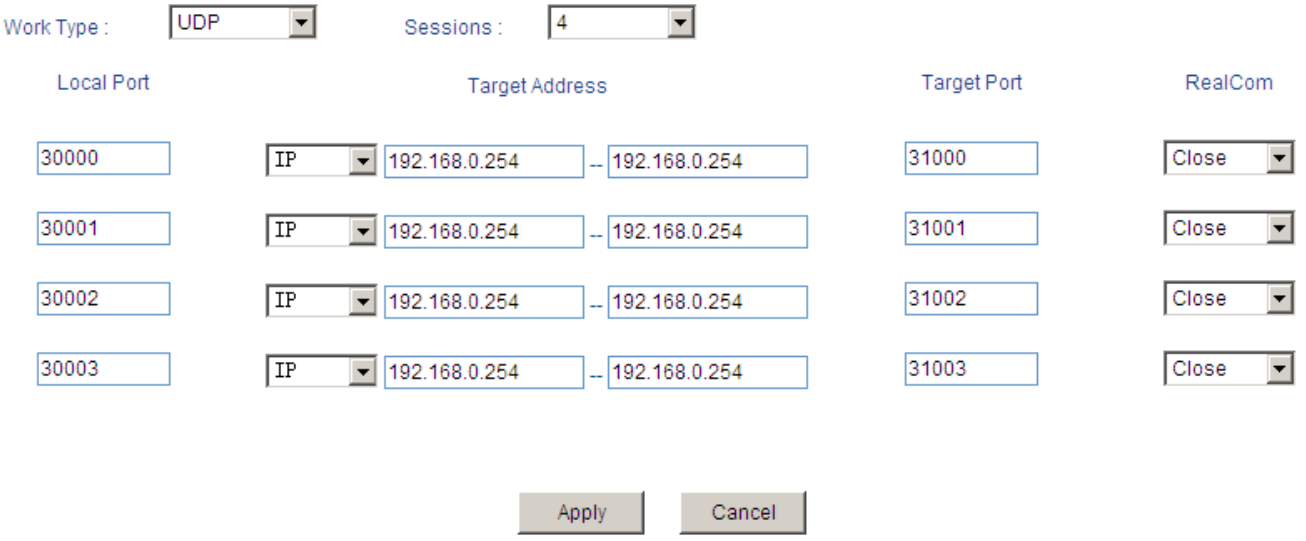
Under this mode, series is server, the switch can choice 0-4 channel connection at the same time, configuration mode is the same based mode. Figure 5.5.2.3 as follows:



(Figure 5.5.2.3)

2. UDP

Under this mode, Target address is a address pool, all of the address in pool can connect with the switches, can choice 0-4 channel connect at the same time. Figure 5.5.2.4 as follows:



(Figure 5.5.2.4)

1. Address pool just support Type A and type B address
2. Start address and end address must in the network segment.
3. Start address value must less than or equal to end address.

5.5.3 COM Information

It main function of serial port information: Display incorrect data statistics and connection information that send by serial port. Figure as 5.5.3

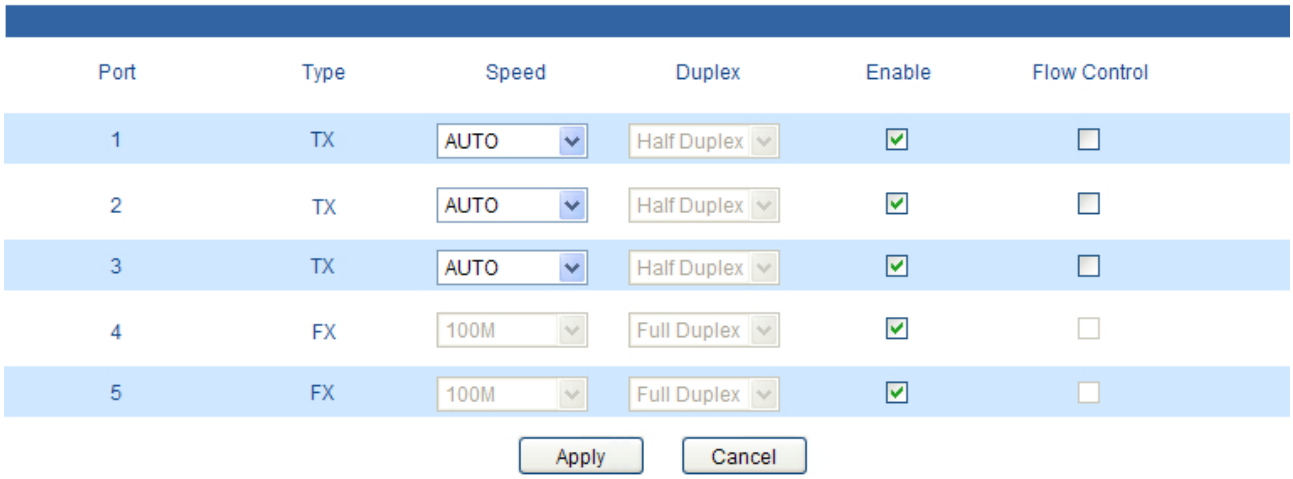


(Figure 5.5.3)

5.6 Port Configuration

5.6.1 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.



(Figure 5.6.1)

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.
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 and 100Base-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. 1000M fiber port uses 1000Base-X standard and single/multi-mode fiber for connection. Main fiber of 1000Base-X standard includes: 62.5nm multi-mode fiber and 50nm multi-mode fiber. Gigabit SFP port slot needs to be used with the SFP optical module.

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 IEEE802.3x 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.

5.6.2 Bandwidth Management

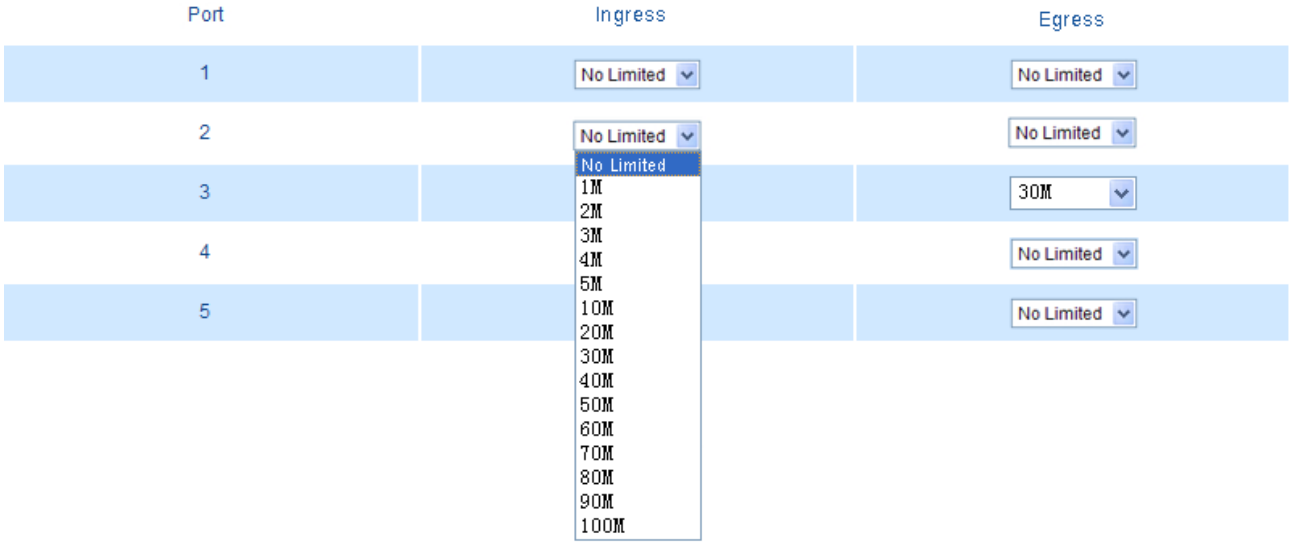
Bandwidth management mainly refers to limit the data's egress and ingress bandwidth to save the network sources.

Click [port setting/bandwidth management] and enter into the following interface.

Egress Bandwidth Configuration:

"----" stands for no limitation for the speed, the others are corresponding speed.

As shown in following figure 5.6.2.1, the forcible egress rate of Port 3 is 30Mbps. Only need to select 30Mbps in egress rate setting of Port 3. The bandwidth of Port 3 as receiver is still 100Mbps, but the forcible egress bandwidth of Port 3 is 30Mbps.

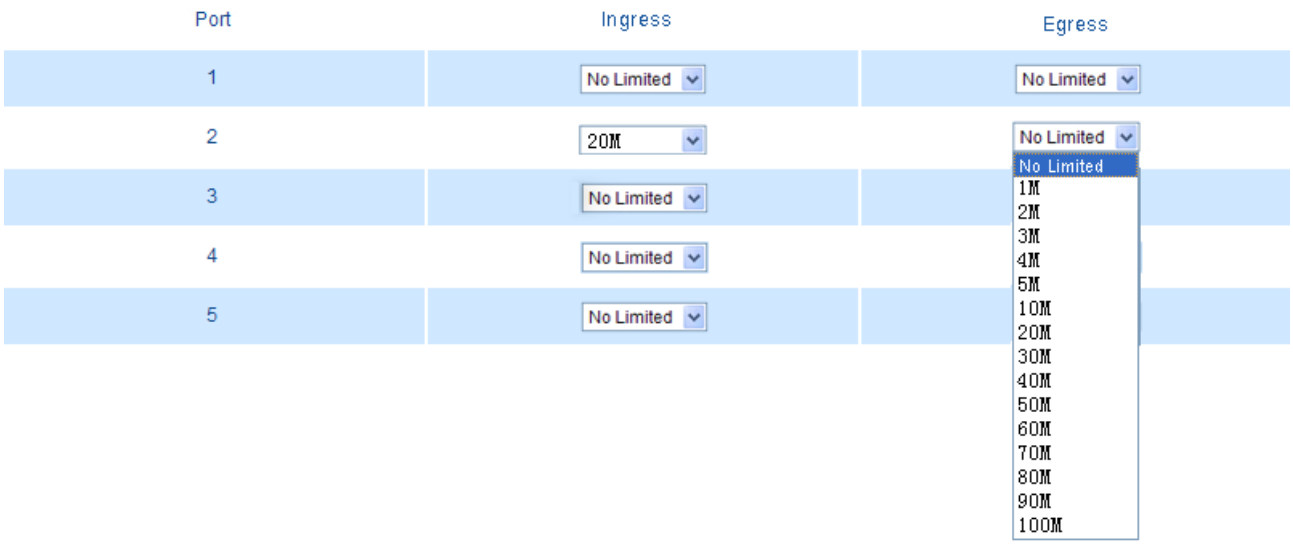


(Figure 5.6.2.1)

Ingress Bandwidth Configuration:

"----" stands for no limitation for the speed, the others are corresponding speed.

The ingress rate is related to CoS priority. As shown in following figure 5.6.2.2, the forcible ingress rate of Port 2 is 20Mbps. Only need to select 20Mbps in ingress rate setting of Port 2. The bandwidth of Port 2 as transmission is still 100Mbps, but the forcible ingress bandwidth of Port 2 is 20Mbps.



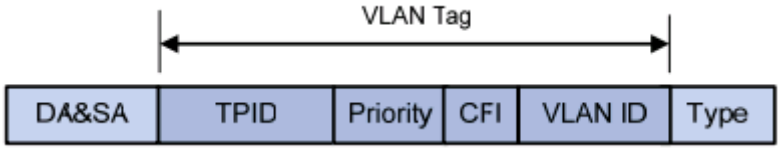
(Figure 5.6.2.2)

5.7 L2 Features

5.7.1 VLAN

The product 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 product 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

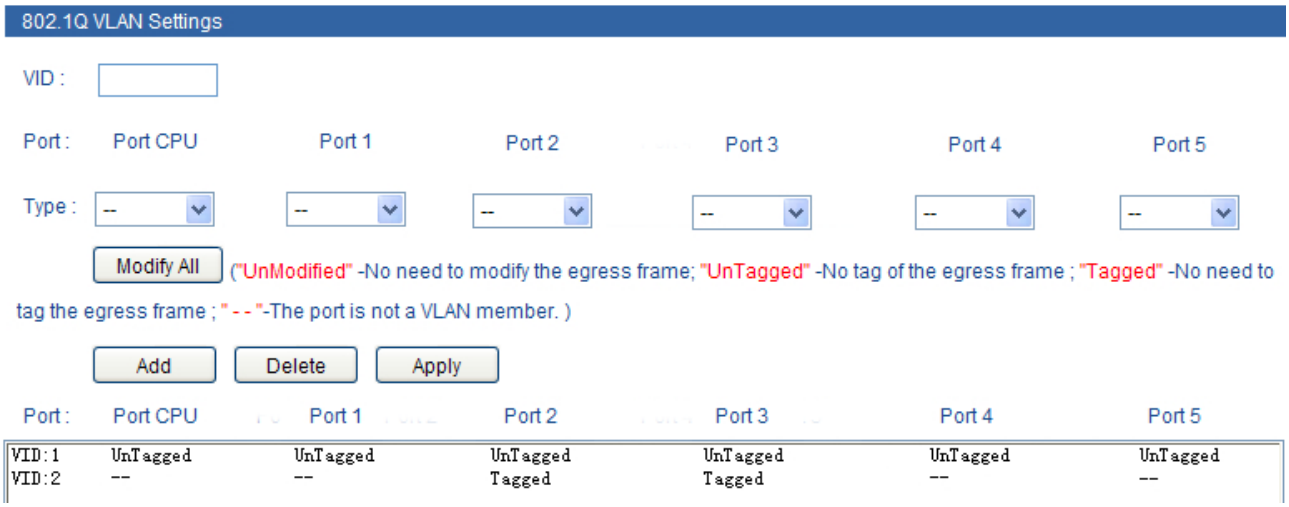
The default VLAN, all port are Access, PVID: 1, all belong to the members of VLAN1

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 5.7.1.1, create VLAN1, port type: Access, member type: Untagged, member included CPU port and port 1~5. Create VLAN2, type of port 2, 3: Trunk, member type: Tagged.



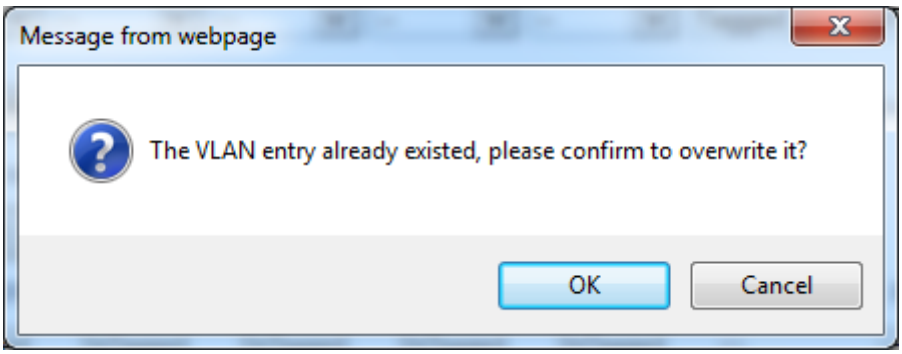
(Figure 5.7.1.1)

We can know as the figure, the type of port 2, 3 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 5.7.1.2. Add new VLAN items into table and click[Apply] and reboot the device. Modify VLAN finished.

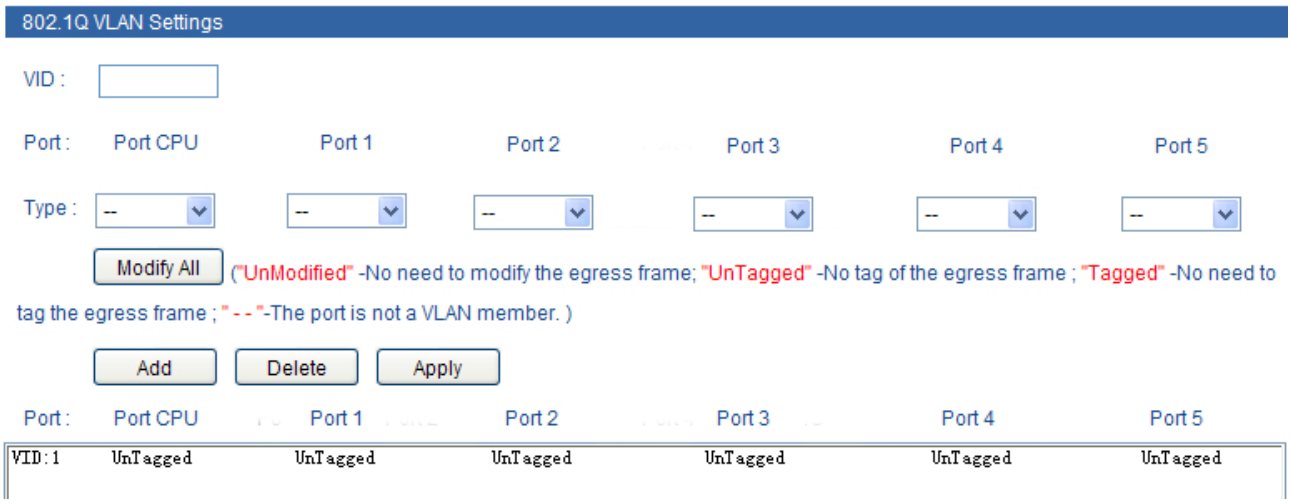


(Figure 5.7.1.2)

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 5.7.1.3:

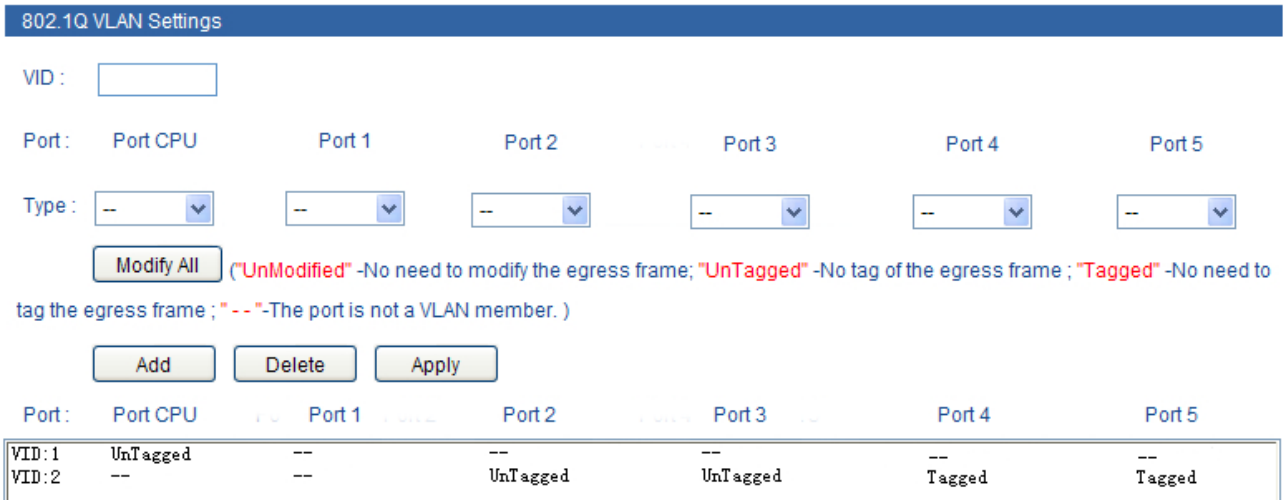


(Figure 5.7.1.3)

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 5.7.1.4, 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 5.7.1.4.



(Figure 5.7.1.4)

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 VLAN, port 3 and port 4 belongs to different VLAN, figure as 5.7.1.5

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.

Port :	Port CPU	Port 1	Port 2	Port 3	Port 4	Port 5
VID:1	UnTagged	UnTagged	UnTagged	--	--	--
VID:2	--	--	--	UnTagged	--	UnTagged
VID:3	--	--	--	--	UnTagged	UnTagged
VID:4	--	--	--	UnTagged	UnTagged	UnTagged

(Figure 5.7.1.5)

:

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

5.7.2 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

Current Location>>Main Menu>>L2 Feature>>Multicast Configuration>>Dynamic Multicast

IGMP Snooping : Enable Disable

IGMP Query : Enable Disable

IGMP Query Interval : 125 S (Range : 60~1000)

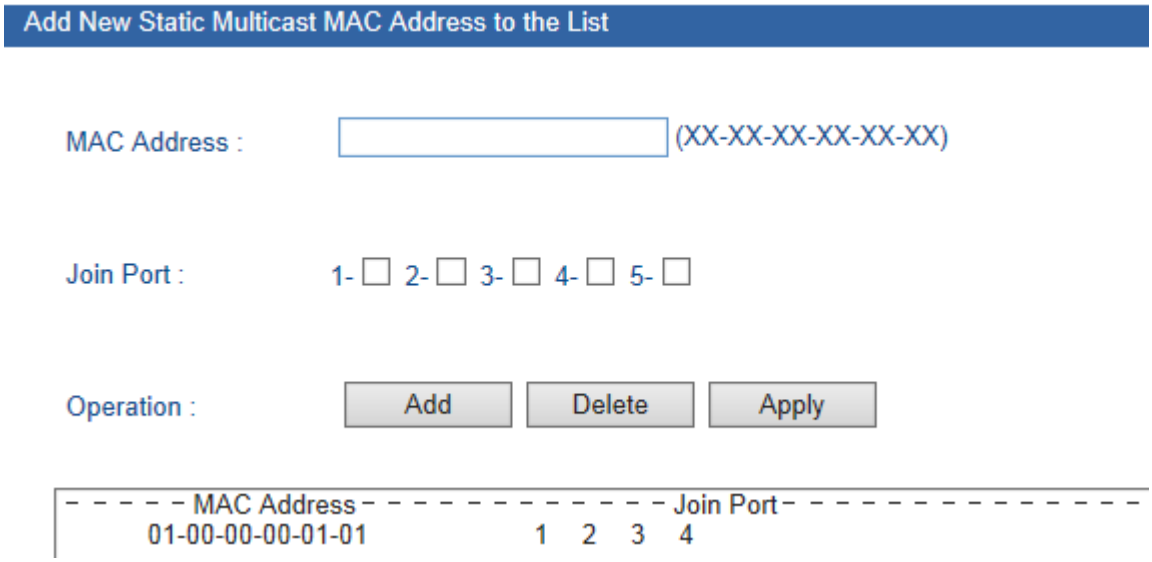
No	MAC Address	Type	Join Port
1	01-00-5E-00-00-FC	Dynamic	4

(Figure 5.7.2.1)

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.

5.7.3 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 6.5.7)

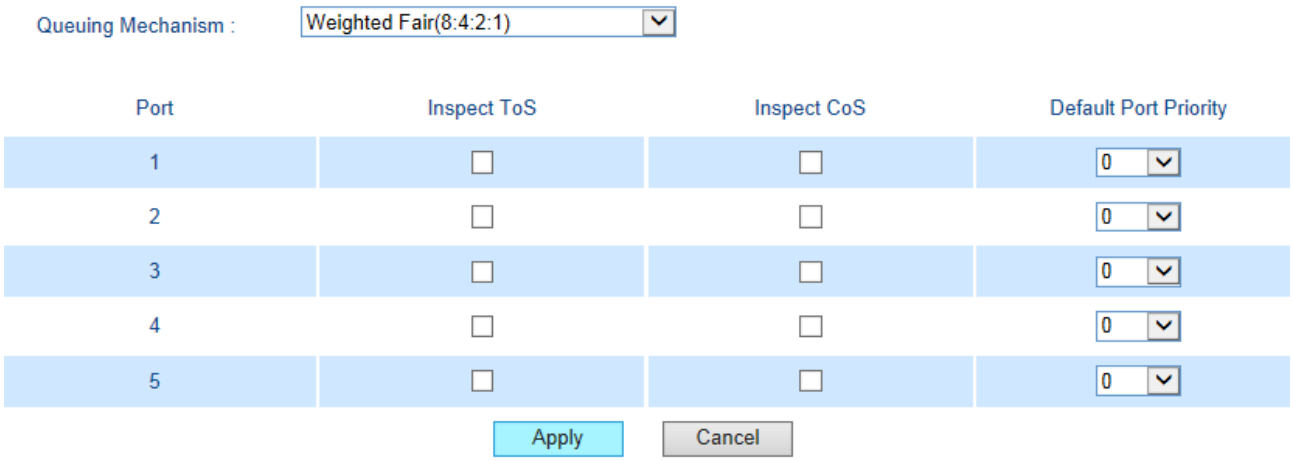
Button [Add/Edit], [Delete] were used for add/delete static Multicast MAC address. Join port is used to choice the transmit port of static MAC address, can point to 1 or more transmit port. Knock[Add], [Delete], static MAC address will be updated. For example, add MAC address “01-00-00-00-01-01” member 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.

5.8 QOS

5.8.1 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 802.1p priority tags and IP TOS, equipment can be able to put the packets to an appropriate level.



(Figure 5.8.1.1)

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

Weighted Fair priority

Weighted Fair refers to this port sends message according to queue priority High, Medium, Normal and low in proportion of 8:4:2:1 when some ports traffic is heavy. If sending speed is less than bandwidth, the message of each priority queues can send normally; if the port keeps sending in full speed, then the rest of the message of each priority queues will be discarded.

Strict priority

Strict priority: it refers to QoS deals with the message from high priority to low priority. If the low priority queues is full but the message of high priority queues don't finish, the message of low priority queues will be discarded; but if the speed of high priority queue does not reach the port's wire speed, then message of lower priority can send one by one, and the data may be lost because of shortage of bandwidth. The ports always finish all messages of high priority queues first then allow the message of lower priority queues

Port Priority

Default priority is based on port priority, default priority is different from COS and TOS, it did not have relationship with data package, it had relationship with switch port's priority. If the port's priority is higher, the data packet will be transferred at first.

When open port priority, must open inspect COS. The example: open inspect port, 1, 2, 3, 4 COS, divide port 1, 2, 3, 4 in different priority, COS value corresponding priority no need to set up. Port 1, 2, 3, 4, port 1, the priority is the highest. When these 4 port 's receive data must transfer from other port, because the limited of bandwidth, will be transferred according to priority queue mechanism(If use strict mode, then port 1's data must be transferred over at first. If use Weighted Fair 8:4:2:1, the 4 port will be transferred according 8: 4: 2: 1 ratio)

5.8.2 COS

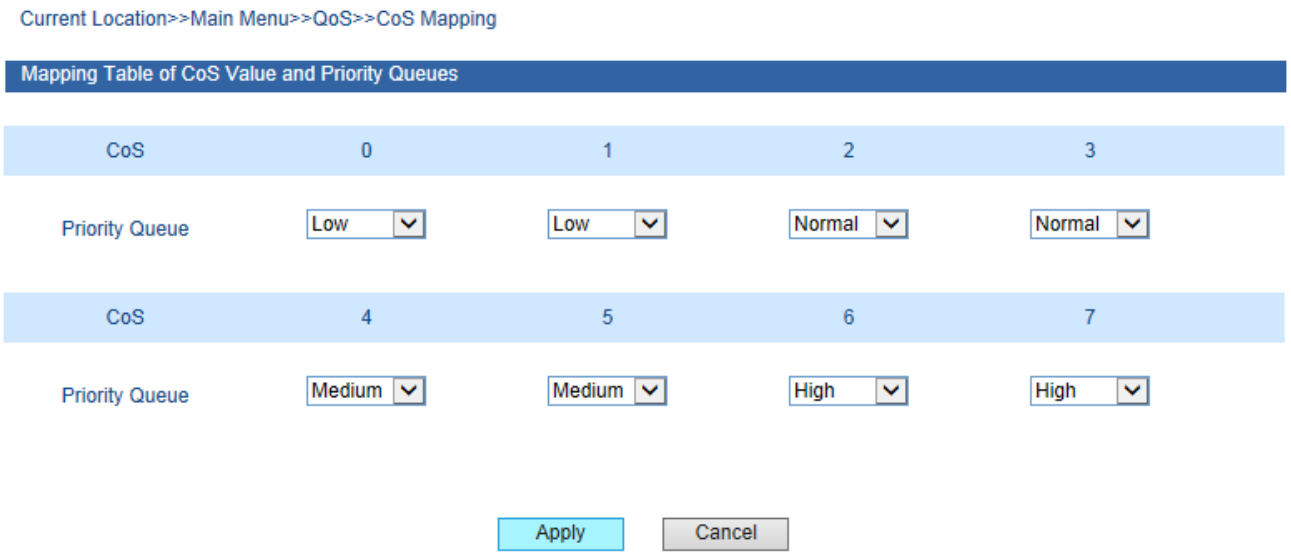
IEEE P802.1p is the name of a task group active during 1995–98 responsible for adding traffic class expediting and dynamic multicast filtering to the IEEE 802.1D standard. Essentially, they provided a mechanism for implementing Quality of Service (QoS) at the media access control (MAC) level. The group's 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 5.8.2.1)

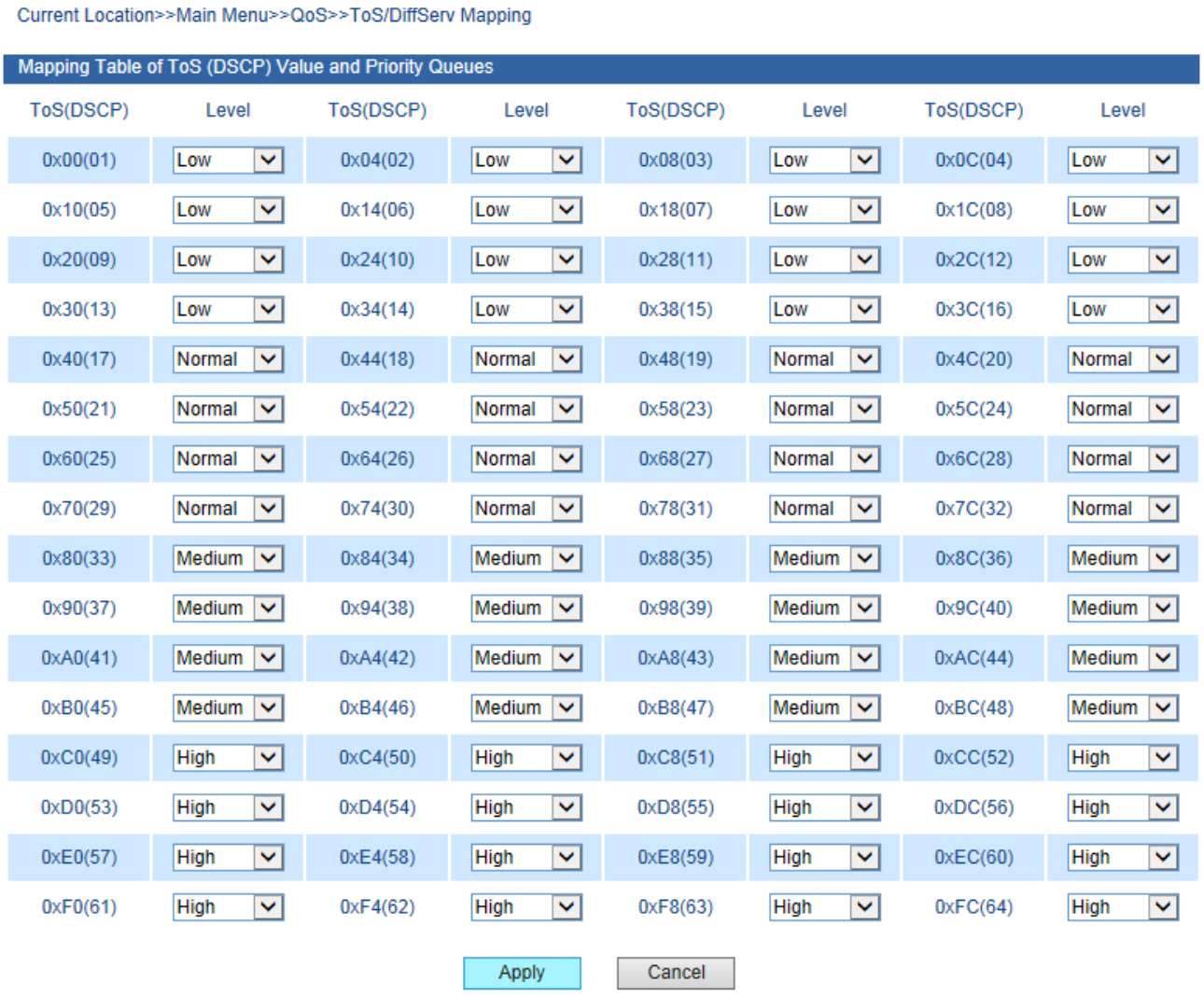
5.8.3 TOS (DSCP)

TOS/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.



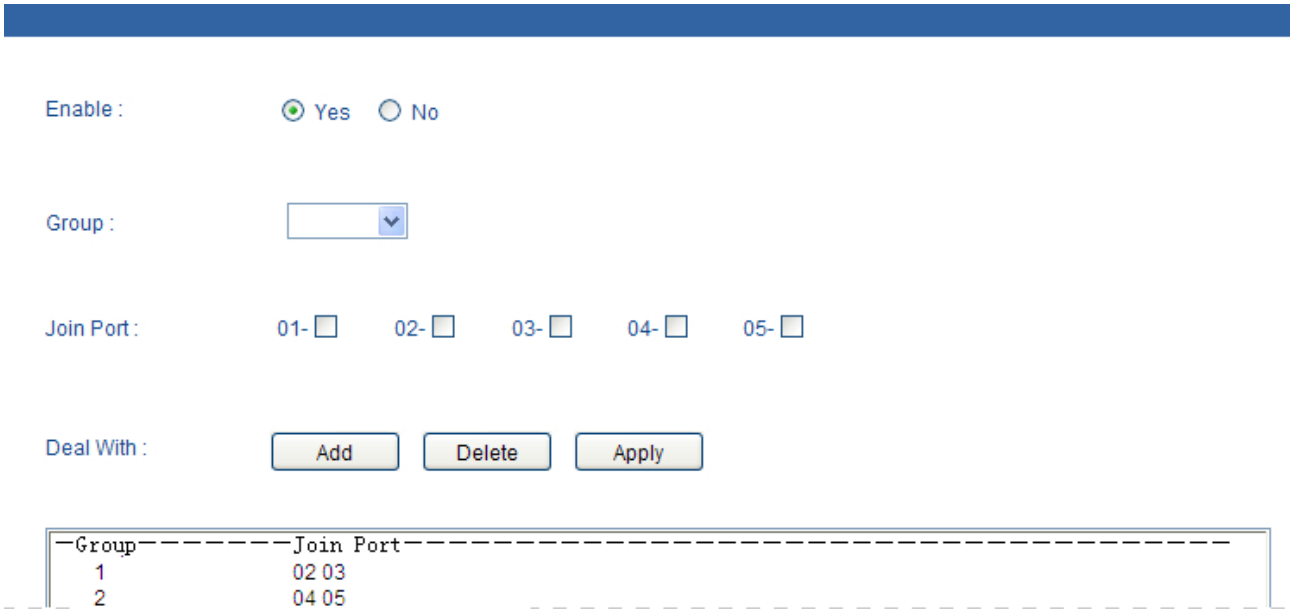
(Figure 5.8.3.1)

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 priorities can be used alone, can also be used at the same time, queuing according to the above rules.

5.9 Redundancy

5.9.1 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 5.9.1)

Devices support two Trunking groups, 2-4 ports connected to each other.

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.

5.9.2 Rapid Ring

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. Ring is the patented technology designed for industrial control network requiring high reliability.
Ring technology support maximum 250 pieces switches, in which the **Ring** its self-recovery time is <20ms.
Each port of switch can be Ring Port to connect other switches. When network is broken, relay for failure alarm will be activated. Redundant organization of **Ring** enable backup link to recover network instantly.

Self-developed patented technology for 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 5.9.2.1:

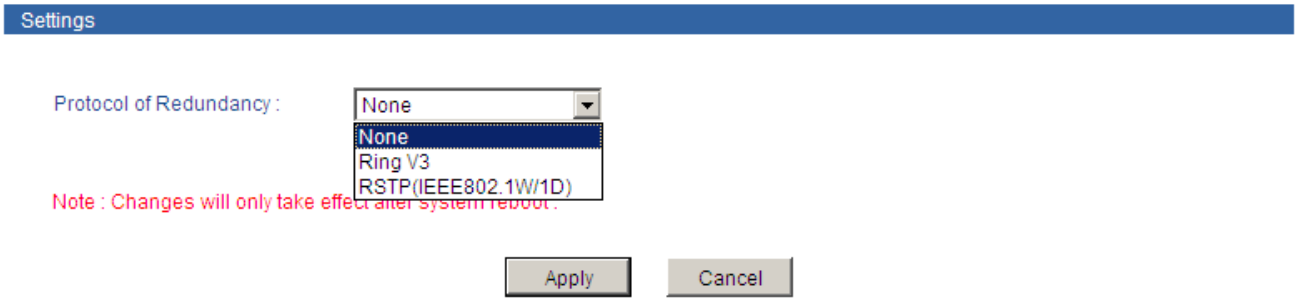


(Figure 5.9.2.1)

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

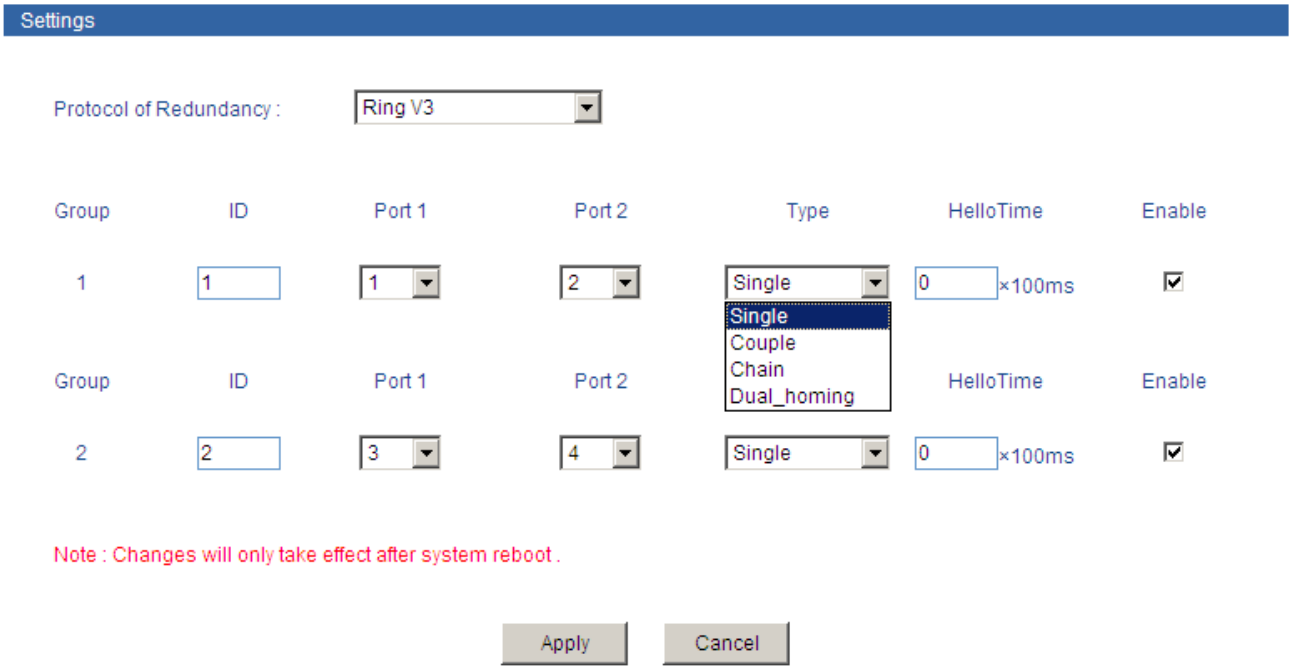
Ring V3 enable method:

1. Open Ring V3, please choice Ring V3 in [Settings], and please check the figure 5.9.2.2



(Figure 5.9.2.2)

2. After select Ring V3, Configuration interface is as figure 5.9.2.3, we can see Ring V3 support 4 different ring group: Single, Coupling, Chain and Dual_homing.



(Figure 5.9.2.3)

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.

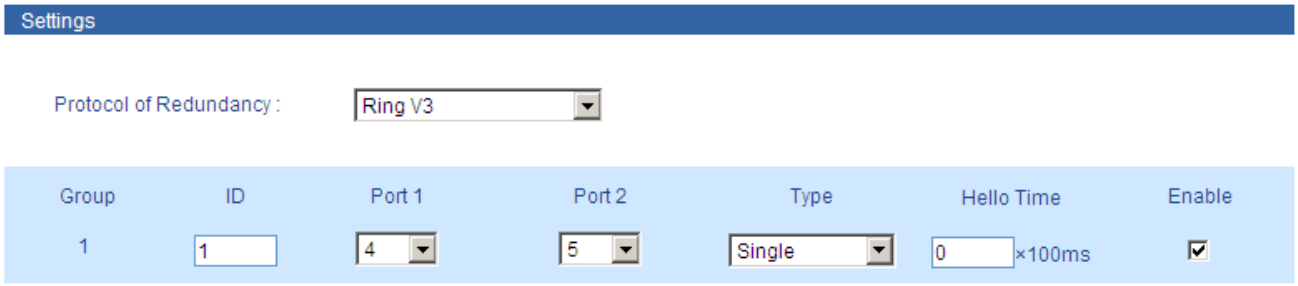
"Chain" refers to strengthen user's capability of making any type of redundant topological structure with flexibility by taking an advanced software technology. In fact, Chain is to cascade several switches already set up to Ring and both sides of chain access to network.

"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].

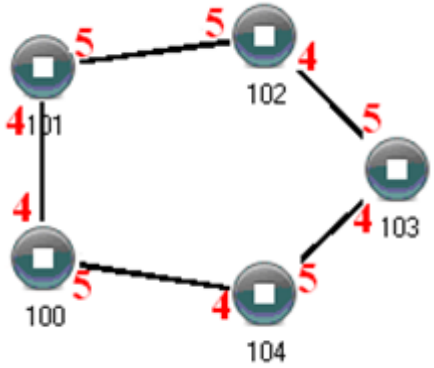
5.9.2.1 **Ring V3 single ring configuration.**

Open Ring v3, open ring group 1(or other groups), configure port 4 and port 5 are ring port, figure as 5.9.2.4.



(Figure 5.9.2.4)

Configure other switches the same as this switch, reboot these switches, then connect port 4 and port 5 through network cable, use network software search the switches, the topology of the ring network is as figure 5.9.2.5

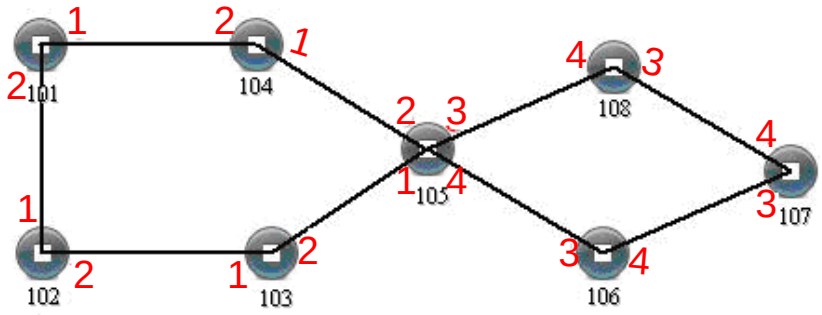


(Figure 5.9.2.5)

5.9.2.2 **Ring V3 dual ring configuration**

Figure as 5.9.2.6, we can send dual ring is 2 rings combining, the point is number 105 switch Operating method:

1. Use the configure method of singe ring to configure 101, 102, 103, 104, 105 switch's port 1 and port 2 as ring port and group is 1
2. Use the configure method of singe ring to configure 105, 106, 107, 108 switch's port 3 and port 4 as ring port and group is 2
3. Connect group 1 through network cable
4. Connect group 2 through network cable
5. Use network software search the switches, the topology of the ring network is as figure 5.9.2.6

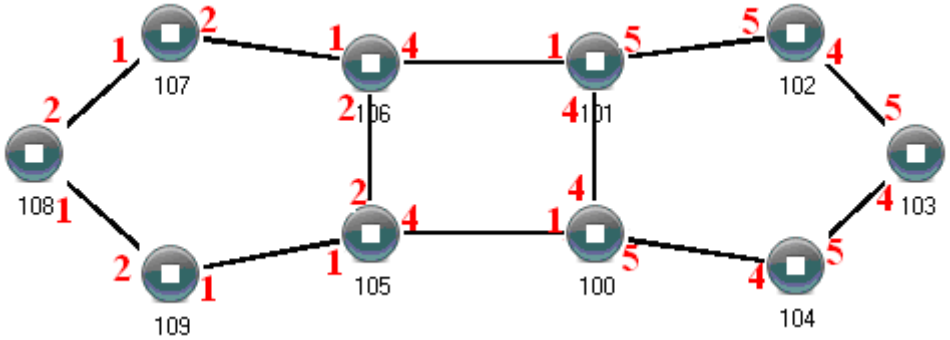


(Figure 5.9.2.6)

105 switch belong to two different ring network group, so the network mark of ring network group must different.

5.9.2.3 **Ring V3 Coupling Configuration**

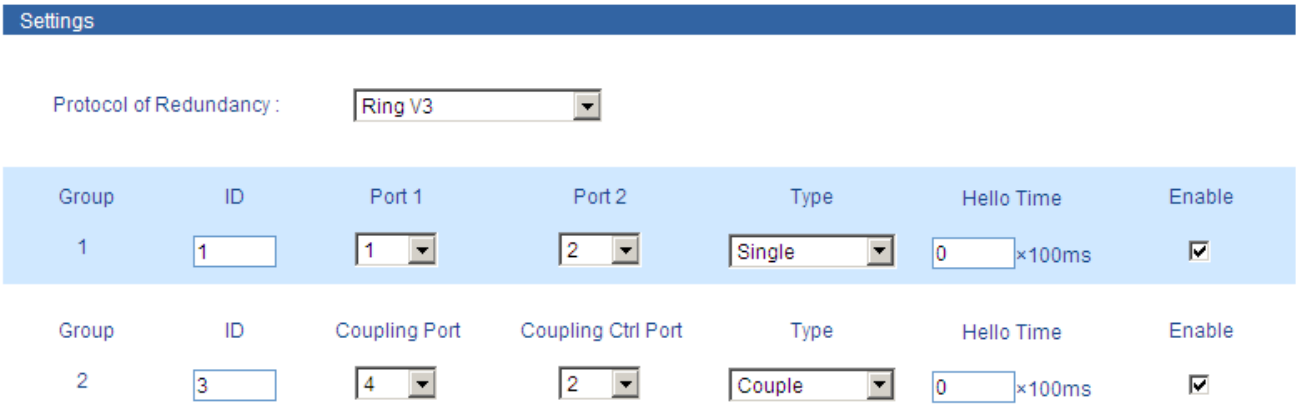
Coupling ring structure figure as 5.9.2.7:



Coupling(Figure 5.9.2.7)

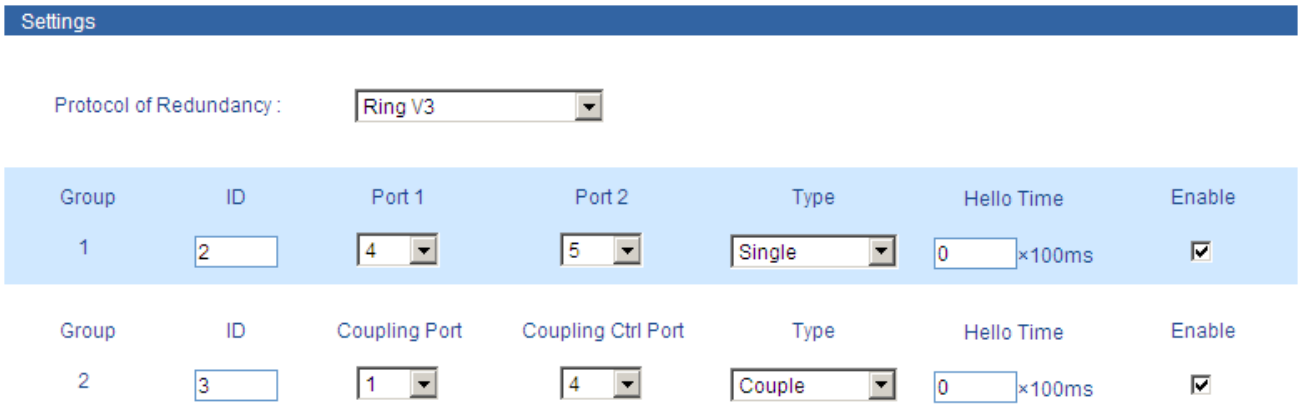
Operating method:

1. Enable Ring Group 1 and Ring Group 2; (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 1 and 2 of Device 105, 106 to be Ring Ports in Ring Group 1, Network ID is 1, Ring Type Single; Set up Port 4 of device to be Coupling Port in Ring Group 2, Coupling Control Port is 2, Network ID is 3, and Ring Type is Couple. As shown in figure 5.9.2.8:



(Figure 5.9.2.8)

3. Set up Port 4 and 5 of Device 100, 101 to be Ring Ports in Ring Group 1, Network ID is 2, Ring Type is Single; Set up Port 1 of device to be Coupling Port in Ring Group 2 , Coupling Control Port is Port 4, Network ID is 3, Ring type is Couple, as shown in figure 5.9.2.9.



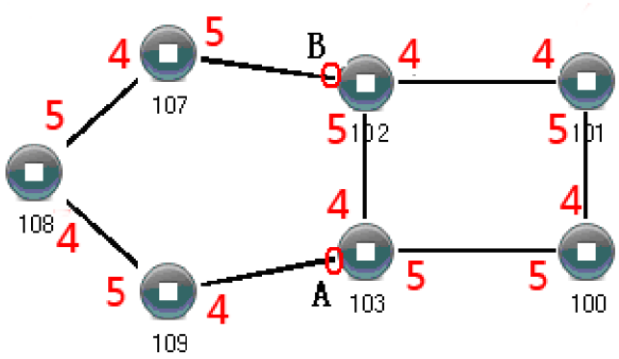
(Figure 5.9.2.9)

4. Set up Port 1 and 2 of Device 107, 108, 109 to be Ring Ports in Ring Group 1, Network ID is 1, Ring Type is Single; Set up Port 4 and 5 of Device 102, 103, 104 to be Ring Port in Ring Group 1, Network ID is 2, Ring Type is Single.
5. Use a wire to connect Port 4 and 5 of Device 100-104 in turn to make a Single Ring. Use a wire to connect Port 1 and 2 of Device 105-109 in turn to make a Single Ring. Then use a wire to connect Port 4 of Device 106 to Port 1 of Device 101, Port 4 of Device 105 to Port 1 of Device 100. The Coupling Ring is completed.

Control port as shown above figure 6.6.8, device 105 and the device 106 connected to two ports, device 100 and device 101 is connected to two ports two, also known as the control port.

5.9.2.4 **Ring V3 Chain Configuration**

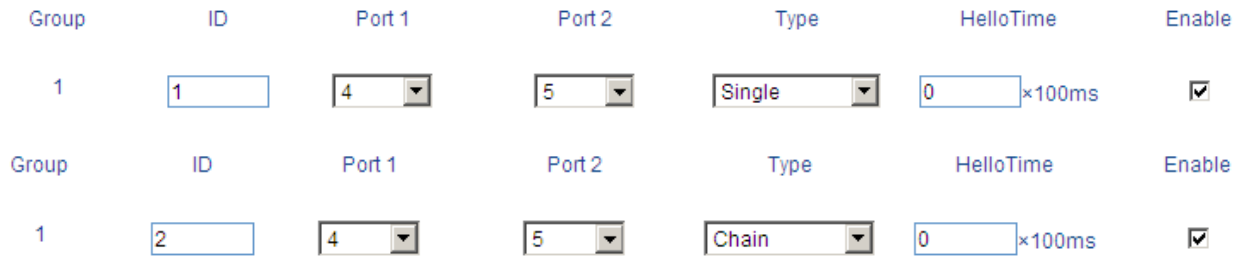
Chain ring structure figure as 5.9.2.10



Chain (Figure 5.9.2.10)

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 4 and 5 of Device 100, 101, 102 and 103 to be Ring Port in Ring Group 1, Network ID is1, Ring Type is Single. Set up Port 4 and 5 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 5.9.2.11.

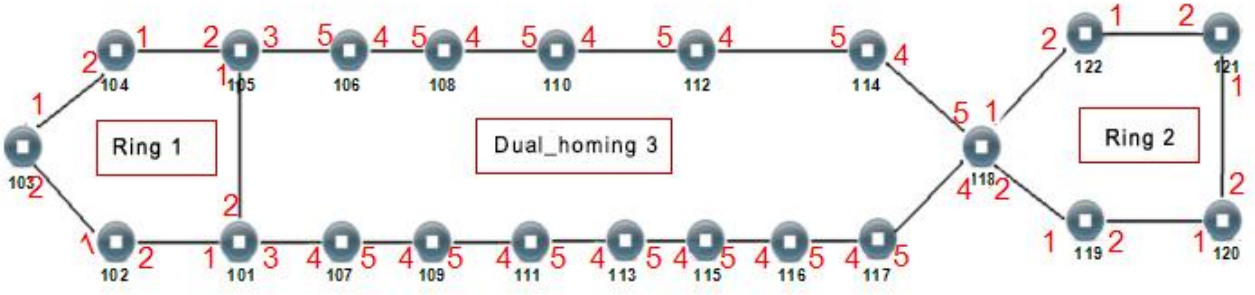


(Figure 5.9.2.11)

3. Use a wire to connect Port 4 and 5 of Device 107-109 in turn to make a chain. Use a wire to connect Port 4 and 5 of Device 100-103 in turn to make a Single Ring, Then use a wire to connect Port 5 of Device 107 and Port 4 of Device 109 to normal port of Device 102 and 103. Chain is finished.

1. Port cannot 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 cannot communicate.
3. All ring ports in the VLAN settings must be TRUNK tagged VLAN member, otherwise cannot 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.

5.9.2.5 **Ring V3 Dual_homing Configuration**

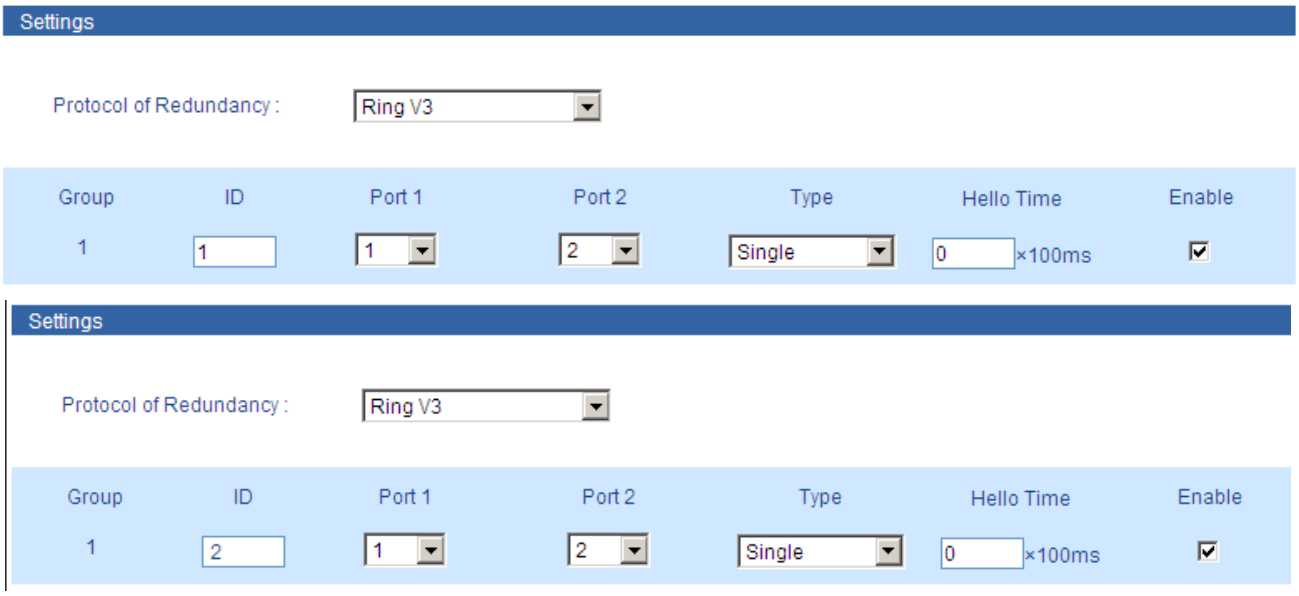


(Figure 5.9.2.12)

Operating method:

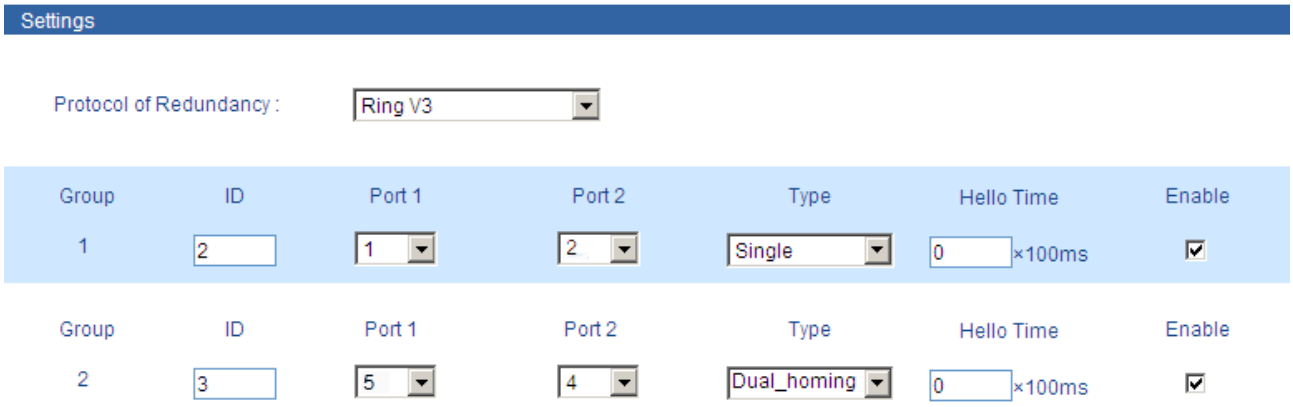
1. Enable Ring Group 1 and Ring Group 2; (Hello_time can be disable too, if it enable, time of sending Hello packet could not be very fast, or it will influence CPU dealing speed.);

2. Set up Port 1 and 2 of Device 101, 102, 103, 104,105 to be Ring Ports in Ring Group 1, Network ID is 1, Ring Type Single; Set up Port 1 and 2 of Device 119, 120, 121,122 to be Ring Ports in Ring Group 1, Network ID is 2, Ring Type Single;. As shown in figure 5.9.2.13:



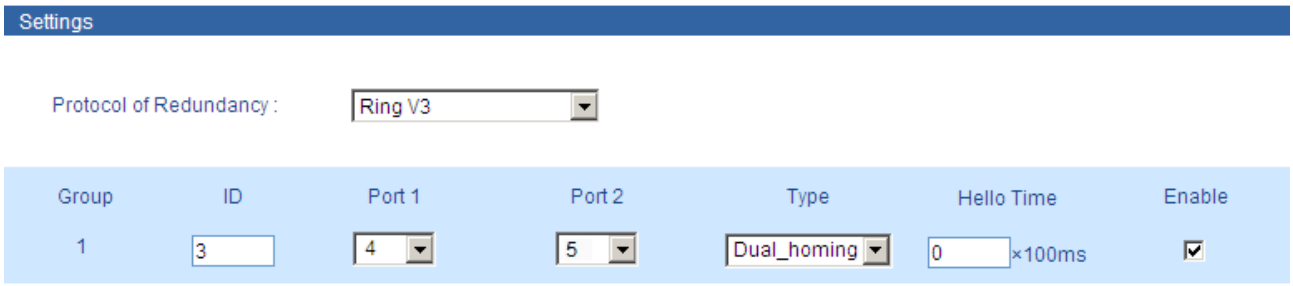
(Figure 5.9.2.13)

3. Set up Port 1 and 2 of Device 118 to be Ring Ports in Ring Group 1, Network ID is 2, Ring Type is Single; Set up Port 4 and 5 of device to be Ring Port in Ring Group 2, Network ID is 3, Ring type is Dual_homing, as shown in figure 5.9.2.14.



(Figure 5.9.2.14)

4. Set up Port 4 and 5 of Device 106-117 to be Ring Ports in Ring Group 1, Network ID is 3, Ring type is Dual_homing, as shown in figure 5.9.2.15.



(Figure 5.9.2.15)

5. Use a wire to connect Port 1 and 2 of Device 101-105 in turn to make a Single Ring. Use a wire to connect Port 1 and 2 of Device 118-122 in turn to make a Single Ring. Use a wire to connect Port 4 and 5 of Device 106-118 in turn to make a dual_homing. Then use a wire to connect Port 5 of Device 104 to Port 3 of Device 105, Port 4 of Device 107 to Port 3 of Device 101. The dual_homing is completed.

5.9.3 Rapid Spanning Tree Protocol (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.

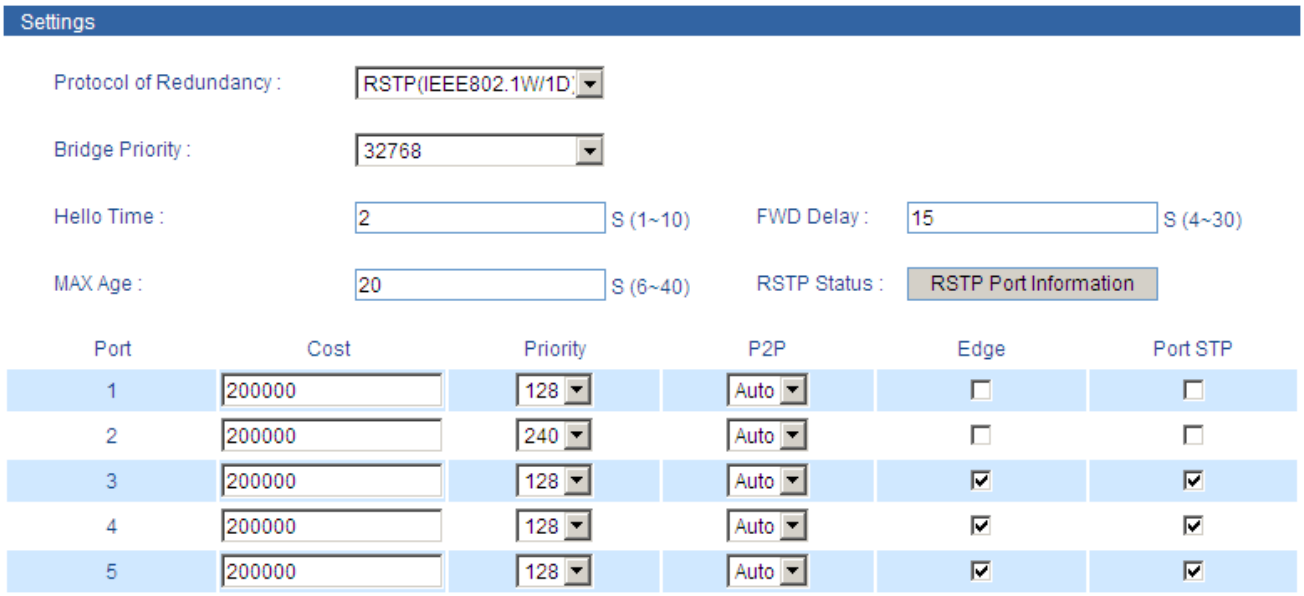
Although the purpose of a standard is to promote interworking of equipment from different vendors, different implementations of a standard are not guaranteed to work, due for example to differences in default timer settings. The IEEE encourages vendors to provide a "Protocol Implementation Conformance 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:

Enter into RSTP interface, figure as 5.9.3.1, the priority of this switch is 32768, port 1 participated in STP and priority is 128, port 2 participated in STP and priority is 240, other ports did not participated in STP and connect to the terminal directly.



(Figure 5.9.3.1)

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

5.10 Access Profile

5.10.1 Login Settings

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

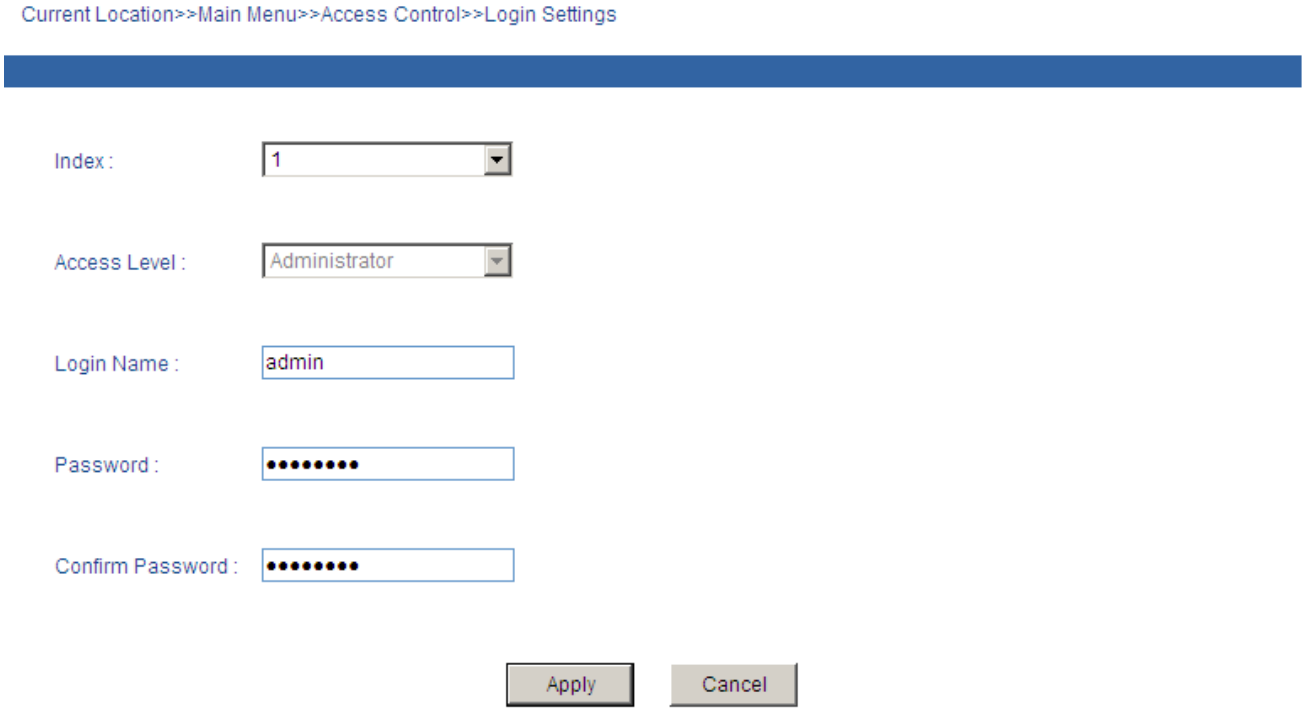
The identity of visitor with the letter combination is no more than 16 bytes

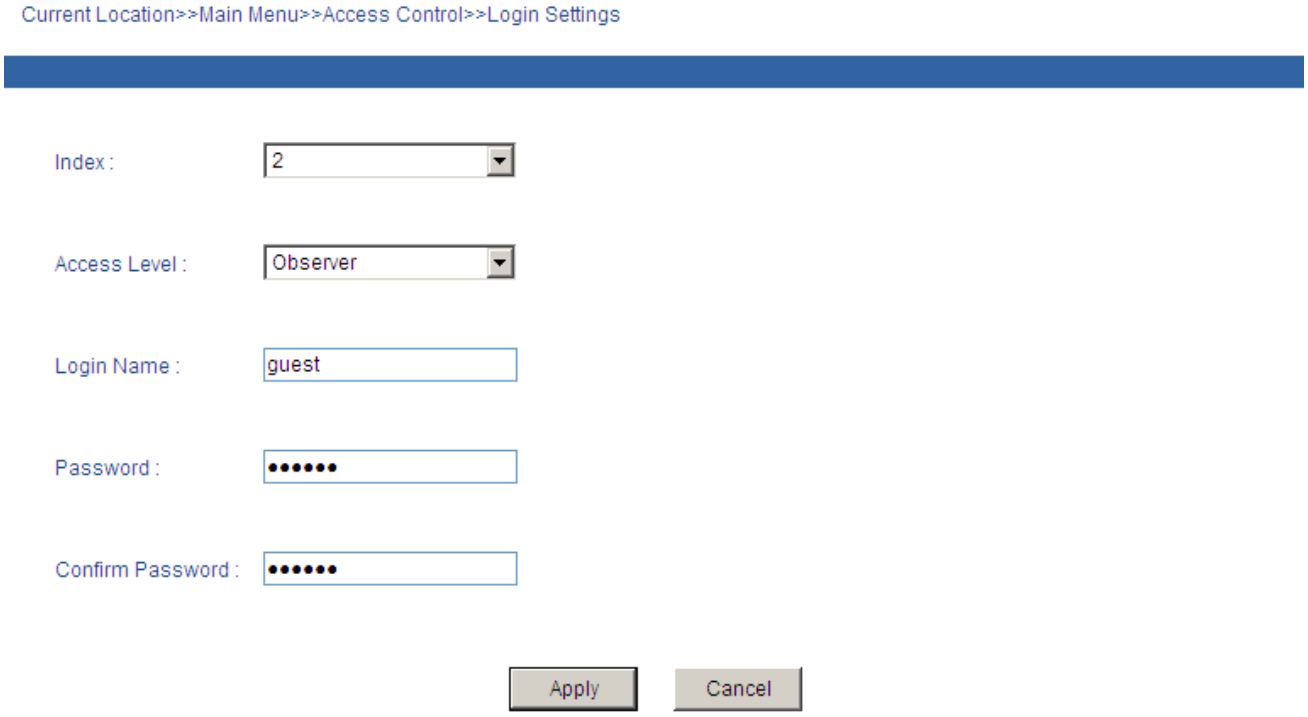
Password:

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 5.10.1)

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.

5.11 Remote monitoring

5.11.1 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.

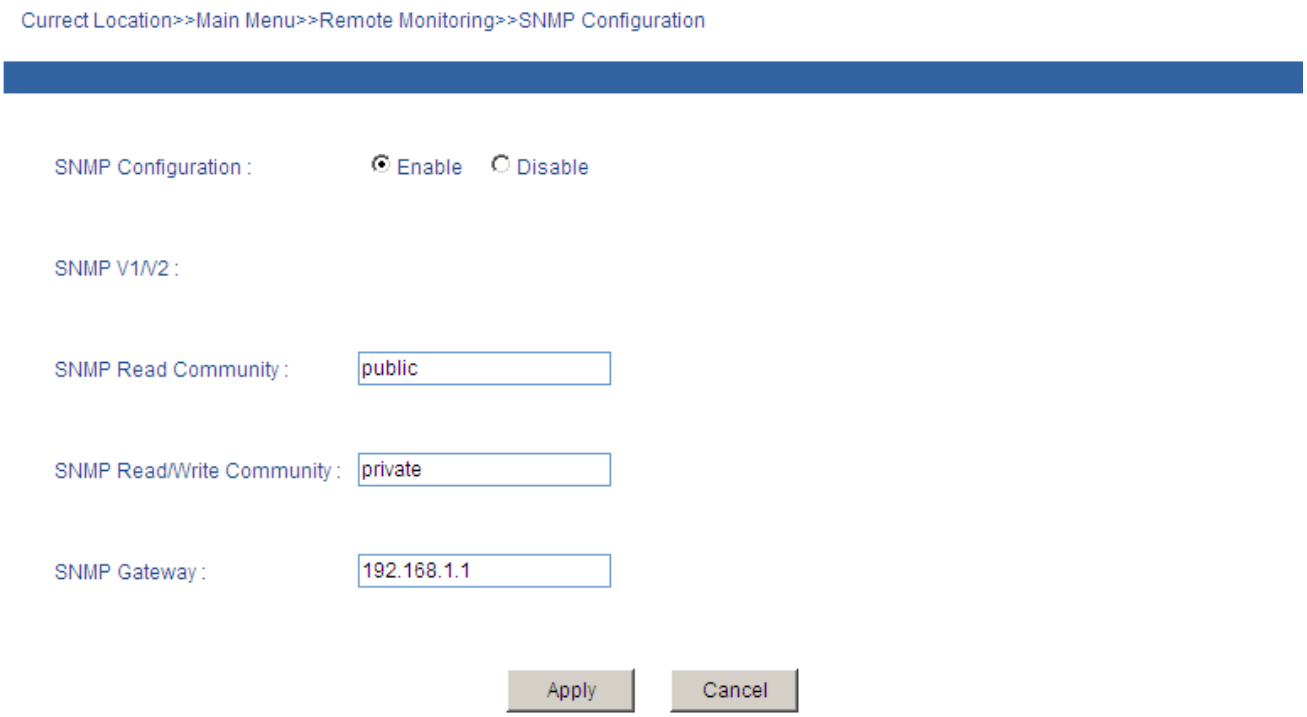
SNMP usually uses UDP Port 161(SNMP) and 162 (SNMP-traps) based on TCP/IP protocol. SNMP protocol agent is existed in network device. MIB (information specific to the device) is uses as device connector. These network devices can be monitored or controlled through the agent. When trap event happens, 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 5.11.1)

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.

5.11.2 Relay Alarm

Warning had 2 type: Power alarm, 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

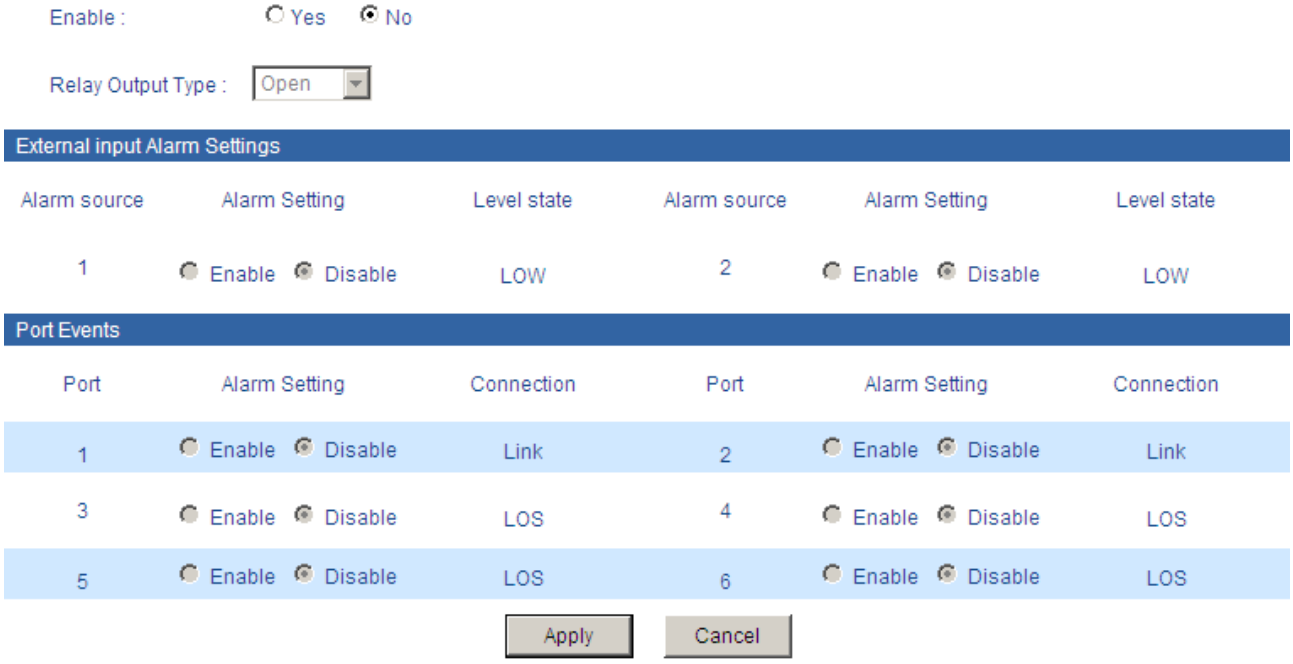
Relay warning input type: Close/Open. Once select Close, the light will be bright when have alarm. Relay will be in open status.

Power alarm

The switch provided dual DC power supply (AC power supply did not have alarm), if one power supply had problem, another will support power supply immediately, dual power supply hot back-up. Select to enable power alarm, if power supply was in unusual status, device will send alarm signal, inform power supply work unusual.

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.



(Figure 5.11.2)

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

5.12 Traffic 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

Current Location>>Main Menu>>Port Statistics>>Frame Statistics

Rx Frame Statistics

Item / Port	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8	Port G1	Port G2
InGoodOctets	174384	3145968	0	0	0	0	0	0	0	0
InBadOctets	0	0	0	0	0	0	0	0	0	0
InUnicast	1459	1208	0	0	0	0	0	0	0	0
InBroadCasts	56	4330	0	0	0	0	0	0	0	0
InMulticasts	8	9896	0	0	0	0	0	0	0	0
InPause	0	0	0	0	0	0	0	0	0	0
InUndersize	0	0	0	0	0	0	0	0	0	0
InFragments	0	0	0	0	0	0	0	0	0	0
InOversize	0	0	0	0	0	0	0	0	0	0
InJabber	0	0	0	0	0	0	0	0	0	0
IN RxErr	0	0	0	0	0	0	0	0	0	0
INFCSErr	0	0	0	0	0	0	0	0	0	0

Tx Frame Statistics

Item / Port	Port 1	Port 2	Port 3	Port 4	Port 5	Port 6	Port 7	Port 8	Port G1	Port G2
OutOctets	3728748	102281	0	0	0	0	0	0	0	0
OutUnicast	2151	845	0	0	0	0	0	0	0	0
OutBroadCasts	4330	56	0	0	0	0	0	0	0	0
OutMulticasts	9874	8	0	0	0	0	0	0	0	0
OutPause	0	0	0	0	0	0	0	0	0	0
Excessive	0	0	0	0	0	0	0	0	0	0
Collisions	0	0	0	0	0	0	0	0	0	0
Deferred	0	0	0	0	0	0	0	0	0	0
Single	0	0	0	0	0	0	0	0	0	0
Multiple	0	0	0	0	0	0	0	0	0	0
OutFCSErr	0	0	0	0	0	0	0	0	0	0
Late	0	0	0	0	0	0	0	0	0	0

(Figure 5.12.1)

5.12.1 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)
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)

5.12.2 TX frame statistics

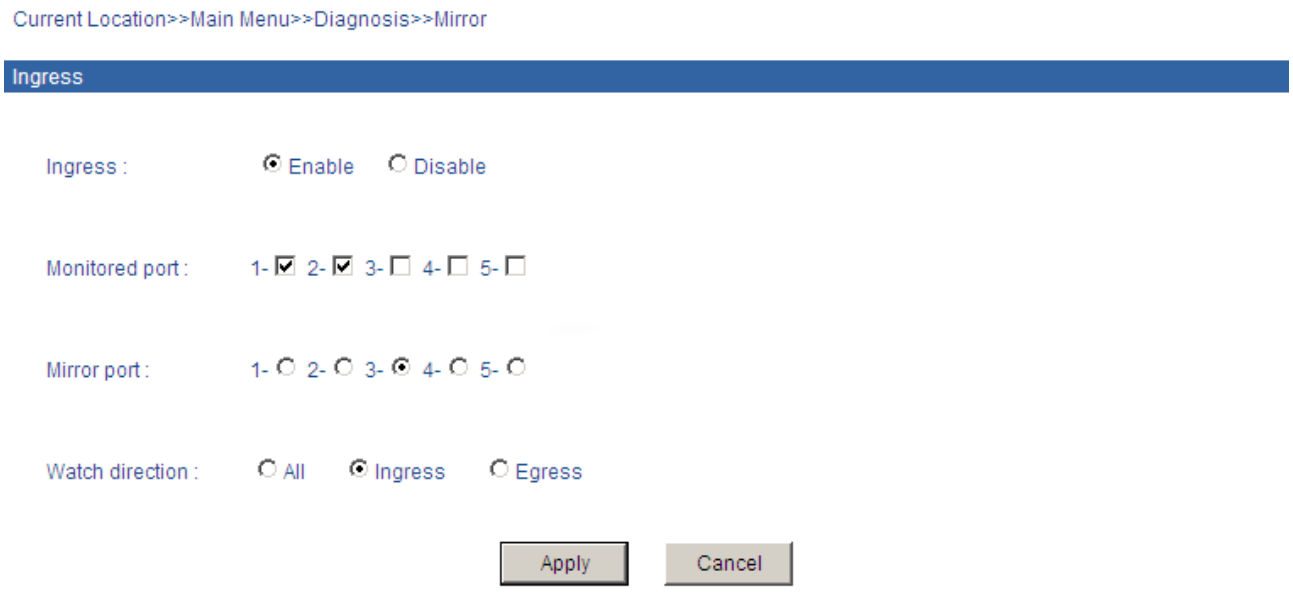
OutUnicasts	unicast data frames output
OutBroadcasts	Broadcast data frames output
OutPause	Number of output flow control pause frames
OutMulticasts	Multicast data frames output
OutFCSErr	Invalid FCS frames output
OutOctets	Number of output bytes(including FCS)
OutMaxOctets	Number of output frames between 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.)

5.13 Diagnosis

5.13.1 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 5.13.1)

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.

5.14 Basic settings

5.14.1 Device 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.

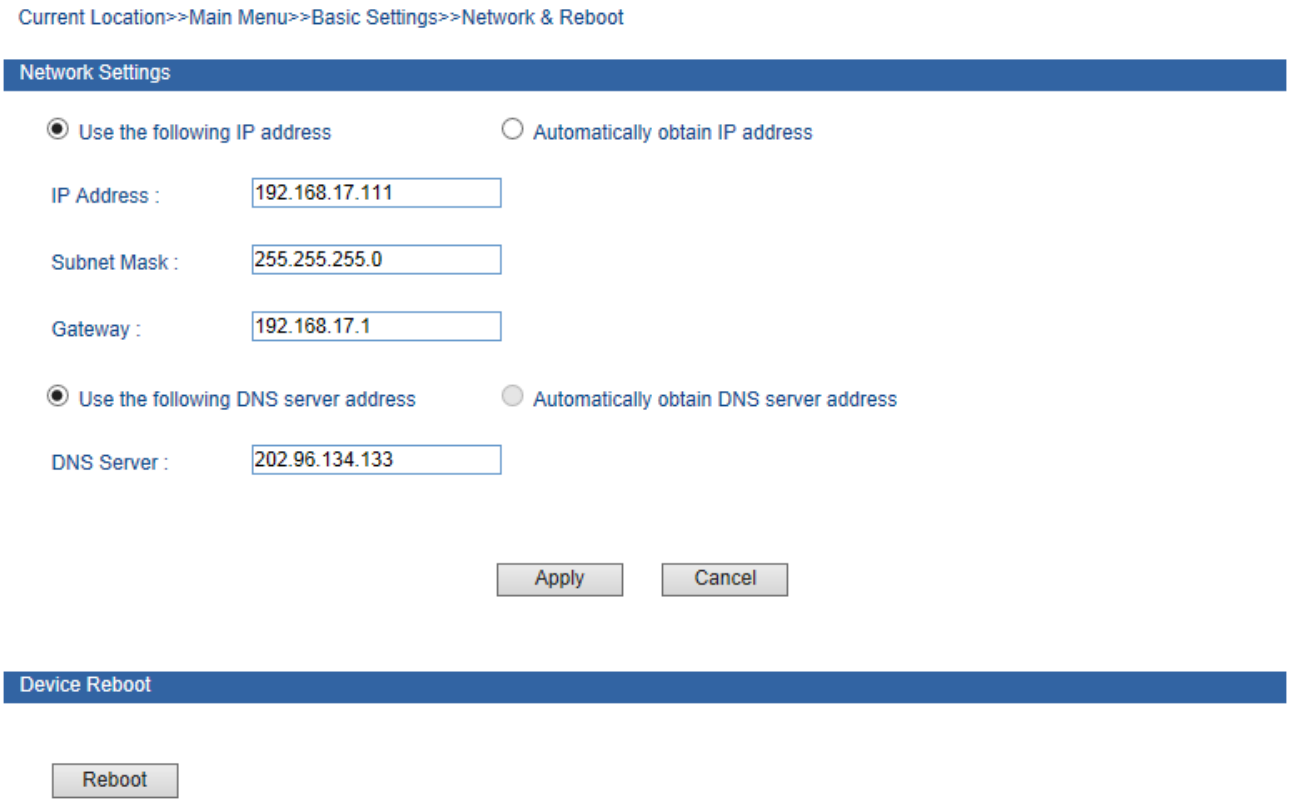
DNS Address

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 5.14.1.

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

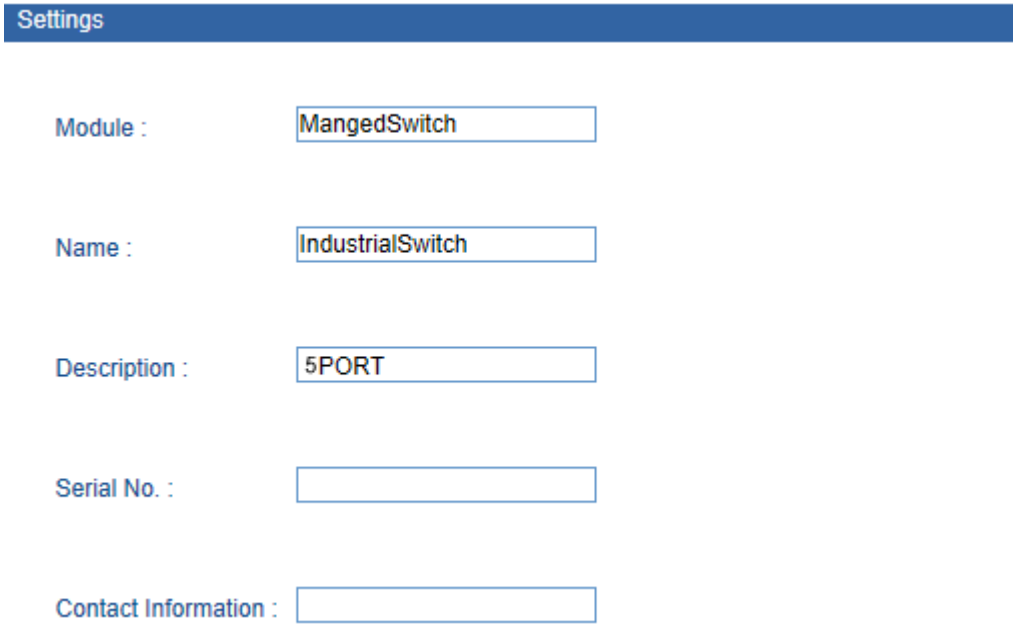


(Figure 5.14.1)

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

5.14.2 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 5.14.2 is initial device settings of the switch.



(Figure 5.14.2)

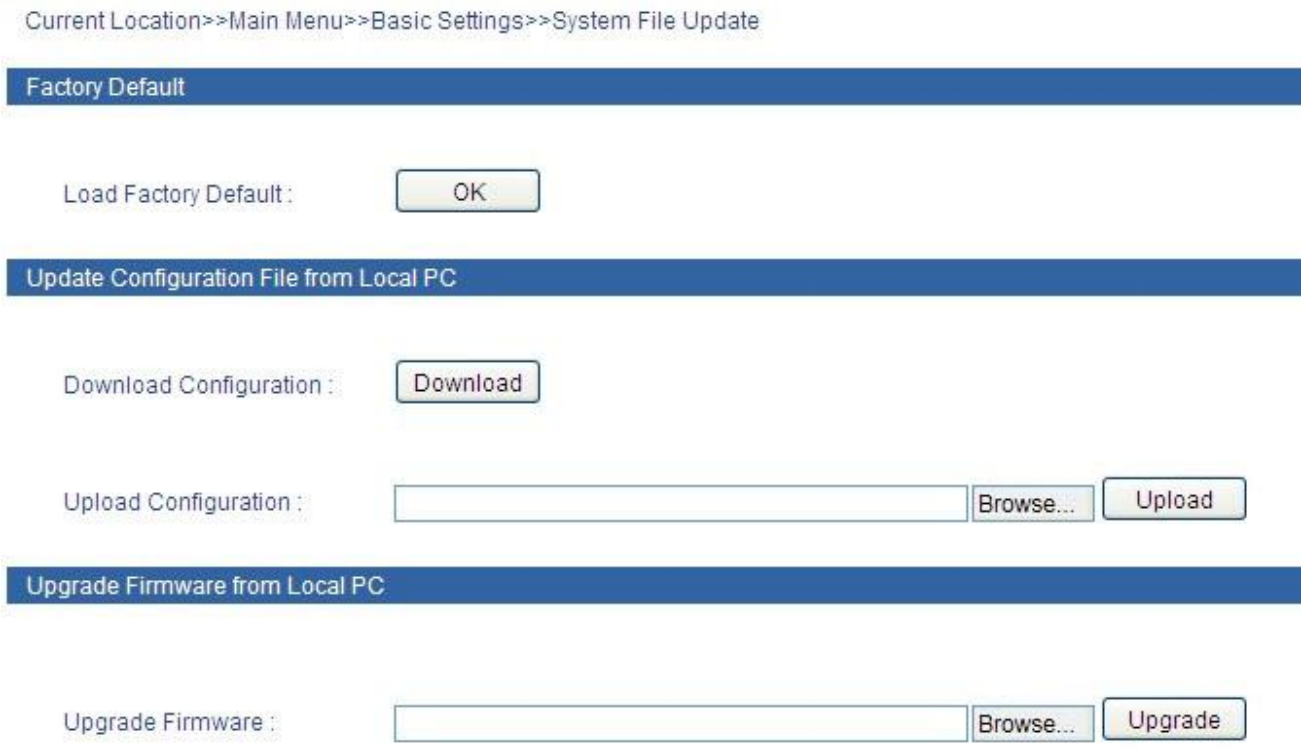
Name
To give a name to each device, length is not more than 16 bytes.

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.

5.14.3 System File Upgrade

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



(Figure 5.14.3)

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.

5.14.4 Logout

As shown in Figure 5.14.4, logout functionality for the system interfaces.



(Figure 5.14.4)

System Logout

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

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 Default factory

Main Menu	Tag	Function	Main Menu
System status	System information	Name	IndustrialSwitch
		Module	ManagedSwitch
		Desription	5PORT
		Serial No.	
		Contact information	
Port configuration	Port configuration	Port enable	Enable
		Speed mode	Consult automatic
		Flow control	enable
	Bandwidth management	Egress	No cofiguration
		Ingress	No cofiguration
Serial Server	COM Setting	Baud rate(bps)	115200
		Parity	none
		Data bits(bits)	8
		Stop bits (bits)	1
		Max frame space(bytes)	500
		Character delay(ms)	20
L2 feature	QoS	802.1p priority	Disable
		Port priority	Disable
		DSCP priority	Disable
	VLAN	802.1Q VLAN	Disable
		Based on port VLAN	Enable
	IGMP snooping		Disable
	Static Unicast		Disable
Redundancy	Port Trunking		Disable
	Rapid Ring	Ring V3	Disable
	RSTP		Disable
Port Statistics	Traffic Statistics		
Diagnosis	Mirror		Disable
Remote Monitoring	SNMP		Disable
	Relay alarm		Disable
System management	Device management	IP	192.168.1.254
		Subnet mask	255.255.255.0
		Default gateway	192.168.1.1

Appendix 3 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 BlueEyes Ⅱ. The initial user name and password is “admin”.

3. Whether the effects are equivalent that make the configuration via web and BlueEyes Ⅱ?
Configuration of both is the same, are not in conflict.

4. What kind of alarms will be informed to technical except displayed in BlueEyes II?
The computer buzzer of monitoring host will continue to make alarm sound when got alarm information.

5. How to deal the problem that some of ports cannot access?
When some of ports cannot 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.

6. 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.