3onedata®

IES5028-4GS series

Managed Industrial Ethernet switches

User manual

Version 2.0.0, Apr. 2015

www.3onedata.com

IES5028-4GS series user manual

Statement

Copyright Notice

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

Trademarks Notice

and is registered trademarks of Shenzhen 3onedata Technology 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
V1.0.3	2014-09	Manual Update
V2.0.0	2015-04	Product Update

Notes

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

Information necessary to explain

Special attention

Content

Chapter 1 Summarize

1.1 Introduction

IES5028-4GS series consists of IES5028-4GS (28 Ethernet ports + 4 Gigabit optical ports), IES5028-4GS-2F (2 Fiber ports +22 Ethernet ports+ 4 Gigabit optical ports), IES5028-4GS-4F (4 Fiber ports +20 Ethernet Ports+ 4 Gigabit optical ports), IES5028-4GS-8F (8 Fiber ports +16 Ethernet Ports+ 4 Gigabit optical ports), IES5028-4GS-12F (12 Fiber ports +12 Ethernet ports+ 4 Gigabit optical ports), IES5028-4GS-16F (16 Fiber ports +8 Ethernet ports+ 4 Gigabit optical ports), IES5028-4GS-20F (20 Fiber ports +4 Ethernet ports+ 4 Gigabit optical ports) and IES5028-4GS-24F（24 Fiber ports+ 4 Gigabit optical ports）.

IES5028-4GS series accorded to CE, FCC standard and Industry grade 4 design requirement, support 1 channel power input and 1 channel relay alarm output, and -40～75℃ working temperature, can meet all kinds of Industrial environment requirement. It can use in power, water conservancy, transportation area etc. SW-Ring^{TM} is a Rapid redundant network arithmetic designed by 3onedata. It provided recover technology for error of rapid redundant network, the recovery time<20ms.

1.2 Features

➢ 8K MAC address table

➢ Back panel bandwidth: 12.8Gbps

➢ Back pressure and flow control

➢ Support Error source address filtering, CRC parity error filtering, and MAC address conflict detection.

➢ Support MAC address learning, aging automatic

➢ Strong aluminum panel shell structure

➢ Support WEB configuration, configuration file up and download

➢ Support port statue display, data update.

➢ Support Based Tag port Tag trunking, IEEE802.3ad, 3 group trunking link

➢ Support Port based VLAN and IEEE 802.1Q VLAN

➢ Support GMRP, IGMP Snooping and static multicast filter

➢ Support RSTP, recovery time<50ms

➢ SW-Ring^{TM} redundant network patent technology, Support single ring, double ring, singe star ring, double star ring(Fault recovery time<20ms)

➢ Support flow statistic

➢ Support single port and multi-port mirroring, network detection

➢ Support rate control, Broadcast storm control, multicast storm control, unknown unicast storm control

➢ Support Password management and static address lock

➢ Support absolutely and opposite priority，support IEEE802.1P, DSCP priority

➢ Support SNMP

➢ Industrial grade 4 design, -40-75℃ work temperature

➢ Support delay alarm output, heat radiation naturally and LED indicator front and back

➢ Iron shell protection grade: IP30

➢ 1U 19inch rack mount installation

Chapter 2 Hardware Description

2.1 Panel Design

IES5028-4GS series panel design is basically the same, only the number of different optical fiber interface.

Front panel
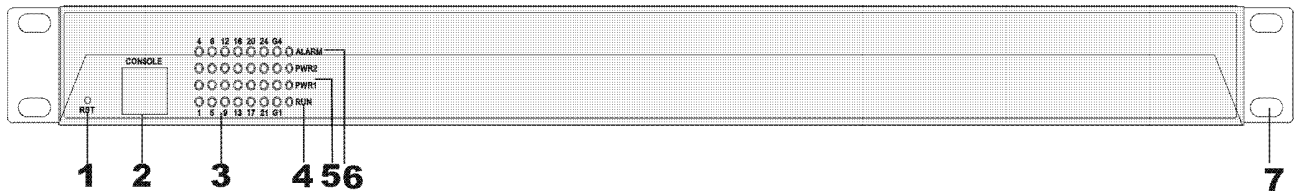
Back panel
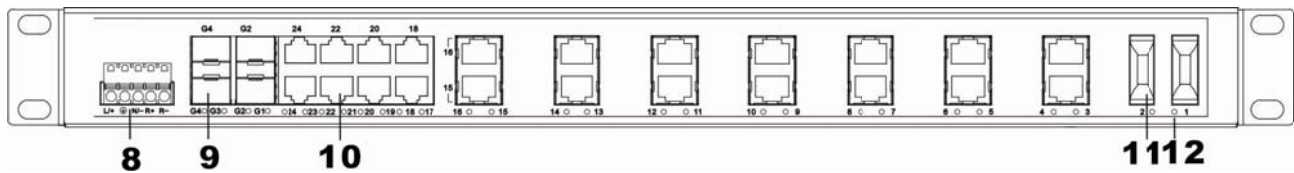
1.   Restore factory settings

2.   Console port

3.   Link/ACT LEDs

4.   Systems running LED

5.   The power LED

6.   Relay alarm LED

7.   Hangers

8.   Power input and Relay output terminal block

9.   1000Base-FX SFP port

10. 10/100BaseT(X) (RJ45) ports

11. 100BaseF(X) ports

12. Rear panel connector LEDs

2.2 Power Input

IES5028-4GS series back panel provided 3 bits terminal block, it used for AC (100-240V) power input;

L/+ ⊕ N/- R+ R-
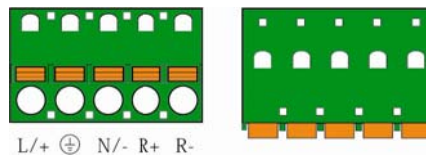
Important notice：

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

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

2.3 Relay connection

The terminal block of relay located in the front panel of the device, R+ and R- is the part of relay output. When in no alarm statues, it is in open statue, when have any alarm information, it is in close statue. IES5028-4GS series support 1 channel relay alarm output, can connect alarm lamp or alarm buzzer or other Digital Signal Input/output acquisition device, easy to remind operator when have alarm.

L/+ ⊕ N/- R+ R-
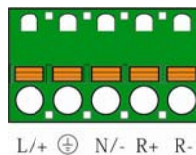
2.4 Console port

IES5028-4GS series provided 1 console port based on procedure of serial port. It adopts RJ45 interface, in front panel, can upgrade program with DB9 to RJ45 cable.
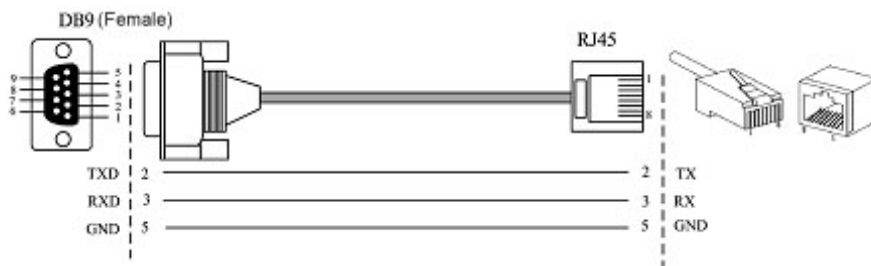
2.5 Communication port

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 120Ω of UTP 5; 10Mbps Ethernet connector takes 120Ω of UTP 3, 4, 5.
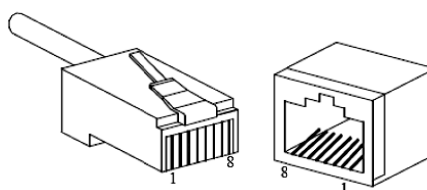
RJ 45 port supports automatically MDI/MDI-X connection. It can connect PC, Server, Converter and HUB .Corresponding connection of Pin 1,2,3,6 is like this: 1→3, 2→6, 3→1, 6→2. The definition of Pin is displayed as below.
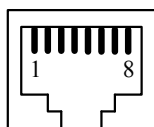
PIN	MDI	MDI-X
1	TX+	RX+
2	TX-	RX-
3	RX+	TX+
6	RX-	TX-
4, 5, 7, 8	—	—

Information necessary to explain:

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

MDI（**straight-through cable**）：


```
RJ45
8
1
TX+    3 ———————————— 3    RX+
TX-    6 ———————————— 6    RX-
RX+    1 ———————————— 1    TX+
RX-    2 ———————————— 2    TX-
```

MDI-X（**Cross over cable**）：


```
RJ45
8
1
(RX+) TX+   3 ———————————— 1    RX+ (TX+)
(RX-) TX-   6 ———————————— 2    RX- (TX-)
(TX+) RX+   1 ———————————— 3    TX+ (RX+)
(TX-) RX-   2 ———————————— 6    TX- (RX-)
```
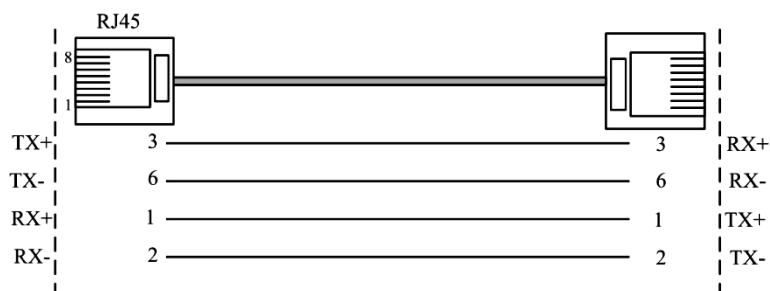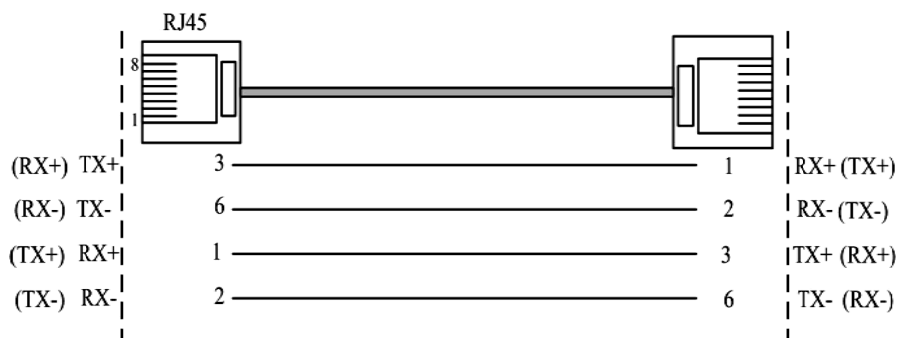
100Base-FX fiber port

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).
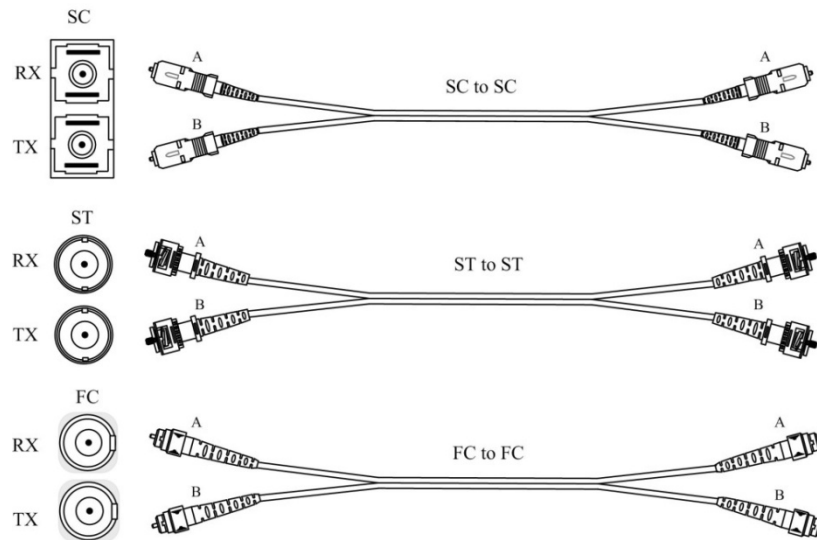
2.6 LED Indicator

IES5028-4GS series LED indictors are on the front panel. The function of each LED is described in the table as below:

System statue LED		
LED	Indicator	Description
PWR1 (Green)	ON	P1 connection regularly
	OFF	P1 Power supply have no connection or unwonted
PWR2 (Green)	ON	P2 connection regularly
	OFF	P2 Power supply have no connection or unwonted
Alarm (Green)	ON	Power, port alarm
	OFF	Power, port have no alarm
Run (Green)	OFF/ON	Device unwonted
	Blinking	Blinking 1 time/second, device working steadily
Link1~24/G1~G2 (Green)	ON	Established effective network connection
	Blinking	Network in activity statues
	OFF	Did not established effective network connection

2.7 Installation

Before installation, confirm that the work environment meet the installation require, including the power needs and abundant space, whether it is close to the connection equipment and other equipments 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. Screw, nut, tool provide by yourself.
5. Power: redundant 100-240VAC power input
6. Environment: working temperature -40～75℃
                  Relative humidity 5%～95%

Rack mount installation

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

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

Wiring Requirements

Cable laying need to meet the following requirements,

1. It is needed to check whether the type, quantity and specification of cable match the requirement before cable laying;
2. It is needed to check the cable is damaged or not, factory records and quality assurance booklet before cable laying;
3. The required cable specification, quantity, direction and laying position need to match construction requirements, and cable length depends on actual position;
4. All the cable cannot have break-down and terminal in the middle;
5. Cables should be straight in the hallways and turning;
6. Cable should be straight in the groove, and cannot beyond the groove in case of holding back the inlet and outlet holes. Cables should be banded and fixed when they are out of the groove;
7. User cable should be separated from the power lines. Cables, power lines and grounding lines cannot be overlapped and mixed when they are in the same groove road. When cable is too long, it cannot hold down other cable, but structure in the middle of alignment rack;
8. Pigtail cannot be tied and swerved as less as possible. Swerving radius cannot be too small (small swerving causes terrible loss of link). Its banding should be moderate, not too tight, and should be separated from other cables;
9. It should have corresponding simple signal at both sides of the cable for maintaining.

Chapter 3 Appearance and Dimension

3.1 Appearance

IES5028-4GS-P (100/240VAC)

IES5028-4GS-2F-P (100/240VAC)

IES5028-4GS-4F-P (100/240VAC)

IES5028-4GS-8F-P (100/240VAC)

IES5028-4GS-12F-P (100/240VAC)

IES5028-4GS-16F-P (100/240VAC)

IES5028-4GS-20F-P (100/240VAC)

IES5028-4GS-24F-P (100/240VAC)

3.2 Dimension

IES5028-4GS series product dimensions length width height, between product series port number is different.
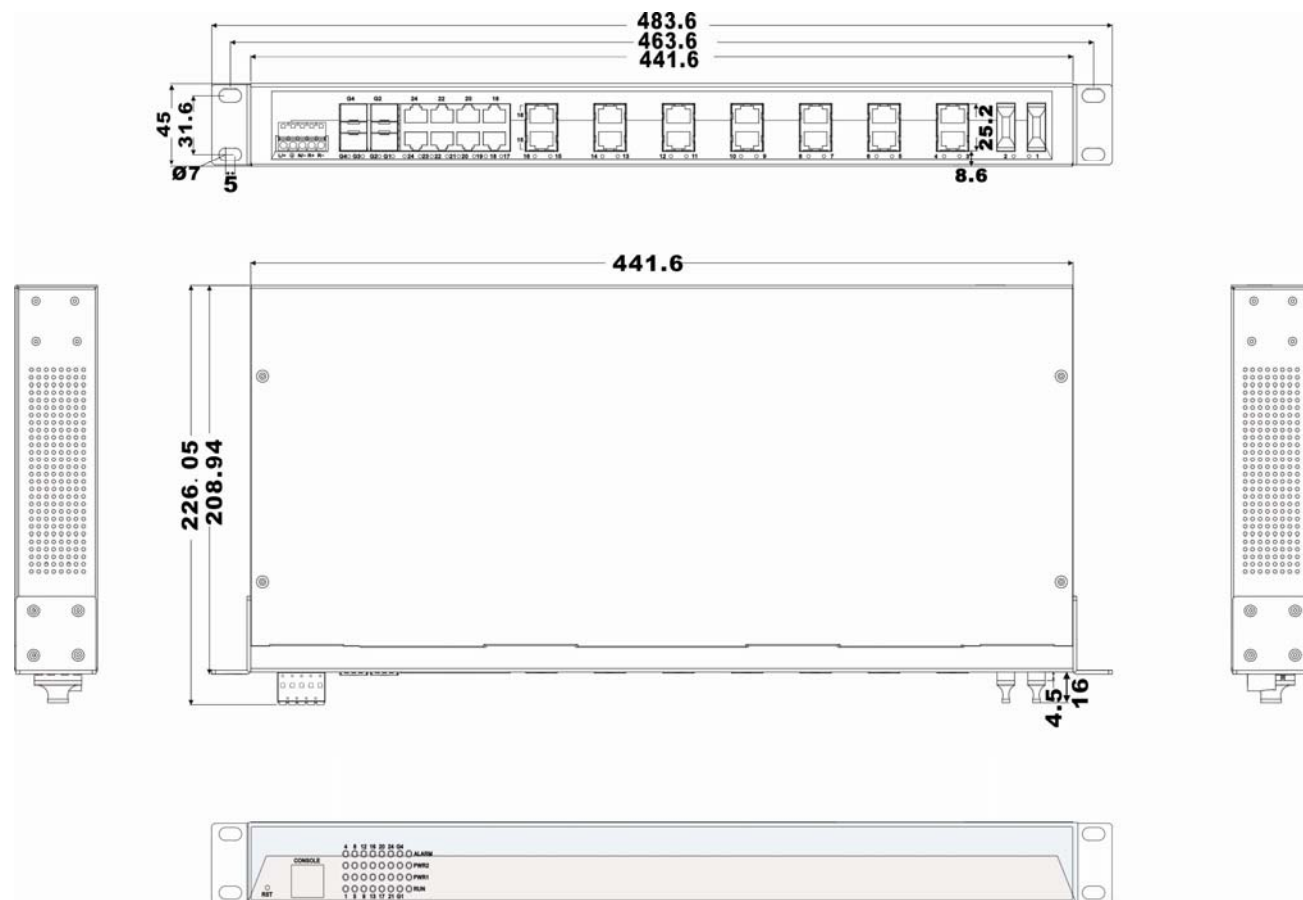
Chapter 4 Packing List

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
3onedata Industrial Ethernet switch	1
User manual	1
CD	1
Warranty card	1
Power supply cable	1
Certificate of quality	1
Hangers（optional）	1

Chapter 5 Network Configuration

IES5028-4GS series can access, configuration and management through WEB, the user manual will introduce the operations step by step.

5.1 Configure PC's IP Address

IES5028-4GS series default address is: 192.168.1.254, subnet mask is: 255.255.255.0. When entering into IES5028-4GS series Web interface through internet explorer, the IP address of IES5028-4GS series and PC must be in the same Local Area Network.

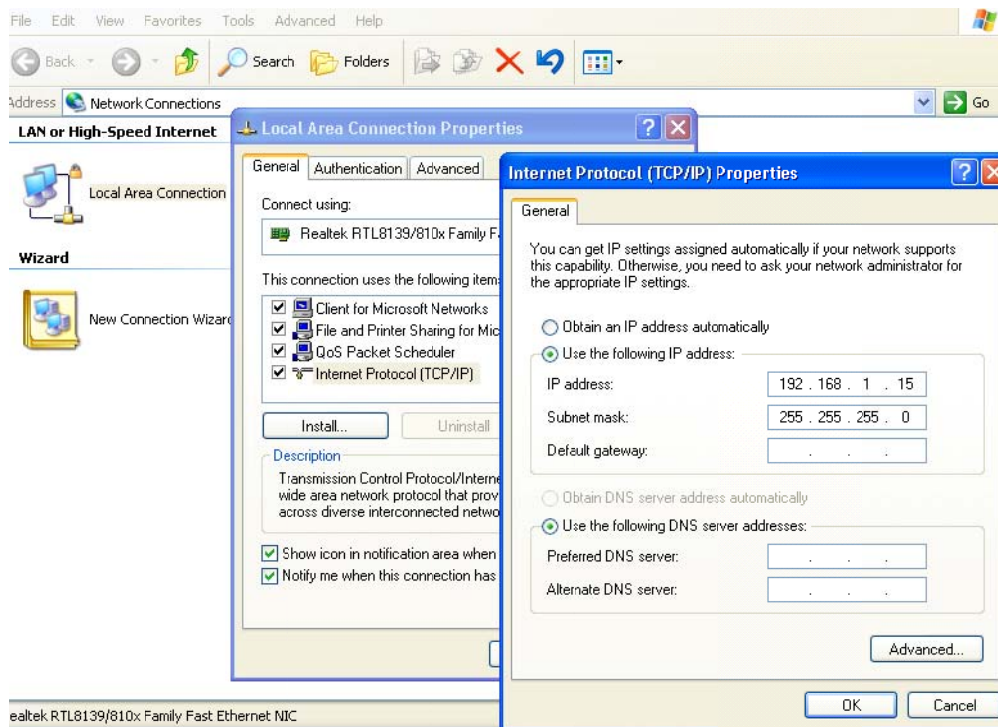You can modify PC's or IES5028-4GS series' IP address to make sure that they are in the same Local Area Network. Operating process can follow method 1 or method 2 as below,

Method 1: Modify PC's IP address

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

➢ Click "OK", IP address modifies successfully

Method 2: Modify IES5028-4GS series' 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.

Chapter 6 WEB Management

IES5028-4GS series have WEB server inside, can manage and maintenance the device very intuitive through WEB interface

6.1 Configurate preparing

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

◆ Install operating system (Windows XP/2000,etc)

◆ Install Ethernet card

◆ Install Web explorer (IE6.0 or higher version)

◆ Install and start TCP/IP protocol

2. The default management IP address of IES5028-4GS series: 192.168.1.254, subnet mask as: 255.255.255.0. Before access to the configuration interface, the computer's IP address and the switch must be configured in the same subnet (IP address configuration, please refer to "5.1") if need local configuration; Computers and switches must be routed reach if for remote configuration.

How to log on to Web Server

Please type in the default IP of switch on the browsers's address bar, and then will pop-up a window by clicking the "enter" key which shows you have to enter your user name and password. The default username and password is "admin". You can enter your username and password 3 times if you found the username and password is incorrect. If the 3 input error, the browser will display a "401 Unauthorized" error message. Refresh the page and then enter the correct user name and password, log on to the Web Server, it will recommend to modify the user name and password. Please contact our customer service center if you have more questions.
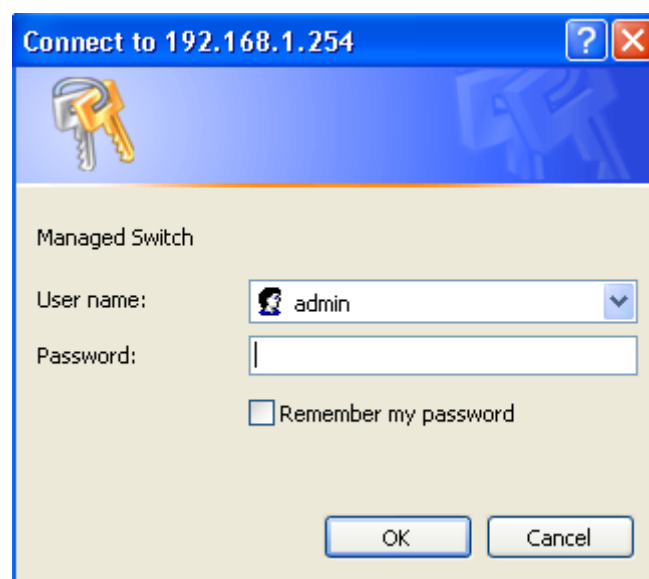
(Figure 6.1.1)

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

Menu Introduction:

Main Menu	Tag	Function
System Status	Overview	Display device information and port information such as software version, IP address, etc.
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.
	Storm Suppression	Set storm inhibition type and flow
L2 Feature	VLAN	Displays the current list of 802.1Q VLAN, configure and manage 802.1Q VLAN. Display port-based VLAN list, and to configure and manage port-based VLAN.
	Dynamic Multicast	IGMP snooping and dynamic GMRP multicast registration.
	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.
	Cos Mapping	Configure the meaning of COS value.
	Tos/Diffserv Mapping	Configure the DSCP priority. Mapping Table of ToS(DSCP) Value and Priority Queues
Redundancy	Rapid Ring	Configure the rapid ring network port and type. Include Ring V3 and RSTP.
	Port Trunking	Configure port trunking group.
Access Control	Login Settings	Configure different permissions for the user name and password.
	DHCP_Server	Set the DHCP server mode, to DHCP client IP address allocation
	Static Unicast FWD	Configure static unicast address and the corresponding port.
Remote Monitoring	SNMP Configuration	Configure the parameters of SNMP
	Email Warning	Configure the mail server, recipient and other parameters.
	Relay Warning	
Port Statistics	Rx Frame	
	Tx Frame	
	Traffic Statistics	Display amount transfer and receive packets of the port
	MAC Address Table	
Diagnosis	Mirror	Configure the mirror port and mirrored port.

Main Menu	Tag	Function
Basic Settings	SNTP	Configure the NTP, time zone and other parameters.
	Network & Reboot	Device IP, gateway, DNS and other information.
	System Identification	Setting the device name, module, description and other information.
	System File Update	Software upgrade, acquires, preserve or restore the switch configuration.
	Logout	Off switch landing

Web Timeout Treatment

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

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

6.2 System status

Device information

(Figure 6.2.1)

Configuration Items	Description
Name	Network mark of the device. It is convenient for management tools to judge.
Module	The device type.
Serial No.	Serial number of the device. It is convenient for device management.
Description	Description of the product features.
Contact Information	Contact information of the operator for device maintenance.

Configuration Items	Description
MAC address	Hardware address of the device. It is a unique address which is made up of hexadecimal number with 48 bits (6 bytes) in length.
Hardware Version	Current hardware version.
Firmware Version	Current firmware version.
Current Time	Current time of the device.

Time display

Current Time : 03-11-2015-Wed 11:16:43
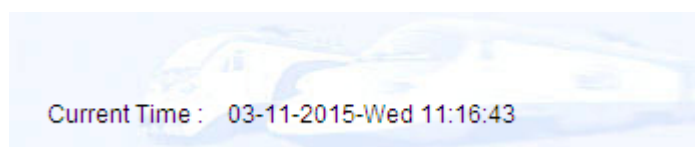
（Figure 6.2.2）

Port information

Port	Connection	Duplex	Speed	Type
1	LOS	FULL	100M	FX
2	LOS	FULL	100M	FX
3	LOS	FULL	100M	FX
4	LOS	FULL	100M	FX
5	LOS	FULL	100M	FX
6	LOS	FULL	100M	FX
7	LOS	FULL	100M	FX
8	LOS	FULL	100M	FX
9	LOS	HALF	10M	TX
10	LOS	HALF	10M	TX
11	LOS	HALF	10M	TX
12	LOS	HALF	10M	TX
13	LINK	FULL	100M	TX
14	LINK	FULL	100M	TX
15	LOS	HALF	10M	TX
16	LOS	HALF	10M	TX
17	LOS	HALF	10M	TX
18	LOS	HALF	10M	TX
19	LOS	HALF	10M	TX
20	LOS	HALF	10M	TX
21	LOS	HALF	10M	TX
22	LOS	HALF	10M	TX
23	LOS	HALF	10M	TX
24	LOS	HALF	10M	TX

（Figure 6.2.3）

Port 1, 2...24, G1, G2, G3, G4 if the port is connected properly the status should be LINK, no connection status will be LOS.

6.3 Port Configuration

6.3.1 Port Settings

The port configuration interface mainly includes 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, and duplex auto-negotiation.

Current Location>>Main Menu>>Port Configuration>>Port Settings

Port	Type	Speed	Duplex	Enable	Flow Control	MDI/MDIX
1	FX	AUTO	Full Duplex	☑	☐	AUTO
2	FX	AUTO	Full Duplex	☑	☐	AUTO
3	FX	AUTO	Full Duplex	☑	☐	AUTO
4	FX	AUTO	Full Duplex	☑	☐	AUTO
5	FX	AUTO	Full Duplex	☑	☐	AUTO
6	FX	AUTO	Full Duplex	☑	☐	AUTO
7	FX	AUTO	Full Duplex	☑	☐	AUTO
8	FX	AUTO	Full Duplex	☑	☐	AUTO
9	TX	AUTO	Full Duplex	☑	☐	AUTO
10	TX	AUTO	Full Duplex	☑	☐	AUTO
11	TX	AUTO	Full Duplex	☑	☐	AUTO
12	TX	AUTO	Full Duplex	☑	☐	AUTO
13	TX	AUTO	Full Duplex	☑	☐	AUTO

（Figure 6.3.1）

Configuration Items	Description
Port	Port name, corresponding to mark in panel.
Type	Display port type (TX or FX).
Speed	Display configurable speed of port or auto-negotiation mode.
Duplex	Auto-negotiation（AUTO）,full duplex（FULL）, half duplex（HALF）optional, default mode is auto-negotiation mode.
Enable	Configurable ports enable or disable. Selecting square frame is for enable the corresponding port. It cannot transmit data if any port disable. The default is "Enable".
Flow Control	Whether selecting flow control to the port. Only can selecting flow control when the port enable. The default is off.

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

Port Speed

Port speed shows the connecting speed of the port. It includes 3 kinds of speed: 10M, 100M and auto-negotiation. 10M uses 10base-T standard and UTP cable for connection. When the port is in 10M speed, Link/Act indicator will blink continuously while data transmitting and status indicator of 10M/100Mbps will stay OFF.

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

Port Enable

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

Duplex Mode

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

Flow Control

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

Two types of flow control:

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

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

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

Polarity (MDI/MDIX auto-negotiation)

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

MDI- II is a kind of standard built by IEEE for RJ-45 UTP cable of fast Ethernet 100BASE-T. X stands for crossover configuration.

6.3.2 Bandwidth Management

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

（Figure 6.3.2）

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

For example, the Figure 6.3.2 shows Port 1 limits the ingress speed only, the maximum speed of this port is 20M, Port 5 limits both egress and ingress speed, the maximum speed of this port is 50M

1. Please enable flow control when using port speed limitation.

2. When using speed limitation, it will not discard the packet unless the flow control disable.

3. Port speed limitation need cables with high quality, otherwise it will cause a lot of conflict packets and incomplete packets.

6.3.3 Storm Suppression

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

Storm Suppression :   ⊙ Enable   ○ Disable

Max Rate :   ○ 3%   ○ 5%   ○ 10%   ○ 20%   ⊙ 30%

Type :   ⊙ Broadcast、 Multicast and Flood

      ○ Only Broadcast

[Apply]   [Cancel]

（Figure 6.3.3）

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

If enable storm suppression, it can stop the attack. Our device can detect 2 kinds of broadcast messages according to the type of broadcast storm.

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

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

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

Maximum Speed

There are 5 levels: 3%, 5%, 10%, 20%, and 30%. The base is 100Mbps.

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

6.4 L2 Feature

6.4.1 Port-based VLAN

Port VLAN provides a solution that can divide the ports of switch into different virtual private domain. The data cannot be exchanged in the different private domain, so it's more secure to maintenance.

About port VLAN，different VLAN with different identity. Use the same ID identity will lead to internal members of the group be replaced, the new ID identity will create a new forwarding rule, all ports must belong to one or more VLAN.

1. Add Item

Group name can use any valid characteristic in port based VLAN. The same group name means you need to modify the members of the group. A new group name means the new transmission rule is built. The transmission item is not more than 32 in port based VLAN. It just changed the inside exchange rule, cannot achieve across switch.

1. Choice "VLAN Group", like as "3", means VLAN1,

2. Choice VLAN member, like as choice port 2 and port 3

3. Choice "Add/Edit"

4. Choice "Apply", then port 2 and port 3 were divided in VLAN3, they are in same VLAN, can transfer and receive data for each other.

（Figure 6.4.1）

2. Delete Item

Delete the item in the table

6.4.2 IEEE 802.1Q VLAN

Main function of IEEE 802.1Q VLAN is the VLAN tag. The tag including VLAN information can insert in the Ethernet frame. The device transmits the data according its transmission rules. VLAN tag protocol in the data frame is 2 byte; the number is 0x8100.

（Figure 6.4.2）

1. Add Item

1. File in VLAN item in 802.1Q VID (Range: 1-4094);

2. Choice port and add into VLAN table, if do not choice the port, it displayed "-" on right side, "U" means the port will be added in VLAN table and no tag of the egress frame. "T" means the port will be added in VLAN table and no need tag the egress frame

3. The default setting of the port is PVID, change the VLAN group member's port PVID the same as VID (For special application, and PVID and VID can be different)

4. Choice "Add/Edit" Button, the VLAN item will be added in VLAN table, Will be replace directly if there have same VLAN before configuration.

5. Choice "Apply"

2. Delete Item

Delete the item in the table

3. VLAN configuration：

VLAN identification replace configuration:

（Figure 6.4.3）

Manage VLAN ID：

There must have members in VLAN, can access switch regularly through VLAN group members.

For example: If configure VLAN to VLAN2, it must have members (Like as port 2 and port3), then port 2 and port 3 can access switch regularly.

（Figure 6.4.4）

Port VID：The default configuration of port VID

（Figure 6.4.5）

1. Keeping the same VID

If data did not have VLAN mark, created VLAN mark with default priority and port VID and add to data frame, priority did not change. If data have VLAN mark, the data frame did not change, priority did not change.

2. Replace identification VID with default VID

If data did not have VLAN mark, created VLAN mark with default priority and port VID and add to data frame, if data have VLAN mark, VLAN mark's VID will be replace by default port VID

For example: Set port 2 and port 3 into VLAN2, PVID is 2, port 4 and port 5 into VLAN 3, PVID is 3, Choice" Keep VID and priority", then port 2 and port 3 can communication, port 4 and port 5 can communicate, port 2 and port 3 cannot communicate with port 4 and port 5.

6.4.3 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

6.4.4 GMRP

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

GMRP software components run on both the switch and on the host. On the host, GMRP is typically used with IGMP: the host GMRP software spawns Layer 2 GMRP versions of the host's Layer 3 IGMP control packets. The switch receives both the Layer 2 GMRP and the Layer 3 IGMP traffic from the host. The switch uses the received GMRP traffic to constrain multicasts at Layer 2 in the host's VLAN. In all cases, you can use IGMP snooping to constrain multicasts at Layer 2 without the need to install or configure software on hosts.

When a host wants to join an IP multicast group, it sends an IGMP join message, which spawns a GMRP join message. Upon receipt of the GMRP join message, the switch adds the port through which the join message was received to the appropriate Multicast group. The switch propagates the GMRP join message to all other hosts in the VLAN, one of which is typically the Multicast source. When the source is multicasting to the group, the switch forwards the multicast only to the ports from which it received join messages for the group. The switch sends periodic GMRP queries. If a host wants to remain in a multicast group, it responds to the query. In this case, the switch does nothing. If a host does not want to remain in the Multicast group, it can either send a leave message or not respond to the periodic queries from the switch. If the switch receives a leave message or receives no response from the host for the duration of the leave all timer, the switch removes the host from the multicast group.

When using this function, as long as you can enable this feature, if the switch that receives the host IGMP join information, then the switch will create a multicast group IGMP join information based on the received join information, and the IGMP port is added to the multicast group, at this time if the destination address of the data for the multicast group address, then the data only from the members of the multicast group forwarded out.

（Figure6.4.6）

1. Must setting the VLAN of 802.1q at first, then open IGMP snooping.

2. Please do not open more IGMP snooping, waste source.

3. IGMP query interval must be less than the group members survival time

6.4.5 Static Multicast FWD

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 4,000 MAC addresses and 256 multicast forwarding ports list.

（Figure 6.4.7）

Button [Add/Edit], [Delete] were used for add/delete static Multicast MAC address. 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. For example, add address "01-22-6F-01-02-03" member is port 2, 3, 4, and then data frame of destination address can just send to port 02, 03, and 04.

1. This function has great impact on forwarding multicast, unless you can make sure the address is no problem, otherwise, please use it with caution.

2. The following multicast addresses are reserved for the device or protocol, please don't use them: 0180C20000xx, 01005E0000xx.

3. IGMP dynamic learning will not update the multicast address, static multicast forwarding is a kind of safety mechanism.

6.5 QOS

6.5.1 QOS Classification

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

Current Location>>Main Menu>>QoS>>QoS Classification

QoS Classification

Queuing Mechanism : Weighted Fair(8:4:2:1) ▼

Port	Inspect DSCP	Inspect Cos	Port Priority
1	☐	☐	0 ▼
2	☐	☐	0 ▼
3	☐	☐	0 ▼
4	☐	☐	0 ▼
5	☐	☐	0 ▼
6	☐	☐	0 ▼
7	☐	☐	0 ▼
8	☐	☐	0 ▼
9	☐	☐	0 ▼
10	☐	☐	0 ▼
11	☐	☐	0 ▼
12	☐	☐	0 ▼
13	☐	☐	0 ▼
14	☐	☐	0 ▼
15	☐	☐	0 ▼
16	☐	☐	0 ▼

(Figure 6.5.1)

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

6.5.1.1 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.

6.5.1.2 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

6.5.2 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 is as figure 6.5.2: 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）

Current Location>>Main Menu>>QoS>>QoS Classification

QoS Classification

Queuing Mechanism : Weighted Fair(8:4:2:1)

Port	Inspect DSCP	Inspect Cos	Port Priority
1	☐	☑	7
2	☐	☑	4
3	☐	☑	3
4	☐	☑	1
5	☐	☐	0
6	☐	☐	
7	☐	☐	
8	☐	☐	
9	☐	☐	
10	☐	☐	

（Figure 6.5.2）

6.5.3 COS

802.1P defined 8 priorities（0-7）, corresponding 4 priority (High, Medium, Normal, Low)

The default setting of 0 priority identification equipment and priority identification 1 mapped to the Low queue, priority queue is the worst. Identification of 2 priority and priority identification 3 mapped to the Normal queue, priority identification 4 and priority identification 5 mapped to the Medium queue, priority identification 6 and priority identification 7 mapped to the High queue is the highest priority queue.

Cos	0	1	2	3
Priority Queue	Low	Low	Normal	Normal

Cos	4	5	6	7
Priority Queue	Medium	Medium	High	High

Apply   Cancel

（Figure 6.5.3）

Default priority mark 0 and 1 is low queue, 2 and 3 is normal queue, 4 and 5 is Medium, 6 and 7 is High.

6.5.4 ToS/DSCP

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

So far, the defined DSCP with default DSCP, the value is 0; class selector DSCP defined as the backward-compatible with IP precedence, the value(8,16,24,32,40,48,56); Expedited Forwarding (EF), generally used for low latency service, the recommended value is 46 (101110); identified by forwarding (AF) defines four service levels, each service level has 3 down process, so spent 12 DSCP values ((10,12,14), (18,20,22), (26,28,30), (34,36,38)).

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

Current Location>>Main Menu>>QoS>>ToS/DSCP

Mapping Table of ToS(DSCP)Value and Priority Queues

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

（Figure 6.5.4）

1. Port priority is the highest level, don't need to check other QoS attributes is discharged into the highest priority queue if you set the port priority as 1.

2. DSCP priority comes second, unless we do not set DSCP, therefore will check 802.1p priority, otherwise it will line up according to the DSCP settings.

3. As above, the three priority can be used alone, can also be used at the same time, queuing according to the above rules.

6.6 Redundancy

6.6.1 Port Trunking

In telecommunications, trunking is a method for a system to provide network access to many clients by sharing a set of lines or frequencies instead of providing them individually. This is analogous to the structure of a tree with one trunk and many branches. Trunking is set by the configuration software, the two or more physical ports get together into a logical path to increase the bandwidth between the switch and the network node. Trunking is a packaging technology, it is a peer to peer link, both ends of the link are switches, it can be a switch and a router, and also can be a host, switch or router. Based on port trunking function that allows between two or more ports

between switches, switches and routers, hosts the switch or router connected in parallel to provide for the simultaneous transmission of higher bandwidth and greater throughput, significantly entire network capacity. Trunking is more economical to increase the bandwidth between the switch and network device, such as servers, routers, workstations, or other switches. Trunking function is to integrate more than one physical port (typically 2-4) to a logical channel.

（Figure 6.6.1）

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.

6.6.2 Rapid Ring

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

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

Each port of IES5028-4GS series switch can be Ring Port to connect other switches. When network is broken, relay for failure alarm will be activated. Redundant organization of **SW-Ring^{TM}** enable backup link to recover network instantly.

Self-developed patented technology for SW-Ring network can realize the intelligent redundancy for industrial

Ethernet switch, which can make you easily and conveniently establish redundant Ethernet, and can facilitate the quick recovery of any network section of automatic system disconnected from the network. IES5028-4GS series supports maximum 4 ring groups. Each group set up 2 ports as Ring Port and a port cannot belong to several rings.

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

Basic interface of Rapid Ring as shown in figure 6.6.2:

（Figure 6.6.2）

Initial interface display redundancy protocol is none, can configure it through [Settings], Ring V3 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 6.6.3

（Figure 6.6.3）

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

（Figure 6.6.4）

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

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

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

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

6.6.2.1 **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 6.6.5
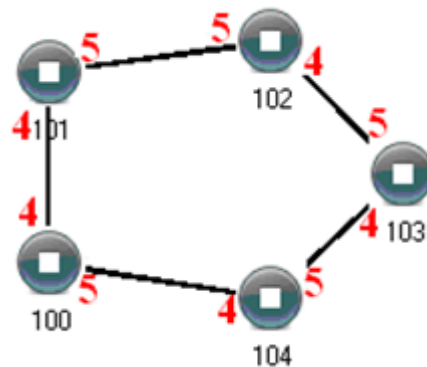

（Figure 6.6.5）

Configure other switches the same as this switch, reboot these switches, then connect port 4 and port 5 through network cable, use BlueEyes software search the switches, the topology of the ring network is as figure 6.6.6
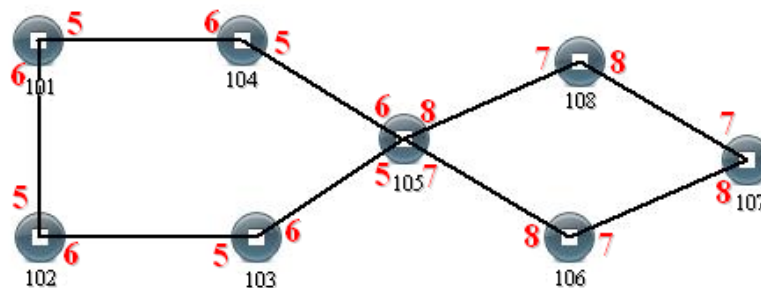

（Figure 6.6.6）

6.6.2.2 **Ring V3 dual ring configuration**

Figure as 6.6.7, 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 5 and port 6 as ring port and group is 1

2. Use the configure method of singe ring to configure 105, 106, 107, 108 switch's port 7 and port 8 as ring port and group is 2

3. Connect group 1 through network cable

4. Connect group 2 through network cable

5. Use BlueEyes software search the switches, the topology of the ring network is as figure 6.6.7
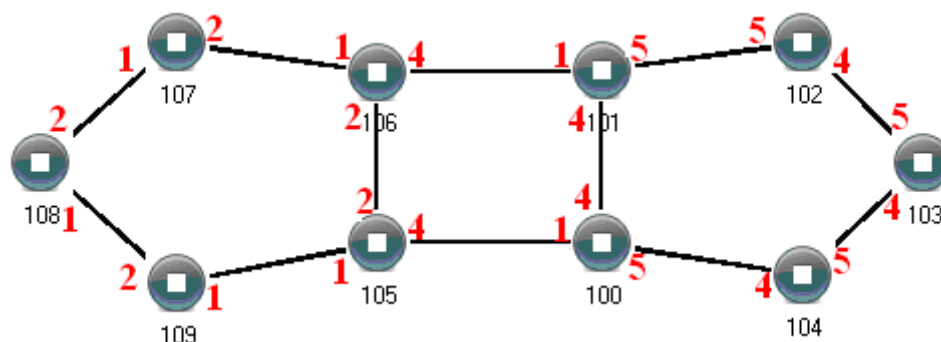

（Figure 6.6.7）

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

6.6.2.3 **Ring V3 Coupling Configuration**

Coupling ring structure figure as 6.6.8:

Coupling（Figure 6.6.8）

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 6.6.9:

（Figure 6.6.9）

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 6.6.10.
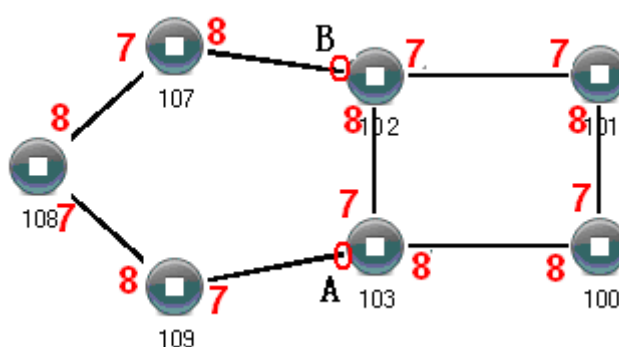

（Figure 6.6.10）

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.

6.6.2.4 **Ring V3 Chain Configuration**

Chain ring structure figure as 6.6.11

Chain（Figure 6.6.11）

Operating method:

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

2. Set up Port 7 and 8 of Device 100, 101, 102 and 103 to be Ring Port in Ring Group 1, Network ID is1, Ring Type is Single. Set up Port 7 and 8 of Device 107, 108 and 109 to be Ring Ports in Ring Group 2, Network ID is 2. Ring Type is Chain; as shown in figure 6.6.12.

（Figure 6.6.12）

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

> 1. Port 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.

6.6.3 Rapid Spanning Tree Protocol (RSTP)

Enter into RSTP interface, figure as 6.6.13，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 6.6.13）

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 remains 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

Four situation of RST：

Blocking：Can receive BPDU packets to change the listening state, if the period did not receive BPDU.

Listening：Can receive packets, after the connection to it, switches stay max age=20s in the blocking，so judge whether switch port can become root port or designated port， the port state will convert listening(the state remains 15 ms) if it works, receive and forward packets during this time to achieve the selection of root for RST ,structure and the direction of port. The decision is root port or specified port to convert learning state， otherwise to convert the blocking state.

Learning：remain forward delay(equal 15s)，continue to be calculated to determine the port can become a root port or designated port, MAC address learning function. If you decide to convert to the forwarding state.

Forwarding;（can receive and send BPDU packet）

6.7 Access control

6.7.1 Login settings

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
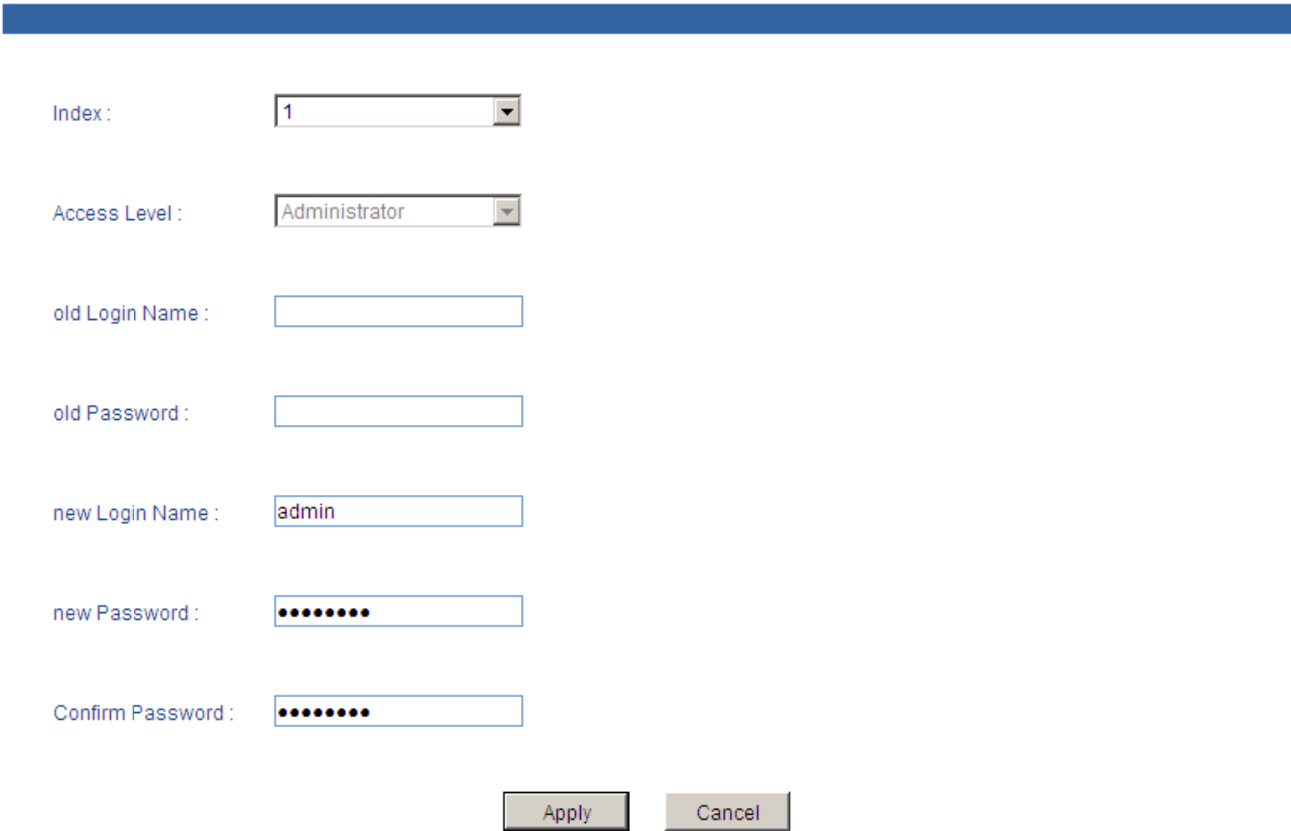
Password:

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.

Current Location>>Main Menu>>Access Control>>Login Settings

Index :   1

Access Level :   Administrator

old Login Name :

old Password :

new Login Name :   admin

new Password :   ••••••••

Confirm Password :   ••••••••

Apply   Cancel

（Figure 6.7.1）

1. Please contact our online technical support   if you forget login name and password
2. The front login name and password is available if you set same login name

6.7.2 DHCP Server

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

（Figure 6.7.2）

（Figure 6.7.3）

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

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

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

DNS address: DHCP clients to automatically obtain DNS address;

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

6.7.3 MAC port lock

Static MAC address table

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

Static MAC address list is designed to limit the movement of the computer, any computer's MAC and port binding, this computer inserts to the other port cannot communicate with another computer, over this interface can still communicate with other computers. Port security is designed to protect the port and the corresponding port

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

（Figure 6.7.6）

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

Do not use a multicast address as the input address.

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

6.8 Remote monitoring

6.8.1 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.

IES5028-4GS series 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.
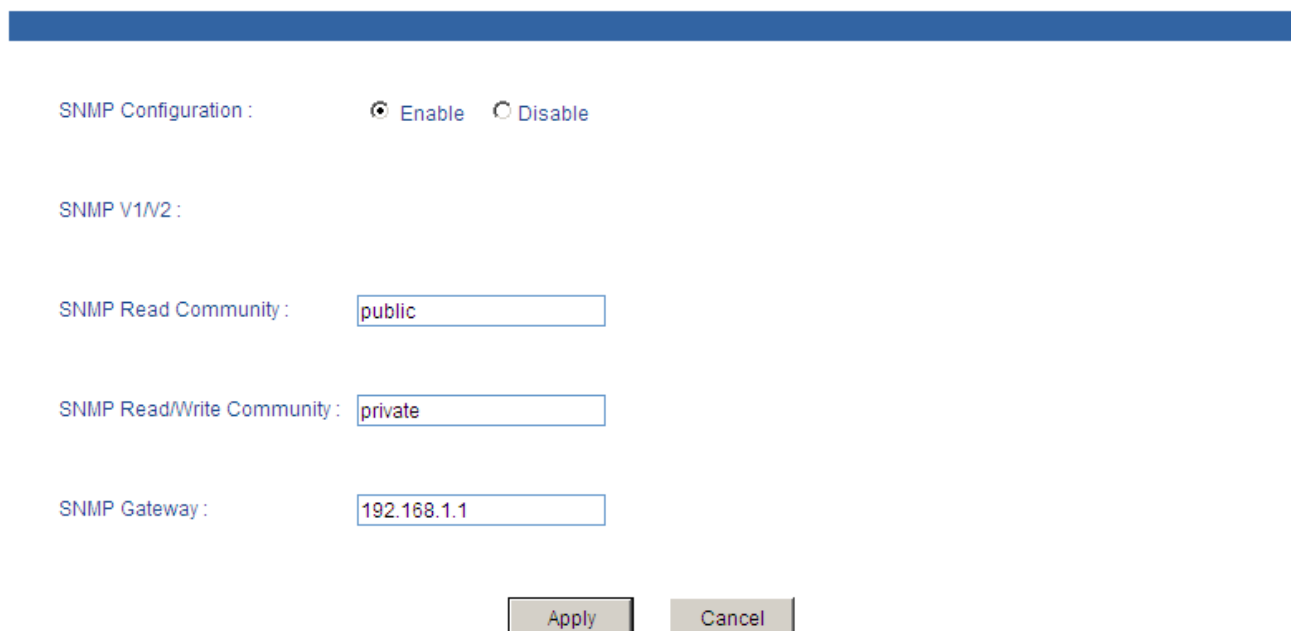
SNMP supports 3 kinds of basic operating in total:

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.

Currect Location>>Main Menu>>Remote Monitoring>>SNMP Configuration

SNMP Configuration :   ⦿ Enable   ○ Disable

SNMP V1/V2 :

SNMP Read Community :   public

SNMP Read/Write Community :   private

SNMP Gateway :   192.168.1.1

Apply   Cancel

（Figure 6.8.1）

Read Community

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

Read/Write Community

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

SNMP TRAP Gateway

IP address of the receiver of the alarm information sent Agent

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

6.8.2 Email Warning

Please make sure the switch can access internet regularly if use Email Warning. The gateway of the switch and local area network must identical
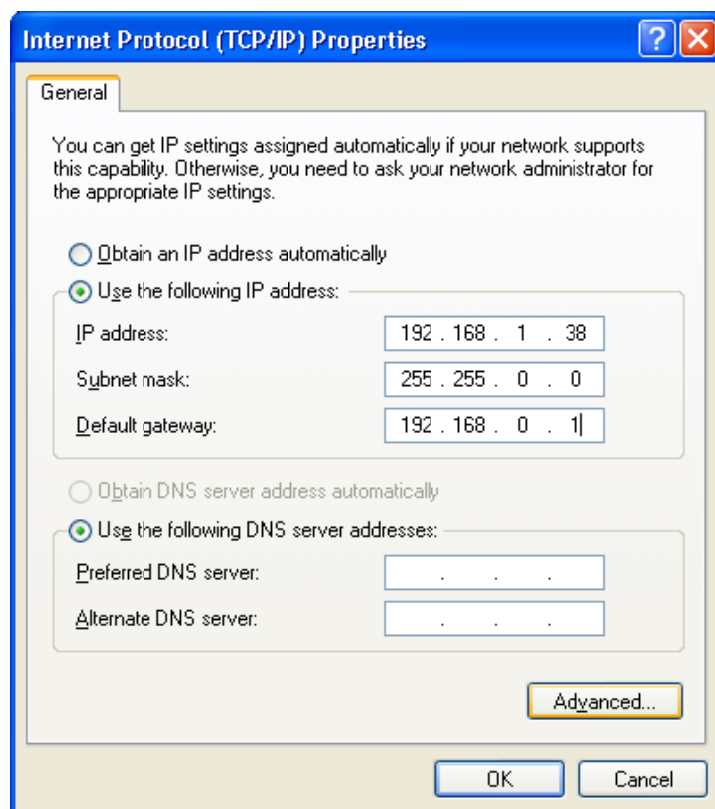
（Figure 6.8.2）

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

Current location>>Main Menu>>Remote Monitoring>>Email Warning

Email Alarm : ⦿ Enable ○ Disable

Mail Server : smtp.163.com

Receiver :

Sender :

Password :

Mail Interval : Any Times ▾ Send System Test Mail

Apply Cancel

（Figure 6.8.3）

Mail server

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

Sender

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

Password

E-mail password.

Receiver

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

Mail Interval

Regularly send log interval time

6.8.3 Relay Warning

Main function: when the device is in an abnormal statue, can timely inform the administrator, and quickly repair equipment, to avoid excessive losses.

Port alarm includes port dropped alarm, port enabled alarm, the device will output a signal to prompt the device is not working properly when the ports in abnormal status (connected or disconnected).

（Figure 6.8.4）

Figure as above: Relay warning mode have 3 types: no warning when have change, warning when have link, warning when have no link, user can choice the type according to their requirements.

6.9 Port Statistics

6.9.1 Rx Frame Statistics

（Figure 6.9.1）

Unicast

Numbers of the unicast data packets received by the port

Multicast

Numbers of the multicast data packets received by the port

Broadcast

Numbers of the broadcast data packets received by the port

Drop

Number of discarded normal data packets because of safety control

Pause

Ethernet control frames of protocol 0x8808 received by the port, in full duplex mode; this data packet is used to control frequency of data sending.

Undersize

Number of data packets (including FCS) less than 64 bytes

Oversize

Number of data packets (including FCS) more than 1518 or 1522 bytes (Enable VLAN)

Fragments

Number of incorrect or incomplete FCS data packets (including FCS) less than 64 bytes

Jabber

Number of incorrect or incomplete FCS data packets (including FCS) more than 1522 bytes

SysbolErr

Number of data packets which is incorrect, incomplete or including invalid characters (including FCS) between 64 bytes and 1518/1522 bytes (Enable VLAN)

6.9.2 Tx Frame Statistics

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

Port	Unicast	Multicast	Broadcast	Drop	Pause	Collision	Multiple Collision	LateCollision	Conflict Discard	Res Busy Discarded
1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0
7	0	0	0	0	0	0	0	0	0	0
8	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0
11	0	0	0	0	0	0	0	0	0	0
12	0	0	0	0	0	0	0	0	0	0

（Figure 6.9.2）

Unicast

Numbers of the unicast data packets sent by the port

Multicast

Numbers of the multicast data packets sent by the port

Broadcast

Numbers of the broadcast data packets sent by the port

Drop

Number of discarded normal packets because of lack of resources or not meeting analytic conditions (excluding discarded packets because of conflict)

Pause

Ethernet control frames of protocol 0x8808 sent by the port, in full duplex mode, this data packet is used to control frequency of data sending

Collision

Number of conflicts encountered in the port while sending data

Multiple Collision

Number of successful output packets (collision more than 1 time)

Late Collision

Numbers of packets less than 64 bytes when a conflict is detected.

Conflict Discard

Numbers of discarded packets caused by conflict happening more than 16 times.

Res Busy Discarded

Number of discarded packets out of stack queue because of lack of resources (large amounts of low priority data after enabling QoS)

6.9.3 Traffic Statistics

Current Location>>Main Menu>>Port Statistics >>Traffic Statistics

Port	Tx	Rx	Unicast	Multicast	Broadcast	Error
1	0	0	0	0	0	0
2	0	0	0	0	0	0
3	0	0	0	0	0	0
4	0	0	0	0	0	0
5	0	0	0	0	0	0
6	0	0	0	0	0	0
7	0	0	0	0	0	0
8	0	0	0	0	0	0
9	0	0	0	0	0	0
10	0	0	0	0	0	0
11	0	0	0	0	0	0
12	0	0	0	0	0	0

（Figure 6.9.3）

Tx

Number of bytes of all data packets sent by the port

Rx

Number of bytes of all data packets received by the port

Unicast

Number of unicast data packets sent and received by the port

Multicast

Number of multicast data packets sent and received by the port

Broadcast

Number of broadcast data packets sent and received by the port

Error

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

6.9.4 MAC address table

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

Current Location>>Main Menu>>Port Statistics >>MAC Address Table

MAC Address List

Address Mode : Auto

Join Port : Port 1

```
—Index—————MAC Address—————Type—————————VLAN—————————Port————
    1        FC-FA-F7-78-8E-48   Dynamic            1             14
    2        3C-97-0E-AC-7F-AC   Dynamic            1             14
```

（Figure 6.9.4）

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

1. Dynamic MAC address

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

2. Static certification (solidify) MAC address

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

3. Permanent static MAC addresses

permanent MAC address generated through configuration will not be aging, regardless of the device is connected switches of the change of the port, the MAC address table of MAC address and port of corresponding relation is always does not change, permanent MAC address does not disappear after the switch   is restart

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

1. The address of the device index according to switch's address, so all MAC address displayed VLAN value is 0.

2. Permanent static address configured in the previous static MAC address port list, need to modify the corresponding item when port changed.

3. Multicast address list displays the IGMP snooping item, in the address list here all unicast address.

4. MAC address aging time is 300 seconds, the port is disconnected our parent program to clear all the corresponding port items.

6.10 Diagnosis

6.10.1 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 collects all of the data from port 1 and port 2

（Figure 6.10.1）

Mirror Port

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

Monitored Port

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

Watch direction

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

1. This function is not often used. Otherwise other port-based higher management function like RSTP,IGMP SNOOPING

2. Port mirroring function can only deal with the normal FCS packets. It cannot deal with error data frames.

6.11Basic settings

6.11.1 SNTP

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

Current Location>>Main Menu>>Basic Settings>>SNTP

SNTP Configuration :　○ Local Time　⊙ Enable NTP

Time Zone :　(GMT+08:00) China, Hong Kong, Australia Western

NTP Server :　time.windows.com　(Opt)

System Time :　01-01-2008-Tues 19:39:13

PC Time :　03-11-2015-Wed 18:27:05

Apply　Cancel

（Figure 6.11.1）

Local Time

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

Enable NTP

To update the time of the device by using NTP protocol

Time Zone

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

NTP Server

It provides host name or IP address of NTP timing.

System Time

Device time

PC Time

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

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

6.11.2 Network & Reboot

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

IP Address

IP address is an 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.
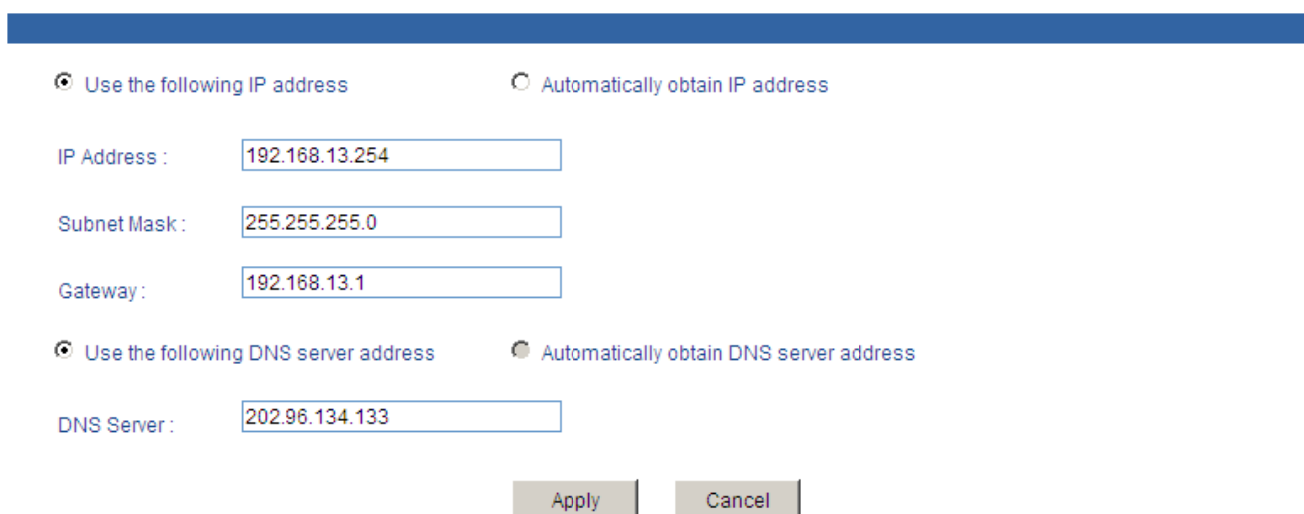
Default Gateway

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.

Current Location>>Main Menu>>Basic Settings>>Network & Reboot

⊙ Use the following IP address   ○ Automatically obtain IP address

IP Address :   192.168.13.254

Subnet Mask :   255.255.255.0

Gateway :   192.168.13.1

⊙ Use the following DNS server address   ○ Automatically obtain DNS server address

DNS Server :   202.96.134.133

Apply   Cancel

（Figure 6.11.2）

We can set the range of IP address as 192.168.x.x, 162.[16-31].x.x, or 10.x.x.x

NTP and EMAIL will use DNS service, please enter correct DNS address if use these two services.

Device Reboot

Click the "Reboot " button is confirmed, the device restarts, 20 seconds, and then click the menu bar returns to the Web network login interface, save the configuration before you restart, or reboot and configuration information not saved will be lost.

（Figure 6.11.3）

6.11.3 System Identification

Device information interface, graph, we can see the device module, device name, device description, device Serial number, contact information; this feature can change the above option, select settings and then restart to take effect.

（Figure 6.11.4）

Name

For marking each device on the network, give the device a different name, support for Chinese character input, is no more than 16 bytes.

Description

A summary description of the equipment is no more than 16 bytes.

Serial NO.

Describe the location of installation, support Chinese input, and most no longer than 30 bytes.

6.11.4 System File Upgrade

This function includes 4 kinds: Factory Defaults, Download Configuration, Upload Configuration and upgrade Firmware.

（Figure 6.11.5）

1. Factory Default

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

Use IE to login Web interface.

Click "System Management"

Click "System File Update"

Choose "Factory Default"

Click "OK"

Notice: the IP address will be "192.168.1.254".

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

2. Download Configuration

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

Use IE to login Web interface.

Click "System Management"

Click "System File Update"

Choose "Download Configuration"

Click "Download"

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

3. Upload Configuration

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

Use IE to login Web interface.

Click "System Management"

Click "System File Update"

Choose "Upload Configuration"

Click "Upload"

4. Upgrade Firmware

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

Use IE to login Web interface.

Click "System Management"

Click "System File Update"

Choose "Upgrade Firmware"

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

Click "Upgrade"

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

1. Load factory default will result in all status be in factory default settings, the IP could be static IP address "192.168.1.254".

2. Upload the configuration file, in the new configuration if static IP is not in the same network segment, the website will not be opened.

3. Use dynamic IP settings, but there is no DHCP server on the network segment, that will result in the relevant part of the IP will not be updated in the new configuration when upload configuration.

6.11.5 Logout

As shown in Figure 6.11.6, logout functionality for the system interfaces.

Current Location>>Main Menu>>Basic Settings>>Logout

Logout

System Logout :   OK

（Figure 6.11.6）

System Logout

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

Chapter 7 Repair and Service

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

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

Internet service.

Make a call to our technical office.

Return or replace product.

7.1 Internet Service

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

7.2 Make a call to our technical office

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

7.3 Repair or Replace

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

Appendix 1 Performance parameters

Electrical character				Environment		
Power input	Voltage	Power	Frequency	Working temperature①	Storage Temperature	Humidity
AC	86～264V	21W	46-63Hz	-40℃ - +75℃	-40℃ - +85℃	5-95%

www.3onedata.com

Appendix 2 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 （DiffServ 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 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. Why cannot increase the bandwidth after configured trunking?

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

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

When some of ports 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.

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

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