IT-ICS5028G-IM Series

Layer 2/Layer 3 Managed Industrial Ethernet Switch

User Manual

Version 1.0.0, Jan. 2016

www.intellisystem.it

Statement

Copyright Notice

Agreement

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

Revision History

Version No.	Date	Reason
V1.0.0	01-01-2016	Document creation

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

The series are high-performance, cost-effective smart rack-mounted industrial layer 3 switches. The increase in bandwidth elevates the data transmission capability, and it is very suitable for the application of large-scale industrial network. The switch supports IPv4, and various advanced administration functions such as IGMP, GMRP, DHCP Server/Client, STP/RSTP/MSTP, QOS, port mirroring, LLDP, static routing, RIP V1/V2, OSPF, VRRP, etc. The IPv4 layer 3 routing protocol, multicast technologies and policy routing mechanism provide users with complete IPv4/IPv6 solutions; meanwhile, this series of products also support SNMPv1/v2/v3 (Simple Network Management Protocol), CLI, Web Management, TELNET management for more convenient device management. Combined with enhanced ACL control and anti-attack function, the management will be more secure.

The switches comply with the FCC and CE standards, and supports 2-way redundant AC inputs and 2-way relay fault alarm output. Users can select flexibly according to actual environment. It adopts industrial no fan design, and is fit for severe industrial environment at a working temperature of -40℃～75℃, which can meet various industrial application requirements and provide reliable and economic solutions for Ethernet access.

1.2 Features

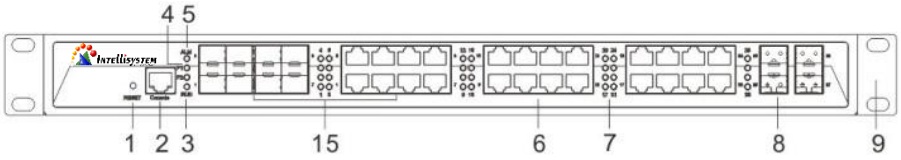
- Support IGMP Snooping and GMRP filter multicast packet
- Support QOS of IEEE 802.1p/1Q TOS/DiffServ to promote network stability
- Support SNMP v1/v2/v3
- Support IEEE802.1X, HTTPS, and SSH to enhance network security
- Support link static / dynamic aggregation to optimize bandwidth
- Support ACL function to enhance flexibility and security of network management
- Support bandwidth management, ensuring network stability
- Support RMON, effectively improve network monitoring and predictive ability
- Support port mirroring for online debugging
- Support STP/RSTP/MSTP to enhance network stability
- Support IEEE802.1Q VLAN for easy network planning
- Support static routing, RIP, VRRP, OSPF Layer 3 Switching Technology
- Working temperature: -40℃-75℃
- Support two 100VAC~240VAC power inputs
- Support two power supplies for redundancy and high reliability
- Support two relay alarms to enhance reliability
- No fan design, industrial and rack-mounted installation

Chapter 2 Hardware Description

2.1 Panel Design

16-port 10/100/1000BaseT(x) + 8-port Gigabit Combo + 4-port 10GbE SFP:

Front panel

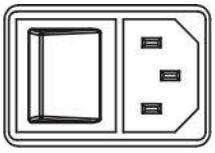


Rear panel

1. Restore factory settings
2. Console port
3. Systems running LED
4. The power LEDs (P1, P2)
5. Relay alarm LED
6. 10/100/1000BaseT(X) (RJ45) ports
7. Ethernet port Link/ACT LEDs(1~28)
8. 10 Gigabit Ethernet SFP+ slot
9. Rack mount ears
10. Relay 1 output terminal block
11. Power 1 input power socket
12. Grounding screw
13. Relay 2 output terminal block
14. Power 2 input power socket
15. 10/100/1000BaseT(X) or 1000Base SFP slot combo ports

2.2 Power Input

The switch support dual redundant power supplies: Power Supply 1 (P1) and Power Supply 2 (P2). The switch rear panel provides power sockets for AC100~240V power entered. Socket diagram is as follows:



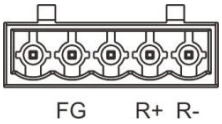
The redundant power can be used independently. P1 and P2 can supply power at the same time, once either of these two powers fails, another power can acts as backup automatically to ensure reliability of the network.

Important notice:

1. Power ON operation: Please connect to the device at first and then connect to the power supply with power cable.
2. Power switch “—” means power ON, “O” means power OFF.
3. Power OFF operation: First, the powers switch to the "O" side and then disconnect the power supply. Finally disconnect the connection between the device and the power cord.

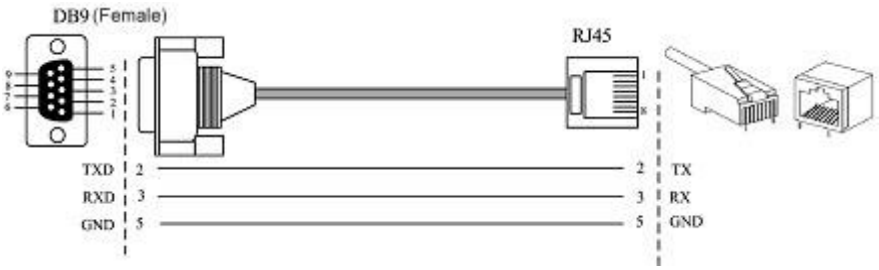
2.3 Relay connection

Relay access terminals in the rear panel of the device, next to the power input parts, R+ and R- are in the middle of the relay alarm output section. 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. This series of switch device have 2 relay alarm output, external alarm lights or alarm buzzer or external switch signal acquisition device in order to timely notify operators when an alarm occurs.



2.4 Console port

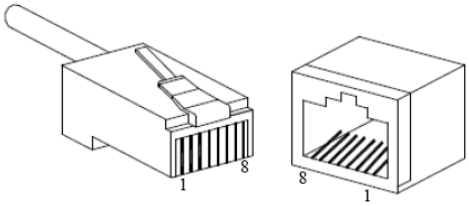
This series product provided 1pcs procedure test port based in serial port. It adopts RJ45 interface, located in top panel, can configure the CLI command through RJ45 to DB9 female cable.



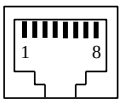
2.5 Communication port

10/100/1000BaseT(X) Ethernet port

The pinot define of RJ45 port display as below, connect by UTP or STP. The connect distance is no more than 100m. 100Mbps is used 120Ωof UTP 5, 10Mbps is used 120Ωof UTP 3, 4, 5.



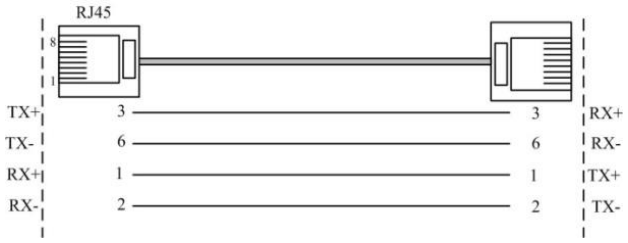
RJ 45 port support automatic MDI/MDI-X operation. That can connect the PC, Server, Converter and HUB. Pin 1, 2, 3, 4, 5, 6, 7, 8 Corresponding connections in MDI. 1→3, 2→6, 3→1, 4→7, 5→8, 6→2, 7→4, 8→5, are used as cross wiring in the MDI-X port of Converter and HUB. In MDI/MDI-X, 100/1000Base-TX PIN defines is as follows:



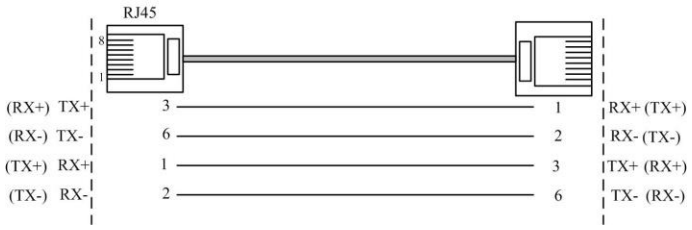
PIN	MDI	MDI-X
1	BI_DA+/TX+	BI_DB+/RX+
2	BI_DA-/TX-	BI_DB-/RX-
3	BI_DB+/RX+	BI_DA+/TX+
4	BI_DC+/—	BI_DD+/—
5	BI_DC-/—	BI_DD-/—
6	BI_DB-/RX-	BI_DA-/TX-
7	BI_DD+/—	BI_DC+/—
8	BI_DD-/—	BI_DC-/—

Note：10Base-T/100Base-TX, “TX±”transmit data±, “RX±”receive data±, “—”not use.

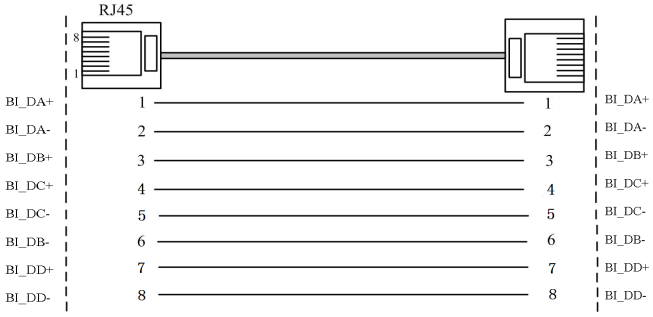
10/100Base-T(X) MDI (straight-through cable)



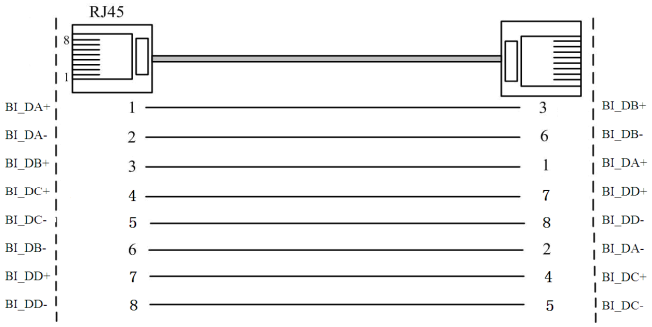
10/100Base-T(X) MDI-X (Cross-over cable)



Gigabit MDI (straight-through cable)



Gigabit MDI-X (Cross-over cable)

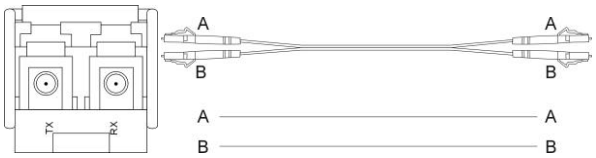


MDI/MDI-X auto connection makes switch easy to use for customers without considering the type of network cable.

1000Base SFP /10GbE SFP+ fiber port

1000BaseSFP and 10GbE SFP+ optical fiber interface is used are SFP optical module communication through optical fiber transmission, can choice different SFP module according to different transfer distance. Fiber interface must use for pair, TX port is transmit side, must connect to RX (receive side). The fiber interface support loss line indicator.

Suppose: If you make your own cable, we suggest labeling the two sides of the same line 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

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

System Indication LED		
LED	State	Description
PWR (P1~P2)	ON	Power is being supplied to power input PWR input
	OFF	Power is **not** being supplied to power input PWR input
RUN	ON/OFF	System is not running well
	Blinking	System is running well
Alarm	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.
Link/ACT (1~28)	ON	Port connection is active
	Blinking	Data transmitted
	OFF	Port connection is not active

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: 100~240VAC power input
6. Environment: working temperature -40～75℃
   Storage Temperature -40～85℃
   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.

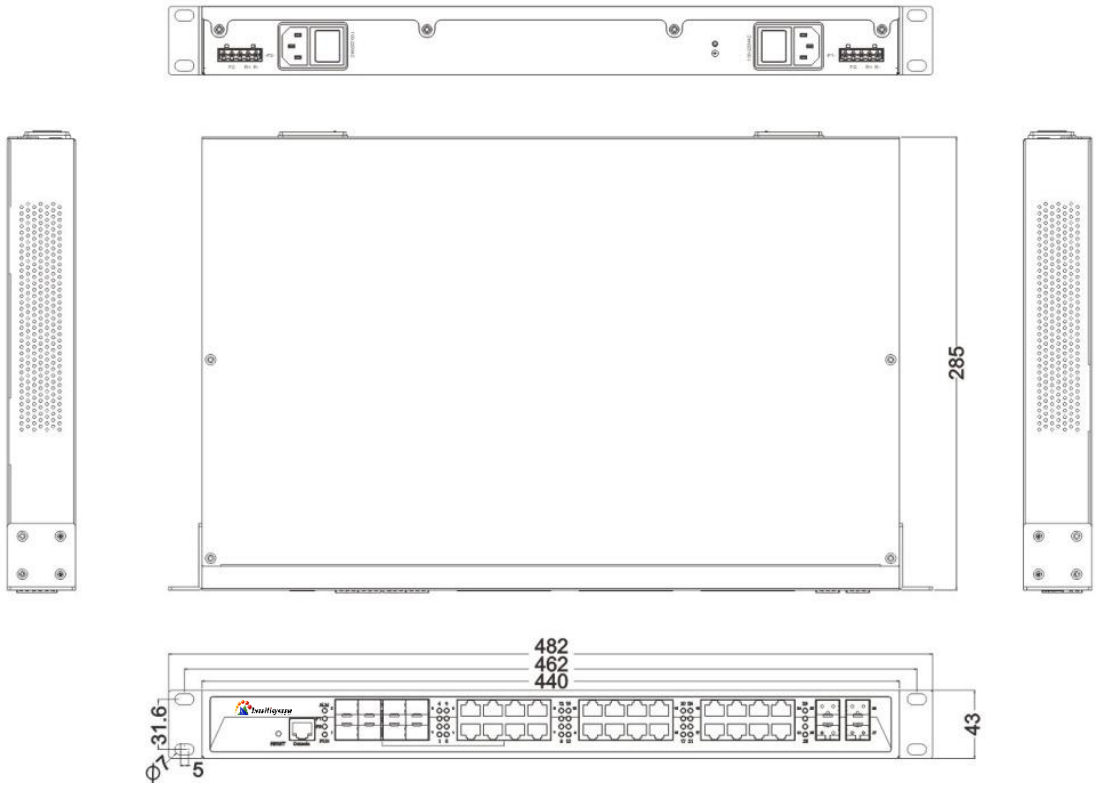
Chapter 3 Appearance and Dimension

3.1 Appearance

IT-ICS5028G-4XGS-8GC-16GT-IM

3.2 Dimension

The series of products are the same size, and the number of the Ethernet interface is 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
Intellisystem Industrial Ethernet switch	1
User manual	1
Documentation and software CD	1
Warranty card	1
Power supply cable	2
Certificate of quality	1
Rackmount ears	2

Intellisystem Technologies S.r.l.
Via Augusto Murri, 1 – 96100 Siracusa - Phone +39 (0)931-1756256 / +39 (0)2-87167549 - Mobile (+39) 335 1880035
em@il: info@intellisystem.it WEB: http://www.intellisystem.it

Chapter 5 Network Configuration

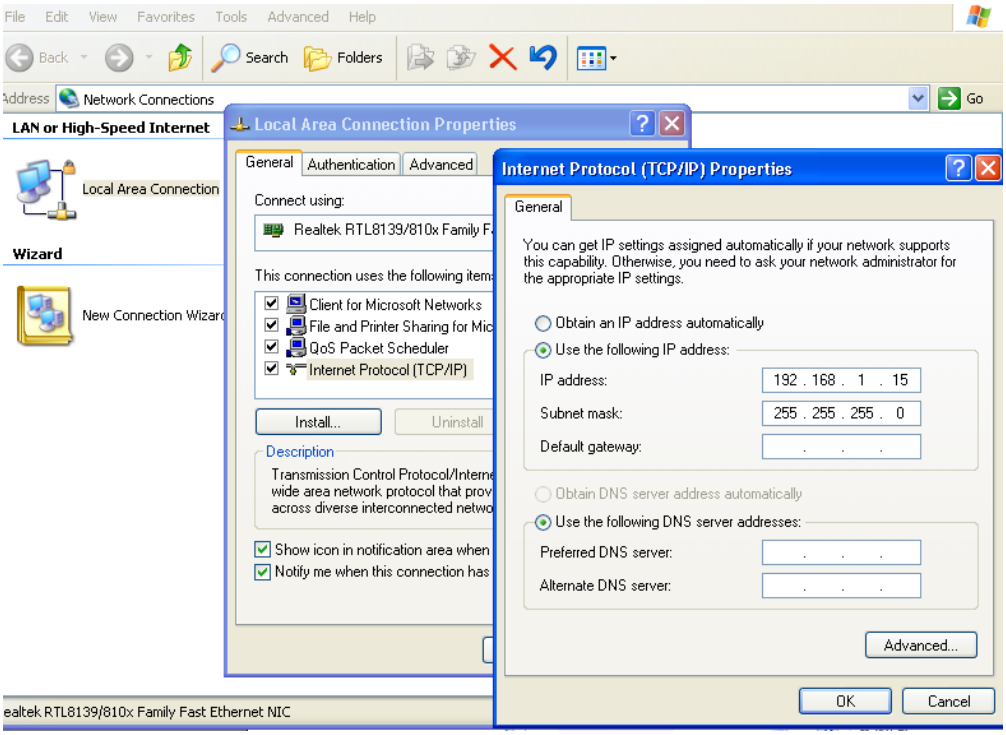
The switch can access, configuration and management through WEB, the user manual will introduce the operations step by step.

5.1 Configure PC's IP Address

The switch default address is: 192.168.1.254, subnet mask is: 255.255.255.0. When entering into 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 switch's IP address to make sure that they are in the same Local Area Network. Operating process can follow method 1 or method 2 as below,

Method 1: Modify PC's IP address

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



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

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

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

Chapter 6 WEB Management

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

6.1 Configurate preparing

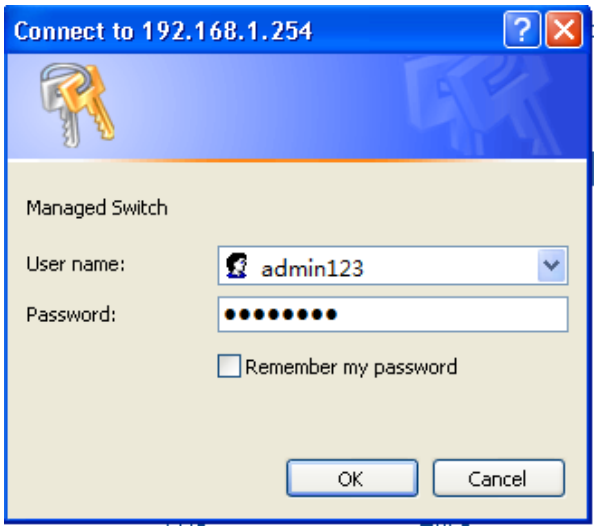
1. The lowest requirement for user's computer is as below:

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

How to log on to Web Server

Please type in the default IP of switch on the browser's address bar, and then will pop-up a window by clicking the "enter" key which shows you have to enter your user name and password. The default username and password are "admin123", case sensitive for this series. The default password is with administrator privileges. 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)

Menu Introduction:

Main Menu	Tag	Function
System Configuration	System information	Can display the system parameters of the switch, such as: device model, MAC address, etc.
	User configuration	Set the user name and password with different permissions
	Device log message	The configuration file upload and view device configuration
	TELNET-config	Through the Telnet connection configuration
	HTTPS-config	WEB interface access
	Diagnosis	By Ping, traceroute, port loopback check network
Port Configuration	Port Settings	Display and configure information of each port: such as connection status, configuration modes, flow status etc.
	Storm control	Set port storm suppression type and flow rate
	Port rate-limit	Set port input rate and output rate
	Mirror	Set source port and destination port
	Alarm setting	Set relay alarm
	Port channel Config	Static and LACP configuration
	Isolate-port Config	Set isolation port
	Port statistic	Port data statistics
Layer 2 Configuration	VLAN Configuration	Displays the list of the current VLAN, and the configuration and management of the VLAN (access, trunk, translate)
	Mac-vlan	Configure Mac-vlan parameters
	Protocol-vlan	Configure Protocol-vlan parameters
	Voice-vlan	Configure Voice-vlan parameters
	MAC config	View MAC address learning and setting MAC aging time, static mac, mac limit config.
	Spanning-tree	Set STP, RSTP, MSTP related parameters
	IGMP-Snooping	Viewing the multicast address and the setting of static multicast
	SW-Ring config	Set ring network type and related parameters
	GMRP config	Set the relevant port parameters and view the multicast address
Layer 3 Configuration	Interface config	Interface add and IP address setting
	ARP config	Show ARP information, static ARP and ARP age-time setting
	VRRP config	VRRP configuration
	ND config	Static ND configuration
Route config	Show config	Show route configuration
	Static config	Add static route
	RIP config	RIP global setting and RIP network setting
	OSFP config	OSFP global setting and OSFP network setting

Intellisystem Technologies S.r.l.
Via Augusto Murri, 1 – 96100 Siracusa - Phone +39 (0)931-1756256 / +39 (0)2-87167549 - Mobile (+39) 335 1880035
em@il: info@intellisystem.it WEB: http://www.intellisystem.it

Main Menu	Tag	Function
	BGP config	BGP configuration
Network security	Access control	access control
	Attack protection	Anti-attack setting
	ACL config	ACL related configuration, including the group ACL configuration, time range configuration, IP ACL and MAC ACL configuration
	802.1x config	802.1X authentication configuration
Advanced configuration	QOS config	The selection and implementation of QOS scheduling mode
	LLDP config	Set to allow the local subnet of network devices to notify their information
	SNMP config	Set SNMP related parameters and view
	RMON config	Set Rmon related information configuration and view
	DHCP Server config	Set the DHCP address pool and the address or port binding
	DHCP-snooping	Set DHCP- snooping related parameters
	DHCP Relay config	Set DHCP Relay related parameters
	DNS config	Set the domain name corresponding to the IP
	NTP config	Set NTP, time zone and other parameters configuration
System management	Management File	Switch software upgrade, access, save or restore the configuration of the switch
	Save	Save the current configuration
	Reboot	reboot device
	Restore	Restore factory settings
	Firmware	System upgrade

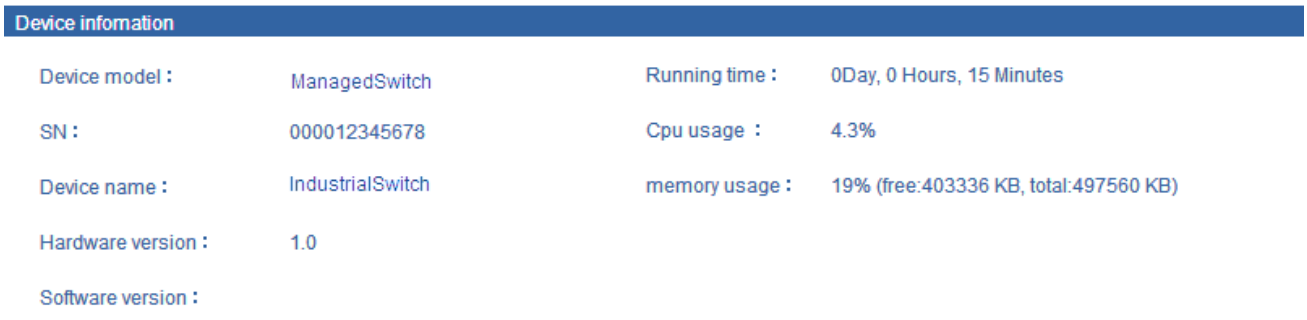
Web Timeout Treatment

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 Configuration

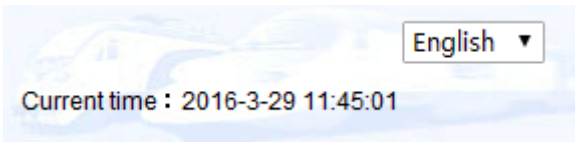
6.2.1 System information



(Figure 6.2.1.1)

Configuration Items	Description
Device Name	Network mark of the device. It is convenient for management tools to judge.
Device Module	The device type.
SN	Serial number of the device. It is convenient for device management.
Hardware Version	Current hardware version.
Firmware Version	Current firmware version.
Running time	Current device usage time
CPU usage	Current device using CPU information
Memory usage	Current devices use memory size information
CPU MAC	Hardware address of the device. It is a unique address, which is made up of hexadecimal number with 48 bits (6 bytes) in length.

Time display and language switching



(Figure 6.2.1.2)

Intellisystem Technologies S.r.l.
Via Augusto Murri, 1 – 96100 Siracusa - Phone +39 (0)931-1756256 / +39 (0)2-87167549 - Mobile (+39) 335 1880035
em@il: info@intellisystem.it WEB: http://www.intellisystem.it

Port information

Port info

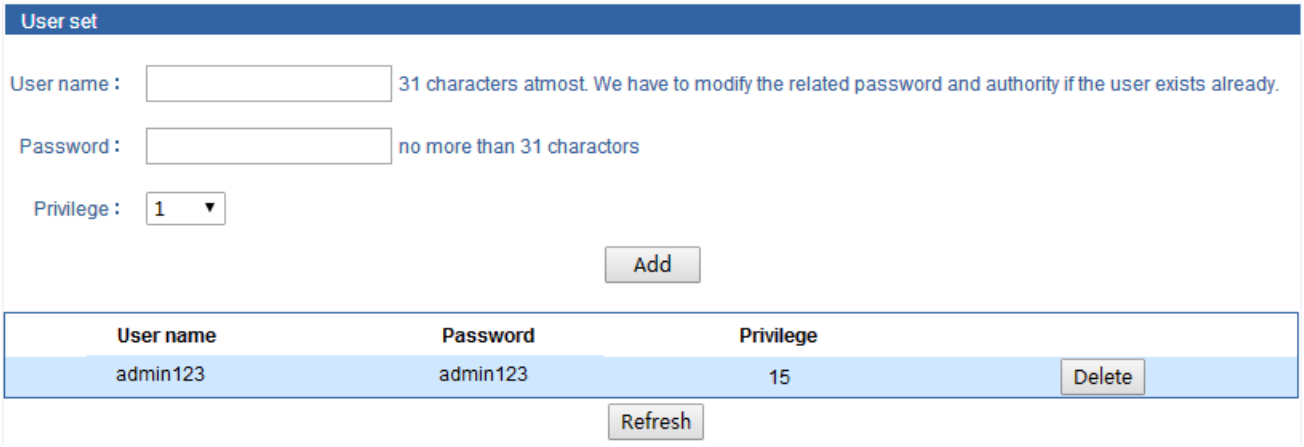
Port number	Connection state	Port state	Rate	Interface type
ge1/1	LINK	FULL	100M	Electricty
ge1/2	LOS	HALF	10M	Electricty
ge1/3	LOS	HALF	10M	Electricty
ge1/4	LOS	HALF	10M	Electricty
ge1/5	LOS	HALF	10M	Electricty
ge1/6	LOS	HALF	10M	Electricty
ge1/7	LOS	HALF	10M	Electricty
ge1/8	LOS	HALF	10M	Electricty

（Figure 6.2.1.3）

Port 1, 2...28, if the port is connected properly the status should be LINK, no connection status will be LOS.

6.2.2 User configuration

User login method by user name and password to access the device, the initial user name and password are: admin123. At the same time, users can also be free to add and delete users.



（Figure 6.2.2.1）

User name: Visitor's identity, does not contain the 'spaces' and '& ; ” ’ \ / ” etc. characters, the length of the character is not more than 31 characters

Password: Visitor use password, does not contain the 'spaces' and '& ; ” ’ \ / ” etc. characters, the length of the character is not more than 31 characters

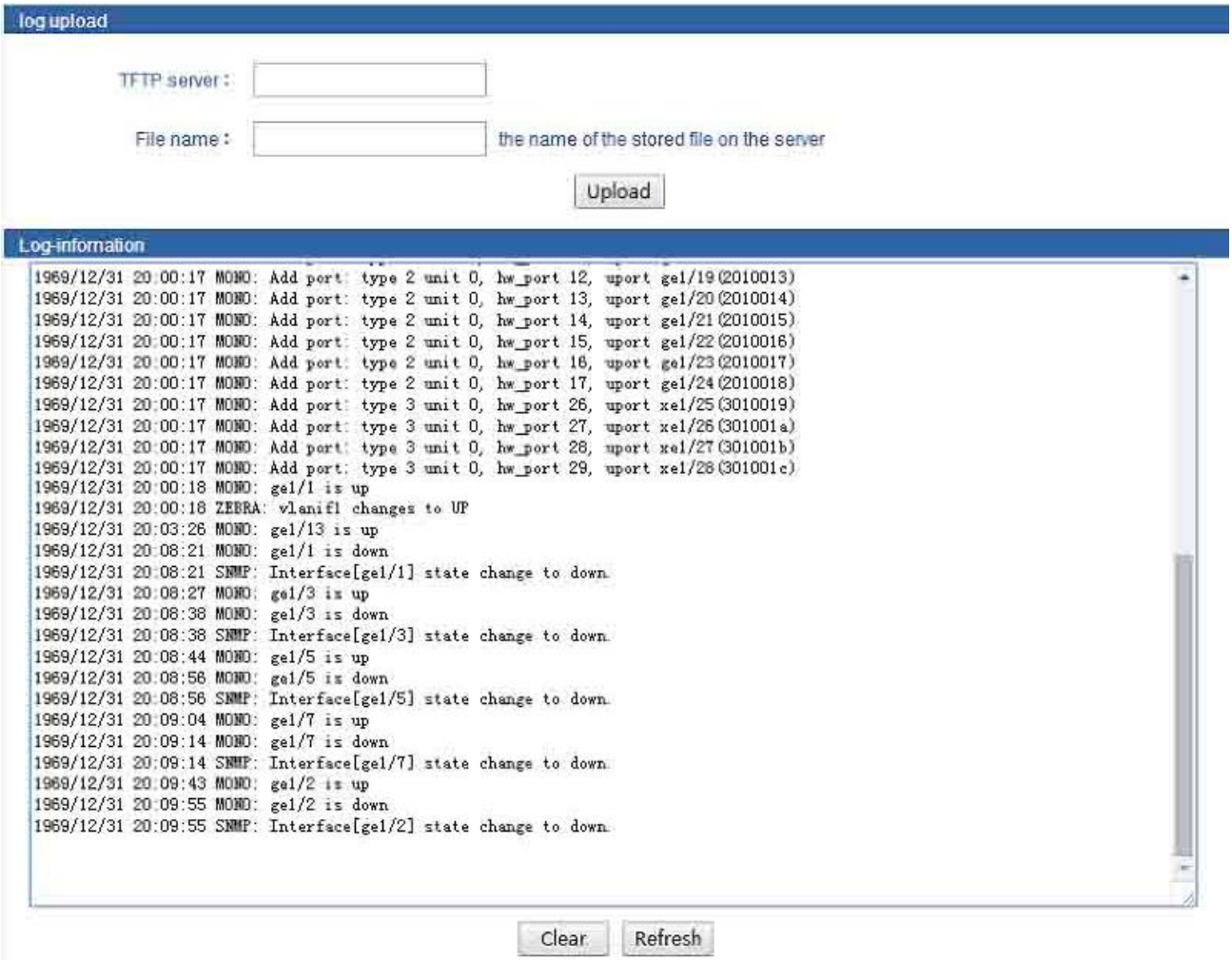
Privilege: The visitor's permission is 1~15

If you forget the user name and password, please contact the company's technical support in the home page in order to get help.

6.2.3 Device log message

Log configuration of the main functions of the role: to view the device log information (history configuration information records), upload device log information to the TFTP server.

In the menu bar, click on the "main menu", "system configuration", "Device log configuration", enter the log configuration interface.



（Figure 6.2.3.1）

Upload log steps:

Step 1: in the TFTP server text box to fill in the TFTP server where the IP address.

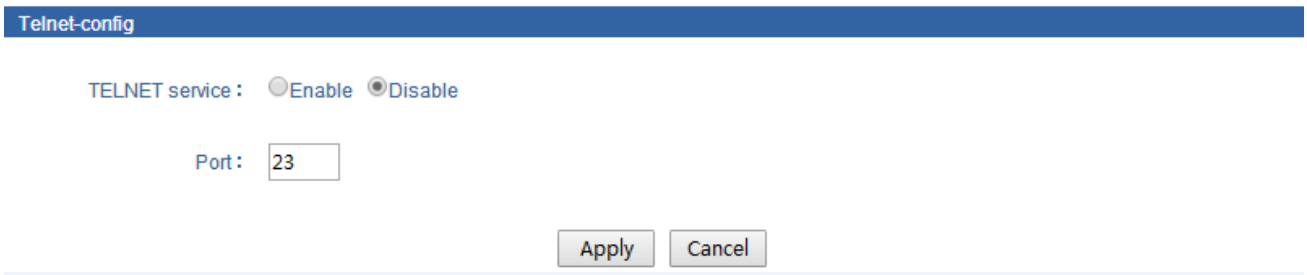
Step 2: fill in the file name in the file box to save the file on the server.

Step 3: click the "Upload" button

6.2.4 Telnet configuration

Enable TELNET services, TELNET terminal can be connected to the switch through the use of Telnet PC program.

In the menu bar, click on the "main menu", "system configuration", "TELNET configuration", enter the TELNET configuration interface.



（Figure 6.2.4.1）

The terminal is connected to the switch by Telnet using the PC program, which is required to have the following conditions:

1, enable switch TELNET services

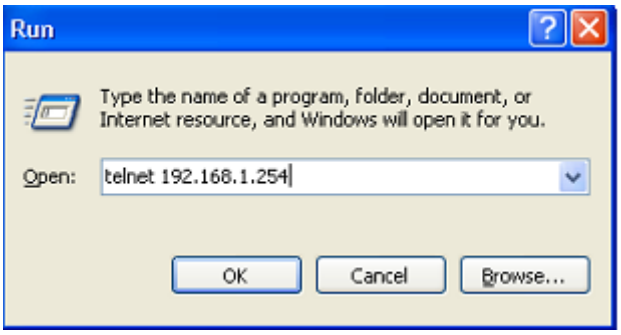
2, know the IP address of the switch equipment, can be modified to obtain (in the system management view can use the IP command);

3, if connected to the PC terminal and the switch port within the same local area network (LAN), the IP address must be set in the same segment; otherwise, terminal and the switch must cross the router.

Meet the above three points you can use the Telnet command to log on to the switch, and then set the switch.

1, the establishment of the environment, only the computer network port through the LAN and the network port of the switch connection.

2, through the Telnet login the switch before you need to enter the ‘Telnet+ space + switch’s IP’ to verify.



（Figure 6.2.4.2）

Intellisystem Technologies S.r.l.
Via Augusto Murri, 1 – 96100 Siracusa - Phone +39 (0)931-1756256 / +39 (0)2-87167549 - Mobile (+39) 335 1880035
em@il: info@intellisystem.it WEB: http://www.intellisystem.it

TELNET configuration steps:

Step 1: choose to enable or disable the radio buttons in TELNET services;

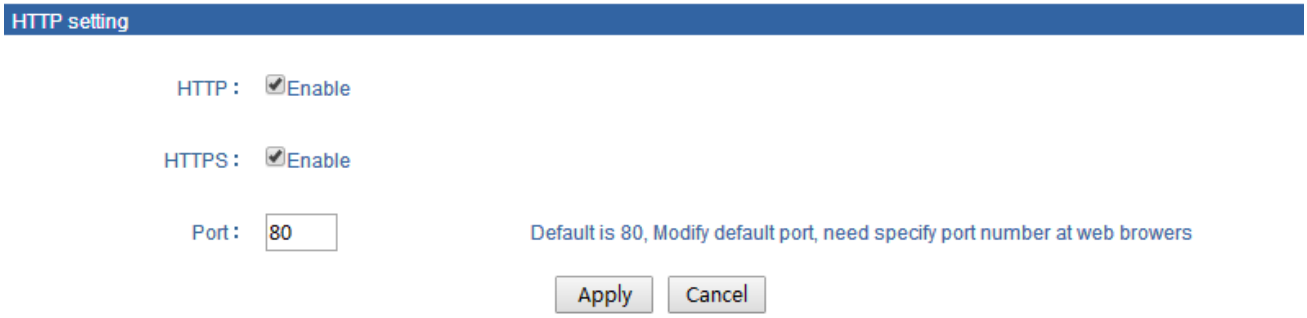
Step 2: in the port of the text box to fill in the port number, the default port number is 23;

Step 3: click the "Settings" button.

6.2.5 HTTPS configuration

HTTPS (Transfer Protocol Hypertext over Secure Socket Layer), is the goal of safety as the goal of the HTTP channel, is simply a safe version of HTTP. HTTPS provides data encryption services to prevent the attacker to intercept the Web browser and the web server for the transmission of messages, in order to obtain some of the sensitive information, such as credit card numbers, passwords, etc.

In the menu bar, click on the "main menu", "system configuration", "HTTPS configuration", enter the HTTPS configuration interface.



（Figure 6.2.5.1）

Enable HTTP, access to the format: HTTP://192.168.1.254.

Enable HTTPS, access to the format: HTTPS://192.168.1.254.

HTTPS configuration steps:

Step 1: check the box in the HTTP check box to enable;

Step 2: check the box in the HTTPS check box to enable;

Step 3: in the port of the text box to fill in the port number, the default port number is 80;

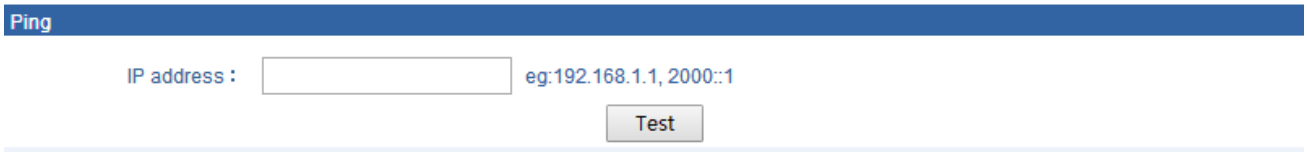
Step 4: click the "Apply" button.

6.2.6 Diagnosis

6.2.6.1 Ping

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

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



（Figure 6.2.6.1）

Ping configuration steps:

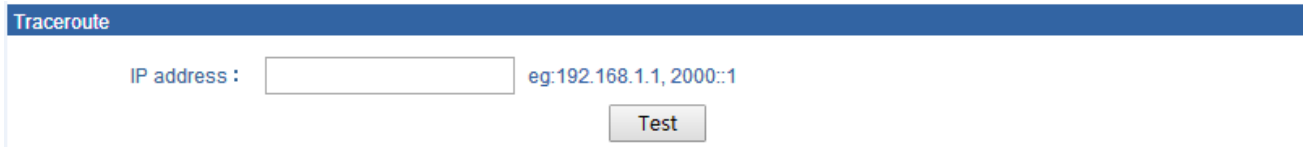
Step 1: In the IP, address text box to fill in the need for IP Ping address;

Step 2: click on the "test" to see the results of the ping.

6.2.6.2 Traceroute

Traceroute to measure the length of time it takes to send a small packet to the destination device until it returns. A path on each device traceroute to be measured 3 times. The output results include the time for each test (MS) and the name of the device (if any) and its IP address.

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



（Figure 6.2.6.2）

Traceroute configuration steps:

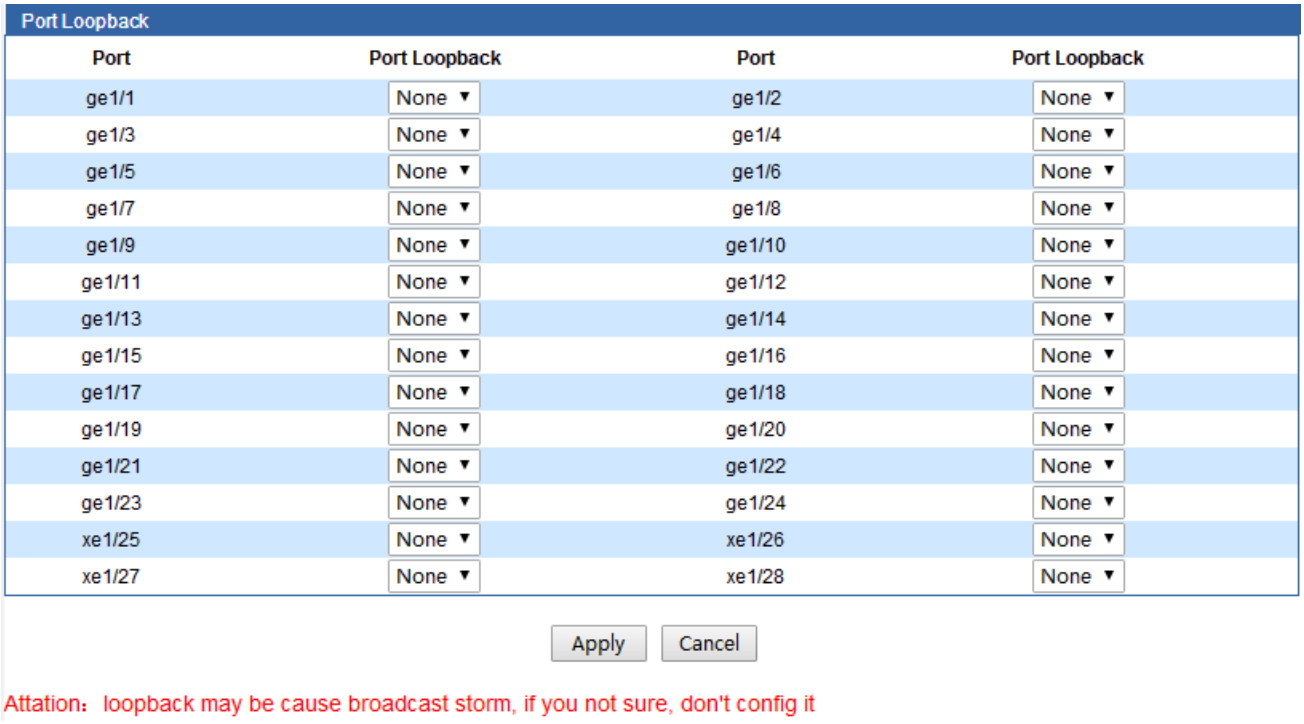
Step 1: fill in the destination IP address in the IP address text box;

Step 2: click "test" to see the results.

6.2.6.3 Port loopback

Port loopback is a common method for the maintenance and troubleshooting communication port line. The receiving end of the test equipment or line is Short circuit with the sending end, so that the device can receive the signal from the signal to judge whether there is a breakpoint on the line or port. The transmission quality of the loop circuit can also be tested by hanging the test instrument on the loop circuit.

In the menu bar, click on the "main menu", "system configuration", "diagnostic", "Port loopback", enter the port loop configuration interface.



Port Loopback

Port	Port Loopback	Port	Port Loopback
ge1/1	None	ge1/2	None
ge1/3	None	ge1/4	None
ge1/5	None	ge1/6	None
ge1/7	None	ge1/8	None
ge1/9	None	ge1/10	None
ge1/11	None	ge1/12	None
ge1/13	None	ge1/14	None
ge1/15	None	ge1/16	None
ge1/17	None	ge1/18	None
ge1/19	None	ge1/20	None
ge1/21	None	ge1/22	None
ge1/23	None	ge1/24	None
xe1/25	None	xe1/26	None
xe1/27	None	xe1/28	None

Apply Cancel

Attation：loopback may be cause broadcast storm, if you not sure, don't config it

（Figure 6.2.6.3）

Configuration port loop back step:

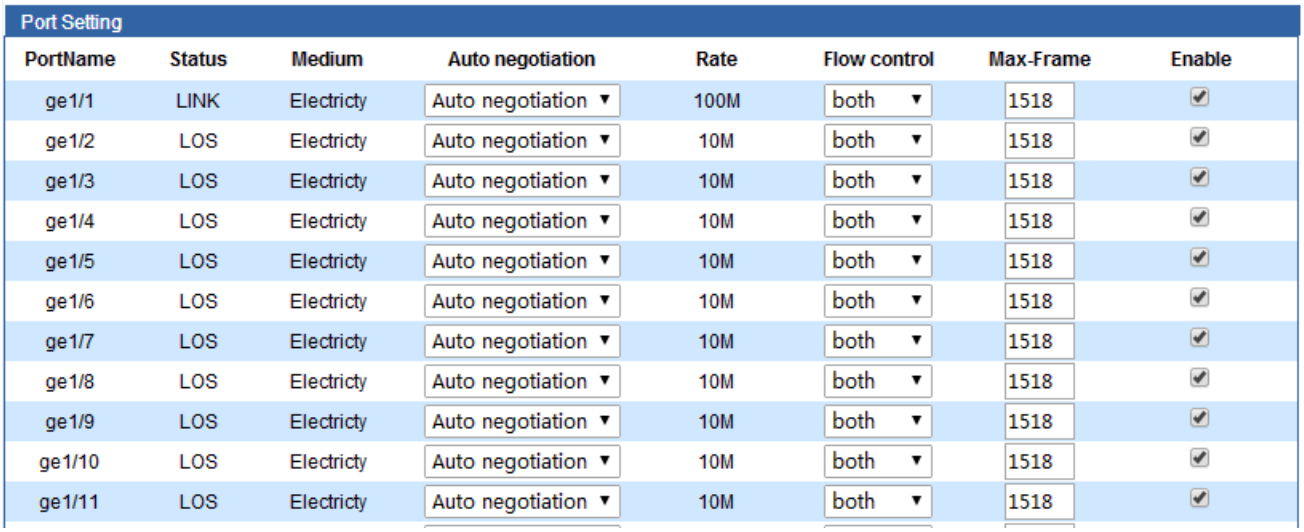
Step 1: select the None, MAC, or PHY in the drop-down box in the port loop;

Step 2: click the "Apply" button.

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.



Port Setting

PortName	Status	Medium	Auto negotiation	Rate	Flow control	Max-Frame	Enable
ge1/1	LINK	Electricty	Auto negotiation	100M	both	1518	☑
ge1/2	LOS	Electricty	Auto negotiation	10M	both	1518	☑
ge1/3	LOS	Electricty	Auto negotiation	10M	both	1518	☑
ge1/4	LOS	Electricty	Auto negotiation	10M	both	1518	☑
ge1/5	LOS	Electricty	Auto negotiation	10M	both	1518	☑
ge1/6	LOS	Electricty	Auto negotiation	10M	both	1518	☑
ge1/7	LOS	Electricty	Auto negotiation	10M	both	1518	☑
ge1/8	LOS	Electricty	Auto negotiation	10M	both	1518	☑
ge1/9	LOS	Electricty	Auto negotiation	10M	both	1518	☑
ge1/10	LOS	Electricty	Auto negotiation	10M	both	1518	☑
ge1/11	LOS	Electricty	Auto negotiation	10M	both	1518	☑

（Figure 6.3.1）

Configuration Items	Description
Port	Port name, corresponding to mark in panel.
Status	Display port connection whether or not
Medium	Display port type (optical interfaces and electrical interfaces).
Auto negotiation	Auto-negotiation（AUTO, full duplex（FULL）, half duplex （HALF）optional, default mode is auto-negotiation mode.
Rate	Display configurable speed of port or auto-negotiation mode.
Flow Control	Whether selecting flow control to the port. Only can selecting flow control when the port enable. The default is off.
Max-Frame	Display port transmission maximum frame length
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”.

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 Storm control

When the host system responds to a packet that is constantly circulating on the web or tries to respond to a system that is not responding, a broadcast storm will occur, and even a network will be blocked or paralyzed. In order to prevent the network storm, you can set the storm suppression. Storm suppression is set to allow the entire system to pass the maximum broadcast, multicast or unknown unicast packet traffic. When each port broadcast, multicast or unknown unicast traffic and achieve the user to set the value, the system will discard beyond the broadcast, multicast or unknown unicast flow limitation message, so that overall broadcast, multicast or unknown unicast traffic accounted for the proportion of reduced to limit the scope of, and ensure the normal operation of the network business.

In the menu bar in order to click on the "main menu", "port configuration", "storm control" into the storm suppression configuration interface.

Storm control

Port	Broadcast(kbps)	Unkown Multicast(kbps)	Unkown Unicast(kbps)
ge1/1	0	0	0
ge1/2	0	0	0
ge1/3	0	0	0
ge1/4	0	0	0
ge1/5	0	0	0
ge1/6	0	0	0
ge1/7	0	0	0
ge1/8	0	0	0
ge1/9	0	0	0
ge1/10	0	0	0
ge1/11	0	0	0
ge1/12	0	0	0
ge1/13	0	0	0
ge1/14	0	0	0
ge1/15	0	0	0
ge1/16	0	0	0

（Figure 6.3.2）

Causes the broadcast storm is a variety of reasons, for example, between the switches, a redundant or incorrect connection, forming a loop, broadcast packets multicast packet through the switch is forwarded to the other port received broadcast packets and multicast packet port will continue to broadcast, resulting in the network and broadcast storm. In some cases, the broadcast storm control to prevent a malicious attack people. For example: DOS (denial of service) attack, DOS by a host requests to a broadcast address to send ICMP, leading to other hosts respond to this broadcast address, due to the DoS attack broadcast storm.

If the storm control function is enabled, this attack can be prevented. For the type of storm, we test the three types of packets:

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.

Unknown unicast packet: the MAC address of the data frame does not exist in the internal index table of the device, which needs to be forwarded to all ports.

Storm suppression configuration step:

Step 1: in the broadcast text box, enter the inhibit value, range is 0-1000000;

Step 2: in the unknown multicast text box to enter the value, the range is 0-1000000;

Step 3: in the unknown unicast text box, enter the inhibit value; range is 0-1000000;

Step 4: click the "Apply" button.

6.3.3 Port rate-limit

This device provides port speed limits, including entry and exit speed limits. Users can limit the communication flow of each port or cancel the port traffic limit. Users can select a fixed speed, its scope in 0kbps~ 1000Mbps (Gigabit), the device will according to whether the flow control is enabled to decide is to drop the message or the use of flow control to limit the transmission speed of end equipment or receiving speed.

In the menu bar, click on the "main menu", "port configuration", "port rate-limit", enter the port speed limit configuration interface.

Port rate-Limit

Port	InputRate(kbps)	InputBurst(kbps)	OutputRate(kbps)	OutputBurst(kbps)
ge1/1	0	0	0	0
ge1/2	0	0	0	0
ge1/3	0	0	0	0
ge1/4	0	0	0	0
ge1/5	0	0	0	0
ge1/6	0	0	0	0
ge1/7	0	0	0	0
ge1/8	0	0	0	0
ge1/9	0	0	0	0
ge1/10	0	0	0	0
ge1/11	0	0	0	0
ge1/12	0	0	0	0
ge1/13	0	0	0	0
ge1/14	0	0	0	0
ge1/15	0	0	0	0
ge1/16	0	0	0	0
ge1/17	0	0	0	0

（Figure 6.3.3）

The device provides a rate limit of two directions, in which the inlet velocity is the actual rate of flow from the PC and other devices to the switch port. Exit speed is the actual speed between the switch port and the flow of the device. If at the same time limit the inlet velocity and outlet velocity between the two devices, the actual speed is smaller.

Port speed limit configuration step:

Step 1: in the input rate of the text box to fill in the input rate value, the range is 0-1000000;

Step 2: in the input burst of the text box to fill in the input burst value, the range is 0-1000000;

Step 3: in the output rate of the text box to fill in the output rate value, the range is 0-1000000;

Step 4: in the output burst of unexpected text box to fill in the output burst value, the range is 0-1000000;

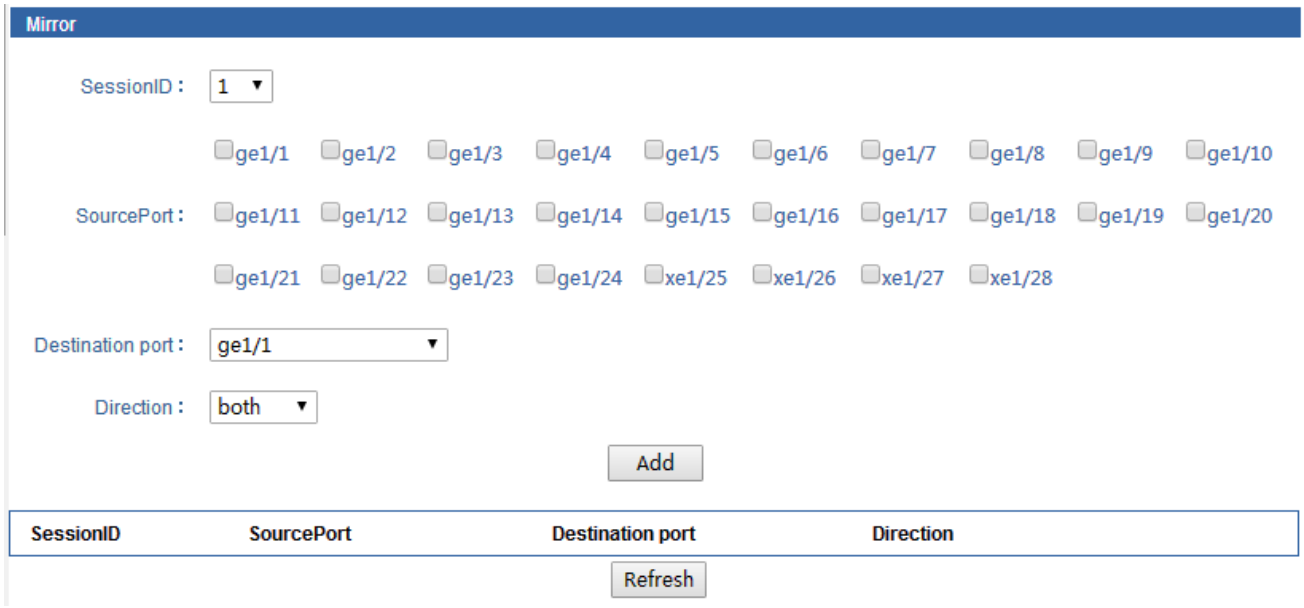
Step 5: click the "Apply" button.

1, the use of port speed limit, flow control should be enabled, otherwise the speed between the device will no longer be a smooth curve;
2, the use of the port speed limit, should not be lost packet unless the flow control is disabled. Packet loss is the representation of the transmission speed of the fast and slow;
3, the port speed limit on the quality of the network cable is higher, otherwise there will be a lot of conflict and broken packet.

6.3.4 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.

In the menu bar, click on the "main menu", "port configuration", "mirror", enter the port mirror configuration interface.



（Figure 6.3.4）

Source port: The group defines a set of monitored ports, which will collect data from these ports in the specified direction, and the mirror port can be one or more.

Destination port: The group defines a port for monitoring, and the device outputs data from the port to the specified direction.

Direction: This parameter specifies the direction of the monitoring port data, a total of "ingress", "egress", "both" three options. Monitor can choose according to their own needs.
Ingress: import data, the message received by the port will be mirrored to the destination port;
Egress: export data, the message sent by the port will be mirrored to the destination port;
Both: all data, while the port to receive and send the message to the mirror.

Configure mirror port steps:
Step 1: select 1, 2, 3, or 4 in the drop-down box of the session ID;
Step 2: select the port by calling the hook in the source port;
Step 3: select the port in the destination port;
Step 4: select ingress, egress, or both in the direction of the drop-down box;
Step 5: click the "add" button.

The function must be shut down in normal use, otherwise all based on port's senior management functions are not available, such as RSTP, IGMP, snooping, mirroring only FCS treatment normal package, cannot handle the wrong data frame.

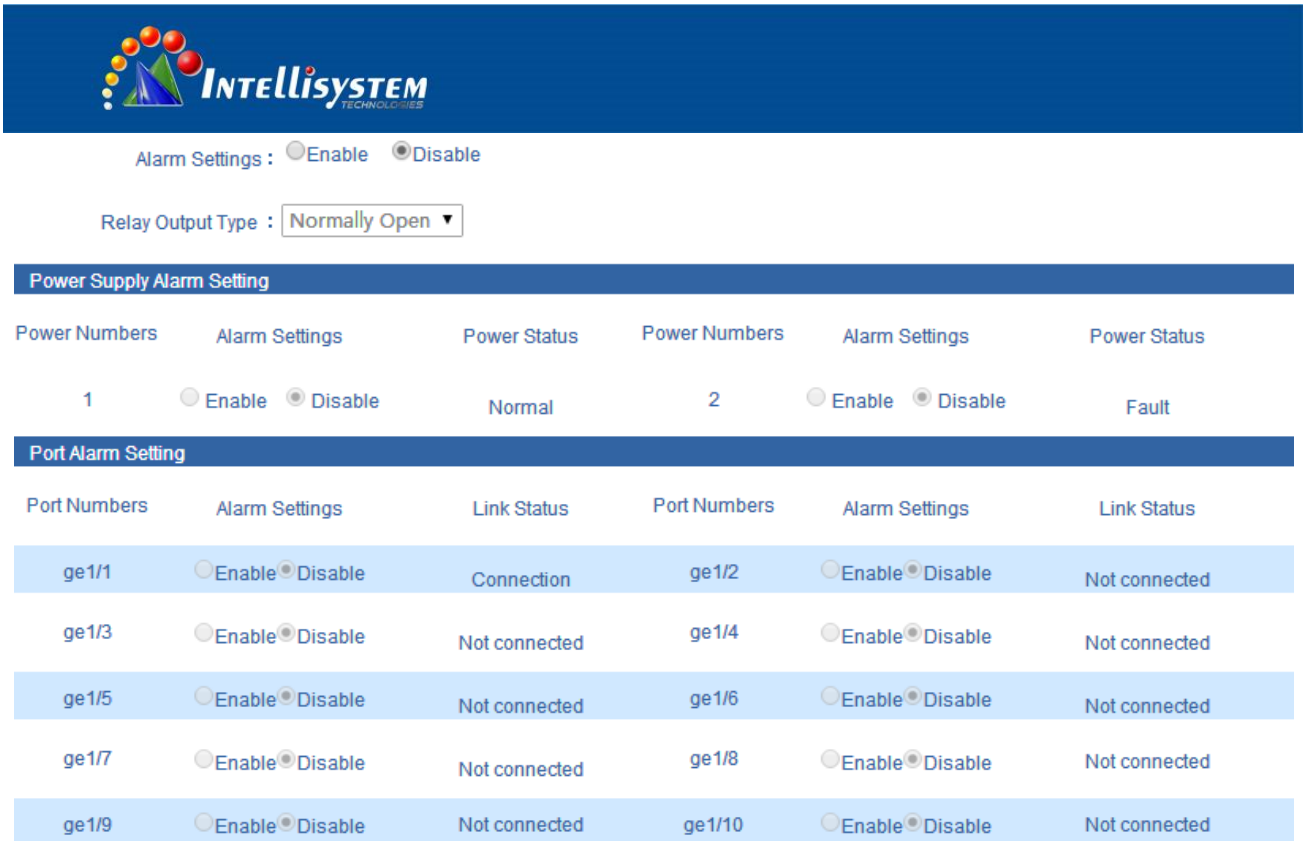
6.3.5 Alarm setting

Alarm is divided into: power supply alarm, port alarm. Its main function is: when the equipment is in abnormal state, can promptly notify the administrator, and quickly repair the equipment status, avoid excessive losses.

Power alarm
Power alarm is the main power outage alarm, enabling power alarm, when the power supply is abnormal (disconnected), the device will output a signal, prompting equipment is not normal.

Port alarm
Alarm port is the main port disconnection alarm, alarm port is enabled, when the port is abnormal (connected or disconnected), the device will output a signal, prompting equipment is not normal.

Relay alarm output type: normally closed / normally open.
If the alarm selection normally closed, when there is an alarm, the alarm light, the relay is in the open state; if the choice is normally open, when there is an alarm, the alarm lamp is not bright, and the relay is in a closed state.



（Figure 6.3.5）

6.3.6 Port channel configuration

Link aggregation, the number of Ethernet physical link bundled into a logical link, to achieve the purpose of increasing the link bandwidth. At the same time, these bundled links can effectively improve the reliability of the link by inter dynamic backup.

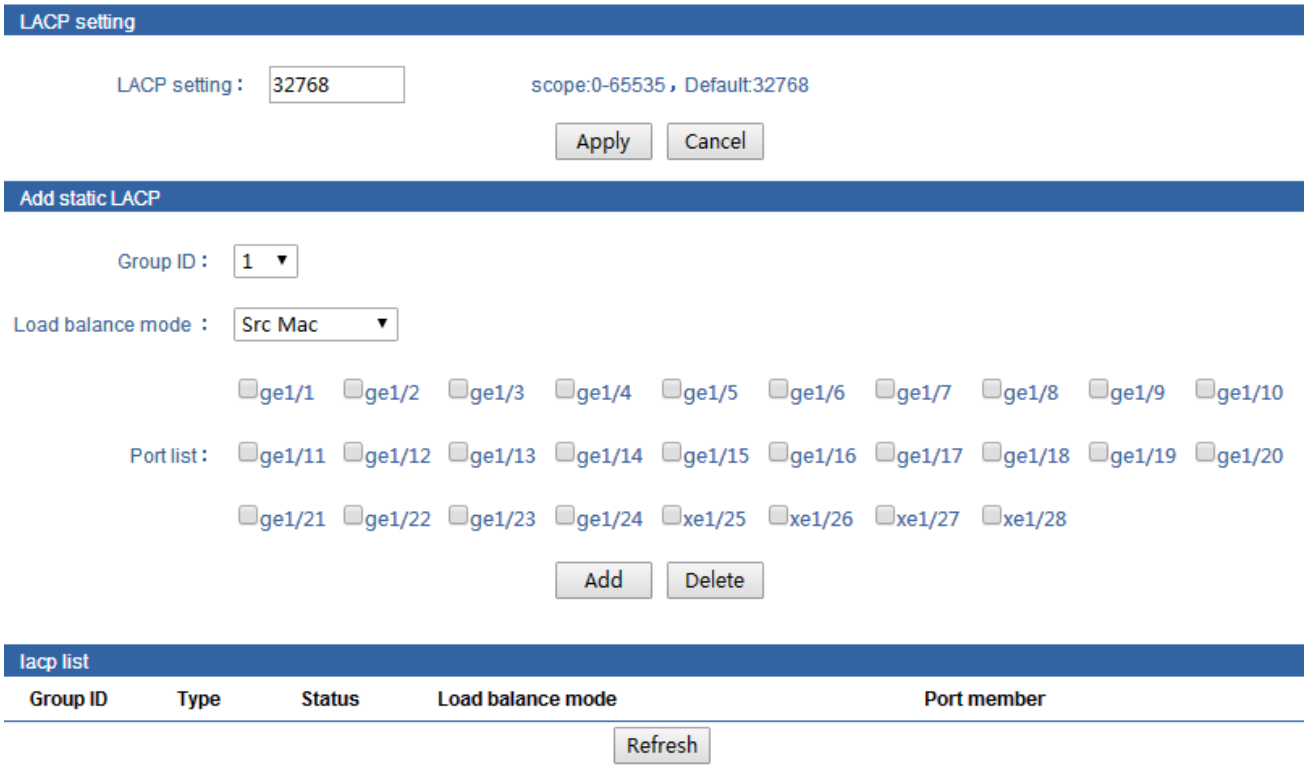
Based on an IEEE802.3ad standard LACP (link aggregation control protocol) protocol is an implementation of dynamic link aggregation protocol, operation equipment of the agreement between the mutual LACPDU (link aggregation control protocol data unit) to make information related to interlink polymerization.

Based on the LACP protocol, the link aggregation can be divided into two modes, static aggregation and dynamic aggregation.

6.3.6.1 Static configuration

Static aggregation is manually configured by the user, and does not allow the system to automatically add or remove ports in the sink group. The aggregation group must contain at least one port. When the aggregation group has only one port, the port can be removed from the aggregation group by deleting the aggregation group.

In the menu bar, click on the "main menu", "port configuration", "port channel configuration", "Static configuration", enter the Static configuration interface.



（Figure 6.3.6.1）

Load balance mode of the aggregation group, there are 3 kinds of:
Src Mac: according to the source MAC address of the message to share the load, when the source MAC address phase at the same time, the message in the same port through, otherwise, the message from different ports through.
Dst Mac: according to the purpose of the message MAC address for load sharing, when the purpose of MAC address at the same time, the message in the same port through, otherwise, the message from different ports through.
Src & Dst Mac: according to the source and destination MAC address for load sharing, when the source and destination MAC address at the same time, the message in the same port through, otherwise, the message from different ports through.

Configuring static aggregation steps:
Step 1: fill in priority in the text box set by LACP;
Step 2: in the group ID drop-down box to select the static convergence group of the group ID, the scope of 1-16;
Step 3: select Dst Mac, Src Mac, or Src & Dst Mac in the drop-down box in the load sharing method;
Step 4: select the port in the list of ports, each group is configured with 8 ports to join together;
Step 5: click the "add" button.

6.3.6.2 LACP configuration

Dynamic aggregation is a kind of system to automatically create or delete the aggregation, dynamic aggregation group of the port to add and delete the LACP agreement is automatically completed. Only the speed and duplex properties are the same, and the ports that are connected to the same device and have

the same basic configuration can be dynamically converged. Even if only one port can also create dynamic convergence, this time for single port aggregation. In dynamic convergence, the LACP protocol of the port is in the state of enable.

In the menu bar, click on the "main menu", "port configuration", " Port channel configuration ", "LACP configuration", enter the LACP configuration interface.

Port Config

PortName	Type	Group ID	Mode	PortPriority
ge1/1	None	1	Active	32768
ge1/2	None	1	Active	32768
ge1/3	None	1	Active	32768
ge1/4	None	1	Active	32768
ge1/5	None	1	Active	32768
ge1/6	None	1	Active	32768
ge1/7	None	1	Active	32768
ge1/8	None	1	Active	32768
ge1/9	None	1	Active	32768
ge1/10	None	1	Active	32768
ge1/11	None	1	Active	32768
ge1/12	None	1	Active	32768

（Figure 6.3.6.2）

Mode refers to the LACP negotiation model, divided into:
Active: Port normal periodic send LACP message;
Passive: Port usually do not send LACP message, once received the LACP message on the end, it will normally send LACP message.

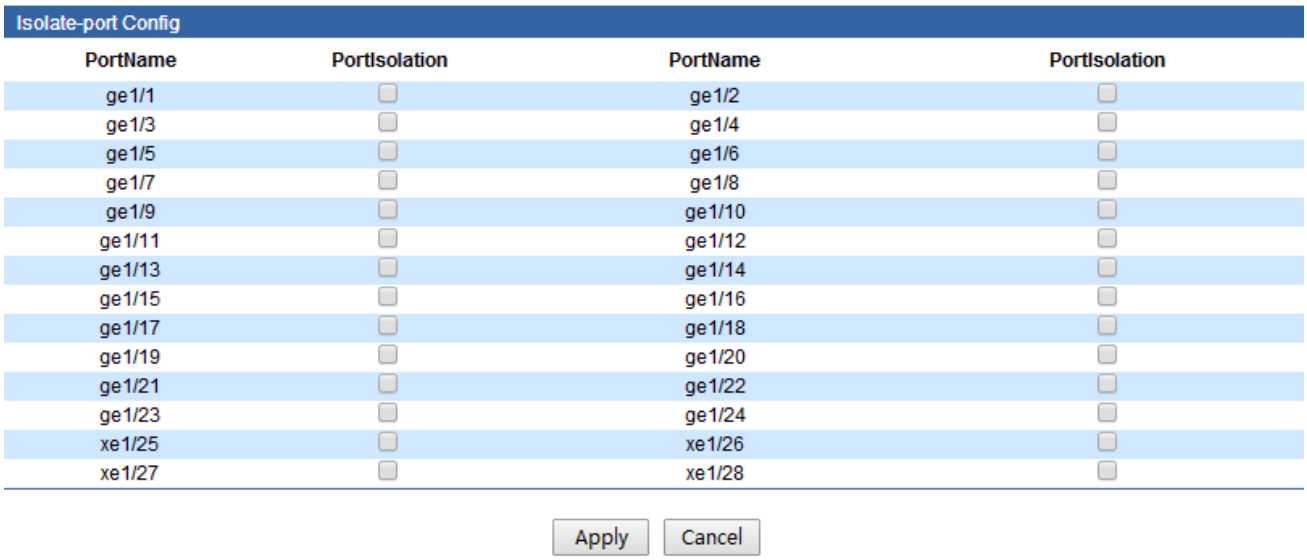
Configure LACP steps:
Step 1: select the dynamic (LACP) in the type of the drop-down box;
Step 2: select Active or Passive in the mode of the drop-down box;
Step 3: fill in priority in the text box with the priority of the port;
Step 4: click the "Apply" button.

6.3.7 Isolate-port configuration

Port isolation is to achieve the message between the two layer of isolation, you can add different ports to different VLAN, but will be a waste of limited VLAN resources. The isolation between the same VLAN port can be realized by using the port isolation characteristics. Users only need to add the port to the isolation group, you can achieve isolation between the two layer of data between the port data. Port isolation provides a more secure and flexible networking solution for the user.

In the menu bar, click on the "main menu", "port configuration", " isolate-port ", enter the port isolation configuration interface.

Intellisystem Technologies S.r.l.
Via Augusto Murri, 1 – 96100 Siracusa - Phone +39 (0)931-1756256 / +39 (0)2-87167549 - Mobile (+39) 335 1880035
em@il: info@intellisystem.it WEB: http://www.intellisystem.it



（Figure 6.3.7）

Configuration port isolation step:

Step 1: check the port isolation in the check box or cancel the check box;

Step 2: click the "Apply" button.

Intellisystem Technologies S.r.l.
Via Augusto Murri, 1 – 96100 Siracusa - Phone +39 (0)931-1756256 / +39 (0)2-87167549 - Mobile (+39) 335 1880035
em@il: info@intellisystem.it WEB: http://www.intellisystem.it

6.3.8 Port statistic

6.3.8.1 Port state

In the menu bar, click on the "main menu", "port configuration", "Port Statistics", "port state", enter the port summary statistics interface.

Port stats

PortName	Packet		Byte		Filter
	Receive	Send	Receive	Send	Receive
ge1/1	2048	4189	282054	2050394	14
ge1/2	0	0	0	0	0
ge1/3	0	0	0	0	0
ge1/4	0	0	0	0	0
ge1/5	0	0	0	0	0
ge1/6	0	0	0	0	0
ge1/7	0	0	0	0	0
ge1/8	0	0	0	0	0
ge1/9	0	0	0	0	0
ge1/10	0	0	0	0	0
ge1/11	0	0	0	0	0
ge1/12	0	0	0	0	0
ge1/13	2659	1262	542893	192591	9
ge1/14	0	0	0	0	0
ge1/15	0	0	0	0	0
ge1/16	0	0	0	0	0
ge1/17	0	0	0	0	0
ge1/18	0	0	0	0	0
ge1/19	0	0	0	0	0
ge1/20	0	0	0	0	0
ge1/21	0	0	0	0	0
ge1/22	0	0	0	0	0
ge1/23	0	0	0	0	0
ge1/24	0	0	0	0	0
xe1/25	0	0	0	0	0
xe1/26	0	0	0	0	0
xe1/27	0	0	0	0	0
xe1/28	0	0	0	0	0

Clear Refresh

（Figure 6.3.8.1）

6.3.8.2 Detail port state

In the menu bar, click the "main menu", "port configuration", "Port Statistics", "Detail port state ", enter the port with statistics interface. In the interface, we can view to every port of different kinds of packet reception and transmission.

Intellisystem Technologies S.r.l.
Via Augusto Murri, 1 – 96100 Siracusa - Phone +39 (0)931-1756256 / +39 (0)2-87167549 - Mobile (+39) 335 1880035
em@il: info@intellisystem.it WEB: http://www.intellisystem.it

Detail port stats

Port: ge1/1 ▼ Refresh Clear

ReceiveTotal		SendTotal	
ReceivePacket num	2102	SendPacket num	4368
ReceiveByte num	287792	SendByte num	2154076
ReceiveUnicast num	1801	SendUnicast num	2473
ReceiveMulticast num	21	SendMulticast num	1312
ReceiveBroadcast num	280	SendBroadcast num	583
ReceivePause frame	0	SendPause frame	0
ReceiveMessage size classification statistics		**SendMessage size classification statistics**	
Receive64Byte size packet num	940	Send64Byte size packet num	774
Receive65-127Byte size packet num	686	Send65-127Byte size packet num	1579
Receive128-255Byte size packet num	96	Send128-255Byte size packet num	281
Receive256-511Byte size packet num	327	Send256-511Byte size packet num	525
Receive512-1023Byte size packet num	50	Send512-1023Byte size packet num	115
Receive1024-1518Byte size packet num	3	Send1024-1518Byte size packet num	1094
Receive1519-2047Byte size packet num	0	Send1519-2047Byte size packet num	0
Receive2048-4095Byte size packet num	0	Send2048-4095Byte size packet num	0
Receive4096-9216Byte size packet num	0	Send4096-9216Byte size packet num	0

（Figure 6.3.8.2）

6.4 Layer 2 Configuration

6.4.1 VLAN Configuration

VLAN (virtual local area network), VLAN is a LAN (LAN) equipment from the logical partition (not physically divided into one segment (or smaller LAN), to achieve the data exchange technology of virtual work groups (unit). The benefits of VLAN are mainly:

1, Port separation. Even on the same switch, the port on the different VLAN is not able to communicate. Such a physical switch can be used as a logical switch.

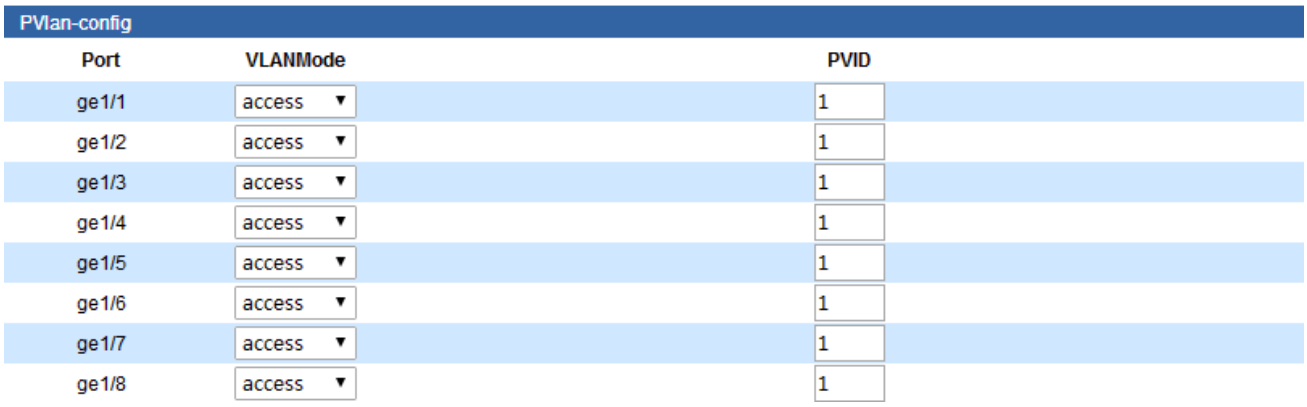
2, Network security. VLAN cannot be directly communication, to eliminate the security of broadcast information.

3, Flexible management. Change users belong to the network does not have to change the port and connection, only to change the software configuration on it.

That is in the same VLAN can communicate with each other, in a different VLAN cannot communicate with each other. A VLAN with VLAN ID to identify, with the same VLAN ID is the same VLAN.

6.4.1.1 PVlan configuration

Port VLAN mode can be configured (access, trunk, translate), VLAN ID: PVID.



（Figure 6.4.1.1）

Access: port can only belong to 1 VLAN, generally used to connect the user equipment. All of the default ports belong to the access port;

Trunk: port can belong to more than one VLAN, you can receive and send multiple VLAN packets, generally used for network equipment connection;

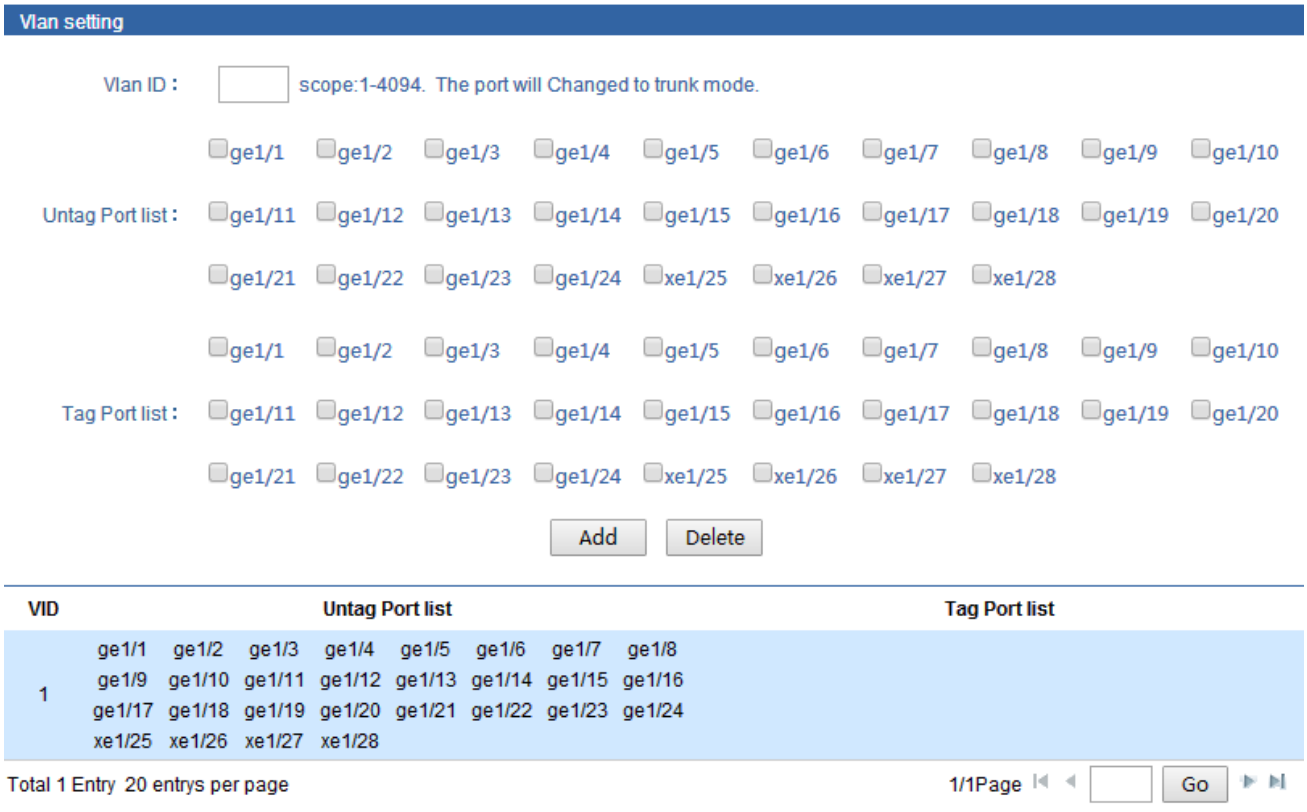
Step 1: select access, trunk, or translate in the drop-down box in the VLAN mode;

Step 2: fill in the PVID text box with the port default VLAN ID;

Step 3: click the "Apply" button.

6.4.1.2 Trunk configuration

In the menu bar, click on the "main menu", "two layer configuration", "VLAN configuration", "Trunk configuration", enter the Trunk configuration interface, in the interface, you can add and delete vlan.



（Figure 6.4.1.2）

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

The port type of Access, Translate port can only be Untag; the port type of Trunk port can be either Untag or Tag.

Trunk configuration steps:

Step 1: fill VID in the text box in the Vlan ID;

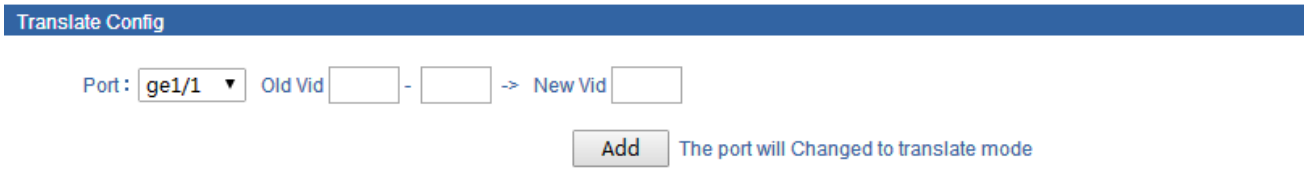
Step 2: select the unTag port list in the check box to select the need to join the VLAN port;

Step 3: select the Tag port list in the check box to select the need to join the VLAN port;

Step 4: click the "add" button.

6.4.1.3 Translate configuration

In the menu bar, click on the "main menu", "two layer configuration", "VLAN configuration", "Translate configuration", enter the Translate configuration interface, in the interface, you can add and delete Translate.



（Figure 6.4.1.3）

Translate configuration steps:

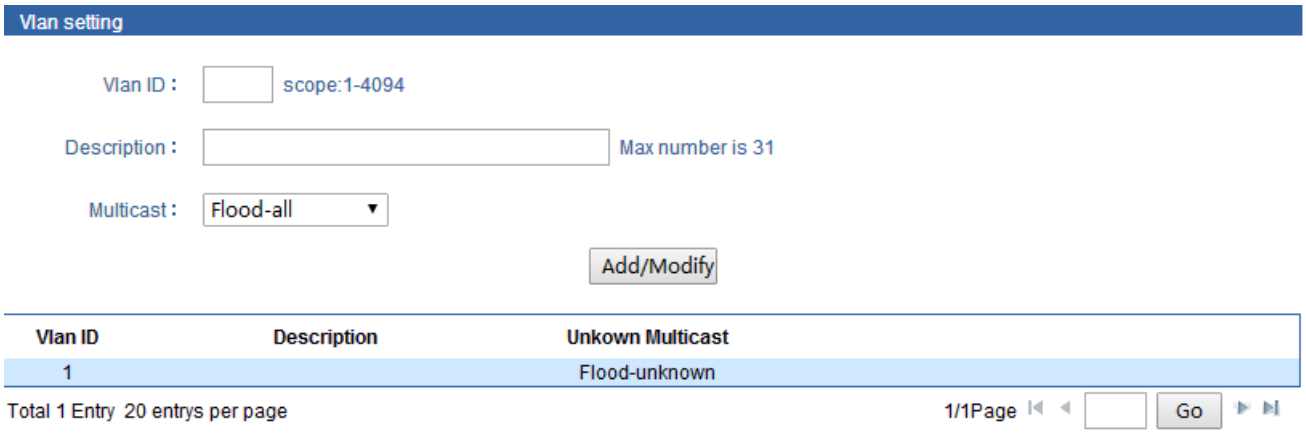
Step 1: select the port in the port's drop-down box;

Step 2: fill Vid in the two text boxes in old Vid;

Step 3: fill Vid in the two text boxes in New Vid;

Step 4: click the "add" button.

6.4.1.4 VLAN configuration



（Figure 6.4.1.4）

Flood-all: flooding all multicast packets

Flood-unknown: flooding unknown multicast package

Drop: drop multicast packets

Vlan configuration steps:

Step 1: fill Vid in the text box in the Vlan ID;

Step 2: fill in the description of the text box to fill in the description of the vlan;

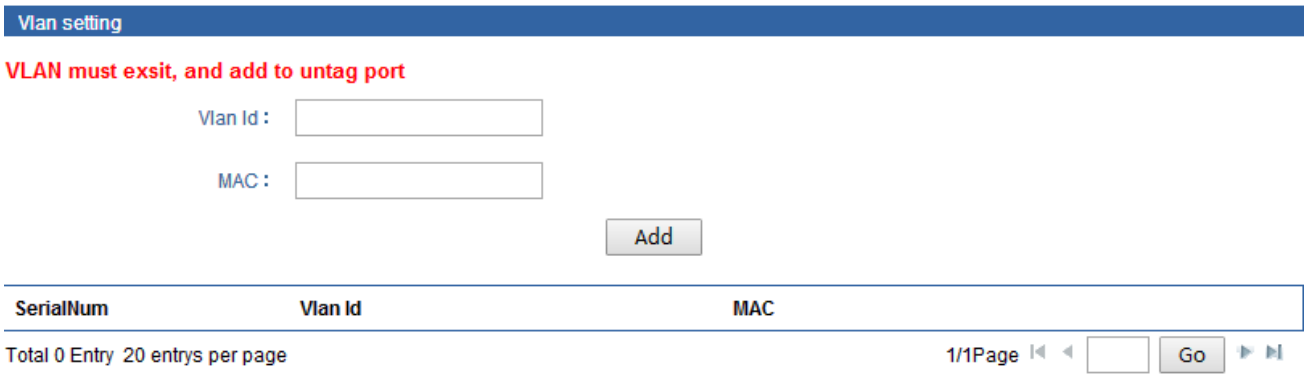
Step 3: select Flood-all, Flood-unknown, or drop in the multicast drop - down box;

Step 4: click the "add / modify" button.

6.4.1.5 MAC-VLAN

Based on MAC partition VLAN is another method of VLAN. It defines the VLAN member in accordance with the source MAC address of the message, and sends the specified message to the Tag of the VLAN. This feature is usually combined with security (such as 802.1X) technology to achieve terminal security, flexible access.

In the menu bar, click on the "main menu", "layer 2 configuration", "mac-vlan", enter the mac-vlan configuration interface.



（Figure 6.4.1.5）

Mac-vlan configuration steps:

Step 1: fill Vid in the text box in the Vlan Id;

Step 2: fill in the MAC address in the MAC text box;

Step 3: click the "add" button.

6.4.1.6 Protocol-vlan

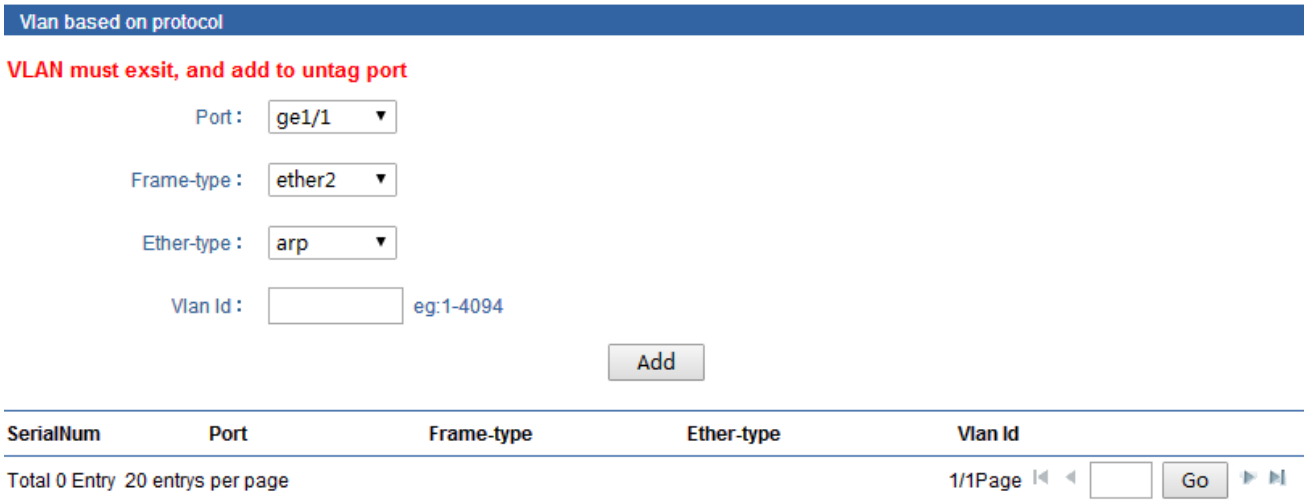
Protocol based VLAN is a protocol that is based on the protocol (family) of the message received by the port, and the package format to distribute the message to the VLAN-ID.

Protocol type + package format, also known as the protocol template, a protocol VLAN can be bound to a number of protocols template, the different protocol template with the protocol-index (protocol index) to distinguish. Therefore, a protocol template can be uniquely identified by "protocol vlan-id + protocol-index". And then through the command line "vlan-id + protocol-index" and port binding. In this way, it will do the following processing for receiving the Untagged message from the port (without carrying the VLAN tag):

If the message is carried by the protocol type and encapsulation format and the "protocol vlan-id + protocol-index" identification of the template match, then it is the agreement vlan-id.

If the message is carried by the protocol type and encapsulation format and the "protocol vlan-id + protocol-index" template does not match the template, then it is the default VLAN-ID. For the port receives the tagged message (carry VLAN tagged message), processing mode and port based VLAN: if port to allow the passage of carrying the message of the VLAN tag, normal forwarding; if not allowed, this feature is mainly used to bind the network to provide the service type and VLAN, convenient management and maintenance.

In the menu bar, click on the "main menu", "two layer configuration", "protocol-vlan", enter the protocol-vlan configuration interface.



（Figure 6.4.1.6）

Protocol-vlan configuration steps:

Step 1: select the port in the port's drop-down box;

Step 2: select ether2, 802.3 (SNAP), LLC, or snap-priv in the frame type drop-down box;

Step 3: select the ARP, IP, IPv6, 802.1Q, or 802.1x (only if the frame type is selected as ether2, the item can be selected) in the drop - down box on the Ethernet type;

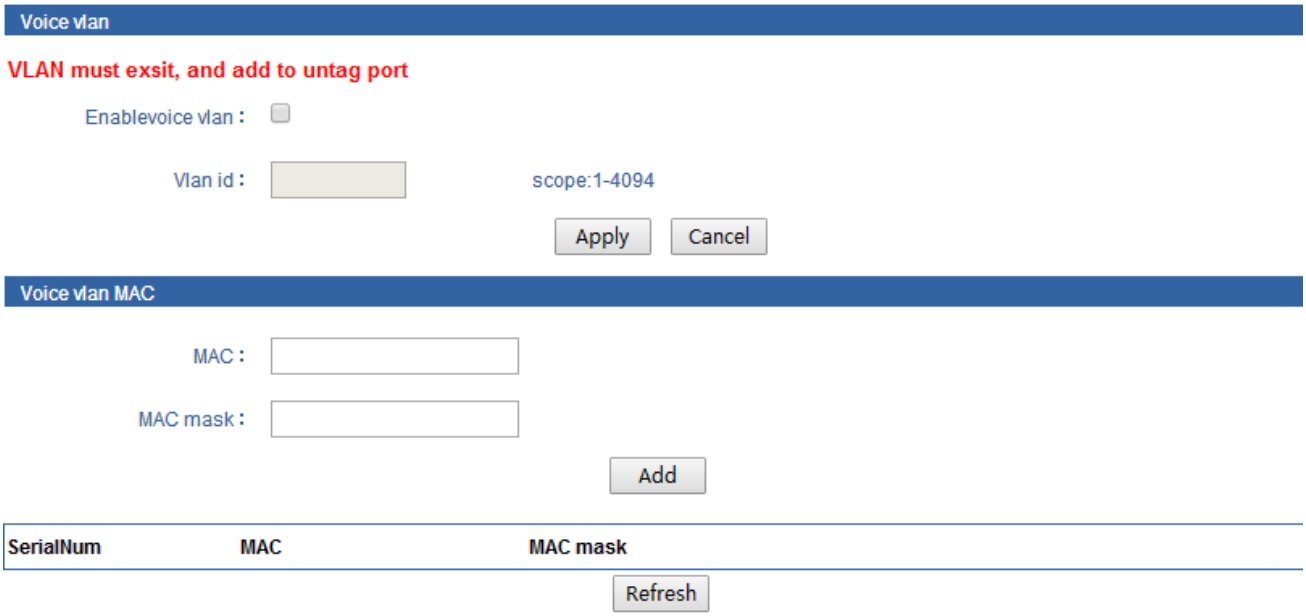
Step 4: fill Vid in the text box in the Vlan Id;

Step 5: click the "add" button.

6.4.1.7 Voice-vlan

VLAN Voice is for the user's voice data streams and specialized division of the VLAN. By dividing the voice VLAN and the connection port on a voice equipment to join the voice VLAN, the system automatically for voice message modified QoS (quality of service, QoS (quality of service) parameters, to improve the voice data packet priority, ensure voice quality.

The device can judge whether the data stream is the voice data stream according to the source MAC address field in the data message of the access port. The source MAC address is in line with the system set of voice equipment OUI (Unique Identifier Organizationally, the global unified identifier) address of the message is considered to be the voice data stream.



（Figure 6.4.1.7）

Voice-vlan configuration steps:

Step 1: enable voice-vlan;

Step 2: fill in Vlan ID, click set;

Step 3: fill in the MAC address and the MAC mask

Step 4: click the "add" button.

6.4.2 MAC configuration

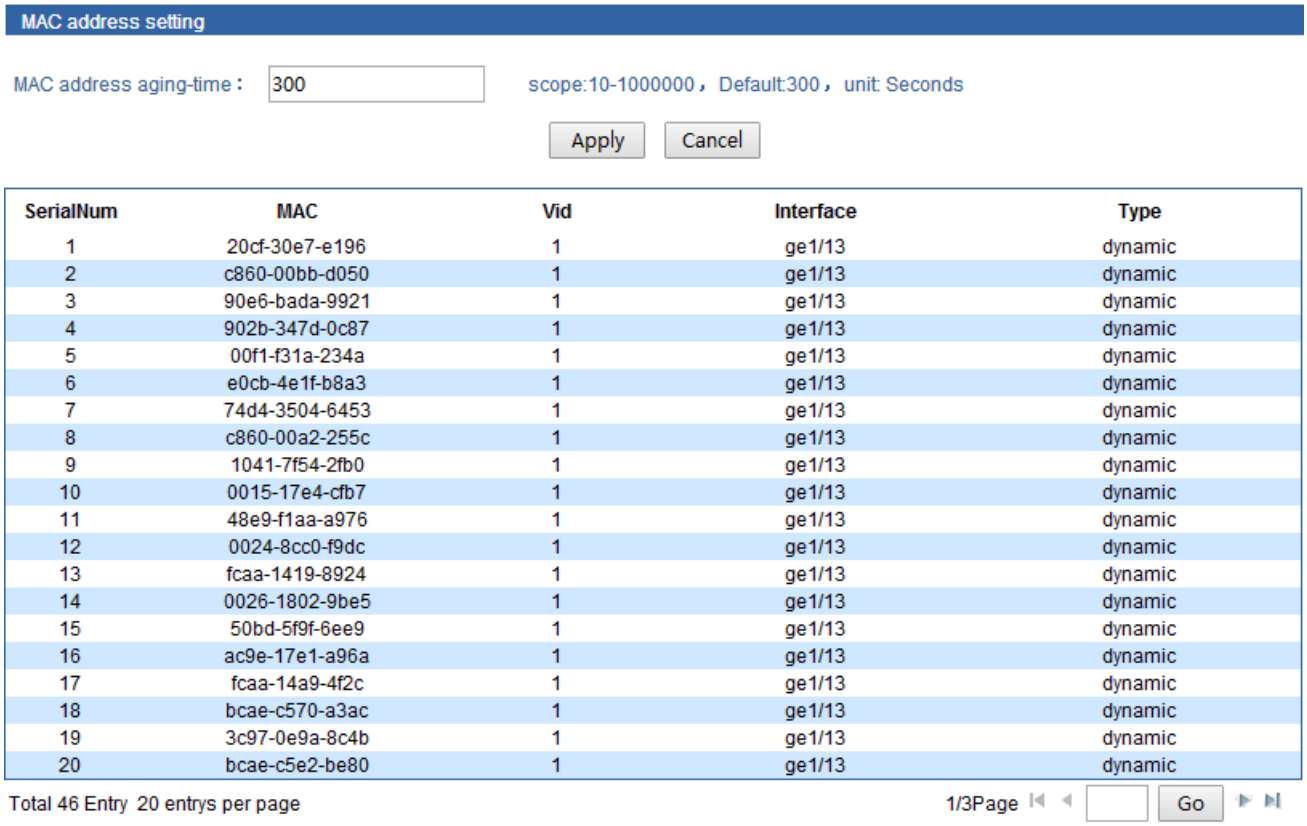
MAC (Access Control Media) address is the network equipment of the hardware logo, the switch according to the MAC address of the packet forwarding. MAC address is unique, which ensures the correct forwarding of packets. Each switch is maintained with a MAC address table. In this table, the MAC address and the port of the switch are corresponding. When the switch receives a data frame, the data frame is

determined according to the MAC address table, and the data frame is filtered or forwarded to the corresponding port of the switch. MAC address table is the basis and premise for the switch to achieve fast forwarding.

6.4.2.1 MAC configuration

Each port of the switch has the function of automatically learning the address, and the source address (the source MAC address and the switch port number) of the transmitting and receiving frame of the port will be stored in the address table. Aging time is a parameter that affects the learning process of the switch. The default is 300 seconds. From an address record to join the address table since the beginning of time, if in the aging time within the port does not receive the source address for the MAC address of the frame, then these addresses will from a dynamic forwarding address table (from the source MAC address, destination MAC addresses and their corresponding switch port number) is removed.

In the menu bar, click "main menu", " layer 2 configuration", "MAC configuration", "MAC configuration" into MAC configuration interface, the interface can be set dynamic MAC address aging time and view the MAC address of the static and dynamic information.



（Figure 6.4.2.1）

MAC aging time configuration step:

Step 1: fill in time in the text box of the aging time of MAC;

Step 2: click the "Settings" button.

The address of the device is based on the MAC address of the switch, so the VLAN value of all the MAC values are 0;

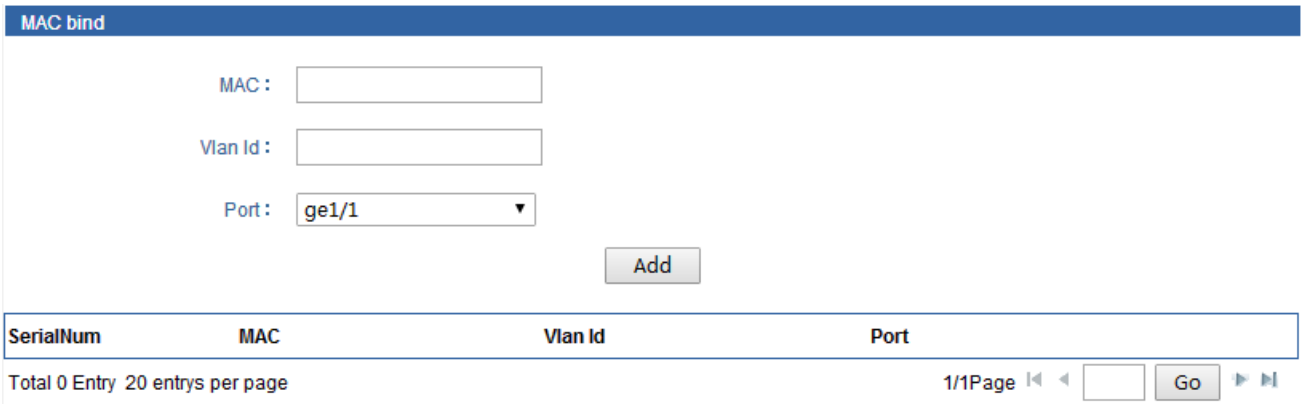
The permanent static address is configured in the static MAC address port list, and the corresponding table entry is required when the port changes;

The multicast address table is displayed in the IGMP listener table entry;

The aging time of the MAC address is 300 seconds. After the port is disconnected, the upper level program clears all the corresponding port list items.

6.4.2.2 Static MAC

Static MAC manually set by the user, not aging. In the menu bar in order to click on the "main menu", "layer 2 configuration", "MAC configuration", "static MAC" into the static MAC configuration interface, in the interface, you can source MAC address binding.



（Figure 6.4.2.2）

MAC address binding step:

Step 1: fill in the MAC address in the MAC text box;

Step 2: fill in Vid on the text box for the Vlan Id;

Step 3: select the port in the port's drop-down box;

Step 4: click the "add" button.

This function is a kind of security mechanism, please carefully confirm the settings, otherwise please caution;

Please do not use the multicast address as the input address;

Please do not enter the reserved MAC address, such as the MAC address of the machine.

6.4.3 Spanning-tree

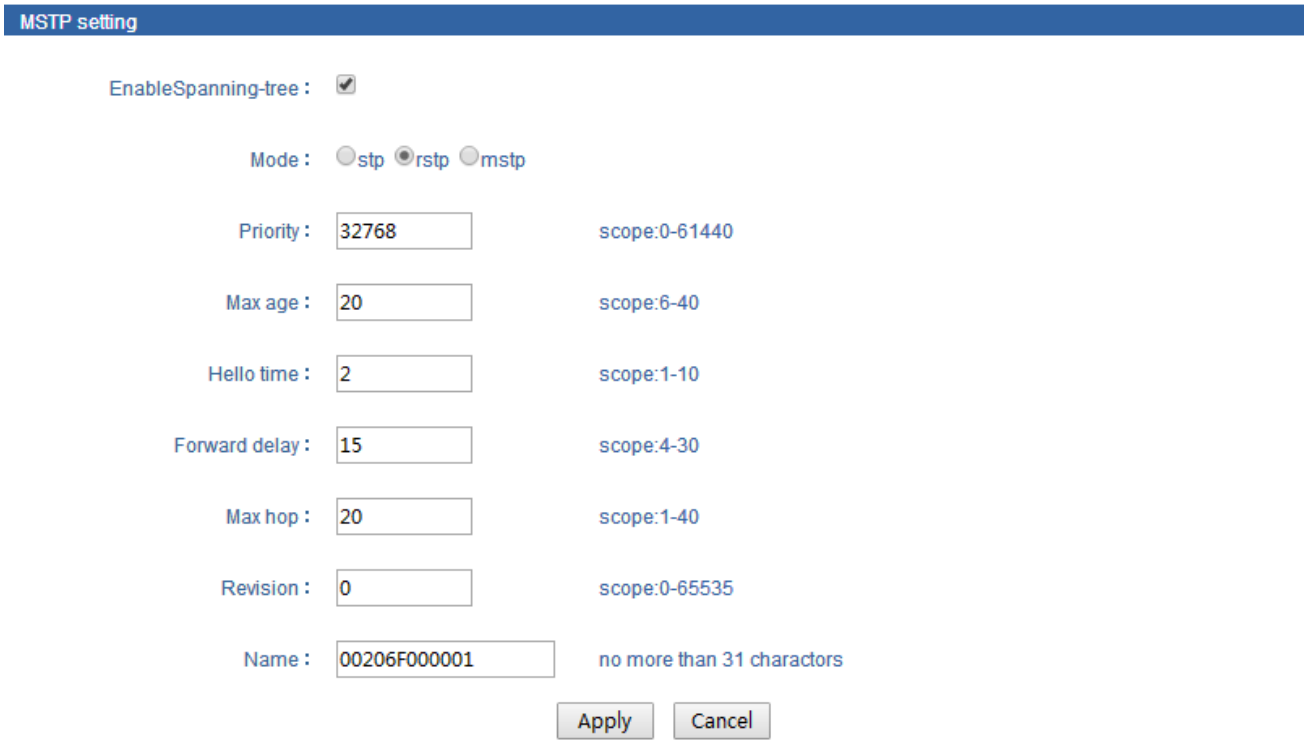
Spanning tree protocol is a two-level management protocol by selectively blocking network redundancy link to achieve the purpose of eliminating network loop on the second floor, and at the same time it has a

backup link function. Here are three kinds of spanning tree protocol: STP (Spanning Tree Protocol), RSTP (Rapid Spanning Tree Protocol), and MSTP (Multiple Spanning Tree Protocol).

There are two main functions of the spanning tree protocol: one is to use the spanning tree algorithm, in the Ethernet network, to create a port for the root of a switch to generate a tree to avoid loop. Two is in the Ethernet topology changes, through the spanning tree protocol to achieve the purpose of convergence protection. Compared to the STP, RSTP in the network structure changes, the faster convergence of the network; MSTP compatible with STP and RSTP, and better than STP and RSTP. It can not only fast convergence, but also make the traffic flow along the different VLAN distribution, so as to provide a better load sharing mechanism for redundant links.

6.4.3.1 Bridge setting

In the menu bar, click the "main menu", "layer 2 configuration", "spanning tree" and " bridge setting", into the bridge configuration interface, the interface can be spanning tree configuration parameters.



（Figure 6.4.3.1）

Max age: Configuring the maximum lifetime of messages in the device

Hello time: Configuration message sending period

Forward delay: Delay time for port state transition

Max hop: configuration of the maximum number of hops in the MST domain

Revision: MSTP configuration revision level

Name: configure domain name in MST domain

Bridge configuration steps:

Step 1: check the Spanning-tree in the check box;

Step 2: select STP, RSTP, or MSTP in the mode selection;

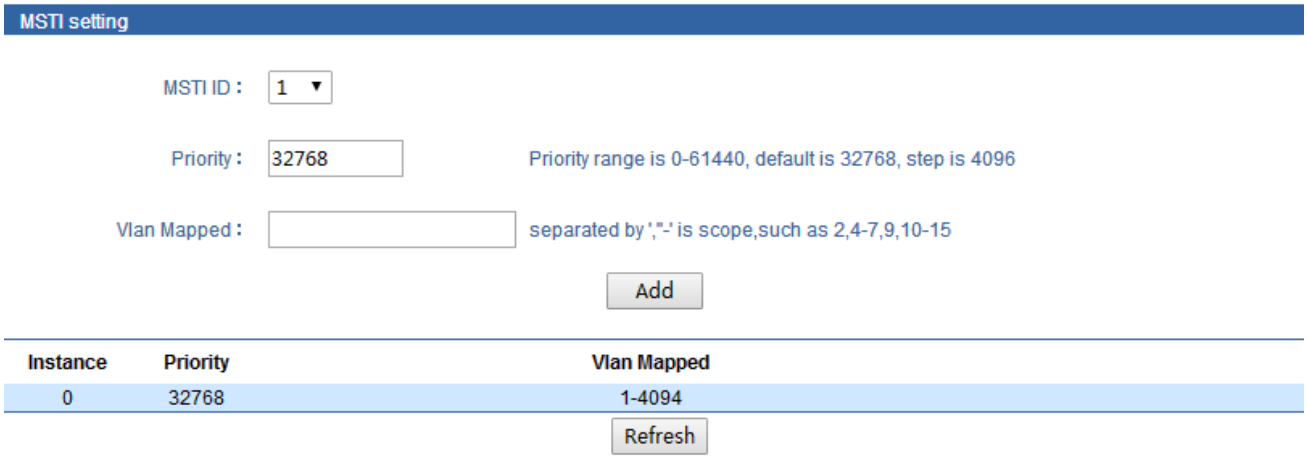
Step 3: the priority of the text box to fill in the value of the priority;

Step 4: fill in the values of Max age, Hello time, Forward delay, Max hop, Revision, and Name;

Step 5: click the "Apply" button.

6.4.3.2 Instance setting

In the menu bar, click on the "main menu", "layer 2 configuration", "spanning tree ", "instance setting" into the instance configuration interface, the interface can be configured with VLAN mapping.



（Figure 6.4.3.2）

The instance configuration steps

Step 1: select an instance in the ID MSTI drop-down box ID;

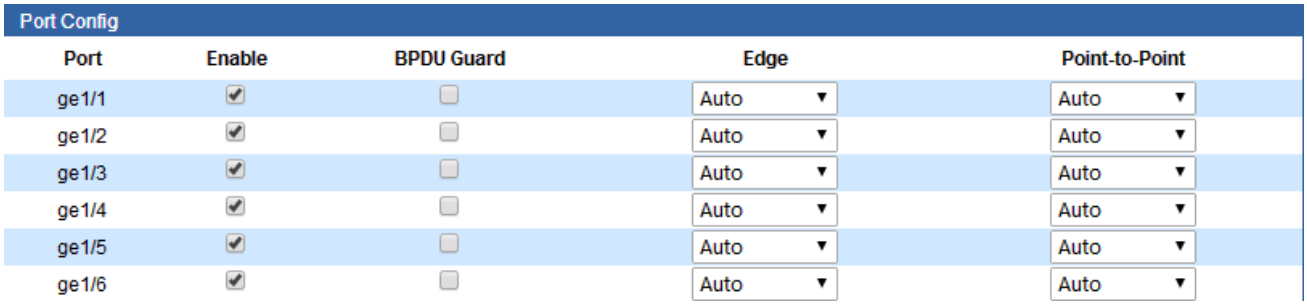
Step 2: fill priority value in the priority text box;

Step 3: fill in Vid on the text box for the Vlan Mapped;

Step 4: click the "add" button.

6.4.3.3 Bridge port

In the menu bar, click "main menu", "layer 2 configuration", "spanning tree", "bridge port" to enter the bridge port configuration interface, the interface can be enabled ports in spanning tree, configuration port type, link type and BPDU protection function.



（Figure 6.4.3.3）

Configuration item	meaning
BPDU Guard	Configuration BPDU protection function
Edge	Configuration port type: Automatic: automatic detection system Force True: Edge port Force False: Non edge port
Point-to-Point	Configure port link type: Automatic: automatic detection system Force True: Point to point link Force False: Non point to point link

Bridge port configuration steps:

Step 1: check the port to participate in the spanning tree in the enable check box;

Step 2: check the BPDU Guard check box to enable port BPDU protection function;

Step 3: select automatic, Force True or Force False in the Edge drop-down box;

Step 4: select automatic, Force True or Force False in the Point-to-Point drop-down box;

Step 5: click the "Apply" button.

6.4.3.4 Instance port configuration

In the menu bar in order to click on the "main menu", "layer 2 configuration", "spanning tree ", "instance port configuration" into the instance port configuration interface, the interface can configure the port priority and cost.

Inst Port Config

MSTID: 0 Refresh

Port	Enable	Instance	Priority	AdminCost	Cost	Role	Status
ge1/1	Yes	0	128	0	200000	Desg	forw
ge1/2	Yes	0	128	0	200000000	Disa	disc
ge1/3	Yes	0	128	0	200000000	Disa	disc
ge1/4	Yes	0	128	0	200000000	Disa	disc
ge1/5	Yes	0	128	0	200000000	Disa	disc
ge1/6	Yes	0	128	0	200000000	Disa	disc
ge1/7	Yes	0	128	0	200000000	Disa	disc
ge1/8	Yes	0	128	0	200000000	Disa	disc
ge1/9	Yes	0	128	0	200000000	Disa	disc
ge1/10	Yes	0	128	0	200000000	Disa	disc
ge1/11	Yes	0	128	0	200000000	Disa	disc
ge1/12	Yes	0	128	0	200000000	Disa	disc
ge1/13	Yes	0	128	0	200000	Desg	forw
ge1/14	Yes	0	128	0	200000000	Disa	disc

（Figure 6.4.3.4）

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 receives 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

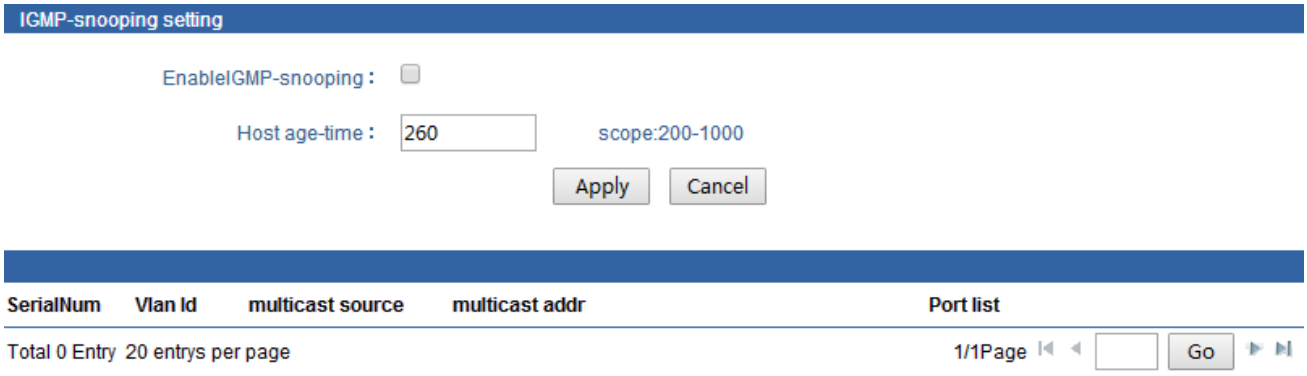
6.4.4 IGMP-Snooping

6.4.4.1 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.



（Figure 6.4.4.1）

IGMP- Snooping configuration steps:

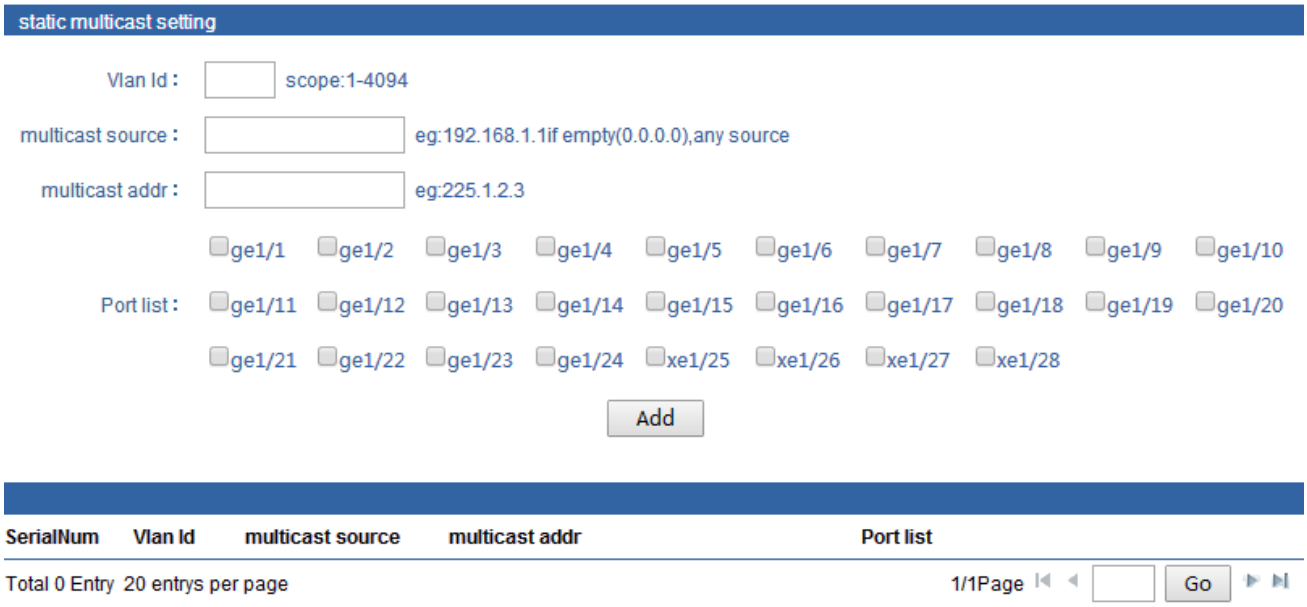
Step 1: in the IGMP- Snooping configuration to enable the check box to enable IGMP;

Step 2: in the host aging time of the text box to fill in the aging time;

Step 3: click the "Apply" button.

6.4.4.2 Static Multicast

The main function of the static multicast: some ports will be added to a multicast group, when data is sent to the multicast address, the data can be received.



（Figure 6.4.4.2）

Static multicast configuration:

Step 1: fill in Vid on the text box for the Vlan Id;

Step 2: in the multicast source of the text box to fill in the multicast source IP address;

Step 3: in the multicast address of the text box to fill in the multicast IP address;
Step 4: select the port in the port checkbox in the list;
Step 5: click the "add" button.

6.4.5 SW-Ring

SW-Ring technology provides auto-recovery and reconnection mechanism for broken network. When network is broken, it has link redundancy and self-recovery capability.

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

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

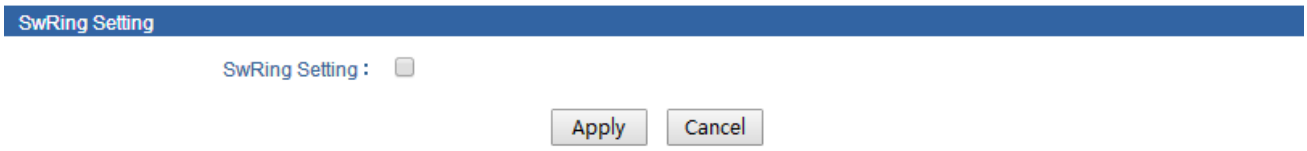
Self-developed patented technology for **SW-Ring** network can realize the intelligent redundancy for industrial Ethernet switch, which can make you easily and conveniently establish redundant Ethernet, and can facilitate the quick recovery of any network section of automatic system disconnected from the network.

The switch supports maximum 4 ring groups. Each group set up 2 ports as Ring Port and a port cannot belong to several rings.

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

6.4.5.1 Global configuration

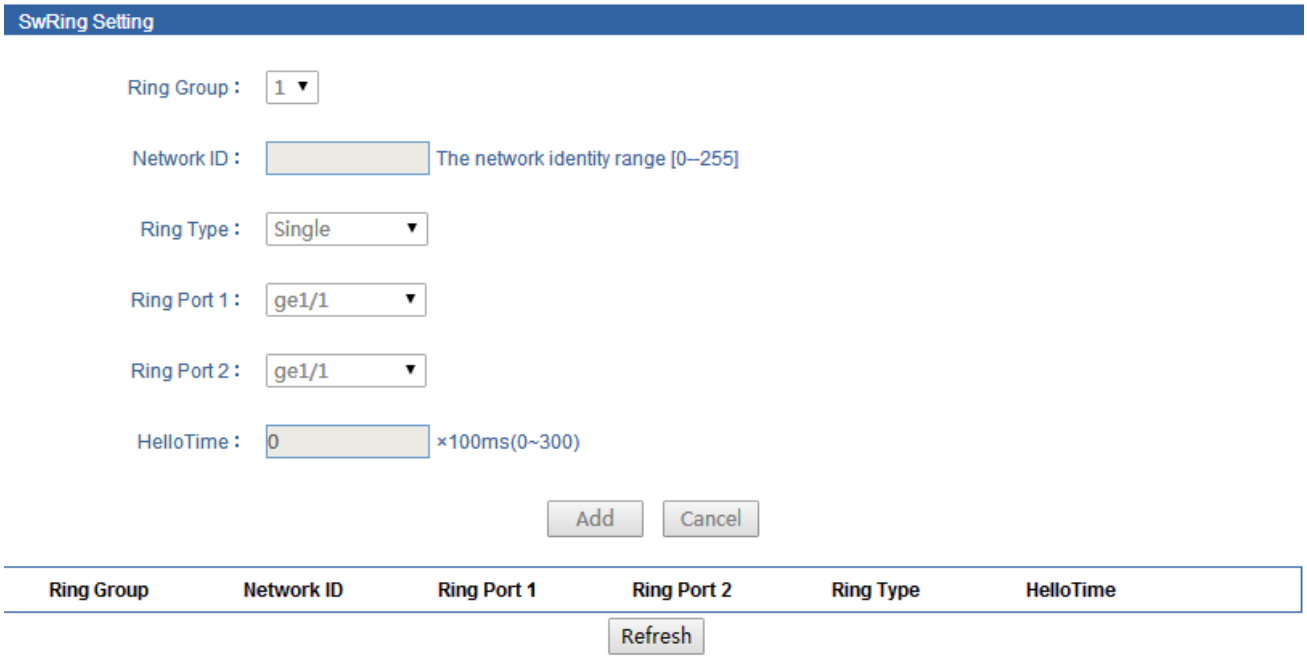
In the menu bar in order to click on the "main menu", "layer 2 configuration", "Sw-Ring configuration", "global configuration" into the global configuration of the ring network interface, the interface can enable / disable the ring network.



（Figure 6.4.5.1）

6.4.5.2 Node configuration

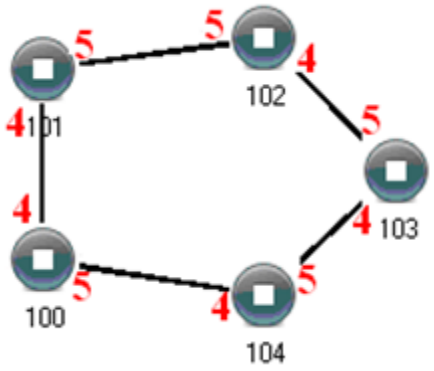
In the menu bar, click "main menu", " layer 2 configuration", "Sw-Ring configuration" and "node configuration" into the node configuration interface and the interface can add and remove ring group, only when enabled Sw-Ring, can of node configuration.



（Figure 6.4.5.2）

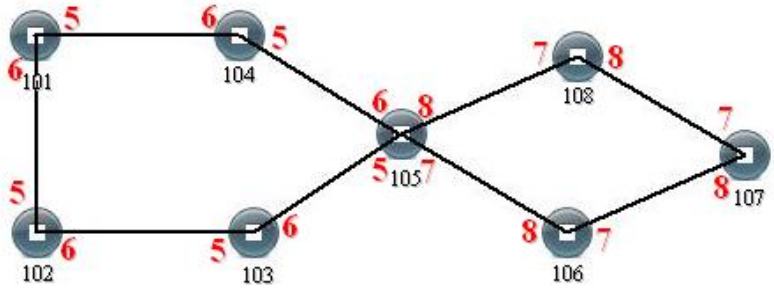
Single ring configuration

Enable ring group 1(or other groups), configure port 4 and port 5 are ring port, ring type is Single. Configure other switches the same as this switch, reboot these switches, then connect port 4 and port 5 through network cable, use our management software to search the switches, the topology of the ring network is as below figure.



Dual ring configuration

Double ring as shown below figure, we can send dual ring is 2 rings combining, the point is number 105 switch.



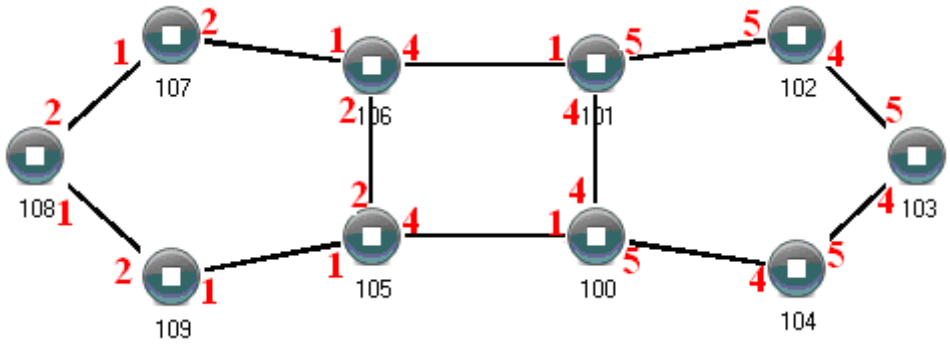
Operating method:

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 our management software to search the switches, the topology of the ring network.

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

Coupling Configuration

Coupling ring structure figure as below:



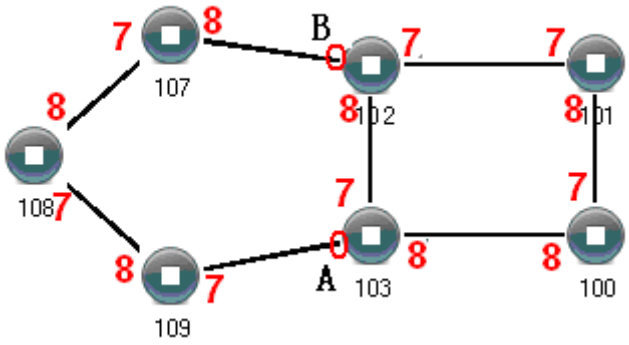
Operating method:

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.
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.
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 figure, 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.

Chain Configuration

Chain ring structure figure as below



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.
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.

Node configuration steps:

Step 1: select 1, 2, 3 or 4 in the drop-down box in the ring network group;

Step 2: in the ring network identification of the text box to fill in the network identification;

Step 3: select Single, Couple, Chain, or Dual homing in the drop-down box of the ring network type;

Step 4: select the port in the drop - down box on the ring network port 1;

Step 5: in the ring network port 2 in the drop-down box to select the port, and cannot be the same as the ring network port 1;

Step 6: fill in the value of the Hello Time in the Hello Time text box;

Step 7: click the "add" button.

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.

6.4.6 GMRP configuration

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.

6.4.6.1 GMRP global configuration

In the menu bar, click on the "main menu", "layer 2 configuration", "GMRP configuration", "GMRP global configuration" to enter the GMRP global configuration interface, the interface can enable / disable GMRP.

（Figure 6.4.6.1）

6.4.6.2 GMRP port configuration

In the menu bar in order to click on the "main menu", "layer 2 configuration", "GMRP configuration", "GMRP port configuration" into the GMRP port configuration interface, the interface can be configured GMRP port of the relevant parameters.

GMRP Port Config

PortName	Enable	ForwardAll	JoinTime	LeaveTime	LeaveAllTime	Registration
ge1/1	☐	☐	20	60	1000	Normal
ge1/2	☐	☐	20	60	1000	Normal
ge1/3	☐	☐	20	60	1000	Normal
ge1/4	☐	☐	20	60	1000	Normal
ge1/5	☐	☐	20	60	1000	Normal
ge1/6	☐	☐	20	60	1000	Normal
ge1/7	☐	☐	20	60	1000	Normal
ge1/8	☐	☐	20	60	1000	Normal
ge1/9	☐	☐	20	60	1000	Normal
ge1/10	☐	☐	20	60	1000	Normal
ge1/11	☐	☐	20	60	1000	Normal
ge1/12	☐	☐	20	60	1000	Normal
ge1/13	☐	☐	20	60	1000	Normal
ge1/14	☐	☐	20	60	1000	Normal
ge1/15	☐	☐	20	60	1000	Normal

（Figure 6.4.6.2）

Configuration item	meaning
ForwardAll	forward
Join Time	In the first time sent the Join message did not get a reply, the second time will send Join messages. Time interval between two Join messages.
Leave Time	When the switch wants other switches to write off their own attribute information, the Leave message will be sent to the outside.
LeaveAllTime	When the switch is started, the LeaveAll timer will be started at the same time, and the LeaveAll message will be sent out after the time out.
Registration	register

GMRP port configuration step:
Step 1: check the port to enable port GMRP on the enabled check box;
Step 2: check the ForwardAll's check box to enable ForwardAll;
Step 3: fill in the Join time in the text box of the Join time;
Step 4: fill in the Leave time in the text box of the Leave time;
Step 5: fill in the LeaveAll time in the text box of the LeaveAll time;
Step 6: select Normal, Fixed, or Forbidden in the Registration drop-down box.
Step 7: click the "Settings" button.

6.4.6.3 GMRP group

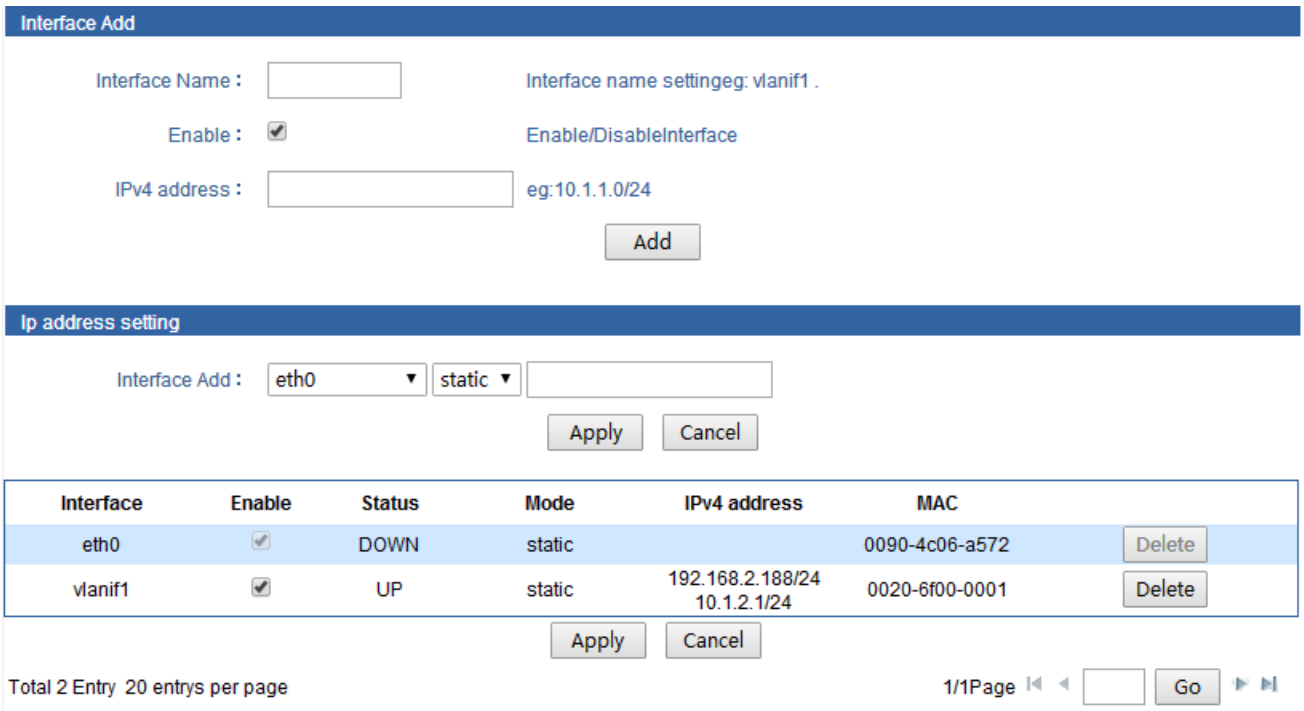
In the menu bar in order to click on the "main menu", "layer 2 configuration", "GMRP configuration", "GMRP group" access to view the GMRP group interface, the interface can view the information of the GMRP group.

（Figure 6.4.6.2）

6.5 Layer 3 Configuration

6.5.1 Interface configuration

Interface settings are mainly set the interface IPV4 address of the device. The configuration of the interface only supports manual configuration and does not support automatic acquisition (DHCP). Users through the choice of interface, fill in the IPV4 address can be. IPV6 address settings can be achieved through the command line.



（Figure 6.5.1）

IPv4 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.

IPv6 address

IPv6 (Internet Protocol version 6) is a network layer protocol of the second generation of standard protocol, also known as IPng (IP next generation), it is the IETF (Internet Engineering Task Force) design of a set of norms, is an upgraded version of IPv4. The most striking difference between IPv6 and IPv4 is that the length of the IP address is increased from 32 to 128 bits.

The IPv6 address is represented with a colon (:) separated by a string of 16bit hexadecimal number. Each IPv6 address is divided into eight groups, each group of 16bit with 4 hexadecimal numbers to indicate that group and group with a colon are separated, such as: 2001:0000:130F:0000:0000:09C0:876A:130B. In order to simplify the IPv6 address, the IPv6 address in the "0" can have the following treatment: in each of the leading "0" can be omitted, that is, the address can be written as 2001:0:130F:0:0:9C0:876A:130B. If the address contains two or more group (0), you can use double colon ":" to replace the, namely the above address can write 2001:0:130F: 9C0:876A:130B.

Only a double colon "::" used in a IPv6 address

The IPv6 address is composed of two parts: the address prefix and the interface identifier. Among them, the address prefix is equivalent to the IPv4 address in the network number field section, the interface identifies the equivalent of the IPv4 address in the host number section.

The representation of the address prefix is: IPv6 address / prefix length. Among them, the IPv6 address is listed in the front of any form, and the prefix length is a decimal number, IPv6 address, the number of the left side of the address prefix.

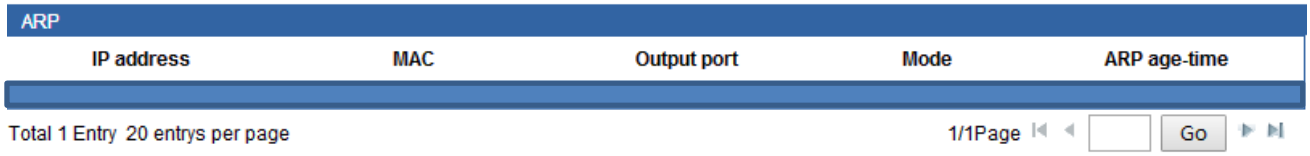
6.5.2 ARP configuration

ARP (Resolution Protocol Address) is the IP address resolution for Ethernet MAC address (or physical address) of the agreement.

In a local area network, when the host or other network equipment has data to be sent to another host or device, it must know the other side of the network layer address (IP address). But only IP address is insufficient, because IP data packets must be encapsulated frame can be sent through the physical network, so the transmitting station must also be a receiving station of the physical address, so we need a mapping from IP addresses to physical addresses. ARP is the protocol to implement this function.

6.5.2.1 Show ARP

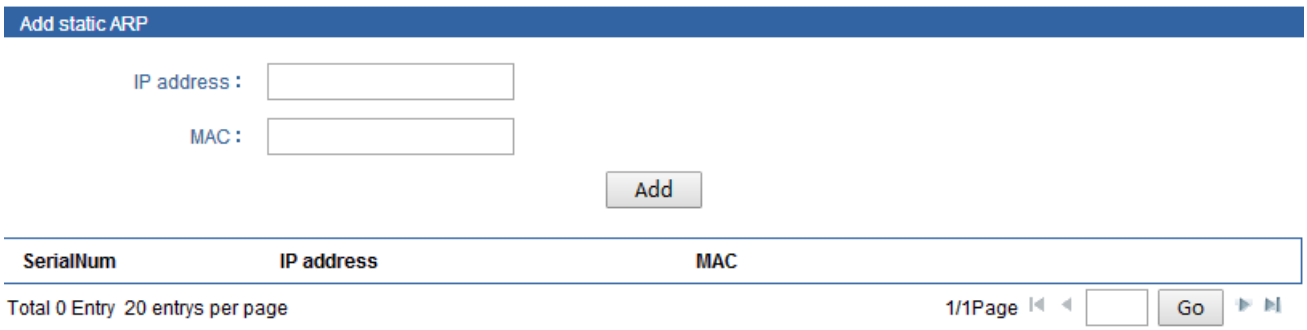
In the menu bar in order to click on the "main menu", "ARP configuration", "Show ARP" to enter the ARP view interface, the interface can view the ARP address, MAC, the interface and other parameters.



（Figure 6.5.2.1）

6.5.2.2 Static ARP

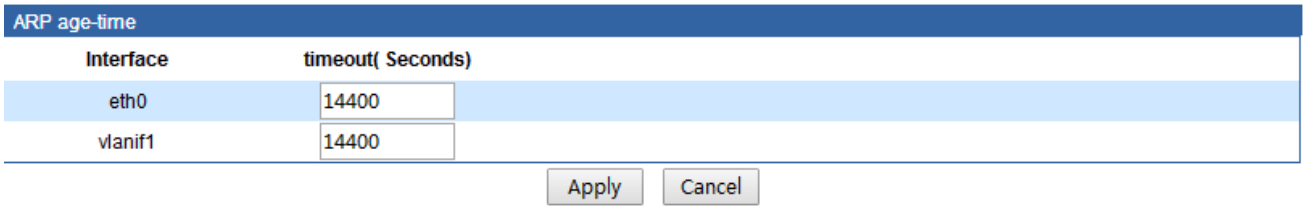
In the menu bar, click on the "main menu", "ARP configuration", "static ARP" into the static ARP configuration interface, the interface can be static ARP configuration.



（Figure 6.5.2.2）

6.5.2.3 ARP age-time

In the menu bar, click on the "main menu", "ARP configuration", "ARP age-time" into the ARP aging time configuration interface, the interface can be configured for ARP aging time.



（Figure 6.5.2.3）

6.5.3 VRRP

VRRP (Virtual Router Redundancy Protocol) is a fault-tolerant protocol. Usually all hosts in a network are set to a default route, so that host sends the destination address not in this segment of the message will be through a default route to router routerA, thereby realizing communication of host and external network. When the router of routerA is broken, in the same segment all of routerA host for a default route will not be able to communication with the outside, resulting in a single point of failure. VRRP is proposed to solve the above problems, it is a local area network with multicast or broadcast capability.

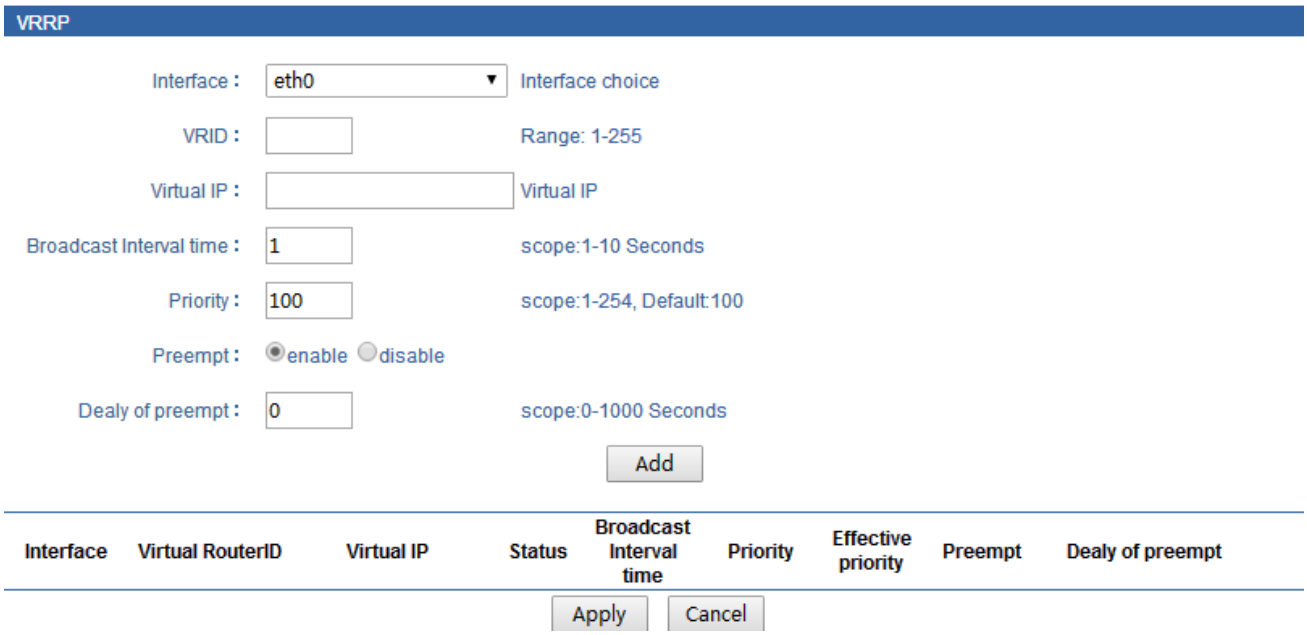
VRRP will be a group of local area network routers 10.100.10.1 (including a Master router and a number of Backup routers) organized into a virtual router, called a backup group. The virtual router has its own IP address (the IP address can be and backup group a router interface address the same, the same is said for IP owners), the router backup group also has its own IP address (such as the IP address of the master for 10.100.10.2. The IP address of the backup is 10.100.10.3). LAN host just know this virtual router IP address 10.100.10.1, and do not know the specific Master router IP address 10.100.10.2 and Backup router IP address 10.100.10.3. They set their own default routing address to the IP address of the virtual

router 10.100.10.1. As a result, the host on the network will be through this virtual router to communicate with other networks. If the Master router in the backup group is broken, the Backup router will choose a new Master router through the election strategy, and continue to provide routing services to the host in the network. In this way, the host can communicate with the external network continuously in the network.

Realization principle:

A VRRP router has a unique identifier: VRID, ranging from 0 to 255. This is the only virtual router's MAC address, the address of the 00-00-5E-00-01-[VRID] format. Master router is responsible for the ARP request with the MAC address for response. So, no matter how switching, ensure to the terminal equipment is the only consistent IP and MAC address, reducing the switching of terminal equipment effects.

There is only one kind of VRRP control message: VRRP advertisement. It uses the IP data packets are encapsulated multicast group address, 224.0.0.18, released only in the same LAN.



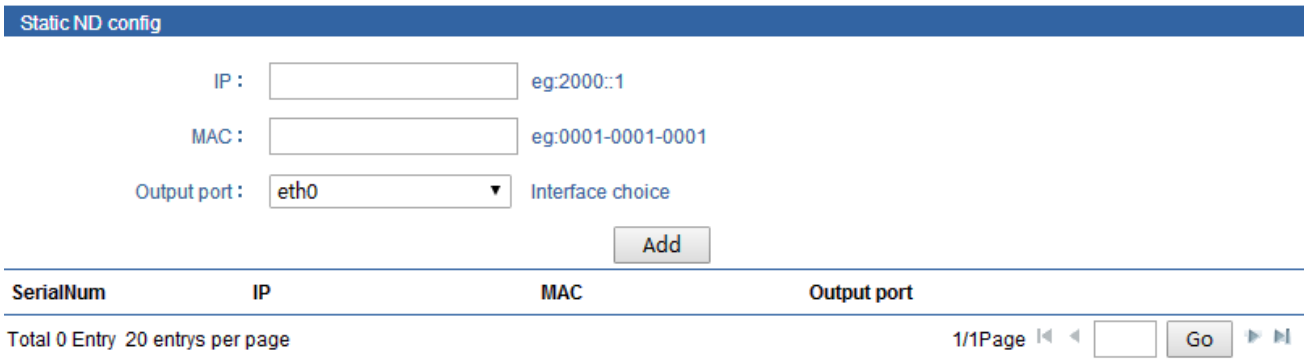
（Figure 6.5.3）

Please refer to the configuration guidance manual "07".

6.5.4 ND configuration

IPv6 Neighbor Discovery (IPv6 ND protocol, referred to as ND) is a kind of base protocol of IPv6, which uses Na, NS, RA, RS and redirect five types of ICMPv6 messages to determine between neighbor nodes and address the relationship information to achieve the address resolution and validate the neighbor is accessibility, and duplicate address detection, router discovery / prefix discovery, address auto configuration and redirect functions.

Neighbor discovery protocol instead of IPv4 ARP, ICMP router discovery and ICMP redirect messages, and provides a series of enhancements to ensure the safety of the device.



（Figure 6.5.4）

Configuration steps:

1, configure the IPV6 address and MAC address, the interface

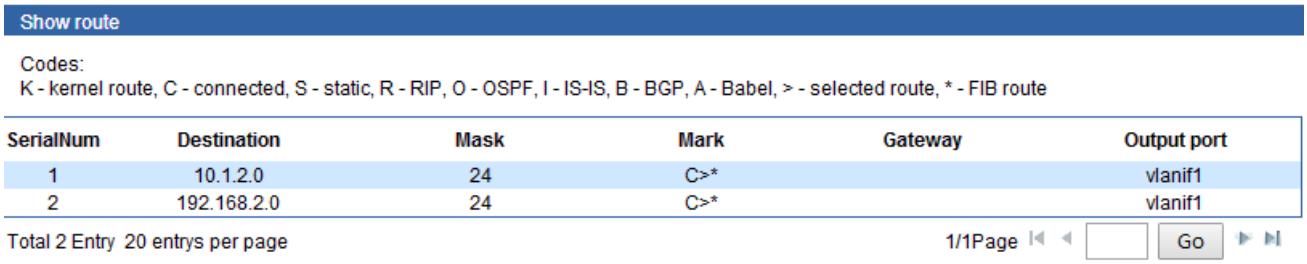
2, click Add

Please refer to the configuration guidance manual "08".

6.6 Route configuration

6.6.1 Show configuration

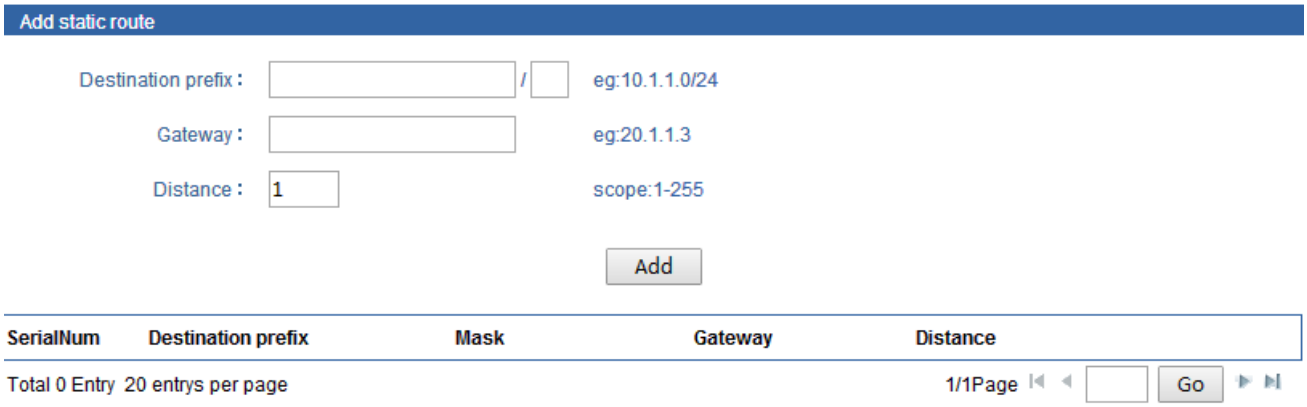
In the menu bar, click on the "main menu", "routing configuration", "view routing" access to view the routing interface, the interface can view all kinds of ways to configure the route.



（Figure 6.6.1）

6.6.2 Static configuration

In the menu bar, click on the "main menu", "routing configuration", "static configuration" to enter the static configuration interface, the interface can be configured static routing.



（Figure 6.6.2）

Configuration steps:
1, add the destination prefix, gateway, distance
2, click Add

Please refer to the configuration guidance manual "09".

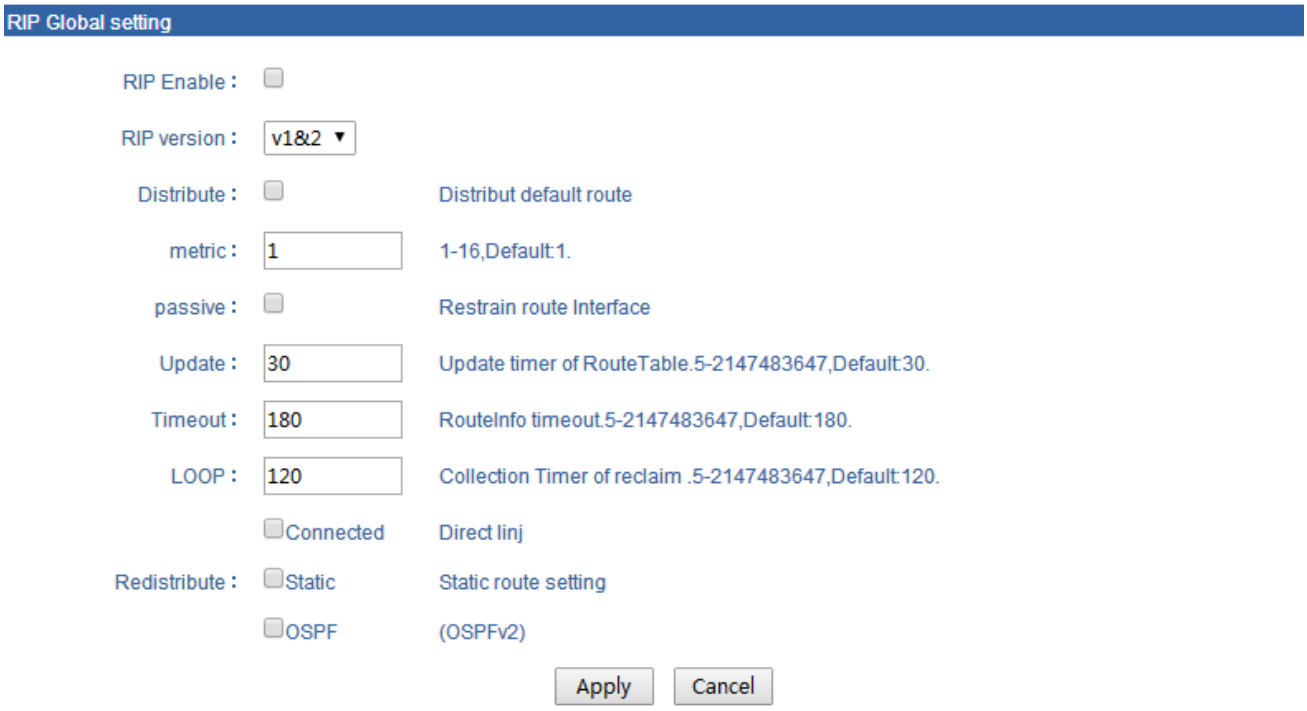
6.6.3 RIP configuration

Rip (routing information protocol) is a relatively simple interior gateway protocol (Interior Gateway Protocol, IGP), mainly used for smaller networks, such as campus network and relatively simple in structure and regional networks. For more complex environments and large networks, the general does not use RIP.

Because the realization of RIP is relatively simple, it is much easier to configure and maintain management than OSPF and IS-IS, so there is still a wide range of applications in the actual network.

6.6.3.1 RIP Global configuration

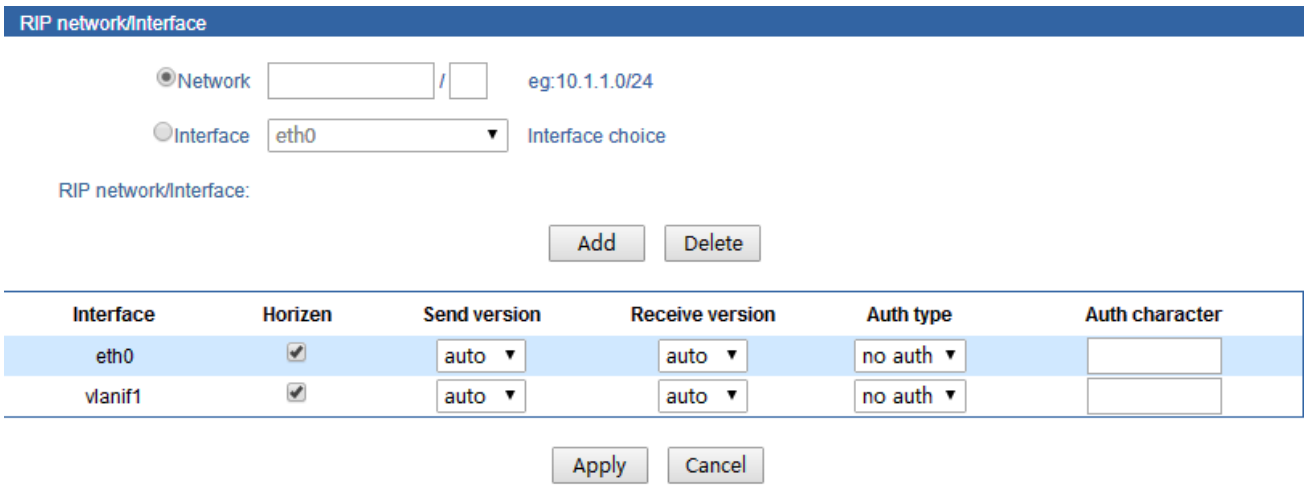
In the menu bar, click on the "main menu", "RIP configuration", "RIP global configuration" to enter the RIP global configuration interface, the interface can be configured on the RIP global correlation parameters.



（Figure 6.6.3.1）

6.6.3.2 RIP network setting

In the menu bar, click on the "main menu", "RIP configuration", "RIP network configuration" into the RIP network configuration interface, the interface can be configured on the RIP network related parameters.



（Figure 6.6.3.2）

Configuration steps:

1, enable rip

2, in the global configuration page, configure the relevant parameters.

3, in the network configuration interface configuration interface or network address.

4, click Add

Please refer to the configuration guidance manual "09".

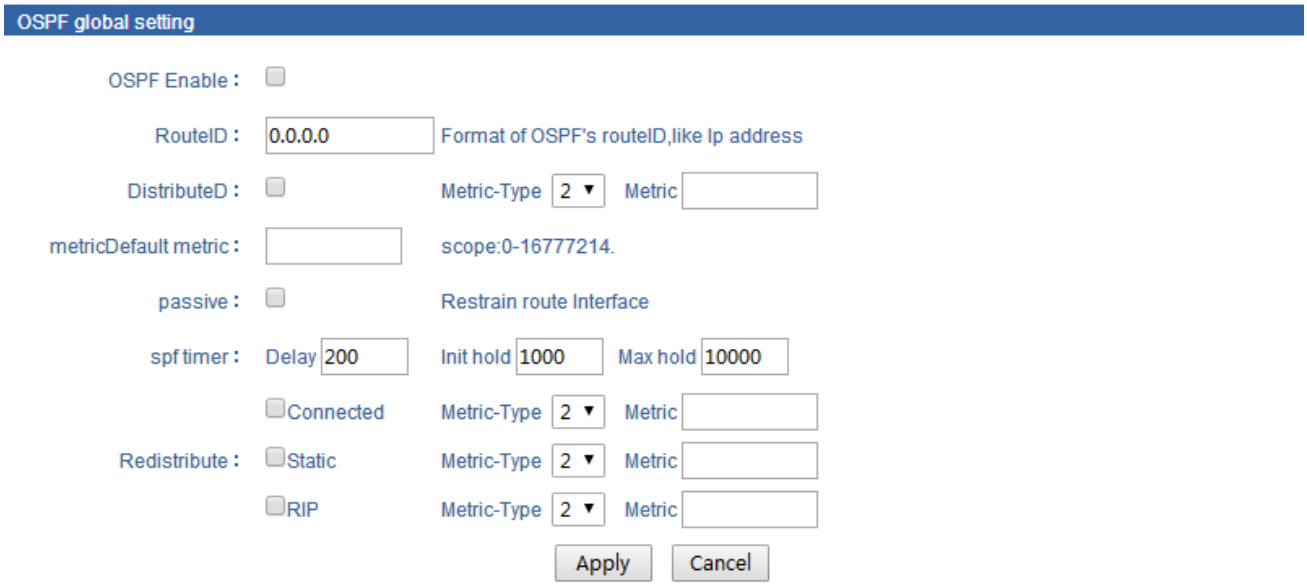
6.6.4 OSPF configuration

OSPF (Open Shortest Path First) is an internal gateway protocol (IGP), used in a single autonomous system (AS) within the decision routing. Is an implementation of link state routing protocol, which belongs to the internal gateway protocol (IGP). By Dix algorithm adding to calculate the shortest path.

OSPF is the IETF OSPF working group developed the IGP routing protocol. OSPF network designed to support the IP sub network and external routing information tags, but also allows the message authentication and support IP multicast.

6.6.4.1 OSPF global configuration

In the menu bar, click on the "main menu", "OSPF configuration", "OSPF global configuration" to enter the OSPF global configuration interface, the interface can be OSPF global parameters configuration.



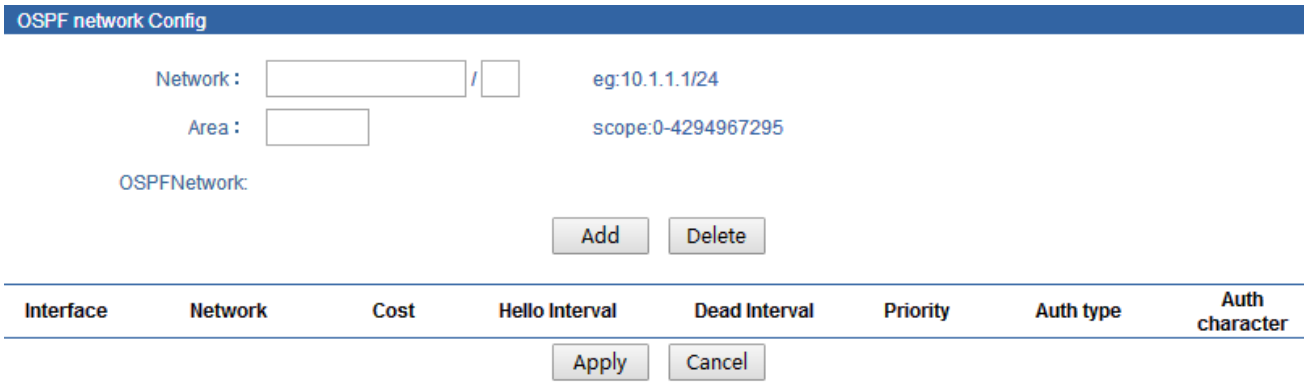
（Figure 6.6.4.1）

Intellisystem Technologies S.r.l.
Via Augusto Murri, 1 – 96100 Siracusa - Phone +39 (0)931-1756256 / +39 (0)2-87167549 - Mobile (+39) 335 1880035
em@il: info@intellisystem.it WEB: http://www.intellisystem.it

Distribute D: to force ASBR to generate the default route to enter the OSPF routing domain.
Metric default metric: Default re distribution routing metric.
SPF timer: set in the middle of a domain by the calculation of the time delay, the initial time interval, the maximum time interval
Configuration steps: can be configured according to the specific needs of the line through the command line. Please refer to the configuration guidance manual "09".

6.6.4.2 OSPF network configuration

In the menu bar, click on the "main menu", "OSPF configuration", "OSPF network configuration" into the OSPF network configuration interface, the interface can be configured for OSPF network parameters.



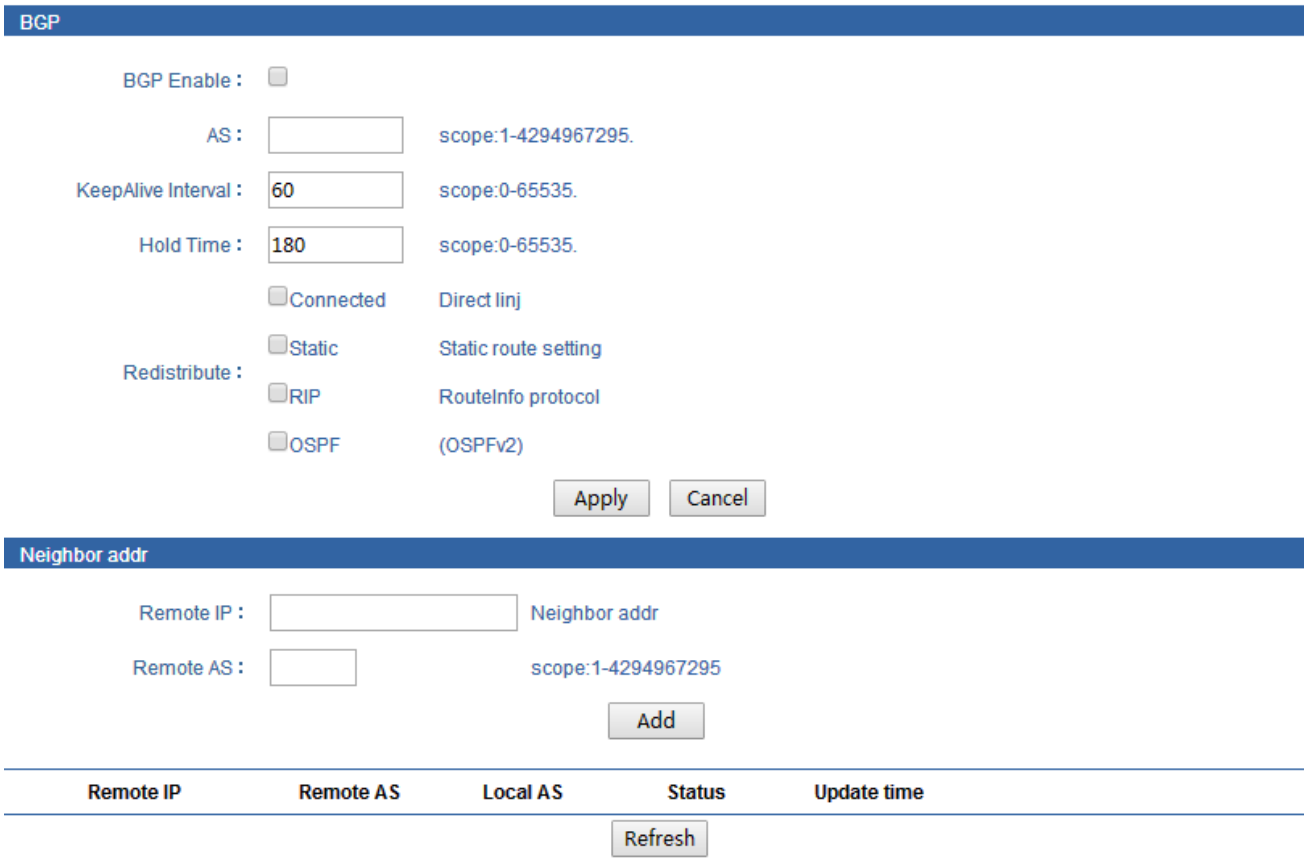
（Figure 6.6.4.2）

Configuration steps: can be configured according to the specific needs of the line through the command line. Please refer to the configuration guidance manual "09".

6.6.5 BGP configuration

The border gateway protocol BGP (Border Gateway Protocol) is a kind of autonomous system routing protocol which runs on TCP. BGP is the only protocol that is used to deal with the network size of the Internet, and is the only protocol that can properly handle the multi link connection between routing domains. BGP builds on EGP's experience. The main function of BGP system is to exchange network reach ability information with other BGP systems. Network reach ability information includes information about the autonomous system (AS) listed. This information effectively constructed as Internet topology graph and thereby removes a routing loop, at the same time as level implementation strategy.

In the menu bar, click on the "main menu", "routing configuration", "BGP" to enter the BGP configuration interface, the interface can be configured for BGP parameters.



（Figure 6.6.5）

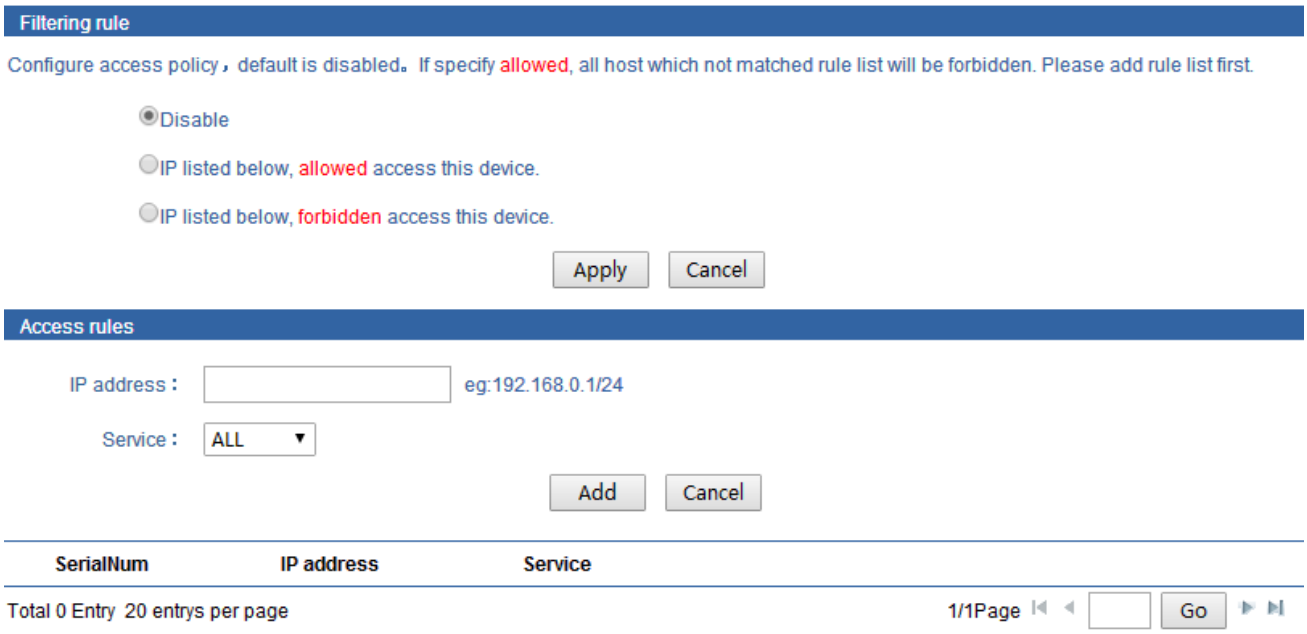
AS: autonomous system
Keep alive interval: the specified peer or peer group survival time interval
Hold time: the specified peer or peer group hold time
Redistribute: select different routing protocols for information distribution
Remote IP: neighbor IP address settings
Remote AS: neighbors belong to AS

Configuration steps: can be configured according to the specific needs of the line through the command line. Please refer to the configuration guidance manual "09".

6.7 Network security

6.7.1 Access control

In the menu bar, click on the "main menu", "network security", "access control" access control interface, the interface can be configured to access rules and filtering rules.



（Figure 6.7.1）

Access control configuration:

Step 1: fill in the IP address in the text box of the IP address;

Step 2: select ALL, HTTP, or TELNET in the service's drop-down box;

Step 3: click the "add" button;

Step 4: select disable, where in accordance with the following rules host in the filtering rules of radio buttons, allowing access to the corresponding equipment service or where in accordance with the following rules host prohibited access to the corresponding equipment service;

Step 5: click the "Apply" button.

6.7.2 Attack protection

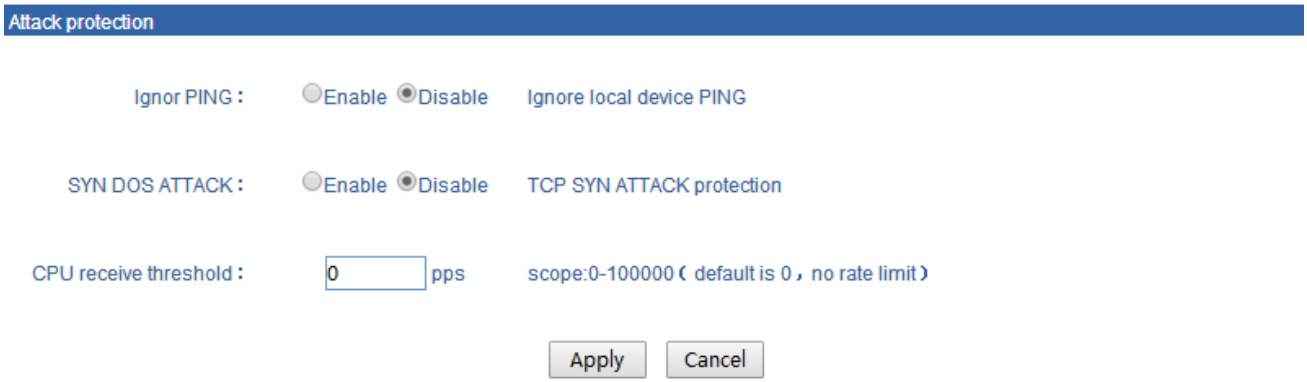
Ping attack

The Ping attack is to send a packet that does not receive a reply to the specified IP address. This attack causes the operating system to crash by sending more than 65536 bytes of ICMP packets;

DOS SYN attack

In general, the establishment of TCP connection needs to go through three times to shake hands. Using TCP connection establishment process, some malicious attackers can carry out SYN Flood attacks. An attacker sends a large number of requests to the server to establish a TCP connection SYN message, and does not respond to the server's SYN ACK message, leading to the establishment of a large number of TCP semi connection servers. Which consumes server resources, so that the server cannot handle the normal business purposes.

In the menu bar, click on the "main menu", "network security", "attack protection" to enter the anti attack settings interface.



（Figure 6.7.2）

Anti attack configuration steps:

Step 1: ignore the Ping packet radio box select to enable or disable;

Step 2: select the checkbox to enable or disable in the prevention of SYN attack in DOS;

Step 3: fill in CPU threshold packet reception threshold in the text box;

Step 4: click the "Apply" button.

6.7.3 ACL configuration

ACL (Access Control List) is a collection of one or more rules for the identification of message flow. The so-called rule, is to describe the message matching condition of the judgment, these conditions can be the source of the message address, destination address, port number, etc. According to these rules, the network device identifies a specific message and processes it according to a predetermined policy.

6.7.3.1 ACL group configuration

In the menu bar, click "main menu", "network security", "ACL configuration", "ACL group configuration into ACL group configuration interface, the interface can port setting MAC access list ID and IP access list ID.

ACL GROUP Config

Port	MACACL ListID	IPACL ListID
ge1/1	0	0
ge1/2	0	0
ge1/3	0	0
ge1/4	0	0
ge1/5	0	0
ge1/6	0	0
ge1/7	0	0
ge1/8	0	0
ge1/9	0	0
ge1/10	0	0
ge1/11	0	0
ge1/12	0	0
ge1/13	0	0
ge1/14	0	0
ge1/15	0	0

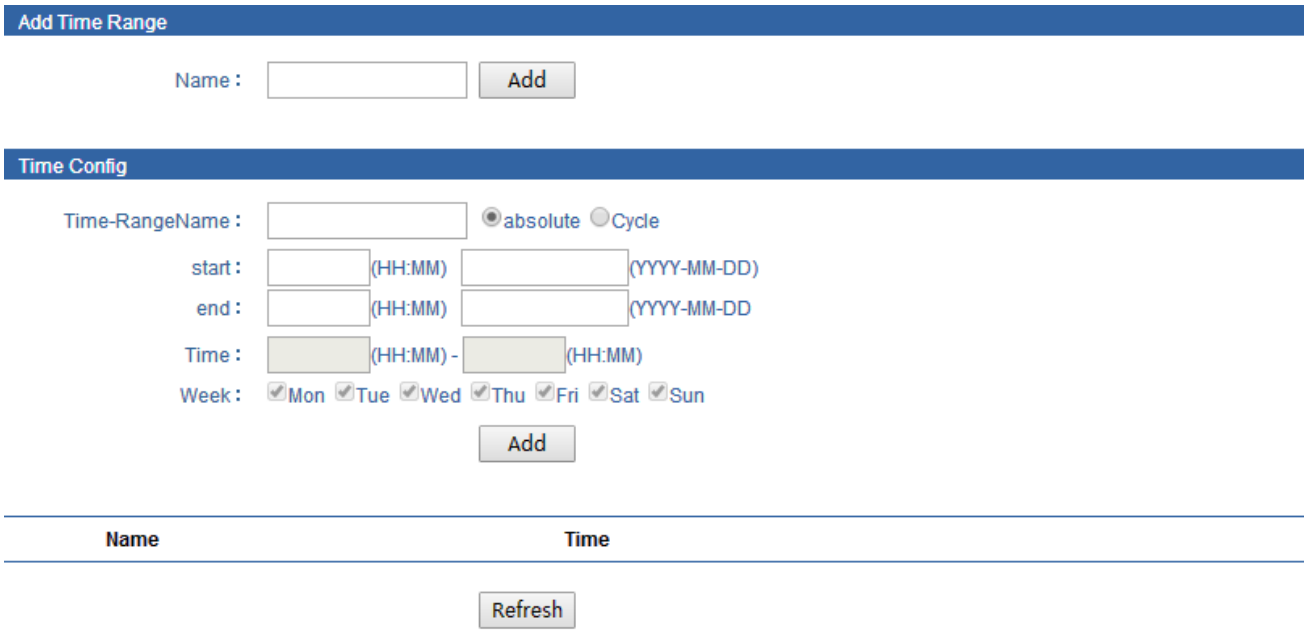
（Figure 6.7.3.1）

ACL GROUP configuration step:
Step 1: fill in the port of the MAC ACL list ID or IP ACL list ID;
Step 2: click the "Settings" button.

6.7.3.2 Time range configuration

When the ACL rule is only required to take effect in a particular time period, a ACL filter based on the time interval can be set. To this end, users can configure one or more time periods, and then refer to these time periods in the rule, and then the rule will only take effect within the specified time period. The effective time period of ACL can be divided into the following two types:
Cycle time period: the rule that takes a week for a cycle (e.g., 8 to 12 points per week) to come into effect.
Absolute time period: indicates that the rule is valid for a specified time period (e.g., 18 points from 8 January 1, 2011 to January 3, 2011).

In the menu bar, click the "main menu", "network security", "ACL configuration", "time range configuration" into the time range configuration interface, the interface can add, delete, absolute time and cycle time.



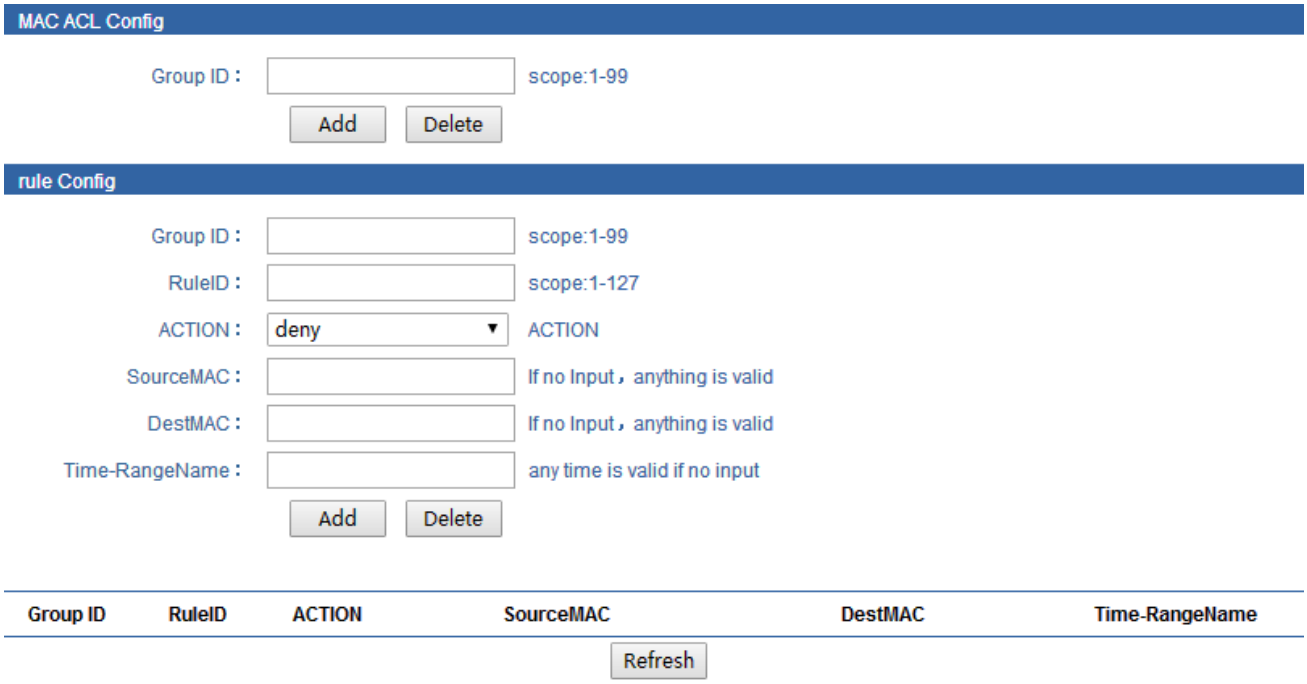
（Figure 6.7.3.2）

Time Range configuration step:
Step 1: fill in the Range Time name in the name of the text box;
Step 2: click the "add" button;
Step 3: fill in step 1 in the Time-Range name text box with the name of the Range Time added;
Step 4: choose the absolute time or cycle time;
Step 5: if the absolute time: in the start time and end time of the text box to fill in the time and date; If the cycle time: fill in the time at the time of the text box, and select the checkbox in the week number of cycles;
Step 6: click the "add" button.

6.7.3.3 MAC ACL configuration

MAC ACL is used to identify the message flow in the purpose of MAC address access control settings in accordance with the rules of MAC ACL to identify a specific message, and according to the preset strategy to deal with it.

In the menu bar in order to click on the "main menu", "network security", "ACL configuration", "MAC ACL configuration" into the ACL MAC configuration interface, the interface can add, delete MAC access list.



（Figure 6.7.3.3）

Configuration item	meaning
Group ID	User in the creation of ACL must be specified for the group ID range of 1 ~ 99;
Rule ID	Users in the creation of ACL must also set the rules for the ID range of 1 to 127;
Action	Restrictions in the rules;
Destination MAC	Each other's MAC address;
Source MAC	Own MAC address;
Time-Range name	Refers to the name of the TIME RANGE configuration.

MAC ACL configuration step:

Step 1: in the configuration of the MAC access list of the group ID in the text box to fill in the value of the group ID;

Step 2: click the "add" button;

Step 3: fill in the added group ID in the text box of the group ID of the configuration rule;

Step 4: fill in the value of rule ID in the text box of rule ID;

Step 5: select deny or permit in the action drop-down box;

Step 6: fill in the blank in the source MAC address or MAC source text box;

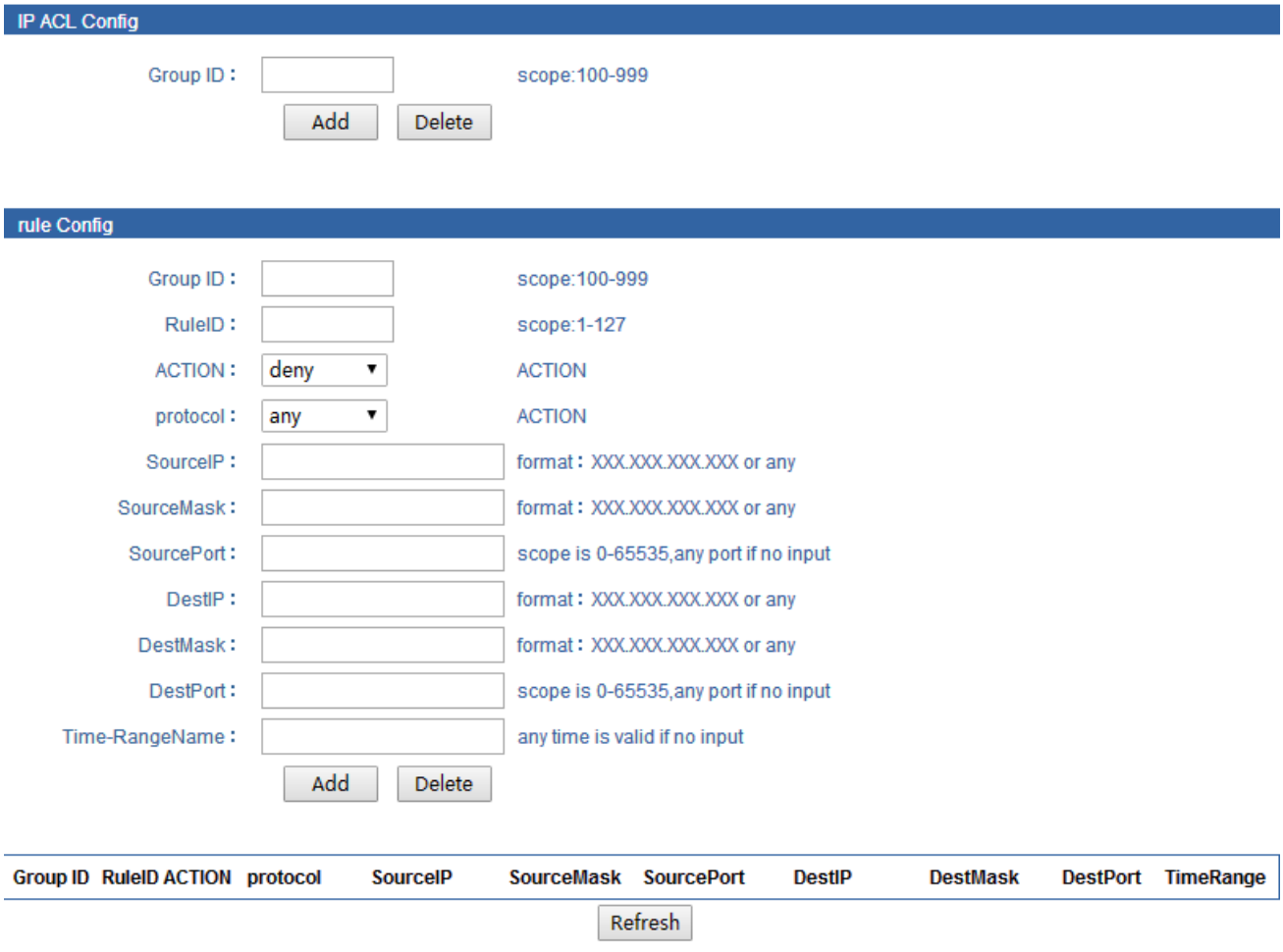
Step 7: fill in the blank in the destination MAC address or MAC text box;

Step 8: fill in the blank or add the Time-Range name in the Time-Range configuration in the Time-Range name in the text box;
Step 9: click the "add" button;
Step 10: in the ACL-GROUP configuration MAC access list ID in the text box to fill in the value of the MAC access list group ID.

6.7.3.4 IP ACL configuration

ACL IP is used to identify the message flow in the purpose of MAC address access control settings in accordance with the rules of MAC ACL to identify a specific message, and according to the preset strategy to deal with it.

In the menu bar in order to click on the "main menu", "network security", "ACL configuration", "IP ACL configuration" into the IP ACL configuration interface, the interface can add, delete MAC access list.



（Figure 6.7.3.4）

MAC ACL configuration step:
Step 1: in the configuration of the IP access list of the group ID in the text box to fill in the value of the group ID;
Step 2: click the "add" button;
Step 3: fill in the added group ID in the text box of the group ID of the configuration rule;
Step 4: fill in the value of rule ID in the text box of rule ID;

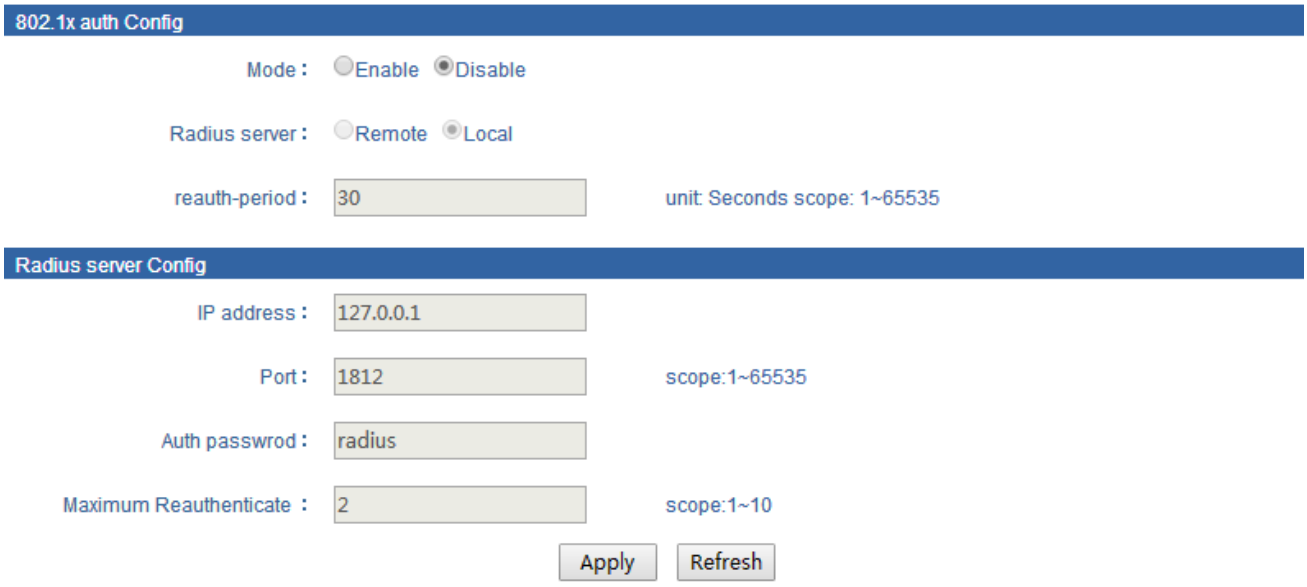
Step 5: select deny or permit in the action drop-down box;
Step 6: select the any, IGMP, IP, TCP, or UDP in the protocol;
Step 7: fill in the blank in the source IP address or IP source text box;
Step 8: fill in the blank in the source source mask or mask in the text box;
Step 9: fill in the blank in the source port or port source text box;
Step 10: fill in the blank in the destination IP address or IP text box;
Step 11: fill in the blank to mask or mask in the text box;
Step 12: fill in the blank in the destination port or destination port in the text box;
Step 13: fill in the blank or add the Time-Range name in the Time-Range configuration in the Time-Range name in the text box;
Step 14: click the "add" button;
Step 15: in the ACL GROUP configuration IP access list ID in the text box to fill in the value of the IP access list group ID.

6.7.4 IEEE802.1x configuration

6.7.4.1 Global configuration

IEEE 802.1x authentication architecture with a "controlled port" and "uncontrollable port" logic functions, which can achieve the separation of business and certification. After the user passed the authentication, business stream and certification flow should separate, no special requirements on the follow-up packet processing, the business can be very flexible, in particular, have a great advantage in carrying out the business of broadband multicast, all business are not subject to certification way limit.
802.1X authentication involves three parties:
Supplicant: It's the users or customers want to get the authentication.
Authentication server: Such as RADIUS server.
Authenticator: Such as wireless access points, switches, etc.

In the menu bar, click the "main menu", "network security", "802.1X configuration", "global configuration" to enter the 802.1X global configuration interface.



（Figure 6.7.4.1）

802.1x

802.1x is used to enhance the security of the authentication.

Radius Server Remote/Local

Build Radius server between devices, the applicant will only can RADIUS database user name and password. If you use an external RADIUS server you need to fill in the IP address and port number of the authentication server. We need to fill in the IP address and port number of the billing server settings, otherwise set by the accounting server IP address is empty if you need to use the AAA accounting system.

Authentication server

Radius remote access authentication server, which is used for authentication and the IP address / domain name that the devices can access, the default Port is 1812.

Authenticate the Shared Password.

For device access the shared secret string of authentication server.

Global configuration step:

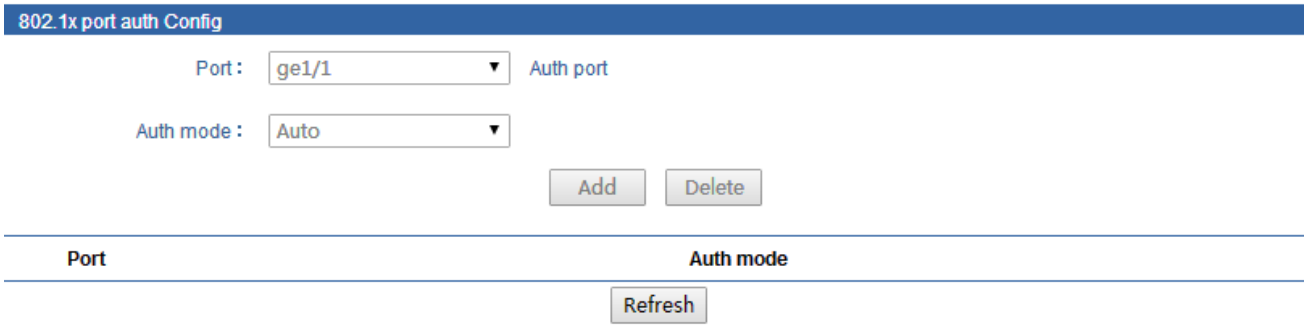
Step 1: select "enable" or "disable" 802.1x authentication;

Step 2: select the Radius server "remote" or "local"; fill in the authentication update interval;

Step 3: fill in the IP server's Radius address, port, authentication and sharing password and authentication repeat times;

Step 4: click "Apply".

6.7.4.2 Port configuration



（Figure 6.7.4.2）

Port configuration steps:

Step 1: select the authentication port;

Step 2: select the authentication mode;

Step 3: click "add".

Between the applicant and the authentication system using the MD5-Challenge, other methods do not support network connection without "authentication" option, Please select "Accessories" -> "Administrative Tools" -> "Component Services" -> "Service", set the "Wired AutoConfig" to "automatic" billing server, if the setting is incorrectly will also result in the applicant cannot pass authentication. We do not need to set the appropriate port as the uplink port if don't have billing system, the default is authenticated, the user can not set up, all uplink ports or downlink ports must be forced to certificate, be "prohibit the use of certification", or cannot use the remote server, the administrator have to make sure that the device can access the remote server if use the remote server, the device address of the gateway settings are correct, if you use the domain name, the DNS must be set correctly.

6.8 Advanced configuration

6.8.1 QOS configuration

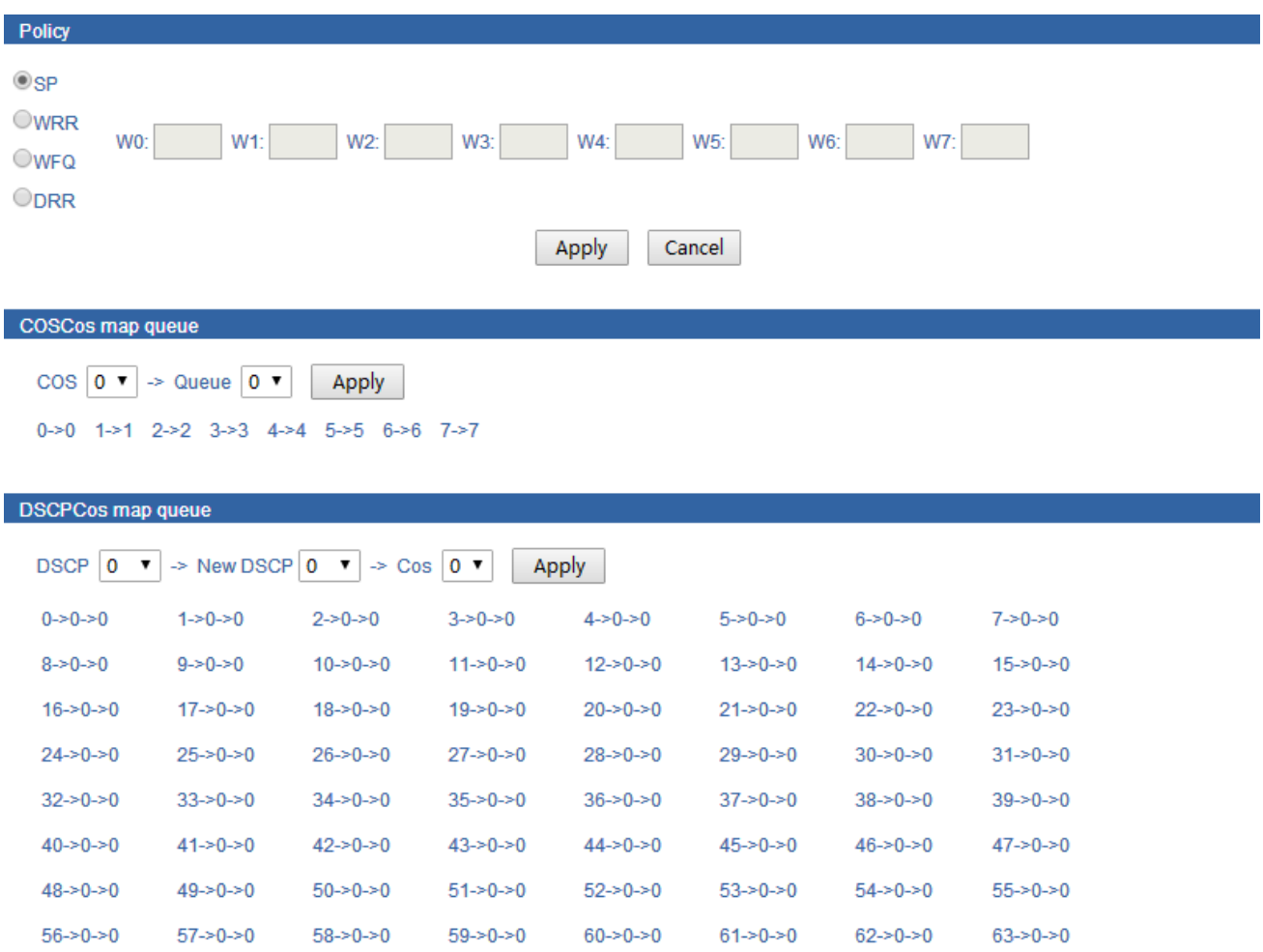
QoS (Quality of Service) is a ubiquitous concept that exists in the service supply and demand relations, it evaluates the ability of service providers to meet customer service requirements. Commonly known as QoS, is the packet forwarding process for delay, jitter, packet loss rate and other core needs to provide support for the assessment of the service capabilities.

6.8.1.1 Global configuration

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.

Users can choose QOS priority queue mechanism, its queue mechanism has four kinds: SP(Strict Priority), WRR(Weighted Round Robin), WFQ(Weighted Fair Queuing), DRR（deficit round robin)
SP: according to the priority order, the higher priority forwarding.
WRR: Each port is divided into a number of output queue, the queue between the scheduling, to ensure that each queue will get a certain service time
WFQ: WFQ weighting is based on the flow in the IP precedence, to ensure that the flow of high IP precedence distribution to more bandwidth. Algorithm for (IP precedence+1)/Sum(IP precedence+1);
DRR: DRR algorithm is an extension of RR algorithm. DRR algorithm for each queue to assign a constant QN (to the weights of the time slice) and a variable DN (difference).

In the menu bar, click "main menu", "advanced configuration", "QoS configuration", "global configuration" into QoS global configuration interface, the interface can configure QoS scheduling strategy, cos queue map and DSCP queue mapping.



（Figure 6.8.1.1）

QOS global configuration:

Step 1: configuring QoS scheduling strategy, scheduling strategy SP, WRR, WFQ or DRR. If the scheduling strategy choice is WRR, WFQ or DRR, need in W0, W1, W2, W3 text box fill ratio, and then click the "apply" button.

Step 2: configure the COS queue mapping, in the COS drop-down box to select the value of 0-3 COS, in the Queue drop-down box to select the value of 0-3 Queue, and then click the "apply" button;

Step 3: configure DSCP queue mapping, in the DSCP drop-down box to select the 0-63 value DSCP, in the DSCP New drop-down box to select the DSCP 0-63 value New, in the Cos drop-down box to select the Cos value 0-3, and then click the "apply" button.

6.8.1.2 Port configuration

In the menu bar in order to click on the "main menu", "advanced configuration", "QOS configuration", "port configuration" into the QOS port configuration interface, the interface can configure the default port COS.

Port Config

Port	Default COS	Port	Default COS	Port	Default COS
ge1/1	0	ge1/2	0	ge1/3	0
ge1/4	0	ge1/5	0	ge1/6	0
ge1/7	0	ge1/8	0	ge1/9	0
ge1/10	0	ge1/11	0	ge1/12	0
ge1/13	0	ge1/14	0	ge1/15	0
ge1/16	0	ge1/17	0	ge1/18	0
ge1/19	0	ge1/20	0	ge1/21	0
ge1/22	0	ge1/23	0	ge1/24	0
xe1/25	0	xe1/26	0	xe1/27	0
xe1/28	0				

Apply Cancel

（Figure 6.8.1.2）

Port configuration steps:

Step 1: fill in the desired COS value for the port;

Step 2: click "Apply".

6.8.2 LLDP configuration

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

6.8.2.1 Global configuration

In the menu bar in order to click on the "main menu", "advanced configuration", "LLDP configuration", "global configuration" into the LLDP global configuration interface, the interface can be configured with the relevant parameters of LLDP.

LLDP Config

LLDP : Enable Disable

Send cycle : 30 scope:5-65535

Hold Time : 120 scope:5-65535

Send interval : 2 scope:2-5

Reinit delay : 2 scope:2-5

TLV Optional to send : Management address Port description System property System description System name

Apply Cancel

（Figure 6.8.2.1）

Configuration item	meaning
Disable	The switch will not send the LLDP message, and will reduce the LLDP message received from the neighbor.
Enable	The switch will send the LLDP message, which will analyze the LLDP message received from the neighbor.
Send cycle	Equipment status is not changed, the device periodically to the neighbor nodes to send LLDP packets, the interval time is called to send LLDP message cycle.
Send interval	The switch regularly sends LLDP frames to its neighbors, which contain the latest information on the web. The time interval between each LLDP frame is determined by the value of the Tx interval. Valid values are restricted to 2~5 seconds.

LLDP global configuration step:

Step 1: select enabled or disabled in the radio buttons in LLDP;

Step 2: fill in the value of the sending period in the text box of the send cycle;

Step 3: the value of the retransmission time in the text box of the retransmission time;

Step 4: fill in the value of the sending interval in the text box of the sending interval;

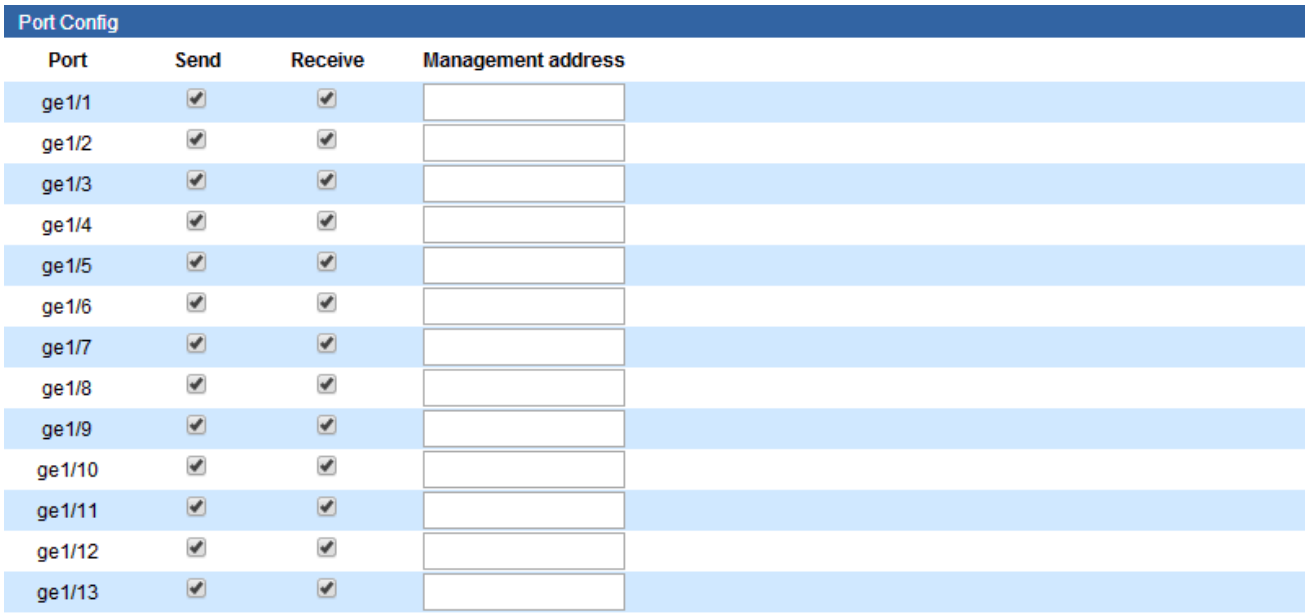
Step 5: fill in the re enable delay value in the text box for re opening delay;

Step 6: in sending TLV optional checkbox selection management address and port description, system attributes, description and name.

Step 7: click the "Settings" button

6.8.2.2 Port configuration

In the menu bar followed by click on the "main menu", "advanced configuration" and "LLDP configuration", port configuration into LLDP port configuration interface, the interface can port configured for sending and receiving mode and management address.



（Figure 6.8.2.2）

Configuration item	meaning
receive	Switch will not send out the LLDP information, but the information from the vicinity of the unit LLDP analysis.
send	Will reduce the LLDP information received from the neighbors, but will send LLDP information.
Management address	LLDP management address is the address of the network management system identification and management. Management address can clearly identify a device, it is conducive to the network topology, network management, network management. The management address is encapsulated in the Management Address TLV field of the LLDP message and is sent to the neighbor node.

LLDP port configuration step:

Step 1: check the port in the sent check box;

Step 2: check the port in the received check box;

Step 3: fill in the IP address in the text box of the management address;

Step 4: click the "Apply" button.

6.8.2.3 LLDP neighbors

In the menu bar in order to click on the "main menu", "advanced configuration", "LLDP configuration", "LLDP neighbor" into the LLDP interface, the interface can be viewed in the neighborhood of the relevant information.

（Figure 6.8.2.3）

6.8.3 SNMP configuration

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.

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.

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.

SNMP Version

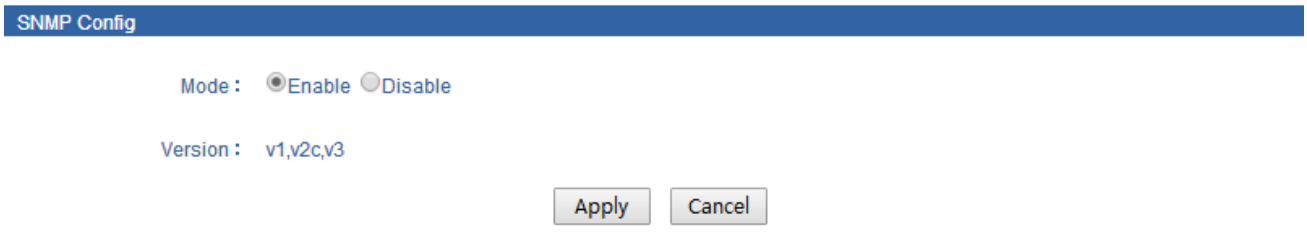
Currently SNMP Agent of the device supports SNMP V3 and it is also compatible with SNMP V1and SNMP V2C. It is authenticated by user name and password in SNMP V3.

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.

6.8.3.1 System information

Select enable or disable SMNP features.



（Figure 6.8.3.1）

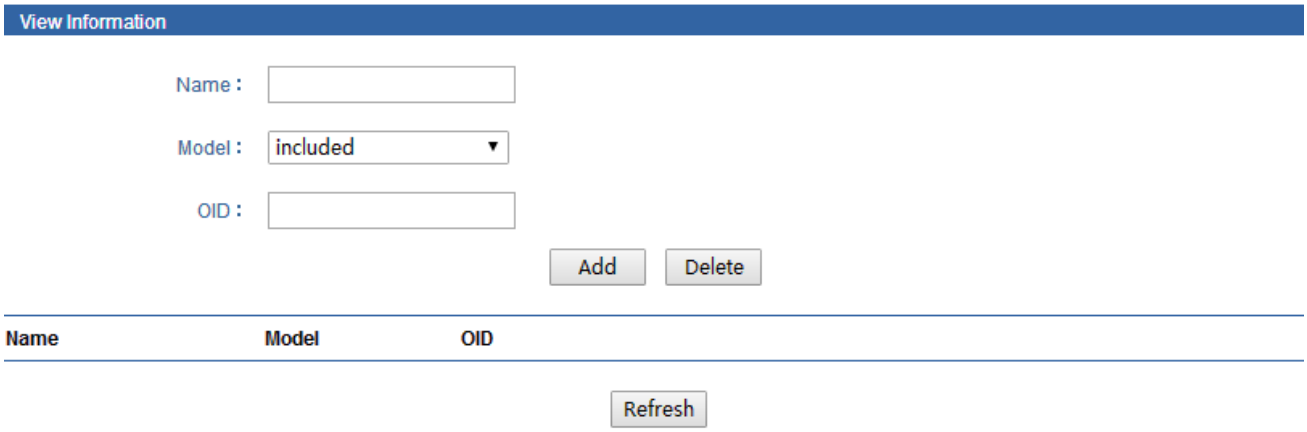
SNMP system configuration steps:

Step 1: select the checkbox to enable or disable in the mode of the;

Step 2: click the "Apply" button.

6.8.3.2 View

Fill in the name of the view as well as the mode, node OID.



（Figure 6.8.3.2）

View configuration steps:

Step 1: fill in the name of the view;

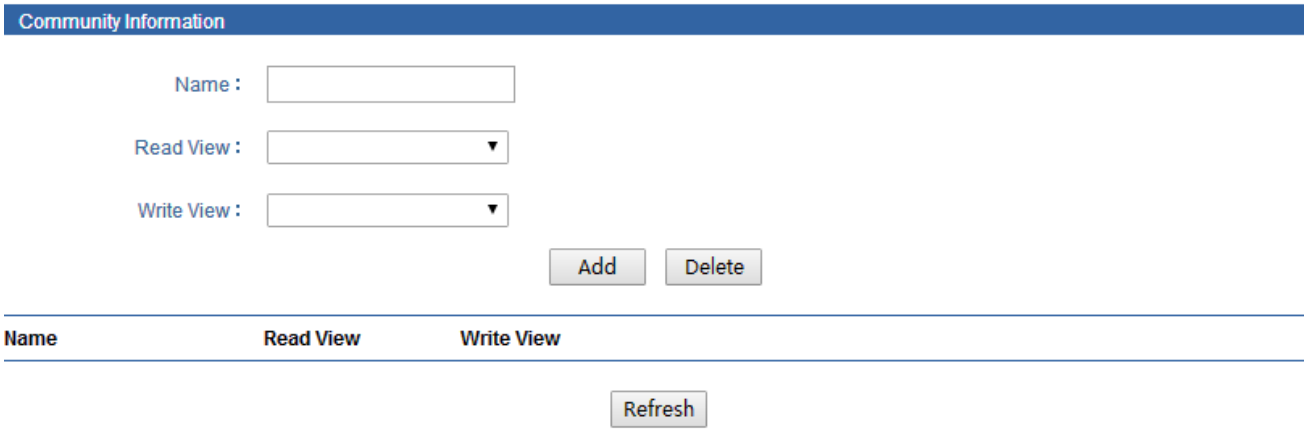
Step 2: select mode;

Step 3: fill in the node OID;

Step 4: click "add".

6.8.3.3 Community

Defines a group name that can access the MIB view, set the access rights for the group name on the MIB to write permissions (write) or read-only permissions (read).



（Figure 6.8.3.3）

Group configuration steps:

Step 1: fill in the name of the group;

Step 2: fill in the name of the read view;

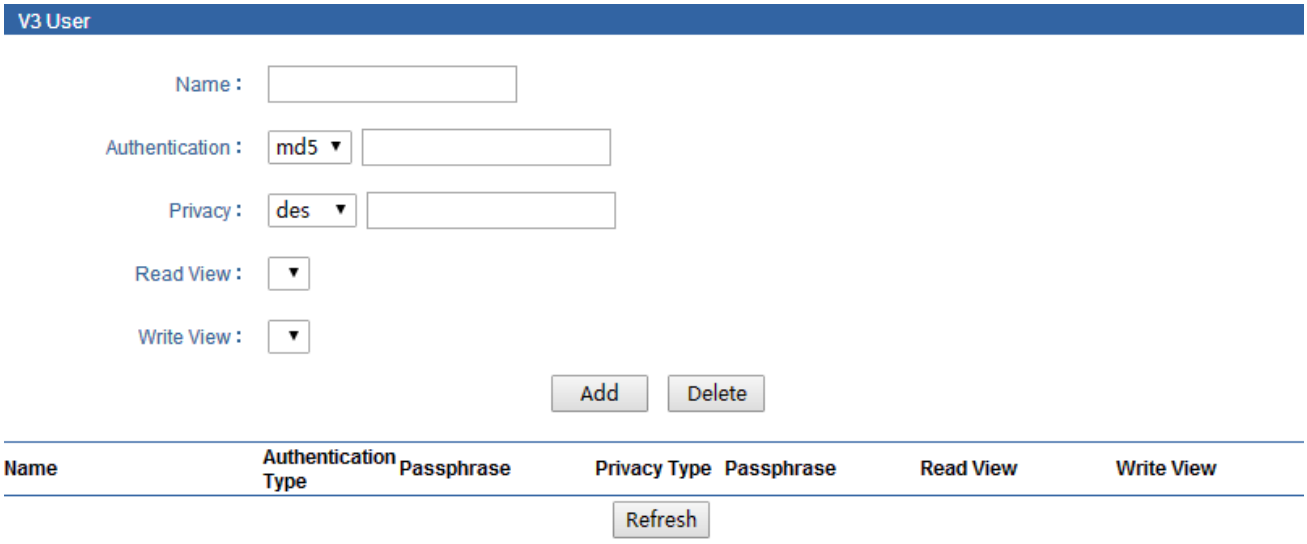
Step 3: fill in the name of the view;

Step 4: click "add".

Intellisystem Technologies S.r.l.
Via Augusto Murri, 1 – 96100 Siracusa - Phone +39 (0)931-1756256 / +39 (0)2-87167549 - Mobile (+39) 335 1880035
em@il: info@intellisystem.it WEB: http://www.intellisystem.it

6.8.3.4 V3 User

SNMPv3 using USM (User-Based Security Model) certification mechanism. Network administrators can set the authentication and encryption functions. Certification for verify the message sender's legitimacy and avoid the illegal user access; encryption is to encrypt the transmission message between NMS and agent, so as not to be tapped. Using authentication and encryption functions, can provide a higher security for the communication between NMS and Agent.



（Figure 6.8.3.4）

V3 user configuration step:

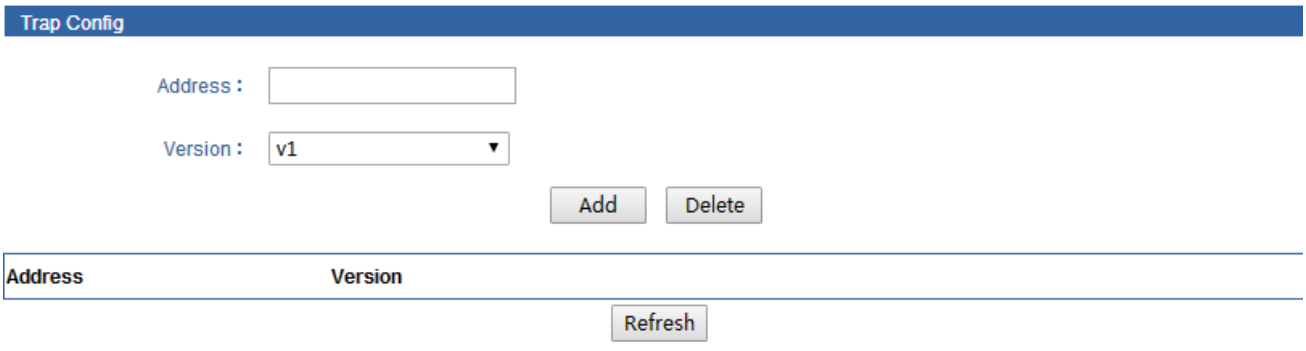
Step 1: fill in the name of the group, select the type of authentication MD5 or Sha, fill in the authentication password, select the type of encryption des or AES, fill in the configuration of the encrypted password;

Step 2: select the read and write views that are added to the view;

Step 3: click the "add" button.

6.8.3.5 Trap

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.



（Figure 6.8.3.5）

Intellisystem Technologies S.r.l.
Via Augusto Murri, 1 – 96100 Siracusa - Phone +39 (0)931-1756256 / +39 (0)2-87167549 - Mobile (+39) 335 1880035
em@il: info@intellisystem.it WEB: http://www.intellisystem.it

Trap configuration steps:

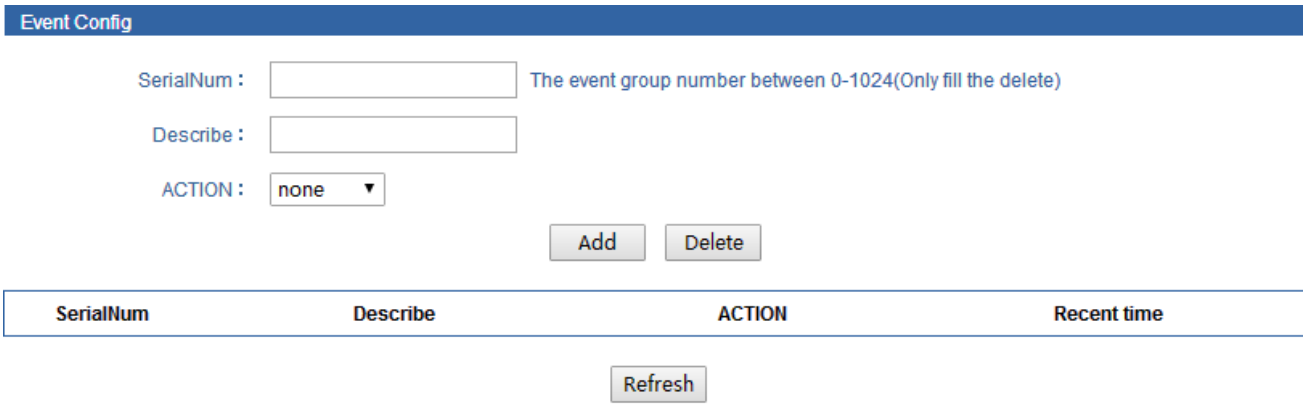
Step 1: fill in the trap event occurs when the message is sent to the destination IP address.

Step 2: click the "add" button.

6.8.4 RMON configuration

6.8.4.1 Event

In the menu bar followed by click on the "main menu", "advanced configuration" and "RMON configuration", "event group" in RMON event group configuration interface, the interface can add, delete event group and view the configuration information for a set of events.



（Figure 6.8.4.1）

Configuration item	meaning
SerialNum	The number of serial numbers and the RMON alarm information configuration are provided by the rising event index and the falling event index corresponding to the event that is triggered when the MIB object is monitored over a threshold value.
Describe	Some descriptive information about the event.
ACTION	None: Do not deal with Log: When the event is triggered, the event is recorded in the log table. Log, trap: This event is triggered when the event is recorded in the log table and generates a trap message

Configure event group steps:

Step 1: in the serial number of the text box to fill in the event group number;

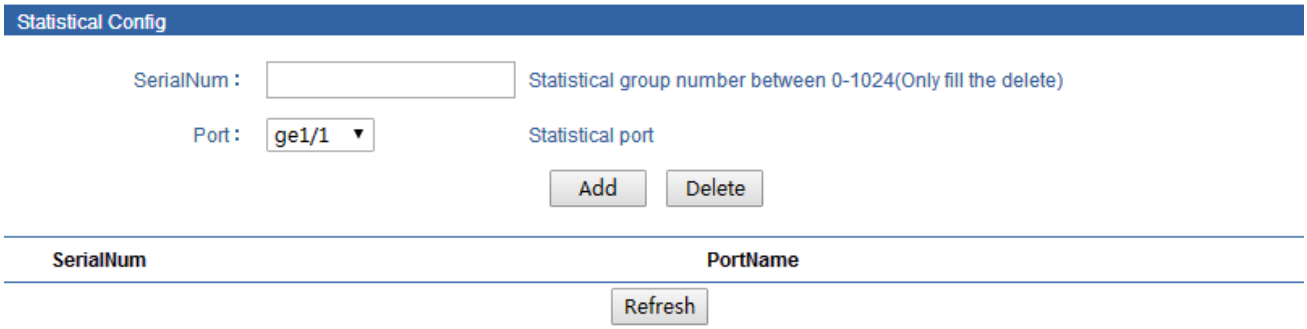
Step 2: fill in the description of the text box for the description of the event group;

Step 3: select none, log, log, trap, and in the action drop-down box;

Step 4: click the "add" button.

6.8.4.2 Statistical

In the menu bar followed by click on the "main menu", "advanced configuration" and "RMON configuration", "Statistics" in RMON statistics group configuration interface and the interface can add, delete statistics group and view the configuration information for a group of statistics. A physical port is set up as the receiving end of the monitoring data information. Serial number is used to identify a specific application interface, when the serial number is the same as the serial number of the application interface, the previous configuration will be replaced.



（Figure 6.8.4.2）

Configure the statistics group step:

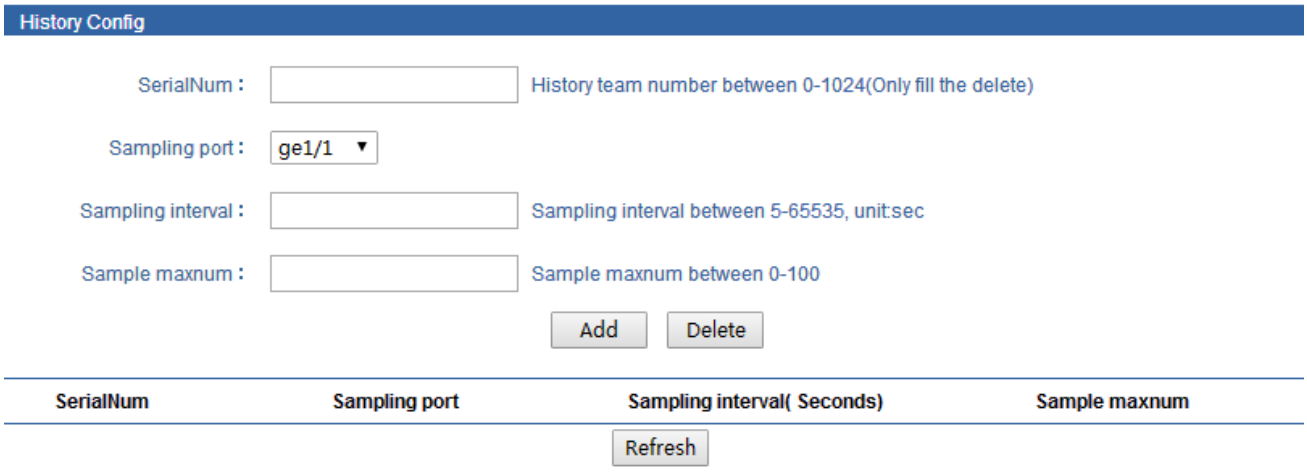
Step 1: in the serial number of the text box to fill in the statistics group number;

Step 2: select the port in the port's drop-down box;

Step 3: click the "add" button.

6.8.4.3 History

In the menu bar followed by click on the "main menu", "advanced configuration" and "RMON configuration", "group of history" into the RMON history group configuration interface, the interface can add, delete history group and view the configuration information for a group of history. Set a physical port, as the receiving end of the monitoring information; serial number is used to identify a specific application interface, when the serial number and the serial number of the application interface before setting the same, the previous configuration will be replaced.



（Figure 6.8.4.3）

Intellisystem Technologies S.r.l.
Via Augusto Murri, 1 – 96100 Siracusa - Phone +39 (0)931-1756256 / +39 (0)2-87167549 - Mobile (+39) 335 1880035
em@il: info@intellisystem.it WEB: http://www.intellisystem.it

Sampling interval: the interval of each two times to obtain statistical data.

Maximum number of samples: a list of items to be retained.

Configuration history group step:

Step 1: fill in the serial number in the text box;

Step 2: select the port in the drop - down box at the sampling port;

Step 3: fill in the value of the sample interval in the text box of the sampling interval;

Step 4: fill in the number of text boxes in the maximum number of samples;

Step 5: click the "add" button.

6.8.4.4 Alarm

Enter into Rmon alarm information configuration interface.

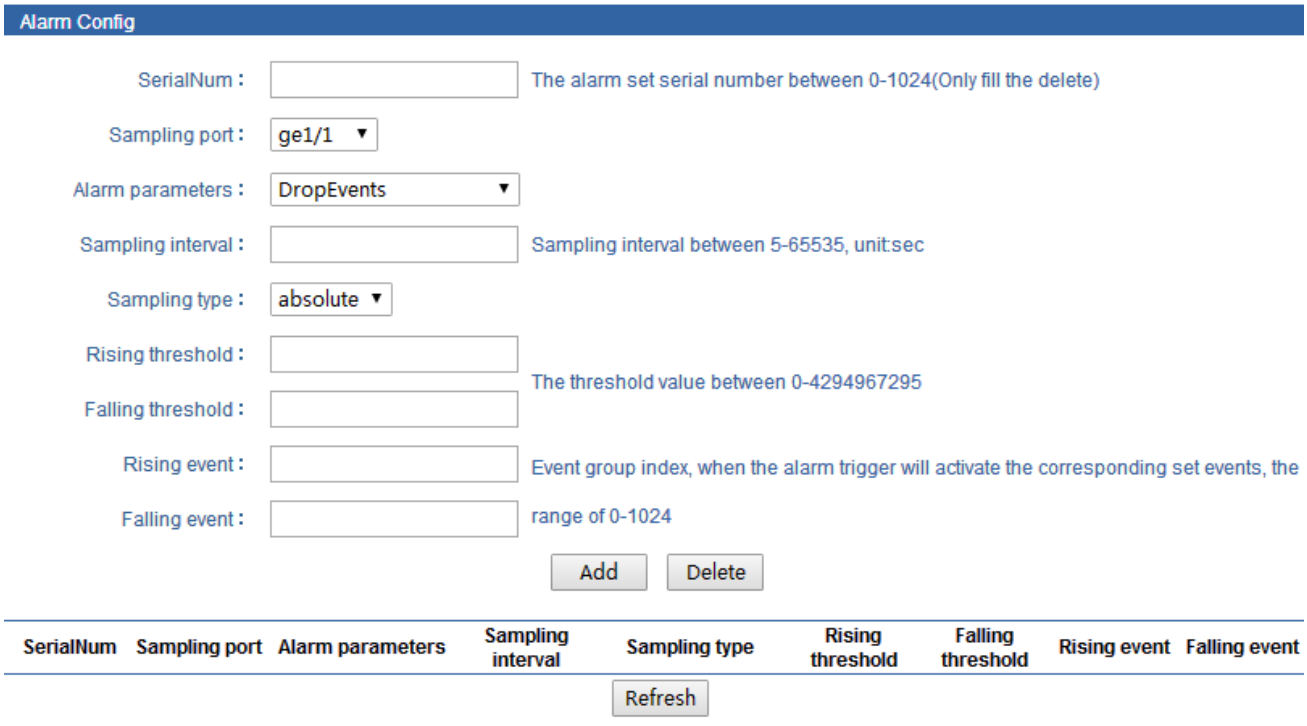
Index use for marking a alarm information configuration, if the index is the same as before, it will replace previous index.

MIB point corresponds to OID.

Alarm type adopt absolute to monitor the value of MIB target. Adopt delta to monitor the change of MIB target value when get sample two times.

When monitor MIB value reach or pass the rising threshold value, will occur event correspond to rising event index.

When monitor MIB value reach or pass the falling threshold value, will occur event correspond to falling event index.



（Figure 6.8.4.4）

Configure alarm group steps:

Step 1: in the serial number of the text box to fill in the alarm group number;

Step 2: select the port in the drop - down box at the sampling port;

Step 3: select the alarm parameter in the drop box of the alarm parameter;

Step 4: fill in the value of the sample interval in the text box of the sampling interval;

Step 5: absolute or delte in the drop box of the sample type;

Step 6: fill in the threshold in the text box of the rising and falling edge;

Step 7: fill in the event number in the text box of the event's rise and fall;

Step 8: click the "add" button.

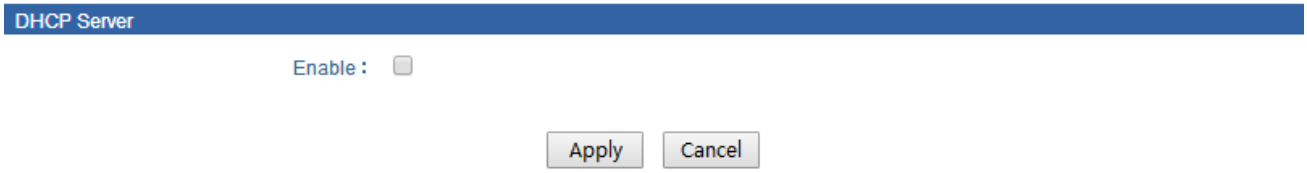
6.8.5 DHCP Server configuration

DHCP (Dynamic Host Configuration Protocol) is usually applied in large local area network environment, the main function is centralized management, IP address allocation, obtain IP address, gateway address, DNS server address information to network environment host dynamics, and can promote the rate of use of address.

6.8.5.1 DHCP Server configuration

DHCP Server enabled, the device is used as a DHCP server, by setting the static allocation address table to achieve, the device can be connected to other devices connected to the device IP address.

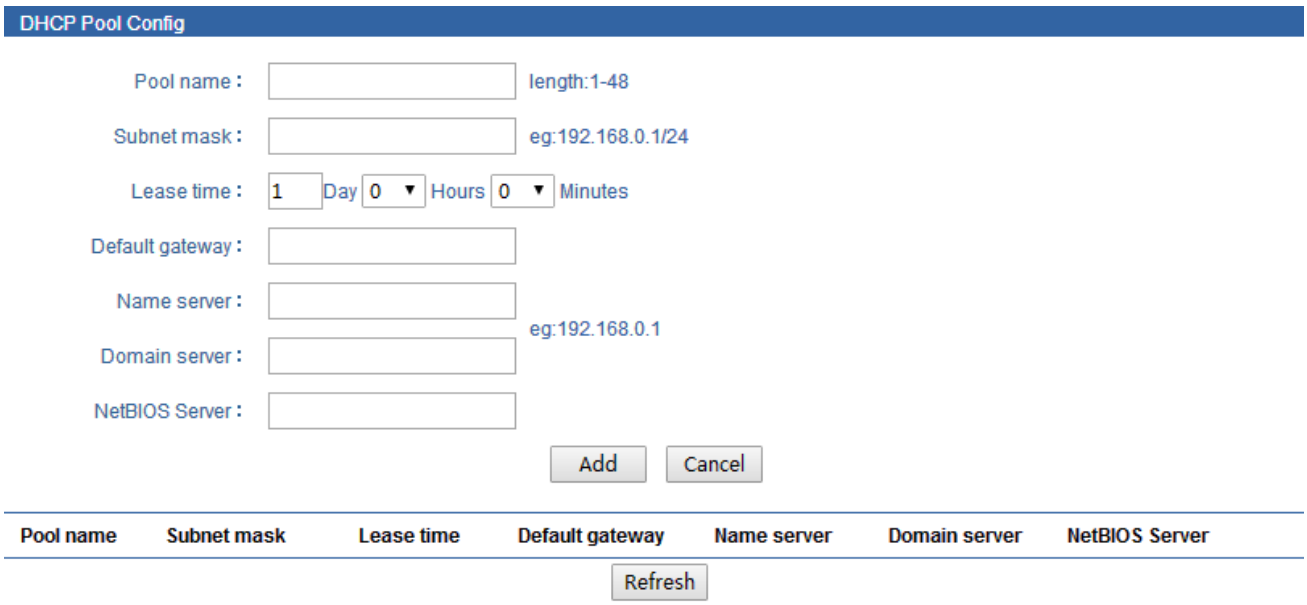
In the menu bar in order to click on the main menu, advanced configuration, DHCP Server configuration, DHCP Server configuration to enter the DHCP Server configuration interface, the interface can enable / disable DHCP Server.



（Figure 6.8.5.1）

6.8.5.2 DHCP pool configuration

In the menu bar, click "main menu", "advanced configuration" and "DHCP server configuration", "address pool configuration into the address pool configuration interface, the interface can add, delete address pool and view address pool configuration information.



（Figure 6.8.5.2）

Configuration item	meaning
Pool name	DHCP Server in the name of the address pool length range of 1~48
Subnet mask	DHCP client can automatically get to the IP
Lease time	DHCP client can automatically get to the address of the effective time. Range for 0-999 days
Default gateway	DHCP client can automatically access to the gateway
DNS address	DHCP client can automatically get to the DNS address
Domain server	DHCP client can automatically get to the domain name
NetBIOS server	DHCP client can automatically get to the NetBIOS server address

Address pool configuration:

Step 1: fill in the name of the address pool in the text box of the name of the address pool;

Step 2: fill in the IP address in the text box of the subnet mask;

Step 3: configure the DHCP client automatically at the lease time to get to the address of the valid time;

Step 4: fill in the IP address in the text box of the default gateway;

Step 5: fill in the IP address in the text box of the DNS server;

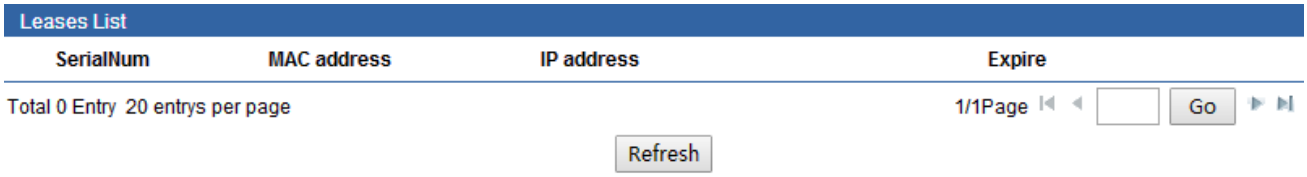
Step 6: fill in the IP address in the text box of the domain name service;

Step 7: fill in the IP address in the text box of the NetBIOS server;

Step 8: click the "add" button.

6.8.5.3 Leases list

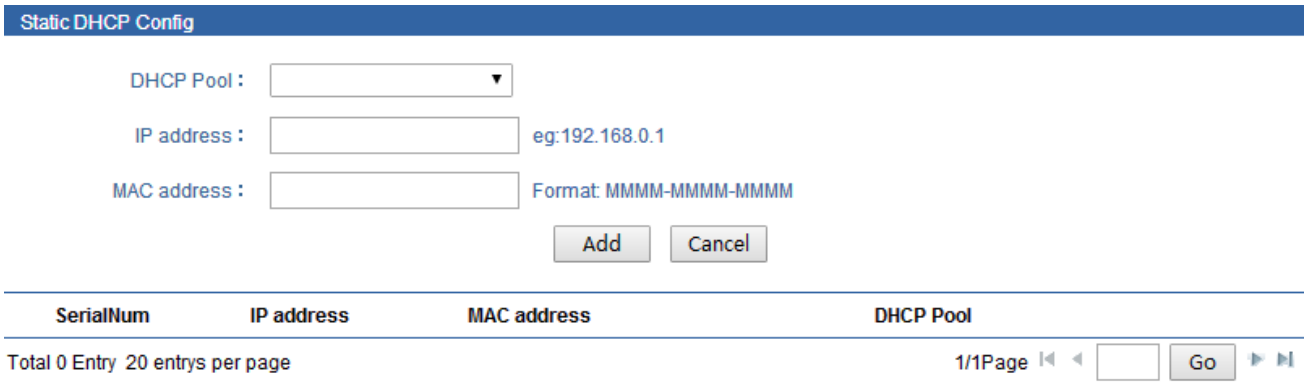
In the menu bar in order to click on the "main menu", "advanced configuration", " DHCP Server configuration", "leases list" into the client list interface, the interface to view the DHCP client information.



（Figure 6.8.5.3）

6.8.5.4 Static leases configuration

Through the MAC address of the client and the DHCP Server assigned to determine the address of the client each time from the server to get the address is bound to the IP address.



（Figure 6.8.5.4）

Static client configuration steps:

Step 1: select the address pool name in the drop-down box in the DHCP Pool;

Step 2: fill in the IP address of the text box to be assigned to the client's IP address;

Step 3: in the MAC address of the text box to fill in the MAC address of the client;

Step 4: click the "add" button.

6.8.5.5 Port binding configuration

In the menu bar in order to click on the "main menu", "advanced configuration", "DHCP Server configuration", "port address binding configuration" into the port address binding configuration interface.

（Figure 6.8.5.5）

Port address binding configuration step:

Step 1: select the address pool name in the drop-down box in the DHCP Pool;

Step 2: select the port you want to bind in the drop - down box on the port;

Step 3: fill in the IP address of the text box to be assigned to the client's IP address;

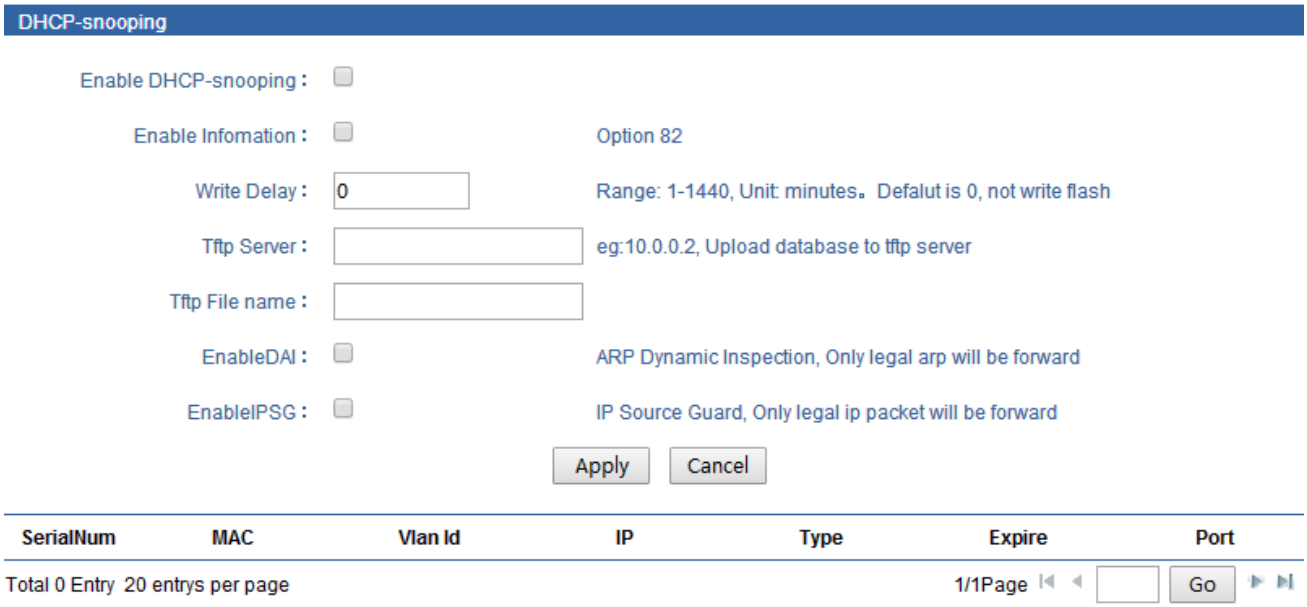
Step 4: click the "add" button.

6.8.6 DHCP-snooping

DHCP-Snooping that is the layer 2 of DHCP service monitoring function, open the DHCP-Snooping function, the device can be extracted from the received DHCP-ACK and DHCP-REQUEST messages and record the IP address and MAC address information.

6.8.6.1 Global configuration

In the menu bar, click "main menu", "advanced configuration", "DHCP- snooping configuration", "global configuration" to enter the DHCP- snooping global configuration interface.



（Figure 6.8.6.1）

Global configuration step:

Step 1: select the check box in the DHCP-Snooping enabled check box;

Step 2: check the Information enabled check box;

Step 3: fill in the delay time in the write delay box;

Step 4: write the Tftp server box to fill in the Tftp server IP address;

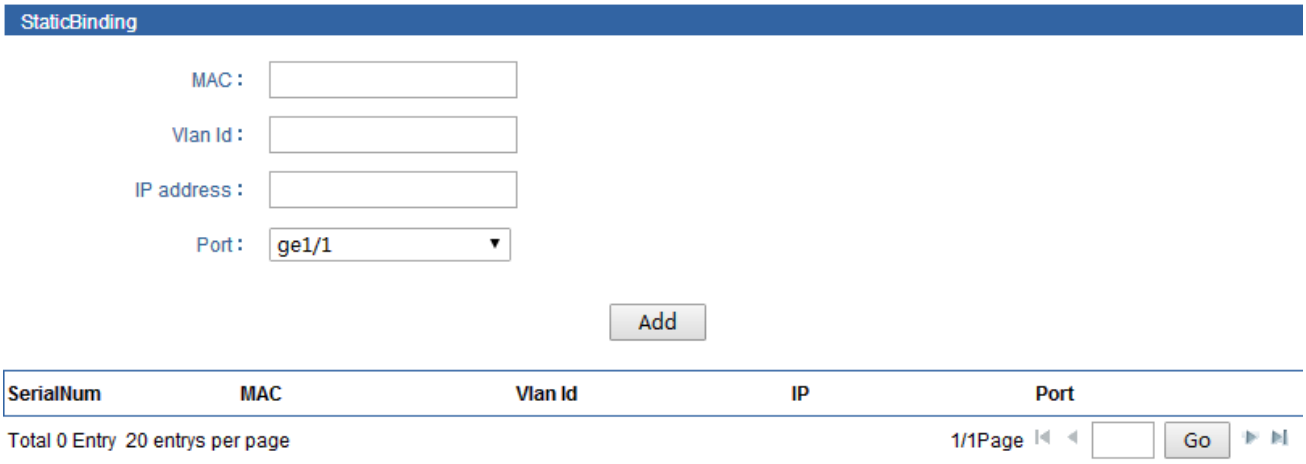
Step 5: write the Tftp file name box to fill in the appropriate file name;

Step 6: select the check box in the DAI enabled check box;

Step 7: select the check box in the IPSG enabled check box;

Step 8: click the "Settings" button.

6.8.6.2 Static binding



（Figure 6.8.6.2）

Static binding step:

Step 1: fill in the MAC address in the MAC text box;

Step 2: fill in the Vlan Id text box Vlan Id;

Step 3: fill in the IP address in the IP address text box;

Step 4: write the Tftp server box to fill in the Tftp server IP address;

Step 5: write the Tftp file name box to fill in the appropriate file name;

Step 6: select the port in the port selection bar;;

Step 7: click the "add" button.

6.8.6.3 Port configuration

DHCP-Snooping trust function, can provide users with further security assurance

DHCP-Snooping trust function can control the DHCP server response message source, in order to prevent the possible existence of counterfeit or illegal DHCP server in the network to distribute IP address and other configuration information to other hosts.

DHCP-Snooping trust feature port is divided into the port of trust and distrust:

A trusted port is a port that is directly or indirectly connected to a legitimate DHCP server. Trust port on the received DHCP message normal forwarding, thus ensuring the DHCP client to get the correct IP address.

Distrust ports are ports that are not connected to the legitimate DHCP server. The DHCP-ACK, DHCP-NAK, and DHCP-OFFER packets that are received by the DHCP server in response to the never trusted port will be discarded, thus preventing the DHCP client from getting the wrong IP address.

Port Config

PortName	Trust	Trust-DAI	Trust-IPSG	Policy(Op82)	Circuit-type	Circuit-id	Remote-type	Remote-id
ge1/1				Replace	Normal		Normal	
ge1/2				Replace	Normal		Normal	
ge1/3				Replace	Normal		Normal	
ge1/4				Replace	Normal		Normal	
ge1/5				Replace	Normal		Normal	
ge1/6				Replace	Normal		Normal	
ge1/7				Replace	Normal		Normal	
ge1/8				Replace	Normal		Normal	
ge1/9				Replace	Normal		Normal	
ge1/10				Replace	Normal		Normal	
ge1/11				Replace	Normal		Normal	
ge1/12				Replace	Normal		Normal	
ge1/13				Replace	Normal		Normal	

（Figure 6.8.6.3）

Port configuration steps:

Step 1: in the corresponding port after the Trust check box check box;

Step 2: in the corresponding port after the Trust-DAI check box check box;

Step 3: in the corresponding port after the Trust-IPSG check box check box;

Step 4: in the corresponding port after the Policy (Op82) drop-down box selection;

Step 5: select the Circuit-type drop-down box at the end of the corresponding port;

Step 6: fill in ID in the Circuit-id text box in the corresponding port;

Step 7: select the Remote-type drop-down box at the end of the corresponding port;

Step 8: fill in ID in the Remote-id text box in the corresponding port;

Step 9: click the "Apply" button.

6.8.7 DHCP Relay configuration

DHCP is only applicable to the DHCP client and server in the same subnet as the broadcast mode is used to send the request message in the dynamic acquisition process of the IP address. For the dynamic host configuration, need to set up a DHCP server in all segments, which is obviously not the economy.

DHCP relay function is introduced to solve this problem: a client can by DHCP relay and other segments of the DHCP server communication, and ultimately get to the IP address. In this way, the DHCP client on the network can use the same DHCP server, which not only saves the cost, but also is convenient for centralized management.

DHCP Relay Config

Interface eth0

Helper-address eg:192.168.1.1

Add Cancel

Interface	Helper-address

Total 0 Entry 20 entrys per page 1/1Page Go

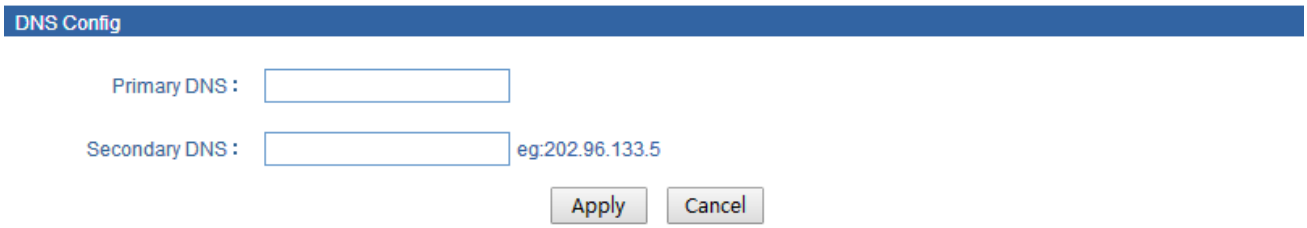
（Figure 6.8.7）

Help-address: relay IP address

6.8.8 DNS configuration

DNS, Domain Name System. DNS to help users find the path on the internet. Every computer on the Internet has a unique address, called "IP" ". IP address (as a string of digits) is not convenient memory, DNS allows users to use a string of common letters (domain name) to replace.

In the menu bar in order to click on the "main menu", "advanced configuration", "DNS configuration" into the DNS configuration interface, the interface can be configured with the main DNS and standby DNS.



（Figure 6.8.8）

DNS configuration steps:

Step 1: fill in the main DNS;

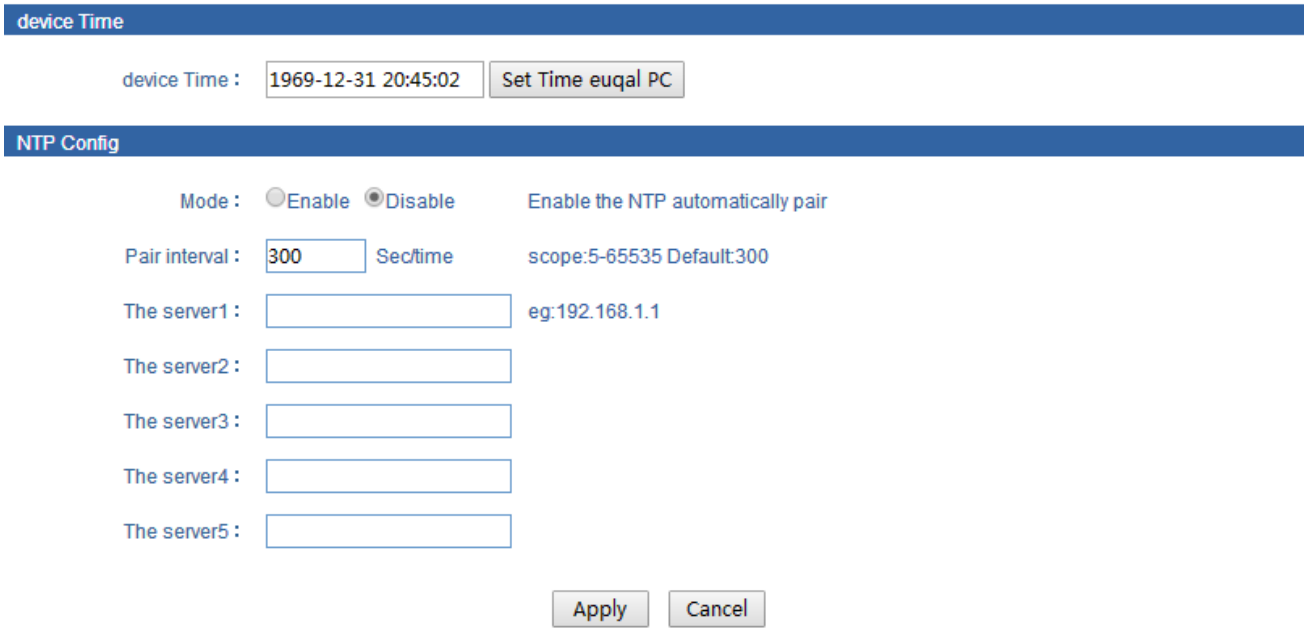
Step 2: fill in the backup DNS;

Step 3: click "Apply".

6.8.9 NTP configuration

NTP: Network Time Protocol. It is designed to deliver uniform and standard time on the Internet. The specific implementation scheme is on the network specifies several clock source web site, to provide users with timing services and between these sites should can compare, improve the time accuracy.

In the menu bar in order to click on the "main menu", "advanced configuration", "NTP settings" to enter the NTP settings interface.



（Figure 6.8.9）

Intellisystem Technologies S.r.l.
Via Augusto Murri, 1 – 96100 Siracusa - Phone +39 (0)931-1756256 / +39 (0)2-87167549 - Mobile (+39) 335 1880035
em@il: info@intellisystem.it WEB: http://www.intellisystem.it

NTP server configuration step:

Step 1: select the checkbox to enable or disable in the mode of the;

Step 2: in the time interval of the text box to fill in time interval;

Step 3: fill in the IP address in the text box of the server 1~5;

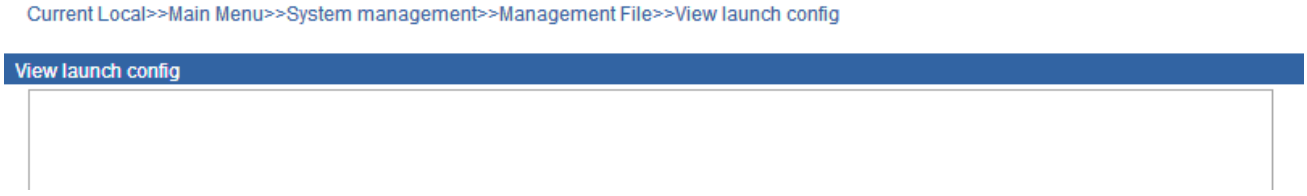
Step 4: click the "Apply" button.

6.9 System management

6.9.1 Management File

6.9.1.1 View launch configuration

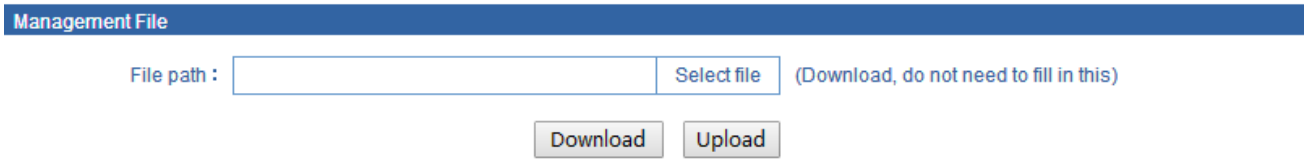
In the menu bar in order to click on the "main menu", "system management ", " management file ", "view launch configuration" to enter the start configuration interface, the interface can view the current configuration information.



（Figure 6.9.1.1）

6.9.1.2 Management file

In the menu bar in order to click on the "main menu", "system management", "management file ", "management file " into the configuration file management interface, the interface can be downloaded, uploaded profile.



（Figure 6.9.1.2）

Download the configuration file:

Step 1: enter the configuration file management"

Step 2: "download" button.

Upload configuration file:

Step 1: enter the configuration file management"

Step 2: click "select file"

Step 3: click the "Browse" button, select the location of the file to upload.

Step 4: click the "Upload" button.

After the completion of the update will automatically open a new page to the "system state".

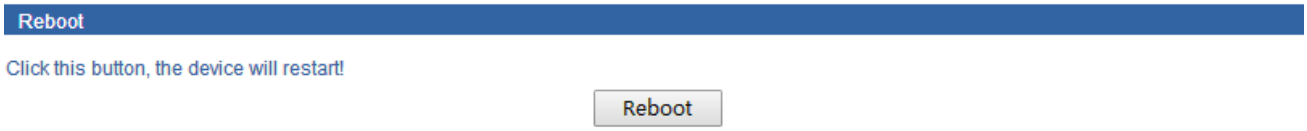
6.9.2 Save

In the menu bar, click on the "main menu", "system management", "save" to enter the storage configuration interface

（Figure 6.9.2）

6.9.3 Reboot

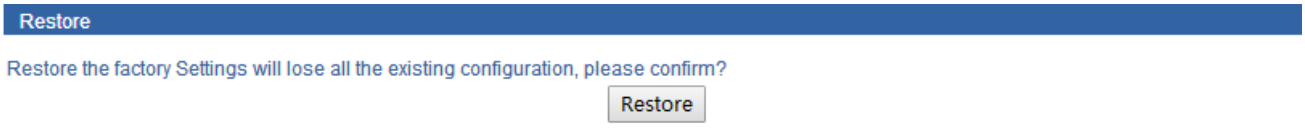
In the menu bar, click on the "main menu", "system management", "Reboot" to reset the settings interface.



（Figure 6.9.3）

6.9.4 Restore

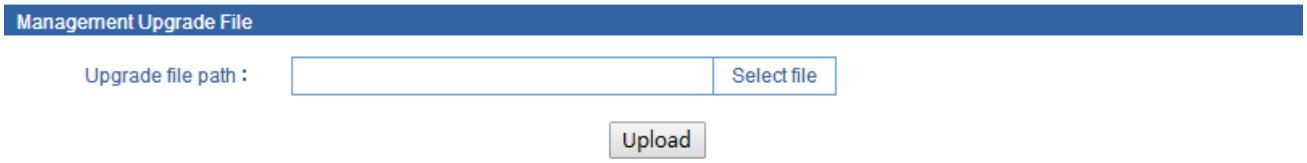
In the menu bar in order to click on the "main menu", "system management", "restore" to restore the factory settings interface.



（Figure 6.9.4）

6.9.5 Firmware

In the menu bar, click "main menu", "system management", "firmware" to enter the online upgrade interface.



（Figure 6.9.5）

Online upgrade steps:

Step 1: click on the "select file" tab.

Step 2: click the "Browse" button, select the location of the file to upload.

Step 3: click the "Upload" button.

1, The upgrade process is prohibited without power, after the confirmation began to burn and write flash.

2, After the completion of the upgrade will automatically open a new page to the system state.

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.intellisystem.it

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.

7.3 Repair or Replace

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

Appendix 1 Glossary table

	Glossary	Description
A	ARP (Address Resolution Protocol)	An IP address to physical address protocol
	Auto-Negotiation	Switches at both ends of the device in accordance with the maximum performance to auto-negotiate the speed and duplex mode
B	Broadcast Storm	A port send excessive broadcast frame meantime on the network, accumulate the respond to send messages on the network , consume too much network resources or cause the network timeout
	Broadcasting	A forwarding way send data to all branch of network
C	CoS （Class of Service）	namely 802.1p priority program, CoS offer a way for data packets to join priority tag, classify packets into 8 level with the value 0~7 range
D	DHCP （ Dynamic Host Configuration Protocol）	Information for the network to assign dynamically IP address, subnet mask and gateway
	DSCP （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.

Intellisystem Technologies S.r.l.
Via Augusto Murri, 1 – 96100 Siracusa - Phone +39 (0)931-1756256 / +39 (0)2-87167549 - Mobile (+39) 335 1880035
em@il: info@intellisystem.it WEB: http://www.intellisystem.it

	IEEE 802.1q	Define the VLAN bridge operation. To manage ,define and operate VLAN on the bridge LAN
Q	QoS (Quality of Service）	A technology to resolve the network delay and block problems and so on.
T	Trunking	To make an aggregated group tied up a group of ports together to increase bandwidth and improve the connection reliability.
	ToS （Type of Service）	Packaged in IP packet header of 8 bit domain to perform the different priority packets
U	UDP （ User Datagram Protocol）	Face to disconnected unreliable transmission layer protocol
	UTP (Unshielded Twisted Pair)	Not shielded media out of twisted pair

Appendix 2 Treatment of common problem

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

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

2. How to do if you forgot password?

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

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

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

4. What kind of alarms will be informed to technical except displayed on the management software?

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

5. Why cannot increase the bandwidth after configured trunking?

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

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

When some of ports 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.