Managed Industrial Fiber Switch

HGW series

Web GUI User’s Manual

Industrial Ethernet Switch
Industrial Ethernet Switch
Industrial Ethernet Switch

www.robofiber.com

ROBOfiber, Inc.
3000F Danville Blvd., Ste 300
Alamo, CA 94507 USA
Tel/Fax: +1-(503)-764-1458
Toll-free: 888-27-FIBER (US only)
www.robofiber.com
sales@robofiber.com

Legal

The information in this publication has been carefully checked and is believed to be entirely accurate at the time of publication. ROBOfiber assumes no responsibility, however, for possible errors or omissions, or for any consequences resulting from the use of the information contained herein. ROBOfiber reserves the right to make changes in its products or product specifications with the intent to improve function or design at any time and without notice and is not required to update this documentation to reflect such changes. ROBOfiber makes no warranty, representation, or guarantee regarding the suitability of its products for any particular purpose, nor does ROBOfiber assume any liability arising out of the application or use of any product and specifically disclaims any and all liability, including without limitation any consequential or incidental damages.

ROBOfiber products are not designed, intended, or authorized for use in systems or applications intended to support or sustain life, or for any other application in which the failure of the product could create a situation where personal injury or death may occur. Should the Buyer purchase or use a ROBOfiber product for any such unintended or unauthorized application, the Buyer shall indemnify and hold ROBOfiber and its officers, employees, subsidiaries, affiliates, and distributors harmless against all claims, costs, damages, expenses, and reasonable attorney fees arising out of, either directly or indirectly, any claim of personal injury or death that may be associated with such unintended or unauthorized use, even if such claim alleges that ROBOfiber was negligent regarding the design or manufacture of said product.

TRADEMARKS

Microsoft is a registered trademark of Microsoft Corp.

HyperTerminal™ is a registered trademark of Hilgraeve Inc.

WARNING:

This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual may cause harmful interference in which case the user will be required to correct the interference at his own expense. NOTICE: (1) The changes or modifications not expressively approved by the party responsible for compliance could void the user's authority to operate the equipment. (2) Shielded interface cables and AC power cord, if any, must be used in order to comply with the emission limits.

CISPR PUB.22 Class A COMPLIANCE:

This device complies with EMC directive of the European Community and meets or exceeds the following technical standard. EN 55022 - Limits and Methods of Measurement of Radio Interference Characteristics of Information Technology Equipment. This device complies with CISPR Class A.

CE NOTICE

Marking by the symbol CE indicates compliance of this equipment to the EMC and LVD directives of the European Community. Such marking is indicative that this equipment meets or exceeds the following technical standards: EN 55022:2006, Class A, EN55024:1998+A1:2001+A2:2003, and EN60950-1:2001

Contents

Note:

This manual includes all models from the HGW managed series as below:

HGW-802SM Gigabit Ethernet Switch 8x 10/100/1000Base-Tx +2x 100/1000Base-X SFP slot ports

HGW-1604SM Gigabit Ethernet Switch 16x 10/100/1000Base-Tx +4x 100/1000Base-X SFP slot ports

HGW-802SM-PSE Gigabit Ethernet Switch 8x 10/100/1000Base-Tx +2x 100/1000Base-X SFP slot ports, 240W available PoE budget

HGW-1604SM-PSE Gigabit Ethernet Switch 16x 10/100/1000Base-Tx +4x 100/1000Base-X SFP slot ports, 480W available PoE budget

HGW-1608SM-PSE Gigabit Ethernet Switch 16x 10/100/1000Base-Tx +8x 100/1000Base-X SFP slot ports, 480W available PoE budget

Chapter 1 Preparation for Configuration

This chapter describes the configuration preparation in detail, including：

- WEB Login
- WEB Configuration
- Device Setting Information

1.1 WEB Login

The system default IP is 192.168.1.6. Please make sure the following notes before login:

- Make sure the management PC IP address is in the same network segment as the switch IP address. Otherwise, the switch management IP address of the switch cannot be accessed.
- Make sure that the ports connected between PC and switch are non-aggregated ports
- WEB browser is IE8 or above

Login Step

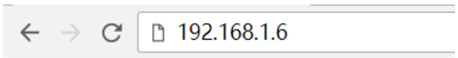
1．Open the browser on your PC

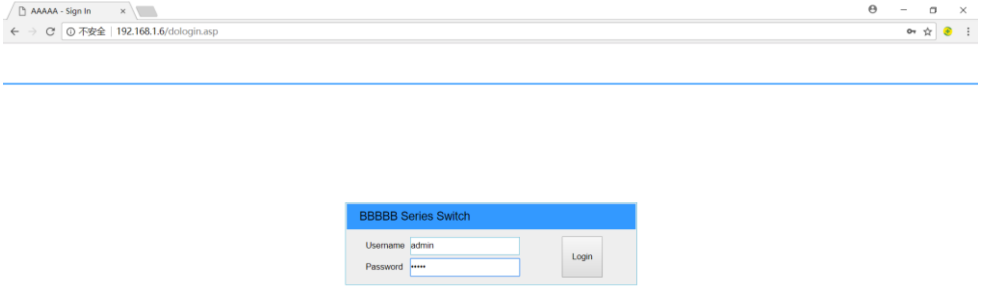
2．Enter the device IP address (default is 192.168.1.6) and press Enter to go for the Web Login Interface, as shown in Figure 1.1

3. Enter username and password

4. Select the language

5. Click <Login> to enter the web configuration interface


192.168.1.6


AAAAA - Sign In

不安全 | 192.168.1.6/dologin.asp

BBBBB Series Switch

Username admin

Password •••••

Figure 1.1 Device Web Login

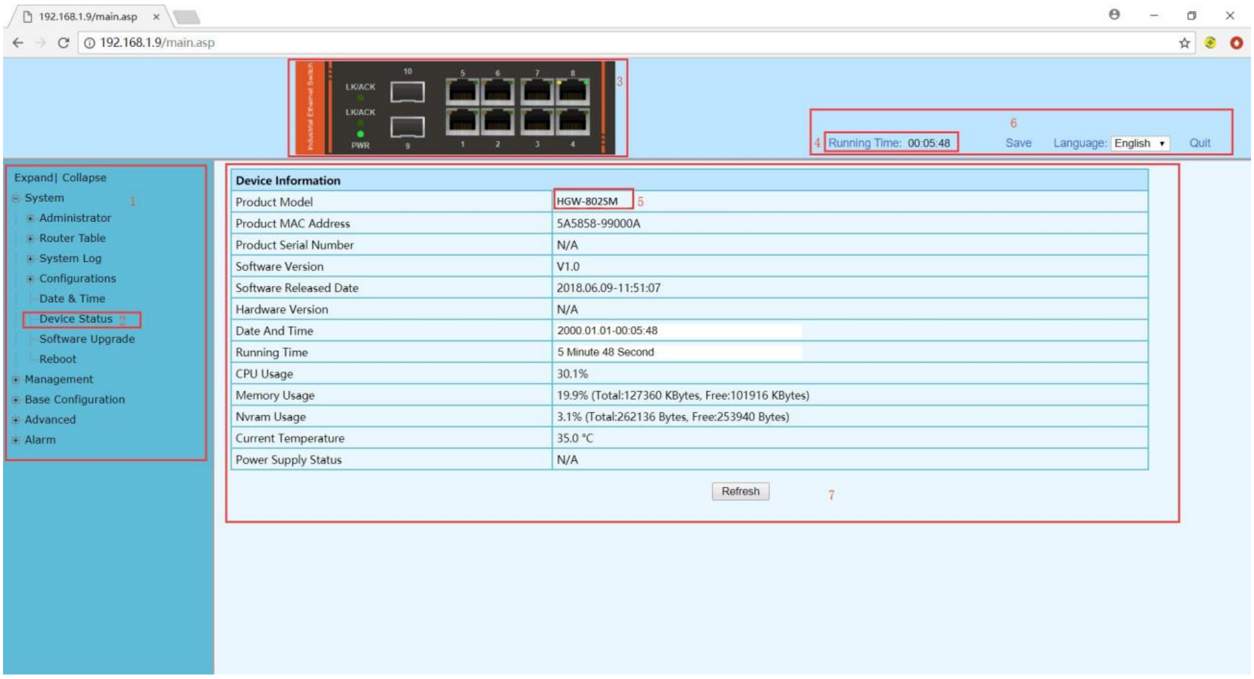
Table 1.1 Web Login Configuration Description

Item	**Description**
Username	Enter the username, default username is admin
Password	Enter the password, default user password is admin
Language	Language display: ●Auto: Select the display mode based on system language automatically (default) ●Chinese: Select Chinese as display ●English: Select English as display Remark: Only support Chinese and English languages.

1.2 WEB Configuration

1.2.1 WEB Configuration

Web Configuration Interface, Figure1.2.



Running Time: 00:05:48

Language: English

Device Information	
Product Model	HGW-802SM
Product MAC Address	5A5858-99000A
Product Serial Number	N/A
Software Version	V1.0
Software Released Date	2018.06.09-11:51:07
Hardware Version	N/A
Date And Time	2000.01.01-00:05:48
Running Time	5 Minute 48 Second
CPU Usage	30.1%
Memory Usage	19.9% (Total:127360 KBytes, Free:101916 KBytes)
Nvram Usage	3.1% (Total:262136 Bytes, Free:253940 Bytes)
Current Temperature	35.0 °C
Power Supply Status	N/A

Figure 1.2 Web Configuration Interface

1. Navigation Bar 2. Selected Page 3. Device Panel 4. Device Operation Time

5. Device Model 6. Common Functions 7. Configuration Page

Web configuration interface description as Table 1.2

Configuration Interface	Description
Navigation Bar	The menu bar where you can find and turn to any of the implemented configuration pages
Selected Page	The current position of configuration page in the navigation bar
Device Panel	The enabling and connection status of each interface
Device Operation Time	The running time after the device powered on
Device Model	The current device model
Common Functions	● Muti-language: Select the interface language ●Save: Save the current configuration to the configuration file (no color changes indicate no configuration to save, and flashing color indicates that there is a configuration that needs to be saved) ●Exit: Exit the Web Configuration Interface
Configuration Page	The main page to be configured

Table 1.2 Web Configuration Interface Description

1.2.2 Device Panel

You can view the enabling and connection status of each interface via the device panel, as shown in Figure 1.3.

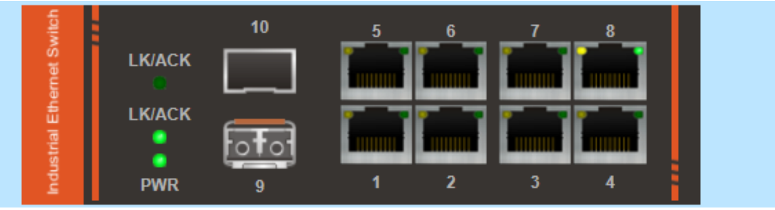
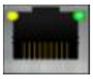


Figure 1.3 Device Panel

Please check Table 1.3 for the Device Panel Interface Description.

Table 1.3 Device Panel Interface Description

Port	Instructions
	Copper Port, Enabled, Connected

	Copper Port, Enabled, not Connected
	Fiber Port, Enabled, Connected
	Fiber Port, Enabled, not Connected

1.2.3 Common Buttons

The common button description of the device configuration interface is shown in Table 1.4.

Table 1.4 Buttons on the Device Configuration Screen

Buttons	Instructions
Expand	Expand all pages in the navigation bar, or expand all port information
Collapse	Close all pages in the navigation bar or close all port information.
Apply	Configure the application to the system
Refresh	Refresh the interface information
Add	Add a new item
Modify	Modify the selected item
Delete	Delete the selected item
Prev	Return to the previous page
Next	Go to the next page
Go	Skip to the specified page
Home	Skip to the home page
Tail	Skip to the last page
Apply	The configuration is applied to the system
Cancel	Cancel the configuration
Clean	Clear the specified port information
Save	Save system configuration

Quit	Exit the interface, and return to the login interface

1.2.4 Save Configuration

1. After the configuration is complete, click [Apply] to configure the application to the system. It is only stored in memory, but not saved in the configuration file. If you do not press [Save], the configuration operation will be lost after the device is powered off or restarted.

2. After all configurations are completed, please click [Save]. The configuration saved in the configuration file will not be lost after the device is powered off or restarted.

1.2.5 Exit the Web Configuration Interface

1. After completing the configuration on the web interface, press [Save] first to avoid loss of configuration. Then click [Exit] to exit the Web configuration interface.

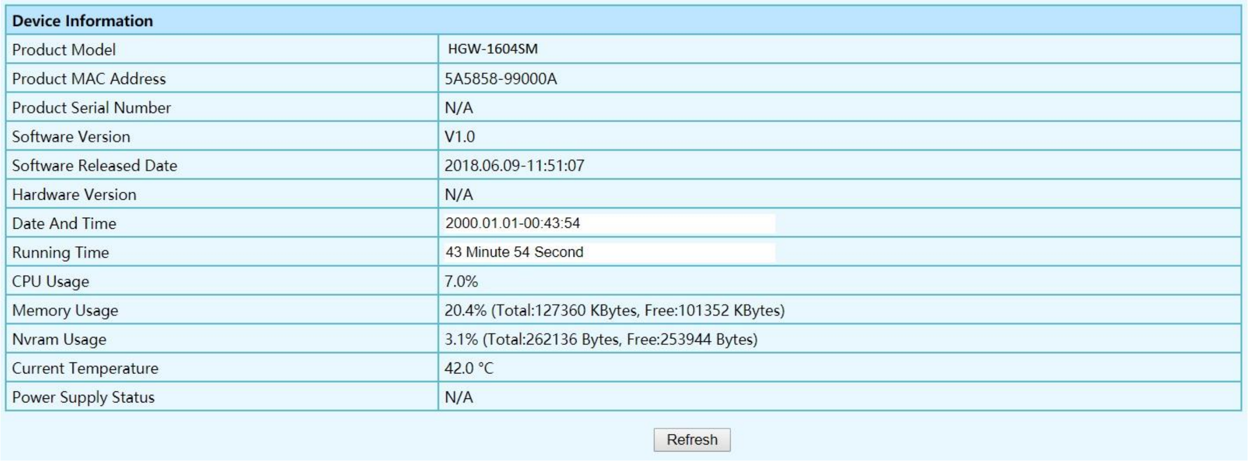
2. Directly closing the browser cannot exit the Web configuration interface. If not time out during the next login, the user can directly enter the Web configuration interface.

1.3 Device Information

Configuration Steps

1. Select the first page in the navigation bar to enter the [System / Status Information] interface. Different devices have different model number, the link name in the first line of the navigation bar will also be different, for example, HGW-1604SM, etc.

2. In the [Device Status] interface, the basic information and the operating status information of the device system are displayed, as shown in figure 1.4.



Device Information	
Product Model	HGW-1604SM
Product MAC Address	5A5858-99000A
Product Serial Number	N/A
Software Version	V1.0
Software Released Date	2018.06.09-11:51:07
Hardware Version	N/A
Date And Time	2000.01.01-00:43:54
Running Time	43 Minute 54 Second
CPU Usage	7.0%
Memory Usage	20.4% (Total:127360 KBytes, Free:101352 KBytes)
Nvram Usage	3.1% (Total:262136 Bytes, Free:253944 Bytes)
Current Temperature	42.0 °C
Power Supply Status	N/A

Table-1.4 Product Information Interface

Configuration Description

Table 1.4 [Device Status] Configuration Description

Item	Description
Device Model	The device model, For Example: HGW-802SM
MAC Address	The device MAC address
Part Number	The device product serial number
Software Version	The current software version running on switch
Software Release Date	The date of release for the running software
Hardware Version	The hardware version of the current device
Date and Time	The device system date and time
Operation Hours	The system running time (since power-up)
CPU Usage	The system's CPU usage.
Memory Usage	The memory usage of the system
Configuration Usage	Configuration space usage of the system

Chapter 2 Ports

This chapter describes the port configuration in detail, including the following:

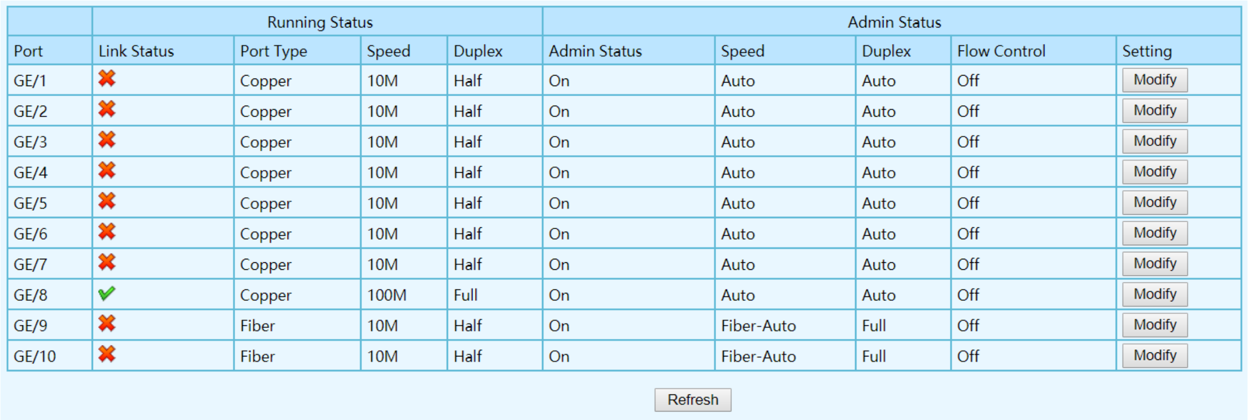
- Port Configuration
- Port Statistics

2.1 Port Configuration

Configuration Steps

1. Select [Base Configuration / Ports / Status and Setting] in the navigation bar to enter the [Status and Setting] interface.

2. The Status and Settings interface (Figure 2.1) shows the operating status and configuration information for each port.



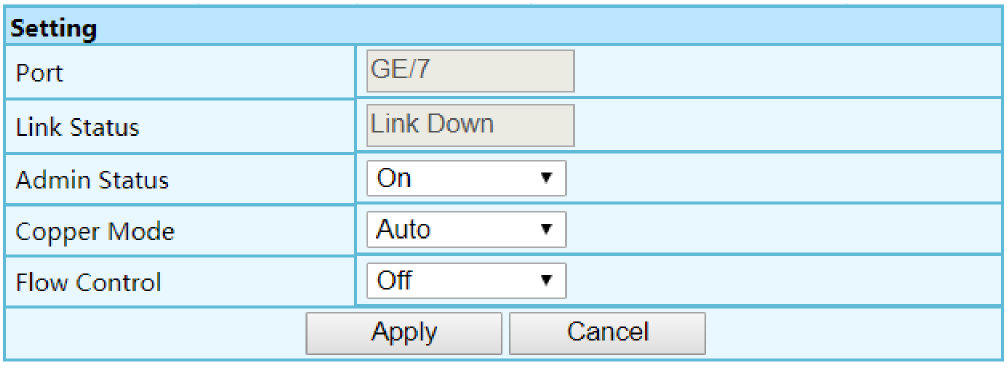
	Running Status				Admin Status				
Port	Link Status	Port Type	Speed	Duplex	Admin Status	Speed	Duplex	Flow Control	Setting
GE/1	✗	Copper	10M	Half	On	Auto	Auto	Off	Modify
GE/2	✗	Copper	10M	Half	On	Auto	Auto	Off	Modify
GE/3	✗	Copper	10M	Half	On	Auto	Auto	Off	Modify
GE/4	✗	Copper	10M	Half	On	Auto	Auto	Off	Modify
GE/5	✗	Copper	10M	Half	On	Auto	Auto	Off	Modify
GE/6	✗	Copper	10M	Half	On	Auto	Auto	Off	Modify
GE/7	✗	Copper	10M	Half	On	Auto	Auto	Off	Modify
GE/8	✓	Copper	100M	Full	On	Auto	Auto	Off	Modify
GE/9	✗	Fiber	10M	Half	On	Fiber-Auto	Full	Off	Modify
GE/10	✗	Fiber	10M	Half	On	Fiber-Auto	Full	Off	Modify

Figure 2.1 Port Status and Settings Interface

Table 2.1 Port Configuration Description

Item	Description
Port	The name and number of the port
Connection Status	✓ Indicates that the port is connected ✗ Indicates that the port is disconnected or unconnected
Port type	Copper or Fiber Port
Rate	The port working speed, unconnected port is always displayed as 10M
Duplex Mode	The port working duplex mode, the unconnected port always shows half duplex

3. If you need to modify the configuration of a port, just click the [Modify] on the right-side corresponding entry as shown in Figure 2.2 to enter the edit interface and modify the available configuration items. Click the [Apply] to complete the modifications or click the [Cancel] to cancel the modifications.



Setting	
Port	GE/7
Link Status	Link Down
Admin Status	On
Copper Mode	Auto
Flow Control	Off

Figure 2.2 Port Configuration

Management Status - Configuration Item Description

Table 2.2 Configuration Item Description on the Settings

Item	Range	Description
Management Status	Close Open Default: open	Turn off / on the port. In the closed state, the connection / disconnection state is link down; in the open state, the connection state is link up.
Speed and Duplex Mode	10M half 10M full 100M half 100M full 1000M Automatic Default: Auto negotiation	The configurable port duplex and rate, such as 10M / 100M / 1000M / Auto, etc bandwidth. It allows only one communication in half-duplex mode and simultaneous two-way communication in full-duplex mode.
Flow Control	Close Open Default: Off	The Layer 2 port flow control function can effectively prevent network congestion when turned on. Flow control is a peer-to-peer function. It is implemented by pause frames. When the ports of the PVRP system are enabled, the peer port must be also enabled.

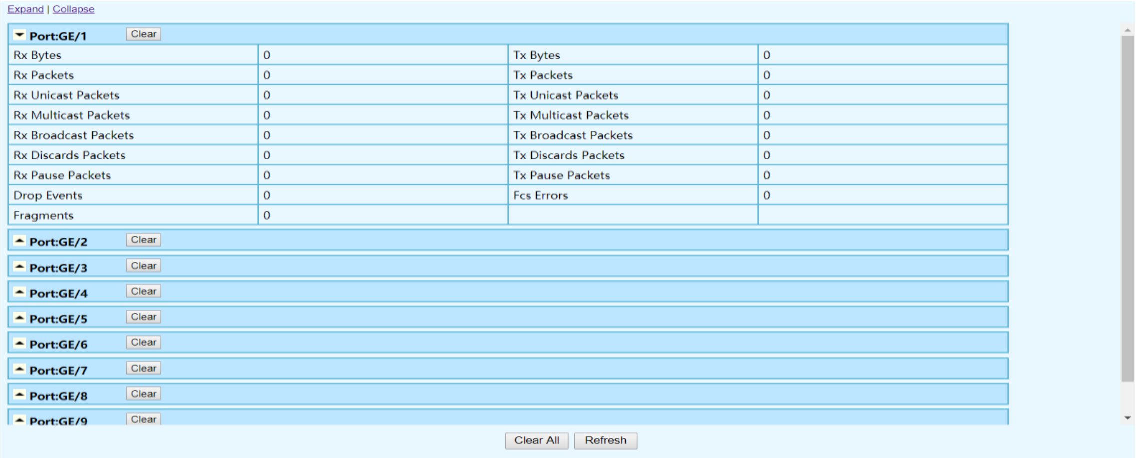
2.2 Port Statistics

Configuration Steps

1. Select [Base Configuration / Ports / Statistics] to enter the port [Statistics] page (as Figure 2.3).

2. The [Statistics] shows each port statistical information. You can expand corresponding port statistics by clicking ▲ flag on the left of port entry and click cleared button on the right to clear the statistics of the port.

3. Click the [Refresh] to update the statistics of all ports. Click [Clear All] to clear the statistics for all ports.



Rx Bytes	0	Tx Bytes	0
Rx Packets	0	Tx Packets	0
Rx Unicast Packets	0	Tx Unicast Packets	0
Rx Multicast Packets	0	Tx Multicast Packets	0
Rx Broadcast Packets	0	Tx Broadcast Packets	0
Rx Discards Packets	0	Tx Discards Packets	0
Rx Pause Packets	0	Tx Pause Packets	0
Drop Events	0	Fcs Errors	0
Fragments	0		

Table 2.3 Port Statistics Information

Table 2.2 Port Statistics Type

Port Statistics Type	**Description**
Rx / Tx **Bytes**	Total received / sent bytes
Rx / Tx Packets	Total received / sent packets
Rx / Tx Unicast Packets	Total received / sent unicast packets
Rx / Tx Multicast Packets	Total received / sent multicast packets
Rx / Tx Broadcast Packets	Total received / sent broadcast packets
Rx / Tx Discards Packets	Total received / sent discarded packets
Rx / Tx Pause Packets	Total received / sent flow control packets
Drop Events	Drop messages (interval sampling)
FCS Errors	FCS error packet
Fragments	Fragment packets (less than 64 bytes)

Chapter 3 FDB Table

This chapter describes the FDB Table in detail, including of the following:

● Base Configuration

● FDB Table

● Delete

3.1 Base Configuration

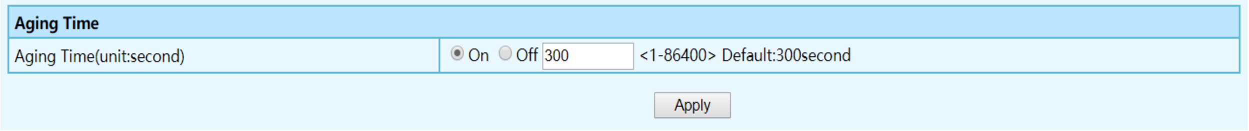
3.1.1 Aging time

Configuration steps

1. Select [Base Configuration / FDB Table / Configuration / Aging Time] to enter the [Aging Time] interface.

2. The aging time related configuration of the FDB Table can be viewed in the [Aging Time] interface.

3. If you need to modify the aging time configuration of the FDB Table, you can modify the corresponding configuration in the aging time configuration box and click [Apply], as shown in Figure 3.1.



Aging Time

Aging Time(unit:second) ● On ○ Off 300 <1-86400> Default:300second

Figure 3.1 Aging Time Configuration

Configuration Description

Table 3.1 The FDB Table [Aging Time] Configuration Description

Configuration Item	Description
Aging time	The FDB Table aging time can be configured via the radio button. ● Enable: The aging time is on. Range 1-86400 seconds, default value 300 seconds. ● Close: The FDB Table never aging, but the system resetting could clear the dynamic forwarding entries. ● Note: Default with Enable, 300 seconds.

3.1.2 Static MAC

Configuration Steps

1. Select [Base Configuration / FDB Table / Configuration / Static MAC Entry] to enter the [Static MAC Entry] configuration interface.

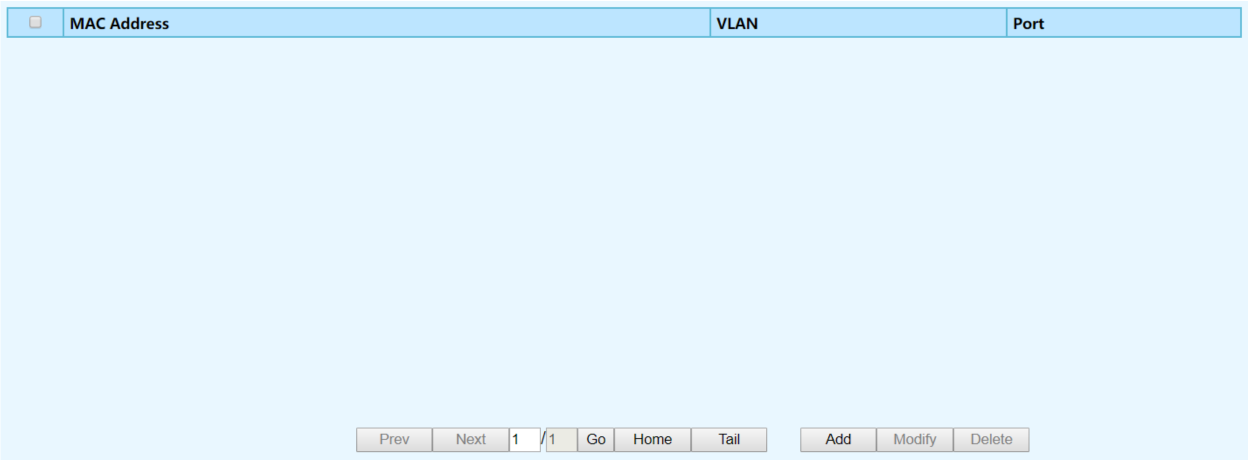
2. On FDB Table [Static MAC Entry] interface, you can view the static MAC related configuration information of FDB Table, as shown in Figure 3.2.

3. If add a new static MAC address, click [Add] to enter the Static MAC configuration interface. Fill in the corresponding configuration items and click [Apply] to complete the addition. There will be prompts if the configuration item is filled in incorrectly.

4. If modify the static MAC address, select the corresponding static MAC address and click [Modify] to enter

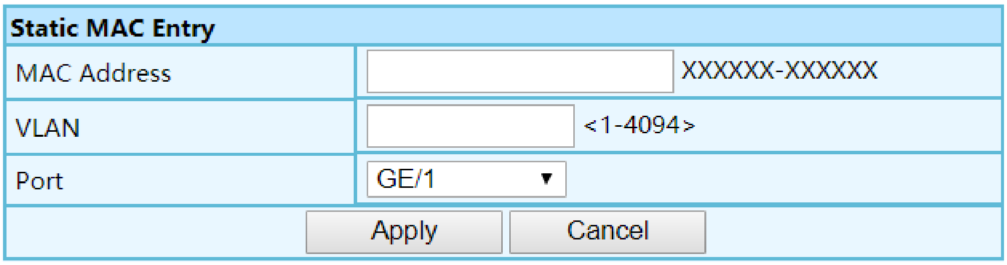
[Static MAC Entry] interface. To modify the corresponding configuration item, click [Apply] to complete the modification. There will be prompts if the configuration item is filled in incorrectly.

5. If delete a static MAC, select the corresponding static MAC and click [Delete] to delete the static MAC.



□	MAC Address	VLAN	Port

Figure 3.2 Static MAC Interface



Static MAC Entry

MAC Address	XXXXXX-XXXXXX
VLAN	<1-4094>
Port	GE/1 ▼

Figure 3.2 Static MAC Configuration

Configuration Description

Table 3.2 FDB Table [Static MAC] Configuration Description

Configuration Item	Description
MAC address	A valid unicast MAC address, format XXXXXX-XXXXXX
VLAN	A valid VLAN ID, range 1-4094
Port	Select a specified port

3.1.3 Port Learning Ability

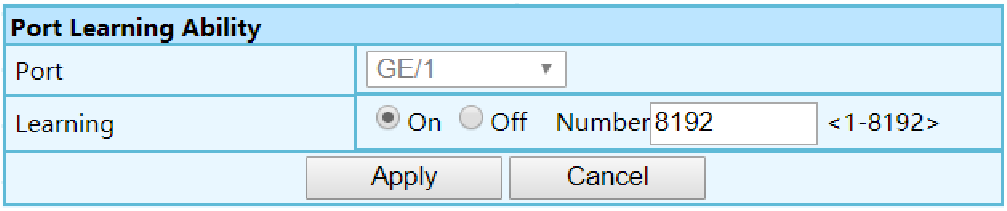
Configuration Steps

1. Select [Base Configuration / FDB Table / Configuration / Port Learning Ability] to enter the [Port Learning Ability] interface.

2. On the FDB Table [Port Learning Ability] interface, you can view the Port Learning Ability related configuration information of FDB Table.

3. To modify the Port Learning Ability configuration, click [Modify] in the corresponding port column to enter the port configuration interface, as shown in Figure 3.3.

4. Select or fill in the configuration items that need to be modified and click [Apply]. There will be prompts if the configuration item is filled in incorrectly.



Port Learning Ability

Port	GE/1
Learning	● On ○ Off Number 8192 <1-8192>

Figure 3.3 Port Learning Ability Configuration

Configuration Description

Table 3.3 FDB Table [Port Learning Ability] Configuration Description

Configuration item	Description
Port	Port name, selected modified port
Learning	Configuration of port learning via radio buttons. Enable: The Port Learning Ability is on. IS3000 / IS2000 series range is 1-8192; Close: Closes the Port Learning Ability. Note: The default is Enable with value 8192.

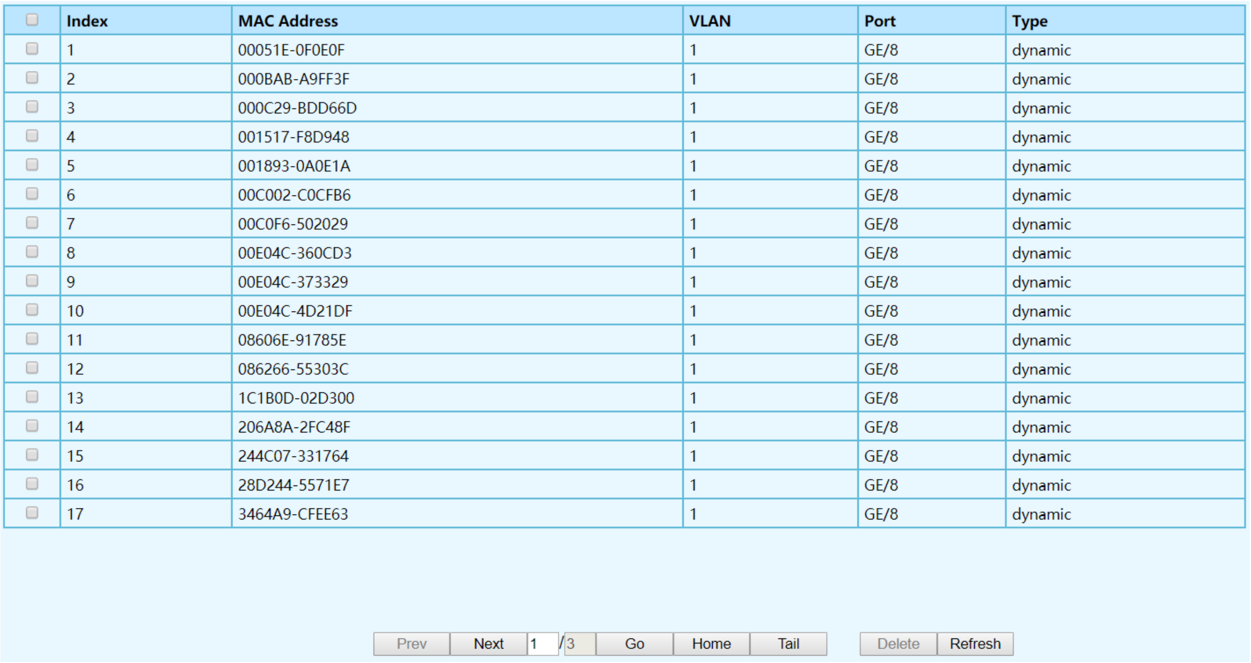
Note: The number of address learning is shared by all ports.

3.2 FDB Table

Configuration Steps

1. Select [Base Configuration / FDB Table / FDB Table] to enter [FDB Table] interface.

2. On the FDB Table interface, you can view the FDB Table information, as shown in Figure 3.4.



□	Index	MAC Address	VLAN	Port	Type
□	1	00051E-0F0E0F	1	GE/8	dynamic
□	2	000BAB-A9FF3F	1	GE/8	dynamic
□	3	000C29-BDD66D	1	GE/8	dynamic
□	4	001517-F8D948	1	GE/8	dynamic
□	5	001893-0A0E1A	1	GE/8	dynamic
□	6	00C002-C0CFB6	1	GE/8	dynamic
□	7	00C0F6-502029	1	GE/8	dynamic
□	8	00E04C-360CD3	1	GE/8	dynamic
□	9	00E04C-373329	1	GE/8	dynamic
□	10	00E04C-4D21DF	1	GE/8	dynamic
□	11	08606E-91785E	1	GE/8	dynamic
□	12	086266-55303C	1	GE/8	dynamic
□	13	1C1B0D-02D300	1	GE/8	dynamic
□	14	206A8A-2FC48F	1	GE/8	dynamic
□	15	244C07-331764	1	GE/8	dynamic
□	16	28D244-5571E7	1	GE/8	dynamic
□	17	3464A9-CFEE63	1	GE/8	dynamic

1 /3

Figure 3.4 FDB Table

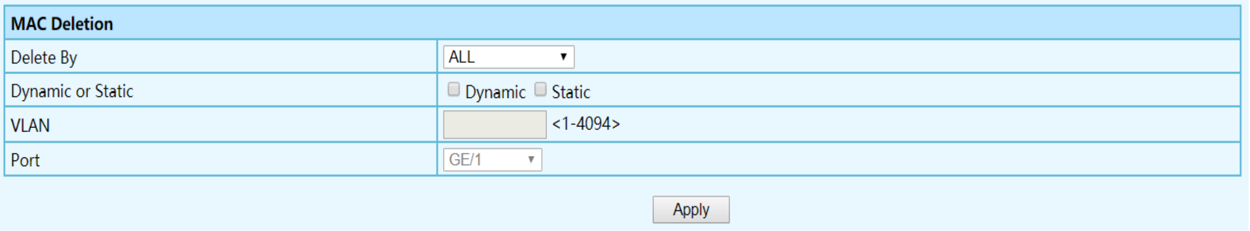
3. If delete a forwarding entry, select the corresponding forwarding entry or select it all and click [Delete] to delete the entry.

3.3 Delete

Configuration Steps

1. Select [Base Configuration / FDB Table / Delete] to enter the [Delete] interface.

2. If delete related entries in the FDB Table in batches, select the corresponding remove condition in the MAC address deletion column, and then click [Apply], as shown in Figure 3.5.



MAC Deletion	
Delete By	ALL ▾
Dynamic or Static	□ Dynamic □ Static
VLAN	<1-4094>
Port	GE/1 ▾

Figure 3.5 FDB Table Delete

Configuration Description

Table 3.4 FDB Table [Delete] Configuration Description

Configuration Item	Description
Delete Type	Select the type of delete operation. All: Deletes all FDB Table entries. VLAN: Specifies the VLAN ID to delete FDB Table entries. Port: Specify the port number to delete the FDB Table entries.
Dynamic or static	Select the delete type, dynamic or static: Dynamic: Delete the dynamic FDB Table entries that have been learned. Static: Delete manually added static FDB Table entries.
VLAN	Delete the forwarding entry of the specified VLAN. The range is 1-4094.
Port	Delete the forwarding entry of the specified port.

Chapter 4 VLAN

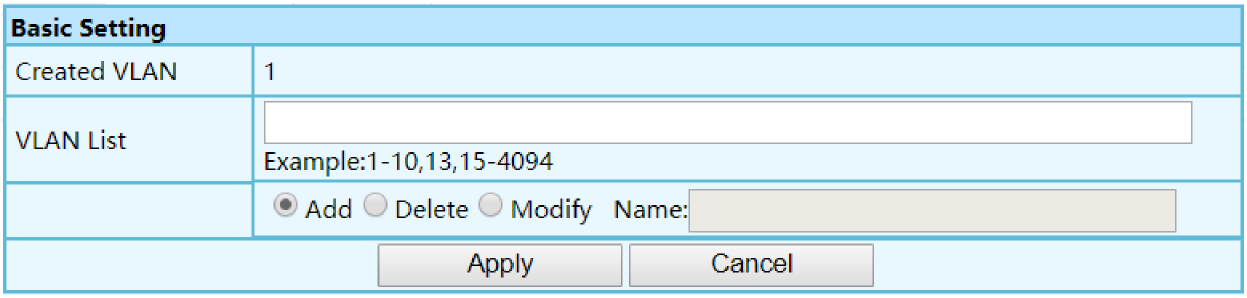
4.1 Base Configuration

Configuration Steps

1. Select [Base Configuration / VLAN / Basic Setting] to enter the VLAN [Basic Setting] interface.

2. On [Basic Setting] interface, you can view the related configuration information of each VLAN. If you want to find information about a VLAN ID, select the range of the VLAN ID in the drop-down box, enter the specified VLAN ID in the input box, and click [Search].

3. To add, modify, or delete VLANs, click [Setup]. Enter the VLAN to be added, modified, or deleted in the <VLAN list> box on setup interface. Then select Add, Modify, or Delete. Click [Apply]. The setting and modification options can only modify the VLAN name, as shown in Figure 4.1.



Basic Setting	
Created VLAN	1
VLAN List	Example:1-10,13,15-4094
	● Add ○ Delete ○ Modify Name:
Apply	Cancel

Figure 4.1 VLAN Basic Setting

Configuration Description

Table 4.1 VLAN [Basic Setting] Configuration

Configuration Item	Description
Search	To search for a VLAN ID 1. Select the interval where the VLAN to be searched in the interval selection box; 2. If you enter a specific VLAN ID in the input box, for example 11, the information bar with the VLAN number 11 turns yellow; 3. If there is no such VLAN, the corresponding information is prompted.
Top	Display the first page of VLAN information
End	Display the last page of VLAN information

Table 4.1 VLAN [Basic Setting] Configuration Description

Configuration item	Instructions
VLAN list box	It is to input the VLAN list to be set and supports multi-VLAN batch input, such as 1,2,3,4-10；
Add	To add the VLAN that is entered in the VLAN list box. VLAN 1 is the default VLAN. It already exists and does not need to be created；

Delete	To delete the VLAN input in the VLAN list box. VLAN 1 is the default VLAN and cannot be deleted.
Modify	To modify the VLAN input in the VLAN list box. The VLAN name can be modified. The new name needs to be entered in the name box.

4.2 VLAN Port Configuration

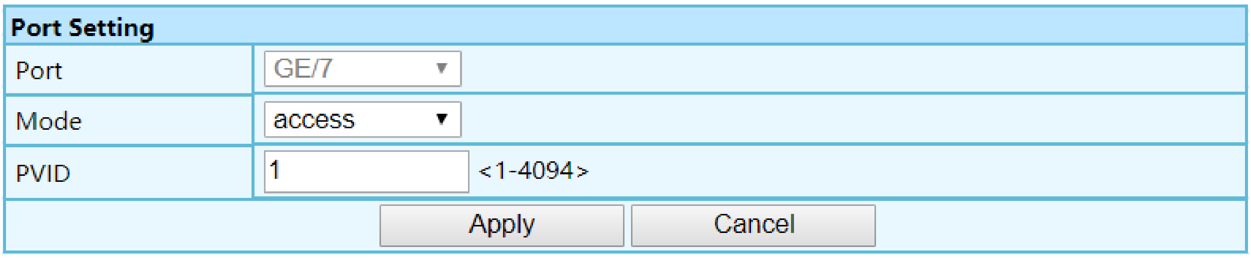
Configuration Steps

1. Select [Base Configuration / VLAN / Port Setting] to enter the VLAN Port Setting interface.

2. On the [Port Setting] interface, you can view the VLAN related configuration information of each port.

3. To modify the VLAN configuration of a port, click [Modify] in the corresponding port display field to enter the port setting interface, as shown in Figure 4.2.

4. Select or fill in the configuration items that need to be modified and click [Apply]. There will be prompts if the configuration item is filled in incorrectly.



Port Setting

Port	GE/7
Mode	access
PVID	1 <1-4094>

Figure 4.2 VLAN Port Setting

Configuration Description

Figure 4.3 VLAN [Port Setting] Configuration

Configuration Item	Description
Modify	Modify the VLAN configuration of the corresponding port
Refresh	Refresh the VLAN configuration information of all ports

Table 4.4 Modify Interface Configuration of VLAN [Port Setting]

Configuration Item	Description
Port	Port name information
VLAN Mode	Port VLAN mode ● Access: access mode ● Trunk mode ● Hybrid mode
PVID	Port PVID;
Tagged VLAN	List of VLANs allowed to pass through the port. It supports batch input of multiple VLANs. For example: ‘1,2,3,4-10’; Add: Add the tagged VLAN to the port as the input VLAN; Delete: Delete the VLAN from the tagged VLAN of the port; Replace: Replace the original tagged VLAN of the port with the input VLAN; All created VLANs: All the created VLANs are tagged VLANs of the port. Even if they are created later, they will be automatically added to the tagged VLAN of the port.
Untagged VLAN	Port untagged VLAN list, supports multi-VLAN batch input, such as: "1,2,3,4-10"; Add: Add the incoming VLAN to the untagged VLAN of the port; Delete: Delete the incoming VLAN from the untagged VLAN of the port. Replace: Replace the original untagged VLAN of the port with the input VLAN.

Chapter 5 QoS

5.1 Priority Mapping Configuration

5.1.1 802.1p Priority (CoS)

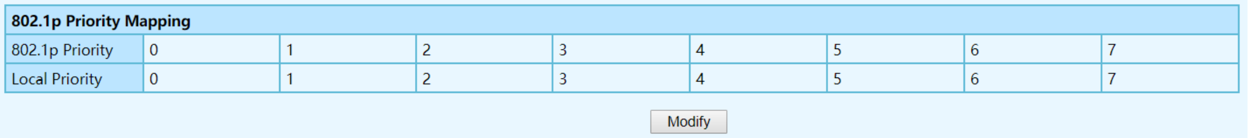
Configuration Steps

1. Select [Base Configuration / QOS / Mapping / 802.1p Priority] in the navigation bar to enter the QOS [802.1p Priority] interface.

2. On the QOS [802.1p Priority] interface, you can view the mapping from 802.1p priorities to

local priorities.

3. To modify the mapping relationship, click [Modify] and select the mapped local priority for the corresponding 802.1p priority in drop-down list box, as shown in Figure 5.1.



802.1p Priority Mapping

802.1p Priority	0	1	2	3	4	5	6	7
Local Priority	0	1	2	3	4	5	6	7

Figure 5.1 QOS 802.1p Priority Mapping Setting

Configuration Description

Table 5.1 QOS [802.1p Priority] Configuration Description

Configuration item	Description
Modify	Modify the mapping between 802.1p priorities and local priorities

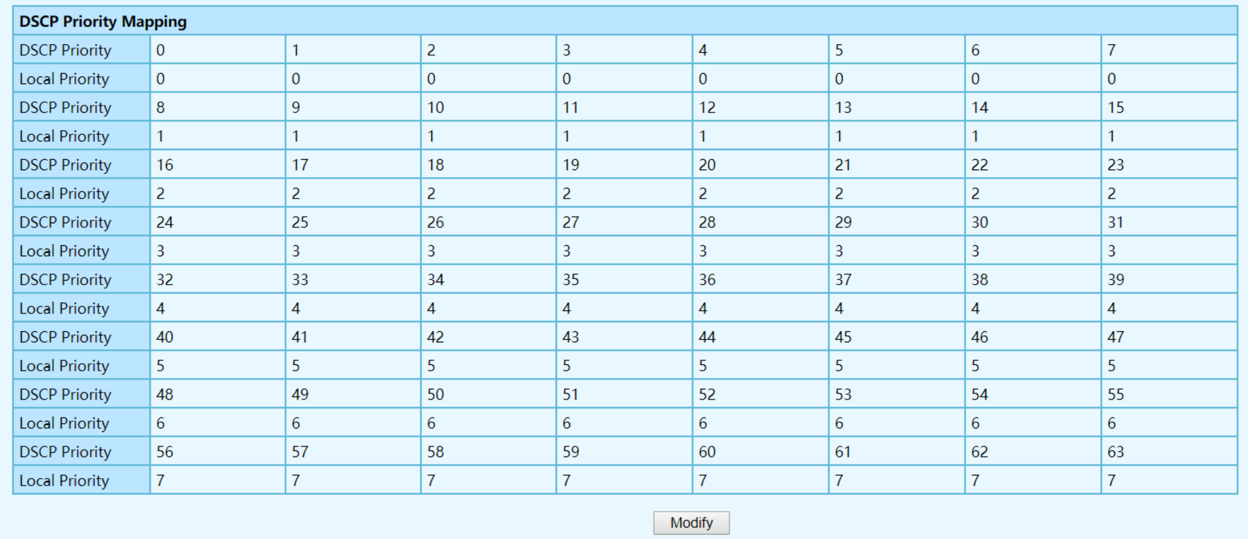
5.1.2 DSCP Priority

Configuration Steps

1. Select [Base Configuration / QOS / Mapping / DSCP Priority] in the navigation bar to enter the QOS DSCP Priority Mapping interface.

2. On the QOS [DSCP Priority] interface, you can view the mapping from DSCP priorities to local priorities.

3. To modify the mapping relationship, click [Modify] and select the mapped local priority for the corresponding DSCP priority in drop-down list box, as shown in Figure 5.2.



DSCP Priority Mapping

DSCP Priority	0	1	2	3	4	5	6	7
Local Priority	0	0	0	0	0	0	0	0
DSCP Priority	8	9	10	11	12	13	14	15
Local Priority	1	1	1	1	1	1	1	1
DSCP Priority	16	17	18	19	20	21	22	23
Local Priority	2	2	2	2	2	2	2	2
DSCP Priority	24	25	26	27	28	29	30	31
Local Priority	3	3	3	3	3	3	3	3
DSCP Priority	32	33	34	35	36	37	38	39
Local Priority	4	4	4	4	4	4	4	4
DSCP Priority	40	41	42	43	44	45	46	47
Local Priority	5	5	5	5	5	5	5	5
DSCP Priority	48	49	50	51	52	53	54	55
Local Priority	6	6	6	6	6	6	6	6
DSCP Priority	56	57	58	59	60	61	62	63
Local Priority	7	7	7	7	7	7	7	7

Figure 5.2 QOS DSCP Priority Mapping Setting

Configuration Description

Table 5.2 QOS [DSCP Priority] Configuration Description

Configuration Item	Instructions
Modify	Modify the mapping between DSCP priorities and local priorities

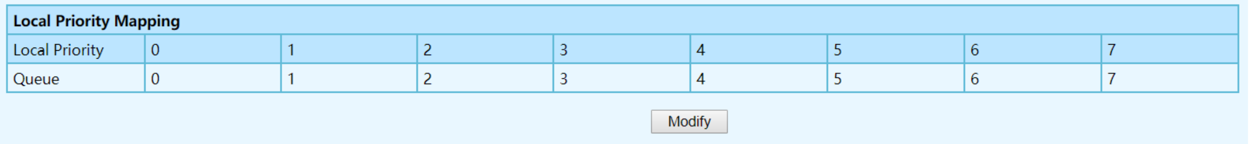
5.1.3 Local Priority

Configuration Steps

1. Select [Base Configuration / QOS / Mapping / Local Priority] in the navigation bar to enter the QOS Local Mapping.

2. You can view the mapping from the local priority to the egress queue on the QOS [Local Priority] interface.

3. To modify the mapping relationship, click [Modify] and select the mapped egress queue for the corresponding local priority in drop-down list box, as shown in Figure 5.3.



Local Priority Mapping

Local Priority	0	1	2	3	4	5	6	7
Queue	0	1	2	3	4	5	6	7

Figure 5.3 QOS Local Priority Mapping Setting

Configuration Description

Table 5.3 QOS [Local Priority] Configuration Description

Configuration Item	Description
Modify	Modify the mapping relationship between the local precedence and the egress queue

5.2 QOS Port Configuration

5.2.1 Port Priority Settings

Configuration Steps

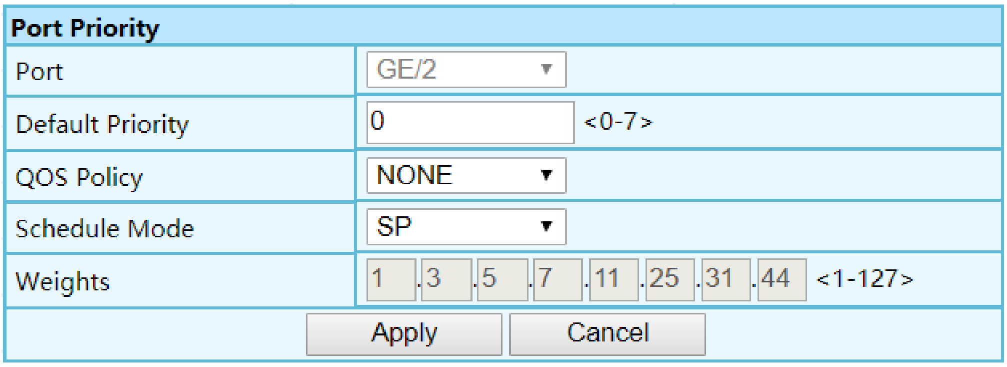
1. Select [Base Configuration / QOS / Ports / Port Priority] in the navigation bar to enter the QOS

[Port Priority] interface.

2. The QOS related configuration of the port can be viewed on the QOS [Port Priority] interface.

3. To modify the QOS configuration of a port, click [Modify] on the corresponding port display to enter the port setting interface, as shown in Figure 5.4.

4. Select or fill in the configuration items that need to be modified and click [Apply] to confirm. There will be prompts if the configuration item is filled in incorrectly.



Port Priority	
Port	GE/2 ▾
Default Priority	0 <0-7>
QOS Policy	NONE ▾
Schedule Mode	SP ▾
Weights	1 .3 .5 .7 .11 .25 .31 .44 <1-127>

Figure 5.4 QOS Port Settings

Configuration Description

Table 5.4 QOS [Port Priority] Configuration Description

Configuration Item	Description
Modify	Modify the port's QOS configuration

Table 5.5 QOS [Port Priority] Modifying Configuration Description

Configuration Item	Description
Port	Port name information
Default Priority	The port default with Priority, range <0-7>
QOS Strategy	Port QOS policy: NONE: indicates no policy. The port does not have a policy by default. COS: COS priority policy DSCP: DSCP priority policy OS-DSCP: COS-DSCP priority policy

Scheduling Mode	QOS Scheduling strategy: SP: Strict Priority scheduling strategy WRR: Weighted Round Robin scheduling strategy WFQ: Weighted Fair Queue scheduling strategy
Weights	If the selected scheduling mode is WRR or WFQ, you need to configure the weight of each queue, total 8 queues. To set 8 weights, the weight of all queues must be 127.

5.2.2 Port Rate Limit

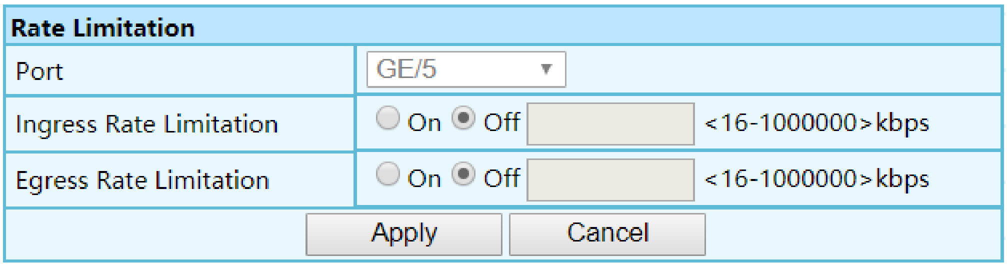
Configuration Steps

1. Select [Base Configuration / QOS / Port / Rate Limitation] in the navigation bar to enter the QOS [Rate Limitation] interface.

2. On the QOS [Rate Limitation] interface, you can view the related configuration of the port's speed limit.

3. To modify the port's speed limit configuration, click [Modify] in the port display column to enter the Rate Limitation setting interface, as shown in Figure 5.5.

4. Select or fill in the configuration items that need to be modified and click [Apply] to confirm. There will be prompts if the configuration item is filled in incorrectly.



Rate Limitation	
Port	GE/5 ▾
Ingress Rate Limitation	○ On ● Off <16-1000000>kbps
Egress Rate Limitation	○ On ● Off <16-1000000>kbps

Figure 5.5 QOS Port Speed Setting

Configuration Description

Table 5.6 QOS Port Rate Configuration Description

Configuration Item	Description
Modify	Modify the related configuration of the Rate Limitation

Table 5.7 QOS [Port Rate Limit] Modifying Configuration Description

Configuration Item	Description
Port	Port name formation
Ingress Rate Limitation	Set the port's entry speed limit: On: Enables the port to limit the rate of ingress. The rate limit ranges from <16-1000000> Disabled: Close the port's ingress rate limit
Egress Rate Limitation	Set the port's output speed limit: On: Enables the port to limit the rate of egress. The rate limit ranges from <16-1000000> Disabled: Close the port's egress rate limit

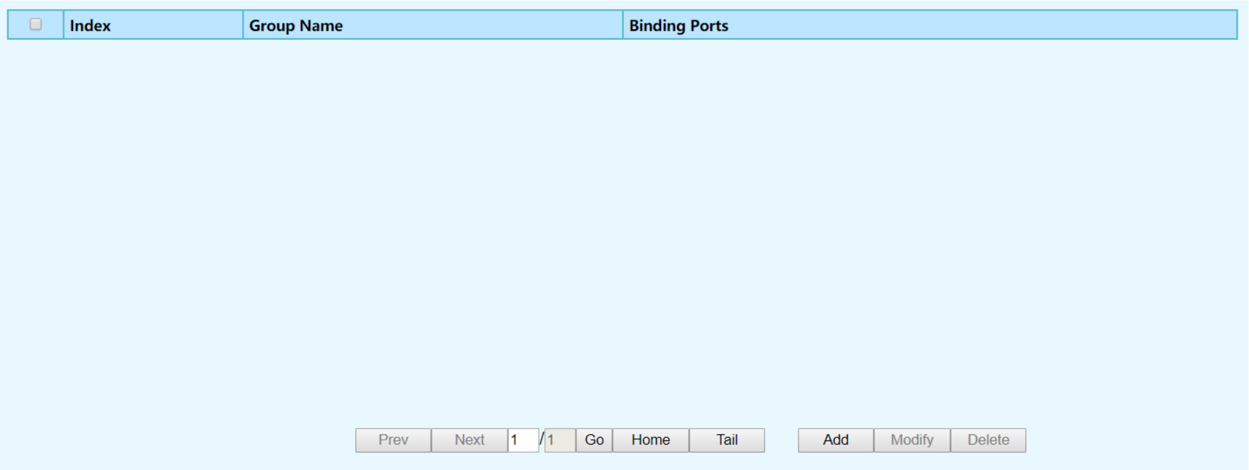
Chapter 6 ACL

6.3 ACL Group Setting

Configuration Step

1. Select [Advanced / ACL / ACL Group Setting] in the navigation bar to enter the ACL interface.

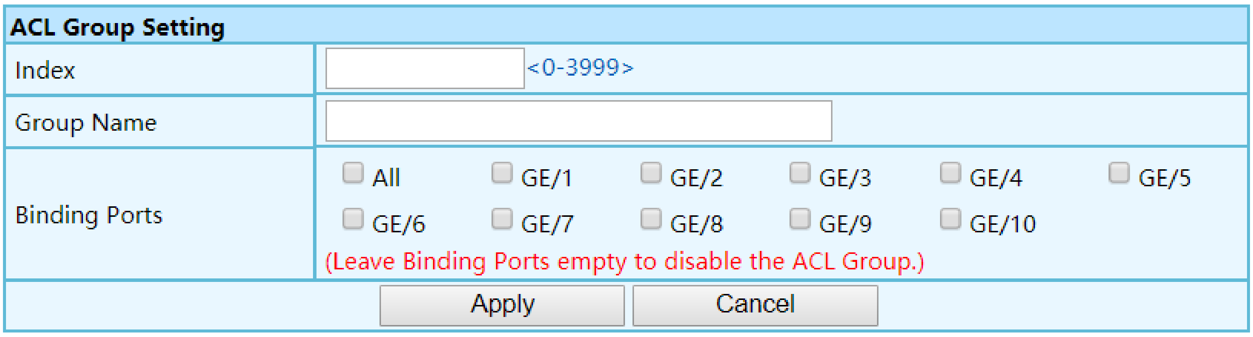
2. The ACL information will be added in [ACL Group Setting] interface, as shown in figure 6.1.



□	Index	Group Name	Binding Ports

Figure 6.1 ACL Group Information

3. Add an ACL Group: click [Add] to enter [ACL Group Setting] interface, as shown in figure 6.2. An ordinal number (0-3999) is assigned to the group. Set a name for the group, not repeatable. Then select the port and bind to the group. It is not workable if port binding not done. Click [Apply] to complete the configuration.



ACL Group Setting	
Index	<0-3999>
Group Name	
Binding Ports	□ All □ GE/1 □ GE/2 □ GE/3 □ GE/4 □ GE/5 □ GE/6 □ GE/7 □ GE/8 □ GE/9 □ GE/10 (Leave Binding Ports empty to disable the ACL Group.)

Figure 6.2 ACL Group Setting

4. Modify an ACL Group Configuration: select an ACL group and click [Modify] to enter the [ACL Group Setting] interface. Fill in the required configuration items and click [Apply] to complete the configuration.

5. Delete an ACL Group Configuration: select an ACL group and click [Delete] to delete the configuration.

ACL Group Configuration Description

Configuration	Description
Serial Number	ACL group index, range <0-3999>, divided into 4 matching groups L2, L3 / L4, Source L2 / L3 / L4, Destination L2 / L3 / L4. The matching items supported by each matching group are as follows: **L2:** Source MAC, Destination MAC, Ethernet type, VLAN, IP protocol, range 0-999. **L3 / L4:** VLAN, Source IP, Destination IP, Source IP port, Destination IP port, IP protocol, range 1000-1999. **Source L2 / L3 / L4:** Source MAC, Ethernet type, VLAN, Source IP, Source IP port, IP protocol, range 2000-2999. **Destination L2 / L3 / L4:** Destination MAC, Ethernet type, VLAN, Destination IP, Destination IP port, IP protocol, range 3000-3999.
ACL	The Group name must be unique and string format, ASCII code A-Z, a-z,0-9, _, no more

Group Name	than 32 characters.
Port Binding	An ACL is applied to a certain port or some port, then the bound port ACL becomes effective.

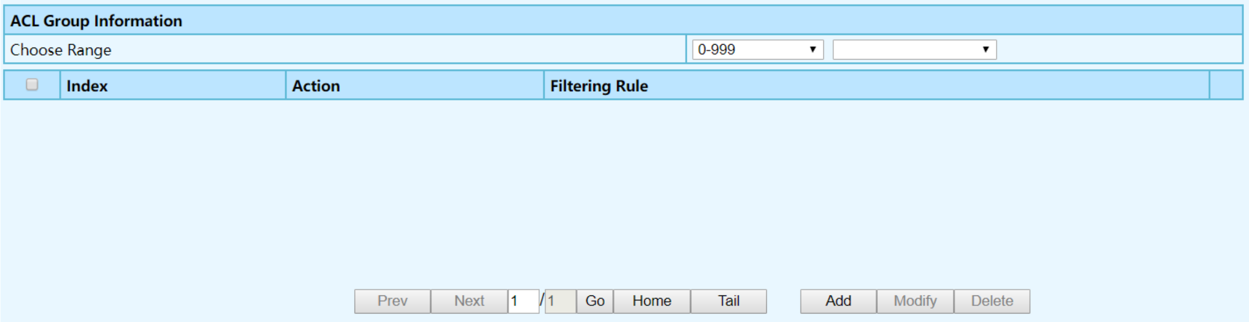
6.4 ACL Rules

6.4.1 ACL Rule Setting

Configuration Step

1. Select [Advanced / ACL / ACL Rule Setting] in the navigation bar to enter the ACL Rule view interface, as shown in figure 6.3.

2. In Select Range, select the interval of the group in the first drop-down list, and select a specific group within the group interval in second drop-down list. The next two lines show the selected group name and the port that the group binds. The table shows the ACL rules that the group has configured. Click the icon ⊞ in the filter rule bar to expand and view the specific content of the filter rule, the icon changed to be ⊟.



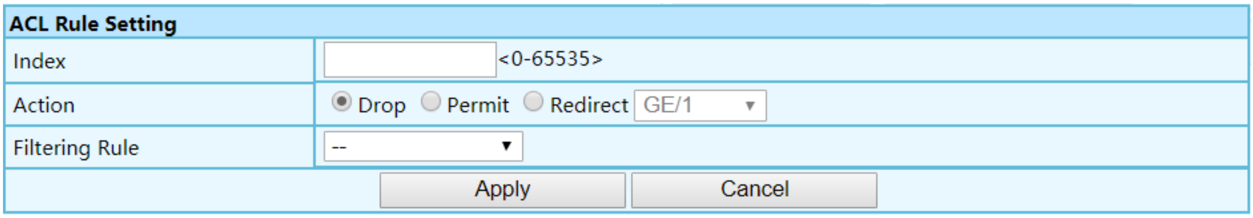
ACL Group Information

Choose Range: 0-999

□	Index	Action	Filtering Rule

Figure 6.3 ACL Rule View

3. Add an ACL Rule: click [Add] to enter the ACL rule setting interface. One of the filtering rules can be selected by selecting different filters via the drop-down list, and then the corresponding filtering items will be automatically generated for users to fill in. You can also remove the filter items by the [Delete] on the right side. Fill in the required configuration items and click [Apply] to complete the configuration.



ACL Rule Setting	
Index	<0-65535>
Action	● Drop ○ Permit ○ Redirect GE/1 ▾
Filtering Rule	-- ▾

Figure 6.4 ACL Rule Setting

4. Modify an ACL Rule: select an ACL and click 'Modify' to enter the [ACL Rule Setting] interface. Fill in the required configuration items and click 'Apply' to complete the configuration.

5. Delete an ACL Rule: select an ACL and click 'Delete' to delete the configuration.

ACL Rule Configuration Description

Configuration	Description
Serial Number	ACL Rule Index
Action	When the message conforms to the filter rule, the action includes: ●Allow ●Discarded ●Redirect to the destination port

Filtering Rule	ACL filtering rules include: ●Source MAC, support the mask ●Destination MAC, support the mask ●Source IP address, support the mask ●Destination IP address and support the mask ●Source IP port ●Destination IP port ●IP Protocol ●Ethernet type, support the mask ●VLAN The filtering items can be filtered by a range via setting the mask. Note: When the match mask is 1, it is matched. Not matched at 0
Matching Description	Source MAC: Format xxxxxx-xxxxxx, support the mask, default mask ffffff-ffffff
	Destination MAC: Format xxxxxx-xxxxxx, support the mask, default mask ffffff-ffffff
	Source IP Address: Format dotted decimal notation, support the mask, default mask 255.255.255.255
	Destination IP Address: Format dotted decimal notation, support the mask, default mask 255.255.255.255
	Source IP Port: IP packet source port, integer form, range 1~65535
	Destination IP Port: IP packet for destination port, integer form, range 1~65535
	IP Protocol: Only supports TCP, UDP, ICMP, IGMP currently
	Ethernet Type: Hexadecimal format, support mask, default mask FFFF

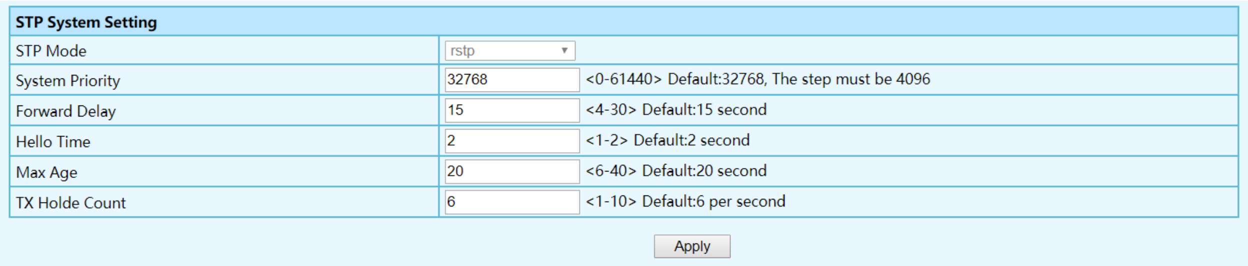
Chapter 7 RSTP

7.3 Global Configuration

Configuration Steps

1. Select [Advanced / STP / Global Setting] in the navigation bar to enter the STP[Global Setting] interface.
2. The STP global setting information can be viewed in the [Global Setting] interface.

3. To modify the configuration, you can enter the values that need to be configured directly in corresponding configuration item, as shown in figure 7.1.



STP System Setting		
STP Mode	rstp ▾	
System Priority	32768	<0-61440> Default:32768, The step must be 4096
Forward Delay	15	<4-30> Default:15 second
Hello Time	2	<1-2> Default:2 second
Max Age	20	<6-40> Default:20 second
TX Holde Count	6	<1-10> Default:6 per second

Figure 7.1 STP System Setting

Configuration Description

Figure 7.1 STP [Global Setting] Description

Configuration	Description
STP Mode	Support RSTP, compatible with STP
System priority	STP System priority
State Transition Delay	Delay when port switch between disabled / listening / learning / forwarding
Packet Sending Interval	The time interval sent by STP protocol message in stable state
Packet Maximum Lifetime	The maximum survival time of the STP protocol packet received by the bridge. If no new protocol packets received at this time, the packet will be discarded
Max. Packets per Second	The maximum number of STP protocol packets sent by Port per second

7.4 Port Configuration

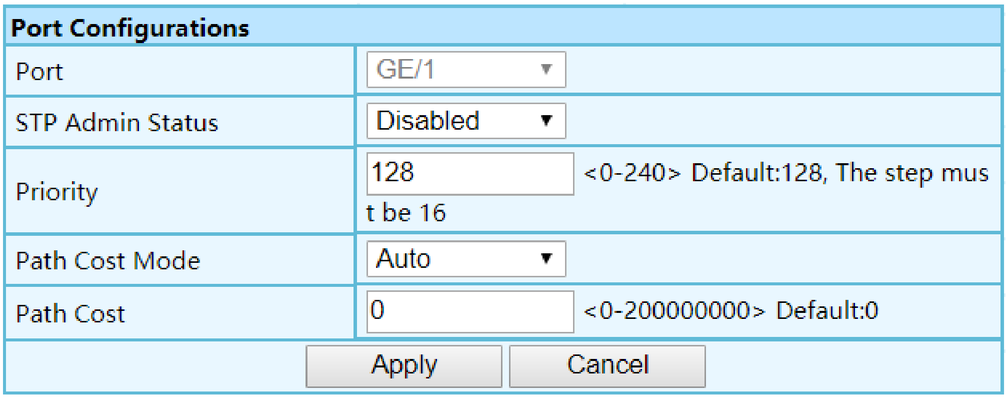
Configuration Steps

1. Select [Advanced / STP / Port Configurations] in the navigation bar to enter the STP [Port Configurations] interface.

2. The STP port configuration information can be viewed in the [Port Configurations] interface.

3. To modify the port configuration, you can click [Modify] on the right side of the corresponding port to enter

the port configuration interface of the STP, as shown in figure 7.2.



Port Configurations	
Port	GE/1 ▼
STP Admin Status	Disabled ▼
Priority	128 <0-240> Default:128, The step mus t be 16
Path Cost Mode	Auto ▼
Path Cost	0 <0-200000000> Default:0

Figure 7.2 STP Port Configurations

Configuration Description

Figure 7.2 STP [Port Configurations] Description

Configuration	Description
Port	Port Name
STP Enable Status	[Disable] or [Enable], default with [Disable]
Port Priority	STP Priority
Path Overhead Calculation	The calculation of STP port path overhead, [Auto] or [Managed], default with [Auto]
STP Port Path Overhead	When the path overhead is calculated in a managed mode, the port's path overhead takes effect as the configured value.

Path Overhead

The STP BPDU message requires a certain Path overhead for each Root port. The Path overhead of each bridge is cumulative, and this value is called Root Path Cost. The path overhead is different corresponding to the root ports of different rates, as shown in the following table:

Figure 7.3 Path Overhead of Different Port Rate

Port Rate	Path Overhead
10Mbps	2,000,000

100Mbps	200,000
1000Mbps	20,000

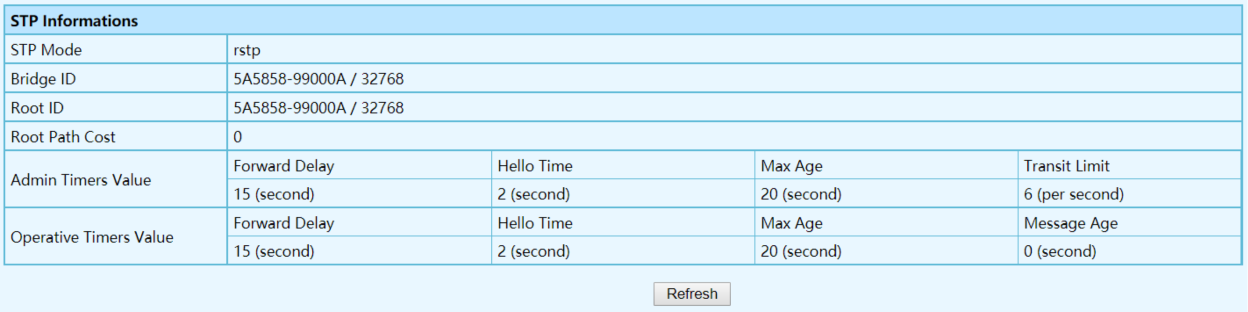
7.5 STP Information

Configuration Step

1. Select [Advanced / STP / STP Information] in the navigation bar and enter the STP [STP information] interface.

2. The STP current running information can be viewed in the [STP information] interface, as shown in figure 7.3

3. Click [Refresh] to show the latest running information.



STP Informations				
STP Mode	rstp			
Bridge ID	5A5858-99000A / 32768			
Root ID	5A5858-99000A / 32768			
Root Path Cost	0			
Admin Timers Value	Forward Delay	Hello Time	Max Age	Transit Limit
	15 (second)	2 (second)	20 (second)	6 (per second)
Operative Timers Value	Forward Delay	Hello Time	Max Age	Message Age
	15 (second)	2 (second)	20 (second)	0 (second)

Figure 7.3 STP Information Interface

7.6 Port Information

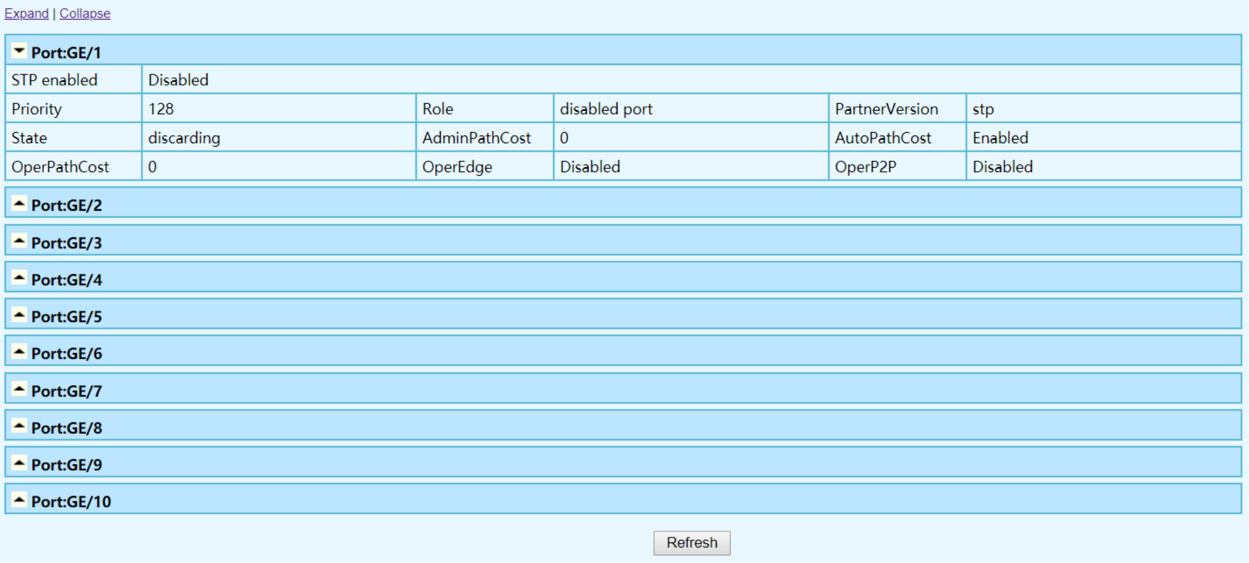
Configuration Step

1. Select [Advanced / STP / Port Information] in the navigation bar and enter the STP [Port information] interface.

2. The STP current running information can be viewed in the [Port Information] interface, as shown in figure

7.4

3. Click [Refresh] to show the latest running information.



Port:GE/1

STP enabled	Disabled				
Priority	128	Role	disabled port	PartnerVersion	stp
State	discarding	AdminPathCost	0	AutoPathCost	Enabled
OperPathCost	0	OperEdge	Disabled	OperP2P	Disabled

Port:GE/2

Port:GE/3

Port:GE/4

Port:GE/5

Port:GE/6

Port:GE/7

Port:GE/8

Port:GE/9

Port:GE/10

Figure 7.4 RSTP Port Information Interface

RSTP Port Information Introduction as following table:

STP Port Information	Description
STP Enable	Disable: Inactive STP Enable: Active STP
Priority	Port Priority
Role	**Root Port:** connect the root bridge port, provide lowest path cost Designated Port: to connect with Root Port, provide lowest path cost **Disable Port:** not responsible for message forwarding, blocking status **Alternate Port:** provide an alternate path for the current root port to the root bridge **Backup Port:** provides a backup path for the designated port
Partner Version	STP Mode: STP / RSTP / MSTP (not support currently)
State	Forwarding or Block
Admin Path Cost	Path cost configuration values
Auto Path Cost	Disable automatic computing path cost Enable automatic computing path cost
Operate Path Cost	Operate path cost

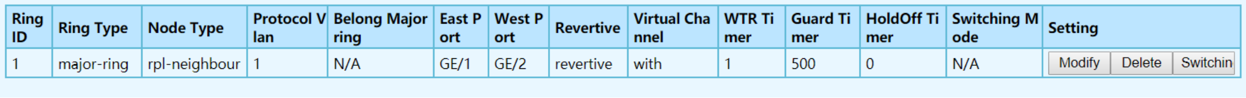
Operate Edge	Disable non-edge port Enable edge port
Operate P2P	Disable non-point-to-point mode Enable point-to-point mode

Chapter 8 ERPS

8.4 ERPS Setting

Configuration Step

1. Select [Advanced / ERPS / Global Setting] in the navigation bar and enter the ERPS [Global Setting] interface, as shown in Figure 8.1

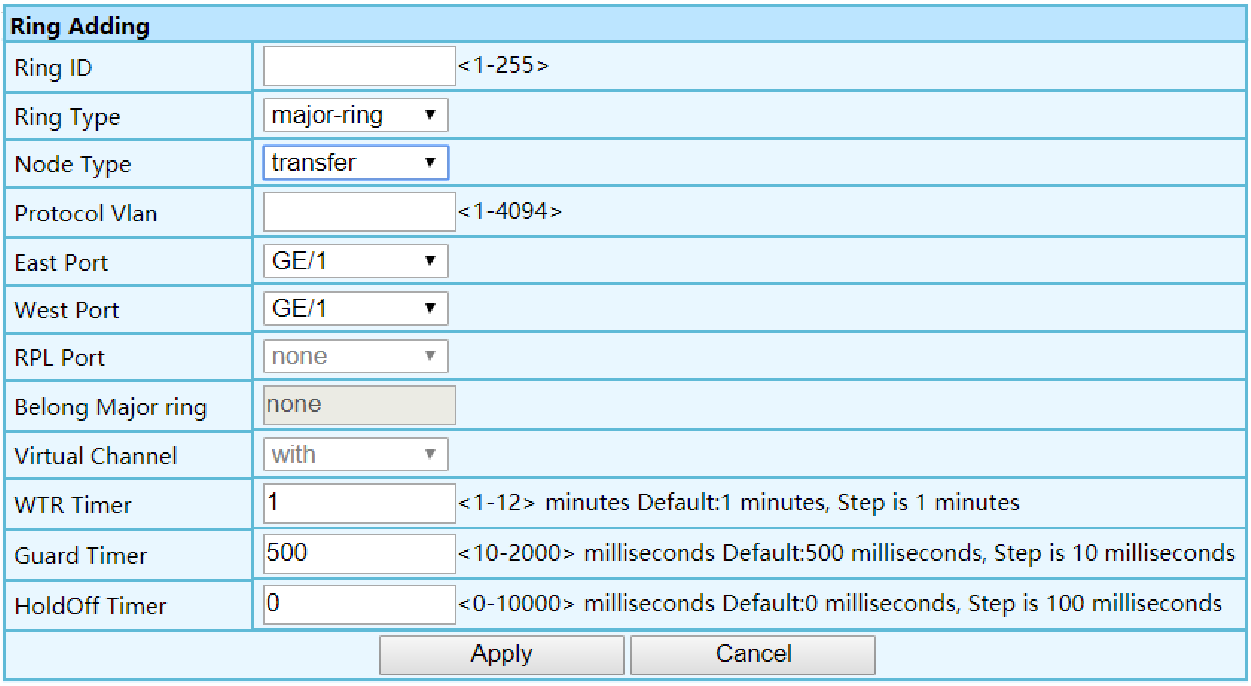


Ring ID	Ring Type	Node Type	Protocol Vlan	Belong Major ring	East Port	West Port	Revertive	Virtual Channel	WTR Timer	Guard Timer	HoldOff Timer	Switching Mode	Setting
1	major-ring	rpl-neighbour	1	N/A	GE/1	GE/2	revertive	with	1	500	0	N/A	Modify Delete Switchin

Figure 8.1 ERPS Setting

2. All ERPS information can be viewed in ERPS [Global Setting] interface

3. Click [Add] button, enter the Ring Adding interface as shown in figure 8.2, enter a valid configuration parameter, and click [Apply] to submit the changes. Click [Cancel] to discard the modification.

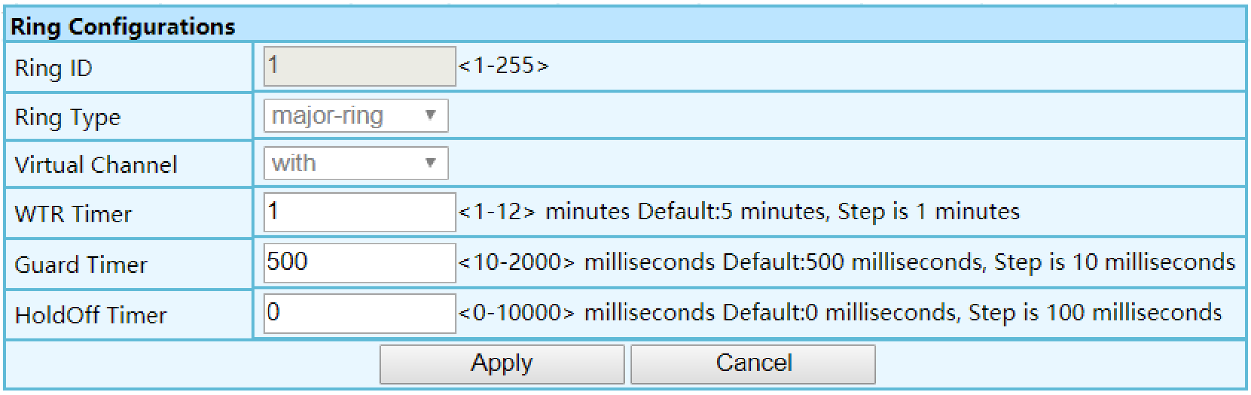


Ring Adding

Ring ID	<1-255>
Ring Type	major-ring ▼
Node Type	transfer ▼
Protocol Vlan	<1-4094>
East Port	GE/1 ▼
West Port	GE/1 ▼
RPL Port	none ▼
Belong Major ring	none
Virtual Channel	with ▼
WTR Timer	1 <1-12> minutes Default:1 minutes, Step is 1 minutes
Guard Timer	500 <10-2000> milliseconds Default:500 milliseconds, Step is 10 milliseconds
HoldOff Timer	0 <0-10000> milliseconds Default:0 milliseconds, Step is 100 milliseconds

Figure 8.2 ERPS Ring Adding

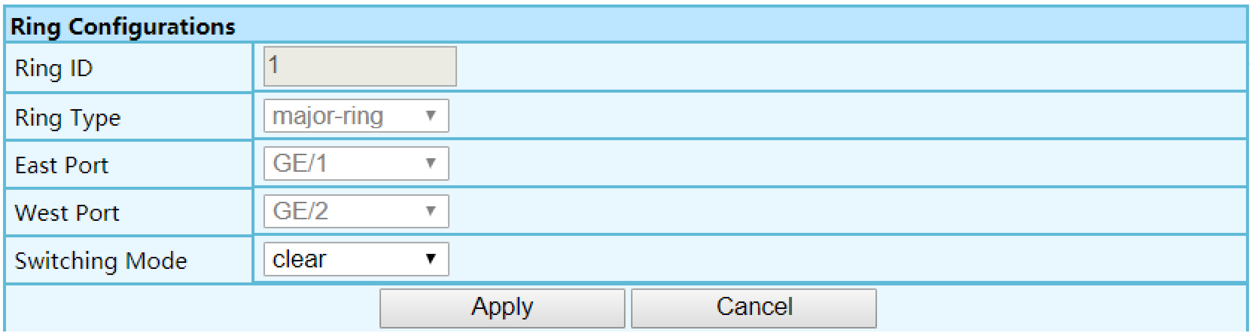
4. Click [Modify], enter the Ring Modification interface, as shown in figure 8.3



Ring Configurations	
Ring ID	1 <1-255>
Ring Type	major-ring ▼
Virtual Channel	with ▼
WTR Timer	1 <1-12> minutes Default:5 minutes, Step is 1 minutes
Guard Timer	500 <10-2000> milliseconds Default:500 milliseconds, Step is 10 milliseconds
HoldOff Timer	0 <0-10000> milliseconds Default:0 milliseconds, Step is 100 milliseconds

Figure 8.3 ERPS Ring Modification

5. Click [Switching] button, enter Ring Flow Switching Configuration Interface, as shown in Figure 8.4



Ring Configurations	
Ring ID	1
Ring Type	major-ring ▼
East Port	GE/1 ▼
West Port	GE/2 ▼
Switching Mode	clear ▼

Figure 8.4 ERPS Flow Switching Configuration

6. Click [Delete] button, delete corresponding Ring

Configuration Description

Figure 8.1 ERPS [Global Setting] Ring Configuration Description

Configuration	Description
Ring ID	Ring adding ID
Ring Type	Choose the adding ring type
Node Type	Node role in ring
Protocol VLAN	Adding ring ERPS protocol VLAN
East Port	A ring port created on this node
West Port	Another ring port created on this node
Main Ring	When the created ring is a sub-ring and this node is an intersecting node, specify the main ring to which it belongs

Sub-ring Virtual Channel	To transmit sub-ring protocol information in the main ring
WTR Timer	Configure the value of WTR Timer
Guard Timer	Configure the value of Guard Timer
Hold Off Timer	Configure the value of Hold Off Timer

Figure 8.2 ERPS [Global Setting] Ring Modification Configuration Description

Configuration	Description
Ring ID	Modified ring ID
Ring Type	Modified ring type
Sub-ring Virtual Channel	To transmit sub-ring protocol information in the main ring
WTR Timer	Configure the value of WTR Timer
Guard Timer	Configure the value of Guard Timer
Hold Off Timer	Configure the value of Hold Off Timer

Figure 8.3 ERPS [Global Setting] Flow Switching Configuration Description

Configuration	Description
Ring ID	Modified ring ID
Ring Type	Modified ring type
East Port	A ring port created on this node
West Port	Another ring port created on this node
Switching Way	Flow Switching

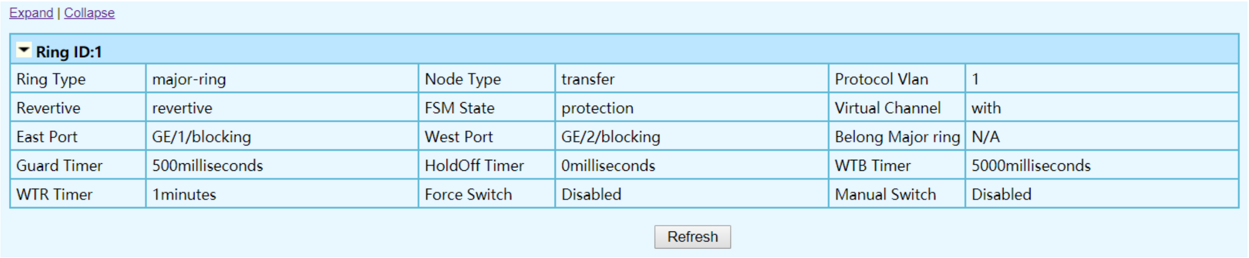
8.5 Ring Information

Configuration Step

1. Select [Advanced / ERPS / Ring Information] in the navigation bar to enter the interface of ERPS [Ring Network Information].

2. The ERPS current running information can be viewed in the [Ring Information] interface, as shown in figure 8.5.

3. Click [Refresh] to show the latest running information.



Ring Type	major-ring	Node Type	transfer	Protocol Vlan	1
Revertive	revertive	FSM State	protection	Virtual Channel	with
East Port	GE/1/blocking	West Port	GE/2/blocking	Belong Major ring	N/A
Guard Timer	500milliseconds	HoldOff Timer	0milliseconds	WTB Timer	5000milliseconds
WTR Timer	1minutes	Force Switch	Disabled	Manual Switch	Disabled

Figure 8.5 ERPS Information

Chapter 9 LLDP

9.3 LLDP Configuration

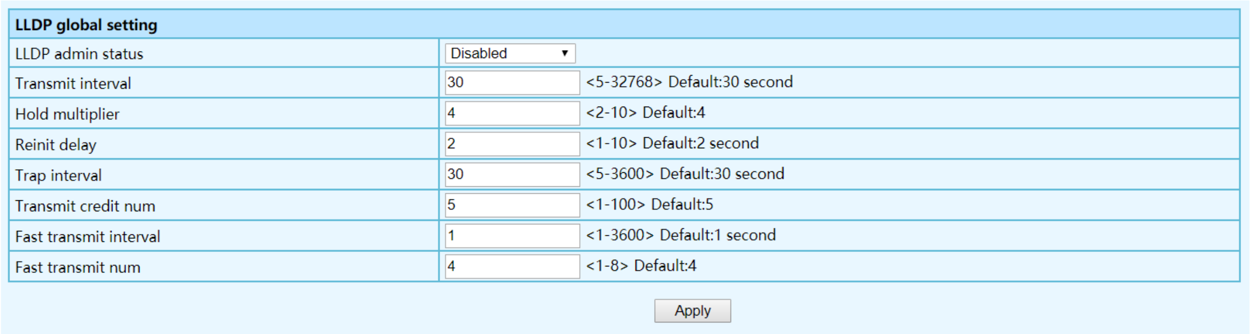
9.3.1 LLDP Global Setting

Configuration Step

1. Select [Management / LLDP / Global Setting] in the navigation bar to enter the LLDP [Global Setting] interface.

2. The LLDP global configuration can be viewed in the LLDP [Global Setting] interface, as shown in figure 9.1.

3. Modify the corresponding LLDP configuration in the LLDP [Global Setting] interface, and then click [Apply].



LLDP global setting		
LLDP admin status	Disabled ▾	
Transmit interval	30	<5-32768> Default:30 second
Hold multiplier	4	<2-10> Default:4
Reinit delay	2	<1-10> Default:2 second
Trap interval	30	<5-3600> Default:30 second
Transmit credit num	5	<1-100> Default:5
Fast transmit interval	1	<1-3600> Default:1 second
Fast transmit num	4	<1-8> Default:4

Figure 9.1 LLDP Global Setting

Configuration Description

Figure 9.1 LLDP [Global Setting] Configuration Description

Configuration	Description
LLDP Enable Status	LLDP Global Enable Switch ●ON：Enable LLDP function ●OFF：Disable LLDP function Note: Default with OFF
Transmit Period	LLDP transmit period range 0-32768, default 30
Neighbor Aging Coefficient	LLDP neighbor aging coefficient range 2-10, default 4
Reboot Delay Time	LLDP reboot delay time range 1-10, default 2
Warning Period	LLDP warning period range 5-3600, default 30
Transmit Volume	LLDP transmit volume range 1-100, default 5
Quick Transmit Period	LLDP quick transmit period range 1-3600, default 1
Quick Transmit Quantity	LLDP quick transmit quantity range 1-8, default 4

9.3.2 LLDP Port Configuration

Configuration Steps

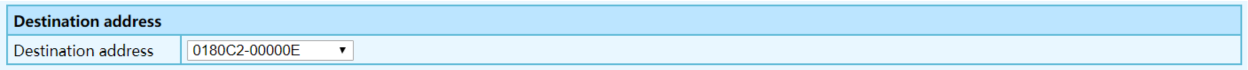
1. Select [Management / LLDP / Port Configuration] in the navigation bar to enter the LLDP [Port Configuration] interface

2. The LLDP port corresponding configuration can be viewed in the LLDP [Port Configuration] interface, as shown in figure 9.1

3. Choose the LLDP configuration of all ports corresponding to any destination address 0180C2-00000E, 0180C2-000003, 0180C2-000000 in the LLDP [Port Configuration] interface, as shown in figure 9.2

4. To modify the LLDP configuration of a destination address port, click [Modify] after selecting the destination address, and enter the port configuration interface, as shown in figure 9.3.

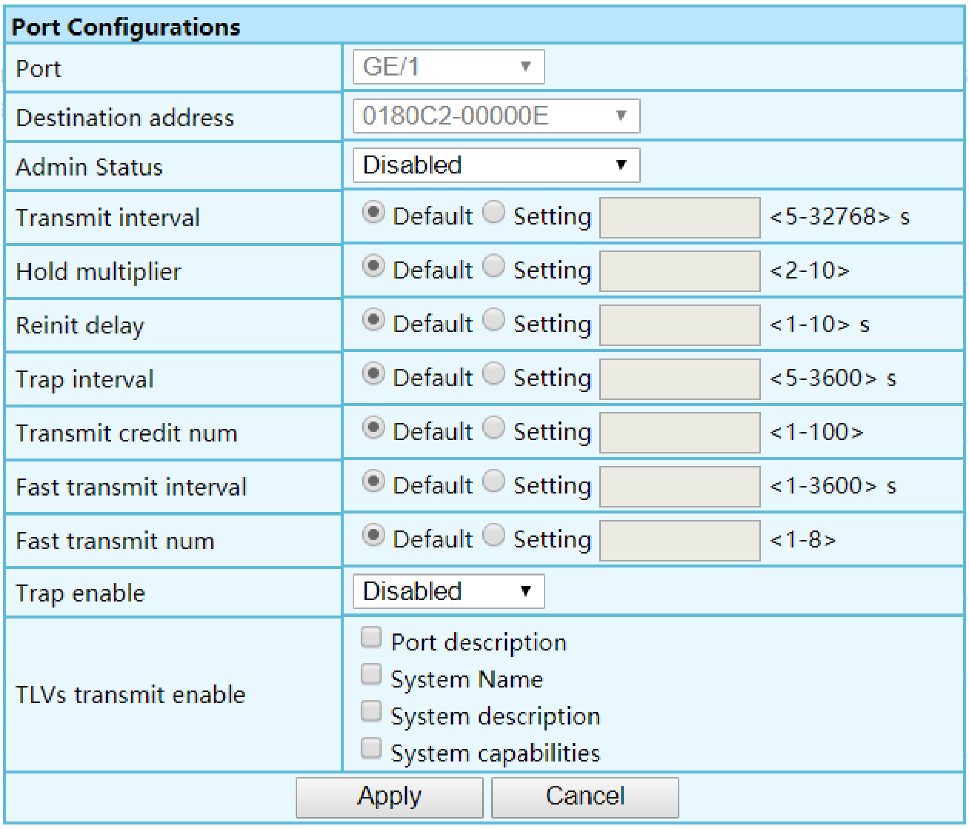
4.Select or fill out the configuration items that need to be modified and click [Apply] to make effective. There will be a corresponding prompt if the configuration item is incorrectly filled.



Destination address

Destination address	0180C2-00000E ▾

Figure 9.2 LLDP Destination Address



Port Configurations

Port	GE/1 ▾
Destination address	0180C2-00000E ▾
Admin Status	Disabled ▾
Transmit interval	● Default ○ Setting <5-32768> s
Hold multiplier	● Default ○ Setting <2-10>
Reinit delay	● Default ○ Setting <1-10> s
Trap interval	● Default ○ Setting <5-3600> s
Transmit credit num	● Default ○ Setting <1-100>
Fast transmit interval	● Default ○ Setting <1-3600> s
Fast transmit num	● Default ○ Setting <1-8>
Trap enable	Disabled ▾
TLVs transmit enable	□ Port description □ System Name □ System description □ System capabilities

Figure 9.3 LLDP Port Configuration

Configuration Description

Figure 9.2 LLDP [Port Configuration] Configuration Description

Configuration	Description

Port	Port name information
Destination Address	LLDP destination address 0180C2-00000E, 0180C2-000003, 0180C2-000000
Management Status	LLDP Port Status ●Only transmit: Enable LLDP port transmit function ●Only receive: Enable LLDP port receive function ●Transmit and receive: Enable LLDP port transmit and receive function ●Disable: Disable LLDP port transmit and receive function Note: Port default with [Disable]
Transmit Period	●Default: Use [Global Setting] transmit period ●Configuration: Set transmit period range 5-32768 Note: Port default with [Default]
Neighbor Aging Coefficient	Port Neighbor Aging Coefficient ●Default: Use [Global Setting] neighbor aging coefficient ●Configuration: Neighbor aging coefficient, range 2-10 Note: Port default with [Default]
Reboot Delay Time	Port Reboot Delay Time ●Default: Use [Global Setting] reboot delay time ●Configuration: Set reboot delay time, range 1-10 Note: Port default with [Default]
Warning Period	Port Warning Period ●Default: Use [Global Setting] warning period ●Configuration: Set warning period range 5-3600 Note: Port default with [Default]
Transmit Volume	Port Transmit Volume ●Default: Use [Global Setting] transmit volume ●Configuration: Set transmit volume range 1-100 Note: Port default with [Default]
Quick Transmit Period	Port Quick Transmit Period ●Default: Use [Global Setting] quick transmit period

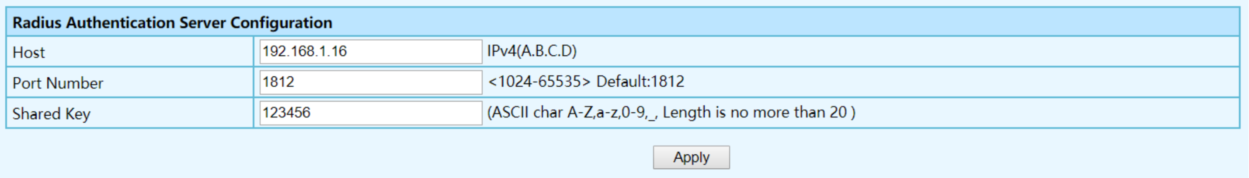
	●Configuration: Set quick transmit period range 1-3600 Note: Port default with [Default]
Quick Transmit Quantity	Port Quick Transmit Quantity ●Default: Use [Global Setting] quick transmit quantity ●Configuration: Set quick transmit quantity range 1-8 Note: Port default with [Default]
Warning Enable	Port Warning Enable ●Enable: Enable LLDP port warning function ●Disable: Disable LLDP port warning function Note: Port default with [Disable]
TLVs Transmit Enable	Support one or more TLVs transmit enable selection of port description, system name, system description and system capability

Chapter 10 802.1X

10.4 Authentication Server

Configuration Steps

1. Select [Advanced / 802.1X / Authentication Server] in the navigation bar to enter Radius Authentication Server Configuration.
2. Check the configuration information in the interface
3. To modify the Authentication Server configuration, click [Modify] in the Authentication Server configuration box, as shown in Figure 10.1



Radius Authentication Server Configuration		
Host	192.168.1.16	IPv4(A.B.C.D)
Port Number	1812	<1024-65535> Default:1812
Shared Key	123456	(ASCII char A-Z,a-z,0-9,_, Length is no more than 20)

Figure 10.1 Radius Authentication Server Configuration

Configuration Description

Table 10.1 802.1X Authentication Server Configuration Description

Configuration Item	Description
Host	The IP of Radius Authenticated Server, IPv4 and Dotted decimal format

Port#	The port of Radius Authenticated Server, range<1-65535>, default with 1812
Shared Key	Must be consistent with Radius server, otherwise it cannot pass authentication. String format, only contain letters, numbers, underscores, and the length cannot be more than 20 bytes

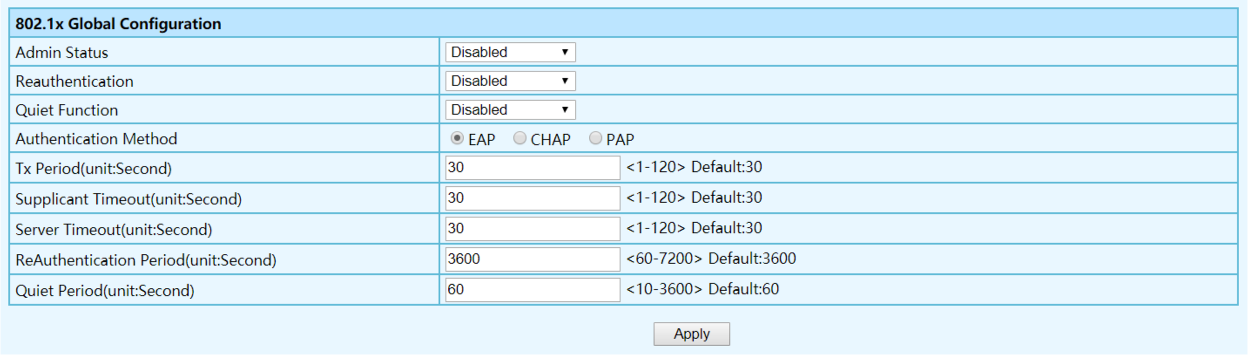
10.5 Global Settings

Configuration Steps

1. Select [Advanced / 802.1X / Global Setting] in the navigation bar to enter the [Global Setting] interface.

2. The global configuration information can be viewed in the interface.

3. To modify the global configuration in the Global Configuration box, click [Apply] as shown in Figure 10.2



802.1x Global Configuration		
Admin Status	Disabled ▾	
Reauthentication	Disabled ▾	
Quiet Function	Disabled ▾	
Authentication Method	● EAP ○ CHAP ○ PAP	
Tx Period(unit:Second)	30	<1-120> Default:30
Supplicant Timeout(unit:Second)	30	<1-120> Default:30
Server Timeout(unit:Second)	30	<1-120> Default:30
ReAuthentication Period(unit:Second)	3600	<60-7200> Default:3600
Quiet Period(unit:Second)	60	<10-3600> Default:60

Figure 10.2 802.1x Global Configuration

Configuration Description

Table 10.2 802.1X Global Configuration Description

Configuration Item	Description
Management Status	• Disable: Prohibit Global 802.1X • Enable: Enable Global 802.1X
Re-certification	• Disable: Prohibit re-authentication • Enable: Enable re-authentication
Silent function	• Disable: Prohibit the silent function • Enable: Enables the silent function
Authentication method	• EAP • PAP

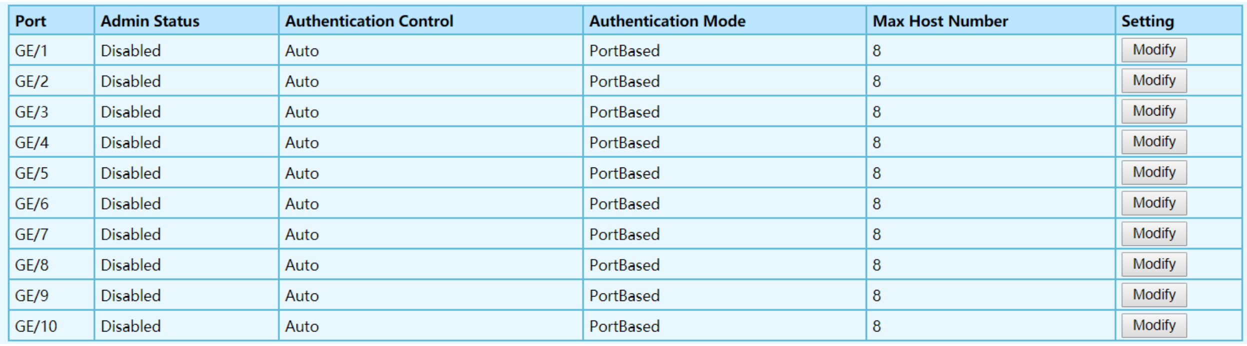
	- CHAP
Request timeout timer	Integer 1-120, default 30
Client timeout timer	Integer 1-120, default 30
Server timeout timer	Integer 1-120, default 30
Re-authentication timer	Integer 60-7200, default 3600
Silent timer	Integer 10-3600, default 60

10.6 Port Configuration

Configuration Steps

1. Select [Advanced / 802.1X / Port Configurations] in the navigation bar to enter the [Port Configurations] interface.

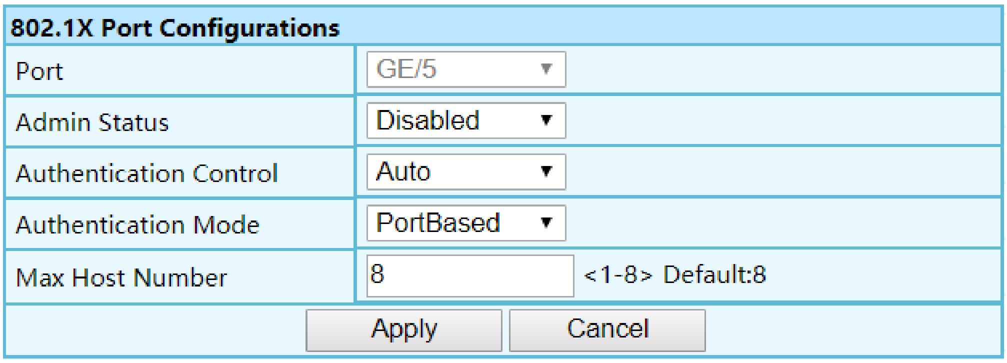
2. On the [Port Configurations] interface, you can view the configuration information of each port. As shown in Figure 10.3, the current 802.1X configuration information of each port is displayed.



Port	Admin Status	Authentication Control	Authentication Mode	Max Host Number	Setting
GE/1	Disabled	Auto	PortBased	8	Modify
GE/2	Disabled	Auto	PortBased	8	Modify
GE/3	Disabled	Auto	PortBased	8	Modify
GE/4	Disabled	Auto	PortBased	8	Modify
GE/5	Disabled	Auto	PortBased	8	Modify
GE/6	Disabled	Auto	PortBased	8	Modify
GE/7	Disabled	Auto	PortBased	8	Modify
GE/8	Disabled	Auto	PortBased	8	Modify
GE/9	Disabled	Auto	PortBased	8	Modify
GE/10	Disabled	Auto	PortBased	8	Modify

Figure 10.3 802.1X Port Configuration

3. To modify the configuration of a port, simply click the [Edit] in corresponding entry to enter modification interface, as shown in Figure 10.4. Modify the corresponding configuration item, click the [Apply] to complete the modification, and click the [Cancel] to cancel the modification.



802.1X Port Configurations

Port	GE/5 ▼
Admin Status	Disabled ▼
Authentication Control	Auto ▼
Authentication Mode	PortBased ▼
Max Host Number	8 <1-8> Default:8

Figure 10.4 802.1X Port Configuration

Precautions: When the 802.1X port is configured to authentication mode, all authenticated users will go offline and re-authentication is required to access the network.

Configuration item Description

Table 10.3 802.1X port configuration Description

Item	Description
Management Status	Prohibited: Disable port 802.1X Enable: Enable 802.1X on the port
Port Control Mode	• Automatic: You cannot access the network before authentication. You can access the network after passing the authentication. • Mandatory Authorization: Always have access to the network • Mandatory Non-authorization: Always cannot access the network
Port Authentication Mode	• Port-based: After a user is authenticated, all users can access the network. • Based on MAC: All users need to be authenticated individually to access the network
Maximum Number of Supported Hosts	There is maximum number of authenticated hosts supported by the port. Authentication will fail if this number is exceeded. Integer 1-8, default 8

10.7 User Authentication Information

Configuration Steps

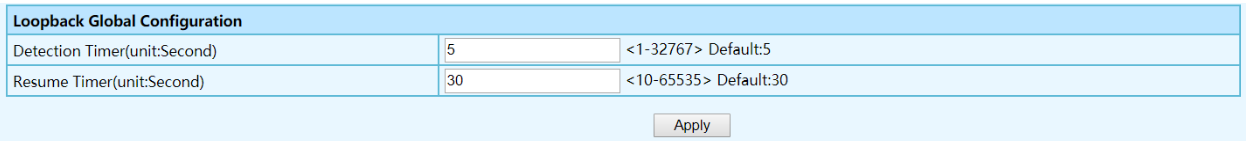
1. Select [Advanced / 802.1X / User Authentication Information] in the navigation bar to enter the [User Authentication Information] interface.
2. Click [Expand] in the upper left corner to expand the user authentication information for all ports and click [Close] to close the user authentication information for all ports. Click the ⊞icon to expand the user authentication information for the corresponding port and click the ⊟icon to close the user authentication information for the corresponding port.
3. The authentication information of the user can be viewed on this interface: username, client MAC address, and the time the authentication passed.
4. Click [Refresh] to refresh the current user authentication information.

Chapter 11 Loop Detection

11.3 Global Configuration

Configuration Steps

1. Select [Advanced / Loopback / Global Setting] in the navigation bar to enter [Global Setting] interface.
2. In the global configuration interface, you can view the global configuration information.
3. To modify the global configuration, modify the corresponding configuration in the Global Configuration box and click [Apply], as shown in Figure 11.1.



Loopback Global Configuration		
Detection Timer(unit:Second)	5	<1-32767> Default:5
Resume Timer(unit:Second)	30	<10-65535> Default:30

Figure 11.1 Loopback Global Configuration

Configuration Description

Table 11.1 Loopback Global Configuration Item Description

Item	Description
Detection Timer	Loop detection packet sending interval, range <1-32767>. The default value is 5

Self-recovery Timer	Port auto recovery period, range <10-65535>, must not be less than 2x detection timer

11.4 Port Configurations

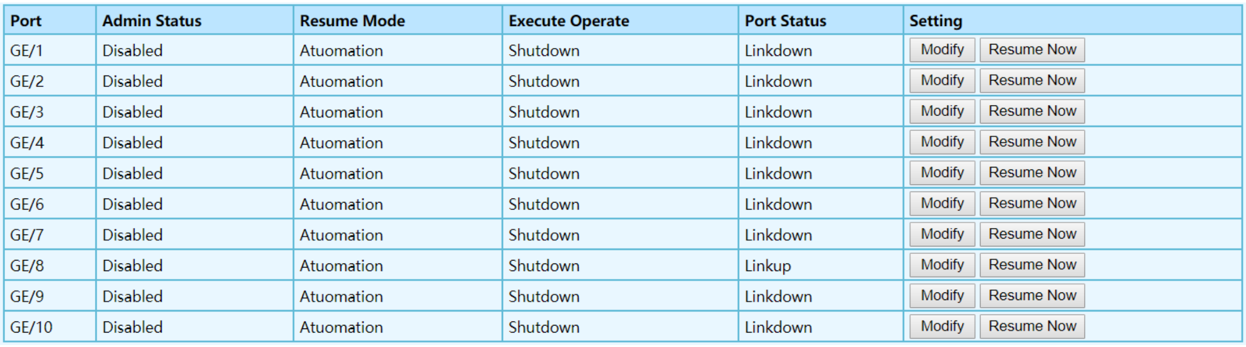
Configuration Steps

1. Select [Advanced / Loop Detection / Port Configuration] in the navigation bar to enter the Port Configuration interface.

2. On the Port Configuration page, you can see the loop detection configuration information and running status of all the ports, as shown in Figure 11.2.

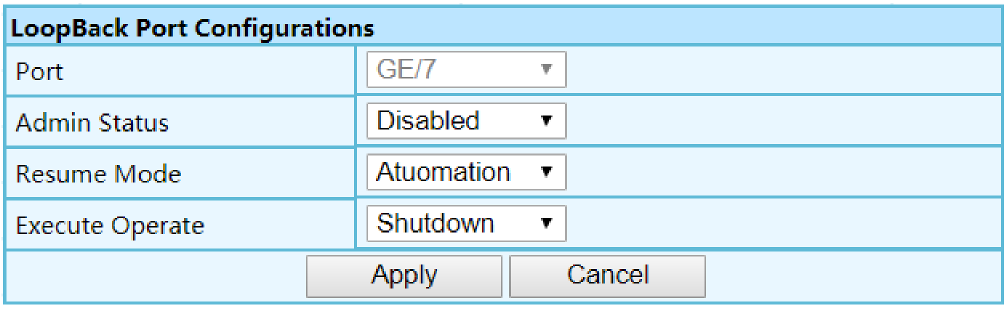
3. To modify the configuration of a port, simply click the [Edit] on the right side of the corresponding entry to enter the modification interface, as shown in Figure 11.3. Modify the corresponding configuration item, click the [Apply] to complete the modification, and click the [Cancel] to cancel the modification.

4. After a loop occurs on a port and the port is shut down or blocked by a specified action, if you want to restore it immediately, you can click the [Restore Now] on the right side of the corresponding entry.



Port	Admin Status	Resume Mode	Execute Operate	Port Status	Setting
GE/1	Disabled	Atuomation	Shutdown	Linkdown	Modify Resume Now
GE/2	Disabled	Atuomation	Shutdown	Linkdown	Modify Resume Now
GE/3	Disabled	Atuomation	Shutdown	Linkdown	Modify Resume Now
GE/4	Disabled	Atuomation	Shutdown	Linkdown	Modify Resume Now
GE/5	Disabled	Atuomation	Shutdown	Linkdown	Modify Resume Now
GE/6	Disabled	Atuomation	Shutdown	Linkdown	Modify Resume Now
GE/7	Disabled	Atuomation	Shutdown	Linkdown	Modify Resume Now
GE/8	Disabled	Atuomation	Shutdown	Linkup	Modify Resume Now
GE/9	Disabled	Atuomation	Shutdown	Linkdown	Modify Resume Now
GE/10	Disabled	Atuomation	Shutdown	Linkdown	Modify Resume Now

Figure 11.2 Loop Detection Port Configuration and Operating Status Viewing



LoopBack Port Configurations	
Port	GE/7 ▼
Admin Status	Disabled ▼
Resume Mode	Atuomation ▼
Execute Operate	Shutdown ▼

Figure 11.3 Loop Detection Port Configuration

Configuration Description

Table 11.2 Loop Detection Port Configuration Description

Item	Description
Management Status	● Prohibited: Disable loop detection ● Enable: Enable loop detection
Recovery Mode	● Automatic: After the loop occurs, the port is closed or blocked, and the port automatically recovers.

	● Manual: After a loop occurs, the port is closed or blocked, need to manually restore the port.
Operations	● Close: After the loop occurs, the port is closed ● Blocked: After a loop occurs, the port is blocked

Chapter 12 Multicast Management

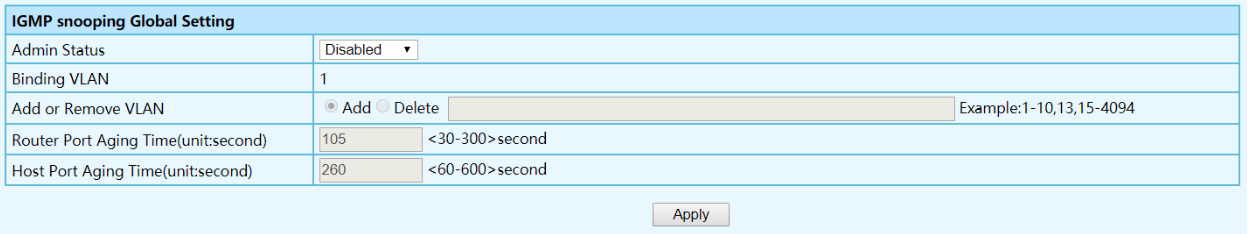
12.1 Global Settings

Configuration Steps

1. Select [Advanced / Multicast / IGMP snooping / Global Setting] in the navigation bar to enter the [Global Setting].

2. You can view the global configuration of IGMP snooping on the IGMP snooping global interface.

3. If you need to modify the global configuration of IGMP snooping, you can modify the corresponding configuration in the configuration box, and then click [Apply], as shown in Figure 12.3.



IGMP snooping Global Setting	
Admin Status	Disabled ▾
Binding VLAN	1
Add or Remove VLAN	● Add ○ Delete [ ] Example:1-10,13,15-4094
Router Port Aging Time(unit:second)	105 <30-300>second
Host Port Aging Time(unit:second)	260 <60-600>second

Figure 12.1 IGMP Snooping Global Settings

Configuration Description

Table 12.1 IGMP Snooping Global Settings Configuration Description

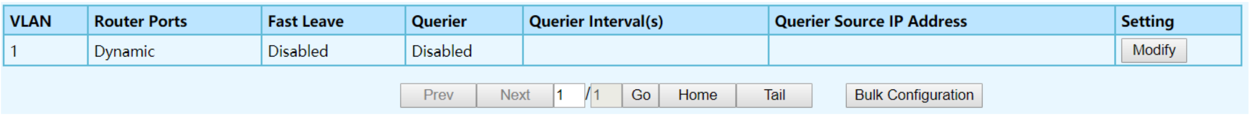
Item	Description
Management status	Select the global enable state of IGMP Snooping: ● Enable: Enable the IGMP snooping function. ● Prohibited: Disable IGMP snooping. Note: It is disabled by default
Bound VLAN	List of VLANs to be bound
Add or Delete VLANs	Select the operation for the VLAN and enter the list of VLANs to add or remove: ● Add: Add a VLAN. The format is as follows: 1-10,13,15-4094; ● Delete: Delete the VLAN. The format is as follows: 1-10,13,15-4094.
Route Port Aging Time	Valid aging time of routed ports, range 30-300. The default is 105. The unit is seconds.
Host Port	Effective host port aging time, range 60-600. The default is 260. The unit is second

Aging Time	

12.2 VLAN settings

Configuration Steps

1. Select [Advanced / IGMP Snooping / VLAN Settings] to enter the VLAN Settings, as shown in Figure 12.2.

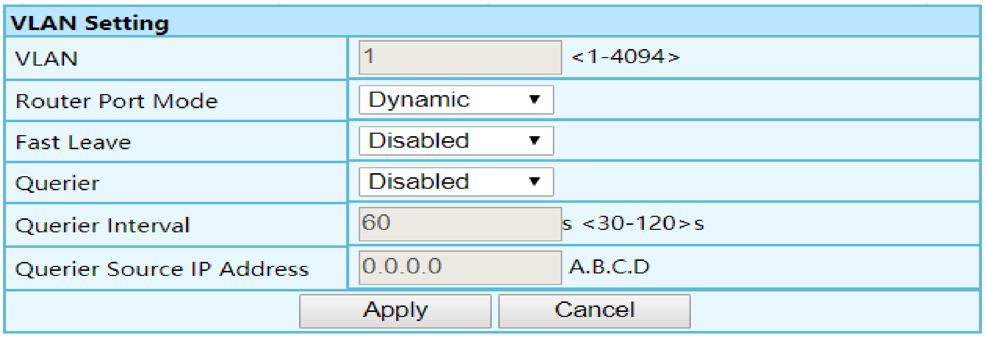


VLAN	Router Ports	Fast Leave	Querier	Querier Interval(s)	Querier Source IP Address	Setting
1	Dynamic	Disabled	Disabled			Modify

Figure 12.2 IGMP Snooping VLAN Setting

2. The IGMP snooping [VLAN Settings] interface displays all the VLAN configuration information of IGMP Snooping.

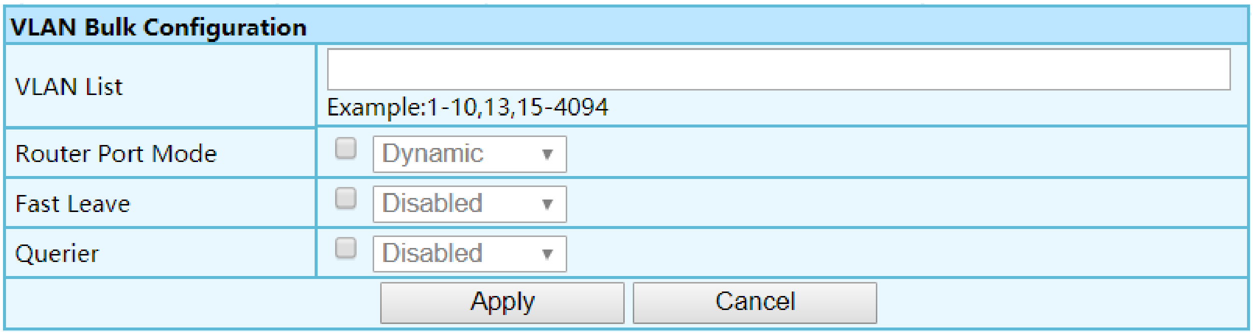
3. Modify individual bound VLAN configuration information. After entering the [VLAN Settings] interface, click the [Modify] to enter the modification interface, as shown in Figure 12.2. Enter valid configuration parameters and click [Apply] to submit the modification. Click [Cancel] to abandon the modification.



VLAN Setting	
VLAN	1 <1-4094>
Router Port Mode	Dynamic
Fast Leave	Disabled
Querier	Disabled
Querier Interval	60 s <30-120>s
Querier Source IP Address	0.0.0.0 A.B.C.D

Figure12.2 IGMP Snooping VLAN Configuration Modification

4. Bind VLAN configuration information in batches. After entering the [VLAN Setting], click the [Bulk Configuration] at the bottom of the page to enter the [VLAN Bulk Configuration], as shown in Figure 12.3. Enter valid configuration parameters and click [Apply] to submit the modification. Click [Cancel] to abandon the modification.



VLAN Bulk Configuration	
VLAN List	Example:1-10,13,15-4094
Router Port Mode	□ Dynamic
Fast Leave	□ Disabled
Querier	□ Disabled

Figure12.3 IGMP snooping VLAN Bulk configuration interface

Configuration Description

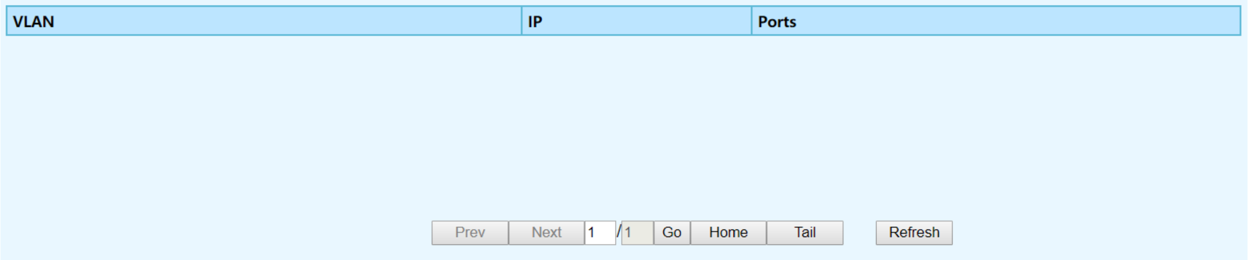
Table 12.3 Configuration Items on the IGMP Snooping

Item	Description
VLAN	VLAN being configured.
Routing Port Mode	Select the mode of the routed port in this VLAN. Use the drop-down box to modify it. ● Dynamic ● Static - If you choose the static routing port mode, you still need to select specific routing ports. ● It can be selected with the check button.
Quick Leave Mode	Select whether to enable the quick leave mode under this VLAN. Use the drop-down box to modify it. ● Prohibited ● Enable
Querier	Select whether to enable the querier function in this VLAN. Use the drop-down box to modify it. ● Prohibited ● Enable - If the querier is enabled, you need to set the corresponding querier interval and query source IP address.
Query Interval	The query interval of the querier is 30-120 seconds.
Query Source IP Address	Set the source IP address of the query message sent by the querier. The valid unicast address is "192.168.1.11". "0.0.0.0" is also available

12.3 IP Group

Configuration Steps

1. Select [Advanced / IGMP snooping / IP Groups] in the navigation bar to enter the IP Group interface, as shown in Figure 12.4.



VLAN	IP	Ports

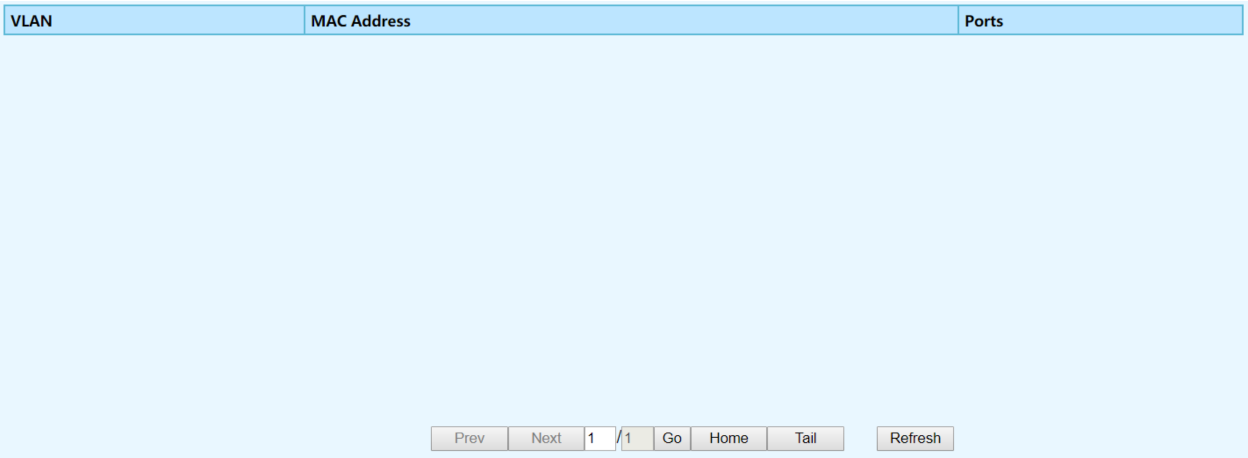
Figure12.4 IGMP Snooping IP Group

2. The IGMP snooping [IP group] interface displays the IP group information maintained by IGMP Snooping and can be refreshed by clicking the [Refresh].

12.4 MAC Groups

Configuration Steps

1. Select [Advanced / IGMP Snooping / MAC Groups] in the navigation bar to enter the MAC Group interface, as shown in Figure 12.5.



VLAN	MAC Address	Ports

Figure 12.5 IGMP snooping MAC group interface

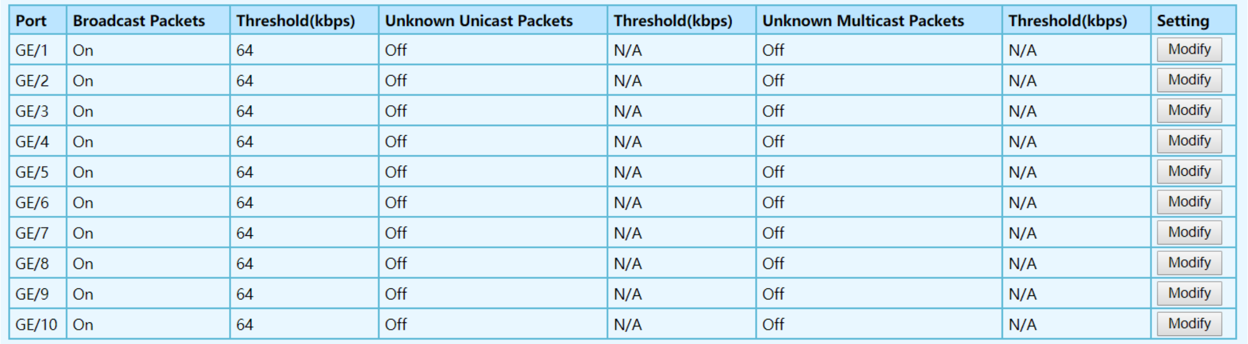
2. The IGMP snooping [MAC Group] interface displays the MAC group information maintained by IGMP Snooping. Click the Refresh button to refresh.

Chapter 13 Security Configuration

13.1 Storm Filter Settings

Configuration Steps

1. Select [Base Configuration / Storm Filters] in the navigation bar to enter [Storm Filters] configuration interface, as shown in Figure 13.1.

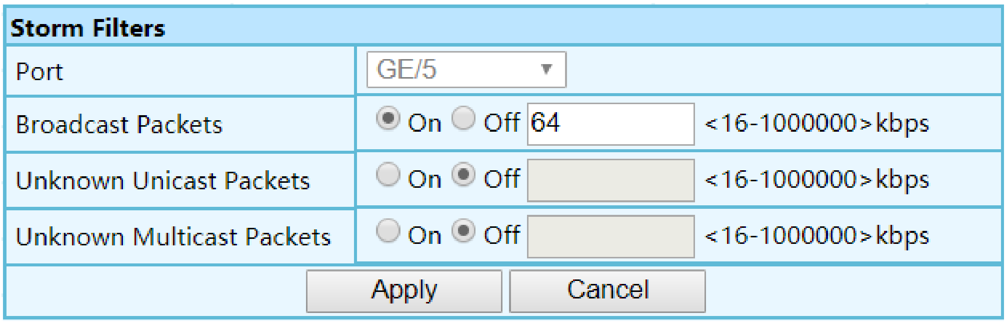


Port	Broadcast Packets	Threshold(kbps)	Unknown Unicast Packets	Threshold(kbps)	Unknown Multicast Packets	Threshold(kbps)	Setting
GE/1	On	64	Off	N/A	Off	N/A	Modify
GE/2	On	64	Off	N/A	Off	N/A	Modify
GE/3	On	64	Off	N/A	Off	N/A	Modify
GE/4	On	64	Off	N/A	Off	N/A	Modify
GE/5	On	64	Off	N/A	Off	N/A	Modify
GE/6	On	64	Off	N/A	Off	N/A	Modify
GE/7	On	64	Off	N/A	Off	N/A	Modify
GE/8	On	64	Off	N/A	Off	N/A	Modify
GE/9	On	64	Off	N/A	Off	N/A	Modify
GE/10	On	64	Off	N/A	Off	N/A	Modify

Figure 13.1 Storm Filter

2. The Storm Filtering interface displays broadcast storm filtering configuration information for each port.

3. To modify the port storm filtering configuration information, click the [Modify] to enter the [Storm Filters] modification interface, as shown in Figure 13.2. Enter valid configuration parameters and click [Apply] to submit the changes. Click [Cancel] to cancel the modification



Storm Filters	
Port	GE/5
Broadcast Packets	● On ○ Off 64 <16-1000000>kbps
Unknown Unicast Packets	○ On ● Off <16-1000000>kbps
Unknown Multicast Packets	○ On ● Off <16-1000000>kbps

Figure13.2 Storm Filter Modify

Configuration Description

Table13.1 Storm Filters Configuration Description

Item	Description
Port	Modify the configured port
Broadcast Message	Select whether to enable rate suppression on broadcast packets, selected by radio button. • ON- If you choose to enable, enter the corresponding rate suppression value, <16-1000000>, and enter 16, unit is kbps • OFF
Unknown Unicast Packets	Select whether to enable rate suppression for unknown unicast packets, selected by radio button. • On - If you choose to enable, enter the corresponding rate suppression value, <16-1000000>, enter 16, unit is kbps • OFF
Unknown Multicast Packet	Select whether to enable rate suppression for unknown multicast packets, selected by radio button. • On - If you choose to enable, enter the corresponding rate suppression value, <16-1000000>, enter 16, unit is kbps • OFF

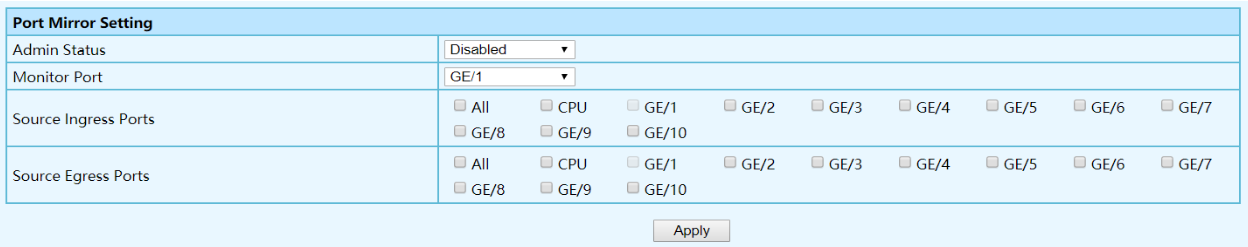
13.2 Port Mirroring

13.2.1 Port Mirroring Setting

Configuration Steps

1. Select [Base Configuration / Port Mirror] in the navigation bar to enter the [Port Mirror]

configuration interface, as shown in Figure 13.3.



Port Mirror Setting	
Admin Status	Disabled ▾
Monitor Port	GE/1 ▾
Source Ingress Ports	□ All □ CPU □ GE/1 □ GE/2 □ GE/3 □ GE/4 □ GE/5 □ GE/6 □ GE/7 □ GE/8 □ GE/9 □ GE/10
Source Egress Ports	□ All □ CPU □ GE/1 □ GE/2 □ GE/3 □ GE/4 □ GE/5 □ GE/6 □ GE/7 □ GE/8 □ GE/9 □ GE/10

Figure13.3 Port Mirror Setting

2. Modify the port mirroring configuration information. Pull down and select to disable or enable mirroring, select the mirroring destination port, check the ingress port and egress port, the ingress or egress cannot contain the destination port, and click [apply] to submit the modification

Configuration Description

Table13.2 Port Mirroring Configuration Description

Item	Description
Management Status	Select whether to enable port mirroring
Destination Port	Select the destination port for port mirroring via drop-down box
Source Port List	Select the source port list in the ingress direction. It can be selected with the check button. (The source port list cannot contain the destination port)
Export source port list	Select the source port list in the egress direction. It can be selected with the check button. (The source port list cannot contain the destination port)

Chapter 14 Reliability Configuration

14.3 Link Aggregation Setting

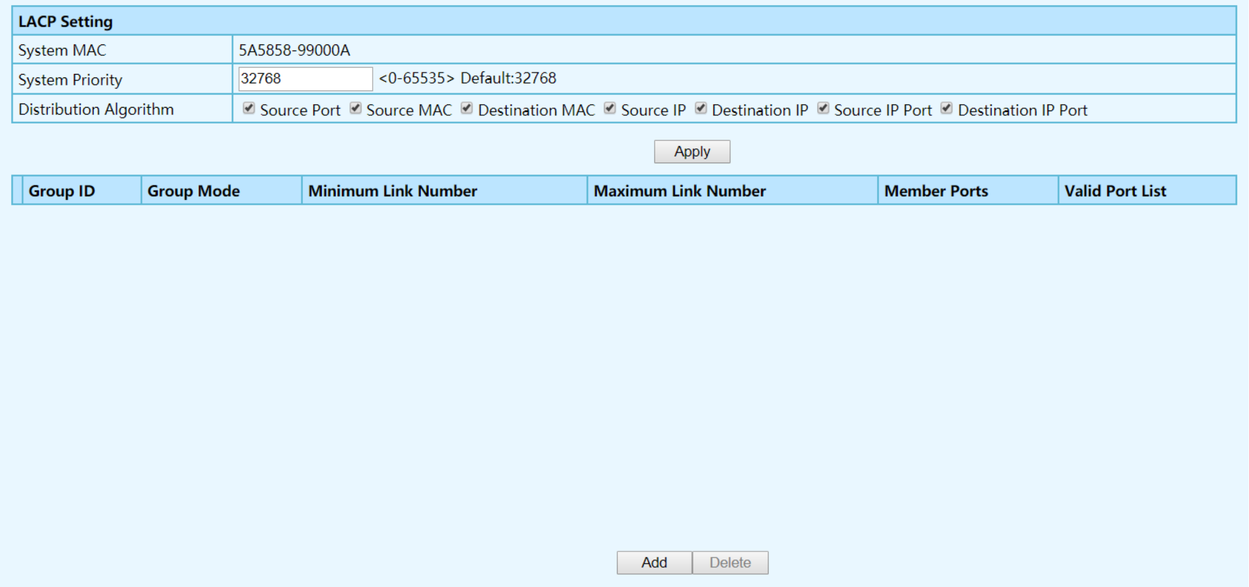
14.3.1 Link Aggregation Global Setting

Configuration Steps

1.Select [Advanced / Link Aggregation / Global Setting] in the navigation bar to enter the [Link Aggregation / Global Setting] interface.

2.The link aggregation global configuration can be viewed in the link aggregation global setting interface.

3.To modify the global configuration of link aggregation, modify the corresponding configuration in the LACP (Link Aggregation Control Protocol) configuration box, and then click [Apply], as shown in figure 14.1.

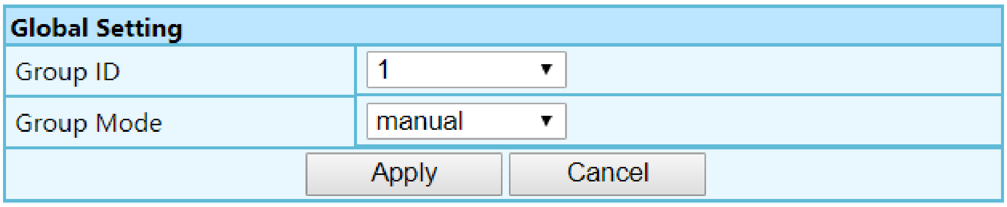


LACP Setting	
System MAC	5A5858-99000A
System Priority	32768 <0-65535> Default:32768
Distribution Algorithm	☑ Source Port ☑ Source MAC ☑ Destination MAC ☑ Source IP ☑ Destination IP ☑ Source IP Port ☑ Destination IP Port

Group ID	Group Mode	Minimum Link Number	Maximum Link Number	Member Ports	Valid Port List

Figure 14.1 LACP Global Setting

4.If you want to add an aggregation group, click [set], as shown in figure 14.2. click [Apply]. There will be hints.



Global Setting	
Group ID	1 ▼
Group Mode	manual ▼

Figure 14.2 Add Aggregation Group

Configuration Description

Table 14.1 Link Aggregation [Global Setting] Configuration Description

Item	Description
Management Status	**Link Aggregation Global Enable Switch** ●Enable: Enable link aggregation function ●Disable: Close link aggregation function
System Priority	Set the link aggregation system priority, range 0-65535, default value 32768, the smaller the better.
Load Sharing Algorithm	The system supports one or more to compute the load ports according to the source port, source MAC, destination MAC, source IP, destination IP, source IP port and destination IP port in the message.

Setting	Select the aggregation group that needs to be modified in the selection box of the aggregation group and click [Set] to modify the corresponding aggregation group configuration.

Table 14.2 Link Aggregation [Global Setting] Setting Configuration Description

Item	Description
Aggregation Group ID	Aggregation Group ID information
Aggregation Group Mode	Set Aggregation Group Mode ●Manual: Manual mode, the port of the aggregation group member is manually configured and the port LACP protocol is closed. ●Static: Static mode, the port of the aggregation group member is manually configured and the port LACP protocol is on.
Minimum Port	The active ports minimum number of aggregation group configuration, ranging <0-8>, and the value cannot exceed the maximum number of links.
Maximum Port	The active ports maximum number of aggregation group configuration, ranging <0-8>, and the value cannot be less than the minimum number of links.
Member Port List	Member port of aggregation group configuration

14.3.2 Link Aggregation Port Setting

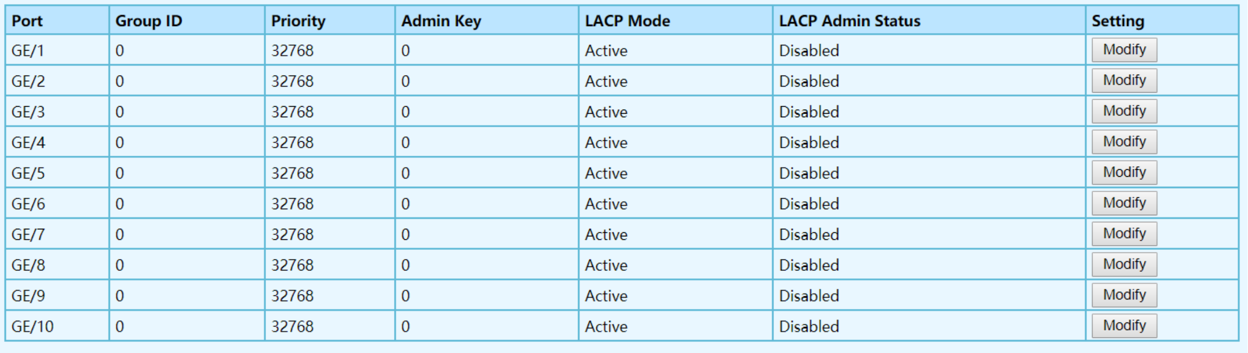
Configuration Steps

1. Select [Advanced / Link Aggregation / Port Configurations] in the navigation bar to enter the link aggregation [Port Configurations] interface, as shown in figure 14.3.

2. In the link aggregation [Port Configuration] interface, you can view the link aggregation related configuration of the port.

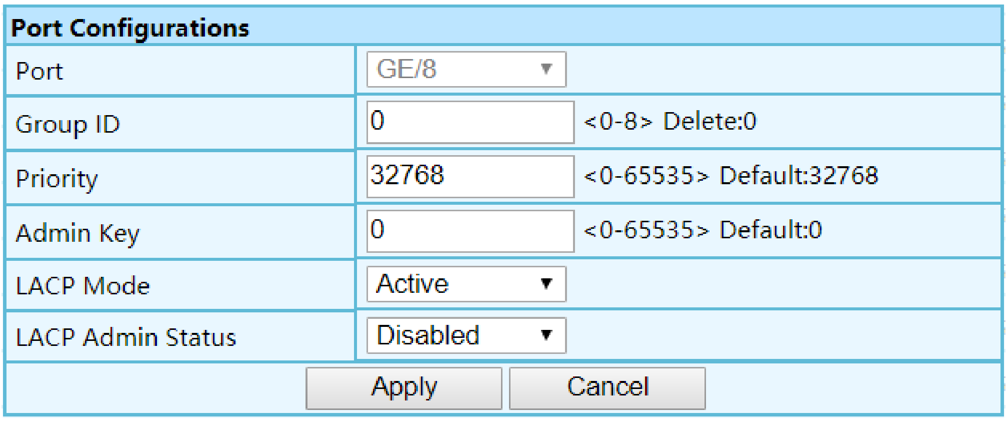
3. If the link aggregation configuration of the port needs to be modified, click the [Modify] to enter the port configuration interface, as shown in figure 14.4.

4. Select or fill in the configuration items that need to be modified and click [Apply] to make effective. If the configuration items are incorrectly filled, there will be corresponding prompts.



Port	Group ID	Priority	Admin Key	LACP Mode	LACP Admin Status	Setting
GE/1	0	32768	0	Active	Disabled	Modify
GE/2	0	32768	0	Active	Disabled	Modify
GE/3	0	32768	0	Active	Disabled	Modify
GE/4	0	32768	0	Active	Disabled	Modify
GE/5	0	32768	0	Active	Disabled	Modify
GE/6	0	32768	0	Active	Disabled	Modify
GE/7	0	32768	0	Active	Disabled	Modify
GE/8	0	32768	0	Active	Disabled	Modify
GE/9	0	32768	0	Active	Disabled	Modify
GE/10	0	32768	0	Active	Disabled	Modify

Figure 14.3 Link Aggregation Port Information



Port Configurations	
Port	GE/8 ▼
Group ID	0 <0-8> Delete:0
Priority	32768 <0-65535> Default:32768
Admin Key	0 <0-65535> Default:0
LACP Mode	Active ▼
LACP Admin Status	Disabled ▼

Figure 14.4 Link Aggregation Port Configuration

Configuration Description

Table 14.3 Link Aggregation [Port Configuration] Configuration Description

Item	Description
Modify	Modify the port configuration of link aggregation

Table 14.4 Link Aggregation [Port Configuration] Modification Configuration Description

Item	Description
Port	Port name
Aggregation Group ID	The port ID of aggregation group

Priority	Port link aggregation priority, range <0-65535>, default value 32768, the smaller the better
LACP Port Mode	Port master-slave mode in LACP protocol ●Active: Active mode, the port sends protocol messages automatically when LACP protocol enabled. ●Passive: Passive mode, the port will not send protocol messages automatically, but only send when received protocol messages. Note: Port default by Active mode
LACP Timeout Mode	Port timeout mode in LACP protocol ●Quick: Quick timeout mode, timeout 1 second ●Slow: Slow timeout mode, timeout 30 seconds Note: Port default by Slow mode
LACP Enable Status	Port LACP Enable Status ●Enable: Turn on port LACP ●Prohibit: Close port LACP Note: Port default by Prohibit

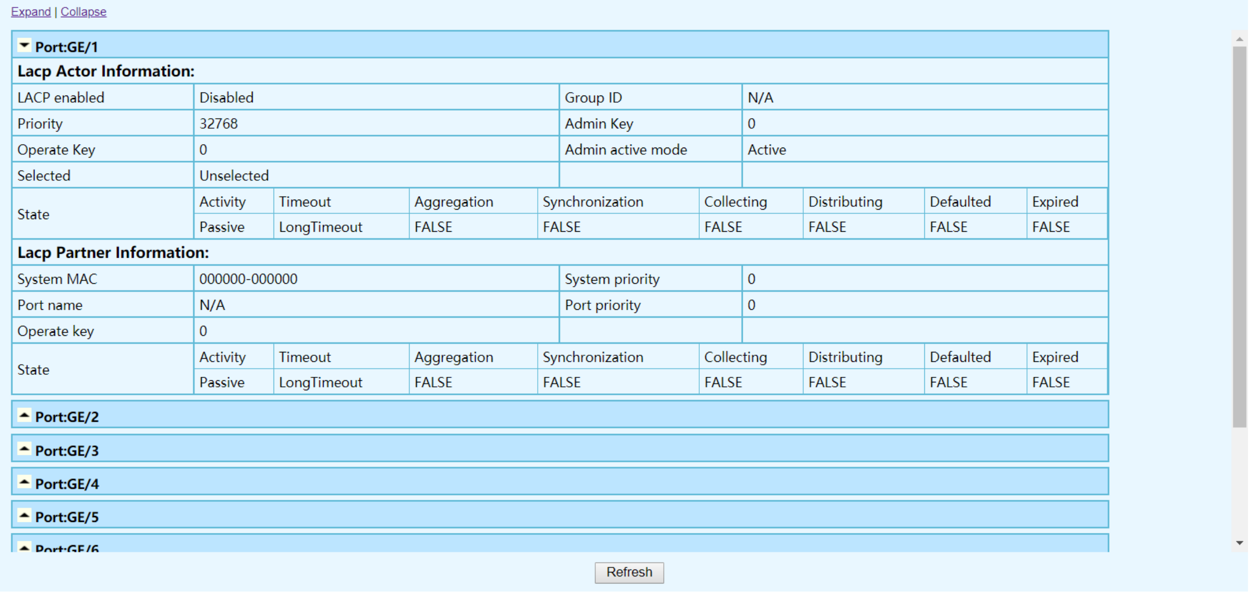
14.3.3 Link Aggregation Information

Configuration Steps

1. Select [Advanced / Link Aggregation / Aggregate Information]in the navigation bar to enter the [Link Aggregation / Aggregation Information] interface.

2. In the link aggregation [Aggregate Information] interface, all port link aggregation related information can be viewed, as shown in figure 14.4.

3. Click [Refresh] to see the latest aggregation information for each port.



Port:GE/1

Lacp Actor Information:

LACP enabled	Disabled	Group ID	N/A
Priority	32768	Admin Key	0
Operate Key	0	Admin active mode	Active
Selected	Unselected		

State	Activity	Timeout	Aggregation	Synchronization	Collecting	Distributing	Defaulted	Expired
	Passive	LongTimeout	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE

Lacp Partner Information:

System MAC	000000-000000	System priority	0
Port name	N/A	Port priority	0
Operate key	0		

State	Activity	Timeout	Aggregation	Synchronization	Collecting	Distributing	Defaulted	Expired
	Passive	LongTimeout	FALSE	FALSE	FALSE	FALSE	FALSE	FALSE

Port:GE/2

Port:GE/3

Port:GE/4

Port:GE/5

Port:GE/6

Figure 14.5 Port Aggregation Information

Chapter 15 SNMP

15.3 Base Configuration

Configuration Steps

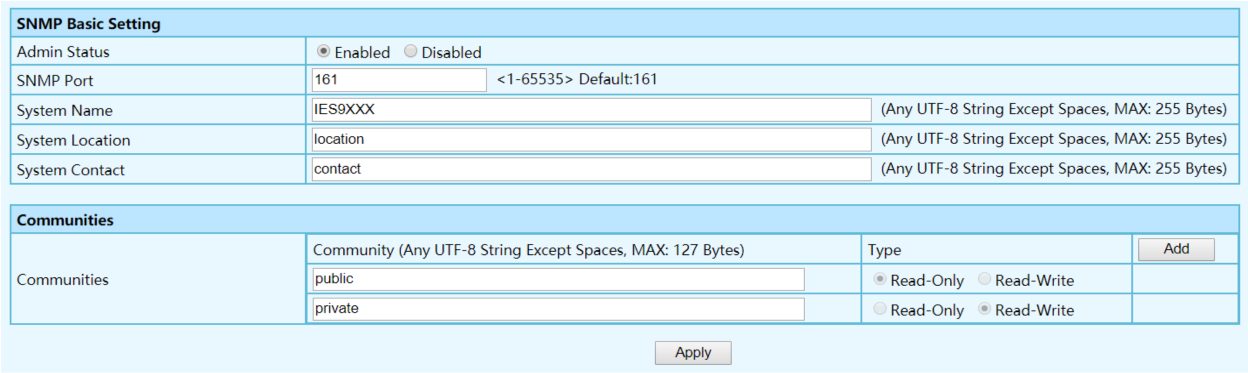
1.Select [Management / SNMP / V1/V2 Setting] in the navigation bar to enter the SNMP [Base Setting] interface.

2.You can view the Base Setting of SNMP in the [SNMP Base Setting] interface.

3.To modify the Base Configuration, modify the corresponding configuration in the configuration box, and then click [Apply] to make effective, as shown in figure 15.1.

4. If you want to add a group word, click [Add] and a group word is added to set the group word name and type. The system supports up to eight group characters, with the first and second being the default, so you can add up to six more. Click [Apply] to make effective.

5. To delete a group word, click [Delete] on the right corresponding entry (the first and second are the system default, cannot be deleted), and click [Apply] to make effective.



SNMP Basic Setting	
Admin Status	● Enabled ○ Disabled
SNMP Port	161 <1-65535> Default:161
System Name	IES9XXX (Any UTF-8 String Except Spaces, MAX: 255 Bytes)
System Location	location (Any UTF-8 String Except Spaces, MAX: 255 Bytes)
System Contact	contact (Any UTF-8 String Except Spaces, MAX: 255 Bytes)

Communities			
Communities	Community (Any UTF-8 String Except Spaces, MAX: 127 Bytes)	Type	Add
	public	● Read-Only ○ Read-Write	
	private	○ Read-Only ● Read-Write	

Apply

Figure 15.2 SNMP Base Configuration

Configuration Description

Table 15.2 SNMP Base Configuration Description

Item	Description
Management Status	SNMP Global Enable Status: ●Enable: Turn on SNMP function ●Prohibit: Close SNMP function Note: Default by Enable
SNMP Port	SNMP port with range <1-65535>, default 161
System Name	System name, any legal character other than a space can be entered with a maximum length of 255
System Location Information	System location information, any legal character other than a space can be entered with a maximum length of 255
System Contact Information	System contact information, any legal character other than a space can be entered with a maximum length of 255
Group Characters	SNMP Group Characters: ●Name: Any legal character other than a space can be entered with a maximum length of 127 ●Type: Read and write Note: The system supports a maximum of 8 group characters and requires at least two group characters. The default two group characters can only change the group name, cannot change the type or delete.Click [Add] to add a group character, add a group character can change the name and

	type, and delete.

15.4 Trap Setting

Configuration Steps

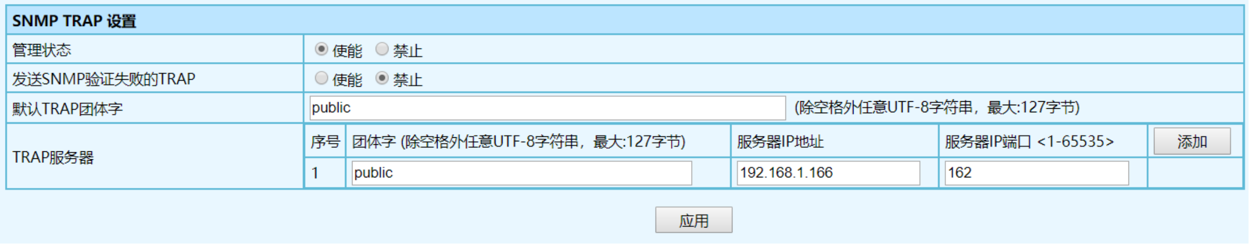
1. Select [Management / SNMP / Trap Setting] in the navigation bar and enter the SNMP [Trap Setting] interface.

2. The current trap configuration of SNMP can be viewed in the SNMP [Trap Setting] interface.

3. If you need to modify the Trap Setting, modify the corresponding configuration in the configuration box, and then click [Apply], as shown in figure 15.3.

4. If you want to add a Trap server, click [Add] and the Trap server entry will occur. The system supports up to 4 groups of Trap servers, the first group is the default of the system and cannot be deleted, so you can add up to 3 groups of Trap servers, click [Apply] to make effective.

5. If you want to delete the Trap server, click [Delete] on the right of the corresponding entry (where group 1 is the default of the system and cannot be deleted), and click [Apply] to make effective.



SNMP TRAP 设置

管理状态: ● 使能 ○ 禁止

发送SNMP验证失败的TRAP: ○ 使能 ● 禁止

默认TRAP团体字: public (除空格外任意UTF-8字符串，最大:127字节)

TRAP服务器:

序号	团体字 (除空格外任意UTF-8字符串，最大:127字节)	服务器IP地址	服务器IP端口 <1-65535>	添加
1	public	192.168.1.166	162	

Figure **15.3 SNMP Trap Setting**

Configuration Description

Table 15.3 SNMP [Trap Setting] Configuration Description

Item	**Description**

Management Status	Trap Global Enable Status: ●Enable: Turn on Trap function ●Enable: Close Trap function Note: Default by Enable
Trap Version	Trap version support V1 and V2
Sending SNMP Authentication Failed Trap	Enable or Disable the Sending SNMP Authentication Failed Trap: ●Enable: Enable the Sending SNMP Authentication Failed Trap ●Enable: Close the Sending SNMP Authentication Failed Trap Note: Default by Prohibit
Default Trap Group Characters	Default trap group characters, any legal character other than a space can be entered with a maximum length of 127
Trap Server	Set Trap Server: ●Group Characters: Any legal character other than a space can be entered with a maximum length of 127 ● Server IP Address: The IP address of trap serve, IPv4, dot decimal format. ● Server IP Port: The IP port of trap serve, range <1-65535>, default 162 Note: The system supports up to 4 servers. Click the [Add]to add. The system default server number:1, group character: public, IP address: 192.168.1.200, IP port: 162. The default server cannot be deleted, but the added server can be deleted.

Chapter 16 IP interface

This chapter describes the IP interface in detail, mainly including the following contents:

- IP Address

- DHCP Client Configuration

16.1 IP Address

16.1.1 IP Address Introduction

IP (Internet Protocol Address) is short for IP Address. IP address is a unified address format provided by the IP protocol, which assigns a logical address to each network and host on the Internet to mask physical address differences.

IP address consists of two parts: network address (Net-id) and Host address (Host-id).

Network address is to distinguish between different networks, and host address is to distinguish between different hosts within a network.

IP address is classified into five categories, as detailed in the following table:

IP Address Type	IP Address Range	Description
A	0.0.0.0-127.255.255.255	The IP address 0.0.0.0 is only used for temporary communication between the host and the current host when the system is started. 127.0.0.1 to 127.255.255.255 is used for loop testing. Groups sent to this address are not output to the link and are treated internally as input groups.
B	128.0.0.0-191.255.255.255	-
C	192.0.0.0-223.255.255.255	It is for small scale LAN, and each network can only contain 254 computers at most
D	224.0.0.0-239.255.255.255	Multicast address
E	240.0.0.0-255.255.255.255	255.255.255.255 is for broadcast address, other address is reserved for future use

Some IP addresses are reserved for special purposes. Users cannot configure IP interfaces as host addresses:

1. The address with each byte being 0 (" 0.0.0.0 ") corresponds to the current host;

2. Each IP address that is 1 (" 255.255.255.255 ") is the broadcast address of the current subnet;

3. Any class E IP address starting with '11110' shall be reserved for future and experimental use;

4. An IP address cannot begin with a decimal '127'. Change the address number 127.0.0.1 to 127.255.255.255 is for loop testing, such as: 127.0.0.1 can represent the local IP address, and 'http: / / 127.0.0.1' can be used to test the local Web server.

5. The first 8-bit group network ID cannot be fully set to '0', '0' indicates the address;

6. In IP network, the same network address can be directly communicated, while the address of different networks cannot.

16.1.2 Base Configuration

Configuration Steps

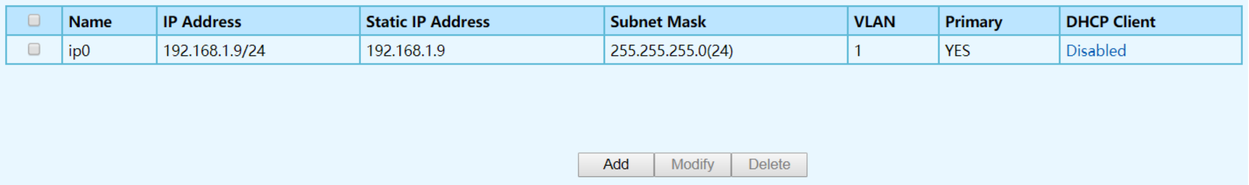
1. Select [Management / IP Interface / Setting] in the navigation bar to enter the IP interface [Setting].

2. All current IP interface and configuration information can be viewed in the IP interface [Setting], as shown in figure 16.1.

3. To add a new IP interface, click [Add], then fill in the relevant configuration, and click [Apply], as shown in figure 16.2.

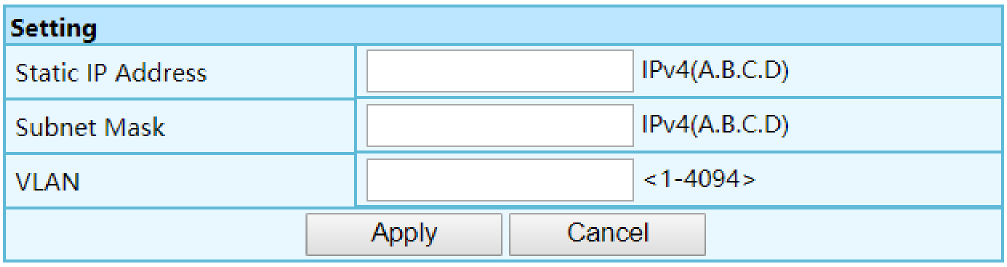
4. To modify an IP interface, check the corresponding IP interface, click [modify], then modify the configuration, and click [Apply], the IP interface is shown in figure 16.2.

5. To delete an IP interface, check the appropriate IP interface and click [Delete].



□	Name	IP Address	Static IP Address	Subnet Mask	VLAN	Primary	DHCP Client
□	ip0	192.168.1.9/24	192.168.1.9	255.255.255.0(24)	1	YES	Disabled

Figure 16.1 IP Interface Viewing



Setting		
Static IP Address		IPv4(A.B.C.D)
Subnet Mask		IPv4(A.B.C.D)
VLAN		<1-4094>

Figure 16.2 IP Interface Setting

Configuration Description

Table 16.1 IP Interface [Setting] Configuration Description

Item	Description
Static IP Address	Static IPv4 address, the format is dot decimal system, each interface IPv4 address cannot be in the same network segment.
Mask	The mask of IPv4 address
VLAN	VLAN bound by assigned IP interface

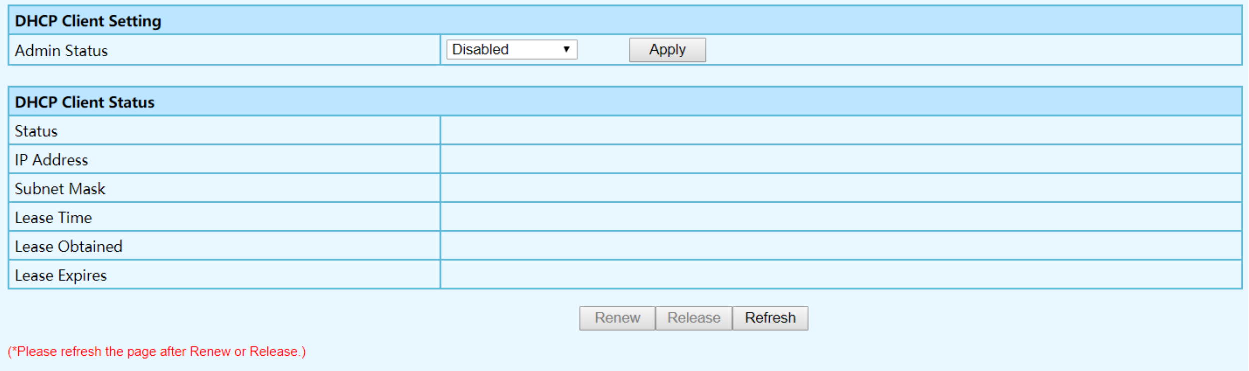
16.2 DHCP Client Configuration

Note: DHCP functions are described in detail in Chapter 17

Configuration Steps

1.Select [Management / IP Interface / DHCP Client] in the navigation bar to enter the [DHCP Client] interface.

2.In the [DHCP Client] interface, you can view the current configuration information and DHCP client status.



DHCP Client Setting	
Admin Status	Disabled ▾ Apply

DHCP Client Status	
Status	
IP Address	
Subnet Mask	
Lease Time	
Lease Obtained	
Lease Expires	

(*Please refresh the page after Renew or Release.)

Figure 16.3 DHCP Client Configuration

Configuration Description

Table 16.2 [DHCP Client] Configuration Description

Item	Description
Management Status	Enable or Prohibit DHCP Client ●Enable: Enable DHCP Client

	●Prohibit: Prohibit DHCP Client Note: Default by Prohibit
Retrieve	DHCP Client retrieves the configuration
Release	DHCP Client s the current configuration

Chapter 17 DHCP

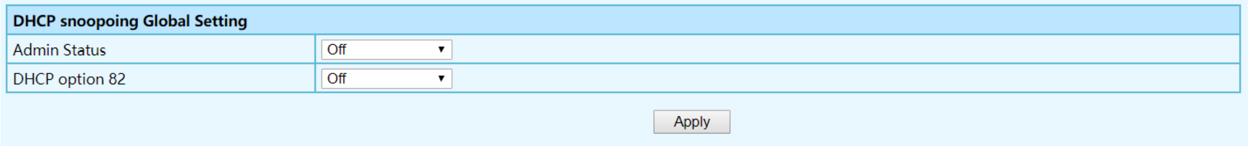
17.1.5 Global Setting

Configuration Steps

1. Select [Advanced / DHCP Snooping / Global Setting] in the navigation bar to enter the [Global Setting] interface of DHCP snooping.

2. The global configuration information can be viewed in of DHCP snooping [Global Setting] interface.

3. To modify the global configuration of DHCP snooping in the DHCP snooping global configuration box, click [Apply], as shown in figure 17.1.



DHCP snoopoing Global Setting

Admin Status	Off
DHCP option 82	Off

Figure 17.1 DHCP Snooping Global Setting

Configuration Description

Table 17.1 DHCP Snooping [Global Setting] Configuration Description

Item	Description
Management	DHCP Snooping Global Enable Switch

Status	●ON: Enable DHCP snooping function ●OFF: Disable DHCP snooping function Note: Default by OFF

17.1.6 Port Setting

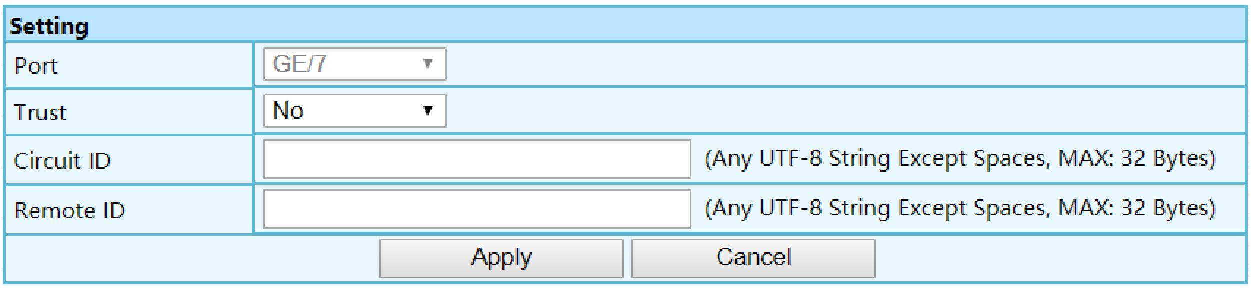
Configuration Steps

1. Select [Advanced / DHCP Snooping / Port Setting] in the navigation bar to enter the DHCP snooping [Port Setting] interface.

2. The port configuration can be viewed in the DHCP snooping [Port Setting] interface.

3. To modify the DHCP snooping configuration for a port, click the [modify] to enter the port configuration interface, as shown in figure 17.2.

4. Select or fill in the configuration items that need to be modified and click [Apply] to make effective. There will be prompts if the configuration items are incorrectly filled.



Setting	
Port	GE/7 ▼
Trust	No ▼
Circuit ID	(Any UTF-8 String Except Spaces, MAX: 32 Bytes)
Remote ID	(Any UTF-8 String Except Spaces, MAX: 32 Bytes)

Figure 17.2 DHCP Snooping Port Setting

Configuration Description

Table 17.2 DHCP Snooping [Port Setting] Modification Configuration Description

Item	Description
Port	The name information
Trust	Port Trust: ●YES: Set as trust port ●NO: Set as untrust port Note: Default by NO
Agent Circuit ID	Default by global agent circuit ID
Agent Remote ID	Default by global agent remote ID

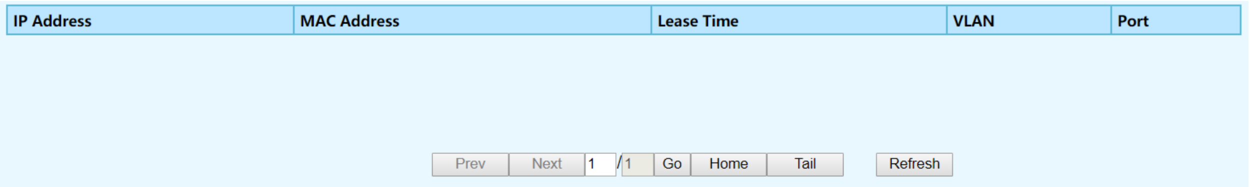
17.1.7 Binding Table

Configuration Steps

1.Select [Advanced / DHCP Snooping / Binding Table] in the navigation bar to enter the DHCP snooping [Binding Table] interface.

2.All bind list information can be viewed in the DHCP snooping [Binding Table] interface, as shown in figure 17.3.

3.Click [Refresh] to update all DHCP snooping bind list information



IP Address	MAC Address	Lease Time	VLAN	Port

Figure DHCP Snooping Binding Table

Chapter 18 Administrator

This chapter describes the administrator in detail, including the following:

- User Management
- Online User
- Login Timeout Setting

18.1 User Management

Configuration Steps

1. Select [System / Administrator / Administrators] in the navigation bar to enter the [Administrators] interface.

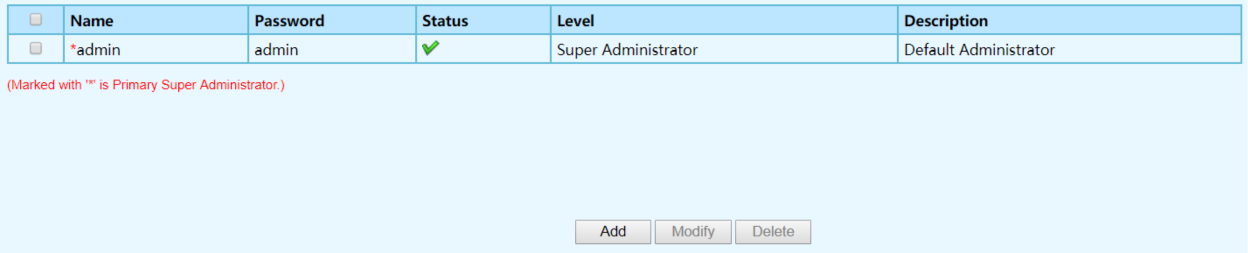
2. The current user configuration information can be viewed in the [Administrators] interface, as shown in figure 18.1.

3. To add a new user, click [Add] to enter the administrator configuration interface, fill in the corresponding configuration items, click [Apply] to finish adding the user, and add the user interface as shown in Figure 18.2.

4. If need to modify the user information, select the corresponding user firstly, and then click

[Modify] to enter the user configuration modification interface and modify the corresponding configuration item. Click [Apply] to complete the configuration modification and modify the user interface as shown in Figure 18.3

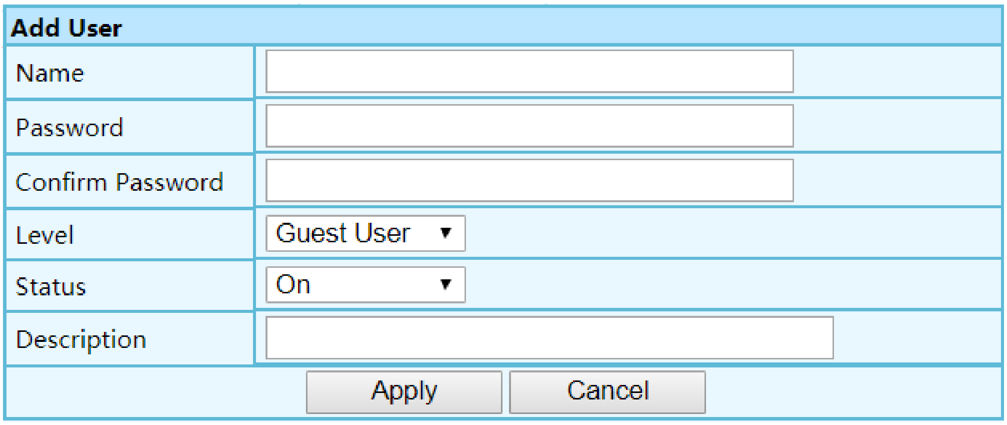
5. To delete a user, firstly select the corresponding user and click [Delete] to delete the user.



□	Name	Password	Status	Level	Description
□	*admin	admin	✓	Super Administrator	Default Administrator

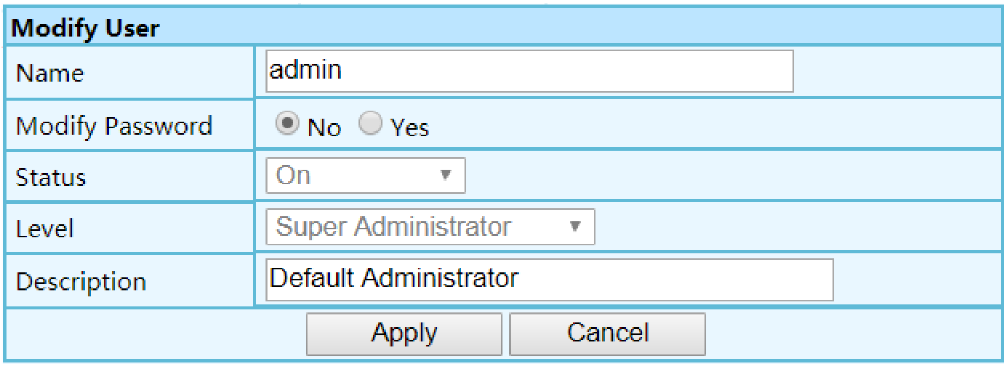
(Marked with "*" is Primary Super Administrator.)

Figure 18.1 Administrator



Add User	
Name	
Password	
Confirm Password	
Level	Guest User
Status	On
Description	

Figure 18.2 Add a User



Modify User	
Name	admin
Modify Password	● No ○ Yes
Status	On
Level	Super Administrator
Description	Default Administrator

Figure 18.3 Modify User Interface

Configuration Description

Table 18.1 [Administrator] Configuration Description

Item	Description

Username	Username information.
Password	User password.
Status	User activation status: ●✓ : Activate ●✗ : Inactive By default, new users are activated
Level	User level including: Super Administrator, Senior Administrator, Junior Administrator, Guest User
Description	User description information

Table 18.2 [User Management] Add User Configuration Description

Item	Description
Username	Username information, valid characters A-Z, a-z, 0-9, _, length 1-32 bytes
Password	User login password, any printable ASCII characters, length 1-16 bytes.
Confirm Password	Re-enter the login password to confirm.
Level	Set the user's level, including: ● Super administrator ● Senior Administrator ● Junior Administrator ● Guest users Note: Default by guest user.
Status	User activation status, including ● On: Activate ● Off: Inactive Note: Default by on.
Description	User description information, any printable ASCII character, length 1-128 bytes.

Table 18.3 [User Management] Modify User Configuration Description

Item	Description

Username	Username information, valid characters A-Z, a-z, 0-9, _, length 1-32 bytes
Old Password	The password for the user to log in to the web interface.
Password	New password set by the user, any printable ASCII character, length 1-16 bytes.
Confirm Password	Re-enter the new password set by the user and confirm the password.
Level	Set the user's level, including: ● Super administrator ● Senior Administrator ● Junior Administrator ● Guest users
Status	User activation status, including ON and OFF.
Description	User description information, any printable ASCII character, length 1-128 bytes.

Precautions

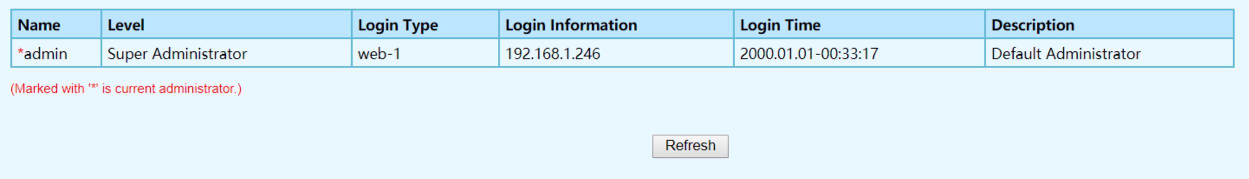
The device has a super administrator (username admin) by default and cannot be deleted. The user level cannot be changed. Extra 15 users can be added in addition to this user.

18.2 Online User

Configuration Steps

1. Select [System / Administrator / Online Users] in the navigation bar to enter the [Online Users] interface.

2. In the interface of [Online Users], you can view the user information of the current logged in device



Name	Level	Login Type	Login Information	Login Time	Description
*admin	Super Administrator	web-1	192.168.1.246	2000.01.01-00:33:17	Default Administrator

(Marked with '*' is current administrator.)

Figure 18.4 Online User Information

Configuration Description

Table 18.4 [Online User] Configuration Description

Item	Description
Username	Username information
Level	User level, including: Super Administrator, Senior Administrator, Junior Administrator, Guest User
Description	User description information.
Login Method	Web, console, telnet
Login IP Address	The client IP address of user login, except the console mode login.
Login Time	The time that the user logs in to the device。

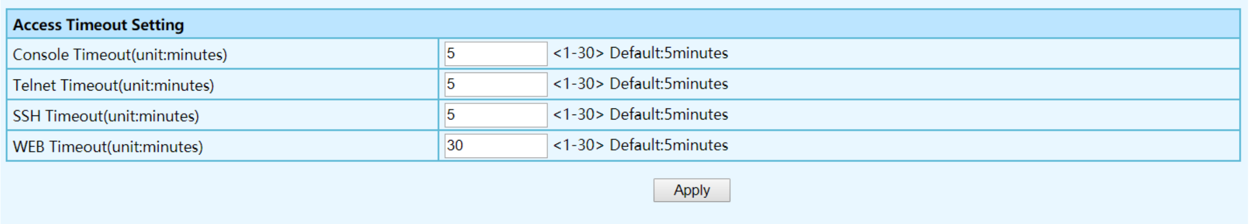
18.3 Login Timeout Setting

Configuration Steps

1. Select [System / Administrator / Management Setting] in the navigation bar to enter the [Login Timeout Setting] interface.

2. In the Login Timeout Settings interface, you can view the settings related to the login timeout.

3. To change the login timeout period, fill in the timeout period of the corresponding login mode and click [Apply] to complete the configuration modification, as shown in Figure 18.5.



Access Timeout Setting		
Console Timeout(unit:minutes)	5	<1-30> Default:5minutes
Telnet Timeout(unit:minutes)	5	<1-30> Default:5minutes
SSH Timeout(unit:minutes)	5	<1-30> Default:5minutes
WEB Timeout(unit:minutes)	30	<1-30> Default:5minutes

Figure 18.5 Login Timeout Setting

Configuration Description

Table 18.5 [Login Timeout Setting] Configuration Description

Item	Description
Console Timeout	The login timeout period via console port, range 1 to 30. The default value is 5 and the unit is minute.
Telnet Timeout	The login timeout period via telnet, range 1 to 30. The default value is 5 and the unit is minute.
Web Timeout	The login timeout period via web, range 1 to 30. The default value is 5 and the unit is minute.

Precautions

The setting can only take effect in next login after setting the timeout period for different login methods.

Chapter 19 System Configuration

This chapter describes the system configuration in detail, including the following:

- System Log
- Configurations
- Date and Time
- Software Upgrade
- Software Restart

After the device is configured, you need to save the configuration information to the device. The newly saved configuration information will cover the original configuration information. After the configuration is complete, if you do not perform the save operation, the new configuration will be lost when the device is restarted, and the original configuration will continue to be executed.

When the device fails, you can try to solve the problem by restarting the device according to the actual situation. In system configuration, you can manage the configuration of the system, including erasing the configuration, saving the configuration, and restarting the device. Users can also view and configure the corresponding system start-up management according to needs.

19.1 System Log

19.1.1 Settings

Configuration steps

1. Select [System / System Log / Setting] in the navigation bar to enter the System Log [Setting] interface.

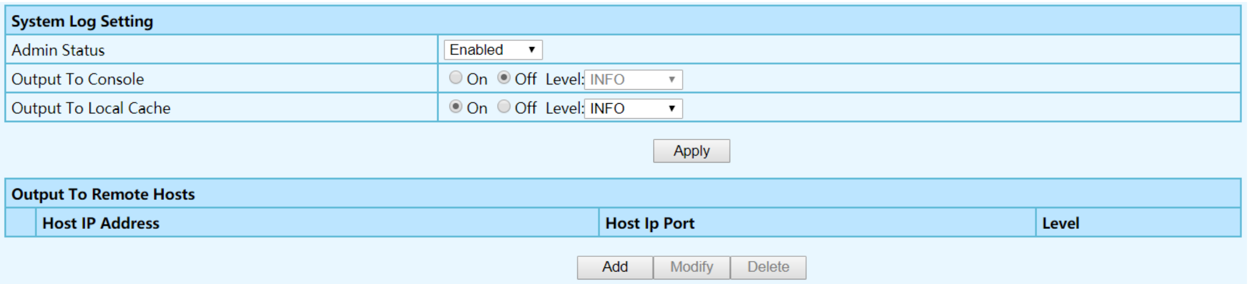
1. In the system log [Setting] interface, you can view the current system log configuration information, as shown in Figure 19.1.

2. To modify the system log configuration, set the corresponding configuration in the System Log Settings box and click [Apply] to complete the configuration, as shown in Figure 19.1.

3. To add a remote log server, click [Add], fill in the corresponding configuration items in the Remote Log Server Setting interface, and click [Apply] to complete the configuration. Maximum 4 remote servers can be added.

4. To modify the remote log server, first select the corresponding remote log server, and then click [Modify] to enter the remote log server setting interface. Modify the corresponding configuration item and click [Apply] to complete the configuration modification.

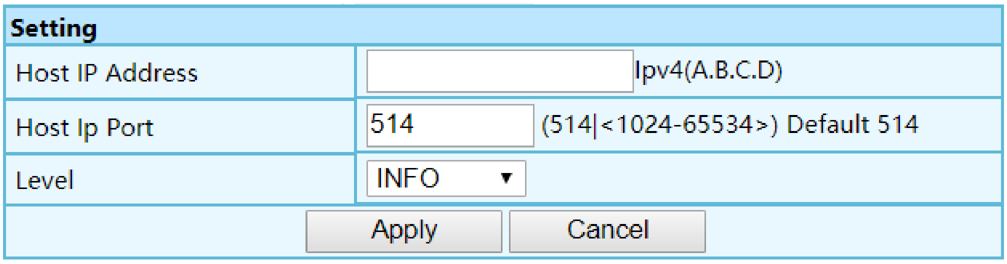
5. To delete a remote log server, first select the corresponding remote log server and click [Delete] to delete the remote log server.



System Log Setting	
Admin Status	Enabled ▾
Output To Console	○ On ● Off Level: INFO ▾
Output To Local Cache	● On ○ Off Level: INFO ▾

Output To Remote Hosts			
	Host IP Address	Host Ip Port	Level

Figure 19.1 System Log Setting



Setting	
Host IP Address	Ipv4(A.B.C.D)
Host Ip Port	514 (514|<1024-65534>) Default 514
Level	INFO ▾

Figure 19.2 Remote Log Server Setting

Configuration Description

Table 19.1 System Log [Setting] Configuration Description

Item	Description
Management Status	System log function status, including: ● Enable ● Prohibited Note: The default is Enable.
Output to Console	System log output to console status, including ● On ● Off Note: The default is Off
Output to Local Cache	System log output to the local cache status, including ●On ●Off Note: The default is on.
Output to Remote Host	System log output to remote log server
Level	System log level, divided into 8 levels according to severity ● EMERG: level 0, system cannot be used ● ALERT: Level 1, need to be processed immediately ● CRIT: Level 2, Severe State ● ERR: Level 3, Error Status ● WARNING: Level 4, Warning Status ● NOTICE: Level 5, normal but important state ● INFO: Level 6, Notification Event ● DEBUG: Level 7, debugging information Note: The default is INFO.

Table 19.2 Remote Log Server Configuration Description

Item	Description
Host IP address	Remote log host IP address, in dotted decimal format, valid host IP address, up to 4 groups
Host IP port	Remote log host port, range 514, 1024-65534, default is 514.
Level	System log level, divided into 8 levels according to severity ● EMERG: level 0, system cannot be used ● ALERT: Level 1, need to be processed immediately ● CRIT: Level 2, severe status ● ERR: Level 3, error Status ● WARNING: Level 4, warning status ● NOTICE: Level 5, normal but important status ● INFO: Level 6, notification event ● DEBUG: Level 7, debugging information Note: The default is INFO

Precautions

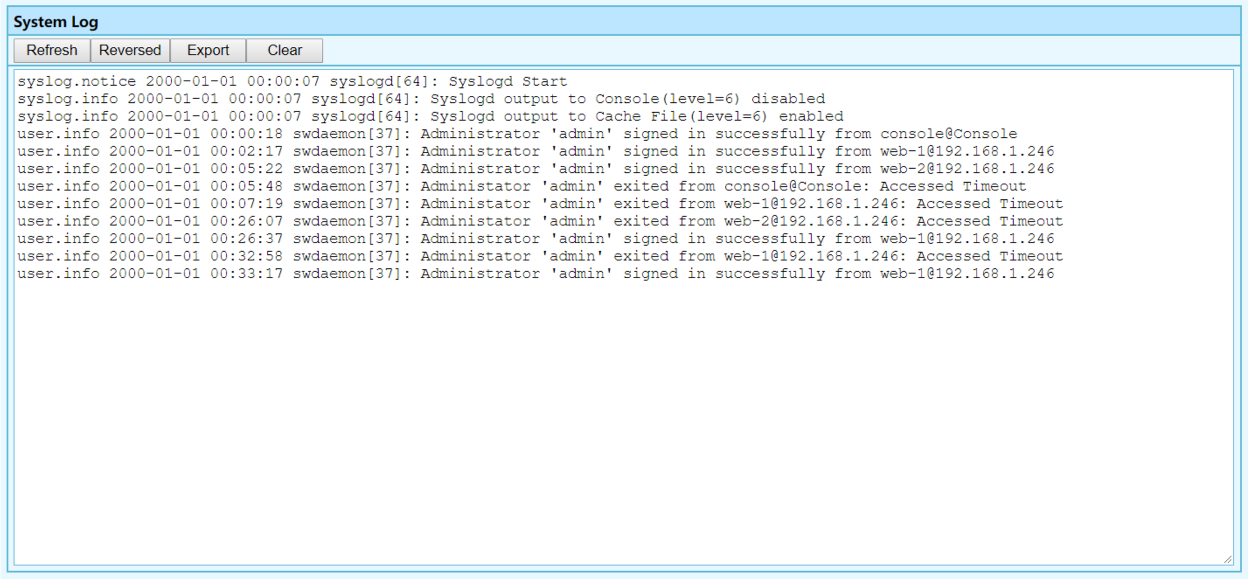
The smaller the log level value, the higher the level. Only logs with a level equal to or greater than the set level will be output. For example, if you set the logging level to the console to 5 (NOTICE), only logs with level 0 to 5 will be output to the console.

19.1.2 View

Configuration Steps

1. Select [System / System Log / View] in the navigation bar to enter the system log [View] interface.

2. In the system log [View] interface, you can view the contents of the system log, as shown in Figure 19.3.



```
syslog.notice 2000-01-01 00:00:07 syslogd[64]: Syslogd Start
syslog.info 2000-01-01 00:00:07 syslogd[64]: Syslogd output to Console(level=6) disabled
syslog.info 2000-01-01 00:00:07 syslogd[64]: Syslogd output to Cache File(level=6) enabled
user.info 2000-01-01 00:00:18 swdaemon[37]: Administrator 'admin' signed in successfully from console@Console
user.info 2000-01-01 00:02:17 swdaemon[37]: Administrator 'admin' signed in successfully from web-1@192.168.1.246
user.info 2000-01-01 00:05:22 swdaemon[37]: Administrator 'admin' signed in successfully from web-2@192.168.1.246
user.info 2000-01-01 00:05:48 swdaemon[37]: Administator 'admin' exited from console@Console: Accessed Timeout
user.info 2000-01-01 00:07:19 swdaemon[37]: Administator 'admin' exited from web-1@192.168.1.246: Accessed Timeout
user.info 2000-01-01 00:26:07 swdaemon[37]: Administator 'admin' exited from web-2@192.168.1.246: Accessed Timeout
user.info 2000-01-01 00:26:37 swdaemon[37]: Administrator 'admin' signed in successfully from web-1@192.168.1.246
user.info 2000-01-01 00:32:58 swdaemon[37]: Administator 'admin' exited from web-1@192.168.1.246: Accessed Timeout
user.info 2000-01-01 00:33:17 swdaemon[37]: Administrator 'admin' signed in successfully from web-1@192.168.1.246
```

Figure 19.3 System Log View

Configuration Description

Table 19.3 System Log [View] Configuration Description

Item	Description
Refresh	Refresh the system log content.
In proper Order	In order of time from old to new, the default is to display in proper order
Reverse Order	New to old display in chronological order.
Export	Export the contents of the system log
Clear	Clear the contents of the system log.

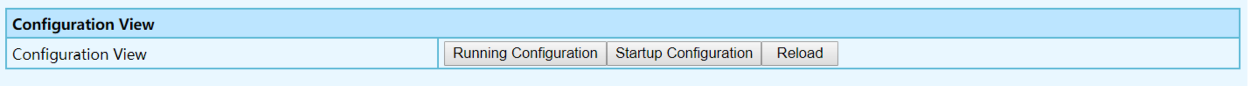
19.2 Configuration

19.2.1 View Configuration

Configuration Steps

1. Select [System / Configurations / View] in the navigation bar to enter the [View] interface.

2. In the [View] configuration interface, you can view the running configuration and startup configuration.



Configuration Descriptions

Table 19.4 Configurations [View] Configuration Description

Item	Description
Run Configuration	View system running configuration file, text style
Enable Configuration	Check the system enable configuration file, text style.
Reload	Reload the running or startup configuration file.

19.2.2 Import Configuration

Configuration Steps

1. Select [System / Configurations / Import] in the navigation bar to enter the [Import] interface of Configurations, as shown in Figure 19.4.

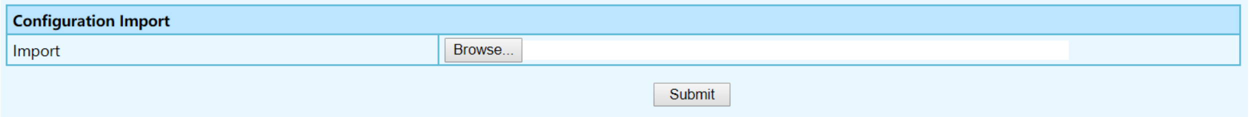


Figure 19.4 Configurations Import

2. In the Configurations [Import] interface, click [Browse], select the configuration file to import, and click [Submit] to start the import.

19.2.3 Export Configuration

Configuration steps

1. Select [System / Configurations / Export] in the navigation bar to enter the Configurations [Export] interface, as shown in Figure 19.5.

2. Export configuration is divided into startup configuration and running configuration. Click [Export] in the corresponding project to prompt up the "File Save" dialog box (different browsers may differ, here take the IE11 browser as an example), click [Save] to export the corresponding configuration file to the local.

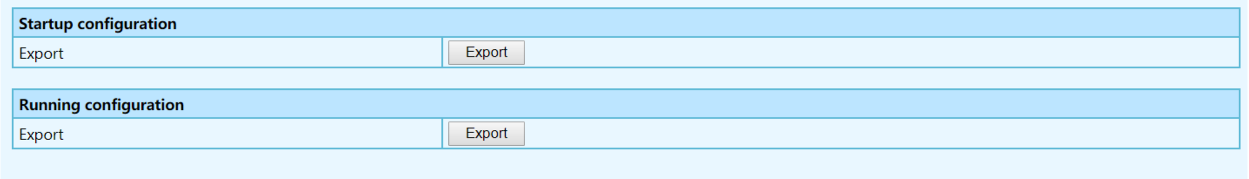
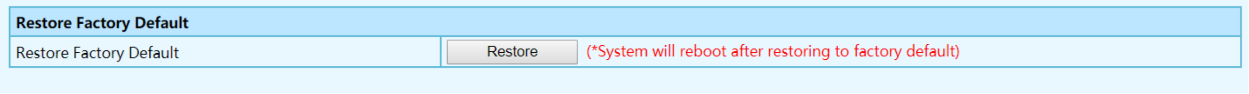


Figure 19.5 Export Configuration

19.2.4 Restore Factory Configuration

Configuration Steps

1. Select [System / Configurations / Restore Factory Default] in the navigation bar to enter the [Restore Factory Default] interface, as shown in Figure 19.6.



Restore Factory Default	
Restore Factory Default	Restore (*System will reboot after restoring to factory default)

Figure 19.6 Restore Factory Setting

2. Click [Restore] and then click [OK] in the confirmation dialog box to restore the factory configuration. Click [Cancel] to cancel the factory configuration restoration. After a successful factory reset, the system automatically restarts to take effect to the factory configuration.

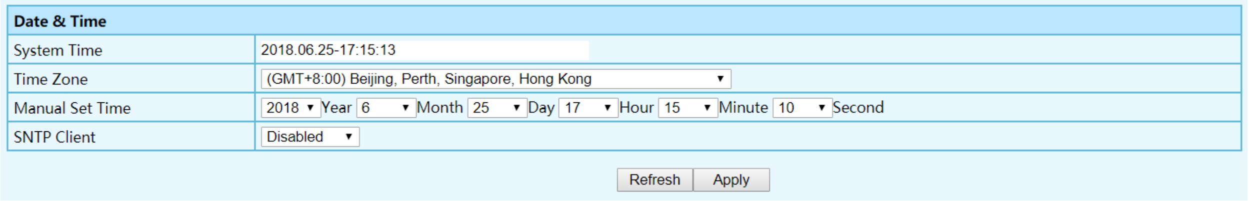
19.3 Date and Time

Configuration Steps

1. Select [System / Date and Time] in the navigation bar to enter the system setting [Date and Time] interface. The system time can be manually set, or automatically synchronized through the SNTP client.

2. The [Date and Time] interface allows you to view system time and related date and time configuration information.

3. To set the system time manually, the SNTP client must be disabled. Select the corresponding time zone in the [Time Zone] column and set the system time in the [Time Setting] column. Click [Apply] to complete the system time setting, as shown in Figure 19.8.

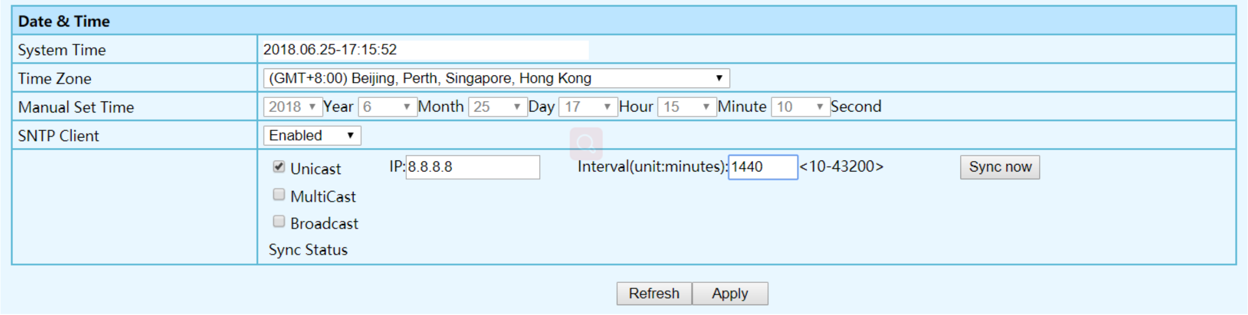


Date & Time	
System Time	2018.06.25-17:15:13
Time Zone	(GMT+8:00) Beijing, Perth, Singapore, Hong Kong
Manual Set Time	2018 Year 6 Month 25 Day 17 Hour 15 Minute 10 Second
SNTP Client	Disabled

Figure 19.8 System Time Setting by Manual

3. Synchronize system time automatically via SNTP client. The SNTP client must be enabled before the SNTP client can be set. The SNTP client time synchronization mode is divided into

unicast, multicast, and broadcast. These three modes can be selected, but at least one mode must be selected. When the unicast mode is selected, the IP address of the time server (8.8.8.8 by default) and the synchronization interval (1440 minutes by default) must also be set. [Sync Now] button means SNTP client requests time synchronization immediately, otherwise it will be synchronized once at the set synchronization interval. Click [Apply] to complete the SNTP client time synchronization setting, as shown in Figure 19.9.



Date & Time	
System Time	2018.06.25-17:15:52
Time Zone	(GMT+8:00) Beijing, Perth, Singapore, Hong Kong
Manual Set Time	2018 Year 6 Month 25 Day 17 Hour 15 Minute 10 Second
SNTP Client	Enabled
	☑ Unicast IP:8.8.8.8 Interval(unit:minutes):1440 <10-43200> □ MultiCast □ Broadcast Sync Status

Figure 19.9 SNTP client setting interface

Configuration Description

Table 19.5 [Date and Time] Configuration Description

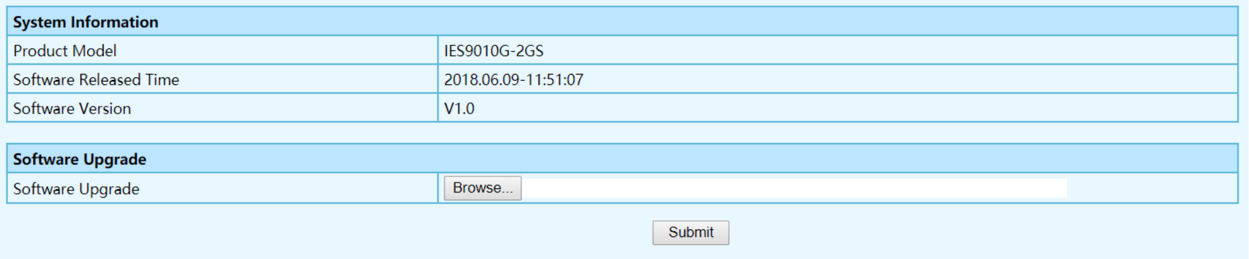
Item	Description
System Time	Displays the actual effective system time.
Time Zone	System time zone setting, select any time zone from the drop-down list.
Time Setting	It can be set after the SNTP client is disabled. The year range is 1970-2037. Others are the same as the common settings.
SNTP Client	The SNTP client two status: ●Enabled: Enable the SNTP client ●Prohibit: Disable SNTP Client Note: The default is Prohibit
Synchronous Mode	The SNTP client synchronization mode is divided into: ●Unicast mode: default IP address 8.8.8.8; interval range 10-43200, and default value 1440. ●Multicast mode ●Broadcast mode These three modes are multi-selectable, but at least one must be selected

IP	IP address of SNTP server, only for unicast mode
Interval	SNTP client time synchronization interval, only for unicast mode
Synchronize	SNTP client immediate synchronizes time, only for unicast mode

19.4 Software Upgrade

Configuration Steps

1. Select [System / Software Upgrade] in the navigation bar to enter the [Software Upgrade] interface, as shown in Figure 19.10.



System Information	
Product Model	IES9010G-2GS
Software Released Time	2018.06.09-11:51:07
Software Version	V1.0

Software Upgrade	
Software Upgrade	Browse...

Figure 19.10 Software Upgrade

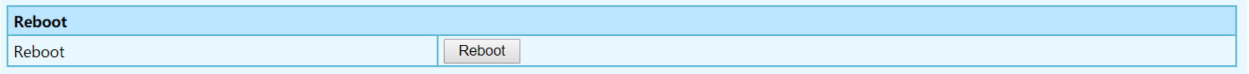
2. On the [Software Upgrade] interface, click [Browse] to select the upgrade file to be imported. (The upgrade files are generally having extension .ub and .urk. Marked with "b" for BOOT files and "r" for "File System". The file is marked with k for the file with the kernel. Click [Submit]. The system starts uploading the upgrade file. After the upload is complete, the device automatically restarts to update the software after the upgrade is complete.

Note: During the software upgrade, make sure that the device is powered up until the upgrade is completed.

19.5 Software Restart

Configuration Steps

1. Select [System / Reboot] in the navigation bar to enter the [Reboot] interface, as shown in Figure 19.11.

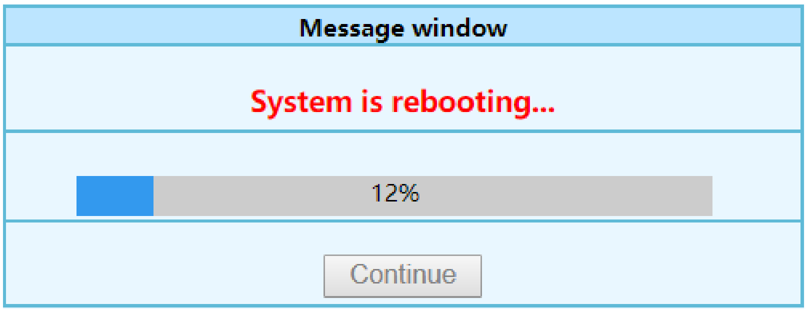


Reboot	
Reboot	Reboot

Figure 19.11 Restart

2. Click [Reboot] and the ‘Confirm Restart’ dialog box will pop up. Click OK to restart the device.

A restart progress bar is displayed. Click [Cancel] to cancel the restart of the device. Restart progress is shown in Figure 19.13.



Message window

System is rebooting...

Figure 19.13 Restart Progress