USER MANUAL

rev. 2.0.0124

Managed Network Switches

MODELS:

CROSS 8/HPoE (II)
CROSS 16/HPoE (II)
CROSS 24/HPoE Plus (II)
CROSS 48/HPoE 10G Plus
CROSS 8/UPoE SP
CROSS 8/HPoE SP
CROSS 4/HPoE SP

DEFAULT PARAMETERS:

IP-ADDRESS: **192.168.1.1** USER NAME: **admin** PASSWORD: **admin**

EVIDENCE®

Content

Chapter 1 Configuration preparation

This chapter describes the configuration preparation in detail, mainly including the following contents:

l Web login interface

l Web configuration interface

l Current setting information

1.1 WEBLogin interface

The default IP address of the system is 192.168.1.1.Before logging in, please ensure the following:

l The IP address of the management PC and the IP address of the switch are in the same network segment, otherwise the switch management IP address cannot be accessed

l Make sure that the port connecting the PC and the switch is a non aggregate port

l The web browser is IE8 or above

Login steps

1. open the browser on the PC.

2Enter the device IP address in the address bar (192.168.1.1 by default), press enter to enter the web login interface,

As shown below:

2. Enter the user name and password in the web login interface.

3. Select the language in the web login interface.

4. Click < logn > to enter the web configuration interface.

Configuration item	explain
user name	Enter the user name to log in. The default user name is admin
password	Enter the login password of the user who needs to log in. The default password is admin
language	Interface language display mode: ı Chinese: Select Chinese display mode; ı English: select the English display mode. Note: at present, only Chinese and English are supported

1.2 WEB Interface

1.2.1 Equipment panel

Through the device panel diagram, you can view the activation and connection status of each interface of the device, as shown in the following figure:

See the following table for the interface description on the equipment panel diagram:

Interface	explain
	Green copper interface, enabled and connected.
	Gray copper interface, enabled and not connected.

1.2.2 Common button

See the following table for the description of common buttons in the equipment configuration interface,

Button	explain
Save	Save button to save the configuration.
Logout	Logout button to exit to the login page.
Reboot	Press the restart button to restart the switch system.

Debug	The debug button enables you to view the switch log.
Edit	Edit button to modify an item selected in the current page.
Add	Add button to add an item in the current page.
Delete	Delete button to delete an item selected in the current page.
Refresh	The refresh button can display the data update of the current page.
Apply	Apply button to apply the current configuration to the system.
Bind	Bind button, which can bind a set rule to the selected item on the current page.
Unbind	Unbound button, which can unbind.

1.2.3 Save configuration

1Click after the current configuration is completed Save , the configuration is applied to the system.If not Save , the configuration after the last save operation will be lost after the device is powered down or restarted.

2. when all current configurations are complete, click Save 。The configuration saved in the configuration file will not be lost after the device is powered down or restarted.

1.2.4 Exit the web configuration interface

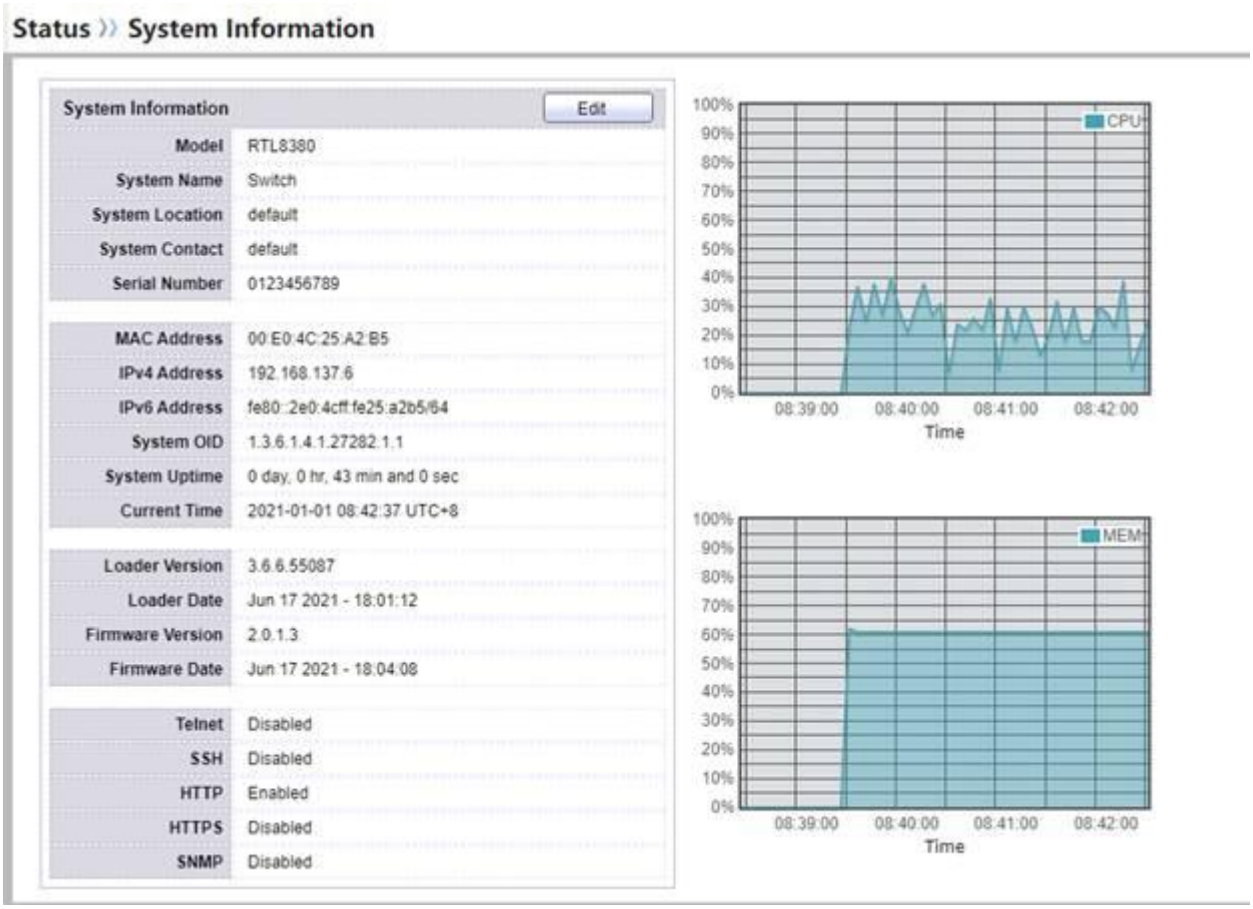
1. After completing the configuration in the web interface, please press Save To avoid configuration loss.Then click Logout You can exit the web configuration interface.
2. Closing the browser directly cannot exit the web configuration interface.If the user does not time out during the next login, he will directly enter the web configuration interface.

1.3 Current device information

Configuration steps

1. Select the first page in the navigation bar to enter the [status] interface. The basic information of the current equipment and the operation status information of the

equipment system are displayed in the [system information] interface, as shown in Figure 1.4.



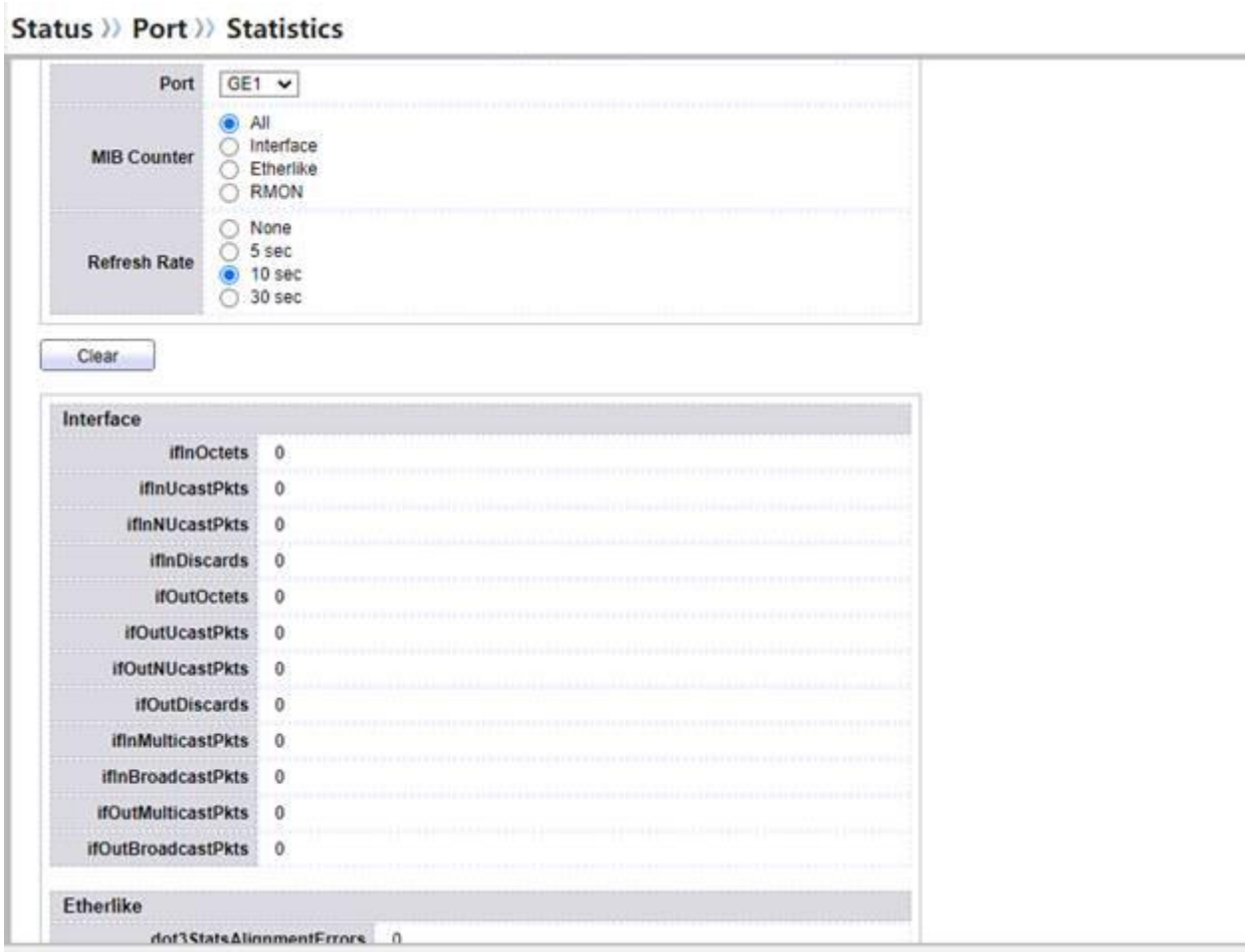
Configuration item description

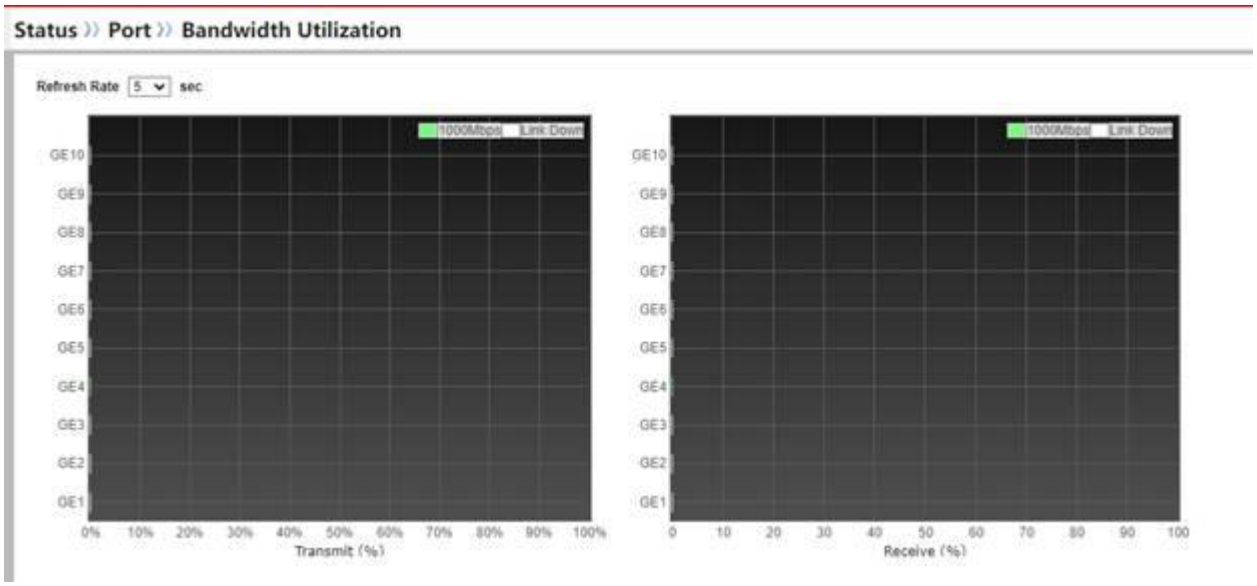
Configuration item	explain
Model	Current equipment model, such as rtl8380.
MAC Address	Current device MAC address.
Serial Number	The product serial number of the current device.
IPv4 Address	IPv4 address of the current device.
IPv6 Address	IPv6 address of the current device.
System OID	Oid of the current equipment system.
System Uptime	The running time of the current equipment system.
Current Time	Current device system time.
Loader Version	The loader version of the current device system.
Loader Date	The loader date of the current device system.
Firmware version	The firmware version of the current device system.

Firmware Date	Firmware date of the current device system.
CPU	Display CPU usage
MEM	display memory

1.3.1 Port information display

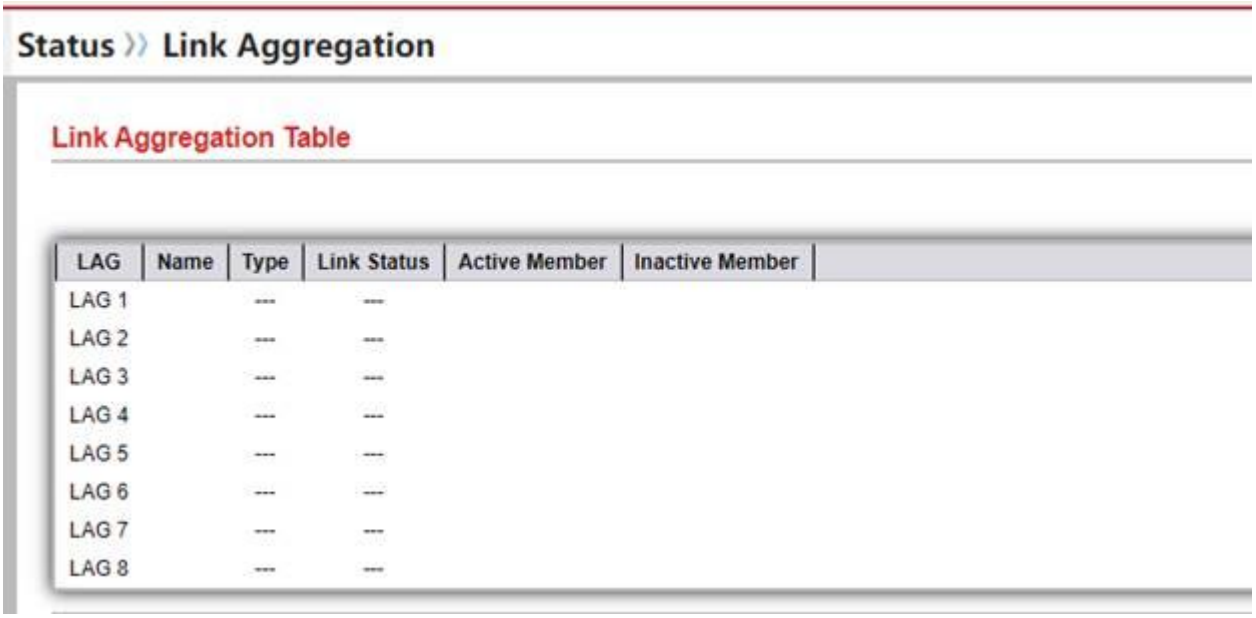
1Select the first page in the navigation bar to enter the [status] interface, and the port statistics and bandwidth utilization are displayed in the [port] interface, as shown in the following figure:





1.3.2 Link aggregation group display

1. select the first page in the navigation bar to enter the [status] interface, and the link aggregation group is displayed in the [link aggregation] interface, as shown in the following figure:



1.3.3 MAC address table display

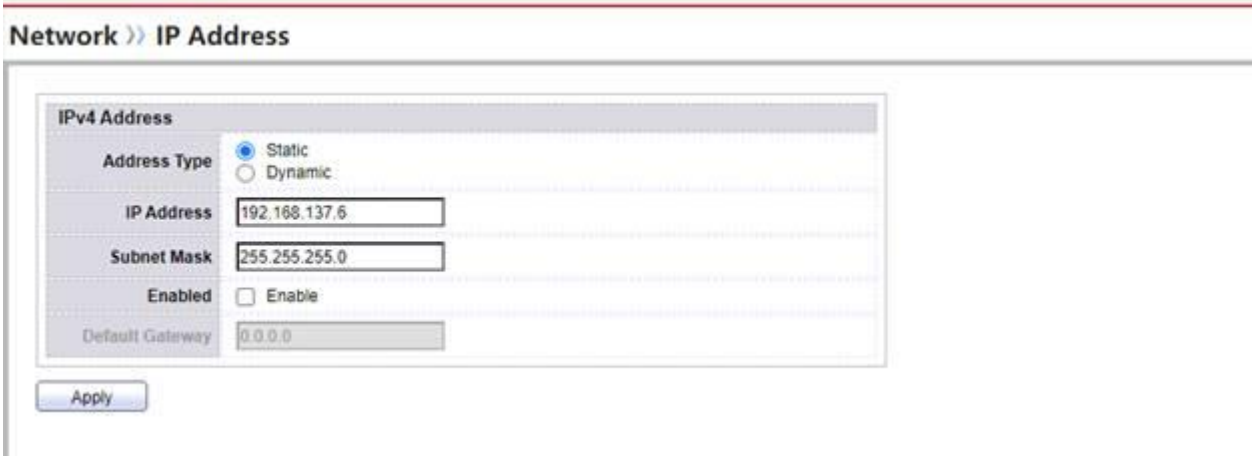
1. select the first page in the navigation bar to enter the [status] interface, and the link aggregation group is displayed in the [link aggregation] interface, as shown in the following figure:

Chapter 2 Network

2.1 IPAddress setting

Configuration steps

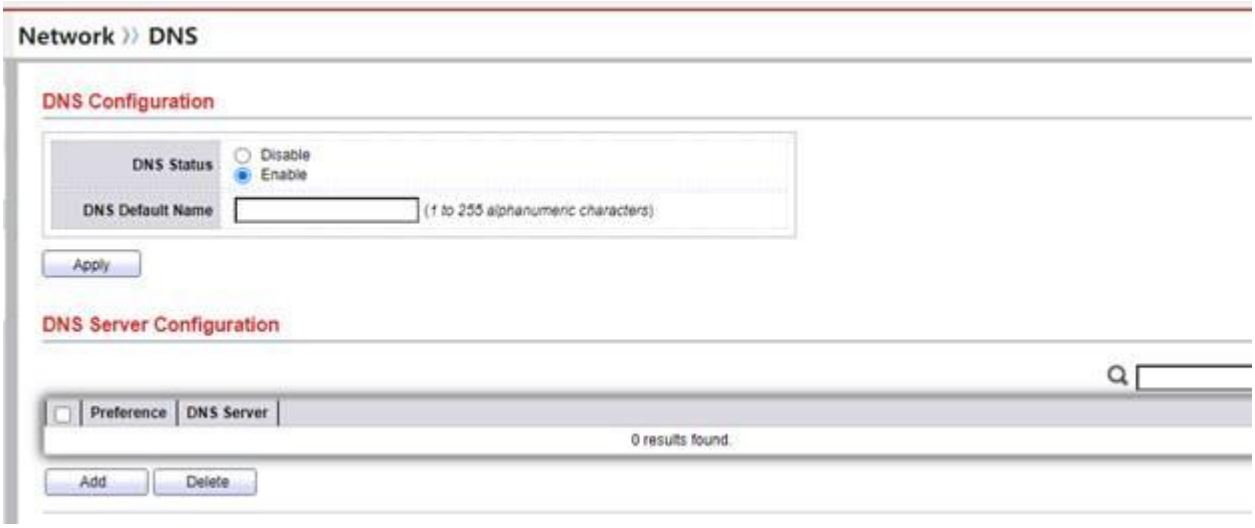
1. Select [IP address / network] in the navigation bar to enter the IP address setting interface, which supports modifying the IP address of the switch and setting the gateway, as shown in the following figure:



2.2 DNSset up

Configuration steps

1.Select [DNS / network] in the navigation bar to enter the IP address setting interface, which supports DNS settings and DNS server settings, as shown in the following figure:



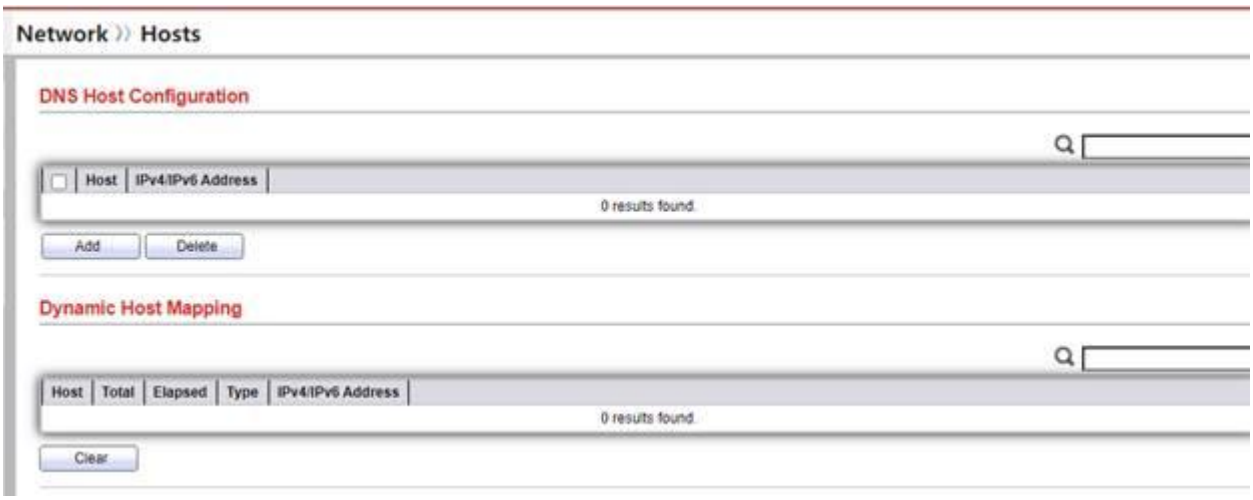
To add a DNS server, click Add Button to enter the page of adding DNS server, as shown in the following figure:

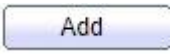
After the configuration is set, you need to click the Apply button in the figure to change and save.

2.3 DNSHost settings

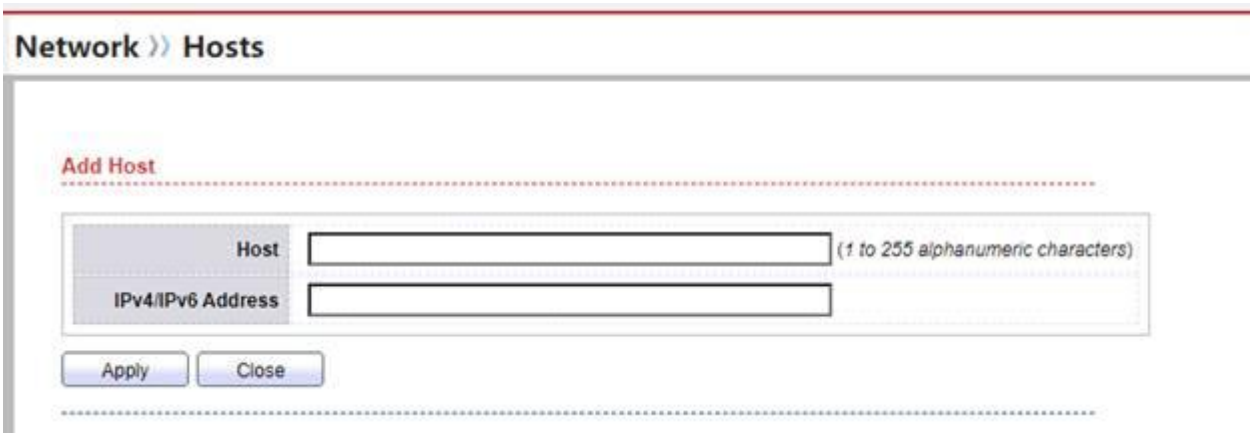
Configuration steps

1. Select [hosts / network] in the navigation bar to enter the DNS host setting interface, which supports DNS host setting, as shown in the following figure:



To add a DNS host, click 

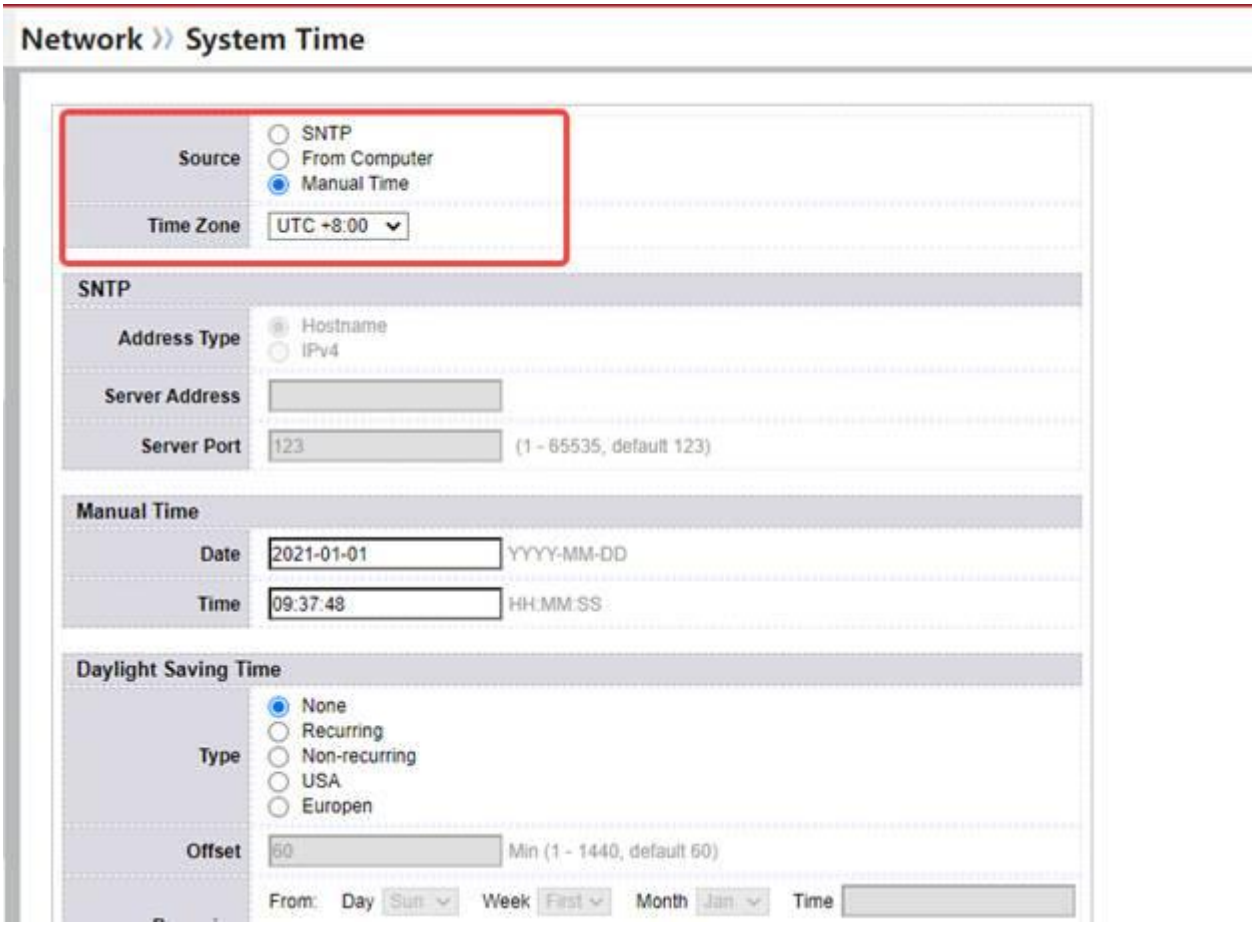
Button to enter the add DNS host page, as shown in the following figure:



2.4 system time

Configuration steps

1.Select [system time / network] in the navigation bar to enter the system time setting interface, as shown in the following figure:



As shown in the figure above, this interface supports three ways to set the system time: SNTP, follow the computer time and manually set the time.

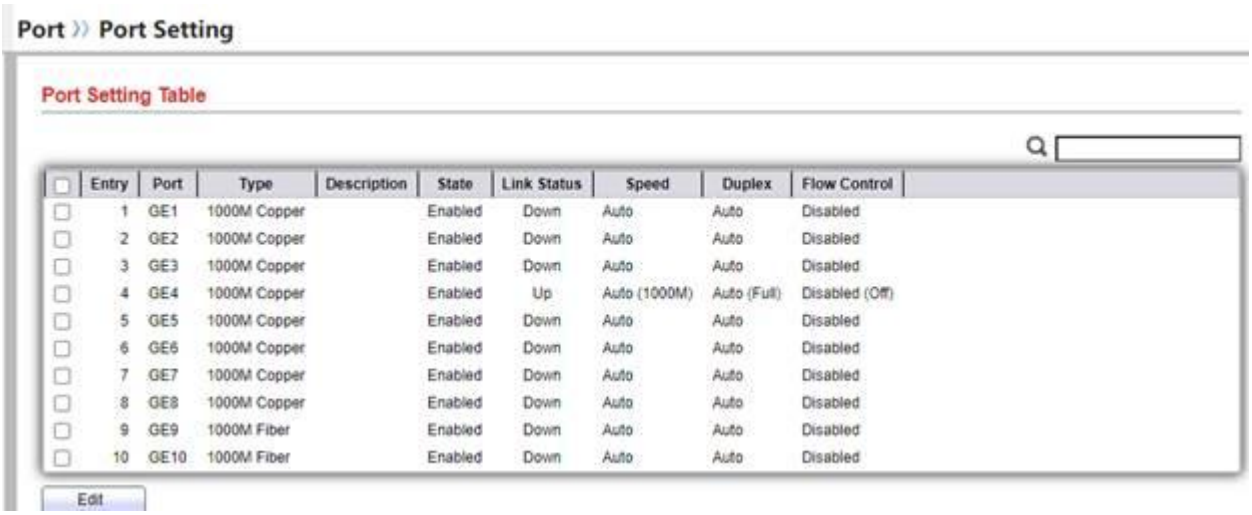
Chapter 3 Port

3.1 port configuration

Configuration steps

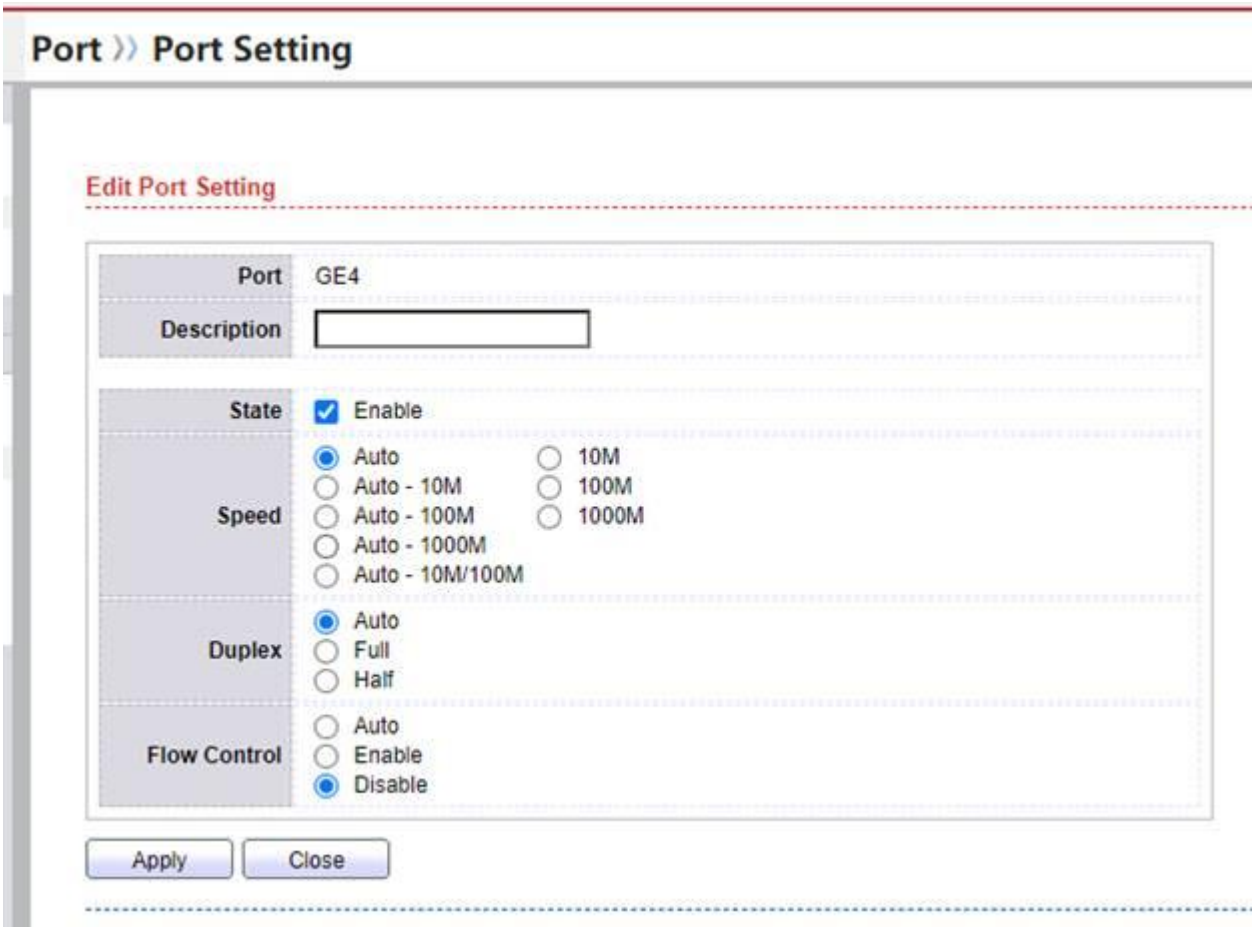
1. select [port] on the navigation bar to enter the [port setting] interface.

2The [port setting] interface displays the operation status and configuration information of each port.



value	describe
Port	Name and serial number of the port
Type	Type of current port, copper or fiber
State	The status of the port. The default is enable
Link Status	Up indicates that the port is currently connected Down indicates that the port is currently disconnected or not connected
Speed	The current working rate of the port. Unconnected ports are always displayed as auto
Duplex	The duplex mode in which the port is currently working, and the unconnected port always displays auto
Flow Control	Flow control function of air control port

3If you need to modify the configuration of a port, just click the [] button on the right side of the corresponding entry in the interface, enter the modification interface (as shown in Figure 2.2), and modify the corresponding configuration item.Click the [apply] button to finish the modification, and click the [Cancel] button to cancel the modification.



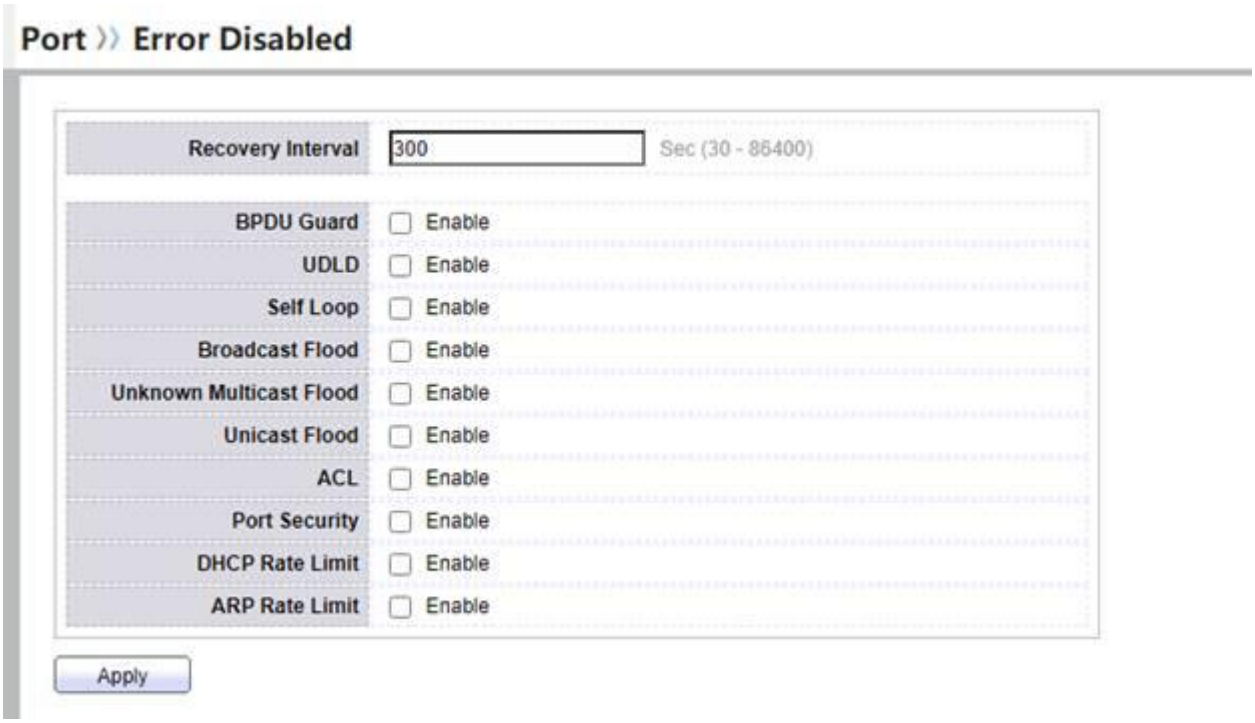
value	range	describe
state	disable， enable Default value: Enable	Close / open the port.In the off state, the connection / disconnection state is link down;When it is on, the connection status is link up.
speed	10M 100M 1000M Auto Default: Auto	The port speed can be configured, such as 10m / 100M / 1000m / automatic bandwidth.
Duplex	Full Half Auto Default: Auto	The working mode of the port can be configured, such as: In half duplex mode, only one direction of communication is allowed, and in full duplex mode, two

		directions of communication can be carried out at the same time.
Flow Control	disable enable Default value: Enable	The second layer port flow control function can effectively prevent network congestion after it is turned on.Flow control is a point-to-point function, which is realized by means of push frame. When the pvrp system port is opened, the opposite port must also be opened.

3.2 Port function configuration

3.2.1 Port exception protection configuration

Select the first page in the navigation bar to enter the [port] interface, and the [error disable] interface displays the port exception protection function, which can prevent the port from being abnormal or before it is abnormal.As shown below:



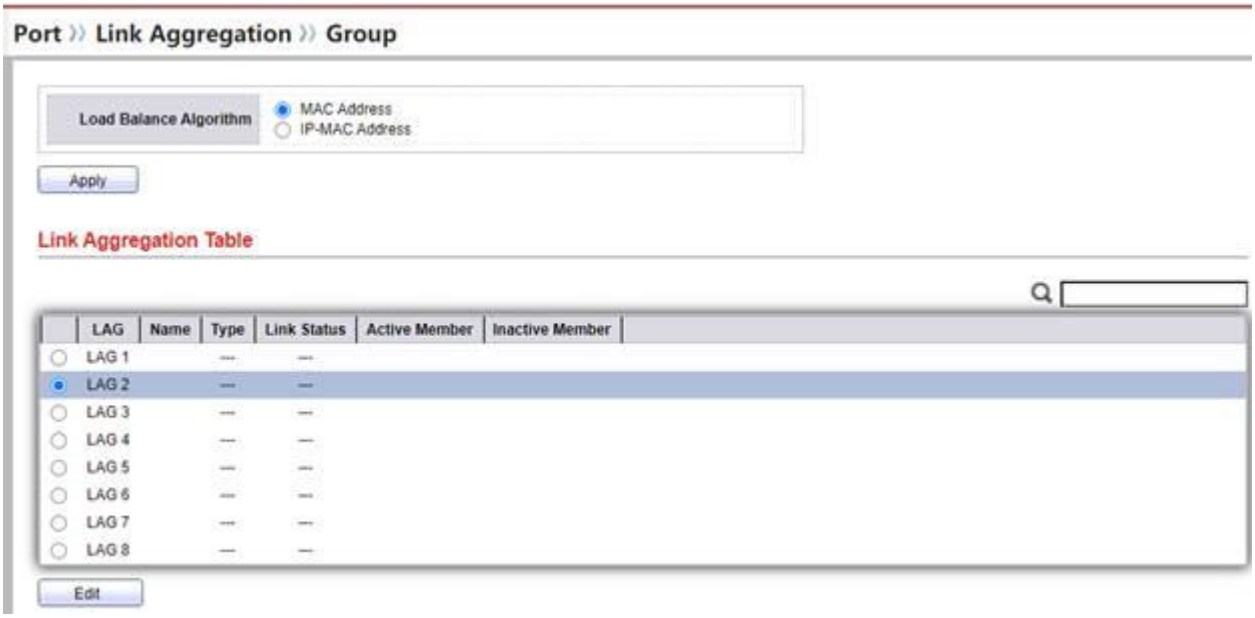
Select the desired function and click  That's it.

3.2.2 Link aggregation configuration

Select the first page in the navigation bar to enter the [port] interface. The configuration and use of link aggregation function are displayed in the [link aggregation] interface,

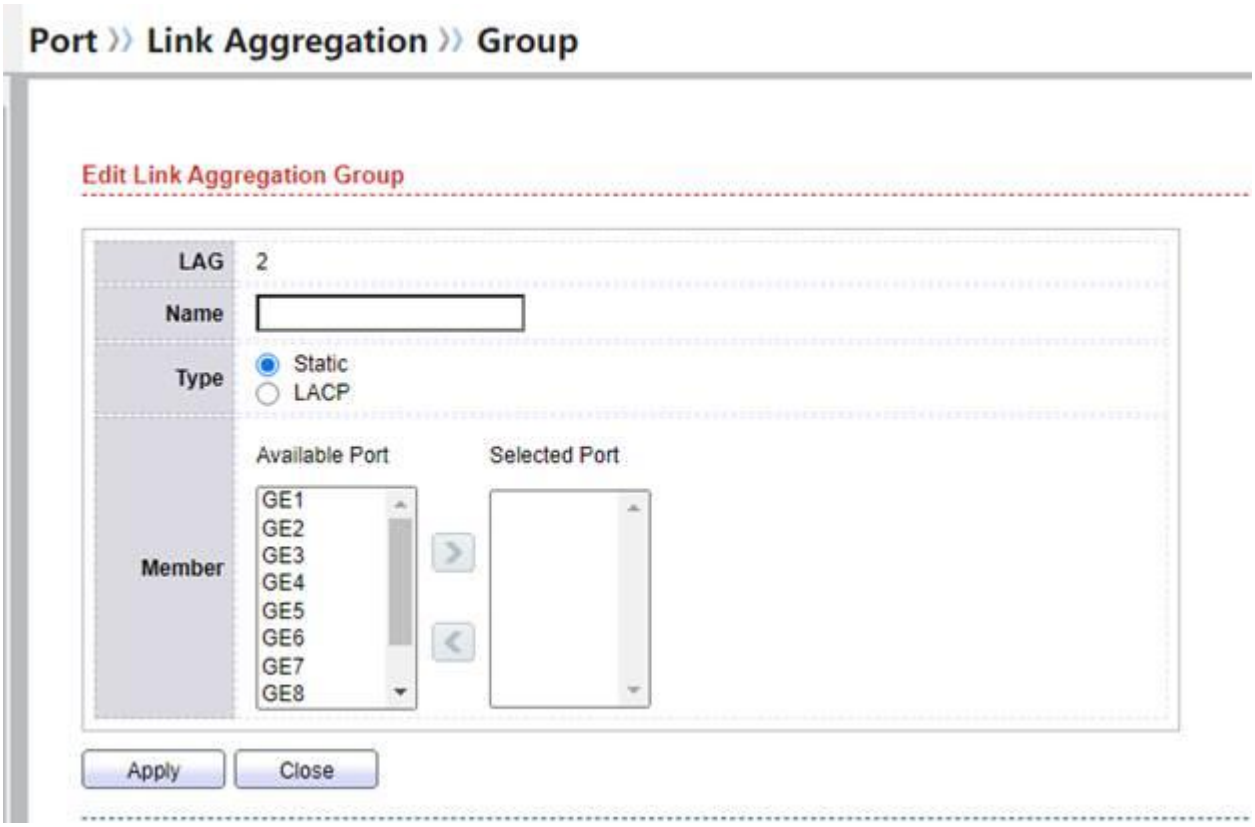
The first step is to configure link aggregation

Closing port, as shown in the figure below:



There are two options for the implementation of link aggregation, one is the implementation of MAC address, and the other is the implementation of IP-MAC address.

In the figure above, select a lag and click Edit , enter the port selection page.

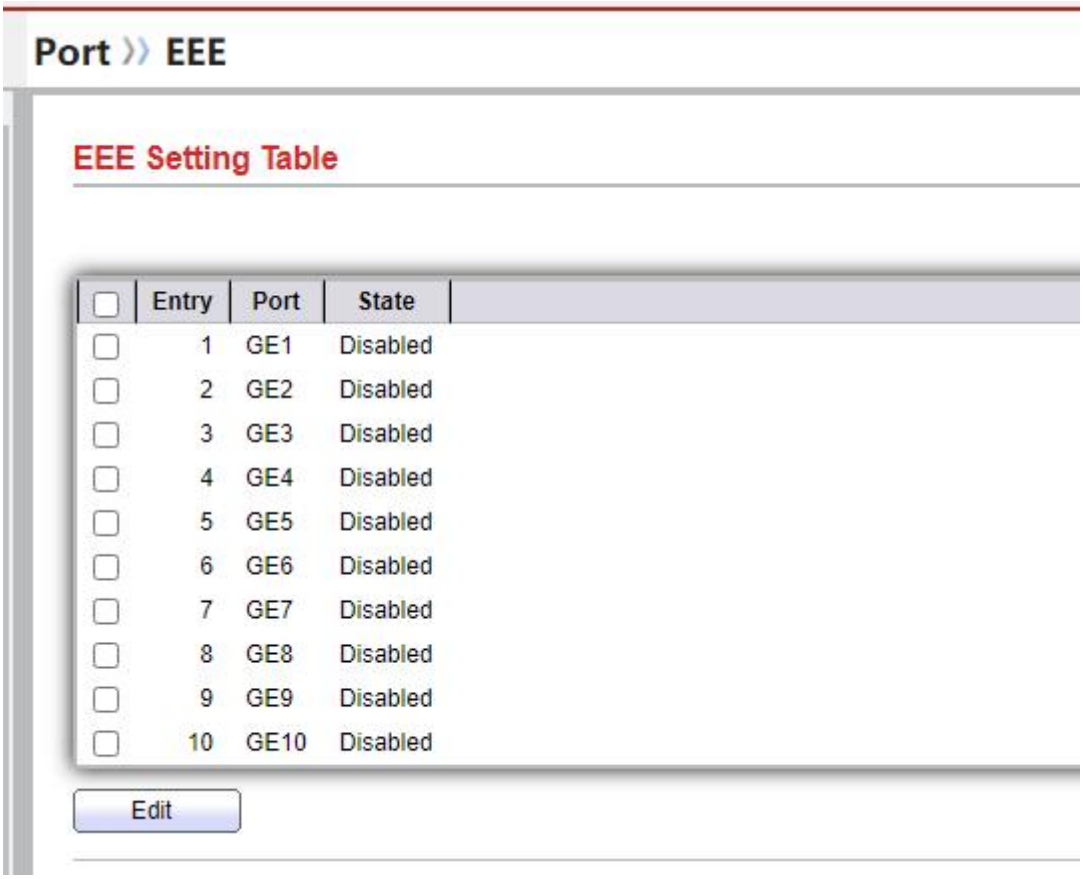


Name	This option allows you to rename the aggregation group
Type	There are two options for this option: one is static and the other is LACP. Both are for port aggregation, but one is static and the other is dynamic

Member	This option is to select the port to become a member of the aggregation group

3.2.3 EEE configuration

Select the first page in the navigation bar to enter the [port] interface. The EEE configuration is displayed in the [EEE] interface, as shown in the following figure:



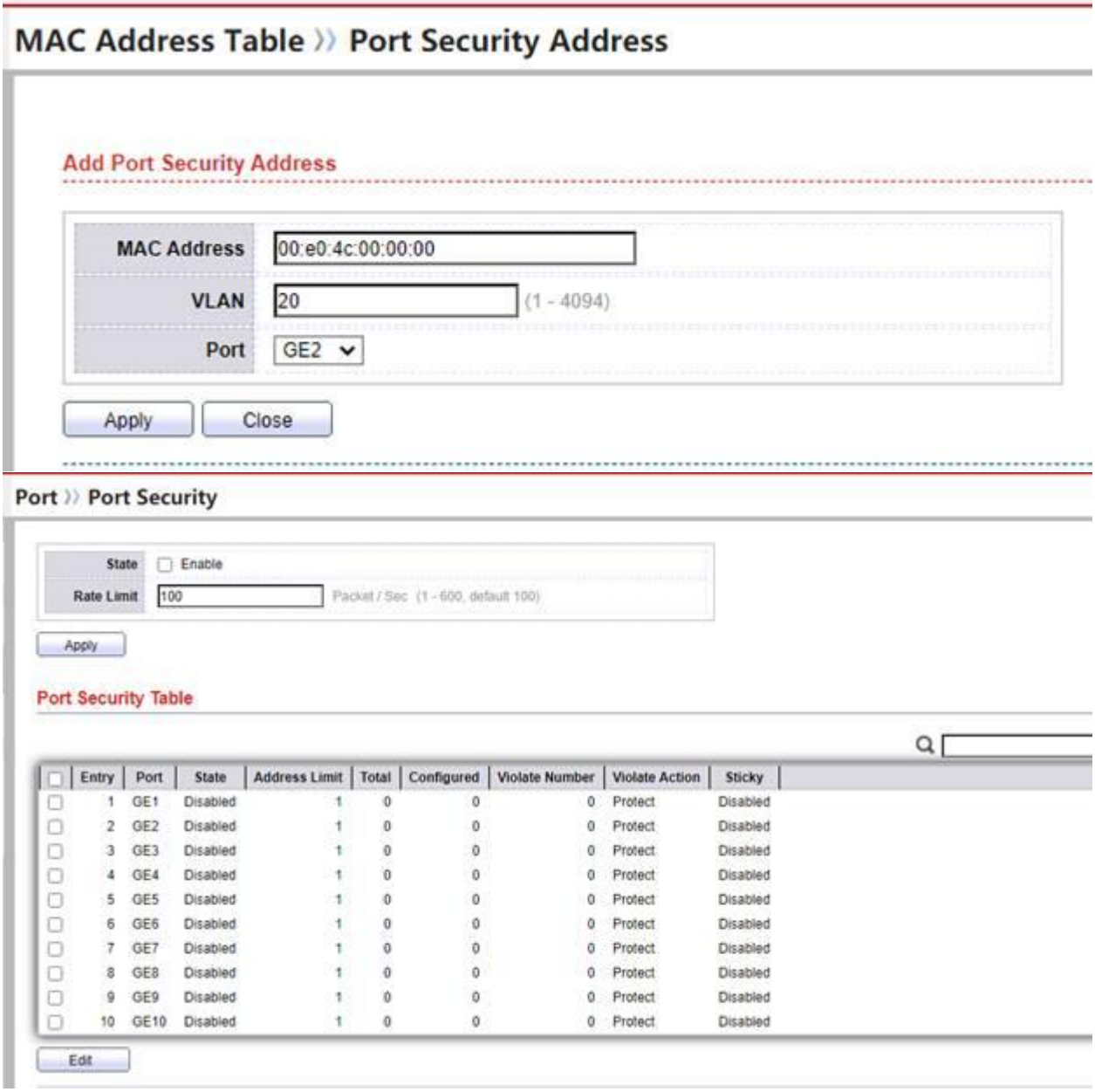
3.2.4 Mega frame configuration

Select the first page in the navigation bar to enter the [port] interface, and the jumbo frame configuration is displayed in the [jumbo frame] interface, as shown in the following figure:

3.2.5 Port security configuration

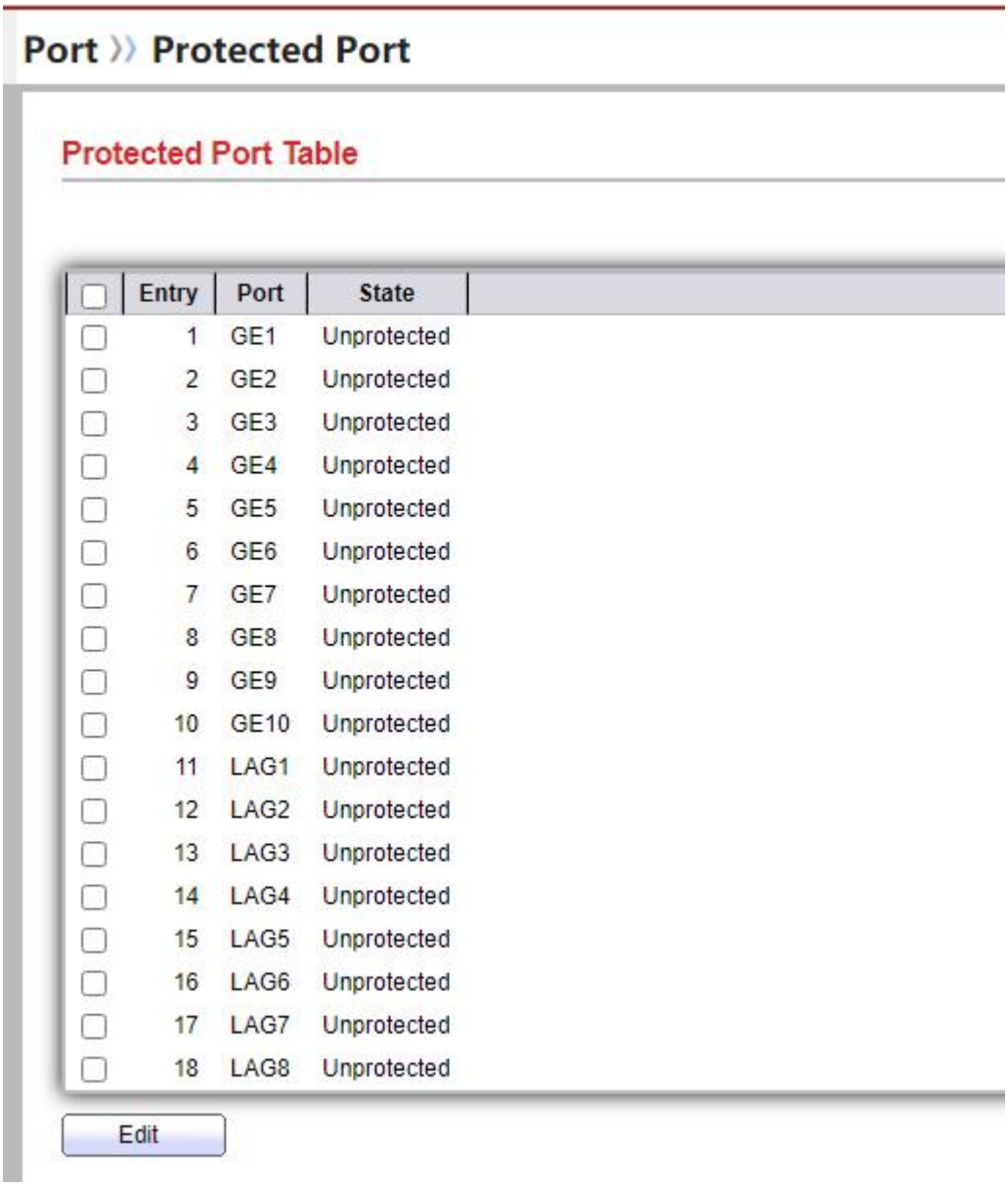
Select the first page in the navigation bar to enter the [port] interface, and the port security function is displayed in the [port security] interface,

This function needs to be used in conjunction with the port security MAC address table, as shown in the following figure:



3.2.6 Port isolation configuration

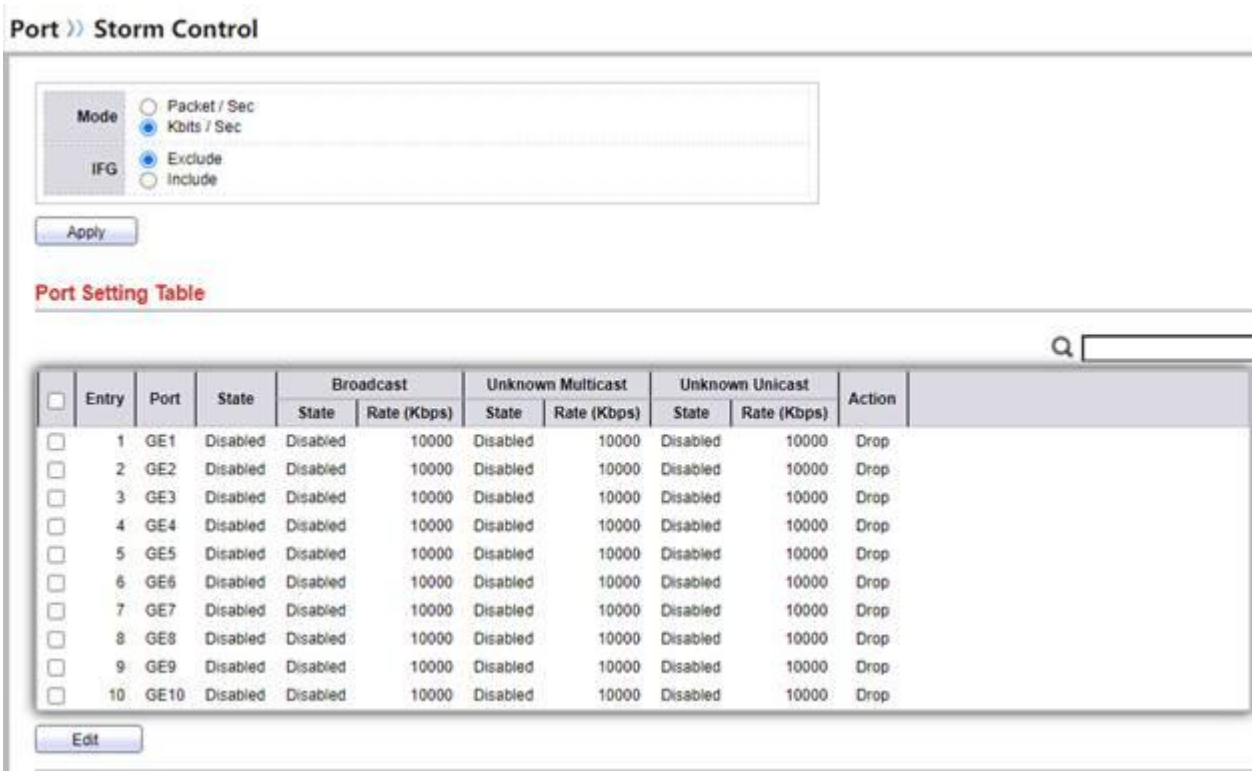
Select the first page in the navigation bar to enter the [port] interface. The port isolation function is displayed in the [protected port] interface. This function is reflected in that the two ports isolated from each other cannot communicate.As shown below:



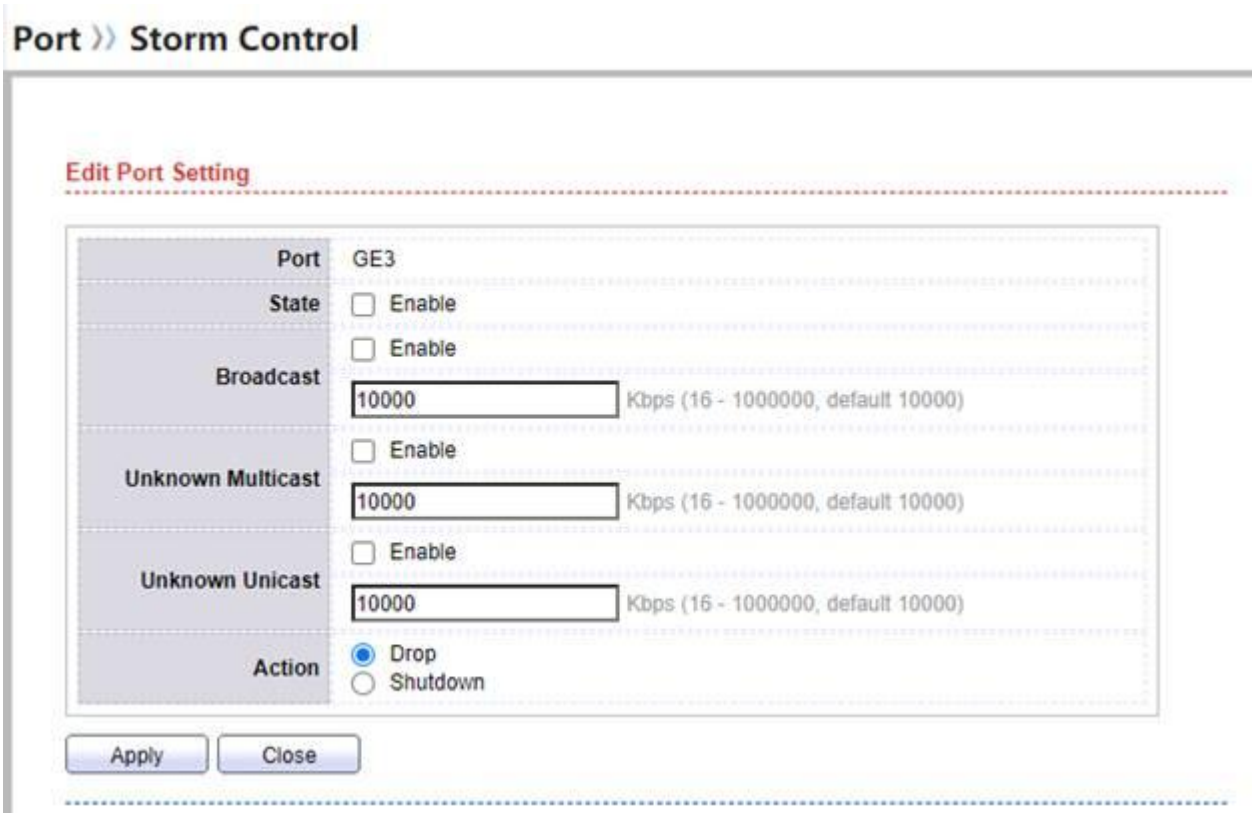
3.2.7 Storm control configuration

Select the first page in the navigation bar to enter the [port] interface, and the storm control function is displayed in the [storm control] interface,

As shown below:



Select a port and click Edit, enter the configuration page, as shown below:

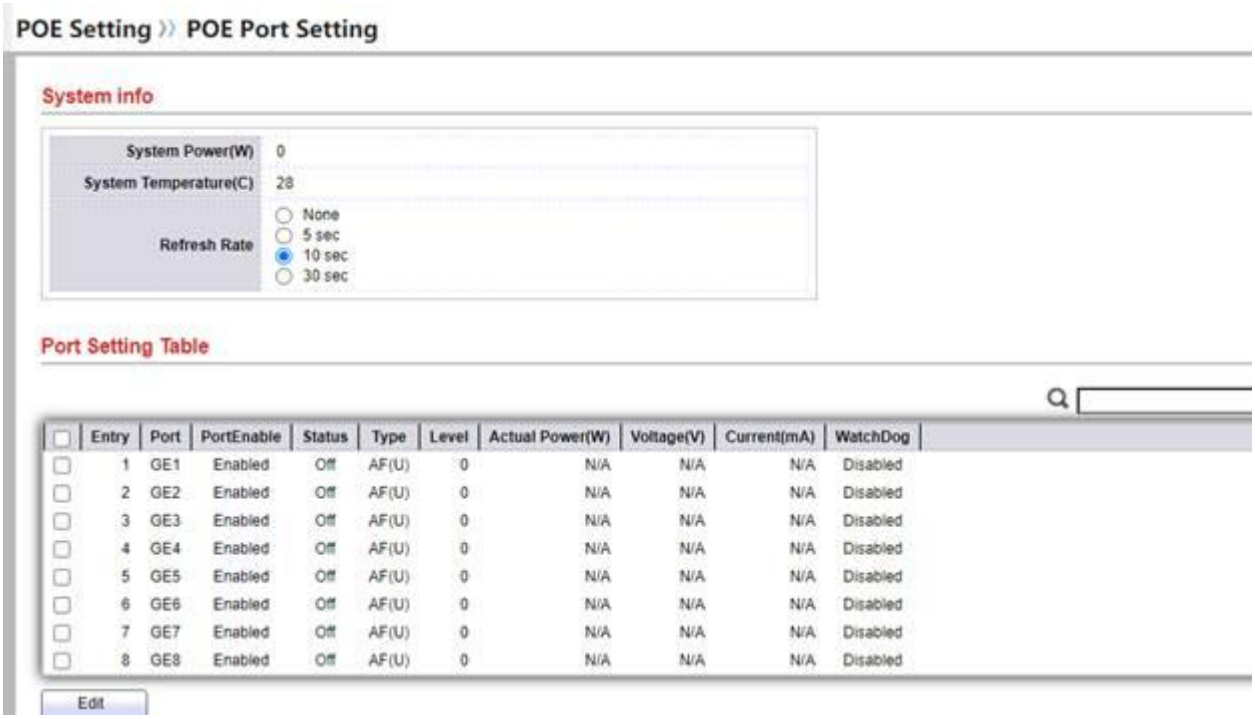


Chapter 4 POE

4.1 Poe port settings

Configuration steps

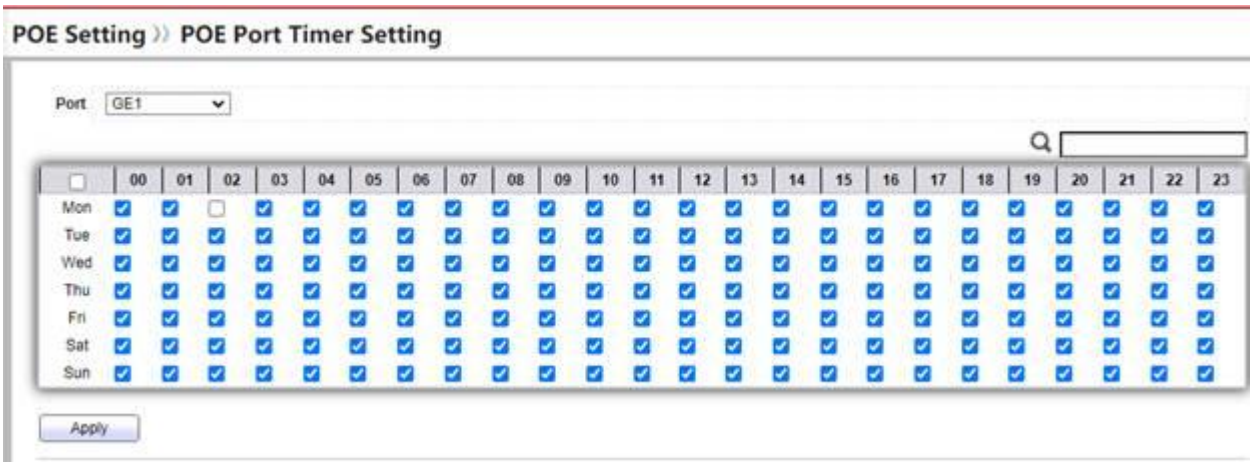
1. Select [Poe setting] in the navigation bar to enter the [Poe port setting] interface, as shown below:



4.2 Poe port timing setting

Configuration steps

1. Select [Poe setting] in the navigation bar to enter the [Poe port time setting] interface, as shown below:



In the figure above, ☑ Indicates Poe work, ☐ Indicates that it does not work.The number above represents the point in time.The left side indicates the day of the week.

Chapter 5 VLAN

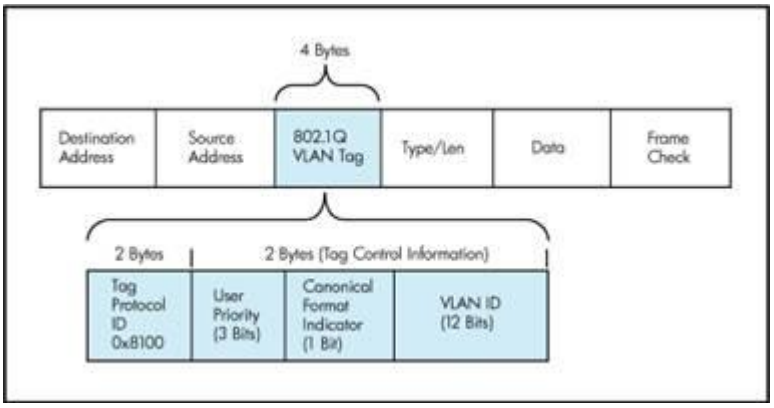
5.1 VLAN overview

The Chinese name of VLAN (virtual local area network) is "virtual local area network".VLAN is a data exchange technology that logically divides LAN devices into networks, so as to separate a large physical network into multiple virtual working groups.These devices and users are not limited by physical location, and can be set as a group according to factors such as function, department and application, so that the communication between them is like in the same physical segment.

The emergence of VLAN technology makes the administrator logically divide different users in the same physical LAN into different broadcast domains according to the actual application requirements. Each VLAN contains a group of computer workstations with the same requirements, which has the same attributes as the physically formed LAN.Because it is logically divided rather than physically divided, each workstation in the same VLAN is not limited to the same physical range, that is, these workstations can be in different physical LANs.According to the characteristics of VLAN, the broadcast and unicast traffic inside a VLAN will not be forwarded to other VLANs, which helps to control

traffic, reduce broadcast domain, simplify network management and improve network reliability.

VLAN packet format:



5.2 VLAN advantage

VLAN is a protocol proposed to solve the broadcasting problem and security of Ethernet. Its advantages are as follows:

● broadcast storm prevention

Limiting the broadcast on the network and dividing the network into multiple VLANs can reduce the number of devices participating in the broadcast storm.VLAN segmentation can prevent broadcast storm from spreading to the whole network.

● safety

Enhance the security of LAN, and the user group containing sensitive data can be isolated from the rest of the network, so as to reduce the possibility of disclosing confidential information.

● performance improvement

Dividing the layer 2 plane network into multiple logical working groups (broadcast domain) can reduce unnecessary traffic diffusion on the network and improve performance.

● increase the flexibility of network connection

With the help of VLAN technology, different locations, different physical networks and different users can be combined to form a virtual network environment, which is as convenient, flexible and effective as using local LAN.

5.3 VIDconcept

Vid is the VLAN identification number of the data frame received by the switch.The switch classifies the data frames according to the VLAN ID (VID) of the received data frames. Those without label are classified as one class, and those with the same label are classified as one class.The switch decides to forward or discard a packet according to the vid. At the same time, the switch with VLAN enabled can also configure a vid to an unmarked frame or a frame with priority tag.If a data frame is not marked with vid, the VLAN enabled switch will configure a vid to it and insert the vid into its frame header.Through this process, the switch processes the packet forwarding and fills in the VLAN of the data frame or the tag field of the priority information.The administrator can set priority to select VLAN type and vid value.

5.4 PVID

PVID is the port base VLAN ID, that is, the virtual LAN ID number of the port, which is related to the VLAN tag tag when the port sends and receives data frames.PVID is an attribute of each port when dividing VLAN.There are three types of ports on the switch. One is the device directly connected to the access layer port, which is called access (access port);There is also a hybrid mode called trunk and access.The specific processing messages of these three ports are described below.

5.5 Port processing message mode

According to different requirements, users need to configure VLAN types and VLAN list for different ports. Table 4.1 below briefly describes the different processing methods of various types of messages:

Three types of VLAN port message processing methods

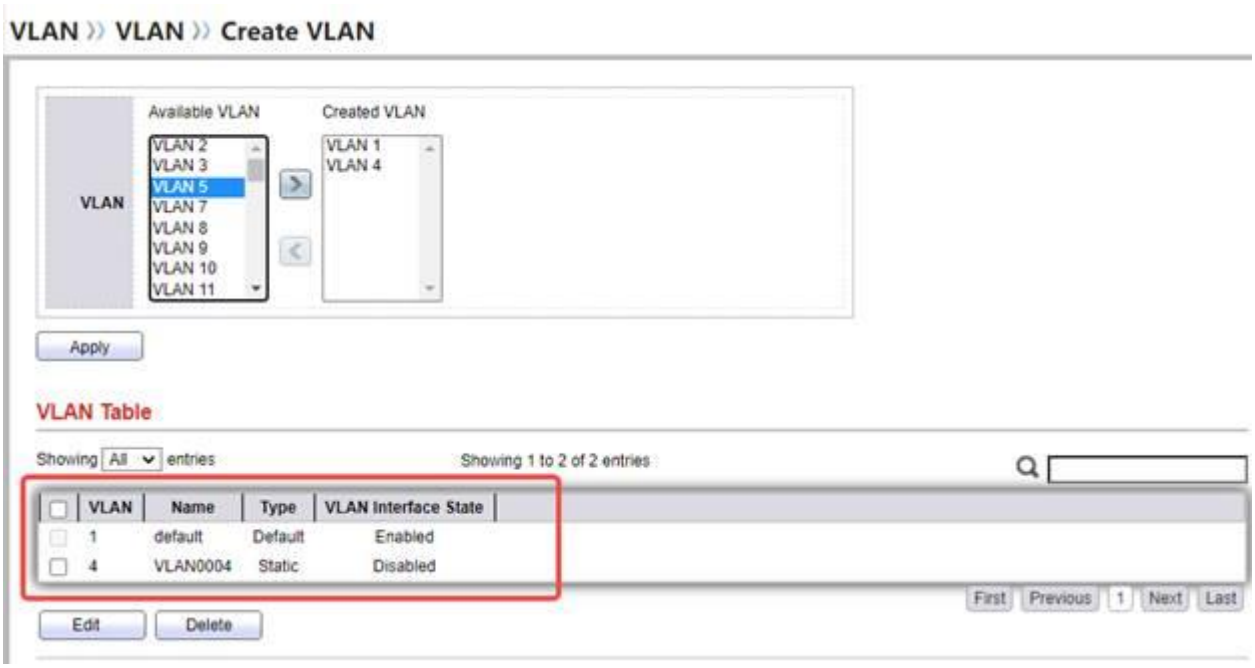
VLAN port type	Processing of entry message	Processing of export message

Access port	1.Receive a message; 2.Judge whether there is VLAN tag: if not, go to step 3, otherwise go to step 4; 3.Mark the PVID of the port and exchange and forward it; 4.Discard message	1.Judge whether there is VLAN tag: If yes, go to step 2, otherwise go to step 3; 2.Judge whether the label of valn is the same as the PVID of the terminal. If it is the same, strip the label and forward it, otherwise discard it 3.Discard message
Trunk port	1.Receive a message; 2.Judge whether there is VLAN tag: if not, go to step 3, otherwise go to step 4; 3.Mark the PVID of the port, and the PVID of the VLAN will be exchanged and forwarded in the port tag table, otherwise it will be discarded; 4.Judge whether the PVID of the VLAN exists in the tag table of the port: if so, forward it, otherwise discard it	1.Compare the PVID of the port and the VLAN tag of the message to be sent; 2.If they are the same, go to step 3, otherwise go to step 4; 3.Judge whether the tag is in the port tag table. If the VLAN tag is stripped, send it again, otherwise discard it; 4. Judge whether the tag is in the port tag table. If it is sent directly, otherwise it will be discarded
Hybrid port	1.Receive a message; 2.Judge whether there is VLAN tag: if not, go to step 3, otherwise go to step 4; 3.Mark the PVID of the port, and the PVID will be exchanged and forwarded in the port tag or untag table, otherwise it will be discarded; 4.Judge whether the vid of the message exists in the tag or untag table of the port: if so, forward it, otherwise discard it	1.Judge whether there is VLAN tag: If yes, go to step 2, otherwise go to step 3; 2.Judge whether the tag is in the port tag or untag table. If it is in the untag table, strip the VLAN tag and send it again. If it is in the tag table, judge whether the tag is the same as the port PVID, strip the tag and forward it directly, and the message not in the tag or untag table is discarded; 3.Discard message

5.6 VLANport configuration

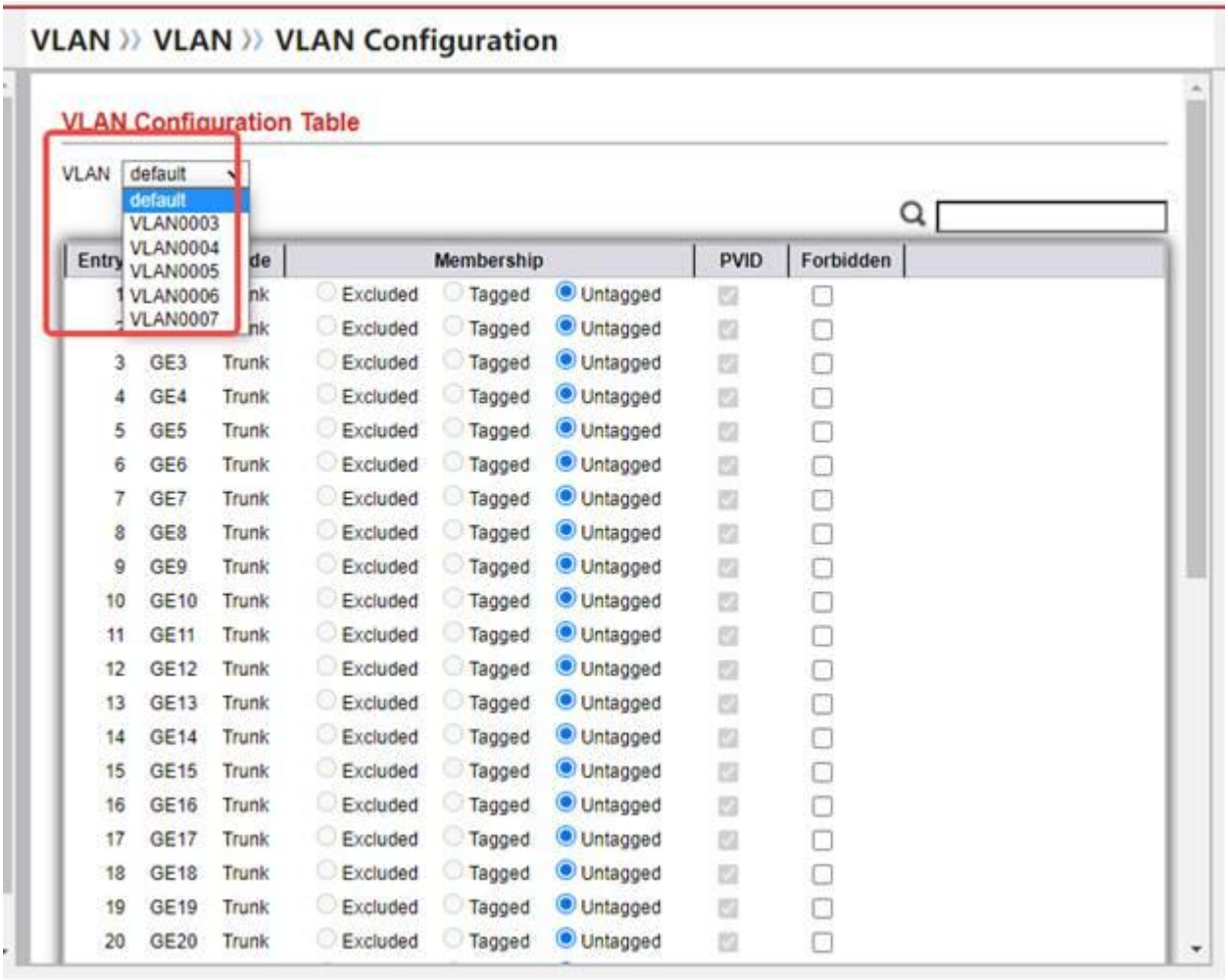
Configuration steps

1. Select [VLAN] in the navigation bar to enter the [create VLAN / VLAN] interface, which can create VLANs, as shown in the following figure:



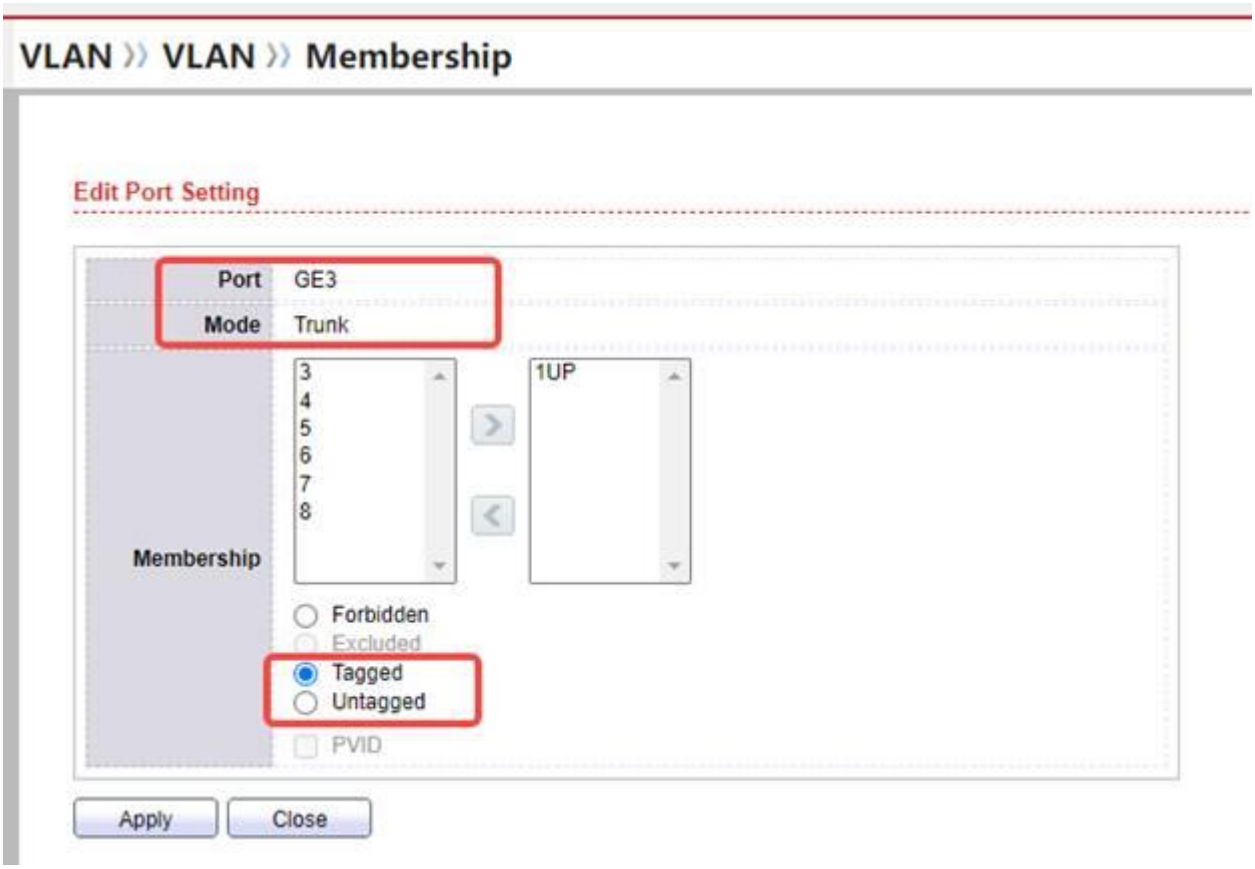
Select the VLAN to be created and click Button, and the created VLAN will be displayed in the red box in the figure above.

2. Select [VLAN] in the navigation bar to enter the [VLAN configuration / VLAN] interface, which can view the ports to which the VLAN belongs, as shown in the following figure:

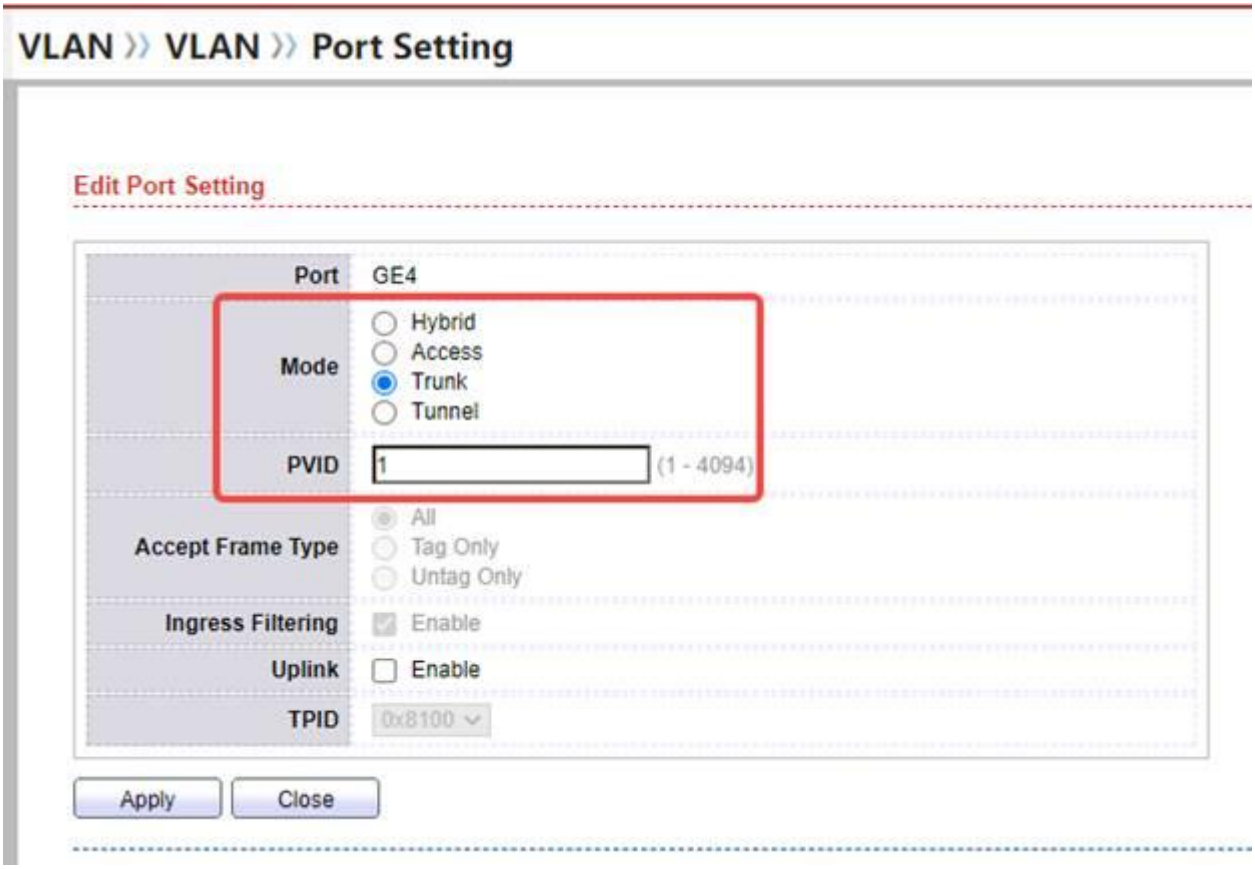


The red box is the VLAN list, but the VLAN must be a VLAN that has been created.

3. Select [VLAN] in the navigation bar to enter the [membership / VLAN] interface, which can set the tagged and untagged parameters of the port, select the port to be modified, and then click Edit Button to enter the setting page, as shown in the following figure:



4. Select [VLAN] in the navigation bar to enter the [port setting / VLAN] interface, which can set the port mode and PVID, select the port to be set, and click Edit Button, as shown below:

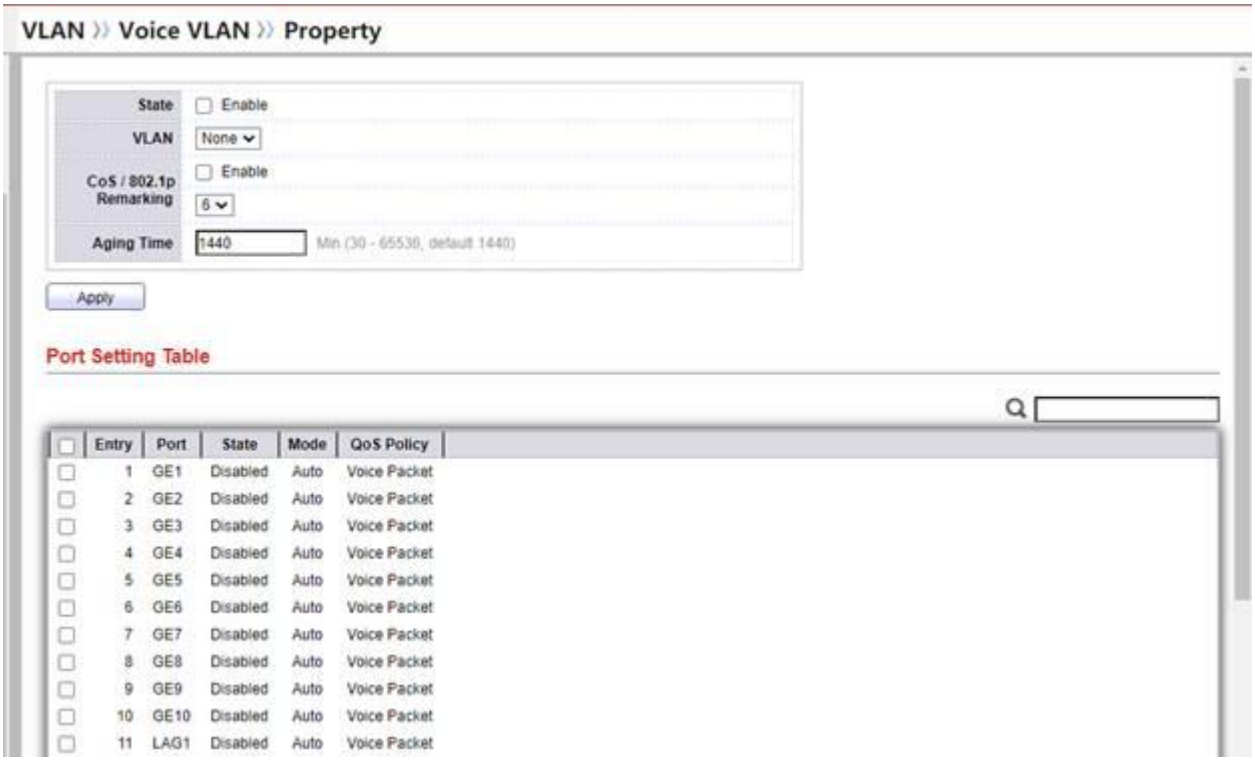


5.7 Voice VLAN

Voice VLAN is a VLAN divided for users' voice data flow.By creating a voice VLAN and adding the port connecting the voice device to the voice VLAN, users can centralize voice data in the voice VLAN for transmission, facilitate targeted QoS (quality of service) configuration of voice flow, improve the transmission priority of voice flow and ensure the call quality.The Ethernet switch supporting voice VLAN can judge whether the data stream is a voice data stream according to the source MAC address field in the data message entering the switch port. The message whose source MAC address conforms to the address of the voice device oui (organizational unique identifier) set by the system is considered to be a voice data stream.

Configuration steps

1. Select [vocie VLAN / VLAN] in the navigation bar to enter the [property] interface, as shown below,

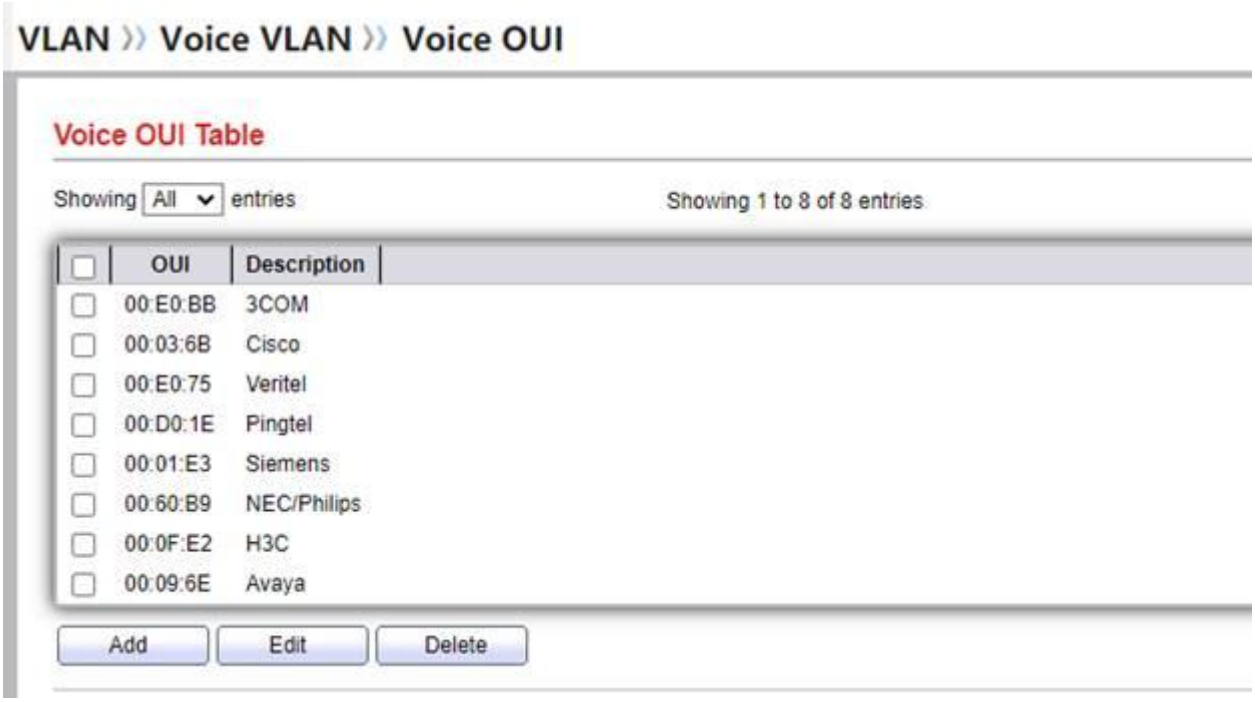


Configuration item description

Description of configuration items of relevant interfaces of VLAN [property / voice VLAN].

State	: not enabled : Enable
VLAN	Use the VLAN corresponding to voice VLAN
COS/802.1P Remarking	Priority, re tagging, messages conforming to vocie VLAN configuration will be added with the set priority
Aging Time	Aging time

The picture of voice oui matched with voice VLAN is as follows:



The MAC address in the figure above is only the display of the first half of the MAC address. As long as the first half of the MAC address conforms to the voice VLAN, the message will be marked with the set priority.

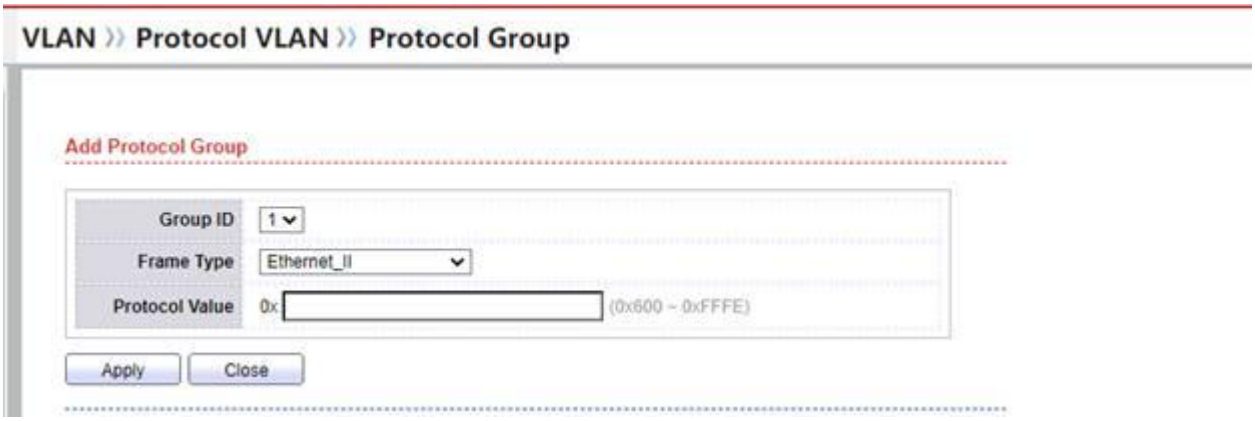
5.8 Protocol VLAN

Protocol based VLAN, also known as protocol VLAN, is another VLAN division method different from port based VLAN.By configuring the VLAN based on the protocol, the switch can analyze the messages received on the port without VLAN tag, match the messages with the protocol template set by the user according to different packaging formats and the values of special fields, and automatically add the corresponding VLAN tag for the successfully matched messages, so as to automatically distribute the data belonging to the specified protocol to the corresponding VLAN for transmission.

Configuration steps

1. Select [protocol VLAN / VLAN] in the navigation bar, enter the [protocol group] interface, and click 

Button to add, as shown in the following figure:



Configuration item description

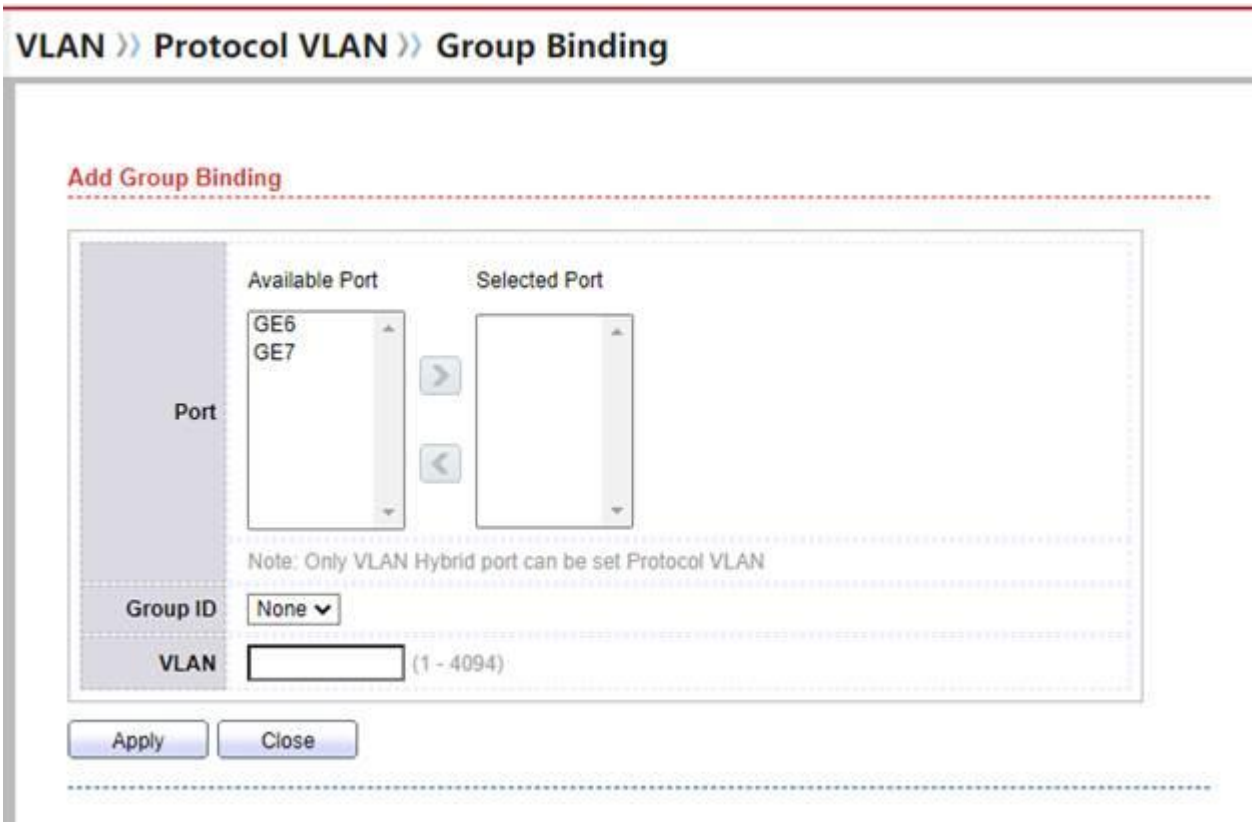
Description of configuration items of relevant interfaces of VLAN [protocol group / protocol VLAN].

Group ID	The protocol VLAN identifier (1-8)
Frame Type	Protocol type for implementing protocol VLAN
Protocol Value	Protocol value for the previous option

This interface only configures protocol VLAN group. After configuration, port binding is also required. The steps are as follows:

Select [protocol VLAN / VLAN] in the navigation bar, enter the [group binding] interface, and click 

Button, as shown in the following figure:



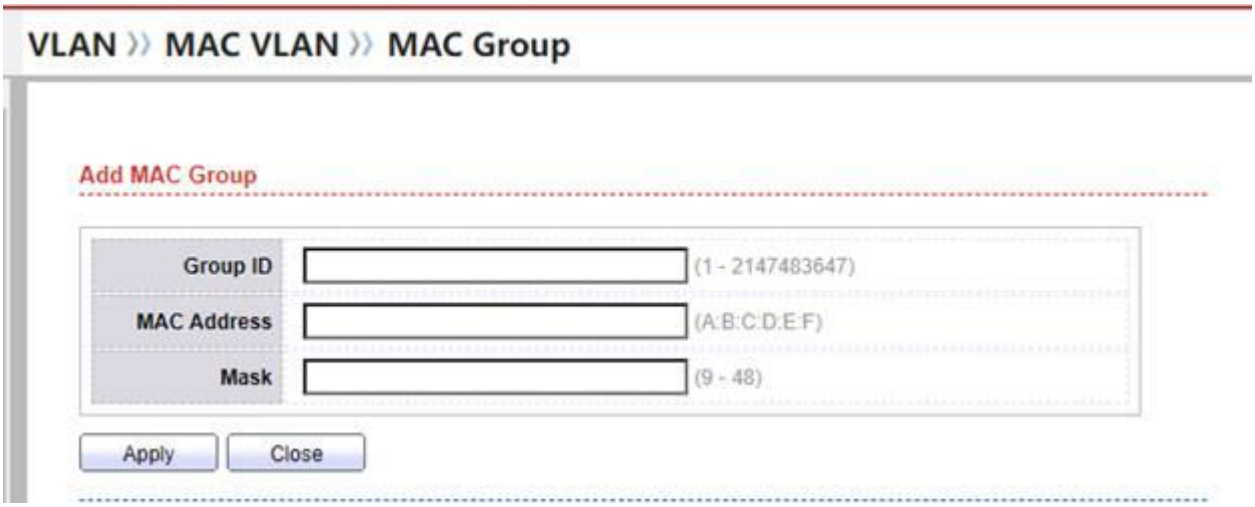
Note: this function requires the port mode to be hybrid

5.9 MAC VLAN

Mac VLAN is a VLAN divided based on MAC address. The biggest advantage of MAC VLAN is that users do not need to be fixed on some ports and can move freely. For example, when users move their physical location, that is, when they change from one switch to another switch, the VLAN does not need to be reconfigured,It can be considered that this method of dividing VLAN according to MAC address is based on the user's MAC address information.The disadvantage of MAC VLAN is that all users must configure the corresponding relationship between MAC and VLAN during initialization.

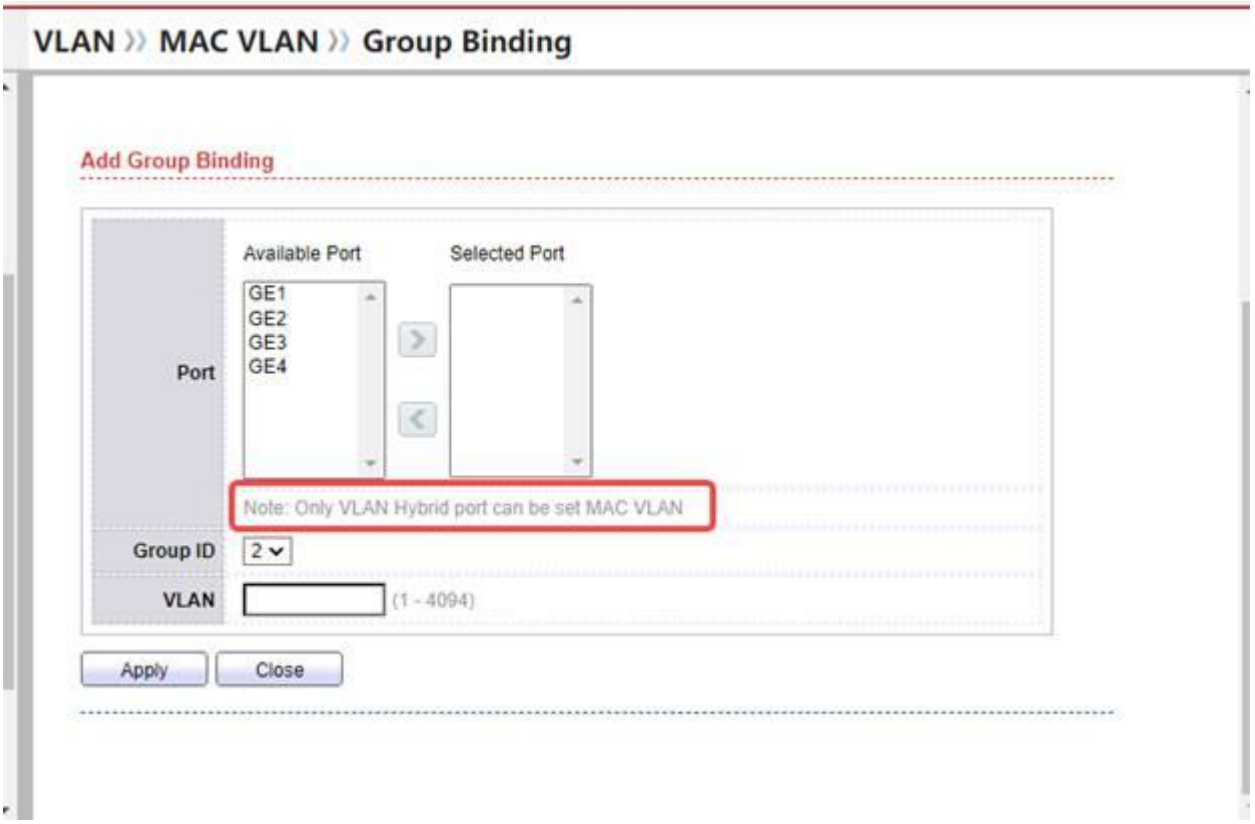
Configuration steps

1. Select [MAC group / Mac VLAN / VLAN] in the navigation bar, enter the [MAC group] interface, and click Add Add MAC VLAN group, as shown in the following figure:



The mask in the above figure refers to the mask of MAC address. After setting the MAC group, the port needs to be bound before it takes effect.

2. Select [VLAN / group] in the [VLAN / group] navigation interface, and click [VLAN / group] Add Bind MAC group, as shown in the following figure:

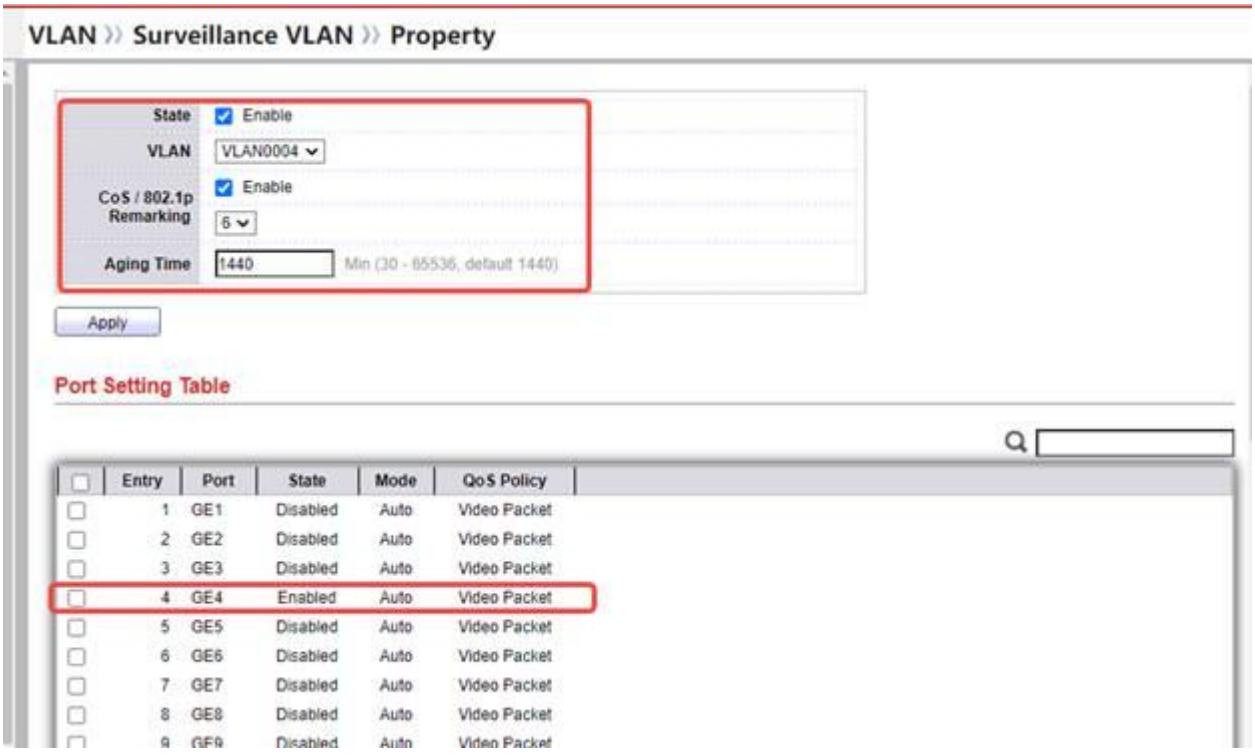


5.10 Surveillance VLAN

Surveillance VLANIs a special VLAN, which is mainly used to carry data packets of image data stream. In order to ensure the transmission of this kind of data, if the source MAC address of image data packet matches the list MAC address defined by surveillance VLAN, the switch will not only mark this kind of data packet with surveillance VLAN,At the same time, the cos value of the data packet is changed into a value with higher priority than the ordinary data packet.At this time, because this kind of data packet has high priority, combined with QoS Technology, this kind of data packet can be transmitted preferentially in the switch.

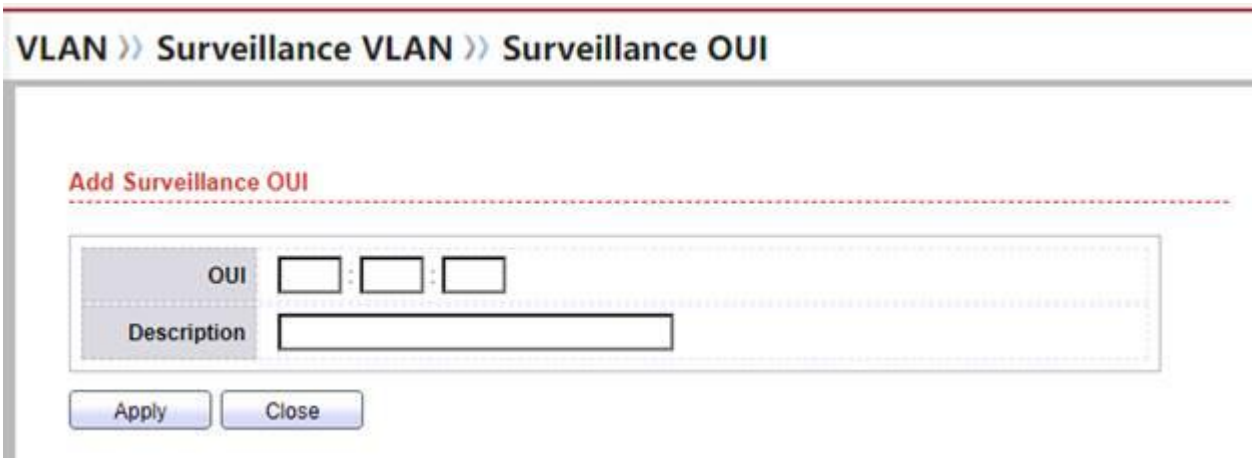
Configuration steps

1. Select [surveillance VLAN / VLAN] in the navigation bar to enter the [property] interface, as shown below:



The figure above is divided into two parts, one is to enable the function, the other is to enable the corresponding port.

2. Select [surveillance VLAN / VLAN] in the navigation bar, enter the [surveillance oui] interface, and click Add Add the surveillance oui interface, as shown in the following figure:



Surveillance oui matches the source MAC address of the data packet of the image data stream.

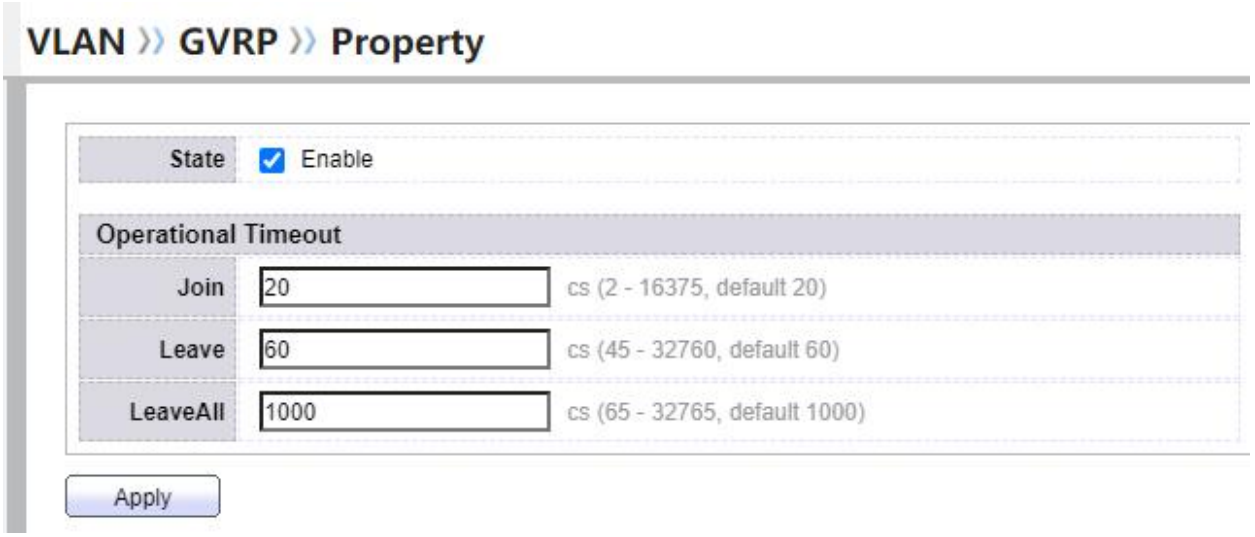
5.11 GVRP

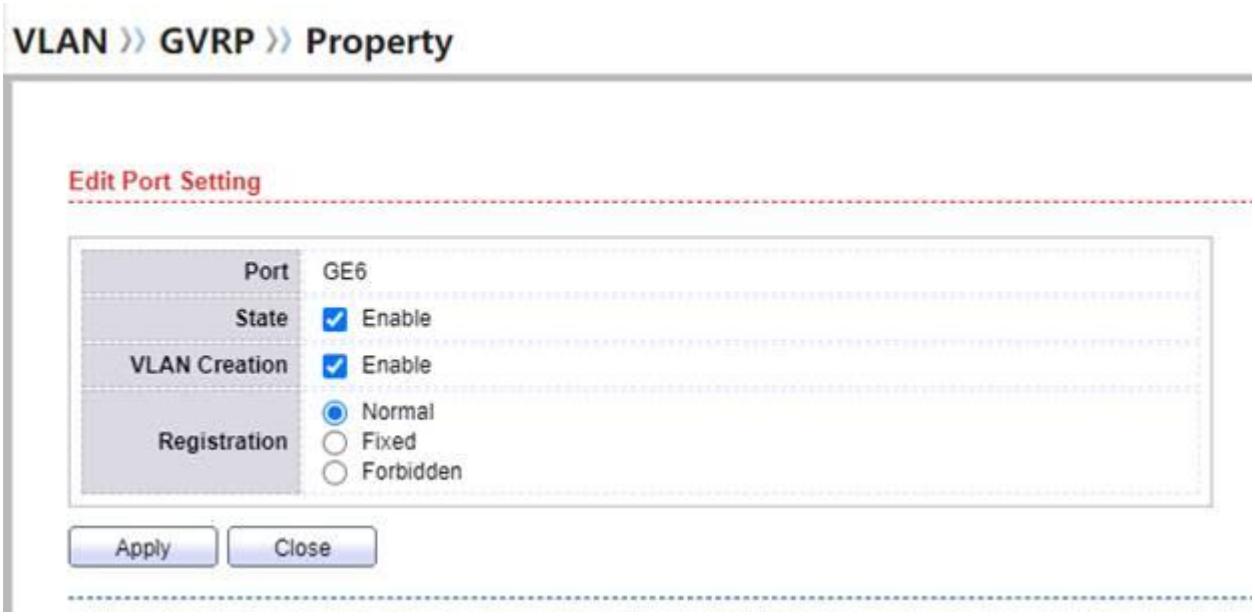
GARPThe protocol is mainly used to establish a mechanism of attribute transmission and diffusion to ensure that entities can register and unregister the attribute.As a carrier of attribute registration protocol, GARP can be used to propagate attributes.Mapping the content of GARP protocol message into different attributes can support different upper layer protocols.

GVRP is an application of GARP, which is used to register and unregister VLAN attributes.

Configuration steps

3. Select [GVRP / VLAN] in the navigation bar, enter the [property] interface, and click Edit The settings are as follows:





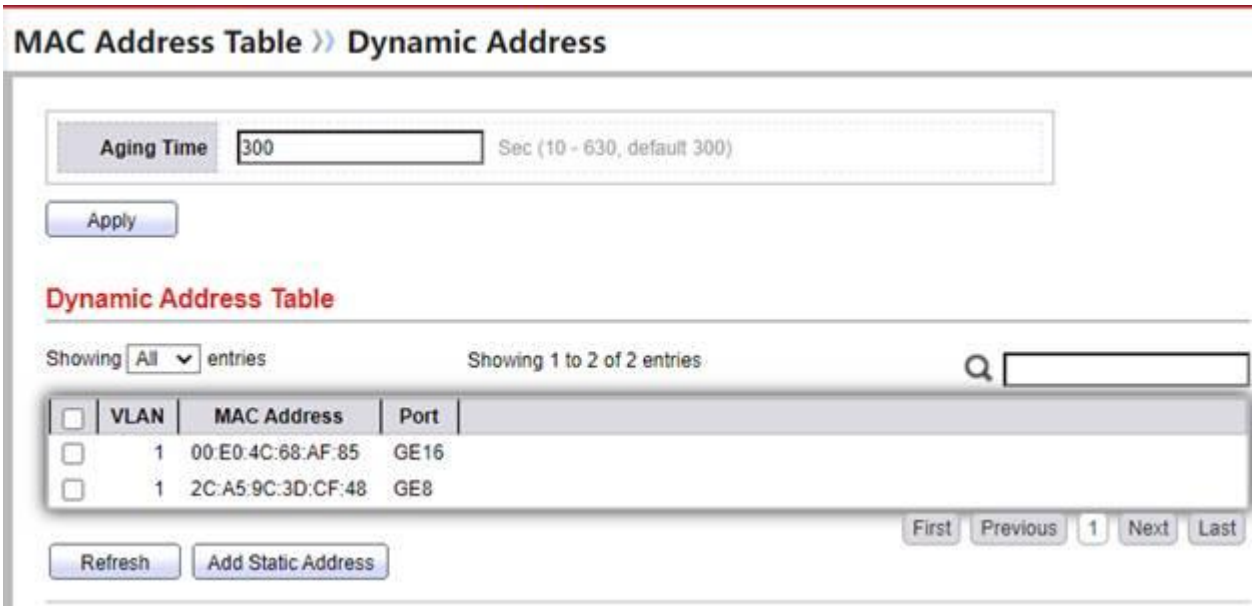
Note: both ends of the link of this function need to be turned on, and the port mode needs to be trunk mode, and the VLAN created needs to be allowed to pass through.

Chapter 6 MAC Address table

6.1 Dynamic MAC address table

Configuration steps

1.Select [MAC address table] in the navigation bar to enter the [dynamic address] interface, which can query the dynamic MAC address and change the dynamic MAC address to a static MAC address, as shown in the following figure:



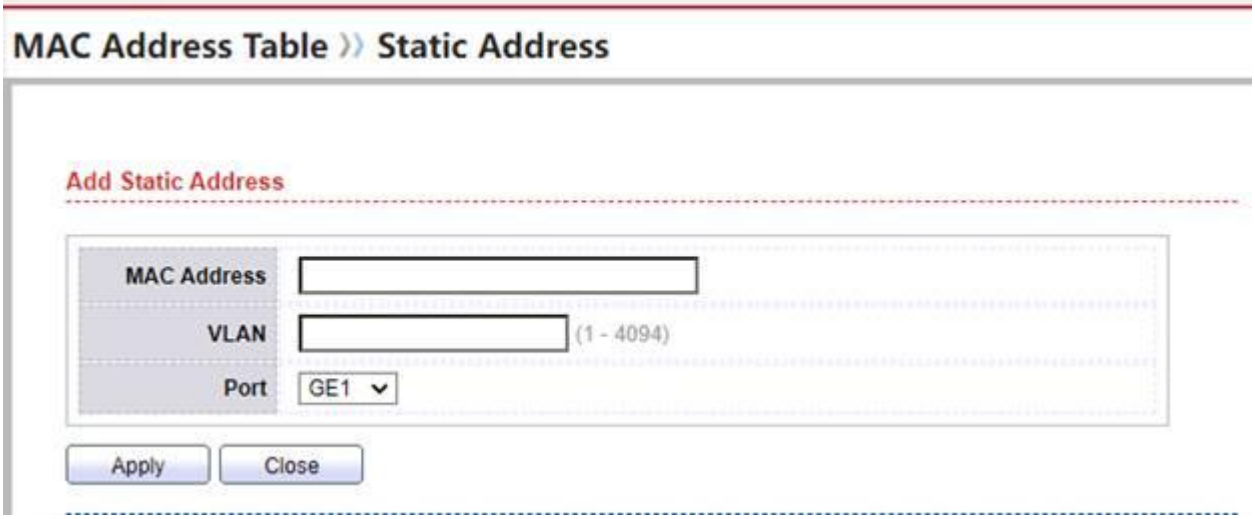
Select the MAC address to be modified, and then click Add Static Address Button to change the dynamic MAC address to the static MAC address.

6.2 Static MAC address table

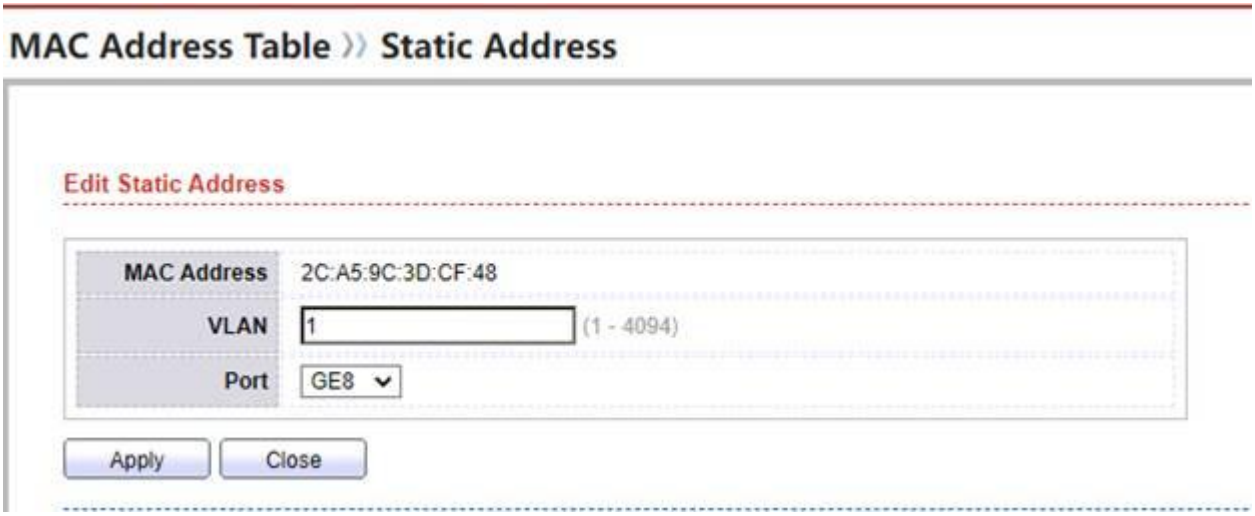
Configuration steps

1.Select [MAC address table] in the navigation bar to enter the [static address] interface, where you can view the static MAC address, add the static MAC address and edit the static MAC address attribution, as shown in the following figure:

click Add Button to add a static MAC address, as shown in the following figure:



Select the static MAC address to be modified and click Edit Button to modify, as shown in the following figure:

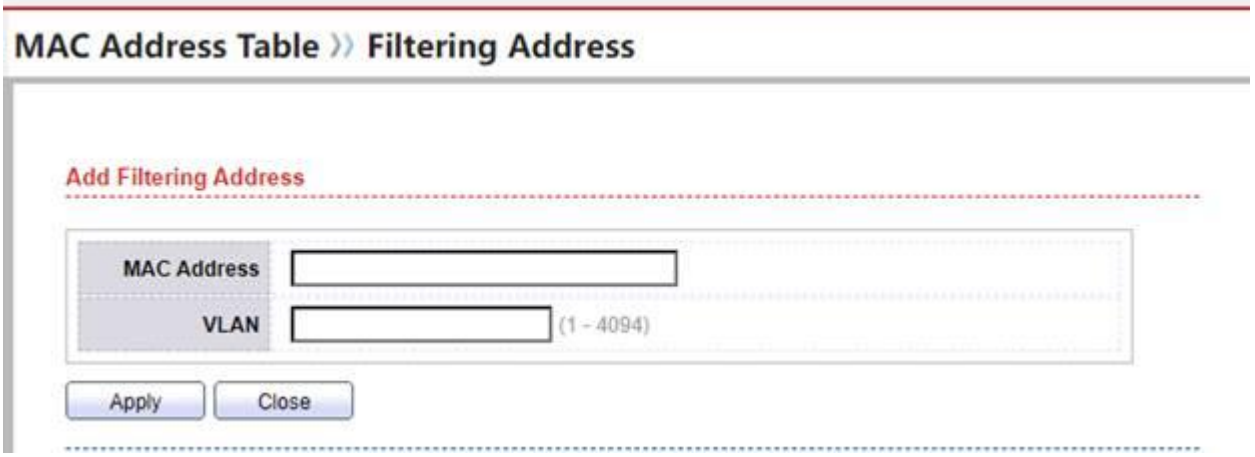


6.3 MACAddress filter table

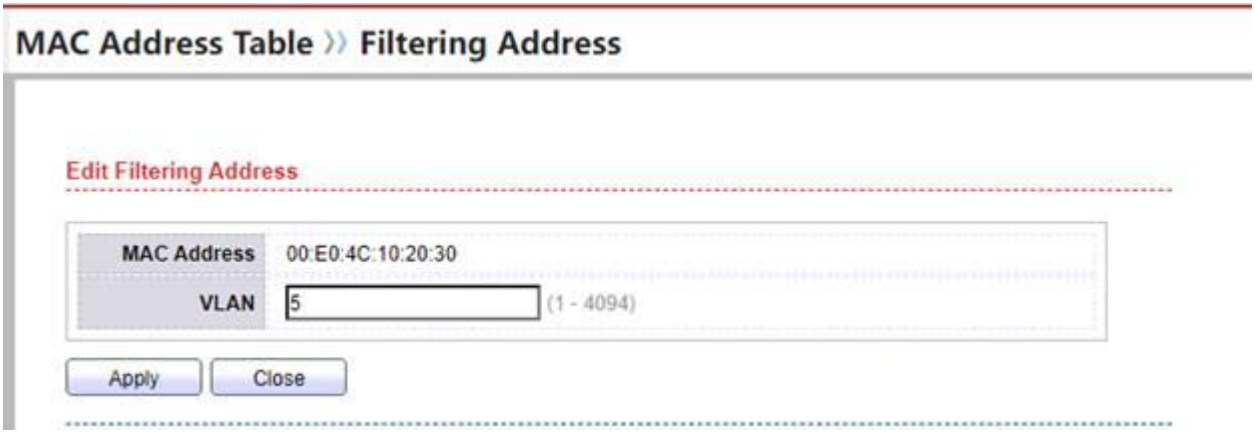
Configuration steps

1.Select [MAC address table] in the navigation bar to enter the [static address] interface, where you can view the MAC address filtering list or add MAC address filtering table items, as shown in the following figure:

click Add Button to add a filtered MAC address table entry, as shown in the following figure:



Select the filter MAC address table item to be modified, and click Edit Button to modify, as shown in the following figure:



6.4 Port security MAC address table

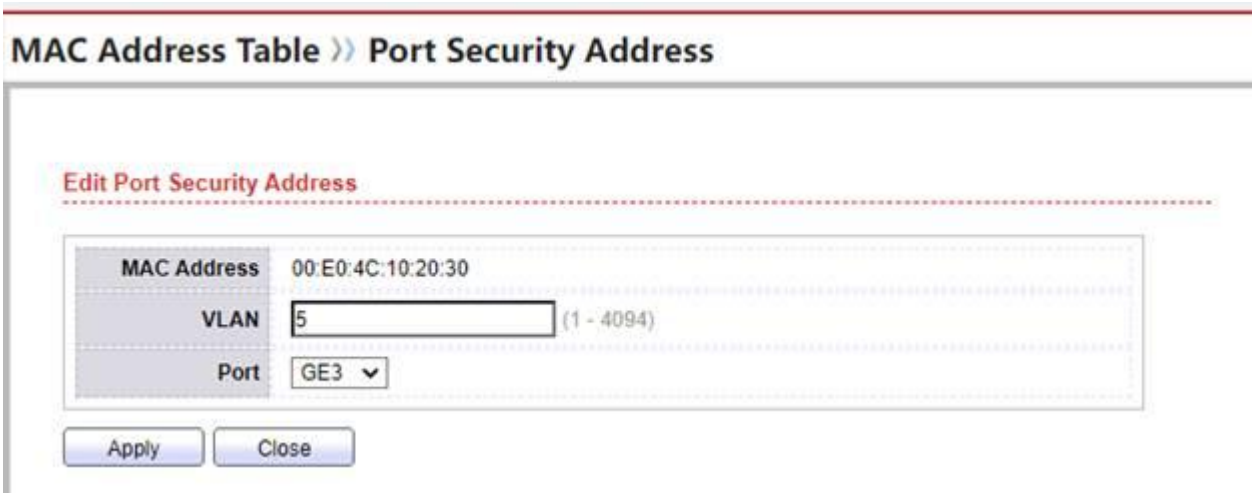
Configuration steps

1.Select [MAC address table] in the navigation bar to enter the [port security address] interface, which can set port security binding, as shown in the following figure:

Note: this interface function needs to be used in conjunction with the port security function of the port interface.

click Add Button to add port security MAC address table entry, as shown in the following figure:

Select the port security MAC address table item to be modified, and click Edit Button to modify, as shown in the following figure:



Chapter 7 Spanning Tree

7.1 STPsummary

STP (spanning tree protocol) is the English abbreviation of spanning tree protocol.The STP protocol defines the concepts of root bridge, root port, designated port and path cost, which are used to prune the loop network into a loop free tree network by constructing a natural tree, so as to avoid the proliferation and infinite circulation of packets in the loop network,At the same time, link backup and path optimization are realized.

STP uses BPDU (bridge protocol data unit), also known as configuration message, to exchange information between bridges.STP BDUp is a layer-2 message. When the destination MAC is multicast address 01-80-c2-00-00-00, all bridges supporting STP protocol will receive and process the received BPDU message.The data area of the message carries all the useful information for spanning tree calculation.

7.2 STPTechnical introduction

7.2.1 Root bridge

The tree network structure must have tree roots, so STP introduces the concept of root bridge.There is only one root bridge in the whole network, and the root bridge will

change according to the change of network topology, so the root bridge is not fixed.After the network converges, the root bridge will generate and send out the configured BPDU at a certain time interval, and other devices will forward the configured BPDU to ensure the stability of the topology.The selection of the root bridge is based on the bridge ID (bridge ID) composed of the bridge priority and the bridge MAC address. The bridge with the smallest bridge ID will become the root bridge in the network.

7.2.2 introduction to STP and RSTP

RSTP (802.1w) is developed from 802.1ad. Its purpose is to solve the problem of long convergence time of STP. The following is an introduction to RSTP and STP:

Table 7.1 STP / RSTP introduction

	STP	RSTP	MSTP
Technical introduction	The data link layer (layer 2) communication protocol based on OSI network model is used to ensure a loopless regional network environment.By selectively blocking redundant links to eliminate the layer-2 loop of the network, it also has the function of link backup, also known as extended tree protocol.	RSTP is developed from STP. Its basic idea is the same, but it further deals with the problem of temporary loss of network connectivity.	MSTP not only involves multiple mstis, but also can be divided into multiple MST domains.In general, an MSTP network can contain one or more MST domains, and each MST domain can contain one or more mstis.Each MSTI is composed of switching devices running STP / RSTP / MSTP, which is a tree network formed by these switching devices after calculation by MSTP protocol.
Same point	1.There is only one spanning tree in the whole switching network, and the topology convergence is affected by the network topology scale;		

	2.The connectivity of the network is affected by the symmetry of the network structure; 3.The link is blocked and the link does not carry any traffic.		
difference	1.It cannot be migrated quickly and needs to wait twice the forward delay time; 2.At point-to-point or edge ports, you need to wait twice the delay time; 3.The edge port needs to wait twice the delay time.	1.It can migrate quickly. When the root port / specified port fails, the replacement port / backup port will enter the forwarding state without delay; 2.The designated port only needs to shake hands with the downstream bridge once to enter the forwarding state without delay; 3.The port directly connected to the terminal rather than other bridges is defined as edge port.The edge port can directly enter the forwarding state without any delay.	1.The whole switch network can have multiple spanning trees; 2. Load balancing of data traffic between VLANs; 3.The link can carry traffic after being blocked; 4.Fast convergence of network topology.

7.3 Global configuration

Configuration steps

1. Select [property / spanning tree] in the navigation bar to enter the configuration interface, where you can view the global configuration information of STP, as shown in the following figure:

Configuration item description

Configuration item	explain
Operation Mode	The current RSTP mode supports STP and MSTP
Path Cost	The path overhead mode of STP port is divided into long mode and short mode
BPDU Handling	The forwarding mode of BPDU is divided into filtering discarding and flooding
Priority	System priority of STP
Hello Time	Time interval of STP sending Hello time message
MaxAge	The maximum lifetime of the STP protocol packet received by the bridge. If no new protocol packet is received beyond this time, the packet will be discarded
Forward Delay	Delay time of STP
Tx Hold Count	The maximum number of STP protocol packets sent by the port per second

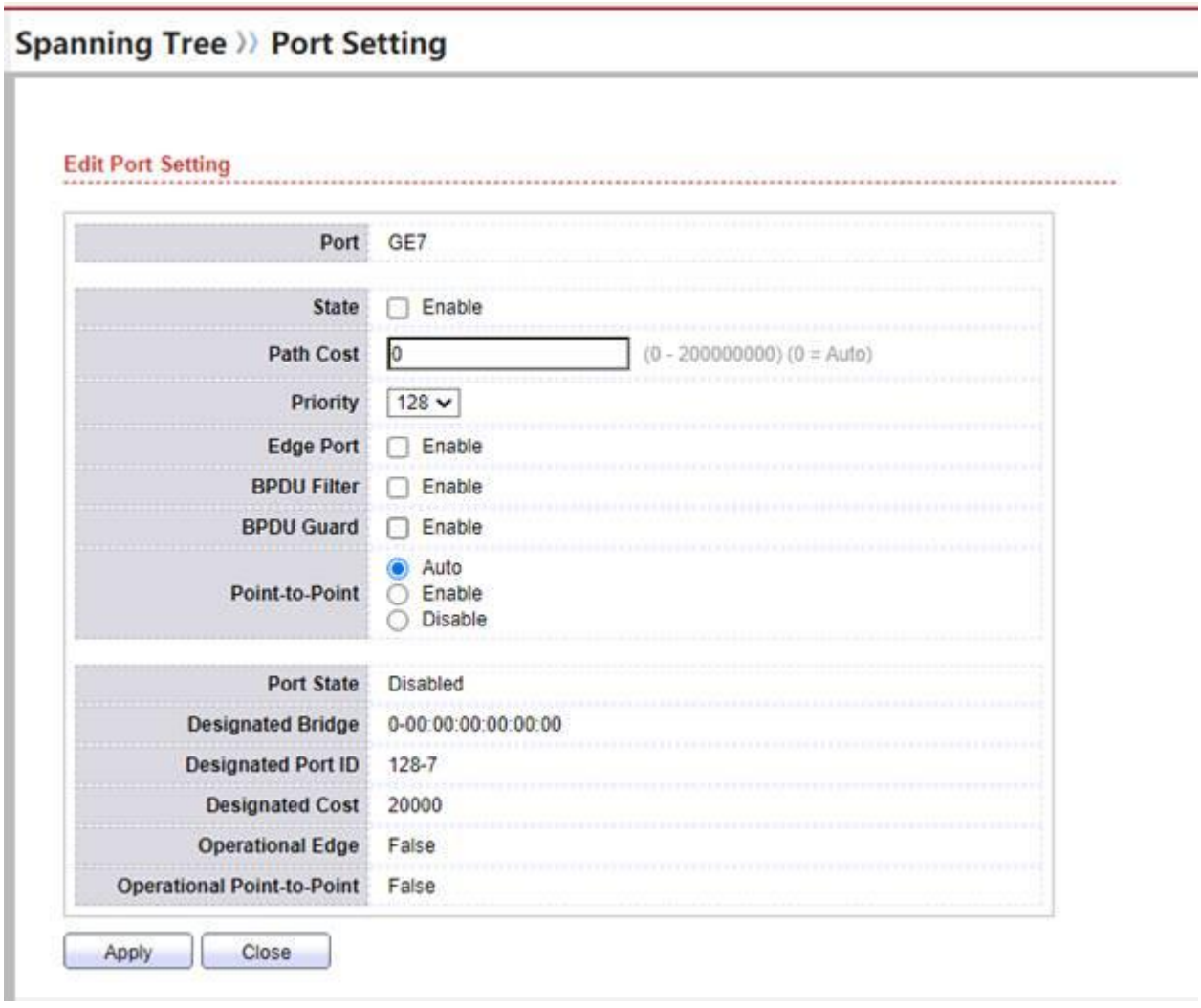
7.4 port configuration

Configuration steps

1Select [port setting / spanning tree] in the navigation bar to enter the STP port setting interface.

2. in the [port setting] interface, you can view the port configuration information of STP.

3If you need to modify the port, you can select it below and click Edit Button to enter the port configuration interface of STP, as shown in the following figure:



Configuration item description

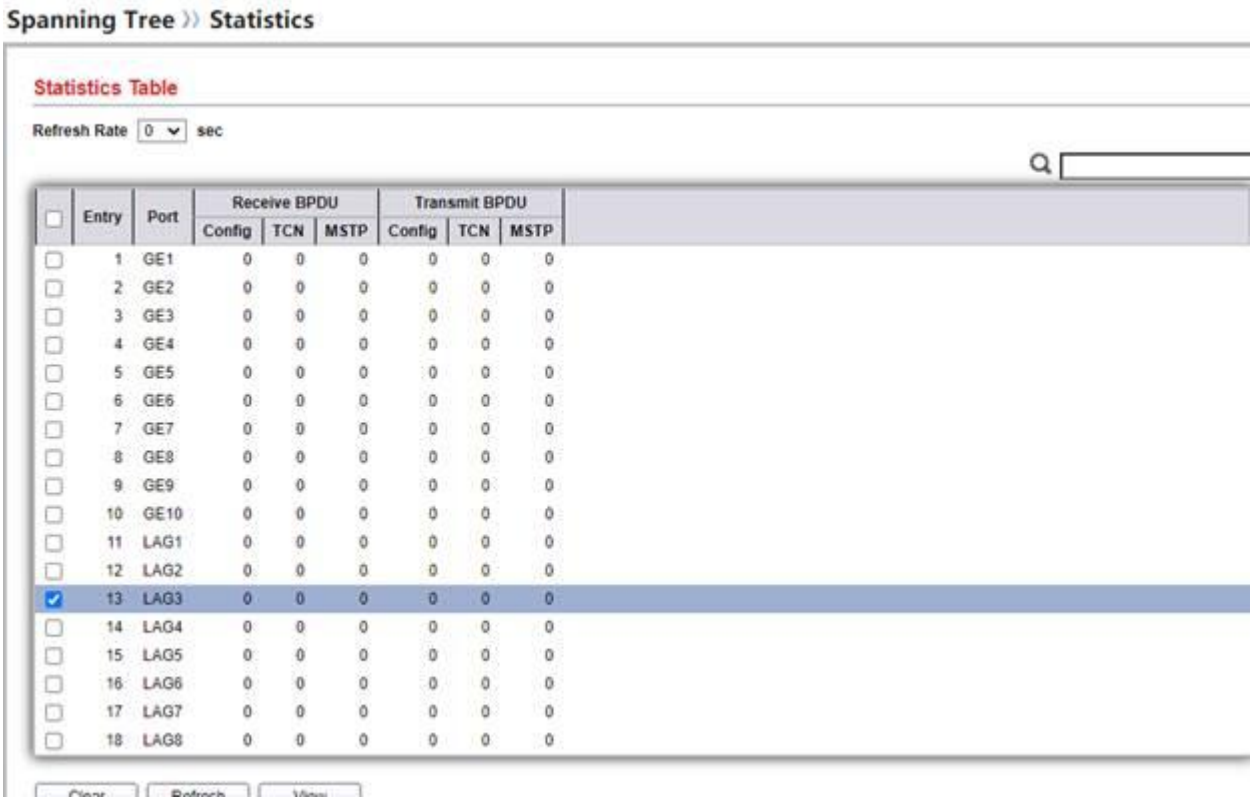
Configuration item	explain
Port	Port name
State	STP enable of port,or, which is disabled by default
Path Cost	STP port overhead
Priority	Priority of STP port

Edge Port	Edge port
BPDU Filter	BPDU filtering
BUDU Guard	BPDU protection

7.5 Port data display

Configuration steps

1. Select [statistics / spanning tree] in the navigation bar to enter the STP port data display interface, which can view the STP message data of the port, as shown in the following figure:



Chapter 8 LLDP

8.1 LLDP summary

Lldp is a protocol used for information announcement and acquisition. However, it should be noted that the information announcement sent by lldp does not need

confirmation and cannot send a request to request to obtain some information. That is to say, lldp is a one-way protocol. There is only one working mode of active announcement, which does not need confirmation and cannot be queriedRequest (for example, request the MAC address of an IP like ARP Protocol).

8.2 LLDPTechnical introduction

Lldp mainly completes the following work:

- l Initialize and maintain the information in the local MIB library
- l The information is extracted from the local MIB library and encapsulated into the lldp frame.There are two trigger modes for sending lldp frames: one is triggered when the timer expires, and the other is triggered when the device state changes.
- l Identify and process the received lldpdu frames
- l Maintain lldp MIB information base of remote equipment
- l When there is a change in the MIB information base of the local or remote device, a notification event is sent

8.3 LLDPto configure

8.3.1 LLDPGlobal settings

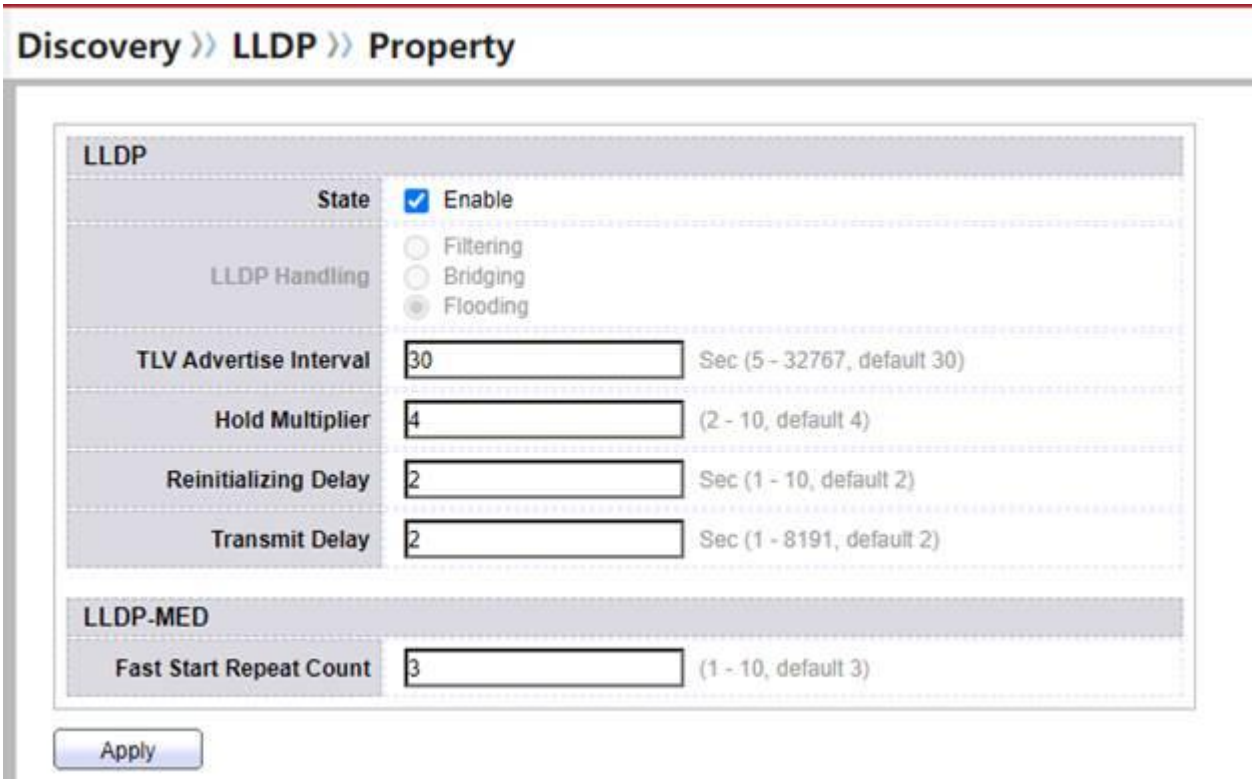
Configuration steps

1. Select [property / lldp / discovery] in the navigation bar to enter the lldp global setting interface.

2. in the lldp global setting interface, you can view the global configuration of lldp, as shown in the following figure:

3. modify the corresponding configuration in the lldp global configuration box, and then click 

。



8.3.2 LLDPport configuration

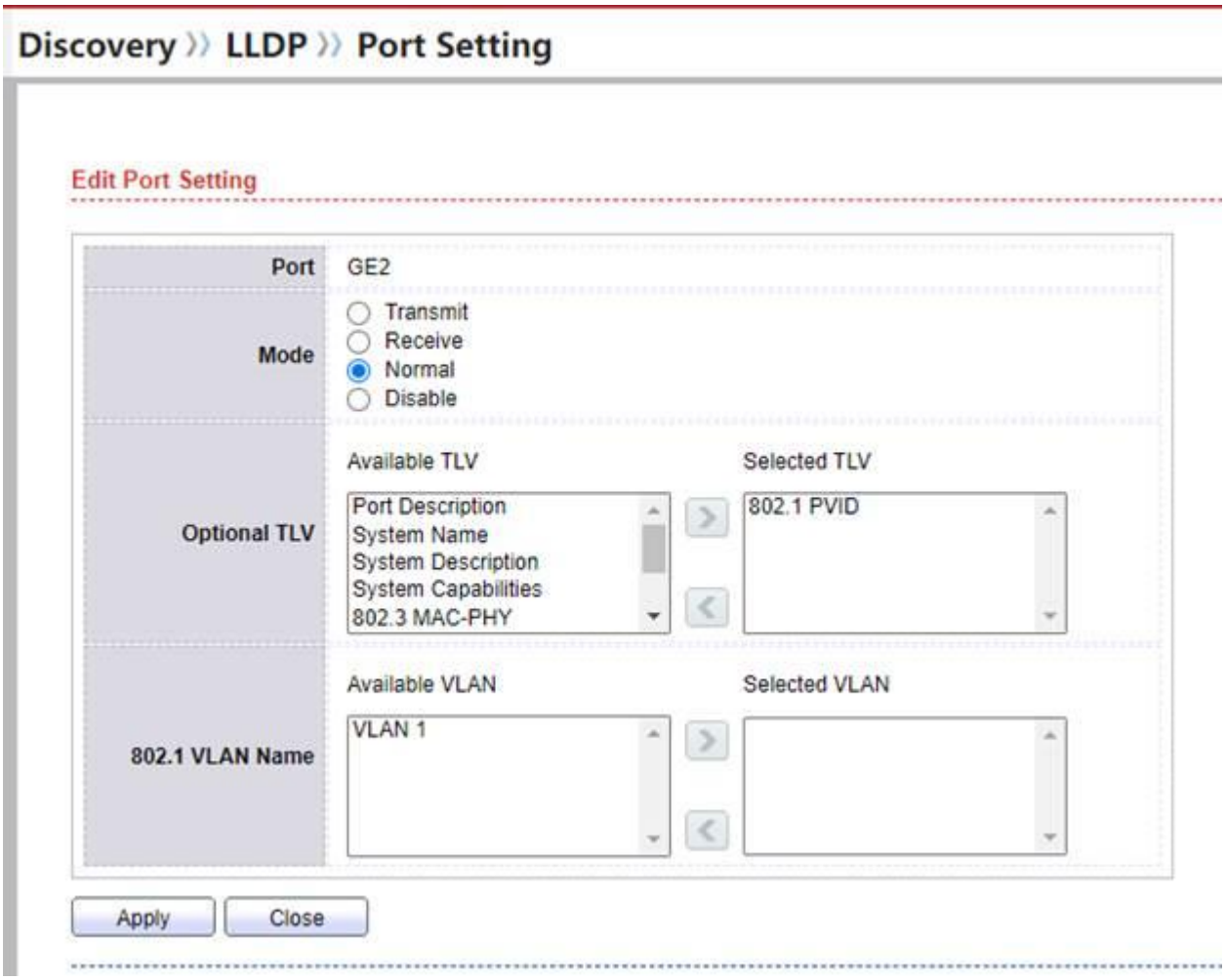
Configuration steps

1. Select [port setting / lldp / discovery] in the navigation bar to enter the lldp port configuration interface.

2. in the lldp [port configuration] interface, you can view the port related configuration of lldp.

3. to modify the lldp configuration of a port, select the port and click the button below 

, as shown below



8.3.2 lldp message statistics

Configuration steps

Select [statistics / lldp / discovery] in the navigation bar to enter the lldp message statistics page, which mainly displays the lldp message data of each port, as shown in the following figure:

Discovery » LLDP » Statistics

Insertions	0
Deletions	0
Drops	0
AgeOuts	0

Clear Refresh

Statistics Table

Entry	Port	Transmit Frame	Receive Frame			Receive TLV		Neighbor
		Total	Total	Discard	Error	Discard	Unrecognized	Timeout
1	GE1	0	0	0	0	0	0	0
2	GE2	0	0	0	0	0	0	0
3	GE3	0	0	0	0	0	0	0
4	GE4	0	0	0	0	0	0	0
5	GE5	0	0	0	0	0	0	0
6	GE6	91	0	0	0	0	0	0
7	GE7	0	0	0	0	0	0	0
8	GE8	0	0	0	0	0	0	0
9	GE9	0	0	0	0	0	0	0

Chapter 9 DHCP

9.1 DHCP Server side

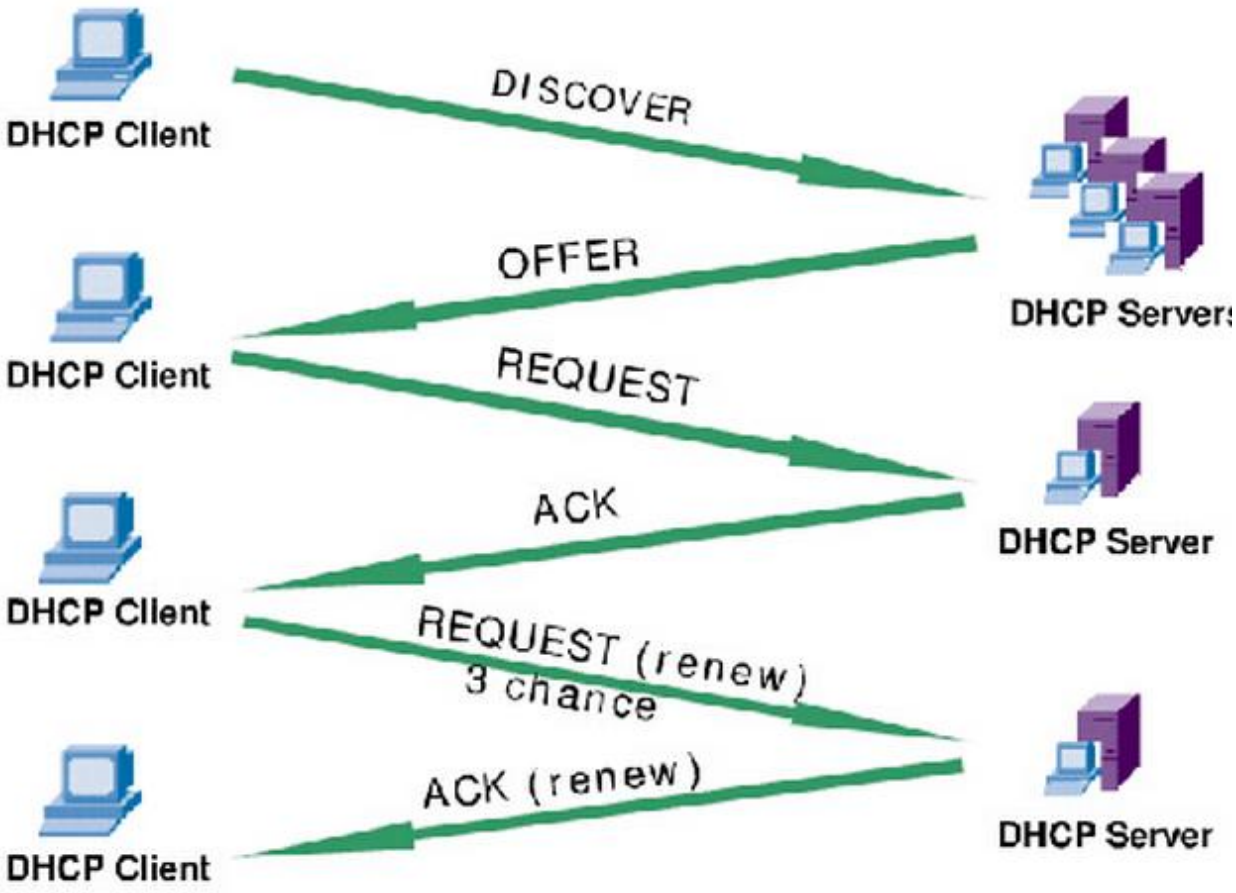
9.1.1 DHCP introduction

DHCP (Dynamic Host Configuration Protocol) is a LAN network protocol. It works with UDP protocol. It has two main purposes: automatically assigning IP addresses to internal networks or network service providers, and giving users or internal network administrators as a means of central management of all computers.

9.1.2 key concepts of DHCP

- DHCP client: DHCP client, which requests IP address through DHCP protocol.DHCP client is an interface level concept. If a host has multiple Ethernet interfaces, each interface on the host can be configured as a DHCP client.Each VLAN interface on the switch can also be configured as a DHCP client.
- DHCP server: DHCP server, which is responsible for providing IP addresses for DHCP clients and managing assigned IP addresses.
- DHCP relay: DHCP repeater, which realizes the forwarding function of DHCP messages when DHCP clients apply for IP addresses across network segments.
- DHCP security: DHCP security feature, which realizes the management function of legal user IP address table
- DHCP snooping: DHCP snooping, which records the user information applied to the IP address through the layer-2 device

17.2.3 introduction to DHCP working principle



Discovery phase:

That is, the process of the DHCP client looking for the DHCP server corresponds to the client sending DHCP discovery. Because the DHCP server corresponds to the DHCP client is unknown, the DHCP discovery message sent by the DHCP client is a broadcast packet, with the source address of 0.0.0.0 and the destination address of 255.255.255.255.All hosts supporting TCP / IP on the network will receive the DHCP discovery message, but only DHCP server will respond to the message.

If there are multiple DHCP servers in the network, multiple DHCP servers will reply to the DHCP discovery message.

If there is no DHCP server in the same VLAN and the vlanif is configured with DHCP relay function, the vlanif is a DHCP relay. The DHCP relay will modify the source IP address of the DHCP message to the IP address of the vlanif, and the destination address is the IP address of the DHCP server configured by DHCP relay.At the same time, modify

the IP address of giaddress vlanif in DHCP message.And send DHCP discovery to DHCP server by unicast.

DHCP server provision phase:

The DHCP server provision phase is the DHCP offer phase sent by the DHCP server in response to DHCP discovery

After receiving the DHCP discovery message, the DHCP server parses the subnet to which the request IP address belongs.And from dhcpdTake out an available IP address from the matching subnet in the conf file(after selecting an IP address from the available address segment, first send ICMP message to Ping the IP address. If the ICMP message of the IP address is received, discard the IP address, reselect the IP address and continue ICMP message test until an IP address not used in the network is found, so as to prevent the conflict between the dynamically allocated IP address and the IP address of other devices in the networkThe address conflict detection mechanism (configurable) is set in the yiaddress field in the DHCP discovery message to represent the IP address assigned to the client, and the option configured for the subnet is set for the lease, such as the default lease term, maximum lease term, router and other information.

DHCP selects the IP address from the address pool with the following priority:

1. the correspondence between the existing IP and MAC

2Previous IP address of client

3. read the value of requested IP address option in the discovery message. If it exists and the IP address is available

4. select the IP address from the configured subnet:

The DHCP server parses the subnet to which the IP requested by DHCP discovery belongs. First, check whether the giaddress in the DHCP discovery message has a DHCP relay. If so, obtain it from the available IP address segment in the subnet described by giaddress and allocate the IP.If giaddress does not have an IP address, the IP address is assigned from the network segment to which the IP address of the interface bound by the DHCP server belongs.

DHCP client selection phase:

After receiving the DHCP offer message from several DHCP servers, the DHCP client selects one of them as the target DHCP server.The selection strategy is usually to select the DHCP server to which the DHCP offer message of the first response belongs.

Then answer a DHCP request message by broadcasting, which contains the IP address and other information requested from the target DHCP.The reason why it is sent by broadcast is to inform other DHCP servers that they will select the IP address provided by the DHCP server.

DHCP server confirmation phase:

After the DHCP server receives the DHCP request sent by the DHCP client and confirms the IP address to be provided for the DHCP client, it wants the DHCP client to respond to a message containing the IP address and other options to tell the DHCP client that the IP address can be used.Then the DHCP client can bind the IP address to the network card.In addition, other DHCP servers will withdraw the IP address they previously provided for the DHCP client.

DHCP client logs back into the network:

After the DHCP client logs in again, it sends a DHCP request message containing the IP address information previously assigned by the DHCP server. When the DHCP server receives the request, it will try to let the DHCP client continue to use the IP address.And answer an ACK message.

However, if the IP address cannot be assigned to the DHCP client again, DHCP will reply to a NAK message. When the DHCP client receives the NAK message, it will resend the DHCP discovery message to obtain the IP address again.

DHCP client update lease:

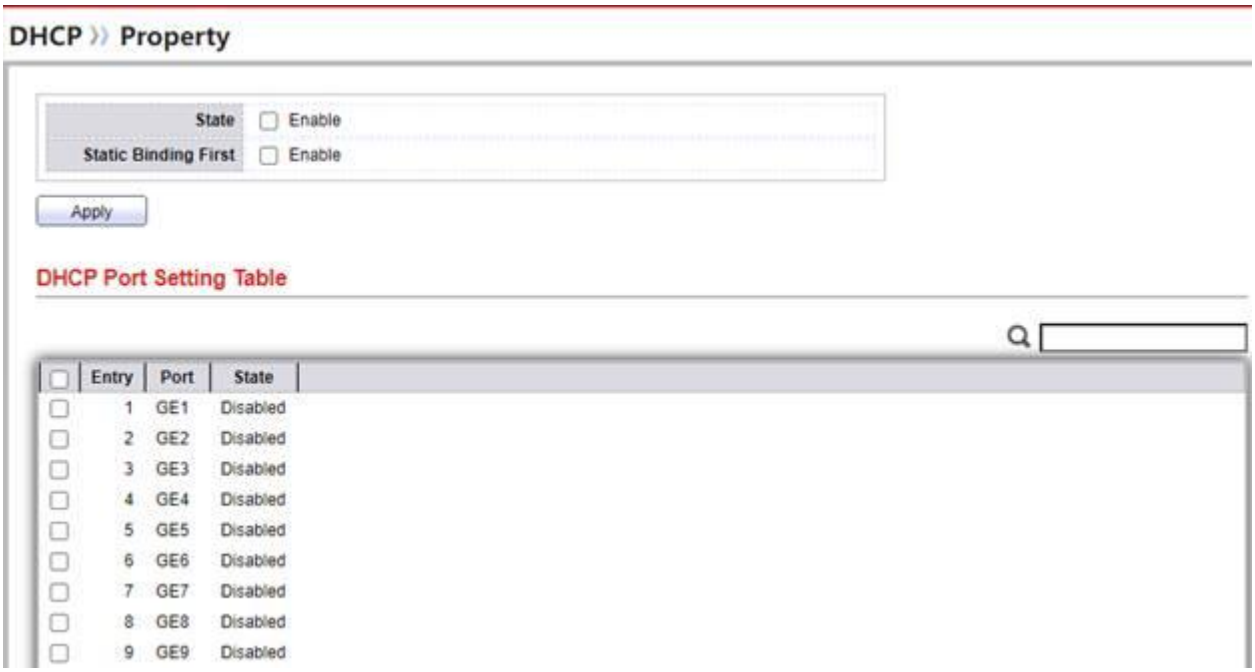
All IP addresses obtained by DHCP have a lease. After the lease expires, the DHCP server will reclaim the IP address. Therefore, if the DHCP client wants to continue to use the IP address, it must update the lease.The update method is that when the current

lease term is half past, the DHCP client will send DHCP renew message to renew the lease term.

9.2.4 Global settings

Configuration steps

1. Select [property / DHCP] in the navigation bar to enter the DHCP setting interface, as shown below:



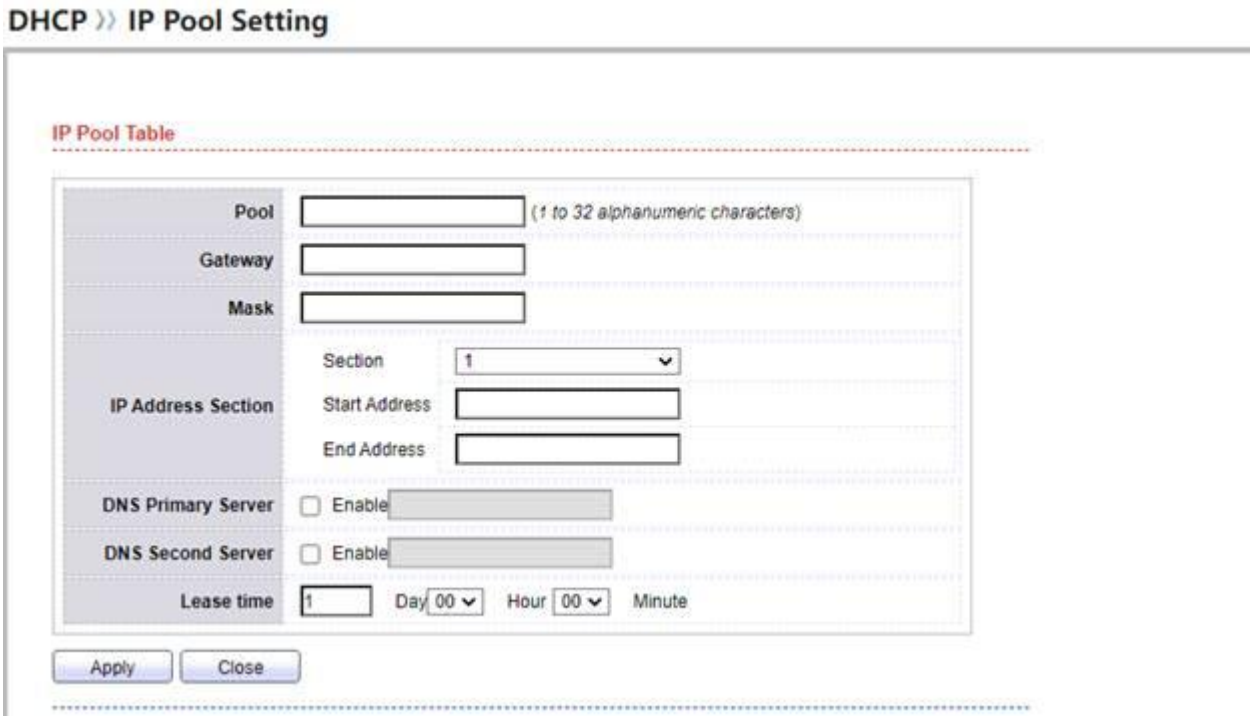
This interface is the main switch interface of DHCP, which is divided into global switch and port switch.When in use, the port also needs to be opened.

9.2.4 Address pool configuration

Configuration steps

1. Select [IP pool setting / DHCP] in the navigation bar to enter the DHCP address pool setting interface, as shown in the following figure:

click Add Button to add DHCP address pool, as shown in the following figure:



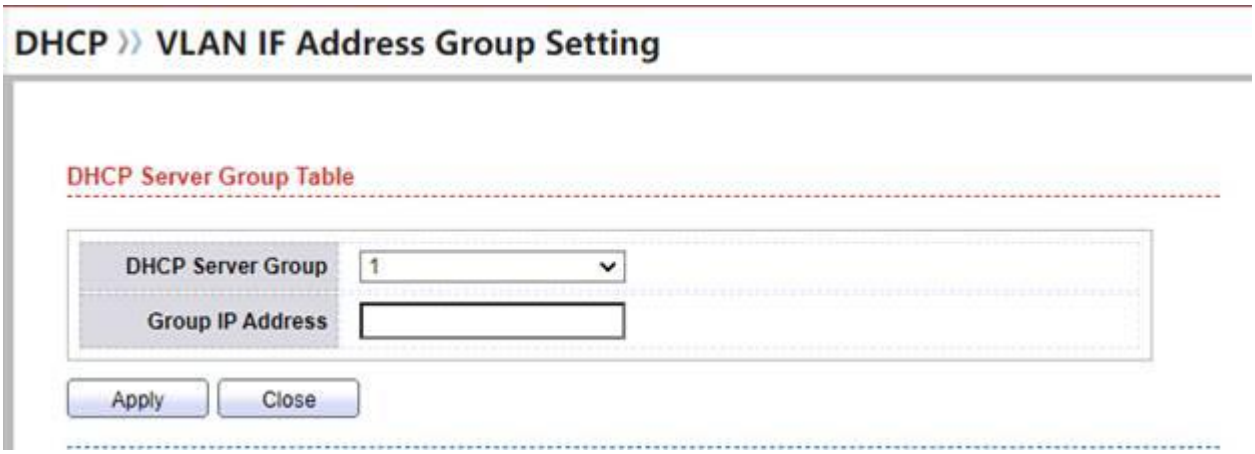
9.2.4 VLAN interface address group configuration

Configuration steps

1.Select [VLAN if address group setting / DHCP] in the navigation bar to enter the VLAN interface address group setting interface, as shown in the following figure:

The red box position is bound to the VLAN interface and DCHP server group.

click Add Click to add DCHP server group, as shown in the following figure:



Chapter 10 Multicast management

10.1 Multicast overview

10.1.1 Generation background

There are two traditional ways of IP communication: one is point-to-point communication between the source host and the destination host, that is, unicast;The other is point to multipoint communication between the source host and all other hosts in the same network segment, that is, broadcasting.If the information is to be sent to multiple hosts instead of all hosts, if it is realized by broadcasting, it will not only send the information to unnecessary hosts and waste bandwidth, but also can not realize cross network segment transmission;If unicast is adopted, repeated IP packets will not only occupy a lot of

bandwidth, but also increase the load of the source host.Therefore, the traditional unicast and broadcast communication methods can not effectively solve the problems of single point transmission and multi-point reception.

Multicast refers to sending data packets to a certain set of nodes (i.e. multicast group) in the form of best effort transmission in IP network. Its basic idea is that the source host (i.e. multicast source) sends only one data, and its destination address is the multicast group address;All receivers in the multicast group can receive the same data copy, and only the host in the multicast group can receive the data, while other hosts cannot.

10.1.2 Technical advantages

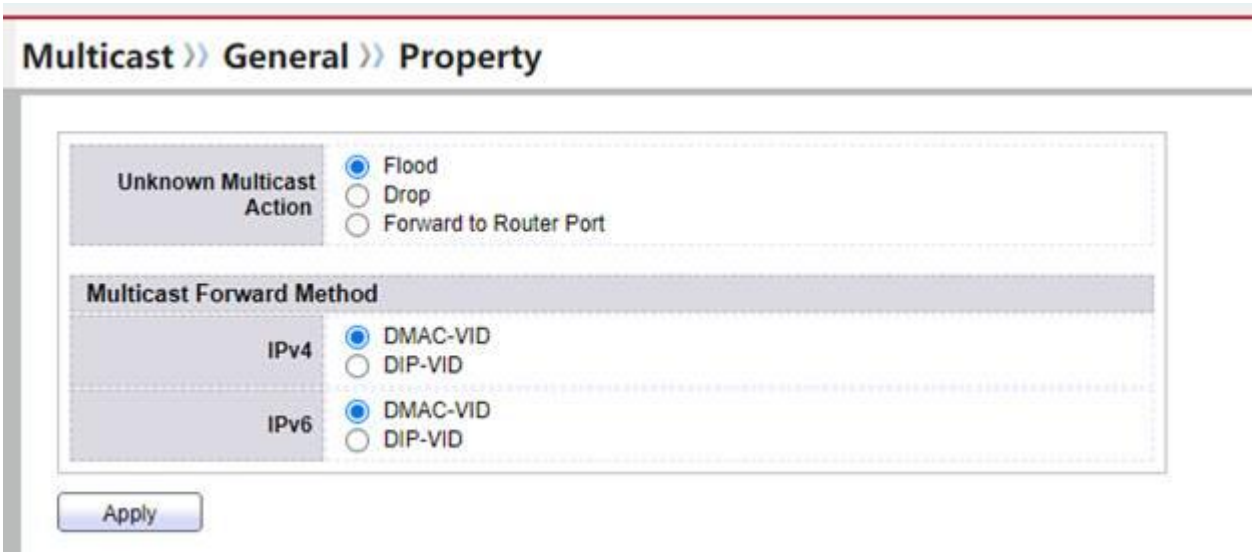
Multicast technology effectively solves the problems of single point sending and multi-point receiving, realizes the efficient data transmission from point to multi-point in IP network, and can greatly save network bandwidth and reduce network load.As a communication mode parallel to unicast and broadcast, the significance of multicast lies not only in this.More importantly, the multicast feature of the network can be used to easily provide some new value-added services, including online live broadcasting, network television, distance education, telemedicine, network radio, real-time video conference and other Internet information services.

10.2 Multicast forwarding

10.2.1 Function configuration

Configuration steps

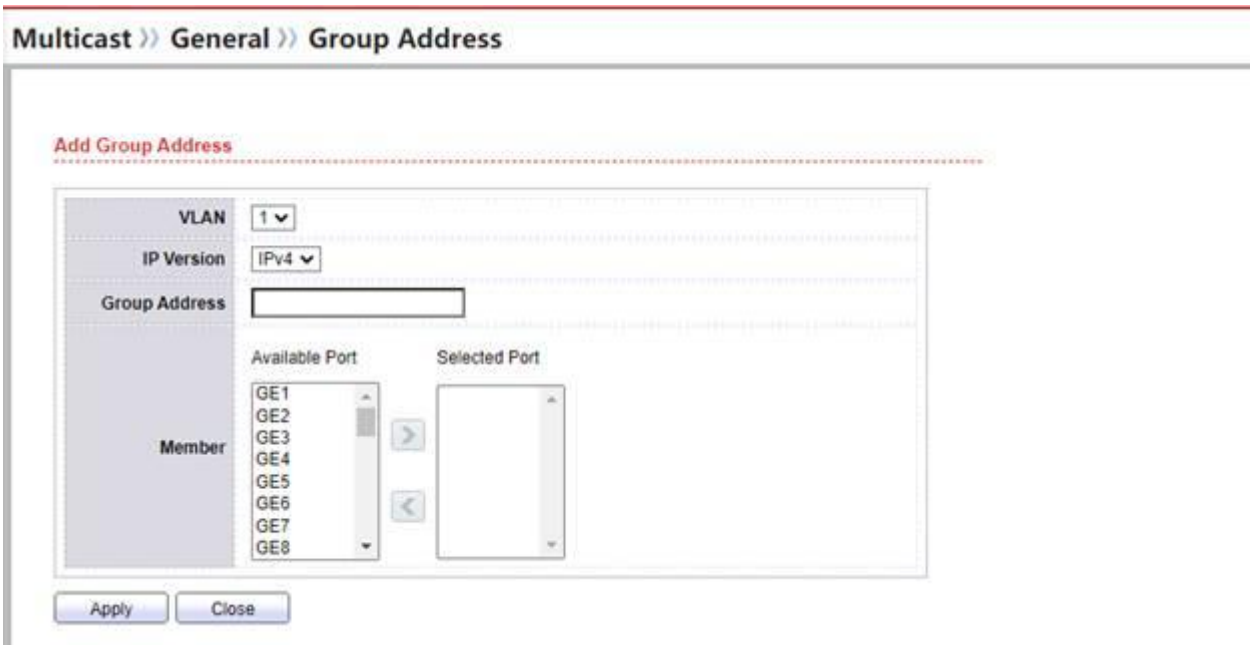
1. Select [property / general / multicast] in the navigation bar to enter the multicast setting interface, where you can select the multicast forwarding method, as shown in the following figure:



10.2.2 Static multicast group configuration

Configuration steps

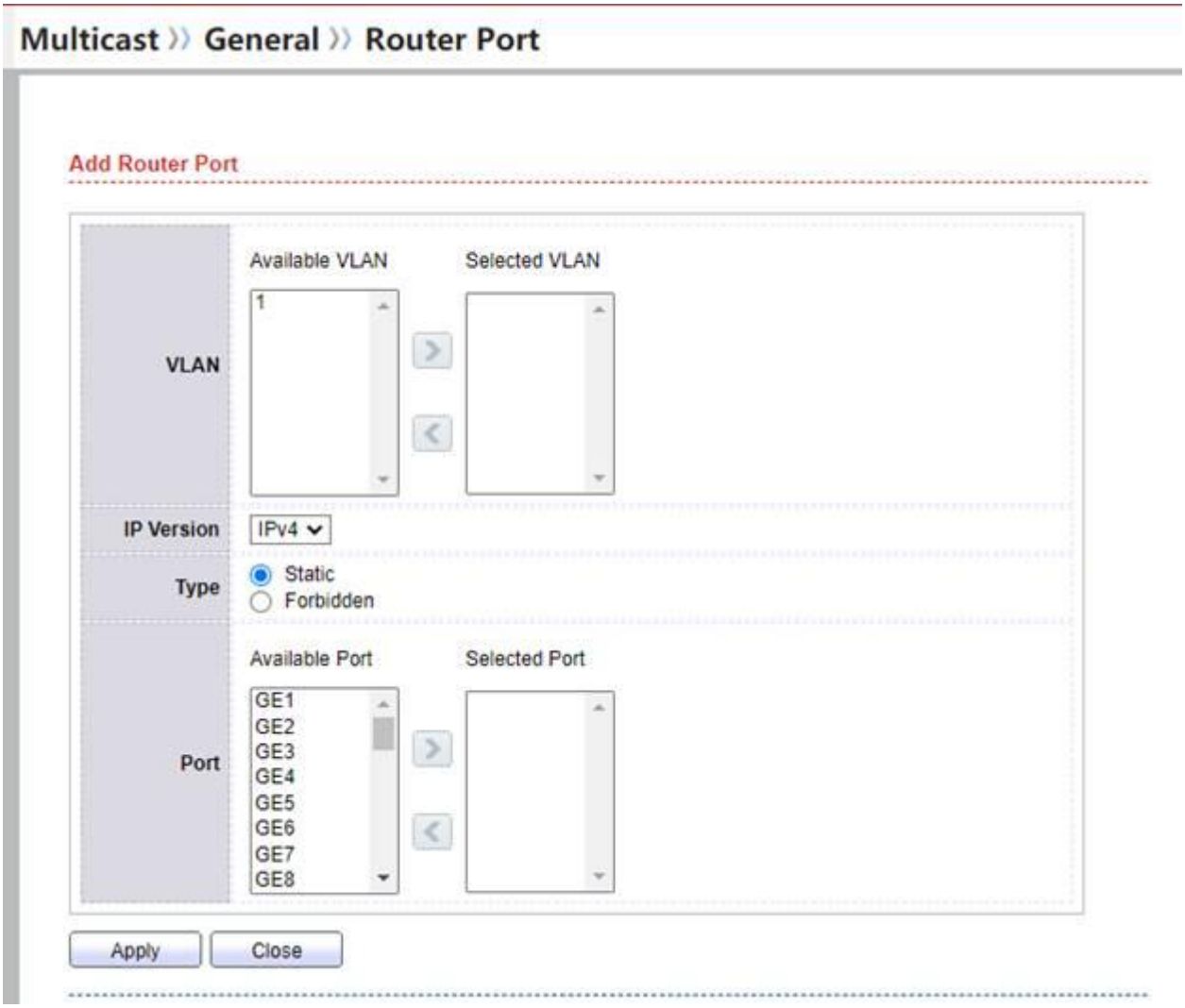
1.Select [group address / general / multicast] in the navigation bar. On this page, you can add or modify static multicast groups. Click Add Button to add. If you need to modify, you need to select the option to be modified and click Edit Button, as shown below:



10.2.3 Routing port configuration

Configuration steps

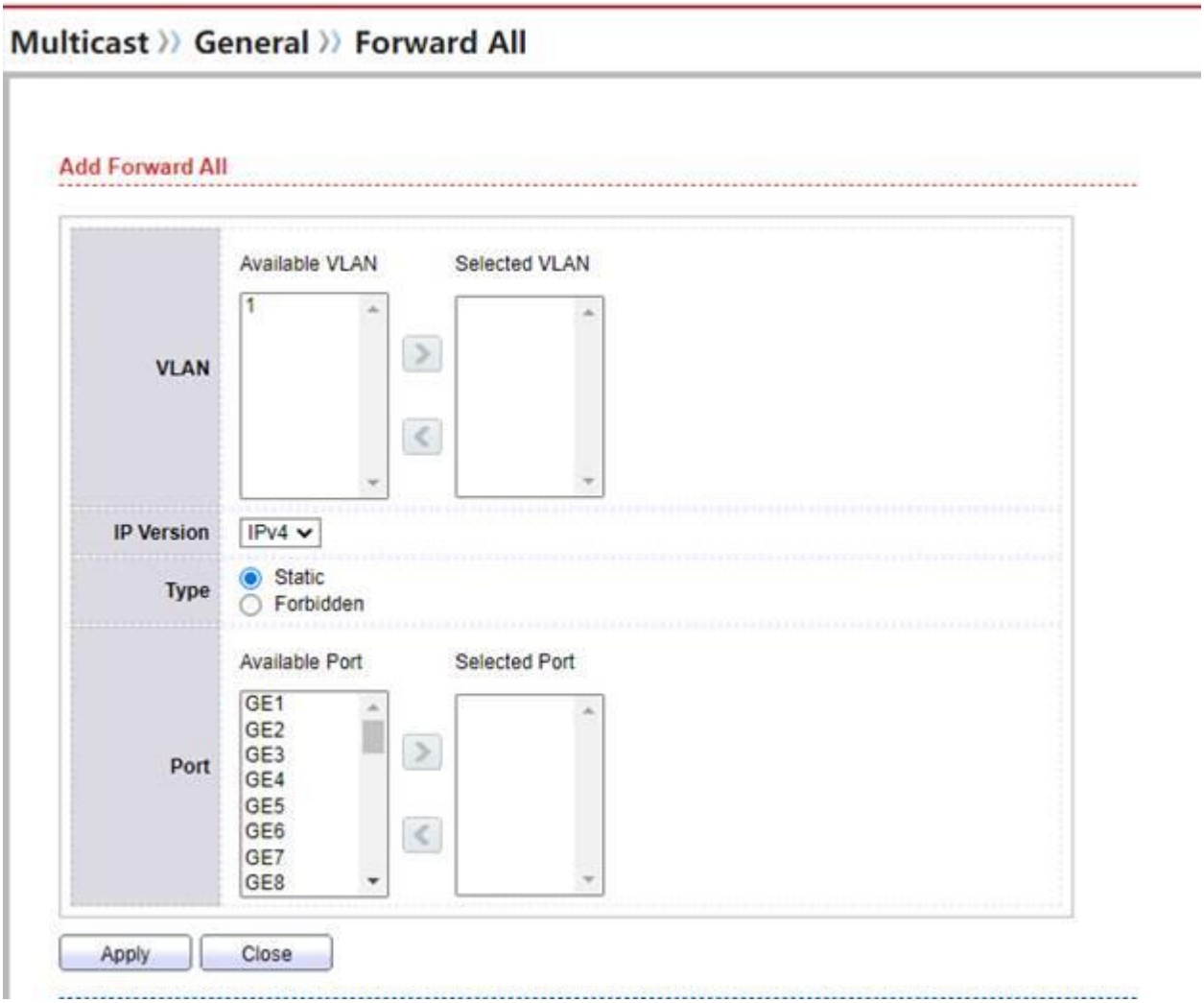
1.Select [route port / general / multicast] in the navigation bar. On this page, you can configure the route port and click Add Button to add. If you need to modify, you need to select the option to be modified and click Edit Button, as shown below:



10.2.4 Forwarding port configuration

Configuration steps

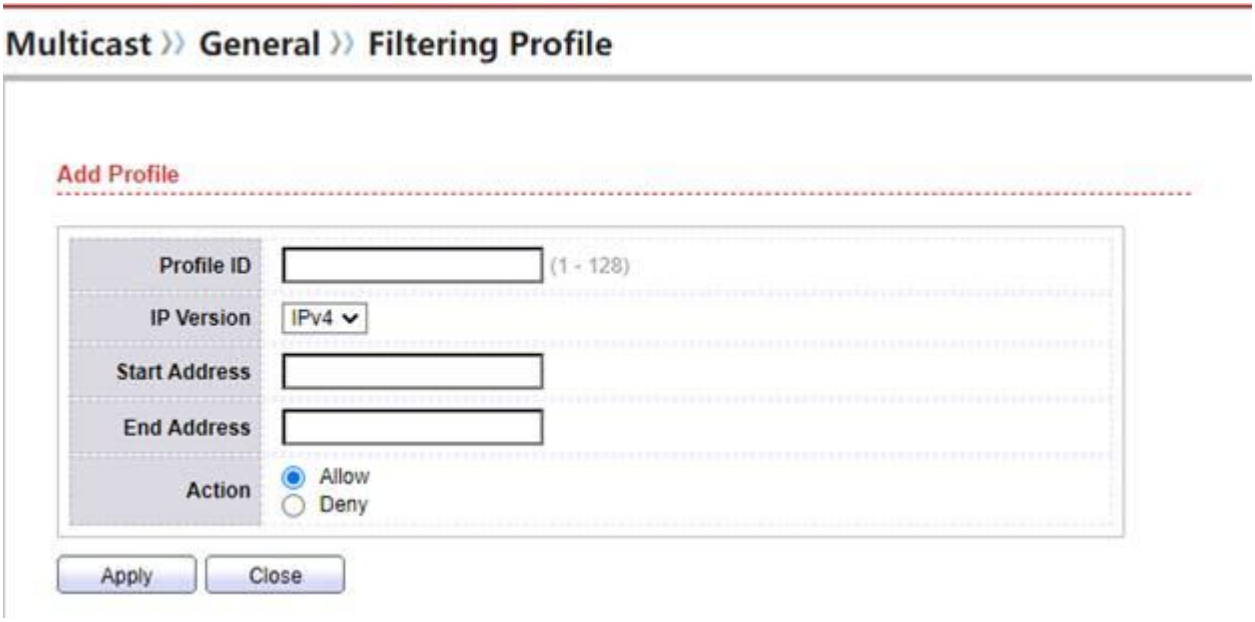
1.Select [forward all / general / multicast] in the navigation bar, and the forwarding port can be configured on this page. Click Add Button to add. If you need to modify, you need to select the option to be modified and click Edit Button, as shown below:



10.2.5 Multicast filtering rule configuration

Configuration steps

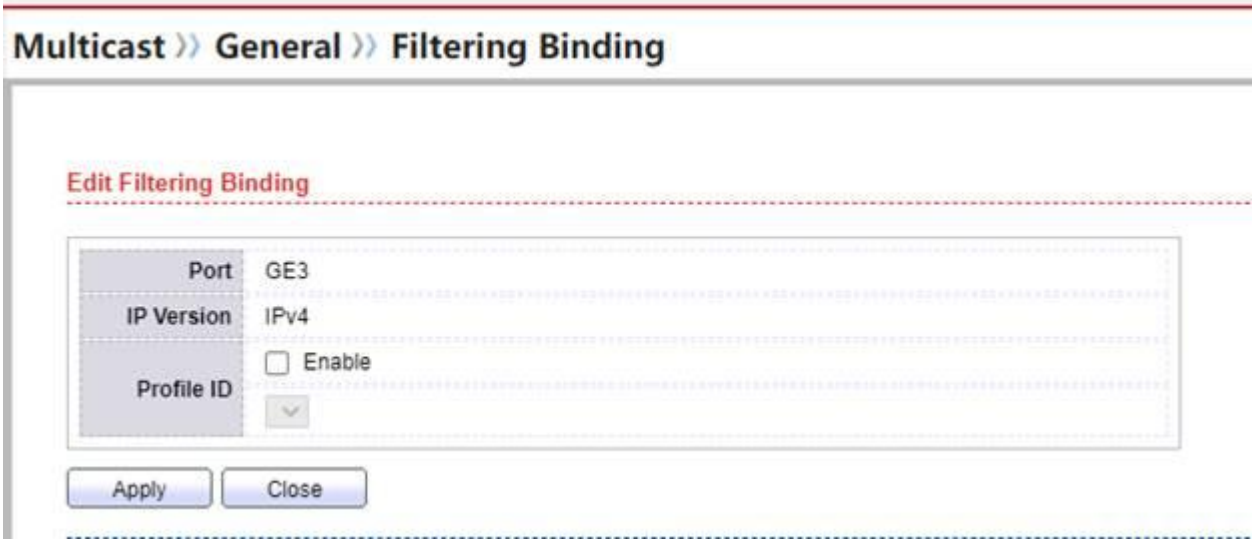
1.Select [filtering profile / general / multicast] in the navigation bar to enter the multicast filtering rule setting interface, where you can set multicast filtering rules. Click Add Button to add. If you need to modify, you need to select the option to be modified and click Edit Button, as shown below:



Note: After setting filtering rules, you need to bind ports to take effect.

Binding port configuration steps

1. Select [filtering binding / general / multicast] in the navigation bar to enter the interface of binding multicast filtering rules to ports, select the port to be bound, and then click Edit Button, as shown below:



10.3 IGMP snooping

10.3.1 IGMP Snoopingintroduce

IGMP snooping is the abbreviation of Internet Group Management Protocol Snooping. It is a multicast constraint mechanism running on layer-2 devices, which is used to manage and control multicast groups.

10.3.2 IGMP SnoopingTechnical introduction

The layer-2 device running IGMP snooping establishes a mapping relationship between the port and MAC multicast address by analyzing the received IGMP message, and forwards multicast data according to this mapping relationship.When layer 2 equipment does not run IGMP snooping, multicast data is broadcast in layer 2;When the layer-2 device runs IGMP snooping, the multicast data of the known multicast group will not be broadcast in layer-2, but will be multicast to the designated receiver in layer-2.

IGMP snooping is the same as IGMP protocol. Both are used for multicast group management and control. They both use IGMP packets.IGMP protocol runs in the network layer, while IGMP snooping runs in the link layer. When the layer-2 Ethernet switch receives the IGMP message transmitted between the host and the router, IGMP snooping analyzes the information carried by the IGMP message, establishes and maintains the MAC table in layer-2, and then forwards the multicast message sent from the router according to the MAC table.IGMP snooping will actively send IGMP specific group query messages to the port only when it receives the IGMP leaving message of a port or the aging time timer of a port times out. In addition, it will not send any IGMP messages to the port.

IGMP snooping is to monitor IGMP protocol packets, extract corresponding information, form a multicast membership table, and then forward multicast services according to group membership to ensure that group members receive correct multicast services, while other hosts cannot.

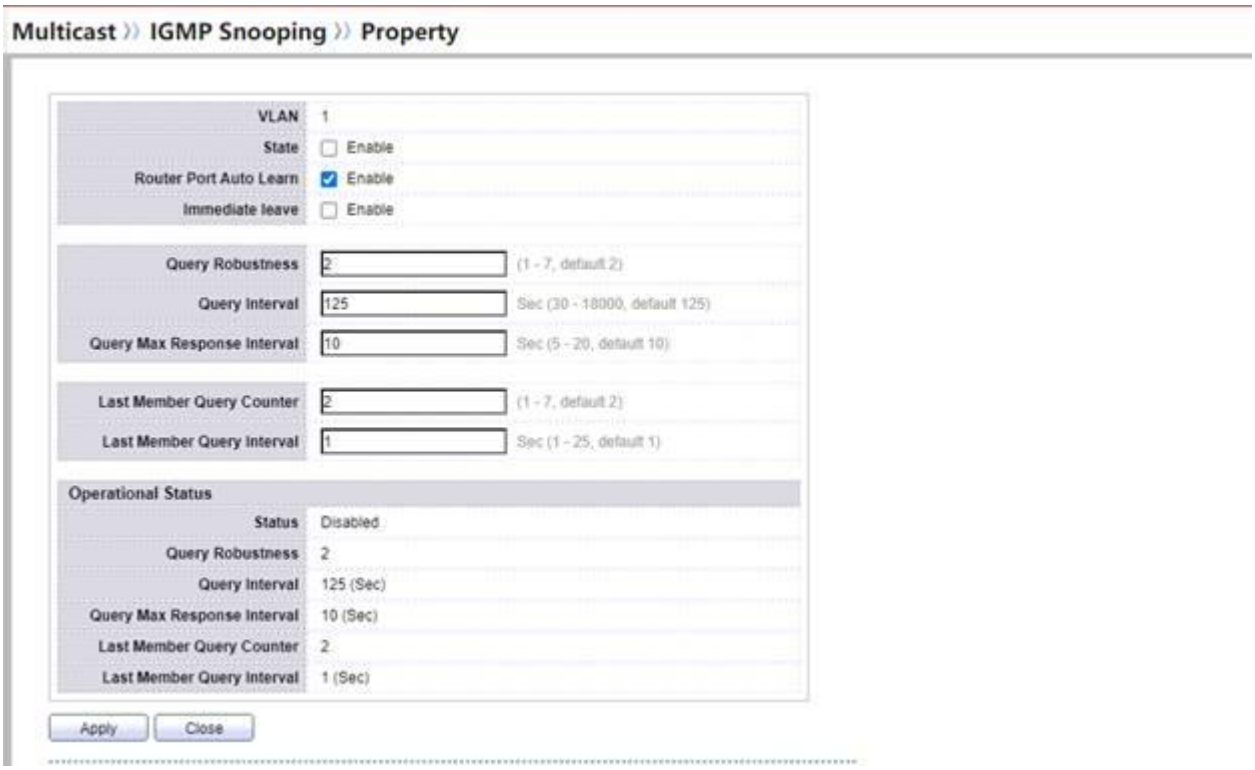
IGMP snooping is transparent to routers and hosts. It only listens to IGMP messages between them to establish its own multicast membership table.

10.3.3 Global settings

Configuration steps

1. Select [property / IGMP snooping / multicast] in the navigation bar to enter the IGMP snooping setting interface. In the IGMP snooping [global setting] interface, you can view the global configuration information of IGMP snooping, as shown in the following figure:

To modify the global configuration of IGMP snooping, check the configuration to be modified and click Edit Button, as shown below:



Configuration item description

Configuration item	explain
VLAN	Multicast VLAN
State	Status, on or off
Route Port Auto Learn	Routing port learning, on or off
Immediate leave	Quickly leave, open or close
Query Robustness	Query times, range ＜ 1-7 ＞, default to 2 times
Query Interval	Query interval, range ＜ 30-18000 ＞, default 125 seconds
Query Max Response Interval	Maximum query response time, range < 5-20 >, default 10 seconds
Last Member Query Counter	Query times of specific group, range < 1-7 >, default 2 times
Last Member Query Interval	Specific group query interval, range < 1-25 >, default 1 second

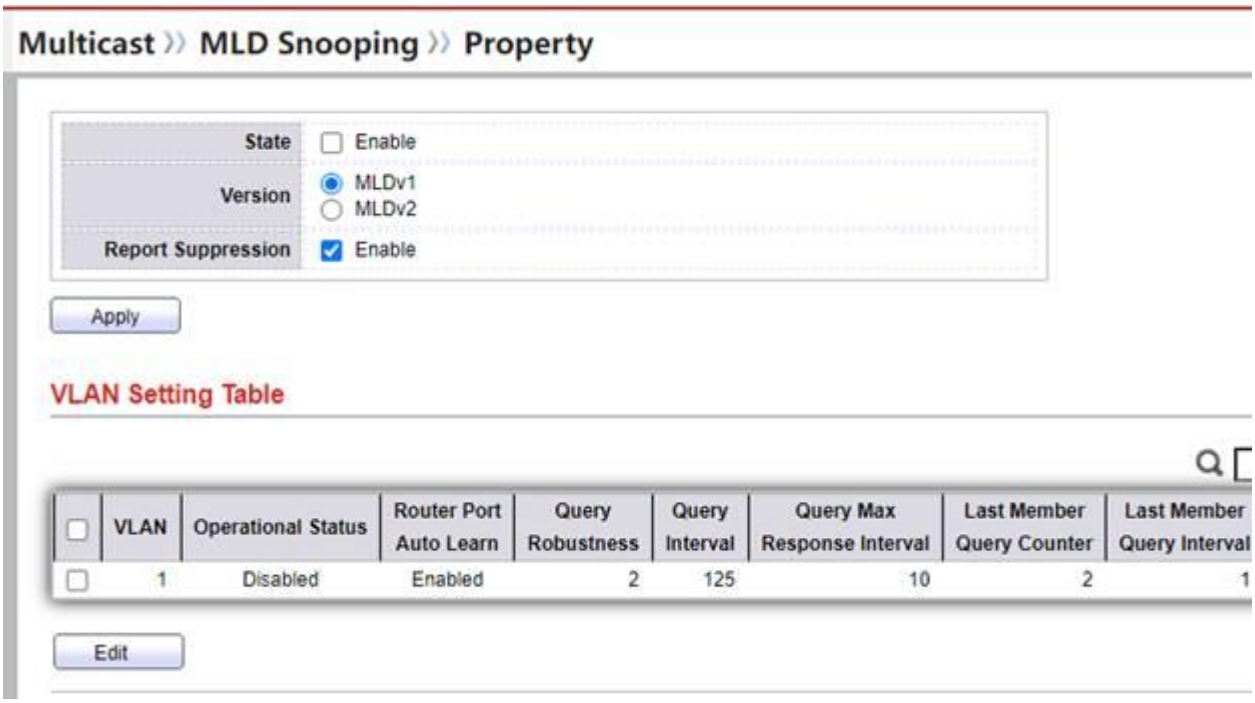
10.4 MLD Snooping

The layer-2 device running MLD snooping establishes a mapping relationship between the port and MAC by analyzing the received MLD, and forwards IPv6 data according to this mapping relationship. When the layer-2 device does not run MLD snooping, IPv6 multicast data is broadcast in layer-2;When the layer 2 device runs MLD snooping, it is known that the multicast data message of IPv6 Multicast Group will not be

broadcast in layer 2, but will be multicast to the designated receiver in layer 2.These benefits can be brought by forwarding the information only to the recipients in need through layer 2: reducing the broadcasting in layer 2 network and saving;Enhance the security of IPv6 information;It brings convenience to realize the separate billing of each machine.Message multicast address multicast message MLD snooping multicast message network bandwidth multicast host

Configuration steps

1. Select [property / MLD snooping / multicast] in the navigation bar to enter the MLD snooping setting interface, as shown below:



10.5 MVR（IGMP）

IGMP runs between the host and the router directly connected to the host, and its functions are bidirectional: on the one hand, the host notifies the router through IGMP that it wants to receive the information of a specific multicast group;On the other hand, the router periodically queries whether the multicast group members in the LAN are active through IGMP, so as to collect and maintain the group membership relationship of the connected network segments.Through IGMP, the information recorded in the router is

whether a multicast group has local group members, rather than the corresponding relationship between the multicast group and the host.

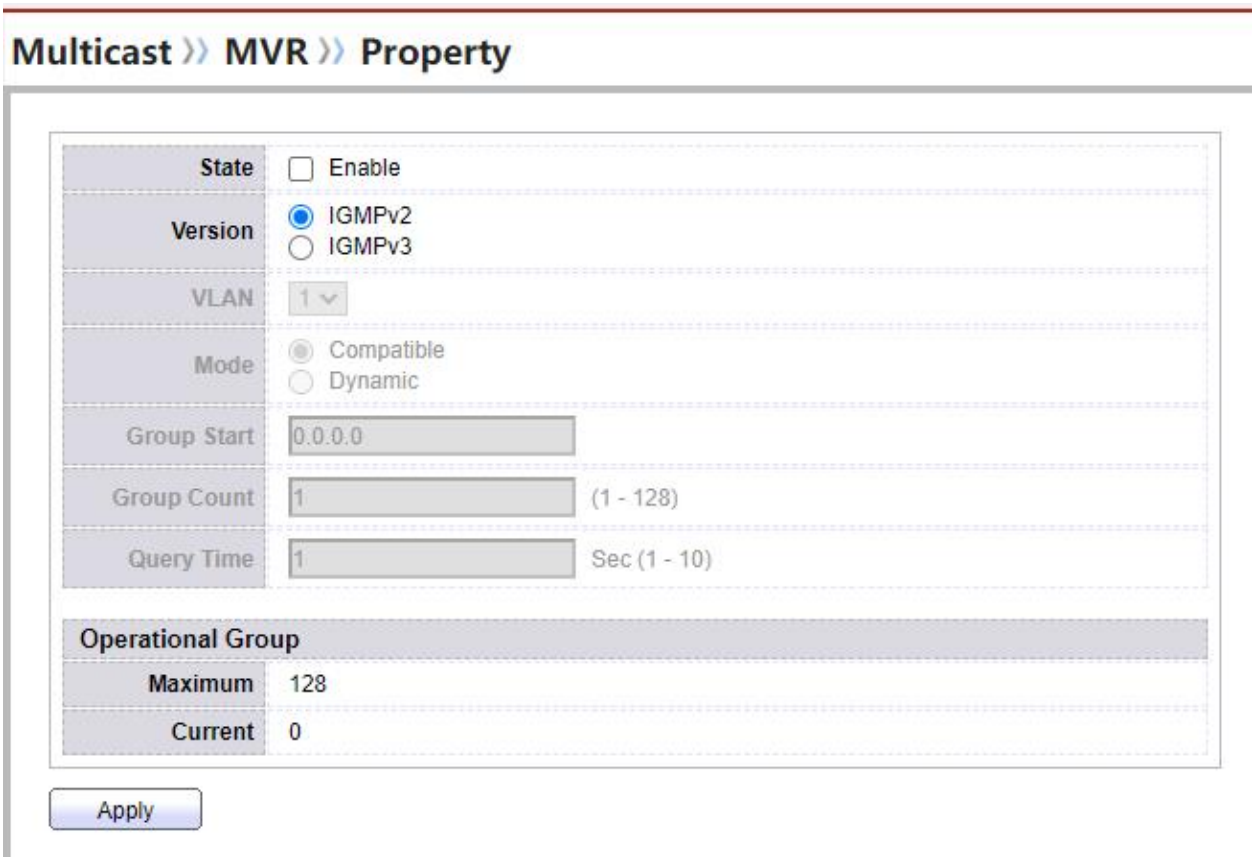
So far, IGMP has three versions: igmpv1, igmpv2 and igmpv3.Igmpv1 defines the basic reporting process of group member query. On this basis, igmpv2 adds the mechanism of querier election and group member departure. The main function added in igmpv3 is that members can specify to receive or not receive messages from some multicast sources.

The comparison of the three versions of IGMP is shown in the following table:

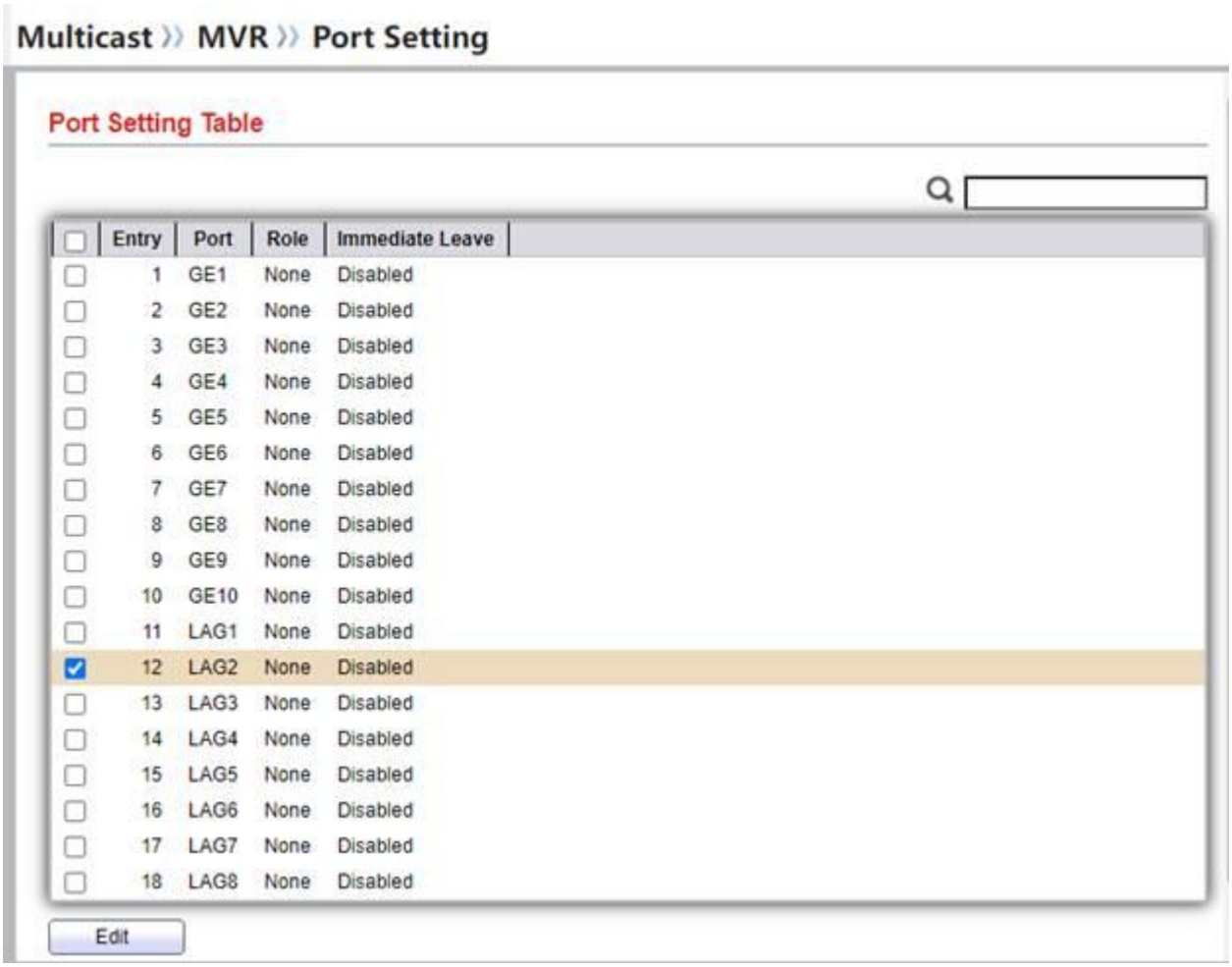
project	IGMPv1	IGMPv2	IGMPv3
Query election method	PIM election based on Multicast Routing Protocol	Competitive election between multicast routers in the same network segment	Competitive election between multicast routers in the same network segment
Universal group query message	support	support	support
Member report message	support	support	support
Specific group query message	I won't support it	support	support
Member leaving message	I won't support it	support	There is no special member leaving message defined, and member leaving is conveyed through a specific type of report message
Specific source group query message	I won't support it	I won't support it	support
Specify multicast source	I won't support it	I won't support it	support
Identifiable message protocol version	IGMPv1	IGMPv1，IGMPv2	IGMPv1，IGMPv2，IGMPv3
ASM model	support	support	support
SSM model	IGMP SSM mapping technical support is	IGMP SSM mapping technical support is	support

	required	required	

1. Select [property / MVR / multicast] in the navigation bar to enter the IGMP setting interface, as shown in the following figure:



2. Select [port setting / MVR / multicast] in the navigation bar to enter the port setting interface, as shown in the following figure:



Chapter 11 Route

11.1 Routing overview

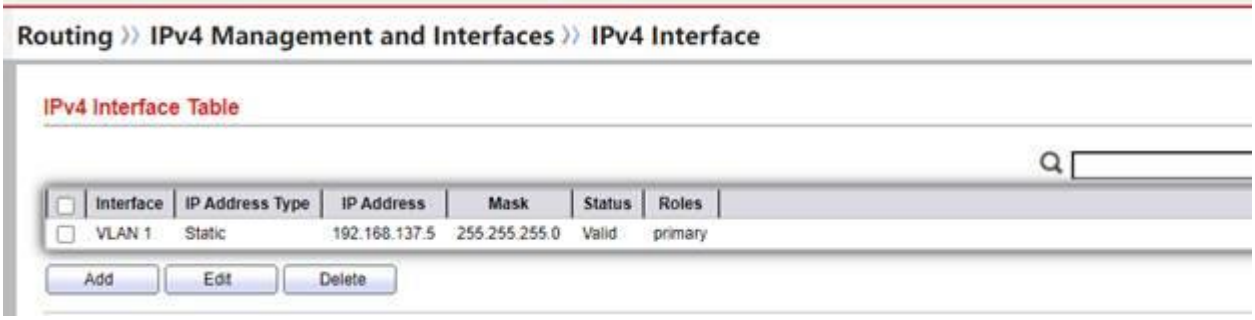
Routing refers to the process of receiving a packet from one interface, orienting it according to the purpose of the packet and forwarding it to another interface.Routing is usually compared with bridging. To the careless person, they seem to accomplish the same thing.Their main is that they occur in the second layer () and routing occurs in the third layer ().This makes them use different information in the process of transmitting information, so as to complete their tasks in different ways.Router packet address difference bridging OSI reference model data link layer network layer difference

11.2 IPv4 Management interface

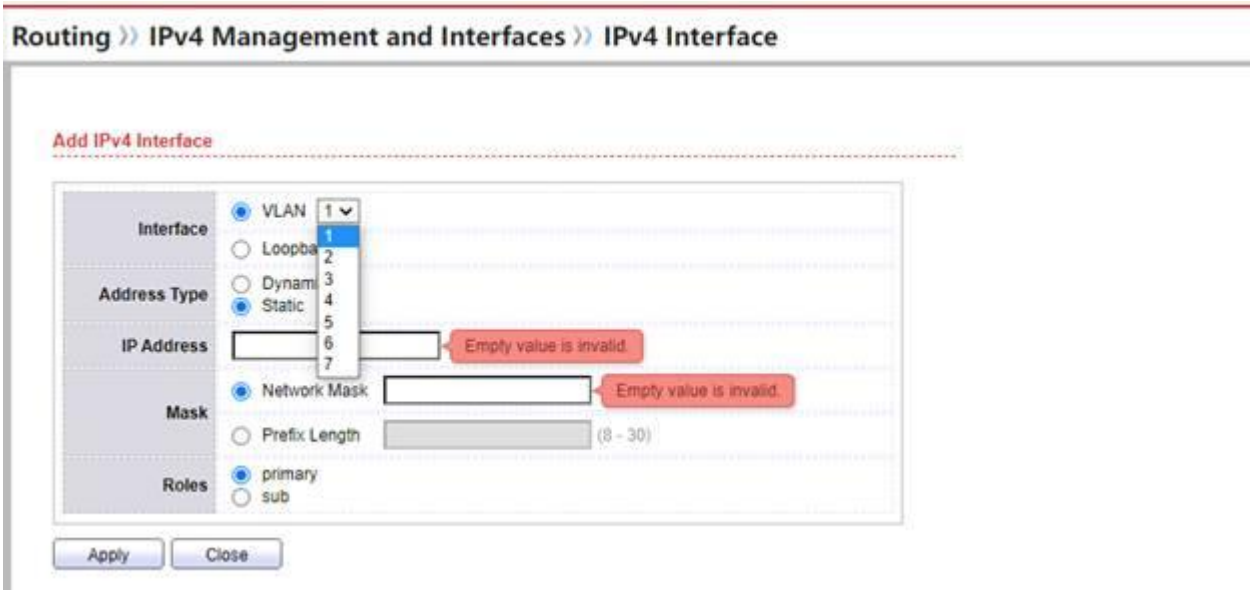
11.2.1 IPv4 interface

Configuration steps

1.Select [IPv4 interface / IPv4 / routing] in the navigation bar to enter the IPv4 interface setting interface, as shown in the following figure:



To add an IPv4 interface, click the button below Add Button to jump to the add interface page, as shown in the following figure:



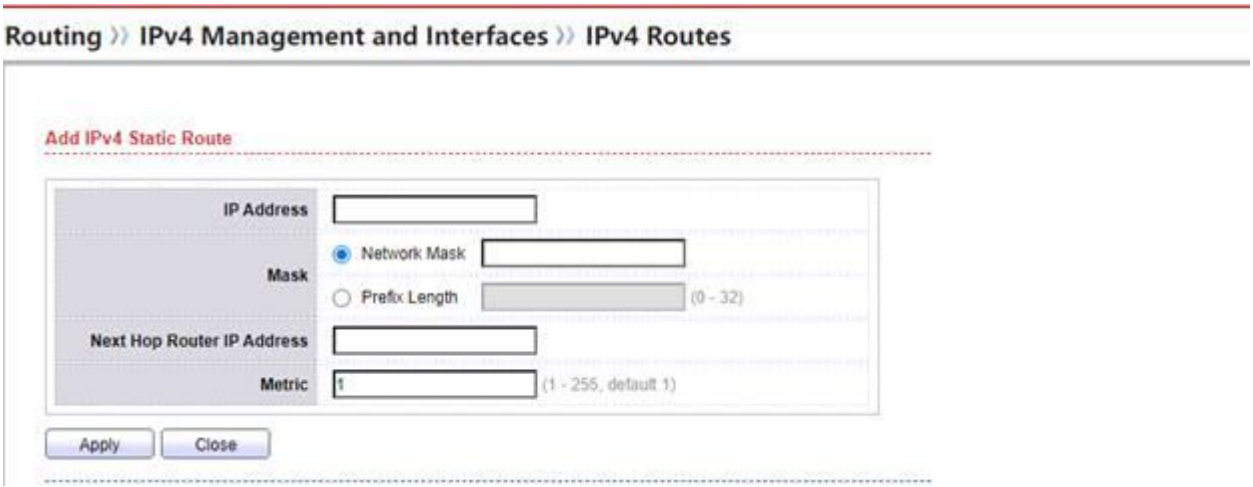
Note: the management interface of the corresponding VLAN must be created.A VLAN cannot create two interfaces, so if you need to modify the interface, select it and click Edit Just press the button.

11.2.2 IPv4 routing

Configuration steps

1.Select [IPv4 routes / IPv4 / routing] in the navigation bar to enter the IPv4 routing setting interface, as shown in the following figure:

To add an IPv4 route, click below Add Button to jump to the add interface page, as shown in the following figure:

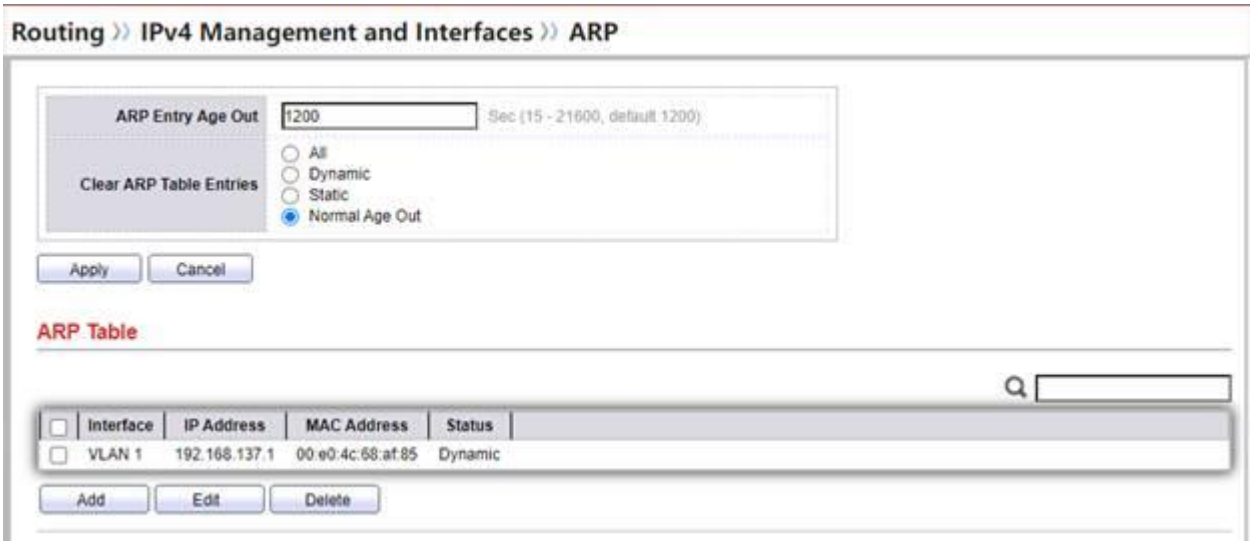


If you need to modify the route, select and click Edit Just press the button.

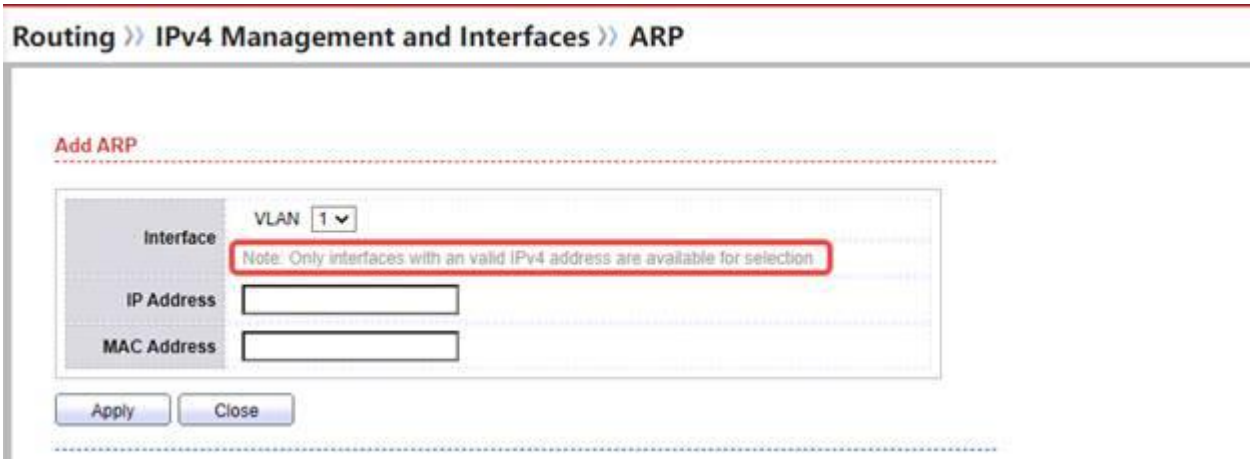
11.2.3 ARP

Configuration steps

1.Select [ARP / IPv4 / routing] in the navigation bar to enter the ARP setting interface, as shown in the following figure:



To add ARPTable item, click Add Button to jump to the add interface page, as shown in the following figure:

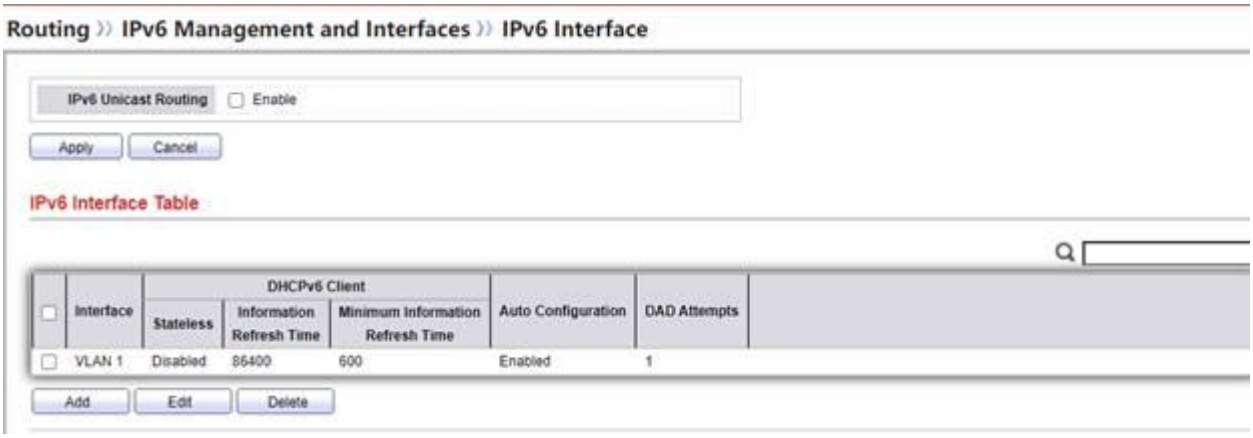


11.3 IPv6 Management interface

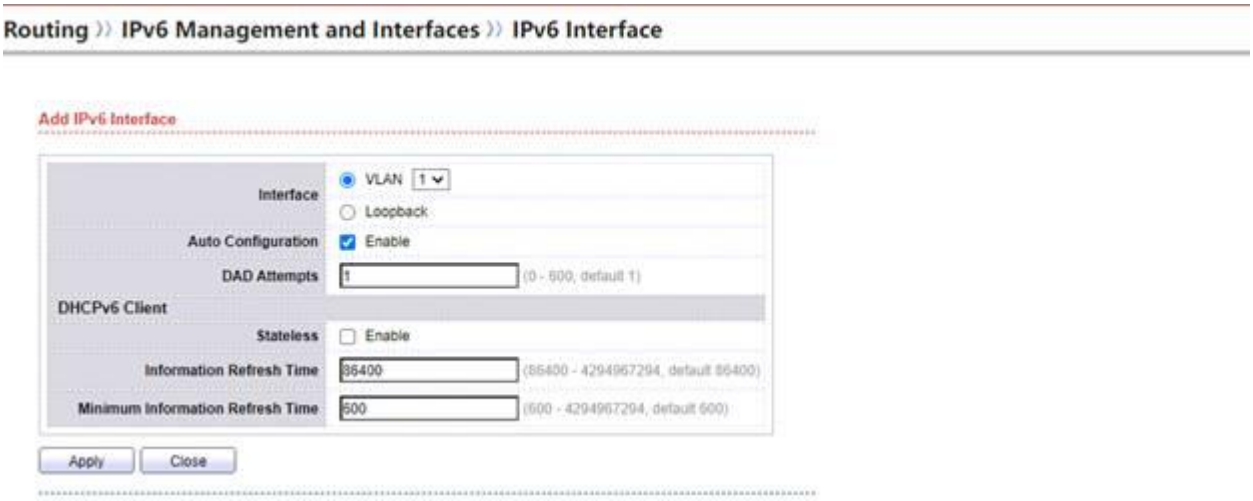
11.3.1 IPv6 interface

Configuration steps

1.Select [IPv6 interface / IPv6 / routing] in the navigation bar to enter the IPv6 interface setting interface, as shown in the following figure:



To add an IPv6 interface, click the button below Add Button to jump to the add interface page, as shown in the following figure:

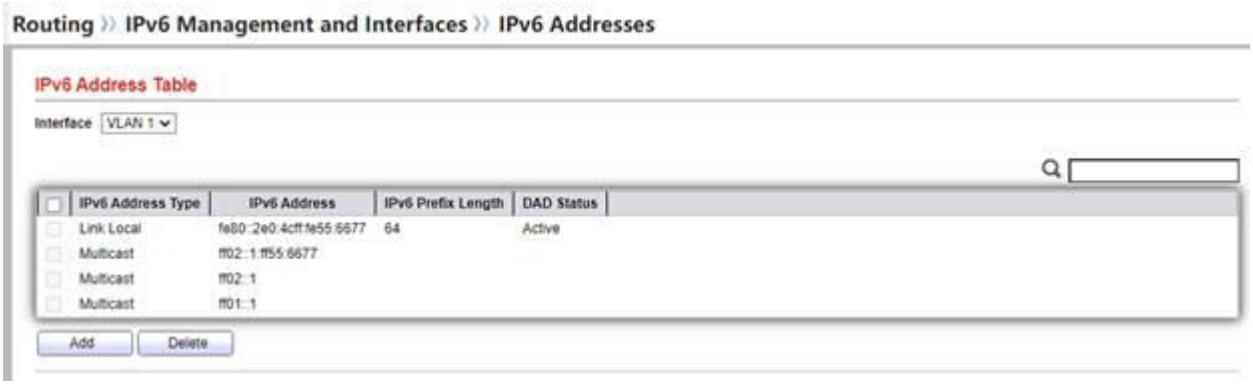


If you need to modify the IPv6 interface, select it and click Edit Just press the button.

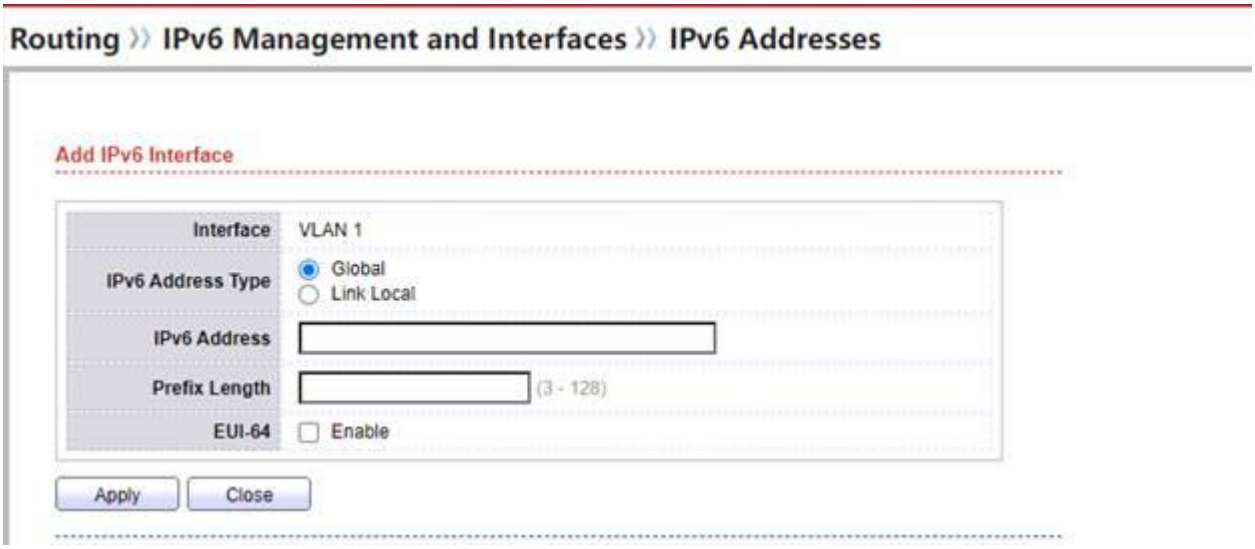
11.3.2 IPv6 address

Configuration steps

1.Select [IPv6 addresses / IPv6 / routing] in the navigation bar to enter the IPv6 address setting interface, as shown in the following figure:



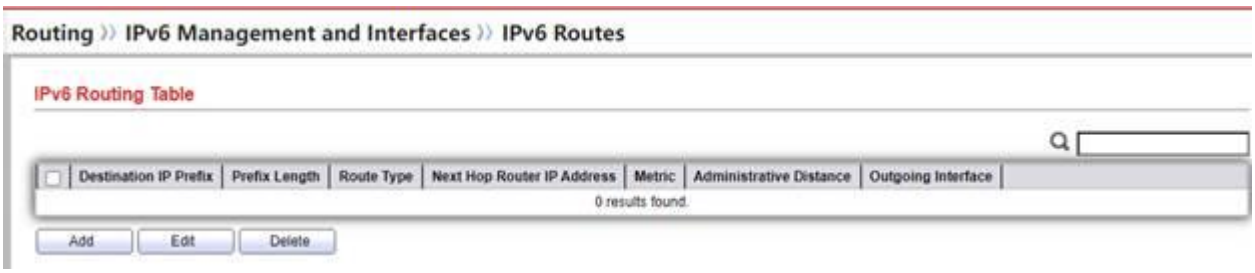
To add an IPv6 address, click below Add Button to jump to the page of adding IPv6 address, as shown in the following figure:



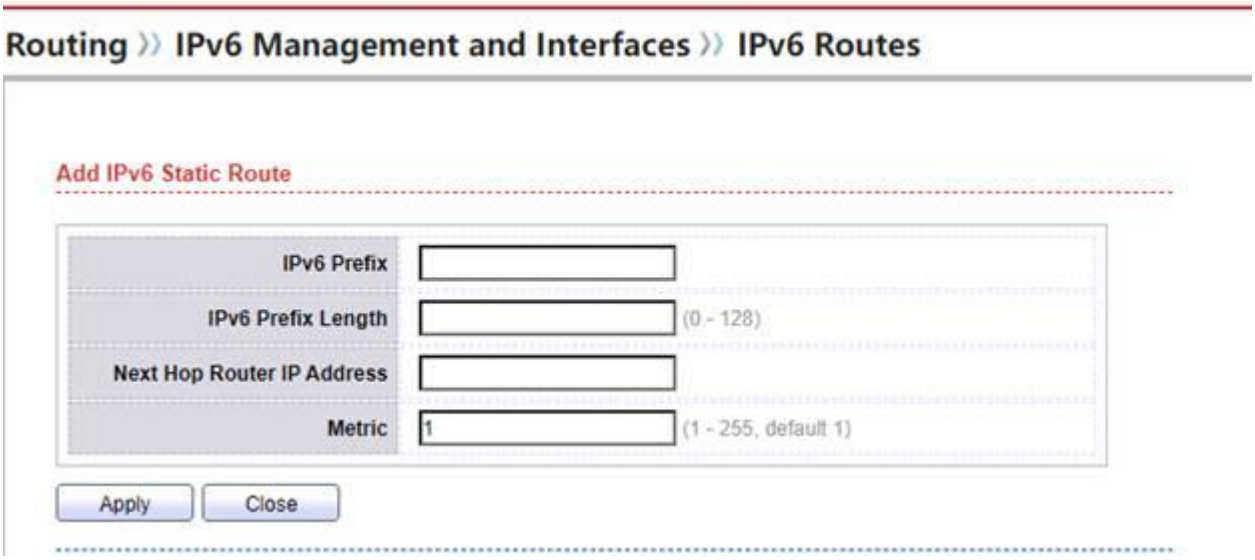
IPv6 Routing 11.3

Configuration steps

1.Select [IPv6 routes / IPv6 / routing] in the navigation bar to enter the IPv6 route setting interface, as shown in the following figure:



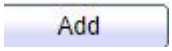
To add an IPv6 route, click below Add Button to jump to the add IPv6 route page, as shown in the following figure:



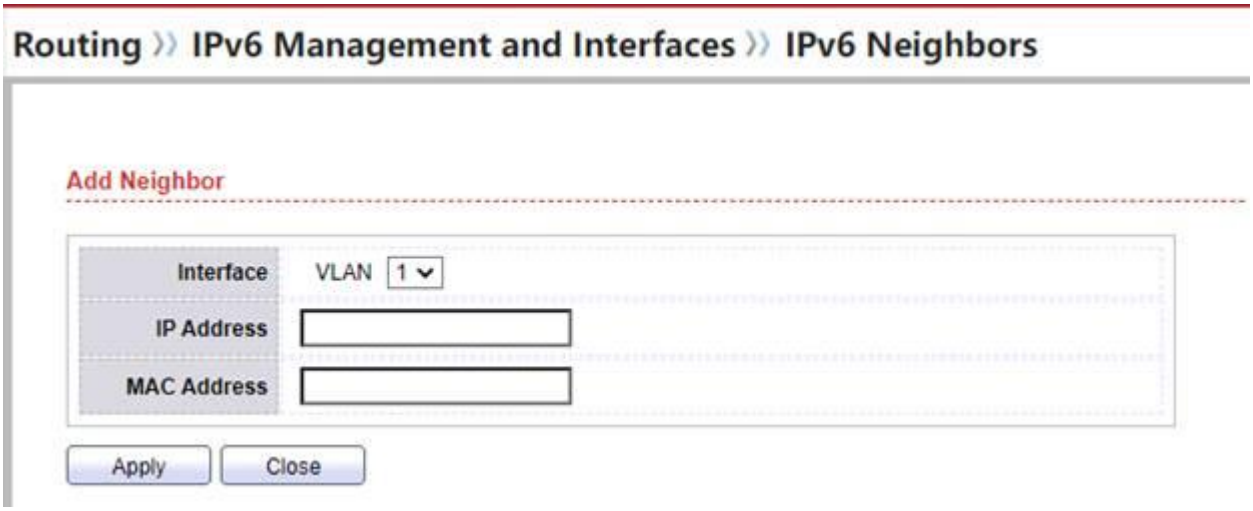
11.3.4 IPv6 neighbors

Configuration steps

1. Select [IPv6 neighbors / IPv6 / routing] in the navigation bar to enter the IPv6 Neighbor setting interface, as shown in the following figure:

To add IPv6 neighbors manually, click 

Button to jump to the page of adding IPv6 neighbors, as shown in the following figure:

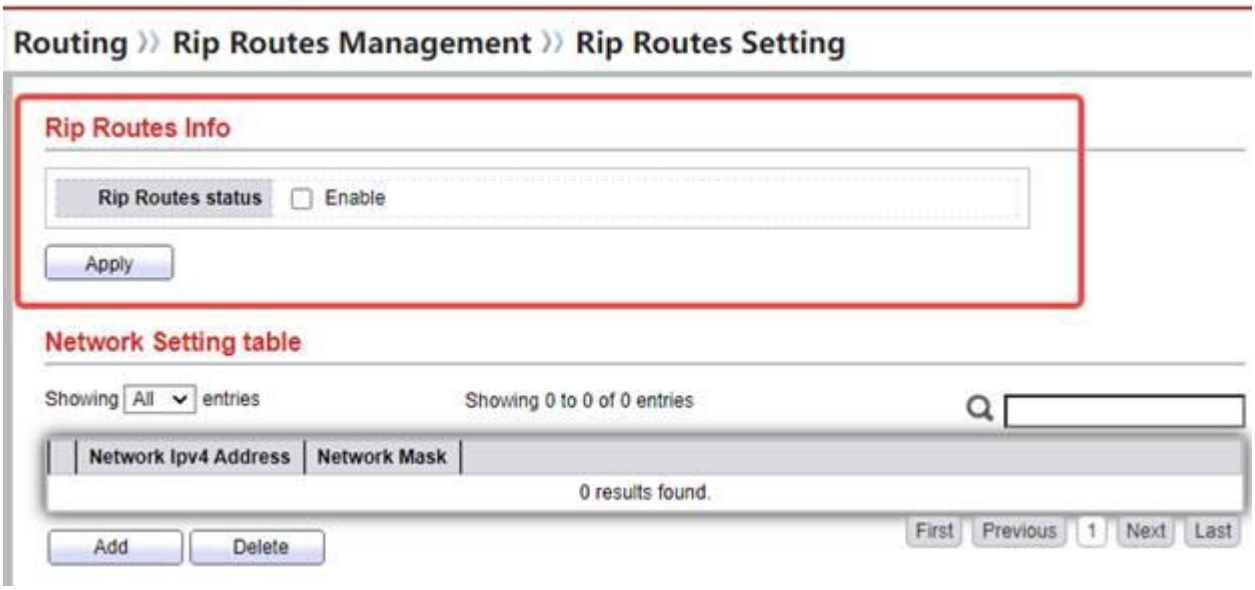


11.4 RIProute

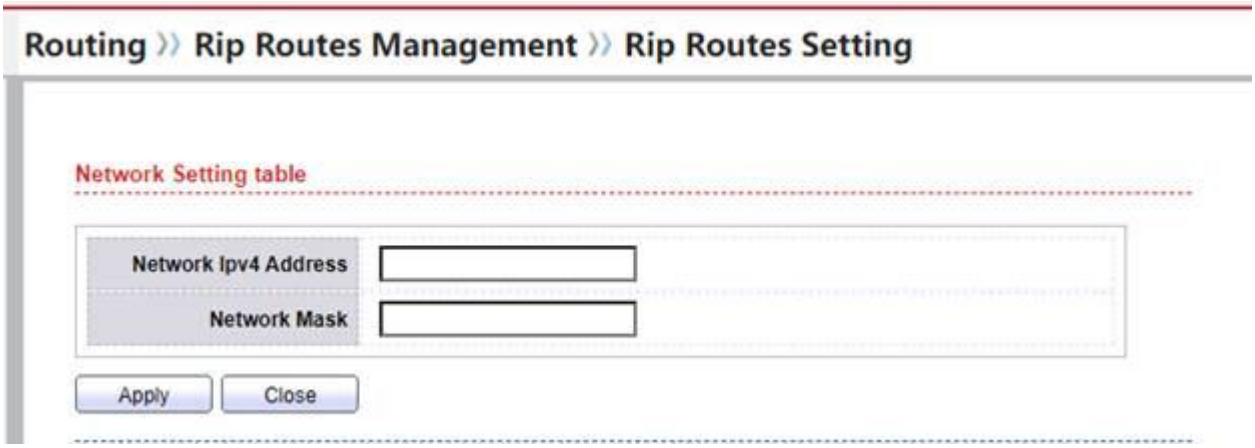
Rip is the abbreviation of routing information protocol. It is a relatively simple internal gateway protocol.Rip is a protocol based on distance vector algorithm. It uses hop count as a measure to measure the distance to the destination network.Rip exchanges routing information through UDP message, and the port number used is 520.

Configuration steps

1.Select [rip routes setting / rip / routing] in the navigation bar to enter the IPv6 Neighbor setting interface, as shown in the following figure:



The red box position in the figure above is the rip enable position. To add rip route, click Add Click to enter the add page, as shown in the following figure:



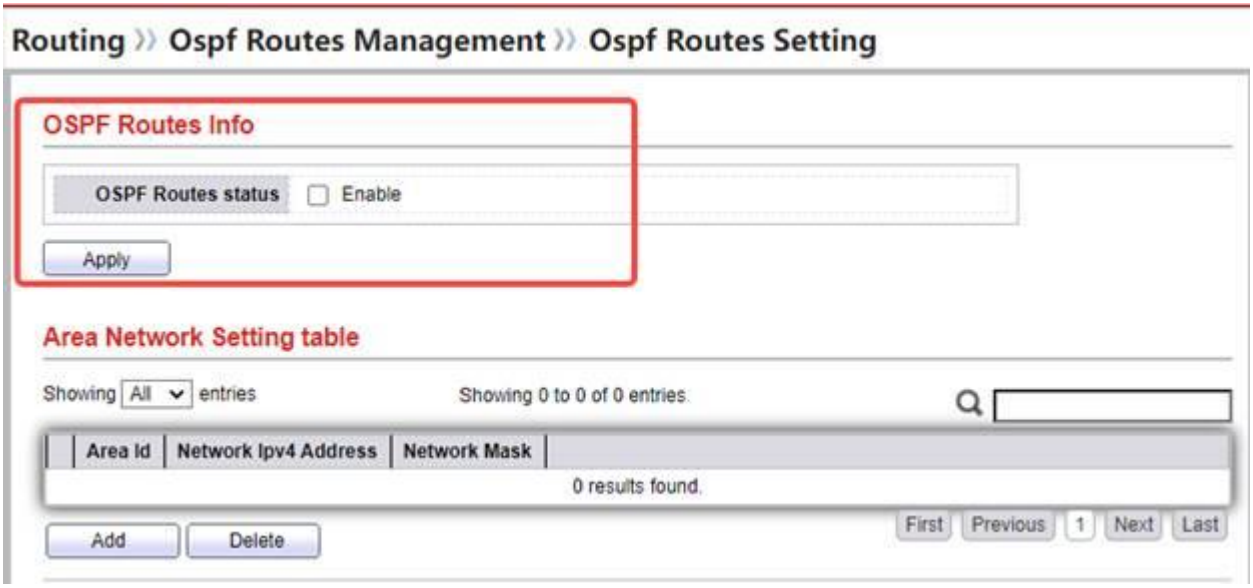
11.5 OSPFroute

Open shortest path first (OSPF) is an internal gateway protocol based on link state developed by IETF.The following table shows the comparison between rip and OSPF:

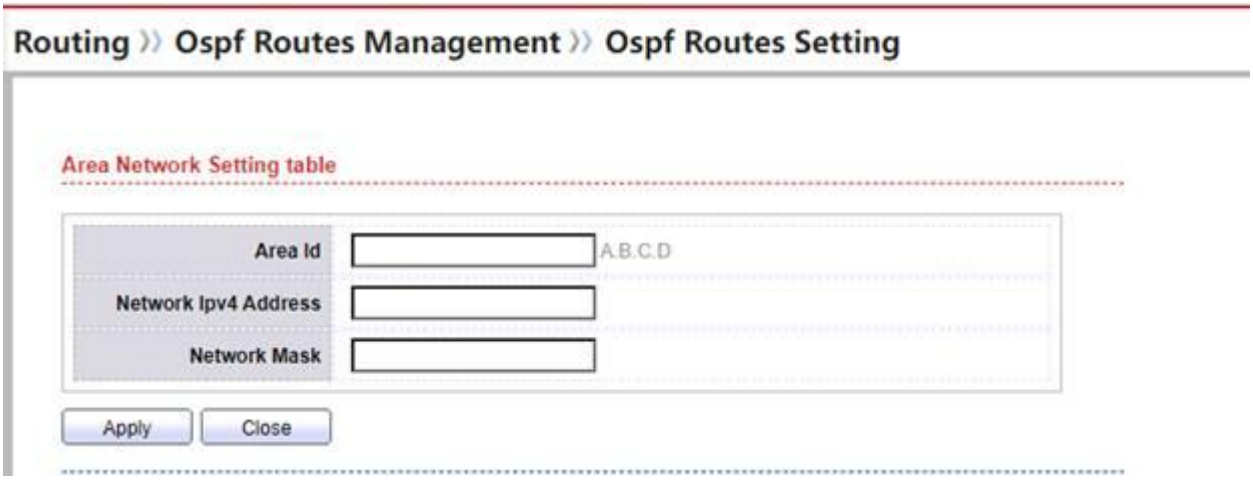
RIP	OSPF
Based on the distance vector algorithm, the number of hops is used as a measure to ignore the impact of bandwidth	Based on the link state, the link overhead is taken as the measurement method, and the bandwidth is taken as the reference value, so the measurement method is more scientific
The number of hops of RIP is limited to 15, which limits the network scale of rip	There is no hop limit, and the applicable network scale is larger
The router updates and selects the route according to the route announcement. The router does not understand the whole network topology and is prone to generate a routing loop.	Each router can master the topology of the whole network and calculate the route through the shortest path first algorithm SPF (shortest path first), without generating a routing loop
The convergence speed is slow, and the route update will experience a period of suppression and garbage collection, which is easy to lead to inconsistent routes between routers	The convergence speed is fast, because the route update is timely and can be quickly transmitted to the whole network
Variable length subnet mask (VLSM) cannot be processed	It can handle VLSM and allocate IP addresses flexibly

Configuration steps

1.Select [OSPF routes setting / OSPF / routing] in the navigation bar to enter the IPv6 Neighbor setting interface, as shown in the following figure:



The red box position in the figure above is the OSPF enable position. To add an OSPF route, click Add Click to enter the add page, as shown in the following figure:



Chapter 12 Ntroduction to switch security functions

12.1 802.1x summary

802.1x protocol is an access control and authentication protocol based on client / server.It can restrict unauthorized users / devices from accessing LAN / WLAN through access port.802.1x authenticates the user / device connected to the switch port before obtaining various services provided by the switch or LAN.Before passing the authentication, 802.1x only allows eapol (LAN based extended authentication protocol) data to pass through the switch port connected to the device;After passing the authentication, the normal data can pass through the Ethernet port smoothly.

12.2 802.1xTechnical introduction

The 802.1x protocol based on Ethernet port authentication has the following characteristics: ieee802.11X protocol is a two-layer protocol, which does not need to reach the third layer. It does not require high overall performance of the equipment, which can effectively reduce the network construction cost;The EAP (extended authentication protocol) commonly used in RAS system is borrowed, which can provide good scalability and adaptability and realize compatibility with the traditional PPP authentication architecture;The authentication architecture of 802.1x adopts the logical functions of "controllable port" and "uncontrollable port", which can realize the separation of service and authentication. Radius and switch use uncontrollable logical ports to jointly complete the authentication and control of users. The service message is directly carried on the normal layer-2 message and exchanged through the controllable port,The authenticated data packet is a pure data packet without encapsulation;The existing background authentication system can be used to reduce the deployment cost and have rich business support;Different user authentication levels can be mapped to different VLANs;The switching port and wireless LAN can have secure authentication access function.

12.3 802.1xworking principle

1.When the user needs to access the Internet, open the 802.1x client program, enter the user name and password that have been applied and registered, and initiate the connection request.At this time, the authentication program will be sent to the client once.

2.After receiving the data frame requesting authentication, the switch will send a request frame to ask the user's client program to send the entered user name.

3.The client program responds to the request sent by the switch and sends the user name information to the switch through the data frame.The switch sends the data frame sent by the client to the authentication server for processing after packet processing.

4.After receiving the user name information forwarded by the switch, the authentication server compares the information with the user name table in the database, finds the password information corresponding to the user name, encrypts it with a randomly generated encryption word, and also transmits the encryption word to the switch and the switch to the client program.

5.After receiving the encrypted word from the switch, the client program encrypts the password part with the encrypted word (this encryption algorithm is usually irreversible) and transmits it to the authentication server through the switch.

6.The authentication server compares the encrypted password information sent to it with its own password information after encryption operation. If it is the same, it considers the user as a legal user, feeds back the authentication message, and sends an instruction to open the port to the switch to allow the user's business flow to access the network through the port.Otherwise, the authentication failure message will be fed back, and the switch port will be kept closed. Only the authentication information data will be allowed to pass, but not the service data.

12.4 Authentication server

12.4.1 AAA (radius authentication)

Radius is a distributed information exchange protocol with client / server structure, which can protect the network from unauthorized access. It is often used in various network environments that require high security and allow remote users to access.The protocol defines the radius message format and its transmission mechanism based on UDP (User Datagram Protocol), and specifies the destination UDP port numbers 1812 and 1813 as the default authentication and billing port numbers respectively.

Configuration steps

1. Select [radius / security] in the navigation bar to enter the radius server setting interface.

2. In the authentication server setting interface, you can view the configuration information of the authentication server.

3. To modify the authentication server configuration, click below 

Button, as shown below:

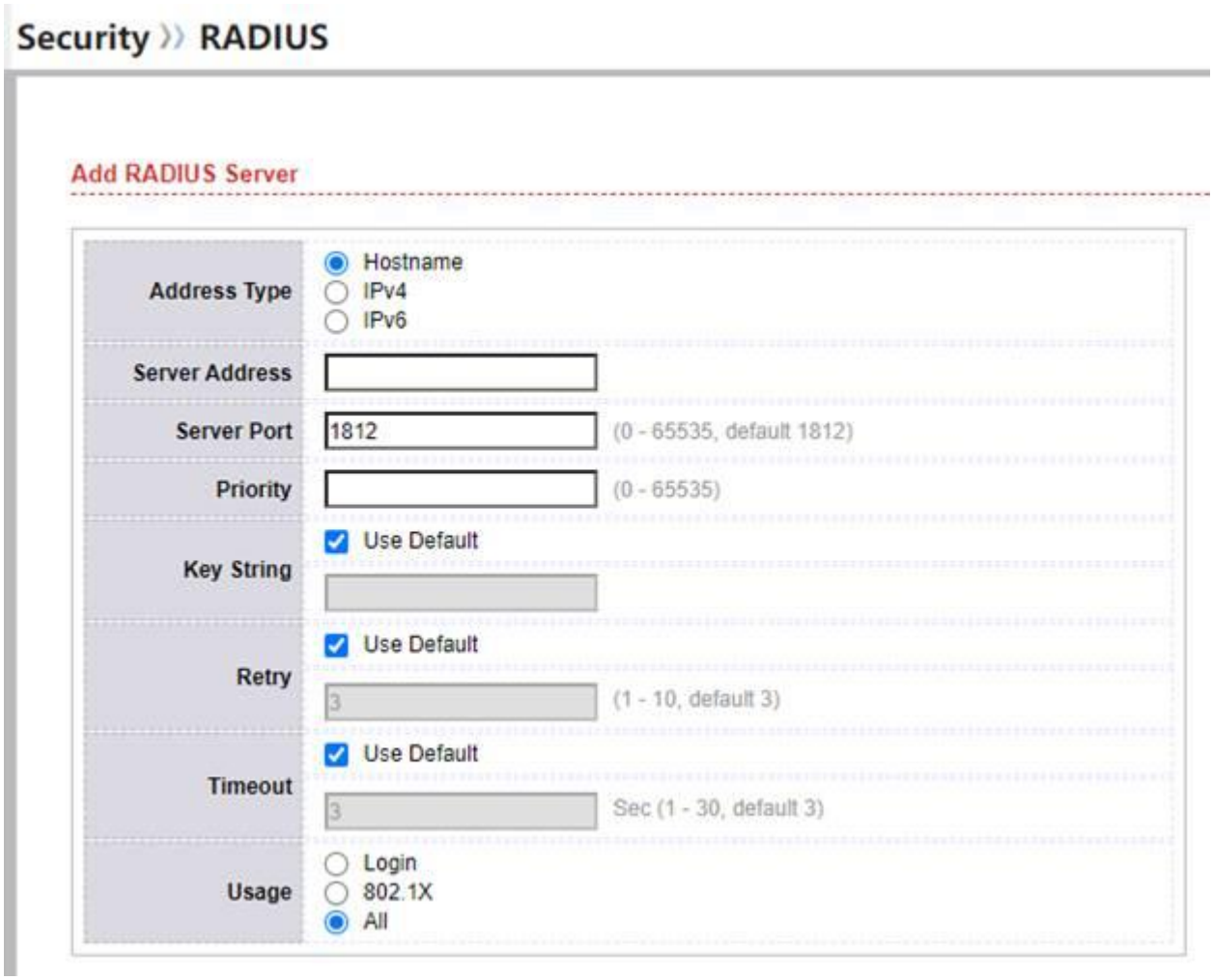


Figure 10.1 radius server configuration interface

Configuration item description

Table 10.1 description of radius authentication server configuration items

Configuration item	explain
Address Type	Address type. The default is host name
Server Address	Radius server address
Server Port	The port number of the radius authentication server. The range is < 1-65535 >, and the default is 1812
Priority	priority
Key String	Radius server key. The default is none
Retry	The number of reconnections of radius server, ranging from < 1-10 >, is 3 by default
Time Out	The timeout time, ranging from < 1-30 > seconds, is 3 seconds by default
Usage	Use objects. The default is all

12.4.2 AAA (TACACS + Certification)

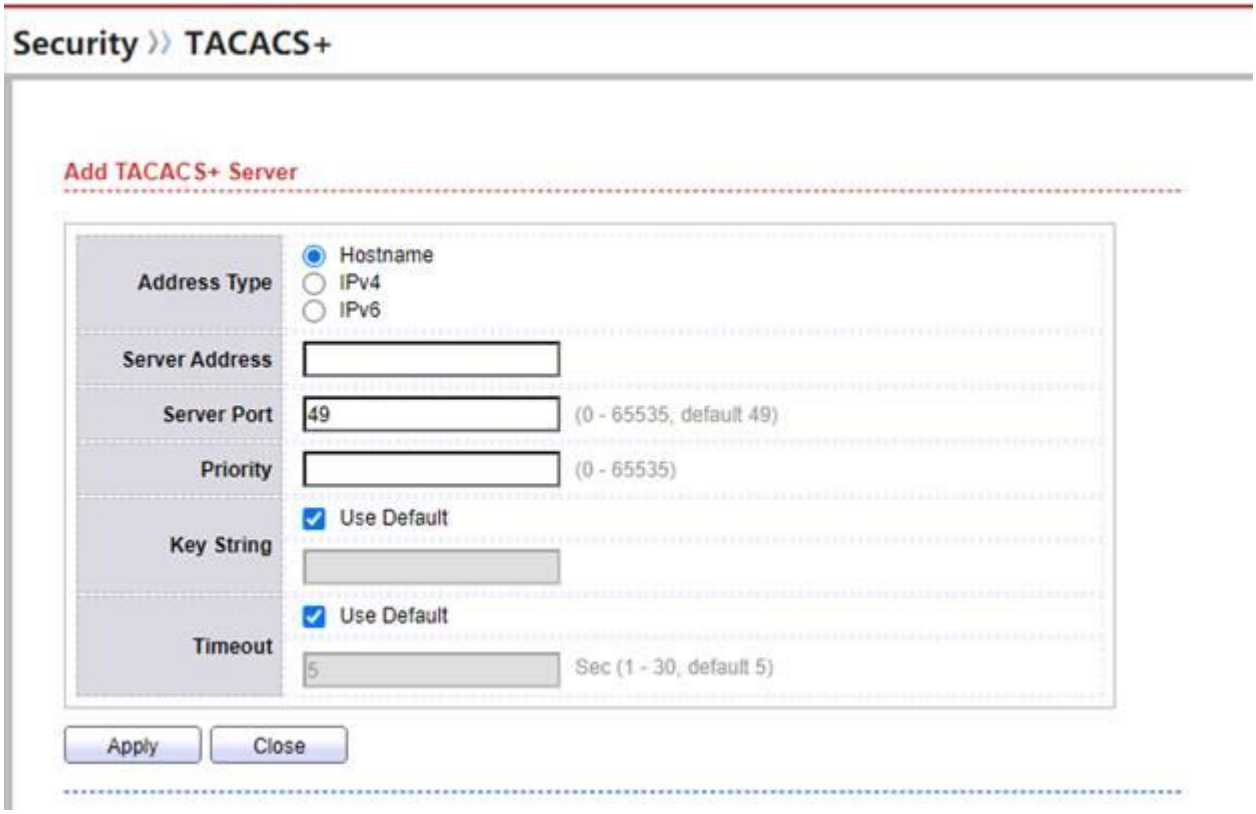
TACACS + (terminal access controller access control system protocol) is a security protocol with enhanced functions based on TACACS protocol.The function of this protocol is similar to that of radius protocol. The client / server mode is adopted to realize the communication between NAS and TACACS + server.

Configuration steps

1. Select [TACACS + / security] in the navigation bar to enter the TACACS server setting interface.

2. In the authentication server setting interface, you can view the configuration information of the authentication server.

3. To modify the authentication server configuration, click below Add Button, as shown below:



12.4.3 comparison between radius and TACACS +

From the above, TACACS + is very similar to radius, which is widely used at present. What are their differences and connections?

Look at the table below:

TACACS + protocol	Radius protocol
Using TCP, network transmission is more reliable	Using UDP, the network transmission efficiency is higher
Except for TACACS + message header, all message bodies are encrypted	Only the password field in the verification message is encrypted
The protocol message is relatively complex, and authentication and authorization are separated, so that authentication and authorization services can be separated and implemented on different security servers	The protocol message is relatively simple, with the combination of authentication and authorization, which is difficult to separate
It supports the configuration command of the device and the authorization of the model.The command line available to users is limited by both user level and AAA authorization. Each command entered by a user at a certain level needs to be authorized through TACACS + server. If the authorization is passed, the command can be executed	Authorization to use the configuration command of the device is not supported The command line that users can use after logging in to the device is determined by the user level. Users can only use the command line whose default level is equal to / lower than the user level

12.5 DosAnti attack

DOS is the abbreviation of denial of service, which is called DoS attack. Its purpose is to make the computer or network unable to provide normal services.The most common DoS attacks include computer network broadband attack and connectivity attack. DoS attack refers to deliberately attacking the defects of network protocol implementation or brutally exhausting the resources of the attacked object directly through barbaric means. The purpose is to make the target computer or network unable to provide normal services or resource access, and make the target system stop responding or even crash,This attack does not include intrusion into the target server or target network device.These

service resources include network bandwidth, file system space capacity, open processes or allowed connections.No matter how fast the bandwidth and the processing speed of the computer are, this kind of attack can not be avoided.

Configuration steps

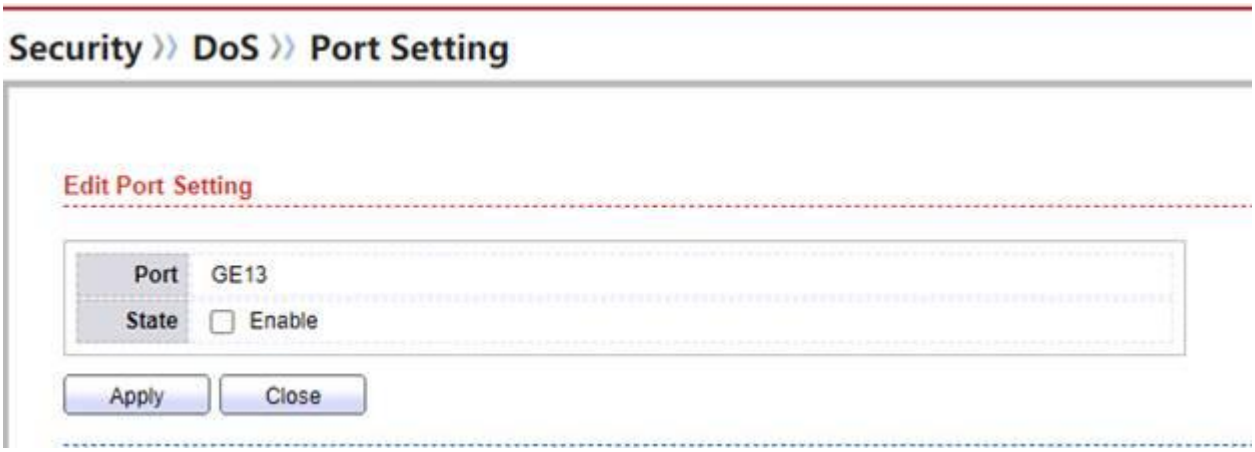
1. Select [property / DOS / security] in the navigation bar to enter the DOS anti attack setting interface, as shown below:

The function of this page is on by default.To modify, click, and at the end, click Apply Just.

port configuration

1. Select [port setting / DOS / security] in the navigation bar to enter the DOS anti attack port setting interface. The port is closed by default. To enable the DOS function,

you need to open the corresponding port. Select the port to be modified in this interface and click Edit Modified as follows:

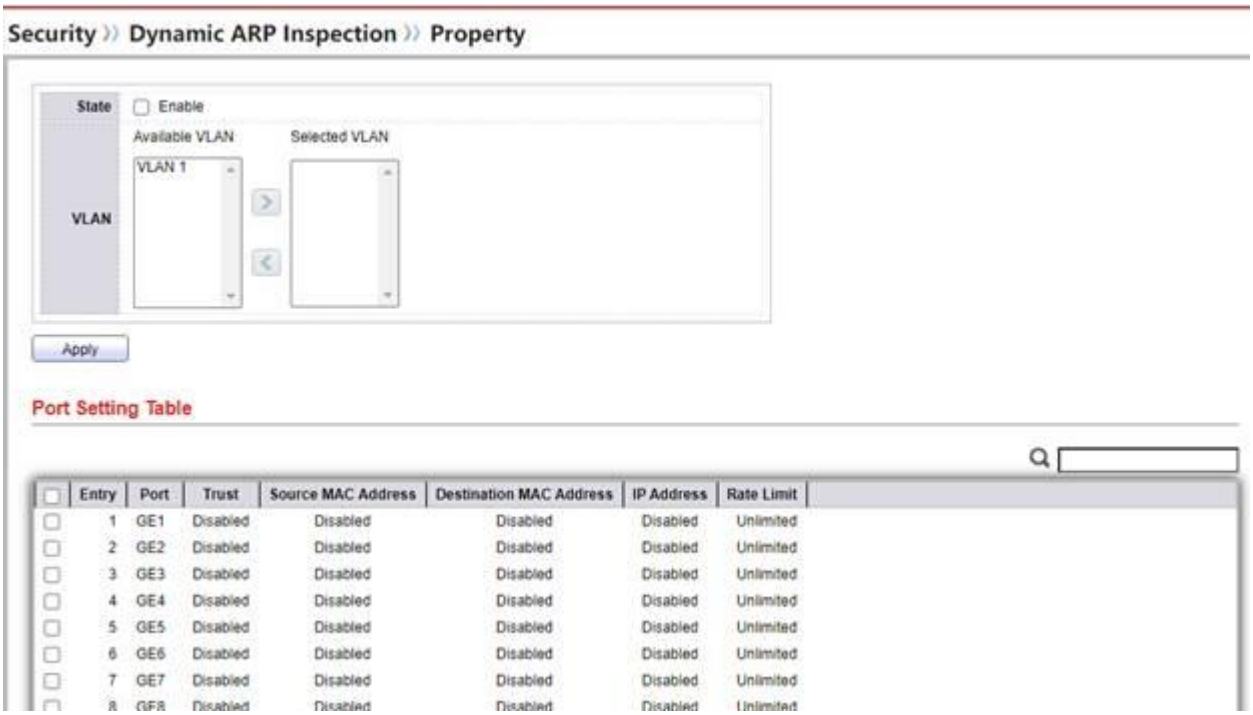


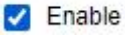
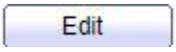
12.6 Dynamic ARP table check

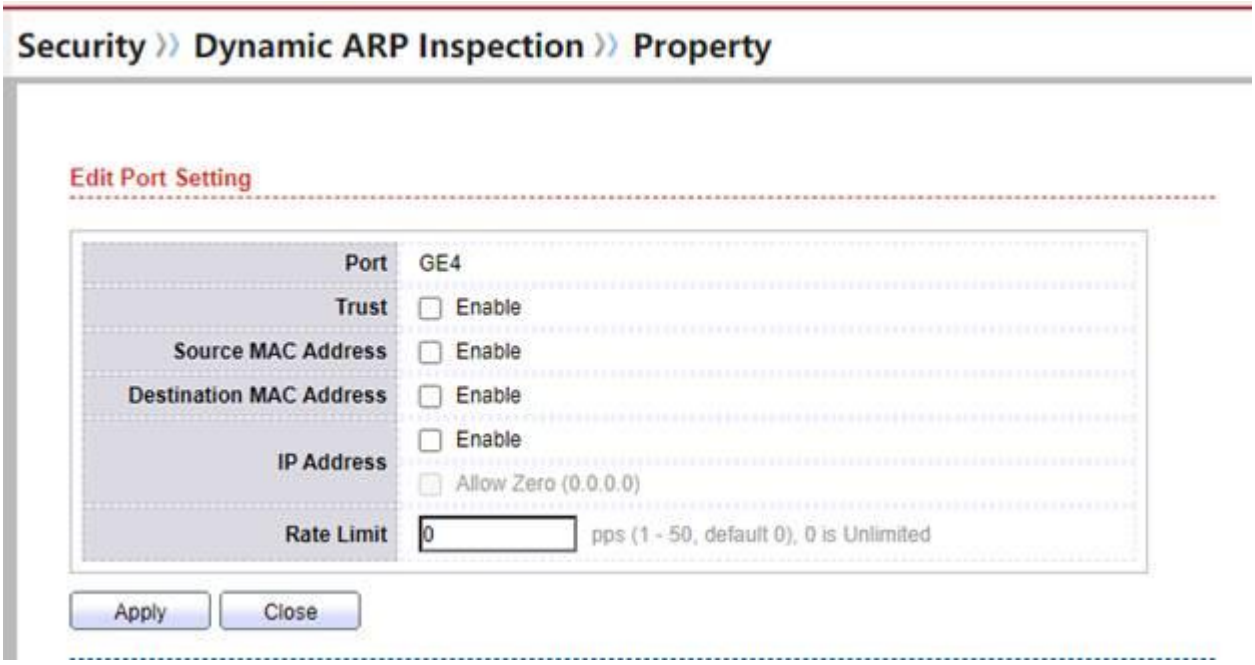
Dynamic ARP inspection function, referred to as Dai function for short.By checking the legitimacy of ARP (address resolution protocol) message, we can find and prevent ARP spoofing attack and enhance network security.The basis of ARP message legitimacy detection is the port IP source guard binding table item. Specific detection principle: in the received ARP message, if the IP address, source MAC address and VLAN ID of the sending end completely match the port IP source guard binding table item, the ARP message is a legal message and forwarded;Otherwise, the ARP message is illegal, discard it and record the log information.

Configuration steps

1.Select [property / dynamic ARP inspection / security] in the navigation bar to enter the dynamic ARP inspection setting interface, as shown below:



State display is required to enable this function  And a VLAN needs to be bound. If you need to modify the port, select the port and click the button below  Button, as shown below:



Configuration item description

Configuration item	explain
Port	Port name
Trust	Do you trust this port

Source MAC Address	The source MAC address of the message passing through this port
Destination MAC Address	The destination MAC address of the message passing through this port
IP Adress	IP address of the message passing through this port (IP address is allowed to be 0.0.0.0)
Rate Limit	Speed limit, range < 1-50, default to 0 >, 0 is no speed limit

Because the dynamic ARP check function needs to be combined with the IP source guard binding table, the configuration steps of the IP source guard binding table are as follows:

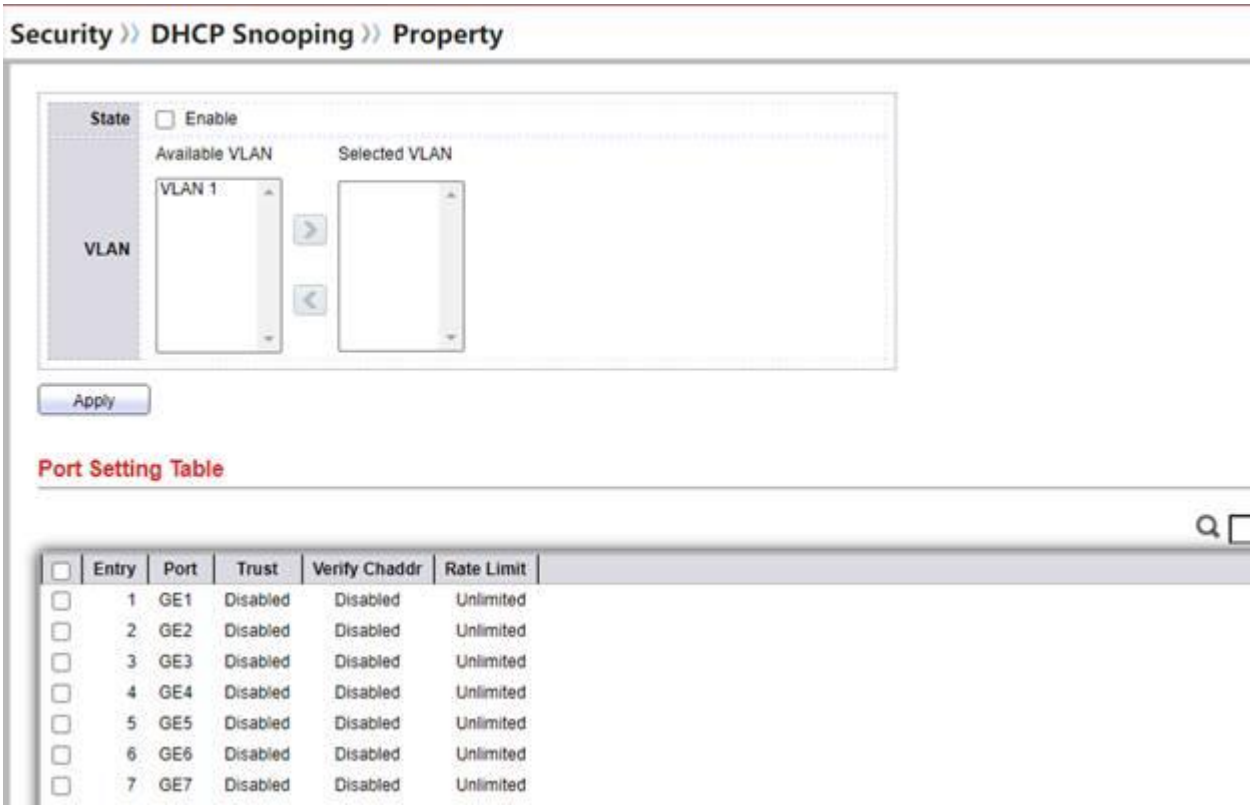
2. Select [impv binding / IP source guard / security] in the navigation bar to enter the dynamic ARP check setting interface, and click Add Button to add a bound table item, as shown in the following figure:

12.7 DHCP Snooping

DHCP SnoopingIt is a security feature of DHCP. It is used to ensure that the DHCP client obtains the IP address from the legal DHCP server, and record the corresponding relationship between the DHCP client's IP address and MAC address, so as to prevent DHCP attacks on the network.This function enables the equipment to defend against DHCP attacks on the network, enhances the reliability of the equipment, ensures the normal operation of the communication network, and provides users with a safer network environment and more stable network services.

Configuration steps

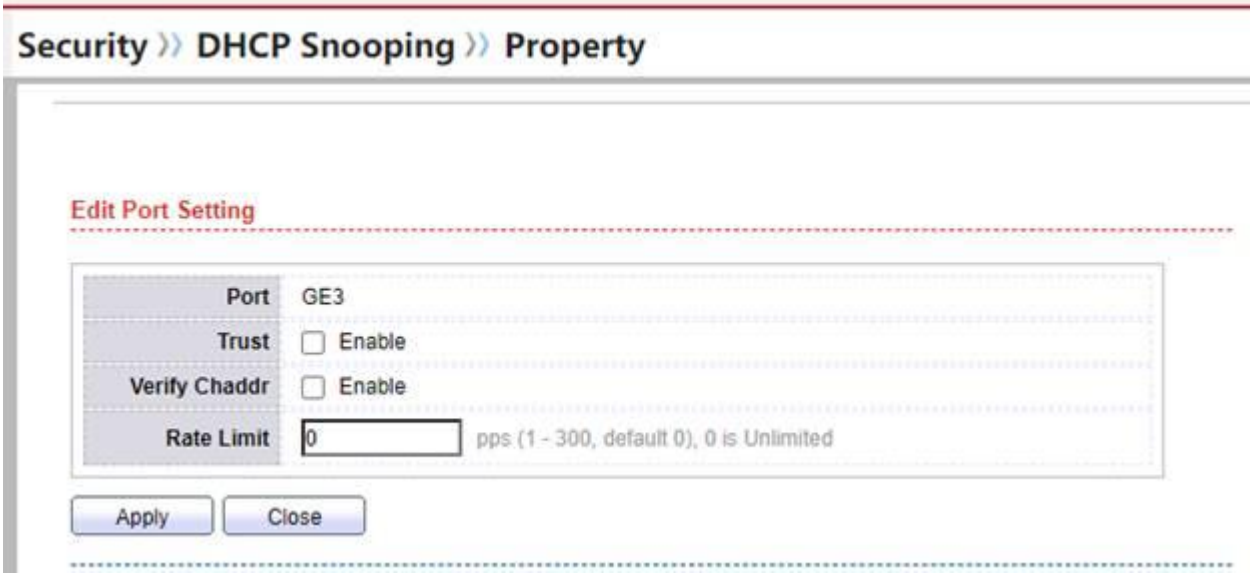
1. Select [property / DHCP snooping / security] in the navigation bar to enter the DHCP snooping setting page, as shown below:



State display is required to enable this function 

And a VLAN needs to be bound. If you need to modify the port, select the port and click the button below 

Button, as shown below:



Configuration item description

Configuration item	explain
Port	Port name
Trust	Do you trust this port

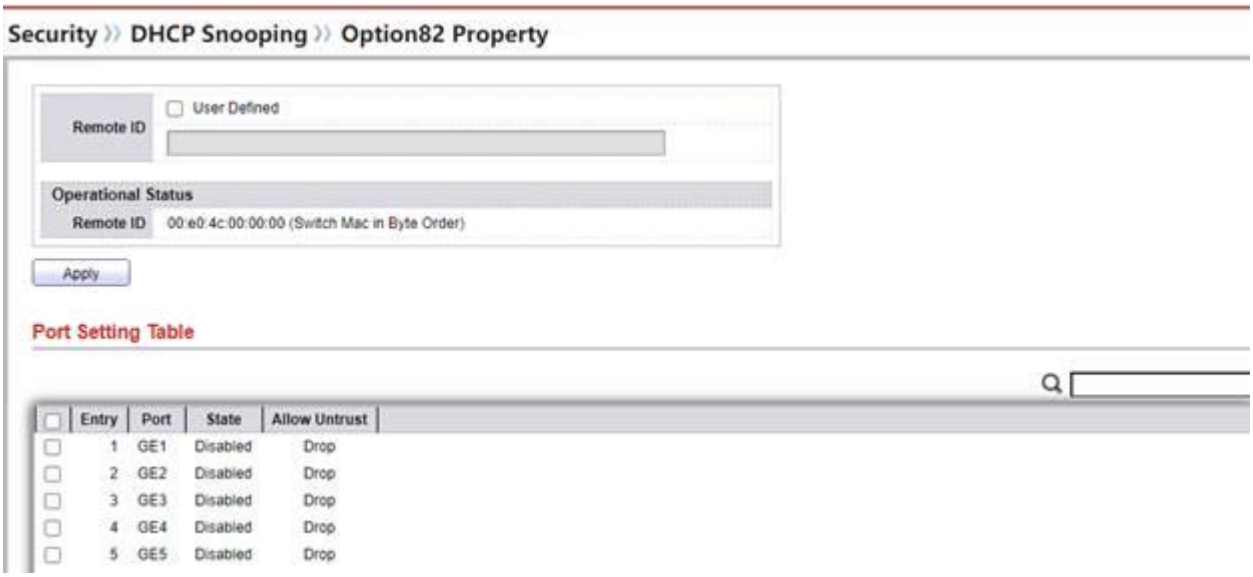
Verify Chaddr	Address check of client
Rate Limit	Speed limit, range < 1-300, default 0 > 0 is no speed limit

12.7.1 option82 function

Option 82 is the relay agent information option in the DHCP message.When the DHCP client sends a request message to the DHCP server, if it needs to go through the DHCP relay, the DHCP relay adds option 82 to the request message.Option 82 contains many sub options. At present, the function of option 82 in the switch only supports sub option 1 and sub option 2The agent circuit ID (i.e. circuit ID) is defined in sub option 1, and the agent remote ID (i.e. remote ID) is defined in sub option 2.

Configuration steps

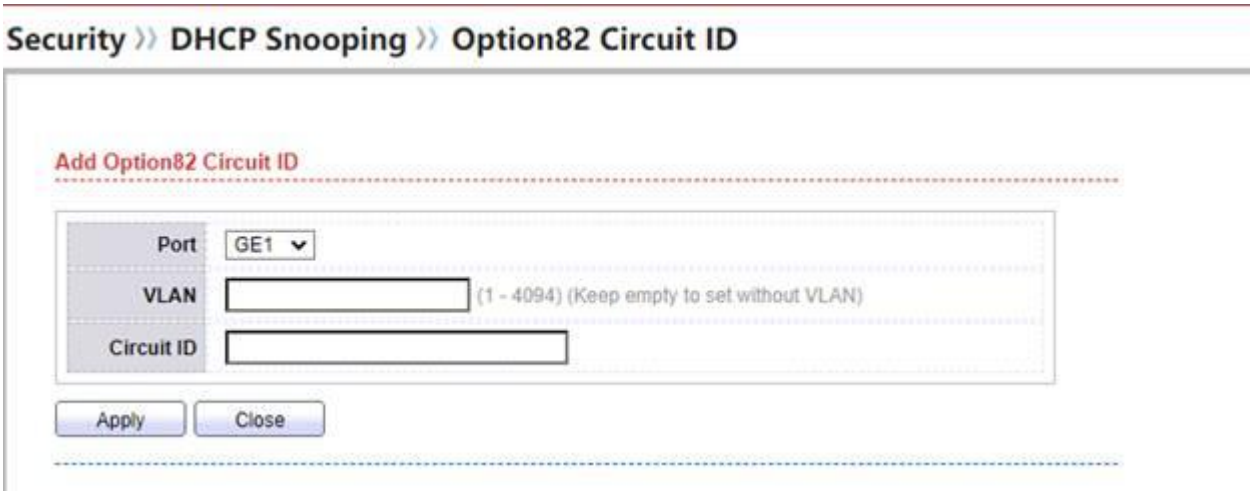
1.Select [option82 property / DHCP snooping / security] in the navigation bar to enter the option82 setting page, as shown below:



To modify the port configuration, select the port and click the button below 

Button, as shown below:

2.Select [option82 circuit ID / DHCP snooping / security] in the navigation bar to enter the option82 setting page. To add an agent circuit ID, click Add Button, as shown below:



Chapter 13 ACL

13.1 ACL summary

Access control list (ACL) is the instruction list of router and switch interface, which is used to control the data packets in and out of the port.After configuring ACL, you can restrict network traffic, allow specific devices to access, and specify to forward data packets on specific ports.Communication between information points and communication between internal and external networks are essential business requirements in the enterprise network. In order to ensure the security of the internal network, security policies need to be adopted to ensure that unauthorized users can only access specific

network resources, so as to achieve the purpose of access control.In short, ACL can filter data packets in the network and is a network technical means to control access.

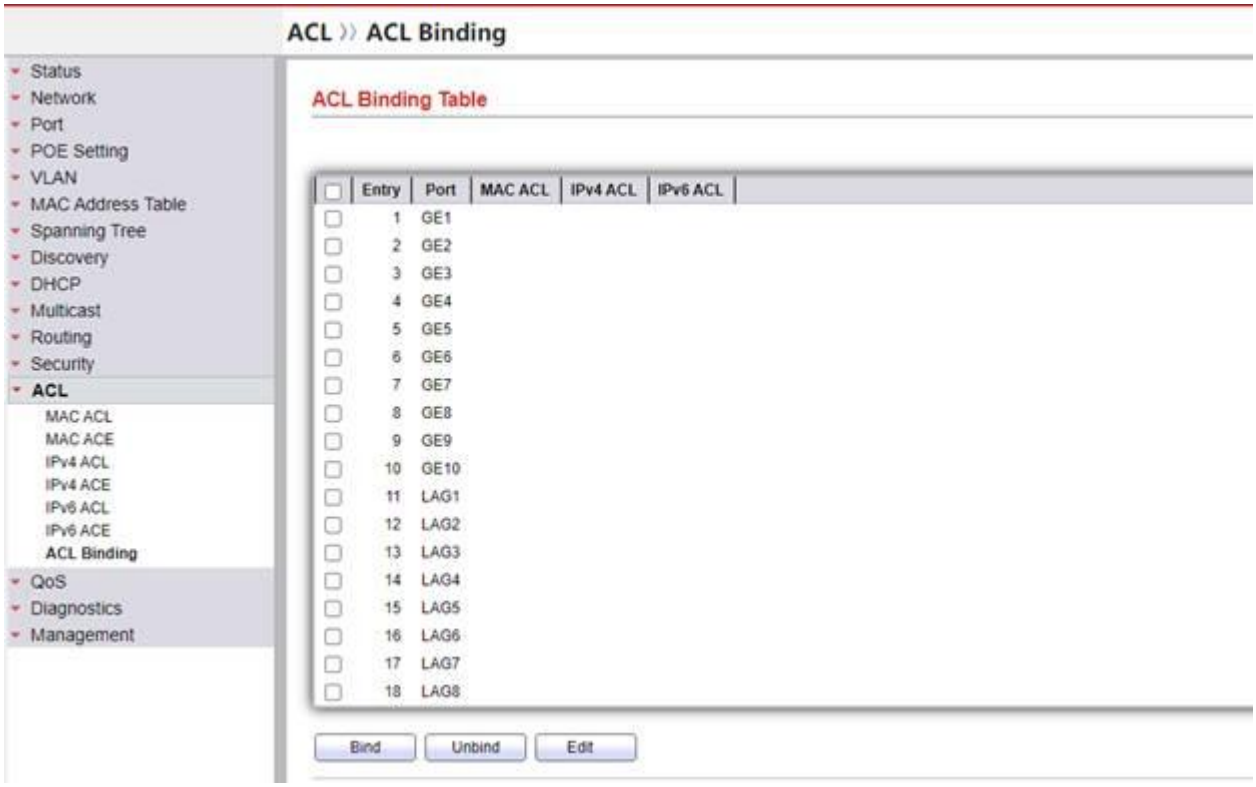
13.2 working principle

Use a single port to explain which ACL a port executes, which needs to be judged according to the execution order of conditional statements in the list.If the header of a packet matches a conditional judgment statement in the table, the subsequent statements will be ignored and will not be checked.

Only when the data packet does not match the first judgment condition, it is handed over to the next condition judgment statement in the ACL for comparison.If it matches (assuming that sending is allowed), the data will be sent to the destination interface immediately regardless of the following statements.If all ACL judgment statements are detected and there is still no matching statement exit, the packet will be regarded as rejected and discarded.

13.3 ACLGroup settings

1. Select [ACL] in the navigation bar to enter the ACL group interface, as shown in the following figure. There are three ACL configurations, namely MAC ACL, IPv4 ACL and IPv6 ACL.

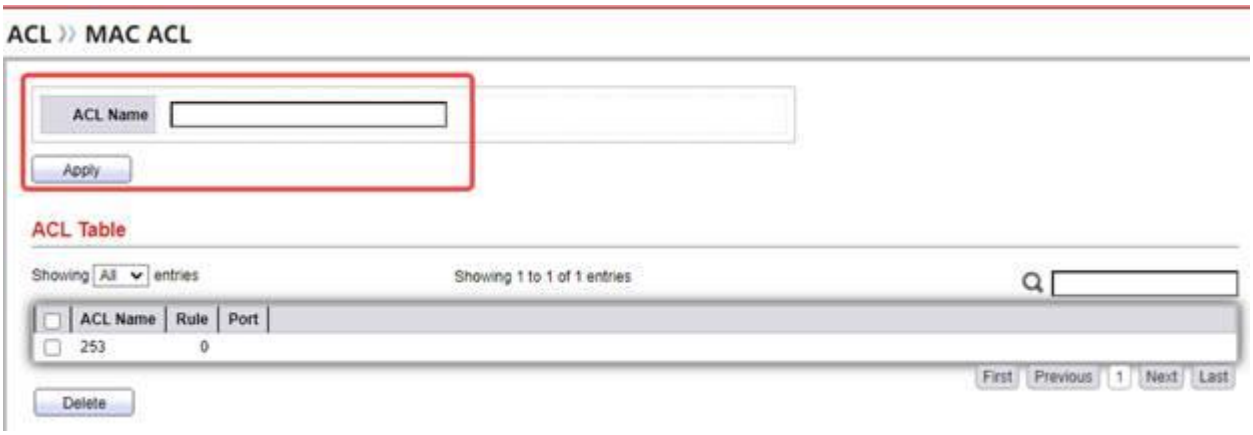


13.4 ACLrule

13.4.1 MAC ACL rule setting

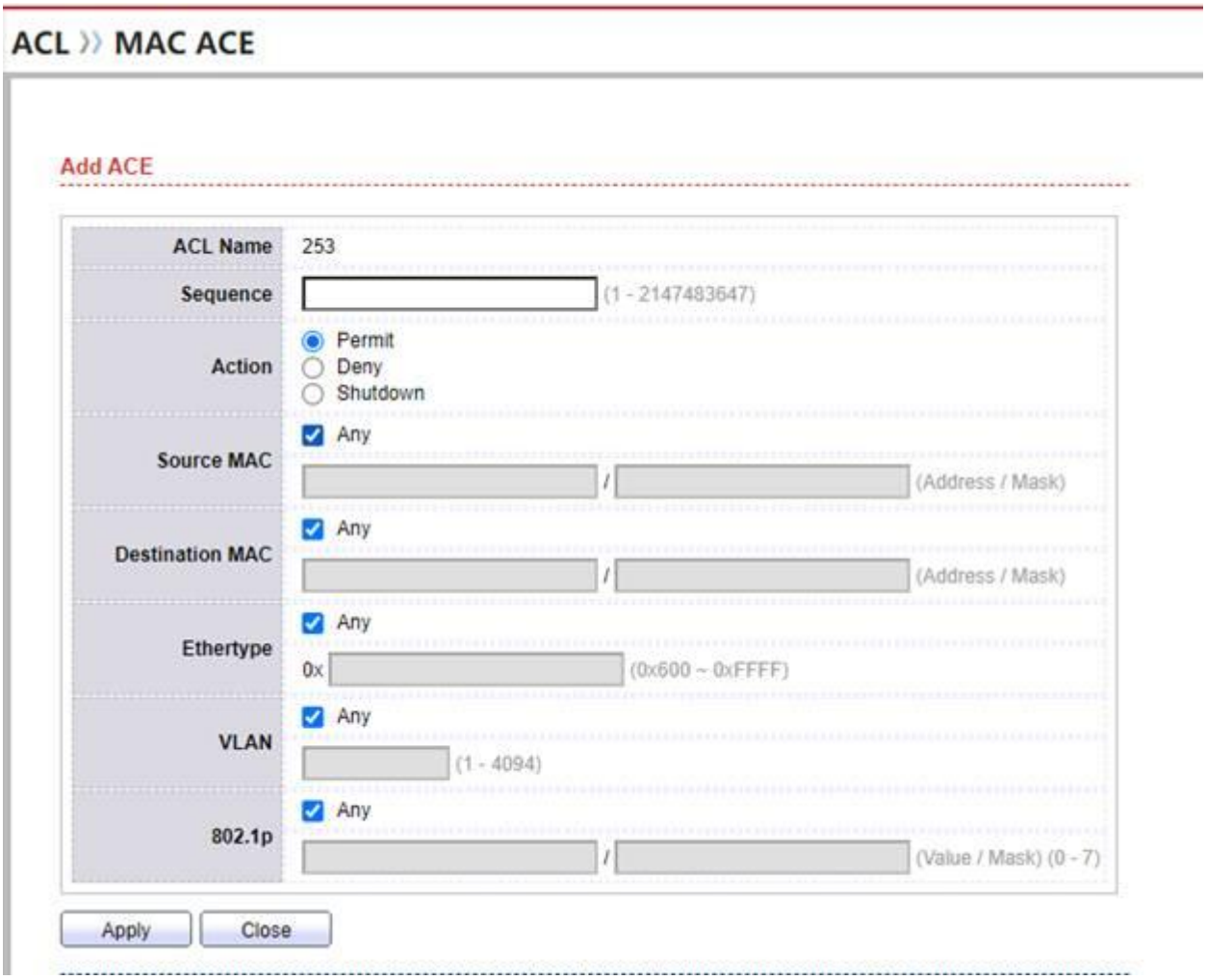
Configuration steps

1. Select [MAC ACL / ACL] in the navigation bar to enter the MAC ACL rule viewing interface, as shown in the following figure:

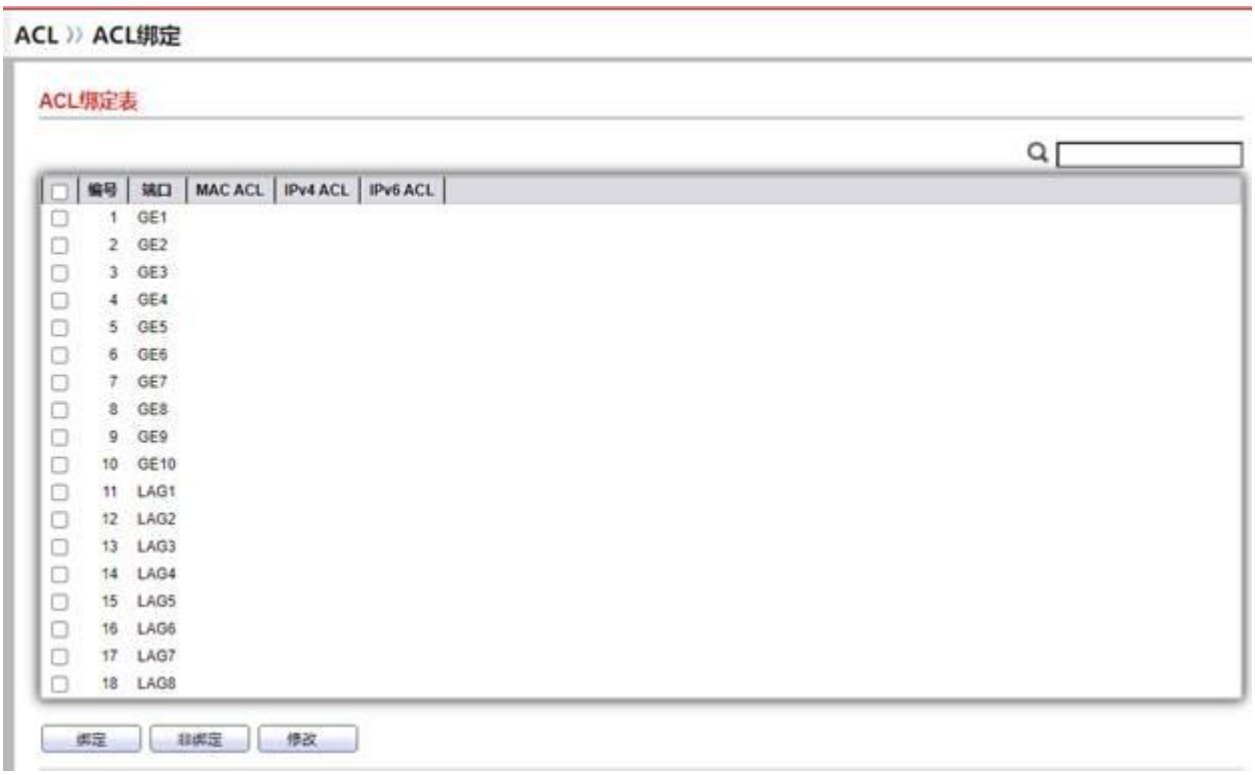


Note: before creating MAC ACL rules, you need to create ACL names in the figure above, and then create corresponding rules under the names.

2. Select [MAC ACE / ACL] in the navigation bar, create the corresponding MAC ACL rule, and click Add Create ACL rules. The creation interface is as follows:



Note: after the ACL rule is created, it needs to be bound to the port to take effect.



click 绑定 Button, the binding page will pop up to bind ACL rules, as shown in the following figure:

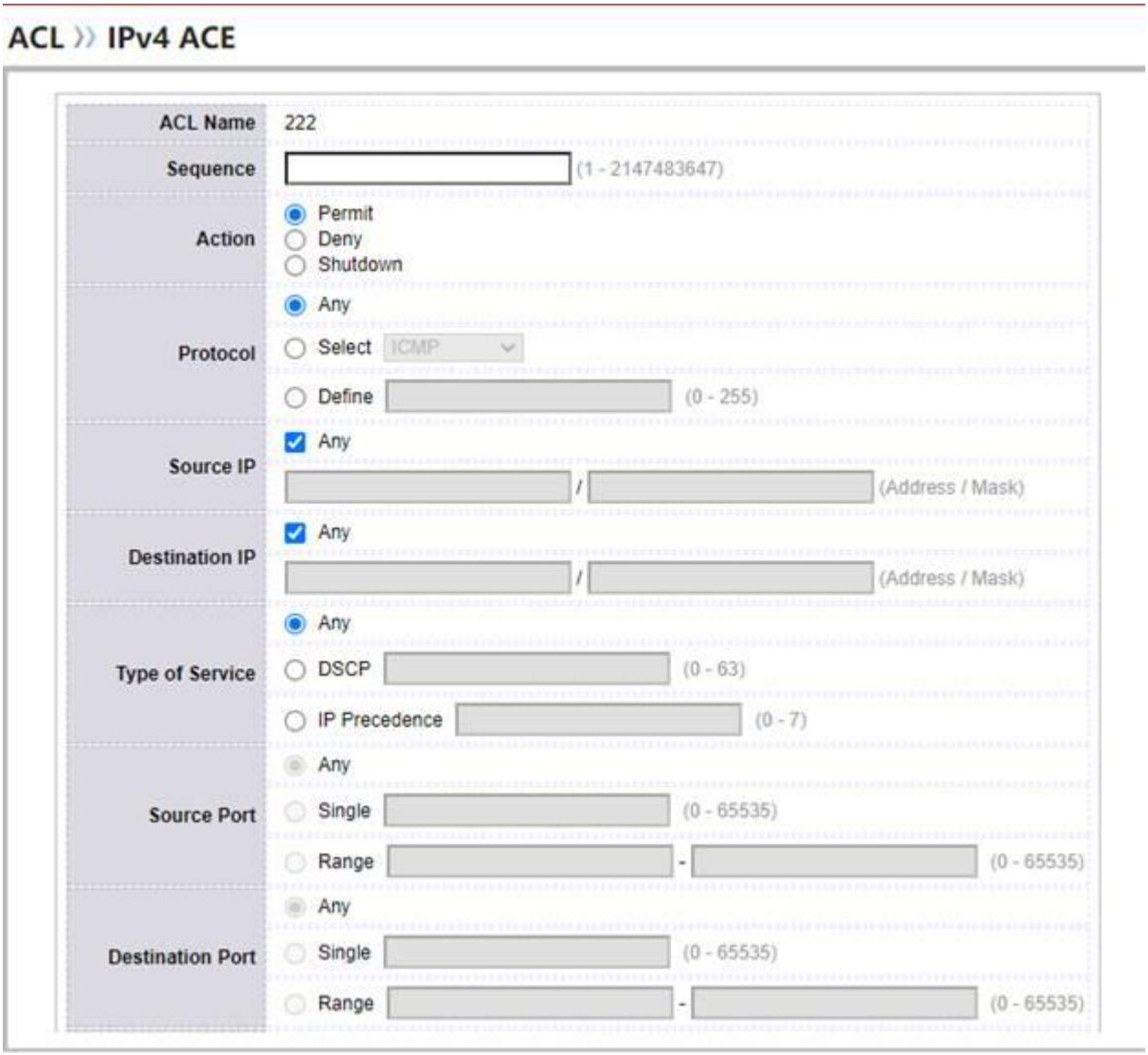
13.4.2 IPv4 ACL rule settings

Configuration steps

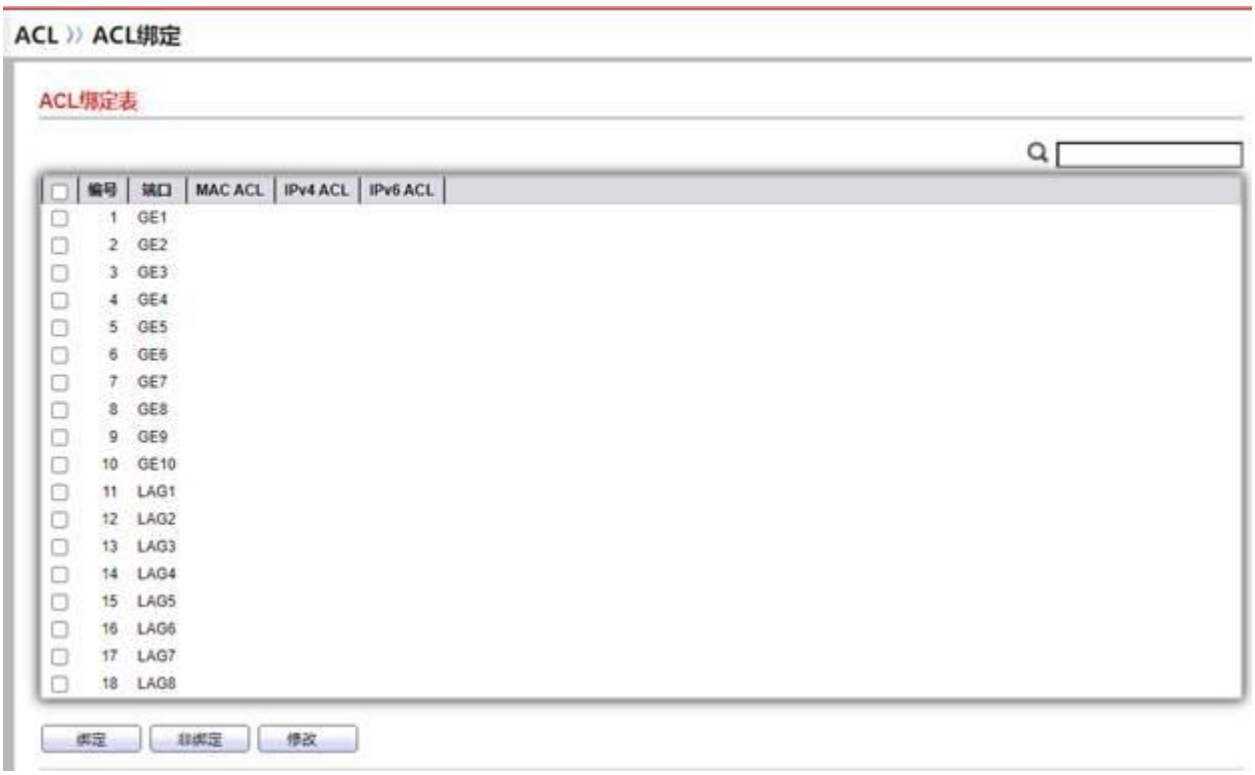
1.Select [IPv4 ACL / ACL] in the navigation bar to enter the IPv4 ACL rule viewing interface, as shown in the following figure:

Note: before creating an IPv4 ACL rule, you need to create the ACL name in the figure above, and then create the corresponding rule under the name.

2.Select [IPv4 ACE / ACL] in the navigation bar, create the corresponding IP V4 ACL rule, and click Add Create ACL rules. The creation interface is as follows:



The configured ACL rules need to bind ports to take effect. The bind port page is shown in the following figure:

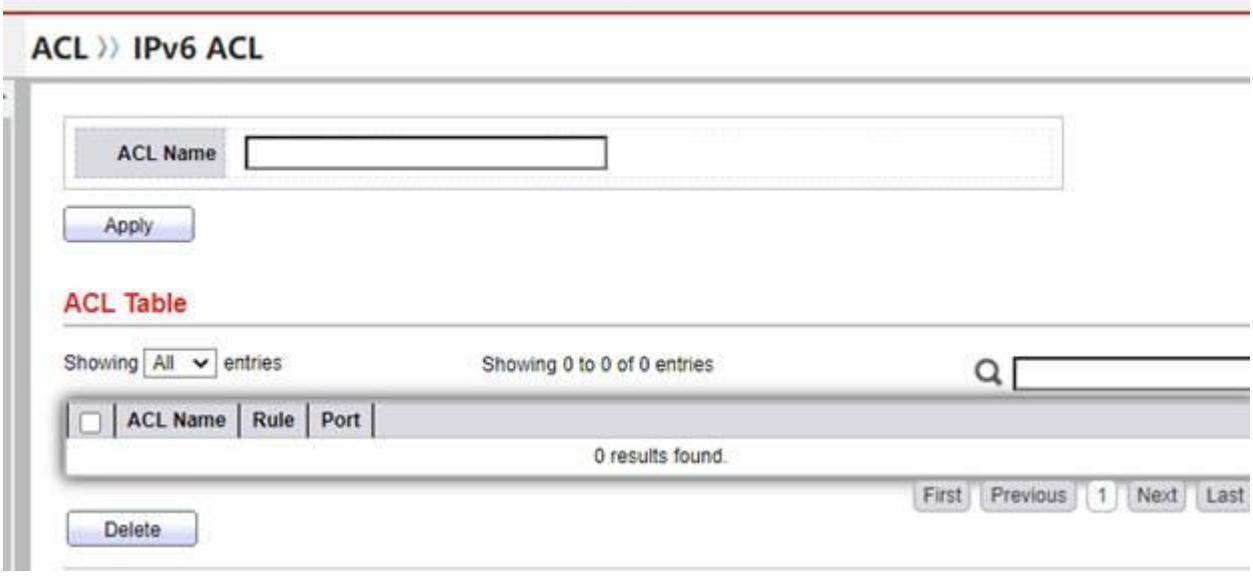


click 绑定 Button, the binding page will pop up to bind ACL rules, as shown in the following figure:

13.4.3 IPv6 ACL rule setting

Configuration steps

1.Select [IPv6 ACL / ACL] in the navigation bar to enter the IPv6 ACL rule viewing interface, as shown in the following figure:



Note: before creating an IPv6 ACL rule, you need to create the ACL name in the figure above, and then create the corresponding rule under the name.

2.Select [IP V6 ACE / ACL] in the navigation bar, create the corresponding IPv6 ACL rule, and click Add Create ACL rules. The creation interface is as follows:

Similarly, the created ACL needs to be bound to the port to take effect

Chapter 14 QoS

14.1 QoSsummary

QoS (quality of service) is a technology to solve the problems of network delay and congestion by various means.When the network is overloaded or congested, QoS can ensure that important traffic and key applications are not delayed or discarded, and ensure the efficient operation of the network.

14.2 Function introduction

When the network is congested, all data streams may be discarded;In order to meet the requirements of users for different applications and different service quality, the network needs to be able to allocate and schedule resources according to the requirements of users, and provide different service quality for different data streams: give priority to the processing of real-time and important data packets;For ordinary data packets with weak real-time performance, it provides lower processing priority and even discards them in case of network congestion.Devices supporting QoS function can provide transmission quality service;For a certain type of data flow, it can be given a certain level of transmission priority to identify its relative importance, and use various priority forwarding strategies, congestion avoidance and other mechanisms provided by the device to provide special transmission services for these data flows.The network environment configured with QoS increases the predictability of network performance, effectively allocates network bandwidth and makes more rational use of network resources.

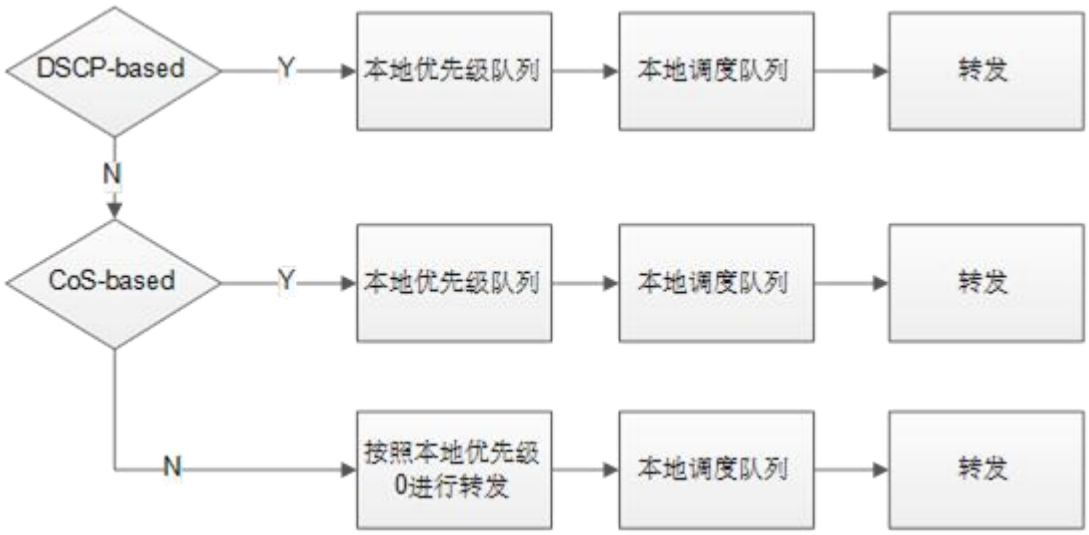
14.3 Congestion management

When congestion occurs, when QoS is not started, all queues in each port of the switch treat all data equally. The strategy used in one port is FIFO (first in, first out). Here, it shows that the role of QoS is on the outbound port. In reality, the importance of different data is generated by the needs of users,Therefore, we have to allocate different data to different output queues, that is, the internal DSCP of QoS. QoS is actually to manage different data when congestion occurs.

14.4 Strategy classification

After QoS is started, the switch will treat different data streams differently. What is the basis for classification?When classifying data packets, is the classification basis of

three-tier data and secondary data the same?Is the classification based on system default or can it be set manually?



For the internal part of the switch, the main classification basis of its QoS is DSCP (this is the internal classification basis of the switch, and the internal DSCP is used later).As can be seen from the above figure, the classification of network data flow is divided into DSCP and COS. When a message has both DSCP and COS classification basis, only the classification basis of DSCP is considered.

14.5 Scheduling mode

Congestion management refers to how to manage and control the network when congestion occurs.The method of processing is to use queue technology.Enter all messages to be sent from one interface into multiple queues and process them according to the priority of each queue.Different queue algorithms are used to solve different problems and produce different effects.Common queue technologies include FIFO, PQ, CQ, CB, WFQ, WRR and sp. WFQ, WRR and SP will be introduced one by one.

14.5.1 SP(Strict Priority)-Strict Priority

Principle: different priorities are set for different queues. The queue with high priority has absolute priority and the queue with low priority. As long as there are packets in the queue with high priority, the queue with high priority is scheduled for forwarding.

14.5.2 WRR(Weighted Round Robin)-Weighted cyclic scheduling algorithm

Weighted round robin (WRR) services all traffic queues and assigns priority to higher priority queues.In most cases, the WRR will handle the high priority services first, but when there are many high priority services, the lower priority services are not completely blocked.Weighted cyclic scheduling algorithm WRR is a strong queue scheduling algorithm, which can effectively distinguish all services in the queue.For queues where all traffic flows are queued for scheduling, WRR allocates bandwidth equally according to the ratio of the weight configured for each queue to the total weight of all traffic flows queued for scheduling.Therefore, when processing the high priority services of multiple users, WRR ensures that each user will not occupy the network bandwidth excessively.Moreover, WRR algorithm is easy to implement in hardware.Therefore, WRR algorithm can achieve the fairness of bandwidth sharing, the isolation ability of malicious streams and the utilization of bandwidth

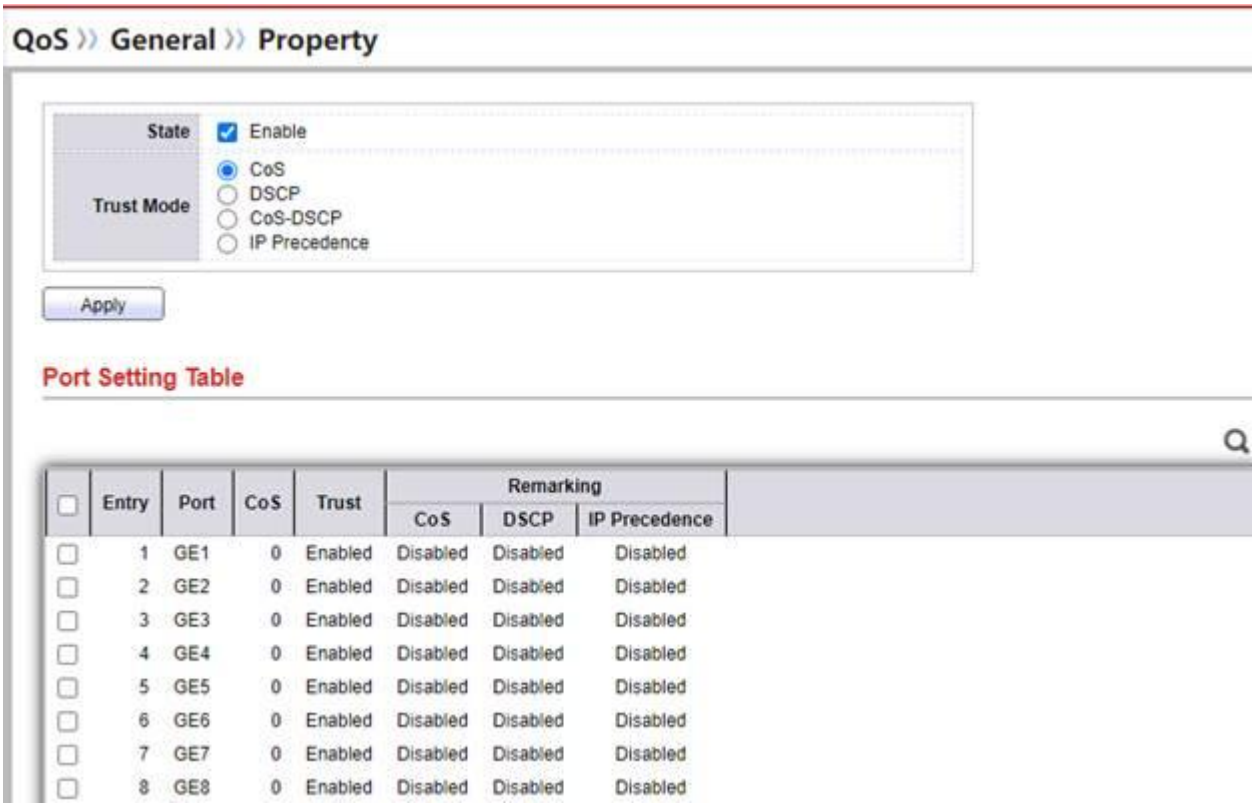
14.5.3 WFQ(Weighted Fair Queuing)-Weighted fair queuing

Weighted fair queuing (WFQ) is a congestion management algorithm, which identifies conversations (in the form of data flow), separates the packets belonging to each conversation, and ensures that the transmission capacity is fairly shared by these independent conversations.WFQ is an automatic method to stabilize the network operation in case of congestion. It can improve the processing performance and reduce the retransmission of packets (almost the same as WRR scheduling, the only difference is the scheduling of the number of integrated packets and bytes).

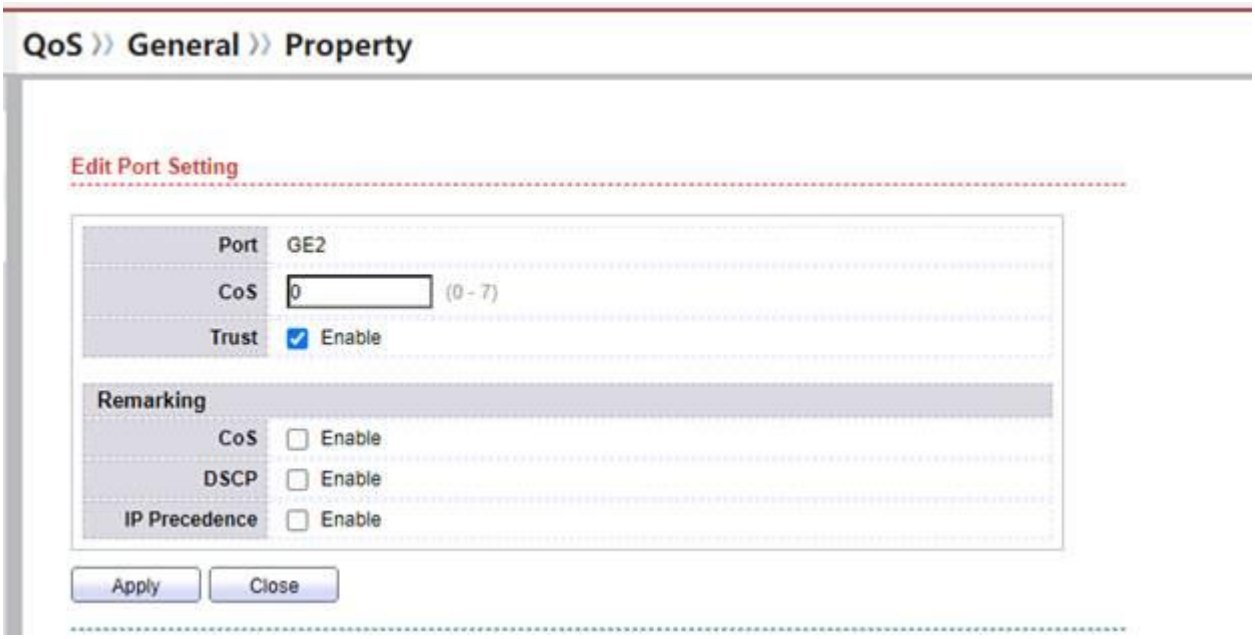
14.6 Priority mapping configuration

Configuration steps

1. Select [property / general / QoS] in the navigation bar to enter the function configuration interface, as shown below:

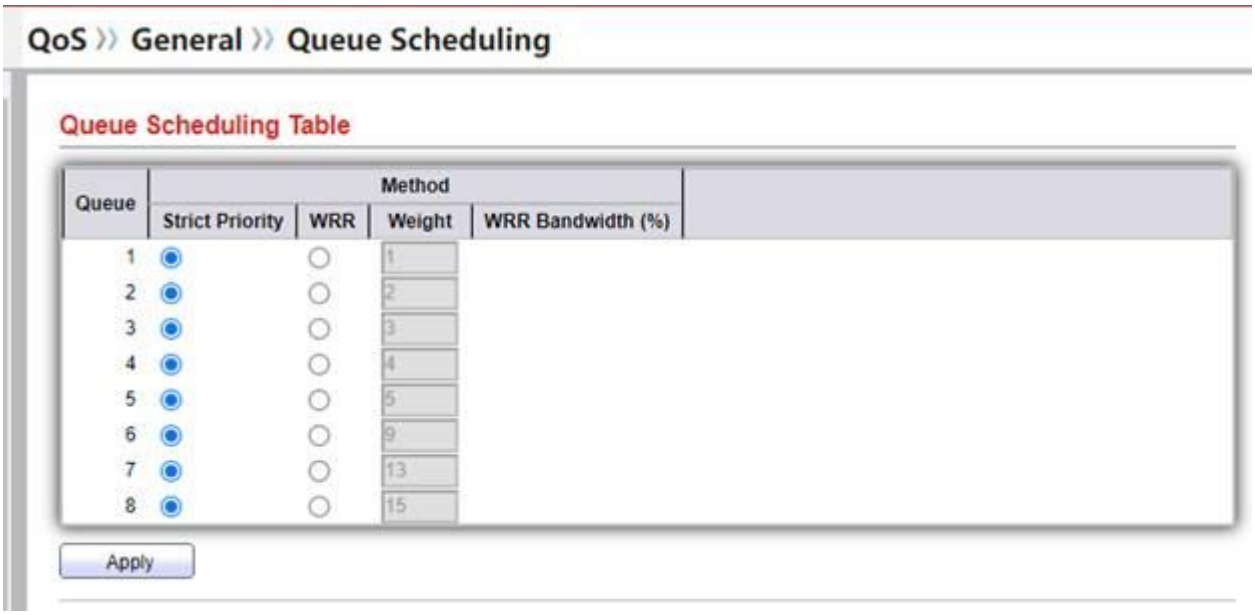


After you click the above figure, you can select four ports for QoS, but you can select them from the following table Edit Button, the following page will appear:

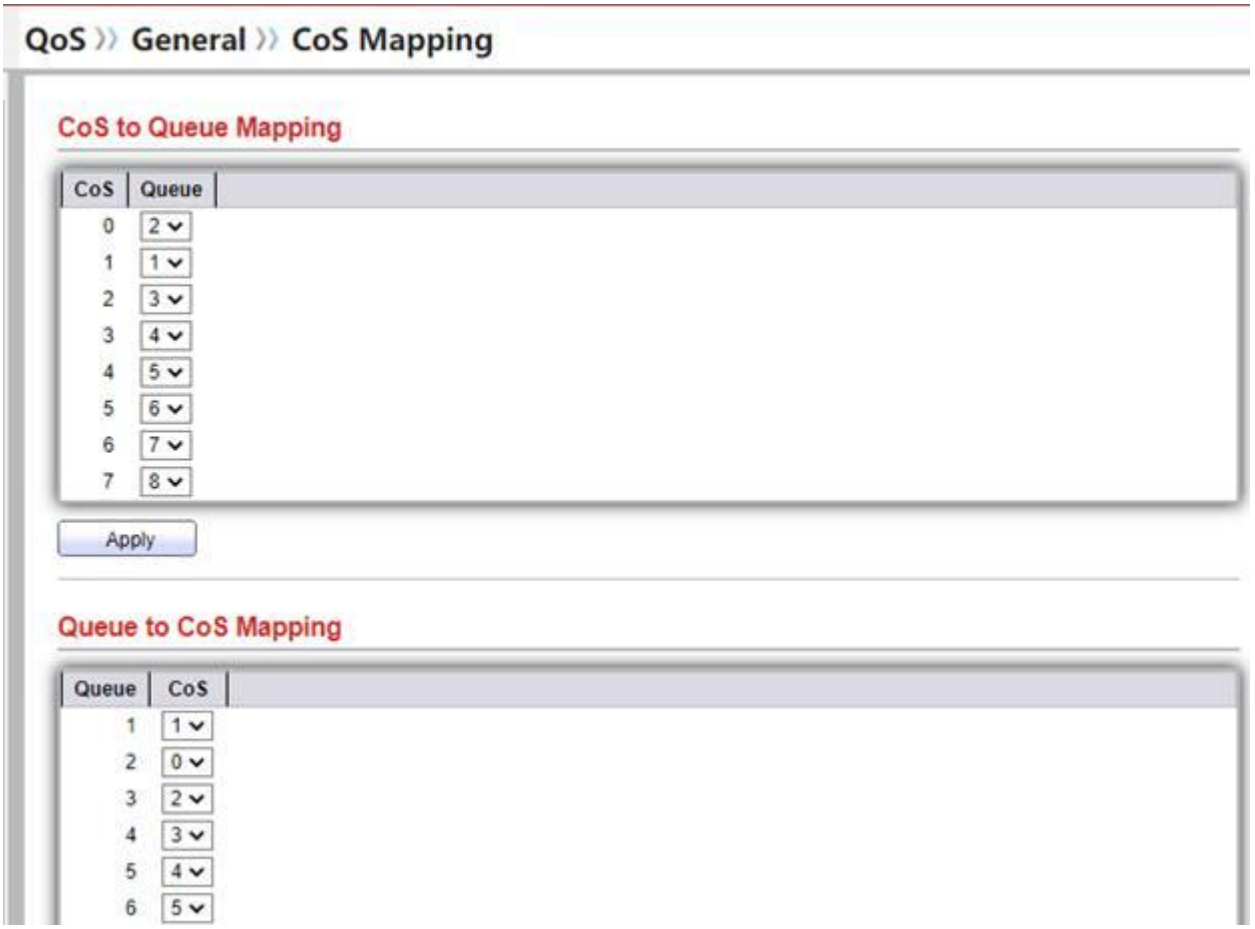


Select the corresponding port according to the above figure and use the required QoS mapping.

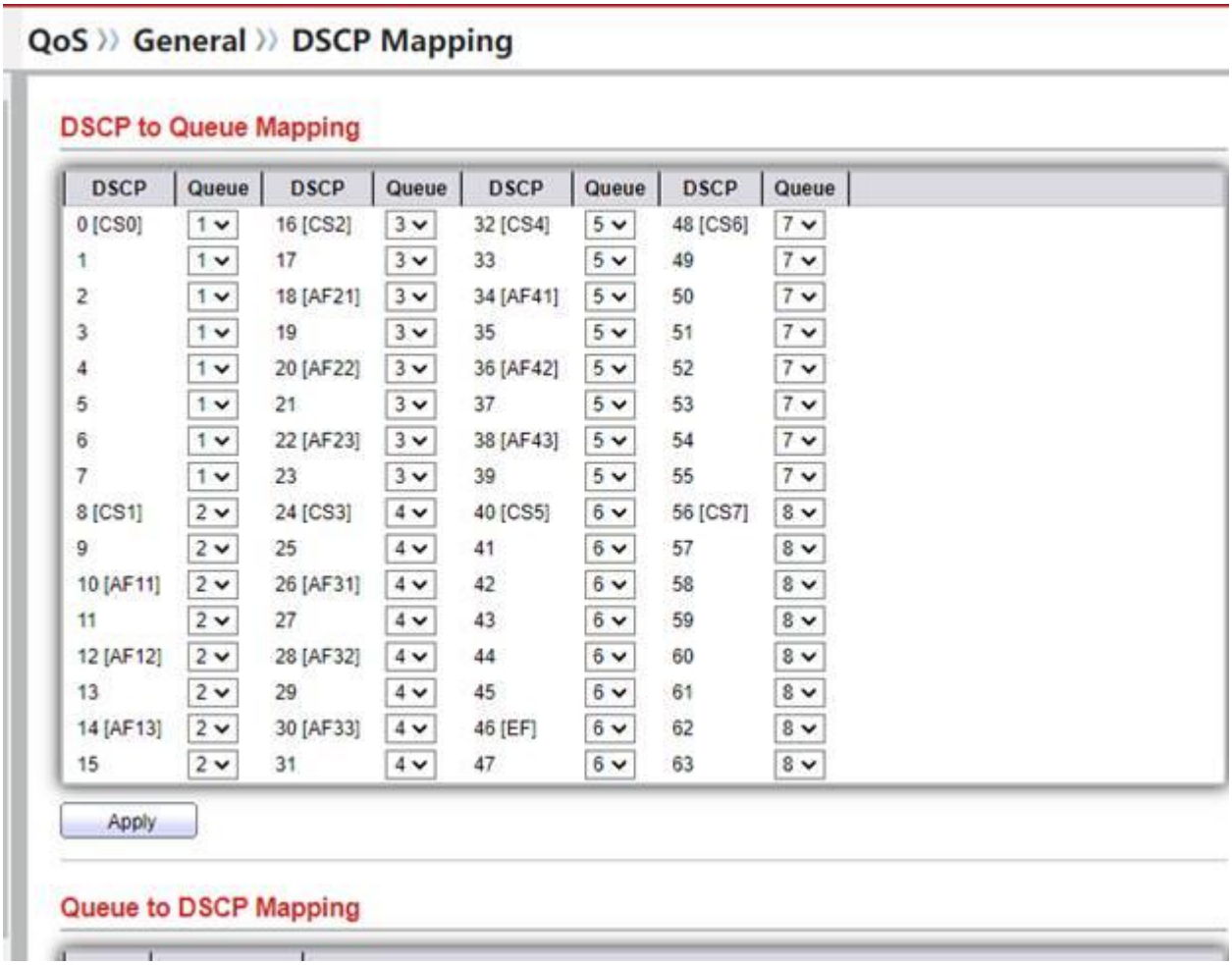
2. Select [queue scheduling / general / QoS] in the navigation bar to enter the queue scheduling setting interface, as shown below:



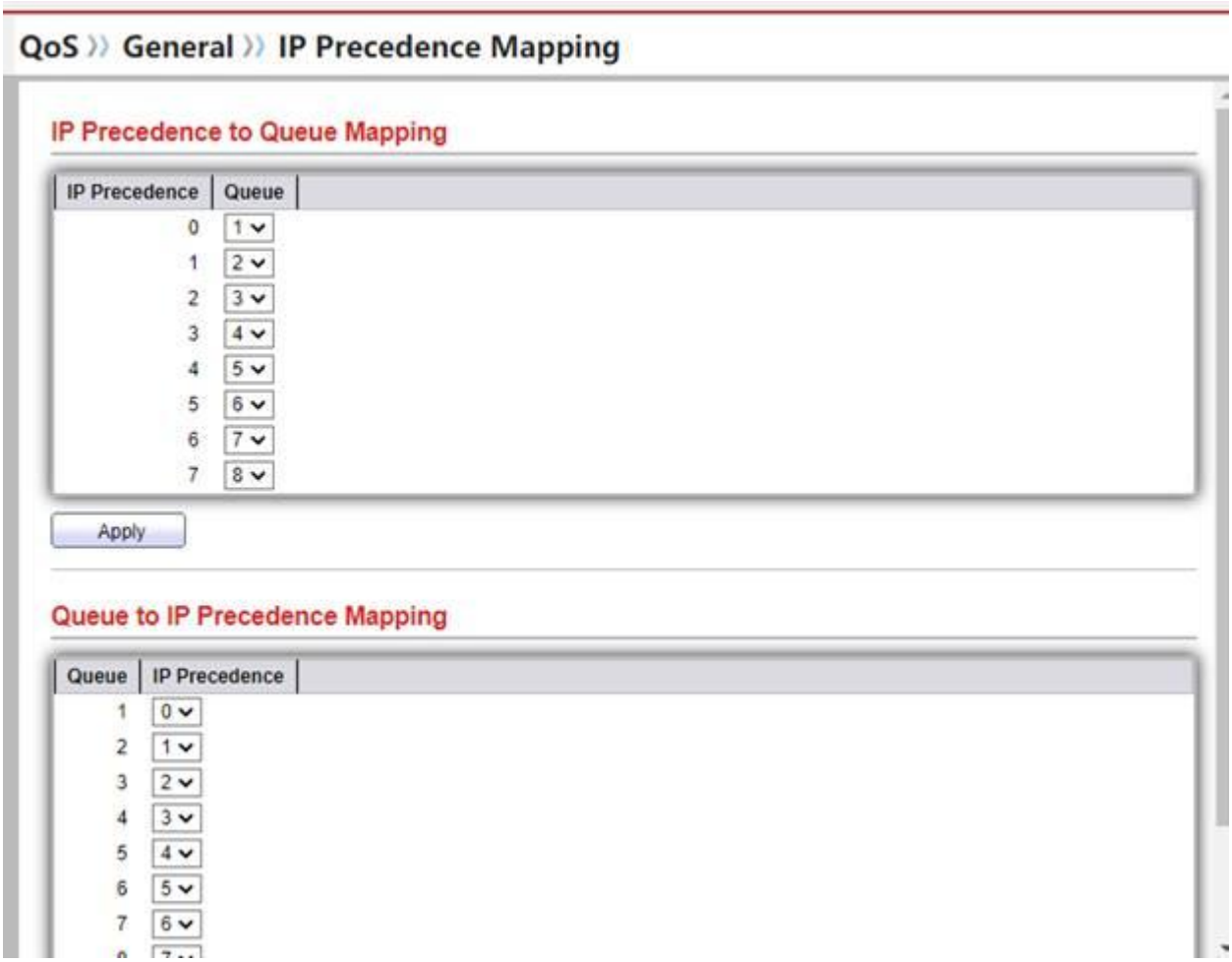
3. Select [cos mapping / general / QoS] in the navigation bar to enter the cos mapping setting interface, as shown below:



4. Select [DSCP mapping / general / QoS] in the navigation bar to enter the DSCP mapping setting interface, as shown below:



5. Select [IP priority mapping / general / QoS] in the navigation bar to enter the IP priority mapping setting interface, as shown below:

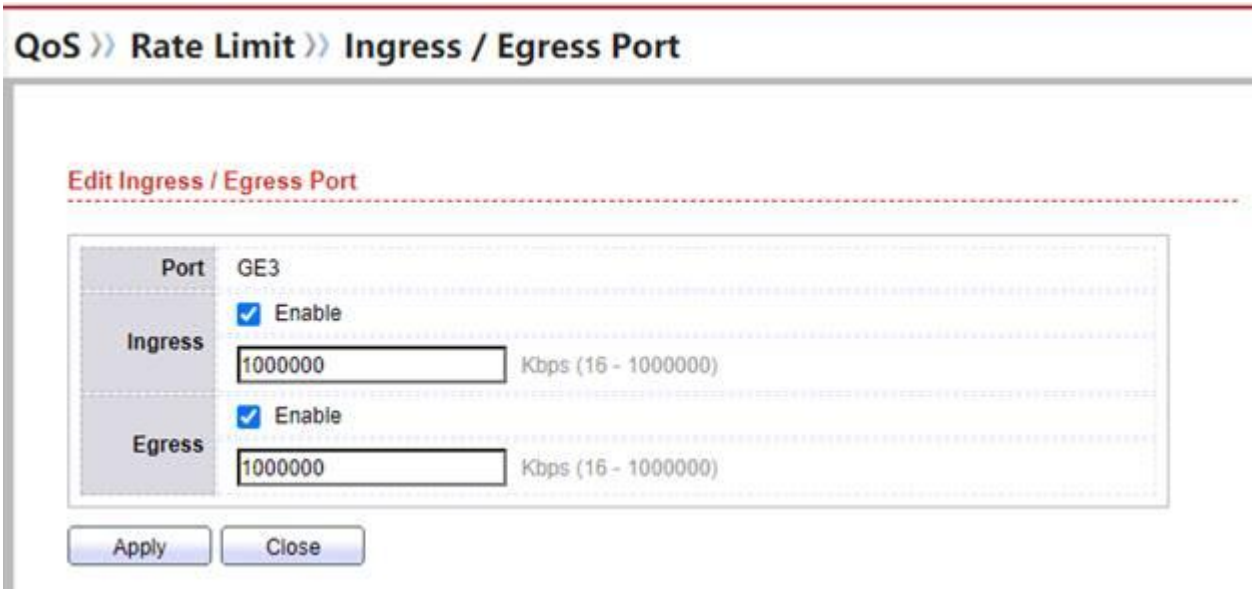


14.7 Bandwidth speed limit

14.7.1 line rate

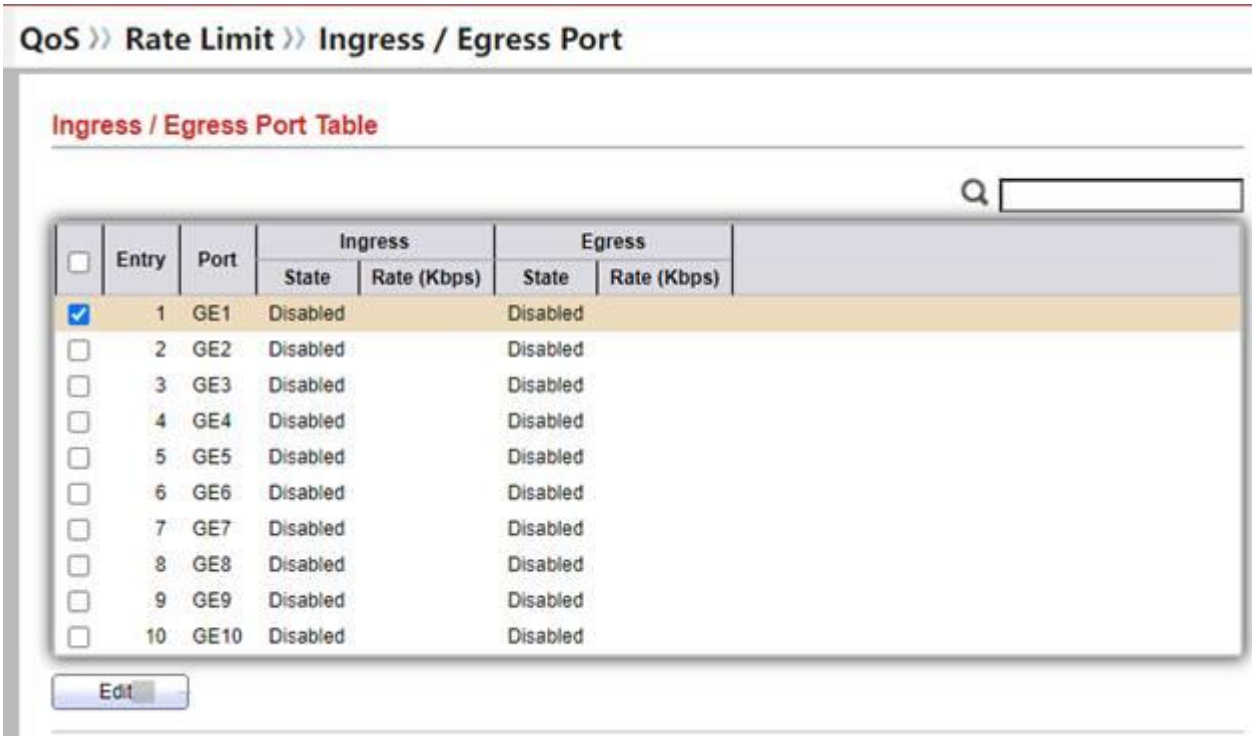
Configuration steps

1Select [rate limit / QoS] in the navigation bar, and you can view the speed limit related configuration of the port in the [progress / progress port] interface. If you need to modify the speed limit configuration of the port, check the corresponding port and click the button below Edit Button to enter the port speed limit setting interface, as shown in the figure below.



14.7.2 Exit queue speed limit

1Select [rate limit / QoS] in the navigation bar, and you can view the speed limit related configuration in the [progress queue] interface, as shown below:



Chapter 15 Equipment diagnosis

15.1 Log function

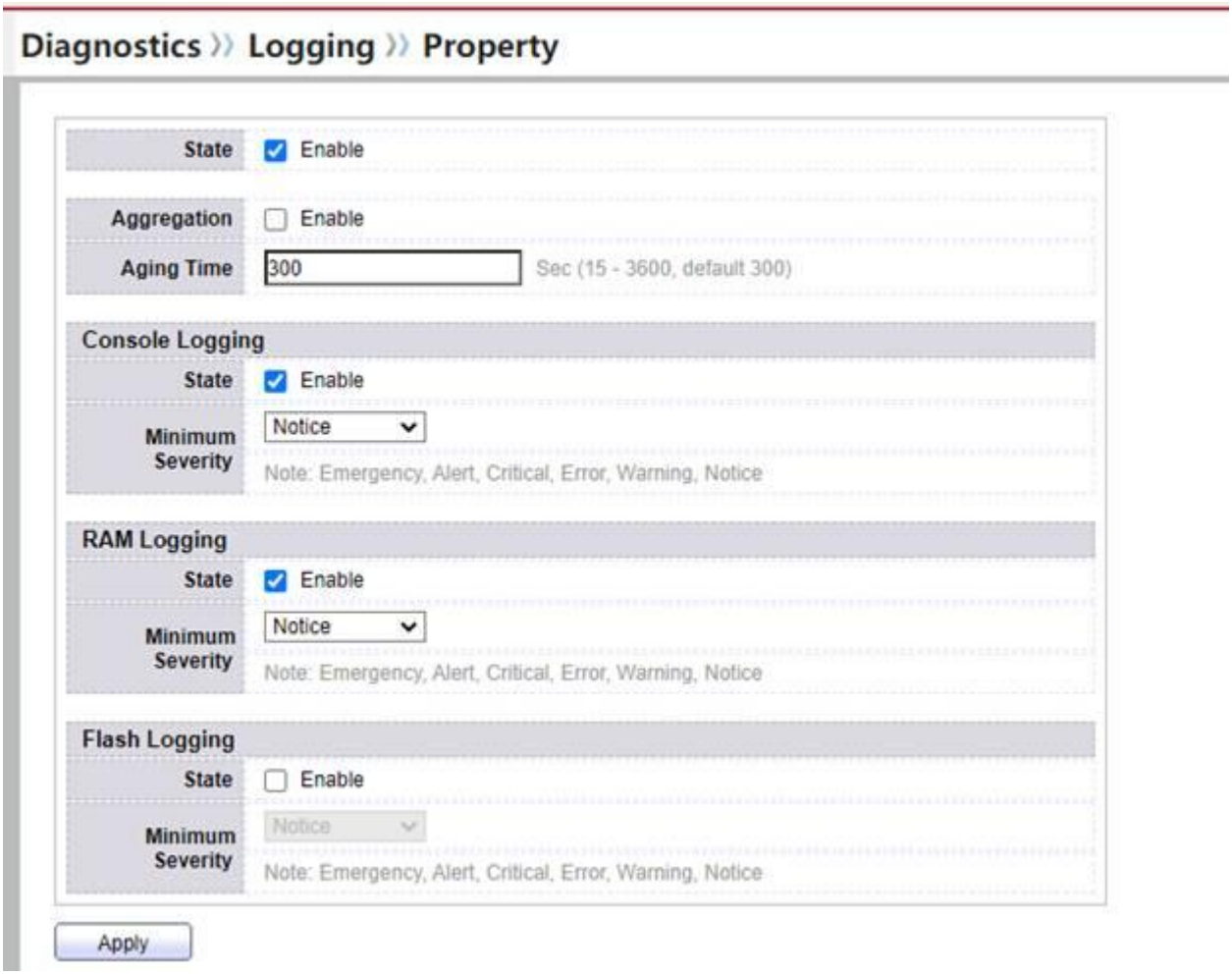
15.1.1 Introduction to log function

Log system is an indispensable part of Ethernet switch. It is the information hub of system software module.The log system manages most of the information output, and can carry out detailed classification, so as to effectively filter the information.By combining with debugging program, the log system provides strong support for network administrators and developers to monitor network operation and diagnose network faults.

15.1.2 Log function settings

Configuration steps

1. Select [property / logging / diagnostic] in the navigation bar to enter the log function configuration interface, as shown in the following figure.



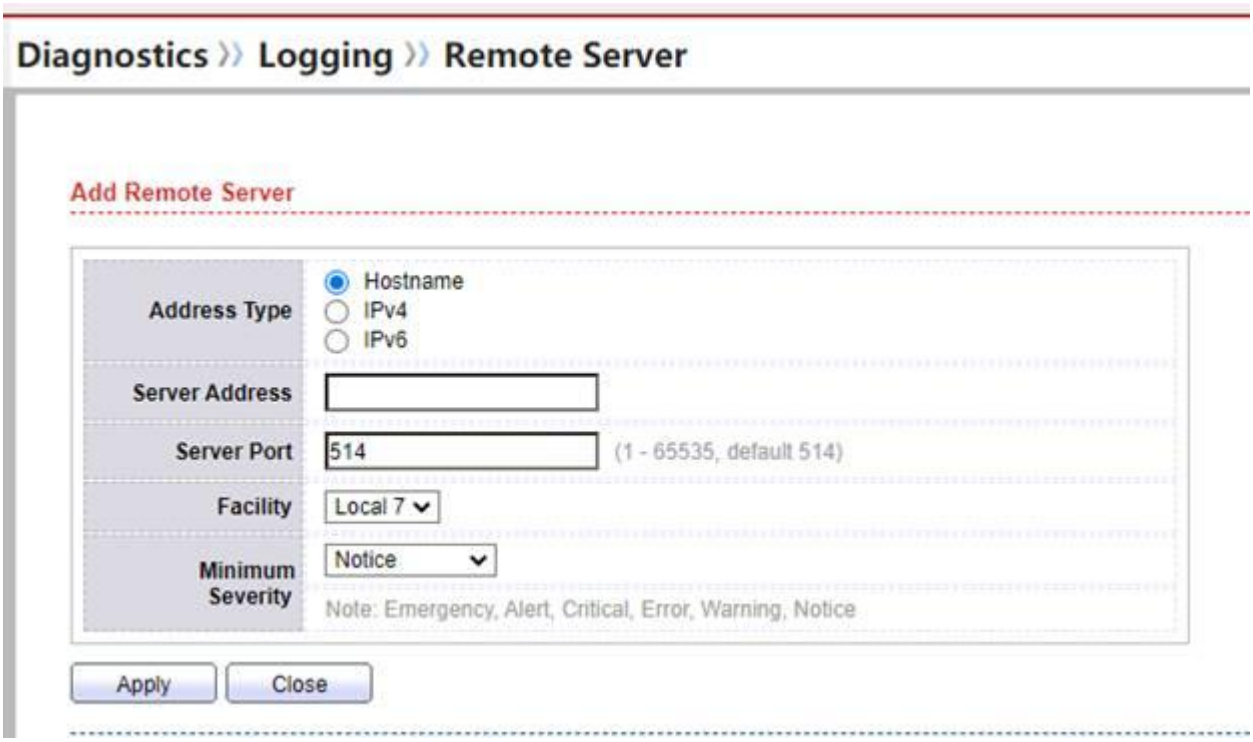
Configuration item description

Configuration item	explain
State	Status to judge whether the log system is enabled
Aggregation	Information merging
Console Logging	Determine whether the console log is enabled
RAM Logging	Judge whether ram log is enabled
Flash Logging	Judge whether flash log is enabled

15.1.3 Log function remote server configuration

Configuration steps

1.Select [remote server / logging / diagnostic] in the navigation bar to enter the remote server configuration interface and click Add Button to add a remote server, as shown in the figure below.



15.2 Mirror function

15.2.1 Introduction to port mirroring

The port mirroring function monitors the network by forwarding the data traffic of one or more source ports to a specified port on the switch or router. The specified port is called "mirror port" or "destination port". Without seriously affecting the normal throughput traffic of the source port,The network traffic can be monitored and analyzed through the image port.Using the image function in the enterprise can well monitor and manage the internal network data of the enterprise, and can quickly locate the fault in case of network failure.

15.2.2 Introduction to port mirroring technology

The function of mirroring is simply to mirror the monitored traffic to the monitoring port for fault location, traffic analysis, traffic backup, etc. the monitoring port is generally directly connected to the monitoring host.

Monitor all data packets in and out of the network for the management server installed with monitoring software to capture data. If Internet cafes need to provide this function, send the data to the public security department for review.For the needs of information security and protecting company secrets, enterprises also urgently need a port in the network to provide this real-time monitoring function.Using the port mirroring function in the enterprise can well monitor and manage the internal network data of the enterprise, and can well locate the fault in case of network failure.

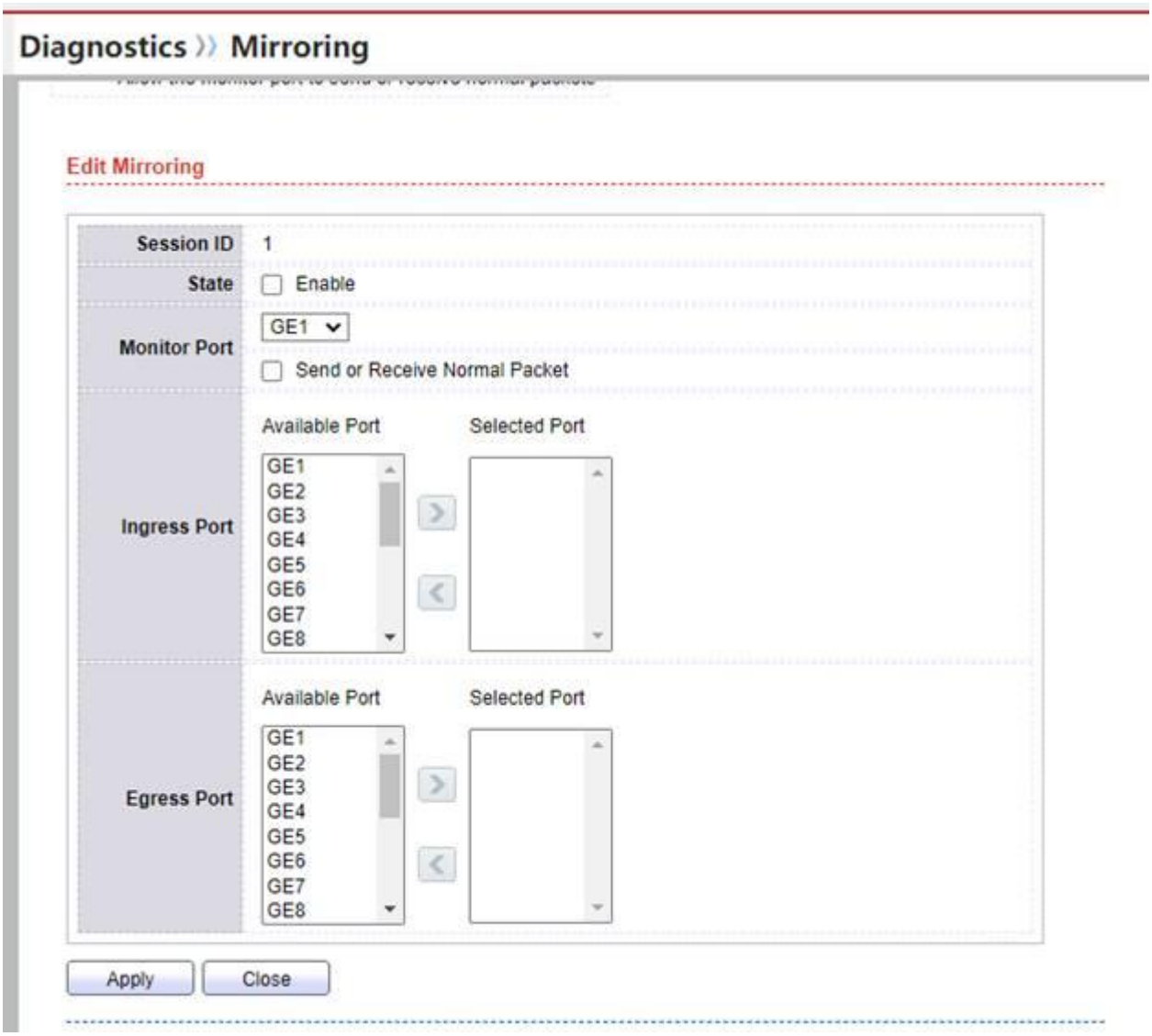
(Note: the switch copies the same data frames received or sent by one port to another port; the copied port is called the mirror source port, and the copied port is called the mirror destination port)

15.2.3 Port mirroring configuration

Configuration steps

1. Select [mirroring / diagnostics] in the navigation bar to enter the port mirroring configuration interface, select an option and click 

Button, as shown in the figure below.



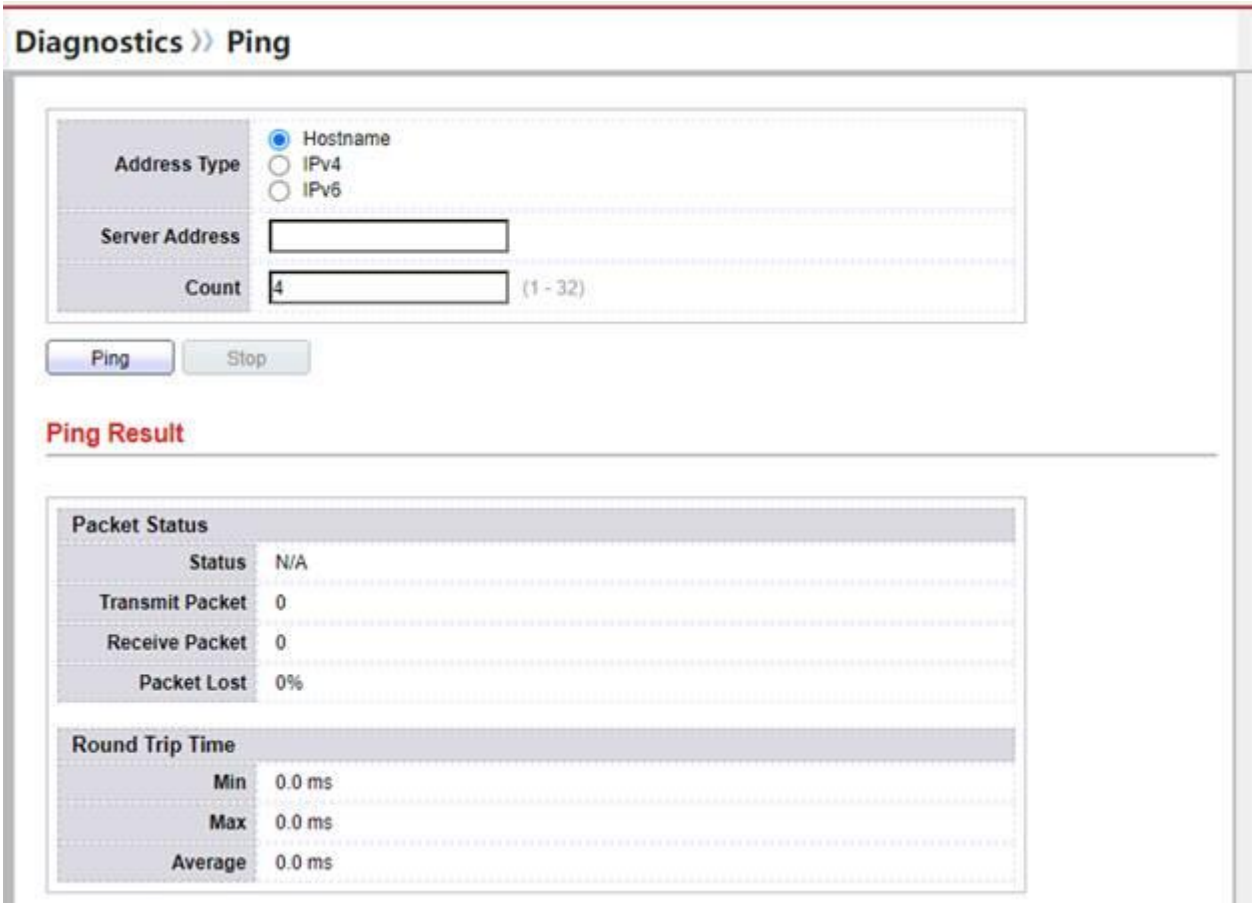
Configuration item description

Configuration item	explain
Session ID	The session ID of the mirroring function. Currently, only 4 session IDs are supported
State	Whether the mirroring function is enabled
Monitor Port	Destination port, the port of your image
Ingress Port	Select the source port in the entry direction
Egress Port	Select the source port in the exit direction

15.3 PING

Configuration steps

1. Select [Ping / diagnostics] in the navigation bar. This interface has the function of Ping package and can display Ping package data, as shown in the following figure:



15.4 UDLD

15.4.1 UDLD introduction

It is a private layer-2 protocol used to monitor the physical configuration of the Ethernet link using optical fiber or connection. When there is a one-way link (which can only be transmitted in one direction, for example, I can send data to you and you can receive it, but I can't receive the data you send to me), UDLD can detect this situation, close the corresponding interface and send a warning message.Unidirectional links can cause many problems, especially loopback.Note: UDLD needs the support of devices at both ends of the link to operate normally.Cisco twisted pair spanning tree

15.4.2 UDLD configuration

Configuration steps

1.Select [property / UDLD / diagnostics] in the navigation bar to enter the UDLD configuration interface. To change the port mode, select a port option and click Edit Button, as shown below:

Configuration item description

Configuration item	explain
Mode	UDLD port operating mode ı Disabled - port inoperative ı Normal - when a unidirectional link is found, this port will be marked as undetermined ı Aggressive - when the neighbor is lost, UDLD will actively re-establish the connection with the neighbor. After 8 attempts, the port state will become disabled

Chapter 16 device management

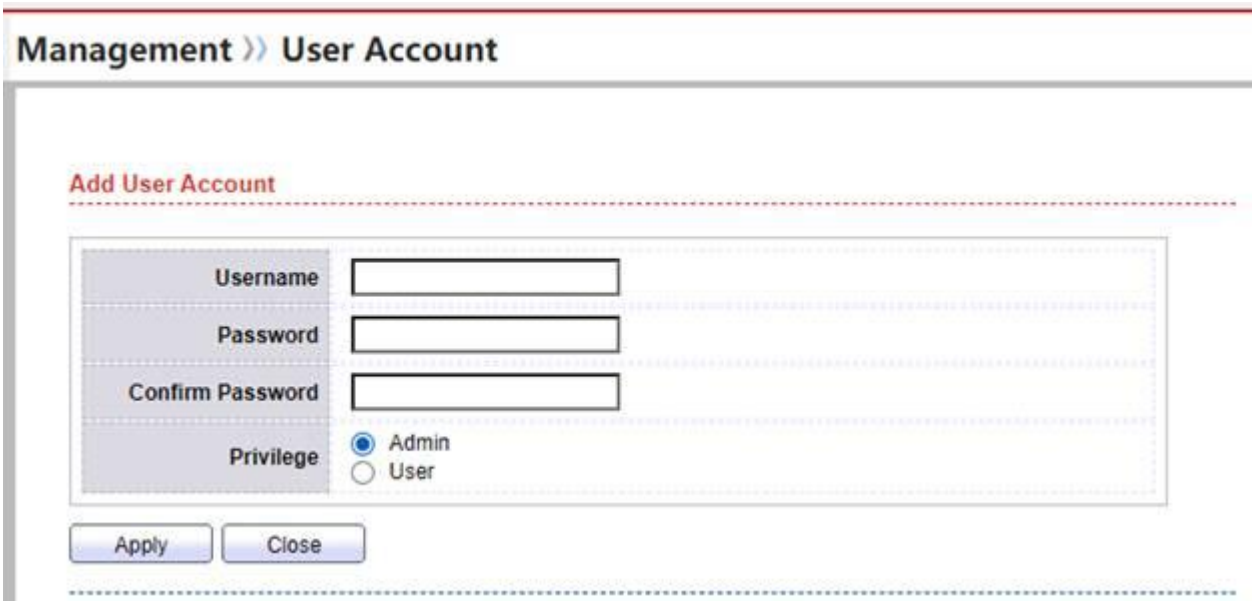
16.1 user management

Configuration steps

1. Select [user account / management] in the navigation bar to enter the user configuration interface;

2. To add a user, click in the configuration interface Add, enter the add user interface, as shown below:

Note: in the privile option, admin means administrator and user means user;These two permissions are different.



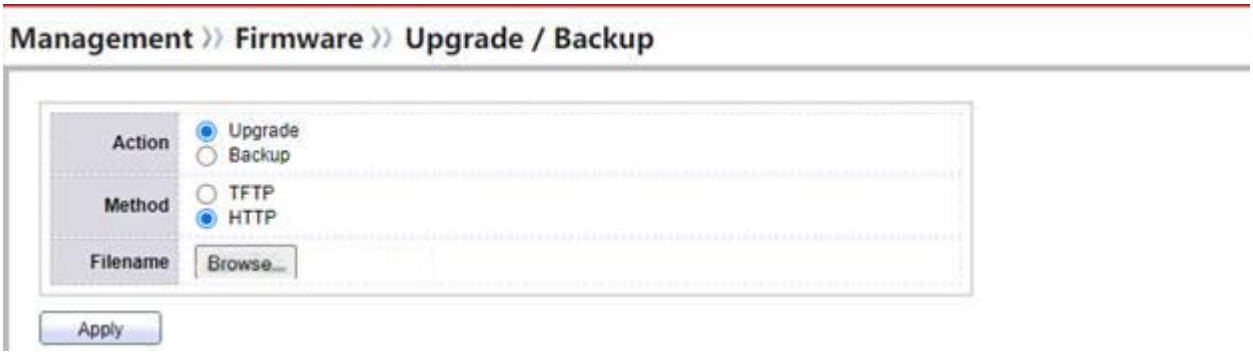
3. To change the password, click on the configuration interface Edit Button to enter the password modification page, similar to the above figure.

4. To delete a user, select the user to delete on the configuration page, and then click Delete, delete the user. The default administrator cannot delete it.

16.2 Firmware management

Configuration steps

1. Select [upgrade / firmware / management] in the navigation bar to enter the software upgrade interface, as shown below:



Click "Browse", select the firmware to be upgraded, and then click Apply Button, the following page will be prompted:

After loading, the following prompt will appear, as shown in the figure:

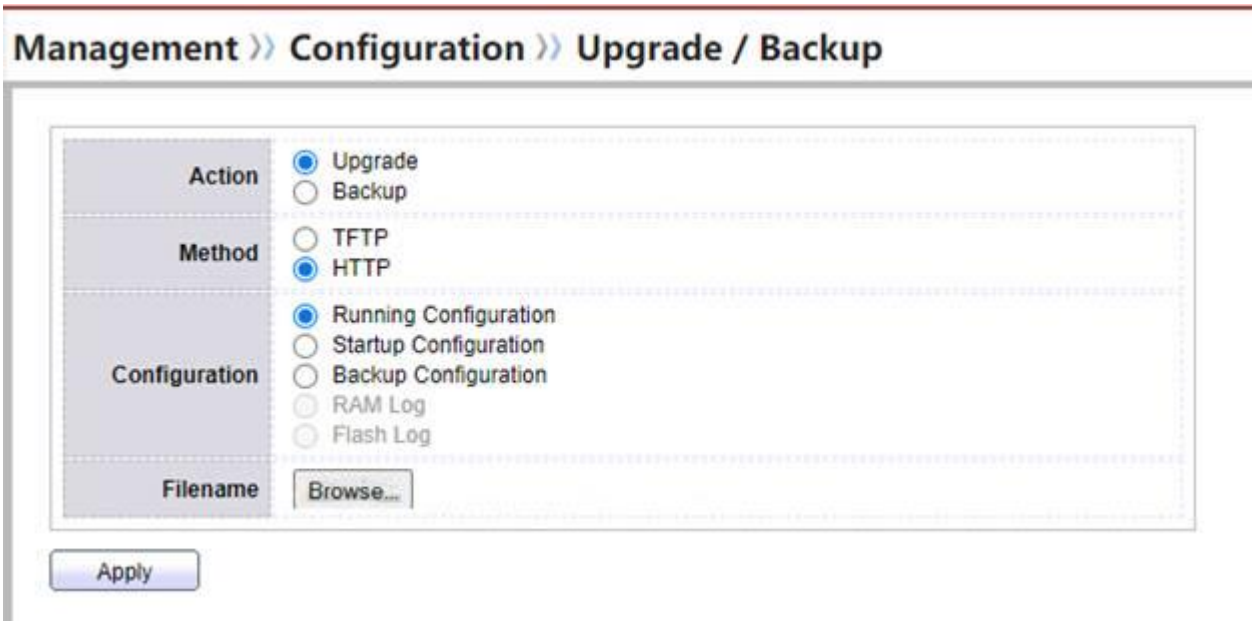
The page as shown in the figure above appears, that is, the upgrade is successful. You need to click the "reboot" button in the red box to load the new firmware.

16.3 configuration management

16.3.1 Import profile

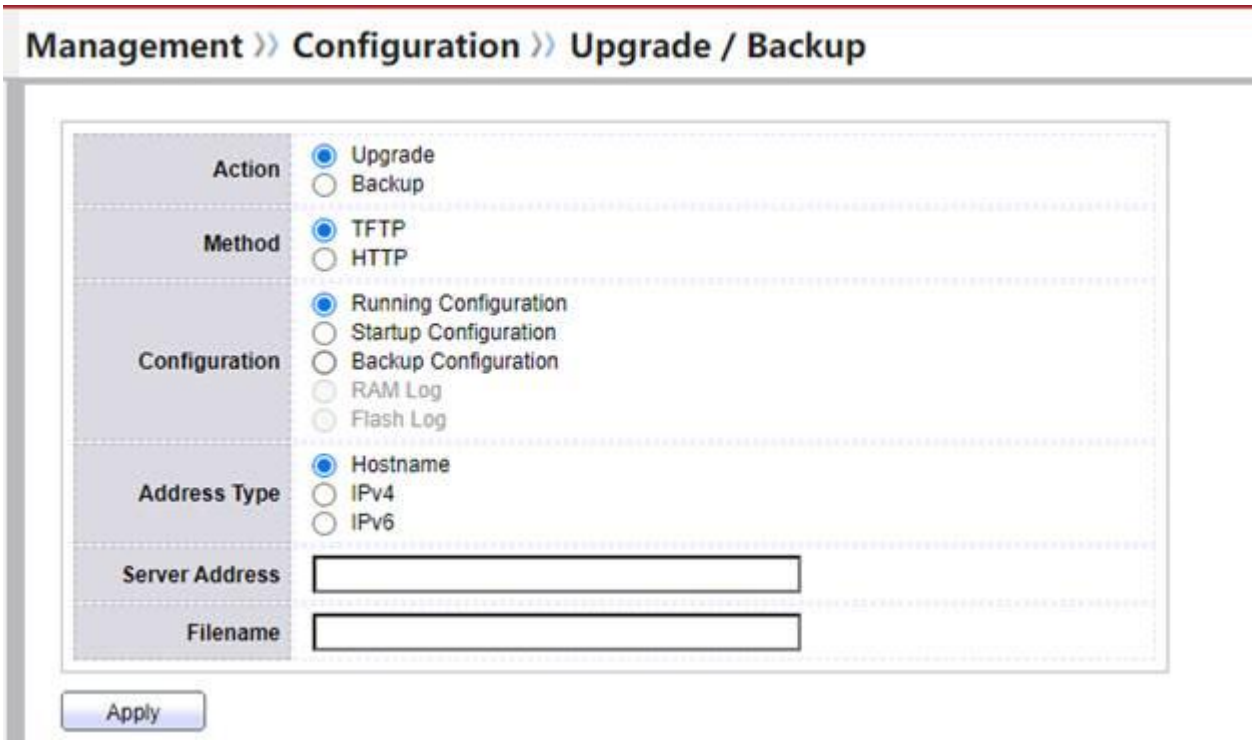
Configuration steps

1.Select [upgrade / configuration / management] in the navigation bar to enter the import configuration interface, as shown below



This page imports the configuration file through HTTP. Click the "Browse" button and select the configuration file to be imported.

To import the configuration file in TFTP mode, see the following figure:



16.4 SNMP

16.4.1 SNMPsummary

Simple network management protocol (SNMP) is composed of a set of network management standards, including an application layer protocol, a database schema and a set of resource objects.The protocol can support the network management system to monitor whether the devices connected to the network have any management concerns.The protocol is a part of the Internet Protocol cluster defined by the Internet Engineering Task Force (IETF).The goal of SNMP is to manage the software and hardware platforms produced by many manufacturers on the Internet. Therefore, SNMP is also greatly affected by the Internet standard network management framework.SNMP has been released to the third version of the protocol.

16.4.2 introduction to SNMP Technology

SNMP is a network management standard based on TCP / IP protocol family. It is a standard protocol for managing network nodes (such as servers, workstations, routers, switches, etc.) in IP network.SNMP can enable network administrators to improve network management efficiency, find and solve network problems in time and plan network growth.Network administrators can also receive notification messages and alarm event reports from network nodes through SNMP to learn about network problems.

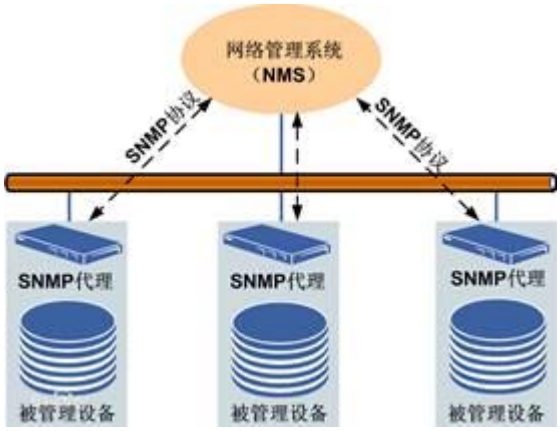


Figure 15.1 SNMP management network topology composition

The network managed by SNMP is mainly composed of three parts:

1.Managed devices

2. SNMP agent

3.Network management system (NMS)

The relationship between them is shown in Figure 15.1:

1.Every device managed in the network has a standard management information base (MIB) for collecting and storing management information.NMS can obtain this information through SNMP protocol.The managed device, also known as network unit or network node, can be a router, switch, server or host that supports SNMP protocol.

2. SNMP agent is a network management software module on the managed device. It has the relevant management information of the local device and is used to convert them into a format compatible with SNMP and transfer them to NMS.

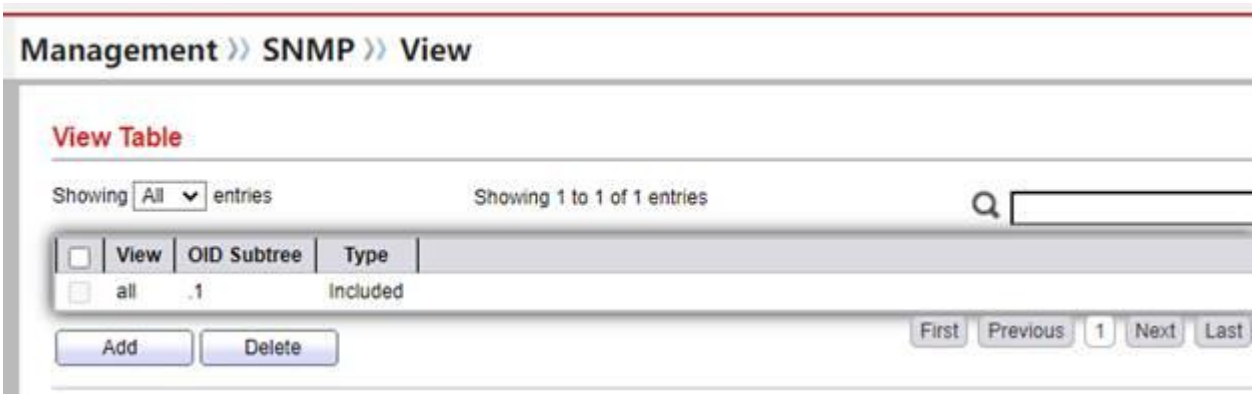
3. NMS runs the application program to realize the function of monitoring the managed equipment.In addition, NMS also provides a large number of processing programs and necessary storage resources for network management.

16.4.3 SNMP configuration

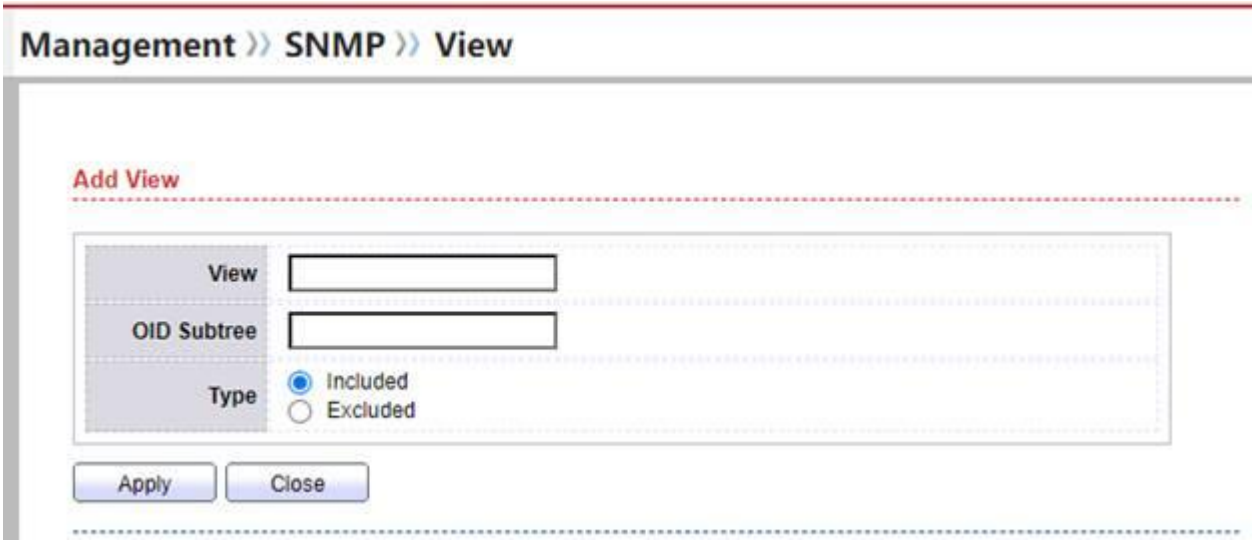
16.4.3.1 View configuration

Configuration steps

1. Select [view / SNMP / management] in the navigation bar to enter the SNMP view configuration interface, as shown in the following figure:



To add a view configuration, click Add Button to enter the add SNMP view page, as shown in the following figure:



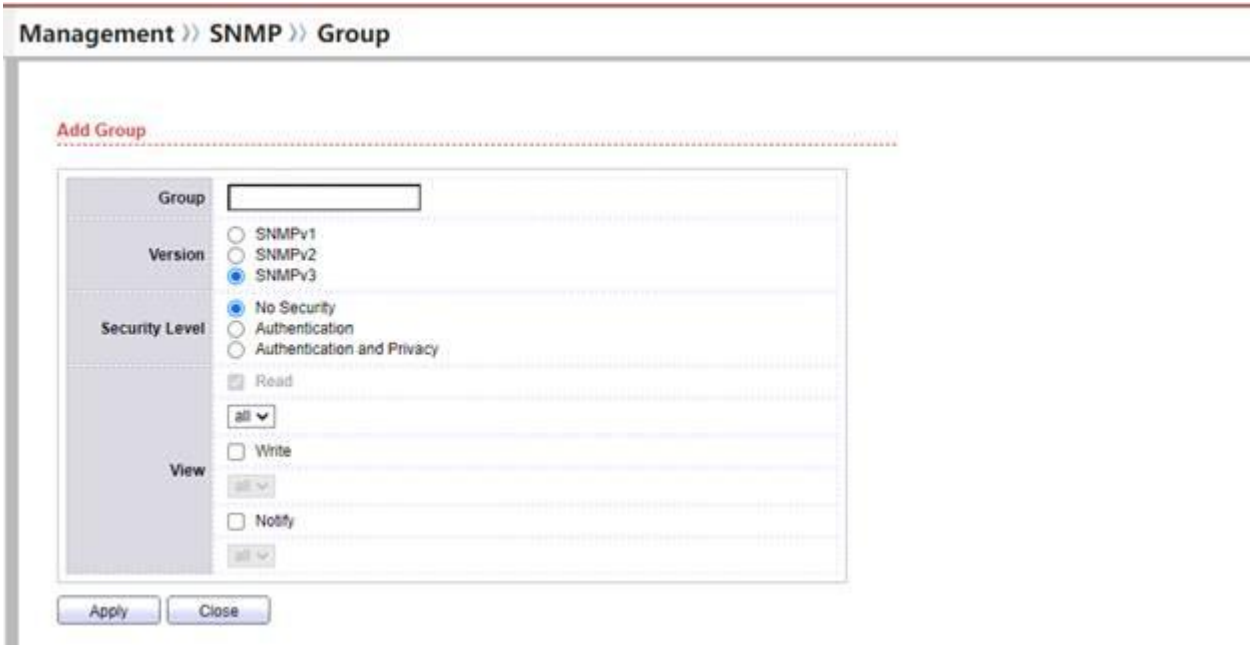
After the configuration is set, you need to click the Apply button in the figure to change and save.

16.4.3.2 Group configuration

Configuration steps

1.Select [group / SNMP / management] in the navigation bar to enter the SNMP group configuration interface, as shown in the following figure:

To add a group configuration, click Add Button to enter the add SNMP group page, as shown in the following figure:

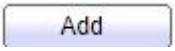


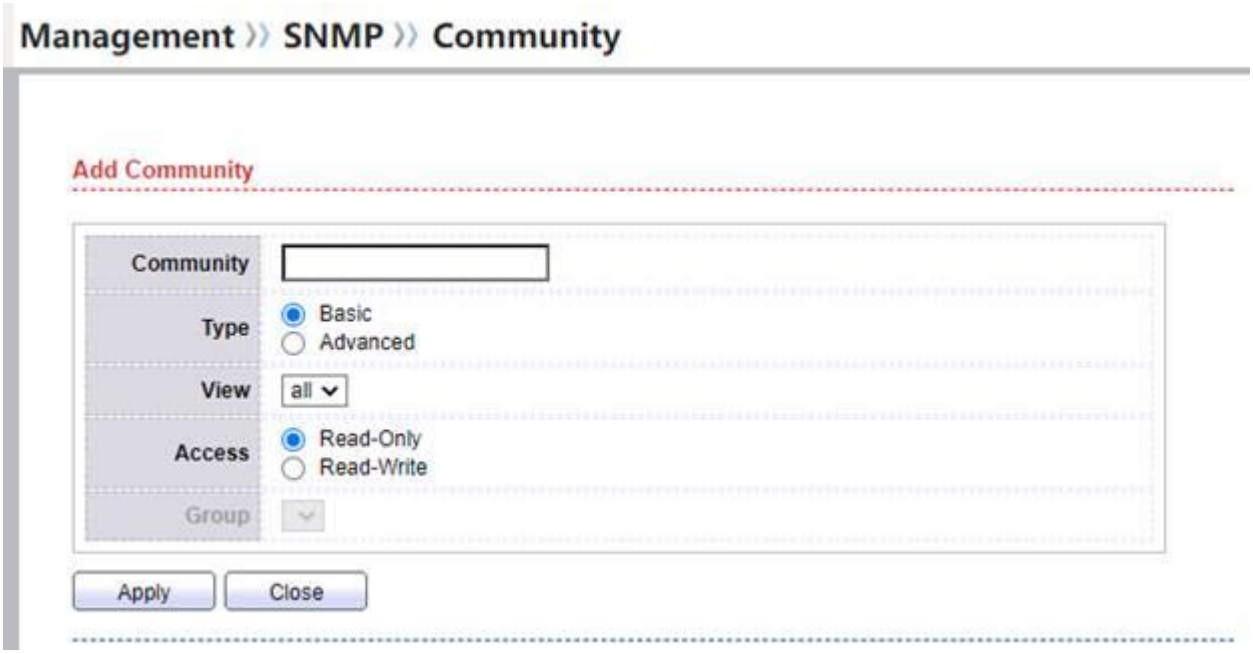
After the configuration is set, you need to click the Apply button in the figure to change and save.

16.4.3.3 Group configuration

Configuration steps

1.Select [community / SNMP / management] in the navigation bar to enter the SNMP community configuration interface, as shown in the following figure:

To add a group configuration, click  Button to enter the add SNMP community page, as shown in the following figure:



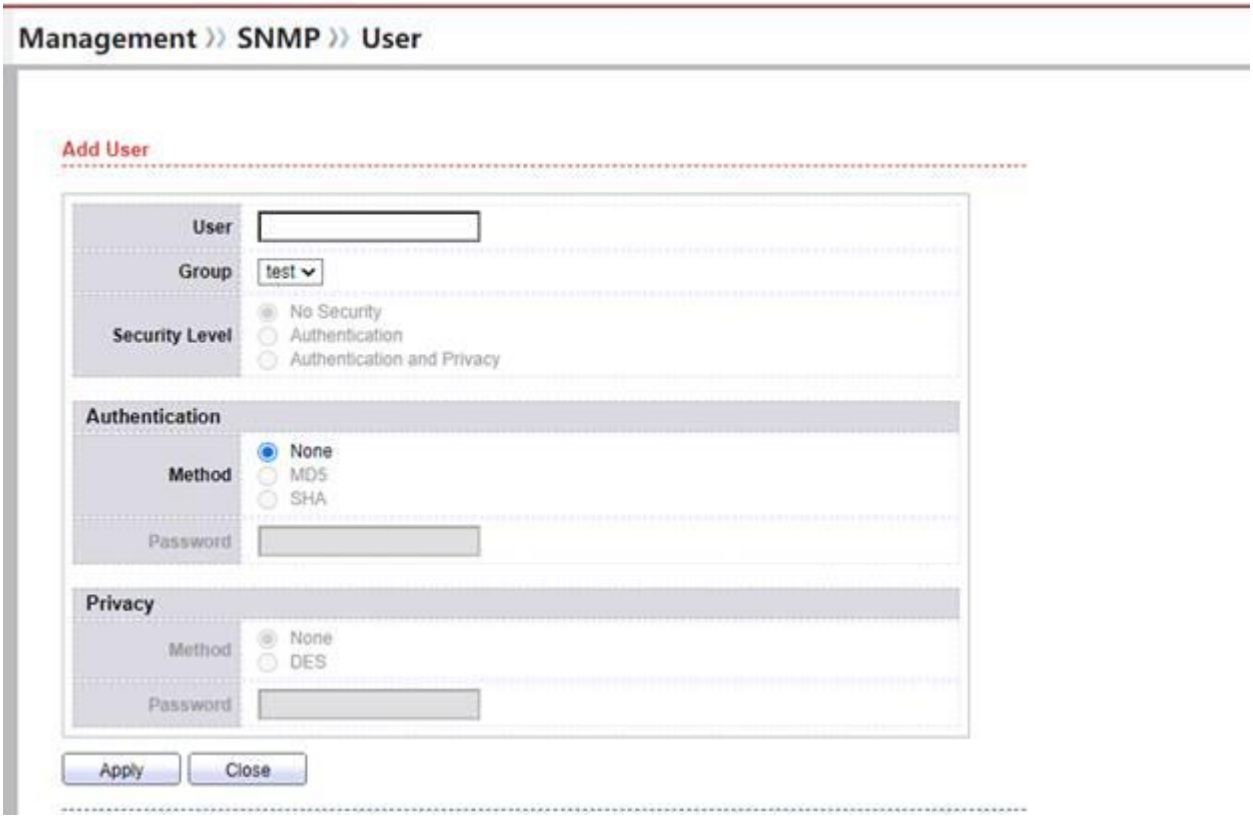
After the configuration is set, you need to click the Apply button in the figure to change and save.

16.4.3.4 User configuration

Configuration steps

1.Select [user / SNMP / management] in the navigation bar to enter the SNMP user configuration interface, as shown in the following figure:

To add a user profile, click Add Button to enter the add SNMP user page, as shown in the following figure:

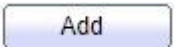


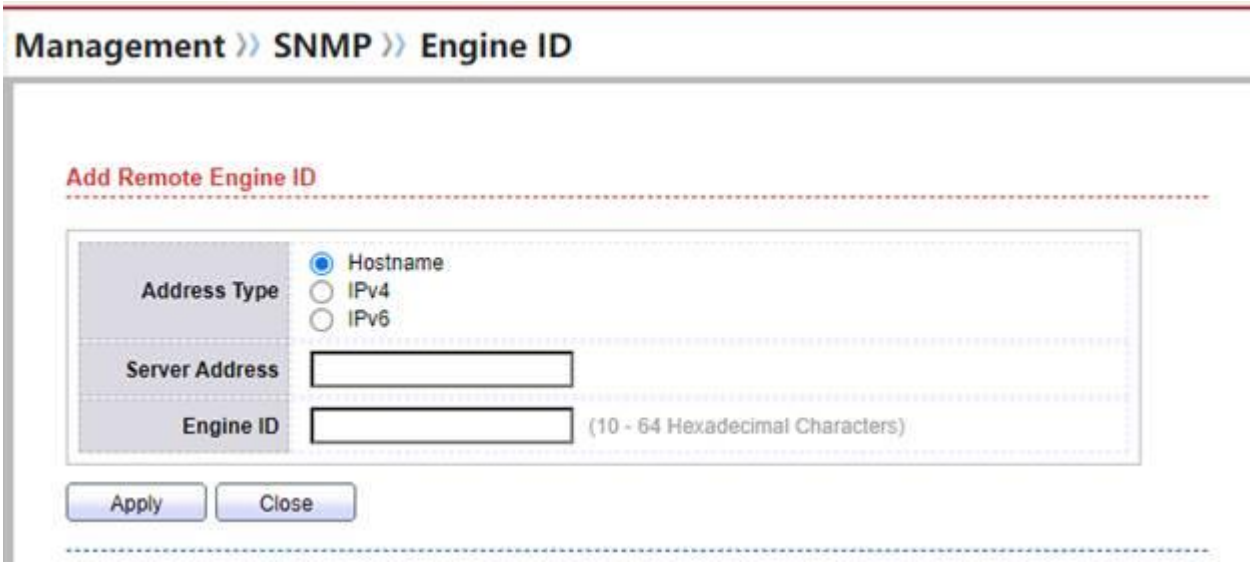
After the configuration is set, you need to click the Apply button in the figure to change and save.

16.4.3.5 engine ID configuration

Configuration steps

1.Select [engine ID / SNMP / management] in the navigation bar to enter the SNMP engine ID configuration interface, as shown in the following figure:

To add a user profile, click  Button to enter the page of adding SNMP engine ID, as shown in the following figure:

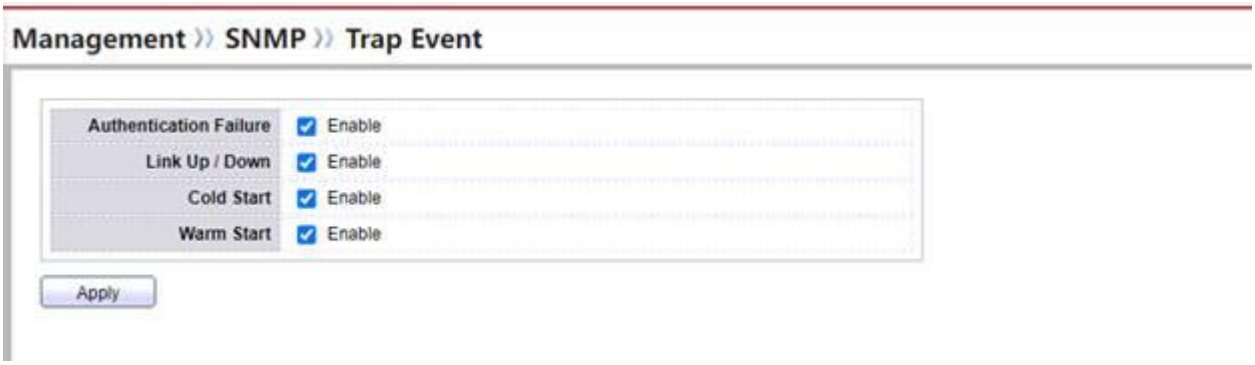


After the configuration is set, you need to click the Apply button in the figure to change and save.

16.4.3.6 trap configuration

Configuration steps

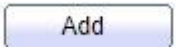
1.Select [trap event / SNMP / management] in the navigation bar to enter the SNMP trap configuration interface, as shown in the following figure:



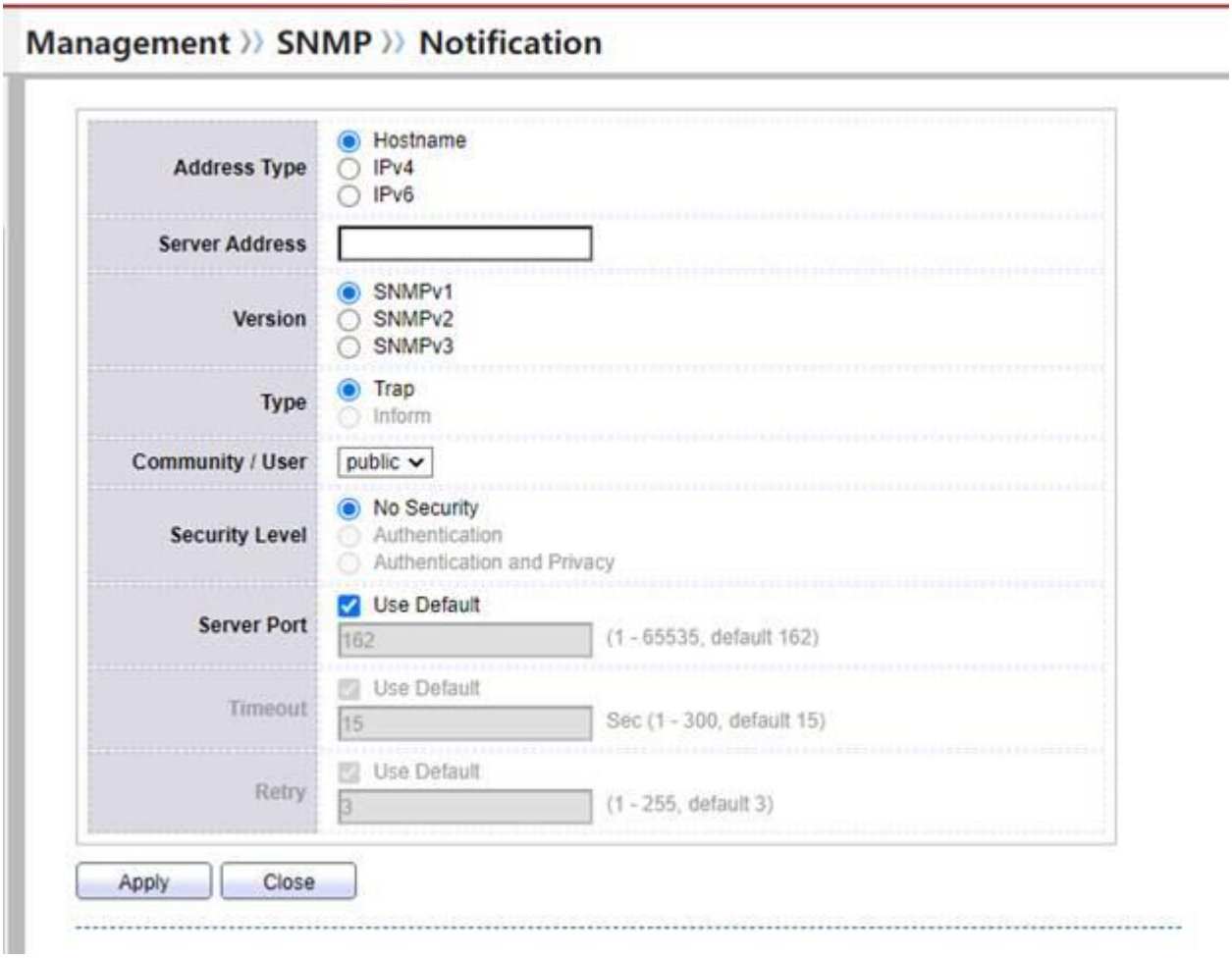
16.4.3.7 notification configuration

Configuration steps

1.Select [notification / SNMP / management] in the navigation bar to enter the SNMP trap configuration interface, as shown in the following figure:

To add a configuration, click 

Button to enter the add SNMP notification page, as shown in the following figure:



After the configuration is set, you need to click the Apply button in the figure to change and save.

16.5 RMON

16.5.1 overview of RMON

RMON (remote network monitoring) remote end is originally designed to solve the problem of managing local area networks and from one central point.RMON specification is extended from MIB.In RMON, network monitoring data includes a set of statistical data and performance indicators, which are exchanged between different monitors (or detectors) and console systems.The resulting data can be used to monitor network utilization, optimize performance and assist in network error diagnosis.Network monitoring remote site SNMP network planning

SNMP is the basis of RMON implementation, and RMON is the enhancement of SNMP function.RMON uses the SNMP trap message sending mechanism to send a trap message to the management device to inform the exception of the alarm variable.Although SNMP also defines the trap function, it is usually used to inform whether a function on the managed device is running normally and the physical state of the interface changes. The monitored objects, trigger conditions and report contents of the two devices are different.

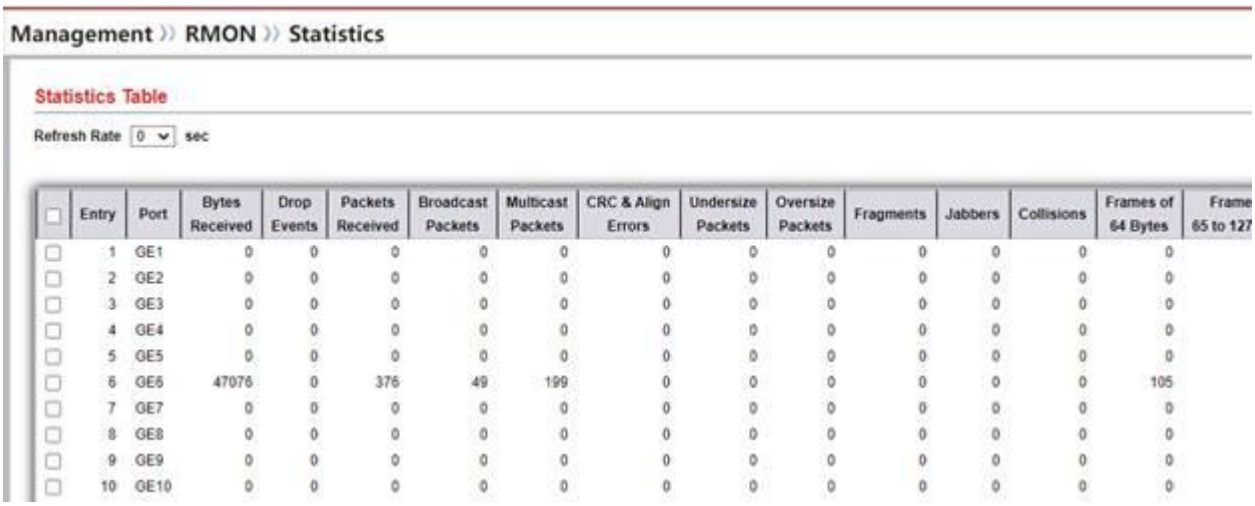
RMON enables SNMP to monitor remote network devices more effectively and actively, and provides an efficient means to monitor the operation of subnet.RMON protocol stipulates that when the alarm threshold is reached, the managed device can automatically send trap information, so the management device does not need to obtain the value of MIB variable for comparison for many times, so as to reduce the communication flow between the management device and the managed device and achieve the purpose of simple and powerful management of large-scale interconnection network.

16.5.2 RMON configuration

16.5.2.1 packet statistics

Configuration steps

1.Select [statistics / RMON / management] in the navigation bar to enter the RMON message statistics interface, as shown in the following figure:



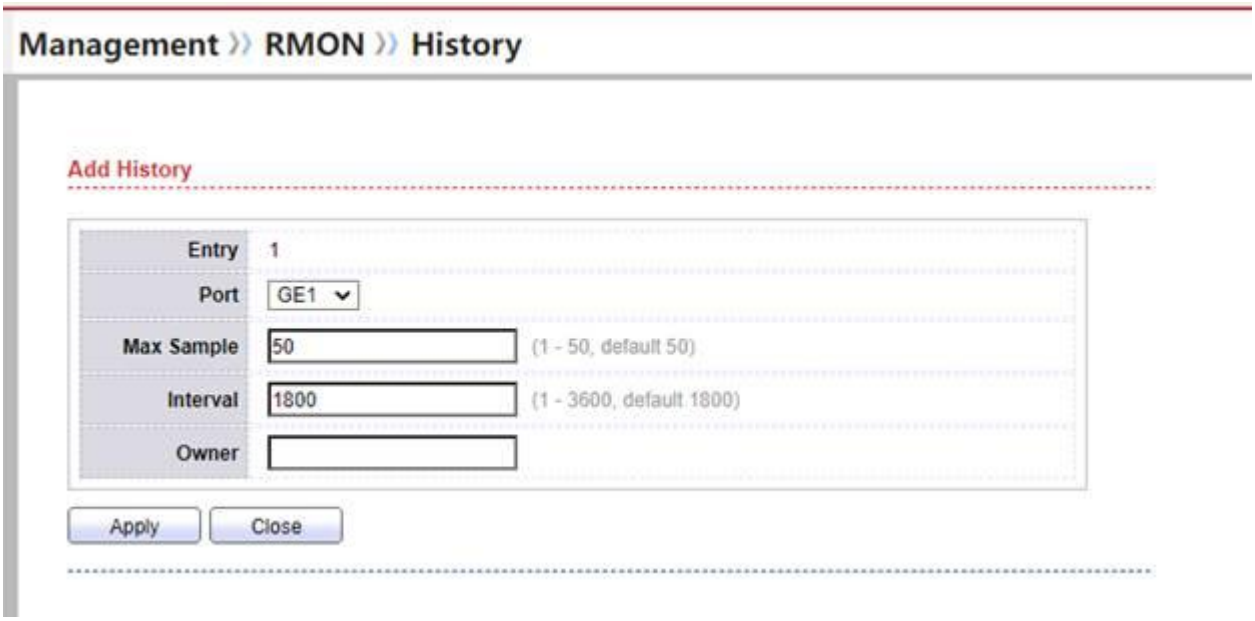
Entry	Port	Bytes Received	Drop Events	Packets Received	Broadcast Packets	Multicast Packets	CRC & Align Errors	Undersize Packets	Oversize Packets	Fragments	Jabbers	Collisions	Frames of 64 Bytes	Frame 65 to 127
1	GE1	0	0	0	0	0	0	0	0	0	0	0	0	
2	GE2	0	0	0	0	0	0	0	0	0	0	0	0	
3	GE3	0	0	0	0	0	0	0	0	0	0	0	0	
4	GE4	0	0	0	0	0	0	0	0	0	0	0	0	
5	GE5	0	0	0	0	0	0	0	0	0	0	0	0	
6	GE6	47076	0	376	49	199	0	0	0	0	0	0	105	
7	GE7	0	0	0	0	0	0	0	0	0	0	0	0	
8	GE8	0	0	0	0	0	0	0	0	0	0	0	0	
9	GE9	0	0	0	0	0	0	0	0	0	0	0	0	
10	GE10	0	0	0	0	0	0	0	0	0	0	0	0	

16.5.2.1 Historical configuration

Configuration steps

1.Select [History / RMON / management] in the navigation bar to enter the RMON history configuration interface, as shown in the following figure:

To add a configuration, click Add Button to enter the page of adding RMON history configuration, as shown in the following figure:

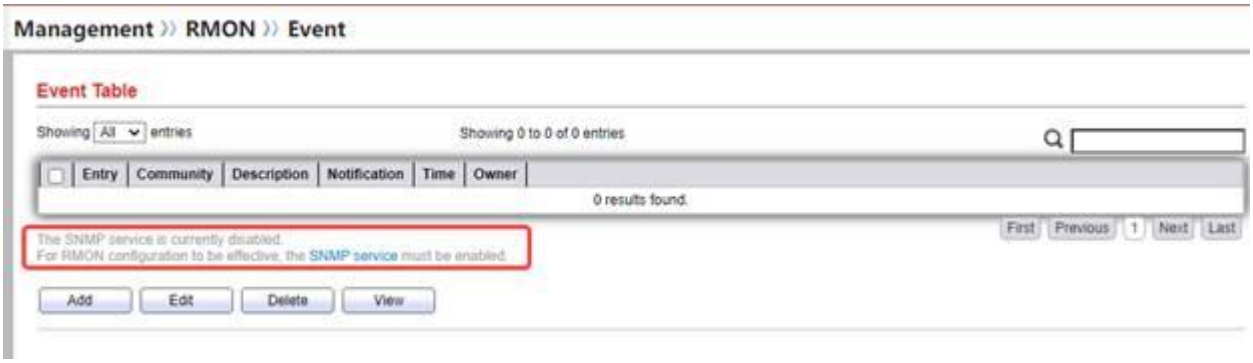


After the configuration is set, you need to click the Apply button in the figure to change and save.

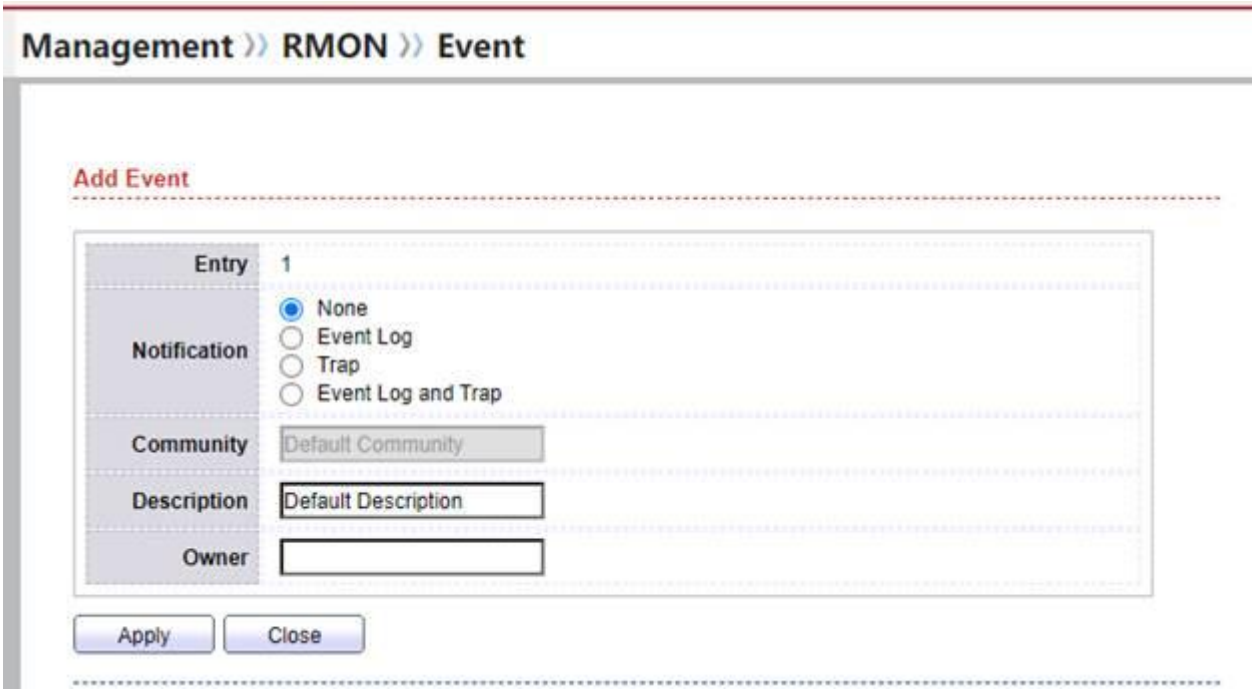
16.5.2.1 Event configuration

Configuration steps

1.Select [event / RMON / management] in the navigation bar to enter the RMON event configuration interface, as shown below:



To add a configuration, click Add Button to enter the add RMON event configuration page, as shown in the following figure:

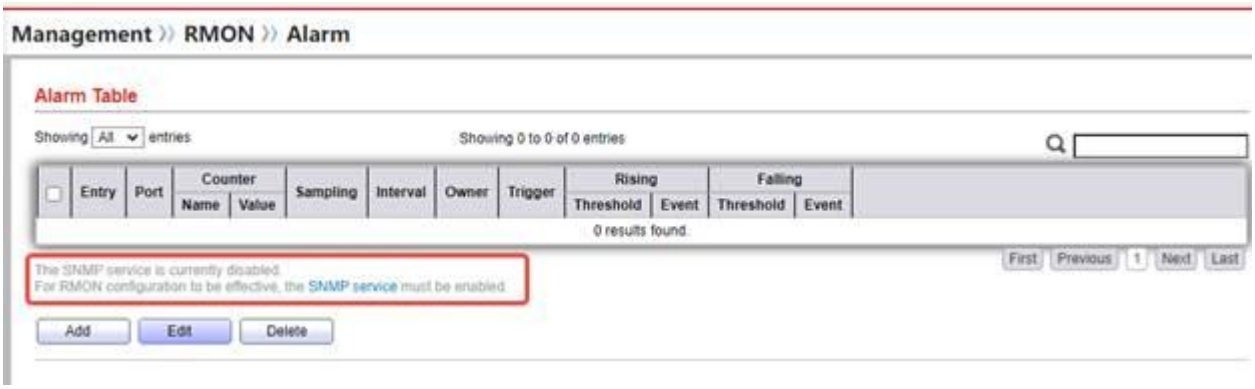


After the configuration is set, you need to click the Apply button in the figure to change and save.

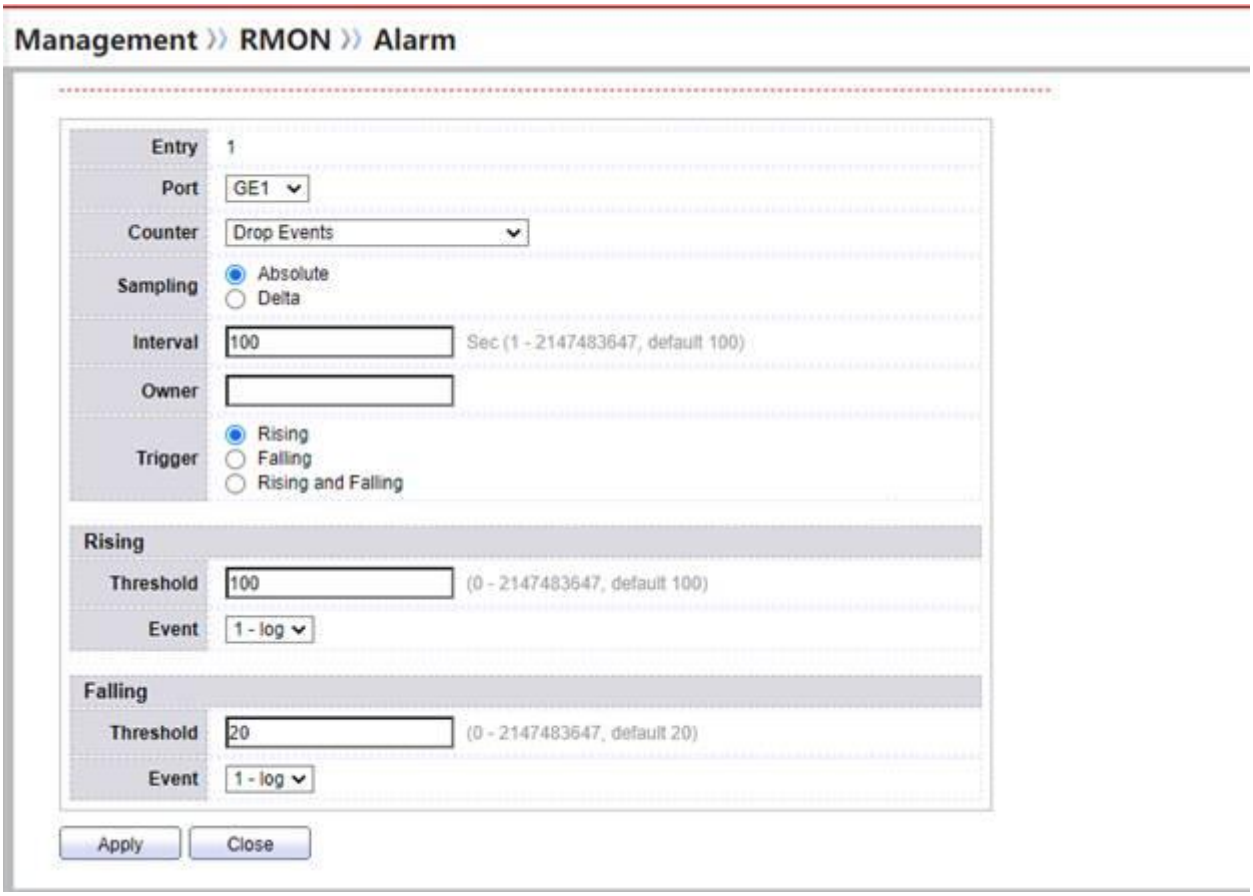
16.5.2.1 Alarm configuration

Configuration steps

1.Select [alarm / RMON / management] in the navigation bar to enter the RMON alarm configuration interface, as shown in the following figure:



To add a configuration, click Add Button (event configuration is required before alarm configuration) to enter the page of adding RMON alarm configuration, as shown in the following figure:



After the configuration is set, you need to click the Apply button in the figure to change and save.