ORIGO

L2 Switch Series

OS6208/OS6208F

User Manual

Introduction:

This manual is provided for this type of switch, which includes the performance and function of this switch. Please read this manual before managing the device.

Suitable users:

This manual is applicable to network administrators of similar IT and network technologies.

Precautions:

Do not put the product too close to water, for example, in a damp basement or near by a swimming pool. Avoid electric storm. Electric shock may occur in case of lightning.

Part 1: Product Introduction 6
1.1 Product characteristic 6
1.2 Specifications 6
Part 2: Installation 7
2.1 Precautions 7
2.2 Installation on table or shelf 7
2.3 Rack mounting 7
2.4 AC power supply 7
Part 3: Login 7
3.1 Computer Configuration 8
3.2 Connection Check 13
3.3 Login 14
3.4 Function Overview 15
Part 4: System 16
4.1 Homepage 16
4.2 Status 16
4.3 System information 17
4.4 Logging message 18
4.5 port 18
4.6 Link Aggregation Management 19
4.7 MAC Address Table 19
Part 5: Network 20
5.1 IP Address 20
5.2 System Time 21
Part 6: Network 22
6.1 Port Setting 22
6.2 Error Disabled 23
6.3 Link Aggregation 24
6.3.1 Group 26
6.3.2 Port Setting 27
6.3.3 LACP 29
6.4 EEE 29
6.5 Jumbo Frame 30
Part 7: VLAN 31
7.1 VLAN 31
7.1.1 Create VLAN 32
7.1.2 VLAN Configuration 34
7.1.3 Membership 35
7.1.4 Port Setting 36
Part 8: MAC Address Table 38
MAC address introduction 38
8.1 Dynamic Address 39
8.2 Static Address 39
8.3 MAC address filtering 42
8.4 MAC Aging time 43
Part 9: Spanning Tree 43
9.1 STP introduction 43

9.1.1 STP application 43
9.1.2 STP protocol messages 43
9.1.3 Basic concept of STP 44
9.1.4 Basic principle of STP 45
9.2 MSTP Introduction 50
9.2.1 MSTP Background 50
9.2.2 Basic Concept of MSTP 50
9.2.3 Basic principle of MSTP 54
9.2.4 Realization of MSTP on equipment 54
9.3 Protocol 55
9.4 Property 55
9.5 Port Setting 56
Part 10: ERPS(G.8032) 56
10.1 introduction 57
Definition 57
Purpose 57
Benefits 58
10.2 Principles 58
10.2.1 Basic ERPS Concepts 58
10.3 Configuration Examples 61
10.3.1 Example for Configuring ERPS Multi-instance 61
Part 11: Routing 64
11.1 IP Routing and Routing Table 64
11.1.1 Routing 64
11.1.2 Routing Through a Routing Table 64
11.2 Routing Protocol Overview 65
11.2.1 Static Routing and Dynamic Routing 65
11.2.2 Classification of Dynamic Routing Protocols 65
11.3 Static Routing Configuration 66
11.3.1 Introduction 66
11.3.2 Configuring a Static Route 67
Part 12: Security 69
12.4 Management Access 69
12.4.1 Management VLAN 69
12.4.2 Management Service 71
Part 15: Diagnostics 71
15.1 Logging 71
15.1.1 Property 71
15.2 Mirroring 73
15.3 Ping 76
15.4 Traceroute 77
15.5 Copper Test 78
Part 16: Management 80
16.1 User Account 80
16.2 Firmware 82
16.2.1 Upgrade/Backup 82
16.3 Configuration 83
16.3.1 Upgrade/Backup 83

16.3.2 Save Configuration 85
Part 17:FAQ 86
17.1 Abnormal display of connection status indicator (connection error) 86
17.2 Normal display of connection status indicator but fail to communicate 86
17.3 Unable to log on the switch 86
17.4 Switch start failure 87
17.5 Power supply failure 87

Part 1: Product Introduction

1.1 Product characteristic

- Support link aggregation
- 802.1Q VLAN Support IEEE 802.1Q VLAN
- Support rate limitation and port statistics
- Support port mirroring
- Support QoS, provide strict priority and weighted priority
- Support MAC address binding
- Support loop detection to avoid loop disaster/fault
- Support IGMP snooping
- Support WEB-based management
- Support serial management
- Support WEB-based firmware upgrade
- Support parameter backup and restore

1.2 Specifications

1.2.1 Front panel

Every port has its corresponding indicator light, LNK/ACT and 1000M bps indicator light.

CONSOLE port: Baud rate: 115200, Data bits: 8, Stop bits: 1

Indicator light:

LED	State	Function
PWR	Normal	Power on
	Off	Power off
10/100/1000M	Normal	Normal connection of corresponding port
	OFF	Abnormal connection of corresponding port
LNK/ACT	Flash	data transmission
	Normal	Normal connection of corresponding port

1.2.2 Rear panel

Power supply: power adapter socket

Part 2: Installation

2.1 Precautions

Make sure that the surface on which the device will be placed is safe enough to prevent it from becoming unstable. Make sure that the power output is 1.8m away from the device. Make sure that the device is connected to the power supply with AC power cord. Ensure good ventilation and heat dissipation around the device.
Do not place heavy objects on the device.

2.2 Installation on table or shelf

Place the switch's bottom up on the table. Install rubber feet on each corner. Turn it over and place on the table.

2.3 Rack mounting

First, install mounting racks on each side of the device with support screws, and then install the switch on the 19-inch rack.

2.4 AC power supply

The switch can use AC to supply power 100 to 240V AC, 50 to 60Hz. The built-in power supply system of the switch can automatically change the operating voltage according to the input voltage. The power connection port is on the switch's rear panel.
One end of the power cord can be plugged into the socket on the switch's rear panel, and the other can be plugged into the power output port.

Part 3: Login

Use a web-based method to configure and manage. It can be configured by web browser, and at least one PC should be connected to the Internet through Ethernet cable.

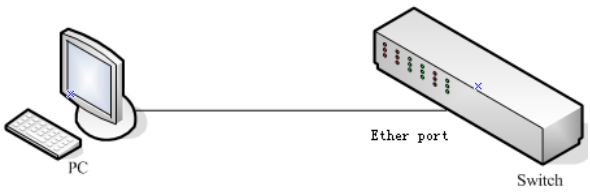


Figure 3-1

Default IP address of the switch:192.168.1.1. Subnet mask: 255.255.255.0.
When logging in the switch, make sure that the IP addresses of the host network card and the switch are in the same network segment: 192.168.1. *** (1 <*** <255， *** is not 11). See the following setting steps：

3.1 Computer Configuration

The managed switch can be managed by web page. The flexible and friendly interface can make it easy to manage the switch.
Web pages may display differently in different operating systems.

3.1.1 Windows XP

Configure your computer as follows:
1. Start menu ---- Control panel

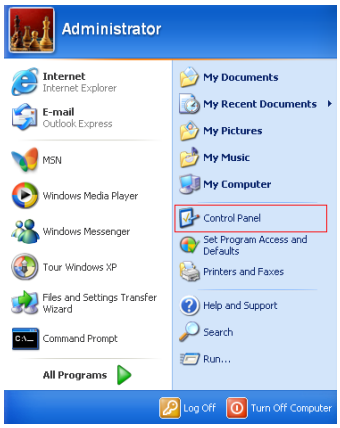


Figure 3-1-1

2. Click “Network and Internet Connection”

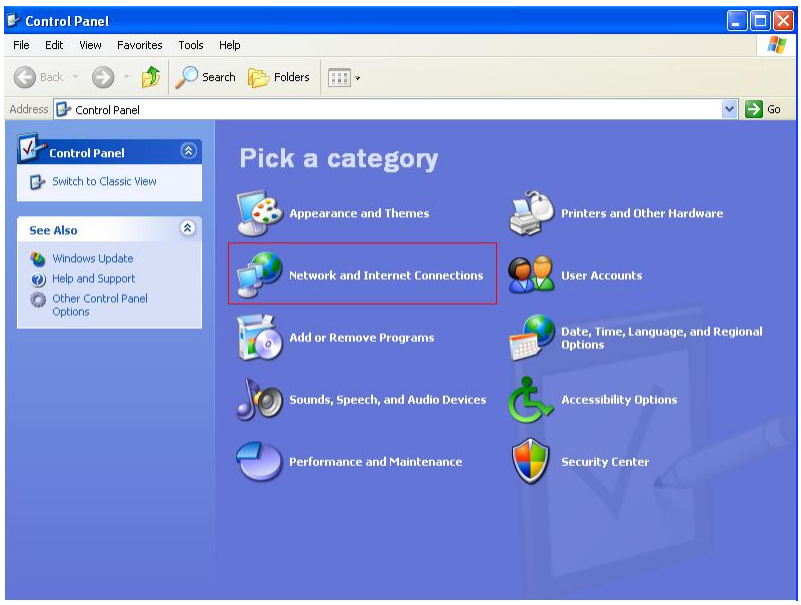


Figure 3-1-2

3. Click “Network connection”

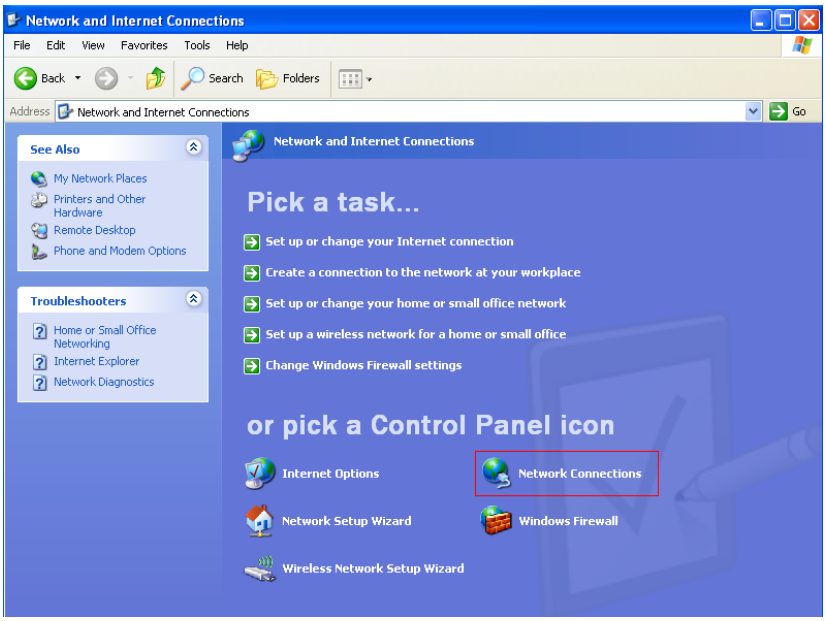


Figure 3-1-3

4. Right click on the adapter icon and select “Properties”

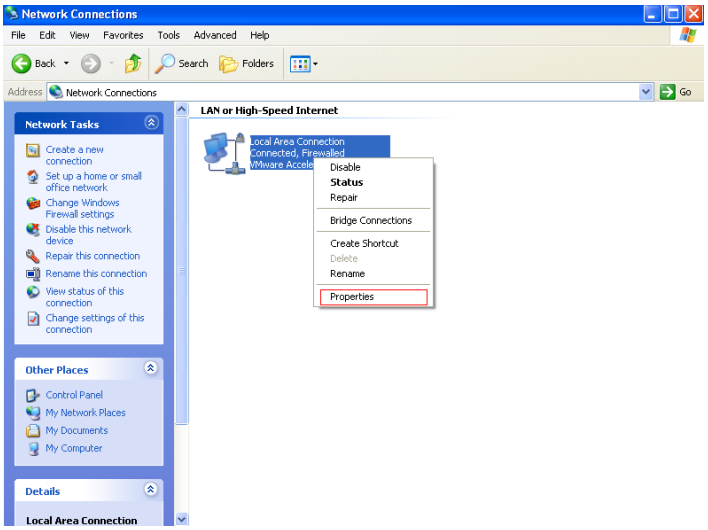


Figure 3-1-4

5. Double click on “Internet protocol (TCP/IP)”

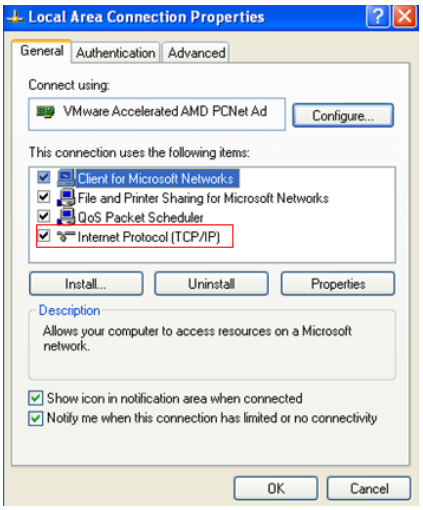


Figure 3-1-5

6. Use the following IP address: input IP 192.168.1. *** (1 <*** <255， *** is not 11, because the default IP of the switch is 192.168.1.1), Subnet mask: 255.255.255.0. The default gateway and DNS server are optional, and then click “OK” to close the Internet TCP / IP properties window.

Figure 3-1-6

7. Click “OK” to close the local connection properties window.

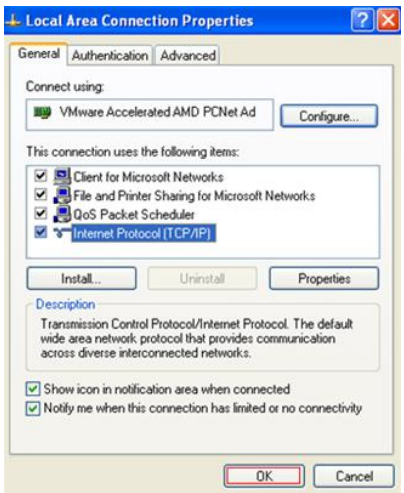


Figure 3-1-7

3.1.2 Windows 7/Windows Vista

Configure your computer as follows:

1. Start menu ---- Control panel

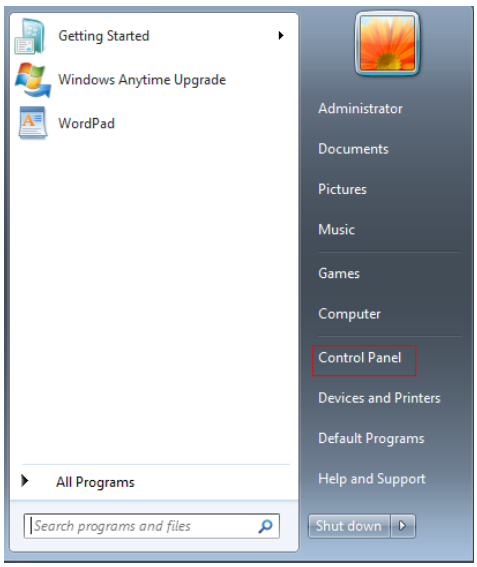


Figure 3-1-8

2. Click “Network and Internet Connection”

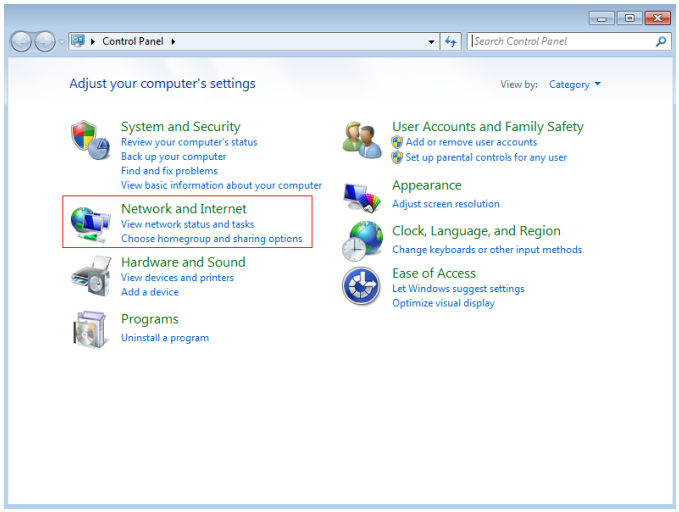


Figure 3-1-9

3. Click “Change Adapter settings”

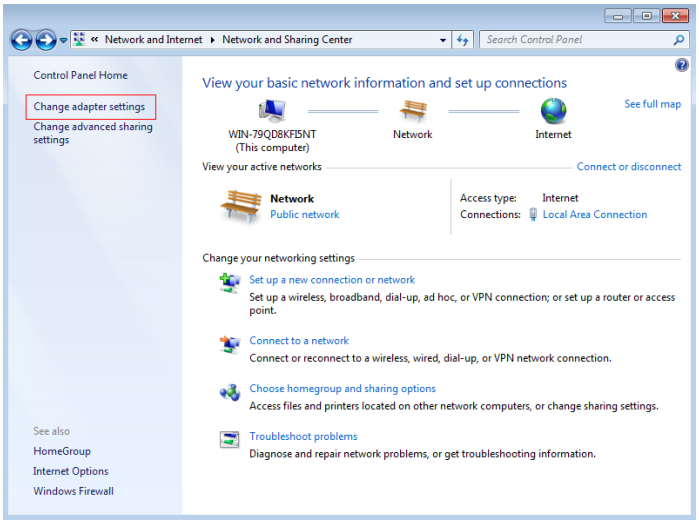


Figure 3-1-10

4. Right click on the adapter icon and select “Properties”

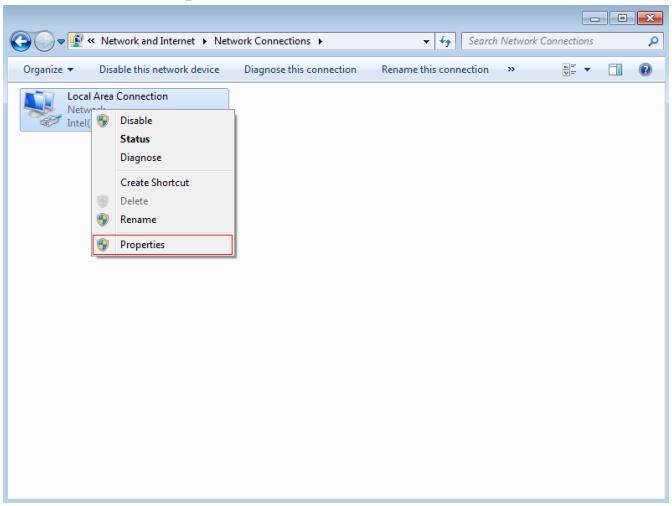


Figure 3-1-11

5. Double click on “Internet protocol (TCP/IP)”

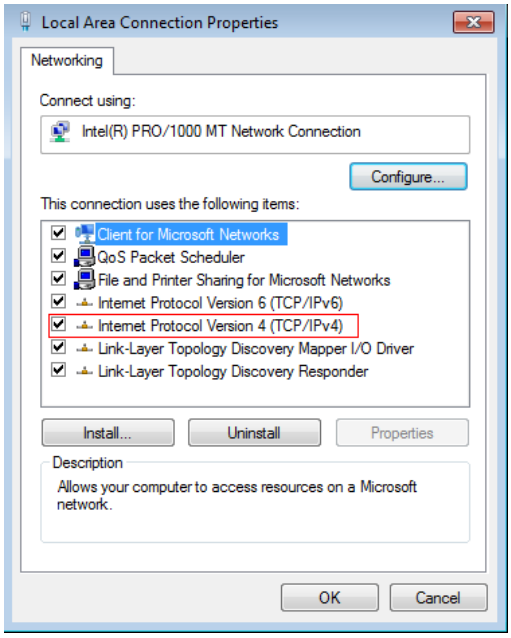


Figure 3-1-12

5. Use the following IP address: input IP 192.168.1. *** (1 <*** <255, *** is not 11, because the default IP of the switch is 192.168.2.11), Subnet mask: 255.255.255.0. The default gateway and DNS server are optional, and then click “OK” to close the Internet TCP / IP properties window.

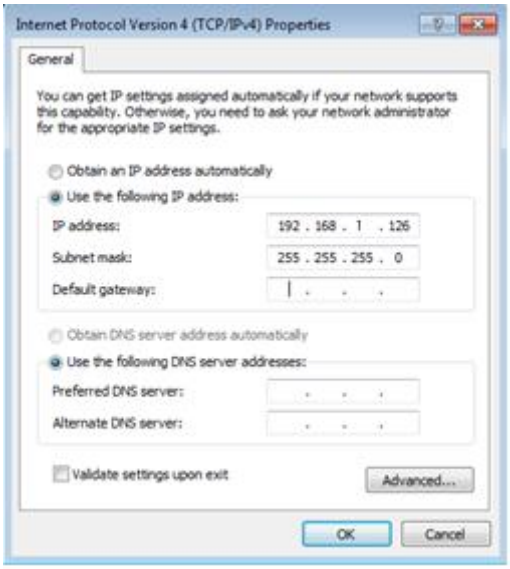


Figure 3-1-13

6. Click “OK” to close the local connection properties window.

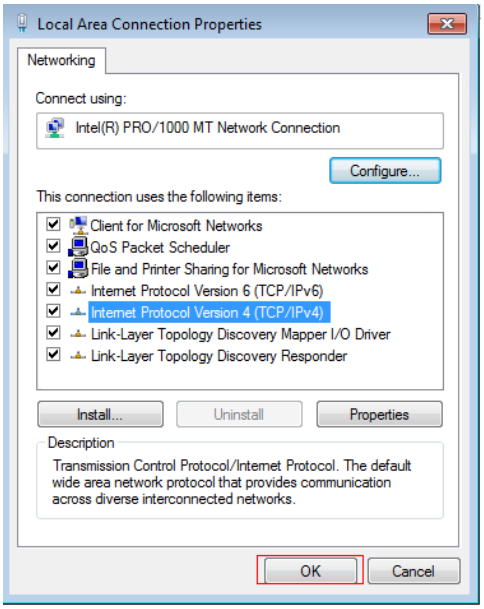


Figure 3-1-14

3.2 Connection Check

After setting the TCP / IP protocol, you can use the ping command to check whether the PC can communicate with the host computer. To execute the ping command, open a command prompt window with the address of.

Enter the command line window and input the following command.
If the command line window shows the following:

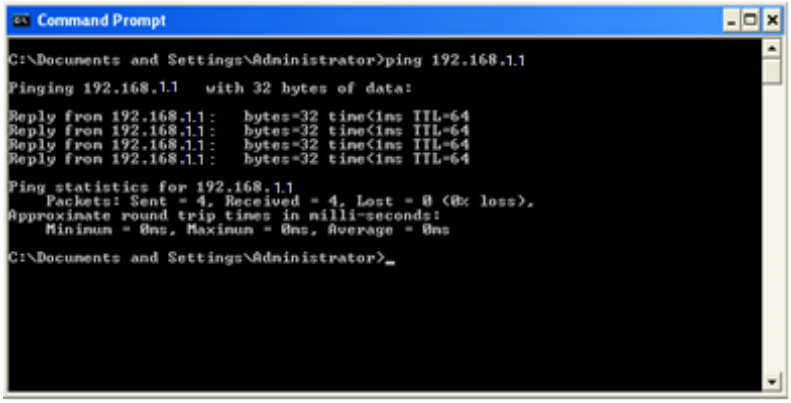


Figure 3-2-1

The connection with PC is successful

If the connection with PC is broken, the command line window will show the following:

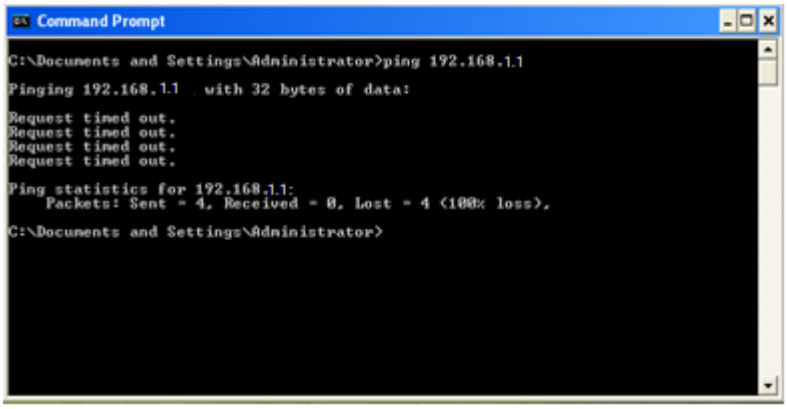


Figure 3-2-2

Please make sure the computer network setting is correct and the network connection is normal..

Note:

Before entering the above command, please use twisted pair to connect the switch port and the network card of your PC.

3.3 Login

Open IE browser, input http://192.168.1.1 in the address bar and press “enter”

Figure 3-3-1

1. In the pop-up window, input the user name: admin, password: admin, and click "OK"

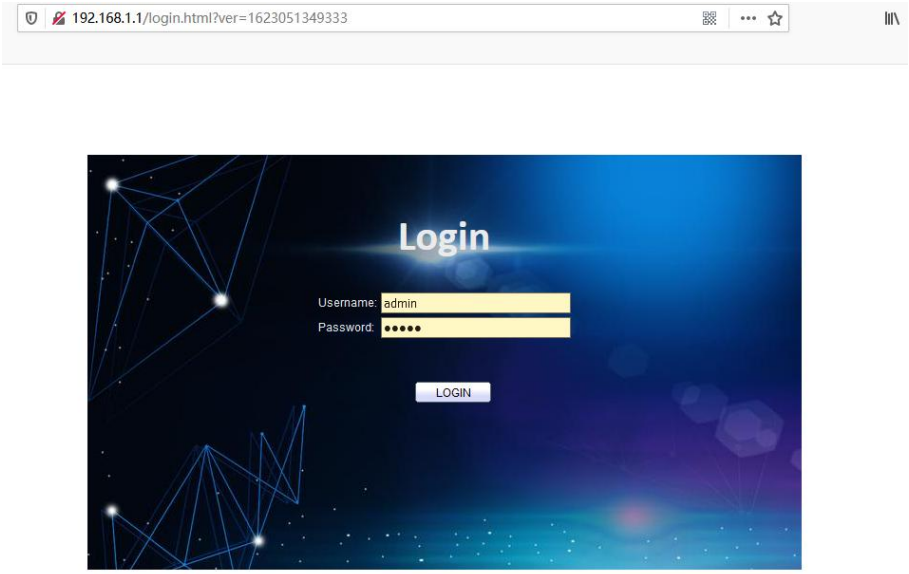


Figure 3-3-2

Notice:

If you successfully log in the switch web page, the page will be refreshed in real time to check port status and other information dynamically.

3.4 Function Overview

This switch owns rich features, including status，Network，port，VLAN，STP，Discovery，Multicast，Security，ACL，QoS，Diagnostics，Management setting. The following part will introduce the above functions.

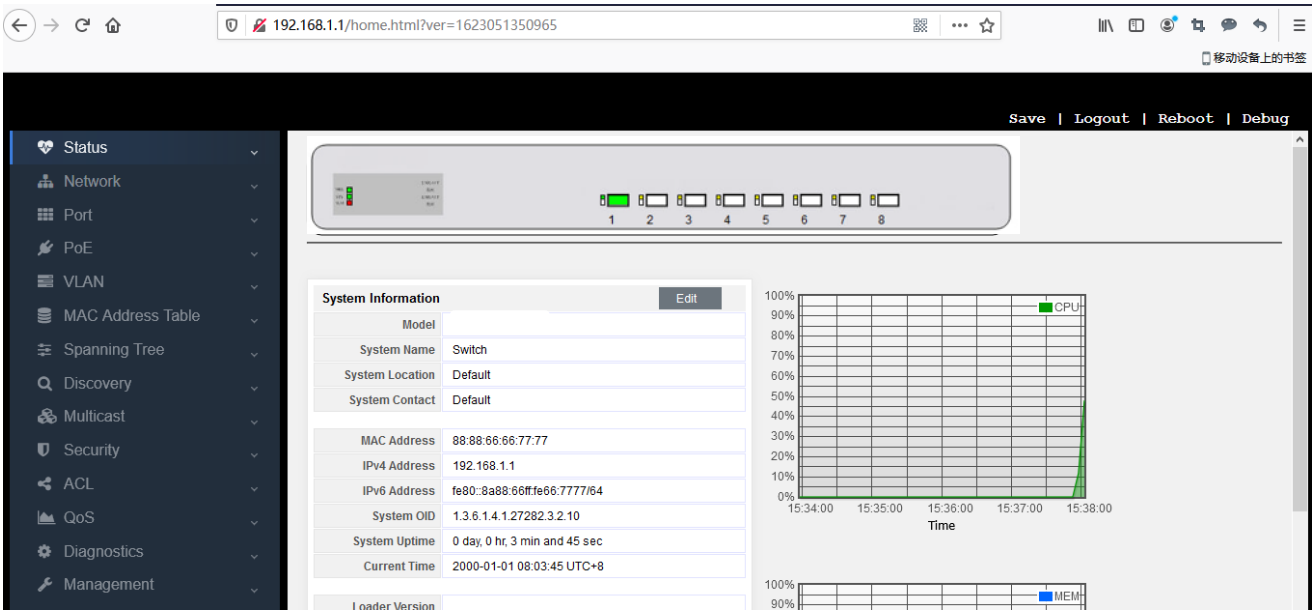


Figure 3-4-1

Part 4: System

4.1 Homepage

After logging in to the switch, you will see the home page as shown in the following figure, which includes three parts:

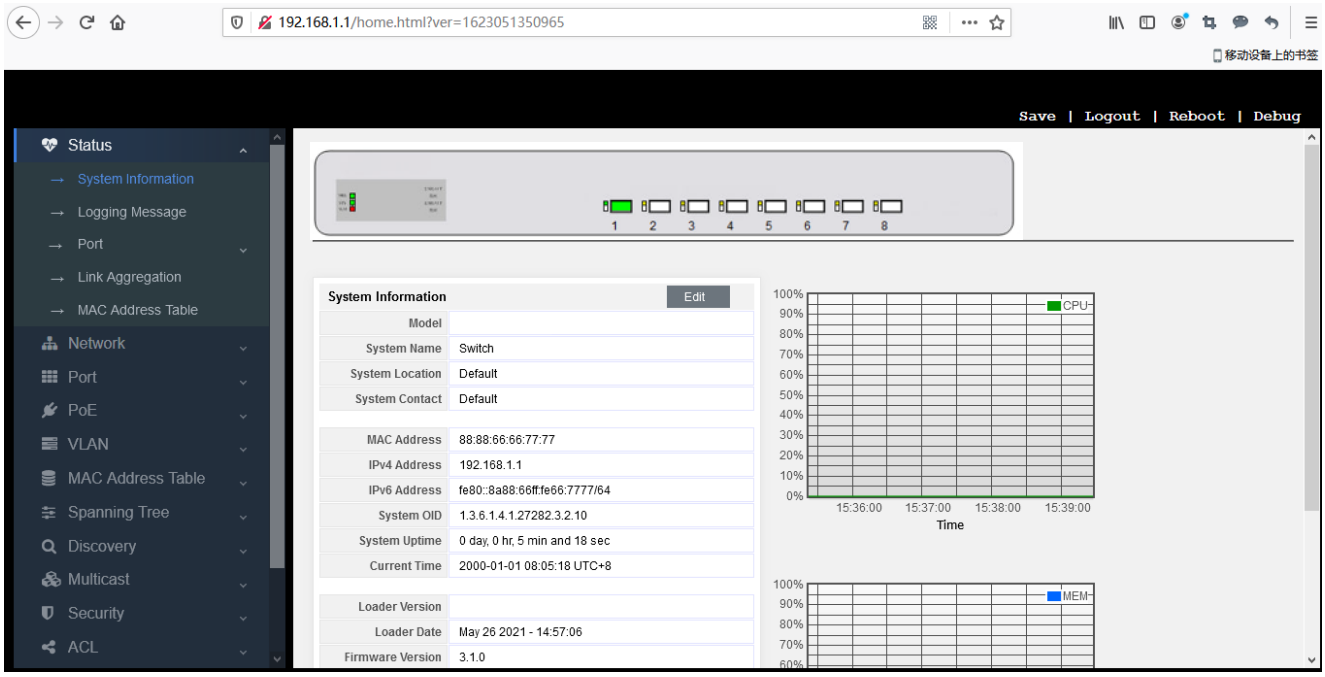


Figure 4-1-1

Part I: A list of port Led Indicator is at the top of the page showing virtual port prompts, in which the green and gray indicate that the port is connected and unconnected respectively.

Part II: The menu list is on the left side of the page, which includes L2 main menus. Every main menu has several submenus. Click the menu to open its submenu and main window.

Part III: It is the main part of this page which shows the configuration page.

4.2 Status

Click "status" to display the following switch management page. The system submenu has some basic information, including system information, log message, port management, aggregation, MAC address table, etc. See the details in the picture below.

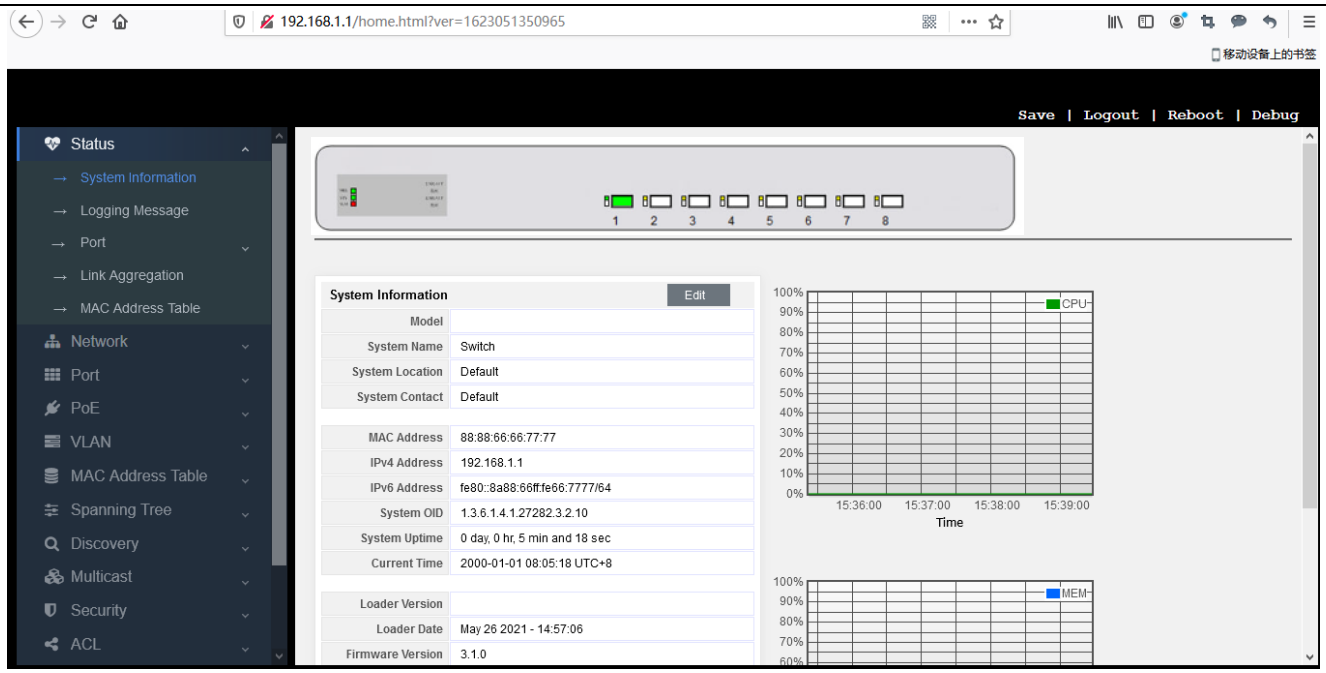


Figure 4-2-1

The system information menu displays some information about the system, such as type, system name, MAC address of the switch, IP address, current time and CPU utilization.

4.3 System information

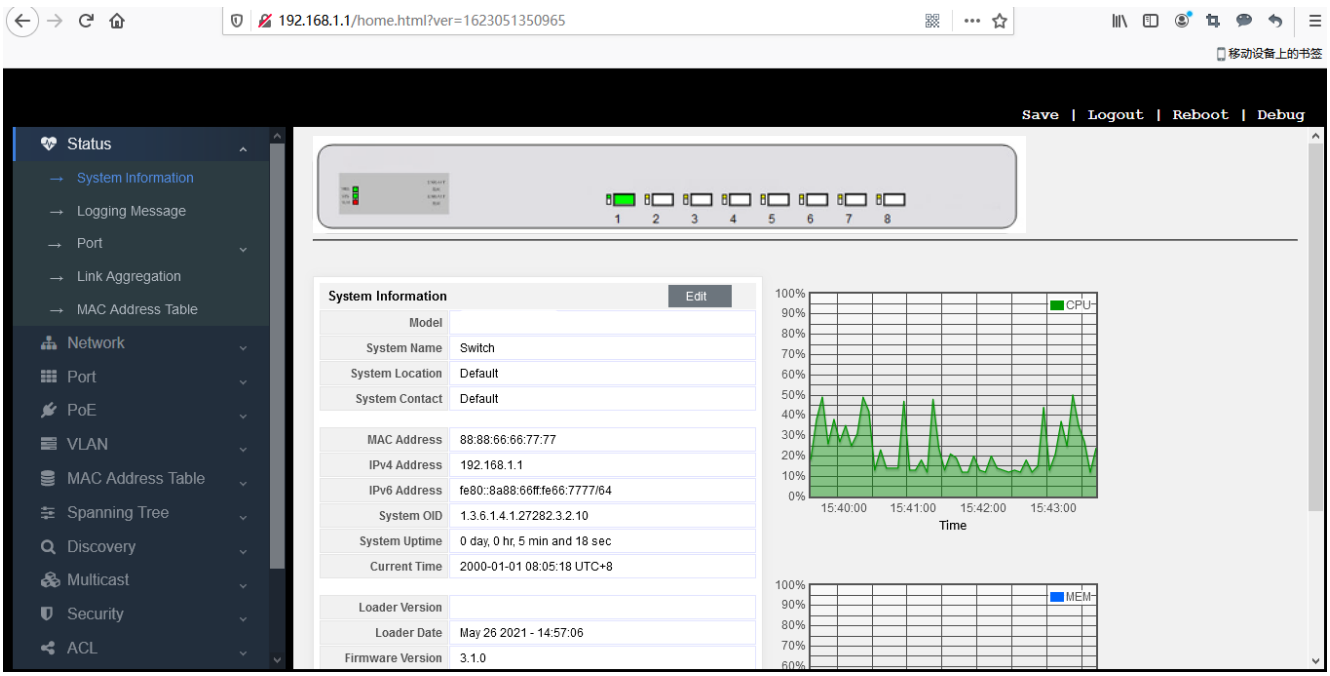


Figure 4-3-1

On this page, you can read the port number of the accessed web page, the running time of the switch system, the current system time of the switch, and the enabled services, such as Telnet, SSH, HTTP, HTTPS and SNMP.
The third interface on the far right shows the real-time utilization of CPU and memory.

4.4 Logging message

Relevant information will be recorded in the log for checking at any time. You can check not only the logs in RAM, but also the logs in flash.

Ram: log information recorded in the memory. When the switch is restarted, the log information recorded in RAM will be gone.
Flash: log information recorded in flash. When the switch is restarted, the log information recorded in flash still exists.

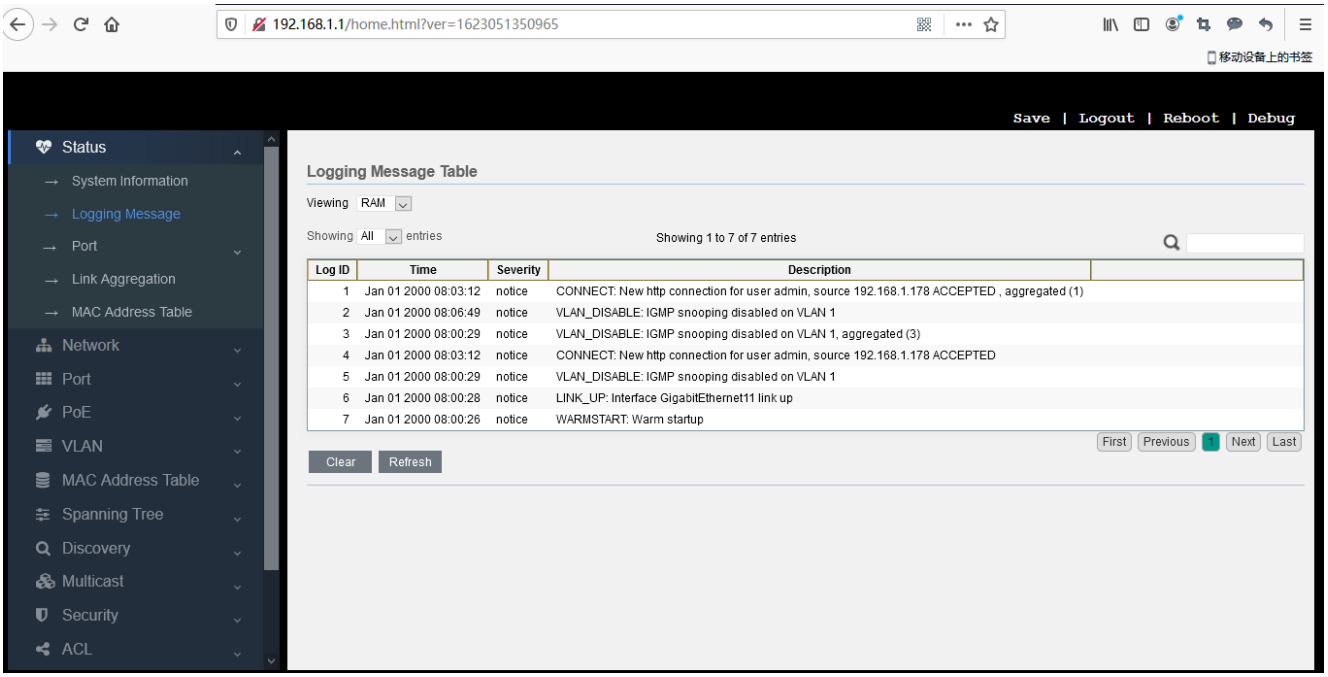


Figure 4-4-1

Figure 4-4-2

You can also select the number of displayed entries. If you select “all”, it means to display all entries on your selected page. If you select 10, it means to display 10 log information entries on one page, and the remaining entries will be displayed in the following pages.
Finally, you can see an input box for searching in this page. You can enter "debug, info, notice..." to display by category.

4.5 port

This is used for checking counter information of the port.

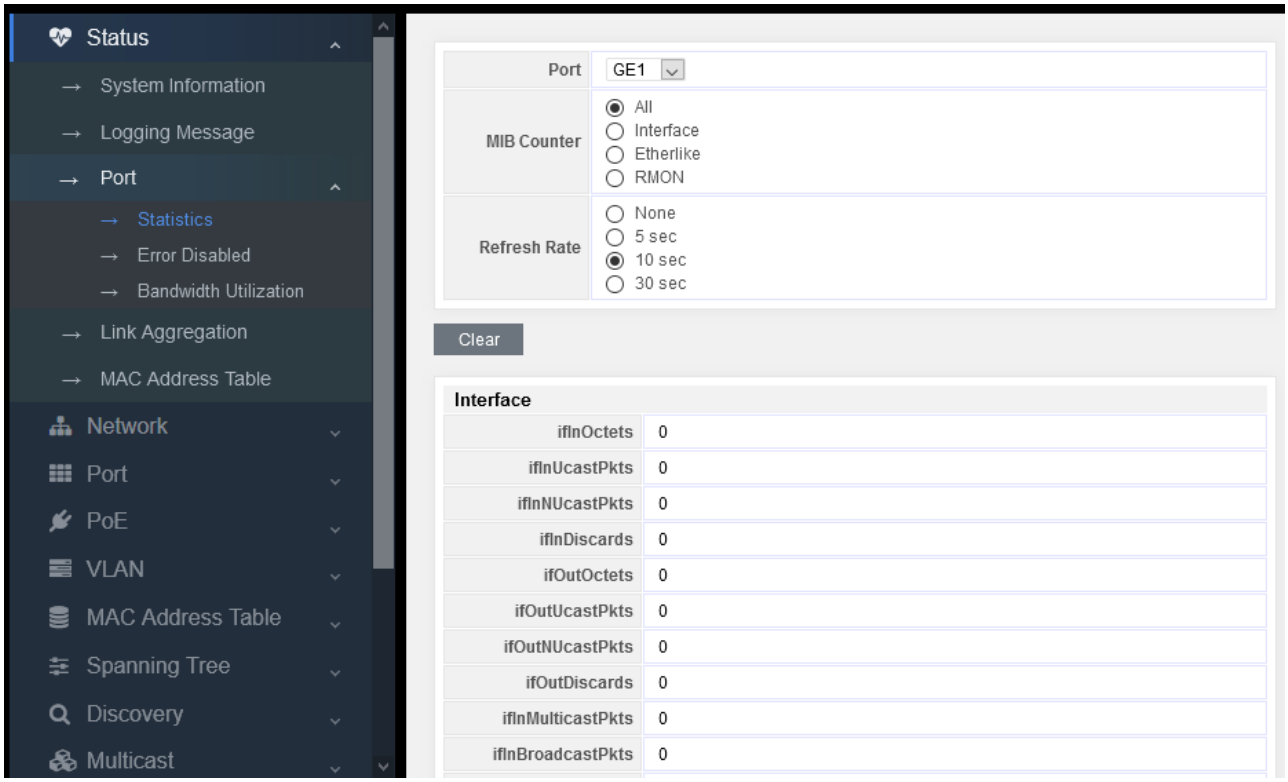


Figure 4-5-1

4.6 Link Aggregation Management

Display of Link aggregation:

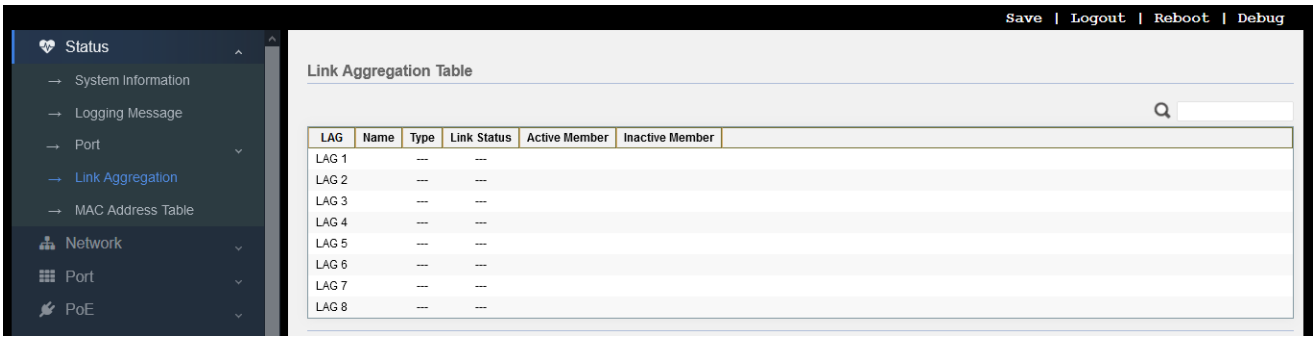


Figure 4-6-1

4.7 MAC Address Table

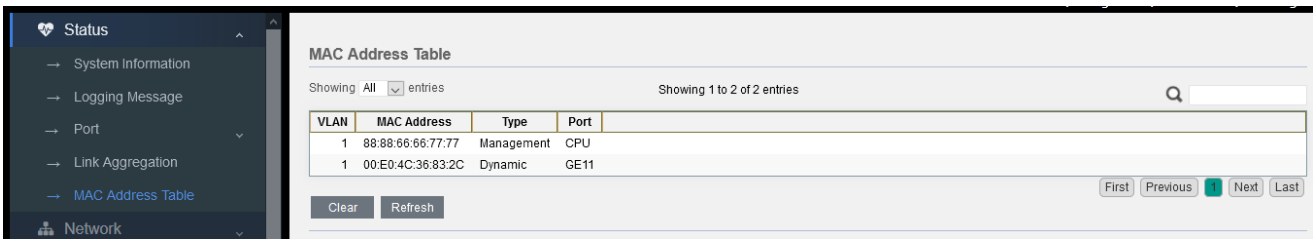


Figure 4-7-1

Part 5: Network

5.1 IP Address

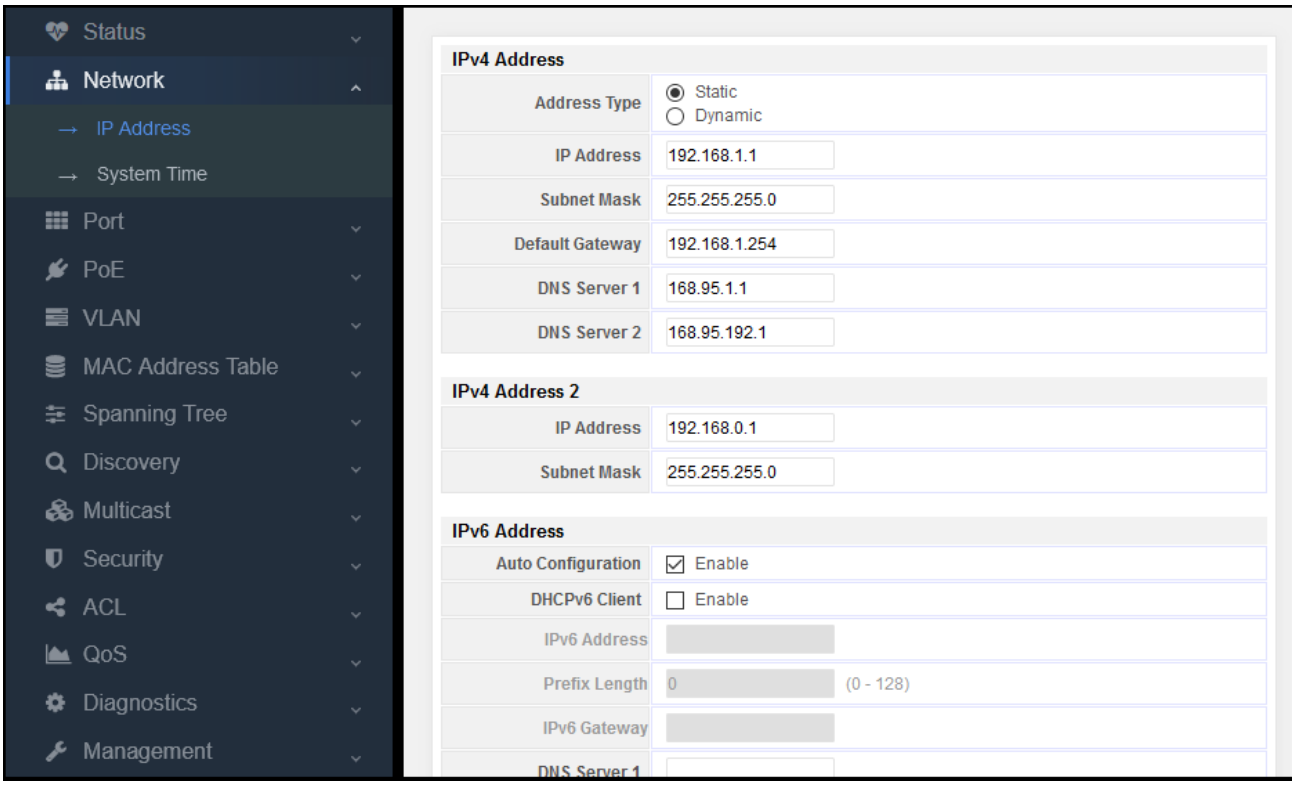


Figure 5-1-1

In this page, you can modify the IPv4 address, subnet mask, gateway and DNS server of the switch, as well as configure DCHP to obtain IP address.

At the same time, the IPv6 address of the switch can also be configured, either automatically or by DHCP acquisition, or static configuration, which can meet user's requirements.

5.2 System Time

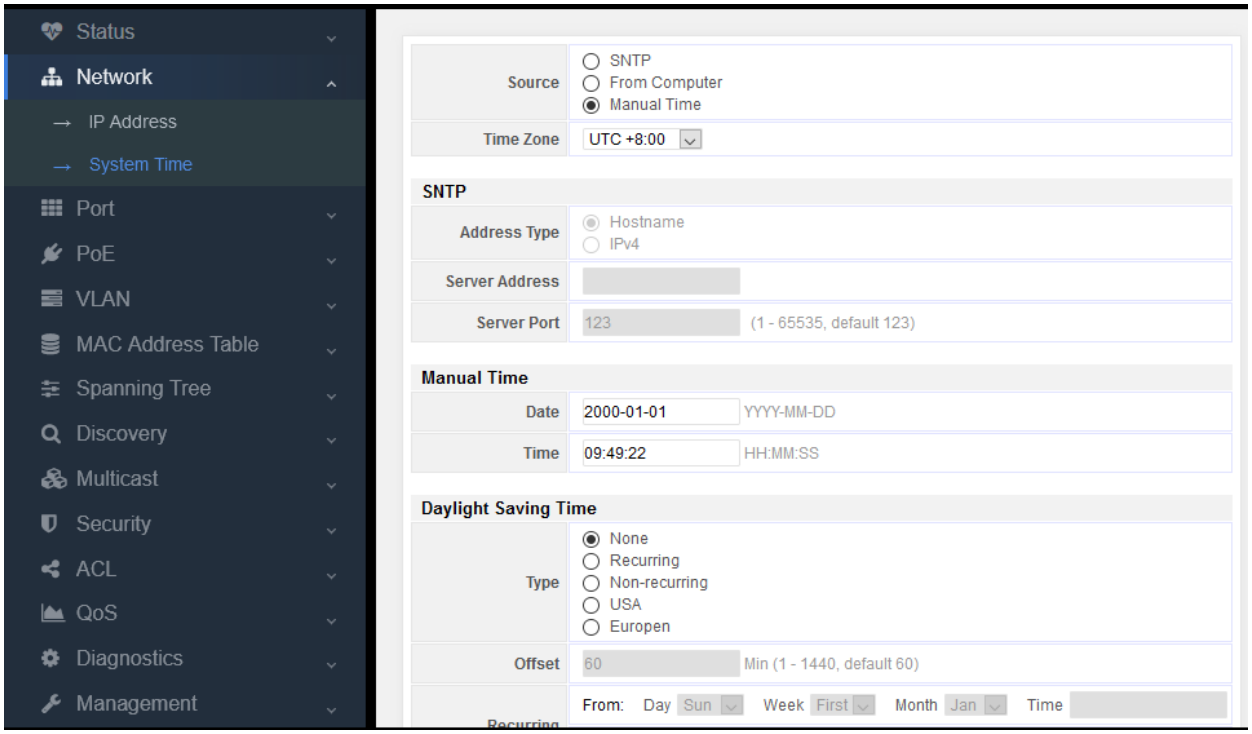


Figure 5-2-1

The system time of the switch can be obtained from SNTP, the computer accessing the switch, and by manual configuration.

If the time is obtained by SNTP:

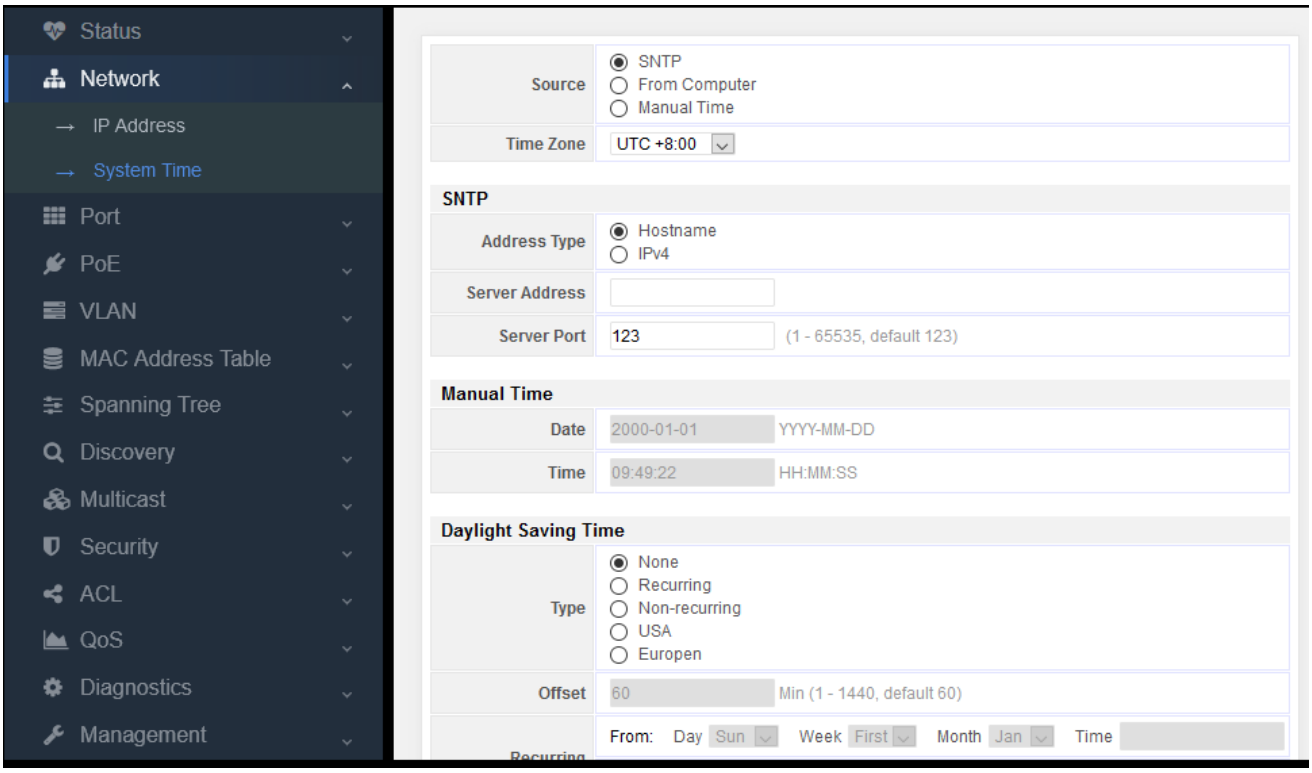
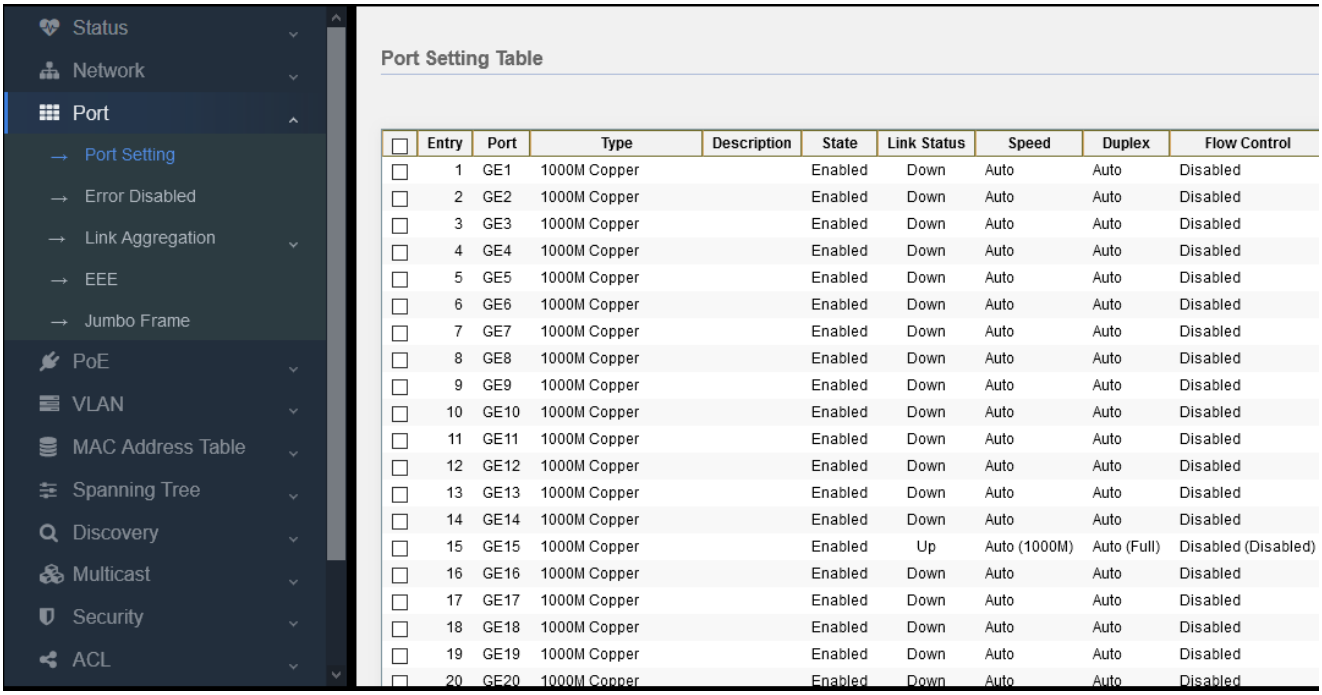


Figure 5-2-2

You can directly fill in the IPv4 address of the time server and 123 of the default port.

Part 6: Network

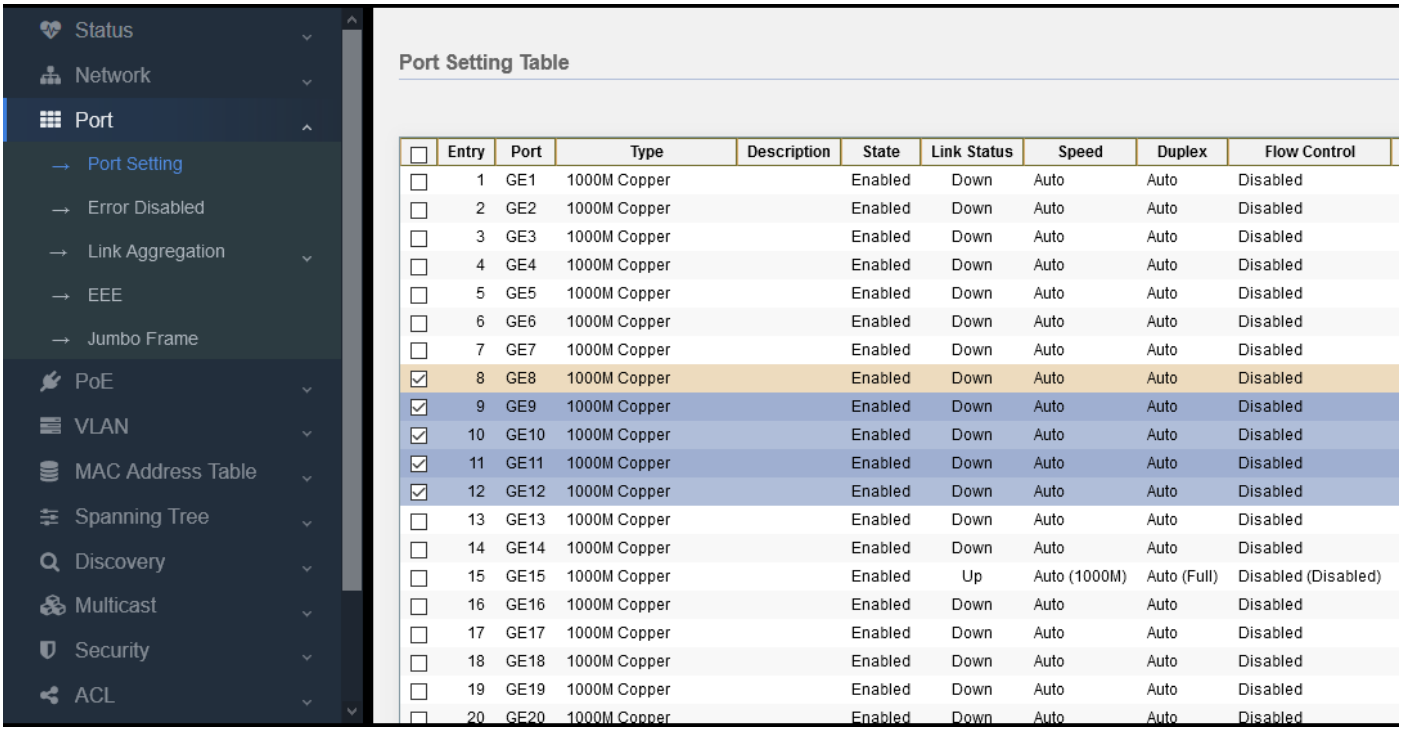
6.1 Port Setting



Entry	Port	Type	Description	State	Link Status	Speed	Duplex	Flow Control
1	GE1	1000M Copper		Enabled	Down	Auto	Auto	Disabled
2	GE2	1000M Copper		Enabled	Down	Auto	Auto	Disabled
3	GE3	1000M Copper		Enabled	Down	Auto	Auto	Disabled
4	GE4	1000M Copper		Enabled	Down	Auto	Auto	Disabled
5	GE5	1000M Copper		Enabled	Down	Auto	Auto	Disabled
6	GE6	1000M Copper		Enabled	Down	Auto	Auto	Disabled
7	GE7	1000M Copper		Enabled	Down	Auto	Auto	Disabled
8	GE8	1000M Copper		Enabled	Down	Auto	Auto	Disabled
9	GE9	1000M Copper		Enabled	Down	Auto	Auto	Disabled
10	GE10	1000M Copper		Enabled	Down	Auto	Auto	Disabled
11	GE11	1000M Copper		Enabled	Down	Auto	Auto	Disabled
12	GE12	1000M Copper		Enabled	Down	Auto	Auto	Disabled
13	GE13	1000M Copper		Enabled	Down	Auto	Auto	Disabled
14	GE14	1000M Copper		Enabled	Down	Auto	Auto	Disabled
15	GE15	1000M Copper		Enabled	Up	Auto (1000M)	Auto (Full)	Disabled (Disabled)
16	GE16	1000M Copper		Enabled	Down	Auto	Auto	Disabled
17	GE17	1000M Copper		Enabled	Down	Auto	Auto	Disabled
18	GE18	1000M Copper		Enabled	Down	Auto	Auto	Disabled
19	GE19	1000M Copper		Enabled	Down	Auto	Auto	Disabled
20	GE20	1000M Copper		Enabled	Down	Auto	Auto	Disabled

Figure 6-1-1

1. Select the port required for configuration, such as port 8-12.



Entry	Port	Type	Description	State	Link Status	Speed	Duplex	Flow Control
1	GE1	1000M Copper		Enabled	Down	Auto	Auto	Disabled
2	GE2	1000M Copper		Enabled	Down	Auto	Auto	Disabled
3	GE3	1000M Copper		Enabled	Down	Auto	Auto	Disabled
4	GE4	1000M Copper		Enabled	Down	Auto	Auto	Disabled
5	GE5	1000M Copper		Enabled	Down	Auto	Auto	Disabled
6	GE6	1000M Copper		Enabled	Down	Auto	Auto	Disabled
7	GE7	1000M Copper		Enabled	Down	Auto	Auto	Disabled
8	GE8	1000M Copper		Enabled	Down	Auto	Auto	Disabled
9	GE9	1000M Copper		Enabled	Down	Auto	Auto	Disabled
10	GE10	1000M Copper		Enabled	Down	Auto	Auto	Disabled
11	GE11	1000M Copper		Enabled	Down	Auto	Auto	Disabled
12	GE12	1000M Copper		Enabled	Down	Auto	Auto	Disabled
13	GE13	1000M Copper		Enabled	Down	Auto	Auto	Disabled
14	GE14	1000M Copper		Enabled	Down	Auto	Auto	Disabled
15	GE15	1000M Copper		Enabled	Up	Auto (1000M)	Auto (Full)	Disabled (Disabled)
16	GE16	1000M Copper		Enabled	Down	Auto	Auto	Disabled
17	GE17	1000M Copper		Enabled	Down	Auto	Auto	Disabled
18	GE18	1000M Copper		Enabled	Down	Auto	Auto	Disabled
19	GE19	1000M Copper		Enabled	Down	Auto	Auto	Disabled
20	GE20	1000M Copper		Enabled	Down	Auto	Auto	Disabled

Figure 6-1-2

2. Click “Edit” on the lower left.
3. Set the management state, speed, duplex, and flow control.

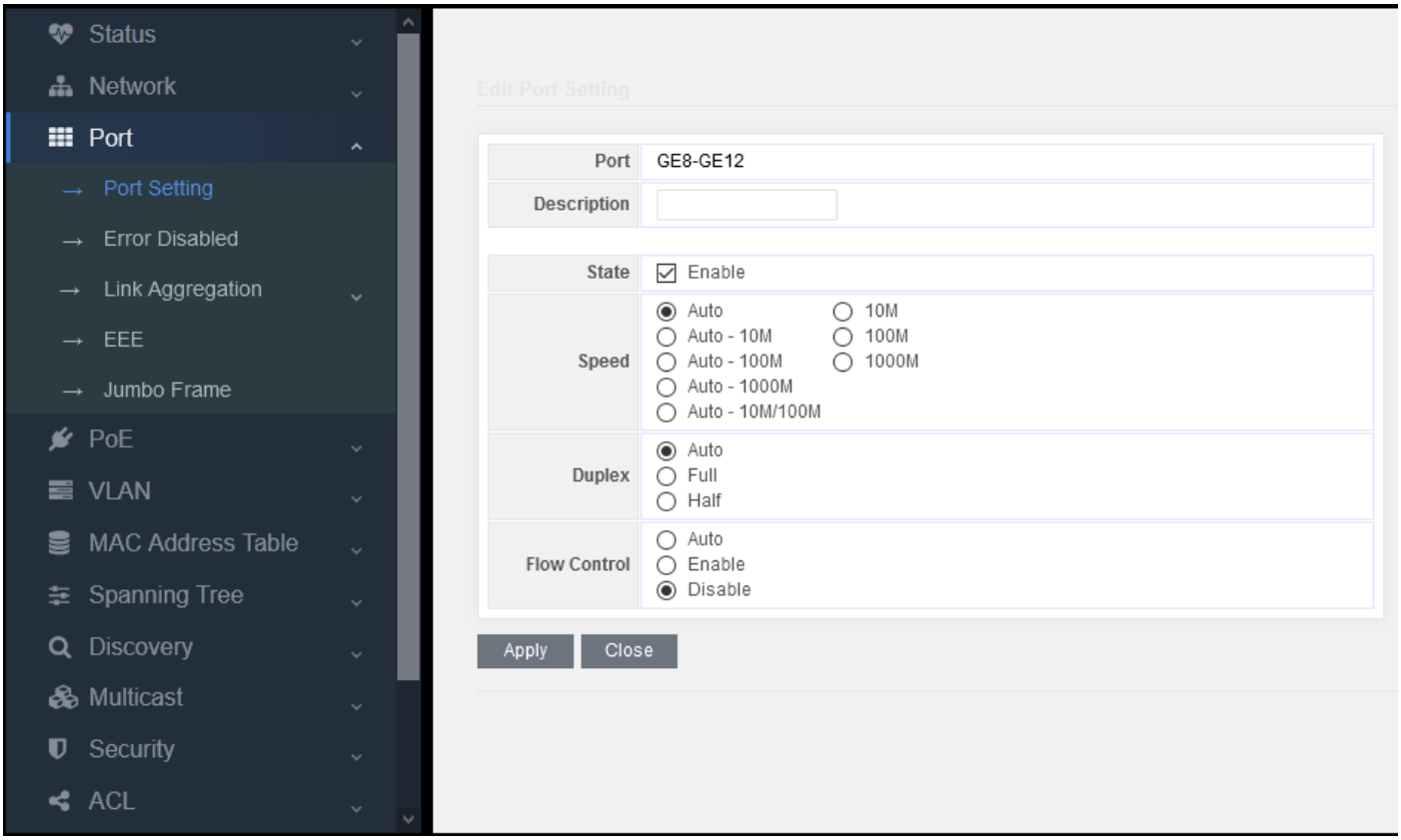


Figure 6-1-3

Management state: Enable/Disable. Select “Enable” means that this port can be used normally. Unselect “Enable” means that this port cannot be used normally.
Speed: Set auto-negotiation default (5 types), as well as enforcing mode (3 types)
Duplex: auto, duplex, and half duplex
Flow control: auto-negotiation, enable, and disable.

6.2 Error Disabled

For troubleshooting when the interface is err-disabled, the fault symptoms include that its line is blocked, the physical indicator is off or orange (the indicator status is different for different platforms)

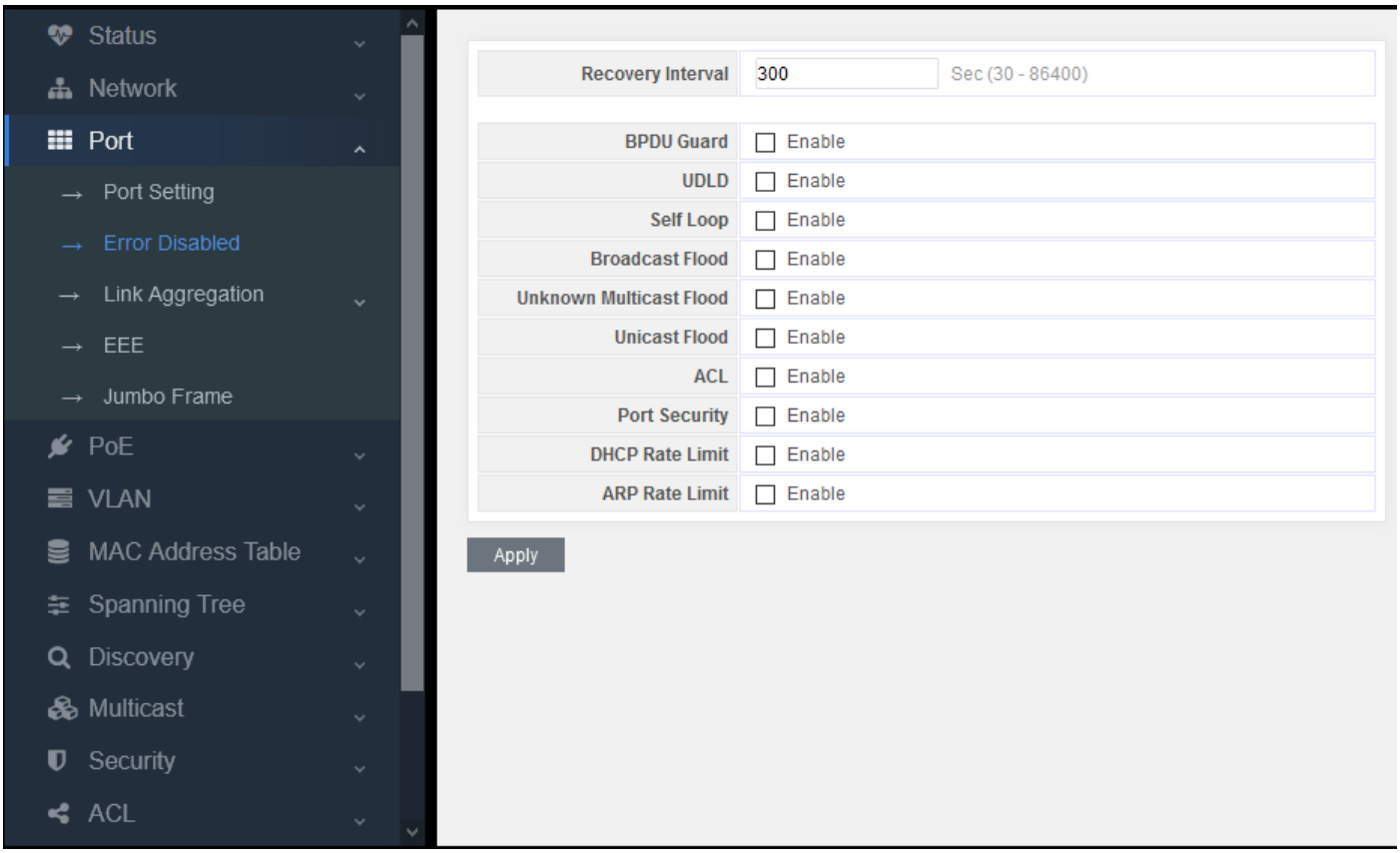


Figure 6-2-1

From the list, we can find that common reasons include UDLD, bpduguard, port security and loop.
The specific reason for err disable of the current interface can be viewed.

The system will attempt to restore the interface which is set as err disable after a period of time, 300 seconds by default. However, if the source of err disable is not solved fundamentally, the interface will be set as err disable again after restoring.
Adjust the timeout of err disable.

6.3 Link Aggregation

Link aggregation description

Link aggregation provides fault-tolerant high-speed connections between switches, routers and servers. You can use it to increase bandwidth between panel and data center, and you can configure it anywhere in the network with bottlenecks appearing. Link aggregation provides automatic repair for lost links by redistributing load communication on the maintained links. If a link is broken, link aggregation will redirect traffic from the broken link to the maintained link without any influence.

A link aggregation will consist of eight properly-configured Ethernet interfaces at most. All interfaces in link aggregation must be at the same speed and configured as layer 2 interfaces.

Introduction to Link Aggregation

Link aggregation can aggregate several Ethernet ports to form a logical aggregation group. On the layer entity, all physical links in an aggregation group are one logical link. Link aggregation is designed in an aggregation group to increase

bandwidth by performing output / input load allocation between member ports. Link aggregation group also allows port redundancy to provide connection reliability.

LACP introduction

Link aggregation control protocol (LACP) is designed to perform dynamic link aggregation and disaggregation. This protocol is based on IEEE802.3ad and adopts the combination of link aggregation control protocol data units (LACPDUs) and peer-to-peer enabled LACP ports. LACP transmits the following information of the port to its opposite end through LACPDUS:system priority and MAC address, port priority, port number and operation key.

When a message is received, the access point compares the message with that of other ports on the peer device to determine whether the port can be aggregated. In this way, the two parts can agree to add / remove ports from the dynamic aggregation group.

The system generates the operation key which is determined by the port, such as port speed, duplex mode, and basic configuration.

- The port selected in manual aggregation group or static aggregation group has the same operation key.
- The member ports of the dynamic aggregation group have a same operation key

Exchange LACP message

Both active and passive LACP modes allow interfaces and opposite port interfaces to negotiate to determine whether they can become an aggregation group based on such criteria as interface speed, two-layer aggregation, trunk status, and VLAN membership.

When interfaces are in different LACP modes, they can become an aggregation group as long as their modes are compatible. For example:

- The interface in active mode can form an aggregation group with the interface in passive mode.

An interface in passive mode cannot become an aggregation group with the interface that is also in passive mode because none of them can start LACP negotiation.

In open mode, ports which have been added as aggregation ports are forced to own the same features as that of the interface in other existing open mode in aggregation group.

Load balance and forwarding method description

Link aggregation balances the traffic load of link in aggregation by randomly assigning a new MAC address learned by a new link.

If a message is forwarded from the source MAC address to an aggregation port, it will pass the ports of the aggregation group distributedly on the basis of the source MAC address of the accessing message. Therefore, by providing load balancing, the messages forwarded from different hosts will adopt different ports in the aggregation group. But the messages forwarded from one host will adopt a same port in the aggregation group. The address of switch to learn MAC address will not change.

If a message is forwarded from the destination address to an aggregation port, it will pass the ports of the aggregation group distributedly on the basis of the destination MAC address of the accessing message. Therefore, messages to the same destination will be forwarded from a same port. And the messages to different destinations may be forwarded from different

aggregation ports.

Many workstations will connect with the switch which will connect a router through an aggregation port.
The link aggregation used on the switch is based on the source load balancing to ensure that the switch can use the router bandwidth effectively and distribute the communication through the physical connection with the workstation. Because the router is a device with single MAC address, it will use the load balancing on the basis of destination to distribute traffic to the workstation effectively through physical connection.

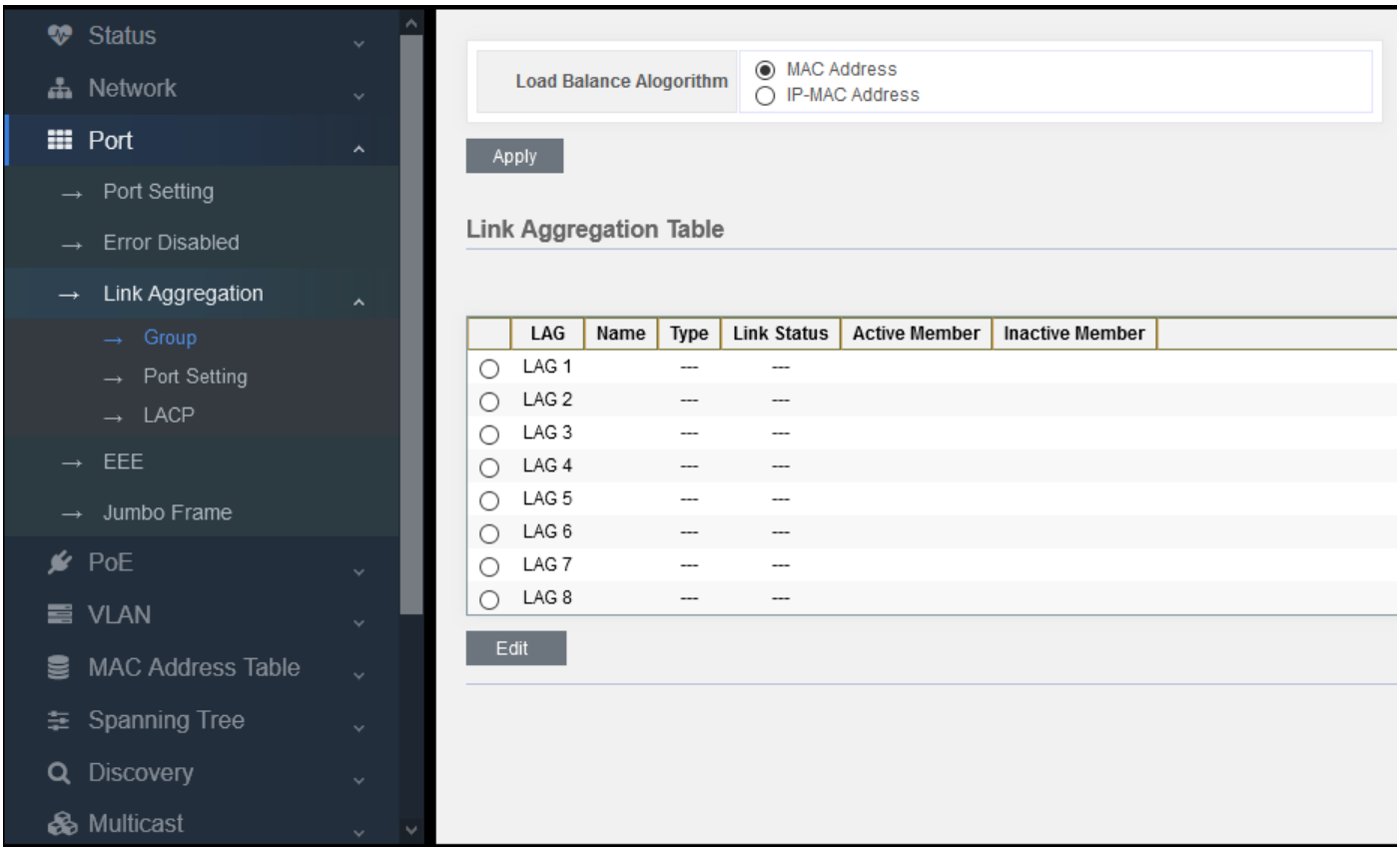


Figure 6-3-1

6.3.1 Group

static aggregation configuration

Load Balance Alogorithm：

- MAC address (source MAC + destination MAC)
- IP-MAC address (source IP + destination IP + source MAC + destination MAC)

This is an aggregate routing algorithm. The route of a message is selected according to its address

1. Select an aggregation group (1-8), LAG 1 ~ LAG 8
2. Click Edit
3. Select static to add the port from the left box to the right to join the aggregation group. It supports 8 aggregation groups at most, and 8 member ports for each aggregation group at most.

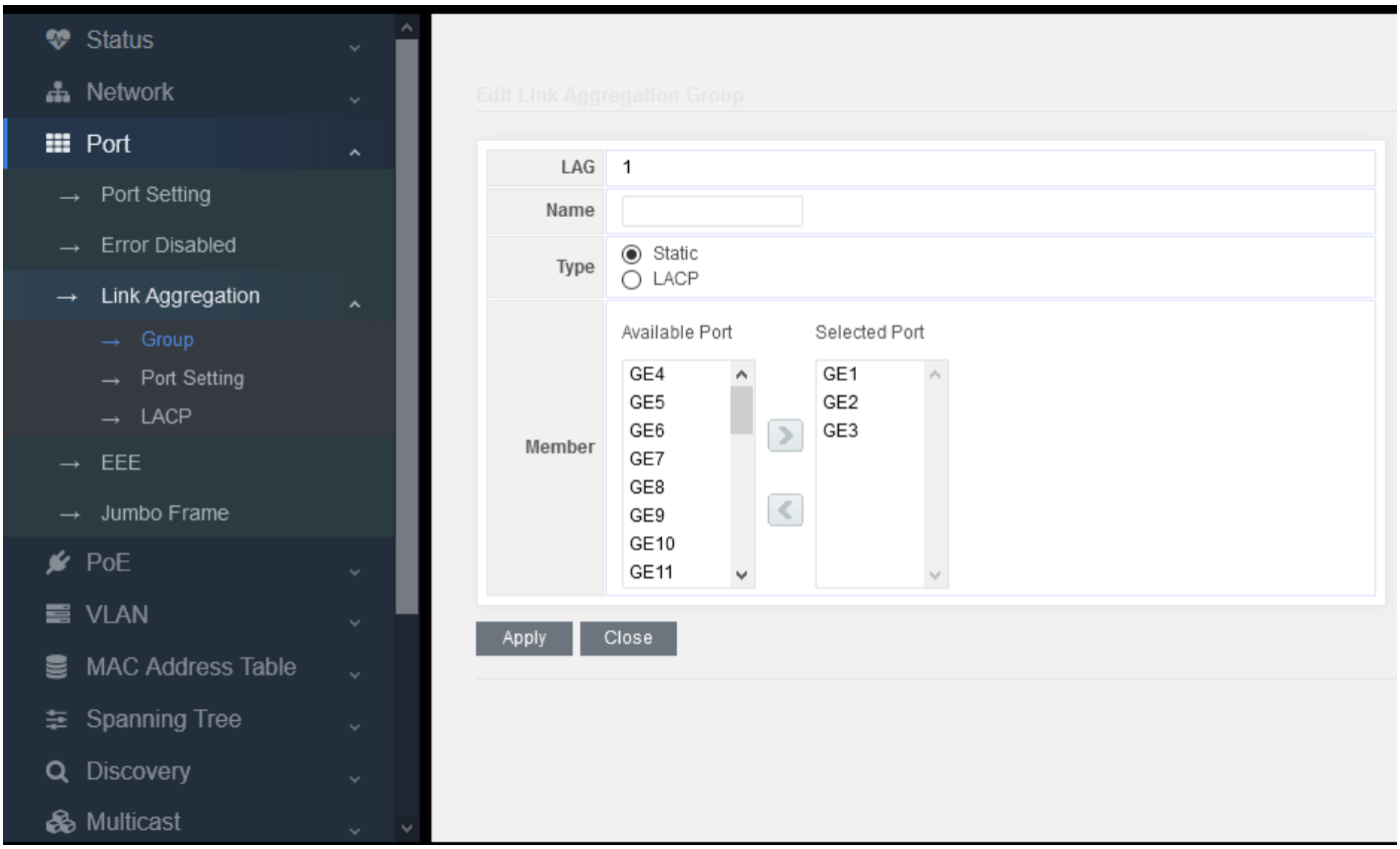


Figure 6-3-2

6.3.2 Port Setting

Aggregation ports properties setting:

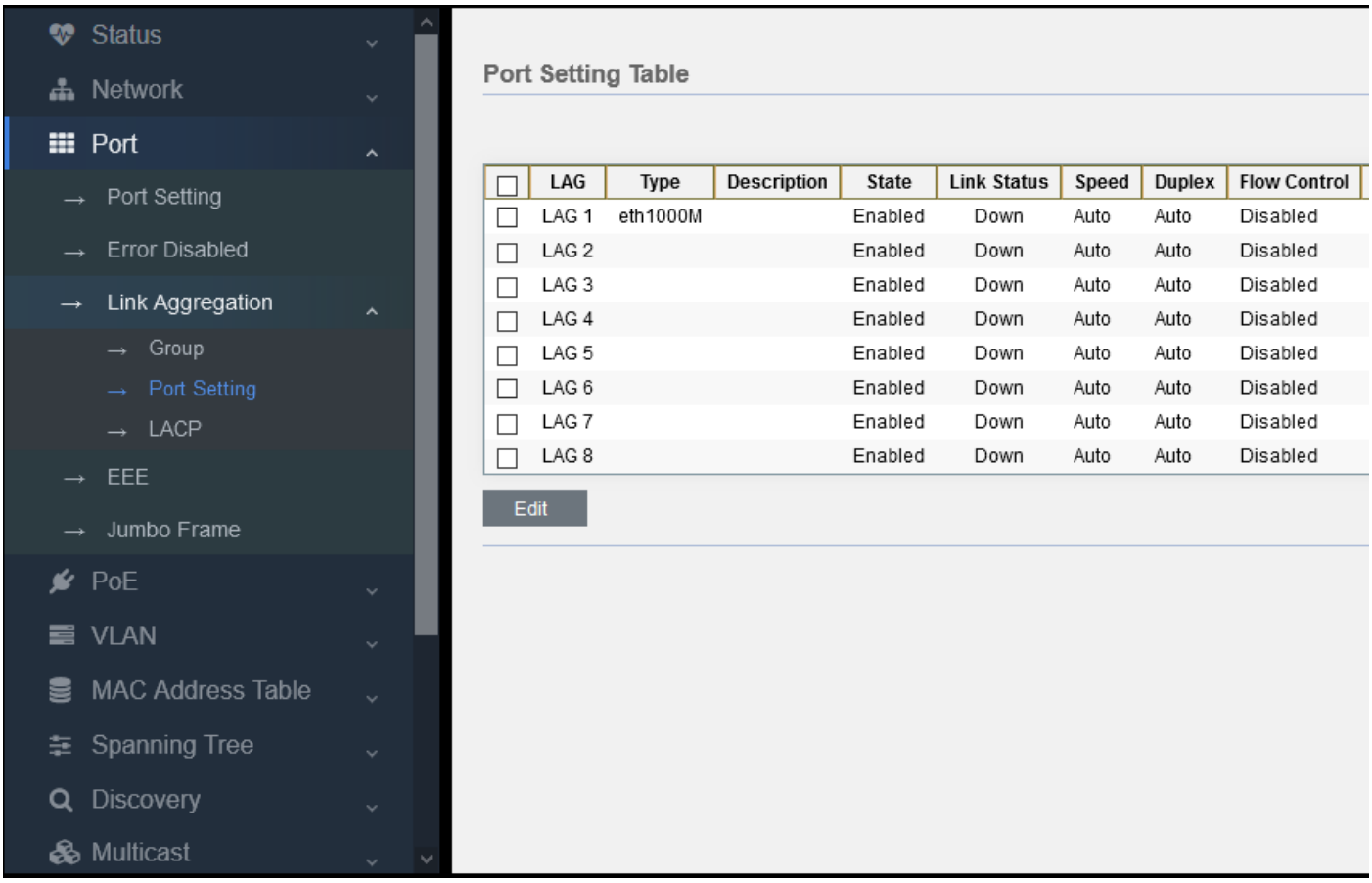


Figure 6-3-3

Set the speed, suplex and flow control of the aggregation port.

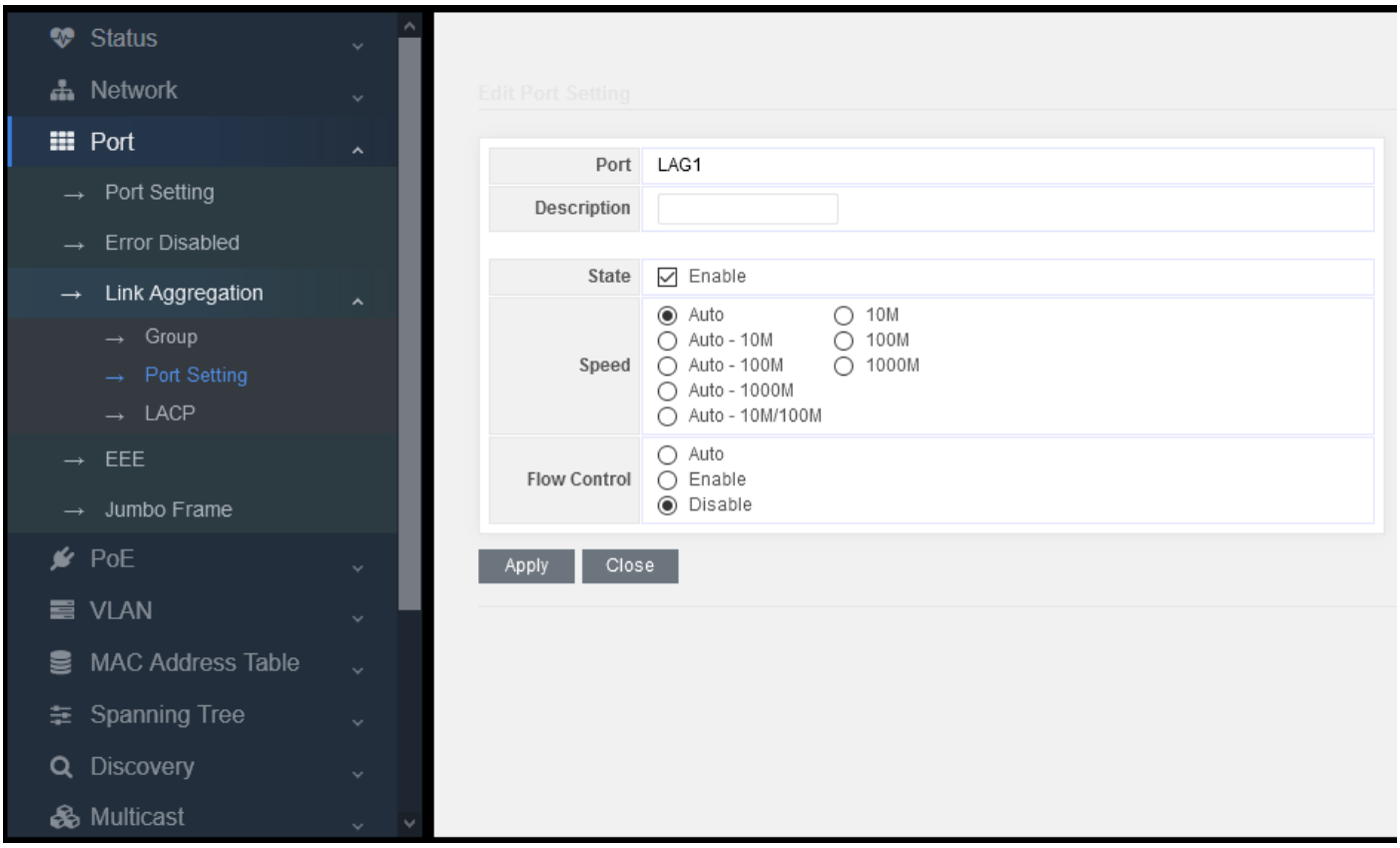


Figure 6-3-4

6.3.3 LACP

Set the system priority of LACP and ports.
The value has been configured by default, and users can modify it according to their own needs.

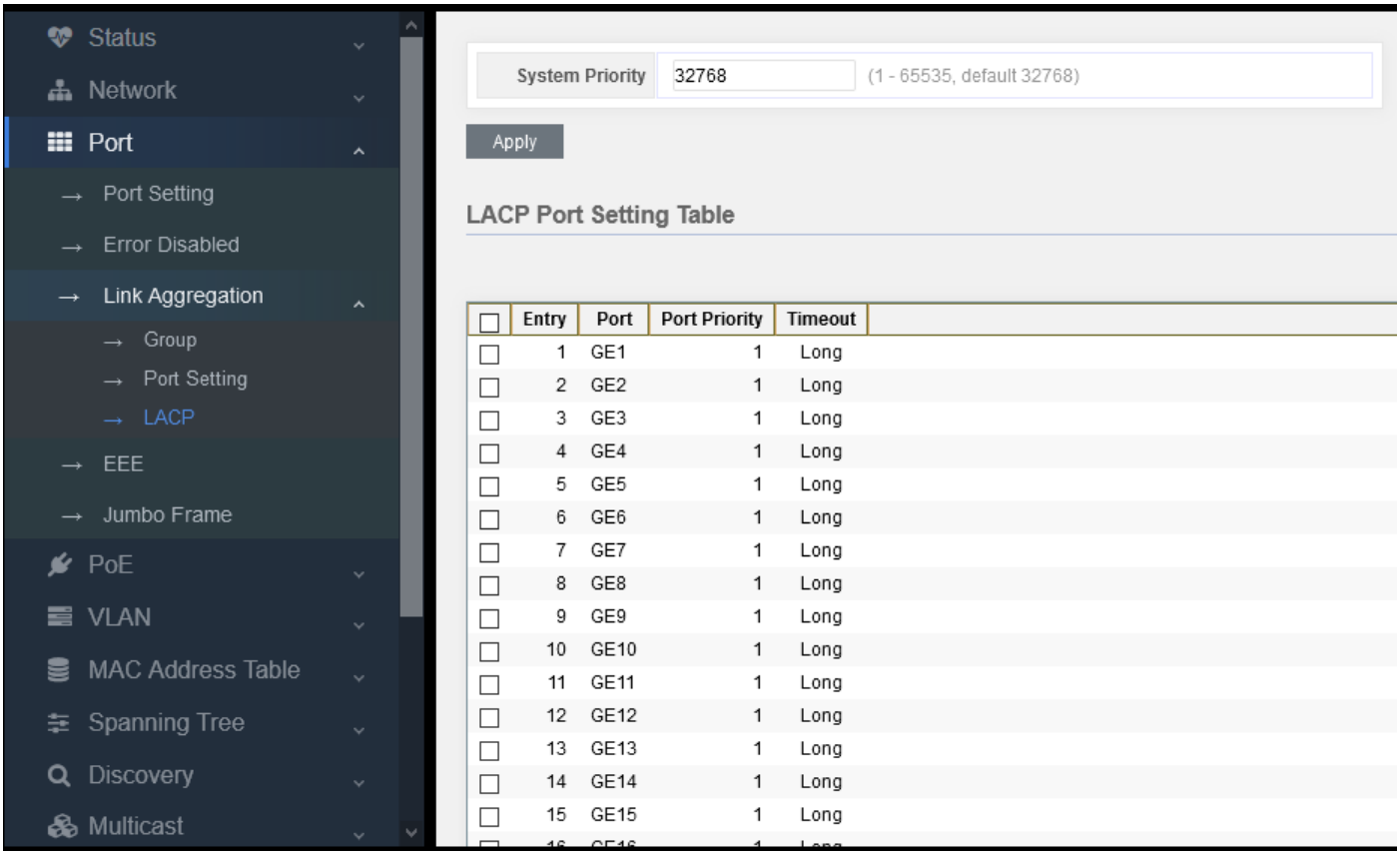


Figure 6-3-5

6.4 EEE

Energy efficient Ethernet, for short EEE, refers to “energy efficient Ethernet technology” with the function to automatically reduce the power consumption when the network card has no traffic. Only when the network utilization is high, the maximum power consumption can be achieved.

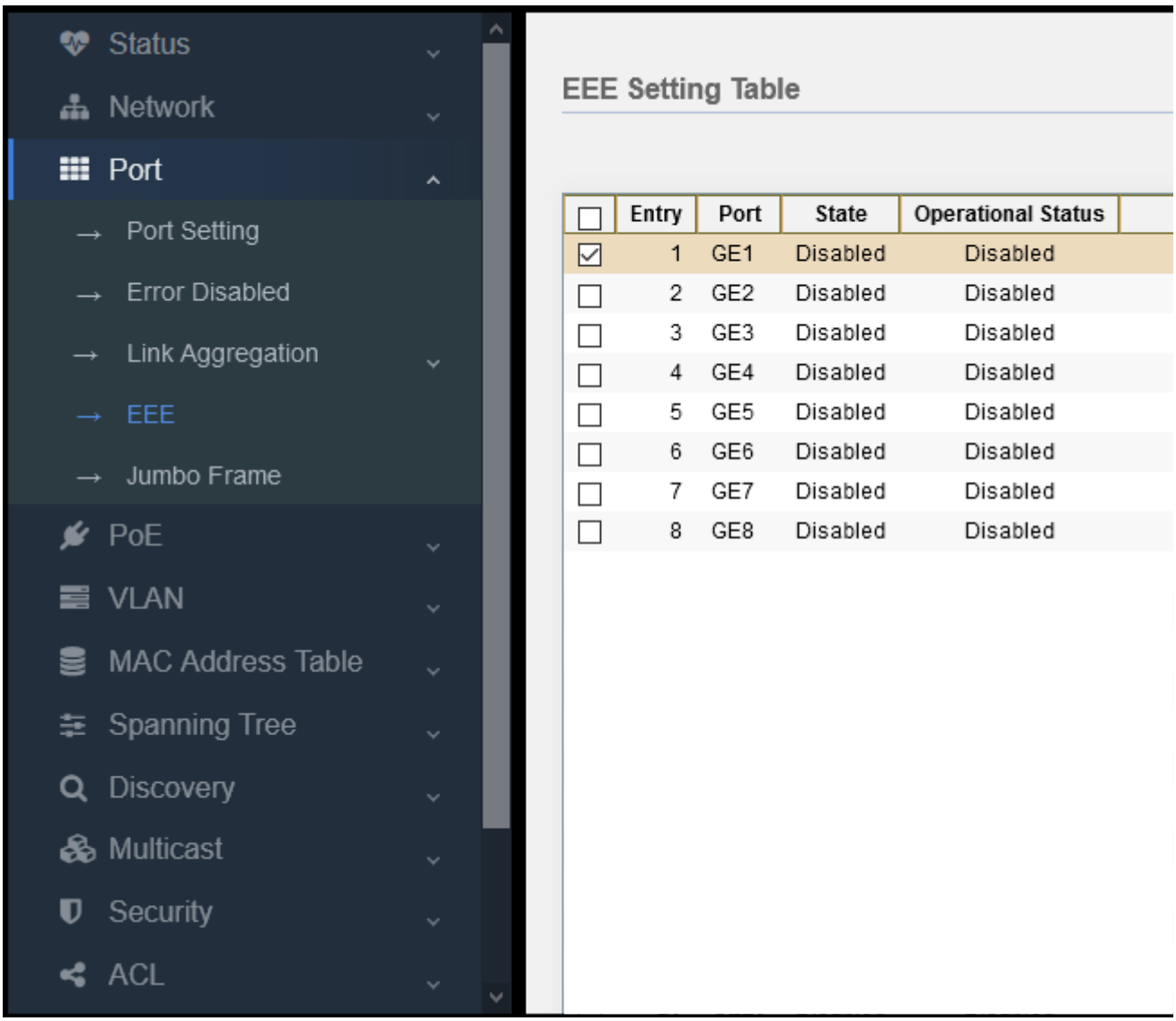


Figure 6-4

By default, EEE of the port is off. If you need this function, just turn it on the port.

Caution: if you want to use this function, not only the port of this switch will turn on EEE function, but the port on the opposite end should turn it on so as to go into operation.

6.5 Jumbo Frame

Jumbo frame refers to an Ethernet frame with frame length of more than 1522 bytes, which is a manufacturer's standard ultra long frame format, specially designed for Gigabit Ethernet. Different manufacturers have different length of the jumbo frame, which varies from 9000 bytes to 64000 bytes. The jumbo frame can fully play the performance of Gigabit Ethernet and improve the data transmission efficiency by 50%-100%. In the application environment of network storage, jumbo frame has more extraordinary significance.

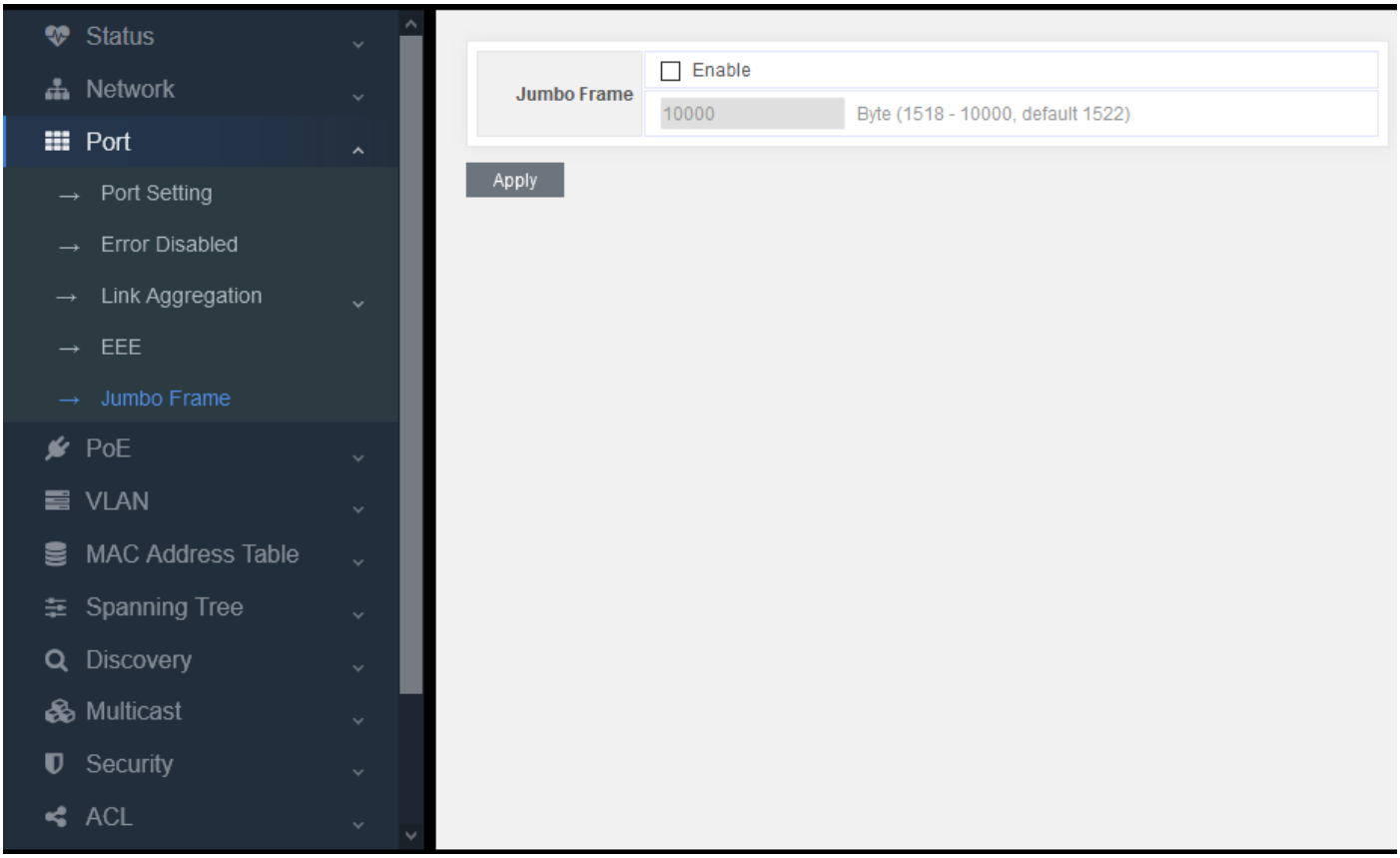


Figure 6-5

As long as jumbo frame is turned on, it can support the transmission speed up to 10K.

Part 7: VLAN

7.1 VLAN

This part is mainly about 802.1Q-VLAN

VLAN introduction

The traditional Ethernet is a broadcast network. All hosts are in the same broadcast domain and communicate with each other through hub or switch. Hub and switch are the basic network connection equipment only with limited forwarding function.

- The hub is a connection device on physical layer without switch function. It forwards the received messages to all ports except the receiving packet port.
- The switch is a link layer device that can forward messages depending on the MAC address of the message. The switch will establish a MAC address table and port mapping table, and only forward the known MAC traffic to one port.

When the switch receives a broadcast packet or an unknown multicast packet whose MAC is not in its MAC address table, it will forward the message to all ports except the port receiving the message.

The above settings may cause the following network problems

- A large number of broadcast packets or unknown unicast packets may exist in the network, which will waste network resources.
- A host will receive many messages that are not intended for the host itself, will will lead to serious potential security problems.
- For the above points, someone in the network can monitor broadcast packets and unicast packets and get their activity in the network. Then they can try to access other resources on the network whether they are authorized to do so.

The solution to the above problem is to isolate the broadcast domain. The traditional way is to use routers that forward packets according to the destination IP address and do not forward broadcast packets at the link layer. Routers are expensive and provide few ports, so they can not separate the network effectively. Therefore, there are many limitations to isolate broadcast domains by routers.

Virtual local area network (VLAN) technology of switch has been developed to control the broadcast in LAN.

A VLAN can cross many physical spaces, which can activate hosts of one VLAN in different physical positions. By creating VLANs in a physical LAN, you can divide the LAN into many logical LANs, each with its own broadcast domain. Hosts in the same VLAN can communicate with each other through the traditional Ethernet mode. However, hosts in different VLANs cannot communicate with each other directly, so they need network layer devices, such as routers or three-layer switches

Advantages of VLAN

Comparing with the traditional ethernet technology, VLAN technology owns the following advantages:

- Limit the broadcast domain in a separate VLAN, which can save bandwidth and improve network performance.
- Improve network security. By assigning user groups to different VLANs, you can isolate them on layer 2. It needs routers of three-layer switches to enable communication between different VLANs.
- Create variable virtual working groups. Users in the same working group can be assigned to the same VLAN, regardless of their physical location, which make network construction and maintenance easier and more variable.

7.1.1 Create VLAN

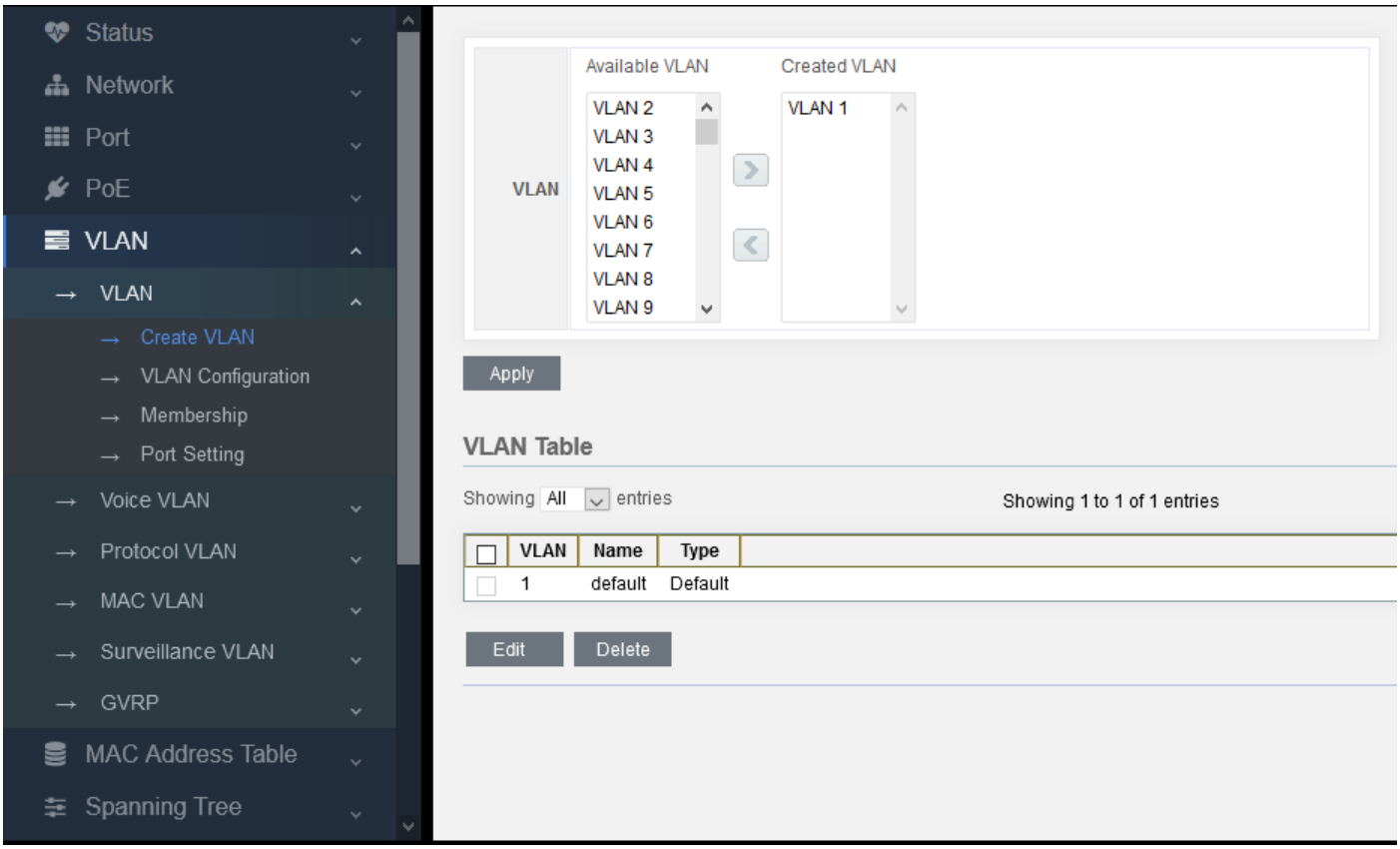


Figure 7-1-1

The total number of VLAN is 1-4094. Select the VLAN number in the left box and add it in the right one to join in and create VLAN 1 by default.

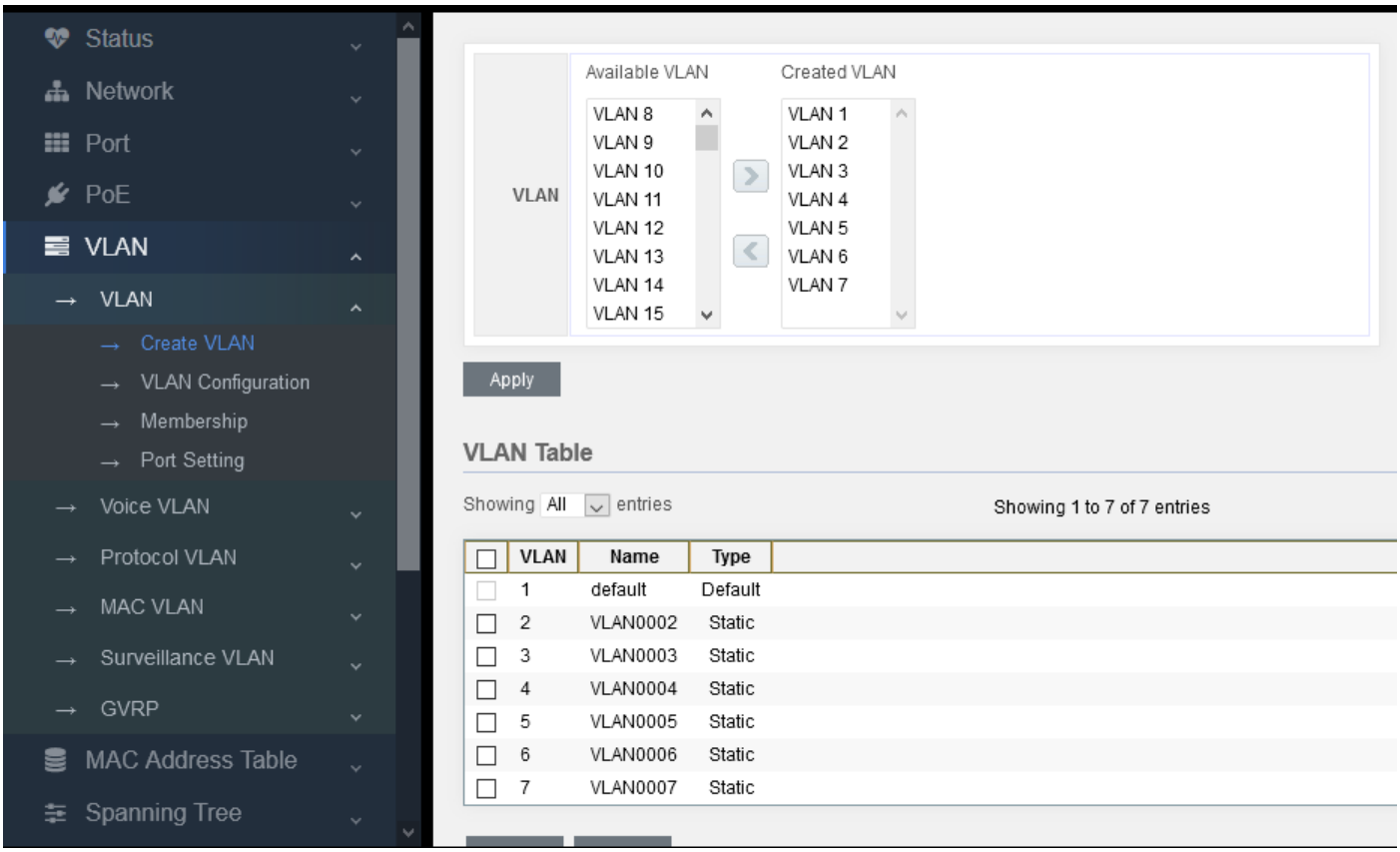


Figure 7-1-2

As above figure, add VLAN 2-7 in this way.

7.1.2 VLAN Configuration

Configure 802.1Q_VLAN for the switch.

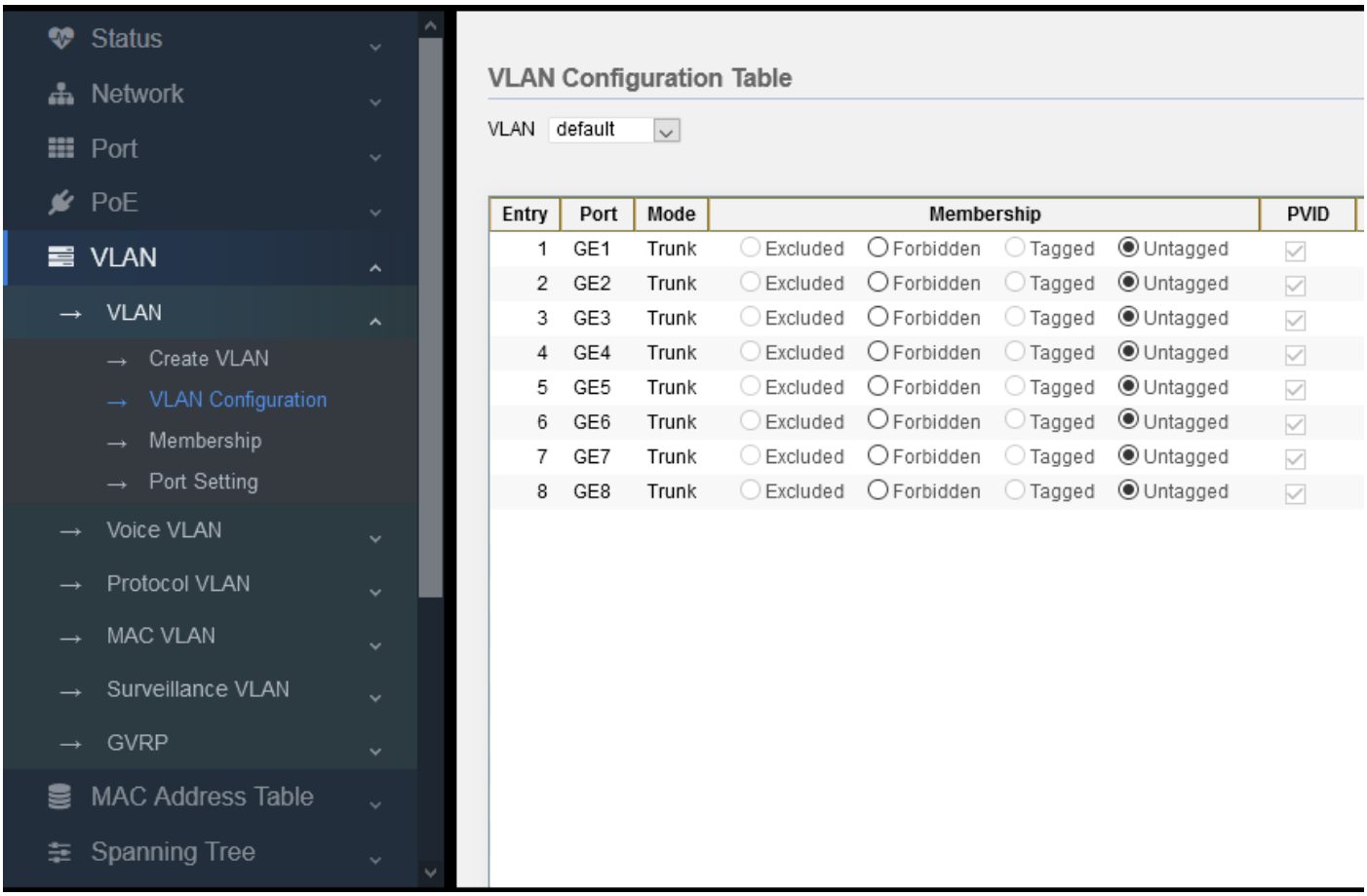


Figure 7-1-3

Default: default means VLAN 1. It is clear that all ports belong to VLAN 1 and they are untagged, PVID=1.

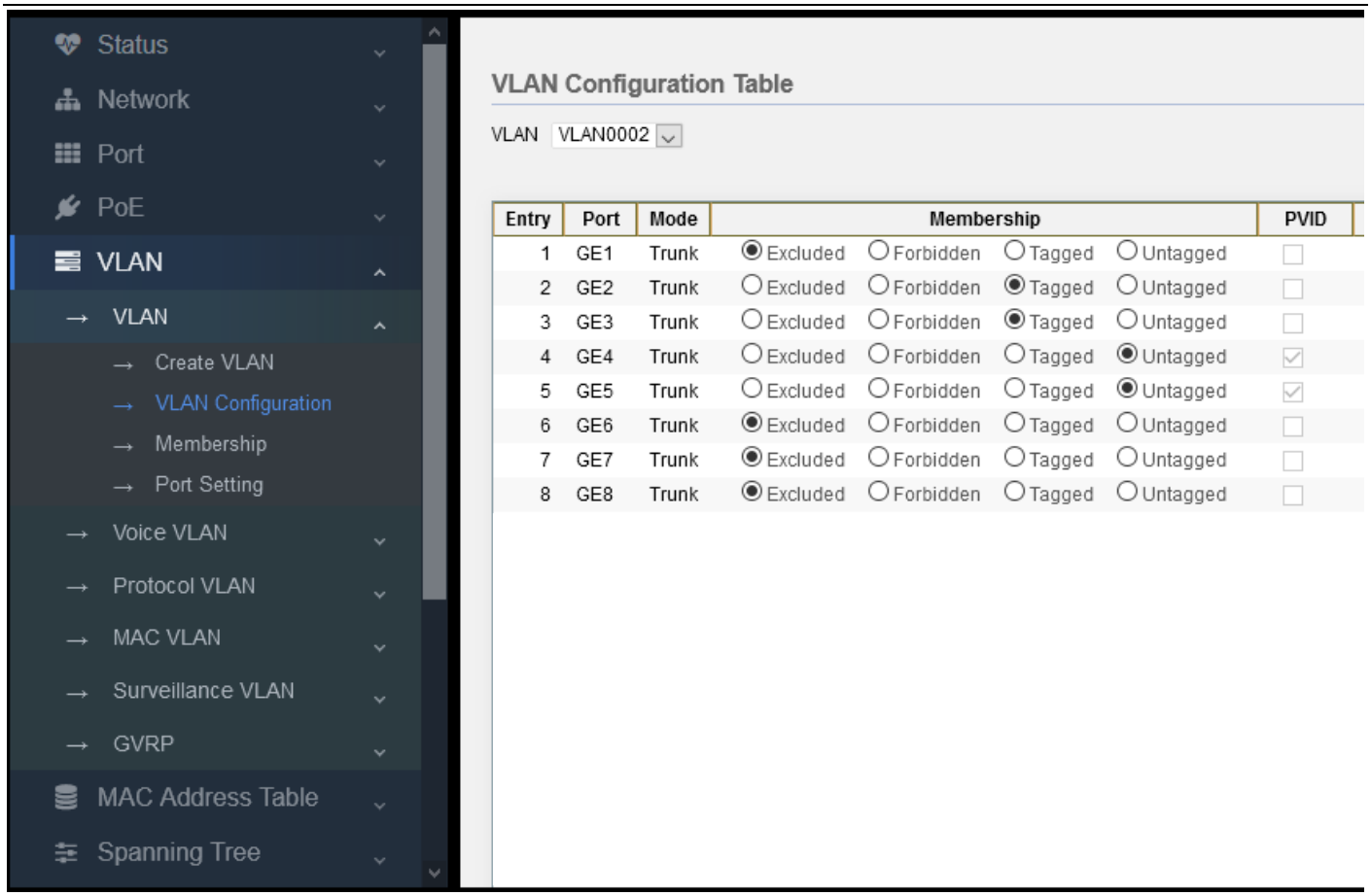


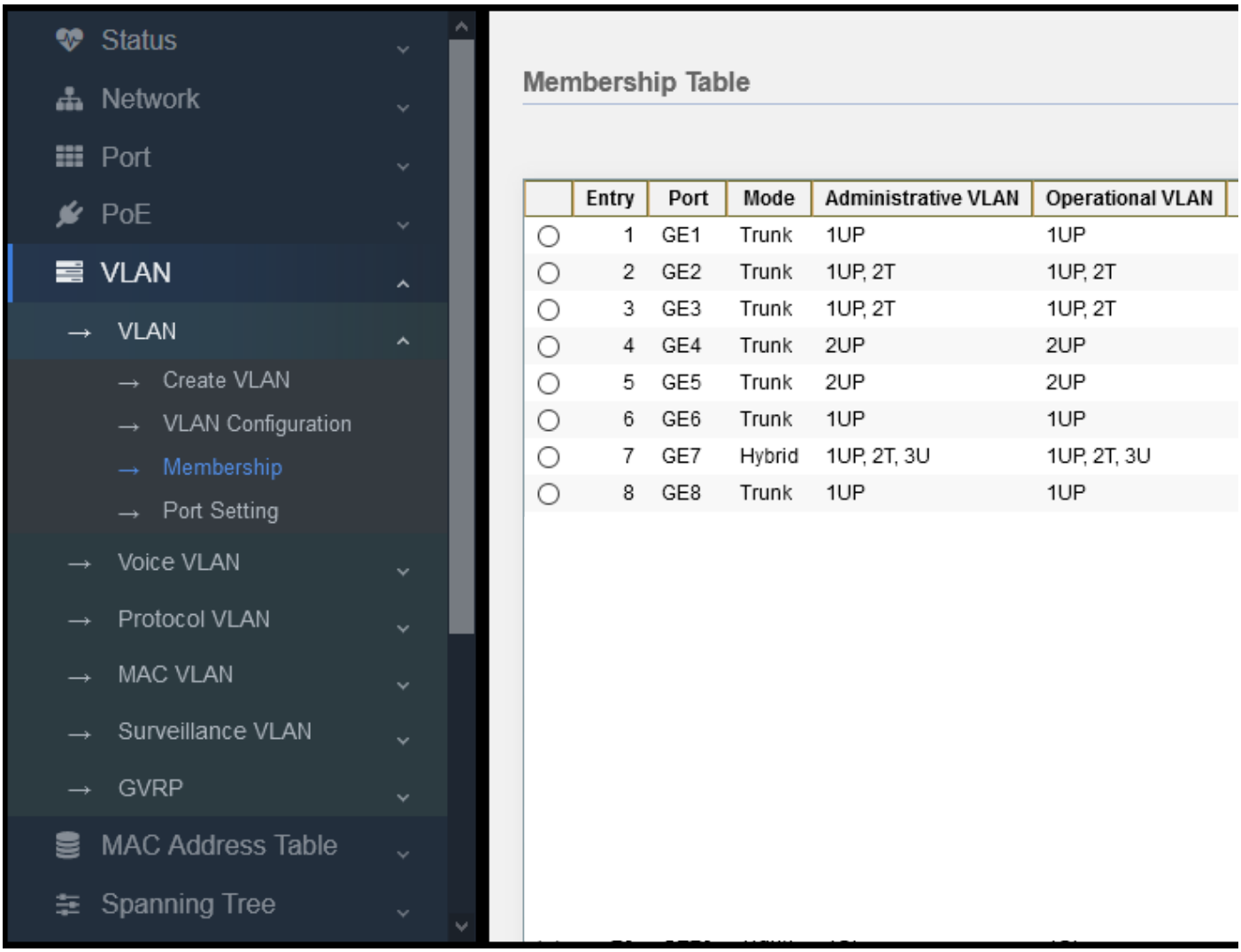
Figure 7-1-4

If VLAN 2 is selected for VLAN, there is no member by default, so it can be set manually.

As shown in the above figure, port 2-3 is added to the tagged member of VLAN 2, and port 4-5 is added to the untagged member of VLAN 2. However, since the port mode is trunk, if selecting untagged, PVID will changed to 2 automatically .

7.1.3 Membership

VLAN configuration of the switch.



	Entry	Port	Mode	Administrative VLAN	Operational VLAN
○	1	GE1	Trunk	1UP	1UP
○	2	GE2	Trunk	1UP, 2T	1UP, 2T
○	3	GE3	Trunk	1UP, 2T	1UP, 2T
○	4	GE4	Trunk	2UP	2UP
○	5	GE5	Trunk	2UP	2UP
○	6	GE6	Trunk	1UP	1UP
○	7	GE7	Hybrid	1UP, 2T, 3U	1UP, 2T, 3U
○	8	GE8	Trunk	1UP	1UP

Figure 7-1-4

As shown in the above figure, UP is Pvid value, T is Tagger, and U is untaged.
Port GE1，Trunk mode，Pvid=1
Port GE2，Trunk mode, Pvid=1，Tag-vid=2
Port GE4，Trunk mode，Pvid=2
Port GE7，Hybrid mode，Pvid=1，Tag-vid=2，Untag-vid=3

In the next section, we will introduce VLAN mode of port.

7.1.4 Port Setting

Configure the port mode, entrance detection function and TPID function.

There are three VLAN modes: Acess, Trunk, Hybird
Access: connect to terminal devices (such as PC, camera, set top box, etc.) and set PVID directly.
Trunk: the port connected between switches. Generally it needs to set many VLANs to perform tagged.
Hybrid: mixed mode. It can perform Tagged for many VLANs or Untagged for other VLANs.

Entrance detection:
When the port is a hybrid link, Tag messages, Untag messages, or all messages can pass the entrance detection.
TPID (tag protocol identifier) is a field in VLAN Tag. According to IEEE 802.1Q protocol, the value of this field is 0x8100. The device default is TPID value specified in the protocol (0x8100). Some manufacturers set 0x9100 or other values as the TPID value which can be identified by the device.

In order to be compatible with these devices, the device provides adjustable function for TPID value of global VLAN-VPN messageas, and users can configure TPID value by themselves. When the VLAN-VPN Uplink port forwards messages, it will replace the TPID value in the outer VLAN tag of the message with the user set value and then send it, so that the VLAN-VPN message sent to the public network can be recognized by the devices of other manufacturers.

So these parameters can be configured according to customer's needs

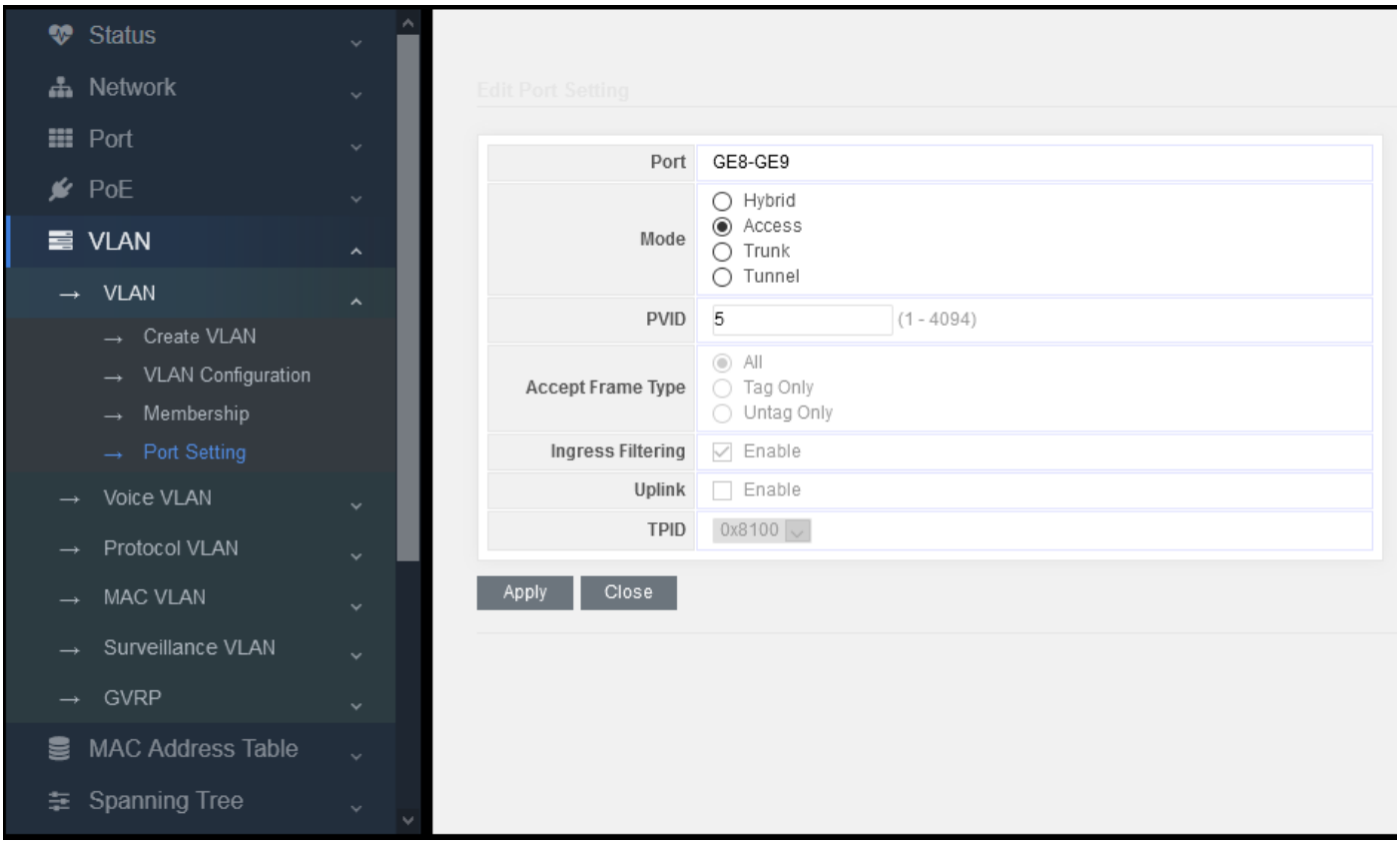


Figure 7-1-5

As shown in the figure above, set Access mode for Port 8 and 9 simultaneously and change PVID value to 5.

Caution:
When setting PVID value, VLAN must be added before setting. Vlan2-7 has been added in Chapter 7.1.1, so you can set 5. But if the value is set as 9, the system will report an error and the setting will be unsuccessful.
In normal conditions, the entrance detection filtering will not set, neither the TPID. Adopt the default value directly.

Caution:
If you need to check the log information, visit “Status-Logging Message” page.

Part 8: MAC Address Table

MAC address introduction

MAC address table introduction

The main function of Ethernet switch is to forward messages on the data link layer, that is, to output the message to the corresponding port according to the message's destination MAC address. MAC address forwarding table is a 2-layer forwarding table which contains the corresponding relationship between MAC address and forwarding port. It is the basis of Ethernet switch to realize layer-2 message fast forwarding, which is the base of forwarding the above 2-layer messages by the Ethernet switch quickly. The MAC address forwarding table entries include the following information:

- MAC destination address
- VLAN ID of the port
- Forwarding port number on the device

When the Ethernet switch forwards messages, it will adopt the following two forwarding methods according to the MAC address table entry information:

- Unicast mode: when the MAC address forwarding table contains a table entry corresponding to the MAC destination address of the message, the switch will send the message from the forwarding port of the table entry directly.
- Broadcast mode: when the switch receives the messages with the destination address of F, or the MAC address forwarding table does not contain the table entry of the corresponding message destination MAC address, the switch will adopt the broadcast mode to forward the message to all ports except the receiving port.

Introduction of MAC address learning process

The entries in MAC address forwarding table can be updated and maintained in two ways:

- Manual configuration mode
- MAC address learning mode

Usually, most MAC address table entries are created and maintained through MAC address learning function

Management of MAC address forwarding table

Aging mechanism of MAC address forwarding table

The MAC address forwarding table of Ethernet switch has capacity limitation. In order to maximize the utilization of address forwarding table resources, Ethernet switch adopts aging mechanism to update MAC address forwarding table, that is, when the system creates a table entry dynamically, it will turn on the aging timer, and if it does not receive the MAC address messages from this table entry again during the aging time, the switch will delete this MAC address table entry.

Classification and features of MAC address table entries.

According to their own features and configuration methods, MAC address table entries can be divided into three categories:

- Static MAC address table entry: also known as "permanent address", which is added and deleted manually by user and will not age with time. For a network with less equipment changes, it can reduce the broadcast traffic in the network to add static address table entries manually.

- Dynamic MAC address table entry: refers to the MAC address table entry that will age in accordance with the aging time set by user. The switch can add dynamic MAC address table entry through MAC address learning mechanism or by user's manual establishment.
- Black hole MAC address table entry: also known as filtered MAC address table, which is a special MAC address configured by users manually. When the switch receives a message whose source MAC address or destination MAC address is black hole MAC address, it will discard this message.

8.1 Dynamic Address

MAC address learned by this switch automatically, and the entries are as follows:

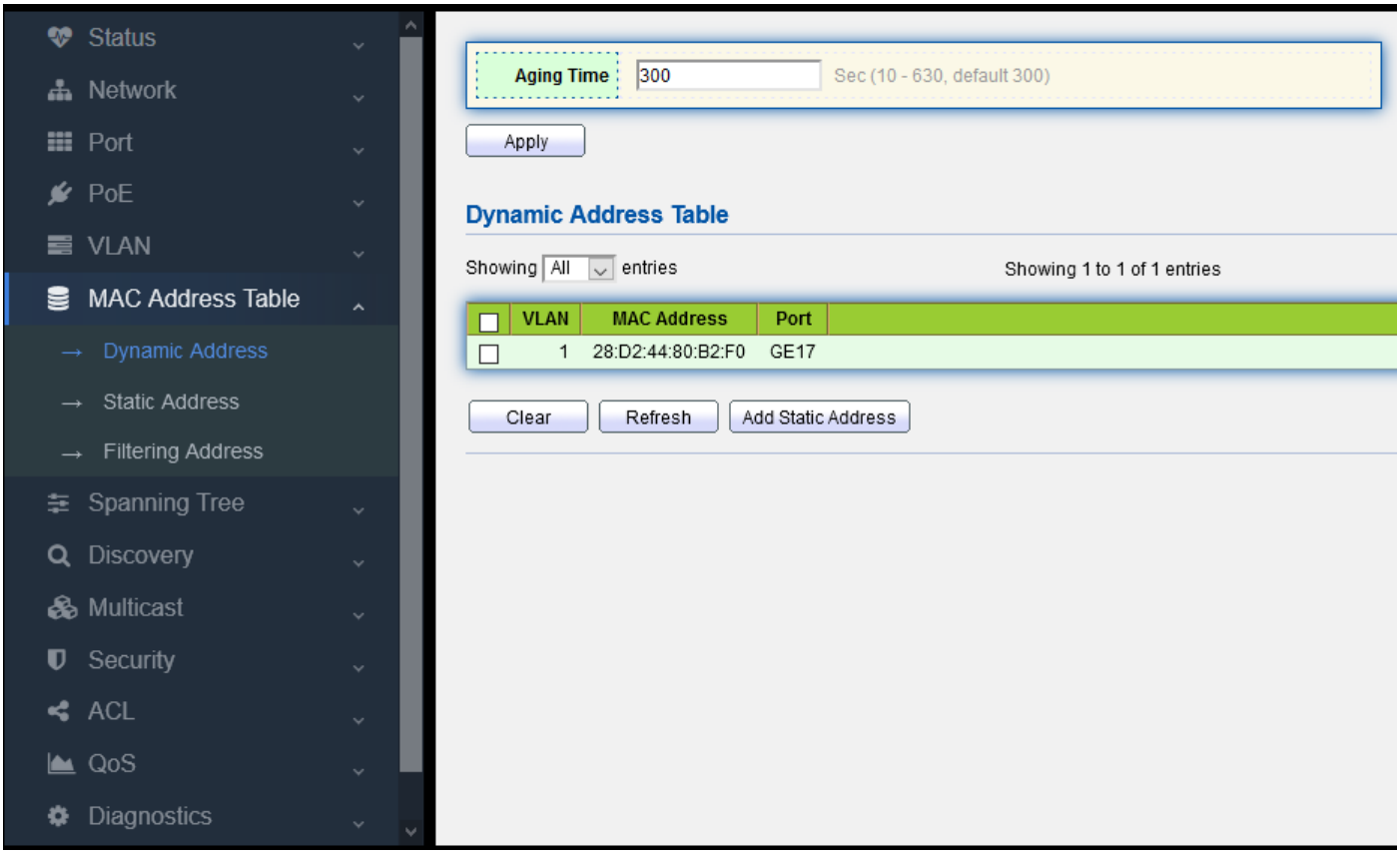


Figure 8-1-1

MAC address: learned by this switch automatically.
Port: transmitting the learned MAC address ta certain port.
VLAN ID (1-4094)：transmitting the learned MAC address to a certain VLAN;

8.2 Static Address

Set MAC address table entry

According to the actual condition, the administrator can add, modify or delete the entries in the MAC address forwarding table manually. He can delete all MAC address table entries related to a certain port, or choose to delete certain types of MAC address table entries, such as dynamic table entries and static table entries.
Users can add or delete static MAC address table entries in the page, which is also known as MAC address binding, that is to bind MAC address, port and VLAN.

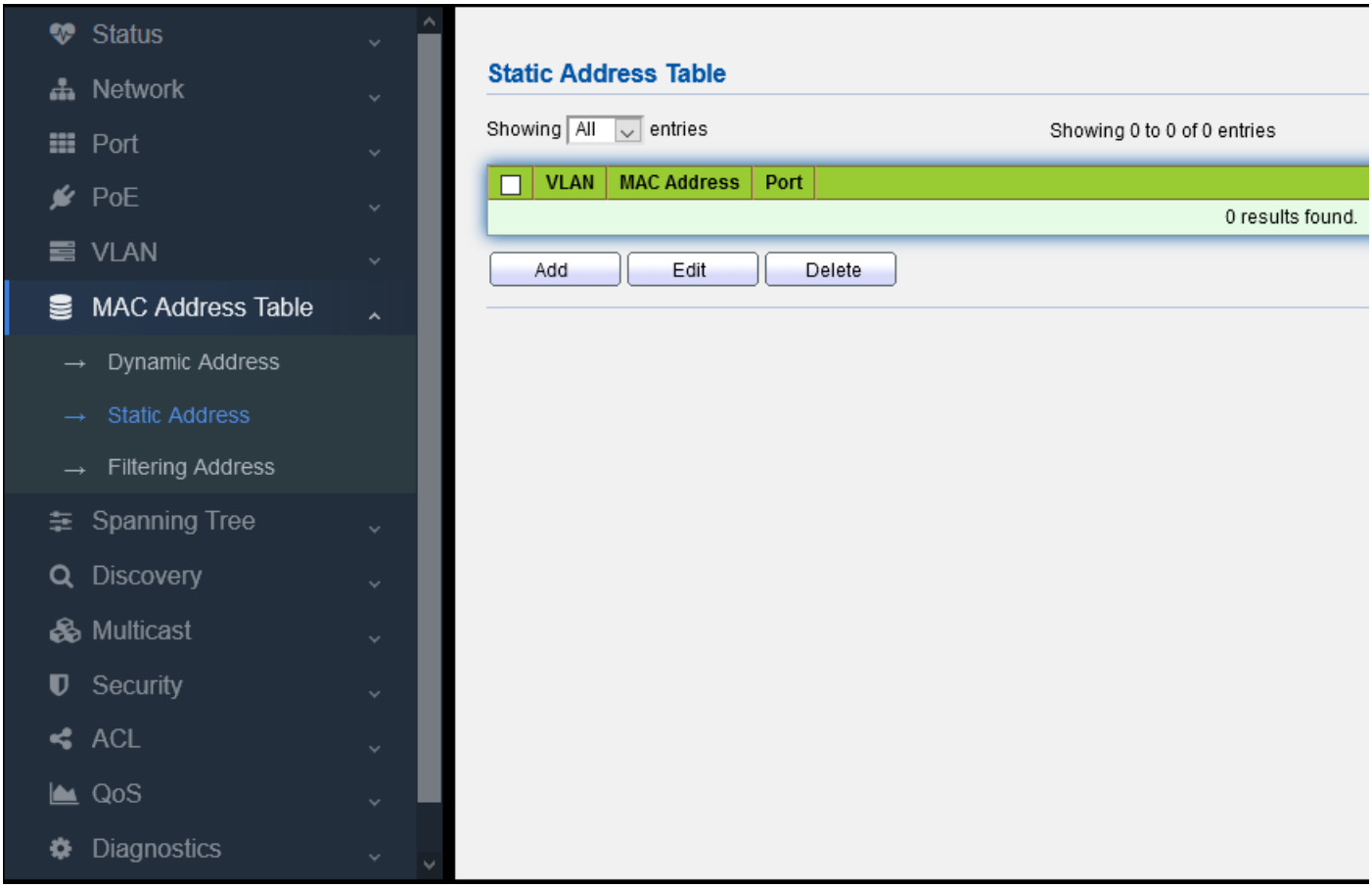


Figure 8-2-1

For example:

Add static MAC address 28:D2:44:80:B2:F0 to port GE 9 manually.

1. click “Add”, pop up the dialogue box of adding static MAC address.
2. input MAC address, VLAN number and port number to be bound
3. click “Apply”

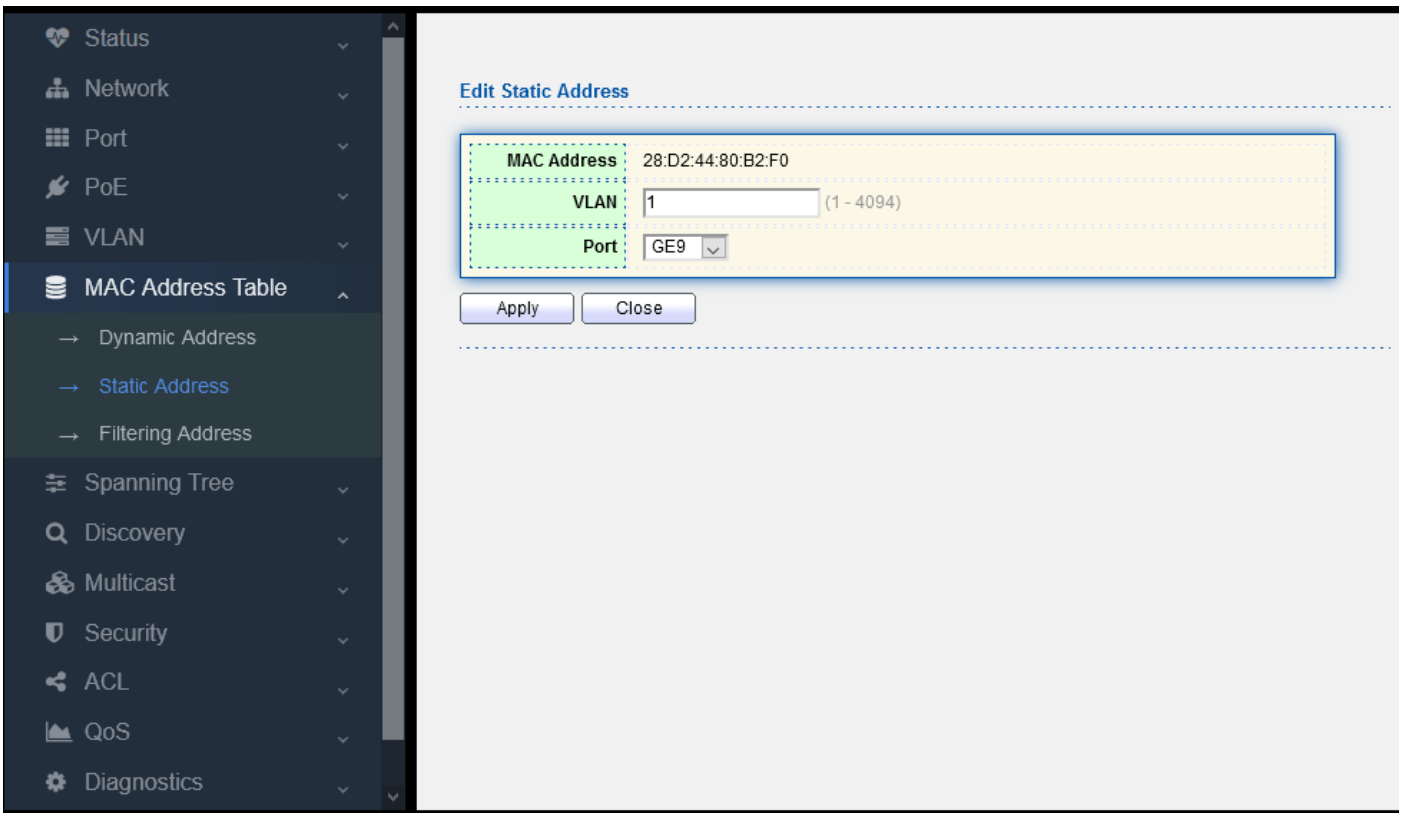


Figure 8-2-2

After the adding process, the page is shown as the following figure:

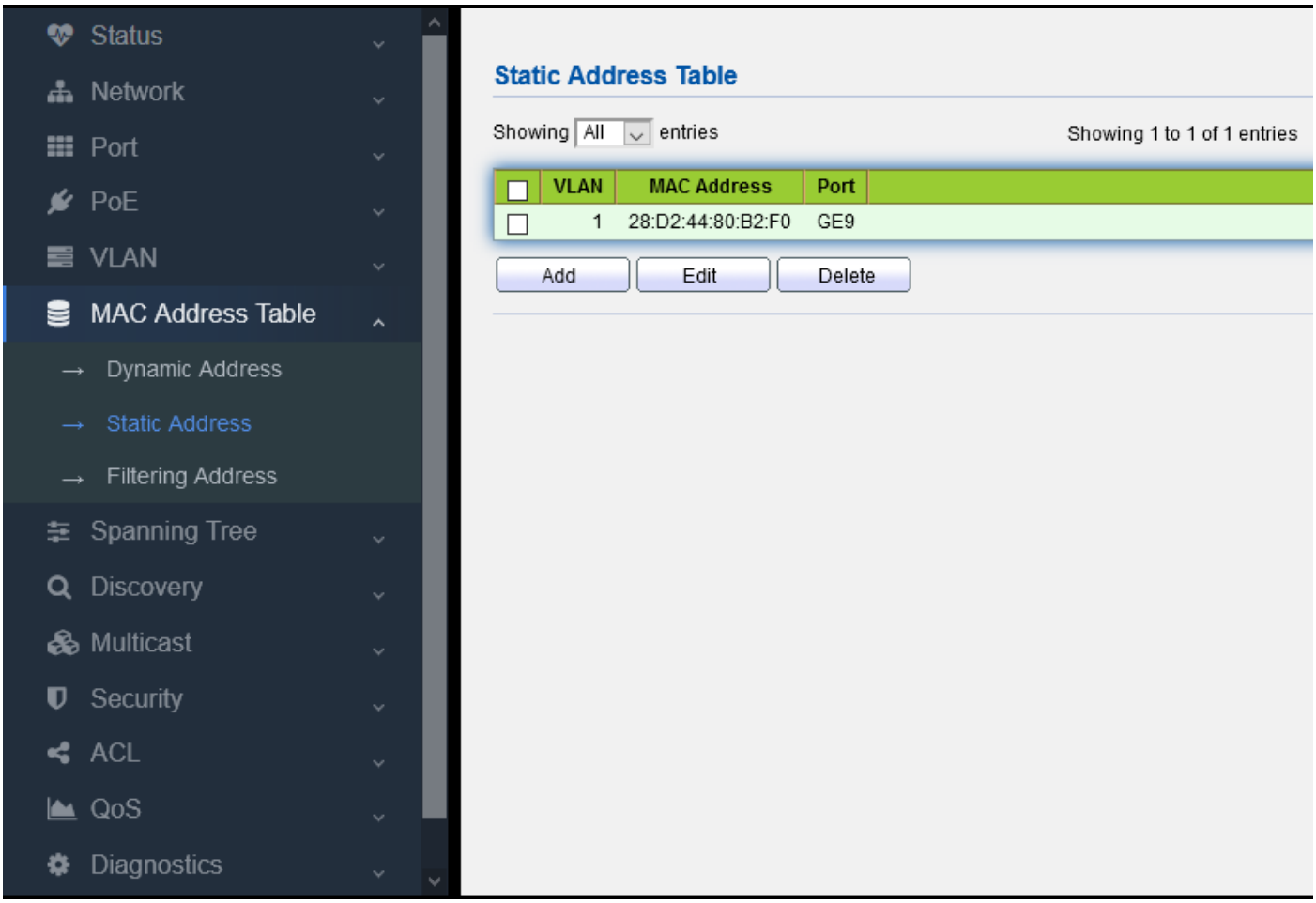


Figure 8-2-3

The results of binding configuration are as follows:

1. This MAC address can only communicate on port GE 9. If this MAC is connected to other port, it can not receive any message in which the destination address is this MAC. If the destination address received by this switch is the bound MAC address, this switch will only forward to this bound port.
2. After configuring the static MAC address, the address table entry that originally existed in the dynamic MAC is deleted.

8.3 MAC address filtering

If the MAC address filtering table entry is set in this switch, if the message with this MAC address whether in source MAC or destination MAC, it will be discarded as long as the switch receives it.

For example:
Add MAC address filtering: 00:E0:4C:20:C1:C0
1. click “Add”, pop up the dialog box of adding static MAC address.
2. input the MAC address and VLAN to be bound
3. click “Apply”

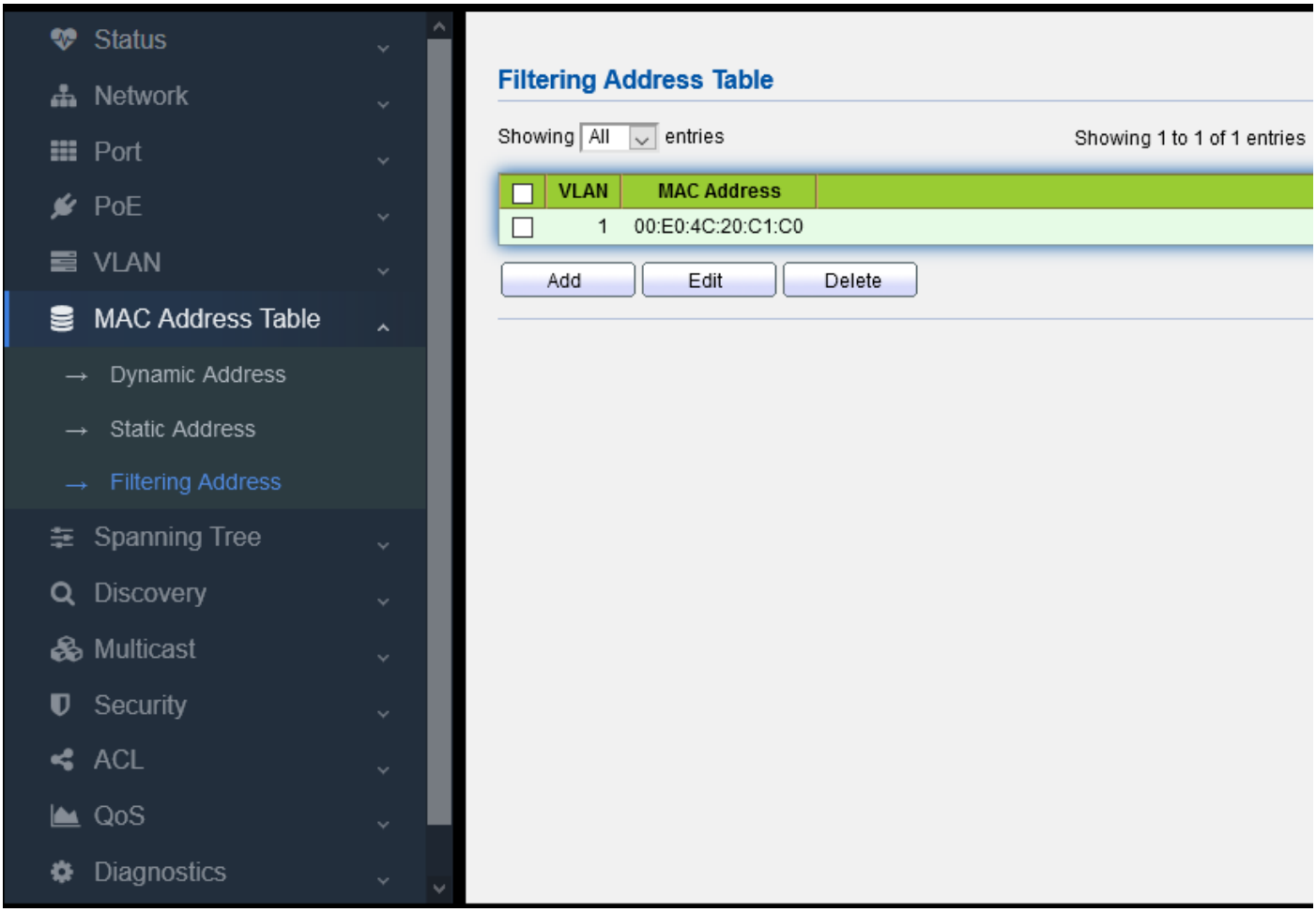


Figure 8-3-1

MAC address: input the MAC address to be rejected
VLAN ID (1-4094): input the VLAN of the rejected MAC address

8.4 MAC Aging time

Users can adjust the aging time of dynamic MAC address table entries. If the aging time configured by user is too long, the device may save many outdated MAC address table entries, thus exhaust the MAC address table resources, which will cause the device unable to update MAC address table according to the changes of the network. If the aging time configured by user is too short, the device may delete the effective MAC address table entries, which may cause the device to broadcast a large number of data packets and affect its operation performance. So users need to configure an appropriate aging time according to the actual situation so as to realize the MAC address aging function effectively.

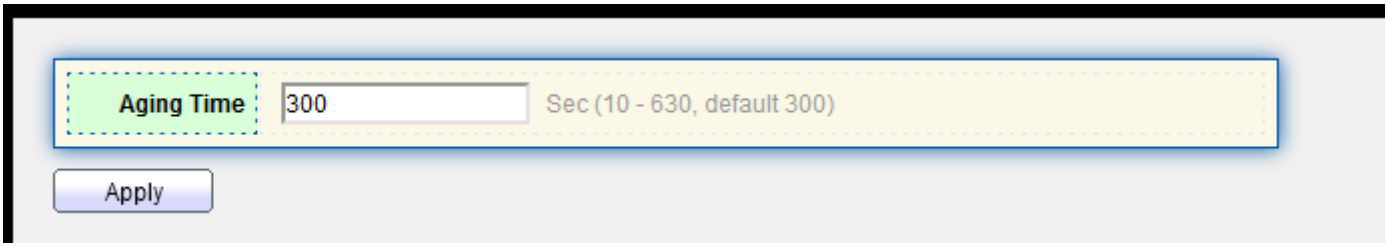


figure 8-4-1

Input aging time and click “OK”

The aging time of dynamic MAC address table will act on all ports, and the address aging will only work on dynamic (learned by the device or dynamic configured by user) MAC address table entries.

Part 9: Spanning Tree

9.1 STP introduction

9.1.1 STP application

STP (Spanning Tree Protocol) is a protocol based on IEEE 802.1D standard, which is used to eliminate the physical loop on data link layer in LAN. The devices running this protocol will find loops in the network through mutual information, and selectively block some ports. Finally, the loop network structure is pruned into a tree network structure without loops, so as to prevent from the continuous proliferation and infinite circulation of messages in the loop network, and avoid declining packet processing capacity caused by repeated receiving same messages.

STP includes two meanings. In narrow sense, STP refers to STP protocol defined in IEEE 802.1D, and in broad sense, it refers to the STP protocol defined in IEEE 802.1D and various improved spanning tree protocols based on it.

9.1.2 STP protocol messages

The protocol message in STP is BPDU (Bridge Protocol Data Unit), also known as configuration message.
STP can determine the network topology by transferring BPDU between devices. BPDU contains enough information to

ensure the device to complete the calculation process of spanning tree.

BPDU can be divided into two types in STP protocol

- Configuration BPDU: a message used to calculate spanning tree and maintain spanning tree topology.
- TCN BPDU (Topology Change Notification BPDU): when the topology changes, it is used to inform the network topology changes to related equipment.

9.1.3 Basic concept of STP

(1) Root bridge:

The tree network structure must have root, so STP introduces the concept of Root Bridge.

There is only one root bridge in the whole network, and the root bridge will change with the network topology, so the root bridge is not fixed.

After the network converges, the root bridge will generate and send the configured BPDU at a certain time interval, and other devices will transmit the configured BPDU to ensure the stability of the topology.

(2) Root port

The root port is the port nearest to the root bridge on a non-root bridge device. The root port is responsible for communicating with the root bridge. There is only one root port on a non-root bridge device. There is no root port on the root bridge.

(3) Specified bridge and specified port

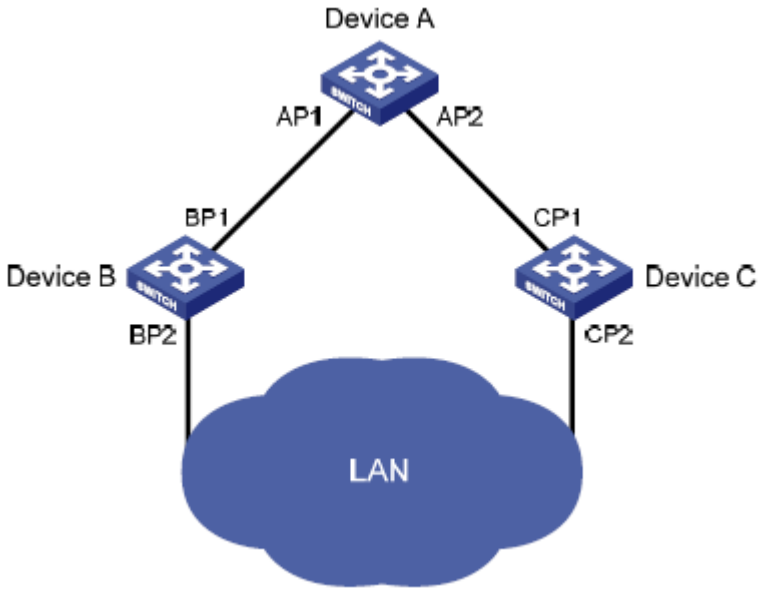
Refer to Table 1-1 for the definition of specified bridge and specified port.

Table 1-1 Definition of specified bridge and specified port

Type	Specified bridge	Specified port
For a device	This device is directly connected with the local machine and responsible for transmitting configuration messages to the local machine	This port will transmit configuration messages from the specified bridge to the local machine.
For LAN	This device is responsible for transmitting configuration messages to the local segment	This port will transmit configuration messages from the specified bridge to the local machine.

The specified bridge and specified port are shown in Figure 1-1, in which AP1, AP2, BP1, BP2, CP1 and CP2 is the ports of Device A, Device B and Device C respectively.

- If Device A transmits configuration messages to Device B through Port AP1, the specified bridge of Device B is Device A and its specified port is AP1.
- There are two devices connecting with LAN: Device B and Device C. If Device B is responsible for transmitting configuration messages to LAN, the specified bridge of LAN is Device B, and its specified port is BP2.



(4) Path cost

Path cost is the reference value of STP protocol for link selection. STP calculates the path cost to select the stronger link and block the redundant link, so as to prune the network into a tree network structure without loop.

9.1.4 Basic principle of STP

STP can determine the network topology by transmitting BPDU between devices. The configuration messages will contain enough information to ensure the device to complete the calculation process of generating trees, including several important information as follows:

- Root bridge ID: it consists of priority and MAC address of root bridge;
- Root path cost: path cost of arriving at the root bridge;
- Specified bridge ID: it consists of priority and MAC address of the specified bridge;
- Specified port ID: it consists of the priority and port name of the specified port;
- Lifetime of configuration messages spreading in the network: message age;
- Maximum lifetime of configuration message saved in the device: Max age;
- Cycle of transmitting configuration messages: Hello time;
- Delay of port state migration: forward delay.

(1) Specific process of STP algorithm implementation

- Initial state

AT the beginning, each port of each device will generate a configuration message taken itself as a root bridge. The root path cost is 0. The specified bridge ID is its own device ID and the specified port is its own port.

- Selection of optimal configuration message

Each device sends its own configuration messages to the outside, and receives the configuration messages sent by other devices.

The selection process of optimal configuration message is shown in table 1-2.

Table 1-2 Selection process of optimal configuration message

step	content
1	After receiving the configuration message, the process of each port is as follows: ● When the priority of the configuration message received by the port is lower than that of the port configuration message, the device will discard the received configuration message without any processing. ● When the priority of the configuration message received by the port is higher than that of the port, the device will replace the content of the port's configuration message by the received configuration message.
2	The device will compare the configuration messages of all ports to select the optimal one.

How to select a root bridge

During network initialization, all STP devices in the network will consider themselves as "root bridge", and the root bridge ID is their own device ID. By exchanging configuration messages, the root bridge IDs will be compared between devices, and the device with the smallest root bridge ID in the network is selected as the root bridge.

How to select a root port and a designated port

The selection process of root port and designated port is shown in table 1-3.

Table 1-3 Selection process of root port and designated port

Step	Content
1	The non-root-bridge device sets the port that receives the optimal configuration message as a root port
2	According to the configuration message and path overhead of the root port, the device calculates a designated port configuration message for each port: ● Replace the root bridge ID with the root bridge ID in the configuration message of the root port; ● Replace the root path overhead with the root path overhead of the root port configuration message plus the path overhead corresponding to the root port; ● Replace the designated bridge ID with its own device ID; ● Replace the designated port ID with its own port ID.
3	The device compares the calculated configuration messages with the configuration messages on the port which needs to determine its role, and take different processing methods on the basis of comparison results: ● If the calculated configuration message is superior, the device will set the port as the designated port, and the configuration message on this port will be replaced by the calculated configuration message and sent out periodically; ● If the configuration message on the port is superior, the device will not update the configuration message of this port and block it. The port will not forward data any more, only receive the configuration message without sending out.

Once the root bridge, root port and specified port are selected successfully, the whole tree topology will be established. The following is an example to illustrate the calculation process of STP algorithm. The specific networking is shown in Figure 1-2. The priority of device A is 0, of device B is 1, of device C is 2. The path overhead of all link is 5, 10, and 4 respectively.

Figure 1-2 Networking diagram of algorithm calculation process

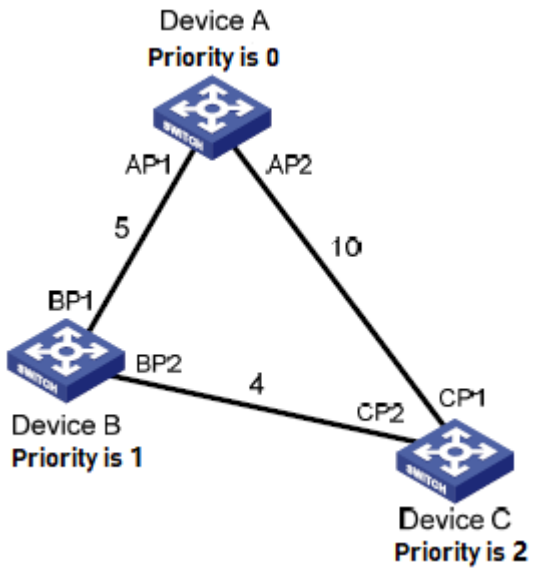


Table 1-4 Initial status of all devices

Device	Port name	Port configuration message
Device A	AP1	{0，0，0，AP1}
	AP2	{0，0，0，AP2}
Device B	BP1	{1，0，1，BP1}
	BP2	{1，0，1，BP2}
Device C	CP1	{2，0，2，CP1}
	CP2	{2，0，2，CP2}

- Comparison process and results of all devices

Shown in table 1-5.

Talbe 1-5 Comparison process and results of all devices

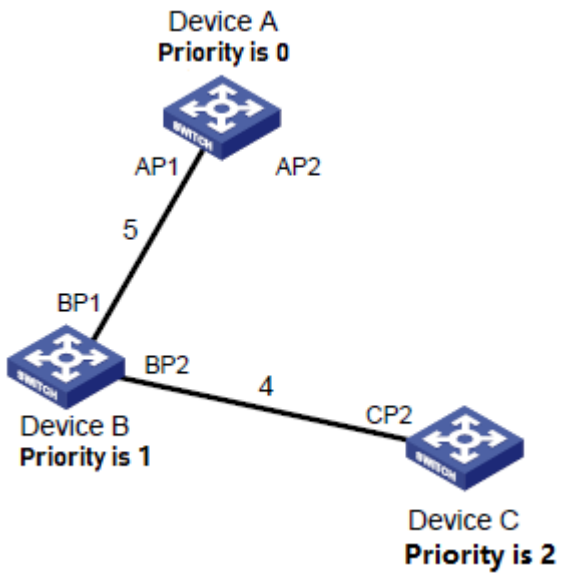
Device	Comparison process	Port configuration message after comparison
Device A	● Port AP1 receives the configuration message {1, 0, 1, BP1} from device B. Device A finds this port configuration message{0, 0, 0, AP1}is superior than the received configuration message, so it will discard the received one. ● Port AP2 receives the configuration message {2, 0, 2, CP1} from device C. Device A finds this port configuration message{0, 0, 0, AP1}is superior than the received configuration message, so it will discard the received one. ● If Device A finds that the root bridge and designated bridge in the configuration message of its own ports, it will regard itself as a root bridge without any modification of the configuration messages of all ports and then send configuration messages outside periodically.	AP1：{0，0，0，AP1} AP2：{0，0，0，AP2}
Device B	● Port BP1 receives the configuration message {0, 0, 0,AP1} from device A. Device B finds that the received configuration message is superior than its configuration one {1, 0, 1, BP1} of this port, so it will update the configuration message of port BP1. ● Port BP2 receives the configuration message {2, 0, 2, CP2} from device C. Device B finds that the configuration message {1, 0, 1, bp2} of this port is	BP1：{0，0，0，AP1} BP2：{1，0，1，BP2}

	superior than the received configuration one, so it will discard the received configuration message.	
	● Device B compares the configuration messages of all ports and selects the configuration message of port BP1 as the optimal one, and then sets port BP1 as the root port without any change of its configuration message. ● Device B calculates a designated port configuration message {0, 5, 1, bp2} for BP2 port on the basis of the configuration message and path overhead 5 of root port BP. ● Device B compares the calculated configuration message {0, 5, 1, bp2} with the configuration message on port BP2. The comparison result is that the calculated configuration message is better, so Device B will set port BP2 as the designated port, and its configuration message will be replaced with the calculated one and sent outside periodically.	Root port BP1: {0，0，0，AP1} Designated port BP2: {0，5，1，BP2}
Device C	● When port CP1 receives the configuration message {0, 0, 0, ap2} from device A, device C finds that the received configuration message is better than the configuration message {2, 0, 2, CP1} of this port, so it will update the configuration message of port CP1. ● Port CP2 receives the configuration message {1, 0, 1, bp2} from BP2 of Device B before update. Device C finds that the received configuration message is better than the configuration message {2, 0, 2, CP2} of this port, so it will update the configuration message of port CP2.	CP1：{0，0，0，AP2} CP2：{1，0，1，BP2}
	After comparison: ● The configuration message of port CP1 is selected as the optimal one, and port CP1 is set as the root port without any change of its configuration message. ● After comparing the calculated configuration message {0, 10, 2, CP2} of the designated port with the configuration message of port CP2, port CP2 will be converted to the designated port, and its configuration message is replaced by the calculated configuration message.	Root port CP1: {0，0，0，AP2} Designated port CP2: {0，10，2，CP2}
	● Then port CP2 will receive the updated configuration message {0, 5, 1, bp2} from device B. Because the received configuration message is better than the original one, device C will trigger the update process. ● At the same time, port CP1 will receive the configuration message periodically sent by device A. After comparison, device C will not trigger the update process.	CP1：{0，0，0，AP2} CP2：{0，5，1，BP2}
	After comparison: ● The root path overhead 9 of port CP2 (root path overhead 5 of the configuration message + path overhead 4 of port CP2) is less than the root path overhead 10 of port CP1 (root path overhead 0 of the configuration message + path overhead 10 of port CP1), so the configuration message of port CP2 is selected as the optimal one, and port CP2 is set as the root port without any change of its configuration message. ● After comparing the configuration message of port CP1 with the calculated configuration message of the designated port, port CP1 is blocked without any change of its port configuration message, and will not receive the data forwarded from device A until a new condition triggers the calculation of spanning tree, such as that the link from device B to device C is down.	Blocked port CP1: {0，0，0，AP2} Root port CP2: {0，5，1，BP2}

After the comparison in the above table, a spanning tree which takes Device A as its root bridge is formed, as shown in Figure

1-3.

Figure 1-3 Spanning tree after calculation



(2) Transmission mechanism of SPT configuration message

- When the network is initialized, all devices take themselves as their root bridge and generate configuration messages taken themselves as the root to send them out periodically with Hello Time .
- If the port receiving the configuration message is the root port, and the received configuration message is superior than that of the port, the device will increment the Message Age in the configuration message by certain principles, start a timer to reckon the time for the configuration message, and forward it from the designated port of the device.
- If the priority of the configuration message received by the designated port is lower than that of the port, it will immediately send its own better configuration message to respond.
- If a path fails, the root port on this path will not receive any new configuration messages, and the old ones will be discarded due to timeout. The device will regenerate the configuration message taken itself as the root and sends it outside, which will cause the recalculation of a spanning tree to get a new path to replace the failed link and restore the network.

However, the new calculated configuration message will not be transmitted to the whole network immediately, so the old root port and designated port will continue to forward data along the original path because they don't find out the change in the network topology. If the newly-selected root port and designated port start to forward data immediately, it may cause a temporary loop.

(3) STP timer

In STP calculation, there are three important time parameters to be used: Forward Delay, Hello Time and Max Age.

- **Forward delay** refers to the delay time of device state migration. Link failure will cause the network to recalculate the spanning tree, and its structure will change accordingly. However, the new calculated configuration message will not be transmitted to the whole network immediately. If the newly-selected root port and designated port start to forward data immediately, it may cause a temporary loop. For this reason, STP adopts a state migration mechanism. The newly-selected root port and designated port can only forward data after two times of forward delay, which ensures that the new configuration message has been transmitted throughout the whole network.
- **Hello time** is used to detect whether there is a failure in the link by the device. At every Hello Time interval, the device will send Hello message to surrounding devices to confirm whether the link is failed.
- **Max Age** parameter is used to determine whether the storage time of configuration messages in the device is "out of

date”. The device will discard the out-of-date configuration messages.

9.2 MSTP Introduction

9.2.1 MSTP Background

(1) Shortages of STP and RSTP
STP can't migrate quickly. Even in a point-to-point link or edge port (which means that this port is directly connected to the user terminal without connection with other devices or shared network segment), it must wait twice forward delay time before migrating to the forwarding state.

RSTP (rapid spanning tree protocol) is an optimized version of STP protocol, in which the "fast" means that when a port is selected as the root port and the designated port, the delay time of entering the forwarding state is shortened greatly under certain conditions, so as to shorten the time required for the network to achieve the final topological stability.

- In RSTP, the condition of the root port state to migrate rapidly is that the old root port on this device has stopped forwarding data, and the upstream designated port has started forwarding data.
- In RSTP, the condition of the designated port state to migrate rapidly is that the designated port is an edge port or a designated port connecting with the point-to-point link. If the designated port is an edge port, this port can enter the forwarding state directly; if the designated port is connecting with a point-to-point link, this device can connect with the downstream device and immediately enter the forwarding state just receiving the response.

RSTP can converge quickly, but it has the following defects similar as STP: all bridges in LAN will share a spanning tree, so it can't block redundant links according to VLAN, and all VLAN packets will be forwarded along one spanning tree.

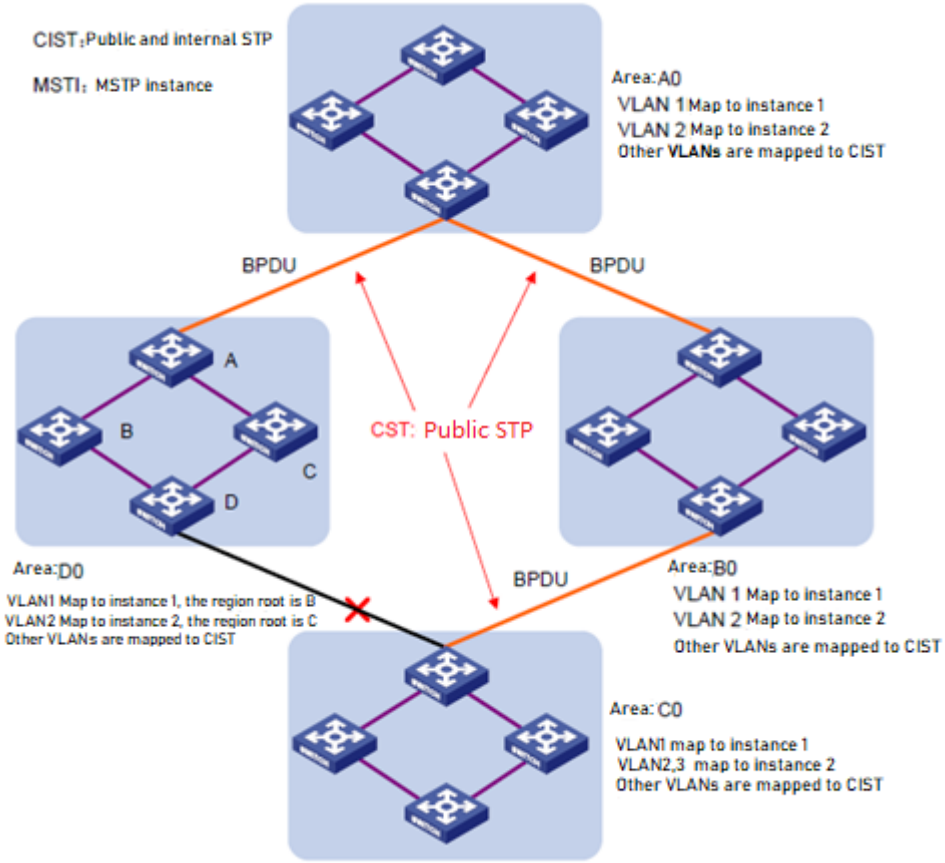
(2) Features of MSTP
MSTP (multiple spanning tree protocol) can make up for the defects of STP and RSTP. It can converge quickly and make the traffic in different VLANs forwarding along their own paths, thus providing a better load sharing mechanism for redundant links. For the introduction of VLAN, please refer to "VLAN Configuration" in "Access Volume".

Features of MSTP:
- MSTP can set a VLAN mapping table (which is a corresponding relationship table between VLAN and spanning tree) to connect VLAN and spanning tree. By adding the concept of "instance" (integrating many VLANs into a set), many VLANs will be bound in one instance to save communication overhead and resource utilization.
- MSTP will divide a switched network into many regions in which there are many independent spanning trees.
- MSTP will prune the loop network into a tree network without loop to avoid the proliferation and infinite circulation of packets in the loop network. At the same time, it will also provide many redundant paths for data forwarding to realize VLAN data load sharing in the process of data forwarding.
- MSTP is compatible with STP and RSTP.

9.2.2 Basic Concept of MSTP

Each device is running MSTP in Figure 4. Some basic concepts of MSTP will be explained with the following graphics. The following will explain some basic concepts of MSTP with graphics.

Figure 1-4 Basic concepts diagram of MSTP



(1) MST Region

MST region (multiple spanning tree regions) is composed of many devices in switched network and network segments between them. These devices have the following features:

- Have same region name;
- Set the same mapping configuration from VLAN to spanning tree instance;
- Set the same MSTP revision-level configuration;
- Have physical links between these devices.

For example, in area A0 in Figure 1-4, all devices in this region have a same MST region configuration:

- Same region name;
- Same mapping relationship between VLAN and spanning tree instance (VLAN 1 is mapped to the spanning tree instance 1, VLAN 2 is mapped to the spanning tree instance 2, and other VLANs are mapped to CIST, in which CIST is the spanning tree instance 0);
- Same MSTP revision level (which is not shown in the above figure).

There will be many MST regions in a switched network. Users can divide many devices into one MST region through MSTP configuration commands.

(2) WLAN mapping table

VLAN mapping table is an attribute of MST region, which is used to describe the mapping relationship between VLAN and spanning tree instance.

For example, in Figure 1-4, the VLAN mapping table of region A0 is: VLAN 1 is mapped to spanning tree instance 1, VLAN 2 is mapped to spanning tree instance 2, and other VLANs are mapped to CIST. MSTP can achieve load sharing on the basis of VLAN mapping table.

(3) IST
IST (internal spanning tree) is a spanning tree in MST region.
IST and CST (common spanning tree) will form the spanning tree CIST (Common and Internal Spanning Tree) of the whole switched network. IST is the fragment of CIST in MST region.
For example, in Figure 1-4, CIST has a fragment in each MST region, which is the IST in each region.

(4) CST
CST is a single spanning tree to connect all MST regions in a switched network. If each MST region is regarded as a "device", CST is a spanning tree generated by these “devices” through STP protocol and RSTP protocol calculation.
For example, the red line in Figure 1-4 is CST.

(5) CIST
CIST is a single spanning tree to connect all devices in a switched network, which is composed of IST and CST.
For example, in Figure 1-4, the IST in each MST region and the CST between MST regions will form the CIST of the whole network.

(6) MSTI
A MST region can generate many spanning trees through MSTP, and these spanning trees are independent of each other. Each spanning tree is called MSTI (multiple spanning tree instance).
For example, in Figure 1-4, there will be many spanning trees in each region, and each spanning tree will correspond to the corresponding VLAN. These spanning trees are called MSTI.

(7) Region Root
The root bridge of IST and MSTI in MST region is the region root. The topology of each spanning tree in MST region is different, so the region root may also be different.
For example, in Figure 1-4, the region root of spanning tree instance 1 in the region D0 is the Device B, and the region root of spanning tree instance 2 is Device C.

(8) Common Root Bridge
Common root bridge refers to the root bridge of CIST.
For example, in Figure 1-4, the common root bridge is a device in region A0.

(9) Region boundary port
Region boundary port is the port located at the edge of MST region to connect different MST regions, MST regions and regions running STP, MST regions and regions running RSTP.
For example, in Figure 1-4, if one device of region A0 is connected to the first port of a device in region D0 and the common root of the whole switched network is located in A0, the first port on this device in region D0 is the region boundary port of region D0.
The role of region boundary port on the spanning tree instance is consistent with that of CIST, except for Master port of which the role on CIST is Root port, but the role on other instances is Master port.

(10) Port role
In MSTP calculation process, port roles mainly include root port, designated port, Master port, Alternate port, Backup port and so on.

- Root port: forwarding data to the root bridge.
- Designated port: forwarding data to downstream network segments or devices.
- Master port: connecting the MST region to the common root, which is located on the shortest path from the whole region to the common root. From the perspective of CST, the Master port is a "root port" of the region (regarding the

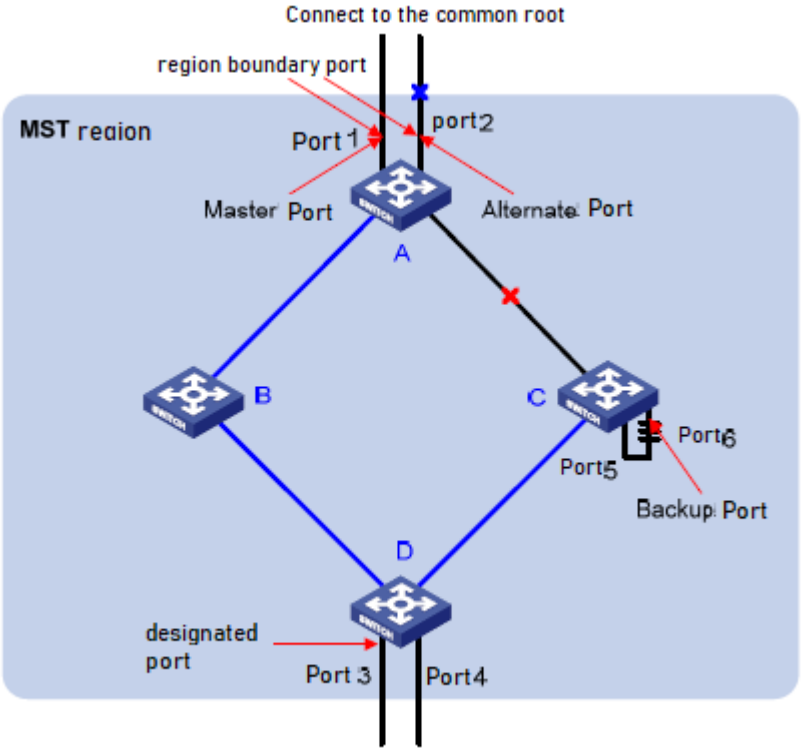
region as a node). The role of Master port in IST/CIST is root port, and the role in other instances is Master port.

- Alternate port: backup port of root port and master port. When the root port or Master port is blocked, the Alternate port will become the new root port or Master port.
- Backup port: designated port of the backup port. When the designated port is blocked, the backup port will convert to a new designated port quickly and forward data without delay. When two ports of one device with MSTP are open and connected with each other, there will be a loop. At this time, the device will block one of the ports, and the backup port is the blocked one.

Ports will play different roles in different spanning tree instances.
Please refer to figure 1-5 to understand the above concepts. In the picture:

- Equipment A, B, C and D form an MST region.
- The port 1 and port 2 of device A are connected to the common root.
- Port 5 and port 6 of device C form a loop.
- Port 3 and port 4 of device D connect to other MST regions downward.

Figure 1-5 Port role diagram



(11) Port status

In MSTP, according to whether the port learns MAC address and forwards user's traffic, its status can be divided into the following three types:

- Forwarding status: learning MAC address and forwarding user's traffic;
- Learning status: Learning MAC address and not forwarding user's traffic;
- Discarding status: Neither learning MAC address nor forwarding user's traffic.

There is no necessary connection between the port status and its role. Table 1-6 shows the port status of various port roles ("√" means that this port role can have this status; "--" means that this port role cannot have this status).

Table 1-6 Port status of various port roles

Port role Port status	Root port/Master port	Designated port	Alternate port	Backup port
Forwarding	√	√	--	--
Learning	√	√	--	--
Discarding	√	√	√	√

9.2.3 Basic principle of MSTP

MSTP divides the whole two-layer network into multiple MST regions, and CST is generated between the regions by calculation; multiple spanning trees are generated in the region by calculation, and each spanning tree is known as a multiple spanning tree instance, in which instance 0 is IST and other multiple spanning tree instances are MSTI. MSTP, like STP, uses configuration message to calculate spanning tree, but the configuration message carries the configuration information of the device MSTP.

(1) Calculation of CIST spanning tree

After comparing the configuration messages, a device with the highest priority in the whole network is selected as the root bridge of CIST. In each MST region, MSTP will generate IST through calculation; meanwhile, MSTP will treat each MST region as a single device and generate CST between regions through calculation. CST and IST constitute the CIST of the whole network.

(2) Calculation of MSTI

In MST region, MSTP will generate different spanning tree instances for different VLANs according to the mapping relationship between VLAN and spanning tree instances. Each spanning tree is calculated independently. The calculation process is similar to that of STP. See “1.1.14. Basic principle of STP”.

In MSTP, a VLAN message will be transmitted along the following path:

- In MST region, transmitted along its corresponding MSTI;
- Between MST regions, transmitted along CST.

9.2.4 Realization of MSTP on equipment

MSTP is compatible with STP and RSTP. Messages of STP and RSTP protocols can be identified by MSTP devices and applied to calculate spanning tree.

In addition to providing the basic functions of MSTP, this device also provides many special functions which are convenient for management from the user's point of view, as follows:

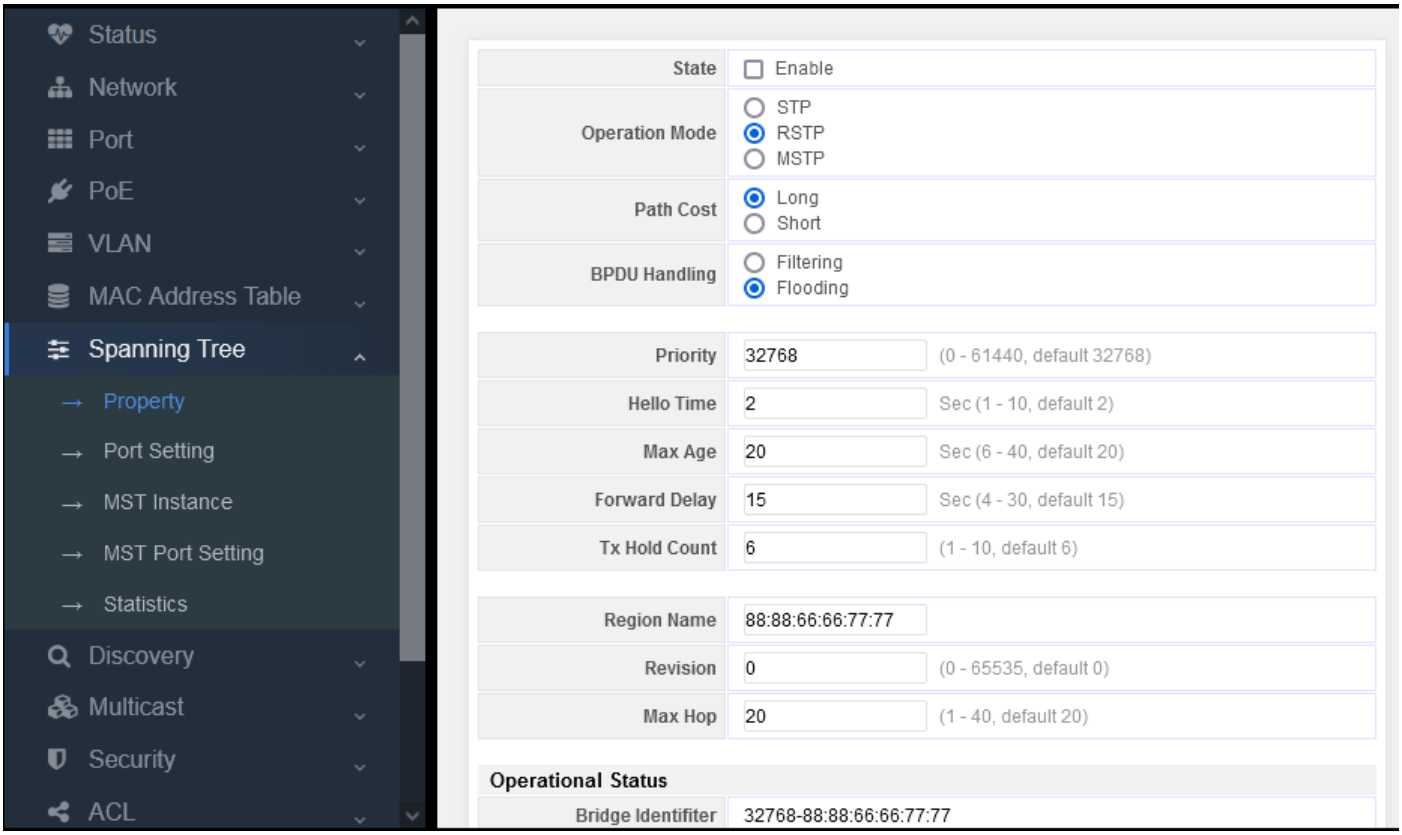
- Root bridge maintenance;
- Root bridge backup;
- Root protection function;
- BPDU protection function;
- Loop protection function;
- Anti-attack function from TC-BPDU message.

9.3 Protocol

Relevant protocols:

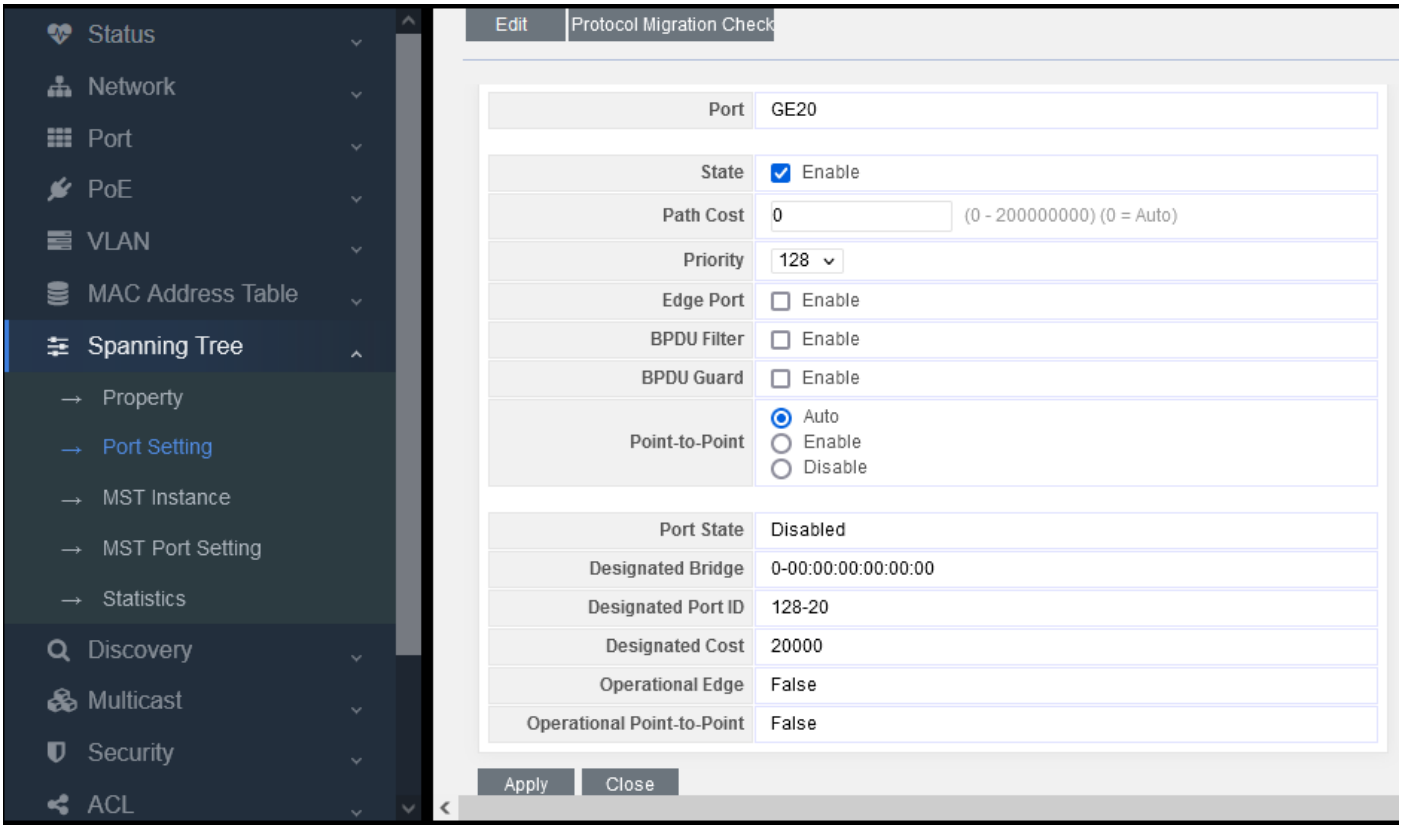
- IEEE 802.1D：Spanning Tree Protocol
- IEEE 802.1w：Rapid Spanning Tree Protocol
- IEEE 802.1s：Multiple Spanning Tree Protocol

9.4 Property



State: enable (complete switch spanning tree configuration, ticked for enabling, not ticked for dis-enabling)
Operation mode: STP/RSTP/MSTP (three modes for selection)
Path cost: Long/Short (the value range is short integer (short: 1-65535) (long: 1-200000000))
BPDU handling: Filtering/Flooding (Filtering or flooding BPDU messages)
Priority: configure the priority for the switch. The value range is 0 to 61440. It is increased by a multiple of 4096. The default value is 32768.
Hello time: configure the time interval of transmitting BPDU messages for the switch. The default value is 2 seconds.
Max age time: configure the longest lifetime of BPDU messages. The default value is 20 seconds.
Forward delay time: configure the time interval of port state change. The default value is 15 seconds.
TX hold count: configure the maximum number of BPDUs transmitted per second. The default value is 3.

9.5 Port Setting



State: Enable (As the spanning tree configuration of the switch port, ticked for enabling, not ticked for dis-enabling)
Path cost: Long/Short (the value range is short integer (short: 1-65535) (long: 1-200000000))
Priority: configure the priority of the switch port, ranging from 0 to 240.
Edge port: a port configured as an edge port can directly change the port state to forwading when it is up
BPDU filter: when BPDU filter is configured on the port, the interface will not send and receive BPDU messages any more.
BPDU guard: when BPDU guard is configured on the port, once a BPDU packet that should not exist is received on a specified interface, the interface will be cut off directly to make it in the soft close err disabled state. Compared with BPDU filter, this method is more robust.
Point to point: when BPDU filter is configured on the port, the interface will not send and receive BPDU messages any more

Part 10: ERPS(G.8032)

Ethernet Ring Protection Switching (ERPS) is a protocol defined by the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) to eliminate loops at Layer 2. It implements convergence of carrier-class reliability standards, and allows all ERPS-capable devices on a ring network to communicate.

10.1 introduction

Definition

Ethernet Ring Protection Switching (ERPS) is a protocol defined by the International Telecommunication Union - Telecommunication Standardization Sector (ITU-T) to eliminate loops at Layer 2. Because the standard number is ITU-T G.8032/Y1344, ERPS is also called G.8032. ERPS defines Ring Auto Protection Switching (RAPS) Protocol Data Units (PDUs) and protection switching mechanisms.

ERPS has two versions: ERPSv1 released by ITU-T in June 2008 and ERPSv2 released in August 2010. EPRSv2, fully compatible with ERPSv1, provides the following enhanced functions:

- Multi-ring topologies, such as intersecting rings
- RAPS PDU transmission on virtual channels (VCs) and non-virtual-channels (NVCs) in sub-rings
- Forced Switch (FS) and Manual Switch (MS)
- Revertive and non-revertive switching

Purpose

Generally, redundant links are used on an Ethernet switching network such as a ring network to provide link backup and enhance network reliability. The use of redundant links, however, may produce loops, causing broadcast storms and rendering the MAC address table unstable. As a result, communication quality deteriorates, and communication services may even be interrupted. Table 10-1 describes ring network protocols supported by devices.

Table 10-1 Ring network protocols supported by devices

Ring Network Protocol	Advantage	Disadvantage
STP/RSTP/MSTP	• Applies to all Layer 2 networks. • Is a standard IEEE protocol that allows Huawei devices to communicate with non-Huawei devices.	Provides low convergence on a large network, which cannot meet the carrier-class reliability requirement.
ERPS	• Provides fast convergence and carrier-class reliability. • Is a standard ITU-T protocol that allows Huawei devices to communicate with non-Huawei devices. • Supports single-ring and multi-ring topologies in ERPSv2.	Requires the network topology to be planned in advance. The configuration is complex.

Ethernet networks demand faster protection switching. STP does not meet the requirement for fast convergence. RRPP and SEP are Huawei proprietary ring protocols, which cannot be used for communication between Huawei and non-Huawei devices on a ring network.

ERPS, a standard ITU-T protocol, prevent loops on ring networks. It optimizes detection and performs fast convergence. ERPS allows all ERPS-capable devices on a ring network to communicate.

Benefits

- Prevents broadcast storms and implements fast traffic switchover on a network where there are loops.
- Provides fast convergence and carrier-class reliability.
- Allows all ERPS-capable devices on a ring network to communicate.

10.2 Principles

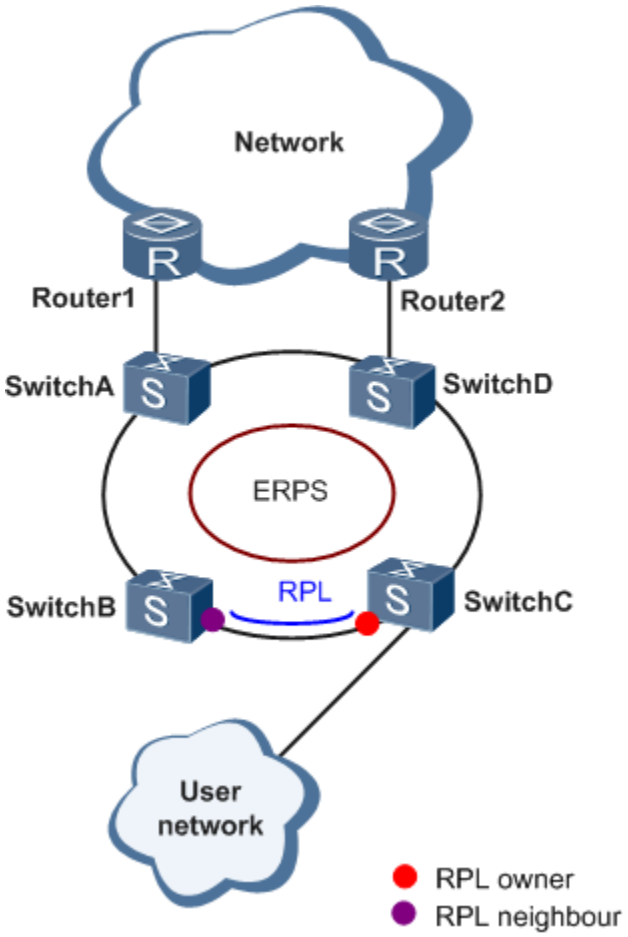
This section describes the implementation of ERPS.

10.2.1 Basic ERPS Concepts

ERPS eliminates loops at the link layer of an Ethernet network. ERPS works for ERPS rings. There are several nodes in an ERPS ring. ERPS blocks the RPL owner port and controls common ports to switch the port status between Forwarding and Discarding and eliminate loops. ERPS uses the control VLAN, data VLAN, and Ethernet Ring Protection (ERP) instance.

On the network shown in Figure 10-1, SwitchA through SwitchD constitute a ring and are dual-homed to the upstream network. This access mode will cause a loop on the entire network. To eliminate redundant links and ensure link connectivity, ERPS is used to prevent loops.

Figure 10-1 ERPS single-ring networking



ERPS can be deployed on the network shown in Figure 10-1.

ERPS Ring

An ERPS ring consists of interconnected Layer 2 switching devices configured with the same control VLAN.

Port Role

ERPS defines three port roles: RPL owner port, RPL neighbor port (only in ERPSv2), and common port.

- RPL owner port

  An RPL owner port is responsible for blocking traffic over the Ring Protection Link (RPL) to prevent loops. An ERPS ring has only one RPL owner port.

  When the node on which the RPL owner port resides receives an RAPS PDU indicating a link or node fault in an ERPS ring, the node unblocks the RPL owner port. Then the RPL owner port can send and receive traffic to ensure nonstop traffic forwarding.

  The link where the RPL owner port resides is the RPL.

- RPL neighbor port

  An RPL neighbor port is directly connected to an RPL owner port.

Both the RPL owner port and RPL neighbor ports are blocked in normal situations to prevent loops.

If an ERPS ring fails, both the RPL owner and neighbor ports are unblocked.

The RPL neighbor port helps reduce the number of FDB entry updates on the device where the RPL neighbor port resides.

- Common port

  Common ports are ring ports other than the RPL owner and neighbor ports.

  A common port monitors the status of the directly connected ERPS link and sends RAPS PDUs to notify the other ports of its link status changes.

Port Status

On an ERPS ring, an ERPS-enabled port has two statuses:

- Forwarding: forwards user traffic and sends and receives RAPS PDUs.
- Discarding: only sends and receives RAPS PDUs.

Control VLAN

A control VLAN is configured in an ERPS ring to transmit RAPS PDUs.

Each ERPS ring must be configured with a control VLAN. After a port is added to an ERPS ring configured with a control VLAN, the port is added to the control VLAN automatically.

Different ERPS rings must use different control VLANs.

Data VLAN

Unlike control VLANs, data VLANs are used to transmit data packets.

ERP Instance

On a Layer 2 device running ERPS, the VLAN in which RAPS PDUs and data packets are transmitted must be mapped to an Ethernet Ring Protection (ERP) instance so that ERPS forwards or blocks the packets based on configured rules. If the mapping is not configured, the preceding packets may cause broadcast storms on the ring network. As a result, the network becomes unavailable.

Timer

ERPS defines four timers: Guard timer, WTR timer, Holdoff timer, and WTB timer (only in ERPSv2).

- Guard timer

  After a faulty link or node recovers or a clear operation is executed, the device sends RAPS No Request (NR) messages to inform the other nodes of the link or node recovery and starts the Guard timer. Before the Guard timer expires, the device does not process any RAPS (NR) messages

to avoid receiving out-of-date RAPS (NR) messages. After the Guard timer expires, if the device still receives an RAPS (NR) message, the local port enters the Forwarding state.

- WTR timer

  If an RPL owner port is unblocked due to a link or node fault, the involved port may not go Up immediately after the link or node recovers. Blocking the RPL owner port may cause network flapping. To prevent this problem, the node where the RPL owner port resides starts the wait to restore (WTR) timer after receiving an RAPS (NR) message. If the node receives an RAPS Signal Fail (SF) message before the timer expires, it terminates the WTR timer. If the node does not receive any RAPS (SF) message before the timer expires, it blocks the RPL owner port when the timer expires and sends an RAPS (no request, root blocked) message. After receiving this RAPS (NR, RB) message, the nodes set their recovered ports on the ring to the Forwarding state.

- Holdoff timer

  On Layer 2 networks running EPRS, there may be different requirements for protection switching. For example, on a network where multi-layer services are provided, after a server fails, users may require a period of time to rectify the server fault so that clients do not detect the fault. You can set the Holdoff timer. If the fault occurs, the fault is not immediately sent to ERPS until the Holdoff timer expires.

10.3 Configuration Examples

This section provides configuration examples of ERPS, including the networking requirements, configuration roadmap, configuration procedure, and configuration files.

10.3.1 Example for Configuring ERPS Multi-instance

This section provides an example illustrating ERPS multi-instance configuration.

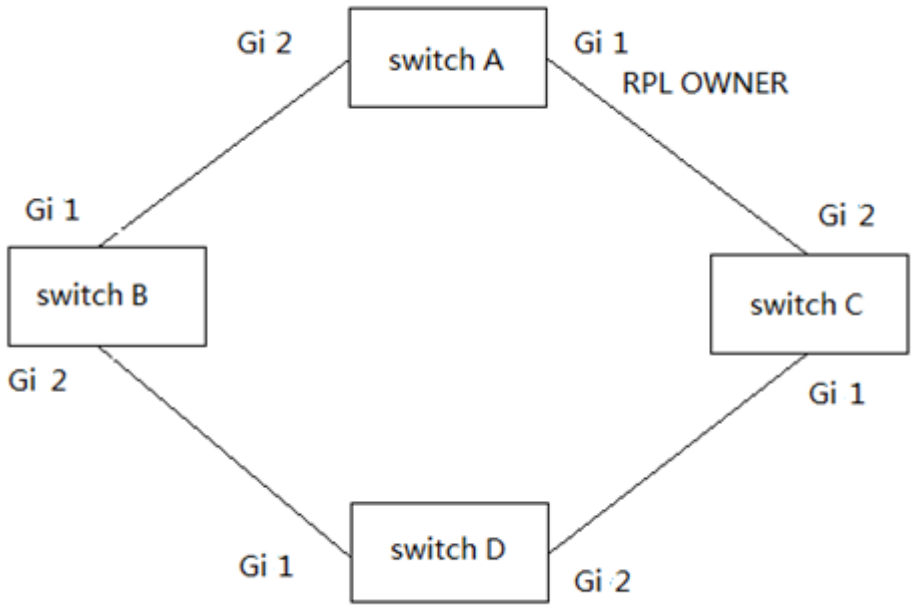
Networking Requirements

Generally, redundant links are used on an Ethernet switching network to provide link backup and enhance network reliability. The use of redundant links, however, may produce loops, causing broadcast storms and rendering the MAC address table unstable. As a result, communication quality deteriorates, and communication services may even be interrupted.

To prevent loops caused by redundant links, enable ERPS on the nodes of the ring network. ERPS is a Layer 2 loop-breaking protocol defined by the ITU-T, and provides fast convergence of carrier-class reliability standards.

Figure 10-3 shows a network on which a multi-instance ERPS ring is used. SwitchA through SwitchD constitute a ring network at the aggregation layer to implement service aggregation at Layer 2 and process Layer 3 services. ERPS is used on the ring network to provide protection switching for Layer 2 redundant links. ERPS ring 1 and ERPS ring 2 are configured on SwitchA through SwitchD. P1 on SwitchB is

a blocked port in ERPS ring 1, and P2 on SwitchA is a blocked port in ERPS ring 2, implementing load balancing and link backup.



Configuration Roadmap

The configuration roadmap is as follows:

1. Configure the link type of all ports to be added to ERPS rings as trunk.
2. Create ERPS rings and configure control VLANs and Ethernet Ring Protection (ERP) instances in the ERPS rings.
3. Add Layer 2 ports to ERPS rings and specify port roles.
4. Configure the Guard timers and WTR timers in the ERPS rings.
5. Configure Layer 2 forwarding on SwitchA through SwitchD.

Adding a Layer 2 Port to an ERPS Ring and Configuring the Port Role

Context

After ERPS is configured, add Layer 2 ports to an ERPS ring and configure port roles so that ERPS can work properly.

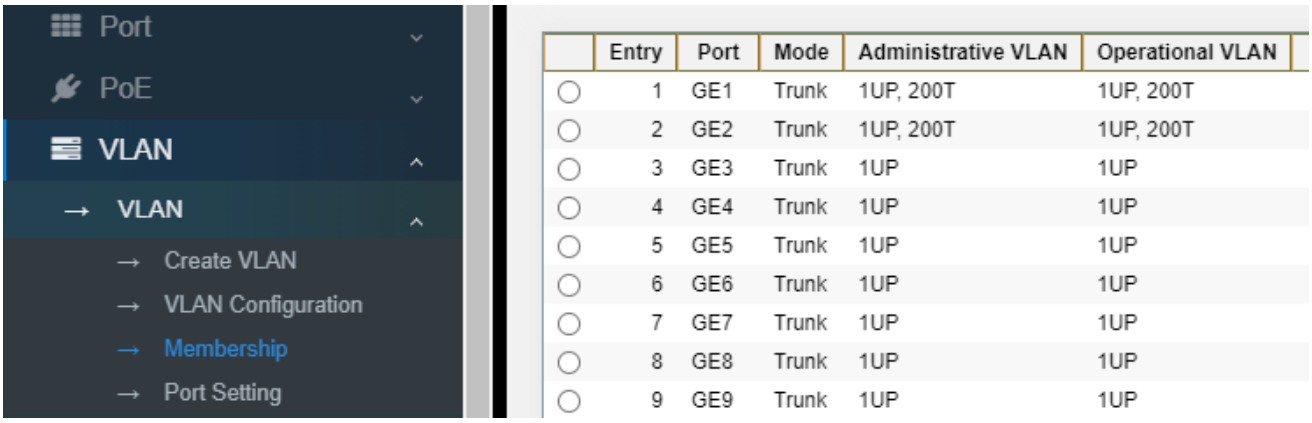
You can add a Layer 2 port to an ERPS ring in either of the following ways:

- In the ERPS ring view, add a specified port to the ERPS ring and configure the port role.
- In the interface view, add the current port to the ERPS ring and configure the port role.

Configure ERPS according to the single loop example diagram of 10-2

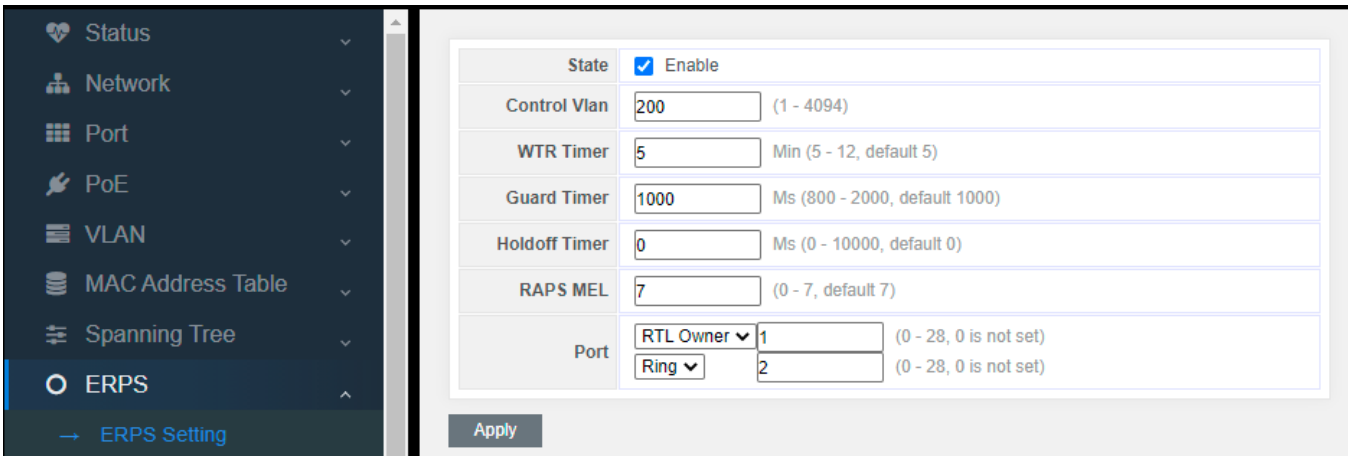
The webpage configuration is as follows:

Configure port1 and port 2, both of which are vlan200 tags

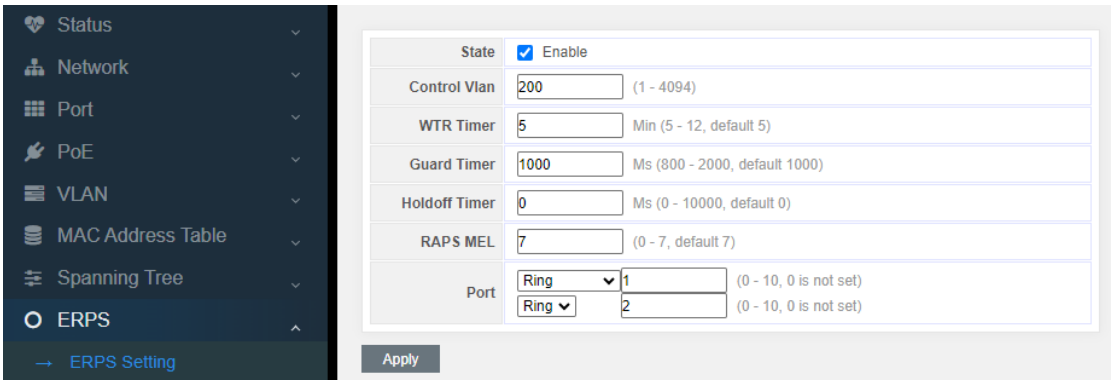


Configure SwitchA to enable ERP, then configure the vlan id of the control vlan to 200, and then configure port 1 to RTL Owner mode and port 2 to ring mode.

Click Apply button, and SwichA configuration is complete.



If you need to configure SwitchB~D, everything else is the same, just configure the port mode to ring.



Part 11: Routing

11.1 IP Routing and Routing Table

11.1.1 Routing

Routing in the Internet is achieved through routers. Upon receiving a packet, a router finds an optimal route based on the destination address and forwards the packet to the next router in the path until the packet reaches the last router, which forwards the packet to the intended destination host.

11.1.2 Routing Through a Routing Table

I. Routing table

Routing tables play a key role in routing. Each router maintains a routing table, and each entry in the table specifies which physical interface a packet destined for a certain destination should go out to reach the next hop (the next router) or the directly connected destination.

Routes in a routing table can be divided into three categories by origin:

- Direct routes: Routes discovered by data link protocols, also known as interface routes.
- Static routes: Routes that are manually configured.
- Dynamic routes: Routes that are discovered dynamically by routing protocols.

II. Contents of a routing table

A routing table includes the following key items:

- Destination address: Destination IP address or destination network.
- Network mask: Specifies, in company with the destination address, the address of the destination network. A logical AND operation between the destination address and the network mask yields the address of the destination network. For example, if the destination address is 129.102.8.10 and the mask 255.255.0.0, the address of the destination network is 129.102.0.0. A network mask is made of a certain number of consecutive 1s. It can be expressed in dotted decimal format or by the number of the 1s.
- Outbound interface: Specifies the interface through which the IP packets are to be forwarded.
- IP address of the next hop: Specifies the address of the next router on the path. If only the outbound interface is configured, its address will be the IP address of the next hop.
- Priority for the route. Routes to the same destination but having different nexthops may have different priorities and be found by various routing protocols or manually configured. The optimal route is the one with the highest priority (with the smallest metric).

Routes can be divided into two categories by destination:

- Subnet routes: The destination is a subnet.
- Host routes: The destination is a host.

Based on whether the destination is directly connected to a given router, routes can be divided into:

- Direct routes: The destination is directly connected to the router.
- Indirect routes: The destination is not directly connected to the router.

To prevent the routing table from getting too large, you can configure a default route. All packets without matching entry in the routing table will be forwarded through the default route.

11.2 Routing Protocol Overview

11.2.1 Static Routing and Dynamic Routing

Static routing is easy to configure and requires less system resources. It works well in small, stable networks with simple topologies. Its major drawback is that you must perform routing configuration again whenever the network topology changes; it cannot adjust to network changes by itself.

Dynamic routing is based on dynamic routing protocols, which can detect network topology changes and recalculate the routes accordingly. Therefore, dynamic routing is suitable for large networks. Its disadvantages are that it is complicated to configure, and that it not only imposes higher requirements on the system, but also eats away a certain amount of network resources.

11.2.2 Classification of Dynamic Routing Protocols

Dynamic routing protocols can be classified based on the following standards:

I. Operational scope

- Interior gateway protocols (IGPs): Work within an autonomous system, including RIP, OSPF, and IS-IS.
- Exterior gateway protocols (EGPs): Work between autonomous systems. The most popular one is BGP.

II. Routing algorithm

- Distance-vector protocols: RIP and BGP. BGP is also considered a path-vector protocol.
- Link-state protocols: OSPF and IS-IS. The main differences between the above two types of routing algorithms lie in the way routes are discovered and calculated.

III.. Version of IP protocol

IPv4 routing protocols: RIP, OSPFv2, BGP4 and IS-IS.
IPv6 routing protocols: RIPng, OSPFv3, IPv6 BGP, and IPv6 IS-IS.

11.3 Static Routing Configuration

11.3.1 Introduction

11.3.1.1 Static Route

A static route is a special route that is manually configured by the network administrator. If a network's topology is simple, you only need to configure static routes for the network to work normally. The proper configuration and usage of static routes can improve network performance and ensure bandwidth for important network applications.

The disadvantage of using static routes is that they cannot adapt to network topology changes. If a fault or a topological change occurs in the network, the routes will be unreachable and the network breaks. In this case, the network administrator has to modify the static routes manually.

11.3.1.2 Default Route

A router selects the default route only when it cannot find any matching entry in the routing table.

If the destination address of a packet fails to match any entry in the routing table, the router selects the default route to forward the packet.

If there is no default route and the destination address of the packet fails to match any entry in the routing table, the packet will be discarded and an ICMP packet will be sent to the source to report that the destination or the network is unreachable.

You can create the default route with both destination and mask being 0.0.0.0, and some dynamic routing protocols, such as OSPF, RIP and IS-IS, can also generate the default route.

11.3.1.3 Application Environment of Static Routing

Before configuring a static route, you need to know the following concepts:

1) Destination address and mask
In the **ip route** command, an IPv4 address is in dotted decimal format and a mask can be either in dotted decimal format or in the form of mask length (the digits of consecutive 1s in the mask).

2) Output interface and next hop address
While configuring a static route, you can specify either the output interface or the next hop address depending on the specific occasion. The next hop address can not be a local interface IP address; otherwise, the route configuration will not take effect.

In fact, all the route entries must have a next hop address. When forwarding a packet, a router first searches the routing table for the route to the destination address of the packet. The system can find the corresponding link layer address and forward the packet only after the next hop address is specified.

When specifying the output interface, note that:

- If the output interface is a NULL 0 or loopback interface, there is no need to configure the next hop address.

- You are not recommended to specify a broadcast interface (such as a VLAN interface) as the output interface, because a broadcast interface may have multiple next hops. If you have to do so, you must specify the corresponding next hop for the output interface.

3) Other attributes

You can configure different preferences for different static routes so that route management policies can be applied more flexibly. For example, specifying the same preference for different routes to the same destination enables load sharing, while specifying different preferences for these routes enables route backup.

You can also enable bidirectional forwarding detection (BFD) to implement fast detection on the next hops of static routes. When a next hop is unreachable, the system can switch to a backup route instantly.

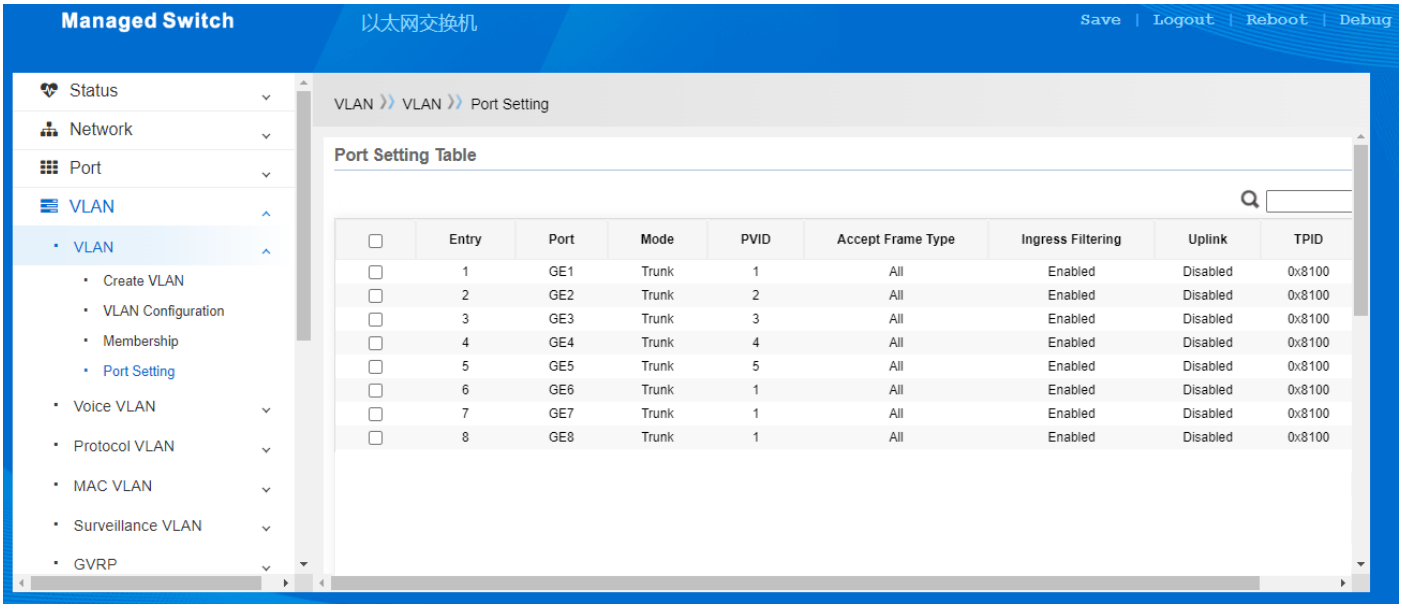
11.3.2 Configuring a Static Route

11.3.2.1 Configuration Prerequisites

Before configuring a static route, you need to configure the IP addresses for related interfaces

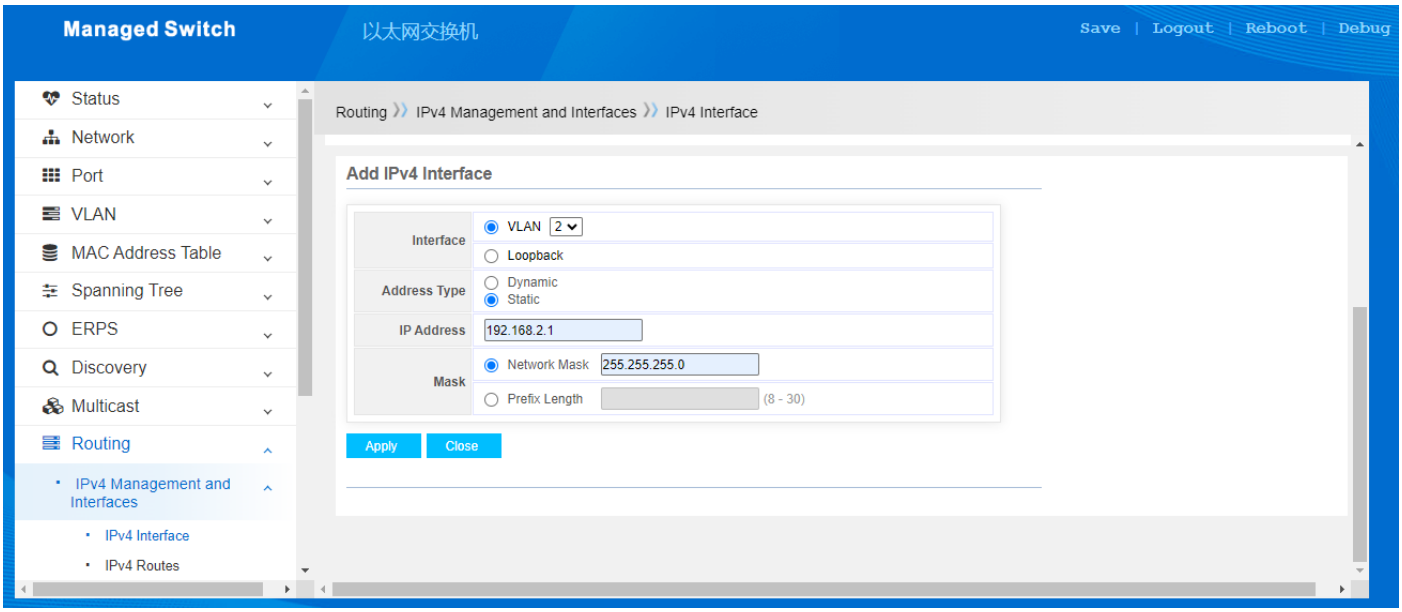
- Configure the physical parameters of relevant interfaces
- Configure the IP address of the relevant interface

Configure ports 2-5 with PVIDs of 2-5

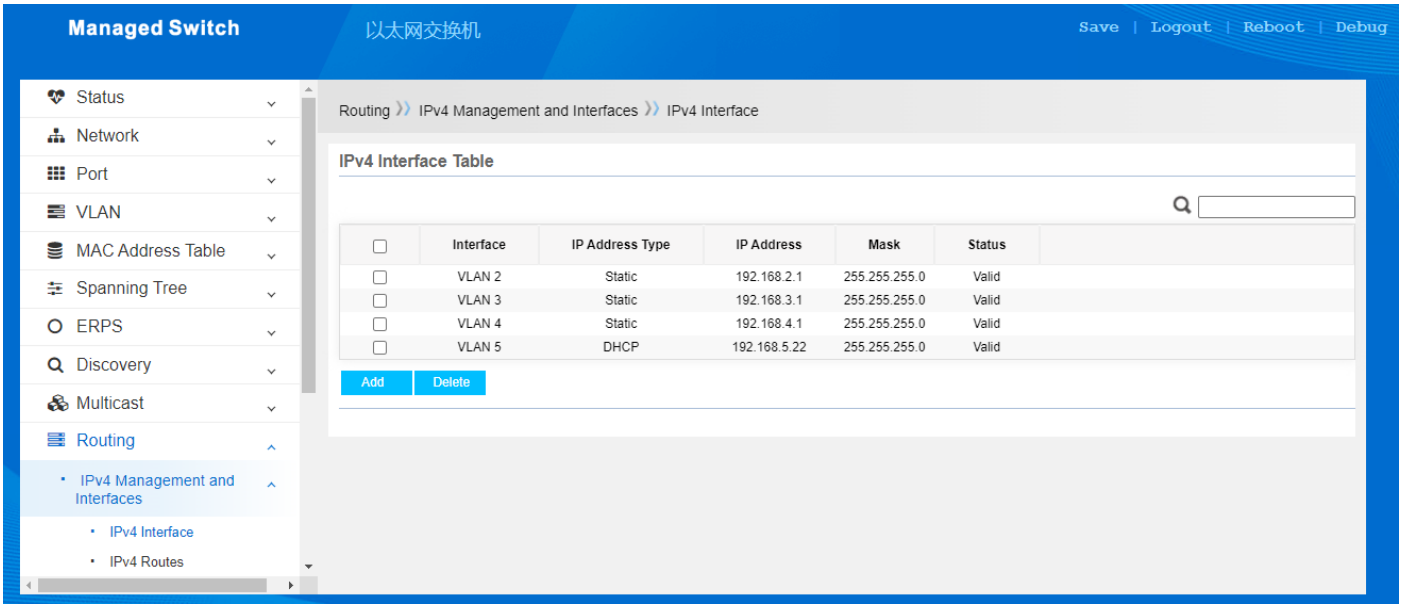


Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
1	GE1	Trunk	1	All	Enabled	Disabled	0x8100
2	GE2	Trunk	2	All	Enabled	Disabled	0x8100
3	GE3	Trunk	3	All	Enabled	Disabled	0x8100
4	GE4	Trunk	4	All	Enabled	Disabled	0x8100
5	GE5	Trunk	5	All	Enabled	Disabled	0x8100
6	GE6	Trunk	1	All	Enabled	Disabled	0x8100
7	GE7	Trunk	1	All	Enabled	Disabled	0x8100
8	GE8	Trunk	1	All	Enabled	Disabled	0x8100

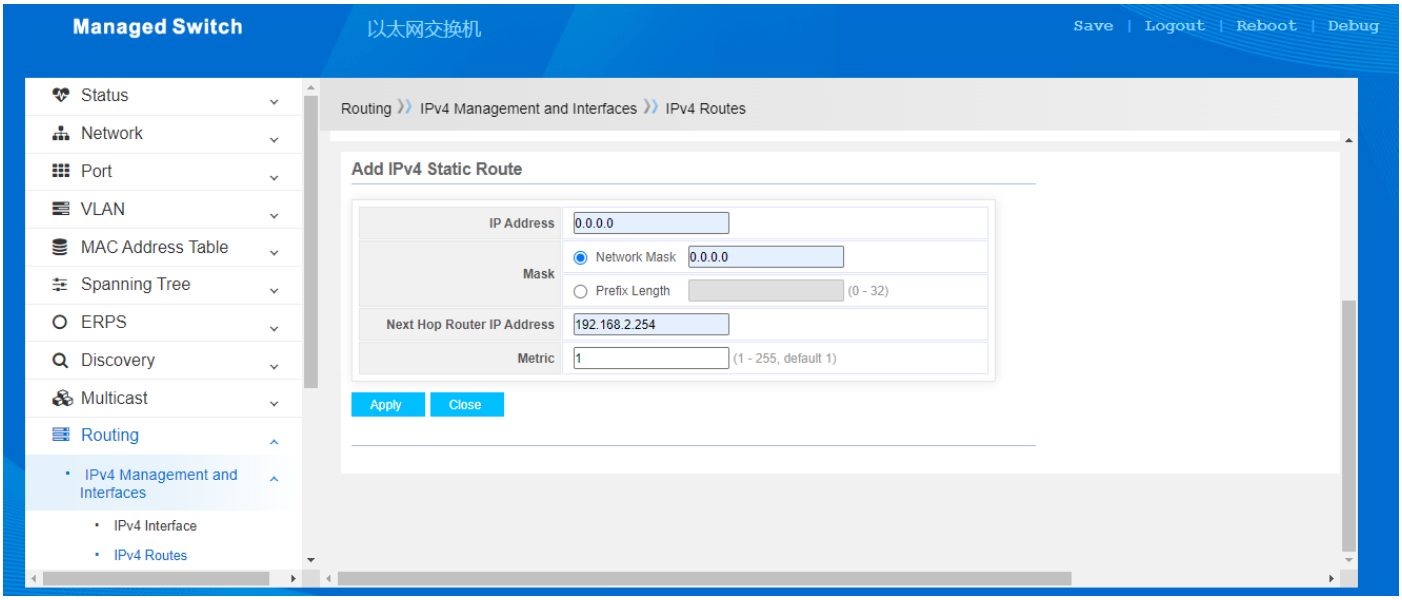
Configure the IP address of the interface. The IP address of VLAN2 is 192.168.2.1



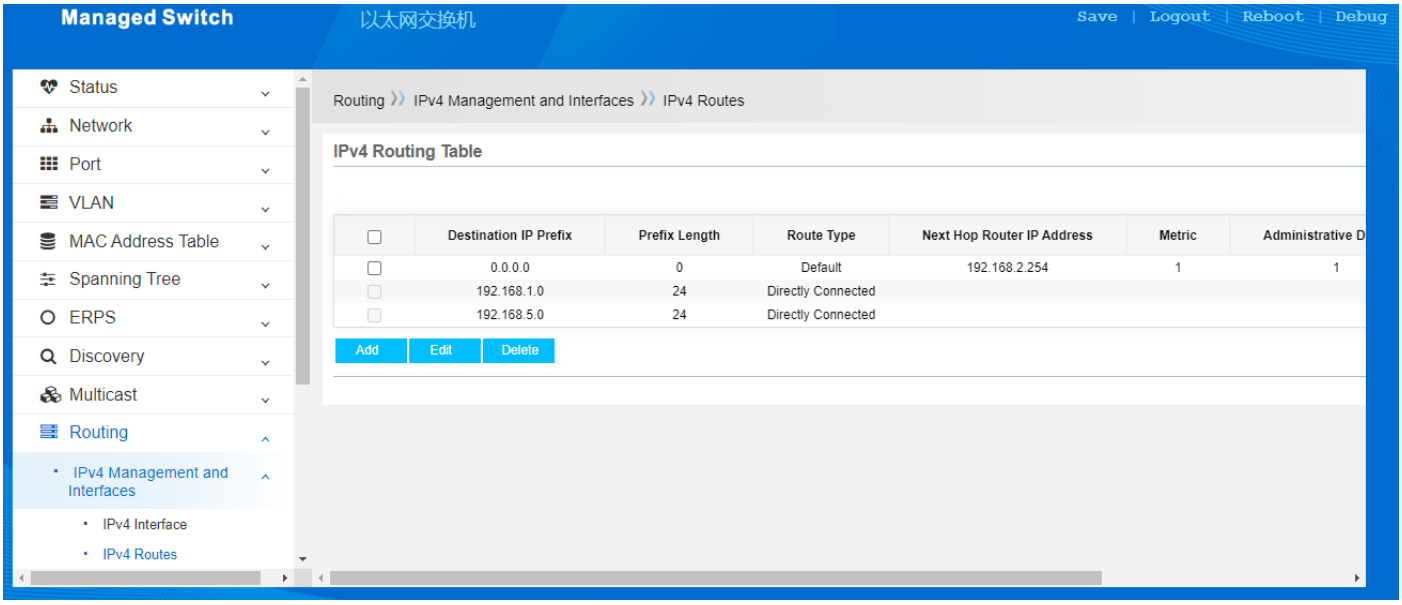
Configure IP addresses for other interfaces



11.3.2.2 Configuring Static Routes



The configuration results are shown in the following figure:



Part 12: Security

12.4 Management Access

12.4.1 Management VLAN

VLAN management means that only the VLAN on the port can communicate with the CPU of switch and manage the switch system.

By default, the member ports of VLAN1 member ports can manage switches.`

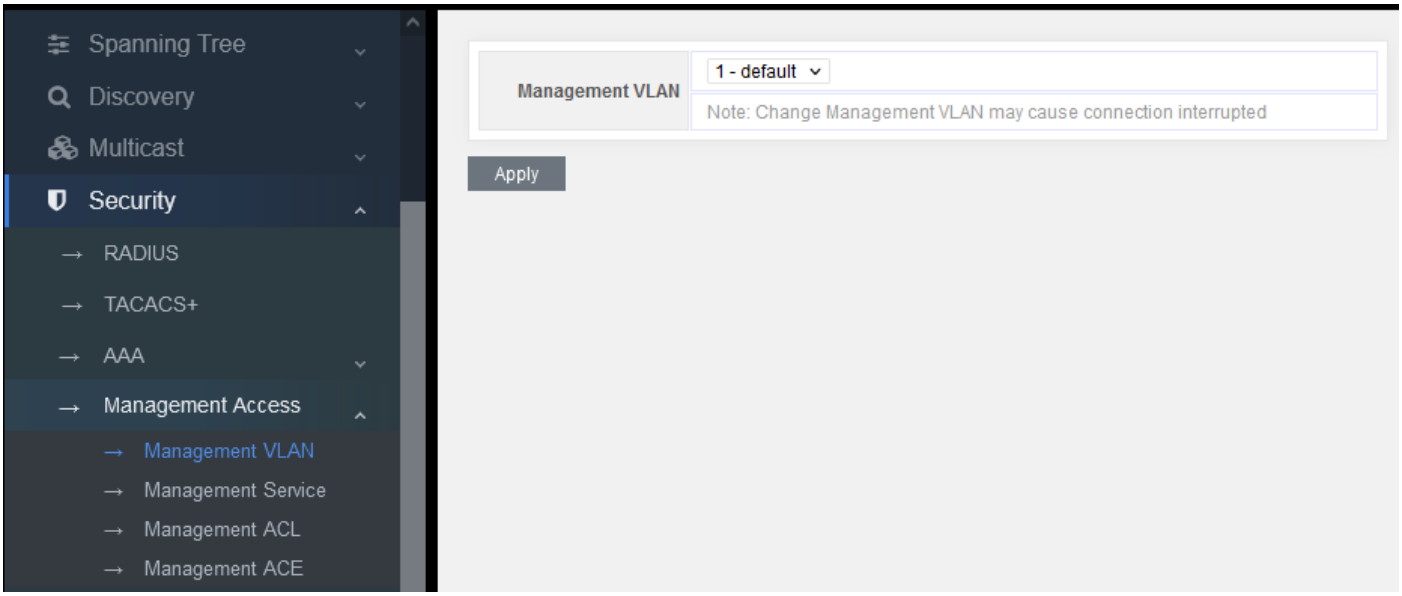


Figure 12-4-1

According to the user's demands, you can choose any VLAN to manage the switch system. But the premise is that the selected VLAN should be established first.

For example:

1. Add VLAN, such as vlan100
2. Add port 5 to VLAN 100
3. Set VLAN100 as the managing VLAN
4. Connect PC with port 5 to manage the switch.

12.4.2 Management Service

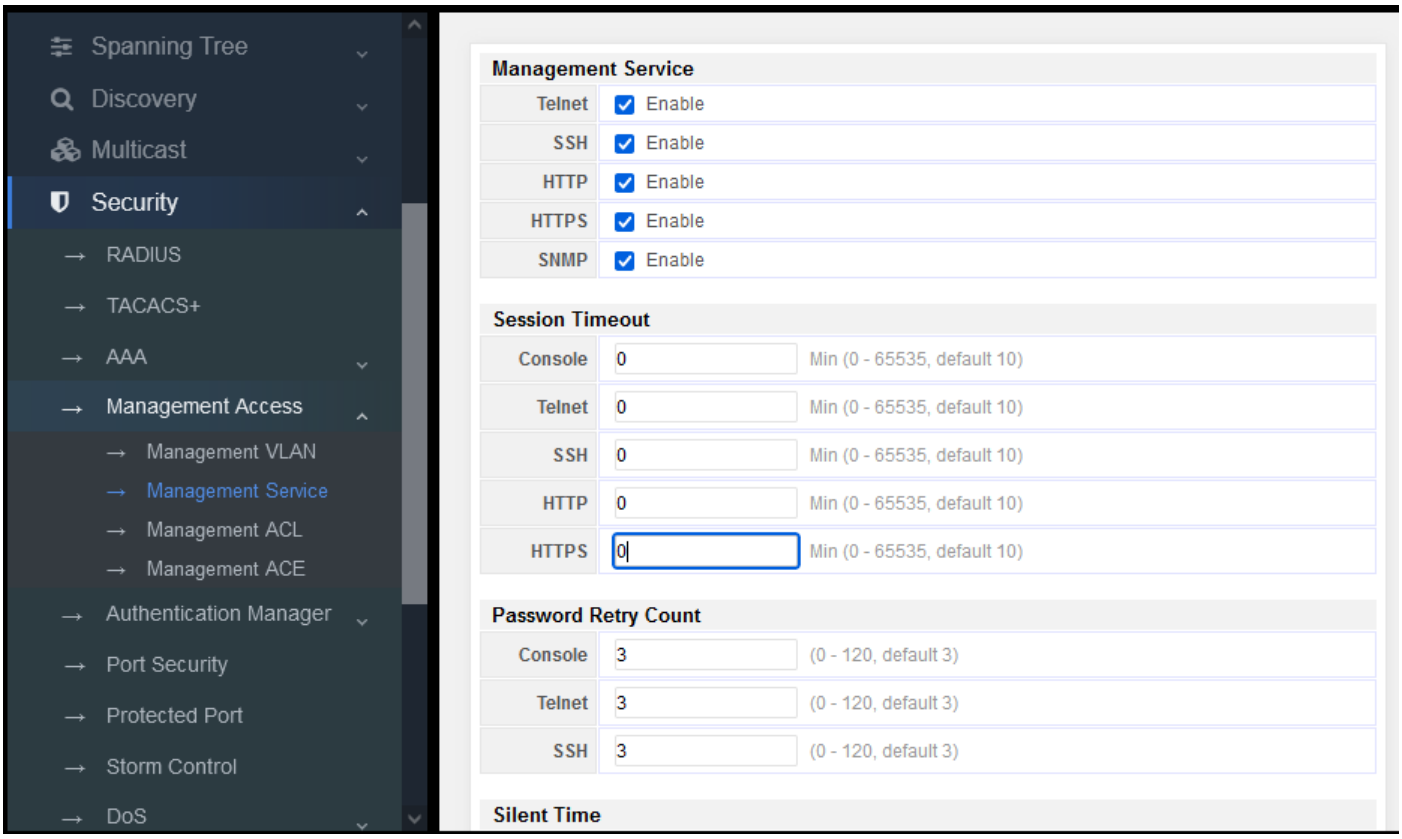


Figure 12-4-2

Management service: according to the users demands, you can select switches to support.
Session Timeout: for example, after logging in the web page, if no operation for 10 seconds, the system will automatically exit the web page. The user should re-enter his name and password to manage the switch.
Password Retry Count: if the times of inputting wrong password exceeds the set value, the user will wait for some time and re-enter the password to prevent brute force.

Part 15: Diagnostics

15.1 Logging

15.1.1 Property

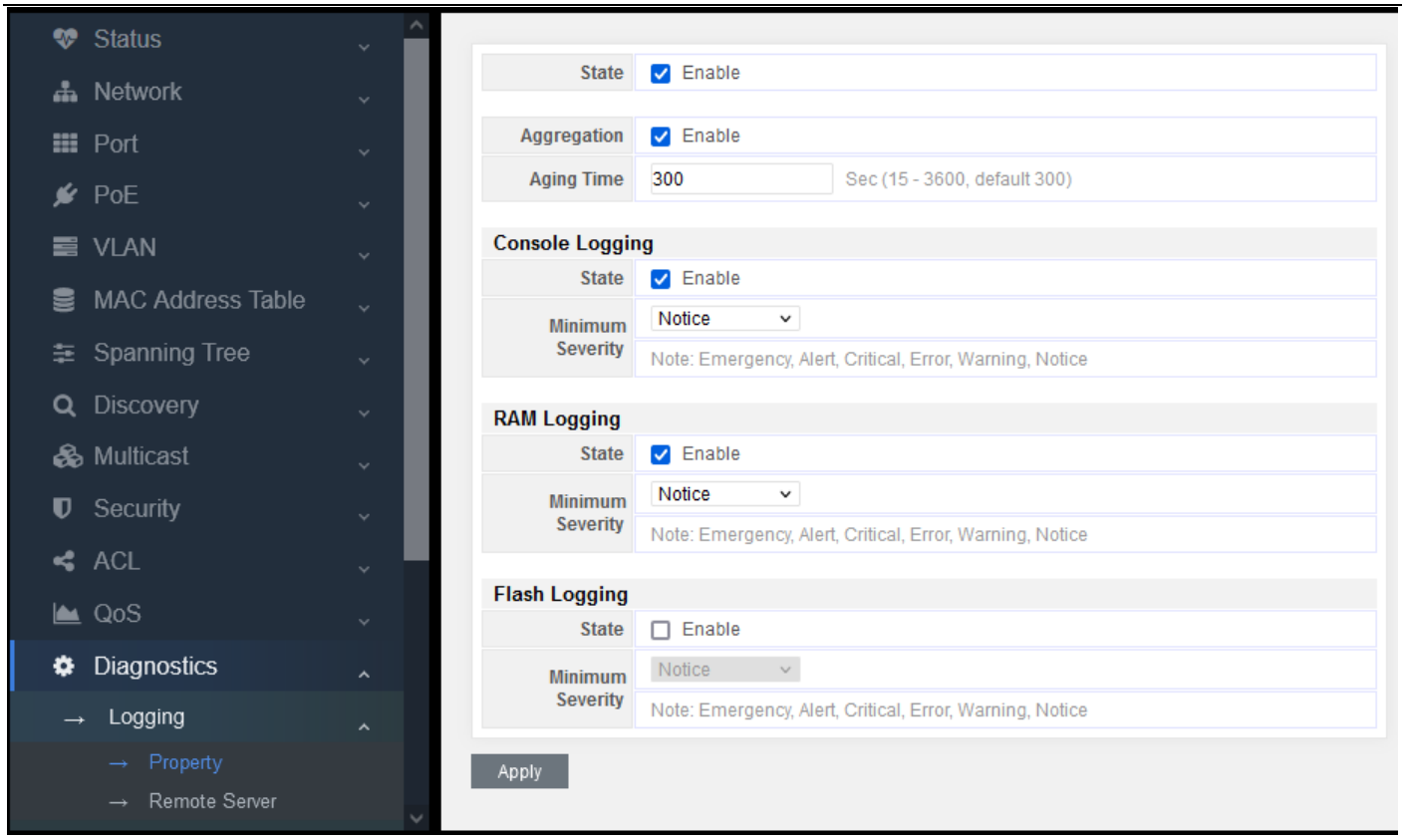


Figure 15-1-1

State: logging information, on/off
Aggregation: merge or display the entries of log information, on/off
Aging time: time of upgrading the log information. The default time is 300 seconds.

Console logging: display the log information on the serial port
RAM logging: display the log information on RAM
Flash logging: display the log information on Flash
Minimum severity: log level, including 8 types: emergency, alert, critical, error, warning, notice, informational, debug

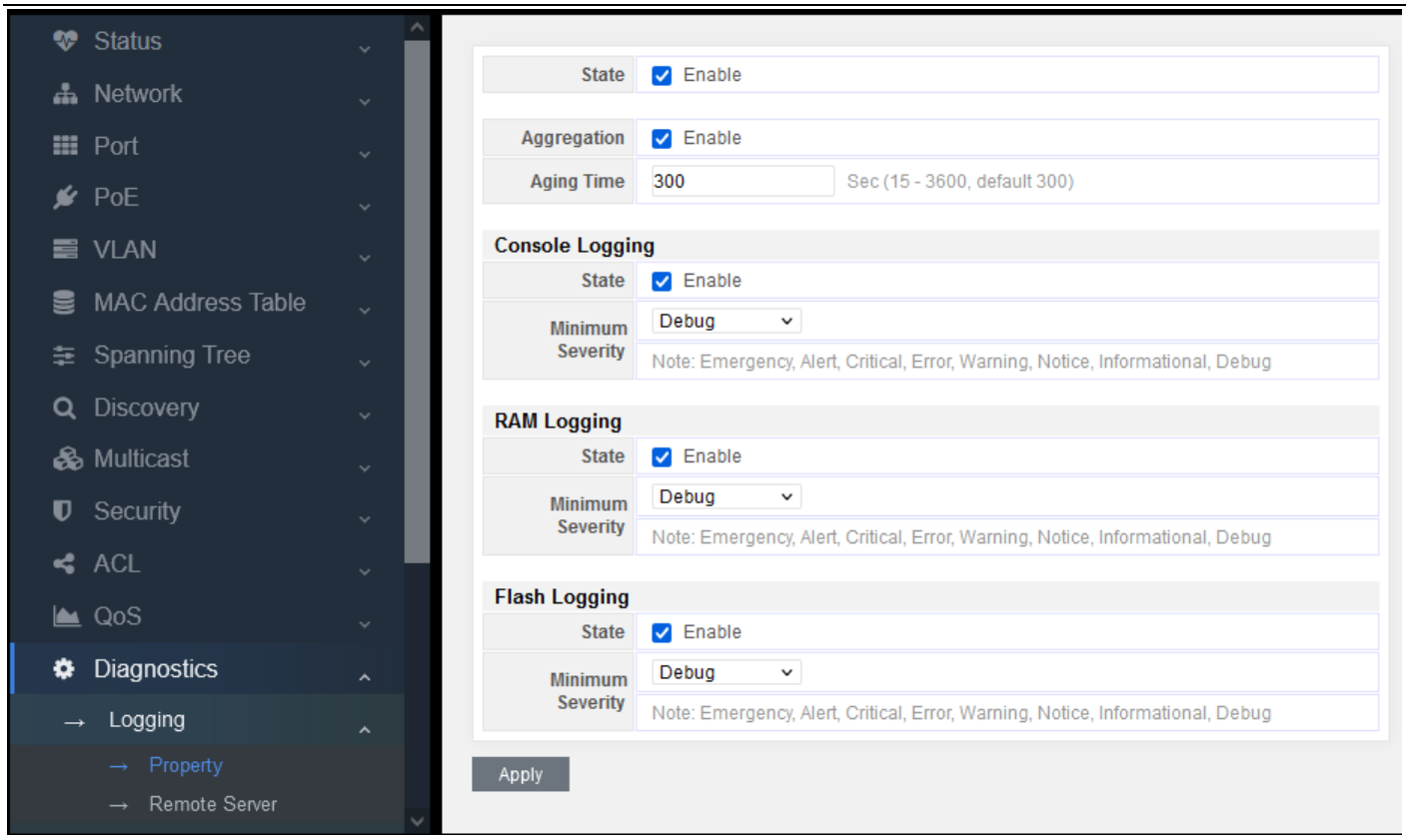


Figure 15-1-2

The above configuration can cover the display of logs completely, which can be taken as reference.

15.2 Mirroring

Support 4 mirroring sessions.

Setting of traffic capturing:

Capturing status: set the status of port mirroring, on/off

Capturing port: select a capturing port, that is, mirror the captured port message to this port

Captured port: capture ingress messages, egress messages or all of them.

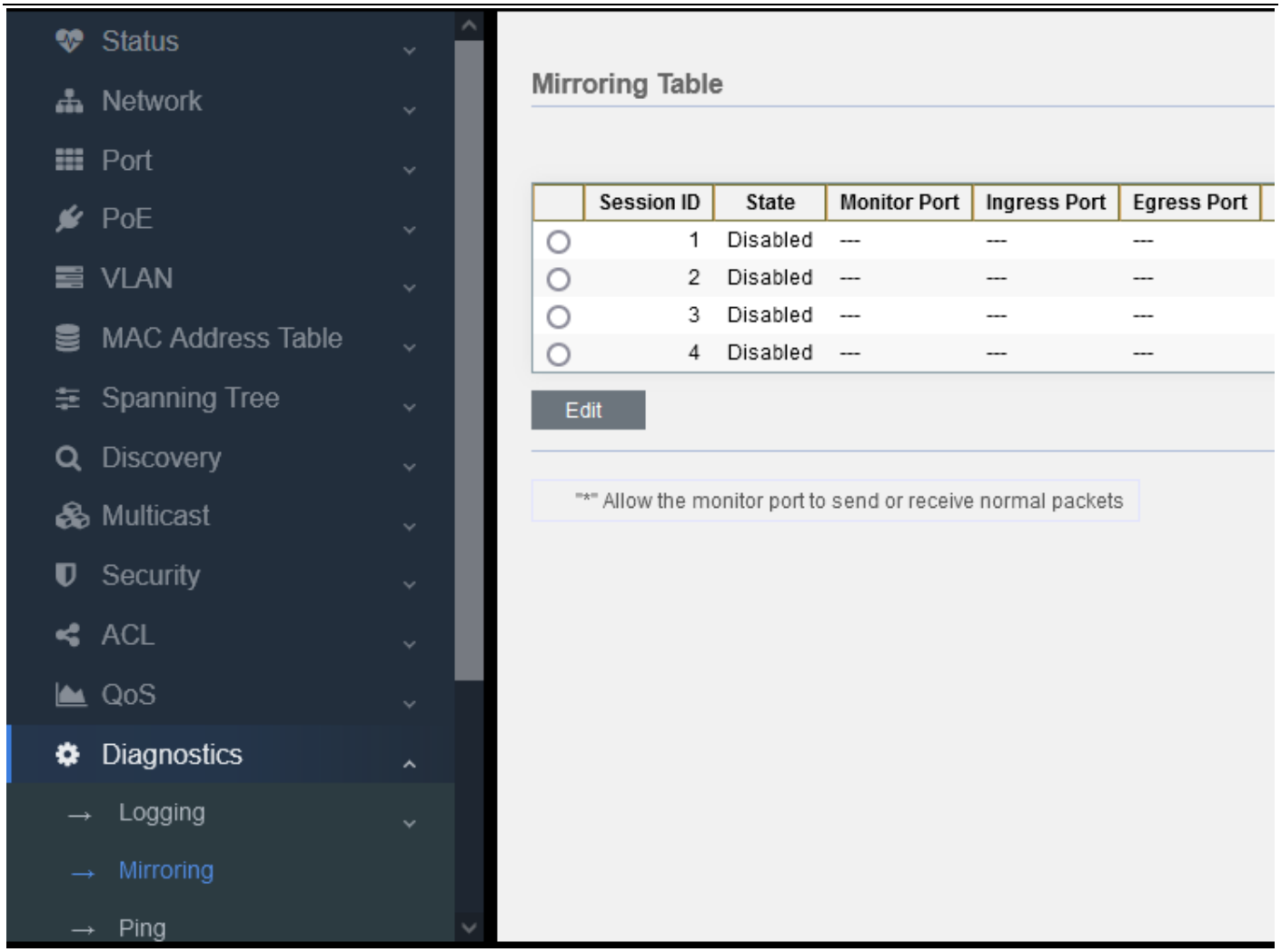


Figure 15-2-1

Select a mirroring session and click “Edit”

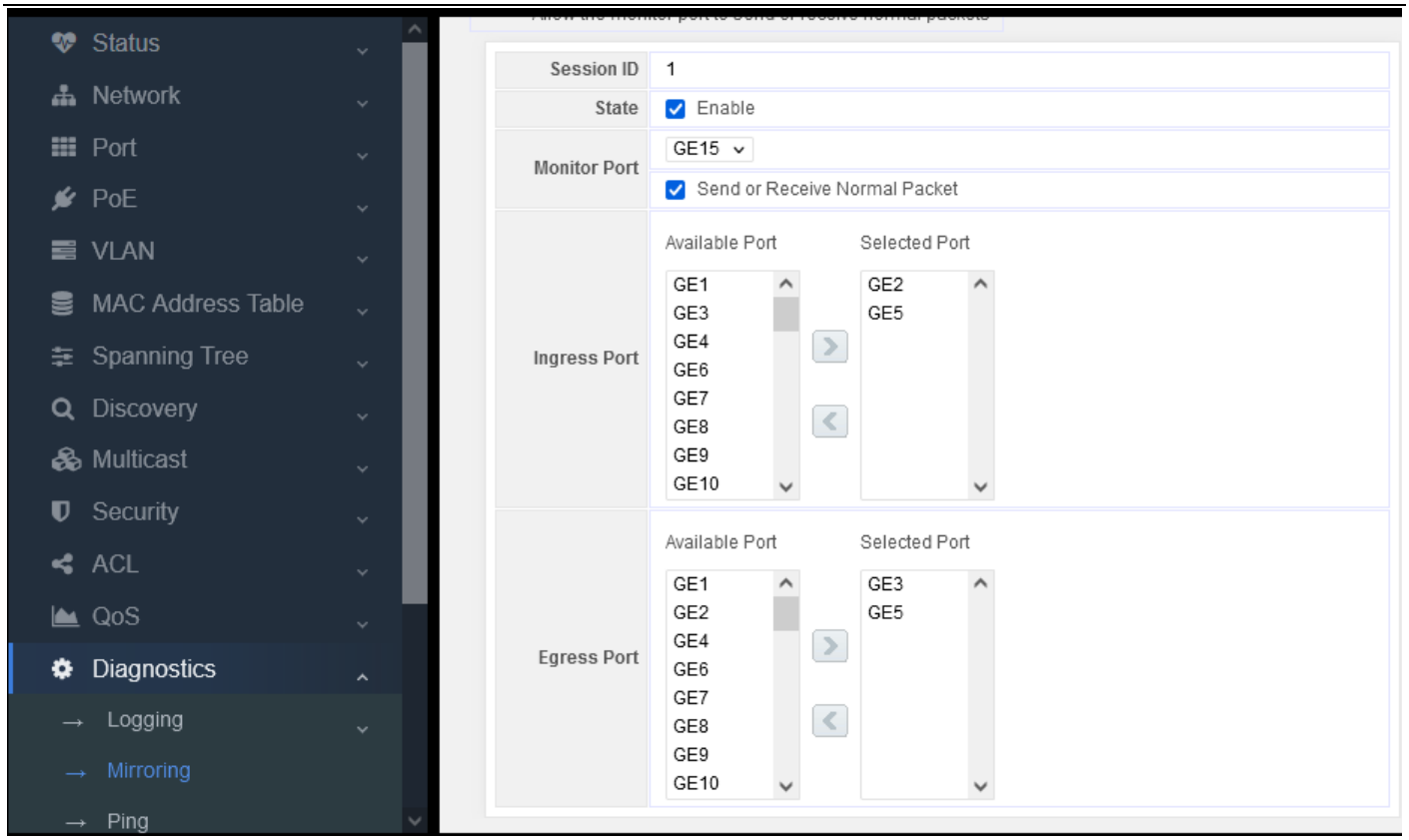


Figure 15-2-2

State: tick Enable
Monitor port: select some ports messages to mirror on this port.

Note: tick "Send or Receive Normal Packet" to control the switch by the PC connected with this port after configuration. If not, this port cannot be accessed to control the switch.

Ingress port: messages sending in this port
Progress port: messages sending out of this port

As shown in the above example:
Mirror the ingress message of GE2 port to GE15 port
Mirror the egress message of GE3 port to GE15 port
Mirror the igress and egress messages of GE5 port to GE15 port

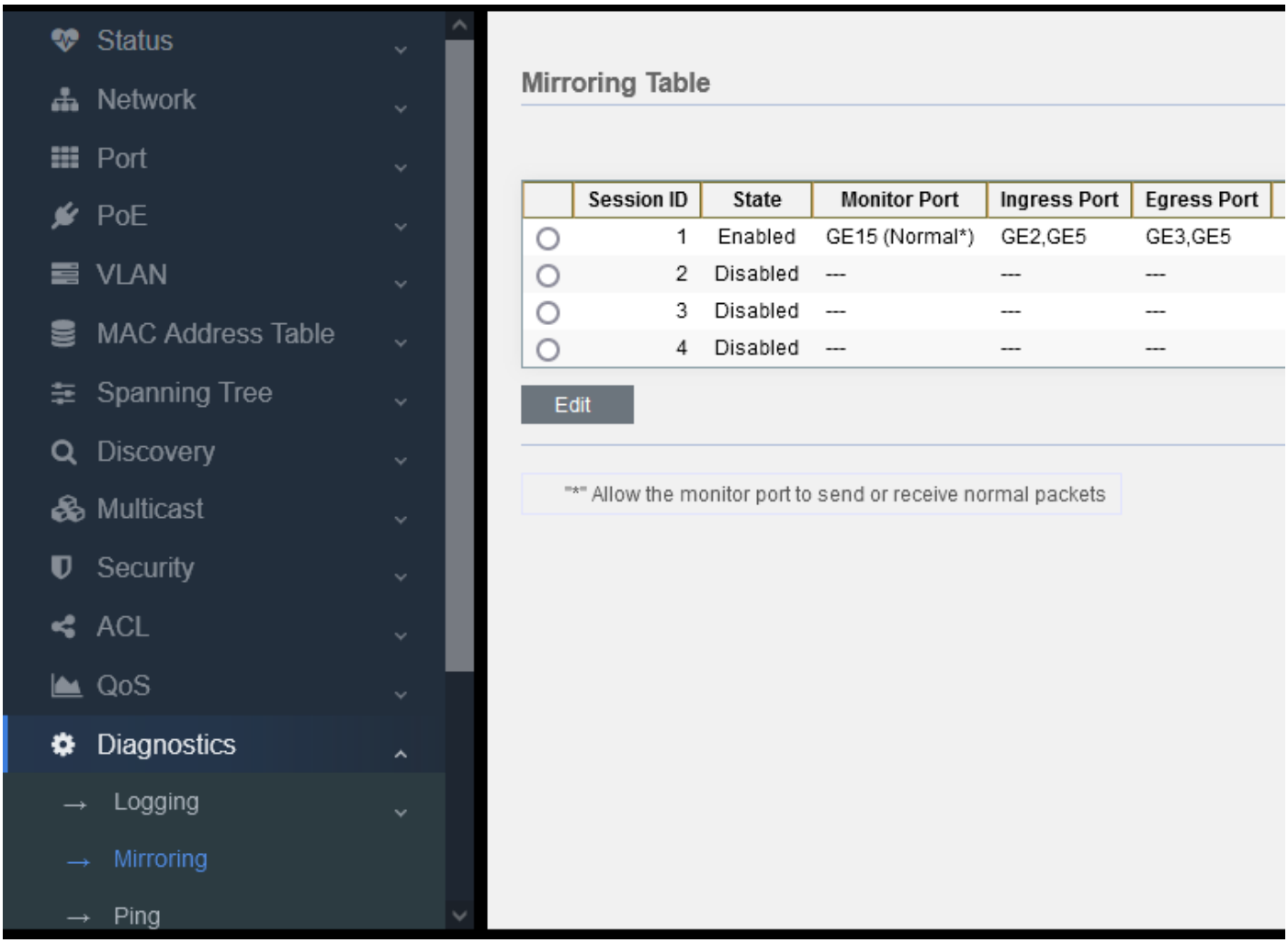


Figure 15-2-3

Check the details of the mirror configuration.

15.3 Ping

。

PING (packet Internet groper) is used to test network connection. Ping is a service command running in the application layer of TCP/IP network architecture mainly to send ICMP ECHO request message to a specific destination host so as to test whether this destination host is reachable and understand its relevant status.

PING is used to ensure whether the local host can exchange (send and receive) packets with another host successfully, so according to the returned information, we can infer whether the TCP/IP parameters are set correctly, the operation is normal, and the network is unobstructed.

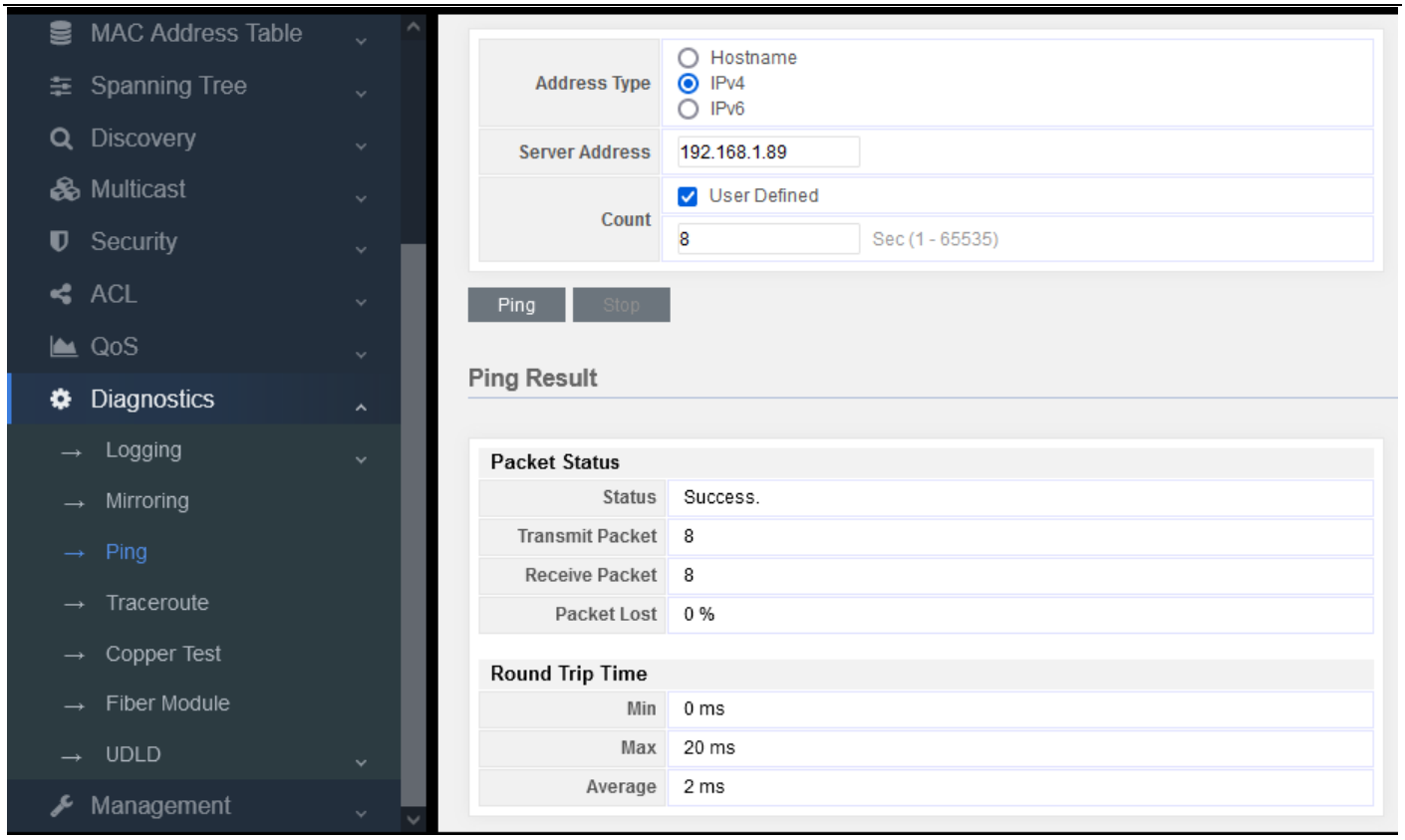


Figure 15-3-1

Address Type: Hostname，IPv4，IPv6
Service address: this requires to input the destination address for PING.
Count: the number of messages for PING continuously. The default is 4. You can also manually input the number of messages for PING.

Ping Result
Status: pass or failure
Transmit packet: how many ping messages have been sent
Receive packet: how many ping messages have been received
Packet lost: compare the data of sent and received messages to count the percentage of messages lost.

15.4 Traceroute

Traceroute command adopts ICMP Protocol to locate all routers between terminal device and target terminal device. The TTL value can reflect the number of routers or gateways passed by the data packet. By controlling the independent ICMP to call the TTL value of messages and observe the discarded return information of this message, the traceroute command can traverse all routers on the packet transmission path.

This program will increase TTL value to realize its functions. The program realizes its function by increasing the TTL value. Every time a packet passes through a router, its lifetime is reduced by 1. When its lifetime is 0, the host will cancel the packet and send an ICMP TTL packet to the sender of the original packet.
The TTL values of the first three packets sent by the program are 1, the next three are 2, and so on, then the program will get a series of packet paths. Note that IP does not guarantee to provide a same path for each packet.

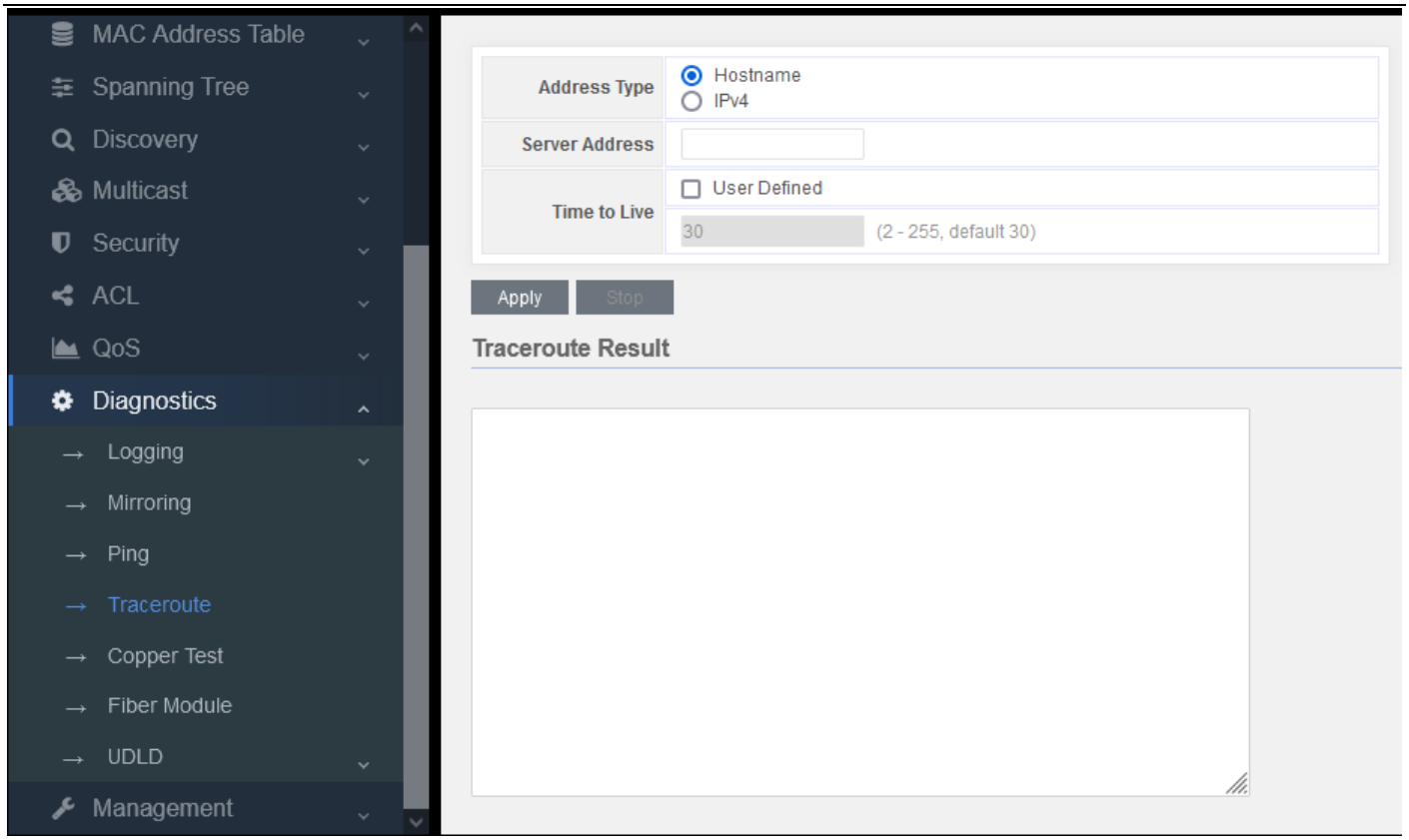


Figure 15-4-1

15.5 Copper Test

This is the function of VCT. VCT is the abbreviation of Virtual Cable Test which is a common function in network communication equipment.

VCT uses TDR (Time Domain Reflectometry) to detect the physical state of network cables.

TDR detection principle is similar to radar. Its working mode is to send a pulse signal through an active guide line and detect the reflection result of the transmitted pulse signal to detect the cable fault. When the transmitted pulse signal passes through the cable end or the fault point of the cable, it will cause part or all of the pulse energy to be reflected back to the original transmission source. VCT technology obtains the time of the signal arriving at the fault point or returning according to its transmission status in the wire, and then converts the corresponding time into the distance value according to the formula. VCT can detect cable status, fault distance, polarity exchange, insertion signal attenuation, return signal attenuation, etc.

The user can use VCT characteristics to detect Ethernet connection cable, and turn on the system to detect Ethernet cable. The detection includes short circuit and open circuit in the receiving and sending direction of the cable, as well as the faulty position on the cable.

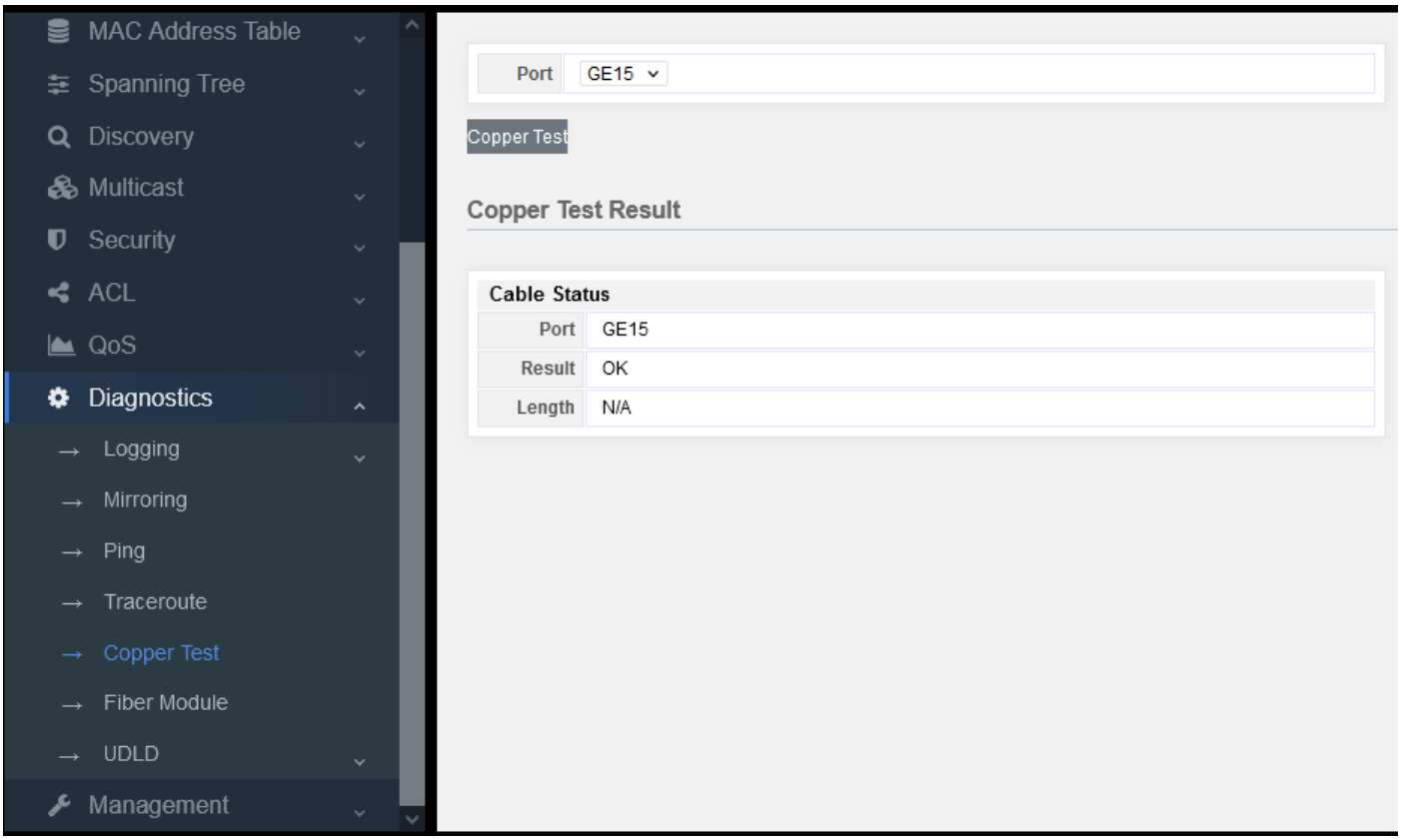


Figure 15-5-1

Select a port and click “copper test” button.

When the network cable is disconnected, there will be a test result showing Length, which indicates how many meters it is disconnected from. Its error is about 1 meter, so this function can be used to check the network cable fault.

Part 16: Management

16.1 User Account

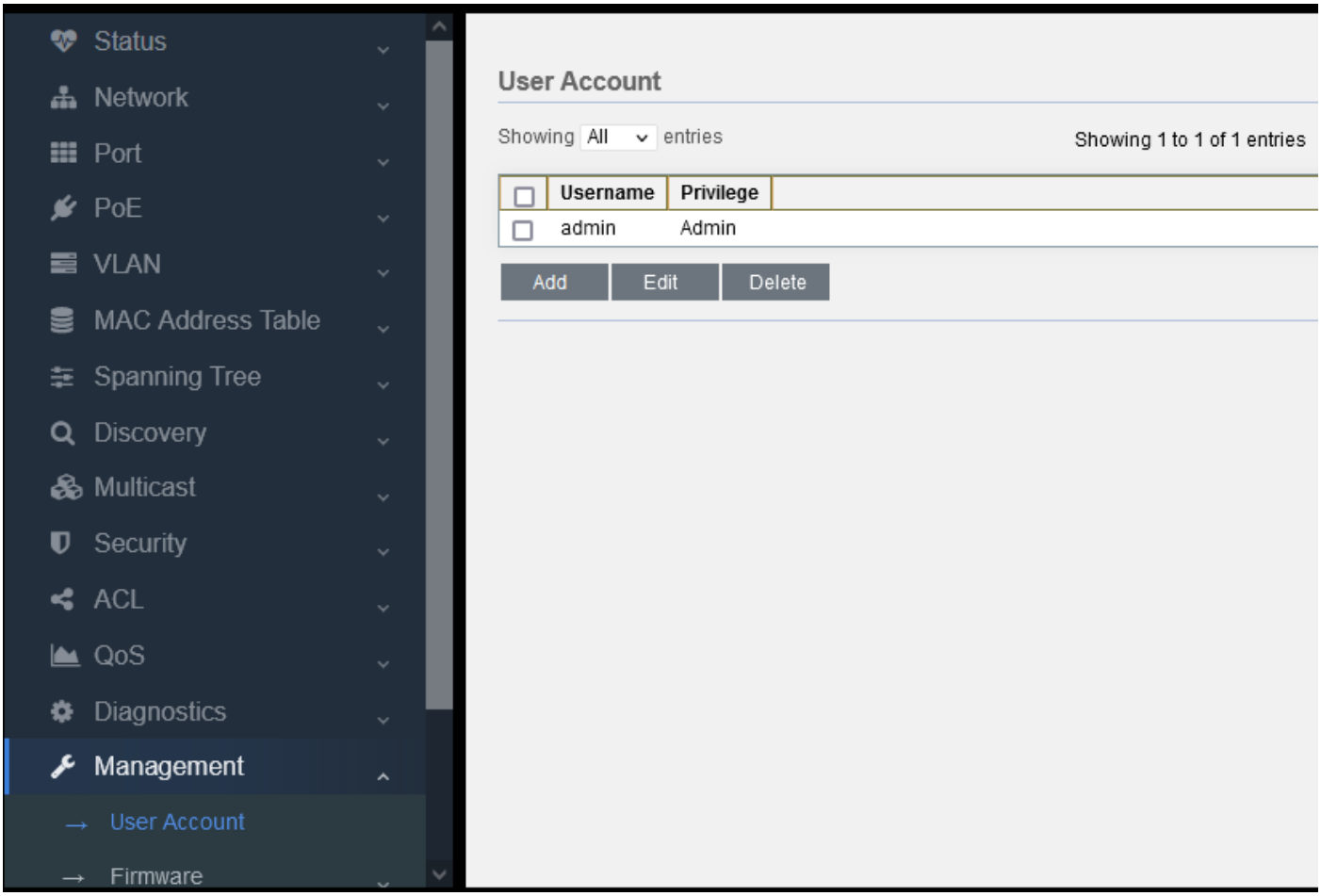


Figure 16-1-1

Click “Add” to add new user.

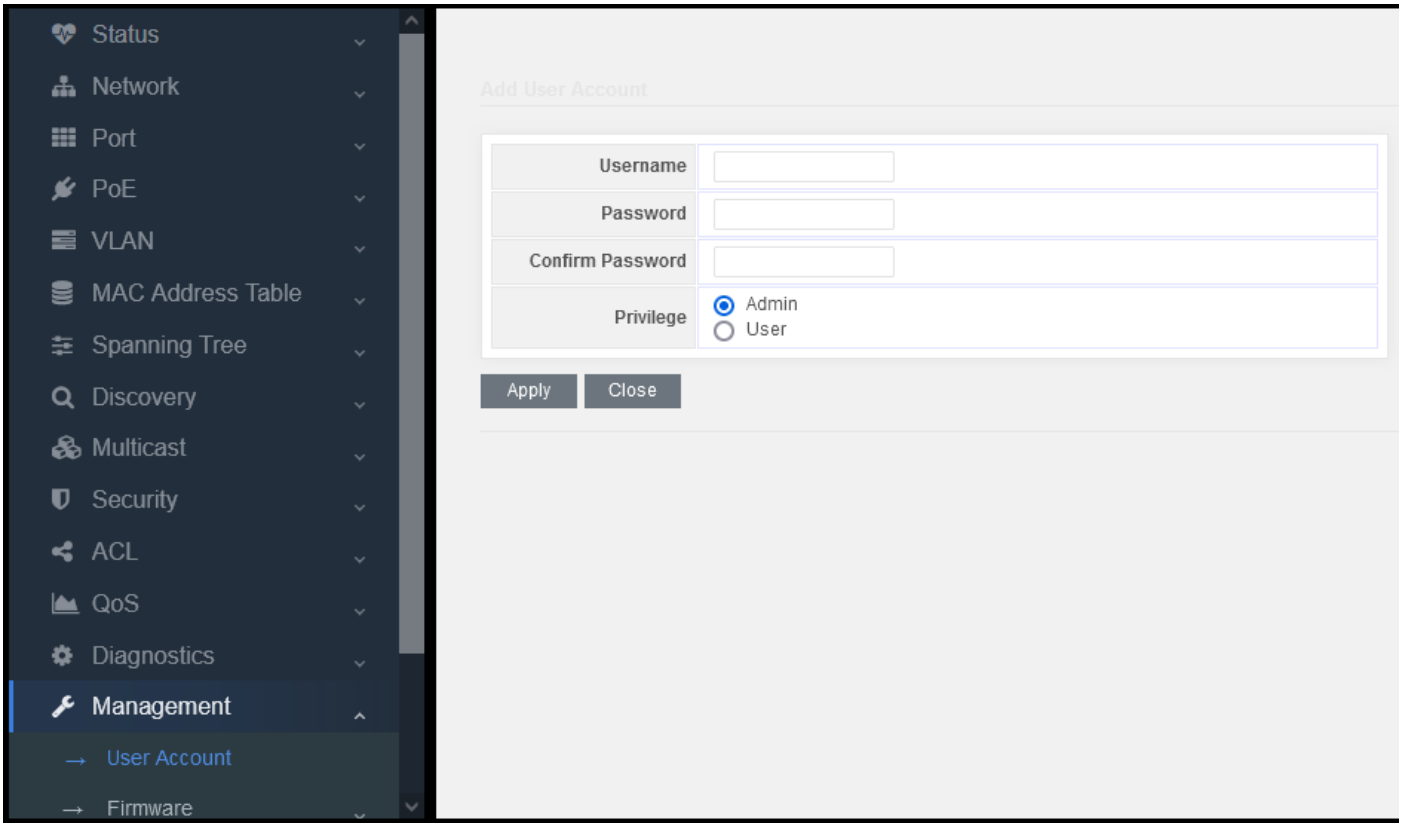


Figure 16-1-2

Input user name and password, and then confirm the password.

There are two levels: Admin and User.

Admin is able to manage all functions of the switch system

User can only manage several functions of the switch,as shown in the following:

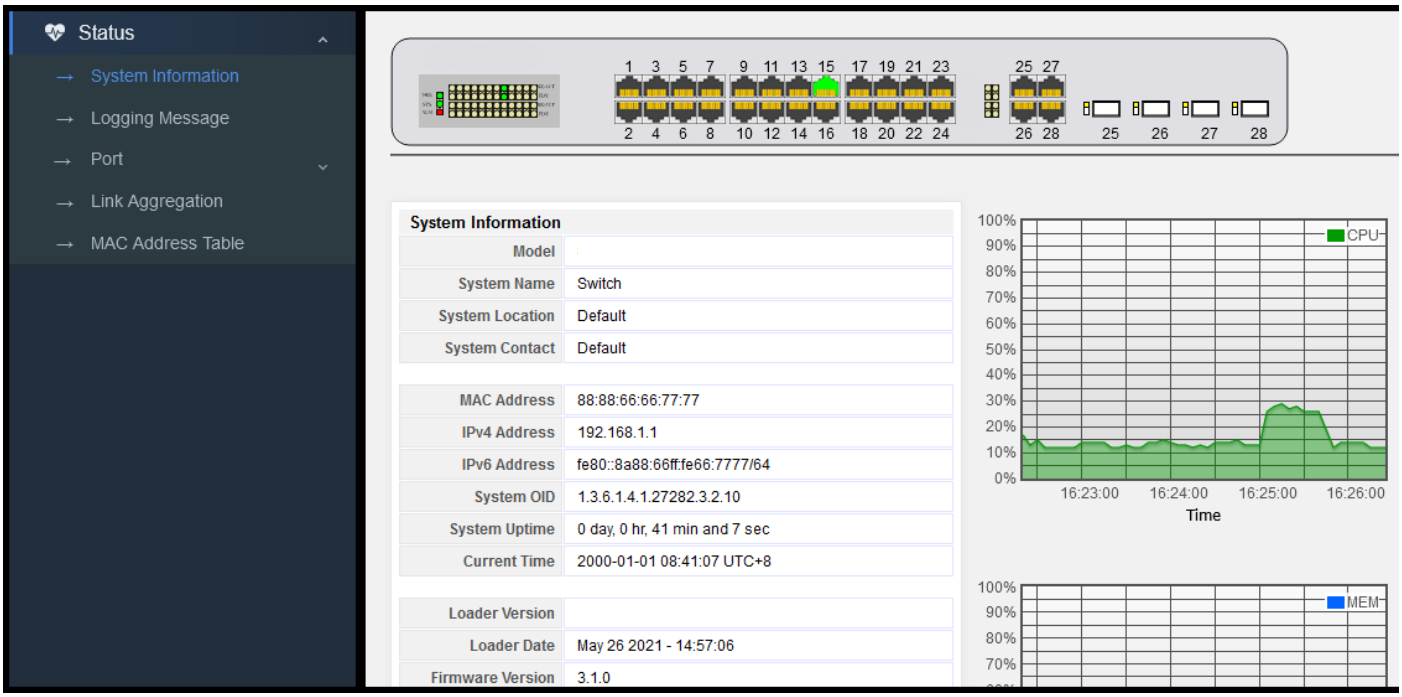


Figure 16-1-3

16.2 Firmware

16.2.1 Upgrade/Backup

The software system can be upgraded and backed up by TFTP or HTTP.

If you want to upgrade, you can select Upgrade or HTTP, and then select the system upgrade file, finally click Apply.

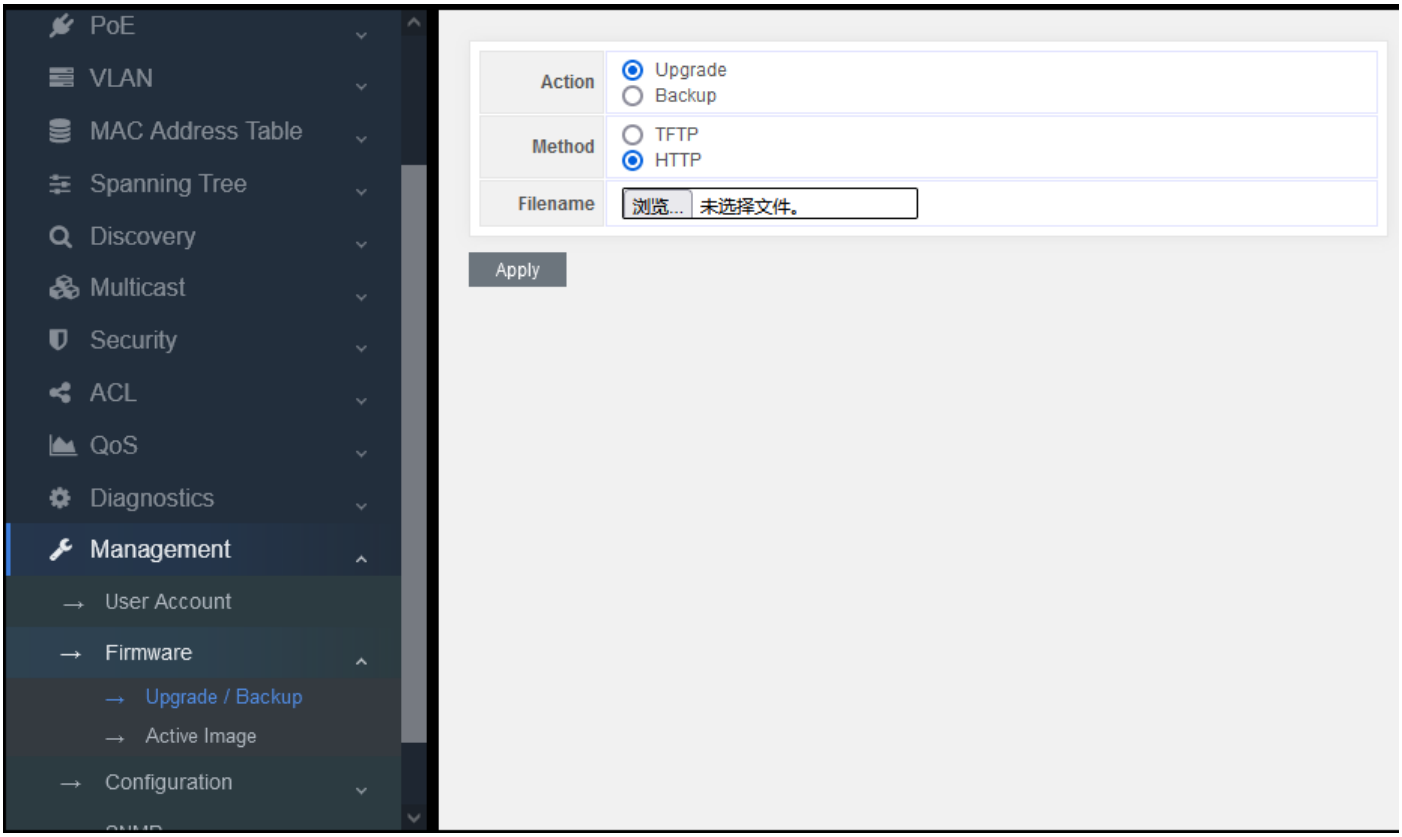


Figure 16-2-1

After the upgrade, pop up the following information. Click OK.

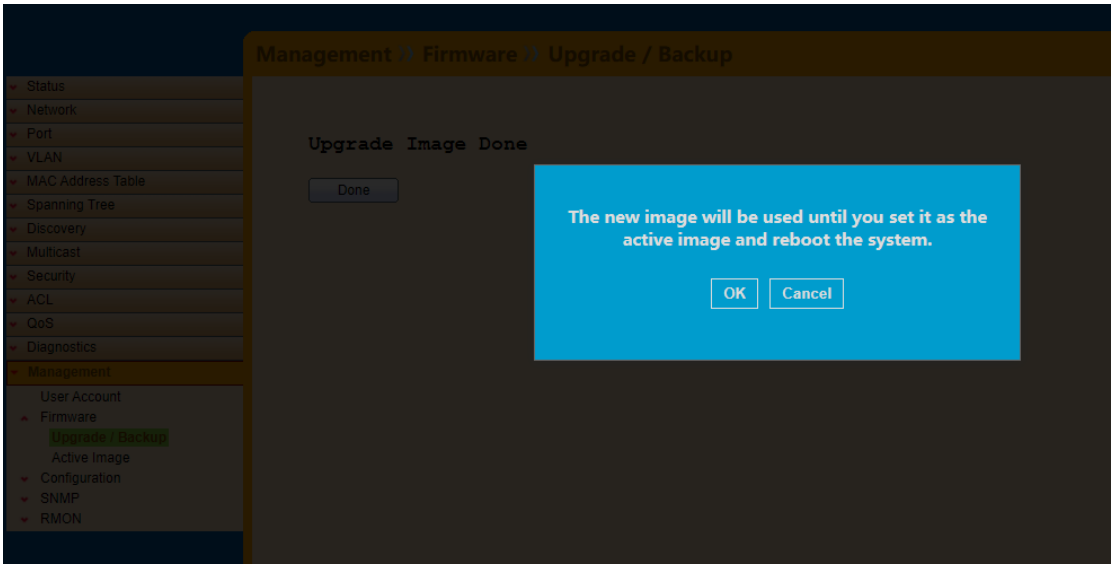


Figure 16-2-2

Then display the following information.

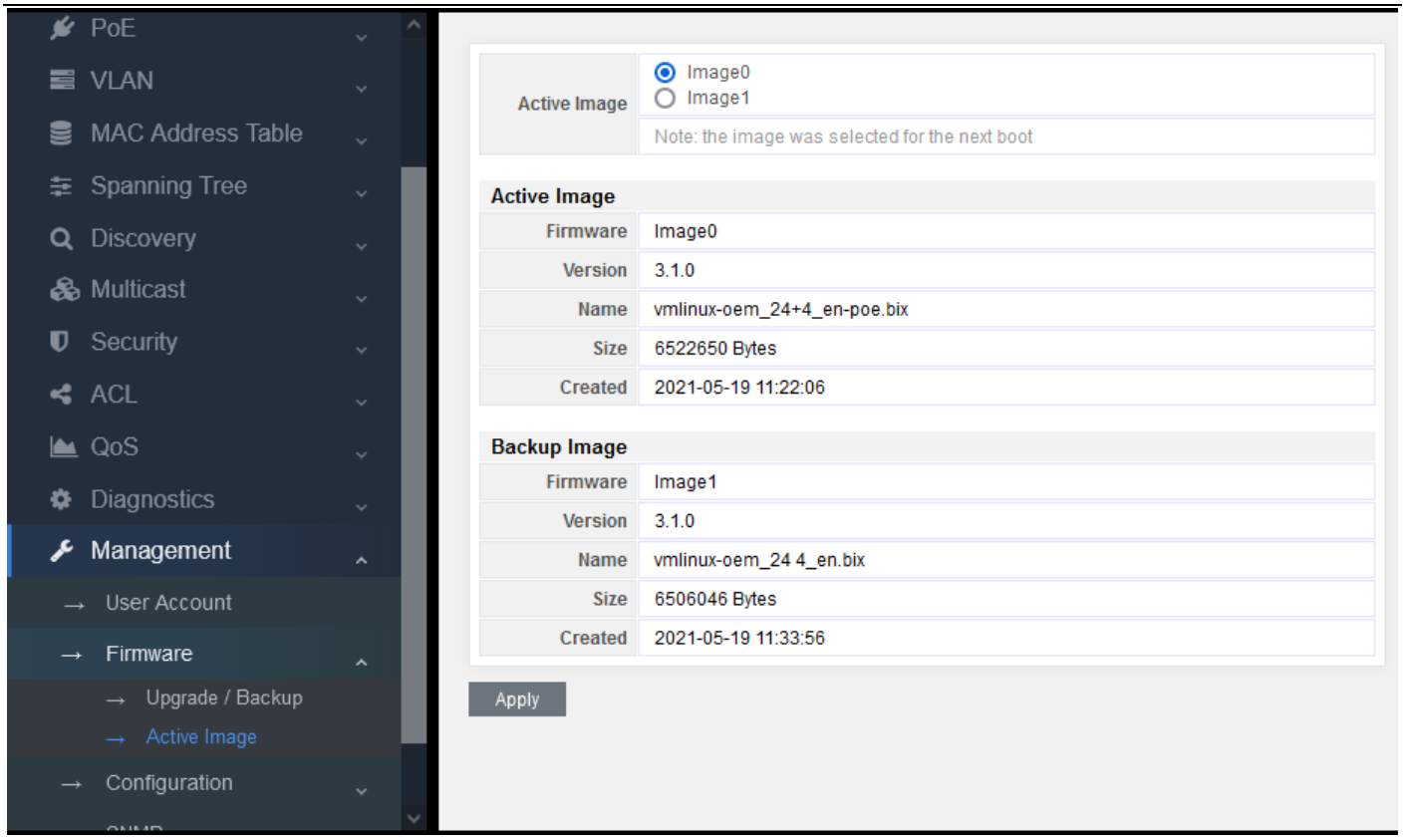


Figure 16-2-3

After the upgrade, you can find out that the upgrade file “vmlinux-oem_24+4_en-poe.bix” we just used is corresponding to the upgraded image0. So now you need to select image0 on the Active Image option, and then click Apply to complete the upgrade, finally click Reboot button.

Note: that the switch is a dual img system. If operating image0 at present, image1 will be upgraded. On the contrary, if image1 is operated, image0 will be upgraded.

16.3 Configuration

16.3.1 Upgrade/Backup

Import parameters/import parameters

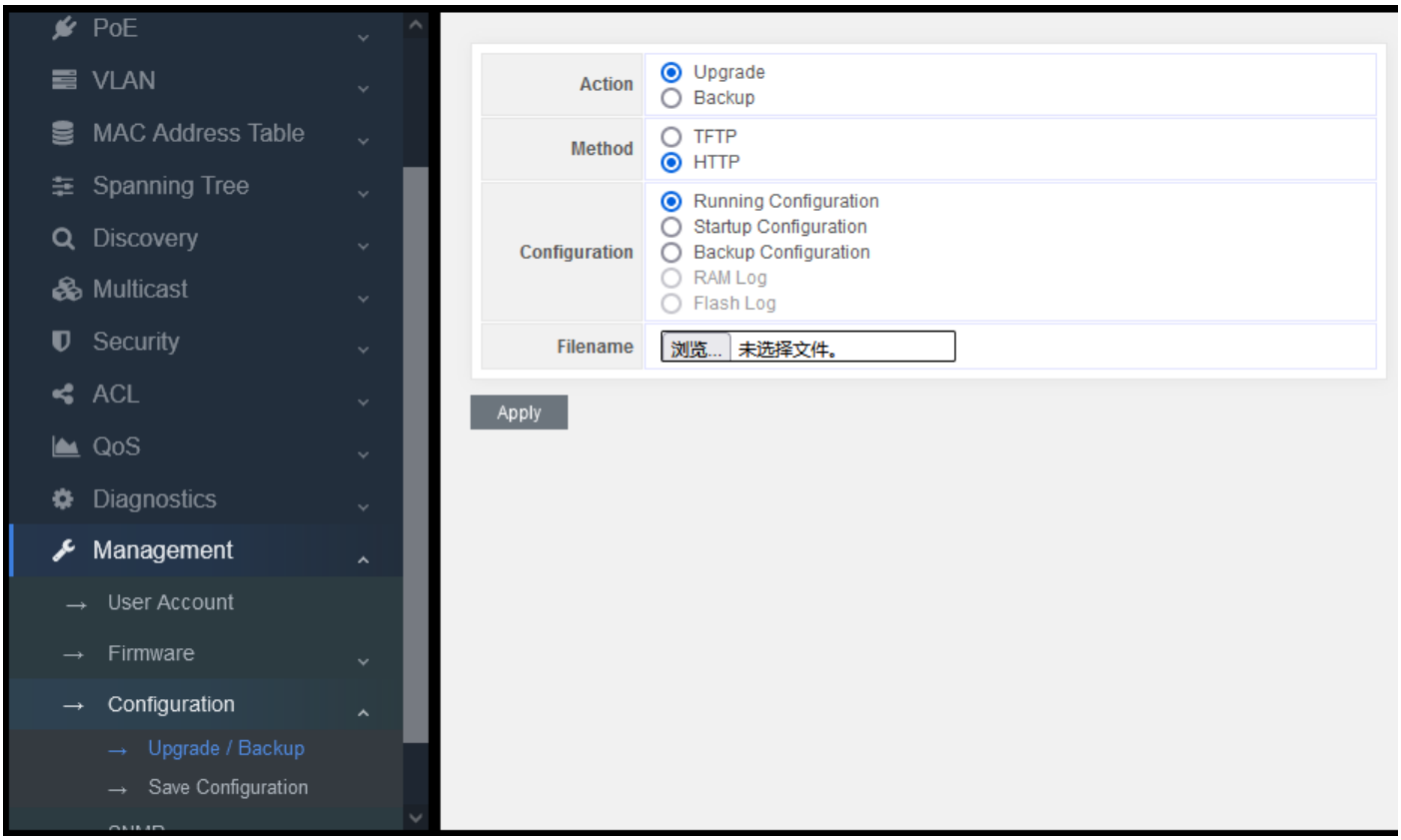


Figure 16-3-1

Action：Upgrade/ Backup
Upgrade: upgrade parameters
Backup: back up parameters

Method：TFTP/HTTP

Configuration：
Running Configuration：Parameters that the system is running
Startup Configuration：Parameters loaded when the system starts
Backup Configuration：Parameters that have been backed up

Note:
When importing parameters, select Startup configuration. Then click restart to complete the parameter import.
When exporting parameters, select Running configuration.

16.3.2 Save Configuration

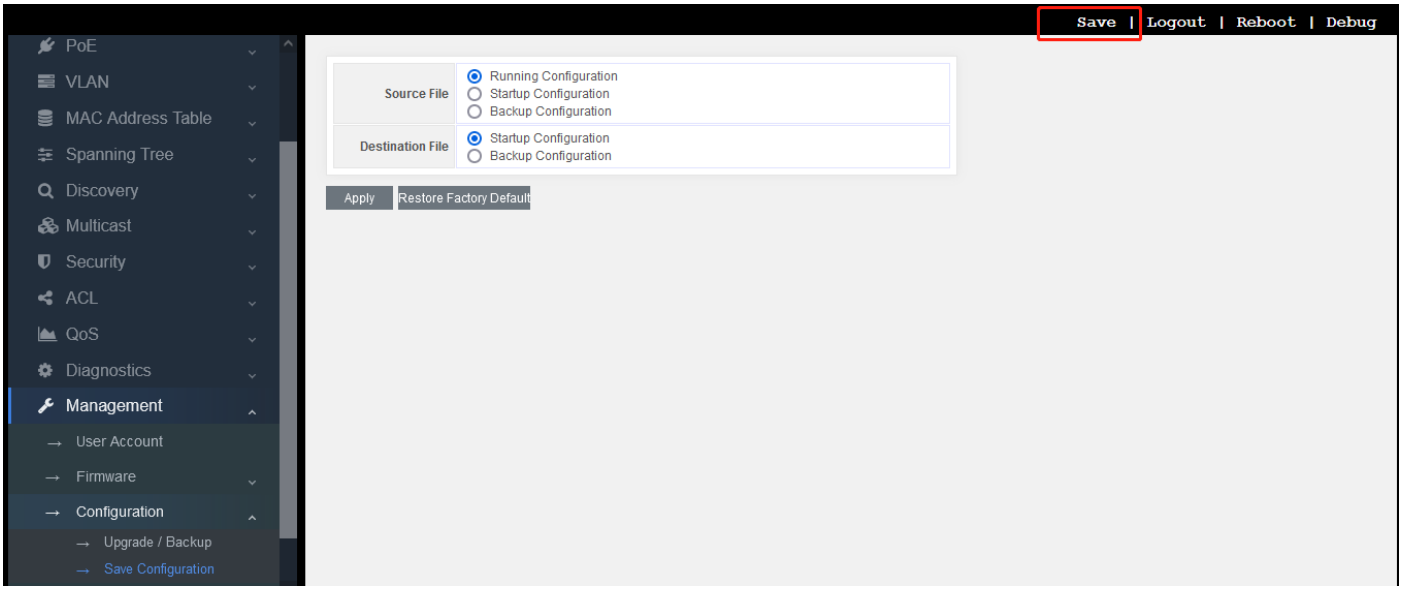


Figure 16-3-2

Copy the source file to the destination file to save the parameters, which is troublesome. The simplest way is to select Save button on the top right.

At the same time, there is also a button to restore the default parameters: “restore factory default”
Click this button, pop up the following interface:

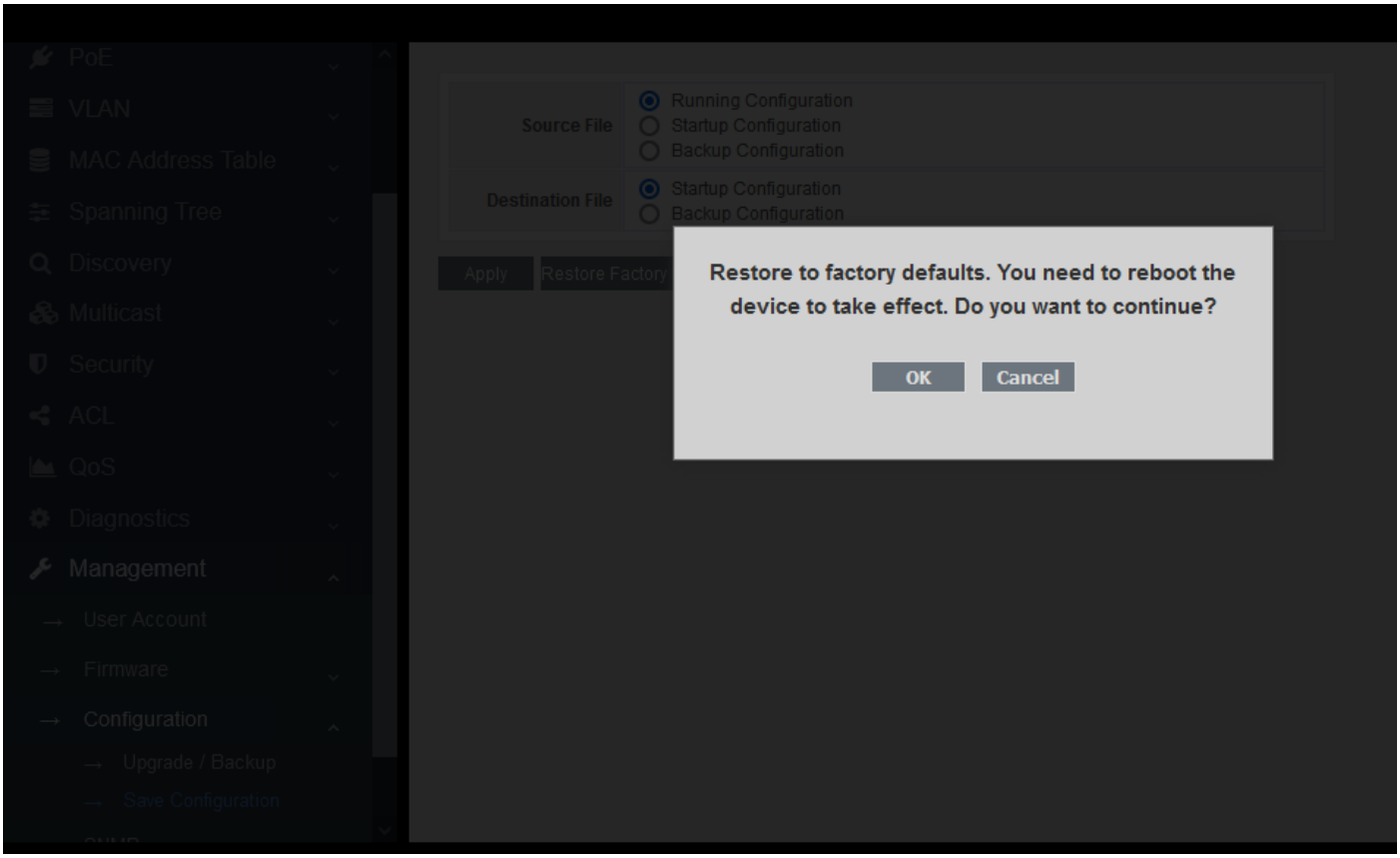


Figure 16-3-3

Click “OK”, and then click Reboot to restore the default parameters.

Part 17:FAQ

17.1 Abnormal display of connection status indicator (connection error)

Check whether the link end is connected to PC network card or other Ethernet interface;
Check whether the link access point is rusty or damaged;
Utilize WEB to check this port connection configuration (duplex and speed) and make sure that its configuration is same as the other end of the link.
Note: if the duplex and speed of this port are both set mandatorily, the configuration of one link must match to that of the other, otherwise the connection cannot be established.

17.2 Normal display of connection status indicator but fail to communicate

If it happens, please follow the following steps:
Check the port stopping or not by WEB page (enter “port configuration”). If the port stops, please enable it.
Check whether the port is isolated with VLAN through WEB page. To compare with other ports, only when the port in same VLAN is set as “access”, they can communicate with each other.

17.3 Unable to log on the switch

Check the switch as the following steps:
Check whether the switch is powered on;
If the connection is failed, check the response of the switch by “ping”. If there is no response, check the IP address configuration of PC and switch. Find out the reason caused such problem according to the return information of HTTP connection.

Check IP address settings
Check the switch as the following steps:
1) Check whether the IP address and subnet mask of the PC are set correctly. Please enter "ipconfig" in the command line window and press enter to check the IP address configuration of the PC.
2) Check whether the IP address, subnet mask and default gateway of the switch are set correctly.
3) Check whether the IP address of the switch is occupied by other devices.

Check login account
When logging in WEB, if the switch continuously requests the user to enter the account and password, this may mean that this account does not exist or this password is invalid.

17.4 Switch start failure

1) Check whether the serial port number is wrong which is usually COM1 and com2;
2) Ensure that the software configuration is as follows: 115200bps, 8 data bits, 1 stop bit, and no parity check and data flow control.
3) Check whether the serial port of PC is normal: you can use the mouse to check whether the serial port fails.
4) Ensure that no other program is using this serial port: in Windows operating system, any serial port cannot be used by more than one program at one time.

17.5 Power supply failure

Check the power indicator. If the indicator is not on, the power connection may be damaged. Please ensure that the power supply is normal, and check whether the connection between the switch and its power supply is stable and reliable.