

Model Number 08015
24+4+4 Giga 400W PoE Switch IEEE802.3af/at

הוראות הפעלה לסוויץ' מנוהל מדגם 08015



חיבור ראשוני

1. בהפעלה הראשונית הסוויץ' מוגדר על כתובת רשת 192.168.2.1, במידה ויש שרת DHCP הוא יקבל כתובת בהתאם לרשת אליה חיברנו. יש לבצע סריקת IP כדי לגלות איזה כתובת הוא קיבל, או לחבר מחוץ לרשת, ולשנות ידנית את כתובת הרשת לסטטית (מפורט יותר לעומק בהמשך).
2. נתחבר לממשק של הסוויץ' בעזרת שם המשתמש - admin והסיסמא - admin.
3. נשנה את השפה לאנגלית בלחיצה על English למעלה מצד ימין.

* בחלון הראשי נוכל להגדיר את כל הפונקציות של הסוויץ' בפאנל משמאל, ולראות את ניצול הזיכרון והמעבד בזמן אמת. במדריך זה נתמקד במספר פונקציות נפוצות - הגדרות רשת בסיסיות, **Vlans**, הגבלת מהירות ב-QoS, **Port security**, **Port mirroring**.

* שימו לב שלאחר כל שינוי הגדרה, יש ללחוץ על SAVE למעלה מצד ימין ואז OK לשמירת ההגדרות בזיכרון הסוויץ', כך שגם לאחר הפעלה מחדש \ הפסקת חשמל ההגדרות יישמרו.

הגדרות רשת בסיסיות

- בפאנל השמאלי ניכנס ל-Network ←
- בשדות המתייחסות ל-IPV4, נוכל לבחור האם לסוויץ תהיה כתובת רשת סטטית או לא ←
- ברירת המחדל היא לא. אם נבחר להגדיר כתובת סטטית, נדרש להזין את הכתובת, ה-Subnet, ←
- וה-Default gateway ←
- כל אלו נגדיר על פי הרשת שאליה נחבר את הסוויץ ←
- לא לשכוח בסיום SAVE

VLAN

הפרדת רשתות לוגית שמאפשרת חיבור רשתות שונות לאותו הסוויץ.

- בפאנל השמאלי ניכנס ל-VLAN ←
- נבחר שוב Vlan ←
- ניכנס ל-Create VLAN ←
- שם נבחר את ה-Vlan שנרצה להוסיף לרשת שלנו, (בדוגמא זו נוסיף את Vlan 2) ←
- נסמן את Vlan 2 ברשימה השמאלית ←
- נלחץ על החץ שיעביר אותו לרשימה הימנית, ונלחץ Apply ←
- כדי לשייך פורטים ל Vlan שהקמנו
- בשדה השמאלי בדיוק מתחת ל-Create VLAN נלחץ על VLAN Configuration ←
- בשורת הבחירה בחלק העליון של הדף נבחר את ה-Vlan החדש שלנו ←
- ועבור הפורטים אותם נרצה להוסיף ל-Vlan פשוט נשנה את הסימון מ Excluded ל-Untagged
- למטה נלחץ Apply ←
- לא לשכוח בסיום SAVE (שימו לב שניהול הסוויץ ב-WEB יכול להתבצע רק מ-Vlan 1 כברירת המחדל).

הגבלת מהירות ב QoS

- במידה ויש עומס רב מפורט מסוים ברשת שלנו, נוכל להגביל את רוחב הפס שלו כדי שלא ישבית לנו את כל הרשת, או נרצה להגביל את שרת הקבצים שלנו לרוחב פס מסוים כדי שלא ישתמש בכל רוחב הפס ויאט את הקצב לכל מי שמחובר לרשת.
- בפאנל השמאלי ניכנס ל-QoS ←
 - ניכנס ל-Rate Limit ←
 - ניכנס ל-Ingress / Egress Port ←
 - נלחץ על Apply ←
 - נבחר את הפורט שעליו נרצה להחיל את ההגבלה ←
 - נסמן Enable ב-Ingress וב-Egress ←
 - ונקליד את רוחב הפס שנרצה להקצות ←
 - 10 מגה לדוגמא זה 10000 (עשרת-אלפים), ו-100 מגה זה 100000 (מאה אלף) ←
 - נלחץ Apply ←
 - לא לשכוח בסיום SAVE ←

Port security

הגנה ברמת הפורט כך שרק מכשיר ספציפי יוכל לגשת לרשת שלנו דרך הפורט, אם תוקף ינסה לחבר את המכשיר שלו אלינו, הסוויץ יזהה את הניסיון ויחסום אותו.

- בפאנל השמאלי ניכנס ל-Port ←
- ניכנס ל-Port security ←
- למעלה נסמן את אפשרות ה-Enable ←
- נלחץ Apply ←
- נסמן למטה את הפורטים שעליהם נרצה להחיל את ההגנה ←
- נלחץ על Edit למטה ←
- ב-State נפעיל את ה-Enable ←
- ב-Violation Action נסמן את Restrict ←
- ב-Sticky נסמן Enable ←
- נלחץ Apply ←
- לא לשכוח בסיום SAVE ←

Port mirroring

מאפשר לנו לשלוח עותק של התעבורה מפורטים כלשהם לפורט מסוים, ובכך לנטר את התעבורה.

- בפאנל השמאלי ניכנס ל-Port ←
- ניכנס ל-Mirroring ←
- נסמן ב-Mirroring Table את אפשרות 1 ונלחץ Edit ←
- נדליק ב-State את ה-Enable ←
- ב-Monitor Port נבחר את הפורט אליו נרצה לשלוח את עותק התעבורה ←
- ב-Ingress Port נבחר את הפורטים שבהם נרצה לנטר את התעבורה הנכנסת (במעבר מהרשימה השמאלית לימנית) ←
- ב-Egress Port נבחר את הפורטים שבהם נרצה לנטר את התעבורה היוצאת (במעבר מהרשימה השמאלית לימנית) ←
- נלחץ Apply ←
- לא לשכוח בסיום SAVE ←

איך מאפסים להגדרות יצרן? – לוחצים עם סיכה על כפתור האיפוס (RESET) שנמצא בקדמת המכשיר למשך 5 שניות, בשחרור הכפתור הנורות חיווי של הפורטים ידלקו יחד. ← כעת נמתין 2 דקות עד שהסוויץ יעלה.

User Manual for Managed Ethernet Switch



WEB Administration Manual

WEB Administration Manual

0 Foreword.....	
0.1 Target Reader.....	
0.2 Icons for the Book.....	
1. Specification of Management Software.....	
2. Interface of WEB Login.....	
2.1 Login WEB Management Client.....	
2.2 Interface of WEB Tree.....	
3. System Configuration.....	
3.1 System Information.....	
3.2 Network Settings.....	
3.3 User Configuration.....	
3.4 Log Configuration.....	
3.5 TELNET Configuration.....	
3.6 HTTPS Configuration.....	
3.7 Diagnostic test.....	
4. Port configuration.....	
4.1 Physical port.....	
4.2 Storm-control.....	
4.3 Port rate limit.....	
4.4 Mirroring.....	
4.5 Link aggregation.....	
4.5.1 Introduction of link aggregation.....	
4.5.2 Adding Static link aggregation	
4.5.3 Adding Dynamic link aggregation.....	
4.6 Port Isolation.....	
4.7 Port statistics.....	
5. Layer 2 configuration.....	
5.1 VLAN configuration.....	
5.2 MAC-VLAN.....	
5.3 PROTOCOL-VLAN.....	
5.4 VOICE VLAN.....	

5.5 MAC configuration.....	
5.5.1 MAC configuration.....	
5.5.2 Static MAC.....	
5.6 MSTP configuration.....	
5.6.1 Global configuration.....	
5.6.2 Example configuration.....	
5.6.3. Instance port configuration.....	
5.6.4 Port configuration.....	
5.7 IGMP-SNOOPING configuration.....	
5.7.1 IGMP-snooping configuration.....	
5.7.2 Static Multicast.....	
5.8 DHCP-SNOOPING configuration.....	
5.8.1 DHCP-snooping global configuration.....	
5.8.2 Static BINDING.....	
5.8.3 DHCP-snooping port configuration.....	
5.9 ERPS-RING configuration.....	
5.9.1 ERPS-Ring global configuration.....	
5.9.2 Node configuration.....	
6 Cybersecurity.....	
6.1 DOS anti-attack settings.....	
6.1.1 Function configuration.....	
6.1.2 Port configuration.....	
6.2 ACL configuration.....	
6.2.1 MAC ACL configuration.....	
6.2.2 IPv4 ACL configuration.....	
6.2.3 IPv6 ACL configuration.....	
6.2.4 ACL binding configuration.....	
7 Advanced configuration.....	
7.1 QOS configuration.....	
7.1.1 Basic configuration.....	
7.1.1.1 Function configuration.....	
7.1.1.2 Queue scheduling.....	
7.1.1.3 CoS mapping.....	
7.1.1.4 DSCP mapping.....	
7.1.1.5 IP priority mapping.....	
7.2 LLDP configuration.....	
7.2.1 LLDP function configuration.....	
7.2.2 Port configuration.....	
7.2.3 Neighbor Information.....	
7.3 SNMP configuration.....	
7.3.1 View configuration.....	
7.3.2 Group configuration.....	

7.3.3 Community configuration.....	
7.3.4 User Configuration.....	
7.3.5 Engine ID configuration.....	
7.3.6 Trap configuration.....	
7.3.7 Notification configuration.....	
7.4 RMON configuration.....	
7.4.1 Port Statistics.....	
7.4.2 Historical configuration.....	
7.4.3 Event Configuration.....	
7.4.4 Alarm configuration.....	
7.6 DNS settings.....	
7.7 System time.....	
8 System Maintenance.....	
8.1.1 Configuration Management.....	
8.1.2 Save configuration.....	
8.2 Restart the device.....	
8.3 Firmware Management.....	
9 POE management settings.....	
9.1.1 POE port configuration.....	
9.1.2 POE timing settings.....	

0 Foreword

0.1 Target Reader

The manual is suitable for installers and system administrators who in charge of installing, configuring, or maintaining the network. This manual assumes that you understand all transport and management protocols used by your network.

This manual also assumes that you are familiar with the terminology, theoretical principles, practical skills, and specific expertise of the protocols and interfaces of network equipment related to networking. At the same time you must have working experience in graphical user interface, command line interface, simple network management protocol and Web browsing.

0.2 Icons for the Book

This manual adopts the following conventions.

GUI conventions	Description
 Description	Description of the operation content, with necessary supplements and instructions.
 Attention	1. Remind the matters needing attention in operation, improper operation may cause data loss or equipment damage. 2. The pictures in the text are subject to the actual UI interface.

1. Management software specifications

1. Layer 2 function			
1.1	Port management	Enable/disable port	support
		speed, duplex, MTU settings	support
		flow-control flow control setting	support
		Port information view support	support
1.2	Port mirroring	Support port aggregation group in and out direction	support
1.3	Port speed limit	Support port speed limit, the speed limit granularity is determined by the chip	Support Granularity 32Kbps
1.4	Port isolation	Support port isolation setting	support
1.5	Storm suppression	Support unknown unicast, unknown multicast, broadcast storm suppression	support
1.6	Link aggregation	Support static manual aggregation	Support
		Support LACP dynamic aggregation	support
1.7	VLAN	access	support
		trunk	support
		hybrid	support
		Support VLAN division based on port, protocol, MAC, QINQ	support
		Support GVRP dynamic VLAN registration	support(128)
		Voice VLAN (support required)	support (16 oui)
1.8	MAC	supports static addition and deletion	support
		MAC address learning limit	support
		Support dynamic aging time setting	support
1.9	Spanning tree	support 802.1d (STP)	support
		Support 802.1w (RSTP)	support
		Support 802.1s (MSTP)	support
1.10	Multicast	Support IGMP-Snooping Support MLD-Snooping	support
		Support MLD-Snooping	support
		Support v1/2/3 dynamic multicast listening	support
1.11	DDM	Support SFP/SFP+DDM	support
2. Extensions			

2.1	ACL	Based on source MAC, destination MAC, protocol type, source IP, destination IP, L4 port number	Support
2.2	QOS	Based on 802.1p (COS) classification	Support
		Based on DSCP classification	Support
		Classification based on source IP, destination IP, port number	Support
		Support SP, WRR scheduling strategy	Support
		Support flow rate limit CAR	Support
2.3	LLDP	Support LLDP link discovery protocol	Support
2.4	User settings	Add/remove users	Support
2.5	Log	User login, operation, status, event recording log	Support
2.6	Anti-attack	DOS defense	Support
		Support CPU protection and limit the rate of sending cpu packets	Support
		ARP binding (IP, MAC, PORT binding)	Support
2.7	Authentication	Support 802.1x port authentication	Support
		Support AAA authentication	Support
2.8	Network diagnosis	Support ping, telnet, trace	Support
2.9	System management	Device reset, configuration save/restore, upgrade management, time setting, etc.	Support
4.Management function			
4.1	CLI	Support serial port command line management	Support
4.2	TELNET	Support telnet remote management	Support
4.3	SSH	Support SSHv1/2 remote management	Support
4.4	SNMP	Support v1/2/3	Support
		Support trap: ColdStart, WarmStart, LinkDown, LinkUp	Support
4.5	WEB	Support two-tier setting, second and third-tier view	Support
4.6	RMON	Support RMON v1	Support
5.Other functions			
5.1 Support DHCP Snooping, Option82			

5.1 Support ring network protection-this function is the ERPS listed above
5.3 POE configuration, POE scheduling management, etc.
5.4 Support dynamic ARP inspection
5.5 Support TACACS+ authentication
5.6 Support DNS settings
5.7 Support port security settings
5.8 Support MVR protocol
5.9 Support cable detection VCT function
5.10 Support UDLD protocol

2.Log in to the web page

2.1 Log in to the web management client

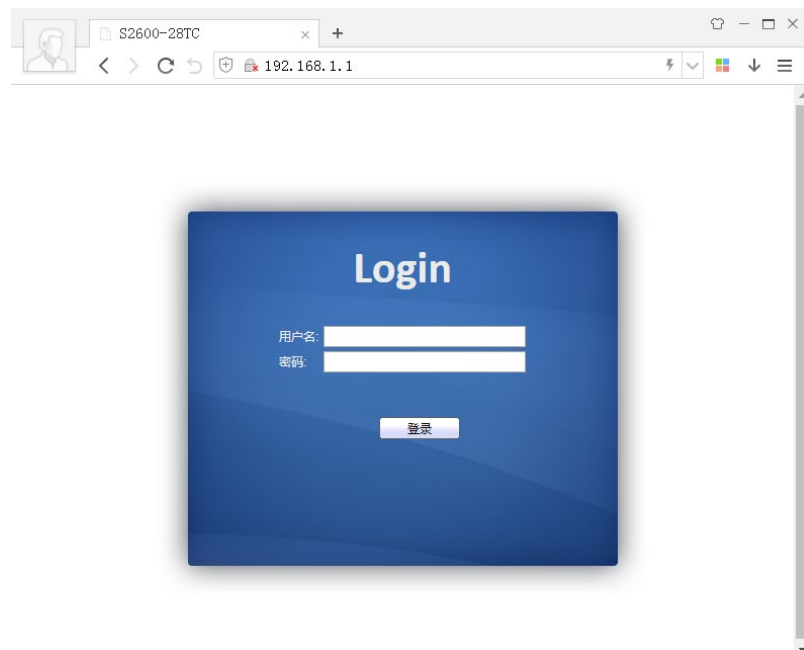
The user can open the web browser, enter the default address of the switch: <http://192.168.2.1>, and press Enter.

 Description:

The device supports browsers: IE8.0 or above, Chrome 23.0 or above, Firefox 20.0 or above

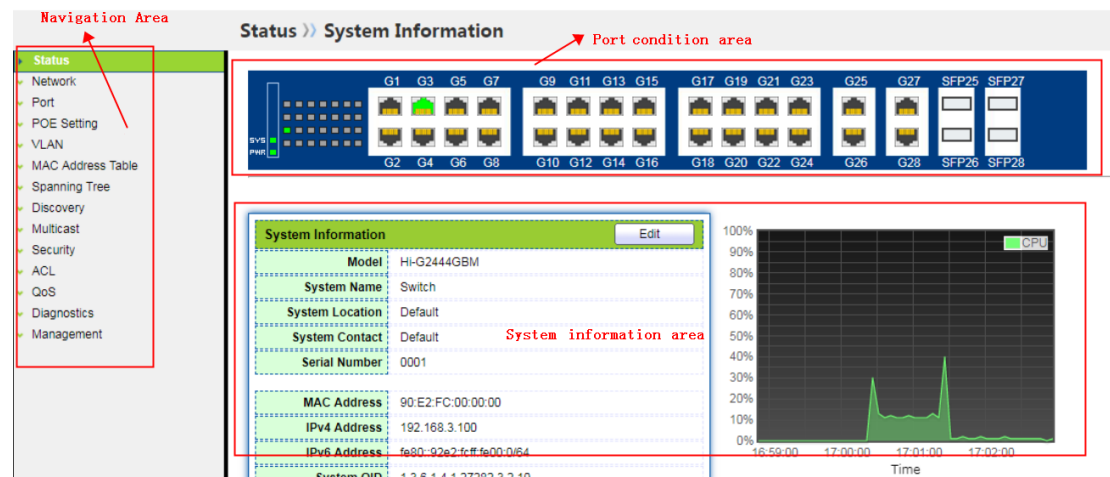
When logging in to the switch, the IP network segment of the PC should be consistent with the network segment of the switch. When logging in for the first time, set the IP address of the PC to 192.168.2.x (x stands for 1~254, except 1), and the subnet mask is set to 255.255.255.0, but the PC IP cannot be the same as the switch, that is, it cannot be 192.168.2.1

The login window appears, as shown in the figure below. Enter the default username: admin and password admin. Click the <Login> button, you will see the switch system information.



2.2 Client interface composition

The introduction of the typical operation interface of the Web network management system is shown in the figure below.



2.3 Web interface navigation tree

The web network management menu mainly provides menu items such as system status, network configuration, ports, POE settings, VLAN functions, MAC address table, spanning tree protocol, topology discovery, multicast, security, ACL, QoS, device diagnosis, and device management. There are submenus under each menu option.

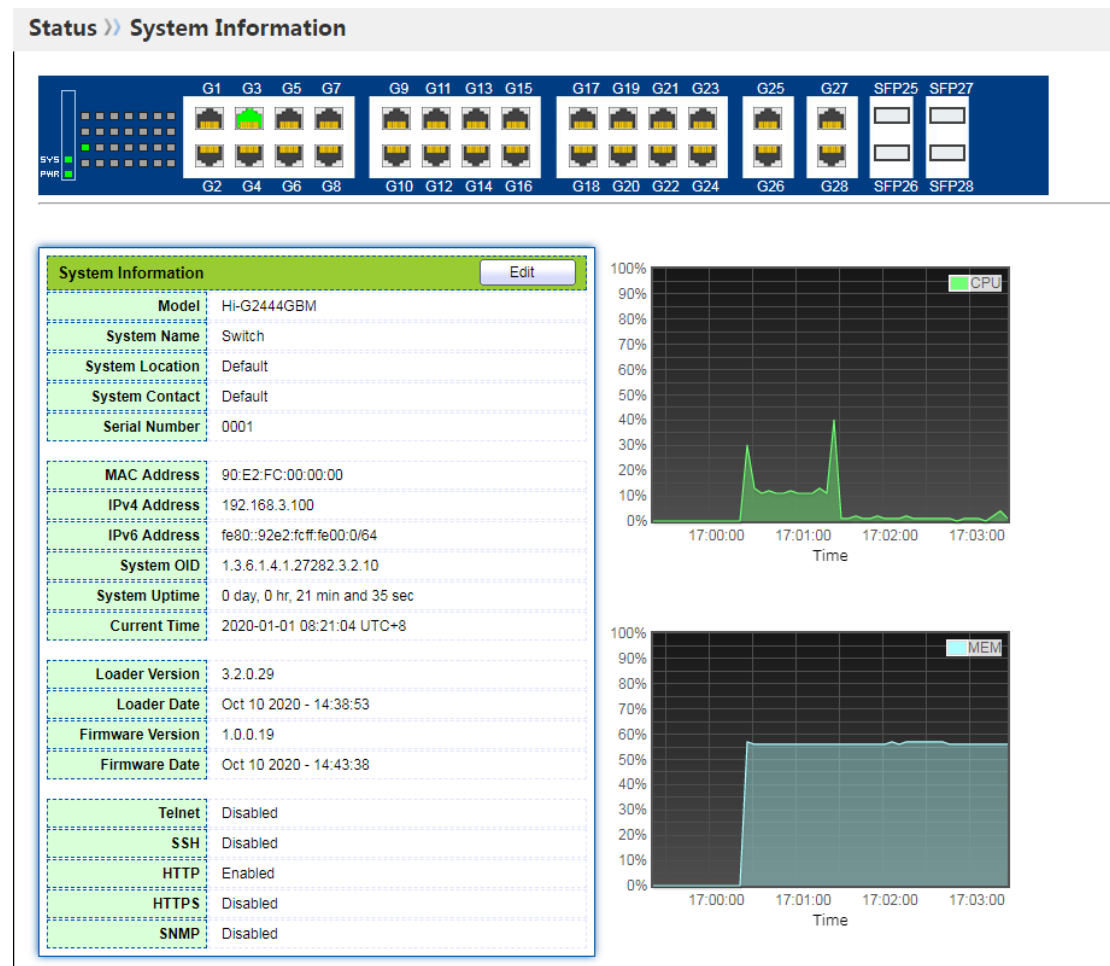
3. System Configuration

3.1 System message

According to the connected switch, the panel display area of the Web network management can display the information and product information of each port on the front panel of the switch very intuitively. The display content includes: the number of ports, the working status of each port, product information, and device status , Function switch status and so on.

Steps:

Click the "System Configuration" menu in the navigation bar to enter the "System Configuration" interface. Click "System Information", as shown in the figure below.



Description:

Place the mouse on a port, the port number, type, speed, and status information of the port will be displayed.

In the product information, you can enter the modification interface to modify the "system name", "location information", and "contact information", click "modify" to enter the modification interface, after filling in the application to complete the configuration.

3.2 Network settings

Enter the web interface to change the management IP address of the switch

Steps:

1. Click the "Network Configuration" menu in the navigation bar to enter the "Network Configuration" interface. Click the "IP Address Settings" submenu, you can see that the default IPv4 address is 192.168.1.1/24, as shown in the figure below.
2. If the user needs to change the IPv4 address to 192.168.1.10/24 and the gateway to 192.168.1.254, click the "Network Configuration" menu in the navigation bar to enter the "Network Configuration" interface. Click the "IP address settings" submenu, select the address type as "static", enter the IPv4 address 192.168.1.10, the subnet mask is 255.255.255.0, and the gateway is 192.168.1.254, click "Apply", as shown in the figure below .

Network >> IP Address

IPv4 Address	
Address Type	☐ Static ☒ Dynamic
IP Address	192.168.3.100
Subnet Mask	255.255.255.0
Default Gateway	192.168.2.254

IPv6 Address	
Auto Configuration	☐ Enable
DHCPv6 Client	☐ Enable
IPv6 Address	
Prefix Length	0 (0 - 128)
IPv6 Gateway	

Operational Status	
IPv4 Address	192.168.3.100
IPv4 Default Gateway	192.168.2.254
IPv6 Address	fe80::92e2:fcff:fe00:0/64
IPv6 Gateway	::
Link Local Address	

Apply

3.3 User configuration

The user can view the current user name, password, and authority of the switch, and the user can modify the user name, password, and authority.

Steps:

1. Click the "Device Management" menu in the navigation bar to enter the "Device Management" interface. Click the "User Configuration" submenu, you can see the default user name: admin, permissions: Administrator. As shown below:

Management >> User Account	
User Account	
Showing: All entries	Showing 1 to 1 of 1 entries
Username	Privilege
admin	Admin
Add Edit Delete	
First Previous Next Last	

Click the Add button to add a user account, and click the Modify button to modify the selected user attributes. The new and modified interface is as shown below:

Management >> User Account

Add User Account

Username	
Password	
Confirm Password	
Privilege	☒ Admin ☐ User

Management >> User Account

Edit User Account

Username	admin
Password	
Confirm Password	
Privilege	☒ Admin ☐ User

3.4 Log configuration

Log configuration can configure the log switch of the device, log information consolidation, log aging time, configure log level, and upload the switch working diary to the TFTP server.

Steps:

1. Click the "device diagnosis" menu in the navigation bar, click the "log function" submenu, select the secondary submenu "function configuration" menu, enter the "function configuration" page, you can choose to open or close the log, select the log output terminal, Configure the log severity level and other functions, the interface is as follows.

Diagnostics >> Logging >> Property

State	☒ Enable
Aggregation	☒ Enable
Aging Time	300 Sec (15 - 3600, default 300)
Console Logging	
State	☒ Enable
Minimum Severity	Notice Note: Emergency, Alert, Critical, Error, Warning, Notice
RAM Logging	
State	☒ Enable
Minimum Severity	Notice Note: Emergency, Alert, Critical, Error, Warning, Notice
Flash Logging	
State	☐ Enable
Minimum Severity	Notice Note: Emergency, Alert, Critical, Error, Warning, Notice

2. Click the "device diagnosis" menu in the navigation bar, click the "log function" submenu, select the secondary submenu "remote server configuration" menu, enter the "remote server configuration" page, this page can add and view remote log server Configuration, the interface is as follows:

Diagnostics >> Logging >> Remote Server

Remote Server Table

	Entry	Server Address	Server Port	Facility	Minimum Severity
0 results found.					

Click the Add button to add a remote log server, and the Modify button to modify the selected log server configuration. The interface is as follows:

Diagnostics >> Logging >> Remote Server

Add Remote Server

Address Type	☒ Hostname ☐ IPv4 ☐ IPv6
Server Address	
Server Port	514 (1 - 65535, default 514)
Facility	Local 7
Minimum Severity	Notice Note: Emergency, Alert, Critical, Error, Warning, Notice

3.5 Telnet configuration

The user can enable and disable the telnet login service in the web interface.

Steps:

Click the "Security" menu in the navigation bar, click the "Management Channel Configuration" submenu, select the secondary submenu "Management Service" menu, enter the "Management Service" configuration page, and click the checkbox behind the Telnet label to open it Or close the Telnet service, the application can take effect. The interface is shown in the figure below:

Management Service		
Telnet	☒	Enable
SSH	☐	Enable
HTTP	☒	Enable
HTTPS	☐	Enable
SNMP	☐	Enable

Session Timeout		
Console	10	Min (0 - 65535, default 10)
Telnet	10	Min (0 - 65535, default 10)
SSH	10	Min (0 - 65535, default 10)
HTTP	10	Min (0 - 65535, default 10)
HTTPS	10	Min (0 - 65535, default 10)

Password Retry Count		
Console	3	(0 - 120, default 3)
Telnet	3	(0 - 120, default 3)
SSH	3	(0 - 120, default 3)

Silent Time		
Console	0	Sec (0 - 65535, default 0)
Telnet	0	Sec (0 - 65535, default 0)
SSH	0	Sec (0 - 65535, default 0)

Apply

3.6 HTTPS configuration

Users can enable and disable HTTP and HTTPS login services in the web interface.

Steps:

Click the "Security" menu in the navigation bar, click the "Management Channel Configuration" submenu, select the secondary submenu "Management Service" menu, enter the "Management Service" configuration page, and click the check box behind the HTTP and HTTPS tags on the page. To enable or disable HTTP and HTTPS services, the application can take effect. The interface is shown in the figure below:

Security » Management Access » Management Service

Management Service		
Telnet	☐	Enable
SSH	☐	Enable
HTTP	☒	Enable
HTTPS	☒	Enable
SNMP	☐	Enable

Session Timeout		
Console	10	Min (0 - 65535, default 10)
Telnet	10	Min (0 - 65535, default 10)
SSH	10	Min (0 - 65535, default 10)
HTTP	10	Min (0 - 65535, default 10)
HTTPS	10	Min (0 - 65535, default 10)

Password Retry Count		
Console	3	(0 - 120, default 3)
Telnet	3	(0 - 120, default 3)
SSH	3	(0 - 120, default 3)

Silent Time		
Console	0	Sec (0 - 65535, default 0)
Telnet	0	Sec (0 - 65535, default 0)
SSH	0	Sec (0 - 65535, default 0)

Apply

3.7 Diagnostic test

The Ping command is used to check whether the specified IP address and host name are reachable, and output corresponding statistics.

Steps:

1. Click the "Device Diagnosis" menu in the navigation bar, click the "Ping" submenu, enter the host name or IP address, and enter the number of tests, as shown in the figure below.

Diagnostics » Ping

Address Type	☒ Hostname ☐ IPv4 ☐ IPv6
Server Address	192.168.1.111
Count	4 (1 - 32)

Ping

Stop

2. Click "Ping", the system will perform a packet sending test to verify whether the address can be

reached, and output the test result, as shown in the following figure:

Ping Result

Packet Status	
Status	Ping failed (timeout)
Transmit Packet	0
Receive Packet	0
Packet Lost	0 %
Round Trip Time	
Min	0 ms
Max	0 ms
Average	0 ms

Traceroute measures how long it takes by sending small packets to the destination device until it returns.

Steps:

1. Click the "Device Diagnosis" menu in the navigation bar, click the "Traceroute" submenu, enter the host name or IP address, you can define the message lifetime, as shown in the figure below.

Diagnostics >> Traceroute

Address Type	☒ Hostname ☐ IPv4
Server Address	192.168.1.122
Time to Live	☐ User Defined 30 (2 - 255, default 30)

2. Click "Apply", the system will start the test, wait for the test to complete, and output the test result, as shown in the figure below:

Traceroute Result

```
traceroute to 192.168.1.122 (192.168.1.122), 30 hops max, 38 byte packets
1traceroute: sendto: Network is unreachable
```

The electrical port test function judges the current state of the network cable connected to the port by the reflected voltage intensity, and locates the fault length position of the network cable (the error is about 5M).

Steps:

1. Click the "Device Diagnosis" menu in the navigation bar, click the "Electrical Port Test" submenu, and select the port to be tested, as shown in the figure below.

Diagnostics >> Copper Test

Port	GE1 ▼
<button>Copper Test</button>	

2. Click "Copper Test", the system will start the test, wait for the test to complete, and output the test results, as shown in the following figure:

Copper Test Result

Cable Status	
Port	GE1
Result	Open Cable
Length	0.97 M

4. Port configuration

4.1 Physical port

To facilitate the identification of the interface, the interface is configured with description information that identifies it. Users can query and configure the Ethernet interface according to their needs.

Steps:

1. Click the "Port" menu in the navigation bar, and click the "Port Configuration" submenu to enter the port configuration page.

Port >> Port Setting

Port Setting Table

☐	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	Up	Auto (1000M)	Auto (Full)	Disabled (Off)
☐	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	Down	Auto	Auto	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
☐	21	GE21	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	22	GE22	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	23	GE23	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	24	GE24	1000M Copper		Enabled	Down	Auto	Auto	Disabled
☐	25	GE25	1000M Combo Copper		Enabled	Down	Auto	Auto	Disabled
☐	26	GE26	1000M Combo Copper		Enabled	Down	Auto	Auto	Disabled
☐	27	GE27	1000M Combo Copper		Enabled	Down	Auto	Auto	Disabled
☐	28	GE28	1000M Combo Copper		Enabled	Down	Auto	Auto	Disabled

Edit

2. Select the port to be configured, you can select multiple ports at the same time, and then click the modify button to enter the modification page.

Port >> Port Setting

Edit Port Setting

Port	GE8-GE12
Description	
State	☒ Enable
Speed	☒ Auto ☐ 10M ☐ Auto - 10M ☐ 100M ☐ Auto - 100M ☐ 1000M ☐ Auto - 1000M ☐ 10G ☐ Auto - 10M/100M
Duplex	☒ Auto ☐ Full ☐ Half
Flow Control	☐ Auto ☐ Enable ☒ Disable

The meaning of configurable item information is as follows:

Configuration item	Description
Description	Users can add description information for the port as needed to identify a specific port
Status	Port opening and closing options, users can switch ports as needed
Speed	Configurable auto-negotiation, mandatory 10M, mandatory 100M, mandatory Gigabit, Gigabit Ethernet electrical interface supports three rates of 10Mbits/s, 100Mbits/s, 1000Mbit/s, you can choose the appropriate interface rate according to your needs.
Duplex	Can be configured with auto-negotiation, full duplex and half duplex mode
Flow control	When the flow control function is enabled on the local and peer devices, if the local device is congested, it will send a message to the peer device to notify the peer device to temporarily stop sending packets; and the peer device is receiving After the message, it will temporarily stop sending messages to the local end, thus avoiding the occurrence of message loss Off — Disable the reception and transmission of PAUSE frames On — enable reception and transmission of PAUSE frames Auto-negotiation—Automatically negotiate the PAUSE frame processing capability with the peer.

4.2 Storm suppression

Basic principles of storm suppression

Storm control uses the following forms to prevent broadcast storms from broadcast, unknown multicast, and unknown unicast packets. The device supports storm control of these three types of packets on the interface according to the packet rate. During a detection interval, the device monitors the average rate of the three types of packets received under the interface and compares it with the configured maximum threshold. When the packet rate is greater than the configured maximum threshold, the device will perform storm control on the interface and execute The configured storm control action.

When a certain Layer 2 Ethernet interface of the device receives a broadcast, multicast, or unknown unicast packet, if the device cannot determine the outgoing interface of the packet based on the destination MAC address of the packet, the device will send it to the same VLAN (Virtual Local Area Network) Other Layer 2 Ethernet interfaces forward these packets, which may cause broadcast storms and reduce device forwarding performance.

The introduction of storm suppression features can control the flow of these three types of messages and prevent broadcast storms.

Steps:

1. Click the "Port" menu in the navigation bar, and click the "Storm Control" submenu to enter the storm control page. The page can configure storm control related attributes, such as mode, etc. The interface is as follows:

Port >> Storm Control

Mode	☐ Packet / Sec
	☒ Kbits / Sec
IFG	☒ Exclude
	☐ Include

Apply

2. On the page, you can configure broadcast, multicast, and unknown unicast storm control rates for each port separately, select the port to be configured, and then click the modify button:

Port Setting Table

☐	Entry	Port	State	Broadcast		Unknown Multicast		Unknown Unicast		Action	
				State	Rate (Kbps)	State	Rate (Kbps)	State	Rate (Kbps)		
☐	1	GE1	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	2	GE2	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	3	GE3	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	4	GE4	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	5	GE5	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	6	GE6	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	7	GE7	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	8	GE8	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	9	GE9	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	10	GE10	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	11	GE11	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	12	GE12	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	13	GE13	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	14	GE14	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	15	GE15	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	16	GE16	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	17	GE17	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	18	GE18	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	19	GE19	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	20	GE20	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	21	GE21	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	22	GE22	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	23	GE23	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	24	GE24	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	25	GE25	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	26	GE26	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	27	GE27	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	
☐	28	GE28	Disabled	Disabled	10000	Disabled	10000	Disabled	10000	Drop	

Edit

3. Enter the modification interface, configure the storm control switch, speed and other information, after the configuration is complete, click Apply to save, the interface is as follows:

Port >> Storm Control

Edit Port Setting

Port	GE11-GE13
State	☐ Enable
Broadcast	☐ Enable
	10000 Kbps (16 - 1000000, default 10000)
Unknown Multicast	☐ Enable
	10000 Kbps (16 - 1000000, default 10000)
Unknown Unicast	☐ Enable
	10000 Kbps (16 - 1000000, default 10000)
Action	☒ Drop ☐ Shutdown

4.3 Port speed limit

Configuring the interface rate limit is to limit the rate at which the physical interface sends or receives data.

Background Information

Before the traffic is sent from the interface, configure the rate limit in the outbound direction of the interface to control the flow of all outgoing packets.

Before the traffic is received from the interface, configure the rate limit in the inbound direction of the interface to control the flow of all incoming packets.

Steps:

1. Click the "QoS" menu in the navigation bar, click the "Bandwidth Speed Limit" submenu, and click the "Port Speed Limit" secondary submenu to enter the port speed limit page, where you can select the speed limit port to view the current speed limit Configuration, as shown below:

QoS >> Rate Limit >> Ingress / Egress Port

Ingress / Egress Port Table

Entry	Port	Ingress		Egress	
		State	Rate (Kbps)	State	Rate (Kbps)
☐	1 GE1	Disabled		Disabled	
☐	2 GE2	Disabled		Disabled	
☐	3 GE3	Disabled		Disabled	
☐	4 GE4	Disabled		Disabled	
☐	5 GE5	Disabled		Disabled	
☐	6 GE6	Disabled		Disabled	
☐	7 GE7	Disabled		Disabled	
☐	8 GE8	Disabled		Disabled	
☐	9 GE9	Disabled		Disabled	
☐	10 GE10	Disabled		Disabled	
☐	11 GE11	Disabled		Disabled	
☐	12 GE12	Disabled		Disabled	
☐	13 GE13	Disabled		Disabled	
☐	14 GE14	Disabled		Disabled	
☐	15 GE15	Disabled		Disabled	
☐	16 GE16	Disabled		Disabled	
☐	17 GE17	Disabled		Disabled	
☐	18 GE18	Disabled		Disabled	
☐	19 GE19	Disabled		Disabled	
☐	20 GE20	Disabled		Disabled	
☐	21 GE21	Disabled		Disabled	
☐	22 GE22	Disabled		Disabled	
☐	23 GE23	Disabled		Disabled	
☐	24 GE24	Disabled		Disabled	
☐	25 GE25	Disabled		Disabled	
☐	26 GE26	Disabled		Disabled	
☐	27 GE27	Disabled		Disabled	
☐	28 GE28	Disabled		Disabled	

2. Select the port that needs speed limit, you can select multiple, and then click the modify button at the bottom of the page to enter the modification page, configure to enable and disable the speed limit function, specify the speed limit rate, and save the application after the configuration is completed. The page is as follows:

QoS >> Rate Limit >> Ingress / Egress Port

[Edit Ingress / Egress Port](#)

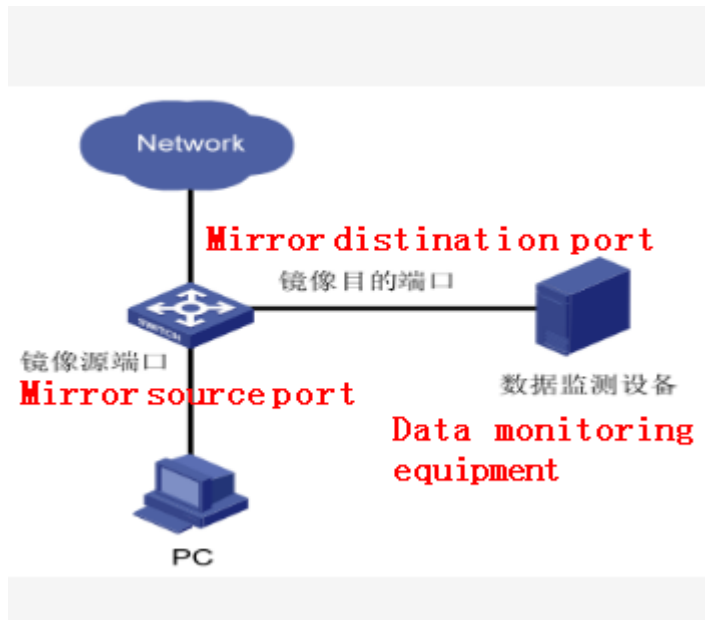
Port	GE8-GE11
Ingress	☐ Enable 1000000 Kbps (16 - 1000000)
Egress	☐ Enable 1000000 Kbps (16 - 1000000)

Configuration parameter description

Configuration item		Description
Entrance	Open	The speed limit switch in the incoming direction
	Rate	The rate limit in the inbound direction, the range is 16-1000000 (Kbps)
Exit	Turn on	The speed limit switch in the exit direction
	Rate	The rate limit in the outbound direction, the range is 16-1000000 (Kbps)

4.4 Port mirroring

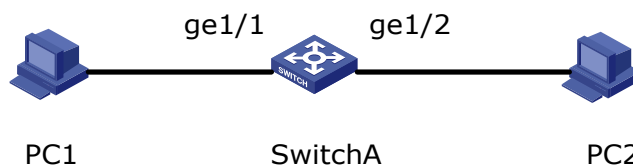
Port mirroring is to copy the packets of the designated port of the switch to the destination port; the copied port is called the source port, and the copied port is called the destination port. The destination port will be connected to the data detection equipment, and the user will use these equipment to analyze the packets received by the destination port for network monitoring and troubleshooting. As shown below:



Configuration example

PC1 connects to SwitchA through interface ge1. PC2 is directly connected to the ge2 interface of SwitchA.

The user wants to monitor the message sent by PC1 through the monitoring device PC2.



Steps:

1. Click the "Port" menu in the navigation bar, and click the "Mirror function" submenu to enter the mirror configuration page. 4 sets of flow mirroring rules can be configured on the page, the interface is as follows:

Port >> Mirroring

Mirroring Table

Session ID	State	Monitor Port	Ingress Port	Egress Port
1	Disabled	---	---	---
2	Disabled	---	---	---
3	Disabled	---	---	---
4	Disabled	---	---	---

Edit

*** Allow the monitor port to send or receive normal packets

2. Select one group of mirroring sessions and click the Modify button to enter the mirroring group configuration interface:

Port >> Mirroring

Edit Mirroring

Session ID: 1

State: ☐ Enable

Monitor Port: GE1

☐ Send or Receive Normal Packet

Ingress Port

Available Port: GE1, GE2, GE3, GE4, GE5, GE6, GE7, GE8

Selected Port:

Egress Port

Available Port: GE1, GE2, GE3, GE4, GE5, GE6, GE7, GE8

Selected Port:

Apply Close

The meaning of the interface information is as follows

Configuration item	Description
Session ID	The switch has 4 mirroring session IDs by default
Status	Whether the mirroring group is enabled
The destination port	cannot be a link aggregation port, only a common physical port can be selected as the destination port, and cannot be selected as the source port at the same time
Source Incoming Port	Any packets received on this port are mirrored to the destination port
Source outgoing port	Any message sent from this port will be mirrored to the destination port.

4.5 Link aggregation

4.5.1 Introduction to link aggregation

Link Aggregation is a method of bundling a group of physical interfaces together as a logical interface to increase bandwidth and reliability.

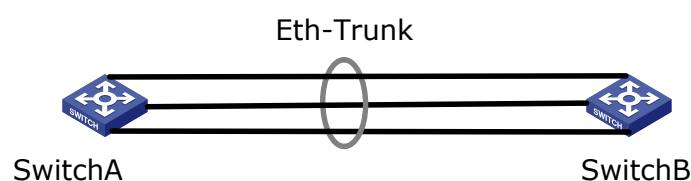
Link Aggregation Group (LAG) refers to a logical link formed by bundling several Ethernet links,

abbreviated as Eth-Trunk.

With the continuous expansion of network scale, users have put forward higher and higher requirements for link bandwidth and reliability. In the traditional technology, the method of replacing the high-speed interface board or the device supporting the high-speed interface board is often used to increase the bandwidth, but this kind of solution requires a high cost and is not flexible enough.

The use of link aggregation technology can achieve the purpose of increasing link bandwidth by bundling multiple physical interfaces into one logical interface without hardware upgrades. The backup mechanism of link aggregation can effectively improve reliability, and at the same time, it can also achieve load sharing of traffic on different physical links.

As shown in the figure below, SwitchA and SwitchB are connected by three Ethernet physical links. Bundling these three links together becomes an Eth-Trunk logical link. The bandwidth of this logical link is equal to the original three Ethernet links. The total bandwidth of the physical links of the network, thereby achieving the purpose of increasing link bandwidth; at the same time, these three Ethernet physical links back up each other, effectively improving the reliability of the link.



You can configure link aggregation to achieve the following requirements:

When the bandwidth of a link connection between two switch devices is insufficient.

When the reliability of the connection between two switch devices through a link does not meet the requirements.

According to whether the link aggregation control protocol LACP is enabled, link aggregation is divided into static mode and LACP mode.

In static mode, the establishment of Eth-Trunk and the joining of member interfaces are manually configured without the participation of link aggregation control protocol. In this mode, all active links participate in data forwarding and share traffic equally, so it is called load sharing mode. If an active link fails, the link aggregation group automatically shares the traffic equally among the remaining active links. When you need to provide a larger link bandwidth between two directly connected devices and the device does not support the LACP protocol, you can use the static mode.

4.5.2 Add static link aggregation

Steps to add static link aggregation:

1. Click the "Port" menu in the navigation bar, click the "Link Aggregation" submenu, and click the "Aggregation Group Configuration" secondary submenu to enter the link aggregation group configuration interface. The device supports two load balancing algorithms. Select one of them by selecting the box, and the application save takes effect, as shown in the figure below:

Port >> Link Aggregation >> Group

☐ Load Balance Algorithm
 ☒ MAC Address
 ☐ IP-MAC Address

Apply

Link Aggregation Table

LAG	Name	Type	Link Status	Active Member	Inactive Member
LAG 1	---	---	---	---	---
LAG 2	---	---	---	---	---
LAG 3	---	---	---	---	---
LAG 4	---	---	---	---	---
LAG 5	---	---	---	---	---
LAG 6	---	---	---	---	---
LAG 7	---	---	---	---	---
LAG 8	---	---	---	---	---

Edit

2. The device supports 8 link aggregation groups, select one of them, and click the Modify button to enter the configuration page, as shown in the figure below:

Port >> Link Aggregation >> Group

Edit Link Aggregation Group

LAG

1

Name

Type

☒ Static
 ☐ LACP

Member

Available Port

GE1
GE2
GE3
GE4
GE5
GE6
GE7
GE8

>
<

Selected Port

Apply Close

The meaning of the interface information is as follows:

Configuration item	Description
LAG	link aggregation group ID, a total of 1 to 8, 8 aggregation groups
Name	The description information of the link aggregation group, which can be modified as needed
Type	Choose whether to aggregate statically or dynamically aggregate based on LACP
Member	The member ports included in the link aggregation group, up to 8 ports

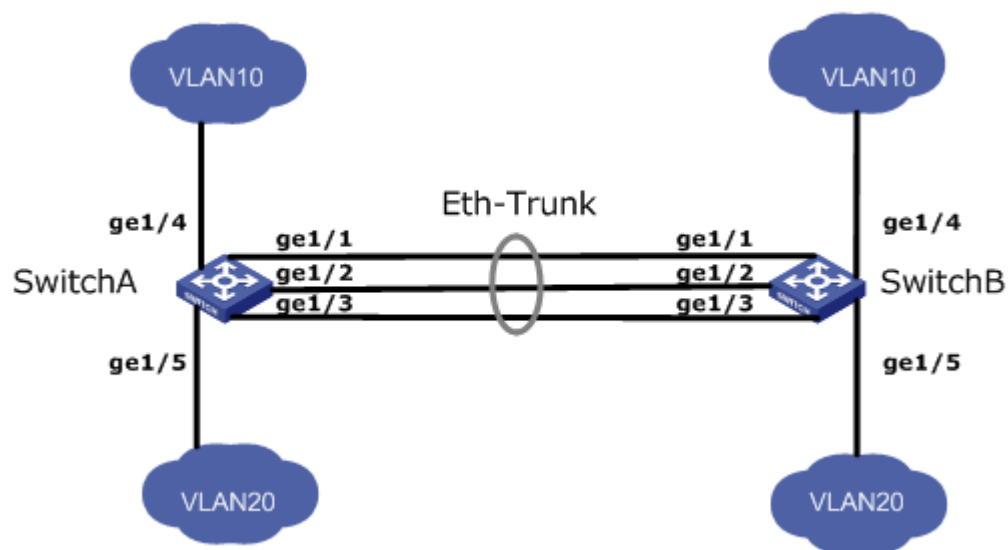
Example:

As shown in the figure below, SwitchA and SwitchB are respectively connected to the networks of VLAN10 and VLAN20 through Ethernet links, and there is a large amount of data traffic between SwitchA and SwitchB.

Users hope that SwitchA and SwitchB can provide a larger link bandwidth to communicate with

each other in the same VLAN. At the same time, users also hope to provide a certain degree of redundancy to ensure the reliability of data transmission and links.

Networking diagram of link aggregation in manual load sharing mode



Steps:

1. Create an Eth-Trunk interface on SwitchA and add member interfaces to increase the link bandwidth. The configuration of SwitchB is similar to that of SwitchA and will not be repeated. Click the "Port" menu in the navigation bar, click the "Link Aggregation" submenu, click the "Aggregation Group Configuration" secondary submenu, enter the link aggregation group configuration interface, select the group "LAG 1", and select the port to be aggregated For ge1, ge2, and ge3, click the right arrow to move to the selected port, and click "Apply" to take effect, as shown in the figure below.

Port >> Link Aggregation >> Group

Edit Link Aggregation Group

LAG	1																				
Name																					
Type	☒ Static ☐ LACP																				
Member	<table><thead><tr><th>Available Port</th><th></th><th>Selected Port</th></tr></thead><tbody><tr><td>GE4</td><td rowspan="8"> > < </td><td>GE1</td></tr><tr><td>GE5</td><td>GE2</td></tr><tr><td>GE6</td><td>GE3</td></tr><tr><td>GE7</td><td></td></tr><tr><td>GE8</td><td></td></tr><tr><td>GE9</td><td></td></tr><tr><td>GE10</td><td></td></tr><tr><td>GE11</td><td></td></tr></tbody></table>	Available Port		Selected Port	GE4	> <	GE1	GE5	GE2	GE6	GE3	GE7		GE8		GE9		GE10		GE11	
Available Port		Selected Port																			
GE4	> <	GE1																			
GE5		GE2																			
GE6		GE3																			
GE7																					
GE8																					
GE9																					
GE10																					
GE11																					

4.5.3 Add dynamic link aggregation

Dynamic link aggregation

LACP (Link Aggregation Control Protocol, Link Aggregation Control Protocol) based on the IEEE802.3ad standard is a protocol for dynamic link aggregation and disaggregation. The LACP protocol exchanges information with the opposite end through LACPDUs (Link Aggregation Control Protocol Data Unit, Link Aggregation Control Protocol Data Unit).

After opening the LACP protocol of a port, the port will send LACPDUs to notify the opposite end of its system priority, system MAC, port priority, port number, and operation key. After receiving the information, the opposite end compares the information with the information stored in other ports to select a port that can be aggregated, so that both parties can reach an agreement on the port joining or leaving a dynamic aggregation group.

Dynamic LACP aggregation is an aggregation that the system automatically creates or deletes. The addition and deletion of ports in a dynamic aggregation group is done automatically by the protocol. Only ports with the same speed and duplex properties, connected to the same device, and the same basic configuration can be dynamically aggregated.

Steps to add dynamic link aggregation:

1. Click the "Port" menu in the navigation bar, click the "Link Aggregation" submenu, click the "Aggregation Group Configuration" secondary submenu, enter the link aggregation group configuration interface, select the link aggregation group ID to be configured, Click the Modify button to enter the modification page, select the type as LACP, as shown in the figure below:

Port >> Link Aggregation >> Group

Edit Link Aggregation Group

LAG 1

Name

Type

Static

LACP

Member

Available Port

Selected Port

GE4

GE5

GE6

GE7

GE8

GE9

GE10

GE11

GE1

GE2

GE3

Apply

Close

2. Click the "Link Aggregation" submenu again, click the "LACP Configuration" secondary submenu, enter the LACP properties configuration page, you can configure LACP related properties, such as system priority, port priority, port timeout mode, etc., as shown below :

Port >> Link Aggregation >> LACP

System Priority 32768 (1 - 65535, default 32768)

Apply

LACP Port Setting Table

Entry	Port	Port Priority	Timeout
1	GE1	1	Long
2	GE2	1	Long
3	GE3	1	Long
4	GE4	1	Long
5	GE5	1	Long
6	GE6	1	Long
7	GE7	1	Long
8	GE8	1	Long
9	GE9	1	Long
10	GE10	1	Long
11	GE11	1	Long
12	GE12	1	Long
13	GE13	1	Long
14	GE14	1	Long
15	GE15	1	Long
16	GE16	1	Long
17	GE17	1	Long
18	GE18	1	Long
19	GE19	1	Long
20	GE20	1	Long
21	GE21	1	Long
22	GE22	1	Long
23	GE23	1	Long
24	GE24	1	Long
25	GE25	1	Long
26	GE26	1	Long
27	GE27	1	Long
28	GE28	1	Long

The meaning of the interface information is as follows

Configuration item	Description
Type	static and LACP, Static mode When you need to increase the bandwidth or reliability between two devices, and one of the two devices does not support the LACP protocol, you can create a static link aggregation on the device and add multiple member

	interfaces to increase the bandwidth and reliability between the devices Sex. LACP mode In the dynamic LACP mode, the link between the two devices has the capability of redundant backup. When part of the link fails, the backup link is used to replace the failed link to keep data transmission uninterrupted.
System priority	LACP determines the choice of active and passive mode between two devices according to priority
Port priority	LACP determines the dynamic aggregation group membership mode based on the device port priority of the higher system priority.
The timeout period	Determines the frequency of LACP protocol message sending

Description:

Before changing the Eth-Trunk working mode, please make sure that no member interface is added to the Eth-Trunk, otherwise the Eth-Trunk working mode cannot be modified.

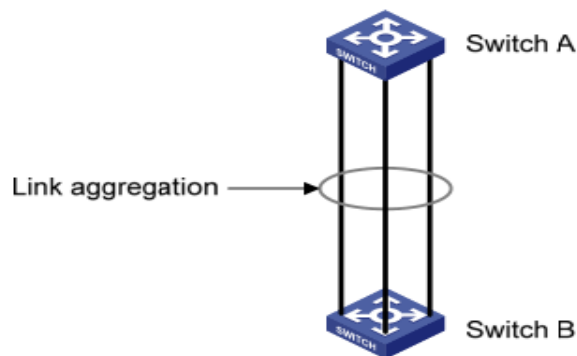
The working mode configured on the local end and the opposite end should be consistent.

for example

Ethernet switch Switch A uses 3 ports (GE1~GE3) for aggregation

Connect to the Ethernet switch Switch B to achieve load sharing among the member ports.

In the actual configuration below, the dynamic convergence method will be used as examples.



Steps:

Description:

The following only lists the configuration for Switch A. The same configuration is also required for Switch B to achieve port aggregation.

Steps:

1. Click the "Port" menu in the navigation bar, click the "Link Aggregation" submenu, click the "Aggregation Group Configuration" secondary submenu, enter the link aggregation group configuration interface, select LAG 2, and click "Modify". Select GE1-GE3, select the type as LACP, and click "Apply", as shown in the figure below:

Port >> Link Aggregation >> Group

Edit Link Aggregation Group

LAG 1

Name

Type ☐ Static ☒ LACP

Member

Available Port

Selected Port

GE4
GE5
GE6
GE7
GE8
GE9
GE10
GE11

GE1
GE2
GE3

Apply

Close

4.6 Port isolation

Port traffic sometimes does not need to communicate with each other, but broadcast, multicast, and other messages will be flooded between ports. In this case, the port isolation function can be used to achieve message isolation between ports.

Steps:

1. Click the "Port" menu in the navigation bar, click the "Port Isolation" sub-menu, enter the port isolation configuration interface, check the ports that need to be isolated, you can select multiple, click modify, configure the isolation function switch, as shown in the figure below :

Protected Port Table

Entry	Port	State
☐	1 GE1	Unprotected
☐	2 GE2	Unprotected
☐	3 GE3	Unprotected
☐	4 GE4	Unprotected
☐	5 GE5	Unprotected
☐	6 GE6	Unprotected
☐	7 GE7	Unprotected
☐	8 GE8	Unprotected
☐	9 GE9	Unprotected

Edit Protected Port

Port GE1-GE4

State ☐ Protected

Apply

Close

The following example illustrates, as shown in the figure below, PC1, PC2 and PC3 are connected to GE1, GE2, and GE3 respectively. The user hopes that PC1, PC2 and PC3 cannot access each other.

Steps:

1. Click the "Port" menu in the navigation bar, click the "Port Isolation" submenu, enter the port

isolation configuration interface, check GE1, GE2, and GE3, click Modify, check isolation, and click Apply to save the effect. The result is as shown in the figure below Show:

Protected Port Table

Entry	Port	State
☐	1 GE1	Protected
☐	2 GE2	Protected
☐	3 GE3	Protected
☐	4 GE4	Unprotected
☐	5 GE5	Unprotected

At this time, GE1, GE2, and GE3 cannot communicate with each other, and can communicate with other non-isolated ports.

4.7 Port Statistics

a. Introduce the detailed information of all interface traffic statistics and the information that users can manually refresh or clear statistics.



Note: After the traffic statistics information is cleared, it cannot be restored. Please confirm carefully before operation. .

Steps:

1. Click the "Device Management" menu in the navigation bar, click the "RMON Settings" submenu, and click the "Message Statistics" secondary submenu, as shown below:

Statistics Table

Refresh Rate: 5 sec

Entry	Port	Bytes Received	Drop Events	Packets Received	Broadcast Packets	Multicast Packets	CRC & Align Errors	Undersize Packets	Oversize Packets	Fragments	Jabbers	Collisions	Frames of 64 Bytes	Frames of 65 to 127 Bytes	Frames of 128 to 255 Bytes	Frames of 256 to 511 Bytes	Frames of 512 to 1023 Bytes	Frames Greater than 1024 Bytes
☐	1 GE1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	2 GE2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	3 GE3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	4 GE4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	5 GE5	415433	0	3876	2454	1099	0	0	0	0	0	0	2462	555	514	24	53	0
☐	6 GE6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	7 GE7	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	8 GE8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	9 GE9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	10 GE10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	11 GE11	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	12 GE12	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	13 GE13	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	14 GE14	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	15 GE15	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	16 GE16	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	17 GE17	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	18 GE18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	19 GE19	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	20 GE20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	21 GE21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	22 GE22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	23 GE23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	24 GE24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	25 GE25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	26 GE26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	27 GE27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	28 GE28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	29 LA21	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	30 LA22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	31 LA23	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	32 LA24	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	33 LA25	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	34 LA26	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	35 LA27	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	36 LA28	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Description:

Click "Refresh" to get the latest traffic statistics on the page.

Click "Clear" to clear the traffic statistics of all ports and refresh the page.

Select a port and click the View button to display the detailed port statistics page.

b. Introduce the detailed information of a certain interface traffic statistics and the information

that users can manually refresh or clear statistics.

1. Click the "System Status" menu in the navigation bar, click the "Port Information" submenu, and click the "Port Statistics" secondary submenu, as shown below:

Status >> Port >> Statistics

Port

GE7 ▼

MIB Counter

☒ All
☐ Interface
☐ Etherlike
☐ RMON

Refresh Rate

☐ None
☐ 5 sec
☒ 10 sec
☐ 30 sec

Clear

Interface	
ifInOctets	0
ifInUcastPkts	0
ifInNUcastPkts	0
ifInDiscards	0
ifOutOctets	0
ifOutUcastPkts	0
ifOutNUcastPkts	0
ifOutDiscards	0
ifInMulticastPkts	0
ifInBroadcastPkts	0
ifOutMulticastPkts	0
ifOutBroadcastPkts	0

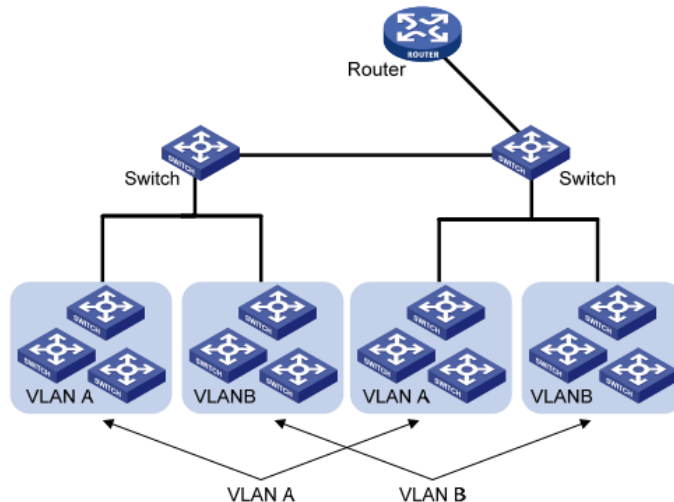
 Description:

Click "Clear" to clear the traffic statistics of the current port and refresh the page.

5. Two-tier configuration

5.1 VLAN configuration

The composition of VLANs is not restricted by physical location, so hosts in the same VLAN do not need to be placed in the same physical space. As shown in the figure below, VLAN divides a physical LAN into multiple logical LANs, and each VLAN is a broadcast domain. Messages can be exchanged between hosts in a VLAN through the traditional Ethernet communication method. If communication between hosts in different VLANs is required, it must be achieved through network layer devices such as routers or layer three switches.



Compared with traditional Ethernet, VLAN has the following advantages:

Control the scope of the broadcast domain: The broadcast messages in the LAN are restricted to one VLAN, which saves bandwidth and improves network processing capabilities.

Enhanced LAN security: Because packets are separated by broadcast domains divided by VLANs at the data link layer, the hosts in each VLAN cannot communicate directly, and the packets need to be processed by network layer devices such as routers or layer three switches. Layer three forwarding.

Flexible creation of virtual workgroups: VLANs can be used to create virtual workgroups across the physical network. When the user's physical location moves within the virtual workgroup, the network can be accessed normally without changing the network configuration.

This managed switch supports 802.1Q VLAN, protocol-based VLAN, MAC-based VLAN, and port-based VLAN. In the default configuration, the VLAN is in 802.1Q VLAN mode.

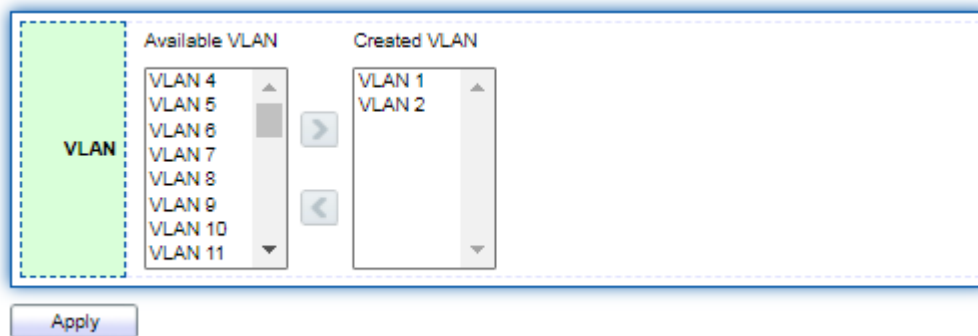
The principle of port-based VLAN is that VLANs are divided according to the interface numbers of switching devices. The network administrator configures a different PVID for each interface of the switch, that is, the VLAN to which an interface belongs by default. When a data frame enters the switch interface, if there is no VLAN tag and PVID is configured on the interface, then the data frame will be marked with the PVID of the interface. If the incoming frame already has a VLAN tag, the switch will not add a VLAN tag, even if the interface has been configured with PVID.

The processing of VLAN frames is determined by the interface type. The advantage is that it is simple to define members. The disadvantage is that the member moves need to reconfigure VLAN.

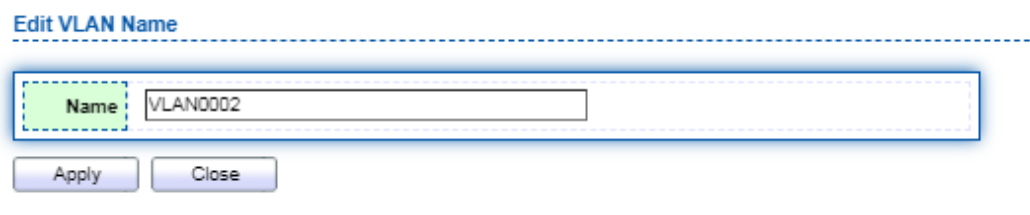
a. New VLAN operation steps:

1. Click the "VLAN Function" menu in the navigation tree, click the "VLAN Configuration" submenu,

click the "Create VLAN" secondary submenu, enter the "Create VLAN" interface, select the VLAN name in the valid VLAN box, and click Right arrow, move to the Create VLAN box (up to 256 VLANs can be created), click Apply to save the effect, as shown in the following figure:



2. After the VLAN is created, the VLAN will be displayed in the VLAN table, select the VLAN that needs to be modified, and click the modify button to enter the VLAN modification page, as shown below:



The meaning of the interface information is shown in the table below.

Configuration item	Description
VLAN ID	Required. Specify the VLAN ID number to be added. The value range is 1 to 4094. Such as: 1-3,5,7,9. Among them, VLAN 1 is the default, and VLAN 1 will not be recreated when it is created.
Name	Optionally, the specific description of VLAN can be modified as needed.

b. Add the current port to the designated VLAN operation steps:

There are two ways to add a port to a VLAN. One is to add multiple ports under one VLAN, and the other is to add one port to multiple VLANs. Because of the different purposes, these two operation modes are implemented in two configuration modes.

Add multiple ports under one VLAN:

1. Click the "VLAN Function" menu in the navigation tree, click the "VLAN Configuration" submenu, and click the "Set VLAN" secondary submenu to enter the VLAN configuration interface. At this time, select the VLAN ID that needs to be configured through the upper left corner of the interface ID.

Then click operation to configure the port information in the VLAN, as shown in the following figure:

VLAN Configuration Table

VLAN [VLAN0052 ▼]

Entry	Port	Mode	Membership			PVID	Forbidden
1	GE1	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
2	GE2	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
3	GE3	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
4	GE4	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
5	GE5	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
6	GE6	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
7	GE7	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
8	GE8	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
9	GE9	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
10	GE10	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
11	GE11	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
12	GE12	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
13	GE13	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
14	GE14	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
15	GE15	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
16	GE16	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
17	GE17	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
18	GE18	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
19	GE19	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
20	GE20	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
21	GE21	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
22	GE22	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
23	GE23	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
24	GE24	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
25	GE25	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
26	GE26	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
27	GE27	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
28	GE28	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
29	LA01	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
30	LA02	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
31	LA03	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
32	LA04	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
33	LA05	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
34	LA06	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
35	LA07	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐
36	LA08	Trunk	☒ Excluded	☐ Tagged	☐ Untagged	☐	☐

Apply

The meaning of the interface information is shown in the table below.

Configuration item	Description
VLAN	VLAN ID to be configured
member	Member role information of ports in this VLAN: Excluded: The port does not belong to this VLAN Tagged: The port is a tagged member of this VLAN Untagged: The port is an Untagged member of this VLAN
PVID	Whether this VLAN is the PVID of the port
Forbidden	Whether the port is forbidden to forward this VLAN packet

Add a port to multiple VLANs:

1. Click the "VLAN Function" menu in the navigation tree, click the "VLAN Configuration" submenu, click the "Member Configuration" secondary submenu, enter the member configuration interface, select the port that needs to be configured, and click Modify to perform the port configuration VLAN attribute configuration:

Edit Port Setting

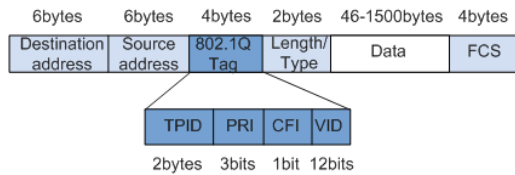
The meaning of the information is shown in the table below.

The meaning of the information is shown in the table below.	Description
port	Port number to be configured
mode	The current VLAN mode of the port, modify in the port settings: Hybrid: Hybrid mode, this mode port can belong to multiple VLAN tagged ports and multiple VLAN untagged ports Access: In this mode, the port can only belong to one VLAN member Trunk: In this mode, the port only belongs to the untagged members of PVID, and can belong to the tagged members of multiple VLANs.
member	The VLAN ID this port belongs to and the attributes in the VLAN: Forbidden: Prohibit forwarding this VLAN packet Excluded: Does not belong to this VLAN Tagged: Tagged members of the VLAN Untagged: Untagged member of VLAN PVID: Whether this VLAN is the PVLAN of the port

c. Introduction to 802.1Q

Trunk configuration, Trunk type interface is used to connect other switch equipment, it is mainly connected to trunk link. The Trunk interface allows frames from multiple VLANs to pass. The encapsulation protocol of the Trunk link is IEEE 802.1q. IEEE 802.1q is the official standard for virtual bridged LANs. The Ethernet frame format has been modified, and a 4-byte 802.1q Tag is added between the source MAC address field and the protocol type field.

802.1q frame format



Introduction to the meaning of each field of the 802.1Q Tag

Field	length	name	Parsing
TPID	2bytes	Tag Protocol Identifier(Tag Protocol Identifier), which indicates the frame type.	When the value is 0x8100, it indicates an 802.1q Tag frame. If a device that does not support 802.1q receives such a frame, it will discard it.
PRI	3bits	Priority indicates the priority of the frame.	The value ranges from 0 to 7. The larger the value, the higher the priority. It is used to send data frames with higher priority when the switch is blocked.
CFI	1bit	Canonical Format Indicator(Standard format indicator), indicating whether the MAC address is in the classic format.	A CFI of 0 indicates a classic format, and a CFI of 1 indicates a non-classical format. For compatibility with Ethernet and token ring networks. In Ethernet, the value of CFI is 0.
VID	12bits	VLAN ID indicates the VLAN to which the frame belongs.	The VLAN ID ranges from 0 to 4095. Since 0 and 4095 are reserved for the protocol, the valid range of VLAN ID is 1 to 4094.

Each packet sent by a switch that supports the 802.1q protocol will contain a VLAN ID to indicate which VLAN the switch belongs to. Therefore, in a VLAN switching network, the Ethernet frame has the following two forms:

Tagged frame: Frame with 4-byte 802.1q Tag added

Untagged frame: the original frame without a 4-byte 802.1q tag

Trunk type interface is used to connect other switch equipment, it is mainly connected to trunk link. The Trunk interface allows frames from multiple VLANs to pass.

d. Trunk port configuration steps:

1. Click the "VLAN Function" menu in the navigation tree, click the "VLAN Configuration" submenu, click the "Port Configuration" secondary submenu, enter the port configuration interface, select the port that needs to be configured, and click Modify to perform the port configuration VLAN attribute configuration:

Port Setting Table

Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
☐	1 GE1	Trunk	1	All	Enabled	Disabled	0x8100
☐	2 GE2	Trunk	1	All	Enabled	Disabled	0x8100
☐	3 GE3	Trunk	1	All	Enabled	Disabled	0x8100
☐	4 GE4	Trunk	1	All	Enabled	Disabled	0x8100
☐	5 GE5	Trunk	1	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
☐	9 GE9	Trunk	1	All	Enabled	Disabled	0x8100
☐	10 GE10	Trunk	1	All	Enabled	Disabled	0x8100
☐	11 GE11	Trunk	1	All	Enabled	Disabled	0x8100
☐	12 GE12	Trunk	1	All	Enabled	Disabled	0x8100
☐	13 GE13	Trunk	1	All	Enabled	Disabled	0x8100
☐	14 GE14	Trunk	1	All	Enabled	Disabled	0x8100
☐	15 GE15	Trunk	1	All	Enabled	Disabled	0x8100
☐	16 GE16	Trunk	1	All	Enabled	Disabled	0x8100
☐	17 GE17	Trunk	1	All	Enabled	Disabled	0x8100
☐	18 GE18	Trunk	1	All	Enabled	Disabled	0x8100
☐	19 GE19	Trunk	1	All	Enabled	Disabled	0x8100
☐	20 GE20	Trunk	1	All	Enabled	Disabled	0x8100
☐	21 GE21	Trunk	1	All	Enabled	Disabled	0x8100
☐	22 GE22	Trunk	1	All	Enabled	Disabled	0x8100
☐	23 GE23	Trunk	1	All	Enabled	Disabled	0x8100
☐	24 GE24	Trunk	1	All	Enabled	Disabled	0x8100
☐	25 GE25	Trunk	1	All	Enabled	Disabled	0x8100
☐	26 GE26	Trunk	1	All	Enabled	Disabled	0x8100
☐	27 GE27	Trunk	1	All	Enabled	Disabled	0x8100
☐	28 GE28	Trunk	1	All	Enabled	Disabled	0x8100
☐	29 LA01	Trunk	1	All	Enabled	Disabled	0x8100
☐	30 LA02	Trunk	1	All	Enabled	Disabled	0x8100
☐	31 LA03	Trunk	1	All	Enabled	Disabled	0x8100
☐	32 LA04	Trunk	1	All	Enabled	Disabled	0x8100
☐	33 LA05	Trunk	1	All	Enabled	Disabled	0x8100
☐	34 LA06	Trunk	1	All	Enabled	Disabled	0x8100
☐	35 LA07	Trunk	1	All	Enabled	Disabled	0x8100
☐	36 LA08	Trunk	1	All	Enabled	Disabled	0x8100

Edit Port Setting

Port

GE4-GE8

Mode

☒ Hybrid
☐ Access
☐ Trunk
☐ Tunnel

PVID

(1 - 4094)

Accept Frame Type

☒ All
☐ Tag Only
☐ Untag Only

Ingress Filtering

☒ Enable

Uplink

☒ Enable

TPID

0x8100 ▼

Apply

Close

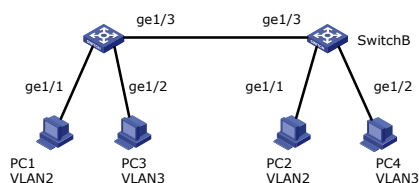
The meaning of the interface information is shown in the table below.

Configuration item	Description
port	Port number to be configured

mode	The current VLAN mode of the port, modify in the port settings: Hybrid: Hybrid mode, this mode port can belong to multiple VLAN tagged ports and multiple VLAN untagged ports Access: In this mode, the port can only belong to one VLAN member Trunk: In this mode, the port only belongs to the untagged members of PVID, and can belong to the tagged members of multiple VLANs.
PVID	Port PVLAN
Accept Frame Type	Types of packets received by the port: All: All messages Tag Only: Only receive tagged packets Untag Only: Only Untagged packets are received
Ingress Filtering	Ingress filtering function switch, whether to filter VLAN packets that do not contain this port
Uplink	Whether it is in up mode
TPID	VLAN Tag identification number

Configuration example

In order for the link between SwitchA and SwitchB to support both user communication in VLAN 2 and user communication in VLAN 3, the connection interface needs to be configured to join two VLANs at the same time. That is, the Ethernet interface ge1/3 of SwitchA and the Ethernet interface ge1/3 of SwitchB should be added to VLAN2 and VLAN3 at the same time.



Steps:

Create VLAN2 and VLAN3 on SwitchA and SwitchB respectively, and add GE1 to VLAN2, GE2 to VLAN3, set GE3 to trunk working mode, and add to VLAN2 and VLAN3 at the same time.

5.2 Mac-vlan

The principle of MAC-based VLAN is to divide VLAN according to the MAC address of the computer network card. The network administrator successfully configures the MAC address and VLAN ID mapping table. If the switch receives an untagged (without VLAN tag) frame, the VLAN ID is added according to the table.

The advantage is: when the physical location of the end user changes, there is no need to reconfigure the VLAN. Improve the safety of end users

Completeness and flexibility of access. The disadvantage is: it is only applicable to scenarios where the network card is not frequently changed and the network environment is relatively simple, and all members in the network need to be defined in advance.

Steps:

1. Click the "VLAN function" menu in the navigation tree, click the "MAC VLAN configuration" submenu, click the "MAC group configuration" secondary submenu, enter the MAC group configuration interface, click the Add button to add a new MAC group, As shown below:

MAC Group Table

Showing 1 to 1 of 1 entries

Group ID	MAC Address	Mask
1	00:22:00:22:00:22	24

Add Edit Delete

Add MAC Group

Group ID: 2 (1 - 2147483647)

MAC Address: 00:22:00:22:00:22

Mask: 48 (0 - 48)

Apply Close

The meaning of the interface information is shown in the table below.

Configuration item	Description
Group ID	MAC VLAN group ID
MAC address	Need to bind the MAC address of the VLAN
Mask	Used to indicate the MAC address end, exactly match the MAC address and fill in 48. Others have the same effect as the IP address mask

Here is an example to illustrate that a company has high requirements for information security, requiring only the company's PC to access the company network. As shown in the figure, the interface GE1 of the Switch is connected to the upstream interface of SwitchA. The downstream interfaces of SwitchA are connected to PC1, PC2, and PC3 respectively. PC1, PC2, and PC3 are required to be able to access the company network through SwitchA and Switch, but cannot be accessed if they are replaced with other PCs.

Configuration idea: Use the following idea to configure VLAN division based on MAC address:

1. Create the relevant VLAN.
2. Configure each Ethernet interface to join the VLAN in the correct way.
3. Configure the MAC addresses of PC1, PC2, and PC3 to associate with the VLAN.

Data preparation: To complete this configuration example, you need to prepare the following data:

Set the PVID of GE1 to 100 on the Switch. ☐

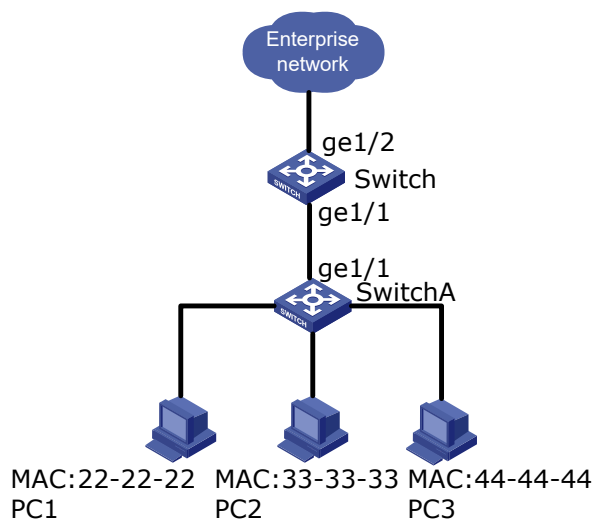
Configure interface GE1 on the Switch to join VLAN 10 in untagged mode.

Configure interface GE2 on the Switch to join VLAN 10 in tagged mode.

The interfaces on SwitchA use the default configuration, that is, all interfaces are added to VLAN 1 in untagged mode.

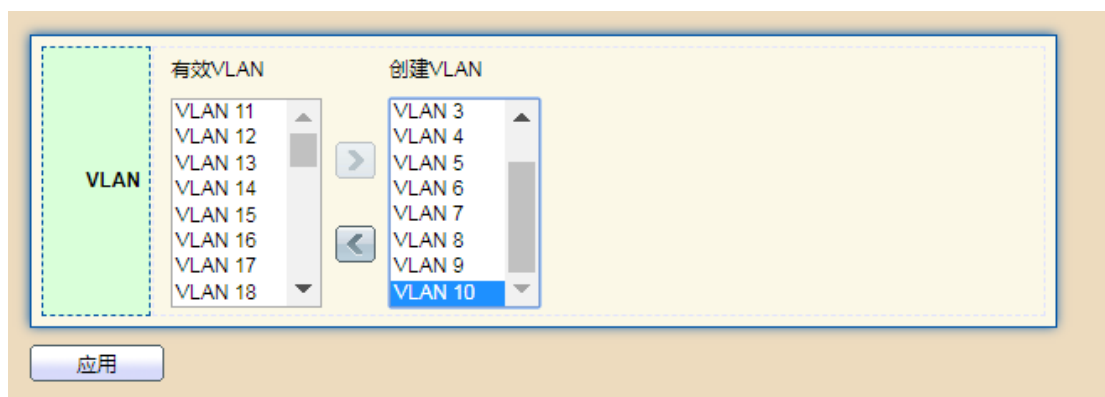
Obtain the MAC addresses of PC1, PC2, and PC3, and configure the MAC addresses to associate with VLAN 10.

Networking diagram for configuring VLAN division based on MAC address



Steps:

1. Create a VLAN and determine the VLAN to which the employee belongs. Click the "VLAN Function" menu in the navigation tree, click the "VLAN Configuration" submenu, click the "Create VLAN" secondary submenu, select VLAN10, add to the create VLAN list to the right, and click Apply to take effect:



2. Configure the switch Ethernet interface GE1 mode as Hybrid, the port PVID is 100, the port belongs to the untagged member of VLAN 10, configure the Switch Ethernet interface GE2 mode as Trunk, and add the port to the VLAN 10 tagged member list.

Port Setting Table							
Entry	Port	Mode	PVID	Accept Frame Type	Ingress Filtering	Uplink	TPID
1	GE1	Hybrid	1	All	Enabled	Disabled	0x8100
2	GE2	Trunk	1	All	Enabled	Disabled	0x8100

成员列表

编号	端口	模式	管理VLAN	Operational VLAN
1	GE1	Hybrid	1U, 10U, 100P	1U, 10U, 100P
2	GE2	Trunk	1UP, 10T	1UP, 10T
3	GE3	Trunk	1UP	1UP

3. The interfaces on SwitchA use the default configuration, that is, all interfaces are added to VLAN 1 in an untagged manner. Configure the MAC addresses of PC1, PC2, and PC3 to associate with VLAN 10. Click the "VLAN function" menu in the navigation tree, click the "MAC VLAN configuration" submenu, click the "MAC group configuration" secondary submenu, enter the MAC group configuration interface, enter PC1 (0022-0022-0022), PC2 respectively (0033-0033-0033), PC3 (0044-0044-0044) MAC address, the mask is 48-bit exact match, as shown in the figure below.

MAC组表

显示: All 条目 Showing 1 to 3 of 3 entries

组ID	MAC地址	掩码
1	00:22:00:22:00:22	48
2	00:33:00:33:00:33	48
3	00:44:00:44:00:44	48

添加 修改 删除 First Previous 1 Next Last

4. Click the "VLAN function" menu in the navigation tree, click the "MAC VLAN configuration" submenu, click the "MAC group binding" secondary submenu, enter the MAC group binding interface, click Add, select the port (only is a Hybrid port), select the binding MAC group ID, specify the binding VLAN ID, and click Apply to complete the configuration.

MAC组绑定表

显示: All 条目 Showing 1 to 3 of 3 entries

端口	组ID	VLAN
GE1	1	10
GE1	2	10
GE1	3	10

添加 修改 删除 First Previous 1 Next Last

5. Check the configuration results

PC1, PC2, and PC3 can access the company network, but cannot be accessed if they are replaced by other PCs from outsiders.

5.3 protocol-vlan

VLANs are divided based on protocols. The principle is to assign different VLAN IDs to packets according to the protocol (family) type and encapsulation format of the packets received by the interface.

The network administrator needs to configure the mapping table between the protocol domain and the VLAN ID in the Ethernet frame. If the received frame is an untagged (without VLAN tag) frame, the VLAN ID is added according to this table. The advantage is: VLAN is divided based on the protocol, and the service type provided in the network is bound to the VLAN, which is convenient for management and maintenance. The disadvantage is that the initial configuration of the mapping table of all protocol types and VLAN IDs in the network is required. Need to analyze the address format of various protocols and

Corresponding conversion consumes more resources of the switch and has a slight disadvantage in speed.

Steps:

1. Click the "VLAN Function> Protocol VLAN Configuration> Protocol Group Configuration" menu in the navigation tree to enter the protocol VLAN group configuration interface, as shown in the figure below.

Protocol Group Table

Showing [All] entries Showing 1 to 1 of 1 entries

Group ID	Frame Type	Protocol Value
1	Ethernet_II	0x8888

Add Edit Delete

Add Protocol Group

Group ID

2

Frame Type

Ethernet_II

Protocol Value

0x

(0x800 ~ 0xFFFFE)

Apply

Close

The meaning of the interface information is shown in the table below.

Configuration item	Description
Group ID	Protocol VLAN Group
Message type	Frame types are ether2, llc, rfc-1042
Agreement value	The protocol value can be optional from 0x600~0xFFFFE

2. Fill in the corresponding configuration items.
3. Click "Apply" to complete the configuration.

Protocol Group Table

Showing [All] entries Showing 1 to 2 of 2 entries

Group ID	Frame Type	Protocol Value
1	Ethernet_II	0x8888
2	RFC_1042	0x8889

Add Edit Delete

4. Click the "VLAN Function> Protocol VLAN Configuration> Protocol Group Binding" menu in the navigation tree, and bind the configured protocol number, port number, and VLANID to make the protocol VLAN configuration effective, as shown in the figure below:

协议组绑定表

显示 [All] 条目 Showing 1 to 1 of 1 entries

端口	组ID	VLAN
GE1	1	10

添加 修改 删除

First Previous 1 Next Last

添加协议组绑定

端口

有效端口

GE1

已选端口

注意: 仅VLAN模式为Hybrid的端口可以匹配协议VLAN

组ID

1

VLAN

(1 - 4094)

应用

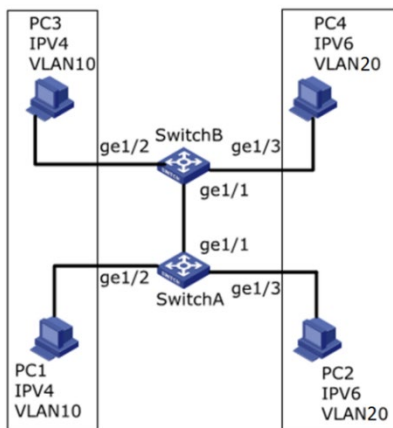
关闭

Description:

To set the matching protocol IPv4 and IPv6, you need to set the ARP protocol at the same time.

Let's take an example to illustrate. As shown in the figure below, PC1 and PC3 can communicate with each other. The communication protocol adopts IPv4, and the IPv4 protocol is bound to VLAN10. PC2 and PC4 can communicate with each other, the communication protocol adopts IPv6, and the IPv6 protocol is bound to VLAN20.

Network diagram of VLAN based on protocol division



Steps:

1. Create a VLAN and determine the VLAN to which each service belongs. Click the "Layer 2 Configuration> VLAN Configuration> VLAN Configuration" menu in the navigation tree to enter the "VLAN Configuration" interface, create vlan10, enter the value 10 for the Vlan' ID, and enter IPV4 for the description. Create vlan20, enter the value 20 for Vlan' ID, and enter IPv6 for the description. Select Flood-unknown and click "Add" to complete the configuration, as shown in the figure below.

Vlan ID	描述	未知组播	
1		Flood-unknown	
10	IPv4	Flood-unknown	删除
20	IPv6	Flood-unknown	删除

2. Configure the Ethernet interfaces ge1/2 and ge1/3 of SwitchA to join the ports that need to be connected in untag mode to join the VLAN. Click the "Layer 2 Configuration> VLAN Configuration> TRUNK Configuration" menu in the navigation tree, enter the "TRUNK Configuration" interface, enter Vlan ID "10", and select port ge1/2 in the "Untag Port List". Similarly, enter the "TRUNK configuration" interface, enter Vlan ID "20", and select port ge1/3 in the "Untag port list". Click "Add" to complete the configuration, as shown in the figure below.

PVLAN配置
TRUNK配置
TRANSLATE配置
VLAN配置

设置Vlan

Vlan ID 范围: 1-4094. 端口将会自动转换为Trunk模式.

Untag 端口列表

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

Tag 端口列表

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

[添加](#)
[删除](#)

VID	Untag 端口列表	Tag 端口列表
1	ge1/1 ge1/2 ge1/3 ge1/4 ge1/5 ge1/6 ge1/7 ge1/8 ge1/9 ge1/10 ge1/11 ge1/12 ge1/13 ge1/14 ge1/15 ge1/16 ge1/17 ge1/18 ge1/19 ge1/20 ge1/21 ge1/22 ge1/23 ge1/24 ge1/25 ge1/26 ge1/27 ge1/28	
10	ge1/2	
20	ge1/3	

添加成功

3. Configure the SwitchB Ethernet interfaces ge1/2 and ge1/3 to join the ports that need to be connected in the untag mode to join the VLAN. The operation is the same as 2.

4. Configure interface ge1/1 on SwitchA to join VLAN 10 and VLAN 20 in tagged mode. Click the "Layer 2 Configuration> VLAN Configuration> TRUNK Configuration" menu in the navigation tree, enter the "TRUNK Configuration" interface, enter Vlan ID "10", select port ge1/1 in the "Tag Port List", and click "Add". In the same way, enter the "TRUNK Configuration" interface, enter the Vlan ID "20", select the port ge1/1 in the "Tag Port List", and click "Add" to complete the configuration, as shown in the figure below.

4

PVLAN配置 TRUNK配置 TRANSLATE配置 VLAN配置

设置Vlan

Vlan ID 范围: 1-4094. 端口将会自动转换为Trunk模式.

Untag 端口列表

Tag 端口列表

VID	Untag 端口列表	Tag 端口列表
1	ge1/1 ge1/2 ge1/3 ge1/4 ge1/5 ge1/6 ge1/7 ge1/8 ge1/9 ge1/10 ge1/11 ge1/12 ge1/13 ge1/14 ge1/15 ge1/16 ge1/17 ge1/18 ge1/19 ge1/20 ge1/21 ge1/22 ge1/23 ge1/24 ge1/25 ge1/26 ge1/27 ge1/28	
10	ge1/2	ge1/1
20	ge1/3	ge1/1

添加成功

5. Associate the protocol and VLAN to assign different VLAN IDs to the message according to the protocol (family) type of the message received by the interface, click the "Layer 2 Configuration>Protocol-vlan" menu in the navigation tree, and enter the "protocol-vlan" interface, enter the corresponding values, bind vlan10 to ipv4 and vlan20 to ipv6, and click "Add". Complete the configuration as shown in the figure below.

序号	端口	帧类型	以太网类型	Vlan Id	
1	ge1/2	ether2	arp	10	删除
2	ge1/2	ether2	ip	10	删除
3	ge1/3	ether2	arp	20	删除
4	ge1/3	ether2	ip	20	删除

共 4 条 每页 20 条

1/1页

5.4 Voice vlan

The traditional processing method to improve the priority of voice data transmission is to use ACL (Access Control List) to distinguish voice data, and to use QoS (Quality of Service) to ensure transmission quality. In order to simplify user configuration and manage the transmission of voice streams more conveniently, the Voice VLAN feature is proposed. The voice VLAN-enabled interface determines whether the data stream is a voice data stream based on the source MAC address field in the data stream entering the interface. A packet whose source MAC address matches the OUI (Organizationally Unique Identifier) address of a voice device set by the system is considered to be a voice data stream. The interface that receives the voice data stream will automatically be added to the Voice VLAN for transmission. This simplifies the user configuration and realizes the user's convenient management of voice data.

OUI address of the Voice VLAN

The OUI address represents a MAC address segment. The 48-bit MAC address and the corresponding bits of the mask can be ANDed to determine the OUI address. The number of bits that the MAC address of the access device matches with the OUI address is determined by the length of all "1"s in the mask. For example, if the MAC address is 1-1-1 and the mask is FFFF-FF00-0000, then the result of the AND operation between the MAC address and its corresponding mask bit is the OUI address 0001-0000-0000.

As long as the first 24 bits of the MAC address of the access device match the first 24 bits of the OUI address, the interface that enables the Voice VLAN function will consider this data stream to be a voice data stream and the connected device is a voice device.

Voice VLAN is a VLAN that divides the user's voice data flow. The user creates a Voice VLAN and

adds the interface connecting the voice device to the Voice VLAN, so that the voice data stream is concentrated in the Voice VLAN for transmission.

There are often both voice data and non-voice data traffic at the same time in the network. Voice data needs to have a higher priority than other service data during transmission to reduce possible delay and packet loss during transmission.

1. Click the "VLAN Function> Voice vlan> Function Configuration" menu in the navigation tree to enter the voice VLAN configuration interface, as shown in the figure below.

State

VLAN

CoS / 802.1p
Remarking

Aging Time

☐ Enable

None

☐ Enable

8

1440

Min (30 - 65536, default 1440)

Apply

Port Setting Table

Entry	Port	State	Mode	QoS Policy	
☐	1	GE1	Disabled	Auto	Voice Packet
☐	2	GE2	Disabled	Auto	Voice Packet
☐	3	GE3	Disabled	Auto	Voice Packet
☐	4	GE4	Disabled	Auto	Voice Packet
☐	5	GE5	Disabled	Auto	Voice Packet
☐	6	GE6	Disabled	Auto	Voice Packet
☐	7	GE7	Disabled	Auto	Voice Packet
☐	8	GE8	Disabled	Auto	Voice Packet
☐	9	GE9	Disabled	Auto	Voice Packet
☐	10	GE10	Disabled	Auto	Voice Packet
☐	11	GE11	Disabled	Auto	Voice Packet
☐	12	GE12	Disabled	Auto	Voice Packet
☐	13	GE13	Disabled	Auto	Voice Packet
☐	14	GE14	Disabled	Auto	Voice Packet
☐	15	GE15	Disabled	Auto	Voice Packet
☐	16	GE16	Disabled	Auto	Voice Packet
☐	17	GE17	Disabled	Auto	Voice Packet
☐	18	GE18	Disabled	Auto	Voice Packet
☐	19	GE19	Disabled	Auto	Voice Packet
☐	20	GE20	Disabled	Auto	Voice Packet
☐	21	GE21	Disabled	Auto	Voice Packet
☐	22	GE22	Disabled	Auto	Voice Packet
☐	23	GE23	Disabled	Auto	Voice Packet
☐	24	GE24	Disabled	Auto	Voice Packet
☐	25	GE25	Disabled	Auto	Voice Packet
☐	26	GE26	Disabled	Auto	Voice Packet
☐	27	GE27	Disabled	Auto	Voice Packet
☐	28	GE28	Disabled	Auto	Voice Packet
☐	29	LAG1	Disabled	Auto	Voice Packet
☐	30	LAG2	Disabled	Auto	Voice Packet
☐	31	LAG3	Disabled	Auto	Voice Packet
☐	32	LAG4	Disabled	Auto	Voice Packet
☐	33	LAG5	Disabled	Auto	Voice Packet
☐	34	LAG6	Disabled	Auto	Voice Packet
☐	35	LAG7	Disabled	Auto	Voice Packet
☐	36	LAG8	Disabled	Auto	Voice Packet

Edit

Edit Port Setting

Port

State

Mode

QoS Policy

GE1

☐ Enable

☒ Auto

☐ Manual

☒ Voice Packet

☐ All

Apply

Close

The meaning of the interface information is shown in the table below.

Configuration item	Description
status	Enable Voice VLAN by tick
VLAN	Specify the VLAN ID number to be added. The value range is 1 to 4094. Such as: 1-3,5,7,9. Among them, VLAN 1 is the default. Other VLANs must exist and join the ports that need to be linked in an untag mode.
CoS re-marking	Check whether you need to redefine the priority of Voice VLAN packets.
Aging time	Entry aging time
port	Voice VLAN enabled port
mode	Port Voice VLAN operation mode, divided into automatic mode and manual mode
QoS strategy	Select which kind of packets QoS takes effect

2. Click the "VLAN Function> Voice vlan> Voice OUI Configuration" menu in the navigation tree to enter the OUI address table configuration interface of the voice VLAN. Configure the OUI address segment of the Voice VLAN on this page, as shown in the figure below.

Voice OUI Table

Showing All entries Showing 1 to 8 of 8 entries

☐	OUI	Description
☐	00:E0:BB	3COM
☐	00:03:BB	Cisco
☐	00:E0:75	Veritel
☐	00:D0:1E	Pingtel
☐	00:01:E3	Siemens
☐	00:00:B9	NEC/Philips
☐	00:0F:E2	H3C
☐	00:09:0E	Avaya

Add Voice OUI

OUI

:

:

:

Description

3. Fill in the corresponding configuration items.

4. Click "Apply" first to complete the configuration, as shown in the figure below.

端口配置表

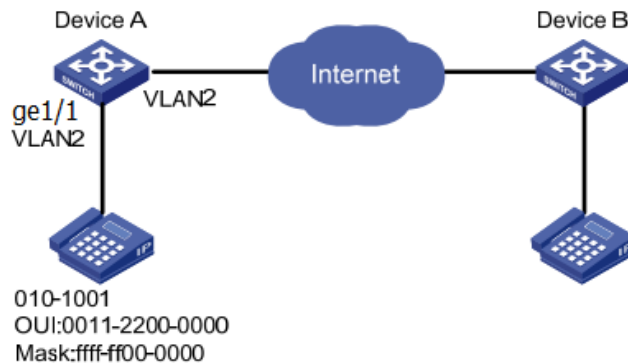
Q

☐	编号	端口	状态	模式	QoS策略
☐	1	GE1	禁用	自动	Voice报文
☐	2	GE2	禁用	自动	Voice报文
☐	3	GE3	禁用	自动	Voice报文
☐	4	GE4	禁用	自动	Voice报文
☐	5	GE5	启用	手工	Voice报文
☐	6	GE6	禁用	自动	Voice报文

Let's take an example to illustrate. By configuring the Voice VLAN in manual mode, the port

connected to the IP phone can be manually controlled to join/exit the Voice VLAN, and the voice stream is transmitted in the VLAN. Create VLAN2 as Voice VLAN, make it work in Voice VLAN security mode, only allow voice

The data passed. The IP phone sends untag voice stream, and the access port is Trunk type port ge1/1. The user needs to set a custom OUI address 0812-f231-05e1, and the mask is ffff-ff00-0000. Network diagram for configuring Voice VLAN in automatic mode



Steps:

1. Create a VLAN and determine the VLAN to which each service belongs. Click the "Layer 2 Configuration> VLAN Configuration> VLAN Configuration" menu in the navigation tree, enter the "VLAN Configuration" interface, create vlan2, select Flood-unknown, and click "Add" to complete the configuration, as shown in the figure below.

Vlan ID	描述	未知组播
1		Flood-unknown
2	Voice VLAN	Flood-unknown

共 2 条 每页 20 条 1/1页 < > Go > >

2. Configure the Switch Ethernet interface ge1/1 to join the port that needs to be connected to the VLAN in untag mode. Click the "Layer 2 Configuration> VLAN Configuration> TRUNK Configuration" menu in the navigation tree, enter the "TRUNK Configuration" interface, enter Vlan ID "2", select port ge1/1 in the "Untag Port List", and click "Add" To complete the configuration, as shown in the figure below.

PVLAN配置 TRUNK配置 TRANSLATE配置 VLAN配置

设置Vlan
Vlan ID 范围: 1-4094. 端口将会自动转换为Trunk模式.

Untag 端口列表

Tag 端口列表

添加 删除

VID	Untag 端口列表	Tag 端口列表
1	ge1/1 ge1/2 ge1/3 ge1/4 ge1/5 ge1/6 ge1/7 ge1/8 ge1/9 ge1/10 ge1/11 ge1/12 ge1/13 ge1/14 ge1/15 ge1/16 ge1/17 ge1/18 ge1/19 ge1/20 ge1/21 ge1/22 ge1/23 ge1/24 ge1/25 ge1/26 ge1/27 ge1/28	
2	ge1/1	

添加成功

3. Click the "Layer 2 Configuration> Voice vlan" menu in the navigation tree, enter the "Voice vlan"

interface, tick Enable voice vlan, enter the Vlan id as 2, click "Settings", enter the MAC address of the language device, 0812-f231-05e1, MAC mask, ffff-ff00-0000, click "Add" to complete the configuration, as shown in the figure below.

Voice vlan

启用voice vlan ☒

Vlan id 范围: 1-4094

设置 取消

Voice vlan MAC

MAC 例如: 0001-0001-0001

MAC mask 例如: ffff-ff00-0000

添加

序号	MAC	MAC mask	
1	0812-f231-05e1	ffff-ff00-0000	删除

刷新

5.5 MAC configuration

The main function of the Ethernet switch is to forward the message at the data link layer, that is, according to the purpose of the message

The MAC address outputs the message to the corresponding port. The MAC address forwarding table is a Layer 2 forwarding table that contains the correspondence between the MAC address and the forwarding port. It is the basis for the Ethernet switch to implement fast forwarding of Layer 2 packets.

The entries in the MAC address forwarding table contain the following information:

- ② Destination MAC address
- ② VLAN ID to which the port belongs
- ② The forwarding port number on this device

When the Ethernet switch forwards packets, according to the MAC address table entry information, the following two forwarding methods are adopted:

② Unicast mode: When the MAC address forwarding table contains an entry corresponding to the destination MAC address of the message,

The switch directly sends the packet from the forwarding port in the entry.

② Broadcast mode: When the switch receives a message with a destination address of all F, or there is no MAC address in the forwarding table

When it contains the table entry corresponding to the destination MAC address of the message, the switch will broadcast the message to the

All ports except the receiving port are forwarded.

5.5.1 MAC configuration

On this page, you can set the MAC address aging time and view the MAC address table information, To adapt to changes in the network, the MAC address table needs to be updated continuously. The automatically generated entries in the MAC address table are not always valid. Each entry has a life cycle. Entries that cannot be refreshed after reaching the life cycle will be deleted. This life cycle is called the aging time. If the record is refreshed before reaching the life cycle, the aging time of the entry is recalculated.

Setting a proper aging time can effectively realize the aging function of the MAC address. The aging time set by the user is too short, which may cause the switch to broadcast a large number of data

packets that cannot find the destination MAC address, which affects the operating performance of the switch.

If the aging time set by the user is too long, the switch may save many outdated MAC address table entries, thereby depleting

The MAC address forwarding table resource prevents the switch from updating the MAC address forwarding table according to network changes.

If the aging time set by the user is too short, the switch may delete valid MAC address entries, reducing forwarding efficiency.

In general, it is recommended to use the default value of 300 seconds for the aging time.

Steps to set the MAC address aging time:

1. Click the "MAC Address Table> Dynamic MAC Address Table" menu in the navigation tree to enter the dynamic MAC address table configuration and display interface:

Aging Time: 300 Sec (10 - 930, default 300)

Apply

Dynamic Address Table

Showing 1 to 41 of 41 entries

VLAN	MAC Address	Port
1	00:ED:4C:24:5F:5C	GE1
1	00:ED:70:45:CC:16	GE1

The meaning of the interface information is as follows

Configuration item	Description
MAC aging time	Enter the MAC aging time

2. Fill in the corresponding configuration items.

3. Click "Apply" to complete the configuration.

The MAC table is used to store the MAC addresses, VLAN numbers, and outbound interface information of other devices learned by the switch. When forwarding data, query the MAC table according to the destination MAC address and VLAN number in the Ethernet frame to quickly locate the outgoing interface of the device.

Steps to view the MAC address table:

1. Click the "System Status> MAC Address Table" menu in the navigation tree to enter the MAC address table display interface, which displays all MAC address information, as shown in the figure below.

MAC地址表

显示 All 条目 Showing 1 to 3 of 3 entries

VLAN	MAC地址	类型	端口
1	00:00:00:11:22:33	管理	CPU
1	00:00:00:11:22:4F	动态	GE26
1	F0:79:59:0C:6A:DE	动态	GE7

清除

刷新

First Previous 1 Next Last

The meaning of the interface information is shown in the table below.

Query item	Description
MAC	Destination MAC address
VLAN	VLAN ID to which the MAC address belongs

port	Outgoing port of packets corresponding to device MAC address
Types of	Dynamic MAC address refers to MAC address table entries that can be aged out according to the aging time configured by the user. The switch can add dynamic MAC address table entries through the MAC address learning mechanism or manually created by the user. Static MAC address refers to the MAC address table entry manually configured by the user and will not be aged. Management MAC address, refers to the device's management interface MAC address

5.5.2 Static MAC

The static entries are manually configured by the user and delivered to each interface board. The entries do not age.

New static MAC address steps

1. Click the "MAC Address Table> Static MAC Address Table" menu in the navigation tree to enter the static MAC address table interface, as shown in the figure below.

The screenshot shows the 'Static Address Table' configuration page. At the top, there's a header 'Static Address Table' and a status bar indicating 'Showing 1 to 1 of 1 entries'. Below this is a table with columns 'VLAN', 'MAC Address', and 'Port'. The table contains one entry: VLAN 1, MAC Address 00:ED:4C:24:5F:5C, and Port GE1. Below the table are buttons for 'Add', 'Edit', and 'Delete'. Below the table is a section titled 'Add Static Address' with a dashed border. Inside this section is a form with three fields: 'MAC Address' (00:00:11:11:22:22), 'VLAN' (10, with a range '(1 - 4094)' shown), and 'Port' (GE1, with a dropdown arrow). Below the form are 'Apply' and 'Close' buttons.

The meaning of the interface information is shown in the table below.

Configuration item	Description
MAC	required. Enter the newly created MAC address. Such as: HH:HH:HH:HH:HH:HH.
VLAN	required. Specify the ID number of the VLAN.
port	required. Select the type of interface and enter the name of the interface. Note: The interface must be a member port of the configured VLAN.

2. Fill in the corresponding configuration items.
3. Click "Apply" to complete the configuration.

5.6 MSTP configuration

In order to perform link backup and improve network reliability in an Ethernet switching network, redundant links are usually used. However, the use of redundant links will cause loops on the

switching network, causing broadcast storms and instability of the MAC address table, which will result in poor user communication quality and even communication interruptions. In order to solve the loop problem in the switching network, the Spanning Tree Protocol (STP) is proposed.

Like the development of many protocols, the Spanning Tree Protocol is constantly updated with the development of the network, from the original STP defined in IEEE 802.1D to the Rapid Spanning Tree Protocol (RSTP) defined in IEEE 802.1W. , And then to the Multiple Spanning Tree Protocol (MSTP) defined in the latest IEEE 802.1S.

Among the spanning tree protocols, MSTP is compatible with RSTP and STP, and RSTP is compatible with STP. The comparison of the three spanning tree protocols is shown in the table.

Comparison of three spanning tree protocols

Spanning Tree Protocol	Features	Application scenario
STP	A loop-free tree is formed to resolve broadcast storms and achieve redundant backup. The convergence rate is slower.	No need to distinguish user or business traffic, all VLANs share a spanning tree.
RSTP	A loop-free tree is formed to resolve broadcast storms and achieve redundant backup. The convergence speed is fast.	
MSTP	A loop-free tree is formed to resolve broadcast storms and achieve redundant backup. The convergence speed is fast. Multiple spanning trees implement load balancing among VLANs, and traffic of different VLANs is forwarded according to different paths.	It is necessary to distinguish user or business traffic and achieve load sharing. Different VLANs forward traffic through different spanning trees, and each spanning tree is independent of each other.

After the Spanning Tree Protocol is deployed in the Ethernet switching network, if a loop occurs in the network, the Spanning Tree Protocol can achieve through topology calculation:

❑ Eliminate loops: Eliminate possible network communication loops in the network by blocking redundant links.

❑ Link backup: When the currently active path fails, the redundant backup link is activated to restore network connectivity.

5.6.1 Global configuration

Provides the function of configuring STP global parameters. In some specific network environments, it is necessary to adjust the STP parameters of some devices in order to achieve the best results.

Steps:

1. Click the "Spanning Tree Protocol> Function Settings" menu in the navigation tree to enter the Spanning Tree Protocol configuration interface, as shown in the following figure:

State	☐ Enable
Operation Mode	☐ STP ☒ RSTP ☐ MSTP
Path Cost	☒ Long ☐ Short
BPDU Handling	☐ Filtering ☒ Flooding
Priority	32768 (0 - 61440, default 32768)
Hello Time	2 Sec (1 - 10, default 2)
Max Age	20 Sec (6 - 40, default 20)
Forward Delay	15 Sec (4 - 30, default 15)
Tx Hold Count	8 (1 - 10, default 8)
Region Name	90:E2:FC:00:00:00
Revision	0 (0 - 65535, default 0)
Max Hop	20 (1 - 40, default 20)
Operational Status	
Bridge Identifier	32768-90:E2:FC:00:00:00
Designated Root Bridge	0-00:00:00:00:00:00
Root Port	N/A
Root Path Cost	0
Topology Change Count	0
Last Topology Change	00/00/00/00

Apply

The meaning of the interface information is shown in the table below.

Configuration item	Description
Turn on	Checked by default, it means that the switch enables Spanning-tree
Operating mode	Supports three spanning tree modes, namely STP, RSTP and MSTP.
Path cost model	Long mode and Short mode
BPDU forwarding method	Indicates the behavior of the device after receiving the BPDU packet and processing the packet
priority	Indicates the priority of the port
Hello Time	Hello packet interval
Max Age	Max Age
Forward Delay	Forward Delay time
domain name	MST domain name. The default value is the MAC address of the main control board of the switch device. The domain name of the switch device is used together with the VLAN mapping table of the MST domain and the revision level of MSTP to determine which domain the switch device can belong to.

2. Fill in the corresponding configuration items.

3. Click "Apply" to complete the configuration

5.6.2 Example configuration

A switching network is divided into multiple domains through MSTP, and multiple spanning trees are formed in each domain, and the spanning trees are independent of each other. Each spanning tree is called a Multiple Spanning Tree Instance (MSTI), and each domain is called an MST Region (MST Region: Multiple Spanning Tree Region).

Description:

The so-called instance is a collection of multiple VLANs. By bundling multiple VLANs into one instance, communication overhead and resource occupancy can be saved. The calculation of the topology of each instance of MSTP is independent of each other, and load balancing can be achieved on these instances. Multiple VLANs with the same topology can be mapped to an instance. The forwarding status of these VLANs on the port depends on the status of the port in the corresponding MSTP instance.

Simply put, it is the mapping of one or more VLANs to a specified MST instance. One or more VLANs can be assigned to a spanning tree instance at a time.

Steps:

1. Click the "Spanning Tree Protocol> Instance Configuration" menu in the navigation tree to enter the instance configuration page, select the MST instance that needs to be configured, and click Modify to enter the modification interface, as shown in the following figure.

MST Instance Table

	MSTI	Priority	Bridge Identifier	Designated Root Bridge	Root Port	Root Path Cost	Remaining Hop	VLAN
☐	0	32768	32768-00-E2-FC-00-00-00-00	0-00-00-00-00-00-00-00	N/A	0	0	1-4094
☐	1	32768	32768-00-E2-FC-00-00-00-00	0-00-00-00-00-00-00-00	N/A	0	0	
☐	2	32768	32768-00-E2-FC-00-00-00-00	0-00-00-00-00-00-00-00	N/A	0	0	
☐	3	32768	32768-00-E2-FC-00-00-00-00	0-00-00-00-00-00-00-00	N/A	0	0	
☐	4	32768	32768-00-E2-FC-00-00-00-00	0-00-00-00-00-00-00-00	N/A	0	0	
☐	5	32768	32768-00-E2-FC-00-00-00-00	0-00-00-00-00-00-00-00	N/A	0	0	
☐	6	32768	32768-00-E2-FC-00-00-00-00	0-00-00-00-00-00-00-00	N/A	0	0	
☐	7	32768	32768-00-E2-FC-00-00-00-00	0-00-00-00-00-00-00-00	N/A	0	0	
☐	8	32768	32768-00-E2-FC-00-00-00-00	0-00-00-00-00-00-00-00	N/A	0	0	
☐	9	32768	32768-00-E2-FC-00-00-00-00	0-00-00-00-00-00-00-00	N/A	0	0	
☐	10	32768	32768-00-E2-FC-00-00-00-00	0-00-00-00-00-00-00-00	N/A	0	0	
☐	11	32768	32768-00-E2-FC-00-00-00-00	0-00-00-00-00-00-00-00	N/A	0	0	
☐	12	32768	32768-00-E2-FC-00-00-00-00	0-00-00-00-00-00-00-00	N/A	0	0	
☐	13	32768	32768-00-E2-FC-00-00-00-00	0-00-00-00-00-00-00-00	N/A	0	0	
☐	14	32768	32768-00-E2-FC-00-00-00-00	0-00-00-00-00-00-00-00	N/A	0	0	
☐	15	32768	32768-00-E2-FC-00-00-00-00	0-00-00-00-00-00-00-00	N/A	0	0	

Edit

Edit MST Instance Setting

The meaning of the interface is shown in the table below

Configuration item	Description
MSTI	Multi-spanning tree instance number, 0~15.
VLAN	VLAN number of instance mapping
priority	Set the priority of the specified instance, which must be a multiple of 4096. Its range is 0 to 65535, and the default value is 32768.
Bridge ID	The bridge ID of the spanning tree instance corresponding to this device, consisting of priority + MAC address
Root bridge ID	The elected root bridge ID of the instance, consisting of priority + MAC address
Root port	Elected instance root port number
Root cost	Path cost from root bridge

2. Fill in the corresponding configuration items.

3. Click "Apply" to complete the configuration, and the result is shown in the figure below.

MST实例配置表

	MSTI	优先级	桥ID	根桥ID	根端口	根花费	Remaining Hop	VLAN
☐	0	32768	32768-00:E0:4C:00:11:1A	32768-00:E0:4C:00:11:1A	N/A	0	20	1-2,5-4094
☐	1	32768	32768-00:E0:4C:00:11:1A	32768-00:E0:4C:00:11:1A	N/A	0	20	3-4
☐	2	32768	32768-00:E0:4C:00:11:1A	32768-00:E0:4C:00:11:1A	N/A	0	20	

5.6.3 Instance Port Configuration

1. Click the "Spanning Tree Protocol> Instance Port Configuration" menu in the navigation tree to

enter the MSTP instance port configuration interface, which lists all the ports included in the device, check the ports that need to be modified, and click the modify button. Enter the detailed configuration interface of the instance port, as shown in the figure below:

MST Port Setting Table

MSTI 0

	Entry	Port	Path Cost	Priority	Port Role	Port State	Mode	Type	Designated Bridge	Designated Port ID	Designated Cost	Remaining Hop
☐	1	GE1	20000	128	Disabled	Forwarding	RSTP	Boundary	0-00:00:00:00:00:00	128-1	0	20
☐	2	GE2	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-2	0	20
☐	3	GE3	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-3	0	20
☐	4	GE4	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-4	0	20
☐	5	GE5	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-5	0	20
☐	6	GE6	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-6	0	20
☐	7	GE7	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-7	0	20
☐	8	GE8	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-8	0	20
☐	9	GE9	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-9	0	20
☐	10	GE10	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-10	0	20
☐	11	GE11	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-11	0	20
☐	12	GE12	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-12	0	20
☐	13	GE13	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-13	0	20
☐	14	GE14	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-14	0	20
☐	15	GE15	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-15	0	20
☐	16	GE16	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-16	0	20
☐	17	GE17	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-17	0	20
☐	18	GE18	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-18	0	20
☐	19	GE19	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-19	0	20
☐	20	GE20	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-20	0	20
☐	21	GE21	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-21	0	20
☐	22	GE22	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-22	0	20
☐	23	GE23	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-23	0	20
☐	24	GE24	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-24	0	20
☐	25	GE25	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-25	0	20
☐	26	GE26	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-26	0	20
☐	27	GE27	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-27	0	20
☐	28	GE28	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-28	0	20
☐	29	LAG1	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-29	0	20
☐	30	LAG2	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-30	0	20
☐	31	LAG3	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-31	0	20
☐	32	LAG4	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-32	0	20
☐	33	LAG5	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-33	0	20
☐	34	LAG6	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-34	0	20
☐	35	LAG7	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-35	0	20
☐	36	LAG8	20000	128	Disabled	Disabled	RSTP	Boundary	0-00:00:00:00:00:00	128-36	0	20

Edit

Edit MST Port Setting

MSTI	0
Port	GE25
Path Cost	0 (0 - 200000000) (0 = Auto)
Priority	128
Port Role	Disabled
Port State	Disabled
Mode	RSTP
Type	Boundary
Designated Bridge	0-00:00:00:00:00:00
Designated Port ID	128-25
Designated Cost	20000
Remaining Hop	20

Apply Close

The meaning of the interface information is shown in the table below.

Configuration item	Description
MSTI	Select the instance to be configured through the drop-down box in the upper left corner
port	The user selects the port to be configured
Path cost	Enter the path cost value of the interface. The value range when using the IEEE 802.1t standard method is 0~200000000
priority	Select the priority of the port. The smaller the value, the higher the priority. The priority of the interface can affect the role of the interface in the specified MSTI. Users can configure different priorities for the same interface on different MSTIs, so that the traffic of different VLANs is forwarded along different physical links to complete the function of VLAN load sharing. Note: When the priority of an interface changes, MSTP will recalculate the role of the interface and perform a state transition.
Port role	Divided into three types of root ports, designated ports, backup ports, and Disabled
Port status	Including three states, Discarding, Forwarding, Disabled
mode	Current Spanning Tree Protocol Mode
Types of	The type of the port in the instance, including boundary ports and internal ports

1. Fill in the corresponding configuration items.

2. Click "Apply" to complete the configuration.

5.6.4 Port configuration

In some specific network environments, it is necessary to adjust the STP parameters of some switch device interfaces in order to achieve the best results.

1. Click the "Spanning Tree Protocol> Port Configuration" menu in the navigation tree to enter the port configuration interface, select the port to be configured and click Modify to enter the detailed modification interface, as shown in the following figure:

Port Setting Table

Entry	Port	State	Path Cost	Priority	BPDU Filter	BPDU Guard	Operational Edge	Operational Point-to-Point	Port Role	Port State	Designated Bridge	Designated Port ID	Designated Cost
☐	1 GE1	Enabled	20000	128	Disabled	Disabled	Disabled	Enabled	Disabled	Forwarding	0-00:00:00:00:00:00	128-1	20000
☐	2 GE2	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-2	20000
☐	3 GE3	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-3	20000
☐	4 GE4	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-4	20000
☐	5 GE5	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-5	20000
☐	6 GE6	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-6	20000
☐	7 GE7	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-7	20000
☐	8 GE8	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-8	20000
☐	9 GE9	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-9	20000
☐	10 GE10	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-10	20000
☐	11 GE11	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-11	20000
☐	12 GE12	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-12	20000
☐	13 GE13	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-13	20000
☐	14 GE14	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-14	20000
☐	15 GE15	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-15	20000
☐	16 GE16	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-16	20000
☐	17 GE17	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-17	20000
☐	18 GE18	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-18	20000
☐	19 GE19	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-19	20000
☐	20 GE20	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-20	20000
☐	21 GE21	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-21	20000
☐	22 GE22	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-22	20000
☐	23 GE23	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-23	20000
☐	24 GE24	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-24	20000
☐	25 GE25	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-25	20000
☐	26 GE26	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-26	20000
☐	27 GE27	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-27	20000
☐	28 GE28	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-28	20000
☐	29 LAG1	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-29	20000
☐	30 LAG2	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-30	20000
☐	31 LAG3	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-31	20000
☐	32 LAG4	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-32	20000
☐	33 LAG5	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-33	20000
☐	34 LAG6	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-34	20000
☐	35 LAG7	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-35	20000
☐	36 LAG8	Enabled	20000	128	Disabled	Disabled	Disabled	Disabled	Disabled	Disabled	0-00:00:00:00:00:00	128-36	20000

Edit Port Setting

Port

GE9

State

☒ Enable

Path Cost

(0 - 200000000) (0 = Auto)

Priority

128 ▼

Edge Port

☐ Enable

BPDU Filter

☐ Enable

BPDU Guard

☐ Enable

Point-to-Point

☒ Auto
☐ Enable
☐ Disable

Port State

Disabled

Designated Bridge

0-00:00:00:00:00:00

Designated Port ID

128-9

Designated Cost

20000

Operational Edge

False

Operational Point-to-Point

False

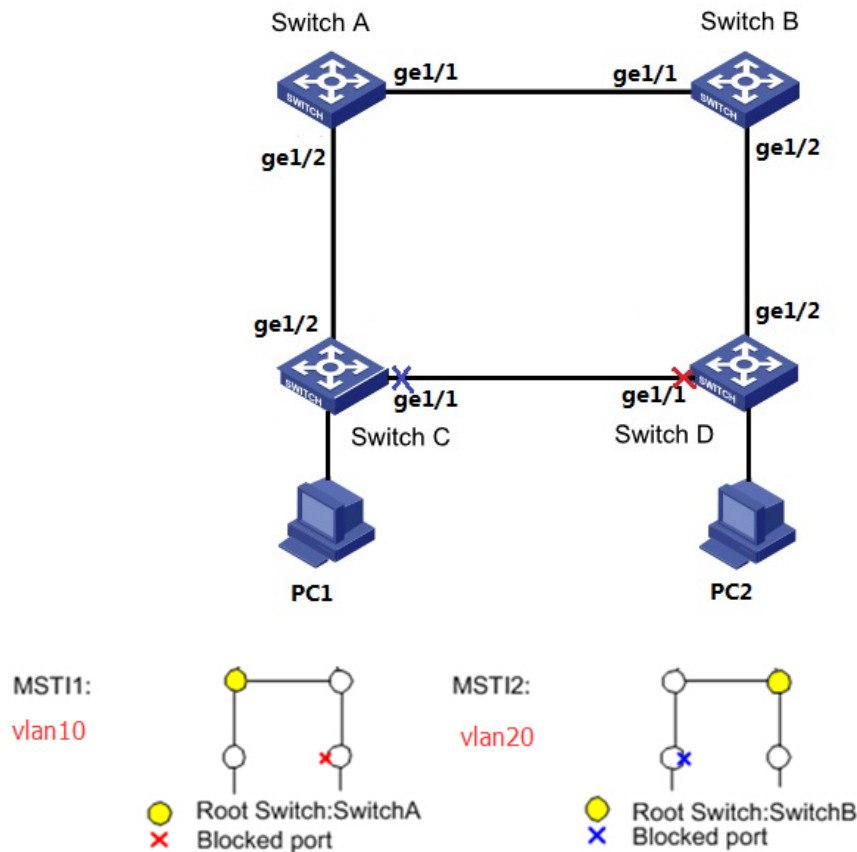
The meaning of the interface information is shown in the table below.

Configuration item	Description
port	Need to configure the port number
status	Whether to enable the Spanning Tree Protocol function
Edge port	The edge port should be directly connected to the user terminal, not another switch or network segment. Edge ports can quickly transition to the forwarding state, because on edge ports, changes in the network topology do not generate loops. By setting a port as an edge port, the spanning tree protocol allows it to quickly transition to the forwarding state. It is recommended to configure the Ethernet ports directly connected to user terminals as edge ports so that they can quickly transition to the forwarding state.
BPDU Filter	Whether to enable the BPDU filtering function.
BPDU Guard	Whether to enable the BPDU protection function. The default is not checked. When the BPDU protection function is enabled on the device, if the interface receives the BPDU, the device shuts down these interfaces and informs the network management system at the same time. The closed interface can only be manually restored by the network manager.
Point-to-Point	Choose on, off and auto. Auto: Indicates that the port is set to the default state of automatically detecting whether it is connected to a point-to-point link. On: Indicates that a specific port is connected to a point-to-point link. Closed: Indicates that the specific port is not connected to the point-to-point link.

1. Fill in the corresponding configuration items.
2. Click "Apply" to complete the configuration.

Example for configuring MSTP function

SwitchA, SwitchB, SwitchC, and SwitchD all run MSTP. To achieve load sharing between VLAN10 and VLAN20, MSTP introduces multiple instances. MSTP can set up a VLAN mapping table to associate VLANs with spanning tree instances. Example 1 maps to VLAN 10 and Example 2 maps to VLAN 20.



Steps:

1. Configure the Layer 2 forwarding function of the devices in the ring network, and create VLAN10 and vlan20 on the switching devices SwitchA, SwitchB, SwitchC and SwitchD. Click the "VLAN Function> VLAN Configuration> Create VLAN" menu in the navigation tree, enter the "Create VLAN" interface, fill in the corresponding configuration, and click "Apply" to complete the configuration, as shown in the following figure.

VLAN

Available VLAN

VLAN 16
VLAN 17
VLAN 18
VLAN 19
VLAN 21
VLAN 22
VLAN 23
VLAN 24

Created VLAN

VLAN 1
VLAN 10
VLAN 20

Apply

VLAN Table

Showing All entries

Showing 1 to 1 of 1 entries

VLAN	Name	Type	VLAN Interface State
1	default	Default	Disabled

Edit

Delete

2. Add the ports in the access loop on the switching equipment to the VLAN. Click the "VLAN

Function> VLAN Configuration> Member Configuration" menu in the navigation tree, enter the "Member Configuration" interface, select the ring port, enter the port setting mode, respectively move VLAN10 and VLAN20 to the right selection box, the attribute is "Tagged" , Click "Apply" to complete the configuration,

Edit Port Setting

Port	GE1
Mode	Trunk
Membership	10 20 1UP ☐ Forbidden ☐ Excluded ☒ Tagged ☐ Untagged ☐ PVID

Apply Close

3. Click the "Spanning Tree Protocol> Function Settings" menu in the navigation tree, enter the "Function Settings", fill in the corresponding configuration, and select the MSTP mode. The interface is as shown in the figure below.

State	☐ Enable
Operation Mode	☐ STP ☐ RSTP ☒ MSTP
Path Cost	☒ Long ☐ Short
BPDU Handling	☐ Filtering ☒ Flooding
Priority	32768 (0 - 61440, default 32768)
Hello Time	2 Sec (1 - 10, default 2)
Max Age	20 Sec (6 - 40, default 20)
Forward Delay	15 Sec (4 - 30, default 15)
Tx Hold Count	6 (1 - 10, default 6)
Region Name	90:E2:FC:00:00:00
Revision	0 (0 - 65535, default 0)
Max Hop	20 (1 - 40, default 20)
Operational Status	
Bridge Identifier	32768-90:E2:FC:00:00:00
Designated Root Bridge	0-00:00:00:00:00:00
Root Port	N/A
Root Path Cost	0
Topology Change Count	0
Last Topology Change	00/00/00/00

Apply

4. Configure the VLAN mapping relationship between instance MSTI1 and MSTI2. Click the

"Spanning Tree Protocol> Instance Settings" menu in the navigation tree, enter the "Instance Settings", fill in the corresponding parameters, and click "Add". The interface is as shown in the figure below.

MST Instance Table

	MSTI	Priority	Bridge Identifier	Designated Root Bridge	Root Port	Root Path Cost	Remaining Hop	VLAN
☐	0	32768	32768-90:E2:FC:00:00:00	0-00:00:00:00:00:00	N/A	0	0	1-4094
☐	1	32768	32768-90:E2:FC:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
☐	2	32768	32770-90:E2:FC:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
☐	3	32768	32771-90:E2:FC:00:00:00	0-00:00:00:00:00:00	N/A	0	0	
☐	4	32768	32772-90:E2:FC:00:00:00	0-00:00:00:00:00:00	N/A	0	0	



note:

When configuring SwitchA, change the priority of MSTI1 to 0 and the priority of MSTI2 to 4096. When configuring SwitchB, change the priority of MSTI1 to 4096 and the priority of MSTI2 to 0. The configuration method is the same as that of SwitchA, and will not be repeated here. Priority must be a multiple of 4096

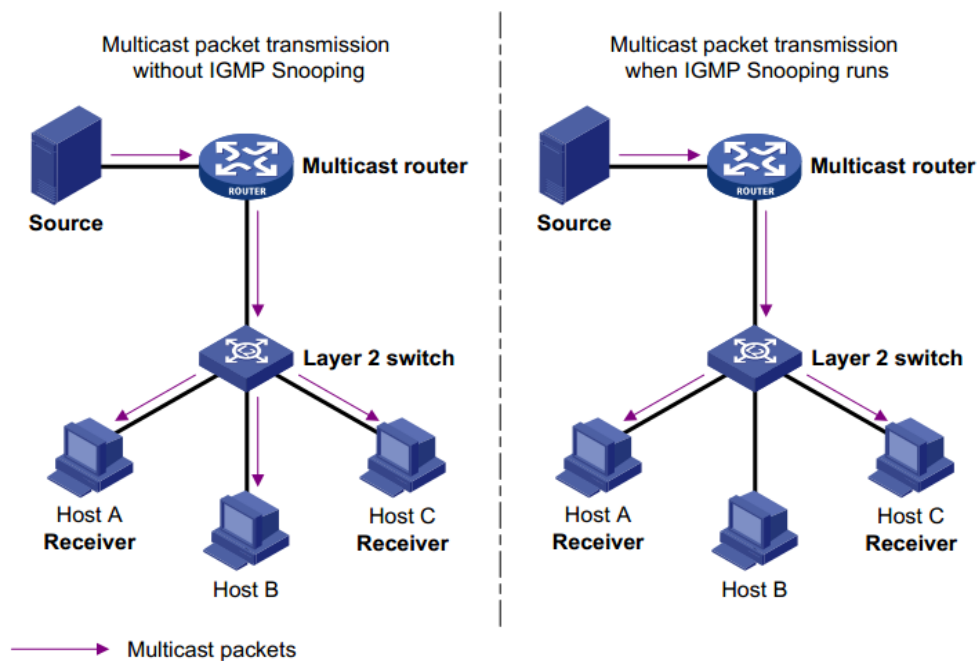
5. In the domain, configure the root bridge and backup root bridge of MSTI1 and MSTI2, configure SwitchB as the root bridge of MSTI2, and configure SwitchB as the backup root bridge of MSTI1. The operation steps are the same as 5, so I won't repeat them.
6. After the above configuration, the network is pruned into a tree shape to achieve the purpose of eliminating loops.

5.7 IGMP-snooping configuration

IGMP Snooping (Internet Group Management Protocol Snooping) is a multicast restriction mechanism running on Layer 2 devices to manage and control multicast groups.

The Layer 2 device running IGMP snooping analyzes the received IGMP messages, establishes a mapping relationship between ports and MAC multicast addresses, and forwards multicast data according to this mapping relationship.

As shown in the figure below, when the Layer 2 device is not running IGMP Snooping, the multicast data is broadcast on the Layer 2. When the Layer 2 device is running IGMP Snooping, it is known that the multicast data of the multicast group will not be on the Layer 2. It is broadcasted and multicasted to designated receivers on the second layer, but unknown multicast data will still be broadcast on the second layer.



5.7.1 IGMP-snooping configuration

IGMP Snooping, used for IPv4 network, deployment location, Layer 2 switch between multicast router and user host, configured in VLAN, function, listen to IGMP/MLD messages sent between router and host to establish multicast data. The second layer forwarding table is used to manage and control the forwarding of multicast data in the second layer network.

By default, the IGMP Snooping function of the switch is disabled, so you need to enable the global IGMP Snooping function of the switch.

Steps:

1. Click the "Multicast> IGMP-snooping> Function Configuration" menu in the navigation tree to enter the IGMP-snooping configuration interface, which contains the created VLAN information, select the VLAN to be configured, and click Modify to enter the detailed configuration interface. As shown below:

State

Version

Report Suppression

☐ Enable
☒ IGMPv2
☐ IGMPv3
☒ Enable

Apply

VLAN Setting Table

VLAN	Operational Status	Router Port Auto Learn	Query Robustness	Query Interval	Query Max Response Interval	Last Member Query Counter	Last Member Query Interval	Immediate Leave
1	Disabled	Enabled	2	125	10	2	1	Disabled
10	Disabled	Enabled	2	125	10	2	1	Disabled
20	Disabled	Enabled	2	125	10	2	1	Disabled

Edit

Edit VLAN Setting

VLAN	10
State	☐ Enable
Router Port Auto Learn	☒ Enable
Immediate leave	☐ Enable
Query Robustness	2 (1 - 7, default 2)
Query Interval	125 Sec (30 - 18000, default 125)
Query Max Response Interval	10 Sec (5 - 20, default 10)
Last Member Query Counter	2 (1 - 7, default 2)
Last Member Query Interval	1 Sec (1 - 25, default 1)
Operational Status	
Status	Disabled
Query Robustness	2
Query Interval	125 (Sec)
Query Max Response Interval	10 (Sec)
Last Member Query Counter	2
Last Member Query Interval	1 (Sec)

The meaning of the interface information is shown in the table below.

Configuration item	Description
VLAN	VLANID to be configured
Status	Enable or disable IGMP-snooping function in this VLAN
Route port learning	
Leave quickly	
Number of queries	Maximum number of multicast queries
Query interval	Interval time of query messages
Maximum query response time	Query message timeout time, exceeding the maximum response time is timeout
Number of queries for a specific group	Maximum number of queries for a specific group
Specific group query interval	Interval of query messages for a specific group

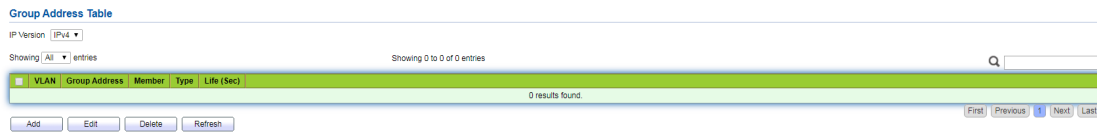
1. Fill in the corresponding configuration items.
2. Click "Apply" to complete the configuration.

5.7.2 Static multicast

Based on the previous multicast on-demand method, when users in different VLANs request the same multicast group, the data will be replicated and forwarded on the multicast router for each VLAN containing the receiver. Such a multicast on-demand method wastes a lot of bandwidth. After the IGMP Snooping function is activated, the port of the switch is added to the multicast VLAN by configuring the multicast VLAN, so that users in different VLANs share a multicast VLAN to receive multicast data, and the multicast stream is only in one multicast VLAN. Transmission is carried out within the VLAN, thereby saving bandwidth. And because of multicast VLAN and users. VLAN is completely isolated, security and bandwidth are guaranteed.

Steps

1. Click the "Multicast> Basic Functions> Static Multicast Configuration" menu in the navigation tree to enter the static multicast configuration interface, click the Add button to add a static multicast item, and click the Modify button to modify the existing static multicast item , The interface is shown in the figure below:



Add Group Address

VLAN

1

IP Version

IPv4

Group Address

Member

Available Port

GE1
GE2
GE3
GE4
GE5
GE6
GE7
GE8

Selected Port

Apply

Close

The meaning of the interface information is shown in the table below.

Configuration item	Description
VLAN	The VLAN ID that the multicast group belongs to, drop down to select an existing VLAN
IP version	Is the version of the multicast IP address v4 or v6
Multicast address	Enter the multicast address
Member	Join the multicast member, you can select multiple

2. Fill in the corresponding configuration items.
3. Click "Apply" to complete the configuration, as shown in the figure below.

Group Address Table

IP Version: IPv4

Showing 1 to 1 of 1 entries

VLAN	Group Address	Member	Type	Life (Sec)
1	224-1.1.1.111	GE2	Static	

Buttons: Add, Edit, Delete, Refresh

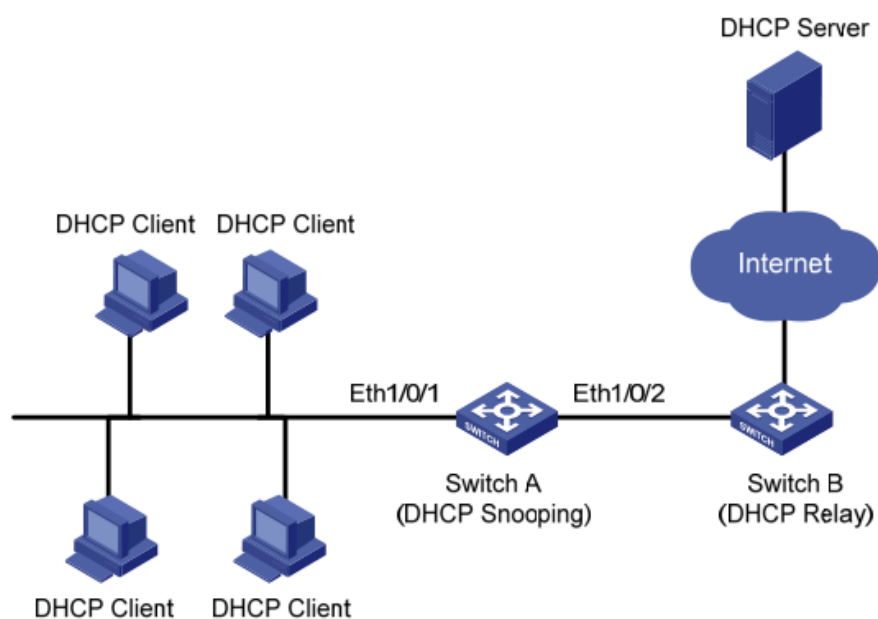
Navigation: First, Previous, Next, Last

5.8 DHCP-snooping configuration

For security reasons, the network administrator may need to record the IP address used by the user when surfing the Internet, and confirm the correspondence between the IP address the user obtains from the DHCP server and the MAC address of the user host.

The switch can record the user's IP address information through the security function of the DHCP relay running at the network layer. The switch can monitor DHCP messages through the DHCP Snooping function running on the data link layer and record the user's IP address information. In addition, if there is a privately set up DHCP server in the network, it may cause users to get the wrong IP address. In order to enable users to obtain IP addresses through a legal DHCP server, the DHCP Snooping security mechanism allows the port to be set as a trusted port or an untrusted port.

A trusted port is a port directly or indirectly connected to a legitimate DHCP server. The trusted port forwards the received DHCP messages normally, thus ensuring that the DHCP client obtains the correct IP address. An untrusted port is a port that is not connected to a legitimate DHCP server. If the DHCP-ACK and DHCP-OFFER messages from the DHCP server are received from the untrusted port, they will be discarded, thus preventing the DHCP client from obtaining the wrong IP address.



DHCP Snooping typical networking

DHCP Snooping uses the following two methods to obtain the IP address obtained by the user from the DHCP server and

User MAC address information:

Monitor DHCP-REQUEST messages

Monitor DHCP-ACK messages

5.8.1 DHCP-snooping global configuration

Enable DHCP-snooping

Steps:

1. Click the "Security> DHCP-snooping> Function Configuration" menu in the navigation tree to enter the DHCP-snooping configuration interface. The interface is divided into global configuration and port configuration. In the port configuration, click the port to be modified, and click Modify Enter the detailed modification interface, as shown below

State ☐ Enable

VLAN

Available VLAN

Selected VLAN

VLAN 1
VLAN 10
VLAN 20

Apply

Port Setting Table

Entry	Port	Trust	Verify Chaddr	Rate Limit
1	GE1	Disabled	Disabled	Unlimited
2	GE2	Disabled	Disabled	Unlimited
3	GE3	Disabled	Disabled	Unlimited
4	GE4	Disabled	Disabled	Unlimited
5	GE5	Disabled	Disabled	Unlimited
6	GE6	Disabled	Disabled	Unlimited
7	GE7	Disabled	Disabled	Unlimited
8	GE8	Disabled	Disabled	Unlimited
9	GE9	Disabled	Disabled	Unlimited
10	GE10	Disabled	Disabled	Unlimited
11	GE11	Disabled	Disabled	Unlimited
12	GE12	Disabled	Disabled	Unlimited
13	GE13	Disabled	Disabled	Unlimited
14	GE14	Disabled	Disabled	Unlimited
15	GE15	Disabled	Disabled	Unlimited
16	GE16	Disabled	Disabled	Unlimited
17	GE17	Disabled	Disabled	Unlimited
18	GE18	Disabled	Disabled	Unlimited
19	GE19	Disabled	Disabled	Unlimited
20	GE20	Disabled	Disabled	Unlimited
21	GE21	Disabled	Disabled	Unlimited
22	GE22	Disabled	Disabled	Unlimited
23	GE23	Disabled	Disabled	Unlimited
24	GE24	Disabled	Disabled	Unlimited
25	GE25	Disabled	Disabled	Unlimited
26	GE26	Disabled	Disabled	Unlimited
27	GE27	Disabled	Disabled	Unlimited
28	GE28	Disabled	Disabled	Unlimited
29	LAG1	Disabled	Disabled	Unlimited
30	LAG2	Disabled	Disabled	Unlimited
31	LAG3	Disabled	Disabled	Unlimited
32	LAG4	Disabled	Disabled	Unlimited
33	LAG5	Disabled	Disabled	Unlimited
34	LAG6	Disabled	Disabled	Unlimited
35	LAG7	Disabled	Disabled	Unlimited
36	LAG8	Disabled	Disabled	Unlimited

Edit

Edit Port Setting

Port	GE10
Trust	☐ Enable
Verify Chaddr	☐ Enable
Rate Limit	0 pps (1 - 300, default 0), 0 is Unlimited

The meaning of the interface is described in the following table

Configuration item	Description
Status	Enable and disable DHCP-snooping
VLAN	DHCP-snooping effective VLAN number
port	Configure the port number for DHCP-snooping
Trust	Whether the port is a trusted port
Client address detection	Whether to enable client address consistency check
Speed limit	Whether rate limit is enabled on the port and the limit value configuration

- Fill in the corresponding configuration items.
- Click "Settings" to complete the configuration, as shown in the figure below.

Port Setting Table

Entry	Port	Trust	Verify Chaddr	Rate Limit
☐ 1	GE1	Disabled	Disabled	100
☐ 2	GE2	Disabled	Disabled	100
☐ 3	GE3	Disabled	Disabled	Unlimited
☐ 4	GE4	Disabled	Disabled	Unlimited
☐ 5	GE5	Disabled	Disabled	Unlimited

5.8.2 Static BINDING

In a DHCP network, users who statically obtain IP addresses (non-DHCP users) may have various attacks on the network, such as spoofing the DHCP Server and constructing fake DHCP Request messages. This will bring certain security risks for legitimate DHCP users to use the network normally.

In order to effectively prevent attacks from non-DHCP users, you can enable the device to generate static MAC entries for interfaces based on the DHCP Snooping binding table. After that, the device will automatically execute commands to generate static MAC entries for these users based on the DHCP Snooping binding entries corresponding to all DHCP users on the interface, and at the same time disable the interface's ability to learn dynamic MAC entries. At this time, only the packets whose source MAC matches the static MAC entry can pass through the interface, otherwise the

packets will be discarded. Therefore, for non-DHCP users on this interface, only the administrator can manually configure the static MAC table entries of such users, and their packets can pass, otherwise the packets will be discarded.

Steps:

1. Click the "Security> IP Source Guard> IMPV Binding" menu in the navigation tree to enter the IP Source Guard binding configuration interface, click Add to add an IP-MAC-Port-VLAN binding group, as shown in the figure below Show:

IP-MAC-Port-VLAN Binding Table

Showing All entries Showing 0 to 0 of 0 entries

☐	Port	VLAN	MAC Address	IP Address	Binding	Type	Lease Time
0 results found.							
Add		Edit		Delete		First Previous 1 Next Last	

Add IP-MAC-Port-VLAN Binding

Port	GE1
VLAN	(1 - 4094)
Binding	☒ IP-MAC-Port-VLAN ☐ IP-Port-VLAN
MAC Address	
IP Address	/ 255.255.255.255
Apply Close	

The meaning of the interface is described in the following table

Configuration item	Description
Port	Port number in the bonding group
VLAN	Bonded VLAN ID
Bind	Select the binding relationship, including IPMV and IPV
MAC address	Bound MAC address
IP address	Bound IP address

2. Fill in the corresponding configuration items.
3. Click "Settings" to complete the configuration, as shown in the figure below.

IP-MAC-Port-VLAN Binding Table

Showing All entries Showing 1 to 1 of 1 entries

☐	Port	VLAN	MAC Address	IP Address	Binding	Type	Lease Time
☐	GE1	1	00:00:11:11:22:22	59.111.239.59 / 255.255.255.255	IP-MAC-Port-VLAN	Static	N/A
Add		Edit		Delete		First Previous 1 Next Last	

5.8.3 DHCP-snooping port configuration

If there is a DHCP server set up privately in the network, it may cause the user to get the wrong IP address. In order to enable users to obtain IP addresses through a legal DHCP server, the DHCP Snooping security mechanism of the PS7024 Ethernet switch allows the port to be set as a trusted port or an untrusted port.

Trusted port is the port directly or indirectly connected to a legal DHCP server. The trusted port forwards the received DHCP messages normally, thus ensuring that the DHCP client obtains the correct IP address.

Untrusted port is a port that is not connected to a legal DHCP server. If the DHCP-ACK and DHCP-OFFER messages from the DHCP server are received from the untrusted port, they will be discarded, thereby preventing the DHCP client from obtaining the wrong IP address.

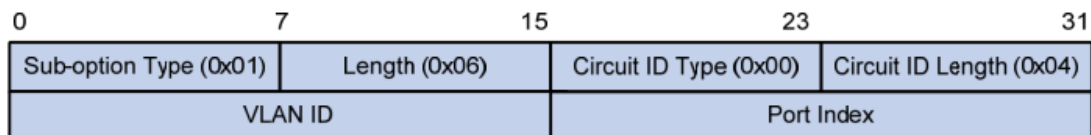
Option 82 is the Relay Agent Information option in the DHCP message. This option records the location information of the DHCP client. After the DHCP relay (or DHCP Snooping device) receives the request message sent by the DHCP client to the DHCP server, it can add Option 82 to the message so that the administrator can locate the DHCP client and realize the security and calculation of the client. Cost control. Servers that support Option 82 can also formulate IP address and other parameter allocation strategies based on the option information, providing a more flexible address allocation method.

Option 82 can contain up to 255 sub-options. If Option 82 is defined, at least one sub-option must be defined. Currently the device supports two sub-options: Circuit ID sub-option and Remote ID sub-option. As RFC 3046 does not have a unified regulation on the content of Option 82, different vendors usually fill in as needed. As a DHCP relay device, the Ethernet switch supports the extended padding format of Option 82 sub-options. The padding content by default is shown in the figure below.

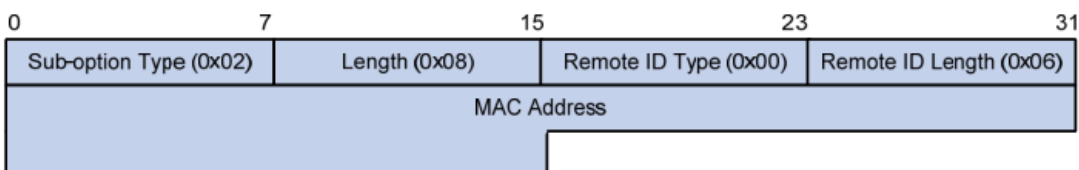
The content of sub-option 1 is the VLAN number and port index of the port that received the DHCP client request message (the value of the port index is the physical port number minus 1).

The content of sub-option 2 is the bridge MAC address of the DHCP relay device that received the DHCP client request message.

The content of sub-option 1 is the VLAN number and port index of the port that received the DHCP client request message (the value of the port index is the port physical number minus 1) as shown in the figure below.



The content of sub-option 2 is the bridge MAC address of the DHCP relay device that received the DHCP client request message.



DHCP relay supports Option 82 working mechanism

The process of obtaining an IP address by a DHCP client from a DHCP server through a DHCP relay is basically the same as the process of obtaining an IP address directly from a DHCP server. It has to go through four stages of discovery, provision, selection, and confirmation. Only the DHCP relay support will be introduced here. The working mechanism of Option 82 is as follows:

(1) After receiving the DHCP request message, the DHCP relay device will check whether there is an Option 82 option in the message and perform corresponding processing.

☐ If there is Option 82 in the request message, the DHCP relay device will process the message according to the configured policy (discard, replace the original Option 82 option in the message with the Option 82 option of the relay device itself, or keep the message The original Option 82 option in the text), and then forward the request message to the DHCP server.

☐ If there is no Option 82 option in the request message, the DHCP relay device will add Option 82 option to the message and forward it to the DHCP server

(2) After receiving the return message from the DHCP server, the DHCP relay device strips the Option 82 information in the message, and then forwards the message with DHCP configuration information to the DHCP client.

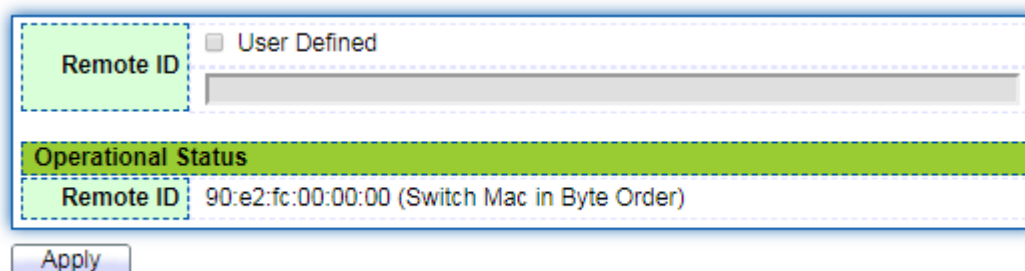
Description:

There are two types of request messages sent by the DHCP client, namely DHCP-DISCOVER messages and DHCP-REQUEST message. Because the DHCP server devices produced by different manufacturers have different processing mechanisms for request messages, some devices process the Option 82 information in the DHCP-DISCOVER message, and some process the Option 82 information in the DHCP-REQUEST message, so DHCP relay equipment Option 82 will be added to both types of messages.

After the switch is configured with DHCP Snooping and supports the Option 82 function, when the DHCP request message sent by the received DHCP client contains the Option 82 option, according to the configured processing strategy and sub-option content, DHCP Snooping responds to the message The processing mechanism is different.

Steps:

1. Click the "Security> DHCP-snooping> Option 82 Function Configuration" menu in the navigation tree to enter the configuration interface of the DHCP-snooping Option 82 function, including Option 82 global settings and port configuration, click the port to be configured, and click the Modify button. Enter the detailed configuration interface of Port Option82, as shown in the figure below:



Remote ID	☐ User Defined
Operational Status	
Remote ID	90:e2:fc:00:00:00 (Switch Mac in Byte Order)
Apply	

Port Setting Table

Entry	Port	State	Allow Untrust
☐ 1	GE1	Disabled	Drop
☐ 2	GE2	Disabled	Drop
☐ 3	GE3	Disabled	Drop
☐ 4	GE4	Disabled	Drop
☐ 5	GE5	Disabled	Drop
☐ 6	GE6	Disabled	Drop
☐ 7	GE7	Disabled	Drop
☐ 8	GE8	Disabled	Drop
☐ 9	GE9	Disabled	Drop
☐ 10	GE10	Disabled	Drop
☐ 11	GE11	Disabled	Drop
☐ 12	GE12	Disabled	Drop
☐ 13	GE13	Disabled	Drop
☐ 14	GE14	Disabled	Drop
☐ 15	GE15	Disabled	Drop
☐ 16	GE16	Disabled	Drop
☐ 17	GE17	Disabled	Drop
☐ 18	GE18	Disabled	Drop
☐ 19	GE19	Disabled	Drop
☐ 20	GE20	Disabled	Drop
☐ 21	GE21	Disabled	Drop
☐ 22	GE22	Disabled	Drop
☐ 23	GE23	Disabled	Drop
☐ 24	GE24	Disabled	Drop
☐ 25	GE25	Disabled	Drop
☐ 26	GE26	Disabled	Drop
☐ 27	GE27	Disabled	Drop
☐ 28	GE28	Disabled	Drop
☐ 29	LAG1	Disabled	Drop
☐ 30	LAG2	Disabled	Drop
☐ 31	LAG3	Disabled	Drop
☐ 32	LAG4	Disabled	Drop
☐ 33	LAG5	Disabled	Drop
☐ 34	LAG6	Disabled	Drop
☐ 35	LAG7	Disabled	Drop
☐ 36	LAG8	Disabled	Drop

Edit Port Setting

Port

State

Allow Untrust

GE1

☐ Enable

☐ Keep
☒ Drop
☐ Replace

The meaning of the interface is described in the following table:

Configuration item	Description
Remote-id	Fill in the content of the Remote-id field in Option 82 (such as user-defined content abcd)
Port	Whether to enable Option82 port number
Allow untrusted	After the option 82 function is enabled on the port, the packet processing mode of the untrusted port:

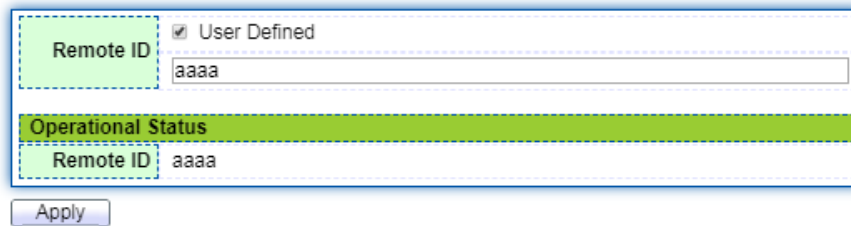
 Description:

The configuration of the content of the Circuit ID sub-option or the Remote ID sub-option in the Option 82 field is independent of each other, and can be configured separately or at the same time, and the configuration sequence is in no particular order.

DHCP Option82 must be configured on the user side of the device, otherwise the DHCP messages sent by the device to the DHCP Server will not carry Option82 option content.

When receiving a DHCP response message from the DHCP server, if the message contains the Option 82 option, the Option 82 field is deleted and forwarded; if the message does not contain the Option 82 option, it is forwarded directly.

2. Fill in the corresponding configuration items.
3. Click "Apply" to complete the configuration, as shown in the figure below.



Remote ID ☒ User Defined
aaaa

Operational Status
Remote ID aaaa

Apply

Port Setting Table

	Entry	Port	State	Allow Untrust
☐	1	GE1	Disabled	Replace
☐	2	GE2	Disabled	Replace
☐	3	GE3	Disabled	Drop
☐	4	GE4	Disabled	Drop
☐	5	GE5	Disabled	Drop

DHCP Snooping Typical Configuration Examples

a. DHCP Snooping supports Option 82 configuration example

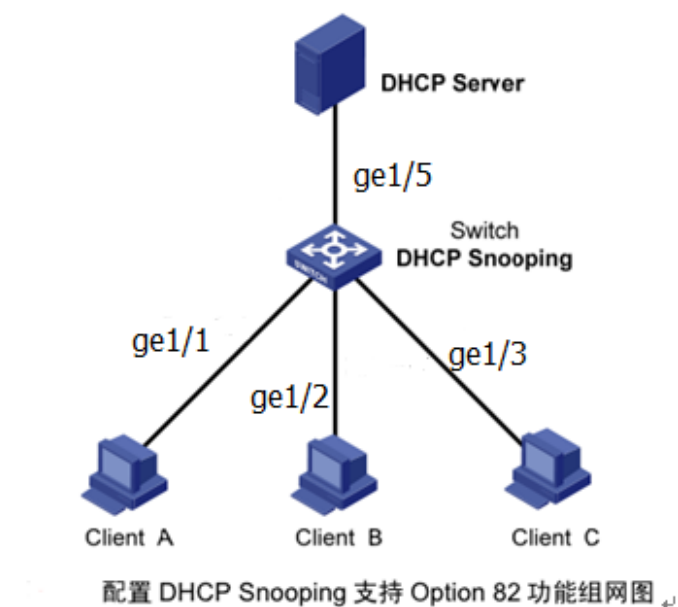
As shown in the figure below, port ge1/5 of the Switch is connected to the DHCP server, and ports ge1/1, ge1/2, and ge1/3 are connected to DHCP Client A, DHCP Client B, and DHCP Client C respectively.

Enable the DHCP Snooping function on the Switch.

Set port ge1/5 on the Switch as a trusted port for DHCP Snooping.

Enable DHCP Snooping on the Switch to support Option 82. For packets passing through port ge1/3, fill Option 82 with the default configuration of the switch's Circuit ID and Remote-id.

组网图



Steps:

1. Turn on the DHCP Snooping function of the switch. Click the "DHCP-snooping Configuration>Function Configuration" menu in the navigation tree to enter the "Function Configuration" interface and enable the function, as shown in the figure below.

2. Set port ge1/5 as a trusted port for DHCP Snooping. , Fill in the corresponding configuration, and click "modify". The interface is shown in the figure below.

Port Setting Table

Entry	Port	Trust	Verify Chaddr	Rate Limit
1	GE1	Disabled	Disabled	Unlimited
2	GE2	Disabled	Disabled	Unlimited
3	GE3	Disabled	Disabled	Unlimited
4	GE4	Disabled	Disabled	Unlimited
5	GE5	Disabled	Disabled	Unlimited
6	GE6	Disabled	Disabled	Unlimited

- Configure on the Ethernet port ge1/3, and set the Remote-id in Option 82 of the DHCP message. Click the "DHCP-snooping configuration> Option 82 function configuration" menu in the navigation tree, enter the "Option 82 function configuration", check the port, enter the port setting page, select the corresponding configuration, and click "Apply" to complete the configuration. The interface is shown in the figure below.

Entry	Port	State	Allow Untrust
1	GE1	Disabled	Drop
2	GE2	Disabled	Drop
3	GE3	Disabled	Replace
4	GE4	Disabled	Drop
5	GE5	Disabled	Drop

- Configure on the Ethernet port ge1/3, and set the Circuit-id in Option 82 of the DHCP message. Click the "DHCP-snooping configuration> Option 82Circuit-id function configuration" menu in the navigation tree, enter the "Option 82Circuit-id function configuration", add the port configuration, enter the port setting page, select the corresponding configuration, and click "Apply" to complete Configuration. The interface is shown in the figure below.

Port	VLAN	Circuit ID
GE3	1	ge1/3

6. Cybersecurity

6.1 DOS anti-attack settings

6.1.1 Function configuration

In order to improve the security of the switch, you can turn on the anti-attack option of the switch

Steps:

- Click the "Security> DOS Attack Defense> Function Settings" menu in the navigation tree, enter the "DOS Attack Defense Global Settings", and enable "Prevent POD Attacks", "Prevent Land Attacks", and "Discard packets with the same source and destination MAC addresses", "Discard ICMP Fragment Packet", click "Apply" to complete the configuration,

the interface is shown in the figure below.

POD	☒ Enable
Land	☒ Enable
UDP Blat	☒ Enable
TCP Blat	☒ Enable
DMAC = SMAC	☒ Enable
Null Scan Attack	☒ Enable
X-Mas Scan Attack	☒ Enable
TCP SYN-FIN Attack	☒ Enable
TCP SYN-RST Attack	☒ Enable
ICMP Fragment	☒ Enable
TCP-SYN	☒ Enable Note: Source Port < 1024
TCP Fragment	☒ Enable Note: Offset = 1
Ping Max Size	☒ Enable IPv4 ☒ Enable IPv6 512 Byte (0 - 65535, default 512)
TCP Min Hdr size	☒ Enable 20 Byte (0 - 31, default 20)
IPv6 Min Fragment	☒ Enable 1240 Byte (0 - 65535, default 1240)
Smurf Attack	☒ Enable 0 Netmask Length (0 - 32, default 0)

Apply

6.1.2 Port configuration

Enable DOS anti-attack option based on port

Steps

1. Click the "Security> DOS Attack Prevention> Port Configuration" menu in the navigation tree, and enter the "DOS Attack Prevention Port Settings", as shown in the figure below

Port Setting Table

				Q	
☐	Entry	Port	State		
☐	1	GE1	Disabled		
☐	2	GE2	Disabled		
☐	3	GE3	Disabled		
☐	4	GE4	Disabled		

2. Select the port and click "Modify", enter to modify the port configuration,

open and close the port DOS anti-attack settings, as shown in the figure below.

Edit Port Setting

Port	GE1
State	☒ Enable

6.2 ACL configuration

With the expansion of network scale and the increase of traffic, the control of network security and the allocation of bandwidth have become important contents of network management. By filtering data packets, you can effectively prevent illegal users from accessing the network. At the same time, you can control traffic and save network resources. ACL (Access Control List) is achieved by configuring matching rules and processing operations for packets. Realize the function of packet filtering. When the switch port receives the message, it analyzes the fields of the message according to the ACL rules applied on the current port, and after identifying the specific message, it allows or prohibits the corresponding data packet to pass through according to the preset policy. The data packet matching rules defined by ACL can also be referenced by other functions that need to distinguish traffic, such as the definition of traffic classification rules in QoS. By setting matching rules and operation processing, access control lists (ACLs) can implement packet filtering. An access control list is a collection of a series of permission and denial conditions applicable to a data packet. When receiving a data packet on the interface, the switch compares the data packet field with the ACL used, and determines that the data packet is permitted to be forwarded based on the criteria specified in the access list. ACL classifies data packets through a series of matching conditions. These conditions can be the source MAC address, destination MAC address, source IP address, destination IP address, port number, etc. of the data packet. ACL classifies data packets through a series of matching conditions. These conditions can be the source address, destination address, and port number of the data packet. According to the application purpose, ACLs can be divided into the following types: Basic IP ACL (Basic IP ACL): Rules are formulated only based on the source IP address of the data packet. ACL ID range: 100~999. Advanced IP ACL (Advanced IP ACL): Formulate rules based on the third and fourth layer information such as the source IP address, destination IP address, IP bearer protocol type, and protocol characteristics of the data packet. ACL ID range: 100~999. Layer 2 ACL (L2 ACL): Formulate rules based on Layer 2 information such as the source MAC address, destination MAC address, 802.1p priority, and Layer 2 protocol type of the data packet. ACL ID range: 1~99.

6.2.1 MAC ACL configuration

Layer 2 ACL: Formulate rules based on Layer 2 information such as source MAC address, destination MAC address, VLAN priority, and Layer 2 protocol type.

Steps:

1. Click the "ACL> MAC ACL Configuration" menu in the navigation tree to enter the "MAC ACL

Configuration" interface, as shown in the figure below.

The meaning of interface information is described in the following table

Configuration item	Description
ACL name	Set the name of the MAC ACL rule

2. Click the "ACL> MAC ACE Configuration" menu in the navigation tree, select the ACL name, and click "Add" as shown in the figure below:

The meaning of interface information is described in the following table

Configuration item	Description
ACL name	List of ACL rules set through the MAC ACL page

3. Fill in the corresponding configuration items:

The meaning of interface information is described in the following table

Configuration item	Description
Serial number	The MAC ACL value range is: 1-2147483647
action	ACL action rules are divided into "Permit" (allow) rules or "Deny" (deny) rules, and "Shutdown" (close the port).
Source MAC	Enter the source MAC address and mask of the ACL rule. The format is H.H.H.H.H.H. Select "any" (all), it means any MAC.
Destination MAC	Enter the destination MAC address and mask of the ACL rule. The format is H.H.H.H.H.H. Select "any" (all), it means any MAC.
Ethernet type	Enter the Ethernet type of the ACL rule, the value range is: 0x600-0Xffff, select "any" (all), it means any Ethernet type.
VLAN	Enter the VLAN of the ACL rule, the value range is: 1-4094, select "any" (all), it means any VLAN.
802.1p	Enter the VLAN priority and mask of the ACL rule, the value range is: 1-7, select "any" (all), it means any VLAN priority.

4. Click "Apply" to complete the configuration, as shown in the figure.

ACE Table

ACL Name

Showing entries Showing 1 to 1 of 1 entries

Sequence	Action	Source MAC		Destination MAC		Ethertype	VLAN	802.1p	
		Address	Mask	Address	Mask			Value	Mask
☐ 1	Permit	00:00:11:11:20:00	FF:FF:FF:FF:FF:00	00:00:11:11:10:00	FF:FF:FF:FF:FF:00	Any	Any	Any	Any

6.2.2 IPv4 ACL configuration

Basic IPv4 ACL (Basic IP ACL): Only formulate rules based on the source IP address of the data packet. ACL ID range: 100~999.

Advanced IP ACL (Advanced IP ACL): Formulate rules based on the third and fourth layer information such as the source IP address, destination IP address, IP bearer protocol type, and protocol characteristics of the data packet. ACL ID range: 100~999

Steps

1. Click the "ACL> IPv4 ACL Configuration" menu in the navigation tree to enter the "IPv4 ACL Configuration" interface, as shown in the figure below.

ACL Name

The meaning of interface information is described in the following table

Configuration item	Description
ACL name	Set the name of the IPv4 ACL rule

2. Click the "ACL> IPv4 ACE Configuration" menu in the navigation tree, select the ACL name, and click "Add" as shown in the figure below:

ACE Table

ACL Name **b**

Showing **All** entries Showing 0 to 0 of 0 entries

Sequence	Action	Protocol	Source IP		Destination IP		Source Port	Destination Port	TCP Flags	Type of Service		ICMP	
			Address	Mask	Address	Mask				DSCP	IP Precedence	Type	Code
0 results found.													

The meaning of interface information is described in the following table

Configuration item	Description
ACL name	List of ACL rules set through the IPv4 ACL page

3. Fill in the corresponding configuration items:

Add ACE

ACL Name	b
Sequence	(1 - 2147483647)
Action	☒ Permit ☐ Deny ☐ Shutdown
Protocol	☒ Any ☐ Select ICMP ☐ Define (0 - 255)
Source IP	☒ Any / (Address / Mask)
Destination IP	☒ Any / (Address / Mask)
Type of Service	☒ Any ☐ DSCP (0 - 63) ☐ IP Precedence (0 - 7)
Source Port	☒ Any ☐ Single (0 - 65535) ☐ Range - (0 - 65535)
Destination Port	☒ Any ☐ Single (0 - 65535) ☐ Range - (0 - 65535)
TCP Flags	Urg: ☐ Set ☐ Unset ☐ Don't care Ack: ☐ Set ☐ Unset ☐ Don't care Psh: ☐ Set ☐ Unset ☐ Don't care Rst: ☐ Set ☐ Unset ☐ Don't care Syn: ☐ Set ☐ Unset ☐ Don't care Fin: ☐ Set ☐ Unset ☐ Don't care
ICMP Type	☒ Any ☐ Select Echo Reply ☐ Define (0 - 255)
ICMP Code	☒ Any ☐ Define (0 - 255)

The meaning of interface information is described in the following table

Configuration item	Description
Serial number	The IPv4 ACL value range is: 1-2147483647
action	ACL action rules are divided into "Permit" (allow) rules or "Deny" (deny) rules, and "Shutdown" (close the port).
protocol	Required, select the type of agreement. icmp, tcp, udp, etc., select "any" (all), it means any protocol
Source IP	Enter the source IP and mask of the ACL rule, select "any", it means any source IP
Destination IP	Enter the destination IP and mask of the ACL rule, select "any" (all), it means any destination IP
Service type	Enter the service type of the ACL rule, DSCP (range 0-63) or IP priority (range 0-7), select "any" (all), it means any service type
Source port	Enter the source port of the ACL rule, a single port number or range (range 0-65535), select "any" (all), it means any source port
Destination port	Enter the destination port of the ACL rule, a single port number or range (range 0-65535), select "any" (all), it means any destination port
TCP flag	Enter the TCP flags of ACL rules, Urg, Ack, Psh, Rst, Sym, Fin flags, actions include "set" (set), "unset" (cancel), and "Don't care" (no processing)
ICMP type	Enter the ICMP packet type of the ACL rule, select "any" (all), it means any ICMP type
ICMP field	Enter the ICMP field value of the ACL rule, select "any" (all), it means any ICMP field value

3. Click "Apply" to complete the configuration, as shown in the figure.

ACE Table

ACL Name

Showing entries Showing 1 to 1 of 1 entries

	Sequence	Action	Protocol	Source IP		Destination IP		Source Port	Destination Port	TCP Flags	Type of Service		ICMP	
				Address	Mask	Address	Mask				DSCP	IP Precedence	Type	Code
☐	100	Permit	Any (IP)	Any	Any	Any	Any				Any	Any		

6.2.3 IPv6 ACL configuration

Steps

1. Click the "ACL> IPv6 ACL Configuration" menu in the navigation tree to enter the "IPv6 ACL Configuration" interface, as shown in the figure below.

ACL Name

Apply

The meaning of interface information is described in the following table

Configuration item	Description
ACL name	Set the name of the IPv6 ACL rule

3. Click the "ACL> IPv6 ACE Configuration" menu in the navigation tree, select the ACL name, and click "Add" as shown in the figure below

ACE Table

ACL Name

Showing entries Showing 0 to 0 of 0 entries

	Sequence	Action	Protocol	Source IP		Destination IP		Source Port	Destination Port	TCP Flags	Type of Service		ICMP	
				Address	Prefix	Address	Prefix				DSCP	IP Precedence	Type	Code
0 results found.														

The meaning of interface information is described in the following table

Configuration item	Description
ACL name	List of ACL rules set through the IPv6 ACL page

3. Fill in the corresponding configuration items:

Add ACE

ACL Name	c
Sequence	(1 - 2147483647)
Action	☒ Permit ☐ Deny ☐ Shutdown
Protocol	☒ Any ☐ Select TCP ☐ Define (0 - 255)
Source IP	☒ Any ☐ / (Address / Prefix (0 - 128))
Destination IP	☒ Any ☐ / (Address / Prefix (0 - 128))
Type of Service	☒ Any ☐ DSCP (0 - 63) ☐ IP Precedence (0 - 7)
Source Port	☒ Any ☐ Single (0 - 65535) ☐ Range - (0 - 65535)
Destination Port	☒ Any ☐ Single (0 - 65535) ☐ Range - (0 - 65535)
TCP Flags	Urg: ☐ Set ☐ Unset ☐ Don't care Ack: ☐ Set ☐ Unset ☐ Don't care Psh: ☐ Set ☐ Unset ☐ Don't care Rst: ☐ Set ☐ Unset ☐ Don't care Syn: ☐ Set ☐ Unset ☐ Don't care Fin: ☐ Set ☐ Unset ☐ Don't care
ICMP Type	☒ Any ☐ Select Destination Unreachable ☐ Define (0 - 255)
ICMP Code	☒ Any ☐ Define (0 - 255)

The meaning of interface information is described in the following table

Configuration item	Description
Serial number	The IPv6 ACL value range is: 1-2147483647
action	ACL action rules are divided into "Permit" (allow) rules or "Deny" (deny) rules, and "Shutdown" (close the port).
Serial number	The MAC ACL value range is: 1-2147483647
protocol	Required, select the type of agreement. icmp, tcp, udp, select "any" (all), it means any protocol
Source IP	Enter the source IP and mask of the ACL rule, select "any", it means any source IP
Destination IP	Enter the destination IP and mask of the ACL rule, select "any" (all), it means any destination IP
Service type	Enter the service type of the ACL rule, DSCP (range 0-63) or IP priority (range 0-7), select "any" (all), it means any service type
Source port	Enter the source port of the ACL rule, a single port number or range (range 0-65535), select "any" (all), it means any source port

Destination port	Enter the destination port of the ACL rule, a single port number or range (range 0-65535), select "any" (all), it means any destination port
TCP flag	Enter the TCP flags of ACL rules, Urg, Ack, Psh, Rst, Sym, Fin flags, actions include "set" (set), "unset" (cancel), and "Don't care" (no processing)
ICMP type	Enter the ICMP packet type of the ACL rule, select "any" (all), it means any ICMP type
ICMP field	Enter the ICMP field value of the ACL rule, select "any" (all), it means any ICMP field value

3. Click "Apply" to complete the configuration, as shown in the figure.

ACE Table

ACL Name

Showing **All** entries Showing 1 to 1 of 1 entries

Sequence	Action	Protocol	Source IP		Destination IP		Source Port	Destination Port	TCP Flags	Type of Service		ICMP	
			Address	Prefix	Address	Prefix				DSCP	IP Precedence	Type	Code
1000	Permit	Any (IP)	Any	Any	Any	Any				Any	Any		

First Previous **1** Next Last

6.2.4 ACL binding configuration

After the list is created, it must be bound to each interface that wants to use it.

Steps:

1. Click the "ACL> ACL Binding" menu in the navigation tree to enter the "ACL Binding Configuration" interface, as shown in the figure below.

ACL Binding Table

Entry	Port	MAC ACL	IPv4 ACL	IPv6 ACL
1	GE1			
2	GE2			
3	GE3			
4	GE4			
5	GE5			

The meaning of the interface is as follows

Configuration item	Description
MAC ACL	Bind to the MAC ACL name on the port
IPv4 ACL	Bind to the IPv4 ACL name on the port (mutually exclusive with IPv6 ACL)
IPv6 ACL	Bind to the IPv6 ACL name on the port (mutually exclusive with IPv4 ACL)

2. Fill in the corresponding configuration items, taking the created MAC ACL a, IPv4 ACL b, and IPv6 ACL c as examples.

3. Click "Apply" to complete the configuration, as shown in the figure.

Add ACL Binding

Port	GE3
Note: ACL without any rules cannot be bound	
MAC ACL	None ▼
IPv4 ACL	b ▼
IPv6 ACL	None ▼

Apply Close

7. Advanced configuration

QoS (Quality of Service) is used to evaluate the service party's ability to meet customer service requirements. In the Internet, QoS is used to evaluate the service ability of the network to transmit packets. Since the services provided by the network are diverse, it can be evaluated based on different aspects. Generally speaking, QoS is an evaluation of the service capability that can support core requirements such as bandwidth, delay, delay jitter, and packet loss rate during the packet delivery process. Bandwidth, also referred to as throughput, represents the average rate of service flow within a certain period of time, and the unit is usually kbit/s. Latency is the average time required for a service flow to pass through the network. For a device in the network, the delay requirement is generally understood as several levels. For example, there are two delay levels. The priority queue scheduling method enables high-priority services to obtain service as quickly as possible, while low-priority services need to wait for no high-priority services to obtain service. Delay jitter, which represents the change in the time that the service flow passes through the network. The packet loss rate indicates the loss rate of the service flow during transmission. Due to the high reliability of modern transmission systems, the loss of information often occurs when the network is congested. The most common situation is that queue overflow causes packet loss. In a traditional IP network, all messages are treated equally without distinction. Each network device uses a first-in, first-out strategy to process all messages. It does its best (Best-Effort) to report The message is sent to the destination, but no guarantee is provided for the reliability of message transmission, transmission delay and other performance.

Network development is changing with each passing day. With the continuous emergence of new applications on IP networks, new requirements are also put forward for the quality of IP networks. For example, delay-sensitive services such as VoIP and video put forward higher requirements on the transmission delay of messages. If the message transmission delay is too long, it will be unacceptable to the user. In order to support services such as voice, video, and data with different service requirements, the network is required to be able to distinguish different service types and then provide corresponding services for them.

The best-effort service of traditional IP networks cannot identify and distinguish the various types of services in the network, and the ability to distinguish service types is the prerequisite for providing differentiated services for different services. Therefore, the best-effort service model of traditional networks can no longer satisfy Application needs. The emergence of QoS technology is dedicated to solving this problem. QoS can regulate network traffic, avoid and manage network congestion, and reduce packet loss rate. At the same time, it supports the provision of dedicated

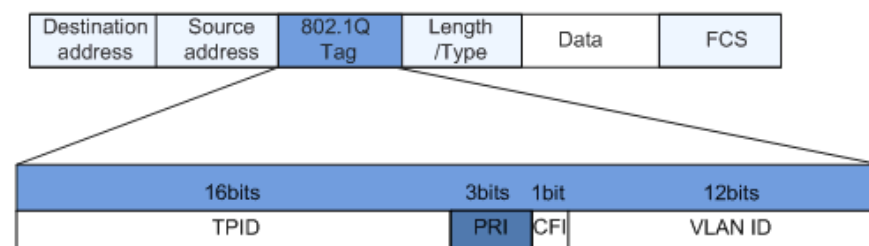
bandwidth for users and different service quality for different services, which improves the service capabilities of the network.

Different packets use different QoS priorities. For example, VLAN packets use 802.1p, or CoS (Class of Service) fields, and IP packets use DSCP. When a message passes through different networks, in order to maintain the priority of the message, it is necessary to configure the mapping relationship of these priority fields at the gateways connecting different networks.

802.1p priority in VLAN frame header

VLAN frames are usually exchanged between Layer 2 devices. According to the definition of IEEE 802.1Q, the PRI field (802.1p priority) in the VLAN frame header, or CoS (Class of Service) field, identifies the quality of service requirements.

802.1p priority in VLAN frames

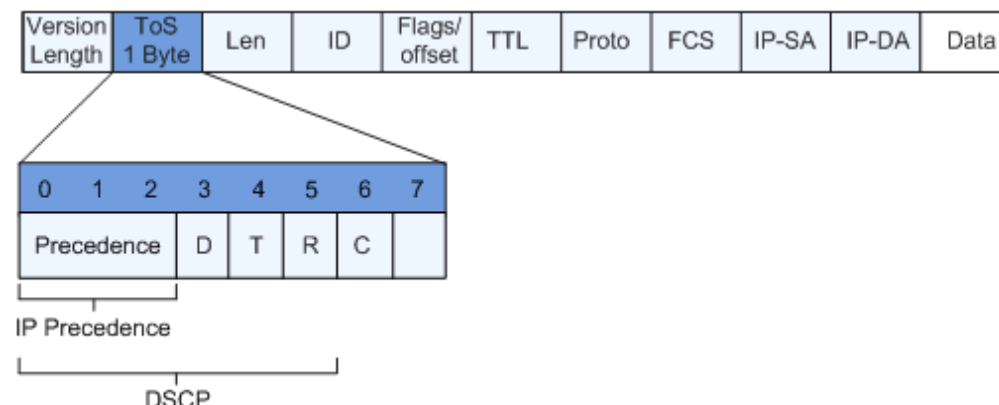


The 802.1Q header contains a 3-bit PRI field. The PRI field defines eight types of service priority CoS, and the values are 7, 6, ..., 1, and 0 in the order of priority from high to low.

IP Precedence/DSCP field

According to the definition of RFC791, the ToS (Type of Service) field of the IP message header consists of 8 bits. The Precedence field of 3 bits identifies the priority of the IP message. The position of the Precedence in the message is shown in the figure.

IP Precedence/DSCP field



Bits 0 to 2 represent the Precedence field, representing 8 priority levels of message transmission, and the values are 7, 6, ..., 1, and 0 in the order of priority from high to low. The highest priority is 7 or 6, which is often reserved for routing or updating network control communications. User-level applications can only use levels 0 to 5.

In addition to the Precedence field, the ToS field also includes three bits D, T, and R: The D bit represents the delay requirement (Delay, 0 represents normal delay, 1 represents low delay). T bit represents throughput (Throughput, 0 represents normal throughput, 1 represents high throughput). R bit represents reliability (Reliability, 0 represents normal reliability, 1 represents high reliability). Bits 6 and 7 in the ToS field are reserved.

RFC1349 redefines the ToS field in IP packets and adds the C bit to indicate the Monetary Cost. Later, the IETF DiffServ working group redefined bits 0 to 5 in the ToS field of the IPv4 packet header as DSCP in RFC2474, and renamed the ToS field to DS (Differentiated Service) bytes. The position of DSCP in the message is shown in the figure above.

The first 6 bits (bits 0 to 5) of the DS field are used as DSCP (DS Code Point), and the upper 2 bits (bits 6 and 7) are reserved bits. The lower 3 bits (bits 0 to 2) of the DS field are the Class Selector Code Point (CSCP). The same CSCP value represents a class of DSCP. The DS node selects the corresponding PHB (Per-Hop Behavior) according to the DSCP value.

7.1 QOS configuration

7.1.1 Basic configuration

When the network is congested, the problem of multiple messages competing for resources at the same time must be solved, and queue scheduling is usually used to solve it. Congestion management generally uses queue scheduling technology to avoid intermittent congestion in the network. Queue scheduling technologies include: SP (Strict-Priority, strict priority queue), WFQ (Weighted Fair Queue, weighted fair queue) and WRR (Weighted Round Robin, weighted round robin), DRR scheduling (DRR (Deficit Round Robin) scheduling It is also an extension of RR).

7.1.1.1 Function configuration

Steps for configuring global and interface scheduling types

1. Click the "QOS> Basic Function> Function Configuration" menu in the navigation tree to enter the "Function Configuration" interface, as shown in the figure below.

Port Setting Table

■	Entry	Port	CoS	Trust	Remarking		
					CoS	DSCP	IP Precedence
☐	1	GE1	0	Enabled	Disabled	Disabled	Disabled
☐	2	GE2	0	Enabled	Disabled	Disabled	Disabled
☐	3	GE3	0	Enabled	Disabled	Disabled	Disabled

The meaning of the global configuration interface is as follows

Configuration item	Description
status	Global QOS function switch.
Trust	There are 4 trust modes: CoS, DSCP, CoS-DSCP, and IP priority

The meaning of the port configuration interface is as follows

Configuration item	Description
CoS	Range 0-7
Port trust	Port QOS function switch
CoS	Mark the CoS field
DSCP	Mark the DSCP field
IP priority	Mark the IP precedence field

7.1.1.2 Queue scheduling

Click the "QOS> Queue Scheduling" menu in the navigation tree, enter the "Queue Scheduling" interface, and click "Apply" to complete the configuration, as shown in the figure below.

Queue Scheduling Table

Queue	Method			
	Strict Priority	WRR	Weight	WRR Bandwidth (%)
1	☐	☐	1	
2	☐	☐	2	
3	☐	☐	3	
4	☐	☐	4	
5	☐	☐	5	
6	☐	☐	9	
7	☐	☐	13	
8	☐	☐	15	

Apply

The meaning of the interface is as follows

Configuration item	Description
Strict Priority (SP)	Strict priority mode
WRR	Weighted polling mode
Weights	Percentage of queues occupying WRR bandwidth

7.1.1.3 CoS mapping

1. Click the "QOS> CoS Mapping" menu in the navigation tree, enter the "CoS Mapping" interface, and click "Apply" to complete the configuration, as shown in the figure below.

CoS to Queue Mapping

CoS	Queue
0	1 ▼
1	2 ▼
2	3 ▼
3	4 ▼
4	5 ▼
5	6 ▼
6	7 ▼
7	8 ▼

Apply

Queue to CoS Mapping

Queue	CoS
1	0 ▼
2	1 ▼
3	2 ▼
4	3 ▼
5	4 ▼
6	5 ▼
7	6 ▼
8	7 ▼

Apply

The meaning of the interface is as follows

Configuration item	Description
Strict Priority (SP)	Strict priority mode
WRR	Weighted polling mode
Weights	Percentage of queues occupying WRR bandwidth

7.1.1.4 DSCP mapping

1. Click the "QOS> Queue Scheduling" menu in the navigation tree, enter the "Queue Scheduling" interface, and click "Apply" to complete the configuration, as shown in the figure below.

DSCP to Queue Mapping

DSCP	Queue	DSCP	Queue	DSCP	Queue	DSCP	Queue
0 [CS0]	1 ▼	16 [CS2]	3 ▼	32 [CS4]	5 ▼	48 [CS6]	7 ▼
1	1 ▼	17	3 ▼	33	5 ▼	49	7 ▼
2	1 ▼	18 [AF21]	3 ▼	34 [AF41]	5 ▼	50	7 ▼
3	1 ▼	19	3 ▼	35	5 ▼	51	7 ▼
4	1 ▼	20 [AF22]	3 ▼	36 [AF42]	5 ▼	52	7 ▼
5	1 ▼	21	3 ▼	37	5 ▼	53	7 ▼
6	1 ▼	22 [AF23]	3 ▼	38 [AF43]	5 ▼	54	7 ▼
7	1 ▼	23	3 ▼	39	5 ▼	55	7 ▼
8 [CS1]	2 ▼	24 [CS3]	4 ▼	40 [CS5]	6 ▼	56 [CS7]	8 ▼
9	2 ▼	25	4 ▼	41	6 ▼	57	8 ▼
10 [AF11]	2 ▼	26 [AF31]	4 ▼	42	6 ▼	58	8 ▼
11	2 ▼	27	4 ▼	43	6 ▼	59	8 ▼
12 [AF12]	2 ▼	28 [AF32]	4 ▼	44	6 ▼	60	8 ▼
13	2 ▼	29	4 ▼	45	6 ▼	61	8 ▼
14 [AF13]	2 ▼	30 [AF33]	4 ▼	46 [EF]	6 ▼	62	8 ▼
15	2 ▼	31	4 ▼	47	6 ▼	63	8 ▼

Apply

Queue to DSCP Mapping

Queue	DSCP
1	0 [CS0] ▼
2	8 [CS1] ▼
3	16 [CS2] ▼
4	24 [CS3] ▼
5	32 [CS4] ▼
6	40 [CS5] ▼
7	48 [CS6] ▼
8	56 [CS7] ▼

Apply

The meaning of the interface is as follows

Configuration item	Description
Strict Priority (SP)	Strict priority mode

WRR	Weighted polling mode
Weights	Percentage of queues occupying WRR bandwidth

7.1.1.5 IP priority mapping

1. Click the "QOS> Queue Scheduling" menu in the navigation tree, enter the "Queue Scheduling" interface, and click "Apply" to complete the configuration, as shown in the figure below.

IP Precedence to Queue Mapping

IP Precedence	Queue
0	1 ▼
1	2 ▼
2	3 ▼
3	4 ▼
4	5 ▼
5	6 ▼
6	7 ▼
7	8 ▼

Apply

Queue to IP Precedence Mapping

Queue	IP Precedence
1	0 ▼
2	1 ▼
3	2 ▼
4	3 ▼
5	4 ▼
6	5 ▼
7	6 ▼
8	7 ▼

Apply

The meaning of the interface is as follows

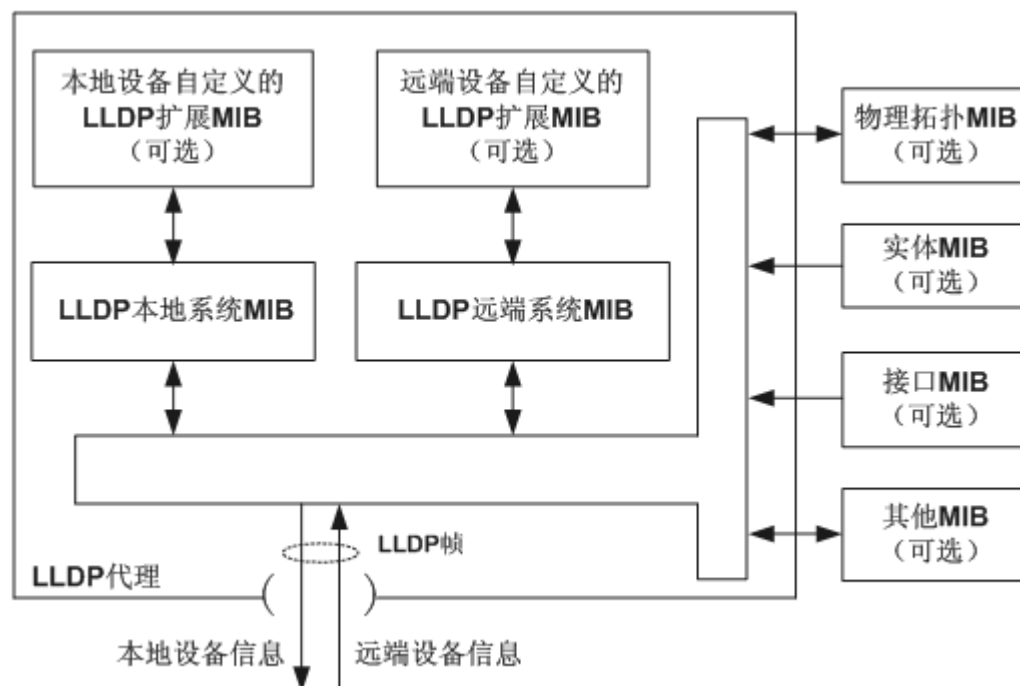
Configuration item	Description
Strict Priority (SP)	Strict priority mode
WRR	Weighted polling mode
Weights	Percentage of queues occupying WRR bandwidth

7.2 LLDP configuration

LLDP (Link Layer Discovery Protocol) is a link layer discovery protocol defined in IEEE 802.1ab. LLDP is a standard two-layer discovery method. It can organize the management address, device ID, interface ID and other information of the local device and publish it to its neighbor devices. After receiving the information, the neighbor device will use the standard The management information base MIB (Management Information Base) is stored in the form for the network management system to query and judge the communication status of the link.

LLDP can organize the information of the local equipment and publish it to its own remote equipment, and the local equipment saves the received remote equipment information in the form of standard MIB. The working principle is shown in the figure below.

LLDP principle block diagram as below:



The basic implementation principle of LLDP:

1. The LLDP module uses the LLDP agent to interact with the physical topology MIB, entity MIB, interface MIB, and other types of MIBs on the device to update its own LLDP local system MIB and local device-defined LLDP extended MIB.
2. Encapsulate the local device information into an LLDP frame and send it to the remote device. Receive LLDP frames sent by the remote device, update own LLDP remote system MIB, and the remote device's customized LLDP extended MIB.
3. By sending and receiving LLDP frames through the LLDP agent, the device clearly knows the information of the remote device, including which interface the remote device is connected to, and the MAC address of the remote device.
4. The LLDP local system MIB is used to store local device information. Including equipment ID, interface ID, system name, system description, interface description, network management address and other information.
5. LLDP remote system MIB is used to store remote device information. Including equipment ID, interface ID, system name, system description, interface description, network management address and other information.)
6. LLDP-MED is based on LLDP, and other organizations can extend it through LLDP-MED. The information found from the network equipment can assist in fault analysis and allow the management system to accurately understand the network topology

7.2.1 LLDP function configuration

Operating step:

1. Click the "Topology Discovery> LLDP> Function Configuration" menu in the navigation tree to

enter the "Function Configuration" interface, as shown in the figure below:

LLDP

状态 ☒ 开启

LLDP报文处理方式

☐ 过滤

☐ 转发

☒ 泛洪

发包周期 30 秒 (5 - 32767, 默认 30)

Hold Multiplier 4 (2 - 10, 默认 4)

重新初始化时延 2 秒 (1 - 10, 默认 2)

传输时延 2 秒 (1 - 8191, 默认 2)

LLDP-MED

快速启动重复计数 3 (1 - 10, 默认 3)

应用

The meaning of the interface as follows

Configuration item	Description
status	Turn on or Turn off LLDP protocol
LLDP Message processing method	When the LLDP protocol is closed, LLDP packet processing methods are divided into three types: "Filtering" (filtering), "Bridging" (forwarding), and "Flooding" (flooding)
Sending cycle	Default 30 seconds, range: 5-32768 seconds
Hold Multiplier	Transmission cycle product, default 4, range: 2-10, transmission cycle * transmission cycle product is not greater than 65535
Reinitialization Delay	Default is 2 seconds, range: 1-10 seconds
Transmission delay	Default is 2 seconds, range: 1-8191 seconds
Quick start repeat count	LLDP-MED port quick start repetition times Default 3, range: 1-10

The Ethernet packet encapsulated with LLDPDU (LLDP Data Unit) is called LLDP packet. TLV is a unit that composes LLDPDU, and each TLV represents a piece of information.

2.Fill in the corresponding configuration items.

3.Click "Apply" to complete the configuration.

7.2.2 Port Configuration

Operating Step:

1.Click the "Topology Discovery> LLDP> Port Configuration" menu in the navigation tree to enter the "Port Configuration" interface, as shown in the figure below.

Port Setting Table

☐	Entry	Port	Mode	Selected TLV
☐	1	GE1	Normal	802.1 PVID
☐	2	GE2	Normal	802.1 PVID
☐	3	GE3	Normal	802.1 PVID
☐	4	GE4	Normal	802.1 PVID
☐	5	GE5	Normal	802.1 PVID
☐	6	GE6	Normal	802.1 PVID
☐	7	GE7	Normal	802.1 PVID
☐	8	GE8	Normal	802.1 PVID
☐	9	GE9	Normal	802.1 PVID
☐	10	GE10	Normal	802.1 PVID
☐	11	GE11	Normal	802.1 PVID
☐	12	GE12	Normal	802.1 PVID
☐	13	GE13	Normal	802.1 PVID
☐	14	GE14	Normal	802.1 PVID
☐	15	GE15	Normal	802.1 PVID
☐	16	GE16	Normal	802.1 PVID
☐	17	GE17	Normal	802.1 PVID
☐	18	GE18	Normal	802.1 PVID
☐	19	GE19	Normal	802.1 PVID
☐	20	GE20	Normal	802.1 PVID
☐	21	GE21	Normal	802.1 PVID
☐	22	GE22	Normal	802.1 PVID
☐	23	GE23	Normal	802.1 PVID
☐	24	GE24	Normal	802.1 PVID
☐	25	GE25	Normal	802.1 PVID
☐	26	GE26	Normal	802.1 PVID
☐	27	GE27	Normal	802.1 PVID
☐	28	GE28	Normal	802.1 PVID

Edit

Interface meaning as follows:

Configuration item	description
port	Support for configuring multiple ports
Transceiver mode	Mode of sending and receiving LLDP packets
TLV selected	Selected TLV information, VLAN information

LLDP has the following four working modes. Transmit (transmit only): send only LLDP packets, Receive (receive only): receive only LLDP packets, Normal (transmit): both send and receive LLDP packets. Disable: Neither send nor receive LLDP packets.

2.Check the corresponding port and click "Modify" to enter the modify port setting page. Click "Apply" to complete the configuration, as shown in the figure below.

Edit Port Setting

The meaning of the interface as follows

Configuration item	Description
Port	Support for configuring multiple ports
Transceiver mode)	The mode of sending and receiving LLDP packets, Transmit (transmit only): send only LLDP packets, Receive (receive only): receive only LLDP packets, Normal (transceive): both send and receive LLDP packets. Disable: neither send nor receive LLDP packets
Optional TLV	Select TLV information, VLAN information
VLAN name	Select VLAN name information

7.2.3 Neighbor information

Click the "Topology Discovery> LLDP> Neighbor Information" menu in the navigation tree to enter the "LLDP Neighbor" interface, as shown in the figure below.

Local Port	Chassis ID Subtype	Chassis ID	Port ID Subtype	Port ID	System Name	Time to Live
GE1	MAC address	E0:D5:5E:69:C2:C5	MAC address	E0:D5:5E:69:C2:C5		3523
GE1	MAC address	B4:2E:99:0C:C4:D2	MAC address	B4:2E:99:0C:C4:D2		3048
GE1	MAC address	38:D5:47:AE:D4:61	MAC address	38:D5:47:AE:D4:61		2969

7.3 SNMP configuration

The Simple Network Management Protocol (SNMP) is a standard network management protocol widely used in TCP/IP networks. SNMP provides a method for managing equipment through a central computer (network management workstation) running network management software. The characteristics of SNMP are as follows:

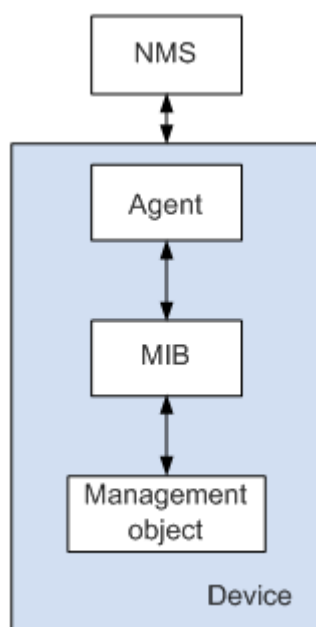
Simple: SNMP uses a polling mechanism to provide the most basic set of functions, suitable for use in a small, fast, and low-cost environment, and SNMP is carried by UDP packets, so it is supported

by most devices. Powerful: The goal of SNMP is to ensure that management information is transmitted at any two points, so that administrators can retrieve information, modify and troubleshoot any node on the network. The SNMP protocol is widely used in three main versions, namely SNMPv1, SNMPv2c and SNMPv3.

The SNMP system consists of four parts: the network management system NMS (Network Management System), the agent process, the managed object Management, and the management information base MIB

NMS manages equipment is as the network management center of the entire network, Each managed device contains Agent process, MIB and multiple managed objects residing on the device. The NMS interacts with the Agent running on the managed device, and the Agent completes the instructions of the NMS by operating the MIB on the device side.

SNMP management model



NMS

NMS plays the role of administrator in the network. It is a system that uses the SNMP protocol to manage/monitor network devices and runs on the NMS server. The NMS can send a request to the Agent on the device to query or modify one or more specific parameter values. The NMS can receive Trap messages sent by the Agent on the device to learn the current status of the managed device.)

Agent

Agent is an agent process in the managed device, used to maintain the information data of the managed device and respond to the request from the NMS, and report the management data to the NMS that sent the request. After receiving the request information from the NMS, the Agent completes the corresponding instructions through the MIB table and responds to the NMS with the operation result. When the device fails or other events, the device will actively send information to the NMS through the Agent, and report the current state change of the device to the NMS.

Management object

Management object refers to the managed object. Each device may contain multiple managed

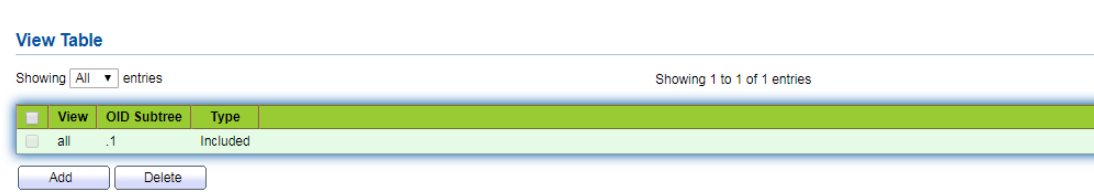
objects, which can be a piece of hardware (such as an interface board) in the device, or a collection of some hardware, software (such as routing protocols) and its configuration parameters.

MIB

MIB is a database that specifies the variables maintained by the managed device (that is, the information that can be queried and set by the Agent). MIB defines a series of attributes of the managed device in the database: the name of the object, the state of the object, the access authority of the object, and the data type of the object. Through MIB, the following functions can be completed: Agent can learn the current status information of the device by querying MIB. Agent can set the status parameters of the device by modifying the MIB.

7.3.1 View configuration

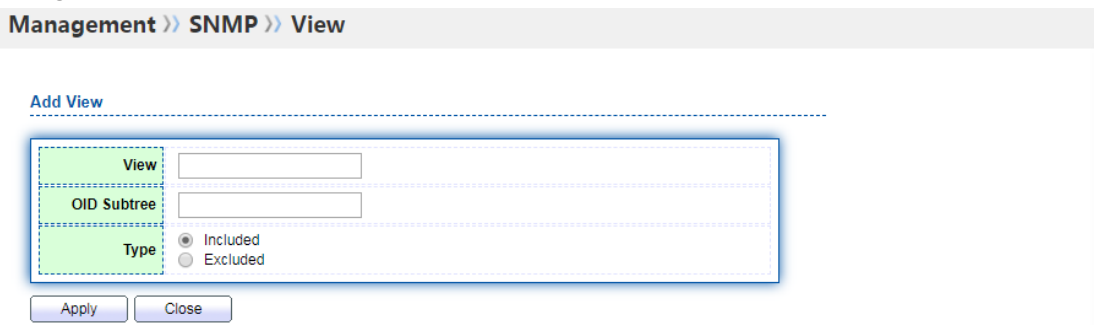
1. Click the "Device Management> SNMP Configuration> View Configuration" menu in the navigation tree to enter the "View Configuration" interface, as shown in the figure below.



The meaning of the interface as follows:

Description
View name
View OID
View type, "Included" or "Excluded"

2. Click "Add", fill in the corresponding configuration, and click "Apply" to complete the configuration.



7.3.2 Group Configuration

1. Click the "Device Management> SNMP Configuration> Group Configuration" menu in the navigation tree to enter the "Group Configuration" interface, as shown in the figure below.

Management >> SNMP >> Group

Group Table

Showing All entries Showing 0 to 0 of 0 entries

	Group	Version	Security Level	View		
				Read	Write	Notify

0 results

Configure SNMP View to associate a non-default view with a group.

Add Edit Delete

The meaning of the interface as follows

Configuration item	Description
Group	Group name
Version	Version, v1,v2,v3
Security Level	Security Level
View	divided into read view, write view, notification view

2.Click "Add", fill in the corresponding configuration, and click "Apply" to complete the configuration.

Add Group

Group

Version

☒ SNMPv1
☐ SNMPv2
☐ SNMPv3

Security Level

☒ No Security
☐ Authentication
☐ Authentication and Privacy

View

☒ Read
☐ Write
☐ Notify

all

all

all

Apply Close

7.3.3 Community Configuration

1.Click the "Device Management> SNMP Configuration> Community Configuration" menu in the navigation tree to enter the "Community Configuration" interface, as shown in the figure below.

Management >> SNMP >> Community

Community Table

Showing All entries Showing 1 to 1 of 1 entries

☐	Community	Group	View	Access
☐	public		all	Read-Only

The access right of a community is defined by a group under advanced mode.
Configure [SNMP Group](#) to associate a group with a community.

The meaning of the interface as follows

Configuration item	Description
Community	Community Name
Group	Group Name
View	View name
Access	Permission, "read-only" or "read-write".

2.Click "Add", fill in the corresponding configuration, and click "Apply" to complete the configuration.

Management >> SNMP >> Community

Add Community

Community

Type

☒ Basic
 ☐ Advanced

View

all

Access

☒ Read-Only
 ☐ Read-Write

Group

7.3.4 User Configuration

1.1. Click the "Device Management> SNMP Configuration> User Configuration" menu in the navigation tree to enter the "User Configuration" interface, as shown in the figure below.

Management >> SNMP >> User

User Table

Showing All entries Showing 0 to 0 of 0 entries

☐	User	Group	Security Level	Authentication Method	Privacy Method
0 results found.					

Configure [SNMP Group](#) to associate an SNMPv3 group with an SNMPv3 user.

The meaning of the interface as follows

Configuration Item	Description
User	Username

Group	Group name
Security Level	Security Level
Authentication	Authentication Mode
Privacy Method	Encryption Mode

2. Click "Add", fill in the corresponding configuration, and click "Apply" to complete the configuration.

Add User

User

Group

a ▼

Security Level

☒ No Security
☐ Authentication
☐ Authentication and Privacy

Authentication

Method

☒ None
☐ MD5
☐ SHA

Password

Privacy

Method

☒ None
☐ DES

Password

7.3.5 Engine ID Configuration.

1. Click the "Device Management > SNMP Configuration > Engine ID Configuration" menu in the navigation tree to enter the "Engine ID Configuration" interface, as shown in the figure below.

Management >> SNMP >> Engine ID

Local Engine ID

Engine ID

☐ User Defined
 (10 - 64 Hexadecimal Characters)

Remote Engine ID Table

Showing All ▼ entries

Showing 0 to 0 of 0 entries

Server Address	Engine ID
0 results found.	

3. Check "User Automatic Definition", fill in the corresponding ID value, and click "Apply" to complete the configuration.

7.3.6 Trap Configuration

1.Click the "Device Management> SNMP Configuration> Trap Configuration" menu in the navigation tree to enter the "Trap Configuration" interface, as shown in the figure below.

Configuration Item	Description
Authentication Failure	Authentication Error
Link Up / Down	Port Link Up/Down event
Cold Start	Cold start
Warm Start	Hot Start

The meaning of the interface as follows

Configuration Item	Description
Authen Failure	Authentication Error
Link Up/Down	Port Link Up/Down event
Cold start	Cold start
Warm start	Hot Start

2.Click "Apply" to complete the configuration.

7.3.7 Notification Configuration.

1.Click the "Device Management> SNMP Configuration> Notification Configuration" menu in the navigation tree to enter the "Notification Configuration" interface, as shown in the figure below.

Configuration Item	Description
Address type	Address type, "host name", "IPv4" or "IPv6"
Server address	Server address information
Version	SNMP version, v1 v2 v3
Type	Notification type, "Trap" or "Inform"
Community/User	Community or username
Security Level	Security Level
Server port number	Port number range 1-65535, default 162
Timeout	Server timeout time, range 1-300 seconds, default 15 seconds.
Retry	Retry interval, range 1-255 seconds, default 3 seconds.

The meaning of the interface as follows

Configuration Item	Description
Address type	Address type, "host name", "IPv4" or "IPv6"
Server address	Server address information
Version	SNMP version, v1 v2 v3
Type	Notification type, "Trap" or "Inform"
Community/User	Community or username
Security Level	Security Level
Server port number	Port number range 1-65535, default 162
Timeout	Server timeout time, range 1-300 seconds, default 15 seconds.
Retry	Retry interval, range 1-255 seconds, default 3 seconds.

2.Click "Add", fill in the corresponding configuration, and click "Apply" to complete the

configuration.

Management >> SNMP >> Notification

Add Notification

Address Type	☒ Hostname ☐ IPv4 ☐ IPv6
Server Address	Empty value is invalid.
Version	☒ SNMPv1 ☐ SNMPv2 ☐ SNMPv3
Type	☒ Trap ☐ Inform
Community / User	public ▾
Security Level	☒ No Security ☐ Authentication ☐ Authentication and Privacy
Server Port	☒ Use Default 162 (1 - 65535, default 162)
Timeout	☒ Use Default 15 Sec (1 - 300, default 15)
Retry	☒ Use Default 3 (1 - 255, default 3)

7.4 RMON Configuration

RMON (Remote Monitoring) is a MIB (Management Information Base) defined by IETF (Internet Engineering Task Force) and is an important enhancement to the MIB II standard. RMON is mainly used to monitor data traffic in a network segment or even the entire network, and is currently one of the widely used network management standards. RMON includes two parts: NMS (Network Management Station) and Agent running on each network device. RMON Agent runs on a network monitor or network probe, and tracks and counts various traffic information on the network segment connected to its port (such as the total number of packets on a network segment within a certain period of time, or the number of packets sent to a host). The total number of correct messages, etc.). The implementation of RMON is completely based on the SNMP architecture, which is compatible with the existing SNMP framework. RMON enables SNMP to monitor remote network devices more effectively and proactively, and provides an efficient means for monitoring the operation of subnets. RMON can reduce the communication traffic between the NMS and the agent (SNMP Agent), so that it can manage large-scale interconnected networks simply and effectively. RMON allows multiple monitors. It can collect data in two ways: Use a dedicated RMON probe to collect data, and NMS directly obtains management information from the RMON probe and controls network resources. In this way, all the information of RMON MIB can be obtained; RMON Agent can be directly implanted into network devices (routers, switches, HUBs, etc.) to make them become network facilities with RMON probe function. RMON NMS uses SNMP basic commands to exchange data information with SNMP Agent and collect network management information. However, this method is limited by device resources and generally cannot obtain all

data of RMON MIB. Most of them only collect information of four groups, which are alarm group, event group, history group and statistics group. The area series Ethernet switches implement RMON in the second method. RMON Agent is directly implanted in the Ethernet switch to become a network facility with RMON probe function. By running the SNMP Agent supporting RMON on the Ethernet switch, the network management station can obtain the overall traffic, error statistics, performance statistics and other information on the network segment connected to the Ethernet switch port to realize network management.

7.4.1 Port statistics

The statistical group information reflects the statistical value of each monitoring interface on the switch. The statistics group counts the cumulative information since the time the statistics group was created. The statistical information includes the number of network conflicts, the number of CRC check error packets, the number of too small (or oversized) data packets, the number of broadcast and multicast packets, the number of bytes received, and the number of packets received. Using the RMON statistical management function, you can monitor the port usage and count errors that occur in the port usage.

Operating Step

1. Click the "Device Management > RMON Configuration > Message Statistics" menu in the navigation tree to enter the "Message Statistics" interface, which mainly displays the statistics of packets related to each port, as shown in the figure below.

Management >> RMON >> Statistics

Statistics Table

Refresh Rate sec

	Entry	Port	Bytes Received	Drop Events	Packets Received	Broadcast Packets	Multicast Packets	CRC & Align Errors	Undersize Packets	Oversize Packets	Fragments	Jabbers	Collisions	Frames of 64 Bytes	Frames of 65 to 127 Bytes	Frames of 128 to 255 Bytes
☐	1	GE1	42508089	0	409815	250082	133995	0	0	0	0	0	0	234242	98780	677
☐	2	GE2	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	3	GE3	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	4	GE4	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	5	GE5	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	6	GE6	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	7	GE7	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	8	GE8	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	9	GE9	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	10	GE10	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	11	GE11	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	12	GE12	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	13	GE13	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	14	GE14	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	15	GE15	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	16	GE16	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	17	GE17	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	18	GE18	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	19	GE19	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	20	GE20	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	21	GE21	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	22	GE22	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	23	GE23	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	24	GE24	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	25	GE25	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	26	GE26	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	27	GE27	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	28	GE28	0	0	0	0	0	0	0	0	0	0	0	0	0	0
☐	29	LAG1	0	0	0	0	0	0	0	0	0	0	0	0	0	0

2. You can select the port, click "Clear", "Refresh" to complete the clearing and refreshing of the corresponding port statistics, and click "View" to enter the port view. As shown below.

View Port Statistics

Port	GE4
Refresh Rate	☒ None ☐ 5 sec ☐ 10 sec ☐ 30 sec
Received Bytes (Octets)	42592695
Drop Events	0
Received Packets	410628
Broadcast Packets Received	250497
Multicast Packets Received	134249
CRC & Align Errors	0
Undersize Packets	0
Oversize Packets	0
Fragments	0
Jabbers	0
Collisions	0
Frames of 64 Bytes	234695
Frames of 65 to 127 Bytes	98981
Frames of 128 to 255 Bytes	67926
Frames of 256 to 511 Bytes	1552
Frames Greater than 1024 Bytes	343

3.You can choose to specify the refresh frequency to automatically refresh the statistics.

7.4.2 Historical configuration

After the RMON history group is configured, the Ethernet switch will periodically collect network statistics. In order to facilitate processing, these statistics are temporarily stored to provide statistics on network segment traffic, error packets, broadcast packets, bandwidth utilization, etc. historical data. Using the historical data management function, you can set the device. The tasks to be set include: collecting historical data, collecting and saving the data of the designated port regularly.

Operating Steps

1.Click the "Device Management> RMON Configuration> History Configuration" menu in the navigation tree to enter the "historical configuration" interface, as shown in the figure below

Management >> RMON >> History

History Table

Showing All entries Showing 0 to 0 of 0 entries

	Entry	Port	Interval	Owner	Sample	
					Maximum	Current
0 results found.						

The SNMP service is currently disabled.
For RMON configuration to be effective, the [SNMP service](#) must be enabled.

The meaning of the interface as follows

Configuration Item	Description
Entry	Event group number
Port	Need statistics port
Interval	The sampling interval is between 1-3600, unit: second The default is 1800 seconds
Owner	owner
Maximum	The maximum number of samples is between 0-50, the default is 50
Current	Current sample number

Click "Add" to enter the history group configuration page and fill in the corresponding configuration items.

Management >> RMON >> History

Add History

Entry	1
Port	GE1 ▼
Max Sample	50 (1 - 50, default 50)
Interval	1800 (1 - 3600, default 1800)
Owner	

3.Click "Apply" to complete the configuration, as shown in the figure below.

Management >> RMON >> History

History Table

Showing All ▼ entries

Showing 1 to 1 of 1 entries

	Entry	Port	Interval	Owner	Sample	
					Maximum	Current
☐	1	GE1	1800		50	50

The SNMP service is currently disabled.
For RMON configuration to be effective, the [SNMP service](#) must be enabled.

7.4.3 Event configuration

The event group is used to define the event number and the processing method of the event. The events defined by the event group are mainly used in the alarm group configuration items and the events generated by the alarm trigger in the extended alarm group configuration items. There are several ways to process events: record the event in the log table; send a Trap message to the network management station; record the event in the log table and send a Trap message to the network management station; do nothing.

Operating Step

1.Click the "Device Management> RMON Configuration> Event Configuration" menu in the

navigation tree to enter the "Event Configuration" interface, as shown in the figure below.

Management >> RMON >> Event

Event Table

Showing All entries Showing 1 to 1 of 1 entries

	Entry	Community	Description	Notification	Time	Owner
☐	1		Default Description	None		

The SNMP service is currently disabled.
For RMON configuration to be effective, the [SNMP service](#) must be enabled.

Add Edit Delete View

The meaning of the interface as follows

Configuration Item	Description
Entry	Event group number
Community	Community name
Description	Description
Notification	Notice
Timer	Time
Owner	Owner

Click "Add" to enter the event group configuration page and fill in the corresponding configuration items

Add Event

Entry1

Notification

☒ None

☐ Event Log

☐ Trap

☐ Event Log and Trap

CommunityDefault Community

DescriptionDefault Description

Owner

应用

关闭

3.Click "Add" to complete the configuration, as shown in the figure below.

Event Table

显示
All
▼
条目

☐	Entry	Community	Description	Notification	Time	Owner
☐	1	Default Community	Default Description	Event Log and Trap		

The SNMP service is currently disabled.
For RMON configuration to be effective, the [SNMP service](#) must be enabled.

添加
修改
删除
View

7.4.4 Alarm configuration.

RMON alarm management can monitor specified alarm variables (such as port statistics). When the value of the monitored data crosses the defined threshold in the corresponding direction, an alarm event will be generated, and then the corresponding processing method will be performed according to the event definition. deal with. The definition of the event is implemented in the event group. After the user defines the alarm entry, the system processes the alarm entry as follows: The defined alarm variable alarm-variable is sampled at the defined time interval sampling-time; the sampled value is compared with the set threshold, once it exceeds The threshold value triggers the corresponding event.

Click the "Device Management> RMON Configuration> Alarm Configuration" menu in the navigation tree to enter the "Alarm Configuration" interface, as shown in the figure below.

Management >> RMON >> Alarm

Alarm Table

Showing All
▼
entries
Showing 0 to 0 of 0 entries

☐	Entry	Port	Counter		Sampling	Interval	Owner	Trigger	Rising		Falling	
			Name	Value					Threshold	Event	Threshold	Event
0 results found.												

The SNMP service is currently disabled.
For RMON configuration to be effective, the [SNMP service](#) must be enabled.

Add
Edit
Delete

The meaning of the interface as follows

Configuration Item	Description
Entry	Alarm Group Number
Port	Enter the required statistics port
Counter	Alarm Sampling Parameters
Interval	The sampling interval is between 1-2147483647, unit: second, default 100 seconds
Sampling	Sampling type Absolute and delete
Owner	Owner
Threshold (Rising)	The rising edge threshold is between 0-2147483647
Event(Rising)	Event group index, when an alarm is triggered, the corresponding event of

	the event group will be activated
Threshold (Falling)	The falling edge threshold is between 0-21474836475
Event(Falling)	Event group index, when an alarm is triggered, the corresponding event of the event group will be activated

2. Click "Add" to enter the alarm group configuration page and fill in the corresponding configuration items.

Management >> RMON >> Alarm

Add Alarm

Entry	1	
Port	GE1 ▼	
Counter	Drop Events ▼	
Sampling	☒ Absolute ☐ Delta	
Interval	100	Sec (1 - 2147483647, default 100)
Owner		
Trigger	☒ Rising ☐ Falling ☐ Rising and Falling	
Rising		
Threshold	100	(0 - 2147483647, default 100)
Event	1 - Default Description ▼	
Falling		
Threshold	20	(0 - 2147483647, default 20)
Event	1 - Default Description ▼	

3. Click "Apply" to complete the configuration, as shown in the figure below.

Alarm Table											
显示 All ▼ 条目		Showing 1 to 1 of 1 entries									
Entry	端口	Counter		Sampling	Interval	Owner	Trigger	Rising		Falling	
		Name	Value					Threshold	Event	Threshold	Event
1	GE1	DropEvents	0	Absolute	100		Rising	100	Default Description	20	Default Description

The SNMP service is currently disabled.
For RMON configuration to be effective, the [SNMP service](#) must be enabled.

7.5 DNS Set Up

DNS is the abbreviation of Domain Name System (DomainName System), which is used to name computers and network services organized into a domain hierarchy. A domain name is composed of a series of words or abbreviations separated by dots. Each domain name corresponds to a unique IP address. There is a one-to-one correspondence between domain names and IP addresses on the Internet. DNS is the server for domain name resolution. DNS naming is used in TCP/IP

networks such as the Internet to find computers and services through user-friendly names. DNS is a core service of the Internet. It serves as a distributed database that can map domain names and IP addresses to each other.

Operating Step:

1.Click the "Network Configuration> DNS Settings" menu in the navigation tree to enter the "DNS Settings" interface, as shown in the figure below.

Network >> DNS

DNS Configuration

DNS Status

☐ Disable

☒ Enable

DNS Default Name

(1 to 255 alphanumeric characters)

Apply

DNS Server Configuration

PreferenceDNS Server

0 results found.

Add

Delete

The meaning of the interface is as follows

Configuration item	Description
DNS Status	DNS switch
DNS default name	Enter DNS default name

2. Click "Add" to set DNS server.

Network >> DNS

Add DNS Server

IPv4/IPv6 Address

Apply

Close

3. Click "Settings" to complete the configuration, as shown in the figure below.

DNS Server Configuration

PreferenceDNS Server

1114.114.114.114

Add

Delete

7.6 System time.

The system time function is mainly used to configure the device system time, select the system time source, and configure the summer time.

Operating Step

1.Click the "Network Configuration> System Time" menu in the navigation tree to enter the

"System Time" interface, as shown in the figure below.

Network >> System Time

Source

☐ SNTP
☐ From Computer
☒ Manual Time

Time Zone

UTC +8:00 ▼

SNTP

Address Type

☒ Hostname
☐ IPv4

Server Address

Server Port

(1 - 65535, default 123)

Manual Time

Date

YYYY-MM-DD
 HH:MM:SS

Daylight Saving Time

Type

☒ None
☐ Recurring
☐ Non-recurring
☐ USA
☐ European

Offset

Min (1 - 1440, default 60)

Recurring

From: Day Week Month Time
 To: Day Week Month Time

Non-recurring

From: YYYY-MM-DD HH:MM
 To: YYYY-MM-DD HH:MM

Operational Status

Current Time

2020-01-01 14:31:48 UTC+8

The meaning of the interface as follows

Configuration Item	Description
Time source	Used to select the time source, can be configured by SNTP protocol, PC or manually
Time zone	Set time zone
Address type	Host name or IPv4 address (set when the time source is SNTP)
Server address	Server Address (set when the time source is SNTP)
Server port number	Server port number (set when the time source is SNTP)
Date	Date information, year-month-day (time source is manually set)
Time	Time information, hour-minute-second (time source is manually set)
Type	Daylight saving time types are divided into None, cyclical, non-cyclical, United States, Europe
Compensation time	Summer time compensation time
Cycle	Daylight Saving Time Cycle Mode Setting
Acyclic	Daylight Saving Time Acyclic Mode Setting

8.System Maintenance

8.1.1 Configuration Management

Click the "Device Management> Configuration Management> Upgrade/Backup" menu in the navigation tree to enter the "Upgrade/Backup" interface, as shown in the figure below.

Management >> Configuration >> Upgrade

Action	☒ Upgrade ☐ Backup
Method	☐ TFTP ☒ HTTP
Configuration	☒ Running Configuration ☐ Startup Configuration ☐ Backup Configuration ☐ RAM Log ☐ Flash Log
Filename	选择文件 未选择任何文件

a. To upgrade the configuration file operation steps, check "Upgrade" for the action, select the upgrade method "TFTP" or "HTTP", select the configuration file that needs to be upgraded (the corresponding server is required for the TFTP mode), and select the corresponding configuration file. Click "Apply" as shown below.

Management >> Configuration >> Upgrade

Action	☒ Upgrade ☐ Backup
Method	☐ TFTP ☒ HTTP
Configuration	☒ Running Configuration ☐ Startup Configuration ☐ Backup Configuration ☐ RAM Log ☐ Flash Log
Filename	选择文件 未选择任何文件

b. Operation steps for backing up the configuration file, check "Backup" for the action, select the download mode "TFTP" or "HTTP", and select the configuration file or log to be downloaded (the TFTP mode needs to fill in the corresponding server). Click "Apply" as shown below.

Management >> Configuration >> Upgrade

Action	☒ Upgrade ☐ Backup
Method	☐ TFTP ☒ HTTP
Configuration	☒ Running Configuration ☐ Startup Configuration ☐ Backup Configuration ☐ RAM Log ☐ Flash Log
Filename	选择文件 未选择任何文件

8.1.2 Save Configuration

Operation Method

1. Click the "Device Management > Configuration Management > Save Configuration" menu in the navigation tree, enter the "Save Configuration" interface, select the source file and target file to be saved, click "Apply" to finish saving, and click "Restore Factory Settings", the configuration can be restored to factory settings, as shown in the figure below

Management >> Configuration >> Save Configuration

Source File	☒ Running Configuration ☐ Startup Configuration ☐ Backup Configuration
Destination File	☒ Startup Configuration ☐ Backup Configuration



Note:

1. Click "Restore Factory Settings", you need to click "Restart Device" again, the device will return to factory settings.
2. "Running configuration" can be saved as "Startup configuration" or "Backup configuration", "Backup configuration" can be saved as "Startup configuration" or "Running configuration", "Startup configuration" can be saved as "Backup configuration" or "Running configuration".

2. Click "Save" in the upper right corner of the page, and follow the prompts to save the running configuration as the startup configuration, as shown in the figure below.

Save running configuration to startup configuration. Do you want to continue?

OK

Cancel

8.2 Restart the device

Click "Restart" in the upper right corner of the page and follow the prompts to restart the device, as shown in the figure below

Reboot the system and unsaved changes in the configuration will be lost. Do you want to continue?

OK

Cancel

8.3 Firmware management

Operating Step:

1. Click the "Device Management > Firmware Management > Upgrade/Backup" menu in the navigation tree to enter the "Upgrade/Backup" Interface, Action check "Upgrade", select download method "TFTP" or "HTTP", and select the system file (xx.bix) to be upgraded. Click "Apply" as shown below.

Management >> Firmware >> Upgrade

Action	☒ Upgrade
Method	☐ TFTP ☒ HTTP
Filename	选择文件 未选择任何文件
Apply	

9. POE Management Settings

9.1.1 POE Port Configuration

Click the "POE Settings> POE Port Configuration" menu in the navigation tree, and enter the "POE Port Configuration" interface, as shown in the figure below.

POE Setting >> POE Port Setting

System info

System Power(mW) 0

System Temperature(C) 52

Refresh Rate
☐ None
☒ 5 sec
☐ 10 sec
☐ 30 sec

Port Setting Table

	Entry	Port	PortEnable	Status	Type	Level	Actual Power(mW)	Voltage(V)	Current(mA)
☐	1	GE1	Enabled	Off	AF(U)	0	N/A	N/A	N/A
☐	2	GE2	Enabled	Off	AF(U)	0	N/A	N/A	N/A
☐	3	GE3	Enabled	Off	AF(U)	0	N/A	N/A	N/A
☐	4	GE4	Enabled	Off	AF(U)	0	N/A	N/A	N/A
☐	5	GE5	Enabled	Off	AF(U)	0	N/A	N/A	N/A
☐	6	GE6	Enabled	Off	AF(U)	0	N/A	N/A	N/A
☐	7	GE7	Enabled	Off	AF(U)	0	N/A	N/A	N/A
☐	8	GE8	Enabled	Off	AF(U)	0	N/A	N/A	N/A
☐	9	GE9	Enabled	Off	AF(U)	0	N/A	N/A	N/A
☐	10	GE10	Enabled	Off	AF(U)	0	N/A	N/A	N/A
☐	11	GE11	Enabled	Off	AF(U)	0	N/A	N/A	N/A
☐	12	GE12	Enabled	Off	AF(U)	0	N/A	N/A	N/A
☐	13	GE13	Enabled	Off	AF(U)	0	N/A	N/A	N/A
☐	14	GE14	Enabled	Off	AF(U)	0	N/A	N/A	N/A
☐	15	GE15	Enabled	Off	AF(U)	0	N/A	N/A	N/A
☐	16	GE16	Enabled	Off	AF(U)	0	N/A	N/A	N/A
☐	17	GE17	Enabled	Off	AF(U)	0	N/A	N/A	N/A
☐	18	GE18	Enabled	Off	AF(U)	0	N/A	N/A	N/A
☐	19	GE19	Enabled	Off	AF(U)	0	N/A	N/A	N/A
☐	20	GE20	Enabled	Off	AF(U)	0	N/A	N/A	N/A
☐	21	GE21	Enabled	Off	AF(U)	0	N/A	N/A	N/A

Operating Step

1. Select the corresponding port "v", click "Modify" to enter a port setting page, and choose whether to enable the POE intelligent management of a port.

POE Setting >> POE Port Setting

Edit Port Setting

Port GE1

PortEnable ☐ Enable

Apply Close

2. Click "Open"-"Apply" to complete the configuration, as shown in the figure below

POE Setting >> POE Port Setting

Edit Port Setting

Port GE1

PortEnable ☐ Enable

Apply Close



- 1