Dahua Gigabit Industrial Managed Switch

Web Config Manual

V1.0.0

Zhejiang Dahua Vision Technology Co., Ltd.

Cybersecurity Recommendations

Mandatory actions to be taken towards cybersecurity

1. Change Passwords and Use Strong Passwords:

The number one reason systems get “hacked” is due to having weak or default passwords. It is recommended to change default passwords immediately and choose a strong password whenever possible. A strong password should be made up of at least 8 characters and a combination of special characters, numbers, and upper and lower case letters.

2. Update Firmware

As is standard procedure in the tech-industry, we recommend keeping NVR, DVR, and IP camera firmware up-to-date to ensure the system is current with the latest security patches and fixes.

“Nice to have” recommendations to improve your network security

1. Enable HTTPS/SSL:

Set up an SSL Certificate to enable HTTPS. This will encrypt all communication between your devices and recorder.

2. Forward Only Ports You Need:

● Only forward the HTTP and TCP ports that you need to use. Do not forward a huge range of numbers to the device. Do not DMZ the device's IP address.

● You do not need to forward any ports for individual cameras if they are all connected to a recorder on site; just the NVR is needed.

3. Limit Features of Guest Accounts:

If your system is set up for multiple users, ensure that each user only has rights to features and functions they need to use to perform their job.

4. SNMP:

Disable SNMP if you are not using it. If you are using SNMP, you should do so only temporarily, for tracing and testing purposes only.

5. Multicast:

Multicast is used to share video streams between two recorders. Currently there are no known issues involving Multicast, but if you are not using this feature, deactivation can enhance your network security.

6. Check the Log:

If you suspect that someone has gained unauthorized access to your system, you can check the system log. The system log will show you which IP addresses were used to login to your system and what was accessed.

7. Physically Lock Down the Device:

Ideally, you want to prevent any unauthorized physical access to your system. The best way to achieve this is to install the recorder in a lockbox, locking server rack, or in a room that is behind a lock and key.

Foreword

General

This Web Config Manual (hereinafter referred to be "the Manual"), introduces operations on web interface of Gigabit Industrial Managed Switch.

Models

Name	Model
Gigabit Industrial Managed Switch with 8 RJ45 Ports, 2 Fiber Ports	DH-PFS4210-8GT-DP
Gigabit Industrial Managed Switch with 6 RJ45 Ports, 4 Fiber Ports	DH-PFS4410-6GT-DP

Safety Instructions

The following categorized signal words with defined meaning might appear in the Manual.

Signal Words	Meaning
 DANGER	Indicates a high potential hazard which, if not avoided, will result in death or serious injury.
 WARNING	Indicates a medium or low potential hazard which, if not avoided, could result in slight or moderate injury.
 CAUTION	Indicates a potential risk which, if not avoided, could result in property damage, data loss, lower performance, or unpredictable result.
 ELECTRICITY	Indicates dangerous high voltage. Take care to avoid coming into contact with electricity.
 LASER BEAM	Indicates a laser radiation hazard. Take care to avoid exposure to a laser beam.
 ESD	Electrostatic Sensitive Devices. Indicates a device that is sensitive to electrostatic discharge.
 TIPS	Provides methods to help you solve a problem or save you time.
 NOTE	Provides additional information as the emphasis and supplement to the text.

Revision History

No.	Version	Revision Content	Release Time
1	V1.0.0	First Release.	May 22, 2018

Privacy Protection Notice

As the device user or data controller, you might collect personal data of others' such as face, fingerprints, car plate number, Email address, phone number, GPS and so on. You need to be in compliance with the local privacy protection laws and regulations to protect the legitimate rights and interests of other people by implementing measures include but not limited to: providing clear and visible identification to inform data subject the existence of surveillance area and providing related contact.

About the Manual

- The Manual is for reference only. If there is inconsistency between the Manual and the actual product, the actual product shall prevail.
- We are not liable for any loss caused by the operations that do not comply with the Manual.
- The Manual would be updated according to the latest laws and regulations of related regions. For detailed information, see the paper User's Manual, CD-ROM, QR code or our official website. If there is inconsistency between paper User's Manual and the electronic version, the electronic version shall prevail.
- All the designs and software are subject to change without prior written notice. The product updates might cause some differences between the actual product and the Manual. Please contact the customer service for the latest program and supplementary documentation.
- There still might be deviation in technical data, functions and operations description, or errors in print. If there is any doubt or dispute, please refer to our final explanation.
- Upgrade the reader software or try other mainstream reader software if the Guide (in PDF format) cannot be opened.
- All trademarks, registered trademarks and the company names in the Manual are the properties of their respective owners.
- Please visit our website, contact the supplier or customer service if there is any problem occurred when using the device.
- If there is any uncertainty or controversy, please refer to our final explanation.

Important Safeguards and Warnings

The Manual helps you to use our product properly. To avoid danger and property damage, read the Manual carefully before using the product, and we highly recommend you to keep it well for future reference.

Operating Requirements

- Do not expose the device directly to the sunlight, and keep it away from heat.
- Do not install the device in the damp environment, and avoid dust and soot.
- Make sure the device is in horizontal installation, and install the device on solid and flat surface to avoid falling down.
- Avoid liquid spattering on the device. Do not place object full of liquid on the device to avoid liquid flowing into the device.
- Install the device in the well-ventilated environment. Do not block the air vent of the device.
- Use the device at rated input and output voltage.
- Do not dissemble the device without professional instruction.
- Transport, use, and store the device in allowed ranges of humidity and temperature.

Power Supply Requirements

- Use the battery properly to avoid fire, explosion, and other dangers.
- Replace the battery with battery of the same type.
- Use locally recommended power cord in the limit of rated specifications.
- Use the standard power adapter. We will assume no responsibility for any problems caused by nonstandard power adapter.
- The power supply shall meet the SELV requirement. Use the power supply that conforms to Limited Power Source, according to IEC60950-1. Refer to the device label.
- Adopt GND protection for I-type device.
- The coupler is the disconnecting apparatus. Keep it at the angle for easy to operate.

Table of Contents

1 Overview

The Gigabit Industrial Managed Switch supports web access. You can visit the switch on web browser, and configure and manage the switch.

2 Login the Switch

Before login, make sure:

- You already configure the IP address of the switch. By default, the IP address of VLAN 1 is 192.168.1.110.
- The PC with web browser is connected to the network, and the PC can ping the switch successfully.

Step 1 Input the IP address of the switch in the address bar of the web browser. The IP address is 192.168.1.110 by default, and press **Enter** key on the keyboard.
See Figure 2-1 for login interface.

Figure 2-1 Web login interface

Step 2 Input user name and password. The user name and the password are “admin” by default.

Step 3 Select the language.

Step 4 Click **Login**.
The web service interface is displayed.

NOTE

After first time login, you need to modify the password. The new password can be set from 8 characters through 32 characters and contains at least two types from number, letter, and special characters (excluding"'", """, ";", ":" and "&"). Modify the password in time.

3 General Settings

3.1 Device Information

You can view the Name, Device Type, Serial Number, and Software Version of the device. And you can view the port status and port information.

Select **General > Device Information**, and you can view the System Information and Port State Overview. See Figure 3-1. In Port Status Overview, if the port is displayed as green, it is connected successfully. And if the port is displayed as white, it is not connected. See Table 3-1 for details about port information.

Figure 3-1 Device information

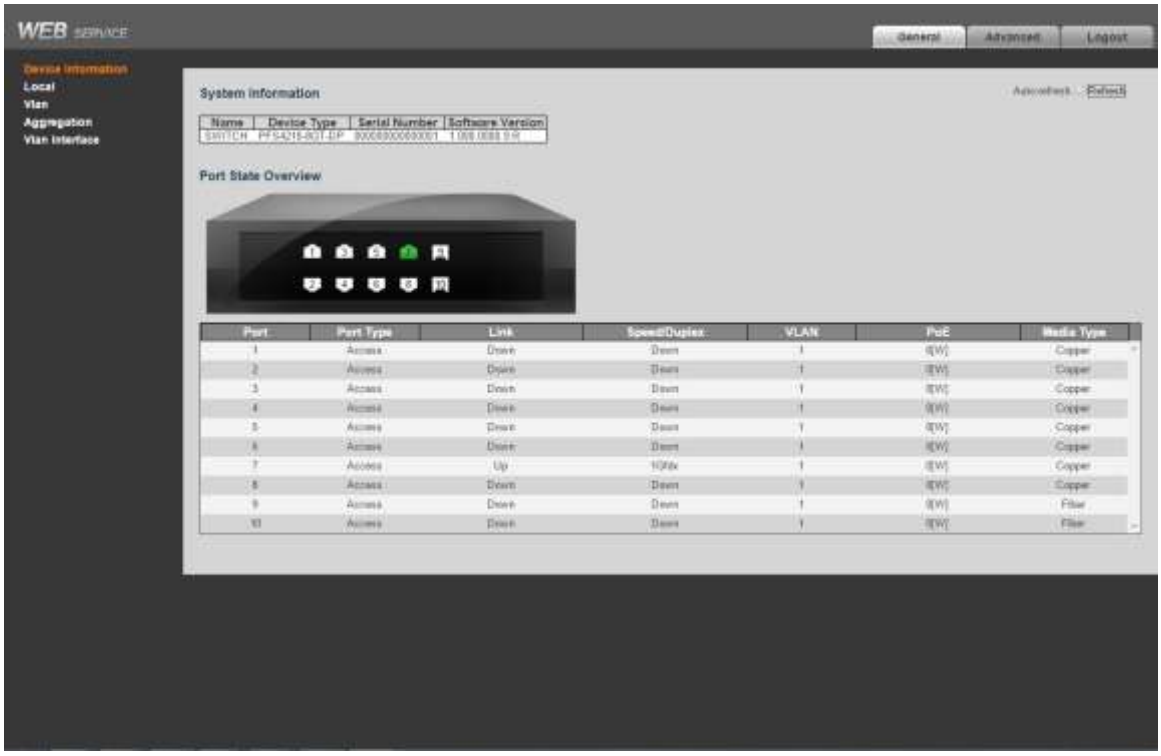


Table 3-1 Port information

Parameter	Description
Port	Display all the ports. NOTE This switch contains 10 ports. Port quantity might vary depending on the model you purchased, and the actual product shall govern.
Port Type	Three types: Access, Hybrid, and Trunk.
Link	Two link states: Up, Down. Up indicated the port is connected successfully, and Down indicates the port is not connected.
Speed/Duplex	Display the port rate and the duplex mode.
VLAN	Display the port VLAN. By default, it is VLAN 1.
PoE	Display the PoE power of the port.

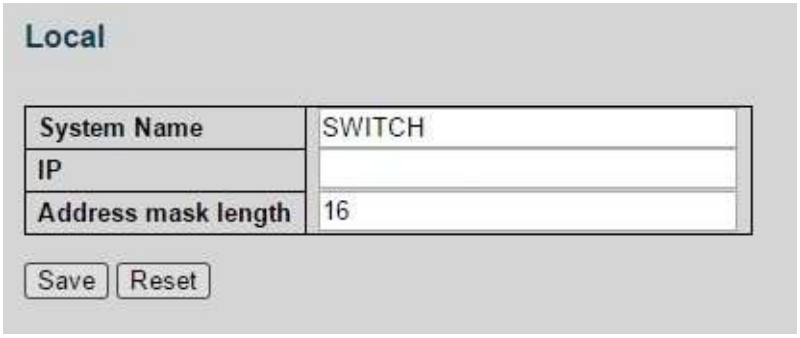
Parameter	Description
Media Type	Two media types: Copper, Fiber. Copper is the RJ45 port, and Fiber is the fiber port.

3.2 Local

You can set the system name, IP address, and address mask length.

Select **General > Local**, and the Local interface is displayed. See Figure 3-2.

Figure 3-2 Local



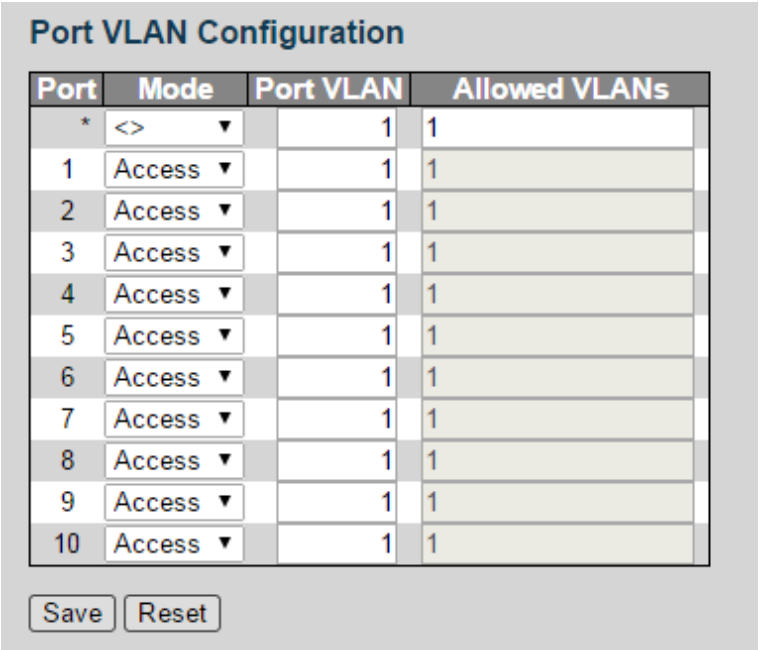
3.3 VLAN

Add the port to the VLAN, and configure the VLAN. By default, the port belongs to VLAN1.

Step 1 Select **General > Vlan**.

VLAN interface is displayed. See Figure 3-3.

Figure 3-3 Port VLAN configuration



Step 2 Configure the port VLAN parameters. See Table 3-2.

Table 3-2 Port VLAN configuration parameter

Parameter	Description
Port	Display all the ports.
Mode	Three modes: Access, Hybrid, and Trunk.

Parameter	Description
Port VLAN	Add the port to a VLAN. By default, the port belongs to VLAN 1. It ranges from 1 through 4094.
Allowed VLANs	Set the allowed VLAN.

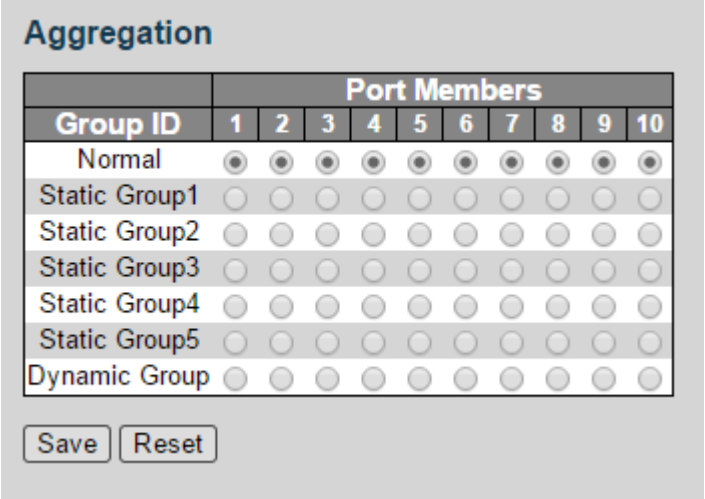
Step 3 Click **Save**.

3.4 Aggregation

Add the port to the aggregation. There are two types of aggregations: static aggregation and dynamic aggregation. See “4.1.5 Aggregation” for details.

Select **General > Aggregation**, and the Aggregation interface is displayed. See Figure 3-4.

Figure 3-4 Aggregation



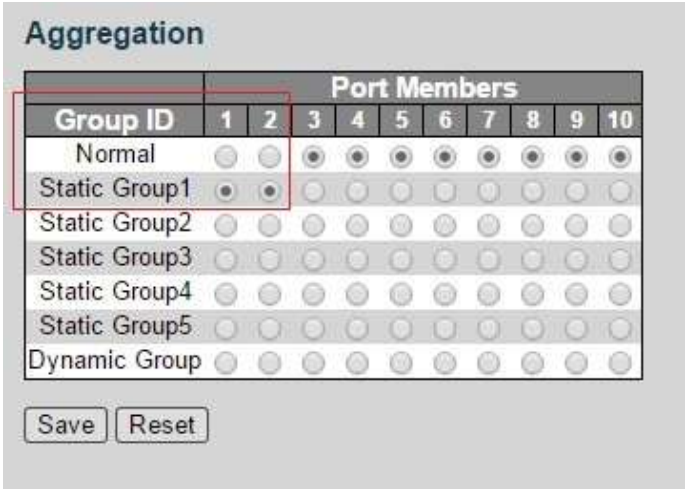
3.4.2 Static Aggregation Configuration

Step 1 Add the port member to the static group. For example, add port 1 and port 2 to Static Group 1. See Figure 3-5.

NOTE

Up to five static groups can be set at the same time.

Figure 3-5 Static group



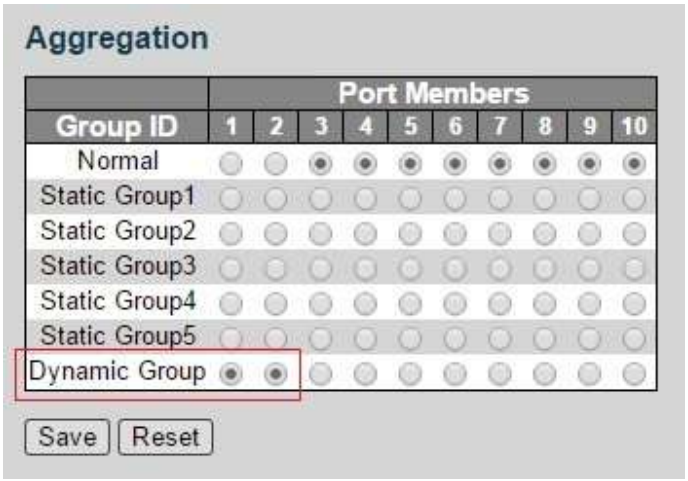
Step 2 Click **Save**.

The port 1 and port 2 form the logical port.

3.4.3 Dynamic Aggregation Configuration

Step 1 Add the port member to the dynamic group. For example, add port 1 and port 2 to Dynamic Group. See Figure 3-6.

Figure 3-6 Dynamic group



Step 2 Click **Save**.

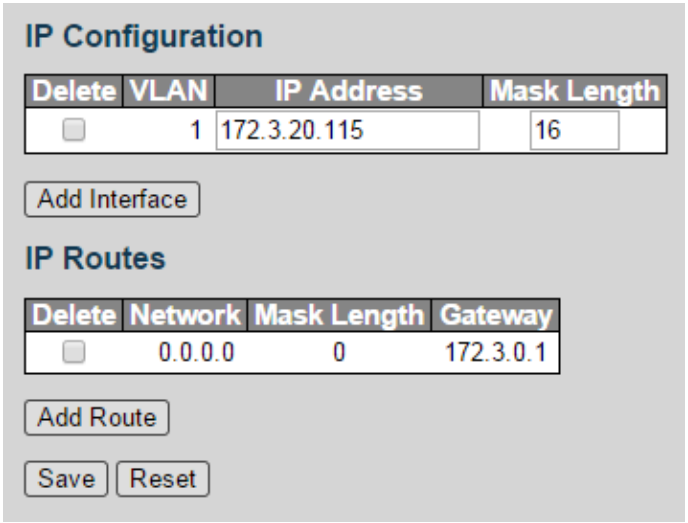
3.5 VLAN Interface

You can add the IP address for VLAN interface, and add new IP route. See “4.1.1.2 VLAN Interface” for configuration details.

Step 1 Select **General > Vlan Interface**.

VLAN interface is displayed. See Figure 3-7.

Figure 3-7 VLAN interface

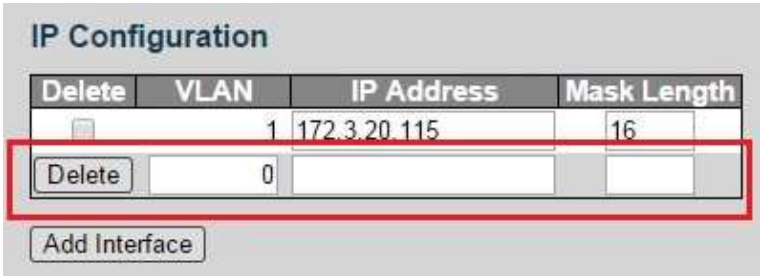


Step 2 Add the VLAN interface.

1) Click **Add Interface**.

A new record is added. See Figure 3-8.

Figure 3-8 VLAN interface



2) Set the parameters. See Table 3-3.

Table 3-3 VLAN interface

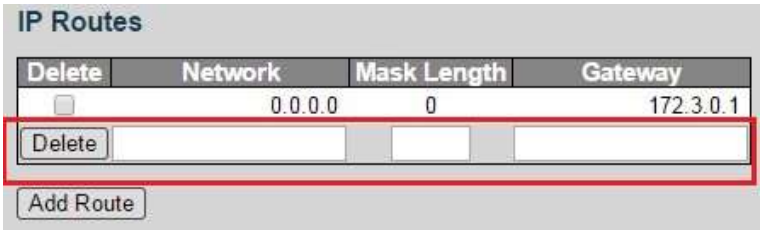
Parameter	Description
VLAN	Input VLAN number.
IP Address	Set the IP address of the VLAN interface.
Mask Length	Set the mask length of the VLAN interface.

Step 3 Add the IP route.

1) Click **Add Routes**.

A new record is added. See Figure 3-9.

Figure 3-9 IP routes



2) Set the parameters. See Table 3-4.

Table 3-4 IP routes

Parameter	Description
Network	It is the destination address of the IP packet.
Mask Length	Mask length, with destination address, is to identify the IP address of the destination host or the route. After logical AND between destination address and network mask, you can get the IP address of the destination host or the route.
Gateway	The gateway IP address of the route.

Step 4 Click **Save**.

4 Advanced Settings

4.1 Configuration

4.1.1 System

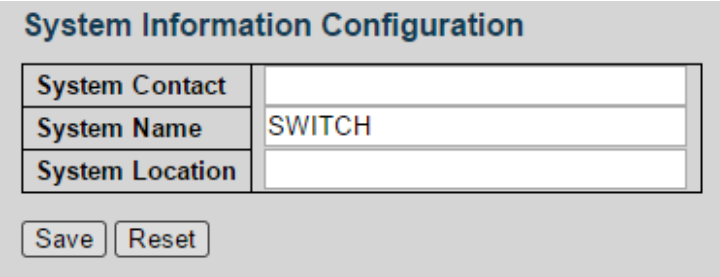
4.1.1.1 Information

You can set the system contact, system name, and system location.

Step 1 Select **Advanced > Configuration > System > Information**.

The Information interface is displayed. See Figure 4-1.

Figure 4-1 System information configuration



Step 2 Set the System Contact, System Name, and System Location.

Step 3 Click **Save**.

4.1.1.2 VLAN Interface

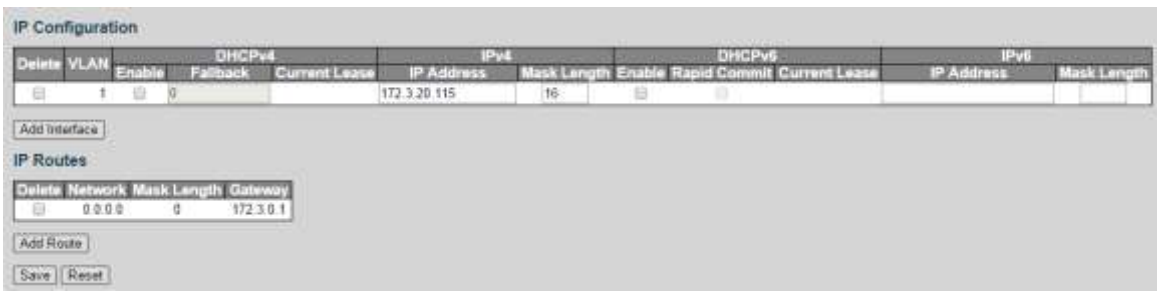
The hosts belong to different VLANs cannot communicate. Route or the layer 3 switch is needed for forwarding. The switch supports layer 3 forwarding through VLAN interface.

VLAN interface is the virtual interface of layer 3 mode, for layer 3 communication between the VLANs. It is not the physical entity on the device. Every VLAN is related to a VLAN interface, and the VLAN interface can forward packet for the VLAN. Generally, because the VLAN can isolate the broadcasting domain, every VLAN corresponds to a network segment. VLAN interface is the gateway of the network segment, and it supports layer 3 forwarding for the mesaage based on IP address.

Step 1 Select **Advanced > Configuration > System > Vlan Interface**.

VLAN interface is displayed. See Figure 4-2.

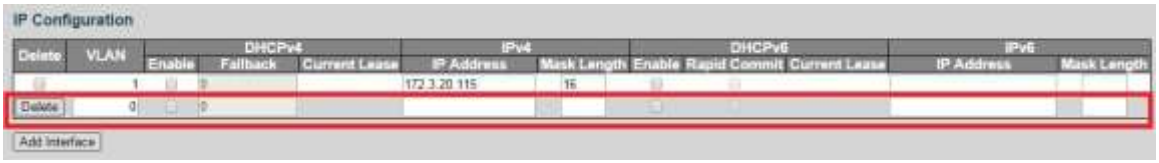
Figure 4-2 VLAN interface



Step 2 Add the VLAN interface.

1) Click **Add Interface**.
A new record is added. See Figure 4-3.

Figure 4-3 VLAN interface



2) Set the parameters. See Table 4-1.

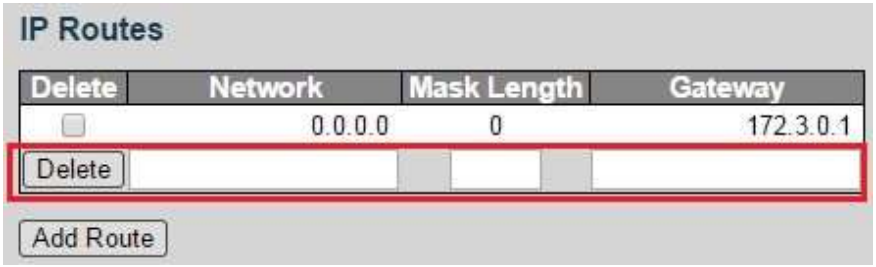
Table 4-1 VLAN interface

Parameter	Sub-parameter	Description
VLAN	-	Input VLAN number.
IPv4	IP Address	Set the IP address of the VLAN interface.
	Mask Length	Set the mask length of the IP address.

Step 3 Add IP route.

1) Click **Add Route**.
A new record is added. See Figure 4-4.

Figure 4-4 IP routes



2) Set the parameters. See Table 4-2.

Table 4-2 IP routes

Parameter	Description
Network	It is the destination address of the IP packet.
Mask Length	Mask length, with destination address, is to identify the IP address of the destination host or the route. After logical AND between destination address and network mask, you can get the IP address of the destination host or the route.
Gateway	The gateway IP address of the route.

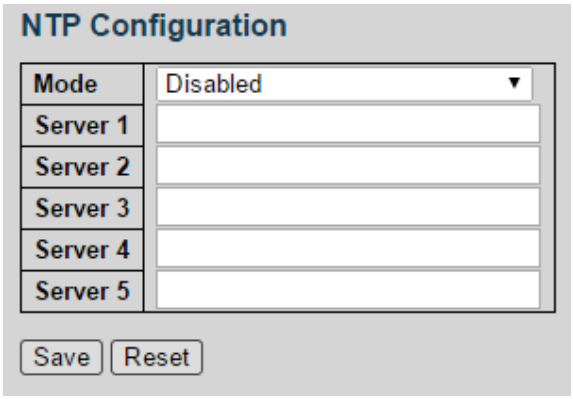
Step 4 Click **Save**.

4.1.1.3 NTP

Enable NTP function, and the switch can synchronize with the network time automatically.。

Step 1 Select **Advanced > Configuration > System > NTP**.
NTP Configure interface is displayed. See Figure 4-5.

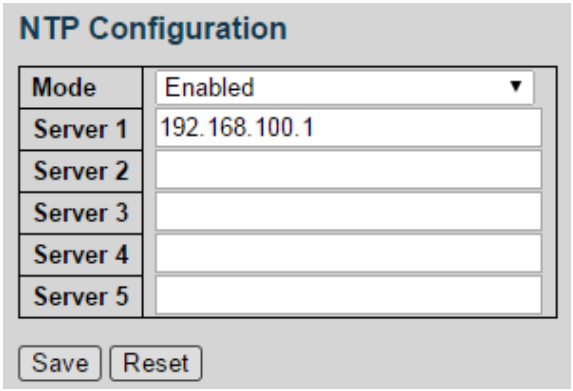
Figure 4-5 NTP configuration (1)



Step 2 Select the mode as **Enabled** to enable the NTP service. By default, the mode is **Disabled**.

Step 3 Set the IP address of the NTP server. See Figure 4-6.

Figure 4-6 NTP configuration (2)



Step 4 Click **Save**.

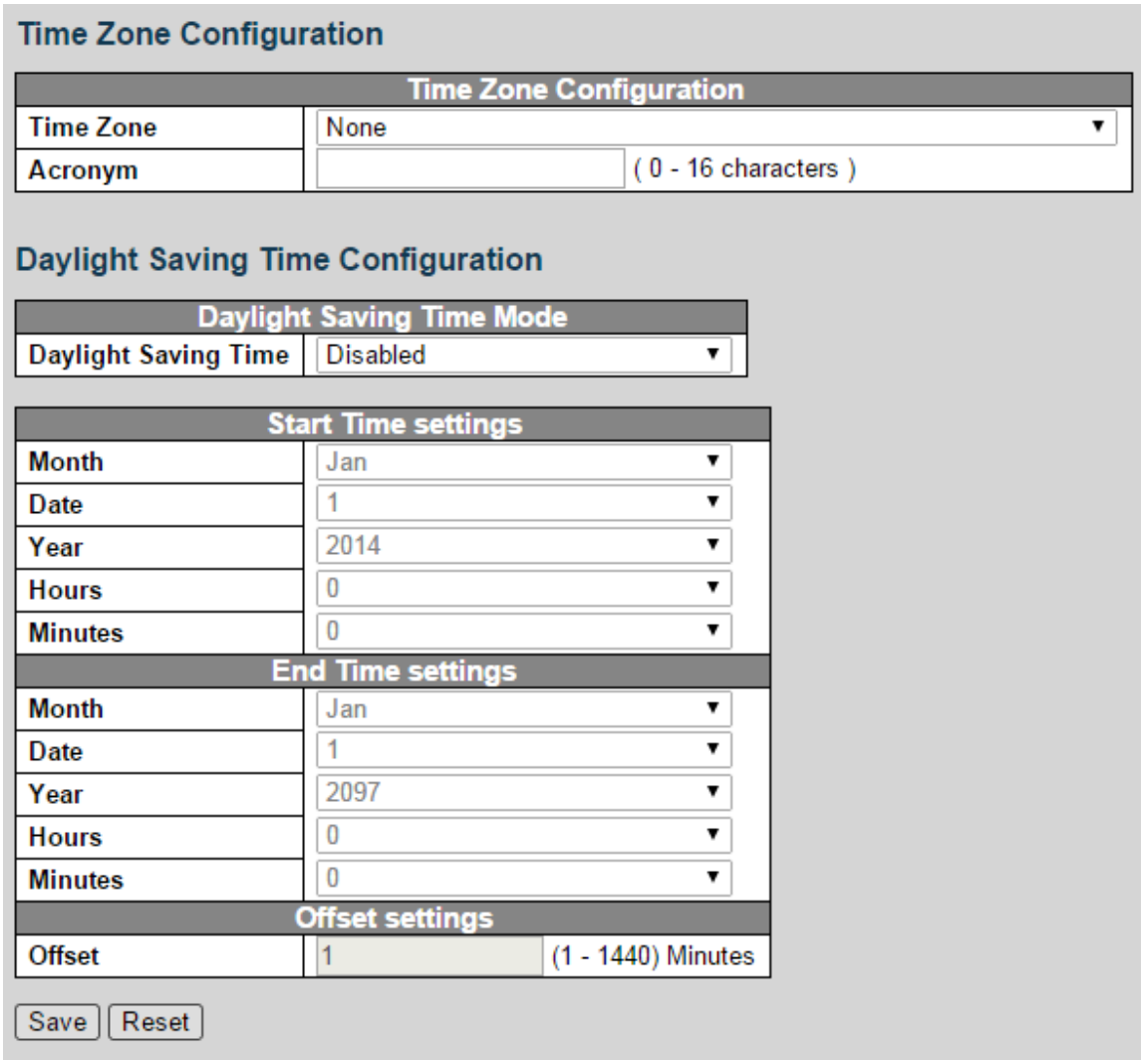
The switch can synchronize with the time of server 1.

4.1.1.4 Time

You can set the time zone and daylight saving time.

Select **Advanced > Configuration > System > Time**. The Time settings interface is displayed. See Figure 4-7.

Figure 4-7 Time settings



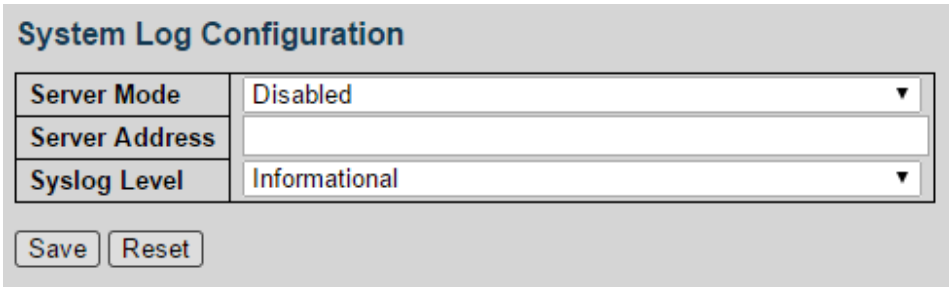
4.1.1.5 Log

You can configure the system log information, including Server Mode, Server Address, and System Log Level.

Step 1 Select **Advanced > Configuration > System > Log**.

The System Log Configuration interface is displayed. See Figure 4-8.

Figure 4-8 System log configuration



Step 2 Set the parameters. See Table 4-3.

Table 4-3 System log configuration

Parameter	Description
Server Mode	Select the server mode: Disabled or Enabled.

Parameter	Description
Server Address	Input the IP address of the log server.
System Log Level	Select the system log lever, including: ● Error ● Warning ● Notice ● Informational

Step 3 Click **Save**.

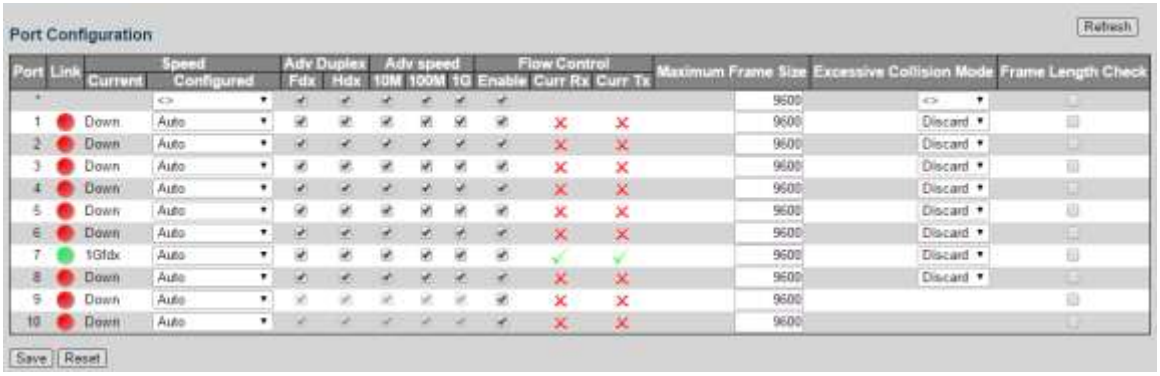
4.1.2 Port

You can set the port parameters, including speed, duplex, flow control, and so on.

Step 1 Select **Advanced > Configuration > Port**.

The Port Configuration interface is displayed. See Figure 4-9.

Figure 4-9 Port configuration



Step 2 Set the parameters. See Table 4-4.

Table 4-4 Port parameter

Parameter	Description
Port	Display all the ports.
Link	If the port link is displayed as green, it is connected successfully. And if the port link is displayed as red, it is not connected.
Speed	Including Current and Configured. In Current list, if it is displayed as Down, the port is not connected, and if it is displayed as a certain speed, the port is connected successfully. In Configured list, you can set the speed from the drop-down list.
Duplex	Set the duplex of the port. Full duplex (Fdx) and half duplex (Hdx) are selectable.
Adv Speed	Set the average speed of the port. 10 M, 100 M, and 1 G are selectable.
Flow Control	You can select **Enable** to enable flow control function.
Maximum Frame Size	Set the Maximum frame size.
Excessive Collision Mode	Select excessive collision mode from the drop-down list.

Parameter	Description
Frame Length Check	Select the checkbox to enable the function.

Step 3 Click **Save**.

4.1.3 DHCP

4.1.3.1 Server

DHCP Server is the server for managing DHCP standard in the specific network. DHCP Server is to allocate IP address for the workstation and make sure that the IP address for every workstation is different. DHCP Server simplifies the network management task which should be done manually before.

Generally, in the following scenes, DHCP Server is adopted to allocate IP address.

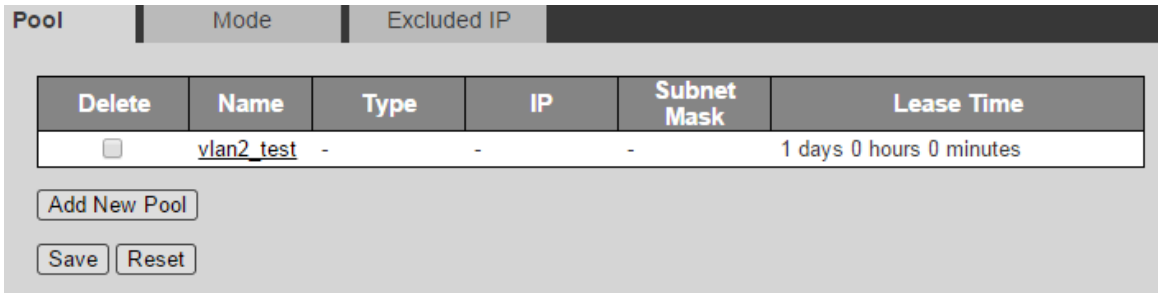
- The network scale is large. The workload is too heavy if manually configured, and centralized management for network will be difficult.
- The quantity of PC is larger than the quantity of IP address in the network, and it is impossible to allocate a static IP address for every PC. For example, the user quantity that can access network at the same time is limited by ISP, and the user needs to acquire the IP address dynamically.
- Only a small number of PC need the static IP address, and most of the PC do not need the static IP address.

There are three parts of DHCP Server configuration: address pool configuration, mode configuration, and excluded IP configuration.

Step 1 Select **Advanced > Configuration > DHCP > Server**.

Address pool configuration interface is displayed. See Figure 4-10.

Figure 4-10 Address pool

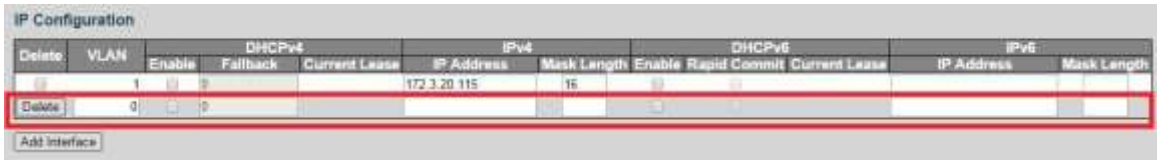


Step 2 Add a new address pool.

1) Click **Add New Pool**.

A new record is added. See Figure 4-11.

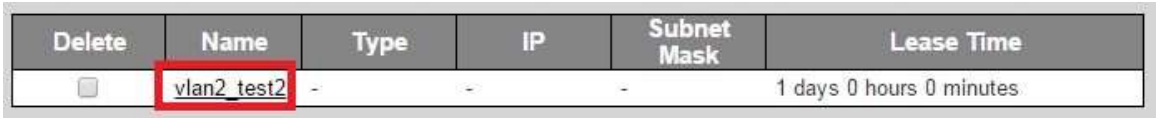
Figure 4-11 Add a new pool



2) Input the pool name. For example, vlan2_test2.
3) Click **Save**.
4) Click the pool name link. See Figure 4-12.

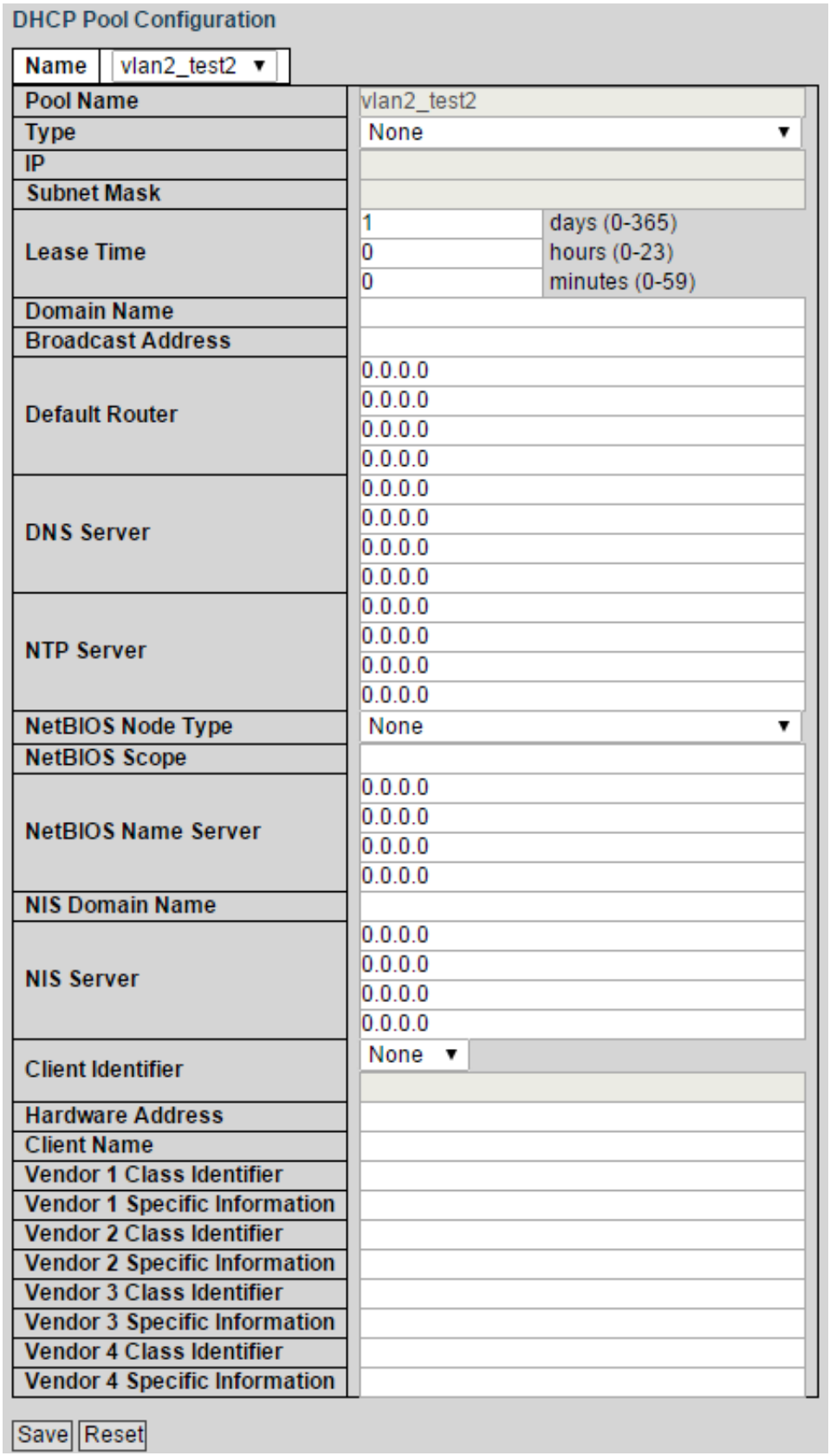
DHCP Pool Configuration interface is displayed. See Figure 4-13.

Figure 4-12 Name link



Delete	Name	Type	IP	Subnet Mask	Lease Time
☐	vlan2_test2	-	-	-	1 days 0 hours 0 minutes

Figure 4-13 DHCP pool configuration



DHCP Pool Configuration

Name: vlan2_test2

Pool Name	vlan2_test2
Type	None
IP	
Subnet Mask	
Lease Time	1 days (0-365) 0 hours (0-23) 0 minutes (0-59)
Domain Name	
Broadcast Address	
Default Router	0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
DNS Server	0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
NTP Server	0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
NetBIOS Node Type	None
NetBIOS Scope	
NetBIOS Name Server	0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
NIS Domain Name	
NIS Server	0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Client Identifier	None
Hardware Address	
Client Name	
Vendor 1 Class Identifier	
Vendor 1 Specific Information	
Vendor 2 Class Identifier	
Vendor 2 Specific Information	
Vendor 3 Class Identifier	
Vendor 3 Specific Information	
Vendor 4 Class Identifier	
Vendor 4 Specific Information	

Save Reset

5) Set the parameters in DHCP Pool Configuration interface. See Figure 4-13. And see Table 4-5 for details about the parameters.

Table 4-5 DHCP pool configuration parameter

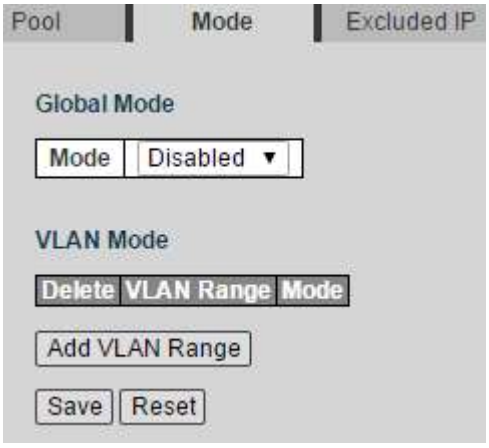
Parameter	Description
Type	Two types: network and host. ● Network: a segment of IP address. ● Host: a specific IP address.
IP	Input the IP address of the host or the network.
Subnet Mask	Input the subnet mask.
Lease Time	Input the lease time of the address pool.
Domain Name	Configure the domain name.
Broadcast Address	Configure the broadcast address.
Default Router	Configure the default gateway of the address pool.
DNS Server	Configure the server IP address of the domain name system.
NTP Server	Configure the NTP server IP address.

6) Click **Save**.

Step 3 Configure the mode.

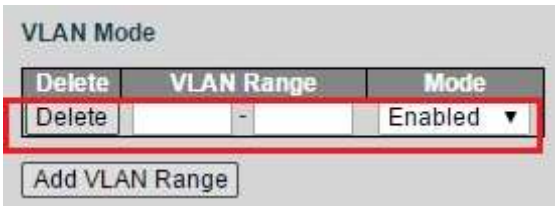
1) Click **Mode** tab.
The Mode interface is displayed. See Figure 4-14.

Figure 4-14 Mode



2) Select the Mode as **Enabled** to enable DHCP Server.
3) Click **Add VLAN Range**.
A new record is added. See Figure 4-15.

Figure 4-15 Add VLAN range

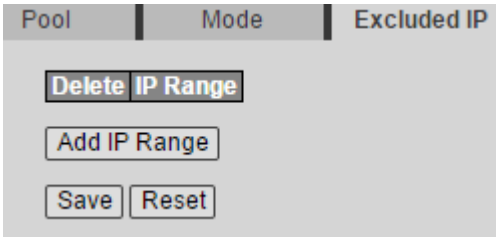


4) Input the VLAN range. For example, 2-4.
5) Click **Save**.

Step 4 Configure the host IP address and the IP address segment.

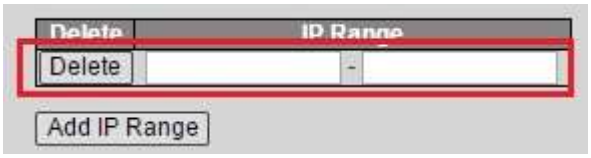
1) Click **Exclude IP** tab.
Excluded IP interface is displayed. See Figure 4-16.

Figure 4-16 Excluded IP



2) Click **Add IP Range**.
A new record is added. See Figure 4-17.

Figure 4-17 Add IP range



3) Input the IP address range. For example, 192.168.100.2-192.168.100.50.
4) Click **Save**.

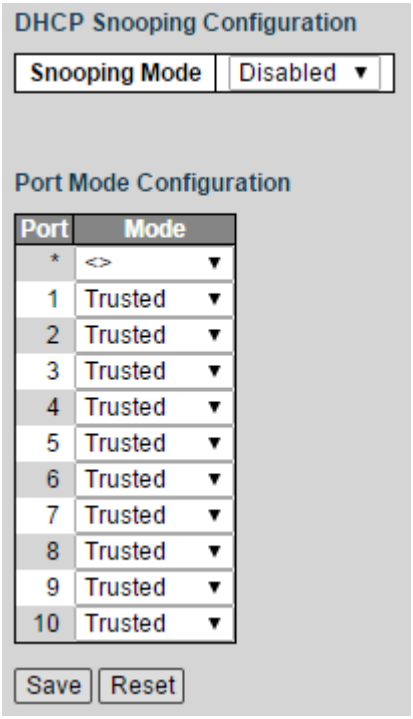
4.1.3.2 DHCP Snooping

DHCP Snooping is a security feature of DHCP to make sure that the client acquires the IP address from the legal server. If there is the illegal server built up privately in the network, the DCHP client might acquire wrong IP address and network configuration parameter, and communication will fail. To make sure that the DHCP client acquires the IP address from the legal DHCP Server, DHCP Snooping security mechanism supports to set the port as **Trusted** and **Untrusted**.

- The trusted port can forward the received DHCP packet normally.
- The untrusted port discards the DHCP-ACK packet and the DHCP-OFFER packet by DHCP Server.

Step 1 Select **Advanced > Configuration > DHCP > Snooping**.
DHCP Snooping interface is displayed. See Figure 4-18.

Figure 4-18 DHCP Snooping configuration



Step 2 Select the Snooping Mode as **Enabled** to enable DHCP Snooping .

Step 3 Set the port as **Trusted** or **Untrusted**.

Step 4 Click **Save**.

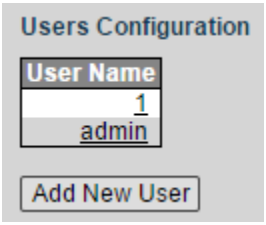
4.1.4 Security

4.1.4.1 Users

You can add, edit, and delete the user.

Select **Advanced > Configuration > Security > Users**. Users Configuration interface is displayed. See Figure 4-19.

Figure 4-19 Users configuration

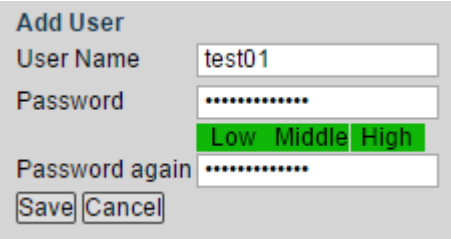


Add a user

Step 1 Click **Add New User**.

The Add User interface is displayed. See Figure 4-20.

Figure 4-20 Add a user.



Step 2 Input the user name and the password, and input the password again to confirm it. The password can be set from 8 characters through 32 characters and contains at least two types from number, letter, and special characters (excluding"'", """, ";", ":" and "&"). For example, add the new user: test01.

Step 3 Click **Save**.

The new user test01 is added. See Figure 4-21.

Figure 4-21 New user added

Edit and delete the user

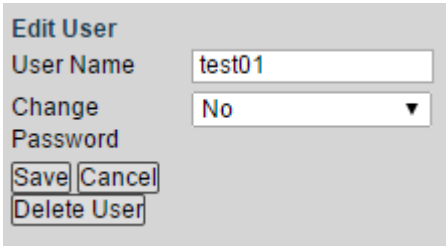
Click the user. For example, test01.

Edit User interface is displayed, and you can edit and delete the user. See Figure 4-22.

NOTE

You can not delete the admin user.

Figure 4-22 Edit user

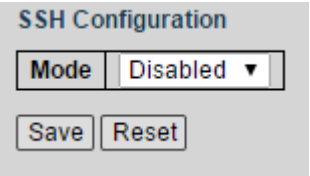


4.1.4.2 SSH

Secure Shell (SSH) is the security procotol to protect the security in remote login session and other network service, and avoid information leakage problem in remote management. You can enable or disable SSH function.

Select **Advanced > Configuration > Security > SSH**. SSH Configuration is displayed. See Figure 4-23.

Figure 4-23 SSH configuration



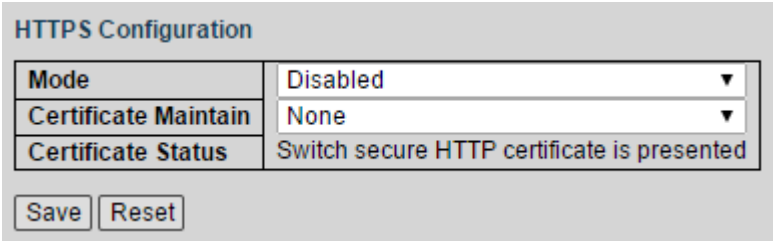
4.1.4.3 HTTPS

HTTPS (Hyper Text Transfer Protocol over Secure Socket Layer) is the HTTP channel for security target. SSL layer and TLS layer are added to HTTP, which are the security foundation. And SSL/TLS are needed for encryption. HTTPS is the URI scheme, and the syntax is similar to HTTP. It is used for security HTTP data transmission. Built in the web Netscape Navigator, it provides authentication and encryption communication. It is widely applied in world wide web for security sensitive communicaiton. For example, to protect account security and use information.

Step 1 Select **Advanced > Configuration > Security > HTTPS**.

HTTPS Configuration interface is displayed. See Figure 4-24.

Figure 4-24 HTTPS configuration



Step 2 Select the Mode as **Enabled** to enable HTTPS service.

Step 3 Select the Certificate Maintain from the drop-down list, including **None**, **Delete**, and **Generate**, respectively means no certificate, to delete the certificate, and to create the certificate.

Step 4 Click **Save**.

4.1.4.4 SNMP

SNMP (Simple Network Management Protocol) is the standard protocol for network management in Internet, and it is widely applied for management device to access and manage the managed devices. SNMP has the following features:

- It supports intelligent management for network device. By using the network management platform based on SNMP, the network administrator can query the running status and the parameters of the network device, and can set the parameter, find the error, perform fault diagnosis, and then to plan the capacity and create the report.
- SNMP supports to manage the devices of different physical features. SNMP provides only the most basic function library. It makes the management task and the physical feature and the networking technology of the managed device independent, to manage the devices from different manufacturers.

SNMP network provides two element, NMS and Agent.

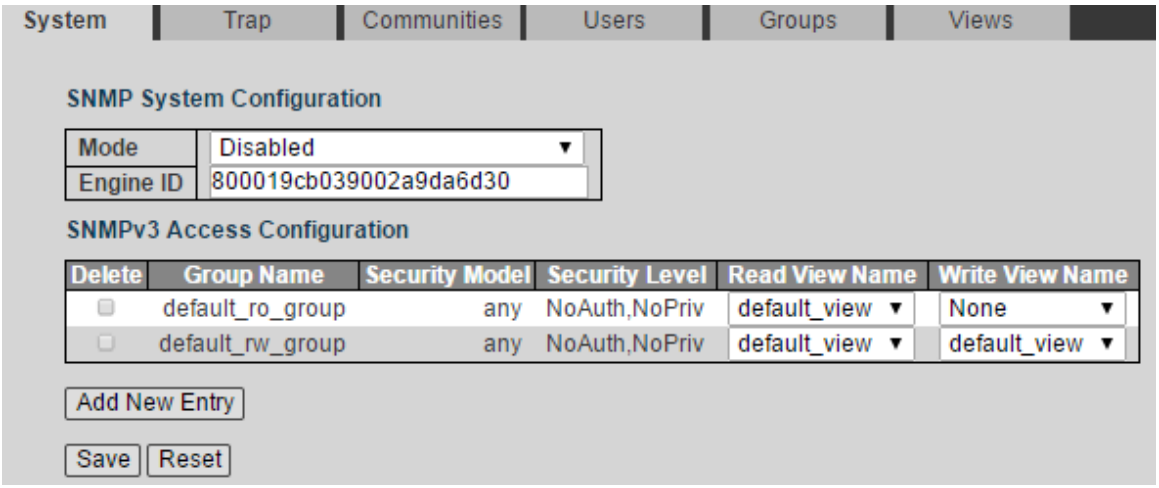
- NMS (Network Management System) is the manager in SNMP network, and it provides friendly human-machine interface, to help the network administrator to finish most of the network management work.
- Agent is the manged role in SNMP network, and it receives and handles the request packet from NMS. In some emergency circumstances, for example, if the port status changes, Agent can send alarm packet to NMS proactively.

Enable SNMP Function

Step 1 Select **Advanced > Configuration > Security > SNMP**.

The System interface in SNMP is displayed. See Figure 4-25.

Figure 4-25 System



Step 2 Select the Mode as **Enabled** in SNMP System Configuration to enable SNMP function.

NOTE

Every SNMP v3 agent has an engine ID as its unique identifier.

Trap

Configure Agent, and it can send SNMP Trap packet to NMS. And configure the related information of the target host (generally NMS) for SNMP Trap packet.

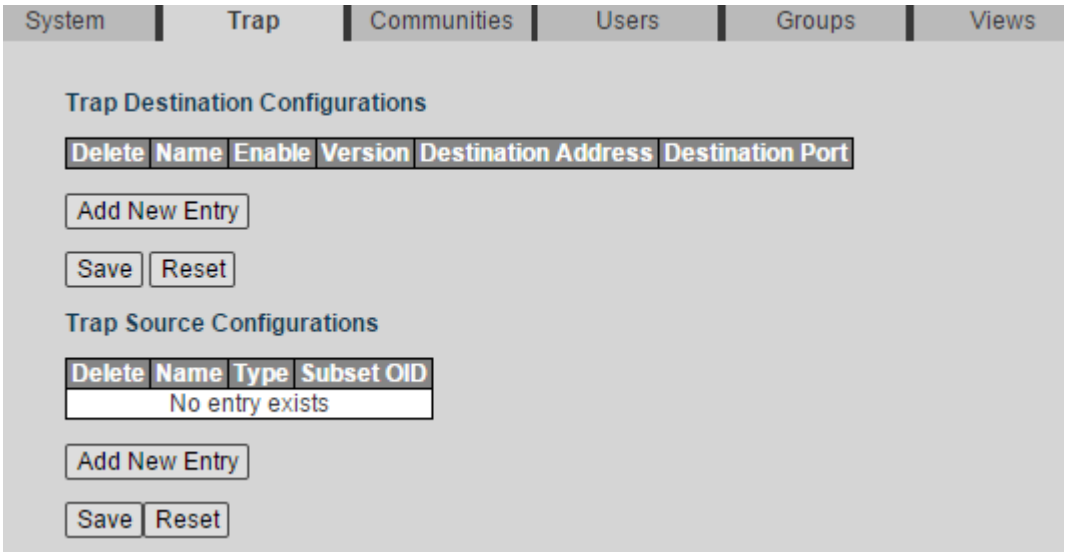
Trap packet is the packet that Agent proactively sends to NMP to report some emergent and important events, for example, the manged device roots.

By default, Agent is allowed to send SNMP Trap packet.

Step 1 Select **Advanced > Configuration > Security > SNMP > Trap**.

The Trap interface is displayed. See Figure 4-26.

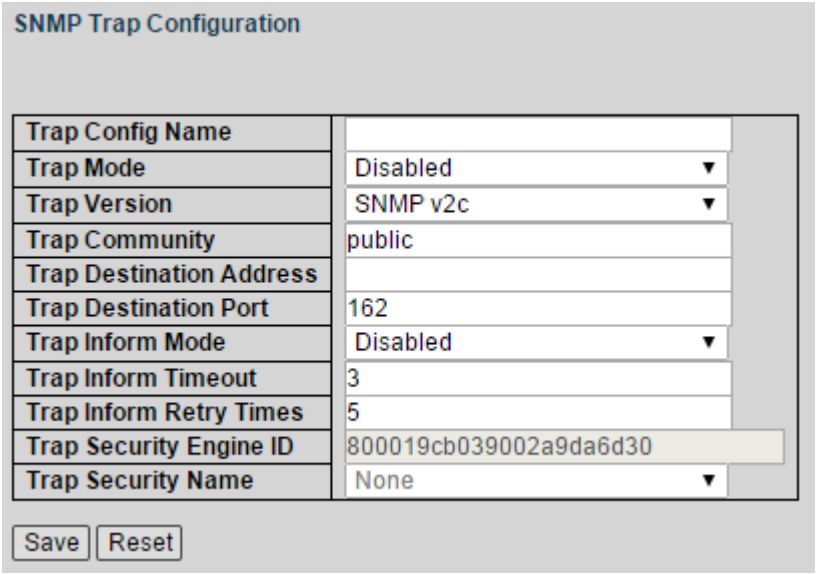
Figure 4-26 Trap



Step 2 Click **Add New Entry** in Trap Destination Configurations.

The SNMP Trap Configuration interface is displayed. See Figure 4-27.

Figure 4-27 SNMP Trap configuration



Step 3 Set the parameters. See Table 4-6.

Table 4-6 NMP Trap configuration parameter

Parameter	Description
Trap Config Name	Input the Trap Config name.
Trap Mode	Select **Enabled** or **Disabled** to enable or disable the function.
Trap Version	Three versions: SNMP v1, SNMP v2c, and SNMP v3.
Trap Community	Input the Trap community name.
Trap Destination Address	Input the Trap destination address.
Trap Destination Port	Input the port number of the target host.
Trap Inform Mode	Select **Enabled** or **Disabled** to enable or disable the function. Only versions of SNMP v2c and SNMP v3 support the function.
Trap Inform Timeout	Input the timeout. Only versions of SNMP v2c and SNMP v3 support the function.

Parameter	Description
Trap Inform Retry Times	Input the retry times. Only versions of SNMP v2c and SNMP v3 support the function.
Trap Security Engine ID	Set the engine ID. Only version SNMP v3 supports the function.
Trap Security Name	Input the Trap security name. Only version SNMP v3 supports the function.

Step 4 Click **Save**.

Communities

Add the community, and set the authority for NMS accessing Agent, using the community.

Step 1 Select **Advanced > Configuration > Security > SNMP > Communities**.

Communities interface is displayed. See Figure 4-28.

Figure 4-28 Communities (1)

Step 2 Click **Add New Entry**.

A new record is added. See Figure 4-29.

Figure 4-29 Communities (2)

Step 3 Set the community name, community secret, source IP, and the source Prefix.

Step 4 Click **Save**.

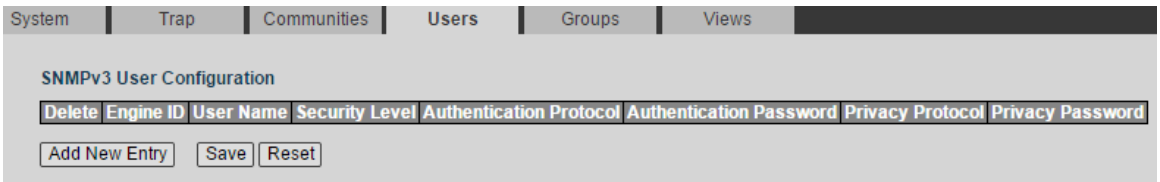
Users

Before configuring the SNMP user, you need to configure the SNMP group the user belongs to.

Step 1 Select **Advanced > Configuration > Security > SNMP > Users**.

The Users interface is displayed. See Figure 4-30.

Figure 4-30 Users



Step 2 Click **Add New Entry**.

A new record is added. See Figure 4-31.

Figure 4-31 Add a user.

Step 3 Set the parameters. See Table 4-7.

Table 4-7 User parameter

Parameter	Description
Engine ID	It is created automatically.
User Name	Input the user name.
Security Level	Select the security level from the drop-down list. ● If you select “Auth, Priv”, you need to set the Authentication Protocol and the Authentication Password, Private Protocol and the Private Password. ● If you select “NoAuth, NoPriv”, you do not need to set the protocol and password. ● If you select “Auth, NoPriv”, you need to set the Authentication Protocol and the Authentication Password.

Step 4 Click **Save**.

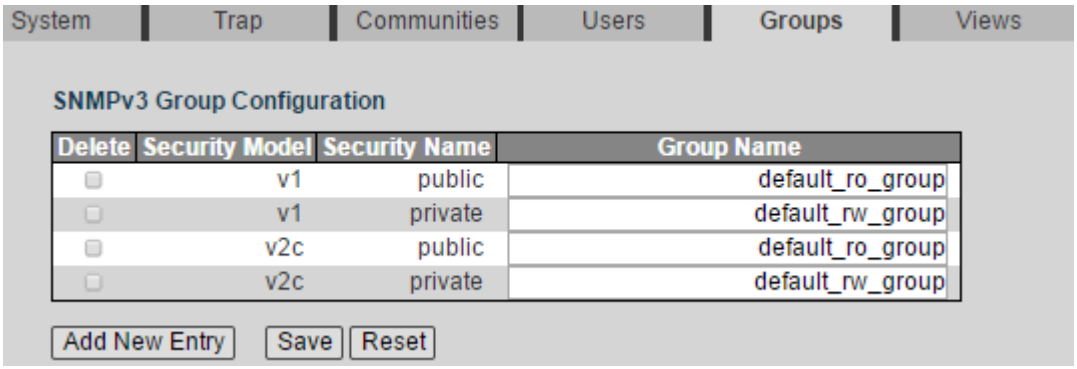
Groups

After SNMP group configured, you can add the SNMP user to the SNMP group when configuring SNMP user. You can manage the users in the group better through managing the group.

Step 1 Select **Advanced > Configuration > Security > SNMP > Groups**.

The Groups interface is displayed. See Figure 4-32.

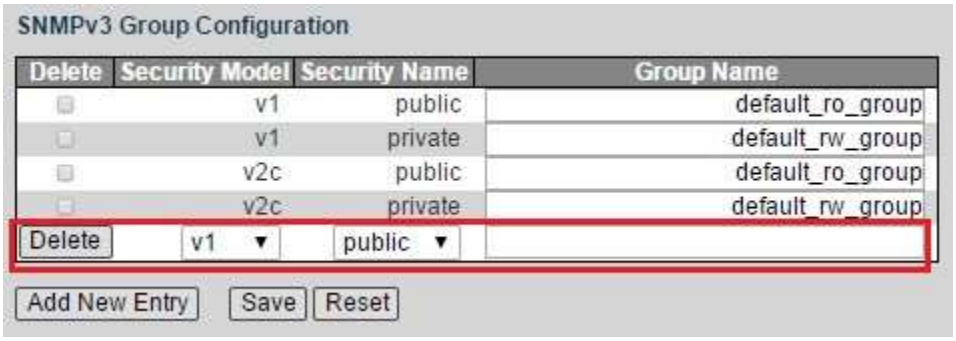
Figure 4-32 Groups



Step 2 Click **Add New Entry**.

A new record is added. See Figure 4-33.

Figure 4-33 Add a group



Step 3 Set the parameters. See Table 4-8.

Table 4-8 Group parameter

Parameter	Description
Security Mode	Select the security mode from the drop-down list, including v1, v2c, and usm.
Security Name	Select the security name from the drop-down list.
Group Name	Input the group name.

Step 4 Click **Save**.

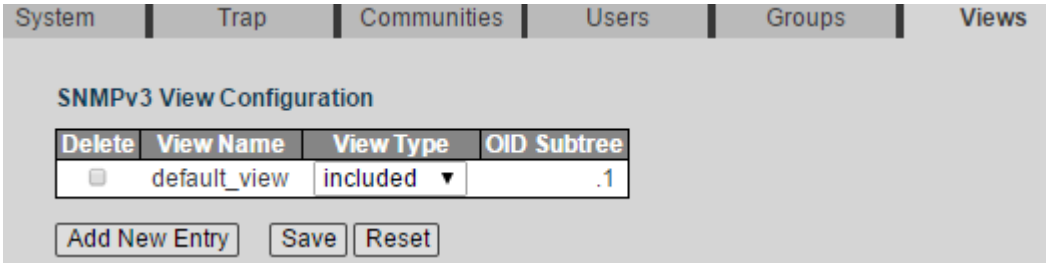
Views

After SNMP views configured, you can specify the SNMP views for the SNMP group to limit the MIB target that the SNMP group can visit.

Step 1 Select **Advanced > Configuration > Security > SNMP > Views**.

The Views interface is displayed. See Figure 4-34.

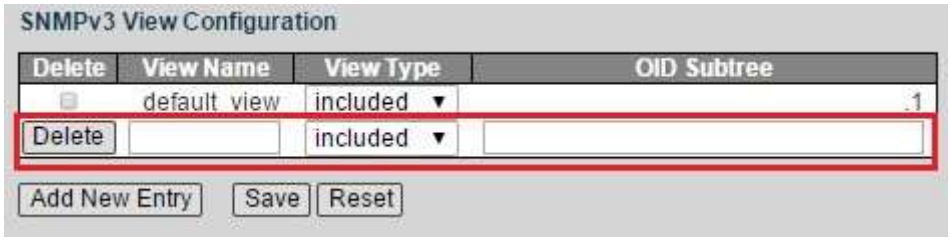
Figure 4-34 Views



Step 2 Click **Add New Entry**.

A new record is added. See Figure 4-35.

Figure 4-35 Add a new view



Step 3 Set the parameters. See Table 4-9.

Table 4-9 Views parameter

Parameter	Description
View Name	Input the view name.

Parameter	Description
View Type	Select the view type from the drop-down list to set whether the object decided by OID of MIB subtree and subtree mask is included in the view type.
OID Subtree	Input the OID of MIB subtree root node (for example, 1.4.5.3.1), or the name (for example, system). OID of MIB subtree indicates the node position in the MIB tree, and it can only identify one object in the MIB library.

Step 4 Click **Save**.

4.1.4.5 RMON

RMON (Remote Network Monitoring) is for statistics and alarm function. It is applied for remote monitoring and management in network. Statistics is the function that the managed device can periodically or continuously record the flow information of the network segment which the port connects to, for example, the packet quantity received by the network segment in a period of time. Alarm function is that the managed device can monitor the value of the specific MIB variable, and when the value reaches the alarm threshold (for example, the port rate reached the specific value, or the ratio of broadcasting packet reaches the specific value), it can automatically record the log, and send Trap packet to the management device.

Statistics

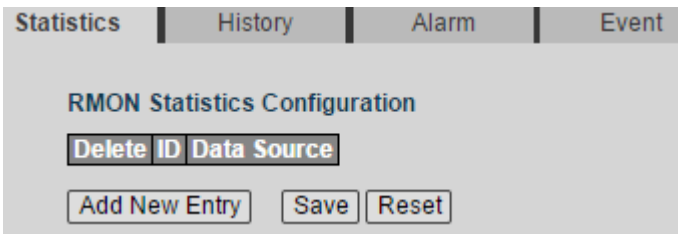
The statistics group regulates that the system continuously records the different types of flow information from the port (only supports Ethernet port currently) and stores the statistics result in the Ethernet statistical table (etherStatsTable), and the management can check the result conveniently. The statistics information contains the quantity of network conflicts, quantity of CRC verification error massage, quantity of data packet too small or too large, quantity of broadcasting packet or multicasting packet, the received byte count, and the quantity of received packet.

After creating the statistics table in the specific port, the statistics table records the packet quantity from the current port. The statistics result is the continuously accumulated value.

Step 1 Select **Advanced > Configuration > Security > RMON**.

The Statistics interface is displayed. See Figure 4-36.

Figure 4-36 Statistics



Step 2 Click **Add New Entry**.

A new record is added. See Figure 4-37.

Figure 4-37 Add a new statistics group

Step 3 Set the parameters. See Table 4-10.

Table 4-10 Statistics group parameter

Parameter	Description
ID	ID number is user-defined.
Date Source	It is the mapping reference number of switch port in SNMP client.

Step 4 Click **Save**.

History

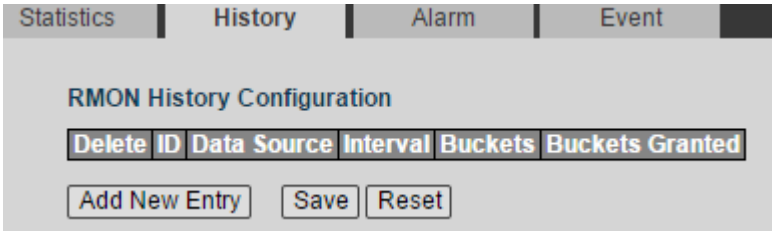
The history group regulates that the system periodically records the different types of flow information from the port and stores the statistics result in the history table (etherHistoryTable), and the management can check the result conveniently. The data contains bandwidth utilization, error package quantity, and total package quantity.

The history group records the packets that the port receives in every period, and the period length is user-defined.

Step 1 Select **Advanced > Configuration > Security > RMON > History**.

The History interface is displayed. See Figure 4-38.

Figure 4-38 History



Step 2 Click **Add New Entry**, and set the ID and the data source.

Step 3 Click **Save**.

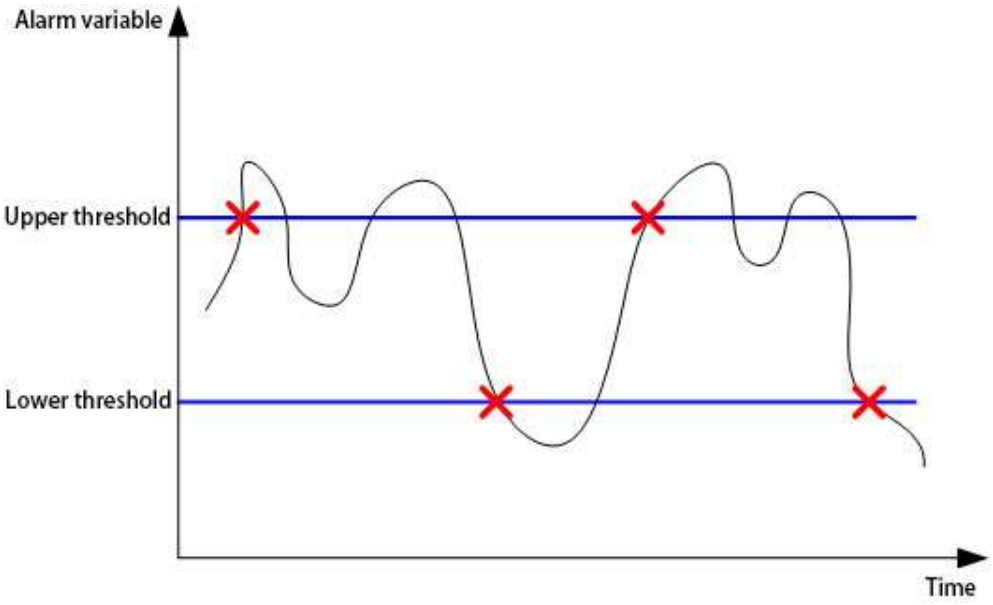
Alarm

RMON alarm management can monitor the specific alarm variable (for example, the packet quantity etherStatsPkts that the port receives). After creating the alarm table, the system can periodically acquire the value of the monitored alarm variable according to the defined time. When the value of the alarm variable reaches the upper threshold, one upper threshold alarm event is triggered. And when the value of the alarm variable reaches the lower threshold, one lower threshold alarm event is triggered. The alarm management can process the alarm events according to the event definition.

When the sampling value of alarm variable continuously exceeds the threshold in the same direction, only the first will trigger alarm. The upper threshold alarm event and the lower threshold alarm event are alternate. When one upper threshold alarm event triggers, the next must be the lower threshold alarm event. As the following figure, the value of alarm variable

(shown as the black curve) exceeds the threshold (shown as the blue curve) for several times, and there are several cross points. Only the points marked with red crosses trigger alarm event.

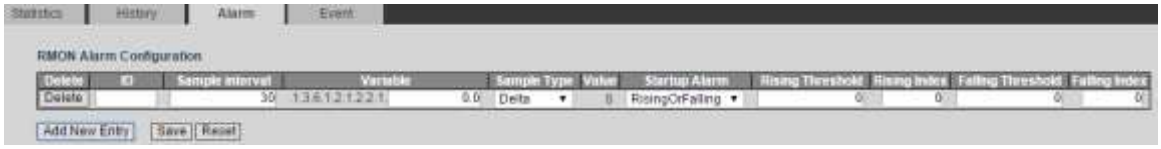
Figure 4-39 Upper threshold and lower threshold alarm



Step 1 Select **Advanced > Configuration > Security > RMON > Alarm**.

The Alarm interface is displayed. See Figure 4-40.

Figure 4-40 Alarm



Step 2 Click **Add New Entry**, and set the parameters according to the interface, including ID, sample interval, variable, sample type, startup alarm, and so on.

Step 3 Click **Save**.

Event

Event group is for defining the event reference number and the processing mode. The events defined in event group are applied in the alarm configuration. When the monitored target reaches the alarm condition, alarm event is triggered. There are several processing mode:

- Log: The corresponding information (the event time and event content) of the alarm event will be recorded in the event log table of the device RMON MIB, and the management device can check the information through SNMP GET operation.
- SNMP Trap: Trap packet will be sent to network management station to inform the alarm event.
- Log and Trap: The alarm event will be recorded in the event log table of the device, and Trap packet will be sent to network management station .
- None: No processing.

Step 1 Select **Advanced > Configuration > Security > RMON > Event**.

The Event interface is displayed. See Figure 4-41.

Figure 4-41 Event

Step 2 Click **Add New Entry**, and set the parameters according to the interface, including ID, Desc, and type.

Step 3 Click **Save**.

4.1.4.6 ACL

ACL (Access Control List) is for flow identification. For filtering the packet, the network device needs to configure a series of matching conditions to classify the packets. The conditions can be the source address, destination address, and the port number of the packet.

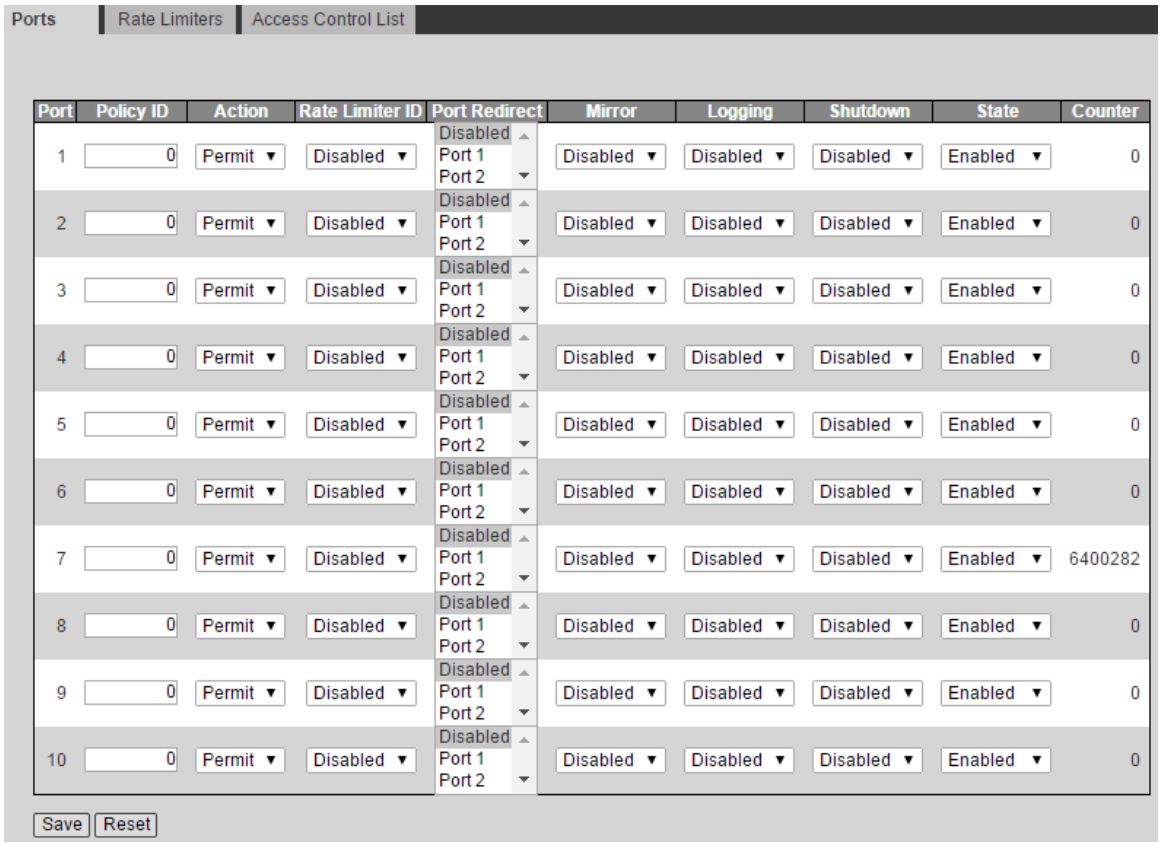
When the device port receives the packet, it can analyze the packet field according to the ACL rule of the current port. And after the specific packet is identified, the packet is allowed or forbidden to pass according the preset rule.

Ports

Step 1 Select **Advanced > Configuration > Security > ACL**.

The ACL interface is displayed. See Figure 4-42.

Figure 4-42 Ports



Step 2 Set the parameters including Policy ID, Action, Rate Limiter ID, and so on.

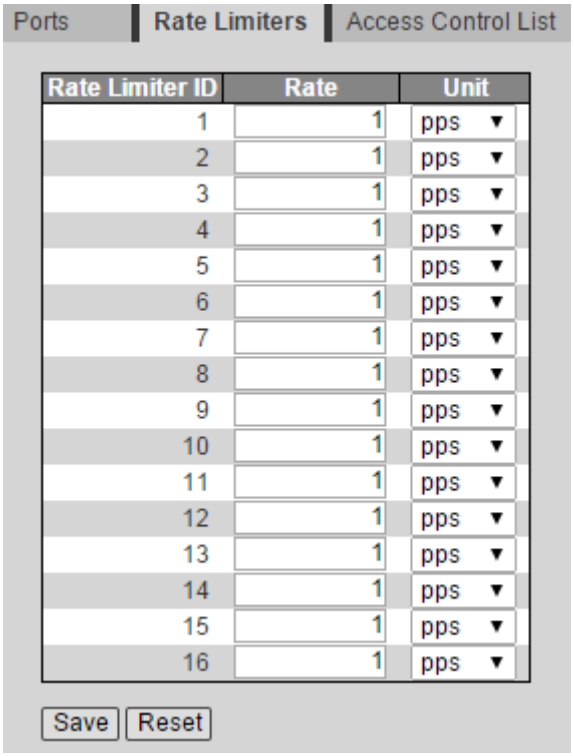
Step 3 Click **Save**.

Rate Limiters

Step 1 Select **Advanced > Configuration > Security > ACL > Rate Limiters**.

The Rate Limiters interface is displayed. See Figure 4-43.

Figure 4-43 Rate limiters



Step 2 Set the parameters including Rate and Unit.

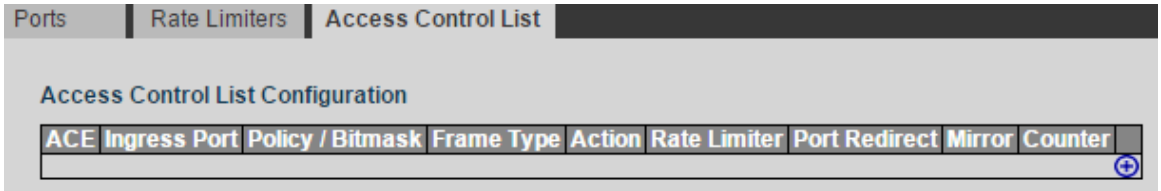
Step 3 Click **Save**.

Access Control List

Step 1 Select **Advanced > Configuration > Security > ACL > Access Control List**.

The Access Control List interface is displayed. See Figure 4-44.

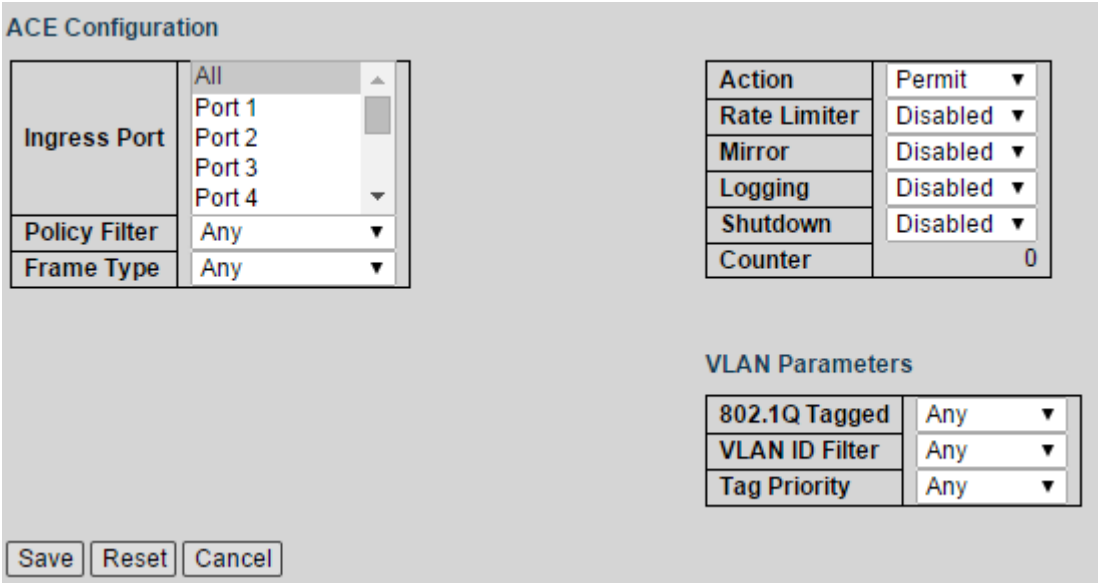
Figure 4-44 Access control list



Step 2 Click ⊕.

The ACE Configuration interface is displayed. See Figure 4-45.

Figure 4-45 ACE configuration



Step 3 Set the parameters.

Step 4 Click **Save**.

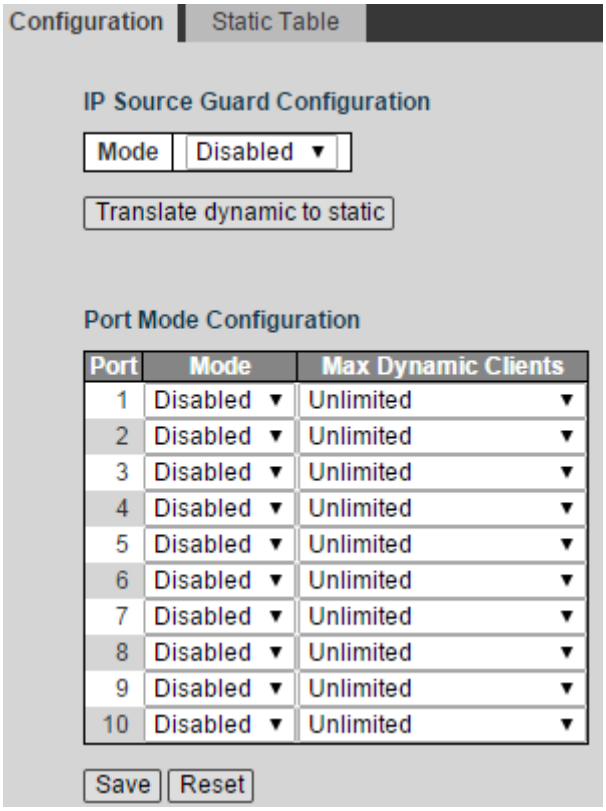
4.1.4.7 IP Source Guard

Through IP Source Guard binding function, the packet forwarded in the port can be filtered and controlled, and the illegal packet cannot pass through the port. The illicit use of network resource is limited, and security performance of the port is enhanced.

IP Source Guard

Step 1 Select **Advanced > Configuration > Security > IP Source Guard**.
The IP Source Guard interface is displayed. See Figure 4-46.

Figure 4-46 IP source guard



Step 2 Select the Mode as **Enabled** to enable IP Source Guard function.

Step 3 Set the parameters. See Table 4-11.

Table 4-11 IP source guard parameter

Parameter	Description
Translate dynamic to static	Click the button to switch dynamic/static. The premise is that the IGMP Snooping is enabled.
Port Mode Configuration	Mode: **Disabled** and **Enabled** are selectable. Max Dynamic Clients: **Unlimited**, **0**, **1**, and **2** are selectable.

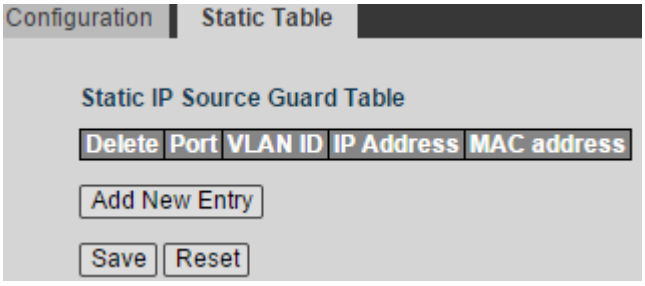
Step 4 Click **Save**.

Static Table

Step 1 Select **Advanced > Configuration > Security > IP Source Guard > Static Table**.

The Static Table interface is displayed. See Figure 4-47.

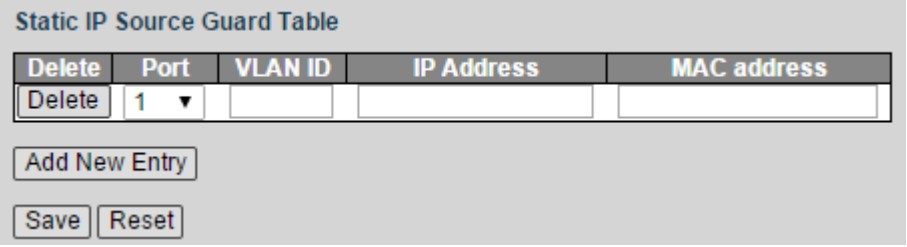
Figure 4-47 Static Table



Step 2 Click **Add New Entry**.

See Figure 4-48 for the Static IP Source Guard Table.

Figure 4-48 Static IP source guard table



Step 3 Set the parameters including Port, VLAN ID, IP Address, and MAC Address.

Step 4 Click **Save**.

4.1.4.8 ARP Inspection

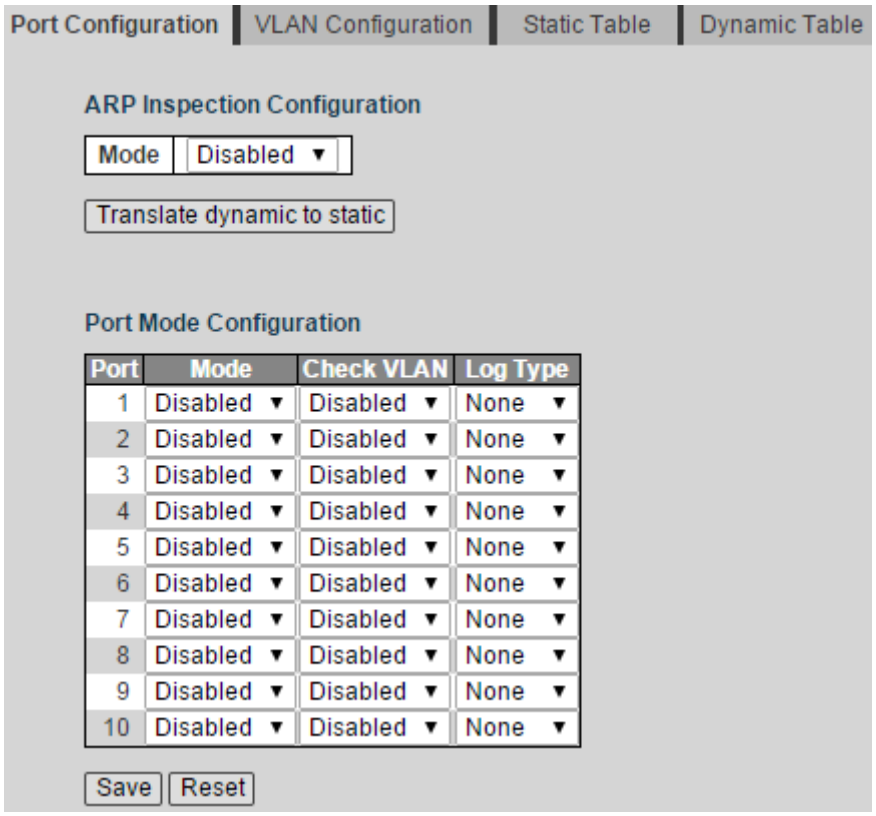
ARP (Address Resolution Protocol) is the protocol to parse the IP address into Ethernet MAC address (the physical address).

In LAN, when the host or other network device needs to forward data to another host or other network device, the IP address of the target host or other network device should be known. Besides IP address, the forwarding station needs to know the physical address of the accepting station, because the IP data packet should be sent through the physical network as packaged frame. A mapping from the IP address to the physical address is needed. ARP is the protocol to realize the function.

Enable ARP Inspection

Step 1 Select **Advanced > Configuration > Security > ARP Inspection**.
The Port Configuration interface is displayed. See Figure 4-49.

Figure 4-49 Port configuration



Step 2 Select the Mode as **Enabled** in ARP Inspection Configuration to enable ARP inspection function.

Step 3 Set the parameters. See Table 4-12.

Table 4-12 ARP inspection parameter

Parameter	Description
Translate dynamic to static	Click the button to switch dynamic/static.
Port Mode Configuration	Mode: **Disabled** and **Enabled** are selectable. Check VLAN: **Disabled** and **Enabled** are selectable. Logy Type: **None**, **Deny**, **Permit**, and **All** are selectable.

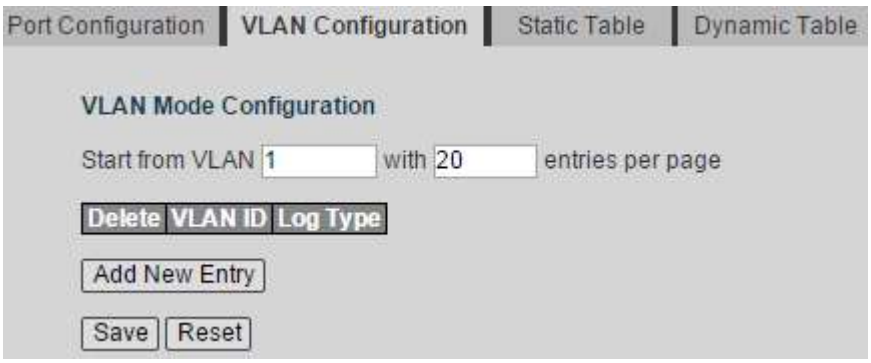
Step 4 Click **Save**.

VLAN Configuration

Step 1 Select **Advanced > Configuration > Security > ARP Inspection > VLAN Configuration**.

The VLAN Configuration interface is displayed. See Figure 4-50.

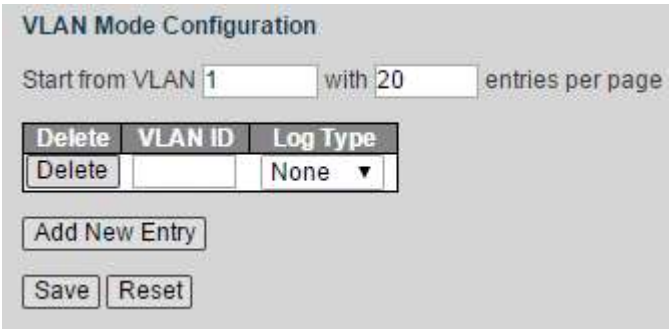
Figure 4-50 VLAN mode configuration (1)



Step 2 Click **Add New Entry**.

A new record is added. See Figure 4-51.

Figure 4-51 VLAN mode configuration (2)



Step 3 Input the VLAN ID, and select the Log Type from the drop-down list.

Step 4 Click **Save**.

Static Table

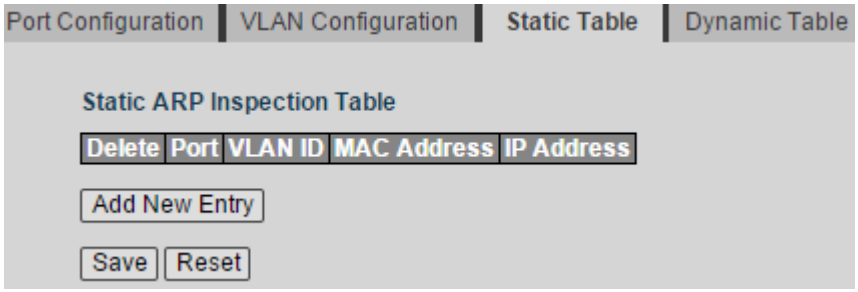
The static table is manually configured and maintained. It will not ageing, and it will not be covered by dynamic ARP table.

Static table can enhance the security performance of communicaiton. Static table can regulate that only the specific MAC address can be used in communication between network devices, and the attack packet can not modify the mapping between the IP address and the physical address of the table. Communication between the device and the other device is protected.

Step 1 Select **Advanced > Configuration > Security > ARP Inspection > Static Table**.

The Static Table interface is displayed. See Figure 4-52.

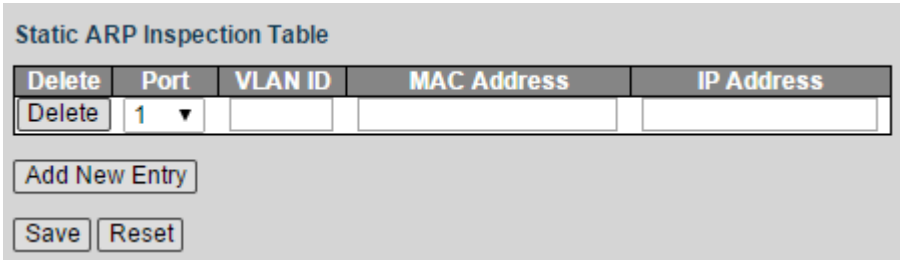
Figure 4-52 Static table



Step 2 Click **Add New Entry**.

A new record is added. See Figure 4-53.

Figure 4-53 Add a new static table



Step 3 Set the parameters including Port, VLAN ID, MAC Address, and IP Address.

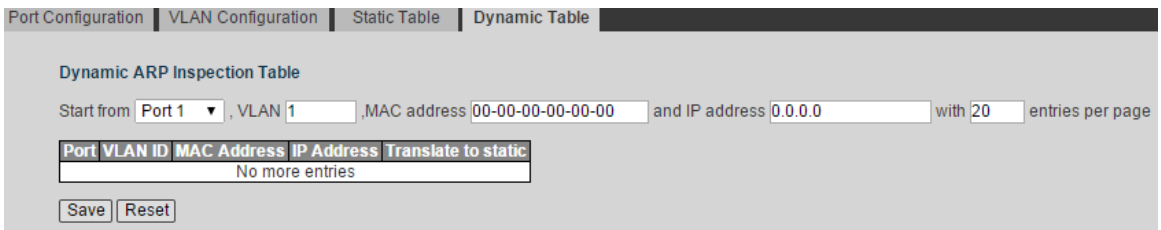
Step 4 Click **Save**.

Dynamic Table

Dynamic table is automatically created and maintained by ARP through ARP packet. It can be aging, and it can be covered by new ARP packet or static ARP table. When reaching ageing and the port is down, the corresponding dynamic table will be deleted.

Select **Advanced > Configuration > Security > ARP Inspection > Dynamic Table**. The Dynamic Table interface is displayed. See Figure 4-54.

Figure 4-54 Dynamic table

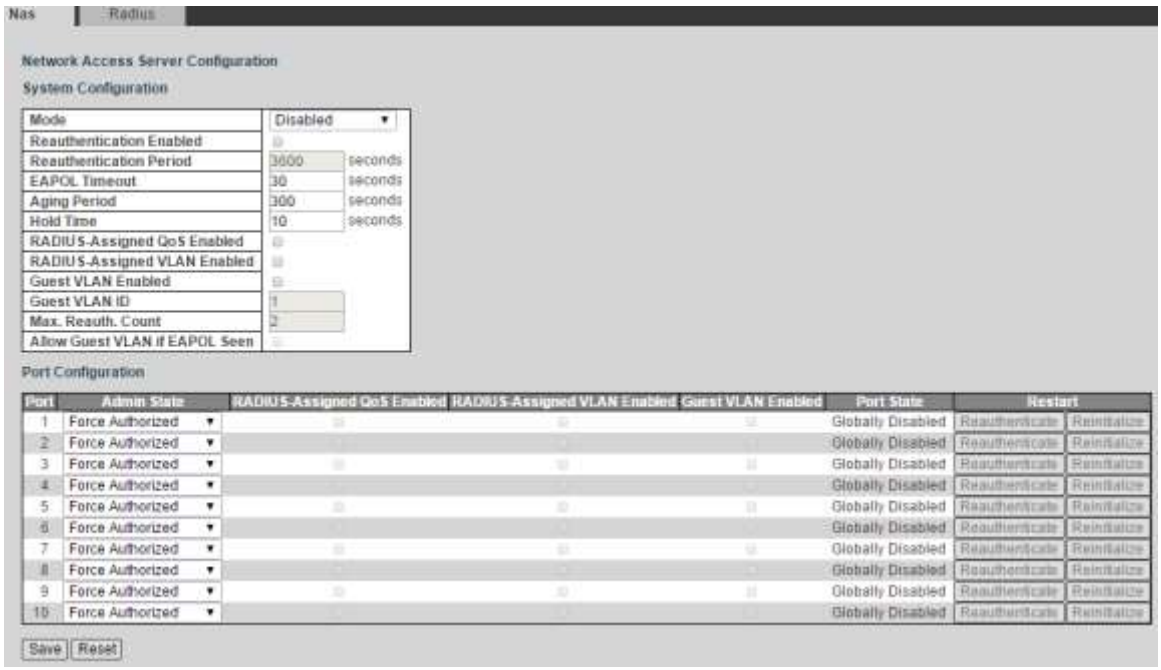


4.1.4.9 802.1X

Nas

Step 1 Select **Advanced > Configuration > Security > 802.1X**.
The Nas interface is displayed. See Figure 4-55.

Figure 4-55 Nas



Step 2 Select the Mode as **Enabled** to enable Nas in System Configuration.

Step 3 Set the parameters including Reauthentication Enabled, Reauthentication Period, EAPOL Timeout, Aging Period, and so on in System Configuration.

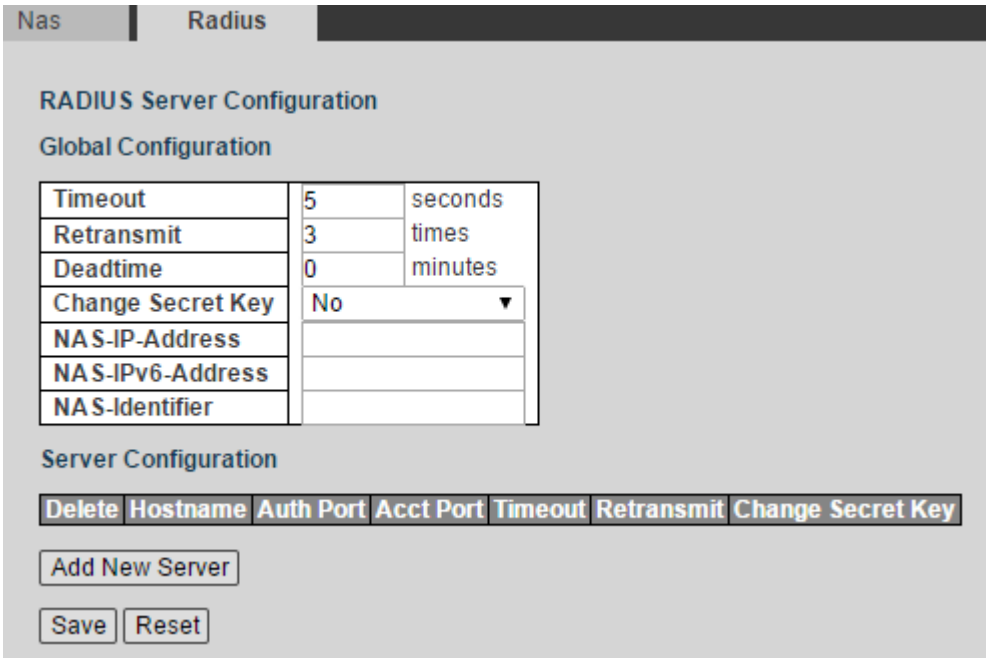
Step 4 Set the parameters including Admin State, Port State, and so on in Port Configuration.

Step 5 Click **Save**.

Radius

Step 1 Select **Advanced > Configuration > Security > 802.1X. > Radius**.
The Radius interface is displayed. See Figure 4-56.

Figure 4-56 Radius

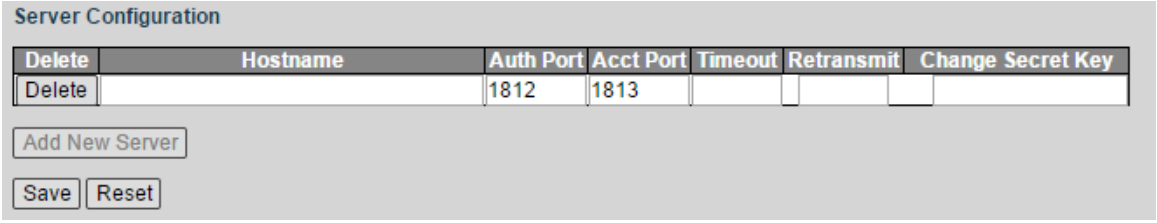


Step 2 Set the parameters including Timeout, Retransmit, Deadtime, and so on in Global Configuration.

Step 3 Click **Add New Server** in Server Configuration.

A new record is added. See Figure 4-57.

Figure 4-57 Server configuration



Step 4 Set the parameters including Hostname, Timeout, Retransmit, and so on.

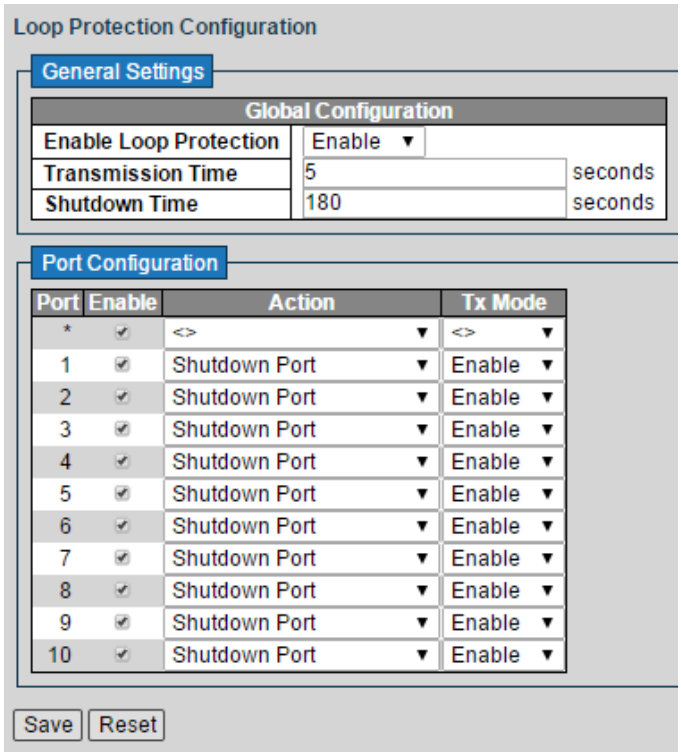
Step 5 Click **Save**.

4.1.4.10 Loop Protection

Step 1 Select **Advanced > Configuration > Security > Loop Protection**.

The Loop Protection interface is displayed. See Figure 4-58.

Figure 4-58 Loop protection



Step 2 Select Enable Loop Protection as **Enabled** to enable the function. You can set the Transmission Time and the Shutdown Time.

Step 3 Set the parameters in Port Configuration, including Enabled, Action, and Tx Mode.

Step 4 Click **Save**.

4.1.5 Aggregation

Aggregation is to form the multiple physical ports of the switch into the logical port. The multiple links in the same group can be regarded as a logical link with the larger bandwidth.

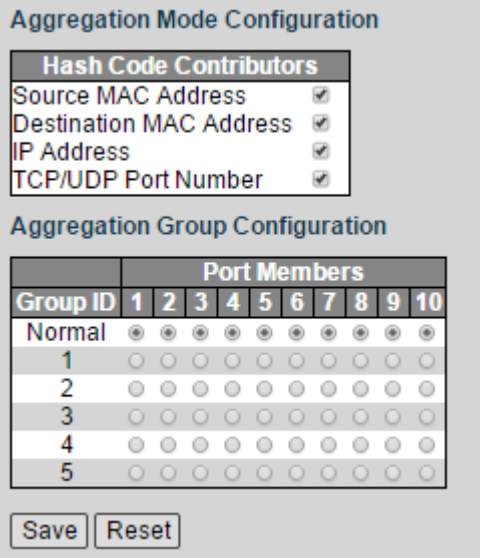
Through aggregation, the ports in the same group can share the communication flow, to make a larger bandwidth. Besides, the ports in the same group can back up reciprocally and dynamically, to enhance the link reliability.

4.1.5.1 Static

Step 1 Select **Advanced > Configuration > Aggregation > Static**.

The Statics interface is displayed. See Figure 4-59.

Figure 4-59 Static configuration (1)



Step 2 Select the Hash Code Contributors in Aggregation Mode Configuration. There are four types:

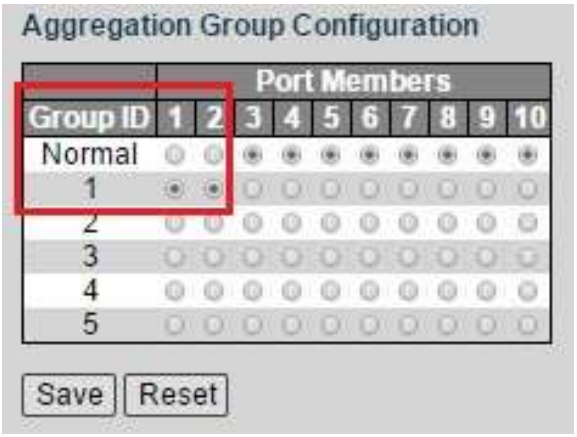
- Source MAC Address: the aggregation load balancing algorithm based on MAC address.
- Destination MAC Address: the aggregation load balancing algorithm based on destination MAC address.
- IP Address: the aggregation load balancing algorithm based on source IPv4 address and destination IPv4 address.
- TCP/UDP Port Number: the aggregation load balancing algorithm based on source and destination TCP/UDP port.

Step 3 Add the port member to the aggregation group in Aggregation Group Configuration. For example, add port 1 and port 2 to Static Group 1. See Figure 4-60.

NOTE

Up to five static groups can be set at the same time.

Figure 4-60 Static configuration (2)



Step 4 Click **Save**.

The port 1 and port 2 form the logical port.

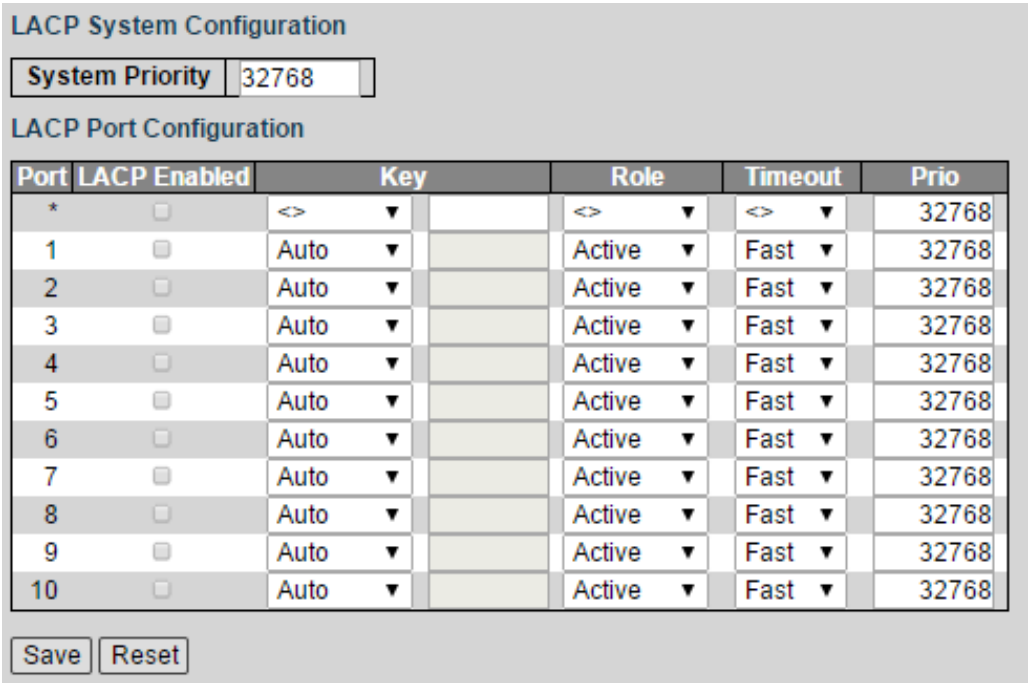
4.1.5.2 LACP

LACP (Link Aggregation Control Protocol) is the protocol for link dynamic aggregation. LACP communication with another port through LACPDU (Link Aggregation Control Protocol Data Unit).

Step 1 Select **Advanced > Configuration > Aggregation > LACP**.

The LACP interface is displayed. See Figure 4-61.

Figure 4-61 LACP



Step 2 Set the System Priority in LACP System Configuration.

Step 3 Set the parameters including Key, Role, Timeout, Prio, and so on in LACP Port Configuration. See Table 4-13 for details.

Table 4-13 LACP port configuration

Parameter	Description
LACP Enabled	Select the checkbox to enable LACP.

Parameter	Description
Key	The key value of the dynamic aggregation port is one of the identifications that the port can be added to the aggregation group. Select the Key from the drop-down list. **Auto** and **Specific** are selectable. By default, the Key value is **Auto**.
Role	Select the Role from the drop-down list. There are two types: ● Active: The port can send LACPDU packet actively to the opposite port, and analyzes the LACP. ● Passive: The port can not send LACPDU packet actively. After receiving the LACP packet sent by the opposite port, the port analyzes the LACP. By default, the Role value is **Active**.
Timeout	Select the Timeout from the drop-down list. There are two types: ● Slow: The port sends a LACP packet every second. ● Fast: The port sends a LACP packet every 30 seconds.
Priority	Set the priority for the LACP port. It ranges from 1 through 65535. The smaller the value is, the higher the priority level is.

Step 4 Click **Save**.

4.1.6 Spanning Tree

The spanning tree protocol is the protocol of layer 2. It can eliminate the ring cycle of layer 2 by choosing to block the redundant links in the network, and it can back up the links.

Similar to other protocols, the spanning tree protocol is updated with the development of the network: from STP (Spanning Tree Protocol), to RSTP (Rapid Spanning Tree Protocol), and to the latest MSTP (Multiple Spanning Tree Protocol). We introduce the features of STP, RSTP, and MSTP, and the relationship between them progressively in this section.

4.1.6.1 Bridge Settings

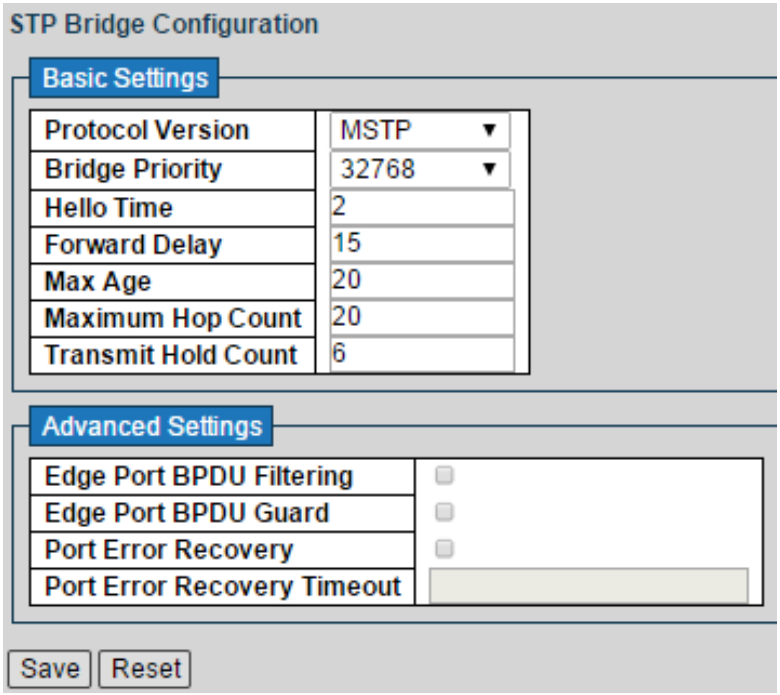
There must be the root in tree-model network, and the concept of Root Bridge is introduced in STP. There is only one root bridge in the whole network, and the root bridge changes with the network topology change. The root bridge is not constant.

In network initialization, all devices regard itself as the root bridge, create their own configuration BPDU (Bridge Protocol Data Unit), and send it periodically. After the network topology is steady, only the root bridge device can send configuration BPDU, and other device forward it.

Step 1 Select **Advanced > Configuration > Spanning Tree > Bridge**.

The STP Bridge Configuration is displayed. See Figure 4-62.

Figure 4-62 STP Bridge Configuration



Step 2 Set the parameters, including Basic Settings and Advanced Settings. See Table 4-14 and Table 4-15.

Table 4-14 Basic settings

Parameter	Description
Protocol Version	Select the protocol version. There are three types selectable: ● STP: The most basic spanning tree protocol. ● RSTP: Improved based on STP, and realizes rapid convergence. ● MSTP: Remedies the defects of STP and RSTP. MSTP not only realizes rapid convergence, but also provides better load sharing mechanism for the redundant links by forwarding the flow from different VLANs through there own paths.
Bridge Priority	Set the bridge priority. The smaller the value is, the higher the priority level is. And the value of bridge priority should be the multiple of 4096.
Hello Time	Set the period for sending packet.
Forward Delay	Set the delay time of the port forwarding.
Max Age	Set the Maximum life cycle that the packet can be saved in the device.
Maximum Hop Count	Set the Maximum hop count for MST domain, and it decides the scale of the MST domain. Only the Maximum hop count configured in the domain root takes effect in the domain. Otherwise the parameter is invalid.
Transmit Hold Count	Set the Maximum number of times that the address table is updated and forwarded in a period of time after the TC-BPDU packet is received.

Table 4-15 Advanced settings

Parameter	Description
Edge Port BPDU Filtering	You can select the checkbox to enable the edge port BPDU filtering function.

Parameter	Description
Edge Port BPDU Guard	You can select the checkbox to enable the edge port BPDU guard function.
Port Error Recovery	You can select the checkbox to enable the port error recovery function.
Port Error Recovery Timeout	Set the port error recovery timeout value.

Step 3 Click **Save**.

4.1.6.2 MSTI Mapping

In an MST domain, multiple spanning trees can be created through MSTP, and the trees are independent. Every spanning tree can be regarded as an MSTI (Multiple Spanning Tree Instance).

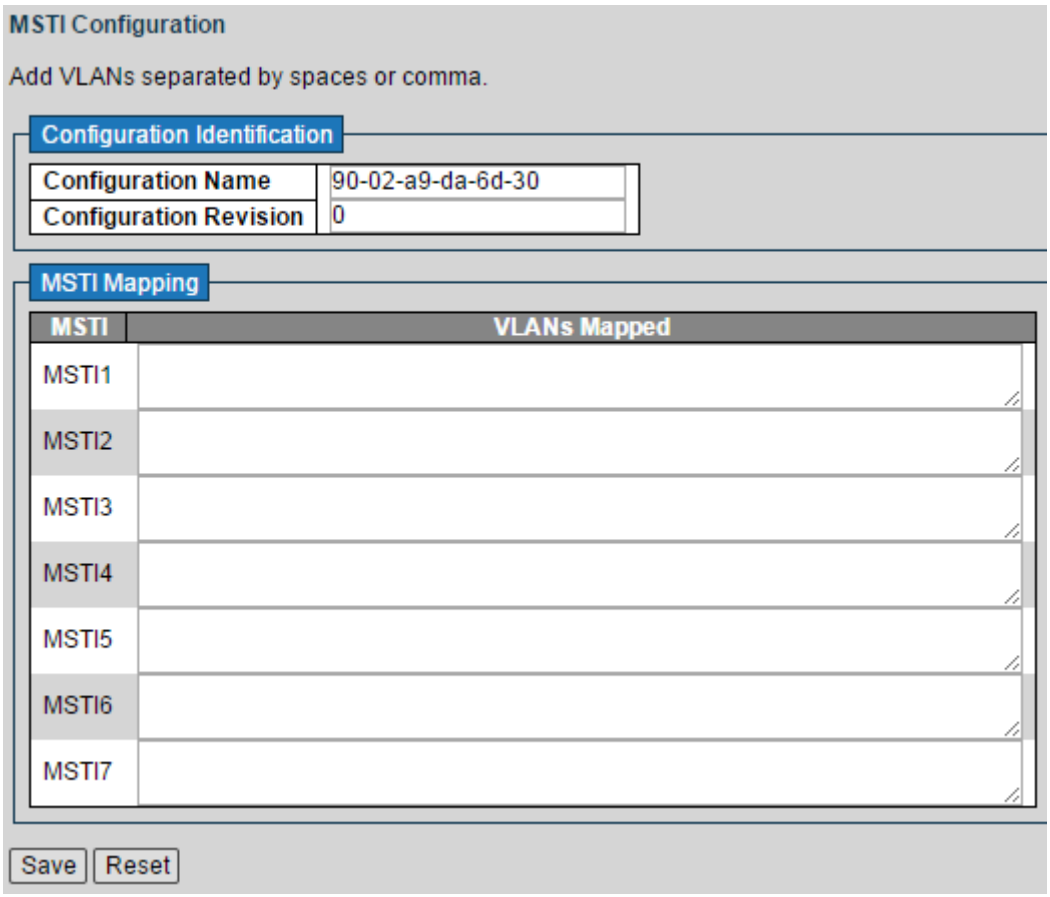
VLAN mapping table is one of the MST domain properties, for describing the mapping relationship between VLAN and spanning tree instance.

MSTP realizes load sharing according to the VLAN mapping table.

Step 1 Select **Advanced > Configuration > Spanning Tree > MSIT Mapping**.

The MSTI Configuration interface is displayed. See Figure 4-63.

Figure 4-63 MSTI configuration



Step 2 Set the parameters including Configuration Identification and MSTI Mapping. See Table 4-16 and Table 4-17.

Table 4-16 Configuration identification

Parameter	Description

Parameter	Description
Configuration Name	Set the domain name of the MST domain. By default, the domain name of the MST domain is the bridge MAC address of the device.
Configuration Revision	Set the MST domain version.

Table 4-17 MSTI mapping

Parameter	Description
MSTI	Displays the multiple spanning tree instances, 7 instances totally.
VLANs Mapped	Input the VLAN number. For example. VLAN 1.

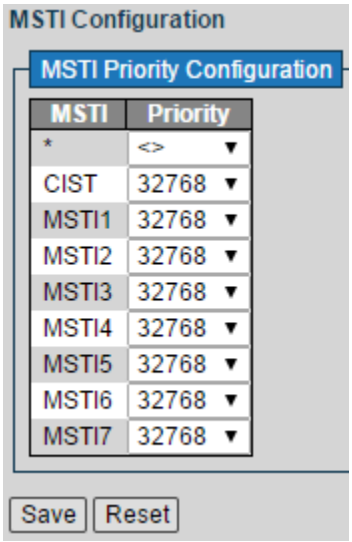
Step 3 Click **Save**.

4.1.6.3 MSTI Priorities

Set the MSTI priorities. By default, it is 32768.

Select **Advanced > Configuration > Spanning Tree > MSIT Priorities**. The MSTI Priorities interface is displayed. See Figure 4-64.

Figure 4-64 MSTI configuration

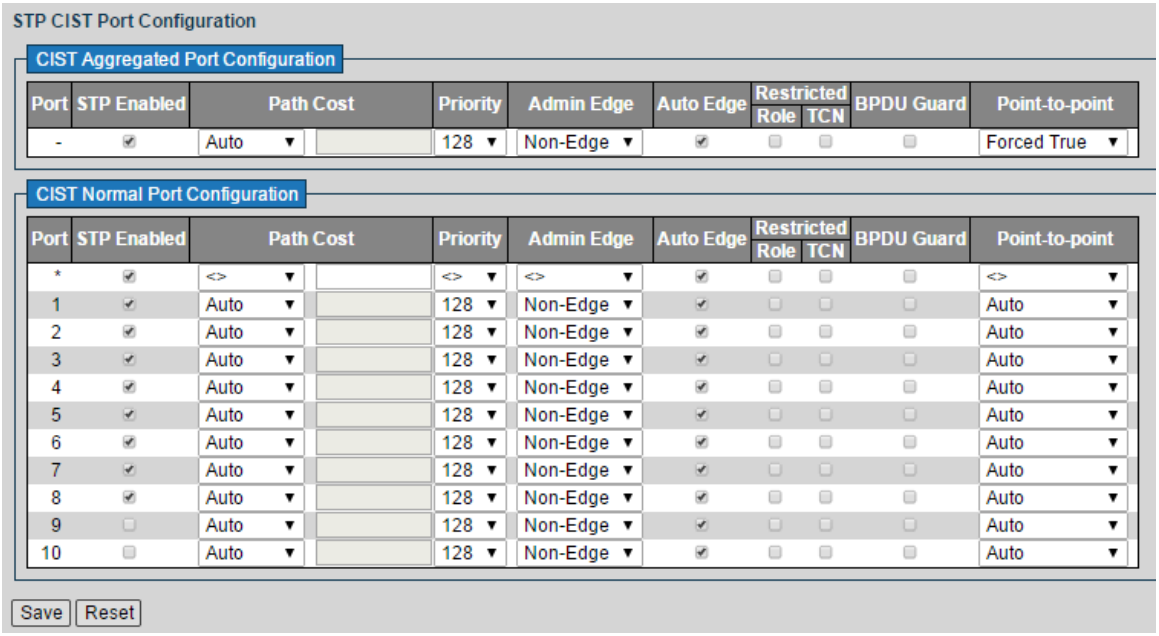


4.1.6.4 CIST Ports

Step 1 Select **Advanced > Configuration > Spanning Tree > CIST Ports**.

The STP CIST Port Configuration interface is displayed. See Figure 4-65.

Figure 4-65 STP CIST port configuration



Step 2 Set the parameters in CIST Aggregated Port Configuration. See Table 4-18.

Table 4-18 CIST aggregated port configuration

Parameter	Description
STP Enabled	Select the checkbox to enable STP.
Path Cost	Select the Path Cost from the drop-down list. **Auto** and **Specific** are selectable. If you select **Spedific**, you can set the path cost value manually.
Priority	Set the priority. By default, it is 128.
Ad min Edge	Select from the drop-down list. **Non-Edge** and **Edge** are selectable.
Auto Edge	You can select the checkbox to enable auto edge.
Restricted	**Role** or **TCN** can be selected.
BPUD Guard	You can select the checkbox to enable BPUD guard.
Point-to-point	Select from the drop-down list. **Forced True**, **Forced False**, and **Auto** are selectable.

Step 3 Set the parameters in CIST Normal Port Configuration. See Table 4-18.

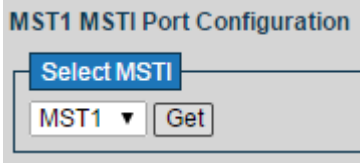
Step 4 Click **Save**.

4.1.6.5 MSTI Ports

Step 1 Select **Advanced > Configuration > Spanning Tree > MSTI Ports**.

The MST1 MSTI Port Configuration interface is displayed. See Figure 4-66.

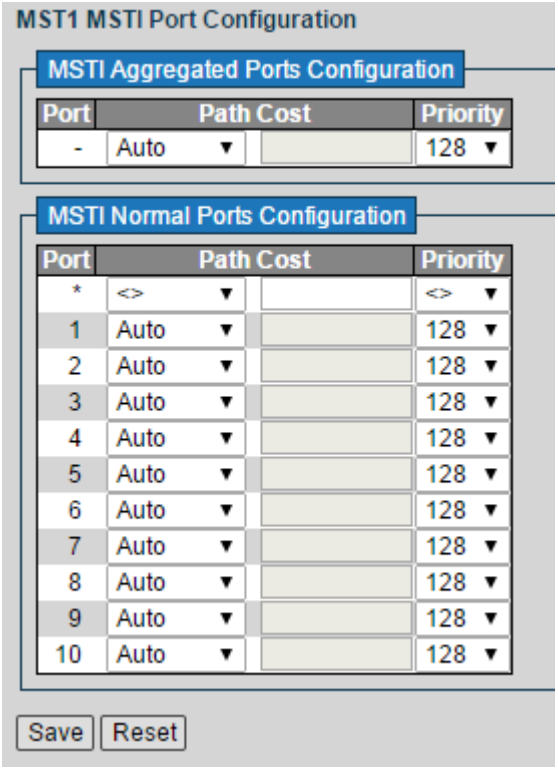
Figure 4-66 MST1 MSTI port configuration (1)



Step 2 Select MSTI from the drop-down list. 7 types are selectable. For example, you can select MST1.

Step 3 Click **Get**. See Figure 4-67 for the interface.

Figure 4-67 MST1 MSTI port configuration (2)



Step 4 Set the Path Cost and the Priority in MSTI Aggregated Ports Configuration.

Step 5 Set the Path Cost and the Priority in MSTI Normal Ports Configuration.

Step 6 Click **Save**.

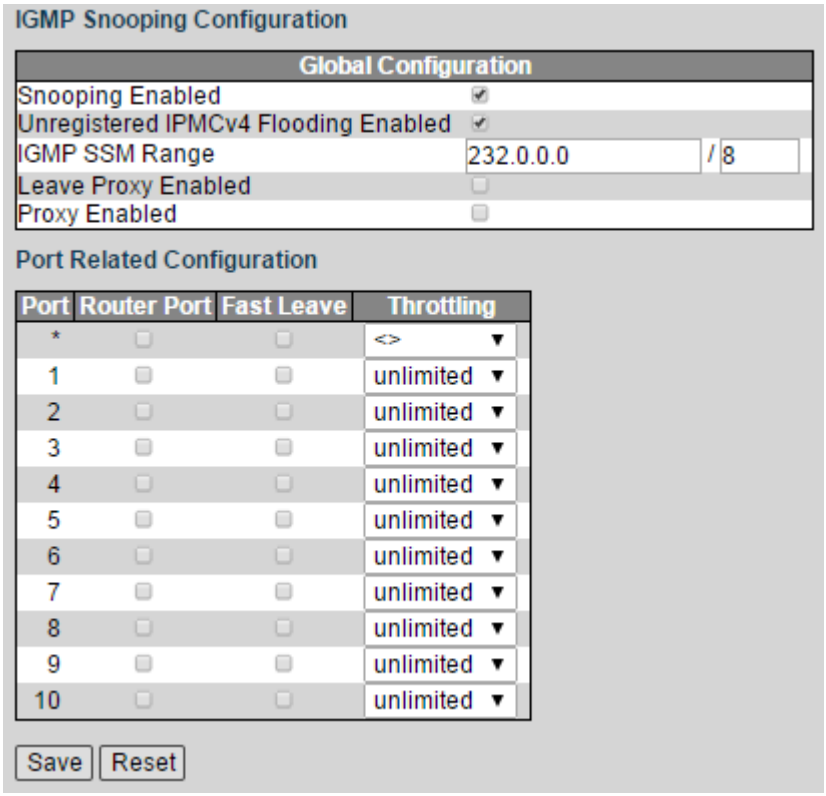
4.1.7 IGMP Snooping

IGMP Snooping (Internet Group Management Protocol Snooping) is the multicast constraint mechanism running on the device of layer 2, for managing and controlling the multicast. Through analyzing the received IGMP packet, the device of layer 2, which runs IGMP Snooping, creates the mapping between the port and the MAC multicast address, and forwards the multicast data according to the mapping.

4.1.7.1 Basic Configuration

Step 1 Select **Advanced > Configuration > IGMP Snooping > Basic Configuration**.
The IGMP Snooping Configuration is displayed. See Figure 4-68.

Figure 4-68 IGMP snooping configuration



Step 2 Set the global parameters. See Table 4-19.

Table 4-19 Global configuration

Parameter	Description
Snooping Enabled	You can select the checkbox to enable IGMP snooping.
Unregistered IPMCv4 Flooding Enabled	You can select the checkbox to enable unregistered IPMCv4 flooding.
IGMP SSM Range	Set the IGMP SSM range.
Leave Proxy Enabled	You can select the checkbox to enable leave proxy.
Proxy Enabled	You can select the checkbox to enable proxy.

Step 3 Set the parameters in Port Related Configuration. See Table 4-20.

Table 4-20 Port related configuration

Parameter	Description
Router Port	Select the checkbox to set the router port.
Fast Leave	You can select the checkbox to enable the fast leave function for the port. Fast leave means when the switch receives the IGMP leave packet from the host through a certain port, the switch deletes the port from the port list in the forward table directly. Then, when the switch receives the IGMP specific group query packet for the multicast, the switch will not forward it to that port. You can enable the port fast leave to reduce bandwidth and resource cost.
Throttling	Set the threshold from the drop-down list.

Step 4 Click **Save**.

4.1.7.2 VLAN Configuration

Step 1 Select **Advanced > Configuration > IGMP Snooping > VLAN Configuration**.

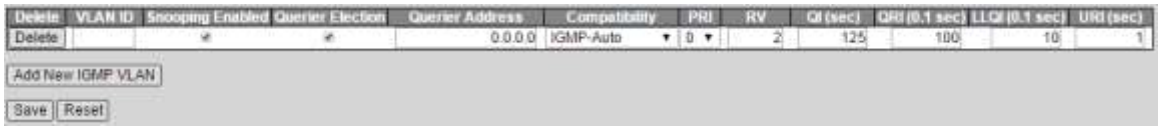
The IGMP Snooping VLAN Configuration is displayed. See Figure 4-69.

Figure 4-69 IGMP snooping VLAN configuration

Step 2 Click **Add New IGMP VLAN**.

A new record is added. See Figure 4-70.

Figure 4-70 Enable IGMP snooping in a certain VLAN.



Step 3 Set the parameters including VLAN ID, Snooping Enabled, and so on.

Step 4 Click **Save**.

4.1.8 LLDP

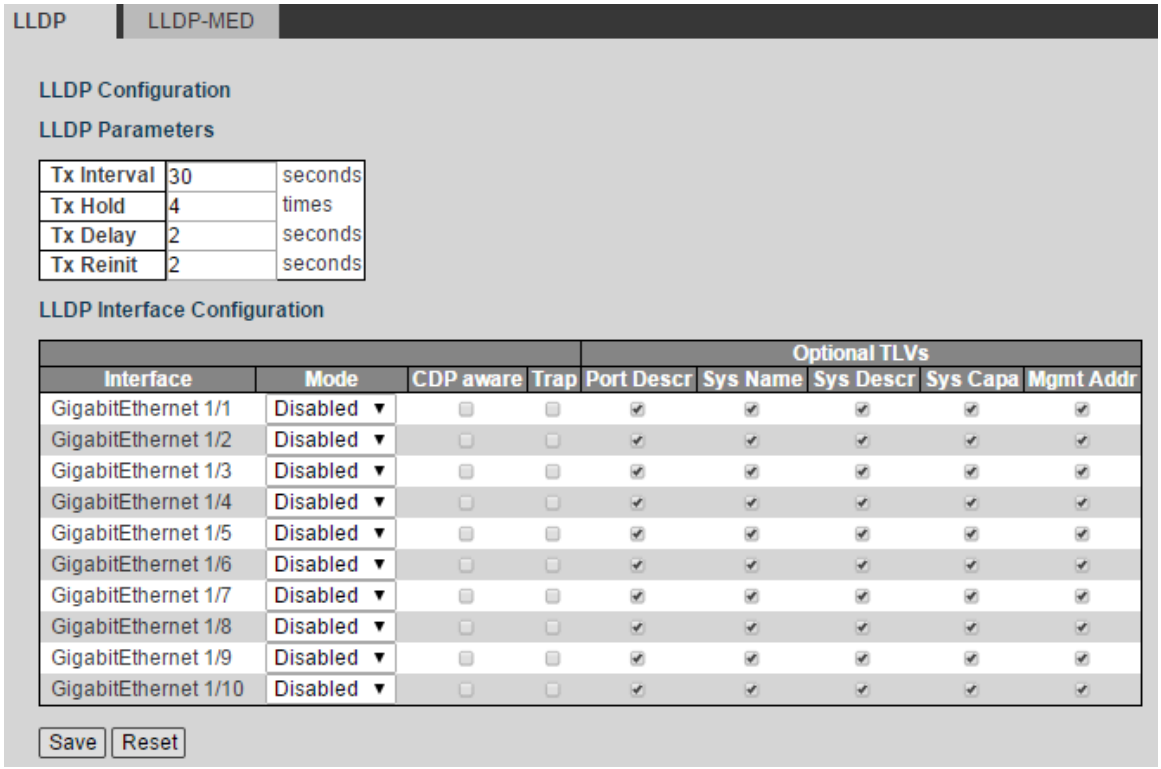
LLDP (Link Layer Discovery Protocol) is the standard link layer discovery protocol. It can organize the information including main ability, management address, device identification, and interface identification of the device into different TLV(Type Length Value), and package in the LLDPDU (Link Layer Discovery Protocol Data Unit) to release to the neighbors connected to itself directly. The neighbors receive the information, and save it in standard MIB (Management Information Base) format, for the network management system to quiry and judge the link communication status.

LLDP

Step 1 Select **Advanced > Configuration > LLDP**.

The LLDP Configuration interface is displayed. See Figure 4-71.

Figure 4-71 LLDP configuration



Step 2 Set the parameters including Tx Interval, Tx Hold, Tx Delay, and Tx Reinit in LLDP Parameters.

Step 3 Set the parameters including Mode, CDP aware, Trap, and son on in LLDP Interface Configuration.

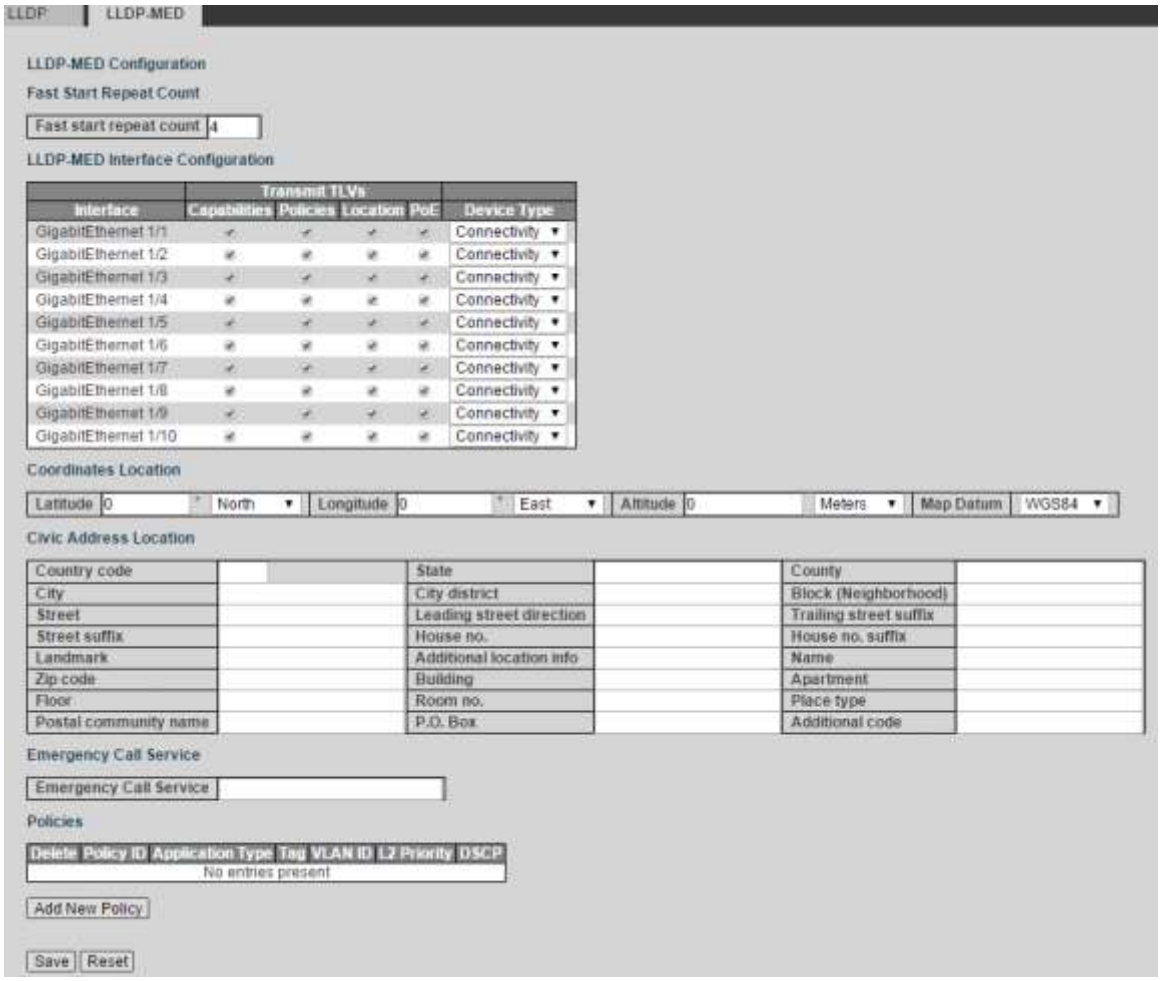
Step 4 Click **Save**.

LLDP-MED

Step 1 Select **Advanced > Configuration > LLDP > LLDP-MED**.

The LLDP-MED Configuration interface is displayed. See Figure 4-72.

Figure 4-72 LLDP-MED configuration



Step 2 Set the Fast Start Repeat Count.

Step 3 Set the Transmit TLVs and the Device Type in LLDP-MED Interface Configuration.

Step 4 Set the location information in Coordinates Location.

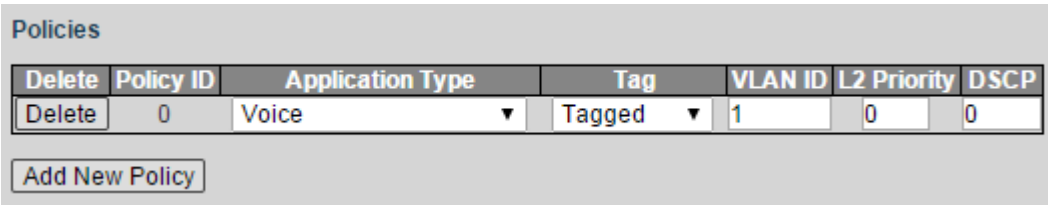
Step 5 Set the parameters including Country code, State, Country, City, City district, and so on in Civic Address Location.

Step 6 Add the ermergency phone number in Emergency Call Service.

Step 7 Click **Add New Policy**.

A new record is added. See Figure 4-73.

Figure 4-73 Add new policy



Step 8 Set the parameters including Application Type, Tag, VLAN ID and so on.

Step 9 Click **Save**.

4.1.9 PoE

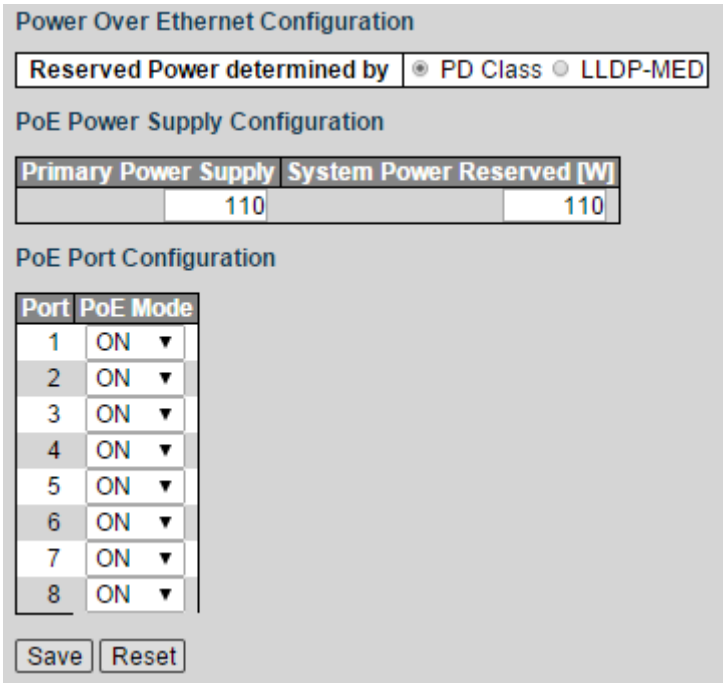
PoE (Power Over Ethernet) is the function that through Ethernet RJ45 port, the device can provide power for the external PD remotely with twisted pair. PoE function helps to centralize power supply and facilitate backup. The network terminal does not need the external power

source anymore, and one network cable is enough, It conforms to the standards of IEEE 802.3af and IEEE 802.3at, adopting the power interface globally agreed. It can be applied in IP telephone, wireless AP (Access Point), portable device charger, card reader, network camera, date collection, and so on.

Step 1 Select **Advanced > Configuration > PoE**.

The Power Over Ethernet Configuration interface is displayed. See Figure 4-74.

Figure 4-74 PoE configuration



Step 2 Select **PD Class** or **LLDP-MED** for Reserved Power. By default, **PD Class** is selected.

Step 3 Set the Primary Power Supply and the System Power Reserved in PoE Power Supply Configuration.

Step 4 Select **ON** or **OFF** for PoE Mode from the drop-down list.

Step 5 Click **Save**.

4.1.10 MAC Table

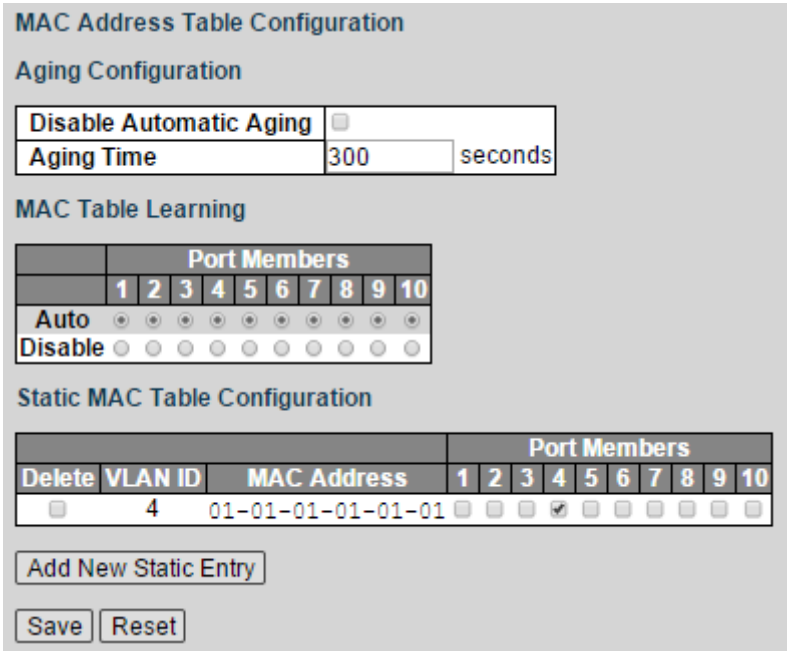
MAC (Media Access Control) Table records the relationship between the MAC address and the port, and the information including the VLAN that the port belongs to. When the device is forwarding the packet, it queries in the MAC address table for the destination MAC address of the packet. If the destination MAC address of the packet is contained in the MAC address table, the packet is forwarded through the port in the table directly. And if the destination MAC address of the packet is not contained in the MAC address table, the device adopts broadcasting to forward the packet to all the ports except the receiving port in VLAN.

You can set aging configuration, MAC table learning, and static MAC table configuration.

Step 1 Select **Advanced > Configuration > MAC Table**.

The MAC Address Table Configuration interface is displayed. See Figure 4-75.

Figure 4-75 MAC address table configuration



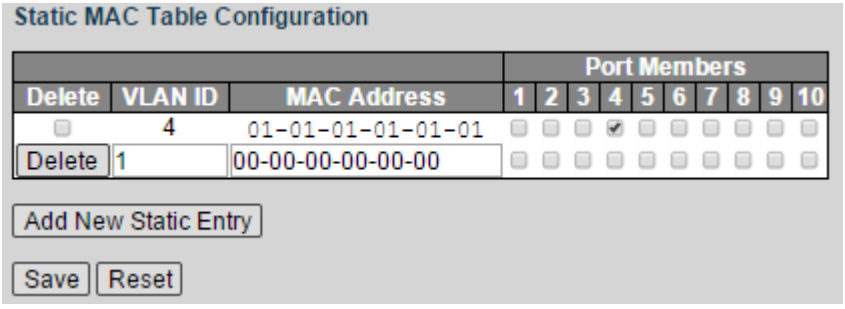
Step 2 Select **Disable Automatic Aging**, and set the Aging Time. By default, it is 300 seconds.

Step 3 Select **Auto** or **Disable** to enable or disable MAC table learning.

Step 4 Bind the MAC address to the port in the certain VLAN. For example, bind the MAC address 00-00-00-00-00-01 to the port 8 in VLAN 2.

1) Click **Add New Static Entry** in Static MAC Table Configuration.
A new record is added. See Figure 4-76.

Figure 4-76 Static MAC table configuration



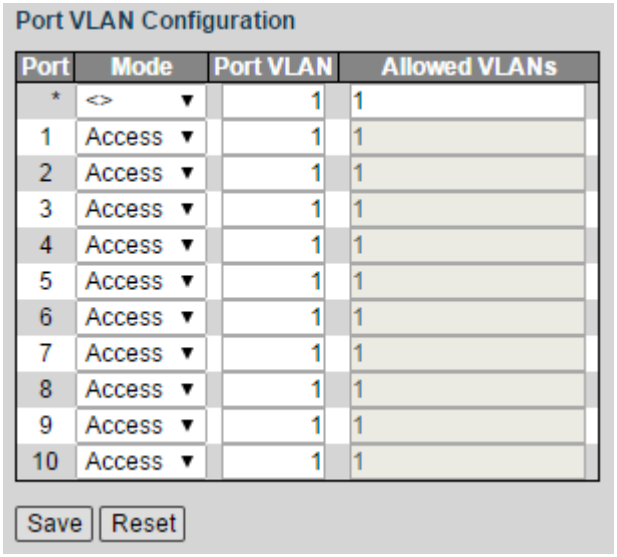
2) Set the parameters including VLAN ID, MAC address, and port members.

Step 5 Click **Save**.

4.1.11 VLANs

Select **Advanced > Configuration > VLANs**. The Port VLAN Configuration interface is displayed. See Figure 4-77. See “3.3 VLAN” for details.

Figure 4-77 Port VLAN configuration



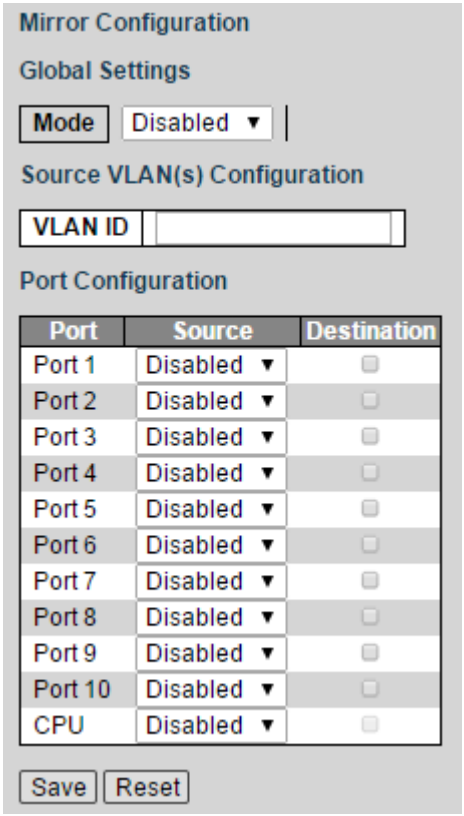
4.1.12 Mirroring

Port mirroring is also called port monitoring. Port monitoring is the data package acquiring technology that through configuring switch, data package from one or several ports (mirroring source ports) can be copied to a specific port (mirroring destination port). The mirroring destination port connects to a PC that data package analyzing software is installed, and it can analyze the received data package for network monitoring and troubleshooting.

Step 1 Select **Advanced > Configuration > Mirroring**.

The Mirror Configuration interface is displayed. See Figure 4-78.

Figure 4-78 Mirror configuration



Step 2 Select Mode as **Enabled** to enable mirroring function.

Step 3 Input the VLAN ID in Source VLAN(s) Configuration.

Step 4 Configure the Source and the Destination in Port Configuration.

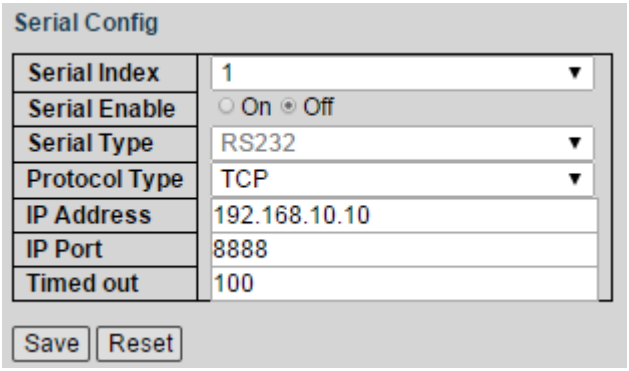
Step 5 Click **Save**.

4.1.13 Serial Config

Set the conversion between the asynchronous serial port and the Ethernet.

Select **Advanced > Configuration > Serial Config**. The Serial Config interface is displayed. See 错误!未找到引用源。.

Figure 4-79 Serial Config



4.2 Monitor

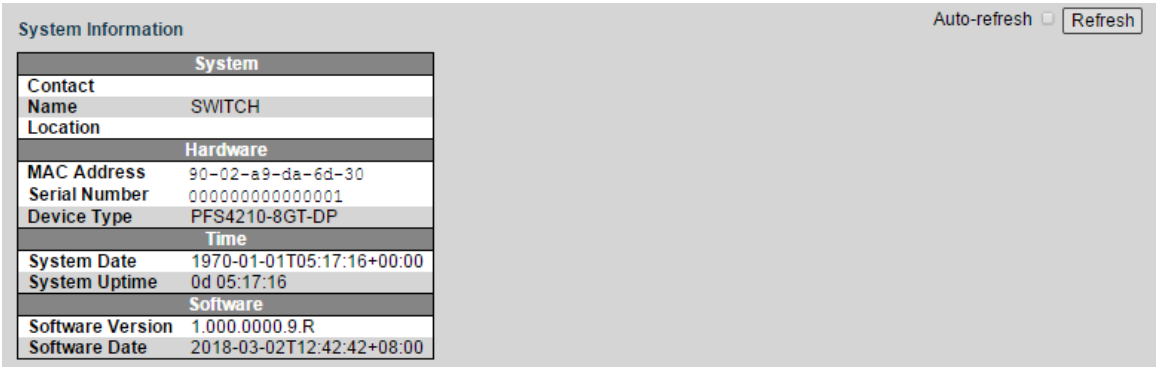
4.2.1 System

4.2.1.1 Information

You can view the system information of the device, including system, hardware, time, and software.

Select **Advanced > Monitor > System > Information**. The System Information interface is displayed. See Figure 4-80.

Figure 4-80 Information



4.2.1.2 CPU Load

You can view the CPU load within the unit interval. The lines of three different colors stand for the CPU load rate in different time intervals.

Select **Advanced > Monitor > System > CPU Load**. The CPU Load interface is displayed. See Figure 4-81.

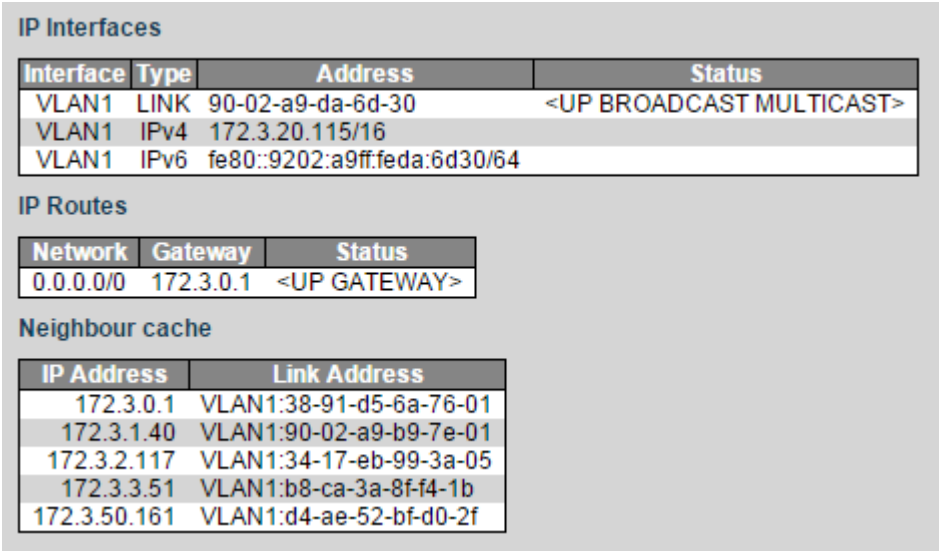
Figure 4-81 CPU load

4.2.1.3 IP Status

You can view the IP status including IP interfaces, IP routes, and neighbour cache.

Select **Advanced > Monitor > System > IP Status**. The IP Status interface is displayed. See Figure 4-82.

Figure 4-82 IP Status



IP Interfaces

Interface	Type	Address	Status
VLAN1	LINK	90-02-a9-da-6d-30	<UP BROADCAST MULTICAST>
VLAN1	IPv4	172.3.20.115/16	
VLAN1	IPv6	fe80::9202:a9ff:feda:6d30/64	

IP Routes

Network	Gateway	Status
0.0.0.0/0	172.3.0.1	<UP GATEWAY>

Neighbour cache

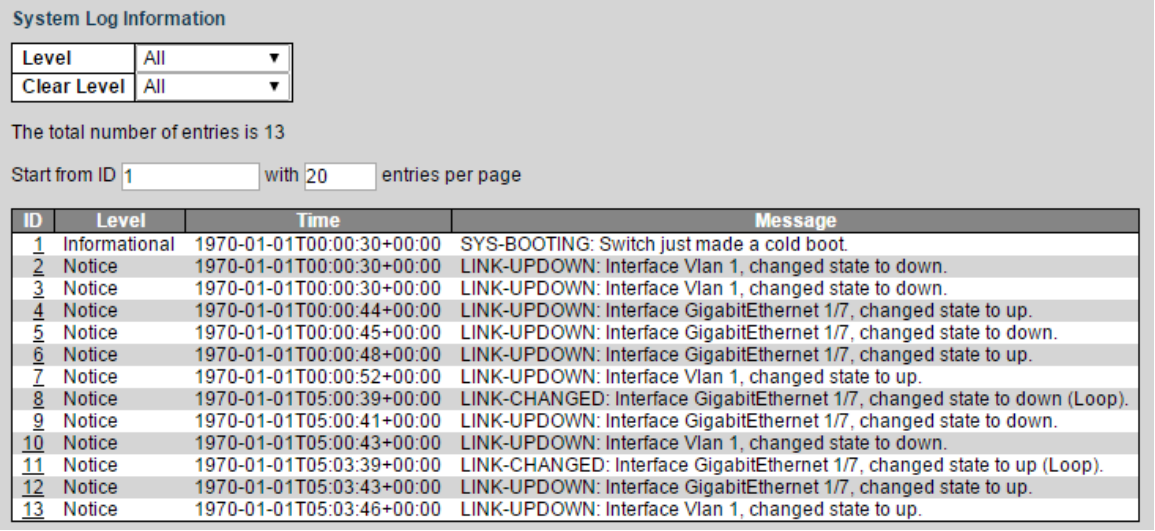
IP Address	Link Address
172.3.0.1	VLAN1:38-91-d5-6a-76-01
172.3.1.40	VLAN1:90-02-a9-b9-7e-01
172.3.2.117	VLAN1:34-17-eb-99-3a-05
172.3.3.51	VLAN1:b8-ca-3a-8f-f4-1b
172.3.50.161	VLAN1:d4-ae-52-bf-d0-2f

4.2.1.4 Log

You can view the logs according to the Level, and clear the logs as the Clear Level.

Select **Advanced > Monitor > System > Log**. The System Log Information interface is displayed. See Figure 4-83.

Figure 4-83 System log information



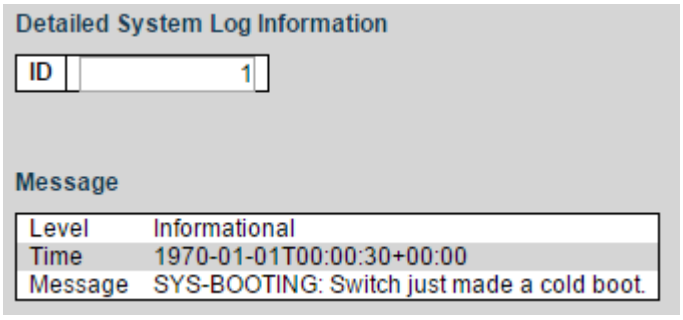
ID	Level	Time	Message
1	Informational	1970-01-01T00:00:30+00:00	SYS-BOOTING: Switch just made a cold boot.
2	Notice	1970-01-01T00:00:30+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
3	Notice	1970-01-01T00:00:30+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
4	Notice	1970-01-01T00:00:44+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/7, changed state to up.
5	Notice	1970-01-01T00:00:45+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/7, changed state to down.
6	Notice	1970-01-01T00:00:48+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/7, changed state to up.
7	Notice	1970-01-01T00:00:52+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.
8	Notice	1970-01-01T05:00:39+00:00	LINK-CHANGED: Interface GigabitEthernet 1/7, changed state to down (Loop).
9	Notice	1970-01-01T05:00:41+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/7, changed state to down.
10	Notice	1970-01-01T05:00:43+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to down.
11	Notice	1970-01-01T05:03:39+00:00	LINK-CHANGED: Interface GigabitEthernet 1/7, changed state to up (Loop).
12	Notice	1970-01-01T05:03:43+00:00	LINK-UPDOWN: Interface GigabitEthernet 1/7, changed state to up.
13	Notice	1970-01-01T05:03:46+00:00	LINK-UPDOWN: Interface Vlan 1, changed state to up.

4.2.1.5 Detailed Log

You can view the detailed information of the logs.

Select **Advanced > Monitor > System > Detailed Log**. The Detailed System Log Information interface is displayed. See Figure 4-84.

Figure 4-84 Detailed system log information



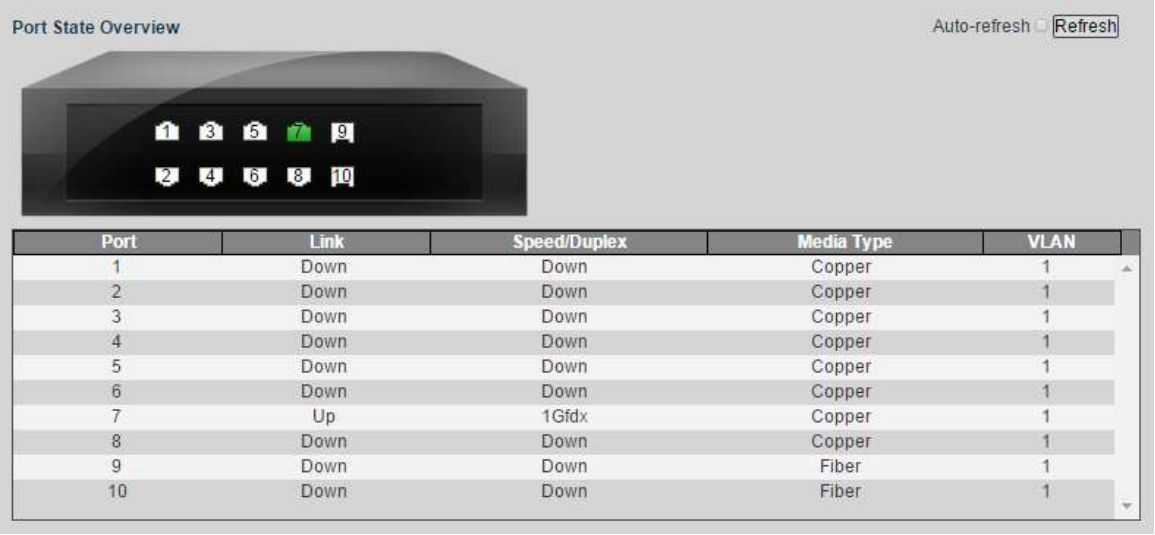
4.2.2 Ports

4.2.2.1 State

You can view the port information including link, speed/duplex, media type, and VLAN. If the port link is displayed as green, it is connected successfully. And if the port link is displayed as white, it is not connected.

Select **Advanced > Monitor > Ports > State**. The Port State Overview interface is displayed. See Figure 4-85. See Table 4-21 for detailed information of port.

Figure 4-85 Port status overview



Port	Link	Speed/Duplex	Media Type	VLAN
1	Down	Down	Copper	1
2	Down	Down	Copper	1
3	Down	Down	Copper	1
4	Down	Down	Copper	1
5	Down	Down	Copper	1
6	Down	Down	Copper	1
7	Up	1Gfdx	Copper	1
8	Down	Down	Copper	1
9	Down	Down	Fiber	1
10	Down	Down	Fiber	1

Table 4-21 Port information

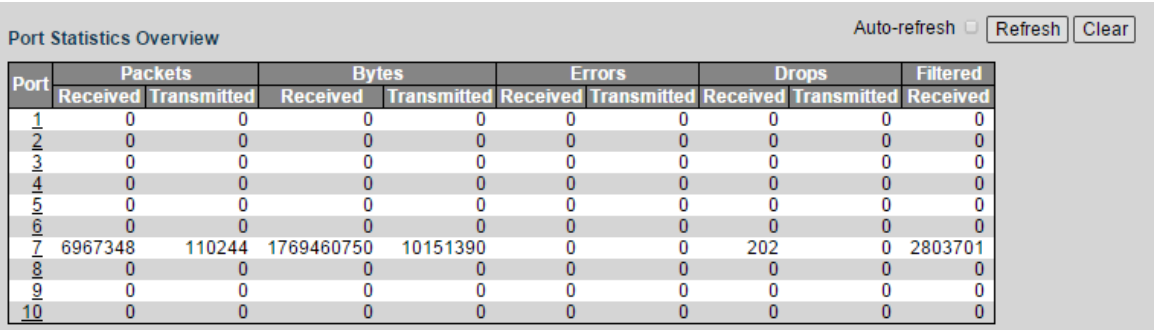
Parameter	Description
Ports	Display all the ports.
Link	Two link states: **Up**, **Down**. Up indicated the port is connected successfully, and Down indicates the port is not connected.
Speed/Duplex	Display the port rate and the duplex mode.
Media Type	Two media types: **Copper**, **Fiber**. Copper is the RJ45 port, and Fiber is the fiber port.
VLAN	Display the port VLAN. By default, it is VLAN 1.

4.2.2.2 Traffic Overview

You can view the packers, bytes, errors, drops, and filerd information of the ports.

Select Advanced > Monitor > Ports > Traffic Overview. The Port Statistics Overview interface is displayed. See Figure 4-86.

Figure 4-86 Port statistics overview



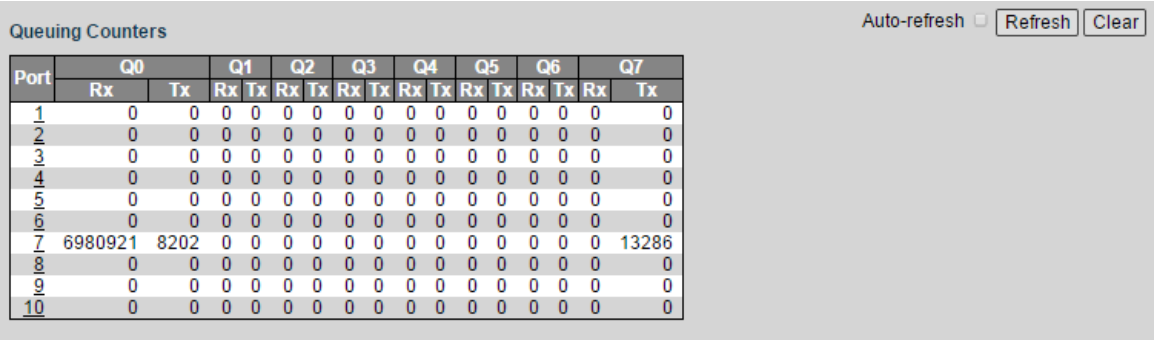
Port	Packets		Bytes		Errors		Drops		Filtered
	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received	Transmitted	Received
1	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0
7	6967348	110244	1769460750	10151390	0	0	202	0	2803701
8	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0

4.2.2.3 QoS Statistics

You can view the QoS statistics of the ports.

Select **Advanced > Monitor > Ports > QoS Statistics**. The Queuing Counters interface is displayed. See Figure 4-87.

Figure 4-87 Queuing counters



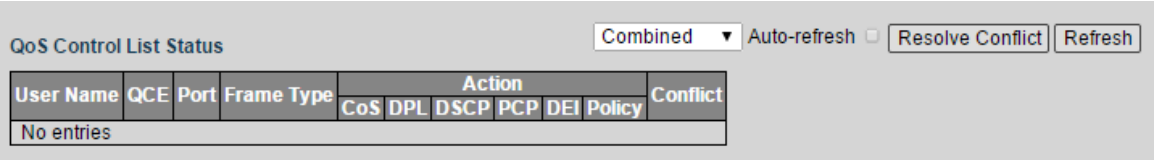
Port	Q0		Q1		Q2		Q3		Q4		Q5		Q6		Q7	
	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx	Rx	Tx
1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	6980921	8202	0	0	0	0	0	0	0	0	0	0	0	0	0	13286
8	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
9	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
10	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

4.2.2.4 QCL Status

You can view the QoS control list status, including user name, QCE, port, frame type, action, and conflict.

Select **Advanced > Monitor > Ports > QCL Status**. The QoS Control List Status interface is displayed. See Figure 4-88.

Figure 4-88 QoS control list status



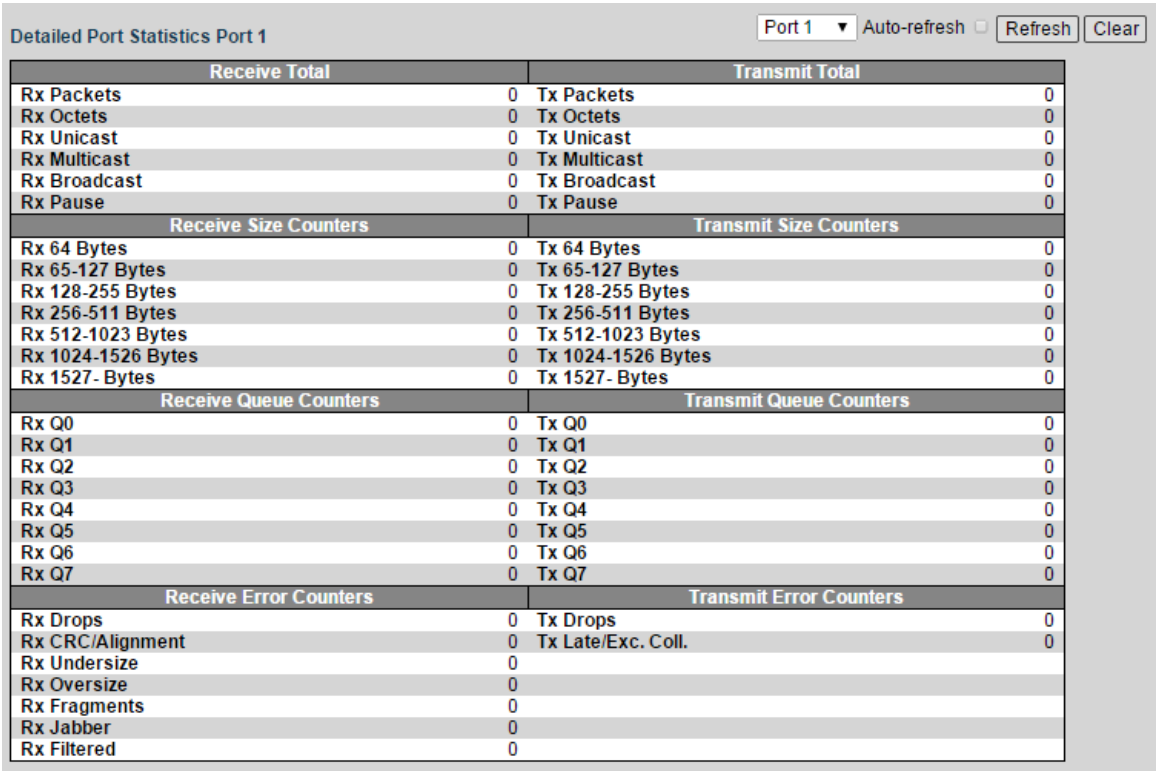
User Name	QCE	Port	Frame Type	Action						Conflict
				CoS	DPL	DSCP	PCP	DEI	Policy	
No entries										

4.2.2.5 Detailed Statistics

You can view the detailed statistics of the port by selecting the port on the upper right in the interface.

Select **Advanced > Monitor > Ports > Detailed Statistics**. The Detailed Port Statistics Port 1 interface is displayed. See Figure 4-89.

Figure 4-89 Detailed Port statistics port 1



Receive Total		Transmit Total	
Rx Packets	0	Tx Packets	0
Rx Octets	0	Tx Octets	0
Rx Unicast	0	Tx Unicast	0
Rx Multicast	0	Tx Multicast	0
Rx Broadcast	0	Tx Broadcast	0
Rx Pause	0	Tx Pause	0
Receive Size Counters		**Transmit Size Counters**	
Rx 64 Bytes	0	Tx 64 Bytes	0
Rx 65-127 Bytes	0	Tx 65-127 Bytes	0
Rx 128-255 Bytes	0	Tx 128-255 Bytes	0
Rx 256-511 Bytes	0	Tx 256-511 Bytes	0
Rx 512-1023 Bytes	0	Tx 512-1023 Bytes	0
Rx 1024-1526 Bytes	0	Tx 1024-1526 Bytes	0
Rx 1527- Bytes	0	Tx 1527- Bytes	0
Receive Queue Counters		**Transmit Queue Counters**	
Rx Q0	0	Tx Q0	0
Rx Q1	0	Tx Q1	0
Rx Q2	0	Tx Q2	0
Rx Q3	0	Tx Q3	0
Rx Q4	0	Tx Q4	0
Rx Q5	0	Tx Q5	0
Rx Q6	0	Tx Q6	0
Rx Q7	0	Tx Q7	0
Receive Error Counters		**Transmit Error Counters**	
Rx Drops	0	Tx Drops	0
Rx CRC/Alignment	0	Tx Late/Exc. Coll.	0
Rx Undersize	0		
Rx Oversize	0		
Rx Fragments	0		
Rx Jabber	0		
Rx Filtered	0		

4.2.3 DHCP

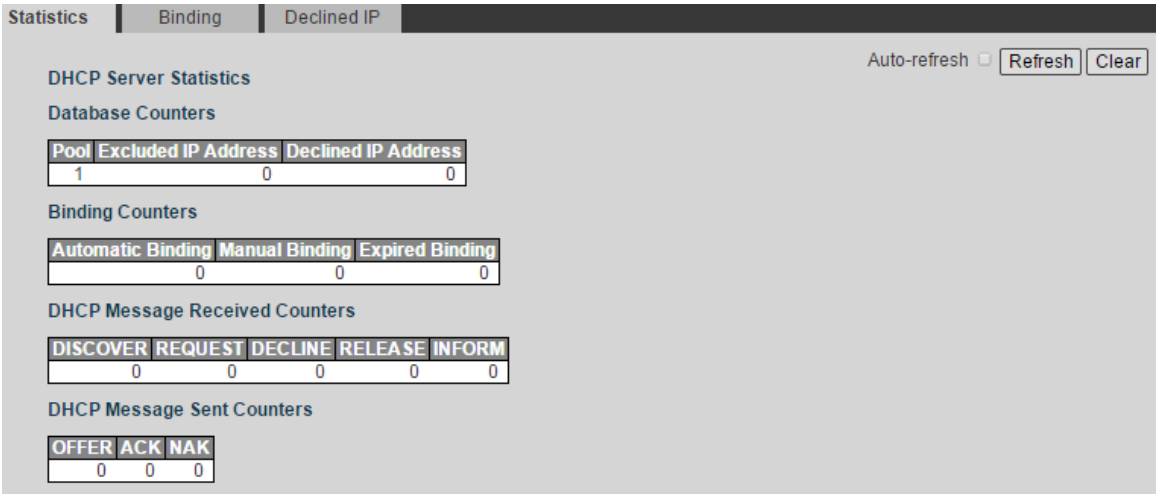
4.2.3.1 Server

Statistics

You can view the DHCP server statistics, including database counters, binding counters, DHCP packet received counters, and DHCP packet sent counters.

Select **Advanced > Monitor > DHCP > Server**. The DHCP Server Statistics interface is displayed. See Figure 4-90.

Figure 4-90 DHCP server statistics



Binding

You can view the DHCP server binding IP address.

Select **Advanced > Monitor > DHCP > Server > Binding**. The DHCP Server Binding IP interface is displayed. See Figure 4-91.

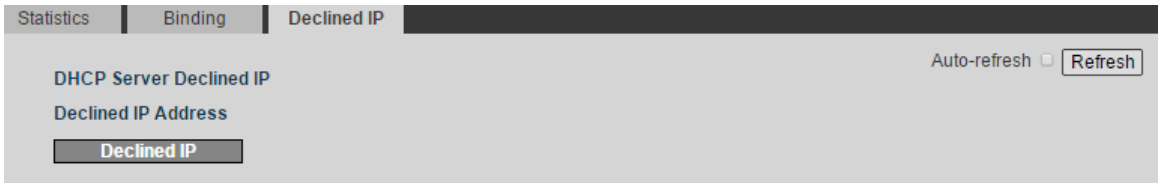
Figure 4-91 DHCP server binding IP

Declined IP

You can view the declined IP.

Select **Advanced > Monitor > DHCP > Server > Declined IP**. The DHCP Server Declined IP interface is displayed. See Figure 4-92.

Figure 4-92 Declined IP

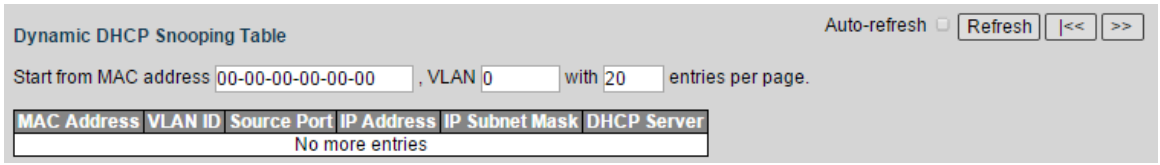


4.2.3.2 Snooping Table

You can view the dynamic DHCP snooping table.

Select **Advanced > Monitor > DHCP > Snooping Table**. The Dynamic DHCP Snooping Table interface is displayed. See Figure 4-93.

Figure 4-93 Dynamic DHCP snooping table

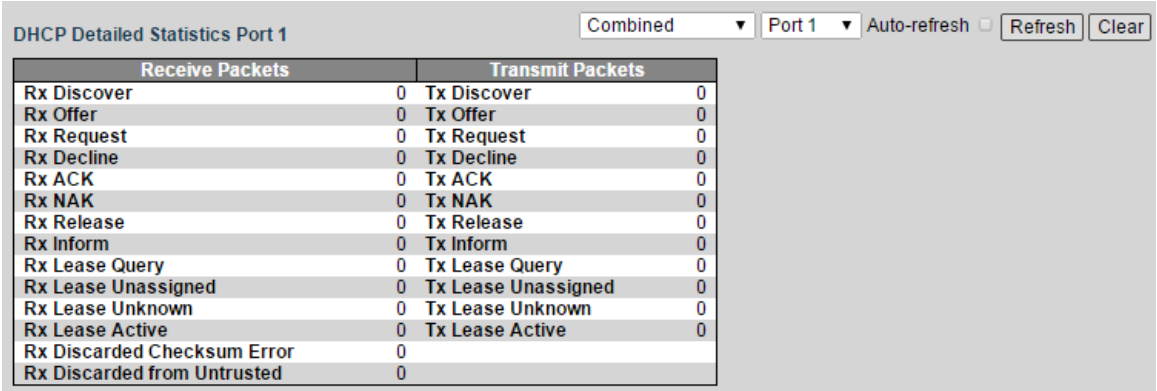


4.2.3.3 Detailed Statistics

You can view the DHCP detailed statistics of the port by selecting the port on the upper right in the interface.

Select **Advanced > Monitor > DHCP > Detailed Statistics**. The DHCP Detailed Statistics Port 1 interface is displayed. See Figure 4-94.

Figure 4-94 DHCP detailed statistics port 1



4.2.4 Security

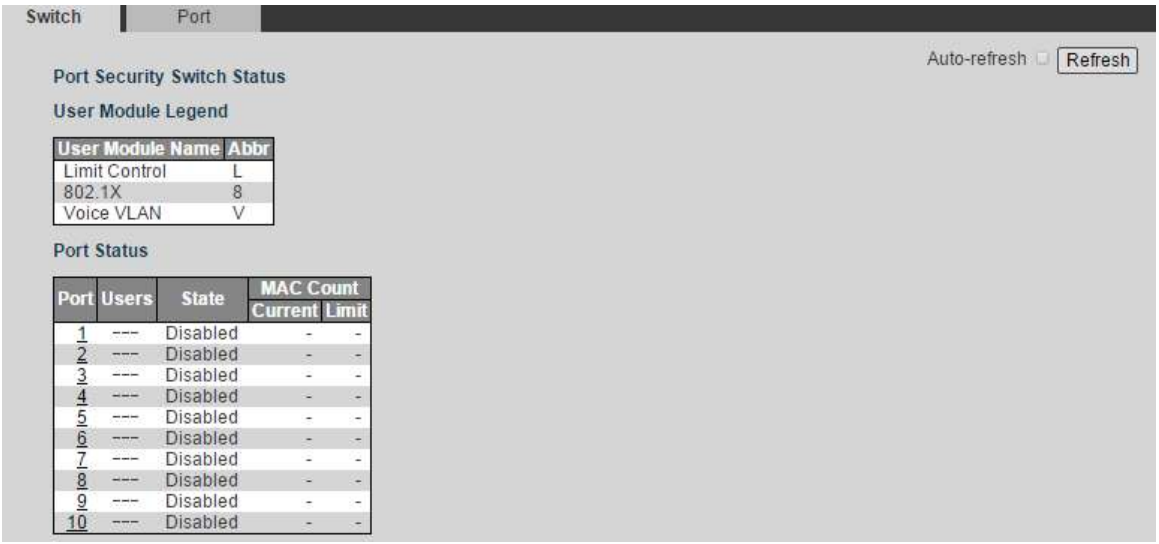
4.2.4.1 Port Security

Switch

You can view the port security switch status.

Select **Advanced > Monitor > Security > Port Security**. The Port Security Switch Status interface is displayed. See Figure 4-95.

Figure 4-95 Port security switch status



Port

You can view the port information including MAC address, VLAN ID, state, time of addition, and aged/hold.

Select **Advanced > Monitor > Security > Port Security > Port**. The Port interface is displayed. See Figure 4-96.

Figure 4-96 Port

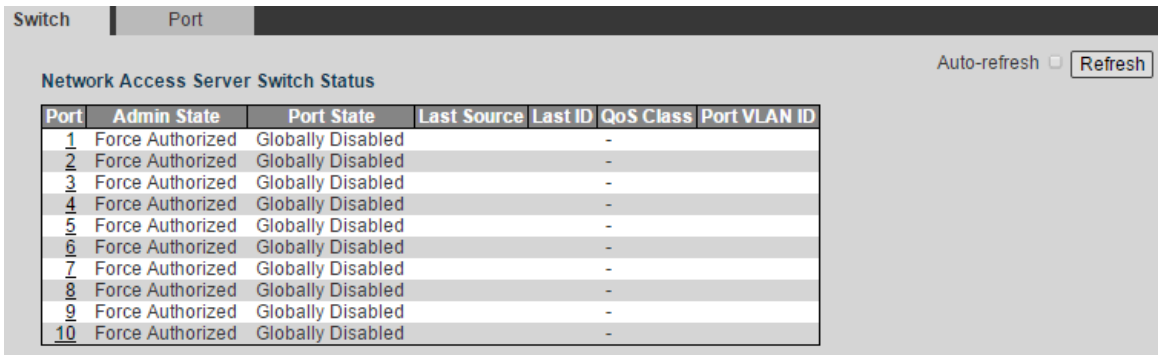
4.2.4.2 NAS

Switch

You can view network access server switch status.

Select **Advanced > Monitor > Security > NAS**. The Network Access Server Switch Status interface is displayed. See Figure 4-97.

Figure 4-97 Network access server switch status

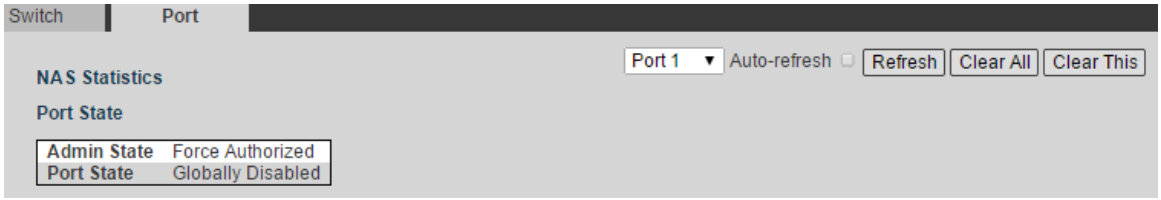


Port

You can view the port status.

Select **Advanced > Monitor > Security > NAS > Port**. The NAS Statistics interface is displayed. See Figure 4-98.

Figure 4-98 NAS statistics

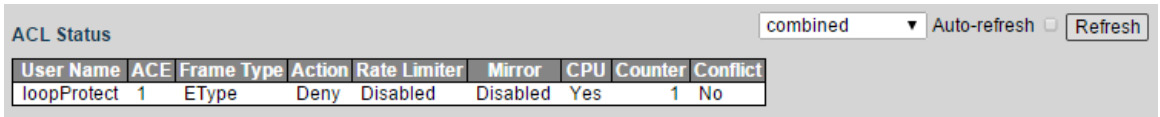


4.2.4.3 ACL Status

You can view the ACL status.

Select **Advanced > Monitor > Security > ACL Status**. The ACL Status interface is displayed. See Figure 4-99.

Figure 4-99 ACL status

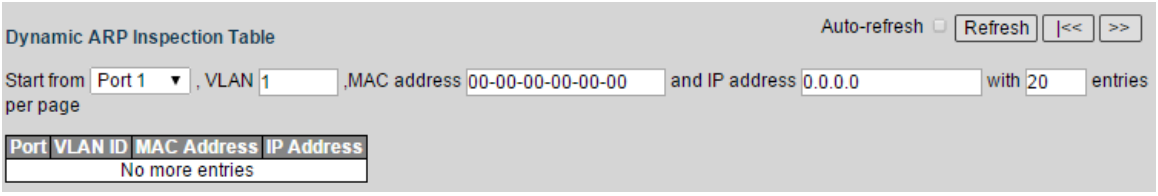


4.2.4.4 ARP Inspection

You can view dynamic ARP inspection table.

Select **Advanced > Monitor > Security > ARP Inspection**. The Dynamic ARP Inspection Table interface is displayed. See Figure 4-100.

Figure 4-100 Dynamic ARP inspection table

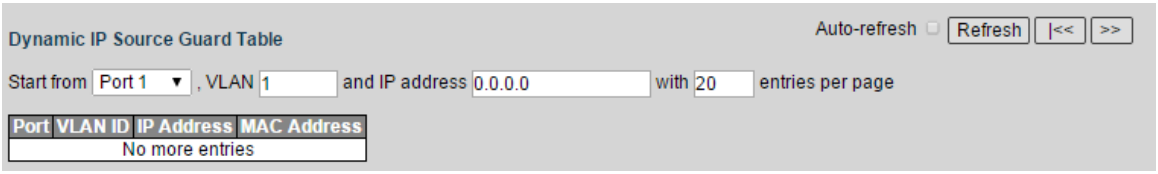


4.2.4.5 IP Source Guard

You can view the dynamic IP source guard table.

Select **Advanced > Monitor > Security > IP Source Guard**. The Dynamic IP Source Guard Table interface is displayed. See Figure 4-101.

Figure 4-101 Dynamic IP source guard table

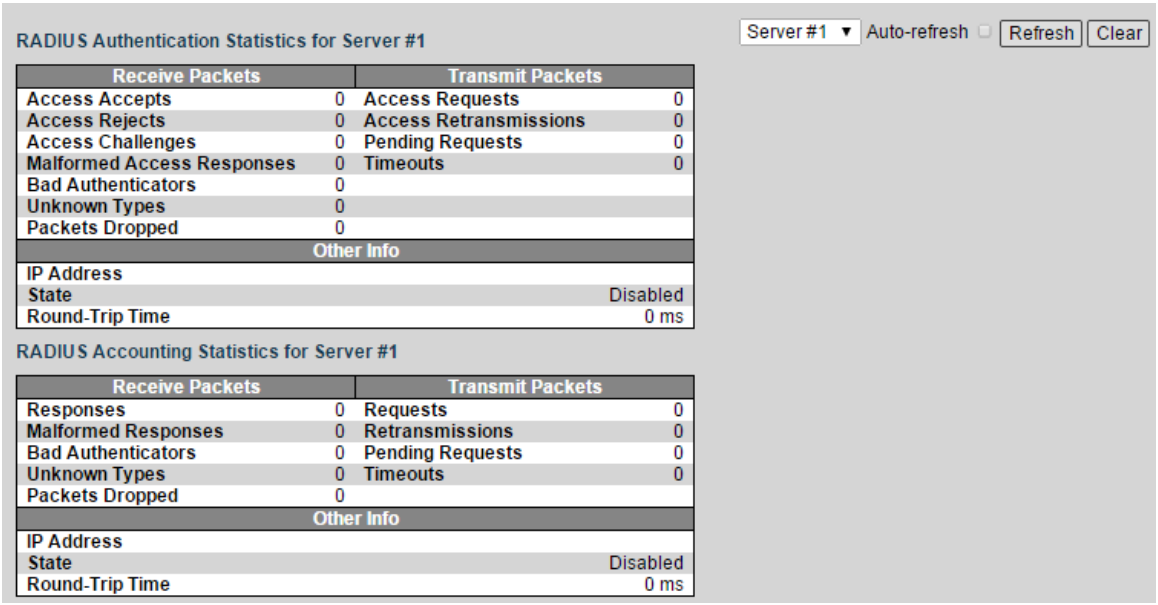


4.2.4.6 RADIUS Details

You can view the RADIUS details.

Select **Advanced > Monitor > Security > RADIUS Details**. The RADIUS Authentication Statistics for Server #1 interface is displayed. See Figure 4-102.

Figure 4-102 RADIUS authentication statistics for server #1



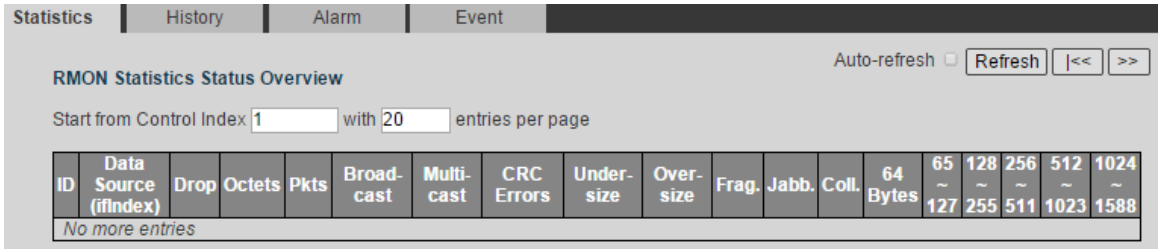
4.2.4.7 RMON

Statistics

You can view the RMON statistics status.

Select **Advanced > Monitor > Security > RMON**. The RMON Statistics Status Overview interface is displayed. See Figure 4-103.

Figure 4-103 RMON statistics status overview

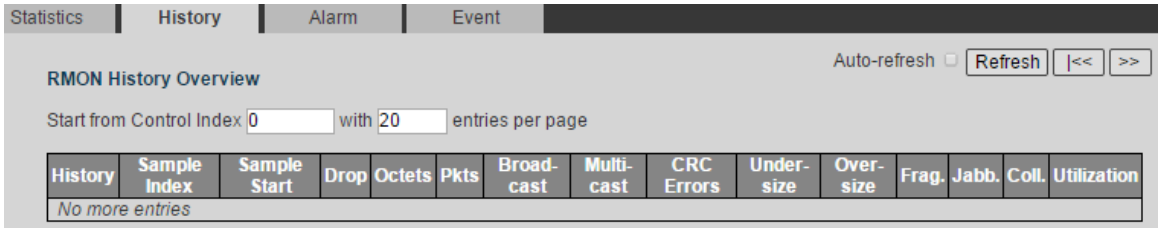


History

You can view the RMON history.

Select **Advanced > Monitor > Security > RMON > History**. The RMON History Overview interface is displayed. See Figure 4-104.

Figure 4-104 RMON history overview

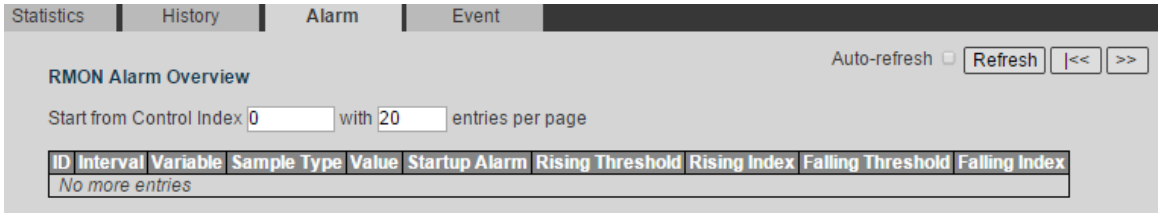


Alarm

You can view the RMON alarm information.

Select **Advanced > Monitor > Security > RMON > Alarm**. The RMON Alarm Overview interface is displayed. See Figure 4-105.

Figure 4-105 RMON alarm overview

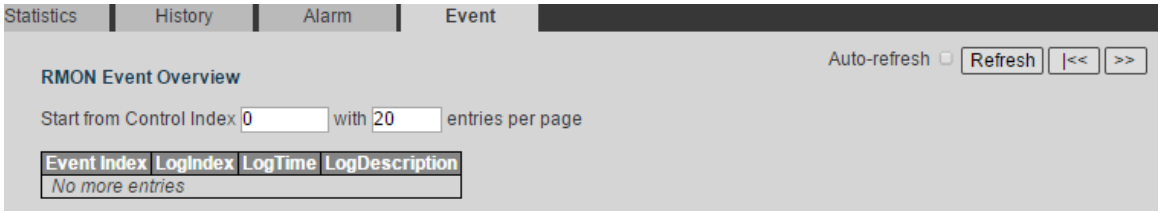


Event

You can view the RMON event information.

Select **Advanced > Monitor > Security > RMON > Event**. The RMON Event Overview interface is displayed. See Figure 4-106.

Figure 4-106 RMON event overview

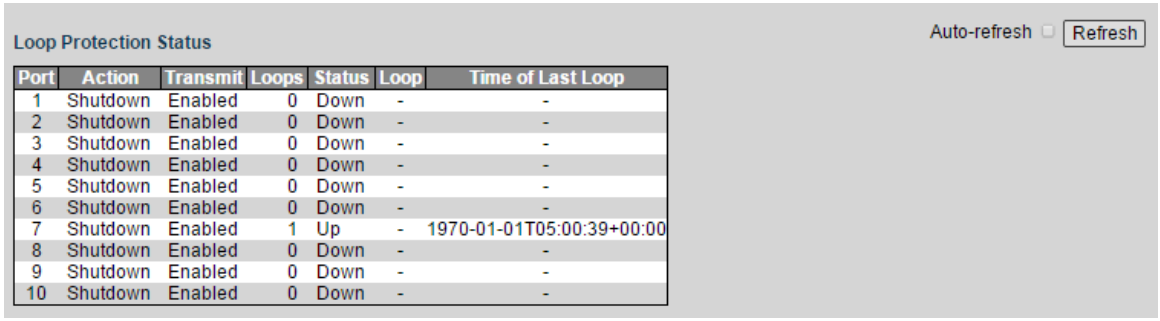


4.2.4.8 Loop Protection

You can view loop protection status.

Select **Advanced > Monitor > Security > Loop Protection**. The Loop Protection Status interface is displayed. See Figure 4-107.

Figure 4-107 Loop protection status



Port	Action	Transmit	Loops	Status	Loop	Time of Last Loop
1	Shutdown	Enabled	0	Down	-	-
2	Shutdown	Enabled	0	Down	-	-
3	Shutdown	Enabled	0	Down	-	-
4	Shutdown	Enabled	0	Down	-	-
5	Shutdown	Enabled	0	Down	-	-
6	Shutdown	Enabled	0	Down	-	-
7	Shutdown	Enabled	1	Up	-	1970-01-01T05:00:39+00:00
8	Shutdown	Enabled	0	Down	-	-
9	Shutdown	Enabled	0	Down	-	-
10	Shutdown	Enabled	0	Down	-	-

4.2.5 Aggregation

4.2.5.1 Static

You can view the aggregation static configuration.

Select **Advanced > Monitor > Aggregation > Static**. The Aggregation Status interface is displayed. See Figure 4-108.

Figure 4-108 Aggregation status

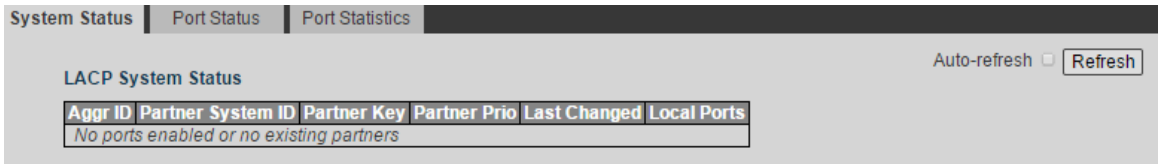
4.2.5.2 LACP

System Status

You can view the system status of aggregation dynamic configuration.

Select **Advanced > Monitor > Aggregation > LACP**. The LACP System Status interface is displayed. See Figure 4-109.

Figure 4-109 LACP system status

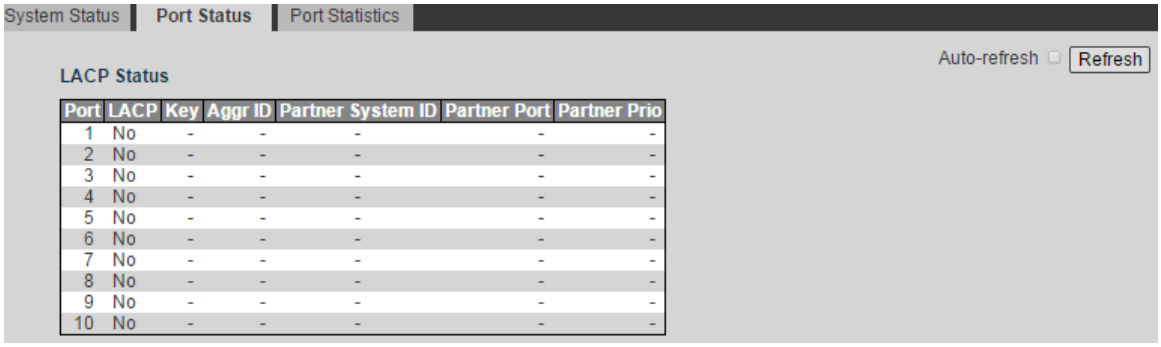


Port Status

You can view the port status of aggregation dynamic configuration.

Select **Advanced > Monitor > Aggregation > LACP > Port Status**. The LACP Status interface is displayed. See Figure 4-110.

Figure 4-110 LACP status

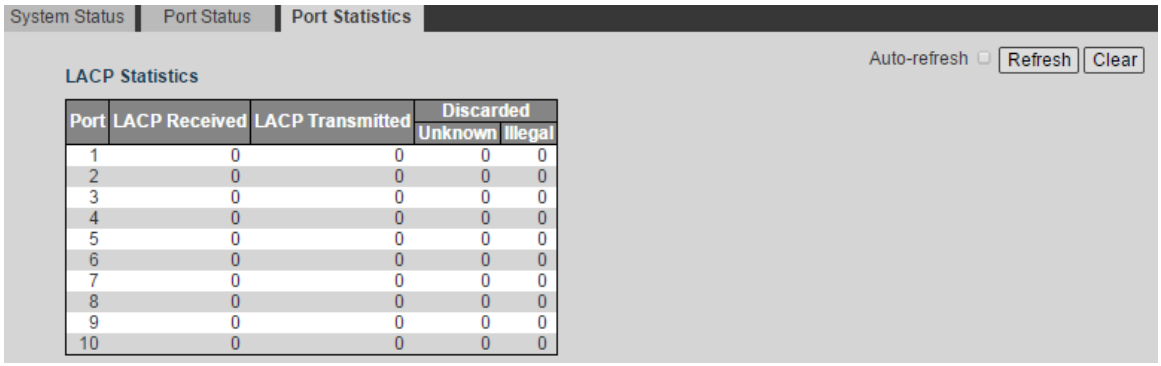


Port Statistics

You can view the port statistics of aggregation dynamic configuration.

Select **Advanced > Monitor > Aggregation > LACP > Port Statistics**. The LACP Statistics interface is displayed. See Figure 4-111.

Figure 4-111 LACP Statistics



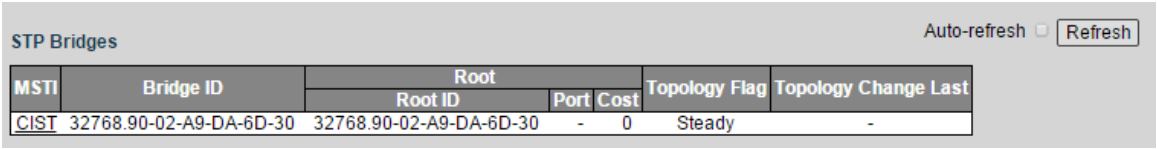
4.2.6 Spanning Tree

4.2.6.1 Bridge Status

You can view the STP bridge status, including MSTI, bridge ID, root, topology flag, and topology change last.

Select **Advanced > Monitor > Spanning Tree > Bridge Status**. The STP Bridge interface is displayed. See Figure 4-112.

Figure 4-112 STP bridge

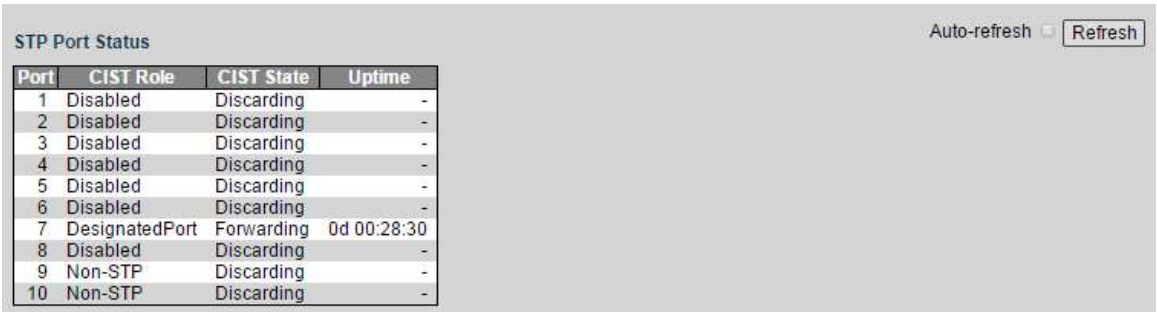


4.2.6.2 Port Status

You can view the STP port status.

Select **Advanced > Monitor > Spanning Tree > Port Status**. The STP Port Status interface is displayed. See Figure 4-113.

Figure 4-113 STP port status

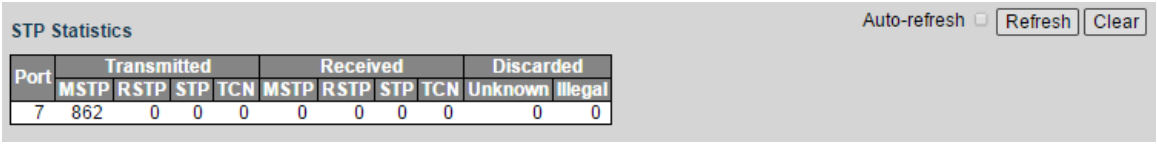


4.2.6.3 Port Statistics

You can view the STP port statistic.

Select **Advanced > Monitor > Spanning Tree > Port Statistics**. The STP Statistics interface is displayed. See Figure 4-114.

Figure 4-114 STP statistics



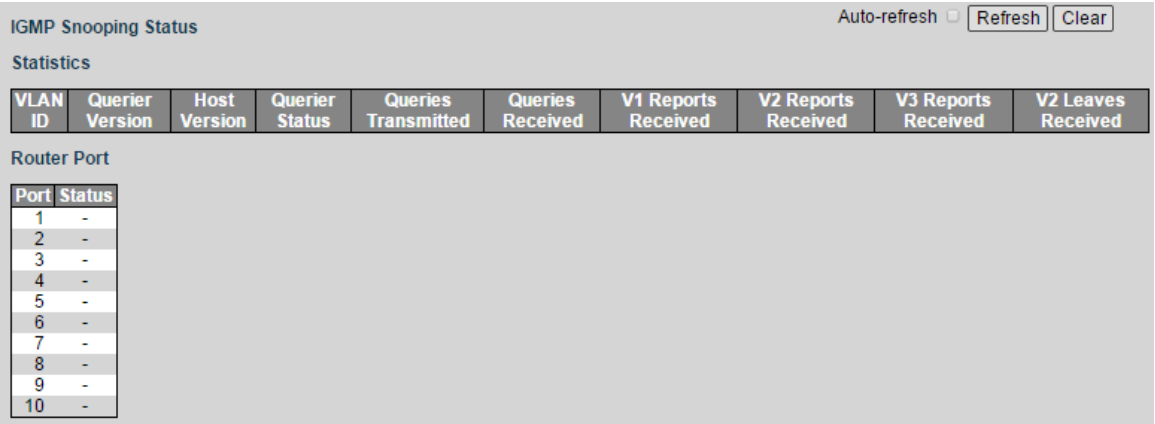
4.2.7 IGMP Snooping

4.2.7.1 Status

You can view the IGMP Snooping status.

Select **Advanced > Monitor > IGMP Snooping > Status**. The IGMP Snooping Status interface is displayed. See Figure 4-115.

Figure 4-115 IGMP Snooping status

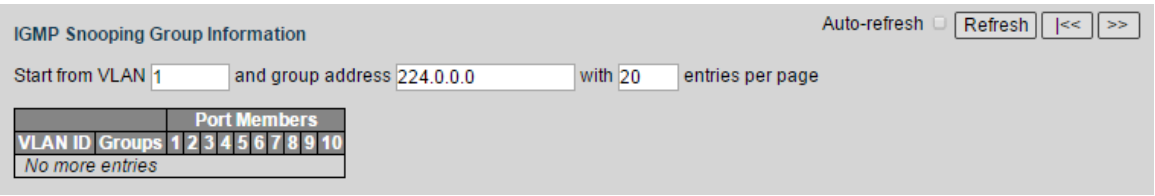


4.2.7.2 Groups Information

You can view the IGMP Snooping group information.

Select **Advanced > Monitor > IGMP Snooping > Groups Information**. The IGMP Snooping Group Information interface is displayed. See Figure 4-116.

Figure 4-116 IGMP Snooping group information

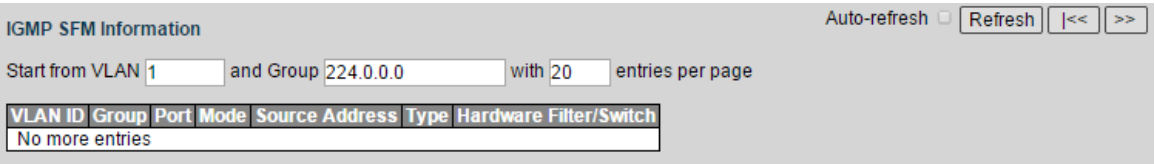


4.2.7.3 IPv4 SFM Information

You can view the IGMP SFM information.

Select **Advanced > Monitor > IGMP Snooping > IPv4 SFM Information**. The IPv4 SFM Information interface is displayed. See Figure 4-117.

Figure 4-117 IPv4 SFM Information



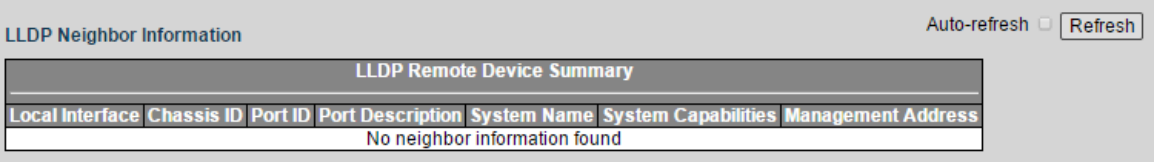
4.2.8 LLDP

4.2.8.1 Neighbors

You can view the LLDP neighbor information.

Select **Advanced > Monitor > LLDP > Neighbors**. The LLDP Neighbor Information interface is displayed. See Figure 4-118.

Figure 4-118 LLDP neighbor information



4.2.8.2 LLDP-MED Neighbors

You can view the LLDP-MED neighbor information.

Select **Advanced > Monitor > LLDP > LLDP-MED Neighbors**. The LLDP-MED Neighbor Information interface is displayed. See Figure 4-119.

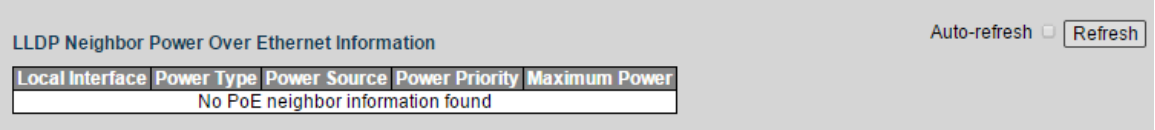
Figure 4-119 LLDP-MED neighbor information

4.2.8.3 PoE

You can view the PoE LLDP neighbor information.

Select **Advanced > Monitor > LLDP > PoE**. The LLDP Neighbor Power Over Ethernet Information interface is displayed. See Figure 4-120.

Figure 4-120 PoE LLDP neighbor information.

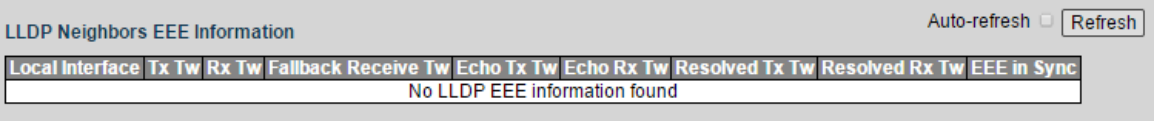


4.2.8.4 EEE

You can view the LLDP neighbors EEE information.

Select **Advanced > Monitor > LLDP > EEE**. The LLDP Neighbors EEE Information interface is displayed. See Figure 4-121.

Figure 4-121 LLDP neighbors EEE information

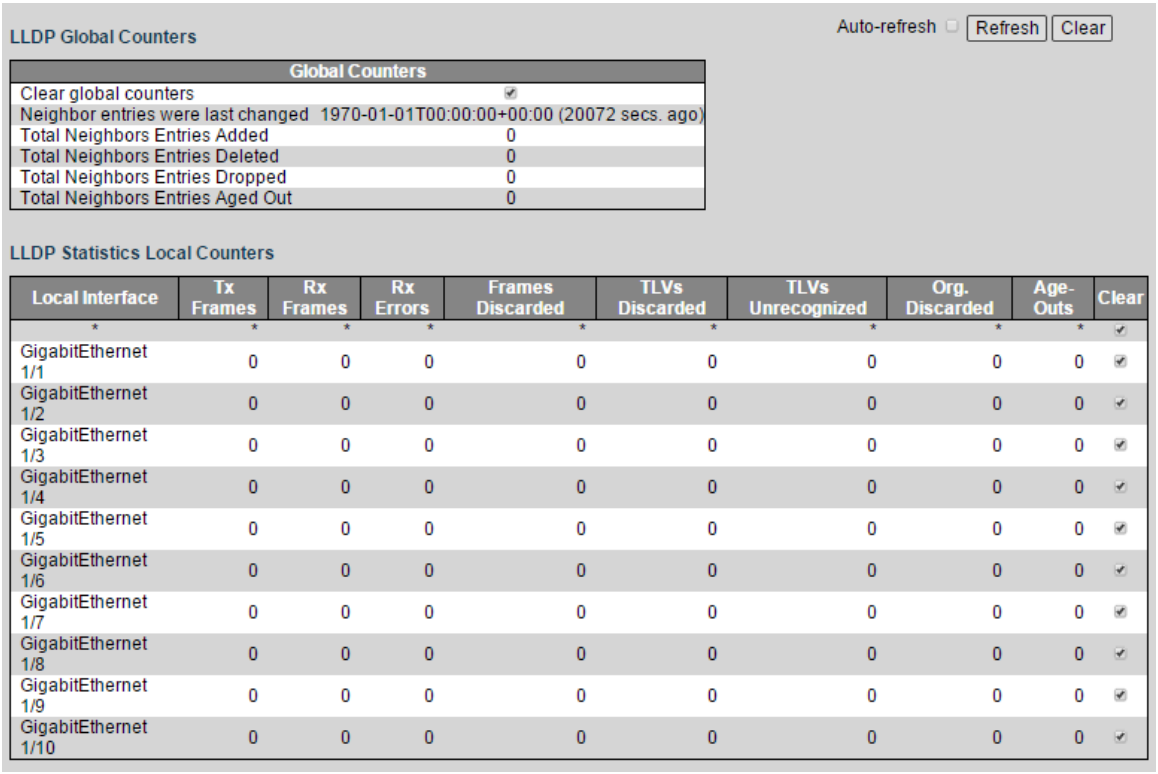


4.2.8.5 Port Statistics

You can view the LLDP port statistics information.

Select **Advanced > Monitor > LLDP > Port Statistics**. The LLDP Global Counters interface is displayed. See Figure 4-122.

Figure 4-122 LLDP global counters

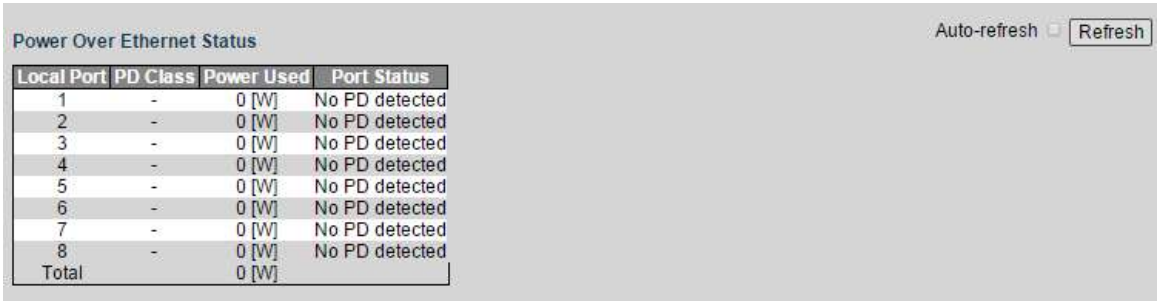


4.2.9 PoE

You can view the port PoE status.

Select **Advanced > Monitor > PoE**. The Power Over Ethernet Status interface is displayed. See Figure 4-123.

Figure 4-123 PoE status

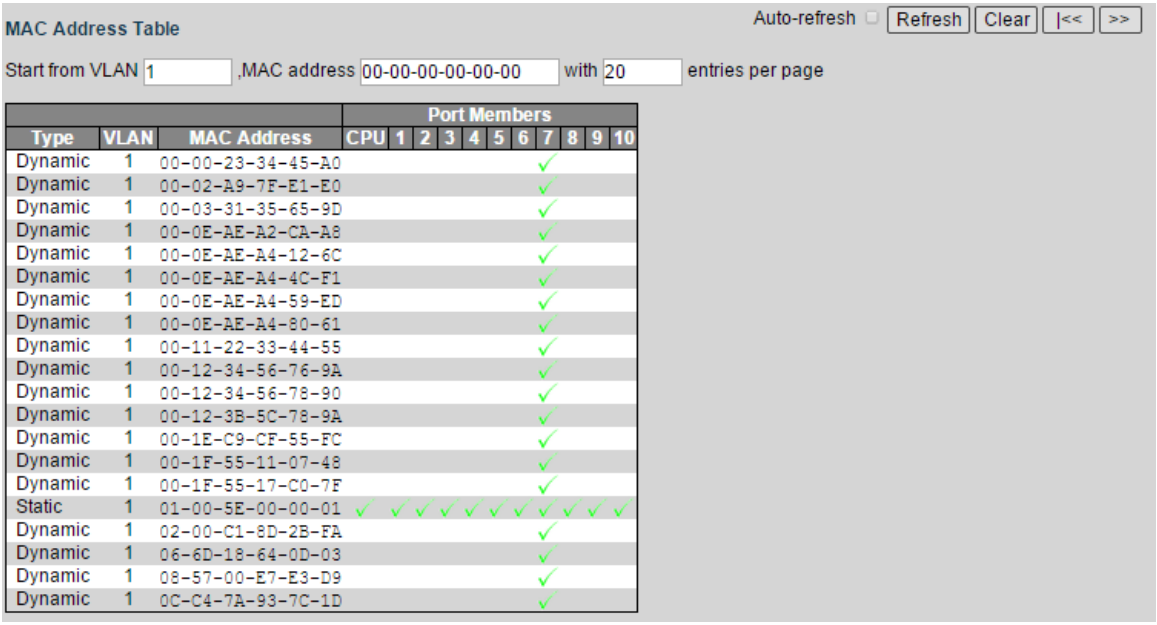


4.2.10 MAC Table

You can view the MAC table of the switch.

Select **Advanced > Monitor > MAC Table**. The MAC Address Table interface is displayed. See Figure 4-124.

Figure 4-124 MAC address table



4.2.11 VLANs

4.2.11.1 Membership

You can view the VLAN the port belongs to.

Select **Advanced > Monitor > VLANs > Membership**. The VLAN Membership Status interface is displayed. See Figure 4-125.

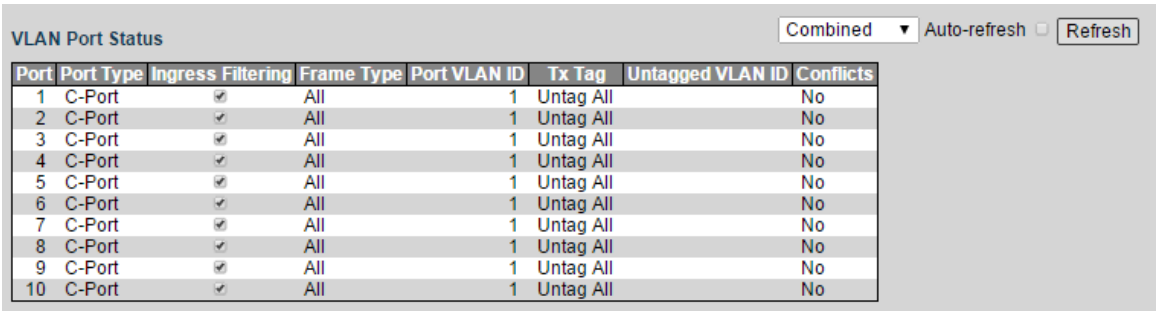
Figure 4-125 VLAN membership status

4.2.11.2 Ports

You can view the VLAN port status, including port type, ingress filtering, frame type, and so on.

Select **Advanced > Monitor > VLANs > Ports**. The VLAN Port Status interface is displayed. See Figure 4-126.

Figure 4-126 VLAN port status



4.3 Diagnostics

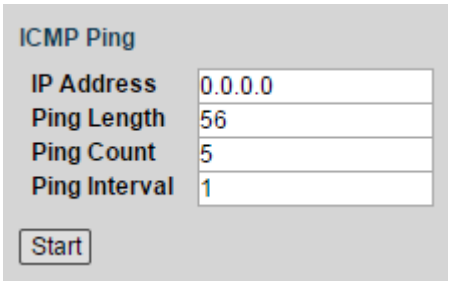
With Ping protocol, you can check whether the device with a specificed IP address can be accessed, or you can check whether there is a network connection failure.

4.3.1 Ping

Step 1 Select **Advanced > Diagnostics > Ping**.

The ICMP Ping interface is displayed. See Figure 4-127.

Figure 4-127 ICMP Ping



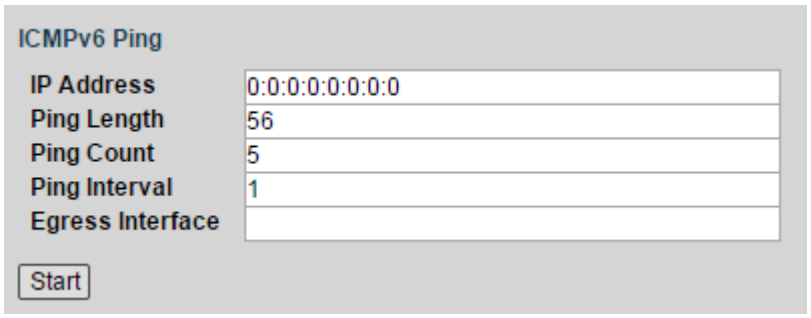
Step 2 Input the IP address, and click **Start**.

4.3.2 Ping6

Step 1 Select **Advanced > Diagnostics > Ping6**.

The ICMPv6 Ping interface is displayed. See Figure 4-128.

Figure 4-128 ICMPv6 Ping



Step 2 Input the IPv6 address, and click **Start**.

4.4 Maintenance

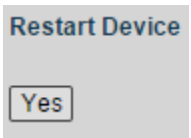
4.4.1 Restart Device

You can reboot the device.

Step 1 Select **Advanced > Maintenance > Restart Device**.

The Restart Device interface is displayed. See Figure 4-129.

Figure 4-129 Restart device



Step 2 Click **Yes**, and the device reboots.

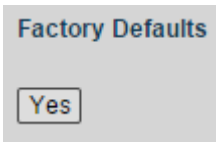
4.4.2 Factory Defaults

You can restore all the switch configuration to the factory defaults, except the VLAN IP address of the switch.

Step 1 Select **Advanced > Maintenance > Factory Defaults**.

The Factory Defaults interface is displayed. See Figure 4-130.

Figure 4-130 Factory defaults



Step 2 Click **Yes**, and all the configuration except VLAN IP address of the switch is restored to factory defaults.

4.4.3 Software

4.4.3.1 Upload

You can upgrade the software of the switch.

Step 1 Select **Advanced > Maintenance > Software > Upload**.

The Software Upload interface is displayed. See Figure 4-131.

Figure 4-131 Software upload

Step 2 Click **Browse**, and select the file in .mif format to upload.

Step 3 Click **Upload**.

Please wait for software upgrade, and the device reboots after upgrade finished. Re login the switch, and all the configuration will not change.

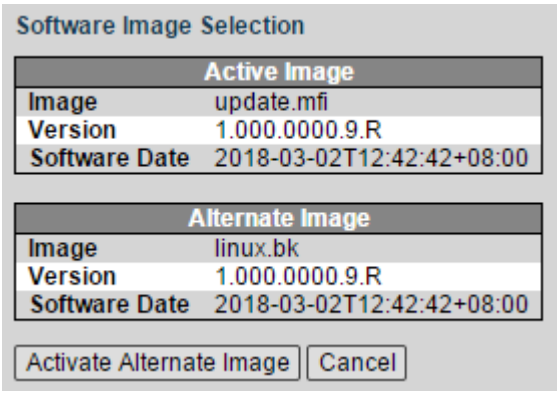
4.4.3.2 Image Select

You can activate the alternate image.

Step 1 Select **Advanced > Maintenance > Software > Image Select**.

The Software Image Selection interface is displayed. See Figure 4-132.

Figure 4-132 Software image selection



Step 2 Click **Activate Alternate Image**.

The device reboots. After reboot, the Alternate Image changes to be the Active Image, and the Active Image changes to be the Alternate Image.

4.4.4 Configuration

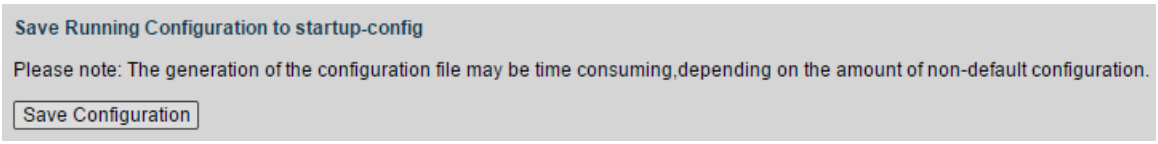
4.4.4.1 Save startup-config

You can save all the current configuration of the switch.

Step 1 Select **Advanced > Maintenance > Configuration> Save startup-config**.

The Save Running Configuration to startup-config interface is displayed. See Figure 4-133.

Figure 4-133 Save running configuration to startup-config



Step 2 Click **Save Configuration**.

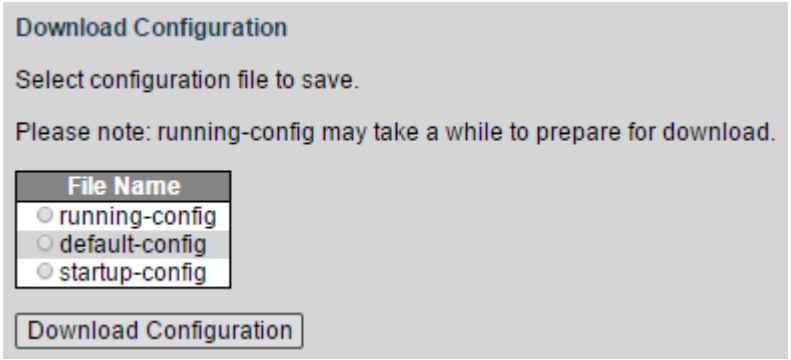
4.4.4.2 Download

You can download the configuration file.

Step 1 Select **Advanced > Maintenance > Configuration> Download**.

The Download Configuration interface is displayed. See Figure 4-134.

Figure 4-134 Download configuration



Step 2 Select the configuration file to download. There are three types:

- running-config: currently running configuration file. It is valid at the moment and will be lost if power off.
- default-config: the default configuration.
- startup-config: the configuration running when the switch starts up. It can be saved when power off.

Step 3 Click **Download Configuration**.

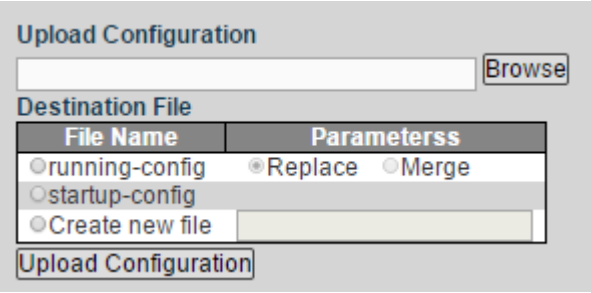
4.4.4.3 Upload

You can upload the configuration file.

Step 1 Select **Advanced > Maintenance > Configuration > Upload**.

The Upload Configuration interface is displayed. See Figure 4-135 .

Figure 4-135 Upload configuration



Step 2 Click **Broswe**, and select the configuration file to upload.

Step 3 Select the File Name and the Parameters in Destination File.

- running-config
- sartup-config
- Create new file

Step 4 Click **Upload Configuration**.

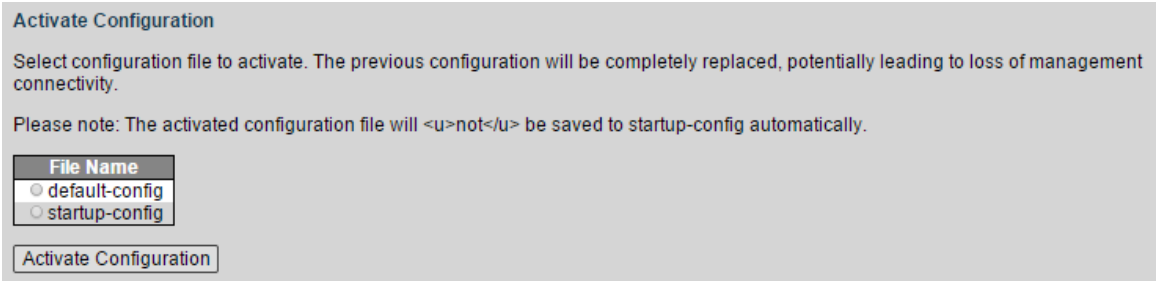
4.4.4.4 Activate

You can activate the configuration file.

Step 1 Select **Advanced > Maintenance > Configuration > Activate**.

The Activate Configuration interface is displayed. See Figure 4-136.

Figure 4-136 Activate configuration



Step 2 Select the **File Name**, default-config and startup-config are selectable.

Step 3 Click **Activate Configuration**.

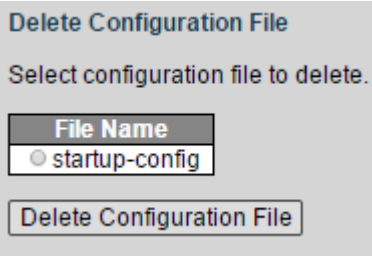
4.4.4.5 Delete

You can delete the configuration file.

Step 1 Select **Advanced > Maintenance > Configuration > Delete**.

The Delete Configuration File interface is displayed. See Figure 4-137.

Figure 4-137 Delete configuration file



Step 2 Select the File Name. Only **startup-config** can be selected currently.

Step 3 Click **Delete Configuration File**.

ZHEJIANG DAHUA VISION TECHNOLOGY CO., LTD.
Address: No.1199, Bin'an Road, Binjiang District, Hangzhou, P.R. China
Postcode: 310053
Tel: +86-571-87688883
Fax: +86-571-87688815
Email: overseas@dahuatech.com
Website: www.dahuasecurity.com