L2+ Managed Switch

Web Configuration Manual

(Applicable to DH-PFS5924-24X and DH-PFS5424-24T)

Document No.: 20150422-L2+ Manage Switch_V 4.2.2

Contents

Packing List

Open the packaging box of the switch carefully and verify that the following items are available in the packaging box:

- A managed switch
- An AC power cord
- A DB9-RJ45 serial port cable
- A user manual CD
- A warranty card and a certificate of quality
- Installation components and other accessories

If any item is damaged or any accessory is missing, contact the local dealer in time.

1 Configuration Preparations

1.1 Accessing the Switch Through a Web Browser

To access the switch through a web browser, ensure that the browser you use meet the following requirements:

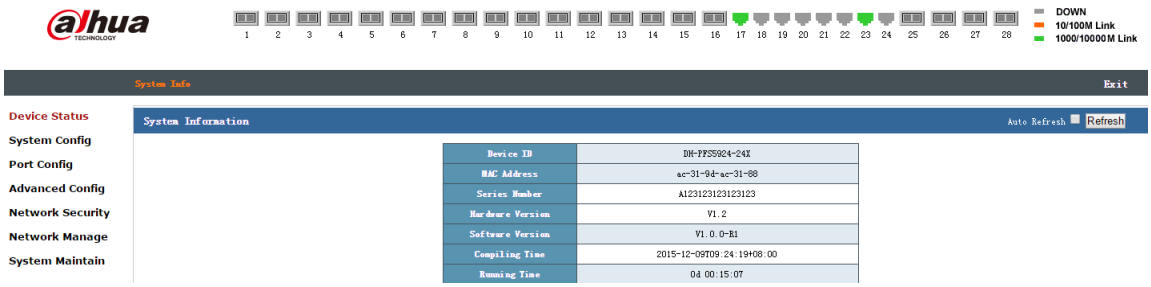
- HTML 7.0
- HTTP 1.1
- JavaScript™ 1.5

In addition, ensure that the main program file running on the switch supports the web-based access to the switch, and your computer has been connected to the network where the switch is located. If it is the first time you use the switch, you can use a browser to access the web interface of the switch as follows without configuring the switch:

1. Change the IP address of the network adapter on your computer to **192.168.1.2** and the subnet mask to **255.255.255.0**.
2. Open your web browser, and enter **192.168.1.110** in the address bar.

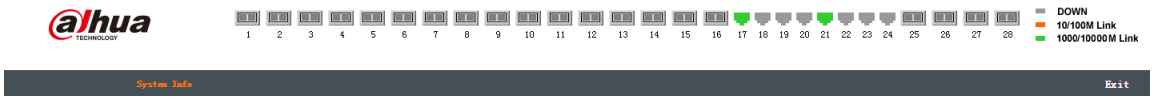
   Note that **192.168.1.110** is the default management address of the switch.
3. Enter the user name and password in the login authentication dialog box. Both the initial user name and password are **admin**, which are case-sensitive.
4. If authentication succeeds, the system information page of the switch is displayed.

1.2 Web Page Introduction



The entire page is divided into the top display area, navigation bar, and configuration area.

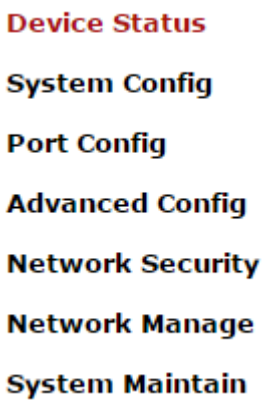
1.2.1 Top Display Area



In the top display area, you can check the link status of each port. A port is displayed in green if the negotiated rate of the port is 1000/10000M, and a port is displayed in orange if the negotiated rate of the port is 10/100M.

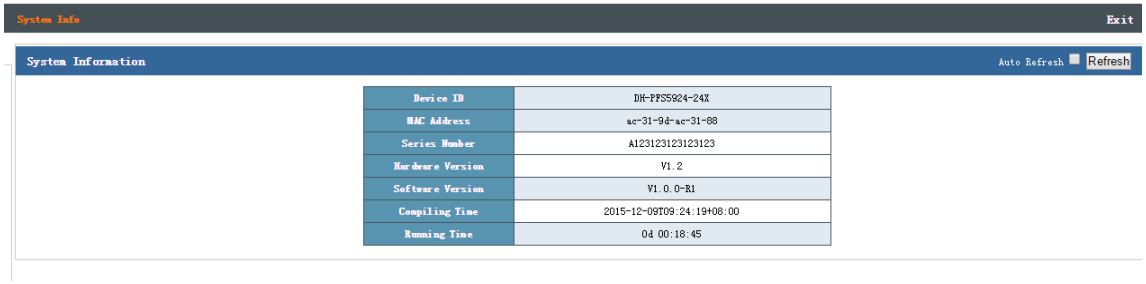
You can click the **Exit** button on the right to log out of the switch.

1.2.2 Navigation Bar



In the navigation bar, you can select the content to be displayed in the configuration area. Content in the navigation bar is listed and grouped by category. To perform a certain configuration, click the group name of the configuration to expand the configuration items, and then select the related configuration item. For example, to view the traffic of the current port, click **Device Status**, and then click **Port Statistics**.

1.2.3 Configuration Display Area



In the configuration display area, the device status information and configuration are displayed. You can select an item in the navigation bar to change the content displayed in this area.

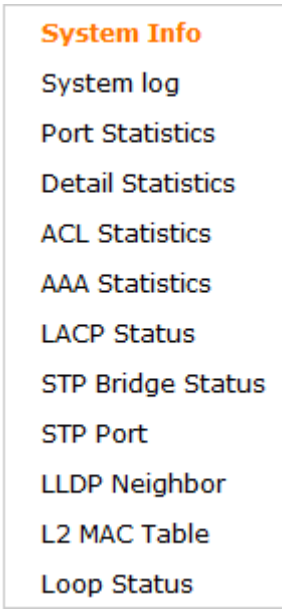
1.2.4 Configuration Area

In the configuration area, the content selected in the navigation bar is display. You can perform configuration operations in this area, for example, viewing and modifying a configuration.

The following chapters describe the seven configuration modules of the system, including **Device Status**, **System Config**, **Port Config**, **Advanced Config**, **Network Security**, **Network Manage**, and **System Maintain**.

2 Device Status

Click **Device Status** in the navigation bar, and then the following items are listed:

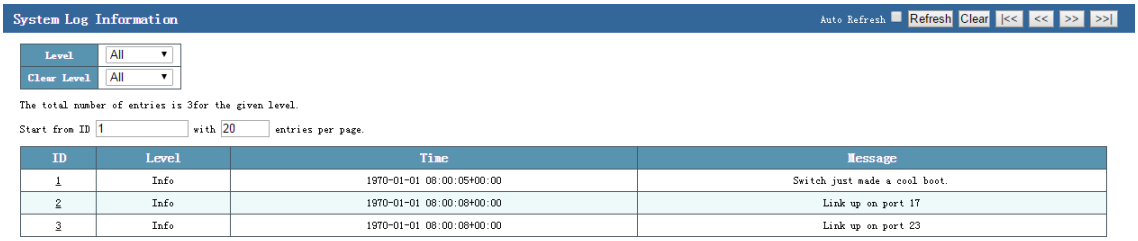


2.1 System Info

Device ID	DH-PFS5924-24X
MAC Address	ac-31-9d-ac-31-88
Series Number	A123123123123123
Hardware Version	V1.2
Software Version	V1.0.0-R1
Compiling Time	2015-12-09T09:24:19+08:00
Running Time	0d 00:21:23

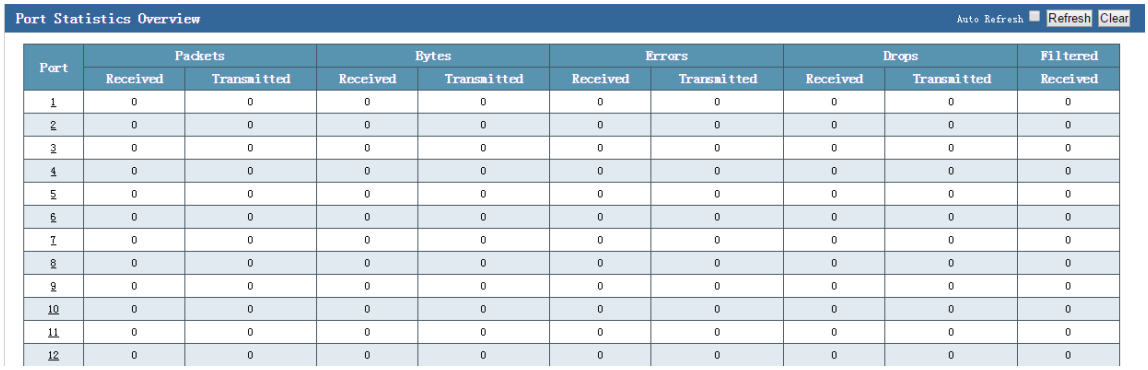
The figure shows the system information page of the switch. On this page, you can query the device model, hardware version, Media Access Control (MAC) address, serial number, software version, compiling time, and running time.

2.2 System Log



The figure shows the system log page of the switch. On this page, you can view system logs recorded when the device is running. These logs help the maintenance personnel with troubleshooting.

2.3 Port Statistics

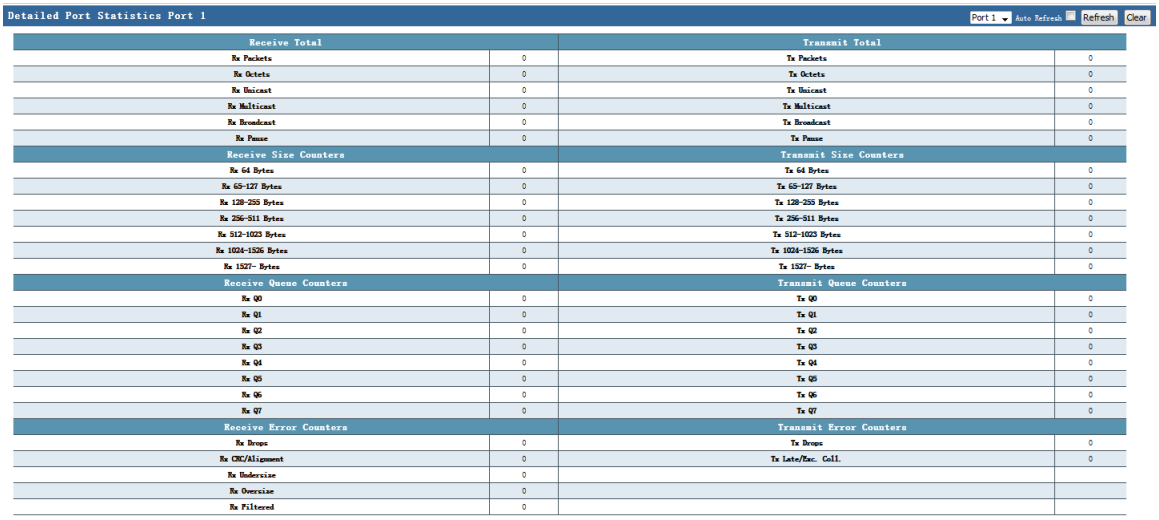


The figure shows the port statistics page of the switch. On this page, you can view the number of packets received or sent on each port, bytes received or sent on each port, and number of error packets received or sent on each port. When the number of error packets sent or received on a port is very large, the working condition of this port is poor. In this case, check whether the network cable is properly connected to this port and check whether the peer device is faulty.

You can select **Auto Refresh** to refresh the data in real time, click **Refresh** to view the latest data, or click **Clear** to clear the statistical data.

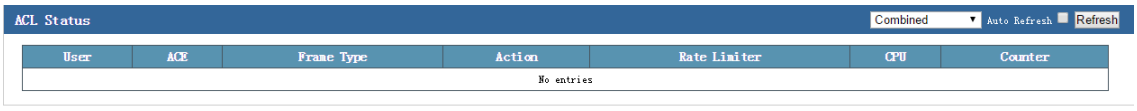
An error packet refers to a packet that encounters the cyclic redundancy check (CRC) error. A dropped packet refers to a packet that is dropped in any of the following cases: (1) The packet rate is too high and the buffer of the switch is insufficient; (2) The port forwarding capability is insufficient; (3) The packet fails to meet certain access control list (ACL) rules.

2.4 Detailed Statistics



The figure shows the detailed statistics page of all the ports on the switch. On this page, you can query the working conditions of each port, including the number of sent/received packets, number of broadcast packets, and number of error packets (including dropped packets, packets with CRC errors, packets with very small frames, packets with jumbo frames, and packets that are filtered out). The information facilitates network maintenance of the network management personnel. You can select a port from the port drop-down list box to view the traffic information of the specified port. In addition, you can select **Auto Refresh** to refresh the data in real time, click **Refresh** to view the latest data, or click **Clear** to clear the statistical data of the port.

2.5 ACL Statistics

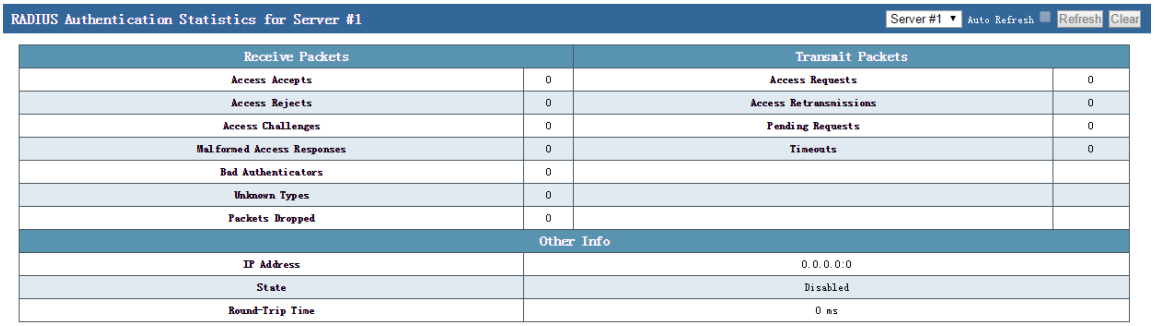


The figure shows the ACL statistics page of the switch. On this page, you can select **combined**, **static**, **ipmc**, or **dhcp** from the drop-down list box to view various types of network security information. You can select **Auto Refresh** to refresh the data in real time, or click **Refresh** to view the latest data.

- User: Indicates the user name and specifies whether the record is DHCP or static information.
- ACE: Indicates the name of an access control entry (ACE).
- Frame Type: Indicates the type of the data frame.

- Action: Indicates the packet processing behavior, which can be **Permit** or **Deny**.
- CPU: Indicates whether to upload this type of packets to the CPU.
- Counter: Indicates the matching times, that is, that number of packets that match the rule.

2.6 AAA Statistics

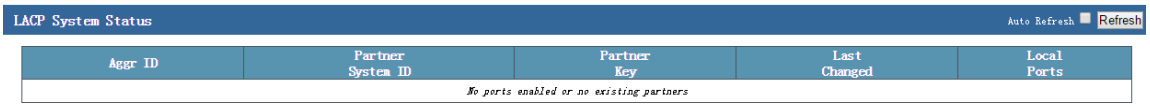


Receive Packets		Transmit Packets	
Access Accepts	0	Access Requests	0
Access Rejects	0	Access Retransmissions	0
Access Challenges	0	Pending Requests	0
Malformed Access Responses	0	Timeouts	0
Bad Authenticators	0		
Unknown Types	0		
Packets Dropped	0		
Other Info			
IP Address	0.0.0.0:0		
State	Disabled		
Round-Trip Time	0 ms		

The figure shows the AAA statistics page of the switch. If the remote RADIUS server has been configured on the network, you can view the related authentication packet statistics on this page.

- Access requests: Authentication request packets sent from the client to the RADIUS server based on the user name and password
- Access accepts: Authentication accepted packets sent from the RADIUS server to the client
- Access rejects: Authentication rejected packets sent from the RADIUS server to the client
- Access retransmissions: Authentication request re-sent from the RADIUS server to the client
- Access challenges: Challenges sent from the RADIUS server to the client to query the user information or authentication negotiation mode.
- Pending requests: Pending requests sent from the client
- Malformed access responses: Client authentication failure messages
- Timeouts: Number of client authentication timeouts
- Bad authenticators: Incorrect client authentication password
- Unknown types: Authentication types that cannot be recognized by the RADIUS server
- Packets dropped: Number of packets dropped by the RADIUS server

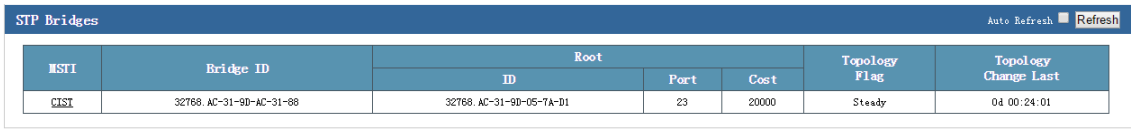
2.7 LCAP Status



The figure shows the LCAP status page of the switch. On this page, you can view the running status of LACP on the port, aggregation group ID, local port number, peer member ID, and communication key.

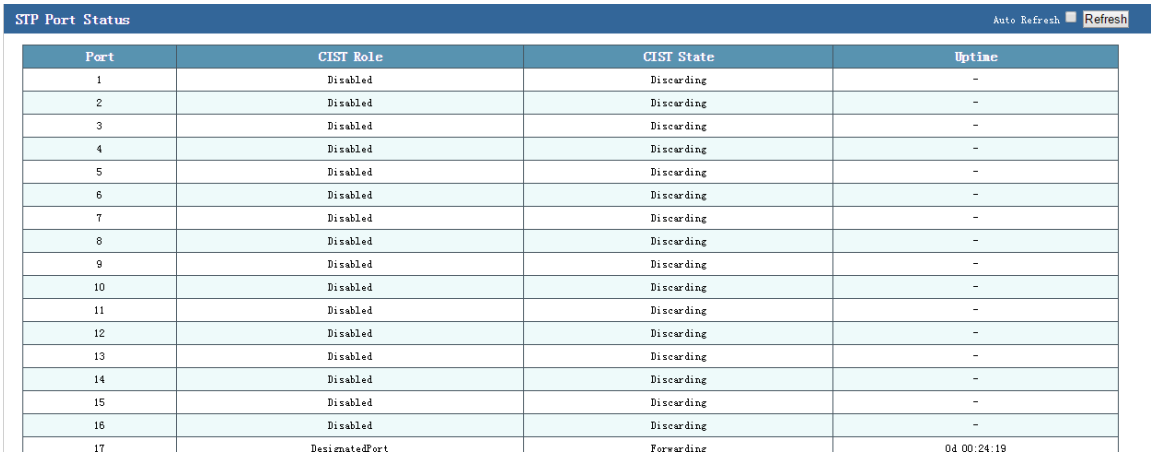
- Aggr ID: Indicates the configured aggregation group ID.
- Partner System ID: Indicates the aggregation group member ID of the peer device.
- Partner Key: Indicates the aggregation member key of the peer device.
- Last Changed: Indicates the last time that the aggregation group is updated.
- Local Ports: Indicates the port number of the device that is added to the aggregation group.

2.8 STP Bridge Status



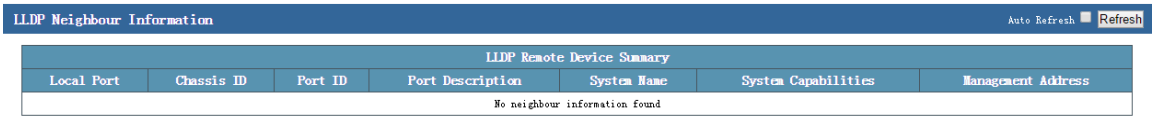
The figure shows the Spanning Tree Protocol (STP) bridge status page of the switch. On this page, you can view the bridge ID, root bridge ID, and port path cost.

2.9 STP Port



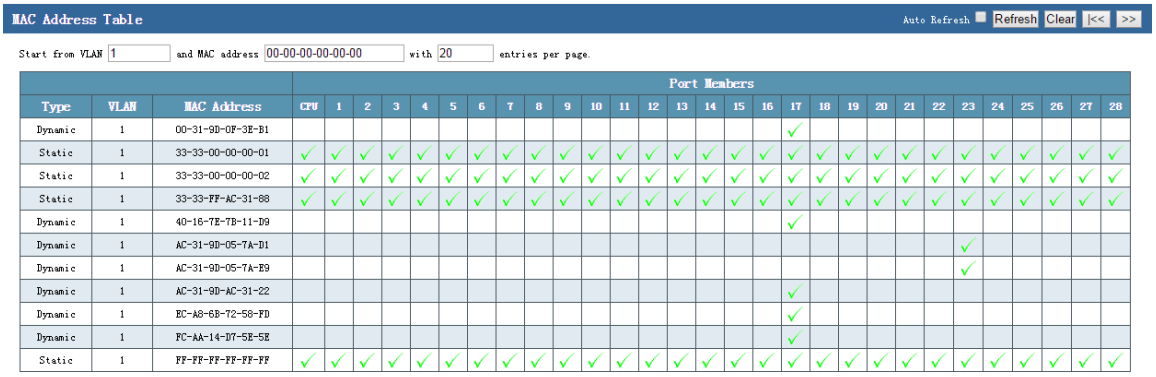
The figure shows the STP port status page of the switch. On this page, you can view the status of each STP port, including the STP role, port status, and update time.

2.10 LLDP Neighbor



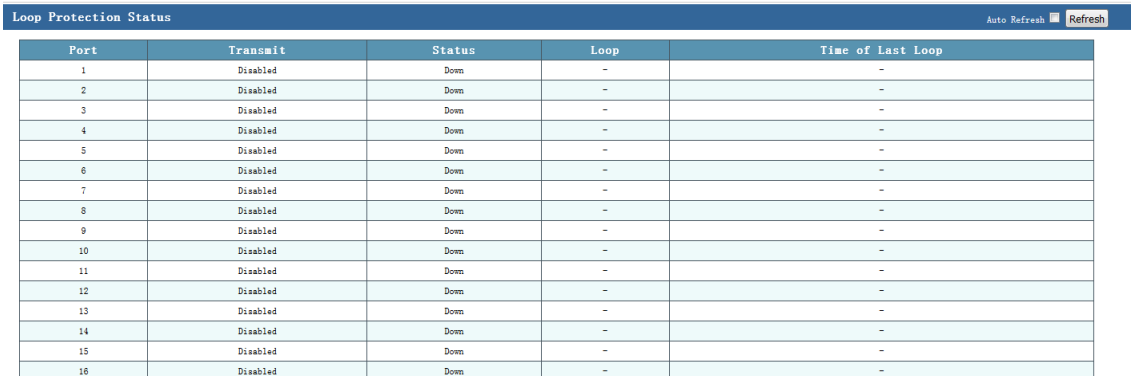
The figure shows the LLDP neighbor information page of the switch. After the Link Layer Discovery Protocol (LLDP) is enabled on the device, you can view the LLDP neighbor information on this page, including the peer port, system name, port description, system performance, and management address.

2.11 L2 MAC Table



The figure shows the L2 forwarding table information page of the switch. On this page, you can view all the L2 MAC address forwarding tables of the switch. The table entries include the type, port, MAC address, and VLAN.

2.12 Loop Protection Status



The figure shows the loop protection status information page of the switch. On this page, you can view information about the loop protection status, including the enabling/disabling status of the transmit mode of the port, current port status, port congestion status, and time of last congestion on the port.

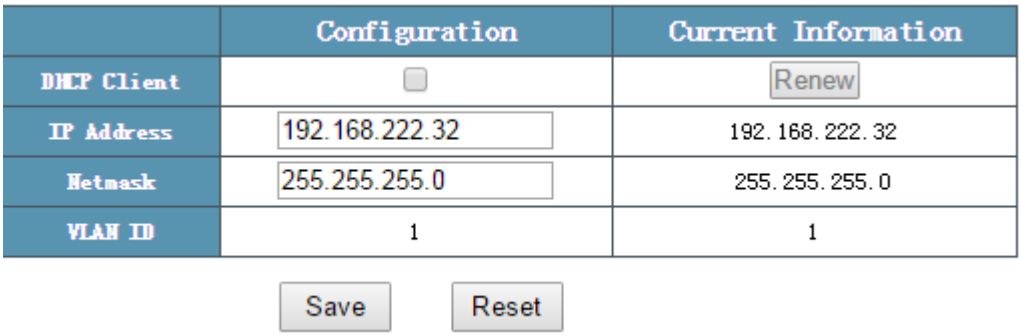
- Transmit: Indicates the transmit (Tx) mode of a port.
- Status: Indicates the current status of a port.
- Loop: Indicates the port congestion status.
- Time of Last Loop: Indicates the last time that the port is congested.

3 System Config

Click **System Config** in the navigation bar, and then the following items are listed:

3.1 IP Config

On the IP configuration page, you can configure the management IP address of the switch. The management VLAN of the switch is VLAN 1 by default, and cannot be modified.



As shown in the figure, you can view the IP address, subnet mask, and management VLAN of the device. The default IP address of the switch is 192.168.255.1, which can be modified on this page.

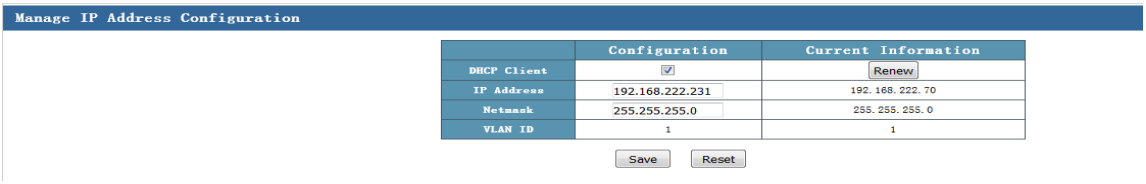
- **DHCP Client**: If this option is selected, the management IP address of the switch is assigned by the DHCP server on the network.
- **IP Address**: Indicates the management IP address of the switch, which can be modified.
- **Netmask**: Indicates the subnet mask of the switch, which can be modified.
- **VLAN ID**: The management VLAN of the switch is VLAN 1 by default, and cannot be modified.

Note: Do not change the subnet mask of the switch unless necessary. If the subnet mask is improperly modified, you may fail to log in to the switch.

Configuration example:

Configure a switch as the DHCP client and automatically obtain the management IP address of the switch.

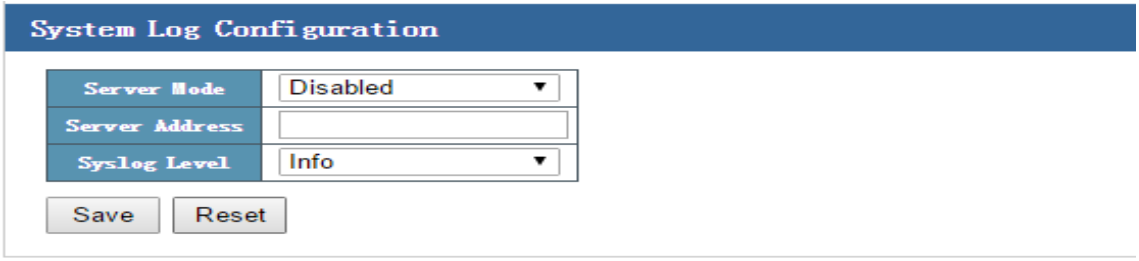
Select **DHCP Client**, as shown in the following figure.



Use a serial port to access the command line mode of the switch and check the IP address obtained by the switch. On the login interface, you can view the IP address obtained by the switch, which is the same as that shown in the preceding figure.

3.2 Log Config

You can perform log configuration to upload logs on the switch to a remote log server.



As shown in the figure, you can configure information about the remote log server on the log configuration page. In this way, logs of the device can be stored as backup on the remote server, and you can view the logs later.

- **Server Mode**: It is a global switch. **Enabled** indicates that the function of uploading logs to the remote server is enabled; and **Disabled** indicates that the function is disabled.
- **Server Address**: Indicates the IP address of the remote log server.
- **Syslog Level**: Indicates the level of the log. The syslog levels include **info**, **warning**, and **error**. **info** is the lowest level, and **error** is the highest level.

Level	Description
Info	Common logs that describe common operations when the device is running normally. For example, a user runs the **display** command.

Level	Description
Warning	Logs that describe warning information for exceptions detected when the device runs abnormally. These exceptions may result in service failures and should be noted. For example, a user shuts down the routing process, or an error protocol packet is detected.
Error	Logs that describe errors, for example, incorrect operations or abnormal processes of the device. These errors do not affect subsequent services, but attention must be paid and the causes must be analyzed. For example, the user command is incorrect, the user password is incorrect, or error packets (obtained by other devices) are detected.

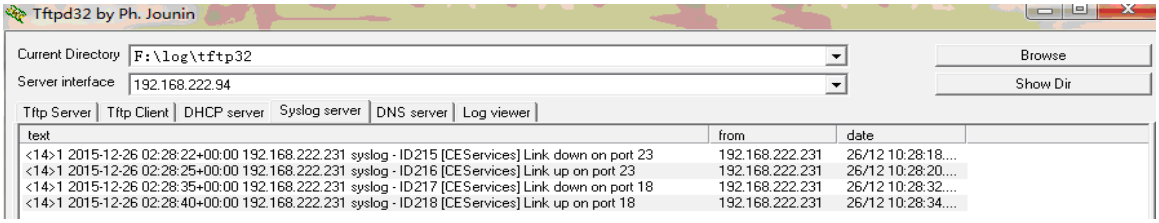
Tip: Currently, the switch displays only logs of the info level. This function will be improved later through software upgrade.

Configuration example:

Enable the server function, configure the IP address of the server, and set the log level to **info**. (A PC installed the TFTP32 software can be configured as a log server.)

Self-loop two ports, and connect and then disconnect a port. Then, log records are generated in the syslog. You can also see the log information in the TFTP32 software. The following two figures show the log information displayed on the device and in the TFTP32 software.

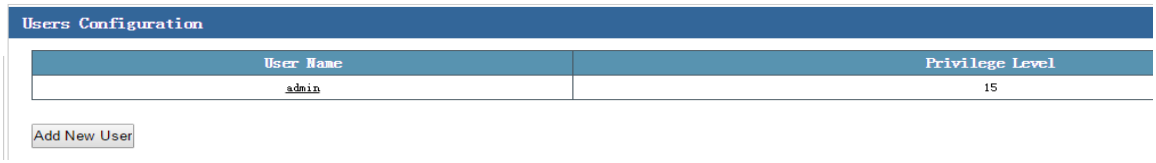
89	Info	1970-01-04T19:21:38+00:00	Link up on port 37
90	Info	1970-01-04T19:21:38+00:00	Link up on port 41
91	Info	1970-01-04T19:21:42+00:00	Link down on port 37
92	Info	1970-01-04T19:21:42+00:00	Link down on port 41



3.3 User Config

On the user configuration page, you can modify the user attributes of the web interface of the switch to protect the switch settings. Two user privilege levels are available.

On the user configuration page as shown in the following figure, you can click **admin** to modify the user name and password of an existing user, or click **Add New User** to add a new user.



- Adding a user

  Click **Add New User**. The following page is displayed:

- Modifying an existing user

  Click **admin**. The following page is displayed:

You can set the user name, password, and privilege level of a new user.

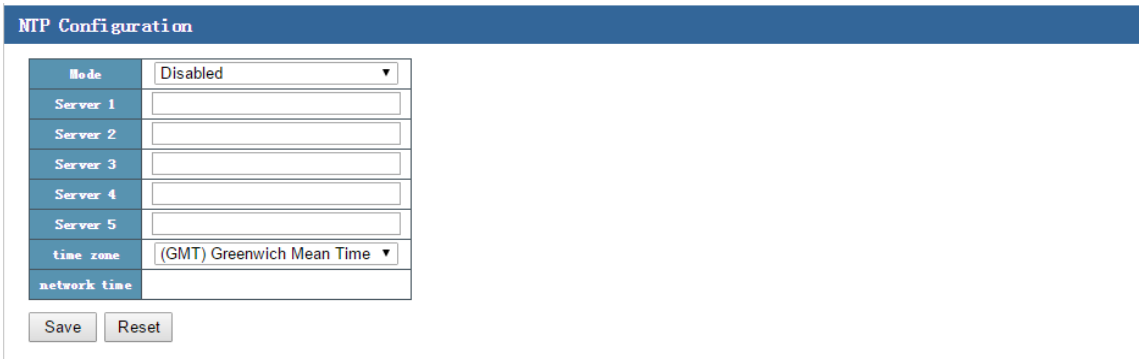
Two user privilege levels are available: **1** and **15**.

Level 1 allows you to view some simple information. Level 15 allows you to run all the commands. The default privilege level is **15**.

Tip: User **admin** is the administrator, and cannot be deleted by default. The default user name and password of the switch is **admin**. If the password is modified, keep the new password in mind; otherwise, you cannot log in to the device.

3.4 NTP Config

The Network Time Protocol (NTP) is defined in RFC1305 and used for time synchronization between the distributed time server and a client. NTP is transmitted through UDP packets, and the used UDP port number is 123.



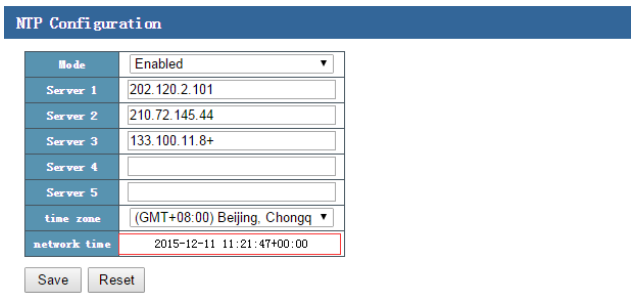
The figure shows the NTP configuration page. NTP is used to synchronize the time among all devices with clocks on the network so that the clocks of all the devices on the network are consistent and the devices can provide multiple applications based on the unified time.

Mode: It is a global switch. **Disabled** indicates that the NTP function is disabled, and **Enabled** indicates that the NTP function is enabled.

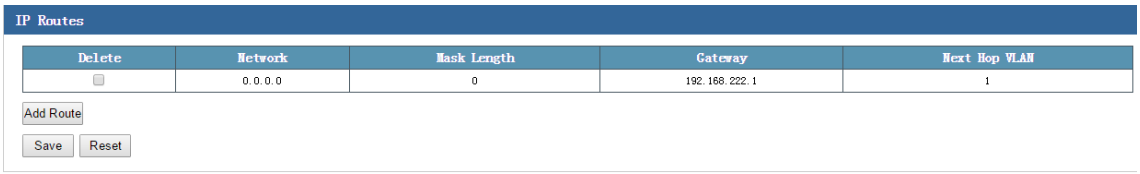
Server 1 to **Server 5**: Fill in the address of the NTP server. Note: You can configure a static route because there is no gateway.

Configuration example:

Enable the NTP function, fill in the IP addresses in **Server 1** and **Server 2**, set **time zone** to the Beijing time zone, and save the configuration, as shown in the following figure. Add a route on the route configuration page.

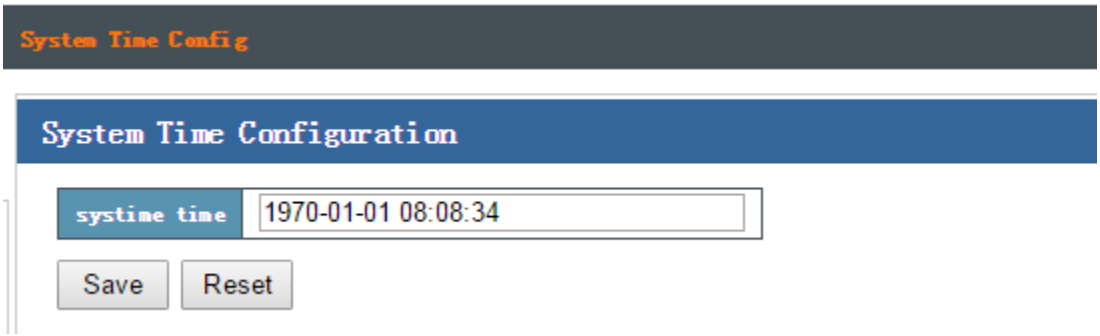


The following figure shows the route configured on the route configuration page.



3.5 System Time Config

On the system time configuration page, you can configure the system time after the device is started.



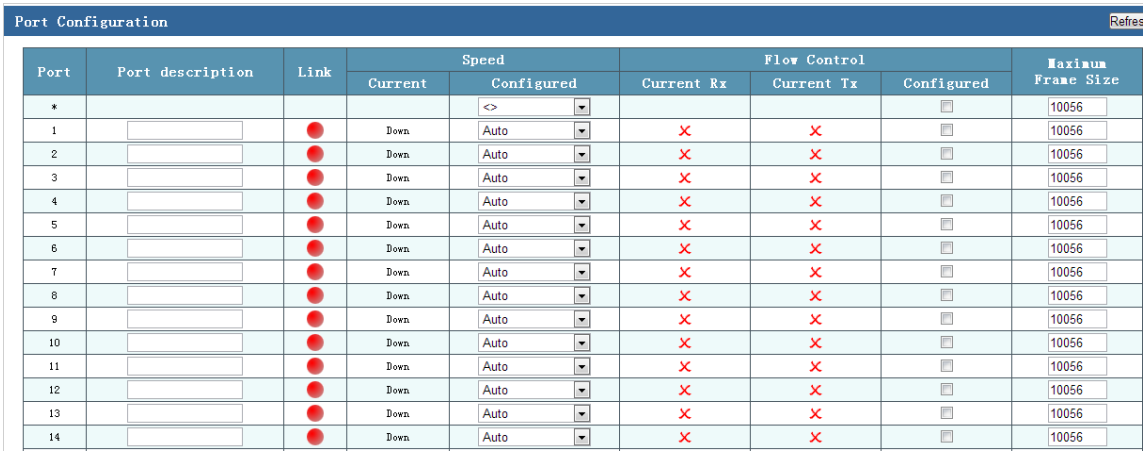
Note: The factory setting of the system time will be restored when the device is powered off. You need to re-configure the system time after the device is powered on again.

4 Port Config

Click **Port Config** in the navigation bar, and then the following items are listed:

4.1 Port Config

On the port configuration page, you can configure basic parameters related to each port of the switch. These basic parameters directly affect the working mode of each port, and must be configured according to the actual requirements.



On the port configuration page shown in the preceding figure, you can view the connection status, speed duplex mode, flow control status, and maximum frame length of each port, and configure the speed duplex mode, flow control function in the transmit (Tx) and receive (Rx) directions, and maximum frame length of each port.

- **Port**: Indicates the port number of the switch.
- **Link**: Indicates the connection status of a port.

Color	Description
Green	The link is in connected state.
Red	The link is in disconnected state.

- **Speed-Current**: Indicates the current speed of a port.

Current Speed	Speed Duplex Mode
10Gfdx	10G full duplex
1Gfdx	1G full duplex
100fdx	100M full duplex
100hdx	100M half duplex
10fdx	10M full duplex
10hdx	10M half duplex
Down	The port is not connected.

- **Speed-Configured**: Indicates the speed duplex mode of a port.

  Tip: Modifying the speed duplex mode of a port directly affects communication on the port. Therefore, be cautious when modifying the speed duplex mode.

Port Type	Speed Mode	Description
Electronic port	Auto (Default)	The speed duplex mode of the port is auto adaptation.
	Disabled	The port is disabled.
	10Mbps HDX	The speed duplex mode of the port is 10M half duplex.
	10Mbps FDX	The speed duplex mode of the port is 10M full duplex.
	100Mbps HDX	The speed duplex mode of the port is 100M half duplex.
	100Mbps FDX	The speed duplex mode of the port is 100M full duplex.

Port Type	Speed Mode	Description
	1Gbps FDX	The speed duplex mode of the port is 1Gbps full duplex.
Optical port	1000-X_AMS (Default)	The speed duplex mode of the optical port is 1000M auto adaptation. This ensures that negotiation can succeed when the speed duplex mode of the peer end is 1000-X_AMS.
	1000-X	The speed duplex mode of the optical port is forced 1000M full duplex. It can be adapted only to the forced 1000M mode of the optical port.
	Disabled	The optical port is disabled.
10 Gbps port	10Gbps FDX	The speed duplex mode of the port is 10 Gbps full duplex.
	Disabled	The 10 Gbps port is disabled.

- **Flow Control**: It indicates the port flow control function of the switch. This function is disabled by default.

  In the **Flow Control-Configured** column, if the check box is selected, the port flow control function is enabled; if the check box is not selected, the port flow control function is disabled. **Current Tx/Rx** indicates the flow control status in the Tx/Rx direction of the port. ✗ indicates that the port flow control function is disabled or flow control currently does not take effect; ✓ indicates that the port flow control function is currently effective and pause frames can be sent or received normally.

  Tip: Flow control can be enabled for an electronic port to synchronize the speeds at the Tx and Rx ends, thus preventing packet loss caused by inconsistent speeds.

- **Maximum Frame Size**: Indicates the maximum size of a frame transmitted on a port. The value ranges from 1,518 to 10,056 bytes. The default value is 10,056 bytes. This parameter is applicable to a port that is currently in use. The maximum frame size can also be considered as the jumbo frame size.

Note:

For an optical port, the differences between auto negotiation and forced 1000M are as follows:

1. The working mode is set to auto negotiation at both ends.

Both ends send the /C/ code streams to each other. If three same /C/ code streams are received consecutively and the received code streams match the working mode of the local end, the local end sends a /C/ code with the Ack message to the peer end. On receiving the Ack message, the peer end determines that two ends can communicate with each other, and therefore, set the port to the UP state.

2. The working mode is set to auto negotiation at one end and forced at the other end.

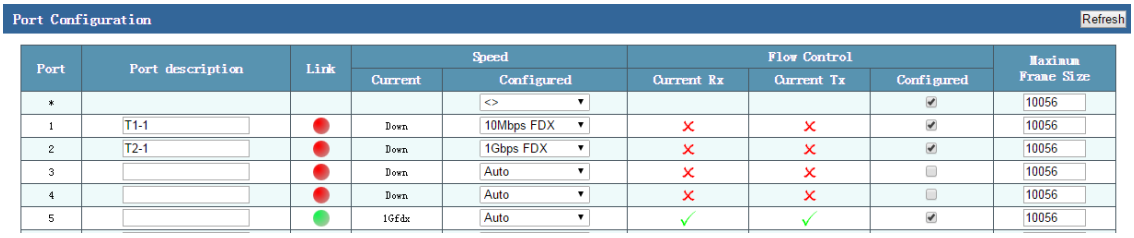
The auto negotiation end sends the /C/ code streams, and the forced end sends the /I/ code streams. The forced end cannot provide the peer end with the local end negotiation information, or return an Ack message to the peer end. Therefore, the port is set to the DOWN state at the auto negotiation end. The forced end itself can identify the /C/ codes, and determines that the peer end is the port that matches the local end. Therefore, the port is set to the UP state at the forced end.

3. The working mode is set to forced at both ends.

Both ends send the /I/ code streams to each other. After one end receives the /I/ code streams, it determines that the peer end is the port that matches the local end, and therefore the port is set to the UP state at the local end.

Configuration example:

Describe port 1 as T1-1 and port 2 as T2-1, set **Speed** to **100Mbps FDX** and **1Gbps FDX**, and enable flow control, as shown in the following figure.

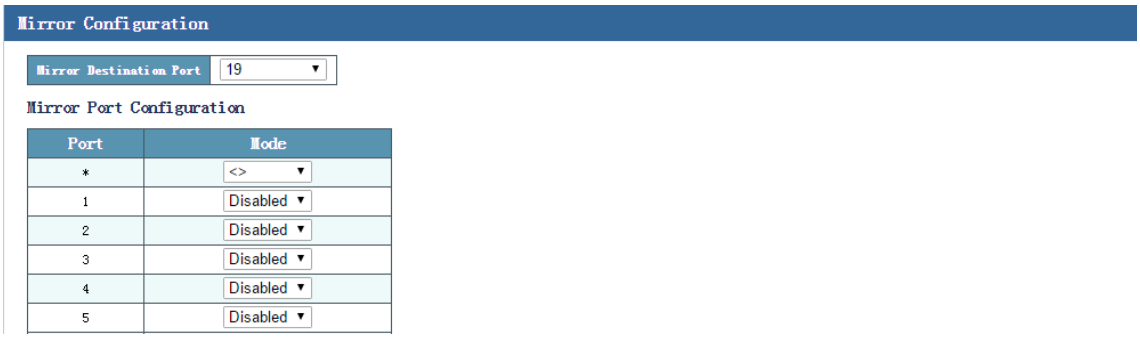


4.2 Port Mirror

Port mirroring is also called port monitoring. Port monitoring is a data packet acquisition technology. It can be configured on a switch to copy data packets from one or more ports (mirror source ports) to a specified port (mirror destination port). The destination port is connected to a host installed with the

packet analysis software. The software analyzes the collected packets to implement network monitoring and eliminating network faults.

On the port mirror page, you can configure port mirroring parameters, as shown in the following figure.



- Mirror Destination Port: Indicates the monitoring port. Only one monitoring port can be selected. By default, the mirror destination port is disabled.
- **Mirror Port Configuration–Port**: Indicates the monitored port. You can select one or more monitored ports.
- **Mirror Port Configuration–Mode**: Four modes are available, including **Disabled**, **Tx only**, **Rx only**, and **Enabled**.

Mode	Description
Disabled (Default)	The monitoring function is disabled.
Tx only	The Tx direction is monitored.
Rx only	The Rx direction is monitored.
Enabled	Both the Rx and Tx directions are monitored.

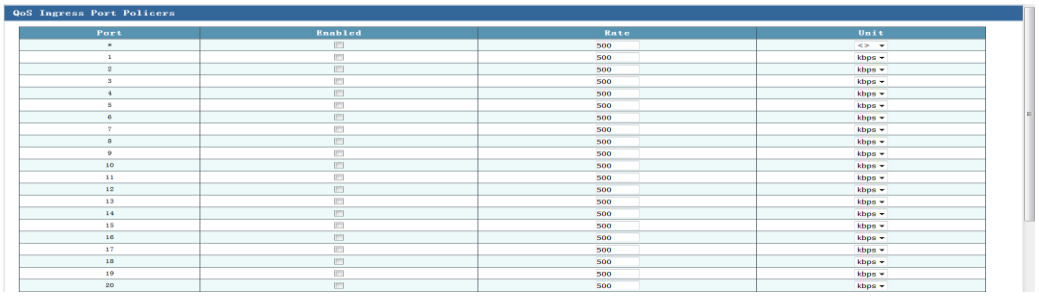
Configuration example:

Select port 1 as the destination port and port 2 and port 3 as the source ports, as shown in the following figure.

On port 1, you can use the packet capturing or monitoring software to view the data streams of port 2 and port 3.

4.3 Bandwidth Control

On the bandwidth control page, you can configure the rate limiting policy of a port to limit the rate at which packets are exchanged on a port.

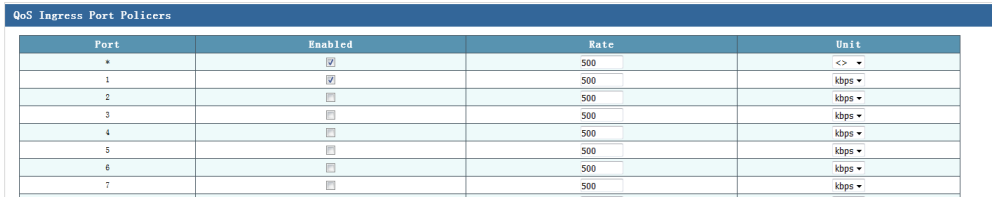


The rate limit parameters are as follows:

- **Port**: Lists the ports.
- **Enabled**: Select this check box to enable the rate limit function of a port. By default, this function is disabled.
- **Rate**: Indicates the rate limit of a port.
- **Unit:** Indicates the rate unit.

Configuration example:

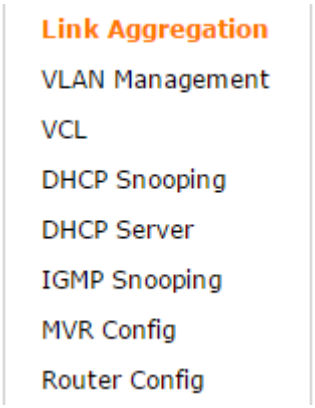
On the bandwidth control page, set the rate limit of port 1 to 500 kbps.



The result of the rate testing software indicates that the total exchange rate of port 1 is 500 kbps.

5 Advanced Config

The **Advanced Config** menu contains the following submenus: **Link Aggregation**, **VLAN Management**, **VCL**, **DHCP Snooping**, **DHCP Server**, **IGMP Snooping**, **MVR Config**, and **Router Config**.



5.1 Link Aggregation

In link aggregation, multiple physical ports of a switch are aggregated into one logical port. Multiple links in the same aggregation group can be treated as a logical link with higher bandwidth.

With link aggregation, communication traffic can be shared among member ports of an aggregation group to increase the bandwidth. In addition, member ports in the same aggregation group serve as dynamic backup for each other, which improves the link reliability.

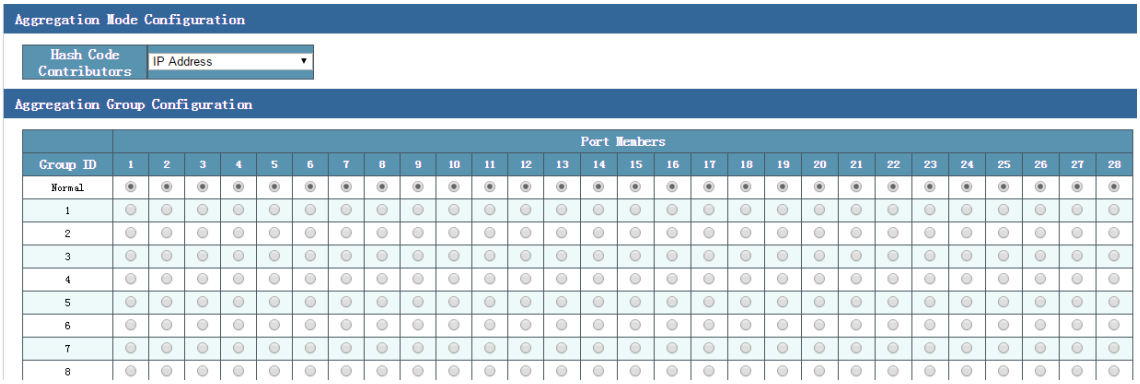
Member ports in the same aggregation group must have consistent configurations, which include the STP, QoS, VLAN, port attributes, MAC address learning, ERPS configuration, loop protection configuration, mirror, 802.1x, IP filtering, MAC filtering, and port isolation.

Tip: If a port is used for link aggregation, port parameters and other software functions should not be configured for this port.

Link aggregation is divided into static aggregation and dynamic aggregation (LACP). The peer device that participates in link aggregation of a switch is generally another switch or a network adapter.

5.1.1 Static Aggregation

Static aggregation must be manually configured. Ports in an aggregation group cannot be automatically added or deleted by the system. The logic of static aggregation configuration is simple and is easy to understand and use.



As shown in the preceding figure, the static aggregation configuration page consists of three parts, including the load balancing mode, aggregation group, and port member.

Tip: A horizontal scroll bar is available at the bottom of the page. You can move the scroll bar to view all the ports on the right of the list.

- **Load balancing mode**

  Port aggregation supports five load balancing modes, as described in the following table.

Load Balancing Mode	**Description**
IP Address (default mode)	Perform load balancing calculation based on the source and destination IP addresses of the packet.
Source MAC Address	Perform load balancing calculation based on the source MAC address of the packet.
Destination MAC Address	Perform load balancing calculation based on the destination MAC address of the packet.
SMAC&DMAC Address	Perform load balancing calculation based on the source and destination MAC addresses of the packet.
TCP/UDP Port Number	Perform load balancing calculation based on the TCP/UDP port number of the packet.

- **Aggregation group**

  An aggregation group is a group of Ethernet ports. The default number of aggregation groups supported by this series of switches is half of the actual number of ports. By default, all aggregation groups are created, and no port member is added.

- **Port member**

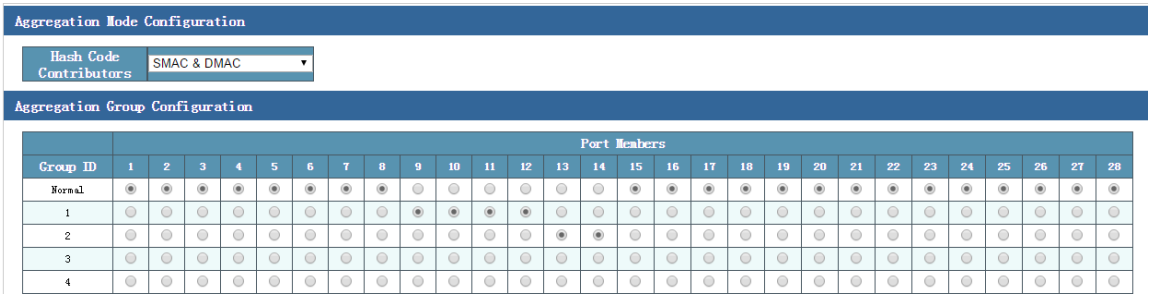
  By default, all aggregation groups are created, and no port member is added for a switch. To add a member port to an aggregation group, select the radio button corresponding to the ID of the aggregation group.

Tip:

- On the same port, only one type of aggregation (either static aggregation or dynamic LACP aggregation) can be configured.
- Configurations of member ports in the same aggregation group must be consistent.
- An aggregation group can contain two to eight member ports.

Configuration example:

Set the load balancing mode to SMAC&DMAC, and add ports 9 to 12 to aggregation group 1 and ports 13 to 14 to aggregation group 2, as shown in the following figure.

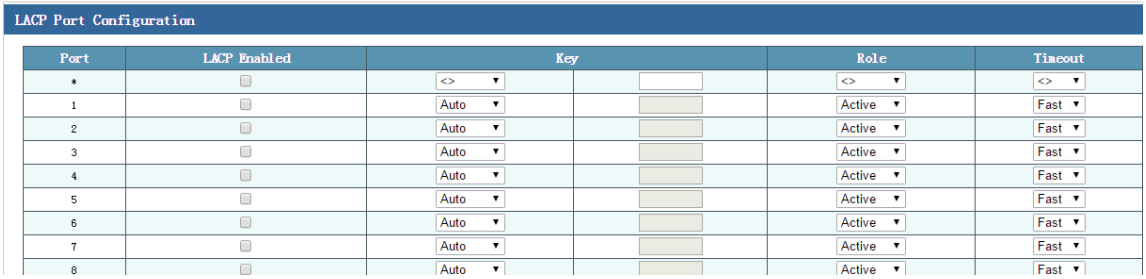


5.1.2 LACP Configuration

Link Aggregation Control Protocol (LACP) implements dynamic aggregation and deaggregation of links based on the IEEE 802.3ad standard. Two aggregation devices exchange aggregation information through LACP data units (LACPDUs) to bundle matched links for data transmission. Addition or deletion of ports to/from an aggregation group is automatically completed by the protocol, which features good flexibility and provides the capability of load balancing.

After LACP is enabled on a port, the port notifies its peer of the following information about the local port: system priority, system MAC address, port priority, port number, and operation key (determined by the physical attribute, upper-layer protocol information, and management key of the port).

The end with a higher device priority takes the lead in aggregation or deaggregation. The device priority is determined by the system priority and system MAC address. A smaller value of the system priority indicates a higher device priority. If the system priorities are the same, the device with a smaller system MAC address has a higher device priority. The end with a higher device priority selects ports for aggregation based on the port priority, port number, and operation key. Only ports with the same operation key can be added to the same aggregation group. In an aggregation group, the port with a smaller port priority value will be preferentially selected. If the port priorities are the same, the port with a smaller port number will be preferentially selected. After two ends exchange the aggregation information, the selected ports will be aggregated to send or receive data.



LACP configuration parameters include **Port**, **LACP Enabled**, **Key**, **Role** (active or passive), and **Timeout**.

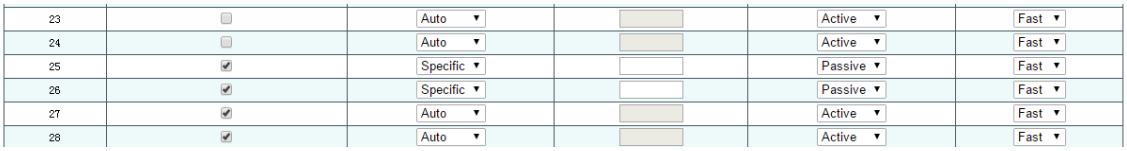
Only LACP-enabled ports perform LACP negotiation, making it possible to form an aggregate link. The key is the foundation of negotiation. Only ports with the same key can negotiate and form an aggregate link. The negotiation mode is either **active** or **passive**. If the negotiation mode is set to **active**, the device proactively initiates an aggregation negotiation. If the negotiation mode is set to **passive**, the device passively accepts an aggregation negotiation initiated by another device. When two devices are interconnected, the negotiation can succeed only when the negotiation mode is set to **active** on one or both of the devices.

- **Port**: Indicates the port number of the switch**.**
- **LACP Enabled**: If this check box is selected, LACP is enabled on the port; otherwise, LACP is disabled.
- **Key**: Members in the same aggregation group must be configured with the same management key. The key can be set to **Auto** or **Specific** (the value must be manually configured and ranges from 1 to 65,535). By default, the key is configured.

- **Role**: Options include **Active** and **Passive**. The default value is **Active**. Set **Role** to **Active** on the device at one end that participates in dynamic aggregation, and to **Passive** on the device at the other end.
- **Timeout**: Options include **Fast** (fast timeout) and **Slow** (slow timeout). The default value is **Fast**.

Configuration example:

On the LACP configuration page, select **LACP Enabled**, set Key to **Auto**, **Role** to **Active**, and retain other default settings for ports 27 and 28; select **LACP Enabled**, set Key to **Specific**, **Role** to **Passive**, and retain other default settings for ports 25 and 26, as shown in the following figure. Then, save the configurations.



5.2 VLAN Management

Ethernet is a shared communication media based on the Carrier Sense Multiple Access/Collision Detect (CSMA/CD) technology. A LAN built using the Ethernet technology is not only a collision domain, but also a broadcast domain. When the number of hosts on the network is large, the collision becomes serious, broadcast flooding occurs, and the performance is significantly degraded. Even worse, the network is unavailable. Deployment of bridges or L2 switches on the Ethernet can resolve the problem of serous collision, but still cannot isolate broadcast packets. To address this issue, the Virtual Local Area Network (VLAN) technology emerges. This technology can divide a physical LAN into multiple logical LANs, that is, VLANs. Hosts located in the same VLAN can directly communicate with each other, but hosts located in different VLANs cannot communicate with each other. In this way, broadcast packets are confined in the same VLAN. That is, each VLAN is a broadcast domain.

Advantages of VLAN are as follows:

- Improve network performance. Broadcast packets are confined in the VLAN, which effectively controls broadcast storms of the network, saves the network bandwidth, and improves the network processing capability.
- Enhance network security. Devices in different VLANs cannot access each other, and hosts in different VLANs cannot directly communicate with each other. Packets must be forwarded at L3 through network layer devices, such as routers or L3 switches.

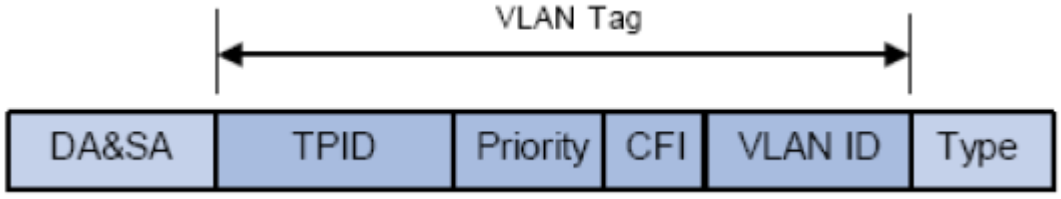
- Simplify network management. Hosts in the same virtual work group are not limited to a certain physical range, which simplifies network management, and makes it convenient for people in different areas to set up work groups.

Division of VLANs is not restricted by physical locations. Hosts in different physical locations may belong to the same VLAN. Users of one VLAN can connect to the same switch or different switches. This switch supports the 802.1Q VLAN, MAC-based VLAN, IP Subnet-based VLAN, and protocol VLAN. The protocol VLAN is effective only for untagged packets and packets with the priority tag. When a packet meets the requirements of the 802.1Q VLAN, MAC-based VLAN, IP subnet-based VLAN, and protocol VLAN, the switch will process the packet in the following order: MAC-based VLAN, IP subnet-based VLAN, protocol VLAN, and Port VLAN ID (PVID), and forward this packet in the corresponding VLAN.

802.1Q VLAN

A common switch works at the data link layer of the OSI model. To enable the switch to identify packets of different VLANs, the data link layer of the packets must be encapsulated. Therefore, the VLAN tag field is added to the data link layer encapsulation.

To standardize the VLAN implementation solution, the structure of packets with the VLAN tag is defined in IEEE 802.1Q. According to the protocol, a 4-byte VLAN tag is encapsulated after the source and destination MAC addresses to identify the VLAN-related information. The VLAN tag contains four fields, including the Tag Protocol Identifier (TPID), Priority, Canonical Format Indicator (CFI), and VLAN ID, as shown in the following figure.



1. **TPID**: This field indicates that the data frame contains the VLAN tag. It is a 16-bit field. According to the protocol, the default value of TPID is **0x8100**.
2. **Priority**: This field indicates the transmission priority of the packet.
3. **CFI**: On an Ethernet switch, CFI is always set to **0**. Due to the compatibility feature, CFI is often used between the Ethernet and token ring networks. If CFI of a frame received on an Ethernet port is set to 1, the frame is not forwarded because this Ethernet port is an untagged port.

4. **VLAN ID**: This field identifies the ID of the VLAN to which the packet belongs. It is a 12-bit field. The value ranges from **0** to **4095**. As **0** and **4095** are reserved values and generally not assigned to users, the VLAN ID generally ranges from **1** to **4094**. The VLAN ID is abbreviated as VID.

A switch uses the VLAN ID to identify the VLAN to which a packet belongs. If a received packet does not contain a VLAN tag, the switch encapsulates the default VLAN ID of the receive port in the packet, and transmits the packet in the default VLAN of the receive port.

In this manual, a packet that contains the VLAN tag field is called tagged frame, and a packet that does not contain the VLAN tag field is called untagged frame. A frame with the priority tag refers to a packet that contains the VLAN tag field, but the VLAN ID is 0.

Three link types of a port:

When creating a 802.1Q VLAN, you need to configure the link type of a port based on the device connected to the port. Three links types of a port are available:

1. Access: A port can belong to only one VLAN. The rule for sending packets over a port is UNTAG. An access port is often connected to a user terminal. When an access port is added to another VLAN, it automatically exits from the original VLAN.

2. Trunk: A trunk port allows packets of multiple VLANs to pass through, and can receive or send packets of multiple VLANs. It is often used for cascading of network devices. A VLAN often spans different switches on the network. For a trunk port, the default rule for sending packets over a port is TAG. When default VLAN data of the port is forwarded, the VLAN information is removed; when other types of VLAN data is forwarded, the VLAN information is retained.

3. Hybrid: A hybrid port allows packets of multiple VLANs to pass through, and can receive or send packets of multiple VLANs. It is often used for connection between network devices or connection with user devices. The rule for sending packets over a hybrid port can be flexibly configured based on the device connected to the port.

Processing relationship between the PVID and VLAN packets:

PVID is the default VLAN ID of a port. When a packet received on a port of a switch does not contain the VLAN tag, the switch inserts a VLAN tag to the packet based on the PVID value of the receive port, and then forwards the packet.

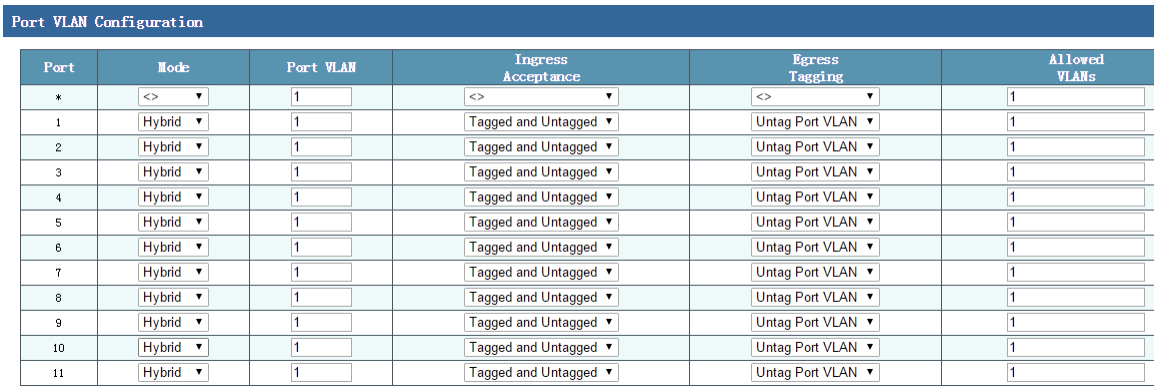
When VLANs are divided in a LAN, the PVID is an important parameter for each port. It indicates the VLAN to which the port belongs by default. Two functions of the PVID are as follows:

1. When an untagged packet is received on a port, the switch inserts a VLAN tag to the packet based on the PVID.

2. The PVID specifies the default broadcast domain of a port. That is, when a UL or broadcast packet is received on a port, the switch broadcasts this packet in the default VLAN of the port.

You configure the IEEE802.1Q VLAN on three pages, including the VLAN configuration, VLAN status, and VLAN port configuration pages.

On the port VLAN configuration page, you can configure parameters shown in the following figure.



- **Mode**: Three modes are available, including **Access**, **Trunk**, and **Hybrid**.

Mode	**Description**
Access	An access port can send packets of only one VLAN. The sent packets do not contain any VLAN tag. An access port is generally used to connect a user terminal, the VLAN tag of which cannot be identified, or used when it is unnecessary to distinguish between VLAN members.
Trunk	A trunk port can send packets of multiple VLANs. For packets sent by a port, you can configure data to determine whether packets of the PVID VLAN contain the VLAN tag, and whether packets of other VLANs contain the VLAN tag. Generally, when packets are sent out of a port, packets of the PVID VLAN do not contain the VLAN tag, and packets of other VLANs must contain the VLAN tag. A trunk port is generally used for interconnection between network transmission devices.
Hybrid	A hybrid port can send packets of multiple VLANs. For packets sent by a port, you can configure the data so that the packets of all the VLANs contain or do not contain the VLAN tag, and packets of the PVID VLAN do not contain the VLAN tag. A hybrid port can

Mode	Description
	be used for interconnection between network transmission devices, or be directly connected to terminals.

- **Port VLAN**: Indicates the PVID of a port. The default VLAN of an access port is the VLAN where the port is located. A trunk or hybrid port allows packets of multiple VLANs to pass through, and its default VLAN is configurable.
- **Egress Tagging**: Specifies whether a tag is added to a packet when the packet is sent out from the port. For an outgoing packet of a port, a tag is not added if the port is an access port, and is generally added if the port is a trunk port.

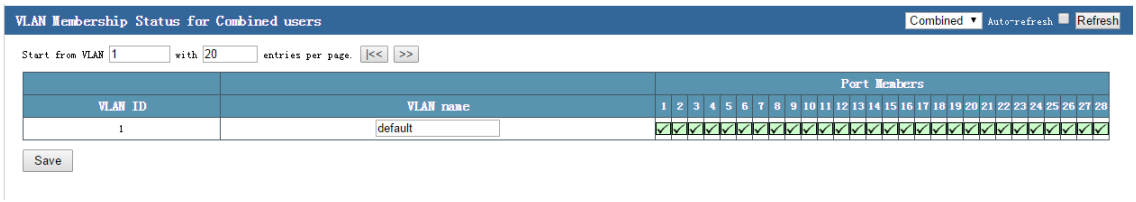
Option	Description
Untag Port Vlan	For outgoing packets of a port, only packets of the PVID VLAN do not contain the tag.
Tag All	For outgoing packets of a port, packets of all the VLANs contain the tag.
Untag All	For outgoing packets of a port, packets of all the VLANs do not contain the tag.

- **Ingress Acceptance**: Specifies whether the port receives tagged packets.

Option	Description
Tagged and Untagged	The port receives all tagged and untagged packets.
Tagged Only	The port receives only tagged packets.
Untagged Only	The port receives only untagged packets.

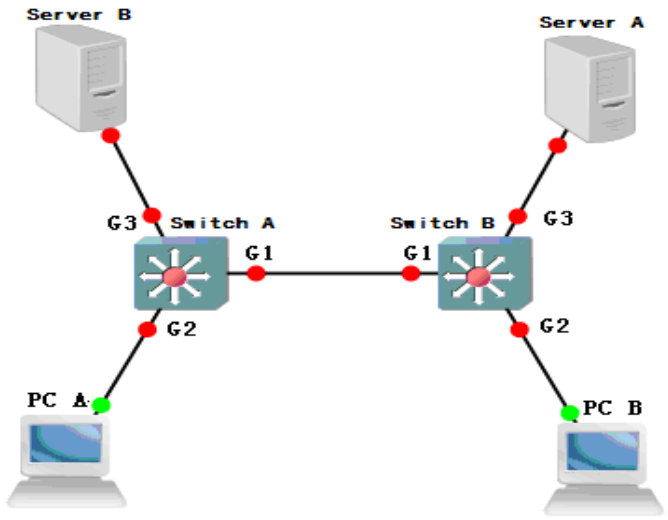
- **Allowed VLANs**: Specifies the VLAN to which the port belongs. For example, if **Allowed VLANs** is set to **1-3** or **1, 2, 3**, the port belongs to VLANs 1 to 3.

  On the VLAN status page, you can view information about VLANs to which ports belong.



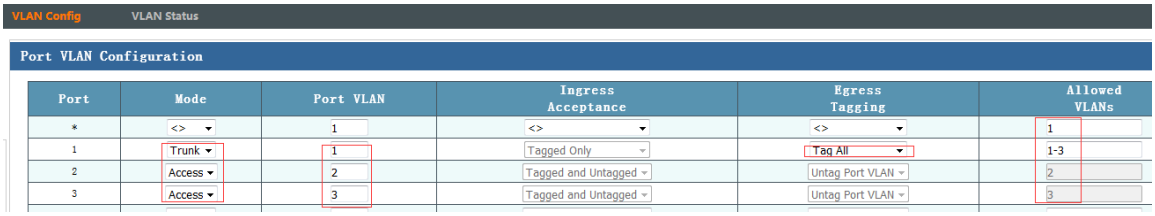
Configuration example:

The following figure shows the network topology.



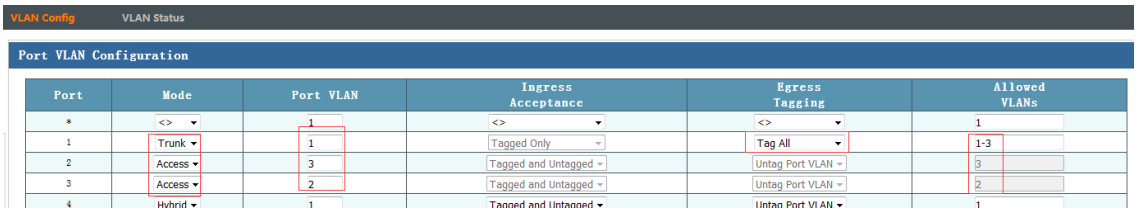
Networking requirement: Switch A is connected to PC A and server B. Switch B is connected to server A and PC B. PC A and server A belong to one department, and PC B and server B belong to another department. Two VLANs are defined respectively for the two departments, and the two departments cannot communicate with each other.

Step 1 Configure switch A as follows: Add the port G3 to VLAN 3, and set the port type to **Access**. Add the port G2 to VLAN 2, and set the port type to **Access**. Add the port G1 to VLANs 1–3, and set the PVID to **1**, port type to **Trunk**, and **Egress Tagging** to **Tag All**. The following figure shows the configuration results.



Step 2 Configure switch B as follows: Add the port G3 to VLAN 2, and set the port type to **Access**. Add the port G2 to VLAN 3, and set the port type to **Access**. Add the port G1 to VLANs 1–3, and set

the PVID to **1**, port type to **Trunk**, and **Egress Tagging** to **Tag All**. The following figure shows the configuration results.



5.3 VCL

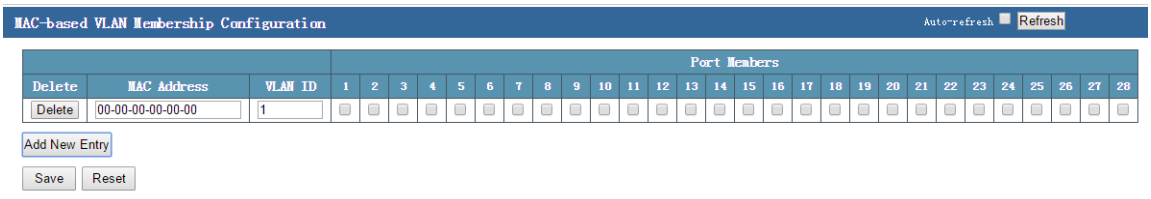
5.3.1 MAC-based VLAN

MAC-based VLAN is another method for dividing VLANs. VLANs are divided based on the MAC address of each host. That is, the MAC address of every host is bound with a VLAN. After the MAC address is bound with a VLAN, the device with the MAC address can change the port flexibly so far as the port is connected to a member port of the corresponding VLAN. In this way, modification of the VLAN member configuration is not required.

In an MAC-based VLAN, packets are processed in the following way:

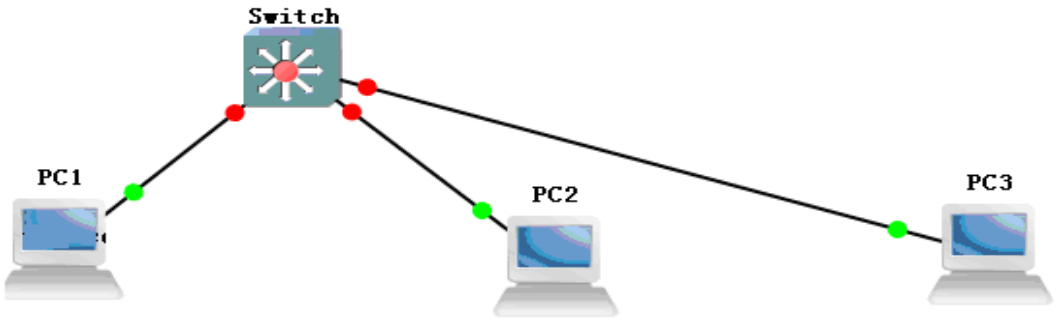
1. When receiving untagged packets on a port, the switch first checks whether the corresponding MAC-based VLAN is created. If yes, an MAC VLAN tag is inserted to the packet. If not, the packet is matched according to other rules (such as the protocol VLAN). If a match is found, the switch forwards the packet. If no match is found, the switch inserts a tag to the packet based on the PVID of the receive port, and forwards the packet in the default VLAN.

2. When receiving a tagged packet on a port, the switch processes the packet according to the method for processing the 802.1Q VLAN packets. If the receive port allows packets of this VLAN to pass through, the switch forwards the packet normally. If the receive port does not allow packets of this VLAN to pass through, the switch drops the packet.



The preceding figure shows the MAC-based VLAN configuration page of the switch. You can divide VLANs on the switch based on MAC addresses, and add ports of the switch to these VLANs.

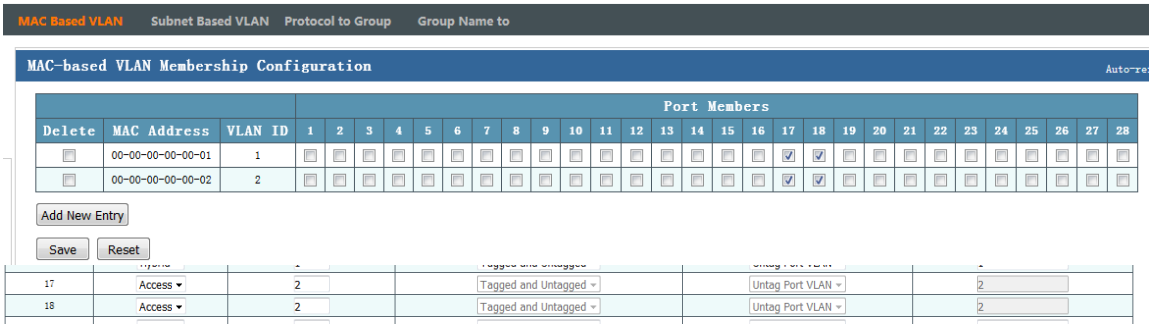
Configuration example:



PC 1 is connected to the port G17 of the switch, and PC 2 is connected to the port G18 of the switch. Configure the MAC-based VLAN so that PC 1 and PC 2 can communicate with each other in VLAN 2, but cannot communicate with each other in other VLANs.

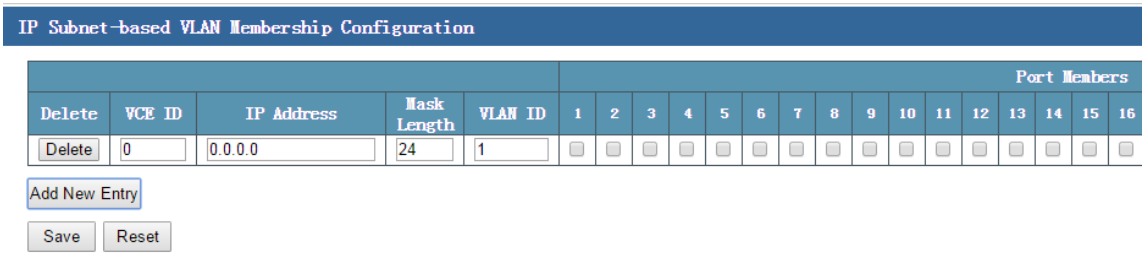
The MAC address of PC 1 is 00-00-00-00-00-01, and the MAC address of PC 2 is 00-00-00-00-00-02.

Add the MAC addresses of PC 1 and PC 2 to VLAN 2, and add ports 17 and 18. On the port VLAN configuration page, add ports 17 and 18 to VLAN 2. The following figures show the configurations.



After the configuration is completed, PC 1 and PC 2 can communicate with each other in VLAN 2, but cannot communicate with each other in other VLANs.

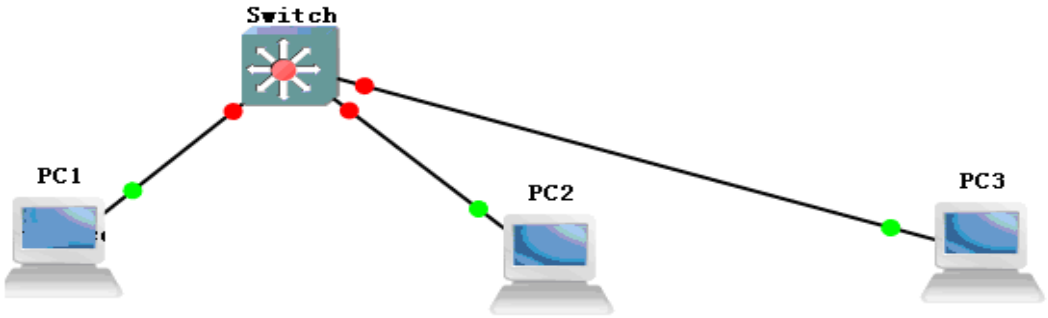
5.3.2 IP Subnet-based VLAN



The preceding figure shows the IP subnet-based VLAN configuration page of the switch. You can divide VLANs on the switch based on the subnet mask of the IP address, and add ports of the switch to these VLANs.

VCE: Indicates the egress ID of the VLAN control list (VCL). The value ranges from **1** to **128**.

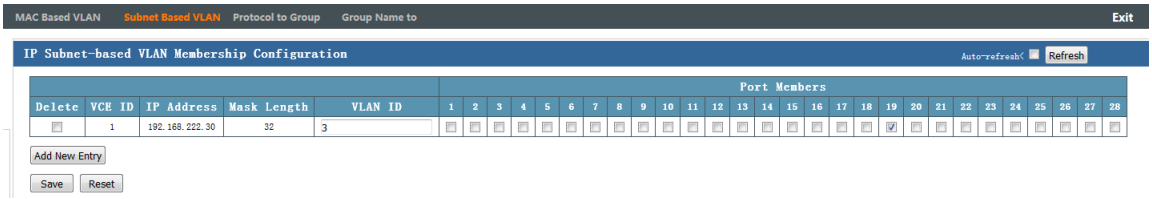
Configuration example:



PC 1 is connected to the port G17 of the switch, PC 2 is connected to the port G18 of the switch, and PC 3 is connected to the port G19 of the switch. On the port-based VLAN configuration page, add all the three ports to VLAN 2. Configure the IP subnet-based VLAN so that PC 1 and PC 2 can ping with each other, but PC 3 cannot ping PC 1 and PC 2.

The IP address of PC 1 is 192.168.222.10, the IP address of PC 2 is 192.168.222.20, and the IP address of PC 3 is 192.168.222.30.

The following figure shows the configuration results.



After the configuration is completed, PC 1 and PC 2 can ping with each other, but PC 3 cannot ping PC 1 and PC 2.

5.3.3 Protocol to Group Name Mapping

Based on the network layer protocol, protocol VLANs can be divided into the IP, IPX, DECnet, AppleTalk, and Banyan VLANs. That is, VLANs are grouped by the network layer protocol, which allows the broadcast domain to span several switches. In addition, users can move freely within the network without changing their VLAN membership. A network administrator can create protocol VLANs if he/she wishes to manage users based on specific applications and services.

The switch supports division of VLANs based on the common protocol types. The following table lists the values of common protocol types. You can create protocol VLANs based on the actual requirements.

Protocol Type	Value
ARP	0x0806
IP	0x0800
LACP	0x8809
802.1X	0x888E
IPX	0x8137

In a protocol VLAN, packets are processed in the following way:

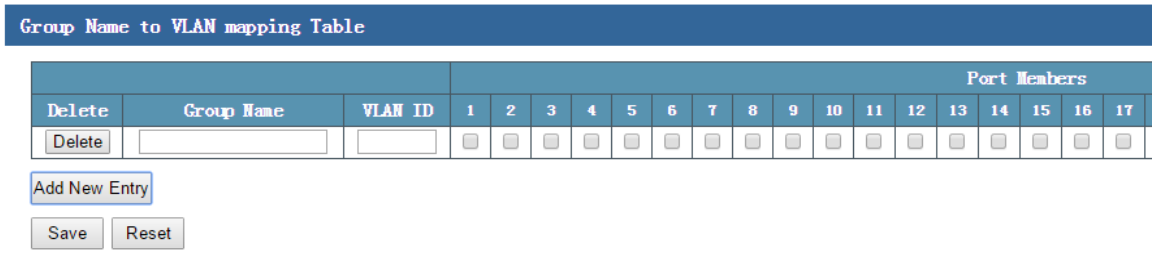
1. When an untagged packet is received on a port, the switch first checks whether the corresponding protocol VLAN is created. If yes, the switch inserts the protocol VLAN tag to the packet. If not, the switch inserts a tag to the packet based on the PVID of the receive port, and forwards the packet in the related VLAN.

2. When receiving a tagged packet on a port, the switch processes the packet according to the method for processing the 802.1Q VLAN packets.If the receive port allows packets containing this VLAN tag to pass through, the switch forwards the packet normally. If the receive port does not allow packets of this VLAN tag to pass through, the switch drops the packet. The following table describes the meaning of each frame type in the protocol to group name mapping table.

Frame Type	Description
Ethernet	Ethernet packet

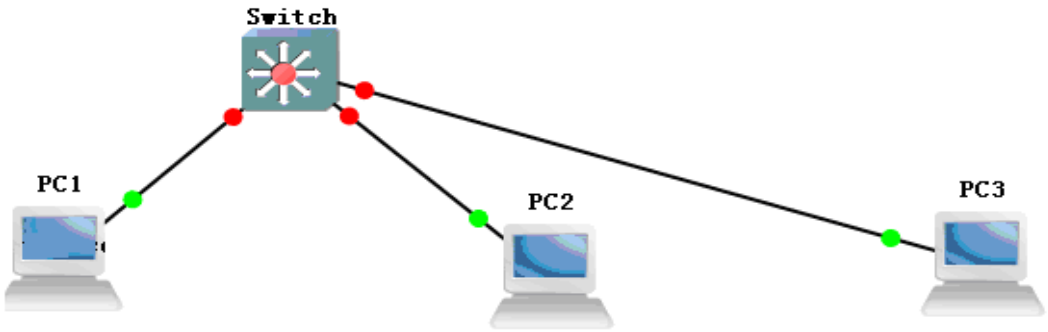
The preceding figure shows the IP subnet-based VLAN configuration page of the switch.

5.3.4 Group Name to VLAN Mapping



Note: The group name defined in the protocol to group name mapping table is mapped to a VLAN. VLANs are divided based on the protocol, and various ports are added to the VLANs.

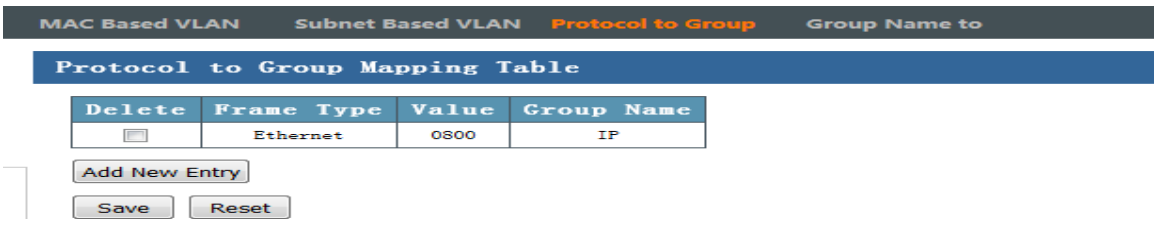
Configuration example:



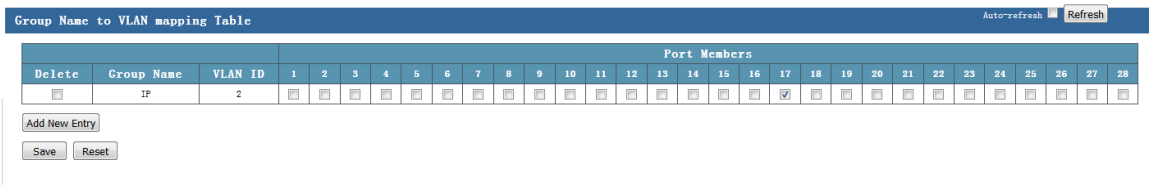
PC 1 is connected to the port G17 of the switch. PC 1 is located in a port-based VLAN. The interface IP address of VLAN 1 is 192.168.222.1/24, and the interface IP address of VLAN 2 is 192.168.2.1/24. Configure the protocol-based VLAN so that IP packets can be transmitted only in VLAN 2. Configure data as follows:

Step 1 On the port-based VLAN configuration page, add G17 to VLAN 2.

Step 2 Configure the protocol-based VLAN, as shown in the following figure.



Step 3 Configure the group name to VLAN mapping table, as shown in the following figure.



After the configuration is completed, PC 1 can use the interface IP address of VLAN 2 to access the web interface of the switch. If G17 is added to VLAN 1 on the port-based VLAN configuration page, PC 1 cannot use the interface IP address of VLAN 1 to access the web interface of the switch.

Note: 1. The VCL must be used together with the port-based VLAN.

2. Priorities of VLANs in the VCL are as follows: MAC-based VLAN > IP subnet-based VLAN > Protocol VLAN

5.4 DHCP Snooping

DHCP snooping is a security feature of DHCP, and provides the following functions:

1. Ensure that a client obtains its IP address from an authorized server.

If an unauthorized DHCP server that is built privately exists on the network, the DHCP clients may obtain incorrect IP addresses and network configuration parameters, and consequently cannot implement communication normally. To ensure that DHCP clients can obtain IP addresses from an authorized DHCP server, the DHCP snooping security mechanism supports configuration of ports as trusted or untrusted ports.

- A trusted port can forward received DHCP packets normally.
- On receiving the DHCP-ACK and DHCP-OFFER packets from the DHCP server, an untrusted port drops the packets.

On the DHCP snooping device, the port connected to the DHCP server must be configured as a trusted port, and other ports must be configured as untrusted ports. In this way, DHCP clients can obtain IP addresses only from an authorized DHCP server, and unauthorized DHCP servers cannot allocate IP addresses to DHCP clients.

2. Record the mapping between IP addresses and MAC addresses of DHCP clients.

By monitoring the DHCP-REQUEST packets and the DHCP-ACK packets received from trusted ports, the DHCP snooping device records the DHCP snooping entries, which contain information such as the MAC address of the client, IP address allocated by the DHCP server to the DHCP client, port connected to the DHCP client, and VLAN. Based on such information, the switch can implement:

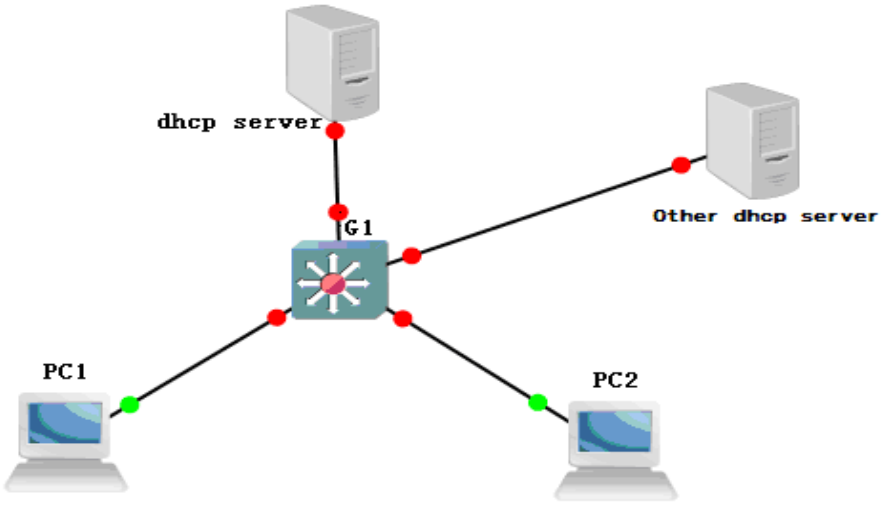
- Address Resolution Protocol (ARP) inspection: Check whether the user sending the ARP packet is an authorized user based on the DHCP snooping entries, thus preventing the ARP attacks initiated by unauthorized users.
- IP source guard: By dynamically obtaining the DHCP snooping entries, the switch filters packets forwarded by a port to prevent invalid packets from passing through the port.

The preceding figure shows the DHCP snooping configuration page. On this page, you can enable the DHCP snooping function globally, and allow a specified port to receive packets only from the trusted or untrusted areas.

- **Snooping mode**: You can select **Enabled** or **Disabled** to enable or disable the DHCP snooping function.
- **Port Mode Configuration**: The port mode can be set to **Trusted** or **Untrusted**.

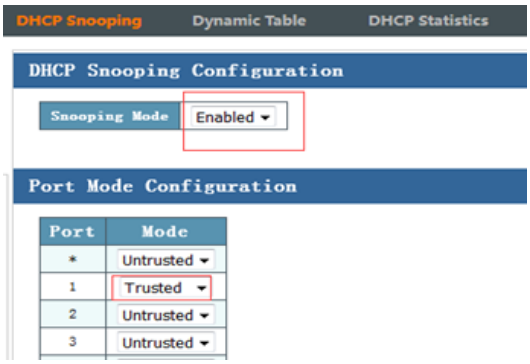
Port Mode	**Description**
Trusted (Default)	The port forwards received DHCP packets normally.
Untrusted	On receiving the DHCP-ACK and DHCP-OFFER packets from the DHCP server, the port drops the packets.

Configuration example:



The port G1 of the switch is cascaded with the DHCP server. All PCs connected to the switch must obtain IP addresses from this server. Other ports of the switch may be connected to devices with the DHCP server function. Configure data so that PCs connected to the switch can obtain IP addresses only from the DHCP server connected to G1.

Enable DHCP snooping globally. Set the port mode of G1 to **Trusted**, and the port mode of other ports to **Untrusted**. The following figure shows the configuration results.



5.5 DHCP Server

In the following scenarios, the DHCP server is often used to allocate IP addresses:

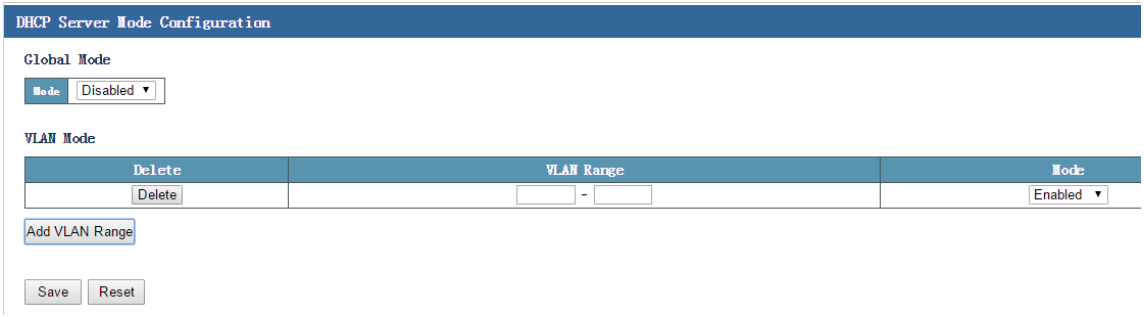
- The network is large in scale. The workload is huge if IP addresses are configured manually. It is difficult to perform centralized management on the entire network.
- The number of hosts on the network is greater than the number of IP addresses supported by the network. It is impossible to allocate a fixed IP address to every host. For example, the Internet

service provider (ISP) restricts the number of users who concurrently access the network, and users must dynamically obtain their own IP addresses.

- Only a few hosts on the network need fixed IP addresses, and most hosts do not need fixed IP addressed.
- The DHCP server configuration consists of three parts, including mode configuration, excluded IP address configuration, and address pool configuration.

5.5.1 DHCP Server Mode Configuration

On the DHCP server mode configuration page, you can configure parameters shown in the following figure.

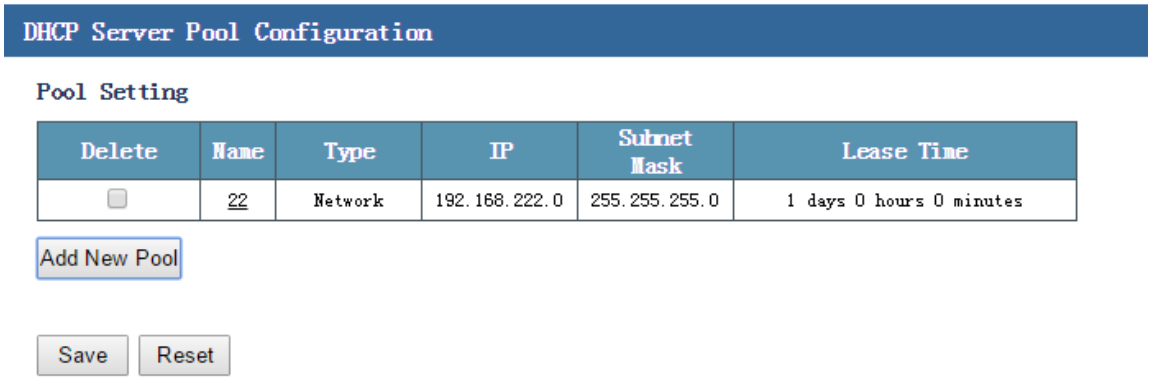


- **Global Mode**: You can select **Enabled** or **Disabled** to globally enable or disable the DHCP server function.
- **VLAN mode**: It is used to add VLANs in which the DHCP server is enabled.

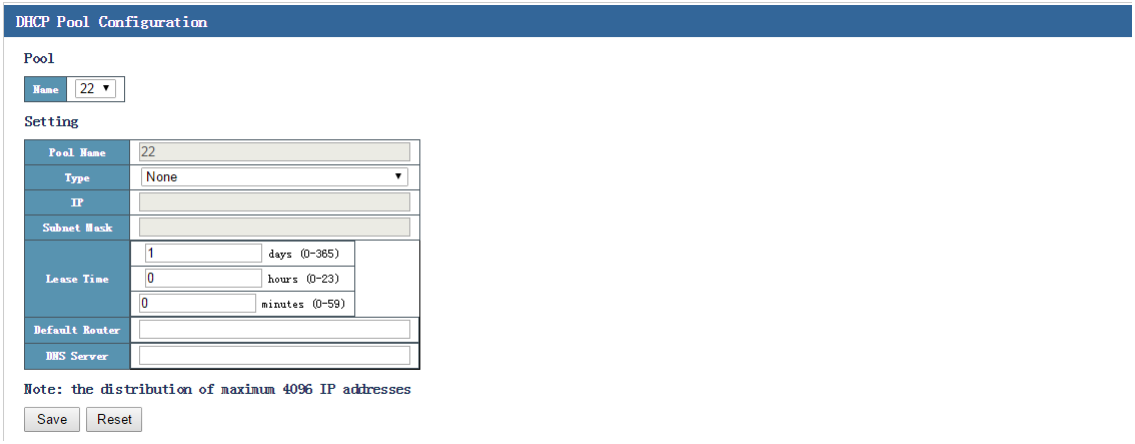
5.5.2 DHCP Server Excluded IP Configuration

- **Excluded IP Address**: Specifies the range of the excluded IP addresses. These IP addresses will not be automatically obtained by clients. Note that the VLAN interface IP addresses must be excluded; otherwise, clients may fail to obtain IP addresses.

5.5.3 DHCP Server Pool Configuration



- **Pool Setting**: Create an address pool name. After the address pool name appears in the list, click the address pool name to configure the address pool.



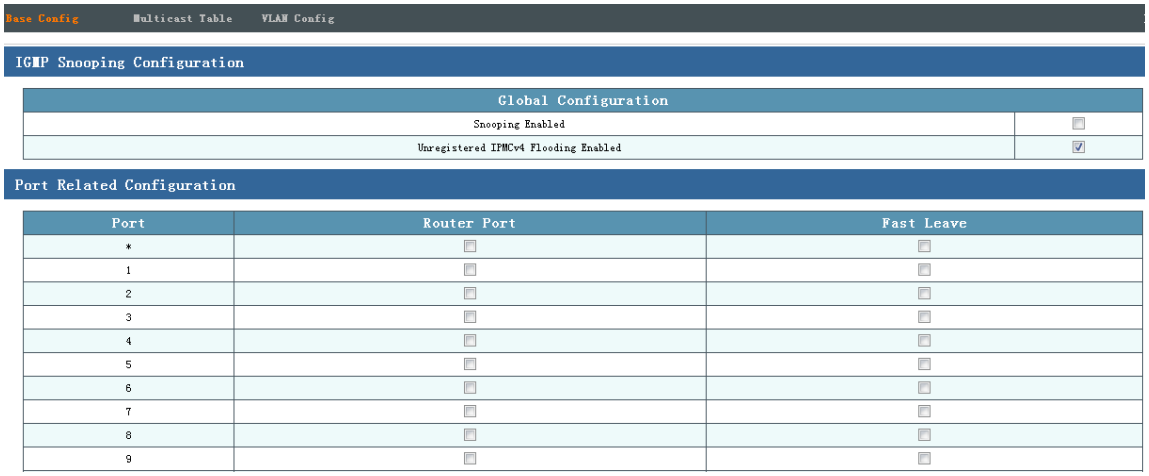
- **Type**: The default value is **None**. The option **Network** indicates the network segment address, and **Host** indicates the host address.
- **IP**: Indicates the network segment address or the host address.
- **Subnet Mask**: Indicates the subnet mask of the network segment address or the host address.
- **Least Time**: Indicates the time that the address obtained from the DHCP server is released.
- **Default router**: (The default router is in fact the default gateway.) After the default gateway is configured on the DHCP server, the gateway can be automatically allocated to PCs. Once the default gateway of the network changes, you only need to modify the settings of the default gateway on the DHCP server, and then all the PCs on the network can obtain the IP address of the new default gateway. This method is applicable to a network in large scale or the TCP/IP parameters of the network may change.

- **DNS Server**: If the DNS server address is configured on the DHCP server, the DNS server address can be automatically allocated to all the PCs on the network.

5.6 IGMP Snooping

Internet Group Management Protocol (IGMP) snooping is a multicast restraining mechanism that runs on L2 devices. It is used to manage and control multicast groups. By analyzing received IGMP packets, an IGMP snooping L2 device sets up a mapping relationship between ports and MAC multicast addresses, and forwards multicast data based on this mapping relationship.

5.6.1 Basic Configuration of IGMP Snooping



IGMP Snooping Configuration:

- **Snooping Enabled**: You can select the check box to globally enable the IGMP snooping function. By default, this function is disabled.
- **Unregistered IPMCv4 Flooding Enabled**: You can select the check box to enable this function.

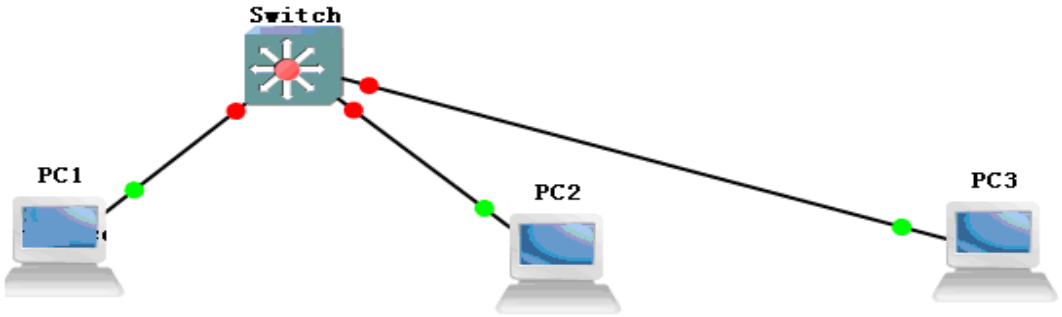
Port Related Configuration:

- **Router Port**: Indicates the port that is connected to an L3 multicast device (DR or IGMP querier) on the switch. The switch records all its router ports in the router port list.
- **Fast Leave**: You can select this check box to enable fast leave. By default, this function is disabled.

Note: If both **Snooping Enable** and **Unregistered IPMCv4 Flooding Enabled** are selected, only **Unregistered IPMCv4 Flooding Enabled** takes effect. If both are not selected, the switch does not support the multicast forwarding function.

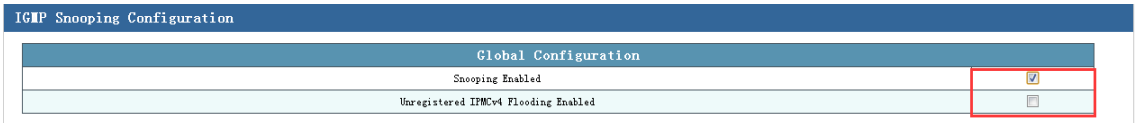
Configuration example:

As shown in the following figure, PC 1 is the broadcast end (multicast source) and transmits a video file to PC 2 for synchronous playing through video software. PC 2 is connected to a specified port of the switch in VLAN 1. The video file cannot be played on PCs connected to other ports. PC 1 is connected to the port G17, PC 2 is connected to G18, and PC 3 is connected to G19.

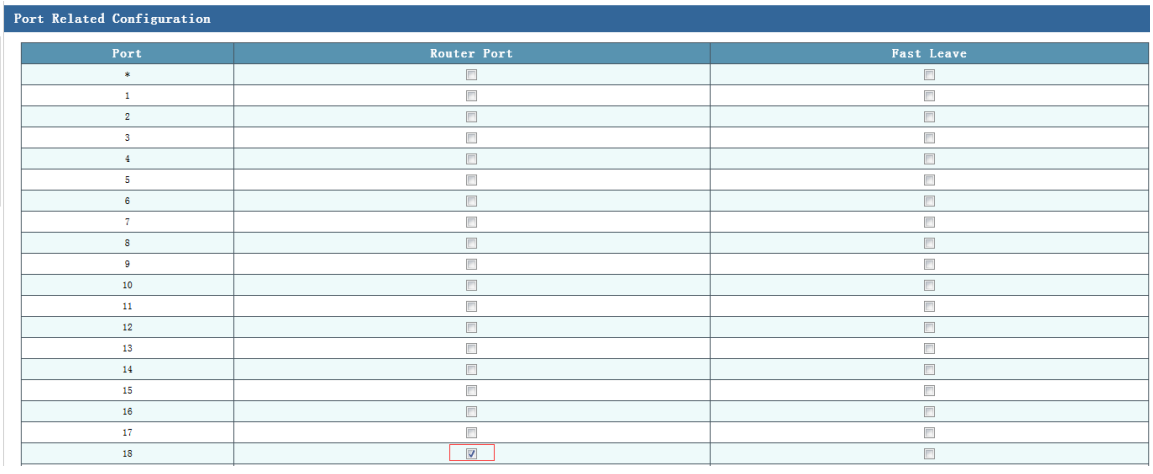


Configure data as follows:

Select **Snooping Enable**, deselect **Unregistered IPMCv4 Flooding Enabled**, configure the multicast address range, and select the port that accepts the video as the router port. The following two figures shows the configuration results.



Note: If **Unregistered IPMCv4 Flooding Enabled** is selected, the multicast address sent by the multicast source will be broadcast to all ports of the switch, and all the PCs connected to the switch can receive the video played by the PC that serves as the multicast source.



Note: As static member ports cannot be added, a non-member port cannot receive the multicast streams If the port is selected as a router port, the port can receive packets of any multicast group.

5.7 MVR Config

The L3 IGMP protocol is widely used for multicast on the IPv4 network. On the L2 network, however, the resource efficiency of IGMP is low. For example, if only a few receivers are connected to several ports of a switch, the switch still needs to flood the multicast traffic to all ports.
To resolve this problem, the IGMP snooping protocol is proposed. However, when receivers are in different VLANs, IGMP snooping is not useful because IGMP snooping is generally configured and effective in a single VLAN. The multicast VLAN register (MVR) function resolves the flooding problem when receivers are in different VLANs. It uses a dedicated and manually configured VLAN, multicast VLAN, to forward the multicast traffic on the L2 network. MVR can also be used in conjunction with IGMP snooping.

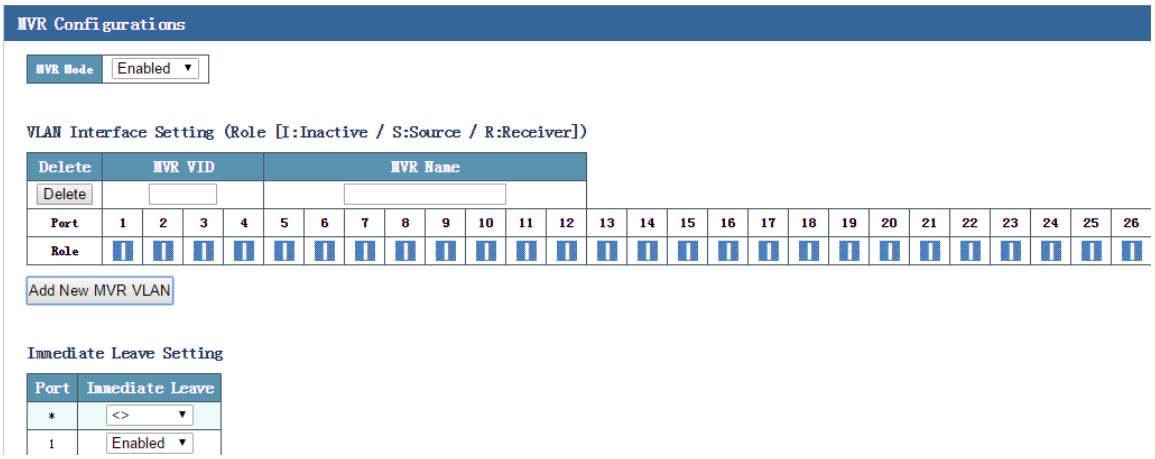
Like IGMP snooping, MVR allows L2 switches to listen to the IGMP control protocol. MVR and IGMP snooping run independently, and both can be configured on a switch. If both functions are enabled, MVR listens to only the join and report packets of groups that are statically configured for the MVR function, and other groups are still managed by IGMP snooping.

During configuration of the MVR function, two types of MVR ports are available:

- Source port: It refers to a port that multicast streams pass through in the multicast VLAN.
- Receive port: It refers to a port of the switch that is connected to a multicast snooping host. It can be placed in any VLAN except the multicast VLAN. This means that the MVR-enabled switch replaces the VLAN tag of the multicast receive port with the VLAN tag of the source port.

A multicast VLAN refers to a VLAN that must be manually configured on a specific network and used exclusively by MVR. It must be explicitly configured. A multicast VLAN is often used to transmit multicast streams on the network. It prevents repetition of multicast streams in different VLANs. The MVR VID must be consistent with the PVID of the VLAN where the multicast source is located.

MVR is designed for large-scale application of multicast on the Ethernet-based service provisioning network. For example, online video uses the multicast protocol, and terminals are large-screen TVs or computers.

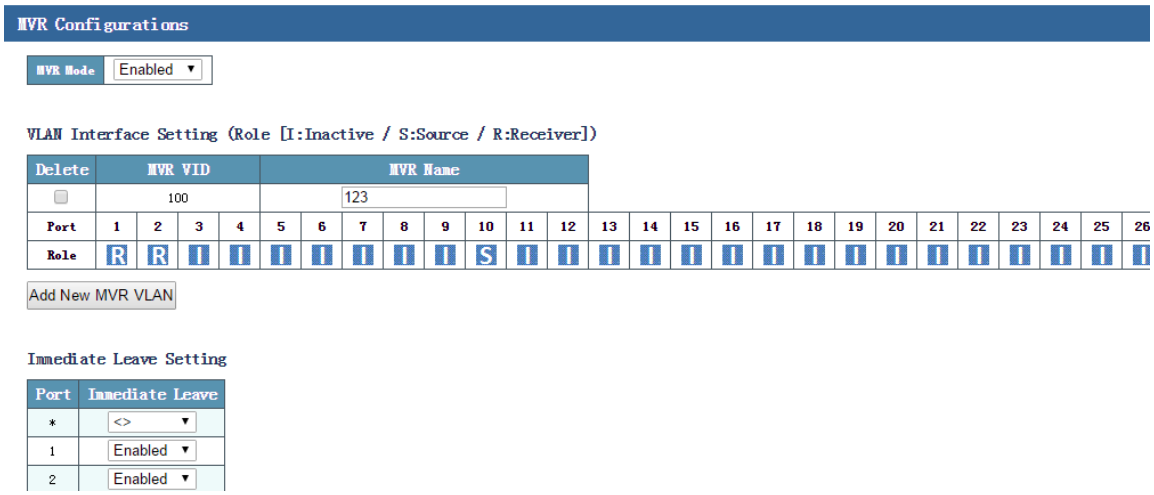


The preceding figure shows the page for creating an MVR VLAN.

- **MVR VID**: Indicates the ID of the VLAN to which the multicast source port belongs.
- **MVR Name**: Indicates the name of the multicast source.

Configuration example:

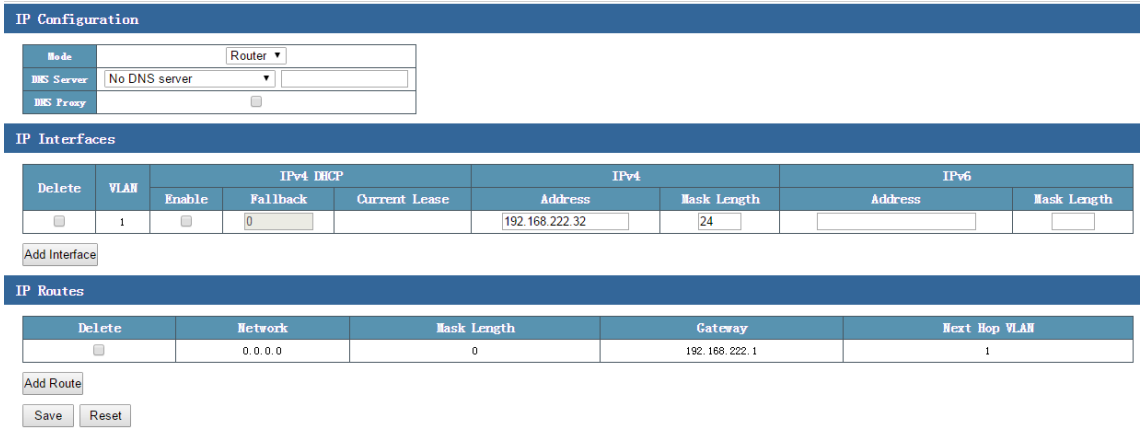
Ports 1 and 2 are access ports. Set PVID of ports 1 and 2 to **10** and **11**, respectively. Set PVID of port 10 to **100**. Enable MVR, set **MVR VID** to **100**, set **MVR Name** to **123**, and retain other default settings. Set **Role** of ports 1 and 2 to **R**, and **Role** of port 10 to **S**. Enable the fast leave function. The following figure shows the configuration results.



Port 10 functions as the source port and is connected to the multicast source. Ports 1, 2, and 3 are connected respectively to PC 1, PC 2, and PC3 to capture packets. After the multicast source starts to play the video, multicast packets can be captured on PC 1 and PC 2, but not on PC 3.

5.8 Router Config

On the IP configuration page, you can configure parameters shown in the following figure.

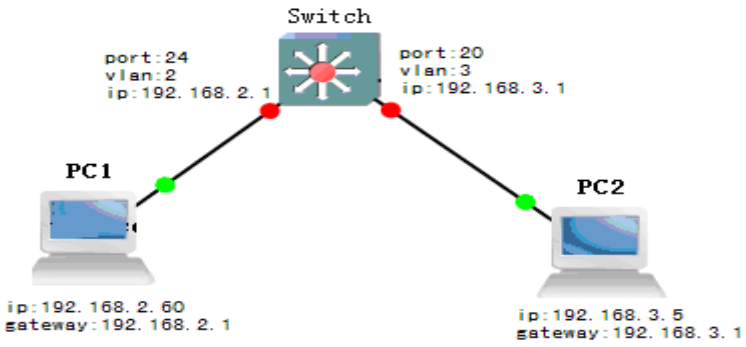


- **Router Config**: Configure the router functions of the switch. The virtual interface interworking and static routing functions can be implemented only after you set **Mode** to **Router**.
- **IP Interfaces**: A virtual interface is created for each VLAN based on the L3 routing principle of the switch so as to configure the L3 address information of every VLAN.
- **IPv4 DHCP**: If the **Enable** check box is selected, the interface IP address is automatically obtained. By default, this function is disabled. **Fallback** indicates the interval of the DHCP request, and **Current Lease** displays the currently obtained IP address.
- Click **Add Interface**, and select the **Enable** check box under **IPv4 DHCP**, or set the static IP address and mask length under **IPv4**.
- Click **Add Route**, fill in the L3 routing address of the switch under **Network**, and set **Mask Length** and **Gateway** according to the L3 routing address. The setting of **Next Hop VLAN** is consistent with that of **VLAN** in the **IP Interfaces** area.

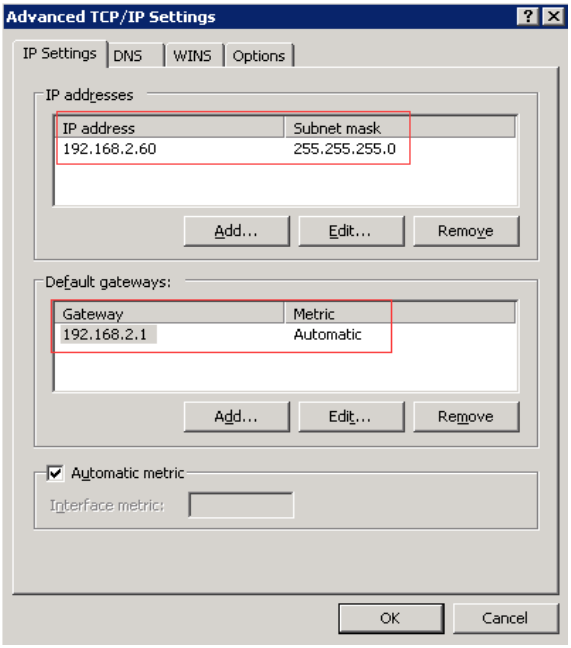
Configuration example 1:

Enable communication between different VLANs of the same switch. Configure data as follows:

Step 1 The following figure shows the network topology.

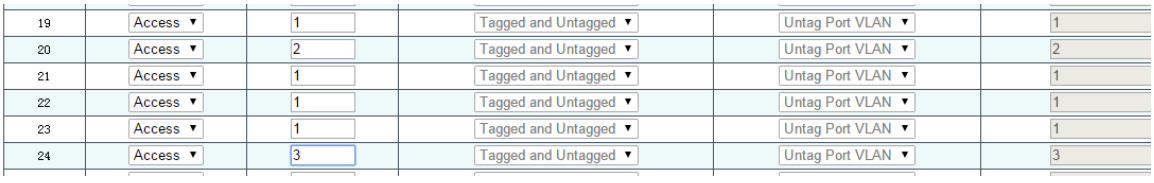


Step 2 Configure parameters on PCs. The following figure shows the configurations on PC 1.



Configurations on PC 2 are similar to those on PC 1.

Step 3 Configure the VLAN on the switch by choosing **Advanced Config** > **VLAN Management**, as shown in the following figure.

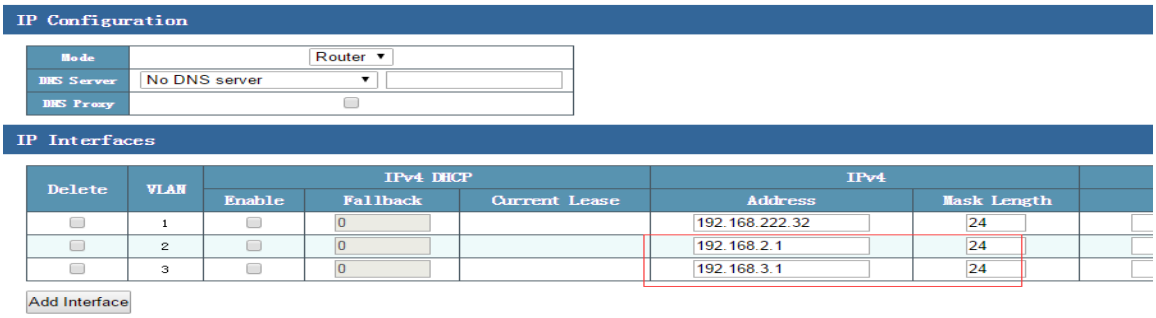


Step 4 Configure the static route by choosing **Advanced Config** > **Router Config**.

1. In the IP Configuration area, set **Mode** to **Router**.
2. In the **IP Interfaces** area, add the IP address 192.168.2.1 to VLAN 2 and set **Mask Length** to **24**.

Add the IP address 192.168.3.1 to VLAN 3 and set **Mask Length** to **24**.

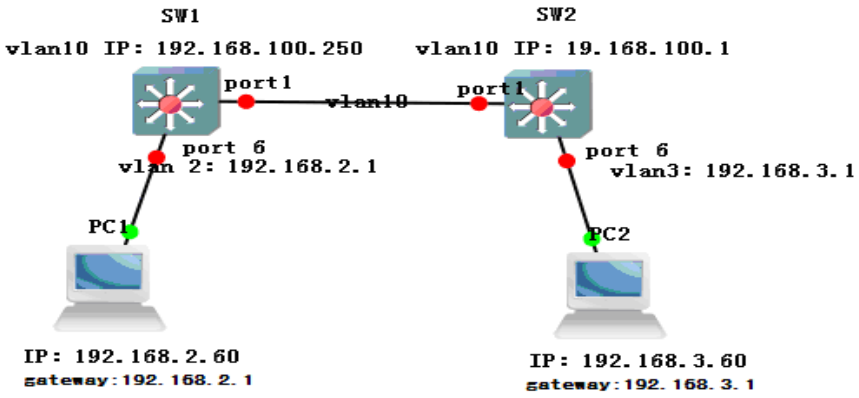
The following figure shows the configuration results.



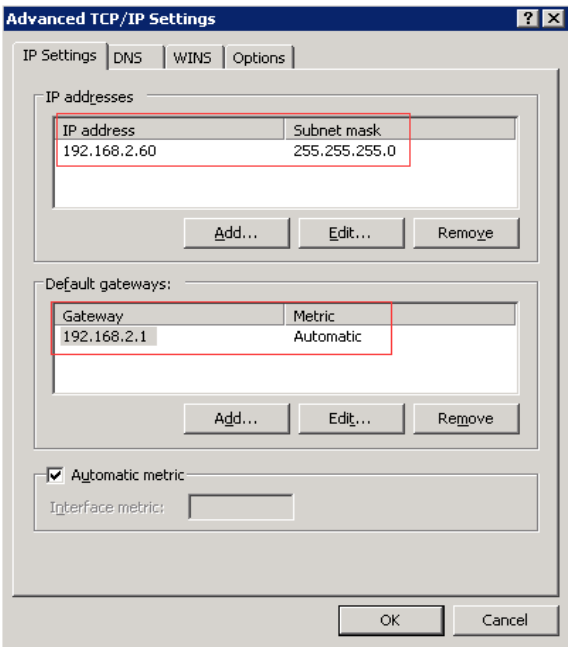
Configuration example 2:

Enable communication between different VLANs across different switches. Configure data as follows:

Step 1 The following figure shows the network topology.



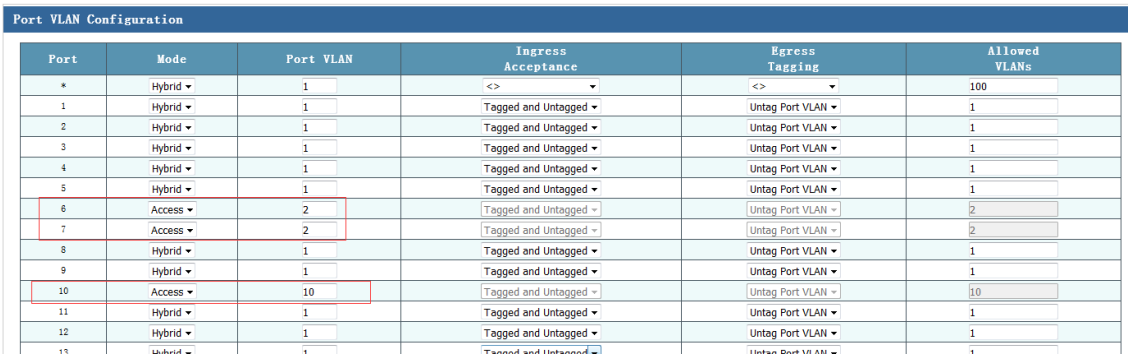
Step 2 Configure parameters on PCs. The following figure shows the configurations on PC 1.



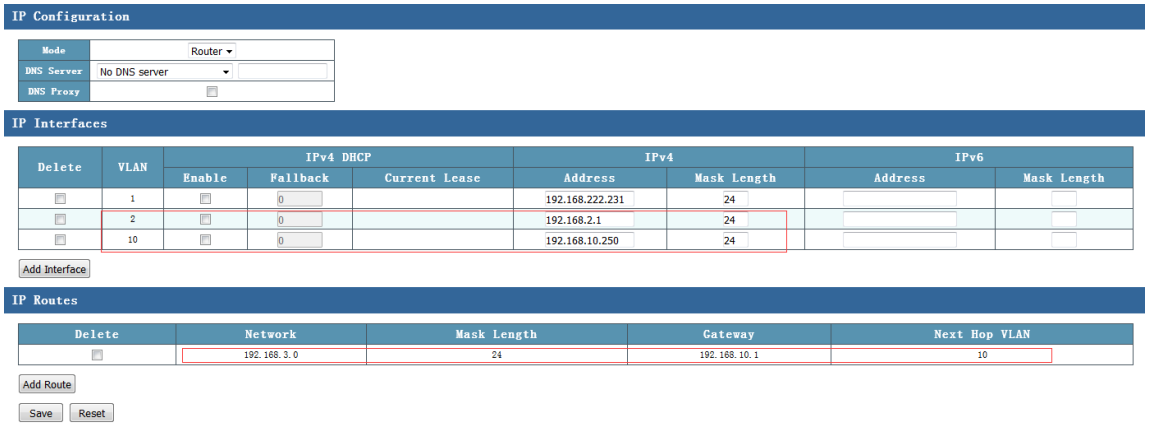
Configurations on PC 2 are similar to those on PC 1. On PC 2, the IP address is set to **192.168.3.*X*** (2-254), and the gateway is set to **192.168.3.1**.

Step 3 Configure data on switch 1 (SW 1).

1. Configure the VLAN by choosing **Advanced Config** > **VLAN Management**, as shown in the following figure.

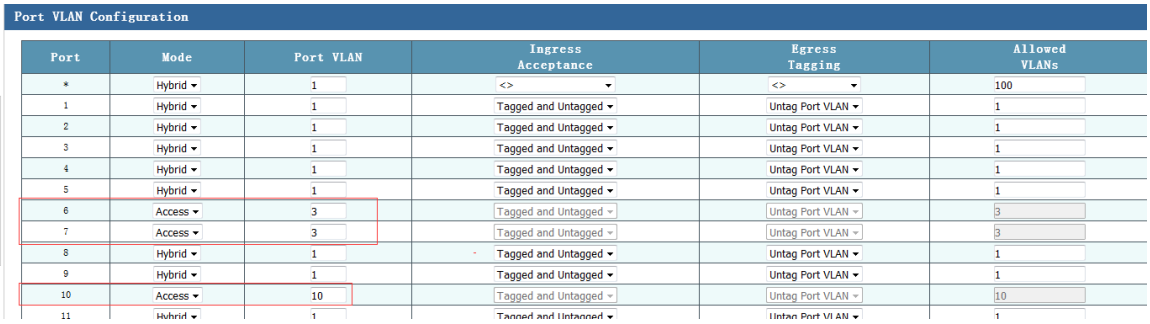


2. Configure the route by choosing **Advanced Config** > **Router Config**, as shown in the following figure.

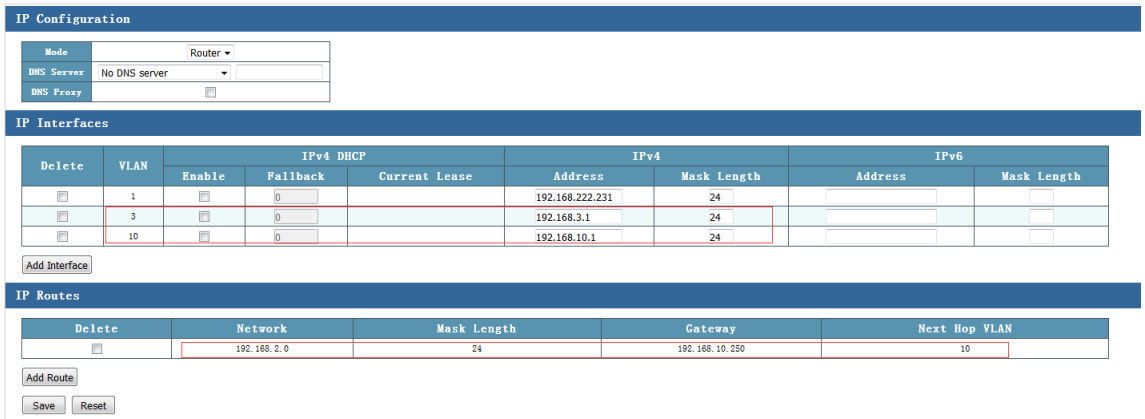


Step 4 Configure data on switch 2 (SW 2).

1. Configure the VLAN by choosing **Advanced Config** > **VLAN Management**, as shown in the following figure.



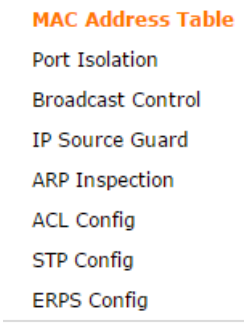
2. Configure the route by choosing **Advanced Config** > **Router Config**, as shown in the following figure.



After the configuration is completed, PC 1 can ping PC 2.

6 Network Security

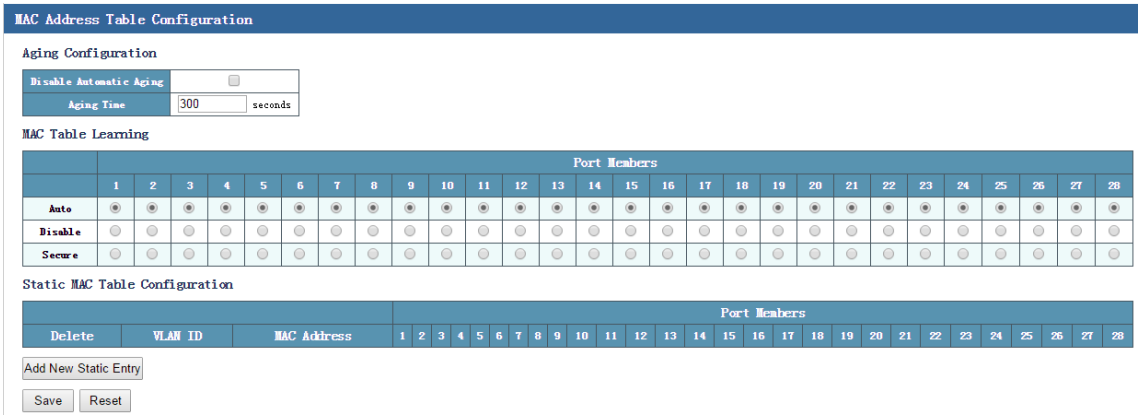
Click **Network Security** in the navigation bar, and then the following items are listed:



6.1 MAC Address Table

The MAC address table records the mapping between MAC addresses and ports, as well as VLANs to which the ports belong. When forwarding packets, the device queries the MAC address table based on the destination MAC address of each packet. If the MAC address table contains an entry that matches the MAC address of the packet, the device directly forwards the packet through the egress port in the entry. If the MAC address table does not contain any entry that matches the MAC address of the packet, the device broadcasts the packet through all ports in the corresponding VLAN except the receive port.

On the MAC address table configuration page, you can configure parameters shown in the following figure.



- **Aging Configuration**: You can configure the aging time of the MAC address table and disable aging.

Configuration Item	Description

Disable Automatic Aging	If the check box is selected, aging is disabled. The aging time is the last saving time.
Aging Time	Indicates the aging time, which is 300s by default.

- **MAC Table Learning:**

  Auto: The dynamic MAC address table is automatically learned.

  Disable: If this radio button is selected, the port cannot learn the dynamic MAC address, but can learn the static MAC address. The MAC port can implement communication no matter whether the port is bound with a static MAC address. If the **Disable** radio button is selected and the port is not bound with a static MAC address, the port sends data in unicast mode, and receives data in broadcast mode. For example, if the **Disable** radio button is selected for port 1 and not selected for other ports, port 1 sends data to other ports in unicast mode, and other ports send data to port 1 in broadcast mode. After the port is bound with a static MAC address, the port sends and receives data in unicast mode.

  Secure: If this radio button is selected, the port cannot learn the dynamic MAC address, but can learn the static MAC address. The MAC port cannot implement communication when the port is not bound with a static MAC address. If the **Secure** radio button is selected and the port is not bound with a static MAC address, the port drops the received packets, and forwards packets normally. After the port is bound with a static MAC address, the port sends and receives data in unicast mode.

- **Static MAC Table Configuration**: You can configure static MAC addresses here, and the entries do not age.
  - **Delete**: Delete the corresponding static MAC address entry.
  - **VLAN ID**: Select the VLAN to which the added static MAC address belongs.
  - **MAC Address**: Fill in the static MAC address to be bound with according to the format of the MAC address.
  - **Port Members**: Click to select the port to be bound with the static MAC address.

Tip: The priority of an entry in a static MAC address table is higher than that of an entry in the MAC address table that is automatically generated.

Configuration example:

1. Port disabling function

(1) Disable port 5. Port 5 cannot learn the MAC address.

(2) Send a packet from port 6 to port 5. All the ports can receive the packet.

(3) Send a packet from port 5 to port 6. Port 6 can receive the packet, but other ports cannot receive the packet.

(4) Add a static MAC address to port 5. The static MAC address is added successfully. PCs that use or do not use the MAC address can communicate normally with other ports, and can successfully ping the management IP address of the switch. Send a packet from the PC connected to port 6 to the PC connected to port 5. The packet is a unicast packet. The PC using this MAC address is connected to another port, and cannot communicate with the switch.

Summary: The port disabling function prohibits a port from automatically learning the dynamic MAC address, but the port can learn the static MAC address. This function does not affect data sending and receiving on the port.

2. Security function

(1) Set port 5 to the secure mode. Port 5 cannot learn the MAC address.

(2) Send a packet from the PC connected to port 6 to the PC connected to port 5. The packet is processed as an unknown unicast packet and is broadcast.

(3) Send packets from the PC connected to port 5 to the PC connected to port 6. All the packets are filtered and dropped by port 5.

(4) Add a static MAC address to port 5. The static MAC address is added successfully. The PC using this MAC address can communicate normally with other ports. Send a packet from the PC connected to port 6 to the PC connected to port 5. The packet is a unicast packet.

(5) Delete the MAC address added in step (4). Add an MAC address that is different from the MAC address of the PC. All the packets sent from this PC are filtered and dropped by port 5.

Summary: The port security function prohibits a port from automatically learning the dynamic MAC address, but the port can learn the static MAC address. In addition, only the data sent from the PC that is bound with an MAC address can be received or forwarded. The port where the secure mode is enabled will filter out and drop the packets that are not bound with the MAC address, but can receive packets forwarded from other ports of the device.

3. Static MAC address binding function

(1) Bind PC 1 with port 18, and set VLAN ID to **1**.

(2) Connect PC 1 to any port except port 18. PC 1 cannot communicate normally with the switch.

(3) Connect PC 2 to port 18. PC 2 can communicate normally with the switch.

(4) A port can be bound with at most 64 MAC addresses. One MAC address can be bound with one port in a VLAN.

Summary: After the static MAC address is bound with a PC, the bound PC can implement communication only after it is connected to the bound port, but the bound port can be connected to any PC.

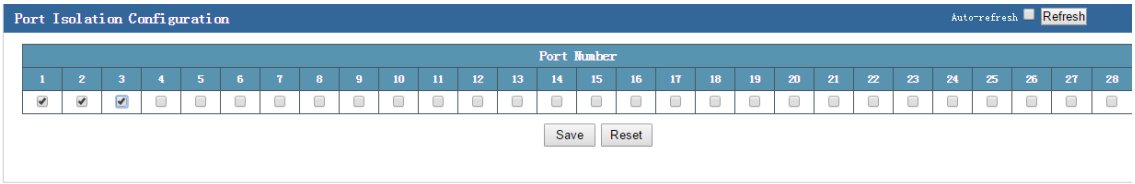
6.2 Port Isolation

The port isolation function can be used to isolate ports in the same VLAN from each other. You only need to add ports to an isolation group to implement isolation of L2 data communication of different ports in the same isolation group. The port isolation function provides users with a more secure, flexible, and convenient networking solution.

The preceding figure shows the port isolation configuration page of the switch. On this page, you can configure data to isolate ports of the same VLAN at L2.

Tip: A horizontal scroll bar is available at the bottom of the page. You can move the scroll bar to view all the ports on the right of the list.

Configuration example: Ports 1 to 6 belong to VLAN 2. Ports 1 to 3 must be isolated from each other, but ports 1 to 3 can communicate normally with ports 4 to 6. Configure data as follows:

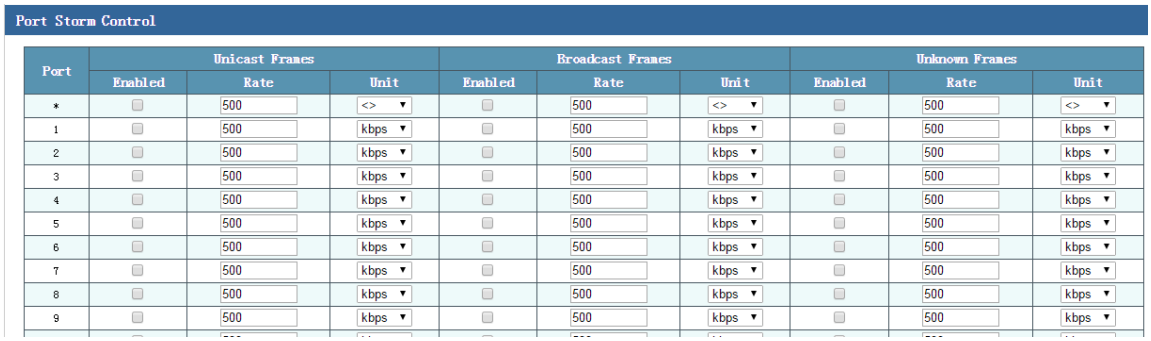


On the port isolation configuration page, select the check boxes corresponding to ports 1 to 3 and click **Save** to isolate ports 1 to 3 from each other. At this time, ports 4 to 6 can communicate normally with ports 1 to 3, and are not isolated.

6.3 Broadcast Control

When broadcast frames on the network are continuously forwarded, the number of broadcast frames increases sharply, which affects normal network communication and seriously degrades the network performance. This symptom is called broadcast storm. Storm control means that users can limit the size of broadcast traffic that can be received on a port. When this type of traffic exceeds the preset threshold, the system drops the broadcast frames beyond the traffic limit to prevent occurrence of broadcast storms and ensure normal operation of the network.

On the port storm control page, you can configure parameters shown in the following figure.



As shown in the preceding figure, the port storm control configuration page consists of four parts, including **Port**, **Unicast Frames**, **Broadcast Frames**, and **Unknown Frames**.

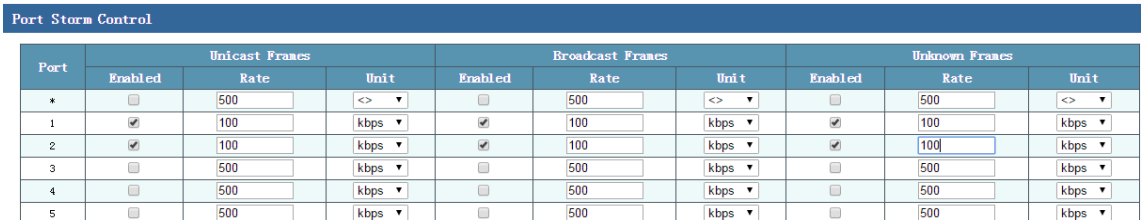
- **Port**: Indicates the port number of the switch.
- **Unicast Frames-Enabled**: You can select this check box to enable the port storm control function, or deselect this check box to disable the function.
- **Unicast Frames-Rate**: The default rate of unicast packets is **500**.
- **Unicast Frames-Unit**: The units of unicast packets include **kbps**, **mbps**, **fps**, and **kfps**. The default unit is **kbps**.
- **Broadcast Frames-Enabled**: You can select this check box to enable the port storm control function, or deselect this check box to disable the function.
- **Broadcast Frames-Rate**: The default rate of broadcast packets is **500**.

- **Broadcast Frames-Unit**: The units of broadcast packets include **kbps**, **mbps**, **fps**, and **kfps**. The default unit is **kbps**.
- **Unknown Frames-Enabled**: You can select this check box to enable the port storm control function, or deselect this check box to disable the function.
- **Unknown Frames-Rate**: The default rate of unknown packets is **500**.
- **Unknown Frames-Unit**: The units of unknown packets include **kbps**, **mbps**, **fps**, and **kfps**. The default unit is **kbps**.

Configuration example:

Enable the broadcast control function of unicast, broadcast, and unknown packets on ports 1 and 2, and set the unit to **100 kbps**. Configure data as follows:

On the port storm control configuration page, select the **Enabled** check boxes for ports 1 and 2, change the rates to **100**, and save the configurations. The following figure shows the configuration results.



6.4 IP Source Guard

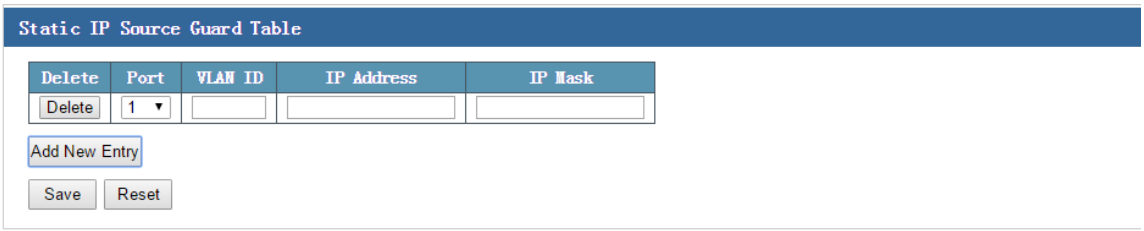
The IP source guard function can be used to filter packets forwarded by a port, thus preventing invalid packets from passing through the port, restricting unauthorized use of network resources (for example, unauthorized hosts may access the network by forging IP addresses of authorized users), and improving the port security.

If IP source guard is enabled on a port of the switch, when packets reach this port, the switch checks the IP source guard entries. If the packet matches an entry, the switch forwards the packet or the packet enters the subsequent flow. If the packet does not match any entry, the switch drops the packet. The binding function is port-based. After a port is bound, only this port is affected by the binding relationship, and other ports are not affected.

As shown in the preceding figure, the global IP source guard configuration page consists of two parts, including **IP Source Guard Configuration** and **Port Mode Configuration**.

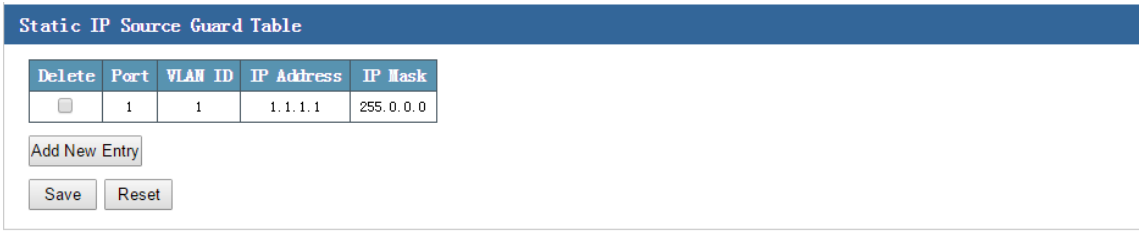
- **IP Source Guard Configuration-Mode**: **Disabled** is selected by default to globally disable the IP source guard function. You can select **Enabled** to globally enable the IP source guard function.
- **Translate dynamic to static**: Click this button to change an entry in the dynamic IP source guard table to a static entry.
- **Port Mode Configuration-Port**: Indicates the port number.
- **Port Mode Configuration-Mode**: Select **Enabled** or **Disabled** to enable or disable the IP source guard function of the corresponding port. By default, the source guard function of a port is disabled.
- **Port Mode Configuration-Max Dynamic Clients**: Indicates the maximum number of dynamic clients supported by the port. The default value is **Unlimited**. Options include **0**, **1**, **2**, and **Unlimited**. If the value is set to **0**, the client cannot communicate with the switch after obtaining an IP address.

The preceding figure shows the configuration page of the dynamic IP source guard table. The dynamic IP source guard table of a port is displayed on this page. A dynamic table entry contains the following information: **Port**, **VLAN ID**, **IP Address**, and **MAC Address**. You can view the dynamic table by specifying the starting port, VLAN ID, or IP address. In addition, you can configure the number of records that can be displayed on a page. At most 99 records can be displayed on a page.



The preceding figure shows the configuration page of the static IP source guard table. The static IP source guard table is displayed on this page. A static table entry contains the following information: **Port**, **VLAN ID**, **IP Address**, and **IP Mask**. In this table, you can manually add communication rules of a single port, and restrict communication on the port by specifying parameters, such as the VLAN ID and IP address.

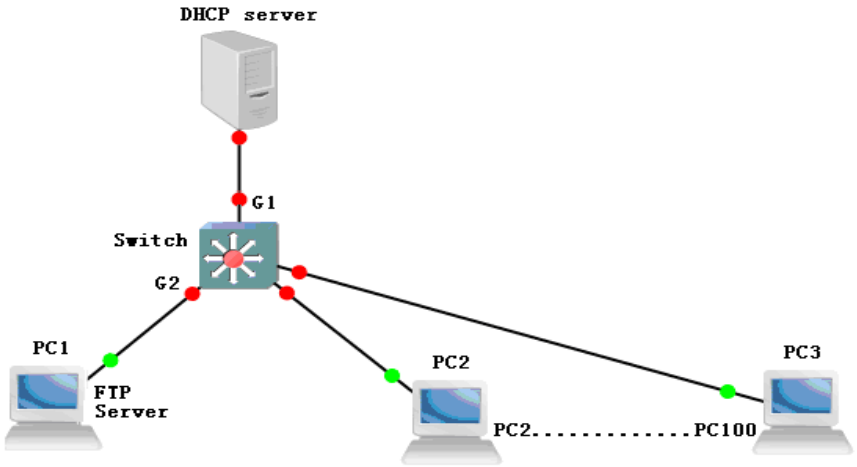
- **Add New Entry**: To manually add a static IP source guard entry, click **Add New Entry**, select a port, set the VLAN ID, IP address, and subnet mask, and click **Save**.



To delete a static IP source guard entry, click the **Delete** check box of the corresponding entry, and then click **Save**.

Tip: On the global IP source guard configuration page, you can click **Translate dynamic to static** to change an entry in the dynamic IP source guard table to a static entry.

Configuration example:



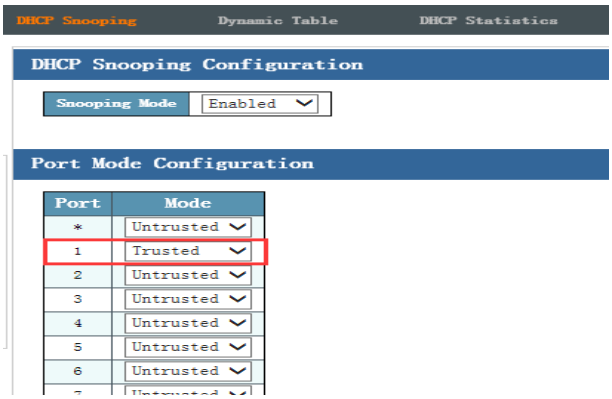
Scenario requirements:

(1) The switch can receive packets sent by the DHCP server only through the port G1. Other ports do not allow packets of the DHCP server to pass through. That is, accessed users are not allowed to configure a DHCP server privately.

(2) The downlink port of the switch, that is, the port connected to a terminal, must obtain an IP address from an authorized DHCP server before it can access the network normally. If the IP address is manually configured by the user or is obtained and then modified, the PC is not allowed to access the network.

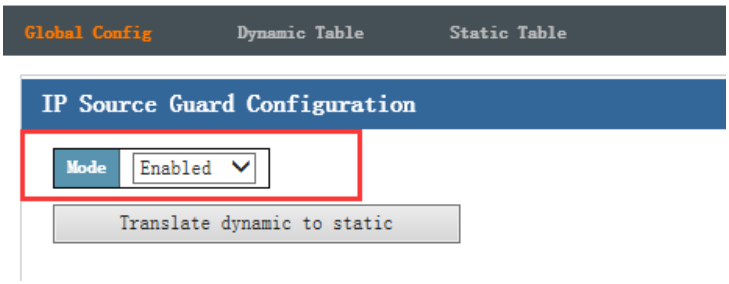
(3) The intranet FTP server connected to the port G2 uses the fixed IP address 192.168.222.94, which is not obtained from the DHCP server. The intranet devices need to communicate with this FTP server normally.

Step 1 To implement IP source guard, enable the DHCP snooping function, and set the mode of the port G1 connected to the DHCP server to **Trusted**, and the mode of other ports to **Untrusted**, as shown in the following figure.

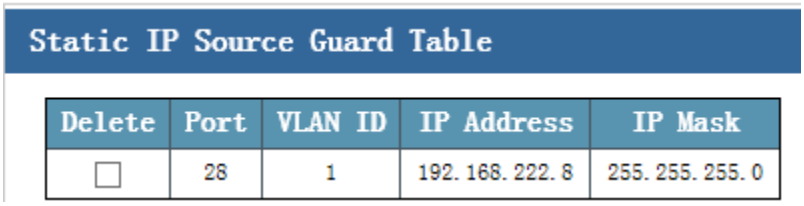


Step 2 Enable IP source guard globally. Add a static IP source guard entry respectively for the PC that is used to configure the switch and the intranet FTP server. (This entry is added to prevent the problem that only PCs that dynamically obtain IP addresses can normally access the switch and network after IP source guard is enabled on all the ports. After the static IP source guard entries are added, the configuration PC and intranet FTP server can access the switch and network normally.) The following figure shows the configuration results.

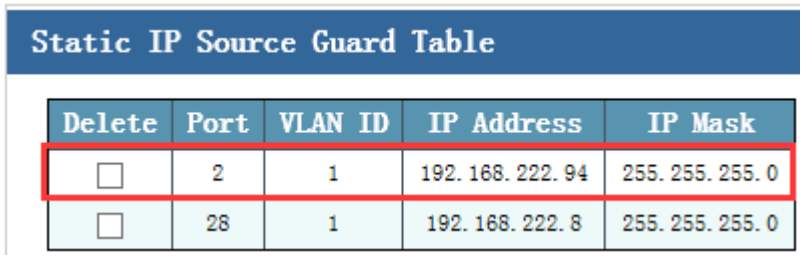
a. Enable IP source guard globally.



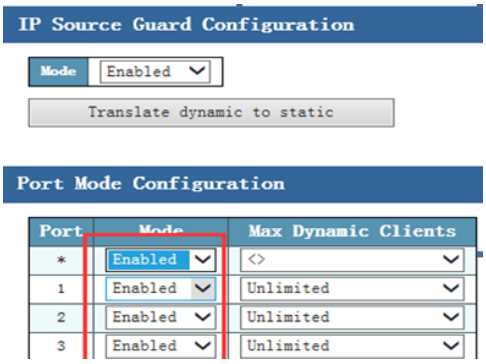
b. Add a static IP source guard entry for the PC that is used to configure the switch.



c. Add a static IP source guard entry for the intranet FTP server.



Step 3 Enable IP source guard for all the ports, and set the maximum number of dynamic clients to **Unlimited**.



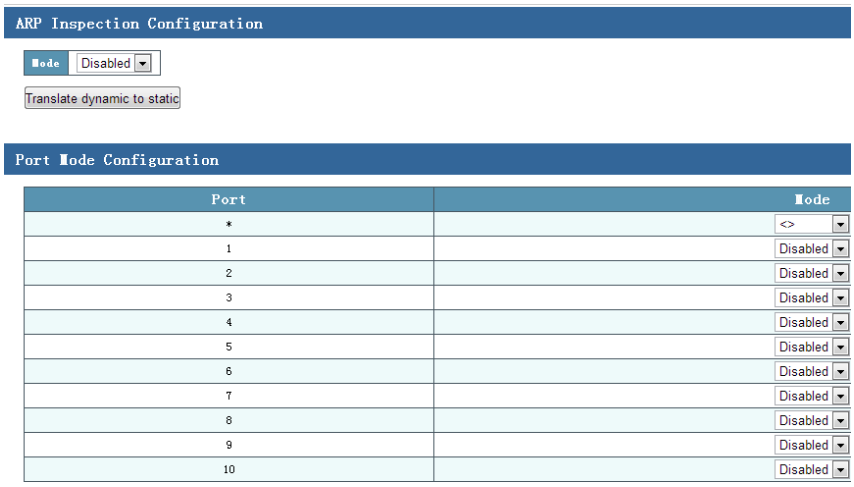
6.5 ARP Inspection

ARP is simple and easy to use, but attackers often take advantage of ARP to initiate attacks because ARP lacks of any security mechanism.

Attackers can send forged ARP packets in the place of other users and gateways to make ARP entries on the gateway or host incorrect, thus attacking the network. Attackers send a huge number of IP packets, the destination IP address of which cannot be translated, to a device. The device makes repeated attempts to translate the destination IP address, and consequently the CPU load is extremely high and the network traffic is extremely heavy. Attackers send a large number of ARP packets to the switch, increasing the CPU usage of the device. Currently, ARP attacks and APR virus have become a major threat to security of LANs. To avoid damages caused by various attacks, the switch provides the ARP inspection technology to prevent, detect, and eliminate the attacks.

After ARP inspection is enabled, related ports of the switch automatically checks whether APR packets come from correct ports and are not modified or spoofed by attackers. The switch can identify the correct ports based on the DHCP snooping binding table. If data received by the switch comes from incorrect ports, the switch automatically drops the packet, preventing attackers from attacking the network.

6.5.1 Port Mode Configuration



ARP Inspection Configuration

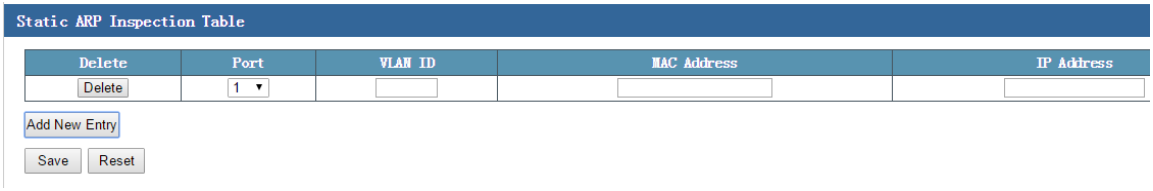
- **Mode**: Select **Disabled** to globally disable ARP inspection, and **Enabled** to globally enable ARP inspection.
- **Translate dynamic to static**: Click this button to change an entry in the dynamic ARP inspection table to a static entry in the static ARP inspection table.

Port Mode Configuration

- **Port**: Indicates the port number.

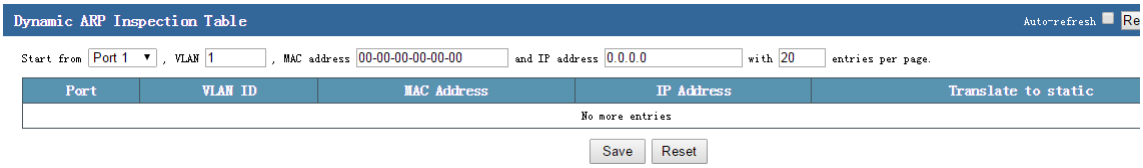
- Mode: Select **Disabled** to disable ARP inspection on a port, and **Enabled** to enable ARP inspection on a port.

6.5.2 Static ARP Inspection Table



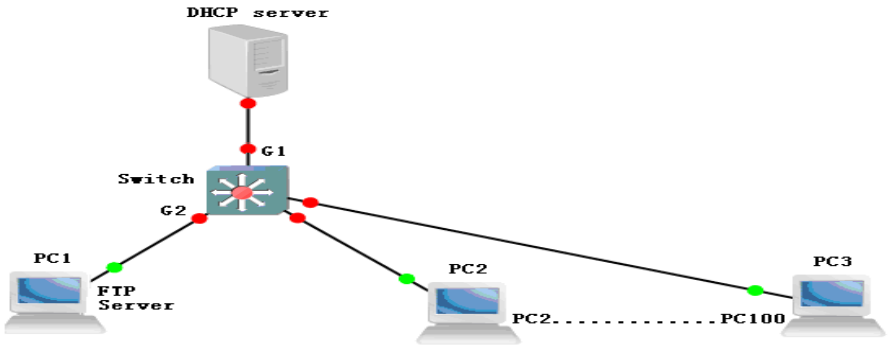
To add an entry to the static APR inspection table, click **Add New Entry**. Then, fill in the port number, VLAN ID, and MAC address and IP address of the device bound with the static ARP inspection table, and click **Save**. If a device (such as the intranet FTP server) uses a fixed IP address, you need to manually add a static ARP inspection entry to bind with the device. Otherwise, the network and the device cannot be successfully accessed when ARP inspection is enabled on a port. At most 1,000 static ARP inspection entries can be configured.

6.5.3 Dynamic ARP Inspection Table



On the page shown in the preceding figure, you can view the current dynamic ARP inspection entries, each of which contains the port number, VLAN ID, MAC address, and IP address. You can select the range of entries to be displayed by specifying the starting port number, starting VLAN number, MAC address, or IP address. At most 1,000 dynamic entries can be displayed.

Configuration example:

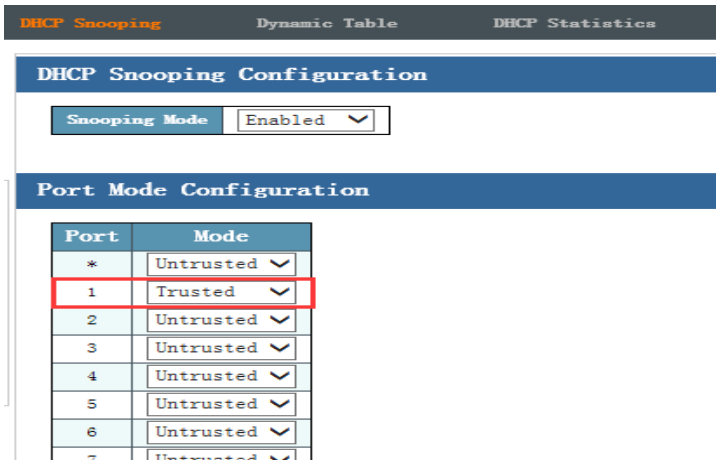


(1) The switch can receive packets sent by the DHCP server only through the port G1. Other ports do not allow packets of the DHCP server to pass through. That is, accessed users are not allowed to configure a DHCP server privately.

(2) ARP inspection is enabled on all the downlink ports of the switch, that is, the ports connected to terminals. Only the packets for which the static or dynamic ARP inspection entry has been added can be sent to or received by the network. It is prohibited to send packets that are inconsistent with the bound entries to the network.

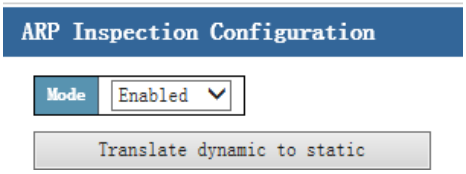
(3) The intranet FTP server connected to the port G2 uses the fixed IP address 192.168.222.94. A static ARP inspection entry is added to allow only this server to implement communication normally through G2. When other unauthorized IP devices are connected to G2, these devices cannot access network sources.

Step 1 To implement ARP inspection, enable the DHCP snooping function, and set the mode of the port G1 connected to the DHCP server to **Trusted**, and the mode of other ports to **Untrusted**, as shown in the following figure.

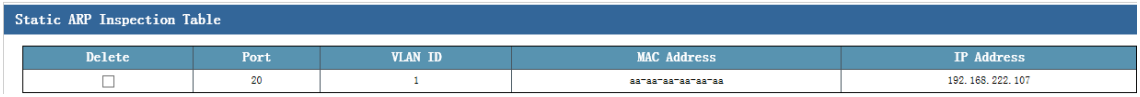


Step 2 Enable ARP inspection globally. Add a static ARP inspection entry respectively for the configuration PC and the intranet FTP server that are connected to the switch. (This entry is added to prevent the problem that only PCs that dynamically obtain IP addresses can normally access the switch and network after ARP inspection is enabled on all the ports. After the static ARP inspection entries are added, the configuration PC and intranet FTP server can access the switch and network normally.) The following figure shows the configuration results.

a. Enable ARP inspection globally.

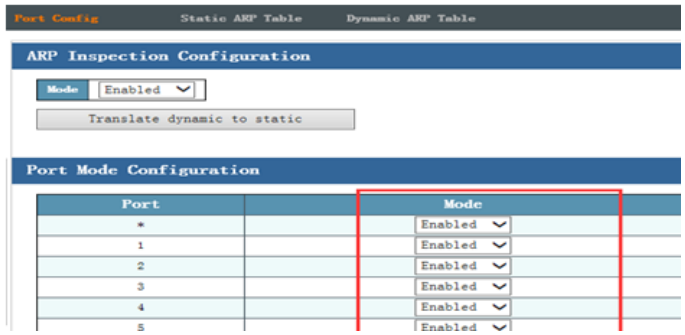


b. Add a static ARP inspection entry for the configuration PC.



c. Add a static ARP inspection entry for the intranet FTP server.

Step 3 Enable ARP inspection for all the ports.



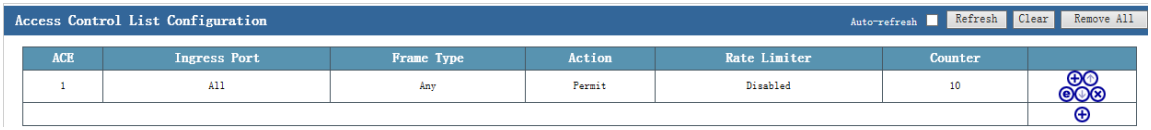
6.6 ACL Config

ACLs are used to filter packets based on the configured packet matching rules and processing operations. After an ACL is applied to a port, fields in each packet are analyzed. After matched packets are identified, these packets are processed according to the preset operations, such as permit, deny, rate limiting, redirection, or port shutdown.

The ACL configuration may be associated with port security (port ACL policy configuration) and bandwidth policies (port ACL bandwidth policies). Each ACE calls the ACL policy ID and bandwidth policy ID according to requirements.

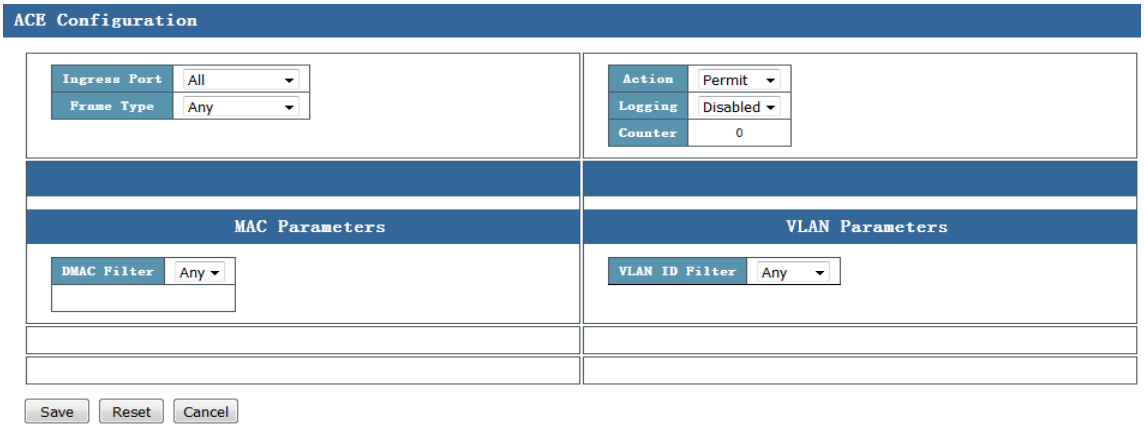
The preceding figure shows the ACL configuration page. Major parameters of ACEs are described as follows:

- **ACE**: Indicates the ACE ID. An ACL supports at most 512 ACEs. By default, the ACE ID starts from 1 and increases sequentially.
- **Ingress port**: Indicates the ingress port information of an ACE. Options include **ALL** and **Port Number**. The default value is **ALL**.
- **Frame Type**: Indicates the frame type of an ACE.
- **Action**: Indicates the forwarding action of an ACE. Options include **Permit** and **Deny**. If the value is **Permit**, frames matching the ACE will be forwarded and learned. If the value is **Deny**, frames matching the ACE will be dropped.
- **Rate Limiter**: Indicates the bandwidth limit policy ID of an ACE.
- **Counter**: Indicates the number of frames that match the ACE.
- **Edit**: Click the plus sign to display the page for adding an ACE.
- Icons on the ACL configuration page are described as follows:



- : Add an ACE in front of the current line.
- : Edit the current ACE.
- : Move the current ACE upward.
- : Move the current ACE downward.
- : Delete the current ACE.
- Click the plus sign at the bottom, and the ACE configuration page is displayed. After the configuration is saved, a new ACE is added.
- Buttons on the ACE configuration page are described as follows:

Click or . The following ACE configuration page is displayed, where you can configure the ingress port, frame type, ACE action, IP address, MAC address, and VLAN ID.

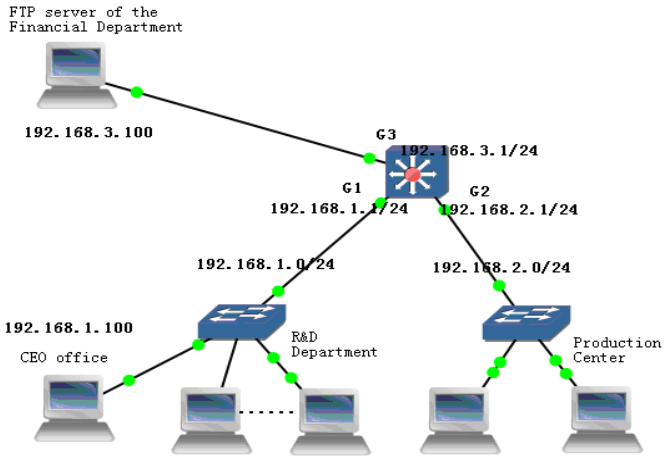


Note: You can configure **VLAN ID Filter** to define an ACL rule based on the VLAN ID, that is, whether to permit or deny packets of a specified VLAN ID.

Configuration example:

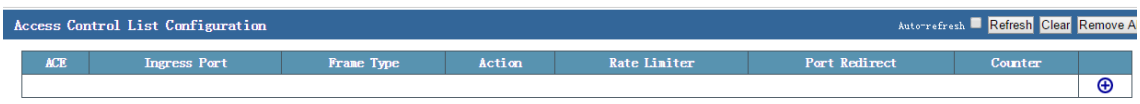
Scenario requirements:

1. The R&D Department and the Production Center cannot communicate with the server 192.168.3.100.
2. In the network segment of the R&D Department, the server 192.168.1.100 in the CEO office can access the FTP server 192.168.3.100 of the Financial Department.



Configure data as follows:

1. Click ⊕ to add an ACE.



2. Configure ACEs as follows to permit the packets sent between the CEO office and the FTP server of the Financial Department.

   1) Configure ACEs in the incoming direction of the port G1.

   2) Set **Frame Type** to **IPv4**.

   3) Set **IP Protocol Filter** to **TCP**, and **Dest. Port No.** to **20** and **21**.

   4) Set **SIP Address** to **192.168.1.100** (CEO office), and **DIP Address** to **192.168.3.100** (FTP server of the Financial Department).

   5) Set **Action** to **Permit**.

Figure 1 Permitting the traffic sent to port 20

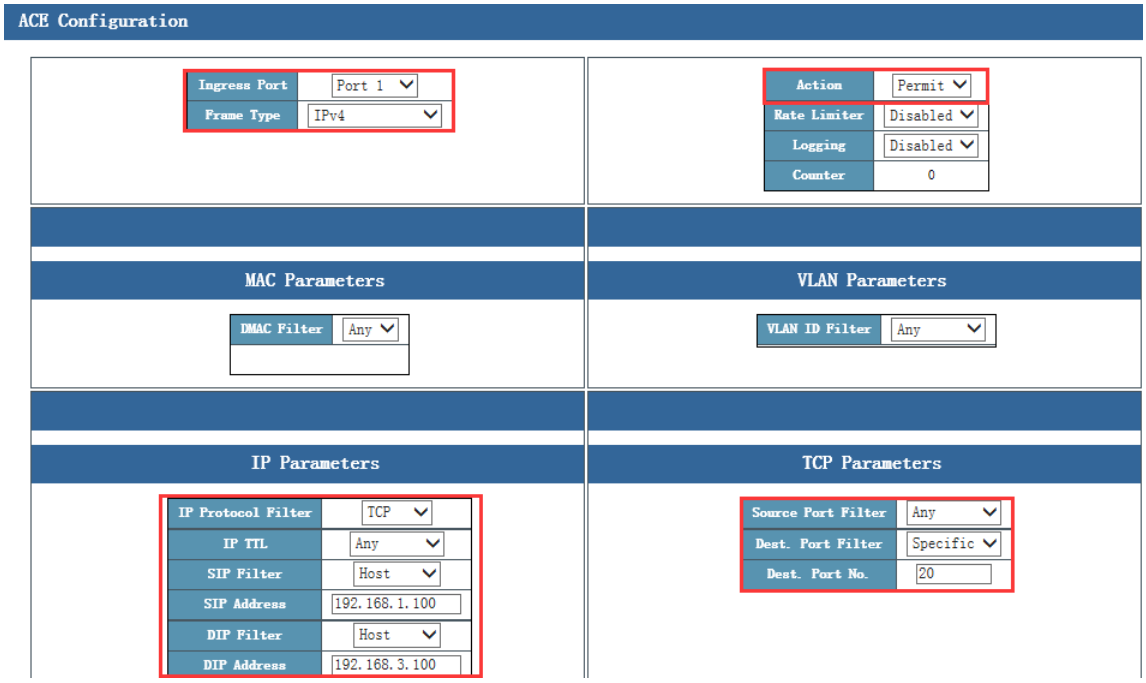
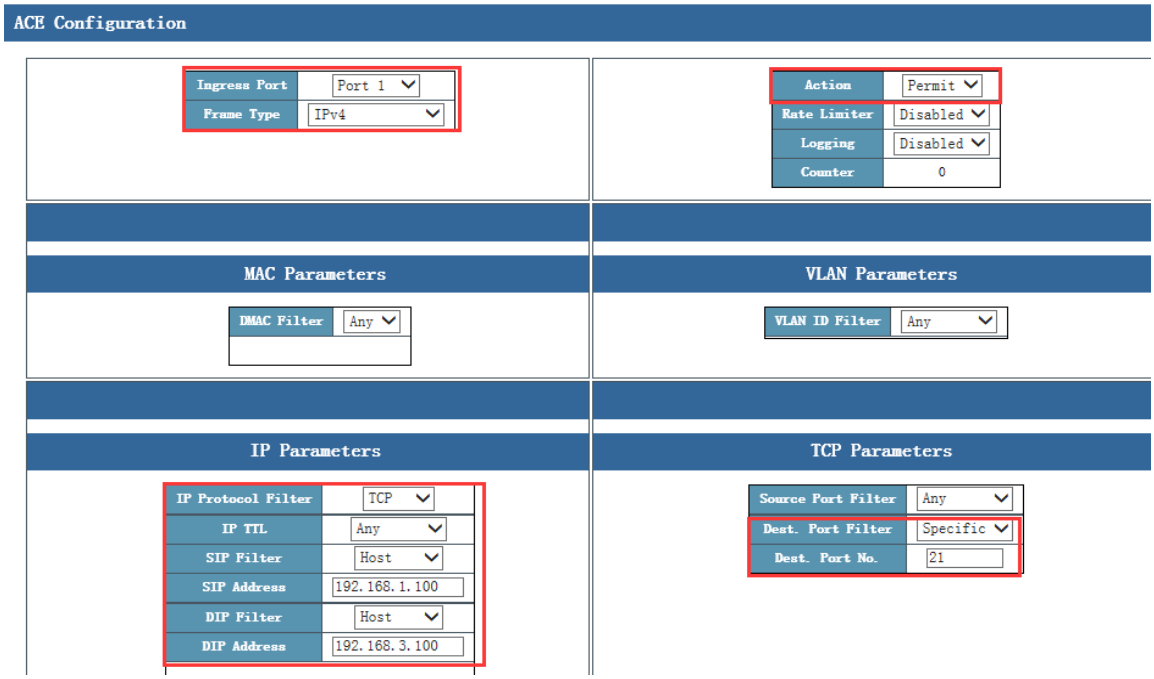
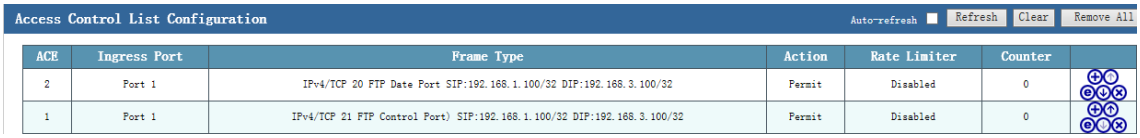


Figure 2 Permitting the traffic sent to port 21



After configuration is completed, ACEs are displayed as follows:



The FTP server access result is as follows (taking port 21 as an example):

3. Prohibit the R&D Department and the Production Center from accessing 192.168.3.100.

    1) Configure ACEs in the incoming direction of the port G1.

    2) Set **Frame Type** to **IPv4**.

    3) Set **IP Protocol Filter** to **Any**, **SIP Address** to the network segment **192.168.1.0/24**, and **DIP Address** to **192.168.3.100**.

    4) Set **Action** to **Deny**.

Figure 1 Prohibiting the R&D Department (except the CEO office) from accessing 192.168.3.100

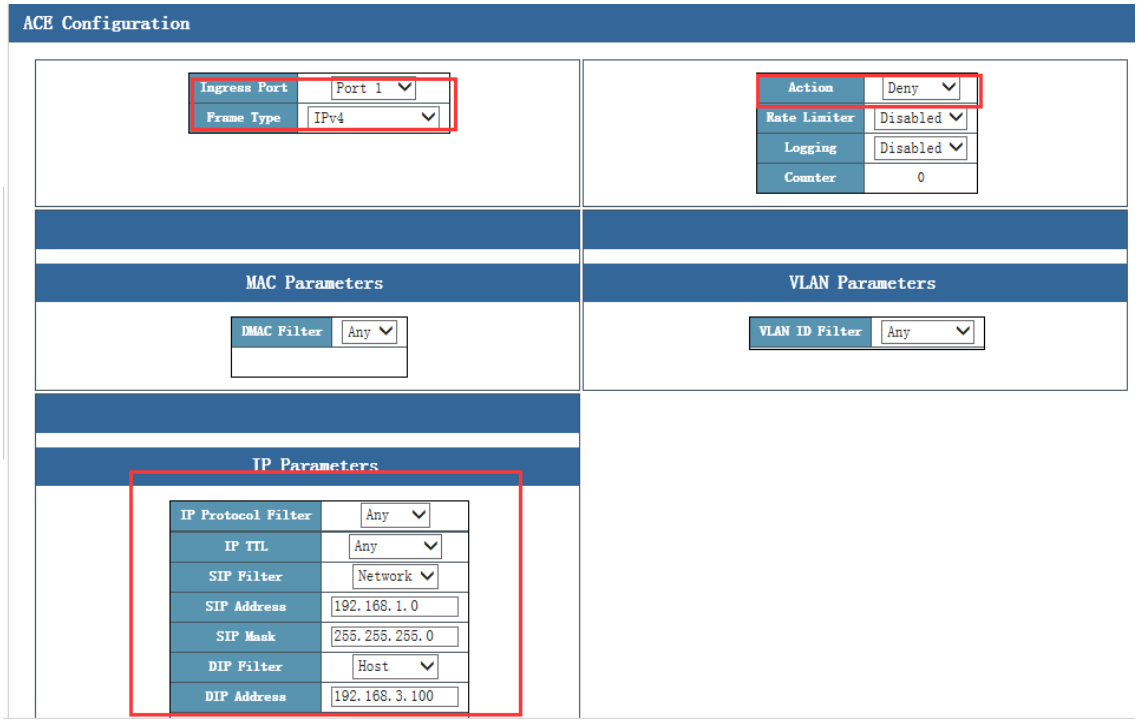


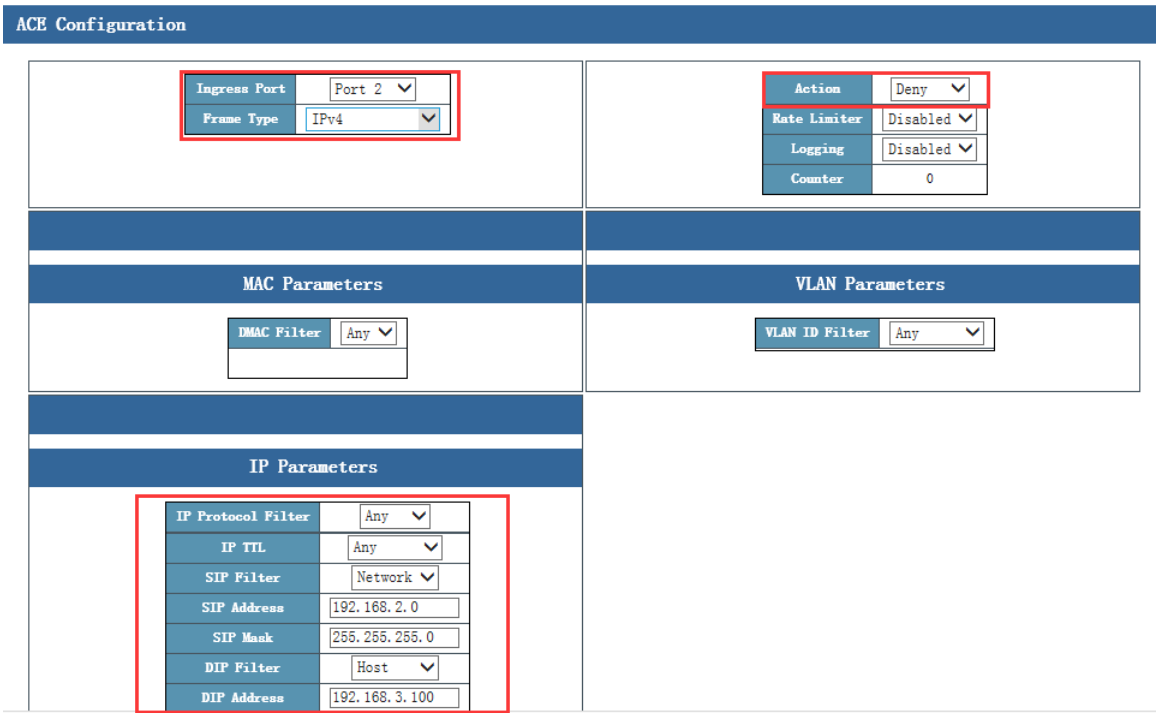
Figure 2 Prohibiting the Production Center from accessing 192.168.3.100

1) Configure the ACE in the incoming direction of the port G2.

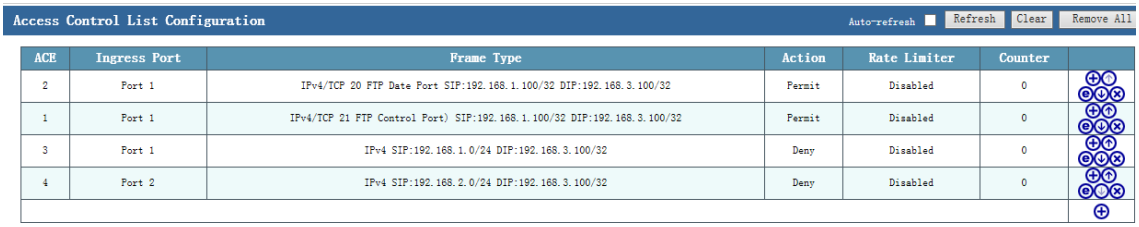
2) Set **Frame Type** to **IPv4**.

3) Set **IP Protocol Filter** to **Any**, **SIP Address** to the network segment **192.168.2.0/24**, and **DIP Address** to **192.168.3.100**.

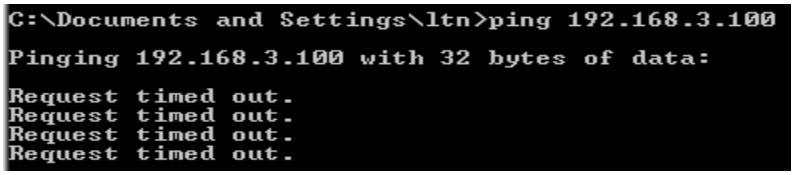
4) Set **Action** to **Deny**.



After configuration is completed, ACEs are displayed as follows:



The following figure shows the ping test result.



6.7 STP Config

STP is developed based on IEEE 802.1D, and is a protocol used to eliminate physical loops at the data link layer in the LAN. STP-enabled devices exchange information to detect loops on the network, and selectively block some ports to change a loop topology into a loop-free tree topology. This prevents continuous growing and infinite loop of packets on the loop network, and prevents occurrence of

problems such as degraded packet processing capability of devices caused by repeated receiving of the same packets.

Protocol packets used by STP are Bridge Protocol Data Units (BPDUs), which are also called configuration messages. A BPDU contains sufficient information to ensure that a device can complete the spanning tree computation process. STP transfers BPDUs between devices to determine the network topology.

Format and fields of the BPDU

To implement the STP function, switches must transfer BPDUs to exchange information. All STP-enabled switches will receive and process received packets. The packet contains all information that can be used for spanning tree computation. BPDU frame format and fields of a standard spanning tree:

On the STP port configuration page, you can configure the following parameters of an STP port:

2	1	1	1	8	4
Protocol Identifier	Version	Message Type	Flag	Root ID	Root Path Cost
Bridge ID	Port ID	Message Age	Max Age	Hello Time	Forward Delay
8	2	2	2	2	2

- Protocol identifier
- Version: Indicates the protocol version.
- Message type: Indicates the BPDU type.
- Flag: Indicates the flag bit.
- Root ID: Indicates the ID of the root bridge. It consists of a 2-byte priority and a 6-byte MAC address.
- Root path cost
- Bridge ID: Indicates the ID of the bridge that sends BPDUs. It consists of a 2-byte priority and a 6-byte MAC address.
- Port ID: Indicates the ID of the port that sends BPDUs.
- Message age: Indicates the life time of the BPDU.

- Maximum age: Indicates the aging time of the current BPDU, that is, the maximum time that the port stores the BPDU.
- Hello time: Indicates the interval at which the root bridge sends BPDUs.
- Forward delay: Indicates the time that the switch stays at the listening and learning state before sending packets after the topology changes.

Basic Concepts of STP

Bridge ID: The bridge ID is the combination of a configurable root priority and its MAC address. A smaller bridge ID indicates a higher root priority, which increases the possibility that the bridge becomes a root bridge.

Root bridge: A switch with the smallest bridge ID is the root bridge. You need to configure the switch with the best performance among all switches in the loop as the root bridge, so as to provide the best network performance and reliability.

Designated bridge: In a network segment, a bridge with the lowest path cost from this network segment to the root bridge is a designated bridge. Packets will be forwarded to this network segment If all the switches have the same root path cost, the switch with the smallest root ID is elected as the designated bridge.

Root path cost: It refers to the sum of all the path costs between two bridges. The root path cost of the root bridge is 0.

Bridge priority: It is a configurable parameter. Its value ranges from 0 t o 61,440. A smaller value indicates a higher priority. A switch with a higher bridge priority is more likely to become the root bridge.

Root port: On a switch that is not a root bridge, a root port is the port that is closest to the root bridge. The root port communicates with the root bridge. The path cost from this port to the root bridge is the lowest. If multiple ports has the same root path cost, the port with the highest port priority becomes the root port.

Designated port: It is the port on the designated bridge that forwards data to the local switch.

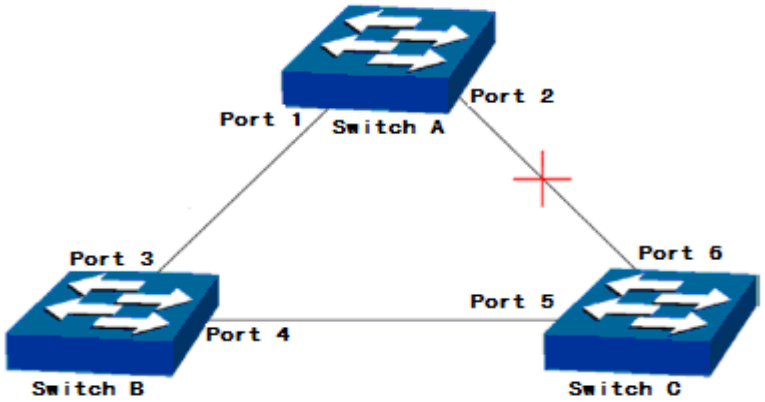
Port priority: The value ranges from 0 to 240, and must be an integer multiple of 16. A smaller port priority value indicates a higher port priority. The port with a higher port priority is more likely to become the root port.

Path cost: STP uses the path cost as a reference to select links. By computing path costs, STP selects more robust links and blocks remaining links to shape the network into a loop-free tree topology.

The following figure illustrates the basic concepts of STP. Switches A, B, and C are connected with each other. After STP computation, switch A is elected as the root bridge, and the link between port 2 and port 6 is blocked.

Bridge: Switch A is the root bridge of the entire network, and switch B is the designated bridge of switch C.

Port: Port 3 is the root port of switch B, and port 5 is the root port of switch C. Port 1 is the designated port of switch A, and port 4 is the designated port of switch B. Port 6 is a blocked port of switch C.



STP timers

- Hello Time

  The value ranges from 1s to 10s. The hello time refers to the interval that the root bridge sends a BPDU to all other switches. It is used by switches to check whether any link is faulty.

- Max. Age

  The value ranges from 6s to 40s. If a switch does not receive the BPDU sent by the root bridge after **Max. Age** expires, the switch sends a BPDU to all other switches to re-compute the spanning tree.

- Forward Delay

  The value ranges from 4s to 30s. The forward delay refers to the time required for port state transition on a switch.

When the spanning tree is re-computed due to a network fault, the structure of the spanning tree changes accordingly. The new configuration message obtained through re-computation cannot be immediately spread on the entire network. If the port status transits immediately, a temporary loop may be formed. Therefore, STP adopts a state transition mechanism. The new root port and designated port can start data forwarding after twice of the forward delay expires. This delay ensures that the new configuration message has been spread all over the network.

Principle for comparing the BPDU priorities in STP mode

Assume that there are two BPDUs, including X and Y.

- If the root bridge ID of X is smaller than that of Y, the priority of X is higher than that of Y.
- If the root bridge IDs of X and Y are the same, but the root path cost of X is smaller than that of Y, the priority of X is higher than that of Y.
- If the root bridge IDs and root path costs of X and Y are the same, but the bridge ID of X is smaller than that of Y, the priority of X is higher than that of Y.
- If the root bridge IDs, root path costs, and bridge IDs of X and Y are the same, but the port ID of X is smaller than that of Y, the priority of X is higher than that of Y.

STP computation process

Initial state: Upon initialization, each switch will generate a BPDU, in which the root bridge is the switch itself, the root path cost is 0, the designated bridge ID is the ID of the switch itself, and the designated port is a local port.

Selection of the optimum BPDU: Each switch sends its own BPDU to other switches, and meanwhile receives BPDUs sent from other switches. The following table describes the comparison process:

Step	Description
1	When the priority of the BPDU received by a port is lower than that of the BPDU sent by the port, the switch drops the received BPDU and retains the BPDU of the port. Otherwise, the switch replaces the BPDU of the port with the received BPDU.
2	The switch compares BPDUs of all the ports, and selects the optimum BPDU as the BPDU of the switch.

Selection of the root bridge: By exchanging the configuration messages, switches compare the root bridge IDs. The switch with the smallest root bridge ID is elected as the root bridge of the network.

Selection of the root port and designated port: The following table describes how the root port and designated port are elected.

Step	Description
1	A switch that is not a root bridge designates the port that receives the optimum BPDU as the root port.
2	Based on the BPDU and path cost of the root port, the switch computes a BPDU for other ports as follows: ● Replace the root bridge ID of the switch with the root bridge ID of the root port. ● Replace the root path cost of the port with the root path cost of the root port plus the path cost from the local port to the root port. ● Replace the designated bridge ID with the ID of the switch itself. ● Replace the designated port ID with the ID of the local port.
3	The switch compares the computed BPDU with the BPDU of the port whose port role must be determined, and takes actions according to the comparison result: ● If the priority of the computed BPDU is higher, the switch selects the port as the designated port, replaces the BPDU of the port with the computed BPDU, and periodically sends the BPDU to other switches. ● If the priority of the BPDU of the port is higher, the switch does not update the BPDU of the port but blocks the port. This port no longer forwards data. It only receives but does not send the configuration message.

Note:

If the topology is stable, only the root port and designated port forward data. Other ports are in blocked state, and only receive BPDUs but not forward data.

Basic Concepts of RSTP

Rapid Spanning Tree Protocol (RSTP) is an optimized STP protocol. It significantly reduces the delay before the port enters the forwarding state, and consequently shortens the time required by the network to achieve a stable topology. RSTP implements fast port state transition when the following conditions are met:

Fast port state transition of the root port: The old root port on the device has stopped forwarding data, and the upstream designated port has started to forward data.

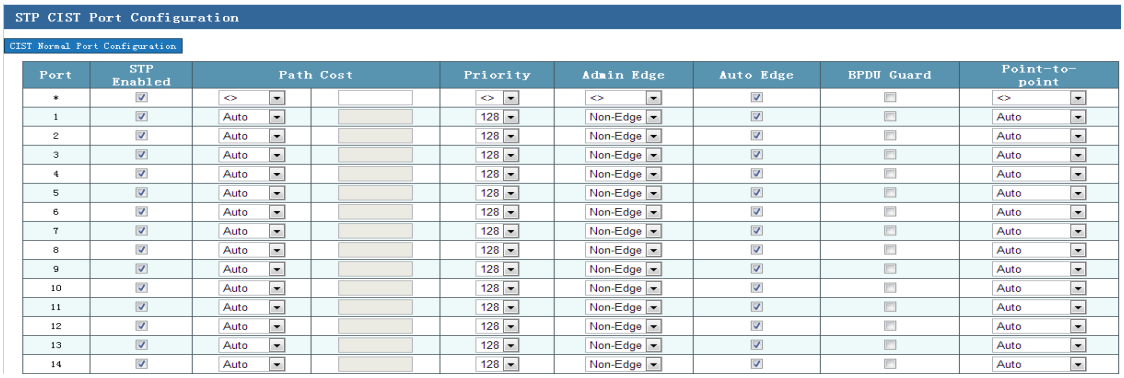
Fast port state transition of the designated port: The designated port is an edge port, or is connected to a point-to-point link.

If the designated port is an edge port, the designated port can directly transit to the forwarding state. If the designated port is connected to a point-to-point link, the switch can perform a handshake with the downstream device, and the port transits to the forwarding state immediately after a response is received from the downstream device.

Edge port: It refers to a port that is directly connected to a terminal instead of another switch.

Point-to-point link: It refers to a direct link between two switches.

The STP module is used to configure the STP function of the switch. It consists of two parts: port configuration and root bridge configuration, as shown in the following figure.



On the STP port configuration page, you can view the CIST port configuration and normal port configuration, including:

- **Port**: Indicates the port number of the switch.
- **STP Enabled**: If this check box is selected, STP is enabled on the port; otherwise, STP is disabled.
- **Path Cost**: STP computes the path costs to select robust links and block remaining links to shape the network into a loop-free tree topology. The option **Auto** indicates auto negotiation, and **Specific** indicates manual configuration. The default value is **Auto**.
- **Priority**: When the priority of a port changes, STP re-computes the role of the port and performs state transition. The priority value of a port can only be an integer multiple of 16. The value ranges from **0** to **240**. The default value is **128**.

- **BPDU Guard**: The BPDU guard function allows an edge port to enter the err-disable state when receiving a BPDU, thus preventing bridge loops. The BPDU filter can prevent the switch from sending a BPDU to the host through an edge port. By default, BPDU guard is disabled.

- **Point-to-point**: Indicates the type of the link connected to a port. **Force true** indicates the point-to-point link type. If a port runs in full duplex mode, the link is a point-to-point link. **Force false** indicates the shared link type. If a port runs in half duplex mode, the link is a shared link. **Auto** indicates that the port automatically sets up a link. The default value is **Auto**. The link between switches is generally a point-to-point link.

6.7.1 Root Bridge Configuration

On the STP bridge configuration page, you can configure root bridge parameters shown in the following figure.

On the STP bridge configuration page, you can view basic and advanced settings related to the STP root bridge.

Basic Settings

- **Protocol Version**: Three versions are available, including **MSTP**, **RSTP**, and **STP**.

- **Bridge Priority**: The bridge priority determines whether the local device can be elected as the root of the spanning tree. The bridge priority value ranges from 0 to 61,440. The default value is 32,768.

- **Forward Delay**: Indicates the delay of state transition. The value ranges from 4s to 30s. The default value is 15s.

- **Max. Age**: It is used to determine whether the storage time of the configuration message on the switch expires. The value ranges from 6s to 40s. The default value is 20s.

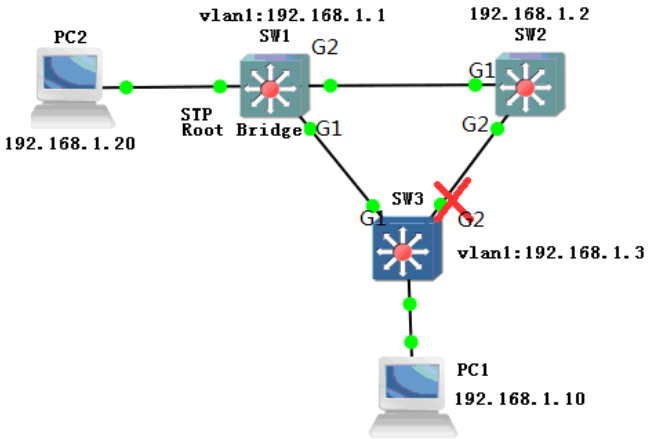
- **Maximum Hop Count**: Indicates the transfer range of a BPDU. The value ranges from 6 to 40. The default value is 20.

Advanced Settings

- **Edge Port BPDU Filtering**: The BPDU filter can prevent the switch from sending a BPDU to the host through an edge port. This function is disabled by default.
- **Edge Port BPDU Guard**: The BPDU guard function allows an edge port to enter the err-disable state when receiving a BPDU, thus preventing bridge loops.
- **Port Error Recovery**: The recovery function is enabled for a port in err-disable state. If the check box is selected, the function is enabled. By default, the function is disabled.
- **Port Error Recovery Timeout**: The port is restarted after the timeout time expires.

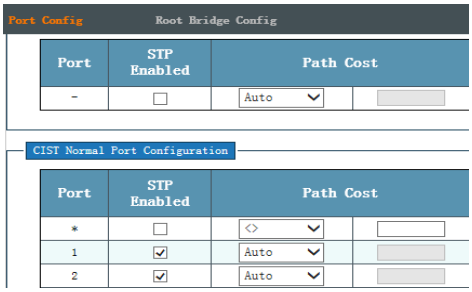
Configuration example:

1. Run STP throughout the network, and elect SW 1 as the root bridge and SW 2 as the backup root bridge.
2. When the direction link between a downstream client and the root bridge is interrupted, the traffic can be quickly switched from the SW 1 to SW 2 without affecting the network communication.

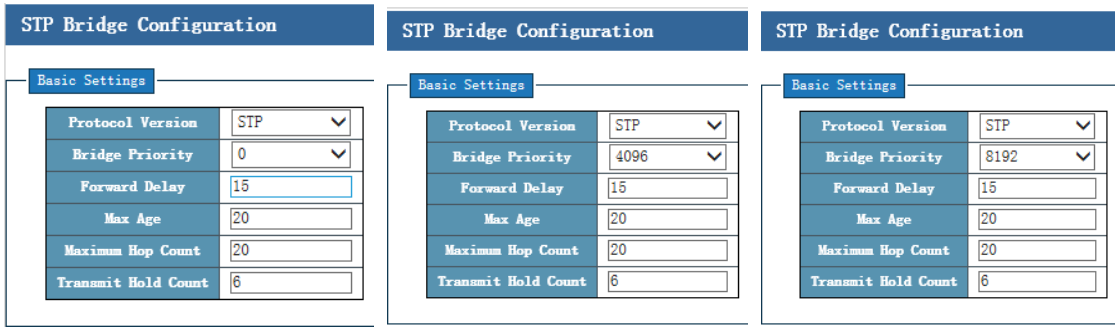


Configure data as follows:

1. Enable STP on ports G1 and G2 of SW 1, SW 2, and SW 3.



2. Set the bridge priority to 0 (smallest) for SW 1, 4,096 for SW 2, and 8,192 for SW 3. Retain default settings of other parameters. On a LAN, the switch with the smallest bridge ID is the root bridge, and the switch with the second smallest bridge ID is the backup root bridge.



3. All the ports on the root bridge are designated ports. The switch elects the root port based on the following requirements:

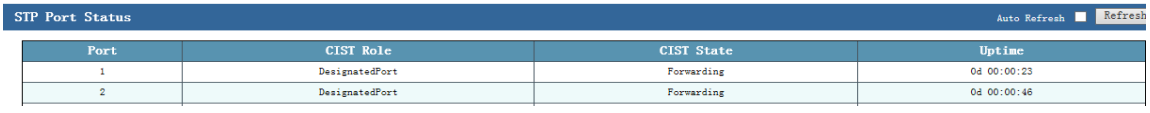
   a. The root path cost is the lowest. (The root path cost is the sum of costs of all links on the path between two bridges, that is, the sum of the path costs of all links between a bridge and the root bridge.)

   b. The bridge ID is the smallest in the sending direction.

   c. The port ID is the smallest. (The port ID consists of the priority and port number, and ensures the uniqueness of the root port.)

   In this scenario, G1 is elected respectively as the root port of SW 2 and SW 3 based on the root path costs.

SW 1:



SW2:

STP Port Status — Auto Refresh ☐ Refresh

Port	CIST Role	CIST State	Uptime
1	RootPort	Forwarding	0d 00:02:04

SW3:

STP Port Status — Auto Refresh ☐ Refresh

Port	CIST Role	CIST State	Uptime
1	RootPort	Forwarding	0d 00:02:04

4. After the root port of each switch is elected, the designated port is elected between G2 ports of SW 2 and SW 3 based on the following requirements:

   a. The root path cost is the lowest.

   b. The bridge ID of the switch is the smallest.

   c. The port number is the smallest.

   As the bridge ID of SW 2 is the smallest, G2 of SW 2 is elected as the designated port.

STP Port Status — Auto Refresh ☐ Refresh

Port	CIST Role	CIST State	Uptime
1	RootPort	Forwarding	0d 00:02:04
2	DesignatedPort	Forwarding	0d 00:10:50

5. After the root bridge, root port, and designated port are elected, the remaining port (that is, G2 of SW 3) is blocked.

2	BackupPort	Discarding	0d 00:00:09

6. Check whether PC 1 and PC 2 can ping each other. The following figures show the ping results between PC 1 and PC 2.

```
C:\Documents and Settings\ltn>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
```

```
C:\Documents and Settings\ltn>ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:

Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
```

7. Switch the links by disconnecting the port G1 on SW 1. Check whether PC 1 and PC 2 can ping each other.

```
C:\Documents and Settings\ltn>ping 192.168.1.10

Pinging 192.168.1.10 with 32 bytes of data:

Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
Reply from 192.168.1.10: bytes=32 time<1ms TTL=128
```

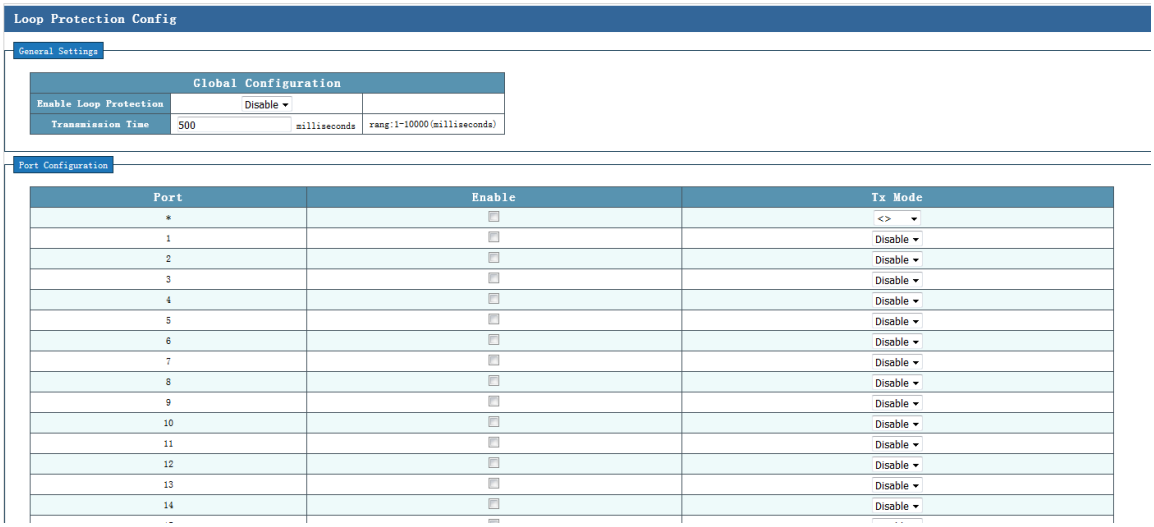
```
C:\Documents and Settings\ltn>ping 192.168.1.20

Pinging 192.168.1.20 with 32 bytes of data:

Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
Reply from 192.168.1.20: bytes=32 time<1ms TTL=128
```

6.8 Loop Protection

Loop protection is similar to STP, but it lacks an IEEE standard and is a private protocol. Loop protection is easy to configure and use. It is suitable for a simple ring topology and common network services, and has obvious advantages in line backup.



The loop protection configuration page consists of three parts: global configuration, port enable, and Tx mode.

- **Global configuration-Enable Loop Protection**: The default value is **Disable**. **Disable** indicates that loop protection is disabled globally; and **Enable** indicates that loop protection is enabled globally.
- **Global configuration-Transmission Time**: The default value is 300ms.
- **Port**: Indicates the port number.
- **Enable**: If this check box is selected, loop protection is enabled on a port.
- **Tx mode**: The default value is **Disable**. **Disable** indicates that the Tx mode is disabled; and **Enable** indicates that the Tx mode is enabled. After the Tx mode is enabled, the port can periodically send loop detection packets to test whether any loop exists on the network.

Tip: STP, ERPS, and loop protection cannot be enabled at the same time. Global and port-based loop protection must be enabled on all ports that form the ring, and the Tx mode must be enabled on at least one port.

Configuration example:

On SW 1 and SW 2, enable loop protection on ports 25 and 26. On SW 1, enable the Tx mode on port 25, and disable the Tx mode on port 26. On SW 2, disable the Tx mode on ports 25 and 26.

Configure data as follows:

(1) Check the configurations on SW 1 and SW 2, and confirm that STP and ERPS are disabled on ports 25 and 26.

(2) On the loop protection configuration page of SW 1, enable loop protection globally, enable loop protection on ports 25 and 26, enable the Tx mode on port 25, disable the Tx mode on port 26, and save the configurations.

(3) On the loop protection configuration page of SW 2, enable loop protection globally, enable loop protection on ports 25 and -26, disable the Tx mode on ports 25 and 26, and save the configurations.

(4) After the configuration is completed, connect ports 25 and 26 on the two switches to form a ring network. On the System Info–Loop Protection Status page, you can check the status of ports that form the ring network.

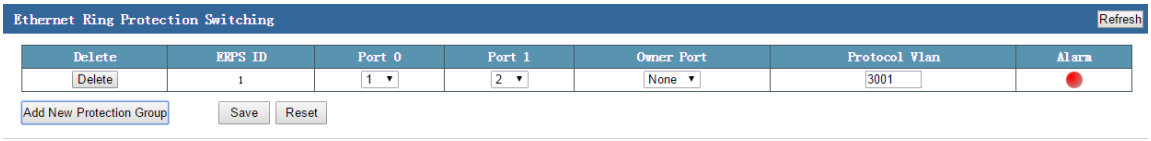
6.9 ERPS Config

Ethernet Ring Protection Switching (ERPS) is an Ethernet multi-ring protection technology defined in ITU-TG.8032. Aiming to improve network performance and security, ERPS is an Ethernet ring technology that becomes an important redundancy protection measure on the L2 network.

On the L2 network, STP is often used to ensure network reliability, and the loop protection protocol may also be used. STP is a standard ring protection protocol developed by IEEE, and has been widely used. In practice, application of STP is restricted by the network size, and the convergence time is affected by the network topology. The convergence time of STP is generally several seconds, or longer if the network diameter is large. The use of RSTP/MSTP can reduce the convergence time to several milliseconds, but still cannot meet the requirements of services (such as 3G and NGN voice services) that require a high Quality of Service (QoS). ERPS emerges to further reduce the convergence time and eliminate the impact caused by the network size.

ERPS is a link layer protocol dedicated for the Ethernet ring. It can prevent broadcast storms caused by data loops in an Ethernet ring. When a link on the Ethernet ring is disconnected, the backup link can be quickly enabled to recover communication between nodes on the ring network. Compared with STP, ERPS features a fast topology convergence speed (less than 20 ms) and the convergence time that is independent of the number of nodes on the ring network. Loop protection is similar to STP and ERPS, but it lacks an IEEE standard and is a private protocol. Loop protection is easy to configure and use. It

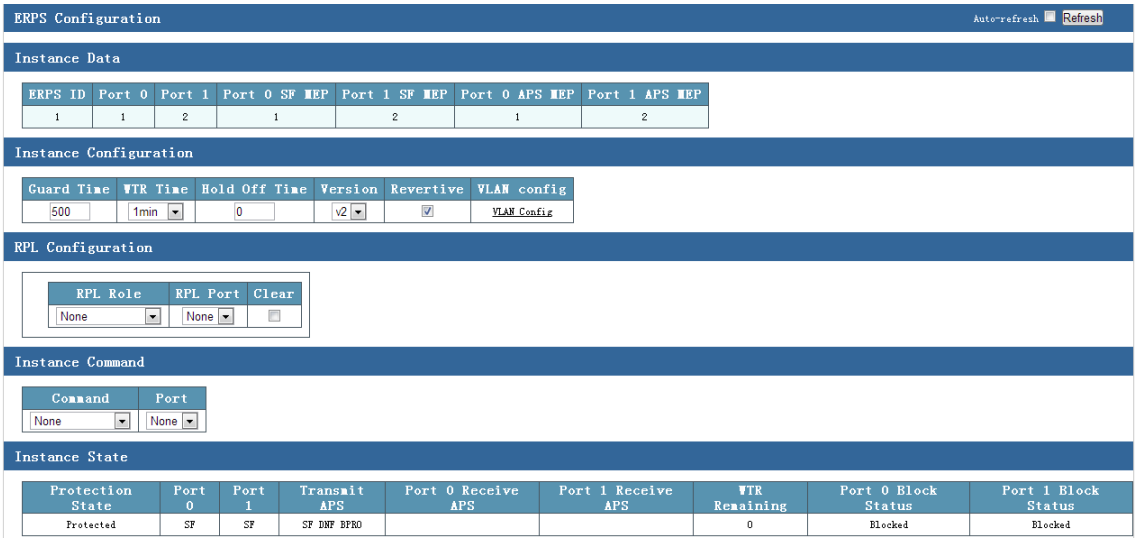
is suitable for a simple ring topology and common network services, and has obvious advantages in line backup.



On the ERPS configuration page, you can configure ERPS groups.

- **ERPS ID**: Indicates the ID of an ERPS domain. The ID of the first ERPS group added is 1, the ID of the second ERPS group added is 2, and so on.
- **Port 0**: Indicates the first port in the ring. It can be set to any port.
- **Port 1**: Indicates the second port in the ring. It can be set to any port, but cannot be the same as **Port 0**.
- **Owner port**: The default value is **None**, indicating that no owner port is configured. Options include **None**, **Port 0**, and **Port 1**. You can select either **Port 0** or **Port 1** as the owner port. There can be only one owner port in the ring, and the corresponding port will control the forwarding state.
- **Protocol VLAN**: Indicates that ERPS packets are transmitted in VLAN 3001 by default when ERPS is enabled. ERPS takes effect only when ports in the ring do not belong to VLAN 3001. ERPS groups in a ring must belong to the same protocol VLAN. The protocol VLAN of the first ERPS group added is 3001 by default. The protocol VLAN ID ranges from 1 to 4,095.
- **Alarm**: Indicates the ERPS state, which may be red or green. Green indicates that the ring is in normal state, and red indicates that the ring is in abnormal state.

You can click **ERPS ID** to add and view the detailed configuration.



ERPS parameters:

- **ERPS ID**: Indicates the ID of an ERPS domain. The ID of the first ERPS group added is 1, the ID of the second ERPS group added is 2, and so on.
- **Port 0**: Indicates the first port in the ring. It can be set to any port.
- **Port 1**: Indicates the second port that forms the ring. It can be set to any port, but cannot be the same as **Port 0**.
- **Port 0 SF MEP**: Indicates that maintenance endpoint (MEP) checking is enabled on port 1 in the ring. When a link disconnection is detected, a local signal failure (SF) message is sent to the ERP control unit of the node.
- **Port 2 SF MEP**: Indicates that MEP checking is enabled on port 2 in the ring. When a link disconnection is detected, a local SF message is sent to the ERP control unit of the node.
- **Port 0 APS MEP**: When ERP of port 1 in the ring receives the local SF message, the ERP control unit sends an Ring Automatic Protection Switching (R-APS) SF message to ports in the ring through a private VLAN to notify the remote RPL-OWNER node, and enables all the nodes to update the FDB table. The first three frames of the signal are sent at the interval of 3.33ms to implement fast switching. Later, during the period that the link fault persists, the R-APS is sent at the interval of 5s.
- **Port 1 APS MEP**: When ERP of port 2 in the ring receives the local SF message, the ERP control unit sends an R-APS SF message to ports in the ring through a private VLAN to notify the remote RPL-OWNER node, and enables all the nodes to update the FDB table. The first three frames of

the signal are sent at the interval of 3.33ms to implement fast switching. Later, during the period that the link fault persists, the R-APS is sent at the interval of 5s.

- **Ring Type**: Indicates the ring type of the current ERPS. Ring types include the master ring and sub-ring.

ERPS configuration:

- **Guard Time**: When a link is recovered from a failure, the neighbor node detects a failure recovery, starts the guard timer, and periodically sends the R-APS (NR) message to indicate that there is no local fault request. But the port connected to the faulty link is still in blocked state.
- **WTR Time**: When the ring protection link (RPL) node receives the first R-APS (NR) message, it starts the WTR timer. When the WTR timer expires, the RPL node re-blocks the RPL port, sends the R-APS (NR RB) message, and then updates the FDB table. The WTR timer prevents flapping of the blocking point that occurs because the RPL owner immediately blocks the RPL owner port after receiving the R-APS (NR) message.
- **Hold Off Time**: For the L2 network that runs ERPS, the requirements for the protection switching sequence may be different. For example, in a multi-layer service application, when the server is faulty, users may require that the server can recover from the fault in a period of time, within which the clients cannot perceive the fault, that is, protection switching is not triggered immediately. To meet this requirement, an appropriate hold off timer can be configured. When a fault occurs, the fault is not immediately reported to ERPS. The fault is reported only if the fault persists when the hold off timer expires.
- **Version**: Indicates the current version of ERPS. The default version is V2.
- **Revertive**: The link is switched to the stable state that is initially negotiated when a failure recovery is detected. If the check box is not selected, link status switching is not performed after the recovery is detected. The blocked link is still the original faulty link, and is not switched back to the RPL.
- **VLAN config**: Indicates the VLAN where ERPS is currently effective. The default value is **VLAN 1**.

RPL Configuration:

- **RPL Role**: Indicates the role of a port in the ring. Three role types are available: RPL owner port, RPL neighbor port, and none port (common port). The RPL neighbor port is supported only by ERPSv2, but not by ERPSv1.

- None port: In an ERPS ring, all ports except the RPL owner port and RPL neighbor ports are none ports. A none port monitors the status of the ERPS link directly connected to the port, and notifies other devices of the port status changes in time.
- RPL owner port: An ERPS ring has only one RPL owner port. The RPL owner port is specified by users. You can prevent loops in an ERPS ring by blocking the RPL owner port so that the port cannot forward traffic. When the device where the RPL owner port is located receives a fault packet and learns that another node or link is faulty in the ERPS ring, the device automatically unblocks the RPL owner port so that the port can send and receive traffic again. This ensures that traffic is not interrupted. The link where the RPL owner port is located is the RPL.
- RPL neighbor port: It refers to the port that is directly connected to the RPL owner port. Normally, both the RPL owner port and the RPL neighbor port are blocked to prevent loops. When the ERPS ring encounters a fault, both the RPL owner port and the RPL neighbor port are unblocked. Introduction of the RPL neighbor port can reduce the number of times that the device where the RPL owner port is located updates the FDB entries.

- **RPL Port**: Indicates the port that takes the RPL port role.
- **Clear**: To modify a port for which a port role is configured, you must first clear the original configuration, and configure the port again.

ERPS command:

- Command: Indicates the ring port configuration commands, including:
  - **Manual Switch**: Allows you to manually block a ring port. The RPL owner port and the RPL neighbor port in the ERPS ring will be unblocked to receive and send traffic. Compared with forced switch, manual switch must be implemented when the ERPS ring is in Idle or Pending state.
  - **Forced Switch**: Allows you to forcibly block a port in an ERPS ring. The RPL owner port and the RPL neighbor port in the ERPS ring will be unblocked to receive and send traffic.
  - **Clear**: Allows you to clear the manual switch or forced switch operation that is previously configured.
- **Port**: Specifies the ring port to which the configuration is issued.

ERPS state:

- **Protection State**: Indicates the state of the ERPS ring.
  - **Pending**: selected state
  - **Idle**: stable state

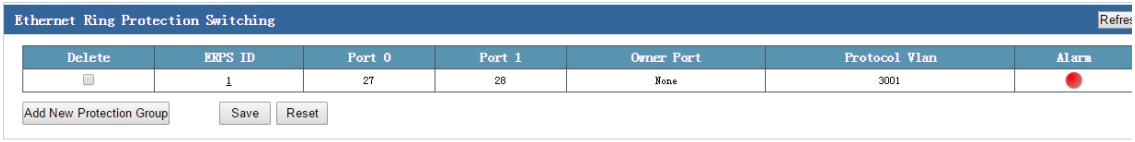
- **Force**: Forced switch is configured for a ring port.
- **Manual**: Manual switch is configured for a ring port.
- **Protect**: A ring is not formed yet.

- **Port 0/Port 1**: Indicates the state of a ring port.
  - **OK**: normal connection state
  - **SF**: faulty state (connection interrupted)
- **Transmit APS**: Indicates the type of the APS packet sent by the ERP node.
- **Port 0 receive APS**: Indicates the type of the APS received by port 1 in the ring, and the MAC address of the packet sending end.
- **Port 1 receive APS**: Indicates the type of the APS received by port 2 in the ring, and the MAC address of the packet sending end.
- **WTR Remaining**: Indicates the countdown time of the WTR timer.
- **Port 0 Block Status**: Indicates the block status of port 1 in the ring.
- **Port 1 Block Status**: Indicates the block status of port 2 in the ring.

Configuration example 1: Add an ERPS group.

Add ERPS group 1. Set **Port 0** to port 27, and **Port 1** to port 28. The owner port is port 27. The protocol VLAN ID is 3001. Configure data as follows:

On the ERPS configuration page, click **Add New Protection Group**. Set **Port 0** to **27**, and **Port 1** to **28**, **Owner Port** to **Port 0**, and **Protocol VLAN** to **3001**, and click **Save**.



Note: ERPS, STP, and loop protection cannot be enabled at the same time. To enable ERPS on a port, confirm that STP and loop protection are disabled on all the ports in the ring.

Configuration example 2: Delete an ERPS group.

Select the **Delete** check box corresponding to the ERPS group to be deleted, and click **Save**.

Configuration example 3: Modify an ERPS group.

Delete the old ERPS group, and add a new ERPS group.

Configuration example 4: Form an ERPS ring.

Ports 27 and 28 of three devices (device IDs: DUT A, DUT B, and DUT C) form an ERPS ring.

[Basic principle 1] To form a ring, configure data and then connect cables. To modify the ring configurations, disconnect any cable, and then modify the configuration.

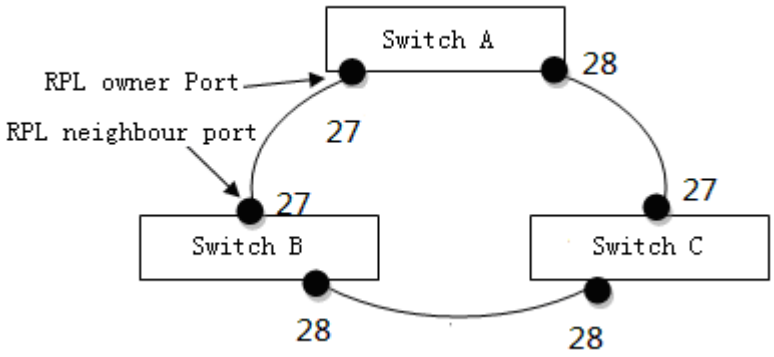
[Basic principle 2] In an ERPS ring, the protocol VLANs of all ERPS groups must be the same.

Recommended configuration method: Do not configure any ring port as the owner port. This configuration method is fast and convenient. The configuration process is as follows:

1. Ports 27 and 28 of three devices (device IDs: DUT A, DUT B, and DUT C) form an ERPS ring. (It is recommended that STP and loop protection be directly disabled.)
2. Configure data on the three devices according to the method described in example 1. Add ERPS group 1. Set **Port 0** to **27**, and **Port 1** to **28**, **Owner Port** to **Port 0**, and **Protocol VLAN** to **3001**, and click **Save**.
3. Connect cables. The ERPS ring is successfully formed. Check that the alarm indicator turns green on the ERPS configuration page.

Note: If this configuration method is used, the blocked port is obtained through automatic negotiation of the ERPS protocol.

Standard configuration method: Elect a ring port as the owner port. If this method is used, a blocked port in the ring is specified. The configuration process is as follows:



1. Confirm that ports 27 and 28 of three devices (device IDs: DUT A, DUT B, and DUT C) form an ERPS ring. (It is recommended that STP and loop protection be directly disabled.)
2. On DUT A, add ERPS group 1. Set **Port 0** to **27**, **Port 1** to **28**, **Owner Port** to **Port 0**, and **Protocol VLAN** to **3001**, and click **Save**.

3. On DUT B, port 27 (the port on the peer device that is connected to the owner port) must be configured as a neighbor port. Add ERPS group 1. Set **Port 0** to **27**, **Port 1** to **28**, and **Protocol VLAN** to **3001**. Click **ERPS ID** to display the ERPS detailed configuration page. In the RPL configuration area, set **RPL Role** to **RPL_Neigbour**, **RPL Port** to **Port 0**, and click **Save**. For other parameters, retain the default settings.

4. On DUT C, add ERPS group 1. Set **Port 0** to **27**, **Port 1** to **28**, and **Protocol VLAN** to **3001**, and click **Save**. For other parameters, retain the default settings.

5. Connect cables. The ERPS ring is successfully formed. Check that the alarm indicator turns green on the ERPS configuration page. At the bottom of the ERPS detailed configuration page, you can check the status of every port in the ERPS ring.

Note: To delete the original RPL configuration, select the **Delete** check box in the RPL configuration area, and then click **Save**.

7 Network Manage

Click **Network Manage** in the navigation bar, and then the following items are listed:

7.1 SSH Config

Secure Shell (SSH) encrypted connection provides functions similar to a Telnet connection. The traditional Telnet remote management mode, however, is not secure because it uses plain text to transfer passwords and data. These passwords and data can be easily intercepted for malicious use. If a device is remotely logged in through an insecure network environment, the SSH function can provide powerful encryption and authentication functions to ensure security. SSH can encrypt all transmitted data to effectively prevent information leakage during remote management.

On the SSH configuration page, you can configure parameters shown in the following figure.

Note: The switch supports only the SSH2.X version.

On the SSH configuration page, you can configure the SSH mode.

- **Mode**: Select **Enabled** to enable SSH or **Disabled** to disable SSH. The default value is **Disabled**.
- **Configuration example: Enable SSH.**

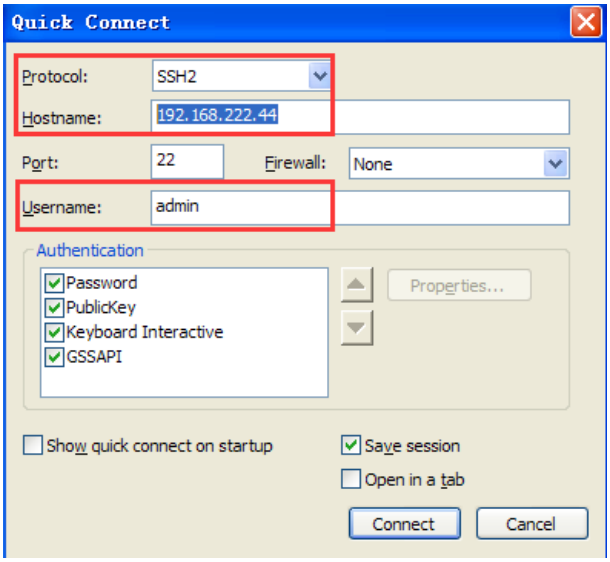
Configure data as follows:

1. Select **Enabled** from the **Mode** drop-down list box, and click **Save**.

The following figure shows the configuration results.

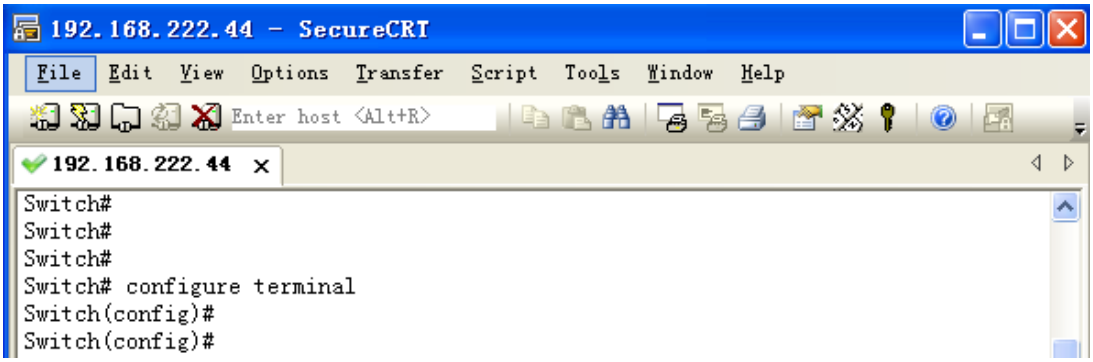
Use an SSH client to access the switch. The following description assumes that SecureCRT is used.

Create a new connection, set the protocol to **SSH2**, host name to the IP address of the switch, and user name to the user name of the switch, and click **Connect**. (The user name of the switch must be consistent with the account configured on the User Config page.)



The following dialog box is displayed:

Enter the password of the switch. (The password of the switch must be consistent with that configured in the user settings.) The following switch interface is displayed, where you can perform operations.



7.2 HTTPS Config

HTTPS is the secure version of HTTP. HTTPS consists of two parts, HTTP and SSL/TLS, that is, a module for processing encrypted information is added on the basis of HTTP. Information transmitted by the server and client is encrypted over TLS. Therefore, data is encrypted before being transmitted.

On the HTTPS configuration page, you can configure parameters shown in the following figure.

On this page, you can configure **Mode** and **Automatic Redirect**.

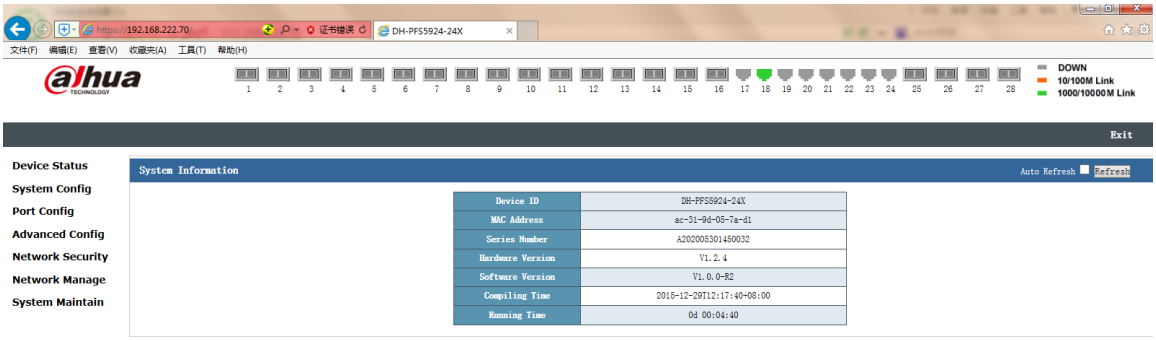
- **Mode**: Select **Enabled** to enable HTTPS or **Disabled** to disable HTTPS. The default value is **Disabled**.
- **Automatic Redirect**: Select **Enabled** to enable the automatic redirection function or **Disabled** to disable this function. The default value is **Disabled**. After the function is enabled, even if HTTP is used to log in to the switch, the device will be automatically redirected to HTTPS to log in to the switch.

Configuration example: Enable HTTP and automatic redirection.

Select **Enabled** from the **Mode** and **Automatic Redirect** drop-down list boxes to enable HTTPS and automatic redirection, and click **Save**.

The following figure shows the configuration results.

After enabling HTTPS, you can use the Chrome browser to access the switch operation interface. As shown in the following figure, you can enter https://192.168.222.32 in the address bar to access the switch. If HTTPS is disabled, you cannot use https://192.168.222.32 to access the switch.

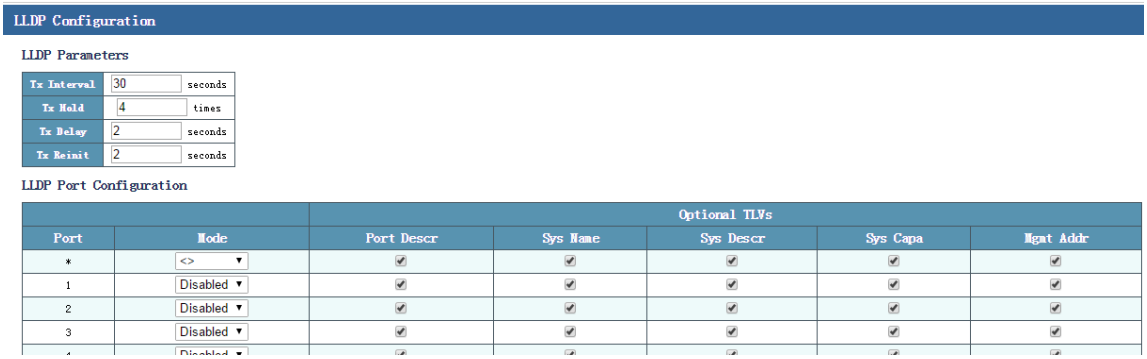


7.3 LLDP Config

LLDP is a L2 topology discovery protocol. Its basic principle is as follows: A device on the network sends a notification containing its own status information to its neighbor devices, and the information about this device is stored on every port of all devices. If the status of the local device changes, the device sends an update message to neighbor devices that are directly connected to this device. Neighbor devices store the information in the standard SNMP management information base (MIB). The network management system can query the current L2 connection information from the SNMP MIB. Note that LLDP is a remote device status discovery protocol. It cannot complete functions, such as network device configuration and port control.

7.3.1 LLDP Configuration

On the LLDP configuration page, you can configure parameters shown in the following figure.



The LLDP configuration parameters include:

- **Tx Interval**: Indicates the interval at which the local device sends an LLDPDU to neighbor devices. The default value is 30s.

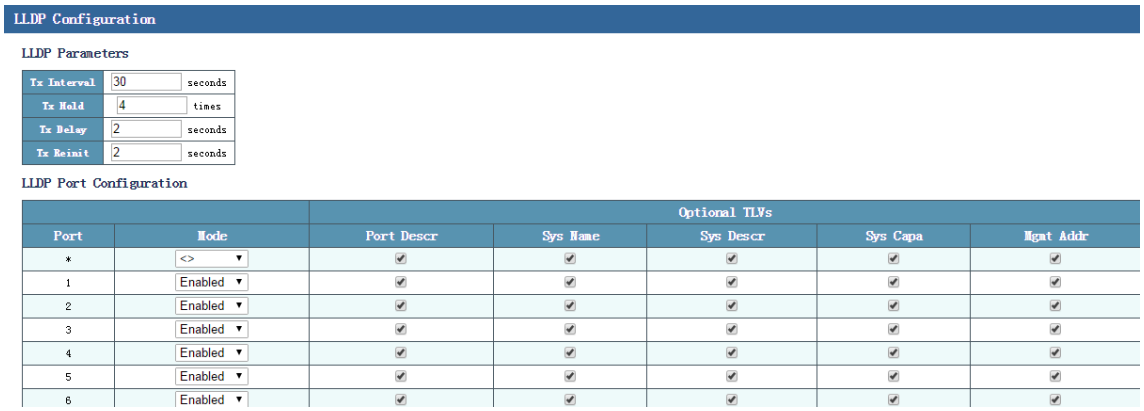
- **Tx hold**: Indicates the aging time of the LLDPDU. The default value is 4 times.
- **Tx Delay**: Indicates that delay after which the LLDPDU is transmitted. The default value is 2s.
- **Port**: Indicates the port number of the switch.
- **Mode**: Indicates the working mode of a port. Options include **Disabled**, **TxRx**, **RX**, and **Tx**.
- **Port Descr**: If this check box is selected, the peer device will save the port description of the local device; otherwise, the port description is hidden.
- **Sys Name**: If this check box is selected, the peer device will save the system name of the local device; otherwise, the system name is hidden.
- **Sys Descr**: If this check box is selected, the peer device will save the system description of the local device; otherwise, the system description is hidden.
- **Sys Capa**: If this check box is selected, the peer device will save the system attributes of the local device; otherwise, the system attributes are hidden.
- **Mgmt addr**: If this check box is selected, the peer device will save the management address of the local device; otherwise, the management address is hidden.

Configuration example:

Enable the LLDP mode on all the ports. Enable the peer device to save the port description, system name, system description, system attributes, and management address of the local device.

Configure data as follows:

Select **Enabled** from the **Mode** drop-down list box, and click **Save**. Retain default settings of the time parameters. The following figure shows the configuration results. (You can check the neighbor information by choosing **Device Status** > **LLDP Neighbor** in the navigation bar.)



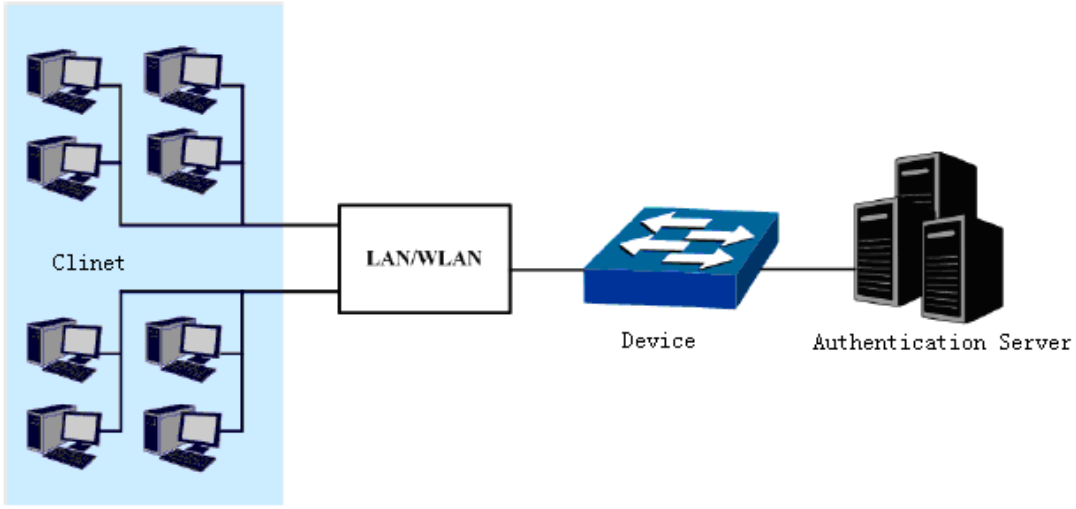
7.4 802.1X Config

802.1x was proposed by IEEE802 LAN/WAN Standards Committee to resolve the security issues of the WLAN. Later this protocol is used on the Ethernet as a common access control mechanism of LAN ports. 802.1x is mainly used to resolve the authentication and security issues on the Ethernet. It implements authentication and control on devices connected to ports of the LAN access devices.

The switch described in this manual can serve as an authentication system to perform authentication on PCs on the network. If user devices connected to ports of the switch can pass the authentication, they can access resources on the LAN. If they fail in authentication, their access to network resources will be denied.

802.1x architecture

The 802.1x system adopts the typical client/server architecture. It consists of three entities, as shown in the following figure.



- Client: It is an entity in the LAN, and is generally a common PC. Users initiate 802.1x authentication through the client software, and the switch performs authentication on the client. The client must be a user terminal that supports 802.1x authentication.
- Switch: It is generally a network device that supports 802.1x. The switch provides a physical or logical port for the client to access the LAN, and performs authentication on the client.
- Authentication server: It is an entity that provides the authentication service for the switch. For example, the RADIUS server can be used to implement the authentication and authorization functions of the authentication server. The server can store client-related information, and implement authentication and authorization on clients. To ensure stability of the authentication

system, a standby authentication server can be deployed on the network. When the active authentication server is faulty, the standby authentication server can take over the work from the active authentication server.

Working process of 802.1x

(1) When a user who needs to access the network, the user starts the 802.1x client program, and enters the user name and password that have been applied for and registered to initiate a connection request. The client sends an authentication request packet to the switch to start an authentication process.

(2) On receiving the authentication request, the switch sends a message to the client, requesting the client to send the entered user name.

(3) In response to the message, the client sends a message containing the user name to the switch. The switch encapsulates the message sent by the client, and forwards this message to the authentication server.

(4) On receiving the user name information forwarded by the switch, the authentication server compares the information with the user name list in the database, locates the password corresponding to the user name, generates a key at random to encrypt the password, and sends the key to the switch. The switch then forwards the key to the client.

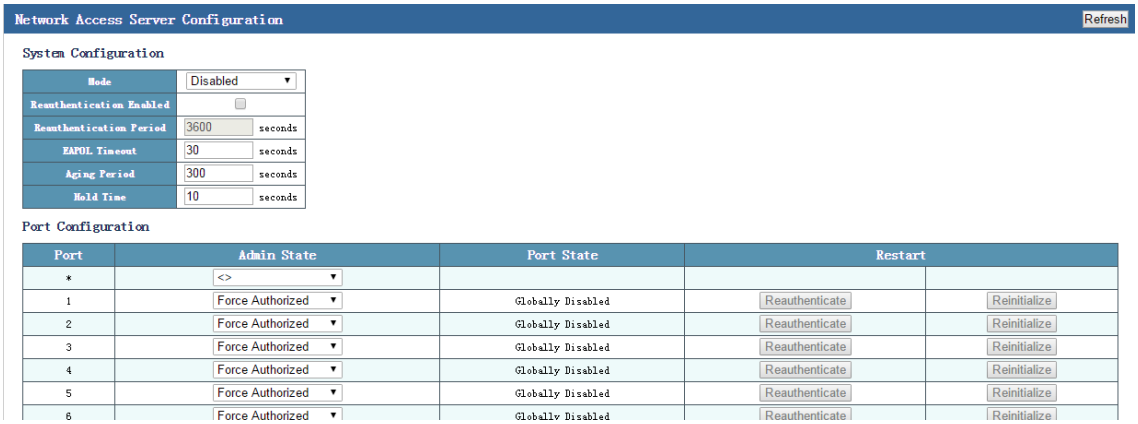
(5) On receiving the key from the switch, the client uses the key to encrypt the password (this encryption algorithm is generally irreversible), and sends the encrypted password to the authentication server through the switch.

(6) The authentication server compares the encrypted password sent from the client with the password that the server obtains using the encryption algorithm. If the two passwords are the same, the authentication server determines that the user is an authorized user, returns an authentication succeeded message, and sends a message to the switch, requesting the switch to enable the port so that the user can access the network through the port. Otherwise, the authentication server returns an authentication failed message, retains the disabled state of the port on the switch, and allows only the authentication data (not the service data) to pass through the port.

7.4.1 NAS Configuration

Network Access Configuration (NAS) is an entity on the LAN that performs authentication on the connected client. The NAS is generally a network device that supports 802.1x. It provides a port for the client to access the LAN. This port can be a physical or logical port.

On the NAS configuration page, you can configure parameters shown in the following figure.



The NAS configuration parameters include:

- **Mode**: Select **Enabled** to enable NAS or **Disabled** to disable NAS. The default value is **Disabled**.
- **Reauthentication Enabled**: Select this check box to enable the reauthentication function. This function is disabled by default.
- **Reauthentication Period**: When the authentication period expires, the switch initiates reauthentication. The default reauthentication period is 3600s.
- **EAPOL Timeout:** Indicates the time after which the EAP-Request is retransmitted. The default value is 30s.
- **Aging Period:** The default value is 300s.
- **Hold Time:** Indicates the EAP-Request retransmission interval upon timeout of the server. The default value is 10s.
- **Port**: Indicates the port number of the switch.
- **Admin State**: The administration states include **Fore Authorized**, **Force Unauthorized**, and **Port-Based 802.1x**. The default value is **Fore Authorized**.
- **Port State**: The default value is **Globally Disabled**.

Port State	**Remarks**
Globally Disabled	This state is displayed for all the ports when the 802.1x authentication function is disabled.
link down	This state is displayed when the port is not up.

Authorized	This state is displayed when the port is up and port authentication succeeds or forcibly succeeds.
Unauthorized	This state is displayed when the port is up and port authentication fails or forcibly fails.

- **Restart**: Two buttons are available: **Reauthenticate** and **Reinitialize**. This configuration is available only when 802.1x authentication is enabled on the port, and is grayed out in other states.

7.4.2 RADIUS Server Configuration

On the RADIUS server configuration page, you can configure parameters shown in the following figure.

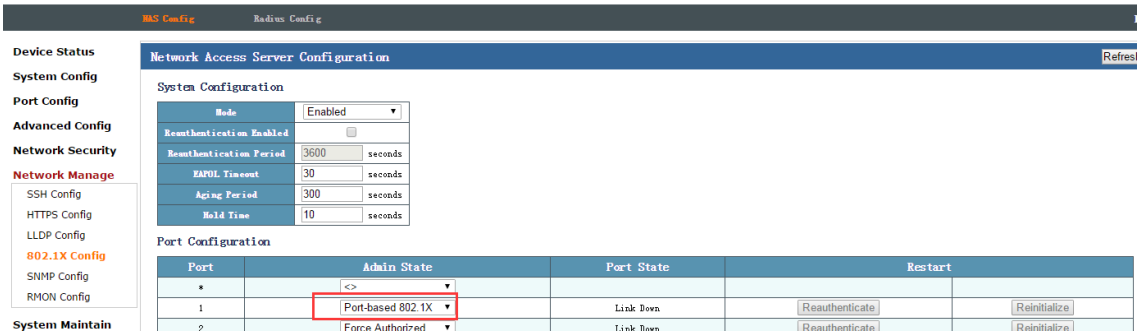
Parameters related to configuration of the RADIUS server include:

- **Timeout**: A request is retransmitted if the RADIUS server does return a reply after the timeout time expires. The value ranges from 1 to 1,000. The default value is 5s.
- **Retransmit**: Indicates the retransmission times. The default value is 3.
- **Deadtime**: After a user sends a packet, if the user does not receive any response within the t seconds, the server is dead, and the time t is called deadtime. The value ranges from 1s to 1,000s.
- **Delete**: Used to delete the server configuration.
- Server address: Indicates the IP address of the server.
- **Auth Port**: Indicates the number of the UDP port used for RADIUS authentication. The default value is 1812.
- **Key**: The switch and the authentication server must authenticate each other, and the same key must be configured on the switch and the authentication server.

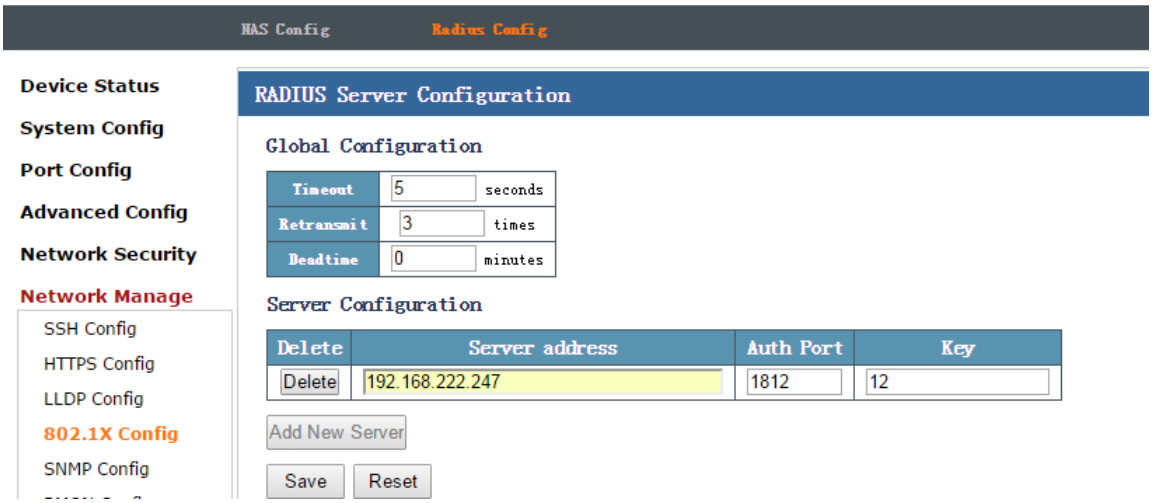
- **Add New Server**: When there is no server configuration, click this button to create a server.

Configuration example:

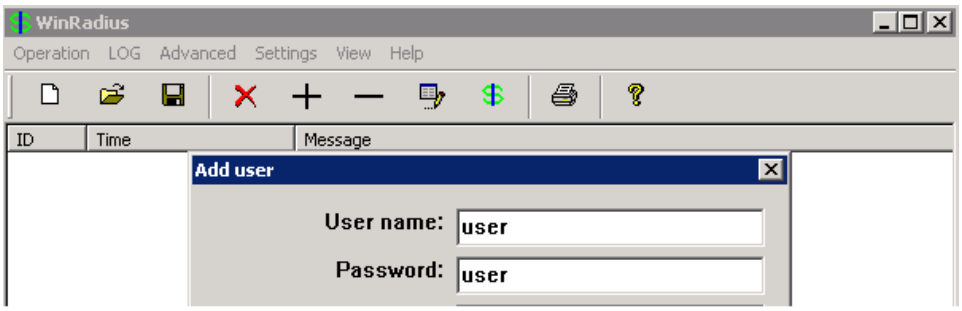
1. Enable NAS, Set **Admin State** of port 1 that is directly connected to the client to **port-based 802.1X**, and retain other default settings, as shown in the following figure.



2. Configure the RADIUS server. Click **Add New Server**, and fill in the IP address of the RADIUS server and the key. (The key value can be set at random. Here, **Key** is set to **12**.)

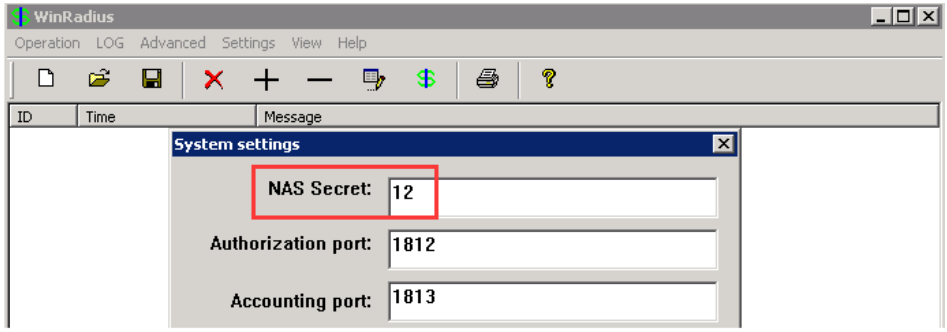


3. Start the WinRadius. Choose **Operation** > **Add Account** to add an account and password.

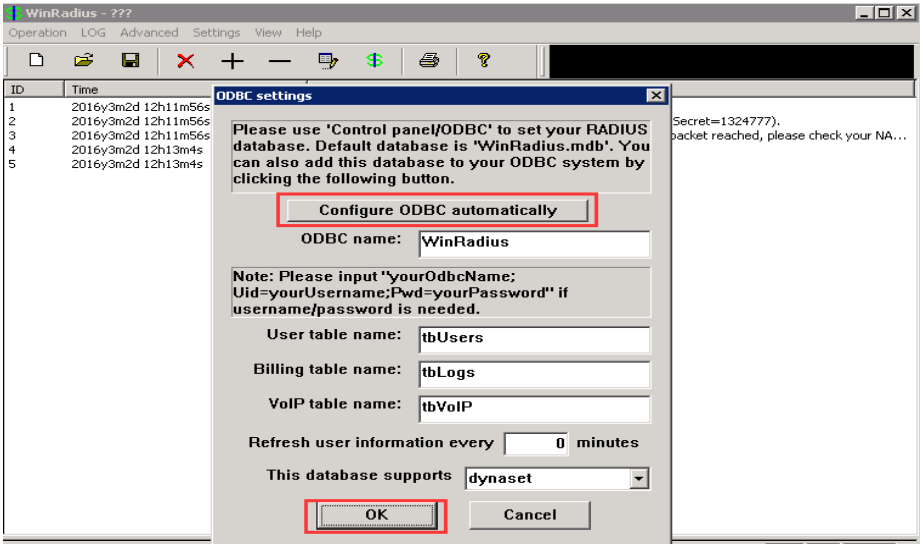


4. Choose **Advanced** > **Create RADIUS Table** to create a RADIUS table.

5. Choose **Settings** > **System Settings**. Modify the NAS key so that the NAS key is the same as the key configured on the web page of the switch.



6. Choose **Settings** > **Data Settings**. Click **Configure ODBC automatically**, and then click **OK**.



7. Restart the WinRadius.

8. Remove and then insert the network cable that is connected to port 1 of the PC where the client is installed. An authentication login page is displayed on the client. Enter the user name and password. Then, the client can access the network normally.

7.5 SNMP Config

SNMP is a network management protocol that is most popular on the UDP/IP network. It provides a management framework to monitor and maintain Internet devices.

SNMP network elements (NEs) are classified into two types: network management station (NMS) and agent.

- The NMS is a workstation on which the SNMP client runs. It provides a user-friendly human-computer interaction interface, with which network administrators can conveniently complete the majority of network management work.
- The agent is a process that resides on a device. It collects and processes requests sent from the NMS. In case of an emergency, for example, when the interface status changes, the agent will notify the NMS of the change.

The NMS is the manager of the SNMP network, whereas the agent is the managed object of the SNMP network. The NMS and the agent exchange management information over SNMP.

SNMP provides four basic operations:

- Get: The NMS uses this operation to query one or more object values of the agent.
- Set: The NMS uses this operation to reconfigure one or more objects in the MIB of the agent.
- Trap: The agent uses this operation to send alarms to the NMS.
- Inform: The agent uses this operation to send warning information to the NMS.

SNMP protocol versions:

Currently, the SNMP agent of the device supports SNMP v3, and is compatible with SNMP v1 and SNMP v2c.

SNMP v1 uses the community name for authentication. The community name defines the relationship between the SNMP NMS and the SNMP agent. If the community name carried by an SNMP packet is not recognized by the device, the packet is dropped. The community name plays a role similar to the password, and is used to restrict the access of the SNMP NMS to the SNMP agent.

SNMP v2c also uses the community name for authentication. It is compatible with SNMP v1, and expands functions of SNMP v1. SNMP v2c provides more operation types (including GetBulk and InformRequest), supports more data types (such as Counter64), and provides more error codes to distinguish errors in a more accurate manner.

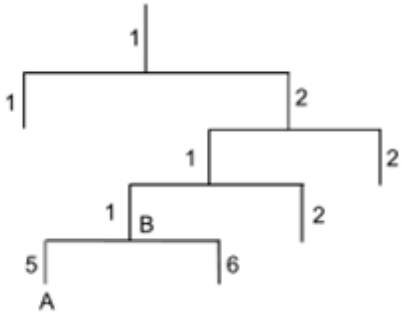
SNMP v3 provides an authentication mechanism that is based on the User-Based Security Model (USM). Users can configure the authentication and encryption functions. The authentication function is used to check whether the packet sending party is authorized to prevent access of unauthorized users. The encryption function is used to encrypt packets transmitted between the NMS and the agent to prevent illegal interception. Different combinations of the authentication and encryption functions can provide higher security for communication between the SNMP NMS and the SNMP agent.

SNMP version matching between the NMS and the agent is a prerequisite for mutual access between them. Multiple versions can be configured on an agent so that different versions are used to interact with different NMSs.

Introduction to the MIB:

Any managed resource is represented as an object, which is also called a managed object. The MIB is a collection of managed objects. It defines a series of attributes for each managed object, including the name, access permission, and data type of the object. Each agent has its own MIB. The NMS can perform read/write operations on objects in the MIB based on the configured permissions. The following figure shows the relationship between the NMS, agent, and MIB.

Data is stored in the MIB using a tree structure. A node on the tree represents a managed object, which can be uniquely identified by a path starting from the root. As shown in the following figure, managed object B can be uniquely identified by a number string {1.2.1.1}. This number string is called object identifier (OID) of the managed object.



7.5.1 SNMP System Configuration

On the SNMP system configuration page, you can configure parameters shown in the following figure.

Parameters related to configuration of the SNMP system include:

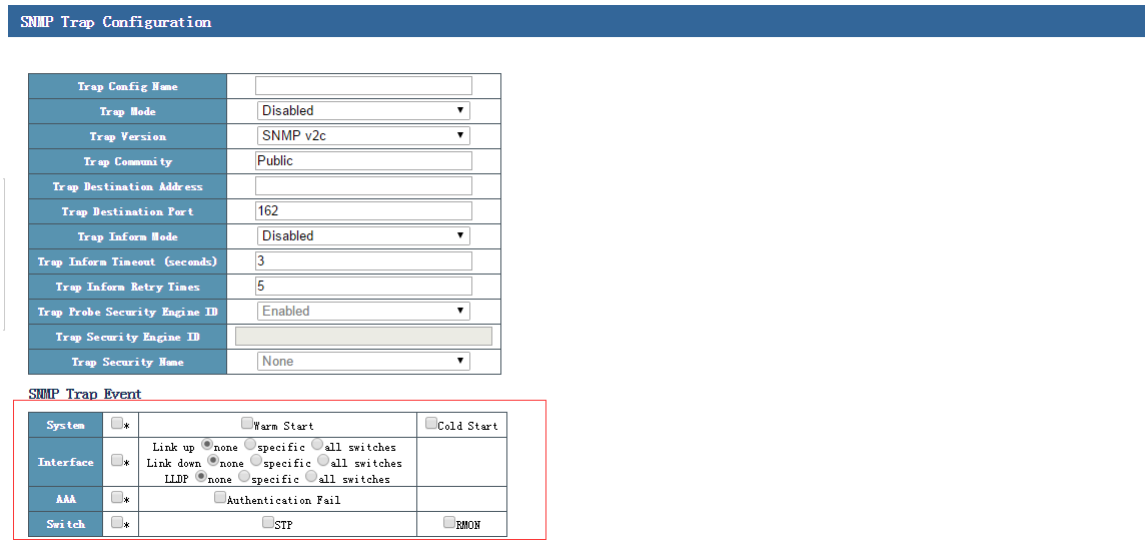
- **Mode**: Two modes are provided, including **Enabled** and **Disabled**. The default value is **Enabled**.
- **Version**: Three versions are available, including **SNMP vl**, **SNMP v2c**, and **SNMP v3**. The default value is **SNMP v2c**.
- **Read Community**: Indicates the community name of the accessing NMS. The permission is readable. The default value is **public**.
- **Write Community**: Indicates the community name of the accessing NMS. The permission is writable. The default value is **private**.
- **Engine ID**: Indicates the SNMP engine ID, which is in one-to-one relationship with the SNMP entity.

7.5.2 Trap Configuration

On the trap configuration page, you can configure parameters shown in the following figure.

A trap is a message proactively sent by an agent to the NMS, and is used to report important or urgent events, for example, restart of a managed device. There are two types of traps: generic traps and enterprise-specific traps. Generic traps supported by the switch include authentication, coldstart, linkdown, linkup, and warmstart. Others are enterprise-specific traps, as shown in the red frame in the following figure [**SNMP Config** > **Trap Configuration** > **Add New Entry**]. The enterprise-specific traps are generated by modules. The amount of traps is generally large and occupies the memory of the device, which affects device performance. Therefore, it is recommended that you enable the trap function of a specified module to generated related traps.

After the trap function is enabled, traps generated by the specified module will be sent to the information center of the device. The information center supports seven output directions. By default, traps of all modules are sent to the console, monitor, log host, and log file; traps of all modules with a priority level equal to or higher than warning are sent to the trap buffer and SNMP agent; traps cannot be sent to the log buffer.



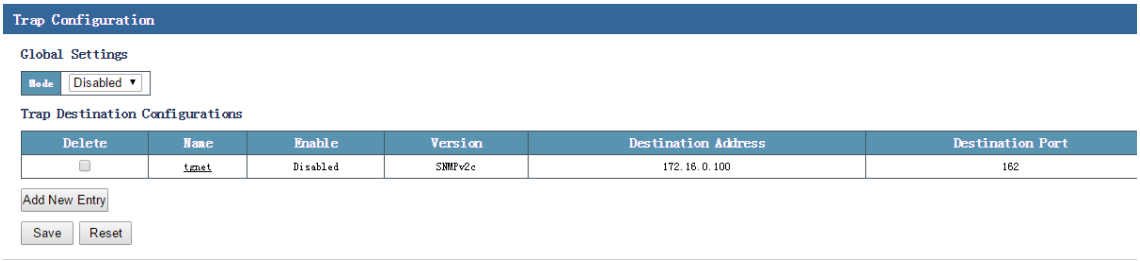
- **Trap Config Name**: Indicates the name of the trap.
- **Trap Mode**: Indicates the status of a trap switch.
- **Trap Version**: Trap versions include **SNMP V1** and **SNMP V2c**. The default value is **SNMP V2c**.
- **Trap Community**: Indicates the name of the trap community.
- **Trap Destination Address**: Specifies the IP address of the server.
- **Trap Destination Port**: The default trap destination port is 162.
- **Trap Inform Mode**: Indicates the trap information switch.
- **Trap Inform Timeout**: Indicates the timeout time. The default value is 3s. The value ranges from 0s to 2,174s.
- **Trap Inform Retry Times**: Indicates the number of times packets are retransmitted. The default value is 5s. The value ranges from 0s to 255s.
- **SNMP Trap Event**: Indicates the supported trap packet.

Configuration example:

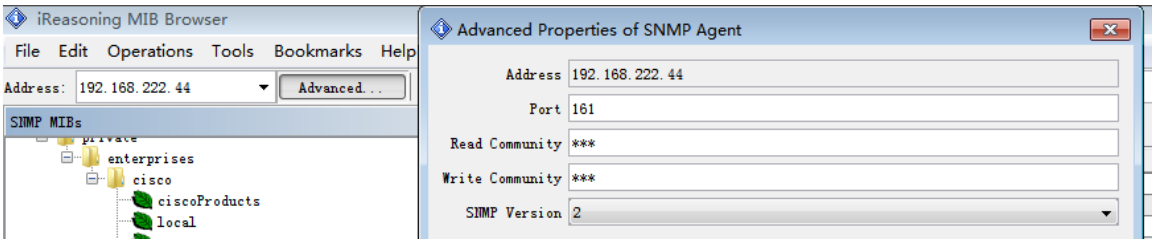
1. Enable SNMP, and set the version to **SNMP V2c**, **Read Community** to 111, and **Write Community** to 111.

2. Click **Add New Entry**, fill in **tgnet** in the **Trap Config Name** text box, select **Enabled** from the **Trap Mode** drop-down list box, set Trap Destination Address to 172.16.0.100, and click Save.

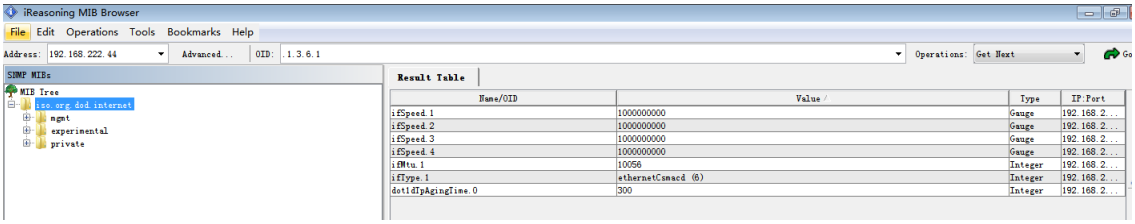
The following figure shows the configuration results.



Use the MIB Browser, load the corresponding MID, fill in the IP address of the managed device, and set **Read Community**, **Write Community**, and **SNMP Version**, as shown in the following figure.



4. Right-click **iso.org.dod.internet**, and choose **Work**, as shown in the following figure. Related information is displayed.



7.6 RMON Config

Remote Monitor (RMON) is a standard monitoring specification that enables exchange of network monitoring data between various network monitors and consoles. RMON provides network administrators with more freedom in selecting consoles and network monitors that meet special network requirements. RMON implements unified remote management on a heterogeneous environment. It provides a solution for remotely monitoring a network segment through a port. Data traffic of a network segment or even the entire network can be monitored. Currently, RMON has become one of the successful network management standards.

RMON enables SNMP to monitor remote devices in a more effective and active manner. Network administrators can quickly trace faults that occur on a network, in a network segment, or on a device. With implementation of RMONMID, some network events, network performance data, and fault history can be recorded. The historical fault data can be accessed at any time to facilitate fault diagnosis.

This method reduces the traffic between the NMS and the agent, and makes it possible to manage a large-sized network in a simple and effective manner.

RMON collects data using either of the following methods:

- Method 1: Use a dedicated RMON probe. The NMS directly obtains the management information from the monitor and controls network resources. If this method is used, all information about the RMON MIB can be obtained.
- Method 2: The RMON agent is directly embedded into network devices (such as routers, switches, and hubs), allowing these devices to implement the RMON probe functions. The NMS uses basic SNMP commands to exchange information with these devices and collect network management information. This method is restricted by device resources. Therefore, not all data of the RMON MIB can be obtained, and information about at most four groups can be collected.

Statistics group	It contains statistics measured by the probe for each monitored Ethernet interface on this device.	Dropped packets, sent packets, broadcast packets, CRC errors, undersized or oversized packets, collisions, and counters. The ranges include 64–128, 128–256, 256–512, 512–1,024, and 1,024–1,518 bytes.
History group	It records periodic statistical samples from an Ethernet network and stores them for later retrieval.	Sampling interval, number of items, and sampled content. This group provides historical data about a network segment, such as the traffic, error packets, broadcast packet, usage, and collision times.
Alarm group	It periodically selects statistical samples from variables in the probe and compares them with previously configured thresholds.	Alarm type, interval, upper limit, and lower limit
Event group	It provides a list of all events generated by the RMON agent.	Event type, event description, and last event sending time

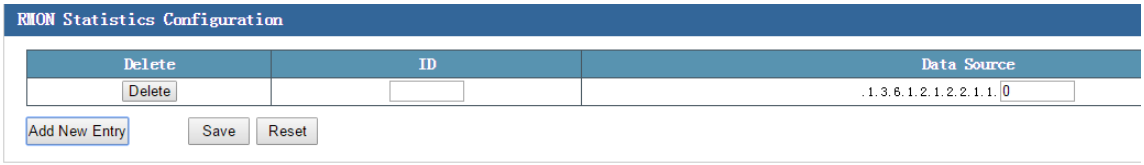
7.6.1 RMON Statistics

The RMON statistics management function can be used to monitor the usage of each port. Statistical information includes the number of network collisions, number of CRC error packets, number of

undersized or oversized packets, number of broadcast/multicast packets, received bytes, and number of received packets.

After an RMON statistics entry is successfully created for a specified interface, the statistics group counts the number of packets on the current interface. The statistical result is a continuous accumulated value.

On the RMON statistics configuration page, you can configure parameters shown in the following figure.



Parameters related to RMON statistics configuration include:

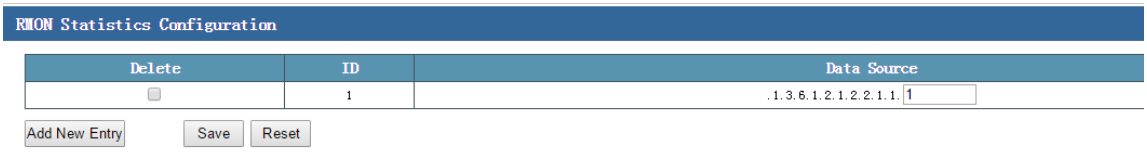
- **Delete**: Select this check box to delete the RMON statistics configuration.
- **ID**: Indicates the ID of the RMON statistics configuration.
- **Data Source**: MIB node, indicating a managed object.

Configuration example:

Add an RMON statistics configuration entry, where the ID is 1, and data source is 1.

Click **Add New Entry**, set **ID** to **1** and **Data Source** to **1**, and click **Save**.

The following figure shows the configuration results.



You can use the command line to view the statistical information, as shown in the following figure.

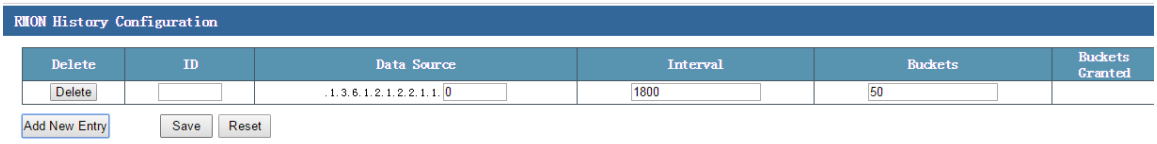
```
S5300-52G-4TF# show rmon statistics 1

Statistics ID :     1
---------------------
    Data Source : .1.3.6.1.2.1.2.2.1.1.3
    etherStatsDropEvents           : 4
    etherStatsOctets               : 55916527
    etherStatsPkts                 : 141105
    etherStatsBroadcastPkts        : 1458
    etherStatsMulticastPkts        : 5190
    etherStatsCRCAlignErrors       : 0
    etherStatsUndersizePkts        : 0
    etherStatsOversizePkts         : 0
    etherStatsFragments            : 0
    etherStatsJabbers              : 0
    etherStatsCollisions           : 0
    etherStatsPkts64Octets         : 33951
    etherStatsPkts65to127Octets    : 66551
    etherStatsPkts128to255Octets   : 4054
    etherStatsPkts256to511Octets   : 4296
    etherStatsPkts512to1023Octets  : 2898
    etherStatsPkts1024to1518Octets: 29355
S5300-52G-4TF#
```

7.6.2 RMON History

The history group periodically takes statistics on the port usage, and stores the statistical results in the history record table for later retrieval. Statistical data includes the bandwidth usage, number of error packets, and total number of packets. After an RMON history entry is successfully created for a specified interface, the statistics group counts the number of packets on the current interface. The statistical result is the information about packets sent or received on the port in a period.

On the RMON history configuration page, you can configure parameters shown in the following figure.



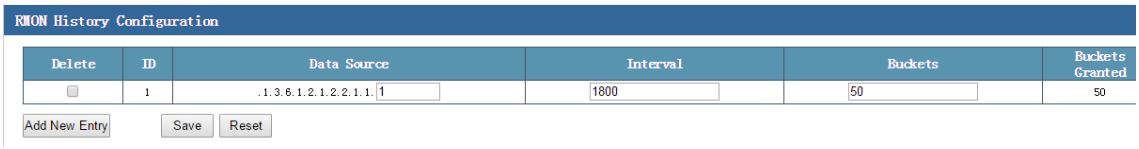
Parameters related to RMON history configuration include:

- **Delete**: Select this check box to delete the RMON history configuration.
- **ID**: Indicates the ID of the RMON history configuration.
- **Data Source**: MIB node, indicating a managed object.
- Interval: Indicates the sampling interval.
- **Buckets**: Indicates the number of buckets, that is, the amount of stored data.
- **Add New Entry**: Click this button to add an RMON history configuration entry.
- **Buckets Granted**: Indicates the maximum number of records.

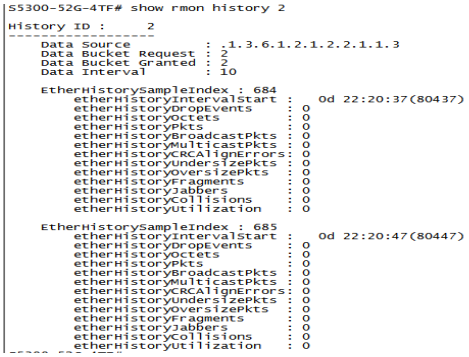
Configuration example:

Click **Add New Entry**, set **ID** to **1** and **Data Source** to **1**, retain default settings of other parameters, and click **Save**.

The following figure shows the configuration results.



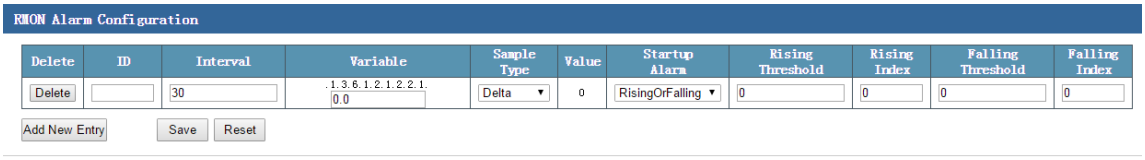
You can use the command line to view the information, as shown in the following figure.



7.6.3 RMON Alarm

The RMON alarm management can monitor specified alarm variables, such as statistical data of ports. When the sampling value of a monitored alarm variable is equal to or greater than the upper limit, an upper limit alarm event is triggered. When the sampling value of a monitored alarm variable is equal to or smaller than the lower limit, a lower limit alarm event is triggered. The alarm management processes events based on the event definitions.

On the RMON alarm configuration page, you can configure parameters shown in the following figure.



Parameters related to RMON alarm configuration include:

- **Delete**: Select this check box to delete the RMON alarm configuration.
- **ID**: Indicates the ID of an RMON alarm.
- **Interval**: Indicates the sampling interval.
- **Variable**: MIB node, indicating a managed object.

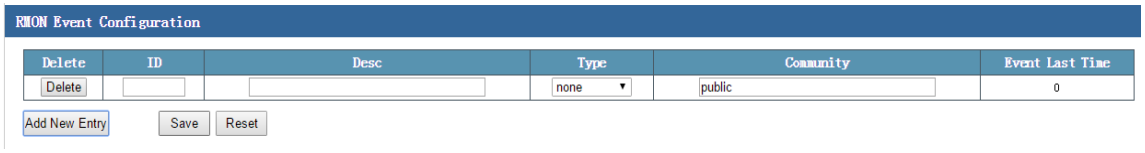
- **Sample Type**: Options include **Absolutely** (absolute value, that is, each sampling value), and **Delta** (relative value, that is, an increase of each sampling value over the previous sampling value)..
- **Value**: Indicates the sampling value. If this value is greater than the upper limit or smaller than the lower limit, an event is triggered and a trap message is sent to the gateway. The default value is 0.
- **Startup Alarm**: Startup alarms include **Rising**, **Falling**, and **RisingOrFalling**.
- **Rising Threshold**: Indicates the upper limit.
- **Falling Threshold**: Indicates the lower limit.
- **Add New Entry**: Click this button to add an RMON alarm configuration entry.

7.6.4 RMON Event

The event group is used to define the event indexes and event processing modes. Events defined in the event group are mainly used in the alarm group configuration items and extended alarm group configuration items. When a monitored object reaches the alarm conditions, an event is triggered. An event may be processed in the following ways:

- Recording event-related information in the event log table
- Sending a trap message to the NMS
- Recording event-related information in the event log table and sending a trap message to the NMS
- None (No action is taken)

On the RMON event configuration page, you can configure parameters shown in the following figure.



Parameters related to RMON event configuration include:

- **Delete**: Select this check box to delete the RMON event configuration.
- **ID**: Indicates the ID of the RMON event configuration.
- **Desc**: Indicates the event description.

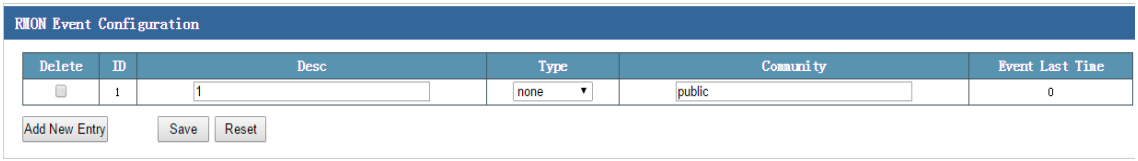
- **Type**: Indicates the event type. Options include **none** (no action), **log** (recording logs), **snmptrap** (sending trap messages), and **logandtrap** (recording logs and sending trap messages).
- **Community**: Indicates the name of a community.
- **Event Last Time**: Indicates the time that the last event occurs.
- **Add New Entry**: Click this button to add an RMON event configuration entry.

Configuration example:

Add an RMON event configuration entry, where ID is 1, description is 1, type is logandtrap, and community name is public.

Click Add New Entry, set ID to 1 and Desc to 1, select logandtrap from the Type drop-down list box, and click Save.

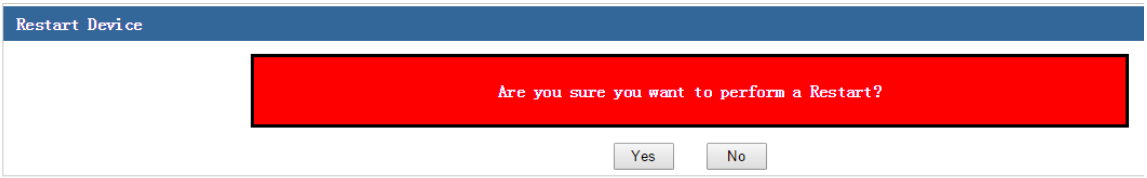
The following figure shows the configuration results.



8 System Maintain

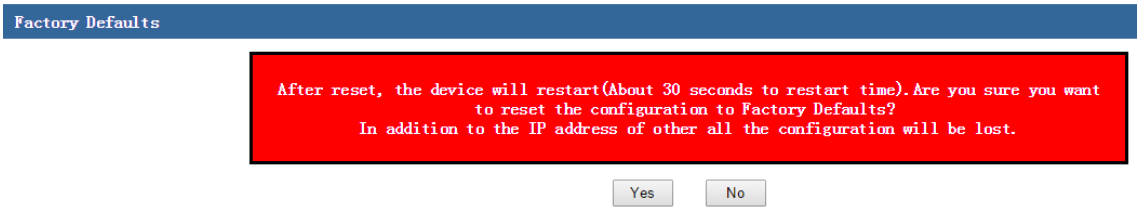
Click **System Maintain** in the navigation bar, and then the following items are listed:

8.1 Device Restart



For some functions of the switch, you need to submit and save the function configuration, and then restart the switch before these functions can take effect.

8.2 Factory Defaults



You can choose **Factory Defaults** to restore default settings of the switch. Except the management IP address, factory settings of other information will be restored.

Tip: Check whether it is necessary to back up the current configurations before restoring factory settings.

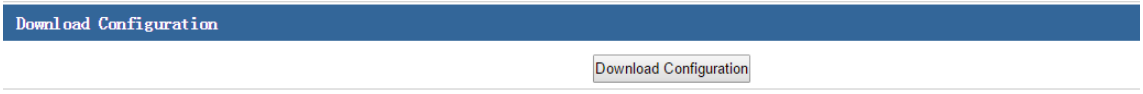
8.3 Firm Upgrade

On the firmware upgrade page, you can upgrade functions of the system file on the web interface of the switch. You can download the system file of the latest version from www.dahuatech.com.

On the firmware upgrade page, click **Select File**, select the upgrade file, and click **Upload** to upgrade the switch.

8.4 Config Export

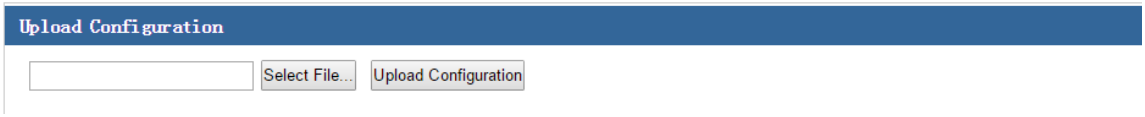
You can export the current configurations of the switch to a local PC for backup purpose.



To export the current configurations of the switch, click **Download Configuration**.

8.5 Config Upload

You can import the configuration file that is previously backed up to the switch to update the configurations.



To import a configuration file, click **Select File**, select the configuration file to be imported, and click **Upload Configuration**.

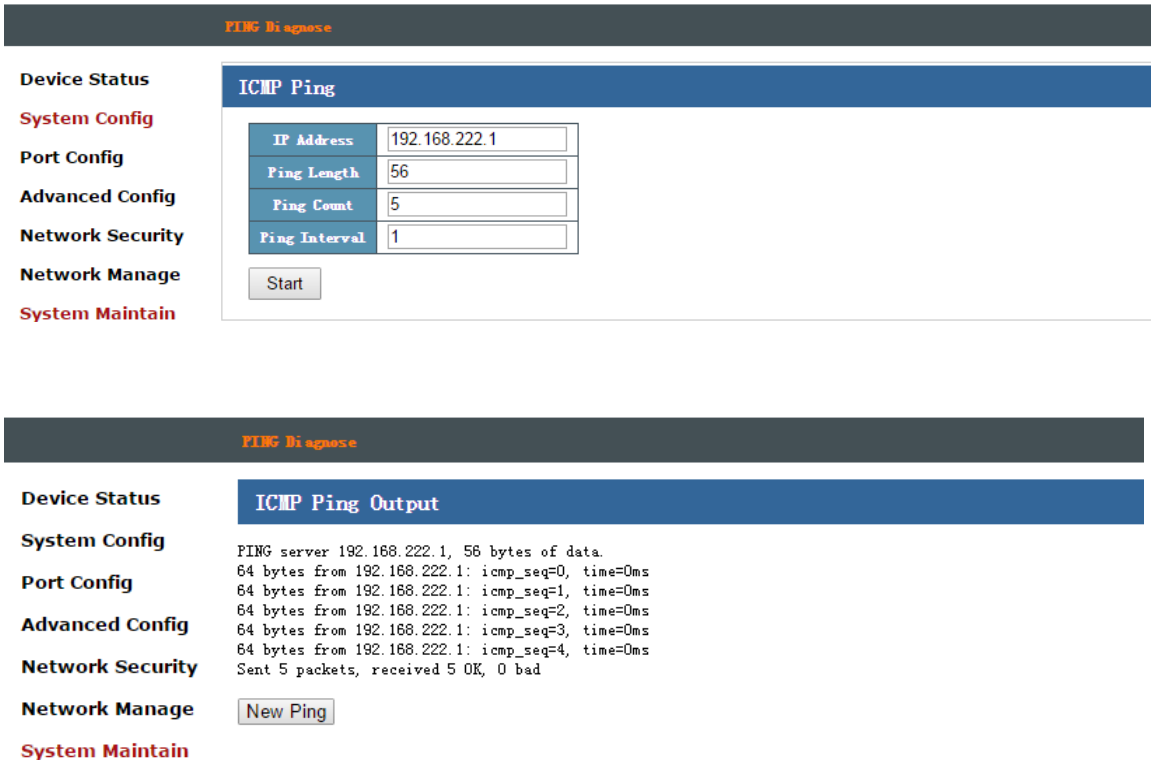
Tip: 1. After the configuration is imported, the management IP address of the device will be changed to the IP address in the configuration file that is previously backed up. Therefore, record the management IP address before importing the configuration file; otherwise, management may fail.

2. The exported configuration file does not have an extension. To view the configurations, use the Notepad or writing pad to open the configuration file.

8.6 PING Diagnose

Like the **ping** command on a common PC, the PING diagnose function is used to test connectivity between two nodes on the network. The difference between the **ping** command and PING diagnose is as follows: The **ping** command executed between two common PCs is used to check whether the physical connection between the two PCs is normal. The PING diagnose function of the switch helps the network administrator test whether a network device is disconnected on a LAN and locate network faults based on the test result.

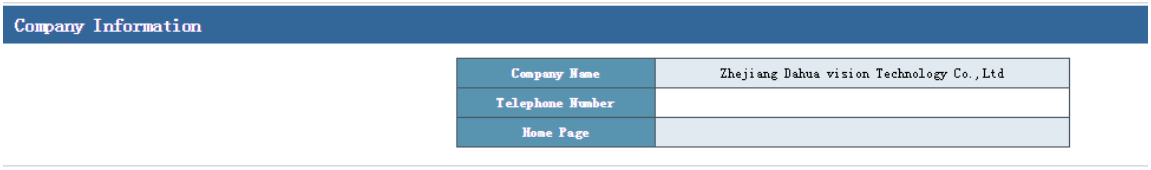
On the PING diagnose page, you can configure parameters shown in the following figure.



- **IP Address**: Indicates the IP address of the destination node to be tested.
- **Ping Length**: Indicates the length of the ping packet sent during the ping test. It is recommended that the default value be used.
- **Ping Count**: Indicates the number of ping packets sent during the ping test.
- **Ping Interval**: If no reply is received after a ping test is initiated, a ping packet is sent at the configured interval until the number of sent packets reaches the preset number of transmission times.

8.7 About Us

On the company information page, you can see the information about the supplier of the switch, as shown in the following figure.



Contact technical support engineers of Dahua if you have any doubt or suggestion for the product, or visit our website at www.dahuatech.com for more information about our products.