www.ip-com.com.cn

User Guide

L3 Managed Switch

IP-COM
World Wide Wireless

Copyright statement

Disclaimer

Pictures, images and product specifications herein are for references only. To improve internal design, operational function, and/or reliability, IP-COM reserves the right to make changes to the products described in this document without obligation to notify any person or organization of such revisions or changes. IP-COM does not assume any liability that may occur due to the use or application of the product or circuit layout(s) described herein. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information and recommendations in this document do not constitute a warranty of any kind, express or implied.

Preface

Thank you for choosing IP-COM! This user guide helps you configure, manage and maintain the product.

This user guide is applicable to layer-3 managed switches of IP-COM.

Tip

Functions of different models may differ. Please refer to the actual web UI of the product. G5324-16F is used for illustration in this guide unless otherwise specified.

Conventions

The typographical elements that may be found in this document are defined as follows.

Item	Presentation	Example
Cascading menus	>	Choose **System** > **Live Users**.
Parameter and value	Bold	Set **User Name** to **Tom**.
Variable	Italic	Format: *XX*:*XX*:*XX*:*XX*:*XX*:*XX*
UI control	Bold	On the **Policy** page, click the **OK** button.

The symbols that may be found in this document are defined as follows.

Item	Meaning
Note	This format is used to highlight information of importance or special interest. Ignoring this type of note may result in ineffective configurations, loss of data or damage to device.
Tip	This format is used to highlight a procedure that will save time or resources.

More documents

Go to our website at www.ip-com.com.cn and search for the latest documents for this product.

Product materials

Document	Description
Data sheet	It introduces the basic information of the device, including product overview, selling points, and specifications.
User guide	It introduces how to set up more functions of the device for more requirements, including all functions on the web UI of the device.
Quick installation guide	It introduces how to set up the device quickly for internet access, the descriptions of LED indicators, ports, and buttons, FAQ, statement information, and so on.

Technical support

If you need more help, contact us using any of the following means. We will be glad to assist you as soon as possible.



(86 755) 2765 3089	info@ip-com.com.cn	www.ip-com.com.cn

Contents

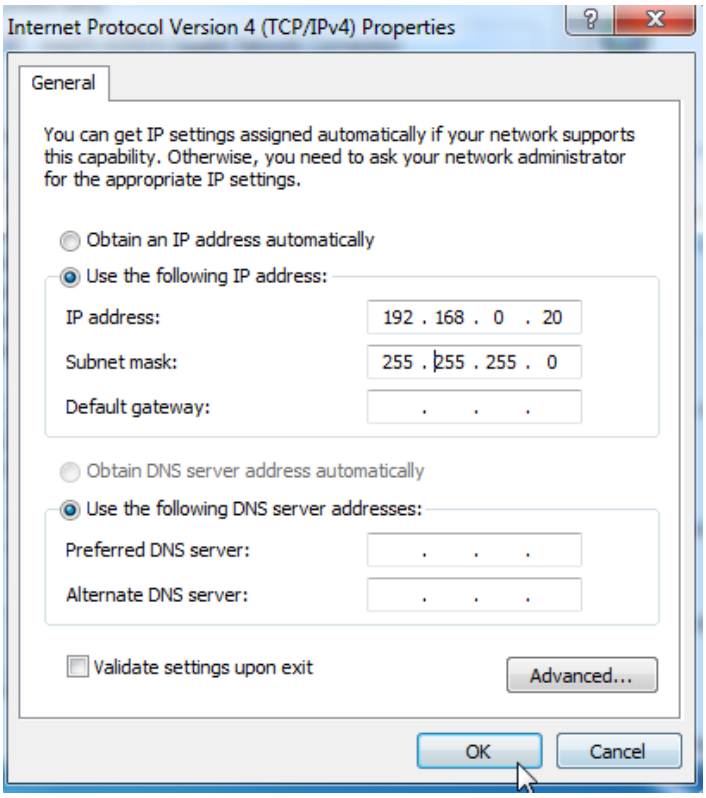
1 Web login

1.1 Login

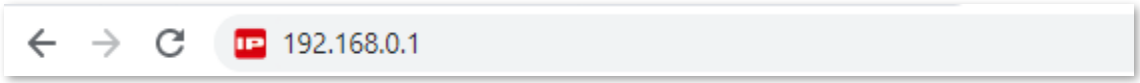
1. Connect the computer to one of the RJ45 ports (excluding the console port) of the switch using an Ethernet cable.

2. Set the IP address of Ethernet (or Local Area Connection) of the computer to an unused one belonging to the same network segment of the IP address of the switch.

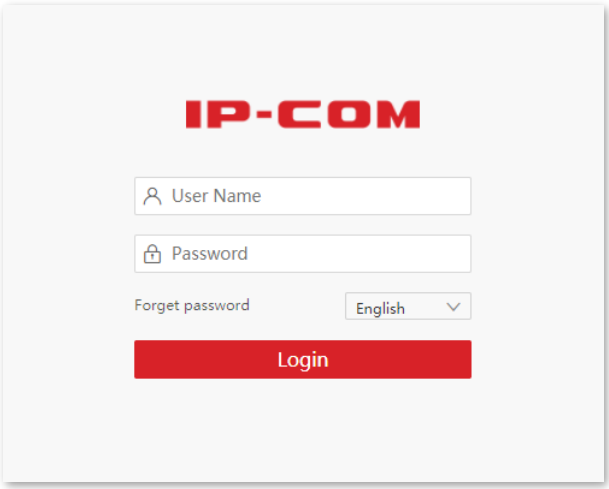
   For example, the default IP address of the switch is **192.168.0.1**, you can set the IP address of the computer to **192.168.0.*X*** (*X* is an unused number ranging from 2 to 254), and subnet mask to **255.255.255.0**.



3. Start a browser (such as Chrome) and enter the IP address of the switch (default: **192.168.0.1**) in the address bar to access the login page.



4. Enter your user name and password (both are **admin** by default) and click **Login**.



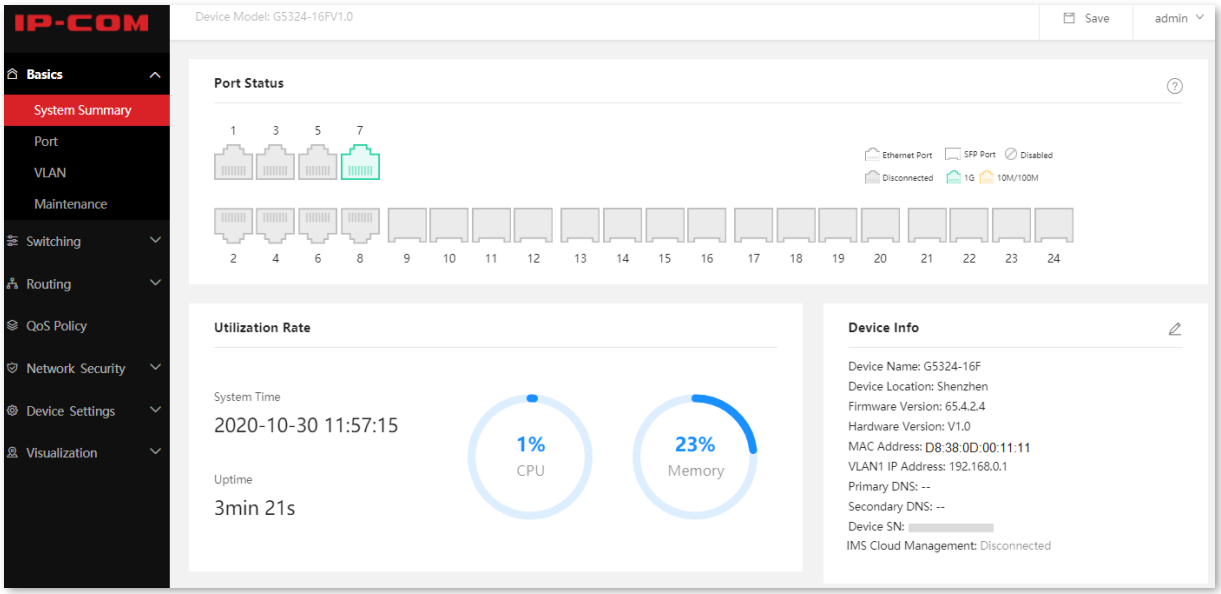
----End

Tip

If the above page does not appear, try the following solutions:

- Clear the cache of the web browser or try another web browser.
- Check whether another device with the IP address 192.168.0.1 exists in the local network.
- If the problem persists, reset the switch and try again. **Reset method**: When the **SYS** LED indicator is blinking, press down the reset button (**Reset**) using a sharp item (such as a pin) for about 10 seconds, and then release it when all LED indicators are solid on. When the **SYS** LED indicator blinks again, the switch is reset successfully.

After logging in to the web UI, you can start to configure the switch.



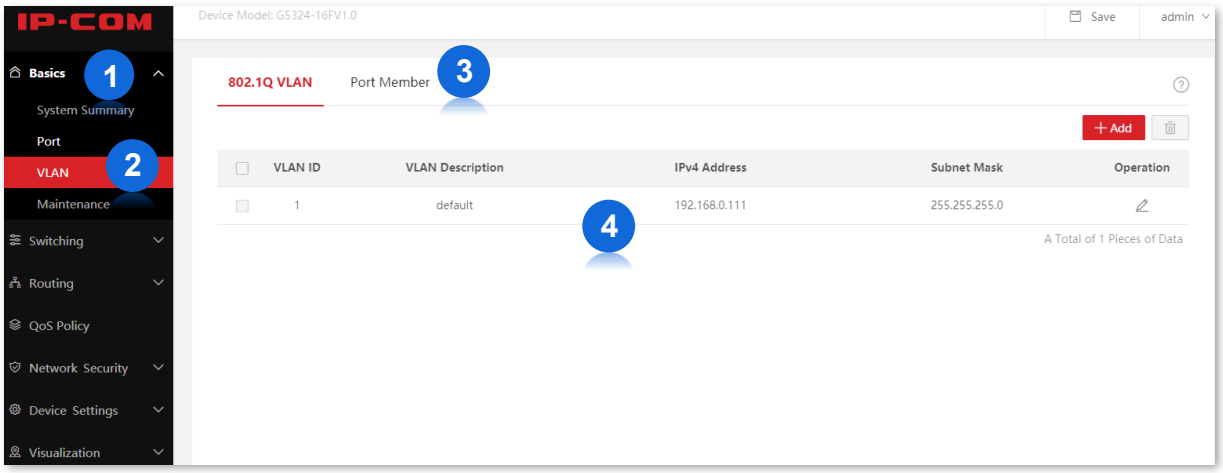
1.2 Logout

After you log in to the switch's web UI page, the system will automatically log you out if there is no operation within the login timeout. Alternatively, you can directly click the user name on the upper right corner, and then click **Exit** to exit the web UI page.

2 Web UI introduction

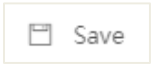
2.1 Web layout

The Web UI page can be divided into four parts: level-1 navigation bar, level-2 navigation bar, tab page area, and the configuration area.



No.	Name	Description
1	Level-1 navigation bar	The navigation bars and tab pages display the function menu of the switch. When you select a function in navigation bar, the configuration of the function appears in the configuration area.
2	Level-2 navigation bar	
3	Tab page area	
4	Configuration area	This area enables you to view and modify configuration.

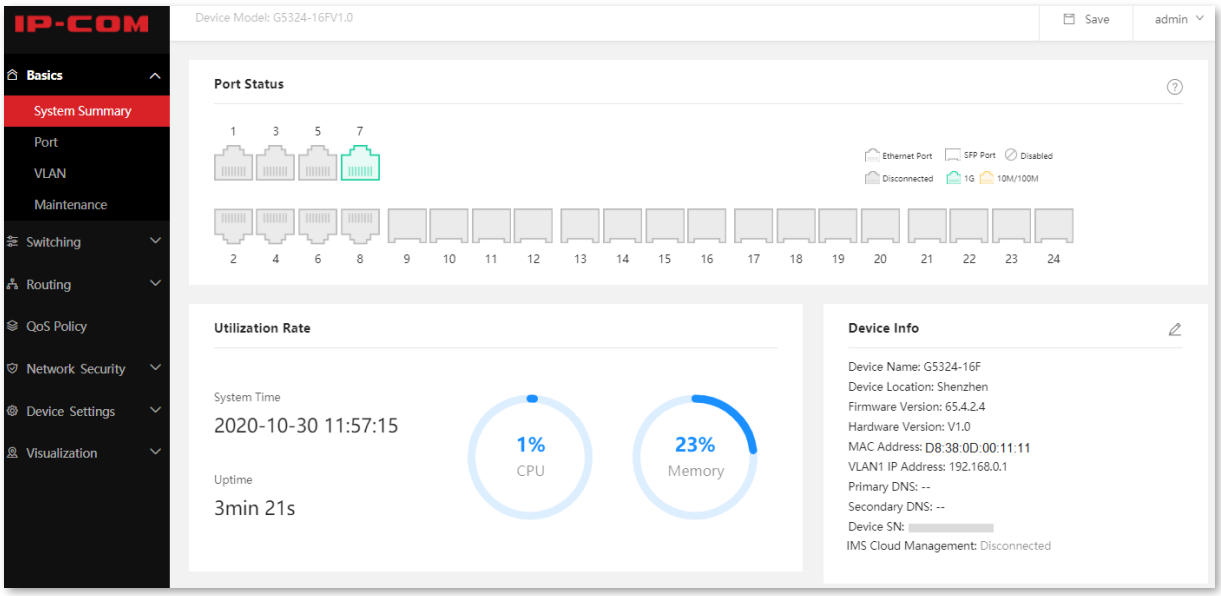
2.2 Common buttons

Common buttons	Description
	Used for refreshing displayed contents on the current page.
	Used for configuring the settings on the current page in batches.
	Used for saving the configurations on the current page and enabling the configurations to take effect. Note You can click Confirm to save the modified configurations temporarily, and they will be cleared after the switch reboots.
	Used for restoring the original configuration without saving the configuration on the current page.
	Used for viewing help information corresponding to the settings on the current page.
	Used for adding new rules on the current page.
	Used for modifying parameters or rules.
	Used for deleting the rules on the current page.
	Used for saving all current configurations of the switch. If you click Save to save the configurations, they still remain after the switch reboots.

3 Basics

3.1 System summary

On the **System Summary** page, you can view the connection status of each port, utilization rate of CPU and memory, system time, and device information.



Parameter description

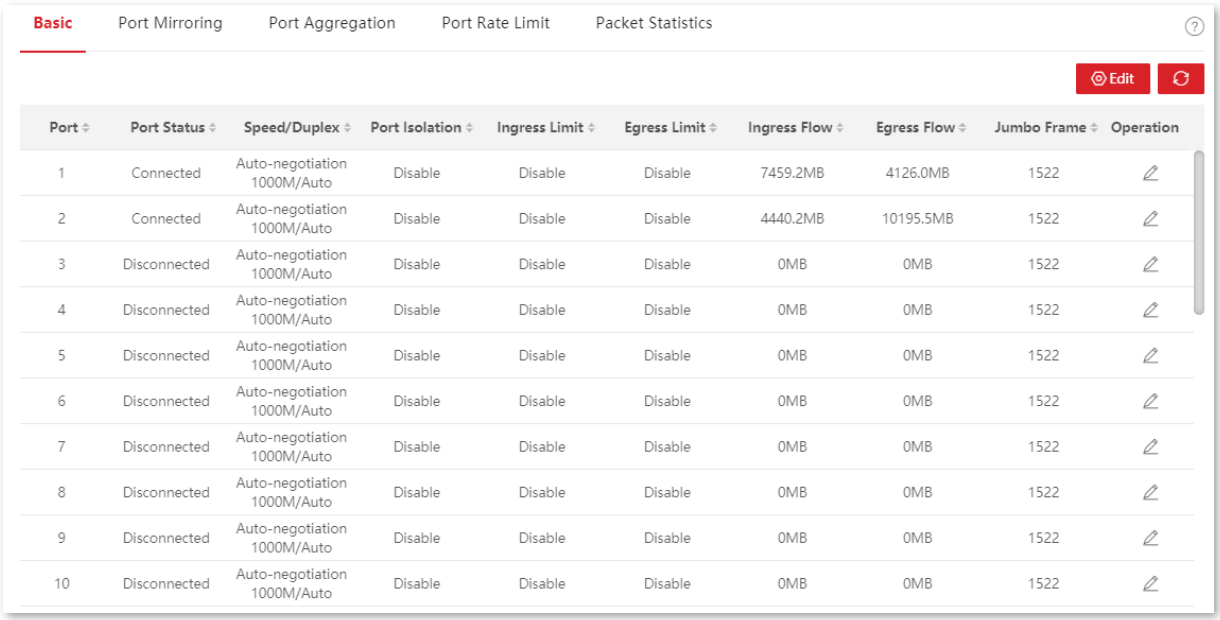
Name	Description
Port Status	It displays the connection status of each port of the switch. indicates an Ethernet (RJ45) port. indicates an SFP port. A green icon indicates that the port is connected to a device and the negotiation rate is 1 Gbps. An orange icon indicates that the port is connected to a device and the negotiation rate is 10 or 100 Mbps. A grey icon indicates that the port is not connected to a device. indicates that the port is disabled.
Utilization Rate	It displays the CPU and memory utilization of the switch.
System Time	It displays the system time of the switch.

Name		Description
Uptime		It displays the time during which this switch is operating since the last reboot.
Device Info	Device Name	It displays the name of the switch, which is the model of the switch by default. You can click to modify it.
	Device Location	It displays the location of the switch, which is Shenzhen by default. You can click to modify it.
	Firmware Version	It displays the firmware version of the switch.
	Hardware Version	It displays the hardware version of the switch.
	MAC Address	It displays the MAC address of the switch.
	VLAN1 IP Address	It displays the IP address of the default VLAN of the switch. The computer belonging to the default VLAN can log in to the web UI of the switch using this IP address.
	Primary DNS	It displays the primary/secondary DNS server address of the switch. The DNS assignment type is set to **Auto** by default. You can click to modify it to **Manual**.
	Secondary DNS	
	Device SN	It displays the device SN info of the switch.
	IMS Cloud Management	It displays whether the switch is connected to the IMS cloud platform.

3.2 Port

3.2.1 Basic

Click **Basics** > **Port** > **Basic** to enter the page. On this page, you can view and configure the basic parameters of the ports.



Port	Port Status	Speed/Duplex	Port Isolation	Ingress Limit	Egress Limit	Ingress Flow	Egress Flow	Jumbo Frame	Operation
1	Connected	Auto-negotiation 1000M/Auto	Disable	Disable	Disable	7459.2MB	4126.0MB	1522	
2	Connected	Auto-negotiation 1000M/Auto	Disable	Disable	Disable	4440.2MB	10195.5MB	1522	
3	Disconnected	Auto-negotiation 1000M/Auto	Disable	Disable	Disable	0MB	0MB	1522	
4	Disconnected	Auto-negotiation 1000M/Auto	Disable	Disable	Disable	0MB	0MB	1522	
5	Disconnected	Auto-negotiation 1000M/Auto	Disable	Disable	Disable	0MB	0MB	1522	
6	Disconnected	Auto-negotiation 1000M/Auto	Disable	Disable	Disable	0MB	0MB	1522	
7	Disconnected	Auto-negotiation 1000M/Auto	Disable	Disable	Disable	0MB	0MB	1522	
8	Disconnected	Auto-negotiation 1000M/Auto	Disable	Disable	Disable	0MB	0MB	1522	
9	Disconnected	Auto-negotiation 1000M/Auto	Disable	Disable	Disable	0MB	0MB	1522	
10	Disconnected	Auto-negotiation 1000M/Auto	Disable	Disable	Disable	0MB	0MB	1522	

Parameter description

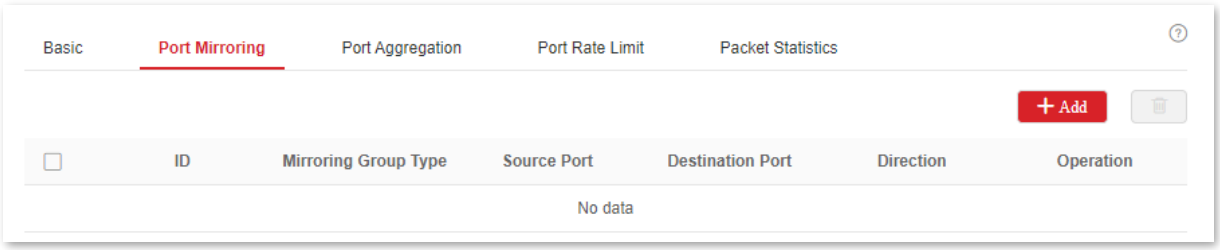
Name	Description
Port	It specifies the ID of the port.
Port Status	It specifies the current connection status of the port, including **Connected**, **Disconnected**, and **Disabled**. – **Connected:** The port is connected to a device. – **Disconnected:** The port is not connected to a device. – **Disabled:** The port is disabled.
Speed/Duplex (Rate/Mode)	It specifies the negotiation speed and duplex mode of the port. – **Auto-negotiation**: The port automatically negotiates the speed and duplex mode with the peer device. – **Mandatory mode**: The speed and duplex mode of the port are fixed. In this mode, the port cannot negotiate the speed and duplex mode with the peer device. – **HDX**: Half duplex mode. – **FDX**: Full duplex mode. – **Auto**: The port can automatically adjust the duplex mode.

Name	Description
Port Isolation	It specifies the isolation group to which the port belongs. Ports belonging to different isolation groups can communicate with each other while ports belonging to the same group cannot. Ports that are not assigned to any isolation group are displayed in the **Disabled** state, indicating that they can communicate with all ports.
Ingress Limit	With the function enabled, the ingress flow of the port will be monitored. When congestion occurs on the ingress port, the switch sends a PAUSE frame to notify the peer device to stop or slow down data transmission, so as to avoid incoming message loss.
Egress Limit	With the function enabled, when the switch receives a PAUSE frame from the peer device, the switch stops or slows down the data transmission of the port to prevent the peer device from discarding messages.
Ingress Flow	It specifies the statistics of data traffic received by the port.
Egress Flow	It specifies the statistics of data traffic transmitted by the port.
Jumbo Frame	It specifies the maximum size of the packet that can be received or transmitted by the port. Packets which exceed this size will be discarded.

3.2.2 Port mirroring

Port mirroring is a method of copying and sending data from a port or multiple ports (source ports) to a specified port (destination port) of the switch. The destination port is usually connected to a data monitoring device, enabling you to monitor data traffic, analyze performance, and diagnose faults.

Click **Basics > Port > Port Mirroring** to enter the page. On this page, you can configure the port mirroring rules.



Parameter description

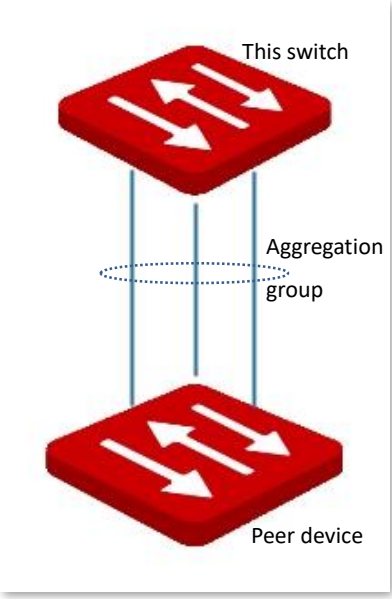
Name	Description
ID	It specifies the ID of the mirroring group.
Mirroring Group Type	This switch only supports local mirroring group types.
Source Port	It specifies the ports whose packets will be copied. Multiple ports can be selected.
Destination Port	Packets of source ports will be copied to this port. A mirroring group can contain only one destination port.

Name	Description
Direction	It specifies the packet type. – **Ingress**: Packets received by source ports will be copied to the destination port. – **Egress**: Packets transmitted by source ports will be copied to the destination port. – **Two-way**: Packets transmitted and received by source ports will be copied to the destination port.

3.2.3 Port aggregation

Port aggregation is used to converge multiple physical ports into a logical aggregation group. Multiple physical links in one aggregation group are regarded as one logical link. The Port Aggregation function binds multiple physical links into one logic link and enables them to share traffic load for each other, thus increasing the bandwidth between the switch and the peer device. Meanwhile, each member in an aggregation group backs up each other's data dynamically, improving connection reliability.

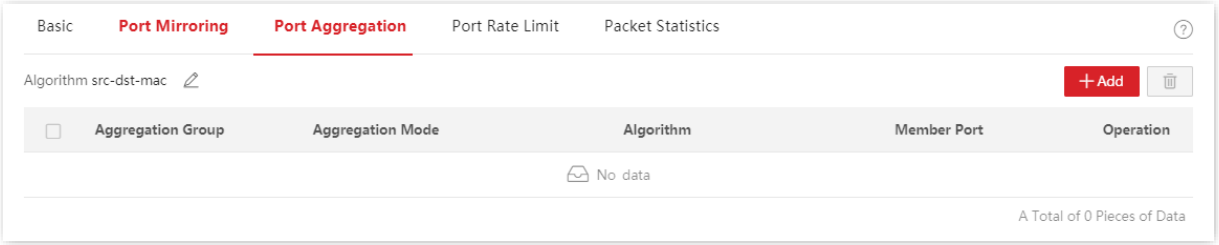
The network topology of port aggregation is as shown below.



Note

In the same aggregation group, all member ports must be set to the same configurations with respect to STP, QoS, VLAN configuration and port management.

Click **Basics** > **Port** > **Port Aggregation** to enter the page. On this page, you can configure the port aggregation rules.

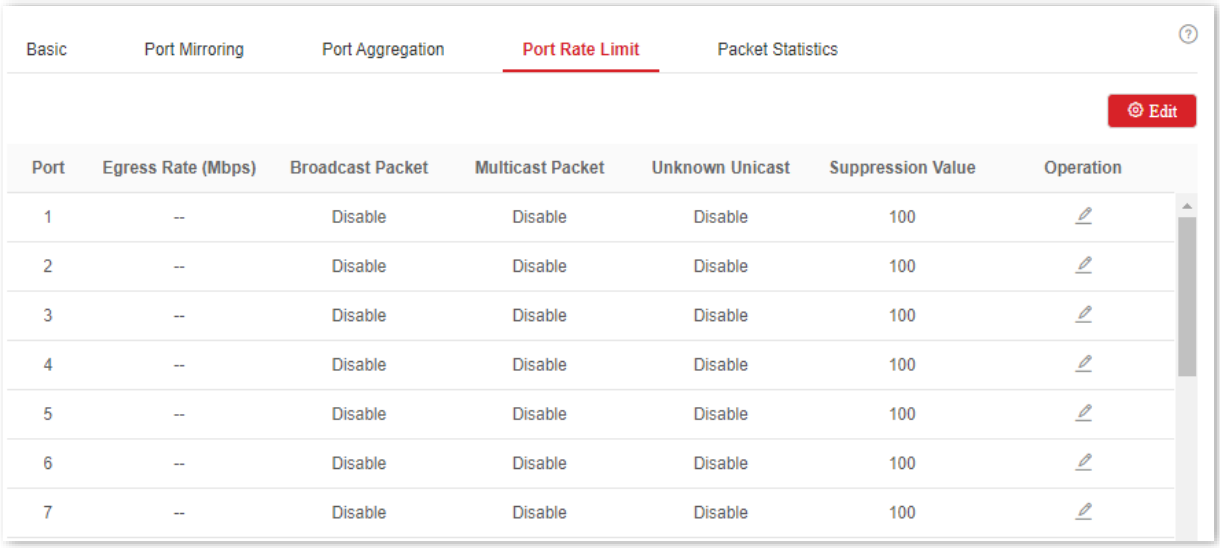


Parameter description

Name	Description
Aggregation Group	It specifies the ID of the aggregation group.
Aggregation Mode	There are two aggregation modes: **Static Aggregation** and **Dynamic Aggregation**. – **Static Aggregation**: All member ports in the aggregation group converge into one logical port. – **Dynamic Aggregation**: LACP (Link Aggregation Control Protocol) for all member ports in the aggregation group is enable, and the actual aggregated ports must be determined together with the peer device through LACP. Note The aggregation mode of the switch needs to be the same as that of the peer device. Otherwise, the data cannot be forwarded properly or the loops occur.
Algorithm	It specifies the routing algorithms for the aggregation group: – **src-dst-mac**: Member ports in the aggregation group share the load according to the source MAC address and destination MAC address in the received packet. – **src-dst-ip**: Member ports in the aggregation group share the load according to the source IP address and destination IP address in the received packet. – **src-dst-mac-ip-port**: Member ports in the aggregation group share the load according to the source MAC address, destination MAC address, source IP address, destination IP address, TCP/UDP source port number and TCP/UDP destination port number in the received packet.
Member Port	It specifies the members of an aggregation group. – In the static aggregation mode, the member ports are members of an aggregation group. – In the dynamic aggregation mode, the member ports are the ports with LACP enabled, and the actual aggregated ports must be determined together with the peer device through LACP.

3.2.4 Port rate limit

Click **Basics** > **Port** > **Port Rate Limit** to enter the page. On this page, you can configure the egress rate of the port and set the rate suppression value of receiving broadcast, multicast and unknown unicast packets for each port.

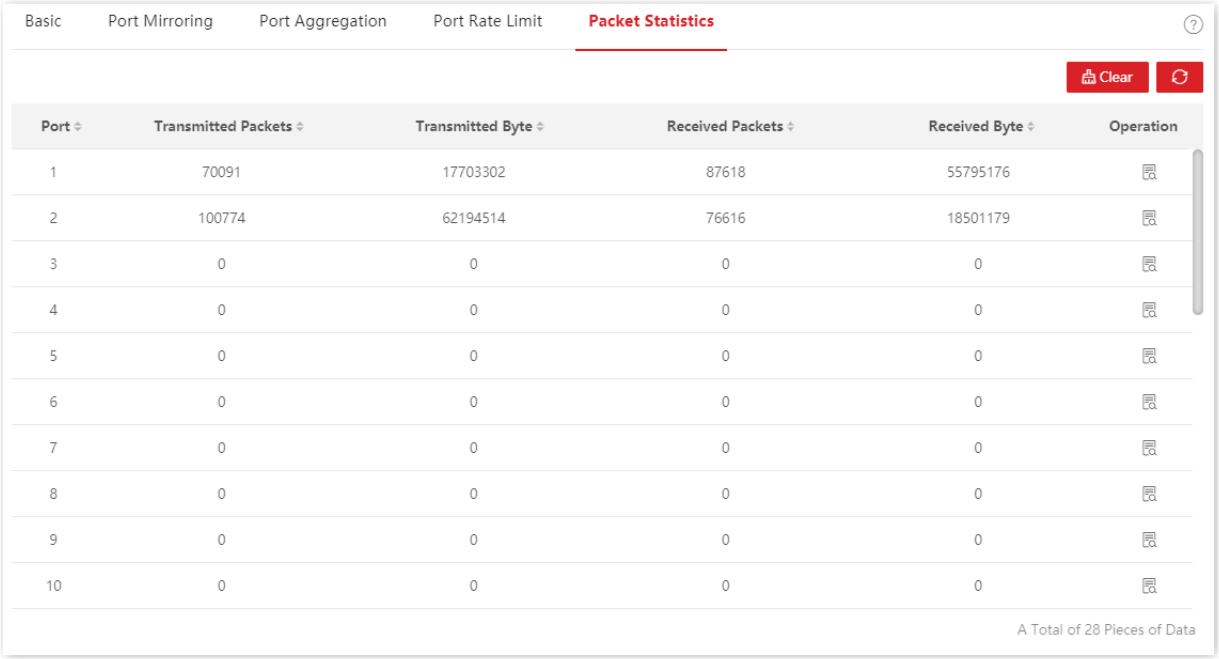


Parameter description

Name	Description
Port	It specifies the ID of the port.
Egress Rate (Mbps)	It specifies the maximum egress rate of the port. "--" stands for no rate limit.
Broadcast Packet	It displays whether the broadcast packet suppression function is enabled or disabled.
Multicast Packet	It displays whether the multicast packet suppression function is enabled or disabled.
Unknown Unicast	It displays whether the unknown unicast packet suppression function is enabled or disabled.
Suppression Value	It specifies the total rate at which broadcast, multicast and unknown unicast packets are allowed to pass by when the suppression function is enabled. There is no suppression when the suppression function is disabled or the suppression value is greater than the ingress or egress rate.

3.2.5 Packet statistics

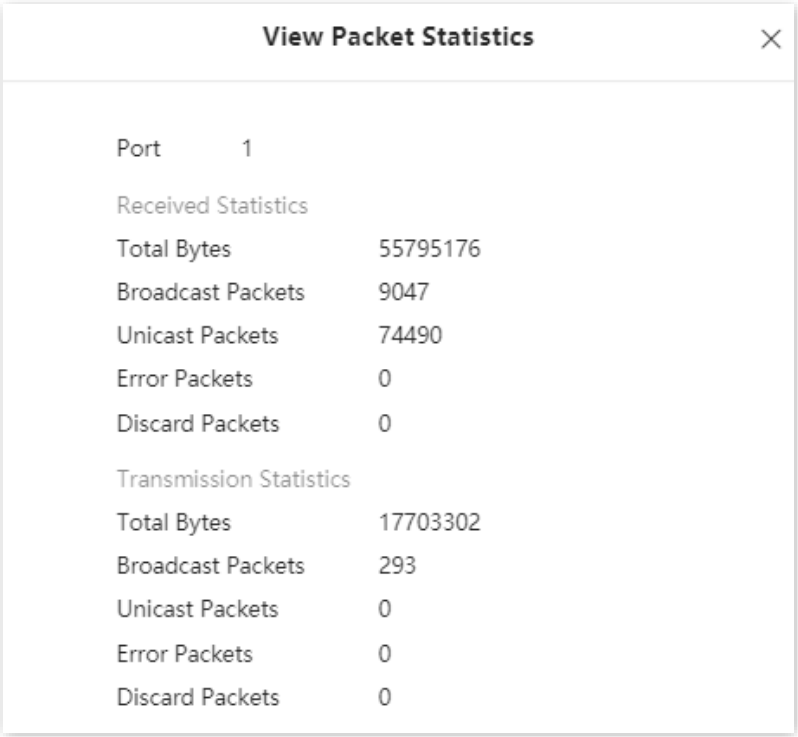
Click **Basics** > **Port** > **Packet Statistics** to enter the page. On this page, you can view and delete the statistics of packets received and sent by each port.



Parameter description

Name	Description
Port	It specifies the ID of the port.
Transmitted Packets	It specifies the total packets sent by a port.
Transmitted Byte	It specifies the total bytes sent by a port.
Received Packets	It specifies the total packets received by a port.
Received Byte	It specifies the total bytes received by a port.

To view the details of packets received and sent by a port, please click the button behind the port.



Parameter description

Name	Description
Total Bytes	It specifies the bytes received/sent by the port.
Broadcast Packets	It specifies the number of the broadcast packets received/sent by the port.
Unicast Packets	It specifies the number of the unicast packets received/sent by the port.
Error Packets	It specifies the number of the error packets received/sent by the port.
Discard Packets	It specifies the number of the discarded packets when the port is receiving/sending packets.

3.3 VLAN

3.3.1 Overview

VLAN (Virtual Local Area Network) is a technology that divides devices in LAN into different logical, instead of physical, network segments to form virtual working groups. VLANs allow a network station constituted by switches to be logically segmented into different domains for broadcast isolation. All members in a VLAN are treated as in the same broadcast domain and communicate as if they were on the same network segment, regardless of their physical locations. Different VLANs cannot intercommunicate directly. Inter-VLAN communication can only be achieved using a router or other layer-3 devices that are able to perform layer-3 forwarding.

The switch supports 802.1Q VLAN and can communicate with devices that support 802.1Q VLAN in VLAN as well.

802.1Q VLAN is defined by IEEE 802.1q protocol. With 802.1Q VLAN, the switch can process messages by identifying the tags in messages.

This switch supports three 802.1Q VLAN port types:

- Access: An access port belongs only 1 VLAN, generally used for connecting the computer.
- Trunk: A trunk port can receive and send messages belonging to multiple VLANs. Usually, a trunk port is used for switches connection.
- Hybrid: A hybrid port can receive and send messages belonging to multiple VLANs. Usually, a hybrid port is used for switches connection, and can be connected to a computer.

Methods of each port type to process packets are shown as follows.

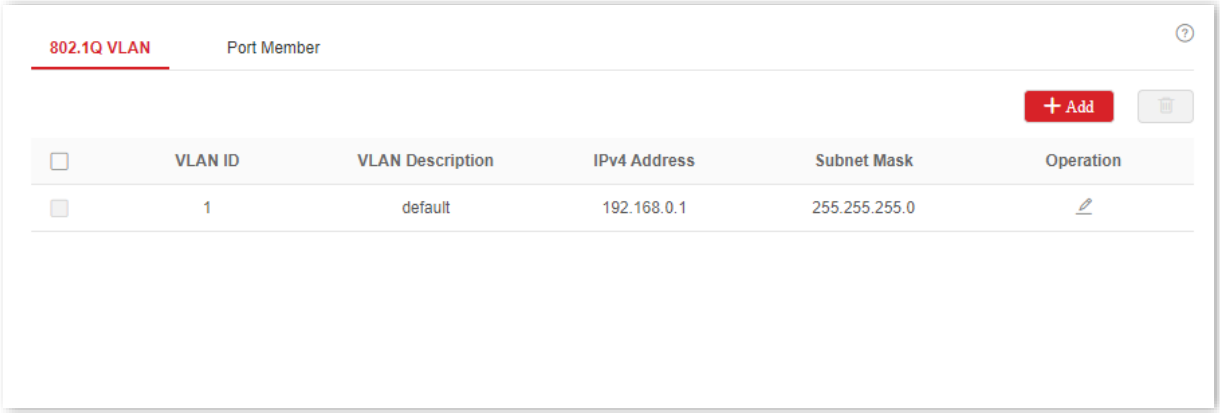
Port Type	Receiving tagged data	Receiving untagged data	Sending data
Access port	Forward to other ports in the corresponding VLAN according to the VID in the tag.	Forward to other ports in the corresponding VLAN according to the PVID on this port.	Messages are forwarded after the tags are removed.
Trunk port			If the VID value of the message is the same as its PVID value, the message is forwarded after the tags are removed. Otherwise, forward it with its tags remained.
Hybrid port			If the VID value of the message belongs to the tagged VLAN, the message is forwarded with its tags remained; if the VID value of the message belongs to the untagged VLAN, the message is forwarded after the tags are removed.

3.3.2 VLAN configuration

Configure 802.1Q VLAN rules

A VLAN rule is created by default to ensure communication between switches in factory settings. All ports are set to be members of this VLAN by default with the VLAN ID of 1 and the IP address of 192.168.0.1. This rule cannot be deleted.

Click **Basics** > **VLAN** > **802.1Q VLAN** to enter the page. On this page, you can configure the rules of 802.1Q VLAN.

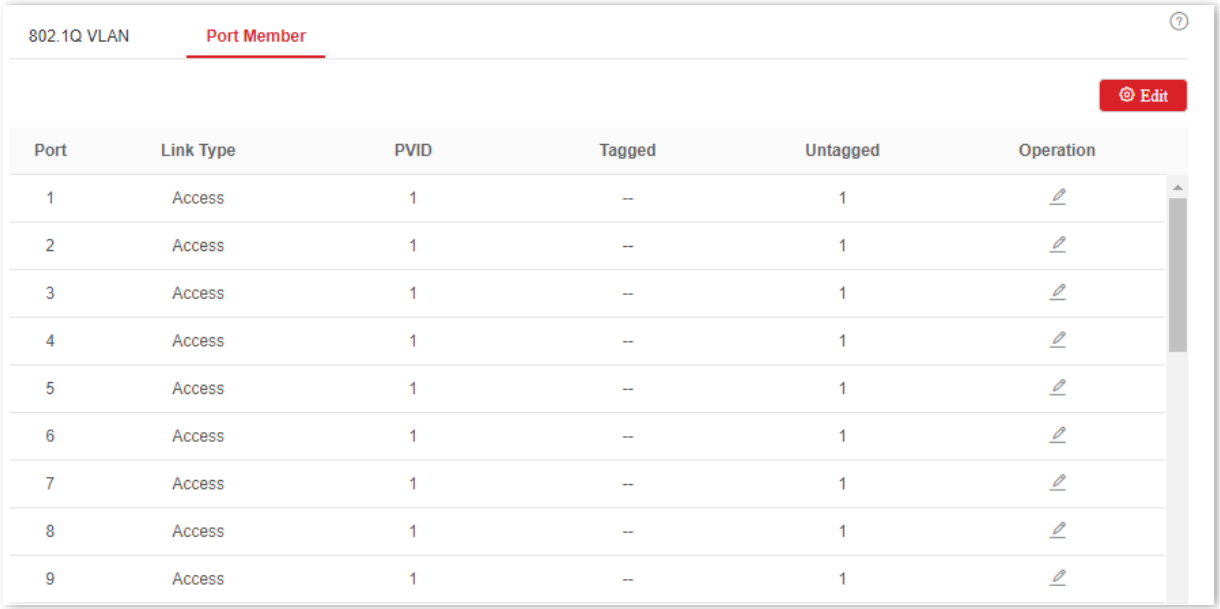


Parameter description

Name	Description
VLAN ID	It specifies the VLAN ID, used for identifying the VLAN to which the packet belongs.
VLAN Description	It is used to identify VLAN groups. If it is not set, the default description is "VLAN and four-digit VLAN ID". For example, when VLAN ID is 3, the VLAN description is VLAN0003.
L3 Virtual Interface	After the L3 virtual interface is enabled, you can configure the IP address and subnet mask for the VLAN interface. After the IP address information is configured, the communication between VLANs can be realized through static routes.
IP Obtaining Type	It specifies the type that the VLAN interface employs to obtain an IP address. – **Manual**: Manually configure the IP address and subnet mask for the VLAN interface. – **DHCP**: Automatically obtain the IP address info from the DHCP server.
IPv4 Address	It specifies the IP address of the VLAN interface. The IP address of the VLAN interface can be configured only when the L3 Virtual Interface is enabled. Devices connected to ports in the VLAN group can use this IP address to log in on the Web UI of the switch.
Subnet Mask	It specifies the subnet mask of the VLAN interface.

Configure port members

Click **Basics** > **VLAN** > **Port Member** to enter the page. On this page, you can configure the PVID and Tag treatment policies of each port to realize VLAN isolation.



Parameter description

Name	Description
Port	It specifies the ID of the port.
Link Type	Three VLAN link types are supported: **Access**, **Trunk**, and **Hybrid**. – **Access**: An access port only belongs to 1 VLAN and transmits untagged messages. It is commonly used to connect to terminals, such as computers. – **Trunk**: A trunk port can receive and transmit messages belonging to multiple VLANs, usually used as a cascade-connected port between switches. – **Hybrid**: A hybrid port can receive and transmit messages belonging to multiple VLANs. A hybrid port can be used as a cascade-connected port between switches, or to connect to terminals.
PVID	It specifies the default VLAN ID of a port. When receiving untagged packets, the port forwards them to the corresponding VLAN based on the PVID of the port itself.
Tagged	If the VID of the tagged packets received by the port is the same with the tagged VLAN, the port retains the tags of the packets and transmit them.
Untagged	If the VID of the tagged packets received by the port is the same with the untagged VLAN, the port removes the tags of the packets and transmit them.

3.3.3 Example of 802.1Q VLAN configuration

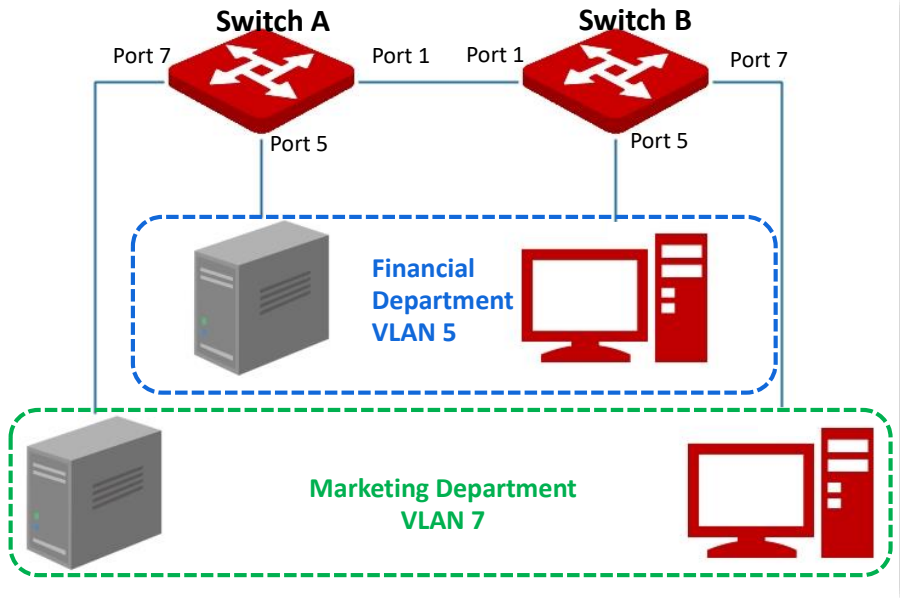
Networking requirement

The staff in the financial department and marketing department of a company work on the second floor, while the servers for these two departments are on the third floor. Now it is required that the communication is available within each department and the servers can be accessible respectively, but the two departments cannot communicate with each other.

Solution

Configure 802.1Q VLAN for two switches:

- Create two VLANs for the switches. Assign the ports connected to the financial department's devices to VLAN 5, and the ports to the marketing department's devices to VLAN 7.
- Add the ports that connect two switches to both VLAN 5 and VLAN 7.



Configuration procedure

Ⅰ. Configure Switch A

1. Add VLANs.

   (1) Log in to the web UI of Switch A and click **Basics** > **VLAN** > **802.1Q VLAN**.

   (2) Click **Add** and enter the following information on the pop-out window, and then click **Confirm**.

   - Set **VLAN ID** to **5**.

– Set **VLAN Description** to **Finance**.

(3) Repeat step (2) and add another VLAN with the **VLAN ID** of **7** and **VLAN Description** of **Marketing**.

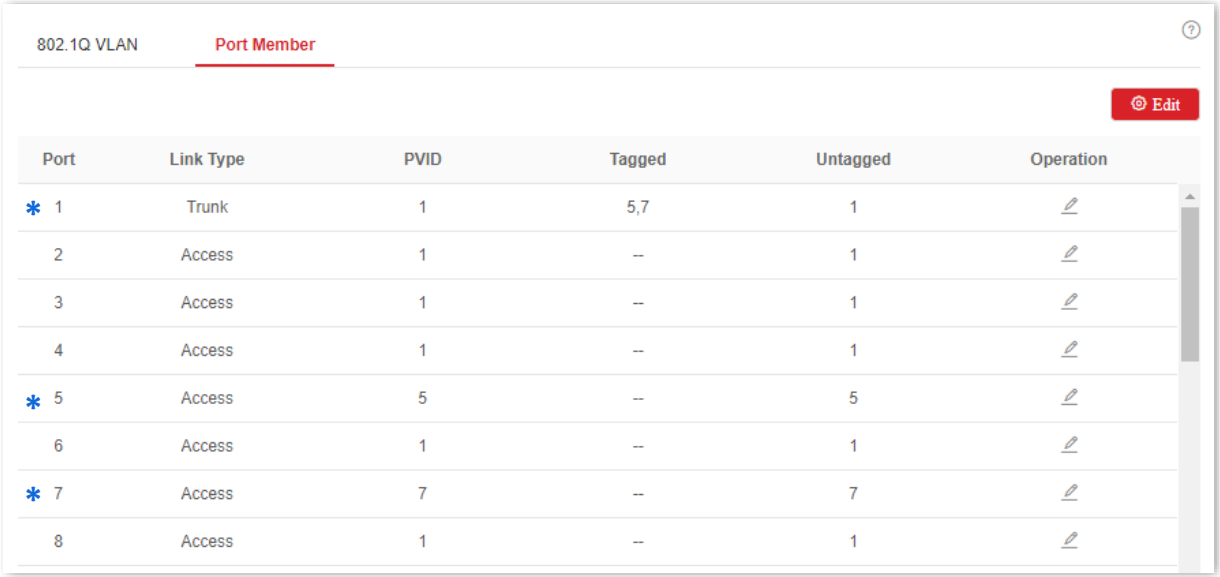
2. Configure port attribute.

(1) Click **Basics** > **VLAN** > **Port Member**.

(2) Click the button behind port 5 and set **PVID** to **5**.

(3) Click the button behind port 7 and set **PVID** to **7**.

(4) Click the button behind port 1 to set **Link Type** to **Trunk** and **Tagged** to **5, 7**.



II. Configure Switch B

Refer to the steps of configuring Switch A.

----End

Verification

The staff can access the server of their department, but cannot access the server of the other department. The staff in the same department can communicate with each other but cannot communicate to the staff of other departments.

3.4 Maintenance

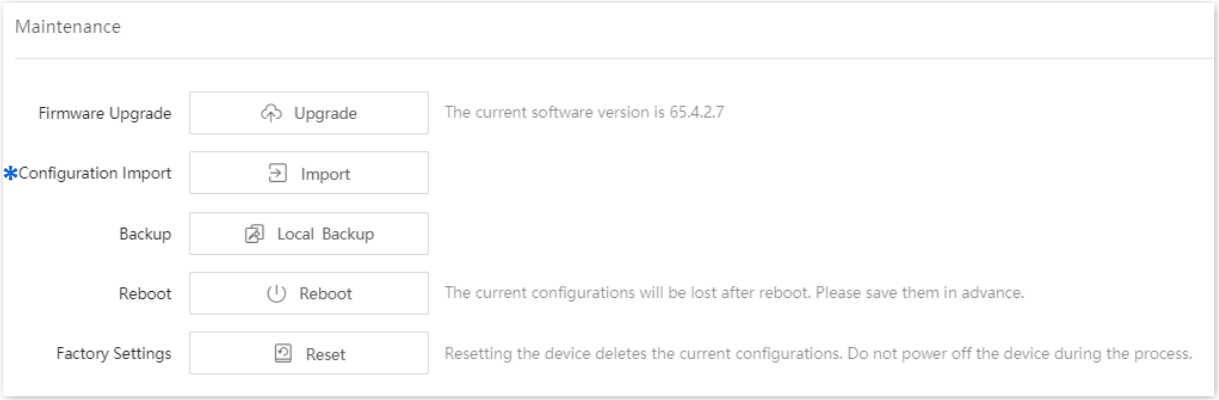
3.4.1 Firmware upgrade

Click **Basics** > **Maintenance** to enter the page. On this page, you can click **Upgrade** to update the switch's firmware, enjoying a better user experience.

Note

To avoid damages to the switch, ensure that the switch is upgraded properly. Please note that:

- Before upgrading, you can download the latest firmware of the switch on the IP-COM official website: www.ip-com.com.cn. Generally, the filename extension of the upgrading file is .bin.
- During the upgrading process, ensure stable power supply to the switch.

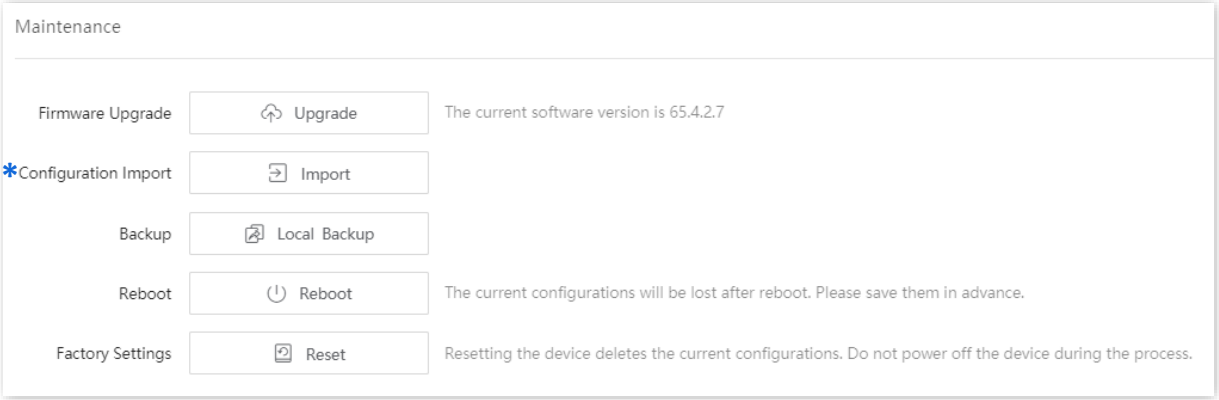


3.4.2 Configuration import

Click **Basics** > **Maintenance** to enter the page. On this page, you can click **Import** to import the backup configuration file to the switch.

Note

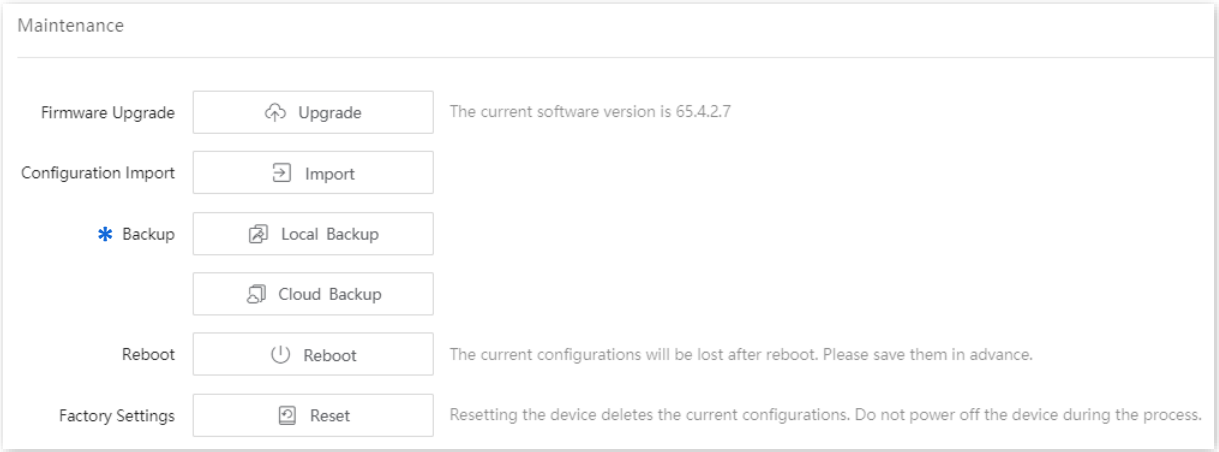
The switch does not verify the contents of the configuration file, so ensure that the file is correct before import.



3.4.3 Backup

If you have made a lot of configurations to the switch for better performance in a specific operating environment, it is recommended to back up the switch's configurations. After you upgrade the switch or restore the switch to factory settings, you can import this backup configuration file to restore the configurations to the switch.

Click **Basics** > **Maintenance** to enter the page. On this page, you can back up the switch's configuration information to the local computer or the IMS cloud platform.



Note

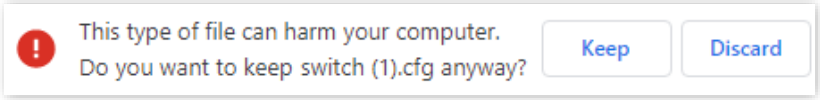
- Please click **Save** on the upper right corner of the page to save all settings before backup.
- Only when the switch is managed by the IMS cloud platform can the configurations be backed up to the IMS cloud platform.

Local backup

To save the configurations of the switch to the local computer, click **Local Backup**. A file named **switch.cfg** will be downloaded.

Tip

If a security prompt appears as below, just click **Keep** to download the backup file.



Cloud backup

To save the configurations of the switch to the IMS cloud platform, click **Cloud Backup**.

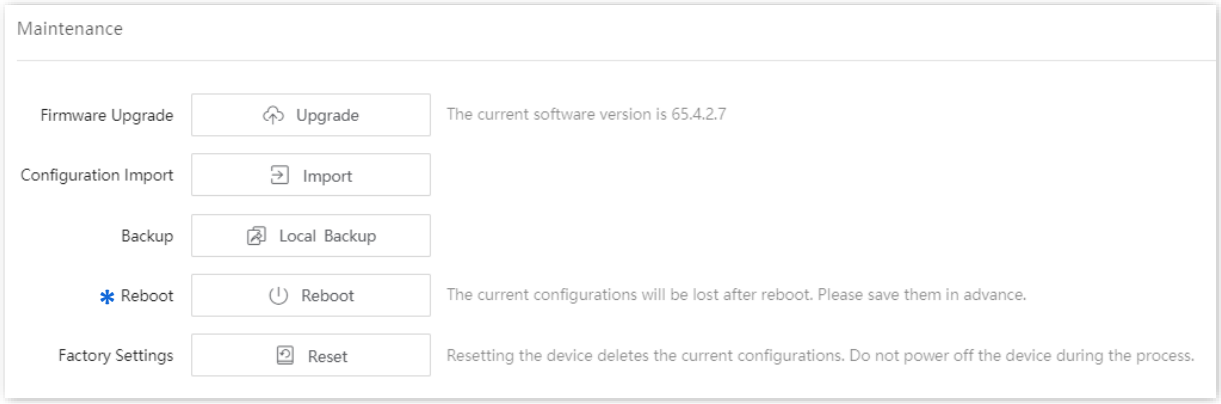
3.4.4 Reboot

When a parameter you set does not work properly, you can try to reboot the switch to fix this issue.

Click **Basics** > **Maintenance** to enter the page. On this page, you can click **Reboot** to restart the switch.

Note

Please click **Save** on the upper right corner to save all settings before rebooting the switch.



3.4.5 Factory settings

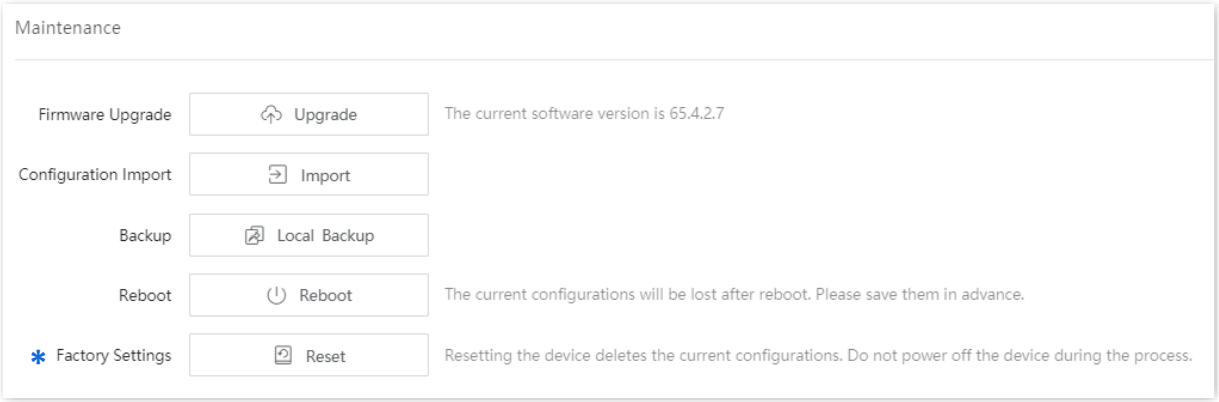
If you forget your username or password when you log in to the web UI of the switch, you can restore the factory settings of the switch, and then use the default username and password (both are **admin**) to log in. This switch supports Software reset and Hardware reset.

Software reset

Click **Basics** > **Maintenance** to enter the page. On this page, you can click **Reset** to restore the switch to factory settings.

Note

To avoid any damages, please ensure stable power supply to the switch during the resetting process.



Hardware reset

When the **SYS** LED indicator is blinking, press down the reset button (**Reset**) using a sharp item (such as a pin) for about 10 seconds, and then release it when all indicators are solid on. When the **SYS** LED indicator blinks again, the switch is restored to factory settings.

4 Switching

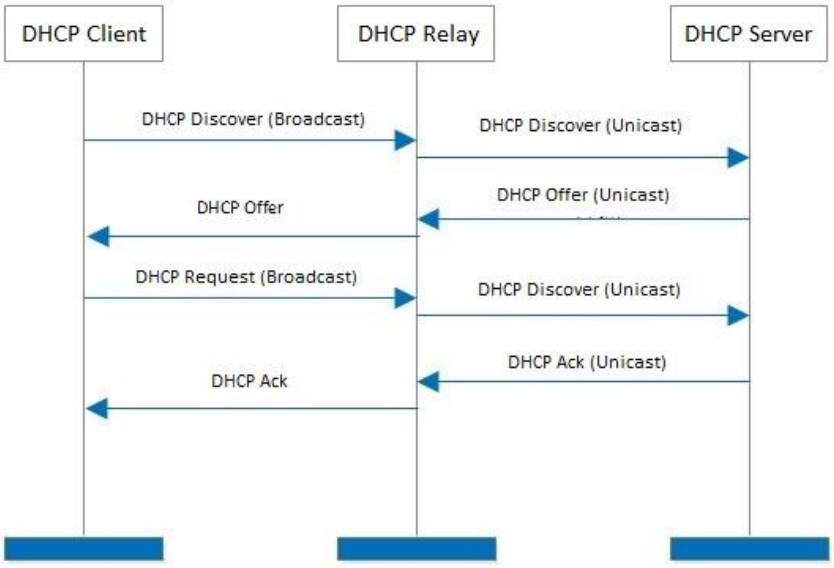
4.1 DHCP relay

4.1.1 Overview

The basic network model of DHCP requires the client and server in the same LAN. In a network with multiple VLANs, it is necessary to configure a DHCP server for each VLAN, which is of high cost.

With the DHCP Relay function enabled, the switch can provide relay service to DHCP server and DHCP clients in different network segments, and forward DHCP protocol messages across multiple VLANs, enabling DHCP clients in multiple VLANs to share one DHCP server.

The working principles of DHCP Relay are as shown below.



- When the DHCP relay receives the DHCP discover or DHCP request messages sent by DHCP clients in broadcast, it fills in the IP address of DHCP relay with the giaddr field in the message, and forwards the message to the specified DHCP server in unicast according to the configuration.
- The DHCP server selects the IP address with the same address segment in the address pool according to the giaddr field in the message, and sends the response message with this IP address information to DHCP relay.

- When DHCP relay receives a response message from the server, the DHCP relay removes the Option 82 field in the packet and broadcasts the DHCP response message to the interface network of the relay device.

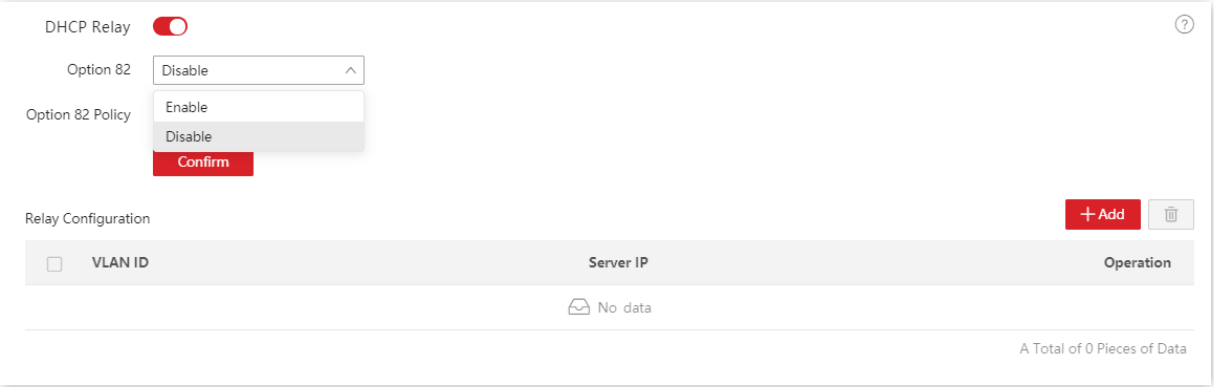
Option 82, also called the DHCP Relay Agent Information Option, is an option in DHCP message that records the location Information of the DHCP clients. You can use this option to locate the DHCP client, thus implementing security and charging control for clients. The corresponding IP address and parameter allocation policies can also be configured on the DHCP server according to the Option 82 information, thus flexibly allocating the IP address.

By default, the Option 82 of this switch is disabled. After it is enabled, the working mechanism of Option 82 of this switch are shown as follows.

Type of received messages	Processing policy
DHCP request message without Option 82	Add the default content of this switch to the Option 82 information of the DHCP request message, and forward the message.  The default content of this switch includes the ID of the port that receives the request packet from the DHCP client, the MAC address of the DHCP client and its VLAN.
DHCP request message with Option 82	DHCP request messages are processed according to the following configuration policies. - **Replace**: Replace the original information of the Option 82 in the message with the default content of the switch, and forward it. - **Retain**: Retain the original state of the Option 82 in the message and forward it. - **Discard**: Discard the DHCP request packet with the Option 82 and forward the DHCP request message without Option 82.
DHCP response message	Delete Option 82 from the DHCP response packet and forward the message.

4.1.2 Configure DHCP relay

Click **Switching** > **DHCP Relay** to enter the page. On this page, you can configure the DHCP Relay rules.



Parameter description

Name	Description
Option 82	It is used to enable or disable the Option 82 policy. Option 82 records the location info of DHCP clients. The Option 82 policy takes effect only when the Option 82 is enabled.
Option 82 Policy	The switch supports three policies. – **Replace**: When the DHCP Relay receives DHCP request messages, it replaces the original Option 82 info with the default content of the switch and forwards the messages. – **Retain**: When the DHCP Relay receives DHCP request messages, it retains the original Option 82 state and forwards the messages. – **Discard**: The DHCP Relay discards the DHCP request message with the Option 82, and forwards the DHCP request message without Option 82.
VLAN ID	It specifies the VLAN to which the clients belong. The VLAN must already exist, and its L3 virtual interface is configured.
Server IP	It specifies the IP address of the remote DHCP server. The IP address of the remote DHCP server cannot belong to the same network segment as that of the VLAN to which the client belongs.

4.2 DHCP snooping

4.2.1 Overview

DHCP Snooping is a security mechanism that protects the DHCP service.

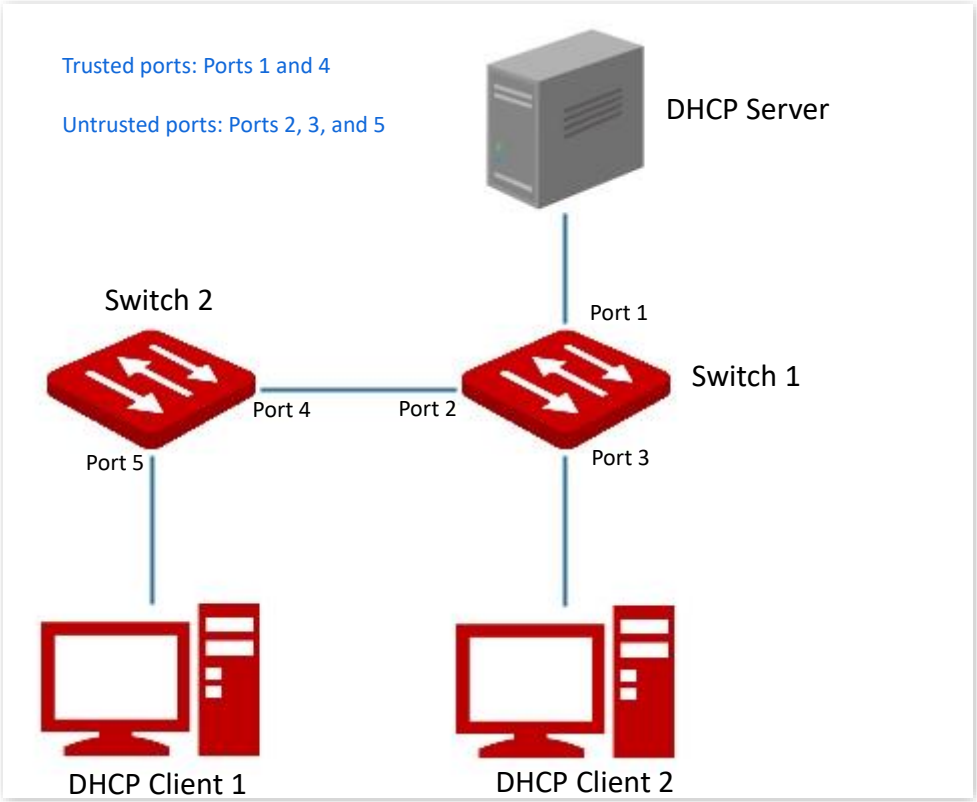
- It ensures that DHCP clients can obtain IP addresses from the correct servers.

  The port connecting to the authorized DHCP server is the trusted port, and other ports are untrusted ports. The switch forwards the DHCP messages received by the trusted ports and discards the response messages received by the untrusted ports from the DHCP server, so as to ensure that the DHCP clients can only obtain the IP addresses from the correct DHCP servers.

- It records the entries of the DHCP Snooping table.

  By snooping DHCP-request message and DHCP-ACK message received by the trusted port, the switch establishes a DHCP Snooping table, which includes the MAC address of the client, the IP address of the DHCP client assigned by the DHCP server, the port connecting the DHCP client, and the VLAN info. The DHCP Snooping table is an important basis for ARP validation.

The network topology of DHCP Snooping is shown in the follow figure. Assume that the DHCP Snooping function of switch 1 and switch 2 is both enabled.

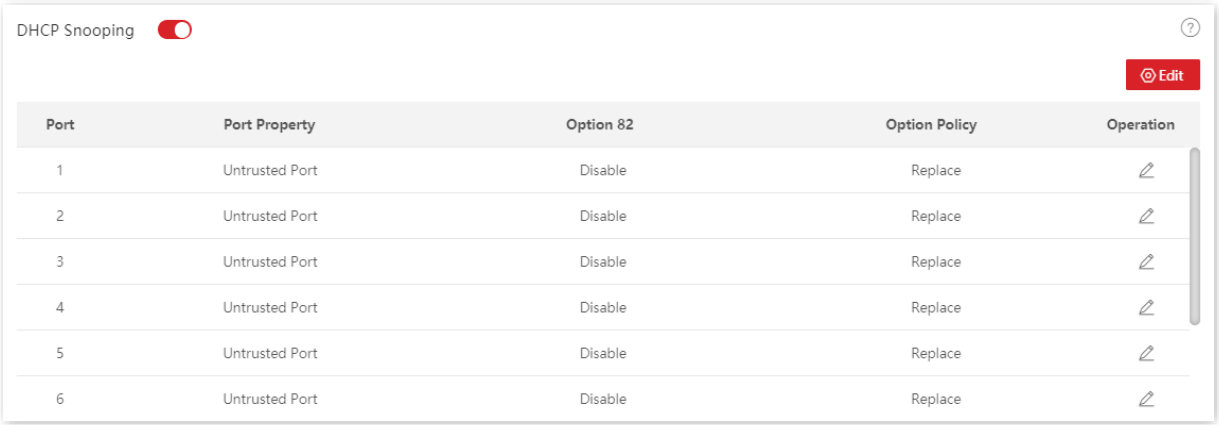


Note

The DHCP snooping function is only available when this function is enabled and the switch is between the DHCP client and DHCP server (or DHCP relay) in the connection network. When the switch is between the DHCP server and DHCP relay, the DHCP snooping function is unavailable.

4.2.2 Configure DHCP Snooping

Click **Switching** > **DHCP Snooping** to enter the page. On this page, you can configure the DHCP Snooping rules.



Parameter description

Name	Description
Port	It specifies the ID of the port.
Port Property	It is used to configure the DHCP snooping property of the current port, including trusted port or untrusted port. – **Trusted port**: It is connected to a legal DHCP server, and forwards received DHCP messages normally. – **Untrusted Port**: After receiving the response messages sent by the DHCP server, the port discards the messages, thus disabling fake DHCP servers erected privately from assigning IP addresses to clients.
Option 82	It specifies the status of Option 82. You can enable or disable the Option 82 function by clicking . Option 82 records the location information of the DHCP client. The option policy takes effect when Option 82 is enabled. Please refer to Option 82 for its working mechanism.

Name	Description
Option Policy	Three Option 82 policies are supported by this switch: – **Replace**: When the DHCP Relay receives DHCP request messages, it replaces the original Option 82 information with the default content of the switch and forwards the messages. – **Retain**: When the DHCP Relay receives DHCP request messages, it retains the original Option 82 state and forwards the message. – **Discard**: The DHCP Relay discard the DHCP request message with the Option 82, and forwards the DHCP request message without Option 82.

4.3 Spanning tree

4.3.1 Overview

Spanning Tree helps avoid loops in the network to protect the network from broadcast storms, and provide link redundancy backup.

This switch supports three spanning tree modes: STP (Spanning Tree Protocol), RSTP (Rapid Spanning Tree Protocol) and MSTP (Multi Spanning Tree Protocol).

STP

STP is a network protocol based on IEEE 802.1d. It is a protocol that ensures a loop-free topology for in local area network and provide backup redundant links. The devices under this protocol discover the loops in the network by communicating with each other, and selectively block some ports, and eventually establish a spanning tree structure without loops, so as to prevent the decline of the message processing capacity of the devices due to the continuous proliferation and endless circulation of messages in the loop network.

STP protocol message

To implement spanning tree function, switches in the network transfer BPDUs (Bridge Protocol Data Unit) between each other to exchange information. BPDUs carry the information that is needed for switches to calculate the spanning tree.

The network topology is determined by BPDU transmission among devices. There are two types of BPDUs of STP protocol:

- Configuration BPDU: It is used for spanning tree calculation and spanning tree topology maintenance.
- TCN BPDU (Topology Change Notification BPDU): It is used to notify the changes of the network topology structure.

Basic concepts of STP

- **Bridge ID**

  The bridge ID contains both bridge priority and MAC address, in which the bridge priority is a configurable parameter. The smaller the bridge ID, the higher the bridge priority. The root bridge is the bridge with the smallest bridge ID.

- **Root bridge**

  Root bridge acts as the root of a tree. There is only one root bridge in the network and it is changeable according to the network topology changes.

  Initially, all devices regard themselves as the root bridges. They generate their own configuration BPDUs and send them out periodically. When the network topology becomes stable, only the root bridge device can send configuration BPDUs out and other devices can

only forward these BPDUs.

- **Root port**

  The root port is the port in a non-root bridge device that has the smallest path cost from the bridge to the root bridge, responsible for communication with the root bridge. There is only one root port on the non-root bridge device and no root port on the root bridge device.

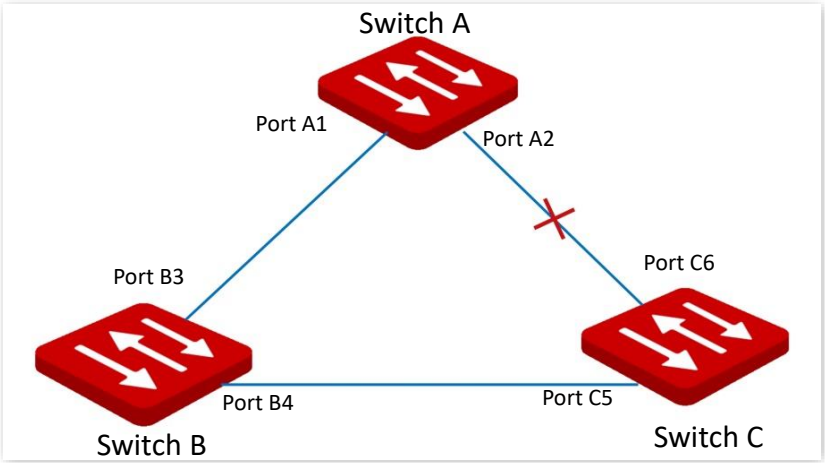
- **Designated bridge and designated port**

  - Designated bridge: For a switch, designated bridge is the device that connects to and forwards BPDUs to the switch. For the LAN, it is the device that forwards BPDUs in the same network segment.
    In each network segment, the device with the least path cost to the root bridge is the designated bridge. If more than one switch has the same path cost to the root bridge, the one with the smallest bridge ID is the designated bridge.
  - Designated port: As for a device, the designated port is the port that forwards BPDUs to the host. As for a LAN, it is the port that forwards BPDUs in the same network segment.

- **Path cost**

  It is a parameter for choosing the link path by STP. By calculating the path cost, STP chooses the better links and blocks the redundant links, so as to disbranch the loop-network to form a tree-topological loop-free network.

  The basic network diagram of STP is shown as the following figure. The switch A, B and C are connected successively.



  After calculation, switch A is selected as the root bridge, and the link between ports A2 and C6 is blocked.

  - Bridges: Switch A is the root bridge of the network, while switch B is the designated bridge of switch C.
  - Ports: Port B3 and port C5 are the root ports of switch B and switch C respectively. Port A1 and port B4 are the designated ports of switch A and switch B respectively. Port C6 is the blocking port of switch C.

BPDU priority in STP mode

The smaller the bridge ID is, the higher the bridge priority is. If the root bridge ID is the same, then the root path costs are compared. The comparison method is to assume the root path cost in BPDU and the path cost corresponding to this port to be S, then the BPDU with smaller S has higher priority.

If the root path costs are the same, compare the designated bridge ID, designated port ID and ID of the port that receives the BPDU successively, one with the smallest ID has higher priority.

STP computing process

1. Initial status

Initially, each port of the switch generates a BPDU regarding the switch as the root bridge, with the root path cost being 0, the ID of the designated bridge being the switch ID, and the designated port being itself.

2. Optimal BPDU selection

Each switch sends out its BPDUs and receives BPDUs from other switches. The following table shows the procedure to select the optimal BPDU.

Step	Content
1	Receiving BPDU with lower priority: If the priority of the BPDU received by a port is lower than that of the port itself, the switch discards the received BPDU and does not deal with the BPDU of that port. Receiving BPDU with higher priority: If the priority of the received BPDU is higher than that of the port itself, the switch replaces the BPDU of the port with the received one.
2	The switch selects the best BPDU by comparing BPDUs on all ports.

3. Root bridge selection

The root bridge is selected by BPDU exchange and root bridge ID comparison. The switch with the smallest root bridge ID is chosen as the root bridge.

4. Root port and designated port selection

The selection procedure is shown in the following table.

Step	Content
1	For each switch (except the root bridge), the port that receives the optimal BPDU is chosen as the root port of the switch.
2	The switch calculates a designated port BPDU for each port according to the root port BPDU and root port path cost. – The ID of the root bridge is replaced with that of the root port. – Root path cost is replaced with the sum of the root path cost of the root port BPDU and the path cost corresponding the root port. – The ID of the designated bridge is replaced with that of the switch itself.

Step	Content
	– The ID of the designated port is replaced with the port ID itself.
3	The switch compares the calculated BPDU with the BPDU of the port whose role requires to be determined, and deal with the port according to different comparison results. – If the calculated BPDU takes the precedence over the BPDU of the port, the port is chosen as the designated port with its BPDU replaced with the calculated BPDU, and regularly sends out the BPDU. – If the BPDU of this ort takes the precedence over the calculated BPDU, the BPDU of this port is not changed and the port is blocked. The port only receives BPDUs but cannot forward BPDU or other data.

In a stable topology, only the root ports and designated ports can forward data, and other ports are blocked. The blocked ports can only receive BPDUs, but not forward data.

STP Timer

- **Hello Time**

  It specifies the interval for the root bridge to send BPDU messages to other switches, used to test if the links malfunction.

- **Maximum Aging Time**

  It specifies the maximum duration during which if a switch does not receive a BPDU message from the root bridge, it sends BPDU packets to all the other switches for recalculate the new STP.

- **Forwarding Delay**

  It specifies the delay time the port state migration takes after the network topology changes.

  Link malfunction leads to STP recalculation in the network, in which case, the STP structure will change accordingly. However, as the new BPDUs cannot be spread to the whole network immediately, the temporal loops might occur if the new root ports and the designated ports forward data at once. Therefore, STP adopts a state migration mechanism, that is, the new root ports and designated ports begin to forward data after twice forwarding delay, which ensures the new BPDUs have been spread to the whole network.

RSTP

RSTP is defined by the IEEE 802.1w standard and downward compatible with IEEE 802.1d STP. In addition to a loop-free network and redundant links, it features with fast convergence. If all bridges in a LAN support RSTP, it enables a rapid topology tree generation when the network topology changes (traditional STP topology tree: 50 seconds, RSTP topology tree: 1 second).

RSTP determines the network topology by exchanging BPDUs among switches. However, the BPDU format of RSTP differs from that of STP. When the topology is changing, RST-BPDU messages are spread by floods to notify the change to the whole network.

Conditions for rapid state migration of the root ports and designated ports in RSTP:

- Root port: The original root port of the switch stops forwarding data and the designated port of the upstream switch begins to forward data.
- Designated port: If the designated port is an edge port, it can directly transit to forwarding state; if the designated port is a P2P port, it can transit to forwarding state once it gets response from the downstream switch through handshake.

- **Edge Port**

An edge port is a designated port on the edge of the switching network. It is directly connected to terminal devices. An edge port can transit to forwarding state immediately without going through listening and learning states. If it receives a BPDU, it immediately turns from an edge port to a common spanning tree port, and joins the STP generation.

- **P2P Port**

A P2P port used to connect to other switches. Under RSTP/MSTP, all ports operating in full-duplex mode are P2P ports.

MSTP

Disadvantages of STP and RSTP in common working environments:

- STP: Ports cannot rapidly transit the states, and even ports on links with point-to-point ports and edge ports can only transit to forwarding states after twice forwarding delay.
- RSTP: It features with fast convergence, but as all VLANs in the LAN share only one spanning tree and all messages of VLANs should be forwarded along this spanning tree. Therefore, the redundant links cannot be blocked by VLANs, and data traffic load cannot be balanced among VLANs.

MSTP is defined by the IEEE 802.1s standard and compatible with STP and RSTP. It not only features fast convergence, but also allows data flows of different VLANs to be forwarded along the paths respectively. These functions lead to better load sharing mechanism for redundant links, and compensate for the limitations of STP and RSTP.

Features of MSTP:

- MSTP supports mapping VLANs to the spanning tree instances through VLAN-to-instance mapping table, and realizes load balancing by mapping multiple VLANs to one instance.
- MSTP divides the spanning tree network into multiple regions, each of which contains internal spanning trees that are independent of one another.
- MSTP prunes a loop network into a loop-free tree network to avoid continuous proliferation and endless circulation of messages, and also provided multiple

redundant paths for data forwarding, thus ensuring load balancing in data forwarding process.

- **MST region**

  The MST region (Multiple Spanning Tree Regions) is made up of multiple devices in a switching network and their network segments.

  These devices have the following features:

  - A spanning tree protocol enabled
  - Same region name
  - Same configuration summary (the configuration of the mapping relationship between VLAN and MSTI is the same)
  - Same MSTP revision level
  - Physically linked together

- **MSTI**

  MSTP can generate multiple independent spanning trees in an MST region, and each spanning tree is regarded as an MSTI (Multiple Spanning Tree Instance). In the MST region, MSTP generates multiple spanning trees according to the VLAN-to-instance mapping table, and maps the VLANs to the spanning trees. The spanning tree calculation method of MSTP is the same with that of STP.

- **IST**

  An IST (Internal Spanning Tree) is a special spanning tree in the MST region. It is commonly called MSTI 0.

- **CST**

  CST (Common Spanning Tree) is a single spanning tree that connects all MST regions within the network. MSTP considers MST regions as separate devices and generates CST connecting to all regions.

- **CIST**

  CIST (Common and Internal Spanning Tree) is a single spanning tree that connects all devices within the network. It consists of the ISTs in all MST regions and the CST.

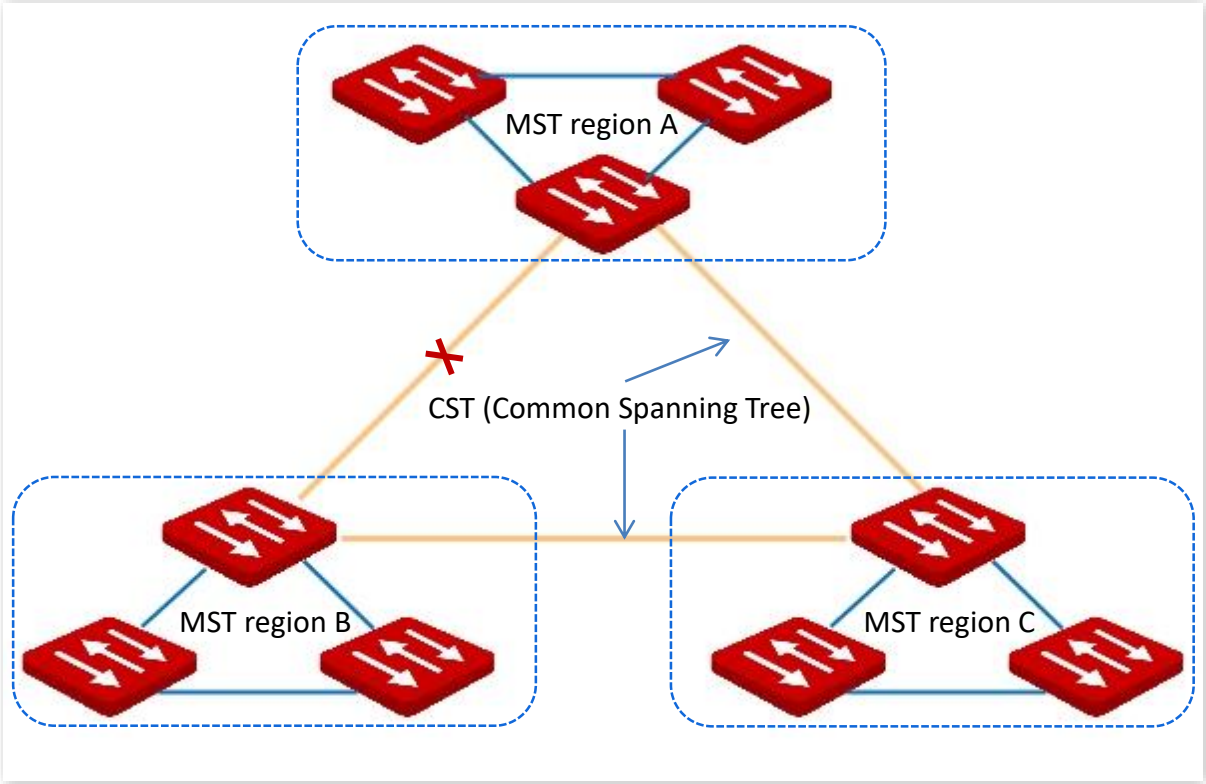
- **Regional Root**

  Regional Root is the root bridge of IST or MSTI within the MST region. Regional roots vary with different spanning tree topologies.

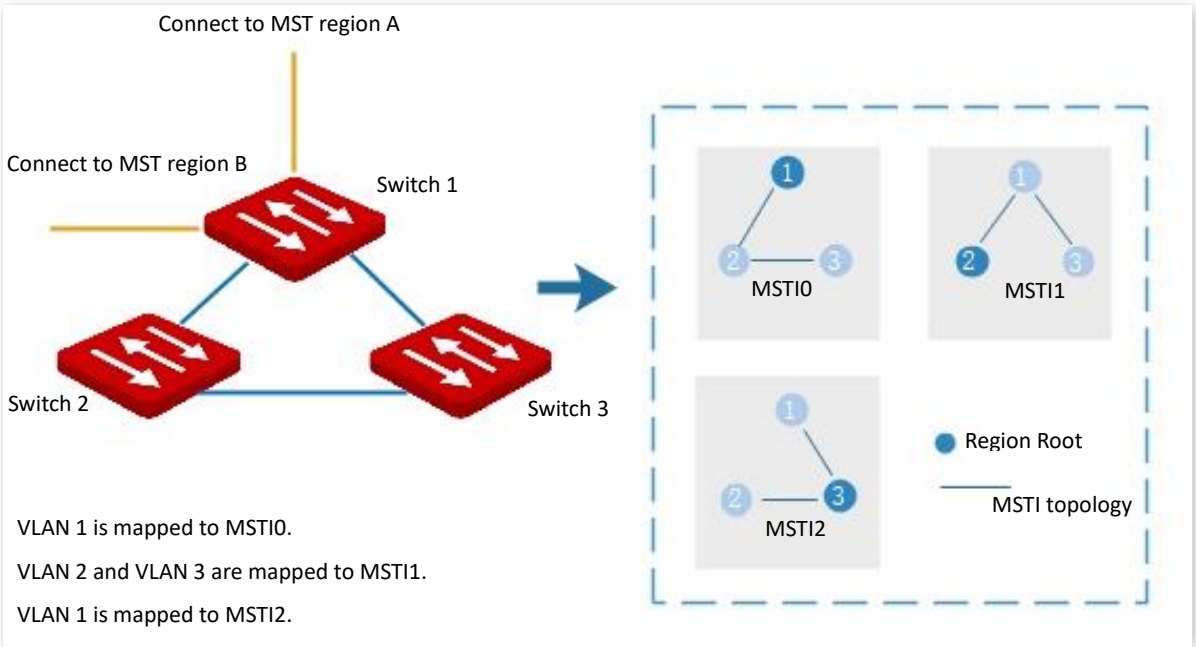
- **Common Root Bridge**

  Common Root Bridge is the root bridge of CIST. Based on BPDUs comparison, MSTP selects an optimal device as the common root bridge in the whole network.

  Similar to STP, MSTP uses BPDUs to calculate spanning trees, except that BPDUs carries MSTP configuration information. The basic concept diagram of MSTP is shown as follows.



The topology of each MSTI in MST region C is as follows.



Port status

In MSTP, port status includes the following four types according to whether the port can forward data and the ways to process BPDUs:

- Forwarding: The port receives and forwards data, receives and sends BPDUs, and learns addresses.

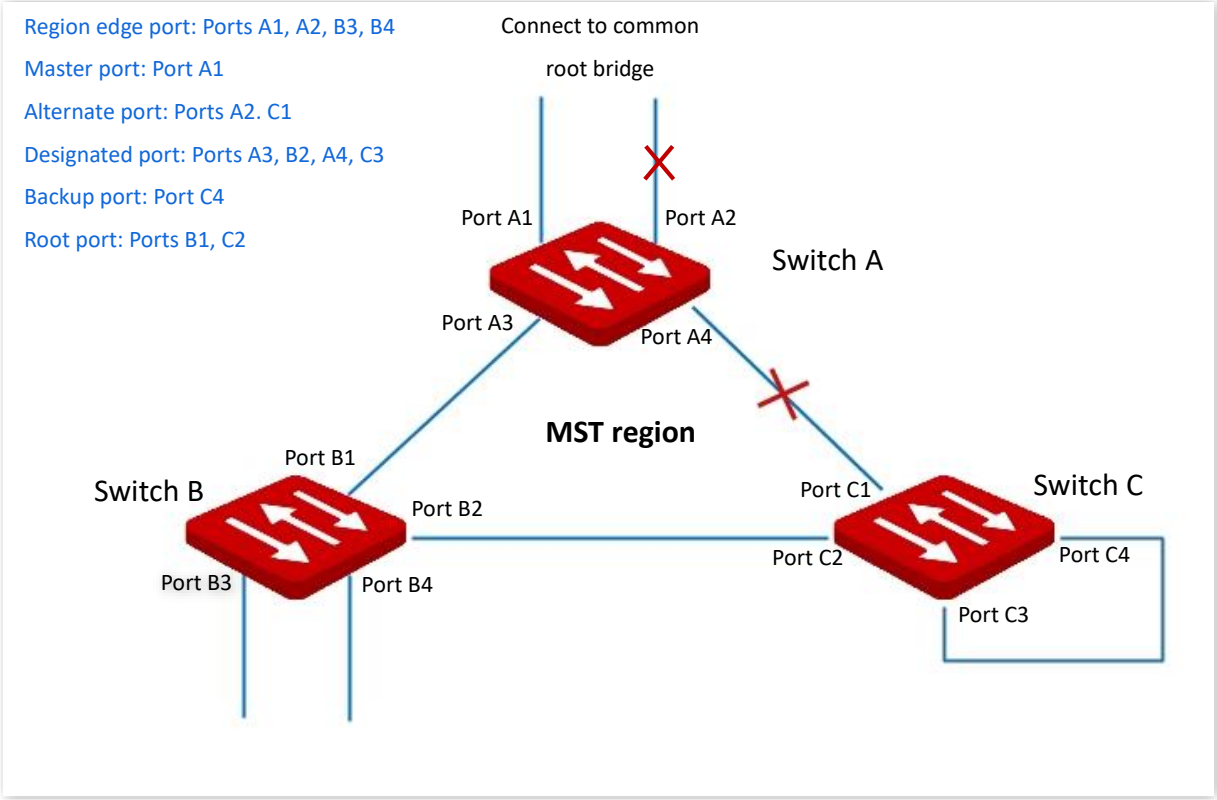
- Learning: The port does not receive or forward data, but receives and sends BPDUs, also learns addresses.
- Discarding: The port neither receives or forwards data, nor sends BPDUs or learns addresses, but receives BPDUs.
- Disabled: The port is not physically linked.

Port role

In MSTP, there are different roles of the ports:

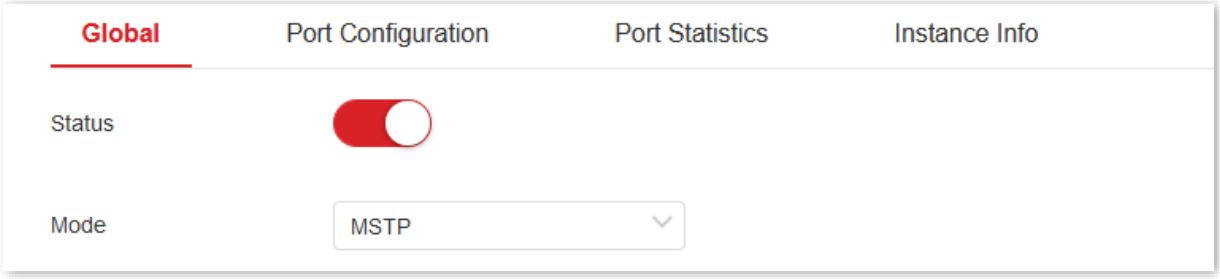
- Root port: It has the least past cost to the root bridge and is responsible for forwarding data from a non-root bridge to the root bridge.
- Designated port: It forwards data to the downstream network segment or device.
- Master port: It is on the shortest path from the MST region to the common root bridge, connecting the MST region to the common root bridge.
- Alternate port: It acts as the backup port for the root port or master port.
- Backup port: It acts as the backup port for the designated port.
- Disable port: It is a port that is not physically linked.

The port roles are shown as the following diagram.



4.3.2 Global

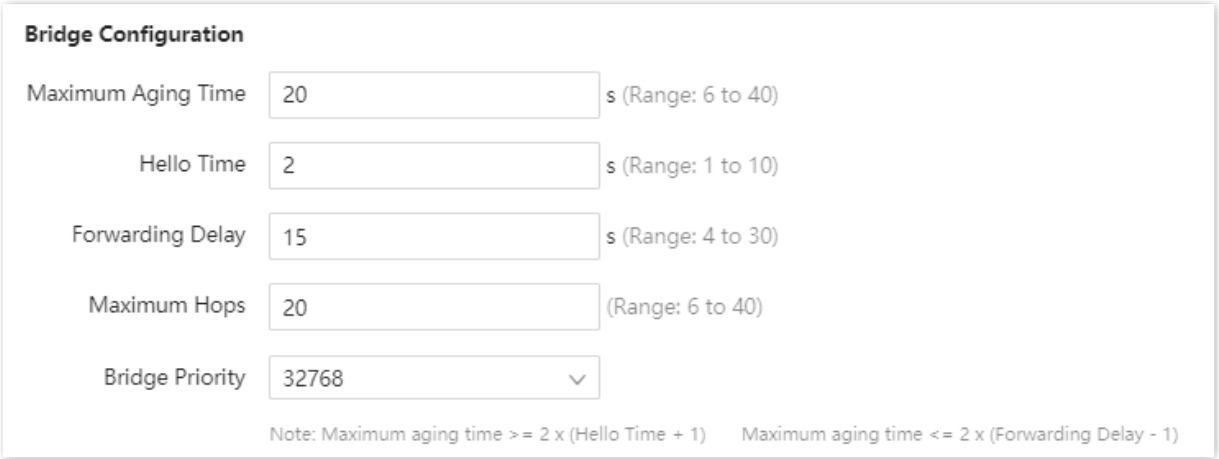
Click **Switching** > **Spanning Tree** > **Global** to enter the page. On this page, you can configure the global parameters of the spanning tree.



Parameter description

Name	Description
Status	It is used to enable or disable the spanning tree function.
Mode	The switch supports three spanning tree modes: STP, RSTP and MSTP. – **STP**: Spanning Tree Protocol. – **RSTP**: Rapid Spanning Tree Protocol, compatible with STP protocol, featuring fast convergence. – **MSTP**: Multiple Spanning Tree Protocol, compatible with RSTP and STP, providing better load sharing mechanism for redundant links.

Bridge Configuration

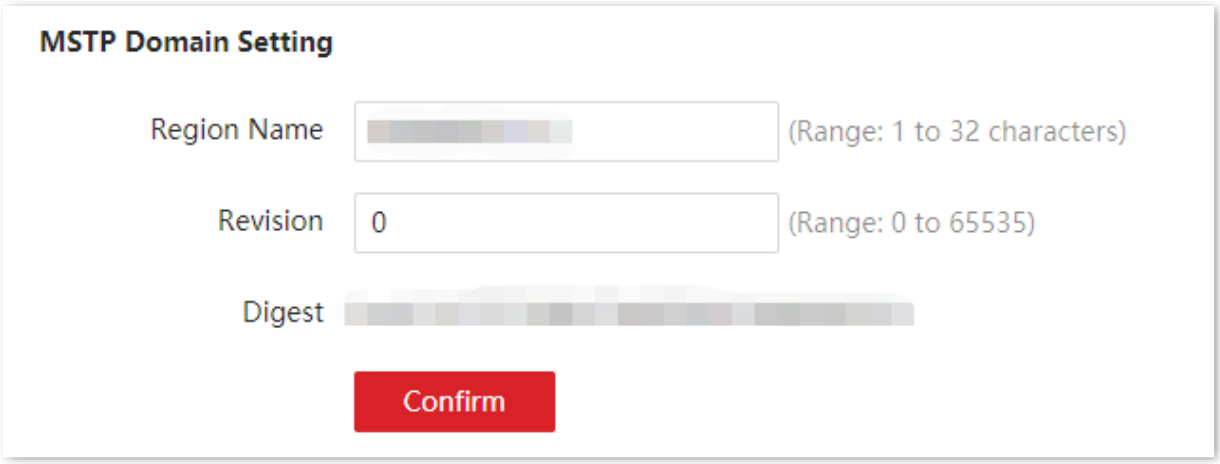


Parameter description

Name	Description
Maximum Aging Time	It specifies the maximum duration during which the BPDU can be kept in the switch. The configuration should meet the following formulas: – Maximum Aging Time ≥ 2 × (Hello Time + 1) – Maximum Aging Time ≤ 2 × (Forwarding Delay - 1)
Hello Time	It specifies the interval at which the switch sends BPDU, which is set to 2 seconds by default.

Name	Description
Forwarding Delay	It specifies the delay that the port state migration takes after the network topology changes, which is set to 15 seconds by default.
Maximum Hops	It specifies the maximum number of the BPDU that can be forwarded, used to limit the scale of the spanning tree.
Bridge Priority	It specifies the system priority of a switch in the participation in the spanning tree calculation. The priority is an important criterion by which the root bridge is determined. Switch with the higher priority will be chosen as the root bridge on equal conditions.

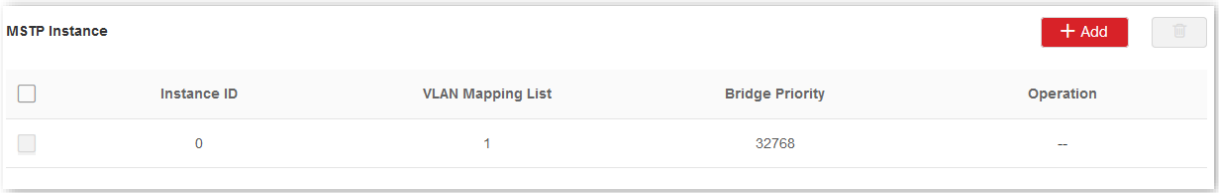
MSTP Domain Setting



Parameter description

Name	Description
Region Name	It specifies the identity of the MST Region. The default value is the MAC address of the switch.
Revision	It specifies the MSTP revision level, which is set to 0 by default.
Digest	It specifies the value calculated based on the VLAN mapping interior.

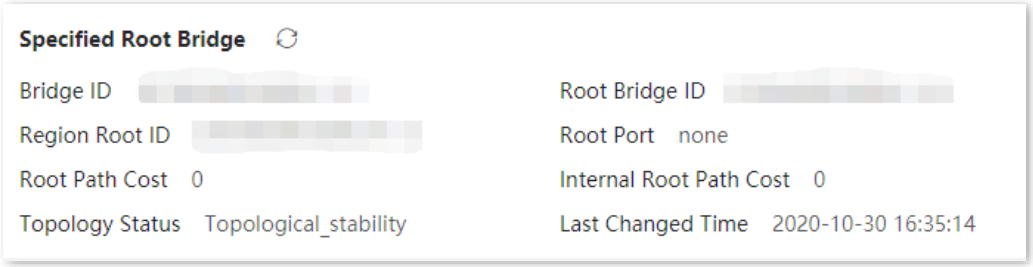
MSTP Instance



Parameter description

Name	Description
Instance ID	A maximum of 32 instances are allowed. 0 indicates internal spanning tree. The spanning tree is calculated by each instance separately.
VLAN Mapping List	It specifies the instance mapping VLAN.
Bridge Priority	It specifies the instance system priority used for root bridge election of instances in MST regions.

Specified Root Bridge

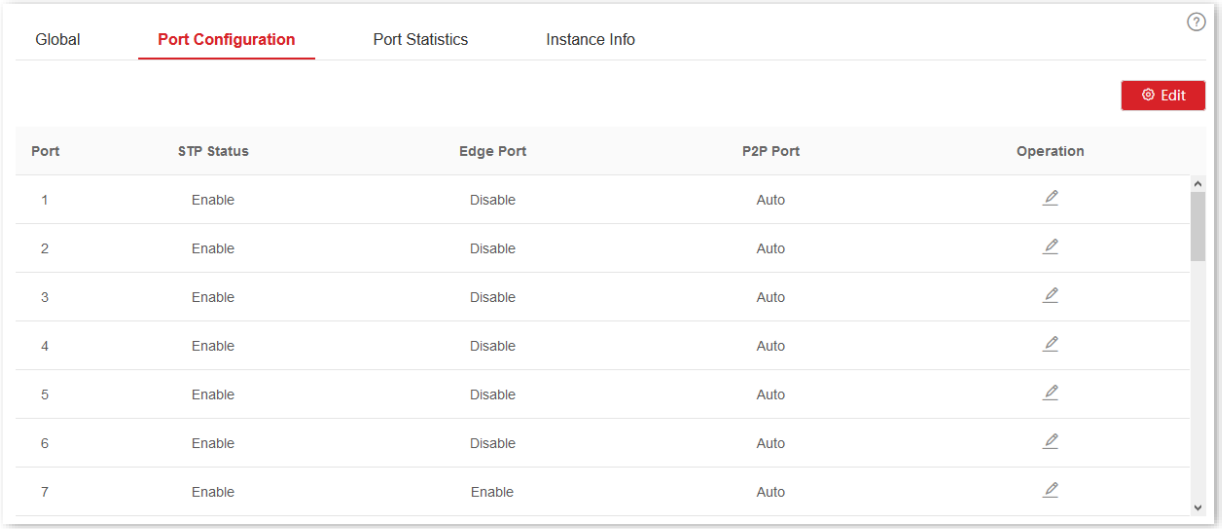


Parameter description

Name	Description
Bridge ID	It specifies the bridge priority and bridge MAC address of this switch.
Region Root ID	It specifies the bridge priority and bridge MAC address of the regional root bridge in the region of this switch.
Root Path Cost	It specifies the sum of root port path cost and the root path cost of all switches packets pass by. The root path cost of the root bridge is 0.
Topology Status	It specifies the topology status of the spanning tree of this switch. – **Topology_calculation**: The port is unstable during the calculation of spanning tree, and the packets cannot be forwarded. Commonly, with the default time parameters, the Topology_calculation status can last up to 50 seconds when the mode is STP, while for RSTP and MSTP, the time duration is less than 3 seconds. – **Topological_stability**: The port is stable, and the network is normal.
Root Bridge ID	For STP and RSTP, it specifies the bridge priority and MAC address of the root bridge; while for MSTP, it specifies the bridge priority and MAC address of the common root bridge.
Root Port	It specifies the port nearest to the root bridge on a non-root-bridge switch.
Internal Root Path Cost	It specifies the reference value used to choose path and calculate path cost in the path of MST region. It is also the criterion used in determining whether the port is chosen as the root port. The smaller the value is, the higher the priority will be.
Last Changed Time	It specifies the time of the last topology change.

4.3.3 Port configuration

Click **Switching** > **Spanning Tree** > **Port Configuration**. On this page, you can configure the STP parameters of the ports.

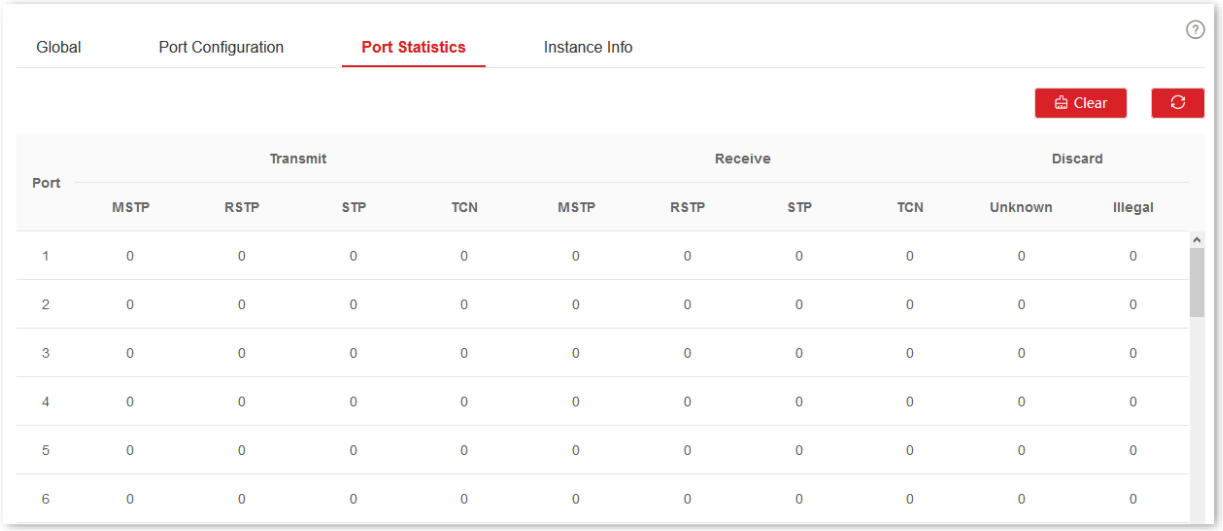


Parameter description

Name	Description
Port	It specifies the ID of the port.
STP Status	It indicates whether the STP function is enabled or not. Only when the STP function in both **Global** and **Port Configuration** is enabled can the port join spanning tree calculation.
Edge Port	The edge port can rapidly migrate to the forwarding state from the congestion state. No need to wait for the delay time. The edge port is commonly connected to terminals. When receiving BPDU messages, the edge port is changed to a non-edge port. All ports are non-edge ports by default. – **Disable**: This port is a non-edge port. – **Enable**: This port is an edge port.
P2P Port	A P2P port can perform fast migration. In RSTP/MSTP mode, all ports in full-duplex mode are considered as P2P ports. The default port automatically identifies links. – **Auto**: P2P port can be automatically identified. – **Enable**: This port is a P2P port. – **Disable**: This port is not a P2P port.

4.3.4 Port statistics

Click **Switching** > **Spanning Tree > Port Statistics** to enter the page. On this page, you can view the spanning tree packets transmitted, received and discarded by each port.

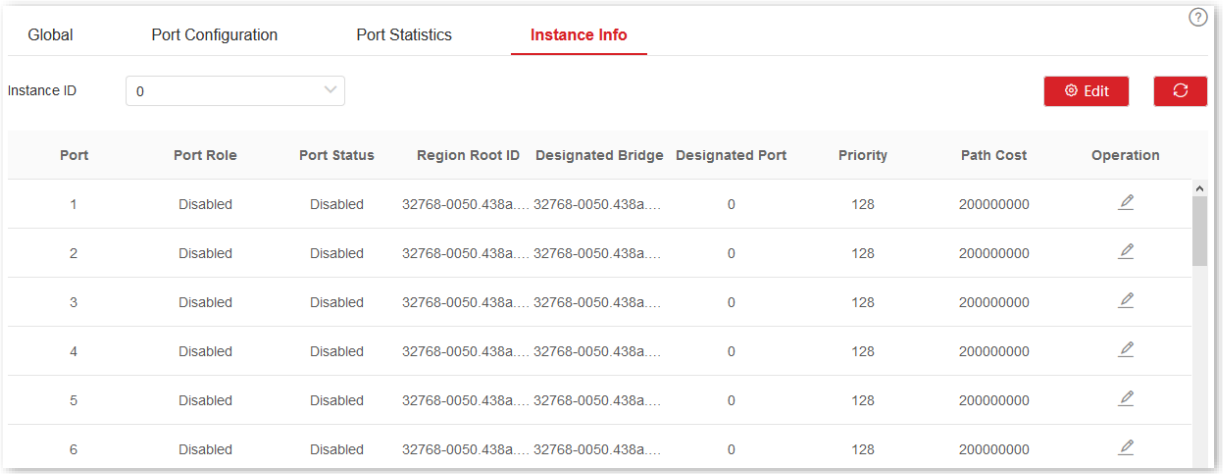


Parameter description

Name	Description
Port	It specifies the ID of the port.
MSTP	It specifies the number of configuration BPDU with MSTP info transmitted or received by the port.
RSTP	It specifies the number of configuration BPDU with RSTP info transmitted or received by the port.
STP	It specifies the number of configuration BPDU with STP info transmitted or received by the port.
TCN	It specifies the number of TCN BPDU message transmitted or received by the port.
Unknown	It specifies the number of discarded unknown STP packets.
Illegal	It specifies the number of discarded error STP packets.

4.3.5 Instance info

Click **Switching** > **Spanning Tree > Instance Info** to enter the page. On this page, you can view and configure the MSTP instance information.



Parameter description

Name	Description
Instance ID	It is used to select the instance ID to check the STP state information of the instance.
Port	It specifies the ID of the port.
Port Role	It specifies the role that the port plays in the spanning tree instance. For more details, please refer to Port role.
Port Status	It specifies the current operating status of the port. For more details, please refer to Port status.
Region Root ID	It specifies the bridge priority and bridge MAC address of the regional root bridge.
Designated Bridge	It specifies the bridge ID of the switch that connects to this switch and is used to forwards BPDU messages to the switch. The designated bridge ID of the root port and backup port is the bridge ID of the switch used to send BPDU messages; while the designated bridge ID of the designated port is the bridge ID of the switch itself.
Designated Port	It specifies the port to which the designated bridge forwards BPDU messages.
Priority	It specifies the priority of the port in spanning tree calculation. When the root bridge ID, root path cost, and bridge ID are the same, priority is an important criterion to determine whether the port is selected as the root port. The smaller the value of the priority is, the higher the priority will be.
Path Cost	It is a reference value used to select the paths and calculate the path costs in the instance within the MST region, also a reference for root port selection. The smaller the value is, the higher the priority will be.

4.4 LLDP configuration

4.4.1 Overview

In a multi-vendor environment, a standard protocol is required that allows network devices from different vendors to discover other devices, exchange system and configuration information.

LLDP (Link Layer Discovery Protocol) provides a standard link layer discovery method that organizes the main capabilities, management address, device identifier, and interface identifier info of devices on this side into different TLVs (Type/Length/Value), and encapsulates them in LLDPDUs (Link Layer Discovery Protocol Data Unit) to release to neighbors to which they are directly connected. After receiving these information, the neighbors will save them as the standard MIB (Management Information Base) to enable the network management system to check and judge the link communication conditions.

Basic concepts

- **LLDP message**

  LLDP message is encapsulated with LLDPDU.

- **LLDPDU**

  LLDPDU is a data unit encapsulated in LLDP message. Each LLDPDU is a sequence of type-length-value (TLV) structures.

- **TLV**

  A TLV is an information element of LLDPDU. Each TLV carries one piece of information.

- **Management address**

  The network management system uses the management address to identify and manage the device for topology maintenance and network management. The management address is encapsulated in the management address TLV of the LLDP message.

Operating mechanism

LLDP is a one-way protocol for information notification or retrieval. It notifies an operating method with no requirement of confirmation and unavailable for query.

Main works of LLDP:

- Initialize and maintain information in the local MIB.
- Obtain required information from the local MIB and encapsulate it in the LLDP frames. There are two ways to trigger sending LLDP frames: One is triggered by timer expiration, and the other one is triggered by the device status change.

- Identify and process the received LLDPDU frames.
- Maintain the LLDP MIBs of the remote devices.
- Notify the MIB information changes of the local or remote devices.

- **LLDP operating status**

  There are four LLDP operating statuses:

  - Send & Receive: In this mode, the switch can send and receive LLDP messages.
  - Send Only: In this mode, the switch can only send LLDP messages.
  - Receive Only: In this mode, the switch can only receive LLDP messages.
  - Disabled: In this mode, the switch cannot send or receive LLDP messages.

  When the LLDP operating status changes, its LLDP protocol state machine reinitializes. You can configure **Initialization Delay** to prevent frequent initializations caused by frequent changes of the operating status. If you have configured the **Initialization Delay**, the switch must wait the specified time to initialize LLDP after the LLDP operating status changes.

- **LLDP message transmission mechanism**

  When the operating status of the port is **Send & Receive** or **Send Only,** the switch sends LLDP messages to its neighbor devices periodically.

  When the local device information changes, the switch immediately notifies the changes to neighbor devices by sending LLDP messages. But to prevent LLDP messages from overwhelmingly sent to the network caused by frequent changes of local device information, each LLDP message needs to be delayed for a specific time after the last message is sent.

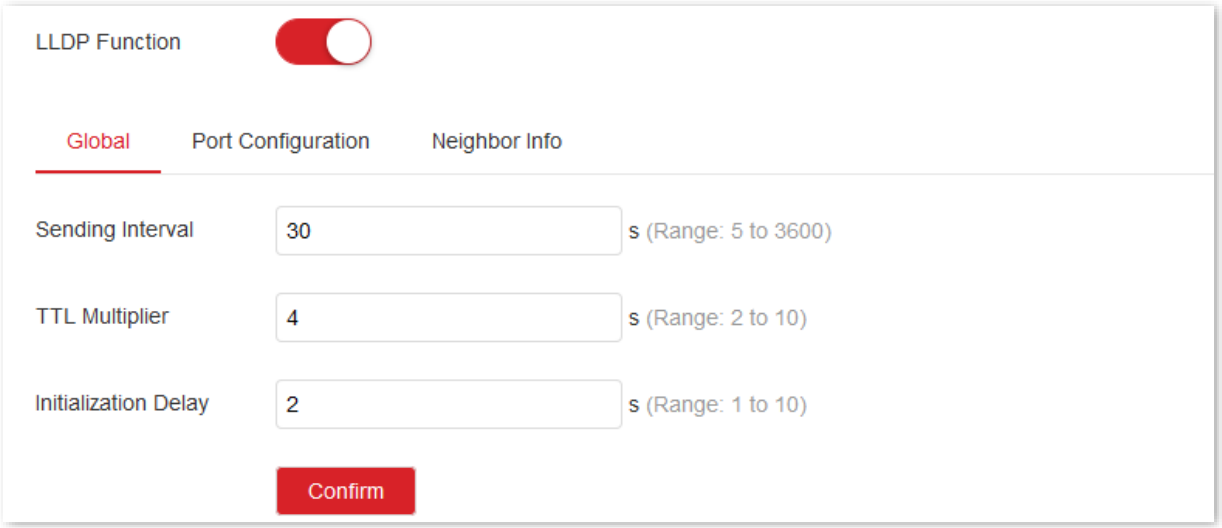
  When the operating status of the port changes from **Disabled** or **Receive Only** to **Send & Receive** or **Send Only**, the switch sends a LLDP message to its neighbor devices immediately.

- **LLDP message receiving mechanism**

  When the operating status of the port is **Send & Receive** or **Receive Only,** the switch confirms the validity of every received LLDP message and its TLVs. After verification, it saves the neighbor device's information and starts an aging timer according to the value of TTL (Time to Live) in Time to Live TLV. If the value is zero, the neighbor device's information ages out immediately.

4.4.2 Global

Click **Switching** > **LLDP Configuration** > **Global** to enter the page. On this page, you can configure the global parameters of LLDP.

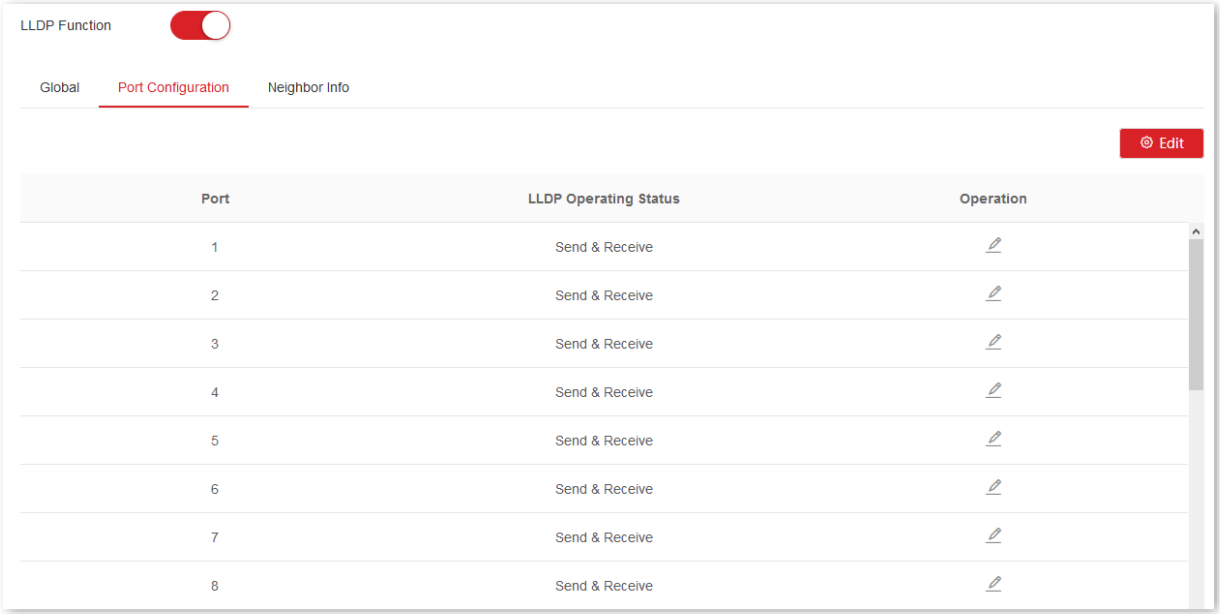


Parameter description

Name	Description
LLDP Function	It is used to enable or disable the LLDP function.
Sending Interval	It specifies the interval at which the switch sends LLDPDUs to neighbors.
TTL Multiplier	The TTL Multiplier is used to control the TTL field value in LLDPDUs transmitted by the switch. The TTL is the duration in which the local info can survive on the neighbor devices. TTL=Min (65535, TTL multiplier x LLDPDU sending interval), indicating the minimum value between 65535 and TTL multiplier × LLDPDU sending interval.
Initialization Delay	To prevent the port from performing initialization continuously as a result of frequent operating status changes, you can configure an initialization delay time for the port which enables the port to perform initialization for the specific time after the operating status changes.

4.4.3 Port configuration

Click **Switching** > **LLDP Configuration** > **Port Configuration** to enter the page. On this page, you can configure the LLDP operating status for each port.

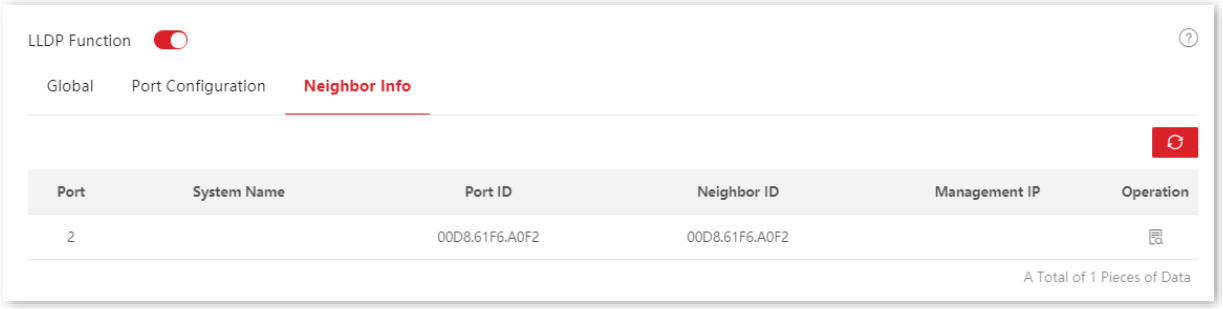


Parameter description

Name	Description
Port	It specifies the ID of the port.
LLDP Operating Status (Port Property)	It indicates the LLDP operating status of each port. – **Disabled**: The LLDP function of this port is disabled. – **Send Only**: The port only sends but not receives LLDP messages. – **Receive Only**: The port only receives but not sends LLDP messages. – **Send & Receive**: The port both sends and receives LLDP messages. – **No Change**: Keep the current configuration.

4.4.4 Neighbor info

Click **Switching** > **LLDP Configuration** > **Neighbor Info** to enter the page. On this page, you can view the neighbor information.



Parameter description

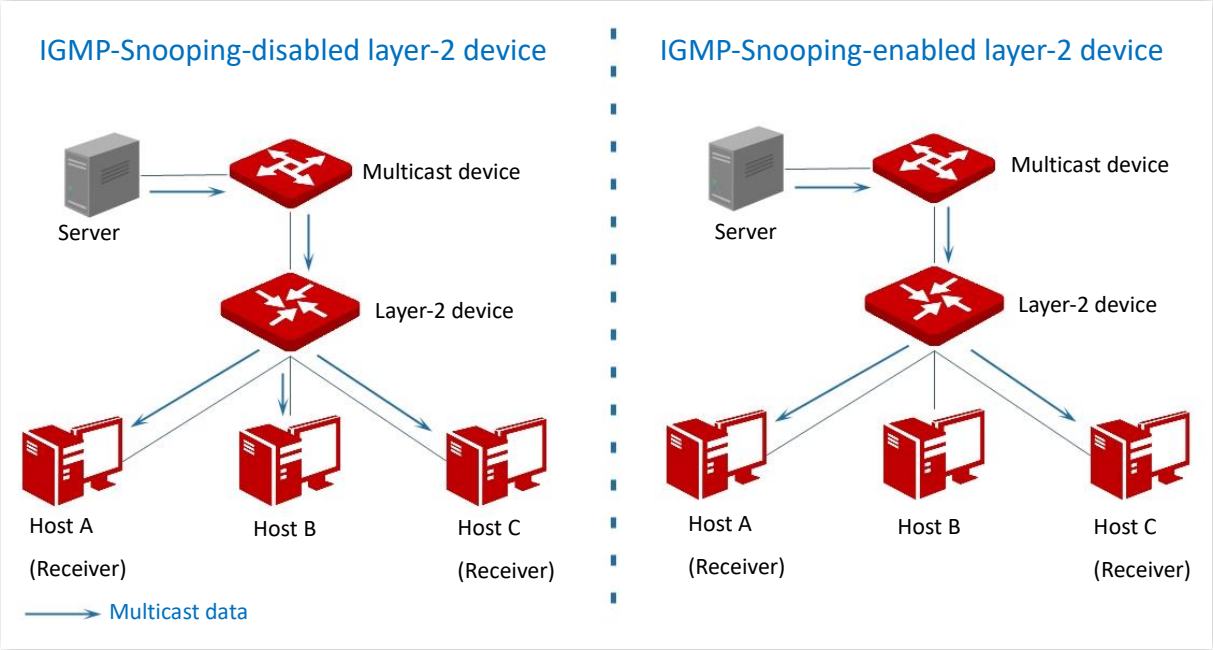
Name	Description
Port	It specifies the ID of the port.
System Name	It specifies the system name of the neighbor device.
Port ID	It specifies the port information of the neighbor device. Tip The port information can be a port number, MAC address, or other information, defined by the information carried in the LLDP message from the neighbor device.
Neighbor ID	It specifies the MAC address of the neighbor device.
Management IP	It specifies the management IP address of the neighbor device.
Survival Time	It specifies the rest of the time that the neighbor info can be saved and displayed on the switch.
Port Description	It specifies the detailed description of the port used to transmit LLDP messages on the neighbor device.
System Description	It specifies the detailed description of the neighbor device.
Performance	It specifies the features supported by the neighbor device.

4.5 IGMP snooping

4.5.1 Overview

IGMP Snooping (Internet Group Management Protocol Snooping) is a multicast constraint mechanism running on the layer 2 Ethernet switches, which is used to manage and control multicast groups.

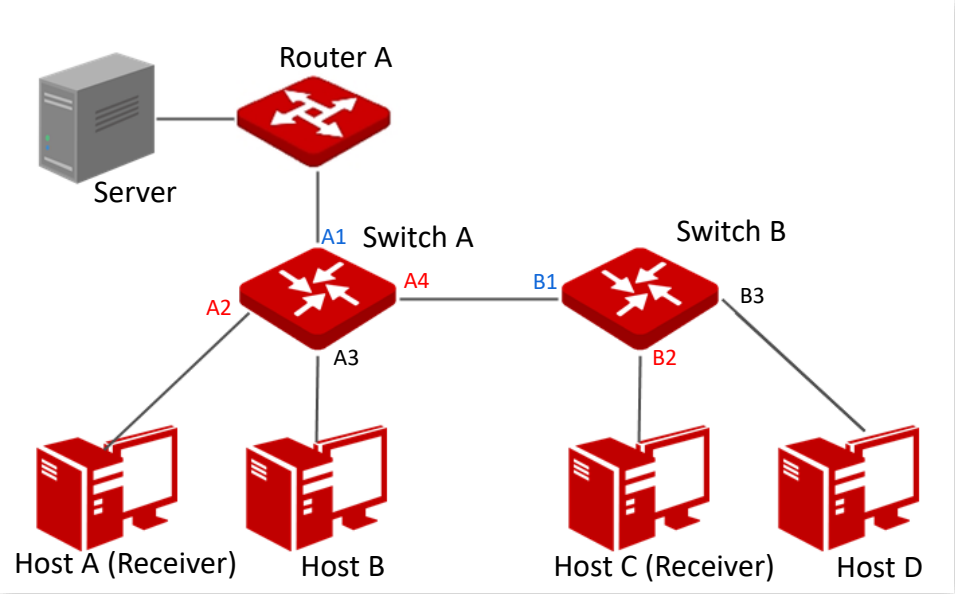
As shown in the figure below, multicast data is broadcasted from the IGMP-Snooping-disabled layer-2 device; But with IGMP Snooping enabled, the layer-2 device will establish a mapping table for ports and multicast MAC addresses by analyzing received IGMP messages, and forward multicast data to the specific receivers.



IGMP snooping only forwards data to the specific receivers through the layer-2 multicast, providing the following advantages:

- Reduce broadcast in layer-2 network and saves network bandwidth.
- Enhance the security of multicast data.
- Provide convenience for charging management to each host.

As shown in the following figure, router A is connected to the multicast source, IGMP snooping of switch A and switch B is enabled, while host A and host C are the receivers of the multicast data.



- **Router port**

  On an IGMP-snooping-enabled layer-2 device, the ports toward upstream layer-3 multicast devices are called router ports (ports A1 and B1 in the above figure).

- **Host port**

  On an IGMP-snooping-enabled layer-2 device, the ports toward downstream receiver hosts are called host ports (Ports A2, A4 and B2 in the above figure).

- **General query**

  The IGMP querier (router A in the above figure) periodically sends IGMP general queries to all hosts and devices in the local network segment to check the multicast group members.

  After receiving an IGMP general query, the layer 2 device (switches A and B in the above figure) forwards the query, and performs the following treatment to the receiving ports:

  - If the receiving port is included in the mapping table, the layer 2 device restarts the aging timer for the port.
  - If the receiving port is excluded in the mapping table, the layer 2 device adds the port to the mapping table and starts an aging timer for the port.

- **Specific query**

  When a host with enabled IGMPv2 or IGMPv3 leaves the multicast group, it sends IGMP leave group messages. When the ports of the layer-2 devices (switches A and B in the above figure) receive the IGMP leave group message, the following actions will be done according to the mapping table:

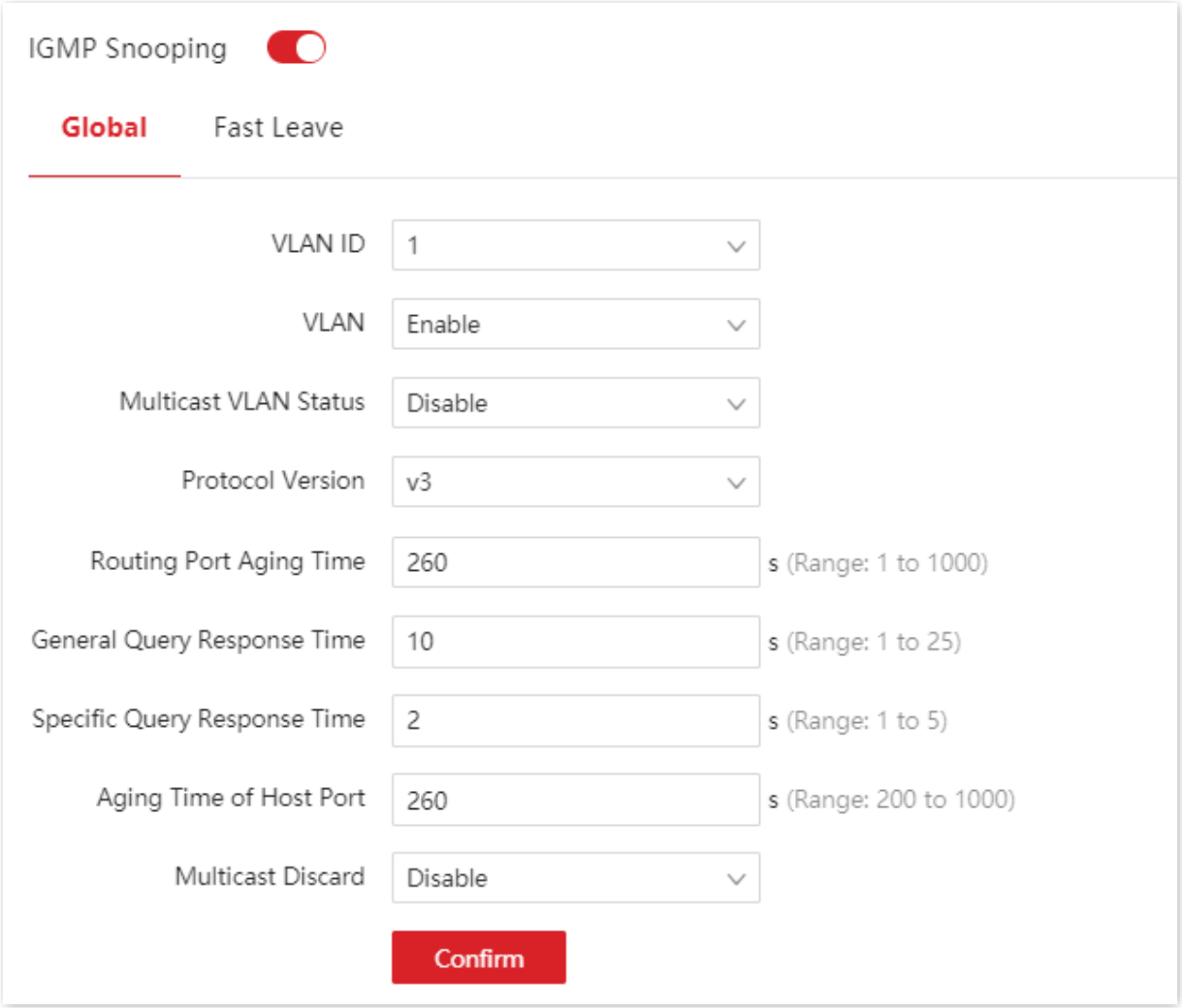
  - If no forwarding entry of the multicast group is found or the matching forwarding entry does not contain the receiving port, the layer 2 device discards the IGMP leave group message directly instead of forwarding it to other ports.
  - If the forwarding entry of the multicast group is found, and the matching forwarding entry contains other host ports, the layer 2 device discards the IGMP leave group

message directly instead of forwarding it to other ports, and sends IGMP specific query message to the leaving host.

- If the forwarding entry of the multicast group is found, and the matching forwarding entry does not contain other host ports, the layer 2 device forwards the message through the router port and also sends IGMP specific query message to the host.

4.5.2 Global

Click **Switching** > **IGMP Snooping** > **Global** to enter the page. On this page, you can configure the global parameters of IGMP snooping.



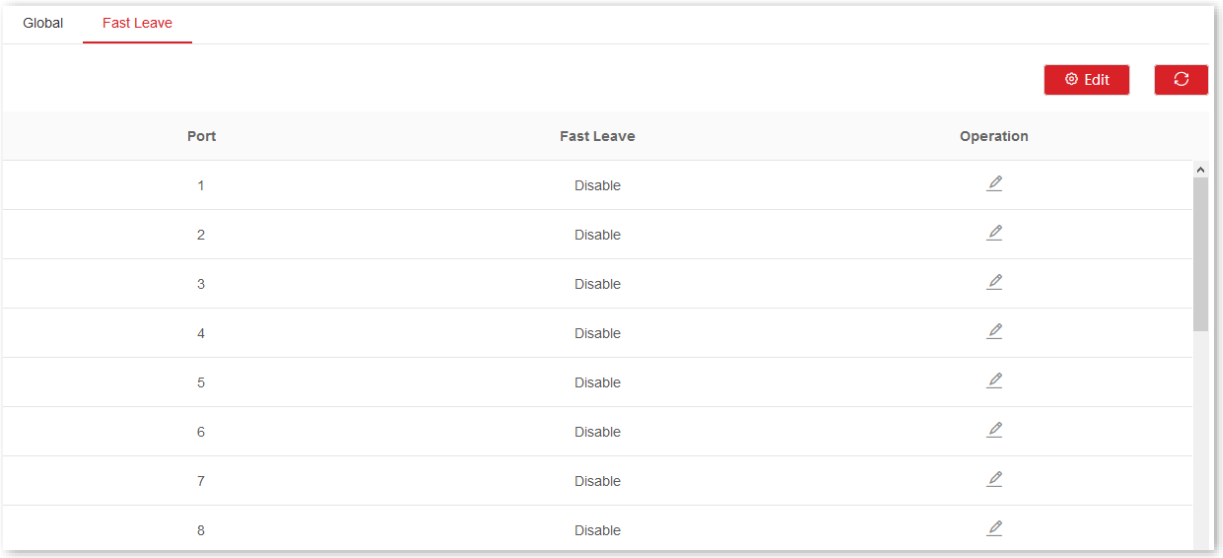
Parameter description

Name	Description
IGMP Snooping	It is used to enable or disable the IGMP snooping function.
VLAN ID	It specifies the VLAN whose IGMP Snooping function is enabled.
VLAN	It is used to enable or disable the IGMP Snooping function of the VLAN.
Multicast VLAN	It is used to enable or disable the multicast VLAN function of the above VLAN.

Name	Description
Status	By default, the multicast VLAN function of the switch is disabled. If devices from different VLANs within a LAN request multicast messages from the same multicast source, the multicast device should copy the multicast data to each VLAN. With this function enabled, the multicast device only needs to send multicast data to this switch, and this switch will send them to the receivers of multicast data, thus saving bandwidth and reducing the burden of the multicast device.
Protocol Version	Supported IGMP message versions: – **v1**: Only process messages of IGMPv1. – **v2**: Only process messages of IGMPv1 and IGMPv2. – **v3**: Process messages of IGMPv1, IGMPv2, and IGMPv3.
Routing Port Aging Time	It specifies the time of the routing port aging timer. During this period, if the routing port does not receive the IGMP general query message, the switch deletes the port from the mapping table.
General Query Response Time	It specifies the maximum response time to the general query. After the switch forwards the general query message, and during this time period, if the port does not receive the IGMP membership message that responds to the general query, the port will be deleted from the mapping table.
Specific Query Response Time	It specifies the maximum response time to the specific query. After the switch forwards the IGMP specific query message to the host ports, and during the time period, if the host port does not receive the IGMP membership message that responds to the specific query by the host, the switch deletes the port in the mapping table.
Aging Time of Host Port	It specifies the time of the host port aging timer. When the host port does not receive the IGMP membership message during this time period, the switch deletes the port from the mapping table.
Multicast Discard	With the Multicast Discard function enabled, the switch forwards the unknown multicast data message only to its router port and does not broadcast in VLAN. If the switch does not have any router port, the unknown multicast data will be discarded and not forwarded.

4.5.3 Fast leave

Click **Switching** > **IGMP Snooping** > **Fast Leave** to enter the page. On this page, you can configure the fast leave mode for each port.



Parameter description

Name	Description
Port	It specifies the ID of the port.
Fast Leave	With the function enabled, when receiving the IGMP leave group messages from this port, the switch removes the port from the corresponding IGMP snooping multicast forwarding list, and does not wait till the aging time of the host port times out.

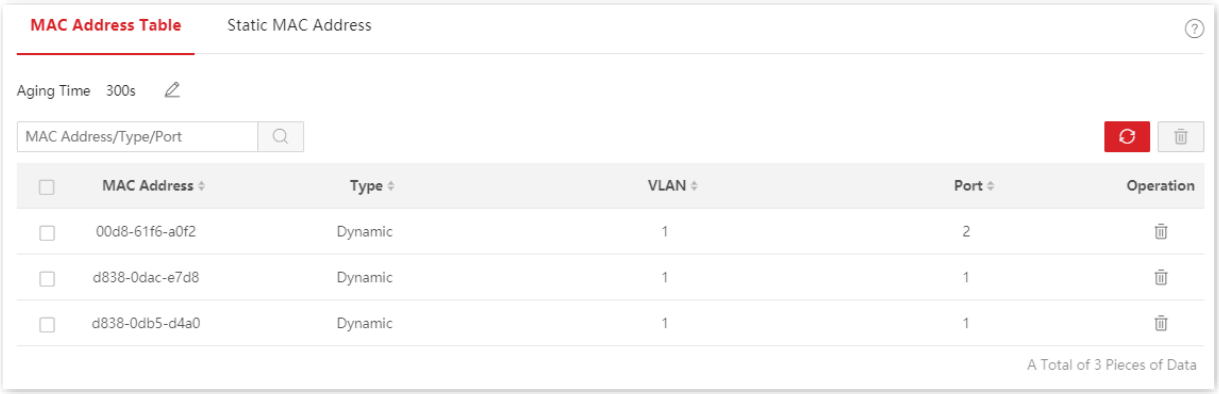
4.6 MAC settings

4.6.1 MAC address table

The switch creates the MAC address forwarding table by address learning mechanism. The table includes such information as MAC address, VLAN ID and port number. When forwarding a message, the switch adopts one of the following two forwarding modes based on the MAC address table information:

- Unicast mode: If an entry in the MAC address forwarding table is available for the destination MAC address, the switch will forward the message to the port indicated by the MAC address table entry.
- Broadcast mode: If the switch receives a message with the destination MAC address whose lowest bit of the second byte is 1, or no entry in the MAC address forwarding table is available for the destination MAC address, the switch forwards the message to all ports except the receiving port in broadcast mode. The broadcast messages, multicast messages and unknown unicast messages will be forwarded in broadcast mode.

Click **Switching** > **MAC Settings** > **MAC Address Table** to enter the page. On this page, you can view and delete the MAC address table entries.



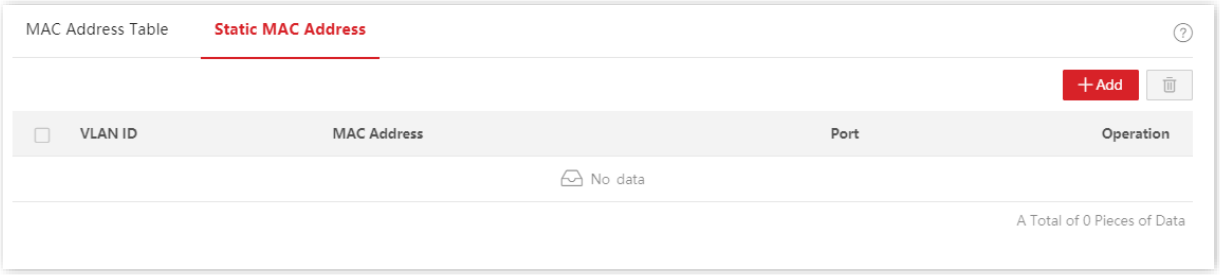
Parameter description

Name	Description
Aging Time	It specifies the aging time of the entries in the MAC address table, which is effective only for dynamic entries. When the switch does not receive messages whose source address is consistent with the source MAC address in the table within the aging time, the MAC address table entry will be automatically deleted.
MAC Address	MAC address, format: *XXXX-XXXX-XXXX*.

Name	Description
Type	It specifies the type of the MAC address. – **Static**: It specifies the MAC address entry manually configured by the administrator. – **Dynamic**: It specifies the MAC address entry automatically generated by the switch.
VLAN	It specifies the VLAN to which the MAC address belongs.
Port	It specifies the physical port of the switch that the device with the MAC address connects to.

4.6.2 Static MAC address

Click **Switching** > **MAC Settings** > **Static MAC Address** to enter the page. On this page, you can configure the static MAC address table. The configuration exists as static entries in the MAC address table, beyond the control of MAC aging time.



Parameter description

Name	Description
VLAN ID	It specifies the VLAN to which the MAC address belongs.
MAC Address	MAC address, format: *XXXX-XXXX-XXXX*.
Port	It specifies the physical port of the switch that the device with the MAC address connects to.

5 Routing

Routing refers to a process that a routing device selects an optimal path for a received packet according to its destination address and forwards it to the next network node. The last routing node on this path forwards the packet to the destination host.

The routing device maintains a routing table which contains the path information of the network, and selects an optimal path to forward data according to the routing protocol (such as RIP and OSPF) supported by the routing device.

Routing table mainly includes three types of routes.

- Direct route: A direct route is discovered by the data link layer protocol, usually a route between the routing device and its directly connected network.
- Static route: A static route is manually configured by the network administrator and will not change even the network topology changes.
- Dynamic route: A dynamic route is calculated by a routing protocol after the routing device exchanges routing information with its neighbor devices. Dynamic routes can change automatically when the network typology changes.

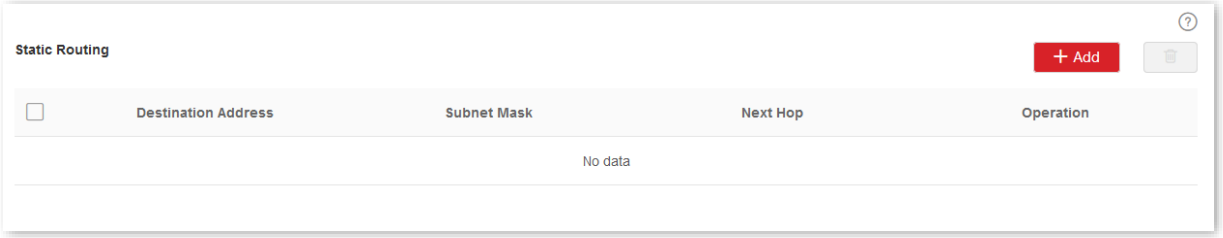
5.1 Static routing

Static route is the fixed route manually configured by the administrator, generally used in a small to medium-sized network with stable topology. Static route is efficient, reliable and easy to configure, and can improve the forwarding speed of packets. But static route cannot automatically change with network topology. So when the network malfunctions or the network topology changes, the administrator needs to manually modify the static routing configuration.

Tip

Except direct routes, static routes own the highest priority among all routes.

Click **Routing** > **Static Routing** to enter the page. On this page, you can view and configure the static routing rules.



Parameter description

Name	Description
Destination Address	It specifies the IP address of the destination network. The destination address and subnet mask of the default route are both 0.0.0.0. Tip The switch adopts the default route to forward packets when there is no specific route that matches the destination address of packets in the routing table.
Subnet Mask	It specifies the subnet mask of the destination network.
Next Hop	It specifies the ingress IP address of the next hop route after packets egress from the switch.

5.2 Dynamic routing

Tip

Not all switch models support dynamic routing. Please refer to the actual web UI and CLI (Command Line Interface) of your switch.

Only RIP dynamic routing can be configured on the web UI of the switch temporarily. For OSPF dynamic routing, you should configure through CLI.

5.2.1 Overview

The switch supports RIP (Routing Information Protocol) and OSPF (Open Shortest Path First). RIP is an IGP (Interior Gateway Protocol), usually used for small to medium sized networks, such as school network. Compared with OSPF, RIP is easier to manage and maintain.

- **RIP operation**

  RIP defines two types of messages:

  - Request message: It refers to messages that request part of or the whole routing table's information from the neighbor routing devices.
  - Response message: It refers to messages that respond to the requests from neighbor routing devices or are sent periodically to the neighbor routing devices with updated information.

  At the initialization stage, the RIP routing table only contains information of directly connected routes. The routing device should exchange and learn routing tables with its neighbor routing devices, and then updates its RIP routing table.

  The procedure is as follows:

1. At the initialization stage of RIP, the switch sends request messages from each interface with the RIP function enabled, which contains the entire routing table information of the switch.
2. After receiving this request message, the neighbor routing device sends a response message with its routing table information to the switch.
3. After receiving this response message, the switch updates its routing table and sends update (response) messages to its neighbor devices. The neighbor routing devices will update their routing table information and send update messages to their neighbor routing devices.

   After the routing table information exchange finishes, the switch generates its final RIP routing table. And all routing devices keep the latest routing information. After that, this switch will send update messages periodically and ages routes according to the aging mechanism, ensuring the validity of the routing table.

- **RIP version**

  RIP has two versions: RIPv1 and RIPv2.

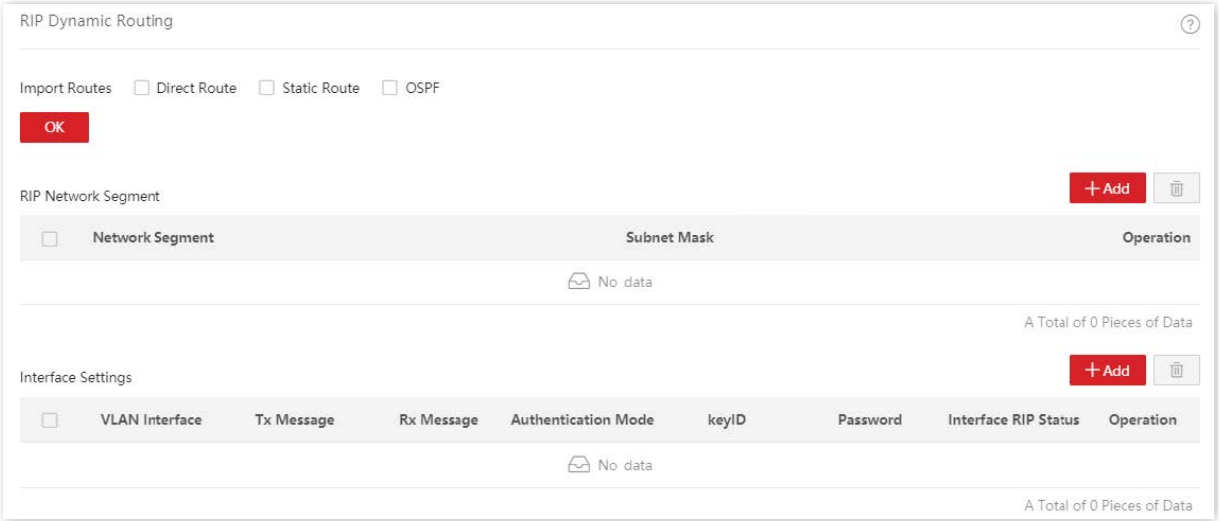
RIPv1 is a classful routing protocol, which only supports sending protocol messages through broadcast. The protocol messages of RIPv1 cannot carry mask information, and can only identify the routes of natural networks, such as Classes A, B and C, so RIPv1 does not support discontinuous subnets.

Backward compatible with RIPv1, RIPv2 is a classless routing protocol. Compared with RIPv1, RIPv2 has the following advantages:

- Supports routing tags, which can be used to flexibly control routes in routing policies.
- Carries mask information and support route summarization and CIDR (Classless Inter-Domain Routing).
- Supports designated next hop to select the optimal next hop on the broadcast network.
- Supports sending multicast update messages, which can reduce resource consumption.
- Supports authenticating protocol messages by Simple and MD5, which can verify the validity of the update message source and enhance security.

5.2.2 RIP dynamic routing

Click **Routing** > **Dynamic Routing** to enter the page. On this page, you can view and configure the RIP dynamic routing rules.



Parameter description

Name		Description
Import Routes		It is used to import route information from other processes or protocols into the RIP routing table. The switch supports importing direct routes, static routes and OSPF routes.
RIP Network Segment	Network Segment	It specifies the IP address segment with RIP enabled. RIP of the switch's interfaces within the specified network segment is enabled.
	Subnet Mask	

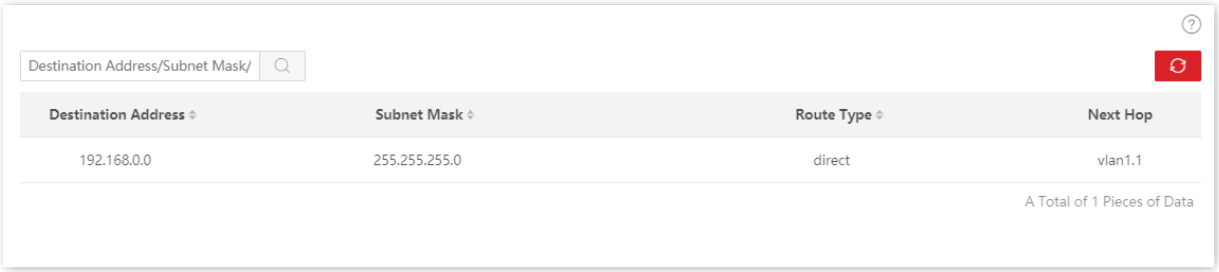
Name		Description
Interface Settings	VLAN Interface	It specifies the VLAN interface with RIP enabled.
	Tx Message	It specifies the RIP version that the VLAN interface supports when transmitting RIP messages. – **Do Not Transmit**: This interface does not transmit RIP messages. – **RIPv1**: This interface transmits RIPv1 request and response messages. – **RIPv2**: This interface transmits RIPv2 request and response messages through multicast. – **RIPv2 Broadcast**: This interface transmits RIPv2 request and response messages through broadcast.
	Rx Message	It specifies the RIP version that the VLAN interface supports when receiving RIP messages. – **Do Not Receive**: This interface does not receive RIP messages. – **RIPv1**: This interface only receives RIPv1 request and response messages. – **RIPv2**: This interface only receives RIPv2 request and response messages. – **RIPv1 & RIPv2**: This interface receives both RIPv1 and RIPv2 request and response messages.
	Authentication Mode	It specifies the authentication mode used by the VLAN interface for receiving and transmitting RIP messages. – **Do Not Authenticate**: The authentication function of this interface is disabled. – **Simple**: The Simple authentication mode is adopted. When the VLAN interface transmits RIP messages, the password will be added to the message head to authenticate the peer routing device. And the VLAN interface will authenticate the received RIP messages according to the password before responding. – **MD5**: The MD5 authentication mode is adopted. When the VLAN interface transmits RIP messages, the password and KeyID will be added to the message head to authenticate the peer routing device. And the VLAN interface will authenticate the received RIP messages according to the password and KeyID before responding. Note RIPv1 does not support authentication. The authentication configuration will not take effect when the interface receives or transmits RIPv1 messages.
	keyID	This field is required when the authentication mode is set to MD5.
	Password	This field is required when the authentication function is enabled for the interface.
	Interface RIP Status	It specifies the RIP operating status of the VLAN interface.

5.3 Routing table

Tip

Not all switch models support a display of the routing table on the web UI of the switch. Please refer to the actual web UI of your switch.

Click **Routing** > **Routing Table** to enter the page. On this page, you can configure the routing table of the switch. This routing table contains all routing information learnt by the switch, including direct routes, static routes and dynamic routes.



Parameter description

Name	Description
Destination Address	It specifies the IP address of the destination network. The destination address and subnet mask of the default route are both 0.0.0.0. Tip The switch adopts the default route to forward packets when there is no specific route that matches the destination address of packets in the routing table.
Subnet Mask	It specifies the subnet mask of the destination network.
Route Type	It specifies the type of the route, including: **direct**, **static**, **RIP** and **OSPF**.
Next Hop	It specifies the ingress interface of the next hop route after packets' egress from the switch.

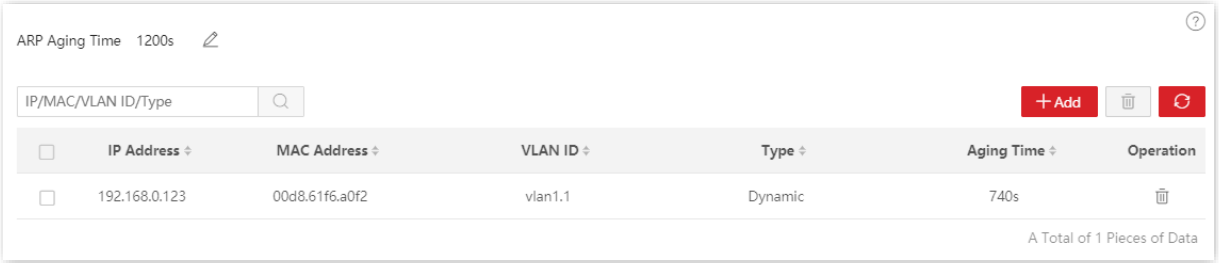
5.4 ARP

In the data transmission process, IP address is the address of the host in the network layer. If you want to send packets to the destination host in the network layer, the data link layer address of the destination host (such as the Ethernet MAC address) is required.

ARP (Address Resolution Protocol) can convert an IP address to MAC address and maintains an internal ARP table in the data base of the switch to record the corresponding relationship between MAC addresses and IP addresses of other hosts which communicates recently with this switch. If the switch requires to communicate with the destination host, it performs the address resolution first based on ARP. The resolution process is as follows:

1. The switch checks if a rule with the corresponding relationship between the IP address and MAC address of the destination host exists in the switch's ARP table. If so, the switch sends data to the destination host according to the queried rule. If not, the switch broadcasts an ARP request data frame in the LAN, which contains the IP address and MAC address of the switch itself as well as the IP address of the destination host.
2. All devices in the LAN can receive this request. When the destination host receives this request, it responds to the switch with an ARP response frame, which contains the MAC address of the destination host.
3. After the switch receives the ARP response, it records the corresponding relationship of the IP address and MAC address of the destination host into its ARP table for further use.

Click **Routing** > **ARP** to enter the page. On this page, you can view and configure the ARP table.



Parameter description

Name	Description
ARP Aging Time	It specifies the aging time of ARP entries. If the switch does not receive the corresponding ARP message within this period of time, the ARP entry will be removed from the ARP table.
IP Address	It specifies the IP address of the host.
MAC Address	It specifies the MAC address of the host corresponding to the IP address.
VLAN ID	It specifies the VLAN layer 3 interface to which the ARP entry belongs.

Name	Description
Type	It specifies the type of the ARP entry. – **Dynamic**: It specifies the ARP entry which is automatically generated by the switch according to ARP. Its life time is defined by the ARP aging time. – **Static**: It specifies the manually configured ARP entries, which is permanently valid, and is free from the limitations of the ARP aging time.
Aging Time	It specifies the remaining aging time of the ARP entry.

5.5 DHCP server

5.5.1 Overview

With increasing network demands, the network expands greatly and becomes more complex, resulting in computers outnumbering the allocable IP addresses. Besides, the locations of the wireless devices often change, so the IP addresses of the devices need to be constantly updated. DHCP (Dynamic Host Configuration Protocol) can solve the above issues by IP address dynamic assignment strategy.

Tip

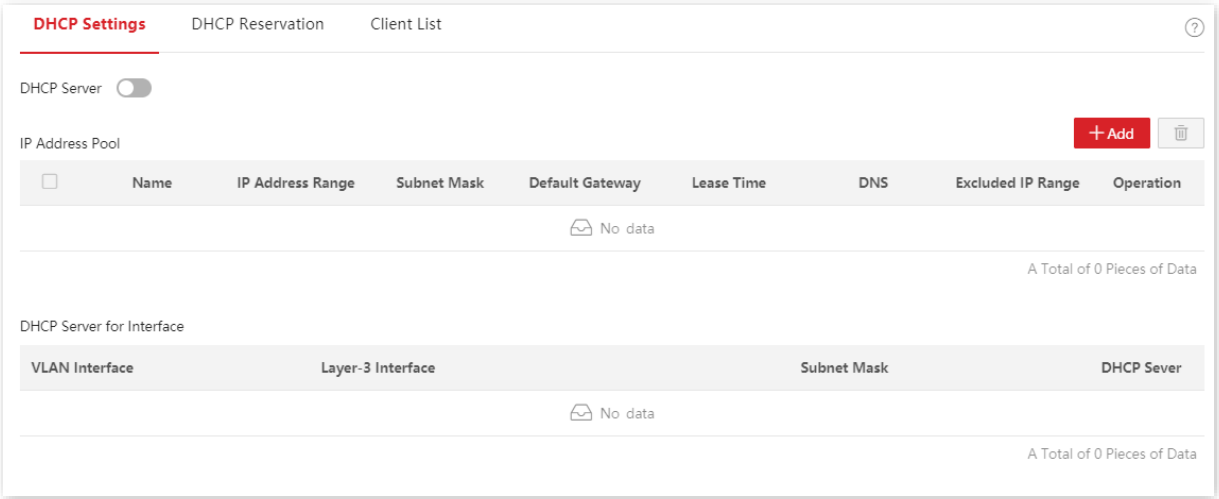
The DHCP server of this switch does not support IP address allocation based on Option 82.

According to different needs of clients, DHCP provides two kinds of IP address assignment strategies:

- Dynamic IP address assignment: DHCP assigns the IP address with a valid period to the client, and the client needs to reapply for the IP address after expiry. This strategy applies to most clients.
- Static IP address assignment: The administrator binds the fixed IP addresses for some specific clients. Assigning a fixed IP address can prevent the failure of some functions based on the IP address due to IP address changes.

5.5.2 DHCP settings

Click **Routing** > **DHCP Server** > **DHCP Settings** to enter the page. On this page, you can view and configure the DHCP server.

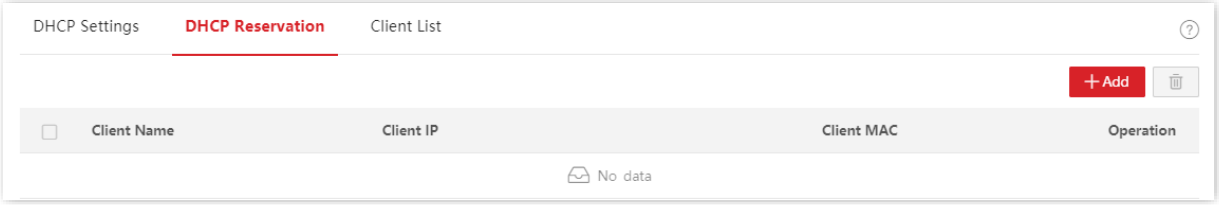


Parameter description

Name		Description
DHCP Server		Enable or disable the DHCP Server function.
IP Address Pool	Name	It specifies the name of the IP address pool.
	IP Address Range	It specifies the range of IP addresses that can be assigned.
	Subnet Mask	It specifies the subnet mask assigned by the DHCP server to a client.
	Default Gateway	It specifies the gateway address assigned by the DHCP server to a client.
	Lease Time	It specifies the validity period of an IP address assigned by the DHCP server to a client. By half of the lease time, the client sends a DHCP request to the DHCP server to renew the lease. If the request succeeds, the lease will be renewed from the time of sending the request; if not, the renewal process restarts at 7/8 of the lease time. If the request succeeds, the lease will be renewed from the time of sending the request; if the request still fails, the client needs to reapply for the IP address after the lease expires. Please modify the lease time based on the actual network environment. It is recommended to keep the default setting if there is no special requirement.
	DNS	It specifies the DNS server address assigned to clients.
	Excluded IP Range	It specifies the IP addresses in the IP address pool that cannot be assigned by the DHCP server by dynamic assignment strategy.
DHCP Server for Interface	VLAN Interface	It specifies the VLAN interface to which the IP address pool is applied.
	Layer-3 Interface	It specifies the IP address of the VLAN interface.
	Subnet Mask	It specifies the subnet mask of the VLAN interface.
	DHCP Server	With it enabled, the DHCP Server function of the VLAN interface takes effect.

5.5.3 DHCP reservation

Click **Routing** > **DHCP Server** > **DHCP Reservation** to enter the page. On this page, you can view and configure the DHCP Reservation policy.



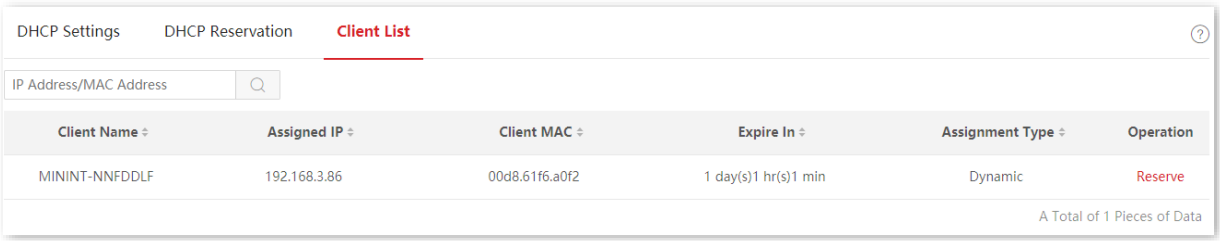
Parameter description

Name	Description
Client Name	It specifies the remark of the DHCP reservation policy. If the reservation policy is added from the client list, it displays the client name or you can customize it.
Client IP	It specifies a fixed address assigned by the DHCP server to the client.
Client MAC	It specifies the MAC address of a client.

5.5.4 Client list

Click **Routing** > **DHCP Server** > **Client List** to enter the page. On this page, you can perform the following operations to the devices whose IP addresses are obtained from this switch.

- View the client name, assigned IP address, and other information.
- Click **Reserve**, and the assigned IP address can be added to the **DHCP Reservation** list and the DHCP server assigns this IP address to the client all the time.



Parameter description

Name	Description
Client Name	It specifies the name of a client.
Assigned IP	It specifies an IP address assigned by the DHCP server to the client.
Client MAC	It specifies the MAC address of a client.
Expire In	It specifies the rest time of the lease.
Assignment Type	It specifies the address assignment policy by the DHCP server to the client. – **Dynamic**: the DHCP server assigns IP address to this client using dynamic IP address assignment policy. – **Static**: the DHCP server assigns static address to this client using static IP address assignment policy.

6 QoS policy

6.1 Overview

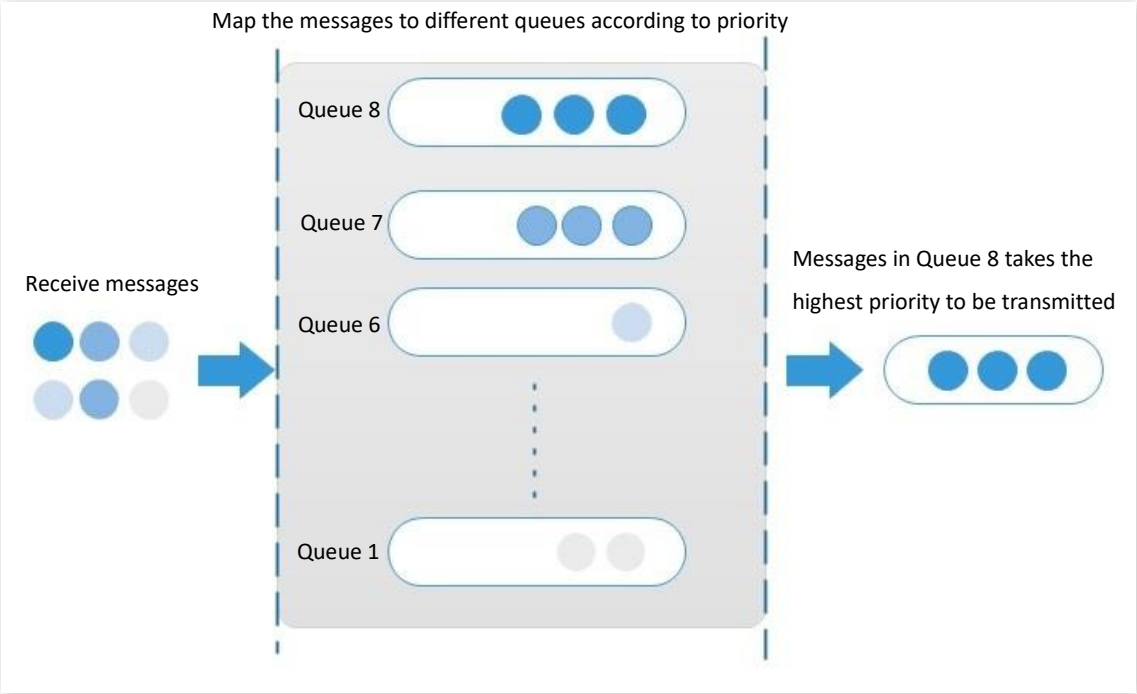
In traditional IP network, packets are treated equally. This network service policy is known as Best-effort, which delivers the packets to their destinations with the best effort, with no assurance and guarantee for delivery delay, reliability, and so on. Nowadays, in addition to traditional applications such as www, FTP and E-mail, new services occur, such as video conference, remote education, Video-on-Demand (VoD) and video telephone, which need higher requirements for bandwidth, delay and jitter. QoS (Quality of Service) policy can meet the above demands and improve the quality of service in the network.

This switch classifies the messages according to priority at the ingress stage, then maps them to different queues at the egress stage, and finally forwards these messages by queues according to the scheduling mode, so as to guarantee the quality of network service.

Scheduling mode

Queue scheduling is used to solve the problem of resource preemption by multiple messages when the network is congested. This switch supports three scheduling modes: strict priority, simple weighted priority and weighted priority. Each scheduling mode has eight queues (queues 0 to 7) with different data forwarding priority.

- **Strict Priority**



Strict priority scheduling algorithm is specially designed for critical service applications. An important feature of critical services is that they demand preferential service in congestion in order to reduce the response delay.

In queue scheduling, the messages are sent in queues strictly following the priority order from high to low (Queue 8 > Queue 7 > … > Queue 1). When the queue with higher priority is empty, messages in the queue with lower priority are sent. You can put critical service messages into the queues with higher priority and put non-critical service messages (such as E-mail) into the queues with lower priority. In this way, critical service messages are sent preferentially, and non-critical service messages are sent when the critical service messages are not sent.

Disadvantage of Strict Priority: If there are messages in the queues with higher priority for a long time during congestion, the messages in the queues with lower priority will keep stuck because they are not served.

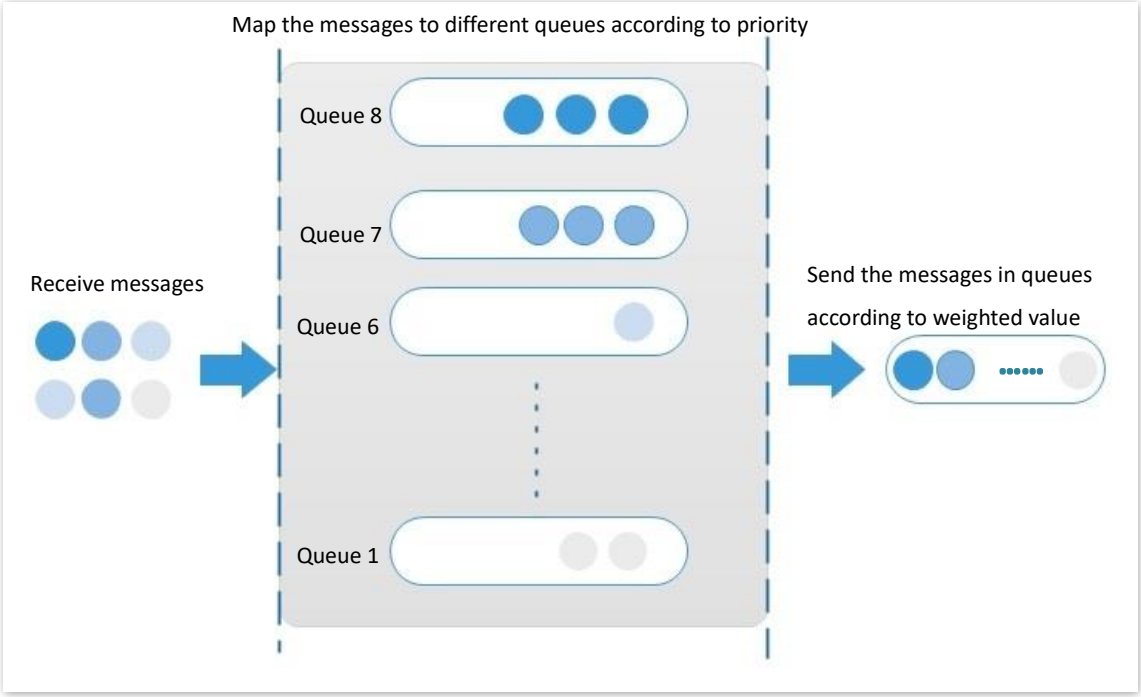
- **Simple Weighted Priority**

In this mode, there is no priority and all queues equally share the bandwidth.

- **Weighted Priority**

This scheduling algorithm schedules all the queues in turn to ensure that every queue can be assigned a certain service time. The weighted value stands for the proportion of assigned resource. Assume that there are eight output queues for a port, and each queue is assigned with a weighted value. For instance, you can configure the eight weighted values of a 100 Mbps port to 25, 20, 15, 15, 10, 5, 5 and 5 respectively. In this way, the queue with the lowest priority can be assured of 5 Mbps of bandwidth at least, thus avoiding the disadvantage of Simple Priority queue-scheduling algorithm that messages in low-priority queues are possibly

not to be served for a long time. Another advantage of Weighted Priority queue-scheduling algorithm is that though the queues are scheduled in turn, the service time for each queue is not fixed, which means if a queue is empty, the next queue will be scheduled immediately. In this way, the bandwidth resources can be fully utilized.

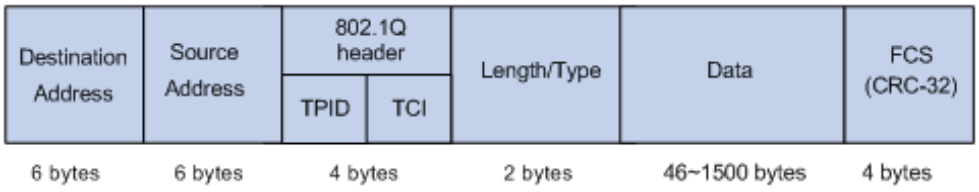


Priority

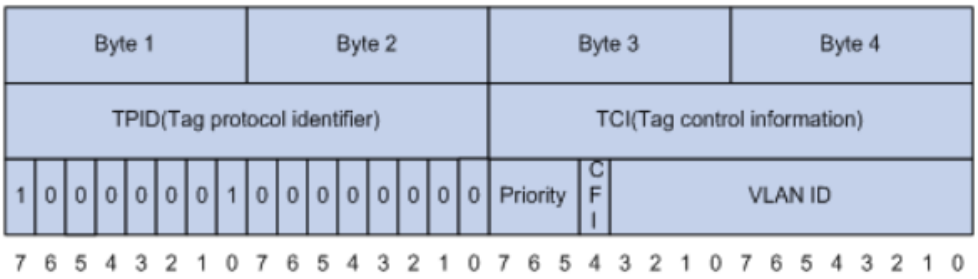
This switch supports three priority modes: 802.1P Priority, DSCP Priority, and Port Priority.

- **802.1P Priority**

802.1P priority lies in Layer 2 packet headers and is applicable to occasions where the Layer 3 packet header does not need analysis but QoS must be assured at Layer 2. 802.1P priority is available only in an 802.1Q tagged packet. As seen below, the 4-byte 802.1Q tag contains a 2-byte TPID (Tag Protocol Identifier, value: 0x8100) and a 2-byte TCI (Tag Control Information).



The figure below displays a detailed view of an 802.1Q tag. The field **Priority** under TCI is the 802.1P priority, which consists of 3 bits ranging from 0 to 7.

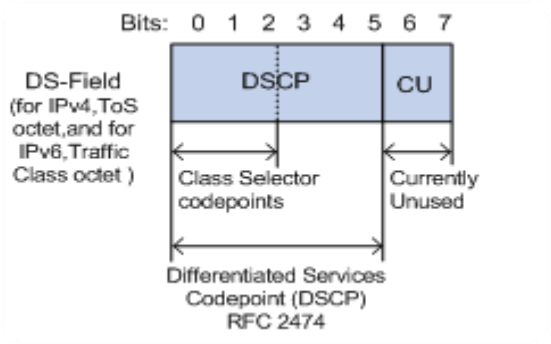


By default, the 802.1P priority, queues, and key words of this switch are mapped as follows.

802.1P Priority	Queue	Key Word
0	1	best-effort
1	2	background
2	3	spare
3	4	excellent-effort
4	5	controlled-load
5	6	video
6	7	voice
7	8	network-management

- **DSCP Priority**

RFC2474 re-defines the ToS (Type of Service) field in the IP message header, which is called the DS (Differentiated Services) field. The first six bits (bits 0 to 5) of the DS field indicate DSCP (Differentiated Services Codepoint) priority ranging from 0 to 63. The last 2 bits (bits 6 and 7) are reserved.



The corresponding relationship between the DSCP priority and key words are as follows.

DSCP Priority (Decimal)	DSCP Priority (Binary)	Key Word
46	101110	ef
10	001010	af11
12	001100	af12
14	001110	af13

DSCP Priority (Decimal)	DSCP Priority (Binary)	Key Word
18	010010	af21
20	010100	af22
22	010110	af23
26	011010	af31
28	011100	af32
30	011110	af33
34	100010	af41
36	100100	af42
38	100110	af43
8	001000	cs1
16	010000	cs2
24	011000	cs3
32	100000	cs4
40	101000	cs5
48	110000	cs6
56	111000	cs7
0	000000	be (default)

By default, the DSCP priority and queues of this switch are mapped as follows.

DSCP Priority	Queue
0 - 7	1
8 - 15	2
16 - 23	3
24 - 31	4
32 - 39	5
40 - 47	6
48 - 55	7
56 - 63	8

- **Port Priority**

  You can manually configure the CoS (Class of Service) priority of physical ports to map the physical ports with queues. The port maps messages to the corresponding queues according to the configured mapping relationship when the following two situations occur:

- The messages received by the port do not carry the priority tags trusted by the port. Example: For a port with 802.1P priority mode enabled, the received messages do not carry the 802.1Q tag.
- The port does not trust the 802.1P priority mode and DSCP priority mode.

The CoS priority of the ports and queues are mapped as follows.

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

6.2 Configuration guidance

Based on 802.P priority

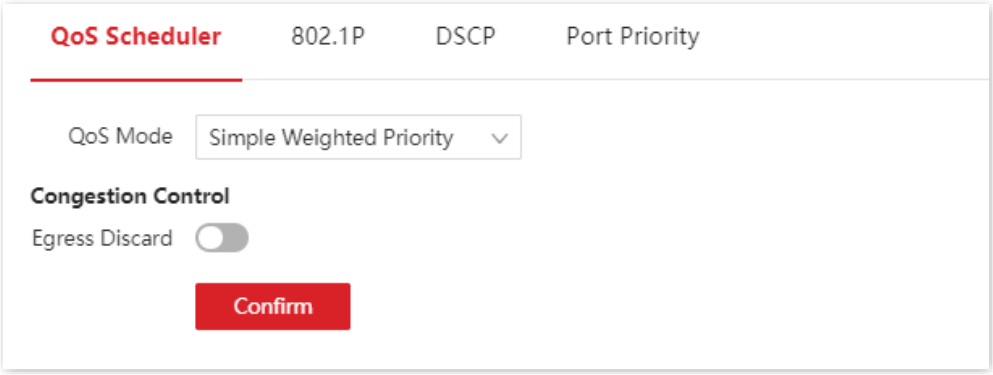
Step	Task	Description
1	QoS Scheduler	**Required.** Select the scheduling mode of the switch based on actual demands.
2	802.1P	**Required.** Configure the mapping relation between 802.1P priority and queues.
3	Port Priority	**Required.** Set the priority mode of corresponding ports to **802.1P Trust** and configure the CoS priority for all ports.

Based on DSCP priority

Step	Task	Description
1	QoS Scheduler	**Required.** Select the scheduling mode of the switch based on actual demands.
2	DSCP	**Required.** Configure the mapping relation between DSCP priority and queues.
3	Port Priority	**Required.** Set the priority mode of corresponding ports to **DSCP Trust** and configure the CoS priority for all ports.

6.3 QoS scheduler

Click **QoS Policy** > **QoS Scheduler** to enter the page. On this page, you can configure the QoS scheduling mode and congestion control policies.

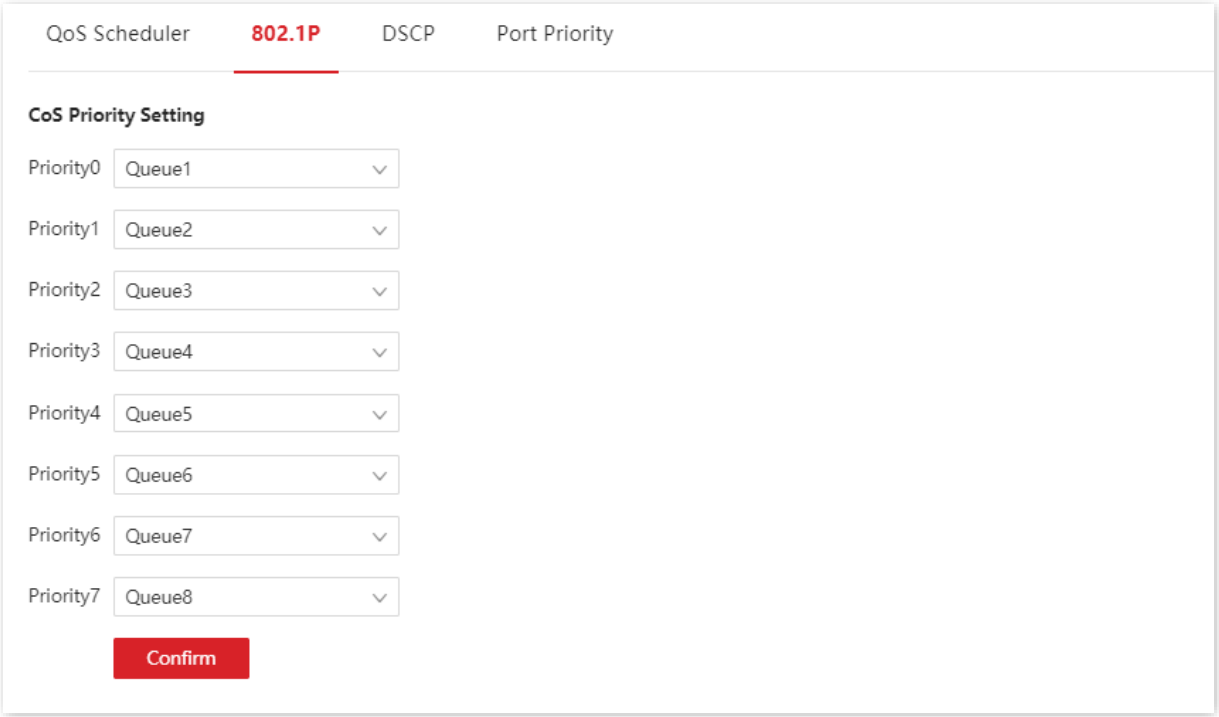


Parameter description

Name	Description
QoS Mode	It specifies the scheduler mode for the port traffic. – **Strict Priority**: The switch forwards the messages strictly based on the message priority from high to low. The queue messages with the lower priority are forwarded only when the queue with higher priority is empty. – **Simple Weighted Priority**: 8 queues equally share the bandwidth. – **Weighted Priority**: You need to configure a weighted value for each queue. The weighted value indicates the weight of obtaining resources. If congestion occurs on the port, the bandwidths are assigned based on the weight of each queue.
Queue Settings	If the **QoS Mode** is set to **Weighted Priority**, you need to configure the weighted value for each queue.
Egress Discard	When this function is enabled, the switch disables the flow control function to meet the requirements of network clone in various environments. Tip This function applies to network clone scenario and is not recommended in common scenarios.

6.4 802.1P

Click **QoS Policy** > **802.1P** to enter the page. On this page, you can configure the mapping relationship between the 802.1P priority and queues.

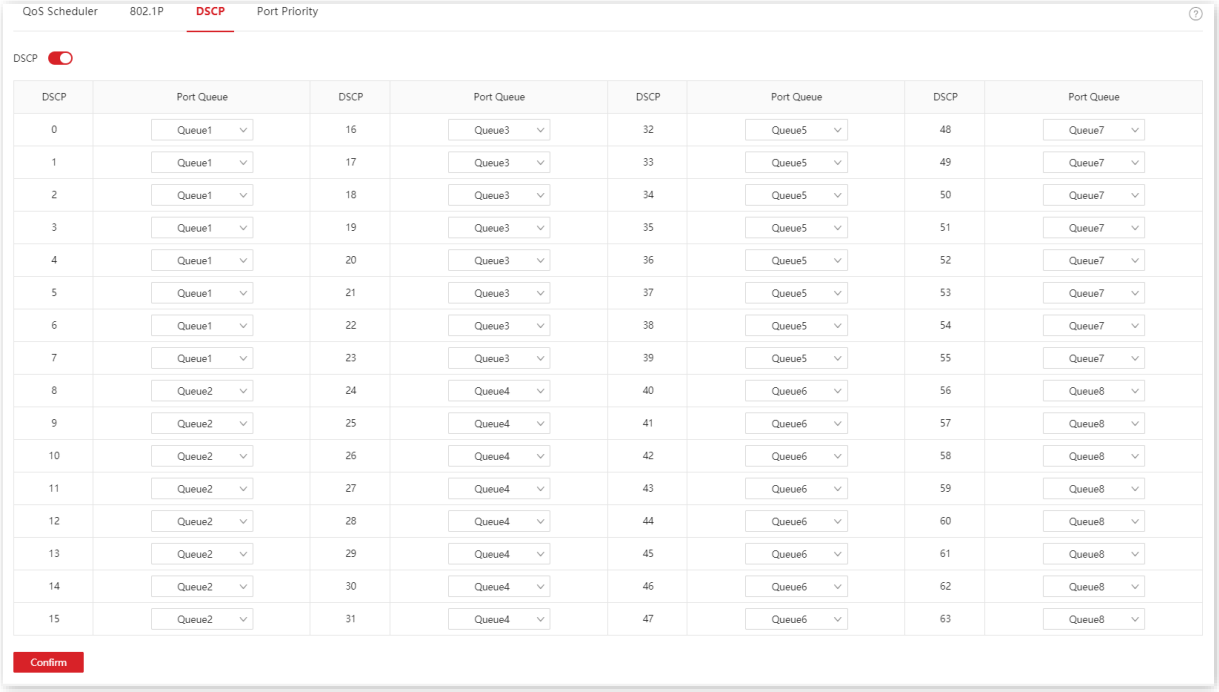


Parameter description

Name	Description
Priority0	It specifies the queue in which the messages' priority is 0.
Priority1	It specifies the queue in which the messages' priority is 1.
Priority2	It specifies the queue in which the messages' priority is 2.
Priority3	It specifies the queue in which the messages' priority is 3.
Priority4	It specifies the queue in which the messages' priority is 4.
Priority5	It specifies the queue in which the messages' priority is 5.
Priority6	It specifies the queue in which the messages' priority is 6.
Priority7	It specifies the queue in which the messages' priority is 7.

6.5 DSCP

Click **QoS Policy** > **DSCP** to enter the page. On this page, you can configure the mapping relationship between the DSCP priority and queues.



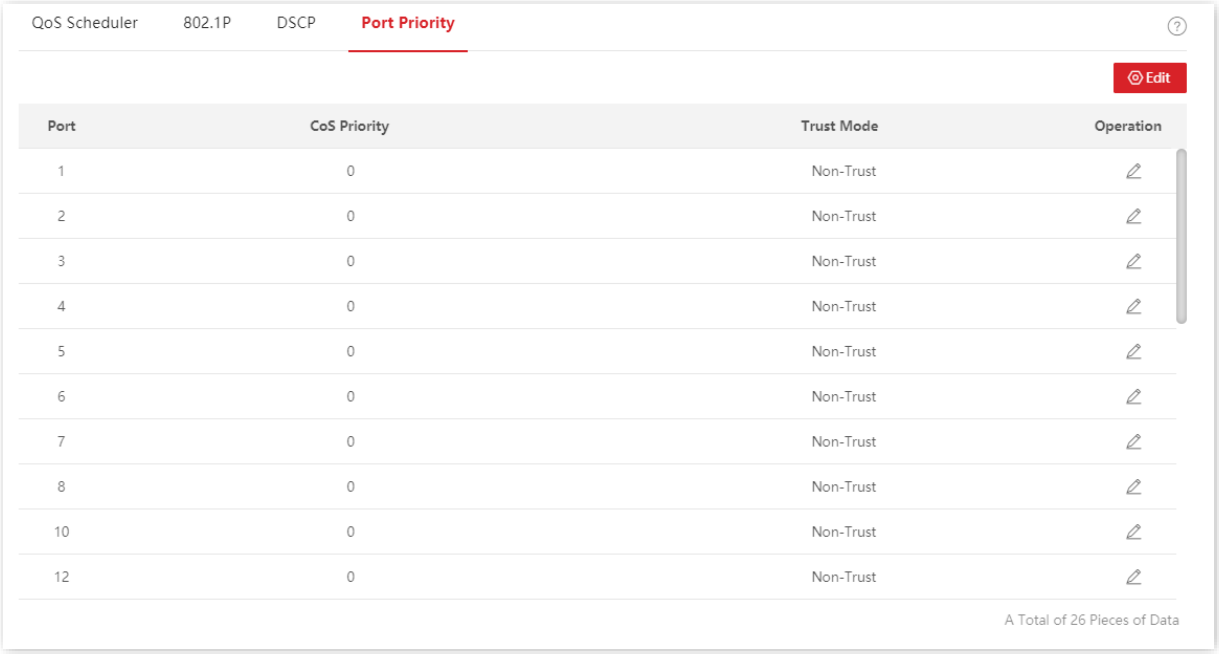
DSCP	Port Queue	DSCP	Port Queue	DSCP	Port Queue	DSCP	Port Queue
0	Queue1	16	Queue3	32	Queue5	48	Queue7
1	Queue1	17	Queue3	33	Queue5	49	Queue7
2	Queue1	18	Queue3	34	Queue5	50	Queue7
3	Queue1	19	Queue3	35	Queue5	51	Queue7
4	Queue1	20	Queue3	36	Queue5	52	Queue7
5	Queue1	21	Queue3	37	Queue5	53	Queue7
6	Queue1	22	Queue3	38	Queue5	54	Queue7
7	Queue1	23	Queue3	39	Queue5	55	Queue7
8	Queue2	24	Queue4	40	Queue6	56	Queue8
9	Queue2	25	Queue4	41	Queue6	57	Queue8
10	Queue2	26	Queue4	42	Queue6	58	Queue8
11	Queue2	27	Queue4	43	Queue6	59	Queue8
12	Queue2	28	Queue4	44	Queue6	60	Queue8
13	Queue2	29	Queue4	45	Queue6	61	Queue8
14	Queue2	30	Queue4	46	Queue6	62	Queue8
15	Queue2	31	Queue4	47	Queue6	63	Queue8

Parameter description

Name	Description
DSCP	It specifies the priority level (range: 0 to 63) defined by DS field of the IP packet.
Port Queue	It specifies the scheduler queue of the corresponding DSCP priority.

6.6 Port priority

Click **QoS Policy** > **Port Priority** to enter the page. On this page, you can configure the trust mode and CoS priority for the physical ports of the switch.



Parameter description

Name	Description
Port	It specifies the ID of the port.
CoS Priority	It specifies the CoS priority of the physical ports. When the switch receives messages not in accordance with the trust mode rules or the port is in non-trust mode, the messages join the queues based on the CoS priority.
Trust Mode	It specifies the method which the port uses to process the received messages. – **Non-Trust**: All messages received by the port join the queues according to the correspondence of the configured CoS priority. – **802.1P Trust**: When the port receives VLAN messages, the messages join the queues according to the correspondence of the 802.1P. When the port receives other messages, the messages rejoin queues according to the correspondence of the CoS priority. – **DSCP Trust**: When the port receives IP messages, the messages join queues according to the correspondence of the DSCP. When the port receives other messages, the messages rejoin queues according to the correspondence of the CoS priority.

7 Network security

7.1 ACL

7.1.1 Overview

ACL (Access Control List) is used to filter messages by configuring matching rules and operations. After the message is received by the port of the switch, it is analyzed according to the ACL rules of this port. And these rules decide what packets can pass and what should be rejected, which can effectively prevent illegal users from accessing the network and improve network security.

This switch supports ACL based on two matching rules: MAC address and IP address.

- MAC ACL: Match the filtering rules according to the source MAC address and destination MAC address of the layer-2 data frame.
- IP ACL: Match the filtering rules based on the source IP address and destination IP address of the layer-3 packet IP head.

An ACL ID can be configured with multiple ACL matching rules, and the message matches the rule according to rule priority. Once a message is matched to a rule with a higher priority, it stops matching to other rules.

7.1.2 Configuration guidance

Flitering rules based on MAC address

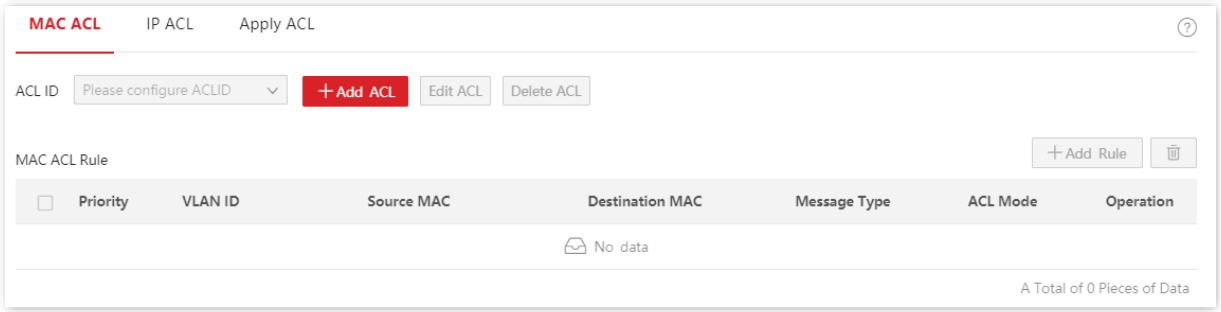
Step	Task	Description
1	MAC ACL	**Required.** You can configure the filtering rule that matches the source and destination MAC addresses of the layer 2 data frame. Multiple MAC ACL rules can be configured with one ACL ID.
2	Apply ACL	**Required.** The MAC ACL rule takes effect when it is applied to the corresponding port of the switch.

Flitering rules based on IP address

Step	Task	Description
1	IP ACL	**Required.** You can configure the filtering rule that matches the source and destination IP addresses of the layer 3 data packet. Multiple IP ACL rules can be configured with one ACL ID.
2	Apply ACL	**Required.** The IP ACL rule takes effect when it is applied to the corresponding port of the switch.

7.1.3 MAC ACL

Click **Network Security** > **ACL** > **MAC ACL** to enter the page. On this page, you can view and configure the MAC ACL rules.



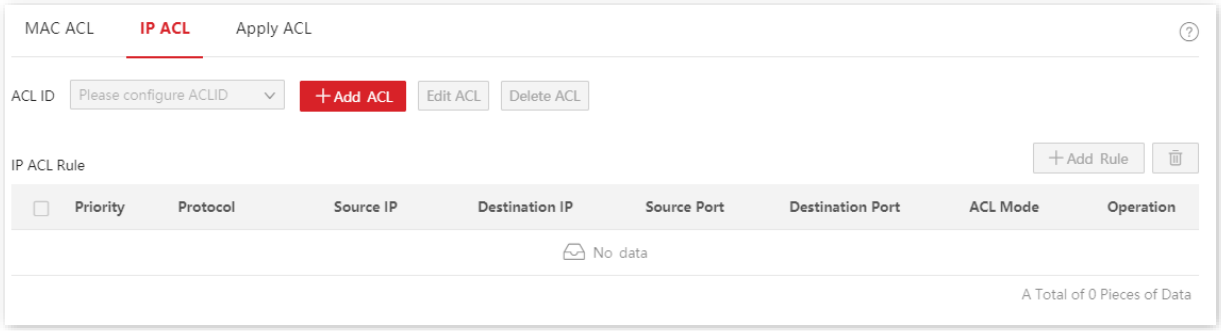
Parameter description

Name	Description
ACL ID	It specifies the ACL ID of the MAC ACL rule. You should add ACL ID here before configuring the MAC ACL rules.
Priority	This field specifies the priority of a rule. A smaller value indicates a higher priority. The message starts matching from the rule with the highest priority. Once matched, the message stops checking rules.
VLAN ID	It specifies the VLAN to which the message belongs. If this field is not configured, it indicates messages of all VLANs.
Source MAC	It specifies the source MAC address of the message. – **Any MAC**: It specifies all MAC addresses. – **Specified MAC**: Combined with mask, it is used to specify a certain MAC address or MAC address segment.
Destination MAC	It specifies the destination MAC address of the message. – **Any MAC**: It specifies all MAC addresses. – **Specified MAC**: Combined with mask, it is used to specify a certain MAC address or MAC address segment.

Name	Description
Message Type	It specifies the message type of the layer-2 data frame. If this field is not configured, it indicates any message type.
ACL Mode	It specifies the ACL mode in which the switch processes the messages that match the rule. – **Allow**: Forward the messages that match the rule. – **Forbid:** Discard the messages that match the rule.

7.1.4 IP ACL

Click **Network Security** > **ACL** > **IP ACL** to enter the page. On this page, you can view and configure the IP ACL rules.



Parameter description

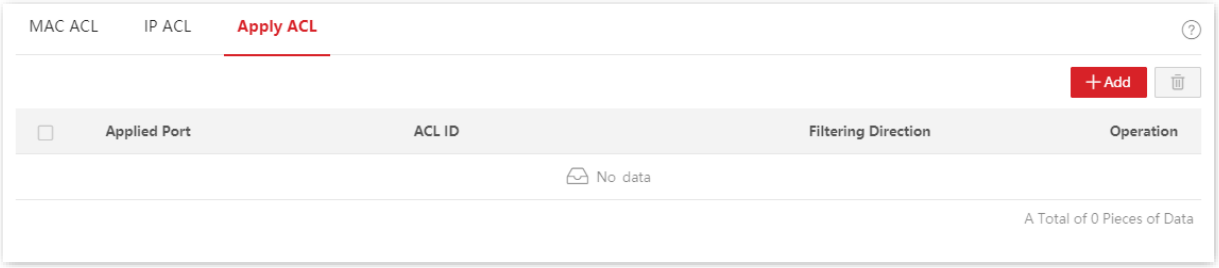
Name	Description
ACL ID	It specifies the ACL ID of the IP ACL rule. You should add ACL ID here before configuring the IP ACL rules.
Priority	It specifies the priority of the rule. A smaller value indicates a higher priority. The message starts matching from the rule with the highest priority. Once matched, the message stops checking rules.
Protocol	It specifies the protocol type of the message, such as IP, ICMP, and so on. You can also enter the protocol number manually.
Source IP	It specifies the source IP address of the message. – **Any IP**: It indicates all IP addresses. – **Specified IP**: Combined with mask, it indicates a certain network address.
Destination IP	It specifies the destination IP address of the message. – **Any IP**: It indicates all IP addresses. – **Specified IP**: Combined with mask, it indicates a certain network address.
Source Port	When the protocol type is TCP or UDP, you can enter the source port number of the message.
Destination Port	When the protocol type is TCP or UDP, you can enter the destination port number of the message.

Name	Description
ACL Mode	It specifies the ACL mode in which the switch processes the messages that match the rule. – **Allow**: Forward the messages that match the rule. – **Forbid:** Discard the messages that match the rule.

7.1.5 Apply ACL

The ACL rules take effect when being applied to physical ports.

Click **Network Security** > **ACL** > **Apply ACL** to enter the page. On this page, you can apply the configured ACL rules to physical ports.



Parameter description

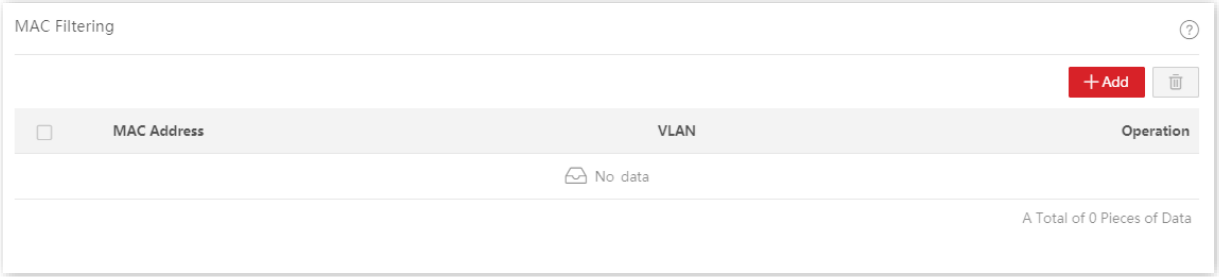
Name	Description
Applied Port	It specifies the physical port number to which the ACL rule applies.
ACL ID	It specifies the ACL rule applied to the port.
Filtering Direction	It specifies the message filtering direction of the port. Only **Ingress** is supported by this switch.

7.2 MAC filtering

With this function enabled, the switch checks the source MAC address and destination MAC address of the received packets. If the source MAC address or destination MAC address of a packet exists in the MAC filtering list, the packet will be discarded.

MAC filtering can effectively prevent illegal users from accessing the network, thus improving network security.

Click **Network Security** > **MAC Filtering** to enter the page. On this page, you can configure the MAC filtering rules.



Parameter description

Name	Description
MAC Address	It specifies the MAC address to be filtered. When the source MAC address or destination MAC address of a packet is the same as the listed MAC address, the packet is discarded.
VLAN	It specifies the VLAN in which the MAC filtering rule takes effect.

7.3 802.1X

7.3.1 Overview

802.1X is a network access control technology brought up by the IEEE. It is used to authenticate and control LAN users. The authentication system involves three parties: client, device, and authentication server.

- Authentication client: A client device sends an authentication request and the authentication server in LAN verifies its validity. A client software supporting 802.1X authentication is required.
- Authentication device: It provides interface for the client to connect to LAN. It is located between the client and the authentication server, and decides whether the client can access LAN or not according to the message returned by the authentication server.
- Authentication server: It provides authentication service for clients. The commonly used one is the RADIUS (Remote Authentication Dial-In User Service) server. The authentication server decides whether the client passes the authentication according to the client authentication message sent by the authentication device, and notifies the result to the authentication device. The device decides whether the client can access LAN or not.

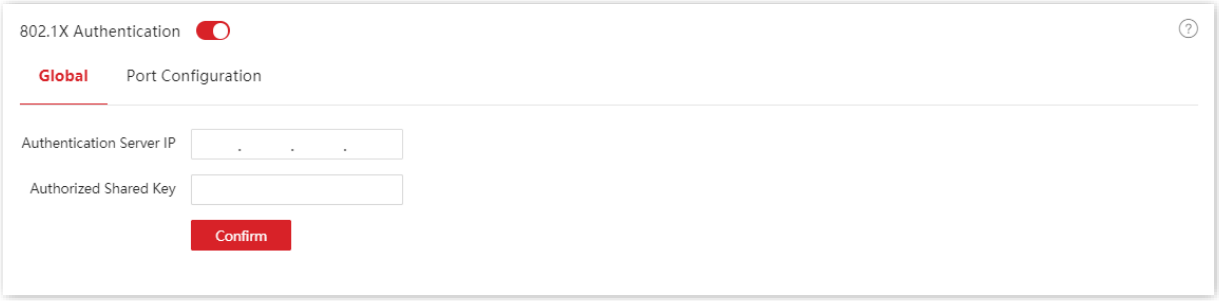
This switch serves as the authentication device in the authentication system. It communicates with the authentication server by means of EAP termination. After receiving the EAP message from the client, the switch encapsulates the client authentication information from the message into the standard RADIUS message, and then forwards the RADIUS message to the authentication server. The basic diagram of the authentication system is shown as follows.

This switch only supports authentication based on port access. If one of the users passes the authentication, the port becomes authorized, and the following users who use this port can access the network without authentication. However, when this user is offline, the port becomes unauthorized, and all the other users under this port are unable to access the network.

7.3.2 Global

Click **Network Security** > **802.1X** > **Global** to enter the page. On this page, you can configure

the parameters of 802.1X authentication server.

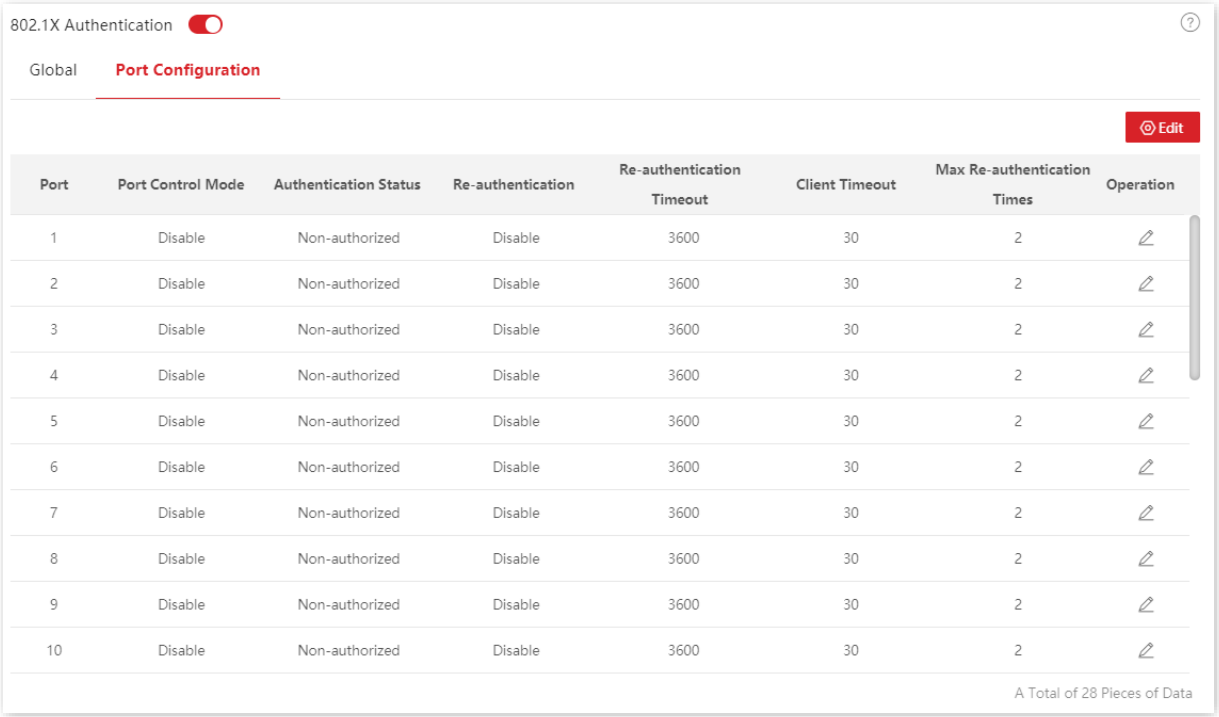


Parameter description

Name	Description
802.1X Authentication	It is used to enable/disable the 802.1X Authentication function.
Authentication Server IP	It specifies the IP address of the RADIUS authentication server. There should be reachable routes between the RADIUS authentication server and this switch.
Authorized Shared Key	It specifies the shared key of a RADIUS authentication/authorization message. It must be the same as the key set at the RADIUS authentication/authorization server side.

7.3.3 Port configuration

Click **Network Security** > **802.1X** > **Port Configuration** to enter the page. On this page, you can configure the 802.1X authentication parameters for each port.



Parameter description

Name	Description
Port	It specifies the ID of the port.
Port Control Mode	It specifies the control mode of the port to access the network. – **Auto:** The 802.1X authentication is enabled on the port. The initial state is unauthorized and the user cannot access the network resources. If a user passes the authentication, the port is authorized and the user is allowed to access the network resources. – **Mandatory Authorization:** The port is always in the authorization state. It allows users to access the network resources. – **Mandatory Non-authorization**: The port is always in the non-authorization state. It forbids users to access the network resources without authentication and authorization. – **Disable**: The authentication is disabled on the port. It allows users to access the network resources.
Authentication Status	It specifies the authentication status of the port. – **Authorized:** The user is allowed to access the network resources over the port. – **Non-authorized:** The user is not allowed to access the network resources over the port.
Re-authentication	It is used to enable/disable the 802.1X re-authentication function of the port. With the function enabled, the switch periodically sends re-authentication request to the authentication client to check the connection status and confirm that the authentication client is online.
Re-authentication Timeout	It specifies the interval at which the switch launches re-authentication to authentication clients. If the re-authentication function is enabled on a port, the switch launches re-authentication requests to the online devices connected to the port at this interval.
Client Timeout	It specifies the timeout period in which the client responds to the re-authentication request. After the switch sends a re-authentication request message to a client, if the switch does not receive any response in this time period, the switch will send the message again.
Max Re-authentication Times	It specifies the maximum times of failed re-authentication for a client. The switch forces the client offline if the failed re-authentication times of the client exceeds this value.

7.4 Attack defense

7.4.1 Overview

These switch support three attack defense methods: ARP Attack Defense, DoS (Denial of Service) Attack Defense and MAC Address Attack Defense.

- **ARP Attack Defense**

  ARP received rate is set to prevent ARP messages in LAN from being overwhelmingly sent to a port, resulting in CPU overload and leading to function failure or even device malfunction.

  If the ARP received rate of the switch exceeds the threshold value you set, the switch randomly discards some ARP messages to ensure that the ARP received rate is within the threshold value you set.

- **DoS Attack Defense**

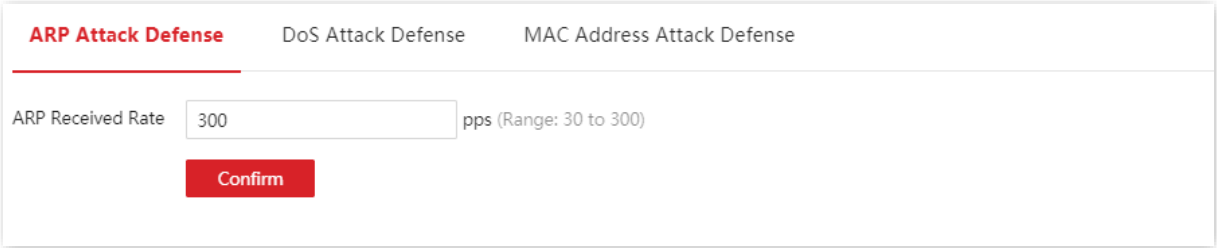
  The DoS Attack Defense function is used to prevent some hosts from maliciously consuming server resources by sending a large number of service requests, leaving other hosts unable to use network services properly.

- **MAC Address Attack Defense**

  MAC Address Attack Defense limits the switch to learn MAC address, so as to prevent it from constantly learning a large number of invalid message source MAC addresses in LAN which can enlarge the MAC address forwarding table and result in forwarding performance degradation.

7.4.2 ARP attack defense

Click **Network Security** > **Attack Defense** > **ARP Attack Defense** to enter the page. On this page, you can configure the threshold value of the switch's ARP Received Rate.

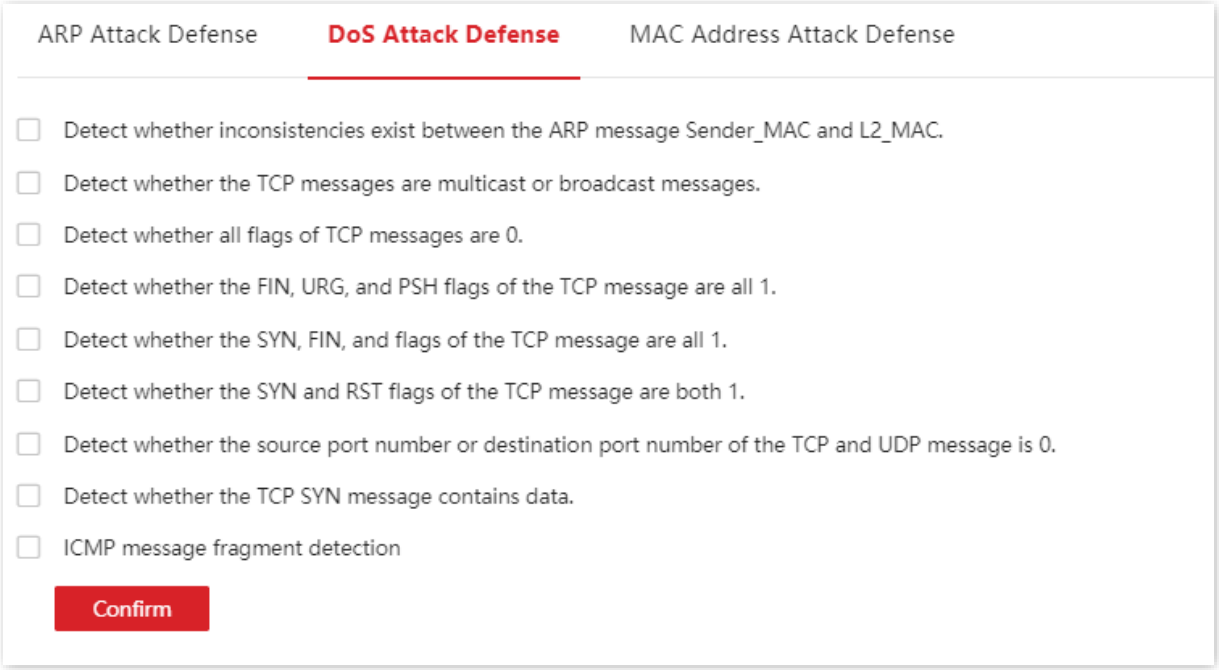


Parameter description

Name	Description
ARP Received Rate	It specifies the maximum rate at which the switch receives the ARP messages. If the ARP messages received by the switch within 1 second exceed this threshold value, the switch is considered to be attacked by ARP, and the switch will randomly discard some ARP messages.

7.4.3 DoS attack defense

Click **Network Security** > **Attack Defense** > **DoS Attack Defense** to enter the page. On this page, you can configure DoS Attack Defense rules.

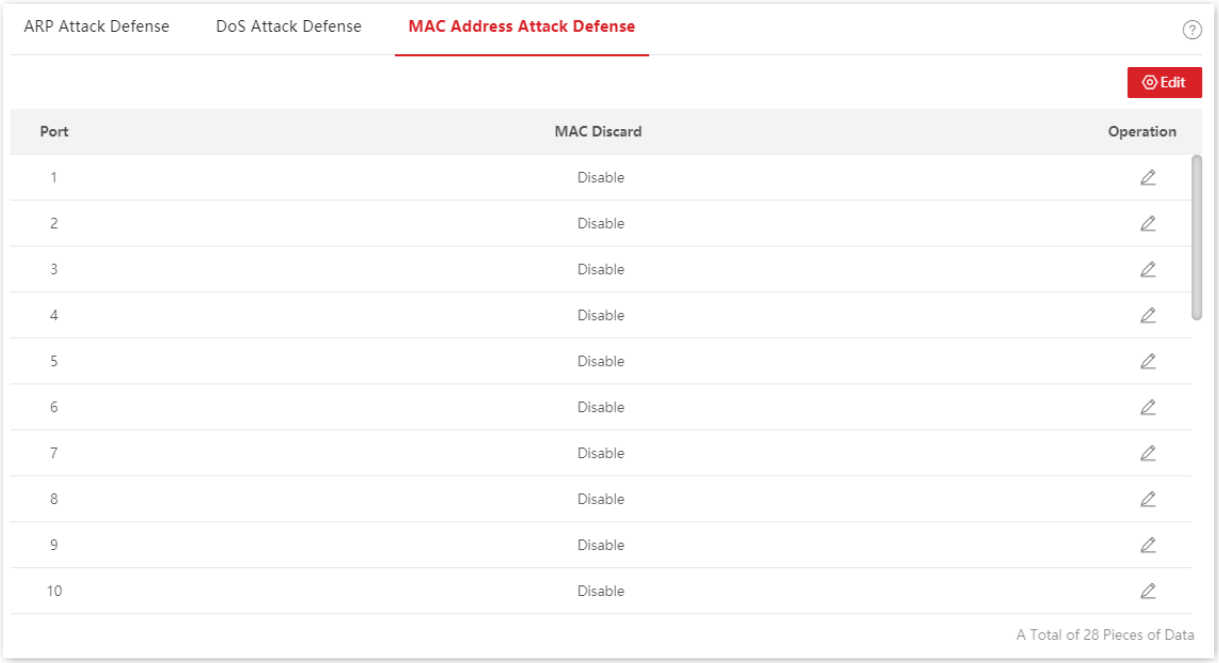


Parameter description

Name	Description
Detect whether inconsistencies exist between the ARP message Sender_MAC and L2_MAC.	After it is ticked, the switch does not forward ARP messages with inconsistent Sender_MAC and L2_MAC.
Detect whether the TCP messages are multicast or broadcast messages.	After it is ticked, the switch does not forward multicast or broadcast TCP messages.
Detect whether all flags of TCP messages are 0.	After it is ticked, the switch does not forward TCP messages whose flags are all 0.
Detect whether the FIN, URG, and PSH flags of the TCP message are all 1.	After it is ticked, the switch does not forward the TCP message whose FIN, URG, and PSH flags are all 1.
Detect whether the SYN, FIN, and flags of the TCP message are all 1.	After it is ticked, the switch does not forward the TCP message whose SYN and FIN flags are all 1.
Detect whether the SYN and RST flags of the TCP message are both 1.	After it is ticked, the switch does not forward the TCP message whose SYN and RST flags are both 1.
Detect whether the source port number or destination port number of the TCP and UDP message is 0.	After it is ticked, the switch does not forward the TCP and UDP message whose source port number or destination port number is 0.
Detect whether the TCP SYN message contains data.	After it is ticked, the switch does not forward the TCP SYN message that contains data.
ICMP message fragment detection	After it is ticked, the switch does not respond to the fragmented ICMP message.

7.4.4 MAC address attack defense

Click **Network Security** > **Attack Defense** > **MAC Address Attack Defense** to enter the page. On this page, you can configure whether the port can forward the unknown unicast message.



Parameter description

Name	Description
Port	It specifies the ID of the port.
MAC Discard	With this function enabled, the port no longer learns the MAC addresses and discards the received unknown unicast messages.

8 Device settings

8.1 User management

Assigning different access permissions to different types of users can reduce the risk of the switch's configuration from being tampered.

This switch supports three types of users: administrator, operation user, and common user.

- **Administrator**

  There is only one administrator created by the system by default. The administrator can perform operations of all functions. The default username and password are both admin.

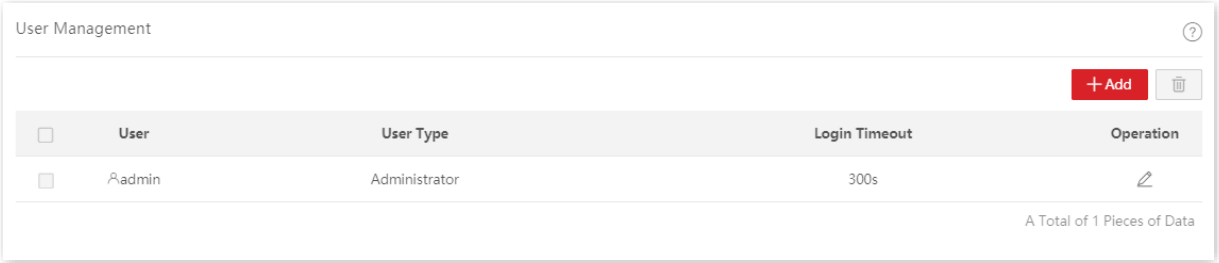
- **Operation User**

  An operation user can perform all operations besides firmware upgrade, reset or user management.

- **Common User**

  A common user can check configuration of the switch.

  Click **Device Settings** > **User Management** to enter the page. On this page, you can add users of this switch (8 users at most).



Parameter description

Name	Description
User	It specifies the user name.
User Type	It specifies the types of users. This switch supports three types of users: administrator, operation user and common user.

Name	Description
Login Timeout	If a user performs no operation on the web UI within the interval, the system logs the user out.

8.2 SNMP

8.2.1 Overview

SNMP (Simple Network Management Protocol) enables a network management station to remotely manage the network devices supporting this protocol, including monitoring network status, modifying network device configuration, receiving network event alarms, and so on.

SNMP can shield the physical differences between devices and realize automatic management of devices from different vendors.

SNMP management framework

SNMP management framework consists of three parts: SNMP manager, SNMP agent and MIB (Management Information Base).

- SNMP manager: A system used for controlling and monitoring network nodes by SNMP. The most commonly used is NMS (Network Management System), which can be a server specially used for network management or an application program for executing management function on a certain network device.
- SNMP agent: Software which runs on managed devices for maintaining management information and reporting management data to a SNMP management system when it is needed.
- MIB: It is a collection of managed objects. When NMS manages the devices, some functional parameters of the managed devices are required, such as the port state, CPU utilization and the like, which are also called managed objects. MIB defines a series of properties for those managed objects: object name, access right, data type, and so on. Each SNMP agent has its corresponding MIB and the SNMP manager can perform read/write operations according to management permissions.

SNMP agent is managed by SNMP manager in the SNMP network and they interact with each other via SNMP.

SNMP basic operations

The following three basic operations are available for this switch to achieve intercommunication between the SNMP manager and SNMP agent:

- Get: The SNMP manager-uses it to retrieve the value(s) of one or more objects of the SNMP agent.
- Set: The SNMP manager-uses it to reconfigure the value(s) of one or more objects in MIB.
- Trap: The SNMP agent uses it to send alert information to SNMP manager.

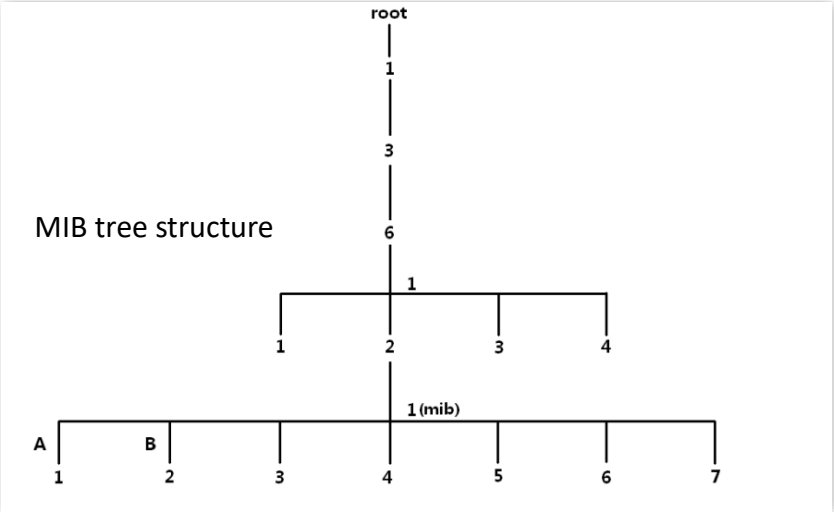
SNMP versions

This switch is compatible with SNMPv1, SNMPv2c and SNMPv3.

- SNMPv3 adopts the authentication method with user name and password.
- SNMPv1 and SNMPv2c adopt Community Name authentication. If the community name of the SNMP message fails to pass the authentication, the message will be discarded. The SNMP community name defines the relationship between SNMP manager and SNMP agent. It functions as a password that limits the SNMP manager to access SNMP agent of the switch.

MIB introduction

MIB features a tree structure and each tree node represents a managed object. An object can be identified with a string of numbers which indicate a path starting from the root. The number string is the OID (Object Identifier). In the following figure, the OID of the object A is (1.3.6.1.2.1.1); while object B is (1.3.6.1.2.1.2).



View

The MIB view is a subset of all managed objects in MIB. A managed object is represented by OID, and the configured view rule (**include**/**exclude**) decides whether the object is managed or not. OID of each managed object can be found on the SNMP management software.

Group

After creating the view, the SNMP groups are required to be created. You can assign different access permissions to users in different groups by adding different views to SNMP groups.

User

After creating the groups, you can add users for each group. The SNMP manager uses the user name and authentication/encryption password created here to log in to the SNMP agent.

Community

For SNMPv1 and SNMPv2c, after the view is created, the community is required to be created. The group name functions as a password for SNMP manager authentication. View access permissions of each group can be added here to achieve access permission management.

8.2.2 Configuration guidance

- **SNMPv3**

Step	Operation	Description
1	Basic	**Required.** Enable the SNMP agent function.
2	Create views	**Optional.** Create views for the managed objects in the View List on Permission Control page. A view named Default is created by system by default.
3	Create groups	**Required.** Create SNMP groups in the Group List on Permission Control page, and add views with different access permissions for the groups.
4	Create users	**Required.** Create SNMP users in the User List on Permission Control page, and configure the authentication/encryption mode as well as password.
5	Configure notification	**Optional.** Configure the notification with the security version of v3 on Notification page.

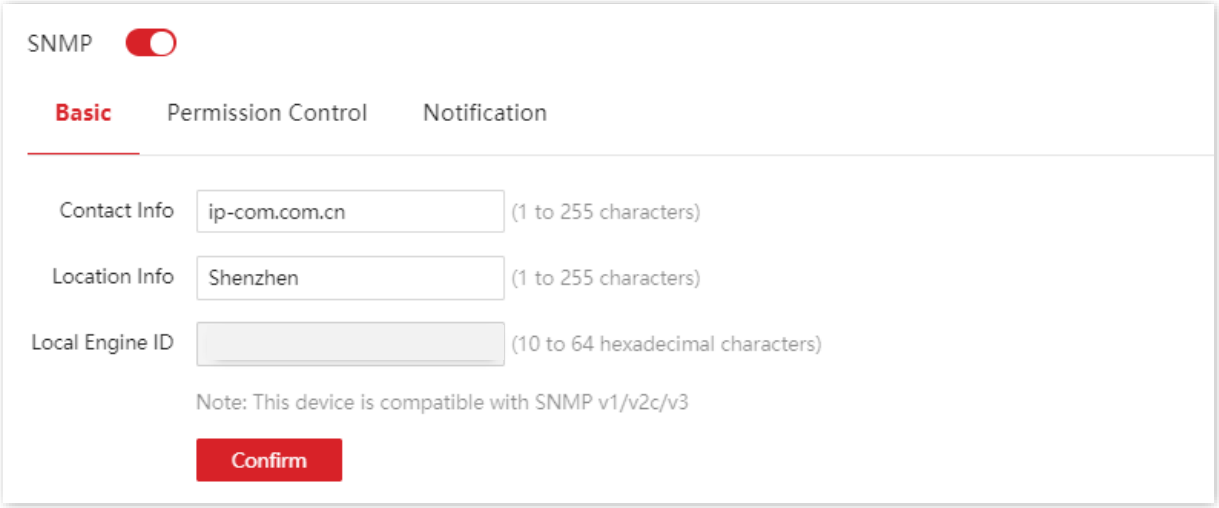
- **SNMPv1/SNMPv2c**

Step	Operation	Description
1	Basic	**Required.** Enable the SNMP agent function.
2	Create views	**Optional.** Create views for the managed objects in the **View List** on Permission Control page. A view named **Default** is created by system by default.

Step	Operation	Description
3	Create communities	**Required.** Create SNMP communities in the **Community List** on Permission Control page.
4	Configure notification	**Optional.** Configure the notification with the security version of v1/v2c on Notification page.

8.2.3 Basic

Click **Device Settings** > **SNMP** > **Basic** to enter the page. On this page, you can configure the basic SNMP parameters.



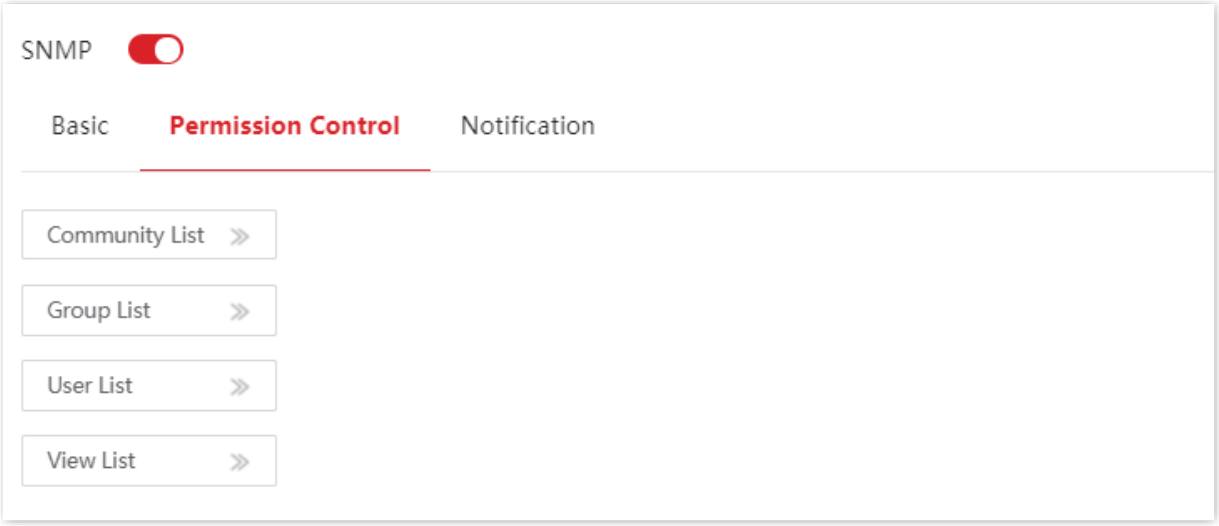
Parameter description

Name	Description
SNMP	It is used to enable/disable the SNMP function.
Contact Info	It is used to configure the contact info of the switch for the SNMP manager to fast locate this switch. The default is ip-com.com.cn, and you can modify it by yourself.
Location Info	It is used to configure the location info of the switch for the SNMP manager to fast locate this switch. The default is Shenzhen, and you can modify it by yourself.
Local Engine ID	It specified the Local Engine ID of the switch. You need to enter this ID at the SNMP manager side in order to manage the switch.

8.2.4 Permission control

Click **Device Settings** > **SNMP** > **Permission Control** to enter the page. On this page, you can

configure the SNMP permissions.



Parameter description

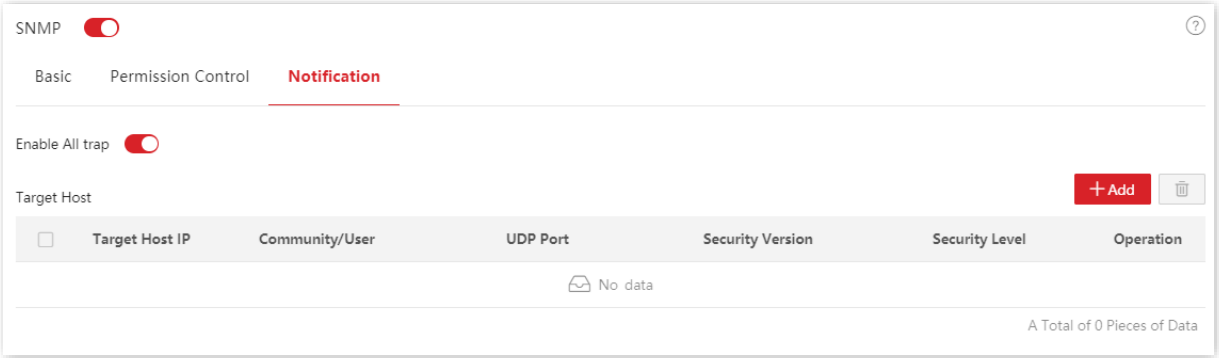
Name		Description
Community List	Community Name	It specifies the name of a community.
	Access Rule	It specifies the access permission for the community to access the views, including **Read Only** and **Read&Write.**
	MIB View	It specifies the views that community can access. The MIB view should be configured in **View List** in advance.
Group List	Group Name	It specifies the name of a group.
	Security Level	It specifies the security level of the group: **No Security**, **Authentication**, **Authentication&Privacy**.
	Read Only	Control the access permissions for users in a group through the view. At least one of the three types should be configured. The MIB view should be configured in **View List** in advance.
	Read&Write	
	Notification	
User List	User Name	It specifies the name of the user.
	User Group	It specifies the group of the user. The group needs to be configured in **Group List** in advance.
	Security Level	It specifies the security level of the user. After the user's group is selected, the security level is filled in automatically.
	Authentication Mode	It specifies the user's authentication mode. This switch only supports MD5 (MD5 Message Digest Algorithm). This parameter can be set only if the security level of the group is **Authentication** or **Authentication&Privacy**.
	Authentication Password	It specifies the authentication password of the user. This parameter can be set only if the security level of the group is **Authentication** or **Authentication&Privacy**.

Name		Description
	Security Mode	It specifies the security mode of the user. This switch supports two security modes: AES and DES. This parameter can be set only if the security level of the group is **Authentication&Privacy**.
	Security Password	It specifies the security password of the user. This parameter can be set only if the security level of the group is **Authentication&Privacy**.
View List	View Name	It specifies the name of a view.
	Rule	It specifies the OID rule. – **include**: This OID can be managed by SNMP. – **exclude**: This OID cannot be managed by SNMP.
	MIB Subtree OID	It specifies the managed objects (represented by OID) of the view.

8.2.5 Notification

The notification function allows the switch to use the Trap mechanism to report important events (such as a device reboot) of the views, so the manager can monitor and deal with the specific events of the switch with SNMP management software.

Click **Device Settings** > **SNMP** > **Notification** to enter the page. On this page, you can configure the SNMP notification function.



Parameter description

Name	Description
Enable All trap	It is used to enable/disable the Trap function.
Target Host IP	It specifies the IP address of trap target host, which is also the IP address of the managed host. Ensure that there are reachable routes between the target host and this switch.
Community/User	It specifies the community name, user name or group name required by authentication.

Name	Description
	You need to enter the corresponding group name, user name or community name. If the **Security Version** is set to **v3**, only a user name or group name is allowed. If the **Security Version** is set to **v1** or **v2c**, only a community name is allowed.
UDP Port	It specifies the UDP port enabled for Trap on the managed host.
Security Version	It is used to select a security version used by Trap, including v1, v2c and v3, which should be consistent with the version of the SNMP manager.
Security Level	When the Security Version is set to v3, you need to select a security level. The Security Level includes **No Security**, **Authentication**, and **Authentication&Privacy**.

8.3 System time

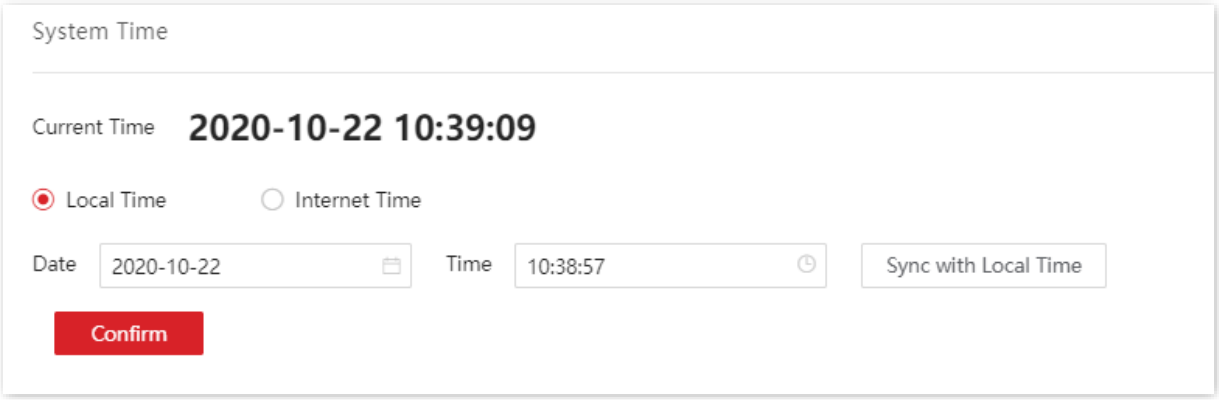
To ensure that the time-based functions of the switch work properly, it is necessary to ensure that the system time of the switch is accurate. This switch supports manual setting and internet calibration.

To access the page, click **Device Settings** > **System Time**.

8.3.1 Manual setting

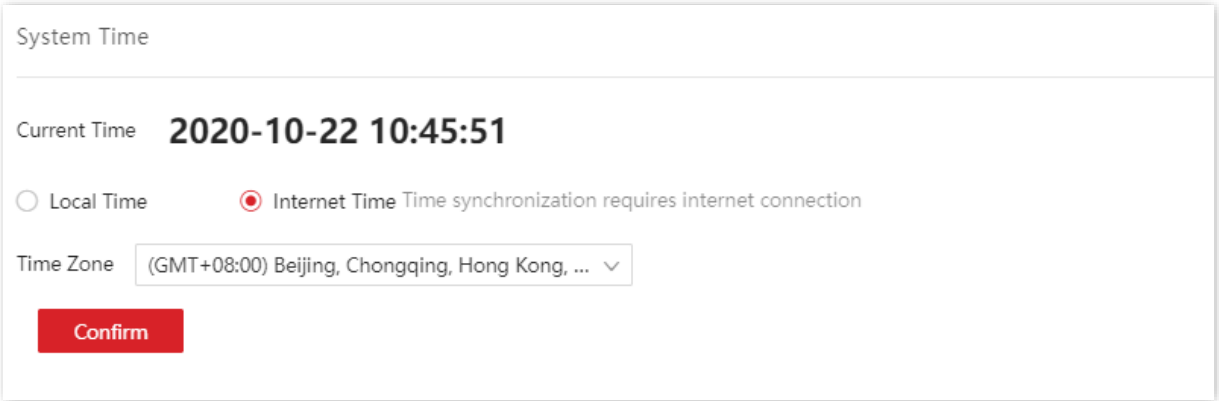
The network administrator needs to manually set the system time of the switch. After the switch restarts for each time, the administrator needs to reset it.

You can manually modify the date and time, or you can click **Sync with Local Time** to synchronize the time of the switch with the management device.



8.3.2 Internet calibration

The switch can automatically synchronize with the Internet time server. As long as the switch can access the internet, it can automatically calibrate its system time. After the switch reboots, it can also calibrate the time automatically.



8.4 Log management

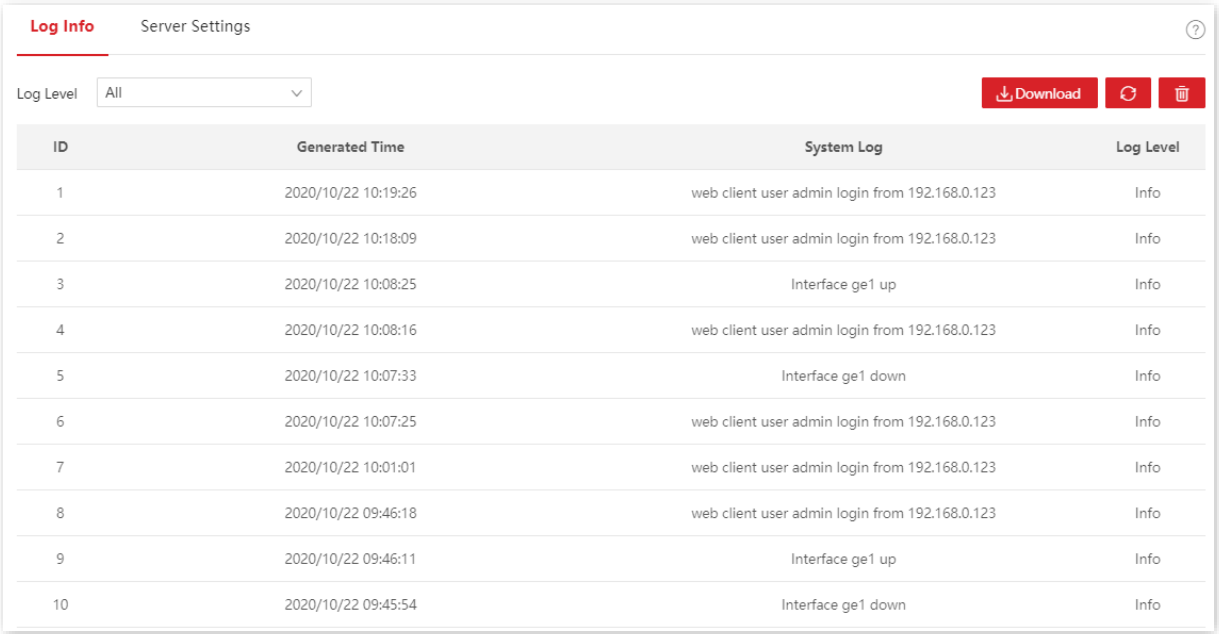
8.4.1 Log info

The logs of a switch record all events and the user's operations after the switch is reset from the last time. You can check the log info of the switch for troubleshooting if there is any network fault.

The logs are divided into eight levels based on importance and can be filtered according to the log level. The smaller the value, the higher the emergency level.

Log level	Value	Description
Emergency	1	System unavailable information
Alert	2	Message that needs to be quickly responded
Critical	3	Critical information
Error	4	Error information
Warning	5	Warning information
info	7	Notification that needs to be recorded
debug	8	Message generated in debugging process

Click **Device Settings** > **Log Management** > **Log Info** to enter the page. On this page, you can view, download and delete the log info of the switch.



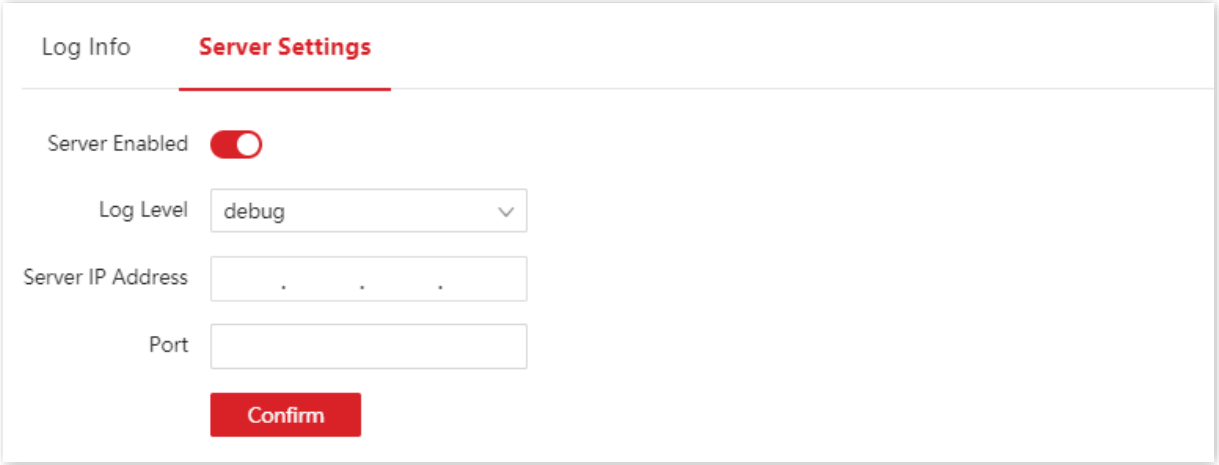
Parameter description

Name	Description
Log Level	It is used to filter which logs are displayed by log level.

Name	Description
ID	It specifies the log ID.
Generated Time	It specifies the time point when the log is generated.
System Log	It displays the content of the log.
Log Level	It specifies the level of the log.

8.4.2 Server settings

Click **Device Settings** > **Log Management** > **Server Settings** to enter the page. On this page, you can configure the log server and upload the log info of the switch to the server.



Parameter description

Name	Description
Server Enabled	It is used to enable/disable the log server.
Log Level	Logs of this level and above will be uploaded to the server.
Server IP Address	It specifies the IP address of the log server. Ensure that there are reachable routes between the log server and this switch.
Port	It specifies the port in transport layer used by the log server.

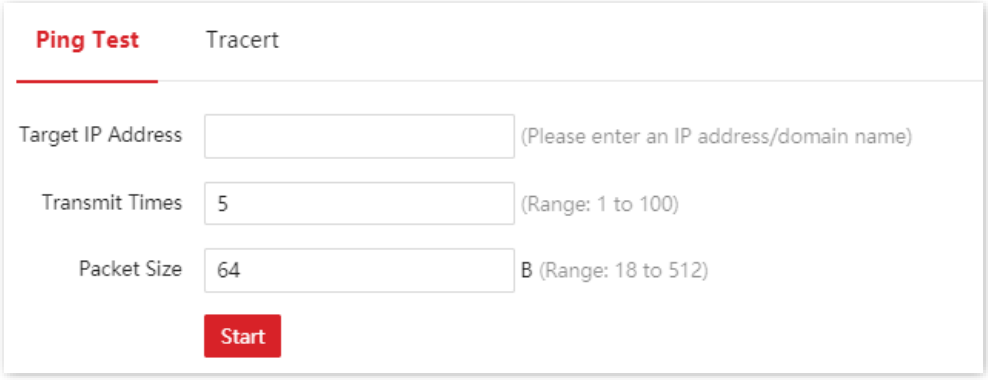
8.5 Diagnostics

Click **Device Settings** > **Diagnostics** to enter the page. On this page, you can perform Ping/Tracert test.

- Ping test: It is used to test network connection and connection quality.
- Tracert test: It is used to test the routes of the packets from switch to the target host.

8.5.1 Ping test

Click **Device Settings** > **Diagnostics** > **Ping Test** to enter the page. On this page, you can test the network connection and connection quality.

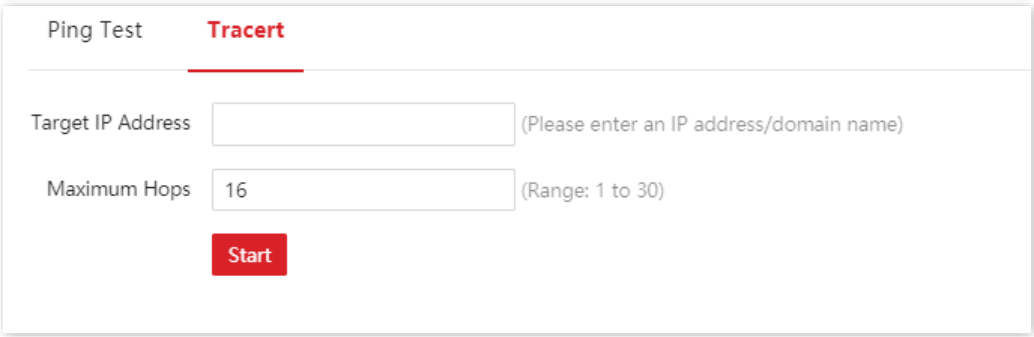


Parameter description

Name	Description
Target IP Address	It specifies the IP address or domain name of the destination device to be pinged.
Transmit Times	It specifies the number of data packets sent by Ping.
Packet Size	It specifies the size of data packets sent by Ping.

8.5.2 Tracert test

Click **Device Settings** > **Diagnostics** > **Tracert** to enter the page. On this page, you can test the routes of the packet from the switch to the destination device.



Parameter description

Name	Description
Target IP Address	It specifies the IP address or domain name of the destination device to be tested.
Maximum Hops	It specifies the survival time of the message, which is the maximum number of routers that the message can pass through.

8.6 IMS cloud

8.6.1 Overview

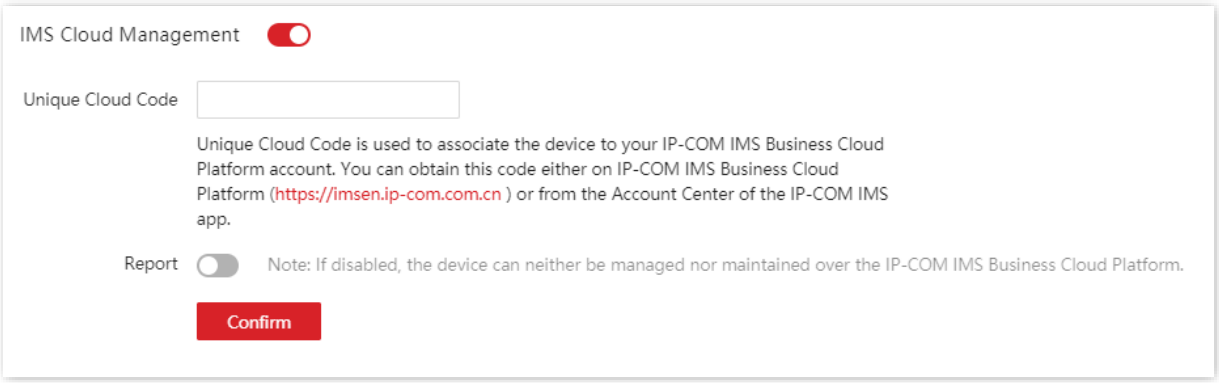
IP-COM IMS Business Cloud Platform is a cloud platform established by IP-COM, providing central management for IP-COM devices that support IMS cloud management.

With this switch managed by the IMS cloud platform, you can configure and check the parameters of the switch on the IMS cloud platform. You can also configure and check these parameters on the web UI of the switch.

To enable IMS Cloud Management function of the switch, click **Device Settings** > **IMS Cloud** to enter the page.

Tip

- Please ensure that the switch can access the internet, otherwise it cannot be managed by the IMS cloud platform.
- With the switch managed by the IMS cloud platform, you can modify the parameters of the switch on both the IMS cloud platform or web UI of the switch. The parameters of the switch take effect based on the last modification.



Parameter description

Name	Description
IMS Cloud Management	It is used to enable or disable the IMS Cloud Management function.
Unique Cloud Code	It is used to associate the device with your IP-COM IMS Business Cloud Platform account. Methods to obtain this code: – **IMS cloud platform**: Log in to the IP-COM IMS Business Cloud Platform, click your account name on the upper right corner, and you can find Unique Cloud Code on the drop-down list. – **IMS app**: Find it in the Account Center of the IP-COM IMS app.

Name	Description
Report	Only with this function enabled, the switch can be managed by the IMS cloud platform, and its configuration can be reported to the IMS cloud platform.

8.6.2 Configure IMS cloud management

1. Configure such parameters of the switch as the IP address, DNS server address, and default route to make the switch accessible to the internet.

Tip

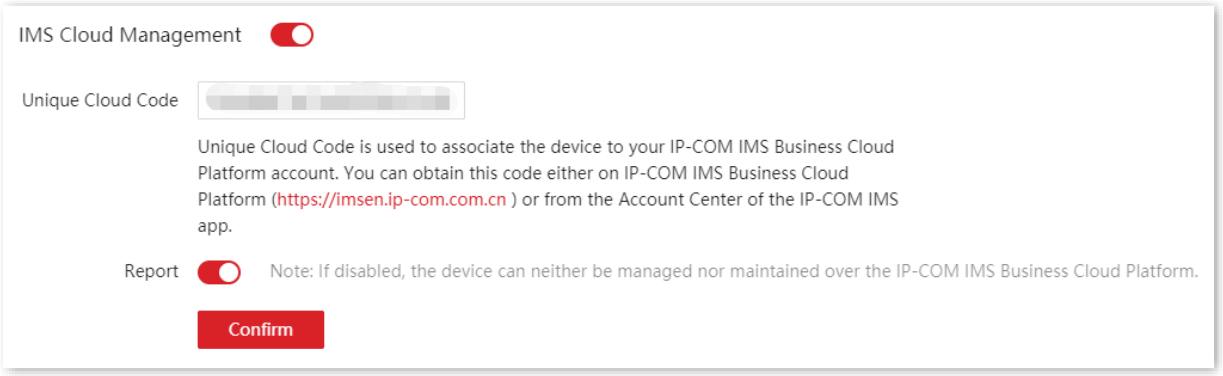
Refer to Configure the switch to access the internet if necessary.

2. Enable the IMS Cloud Management function of the switch.

   (1) Choose **Device Settings** > **IMS Cloud,** and enable the **IMS Cloud Management** function.

   (2) Log in to the IP-COM IMS cloud platform and copy the unique cloud code.

   (3) Paste the unique cloud code in the **Unique Cloud Code** box. Enable the **Report** function, and click **Confirm**.



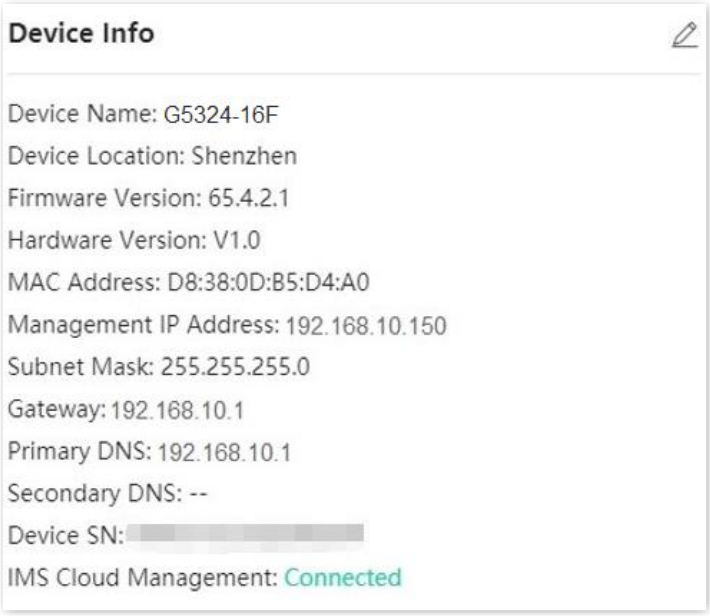
3. Log in to the IMS cloud platform and add the switch to a project.

   (1) Log in to the IMS cloud platform, click the account icon on the upper right corner of the page, and select **Device-Joining Alert** from the drop-down list.

   (2) Find the switch from the list and add it to a project.

----End

After successful configuration, you can find the status of IMS Cloud Management on **Basics** > **System Summary** page is Connected, which indicates that you can use the IMS cloud platform to remotely manage the switch.


Device Info
Device Name: G5324-16F
Device Location: Shenzhen
Firmware Version: 65.4.2.1
Hardware Version: V1.0
MAC Address: D8:38:0D:B5:D4:A0
Management IP Address: 192.168.10.150
Subnet Mask: 255.255.255.0
Gateway: 192.168.10.1
Primary DNS: 192.168.10.1
Secondary DNS: --
Device SN:
IMS Cloud Management: Connected

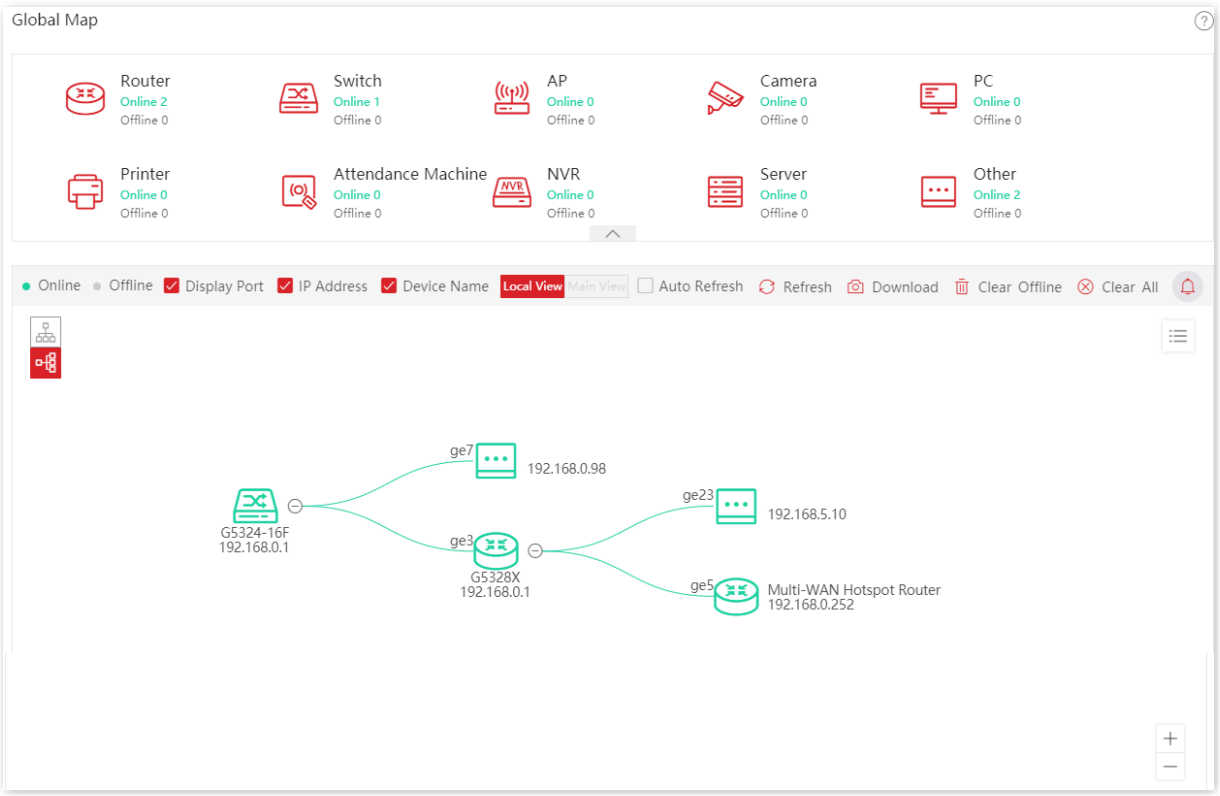
9 Visualization

For some networks that need not access the internet (such as medium and large security monitoring networks), IMS cloud management is unavailable. Visualization function of this switch provides central management and maintenance for these networks.

With the Visualization function, the switch can locally manage the devices in the network. Based on such protocols as LLDP, UPnP, and ARP, the system can automatically discover the devices connected to this switch (such as router, switch, IP camera, AP), and generate a network topology, on which you can view and configure the basic parameters of these devices.

9.1 Global map

Click **Visualization** > **Global Map** to enter the page. On this page, you can view and configure the basic parameters of the devices connected to this switch.



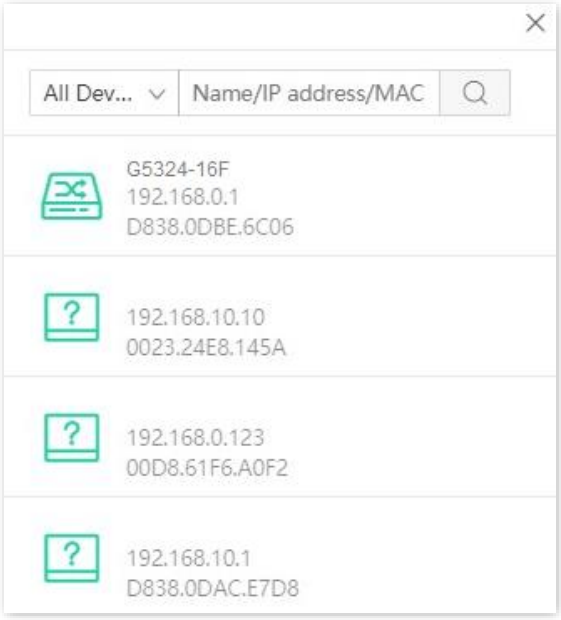
Interface description

Name	Description
Online Offline	Green device icons stand for online devices while grey for offline devices.
Display Port	With this function enabled, the switch's ports that are connected to the devices are displayed on the topology. For example, ge5 refers to port 5.
IP Address Device Name	With this function enabled, the IP addresses and device names of the devices are displayed on the topology.
Local View Main View	It specifies the view mode of the network topology. – **Local View**: It specifies the topology with this switch as the root node. – **Main View**: It specifies the topology with the main device as the root node. Note – When there is only one main device which is not this switch in the topology, you can switch to the main view. – Main device is the core switching device in the network. You can designate it by yourself.
Auto Refresh	With this function enabled, the network topology is refreshed automatically. Auto Refresh cycle: 10 minutes.
Refresh	It is used to refresh the network topology manually.
Download	It is used to save the topology in PNG format locally.
Clear Offline	It is used to clear the offline devices in the topology while removing all configuration of these devices in the Visualization section.
Clear All	It is used to clear all devices and regenerate a topology.
	It is used to view the loop alert messages of the topology. The alert messages automatically refresh every 30 s.
	Vertical expansion/horizontal expansion. – Click to expand the topology vertically. – Click to expand the topology horizontally.

- **Search a device**

To search a device, click .

You can search the device by filtering the device type or directly enter the device name/IP address/MAC address in the search bar. Click the icon of the device, and you can be directed to the location of this device on the network topology.

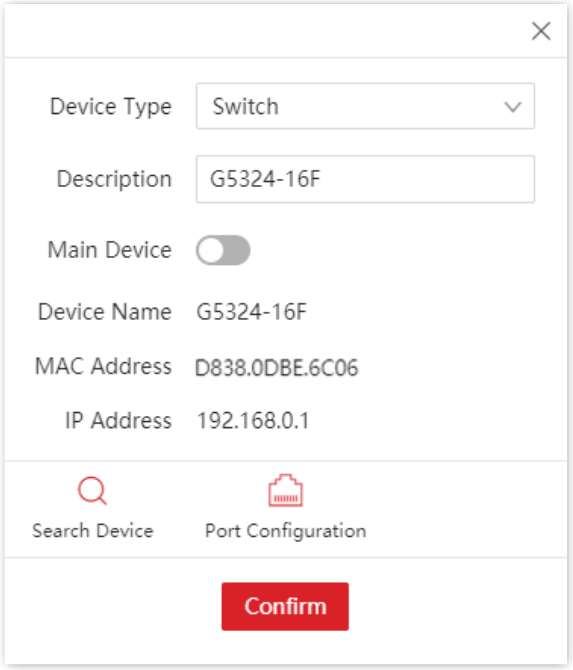


- **Zoom in/out**

  You can zoom in or out the typology by clicking + / − or scrolling the mouse wheel.

- **View & modify parameters**

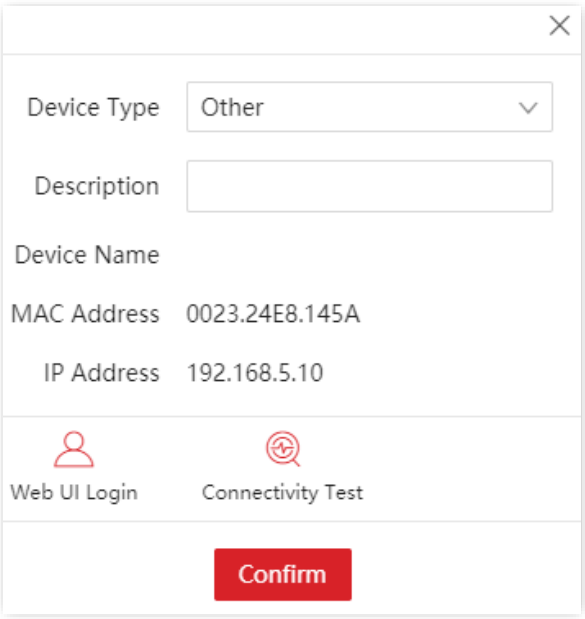
  You can view and modify related parameters of this switch by clicking the icon of this switch.



: It is used to refresh the network topology.

: It is used to enable/disable each port.

You can view and modify related parameters of other devices by clicking the icon of the device.

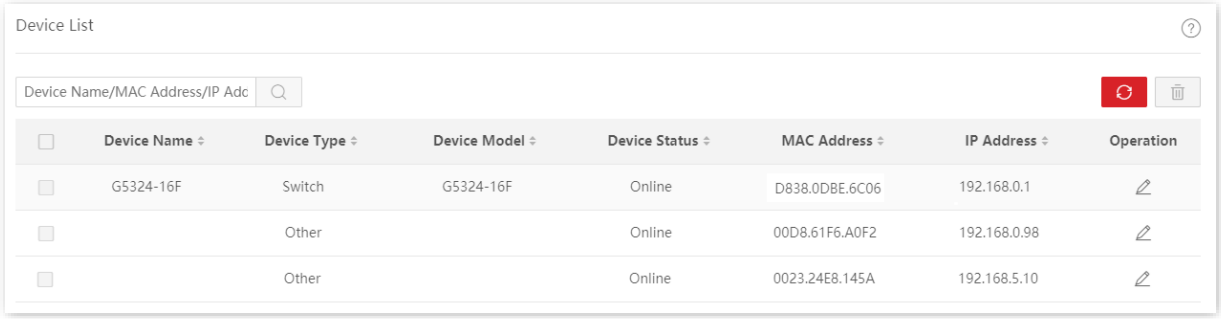


Web UI Login : It is used to enter the web login page of the device.

Connectivity Test : It is used to test the network connectivity between this device and the switch.

9.2 Device list

Click **Visualization** > **Device List** to enter the page. On this page, you can view and modify the basic information of all devices.



Parameter description

Name	Description
Device Name	It specifies the name of the device. If it is blank, it indicates that there is no corresponding field in the protocol message. You can click to modify the device name. Tip The device name modified here is only displayed on the Visualization page, and the corresponding field in the protocol message will not be changed.
Device Type	It specifies the type of the device. You can click to modify the device type. Tip The device type modified here is only displayed on the **Visualization** page, and the corresponding field in the protocol message will not be changed.
Device Model	It specifies the model of the device. If it is blank, it indicates that there is no corresponding field in the protocol message. You can click to modify the device model.
Device Status	It specifies the online/offline status of the device.
MAC Address	It specifies the MAC address of the device.
IP Address	It specifies the IP address of the device.

Appendix

Acronyms and Abbreviations

Acronym or Abbreviation	Full Spelling
ACL	Access Control List
ARP	Address Resolution Protocol
BPDU	Bridge Protocol Data Unit
CIST	Common and Internal Spanning Tree
CLI	Command Line Interface
CoS	Class of Service
CST	Common Spanning Tree
DHCP	Dynamic Host Configuration Protocol
DoS	Denial of Service
DS	Differentiated Services
DSCP	Differentiated Services Code Point
IGMP	Internet Group Management Protocol
IST	Internal Spanning Tree
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
MIB	Management Information Base
MSTI	Multiple Spanning Tree Instance
MSTP	Multi Spanning Tree Protocol
NMS	Network Management System
OID	Object Identifier
OSPF	Open Shortest Path First
QoS	Quality of Service
RADIUS	Remote Authentication Dial-In User Service
RIP	Routing Information Protocol

Acronym or Abbreviation	Full Spelling
RSTP	Rapid Spanning Tree Protocol
SNMP	Simple Network Management Protocol
STP	Spanning Tree Protocol
TCI	Tag Control Information
TCN BPDU	Topology Change Notification BPDU
TLV	Type/Length/Value
ToS	Type of Service
TPID	Tag Protocol Identifier
TTL	Time to Live
VoD	Video-on-Demand
VLAN	Virtual Local Area Network

Configure the switch to access the internet

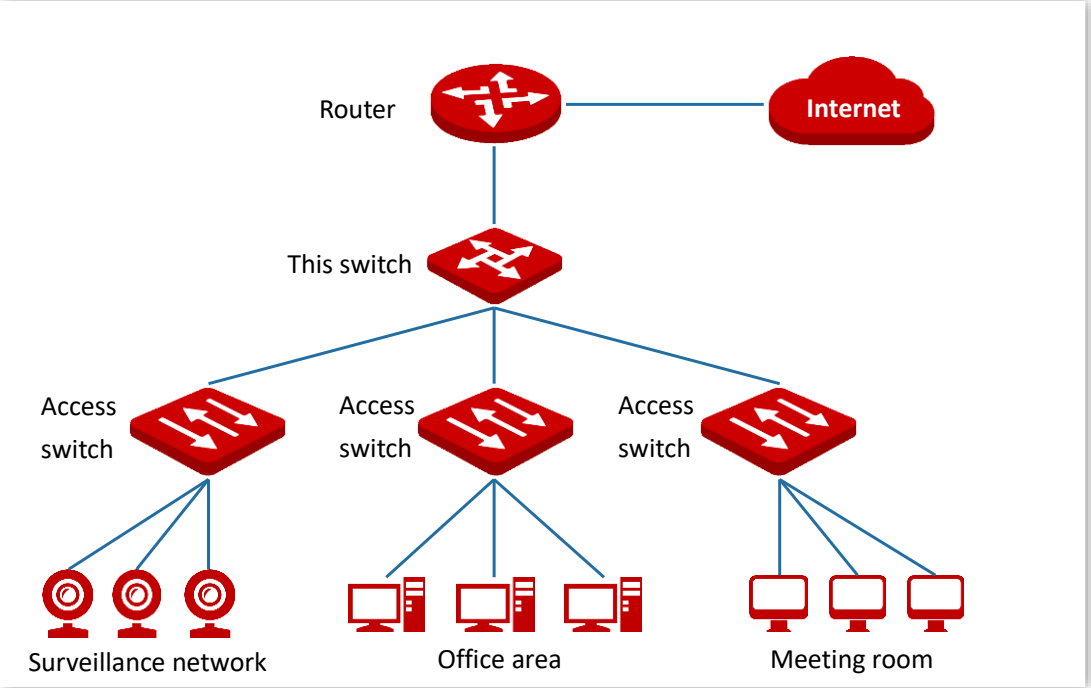
Networking requirement

You want to configure the switch to access the internet

Assume that:

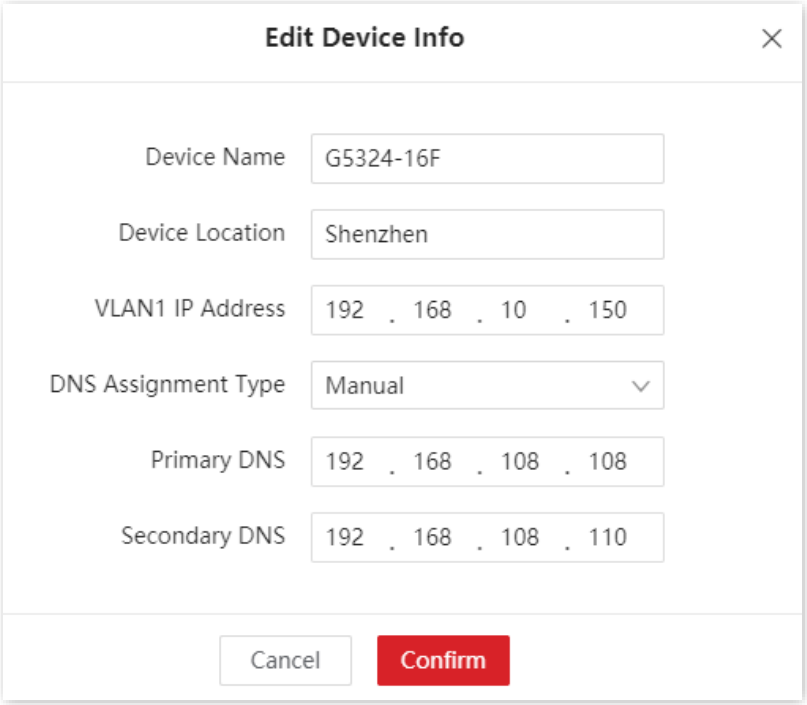
- LAN IP address/subnet mask of the upstream router: 192.168.10.1/255.255.255.0
- Primary & secondary DNS server address: 192.168.108.108, 192.168.108.110

The network topology is as shown below.



Configuration procedure

1. Log in to the web UI of the switch.
2. Configure the IP address and DNS server addresses of the switch.
   (1) Click **Basics** > **System Summary** to enter the page, then click ✎ behind **Device Info**.
   (2) Set **VLAN1 IP Address** to an IP address in the same network segment as that of the LAN IP address of the router, which is **192.168.10.150** in this example.
   (3) Set **DNS Assignment Type** to **Manual**. Then set the **Primary DNS** and **Secondary DNS** to DNS server addresses that can properly resolve the URL of the IMS cloud platform, which are **192.168.108.108, 192.168.108.110** respectively in this example.
   (4) Click **Confirm**.



3. Configure the default route.

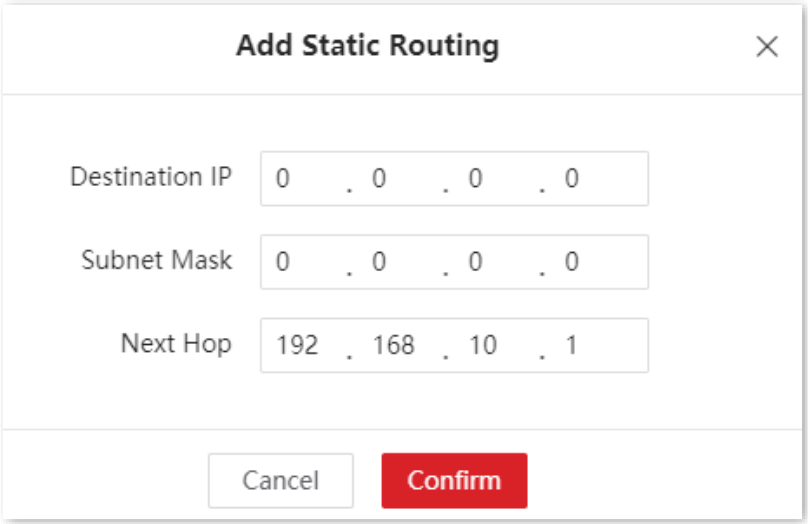
(1) Click **Routing** > **Static Routing** to enter the page, then click **Add**. A configuration window appears.

(2) Set **Destination IP** to **0.0.0.0**.

(3) Set **Subnet Mask** to **0.0.0.0**.

(4) Set **Next Hop** to the LAN IP address of the router, which is **192.168.10.1** in this example.

(5) Click **Confirm**.



----End

Verification

After configuration, you can test whether the switch can access the internet through the Ping test on **Device Settings** > **Diagnostics** page.

You can ping a domain name to test the internet connection status, which is **www.google.com** in this example. The switch accesses the internet successfully if the test results are as shown below.