



User Guide

L3 Managed PoE Switch With 4-Port
10G SFP+
G5328XP-24-410W

Copyright statement

Copyright © 2022 IP-COM Networks Co., Ltd. All rights reserved.

IP-COM is the registered trademark of IP-COM Networks Co., Ltd. Other brand and product names mentioned herein are trademarks or registered trademarks of their respective holders. Copyright of the whole product as integration, including its accessories and software, belongs to IP-COM Networks Co., Ltd. No part of this publication can be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language in any form or by any means without the prior written permission of IP-COM Networks Co., Ltd.

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 switch.

Conventions



This user guide applies to G5328XP-24-410W (L3 Managed PoE Switch With 4-Port 10G SFP+).

The web UI screenshots and related parameters mentioned herein are only for reference. Please refer to the actual product.

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	<i>Italic</i>	Format: <i>XX:XX:XX:XX:XX:XX</i>
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 the device.
 Tip	This format is used to supplement or explain relevant operations.

For 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	Introduces the basic information of the device, including product overview, selling points, and specifications.
Quick installation guide	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.
User guide	Introduces how to set up more functions of the device for more requirements, including all functions on the web UI of the device.

Technical Support

Contact us if you need more help. We will be glad to assist you as soon as possible.

Email: info@ip-com.com.cn

Website: www.ip-com.com.cn

Revision History

IP-COM is constantly searching for ways to improve its products and documentation. The following table indicates any changes that might have been made since the user guide was released.

Version	Description	Date
V1.0	Original publication.	2022-10-24

Contents

1 Login and logout.....	1
1.1 Login	1
1.2 Logout.....	4
2 Web UI introduction	5
2.1 Web layout	5
2.2 Common buttons.....	6
3 Basics	7
3.1 System summary	7
3.2 Port.....	10
3.2.1 Basic.....	10
3.2.2 Port mirroring	11
3.2.3 Port aggregation	12
3.2.4 Port rate limit.....	14
3.2.5 Packet statistics.....	15
3.3 VLAN.....	17
3.3.1 Overview.....	17
3.3.2 VLAN configuration	18
3.3.3 Example of 802.1Q VLAN configuration	20
3.4 Maintenance.....	23
3.4.1 Firmware upgrade.....	23
3.4.2 Configuration import	23
3.4.3 Backup	24
3.4.4 Reboot	25
3.4.5 Factory settings.....	26
3.5 Diagnostics	27
3.5.1 Ping test	27
3.5.2 Tracert test.....	28
3.6 Cloud management	29

4 Switching	30
4.1 DHCP relay	30
4.2 DHCP snooping	33
4.2.1 Overview.....	33
4.2.2 Configure DHCP snooping.....	34
4.3 Spanning tree	36
4.3.1 Overview.....	36
4.3.2 Global	43
4.3.3 Port configuration	47
4.3.4 Port statistics	48
4.3.5 Instance info	49
4.4 LLDP configuration.....	51
4.4.1 Overview.....	51
4.4.2 Global	53
4.4.3 Port configuration	54
4.4.4 Neighbor info	55
4.5 LLDP-MED	56
4.5.1 Overview.....	56
4.5.2 Basic.....	58
4.5.3 TLV settings.....	59
4.5.4 Local information.....	60
4.5.5 Neighbor info	61
4.6 IGMP snooping	62
4.6.1 Overview.....	62
4.6.2 Global	64
4.6.3 Fast leave	66
4.7 MAC settings.....	67
4.7.1 MAC address table.....	67
4.7.2 Static MAC address	68
5 Routing	69

5.1 Static routing	69
5.1.1 Overview.....	69
5.1.2 Configure static routing	69
5.1.3 Example of static routing configuration	70
5.2 ARP	74
5.3 DHCP server.....	76
5.3.1 Overview.....	76
5.3.2 DHCP settings	76
5.3.3 DHCP reservation.....	78
5.3.4 Client list.....	78
6 QoS policy	80
6.1 Overview	80
6.2 Configuration guidance.....	86
6.3 QoS scheduler.....	87
6.4 802.1P.....	88
6.5 DSCP	89
6.6 Port priority	90
7 Network security.....	91
7.1 ACL.....	91
7.1.1 Overview.....	91
7.1.2 Configuration guidance.....	91
7.1.3 MAC ACL	92
7.1.4 IP ACL.....	93
7.1.5 Apply ACL.....	94
7.1.6 Example of ACL configuration	95
7.2 MAC filtering.....	98
7.3 802.1X.....	99
7.3.1 Overview.....	99
7.3.2 Global	100
7.3.3 Port configuration	101

7.4 Attack defense	103
7.4.1 Overview.....	103
7.4.2 ARP attack defense	103
7.4.3 DoS attack defense	104
7.4.4 MAC address attack defense.....	105
8 Device settings	106
8.1 User management	106
8.2 SNMP.....	107
8.2.1 Overview.....	107
8.2.2 Configuration guidance.....	109
8.2.3 Basic.....	110
8.2.4 Permission control	111
8.2.5 Notification	112
8.3 System time	114
8.4 Log management.....	115
8.4.1 Log info	115
8.4.2 Server settings	116
8.5 Time period	117
8.6 RMON	118
8.6.1 Overview.....	118
8.6.2 Statistics.....	119
8.6.3 History	120
8.6.4 Alarm	121
8.6.5 Event.....	122
8.6.6 Log	123
9 Visualization.....	124
9.1 Global map	124
9.2 Device list	128
10 PoE management	129
10.1 Overview	129

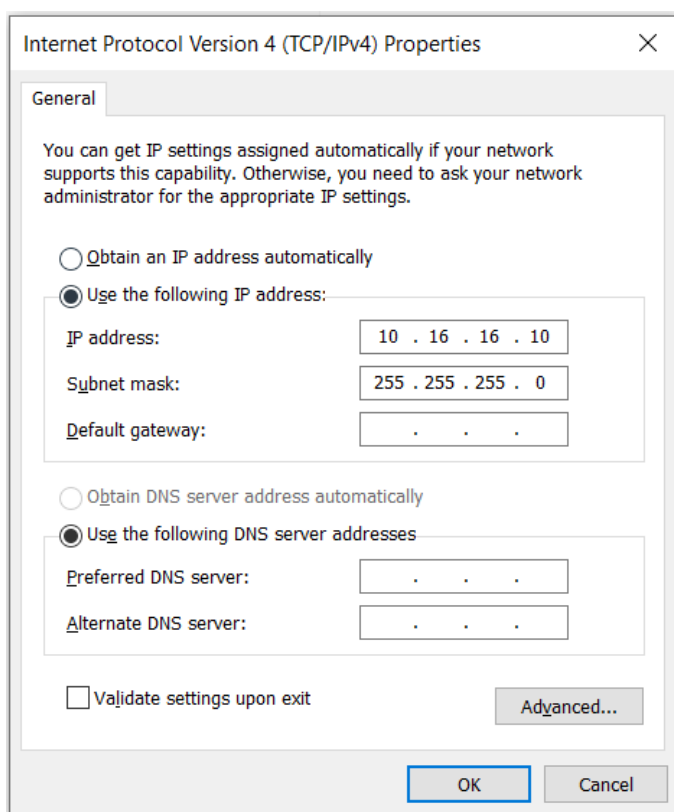
10.2 Global	130
10.3 Port configuration.....	131
Appendix.....	133

1 Login and logout

1.1 Login

1. Connect the computer to one of the RJ45 ports 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 **10.16.16.168**, you can set the IP address of the computer to **10.16.16.X** (X ranges from 2 to 254 excluding 168 and is not occupied), and subnet mask to **255.255.255.0**.



3. Start a browser and enter the IP address of the switch (default: **10.16.16.168**) in the address bar to access the login page.



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

The image shows the IP-COM login interface. At the top, the "IP-COM" logo is displayed in red. Below the logo are two input fields: "User Name" with a person icon and "Password" with a lock icon. Under the "Password" field, there is a "Forget password" link and a language dropdown menu currently set to "English". At the bottom of the form is a prominent red "Login" button.

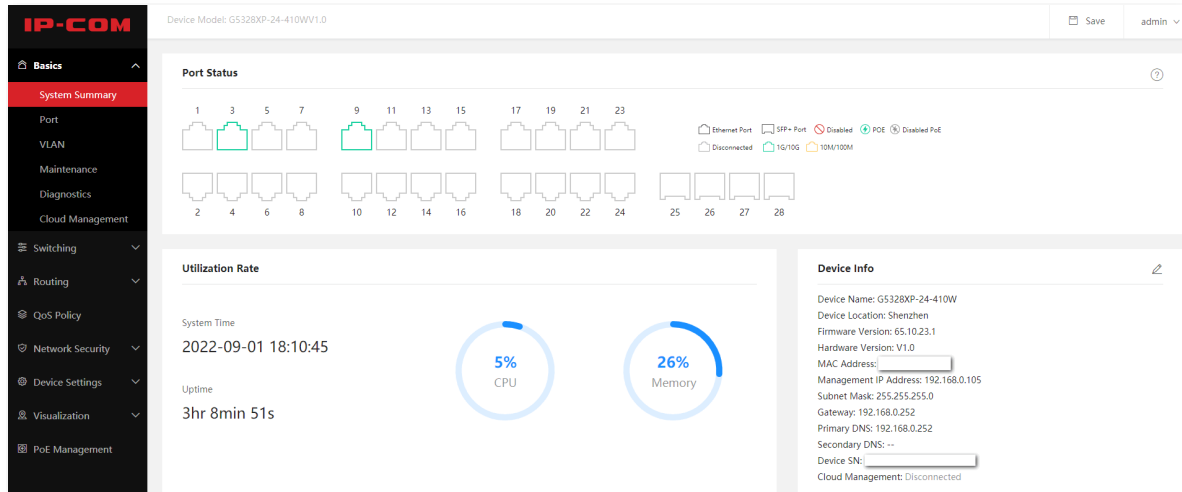
----End



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

- Check whether the computer is connected to the switch properly.
 - Check whether the IP address of Ethernet (or Local Area Connection) of the computer is set to **10.16.16.X** (X ranges from 2 to 254 excluding 168 and is not occupied).
 - Clear the cache of the web browser or try another web browser.
 - Check whether another device with the IP address 10.16.16.168 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 and hold the **LED Mode** button for about 10 seconds, and then release when all LED indicators are solid on. When the **SYS** LED indicator blinks again, the switch is restored to factory settings.
-

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.













The screenshot shows the IP-COM web UI for a device model GS328XP-24-410WV1.0. The interface is divided into four numbered regions:

- 1**: Level-1 navigation bar (Basics)
- 2**: Level-2 navigation bar (Port)
- 3**: Tab page area (Basic, Port Mirroring, Port Aggregation, Port Rate Limit, Packet Statistics)
- 4**: Configuration area (Table of ports)

Port	Port Status	Speed/Duplex	Port Isolation	Ingress Limit	Egress Limit	Ingress Flow	Egress Flow	Jumbo Frame	Operation
1	Disconnected	Auto-negotiation 1000M/FDX	Disable	Disable	Disable	0MB	0MB	1522	
2	Disconnected	Auto-negotiation 1000M/FDX	Disable	Disable	Disable	0MB	0MB	1522	
3	Connected	Auto-negotiation 1000M/FDX	Disable	Disable	Disable	41.3MB	187.3MB	1522	
4	Disconnected	Auto-negotiation 1000M/FDX	Disable	Disable	Disable	0MB	0MB	1522	
5	Disconnected	Auto-negotiation 1000M/FDX	Disable	Disable	Disable	0MB	0MB	1522	
6	Disconnected	Auto-negotiation 1000M/FDX	Disable	Disable	Disable	0MB	0MB	1522	
7	Connected	Auto-negotiation 1000M/FDX	Disable	Disable	Disable	184.1MB	47.7MB	1522	
8	Disconnected	Auto-negotiation 1000M/FDX	Disable	Disable	Disable	0MB	0MB	1522	

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

2.2 Common buttons

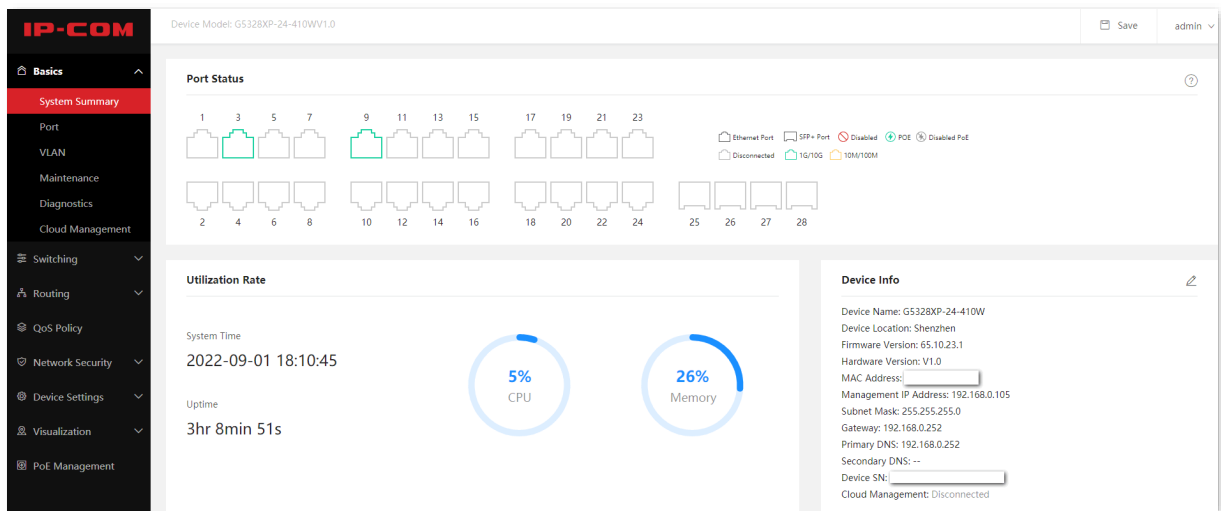
Common buttons	Description
	Used for refreshing displayed contents on the current page.
	Used for configuring the settings on the current page in batches.
	Used for saving the configurations on the current page and enabling the configurations to take effect.
 Note	If you only click  to save the configurations, 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 deleting the rules on the current page.
	Used for editing the rules on the current page.
	Used for saving all current configurations of the switch. If you click  to save the configurations, they still remain after the switch reboots.

3 Basics

3.1 System summary





Navigate to **Basics > System Summary** to enter the page.


On this page, you can view the connection status of each port, utilization rate, system time, uptime, and device information.



Parameter description

Name	Description
Port Status	<p>Displays the connection status of each port of the switch.</p> <ul style="list-style-type: none"> indicates that the port is connected to a device. For RJ-45 ports (1 – 24), the rate is 1 Gbps; and for SFP+ ports (25 -28), the rate is 1 or 10 Gbps. indicates that the port is connected to a device and the rate is 10 or 100 Mbps. indicates that the port is not connected to a device. indicates that the port is disabled. indicates that the port is supplying power to a PoE-powered device. indicates that the port's PoE function is disabled.
Utilization Rate	Displays the CPU and memory utilization of the switch.

Name	Description
System Time	Displays the system time of the switch.
Uptime	Displays the time during which this switch is operating since the last reboot.
Device Name	Displays the name of the switch. You can click  to modify it.
Device Location	Displays the location of the switch. You can click  to modify it.
Firmware Version	Displays the firmware version of the switch.
Hardware Version	Displays the hardware version of the switch.
MAC Address	Displays the MAC address of the switch.
IP Obtaining Type	Specifies the IP obtaining type of the switch. You can click  to set it to Auto or Manual .
Device Info	<p>Displays the IP address of the management VLAN of the switch.</p> <p>It can be modified only when the IP Obtaining Type is set to Manual.</p> <p>Computers belonging to the management VLAN can log in to the web UI of the switch using this IP address.</p>
	<p>Displays the subnet mask of the management VLAN of the switch.</p> <p>It can be modified only when the IP Obtaining Type is set to Manual.</p>
	<p>Displays the gateway address of the management VLAN of the switch.</p>
	<p>Specifies the DNS assignment type for primary DNS and secondary DNS.</p> <p>You can click  to set it to Auto or Manual.</p>
Primary DNS	Displays the primary/secondary DNS server address of the switch.
Secondary DNS	<p>By default, the parameters are automatically obtained from the uplink network.</p> <p>They can be modified only when the DNS Assignment Type is set to Manual.</p>
Device SN	Displays the serial number of the switch.

Name	Description
Cloud Management	<p data-bbox="555 248 1342 309">Displays whether the switch is connected to the IP-COM ProFi Cloud platform.</p> <ul data-bbox="555 338 1433 450" style="list-style-type: none"><li data-bbox="555 338 1433 371">– Connected: The switch is connected to the IP-COM ProFi Cloud platform.<li data-bbox="555 383 1433 450">– Disconnected: The cloud management function is disabled, or the switch fails to connect to the IP-COM ProFi Cloud platform. <p data-bbox="555 495 651 539"> Tip</p> <p data-bbox="555 577 1401 741">To connect to the IP-COM ProFi Cloud platform, the switch must be connected to the internet and can resolve the domain name properly. So, ensure that the primary DNS server address you enter is correct, and the secondary DNS server address is optional (recommended: primary DNS server: 114.114.114.114; secondary DNS server: 8.8.8.8).</p>

3.2 Port

3.2.1 Basic

Navigate to **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	Disconnected	Auto-negotiation 1000M/FDX	Disable	Disable	Disable	0MB	0MB	1522	✎
2	Disconnected	Auto-negotiation 1000M/FDX	Disable	Disable	Disable	0MB	0MB	1522	✎
3	Connected	Auto-negotiation 1000M/FDX	Disable	Disable	Disable	225.1MB	1101.1MB	1522	✎
4	Disconnected	Auto-negotiation 1000M/FDX	Disable	Disable	Disable	0MB	0MB	1522	✎
5	Disconnected	Auto-negotiation 1000M/FDX	Disable	Disable	Disable	0MB	0MB	1522	✎
6	Disconnected	Auto-negotiation 1000M/FDX	Disable	Disable	Disable	0MB	0MB	1522	✎
7	Disconnected	Auto-negotiation 1000M/FDX	Disable	Disable	Disable	105.2MB	16.2MB	1522	✎
8	Disconnected	Auto-negotiation 1000M/FDX	Disable	Disable	Disable	0MB	0MB	1522	✎
9	Connected	Auto-negotiation 1000M/FDX	Disable	Disable	Disable	971.5MB	218.5MB	1522	✎
10	Disconnected	Auto-negotiation 1000M/FDX	Disable	Disable	Disable	0MB	0MB	1522	✎

Parameter description

Name	Description
Port	Specifies the ID of the port.
Port Status	Specifies the current connection status of the port, including Connected , Disconnected , and Disabled .
Speed/Duplex (Rate/Mode)	<p>Specifies the negotiation speed and duplex mode of the port.</p> <ul style="list-style-type: none"> – 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.
Port Isolation	<p>Specifies the isolation group to which the port belongs.</p> <p>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 Disable state, indicating that they can communicate with all ports.</p>

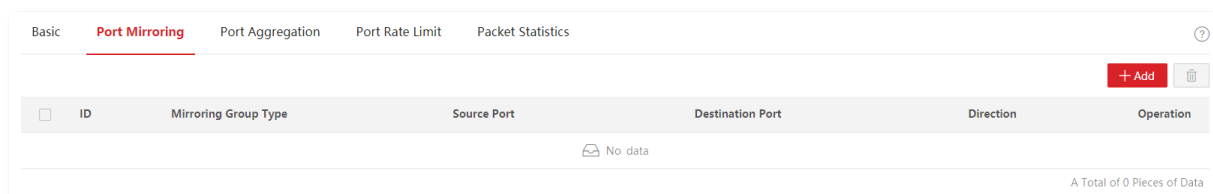
Name	Description
Ingress Limit	With the function enabled, the ingress flow of the port will be monitored. When congestion occurs on the ingress port, the switch sends a PAUSE frame to notify the peer device to stop or slow down data transmission for a specific period of time, so as to avoid incurred 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 speed of the corresponding port for a specific period of time to avoid incurred message loss.
Ingress Flow	Specifies the statistics of data traffic received by the port.
Egress Flow	Specifies the statistics of data traffic transmitted by the port.
Jumbo Frame	Specifies the 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 network packets from a port or multiple ports (source ports) to a specified port (destination port) of the switch. The destination port is commonly connected to a data monitoring device, enabling you to monitor data traffic, analyze performance, and diagnose fault.

Navigate to **Basics > Port > Port Mirroring** to enter the page.

On this page, you can configure the mirroring rules.



Parameter description

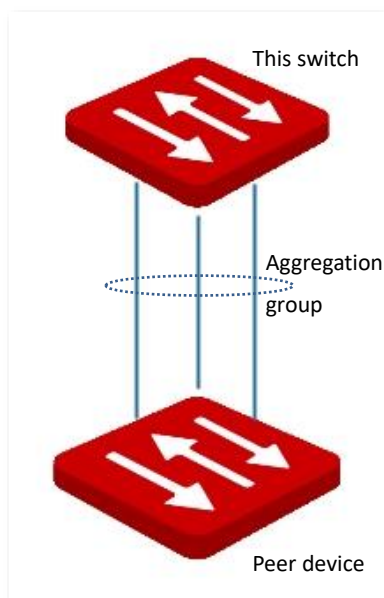
Name	Description
ID	Specifies the ID of the mirroring group.
Mirroring Group Type	This switch only supports the local mirroring group type.
Source Port	Specifies the ports whose packets will be copied. Multiple ports can be selected.
Destination Port	Packets of source ports will be copied to this port.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

Name	Description
Direction	<p>Specifies the packet type.</p> <ul style="list-style-type: none"> - 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 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 shown below.

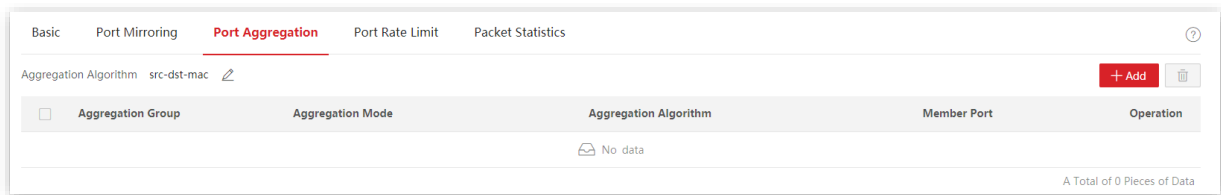


Note


- 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.
- Ports already configured for port mirroring cannot be added to the aggregation group.

Navigate to **Basics > Port > Port Aggregation** to enter the page.

On this page, you can configure the port aggregation rules.



Parameter description

Name	Description
Aggregation Group	<p>Specifies the ID of aggregation groups.</p> <ul style="list-style-type: none"> When the mode is set to Static Aggregation, the ID ranges from 1 to 32. When the mode is set to Dynamic Aggregation, the ID ranges from 33 to 64.
Aggregation Mode	<p>There are two aggregation modes: Static Aggregation and Dynamic Aggregation.</p> <ul style="list-style-type: none"> 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 enabled, and the actual aggregated ports must be determined together with the peer device through LACP protocol. <p> Note</p> <p>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.</p>
Aggregation Algorithm	<p>Specifies the routing algorithms for the aggregation group:</p> <ul style="list-style-type: none"> 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 destination port number in the received packet.
Member Port	<p>Specifies the members of an aggregation group.</p> <ul style="list-style-type: none"> 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

Navigate to **Basics > Port > Port Rate Limit** to enter the page.

On this page, you can configure the egress rate of the port and set the suppression value of each port for receiving broadcast, multicast and unknown unicast packets.

Port	Egress Rate (Mbps)	Broadcast Packet	Multicast Packet	Unknown Unicast	Suppression Value	Operation
1	--	Disable	Disable	Disable	100	✎
2	--	Disable	Disable	Disable	100	✎
4	--	Disable	Disable	Disable	100	✎
5	--	Disable	Disable	Disable	100	✎
6	--	Disable	Disable	Disable	100	✎
7	--	Disable	Disable	Disable	100	✎
8	--	Disable	Disable	Disable	100	✎
9	--	Disable	Disable	Disable	100	✎
10	--	Disable	Disable	Disable	100	✎

Parameter description

Name	Description
Port	Specifies the ID of the port.
Egress Rate (Mbps)	Specifies the maximum egress rate of the port. "--" stands for no rate limit.
Broadcast Packet	Displays whether the broadcast packet suppression function is enabled or disabled.
Multicast Packet	Displays whether the multicast packet suppression function is enabled or disabled.
Unknown Unicast	Displays whether the unknown unicast packet suppression function is enabled or disabled.
Suppression Value	Specifies the maximum rate at which broadcast, multicast and unknown unicast packets are allowed to pass by when the suppression function is enabled. When the broadcast/multicast/unknown unicast packets exceed the limit value set by the user, the system discards the excess packets, to lower the proportion of broadcast/multicast/unknown unicast packets for the normal operation of network service.

3.2.5 Packet statistics


Navigate to **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.

Port	Transmitted Packets	Transmitted Byte	Received Packets	Received Byte	Operation
1	0	0	0	0	🗑️
2	0	0	0	0	🗑️
3	1606550	1168690972	1049721	239964954	🗑️
4	0	0	0	0	🗑️
5	0	0	0	0	🗑️
6	0	0	0	0	🗑️

Parameter description

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

View Packet Statistics		×
Port	1	
Received Statistics		
Total Bytes	0	
Broadcast Packets	0	
Unicast Packets	0	
Error Packets	0	
Discard Packets	0	
Transmission Statistics		
Total Bytes	0	
Broadcast Packets	0	
Unicast Packets	0	
Error Packets	0	
Discard Packets	0	

Parameter description

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

3.3 VLAN

3.3.1 Overview

Virtual Local Area Network (VLAN) 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.

This 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 to only one 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			Messages are forwarded after the tags are removed.
Trunk 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.	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. This rule cannot be deleted.

Navigate to **Basics > VLAN > 802.1Q VLAN** to enter the page.

On this page, you can configure the rules of 802.1Q VLAN.

VLAN ID	VLAN Description	IPv4 Address	Subnet Mask	Operation
1	default	192.168.0.105	255.255.255.0	

Parameter description

Name	Description
VLAN ID	Specifies the VLAN ID, used for identifying the VLAN to which the packet belongs. The VLAN ID of management VLAN is 1 .
VLAN Description	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	<p>After the L3 virtual interface is enabled, you can configure the IP address and subnet mask for the VLAN interface.</p> <p>After the IP address information is configured, the communication between VLANs can be realized through static routes.</p>
IP Obtaining Type	<p>Specifies the type that the VLAN interface employs to obtain an IP address.</p> <ul style="list-style-type: none"> Manual: Manually configure the IP address and subnet mask for the VLAN interface. DHCP: Automatically obtain the IP address info from the DHCP server. <p> Note</p> <p>When the IP Obtaining Type is set to DHCP, ensure that there is a DHCP server belonging to the VLAN.</p>
IPv4 Address/Mask	Specifies the IP address and subnet mask of the VLAN interface. Devices connected to ports in the VLAN group can use this IP address to log in to the Web UI of the switch.
Subnet Mask	Specifies the subnet mask of the VLAN interface.

Configure port members

Navigate to **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.

Port	Link Type	PVID	Tagged	Untagged	Operation
1	Access	1	--	1	
2	Access	1	--	1	
3	Access	1	--	1	
4	Access	1	--	1	
5	Access	1	--	1	
6	Access	1	--	1	
7	Access	1	--	1	
8	Access	1	--	1	

Parameter description

Name	Description
Port	Specifies the ID of the port.
Link Type	<p>Three VLAN link types are supported: Access, Trunk, and Hybrid.</p> <ul style="list-style-type: none"> – Access: An access port belongs to only one 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	<p>Specifies the default VLAN ID of a port.</p> <p>When receiving untagged packets, the port forwards them to the corresponding VLAN based on the PVID of the port itself.</p>
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 transmits 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 transmits them.

3.3.3 Example of 802.1Q VLAN configuration

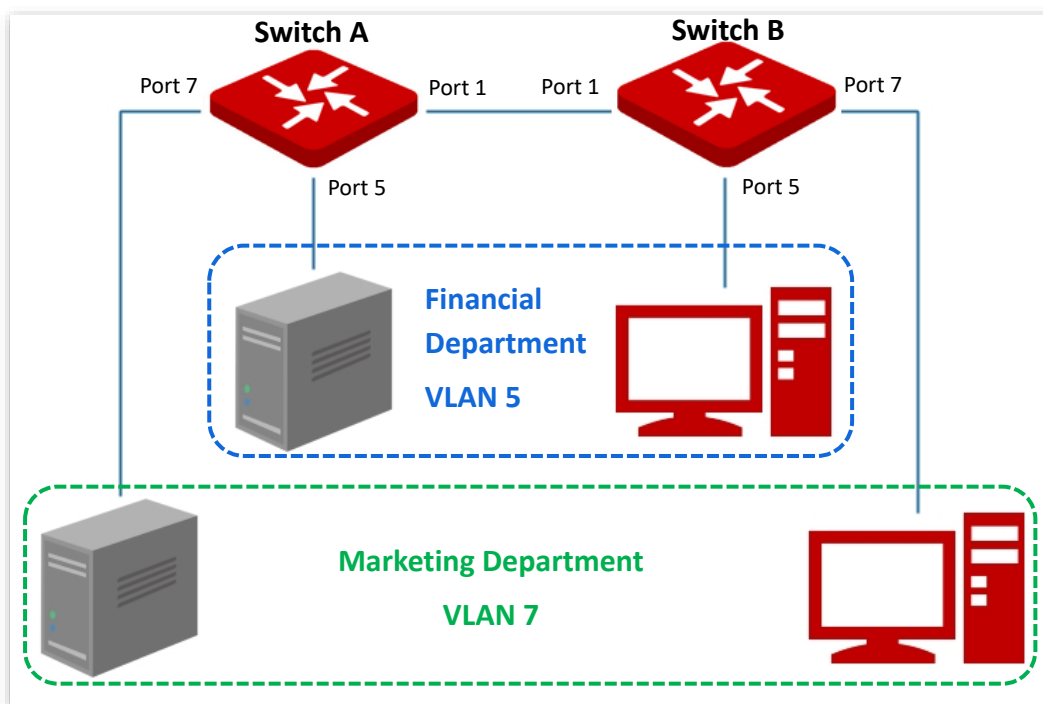
Network requirement

The staff of 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 navigate to **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**.

<input type="checkbox"/>	VLAN ID	VLAN Description	IPv4 Address	Subnet Mask	Operation
<input type="checkbox"/>	1	default	192.168.0.105	255.255.255.0	
<input type="checkbox"/>	5	Finance	--	--	
<input type="checkbox"/>	7	Marketing	--	--	

A Total of 3 Pieces of Data

2. Configure port property.

- (1) Navigate to **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**.

Port	Link Type	PVID	Tagged	Untagged	Operation
1	Trunk	1	5,7	1	
2	Access	1	--	1	
3	Access	1	--	1	
4	Access	1	--	1	
5	Access	5	--	5	
6	Access	1	--	1	
7	Access	7	--	7	
8	Access	1	--	1	

3. Save the configurations

Click **Save** at the upper right corner to save the configurations.

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

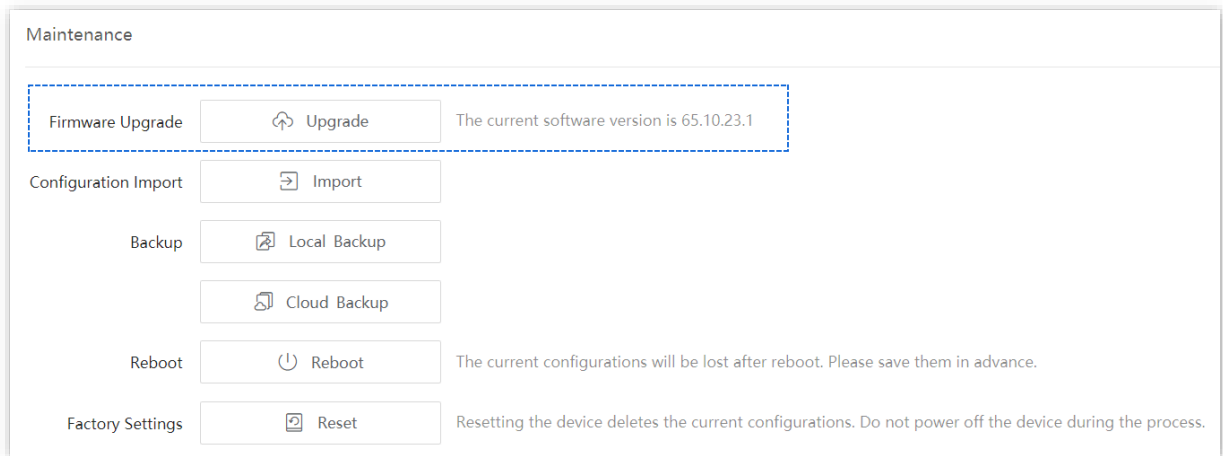
Navigate to **Basics > Maintenance** to enter the page.

On this page, you can click **Upgrade** to update the switch's firmware, enjoying better user experience.



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.



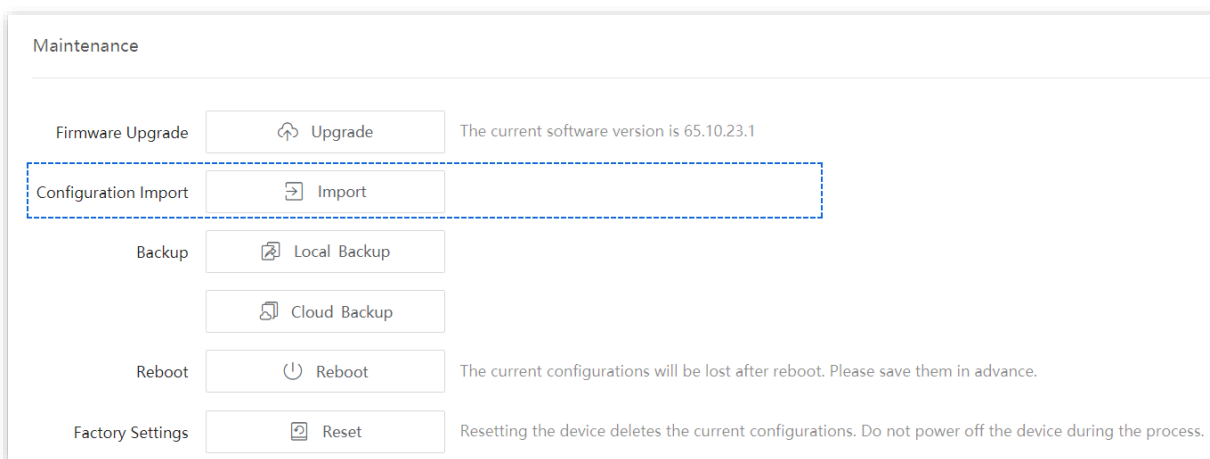
3.4.2 Configuration import

Navigate to **Basics > Maintenance** to enter the page.

On this page, you can click **Import** to import the backup configuration file to the switch.



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



3.4.3 Backup

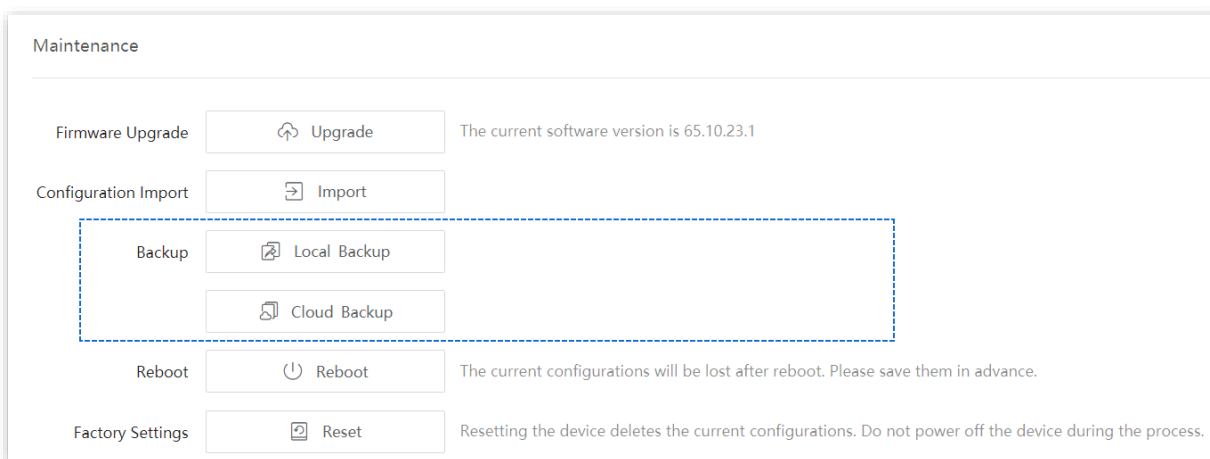
If you have made a lot of configurations to the switch for better performance in a specific operating environment, it is recommended to back up the switch’s configurations. After you upgrade the switch or restore the switch to factory settings, you can import this backup configuration file to restore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

Navigate to **Basics > Maintenance** to enter the page.

On this page, you can back up the switch’s configuration information to the local computer or the IP-COM **ProFi Cloud** platform.

 **Note**

- Click **Save** on the upper right corner of the page to save all settings before backup.
- The configurations can be backed up to the IP-COM **ProFi Cloud** platform [only when the switch is managed by the IP-COM ProFi Cloud platform.](#)

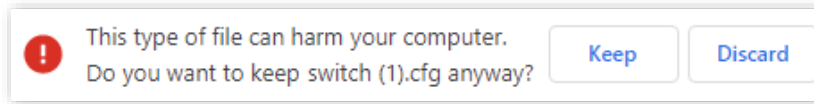


Local Backup

Click **Local Backup**, then a file named **switch.cfg** is downloaded to a local computer.



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



Cloud Backup

Click **Cloud Backup**, you can back up the switch's configurations to the IP-COM **ProFi Cloud** platform.

3.4.4 Reboot

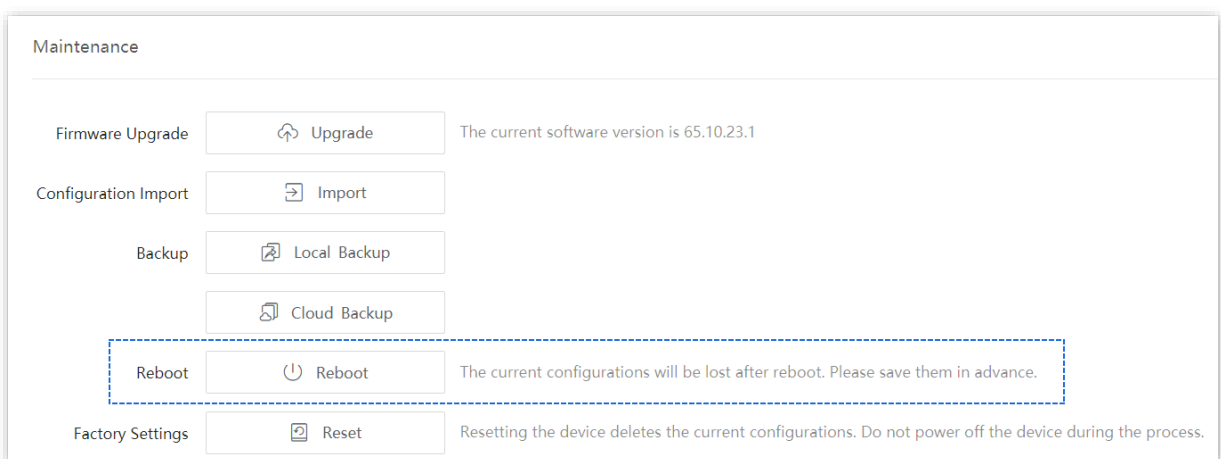
When a parameter you set does not work properly, you can try to reboot the switch to fix this issue.

Navigate to **Basics > Maintenance** to enter the page.

On this page, you can click **Reboot** to restart the switch.



To avoid loss of configurations, click **Save** on the upper right corner to save all settings before rebooting the switch.



3.4.5 Factory settings

If you cannot locate a problem affecting the switch's normal operation, or you forget your username or password when logging 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

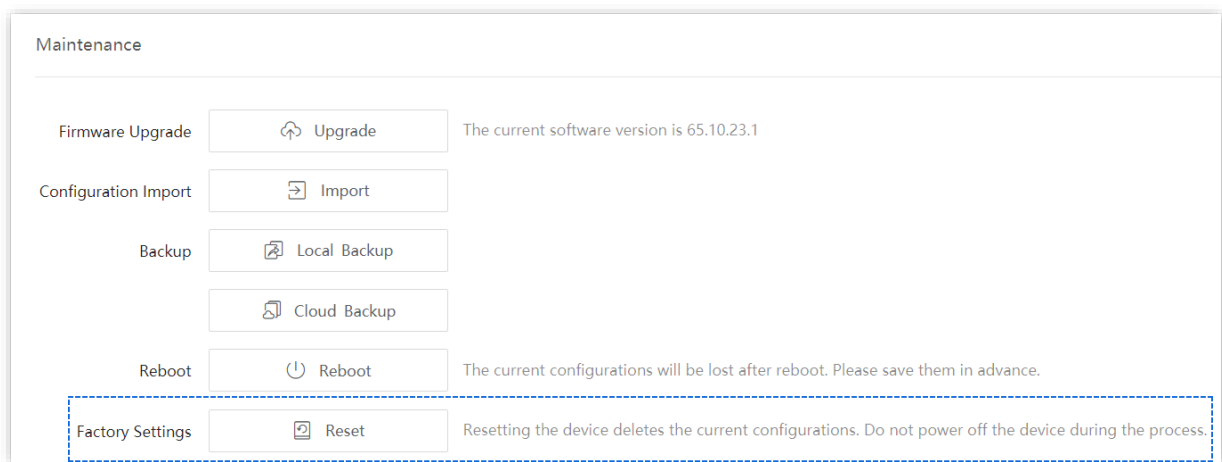
Navigate to **Basics > Maintenance** to enter the page.

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 **LED Mode** button 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.

3.5 Diagnostics

Navigate to **Basics > 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.

3.5.1 Ping test

Navigate to **Basics > Diagnostics > Ping Test** to enter the page.

On this page, you can test the network connection and connection quality.

Ping Test
Tracert

Target IP Address

(Please enter an IP address/domain name)

Transmit Times

(Range: 1 to 100)

Packet Size

B (Range: 18 to 512)

Parameter description

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

3.5.2 Tracert test

Navigate to **Basics > Diagnostics > Tracert** to enter the page.

On this page, you can test the routes of the packets passing from the switch to the destination device.

Ping Test **Tracert**

Target IP Address (Please enter an IP address/domain name)

Maximum Hops (Range: 1 to 30)

Parameter description

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

3.6 Cloud management

IP-COM **ProFi Cloud** platform is developed by IP-COM, providing central management for IP-COM devices that support cloud management.

Navigate to **Basics > Cloud Management** to enter the page.

On this page, you can enable or disable the cloud management function of the switch.

With the switch managed by the IP-COM **ProFi Cloud** platform (**ProFi Cloud** web UI or **ProFi App**), you can configure and check the parameters of the switch on the IP-COM **ProFi Cloud** platform.



- For how to add the switch to the IP-COM **ProFi Cloud** platform, refer to the user guides of **ProFi Cloud** web UI and **ProFi App** at www.ip-com.com.cn.
- With the switch managed by the IP-COM **ProFi Cloud** platform, you can modify the parameters of the switch on both the IP-COM **ProFi Cloud** platform or local web UI of the switch. The parameters of the switch take effect upon the last modification.

Cloud Management

You can manage the device on the web UI of IP-COM cloud platform (<https://imsen.ip-com.com.cn>) or through IP-COM ProFi App.

Confirm

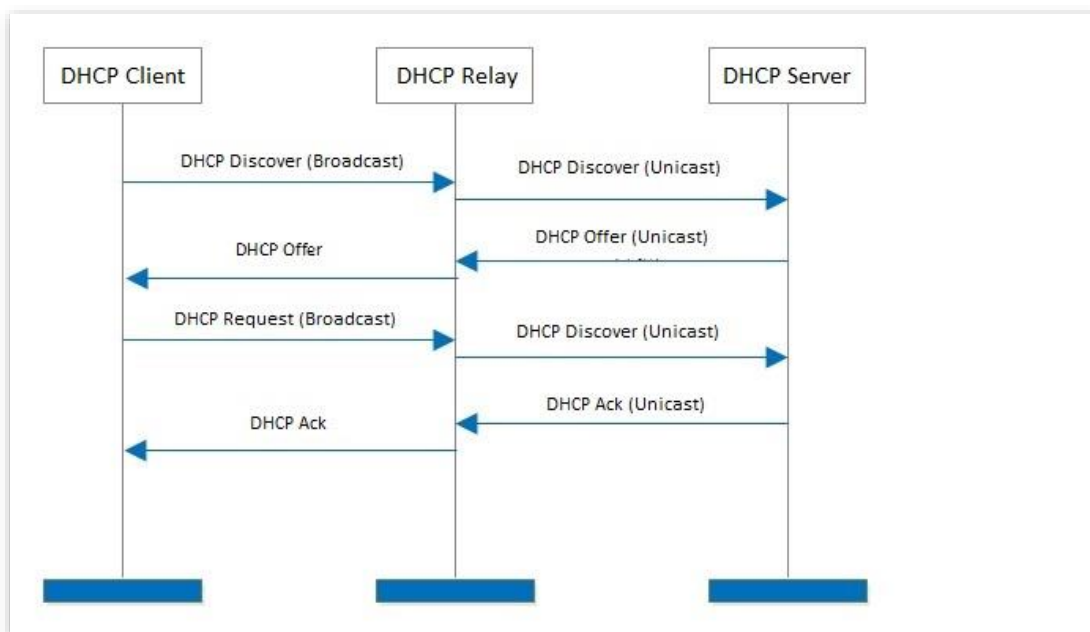
4 Switching

4.1 DHCP relay

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 network segments, enabling DHCP clients in multiple networks to share a same DHCP server.


The working principles of DHCP Relay are shown below.



- When DHCP relay receives the DHCP discover or DHCP request messages sent by DHCP client 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.

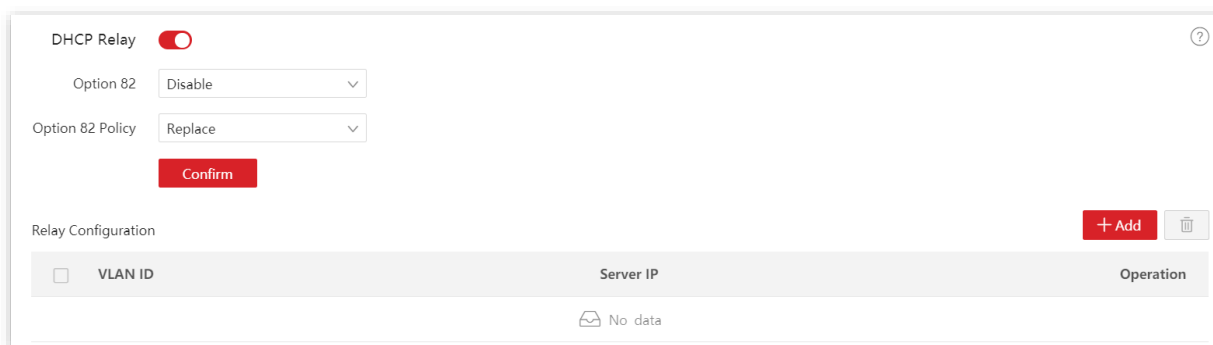
Option 82, also called the DHCP Relay Agent Information Option, is an option in DHCP message that records the location information of the DHCP clients. You can use this option to locate the DHCP client, thus implementing security and charging control for clients. The corresponding IP address and parameter 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.  Tip 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. <ul style="list-style-type: none"> - 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.

Navigate to **Switching > DHCP Relay** to enter the page.

On this page, you can configure the DHCP relay rules.



Parameter description

Name	Description
DHCP Relay	Used to enable or disable the DHCP relay function. By default, it is disabled.
Option 82	<p>Used to enable or disable the Option 82 policy.</p> <p>Option 82 records the location info of DHCP clients. The Option 82 policy takes effect only when the Option 82 is enabled.</p>
Option 82 Policy	<p>The switch supports three policies:</p> <ul style="list-style-type: none"> – 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	<p>Specifies the VLAN to which the clients belong.</p> <p>The VLAN must already exist, and its L3 virtual interface is configured.</p>
Server IP	<p>Specifies the IP address of the remote DHCP server.</p> <p>The IP address of the remote DHCP server cannot belong to the same network segment as that of the VLAN to which clients belong.</p>

4.2 DHCP snooping

4.2.1 Overview

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

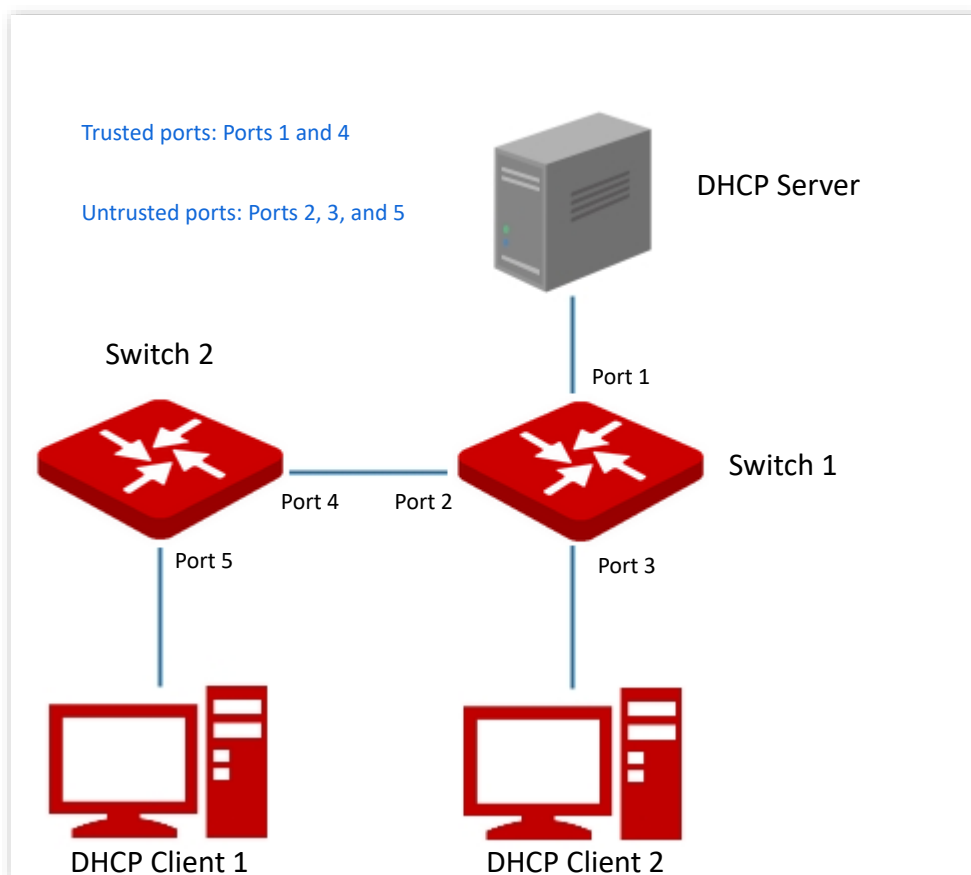
- It ensures that DHCP clients can obtain IP addresses from the correct servers.

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.






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.

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	<p>Add the default content of this switch to the Option 82 information of the DHCP request message, and forward the message.</p> <p> Tip</p> <p>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.</p>
DHCP request message with Option 82	<p>DHCP request messages are processed according to the following configuration policies.</p> <ul style="list-style-type: none"> - 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.

4.2.2 Configure DHCP snooping

Navigate to **Switching > DHCP Snooping** to enter the page.

On this page, you can configure the DHCP Snooping rules.

DHCP Snooping <input checked="" type="checkbox"/>				
Port Configuration Edit				
Port	Port Property	Option 82	Option Policy	Operation
1	Untrusted Port	Disable	Replace	
2	Untrusted Port	Disable	Replace	
3	Untrusted Port	Disable	Replace	
4	Untrusted Port	Disable	Replace	
5	Untrusted Port	Disable	Replace	
6	Untrusted Port	Disable	Replace	

Parameter description

Name	Description
DHCP Snooping	Used to enable or disable the DHCP snooping function.
Port	Specifies the ID of the port.
Port Property	<p>Used to configure the DHCP snooping property of the current port, including trusted port or untrusted port.</p> <ul style="list-style-type: none"> – 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	<p>Specifies the status of Option 82. You can enable or disable the Option 82 function by clicking .</p> <p>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.</p>
Option Policy	<p>Three Option 82 policies are supported by this switch:</p> <ul style="list-style-type: none"> – 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: Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP) and Multi Spanning Tree Protocol (MSTP).

STP

STP is a network protocol based on IEEE 802.1d. It is a protocol that ensures a loop-free topology in local area network and provides 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.
- Topology Change Notification BPDU (TCN BPDU): It is used to notify the changes of 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.

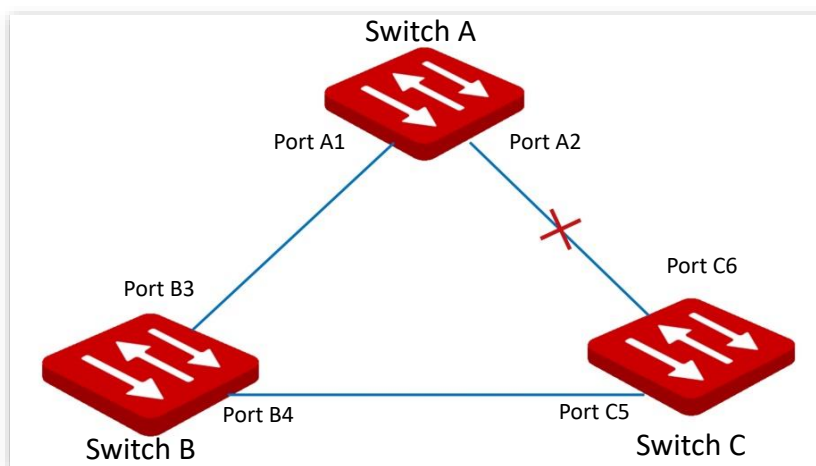
■ Designated bridge and designated port

- 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, it 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

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	<p>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.</p> <p>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.</p>
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	<p>The switch calculates a designated port BPDU for each port according to the root port BPDU and root port path cost.</p> <ul style="list-style-type: none"> - 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.

Step	Content
	<ul style="list-style-type: none"> - The ID of the designated bridge is replaced with that of the switch itself. - The ID of the designated port is replaced with the port ID itself.
3	<p>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.</p> <ul style="list-style-type: none"> - 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 port 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 considered to be 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 with fast convergence, but also allows data flows of different VLANs to be forwarded along the paths respectively, thus enabling better load sharing mechanism for redundant links, which compensates 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 Multiple Spanning Tree (MST) region 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 a Multiple Spanning Tree Instance (MSTI). 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**

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

■ **CST**

Common Spanning Tree (CST) 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**

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

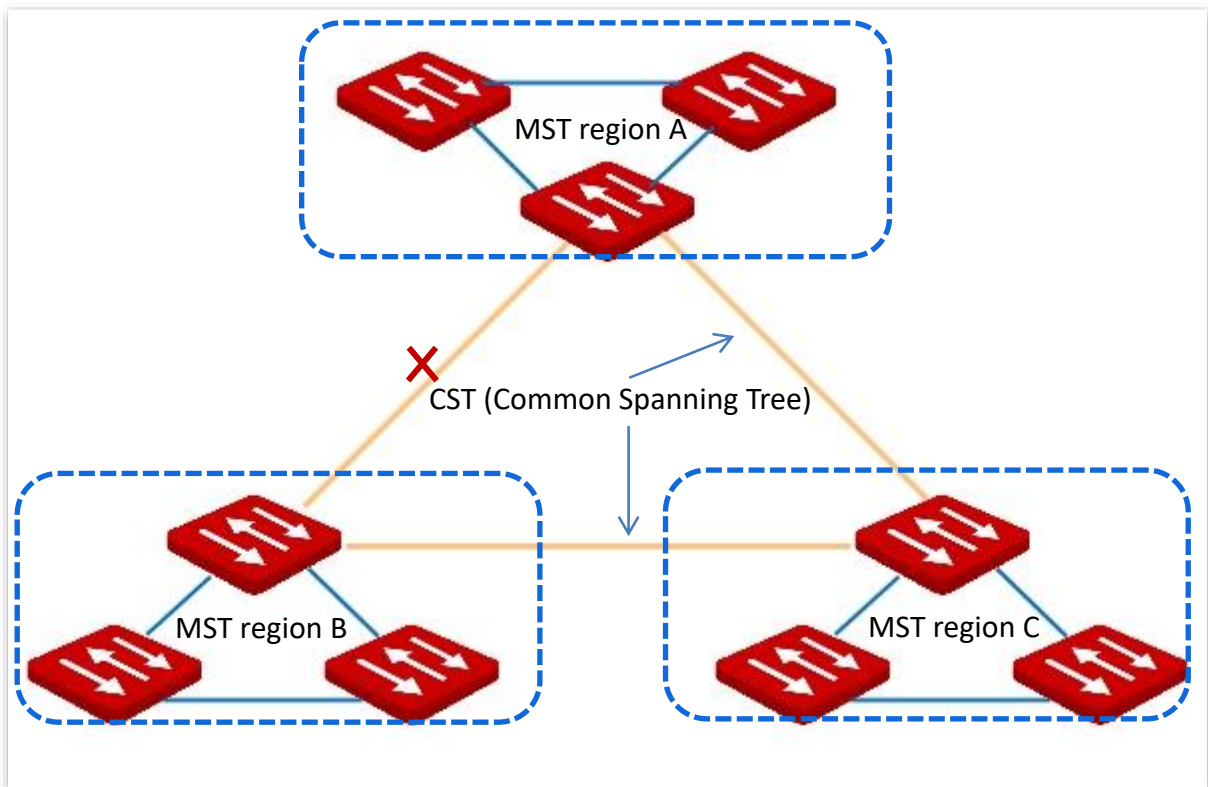
■ **Regional Root**

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

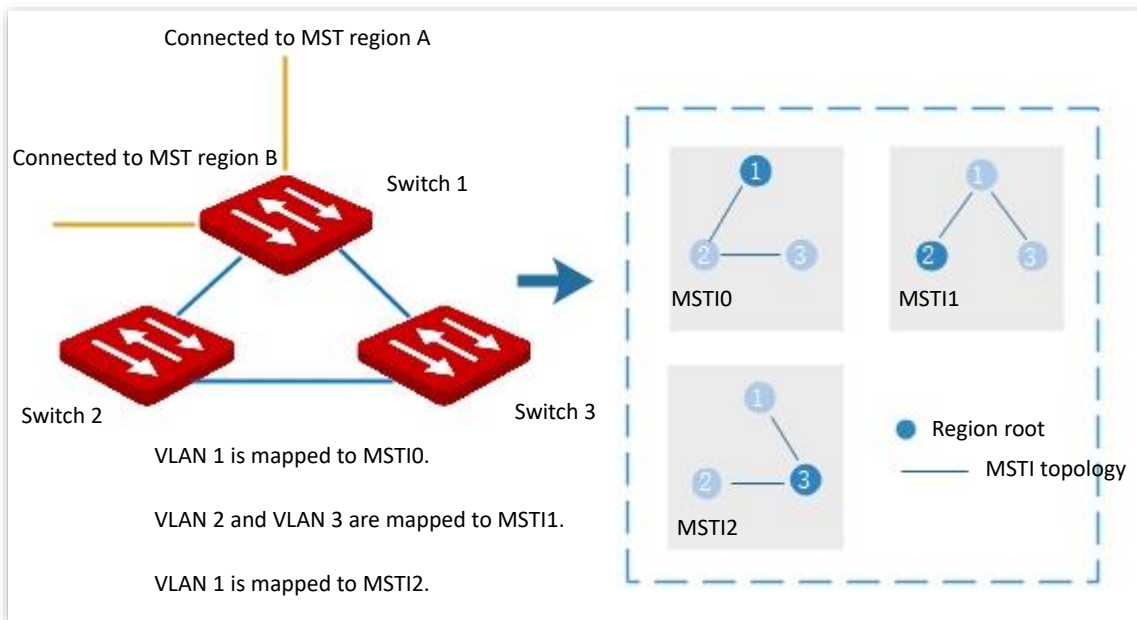
■ **Common Root Bridge**

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.

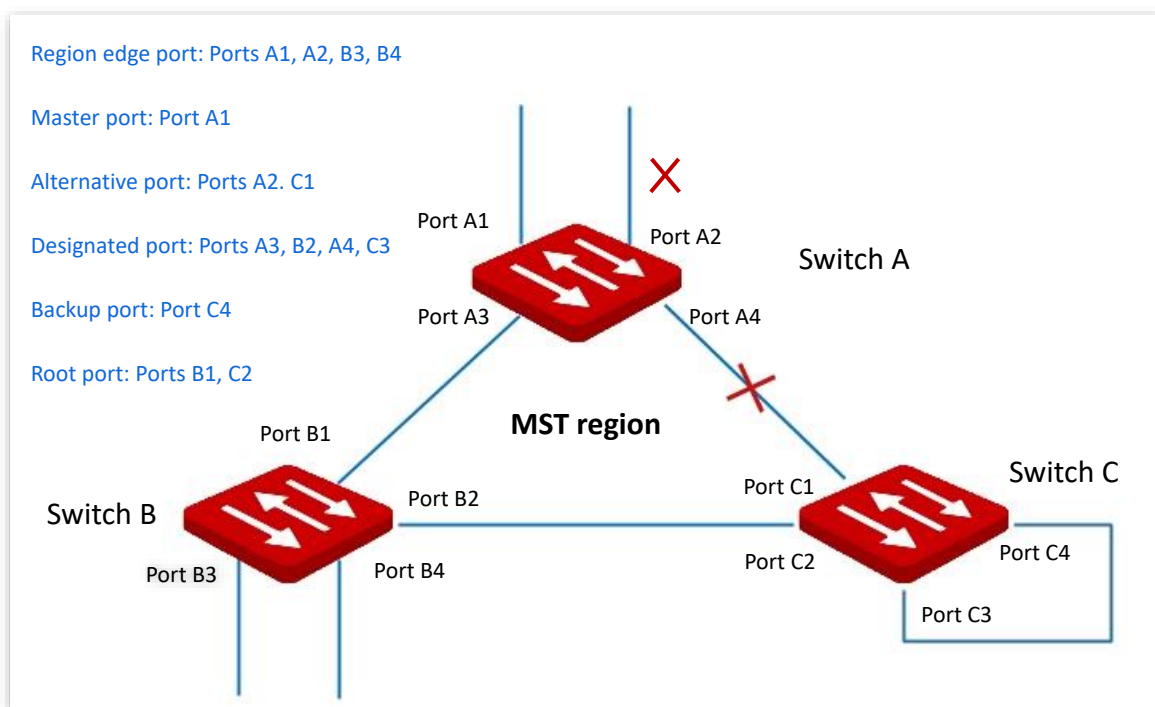
- Learning: The port does not receive or forward data, but receives and sends BPDUs, also learns addresses.
- Discarding: The port neither receives or forwards data, nor sends BPDUs or learns addresses, but receives BPDUs.
- Disabled: The port is not physically linked.

Port role

In MSTP, there are different roles of the ports:

- Root port: It has the least path 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

Navigate to **Switching > Spanning Tree > Global** to enter the page.

On this page, you can configure the global parameters of the spanning tree.

Global	Port Configuration	Port Statistics	Instance Info
Status	<input checked="" type="checkbox"/>		
Mode	MSTP ▼		

Parameter description

Name	Description
Status	Used to enable or disable the spanning tree function.
Mode	<p>The switch supports three spanning tree modes: STP, RSTP and MSTP.</p> <ul style="list-style-type: none"> - 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

Bridge Configuration

Maximum Aging Time s (Range: 6 to 40)

Hello Time s (Range: 1 to 10)

Forwarding Delay s (Range: 4 to 30)

Maximum Hops (Range: 6 to 40)

Bridge Priority ▼

Note: Maximum aging time $\geq 2 \times (\text{Hello Time} + 1)$ Maximum aging time $\leq 2 \times (\text{Forwarding Delay} - 1)$

Parameter description

Name	Description
Maximum Aging Time	<p>Specifies the maximum duration during which the BPDU can be kept in the switch. The configuration should meet the following formulas:</p> <ul style="list-style-type: none"> - Maximum Aging Time $\geq 2 \times (\text{hello time} + 1)$ - Maximum Aging Time $\leq 2 \times (\text{forwarding delay} - 1)$

Name	Description
Hello Time	Specifies the interval at which the switch sends BPDU, which is set to 2 seconds by default.
Forwarding Delay	Specifies the delay that the port state migration takes after the network topology changes, which is set to 15 seconds by default.
Maximum Hops	Specifies the maximum number of the BPDU that can be forwarded, used to limit the scale of the spanning tree.
Bridge Priority	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 region configuration

MSTP Region Configuration

Region Name (Range: 1 to 32 characters)

Revision (Range: 0 to 65535)

Digest 0xAC36177F50283CD4B83821D8AB26DE62

Confirm

Parameter description

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

MSTP Instance


MSTP Instance + Add ✖

	Instance ID	VLAN Mapping List	Bridge Priority	Operation
<input type="checkbox"/>	0	1	32768	--

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	Specifies the instance mapping VLAN.
Bridge Priority	Specifies the instance system priority used for root bridge election of instances in MST regions.

Designated root bridge

Designated Root Bridge 	
Bridge ID 32768:0050.437e.7e7f	Root Bridge ID 32768:0050.437e.7e7f
Region Root ID 32768:0050.437e.7e7f	Root Port none
Root Path Cost 0	Internal Root Path Cost 0
Topology Status Topological_stability	Last Changed Time 2022-09-03 19:51:11

Parameter description

Name	Description
Bridge ID	Specifies the bridge priority and bridge MAC address of this switch.
Region Root ID	Specifies the bridge priority and bridge MAC address of the regional root bridge in the region of this switch.
Root Path Cost	Specifies the sum of root port path cost and the root path cost of all switches that packets pass by. The root path cost of the root bridge is 0.
Topology Status	<p>Specifies the topology status of the spanning tree of this switch.</p> <ul style="list-style-type: none"> – 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	Specifies the port nearest to the root bridge on a non-root-bridge switch.

Name	Description
Internal Root Path Cost	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	Specifies the time of the last topology change.

4.3.3 Port configuration

Navigate to **Switching > Spanning Tree > Port Configuration** to enter the page.

On this page, you can configure the STP parameters of the ports.

Port	STP Status	Edge Port	P2P Port	Operation
1	Enable	Disable	Auto	
2	Enable	Disable	Auto	
3	Enable	Disable	Auto	
4	Enable	Disable	Auto	
5	Enable	Disable	Auto	
6	Enable	Disable	Auto	
7	Enable	Enable	Auto	

Parameter description

Name	Description
Port	Specifies the ID of the port.
STP Status	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 edge ports by default. <ul style="list-style-type: none"> - 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. <ul style="list-style-type: none"> - 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

Navigate to **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.

Port	Transmit				Receive				Discard	
	MSTP	RSTP	STP	TCN	MSTP	RSTP	STP	TCN	Unknown	Illegal
1	0	0	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	0	0	0
3	0	0	0	0	0	0	0	0	0	0
4	0	0	0	0	0	0	0	0	0	0
5	0	0	0	0	0	0	0	0	0	0
6	0	0	0	0	0	0	0	0	0	0

Parameter description

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

4.3.5 Instance info

Navigate to **Switching > Spanning Tree > Instance Info** to enter the page.

On this page, you can view and configure the MSTP instance information.

Port	Port Role	Port Status	Region Root ID	Designated Bridge	Designated Port	Priority	Path Cost	Operation
1	Disabled	Disabled	32768-0050.437e.7e7f	32768-0050.437e.7e7f	1	128	20000	
2	Disabled	Disabled	32768-0050.437e.7e7f	32768-0050.437e.7e7f	2	128	20000	
4	Disabled	Disabled	32768-0050.437e.7e7f	32768-0050.437e.7e7f	4	128	20000	
5	Disabled	Disabled	32768-0050.437e.7e7f	32768-0050.437e.7e7f	5	128	20000	
6	Disabled	Disabled	32768-0050.437e.7e7f	32768-0050.437e.7e7f	6	128	20000	
7	Disabled	Disabled	32768-0050.437e.7e7f	32768-0050.437e.7e7f	7	128	20000	
8	Disabled	Disabled	32768-0050.437e.7e7f	32768-0050.437e.7e7f	8	128	20000	

Parameter description

Name	Description
Instance ID	Used to select the instance ID to check the STP state information of the instance.
Port	Specifies the ID of the port.
Port Role	Specifies the role of the port plays in the spanning tree instance. For more details, please refer to Port role .
Port Status	Specifies the current operating status of the port. For more details, please refer to Port status .
Region Root ID	Specifies the bridge priority and bridge MAC address of the regional root bridge.
Designated Bridge	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	Specifies the port to which the designated bridge forwards BPDU messages.
Priority	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.

Link Layer Discovery Protocol (LLDP) 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 Link Layer Discovery Protocol Data Units (LLDPDUs) to release to neighbors to which they are directly connected. After receiving the info, the neighbors will save them as the standard Management Information Base (MIB) 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.
- **Disable:** 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 **Disable** or **Receive only** to **Send & receive** or **Send only**, the switch sends an 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

Navigate to **Switching > LLDP Configuration > Global** to enter the page.

On this page, you can configure the global parameters of LLDP.

LLDP Function

Global Port Configuration Neighbor Info

Transmission Interval s (Range: 5 to 3600)

TTL Multiplier s (Range: 2 to 10)

Initialization Delay s (Range: 1 to 10)

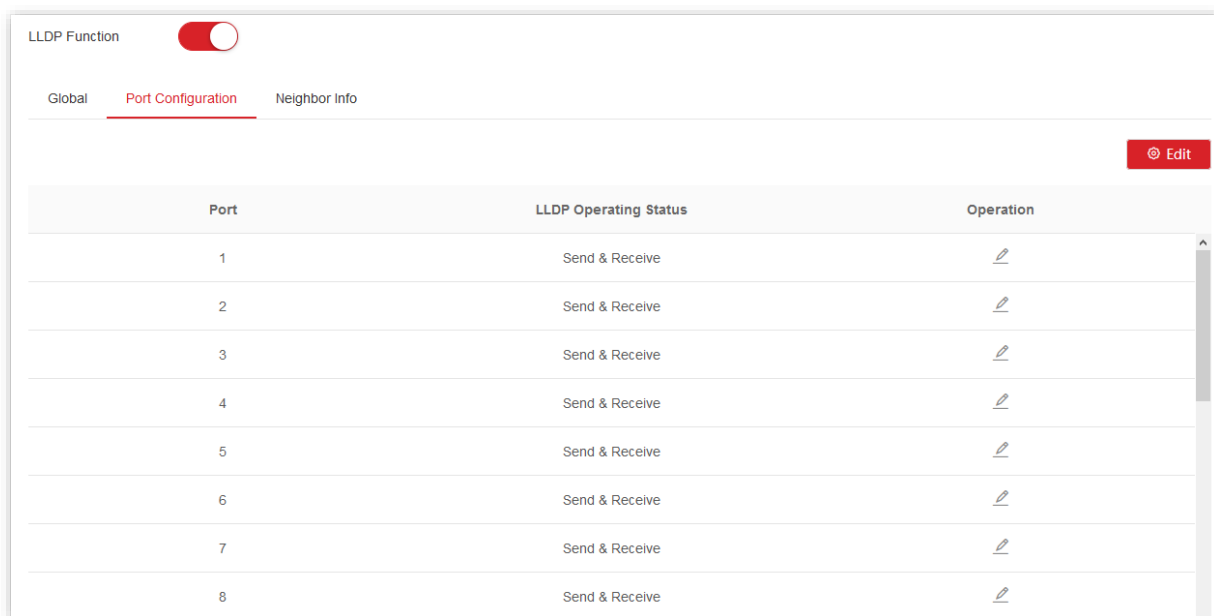
Parameter description

Name	Description
LLDP Function	Used to enable or disable the LLDP function.
Transmission Interval	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 × LLDPDU transmission interval), indicating the minimum value between 65535 and TTL multiplier × LLDPDU transmission 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 change.

4.4.3 Port configuration

Navigate to **Switching > LLDP Configuration > Port Configuration** to enter the page.

On this page, you can configure the LLDP operating status for each port.



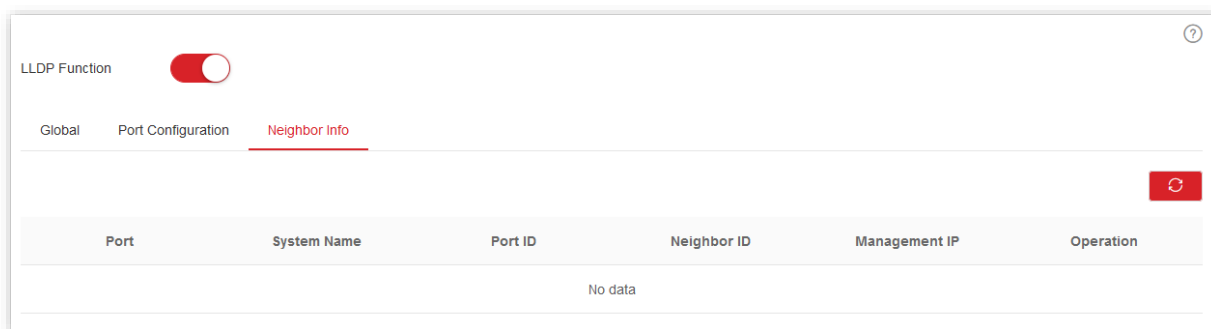
Parameter description

Name	Description
Port	Specifies the ID of the port.
LLDP Operating Status	<p>Indicates the LLDP operating status of each port.</p> <ul style="list-style-type: none"> - 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

Navigate to **Switching > LLDP Configuration > Neighbor Info** to enter the page.

On this page, you can view the neighbor information.



Parameter description

Name	Description
Port	Specifies the ID of the port.
System Name	Specifies the system name of the neighbor device.
Port ID	<p>Specifies the port information of the neighbor device.</p> <p> Tip</p> <p>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.</p>
Neighbor ID	Specifies the MAC address of the neighbor device.
Management IP	Specifies the management IP address of the neighbor device.
Survival Time	Specifies the rest of the time that the neighbor info can be saved and displayed on the switch.
Port Description	Specifies the detailed description of the port used to transmit LLDP messages on the neighbor device.
System Description	Specifies the detailed description of the neighbor device.
Performance	Specifies the features supported by the neighbor device.

4.5 LLDP-MED

4.5.1 Overview

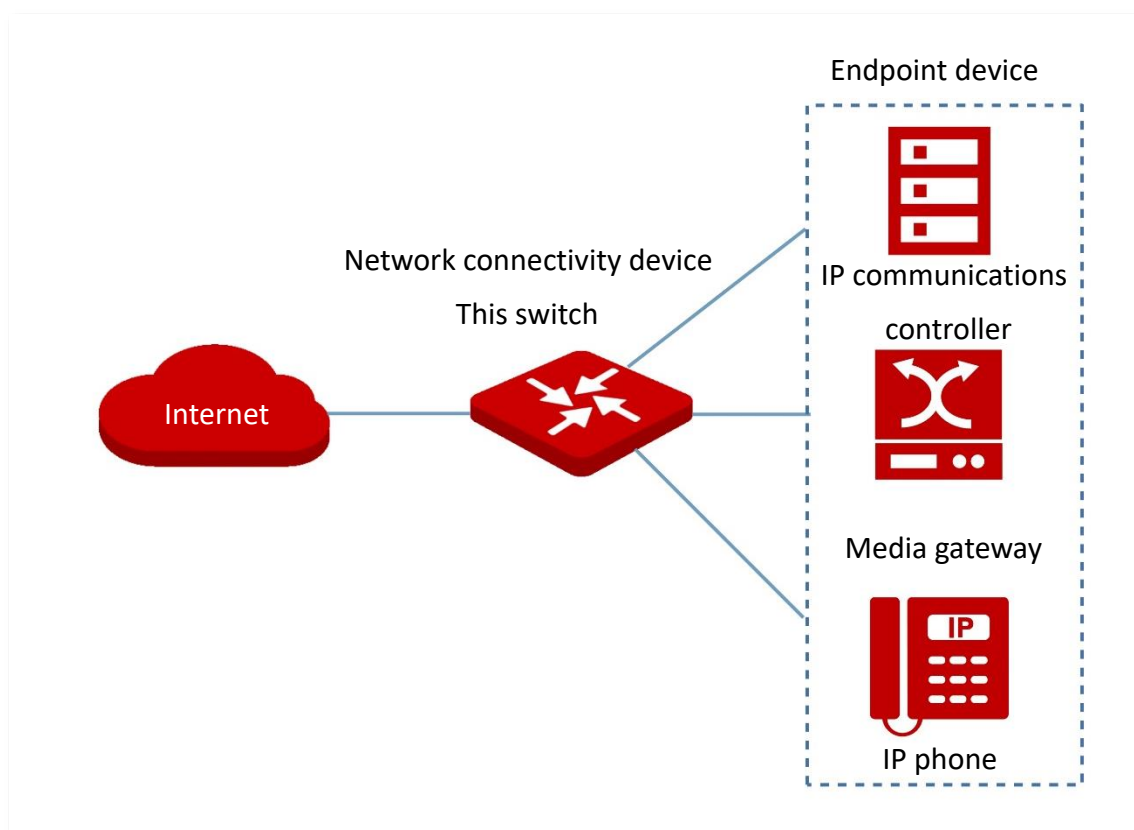
Link Layer Discovery Protocol - Media Endpoint Discovery (LLDP-MED) is an extension of LLDP and is used to advertise information between network devices and media endpoints. It is specially used together with Auto Voice over Internet Protocol (VoIP) to allow the network access and auto-configuration of VoIP devices.

With LLDP-MED, this switch offers three kinds of TLVs: Capabilities, Network Policy and Location Identification, helping network administrators to troubleshoot the network faults occurred and facilitating the deployment and management of VoIP devices in the Ethernet at lower costs.

Device type

LLDP-MED defines two device types: Network Connectivity Device and Endpoint Device. This switch is a Network Connectivity Device.

The network topology of LLDP-MED is shown as below.



Network connectivity device

LLDP-MED Network Connectivity Devices, provide access to the IEEE 802 based LAN infrastructure for LLDP-MED Endpoint Devices. An LLDP-MED Network Connectivity Device is a LAN access device based on any of the following technologies:

- LAN Switch/Router
- IEEE 802.1 Bridge
- IEEE 802.3 Repeater
- IEEE 802.11 Wireless Access Point
- Any device that supports the IEEE 802.1AB and MED extensions and can relay IEEE 802 frames via any method.

Endpoint device

LLDP-MED Endpoint Devices, are located at the IEEE 802 LAN network edge, and divided into Class I, Class II and Class III.

■ **Generic endpoint (Class I)**

Basic participant endpoints in LLDP-MED, such as IP communications controllers.

■ **Media endpoint (Class II)**

Supports IP media streams, such as media gateways, conference bridges and media servers.

■ **Communication endpoint (Class III)**

Supports IP communication end users, such as IP telephones and softphones.

4.5.2 Basic

Navigate to **Switching > LLDP-MED > Basic** to enter the page.

On this page, you can configure the basic parameters of LLDP-MED.

The screenshot shows a configuration interface with the following elements:

- Navigation tabs: **Basic**, TLV Settings, Local Information, Neighbor Info.
- Fast LLDPDU Count: (Range: 1 to 10)
- Device Type:
- Confirm button:

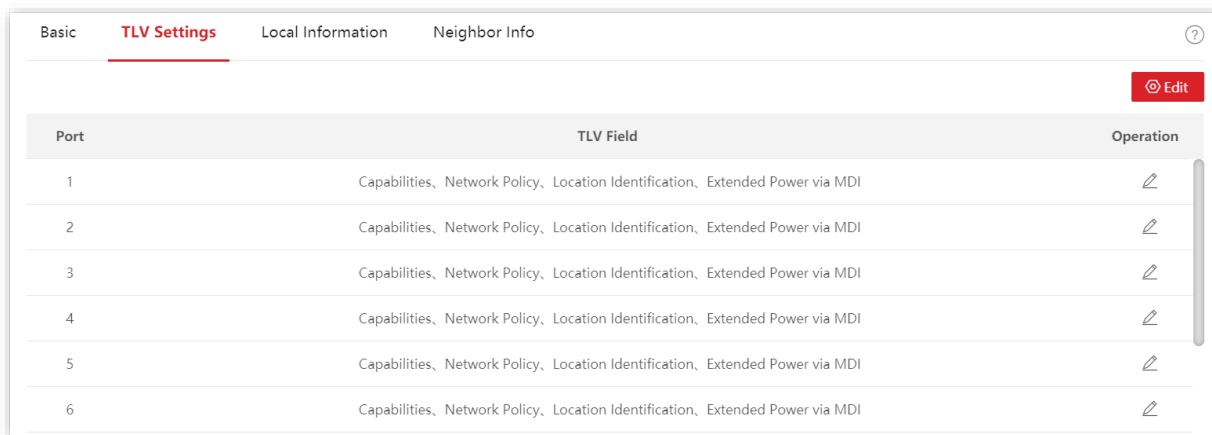
Parameter description

Name	Description
Fast LLDPDU Count	Specifies the number of successive LLDP-MED packets that the switch sends when it receives the LLDP-MED packets from the neighbor endpoints. The default value is 4.
Device Type	Specifies the current LLDP-MED device type. The switch is a Network Connectivity device.

4.5.3 TLV settings

Navigate to **Switching > LLDP-MED > TLV Settings** to enter the page.

On this page, you can configure the TLV information of LLDP-MED.



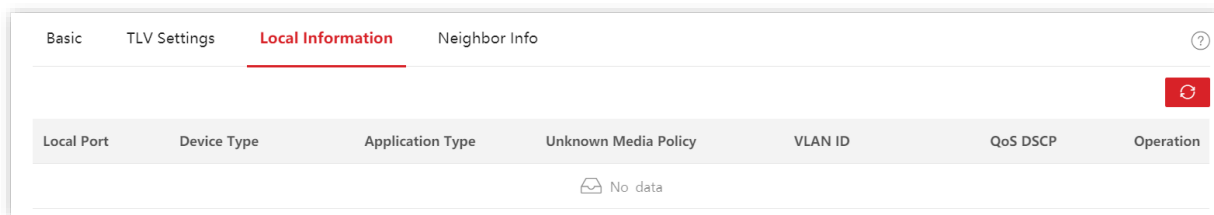
Parameter description

Name	Description
Port	Specifies the port number of the switch.
TLV Field	<p>Used to select the TLV information included in the LLDPDU.</p> <ul style="list-style-type: none"> - Capabilities: It allows a network device to advertise the LLDP-MED TLVs that it supports. - Network Policy: It allows the connected switch and endpoint devices to advertise VLAN configurations and associated Layer 2 and Layer 3 attributes for the specific application on that port. - Location Identification: It is used to advertise the appropriate location identifier information of a local device to a neighbor device. - Extended Power via MDI: It allows LLDP-MED connectivity devices and endpoints to convey detailed power information, such as power priority and power status.

4.5.4 Local information

Navigate to **Switching > LLDP-MED > Local Information** to enter the page.

On this page, you can view the LLDP-MED configurations of all ports.



Parameter description

Name	Description
Local Port	Specifies the port number of the switch.
Device Type	Specifies the local device types defined by LLDP-MED.
Application Type	Specifies the application types supported by the local devices.
Unknown Media Policy	Specifies the setting of unknown tag included in the network policy.
VLAN ID	Specifies the 802.1Q VLAN ID of the port.
QoS DSCP	Specifies the DSCP value of certain application.

4.5.5 Neighbor info

Navigate to **Switching > LLDP-MED > Neighbor Info** to enter the page.

On this page, you can view the LLDP-MED information of neighbor devices on all ports.

Local Port	System Name	Neighbor ID	Device Type	Application Type	Location Type	Power Port Class	Operation
No data							

Parameter description

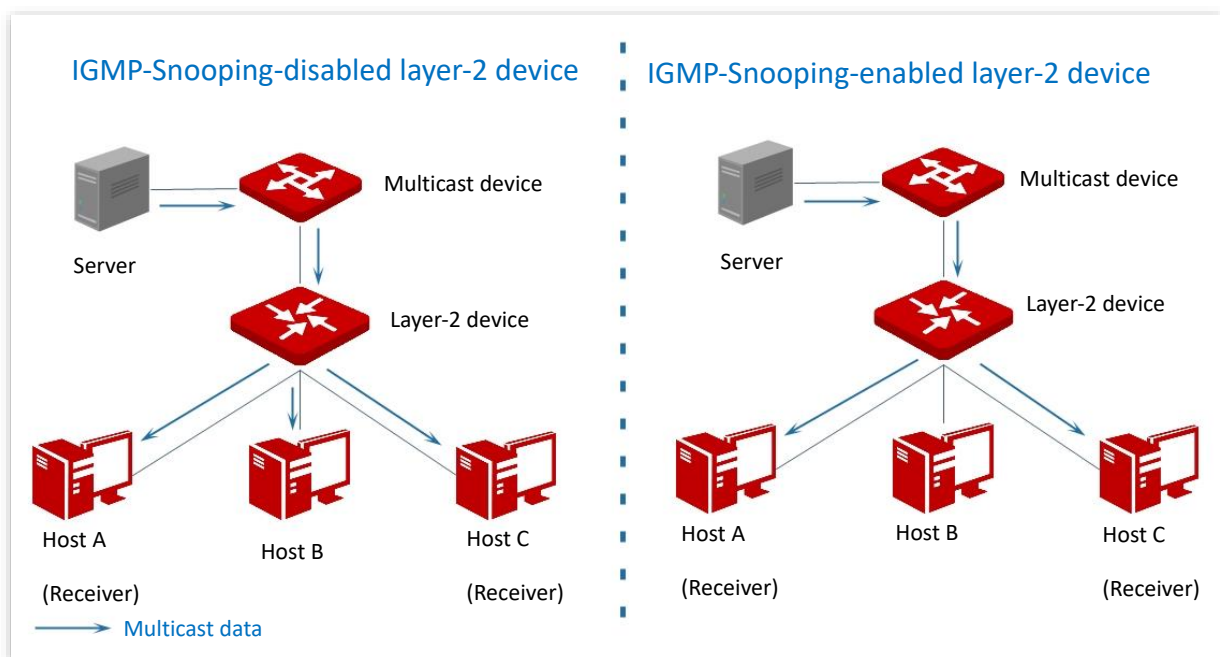
Name	Description
Local Port	Specifies the port number of this switch.
System Name	Specifies the system name of the neighbor device.
Neighbor ID	Specifies the MAC address of the neighbor device.
Device Type	Specifies the neighbor device types defined by LLDP-MED.
Application Type	Specifies the application types supported by the neighbor devices.
Location Type	Specifies the location types of neighbor devices.
Power Port Class	Specifies the power port classes of neighbor devices.

4.6 IGMP snooping

4.6.1 Overview

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

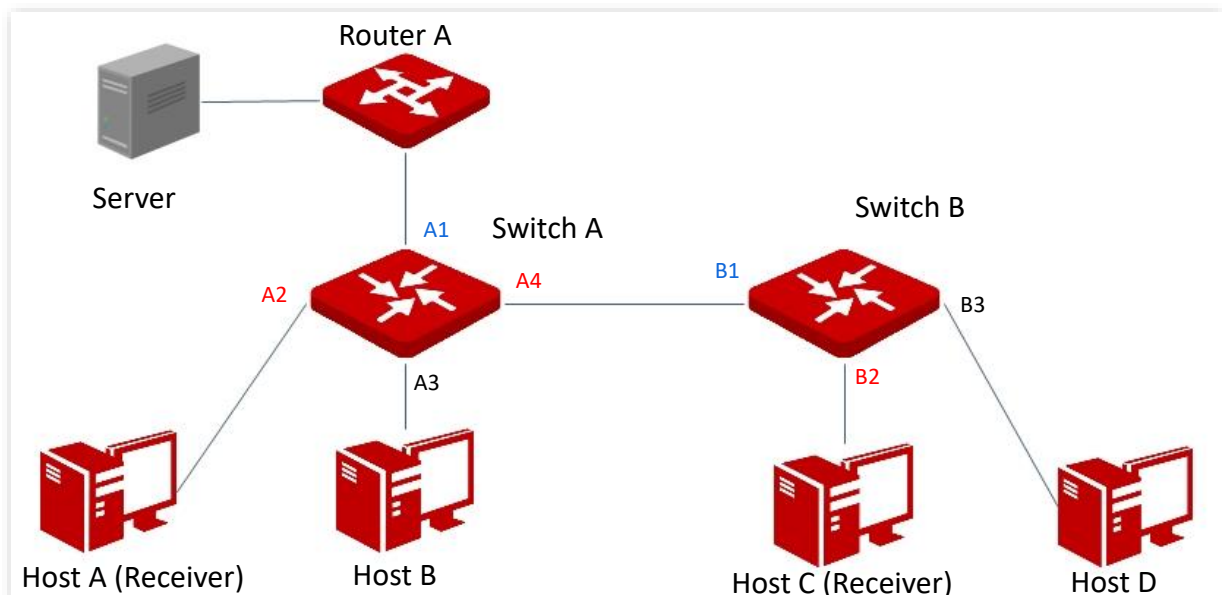
As shown in the figure below, multicast data is broadcasted from the IGMP-Snooping-disabled layer-2 device. But with IGMP Snooping enabled, the layer-2 device will establish a mapping table for ports and multicast MAC addresses by analyzing received IGMP messages, and forward multicast data to the specific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

4.6.2 Global

Navigate to **Switching > IGMP Snooping > Global** to enter the page.

On this page, you can configure the global parameters of IGMP snooping.

IGMP Snooping

Global Fast Leave

VLAN ID

VLAN

Multicast VLAN Status

Protocol Version

Routing Port Aging Time s (Range: 1 to 1000)

General Query Response Time s (Range: 1 to 25)

Specific Query Response Time s (Range: 1 to 5)

Aging Time of Host Port s (Range: 200 to 1000)

Multicast Discard

Parameter description

Name	Description
IGMP Snooping	Used to enable or disable the IGMP snooping function.
VLAN ID	Specifies the VLAN whose IGMP Snooping function is enabled.

Name	Description
VLAN	Used to enable or disable the IGMP Snooping function of the VLAN.
Multicast VLAN Status	<p>Used to enable or disable the multicast VLAN function of the above VLAN.</p> <p>By default, the multicast VLAN function of the switch is disabled. If devices from different VLANs within the 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.</p>
Protocol Version	<p>Supported IGMP message versions:</p> <ul style="list-style-type: none"> - 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	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	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	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	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.

4.6.3 Fast leave

Navigate to **Switching > IGMP Snooping > Fast Leave** to enter the page.

On this page, you can configure the fast leave mode for each port.

Port	Fast Leave	Operation
1	Disable	
2	Disable	
4	Disable	
5	Disable	
6	Disable	
7	Disable	
8	Disable	

Parameter description

Name	Description
Port	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.

4.7 MAC settings

4.7.1 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.

Navigate to **Switching > MAC Settings > MAC Address Table** to enter the page.

On this page, you can view and delete the MAC address table entries.

MAC Address	Type	VLAN	Port	Operation
002b-672c-2010	Dynamic	1	AGG1	
c83a-3583-efd0	Dynamic	1	9	

Parameter description

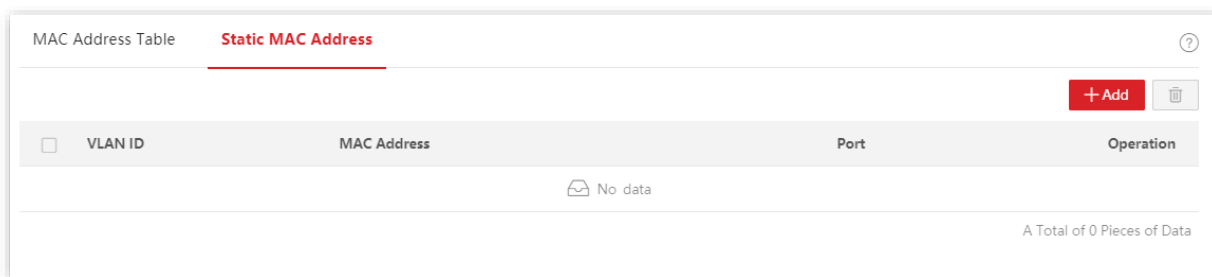
Name	Description
Aging Time	Specifies the aging time of the entries in the MAC address table, which is effective only for dynamic entries. When the switch does not receive messages whose source address is consistent with the source MAC address in the table within the aging time, the MAC address table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

Name	Description
Type	<p>Specifies the type of the MAC address.</p> <ul style="list-style-type: none"> - Static: Specifies the MAC address entry manually configured by the administrator. - Dynamic: Specifies the MAC address entry automatically generated by the switch.
VLAN	Specifies the VLAN to which the MAC address belongs.
Port	Specifies the physical port of the switch that the device with the MAC address connects to.

4.7.2 Static MAC address

Navigate to **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	Specifies the VLAN to which the MAC address belongs.
MAC Address	MAC address, format: XXXX-XXXX-XXXX.
Port	Specifies the physical port of the switch that the device with the MAC address connects to.

5 Routing

5.1 Static routing

5.1.1 Overview

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



The static route owns the highest priority among all routes.

5.1.2 Configure static routing

Navigate to **Routing > Static Routing** to enter the page.

On this page, you can view and configure the static routing rules.

Static Routing				?
<input type="checkbox"/>	Destination Address	Subnet Mask	Next Hop	Operation
<input type="checkbox"/>	0.0.0.0	0.0.0.0	192.168.0.252	

Parameter description

Name	Description
Destination Address	Specifies the network segment of the destination network.
Subnet Mask	Specifies the subnet mask of the destination network.
Next Hop	Specifies the ingress IP address of the next hop route after packets egress from the switch.

5.1.3 Example of static routing configuration

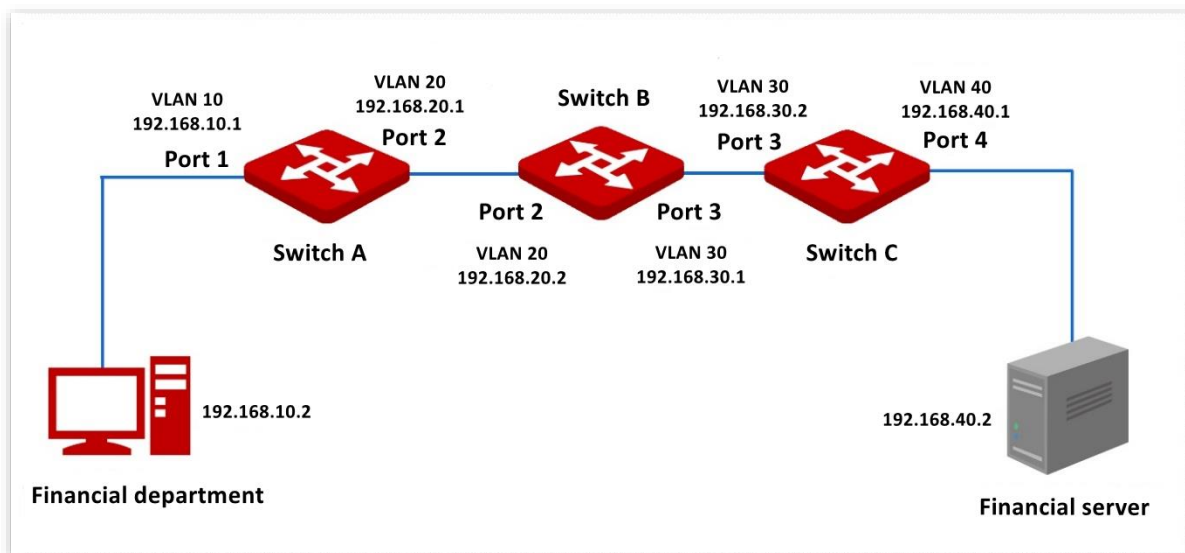
Network requirement

The staff of the financial department work on the second floor, while the server for the financial department is on the third floor. Now it is required that the financial staff can access the financial server.

Solution

Configure devices as follows:

- Create VLANs on the switches, and configure the IP address and port member of each VLAN to enable network communication among neighbor devices.
- Configure static routing on switches to enable communication among different network segments.
- Assign a static IP address to the financial server to avoid the problem that the staff cannot access the server due to the change of IP address.
- Set computers of financial staff to **Obtain an IP address automatically** and **Obtain DNS server address automatically**. Assume that the IP address information obtained by the computers through DHCP is as follows:
 - IP address: 192.168.10.2
 - Subnet mask: 255.255.255.0
 - Default gateway: 192.168.10.1



Configuration procedure

I. Configure VLANs

Configure VLANs for switch A, switch B and switch C. Assume the configurations are as follows:

Switch	Port	VLAN	IP Address
Switch A	1	10	192.168.10.1/24
	2	20	192.168.20.1/24
Switch B	2	20	192.168.20.2/24
	3	30	192.168.30.1/24
Switch C	3	30	192.168.30.2/24
	4	40	192.168.40.1/24

Here, the configuration of switch A is used as an example. For switch B and switch C, the configurations are similar.

1. Add VLANs.

- (1) Log in to the web UI of switch A, and navigate to **Basics > VLAN > 802.1Q VLAN**.
- (2) Click **+ Add** to add the following two VLANs.

<input type="checkbox"/>	VLAN ID	VLAN Description	IPv4 Address	Subnet Mask	Operation
<input type="checkbox"/>	1	default	192.168.0.100	255.255.255.0	
<input type="checkbox"/>	10	10	192.168.10.1	255.255.255.0	
<input type="checkbox"/>	20	20	192.168.20.1	255.255.255.0	

2. Configure port properties.

- (1) Log in to the web UI of switch A, and navigate to **Basics > VLAN > Port Member**.
- (2) Click the button behind port 1 and set **PVID** to **10**.
- (3) Click the button behind port 2 and set **PVID** to **20**.

Port	Link Type	PVID	Tagged	Untagged	Operation
1	Access	10	--	10	
2	Access	20	--	20	

II. Configure static routing

Configure static routing for switch A, switch B and switch C. Assume that the configuration are as follows:

Switch	Destination IP Address	Subnet Mask	Next Hop
Switch A	192.168.40.0	255.255.255.0	192.168.20.2
Switch B	192.168.40.0	255.255.255.0	192.168.30.2
	192.168.10.0	255.255.255.0	192.168.20.1
Switch C	192.168.10.0	255.255.255.0	192.168.30.1

Here, the configuration of switch A is used as an example. For switch B and switch C, the configurations are similar.

1. Log in to the web UI of switch A, and navigate to **Routing > Static Routing**.
2. Click **+ Add** to add the following static route.

Destination Address	Subnet Mask	Next Hop	Operation
192.168.40.0	255.255.255.0	192.168.20.2	

III. Assign IP addresses to computers of financial staff dynamically

1. Log in to the web UI of switch A, and navigate to **Routing > DHCP Server**.
2. Enable the general **DHCP Server**, and enable **DHCP Server** for VLAN 10.
3. Click **+ Add** to configure the following DHCP address pool.


Name	IP Address Range	Subnet Mask	Default Gateway	Lease Time	DNS	Excluded IP Range	Operation
Financialdepartment	192.168.10.2 ~ 192.168.10.250	255.255.255.0	192.168.10.1	30 min	192.168.10.1	--	

A Total of 1 Piece of Data

VLAN Interface	Layer-3 Interface	Subnet Mask	DHCP Server
1	192.168.0.100	255.255.255.0	<input type="checkbox"/>
10	192.168.10.1	255.255.255.0	<input checked="" type="checkbox"/>
20	192.168.20.1	255.255.255.0	<input type="checkbox"/>

A Total of 3 Pieces of Data

IV. Save the configurations

Click  **Save** at the upper right corner to save the above configurations.

V. Configure the IP address and gateway of financial server

Assign a static IP address and related information to the financial sever, as shown below:

Switch	Destination IP Address	Subnet Mask	Next Hop
Financial Server	192.168.40.2	255.255.255.0	192.168.40.1

----End

Verification

After the configuration, financial staff's computers can access the financial server.

5.2 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, the ARP address will be resolved first. The resolution process are 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 the data to the destination host according to the queried rule. If not, the switch broadcasts an ARP request data frame in the data link layer of 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 IP address and MAC address of the destination host into its ARP table for further use.

Navigate to **Routing > ARP** to enter the page.

On this page, you can view and configure the ARP cable.

IP Address	MAC Address	VLAN ID	Type	Aging Time	Operation
192.168.0.103	002b.672c.2010	vlan1.1	Dynamic	340s	
192.168.0.252	c83a.3583.efd0	vlan1.1	Dynamic	1160s	

Parameter description

Name	Description
ARP Aging Time	Specifies the aging time of ARP. If the switch does not receive the ARP message within this period of time, the ARP routing rule will be deleted from the ARP table.
IP Address	Specifies the IP address of the destination host.
MAC Address	Specifies the MAC address of the destination host corresponding to the IP address.

Name	Description
VLAN ID	Specifies the VLAN layer 3 interface at which the ARP rule is located.
Type	Specifies the types of the table. <ul style="list-style-type: none"><li data-bbox="501 376 1374 439">– Dynamic: Specifies the ARP table which is automatically identified by the switch. The life cycle is the ARP aging time.<li data-bbox="501 454 1406 517">– Static: Specifies the manually configured ARP table. The rule is permanently valid, and is free from the limitations of the ARP aging time.
Aging Time	Specifies the remaining aging time of the ARP routing rule.

5.3 DHCP server

5.3.1 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. Dynamic Host Configuration Protocol (DHCP) can solve the above issues by IP address dynamic assignment strategy.



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

IP address allocation strategy

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.

5.3.2 DHCP settings

Navigate to **Routing > DHCP Server > DHCP Settings** to enter the page.

On this page, you can view and configure the DHCP server.

The screenshot displays the DHCP Settings configuration page. At the top, there are tabs for 'DHCP Settings', 'DHCP Reservation', and 'Client List'. The 'DHCP Server' toggle is turned on. Below this, there is an 'IP Address Pool' section with a '+ Add' button and a trash icon. A table with columns: Name, IP Address Range, Subnet Mask, Default Gateway, Lease Time, DNS, Excluded IP Range, and Operation is shown, with a 'No data' message. At the bottom, the 'DHCP Server for Interface' section contains a table with columns: VLAN Interface, Layer-3 Interface, Subnet Mask, and DHCP Server. The table shows configuration for VLAN Interface 1 with Layer-3 Interface 192.168.0.105, Subnet Mask 255.255.255.0, and the DHCP Server toggle is turned off.

Name	IP Address Range	Subnet Mask	Default Gateway	Lease Time	DNS	Excluded IP Range	Operation
No data							

VLAN Interface	Layer-3 Interface	Subnet Mask	DHCP Server
1	192.168.0.105	255.255.255.0	<input type="checkbox"/>

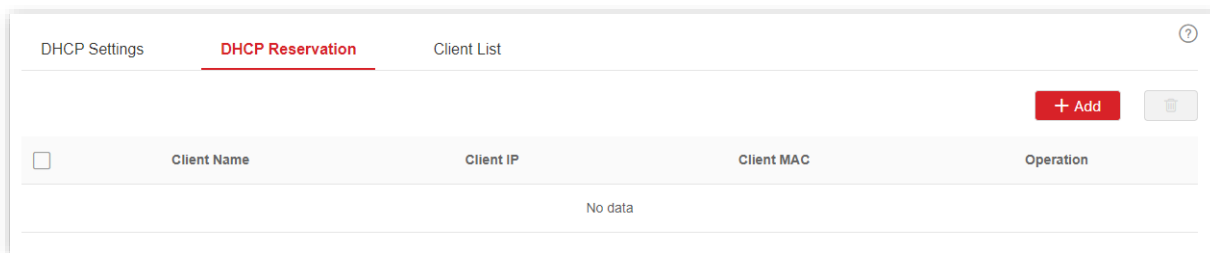
Parameter description

Name	Description	
DHCP Server	Enable or disable the DHCP Server function.	
IP Address Pool	Name	Specifies the name of the IP address pool policy.
	IP Address Range	Specifies the range of IP addresses that can be assigned through this rule.
	Subnet Mask	Specifies the subnet mask assigned by the DHCP server to a client.
	Default Gateway	Specifies the gateway address assigned by the DHCP server to a client.
	Lease Time	<p>Specifies the validity period of an IP address assigned by the DHCP server to a client. When the lease time expires:</p> <ul style="list-style-type: none"> – If the client is still connected to the switch, the client will renew the lease and continue to keep the IP address. – If the client is no longer connected to the switch, the switch will release the IP address. If another client sends a request to apply for an IP address, the switch can assign the IP address to such client. <p>For less resource consumption, please set the lease time according to the actual network environment and try to reduce the number of sending messages. it is recommended to set to 1 day if there is no other special requirement.</p>
	DNS	Specifies the DNS server address assigned to clients.
DHCP Server for Interface	Excluded IP Range	Specifies the IP addresses in the IP address pool that are not assigned by the DHCP server by dynamic assignment strategy.
	VLAN Interface	Specifies the VLAN where the address pool policy takes effect.
	Layer-3 Interface	Specifies the IP address of the VLAN interface.
	Subnet Mask	Specifies the subnet mask of the VLAN interface.
	DHCP Server	With it enabled, the DHCP Server function of the VLAN interface takes effect.

5.3.3 DHCP reservation

Navigate to **Routing > DHCP Server > DHCP Reservation** to enter the page.

On this page, you can view and configure the DHCP reservation policy.



Parameter description

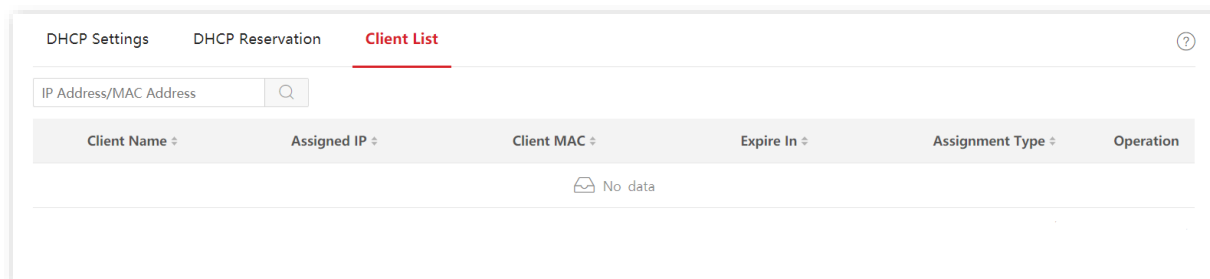
Name	Description
Client Name	Specifies the description of the DHCP reservation policy. If the reservation policy is added from the client list, it displays the client name or you can customize it.
Client IP	Specifies a fixed address assigned by the DHCP server to the client.
Client MAC	Specifies the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

5.3.4 Client list

Navigate to **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**, 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	Specifies the name of a client.
Assigned IP	Specifies an IP address assigned by the DHCP server to the client.
Client MAC	Specifies the MAC address of a client.
Expire In	Specifies the remaining time of the lease.
Assignment Type	<p>Specifies the address assignment policy by the DHCP server to the client.</p> <ul style="list-style-type: none"> - Dynamic: The DHCP server assigns a dynamic IP address to this client using dynamic IP address assignment policy. - Static: The DHCP server assigns a static IP address to this client using static IP address assignment policy.

6 QoS policy

6.1 Overview

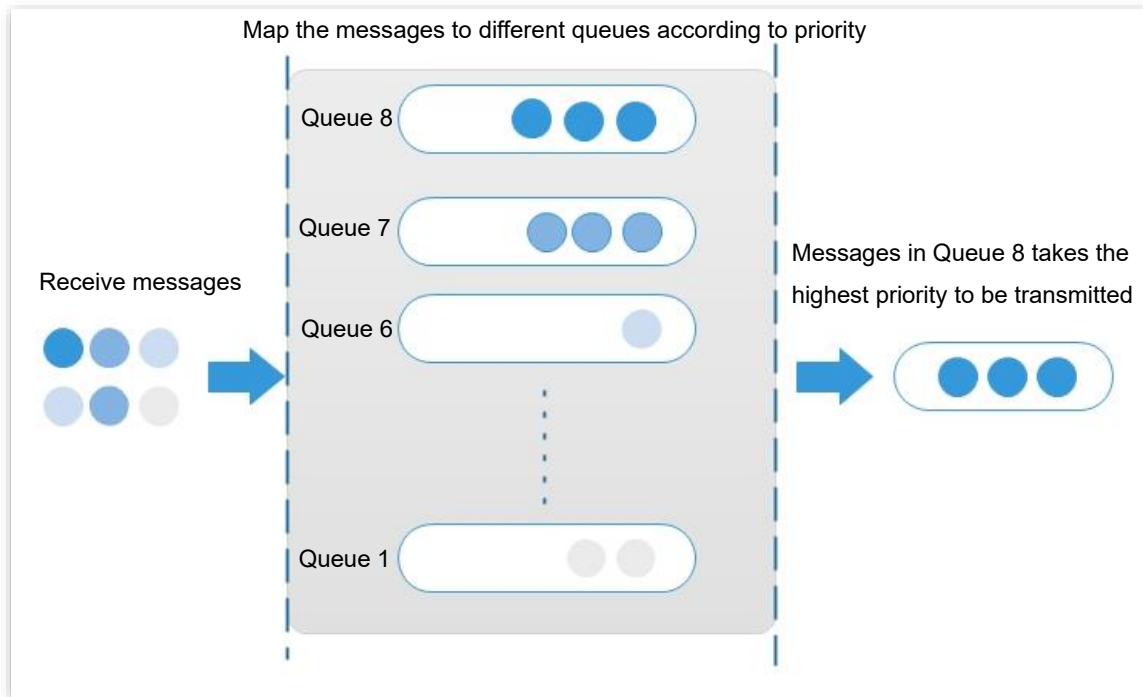
In traditional IP network, packets are treated equally. This network service policy is known as Best-effort, which delivers the packets to their destination with the best effort, with no assurance and guarantee for delivery delay, reliability, and so on. Nowadays, in addition to traditional applications 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 of bandwidth, delay and jitter. Quality of Service (QoS) 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 1 to 8) 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.

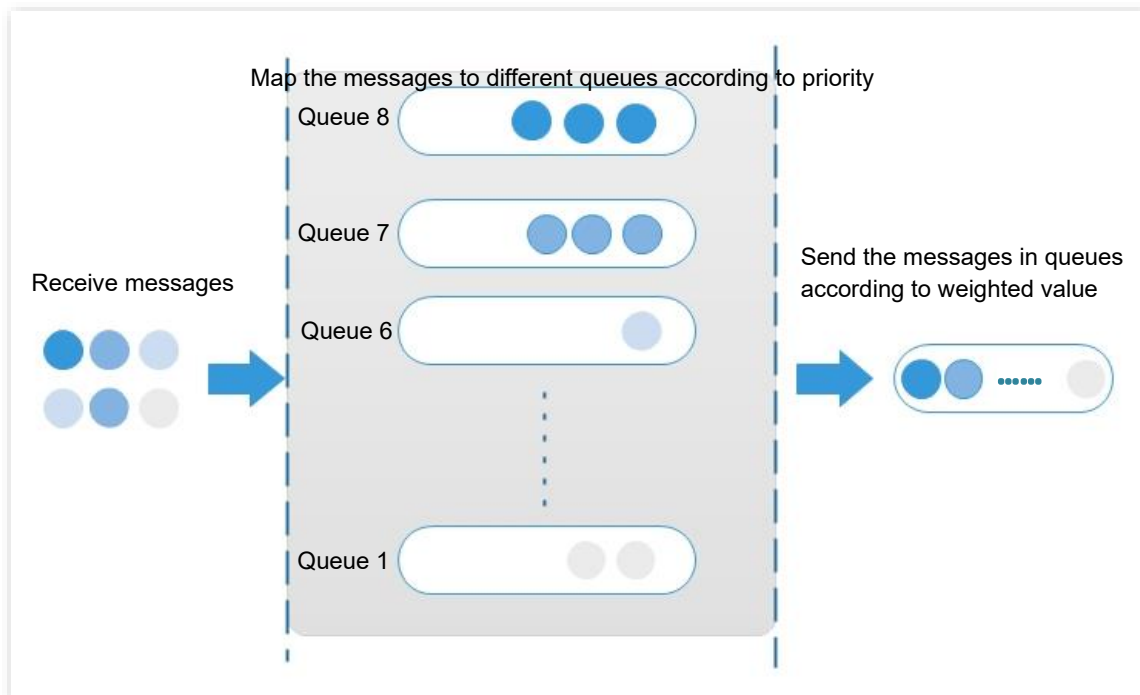
■ Simple Weighted Priority

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. Assuming 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.

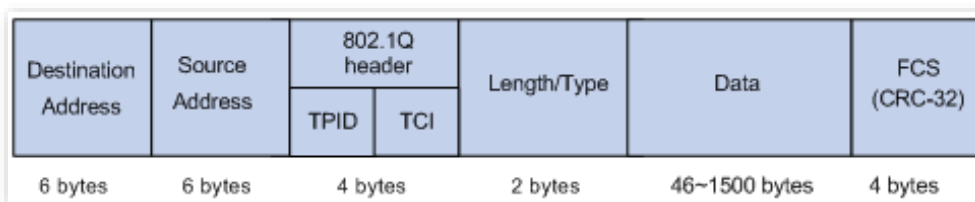


Priority

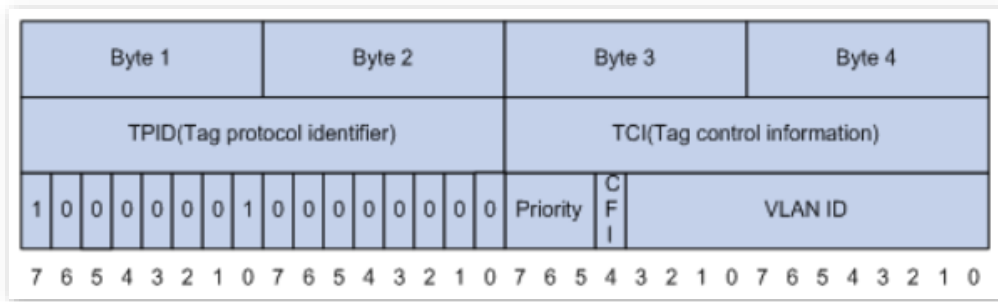
This switch supports three priority modes: [802.1P Priority](#), [DSCP priority](#), and [Port Priority](#).

■ 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 Tag Protocol Identifier (TPID, value: 0x8100) and a 2-byte Tag Control Information (TCI).



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.

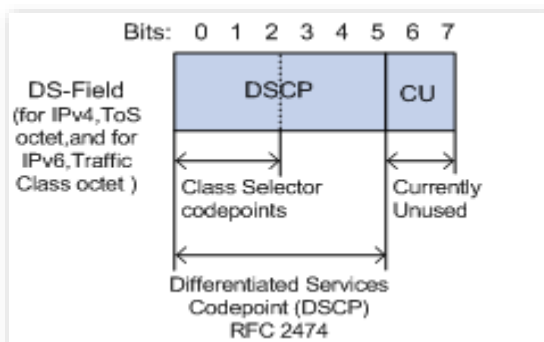


By default, the 802.1P priority, queues, and key words of this switch are mapped as follows.

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 Type of Service (ToS) field in the IP message header, which is called the Differentiated Services (DS) field. The first six bits (bits 0 to 5) of the DS field indicate the Differentiated Services Codepoint (DSCP) 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
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 Class of Service (Cos) 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 802.1P priority

Step	Task	Description
1	QoS Scheduler	Required. Select the scheduler 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 scheduler 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

Navigate to **QoS Policy > QoS Scheduler** to enter the page.

On this page, you can configure the QoS scheduling mode and congestion control policies.

QoS Scheduler
802.1P
DSCP
Port Priority


QoS Mode Simple Weighted Priority ▼

Congestion Control

Egress Discard

Confirm

Parameter description

Name	Description
QoS Mode	<p>Specifies the scheduler mode for the port traffic.</p> <ul style="list-style-type: none"> – 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	<p>If the QoS Mode is set to Weighted Priority, you need to configure the weighted value for each queue.</p>
Egress Discard	<p>When this function is enabled, the switch disables the flow control function to meet the requirements of network clone in various environments.</p> <p> Tip</p> <p>This function applies to network clone scenario and is not recommended in common scenarios.</p>

6.4 802.1P

Navigate to **QoS Policy > 802.1P** to enter the page.

On this page, you can configure the mapping relationship of the 802.1P priority and queues.

QoS Scheduler
802.1P
DSCP
Port Priority

CoS Priority Setting

Priority0 ▼

Priority1 ▼

Priority2 ▼

Priority3 ▼

Priority4 ▼

Priority5 ▼

Priority6 ▼

Priority7 ▼

Parameter description

Name	Description
Priority 0	Specifies the queue in which the messages' priority is 0.
Priority 1	Specifies the queue in which the messages' priority is 1.
Priority 2	Specifies the queue in which the messages' priority is 2.
Priority 3	Specifies the queue in which the messages' priority is 3.
Priority 4	Specifies the queue in which the messages' priority is 4.
Priority 5	Specifies the queue in which the messages' priority is 5.
Priority 6	Specifies the queue in which the messages' priority is 6.
Priority 7	Specifies the queue in which the messages' priority is 7.

6.5 DSCP

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

Parameter description

Name	Description
DSCP	Specifies the priority level (range: 0 to 63) defined by DS field of the IP message heads.
Port Queue	Specifies the scheduler queue of the egress port.

6.6 Port priority

Navigate to **QoS Policy > Port Priority** to enter the page.

On this page, you can configure the application priority mode and Cos priority for the physical ports of the switch.

Port	CoS Priority	Trust Mode	Operation
1	0	Non-Trust	✎
2	0	Non-Trust	✎
3	0	Non-Trust	✎
4	0	Non-Trust	✎
5	0	Non-Trust	✎
6	0	Non-Trust	✎
7	0	Non-Trust	✎
8	0	Non-Trust	✎

Parameter description

Name	Description
Port	Specifies the ID of the port.
Cos Priority	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 rejoin queues based on the correspondence.
Trust Mode	<p>Specifies the method which the port uses to process the received messages.</p> <ul style="list-style-type: none"> – Non-Trust: All messages received by the port rejoin queues according to the correspondence of the configured Cos priority. – 802.1P Trust: When the port receives VLAN messages, the messages rejoin 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 rejoin 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

Access Control List (ACL) 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

Filtering 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.

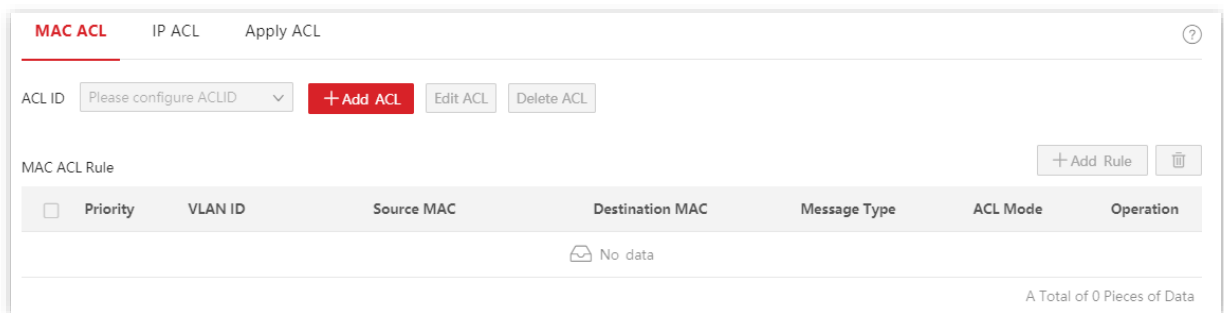
Filtering rules based on IP address

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

Navigate to **Network Security > ACL > MAC ACL** to enter the page.

On this page, you can view and configure the MAC ACL rules.



Parameter description

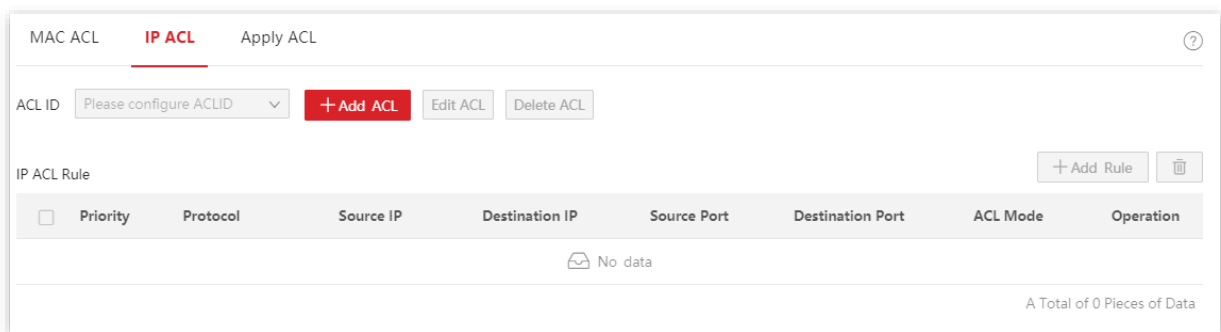
Name	Description
ACL ID	Specifies the ACL ID of the MAC ACL rule. You should add ACL ID here before configuring the MAC ACL rules.
Priority	Specifies the priority of a rule. A smaller value indicates a higher priority. The message starts matching from the rule with the highest priority. Once matched, the message stops checking rules.
VLAN ID	Specifies the VLAN to which the message belongs. If this field is not configured, it indicates messages of all VLANs.
Source MAC	Specifies the source MAC address of the message. <ul style="list-style-type: none"> Any MAC: Specifies all MAC addresses. Specified MAC: Combined with mask, it is used to specify a certain MAC address or MAC address segment.

Name	Description
Destination MAC	<p>Specifies the destination MAC address of the message.</p> <ul style="list-style-type: none"> – Any MAC: Specifies all MAC addresses. – Specified MAC: Combined with mask, it is used to specify a certain MAC address or MAC address segment.
Message Type	<p>Specifies the message type of the layer-2 data frame.</p> <p>If this field is not configured, it indicates any message type.</p>
ACL Mode	<p>Specifies the ACL mode in which the switch processes the messages that match the rule.</p> <ul style="list-style-type: none"> – Allow: Forwards the messages that match the rule. – Forbid: Discards the messages that match the rule.

7.1.4 IP ACL

Navigate to **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	Specifies the ACL ID of the IP ACL rule. You should add ACL ID here before configuring the IP ACL rules.
Priority	<p>Specifies the priority of the rule. A smaller value indicates a higher priority.</p> <p>The message starts matching from the rule with the highest priority. Once matched, the message stops checking rules.</p>
Protocol	Specifies the protocol type of the message, such as IP and ICMP. You can also enter the protocol number manually.

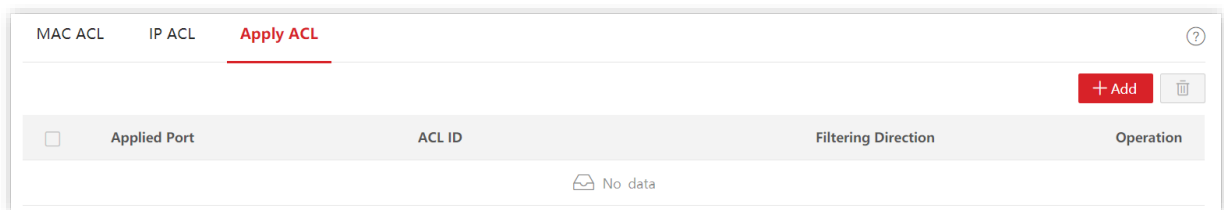
Name	Description
Source IP	<p>Specifies the source IP address of the message.</p> <ul style="list-style-type: none"> – Any IP: Specifies all IP addresses. – Specified IP: Combined with mask, it specifies a certain network address.
Destination IP	<p>Specifies the destination IP address of the message.</p> <ul style="list-style-type: none"> – Any IP: Specifies all IP addresses. – Specified IP: Combined with mask, it specifies a certain network address.
Source Port	<p>When the protocol type is TCP or UDP, enter the source port number of the message.</p>
Destination Port	<p>When the protocol type is TCP or UDP, enter the destination port number of the message.</p>
ACL Mode	<p>Specifies the ACL mode in which the switch processes the messages that match the rule.</p> <ul style="list-style-type: none"> – Allow: Forwards the messages that match the rule. – Forbid: Discards the messages that match the rule.

7.1.5 Apply ACL

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

Navigate to **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	Specifies the physical port number to which the ACL rule applies.
ACL ID	Specifies the ACL rule applied to the port.
Filtering Direction	Specifies the message filtering direction of the port. Only Ingress is supported by this switch.

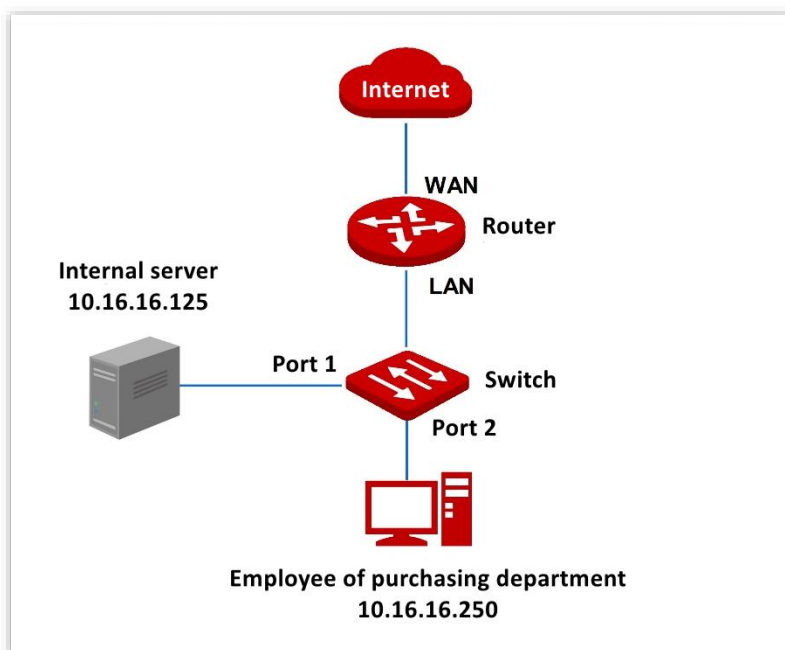
7.1.6 Example of ACL configuration

Network requirement

A certain employee of purchasing department is only allowed to access the internal server of the company, and forbidden to access the internet.

Solution

The IP ACL function of the switch can achieve the requirement. Assume that the IP address of the employee's computer is 10.16.16.250, and the IP address of the internal server is 10.16.16.125.

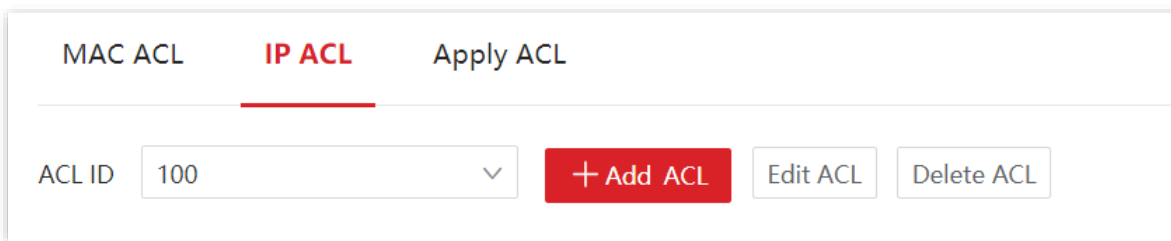


Configuration procedure

I. Add IP ACL rules

1. Log in to web UI of the switch, and navigate to **Network Security > ACL > IP ACL**.
2. Add ACL.

Click + **Add ACL** to add an ACL, which is ACL ID **100** in this example.

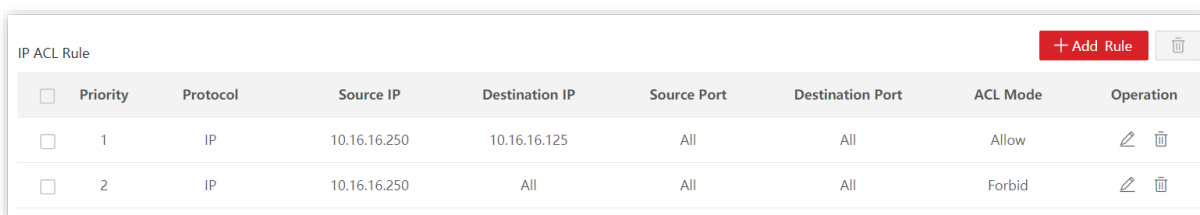


3. Add IP ACL rules

Click **+Add Rule** to add the following two IP ACL rules.

No.	ACL ID	Priority	Protocol	Source IP	Destination IP	ACL Mode
1	100	1	IP	10.16.16.250/32 (IP address of the employee's computer)	10.16.16.125/32 (IP address of the internal server)	Allow
2	100	2	IP	10.16.16.250/32 (IP address of the employee's computer)	Any IP	Forbid

The rules are added successfully. See the following figure.

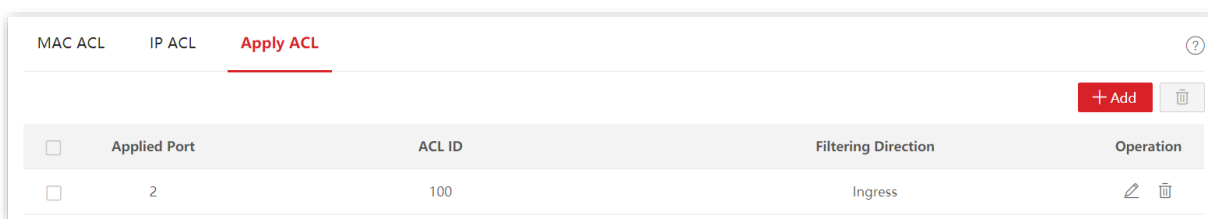


II. Apply ACL


1. Log in to the web UI of the switch, and navigate to **Network Security > ACL > Apply ACL**.
2. Click **+ Add** to apply an ACL.

Bind ACL	ACL ID	Filtering Direction	Applied Port
IP ACL	100	Ingress	Port 2

The IP ACL is applied successfully. See the following figure.



III. Save the configurations

Click  Save at the upper right corner to save the configurations.

----End

Verification

After the configuration, the employee of purchasing department can access the internal server of the company, and cannot access the internet.

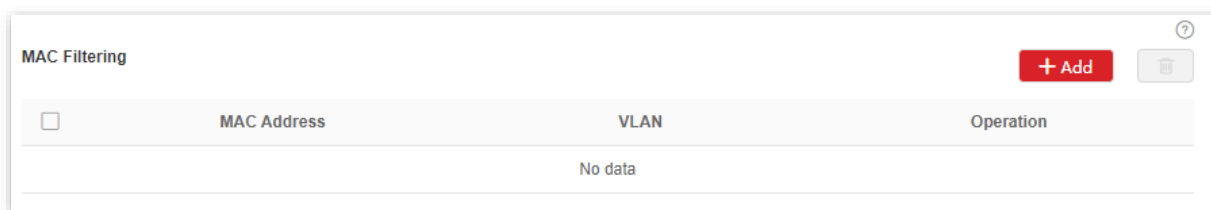
7.2 MAC filtering

With this function enabled, the switch can check 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.

Navigate to **Network Security > MAC Filtering** to enter the page.

On this page, you can configure the MAC filtering rules.



Parameter description

Name	Description
MAC Address	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 will be discarded.
VLAN	Specifies the VLAN in which the MAC filtering rule takes effect.

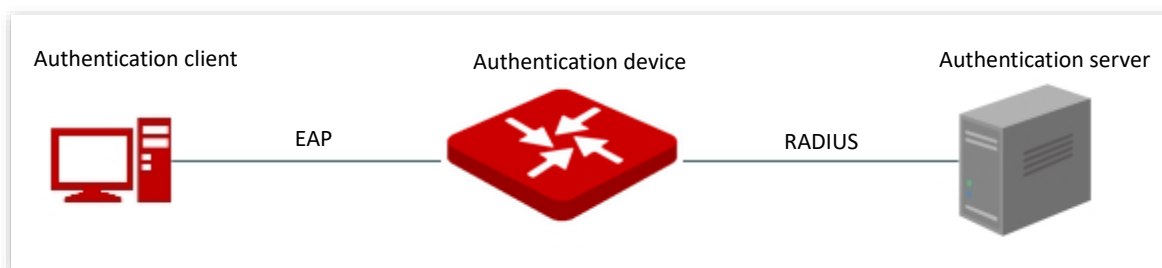
7.3 802.1X

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

Navigate to **Network Security > 802.1X > Global** to enter the page.

On this page, you can configure the parameters of 802.1X authentication server.

802.1X Authentication

Global Port Configuration

Authentication Server IP

Authorized Shared Key

Parameter description

Name	Description
Authentication Server IP	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	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


Navigate to **Network Security > 802.1X > Port Configuration** to enter the page.

On this page, you can configure the 802.1X authentication parameters for each port.

Port	Port Control Mode	Authentication Status	Re-authentication	Re-authentication Timeout	Client Timeout	Max Re-authentication Times	Operation
1	Disable	Non-authorized	Disable	3600	30	2	
2	Disable	Non-authorized	Disable	3600	30	2	
4	Disable	Non-authorized	Disable	3600	30	2	
5	Disable	Non-authorized	Disable	3600	30	2	
6	Disable	Non-authorized	Disable	3600	30	2	
7	Disable	Non-authorized	Disable	3600	30	2	
8	Disable	Non-authorized	Disable	3600	30	2	

Parameter description

Name	Description
Port	Specifies the ID of the port.
Port Control Mode	<p>Specifies the control mode of the port to access the network.</p> <ul style="list-style-type: none"> 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	<p>Specifies the authentication status of the port.</p> <ul style="list-style-type: none"> 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	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.

Name	Description
Re-authentication Timeout	<p>Specifies the interval at which the switch launches re-authentication to authentication clients.</p> <p>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.</p>
Client Timeout	<p>Specifies the timeout period in which the client responds to the re-authentication request.</p> <p>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.</p>
Max Re-authentication Times	<p>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.</p> <p> Note</p> <p>The number of authentication timeout is also considered as the failed re-authentication times. If the authentication timeout number of the client exceeds the max re-authentication times, the switch forces the client offline.</p>

7.4 Attack defense

7.4.1 Overview

The switch supports three attack defense methods: ARP Attack Defense, Denial of Service (DoS) 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

Navigate to **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	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

DoS 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.

Navigate to **Network Security > Attack Defense > DoS Attack Defense** to enter the page.

On this page, you can configure DoS Attack Defense rules.

ARP Attack Defense **DoS Attack Defense** MAC Address Attack Defense

- Detect whether inconsistencies exist between the ARP message Sender_MAC and L2_MAC.
- Detect whether the TCP messages are multicast or broadcast messages.
- Detect whether all flags of TCP messages are 0.
- Detect whether the FIN, URG, and PSH flags of the TCP message are all 1.
- Detect whether the SYN, FIN, and flags of the TCP message are all 1.
- Detect whether the SYN and RST flags of the TCP message are both 1.
- Detect whether the source port number or destination port number of the TCP and UDP message is 0.
- Detect whether the TCP SYN message contains data.
- ICMP message fragment detection

Confirm

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.

Name	Description
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 ICMP message fragment.

7.4.4 MAC address attack defense

Navigate to **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.

Port	MAC Discard	Operation
1	Disable	
2	Disable	
3	Disable	
4	Disable	
5	Disable	
6	Disable	

Parameter description

Name	Description
Port	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**

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 except software upgrade, reset or user management.

- **Common User**

A common user can check configuration of the switch.

Navigate to **Device Settings > User Management** to enter the page.

On this page, you can add users of this switch (8 users at most).

User Management				
<input type="checkbox"/>	User	User Type	Login Timeout	Operation
<input type="checkbox"/>	Admin	Administrator	300s	

Parameter description

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

Simple Network Management Protocol (SNMP) 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 ignore the physical differences among devices and realize automatic management for devices from different vendors.

SNMP management framework

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

- 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 functions on a certain network device.
- SNMP agent: Software which runs on managed devices for maintaining management information and reporting management data to an SNMP management system when 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 and CPU utilization, 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.

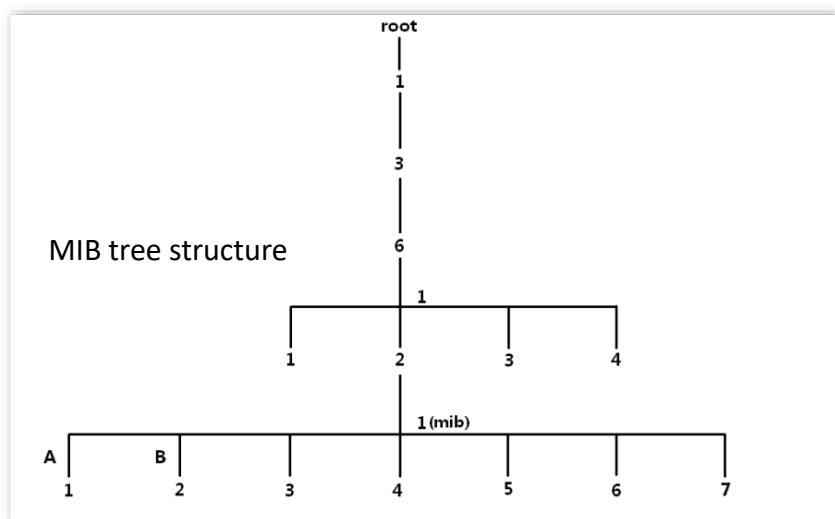
SNMP versions

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

SNMP 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 OIDs, 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, you can create SNMP groups. You can add **Read Only/Read & Write/Notification** view for each SNMP group to assign different access permissions to users in different 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.

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

8.2.3 Basic

Navigate to **Device Settings > SNMP > Basic** to enter the page.

On this page, you can configure the basic SNMP parameters.

SNMP

Basic Permission Control Notification

Contact Info (1 to 255 characters)

Location Info (1 to 255 characters)

Local Engine ID (10 to 64 hexadecimal characters)

Note: This device is compatible with SNMP v1/v2c/v3

Parameter description

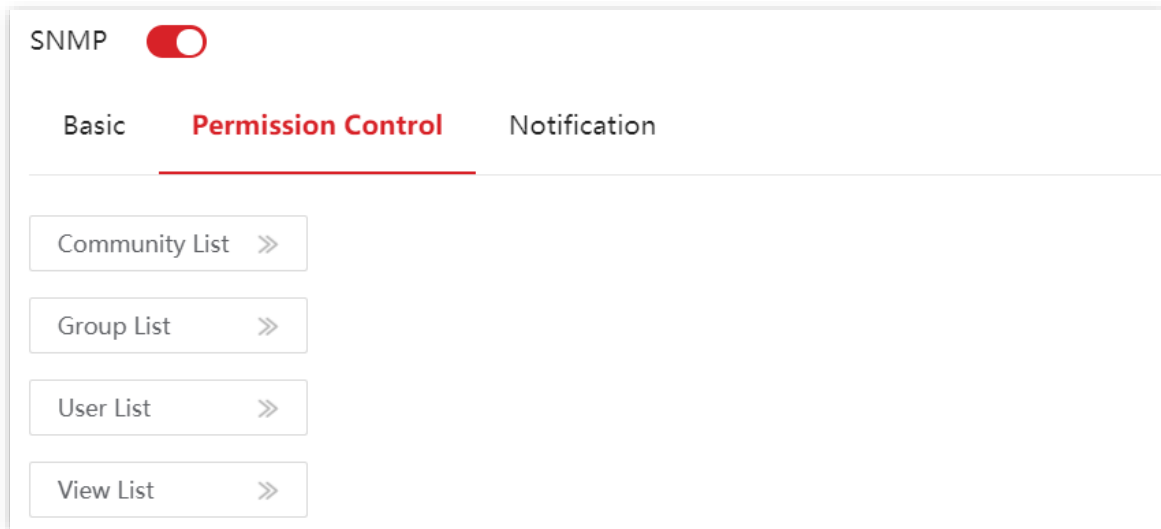
Name	Description
SNMP	Used to enable/disable the SNMP function.
Contact Info	Used to configure the contact info of the switch for the SNMP manager to fast locate this switch.
Location Info	Used to configure the location info of the switch for the SNMP manager to fast locate this switch.

Name	Description
Local Engine ID	Specifies the Local Engine ID of the switch. You need to enter this ID at the SNMP manager side to manage the switch.

8.2.4 Permission control

Navigate to **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	Specifies the name of a community.
	Access Rule	Specifies the access permission for the community to access the views, including Read Only and Read&Write .
	MIB View	Specifies the views that the community can access. The MIB view should be configured in View List in advance.
Group List	Group Name	Specifies the name of a group.
	Security Level	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.
	Read&Write	
Notification	The MIB view should be configured in View List in advance.	

Name	Description	
User Name	Specifies the name of the user.	
User Group	Specifies the group of the user. The group needs to be configured in Group List in advance.	
Security Level	Specifies the security level of the user. After the user's group is selected, the security level is filled in automatically.	
Authentication Mode	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 .	
User List	Authentication Password	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 .
	Security Mode	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	Specifies the security password of the user. This parameter can be set only if the security level of the group is Authentication&Privacy .
	View Name	Specifies the name of a view.
View List	Rule	Specifies the OID rule. – include : This OID can be managed by the SNMP. – exclude : This OID cannot be managed by the SNMP.
	MIB Subtree OID	Specifies the managed objects (represented by OID) of the view.

8.2.5 Notification

The notification function enables the switch to send messages to the SNMP manager and notify some important events (such as the device is restarting), so the manager can monitor and deal with the specific events of the switch with SNMP management software.

Navigate to **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	Used to enable/disable all trap.
Target Host IP	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	Specifies the community name, user name or group name required by authentication. 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	Specifies the UDP port enabled for Trap on the managed host.
Security Version	Used to select a security version used by Trap, including v1 , v2c and v3 , which should be consistent with the software 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](#).

Navigate to **Device Settings > System Time** to enter the page.

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 computer.

The screenshot shows the 'System Time' configuration interface. At the top, it displays 'System Time'. Below this, the 'Current Time' is shown as '2022-09-26 14:12:15'. There are two radio buttons: 'Local Time' (which is selected) and 'Internet Time'. Below the radio buttons, there are two input fields: 'Date' with the value '2022-09-26' and a calendar icon, and 'Time' with the value '14:11:18' and a clock icon. To the right of these fields is a button labeled 'Sync with Local Time'. At the bottom left, there is a red 'Confirm' button.

Internet calibration

The switch automatically synchronizes with the Internet time server. As long as the switch is connected to the Internet, it can automatically calibrate its system time. After the switch is restarted, it can also calibrate automatically.

The screenshot shows the 'System Time' configuration interface for Internet calibration. At the top, it displays 'System Time'. Below this, the 'Current Time' is shown as '2022-09-26 14:14:15'. There are two radio buttons: 'Local Time' and 'Internet Time' (which is selected). To the right of the 'Internet Time' radio button, there is a note: 'Time synchronization requires internet connection'. Below the radio buttons, there is a 'Time Zone' dropdown menu with the selected value '(GMT+08:00) Beijing, Chongqing, Hong Kong, ...'. At the bottom left, there is a red 'Confirm' button.

8.4 Log management

8.4.1 Log info

The logs of a switch record all situations 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.

By default, the switch saves the latest 2,000 logs. If the logs exceed the limit, the switch will clear the earlier logs.

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

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	6	Notification that needs to be recorded
debug	7	Message generated in debugging process

Navigate to **Device Settings > Log Management > Log Info**.

On this page, you can view, download and delete the log info of the switch.

ID	Generated Time	System Log	Log Level
1	2022/09/01 19:57:32	Interface sa1 up	Info
2	2022/09/01 19:57:32	Interface ge3 up	Info
3	2022/09/01 18:58:37	Interface sa1 down	Info
4	2022/09/01 18:58:37	Interface ge3 down	Info
5	2022/09/01 18:28:05	Interface sa1 up	Info

Parameter description

Name	Description
Log Level	Used to filter which logs are displayed by log level.
ID	Specifies the log ID.
Generated Time	Specifies the time point when the log is generated.
System Log	Displays the content of the log.
Log Level	Specifies the level of the log.

8.4.2 Server settings

Navigate to **Device Settings > Log Management > Server Settings**.

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	Used to enable/disable the log server.
Log Level	Logs of this level and above will be uploaded to the server.
Server IP Address	Specifies the IP address of the log server. Ensure that there are reachable routes between the log server and this switch.
Port	Specifies the port number used by the log server.

8.5 Time period

Time Period is used to configure the specified date, cycle and time period to control the specified time periods during which the PoE function takes effect.

Navigate to **Device Settings > Time Period** to enter the page.

On this page, you can configure the time according to actual situations.

Time Period ID	Date	Cycle	Time Period	Operation
1	2022-09-26 00:00~2022-10-31 23:59	Mon. ~ Sun.	00:00-23:59	

Parameter description

Name	Description
Time Period ID	Specifies the ID of the time period.
Date	Used to specify the start and end dates.
Cycle	Used to specify the days of the cycle.
Time Period	Used to specify the period of time, and a maximum of 3 time periods are allowed.

Note

- If you configured only one of **Date**, **Cycle**, and **Time Period**, only the configured parameter is effective. If you configured two or three of the parameters, the overlap time is effective.
- If you configured only the **Time Period**, the configured time period is effective every day by default.
- If you configured only the **Cycle**, such as Mon., but did **NOT** configure the **Time Period**, all the 24 hours every Mon. are effective.

8.6 RMON

8.6.1 Overview

Remote Network Monitoring (RMON), based on SNMP, is a standard monitoring specification developed by Internet Engineering Task Force (IETF) that enables network administrators to detect network issues such as dropped packets, network collisions and traffic congestion. Through RMON MIB, network administrators can monitor remote network devices efficiently by analyzing the historical data. RMON reduces traffic flow between the NMS and managed devices, which is convenient to manage large networks.

RMON mechanism

RMON includes two parts: the NMS and the Agents running on every network device. The switch is a RMON Agent.

The Agents collect and save traffic statistics in the RMON MIB. The switch is embedded with the agents function to probe.

Based on SNMP protocol, the NMS collects network data by communicating with Agents.

RMON group

The switch supports RMONv1 that defines multiple RMON groups. The switch implements statistics group, history group, alarm group and event group supported by the public MIB.

■ Statistics

The statistics group defines that the system collects various traffic statistics on an Ethernet interface, and saves the statistics in the Ethernet statistics table for future retrieval. The interface traffic statistics include network collisions, CRC alignment errors, undersize/oversize packets, broadcasts, multicasts, bytes received, and packets received.

After you create a statistics entry for an interface, the statistics group starts to collect traffic statistics on the interface. The statistics in the Ethernet statistics table are cumulative sums.

■ History

The history group defines that the system periodically collects traffic statistics on interfaces and saves the statistics in the history record table. The statistics include dropped events, bytes received, unicasts, broadcasts, multicasts, CRC alignment errors, undersize/oversize packets, and conflict packets.

The history statistics table record traffic statistics collected for each sampling interval. The sampling interval is user-configurable.

■ Alarm

The alarm group monitors alarm variables, such as the count of incoming packets on an interface. After you define an alarm entry, the system gets the value of the monitored alarm variable at the specified interval. If the value of the monitored variable is greater than or equal to the rising threshold, a rising event is triggered. If the value of the monitored variable is smaller than or equal to the falling threshold, a falling event is triggered. The event is handled as defined in the event group.

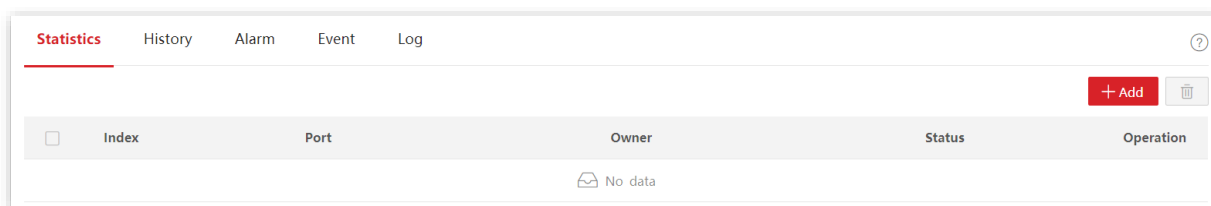
■ Event

The event group defines event indexes and controls the generation and notifications of the events triggered by the alarms defined in the alarm group. The events can be handled in two ways: Log and Trap.

8.6.2 Statistics

Navigate to **Device Settings > RMON > Statistics** to enter the page.

On this page, you can configure the RMON statistics group.



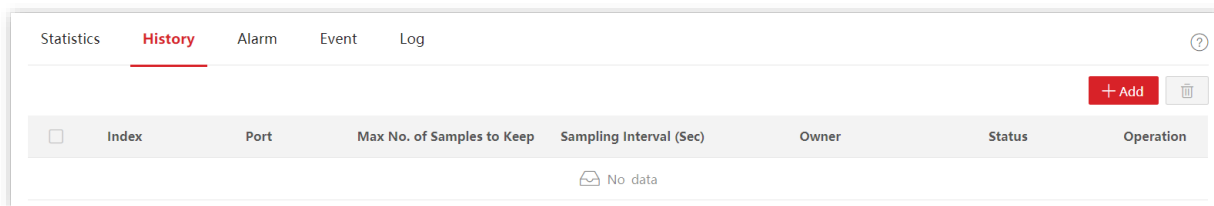
Parameter description

Name	Description
Index	Specifies the index number of statistics entry.
Port	Used to choose a port for which the statistics entry is to be displayed. Each port corresponds to only one statistics entry.
Owner	Specifies the owner of the entry.
Status	Specifies the status of statistics entry, active or inactive.

8.6.3 History

Navigate to **Device Settings > RMON > History** to enter the page.

On this page, you can configure the RMON history group.



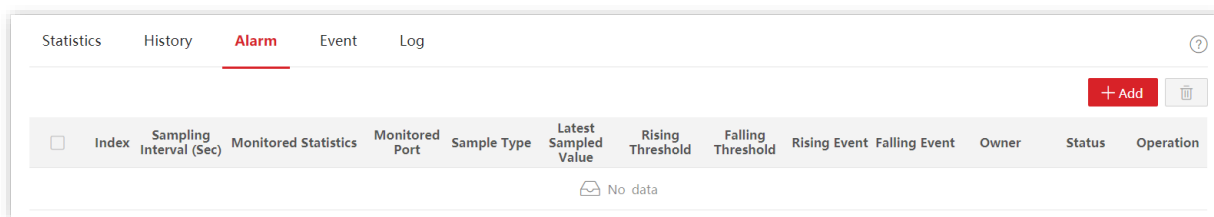
Parameter description

Name	Description
Index	Specifies the index number of history entry.
Port	Used to choose a port for which the history entry is to be displayed.
Max No. of Samples to Keep	Used to set the capacity of the history table. When the samples reach the maximum, the system will delete earlier records to save new samples.
Sampling Interval (Sec)	Specifies the time in seconds that samples are collected from the ports.
Owner	Specifies the owner of the entry.
Status	Specifies the status of the history entry, active or inactive .

8.6.4 Alarm

Navigate to **Device Settings > RMON > Alarm** to enter the page.

On this page, you can configure the RMON alarm group.



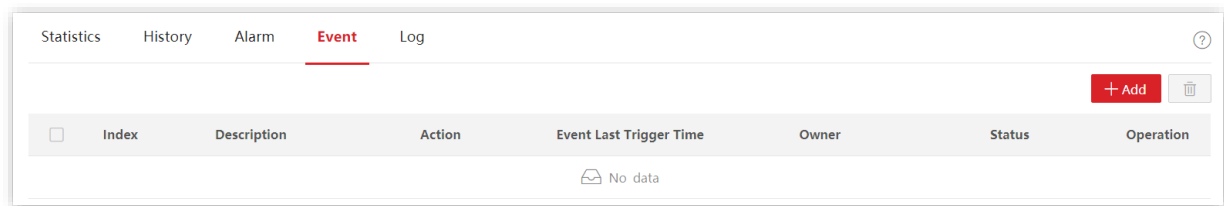
Parameter description

Name	Description
Index	Specifies the index number of alarm entry.
Sampling Interval (Sec)	Specifies the time in seconds that samples are collected from the ports.
Monitored Statistics	Specifies the traffic statistics to be collected and monitored.
Monitored Port	Specifies the port whose traffic statistics are collected and monitored.
Sample Type	Specifies the sampling method to generate an alarm - Absolute or Delta. <ul style="list-style-type: none"> - Absolute: The switch compares the sampling value against the preset rising and falling thresholds. - Delta: The switch obtains the difference between the sampling values of the current interval and the previous interval, and then compares the difference against the preset rising and falling thresholds.
Latest Sampled Value	Specifies the most recent sampled value.
Rising Threshold	Specifies the alarm rising threshold.
Falling Threshold	Specifies the alarm falling threshold.
Rising Event	Used to set the action that the system takes when the value of the alarm variable is higher than the alarm rising threshold.
Falling Event	Used to set the action that the system takes when the value of the alarm variable is lower than the alarm falling threshold.
Owner	Specifies the owner of the entry.
Status	Specifies the status of the alarm entry, active or inactive .

8.6.5 Event

Navigate to **Device Settings > RMON > Event** to enter the page.

On this page, you can configure the RMON event group.



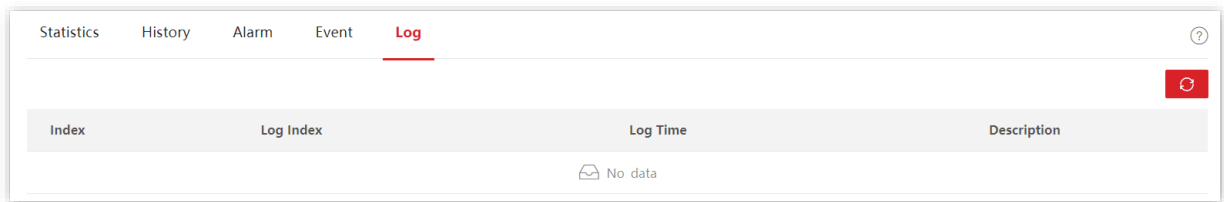
Parameter description

Name	Description
Index	Specifies the index number of event entry.
Description	Specifies the description of the event.
Action	<p>Specifies the action to be executed when an event is triggered.</p> <ul style="list-style-type: none"> - Log: The switch logs event information (including event time and description) in the event log table so the management device can get the logs through SNMP. - Trap: The switch sends an SNMP notification to the NMS.
Event Last Trigger Time	Specifies the most recent time of a triggered event.
Owner	Specifies the owner of the entry.
Status	Specifies the status of the event entry, active or inactive .

8.6.6 Log

Navigate to **Device Settings > RMON > Log** to enter the page.

On this page, you can view the generated logs about the triggered events of RMON.



Parameter description

Name	Description
Index	Specifies the index number of event entry.
Log Index	Specifies the serial number of the log.
Log Time	Specifies the generation time of log information.
Description	Specifies the description of the event.

9 Visualization

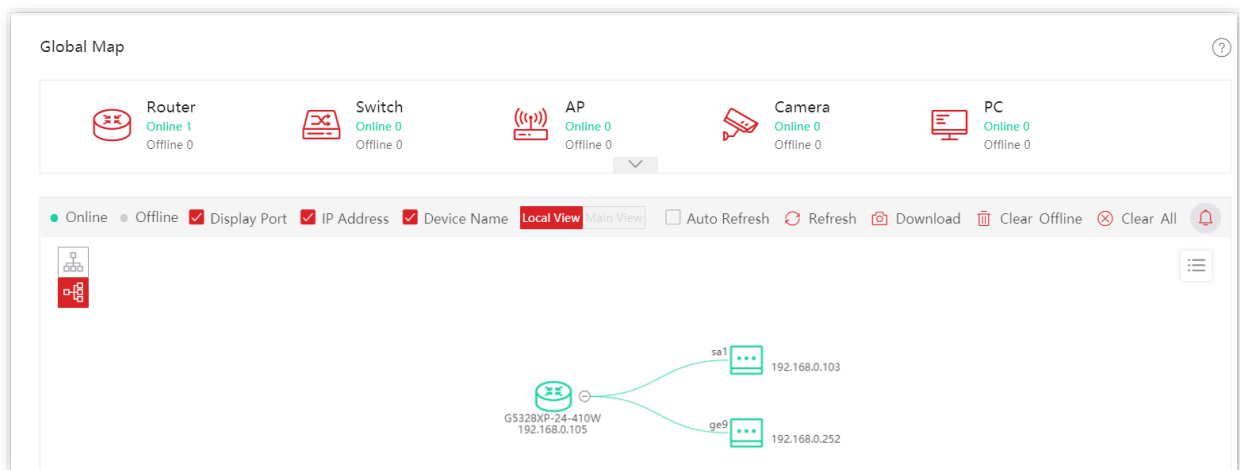
For networks with no need for internet access (such as medium and large security monitoring networks), cloud management is unavailable. Visualization function of this switch provides central management and maintenance for these networks.

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


Navigate to **Visualization > Global Map** to enter the page.

On this page, you can view and configure the basic parameters of the switch and devices connected to this switch.




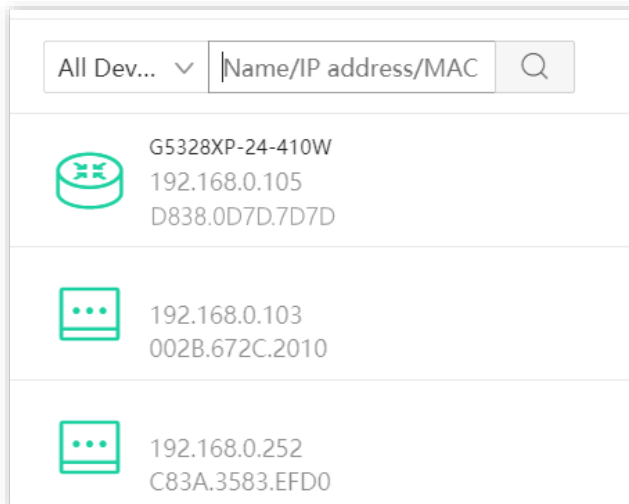
Parameter description




Name	Description
Global Map	Displays all kinds of online and offline devices in the LAN network.
<input checked="" type="radio"/> Online <input type="radio"/> Offline	On the topology, green device icons stand for online devices while grey for offline devices.
<input checked="" type="checkbox"/> 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.
<input checked="" type="checkbox"/> IP Address	With these functions enabled, the IP addresses and device names of devices are displayed on the topology.
<input checked="" type="checkbox"/> Device Name	
Local View/Main View	<p>Specifies the topological view of the current network.</p> <ul style="list-style-type: none"> - Local View: Specifies the topology with this device as the root node. - Main View: Specifies the topology with the main device as the root node. <p> Tip</p> <ul style="list-style-type: none"> - When there is only one main device which is not this device in the topology, you can switch to the main view. - Main device is the core switching device in the network. You can customize it.
<input type="checkbox"/> Auto Refresh	With this function enabled, the network topology is refreshed automatically. Auto refresh cycle: 10 minutes.
 Refresh	Used to refresh the network topology manually.
 Download	Used to download and save the topology in PNG format locally.
 Clear Offline	Used to clear the offline devices in the topology while removing all configuration of these devices in the Visualization section.
 Clear All	Used to clear all devices in the topology and regenerate a topology.
	Used to view the loop alert messages of the topology. The alert messages automatically refresh every 30 s.
	Click  to expand the topology vertically.
	Click  to expand the topology horizontally.

Name	Description
	Zoom in/out the topology. You can also scroll the mouse wheel to achieve this.

■ Search a device

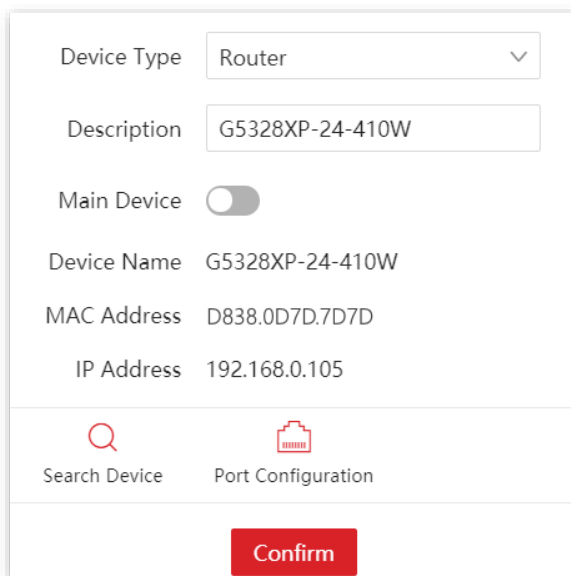
If you want to search a device, click . Then you can search the device by filtering the device type or directly entering the device name/IP address/MAC address in the search bar. Click the icon of the device, and you can be directed to the location of this device on the network topology.





Device Type	Name	IP Address	MAC Address
	G5328XP-24-410W	192.168.0.105	D838.0D7D.7D7D
	192.168.0.103	002B.672C.2010	
	192.168.0.252	C83A.3583.EFD0	


■ View & modify parameters

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

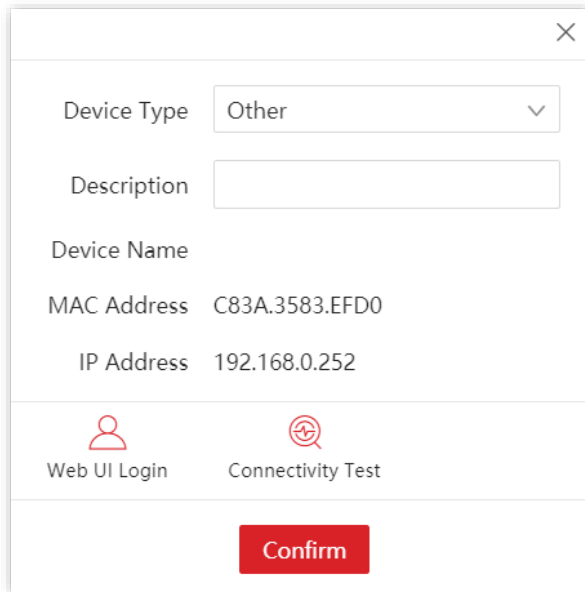


Device Type	Router
Description	G5328XP-24-410W
Main Device	<input type="checkbox"/>
Device Name	G5328XP-24-410W
MAC Address	D838.0D7D.7D7D
IP Address	192.168.0.105
	
Search Device	Port Configuration
Confirm	

 : Used to refresh the network topology.

 : Used to enable/disable each port.



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




A screenshot of a device configuration dialog box. The dialog has a close button (X) in the top right corner. It contains the following fields and options:


- Device Type:** A dropdown menu with "Other" selected.
- Description:** An empty text input field.
- Device Name:** A label with no input field.
- MAC Address:** C83A.3583.EFD0
- IP Address:** 192.168.0.252

At the bottom, there are two icons with labels:

-  Web UI Login
-  Connectivity Test

A red "Confirm" button is located at the bottom center of the dialog.

 : Used to enter the web UI of the device.
Web UI Login

 : Used to test the connectivity of the device.
Connectivity Test

9.2 Device list

Navigate to **Visualization > Device List** to enter the page.

On this page, you can view and modify the basic information of all devices.

<input type="checkbox"/>	Device Name	Device Type	Device Model	Device Status	MAC Address	IP Address	Operation
<input type="checkbox"/>	G5328XP-24-410W	Router	G5328XP-24-410W	Online	D838.0D7D.7D7D	192.168.0.105	
<input type="checkbox"/>		Other		Online	002B.672C.2010	192.168.0.103	
<input type="checkbox"/>		Other		Online	C83A.3583.EFD0	192.168.0.252	

Parameter description

Name	Description
	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.
Device Name	Tip The device name modified here is only displayed on the Visualization section, and the corresponding field in the protocol message will not be changed.
	Specifies the type of the device. You can click to modify the device type.
Device Type	Tip The device type modified here is only displayed on the Visualization section, and the corresponding field in the protocol message will not be changed.
Device Model	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	Specifies the online/offline status of the device.
MAC Address	Specifies the MAC address of the device.
IP Address	Specifies the IP address of the device.

10 PoE management

10.1 Overview

Power over Ethernet (PoE, also known as remote Power supply) refers to the power supply of the device through external connection of the Ethernet cable to the Powered Device (PD), such as IP phone, wireless AP, network camera.

The advantages of PoE power supply are shown as below:

- Convenient connection: Network terminal only needs an Ethernet cable instead of external power supply.
- Stability: PD supports PoE power and can be connected to other power supply to realize redundancy power supply.
- Standard: It complies with IEEE 802.3af and IEEE 802.3at standards, with globally unified power interface.
- Wide application: It can be used for IP phone, wireless Access Point (AP), portable device charger, card reader, webcam, data acquisition, and so on.

All 1-24 ports of this switch support PoE function, can automatically detect PD, and supply power for PD conforming to IEEE 802.3af and IEEE 802.3at standards. Due to the limited power of the system and each port, some configurations must be made for the switch to ensure the proper power for each PD and to make full use of the system power.

10.2 Global

Navigate to **PoE management > Global** to enter the page.

On this page, you can check the power supply information and configure the power management mode.

The screenshot shows a web interface for PoE management. At the top, there are two tabs: 'Global' (selected) and 'Port Configuration'. Below the tabs, there are four rows of configuration items:

- Power Mode:** A dropdown menu currently showing 'Dynamic Allocation'.
- Total Available Power:** 370W
- Total Remaining Power:** 370W
- PoE Chip Temperature:** 52.75°C

A red 'Confirm' button is positioned at the bottom center of the configuration area.

Parameter description

Name	Description
Power Mode	<p>Used to select a power mode for PoE power supply of the switch.</p> <ul style="list-style-type: none"> – Static Allocation: It allows you to configure a power for each port of the switch. When the switch supplies PoE power, the configured power will be compulsorily reserved to this port, and cannot be used by other ports. – Dynamic Allocation: The switch allocates power based on the power consumed by each port. When reaching the full load, the switch allocates power based on the configured port priority (priority + port number). If the priorities are the same, the port with the smaller port number has a higher priority.
Total Available Power	Specifies the maximum power supported by the switch.
Total Remaining Power	Specifies the remaining power of the switch.
PoE Chip Temperature	Specifies the temperature of the PoE chip.

10.3 Port configuration

Navigate to **PoE Management > Port Configuration** to enter the page.

On this page, you can configure the PoE parameters of the ports of this switch.

Port	Enable PoE	Power Standard	Transmitted Power	PD Level	Priority	Static Allocation Power	Time Period ID	Operation
1	Enable	AT	0.00W	--	Low	30.0W	--	
2	Enable	AT	0.00W	--	Low	30.0W	--	
3	Enable	AT	0.00W	--	Low	30.0W	--	
4	Enable	AT	0.00W	--	Low	30.0W	--	
5	Enable	AT	0.00W	--	Low	30.0W	--	
6	Enable	AT	0.00W	--	Low	30.0W	--	
7	Enable	AT	0.00W	--	Low	30.0W	--	
8	Enable	AT	0.00W	--	Low	30.0W	--	

Parameter description

Name	Description
Port	Specifies the port number.
Enable PoE	<p>Specifies the PoE power supply status of the port.</p> <ul style="list-style-type: none"> – Enable: The PoE power supply function of the port is enabled. – Disabled: The PoE power supply function of the port is disabled. – No Change: The PoE power supply status of the port keeps unchanged.
Power Standard	Specifies the power supply standard of the ports: AT (IEEE 802.3at) or AF (IEEE 802.3af). The maximum power of each port under the AT standard is 30 W while that under the AF standard is 15.4 W.
Transmitted Power	Specifies the real-time PoE power of the port.
PD Level	Specifies the level of the PoE-powered device connected to the current port when the power supply is normal. The switch automatically obtains the device level.

Name	Description
Priority	<p>Ports with priorities only take effect in dynamic mode, including Low, Medium and High.</p> <p>Specifies the priority of the current port, which takes effect only when the Power Mode is set to Dynamic Allocation. A reasonable port priority ensures that specified ports can still supply power properly under the full load state. Among ports with different priorities, ports with higher priorities should be guaranteed the required power first. Among ports with a same priority, ports with smaller IDs should be guaranteed the required power first.</p>
Static Allocation Power	<p>Specifies the static allocation power of the current port, which takes effect only when the Power Mode is set to Static Allocation.</p>
Time period ID	<p>Specifies the enabled period of the PoE function for the port, which needs to be set in the Time period section. "--" indicates that the port is not assigned with the time period, and the PoE power is enabled all the time.</p>

Appendix

Acronyms and Abbreviations

Acronym or Abbreviation	Full Spelling
ACL	Access Control List
AES	Advanced Encryption Standard
AP	Access Point
ARP	Address Resolution Protocol
BPDU	Bridge Protocol Data Unit
CIST	Common and Internal Spanning Tree
CPU	Central Processing Unit
CRC	Cyclic Redundancy Check
CST	Common Spanning Tree
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DoS	Denial of Service
DS	Differentiated Services
DSCP	Differentiated Services Codepoint
EAP	Extensible Authentication Protocol
FDX	Full Duplex

Acronym or Abbreviation	Full Spelling
FTP	File Transfer Protocol
HDX	Half Duplex
ICMP	Internet Control Message Protocol
IEEE	Institute of Electrical and Electronics Engineers
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IP	Internet Protocol
IST	Internal Spanning Tree
LACP	Link Aggregation Control Protocol
LAN	Local Area Network
LLDP	Link Layer Discovery Protocol
LLDPDU	Link Layer Discovery Protocol Data Unit
MAC	Medium Access Control
MD5	Message Digest Algorithm
MDI	Medium Dependent Interface
MED	Media Endpoint Discovery
MIB	Management Information Base
MST	Multi Spanning Tree
MSTI	Multiple Spanning Tree Instance
MSTP	Multi Spanning Tree Protocol
NMS	Network Management System
OID	Object Identifier
PD	Powered Device

Acronym or Abbreviation	Full Spelling
PoE	Power over Ethernet
PVID	Port-based VLAN ID
QoS	Quality of Service
RADIUS	Remote Authentication Dial In User Service
RMON	Remote Monitoring
RSTP	Rapid Spanning Tree Protocol
SN	Serial Number
SNMP	Simple Network Management Protocol
STP	Spanning Tree Protocol
SYN	Synchronize Sequence Numbers
TPID	Tag Protocol Identifier
TCI	Tag Control Information
TCP	Transmission Control Protocol
TLV	Type-Length-Value
ToS	Type of Service
TPID	Tag Protocol Identifier
TTL	Time to Live
UDP	User Datagram Protocol
UI	User Interface
UPnP	Universal Plug and Play
VID	VLAN Identifier
VLAN	Virtual Local Area Network
VoD	Video on Demand

Acronym or Abbreviation	Full Spelling
VoIP	Voice over IP
