Lysora

LS Series Switches

Lysora 2.400 Configuration Guide

Document version: V1.0
Date: December 19, 2025

Copyright

Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms. Availability may vary by jurisdiction or contract, and some or all of the products, services, or features described in this document may not be available for you to purchase or use. **Except as expressly provided in a written agreement between you and Lysora Technology Inc.**, **all representations and warranties**, **regarding the content of this document**, **to the maximum extent permitted by applicable law** — **including implied warranties of merchantability**, **fitness for a particular purpose**, **and non-infringement**—**are hereby disclaimed**.

The names, links, descriptions, screenshots, and any other information regarding third-party software mentioned in this document are provided for informational purposes only. **Lysora Technology Inc. does not endorse**, **recommend, guarantee**, **or assume liability for such third-party software's functionality**, **security**, **legality**, **accuracy**, **or fitness**. You are solely responsible for: (a) evaluating and selecting any third-party software based on your specific business requirements; (b) ensuring you have obtained all necessary licenses and authorizations for its use; and (c) assuming all risks associated with its use. **Lysora Technology Inc. shall have no liability for any claims or damages arising from your use of or reliance upon any third-party software**.

Lysora Technology Inc. reserves the right, at its sole discretion and without prior notice, to modify the content of this document at any time. These modifications may occur due to product updates, corrections, regulatory changes, or other reasons. **Lysora Technology Inc. undertakes no obligation to update or notify users of changes to this document**.

This document is provided “AS IS” and for general informational and guidance purposes only. While Lysora Technology Inc. strives to ensure the accuracy and reliability of the content at the time of publication, **it makes no warranty**, **express or implied**, **that the content is error-free**, **complete**, **or current**. All information contained herein is provided without any warranty of merchantability, fitness for a particular purpose, or non-infringement. **You assume all risk for the use or application of this information**. For regulatory compliance queries (e.g., FCC/CPSC standards), please contact our support channel.

Preface

Intended Audience

This document is intended for:

- Network engineers
- Technical support and servicing engineers
- Network administrators

Technical Support

- Official website: https://help.lysoratech.com/
- Technical support email: support@lysoratech.com

Conventions

1. UI Conventions

UI Convention	Description	Example
Boldface	The interactive UI elements are in **boldface**, including buttons, tabs, menus, and so on.	(1) Click **OK**. (2) Select **Config Wizard**. (3) Click the **Clients** tab.
>	The ">" symbol indicates a hierarchical relationship or a path to a specific item.	Select **System** > **Time**.

2. Symbols

The symbols that may be found in this document are described as follows:

Warning

An alert that calls attention to important information which, if not understood or followed, can result in data loss or equipment damage.

⚠️ Caution

An alert that calls attention to essential information which, if not understood or followed, can result in function failure or performance degradation.

ℹ️ Note

An alert that contains additional or supplementary information.

✅ Specification

An alert that contains a description of product or version support.

3. Notes

This document provides configuration details (including model, description, port type, and software interface) of the expected version for reference purposes only. In the event of any discrepancy or inconsistency between the expected version and the actual version, the actual version shall take precedence.

Contents

1 Change Description

This chapter describes the major changes in software and hardware of different versions and related documentation. For details about hardware changes, see the release notes published with software versions.

Lysora 2.400

1.1.1 Hardware Change

The following table lists the applicable hardware models of this version.

Model	Hardware Version
LS2-24GT4SFP-P	1.xx

1.1.2 Software Feature Change

This is the first official release.

2 Login

2.1 Configuration Environment Requirements

- Google Chrome, Internet Explorer 9.0, 10.0, and 11.0, and some Chromium/Internet Explorer kernel-based browsers (such as 360 Extreme Explorer) are supported. Exceptions such as garble characters or format error may occur if an unsupported browser is used.
- 1024 x 768 or a higher resolution is recommended. If other resolutions are used, the page fonts and formats may not be aligned, the GUI is less artistic, or other exceptions may occur.

2.2 Logging in to the Web Page

2.2.1 Connecting to the Device

Use a network cable to connect the switch port to the network port of the PC, and configure an IP address for the PC that is on the same network segment as the default IP of the device to ensure that the PC can ping through the switch. For example, set the IP address of the PC to 10.100.111.100.

Table 2-1 Default settings

Feature	Default Value
Device IP Address	10.100.111.200
Password	A username is not required when you log in for the first time. The default password is admin.

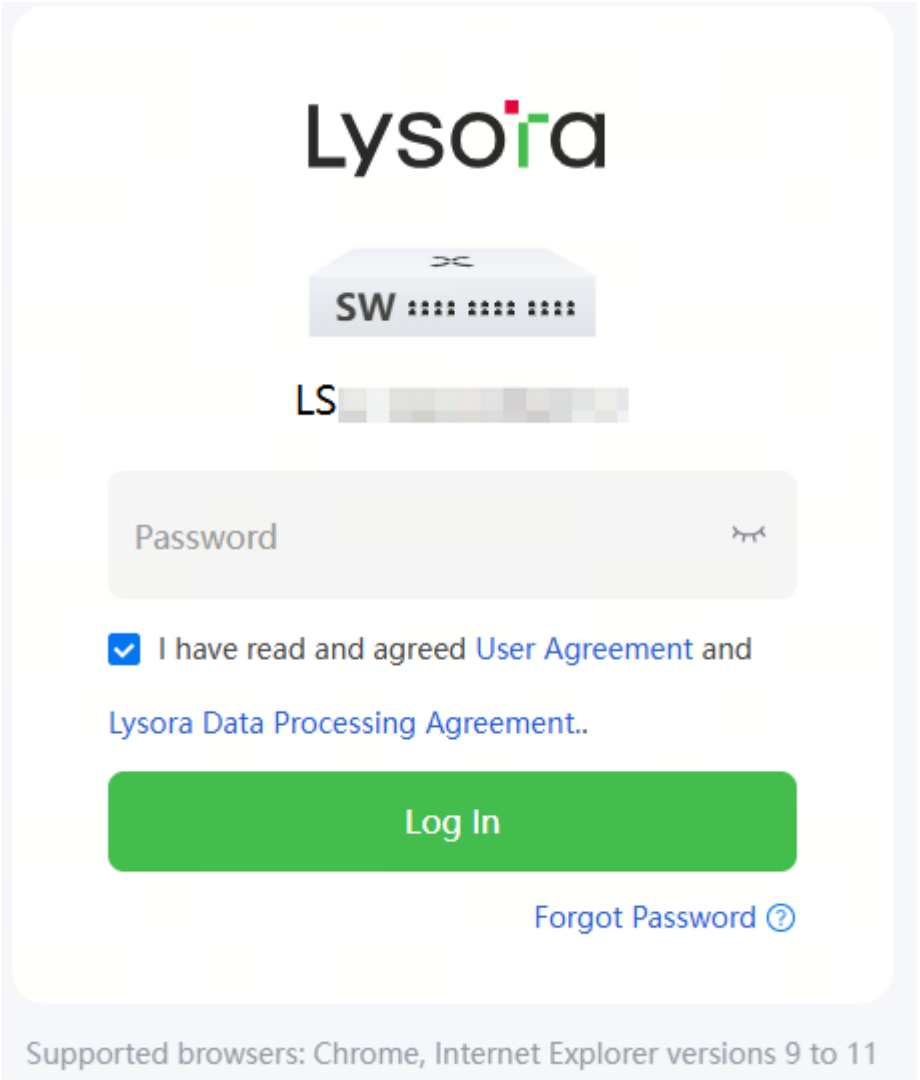
2.2.2 Logging in to the Web Page

(1) Enter the IP address (10.100.111.200 by default) of the device in the address bar of the browser to open the login page.

Note

- If the static IP address of the device is changed, or the device dynamically obtains a new IP address, the new IP address can be used to access the Web page of the device as long as the PC and the device are on the same LAN, and their IP addresses are in the same network segment.
- The login page varies with products. The actual login page prevails.

(2) Enter the password and click **Log In** to open the homepage of the web page.



You can use the default password admin to log in to the device for the first time. For security purposes, you are advised to change the default password as soon as possible after logging in, and to regularly update your password thereafter.

If you forget the Device IP address or password, hold down the **Reset** button on the device panel for more than 5s when the device is connected to the power supply to restore factory settings. After restoration, you can use the default IP address and password to log in.

Caution

- Restoring factory settings will delete all configurations of the device. Therefore, exercise caution when performing this operation.
- The method for restoring factory settings varies with the device model. For details, see the installation guide of the device.

2.2.3 Layout Configuration

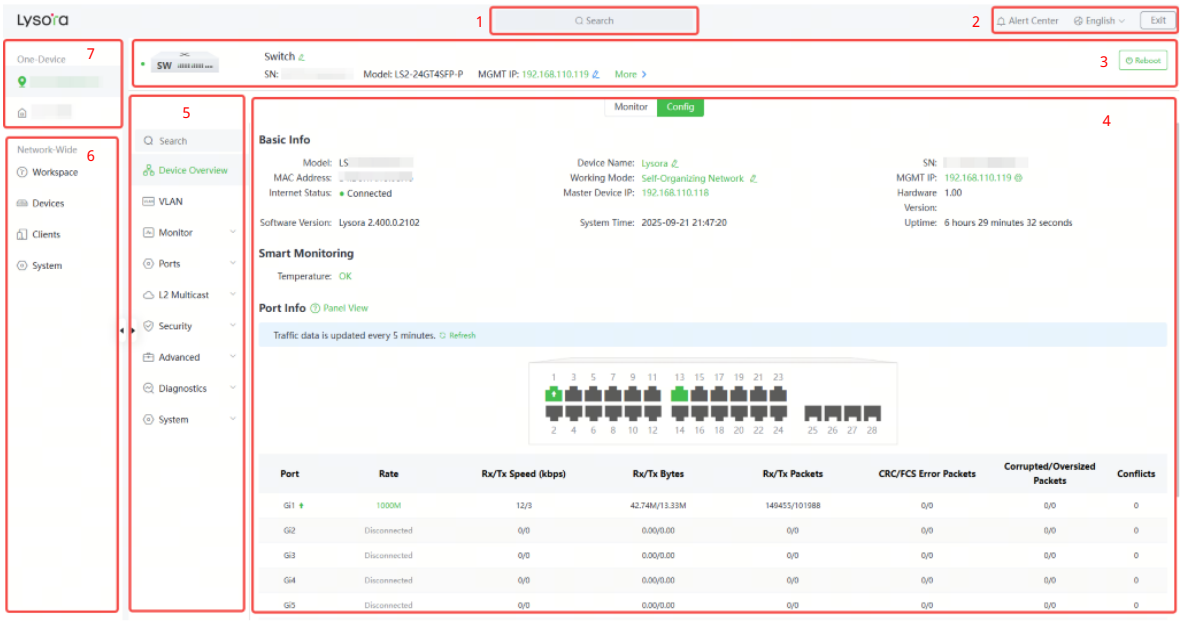


Table 2-2 Layout Configuration

No.	Description
1	Navigation of frequently used device functions, including Network, Gateway, and Device & System related functionalities
2	Quick view of device alarms, change web page language, and exit web
3	Device information and device restart button

No.	Description
4	Device function configuration and display area. Click **Monitor** to display the interface traffic and PoE power usage of the device (only PoE switches with model names containing –P, -LP, -HP, and -UP support this function). Click **Config** to view the device's configuration and operational status
5	The navigation bar
6	Bulk settings can be applied to commonly used functions of all wired and wireless Lysora products within the self-organizing network.
7	It allows for the configuration of all functions of the local device, as well as rapid setup of the Gateway

2.3 Quick Setup

2.3.1 Configuration Preparations

Connect the device to the power supply, and connect the device port to an uplink device with a network cable.

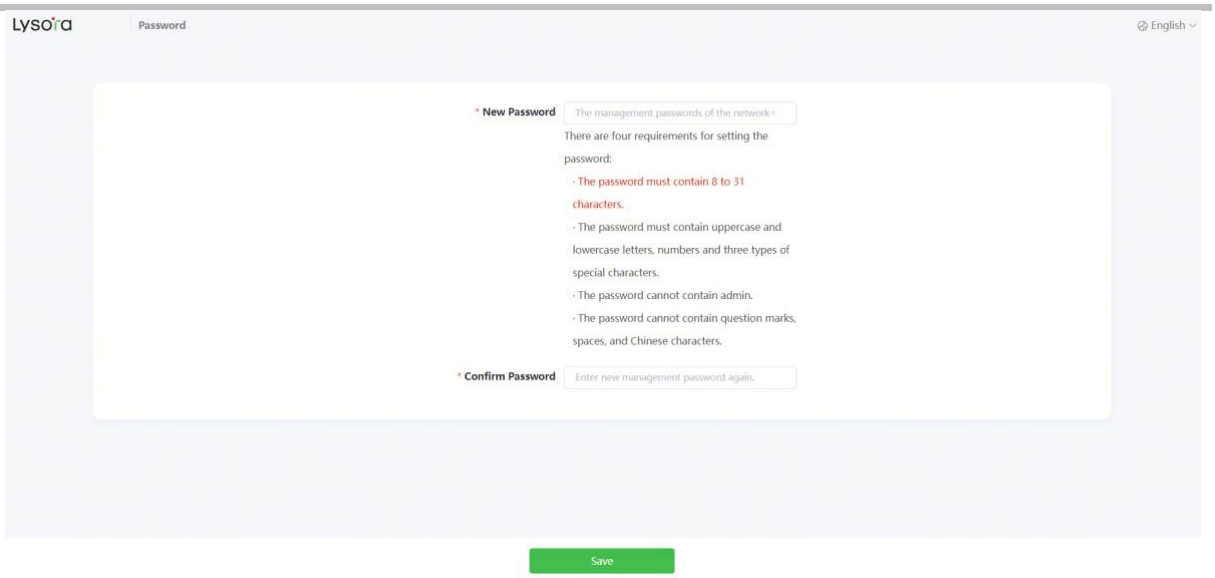
2.3.2 Procedure

1. Configuring the Management Password

Specification

You need to reset the management password after logging in to the management page for the first time.

Set a password for logging into the management system and click **Save**.



Note

- The management password is used to log in to web of the device. Please remember it. If you forget the device management password, hold and press the Reset button on the device for more than 5 seconds to restore factory settings. After restoration, all configurations will be reset. Exercise caution when performing this operation.
- After the configuration, all devices on the network have the same management password.

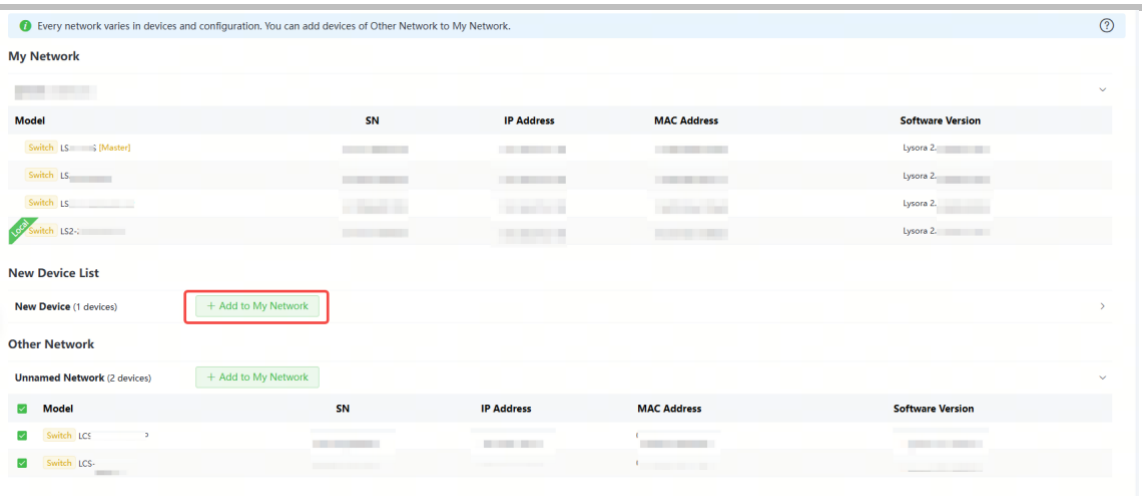
2. Adding Devices to the Network

By default, users can perform batch settings and centralized management of all devices in the network. Therefore, before starting configuration, you need to check and confirm the number of online devices and network status in the network.

Note

Under normal circumstances, when multiple new devices are powered on and connected, they will be automatically interconnected into a network, and the user only needs to confirm that the number of devices is correct.

If a new device is detected not in the network, select the device, click **Add to My Network** and enter its management password to add the device manually. This will incorporate the respective devices into the appropriate network, allowing you to proceed with the network-wide configuration.



3. Creating a Network Project

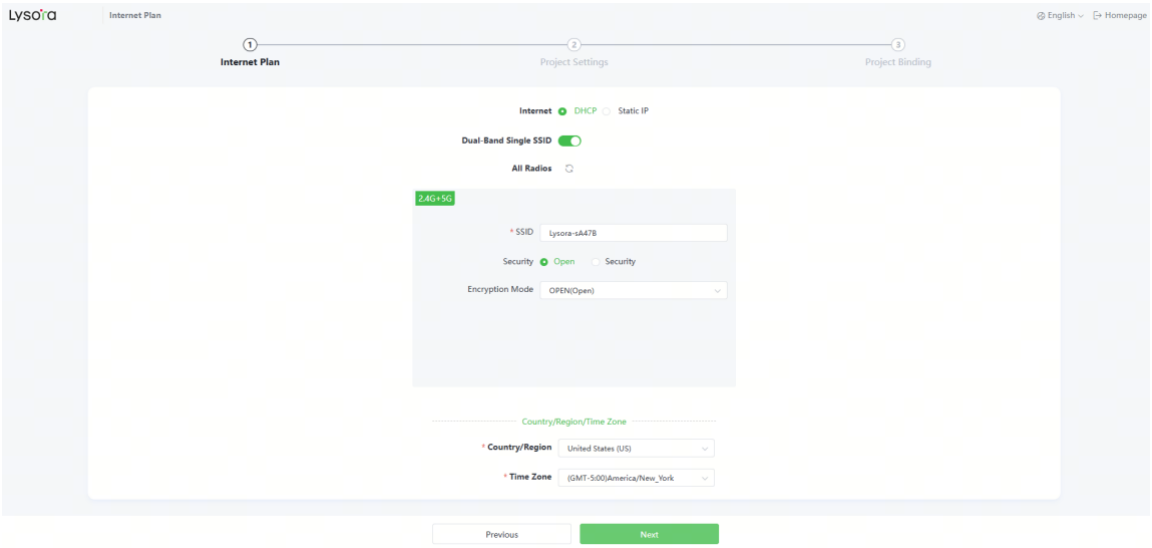
(1) Click **Next** to configure the Internet connection type.

Note

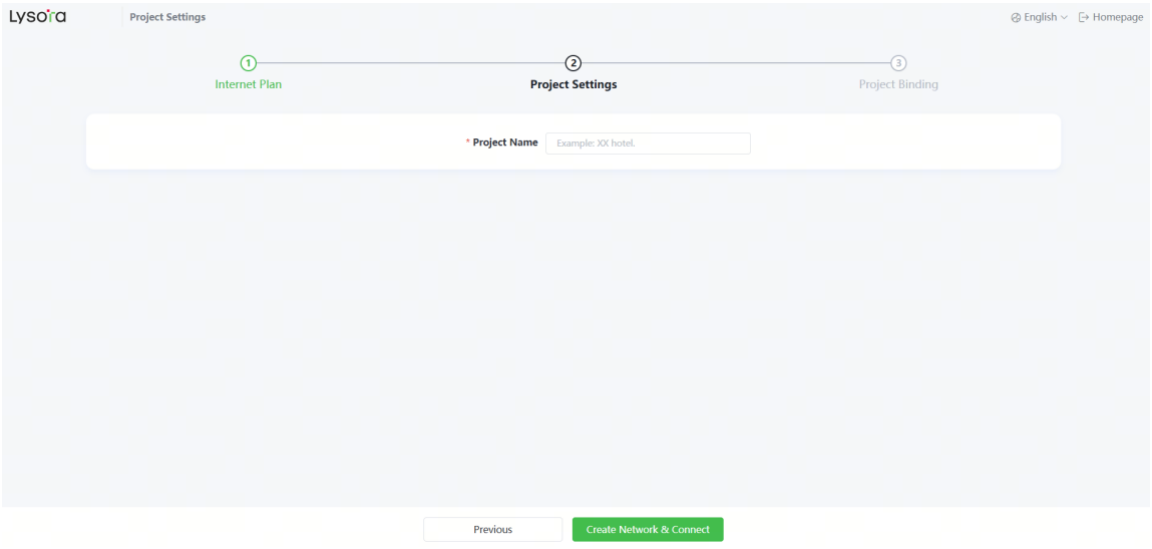
Parameters displayed on the **Network Settings** page vary according to device types on the network. The following parameters are displayed when the network contains gateways, switches, and APs.

- **Internet**: Configure the Internet access mode according to requirements of the local Internet Service Provider (ISP).
  - DHCP: The access point detects whether it can obtain an IP address via DHCP by default. If the access point connects to the Internet successfully, you can click **Next** without entering an account.
  - PPPoE: Click PPPoE, and enter the username, password, and service name. Click **Next**.
  - Static IP: Enter the IP address, subnet mask, gateway, and DNS server, and click **Next**.
- **Dual-Band Single SSID**: When it is toggled on, the 2.4 GHz and 5 GHz frequency bands share the same Wi-Fi configuration. When it is toggled off, separate Wi-Fi configurations will be required for each band.
- **SSID** and **Wi-Fi Password**: The device has no Wi-Fi password by default, indicating that the Wi-Fi network is an open network. You are advised to configure a complex password to enhance the network security.

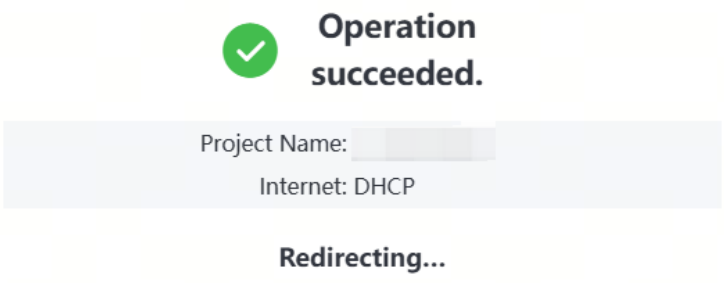
- **Country/Region**: The Wi-Fi channel may vary from country to country. To ensure that a client searches for a Wi-Fi network successfully, you are advised to select the actual country or region.
- **Time Zone**: Set the system time. The network time server is enabled by default to provide the time service. You are advised to select the actual time zone.



(2) Click **Next**. On the page that is displayed, set the project name. **Project Name** identifies the network project where the device is located.



(3) Click **Create Network & Connect**. The device will deliver the initialization and check the network connectivity.



After completing the quick setup, the new device can access the Internet. You can bind the device with a Lysora Cloud account for remote management. Follow the instruction to log in to Lysora Cloud for further configuration. If you do not attempt to bind a Lysora Cloud account, click **Homepage** to access the device's web.

Note

If your device is not connected to the Internet, click **Service is unavailable.** in the displayed **Internet connection failed.** dialog box to exit the configuration wizard. To connect your device to the Internet in the future, see 7.6 MGMT IP Configuration.

2.4 Work Mode

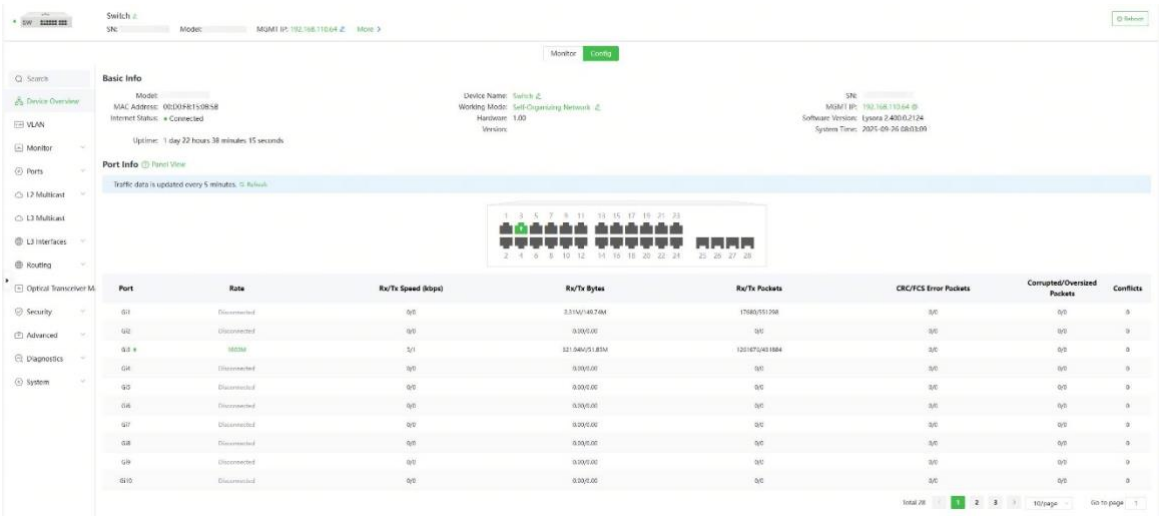
The device supports two work modes: **Standalone** and **Self-Organizing Network**. It works in **Self-Organizing Network** mode by default. The system presents different menu items based on the work mode. To modify the work mode, see 4.1.2 Switching the Work Mode.

- **Standalone mode**: If the self-organizing network discovery function is disabled, the device will not be discovered in the network. After logging in to the web page, you can configure and manage only the currently logged in device. If only one device is configured or global configuration does not need to be synchronized to the device, you can disable the self-organizing network discovery function.
- **Self-Organizing Network**: After the self-organizing network discovery function is enabled, the device can be discovered in the network and discover other devices in the network. Devices network with each other based on the device status and synchronize global configuration. You can log in to the web page of the device to check management

information about all devices in the network. After self-organizing network discovery is enabled, users can maintain and manage the current network more efficiently. You are advised to keep this function enabled.

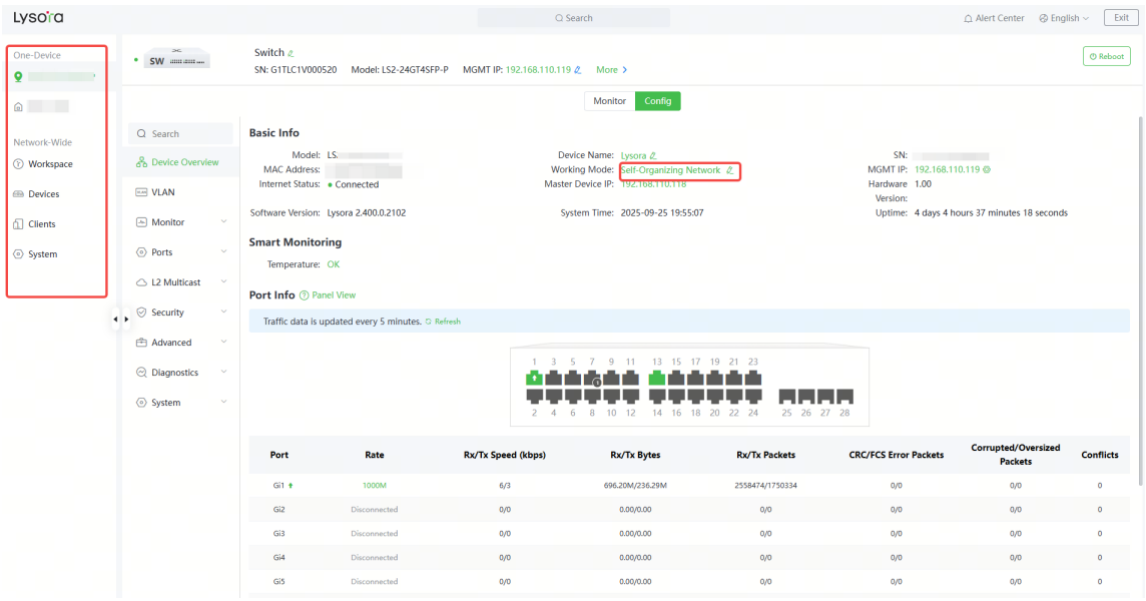
In standalone mode, you can configure and manage only the current logged in device without self-organizing network function.

Figure 2-1 The web Page in Standalone Mode



In Self-organizing mode, you can batch set the commonly used functions of all wired and wireless Lysora products within the self-organizing network, including the currently logged-in device.

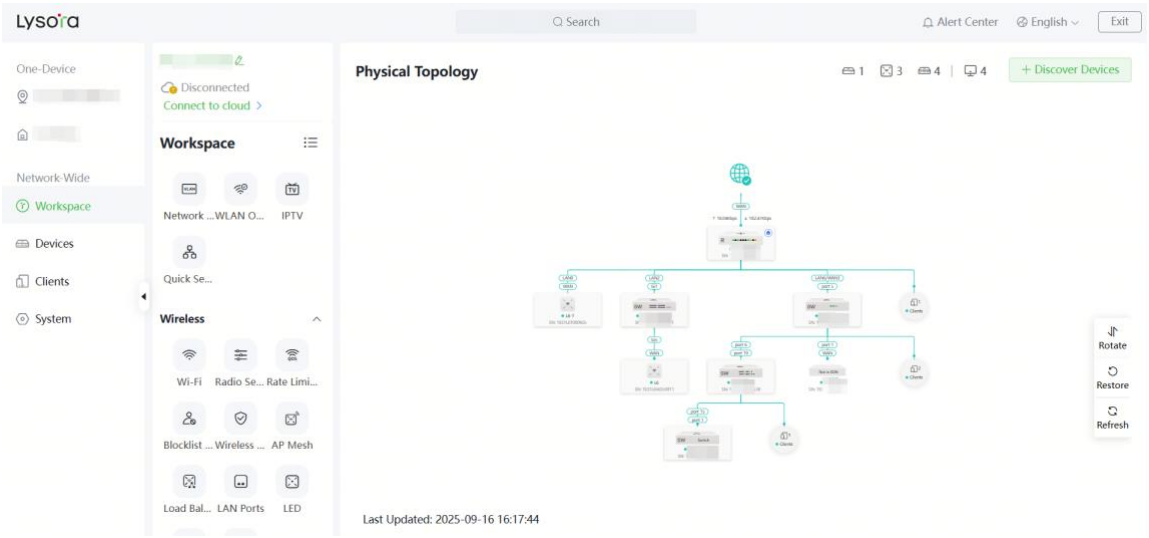
Figure 2-2 The Web Page in Self-Organizing Mode



3 Network-Wide Management

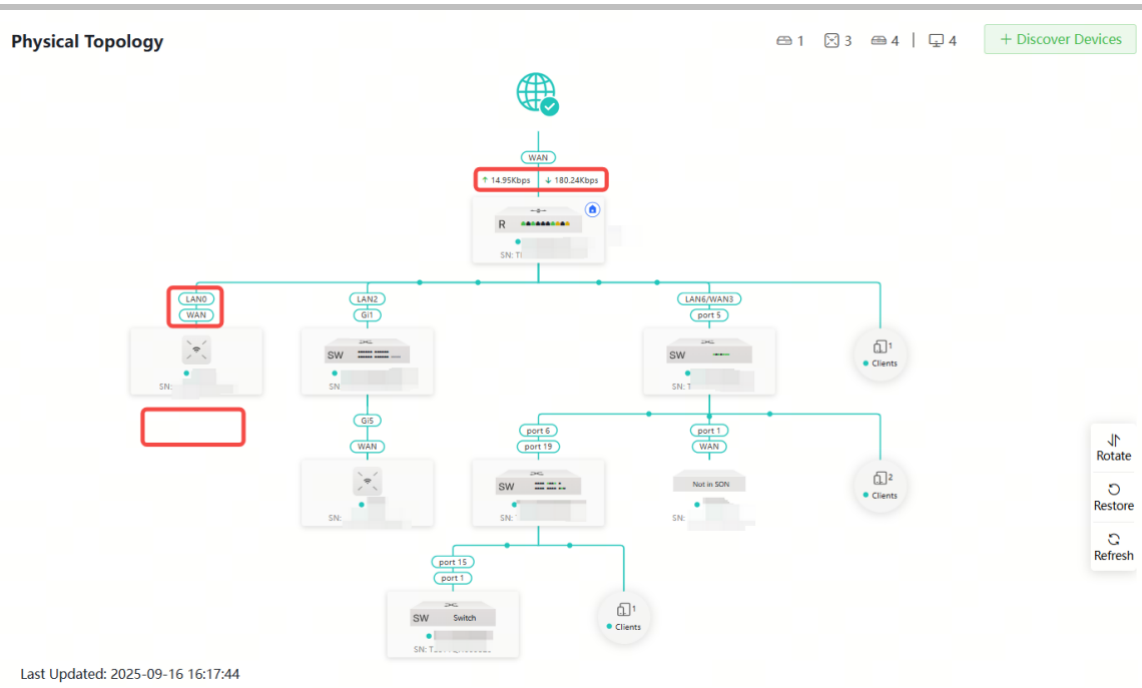
Choose **Network-Wide** > **Workspace** > **Physical Topology**.

The **Physical Topology** webpage displays the current network topology, real-time uplink and downlink flow, networking status, and the number of users. The quick access to network and device settings is also provided on the **Physical Topology** webpage. Users can monitor, configure and manage the network status on the current page.

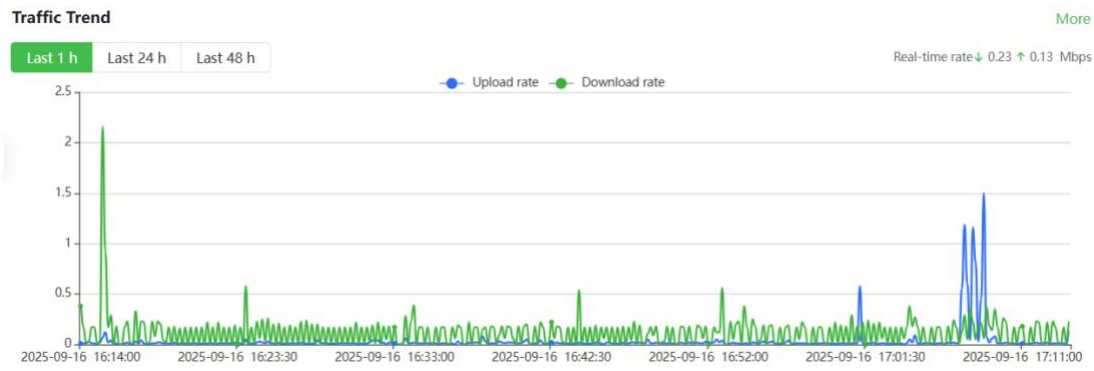


3.1 Viewing the Network Information

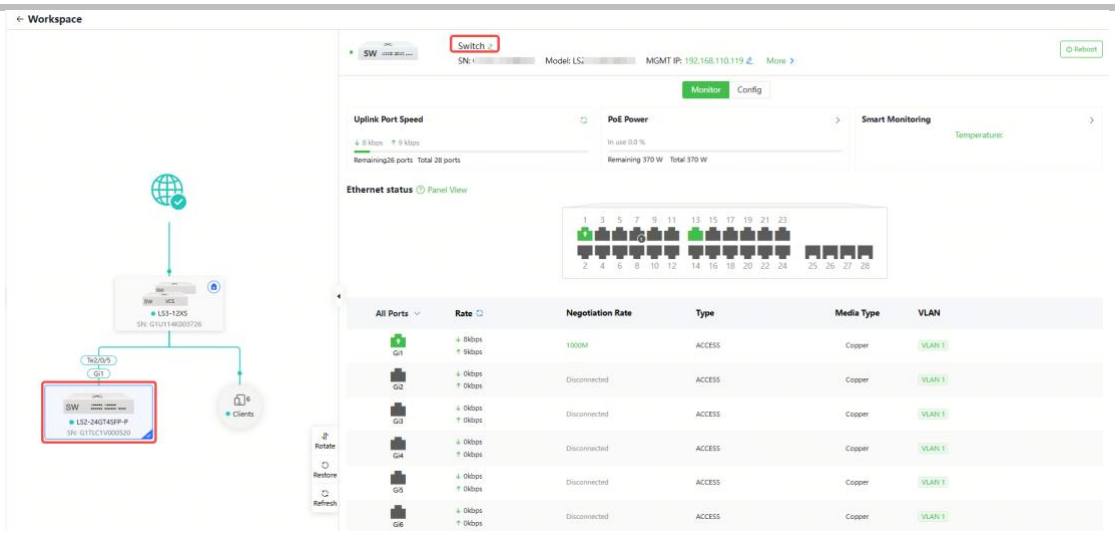
You can view the online device, port ID, device SN as well as the real-time uplink and downlink flow in the network topology.



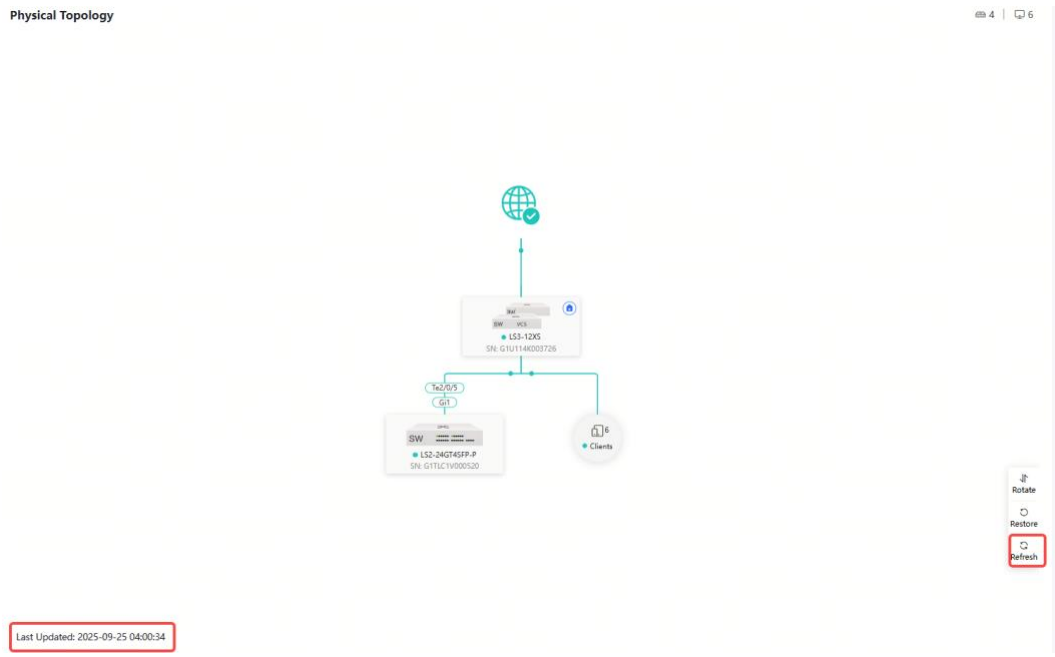
- Click the egress gateway in the topology to view real-time traffic information of the device.



- Click the device in the topology to view the operating status and configuration of the device and configure the device functions. The hostname is set to the product model by default. You can click to modify the hostname.



- The update time of the topology is displayed at the bottom left corner. Click **Refresh** to update the topology to the latest status. Please wait for a few minutes for the update.

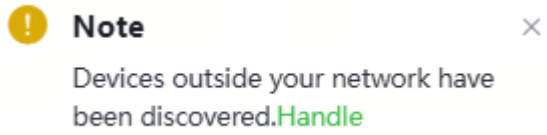


3.2 Adding Network Devices

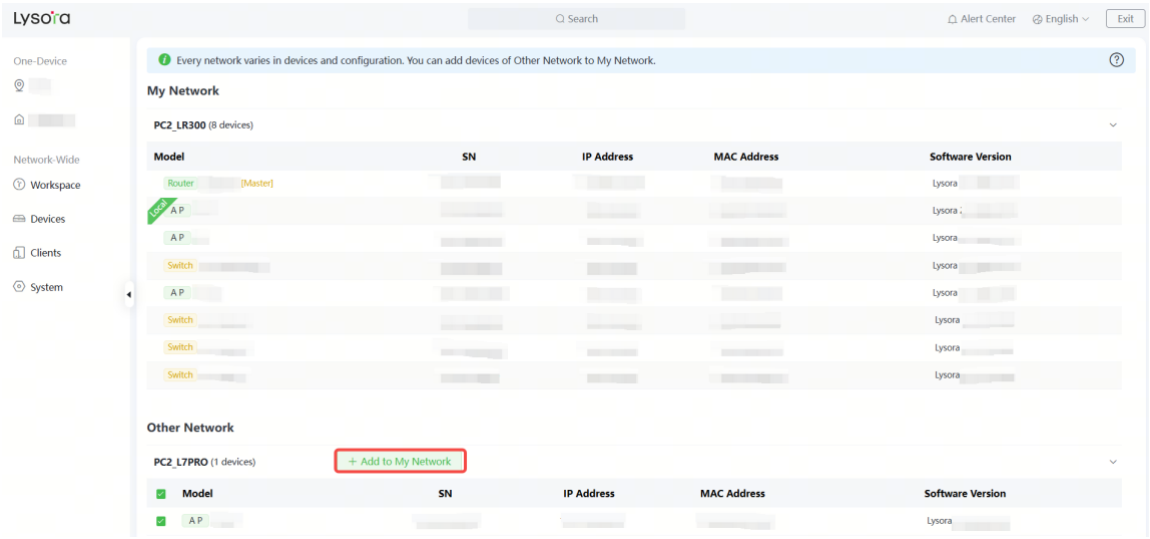
3.2.1 Wired Connection

(1) If a new device is connected to the device in the network through wired connection, a prompt message will pop up, indicating that a device not in self-organizing network is

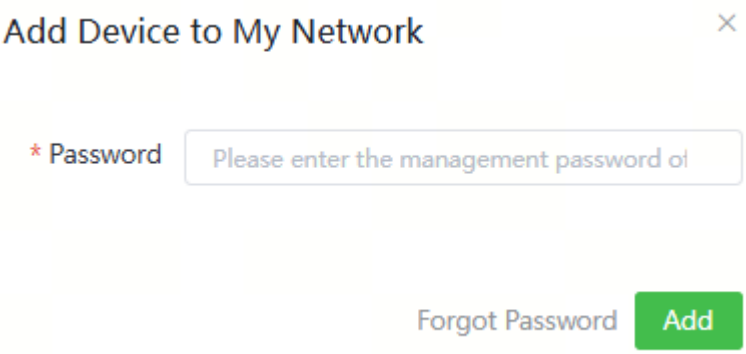
discovered. The number (in orange) of devices that are not in self-organizing network is displayed under the **Devices** at the top left corner of the page. Click **Handle** to add the device to the current network.



(2) On the network list page, click the downward arrow next to **Other Network** to expand this list. Select the desired device(s) and click **Add to My Network**.



(3) If the target device is not configured yet, you can add the device directly without a password. If the device is configured with a password, please enter the management password of the device. If the password is incorrect, the device cannot be added to the network.



3.2.2 AP Mesh

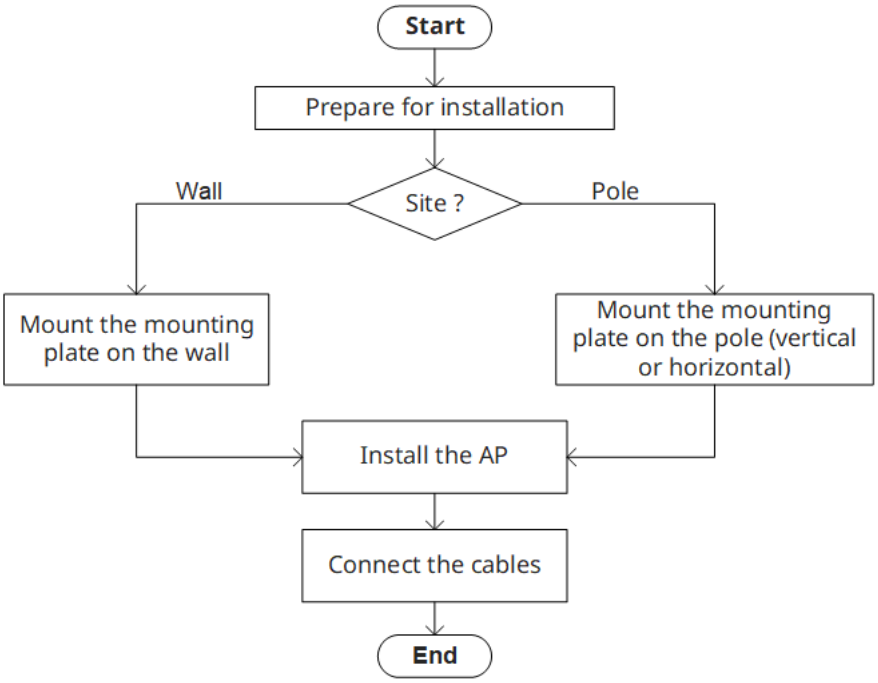
1. Overview

After being powered on and enabled with the AP Mesh feature, a Mesh-capable new AP can be paired with other Mesh-capable wireless devices on the target network through multiple ways. Then the AP will be synchronized its Wi-Fi configuration with other devices automatically. Mesh networking addresses pain points such as complex wireless networking and cabling. A new AP can be connected to any uplink wireless device among AP, gateway, and wireless router in the following ways:

- Button-based pairing: Short press the Mesh button on the router on the target network to implement fast pairing of the AP with the wireless router.
- Search-based pairing: Log in to the web page of a device on the target network. Search and add APs to be paired.
- Wired pairing: Connect the new AP to a wireless device on the target network using an Ethernet cable. The new AP will go online on the target network.

After pairing finishes, the new AP obtains the wireless backhaul information from network-wide neighboring APs. Install the new AP as planned, and it will connect to the optimal neighboring AP.

2. Configuration Steps



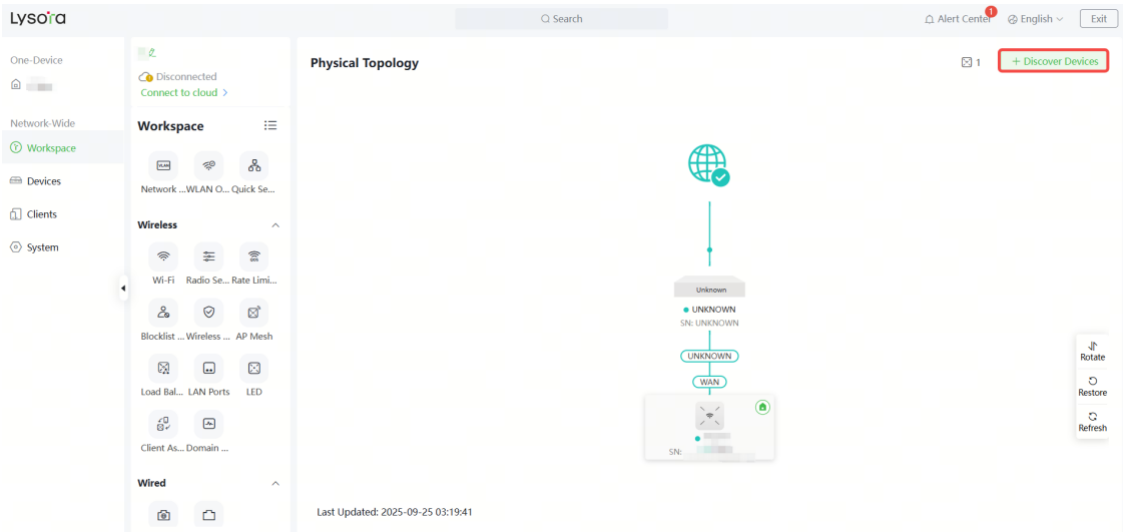
3. Configuration Steps for Search-based Pairing

⚠ Caution

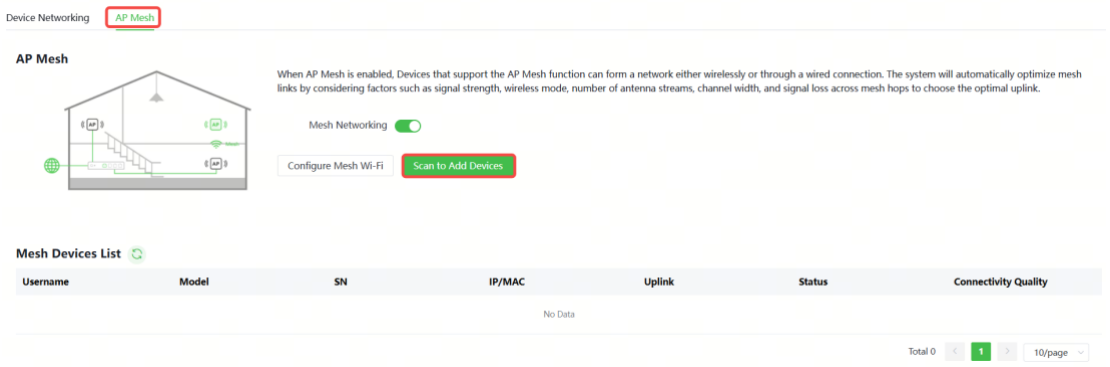
- Uplink device is an AP.
- The new AP must be in factory status.
- It can be scanned only when the live network is enabled with Mesh.
- Place the new AP no more than 2 meters away from the uplink device to ensure that the new AP can receive the Wi-Fi signal from the uplink device. The new AP may fail to be scanned due to the long distance or obstacles between it and the uplink device.

(1) Power on the new AP and place it near the AP or EGW router on the target network.

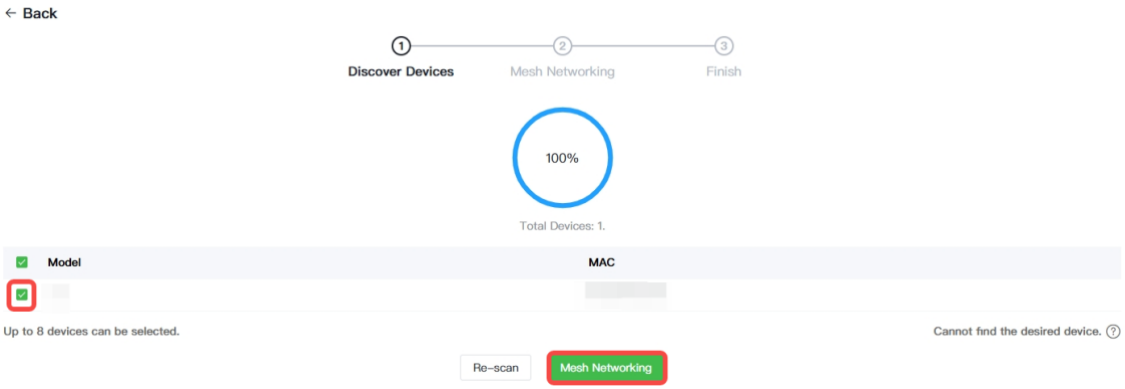
(2) Log in to the web page of a device on the target network. In **Network-Wide** mode, click **+Discover Devices** in the upper right corner of the **Physical Topology** page to scan the APs in other networks not plugged in with Ethernet cables.

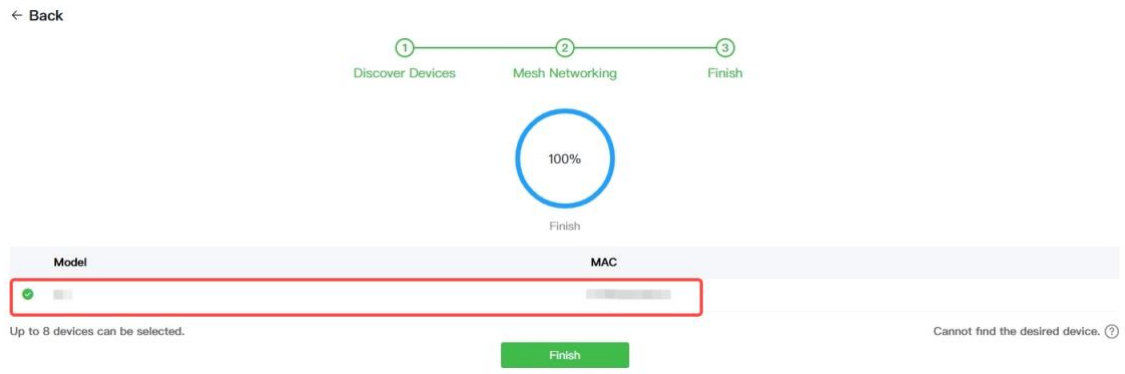


(3) On the **AP Mesh** page, click **Scan** to scan devices that are not connected to the network via an Ethernet cable.

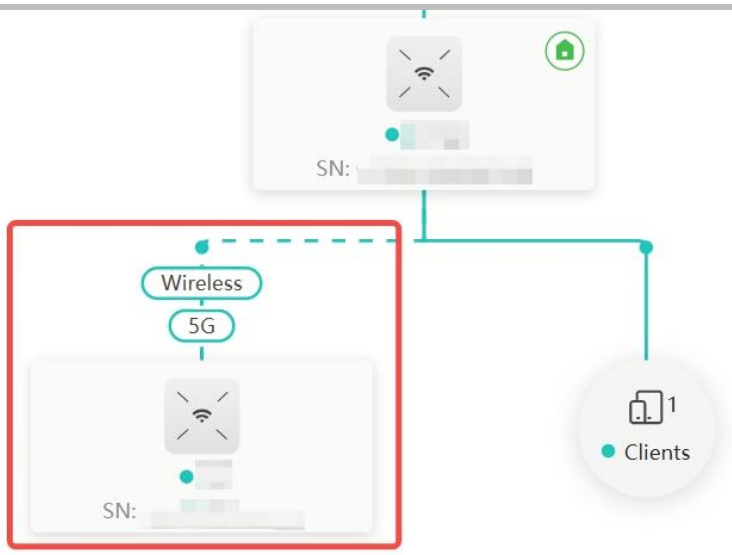


(4) Select the APs to be added and click **Mesh Networking**. No more than eight APs are allowed at a time. Wait until network merging finishes.



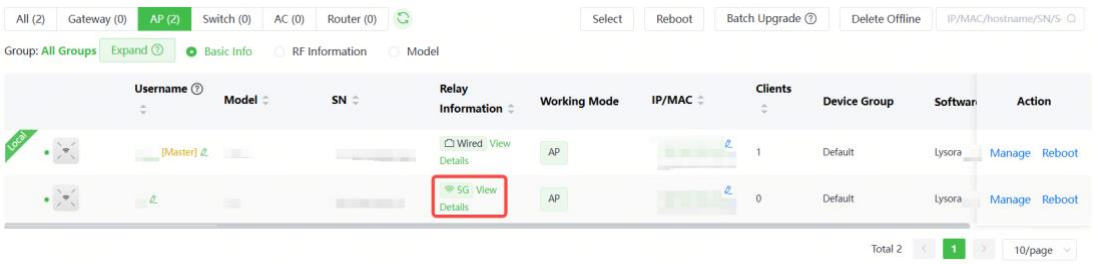


(5) Check the topology on the **Physical Topology** page to make sure that the new AP has connected to the uplink device in wireless mode.

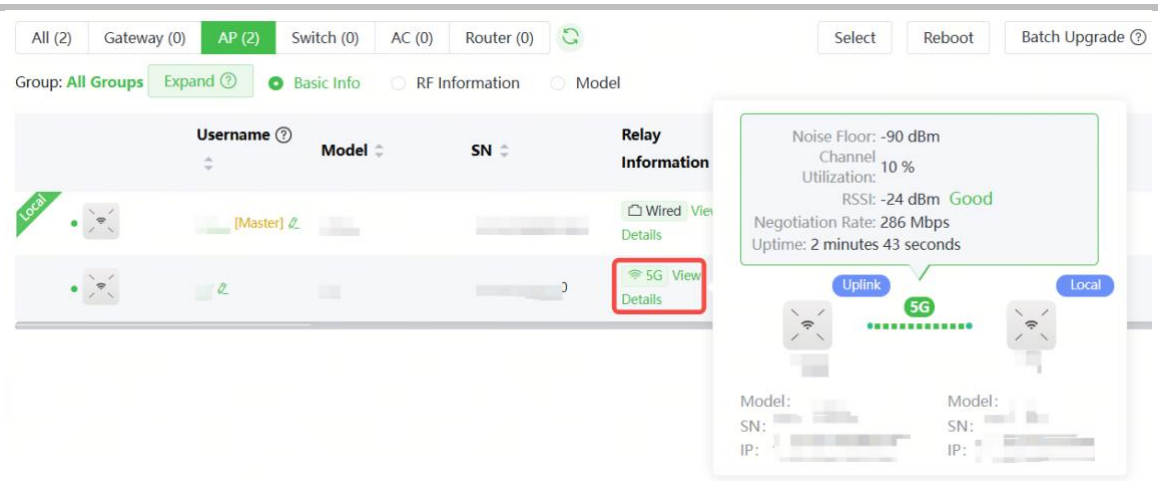


(6) Power off the new AP and install it as planned.

(7) Log in to the web page of a device on the target network. In **Network-Wide** mode, choose **Devices** > **AP**. Make sure that the new AP is online and the corresponding entry contains icon 5G in the **Relay Information** column. The icon indicates that wireless backhaul is performed through the 5 GHz radio.



(8) Click **View Details** following the 5G icon to obtain information about the uplink device and RSSI.



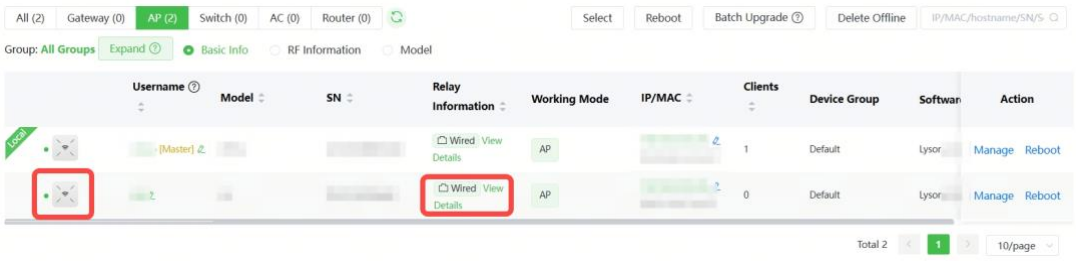
4. Configuration Steps for Wired Pairing

Caution

- Uplink device is an AP, or router.
- The new AP must be in factory status.
- It can be scanned only when the live network is enabled with Mesh.

(1) Plug one end of the Ethernet cable to the uplink port of the new AP, and the other end to the downlink port of an AP, EG router, or EGW router on the target network. Mesh networking takes one to three minutes. When the system status LED is steady on, it indicates that Mesh networking finishes.

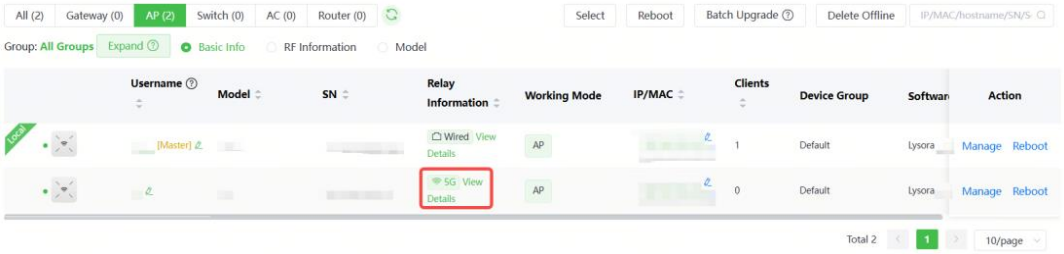
(2) Log in to the web page of a device on the target network. In **Network-Wide** mode, choose **Devices** and make sure that the new AP is online.



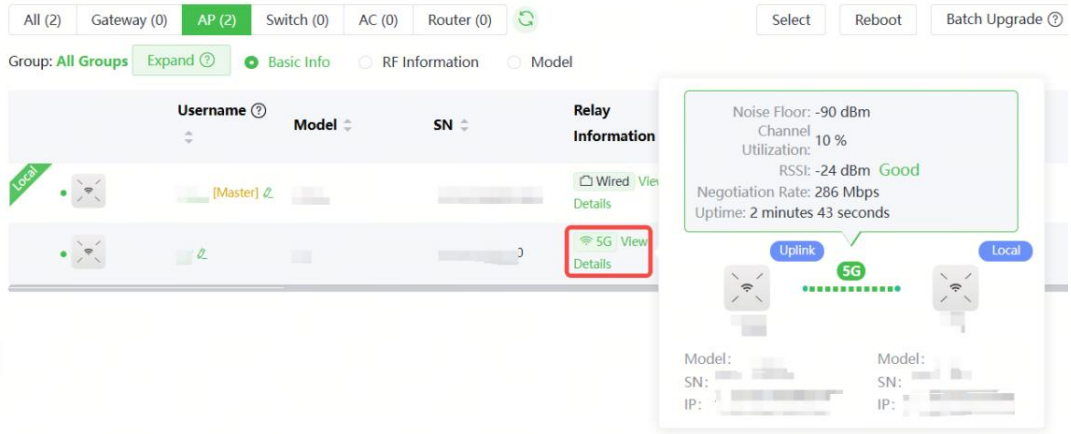
(3) Unplug the Ethernet cable, power off the new AP, and install it as planned.

(4) Log in to the web page of a device on the target network. In **Network-Wide** mode, choose **Devices** > **AP**. Make sure that the new AP is online and the corresponding entry

contains icon  in the **Relay Information** column. The icon indicates that wireless backhaul is performed through the 5 GHz radio.



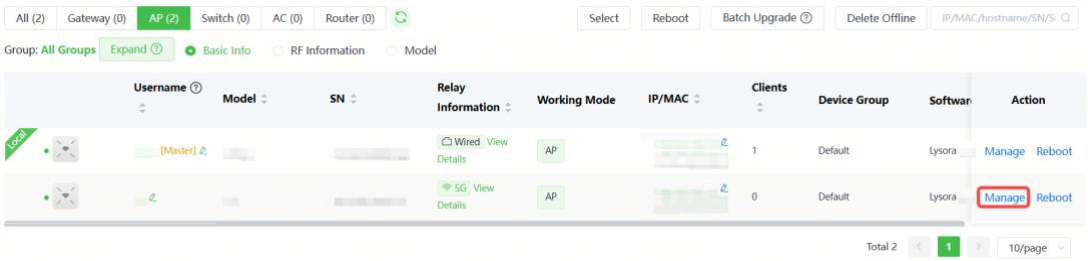
(5) Click **View Details** following the  icon to obtain information about the uplink device and RSSI.



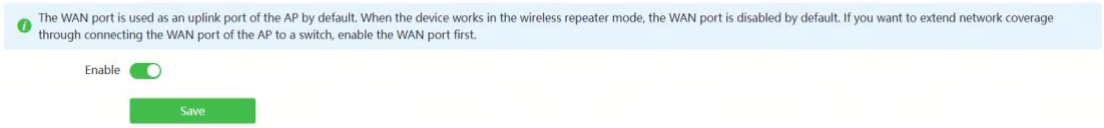
5. Enabling WAN Port

The WAN port works as the wired uplink port of the AP by default. For the AP added to the target network through AP Mesh, the WAN port is disabled by default. If you want to connect the Mesh AP to other downlink device in wired mode to expand the network, enable this port.

(1) Log in to the web page of the network project. Choose **Network-Wide** > **Devices** > **AP**, and click **Manage** next to a device in the AP list.



(2) Choose **Config** > **Advanced** > **Enable WAN**, toggle on **Enable**, and click **Save**.

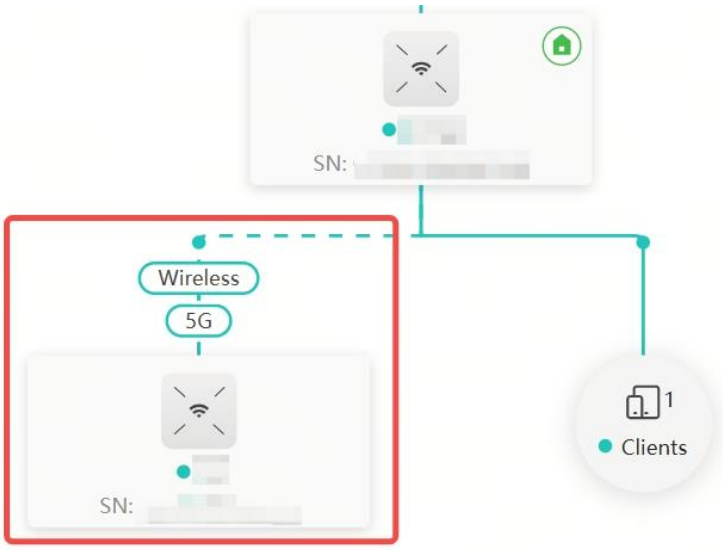


6. Querying Mesh APs and Mesh Details

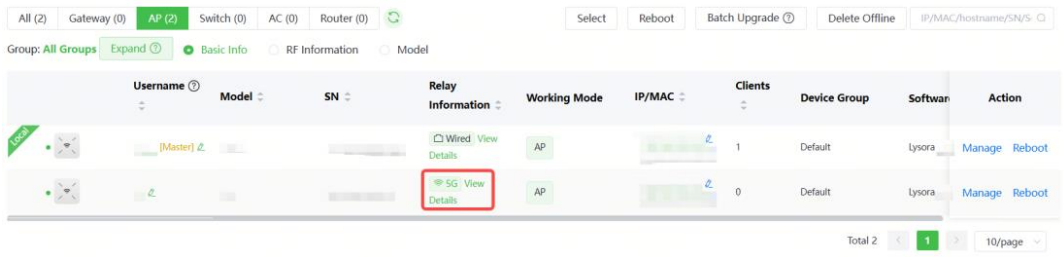
(1) Log in to the web page of a device on the target network.

(2) Query Mesh APs.

- Method 1: In **Network-Wide** mode, check the topology on the **Physical Topology** page. The AP that connects to the uplink device in wireless mode is a Mesh AP.

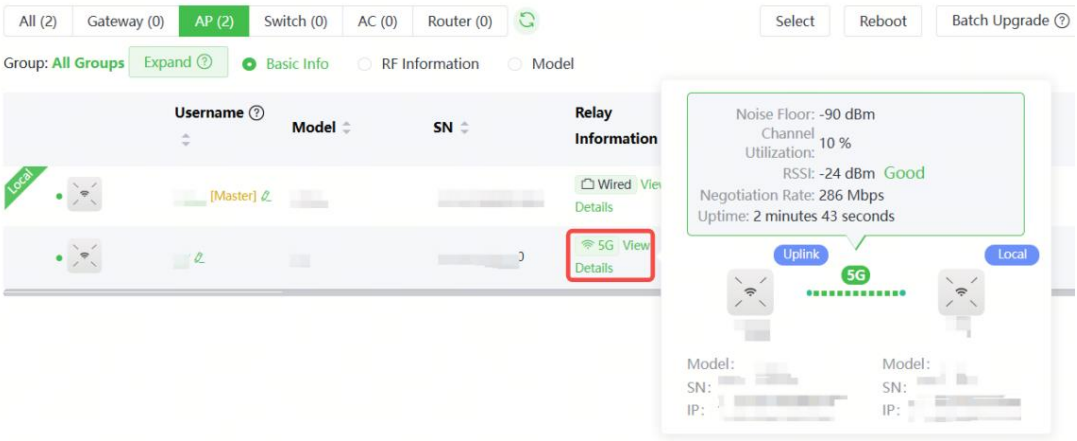


- Method 2: In **Network-Wide** mode, choose **Devices** > **AP**. If an entry contains icon 5G in the **Relay Information** column, the corresponding AP is a Mesh AP.



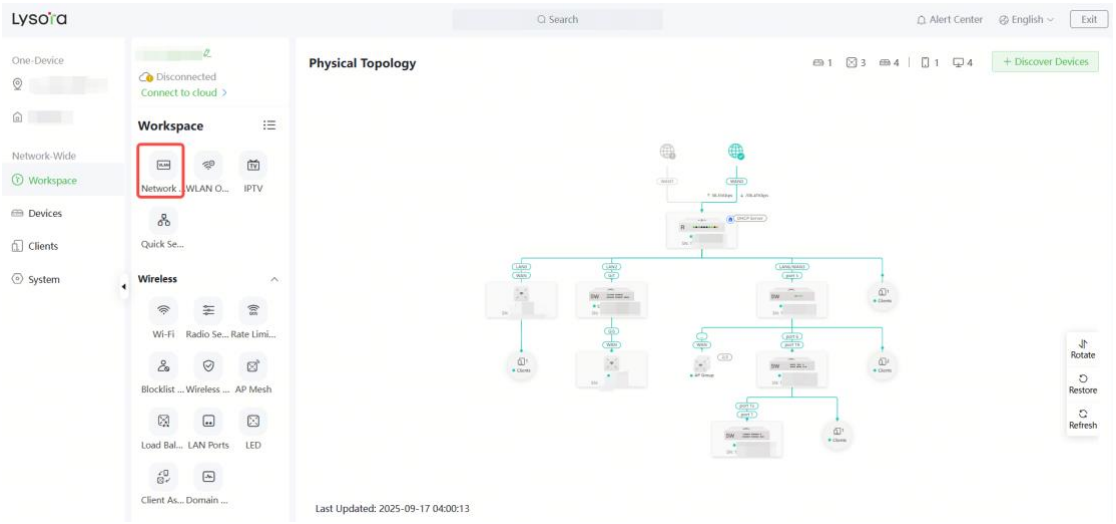
(3) Query Mesh networking details.

In **Network-Wide** mode, choose **Devices** > **AP**. Select the target AP, and click **View Details** in the **Relay Information** column to obtain the Mesh networking details.



3.3 Configuring Network Planning

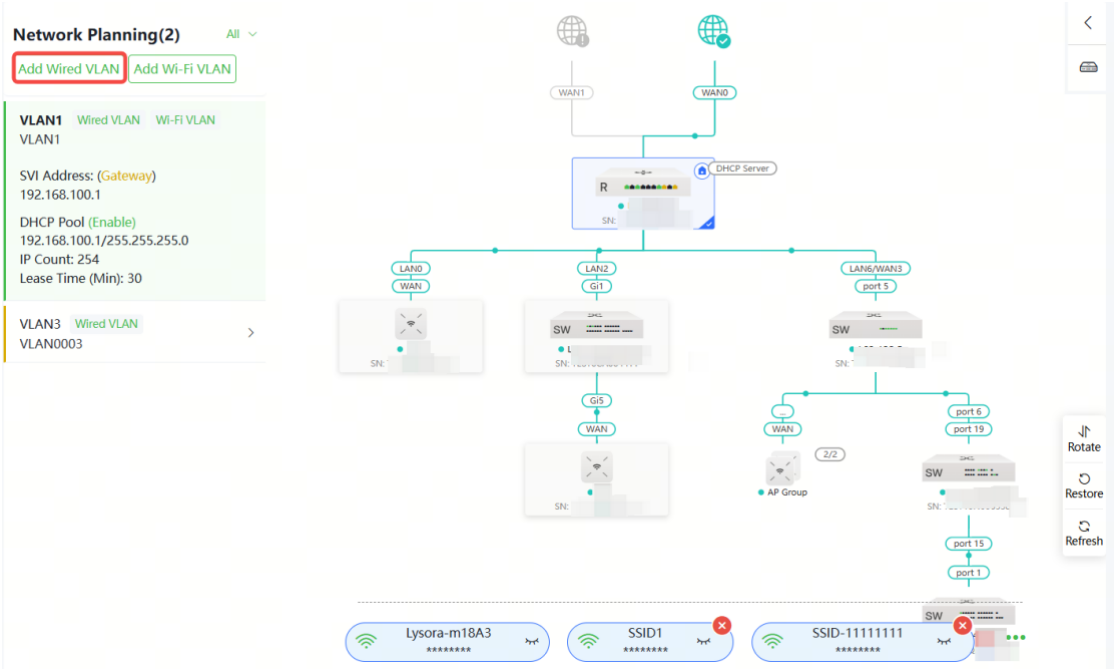
Choose **Network-Wide** > **Workspace** > **Network Planning**.



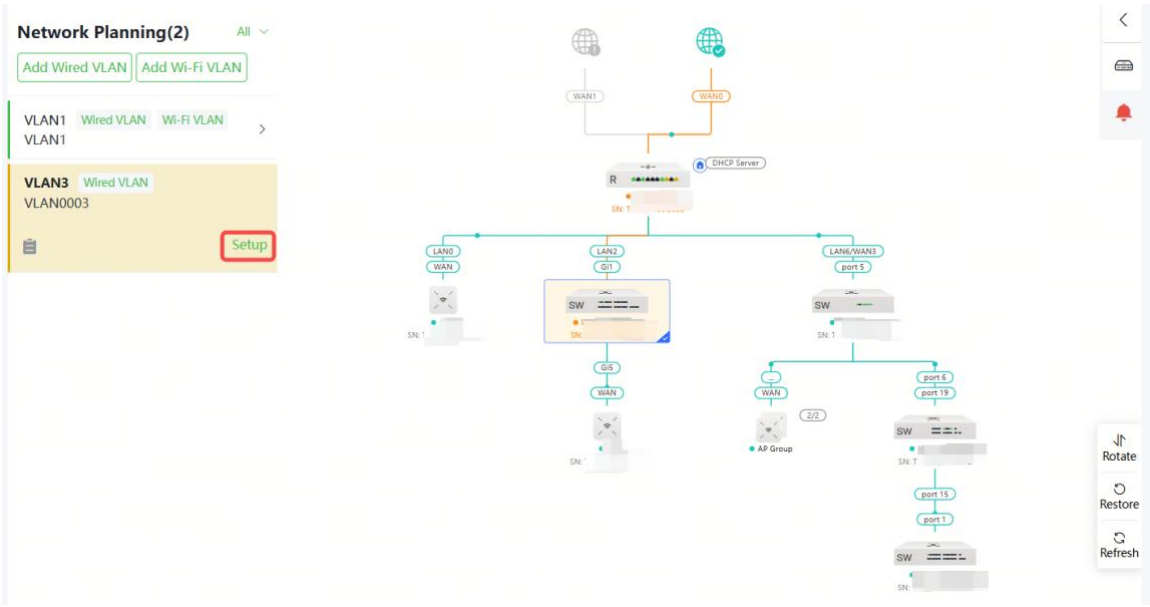
3.3.1 Configuring Wired VLAN

Choose **Network-Wide** > **Workspace** > **Network Planning**.

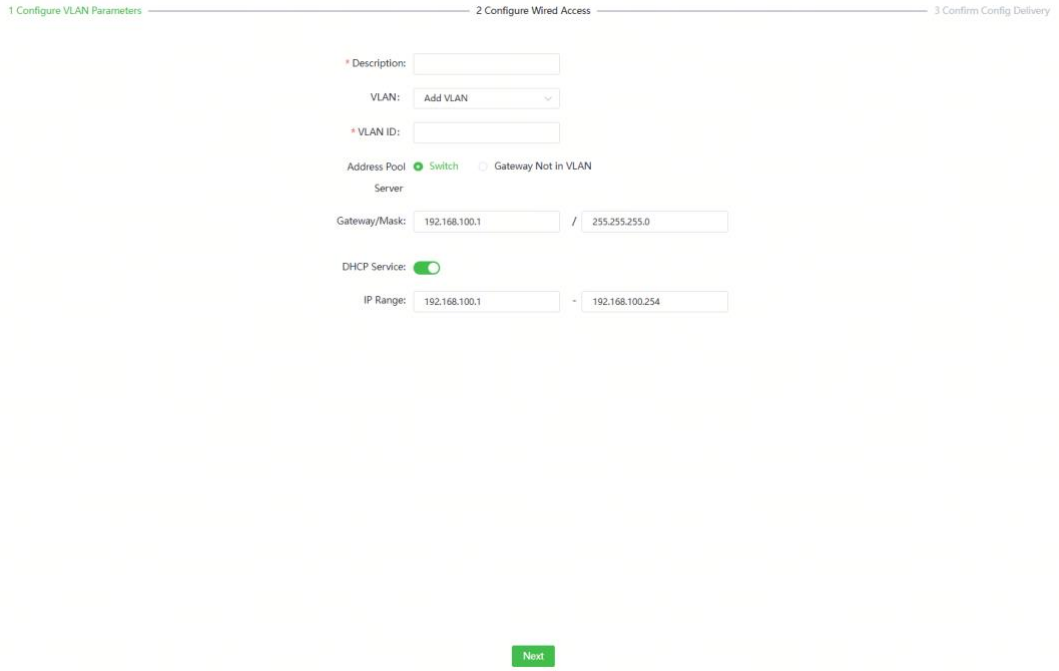
On the **Network Planning** page, click **Add Wired VLAN**.



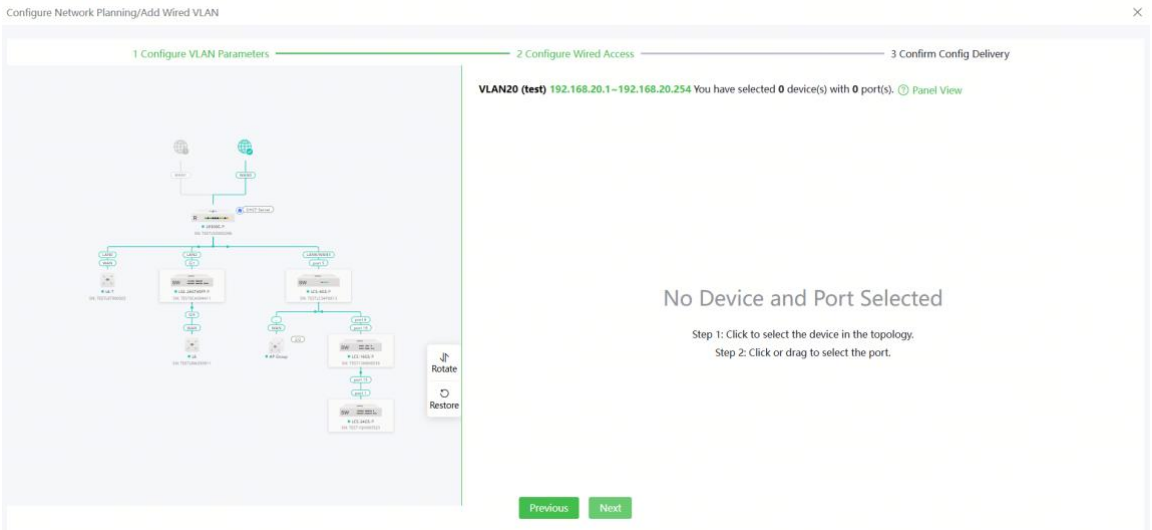
Alternatively, you can select an existing wired VLAN and click **Setup** to edit the VLAN.



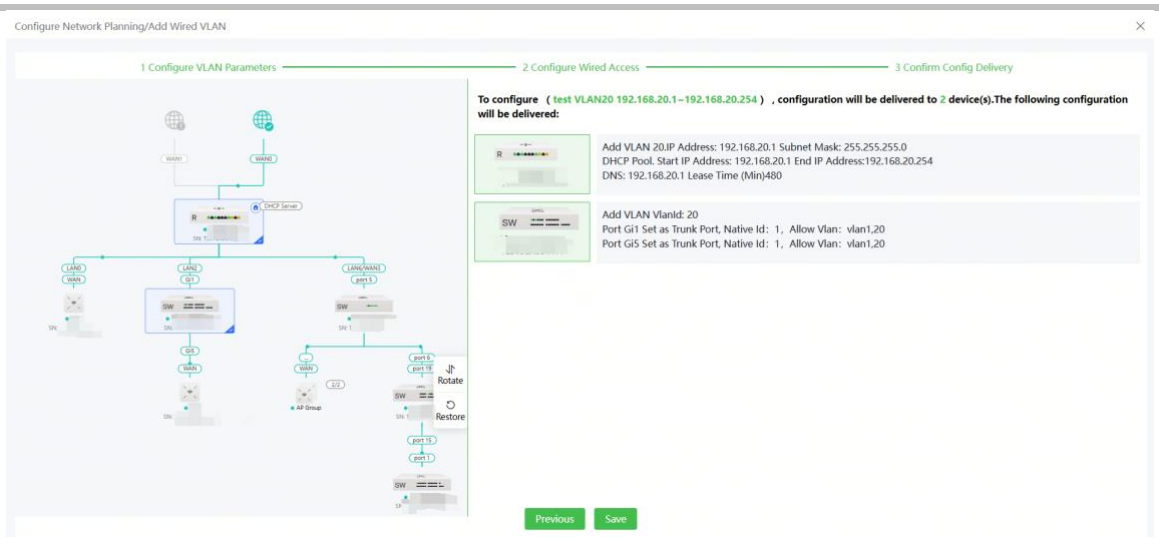
(1) Configure the VLAN ID, address pool server, and DHCP pool. The gateway is configured as the address pool server by default to assign IP addresses to clients. If an access switch exists in the network, you can select the access switch as the address pool server. Click **Next** after VLAN parameters are configured.



(2) Select the target switch in the topology and all member ports in the VLAN, and click **Save**.



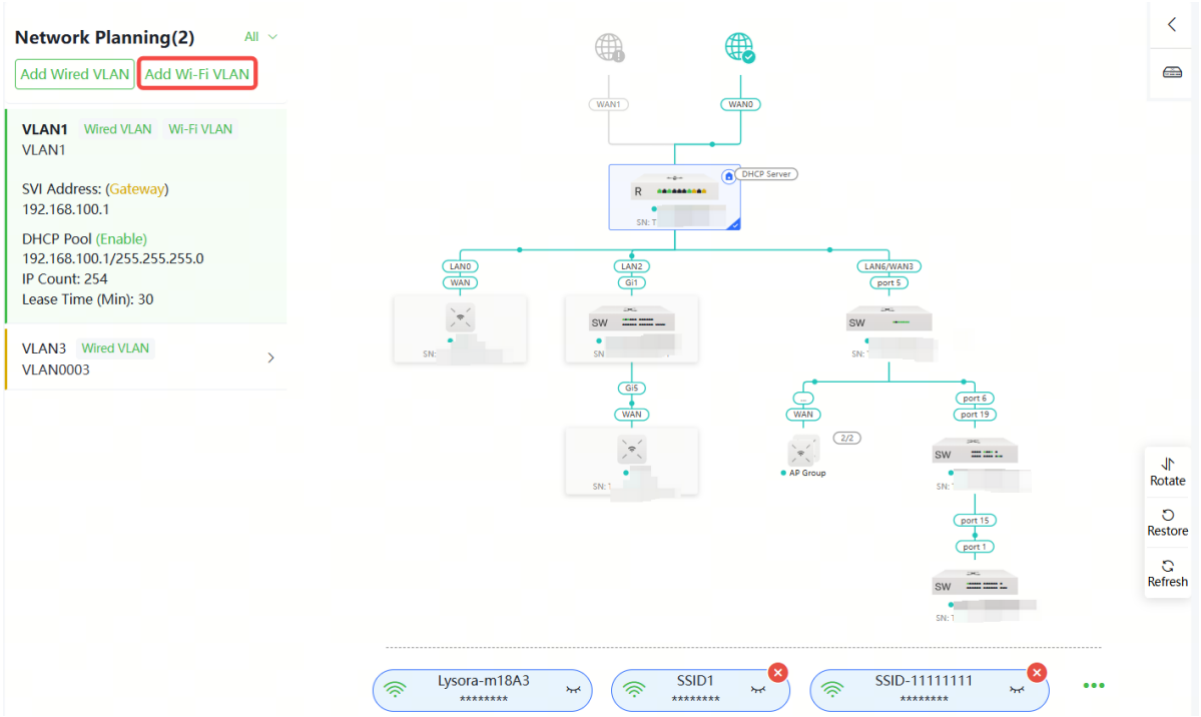
(3) Please confirm the delivered configurations and click **Save**. The configurations will take effect after a few minutes.



3.3.2 Configuring Wi-Fi VLAN

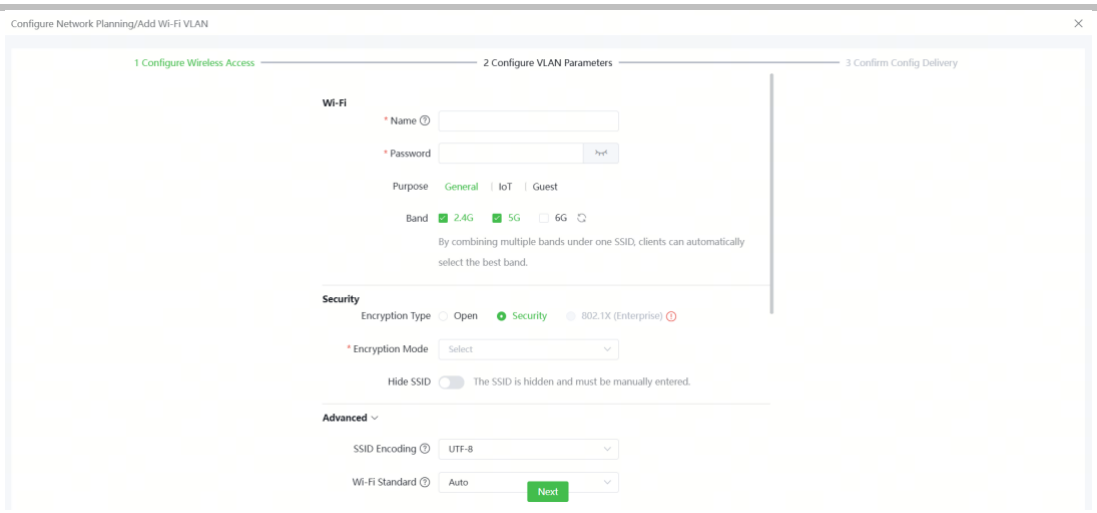
Choose **Network-Wide** > **Workspace** > **Network Planning**.

On the **Network Planning** page, click **Add Wi-Fi LAN**.

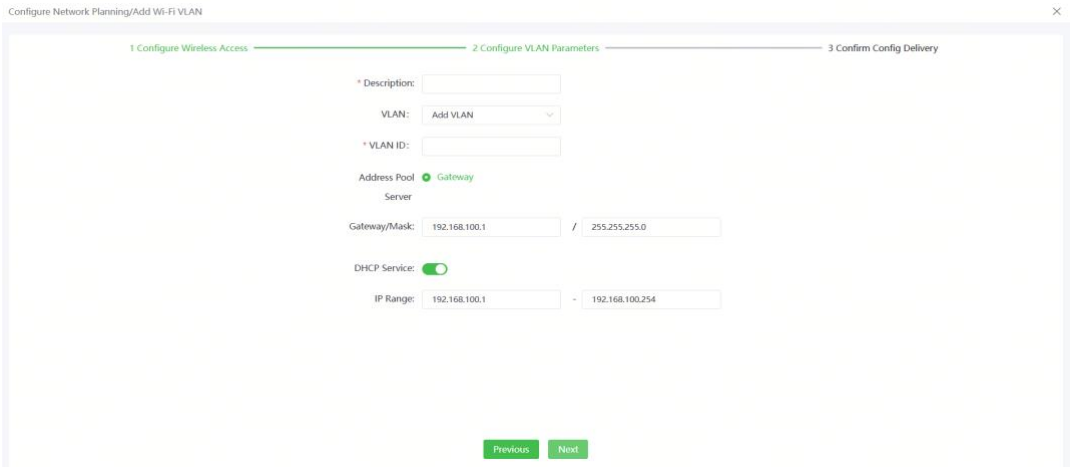


Alternatively, you can select an existing wireless VLAN and click **Setup** to edit the VLAN.

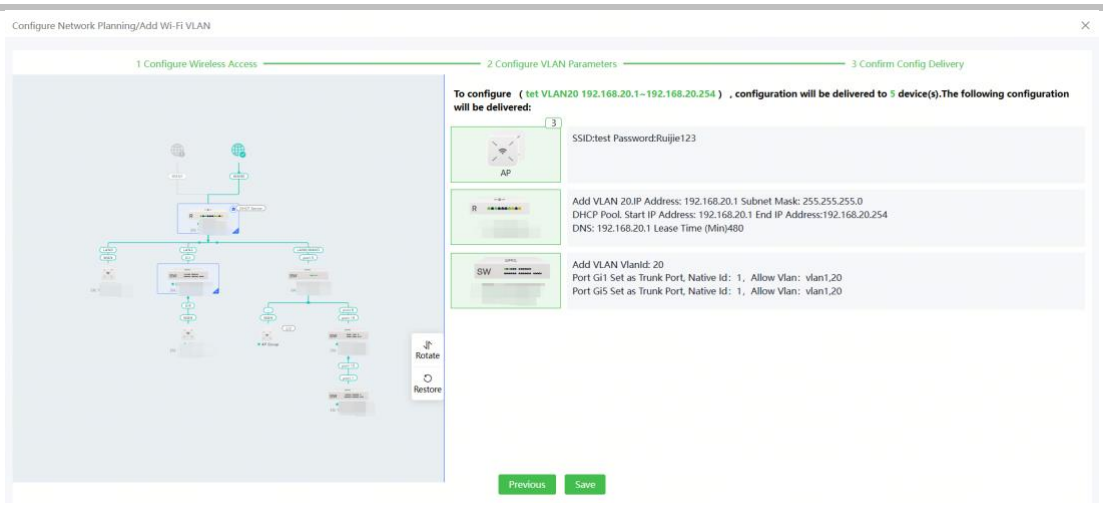
(1) Configure the SSID, Wi-Fi password and band. Click **Advanced Settings** to expand the advanced settings and set the parameters. Then, click **Next**.



(2) Configure the VLAN ID, address pool server and DHCP pool. The gateway is configured as the address pool server by default to assign IP addresses to clients. If an access switch exists in the network, you can select the access switch as the address pool server. Click **Next** after VLAN parameters are configured.



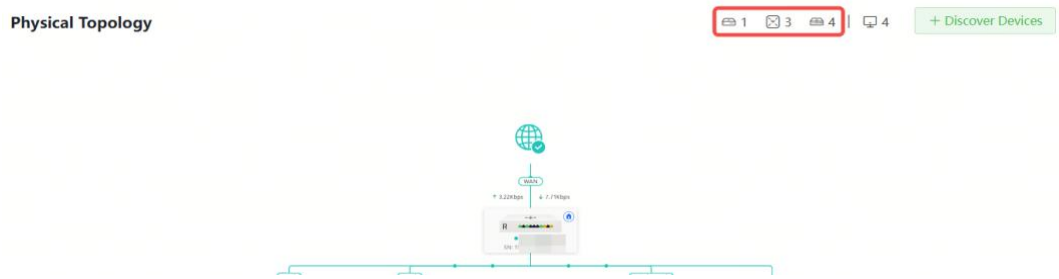
(3) Please confirm the delivered configurations and click **Save**. The configurations will take effect after a few minutes.



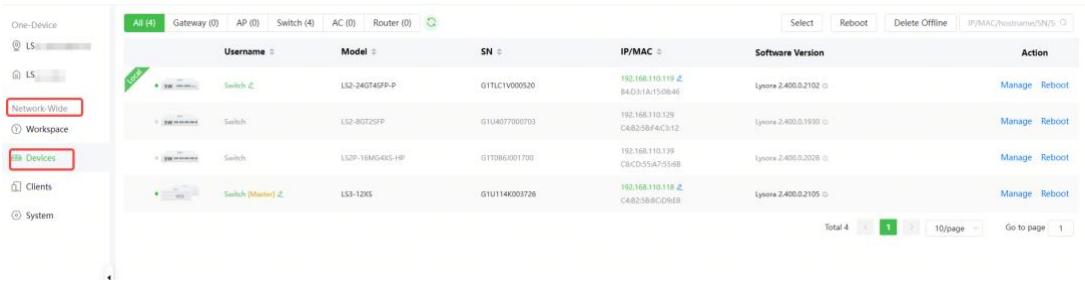
3.4 Device Management

View all device information in the current network. Users can configure and manage the entire network of devices simply by logging into one device in the network. The methods to access device management are as follows:

- Method 1: Click the device icon in the top right corner of the **Physical Topology** to switch to the device list view.

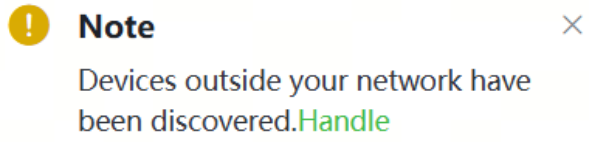


- Method 2: Choose **Network-Wide** > **Devices**

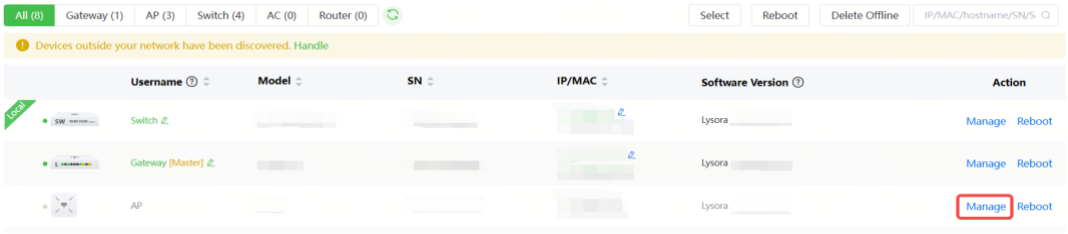


Device management operations are as follows:

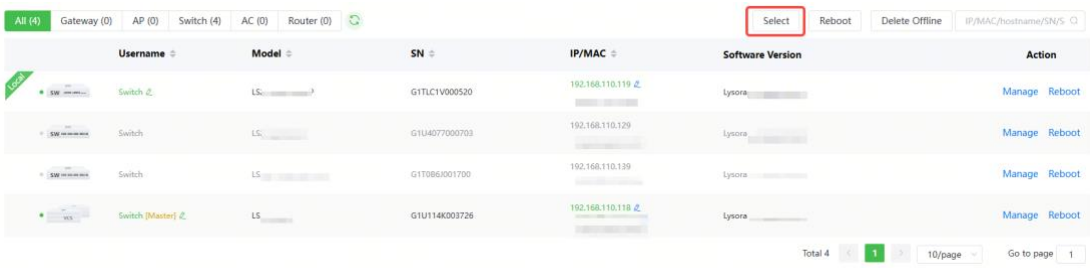
- Click **Handle** to add an ungrouped device to the current network.



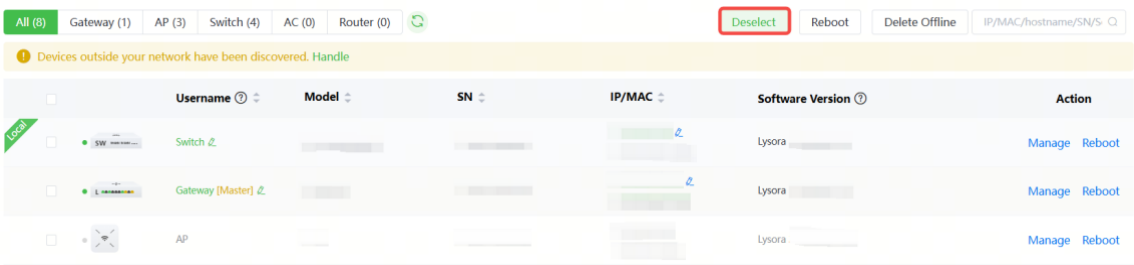
- Click **Manage** to configure a specific device.

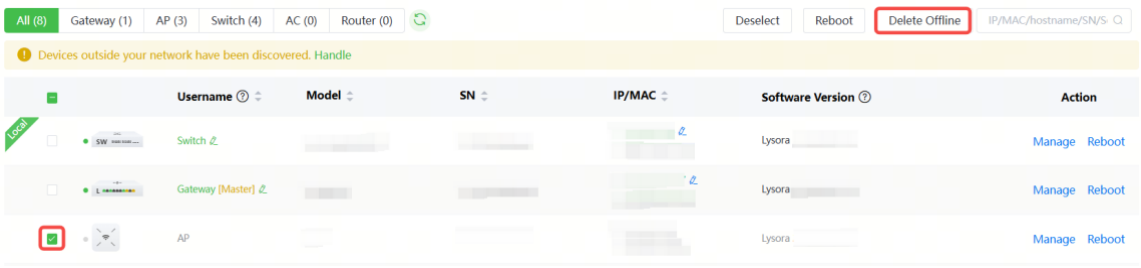


- Click **Reboot** to restart a specific device.



- Click **Select**, select the disconnected devices, and click **Delete Offline**. In the confirmation dialog box, click **OK** to remove them from the list and network topology.

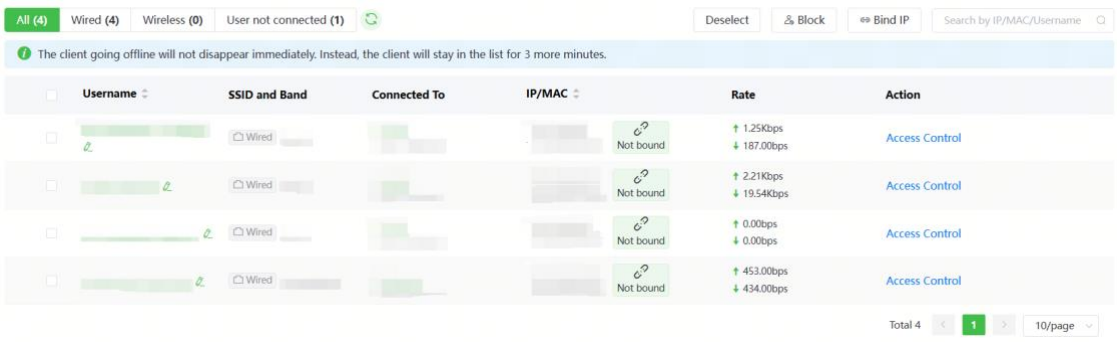




3.5 Online Client Management

Choose **Network-Wide** > **Clients**.

The client list displays wired, wireless, and users not connected on the current network, including the username, connection mode, associated device, IP/MAC address, IP address binding status, rate, and related operations.



- Click **Not Bound** in the **IP/MAC** column to bind the client to a static IP address.
- Click a button in the **Action** column to perform the corresponding operation on the online client.
  - Wired: Only access control can be configured.
  - Wireless: Access control, associate, and block can be configured.

Note

You can perform IP binding and access control only when the primary device is in router mode.

Table 3-1 Online Client Management Configuration Parameters

Parameter	Description
Username	Name of the connected client.
SSID and Band	Indicates the access mode of the client, which can be wireless or wired. The SSID and frequency band is displayed when a client is connected wirelessly.
Signal Quality	The Wi-Fi signal strength of the client and the associated channel. **Note** This information is displayed only in the wireless online client list.
Connected To	Indicates wired or wireless connection, the associated device and SN.
IP/MAC	Indicates the IP address and MAC address of the client.
Negotiated Rate	The uplink data rate and downlink data rate of the client. **Note** This information is displayed only in the wireless online client list.
Online Duration	Client access duration. **Note** This information is displayed only in the wireless online client list.
Limit Speed	Implement wireless speed limiting for clients to prevent certain clients from consuming large amounts of bandwidth resources. For details, see 3.5.5 Configuring Client Rate Limiting. **Note** This information is displayed only in the wireless online client list.

Parameter	Description
Action	You can click the corresponding button to perform access control, association, and block operations on online clients.

3.5.2 Configuring Client IP Binding

Note

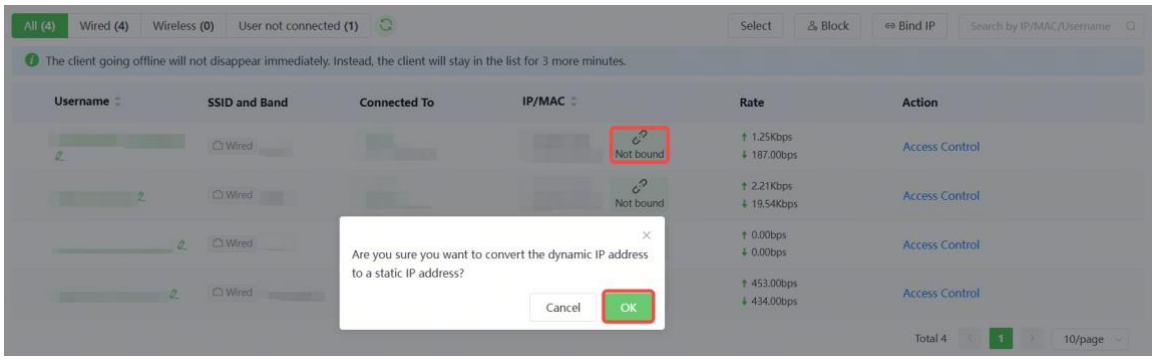
This feature is supported only when the primary device is in router mode.

Choose **Network-Wide** > **Clients**.

IP address binding is a security and access control policy that associates a specific IP address with a specific device or user to achieve identity authentication, access control, monitoring, and accounting.

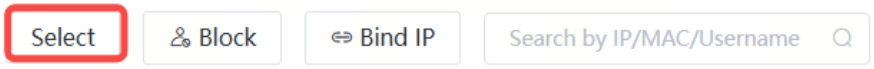
- Single client IP address binding

  Select the client to be bound with an IP address in the list, click **Not bound**, and click **OK** in the pop-up box to bind the client to a static IP address.

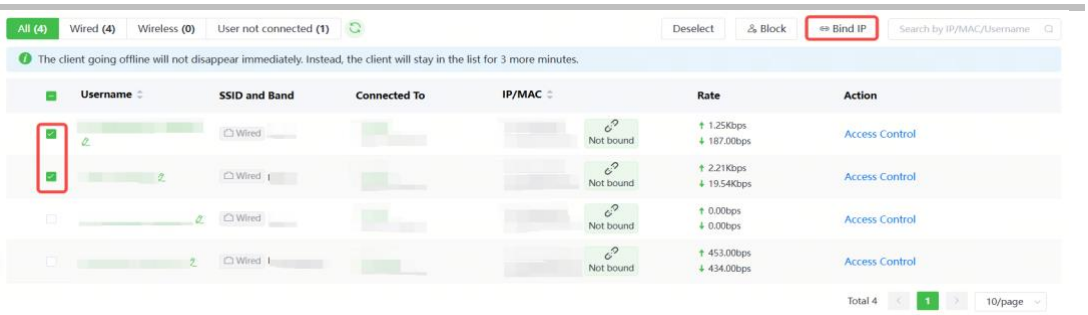


- Batch IP binding

  a Click **Select**.

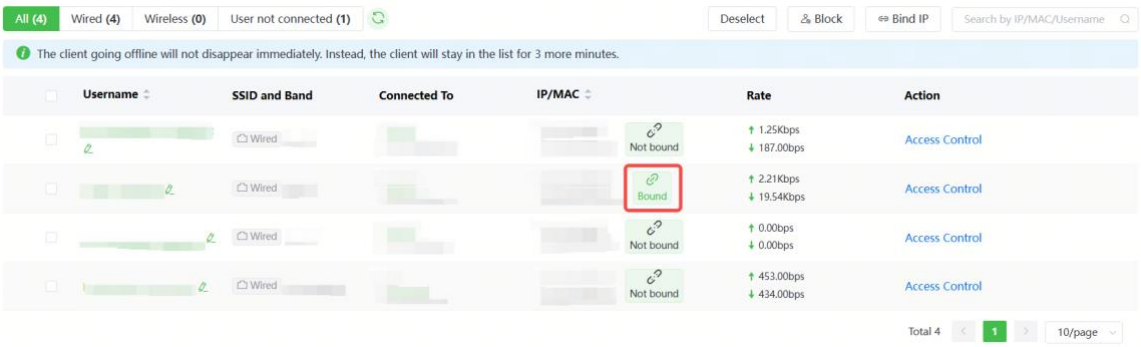


  b Select the clients to be bound, click **Bind IP**, and click **OK** in the pop-up box to bind the selected clients to a static IP address.



- Unbind an IP address

  Select the client to be unbound from the list, click **Bound**, and click **OK** in the pop-up box.



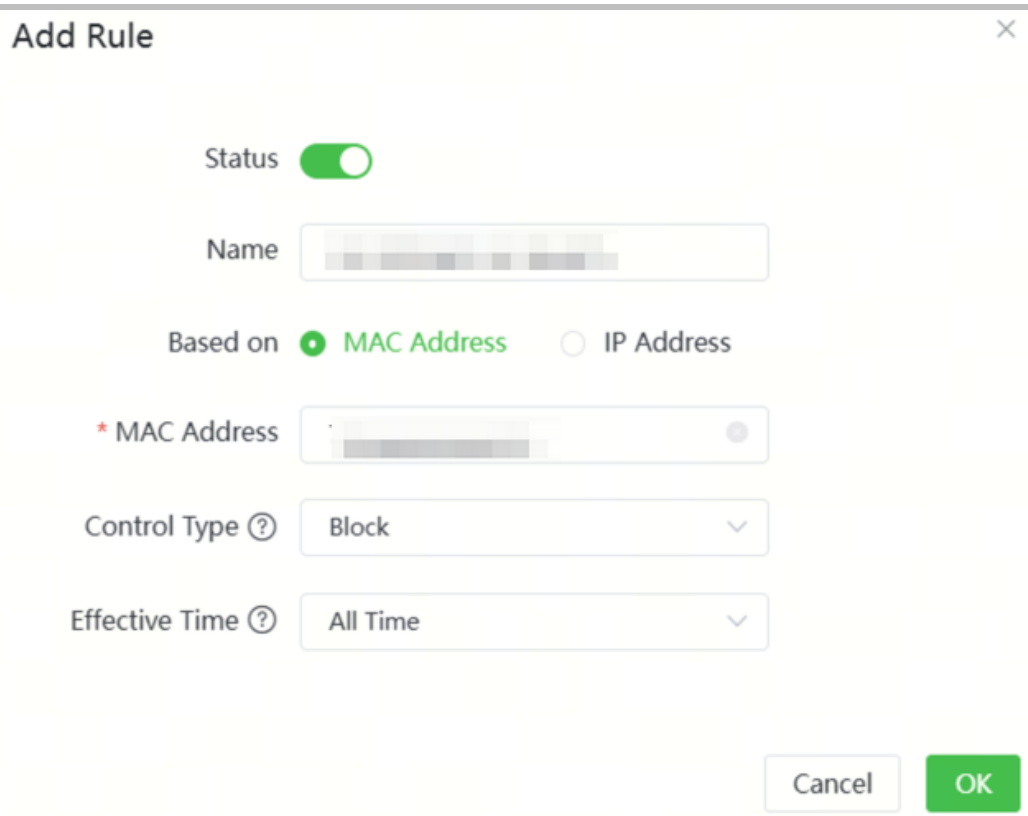
3.5.3 Configuring Client Access Control

Note

This function is supported only when the primary device is in router mode.

Choose **Network-Wide** > **Clients**.

Select a client in the list and click **Access Control** in the **Action** column. You will be redirected to the **Add Rule** page, where a MAC-based access control rule is automatically generated. The name and MAC address are automatically generated based on the selected client. After selecting the control type and effective time, click **OK** to create an access control rule for the client.



3.5.4 Blocking Clients

Choose **Network-Wide** > **Clients**.

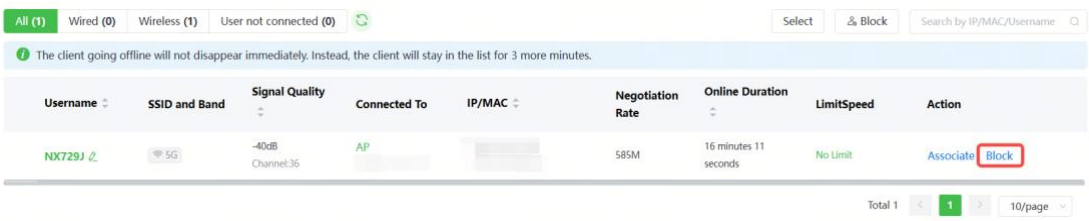
An unauthorized client may occupy network bandwidth and pose security risks. You can block specified clients to solve the unauthorized access problem.

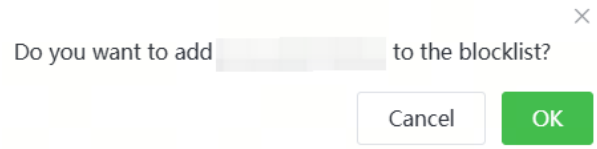
Note

Client block is available only for wireless clients.

- Block a single client

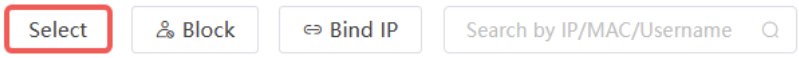
  Select a client to block in the list, click **Block** in the **Action** column, and click **OK** in the pop-up box to block the selected client.



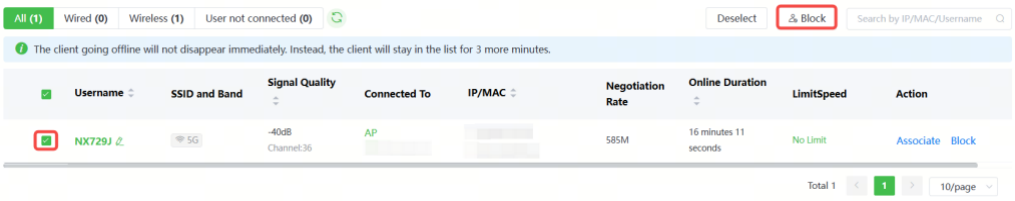


- Batch block clients

  a Click **Select**.



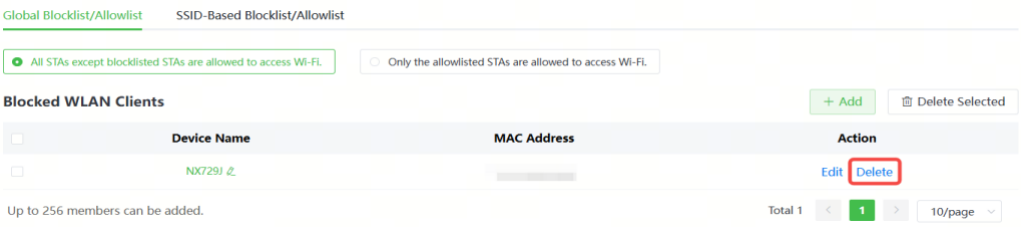
  b Select the target clients, click **Block**, and click **OK** in the pop-up box to block the selected clients.



- Cancel block

  Choose **Network-Wide > Workspace > Wireless > Blocklist/Allowlist > Global Blocklist/Allowlist.**

  Select the client to be removed from the blocklist in the wireless blocklist and click **Delete**.



3.5.5 Configuring Client Rate Limiting

Choose **Network-Wide** > **Clients** > **Wireless**.

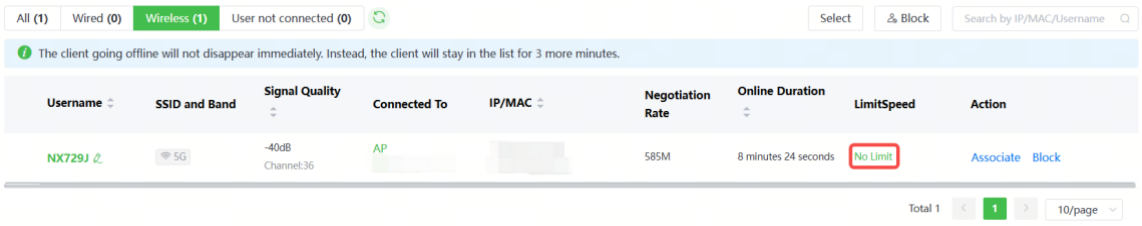
To ensure fair resource allocation, the network administrator can implement wireless rate limiting to prevent some users or devices from occupying a large amount of bandwidth and affecting the network experience of other users.

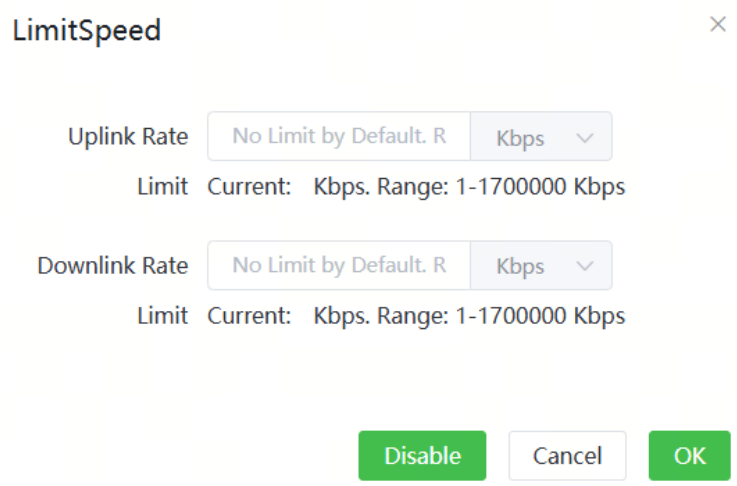
Note

Rate limiting applies only to wireless clients.

- Configure rate limits for clients

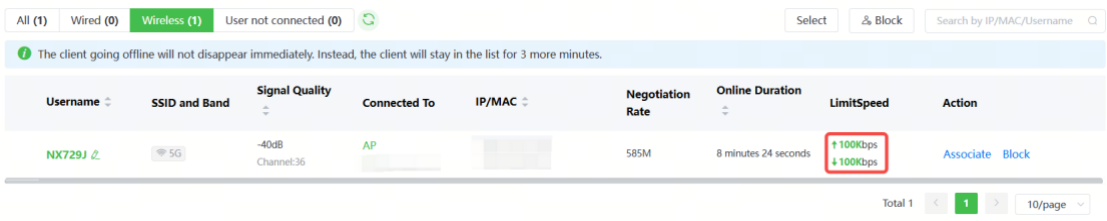
  Click the **Wireless** tab, click the **LimitSpeed** column in the table, set the uplink rate limit and downlink rate limit, and click **OK**.

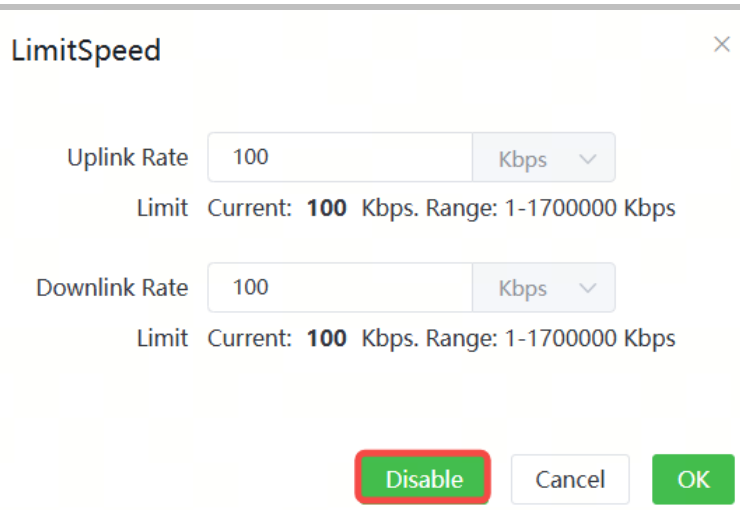




- Cancel rate limits

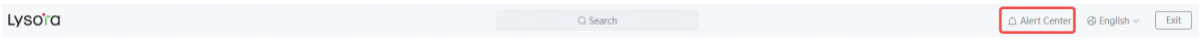
  Click the **Wireless** tab, click the **LimitSpeed** column in the table, and click **Disable**.





3.6 Alerts

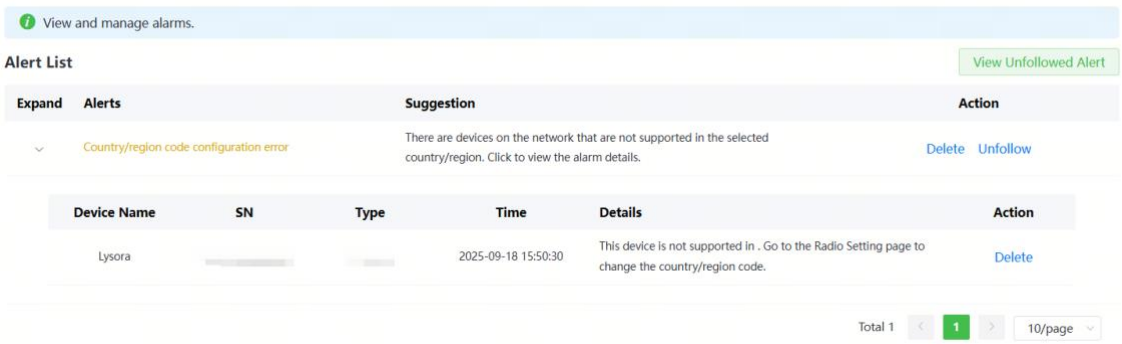
When a network exception occurs, the network overview page will display an alert and provide a suggestion. Click an alert in the **Alert Center** to view the faulty device, problem details, and description. You can troubleshoot the fault based on the suggestion.

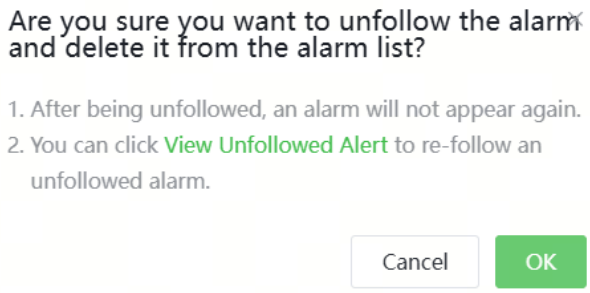


The **Alert List** page displays possible problems on the network environment and device. All types of alarms are followed by default. You can click **Unfollow** in the **Action** column to unfollow this type of alarm.

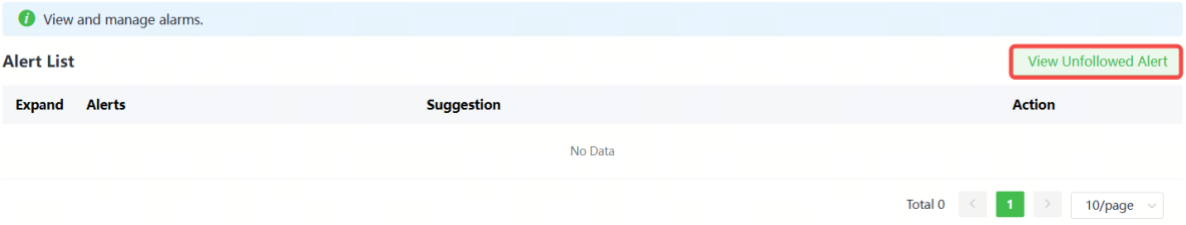
Caution

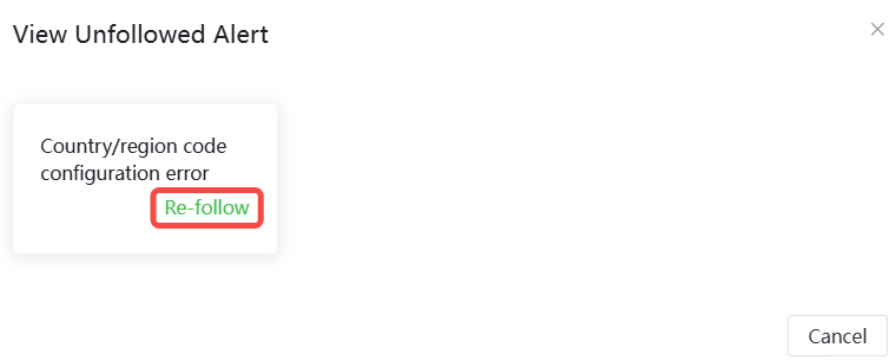
After unfollowing a specified alert type, you will not discover and process all alerts of this type promptly. Therefore, exercise caution when performing this operation.





Click **View Unfollowed Alert** to view the unfollowed alert. You can follow the alert again in the pop-up window.



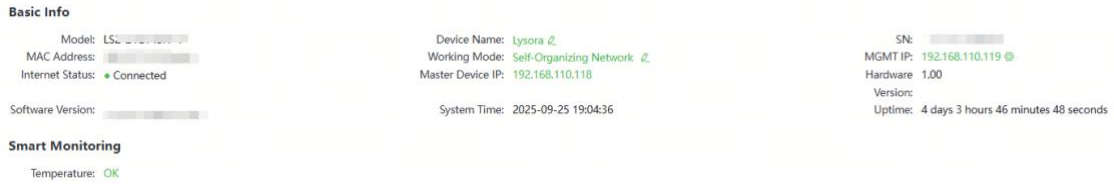


4 One-Device Information

4.1 Basic information about the One-Device

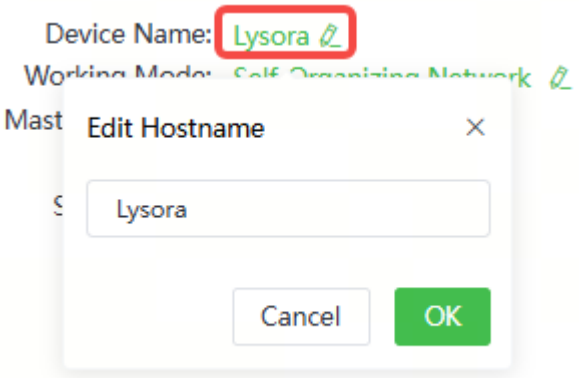
Choose **Local Device** > **Device Overview** > **Basic Info**.

Basic information includes device name, device model, SN number, software version, management IP, MAC address, networking status, system time, working mode, etc.



4.1.1 Setting the device name

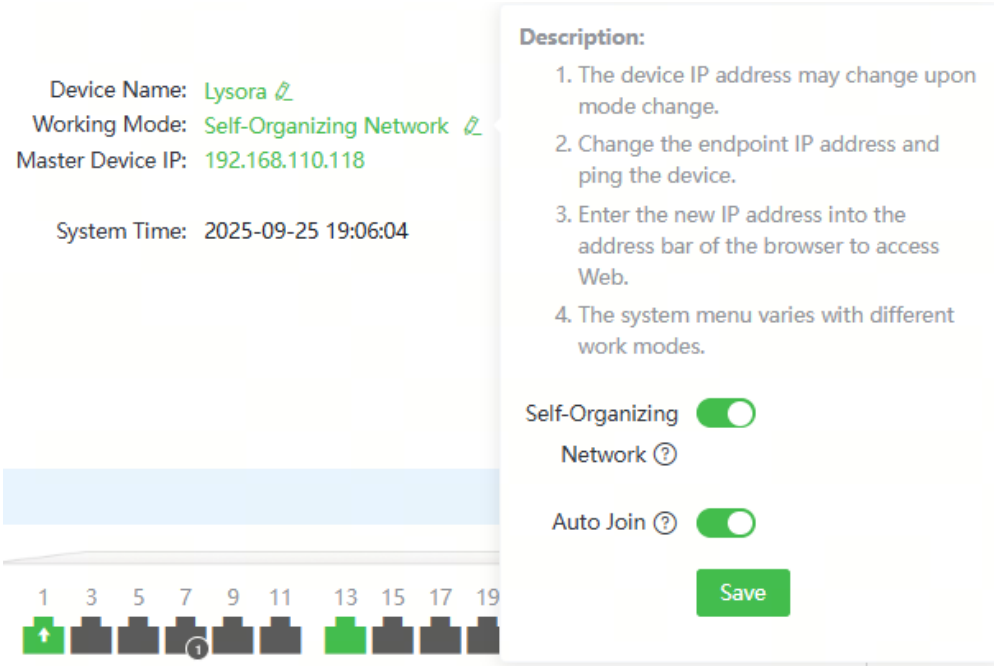
Click the device name to modify the device name in order to distinguish between different devices.



4.1.2 Switching the Work Mode

Click the current work mode to change the work mode. When you toggle on **Self-Organizing Network** on a device, you can toggle on or off **Auto Join** as required. When **Auto Join** is toggled on, and the Lysora gateway and AC function as the primary devices, any device in factory status within the network will automatically join the network. When

Auto Join is toggled off, the device in factory status within the network cannot automatically join the network.



4.1.3 Setting MGMT IP

Click current management IP address to jump to the management IP configuration page. For more information, see 7.6 MGMT IP Configuration.

4.2 Smart Monitoring

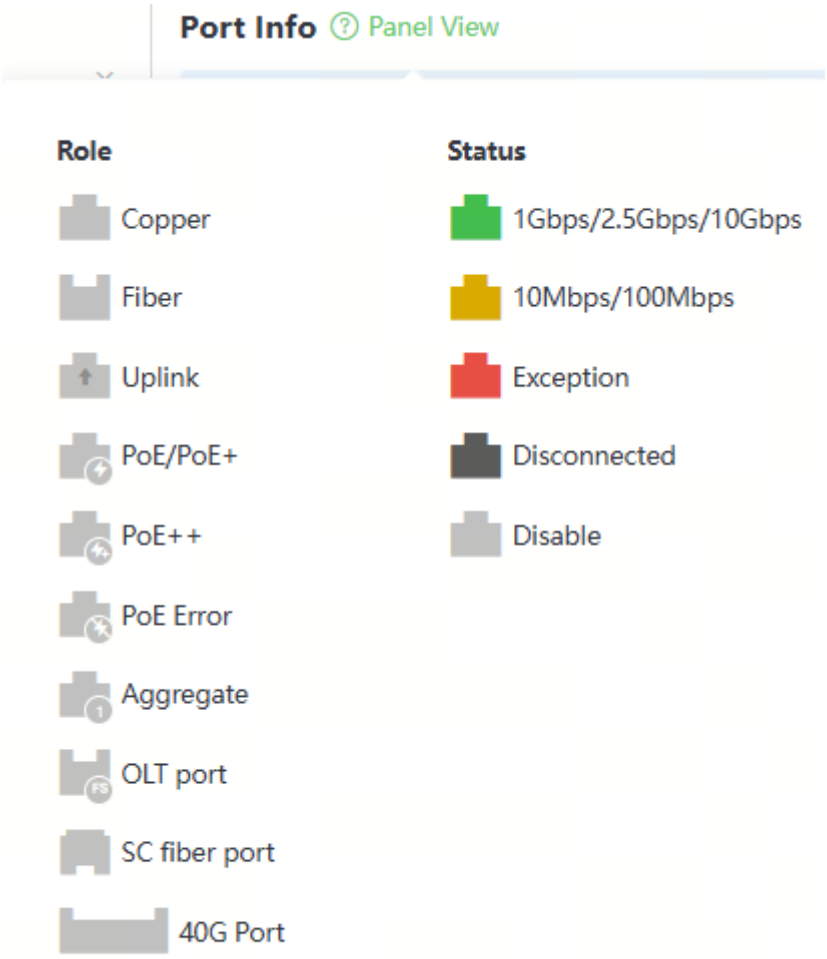
Choose **Local Device** > **Device Overview** > **Smart Monitoring**.

Display the current hardware operating status of the device, such as the device temperature.

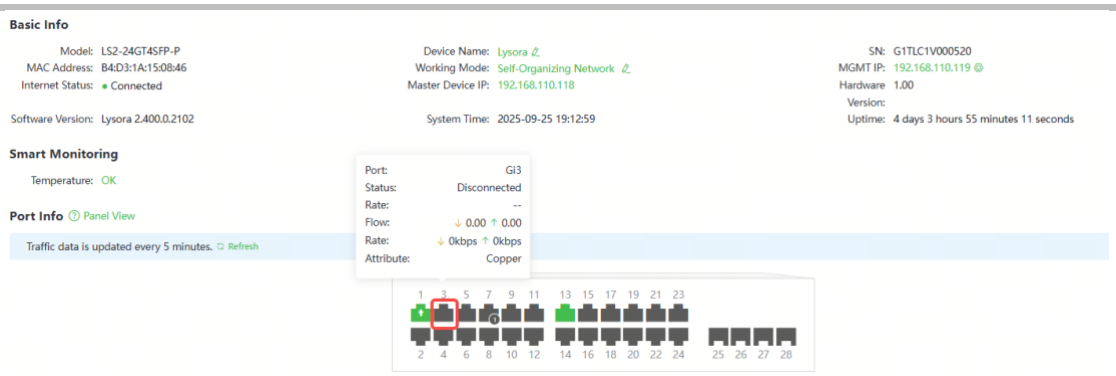
4.3 Port Info

Choose **Local Device** > **Device Overview** > **Port Info**.

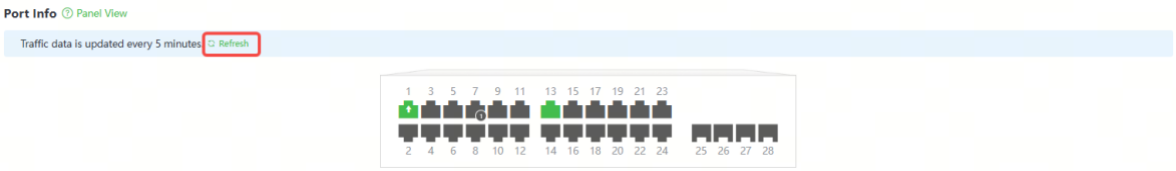
- The port info page displays the details of all ports currently on the switch. Click **Panel View** to view the port roles and statuses corresponding to port icons of different colors or shapes.



- Move the cursor to the icon of a port (for example, Gi1) on the port panel, and more information about the port will be displayed, including the port ID, port status, port rate, uplink and downlink traffic, transmission rate, and optical/electrical attribute of the port.



- Traffic data is automatically updated every five minutes. You can click **Refresh** above the port panel to obtain the latest port traffic and status information simultaneously.



5 VLAN

5.1 VLAN Overview

A virtual local area network (VLAN) is a logical network created on a physical network. A VLAN has the same properties as a normal physical network except that it is not limited by its physical location. Each VLAN has an independent broadcast domain. Different VLANs are Layer 2-isolated. Layer 2 unicast, broadcast, and multicast frames are forwarded and spread within one VLAN and will not be transmitted to other VLANs.

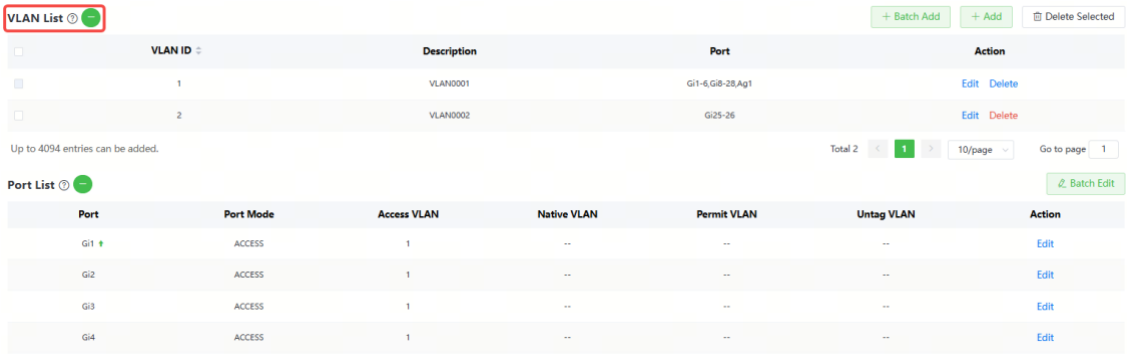
When a port is defined as a member of a VLAN, all clients connected to the port are a part of the VLAN. A network supports multiple VLANs.

VLAN division includes two functions: creating VLANs and setting port VLANs.

5.2 Configuring a VLAN

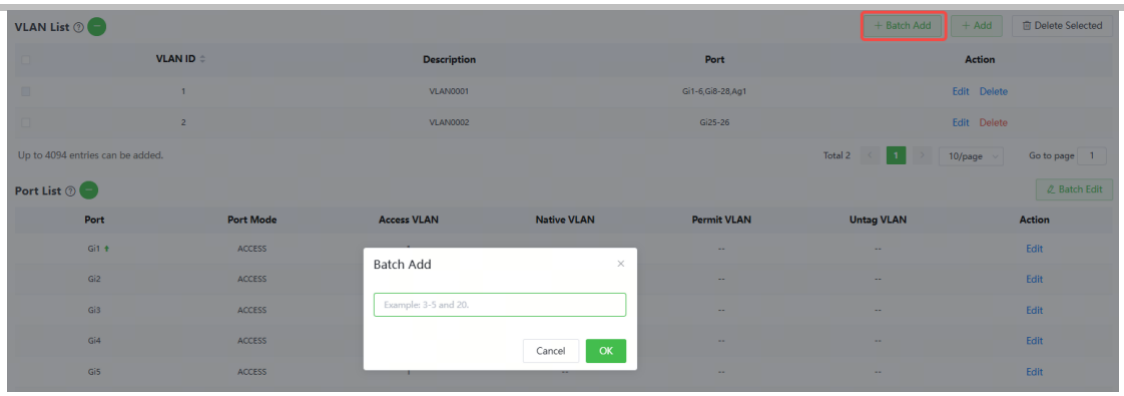
Choose **Local Device** > **VLAN** > **VLAN List**.

The VLAN list contains all the existing VLAN information. You can modify or delete the existing VLAN, or create a new VLAN.

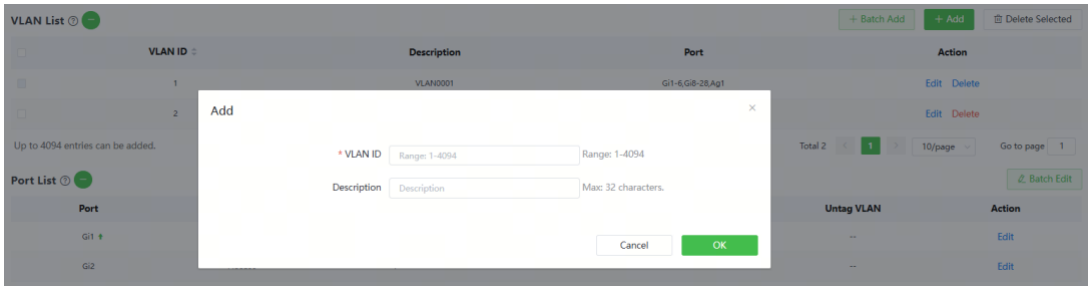


5.2.1 Adding a VLAN

- Create multiple VLANs: Click **Batch Add**. In the displayed dialog box, enter VLAN ID range (separate multiple VLAN ID ranges with commas (,)), and click **OK**. The VLANs added will be displayed in **VLAN List**.



- Create a VLAN: Click **Add**. Enter the VLAN ID and description for the VLAN, and click **OK**. The VLAN added will be displayed in **VLAN List**.

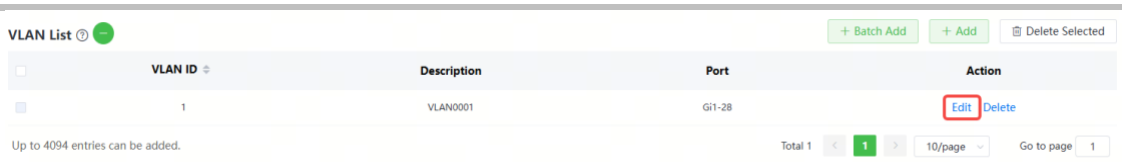


Note

- The range of a VLAN ID is from 1 to 4094.
- You can separate multiple VLANs to be added in batches with commas (,), and separate the start and end VLAN IDs of a VLAN range with a hyphen (-).
- If no VLAN description is configured when the VLAN is added, the system automatically creates a VLAN description in the specified format, for example, VLAN000XX. The VLAN descriptions of different VLANs must be unique.
- If resources are insufficient, a message indicating resource insufficiency for VLAN will be displayed.

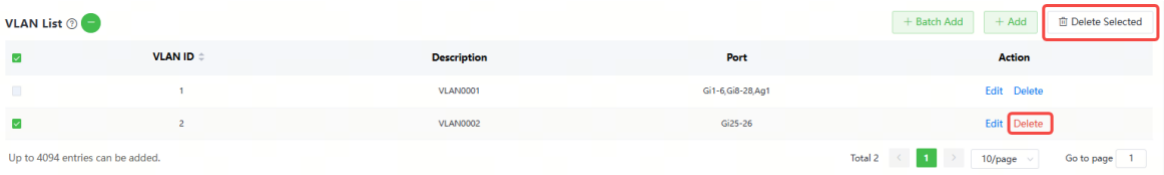
5.2.2 Modifying the VLAN Description

In **VLAN List**, Click **Edit** in the last **Action** column to modify the description information of the specified VLAN.



5.2.3 Deleting a VLAN

- Batch deletion: In **VLAN List**, select the VLAN entries to be deleted and click **Delete Selected** to delete VLANs in a batch.
- Deleting a VLAN: In **VLAN List**, click **Delete** in the last **Action** column to delete the specified **VLAN**.



Note

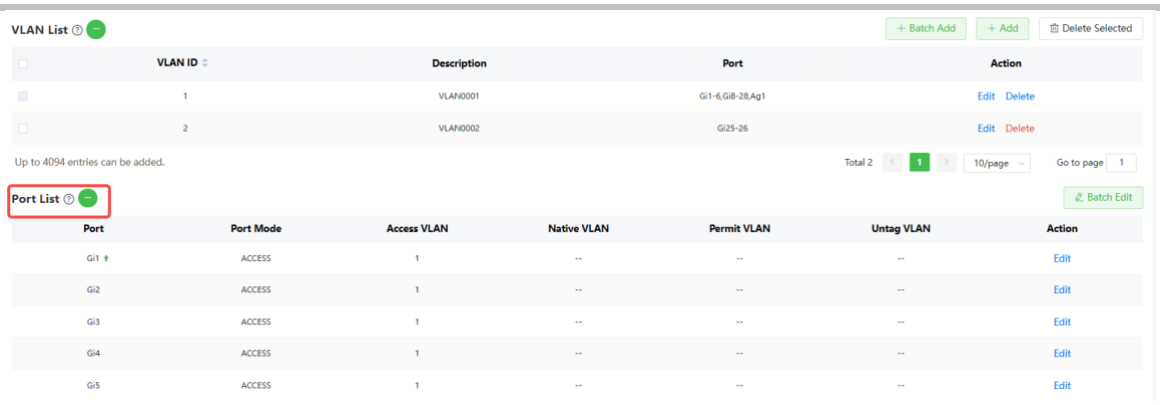
The default VLAN (VLAN 1), management VLAN, native VLAN, and access VLAN cannot be deleted. For these VLANs, the **Delete** button is unavailable in gray.

5.3 Configuring a Port VLAN

5.3.1 Overview

Choose **Local Device** > **VLAN** > **Port List**.

Port List displays the VLAN division of the current port. Create VLANs in **VLAN List** page (see 5.2 Configuring a VLAN) and then configure the port based on the VLANs.



You can configure the port mode and VLAN members for a port to determine VLANs that are allowed to pass through the port and whether packets to be forwarded by the port carry the tag field.

Table 5-1 Port Modes Description

Port mode	Function
Access port	One access port can belong to only one VLAN and allow only frames from this VLAN to pass through. This VLAN is called an access VLAN. Access VLAN has attributes of both Native VLAN and Permitted VLAN The frames sent from the Access port do not carry tags. When the access port receives an untagged frame from a peer device, the local device determines that the frame comes from the Access VLAN and adds the access VLAN ID to the frame.
Trunk port	One trunk port supports one native VLAN and several allowed VLANs. Native VLAN frames forwarded by a trunk port do not carry tags while allowed VLAN frames forwarded by the trunk port carry tags. A trunk port belongs to all VLANs of the device by default, and can forward frames of all VLANs. You can set the allowed VLAN range to limit VLAN frames that can be forwarded. Note that the trunk ports on both ends of the link must be configured with the same Native VLAN.
Hybrid port	A hybrid port supports one native VLAN and several allowed VLANs. The allowed VLANs are divided into Tag VLAN and Untagged VLAN. The frames

Port mode	Function
	forwarded by the hybrid port from a Tag VLAN carry tags, and the frames forwarded by the hybrid port from an Untagged VLAN do not carry tags. The frames forwarded by the hybrid port from Native VLAN must not carry tags, therefore Native VLAN can only belong to Untagged VLAN List.

Note

Whether the hybrid mode function is supported depends on the product version.

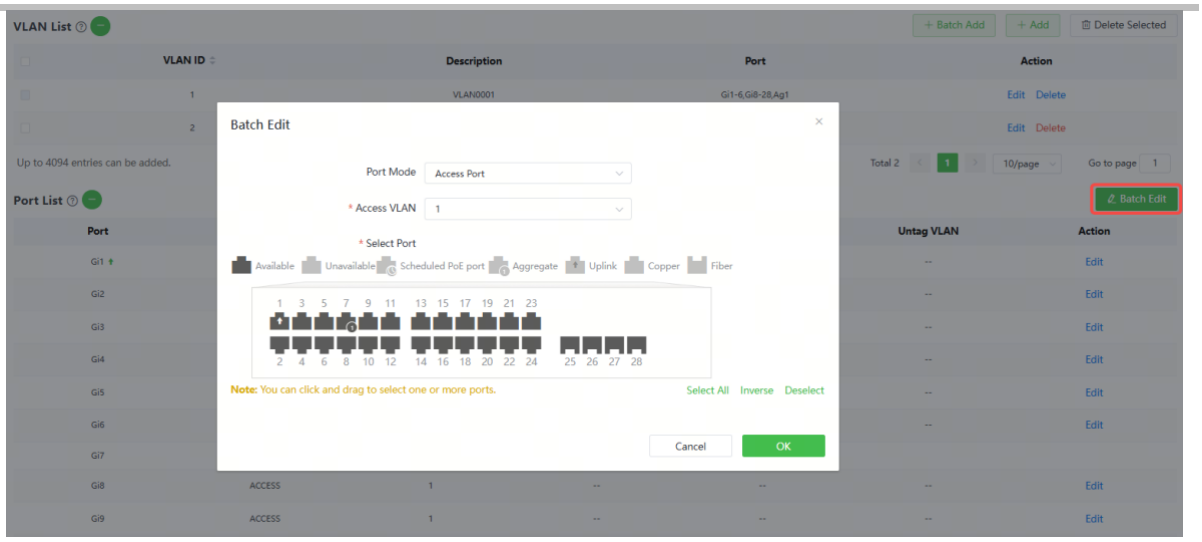
5.3.2 Procedure

Choose **Local Device** > **VLAN** > **Port List**.

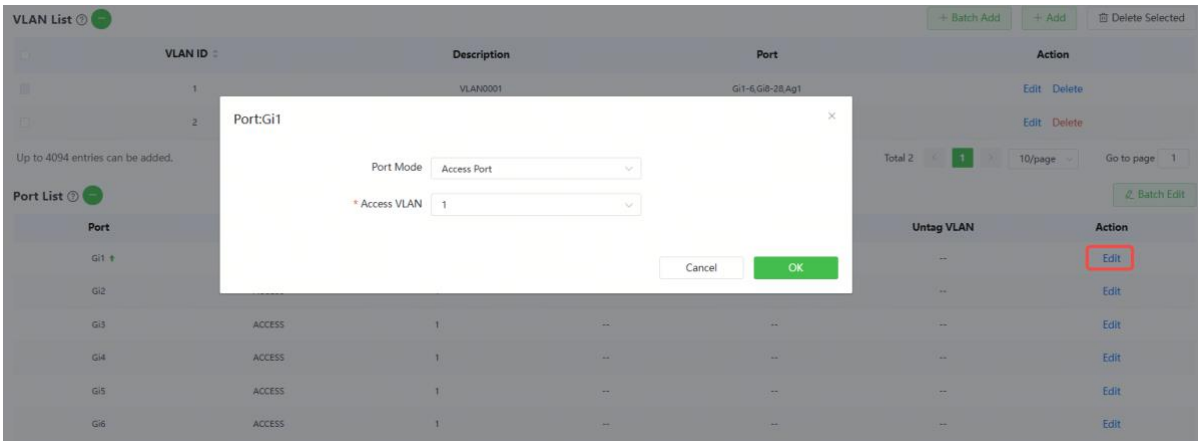
Configure port VLANs in a batch: Click **Batch Edit**, select the port to be configured on the port panel, and select the port mode. If the port mode is Access port, you need to select Access VLAN; if the port mode is Trunk port, you need to select Native VLAN and enter the allowed VLAN ID range; if the port mode is Hybrid port, you need to select Native VLAN and enter the allowed VLAN range and Untagged VLAN range. Click **OK** to complete the batch configuration.

Note

In Hybrid mode, the allowed VLANs include Tag VLAN and Untagged VLAN, and the Untagged VLAN range must include Native VLAN.



Configure one port: In **Port List**, click **Edit** in the last **Action** column of a specified port, configure the port mode and corresponding VLAN, and click **OK**.



Note

- VLAN ID range is from 1 to 4094, among which VLAN 1 is the default VLAN that cannot be deleted.
- When hardware resources are insufficient, the system displays a VLAN creation failure message.
- Improper configuration of VLANs on a port (especially uplink port) may cause the failure to log in to the web page. Therefore, exercise caution when configuring VLANs.

5.4 Batch Switch Configuration

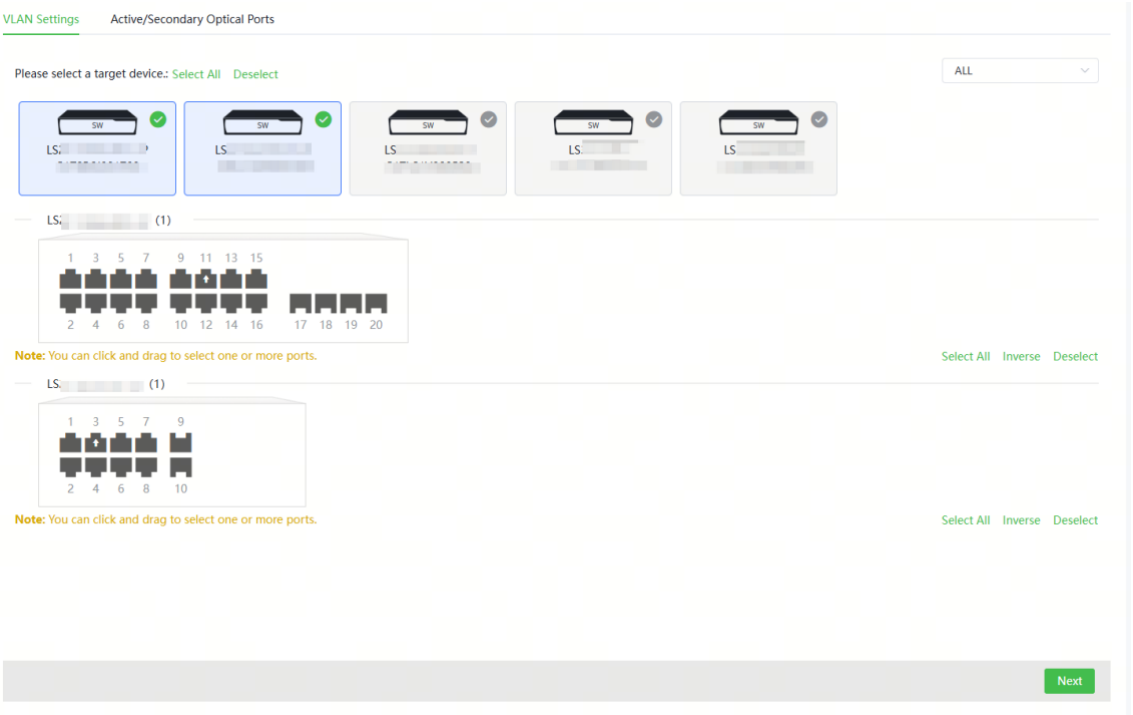
5.4.1 Overview

You can batch create VLANs, configure port attributes, and divide port VLANs for switches on the network.

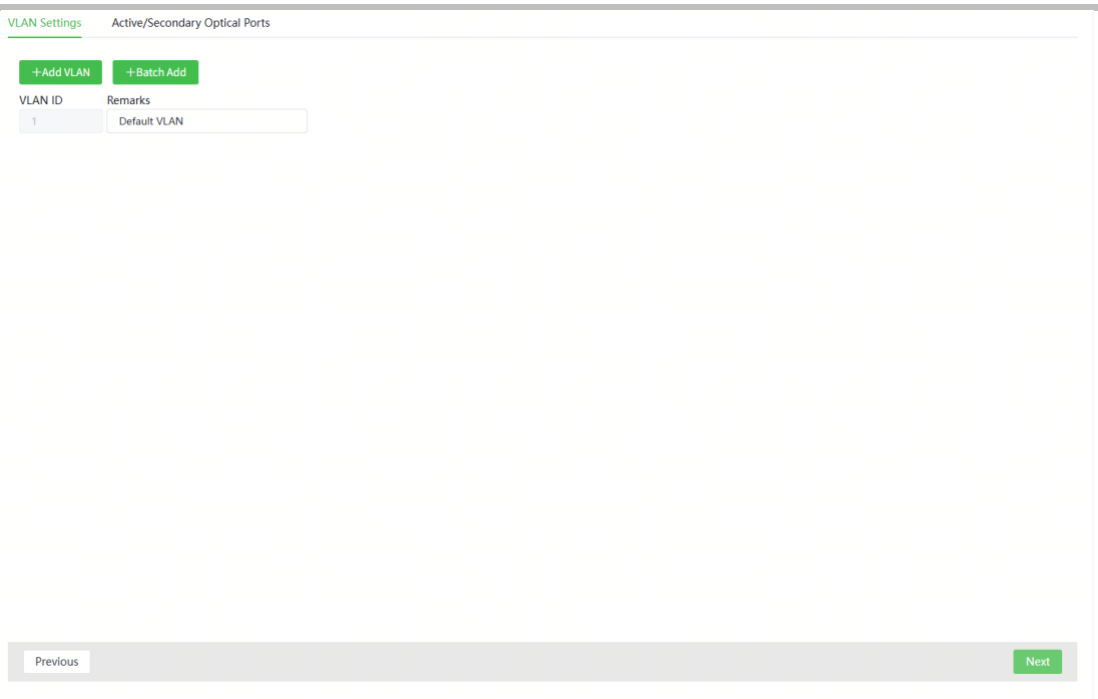
5.4.2 Procedure

Choose **Network** > **Batch Config**. Choose **Network-Wide > Workspace** > **Wired** > **SW Config**.

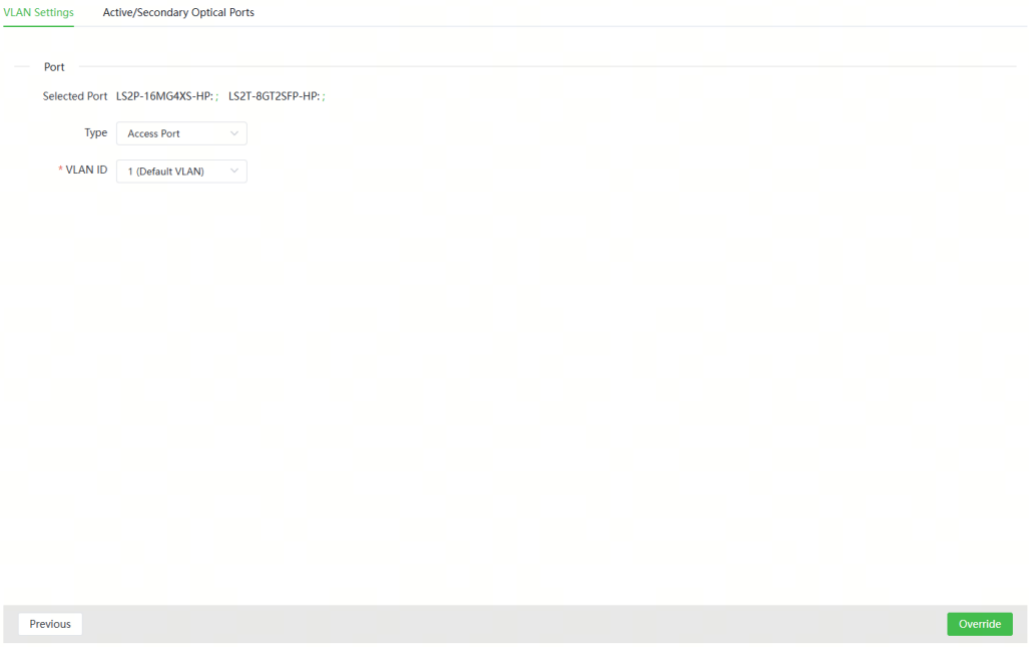
(1) The page displays all switches in the current network. Select the switches to configure, and then select the desired ports in the device port view that appears below. If there are a large number of devices in the current network, select a product model from the drop-down list box to filter the devices. After the desired devices and ports are selected, click **Next**.



(2) Click **Add VLAN** to create a VLAN for the selected devices in a batch. If you want to create multiple VLANs, click **Batch Add** and enter the VLAN ID range, such as 3-5,100. After setting the VLANs, click **Next**.

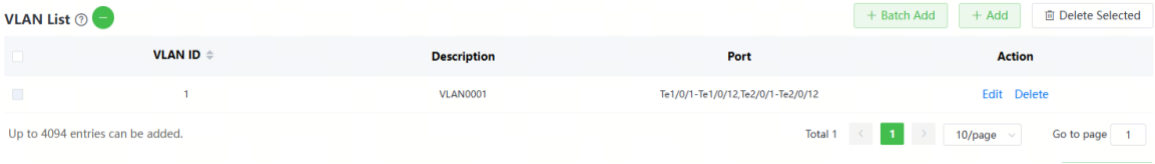


(3) Configure port attributes for the ports selected in Step 1 in a batch. Select a port type. If you set **Type** to **Access Port**, you need to configure **VLAN ID**. If you set **Type** to **Trunk Port**, you need to configure **Native VLAN** and **Permitted VLAN**. After setting the port attributes, click **Override** to deliver the batch configurations to the target devices.



5.4.3 Verifying Configuration

Choose **Local Device** > **VLAN** > **VLAN List**. View the VLAN and port information of switches to check whether the batch configurations are successfully delivered.



6 Monitor

6.1 Port Flow

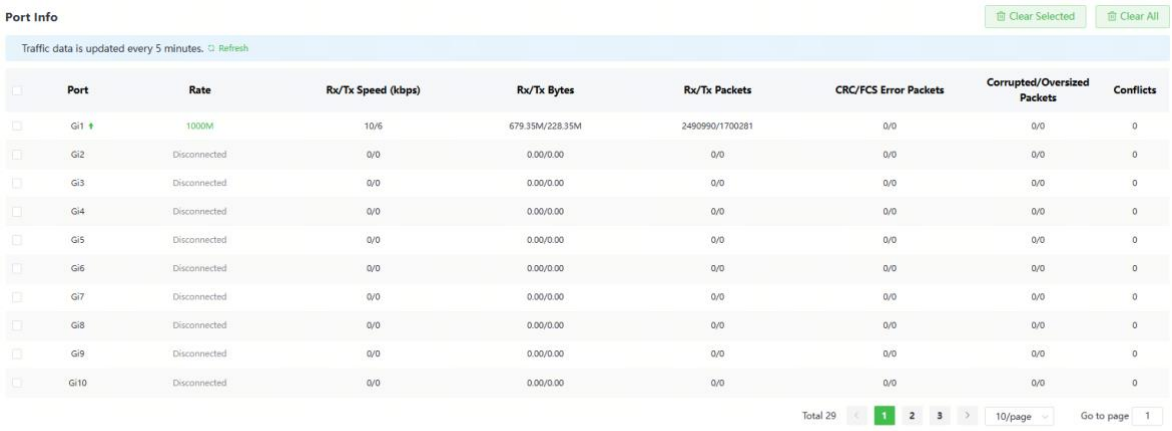
Choose **Local Device** > **Monitor** > **Port Flow**.

Display traffic statistics such as the rate of the device port, the number of sent and received packets, and the number of error packets. The rate of the port is updated every five seconds. Other traffic statistics are updated every five minutes.

Select a port and click **Clear Selected**, or click **Clear All** to clear statistics such as current port traffic and start statistics collection again.

Note

Aggregate ports can be configured. Traffic of an aggregate interface is the sum of traffic of all member ports.



6.2 Client Management

6.2.1 Overview

A MAC address table records mappings of MAC addresses and interfaces to virtual local area networks (VLANs).

A device queries the MAC address table based on the destination MAC address in a received packet. If the device finds an entry that is consistent with the destination MAC Address in the packet, the device forwards the packet through the interface corresponding to the entry in unicast mode. If the device does not find such an entry, it forwards the packet through all interfaces other than the receiving interface in broadcast mode.

MAC address entries are classified into the following types:

- Static MAC address entries: Manually configured by the user. Packets whose destination MAC address matches the one in such an entry are forwarded through the correct interface. This type of entries does not age.
- Dynamic MAC address entries: Automatically generated by devices. Packets whose destination MAC address matches the one in such an entry are forwarded through the correct interface. This type of entries ages.
- Filtering MAC address entries: Manually configured by the user. Packets whose source or destination MAC address matches the one in such an entry are discarded. This type of entries does not age.

Note

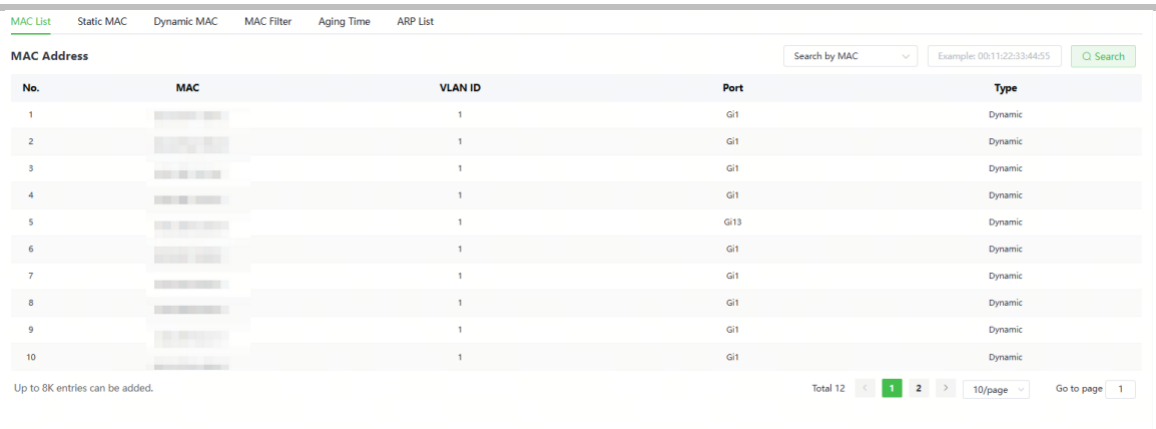
This section describes the management of static, dynamic, and filtering MAC address entries, without involving multicast MAC address entries.

6.2.2 Displaying the MAC Address Table

Choose **Local Device** > **Monitor** > **Clients Management** > **MAC List**.

Displays the MAC address information of the device, including the static MAC address manually set by the user, the filtering MAC address, and the dynamic MAC address automatically learned by the device.

Querying MAC address entries: Support querying MAC address entries based on MAC address, VLAN ID or port. Select the search type, enter the search string, and click **Search**. MAC entries that meet the search criteria are displayed in the list. Support fuzzy search.

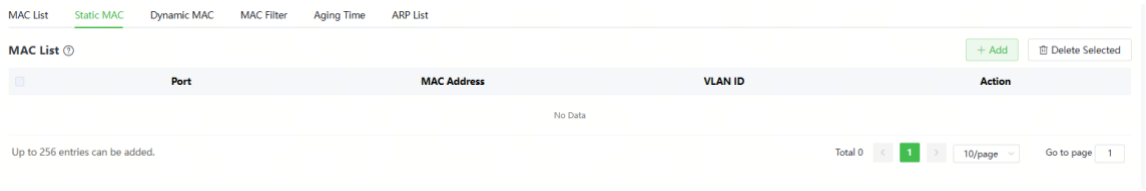


Note

The MAC address entry capacity depends on the product. For example, the MAC address entry capacity of the device shown in the figure above is 16K.

6.2.3 Configuring Static MAC Binding

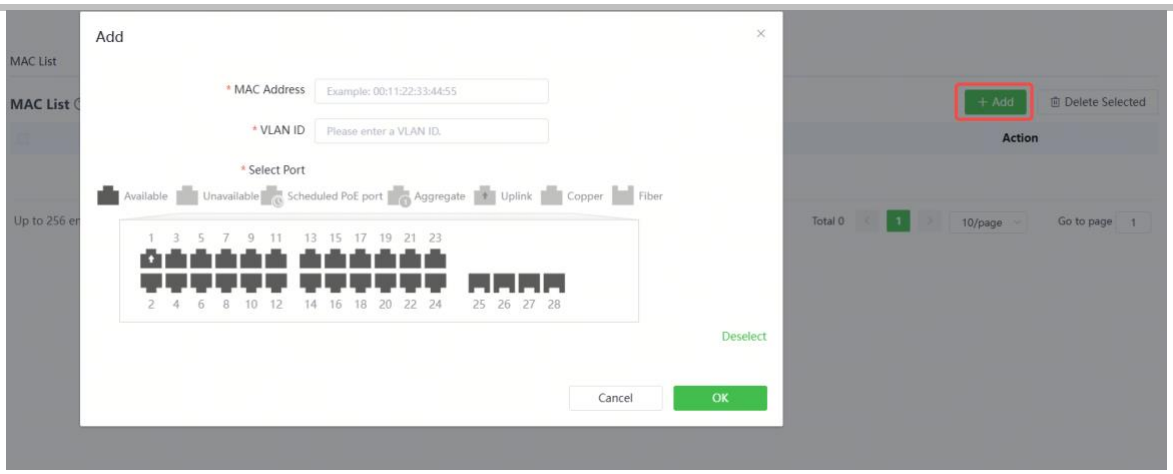
The switch forwards data based on the MAC address table. You can set a static MAC address entry to manually bind the MAC address of a downlink network device with the port of the device. After a static address entry is configured, when the device receives a packet destined to this address from the VLAN, it will forward the packet to the specified port. For example, when 802.1X authentication is enabled on the port, you can configure static MAC address binding to implement authentication exemption.



1. Adding Static MAC Address Entries

Choose **Local Device** > **Monitor** > **Clients Management** > **Static MAC**.

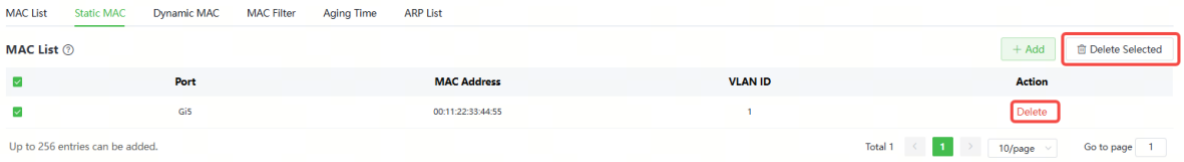
Click **Add**, enter the MAC address and VLAN ID, select the port for packet forwarding, and click **OK**. After the addition is successful, the MAC address table will update the entry data.



2. Deleting Static MAC Address Entries

Choose **Local Device** > **Monitor** > **Clients Management** > **Static MAC**.

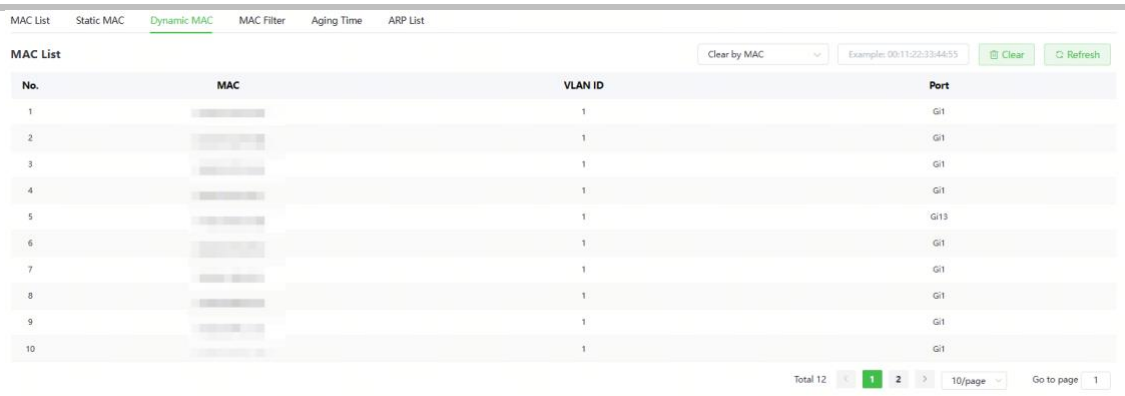
- Batch deletion: In **MAC List**, select the MAC address entries to be deleted and click **Delete Selected**. In the displayed dialog box, click **OK**.
- Deleting an entry: In **MAC List**, find the entry to be deleted, click **Delete** in the last **Action** column. In the displayed dialog box, click **OK**.



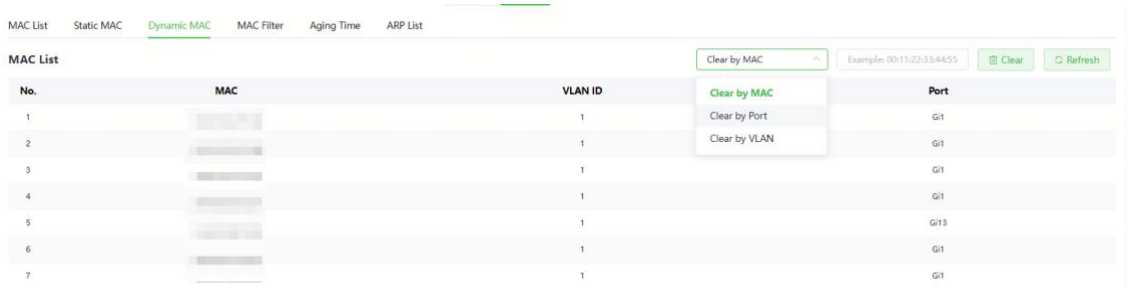
6.2.4 Displaying Dynamic MAC Addresses

Choose **Local Device** > **Monitor** > **Clients Management** > **Dynamic MAC**.

After receiving the packet, the device will automatically generate dynamic MAC address entries based on the source MAC address of the packet. The current page displays the dynamic MAC address entries learned by the device. Click **Refresh** to obtain the latest dynamic MAC address entries.

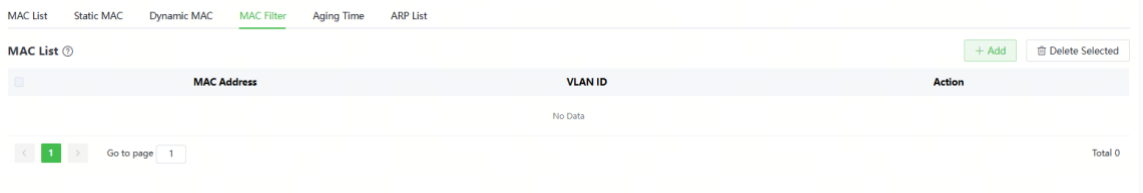


Delete dynamic MAC address: Select the clear type (by MAC address, by VLAN, or by port), enter a string for matching the dynamic MAC address entry, and click **Clear**. The device will clear MAC address entries that meet the conditions.



6.2.5 Configuring MAC Address Filtering

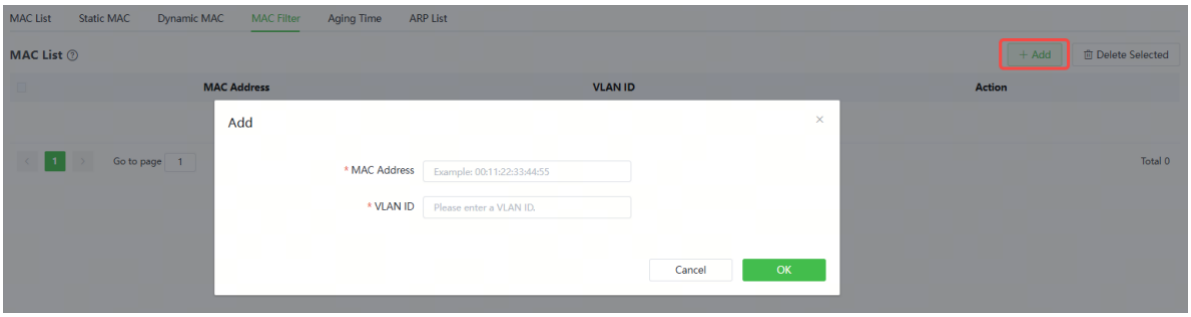
To prohibit a user from sending and receiving packets in certain scenarios, you can add the MAC address of the user to a filtering MAC address entry. After the entry is configured, packets whose source or destination MAC address matches the MAC address in the filtering MAC address entry are directly discarded. For example, if a user initiates ARP attacks, the MAC address of the user can be configured as a to-be-filtered address to prevent attacks.



1. Adding Filtering MAC Addresses

Choose **Local Device** > **Monitor** > **Clients Management** > **MAC Filter**.

Click **Add**. In the dialog box that appears, enter the MAC addresses and VLAN ID, and then click **OK**.



2. Deleting Filtering MAC Addresses

Choose **Local Device** > **Monitor** > **Clients Management** > **MAC Filter**.

- Batch deletion: In **MAC List**, select the MAC address entries to be deleted and click **Delete Selected**. In the displayed dialog box, click **OK**.
- Deleting an entry: In **MAC List**, find the entry to be deleted, click **Delete** in the last **Action** column. In the displayed dialog box, click **OK**.

6.2.6 Configuring Aging Time for MAC Addresses

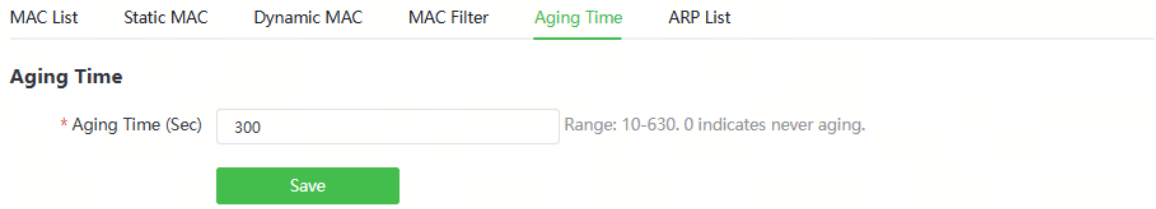
Set the aging time of dynamic MAC address entries learned by the device. Static MAC address entries and filtering MAC address entries do not age.

The device deletes useless dynamic MAC address entries based on the aging time to save entry resources on the device. An overly long aging time may lead to untimely deletion of useless entries, whereas an overly short aging time may lead to deletion of some valid entries and repeated learning of MAC addresses by the device, which increases the packet broadcast frequency. Therefore, you are advised to configure a

proper aging time of dynamic MAC address entries as required to save device resources without affecting network stability.

Choose **Local Device** > **Monitor** > **Clients Management** > **Aging Time**.

Enter valid aging time and click **Save**. The value range of the aging time is from 10 to 630, in seconds. The value 0 specifies no aging.



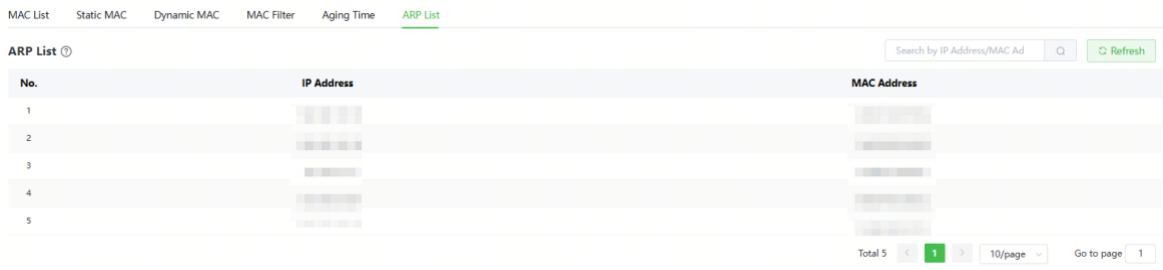
6.2.7 Displaying ARP Information

Choose **Local Device** > **Monitor** > **Clients Management** > **ARP List**.

When two IP-based devices need to communicate with each other, the sender must know the IP address and MAC address of the peer. With MAC addresses, an IP-based device can encapsulate link-layer frames and then send data frames to the physical network. The process of obtaining MAC addresses based on IP addresses is called address resolution.

The Address Resolution Protocol (ARP) is used to resolve IP addresses into MAC addresses. ARP can obtain the MAC Address associated with an IP address. ARP stores the mappings between IP addresses and MAC addresses in the ARP cache of the device.

The device learns the IP address and MAC address of the network devices connected to its interfaces and generates the corresponding ARP entries. The **ARP List** page displays ARP entries learned by the device. The ARP list allows you search for specified ARP entries by IP or MAC address. Click **Refresh** to obtain the latest ARP entries.



7 Ports

7.1 Overview

Ports are important components for data exchange on network devices. The port management module allows you to configure basic settings for ports, and configure port aggregation, switched port analyzer (SPAN), port rate limiting, management IP address, etc.

Table 1-1 Description of Port Type

Port Type	Note	Remarks
Switch port	A switch port consists of a single physical port on the device and provides only the Layer 2 switching function. Switch ports are used to manage physical port and their associated Layer 2 protocols.	Described in this section
Layer 2 aggregate interface	An Interface binds multiple physical members to form a logical link. For Layer 2 switching, an aggregate interface is like a high-bandwidth switch port. It can combine the bandwidths of multiple ports to expand link bandwidth. In addition, for frames sent through a Layer 2 aggregate interface, load balancing is performed on member ports of the Layer 2 aggregate interface. If one member link of the aggregate interface fails, the Layer 2 aggregate interface automatically transfers traffic on this link to other available member links, improving connection reliability.	Described in this section

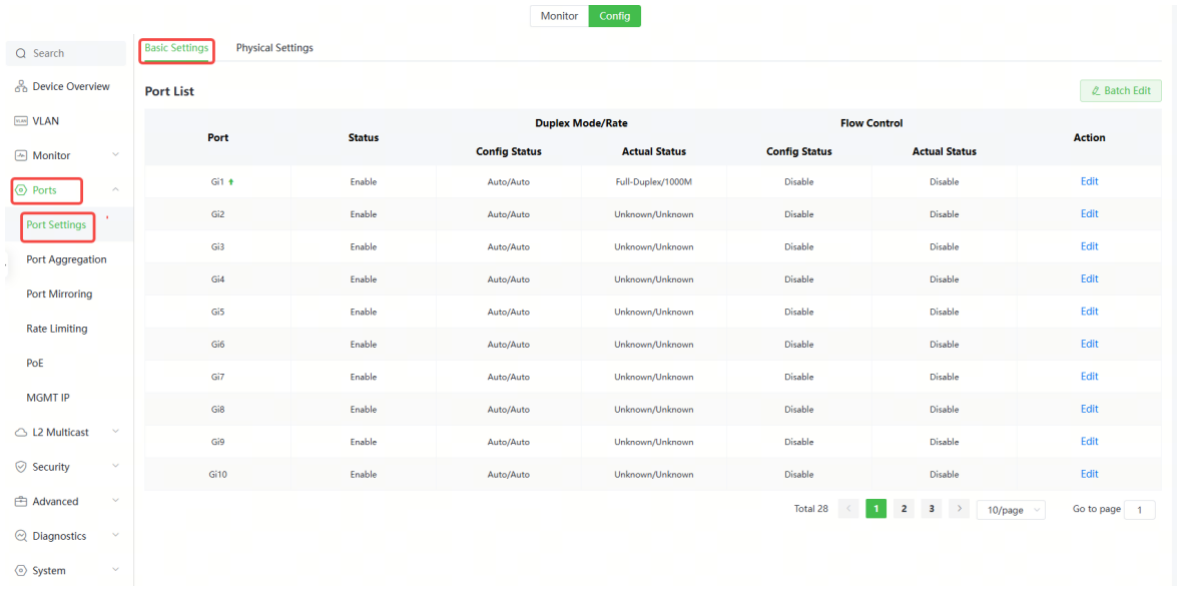
7.2 Port Configuration

Port configuration includes common attributes such as basic settings and physical settings of the port. Users can adjust the port rate, set port switch, duplex mode, flow control mode, energy efficient Ethernet switch, port media type and MTU, etc.

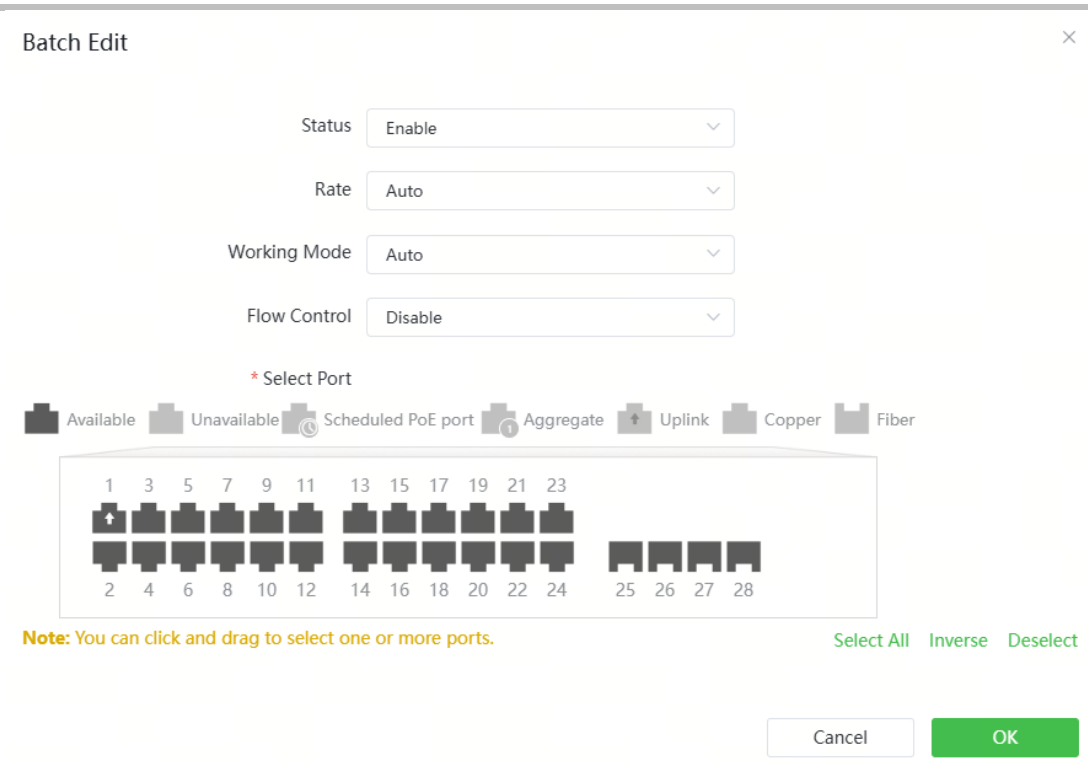
7.2.1 Basic Settings

Choose **Local Device** > **Ports** > **Port Settings** > **Basic Settings**.

Support setting whether to enable the port, the speed and duplex mode of the port, and the flow control mode, and display the current actual status of each port.



- Batch configure: Click **Batch Edit**, select the port to be configured In the displayed dialog box, select the port switch, rate, work mode, and flow control mode, and click **OK** to deliver the configuration. In batch configuration, optional configuration items are a common collection of selected ports (that is, attributes supported the selected ports).



- Configure one port: In **Port List**, select a port entry and click **Edit** in the **Action** column. In the displayed dialog box, select port status, rate, work mode, and flow control mode, and click **OK**.

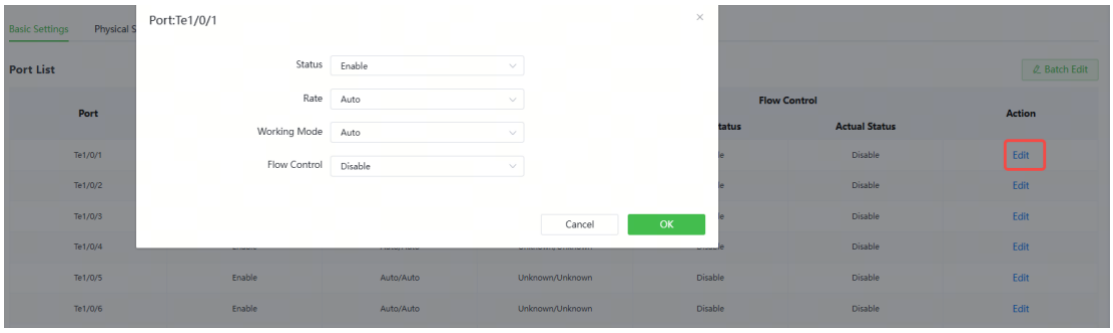


Table 7-1 Description of Basic Port Configuration Parameters

Parameter	Description	Default Value
Status	If a port is closed, no frame will be received and sent on this port, and the corresponding data processing function will be lost.	Enable

Parameter	Description	Default Value
Rate	Set the rate at which the Ethernet physical interface works. Set to Auto means that the port rate is determined by the auto-negotiation between the local and peer devices. The negotiated rate can be any rate within the port capability.	Auto
Work Mode	● Full duplex: realize that the port can receive packets while sending. ● Half duplex: control that the port can receive or send packets at a time. ● Auto: the duplex mode of the port is determined through auto negotiation between the local port and peer port	Auto
Flow Control	After flow control is enabled, the port will process the received flow control frames, and send the flow control frames when congestion occurs on the port.	Disable

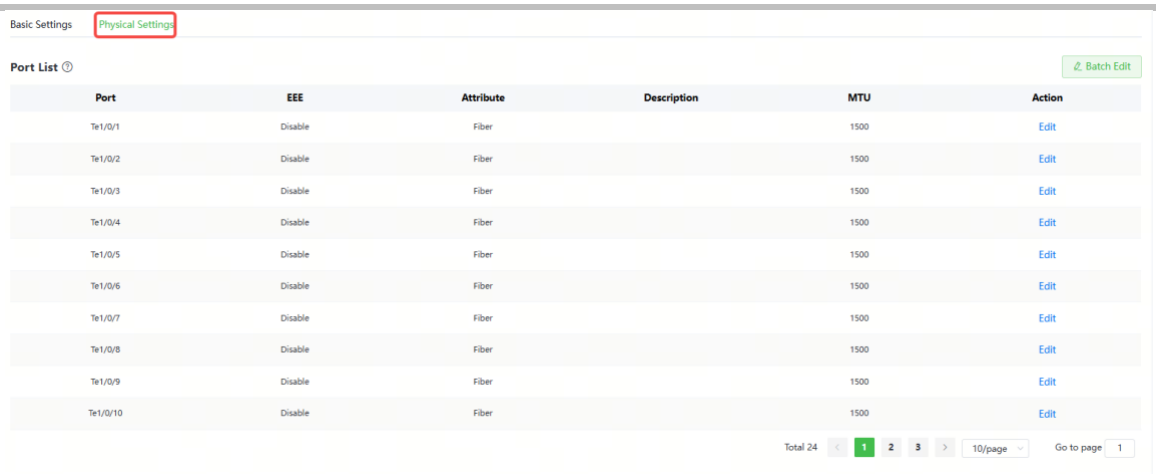
Note

The rate of a GE optical port can be set to **1000M**, **100M**, or **Auto**. The rate of a GE electrical port can be set to **1000M**, **100M**, **10M**, or **Auto**. The rate of a 10GE port can be set to **1000M** or **Auto**.

7.2.2 Physical Settings

Choose **Local Device** > **Ports** > **Port Settings** > **Physical Settings**.

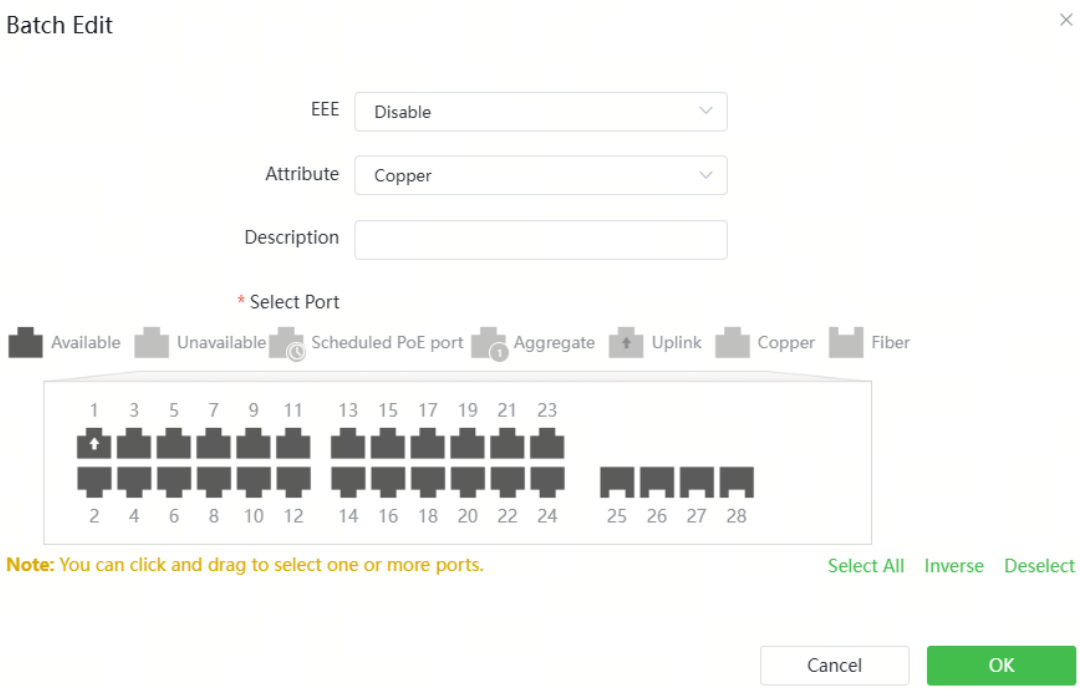
Support to enable the energy-efficient Ethernet (EEE) function of the port, and set the media type and MTU of the port.



- Batch configure: Click **Batch Edit**. In the displayed dialog box, select the port to be configured, configure the EEE switch, MTU, enter the port description, and click **OK**.

Note

Copper ports and SFP ports cannot be both configured during batch configuration.



- Configure one port: Click **Edit** in the **Action** column of the list. In the displayed configuration box, configure the EEE switch, port mode, enter the port description, and click **OK**.

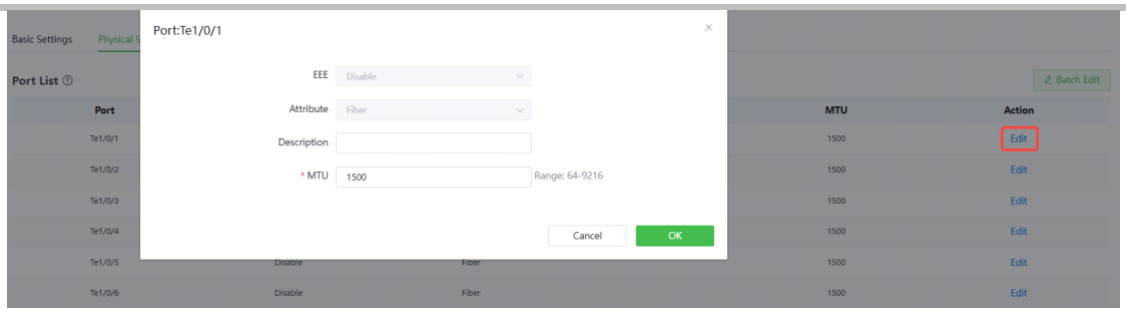


Table 7-2 Description of Physical Configuration Parameters

Parameter	Description	Default Value
EEE	It is short for energy-efficient Ethernet, which is based on the standard IEEE 802.3az protocol. When enabled, EEE saves energy by making the interface enter LPI (Low Power Idle) mode when the Ethernet connection is idle. Value: Disable/Enable	Disable
Attribute	The port attribute indicates whether the port is a copper port or an SFP port. Copper port: copper mode (cannot be changed); SFP port: fiber mode (cannot be changed); Only combo ports support mode change.	Depending on the port attribute
Description	You can add a description to label the functions of a port.	NA
MTU	MTU (Maximum Transmission Unit) is used to notify the peer of the acceptable maximum size of a data service unit. It indicates the size of the payload acceptable to the sender. You can configure the MTU of a port to limit the length of	1500

Parameter	Description	Default Value
	a frame that can be received or forwarded through this port.	

Note

- Different ports support different attributes and configuration items.
- Only the SFP combo ports support port mode switching.
- SFP ports do not support enabling EEE.

7.3 Aggregate Interfaces

7.3.1 Aggregate Interface Overview

An aggregate interface is a logical link formed by binding multiple physical links. It is used to expand link bandwidth, thereby improving connection reliability.

This function supports load balancing and therefore, evenly distributes traffic to member links. It implements link backup. When a member link of an aggregate interface is disconnected, the system automatically distributes traffic of this link to other available member links. Broadcast or multicast packets received by one member link of an aggregate interface are not forwarded to other member links.

- If a single interface that connects two devices supports the maximum rate of 1000 Mbps (assume that interfaces of both devices support the rate of 1000 Mbps), when the service traffic on the link exceeds 1000 Mbps, the excess traffic will be discarded. Link aggregation can solve this problem. For example, use *n* network cables to connect the two devices and bind the interfaces together. In this way, the interfaces are logically bound to support the maximum traffic of 1000 Mbps × *n*.
- If two devices are connected through a single cable, when the link between the two interfaces is disconnected, services carried on this link are interrupted. After multiple interconnected interfaces are bound, as long as there is one link available, services carried on these interfaces will not be interrupted.

7.3.2 Overview

1. Static Aggregation Address

In static aggregation mode, you can manually add a physical port to an aggregate interface. An aggregate interface in static aggregation mode is called a static aggregate interface and the member ports are called member ports of the static aggregate interface. Static aggregation can be easily implemented. You can aggregate multiple physical links by running commands to add specified physical ports to an aggregate interface. Once a member interface is added to an aggregate interface, it can send and receive data and balance traffic in the aggregate interface.

2. Automatic Aggregation

Automatic aggregation mode is a special port aggregation function developed for the WAN port of gateway devices. The maximum bandwidth of the WAN port of the gateway device is 2000M, but after the intranet port is connected to the switch, a single port can only support a maximum bandwidth of 1000M. In order to prevent the downlink bandwidth from being wasted, it is necessary to find a way to increase the maximum bandwidth of the port between the MR device and the switch, and the automatic aggregation function emerged to meet the need.
After connecting the two fixed aggregation member ports on the gateway device to any two ports on the switch, through packet exchange, the two ports on the switch can be automatically aggregated, thereby doubling the bandwidth. The aggregate interface automatically generated in this way on the switch is called an automatic aggregate interface, and the corresponding two ports are the member ports of the aggregate interface.

Note

Automatic aggregate interfaces do not support manual creation and can be deleted after they are automatically generated by the device, but member ports cannot be modified.

3. Load Balancing

An aggregate interface, based on packet characteristics such as the source MAC address, destination MAC address, source IP address, destination IP address, L4 source port ID, and L4 destination port ID of packets received by an inbound interface, differentiates packet flows according to one or several combined algorithms. It sends

the same packet flow through the same member link, and evenly distributes different packet flows among member links. For example, in load balancing mode based on source MAC addresses, packets are distributed to different member links of an aggregate interface based on their source MAC addresses. Packets with different source MAC addresses are distributed to different member links; packets with a same source MAC address are forwarded along a same member link.
Currently, the aggregate interface supports the traffic balancing modes based on the following:

- Source MAC address or destination MAC address
- Source MAC address + destination MAC address
- Source IP address or destination IP address
- Source IP address + destination IP address
- Source port
- L4 source port or L4 destination port
- L4 source port + L4 destination port

4. LACP

Link Aggregation Control Protocol (LACP) is a standardized protocol for dynamically aggregating multiple physical links into a single logical link to enhance network bandwidth and reliability. LACP defines the negotiation process and parameters of link aggregation, which enables the exchange of link aggregation information and the negotiation of link aggregation parameters among network devices and ensures the reliability and stability of the link aggregation. LACP supports dynamic addition and deletion of links, achieving dynamic link adjustment and optimization.

In LACP, two roles are defined: the actor and the partner. The actor sends a link aggregation request, while the partner responds to the request and joins the link aggregation group.

7.3.3 Aggregate Interface Configuration

Choose **Local Device** > **Ports** > **Port Aggregation** > **Aggregate Interface** > **Aggregate Interface**.

1. Adding an Aggregate Interface

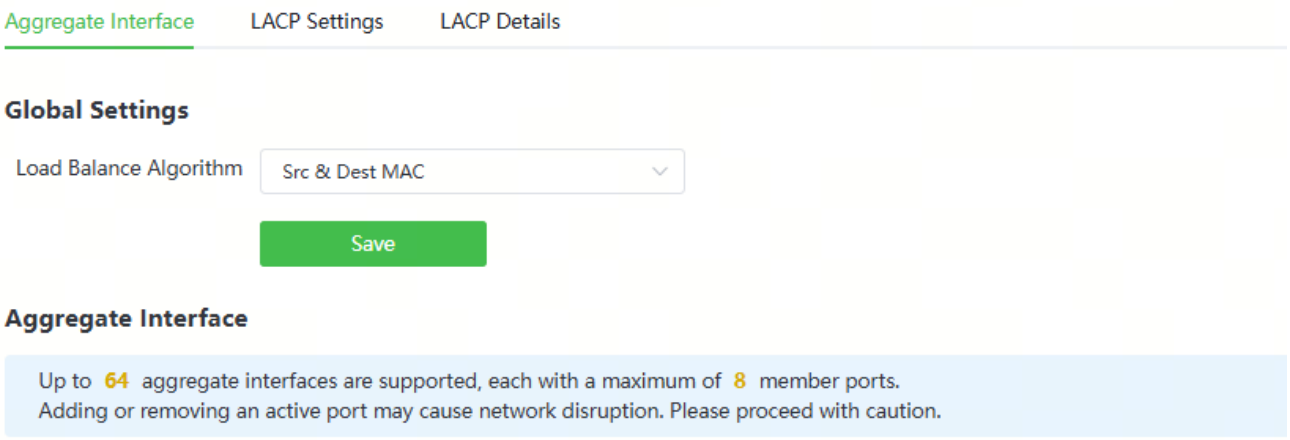
Enter an aggregate interface ID, select member ports (ports that are already a member of an aggregate interface cannot be selected), toggle on **LACP**, and click **Save**. You can

enable **LACP** to dynamically aggregate links to enhance network reliability and flexibility. The port panel displays a successfully added aggregate interface.

Specification

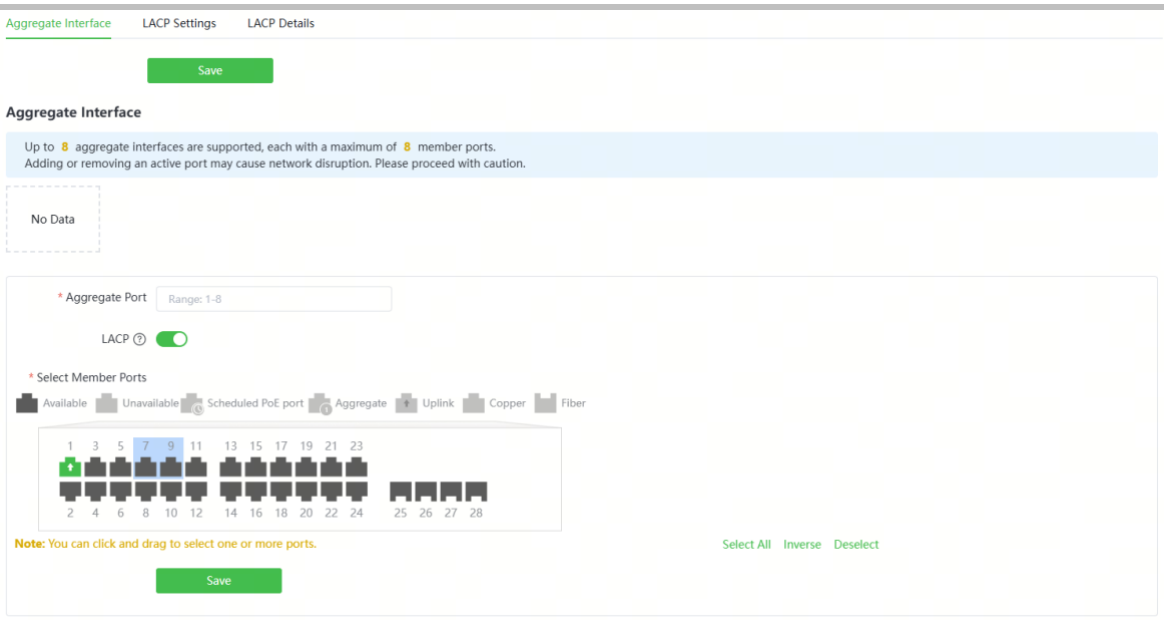
The maximum number of aggregate interfaces that can be configured on a switch varies with the switch model.

For details about the maximum number of aggregate interfaces that can be configured, see the web page.



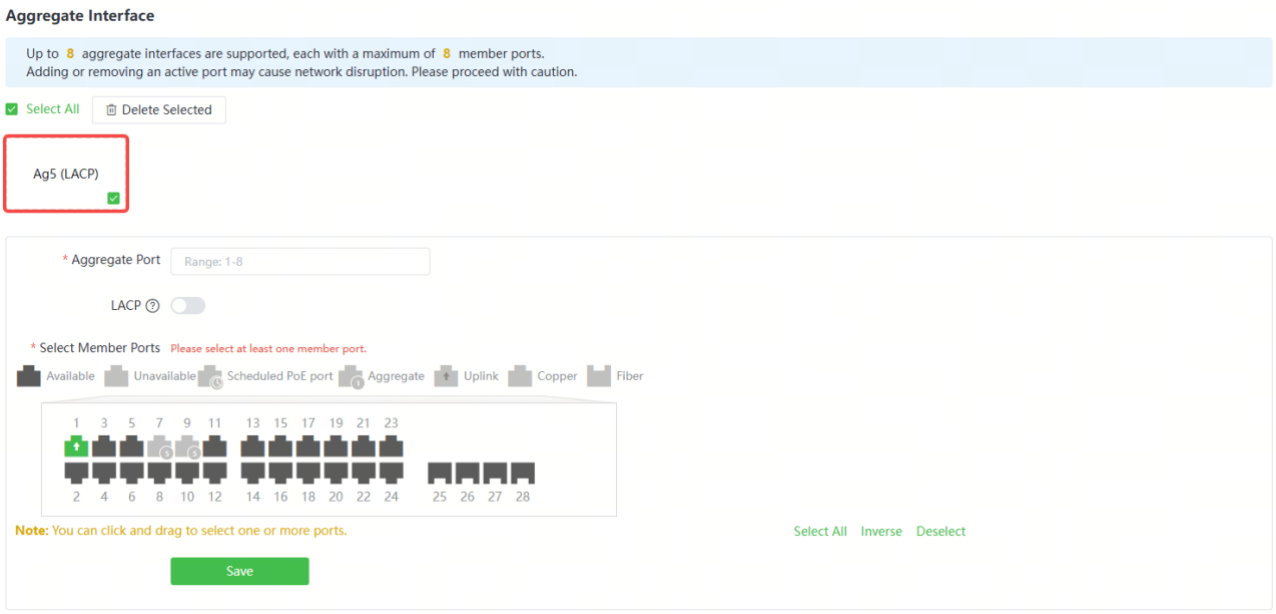
Note

- An aggregate interface contains a maximum of eight member ports.
- The attributes of aggregate interfaces must be the same, and copper ports and SFP ports cannot be aggregated.
- Automatic aggregate interfaces do not support manual creation.
- The LACP state cannot be modified once a static aggregate interface is created.



2. Modifying Member Ports of an Aggregate Interface

Click an added static aggregate interface. Member ports of the aggregate interface will become selected. Click a port to deselect it; or select other ports to join the current aggregate interface. Click **Save** to modify the member ports of the aggregate interface.



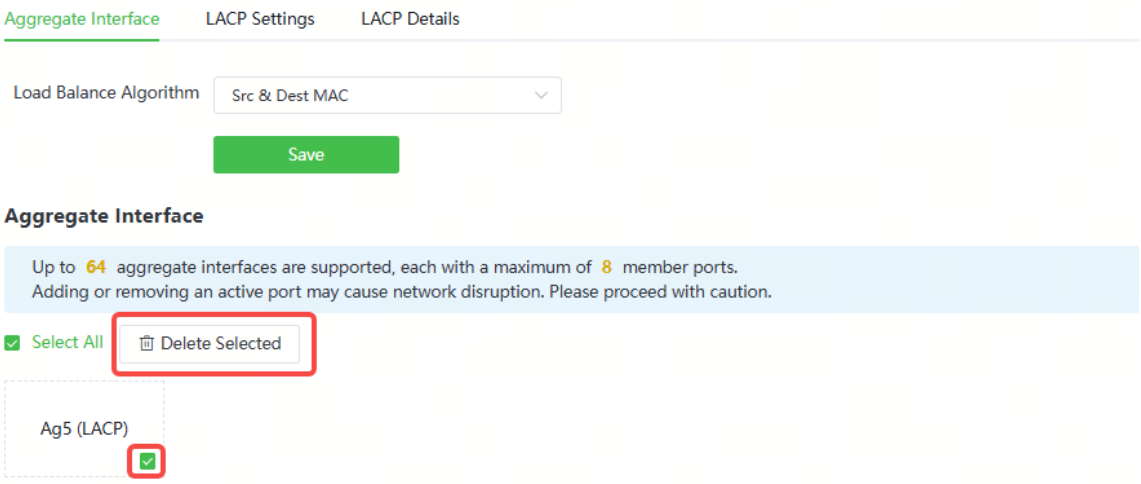
3. Deleting an Aggregate Interface

Move the cursor over an aggregate interface icon and click upper-right, or select the aggregate interface to be deleted, and click **Delete Selected** to delete the selected

aggregate interface. After deleted, the corresponding ports become **available** on the port panel to set a new aggregate interface.

Caution

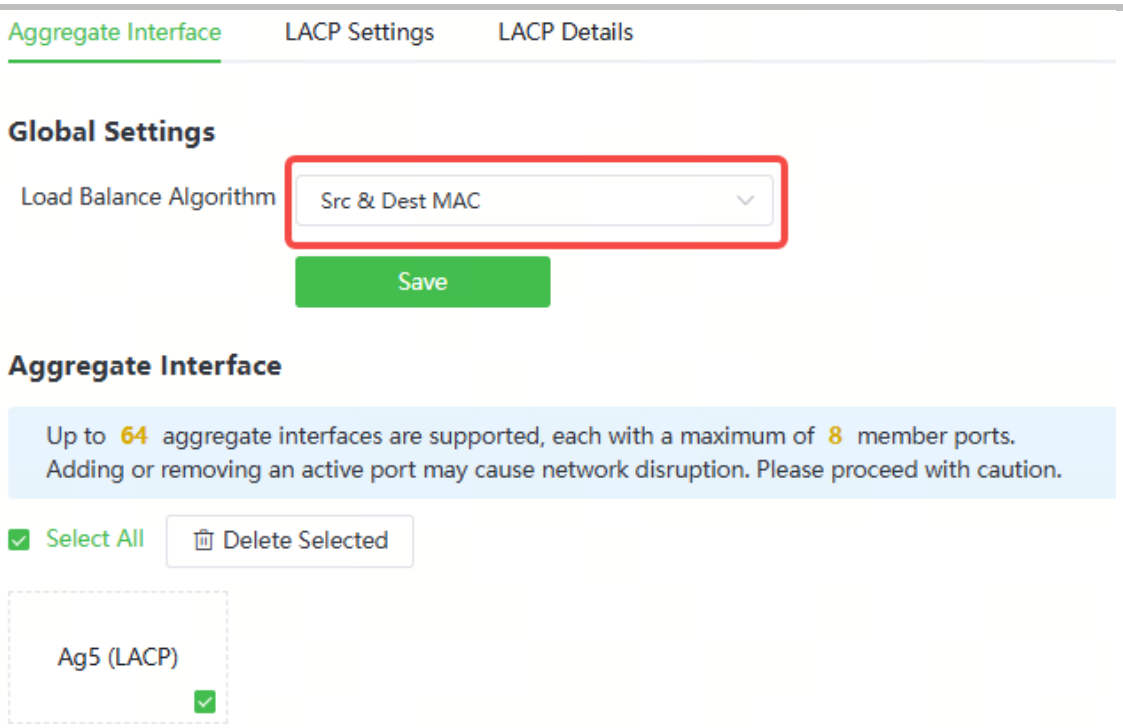
- After an aggregate interface is deleted, its member ports are restored to the default settings and are disabled.



7.3.4 Configuring a Load Balancing Mode

Choose **Local Device** > **Ports** > **Port Aggregation** > **Aggregate Interface** > **Global Settings**.

Select **Load Balance Algorithm** and click **Save**. The Device distributes incoming packets among member links by using the specified load balancing algorithm. The packet flow with the consistent feature is transmitted by one member link, whereas different packet flows are evenly distributed to various links.

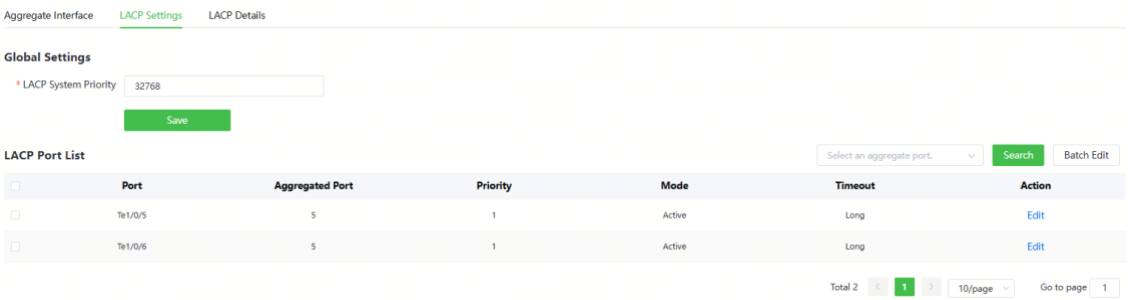


7.3.5 Configuring LACP Settings

1. LACP System Priority

Choose **Local Device** > **Ports** > **Port Aggregation** > **LACP Settings** > **Global Settings**.

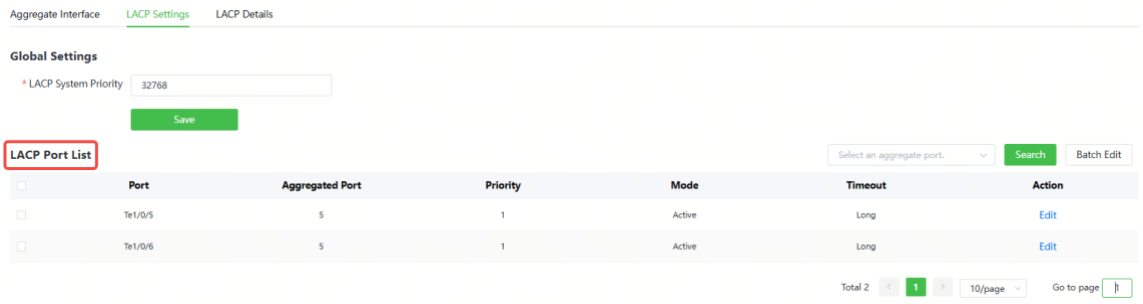
In LACP, the device with a higher system priority becomes the actor in the link aggregation group and controls the working state and parameters of the link aggregation group. The value of system priority ranges from 1 to 65535, and the default value is 32768. The lower the value of system priority, the higher the device priority. When two devices have the same system priority, their MAC addresses are compared, and the device with the smaller MAC address becomes the actor in the link aggregation group.



2. LACP Port List

Choose **Local Device** > **Ports** > **Port Aggregation** > **LACP Settings** > **LACP Port List**.

The **LACP Port List** page shows the port ID, priority, mode, and timeout mode of each LACP-enabled port. You can view the member port details of the corresponding link aggregation group by selecting an aggregate interface.



You can select a specific port and click **Edit**, or select multiple ports and click **Batch Edit** to modify the port priority, mode, and timeout mode in the pop-up window. Then, click **OK** to confirm and apply the changes.

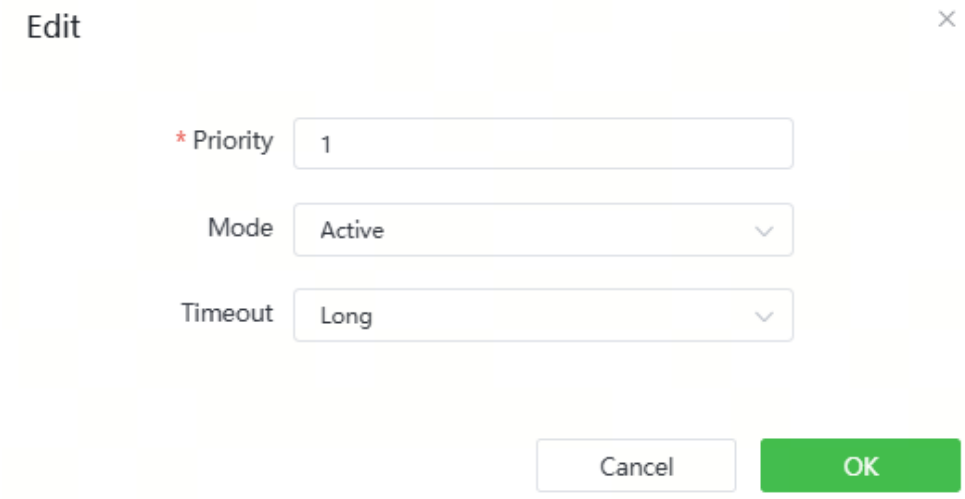


Table 7-3 Description of LACP Port List Configuration Parameters

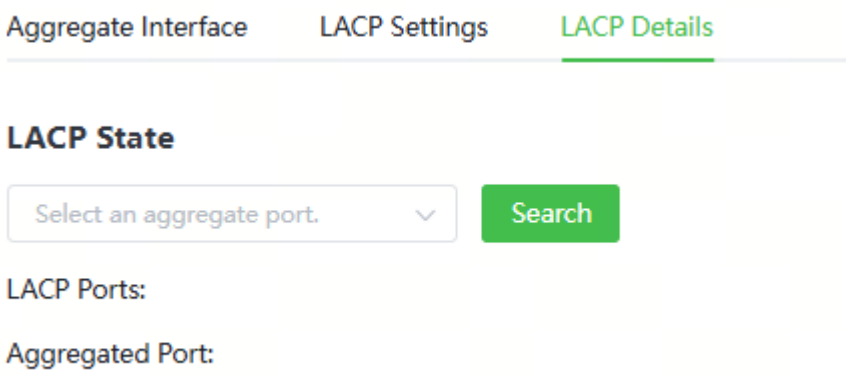
Parameter	Description	Default Value
Priority	Priority is used to determine which port is the master, with the highest-priority port being selected as the active	32768

Parameter	Description	Default Value
	port. The priority value ranges from 1 to 65535, and a lower priority value indicates a higher priority. If multiple ports have the same priority, their priority ranking is determined by evaluating their port IDs, and the port with the lower port ID will be given a higher priority.	
Mode	Mode refers to the method by which two devices within a link aggregation group negotiate their operating mode. ● Active: In active mode, the device assumes the role of the actor and sends requests to establish link aggregation. ● Passive: In passive mode, the device assumes the role of the partner and waits for the peer device to send a request.	Active
Timeout	The purpose of the timeout mode is to determine the timeout period and mechanism for LACP link aggregation. When no LACP frames are received from the peer device within the specified timeout duration, it is assumed that the peer device has experienced a failure. As a result, the failure detection and recovery mechanism of the link aggregation is triggered. ● Long: In long timeout mode, LACP frames are sent every 30 seconds, and the timeout duration is set to 90 seconds. This mode enhances the reliability and stability of link aggregation, but it can potentially lead to delayed detection of faults. ● Short: In short timeout mode, LACP frames are sent every second, and the timeout duration is set to 3 seconds. This mode enhances the response speed of link aggregation and ensures timely fault detection, but it may impose additional network load and resource consumption.	Long

3. Viewing LACP State

Choose **Local Device** > **Ports** > **Port Aggregation** > **LACP Details**.

You can select an LACP-enabled aggregate interface and click **Search** to view the LACP-enabled member ports and the aggregate interface information on this page.



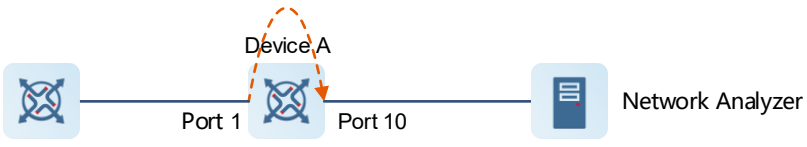
7.4 Port Mirroring

7.4.1 Overview

The switched port analyzer (SPAN) function is a function that copies packets of a specified port to another port that is connected to a network monitoring device, After port mirroring is set, the packets on the source port will be copied and forwarded to the destination port, and a packet analyzer is usually connected to the destination port to analyze the packet status of the source port, so as to monitor all incoming and outgoing packets on source ports.

As shown, by configuring port mirroring on Device A, the device copies the packets on Port 1 to Port 10. Although the network analysis device connected to Port 10 is not directly connected to Port 1, it can receive packets through Port 1. Therefore, the aim to monitor the data flow transmitted by Port 1 is realized.

Figure 7-1 Port Mirroring Principles Figure



The SPAN function not only realizes the data traffic analysis of suspicious network nodes or device ports, but also does not affect the data forwarding of the monitored device. It is mainly used in network monitoring and troubleshooting scenarios.

7.4.2 Procedure

Choose **Local Device** > **Ports** > **Port Mirroring**.

Click **Edit**, select the source port, destination port, monitor direction, and whether to receive packets from non-source ports, and click **OK**. A maximum of four SPAN entries can be configured.

To delete the port mirroring configuration, click **Delete** in the corresponding **Action** column.

Caution

- You can select multiple source traffic monitoring ports but only one destination port. Moreover, the source traffic monitoring ports cannot contain the destination port.
- An aggregate interface cannot be used as the destination port.
- A maximum of four SPAN entries can be configured. SPAN cannot be configured for ports that have been used for SPAN.

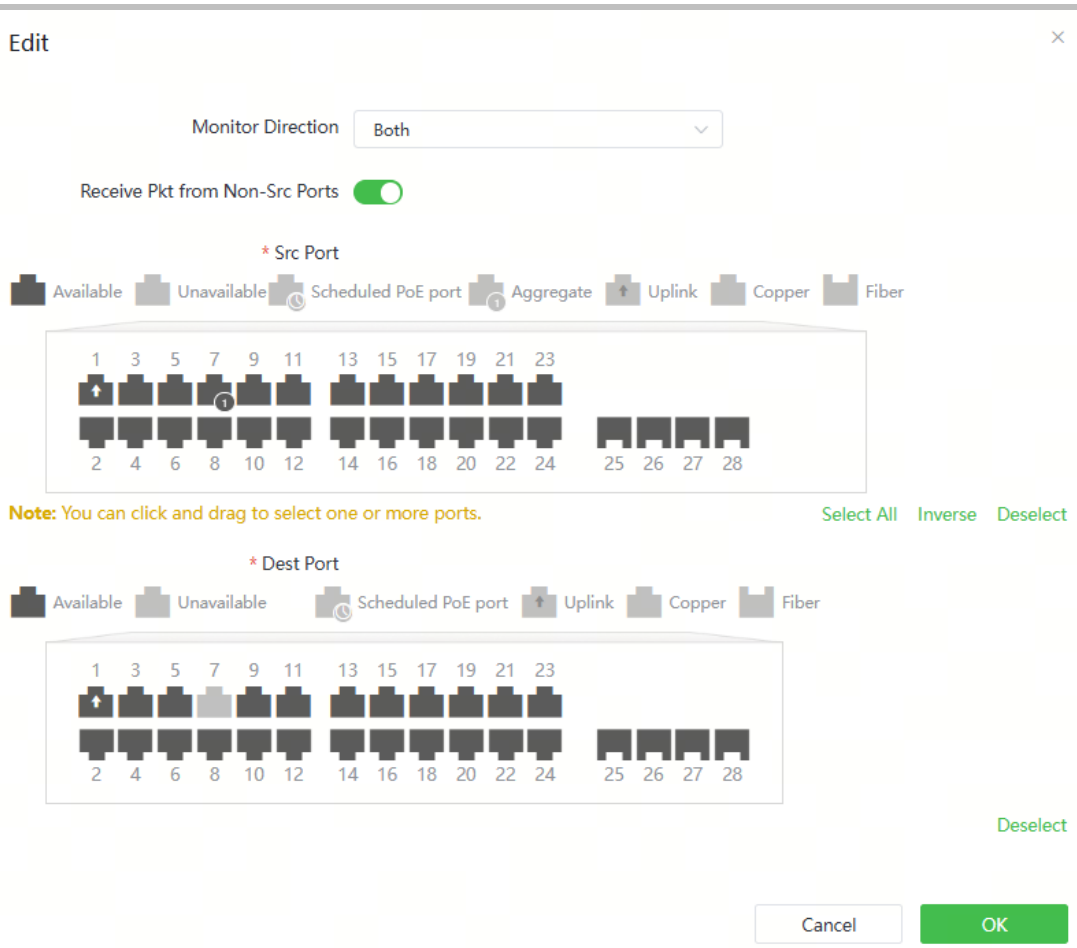


Table 7-4 Description of Port Mirroring Parameters

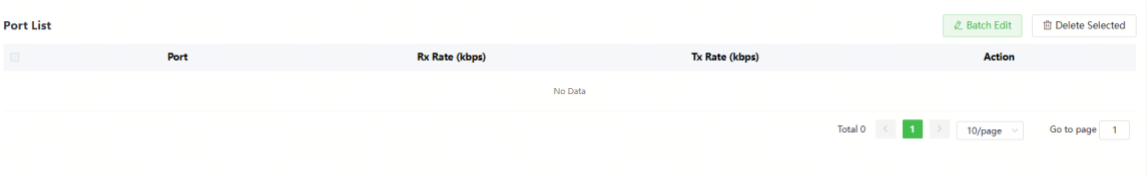
Parameter	Description	Default Value
Src Port	A source port is also called a monitored port. Data flows on the source port are monitored for network analysis or troubleshooting. Support selecting multiple source ports and mirroring multiple ports to one destination port	N/A
Dest Port	The destination port is also called the monitoring port, that is, the port connected to the monitoring device, and forwards the received packets from the source port to the monitoring device.	N/A

Parameter	Description	Default Value
Monitor Direction	The type of packets (data flow direction) to be monitored by a source port. ● Both: All packets passing through the port, including incoming and outgoing packets ● Incoming: All packets received by a source port are copied to the destination port ● Outgoing: All packets transmitted by a source port are copied to the destination port	Both
Receive Pkt from Non-Src Ports	It is applied to the destination port and indicates whether a destination port forwards other packets while monitoring packets. ● Enabled: While monitoring the packets of the source port, the packets of other non-source ports are normally forwarded ● Disabled: Only monitor source port packets	Enable

7.5 Rate Limiting

Choose **Local Device** > **Ports** > **Rate Limiting**.

The **Rate Limiting** module allows you to configure traffic limits for ports, including rate limits for inbound and outbound direction of ports.



7.5.1 Rate Limiting Configuration

Click **Batch Edit**. In the displayed dialog box, select ports and enter the rate limits, and click **OK**. You must configure at least the ingress rate or egress rate. After the configuration is completed, it will be displayed in the list of port rate limiting rules.

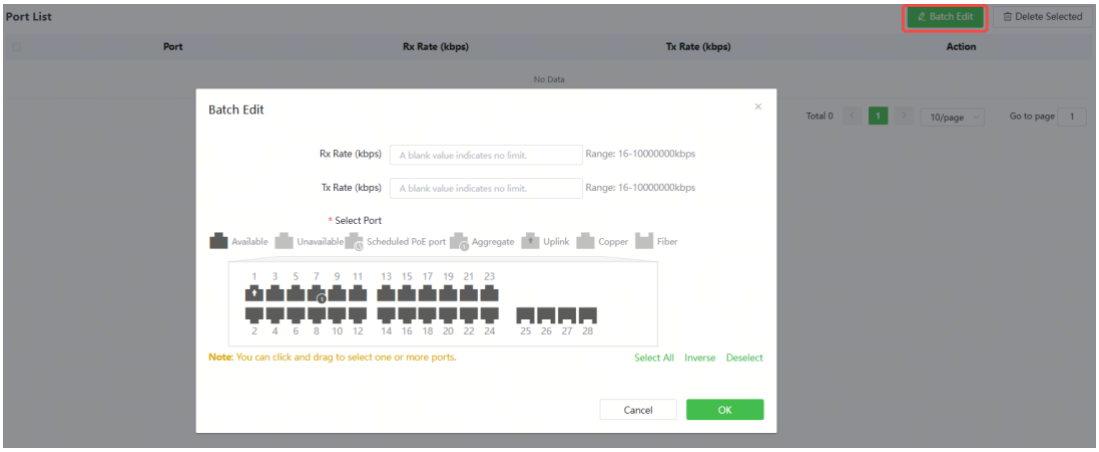
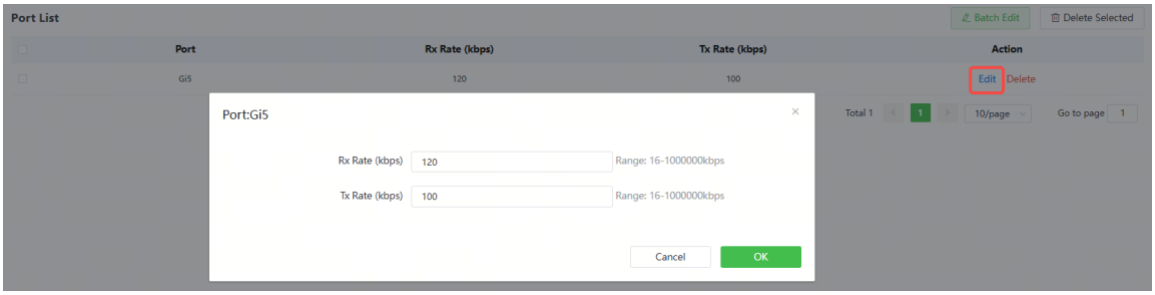


Table 7-5 Description of Rate Limiting Parameters

Parameter	Description	Default Value
Rx Rate	Max Rate at which packets are sent from a port to a switch, in kbps.	Not limited
Tx Rate	Max Rate at which packets are sent out of a switch through a port, in kbps.	Not limited

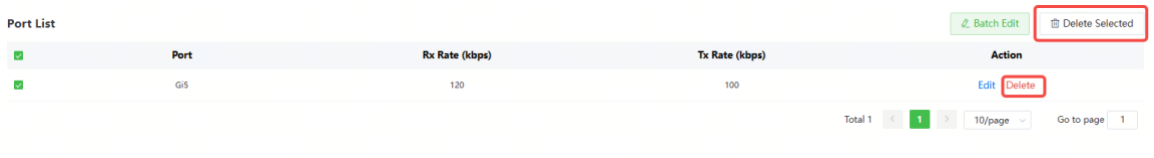
7.5.2 Changing Rate Limits of a Single Port

In the port list for which the rate limit has been set, click **Edit** on the corresponding port entry, enter the ingress rate and egress rate in the displayed dialog box, and click **OK**.



7.5.3 Deleting Rate Limiting

- Batch configuration: Select multiple records in **Port List**, click **Delete Selected** and click **OK** in the confirmation dialog box**.**
- Configuring one port: In **Port List**, click **Delete** on the corresponding port entry, and click **OK** in the confirmation dialog box.



Note

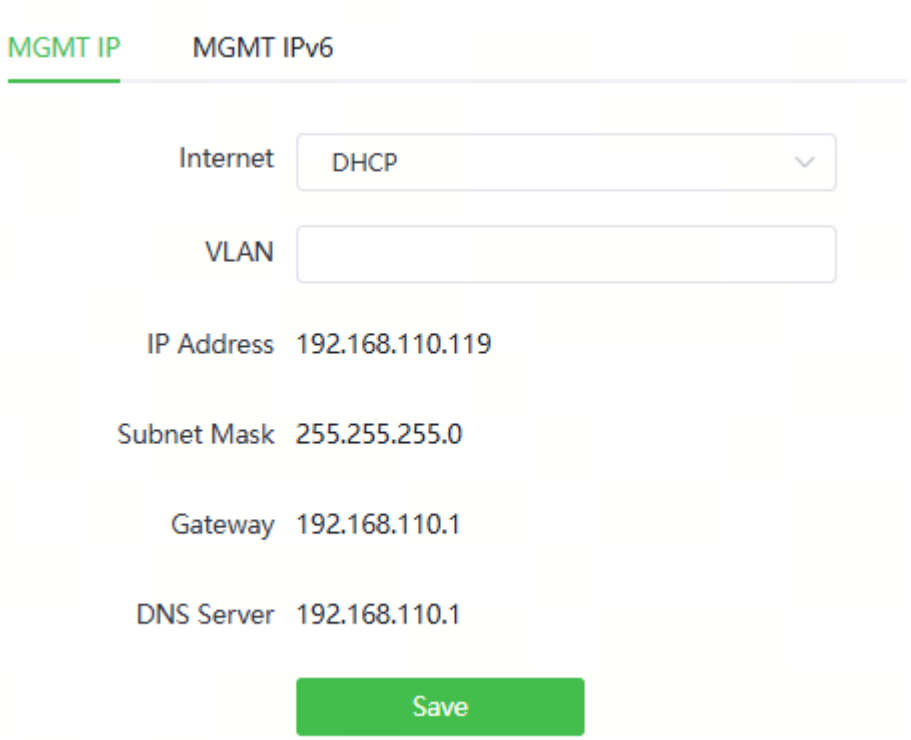
- When configuring rate limits for a port, you must configure at least the ingress rate or egress rate.
- When the ingress rate or egress rate is not set, the port rate is not limited.

7.6 MGMT IP Configuration

7.6.1 Configuring the Management IPv4 Address

Choose **Local Device** > **Ports** > **MGMT IP** > **MGMT IP**.

The **MGMT IP** page allows you to configure the management IP address for the device. Users can configure and manage the device by accessing the management IP.



The device can be networked in two modes:

- DHCP: Uses a temporary IP address dynamically assigned by the upstream DHCP server for Internet access.
- Static IP: Uses a static IP address manually configured by users for Internet access.

If you select DHCP, the device obtains parameters from the DHCP Server. If Static IP is selected, you need to enter the management VLAN, IP address, subnet mask, default gateway IP address, and address of a DNS server. Click **Save** to make the configuration take effect.

Note

- If the management VLAN is null or not specified, VLAN 1 takes effect by default.
- The management VLAN must be selected from existing VLANs. If no VLAN is created, go to the VLAN list to add a VLAN (for details, see 5.2 Configuring a VLAN).
- You are advised to bind a configured management VLAN to an uplink port. Otherwise, you may fail to access the web page.

7.6.2 Configuring the Management IPv6 Address

Configure the IPv6 address used to log in to the device management page.

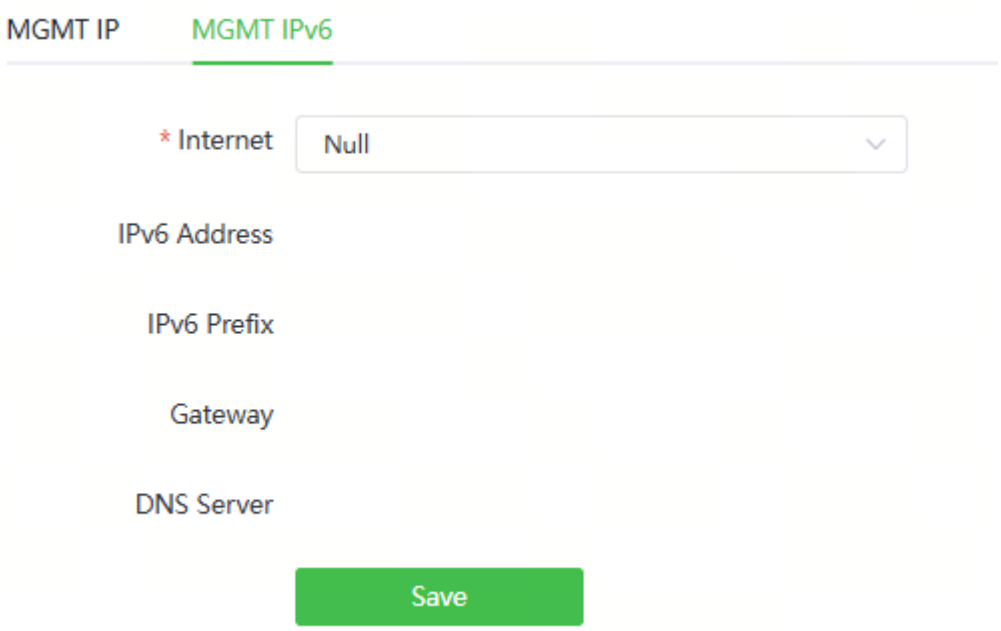
Choose **Local Device** > **Ports** > **MGMT IP** > **MGMT IPv6**.

Configure the management IPv6 address so that you can log in to the device management page using the IPv6 address of the device.

The device supports the following Internet connection types:

- **Null**: The IPv6 function is disabled on the current port.
- **DHCP**: The device dynamically obtains an IPv6 address from the upstream device.
- **Static IP**: You need to manually configure the IPv6 address, length, gateway address, and DNS server.

Click **Save**.



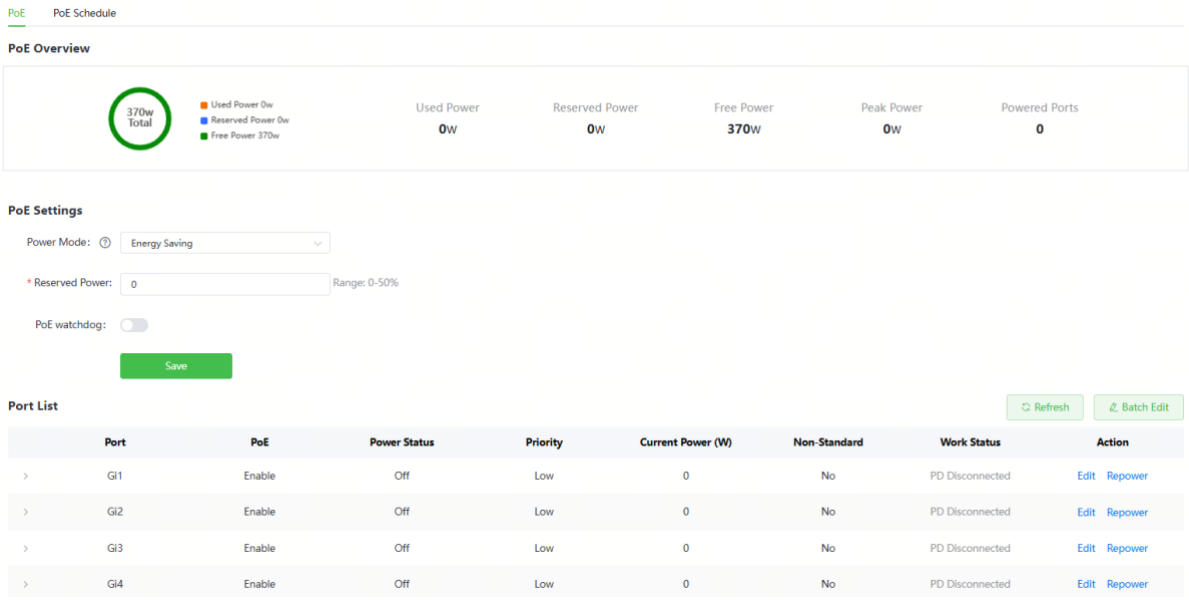
7.7 PoE Configuration

Specification

Only PoE switches (model name containing –P, -LP, -HP, and -UP) support this function.

Choose **Local Device** > **Ports** > **PoE**.

The device supplies power to PoE powered devices through ports. Users can view the current power supply status, and set the system power supply and port power supply policies respectively to achieve flexible power distribution.



7.7.1 PoE Global Settings

Choose **Local Device** > **Ports** > **PoE** > **PoE** > **PoE Settings**.

PoE Transmit Power Mode refers to the way that a device allocates power to a connected PD (Powered Device). It supports Auto mode and Energy-saving mode.

In Auto mode, the system allocates power based on the classes of PDs detected on ports. The device allocates power to PD devices of Class 0~4 based on a fixed value: Class 0 is 15.4W, Class 1 is 4W, Class 2 is 7W, Class 3 is 15.4W, Class 4 Type 1 is 15.4W, and Class 4 Type 2 is 30W. In this mode, if the port is connected to a device of Class 3, even if the actual power consumption is only 11W, the PoE power supply device will allocate power to the port based on the power of 15.4W.

In energy-saving mode, the PoE device dynamically adjusts allocated power based on actual consumption of PDs. In this mode, in order to prevent the power supply of the port from fluctuating due to the fluctuation of the actual power consumption of the PD when the power is fully loaded, you can set the Reserved Transmit Power, and the reserved power will not be used for power supply, so as to ensure that the total power consumed by the current system does not exceed the limit of the PoE device. The size of

the reserved power is expressed as a percentage of the total PoE power. The value ranges from 0 to 50.

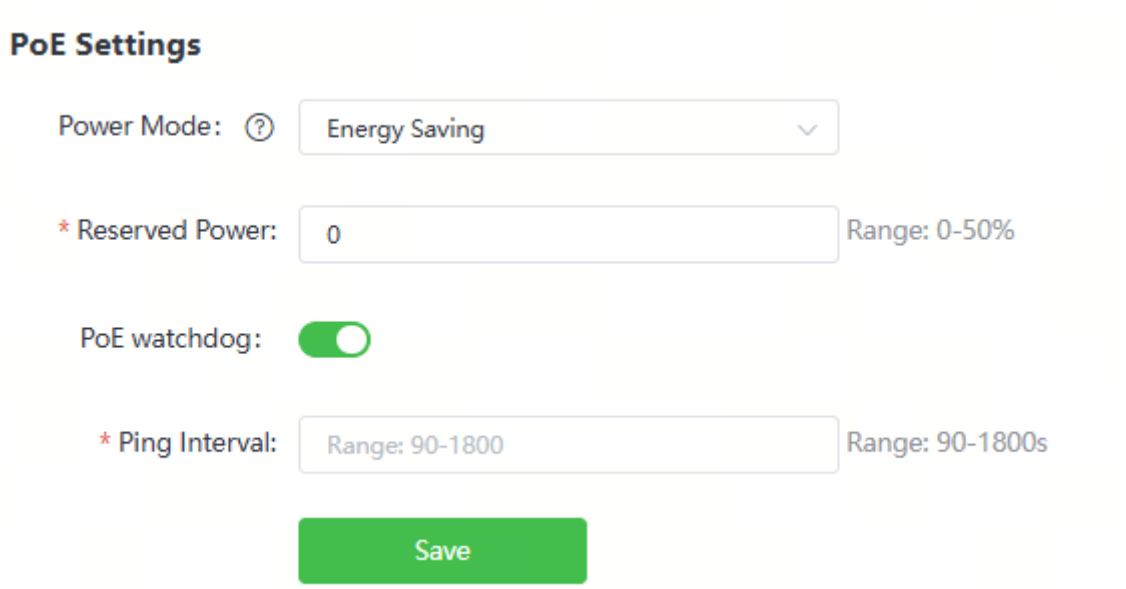
PoE watchdog: This feature is mainly applicable to security surveillance scenarios. After this feature is enabled, when a PoE port of the device suddenly stops receiving packets during the ping interval, the powered device (PD) will be restarted after the ping interval expires to restore normal operation.

Table 7-6 PoE Watchdog Configuration Description

Packet Receiving Status of the PoE Port	PoE Watchdog is Enabled	Action Taken on the PD
During the ping interval, a PoE port of the device suddenly stops receiving packets.	Yes	The PD is restarted to restore normal operation, and the ping interval is reset.
	No	No action is initiated on the PD.
During the ping interval, a PoE port of the device still stops receiving packets.	Yes	No action is initiated on the PD.
	No	No action is initiated on the PD.
During the ping interval, a PoE port of the device starts to receive packets.	Yes	The ping interval is reset.
	No	No action is initiated on the PD.

Note

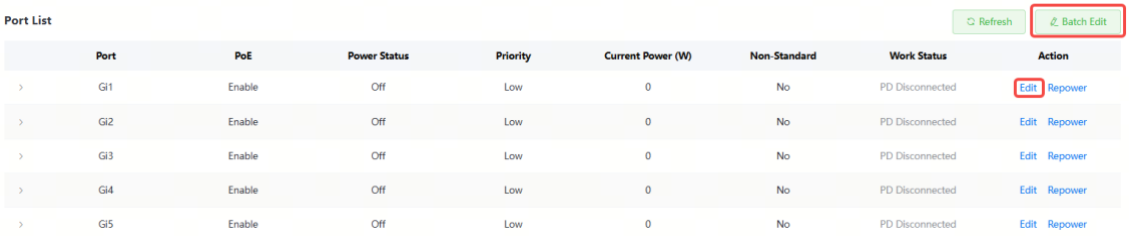
If a non-PD, such as a computer, is connected to a PoE-enabled port of this device, the PoE watchdog will not initiate any action on the non-PD even if the trigger condition is met.



7.7.2 Power Supply Configuration of Ports

Choose **Local Device** > **Ports** > **PoE** > **PoE** > **Port List**.

Click **Edit** in the port entry or click **Batch Edit** to set the PoE power supply function of the port.



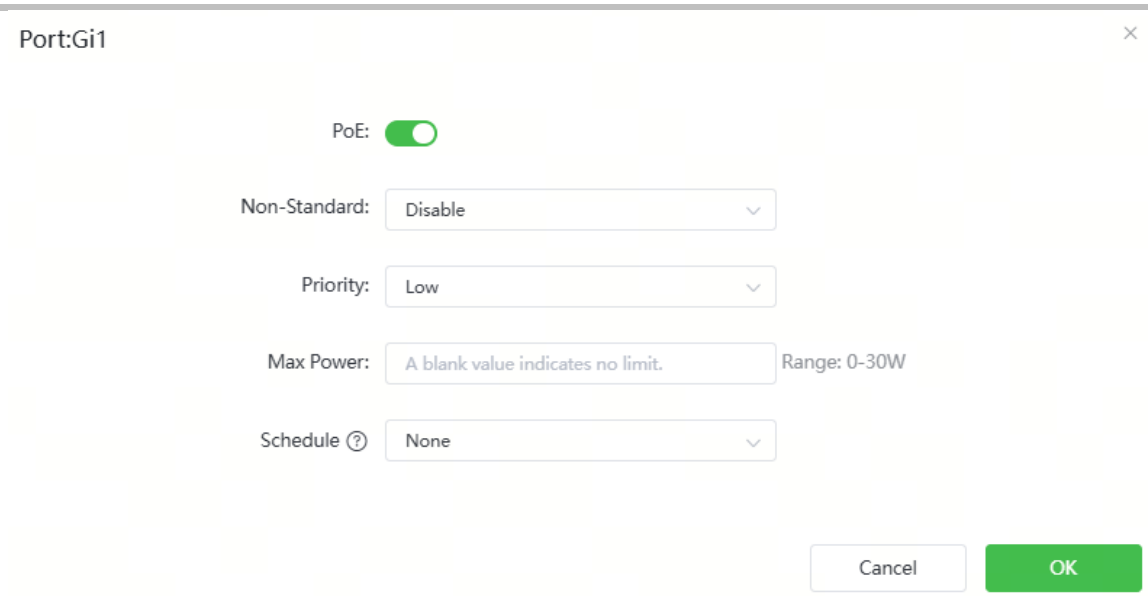


Table 7-7 Description of Parameters for Power Supply Configuration of Ports

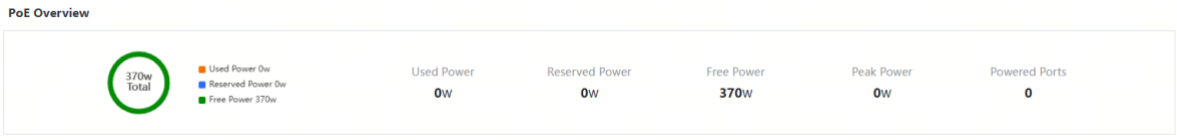
Parameter	Description	Default Value
PoE	Whether to enable the power supply function on the ports	Enable
Non-Standard	By default, the device only supplies power to PDs that comply with the standard IEEE 802.3af and 802.3at protocols. In practical applications, there may be PDs that do not conform to the standard. After the non-standard mode is enabled, the device port can supply power to some non-standard PD devices.	Disable
Priority	The power supply priority of the port is divided into three levels: High, Medium, and Low In auto and energy-saving modes, ports with high priorities are powered first. When the system power of the PoE device is insufficient, ports with low priorities are powered off first.	Low

Parameter	Description	Default Value
	Ports with the same priority are sorted by the port number. A smaller port number indicates a higher priority.	
Max Transmit Power	The maximum power that the port can transmit, ranging from 0 to 30, in watts (W). A blank value indicates no limit	Not limit
Schedule	You can set a PoE schedule for a port. ● Set it to **None** to disable the PoE schedule for a port. ● Set it to a specific schedule to forcibly disable PoE on the port during the specified time period. ● Set it to **Add Schedule** to redirect to the **PoE Schedule** page on which you can add PoE schedules. For details, see 7.7.5 Configuring PoE Schedules.	None

7.7.3 Displaying Global PoE Information

Choose **Local Device** > **Ports** > **PoE** > **PoE** > **PoE Overview**.

Displays the global power supply information of the PoE function, including the total system power, used power, reserved power, remaining available power, peak maximum power, and the number of ports currently powered.



7.7.4 Displaying the Port PoE Information

Choose **Local Device** > **Ports** > **PoE** > **PoE** > **Port List**.

The **Port List** displays the PoE configuration and status information of each port. Click to expand the detailed information.

When the PD device connected to the port needs to be restarted, for example, when the AP connected to the port is abnormal, you can click **Repower** to make the port power off briefly and then power on again to restart the device connected to the power supply port.

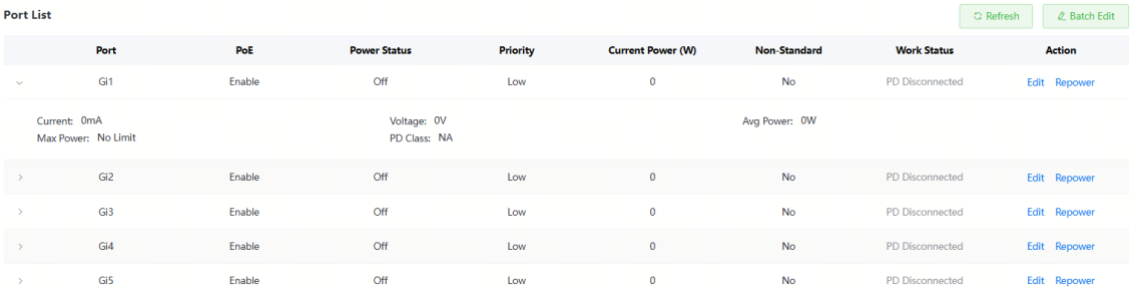


Table 7-8 Description of Port Power Supply Info

Field	Description
Port	Device Port ID
PoE Status	Whether to enable the PoE function on the ports.
Transmit Power Status	Whether the port supplies power for PDs currently.
Priority	The power supply priority of the port is divided into three levels: High, Medium, and Low.
Current Transmit Power	Indicates the power output by the current port, in watts (W).
Non-Standard	Indicates whether the non-standard compatibility mode is enabled.
Work Status	Current work status of PoE ports.
Current	Indicates the present current of the port in milliamps (mA).
Voltage	Indicates the present current of the port in volts (V).
Avg Transmit Power	Indicates the current average power of the port, namely, the sampling average of current power after the port is powered on, in watts (W).

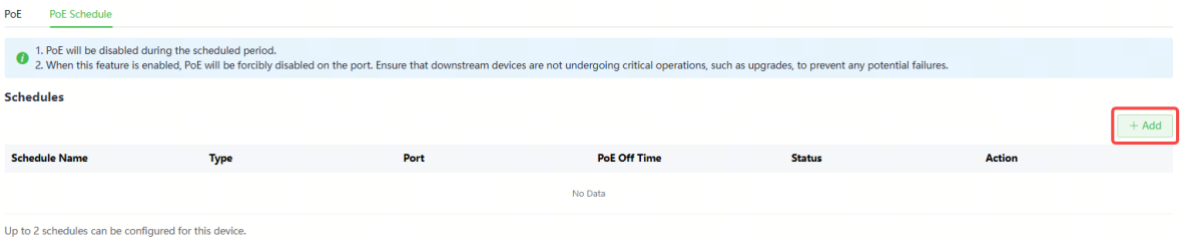
Field	Description
Max Transmit Power	The maximum output power of the port in watts (W).
PD Requested Transmit Power	The power requested by the PD to the PSE (Power Sourcing Equipment, power supply equipment), in watts (W).
PSE Allocated Transmit Power	Indicates the power allocated to a PD by PSE in watts (W).
PD Type	Information of PD type obtained through LLDP classification are divided into Type 1 and Type 2.
PD Class	The classification level of the PD connected to the port is divided into Class 0~4, based on the IEEE 802.3af/802.3at standard.

7.7.5 Configuring PoE Schedules

Choose **Local Device** > **Ports** > **PoE** > **PoE Schedule**.

Once a schedule is enabled, PoE will be forcibly disabled during the specified time period. Please ensure that downlink devices are not undergoing upgrades or other operations that require an uninterrupted power supply to avoid potential malfunctions.

Click **Add**, set the schedule parameters, and click **OK**.



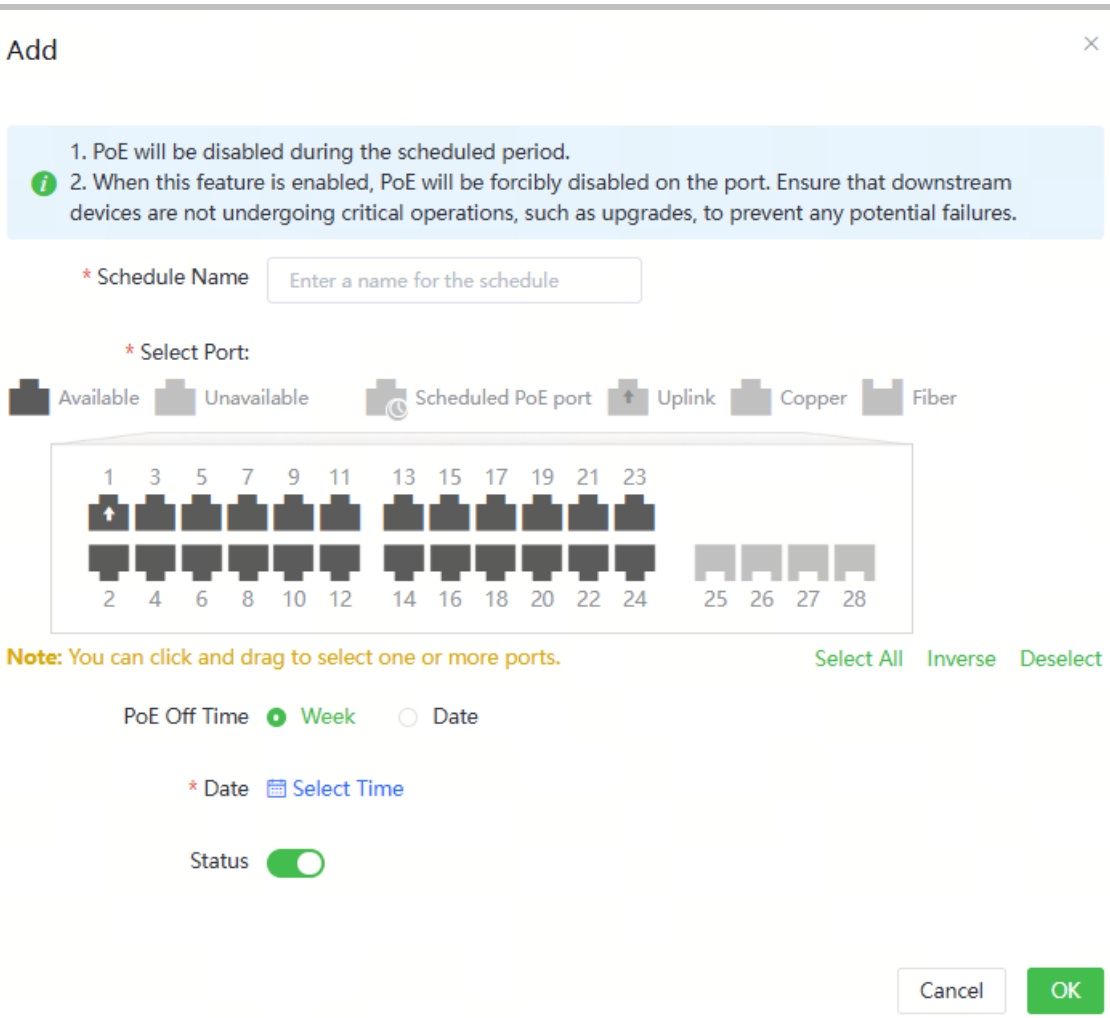


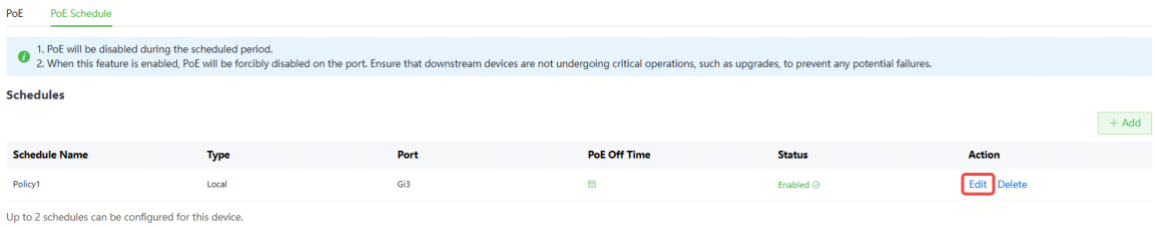
Table 7-9 PoE Schedule Parameters

Parameter	Description
Schedule Name	Custom PoE schedule name.
Select Port	Device port or ports on which a PoE schedule is to be configured.
PoE Off Time	Week or date during which PoE is disabled.
Date	Time period during which PoE is disabled.
Status	Whether to enable the PoE schedule.

After a schedule is configured, it is displayed in the schedule list. You can click **Edit** or **Delete** in the **Action** column to modify or remove a specified schedule.

Note

The PoE schedules with **Type** set to **Total** cannot be removed from the web page.



8 Layer 2 Multicast

8.1 Multicast Overview

IP transmission methods are categorized into unicast, multicast, and broadcast. In IP multicast, an IP packet is sent from a source and forwarded to a specific group of receivers. Compared with unicast and broadcast, IP multicast saves bandwidth and reduces network loads. Therefore, IP multicast is applied to different network services that have high requirements for real timeliness, for example, Internet TV, distance education, live broadcast and multimedia conference.

8.2 Multicast Global Settings

Choose **Local Device > L2 Multicast > IGMP Snooping > Global Settings**.

Global Settings allow you to specify the version of the IGMP protocol, whether to enable report packet suppression, and the behavior for processing unknown multicast packets.

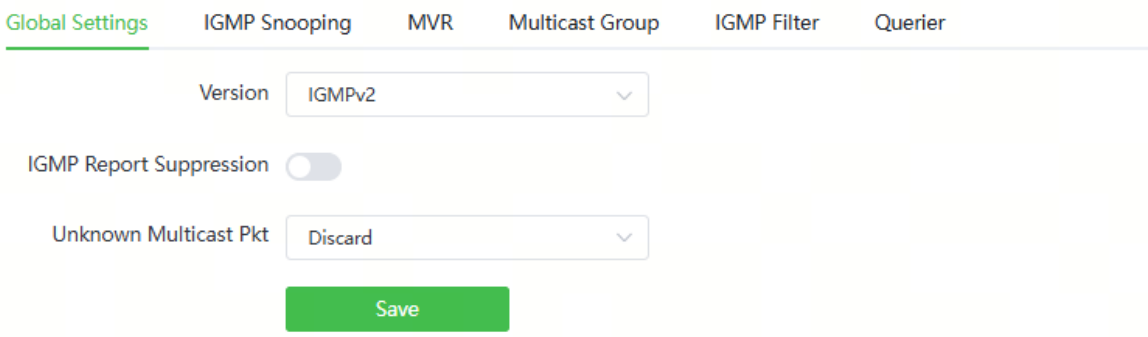


Table 8-1 Description of Configuration Parameters of Global Multicast

Parameter	Description	Default Value
Version	The Internet Group Management Protocol (IGMP) is a TCP/IP protocol that manages members in an IPv4 multicast group and runs on the multicast devices and hosts residing on	IGMPv2

Parameter	Description	Default Value
	the stub of the multicast network, creating and maintaining membership of the multicast group between the hosts and connected multicast devices. There are three versions of IGMP: IGMPv1, IGMPv2, and IGMPv3. This parameter is used to set the highest version of IGMP packets that can be processed by Layer 2 multicast, and can be set to IGMPv2 or IGMPv3.	
IGMP Report Suppression	After this function is enabled, to reduce the number of packets in the network, save network bandwidth and ensure the performance of the IGMP multicast device, the switch forwards only one report packet to the multicast router if multiple downlink clients connected to the switch simultaneously send the report packet to demand the same multicast group.	Disable
Unknown Multicast Pkt	When both the global and VLAN multicast functions are enabled, the processing method for receiving unknown multicast packets can be set to **Discard** or **Flood**.	Discard

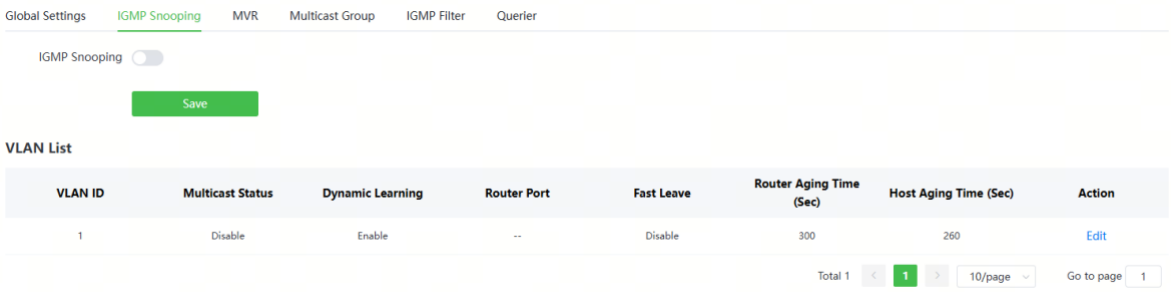
8.3 IGMP Snooping

8.3.1 Overview

The Internet Group Management Protocol (IGMP) snooping is an IP multicast snooping mechanism running on a VLAN to manage and control the forwarding of IP multicast traffic within the VLAN. It implements the Layer 2 multicast function.

Generally, multicast packets need to pass through Layer 2 switches, especially in some local area networks (LANs). When the Layer 2 switching device does not run IGMP Snooping, the IP multicast packets are broadcast in the VLAN; when the Layer 2

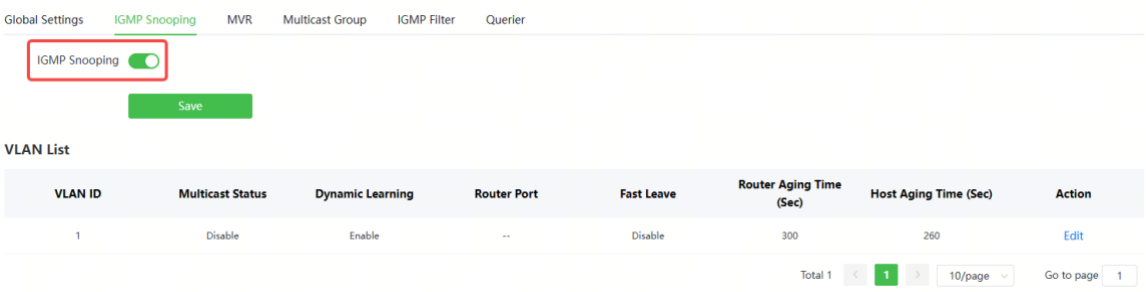
switching device runs IGMP Snooping, the Layer 2 device can snoop the IGMP protocol packets of the user host and the upstream PIM multicast device. In this way, a Layer 2 multicast entry is established, and IP multicast packets are controlled to be sent only to group member receivers, preventing multicast data from being broadcast on the Layer 2 network.



8.3.2 Enabling Global IGMP Snooping

Choose **Local Device** > **L2 Multicast** > **IGMP Snooping** > **IGMP Snooping**.

Turn on **IGMP Snooping** and click **Save**.



8.3.3 Configuring Protocol Packet Processing Parameters

By controlling protocol packet processing, a Layer 2 multicast device can establish static or dynamic multicast forwarding entries. In addition, the device can adjust parameters to refresh dynamic multicast forwarding entries and IGMP snooping membership quickly.

Choose **Local Device** > **L2 Multicast** > **IGMP Snooping** > **IGMP Snooping**.

The IGMP Snooping function is implemented based on VLANs. Therefore, each VLAN corresponds to an IGMP Snooping setting entry. There are as many IGMP Snooping entries as VLANs on the device.

Click **Edit** in the VLAN entry. In the displayed dialog box enable/disable the VLAN multicast function, dynamic learning function, fast leave function and static route connection port, and set the router aging time and the host aging time, and click **OK**.

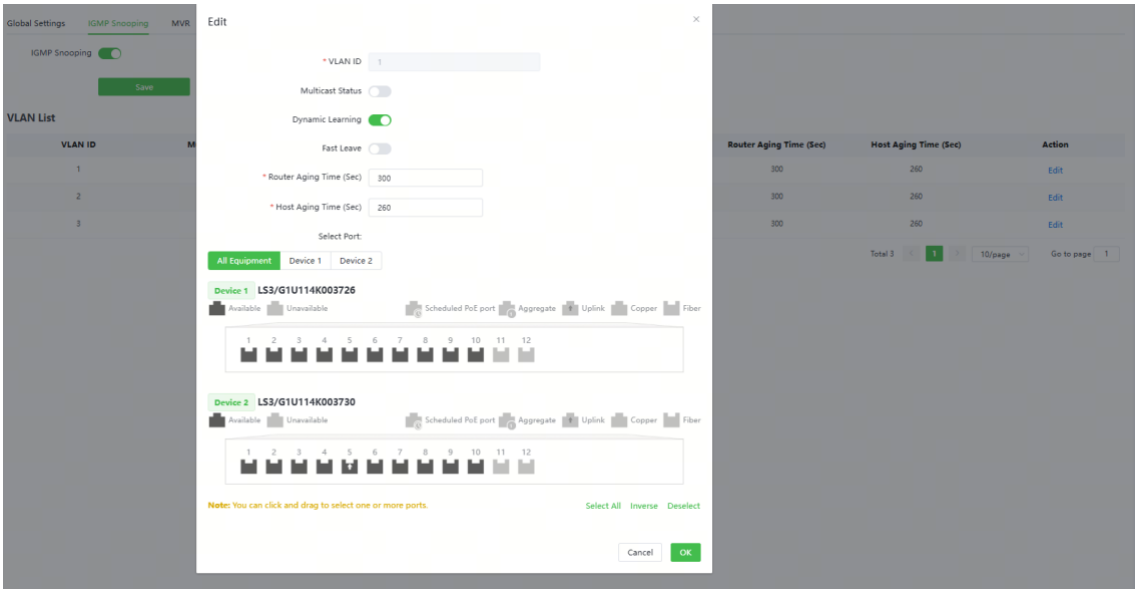


Table 8-2 Description of VLAN Configuration Parameters of IGMP Snooping

Parameter	Description	Default Value
Multicast Status	Whether to enable or disable the VLAN multicast function. The multicast function of a VLAN takes effect only when both the global IGMP snooping and VLAN multicast functions are enabled.	Disable
Dynamic Learning	The device running IGMP Snooping identifies the ports in the VLAN as router ports or member ports. The router port is the port on the Layer 2 multicast device that is connected to the Layer 3 multicast device, and the member port is the host port connected to the group on the Layer 2 multicast device. By snooping IGMP packets, the Layer 2 multicast device can automatically discover and maintain dynamic multicast router ports.	Enable

Parameter	Description	Default Value
Router Port	List of current multicast router ports includes dynamically learned routed ports (if Dynamic Learning function is enabled) and statically configured routed ports.	NA
Fast Leave	After it is enabled, when the port receives the Leave packets, it will immediately delete the port from the multicast group without waiting for the aging timeout. After that, when the device receives the corresponding specific group query packets and multicast data packets, the device will no longer forward it to the port. This function is applicable when only one host is connected to one port of the device, and is generally enabled on the access switch directly connected to the endpoint.	Disable
Router Aging Time (Sec)	Aging time of dynamically learned multicast router ports ranges from 30 to 3600, in seconds.	300 seconds
Host Aging Time (Sec)	Aging time of dynamically learned member ports of a multicast group, in seconds.	260 seconds
Select Port	In the displayed dialog box, select a port and set it as the static router port. When a port is configured as a static router port, the port will not age out	NA

8.4 Configuring MVR

8.4.1 Overview

IGMP snooping can forward multicast traffic only in the same VLAN. If multicast traffic needs to be forwarded to different VLANs, the multicast source must send multicast

traffic to different VLANs. In order to save upstream bandwidth and reduce the burden of multicast sources, multicast VLAN register (MVR) comes into being. MVR can copy multicast traffic received from an MVR VLAN to the VLAN to which the user belongs and forward the traffic.

8.4.2 Configuring Global MVR Parameters

Choose **Local Device** > **L2 Multicast** > **IGMP Snooping** > **MVR**.

Click to enable the MVR, select the MVR VLAN, set the multicast group supported by the VLAN, and click **Save**. Multiple multicast groups can be specified by entering the start and end multicast IP addresses.

Table 8-3 Description of Configuring Global MVR Parameters

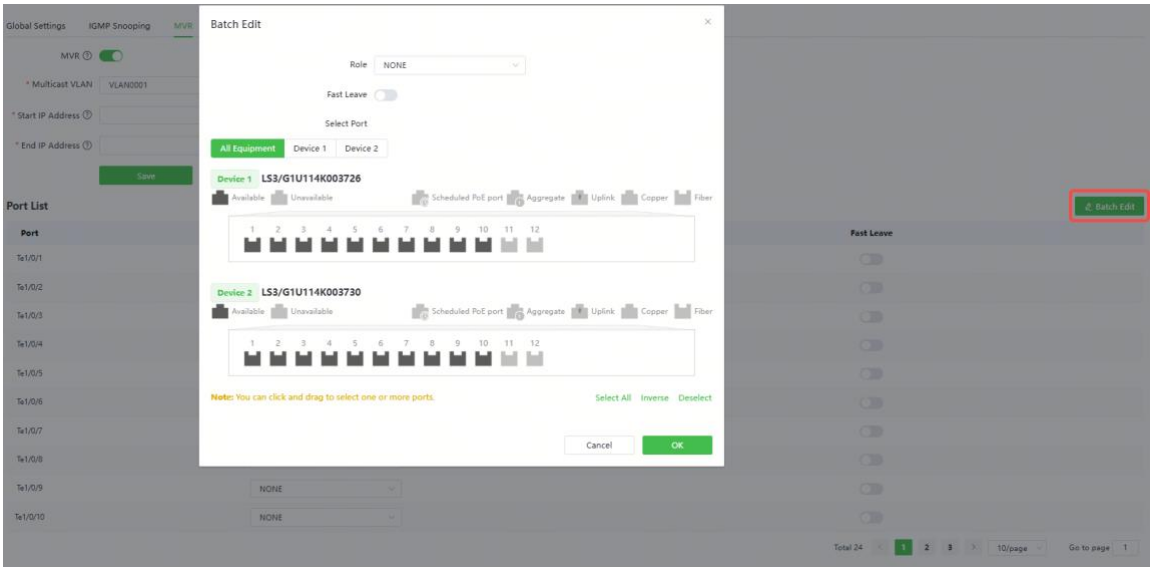
Parameter	Description	Default Value
MVR	Enables/Disables MVR globally	Disable
Multicast VLAN	VLAN of a multicast source	1
Start IP Address	Learned or configured start multicast IP address of an MVR multicast group.	N/A

Parameter	Description	Default Value
End IP Address	Learned or configured end multicast IP address of an MVR multicast group.	N/A

8.4.3 Configuring the MVR Ports

Choose **Local Device** > **L2 Multicast** > **IGMP Snooping** > **MVR**.

- Batch configure: Click **Batch Edit**, select the port role, the port to be set, and whether to enable the Fast Leave function on the port, and click **OK**.



- Configure one port: Click the drop-down list box to select the MVR role type of the port. Click the switch in the **Fast Leave** column to set whether the port enables the fast leave function.

Table 8-4 Description of MVR Configuration Parameters of Ports

Parameter	Description	Default Value
Role	**NONE**: Indicates that the MVR function is disabled. **SOURCE**: Indicates the source port that receives multicast data streams. **RECEIVER**: Indicates the receiver port connected to a client.	NONE
Fast Leave	Configures the fast leave function for a port. After the function is enabled, if the port receives the leave packet, it is directly deleted from the multicast group.	Disable

Note

- If a source port or a receiver port is configured, the source port must belong to the MVR VLAN and the receiver port must not belong to the MVR VLAN.
- The fast leave function takes effect only on the receiver port.

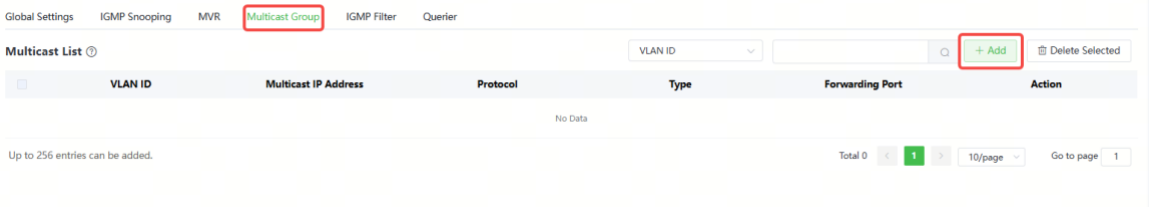
8.5 Configuring Multicast Group

Choose **Local Device** > **L2 Multicast** > **IGMP Snooping** > **Multicast Group**.

A multicast group consists of the destination ports, to which multicast packets are to be sent. Multicast packets are sent to all ports in the multicast group.

You can view the **Multicast List** on the current page. The search box in the upper-right corner supports searching for multicast group entries based on VLAN IDs or multicast addresses.

Click **Add** to create a multicast group. After configuration, click **OK**.



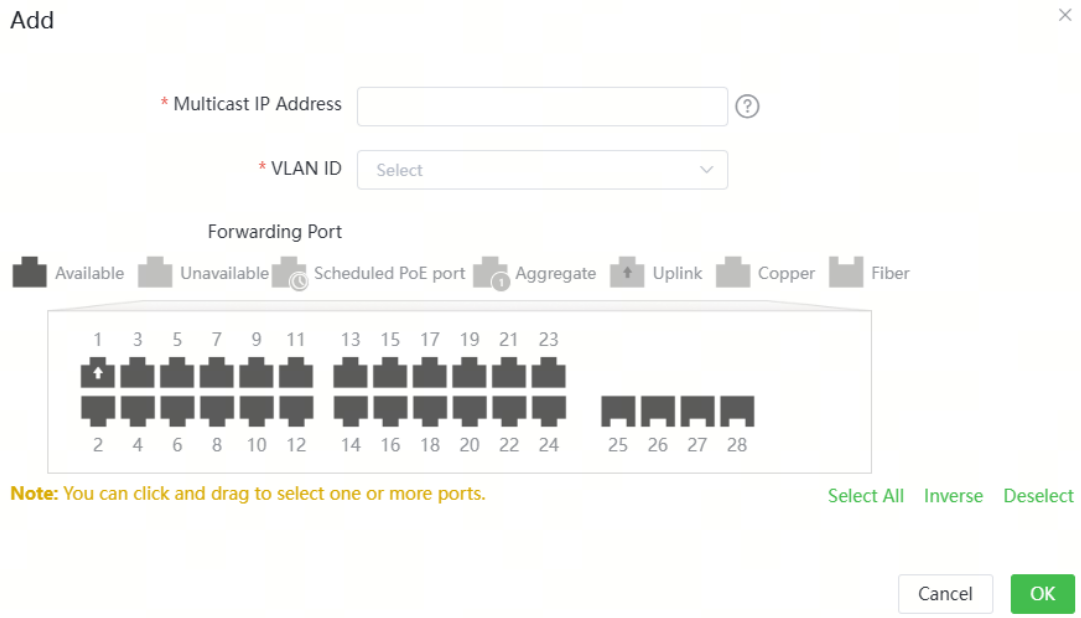


Table 8-5 Description of Multicast Group Configuration Parameters

Parameter	Description	Default Value
VLAN ID	VLAN, to which received multicast traffic belongs	N/A
Multicast IP Address	Multicast IP address. The value range is from 224.0.1.0 to 239.255.255.255.	N/A
Multicast Source IP Address	IP address of a multicast source. **Note** When the IGMP version configured globally is IGMPv3, this parameter can be set and displayed in the multicast list.	N/A
Protocol	If the VLAN ID is a multicast VLAN and the multicast address is within the multicast IP address range of the MVR, the protocol is MVR. In other cases, the protocol is IGMP snooping.	N/A
Type	Multicast group generation mode can be statically configured or dynamically learned.	N/A

Parameter	Description	Default Value
	In normal cases, a port can join a multicast group only after the port receives an IGMP Report packet from the multicast, that is, dynamically learned mode. If you manually add a port to a group, the port can be statically added to the group and exchanges multicast group information with the PIM router without IGMP packet exchange.	
Forwarding Port	List of ports that forward multicast traffic	N/A
INCLUDE Port	The INCLUDE port only receives traffic from specified multicast source addresses. As shown in the previous figure, the INCLUDE port is Te1/0/4, and receives only traffic with the source address 2.2.2.6 from the multicast traffic with the address 224.2.2.2. **Note** When the IGMP version configured globally is IGMPv3, this parameter can be set and displayed in the multicast list.	N/A
EXCLUDE Port	The EXCLUDE port does not receive traffic from specified multicast source addresses. As shown in the previous figure, the EXLUDE port is Te1/0/5, and does not receive multicast traffic with the source address 2.2.2.6 from the multicast traffic with the address 224.2.2.2. **Note** When the IGMP version configured globally is IGMPv3, this parameter can be set and displayed in the multicast list.	N/A

Note

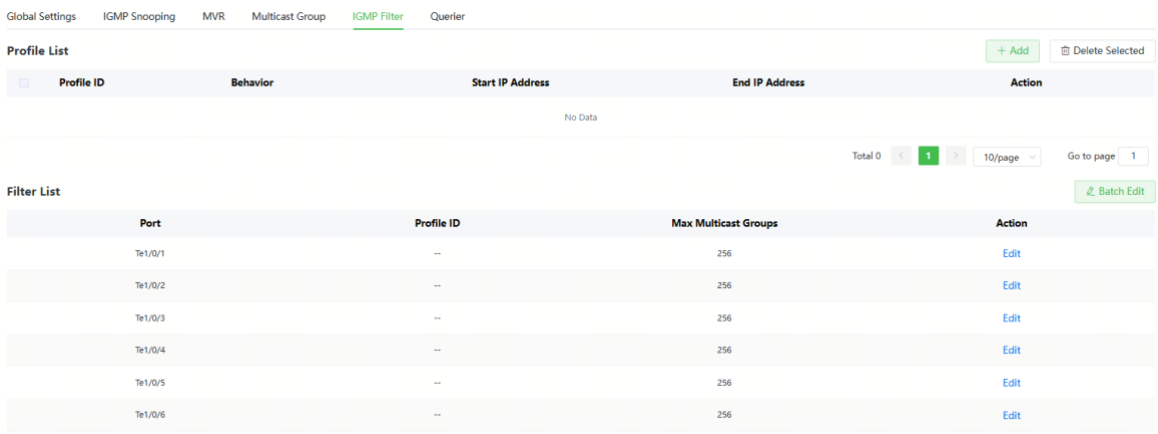
Static multicast groups cannot learn other dynamic forwarding ports.

8.6 Configuring a Port Filter

Choose **Local Device** > **L2 Multicast** > **IGMP Snooping** > **IGMP Filter**.

Generally, the device running ports can join any multicast group. A port filter can configure a range of multicast groups that permit or deny user access, you can customize the multicast service scope for users to guarantee the interest of operators and prevent invalid multicast traffic.

There are 2 steps to configure the port filter: configure the profile and set a limit to the range of the port group address.



8.6.1 Configuring a Profile

Choose **Local Device** > **L2 Multicast** > **IGMP Snooping** > **IGMP Filter** > **Profile List**.

Click **Add** to create a **Profile**. A profile is used to define a range of multicast groups that permit or deny user access for reference by other functions.

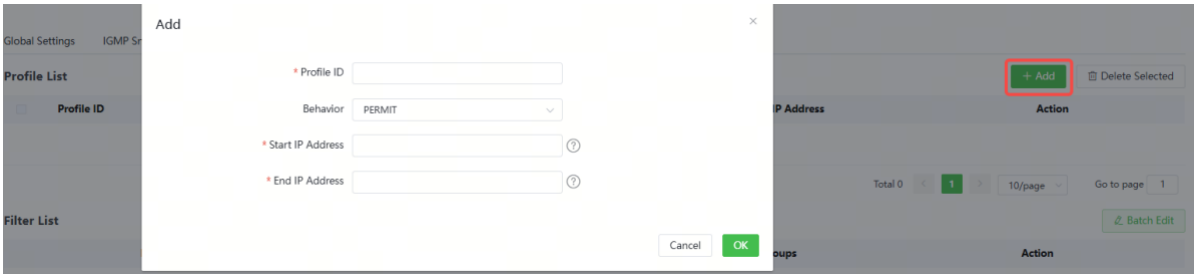


Table 8-6 Description of Profile Configuration Parameters

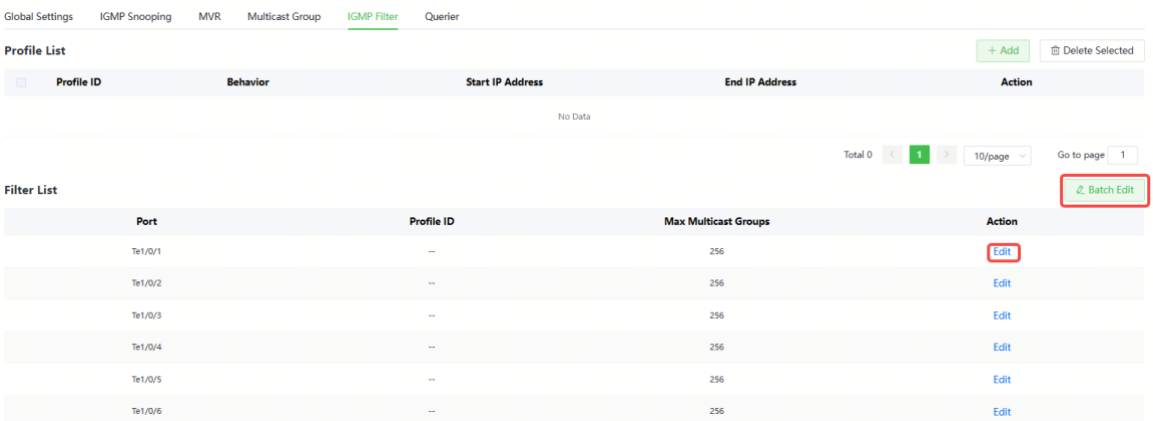
Parameter	Description	Default Value
Profile ID	Profile ID	N/A
Behavior	**DENY**: Forbids demanding multicast IP addresses in a specified range. **PERMIT**: Only allows demanding multicast IP addresses in a specified range.	N/A
Start IP Address	Start Multicast IP address of the range of multicast group addresses	N/A
End IP Address	End Multicast IP address of the range of multicast group addresses	N/A

8.6.2 Configuring a Range of Multicast Groups for a Profile

Choose **Local Device** > **L2 Multicast** > **IGMP Snooping** > **IGMP Filter** > **Filter List**.

The port filter can cite a profile to define the range of multicast group addresses that can be or cannot be demanded by users on a port.

Click **Batch Edit**, or click **Edit** of a single port entry. In the displayed dialog box, select profile ID and enter the maximum number of multicast groups allowed by a port and click **OK**.



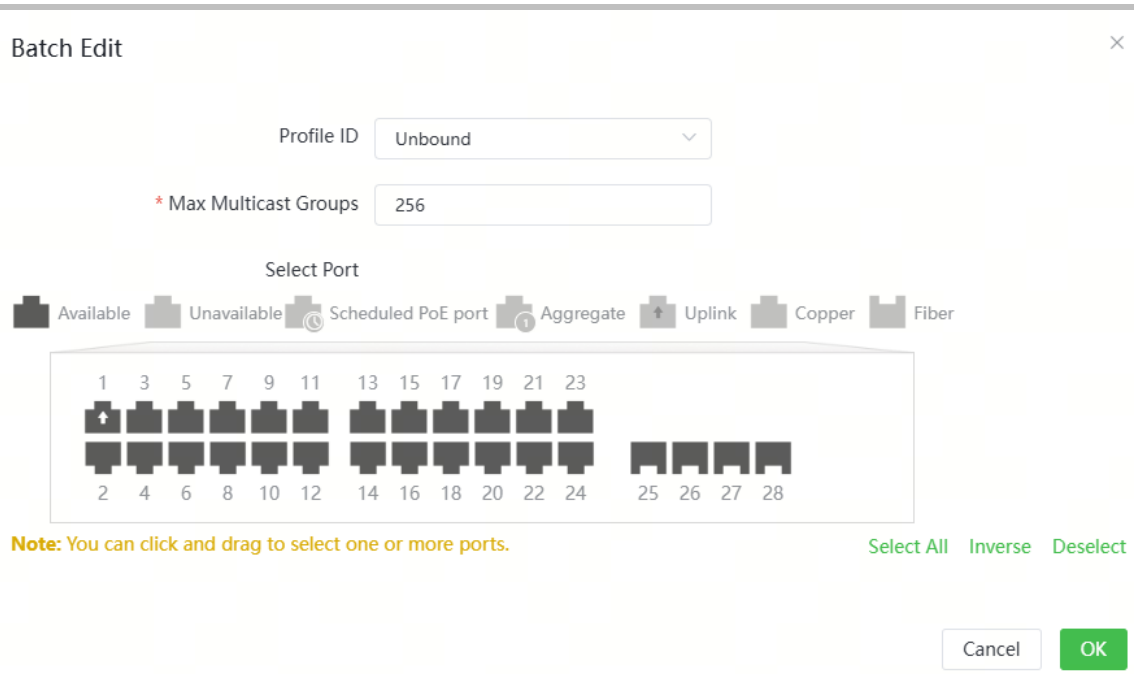


Table 8-7 Description of Port Filter Configuration Parameters

Parameter	Description	Default Value
Profile ID	Profile that takes effect on a port. If it is not set, no profile rule is bound to the port.	NA
Max Multicast Groups	Maximum number of multicast groups that a port can join. If too much multicast traffic is requested concurrently, the multicast device will be severely burdened. Therefore, configuring the maximum number of multicast groups allowed for the port can guarantee the bandwidth.	256

8.7 Setting an IGMP Querier

8.7.1 Overview

In a three-layer multicast network, the Layer 3 multicast device serves as the querier and runs IGMP to maintain group membership. Layer 2 multicast devices only need to

listen to IGMP packets to establish and maintain forwarding entries and implement Layer 2 multicasting. When a multicast source and user host are in the same Layer 2 network, the query function is unavailable because the Layer 2 device does not support IGMP. To resolve this problem, you can configure the IGMP snooping querier function on the Layer 2 device so that the Layer 2 device sends IGMP Query packets to user hosts on behalf of the Layer 3 multicast device, and listens to and maintains IGMP Report packets responded by user hosts to establish Layer 2 multicast forwarding entries.

8.7.2 Procedure

Choose **Local Device** > **L2 Multicast** > **IGMP Snooping** > **Querier**.

One querier is set for each VLAN. The number of queriers is the same as that of device VLANs.

In **Querier List**, click **Edit** in the last **Action** column. In the displayed dialog box, select whether to enable the querier, set the querier version, querier source IP address, and packet query interval, and click **OK**.

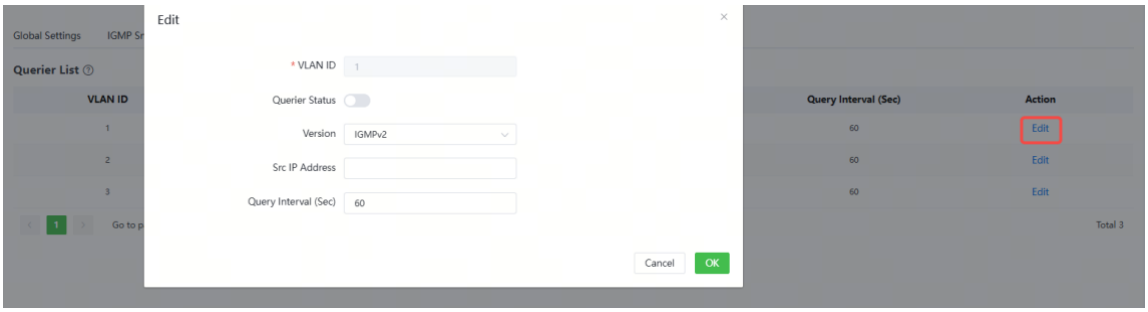


Table 8-8 Description of Querier Configuration Parameters

Parameter	Description	Default Value
Querier Status	Whether to enable or disable the VLAN querier function.	Disable
Version	IGMP Protocol version of query packets sent by the querier. It can be set to IGMPv2 or IGMPv3.	IGMPv2
Src IP Address	Source IP address carried in query packets sent by the querier.	N/A

Parameter	Description	Default Value
Query Interval (Sec)	Packet transmission interval, of which the value range is from 30 to 18000, in seconds.	60 seconds

Note

- The querier version cannot be higher than the global IGMP version. When the global IGMP version is lowered, the querier version is lowered accordingly.
- If no querier source IP is configured, the device management IP is used as the source IP address of the querier.

9 Viewing Optical Transceiver Info

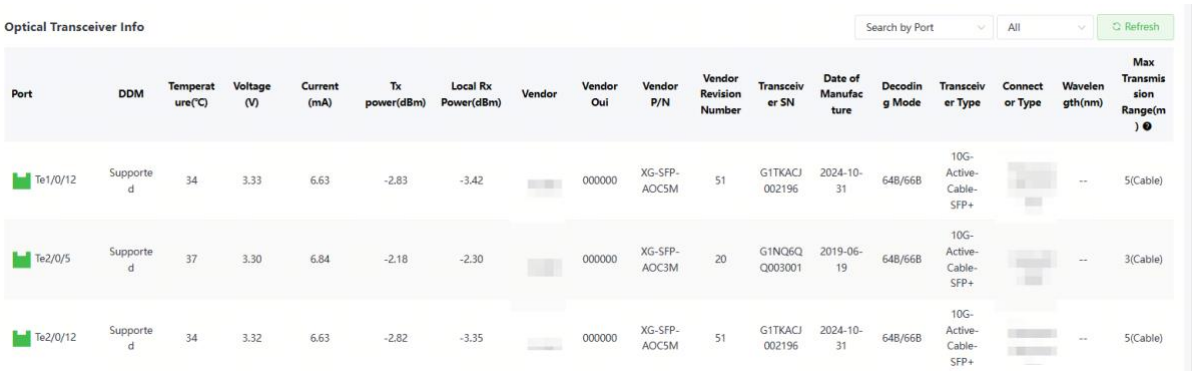
Specification

The information depends on the actual product.

Choose **Local Device** > **Optical Transceiver Monitoring** > **Optical Transceiver Info**.

The **Optical Transceiver Info** page displays the basic information of an optical transceiver, including the port to which it is connected, DDM, temperature, voltage, current, Tx power, local Rx power, and so on. You can query the information of an optical transceiver by entering the port to which it is connected in the search box.

The data on this page is automatically updated every 5 seconds. You can also click **Refresh** to refresh the optical transceiver information.



Port	DDM	Temperature(℃)	Voltage (V)	Current (mA)	Tx power(dBm)	Local Rx Power(dBm)	Vendor	Vendor Oui	Vendor P/N	Vendor Revision Number	Transceiver SN	Date of Manufacture	Decoding Mode	Transceiver Type	Connector Type	Wavelength(nm)	Max Transmission Range(m)
Te1/0/12	Supported	34	3.33	6.63	-2.83	-3.42		000000	XG-SFP-AOC5M	51	G1TKACJ002196	2024-10-31	64B/66B	10G-Active-Cable-SFP+		--	5(Cable)
Te2/0/5	Supported	37	3.30	6.84	-2.18	-2.30		000000	XG-SFP-AOC3M	20	G1NQ6QQ003001	2019-06-19	64B/66B	10G-Active-Cable-SFP+		--	3(Cable)
Te2/0/12	Supported	34	3.32	6.63	-2.82	-3.35		000000	XG-SFP-AOC5M	51	G1TKACJ002196	2024-10-31	64B/66B	10G-Active-Cable-SFP+		--	5(Cable)

10 Security

10.1 DHCP Snooping

10.1.1 Overview

The Dynamic Host Configuration Protocol (DHCP) snooping function allows a device to snoop DHCP packets exchanged between clients and a server to record and monitor the IP address usage and filter out invalid DHCP packets, including request packets from the clients and response packets from the server. DHCP snooping records generated user data entries to serve security applications such as IP Source Guard.

10.1.2 Standalone Device Configuration

Choose **Local Device** > **Security** > **DHCP Snooping**.

Turn on the DHCP snooping function, select the port to be set as trusted ports on the port panel and click **Save**. After DHCP Snooping is enabled, request packets from DHCP clients are forwarded only to trusted ports; for response packets from DHCP servers, only those from trusted ports are forwarded.

Note

Generally, the uplink port connected to the DHCP server is configured as a trusted port.

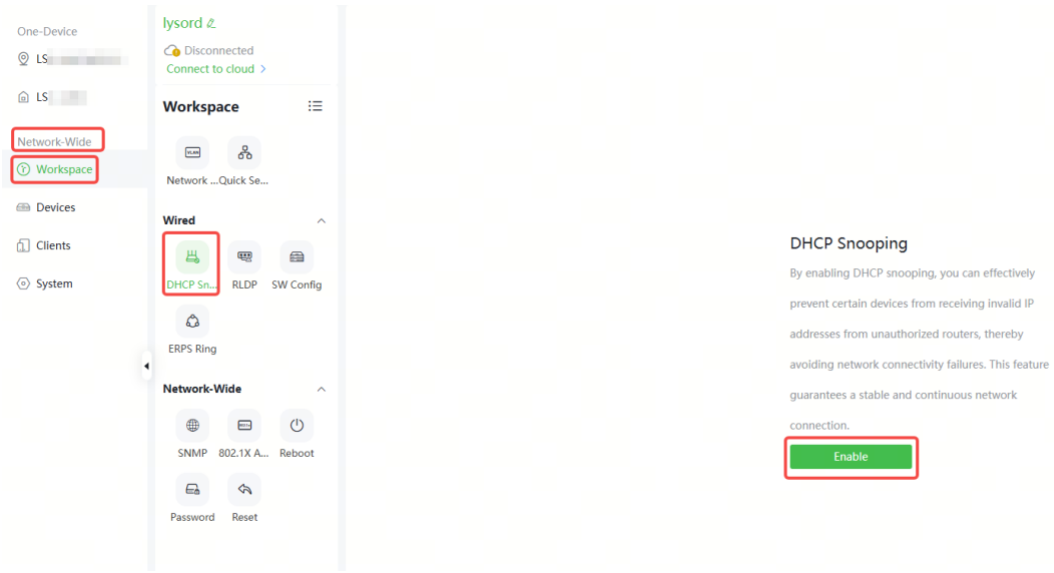
Option 82 is used to enhance the DHCP server security and optimize the IP address assignment policy. Option 82 information will be carried in the DHCP request packet when Option 82 is turned on.

10.1.3 Batch Configuring Network Switches

Choose **Network-Wide** > **Workspace** > **Wired** > **DHCP Snooping**.

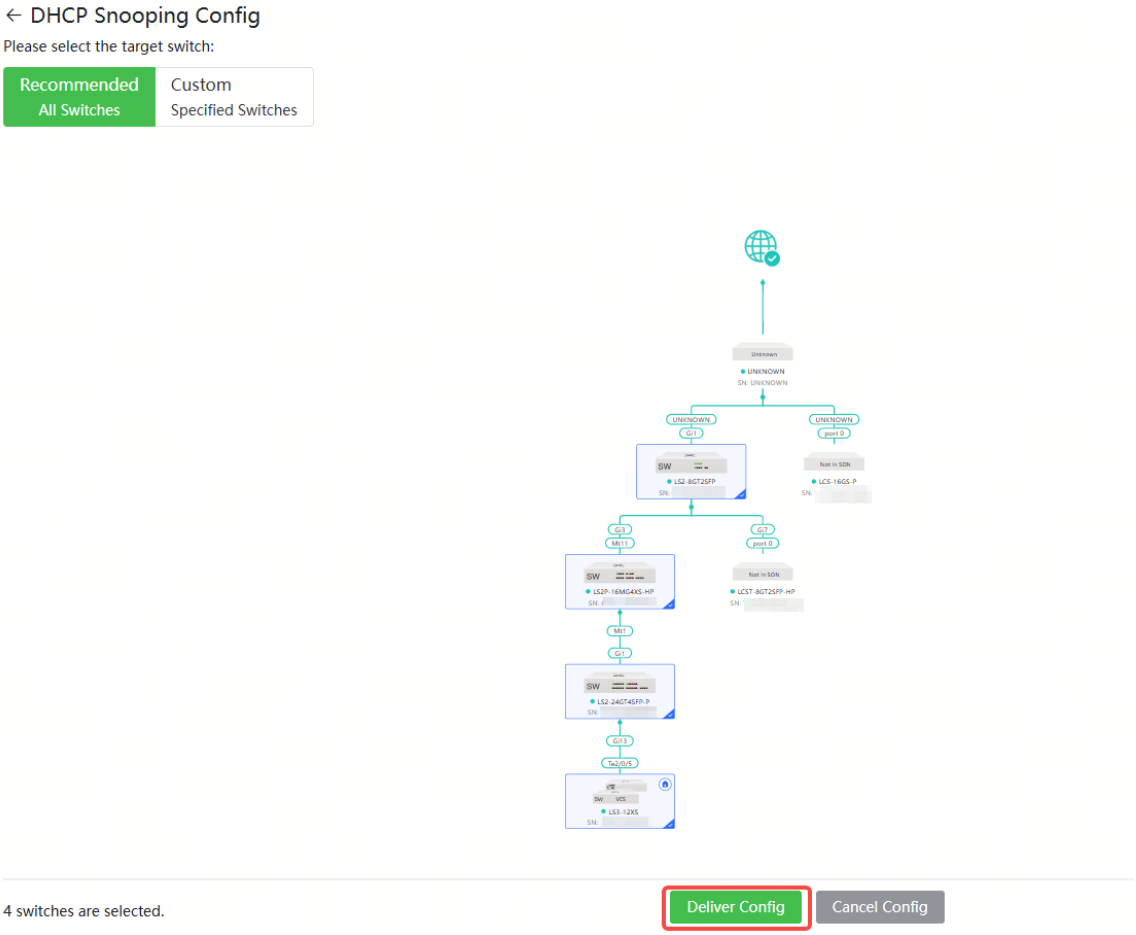
Enabling DHCP Snooping on network switches can ensure that users can only obtain network configuration parameters from the DHCP server within the control range, and avoid a host on the original network obtaining an IP address assigned by an unauthorized router, so as to guarantee the stability of the network.

(1) Click **Enable** to access the **DHCP Snooping Config** page.

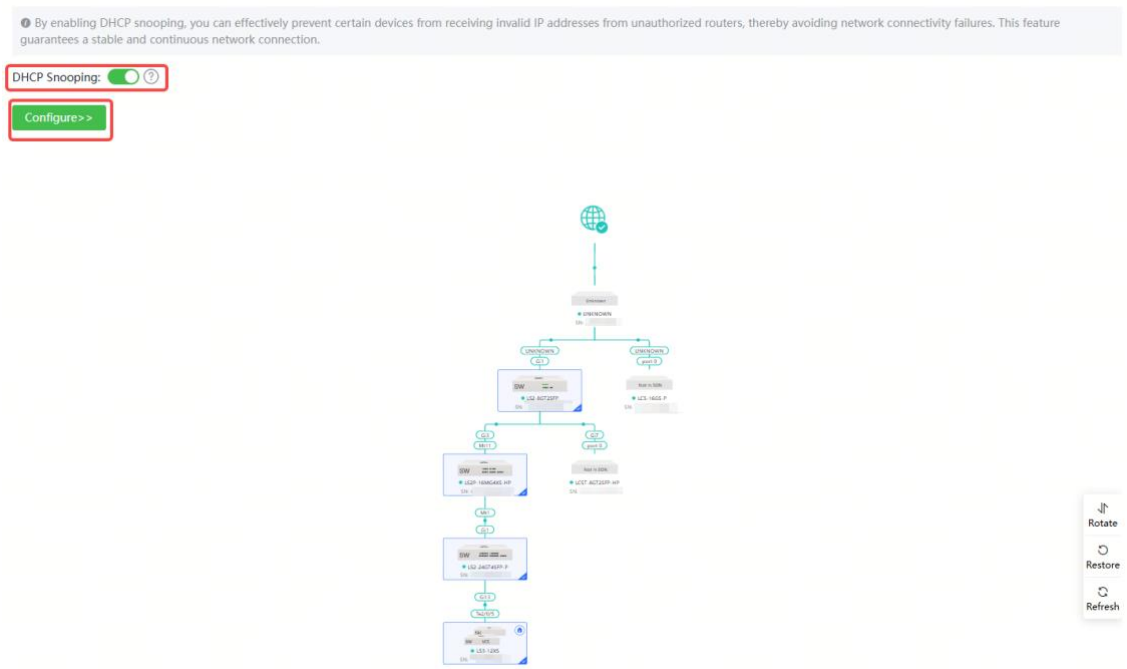


(2) In the networking topology, you can select the access switches on which you want to enable DHCP Snooping in either recommended or custom mode. If you select the recommended mode, all switches in the network are selected automatically. If you select

the custom mode, you can manually select the desired switches. Click **Deliver Config**. DHCP Snooping is enabled on the selected switches.



(3) After the configuration is delivered, if you need to modify the effective range of the anti-private connection function, click **Configure** to reselect the switch that enables the anti-private connection in the topology. After the configuration is delivered, if you want to modify the effective range of the DHCP Snooping function, click **Configure** to select desired switches in the topology again. Turn off **DHCP Snooping** to disable DHCP Snooping on all switches with one click.



10.2 Storm Control

10.2.1 Overview

When a local area network (LAN) has excess broadcast, multicast, or unknown unicast data flows, the network speed will slow down and packet transmission will have an increased timeout probability. This is called LAN storm, which may be caused by topology protocol execution errors or incorrect network configuration.

Users can perform storm control separately for the broadcast, multicast, and unknown unicast data flows. When the rate of broadcast, multicast, or unknown unicast data flows received over a device port exceeds the specified range, the device transmits only packets in the specified range and discards packets beyond the range until the packet rate falls within the range. This prevents flooded data from entering the LAN and causing a storm.

10.2.2 Procedure

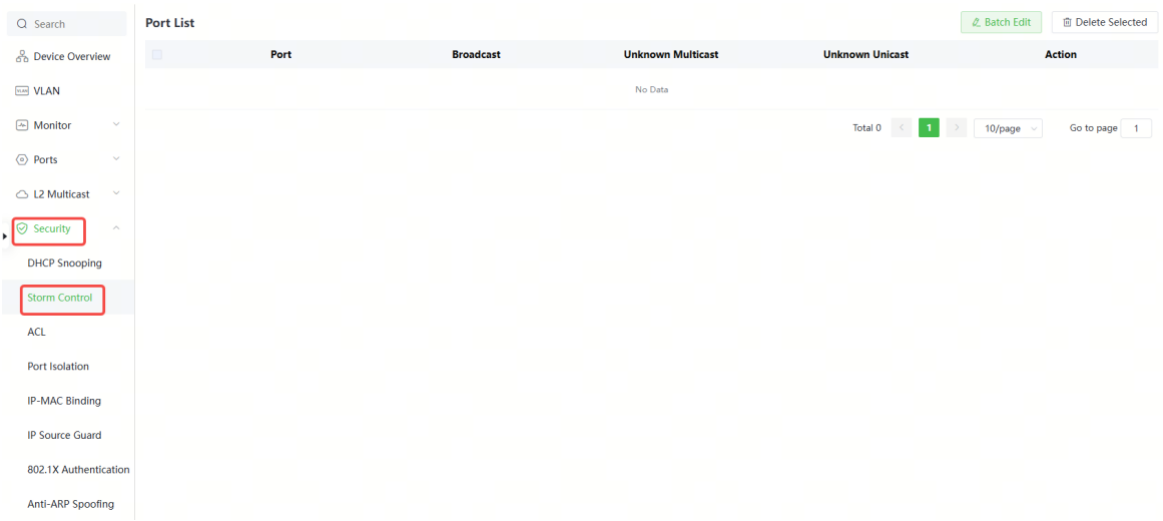
Choose **Local Device** > **Security** > **Storm Control**.

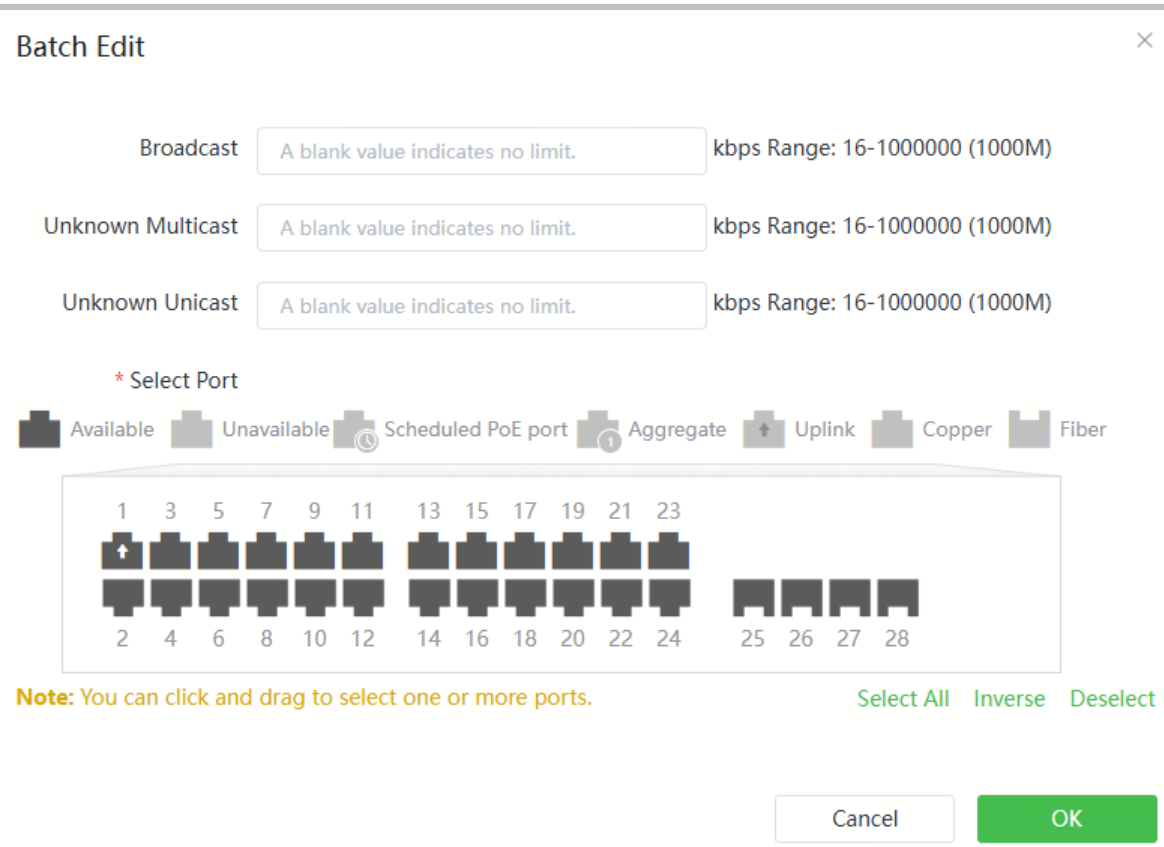
Click **Batch Edit**. In the displayed dialog box, select configuration types and ports, enter the rate limits of broadcast, unknown multicast, and unknown unicast, and click **OK**. To

modify or delete the rate limit rules after completing the configuration, you can click **Edit** or **Delete** in the **Action** column.

There are two configuration types:

- Storm control based on packets per second: If the rate of data flows received over a device port exceeds the configured packets-per-second threshold, excess data flows are discarded until the rate falls within the threshold.
- Storm control based on kilobytes per second: If the rate of data flows received over a device port exceeds the configured kilobytes-per-second threshold, excess data flows are discarded until the rate falls within the threshold.





10.3 ACL

10.3.1 Overview

An access control list (ACL) is commonly referred to as packet filter in some documents. An ACL defines a series of permit or deny rules and applies these rules to device interfaces to control packets sent to and from the interfaces, so as to enhance security of the network device.

You can add ACLs based on MAC addresses or IP addresses and bind ACLs to ports.

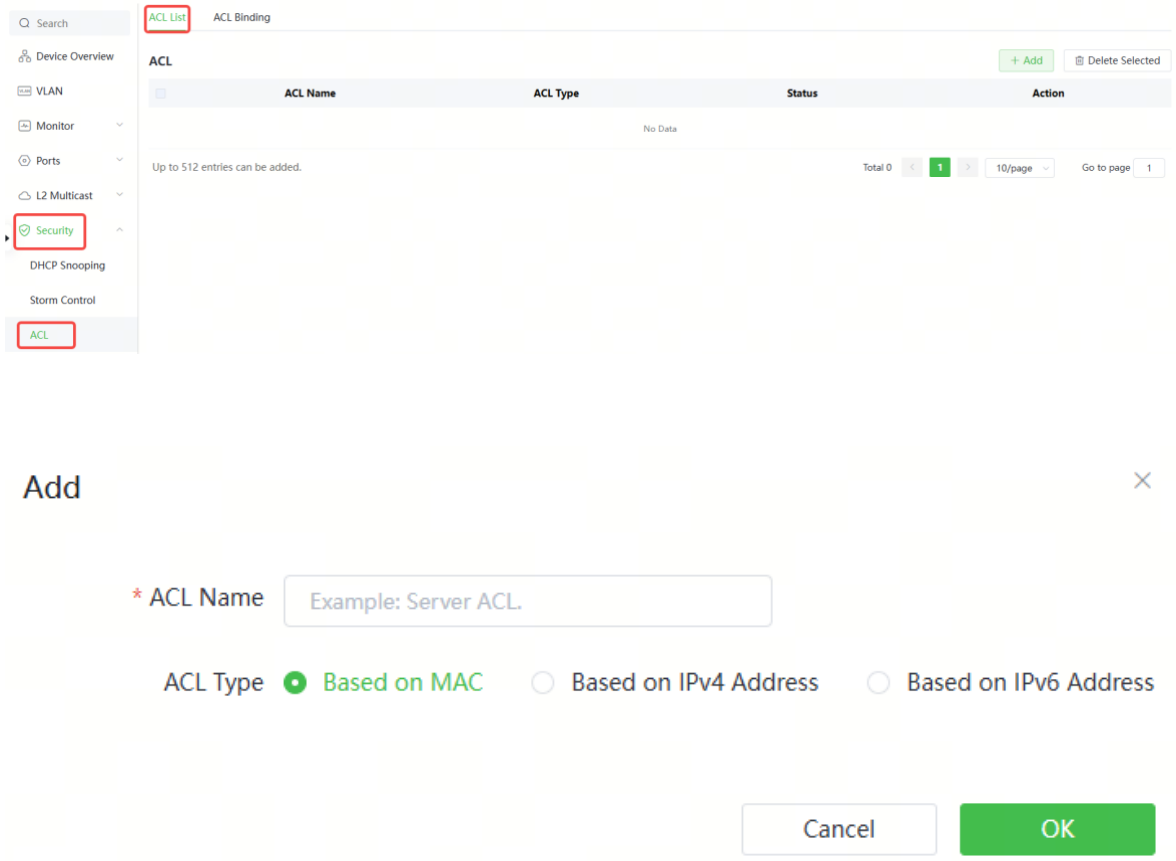
10.3.2 Creating ACL Rules

Choose **Local Device** > **Security** > **ACL** > **ACL List**.

(1) Click **Add** to set the ACL control type, enter an ACL name, and click **OK**.

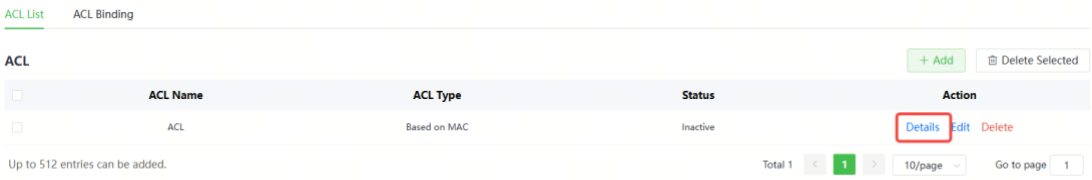
- Based on MAC address: To control the Layer 2 packets entering/leaving the port, and deny or permit specific Layer 2 packets destined to a network.
- Based on IP address: To control the IP packets entering/leaving a port, and deny or

permit specific IP packets destined to a network.



(2) Click **Details** in the **Action** column of the ACL entry, set the filtering rules in the pop-up sidebar, and click **Save** to add rules for the ACL. Multiple rules can be added.

The rules include two actions of **Allow** or **Block**, and the matching rules of packets. The sequence of a Rule in an ACL determines the matching priority of the Rule in the ACL. When processing packets, the network device matches packets with ACEs based on the Rule sequence numbers. Click **Move** in the rule list to adjust the matching order.



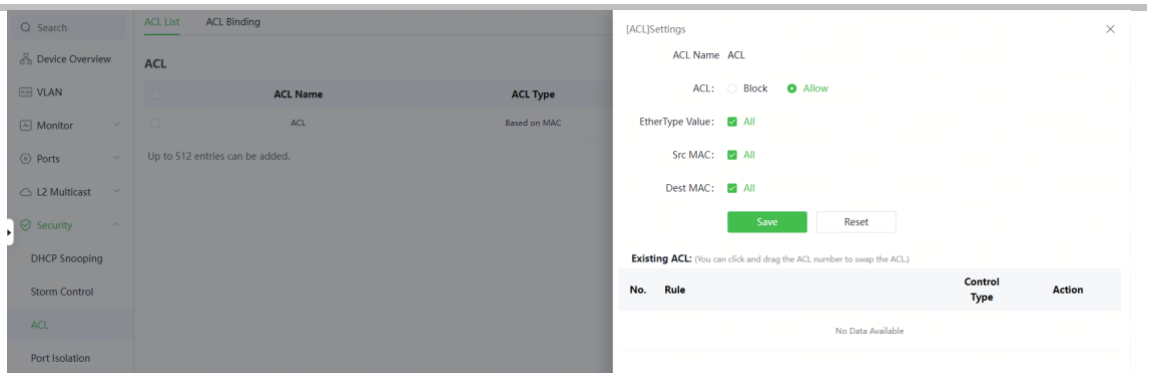


Table 10-1Description of ACL Rule Configuration Parameters

Parameter	Description
ACL	Configuring ACL Rules Action Block: If packets match this rule, the packets are denied. Allow: If packets match this rule, the packets are permitted.
IP Protocol Number	Match IP protocol number The value ranges from 0 to 255. Check **All** to match all IP protocols.
Src IP Address	Match the source IP address of the packet. Check **All** to match all source IP addresses.
Dest IP Address	Match the destination IP address of the packet. Check **All** to match all destination IP addresses.
EtherType Value	Match Ethernet protocol type. The value range is 0x600~0xFFFF. Check **All** to match all protocol type numbers.
Src Mac	Match the MAC address of the source host. Check **All** to match all source MAC addresses.
Dest MAC	Match the MAC address of the destination host. Check **All** to match all destination MAC addresses.

Note

- ACLs cannot have the same name. Only the name of a created ACL can be edited.

- An ACL applied by a port cannot be edited or deleted. To edit, unbind the ACL from the port first.
- There is one default ACL rule that denies all packets hidden at the end of an ACL.

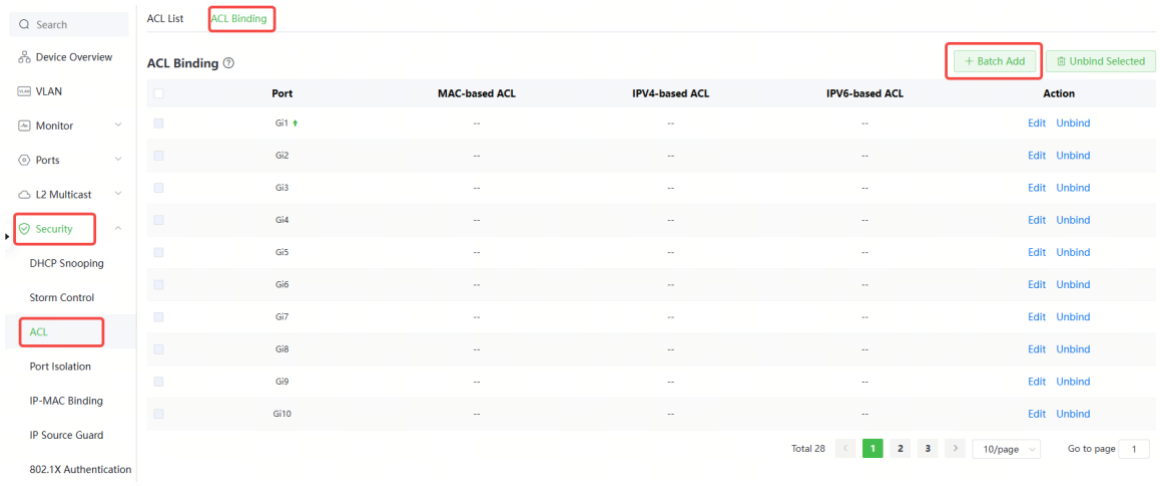
10.3.3 Applying ACL Rules

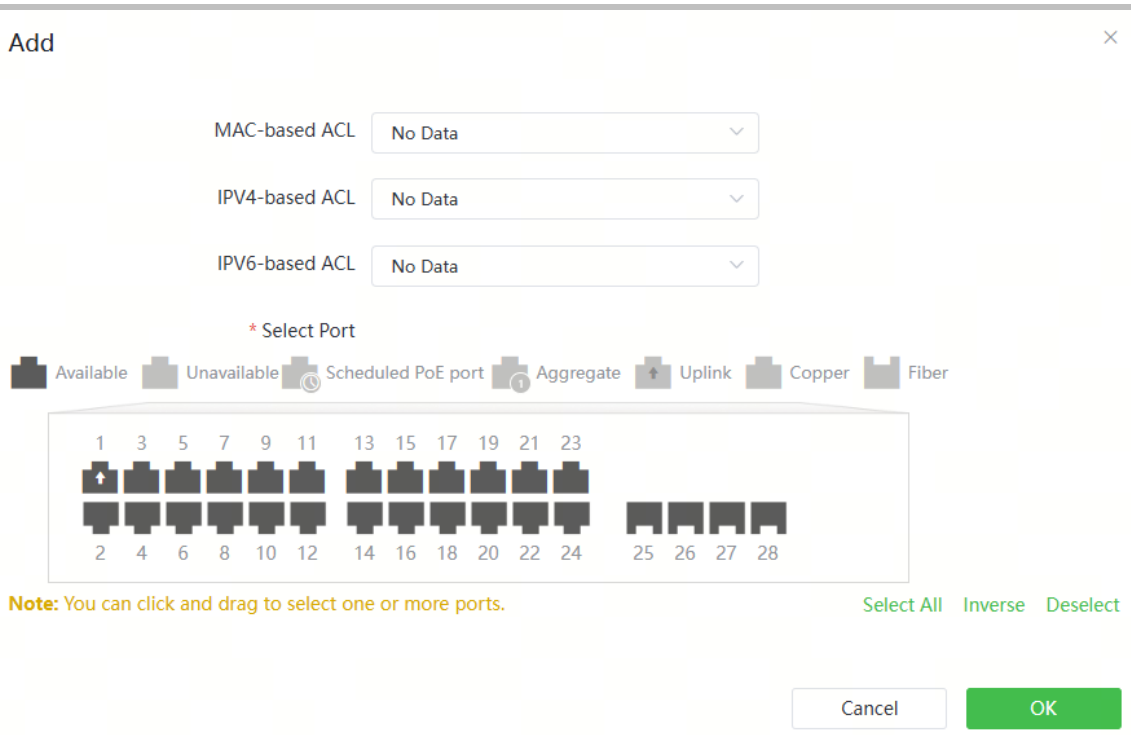
Choose **Local Device** > **Security** > **ACL** > **ACL List**.

Click **Batch Add** or **Edit** in the **Action** column, select the desired MAC ACL and IP ACL for ports, and click **OK**.

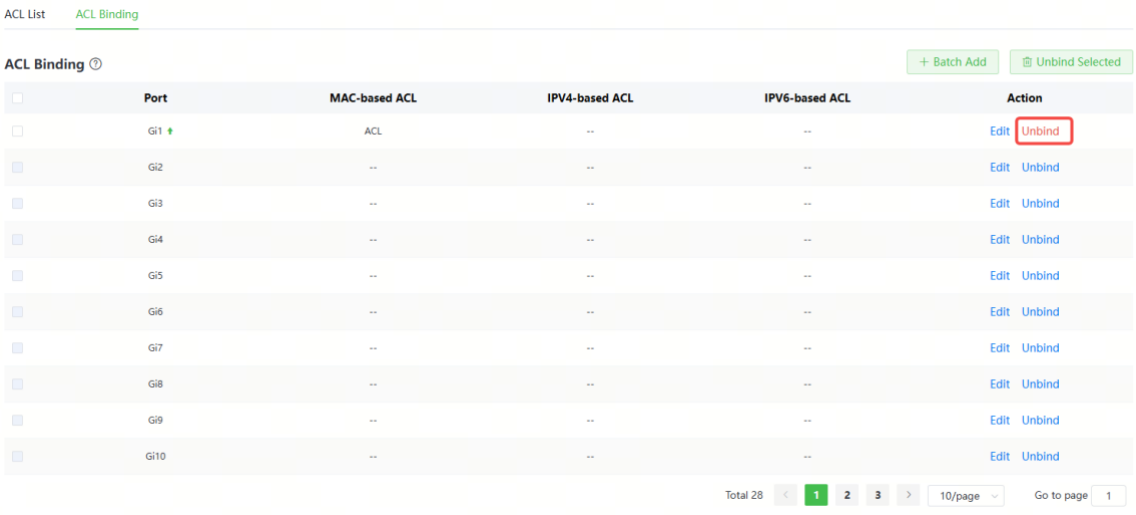
Note

Currently, ACLs can be applied only in the inbound direction of ports, that is, to filter incoming packets.





After an ACL is applied to a port, you can click **Unbind** in the **Action** column, or check the port entry and click **Delete Selected** to unbind the ACL from the port.



10.4 Port Isolation

Choose **Local Device** > **Security** > **Port Isolation**.

In some scenarios, communication is required to be disabled between some ports on the device. For this purpose, you can configure some ports as isolated ports. Ports with

port isolation enabled cannot communicate with each other, and Layer 2 isolation is implemented on users connecting to the ports. However, the isolated and non-isolated ports can communicate with each other.

Port isolation is disabled by default, which can be enabled by clicking to batch enable port isolation for multiple ports, you can click **Batch Edit** to enable port isolation**,** select desired port and click **OK.**

10.5 IP-MAC Binding

10.5.1 Overview

After IP-MAC binding is configured on a port, to improve security, the device checks whether the source IP addresses and source MAC addresses of IP packets are those configured for the device, filters out IP packets not matching the binding, and strictly control the validity of input sources.

10.5.2 Procedure

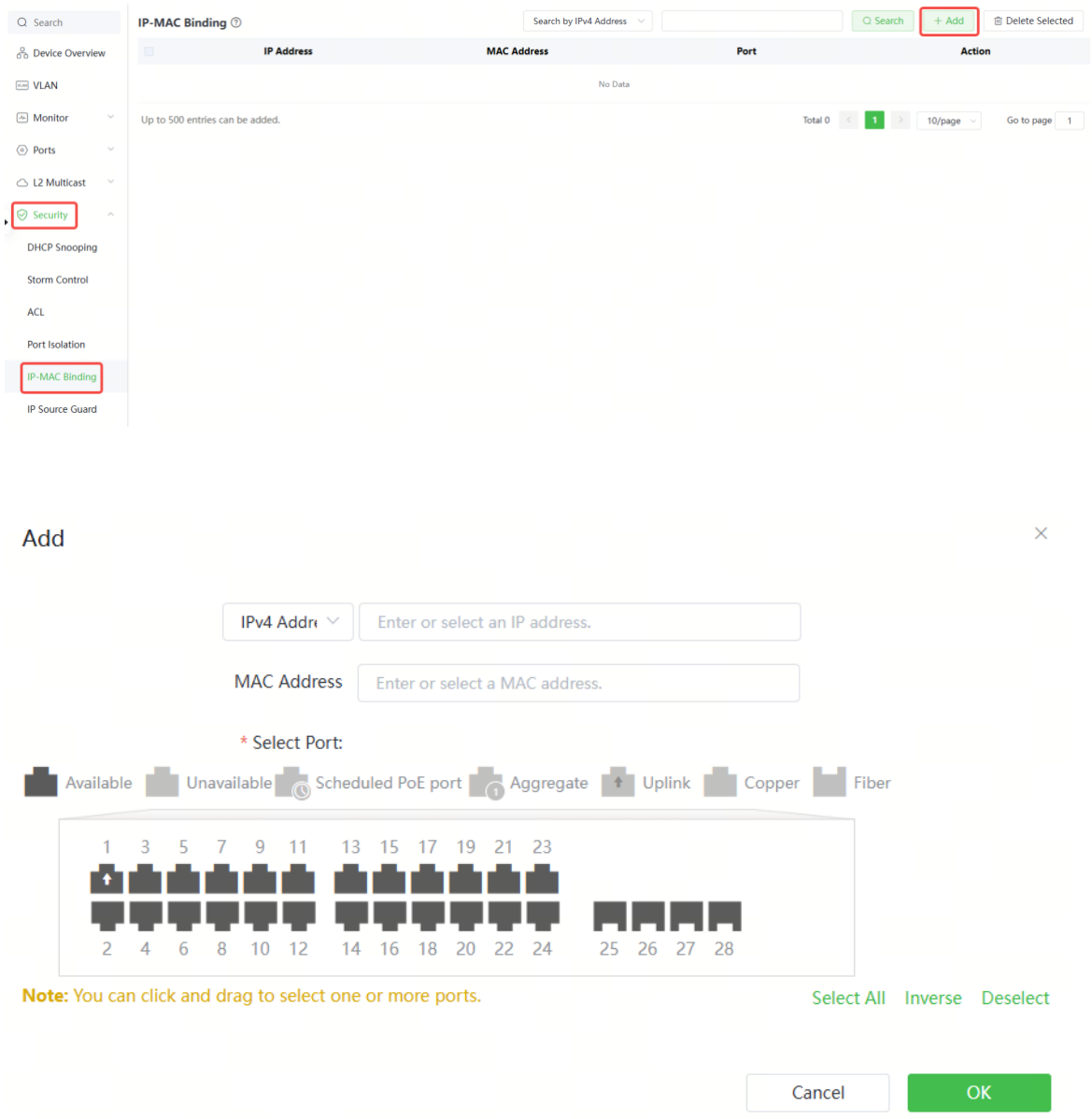
Choose **Local Device** > **Security** > **IP-MAC Binding**.

1. Adding an IP-MAC Binding Entry

Click **Add**, select the desired port, enter the IP address and MAC address to be bound, and click **OK**. At least one of the IP address and MAC address needs to be entered. To modify the binding, you can click **Edit** in the **Action** column.

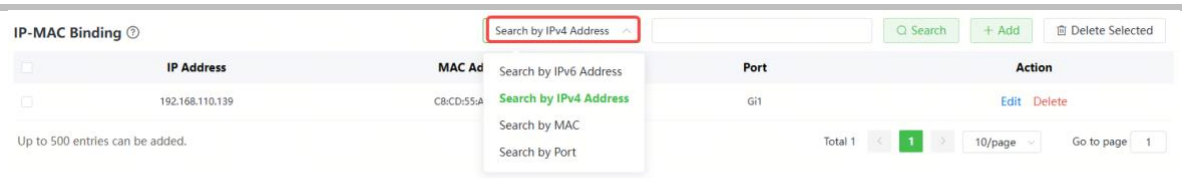
Caution

IP-MAC Binding take effects prior to ACL, but it has the same privilege with IP Source Guard. The packet matching either configuration will be allowed to pass through.



2. Searching Binding Entries

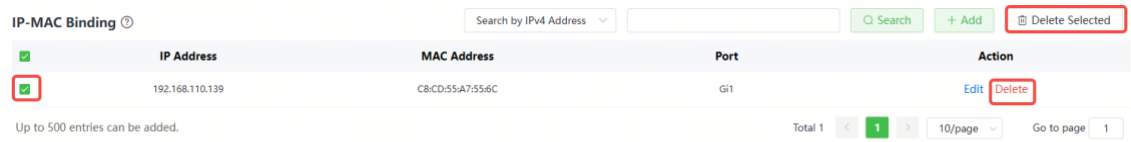
The search box in the upper-right corner supports finding binding entries based on IP addresses, MAC addresses or ports. Select the search type, enter the search string, and click **Search**. Entries that meet the search criteria are displayed in the list.



3. Deleting an IP-MAC Binding Entry

Batch Configure: In **IP-MAC Binding List**, select an entry to be deleted and click **Delete Selected**. In the displayed dialog box, click **OK**.

Delete one binding entry: click **Delete** in the last **Action** column of the entry in the list. In the displayed dialog box, click **OK**.



10.6 IP Source Guard

10.6.1 Overview

After the IP Source Guard function is enabled, the device checks IP packets from DHCP non-trusted ports. You can configure the device to check only the IP field or IP+MAC field to filter out IP packets not matching the binding list. It can prevent users from setting private IP addresses and forging IP packets.

Caution

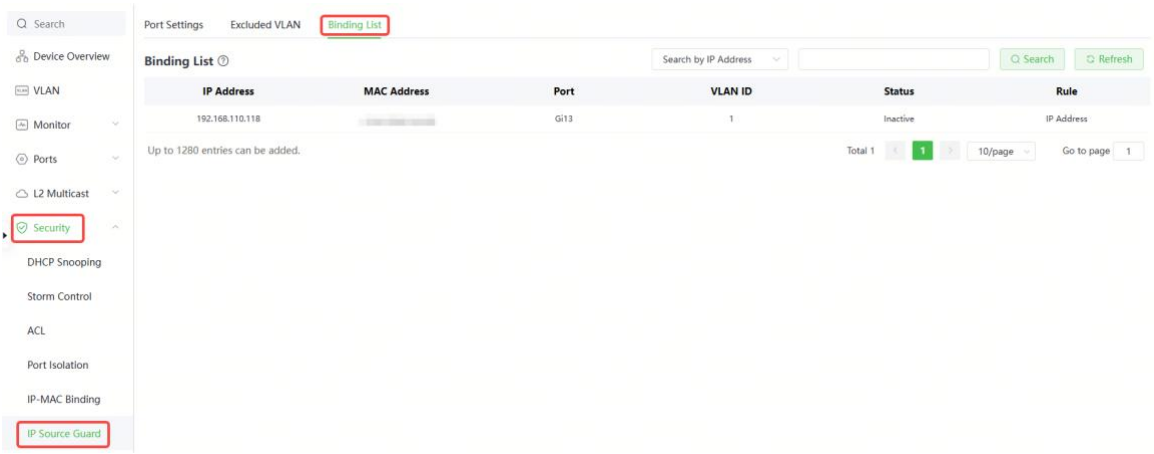
IP Source Guard should be enabled together with DHCP snooping. Otherwise, IP packet forwarding may be affected. To configure DHCP Snooping function, see 10.1 DHCP Snooping for details.

10.6.2 Viewing Binding List

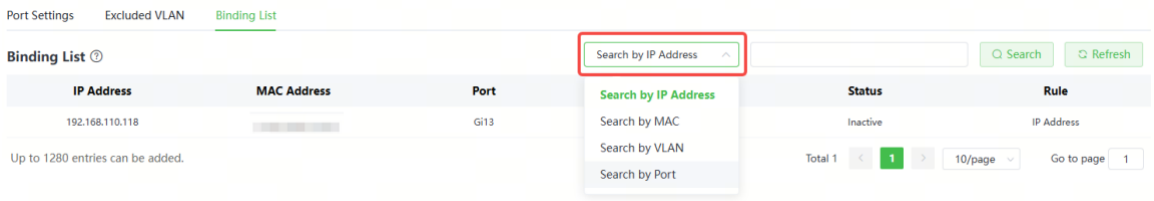
Choose **Local Device** > **Security** > **IP Source Guard** > **Binding List**.

The binding list is the basis for IP Source Guard. Currently, data in **Binding List** is sourced from dynamic learning results of DHCP snooping binding database. When IP Source Guard is enabled, data of the DHCP Snooping binding database is synchronized to the binding list of IP Source Guard. In this case, IP packets are filtered strictly through IP Source Guard on devices with DHCP Snooping enabled.

Click **Refresh** to obtain the latest data in **Binding List**.



The search box in the upper-right corner supports finding the specified entry in **Binding List** based on IP addresses, MAC addresses, VLANs or ports. Click the drop-down list box to select the search type, enter the search string, and click **Search**.



10.6.3 Enabling Port IP Source Guard

Choose **Local Device** > **Security** > **IP Source Guard** > **Basic Settings**.

In Port List, click **Edit** in the **Action** column. Select **Enabled** and select the match rule, and click **OK**.

There are two match rules:

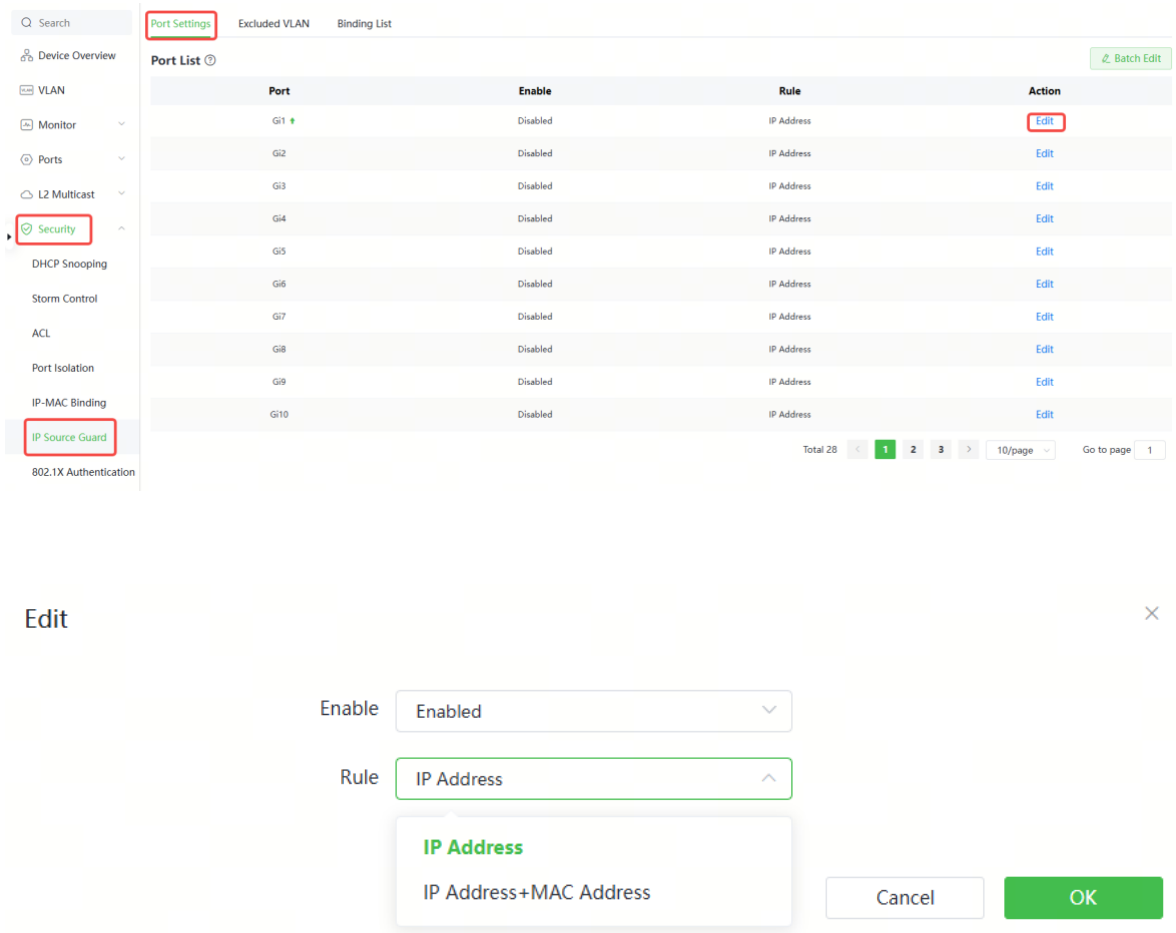
- IP address: The source IP addresses of all IP packets passing through the port are checked. Packets are allowed to pass through the port only when the source IP

addresses of these packets match those in the binding list.

- IP address + MAC address: The source IP addresses and MAC addresses of IP packets passing through the port are checked. Packets are allowed to pass through the port only when both the Layer 2 source MAC addresses and Layer 3 source IP addresses of these packets match an entry in the binding list.

Caution

- IP Source Guard cannot be enabled on a DHCP Snooping trusted port.
- Only on a Layer 2 interface can IP Source Guard be enabled.



10.6.4 Configuring Exceptional VLAN Addresses

Choose **Local Device** > **Security** > **IP Source Guard** > **Excluded VLAN**.

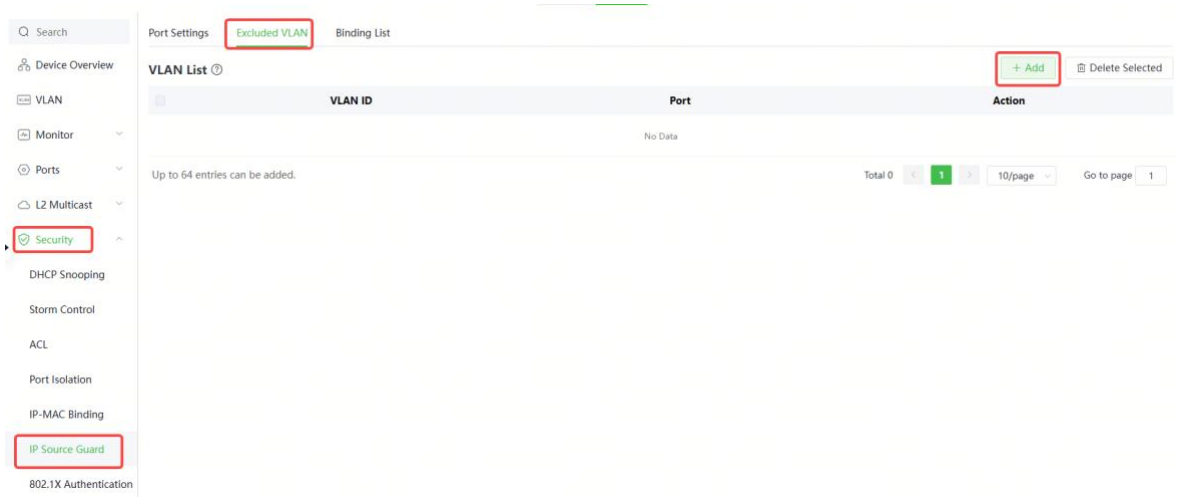
When IP Source Guard is enabled on an interface, it is effective to all the virtual local area networks (VLANs) under the interface by default. Users can specify excluded

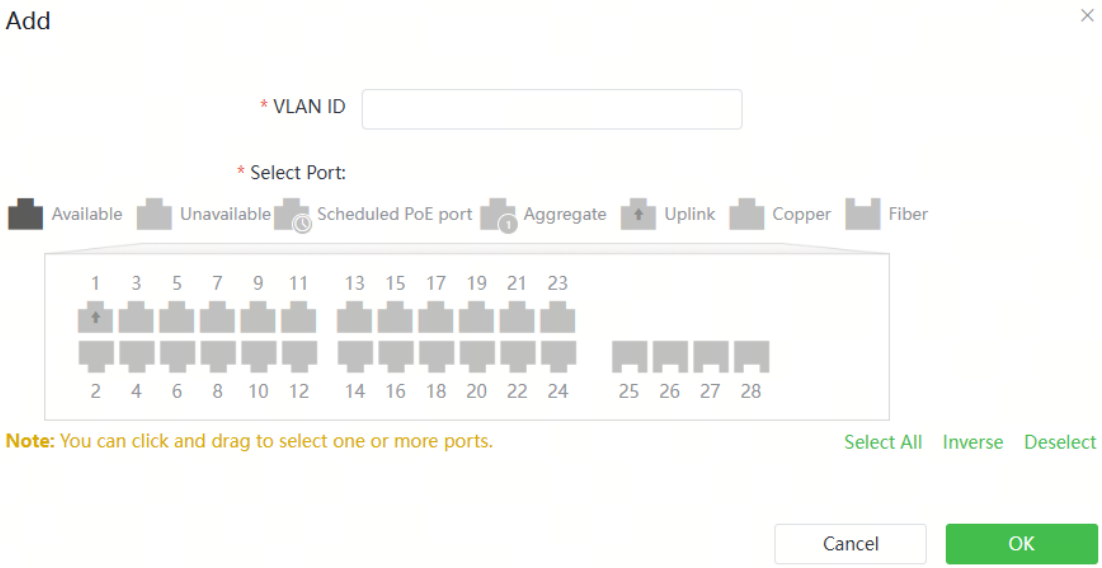
VLANs, within which IP packets are not checked or filtered, that is, such IP packets are not controlled by IP Source Guard.

Click **Edit**, enter the Excluded VLAN ID and the desired port, and click **OK**.

Caution

Excluded VLANs can be specified on a port only after IP Source Guard is enabled on the port. Specified excluded VLANs will be deleted automatically when IP Source Guard is disabled on the port.





10.7 Configuring IEEE 802.1X Authentication

10.7.1 Function Introduction

1. Overview of IEEE 802.1X Authentication

IEEE 802.1X, an IEEE standard for port-based network access control (PNAC), provides protected authentication for a secure access to LANs. Its main purpose is to determine port availability. When the authentication succeeds, IEEE 802.1X enables the port. Otherwise, the port is disabled.

On a traditional IEEE 802-compliant LAN, users can access network resources without authentication, posing security risks. This is where IEEE 802.1X comes in.

Compared with traditional access methods, IEEE 802.1X has the following advantages:

- Security and reliability: IEEE 802.1X authentication is performed on a user or device before they access the switch or LAN services. Data can pass through the Ethernet ports only after the authentication succeeds.
- User identification: Identity authentication prevents unauthorized users and devices from accessing LANs and WLANs, and records their login and logout time.
- Simple and efficient quality: IEEE 802.1X uses Ethernet technology to retain the connectionless nature of IP networks, reducing unnecessary overhead and redundancy.

IEEE 802.1X provides authentication, authorization, and accounting (AAA) security applications.

- Authentication: Determines whether a user can access network resources and denies unauthorized users.
- Authorization: Authorizes users to access resources, and controls the permissions of authorized users.
- Accounting: Records network resources used by users for subsequent accounting.

IEEE 802.1X can be deployed on networks to control user access, authenticate users, and authorize services.

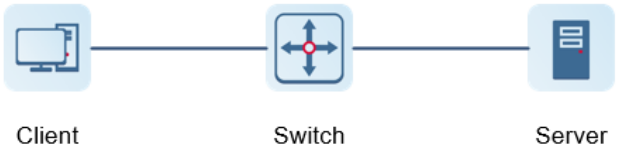
Note

Lysora switches only support authentication.

2. IEEE 802.1X authentication architecture

IEEE 802.1X has a typical client-server model that consists of three entities: client, network access device, and authentication server, as shown in Figure 10-1 Typical IEEE 802.1X Architecture. The access control, as well as authenticating and authorizing a client device can be implemented only when all three entities participate in the IEEE 802.1X authentication.

Figure 10-1 Typical IEEE 802.1X Architecture



- Authentication client: Indicates a client device that connects to a network and initiates access authentication, such as PCs. Users need to enable the IEEE 802.1X authentication clients on their devices and enter the necessary usernames and passwords to trigger authentication. Common authentication clients include the IEEE 802.1X authentication client software embedded in Windows, macOS, and Linux operating systems.
- Access device: Indicates an IEEE 802.1X-capable network device, which can be switches in most cases. The access device provides network access for an authentication client and serves as the intermediary between the authentication client and the authentication server. The access device interworks with a client through the Extensible Authentication Protocol over LAN (EAPOL) protocol and with a server through the Remote Authentication Dial in User Service (RADIUS) protocol.
- Authentication server: Verifies the identity information (such as the username and password) sent by a client to determine whether the client has permission to access network services. The authentication server performs client authorization and accounting based on network requirements. Open-source FreeRADIUS and Lysora SMP are typically used to provide authentication services.

10.7.2 IEEE 802.1X Configuration

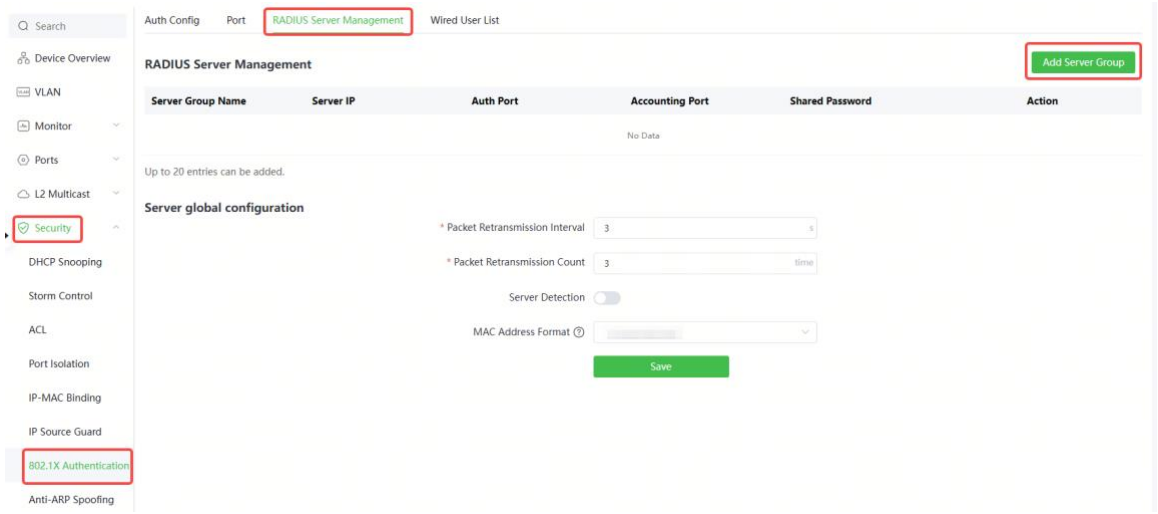
1. Adding a Server

Choose **Local Device > Security** > **802.1X Authentication** > **RADIUS Server Management**.

Before configuration, please confirm:

- The Radius server is fully built and configured as follows.
  - Add username and password for client login.
  - Close the firewall, otherwise the authentication message may be intercepted, resulting in authentication failure.
  - A trusted IP on the Radius server.
- The network connection between the authentication device and the Radius server.
- IP addresses of the Radius server and the authentication device have been obtained.

Click **Add Server Group**, configure server group parameters, and click **Save**.



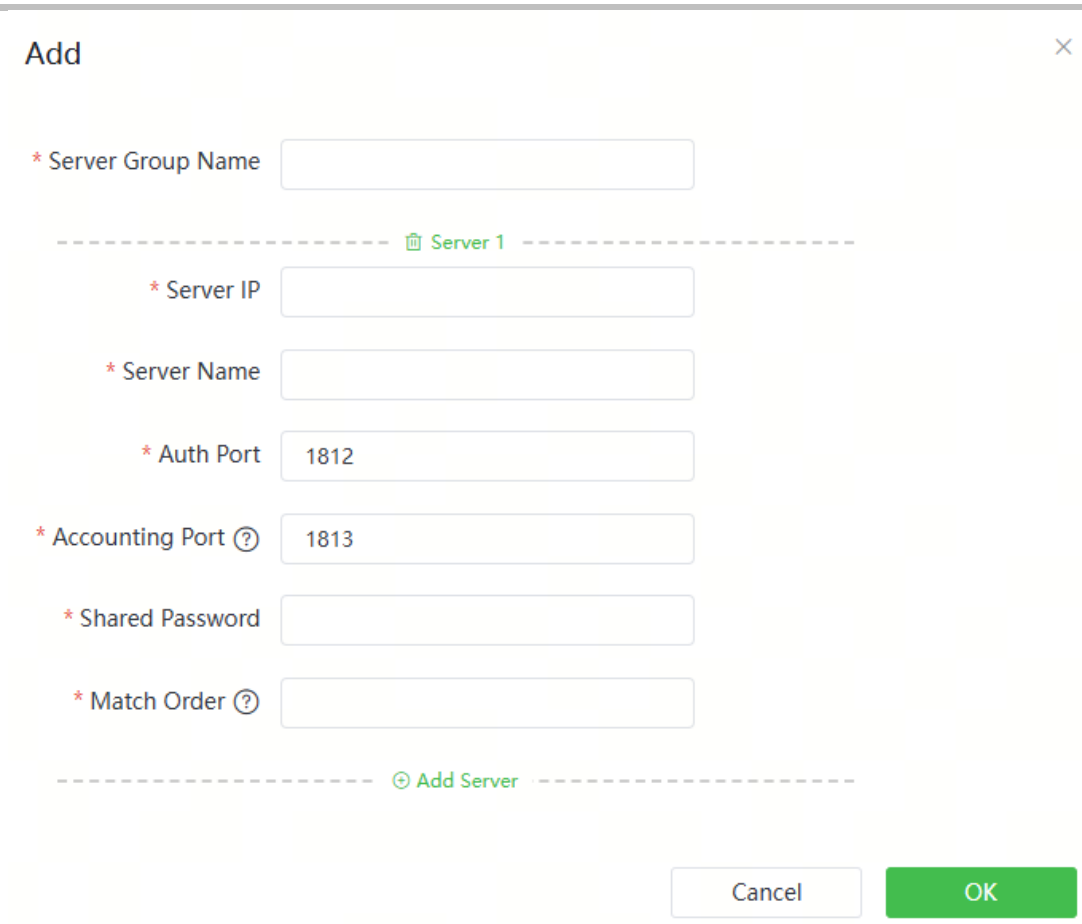


Table 10-2Parameters of Adding a Server Group

parameter	Description
Server group name	Name of a server group. You can add multiple servers to a group. If a server with a higher priority does not respond to the request of a client, other servers in the group will perform the response according to the matching sequence. **Note** To use this function, enable server detection. For details, see 10.7.2 2. Setting Up the Server.
Server IP	Radius server address.
Auth Port	The port number used for accessing user authentication on the Radius server.

parameter	Description
Accounting Port	The port number used to access the accounting process on the Radius server.
Shared Password	Radius server shared key.
Match Order	The system supports adding up to 5 Radius servers. The higher the matching order value is, the higher the priority is.

2. Setting Up the Server

Choose **Local Device > Security** > **802.1X Authentication** > **RADIUS Server Management**.

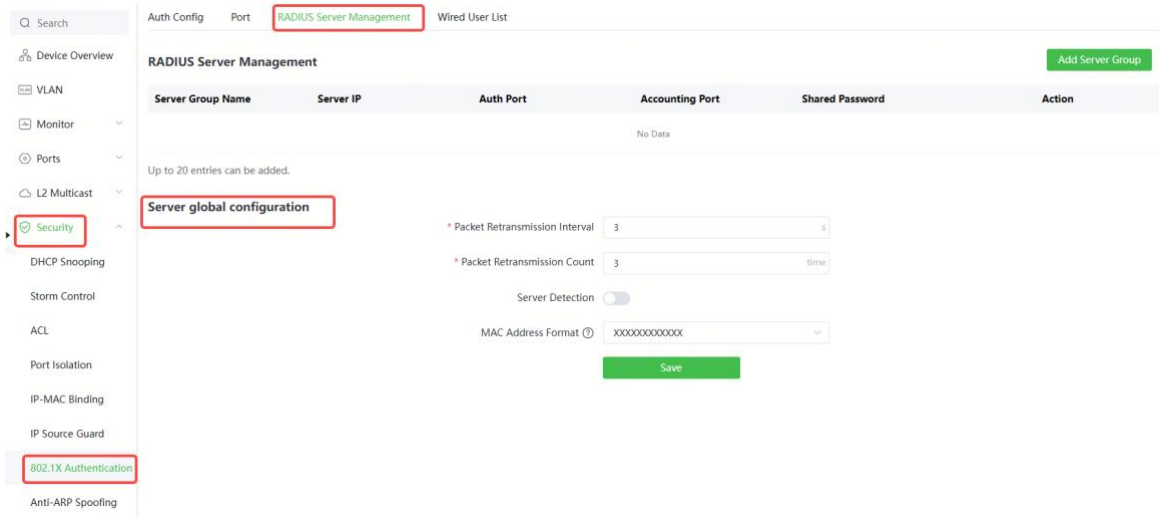


Table 10-3Description of Configuring Global Server Group Parameters

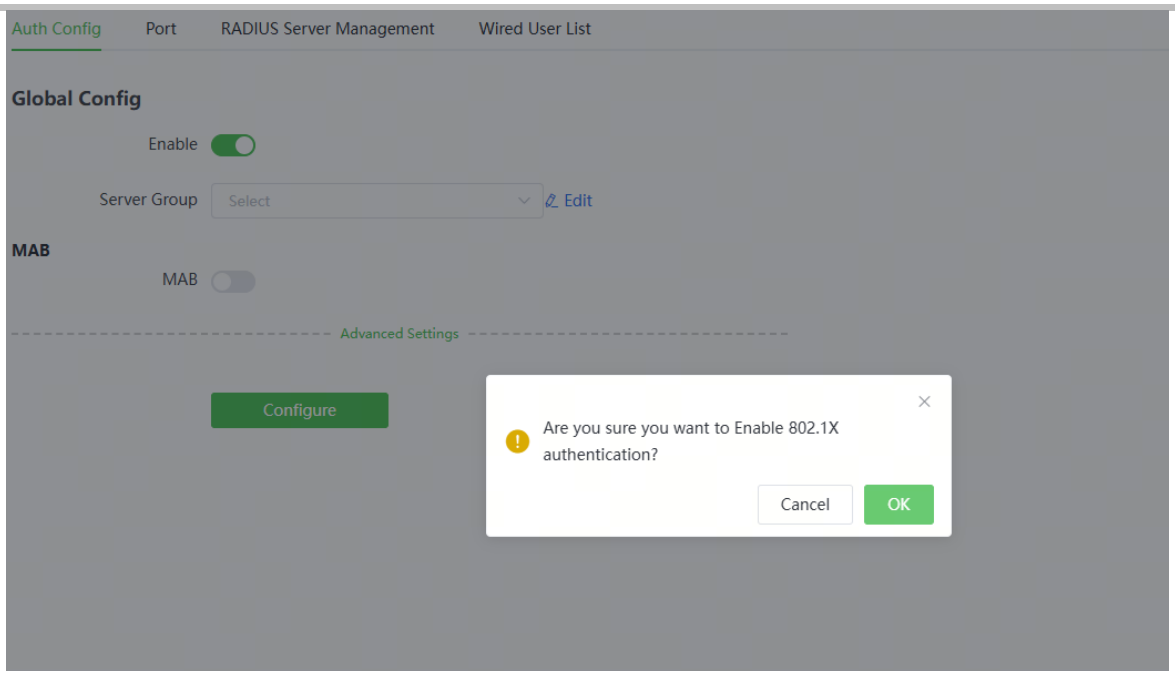
Parameter	Description
Packet Retransmission Interval	Configure the interval for the device to send request packets before confirming that there is no response from RADIUS

Parameter	Description
Packet Retransmission Count	Configure the number of times the device sends request packets before confirming that there is no response from RADIUS
Server Detection	If this function is enabled, you need to set "Server Detection Period", "Server Detection Times" and "Server Detection Username". It is used to determine the status of the server, so as to decide whether to enable functions such as escape.
MAC Address Format	Configure the MAC address format of RADIUS attribute No. 31 (Calling-Stationg-ID). The following formats are supported: ● Dotted hexadecimal format, such as 00d0.f8aa.bbcc ● IETF format, such as 00-D0-F8-AA-BB-CC ● No format (default), e.g. 00d0f8aabbcc

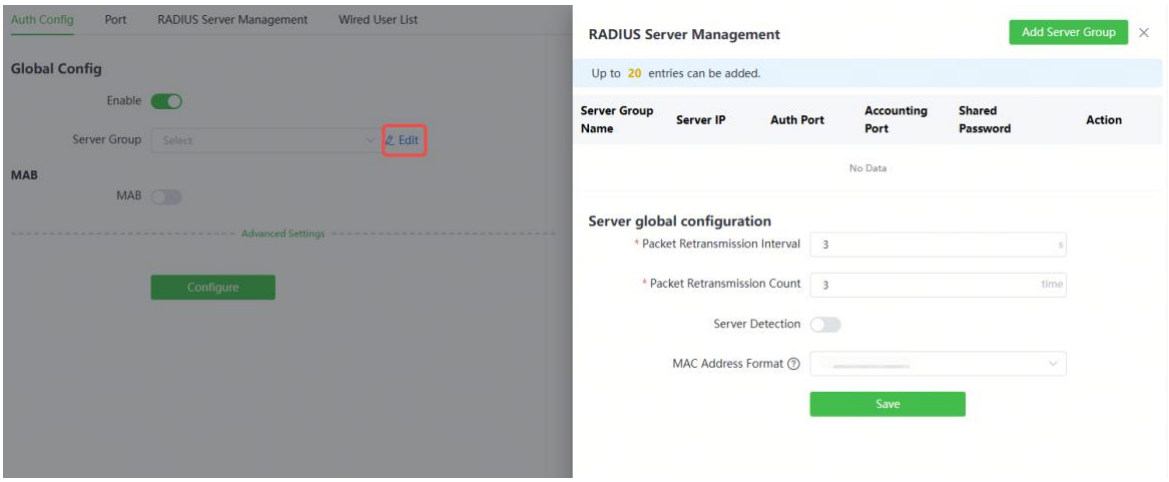
3. Enabling the IEEE 802.1X Authentication

Choose **Local Device > Security** > **802.1X Authentication** > **Auth Config**.

(1) Toggle on **Enable** under **Global Config**, and click **OK** on the displayed confirmation window.



(2) Select a server group. If no server group is created, click **Edit** to go to the **RADIUS Server Management** page and add a server group. For details, see 10.7.2 1. Adding a Server.

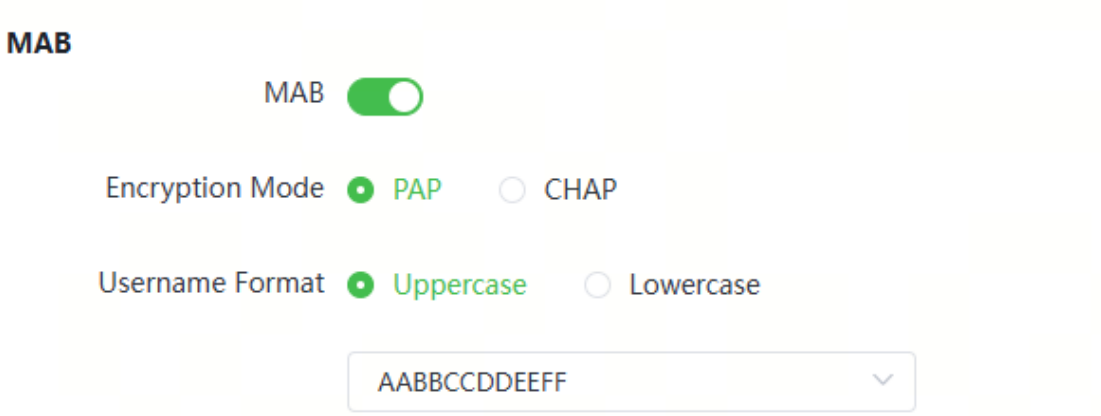


(3) Toggle on **MAB**, and set **Encryption Mode** and **Username Format**.

Note

MAB is an authentication technology for network devices and provides access control for devices, such as dumb terminals, on which 802.1X authentication cannot be performed.

- Encryption Mode: indicates the encryption mode supported by authentication servers. For MAB, **Encryption Mode** can be set to **PAP** or **CHAP**. Password Authentication Protocol (PAP) features simple but unencrypted authentication, suitable for scenarios with low security requirements. Challenge-Handshake Authentication Protocol (CHAP) offers enhanced security by preventing authentication information from being transmitted in cleartext, reducing the risk of attacks.
- Username Format: indicates the username format supported by authentication servers.



(4) Click **Advanced Settings** to configure parameters such as Guest VLAN.

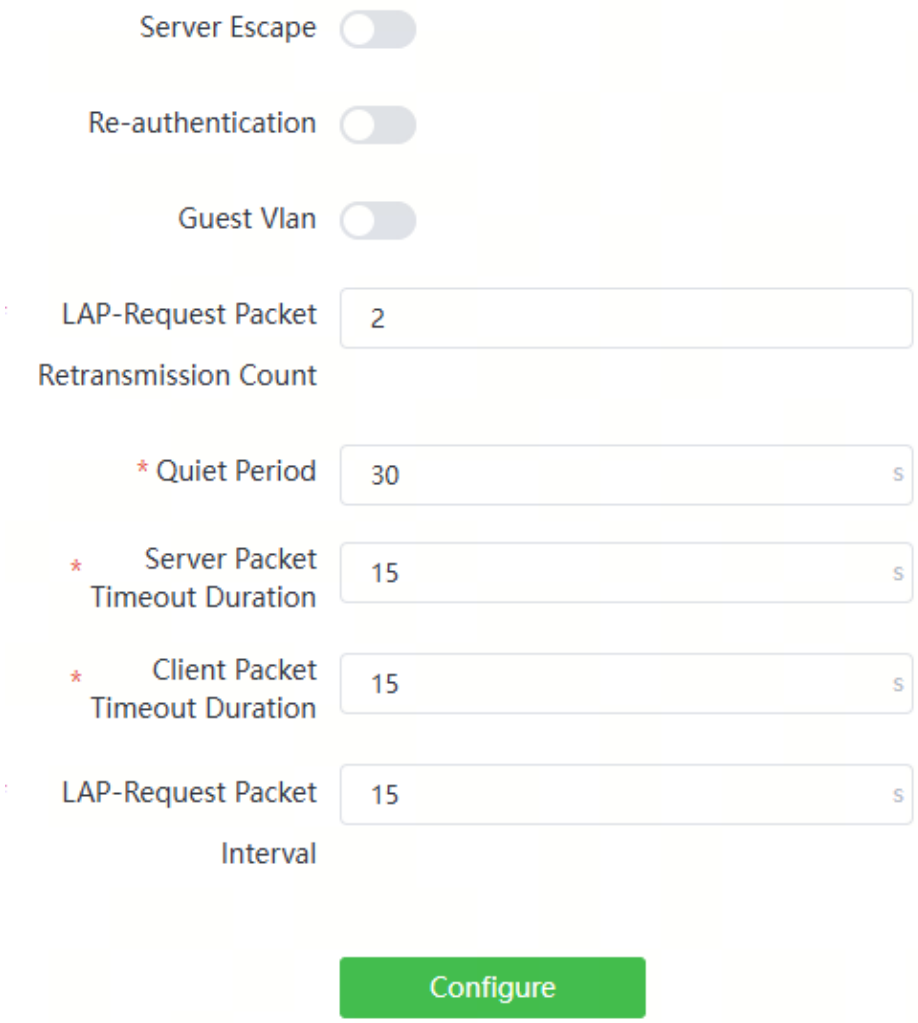


Table 10-4Description of Parameters in the Advanced IEEE 802.1X Settings

Parameter	Description
Server Escape	If the server disconnection is detected, all users will be allowed to access the Internet
Re-authentication	Require clients to re-authenticate at certain intervals to ensure network security
Guest VLAN	Provide a VLAN for unauthenticated clients to restrict their access

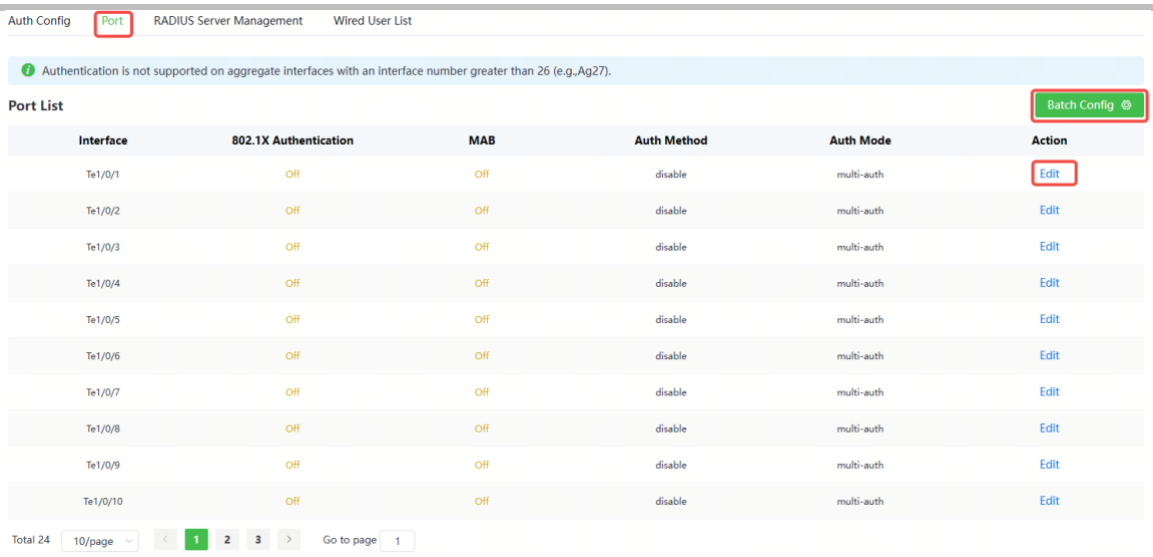
Parameter	Description
EAP-Request Packet Retransmission Count	Define the number of times the EAP request message will be retransmitted when no response is received, value range: 2- 10 times
Quiet Period	During the authentication process, the idle time between the client and the server does not exchange authentication messages, value range: 0-65535 seconds
Client Packet Timeout Duration	The time limit for the server to wait for the response from the client. Exceeding this time will be regarded as an authentication failure. Value range: 1-65535 seconds
Client Packet Timeout Duration	The time limit for the client to wait for the server to respond, exceeding this time will be considered as an authentication failure, value range: 1-65535 seconds
EAP-Request Packet Interval	Define the time interval between sending EAP request messages to control the rate of the authentication process, value range: 1-65535 seconds

(5) After configuration, click **Configure**.

4. Configuring the Effective Interface

Choose **Local Device > Security** > **802.1X Authentication** > **Port**.

Click **Edit** for an individual interface or **Batch Configure** to edit authentication parameters for interfaces.



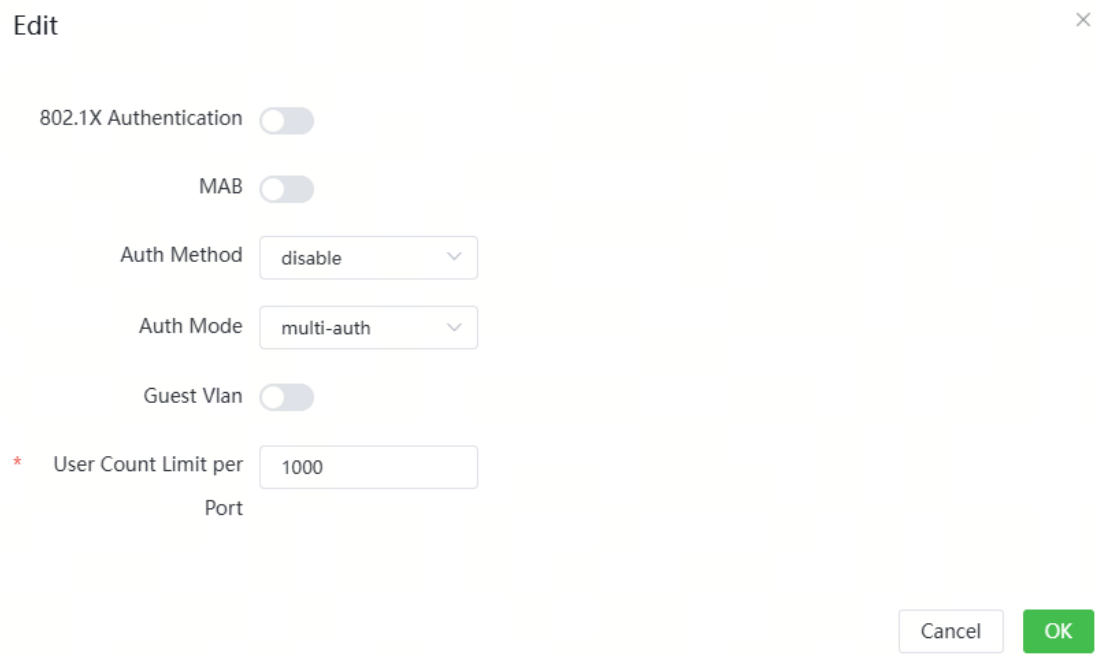


Table 10-5Description of Port Configuration Parameters

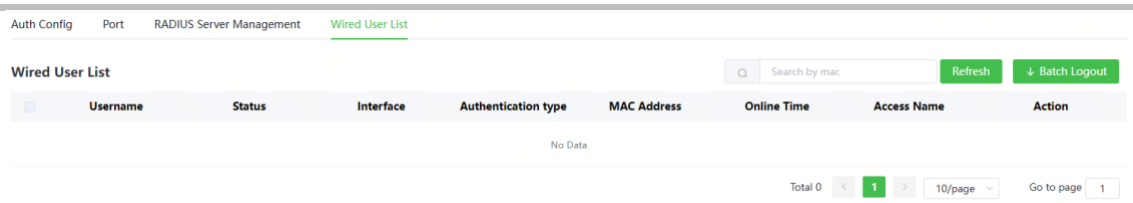
Parameter	Description
802.1X Authentication	When it is toggled on, 802.1X authentication will be enabled on the selected interface.
MAB	When it is toggled on, MAB will be enabled on the selected interface.

Parameter	Description
Auth Method	● disable: Turn off the authentication method, which has the same effect as turning off the 802.1X authentication switch ● force-auth: Mandatory authentication, the client can directly access the Internet without a password ● force-unauth: force no authentication, the client cannot authenticate and cannot access the Internet ● auto: automatic authentication, the device needs to be authenticated, and can access the Internet after passing the authentication It is recommended to select the auto authentication method.
Auth Mode	● multi-auth: Supports multiple devices using the same port for authentication, but each device needs to be authenticated independently ● multi-host: Multiple devices are allowed to share the same port. As long as one user passes the authentication, subsequent users can access the Internet ● single-host: Each port only allows one device to be authenticated, and can access the Internet after successful authentication
Guest Vlan	When enabled, devices that fail authentication will be dynamically assigned to the specified Guest VLAN **Notice** You need to create a VLAN ID first and apply it to the interface, then in Security Management > 802.1X Authentication > Advanced settings in the authentication configuration enable Guest VLAN and enter the ID
User Count Limit per Port	Limit the number of users under the interface.

10.7.3 Viewing the List of Wired Authentication Users

802.1X function is configured on the entire network and a terminal is authenticated and connected to the network, you can view the list of authenticated users.

Choose **Local Device** > **Security Management** > **802.1X Authentication** > **Wired User List** to obtain specific user information.



Click **Refresh** to get the latest user list information.

If you want to disconnect a certain user from the network, you can select the user and click **Offline** in the "Operation" column; you can also select multiple users and click **Batch Offline**.

10.8 Anti-ARP Spoofing

10.8.1 Overview

Gateway-targeted ARP spoofing prevention is used to check whether the source IP address of an ARP packet through an access port is set to the gateway IP address. If yes, the packet will be discarded to prevent hosts from receiving wrong ARP response packets. If not, the packet will not be handled. In this way, only the uplink devices can send ARP packets, and the ARP response packets sent from other clients which pass for the gateway are filtered out.

10.8.2 Procedure

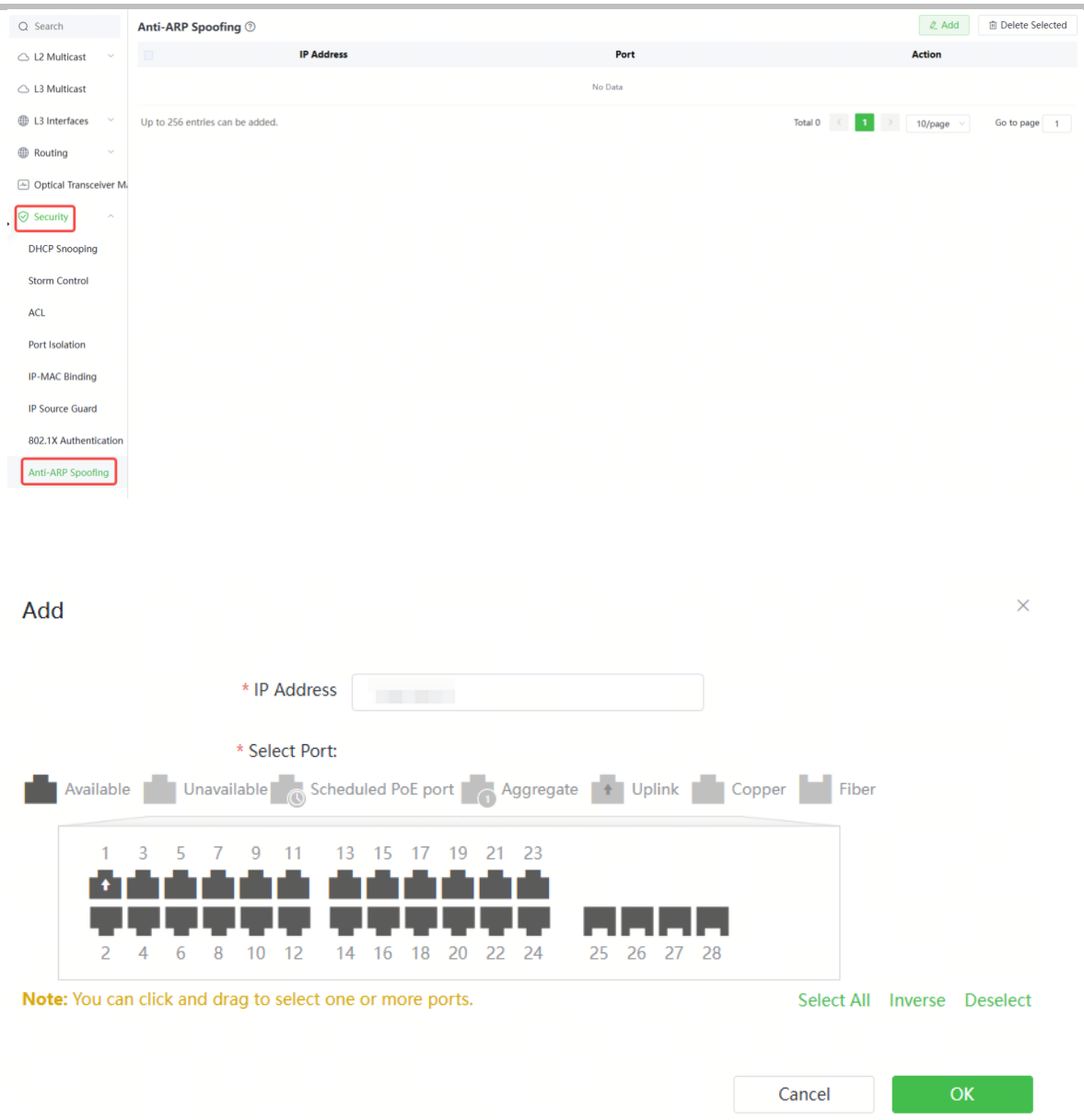
Choose **Local Device** > **Security** > **IP Source Guard** > **Anti-ARP Spoofing** .

1. Enabling Anti-ARP Spoofing

Click **Add**, select the desired port and enter the gateway IP, click **OK**.

Note

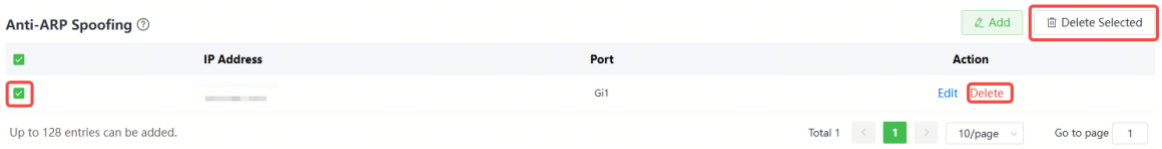
Generally, the anti-ARP spoofing function is enabled on the downlink ports of the device.



2. Disabling Anti-ARP Spoofing

Batch disable: Select an entry to be deleted in the list and click **Delete Selected**.

Disable one port: click **Delete** in the last **Action** column of the corresponding entry.



11 Advanced Configuration

11.1 STP

The switches support the following spanning tree modes:

- Spanning Tree Protocol (STP) is a Layer 2 management protocol that eliminates Layer 2 loops by selectively blocking redundant links over the network and provides the link backup function.
- Building on STP, Rapid Spanning Tree Protocol (RSTP) achieves fast convergence of network topology. However, like STP, MSTP also has the defect that all VLANs share one spanning tree and load sharing cannot be achieved.
- Multiple Spanning Tree Protocol (MSTP) can overcome the previous defect. It can achieve fast convergence and forward traffic of different VLANs along their respective paths, thereby providing a better load balancing mechanism for redundant links.

11.1.1 Global STP Settings

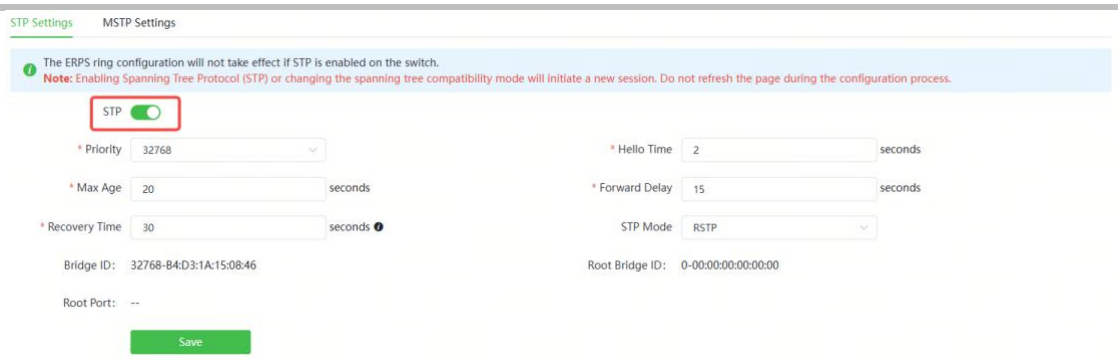
Choose **Local Device** > **Advanced** > **STP** > **STP Settings**.

1. Global STP Configurations

(1) Click to enable the STP function, and click OK in the displayed box. The STP function is disabled by default.

Caution

- After enabling the STP configuration of the device, the ERPS configuration cannot take effect normally.
- Enabling the STP or changing the STP mode will initiate a new session. Do not refresh the page during the configuration.



(2) Configure the STP global parameters, and click **Save**.

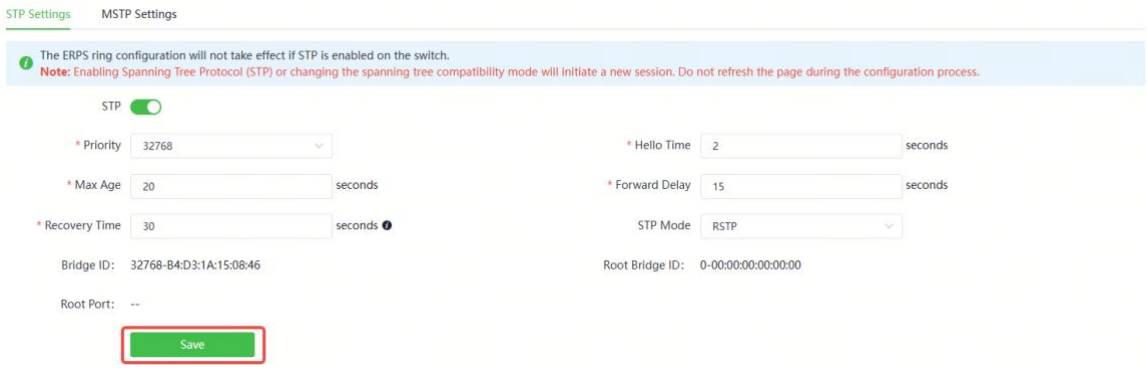


Table 11-1Description of STP Global Configuration Parameters

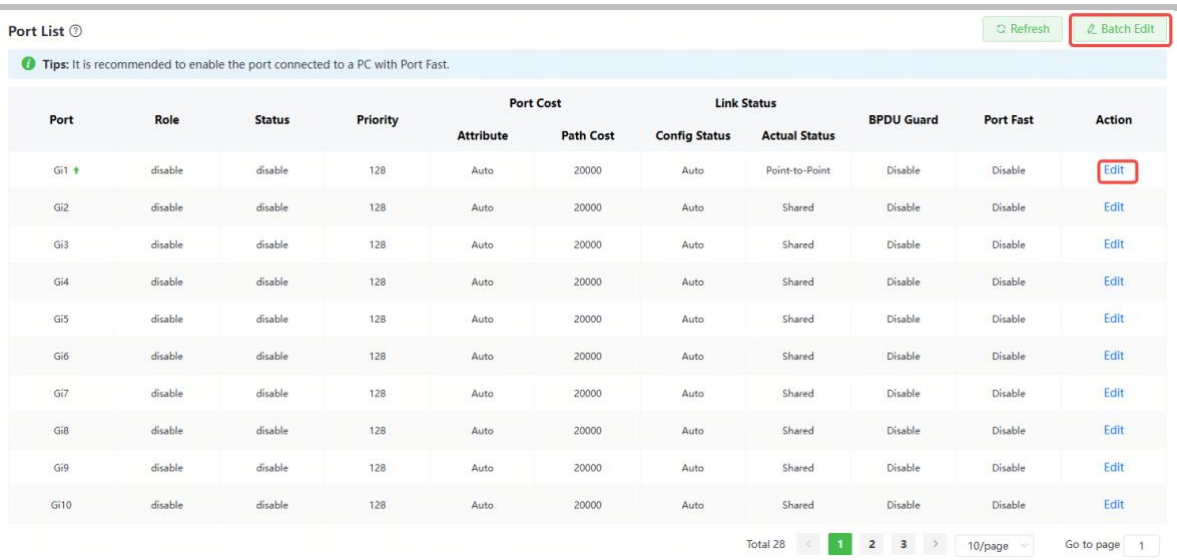
Parameter	Description	Default Value
STP	Whether to enable the STP function. It takes effect globally. STP attributes can be configured only after STP is enabled.	Disable
Priority	Bridge priority. The device compares the bridge priority first during root bridge selection. A smaller value indicates a higher priority.	32768
Hello Time	Interval for sending two adjacent BPDUs	2 seconds
Max Age	The maximum expiration time of BPDUs The packets expiring will be discarded. If a non-root bridge fails to receive a BPDU from the root bridge before the aging time	20 seconds

Parameter	Description	Default Value
	expires, the root bridge or the link to the root bridge is deemed as faulty	
Forward Delay	The interval at which the port status changes, that is, the interval for the port to change from Listening to Learning, or from Learning to Forwarding.	15 seconds
Recovery Time	Network recovery time when redundant links occur on the network.	30 seconds
STP Mode	The versions of Spanning Tree Protocol. Currently the device supports STP (Spanning Tree Protocol), RSTP (Rapid Spanning Tree Protocol) and MSTP (Multiple Spanning Tree Protocol).	RSTP
Bridge ID	STP identifies a switch by a bridge ID, which consists of the bridge priority and bridge MAC address.	NA
Root Bridge ID	As the root node of an STP tree, the root bridge is identified by the root bridge ID and functions as the logical center of the entire Layer 2 network.	NA
Root Port	A root port exists on a non-root bridge and has the smallest path cost to the root bridge. Each non-root bridge has only one root port.	NA

2. Applying STP to a Port

Choose **Local Device** > **Advanced** >**STP** > **STP Settings > Port List**.

Configure the STP properties for a port Click **Batch Edit** to select ports and configure STP parameters, or click **Edit** in the **Action** column in **Port List** to configure designated ports.



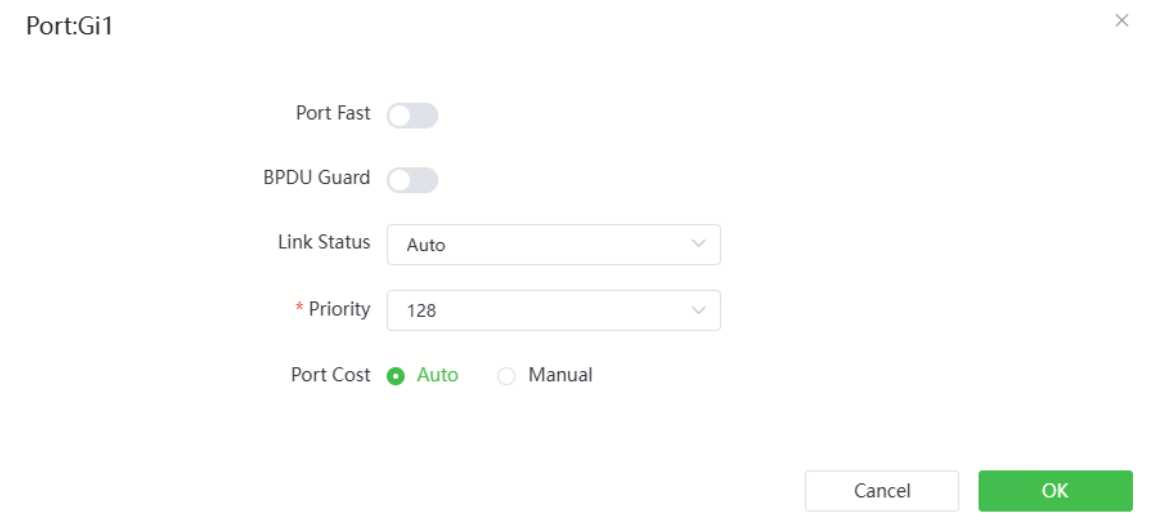


Table 11-2Description of STP Configuration Parameters of Ports

Parameter	Description	Default Value
Role	● Root: A port with the shortest path to the root ● Alternate: A backup port of a root port. Once the root port fails, the alternate port becomes the root port immediately.	NA

Parameter	Description	Default Value
	● Designated (designated ports): A port that connects a root bridge or an upstream bridge to a downstream device. ● Disable (blocked ports): Ports that have no effect in the spanning tree.	
Status	● Disable: The port is closed manually or due to a fault, does not participate in spanning tree and does not forward data, and can be turned into a blocking state after initialization or opening. ● Blocking: A port in the blocking state cannot forward data packets or learn addresses, but can send or receive configuration BPDUs and send them to the CPU. ● Listening: If a port can become the root port or designated port, the port will enter the listening state. **Listening**: A port in the listening state does not forward data or learn addresses, but can receive and send configuration BPDUs. ● Learning: A port in the learning state cannot forward data, but starts to learn addresses, and can receive, process, and send configuration BPDUs. ● Forwarding: Once a port enters the state, it can forward any data, learn addresses, and receive, process, and send configuration BPDUs.	NA
Priority	The priority of the port is used to elect the port role, and the port with high priority is preferentially selected to enter the forwarding state	128
Port Cost	It can be set to **Auto** or **Manual**:	Auto

Parameter	Description	Default Value
Attribute	● **Auto**: The port cost is automatically calculated based on the port rate. ● **Manual**: The configured value is used as the port cost.	
Port Cost Path Cost	Actual path cost.	NA
Link Status Config Status	Configure the link type, the options include: Shared, Point-to-Point and Auto. In auto mode, the interface type is determined based on the duplex mode. For full-duplex ports, the interface type is point-to-point, and for half-duplex ports, the interface type is shared.	Auto
Link Status Actual Status	Actual link type: Shared, Point-to-Point	NA
BPDU Guard	Whether to enable the BPDU guard function. After the function is enabled, if Port Fast is enabled on a port or the port is automatically identified as an edge port connected to an endpoint, but the port receives BPDUs, the port will be disabled and enters the Error-disabled state. This indicates that an unauthorized user may add a network device to the network, resulting in network topology change.	Disable
Port Fast	Whether to enable the Port Fast function. After Port Fast is enabled on a port, the port will neither receive nor send BPDUs. In this case, the host directly connected to the port cannot receive BPDU.s. If a port, on which Port Fast is enabled exits the Port Fast state automatically when it receives BPDUs, the BPDU filter feature is automatically disabled. Generally, the port connected to a PC is enabled with Port Fast.	Disable

Note

- It is recommended to enable Port Fast on the port connected to a PC.
- A port switches to the forwarding state after STP is enabled more than 30 seconds. Therefore transient disconnection may occur and packets cannot be forwarded.

11.1.2 MSTP Settings

Choose **Local Device** > **Advanced** > **STP** > **MSTP Settings**.

1. MSTP Global Configurations

The MSTP configuration takes effect only when **STP Mode** in STP global configurations is set to **MSTP**.

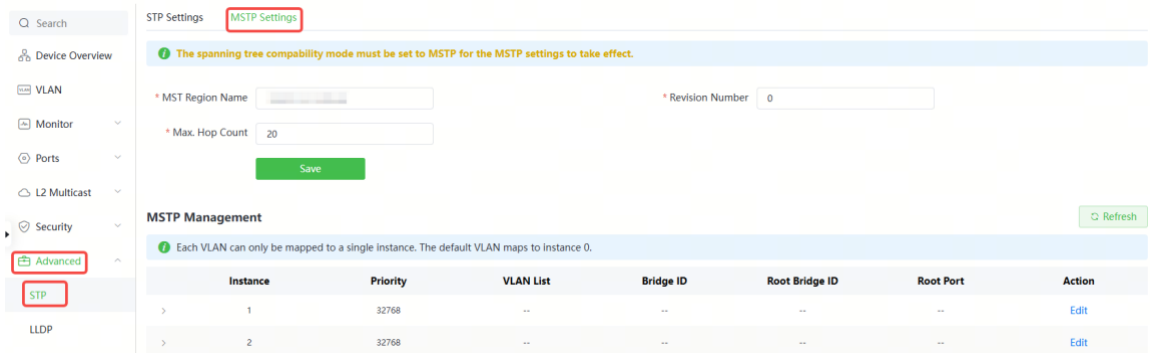


Table 11-3Description of Parameters in MSTP Global Configurations

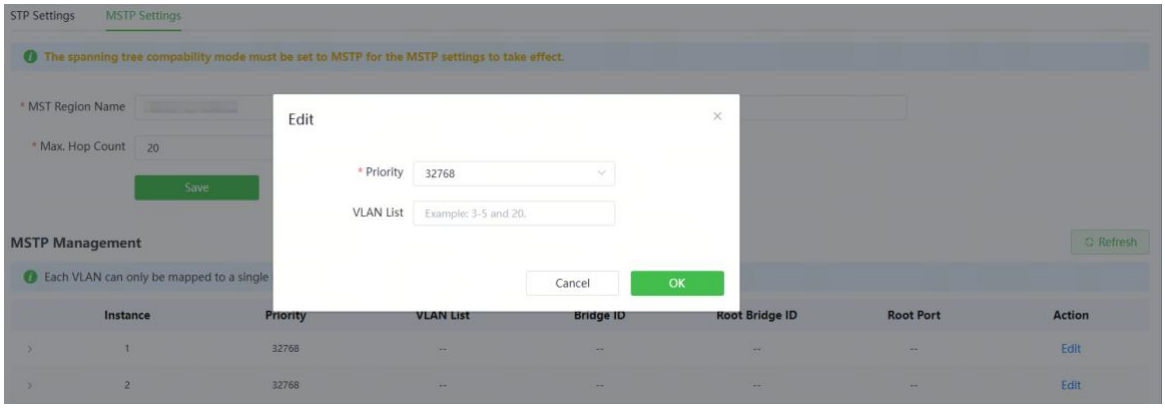
Parameter	Description	Default Value
MST Region Name	Name of an MST region. The name is an identifier, ranging from 1 to 32 characters, and distinguishes different MST regions.	NA
Revision Number	Revision level of an MST region, which is used to distinguish different MST regions.	0
Max. Hop Count	Maximum hops of BPDU packets in an MST region. It also refers to the maximum hops from the root bridge to other bridges or terminal devices.	20

2. Applying MSTP

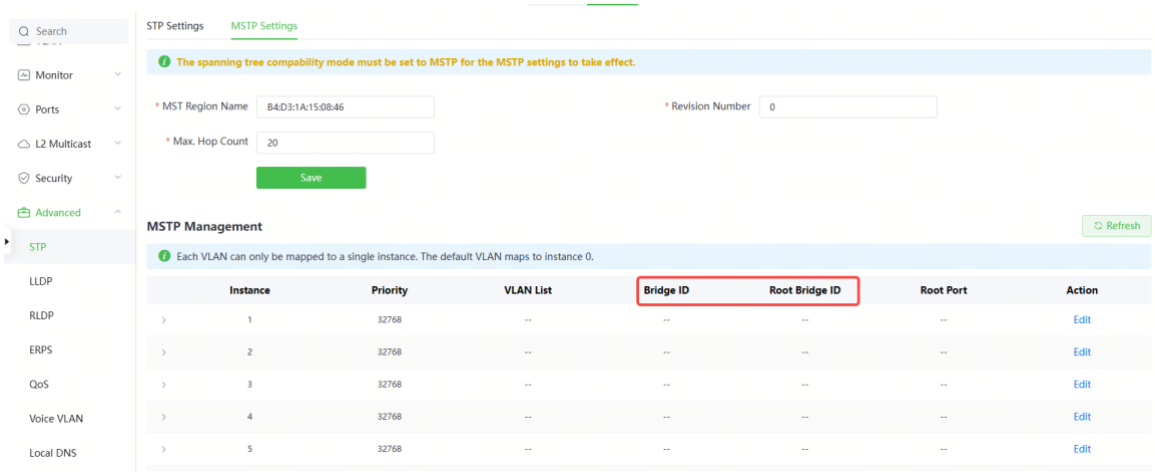
Click **Edit** in the **Action** column of a specified instance, set **Priority** and **VLAN List**, and click **OK**.

Note

If you want to add multiple VLAN IDs, separate them with commas (,). If you attempt to add consecutive VLANs, separate them with a hyphen (-), for example, 14-15.



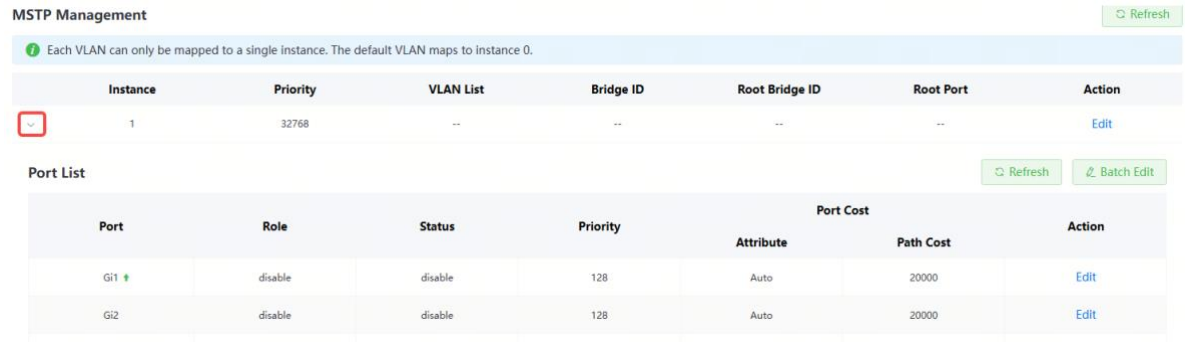
The bridge ID, root bridge ID, and root port number of the instance can be displayed in the list only after the VLAN ID is added.



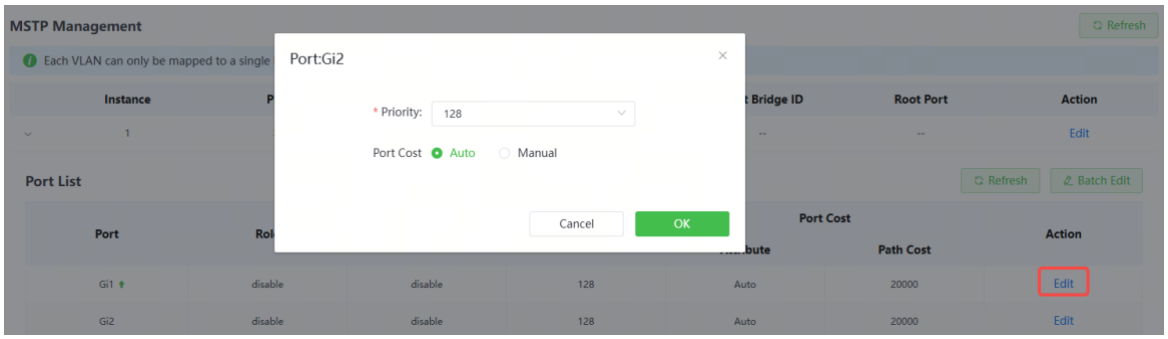
Note

If a device acts as the root bridge, it has no root port, and no port number is displayed in the **Root Port** column.

Click the drop-down button before an instance to display the corresponding port configuration.



Click **Edit** in the **Action** column to modify the port priority and cost.



11.2 LLDP

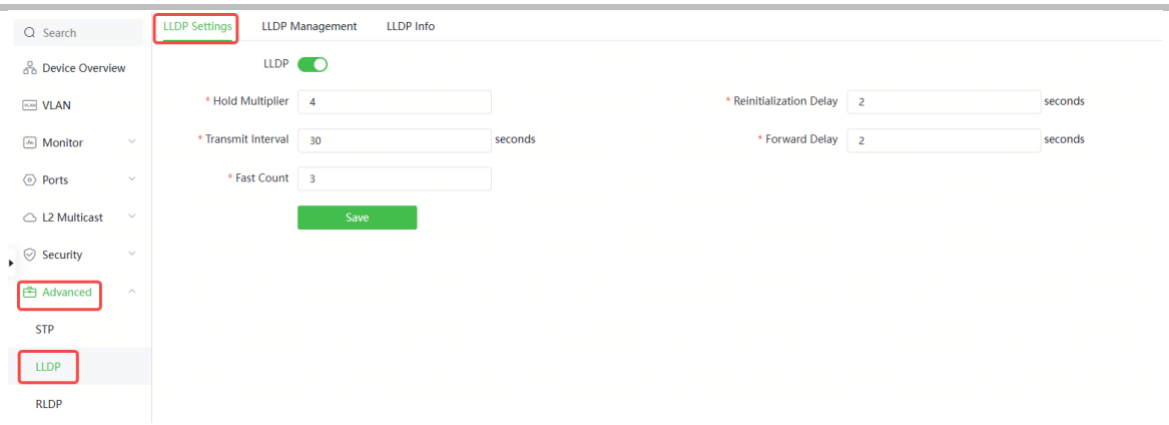
11.2.1 Overview

LLDP (Link Layer Discovery Protocol) is defined by IEEE 802.1AB. LLDP can discover devices and detect topology changes. With LLDP, the web page can learn the topological connection status, for example, ports of the device that are connected to other devices, port rates at both ends of a link, and duplex mode matching status. An administrator can locate and troubleshoot faults quickly based on the preceding information.

11.2.2 LLDP Global Settings

Choose **Local Device** > **Advanced** >**LLDP** > **LLDP Settings**.

(1) Click to enable the LLDP function, and click **OK** in the displayed box. The STP function is enabled by default. When the LLDP is enabled, this step can be skipped.



(2) Configure the global LLDP parameters and click **Save**.

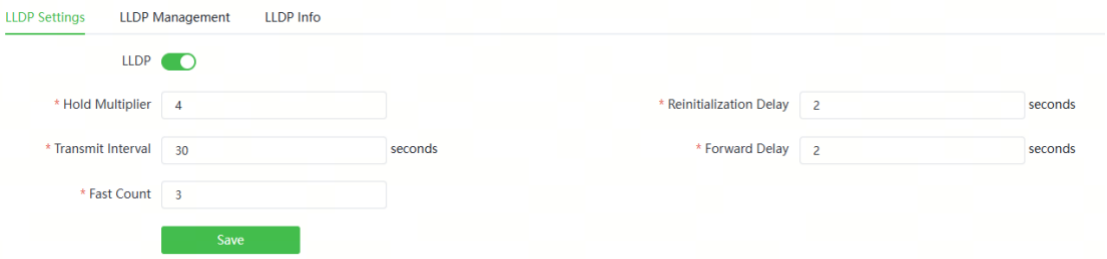


Table 11-4Description of LLDP Global Configuration Parameters

Parameter	Description	Default Value
LLDP	Indicates whether the LLDP function is enabled.	Enable
Hold Multiplier	TTL multiplier of LLDP In LLDP packets, TTL TLV indicates the TTL of local information on a neighbor. The value of TTL TLV is calculated using the following formula: TTL TLV = TTL multiplier × Packet transmission interval + 1. The TTL TLV value can be modified by configuring the TTL multiplier and LLDP packet transmission interval.	4
Transmit Interval	Transmission interval of LLDP packets, in seconds The value of TTL TLV is calculated using the following formula: TTL TLV = TTL multiplier ×	30 seconds

Parameter	Description	Default Value
	Packet transmission interval + 1. The TTL TLV value can be modified by configuring the TTL multiplier and LLDP packet transmission interval.	
Fast Count	Number of packets that are transmitted rapidly When a new neighbor is discovered, or the LLDP working mode is changed, the device will start the fast transmission mechanism in order to let the neighboring devices learn the information of the device as soon as possible. The fast transmission mechanism shortens the LLDP packet transmission interval to 1s, sends a certain number of LLDP packets continuously, and then restores the normal transmission interval. You can configure the number of LLDP packets that can be transmitted rapidly for the fast transmission mechanism.	3
Reinitialization Delay	Port initialization delay, in seconds You can configure an initialization delay to prevent frequent initialization of the state machine caused by frequent changes of the port work mode.	2 seconds
Forward Delay	Delay for sending LLDP packets, in seconds. When local information of a device changes, the device immediately transmits LLDP packets to its neighbors. You can configure a transmission delay to prevent frequent transmission of LLDP packets caused by frequent changes of local information. If the delay is set to a very small value, frequent change of the local information will cause frequent transmission of LLDP packets. If the delay is set to a very large value, no LLDP packet may be transmitted even if local information is changed.	2 seconds

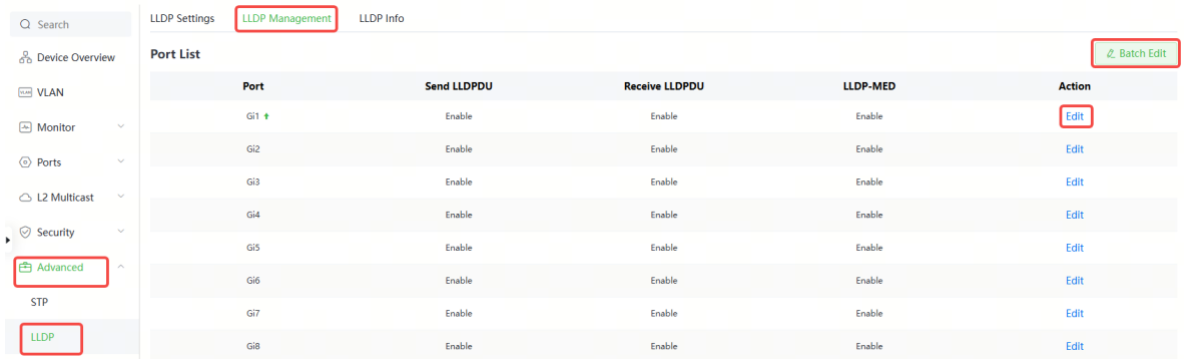
Parameter	Description	Default Value
	Set an appropriate delay according to actual conditions.	

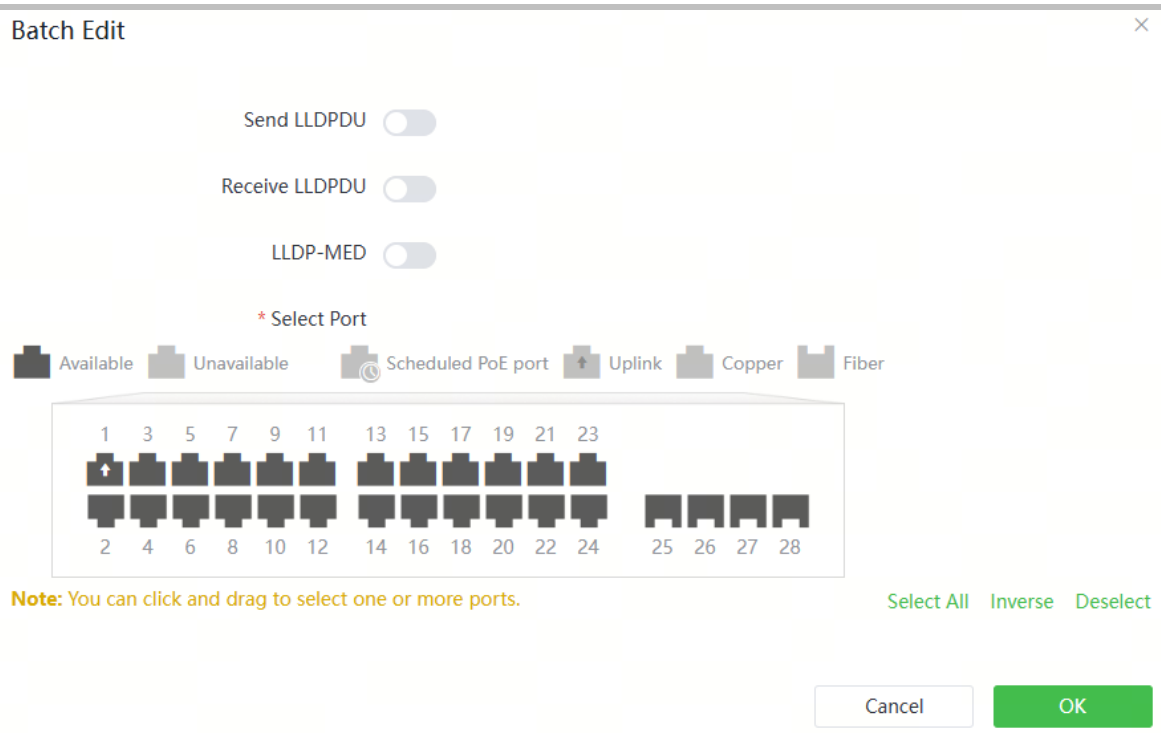
11.2.3 Applying LLDP to a Port

Choose **Local Device** > **Advanced** > **LLDP** > **LLDP Management**.

In **Port List**, Click **Edit** in the **Action** column, or click **Batch Edit**, select the desired port, configure the LLDP working mode on the port and whether to enable LLDP-MED, and click **OK**.

- **Send LLDPDU**: After **Send LLDPDU** is enabled on a port, the port can send LLDPDUs.
- **Receive LLDPDU**: After **Receive LLDPDU** is enabled on a port, the port can receive LLDPDUs.
- **LLDPMED**: After **LLDPMED** is enabled, the device is capable of discovering neighbors when its peer endpoint supports LLDP-MED (the Link Layer Discovery Protocol-Media Endpoint Discovery).



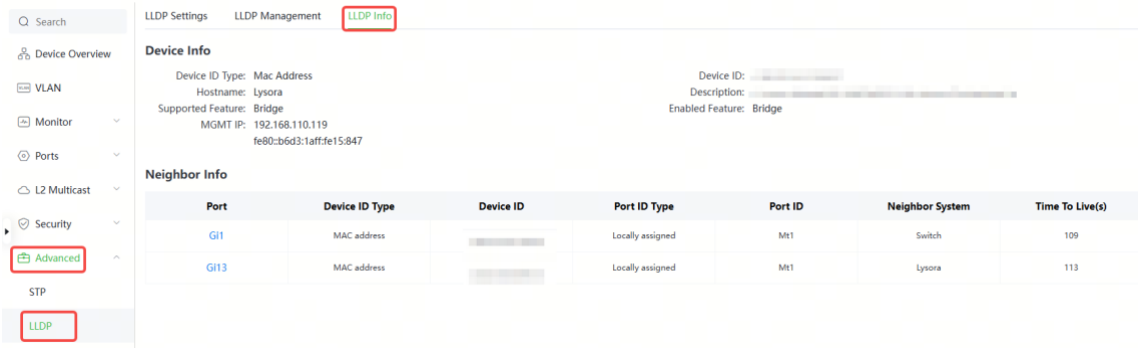


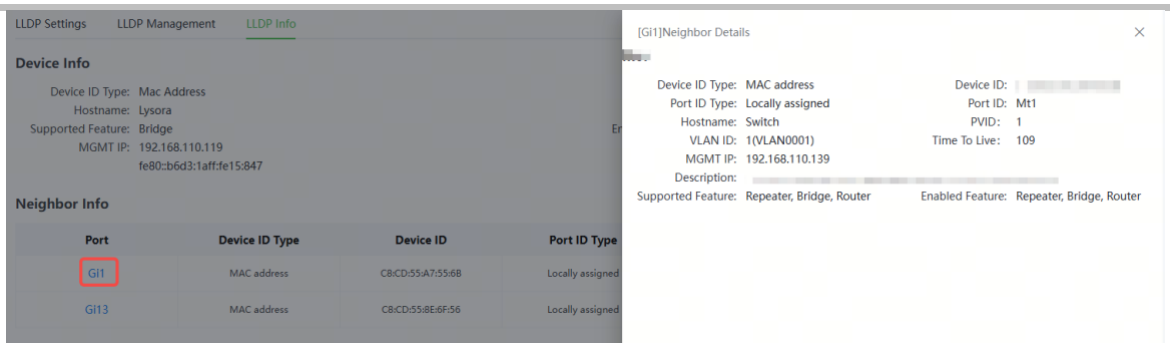
11.2.4 Displaying LLDP Information

Choose **Local Device** > **Advanced** > **LLDP** > **LLDP Info**.

To display LLDP information, including the LLDP information of the local device and the neighbor devices of each port. Click the port name to display details about port neighbors.

You can check the topology connection through LLDP information, or use LLDP to detect errors. For example, if two switch devices are directly connected in the network topology. When an administrator configures the VLAN, port rate, duplex mode, an error will be prompted if the configurations do not match those on the connected neighbor.





11.3 RLDP

11.3.1 Overview

The Rapid Link Detection Protocol (RLDP) is an Ethernet link failure detection protocol, which is used to rapidly detect unidirectional link failures, bidirectional link failures, and downlink loop failures. When a failure is found, RLDP automatically shuts down relevant ports or asks users to manually shut down the ports according to the configured failure handling methods, to avoid wrong forwarding of traffic or Ethernet Layer 2 loops.

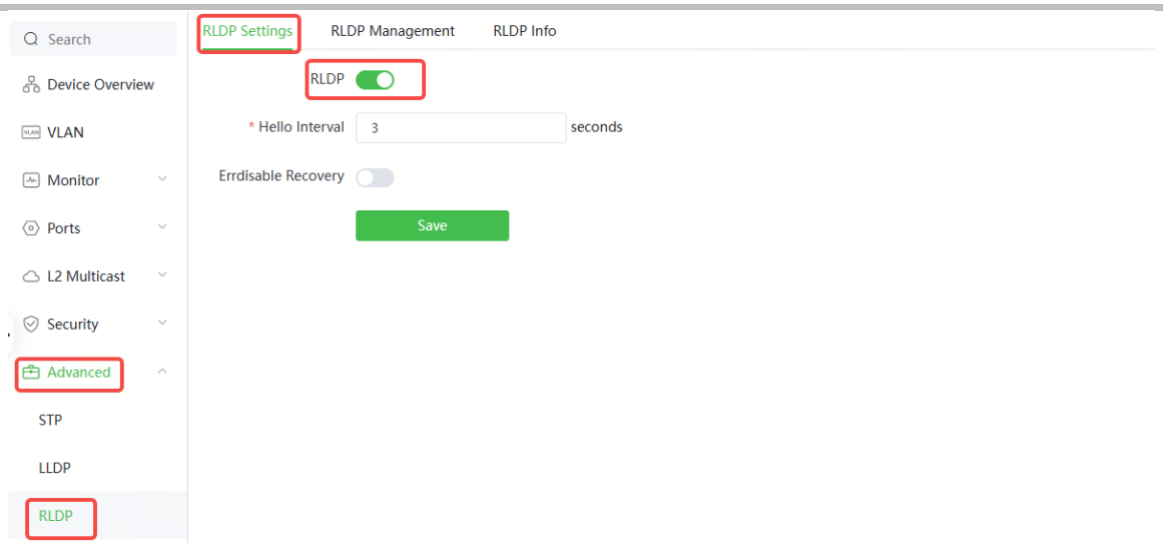
Supports enabling the RLDP function of the access switches in the network in a batch. By default, the switch ports will be automatically shut down when a loop occurs. You can also set a single switch to configure whether loop detection is enabled on each port and the handling methods after a link fault is detected

11.3.2 Standalone Device Configuration

1. RLDP Global Settings

Choose **Local Device** > **Advanced** > **RLDP** > **RLDP Settings**.

(1) Enable the RLDP function and click **OK** in the displayed dialog box. The RLDP function is disabled by default.



(2) Configure RLDP global parameters and click **Save**.

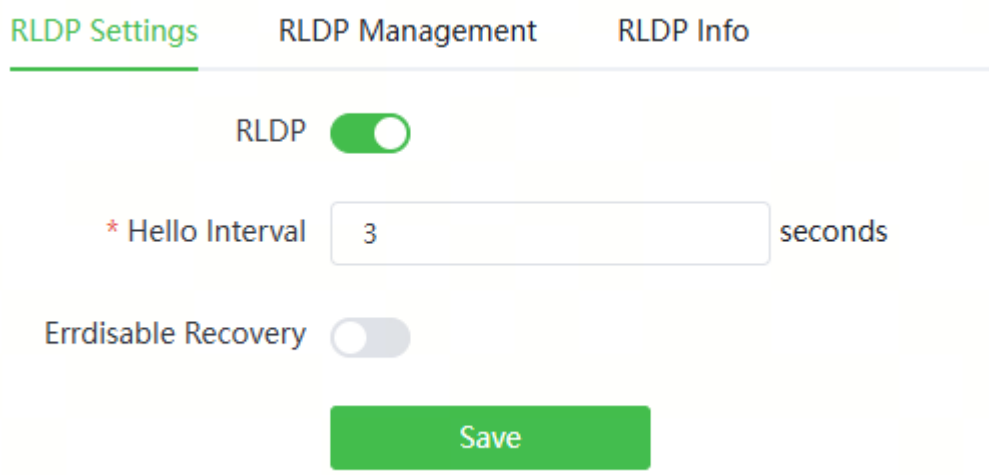


Table 11-5Description of RLDP Global Configuration Parameters

Parameter	Description	Default Value
RLDP	Indicates whether the RLDP function is enabled.	Disable
Hello Interval	Interval for RLDP to send detection packets, in seconds	3 seconds

Parameter	Description	Default Value
Errdisable Recovery	After it is enabled, a port automatically recovers to the initialized state after a loop occurs.	Disable
Errdisable Recovery Interval	The interval at which the failed ports recover to the initialized state regularly and link detection is restarted, in seconds.	30 seconds

2. Applying RLDP to a Port

Choose **Local Device** > **Advanced** > **RLDP** > **RLDP Management**.

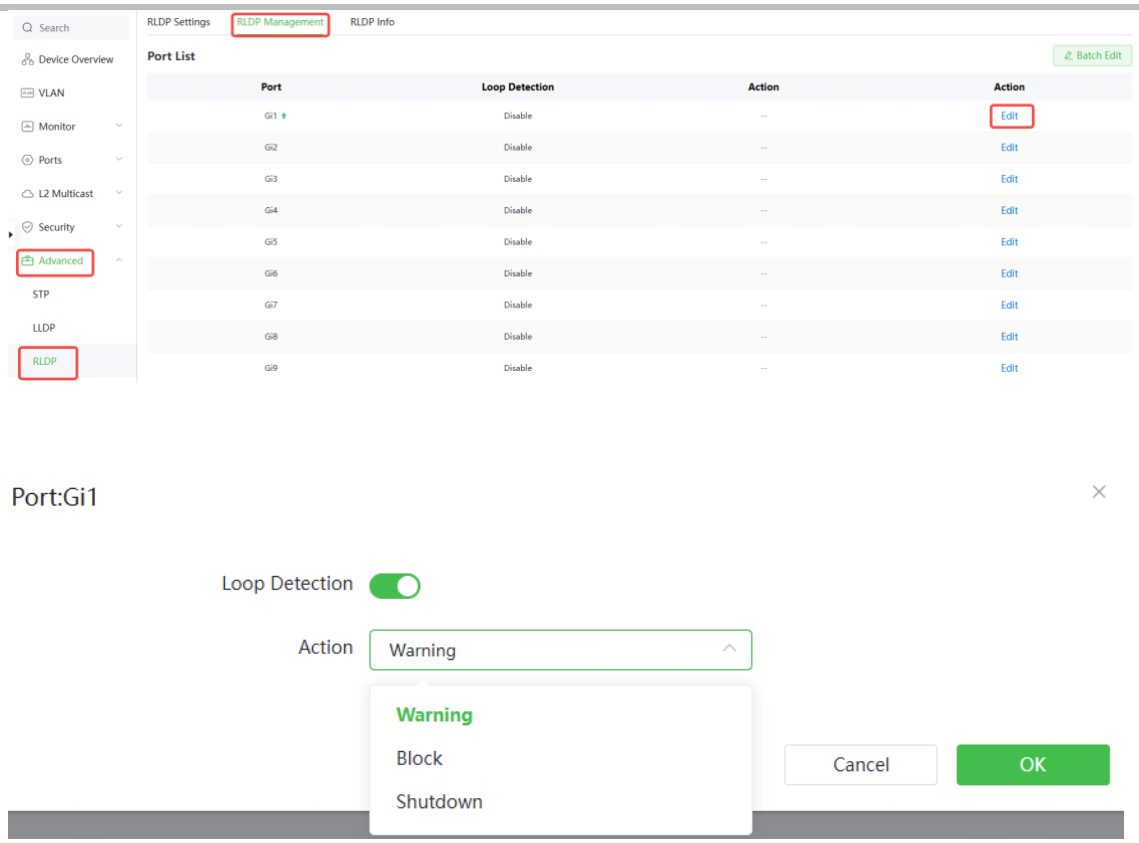
In **Port List,** click **Edit** in the Action column or click **Batch Edit**, select the desired port, configure whether to enable loop detection on the port and the handling method after a fault is detected, and click **OK**.

There are three methods to handle port failures:

- Warning: Only the relevant information is prompted to indicate the failed port and the failure type.
- Block: After alerting the fault, set the faulty port not to forward the received packets
- Shutdown port: After alerting the fault, shutdown the port.

⚠ Caution

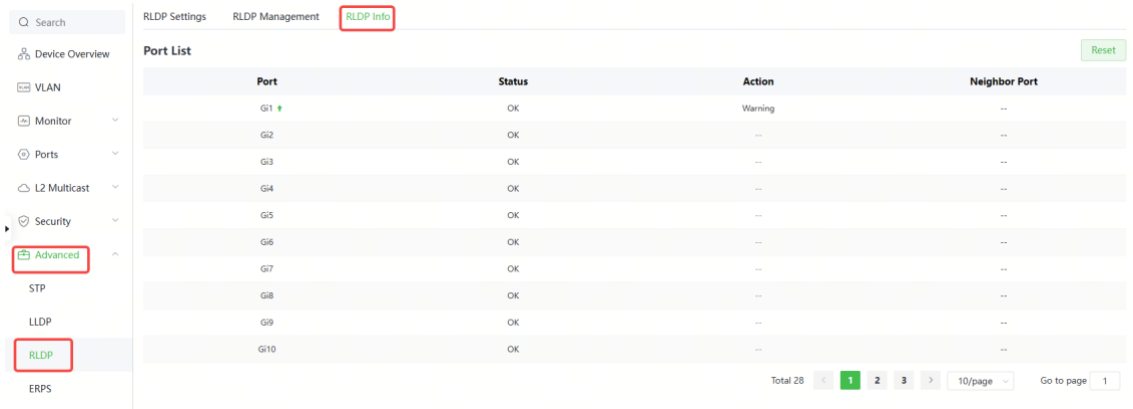
- When RLDP is applied to an aggregate interface, the **Action** can only be set to **Warning** and **Shutdown**.
- When performing RLDP detection on an aggregate interface, if detection packets are received on the same device, even if the VLANs of the port sending the packets and the port receiving them are different, it will not be judged as a loop failure.



3. Displaying RLDP Information

Choose **Local Device** > **Advanced** > **RLDP** > **RLDP Info**.

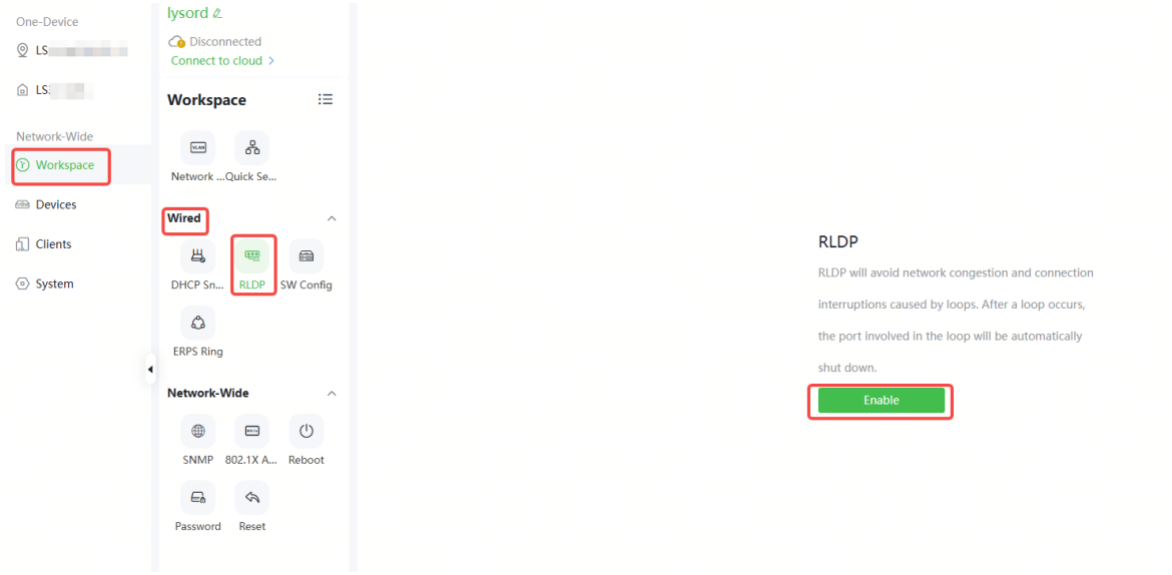
You can view the detection status, failure handling methods, and ports that connect the neighbor device to the local device. You can click **Reset** to restore the faulty RLDP status triggered by a port to the normal state.



11.3.3 Configuring Network Switches in Batches

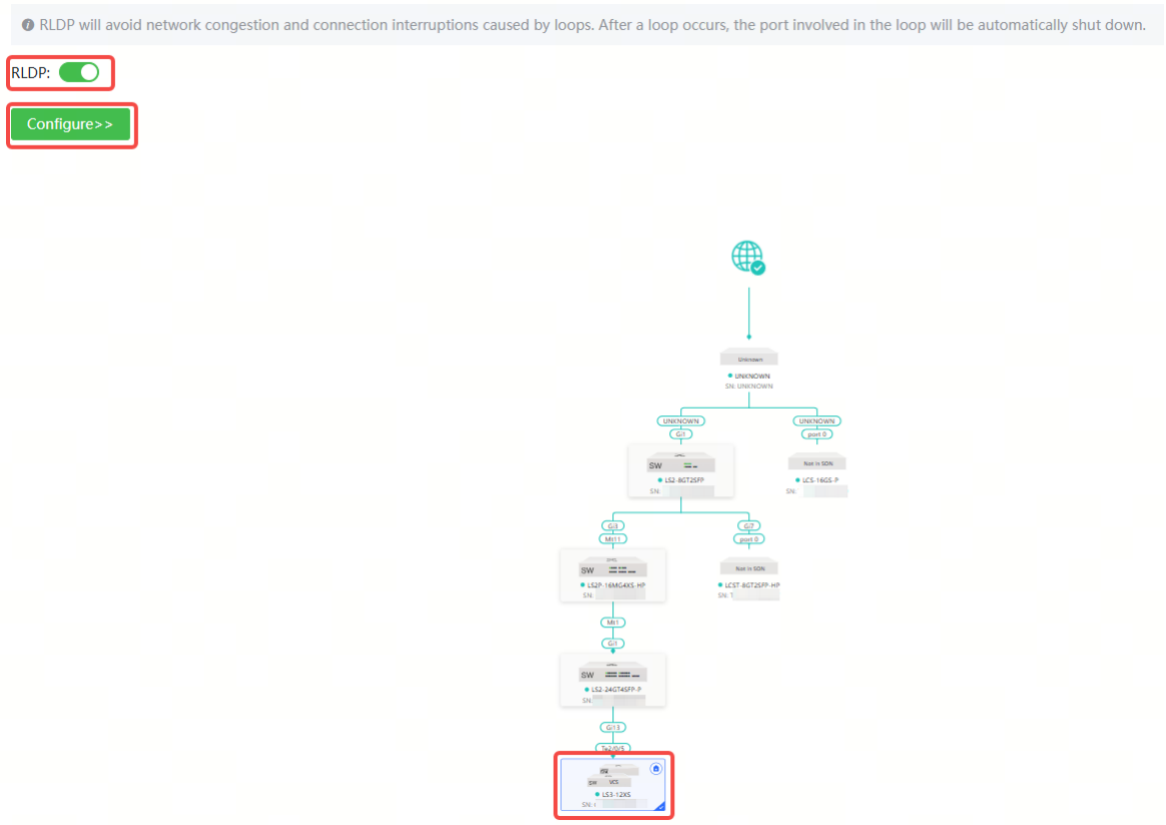
Choose **Network-Wide > Workspace > Wired > RLDP**.

(1) Click **Enable** to access the **RLDP Config** page.



(2) In the networking topology, you can select the access switches on which you want to enable RLDP in either recommended or custom mode. If you select the recommended mode, all access switches in the network are selected automatically. If you select the custom mode, you can manually select the desired access switches. Click **Deliver Config**. RLDP is enabled on the selected switches.

(3) After the configuration is delivered, if you want to modify the effective range of the RLDP function, click **Configure** to select desired switches in the topology again. Turn off **RLDP** to disable RLDP on all the switches with one click.



11.4 ERPS

Specification

VCS and ERPS are mutually exclusive and cannot be configured simultaneously.

11.4.1 Overview

Ethernet Ring Protection Switching (ERPS), also known as G.8032, is a ring protection protocol developed by the International Telecommunication Union (ITU). It is a data link layer protocol specially designed for Ethernet rings. ERPS prevents broadcast storms caused by data loops when an Ethernet ring network is intact, and can rapidly perform link switching and recover the communication between nodes when a link is disconnected in the Ethernet ring, so as to implement data link redundancy.

Currently, the Spanning Tree Protocol (STP) is another solution to the Layer 2 network loop problem. STP is at mature application stage but requires a relatively long (within seconds) convergence time. Compared with STP, ERPS provides faster convergence, with the Layer 2 convergence time less than 50 ms.

11.4.2 Control VLAN and Data VLAN

ERPS supports two types of virtual local area networks (VLANs): control VLANs and data VLANs.

- Control VLAN: Also known as the Ring Auto Protection Switching VLAN (R-APS VLAN) for transmitting ERPS protocol packets. On a device, the ports connecting to an ERPS ring belong to a control VLAN, and only such ports can be added to a control VLAN.
- Data VLAN: A data VLAN is used to transmit data packets. Both ERPS ports and non-ERPS ports can be assigned to a data VLAN. A data VLAN is also known as a protected VLAN.

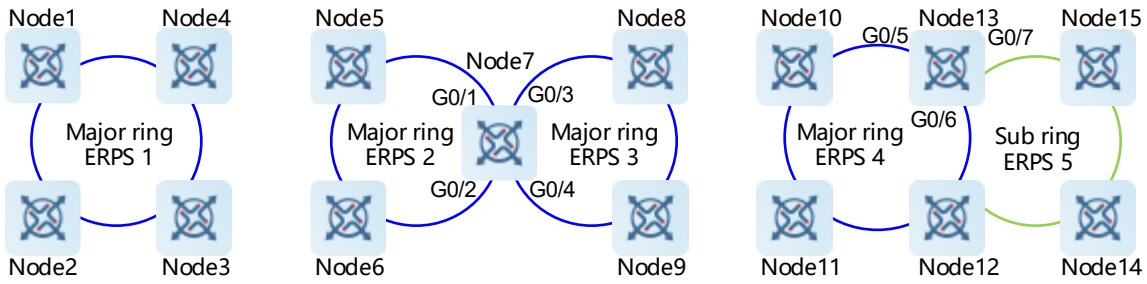
11.4.3 Basic Model of an Ethernet Ring

A group of interconnected devices in the same control VLAN (R-APS VLAN) constitute an Ethernet ring (ERPS ring), in which each device is called a node. ERPS rings can be classified into major rings and subrings based on whether a ring is closed.

1. Major Ring and Subring

- Major ring and major ring link: A major ring is a topology of a closed network connected in a ring, such as the blue rings shown in Figure 11-1. In an ERPS ring, links that belong to and are controlled by a major ring are called major ring links.
- Subring and subring link: A subring is a topology of a non-closed network attached to a major ring, such as the green ring shown in Figure 11-1. In an ERPS ring, links that belong to and are controlled by a subring are called subring links.
- R-APS virtual channel of a subring: As shown in Figure 11-1, all the links on the major ring can be regarded as R-APS virtual channels of subrings, which are used to forward subring protocol packets. They belong to the major ring instead of the subring. The major ring must associate with the control VLAN of the subring and allow packets from this VLAN to pass through.

Figure 11-1 Basic Topologies of Ethernet Rings



2. Basic Topologies

Major rings, subrings, and nodes can form basic topologies with different characteristics, depending on the connection modes, as shown in Figure 11-1.

- Single ring: Major ring ERPS 1 (node 1-2-3-4) constitutes a single-ring topology.
- Tangent rings: A topology in which two ERPS rings share one device is called tangent rings. Major ring ERPS 2 (node 5-6-7) and major ring ERPS 3 (node 7-8-9) constitute a tangent-ring topology, and are tangent to each other on one node, namely, node 7.
- Intersecting rings: A topology in which two ERPS rings share two devices is called intersecting rings. Major ring ERPS 4 (node 13-10-11-12) and subring ERPS 5 (node 13-15-14-12) constitute an intersecting-ring topology, and intersect on two directly connected intersecting nodes, namely, node 13 and node 12.

In practice, a network is a combination of multiple basic topologies, with multiple major rings and multiple subrings.

3. Node

According to the different topological relationships between nodes and Ethernet rings, nodes are classified into single-ring nodes, tangent nodes, and intersecting nodes by role.

- Single-ring node: In an Ethernet ring, the nodes that belong to only one Ethernet ring (either major ring or subring) are called single-ring nodes. Two interfaces need to be provided on a single-ring node so that the node can be added to one ERPS ring. As shown in Figure 11-1, nodes 1-4 in the single-ring topology, nodes 5, 6, 8, and 9 in the tangent-ring topology, and nodes 10, 11, 14, and 15 in the intersecting-ring topology are all single-ring nodes.

- Tangent node: A device shared in tangent rings is called a tangent node. Four interfaces need to be provided on each tangent node, with two added to a major ring and the other two added to another major ring. As shown in Figure 11-1, node 7 in the tangent-ring topology is a tangent node.
- Intersecting node: The nodes in intersecting rings that belong to multiple rings are called intersecting nodes. Three interfaces need to be provided on a tangent node, with two added to a major ring and the other added to a subring. As shown in Figure 11-1, nodes 12 and 13 in the intersecting-ring topology are intersecting nodes. ERPS rings can intersect with other multiple ERPS rings and share links to implement data link redundancy. Services can be quickly switched from a failed link in one ERPS ring to a normal link.

4. Ring Member Port

An Ethernet ring has two ring member ports on each node that it passes through: the **west** and **east** ports. As shown in Figure 11-1:

- If an ERPS ring is a closed major ring, each node that the ring passes through has two interfaces used as the **west** and **east** ports for adding the node to the ERPS ring. For example, on node 7, GigabitEthernet 0/1 and 0/2 are added to the major ring ERPS 2, and GigabitEthernet 0/3 and 0/4 are added to the major ring ERPS 3. On node 13, GigabitEthernet 0/5 and 0/6 are added to the major ring ERPS 4.
- If an ERPS ring is a non-closed subring (in an intersecting-ring topology), a non-intersecting node has two interfaces used as the **west** and **east** ports for adding the node to the ERPS subring, such as node 15. On an intersecting node, only one physical port is added to the ERPS subring as a ring member port, and the other ring member port is a virtual channel (indicated by **virtual-channel**). For example, on node 13, only GigabitEthernet 0/7 is added to the subring ERPS 5.

There are two states for a port running the ERPS protocol: forwarding and block. Their functions are listed in Table 11-6.

Table 11-6ERPS Protocol Port States

Port State	Receiving Protocol Packets	Sending Protocol Packets	Address Learning	Receiving Data Packets	Sending Data Packets
Block	Yes	Yes	No	No	No
Forwarding	Yes	Yes	Yes	Yes	Yes

11.4.4 RPL and Nodes

An Ethernet ring can be in either of the following two states regardless of whether it is a major ring or subring:

- **Idle** state: The physical links in the entire ring network are connected.
- **Protection** state: A physical link in the ring network is disconnected.

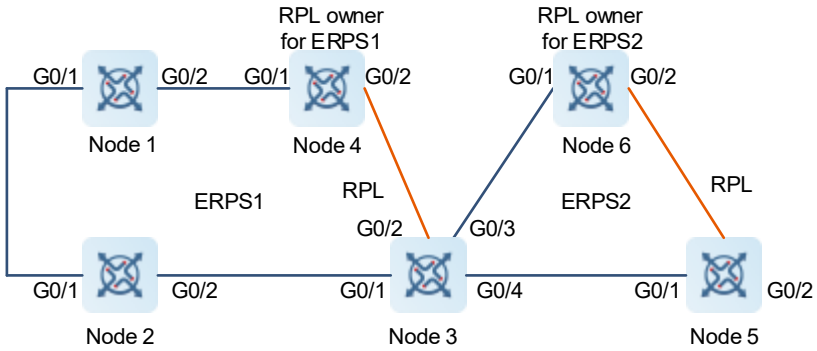
Ring protection link (RPL): When the physical links in a ring network are connected, the ERPS ring is in the idle state, and the links in the logic blocking state are RPLs. Each Ethernet ring has only one RPL. For example, the links indicated by the orange lines shown in Figure 11-2 are RPLs, the link between node 3 and node 4 is the RPL of the Ethernet ring ERPS 1 (node 1-2-3-4), and the link between node 5 and node 6 is the RPL of the Ethernet ring ERPS 2 (node 3-5-6).

A node that is adjacent to an RPL and is used to block the RPL to prevent loops when the Ethernet ring is free of faults is called an RPL **owner** node. As shown in Figure 11-2, node 4 is the RPL owner node of the Ethernet ring ERPS 1 (node 1-2-3-4) and node 6 is the RPL owner node of the ERPS 2 (node 3-5-6).

Any nodes other than the RPL owner node in an Ethernet ring are non-RPL owner nodes. As shown in Figure 11-2, nodes except node 4 and node 6 are non-RPL owner nodes of the rings.

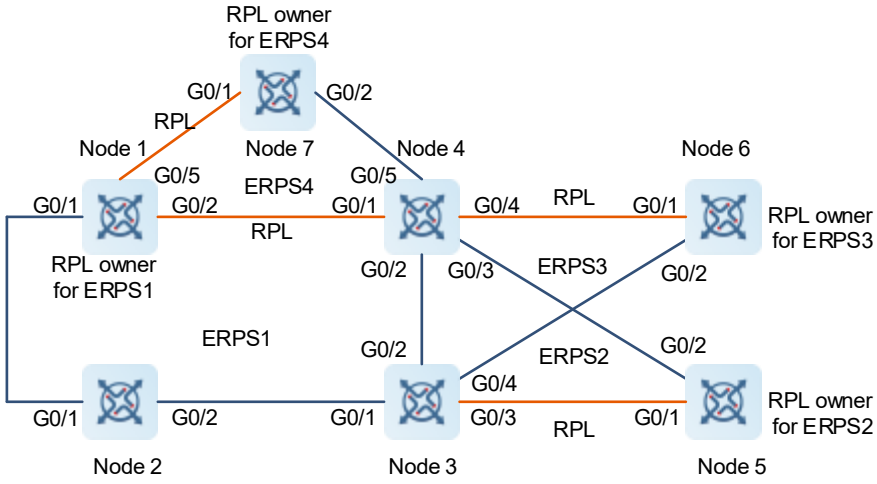
Blocked ports on RPLs are RPL ports, and RPL ports do not forward data packets to prevent loops. RPL ports are on RPL owner nodes, and the RPL owner nodes block the RPL ports. Each Ethernet ring has only one RPL owner node.

Figure 11-2 Typical Topology of Tangent Rings



As shown in Figure 11-2, the link between node 3 and node 4 is the RPL of the Ethernet ring ERPS 1. As the RPL owner node of ERPS 1, node 4 blocks the RPL port. The link between node 5 and node 6 is the RPL of the Ethernet ring ERPS 2. As the RPL owner node of ERPS 2, node 6 blocks the RPL port. ERPS 1 (node 1-2-3-4) and ERPS 2 (node 3-5-6) share node 3, forming a tangent-ring topology. Node 3 is the tangent node.

Figure 11-3 Typical Topology of Intersecting Rings



As shown in Figure 11-3, ERPS 1 (node 1-2-3-4) is a major ring, and ERPS 2 (node 3-4-5) is a subring. ERPS 1 and ERPS 2 share node 3 and node 4, forming an intersecting-ring topology. The links between node 4 and node 5, and between node 3 and node 5 are links of the subring ERPS 2 and are controlled by ERPS 2. The link between node 3 and node 4 belongs to the major ring not the subring, and is not controlled by the subring. However, the protocol packets of the subring are transmitted through the direct link between node 3 and node 4. This direct link is the R-APS virtual channel of the subring ERPS 2. Node 2 only belongs to the major ring ERPS 1, and is called a single-ring node.

Node 6 only belongs to the subring ERPS 3, and is also called a single-ring node. Node 3 and node 4 are tangent nodes.

11.4.5 ERPS Packet

ERPS packets (also called R-APS packets) are classified into Signal Fail (SF) packets, No Request (NR) packets, No Requests-RPL Blocked (NR-RB) packets, and Flush packets.

- SF packet: When the link of a node is down, the node sends an SF packet to notify other nodes of its link failure.
- NR packet: When the failed link is restored, the node sends an NR packet to notify the RPL owner node of its link recovery.
- NR-RB packet: When all nodes in an ERPS ring function properly, the RPL owner node sends NR-RB packets periodically.
- Flush packet: In intersecting rings, when a topology change occurs in a subring, the intersecting nodes send flush packets to notify other devices in the Ethernet ring to which the subring is connected.

11.4.6 ERPS Timer

ERPS supports three timers: Holdoff timer, Guard timer, and **Wait-To-Restore** (WTR) timer.

- **Holdoff** timer: The timer is used to minimize frequent ERPS topology switching due to intermittent link failures. After you configure the Holdoff timer, ERPS performs topology switching only if the link failure still persists after the timer times out.
- **Guard** timer: The timer is used to prevent a device from receiving expired R-APS PMDU packets. When a device detects that a link failure is cleared, it sends link recovery packets and starts the **Guard** timer. Before the timer expires, all packets except Flush packets indicating a subring topology change will be discarded.
- WTR timer: The timer is effective only for RPL owner nodes. It is used to avoid ring status misjudgment by the RPL owner node. When an RPL owner node detects that a failure is cleared, it will not perform topology switching immediately but only if the Ethernet ring is recovered after the WTR timer times out. If a ring failure is detected again before the timer expires, the RPL owner node cancels the timer and does not perform topology

switching.

11.4.7 Ring Protection

The ring protection function prevents broadcast storms caused by data loops and can rapidly recover the communication between nodes when a link is disconnected in the Ethernet ring.

- Normal state
  - All nodes in the physical topology are connected in ring mode.
  - ERPS blocks the RPL to prevent loops.
  - ERPS detects failures on each link between adjacent nodes.
- Link fault

  A node adjacent to a failed node detects the fault.

  The node adjacent to the failed link blocks the failed link and sends SF packets to notify other nodes in the same ring.

  An SF packet triggers the RPL owner node to enable the RPL port, and also triggers all nodes to update their MAC address entries and ARP/ND entries and enter the protection state.
- Link recovery

  When a failed link is restored, an adjacent node still blocks the link and sends NR packets indicating that no local fault exists.

  When the RPL owner node receives the first NR packet, it starts the WTR timer.

  When the WTR timer times out, the RPL owner node blocks the RPL and sends an NR-RB packet.

  After receiving this NR-RB packet, other nodes update their MAC address entries and ARP/ND entries, and the node that sends the NR packet stops sending the NR packet and enables the blocked ports.
  - The ring network is restored to the normal state.

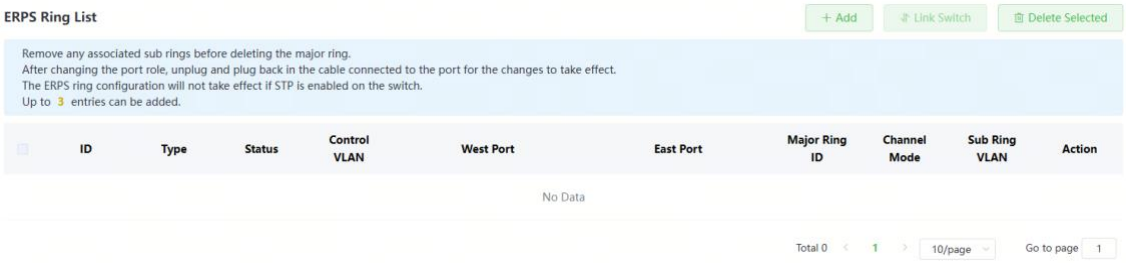
11.4.8 Protocols and Standards

- ITU-T G.8032/Y.1344: Ethernet ring protection switching

11.4.9 Configuring ERPS

1. Adding and Deleting an ERPS Ring

Choose **Local Device** > **Advanced** > **ERPS**.



(1) Click **Add** on the **ERPS Ring List** page.

(2) Configure the parameters on the page based on the service requirements.

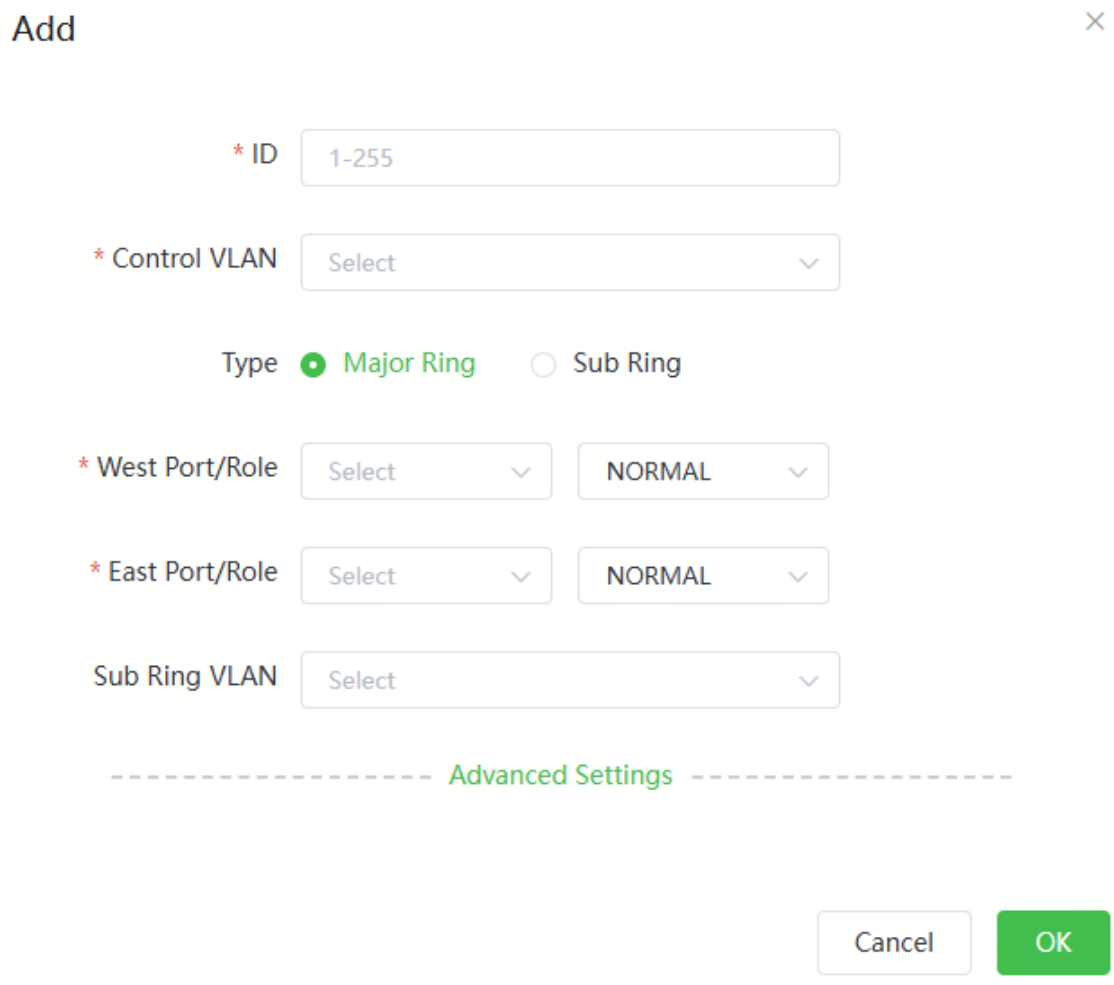
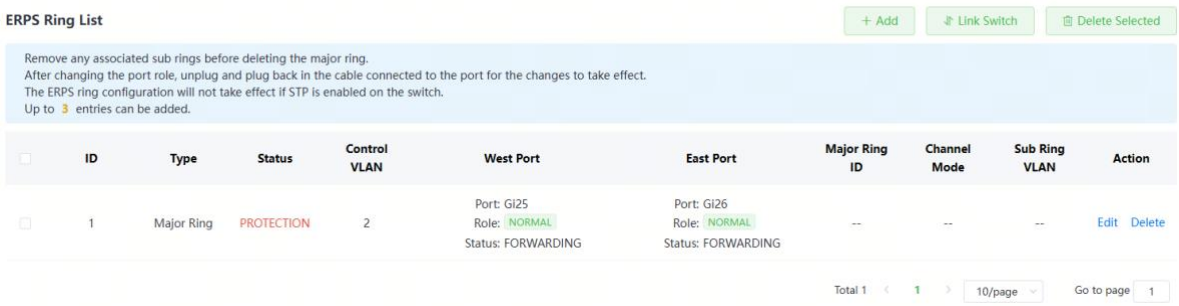


Table 11-7Parameter Description

Parameter	Description	Default Value
ID	Specifies the ID of an ERPS instance.	N/A
Control VLAN	It is used to forward ERPS protocol packets.	N/A
Type	Indicates the type of the ERPS ring. The ring can be a major ring or a sub ring.	N/A
West Port/Role	Specifies the west port in the ERPS ring and its role. The values of a port role include: ● NORMAL: Indicates a normal node. ● RPL OWNER: Indicates an RPL owner node. ● RPL NEIGHBOR: Indicates an RPL neighbor node.	N/A
East Port/Role	Specifies the east port in the ERPS ring and its role. The values of a port role include: ● NORMAL: Indicates a normal node. ● RPL OWNER: Indicates an RPL owner node. ● RPL NEIGHBOR: Indicates an RPL neighbor node.	N/A
Sub Ring VLAN	Specifies the control VLAN of a sub ring.	N/A
WTR Timer	Specifies the interval of the WTR timer.	5 min
Guard Timer	Specifies the interval of the Guard timer.	500 ms
Hold-off Timer	Specifies the interval of the Hold-off timer.	0 ms, indicating a topology switch is performed immediately after a link

Parameter	Description	Default Value
		failure is detected.
MEL Level	Indicates the maintenance entity group (MEG) level. The MEL level of devices in the same ERPS ring must be consistent.	7
Revertive Mode	When this switch is toggled on, once the condition causing a switch has cleared, traffic is blocked on the RPL.	Enabled.

(3) (Optional) Select existing ERPS rings, and then click **Delete Selected** to delete selected ERPS rings.



2. Link Switch

Choose **Local Device** > **Advanced** > **ERPS**.

(1) Click **Link Switch** on the **ERPS Ring List** page.

(2) Configure the parameters on the page based on the service requirements.

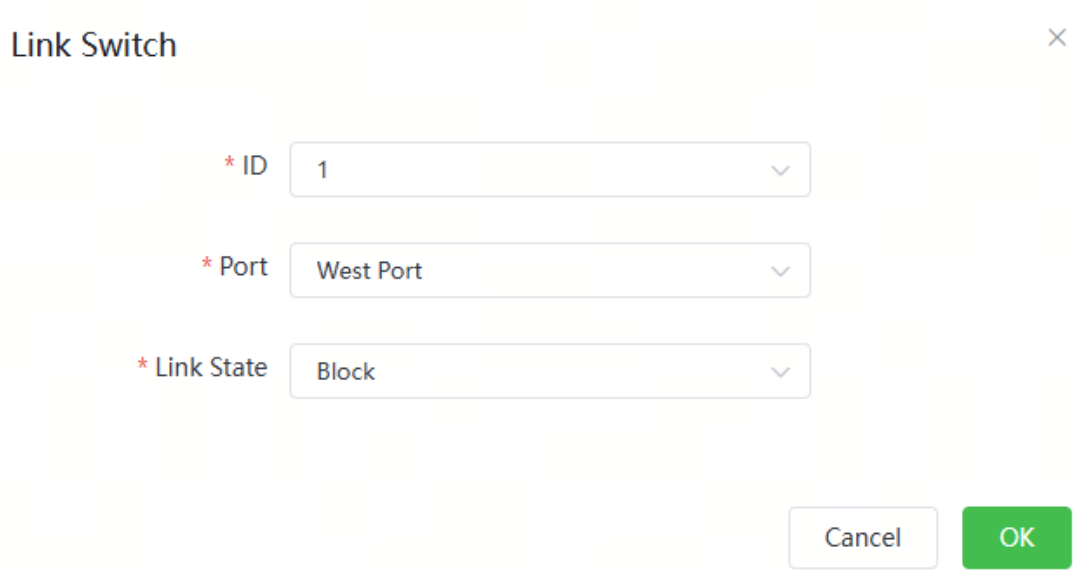


Table 11-8Parameter Description

Parameter	Description	Default Value
ID	Specifies the ID of an ERPS instance.	N/A
Port	Specifies the port in the ERPS ring. The values include West Port and East Port.	N/A
Link State	Specifies the link state of the selected port. The values include Clear and Block. ● Clear: Indicates that the port is blocked by a forced switch operation. ● Block: Indicates that the port is blocked by a manual switch operation.	N/A

11.5 QoS

11.5.1 Overview

Quality of service (QoS) can meet users' requirements for different applications and different levels of service quality. It allocates and schedules resources based on users' requirements and provides different levels of service quality for different packets.

On a traditional IP network, a device treats all the packets in the same way, in which the device processes packets based on their arrival time according to the queuing strategy of first in first out (FIFO), and transmits the packets to the destination on a best-effort basis. When the network bandwidth is abundant, all the packets are properly processed; when the network is congested, all the packets may be discarded.

QoS assigns a transmission priority to the packets of a type to highlight the importance of the packets. Then, the devices provide special transmission services for these packets according to forwarding policies for different priorities, congestion avoidance, and other mechanisms. With QoS, a device processes real-time and important packets preferentially, processes non-real-time and common packets with lower priorities and even discards the packets upon network congestion.

QoS enhances the network performance predictability, effectively allocates network bandwidth, and reasonably utilizes network resources.

11.5.2 Principles

1. Basic Concepts

- DiffServ model

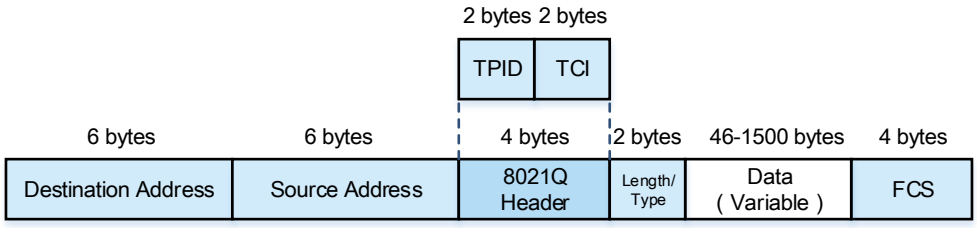
  The differentiated services (DiffServ) model classifies all packets transmitted on a network into different types. The classification information related to QoS priority marking is recorded in some fields of Layer 2 or Layer 3 packets, for example, the PRI field of IEEE 802.1Q frames, type of service (ToS) field of IPv4 packets, traffic class (TC) field of IPv6 packets, and the MPLS experimental bits (EXP) field of multiprotocol label switching (MPLS) packets.

  In the network of DiffServ model, the classification information of packets can be assigned by hosts or other network devices or based on different application policies or different packet contents. A device applies the same transmission service policy to packets containing the same classification information and applies different transmission service policies to packets containing different classification information. Based on the classification information carried by packets, a device may provide different transmission priorities for different packets, reserve bandwidth for a kind of packets, discard certain packets with lower priorities, or take some other actions.

- PRI field of the IEEE 802.1q frames

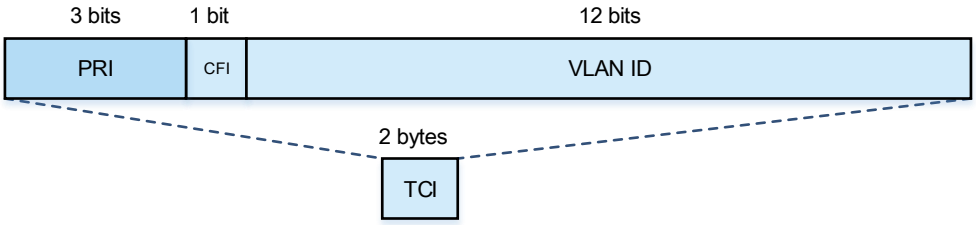
The PRI field of IEEE 802.1Q frames (namely, the IEEE 802.1p priority) is located in the header of a Layer 2 packet containing an IEEE 802.1Q tag header, as shown in Figure 11-4.

Figure 11-4 Format of a Layer 2 Frame with an IEEE 802.1Q Tag Header



The 4-byte IEEE 802.1Q tag header contains the 2-byte tag protocol identifier (TPID) and 2-byte tag control information (TCI). TCI contains the 3-bit PRI field, as shown in Figure 11-5.

Figure 11-5 PRI Field of the IEEE 802.1q Frames

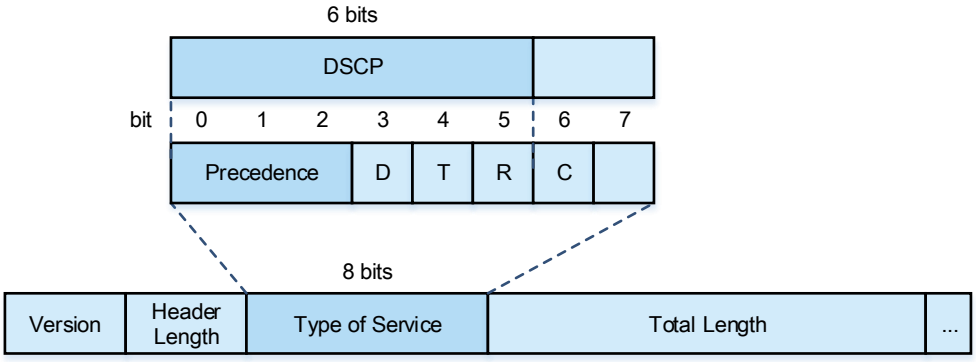


The PRI field represents eight priorities for packet transmission, and the priority values from high to low are 7, 6, ..., 1, and 0. The IEEE 802.1p priority is applicable to scenarios where Layer 3 headers do not need to be analyzed and QoS needs to be implemented only at Layer 2.

- ToS field of the IPv4 packets

  IPv4 packets use the ToS field in the IP header to indicate the priority of the packets, as shown in Figure 11-6.

Figure 11-6 ToS Field in the IP Header



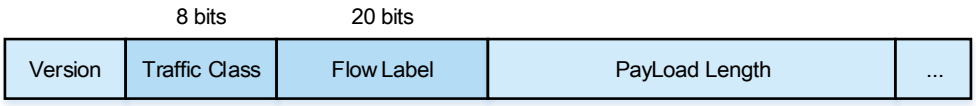
The ToS field contains eight bits, of which the first three bits are the IP PRE (precedence) field and represent eight priorities for packet transmission, with the priority values from high to low being 7, 6, ..., 1, and 0.

RFC 2474 redefines the ToS field of the IP header, in which the first 6 bits (bits 0 to 5) represent the differentiated services code point (DSCP). DSCP is used to classify packets into a maximum of 64 different categories.

- ToS field of the IPv6 packets

  IPv6 packets use the TC field in the IPv6 header to indicate the packet priority, as shown in Figure 11-7Figure 11-7.

Figure 11-7 TC Field in the IPv6 Header



The TC field contains eight bits and provides the same function as the ToS field of IPv4 packets. The first six bits of the TC field indicate DSCP.

2. Priority Mapping

Priorities are used to identify the scheduling weights or forwarding priority of packets. Different priority types are defined for different packet types: IEEE 802.1q frames use the IEEE 802.1p priority, IP packets use the DSCP, and so on.

After a packet enters a device interface, the packet priority is mapped to the CoS according to the trust mode configured for the interface. Table 11-9 shows the mappings between trust mode configured for an interface and the priorities.

Table 11-9Interface Trust Mode and Priority Mapping

Trust Mode	Priority Mapping
Untrusted	● The device does not trust any priority information carried in the packet. ● A packet received by the interface is assigned to a queue based on the 802.1p-queue mapping table using the 802.1p value (interface priority) configured for the interface. ● For a packet with a VLAN tag sent by the interface, the device re-marks the 802.1p value of the packet based on the queue-802.1p mapping table. ● For a packet without a VLAN tag sent by the interface, the device does not re-mark the 802.1p value of the packet. ● If the packet sent by the interface is an IP packet, the device re-marks the DSCP value of the packet based on the queue-DSCP mapping table.
802.1p	● After an interface receives a packet: ○ If the packet carries a VLAN tag, the 802.1p value carried by the packet will be used as the input for mapping, and the packet will be assigned to a queue based on the 802.1p-queue mapping table. ○ If the packet does not carry any VLAN tag, it will be processed by the device in the same way as that in untrusted mode. ● For a packet with a VLAN tag sent by the interface, the device re-marks the 802.1p value of the packet based on the queue-802.1p mapping table. ● For a packet without a VLAN tag sent by the interface, the device does not re-mark the 802.1p value of the packet. ● If the packet sent by the interface is an IP packet, the device re-marks the DSCP value of the packet based on the queue-DSCP mapping table.
DSCP	● After an interface receives a packet: ○ If the packet is not an IP packet, it will be processed by the device in the same way as that in 802.1p mode. ○ If the packet is an IP packet, the DSCP value of the packet will be used as the input for mapping, and the packet will be assigned to a queue based on the DSCP-queue mapping table. ● If the packet sent by the interface is an IP packet, the device re-marks the DSCP value of the packet based on the queue-DSCP mapping table. ● If the packet sent by the interface is not an IP packet, the packet is processed depending on whether it carries a VLAN tag:

Trust Mode	Priority Mapping
	○ If the packet carries a VLAN tag, the device re-marks the 802.1p value of the packets based on the queue-802.1p mapping table. ○ If the packet does not carry a VLAN tag, the device does not re-mark the 802.1p value of the packet.

3. Congestion Management

When the receiving rate of packets exceeds the sending rate, congestion occurs on the sending interface. If no sufficient buffer is provided to store these packets, packet loss may occur. The congestion management mechanism determines the sending order of packets based on their local priorities. The congestion management function controls congestion and improves the local priorities of packets for some important data. When congestion occurs, the packets of higher priorities are sent first to ensure that key services are provided in time.

Congestion management adopts the queue scheduling mechanism. The processing is as follows:

(1) Each packet is assigned to a queue based on priority-to-queue mappings.

(2) The outbound interface selects the packets in a queue for sending according to various queue scheduling policies (such as SP, WRR, and SP+WRR).

- SP scheduling policy

  In strict-priority (SP) scheduling, packets are scheduled strictly based on their queue priorities from high to low (a larger queue ID indicates a higher priority). Before sending a packet, check whether there is a packet to be sent in a high-priority queue. If there is, send it. If not, check whether there is a packet to be sent in the next-level queue, and so on.

  The weakness of SP scheduling is that, when congestion occurs, if the packets in a higher priority queue exist for a long time, the packets in a lower priority queue have no opportunity of being scheduled.

- WRR scheduling policy

  Weighted Round Robin (WRR) ensures that all queues are scheduled in turn. Taking eight output queues as an example, the device allocates bandwidth resources based on the weight of each queue. For example, if the WRR weights of a 1000 Mbps port are set to 50, 50, 30, 30, 10, 10, 10, and 10, WRR ensures that at least 50 Mbps of

bandwidth is allocated to the queue with the lowest priority. WRR also allows for efficient use of bandwidth by immediately switching to the next queue when a queue is empty.

- SP+WRR scheduling policy

  SP scheduling is configured for one or more sending queues, and the other queues are scheduled in the WRR mode. Among SP queues, only after all the packets in an SP queue with a higher priority are sent, can the packets in an SP queue with a next higher priority be sent. Among SP and WRR queues, only after the packets in all SP queues are sent, can the packets in WRR queues be sent.

11.5.3 Configuring QoS

1. Global Configuration

In local device mode, choose **Advanced** > **QoS** > **Global Config**.

In the **Global Config** page, you can configure the trust mode, modify the 802.1p-Queue Mapping Table for inbound packets, modify the DSCP-Queue Mapping Table for inbound packets, modify the Queue-802.1p Mapping Table for outbound packets, and modify the Queue-DSCP Mapping Table for outbound packets.

Click **Batch Config** to batch configure these mapping tables.

Click **Reset** to restore a mapping table to default values.

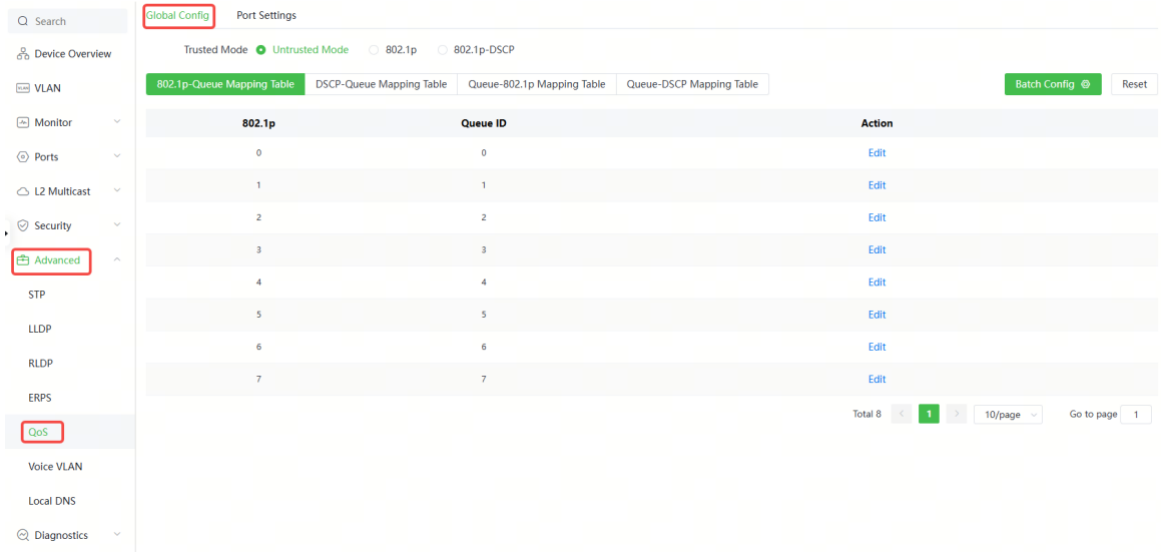


Table 11-10 Global Configuration Parameter Description

Parameter	Description	Default Value
Trusted Mode	Priority designations of an inbound packet: **Untrusted Mode**: The device does not trust any priority information carried in the packet, and uses the interface priority as the 802.1p value of the packet. The device assigns the packet into a queue based on the 802.1p-queue mapping table. If **Untrusted Mode** is selected, any packets received by any interface on the device will be assigned to queues based on the interface priority regardless of the trust mode status configured in the **Port Settings** page. **802.1p**: The device trusts the 802.1p value carried in the packet, and use the 802.1p value to assign the packet to a queue based on the 802.1p-queue mapping table. If the packet does not carry an 802.1p value, that is, the packet does not carry a VLAN tag, the device will process the packet in the same way as that in untrusted mode. If **802.1p** is selected, and the designated interface is in untrusted mode in the **Port Settings** page, the device will process the packet in the same way as that in untrusted mode. **802.1p-DSCP**: The device trusts the 802.1p value (for non-IP packets) or DSCP value (for IP packets) of the packet, and assigns the packet to a queue based on the 802.1p-queue mapping table or the DSCP-queue mapping table depending on the 802.1p value or DSCP value of the packet. If **802.1p-DSCP** is selected, and the designated interface is in untrusted mode in the **Port Settings** page, the device will process the packet in the same way as that in untrusted mode.	Untrusted Mode

Parameter	Description	Default Value
802.1p-Queue Mapping Table	An input queue mapping table, which contains the mappings between the 802.1p value and the queue ID. For example, if the 802.1p value is 0, and the queue ID is 1, packets with the 802.1p value 0 will be assigned to queue 1.	As shown in Table 11-11
DSCP-Queue Mapping Table	An input queue mapping table, which contains the mappings between the DSCP value and the queue ID. For example, if the DSCP value falls within 0 to 7, and the queue ID is 0, packets with a DSCP value between 0 and 7 will be assigned to queue 0.	As shown in Table 11-12
Queue-802.1p Mapping Table	An output queue mapping table, which contains the mappings between the queue ID and the 802.1p value. The 802.1p value of an outgoing packet in a queue is re-marked based on the mapping. For example, if the queue ID is 0, and the packets carrying a VLAN tag in queue 0 have an 802.1p value, then the 802.1p value of the packets in queue 0 are re-marked to 2. If a packet does not carry any 802.1p value, that is, the packet does not carry any VLAN tag, the device does not re-mark the 802.1p value of the packet.	As shown in Table 11-13
Queue-DSCP Mapping Table	An output queue mapping table, which contains the mappings between the queue ID and the DSCP value. The DSCP value of packets in the output queue is re-marked based on the mapping. For example, if the queue ID is 0, and the mapped DSCP value is 8, then the DSCP value of packets in queue 0 is re-marked to 8.	As shown in Table 11-14

Table 11-11 Default 802.1p-Queue Mapping Table of the Device

802.1p Value	Queue ID
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Table 11-12 Default DSCP-Queue Mapping Table of the Device

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

Table 11-13 Default Queue–802.1p Mapping Table of the Device

Queue ID	802.1p Value After Remarking
0	0
1	1
2	2
3	3
4	4
5	5
6	6
7	7

Table 11-14 Default Queue-DSCP Mapping Table of the Device

Queue ID	DSCP Value After Re-marking
0	0
1	8
2	16
3	24
4	32
5	40
6	48
7	56

2. Port Settings

In local device mode, choose **Advanced** > **QoS** > **Port Settings**.

In the **Port Settings** page, you can set the priority, trust mode, 802.1p remarking, DSCP remarking, queue algorithm, and queue ID/weight for a designated interface.

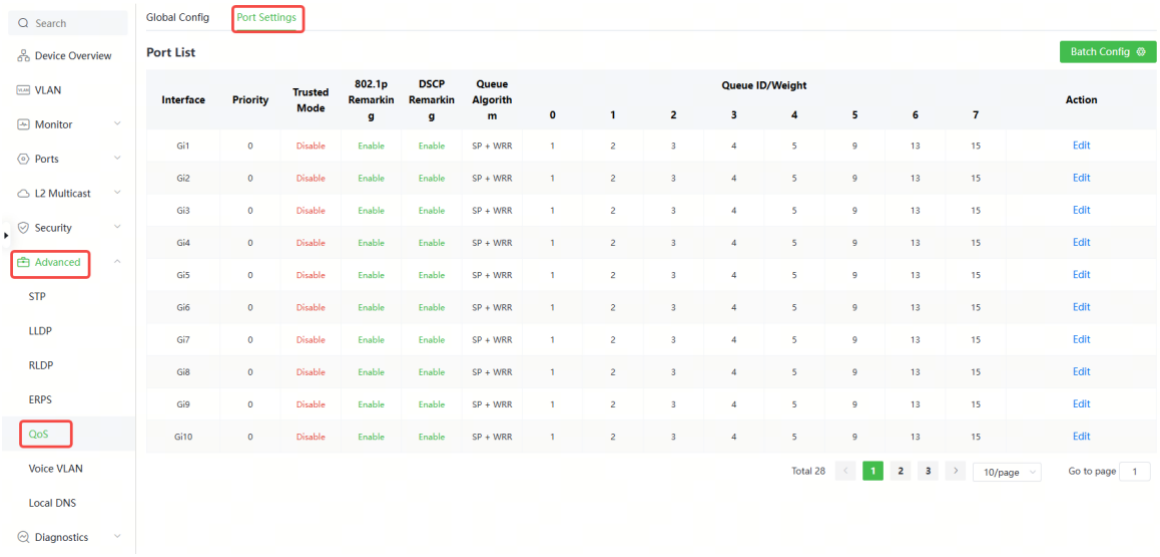


Table 11-15 Port Configuration Parameter Description

Parameter	Description	Default Value
Priority	Interface priority. When the device is in untrusted mode, packets are assigned to a queue based on this priority, which is equivalent to the 802.1p value of a packet.	0
Trusted Mode	Priority designations of an inbound packet: Disable: The device does not trust any priority information carried in the packet, and uses the interface priority as the 802.1p value of the packet. The device assigns the packet into a queue based on the 802.1p-queue mapping table. Enable: The device trusts the 802.1p value (for non-IP packets) or DSCP value (for IP packets) of the packet, and assigns the packet to a queue based on the 802.1p-queue mapping table or the DSCP-queue mapping table	Disable

Parameter	Description	Default Value
	depending on the 802.1p value or DSCP value of the packet. If Untrusted Mode is selected in the Global Config page, any packets received by any interface on the device will be assigned to queues based on the interface priority regardless of the trust mode status configured in the Port Settings page. If 802.1p or 802.1p-DSCP is selected in the Global Config page, the device will only process packets received by the specified interface in the same way as that in trusted mode when the Trusted Mode of the designated interface is set to Enable in the Port Settings page.	
802.1p Remarking	Enable: The 802.1p value of packets in the queue is re-marked based on the Queue-802.1p Mapping Table. Disable: The device does not re-mark the 802.1p value of packets in the queue based on the Queue-802.1p Mapping Table, and marks the priority of the outgoing packets based on the priority of the input queue.	Enable
DSCP Remarking	Enable: The DSCP value of packets in the queue is re-marked based on the DSCP-802.1p Mapping Table. Disable: The device does not re-mark the DSCP value of packets in the queue based on the Queue-802.1p Mapping Table, and marks the priority of the outgoing packets based on the priority of the input queue.	Enable
Queue Algorithm	The queue algorithm adopted by the interface.	SP+WRR
Queue ID/Weight	WRR weight of a queue. The value 0 indicates that the SP algorithm is adopted for the queue. After all packets in all SP queues are sent, the device will send packets in	As shown in Table 11-16

Parameter	Description	Default Value
	WRR queues. Among SP queues, the queue with a larger ID is scheduled first.	

Table 11-16 Default Interface Queue ID/Weight of the Device

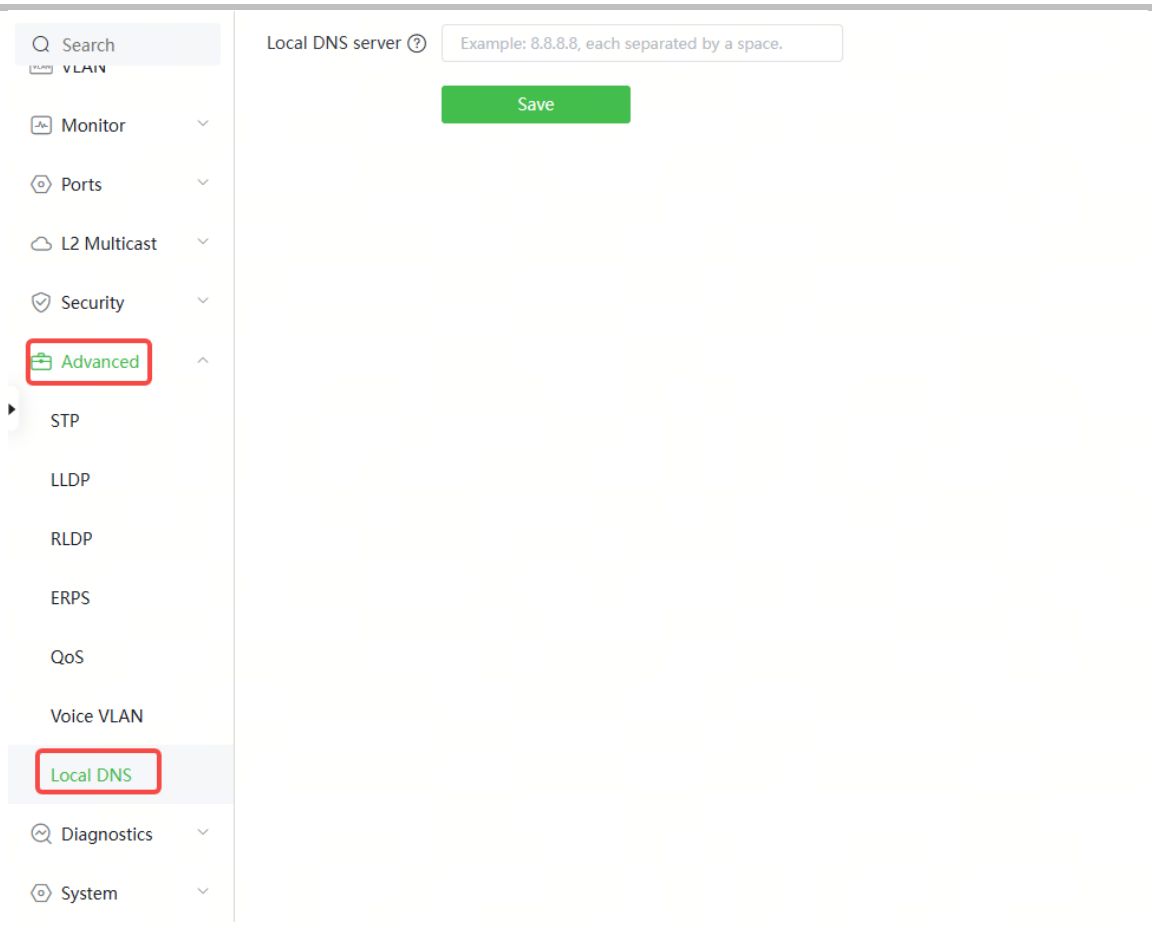
Queue ID	WRR Weight
0	1
1	2
2	3
3	4
4	5
5	9
6	13
7	15

11.6 Configuring the Local DNS

The local DNS server is optional. The device obtains the DNS server address from the connected uplink device by default.

Choose **Local Device** > **Advanced** > **Local DNS**.

Enter the DNS server address used by the local device. If multiple addresses exist, separate them with spaces. Click **Save**. After configuring the local DNS, the device first use the DNS of the management IP address for parsing domain names. If the device fail to parse domain names, then use this DNS address instead.



11.7 Voice VLAN

11.7.1 Overview

A voice virtual local area network (VLAN) is a VLAN dedicated to voice traffic of users. By creating a voice VLAN and adding ports connected to voice devices to the voice VLAN, you can have voice data transmitted in the voice VLAN and deliver specified policy of the quality of service (QoS) for voice streams, to improve the transmission priority of voice traffic and ensure the call quality.

11.7.2 Configuring a Voice VLAN Globally

Choose **Local Device** > **Advanced** > **Voice VLAN** > **Global Settings**.

Turn on the voice VLAN function, configure global parameters, and click **Save**.

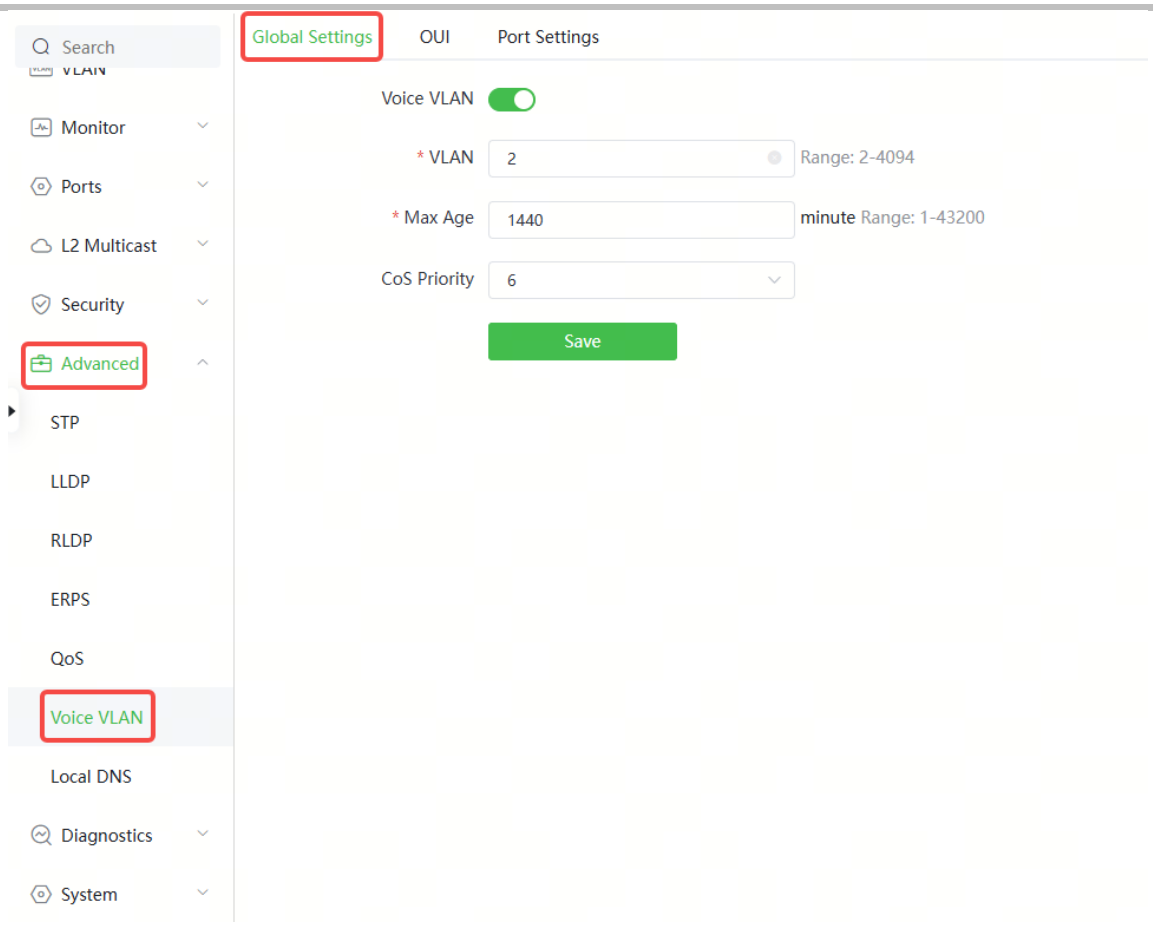


Table 11-17 Description of VLAN Global Configuration Parameters

Parameter	Description	Default Value
Voice VLAN	Whether to enable the Voice VLAN function	Disable
VLAN	VLAN ID as Voice VLAN	NA
Max Age	Aging time of voice VLAN, in minutes. In automatic mode, after the MAC address in a voice packet ages, if the port does not receive any more voice packets within the aging time, the device removes this port from the voice VLAN	1440 minutes
CoS Priority	The Layer 2 Priority of voice stream packets in a Voice VLAN. The value range is from 0 to 7. A greater value indicates a higher priority.	6

Parameter	Description	Default Value
	You can modify the priority of the voice traffic to improve the call quality.	

11.7.3 Configuring a Voice VLAN OUI

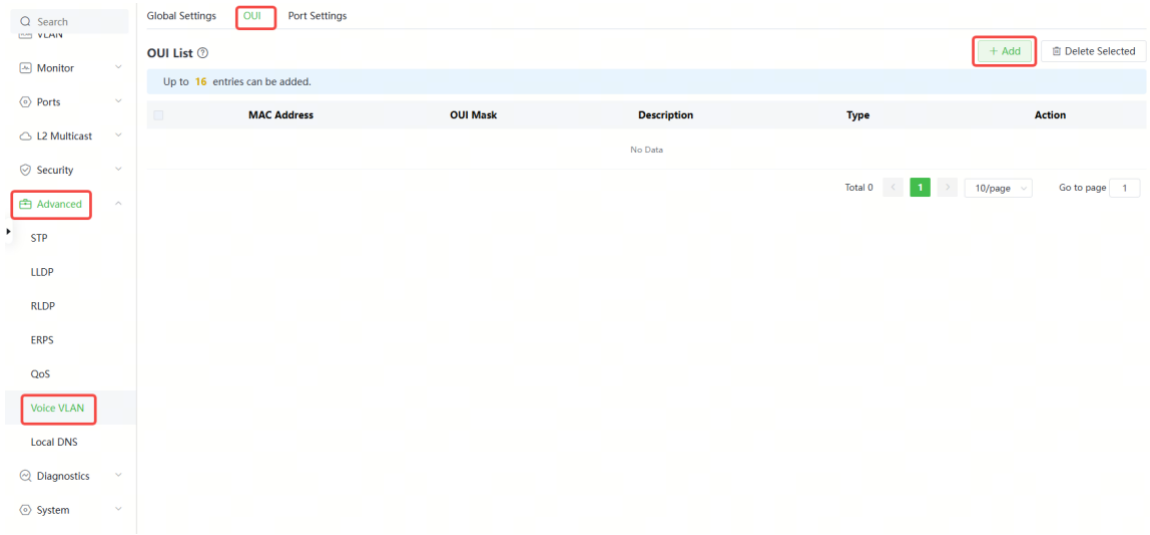
Choose **Local Device** > **Advanced** > **Voice VLAN** > **OUI**.

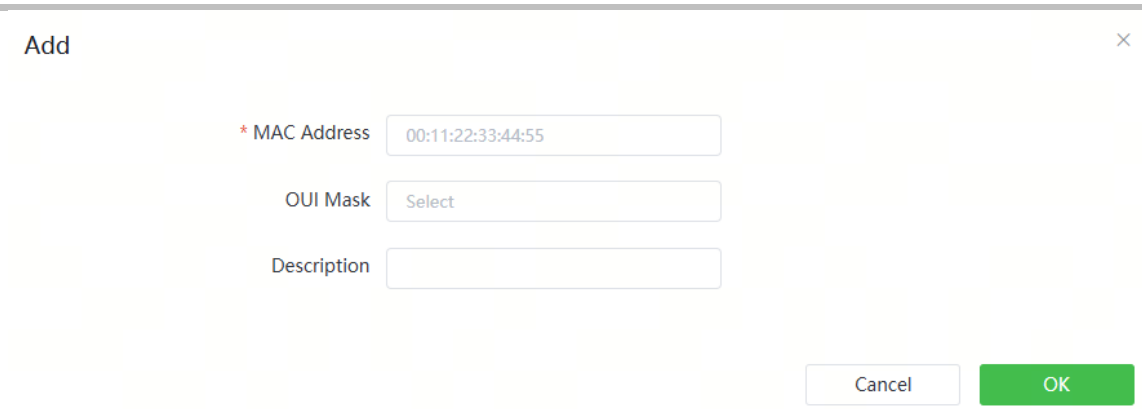
The source MAC address of a voice packet contains the organizationally unique identifier (OUI) of the voice device manufacturer. After the voice VLAN OUI is configured, the device compares the voice VLAN OUI with the source MAC address in a received packet to identify voice data packets, and sends them to the voice VLAN for transmission.

Note

After the voice VLAN function is enabled on a port, when the port receives LLDP packets sent by IP phones, it can identify the device capability fields in the packets, and identify the devices with the capability of **Telephone** as voice devices. It also extracts the source MAC address of a protocol packet and processes it as the MAC address of the voice device. In this way, the OUI can be added automatically.

Click **Add**. In the displayed dialog box, enter an MAC address and OUI, and click **OK**.

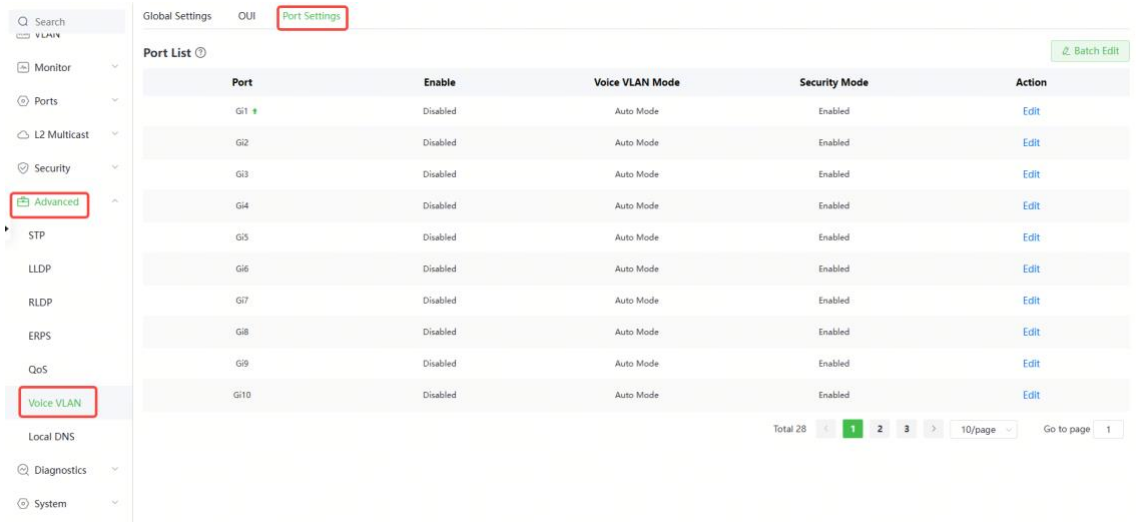




11.7.4 Configuring the Voice VLAN Function on a Port

Choose **Local Device** > **Advanced** > **Voice VLAN** > **Port Settings**.

Click **Edit** in the port entry or click **Batch Edit** on the upper-right corner. In the displayed dialog box, select whether to enable the voice VLAN function on the port, voice VLAN mode to be applied, and whether to enable the security mode, and Click **OK**.



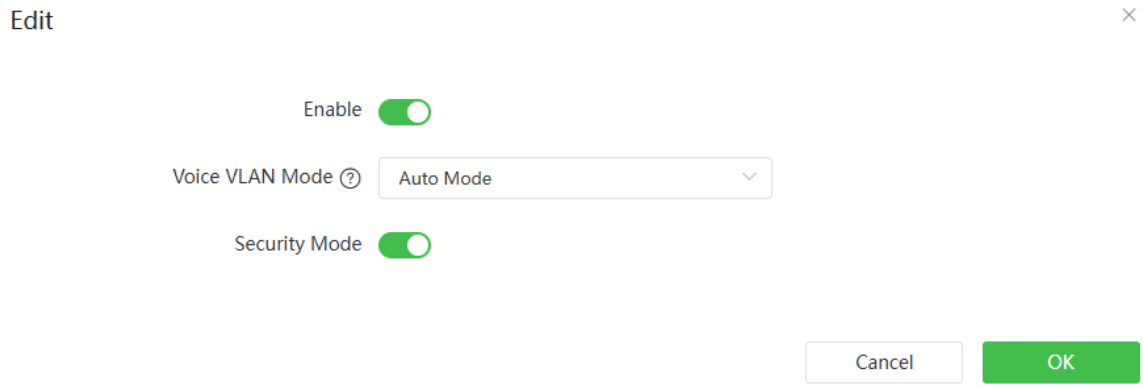


Table 11-18 Description of the Voice VLAN Configuration Parameters on a Port

Parameter	Description	Default Value
Voice VLAN Mode	Based on different ways the Voice VLAN function is enabled on the port, the Voice VLAN Mode can be Auto Mode or Manual Mode: ● **Auto Mode**: In this mode, the device checks whether the permit VLANs of a port contain the voice VLAN after the voice VLAN function is enabled on the port. If yes, the device deletes the voice VLAN from the permit VLANs of the port until the port receives a voice packet containing a specified OUI. Then, the device automatically adds the voice VLAN to the port's permit VLANs. If the port does not receive a voice packet containing the specified OUI within the global aging time, the device removes the Voice VLAN from the permit VLANs of the port. ● **Manual Mode**: If the permit VLANs of a port contains the voice VLAN, voice packets can be transmitted in the voice VLAN.	Auto Mode
Security Mode	When the security mode is enabled, only voice traffic can be transmitted in the voice VLAN. The device checks the source MAC address in each packet. When the source MAC address in the packet matches the voice VLAN OUI, the packet can be transmitted in the voice VLAN. Otherwise, the device discards the packet. When the security mode is disabled, the source MAC addresses of packets are not checked and all packets can be transmitted in the voice VLAN.	Enable

Caution

- The voice VLAN mode of the port can be set as the auto mode only when the VLAN mode of the port is Trunk mode. When the voice VLAN mode of the port work in the

auto mode, the port exits the voice VLAN first and is automatically added to the voice VLAN only after receiving voice data.

- After the voice VLAN function is enabled on a port, do not switch the Layer 2 mode (trunk or access mode) of the port to ensure normal operation of the function. If you need to switch the Layer 2 mode of the port, disable the voice VLAN function on the port first.
- It is not recommended that both voice data and service data be transmitted over the voice VLAN. If you want to transmit both voice data and service data over the voice VLAN, disable the voice VLAN function in security mode.
- The voice VLAN function is unavailable on Layer 3 ports or aggregate interfaces.

12 Diagnostics

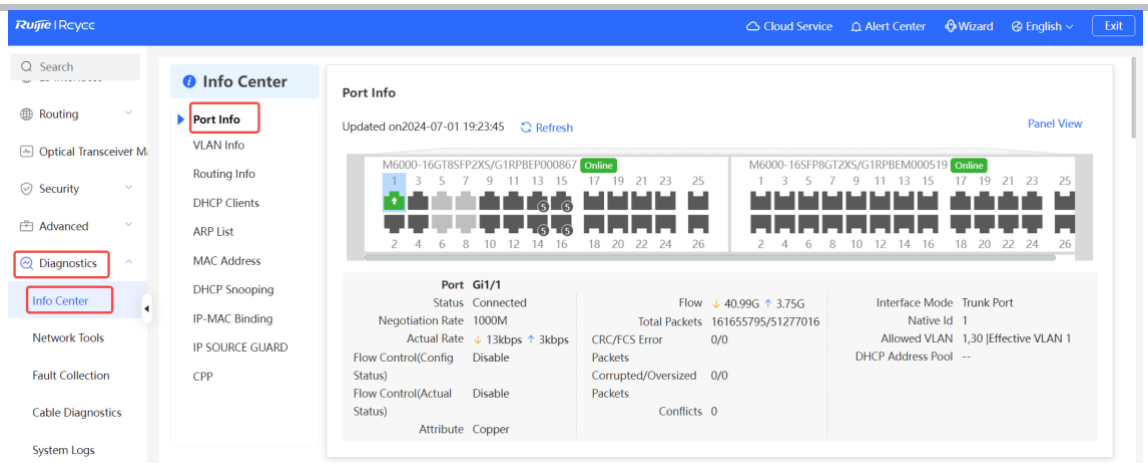
Caution

If the issue persists despite following the troubleshooting methods provided in this section, you may require remote support from a technician who will enable developer mode to resolve the issue. We will ensure your data is protected during this process.

12.1 Info Center

Choose **Local Device** > **Diagnostics** > **Info Center**.

In **Info Center**, you can view port traffic, VLAN information, routing information, client list, ARP list, MAC address, DHCP snooping, IP-MAC binding, IP Source Guard, and CPP statistics of the device and relevant configurations.



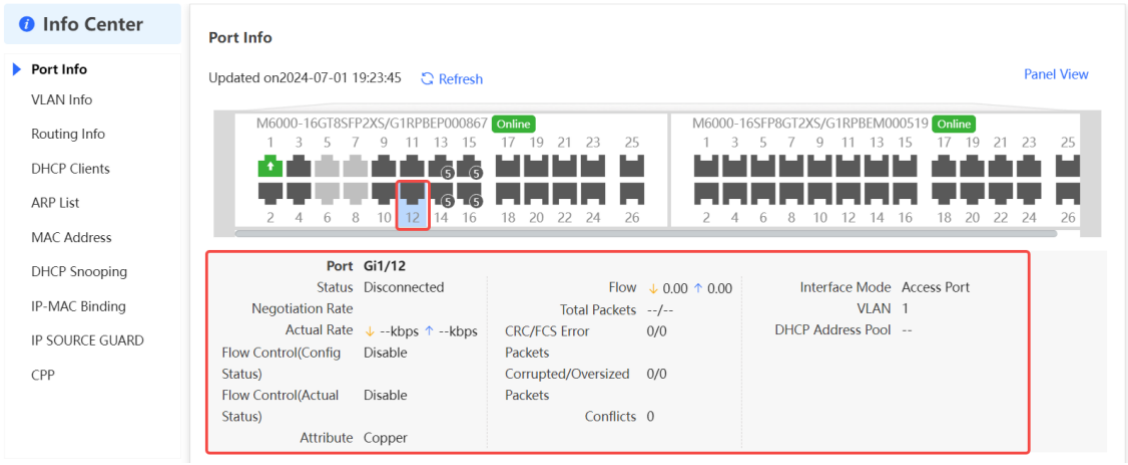
12.1.1 Port Info

Choose **Local Device** > **Diagnostics** > **Info Center** > **Port Info**.

Port Info displays the status and configuration information of the port. Click the port icon to view the detailed information of the port.

Note

- To configure the flow control of the port or the optical/electrical attribute of a combo port, see 7.2 Port Configuration.
- To configure the Layer 2 mode of the port and the VLAN to which it belongs, see 5.3 Configuring a Port VLAN.



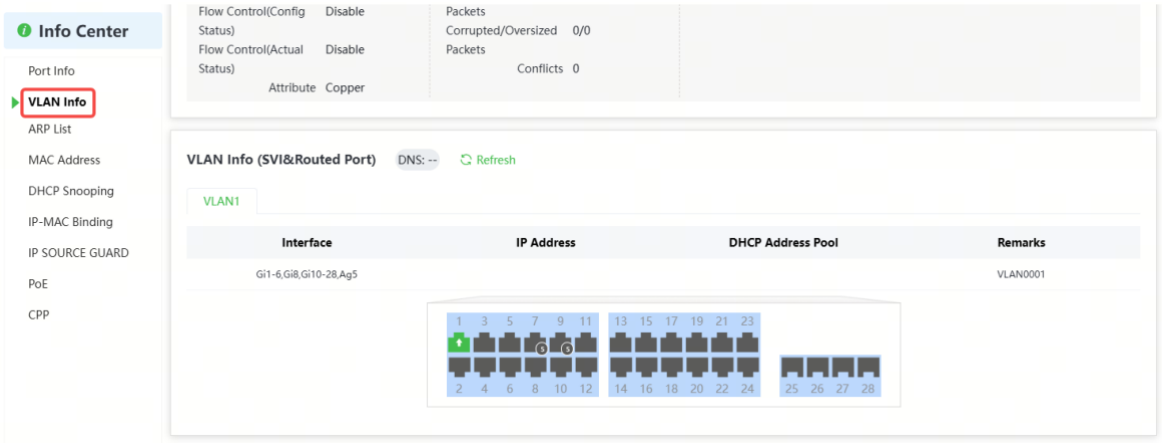
12.1.2 VLAN Info

Choose **Local Device** > **Diagnostics** > **Info Center** > **VLAN Info**.

Display SVI port and routed port information, including the port information included in the VLAN, the port IP address, and whether the DHCP address pool is enabled.

Note

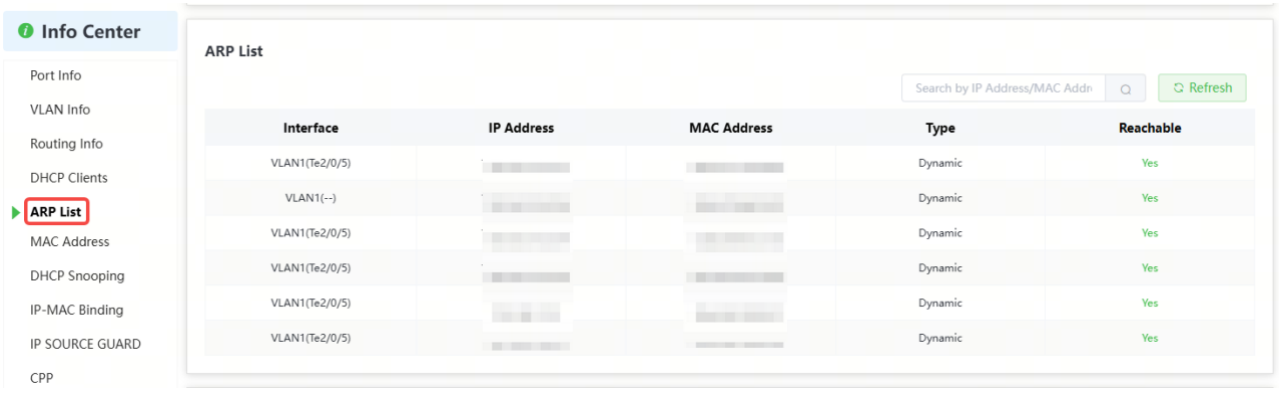
To configure VLAN, see 5 VLAN.



12.1.3 ARP List

Choose **Local Device** > **Diagnostics** > **Info Center** > **ARP List**.

The ARP List displays dynamically learned and statically configured ARP entries on the device. You can view the reachability, type, IP address, MAC address, and the physical interface corresponding to each MAC address.



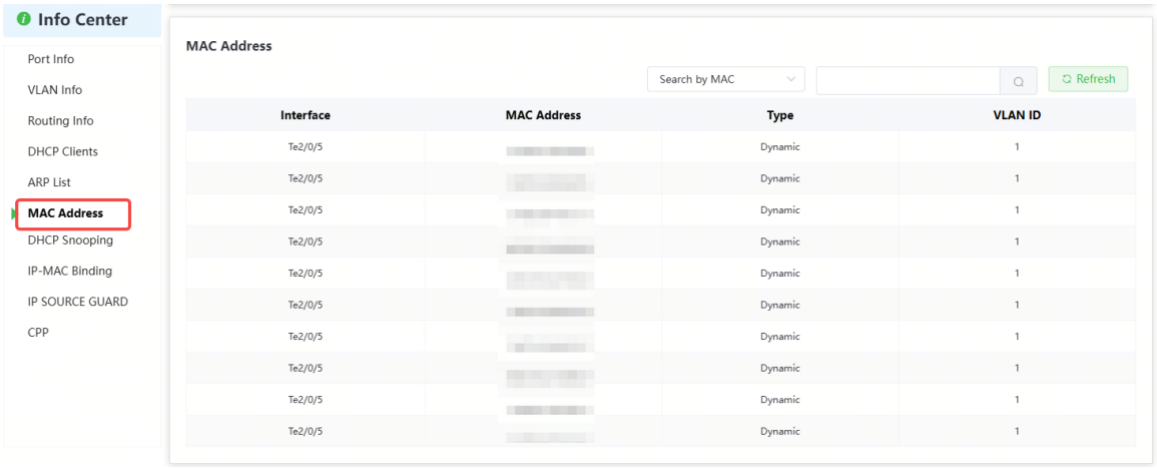
12.1.4 MAC Address

Choose **Local Device** > **Diagnostics** > **Info Center** > **MAC address**.

Displays the MAC address information of the device, including the static MAC address manually configured by the user, the filtering MAC address, and the dynamic MAC address automatically learned by the device.

Note

To configure and manage the MAC address, see 6.2 Client Management.



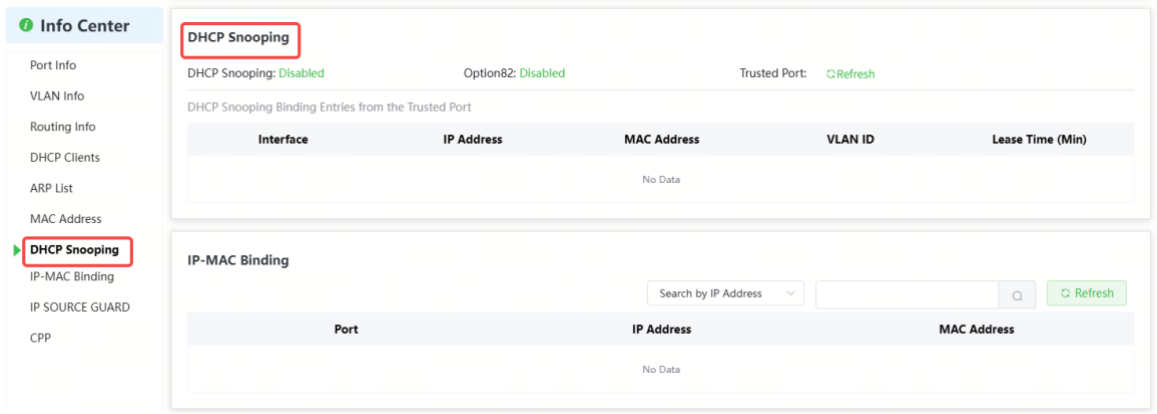
12.1.5 DHCP Snooping

Choose **Local Device** > **Diagnostics** > **Info Center** > **DHCP Snooping**.

Displays the current configuration of the DHCP snooping function and the user information dynamically learned by the trust port.

Note

To modify DHCP Snooping related configuration, see 10.1 DHCP Snooping.



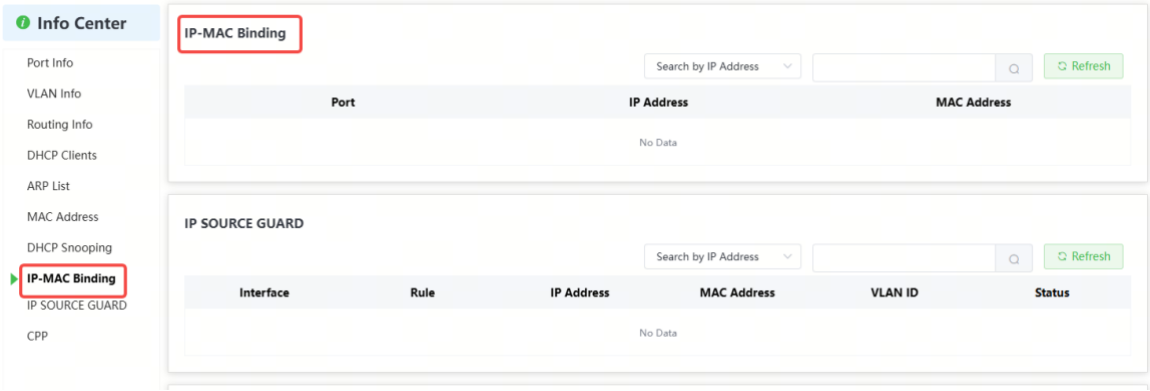
12.1.6 IP-MAC Binding

Choose **Local Device** > **Diagnostics** > **Info Center** > **IP-MAC Binding**.

Displays the configured IP-MAC binding entries. The device checks whether the source IP addresses and source MAC addresses of IP packets match those configured for the device and filters out IP packets not matching the binding.

Note

To add or modify the IP-MAC binding, see 10.5 IP-MAC Binding.



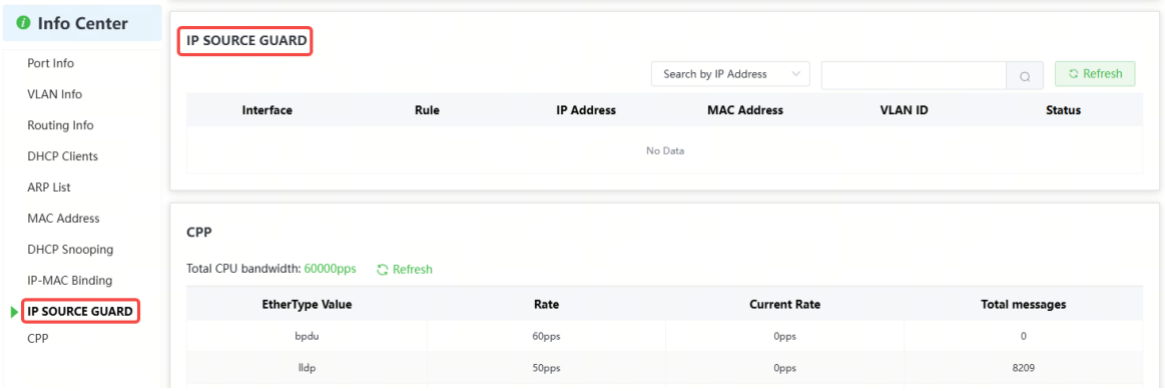
12.1.7 IP Source Guard

Choose **Local Device** > **Diagnostics** > **Info Center** > **Source Guard**.

Displays the binding list of the IP Source Guard function. The IP Source Guard function will check the IP packets from non-DHCP trusted ports according to the list, and filter out the IP packets that are not in the binding list.

Note

To configure IP Source Guard function, see 10.5 IP-MAC Binding.

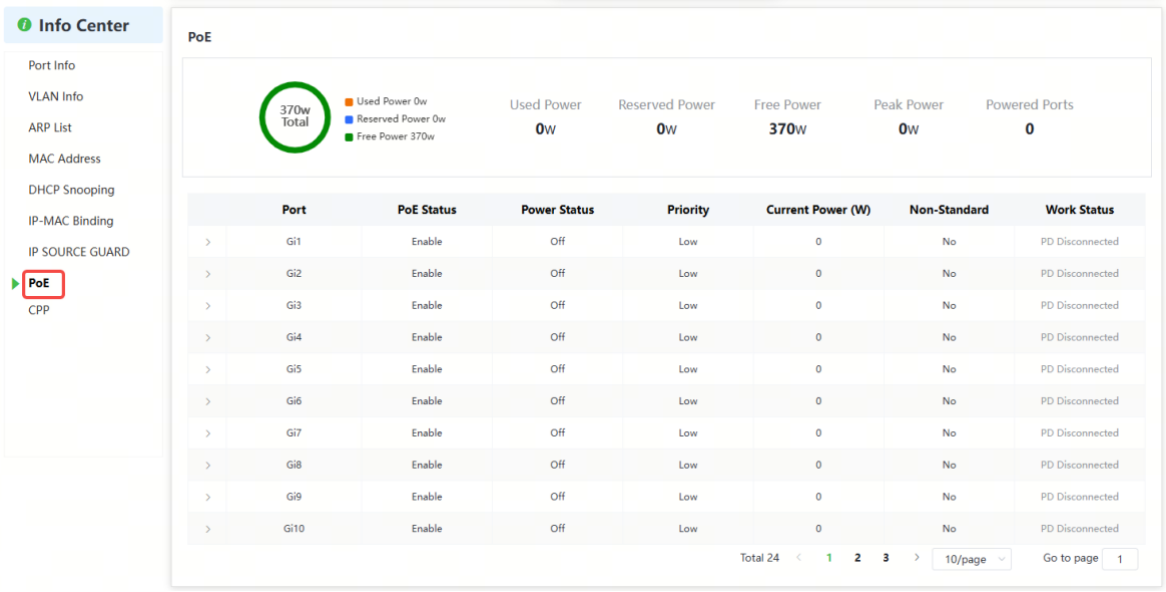


12.1.8 PoE

Specification

Only PoE switches (model name containing –P, -LP, -HP, and -UP) support this function.

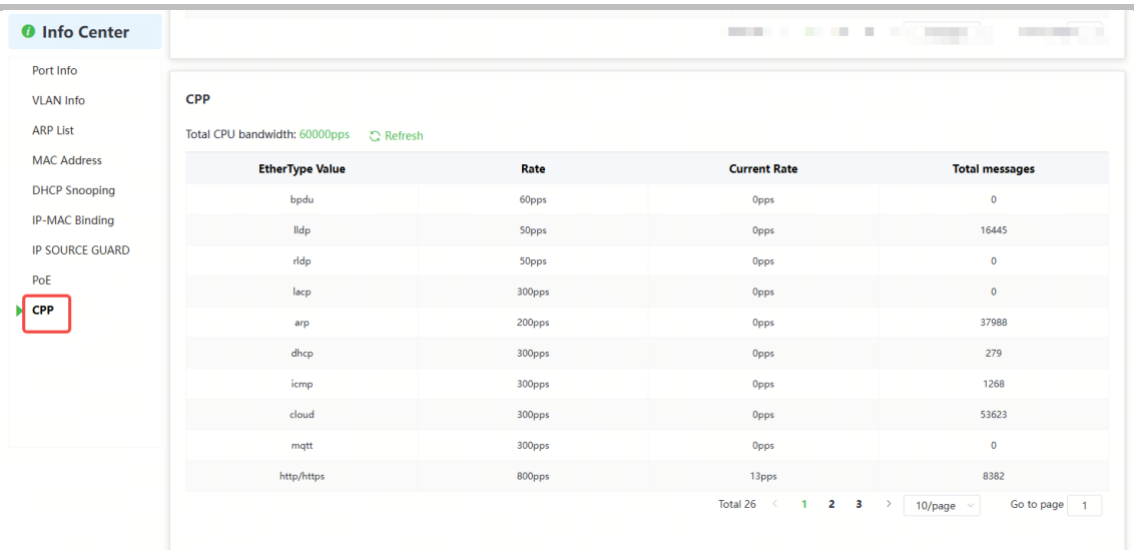
Choose **Local Device** > **Diagnostics** > **Info Center** > **PoE.**



12.1.9 CPP Info

Choose **Local Device** > **Diagnostics** > **Info Center** > **CPP**.

Displays the current total CPU bandwidth and statistics of various packet types, including the bandwidth, current rate, and total number of packets.



12.2 Network Tools

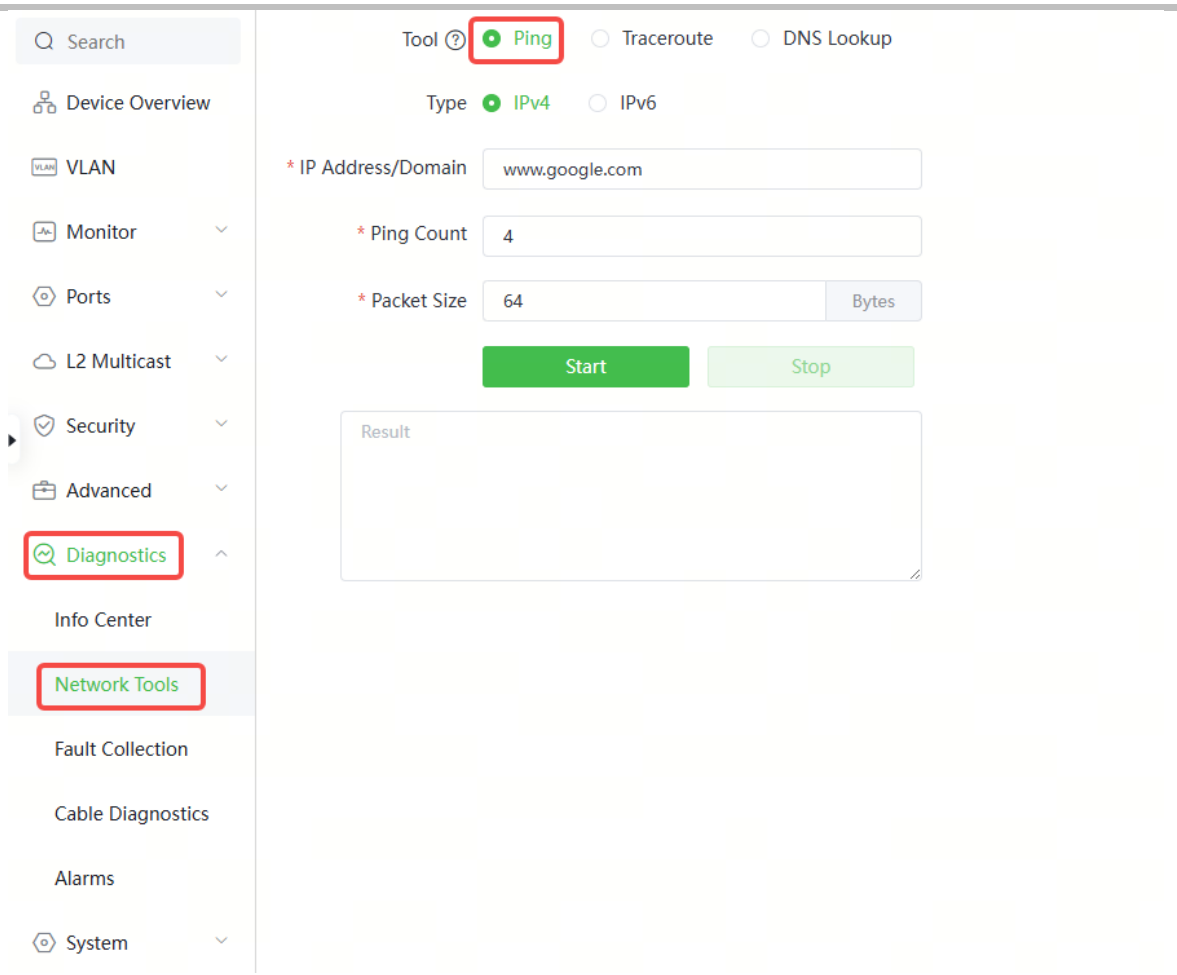
The **Network Tools** page provides three tools to detect the network status: **Ping**, **Traceroute**, and **DNS Lookup**.

12.2.1 Ping

Choose **Local Device** > **Diagnostics** > **Network Tools**.

The **Ping** command is used to detect the network connectivity.

Select **Ping** as the diagnosis mode, set **Type**, enter the destination IP address or website address, configure the ping count and packet size, and click **Start** to test the network connectivity between the device and the IP address or website. If "Ping failed" is displayed, the device is not reachable to the IP address or website.

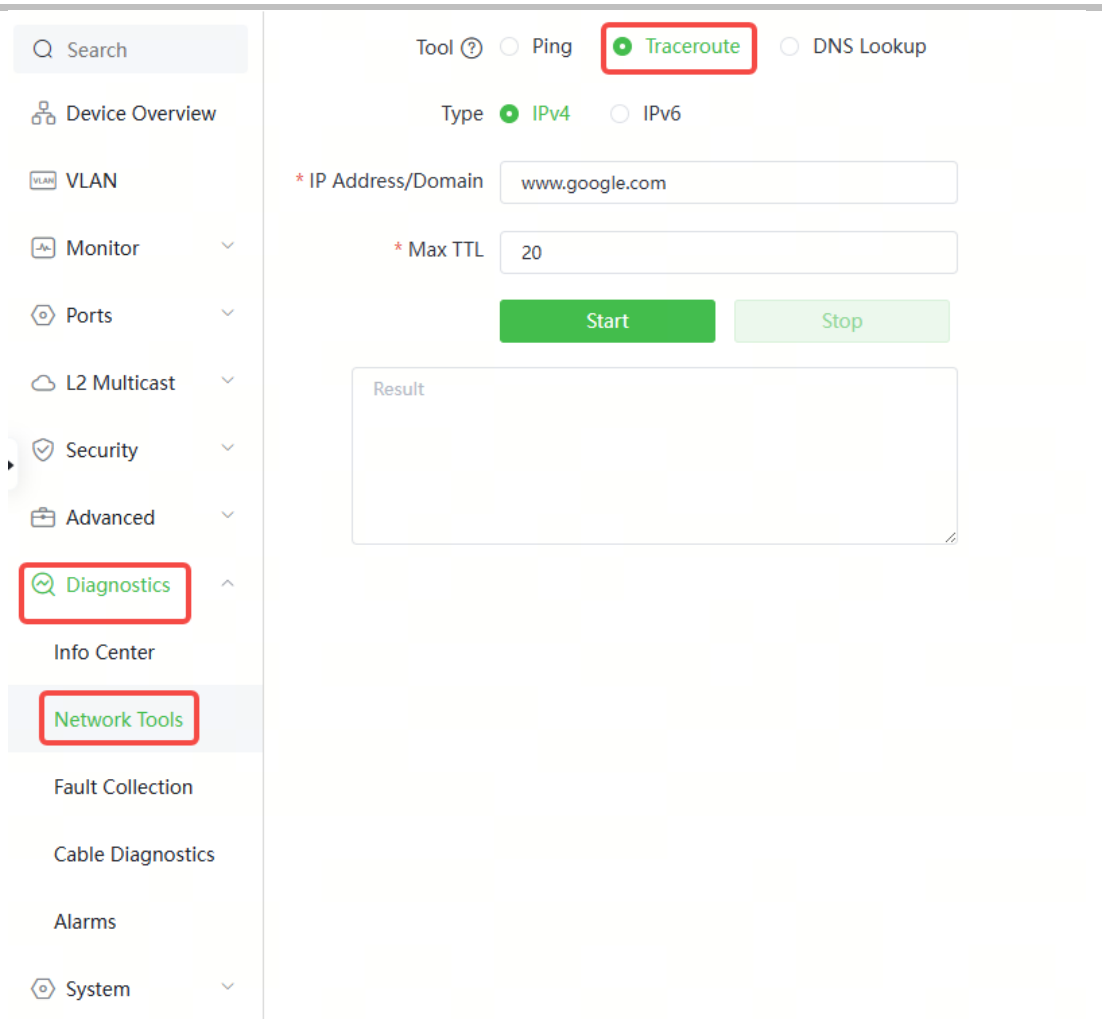


12.2.2 Traceroute

Choose **Local Device** > **Diagnostics** > **Network Tools**.

The **Traceroute** function is used to identify the network path from one device to another. On a simple network, the network path may pass through only one routing node or none at all. On a complex network, packets may pass through dozens of routing nodes before reaching their destination. The traceroute function can be used to judge the transmission path of data packets during communication.

Select **Traceroute** as the diagnosis mode, set **Type**, enter the destination IP address or website address, configure the maximum TTL value used by the traceroute, and click **Start**.

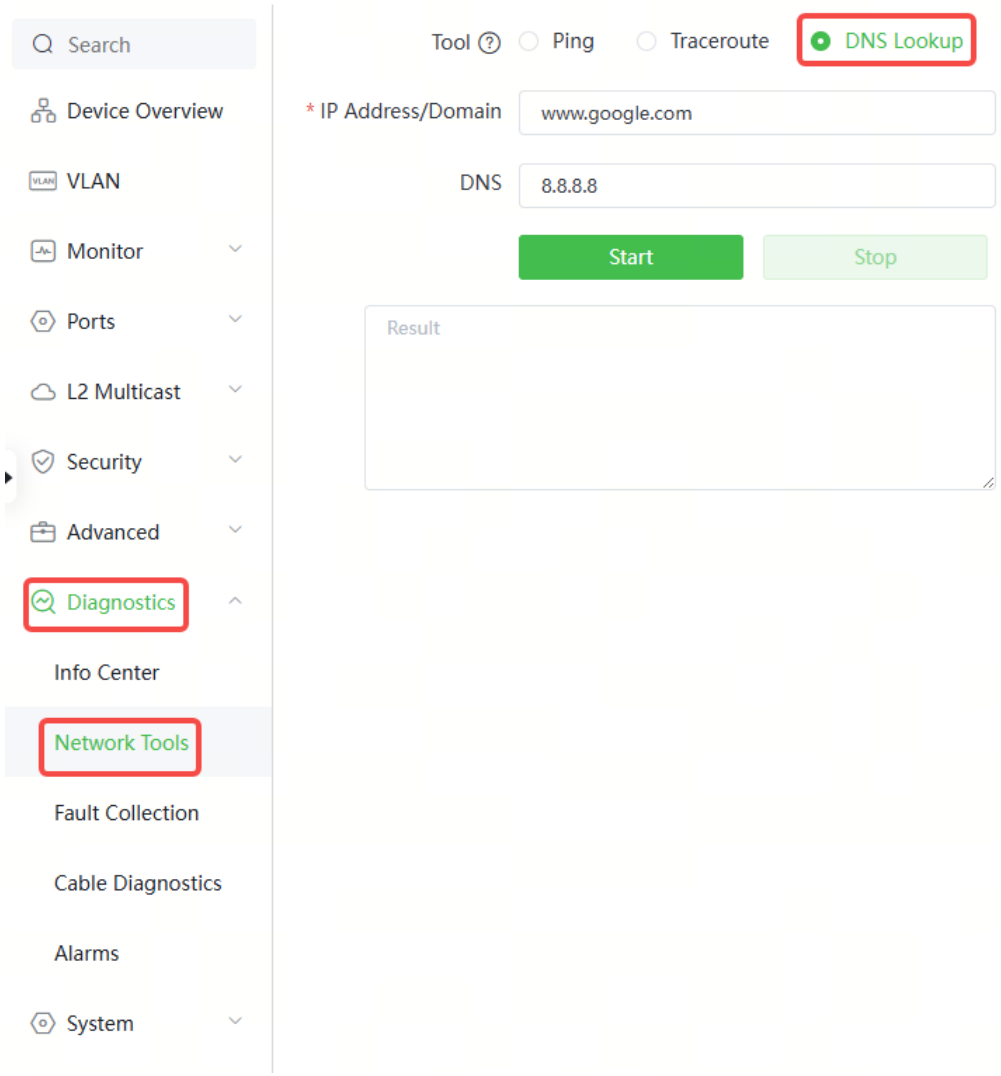


12.2.3 DNS Lookup

Choose **Local Device** > **Diagnostics** > **Network Tools**.

DNS Lookup is used to query the information of network domain name or diagnose DNS server problems. If the device can ping through the IP address of the Internet from your web page but the browser cannot open the web page, you can use the DNS lookup function to check whether domain name resolution is normal.

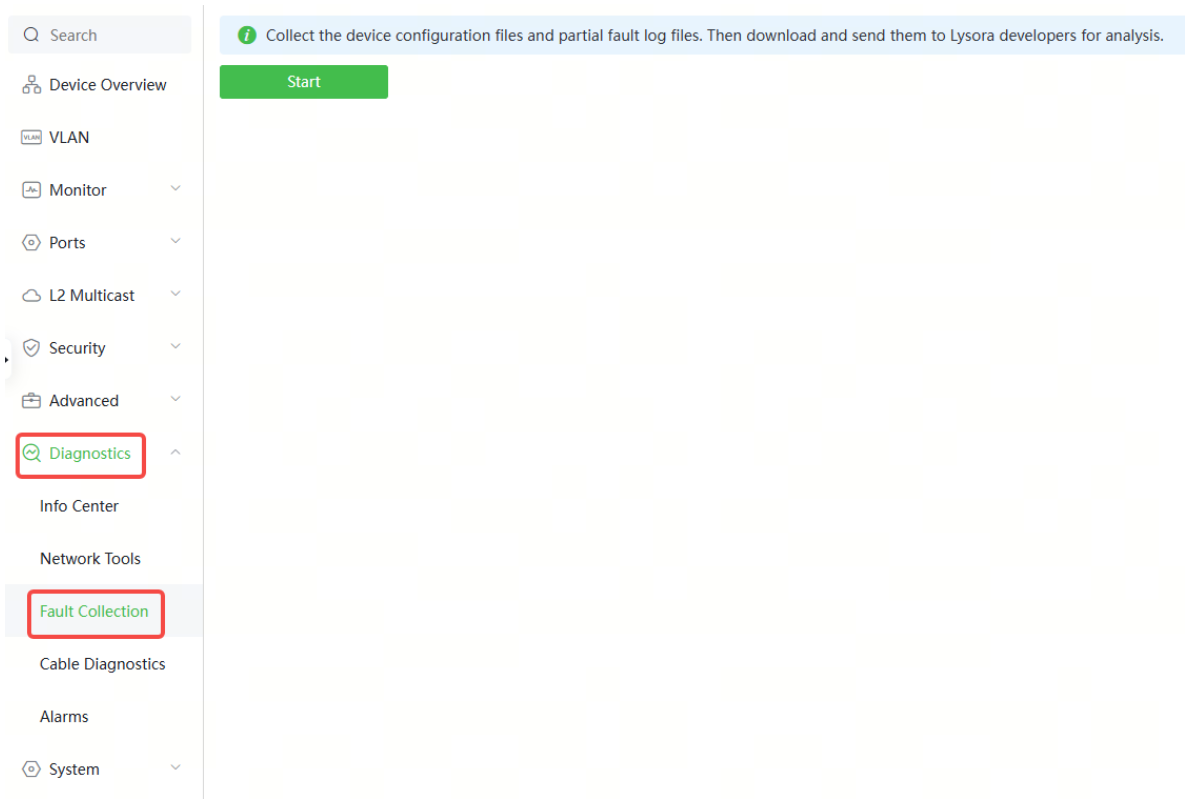
Select **DNS Lookup** as the diagnosis mode, enter a destination IP address or URL, configure the DNS server address, and click **Start**.



12.3 Fault Collection

Choose **Local Device** > **Diagnostics** > **Fault Collection.**

When an unknown fault occurs on the device, you can collect fault information by one click on this page. Click **Start**. The configuration files of the device will be packed into a compressed file. Download the compressed file locally and provide it to R&D personnel for fault locating.

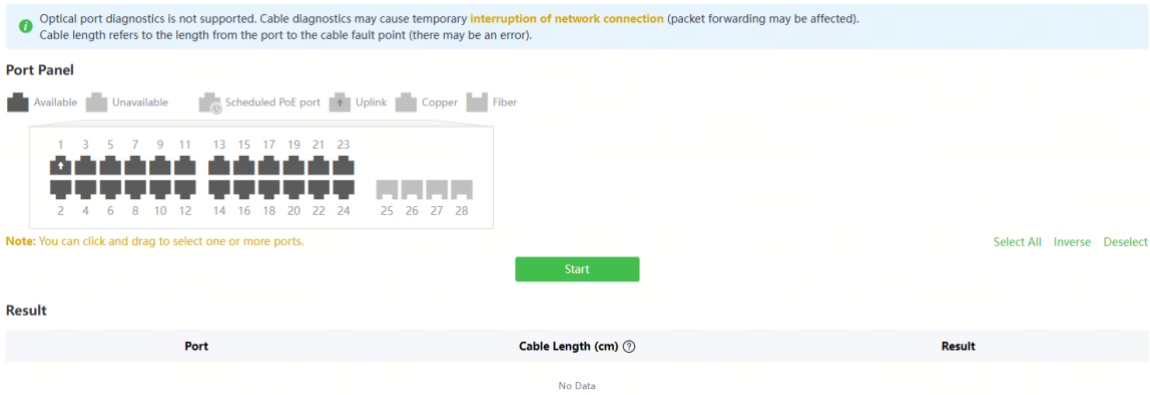


12.4 Cable Diagnostics

Choose **Local Device** > **Diagnostics** > **Cable Diagnostics**.

The cable diagnostics function can detect the approximate length of a cable connected to a port and whether the cable is faulty.

Select the port to be detected on the port panel and click **Start**. The detection results will be displayed below.



Caution

- The SFP port does not support the function.
- If a detected port contains an uplink port, the network may be intermittently disconnected. Exercise caution when performing this operation.

12.5 Alerts

Choose **Local Device** > **Diagnostics** > **Alerts**.

Note

Click an alert in the **Alert Center** to view the faulty device, problem details, and description.

Displays possible problems on the network environment to facilitate fault prevention and troubleshooting. You can view the alert occurrence time, port, alert impact, and handling suggestions, and rectify device faults according to handling suggestions.

All types of alerts are concerned by default. You can click **Unfollow** to unfollow this type of alert. The system will no longer display this type of alert. To enable the notification function of a type of alert again, follow the alert type on the **Removed Alert** page.

Caution

After unfollowing an alert, the system will not issue an alert prompt for this type of fault, and users cannot find and deal with the fault in time. Exercise caution when performing this operation.

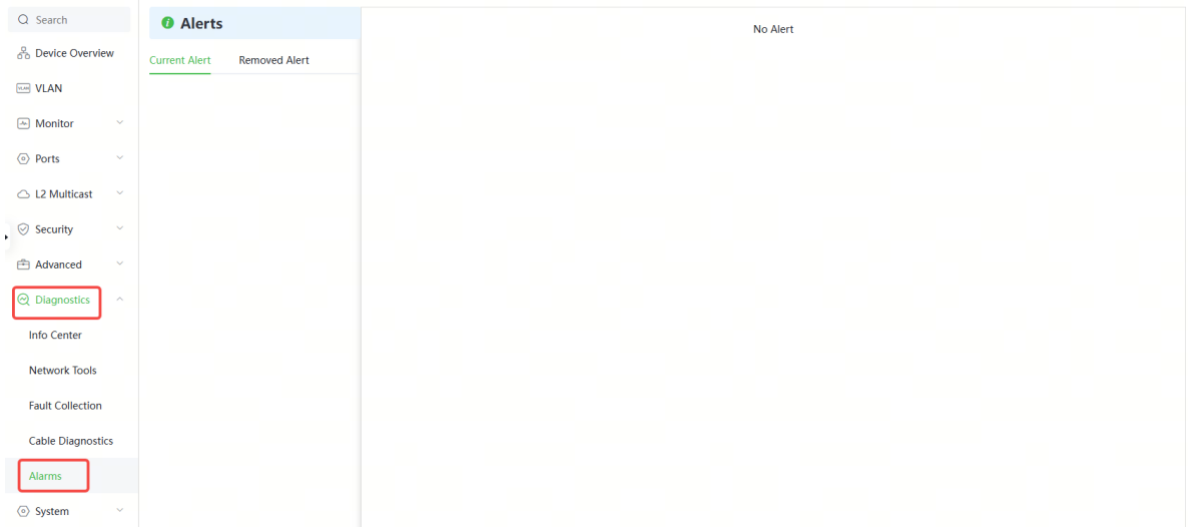


Table 12-1Alert Types and Product Support

Alert Type	Description	Support Description
Addresses in the DHCP address pool are to be exhausted.	The device acts as a DHCP server, and the number of allocated addresses is about to reach the maximum number of addresses that can be allocated in the address pool.	It is applicable only to devices that support Layer 3 functions.
The IP address of the local device conflicts with that of another device.	The IP address of the local device conflicts with that of another client on the LAN.	N/A
An IP address conflict occurs on downlink devices connected to the device.	Among the devices connected to the current device on the LAN, an IP address conflict occurs on one or more devices.	N/A

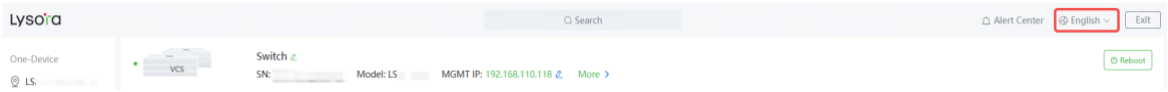
Alert Type	Description	Support Description
The MAC address table is full of entries.	The number of Layer 2 MAC address entries is about to reach the hardware capacity limit of the product.	N/A
The ARP table is full of ARP entries.	The number of ARP entries on the network exceeds the ARP capacity of the device.	N/A
The PoE process is not running.	The PoE service of the device fails and no power can be supplied.	It is applicable only to switches that support the PoE function. (The device models are marked with "-P".)
The total PoE power is overloaded.	The total PoE power of the device is overloaded, and the new connected PD cannot be powered properly.	It is applicable only to switches that support the PoE function. (The device models are marked with "-P".)
The device has a loop alarm.	A network loop occurs on the LAN.	N/A

13 System Configuration

13.1 Changing the Web Page Language

Click **English** in the top right corner of the web page.

Select the desired language from the dropdown menu to change the language of the web page.



13.2 System Logs

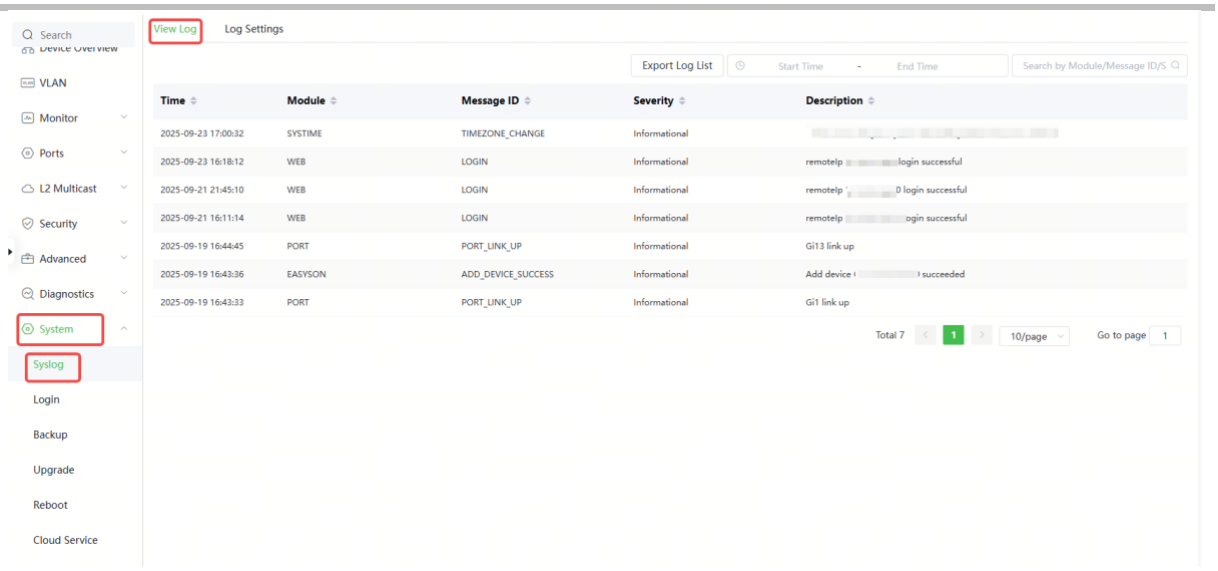
On medium- and large-sized network projects, the network administrator usually uses third-party software to connect to all devices, monitor each data indicator of the system, and determine whether any abnormal behavior exists, thereby securing the system. The devices typically run network management protocols, such as Simple Network Management Protocol (SNMP) and Syslog, to connect to third-party software.

13.2.1 Viewing logs

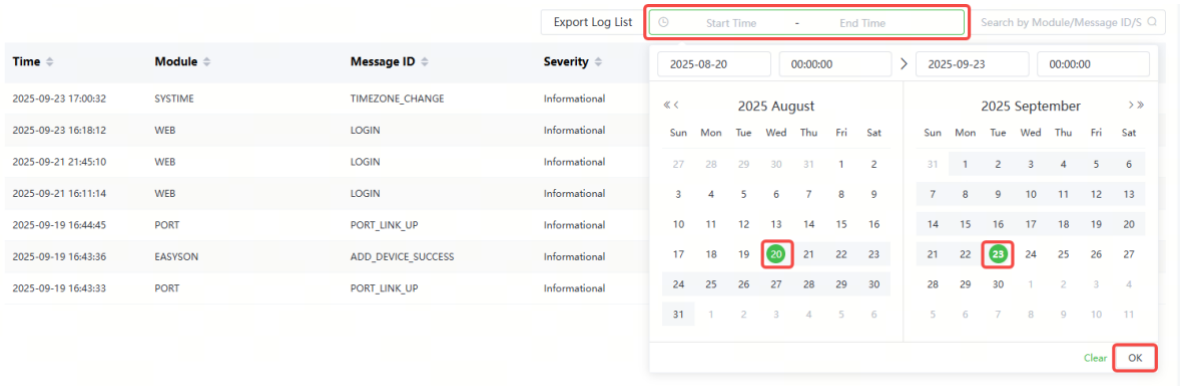
Choose **Network Wide** > **System** > **Syslog** > **View Log**.

Choose **Local Device** > **System** > **Syslog** > **View Log**.

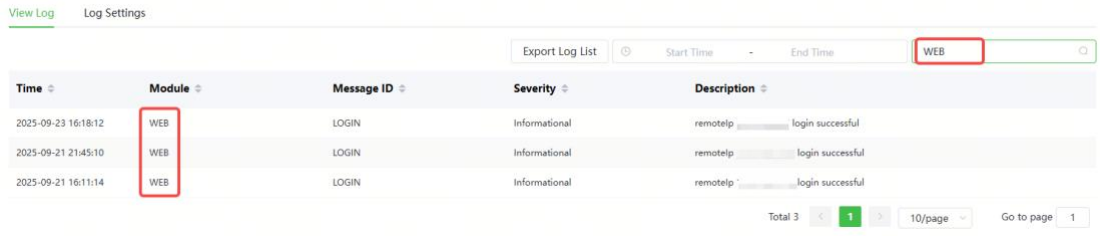
The log list displays the operation logs of the local device. On the **View Log** page, you can specify a duration or module to view logs, or export the log list and log file to the local device for backup or viewing.



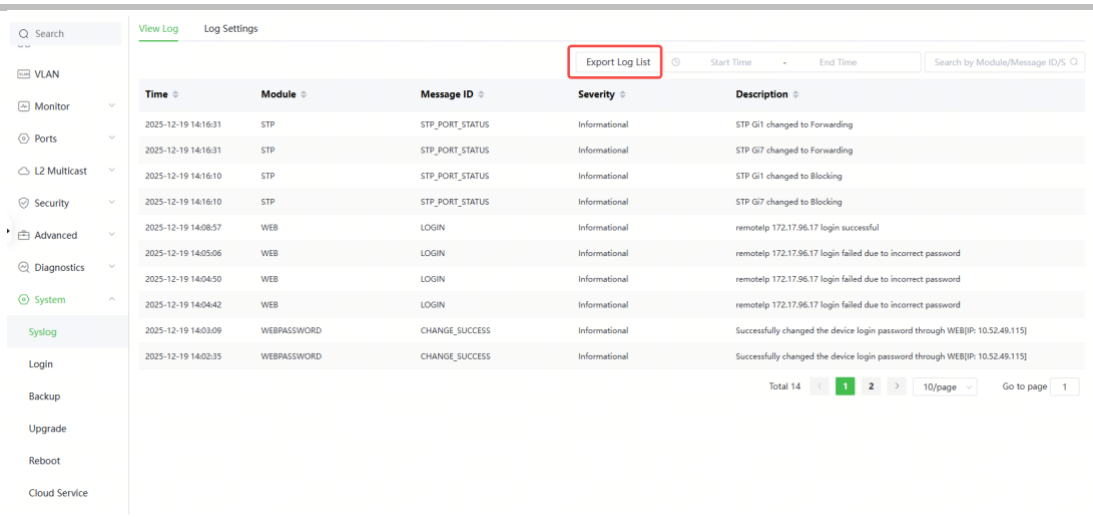
- View logs in a specified duration. Click **Start Time**, select the start and end dates, and click **OK** to filter logs by date.



- View logs of a specified module. Enter a module name in the search box to view the operation logs of a specified module.

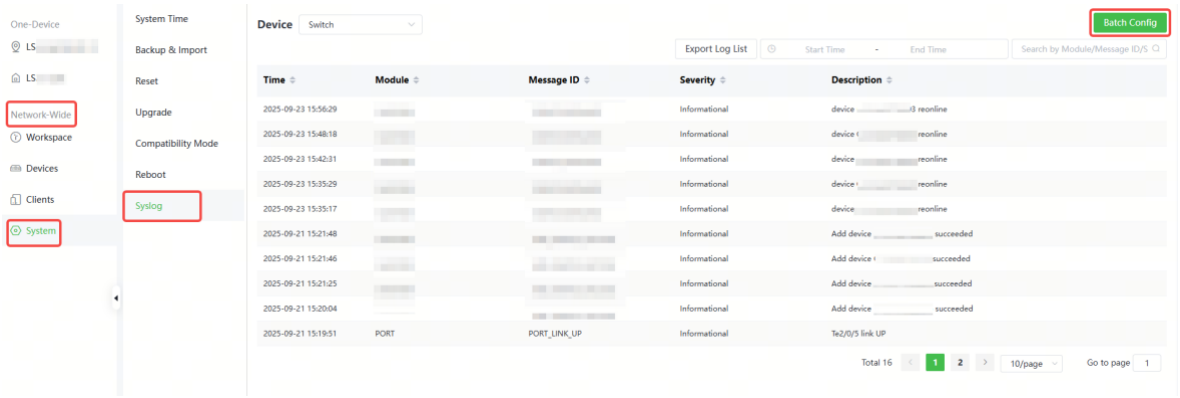


- Export the log list. Click **Export Log List** to download the log list in .csv format to the local device for viewing.

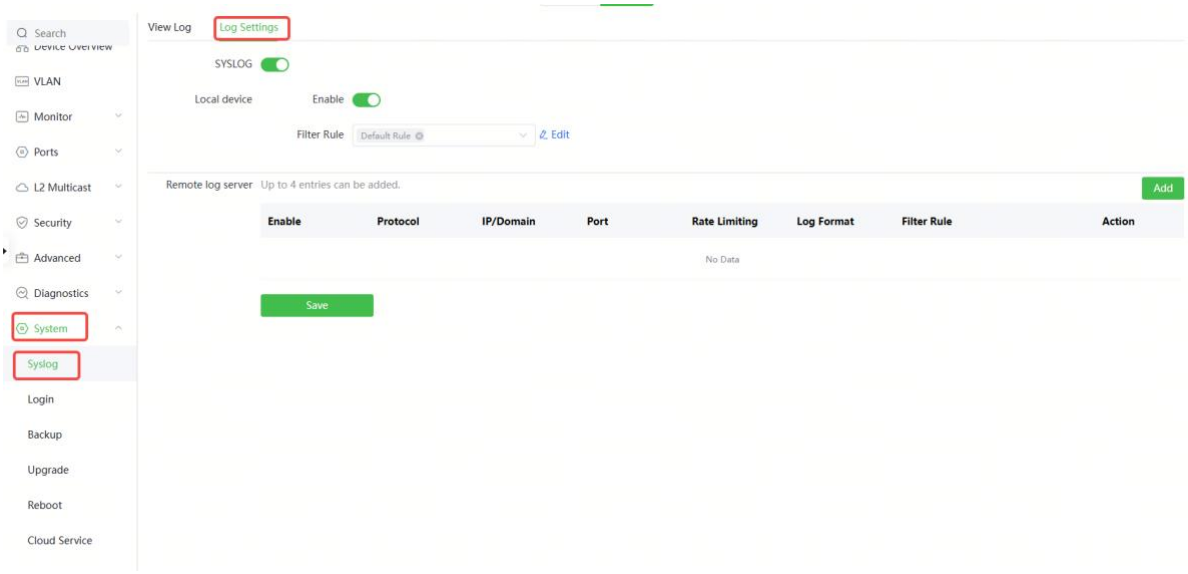


13.2.2 Setting Logs

Method 1: Choose **Network-Wide** > **System** > **Syslog**. Click **Batch Config.**

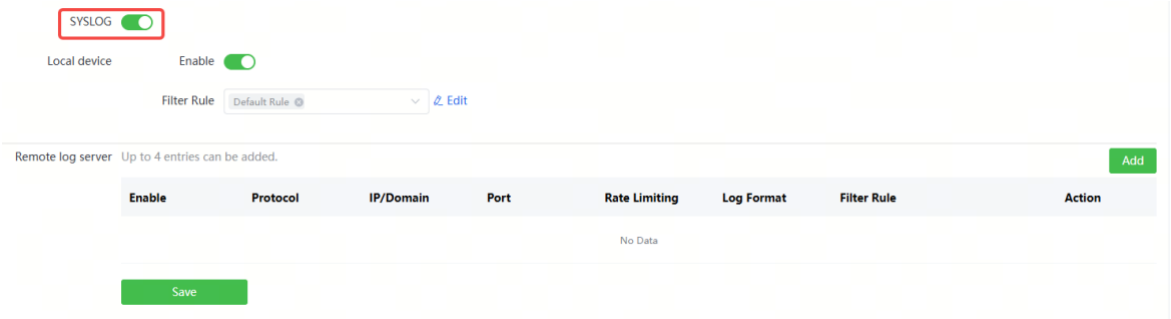


Method 2: Choose **Local Device** > **System** > **Syslog** > **Log Settings**.



1. Enabling Syslog

After **SYSLOG** is enabled, the switch can interconnect with the remote log server through Syslog and send log information to the remote log server over the network.

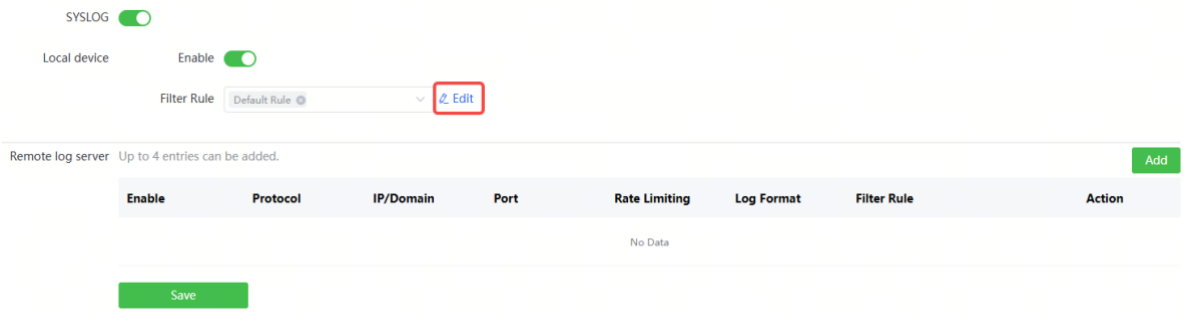


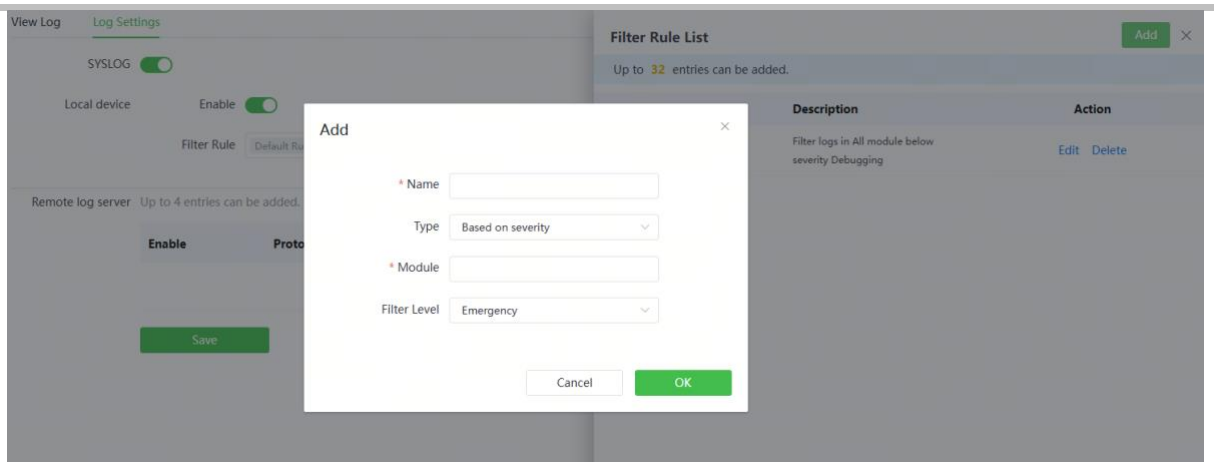
2. Configuring Local Logs

The log storage of the local device is enabled by default. Click **Edit**, and then click **Add** to add a filtering rule for the device operation logs. For example, you can filter the debugging information of all modules to prevent them from being displayed in the log list.

Caution

If the logging function of the local device is disabled, no operation performed on the device will be displayed in the log list. Exercise caution when disabling log storage of the local device.





3. Configuring the Remote Log Server

Click **Add** next to a remote server to add the basic information of the remote server.

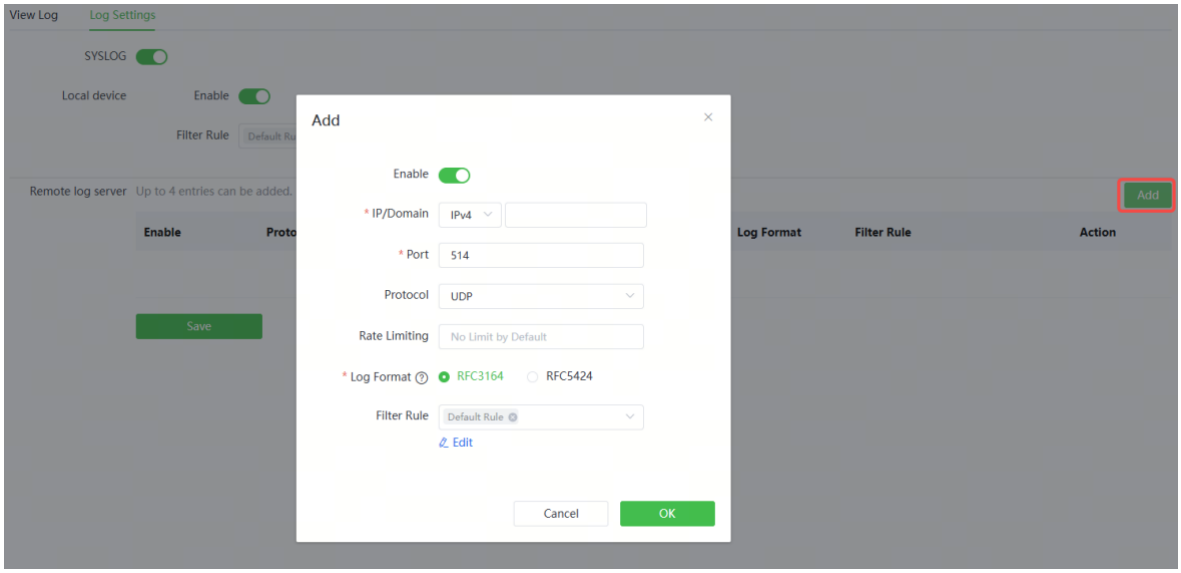


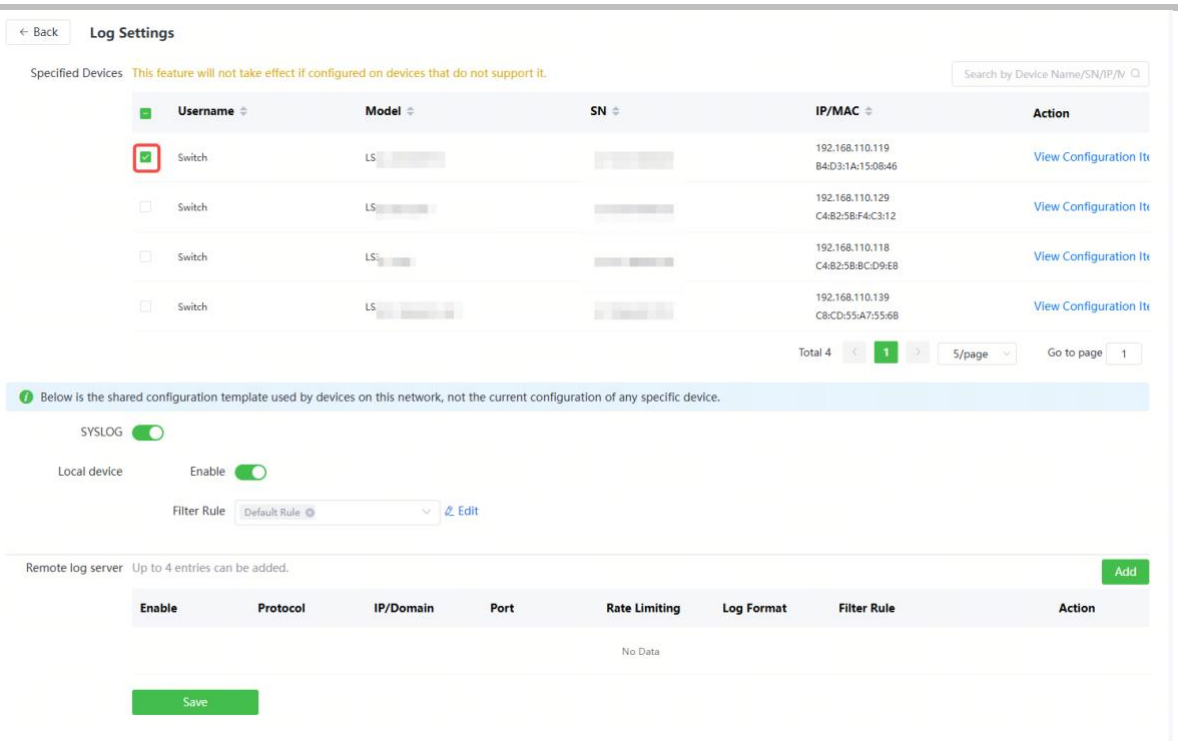
Table 13-1Description of Configuring Remote Server Parameters

Parameter	Description	Default Value
Enable	Whether to enable the remote server. If so, the device will send the operation logs of the local device to the remote server.	Enabled by default.
IP Address	IP address of the remote server. An IPv4 or IPv6 address can be entered.	N/A

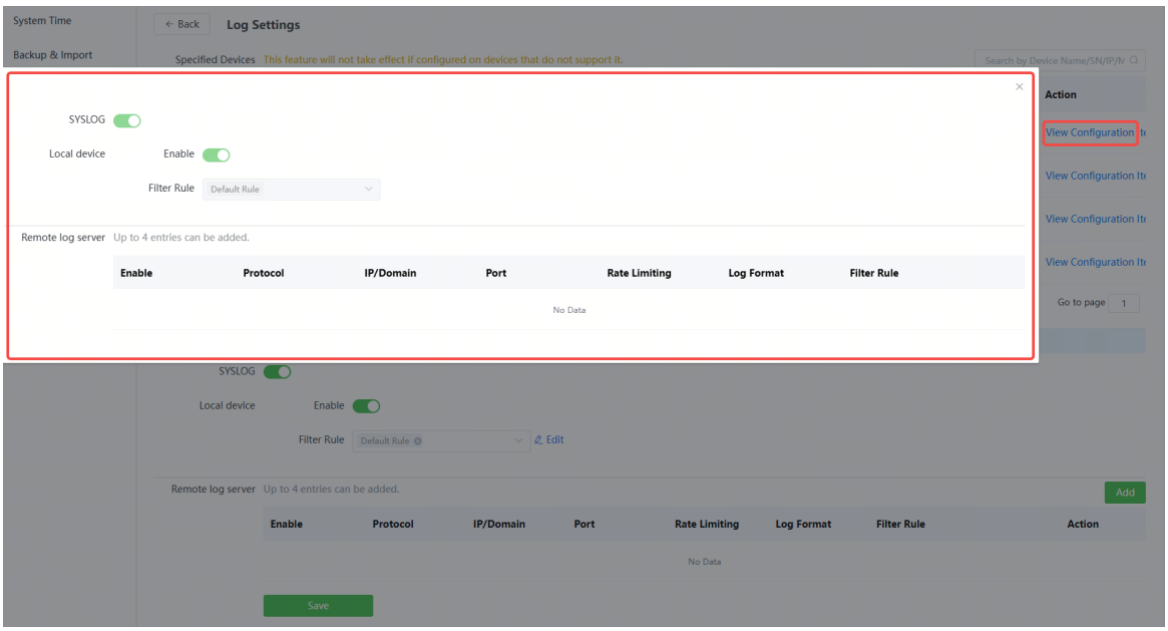
Parameter	Description	Default Value
Port	Port number of the remote server.	N/A
Protocol	Protocols used by the device to communicate with a remote server. Currently, only UDP is supported.	UDP by default.
Rate Limiting	Maximum transmission rate used by the device to send log information to the remote server.	No rate limit by default.
Log Format	Format of device logs sent to the remote log server. ● RFC3164: <Priority> Local time in seconds Host name Module name%message identifier: Log content ● RFC5424: <Priority> UTC time in microseconds Host name Module name Process ID Message flag - Log content	RFC3164
Filter Rule	Filtering rules for device operation logs. The operation logs that are filtered out will not be sent to the log server.	N/A

4. Batch Configuration

On the **Log Settings** page in Network-Wide mode, select the targeted devices and configure the log settings. Then, click **Save** to apply the settings to the selected devices.

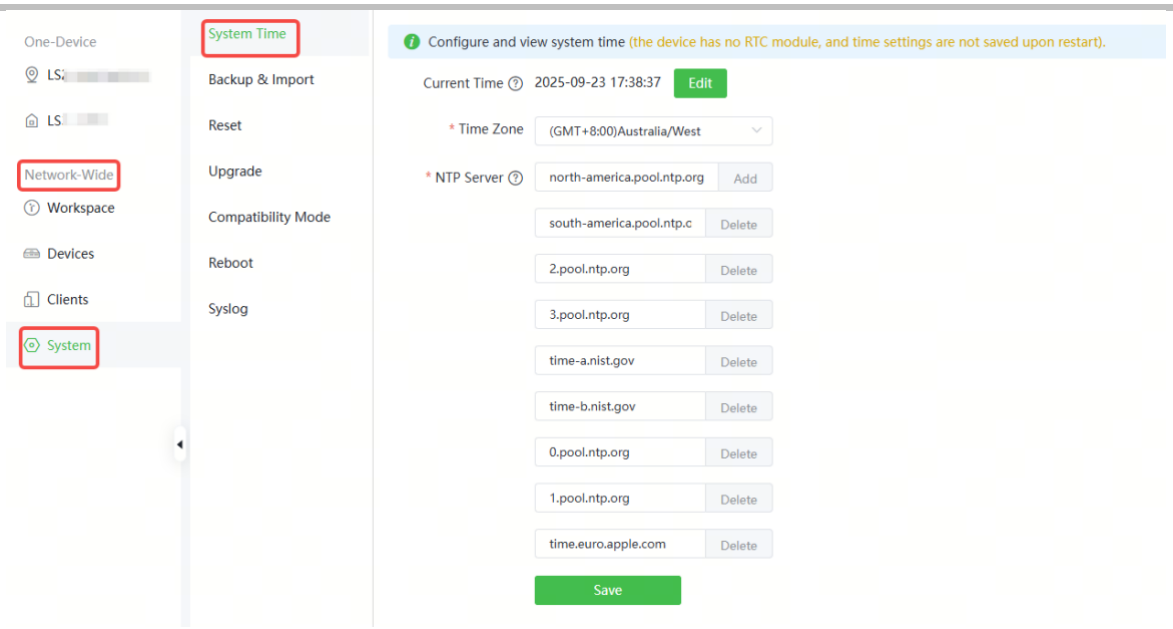


After the log settings are successfully applied, click **View Configuration** to view the log settings of individual devices.

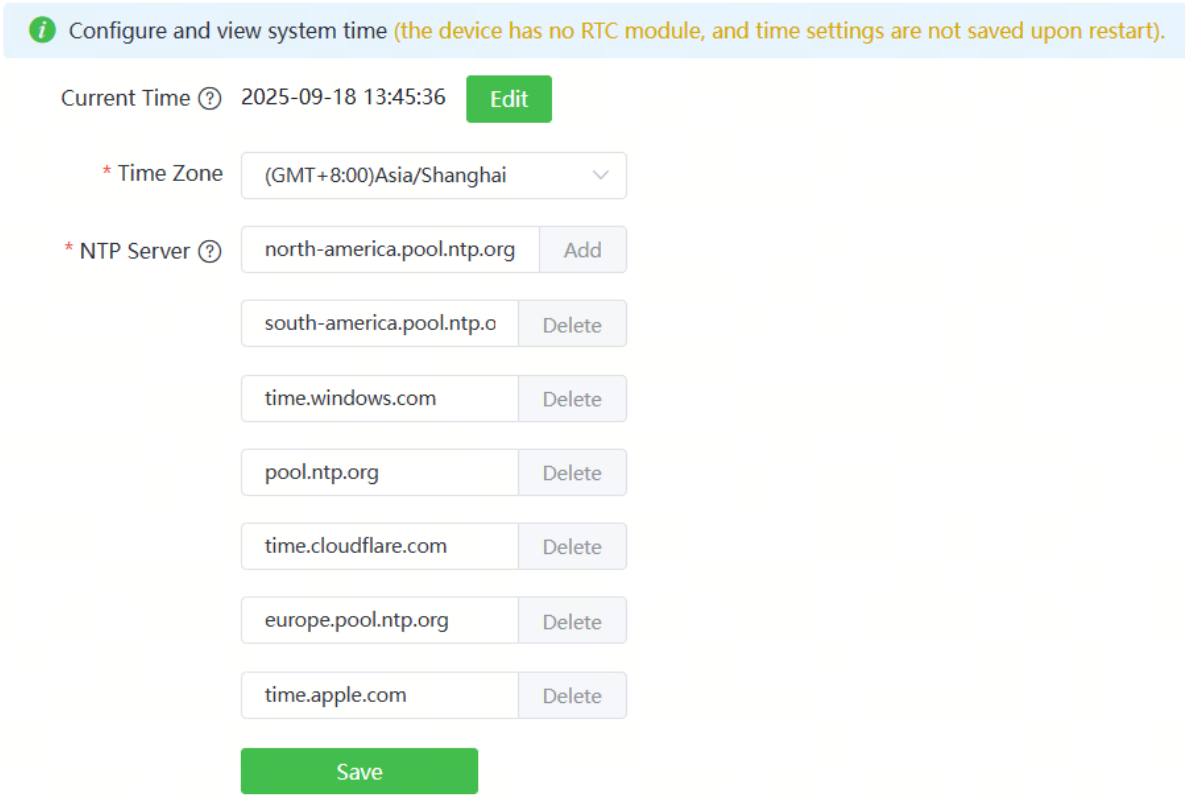


13.3 Setting the System Time

Method 1: Choose **Network-Wide** > **System** > **System Time**.



Method 2: Choose **Local Device** > **System** > **System Time**.



You can view the current system time. If the time is incorrect, check and select the local time zone. If the time zone is correct but time is still incorrect, click **Edit** to manually set the time. In addition, the device supports Network Time Protocol (NTP) servers. By

default, multiple servers serve as the backup of each other. You can add or delete the local server as required.

Click **Current Time** when modifying the time, and the system time of the currently logged-in device will be automatically filled in.

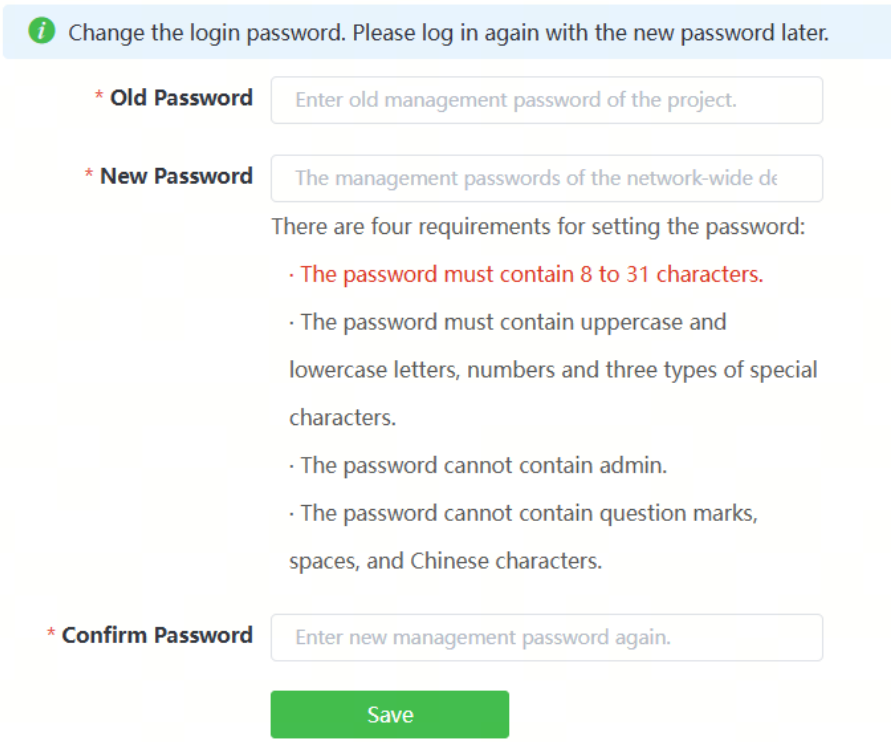
13.4 Setting the Web Login Password

Choose **Local Device** > **System** > **Login** > **Password**.

Enter the old password and new password. After saving the configuration, use the new password to log in.

Caution

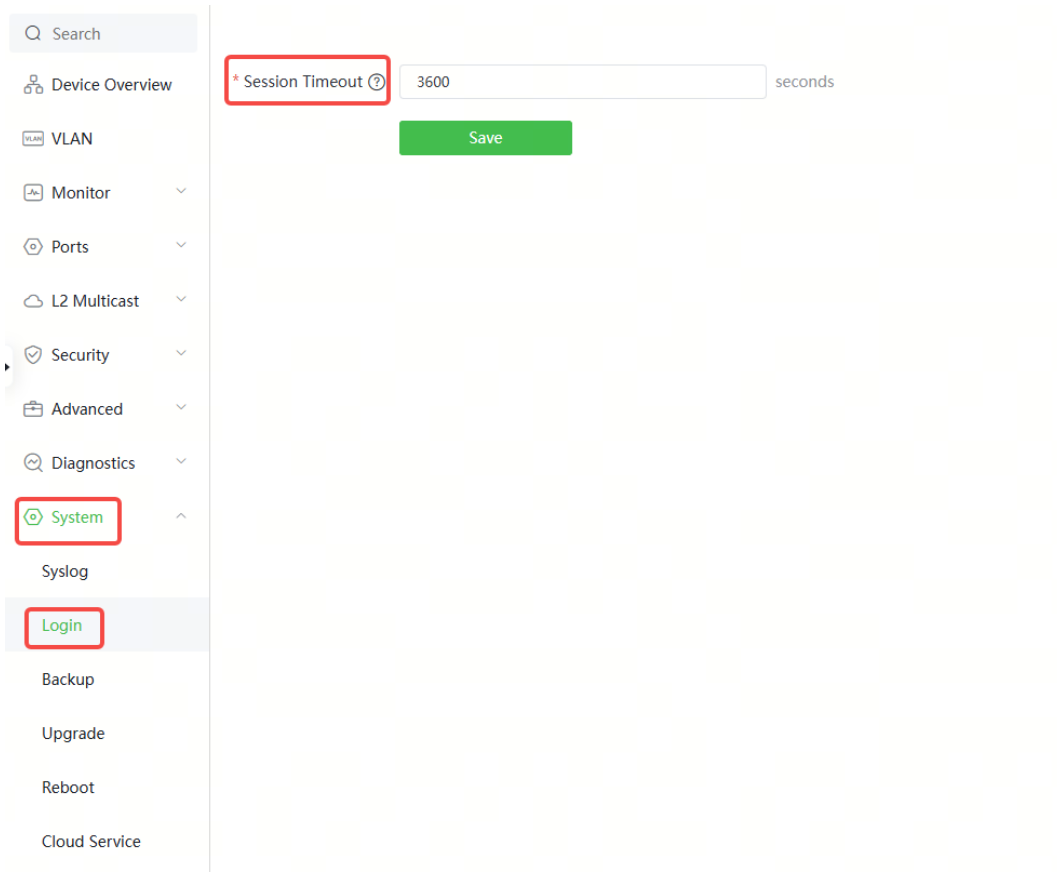
When self-organizing network discovery is enabled, the login password of all devices in the network will be changed synchronously.



13.5 Setting the Session Timeout Duration

Choose **Local Device** > **System** > **Login** > **Session Timeout**.

If you do not log out after login, the web page allows you to continue the access without authentication on the current browser within one hour by default. After one hour, the web page automatically refreshes the page and you need to relog in before continuing your operations. You can change the session timeout duration.



13.6 Configuring SNMP

13.6.1 Overview

The Simple Network Management Protocol (SNMP) is a protocol for managing network devices. Based on the client/server model, it can achieve remote monitoring and control of network devices.

SNMP uses a manager and agent architecture. The manager communicates with agents through the SNMP protocol to retrieve information such as device status, configuration details, and performance data. It can also be used to configure and manage devices.

SNMP can be used to manage various network devices, including routers, switches, servers, firewalls, etc. You can achieve user management through the SNMP configuration interface and monitor and control devices through the third-party software.

13.6.2 Global Configuration

1. Overview

The purpose of global configuration is to enable the SNMP service and make the SNMP protocol version (v1/v2c/v3) take effect, so as to achieve basic configuration of local port, device location, and contact information.

SNMP v1: As the earliest version of SNMP, SNMP v1 has poor security, and only supports simple community string authentication. SNMP v1 has certain flaws, such as plaintext transmission of community strings and vulnerability to attacks. Therefore, SNMP v1 is not recommended for modern networks.

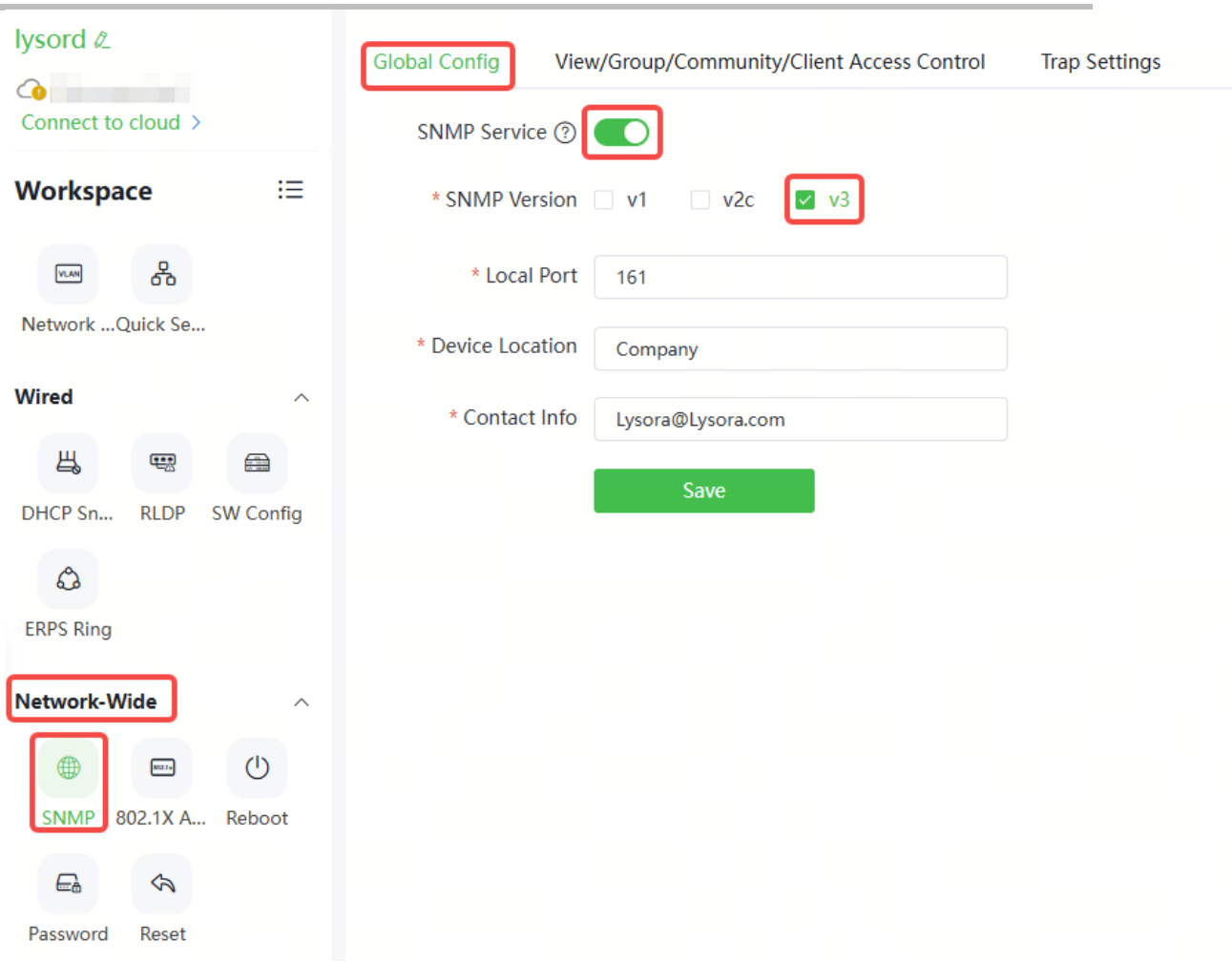
SNMP v2c: As an improved version of SNMP v1, SNMP v2c supports richer functions and more complex data types, with enhanced security. SNMP v2c performs better than SNMP v1 in terms of security and functionality, and is more flexible. It can be configured according to different needs.

SNMP v3: As the newest version, SNMP v3 supports security mechanisms such as message authentication and encryption compared to SNMP v1 and SNMP v2c. SNMP v3 has achieved significant improvements in security and access control.

2. Configuration Steps

Choose **Workspace** > **Network-wide** > **SNMP** > **Global Config**.

(1) Enable the SNMP service.



When it is enabled for the first time, SNMP v3 is enabled by default. Click **OK**.

(2) Set SNMP service global configuration parameters.

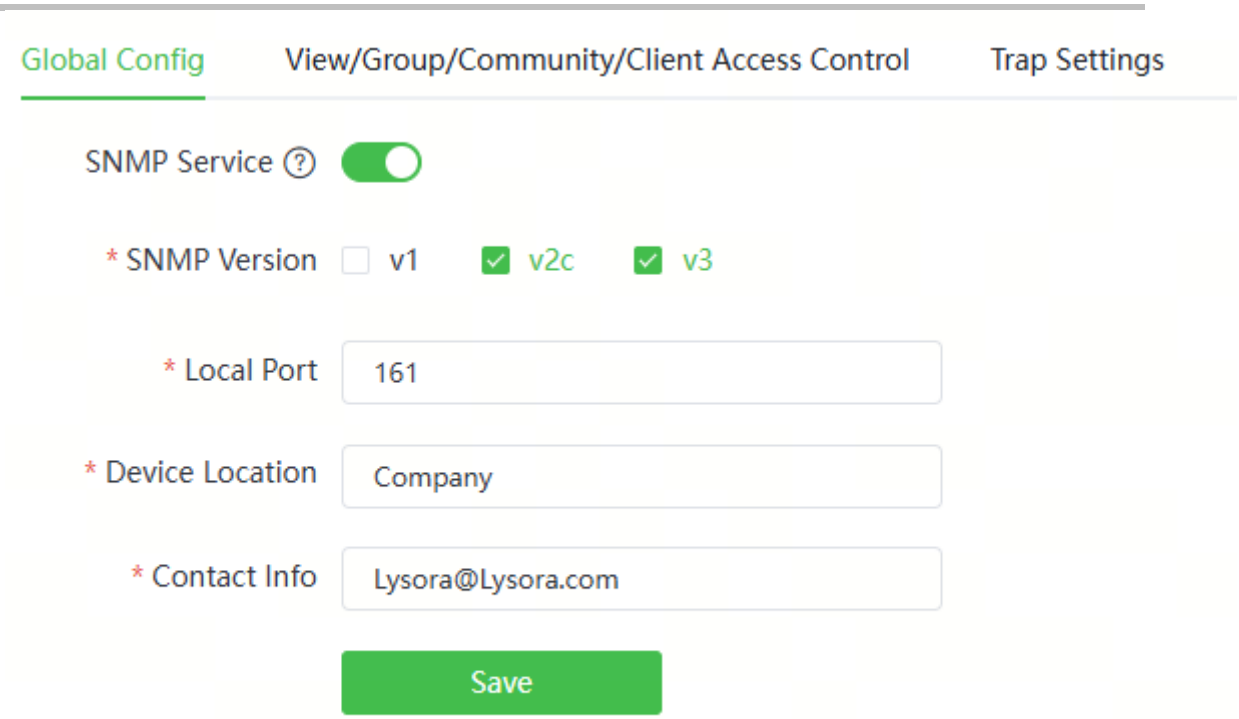


Table 13-2Global Configuration Parameters

Parameter	Description
SNMP Server	Indicates whether SNMP service is enabled.
SNMP Version	Indicates the SNMP protocol version, including v1, v2c, and v3 versions.
Local Port	The port range is 1 to 65535.
Device Location	1-64 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed.
Contact Info	1-64 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed.

(3) Click **Save**.

After the SNMP service is enabled, click **Save** to make basic configurations such as the SNMP protocol version number take effect.

13.6.3 Group/Community/Client Access Control

1. View Group/Community/Client Access Control

Management Information Base (MIB) can be regarded as a database storing the status information and performance data of network devices. It contains a large number of object identifiers (OIDs) to identify the status information and performance data of these network devices.

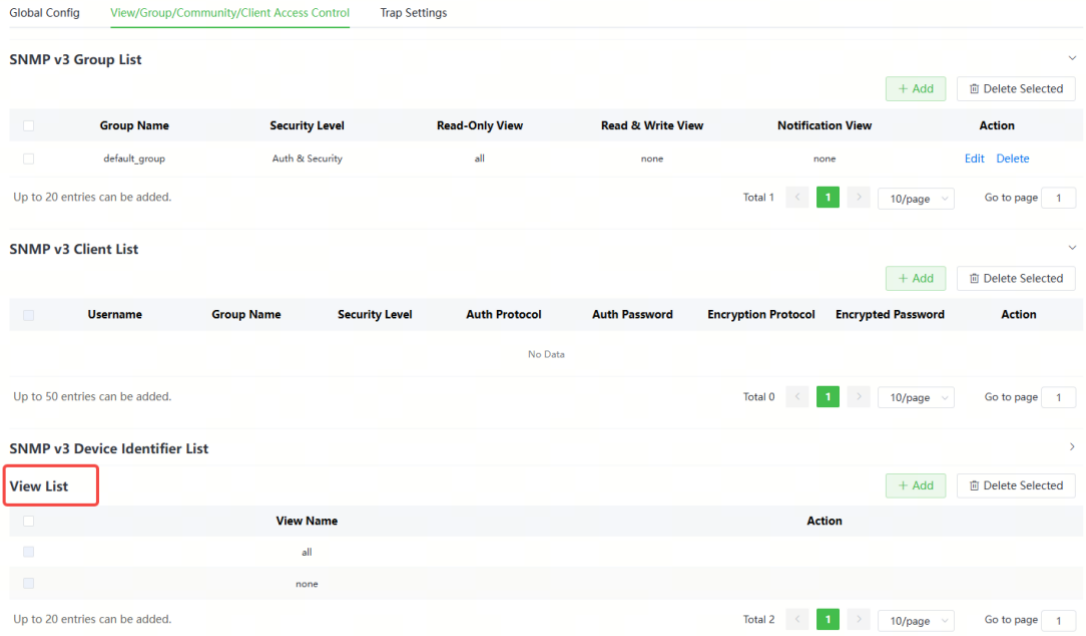
Views in SNMP can limit the range of MIB nodes that the management system can access, thereby improving the security and reliability of network management. Views are an indispensable part of SNMP and need to be configured or customized according to specific management requirements.

A view can have multiple subtrees. The management system can only access MIB nodes in these subtrees, and cannot access other unauthorized MIB nodes. This can prevent unauthorized system administrators from accessing sensitive MIB nodes, thereby protecting the security of network devices. Moreover, views can also improve the efficiency of network management and speed up the response from the management system.

- Configuration Steps

Choose **Local Device** > **System** > **SNMP** > **View/Group/Community/Client Access Control.**

(1) Click **Add** under the **View List** to add a view.



(2) Configure basic information of a view. After configuration, click **OK**.

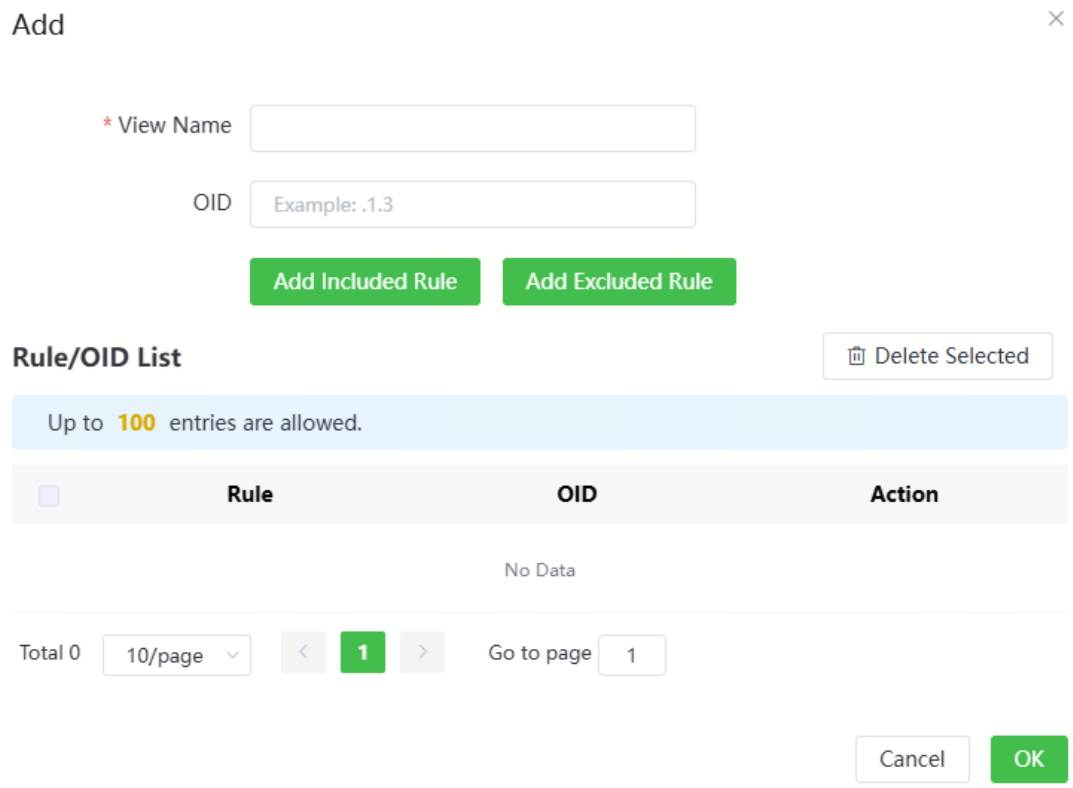


Table 13-3View Configuration Parameters

Parameter	Description
View Name	Indicates the name of the view. 1-32 characters. Chinese or full width characters are not allowed.
OID	Indicates the range of OIDs included in the view, which can be a single OID or a subtree of OIDs.
Type	There are two types of rules: included and excluded rules. ● The included rule only allows access to OIDs within the OID range. Click **Add Included Rule** to set this type of view. ● Excluded rules allow access to all OIDs except those in the OID range. Click **Add Excluded Rule** to configure this type of view.

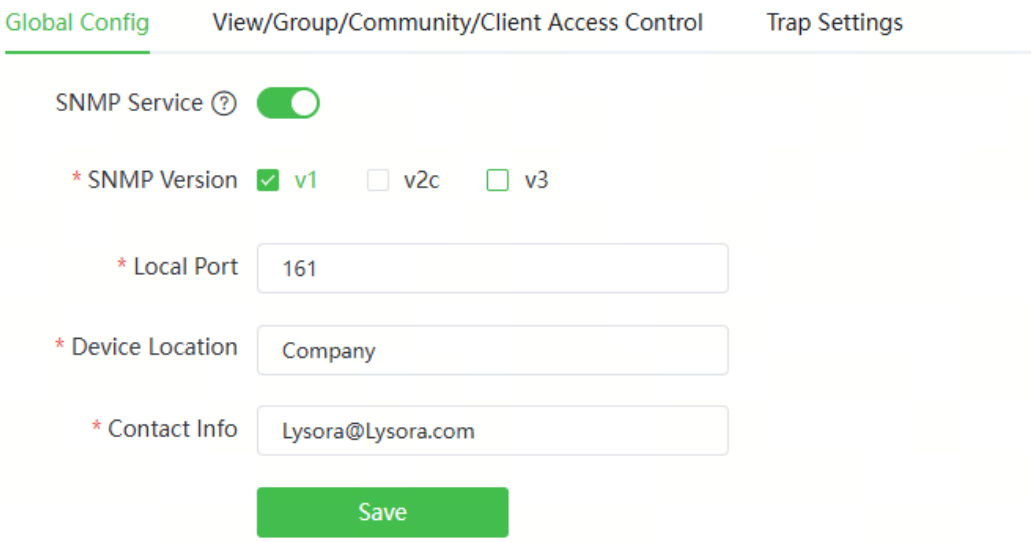
Note

At least one OID rule must be configured for a view. Otherwise, an alarm message will appear.

2. Configuring v1Orv2c Users

- Overview

  When the SNMP version is set to v1/v2c, user configuration is required.



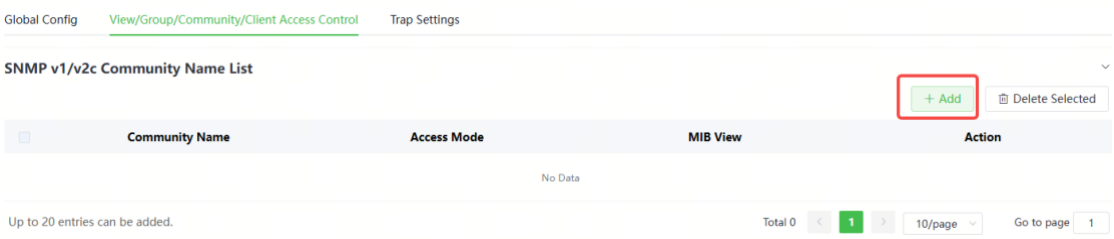
Note

Select the SNMP protocol version, and click **Save**. The corresponding configuration options will appear on the **View/Group/Community/User Access Control** page.

- Configuration Steps

Choose **Local Device** > **System** > **SNMP** > **View/Group/Community/Client Access Control.**

(1) Click **Add** in the **SNMP v1/v2c Community Name List** pane.



(2) Add a v1/v2c user. After configuration, click **OK**.

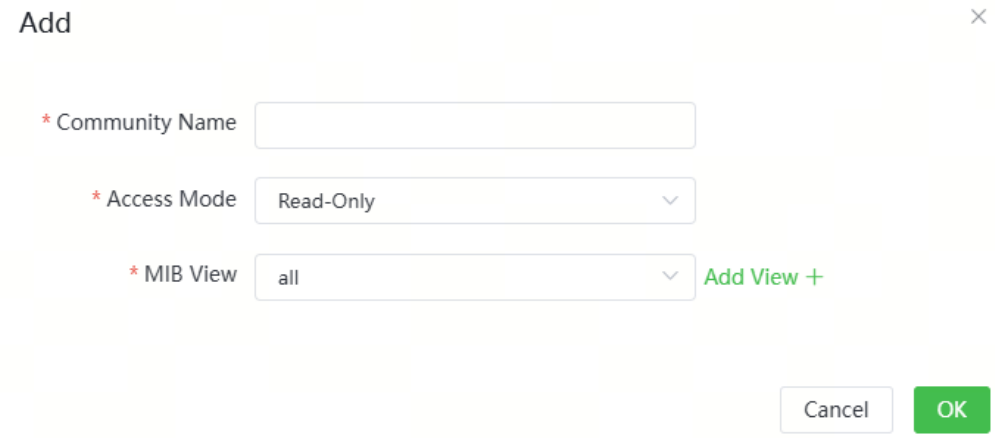


Table 13-4v1/v2c User Configuration Parameters

Parameter	Description
Community Name	At least 8 characters. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Admin, public or private community names are not allowed. Question marks, spaces, and Chinese characters are not allowed.
Access Mode	Indicates the access permission (read-only or read & write) for the community name.
MIB View	The options under the drop-down box are configured views (default: all, none).

Caution

- Community names cannot be the same among v1/v2c users.
- Click **Add View** to add a view.

3. Configuring v3 Groups

- Overview

  SNMP v3 introduces the concept of grouping to achieve better security and access control. A group is a group of SNMP users with the same security policies and access control settings. With SNMP v3, multiple groups can be configured, each with its own security policies and access control settings. Each group can have one or more users.

- Prerequisites

  When the SNMP version is set to v3, the v3 group configuration is required.

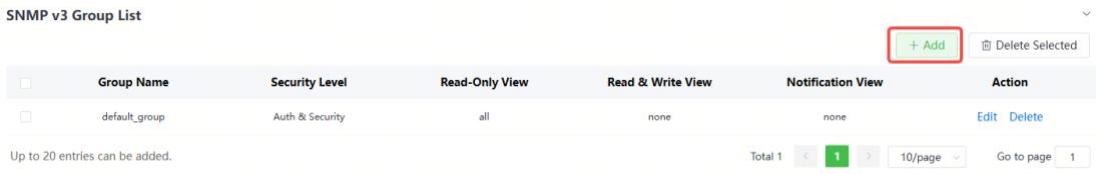
Note

Select the SNMP protocol version, and click **Save**. The corresponding configuration options will appear on the **View/Group/Community/User Access Control** page.

- Configuration Steps

Choose **Local Device** > **System** > **SNMP** > **View/Group/Community/Client Access Control.**

(1) Click **Add** in the **SNMP v3 Group List** pane to create a group.



(2) Configure v3 group parameters. After configuration, click **OK**.

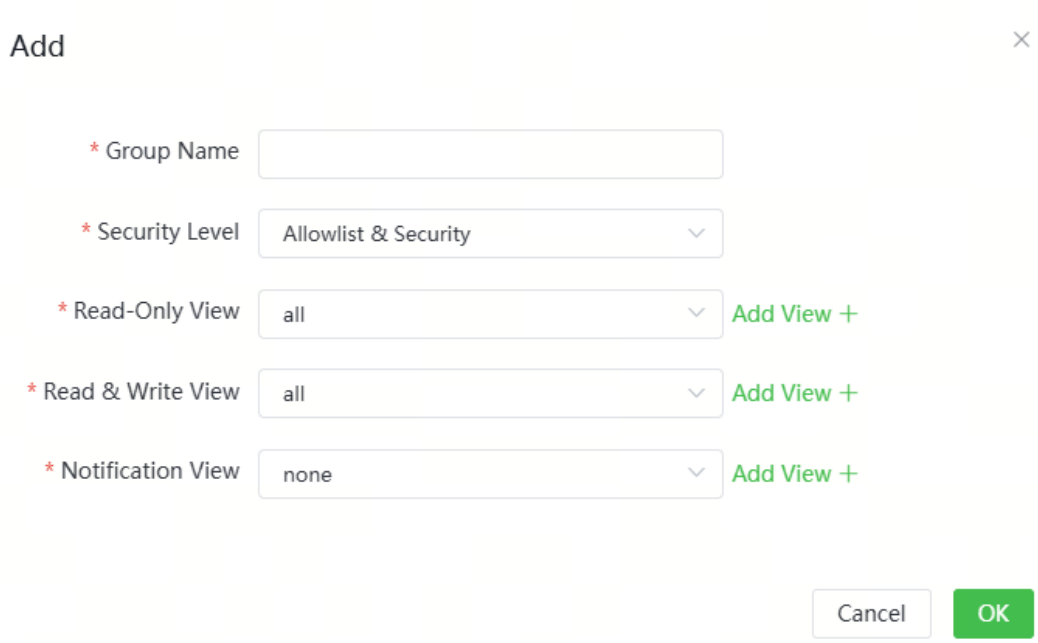


Table 13-5v3 Group Configuration Parameters

Parameter	Description
Group Name	Indicates the name of the group. 1-32 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed.
Security Level	Indicates the minimum security level (authentication and encryption, authentication but no encryption, no authentication and encryption) of the group.
Read-Only View	The options under the drop-down box are configured views (default: all, none).
Read & Write View	The options under the drop-down box are configured views (default: all, none).
Notify View	The options under the drop-down box are configured views (default: all, none).

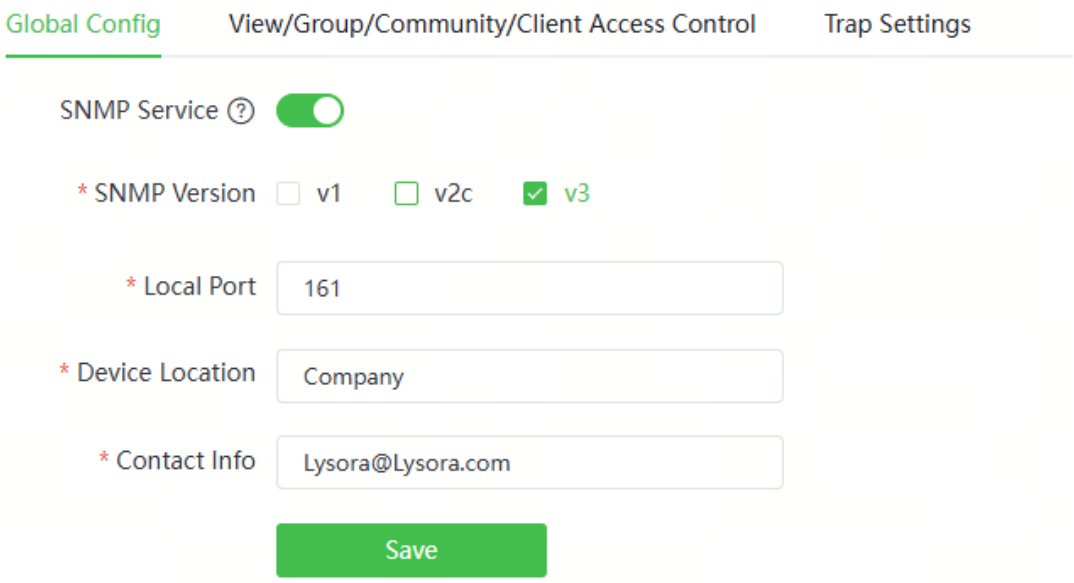
Caution

- A group defines the minimum security level, read and write permissions, and scope for users within the group.
- The group name must be unique. To add a view, click **Add View**.

4. Configuring v3 Users

- Prerequisites

When the SNMP version is set to v3, the v3 group configuration is required.



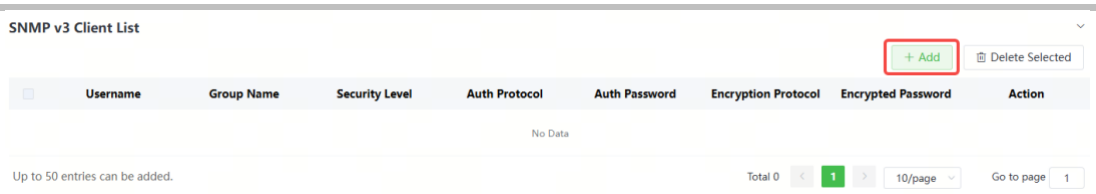
Note

Select the SNMP protocol version, and click **Save**. The corresponding configuration options will appear on the **View/Group/Community/User Access Control** page.

- Configuration Steps

Choose **Local Device** > **System** > **SNMP** > **View/Group/Community/Client Access Control**.

(1) Click **Add** in the **SNMP v3 Client List** pane to add a v3 user.



(2) Configure v3 user parameters. After configuration, click **OK**.

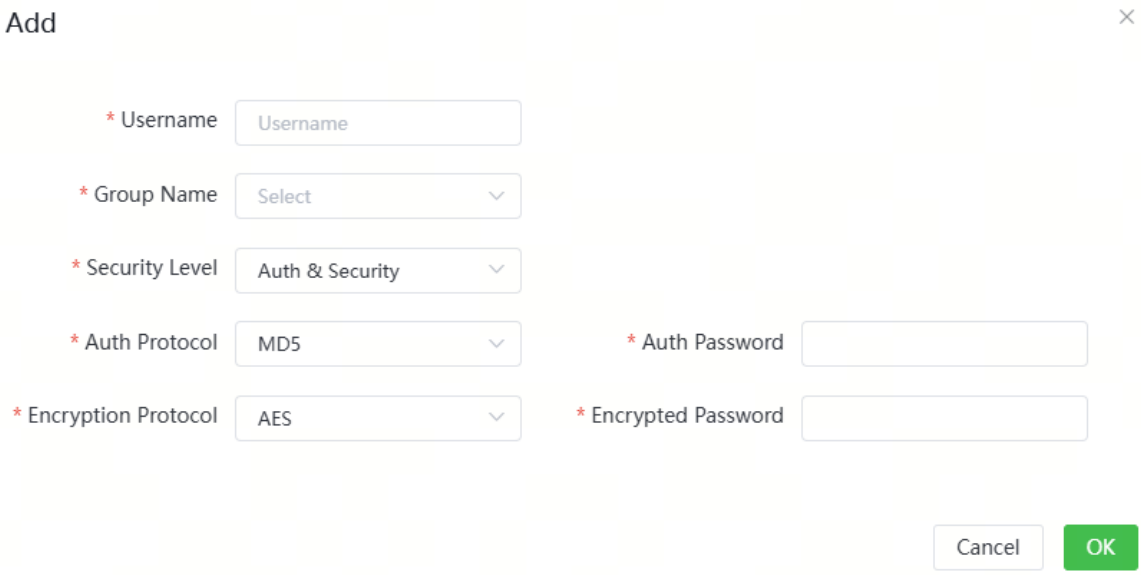


Table 13-6v3 User Configuration Parameters

Parameter	Description
Username	Username At least 8 characters. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Admin, public or private community names are not allowed. Question marks, spaces, and Chinese characters are not allowed.
Group Name	Indicates the group to which the user belongs.

Parameter	Description
Security Level	Indicates the security level (authentication and encryption, authentication but no encryption, and no authentication and encryption) of the user.
Auth Protocol, Auth Password	Authentication protocols supported: MD5/SHA/SHA224/SHA256/SHA384/SHA512. Authentication password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Note: This parameter is mandatory when the security level is authentication and encryption, or authentication but no encryption.
Encryption Protocol, Encryption Password	Encryption protocols supported: DES/AES/AES192/AES256. Encryption password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Note: This parameter is mandatory when the security level is authentication and encryption.

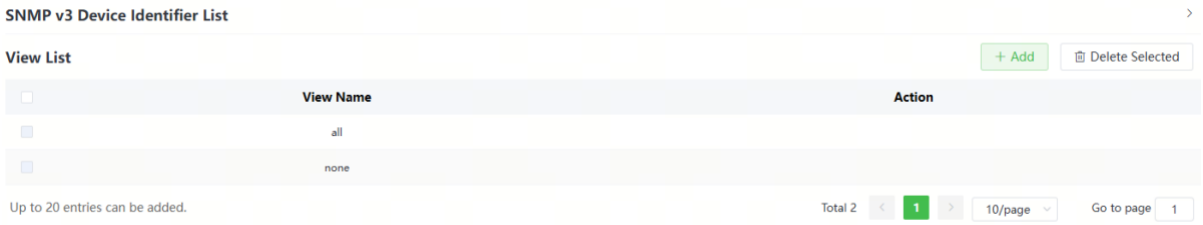
Caution

- The security level of v3 users must be greater than or equal to that of the group.
- There are three security levels, among which authentication and encryption requires the configuration of authentication protocol, authentication password, encryption protocol, and encryption password. Authentication but no encryption only requires the configuration of authentication protocol and encryption protocol, while no authentication and encryption does not require any configuration.

5. Checking SNMP v3 Device Identifiers

Choose **Local Device** > **System** > **SNMP** > **View/Group/Community/Client Access Control** > **SNMP v3 Device Identifier List**.

Check the SNMP v3 device identifiers in the **SNMP v3 Device Identifier List** area.



13.6.4 Typical Configuration Examples of SNMP Services

1. Configuring SNMP v2c

- Application Scenario

  You only need to monitor the device information, but do not need to set and deliver it. A third-party software can be used to monitor the data of nodes like 1.3.6.1.2.1.1 if v2c version is configured.

- Configuration Specification

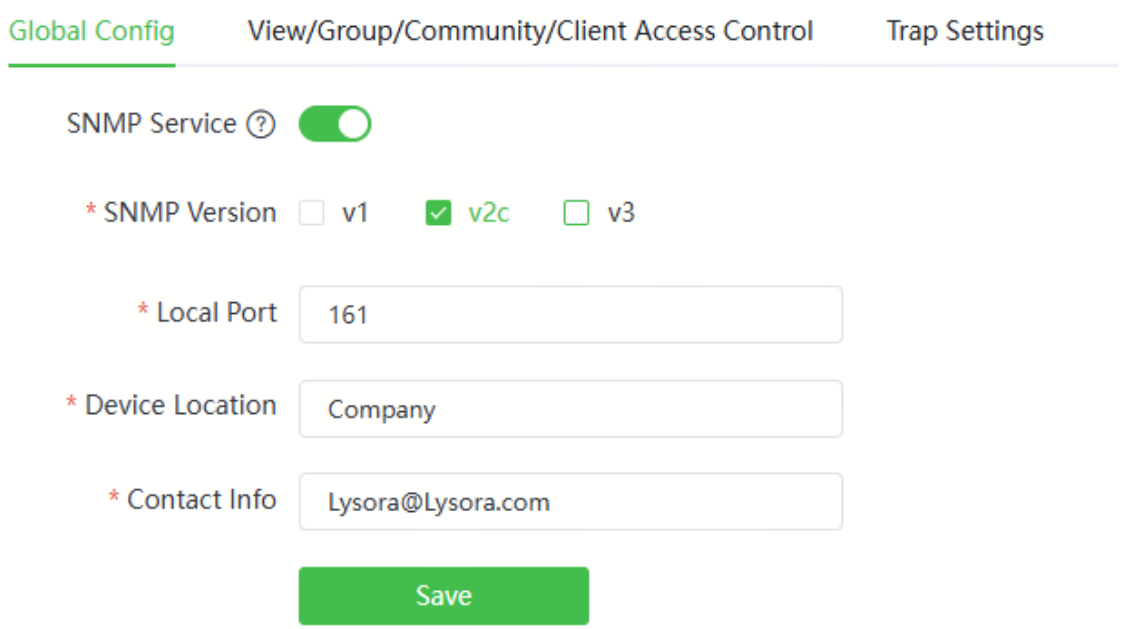
  According to the user's application scenario, the requirements are shown in the following table:

Table 13-7User Requirement Specification

Item	Description
View range	Included rule: the OID is .1.3.6.1.2.1.1, and the custom view name is "system".
Version	For SNMP v2c, the custom community name is "public", and the default port number is 161.
Read & write permission	Read-only permission.

- Configuration Steps

(2) Choose **Local Device** > **System** > **SNMP** > **Global Config**, select **v2c** and set other settings as default. Then, click **Save**.

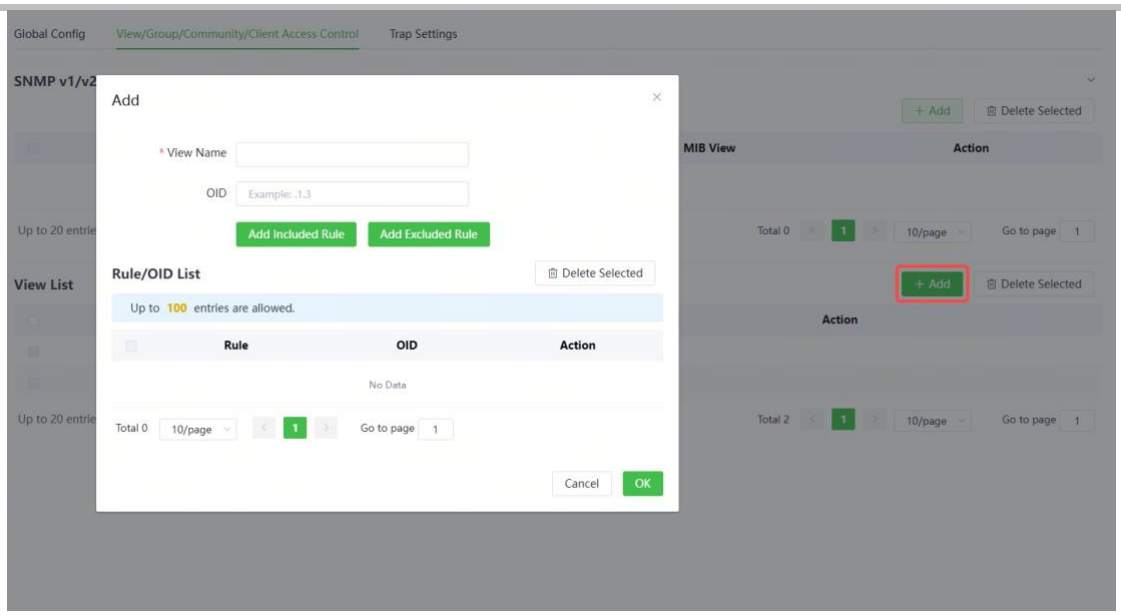


(3) Choose **Local Device** > **System** > **SNMP** > **View/Group/Community/Client Access Control** ,Add a view on the View/Group/Community/Client Access Control interface.

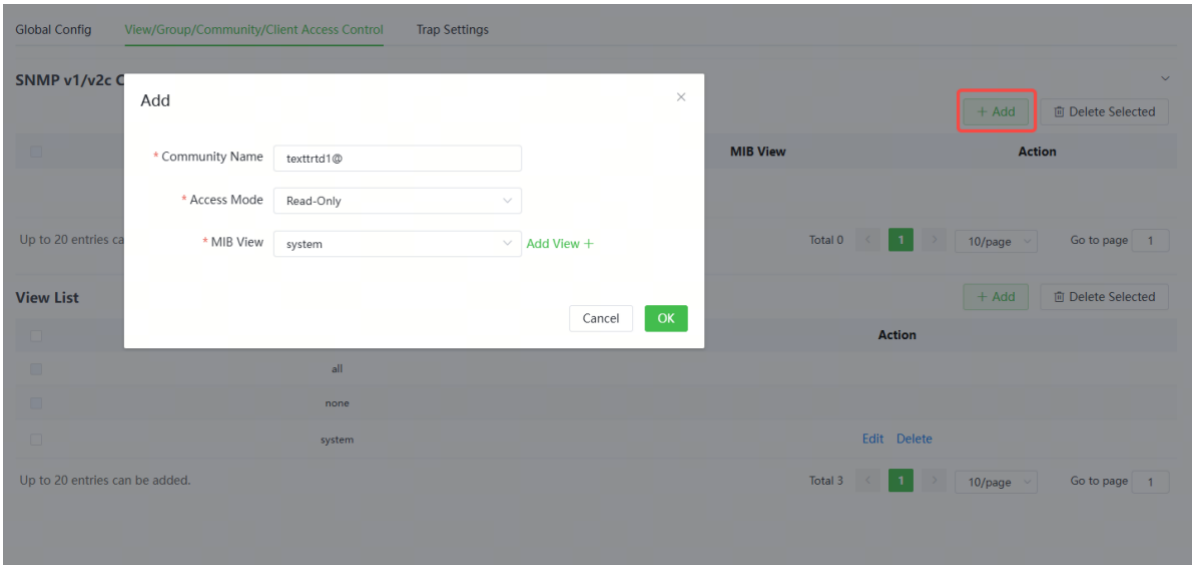
a Click **Add** in the **View List** pane.

b Enter the view name and OID in the pop-up window, and click **Add Included Rule**.

c Click **OK**.



(4) Click **Add** in the **SNMP v1/v2c Community Name List**, fill in the community name, access mode and view in the pop-up window, and click **OK** after the operation is completed.



2. Configuring SNMP v3

- Application Scenario

  You need to monitor and control devices, and use the third-party software to monitor and deliver device information to public nodes (1.3.6.1.2.1). The security level of v3 is authentication and encryption.

- Configuration Specification

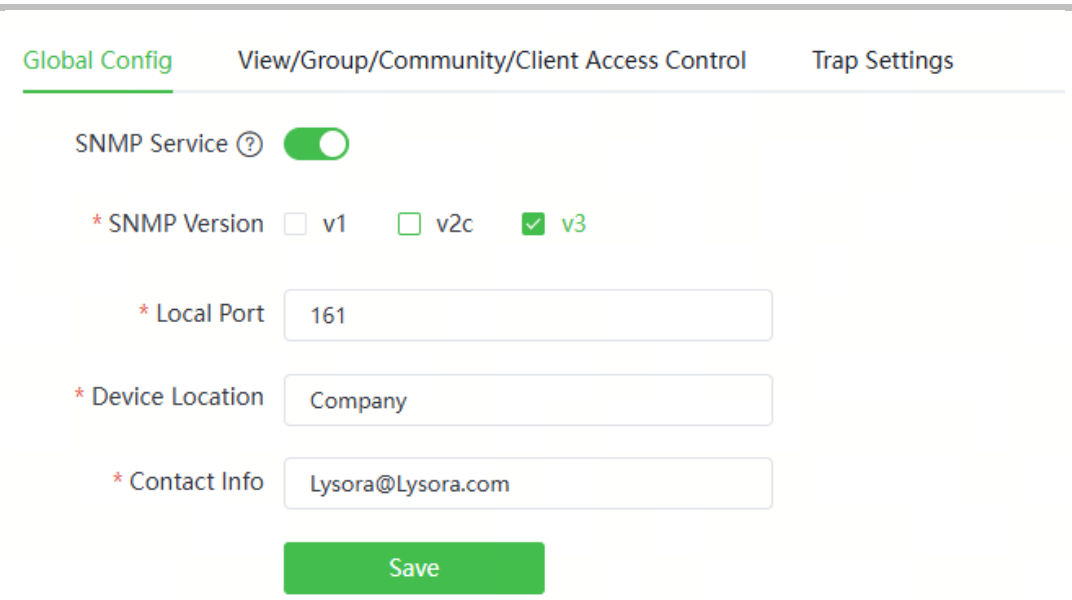
  According to the user's application scenario, the requirements are shown in the following table:

Table 13-8User Requirements Description Form

Item	Description
View range	Included rule: the OID is .1.3.6.1.2.1, and the custom view name is "public_view".
Group configuration	Group name: group Security level: authentication and encryption Select public_view for a read-only view. Select public_view for a read & write view. Select none for a notify view.
Configuring v3 Users	User name: v3_user Group name: group Security level: authentication and encryption Authentication protocol/password: MD5/Lysora123 Encryption protocol/password: AES/Lysora123
Version	For SNMP v3, the default port number is 161.

- Configuration Steps

(2) Choose **Local Device** > **System** > **SNMP** > **Global Config**, select **v3**, and change the port number to 161. Set other settings to defaults. Then, click **Save**.

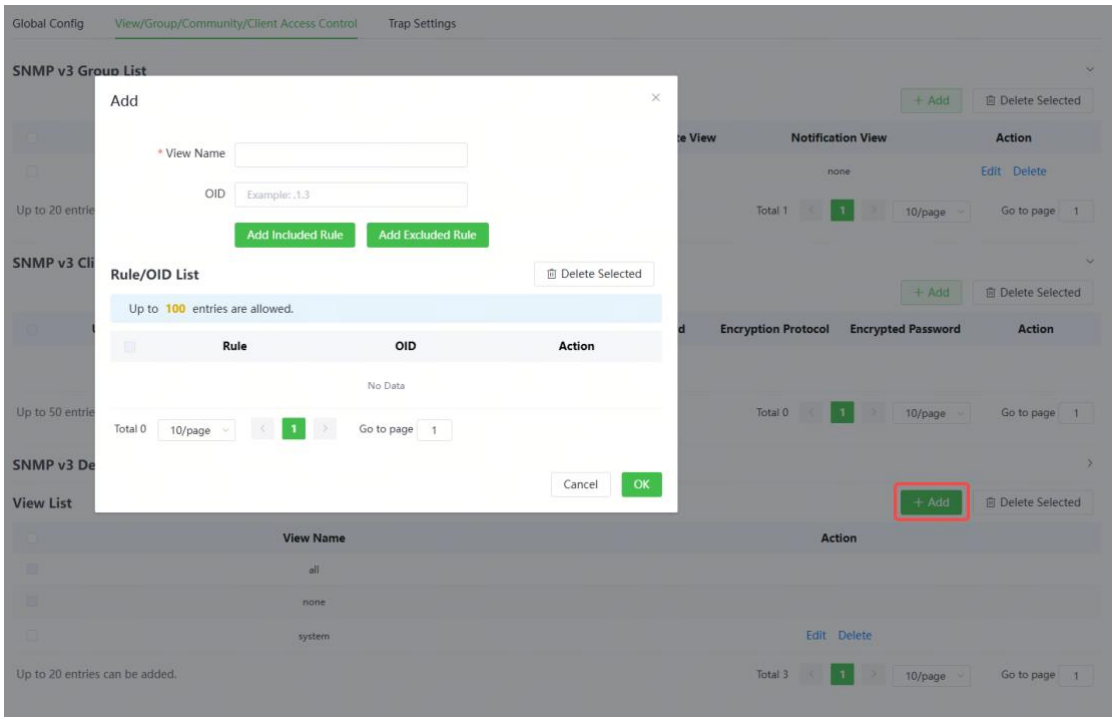


(3) Choose **Local Device** > **System** > **SNMP** > **View/Group/Community/Client Access Control**. Add a view on the View/Group/Community/Client Access Control interface.

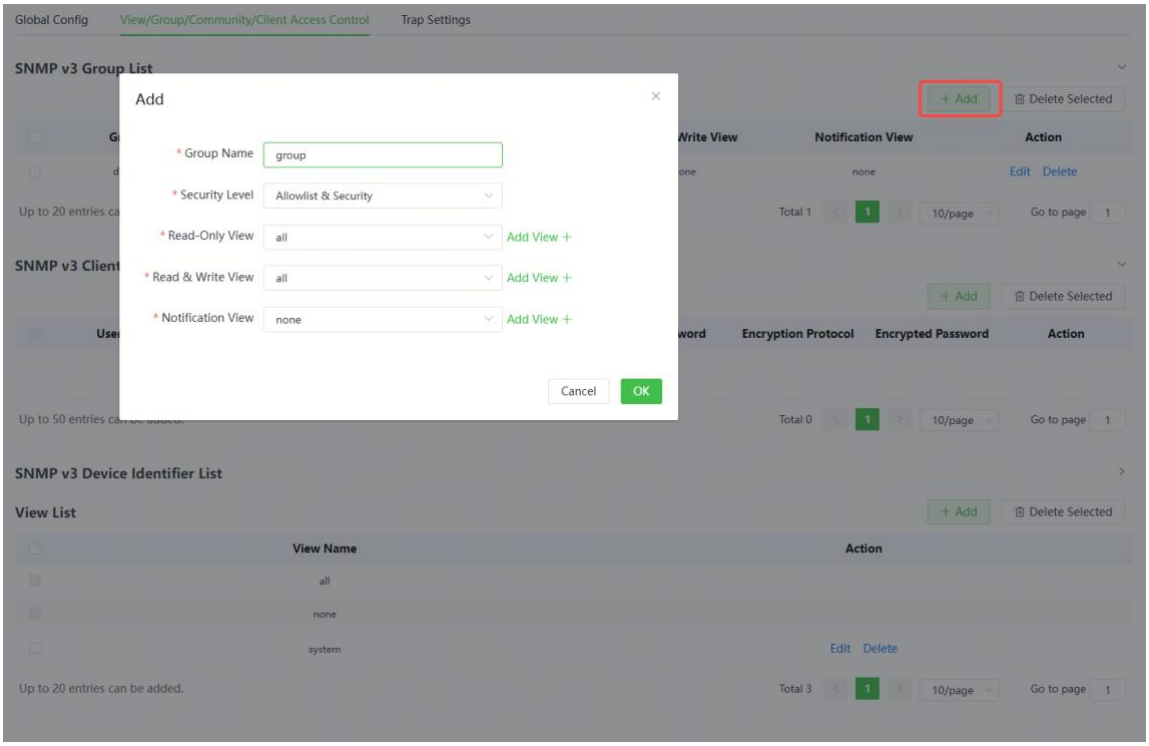
a Click **Add** in the **View List** pane.

b Enter the view name and OID in the pop-up window, and click **Add Included Rule**.

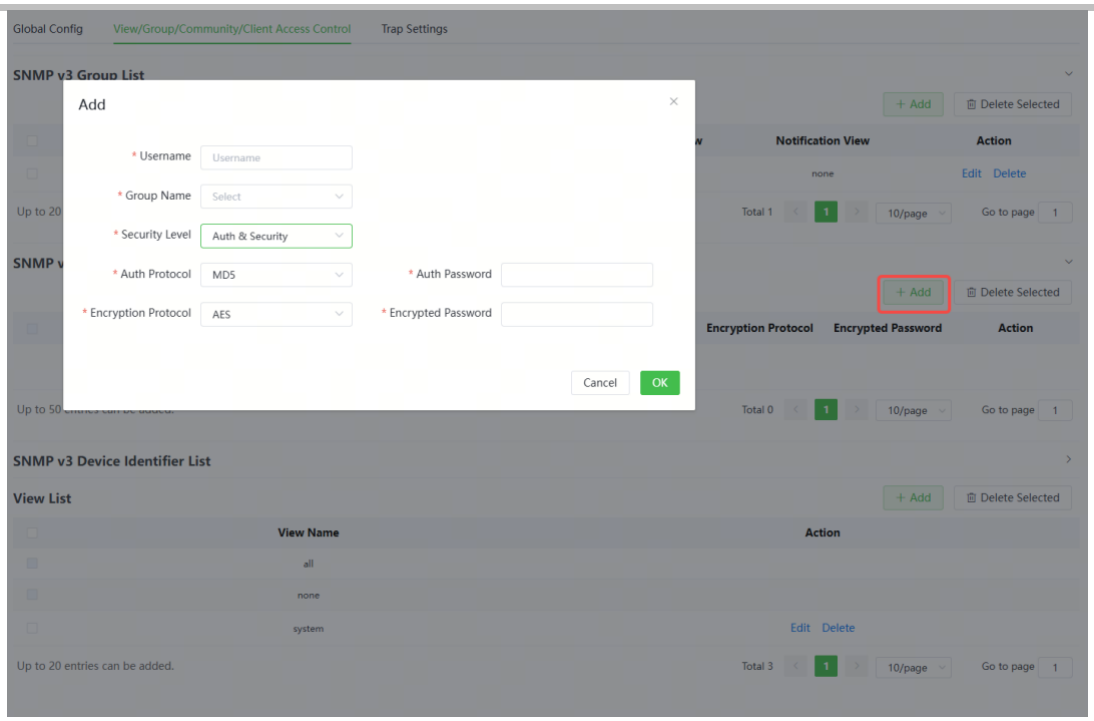
c Click **OK**.



(4) Click **Add** in the **SNMP v3 Group List**, fill in the group name and security level in the pop-up window, the user has read and write permissions, select"public _view"for the readable view and read and write view, and set the notification view to none. After the operation is complete, click **OK**.



(5) Click **Add** in the **SNMP v3 Client List**, fill in the user name and group name in the pop-up window, the user security level adopts authentication and encryption mode, fill in the corresponding authentication protocol, authentication password, encryption protocol, and encryption password, and click **OK**.



13.6.5 Trap Service Configuration

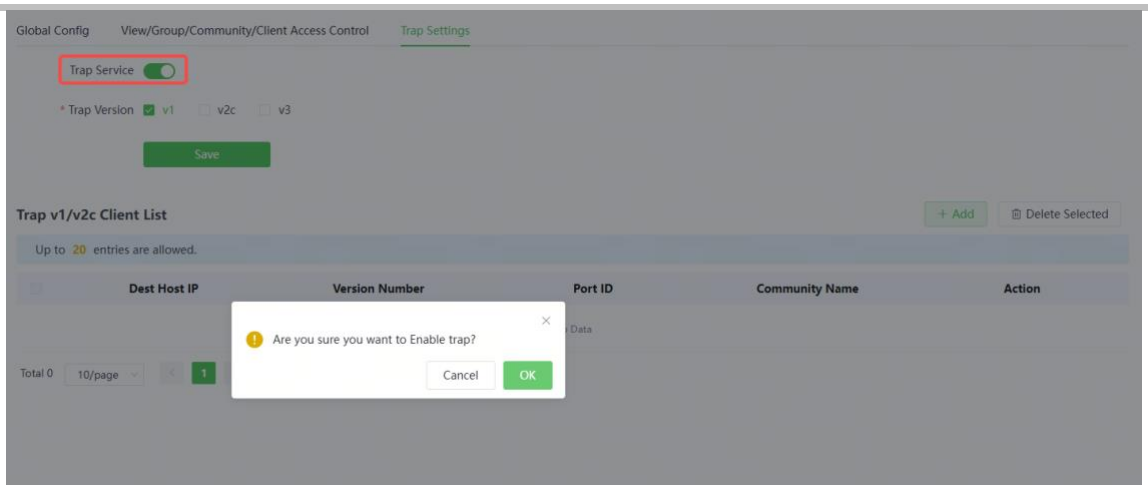
Trap is a notification mechanism of the SNMP (Simple Network Management Protocol) protocol, which is used to report the status and events of network devices to managers, including device status reports, fault reports, performance reports, configuration reports and security management. Trap can provide real-time network monitoring and fault diagnosis to help administrators find and solve network problems in time.

1. Trap Open Settings

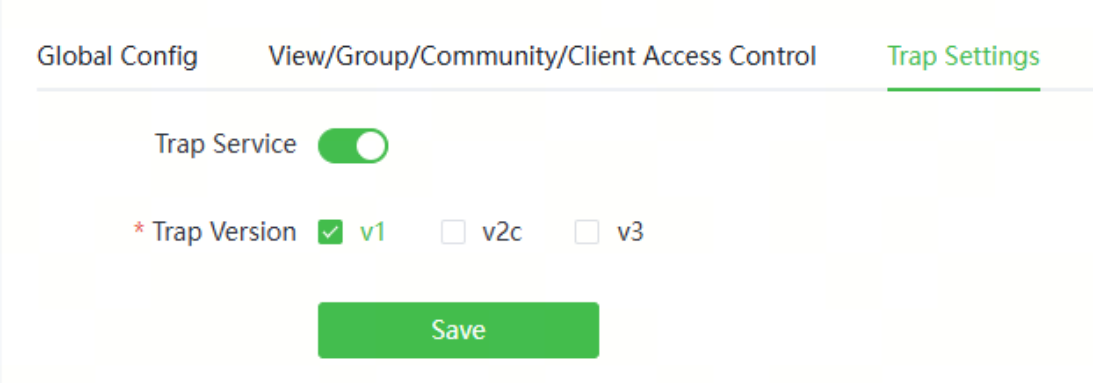
Enable the trap service and select the effective trap protocol version, including v1, v2c, and v3.

Choose **Local Device** > **System** > **SNMP** > **Trap Settings**.

(1) Enable the trap service switch.



When the first open is turned on, the system pops up a prompt message. Click **OK**.



(2) Set the trap version.

The trap protocol version number includes v1 version, v2c version, and v3 version.

(3) Click **OK**.

After the trap service is enabled, you need to click **Save**, and the configuration of the trap protocol version number will take effect.

2. Trap v1Or v2c User Configuration

- Introduction

A trap is a notification mechanism used to send an alert to administrators when important events or failures occur on a device or service. Trap v1/v2c are two versions of SNMP protocol, used for network management and monitoring.

Trap v1 is the first version in the SNMP protocol, which supports basic alarm notification functions. trap v2c is the second version in the SNMP protocol, which supports more alarm notification options and more advanced security.

By using trap v1/v2c, the administrator can know the problems in the network in time and take corresponding measures.

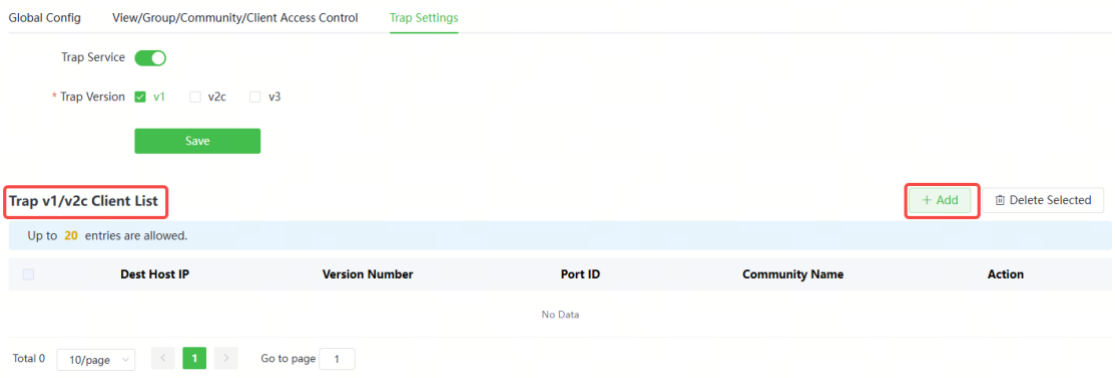
- Prerequisites

  When the trap service version selects v1 or v2c, a trap v1v2c user needs to be created.

- Configuration Steps

Choose **Local Device** > **System** > **SNMP** > **Trap Settings.**

(1) Click **Add** in the **Trap v1/v2c Client List** to create a trap v1v2c user.



(2) Configure trap v1v2c user-related parameters. After configuration, click **OK**.

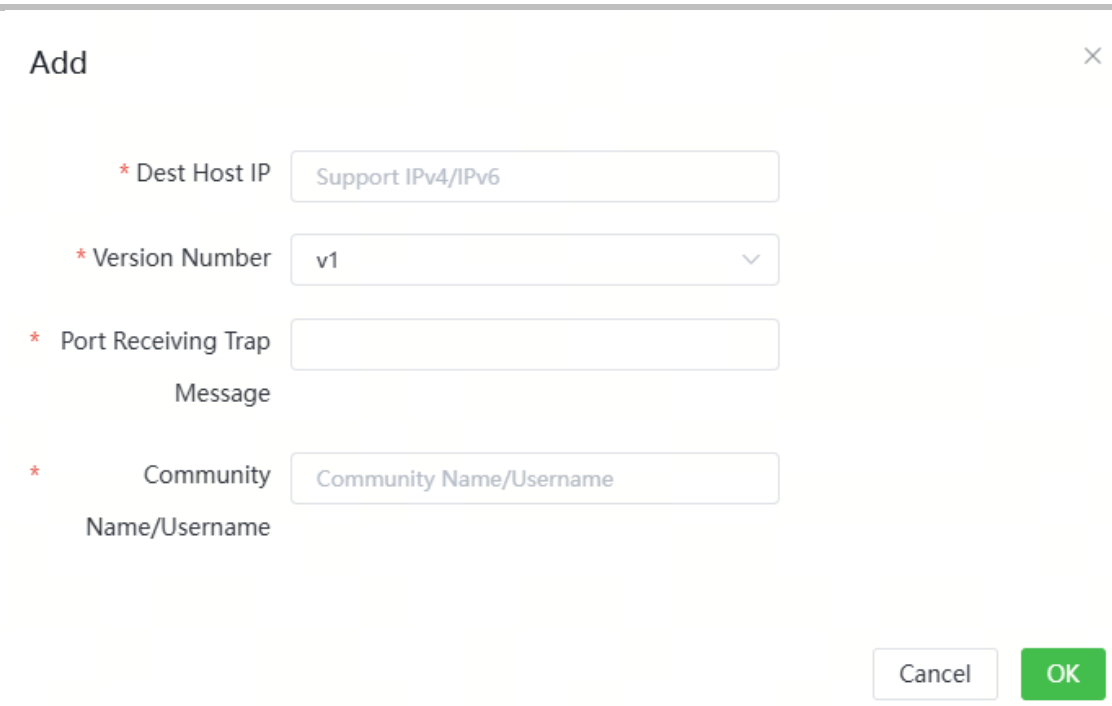


Table 13-9Trap v1/v2c user information description table

Parameter	Description
Dest Host IP	IP address of the trap peer device. An IPv4 or IPv6 address is supported.
Version Number	Trap version, including v1 and v2c.
Port Receiving Trap Message	The port range of the trap peer device is 1 to 65535.
Community name/User name	Community name of the trap user. At least 8 characters. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Admin, public or private community names are not allowed. Question marks, spaces, and Chinese characters are not allowed.

Caution

- The destination host IP address of trap v1/v2c/v3 users cannot be the same.
- Community names of trap v1/v2c/v3 users cannot be the same.

3. Trap v3 User Configuration

- Introduction

  Trap v3 is a network management mechanism based on SNMP protocol, which is used to send alarm notifications to management personnel. Unlike previous versions, trap v3 provides more secure and flexible configuration options, including authentication and encryption.

  Trap v3 can be customized to choose the conditions and methods to send alerts, as well as who receives alerts and how to be notified. This enables administrators to understand the status of network devices more accurately and take timely measures to ensure network security and reliability.

- Prerequisites

  When v3 is selected as the trap service version, a trap v3 user needs to be created.

- Configuration Steps

Choose **Local Device** > **System** > **SNMP** > **Trap Settings.**

(1) Click **Add** in the **Trap v3 Client List** to create a trap v3 user.

(2) Configure parameters related to trap v3 users. After configuration, click **OK**.

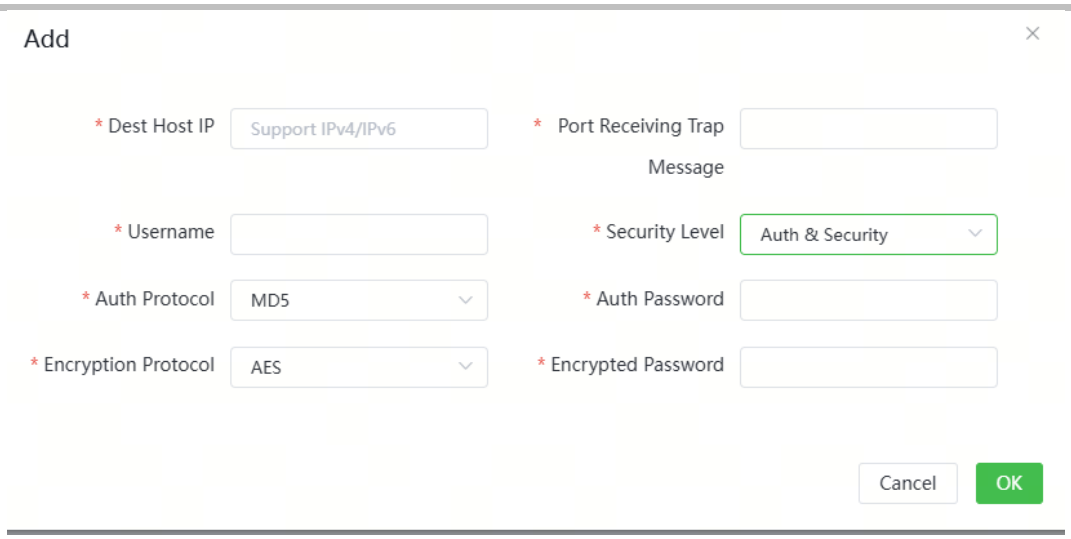


Table 13-10 trap v3 user information description table

Parameter	Description
Dest Host IP	IP address of the trap peer device. An IPv4 or IPv6 address is supported.
Port Receiving Trap Message	The port range of the trap peer device is 1 to 65535.
Username	Name of the trap v3 user. At least 8 characters. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Admin, public or private community names are not allowed. Question marks, spaces, and Chinese characters are not allowed.
Security Level	Indicates the security level of the trap v3 user. The security levels include authentication and encryption, authentication but no encryption, and no authentication and encryption.

Parameter	Description
Auth Protocol, Auth Password	Authentication protocols supported: MD5/SHA/SHA224/SHA256/SHA384/SHA512. Authentication password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Note: This parameter is mandatory when the security level is authentication and encryption, or authentication but no encryption.
Encryption Protocol, Encryption Password	Encryption protocols supported: DES/AES/AES192/AES256. Encryption password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Note: This parameter is mandatory when the security level is authentication and encryption.

Caution

IP of trap v1/v2c/v3 users cannot be repeated.

13.6.6 Typical Configuration Examples of the Trap Service

1. v2c Version Trap Configuration

- Application Scenarios

  When the user is monitoring the device, if the device is suddenly interrupted or abnormal, the third-party monitoring software cannot detect and deal with the abnormal situation in time, so configure the device with the destination ip 192.1

68.110.85 and port number 166, so that the device sends a trap of the v2c version in case of an exception.

- Configuration Specification

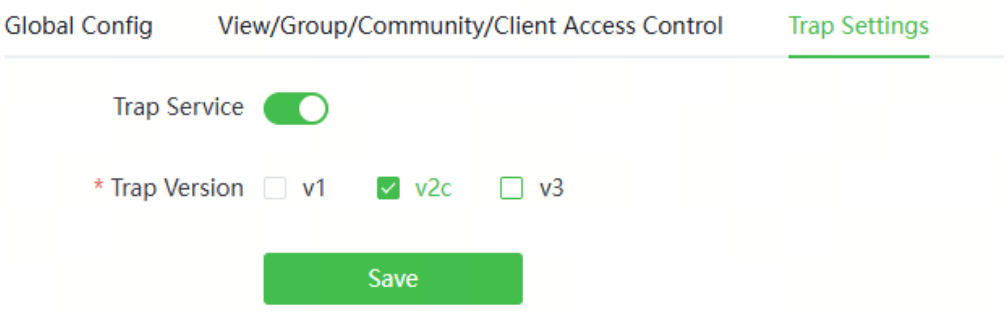
  According to the analysis of the user's usage scenario, the requirements are shown in the table:

Table 13-11 User Requirements Description Form

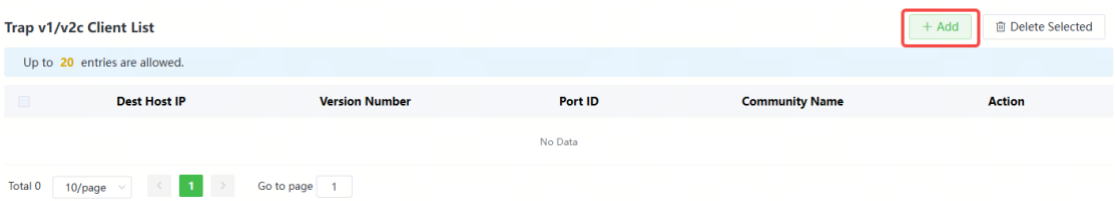
Item	Description
IP address and port number	The destination host IP is 192.168.100.85, and the port number is 166.
Version	Select the v2c version.
Community name/User name	Trap_user

- Configuration Steps

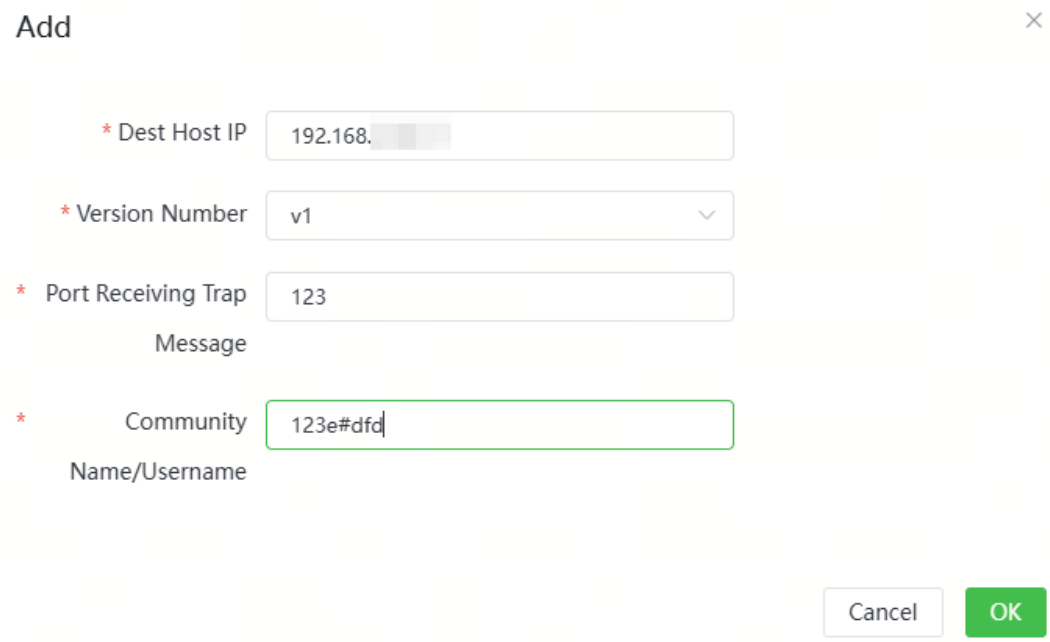
(2) Choose **Local Device** > **System** > **SNMP** > **Trap Settings**, select the v2c version on the trap setting interface, click **Save**.



(3) Click **Add** in the **Trap v1/v2c Client List**.



(4) Fill in the target host IP, version number, port number, user name and other information, and click **OK** after the configuration is complete.



2. v3 Version Trap Configuration

- Application Scenarios

  When the user is monitoring the device, if the device is suddenly interrupted or abnormal, the third-party monitoring software cannot detect and deal with the abnormal situation in time, and the device with the destination IP of 192.168.100.87 and the port number of 167 is configured, and use the more secure v3 version to send traps.

- Configuration Specification

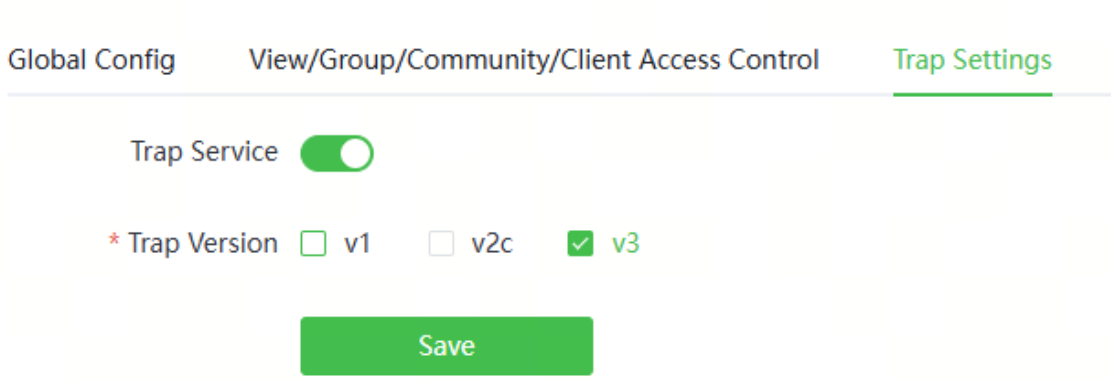
  According to the analysis of the user's usage scenario, the requirements are shown in the table:

Table 13-12 User Requirements Description Form

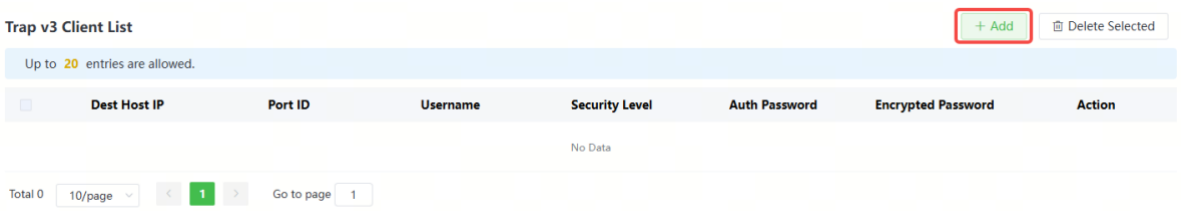
Item	Description
IP address and port number	The destination host IP is 192.168.100.87, and the port number is 167.
Version and user name	Select the v3 version and trapv3_user for the user name.
Authentication protocol/authentication password Encryption protocol/encryption password	Authentication protocol/password: MD5/Lysora123 Encryption protocol/password: AES/Lysora123

- Configuration Steps

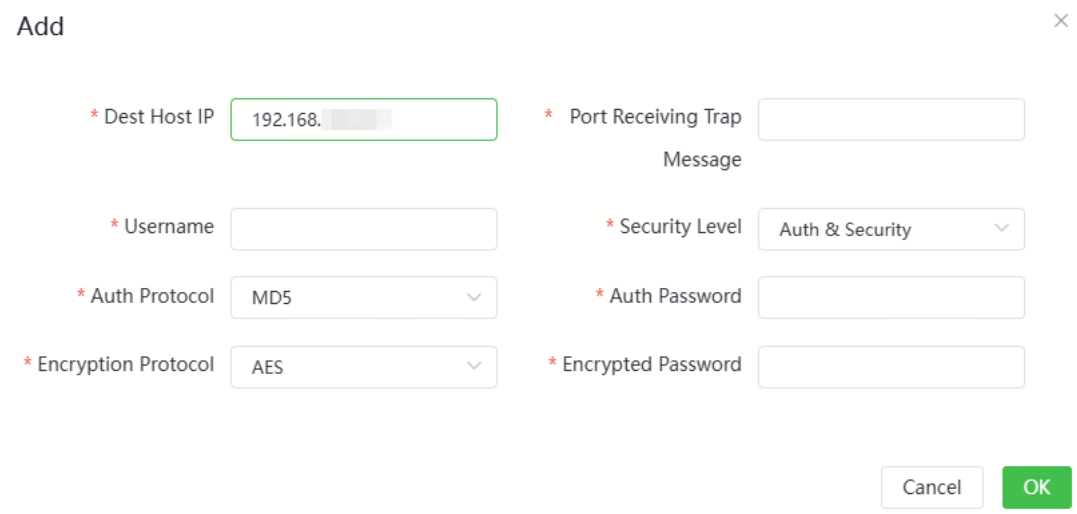
(2) Select the v3 version on the trap setting interface, and click **Save**.



(3) Click **Add** in the **Trap v3 Client List**.



(4) Fill in the target host IP, port number, user name and other information, and click **OK** after the configuration is complete.

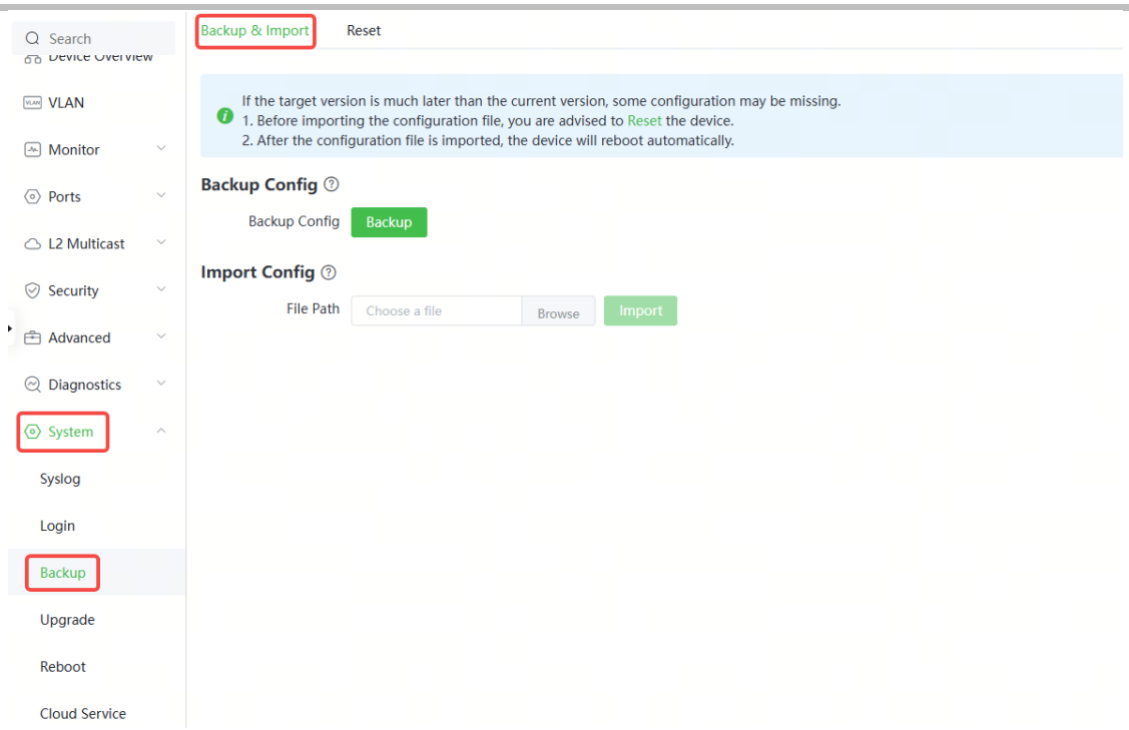


13.7 Configuration Backup and Import

Choose **Local Device** > **System** > **Backup** > **Backup & Import.**

Configure backup: Click **Backup** to generate the backup configuration and download it locally.

Configure import: Click **Browse**, select a backup configuration file locally, and click **Import** to apply the configuration specified by the file to the device After importing the configuration, the device will restart.

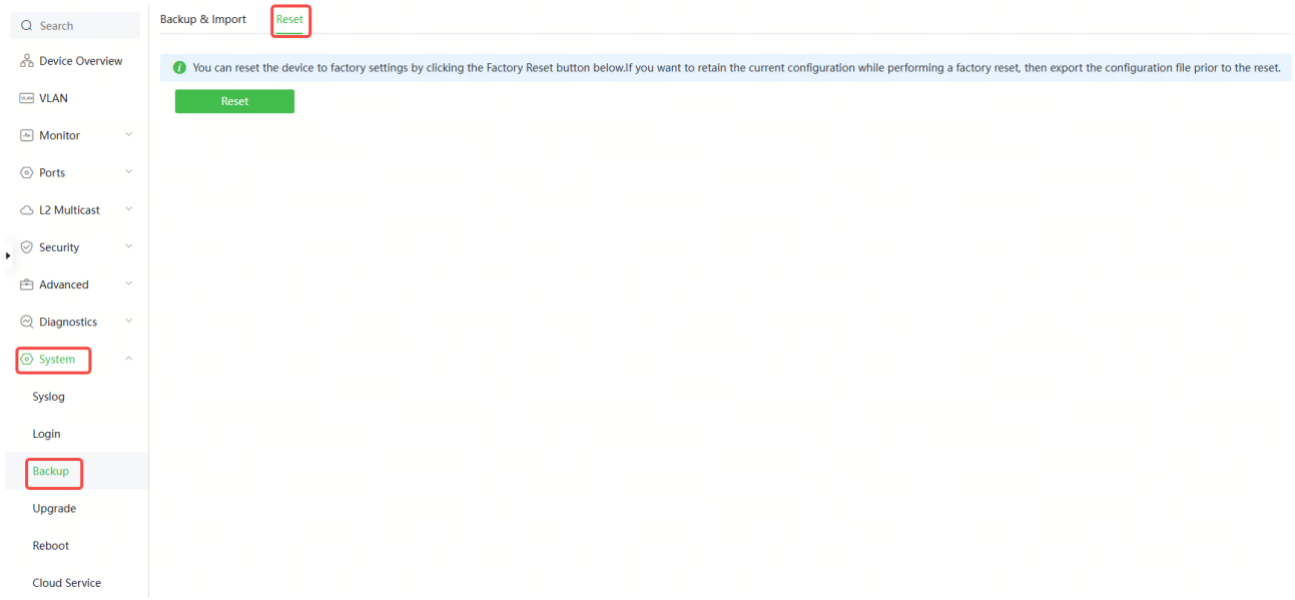


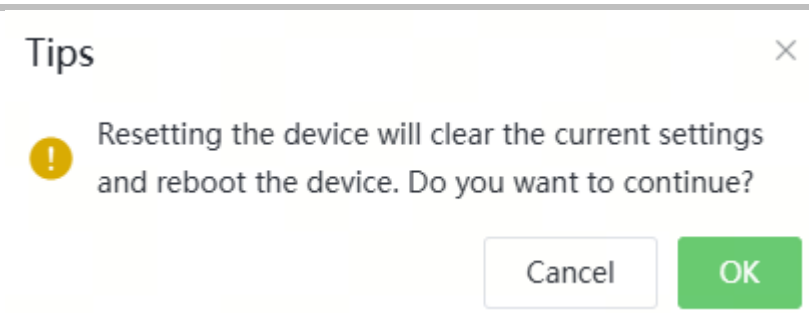
13.8 Reset

13.8.1 Resetting the Device

Choose **Local Device** > **System** > **Backup** > **Reset**.

Click **Reset**, and click **OK** to restore factory settings.





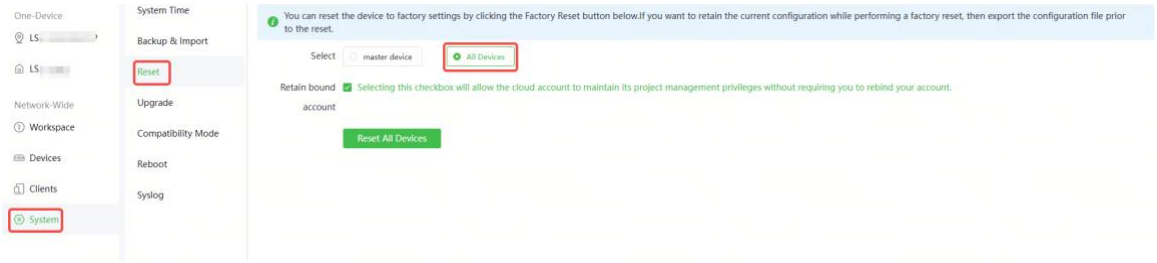
Caution

Resetting the device will clear current settings and reboot the device. If a useful configuration exists in the current system, you can export the current configuration (see 13.7 Configuration Backup and Import) before restoring the factory settings. Exercise caution when performing this operation.

13.8.2 Resetting the Devices in the Network

Choose **Network-Wide** > **System** > **Reset**.

Select **All Devices** and choose whether to **Unbind Account**, click **Reset All Devices** and all devices in the current network will be restored to their factory settings.



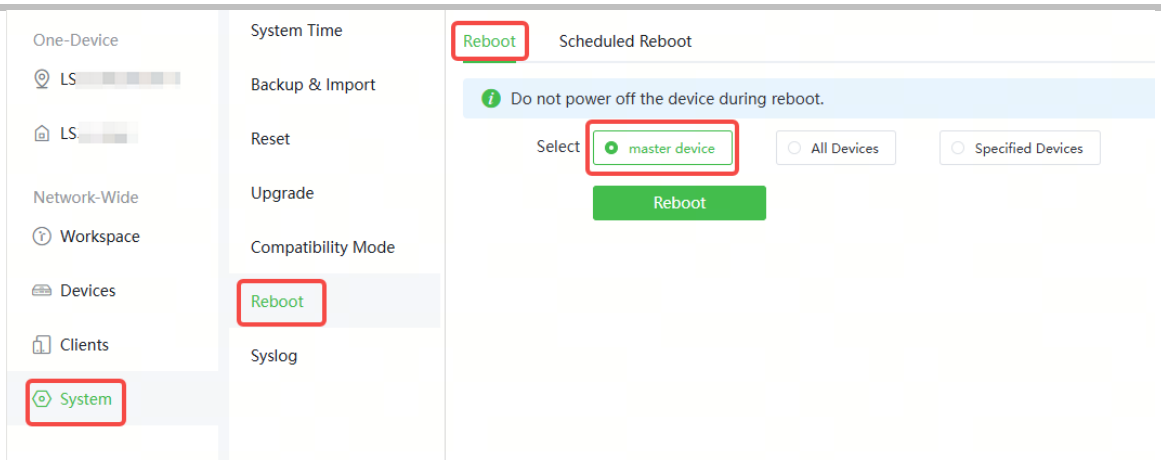
Caution

Resetting the network will clear current settings of all devices in the network and reboot the devices. Exercise caution when performing this operation.

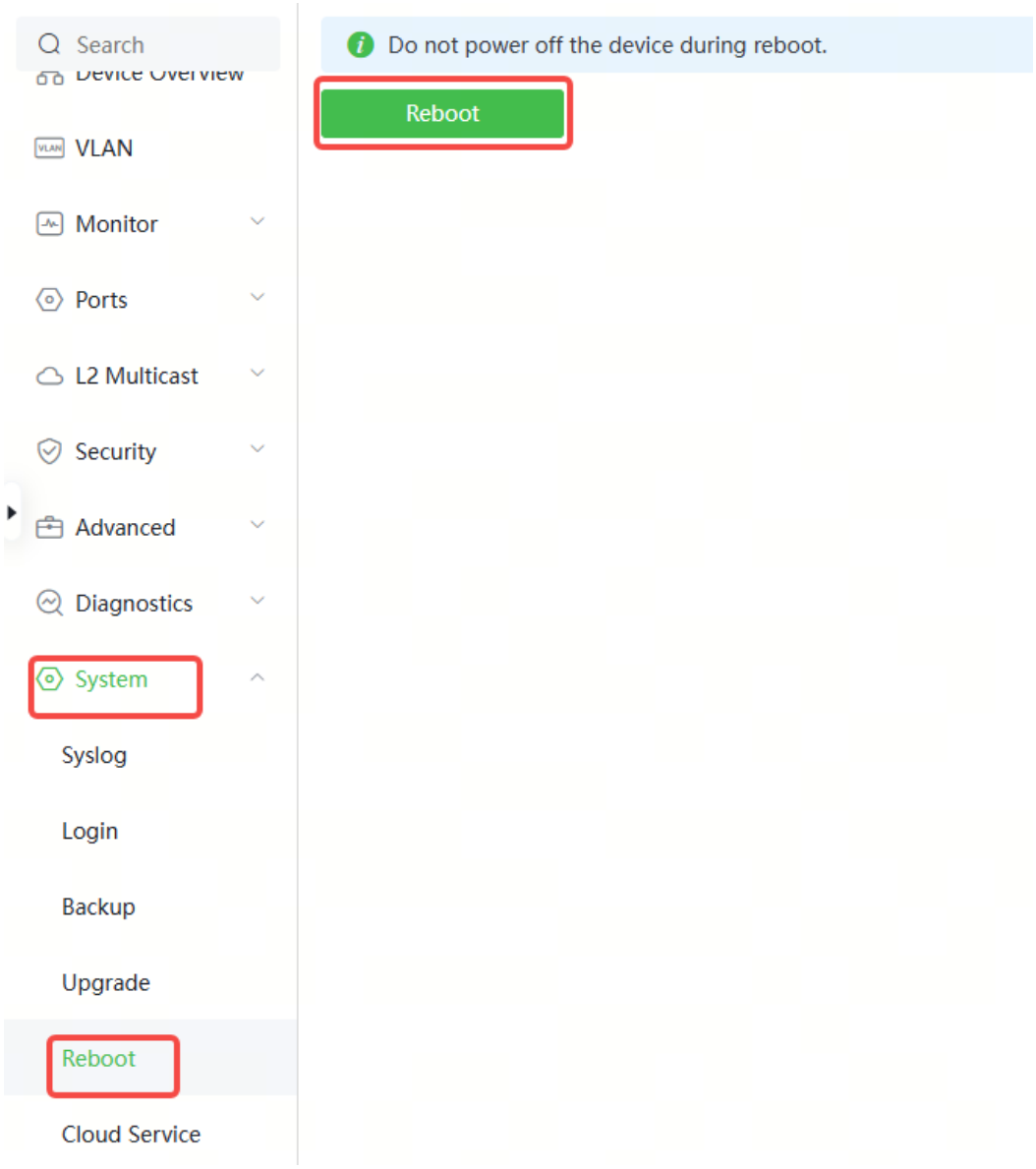
13.9 Rebooting the Device

13.9.1 Rebooting the Device

Choose **Network-Wide** > **System** > **Reboot** > **Reboot**.



Choose **Local Device** > **System** > **Reboot**.

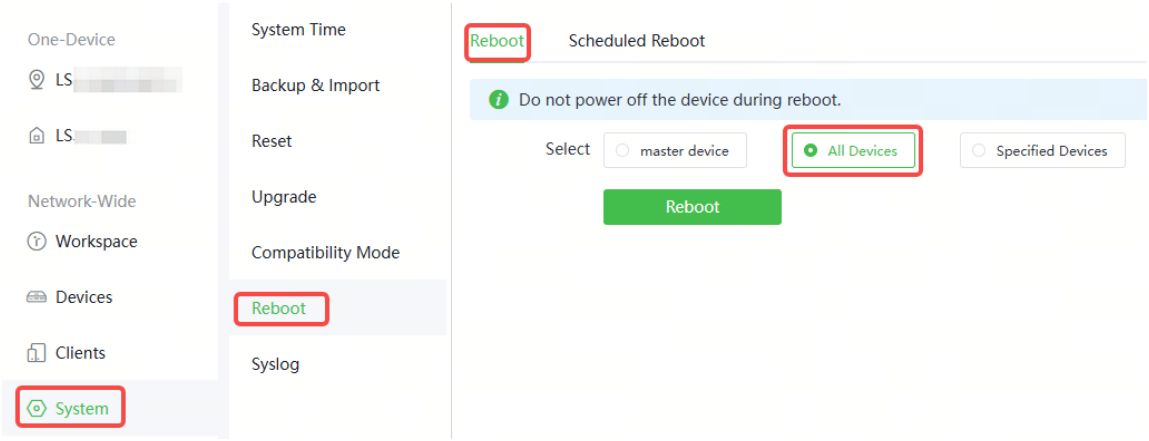


Do not refresh the page or close the browser during the reboot. After the device is successfully rebooted and the Web service becomes available, the device automatically jumps to the login page.

13.9.2 Rebooting the Devices in the Network

Choose **Network-Wide** > **System** > **Reboot** > **Reboot**.

Select **All Devices**, and click **Reboot** to reboot all devices in the current network.



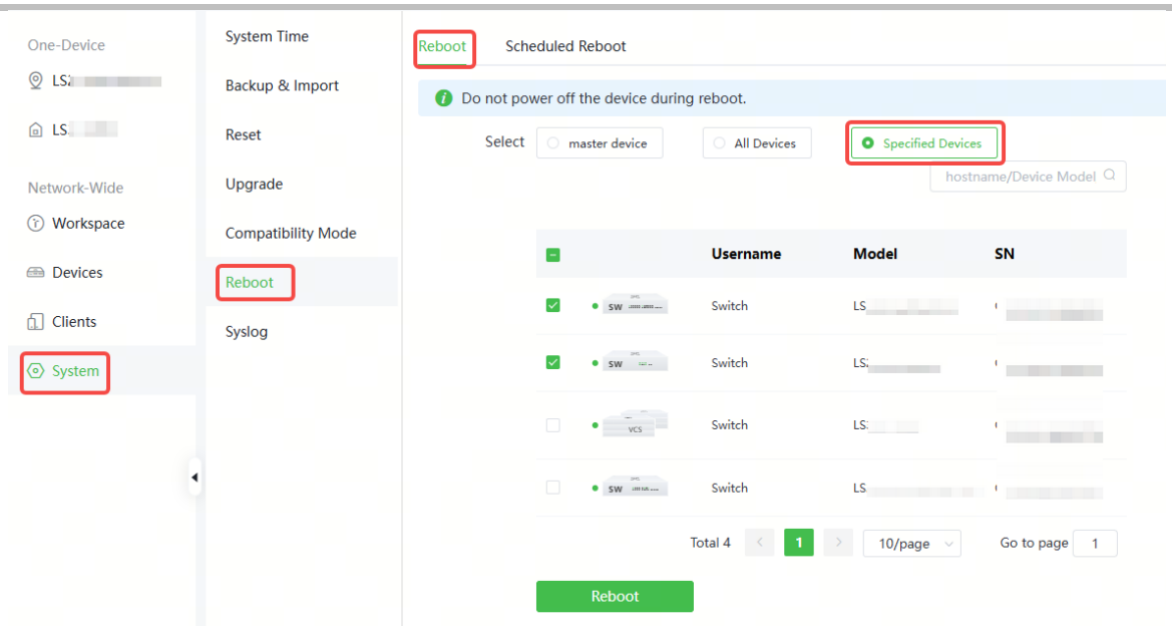
Caution

It will take some time for the network to reboot, please be patient. The network operation will affect the entire network. Therefore, exercise caution when performing this operation.

13.9.3 Rebooting Specified Devices in the Network

Choose **Network-Wide** > **System** > **Reboot** > **Reboot**.

Click **Specified Devices**, select desired devices from the **Available Devices** list, and click **Add** to add devices to the **Selected Devices** list on the right. Click **Reboot**. Specified devices in the **Selected Devices** list will be rebooted.



13.9.4 Configuring Scheduled Reboot

Confirm that the system time is accurate. For details about how to configure the system time, see 13.3 Setting the System Time. To avoid network interruption caused by device reboot at wrong time.

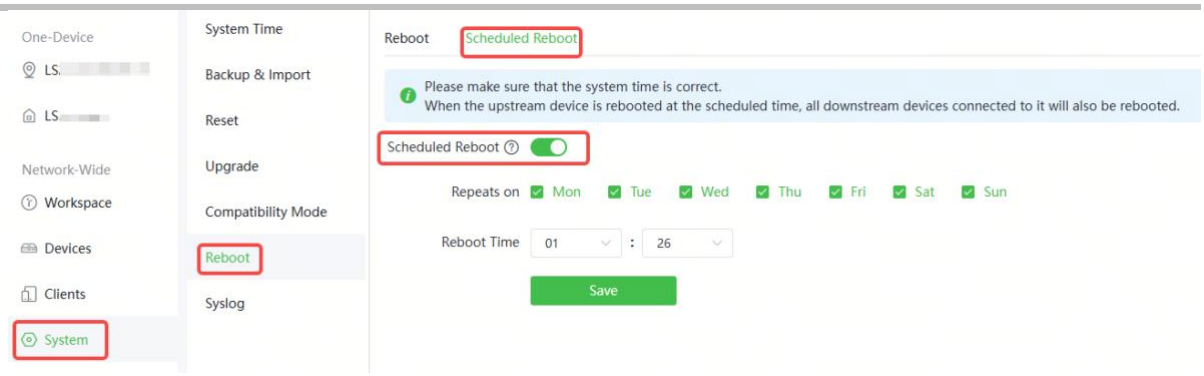
Choose **Network-Wide** > **System** > **Reboot** > **Scheduled Reboot**.

Choose **Local Device** > **System** > **Scheduled Reboot**.

Click **Enable**, and select the date and time of scheduled reboot every week. Click **Save**. When the system time matches the scheduled reboot time, the device will restart.

Caution

Once enable scheduled reboot in the network mode, all devices in the network will reboot when the system time matches to the timed time. Therefore, exercise caution when performing this operation.



13.10 Upgrade

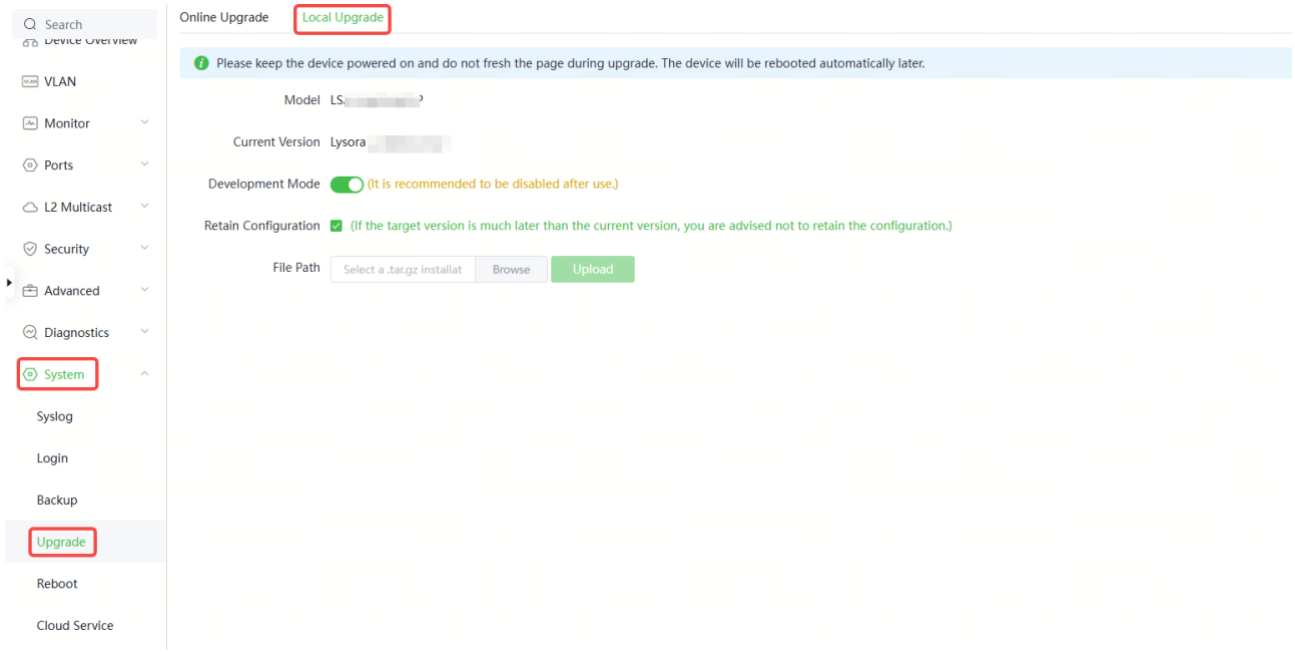
Caution

- It is recommended to back up the configuration before software upgrade.
- Version upgrade will restart the device. Do not refresh or close the browser during the upgrade process.

13.10.1 Local Upgrade

Choose **Local Device** > **System** > **Upgrade** > **Local Upgrade**.

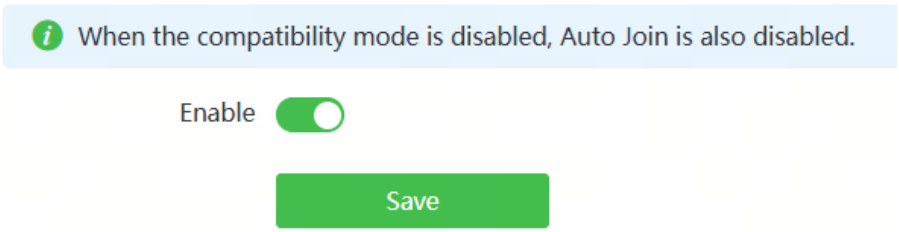
Displays the device model and current software version. You can choose whether to keep the configuration upgrade or not. Click **Browse** to select the local software installation package, click **Upload** to upload the installation package and upgrade.



13.11 Configuring the Compatibility Mode

Choose **Network-Wide** > **System** > **Compatibility Mode**.

Enabling compatibility mode can improve interoperability between devices running the early and latest versions during networking. If the compatibility mode is disabled, **Auto Join** will be disabled as well.



13.12 Cloud Service

13.12.1 Overview

The Cloud Service feature provides powerful remote network management and operation capabilities, making it convenient and efficient to manage geographically dispersed networks with diverse device types. This feature supports wireless devices, switches, and gateways, enabling unified network management and visualized monitoring and operation. Additionally, it also offers various components such as real-name authentication, dedicated Wi-Fi, and passenger flow analysis, allowing for flexible expansion of network services.

By configuring Cloud Service, you can conveniently mange networks through Lysora Cloud or the Lysora app.

13.12.2 Configuration Steps

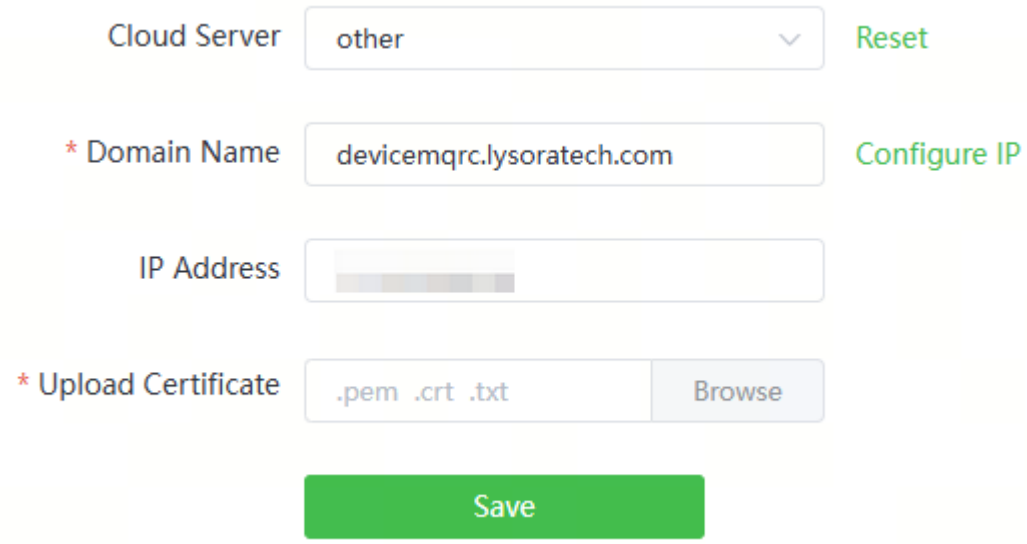
Choose **One-Device** > **Config** > **System** > **Cloud Service**.

If the device is not currently associated with a cloud account, simply follow the on-screen instructions to add it to the network. Open up the Lysora app, click the scan icon at the upper left corner on the **Project** page, and enter the device's management password.

Once the device is associated with a cloud account, it will automatically be bound to a cloud server based on its geographic location.

Caution

Exercise caution when modifying cloud service configurations as improper modifications may lead to connectivity issues between the device and the cloud service.



To change the Cloud Service configurations, select the cloud server from the **Cloud Server** drop-down list, enter the domain name and IP address, and click **Save**.

Note

If the server selected is not **Other**, the system automatically fills in the domain name and IP address of the cloud server. When **Other** is selected, you need to manually configure the domain name and IP address and upload the cloud server certificate.

Table 13-13 Cloud Server Description

Parameter	Description
Cloud Server	Geographic location of the cloud server.
Domain Name	Domain name of the cloud server.
IP Address	IP address of the cloud server.

13.12.3 Unbinding Cloud Service

Choose **One-Device** > **Config** > **System** > **Cloud Service**.

You can click **Unbind** to unbind the account if you no longer wish to manage this project remotely.