Ruijie Reyee RG-ES Series Switches 1.0(1)B1P52

Configuration Guide

Document Version: V1.0
Date: March 24, 2026

Copyright

Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms. Some or all of the products, services or features described in this document may not be within the scope of your purchase or use. Unless otherwise agreed in the contract, Ruijie Networks does not make any express or implied statement or guarantee for the content of this document.

The names, links, descriptions, screenshots, and any other information regarding third-party software mentioned in this document are provided for your reference only. Ruijie Networks does not explicitly or implicitly endorse or recommend the use of any third-party software and does not make any assurances or guarantees concerning the applicability, security, or legality of such software. You should choose and use third-party software based on your business requirements and obtain proper authorization. Ruijie Networks assumes no liability for any risks or damages arising from your use of third-party software.

Due to product version upgrades or other reasons, the content of this document will be updated from time to time. Ruijie Networks reserves the right to modify the content of the document without any notice or prompt.

This manual is for reference only. Ruijie Networks endeavors to ensure content accuracy and will not shoulder any responsibility for losses and damages caused due to content omissions, inaccuracies or errors.

Preface

Intended Audience

This document is intended for:

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

Technical Support

- Ruijie Reyee website: https://reyee.ruijie.com
- Online support center: https://reyee.ruijie.com/en-global/support
- Case portal: https://www.ruijie.com/support/caseportal
- Community: https://community.ruijie.com
- Email support: service_rj@ruijie.com
- Live chat: https://reyee.ruijie.com/en-global/rita

Conventions

1. GUI Symbols

Interface symbol	Description	Example
Boldface	1. Button names 2. Window names, tab name, field name and menu items 3. Link	1. Click **OK**. 2. Select **Config Wizard**. 3. Click the **Download File** link.
>	Multi-level menus items	Select **System** > **Time**.

2. Signs

The signs used in this document are described as follows:

Warning

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

Caution

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

Note

An alert that contains additional or supplementary information that if not understood or followed will not lead to serious consequences.

Specification

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

3. Note

This manual introduces the product model, port type and GUI for your reference. In case of any discrepancy or inconsistency between the manual and the actual version, the actual version prevails.

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.

1.1 1.0(1)B1P52

1.1.1 Hardware Change

The following table lists the hardware models supported by this version.

Table 1-1 Supported Hardware Models

Model	Hardware Version Number
RG-ES205GC-V2	1.0x
RG-ES207GS-AC-OD	1.0x
RG-ES207GS-HP	1.0x
RG-ES207GS-LP	1.0x
RG-ES207GS-PI-OD	1.0x
RG-ES207GS-P	1.0x
RG-ES208GC-V2	1.0x
RG-ES211GS-LP	1.0x
RG-ES211GS-P	1.0x
RG-ES216GC2MS	1.0x
RG-ES220GS-P-V2	1.0x
RG-ES224GC2MS	1.0x
RG-ES228GS-P-V2	1.0x

1.1.2 Software Feature Change

Note

New features refer to those supported from ESW_1.0(1)B1P52.

Table 1-2 Changed Features

Change Content	Change Description
Aggregate interface	The RG-ES2 series switches support port aggregation. For details, see 3.3 Port Aggregation.
Ping	The RG-ES2 series switches support the ping tool. For details, see 8.1 PING.
Perpetual PoE	The **Perpetual PoE** feature can be enabled on PoE switches to ensure an uninterrupted PoE power supply during a switch restart. For details, see 6.2.4 Perpetual PoE .
PoE Port Restart Scheduler	You can check the configuration status of the **PoE Port Restart Scheduler** feature on eWeb of the RG-ES2 series switches. For details, see 6.2.3 PoE.
PoE In	The RG-ES207GS-PI-OD switch can be powered through a PoE In port. When the switch adopts the power mode and the uplink Power Sourcing Equipment (PSE) provides insufficient power to support the PoE output of the switch, the PoE output will be unavailable. For details, see 6.2 PoE.
ERPS	The RG-ES2 series switches support Ethernet Ring Protection Switching (ERPS). For details, see 7 ERPS.
Encryption Mode	The **Encryption Mode(coaps)** feature can be configured to improve data transmission security. For details, see 8.2 Cloud Settings.

2 Login

2.1 Configuration Environment Requirements

- Google Chrome and Microsoft Edge are supported. Exceptions such as garbled characters or format errors may occur when other browsers are used.
- 1024 x 768 or a higher resolution is recommended. Exceptions such as font alignment errors and format errors may occur when other resolutions are used.

2.2 Connecting the Device

Connect the switch port with the network port of the PC through an Ethernet cable. Configure the PC to obtain an IP address automatically via DHCP, or manually assign a static IP address within the same subnet as the device, avoiding IP conflicts. Ensure that the PC can reach the switch using the ping command. For example, you can set the PC's IP address to 10.44.77.XXX (range: 1–254, excluding 200).

Table 2-1 Default Configuration

Feature	Default Setting
Device IP Address	10.44.77.200
Password	admin

2.3 Login to eWeb

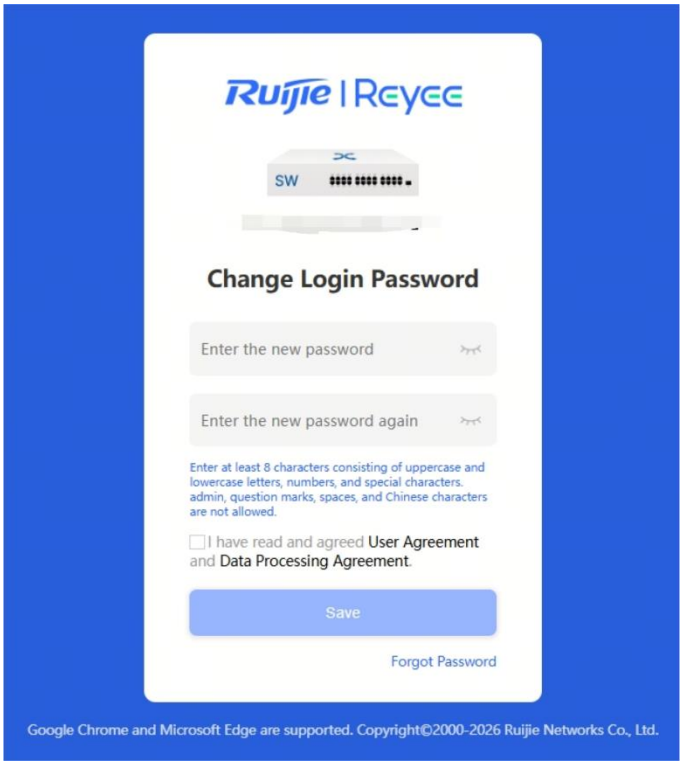
(1) Enter the IP address (10.44.77.200 by default) of the device in the address bar of the browser to access the login page.

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 device's eWeb as long as the PC and the device are on the same LAN, and their IP addresses are on the same network segment.

(2) (Optional) When logging in for the first time, set the login password and click **Save**.

Figure 2-1 Login to eWeb Upon the First Time

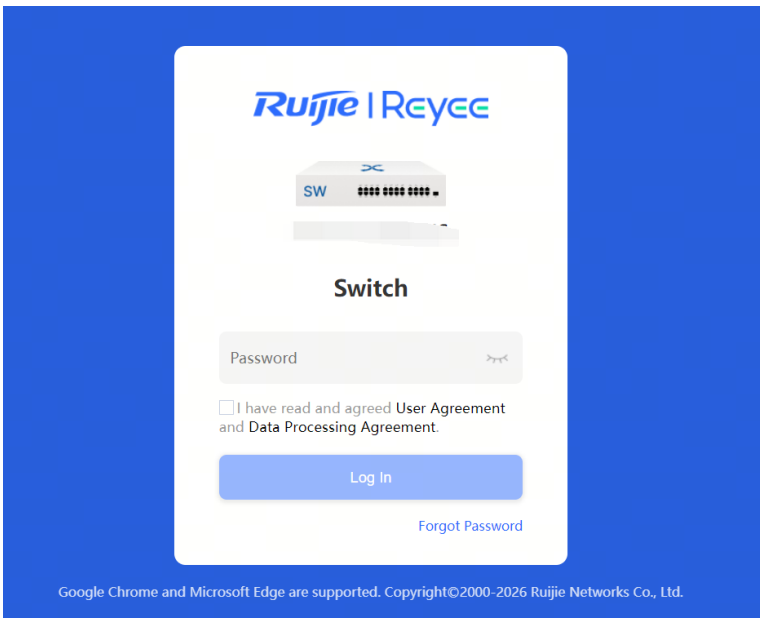


(3) On the login page, enter the password and click **Log In** to enter the homepage of eWeb.

Note

To change the login password, see 9.2 Login Password Settings.

Figure 2-2 eWeb Login Page



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

Caution

Restoring factory settings will clear all configurations on the device. Exercise caution when performing this operation.

3 Port Management

3.1 Managing Port Information

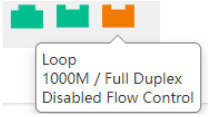
3.1.1 Port Status Bar

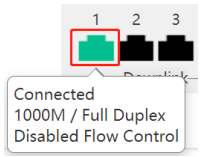
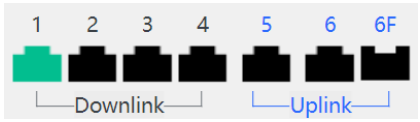
The port status bar is at the top of eWeb, showing the port ID, port attribute (uplink/downlink), connection status, and other information.

Figure 3-1 Port Status Bar

Different colors and shapes of the port icons represent different port statuses. See Table 3-1 for details. Move the cursor over a port icon and the port status will be displayed, including the connection status, port rate, duplex mode, and flow control status.

Table 3-1 Port Icons

Port Icon	Description
	The port icon is in the shape of a square, showing the port is a fiber port.
	The port icon is in the shape of an RJ-45 connector, showing the port is a copper port.
	The number in the lower right corner of the port icon shows a port number. This port icon indicates that the port is a member port of an aggregate interface.
	The color of the port icon is black, showing the port is disconnected.
	The color of the port icon is gray, showing the port is disabled and cannot receive or transmit packets.
	The color of the port icon is yellow, showing there is a loop.

Port Icon	Description
	The color of the port icon is green, showing the port is working normally.
	The number above the port icon is the port ID used to identify the device port. With the port ID, you can specify the target port.
	● The device port is classified into the uplink port and the downlink port. The uplink port is used to connect network devices in the upper layer and access the core network. The downlink port is used to connect the endpoints. ● When port isolation is enabled, the downlink ports of the device are isolated from each another, and they can only communicate with the uplink ports. For details, see 3.5 Port Isolation

3.1.2 Port Info Overview

Choose **Home** from the navigation page.

The **Home** page displays the global port information, including the port status, port VLAN settings, packet receiving/transmission rate (Rx/Tx rate), port isolation status, loop status, and port PoE settings. In addition, you can query and view information about downlink devices.

Click a port feature to go to the feature configuration page.

- Click **Port Status** to configure the basic port attributes. For details, see 3.2 Port Settings.
- Click **VLAN** to set the VLAN of the port. For details, see4.2 VLAN Settings.

Note

Port VLAN settings can only be configured and viewed in the **Port Info** pane after the **VLAN Settings** switch is toggled on.

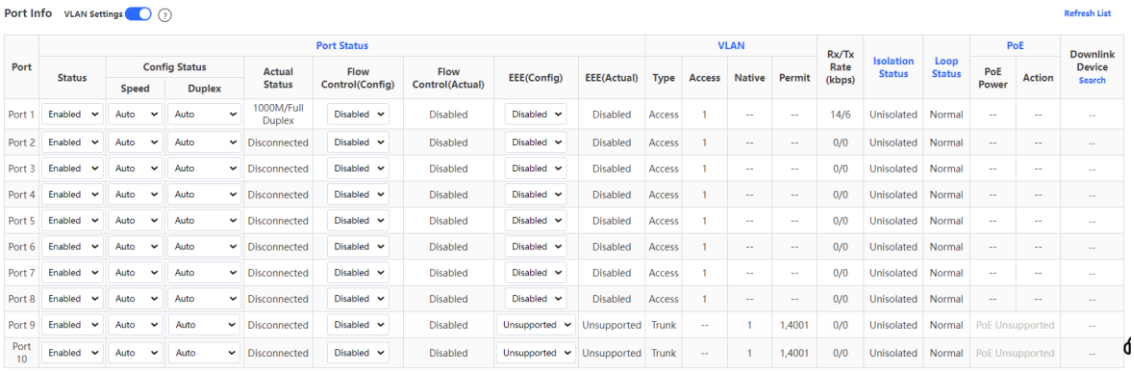
- Click **Isolation Status** to configure port isolation so that the downlink ports of the device are isolated from each other. For details, see 3.5 Port Isolation.
- Click **Loop Status** to enable loop guard function. After a loop occurs, the port causing the loop will be shut down automatically. For details, see 5.3 Loop Guard.
- Click **PoE** to view and set PoE parameters of the port. For details, see 6 PoE Settings.

Note

The PoE information will be shown in the port information list only when the devices support PoE.

- Click **Search** in the **Downlink Device** column to search for the downlink device of the selected port. After the search is done, click **View** to view the MAC address of the downlink device.
- Click **Refresh List** to fetch the latest port information.

Figure 3-2 Viewing or Configuring Port Settings



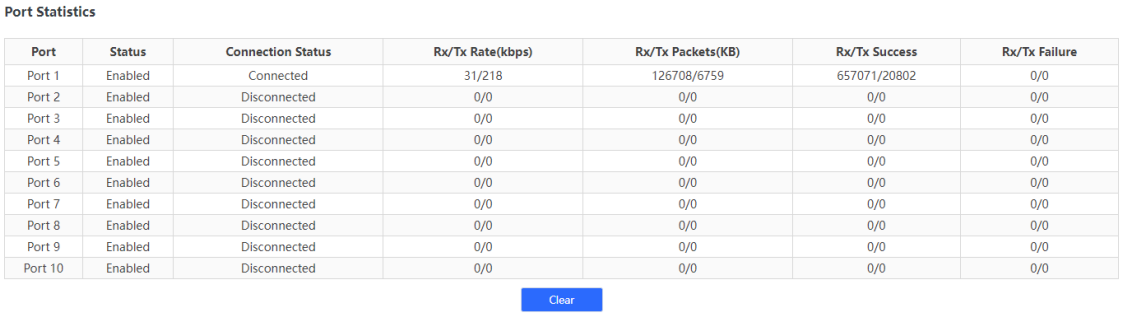
3.1.3 Port Packet Statistics

Choose **Monitoring** > **Port Statistics**.

The **Port Statistics** page displays the port status, the connection status, Rx/Tx rate (kbps), Rx/Tx packets (KB), Rx/Tx success, and Rx/Tx failure.

Click **Clear** to clear current packet statistics of all ports and reset the statistics.

Figure 3-3 Port Packet Statistics



3.2 Port Settings

Note

- Conditions for enabling Energy Efficient Ethernet (EEE): The local port is an RJ45 port, the port rate is 100 Mbps or 1000 Mbps, the duplex mode is set to **Auto**, and the EEE feature is enabled on the peer port.
- Optical ports do not support the EEE feature.

Choose **Configuration** > **Port Settings**.

You can set the basic attributes of the Ethernet ports in batches.

(1) Click **Select** in the **Port** column to display options of all device ports. Select the ports you want to configure.

(2) Set the feature parameters for the ports.

(3) Click **Save**.

The port list below provides the basic attributes of all ports and can also be used to verify whether the configuration of a specified port takes effect.

Caution

Shutting down all ports will make the switch unmanageable. Exercise caution when performing this operation.

Figure 3-4 Port Configuration and Status

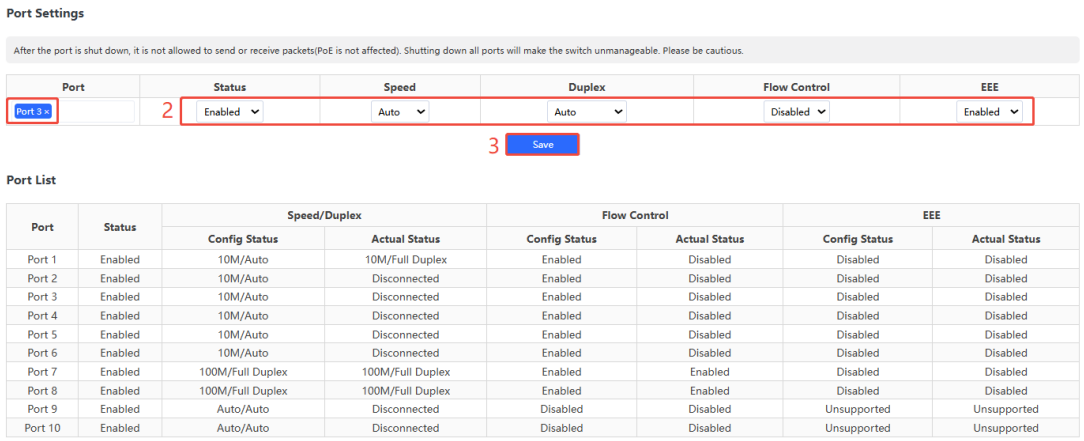


Table 3-2 Basic Port Configuration Parameters

Parameter	Description	Default
Port	Select the ports you want to configure.	No default value
Status	● **Enabled**: When the port is enabled, it can receive or transmit packets. ● **Disabled**: When the port is disabled, it cannot receive or transmit packets (The PoE feature of the ports will not be affected).	Enabled
Speed	Configure the operating speed of the Ethernet physical port. When the speed is set to **Auto**, it is determined by the auto-negotiation between the local port and the peer port. The negotiated speed can be any speed within the port capability.	Auto
Duplex	● **Full Duplex**: The port can receive packets while sending packets. ● **Half Duplex**: The port can receive or send packets at a time. ● **Auto**: The duplex mode of the port is determined by the auto-negotiation between the local port and the peer port.	Auto
Flow Control	When **Flow Control** is set to **Enabled**, the port will process the received flow control frames and send them when flow congestion occurs.	Disabled

Parameter	Description	Default
EEE	When Energy Efficient Ethernet (EEE) based on the IEEE 802.3az standard is enabled on an Ethernet port and the port is in idle state, it enters the Low Power Idle (LPI) mode, thereby achieving energy saving.	Disabled

3.3 Port Aggregation

3.3.1 Overview

1. Aggregate Interface Overview

An aggregate interface can bind multiple physical links to form a logical link, expanding link bandwidth and improving link reliability.

- Expanding link bandwidth: If a link between two devices supports a maximum bandwidth of 1,000 Mbps (assuming that 1,000 Mbps ports are used on both devices), and the service traffic carried by the link exceeds 1,000 Mbps, the excessive traffic will be discarded. Aggregate interfaces can be used to solve the issue. For example, use *n* Ethernet cables to connect the two devices and bind the ports together to become an aggregate interface. In this way, the aggregate interface supports the maximum traffic of 1000 Mbps x *n*.
- Improving link reliability: If the two devices are connected by only one Ethernet cable and the link is disconnected, services carried by the link will be interrupted. However, if the two devices are connected by multiple cables and the connected ports are aggregated, the service traffic can be transmitted properly as long as one link remains connected.

2. Static Aggregate Interfaces

A static aggregate interface is a logical interface configured by manually binding multiple physical ports. Each physical port is called a member port of the static aggregate interface. The static aggregate interface is easy to configure. You can add specified physical ports to the same static aggregate interface to aggregate multiple physical links. After a member port is added to a static aggregate interface, the port starts to send and receive data on the aggregate interface and is controlled by the load balancing algorithm configured on the aggregate interface.

3. Load Balancing

Link aggregation, based on packet features such as the source MAC address, destination MAC address, source IP address, destination IP address, Layer 4 source port number, and Layer 4 destination port number of packets received by an inbound interface, differentiates packet flows according to one or several combined algorithms. Link aggregation sends the same packet flow over the same member link, and evenly distributes different packet flows among member links. For example, in source MAC-based load balancing mode, packets are distributed to member ports of the aggregate interface based on the source MAC addresses of the packets. Packets with different source MAC addresses are evenly distributed among member ports, while those with the same source MAC address are forwarded through the same member port.

Load balancing is performed on aggregate interfaces based on the following packet features.

- Src & Dest MAC

- Src MAC
- Src IP
- Src L4 Port
- Src Port
- Dest MAC
- Dest IP Address
- Dest L4 Port
- Src & Dest IP Address
- Src & Dest L4 Port

3.3.2 Configuring a Static Aggregate Interface

Choose **Configuration** > **Port Aggregation**.

1. Adding an Aggregate Interface

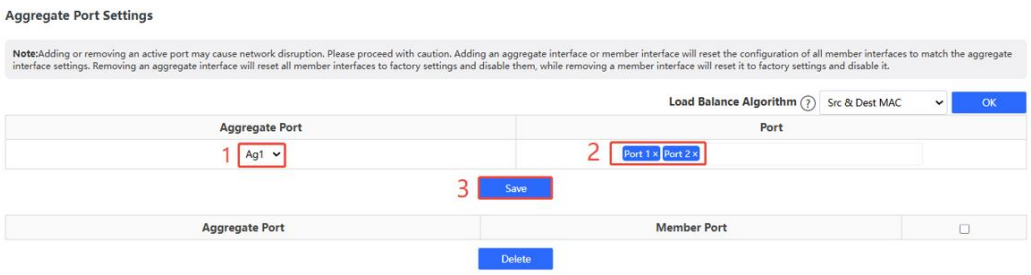
Note

- The maximum number of aggregate interfaces that can be created varies with the device model. Please refer to the maximum number shown on the configuration page.
- An aggregate interface contains a maximum of four member ports.
- Due to chip limitations, devices with 5–7 ports support a maximum of two aggregate interfaces. Aggregate interface 1 uses ports 1 to 4, while aggregate interface 2 uses ports 5 to 7. The actual member ports of aggregate interface 2 depend on the available physical ports. For example, if the device has only five ports, port 5 will be the only member port of aggregate interface 2. The switches with 5–7 ports include the RG-ES205GC-V2, RG-ES207GS-P, RG-ES207GS-LP, RG-ES207GS-HP, RG-ES207GS-AC-OD, and RG-ES207GS-PI-OD.
- The attributes of member ports must be consistent. An RJ45 port and an optical port cannot be aggregated.
- **Load Balance Algorithm** is set to **Src & Dest MAC** by default.

(1) Set Aggregate Port to Ag1 or Ag2.

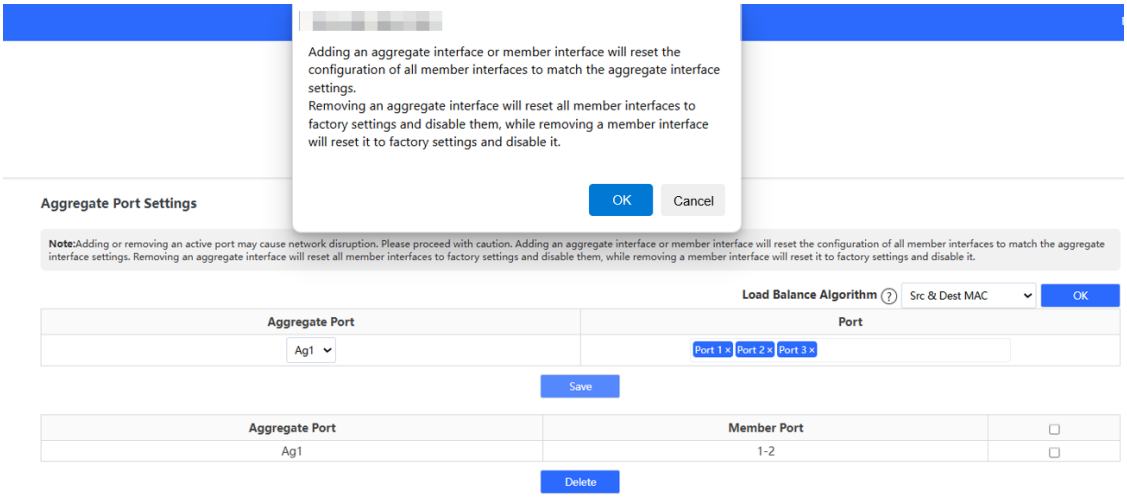
(2) Select member ports, each of which can be added to only one aggregate interface, and click **Save**.

Figure 3-5 Adding an Aggregate Interface



(3) Read the message in the pop-up window, and click **OK**.

Figure 3-6 Secondary Confirmation Pop-up Window for Adding an Aggregate Interface



Caution

- Exercise caution when configuring a running port as a member port of an aggregate interface, as this operation may cause network interruption.
- When an aggregate interface is added, the configuration of its member ports will be reset and the configuration of the aggregate interface is applied to them.

Information about the configured aggregate interfaces is displayed in the lower part of the page. You can also check the aggregate interface information in the port status bar at the top of the page.

Figure 3-7 Aggregate Interface Information in the Lower Part of the Page

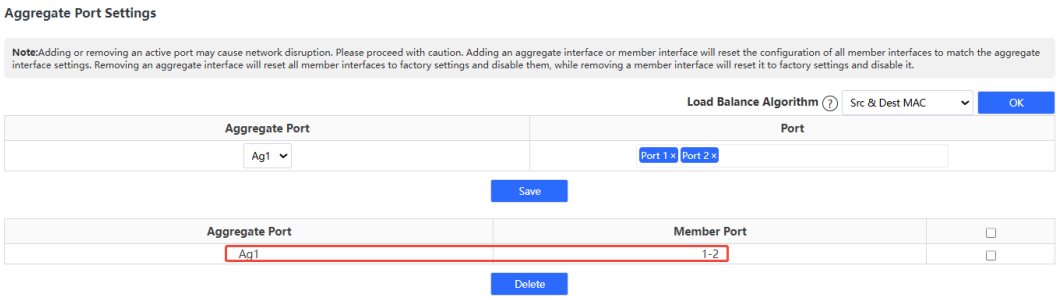


Figure 3-8 Aggregate Interface Information in the Port Status Bar at the Top of the Page

2. Modifying Member Ports of an Aggregate Interface

Caution

- You cannot select ports that have been added to other aggregate interfaces.
- When a member port is added to an aggregate interface, the configuration of the member port is reset and the configuration of the aggregate interface is applied to it.
- When a member port is removed from an aggregate interface, the port is restored to factory settings and disabled.

(1) Select the name of an aggregate interface whose member ports need to be modified. The member ports of the aggregate interface are automatically displayed.

(2) Click **Port**, and select or deselect member ports in the displayed drop-down list (adding member ports as an example).

(3) Click **Save**, read the message in the pop-up window, and click **OK**.

Figure 3-9 Modifying Member Ports of an Aggregate Interface

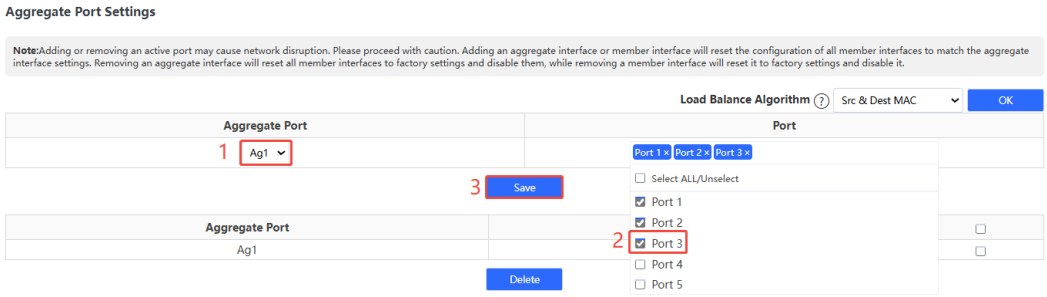
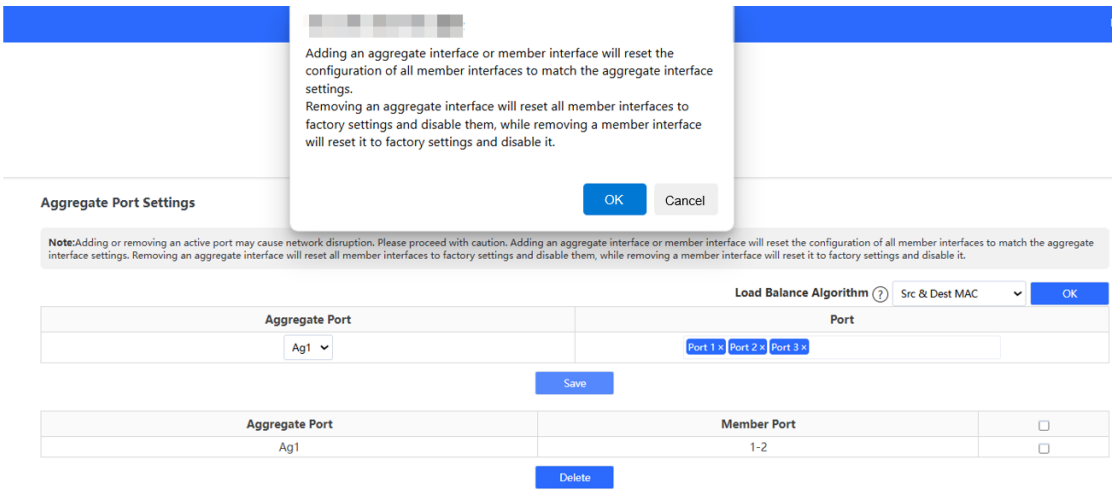
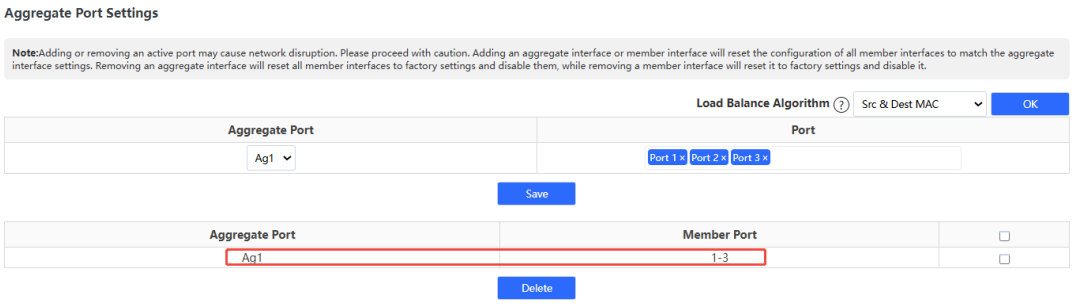


Figure 3-10 Secondary Confirmation for Modifying Member Ports



(4) Wait until the member ports of the aggregate interface are updated in the list below.

Figure 3-11 Succeeded in Modifying Member Ports of an Aggregate Interface



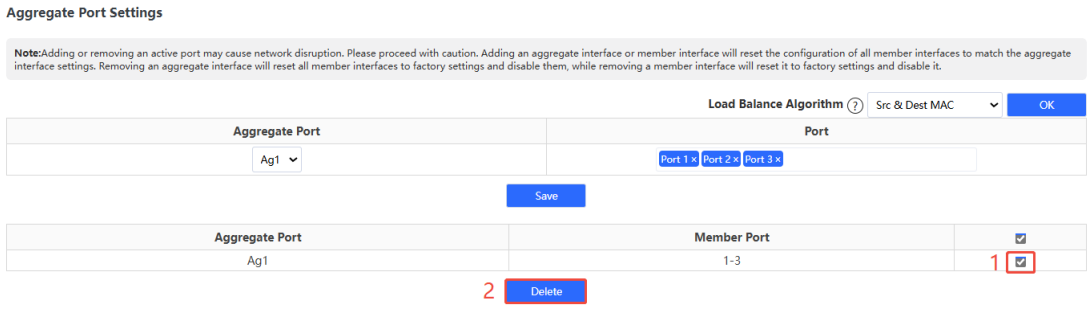
3. Deleting an Aggregate Interface

Select one or two aggregate interfaces to be deleted and click **Delete**. Read the message displayed on the pop-up window and click **OK** to confirm deletion.

Caution

- Exercise caution when deleting a running member port, as this operation may cause network interruption.
- When you delete an aggregate interface, its member ports are reset to factory settings and disabled.

Figure 3-12 Deleting an Aggregate Interface



3.3.3 Configuring Load Balancing Algorithms

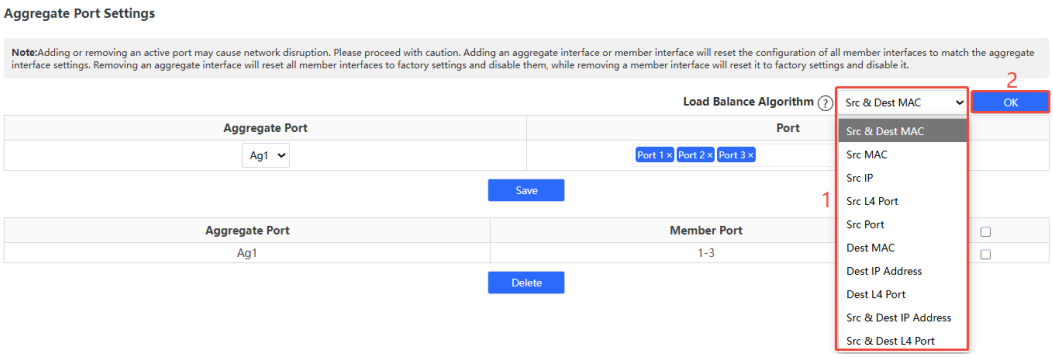
Choose **Configuration** > **Port Aggregation**.

Click **Load Balance Algorithm** in the upper right corner, select a load balancing algorithm from the drop-down list, and click **OK**. The device will distribute incoming packets of all aggregate interfaces according to the specified load balancing algorithm.

Caution

The load balancing algorithm takes effect globally. After configuration, it takes effect on all aggregate interfaces of the device.

Figure 3-13 Configuring a Load Balancing Algorithm for All Aggregate Interfaces



3.4 Port Mirroring

3.4.1 Overview

In network monitoring and troubleshooting scenarios, users need to analyze data traffic on suspicious network nodes or device ports. When port mirroring is enabled, packets received and transmitted on the source port will be mirrored to the mirror port (destination port). You can monitor and analyze the packets on the mirror port through network analyzer without affecting the normal data forwarding of the monitored device.

As Figure 3-14 shows, by configuring port mirroring on Device A, the packets on Port 1 are mirrored to Port 10. Though the network analyzer is not directly connected to Port 1, it can receive all packets on Port 1 and is able to monitor the data traffic on Port 1.

Figure 3-14 Operating Principle of Port Mirroring

3.4.2 Configuration Steps

Choose **Configuration** > **Port Mirroring**.

Select the source port, the monitoring direction, and the mirror port, and click **Save**. The device supports configuring one port mirroring rule.

If you want to delete port mirroring configuration, click **Delete**.

Caution

- You can select multiple source ports but only one mirror port. The source ports cannot contain the mirror port.
- Only one port mirroring rule can be configured. If multiple rules are configured, the latest configuration takes effect.

Figure 3-15 Configuring Port Mirroring

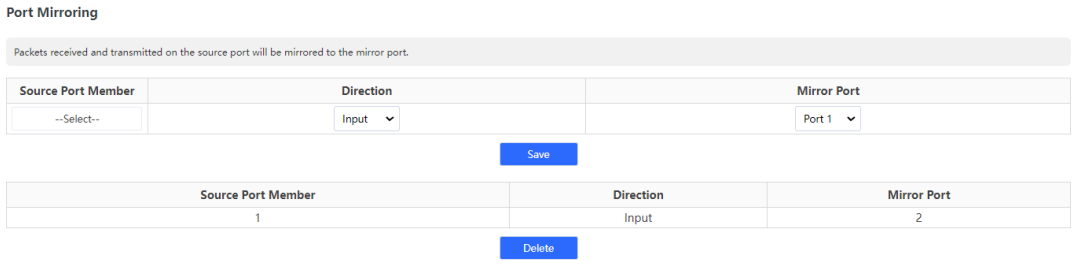


Table 3-3 Port Mirroring Parameters

Parameter	Description
Source Port Member	The source port is also called the monitored port. Packets on the source port will be mirrored to the mirror port for network analysis or troubleshooting. You can select multiple source ports. Packets on these ports will be mirrored to one mirror port.
Direction	Direction of the data traffic monitored on the source port: ● Bi-directions (input & output): All packets on the source port, including the received packets and the transmitted packets, will be mirrored to the mirror port. ● Input: The packets received by the source port will be mirrored to the mirror port. ● Output: The packets transmitted from the sourced port will be mirrored to the mirror port.
Mirror Port	The mirror port is also called the monitoring port. The mirror port is connected with a monitoring device, and it transmits packets on the source port to the monitoring device.

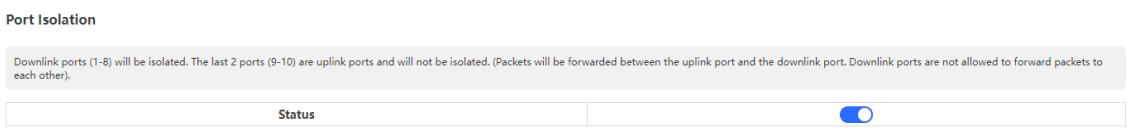
3.5 Port Isolation

Choose **Configuration** > **Port Isolation**.

Port isolation is used for isolating layer-2 packets. When port isolation is enabled, the downlink ports are isolated from each other but can communicate with uplink ports.

Port isolation is disabled by default. Toggle the switch to **On** to enable port isolation.

Figure 3-16 Port Isolation



Note

The number of the uplink/downlink ports and port IDs of different devices vary. Please refer to the specific device's documentation for accurate information.

3.6 Port-based Rate Limiting

Choose **QoS** > **Rate Limiting**.

You can configure rate limiting rules for packets in the input direction and the output direction of ports. There is no rate limiting on ports by default.

Select the port you want to configure, then select the rate limiting type and status, and enter the rate limit. Click **Save** to save the configuration. The configuration will be displayed accordingly in the **Port Rate** table right below the **Save** button.

Figure 3-17 Port Rate Limiting

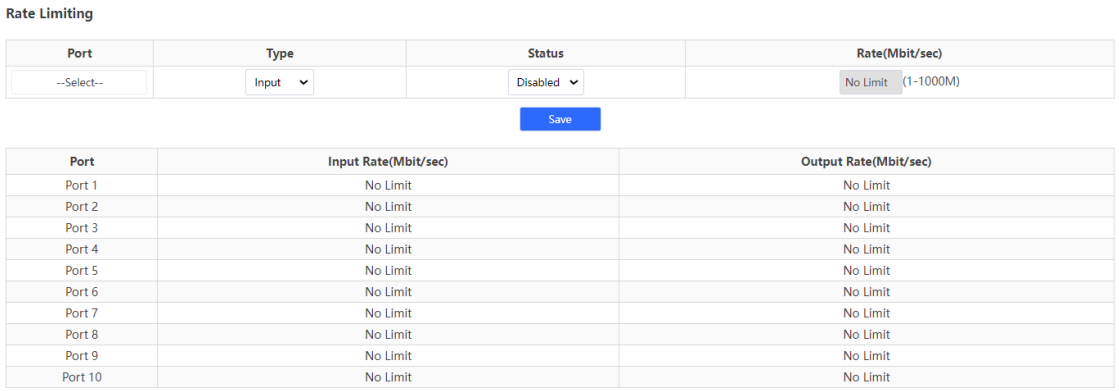


Table 3-4 Rate Limiting Parameters

Parameter	Description	Default
Port	You can select multiple ports for rate limiting configuration in batches.	No default value
Type	The direction of the rate-limited data traffic: ● Input & output: Rate limiting for all packets forwarded over the port, including the received packets and the transmitted packets. ● Input: Rate limiting for packets received by the port. ● Output: Rate limiting for packets transmitted from the port.	No default value
Status	You can decide whether to enable or disable rate limiting.	Disabled
Rate (Mbit/sec)	The maximum rate at which packets are forwarded over the port.	No Limit

Note

The port rate limit range varies with the switch model.

3.7 Management IP Address

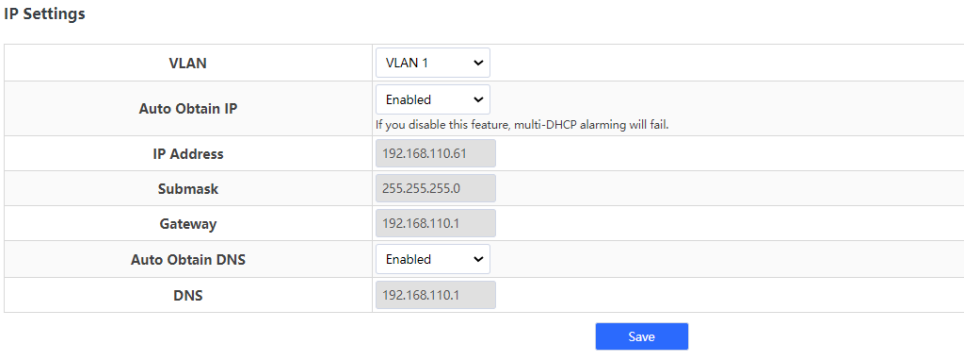
Choose **Configuration** > **IP Settings**.

You can configure the management IP address of the device. By accessing the management IP address, you can configure and manage the device.

- There are two methods for obtaining IP addresses:
  - Dynamic IP address: Enable **Auto Obtain IP** to use the IP address assigned dynamically by the uplink DHCP server.

    If you enable **Auto Obtain IP**, the device automatically obtains various parameters from the DHCP server. You can select whether to obtain the DNS address from the DHCP server. If you disable **Auto Obtain DNS**, you need to manually set the DNS server address.
  - Static IP address: Disable **Auto Obtain IP** to use the fixed IP address configured manually by the user. If **Auto Obtain IP** is disabled, you need to manually enter the IP address, subnet mask, gateway IP address, and DNS server address. Click **Save** to enforce the configuration.
- **VLAN** is used for managing VLAN tag of the management packets. If VLAN settings are disabled, the management packets will be untagged, and management VLAN configuration is not supported. The management VLAN of the device is VLAN 1 by default.

Figure 3-18 IP Settings



Note

- Disable VLAN settings, and the management packets will be untagged. If you want to tag packets, please enable VLAN settings. For details, see 4.2.1 Global VLAN Settings.
- The management VLAN must be selected from the existing VLANs. To create a static VLAN, refer to 4.2.2 Static VLANs Settings.
- You are advised to bind a configured management VLAN to an uplink port. Otherwise, you may fail to access the web interface. For details, see 4.2.3 Port VLAN Settings.
- If you disable **Auto Obtain IP** feature, multi-DHCP alarming will fail. For details about multi-DHCP alarming, see 10.2 Multi-DHCP Alarming.

4 Switch Settings

4.1 Managing MAC Address

4.1.1 Overview

The MAC address table records mappings of MAC addresses and ports to VLANs.

The 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 port specified by the entry in unicast mode. If the device does not find such an entry, it forwards the packet through all ports other than the receiving port in broadcast mode.

MAC address entries are classified into the following types:

- **Static MAC** address entries: Static MAC address entries are manually configured by the users. Packets whose destination MAC address matches the one in such an entry are forwarded through the corresponding port.
- **Dynamic MAC address entries**: Dynamic MAC address entries are learned dynamically by the device. They are generated automatically by the device.

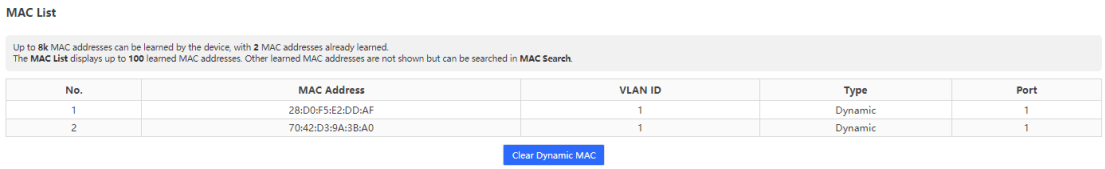
4.1.2 Viewing MAC Address Table

Choose **Configuration** > **MAC List**.

This page displays the MAC address of the device, including the static MAC address configured manually by the users and the dynamic MAC address learned automatically by the device.

Click **Clear Dynamic MAC** to clear the dynamic MAC address learned by the device. The device will re-learn the MAC address and generate a MAC address table.

Figure 4-1 MAC Address Table



Note

- If you disable VLAN, the device will forward packets according to only the destination MAC address. VLAN ID is not displayed in the MAC address table.
- Up to 100 MAC addresses are displayed.

4.1.3 Searching for MAC Address

Choose **Configuration** > **MAC Search**.

You can search for MAC address entries according to MAC address and VLAN ID.

Caution

If you disable VLAN, the VLAN ID will not be recorded in the MAC address table.MAC address entries can only be found through MAC address.

Enter MAC address and VLAN ID, and then click **Search**. The MAC address entries that meet the search criteria will be displayed in table right below the **Search** button. Moreover, you can enter partial characters of the MAC address for fuzzy search.

Figure 4-2 Searching for MAC Addresses (with VLAN Enabled)

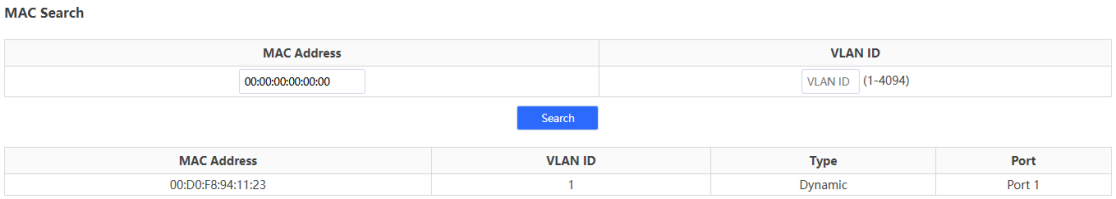
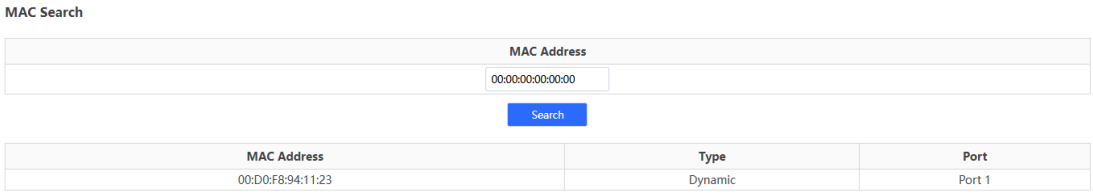


Figure 4-3 Searching for MAC Addresses (with VLAN Disabled)



4.1.4 Configuring Static MAC Address

Choose **Configuration** > **Static MAC**.

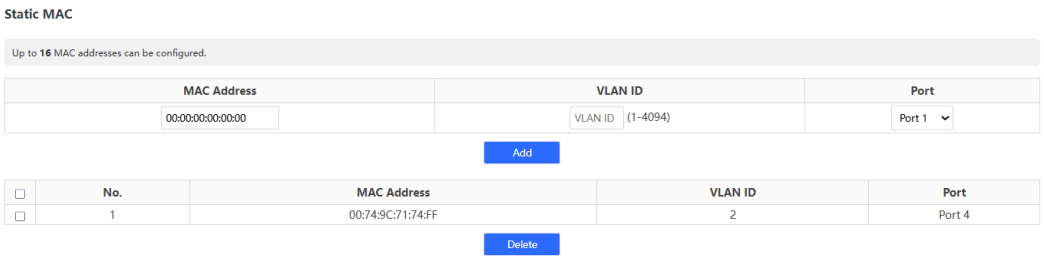
By configuring a static MAC address, you can manually bind the MAC address of a downlink network device with a port of the switch. After you add a static MAC address, when the device receives a packet destined to this address from VLAN, it forwards the packet to the specified port.

Caution

If you disable VLAN, the VLAN ID will not be recorded in the MAC address table. It is not allowed to configure a VLAN to which the static MAC address belongs.

Enter a MAC address, specify a VLAN ID and select the outbound port. Then click **Add** to add a static MAC address. The MAC address entries will be updated accordingly in the MAC address table.

Figure 4-4 Configuring Static MAC Address



If you want to delete a static MAC address, select the MAC address entry you want to delete in the table and click **Delete**.

4.2 VLAN Settings

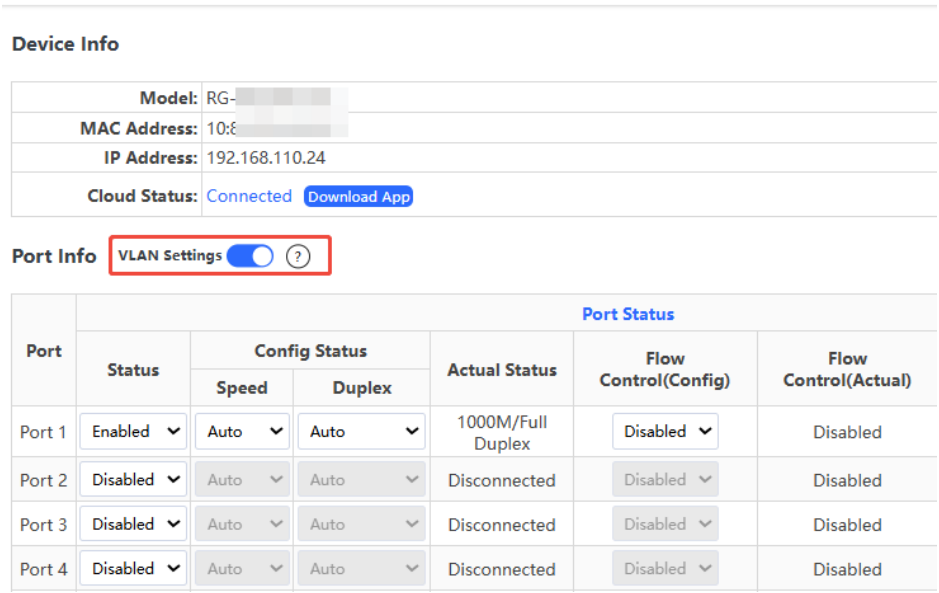
4.2.1 Global VLAN Settings

Choose **Home** from the navigation page.

This page displays the status of VLAN settings. You can toggle on or off **VLAN Settings**.

- When VLAN is disabled, the device operates like an un-managed switch. The device forwards packets according to the destination MAC address, and the VLAN information of the forwarding packets remains unchanged during the forwarding process.
- When VLAN is enabled, the device operates like a managed switch. The device forwards packets according to the destination MAC address and VLAN ID. You can configure the port mode (access or trunk) based on whether a VLAN tag is carried in packets. Besides, all device ports will be initialized to access ports.

Figure 4-5 VLAN Settings



Note

Apart from choosing **Home** from the navigation page, you can also choose **VLAN** > **VLAN List** or **VLAN** > **VLAN Settings** to toggle on or off **VLAN Settings**. Configuration through three paths has the same effects and takes effect instantly for all the paths.

4.2.2 Static VLANs Settings

Choose **VLAN** > **VLAN List**.

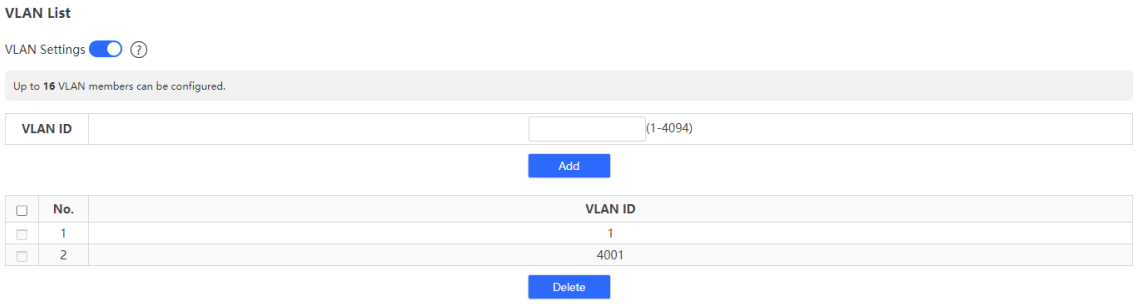
Enter VLAN ID and click **Add** to create a static VLAN.

Note

- You can create static VLANs only when **VLAN Settings** is toggled on.
- The VLAN ID ranges from 1 to 4094. VLAN 1 is the default VLAN.
- The maximum number of static VLANs that can be created varies with the device model. Please refer to the maximum number shown on the configuration page.
- The Management VLAN (VLAN 1), Native VLAN, Permit VLAN, and Access VLAN cannot be deleted.

The VLAN table contains the existing VLANs. Select the VLANs and click **Delete**, and the corresponding VLANs will be deleted. VLAN 1 cannot be deleted.

Figure 4-6 Static VLANs Settings



4.2.3 Port VLAN Settings

Caution

Improper configuration of VLANs on a port (especially uplink port) may cause the failure to log in to eWeb. Therefore, exercise caution when configuring VLANs.

Choose **VLAN** > **VLAN Settings**.

Configure the port mode and VLAN members of a port, and you will know the allowed VLANs of the port and whether the packets forwarded by the port carry tags.

(1) Select the target ports. Multiple ports can be selected.

(2) Configure the port type.

- Access: If the port is an access port, select **Access** for the port.

- Trunk: If the port is a trunk port, select a native VLAN for the port, and enter the VLAN ID range of permit VLANs.

(3) Click **Save**.

The configured port information is synchronized to the table on the **VLAN Settings** page.

Note

- You are advised to create VLAN members (refer to 4.2.2 Static VLANs Settings) before configuring the port based on VLANs. Click **VLAN List** to access the **VLAN List** page where you can add VLAN members.
- You can configure VLANs on ports only when **VLAN Settings** is toggled on.
- VLAN configuration is disabled on the RG-ES series switches by default.

Figure 4-7 Configuring Port VLANs

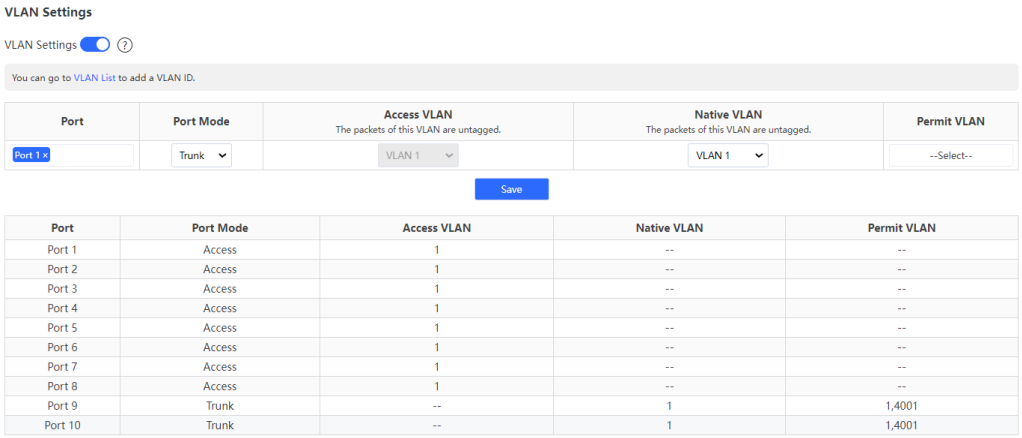


Table 4-1 Port Modes

Port Mode	Description
Access	● One access port can belong to only one VLAN and allow frames from this VLAN only to pass through. This VLAN is called an access VLAN. ● The frames from the access port do not carry VLAN tag. 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. ● Access port is connected to the endpoints.
Trunk	● One trunk port supports one Native VLAN and several Permit VLANs. Native VLAN frames forwarded by a trunk port do not carry tags while Permit VLAN frames forwarded by the trunk port carry tags. Trunk port is connected to switches. ● You can set the Permit VLAN range to limit VLAN frames that can be forwarded. ● Make sure the trunk ports at the two ends of the link are configured with the same Native VLAN.

5 Security

5.1 DHCP Snooping

5.1.1 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.

5.1.2 Configuration Steps

Choose **Configuration** > **DHCP Snooping**.

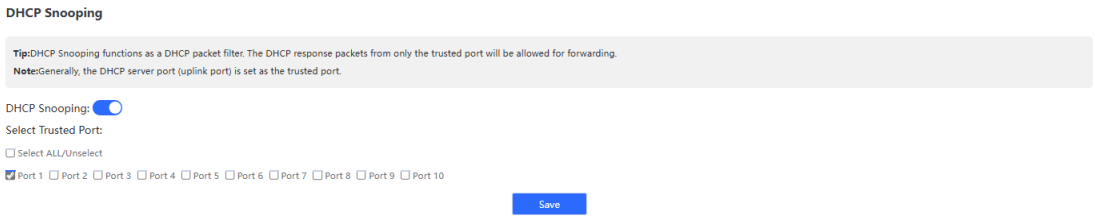
Toggle the switch to **On** to enable DHCP snooping, select the trusted ports, and then click **Save**.

When DHCP snooping is enabled, response packets are forwarded from only trusted ports of the DHCP servers.

Caution

The uplink port connected to the DHCP server is configured as the trusted port generally.

Figure 5-1 DHCP Snooping



5.2 Storm Control

5.2.1 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 situation is called a LAN storm, which may be caused by topology protocol execution errors or incorrect network configuration.

You can perform storm control separately for the broadcast, unknown multicast, and unknown unicast data flows. When the rate of broadcast, unknown 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.

5.2.2 Configuration Steps

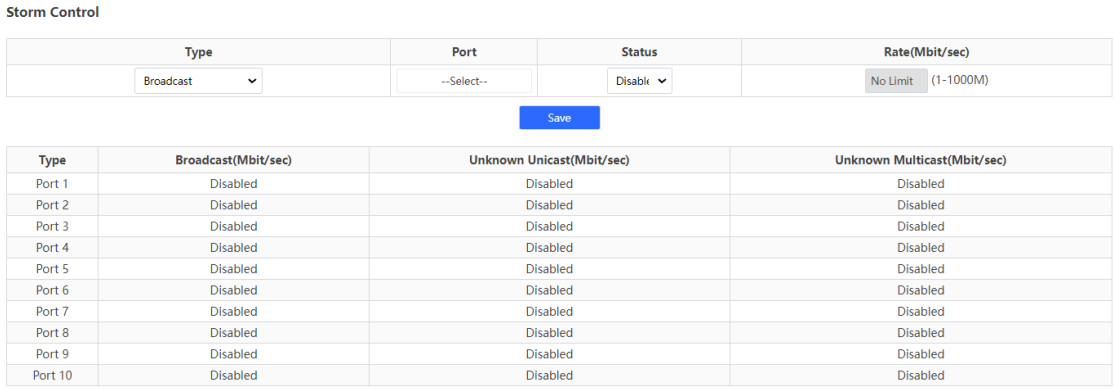
Choose **QoS** > **Storm Control**.

Select the storm control type, port, status, and enter the rate limit, and then click **Save**.

Figure 5-2 shows the storm control types and corresponding rates on device ports.

- When storm control is enabled, the corresponding rate limits will be displayed.
- When storm control is disabled, the rate of broadcast, unknown multicast, and unknown unicast data flows is not limited. The corresponding status is displayed **Disabled**.

Figure 5-2 Storm Control



5.3 Loop Guard

Choose **Monitoring** > **Loop Prevention**.

When loop guard feature is enabled, the port causing the loop will be shut down automatically. After the loop is removed, the port will be up automatically. The loop guard feature is enabled by default.

Figure 5-3 Loop Prevention

6 PoE Settings

Specification

- In Table 1-1, switch models with the suffixes -P, -LP, or -HP, such as RG-ES207GS-P, support PoE.
- The RG-ES207GS-AC-OD and RG-ES207GS-PI-OD also support PoE.

6.1 PoE Information

The devices supply power to powered devices (PDs) through PoE ports. On the PoE Info page, you can view the total power, used power, remaining power, and current work status of the PoE system.

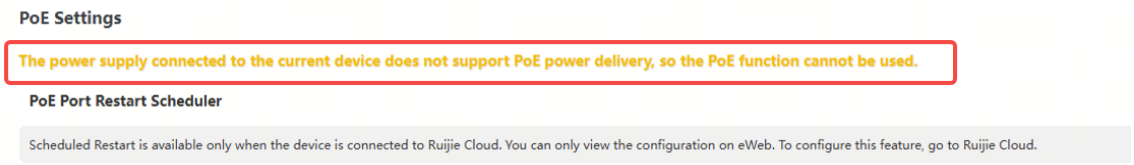
6.2 PoE Settings

6.2.1 PoE In Settings

The RG-ES207GS-PI-OD can be powered through a DC power cord or through port 5 from an uplink Power Sourcing Equipment (PSE) using an Ethernet cable.

- When the switch is powered only by DC and port 5 is not connected to a PSE, the PoE function of the switch is unavailable. The following notification is displayed on the web interface, as shown in Figure 6-1.

Figure 6-1 Figure 1-1 PoE Unavailable Notification



- When the switch is powered by both DC power and PoE input, PoE input takes precedence over DC power.
- When the RG-ES207GS-PI-OD is powered by PoE input, its PoE output capability (PoE budget) depends on the PoE input power. For details, see Table 6-1.

Table 6-1 Relationship Between PoE Input Power and PoE Budget

PoE Input Power	PoE Budget
90 W (PoE++)	60 W
60 W (PoE++)	40 W
30 W (PoE+)	19 W
15.4 W (PoE)	6 W

< 15.4 W	The RG-ES207GS-PI-OD continuously attempts to supply power to the downlink PDs, but fails to do so properly.

6.2.2 PoE watchdog

PoE watchdog: This feature is mainly applicable to Closed-Circuit Television (CCTV) scenarios for security purposes. 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.

Note

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

Table 6-2 PoE Watchdog Application Description

Packet Receiving Status of the PoE Port	Whether PoE Watchdog is Enabled	Action Taken on the PD
During the ping interval, a PoE port of the device suddenly stops receiving packets.	Yes	Restart the PD to restore normal operation and reset the ping interval.
	No	No action is initiated on the PD.
During the ping interval, a PoE port of the device stops receiving packets all the time.	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	Reset the ping interval.
	No	No action is initiated on the PD.

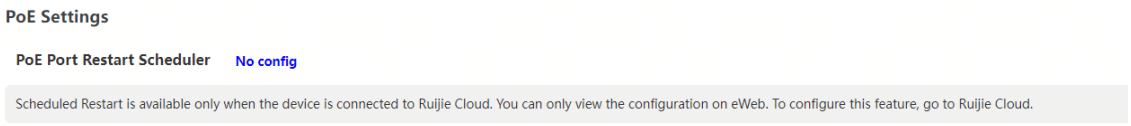
6.2.3 PoE Port Restart Scheduler

The **PoE Port Restart Scheduler** feature allows the network administrator to configure a scheduled restart plan for one or more PoE ports on Ruijie Cloud or Ruijie Reyee App. The system automatically cuts off and restores PoE power supply to specified ports according to the preset time (accurate to minutes, range: 00:00 to 23:59), thereby restarting downlink PDs remotely and automatically to restore their optimal operation.

Note

- Only one scheduled restart policy can be configured.
- You can configure this feature only on Ruijie Cloud or Ruijie Reyee App. The eWeb interface only allows you to view the configuration status.

Figure 6-2 PoE Port Restart Scheduler Is Not Configured

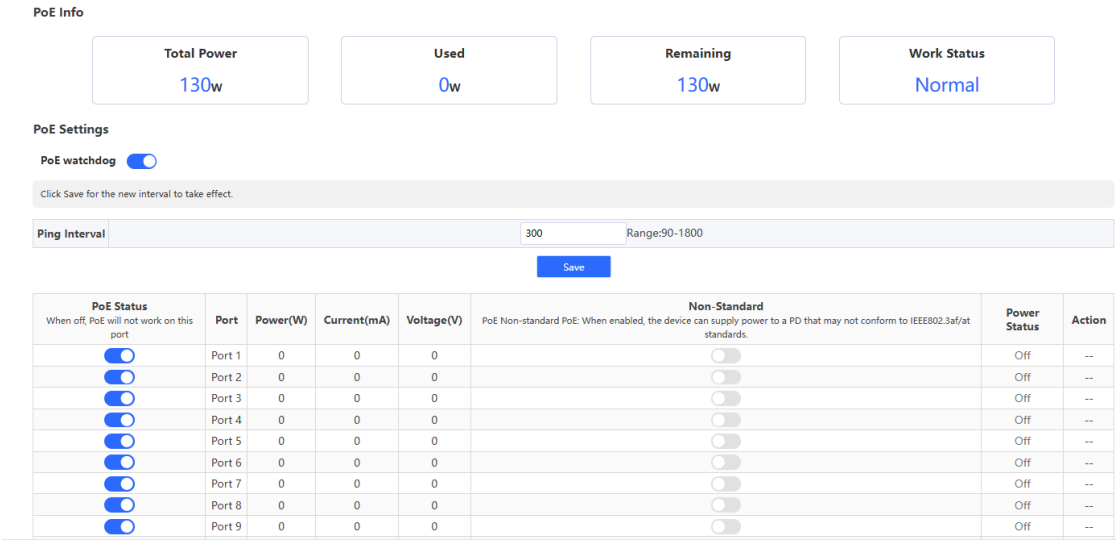


6.2.4 Perpetual PoE

The **Perpetual PoE** feature ensures that the switch supplies uninterrupted power to connected PDs during a switch restart (for example, during a firmware upgrade). This feature is enabled by default.

Port status

- The voltage, current, output power, and current power status of the device ports are displayed.
- You can toggle on or off PoE Status to enable or disable the PoE feature. When PoE is disabled, the port will not supply power to PDs.
- When the switch needs to supply power to a PD that does not comply with IEEE 802.3af/at, you can toggle on Non-Standard.



7 ERPS

Specification

This feature is supported only on optical ports of switches, such as RG-ES207GS-AC-OD, RG-ES207GS-PI-OD, RG-ES216GC2MS, RG-ES224GC2MS, RG-ES220GS-P-V2, and RG-ES228GS-P-V2.

7.1 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.

7.2 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.

7.3 Basic Model of an Ethernet Ring

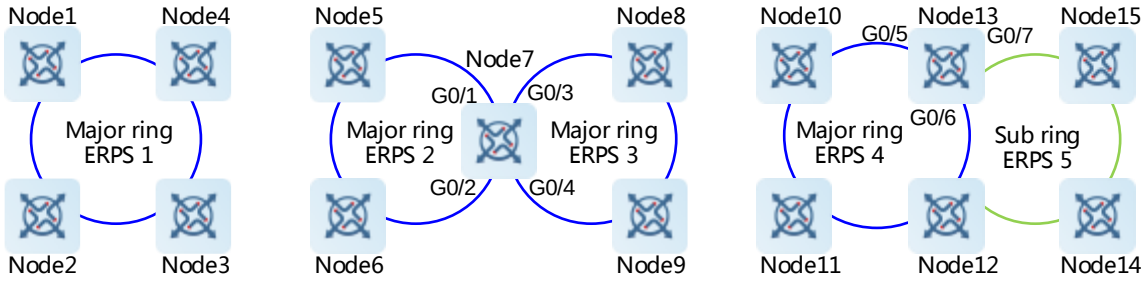
A group of interconnected devices in the same control VLAN (R-APS VLAN) constitute an Ethernet ring (ERPS ring), in which each device is called a node. ERPS rings can be classified into major rings and subrings based on whether a ring is closed.

7.3.1 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 7-1. 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 7-1. 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 7-1, 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 7-1 Basic Topologies of Ethernet Rings



7.3.2 Basic Topologies

Major rings, subrings, and nodes can form basic topologies with different characteristics, depending on the connection modes, as shown in Figure 7-1.

- 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.

7.3.3 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 7-1, 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 7-1, 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 7-1, 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.

7.3.4 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 7-1:

- 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 7-1.

Table 7-1 ERPS 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

7.4 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.

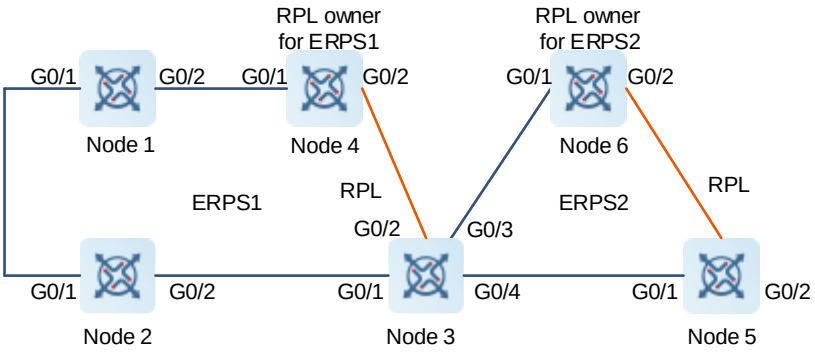
Ring protection link (RPL): When the physical links in a ring network are connected, the ERPS ring is in the idle state, and the links in the logic blocking state are RPLs. Each Ethernet ring has only one RPL. For example, the links indicated by the orange lines shown in Figure 7-2 are RPLs, the link 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 7-2, 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 7-2, nodes except node 4 and node 6 are non-RPL owner nodes of the rings.

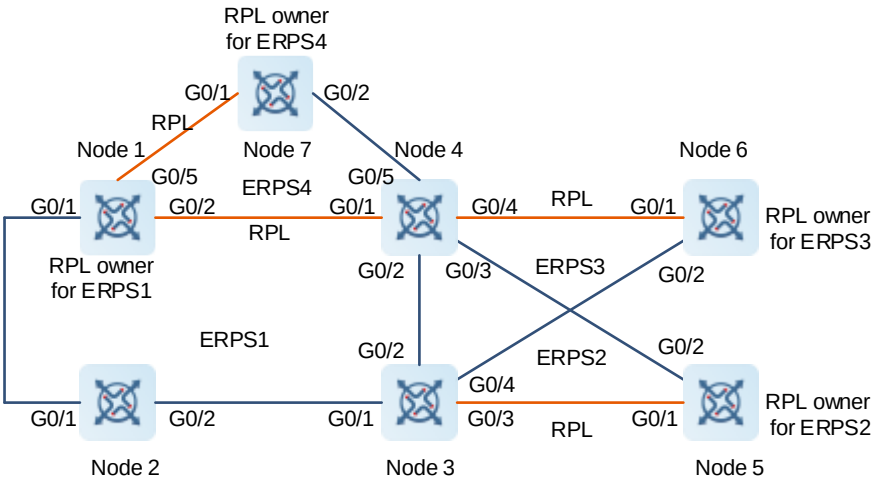
Blocked ports on RPLs are RPL ports, and RPL ports do not forward data packets to prevent loops. RPL ports are on RPL owner nodes, and the RPL owner nodes block the RPL ports. Each Ethernet ring has only one RPL owner node.

Figure 7-2 Typical Topology of Tangent Rings



As shown in Figure 7-2, 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 7-3 Typical Topology of Intersecting Rings



As shown in Figure 7-3, 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.

7.5 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.

7.6 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.

7.7 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.

7.8 Protocols and Standards

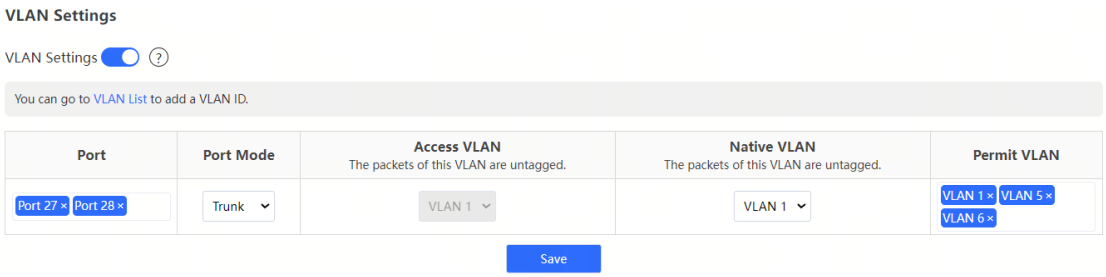
ITU-T G.8032/Y.1344: Ethernet ring protection switching

7.9 Configuring ERPS

7.9.1 Prerequisites

Choose **VLAN** > **VLAN Settings**.

Before configuring ERPS, configure all optical ports of the device as trunk ports and configure **Permit VLAN**.



7.9.2 Adding and Deleting an ERPS Ring

Choose **ERPS** > **Ring Configuration**.

Configure ring parameters based on service requirements.

Note

- After a port role is changed, remove and reconnect the cable for the port configuration to take effect.
- A maximum of one ERPS ring can be configured.

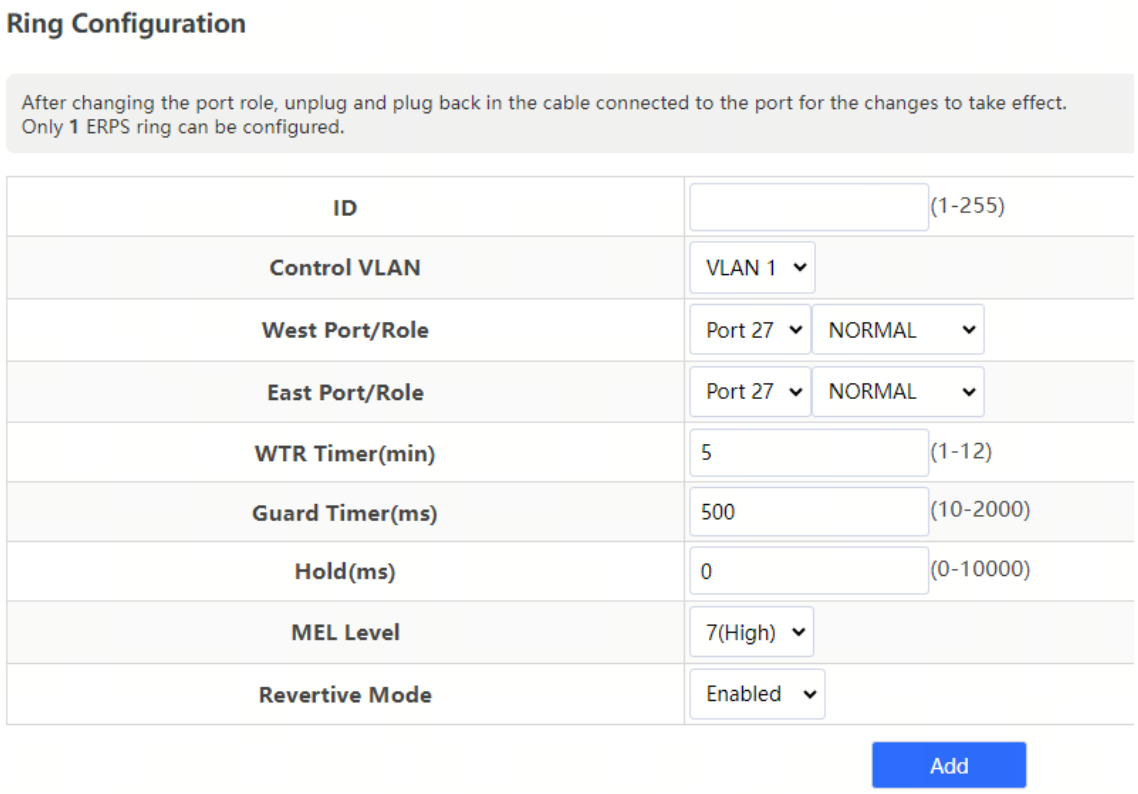


Table 7-2 Parameters of Adding an ERPS Ring

Parameter	Description	Default Value
ID	Specifies the ID of an ERPS instance, ranging from 1 to 255.	N/A
Control VLAN	It is used to forward ERPS packets.	N/A
West Port/Role	Specifies the west port in the ERPS ring and the port 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 the port 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
WTR timer(min)	Specifies the interval of the WTR timer. The duration ranges from 1 minute to 12 minutes.	Five minutes
Guard Time(ms)	Specifies the interval of the Guard timer. The duration ranges from 10 ms to 2,000 ms.	500 ms

Parameter	Description	Default Value
Hold(ms)	Specifies the interval of the Hold-off timer. The duration ranges from 0 ms to 10,000 ms. The value 0 indicates that topology switching is performed immediately after a link failure is detected.	0 ms
MEL Level	Indicates the maintenance entity group (MEG) level. The MEL level of devices in the same ERPS ring must be consistent. The value ranges from 1 to 7.	7
Revertive Mode	When it is set to **Enabled** and the link failure is cleared, traffic is blocked on the RPL.	Enabled

7.9.3 Link Switch

Choose **ERPS** > **Link Switch**.

Configure link switching parameters based on service requirements.

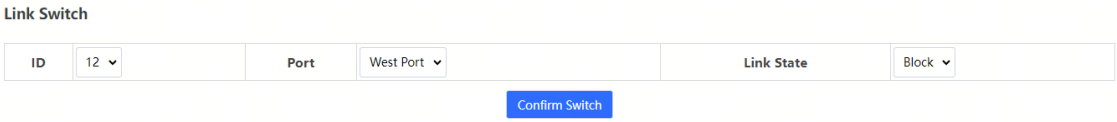


Table 7-3 Parameter Description

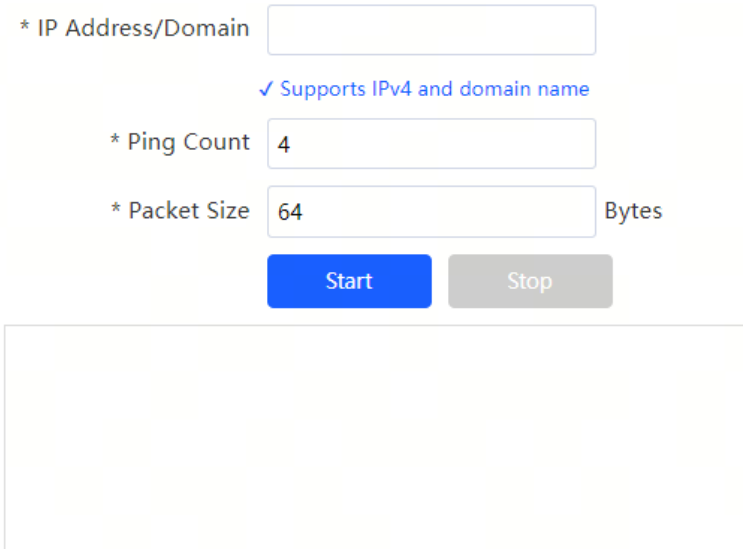
Parameter	Description	Default Value
ID	Specifies the ID of an ERPS instance.	N/A
Port	Specifies the port in the ERPS ring. The values include **West Port** and **East Port**.	N/A
Link State	Specifies the link state of the selected port. The values include **Clear** and **Block**. ● **Clear**: Indicates that the port is elected and blocked automatically through protocol negotiation rather than by manual switching. ● **Block**: Indicates that the port is blocked by manual switching.	N/A

8 Toolkit

8.1 PING

Choose **Toolkit** > **Ping Tool**.

The ping tool checks network connectivity. Set a destination IP address or domain name, ping count, and packet size, and click **Start** to test the network connectivity between the device and the IP address or domain name. If the prompt **Ping failed. Please check the network** is displayed, the device cannot reach the IP address or domain name.



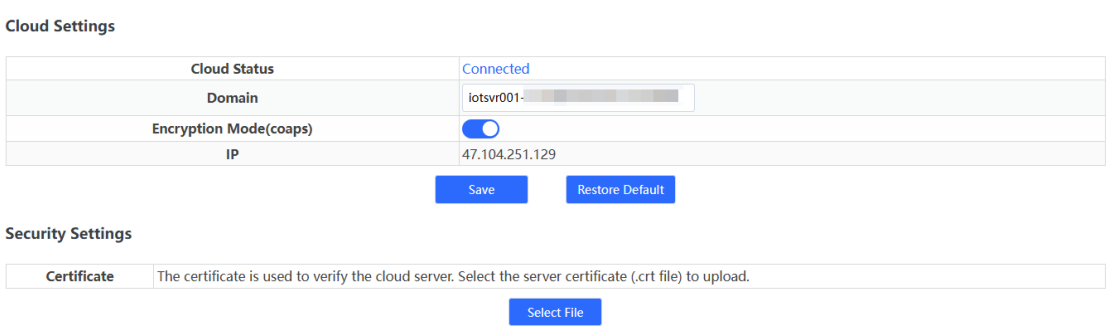
8.2 Cloud Settings

8.2.1 Checking the Cloud Information

Choose **Toolkit** > **Cloud Settings**.

On this page, you can check the status of your device, including its cloud connectivity status, reason for connection failure (if the connection to Ruijie Cloud fails), the domain name and IP address of the cloud server, and whether to toggle on encryption mode (CoAPs).

Figure 8-1 Cloud Settings



On the **Cloud Settings** page, you can modify cloud configurations or restore the default settings.

- To change the domain name and port number of the device, enter the new domain name and port number in the **Domain** field, and then click **Save**.
- To restore the default settings, click **Restore Default**, and then click **OK** on the pop-up window to restore the domain name and encryption mode (CoAPs) to default settings. For example, when the device fails to connect to Ruijie Cloud, you can attempt to restore the connection by clicking **Restore Default**.

Table 8-1 Cloud Settings Parameters

Parameter	Description
Cloud Status	Indicates the connectivity status of the device on the cloud, including **Connected**, **Unconnected**, **Connectable**, and **Certificate verification failure**.
Reason	Indicates the reason for device connection failure. The reasons for connection failure in different cloud status are as follows: ● Connected: No reason is displayed. ● Unconnected: ○ The network connection is down or a DNS resolution error has occurred. ○ This device failed to connect to Ruijie Cloud. ● Connectable: This device is not registered to Ruijie Cloud. ● Certificate verification failure: This device failed to connect to Ruijie Cloud.
Domain	Indicates the domain name of the cloud server. **Caution** ● The coap:// prefix is not required in the domain name field as it is added by default. ● After the domain name is changed, the page is refreshed after 5 seconds by default.
Encryption Mode(coaps)	Indicate whether the encryption mode (CoAPs) is enabled on the current device. If it is enabled, **Security Settings** will be displayed below. For details, see 8.2.2 Introduction to CoAP.
IP	Indicates the IP address of the cloud server resolved from the cloud address.

8.2.2 Introduction to CoAP

The Constrained Application Protocol (CoAP) is an application-layer protocol designed for compact devices and mainly used for communication in the Internet of Things (IoT) field. Thanks to the lightweight design, this protocol greatly reduces network overheads and memory usage. It is widely used in the IoT field, especially on compact, low-power, and resource-limited devices. CoAPs, the secure version of CoAP, use Datagram Transport Layer Security (DTLS) to secure data transmission.

8.2.3 Configuring CoAPs-based Encryption

After **Encryption Mode(coaps)** is toggled on, the device uses a certificate to verify the identity of a cloud server. If the verification succeeds, the device can connect to the server.

- When the device connects to a public cloud server, the device has an embedded public cloud certificate, which does not need to be imported externally.
- When the device connects to the private cloud server of RG-OCE Network Manager, you need to import the private cloud certificate for verification.

Note

Encryption Mode(coaps) can be used only in the previous two scenarios.

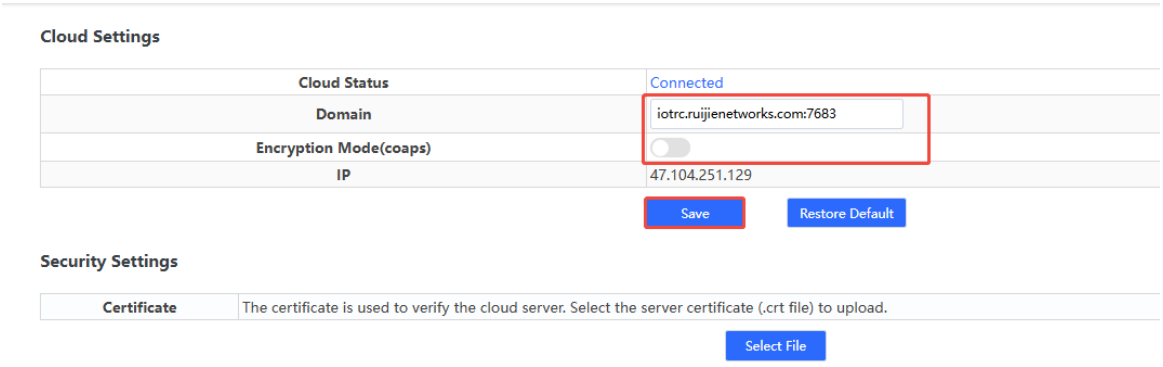
The configuration procedure in the two scenarios is described as follows.

1. Public Cloud

When the device is properly connected to the public cloud server, **Encryption Mode(coaps)** is enabled by default and does not need to be configured. This section describes how to disable **Encryption Mode(coaps)** and how to enable it again.

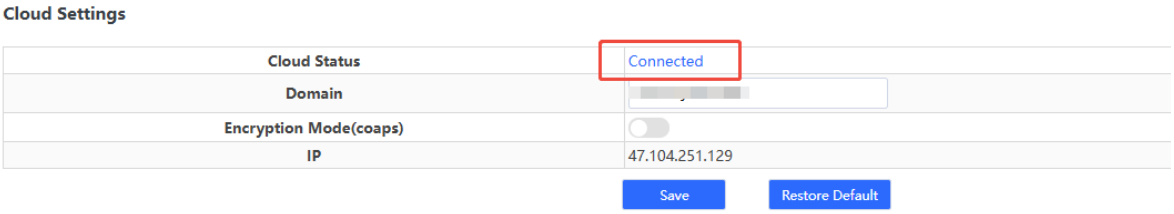
- Disable **Encryption Mode(coaps)**.
  a Toggle off Encryption Mode(coaps).
  b Change the domain name to iotrc.ruijienetworks.com:7683 and click **Save**.

Figure 8-2 Disabling the Encryption Mode



c After the web page is refreshed, if **Cloud Status** changes to **Connected**, disabling the encryption mode (CoAPs) is successful.

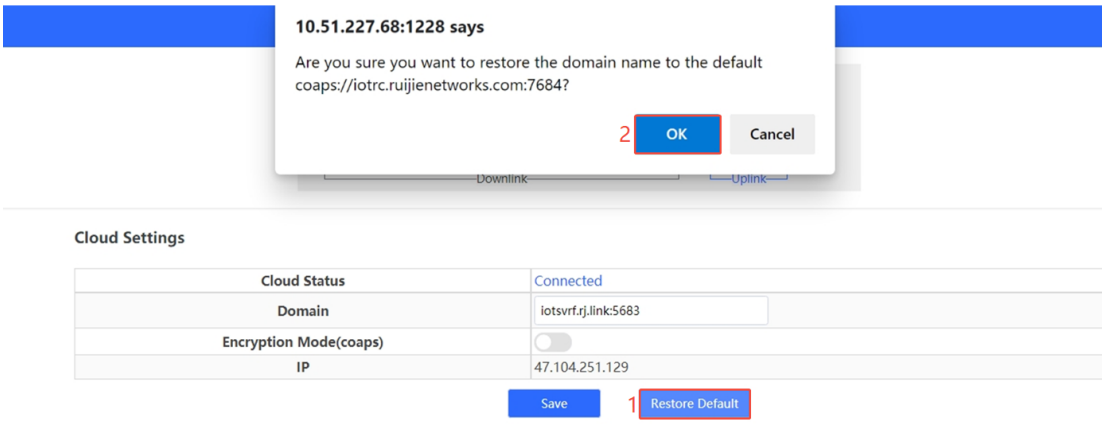
Figure 8-3 Succeeded in Disabling the Encryption Mode



- Enable **Encryption Mode(coaps)** again.
  a Click **Restore Default**. A prompt is displayed.

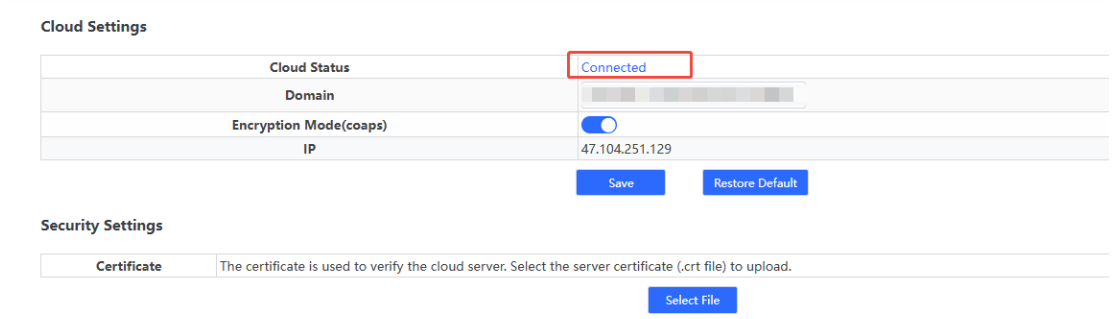
b After confirming the prompt information, click **OK**.

Figure 8-4 Enabling the Encryption Mode



c After the web page is refreshed, if **Cloud Status** changes to **Connected**, enabling the encryption mode (CoAPs) is successful.

Figure 8-5 Succeeded in Enabling the Encryption Mode



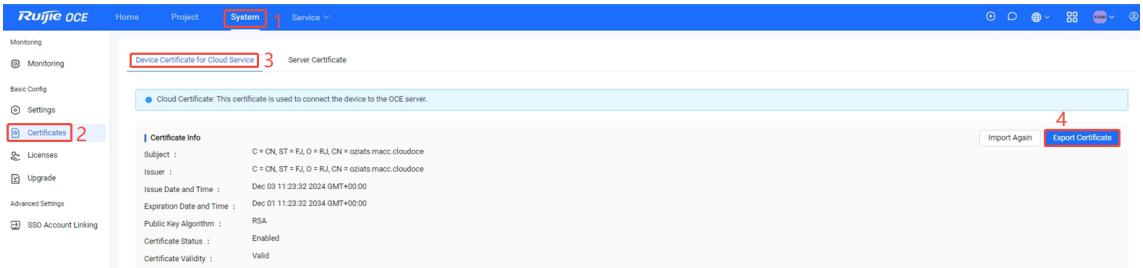
2. Private Cloud of RG-OCE Network Manager

After **Encryption Mode(coaps)** is enabled, to enable the encryption mode to take effect, you need to configure the domain name and port number, and upload the certificate of a private cloud server.

(1) Obtain the certificate.

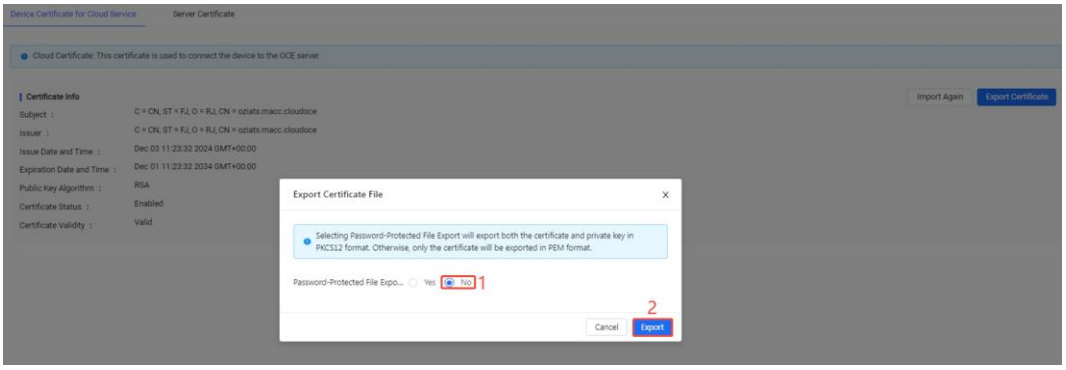
a Log in to the private cloud server of RG-OCE Network Manager, choose **System** > **Certificates** > **Device Certificate for Cloud Service**, and click **Export Certificate**.

Figure 8-6 Downloading the Private Cloud Certificate (1/2)



b Set **Password-Protected File Export** to **No** and click **Export** to download the private cloud certificate.

Figure 8-7 Downloading the Private Cloud Certificate (2/2)



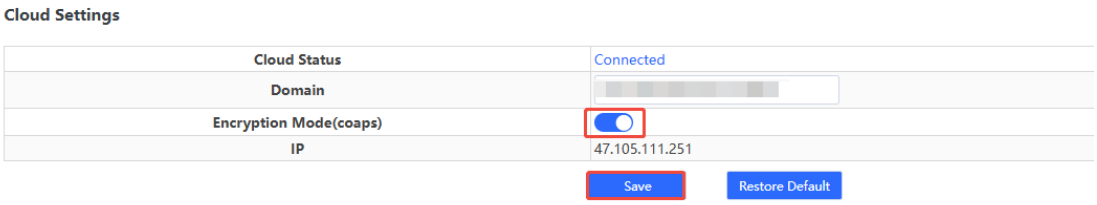
(2) Configure the domain name and port number.

a (Optional) Toggle on **Encryption Mode(coaps)** and click **Save** to enable the encryption mode.

Note

If **Encryption Mode(coaps)** is already toggled on, skip the step of enabling it.

Figure 8-8 Toggling on the Encryption Mode

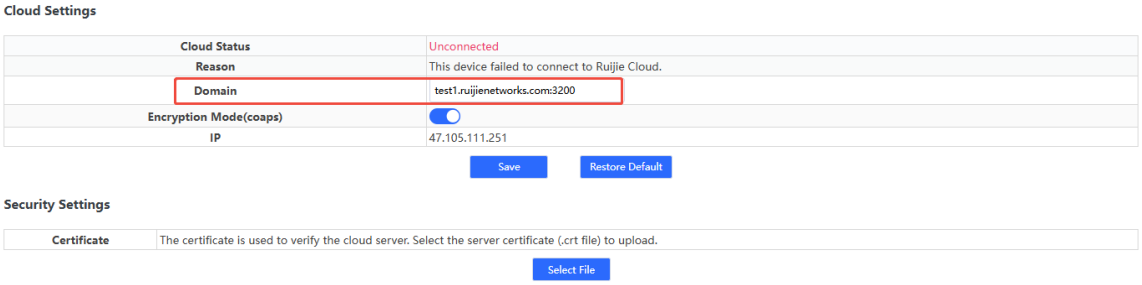


b Confirm that the domain name of a private cloud server is used and the port number is changed to the management port number for CoAPs services. Click **Save**.

Note

- The management port number for CoAPs services needs to be planned and configured during deployment of the private cloud server of RG-OCE Network Manager.
- The domain name test1.ruijienetworks.com for a private server and the management port number 3200 of the CoAPs services are only used as examples. Set the domain name and port number as required.

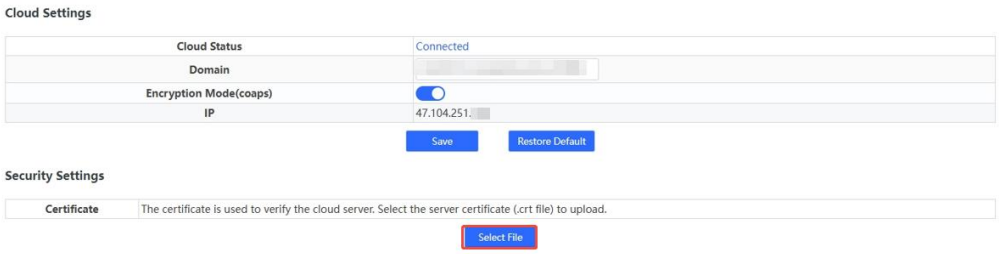
Figure 8-9 Configuring the Domain Name and Port Number for a Private Cloud Server



(3) Upload the certificate of a private cloud server.

a Click **Select File**, select the downloaded certificate of a private cloud server, and upload the certificate.

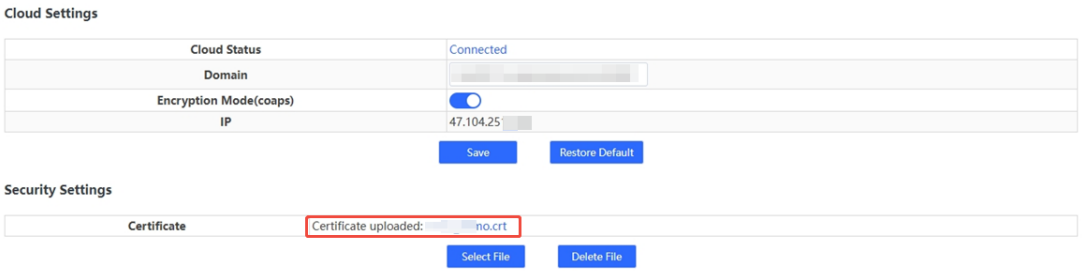
Figure 8-10 Uploading the Certificate of a Private Cloud Server



b When **Certificate uploaded** is displayed and **Cloud status** changes to **Connected**, the encryption mode is configured successfully.

To delete the imported certificate, click **Delete File**.

Figure 8-11 Succeeded in Uploading the Certificate



Caution

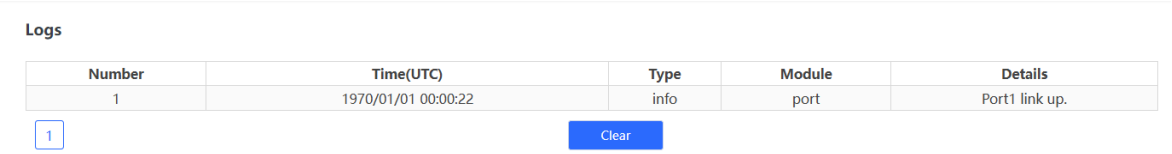
If you want to disable the encryption mode, change the port number to the management port number of the CoAP services, toggle off **Encrypted Mode(coaps)**, and click **Save**.

8.3 System Logs

Choose **Toolkit** > **Logs**.

System logs record the log generation time, log type, module that generates a log, and log details. System logs enable you to analyze and diagnose device status.

Figure 8-12 System Logs



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.

9 System Settings

9.1 Managing Device Information

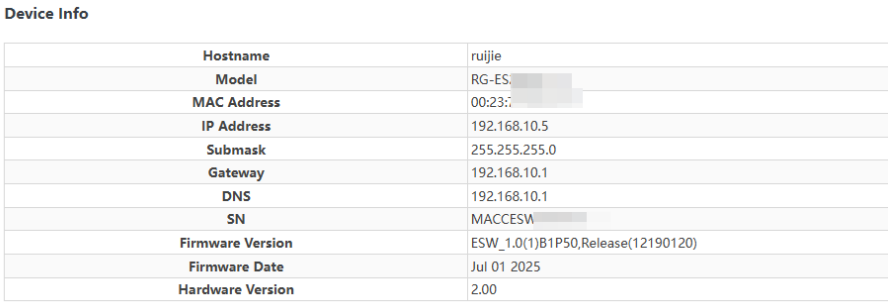
9.1.1 Viewing Device Information

Choose **Home** from the navigation page.

The **Device Info** pane on the **Home** page displays basic information about the device, including hostname, device model, serial number, firmware version, IP address, MAC address, cloud status, and uptime. You can view more information about the device by choosing **Monitoring** > **Device Info**.

Figure 9-1 Device Info

Figure 9-2 Viewing Device Information



9.1.2 Editing the Hostname

Choose **Home** from the navigation page.

Enter the hostname and click **Edit** to edit the hostname in order to distinguish different devices.

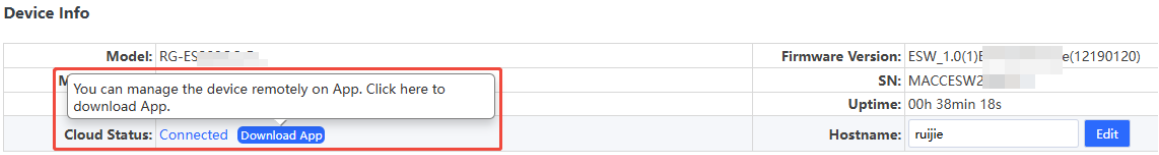
Figure 9-3 Editing the Hostname

9.1.3 Cloud Management

Choose **Home** from the navigation page.

Cloud status displays whether the device is connected to the cloud. After the device is bound to a cloud management account, the Cloud Status will display **Connected**, and you can manage the device remotely through Ruijie Cloud webpage or APP. Click **Connected** to access the homepage of Ruijie Cloud (https://cloud-as.ruijienetworks.com). Click **Download APP** to download Ruijie Cloud APP.

Figure 9-4 Cloud Management

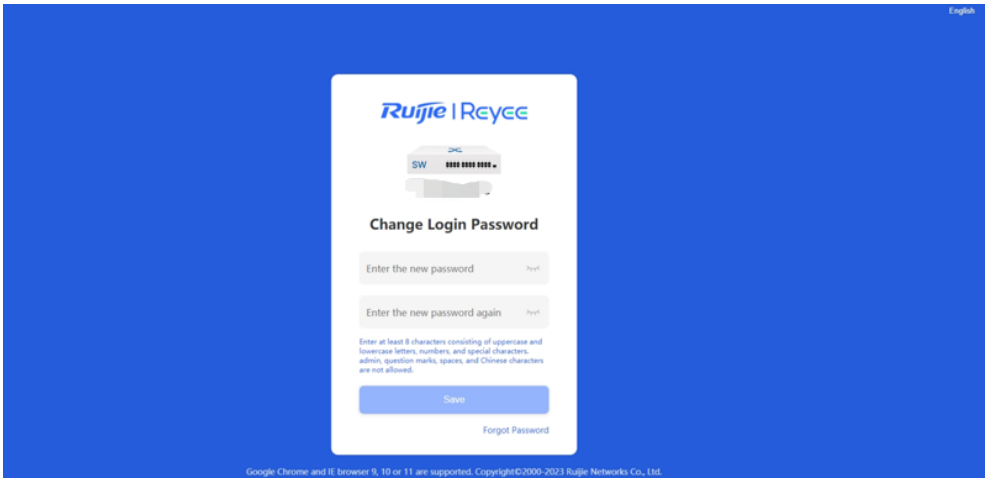


9.2 Login Password Settings

- Set the login password on the login page.

  When logging in to the device for the first time or after resetting it to factory settings, you need to set a new login password on the login page. Click **Save** to apply changes and log in to the device with your new password.

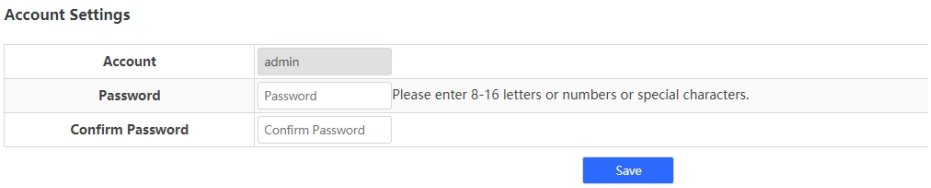
Figure 9-5 Setting the Login Password on the Login Page



- Change the login password after login.

  After logging in to the device, choose **System** > **Account Settings**. On the **Account Settings** page, set a new password and click **Save**. The system will automatically redirect you to the login page, where you can log in using the new password.

Figure 9-6 Setting the Login Password



Caution

A new management password cannot be set on the **Account Settings** page in the following scenarios:

- This device, when in network-management mode, cannot be configured with an individual management password. You can log in to the primary device to modify the network-wide management password.
- If this device is managed by Ruijie Cloud or Ruijie Reyee App, you can modify the network-wide management password through Ruijie Cloud or Ruijie Reyee App. Changing the management password on the device will not synchronize the changes on Ruijie Cloud or Ruijie Reyee App with the device.

Figure 9-7 Network-Management Mode

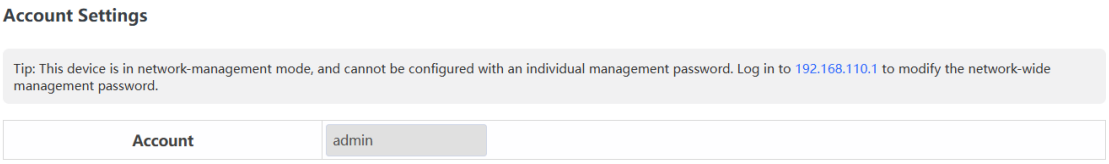
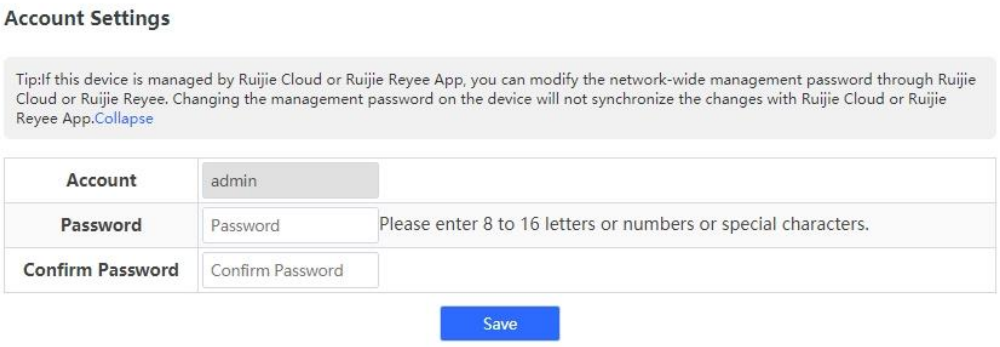


Figure 9-8 Management Through Ruijie Cloud or Ruijie Reyee App



9.3 Device Reboot

Choose **System** > **Reboot**.

Click **Reboot** to reboot the switch.

Figure 9-9 Device Reboot

9.4 System Upgrade

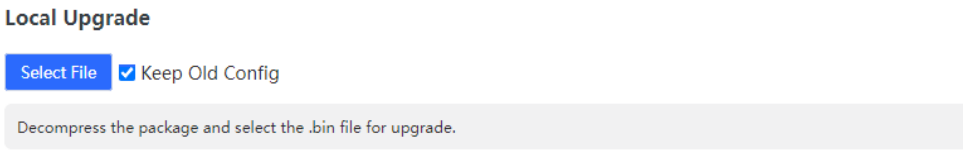
9.4.1 Local Upgrade

Choose **System** > **Upgrade**.

Click **Select File** to select the upgrade package from the local files (the upgrade package is a bin file. If it is a tar.gz file, you need to decompress the package and select the bin file for upgrade).

Keep Old Config is selected by default. That means the current configuration will be saved after device upgrade. If there is a huge difference between the current version and the upgrade version, you are advised not to select **Keep Old Config**.

Figure 9-10 Local Upgrade

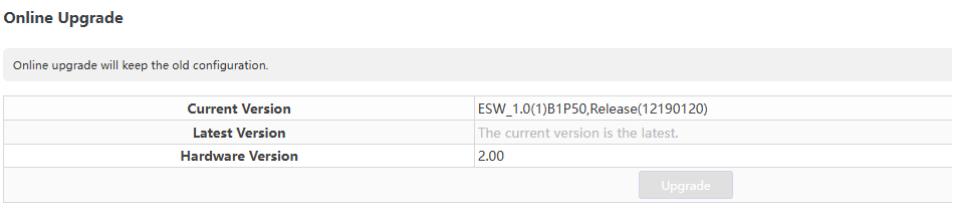


9.4.2 Online Upgrade

Choose **System** > **Upgrade**.

When there is a new version in the cloud, the version number of the latest version will be displayed on this page, and the **Upgrade** button will become available. The device will download the installation package of the recommended version from the cloud and it will be updated to the latest version. Online upgrade will keep the old configuration by default.

Figure 9-11 Online Upgrade



Note

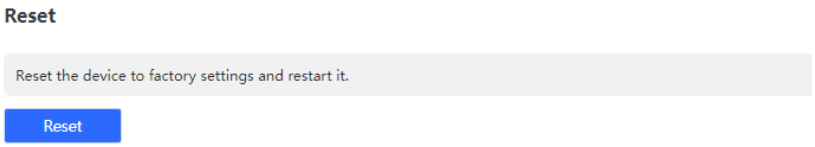
The time that online upgrade takes depends on the current network speed. It may take some time. Please be patient.

9.5 Restoring Factory Configuration

Choose **System** > **Reset**.

Click **Reset** to restore factory configuration and reboot the device.

Figure 9-12 Restoring Factory Configuration



10 Monitoring

10.1 Cable Test

Note

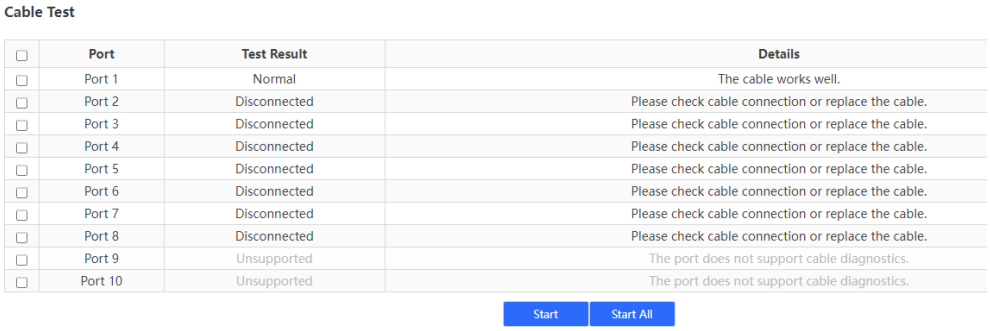
This feature is not supported on an SFP port.

Choose **Monitoring** > **Cable Test.**

Cable Test allows you to check the status of Ethernet cables. For example, you can check whether the cables are short-circuited or disconnected.

Select the ports you want to detect, and then click **Start** to start cable diagnostics. The test result will be displayed accordingly. Click **Start All** to perform one-click cable diagnostics on all ports.

Figure 10-1 Cable Test



Caution

If you select an uplink port for diagnostics, the network may be intermittently disconnected. Exercise caution when performing this operation.

10.2 Multi-DHCP Alarming

Caution

Multi-DHCP alarming will fail when the device IP address is not obtained dynamically. For relevant IP address configuration, see 3.7 Management IP Address.

Choose **Home** from the navigation page.

When there are multiple DHCP servers in a LAN, the system will send a conflicting alarm. An alarming message will be displayed in the **Device Info** column.

Figure 10-2 Multi-DHCP Alarming

Move the cursor to ⓘ to view the alarm details, including the VLAN where the conflicts occur, port, IP address of DHCP server, and MAC address.

10.3 Viewing Switches on the Network

Choose **Monitoring** > **Device List**.

- Primary device for global management

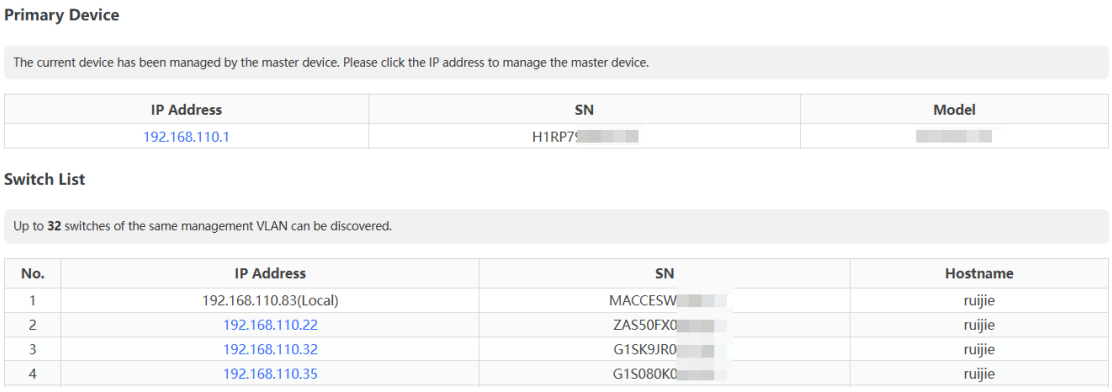
  If the switch is under uniform management, some features cannot be configured independently (such as password settings). To facilitate configuration, information of the primary device in the VLAN will be displayed on this page. Click the IP address of the primary device to access the **Primary Device** page for global configuration.

- Devices in the same management VLAN

  The device is able to automatically discover other switches in the same management VLAN. Information of these switches will be displayed in **Switch List**.

  The first row of **Switch List** displays information of the current device, and the following rows display information of other devices. Click the **IP address** of a device to access eWeb of the device (login required).

Figure 10-3 Viewing Switches on the Network



Note

The number of switches that can be discovered varies with product models.

11 FAQs

11.1 I failed to log in to eWeb. What can I do?

(1) Verify that an Ethernet cable is properly connected to the LAN port of the device and the LED blinks or is steady on.

(2) Before accessing eWeb, you are advised to configure a static IP address for a PC on the same network segment as the device IP address (default device IP address: 10.44.77.200 and subnet mask: 255.255.255.0). For example, set the IP address of the PC to 10.44.77.100 and the subnet mask to 255.255.255.0.

(3) Run the **ping** command to test the connectivity between the PC and the device.

(4) If the login failure persists, restore the device to factory settings.

11.2 What can I do if I forget my password? How can I restore the factory settings?

Caution

Press and hold the **Reset** button on the device panel for more than 5 seconds. This action will restore the device to factory settings, clearing all configurations. Exercise caution when performing this operation.

If you forget the password and cannot log in to the device, follow these steps:

(1) With the device powered on, press and hold the **Reset** button on the device panel for more than 5 seconds. Release the button when the system LED blinks to restore the device to factory settings.

(2) Once the device restarts, log in to eWeb using the default management IP address (10.44.77.200).

(3) On the login page, set a new password and use it to log in to the device.