# Ruijie Reyee RG-ES, RG-NIS2100 Series Switches 1.0(1)B1P48

## Configuration Guide

Document Version: V1.1
Date: 2025.09.24

## 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.ruijienetworks.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<br>2. Window names, tab name, field name and menu items<br>3. Link | 1. Click **OK**.<br>2. Select **Config Wizard**.<br>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 Release Note

This section describes the hardware support and new software features in the ESW_1.0(1)B1P48 version. For details about the software version, see the release note published with the software version.

## 1.1 Hardware Support

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

**Table 1-1 Supported Hardware Models**

| Hardware Type | Model | Hardware Version Number |
|---|---|---|
| Switch | RG-ES205GC-P | 1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 1.5x, 1.6x, 2.0x, 2.1x, 2.2x, 2.3x, 2.4x, 2.5x, 2.6x, 2.7x, 2.8x |
| Switch | RG-ES209GC-P | 1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 1.5x, 1.6x, 1.7x, 1.8x, 1.9x, 1.Ax, 1.Bx, 1.Cx, 1.Dx, 1.Ex |
| Switch | RG-ES205GC | 1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 1.5x, 1.6x, 1.7x |
| Switch | RG-ES206GC-P | 1.0x, 1.1x, 1.2x |
| Switch | RG-ES208GC | 1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 1.5x, 1.6x |
| Switch | RG-ES210GC-LP | 1.0x, 1.1x, 1.2x, 1.3x |
| Switch | RG-ES210GS-P | 1.0x, 1.1x, 1.2x, 1.3x, 1.4x |
| Switch | RG-ES206GS-P | 1.0x, 1.1x, 1.2x, 1.3x |
| Switch | RG-ES216GC | 1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 2.0x, 2.1x, 2.2x, 3.0x, 3.1x, 3.2x, 3.3x |
| Switch | RG-ES224GC | 1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 2.0x, 2.1x, 2.2x, 3.0x, 3.1x, 3.2x |
| Switch | RG-ES220GS-P | 1.0x, 1.1x, 1.2x, 1.3x, 1.4x |
| Switch | RG-ES228GS-P | 1.0x, 1.1x, 1.2x, 1.3x, 1.4x |
| Switch | RG-ES226GC-P | 1.0x, 1.1x, 1.2x, 1.3x, 2.0x, 2.1x, 2.2x, 2.3x, 3.0x, 3.1x |
| Switch | RG-ES218GC-P | 1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 2.0x, 2.1x, 2.2x, 3.0x, 3.1x, 3.2x |
| Switch | RG-ES224GC-V2 | 1.0x, 1.1x, 1.2x, 1.3x, 1.4x |
| Switch | RG-ES216GC-V2 | 1.0x, 1.1x, 1.2x, 1.3x, 1.4x |
| Switch | RG-NIS2100-8GT2SFP-HP | 1.0x, 1.1x, 1.2x, 1.3x |
| Switch | RG-NIS2100-4GT2SFP-HP | 1.0x, 1.1x, 1.2x 1.3x |

## 1.2 New Software Features

The ESW_1.0(1)B1P48 version introduces no new features but includes optimizations to some existing features.

# 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 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 with an IP address in the same network segment as the default IP address of the switch so that the PC can ping the switch. For example, set the IP address of the PC to 10.44.77.100.

**Table 2-1 Default Configuration**

| Feature | Default Setting |
|---|---|
| Device IP Address | 10.44.77.200 |
| Password | admin |

## 2.3 Login to eWeb

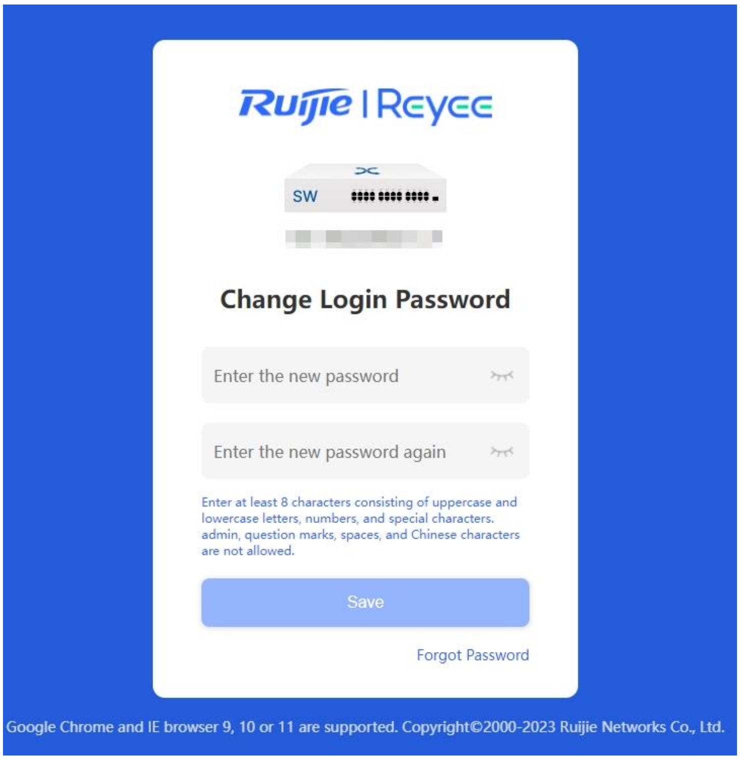
(1) Enter the IP address (10.44.77.200 by default) of the device in the address bar of the browser to access the login page.

**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 1-1 Login to eWeb Upon the First Time**



[redacted]

Change Login Password

Enter the new password

Enter the new password again

Enter at least 8 characters consisting of uppercase and lowercase letters, numbers, and special characters. admin, question marks, spaces, and Chinese characters are not allowed.

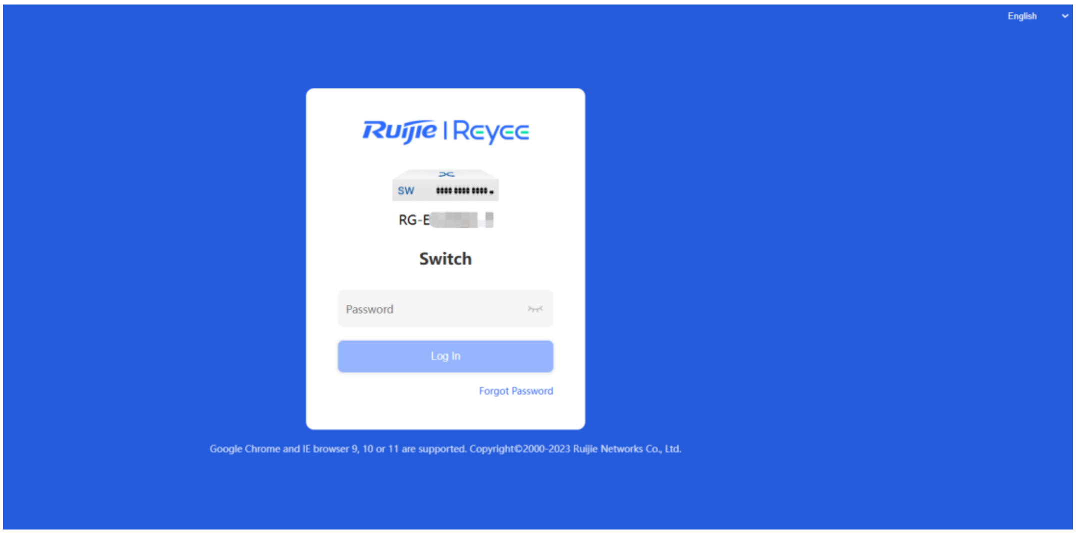
Google Chrome and IE browser 9, 10 or 11 are supported. Copyright©2000-2023 Ruijie Networks Co., Ltd.

(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 1-2 eWeb Login Page**



RG-E[redacted]

Switch

Google Chrome and IE browser 9, 10 or 11 are supported. Copyright©2000-2023 Ruijie Networks Co., Ltd.

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.

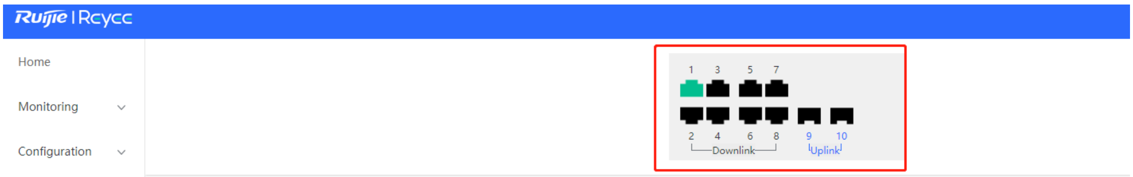
# 3 Port Management

## 3.1 Managing Port Information

### 3.1.1 Port Status Bar

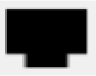
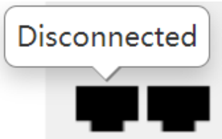
The port status bar is at the top of eWeb, showing the port ID, port attribute (uplink/downlink), connection status, and other information.

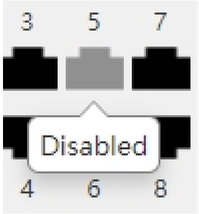
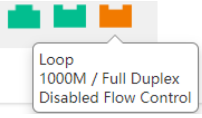
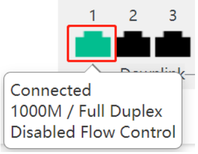
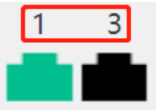
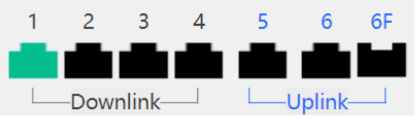
**Figure 1-3 Port Status Bar**



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 color of the port icon is black, showing the port is disconnected. |

| Port Icon | Description |
|---|---|
|  | 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. |
|  1 2 3<br>Connected<br>1000M / Full Duplex<br>Disabled Flow Control | 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.<br>● 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 3.4 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.

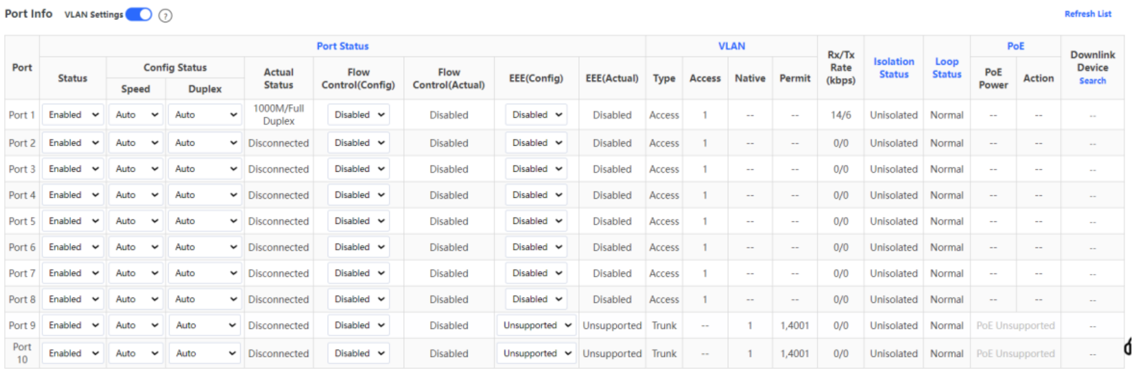
**Note**

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 3.4 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.
- 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 1-4 Viewing or Configuring Port Settings**



Port Info VLAN Settings

Refresh List

| Port | Port Status | | | | | | | | VLAN | | | | Rx/Tx Rate (kbps) | Isolation Status | Loop Status | PoE | | Downlink Device<br>Search |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | Status | Config Status | | Actual Status | Flow Control(Config) | Flow Control(Actual) | EEE(Config) | EEE(Actual) | Type | Access | Native | Permit | | | | PoE Power | Action | |
| | | Speed | Duplex | | | | | | | | | | | | | | | |
| Port 1 | Enabled | Auto | Auto | 1000M/Full Duplex | Disabled | Disabled | Disabled | Disabled | Access | 1 | -- | -- | 14/6 | Unisolated | Normal | -- | -- | -- |
| Port 2 | Enabled | Auto | Auto | Disconnected | Disabled | Disabled | Disabled | Disabled | Access | 1 | -- | -- | 0/0 | Unisolated | Normal | -- | -- | -- |
| Port 3 | Enabled | Auto | Auto | Disconnected | Disabled | Disabled | Disabled | Disabled | Access | 1 | -- | -- | 0/0 | Unisolated | Normal | -- | -- | -- |
| Port 4 | Enabled | Auto | Auto | Disconnected | Disabled | Disabled | Disabled | Disabled | Access | 1 | -- | -- | 0/0 | Unisolated | Normal | -- | -- | -- |
| Port 5 | Enabled | Auto | Auto | Disconnected | Disabled | Disabled | Disabled | Disabled | Access | 1 | -- | -- | 0/0 | Unisolated | Normal | -- | -- | -- |
| Port 6 | Enabled | Auto | Auto | Disconnected | Disabled | Disabled | Disabled | Disabled | Access | 1 | -- | -- | 0/0 | Unisolated | Normal | -- | -- | -- |
| Port 7 | Enabled | Auto | Auto | Disconnected | Disabled | Disabled | Disabled | Disabled | Access | 1 | -- | -- | 0/0 | Unisolated | Normal | -- | -- | -- |
| Port 8 | Enabled | Auto | Auto | Disconnected | Disabled | Disabled | Disabled | Disabled | Access | 1 | -- | -- | 0/0 | Unisolated | Normal | -- | -- | -- |
| Port 9 | Enabled | Auto | Auto | Disconnected | Disabled | Disabled | Unsupported | Unsupported | Trunk | -- | 1 | 1,4001 | 0/0 | Unisolated | Normal | PoE Unsupported | | -- |
| Port 10 | Enabled | Auto | Auto | Disconnected | Disabled | Disabled | Unsupported | Unsupported | Trunk | -- | 1 | 1,4001 | 0/0 | Unisolated | Normal | PoE Unsupported | | -- |

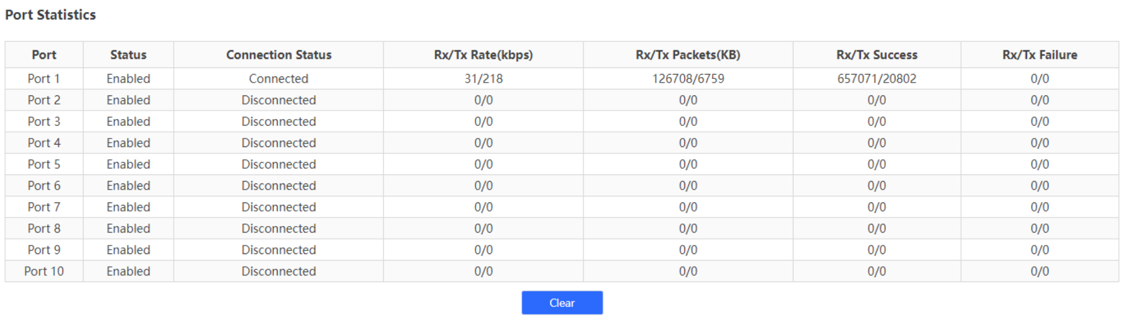
### 3.1.3 Port Packet Statistics

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 1-5 Port Packet Statistics**



Port Statistics

| Port | Status | Connection Status | Rx/Tx Rate(kbps) | Rx/Tx Packets(KB) | Rx/Tx Success | Rx/Tx Failure |
|---|---|---|---|---|---|---|
| Port 1 | Enabled | Connected | 31/218 | 126708/6759 | 657071/20802 | 0/0 |
| Port 2 | Enabled | Disconnected | 0/0 | 0/0 | 0/0 | 0/0 |
| Port 3 | Enabled | Disconnected | 0/0 | 0/0 | 0/0 | 0/0 |
| Port 4 | Enabled | Disconnected | 0/0 | 0/0 | 0/0 | 0/0 |
| Port 5 | Enabled | Disconnected | 0/0 | 0/0 | 0/0 | 0/0 |
| Port 6 | Enabled | Disconnected | 0/0 | 0/0 | 0/0 | 0/0 |
| Port 7 | Enabled | Disconnected | 0/0 | 0/0 | 0/0 | 0/0 |
| Port 8 | Enabled | Disconnected | 0/0 | 0/0 | 0/0 | 0/0 |
| Port 9 | Enabled | Disconnected | 0/0 | 0/0 | 0/0 | 0/0 |
| Port 10 | Enabled | Disconnected | 0/0 | 0/0 | 0/0 | 0/0 |

## 3.2 Port Settings

**Note**

- The EEE feature can be configured on RJ45 ports that operate at 100 or 1000 Mbps with **Duplex** set to **Auto**.
- For the RG-NIS2100 series, set the port speed to 10 Mbps through the DIP switch on the device's front panel or through the web interface. On the web interface, set **Speed** to **10M**, **Duplex** to **Auto**, and **Flow Control** to **Enabled**. The latest configuration takes effect.

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.

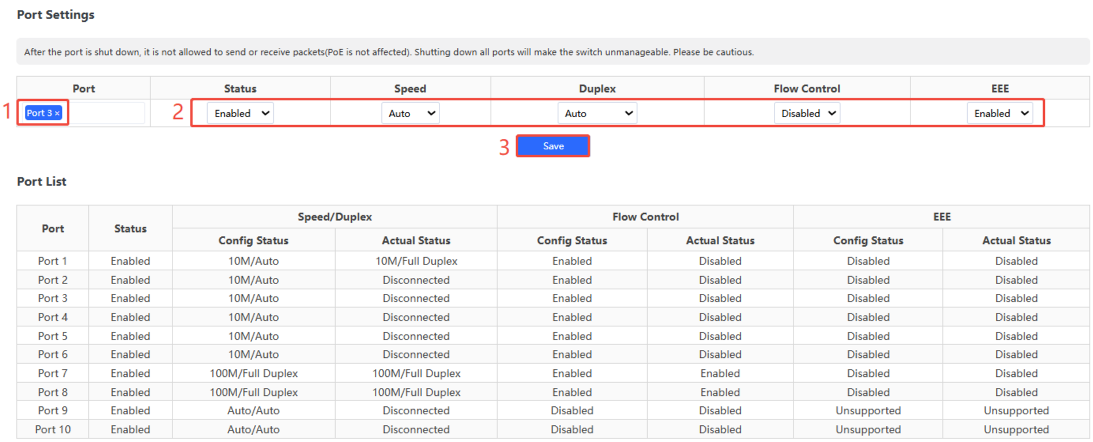
(3) Click **Save**.

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 1-6 Port Configuration and Status**



Port Settings

After the port is shut down, it is not allowed to send or receive packets(PoE is not affected). Shutting down all ports will make the switch unmanageable. Please be cautious.

| Port | Status | Speed | Duplex | Flow Control | EEE |
|---|---|---|---|---|---|
| 1 Port 3 × | 2 Enabled | Auto | Auto | Disabled | Enabled |

3 Save

Port List

| Port | Status | Speed/Duplex | | Flow Control | | EEE | |
|---|---|---|---|---|---|---|---|
| | | Config Status | Actual Status | Config Status | Actual Status | Config Status | Actual Status |
| Port 1 | Enabled | 10M/Auto | 10M/Full Duplex | Enabled | Disabled | Disabled | Disabled |
| Port 2 | Enabled | 10M/Auto | Disconnected | Enabled | Disabled | Disabled | Disabled |
| Port 3 | Enabled | 10M/Auto | Disconnected | Enabled | Disabled | Disabled | Disabled |
| Port 4 | Enabled | 10M/Auto | Disconnected | Enabled | Disabled | Disabled | Disabled |
| Port 5 | Enabled | 10M/Auto | Disconnected | Enabled | Disabled | Disabled | Disabled |
| Port 6 | Enabled | 10M/Auto | Disconnected | Enabled | Disabled | Disabled | Disabled |
| Port 7 | Enabled | 100M/Full Duplex | 100M/Full Duplex | Enabled | Enabled | Disabled | Disabled |
| Port 8 | Enabled | 100M/Full Duplex | 100M/Full Duplex | Enabled | Enabled | Disabled | Disabled |
| Port 9 | Enabled | Auto/Auto | Disconnected | Disabled | Disabled | Unsupported | Unsupported |
| Port 10 | Enabled | Auto/Auto | Disconnected | Disabled | Disabled | Unsupported | Unsupported |

**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.<br>● **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 |

| Parameter | Description | Default |
|---|---|---|
| Duplex | ● **Full Duplex**: The port can receive packets while sending packets.<br>● **Half Duplex**: The port can receive or send packets at a time.<br>● **Auto**: The duplex mode of the port is determined by the auto-negotiation between the local port and the peer port. | Auto |
| Flow Control | ● **Enabled**: The port will process the received flow control frames and send them when flow congestion occurs.<br>● **Disabled**: The flow control is disabled. | Disabled |
| 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 |

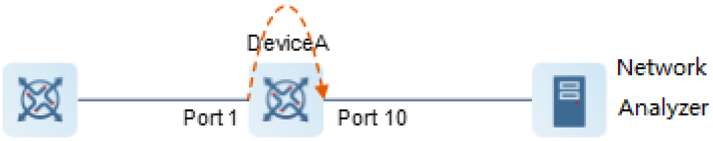
# 3.3 Port Mirroring

## 3.3.1 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 1-7 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 1-7 Operating Principle of Port Mirroring**



## 3.3.2 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.

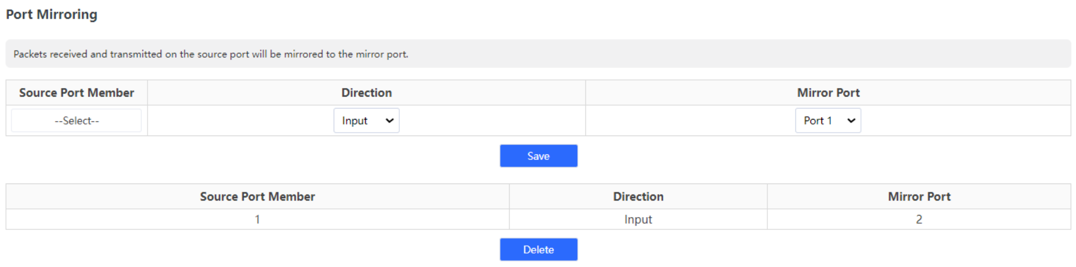
If you want to delete port mirroring configuration, click **Delete**.

⚠ **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 1-8 **Configuring Port Mirroring**



Port Mirroring

Packets received and transmitted on the source port will be mirrored to the mirror port.

| Source Port Member | Direction | Mirror Port |
|---|---|---|
| --Select-- | Input | Port 1 |

| Source Port Member | Direction | Mirror Port |
|---|---|---|
| 1 | Input | 2 |

**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.<br>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:<br>● 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.<br>● Input: The packets received by the source port will be mirrored to the mirror port.<br>● 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. |

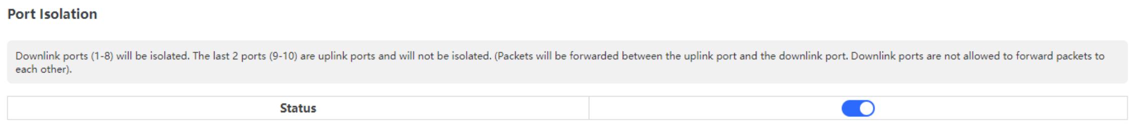
## 3.4 Port Isolation

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 1-9 Port Isolation**



**Port Isolation**

Downlink ports (1-8) will be isolated. The last 2 ports (9-10) are uplink ports and will not be isolated. (Packets will be forwarded between the uplink port and the downlink port. Downlink ports are not allowed to forward packets to each other).

| Status | ● |
|---|---|

**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.
- Port isolation can be enabled on devices featuring DIP switches on the panel. The last configuration applied takes effect.

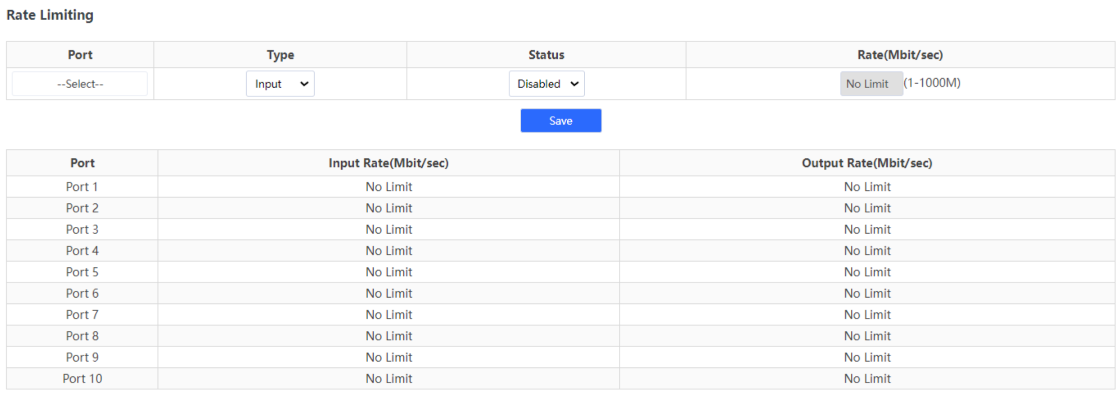
## 3.5 Port-based Rate Limiting

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 1-10 Port Rate Limiting**



**Rate Limiting**

| Port | Type | Status | Rate(Mbit/sec) |
|---|---|---|---|
| --Select-- | Input | Disabled | No Limit (1-1000M) |

| Port | Input Rate(Mbit/sec) | Output Rate(Mbit/sec) |
|---|---|---|
| Port 1 | No Limit | No Limit |
| Port 2 | No Limit | No Limit |
| Port 3 | No Limit | No Limit |
| Port 4 | No Limit | No Limit |
| Port 5 | No Limit | No Limit |
| Port 6 | No Limit | No Limit |
| Port 7 | No Limit | No Limit |
| Port 8 | No Limit | No Limit |
| Port 9 | No Limit | No Limit |
| Port 10 | No Limit | No Limit |

**Table 3-4 Rate Limiting Parameters**

| Parameter | Description | Default |
|---|---|---|
| Port | You can select multiple ports for rate limiting configuration in batches. | No default value |

| Parameter | Description | Default |
|---|---|---|
| Type | The direction of the rate-limited data traffic:<br>● Input & output: Rate limiting for all packets forwarded over the port, including the received packets and the transmitted packets.<br>● Input: Rate limiting for packets received by the port.<br>● 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.

## 3.6 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 Internet types available:

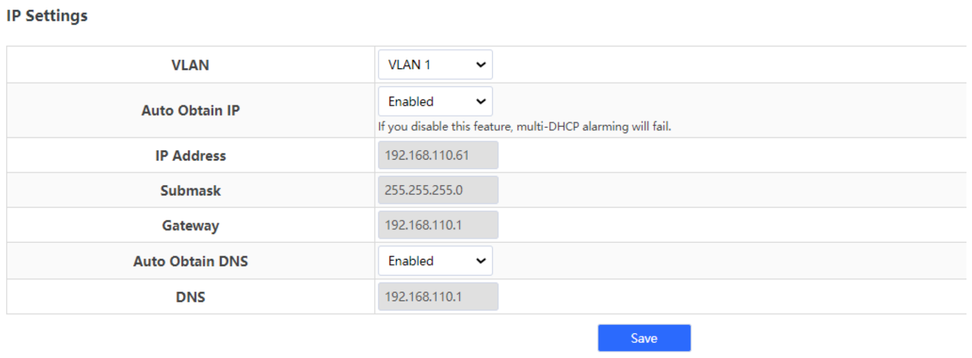
- Dynamic IP address: Enable **Auto Obtain IP** feature to use the IP address assigned dynamically by the uplink DHCP server.
- Static IP address: Disable **Auto Obtain IP** feature to use the fixed IP address configured manually by the user.

Enable **Auto Obtain IP** feature, and the device will automatically obtain various parameters from the DHCP server. You can select whether to obtain a DNS address automatically from the DHCP server. If **Auto Obtain DNS** feature is disabled, you need to configure a DNS address manually.

After disabling **Auto Obtain IP** feature, you need to manually configure the IP address, subnet mask, gateway IP address, and DNS address. Click **Save** to enforce the configuration.

**VLAN** is used for managing VLAN tag of the management packets. Disable VLAN settings, and 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 1-11 IP Settings**



IP Settings

| | |
|---|---|
| VLAN | VLAN 1 |
| Auto Obtain IP | Enabled<br>If you disable this feature, multi-DHCP alarming will fail. |
| IP Address | 192.168.110.61 |
| Submask | 255.255.255.0 |
| Gateway | 192.168.110.1 |
| Auto Obtain DNS | Enabled |
| DNS | 192.168.110.1 |

**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.

## 3.7 Setting the Port Media Type

**Specification**

This function is only supported on the RG-ES206GS-P and the RG-ES210GS-P switches.

Choose **Configuration** > **Port Media Type**.

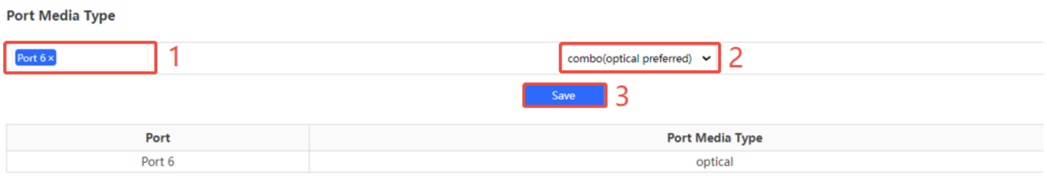
(1) Select a combo port. Only combo ports are displayed in the drop-down list.

(2) Select the port type. You can select **combo(optical preferred)**, **electrical**, or **optical** from the drop-down list.

- **combo(optical preferred)**: The port type is automatically selected based on the access status of the combo port. The optical port is selected by default.
- **Electrical**: Indicates the RJ45 port type.
- **Optical**: Indicates the optical port type.

(3) Click **Save**. The configured combo port type is displayed in the lower list.

Figure 1-12  Setting the Port Media Type



Port Media Type

Port 6 ×

combo(optical preferred)

| Port | Port Media Type |
|---|---|
| Port 6 | optical |

# 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.

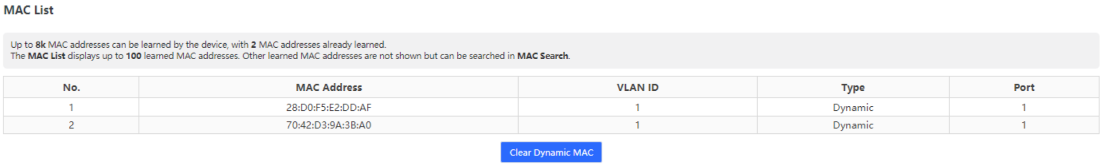
### 4.1.2 Viewing MAC Address Table

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 1-13  MAC Address Table



MAC List

Up to **8k** MAC addresses can be learned by the device, with **2** MAC addresses already learned.
The **MAC List** displays up to **100** learned MAC addresses. Other learned MAC addresses are not shown but can be searched in **MAC Search**.

| No. | MAC Address | VLAN ID | Type | Port |
|---|---|---|---|---|
| 1 | 28:D0:F5:E2:DD:AF | 1 | Dynamic | 1 |
| 2 | 70:42:D3:9A:3B:A0 | 1 | Dynamic | 1 |

**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**.

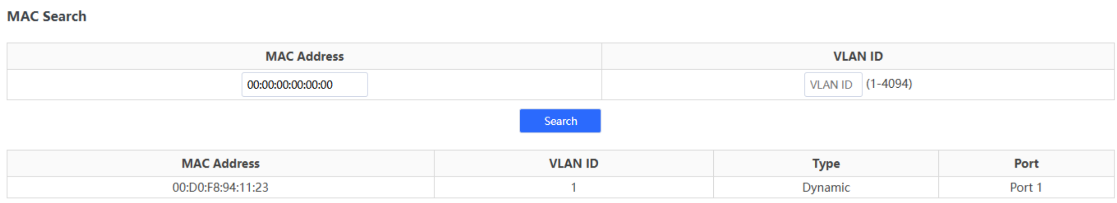
You can search for MAC address entries according to MAC address and VLAN ID.

**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 1-14 Searching for MAC Addresses (with VLAN Enabled)**



MAC Search

| MAC Address | VLAN ID |
|---|---|
| 00:00:00:00:00:00 | VLAN ID (1-4094) |

| MAC Address | VLAN ID | Type | Port |
|---|---|---|---|
| 00:D0:F8:94:11:23 | 1 | Dynamic | Port 1 |

### 4.1.4 Configuring Static MAC Address

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

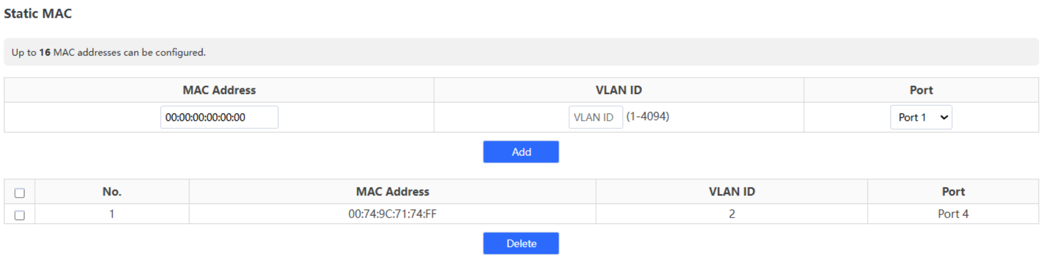
By configuring a static MAC address, you can manually bind the MAC address of a downlink network device with a port of the switch. After you add a static MAC address, when the device receives a packet destined to this address from VLAN, it forwards the packet to the specified port.

**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 1-15 Configuring Static MAC Address**



Static MAC

Up to **16** MAC addresses can be configured.

| MAC Address | VLAN ID | Port |
|---|---|---|
| 00:00:00:00:00:00 | VLAN ID (1-4094) | Port 1 |

Add

| □ | No. | MAC Address | VLAN ID | Port |
|---|---|---|---|---|
| □ | 1 | 00:74:9C:71:74:FF | 2 | Port 4 |

Delete

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

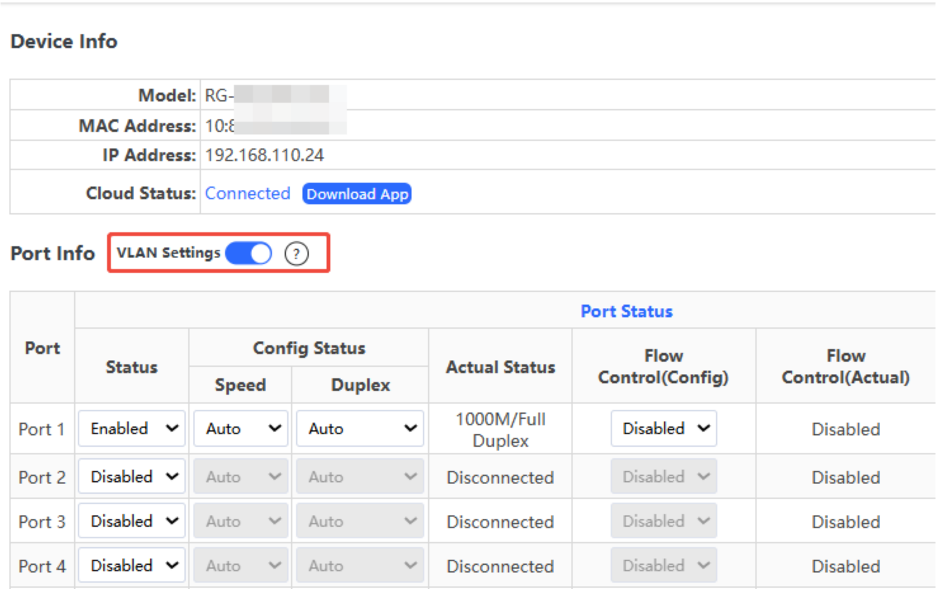
## 4.2.1 Global VLAN Settings

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 1-16 VLAN Settings**



Device Info

| | |
|---|---|
| Model: | RG-[redacted] |
| MAC Address: | 10:[redacted] |
| IP Address: | 192.168.110.24 |
| Cloud Status: | Connected Download App |

Port Info VLAN Settings ● ?

| Port | Port Status | | | | | |
|---|---|---|---|---|---|---|
| | Status | Config Status | | Actual Status | Flow Control(Config) | Flow Control(Actual) |
| | | Speed | Duplex | | | |
| Port 1 | Enabled | Auto | Auto | 1000M/Full Duplex | Disabled | Disabled |
| Port 2 | Disabled | Auto | Auto | Disconnected | Disabled | Disabled |
| Port 3 | Disabled | Auto | Auto | Disconnected | Disabled | Disabled |
| Port 4 | Disabled | Auto | Auto | Disconnected | Disabled | Disabled |

**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**.

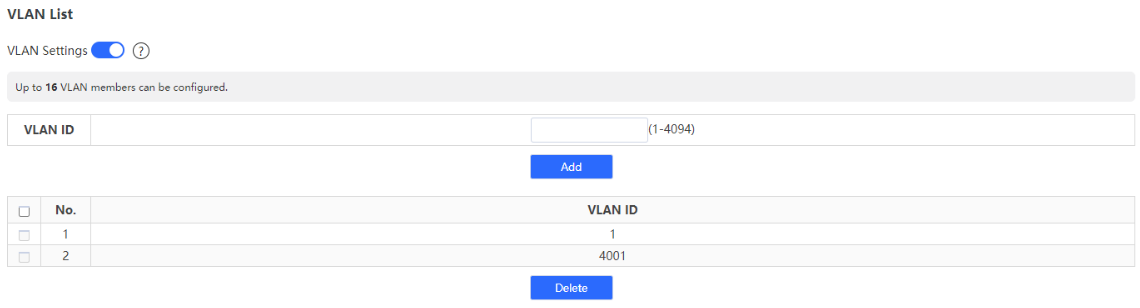
Enter VLAN ID and click **Add** to create a static VLAN.

**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.
- A maximum of 16 VLANs can be created.
- 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 1-17 Static VLANs Settings**



VLAN List

VLAN Settings ● ?

Up to **16** VLAN members can be configured.

| | | |
|---|---|---|
| VLAN ID | | (1-4094) |

| □ | No. | VLAN ID |
|---|---|---|
| □ | 1 | 1 |
| □ | 2 | 4001 |

### 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.

**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.

- On the **VLAN Settings** page, VLAN settings are the same as those on the **Home** page. The settings are globally applied and the latest configuration takes effect.

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

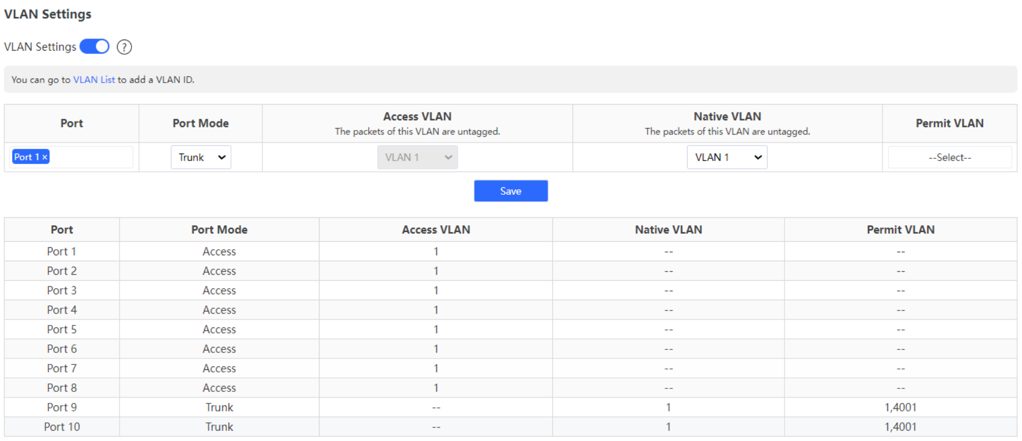
(2) Configure the port type.

- 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.

**Figure 1-18 Configuring Port VLANs**



VLAN Settings

VLAN Settings ● ?

You can go to VLAN List to add a VLAN ID.

| Port | Port Mode | Access VLAN<br>The packets of this VLAN are untagged. | Native VLAN<br>The packets of this VLAN are untagged. | Permit VLAN |
|---|---|---|---|---|
| Port 1 × | Trunk | VLAN 1 | VLAN 1 | --Select-- |

| Port | Port Mode | Access VLAN | Native VLAN | Permit VLAN |
|---|---|---|---|---|
| Port 1 | Access | 1 | -- | -- |
| Port 2 | Access | 1 | -- | -- |
| Port 3 | Access | 1 | -- | -- |
| Port 4 | Access | 1 | -- | -- |
| Port 5 | Access | 1 | -- | -- |
| Port 6 | Access | 1 | -- | -- |
| Port 7 | Access | 1 | -- | -- |
| Port 8 | Access | 1 | -- | -- |
| Port 9 | Trunk | -- | 1 | 1,4001 |
| Port 10 | Trunk | -- | 1 | 1,4001 |

**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.<br>● 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.<br>● 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.<br>● You can set the Permit VLAN range to limit VLAN frames that can be forwarded.<br>● 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**.

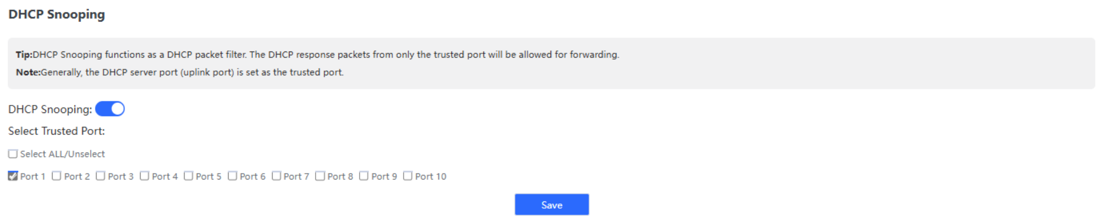
Toggle the switch to **On** to enable DHCP snooping, select the trusted ports, and then click **Save**.

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 1-19  DHCP Snooping**



**DHCP Snooping**

**Tip:**DHCP Snooping functions as a DHCP packet filter. The DHCP response packets from only the trusted port will be allowed for forwarding.
**Note:**Generally, the DHCP server port (uplink port) is set as the trusted port.

DHCP Snooping: ●

Select Trusted Port:

□ Select ALL/Unselect

☑ Port 1 □ Port 2 □ Port 3 □ Port 4 □ Port 5 □ Port 6 □ Port 7 □ Port 8 □ Port 9 □ Port 10

## 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.

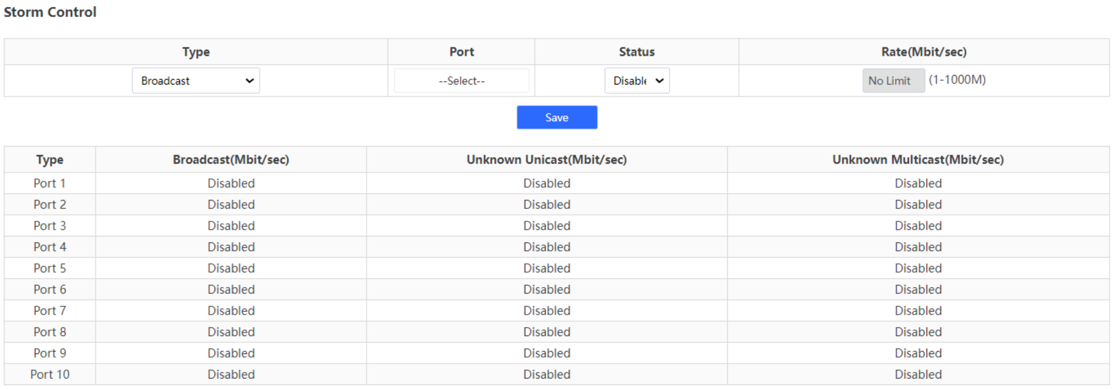
### 5.2.2 Configuration Steps

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

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

The storm control type and corresponding rate are displayed in the table right below the **Save** button. 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**. When storm control is enabled, the corresponding rate limits will be displayed.

**Figure 1-20 Storm Control**



Storm Control

| Type | Port | Status | Rate(Mbit/sec) |
|---|---|---|---|
| Broadcast | --Select-- | Disable | No Limit (1-1000M) |

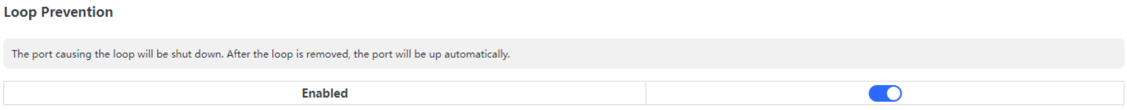
| Type | Broadcast(Mbit/sec) | Unknown Unicast(Mbit/sec) | Unknown Multicast(Mbit/sec) |
|---|---|---|---|
| Port 1 | Disabled | Disabled | Disabled |
| Port 2 | Disabled | Disabled | Disabled |
| Port 3 | Disabled | Disabled | Disabled |
| Port 4 | Disabled | Disabled | Disabled |
| Port 5 | Disabled | Disabled | Disabled |
| Port 6 | Disabled | Disabled | Disabled |
| Port 7 | Disabled | Disabled | Disabled |
| Port 8 | Disabled | Disabled | Disabled |
| Port 9 | Disabled | Disabled | Disabled |
| Port 10 | Disabled | Disabled | Disabled |

## 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. Loop guard function is disabled by default.

**Figure 1-21 Loop Prevention**



Loop Prevention

The port causing the loop will be shut down. After the loop is removed, the port will be up automatically.

| | |
|---|---|
| Enabled | ● |

# 6 PoE Settings

**Specification**

This function is supported by switch models suffixed with -P, -LP, -HP, or -UP in the Supported Hardware Models, such as the RG-ES220GS-P.

Choose **PoE** from the navigation pane.

The device supplies power to PoE powered devices through ports. You can view the power supply status of the current system and ports and configure whether to enable the power supply feature on a specified port.

- **PoE Info**: The total power, used power, remaining power, and current work status of the PoE system are displayed.
- **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.

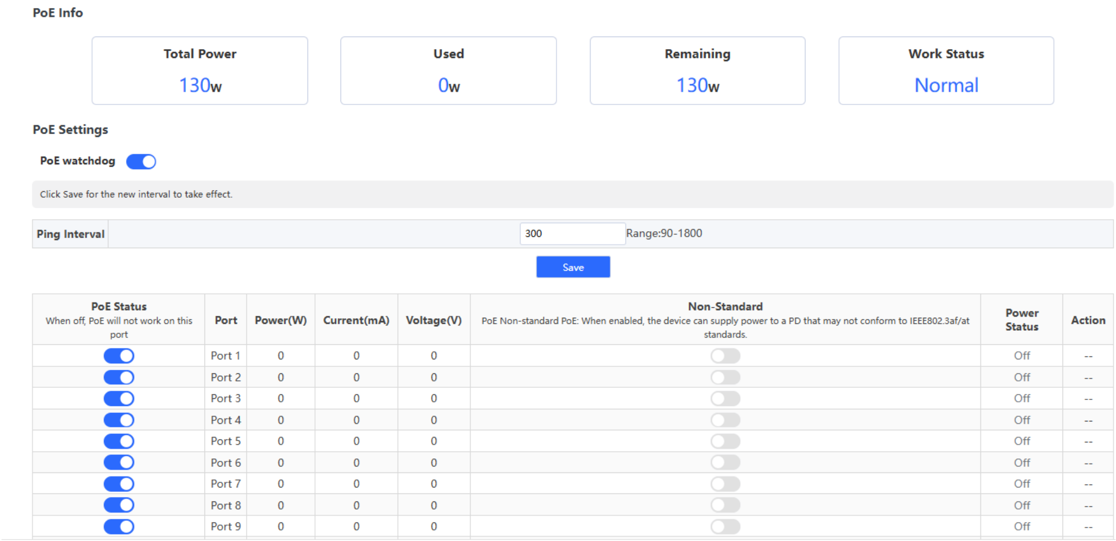
**Table 6-1 PoE Watchdog Application Description**

| 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. |

- 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.

**Figure 1-22  PoE Information and Configuration**



PoE Info

| Total Power | Used | Remaining | Work Status |
|---|---|---|---|
| 130w | 0w | 130w | Normal |

PoE Settings

PoE watchdog ●

Click Save for the new interval to take effect.

Ping Interval: 300 Range:90-1800

| PoE Status<br>When off, PoE will not work on this port | Port | Power(W) | Current(mA) | Voltage(V) | Non-Standard<br>PoE Non-standard PoE: When enabled, the device can supply power to a PD that may not conform to IEEE802.3af/at standards. | Power Status | Action |
|---|---|---|---|---|---|---|---|
| ● | Port 1 | 0 | 0 | 0 | ○ | Off | -- |
| ● | Port 2 | 0 | 0 | 0 | ○ | Off | -- |
| ● | Port 3 | 0 | 0 | 0 | ○ | Off | -- |
| ● | Port 4 | 0 | 0 | 0 | ○ | Off | -- |
| ● | Port 5 | 0 | 0 | 0 | ○ | Off | -- |
| ● | Port 6 | 0 | 0 | 0 | ○ | Off | -- |
| ● | Port 7 | 0 | 0 | 0 | ○ | Off | -- |
| ● | Port 8 | 0 | 0 | 0 | ○ | Off | -- |
| ● | Port 9 | 0 | 0 | 0 | ○ | Off | -- |

# 7 ERPS

**Specification**

This feature is only supported on the RG-NIS2100 series.

## 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.

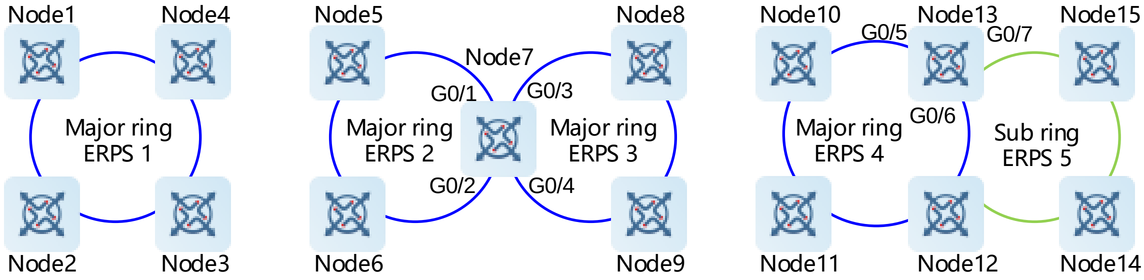
## 7.3 Basic Model of an Ethernet Ring

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 1-23. 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 1-23. 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 1-23, 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 1-23 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 1-23.

- 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 1-23, 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 1-23, 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 1-23, 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 1-23:

- 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.

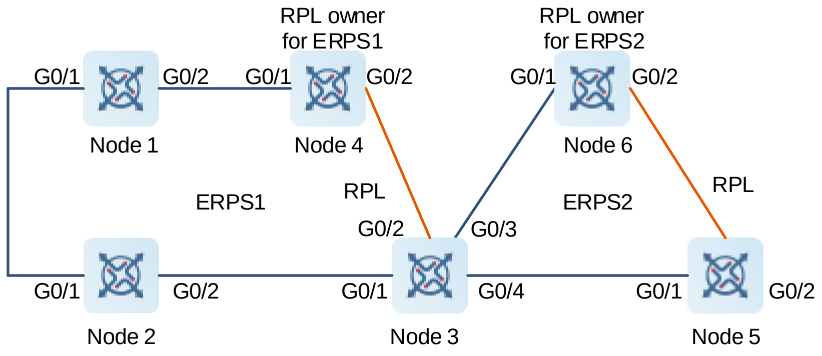
Ring protection link (RPL): When the physical links in a ring network are connected, the ERPS ring is in the idle state, and the links in the logic blocking state are RPLs. Each Ethernet ring has only one RPL. For example, the links indicated by the orange lines shown in Figure 1-24 are RPLs, the link 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 1-24, 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 1-24, nodes except node 4 and node 6 are non-RPL owner nodes of the rings.

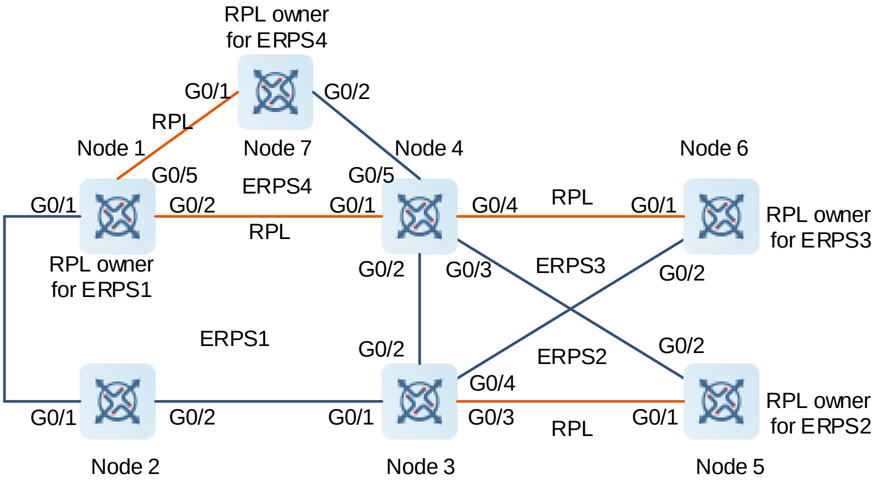
Blocked ports on RPLs are RPL ports, and RPL ports do not forward data packets to prevent loops. RPL ports are on RPL owner nodes, and the RPL owner nodes block the RPL ports. Each Ethernet ring has only one RPL owner node.

**Figure 1-24 Typical Topology of Tangent Rings**



As shown in Figure 1-24, 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 1-25 Typical Topology of Intersecting Rings**



As shown in Figure 1-25, 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

✓ **Specification**

A maximum of one ERPS ring can be configured in this ERPS version.

### 7.9.1 Adding an ERPS Ring

Choose **ERPS** from the navigation pane.

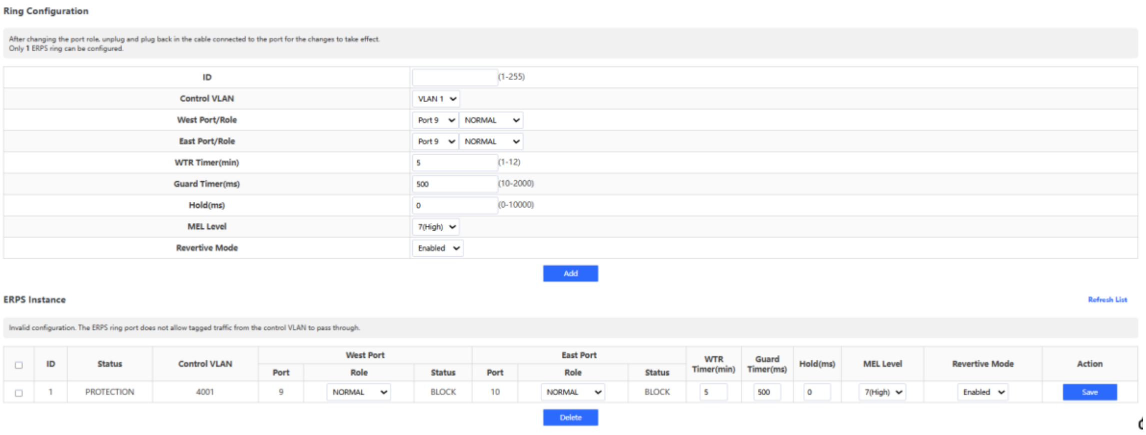
As shown in Figure 1-26, after configuring the ERPS ring parameters, click **Add** to add the ERPS ring.

Once the ERPS ring is successfully added, it will appear in the ERPS instances below.

**Table 7-2 Parameter Description**

| Parameter | Description | Default Value |
|---|---|---|
| ID | Specifies the ID of an ERPS instance. | No default value |
| Control VLAN | It is used to forward ERPS protocol packets. | No default value |
| West Port/Role | Specifies the west port in the ERPS ring and its role.<br>The values of a port role include:<br>● **NORMAL**: Indicates a normal node.<br>● **RPL OWNER**: Indicates an RPL owner node.<br>● **RPL NEIGHBOR**: Indicates an RPL neighbor node. | No default value |
| East Port/Role | Specifies the east port in the ERPS ring and its role.<br>The values of a port role include:<br>● **NORMAL**: Indicates a normal node.<br>● **RPL OWNER**: Indicates an RPL owner node.<br>● **RPL NEIGHBOR**: Indicates an RPL neighbor node. | No default value |
| 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 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 it is toggled on, once the condition causing a link failure has been cleared, traffic is blocked on the RPL. | Enabled. |

Figure 1-26  Adding an ERPS Ring



Ring Configuration

After changing the port role, unplug and plug back in the cable connected to the port for the changes to take effect.
Only 1 ERPS ring can be configured.

| | |
|---|---|
| ID | (1-255) |
| Control VLAN | VLAN 1 |
| West Port/Role | Port 9 NORMAL |
| East Port/Role | Port 9 NORMAL |
| WTR Timer(min) | 5 (1-12) |
| Guard Timer(ms) | 500 (10-2000) |
| Hold(ms) | 0 (0-10000) |
| MEL Level | 7(High) |
| Revertive Mode | Enabled |

ERPS Instance

Invalid configuration. The ERPS ring port does not allow tagged traffic from the control VLAN to pass through.

| □ | ID | Status | Control VLAN | West Port | | | East Port | | | WTR Timer(min) | Guard Timer(ms) | Hold(ms) | MEL Level | Revertive Mode | Action |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | Port | Role | Status | Port | Role | Status | | | | | | |
| □ | 1 | PROTECTION | 4001 | 9 | NORMAL | BLOCK | 10 | NORMAL | BLOCK | 5 | 500 | 0 | 7(High) | Enabled | Save |

**Note**

- The west port and the east port must be trunk ports. For details on how to configure trunk ports, see 4.2.3 Port VLAN Settings.
- You can select a control VLAN when it is a permit VLAN rather than a native VLAN, and the west or east port is a trunk port.
- ERPS can be enabled or disabled through the DIP switch on the device's front panel or through the web interface. The latest configuration takes effect.
- If ERPS is enabled through the DIP switch on the device's front panel but not the web interface, the device will automatically create an ERPS ring with the following default settings: Ring ID 1, Control VLAN 4001, west port 9 in NORMAL state, east port 10 in NORMAL state, WTR timer set to 5 minutes, Guard timer set to 500 milliseconds, Hold timer set to 0 milliseconds, MEL level 7, and revertive mode enabled.
- When ERPS is enabled on the web interface, it is disabled through the DIP switch on the device's front panel, and then it is enabled, the configuration on the web interface takes effect.

## 7.9.2 Checking, Modifying, or Deleting an ERPS Ring

Choose **ERPS**.

- Check an ERPS ring. Once a ring is created, you can check its status and configuration details in the ERPS instances.

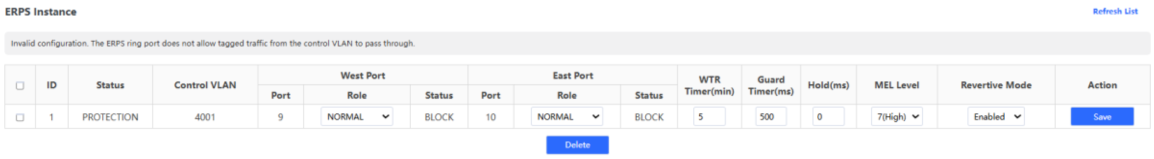
Figure 1-27  ERPS Ring Status

| Status | Description |
|---|---|
| IDLE | When the ring network is operating stably, one port of the device on the ring network will be in blocked state. |
| PENDING | The protocol negotiation is in progress within the ring network which has already been formed, and after the negotiation is completed, the ring network will enter the **IDLE** state. |
| PROTECTION | A device in the ring network is faulty, and the ring network cannot be formed. |
| Forced switch | The configuration in **Link Switch** is being delivered to the devices on the ring network. |

- Modify an ERPS ring. After an ERPS ring is created, you can modify parameters such as the roles of the west and east ports, **WTR Timer**, and **Guard Timer**. When the modifications are complete, click **Save**.

- Delete an ERPS ring. To delete a created ERPS ring, select it and click **Delete** to remove it.

**Figure 1-28 Checking, Modifying, or Deleting an ERPS Ring**



ERPS Instance

Invalid configuration. The ERPS ring port does not allow tagged traffic from the control VLAN to pass through.

| □ | ID | Status | Control VLAN | West Port |  |  | East Port |  |  | WTR Timer(min) | Guard Timer(ms) | Hold(ms) | MEL Level | Revertive Mode | Action |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
|  |  |  |  | Port | Role | Status | Port | Role | Status |  |  |  |  |  |  |
| □ | 1 | PROTECTION | 4001 | 9 | NORMAL | BLOCK | 10 | NORMAL | BLOCK | 5 | 500 | 0 | 7(High) | Enabled | Save |

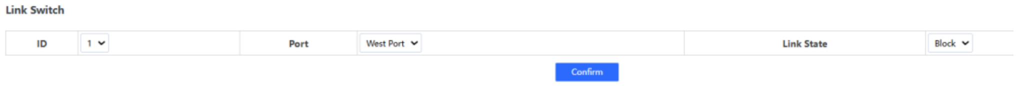
### 7.9.3 Link Switchover

Choose **ERPS**.

When a ring network is operating normally, one of the west or east ports will be used for data transmission, while the other will be in the blocked state. Through link switchover, you can specify which port on the current device is used for data transmission and which port is in blocked state.

Set **ID**, **Port**, and **Link State** based on service requirements. Then click **OK** to complete the link switchover for the ERPS ring.

**Figure 1-29 Link Switchover**



Link Switch

|  |  |  |  |  |  |
|---|---|---|---|---|---|
| ID | 1 | Port | West Port | Link State | Block |

**Figure 1-30 Parameter Description**

| Parameter | Description | Default Value |
|---|---|---|
| ID | Specifies the ID of an ERPS instance. | No default value |
| Port | Specifies the port in the ERPS ring. The values include **West Port** and **East Port**. | No default value |
| Link State | Specifies the link state of the selected port.<br>● **Clear**: Clears the forced switch state of the port, and allows the protocol to elect the port to be blocked.<br>● **Block**: Indicates that the port is blocked by a forced switch operation. | No default value |

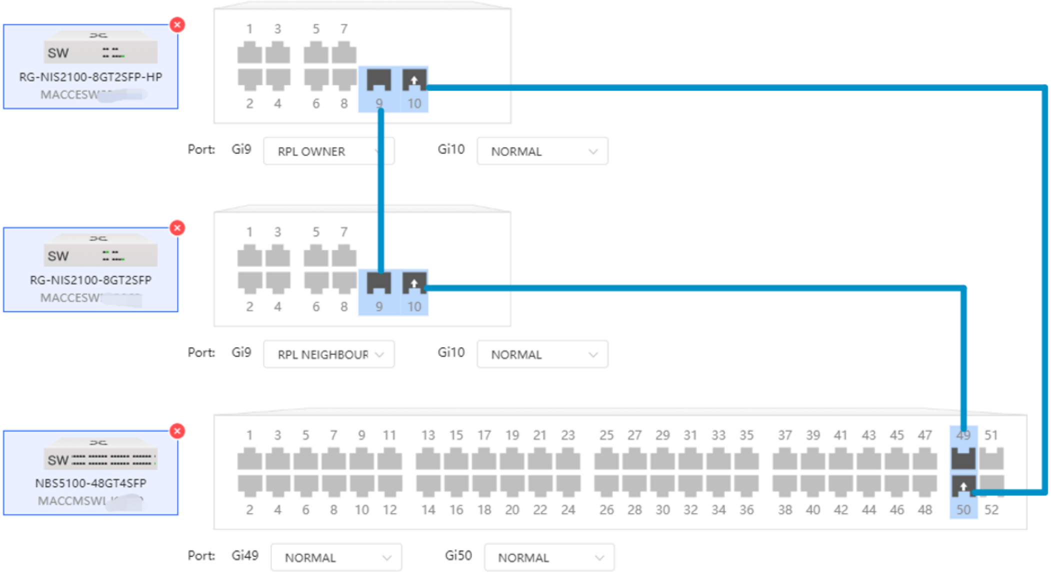
## 7.10 Typical ERPS Configuration Examples

**Specification**

ERPS ring network-wide configuration is supported only on ReyeeOS version 2.280 or later. Thus, the primary device on the network where the ERPS ring will be established must run ReyeeOS 2.280 or later.

Requirements: There are three devices on the user's network that need to form an ERPS ring. The specific topology is shown below.

**Figure 1-31 Network Diagram**



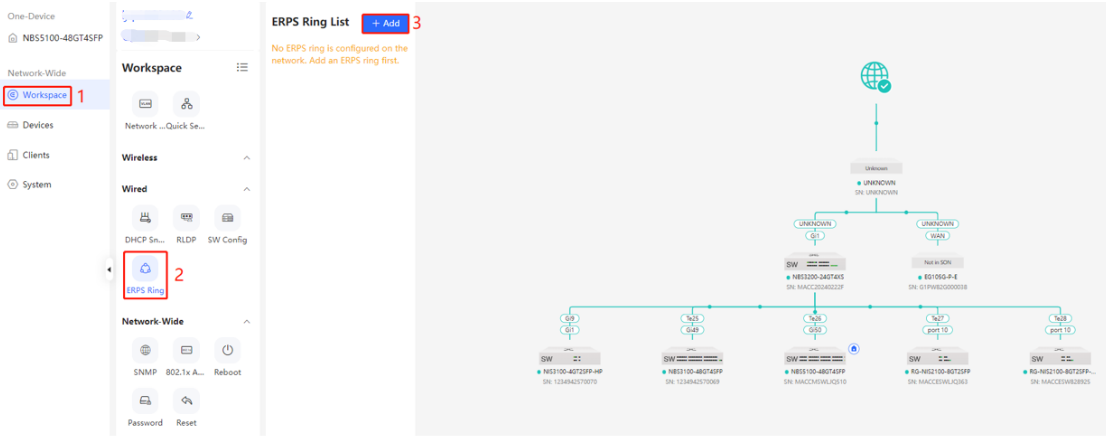
> **Note**
>
> - To prevent loops, configure ERPS before performing cable connections.
> - For an ERPS ring, only one interface can be the RPL Owner, and its peer interface must be the RPL Neighbor.

(1) Log in to the web interface of the primary device.

(2) Choose **Network-Wide** > **Workspace** > **Wired** > **ERPS Ring** to access the **ERPS Ring** configuration page.

(3) Click **+Add** on the page to add an ERPS ring.

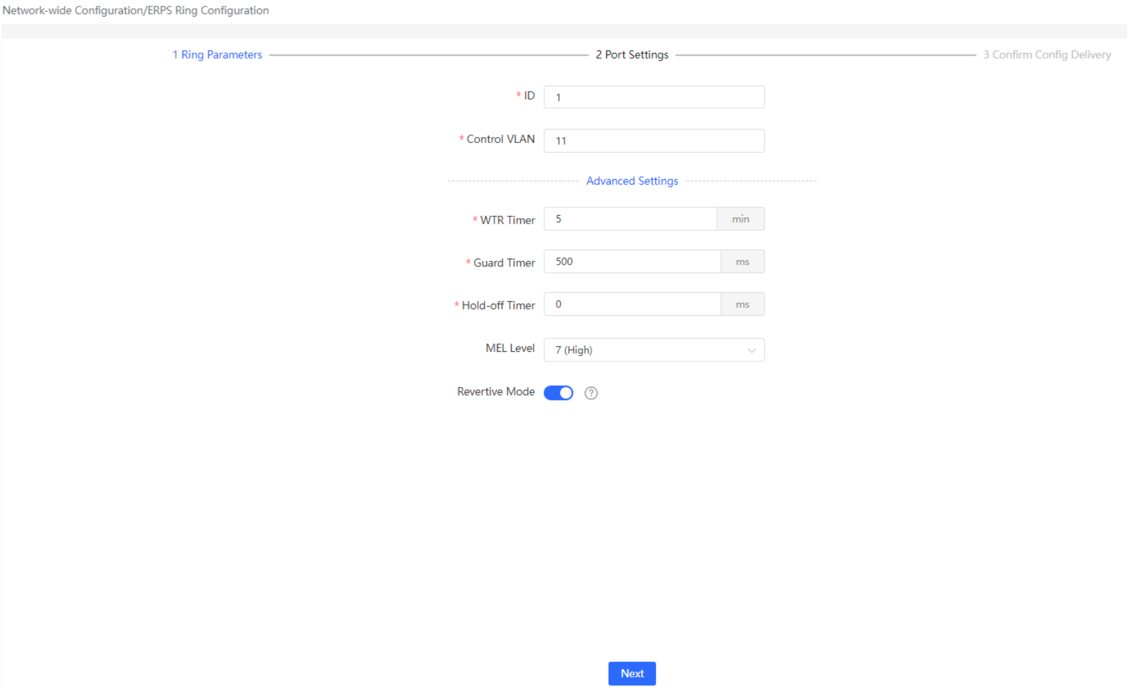
**Figure 1-32 ERPS Ring List**



No ERPS ring is configured on the network. Add an ERPS ring first.

(4) Set the ERPS ring parameters (only **ID** and **Control VLAN** are mandatory, and should be configured according to the user's network setup. Other parameters can remain at their default values). Then, click **Next**.

**Figure 1-33 Ring Parameter Settings**



Network-wide Configuration/ERPS Ring Configuration

1 Ring Parameters — 2 Port Settings — 3 Confirm Config Delivery

* ID: 1

* Control VLAN: 11

Advanced Settings

* WTR Timer: 5 min

* Guard Timer: 500 ms

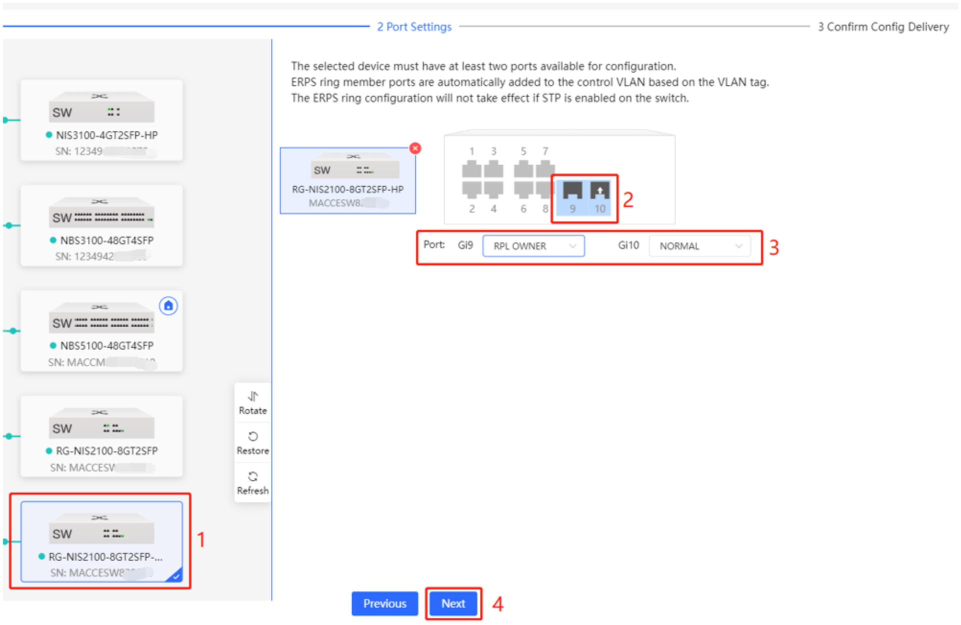
* Hold-off Timer: 0 ms

MEL Level: 7 (High)

Revertive Mode: on

(5) Select a device for the ERPS ring, set **Gi9** to **RPL OWNER**, and **Gi10** to **NORMAL**. Click **Next**.

**Figure 1-34 Port Settings**



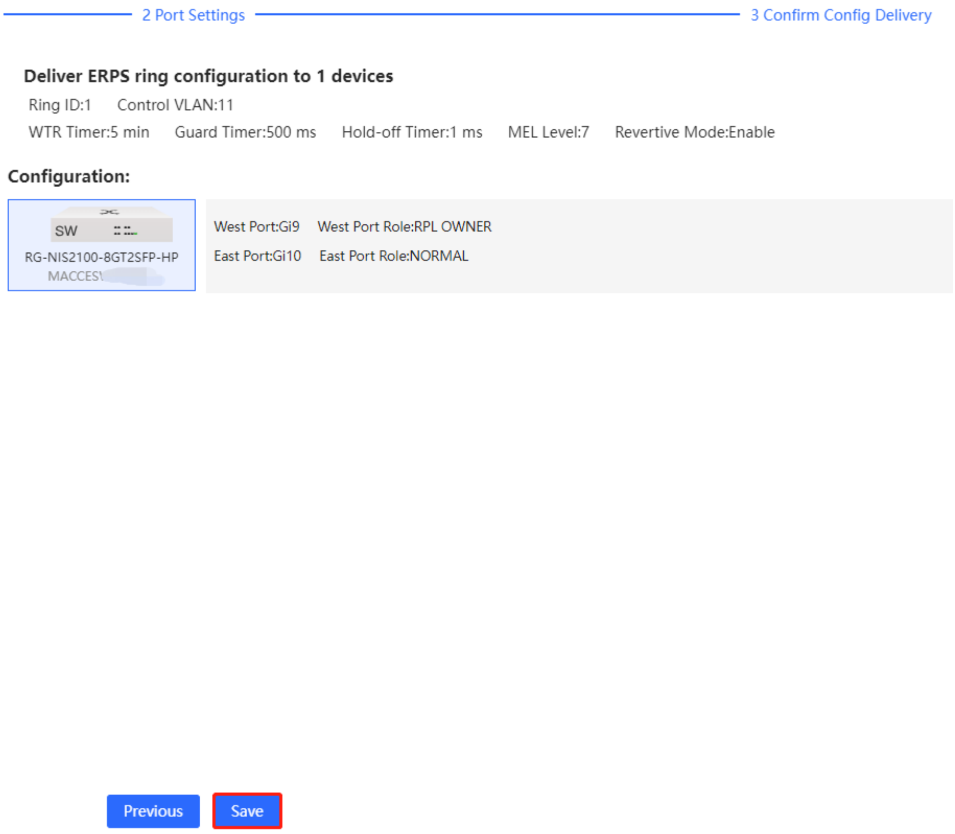
2 Port Settings — 3 Confirm Config Delivery

The selected device must have at least two ports available for configuration.
ERPS ring member ports are automatically added to the control VLAN based on the VLAN tag.
The ERPS ring configuration will not take effect if STP is enabled on the switch.

Port: Gi9 RPL OWNER Gi10 NORMAL

(6) Click **Save**.

Figure 1-35 Configuration Delivery Confirmation



**Deliver ERPS ring configuration to 1 devices**

Ring ID:1 Control VLAN:11

WTR Timer:5 min Guard Timer:500 ms Hold-off Timer:1 ms MEL Level:7 Revertive Mode:Enable

**Configuration:**

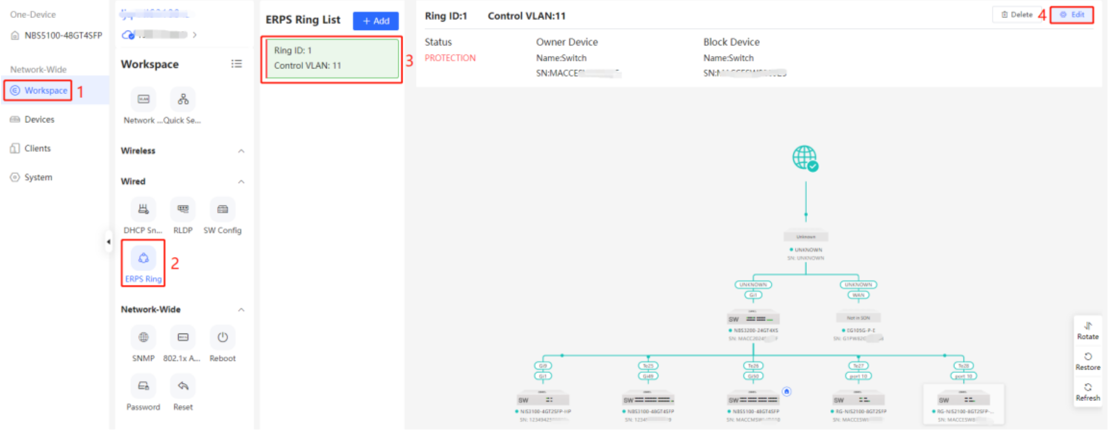
RG-NIS2100-8GT2SFP-HP
MACCES

West Port:Gi9 West Port Role:RPL OWNER

East Port:Gi10 East Port Role:NORMAL

(7) Choose **Network-Wide** > **Workspace** > **Wired** > **ERPS Ring**. On the page that opens, click **Edit**.

Figure 1-36 Editing the Created Ring



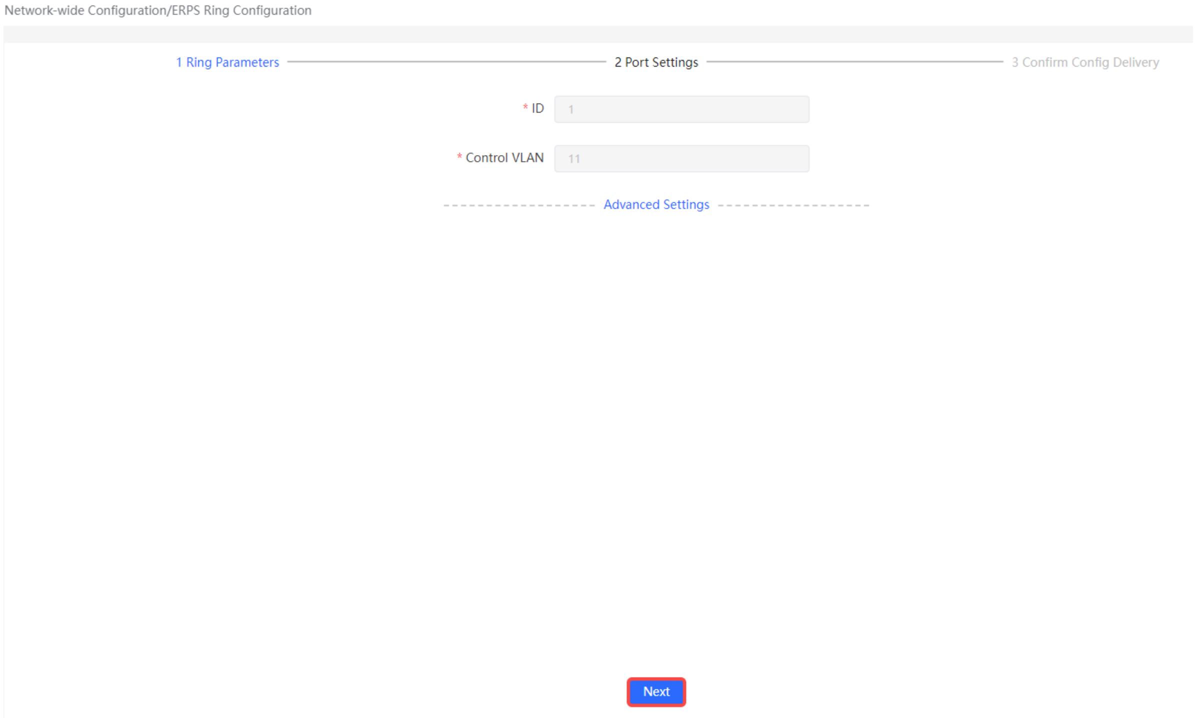
Ring ID: 1
Control VLAN: 11

Ring ID:1 Control VLAN:11

| Status | Owner Device | Block Device |
|---|---|---|
| PROTECTION | Name:Switch<br>SN:MACCE | Name:Switch<br>SN: |

(8) Click **Next** to access the **ERPS Ring Configuration** page.

**Figure 1-37 Confirming the Ring Information**



Network-wide Configuration/ERPS Ring Configuration

1 Ring Parameters — 2 Port Settings — 3 Confirm Config Delivery

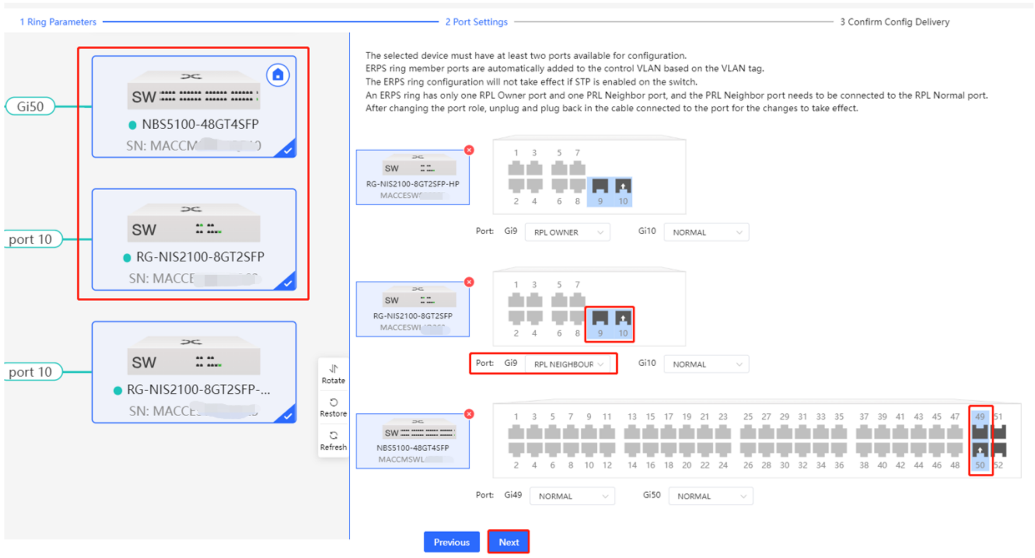
* ID: 1

* Control VLAN: 11

Advanced Settings

(9) Add the remaining devices on the **ERPS Ring Configuration** page. Select the optical ports on the devices and configure the interfaces connected to the RPL OWNER as RPL NEIGHBOR, following the example of Gi9 in the figure below. Configure other interfaces as NORMAL. After completing the configuration, click **Next**.

**Figure 1-38 Adding Remaining Ring Devices**



1 Ring Parameters — 2 Port Settings — 3 Confirm Config Delivery

The selected device must have at least two ports available for configuration.
ERPS ring member ports are automatically added to the control VLAN based on the VLAN tag.
The ERPS ring configuration will not take effect if STP is enabled on the switch.
An ERPS ring has only one RPL Owner port and one PRL Neighbor port, and the PRL Neighbor port needs to be connected to the RPL Normal port.
After changing the port role, unplug and plug back in the cable connected to the port for the changes to take effect.

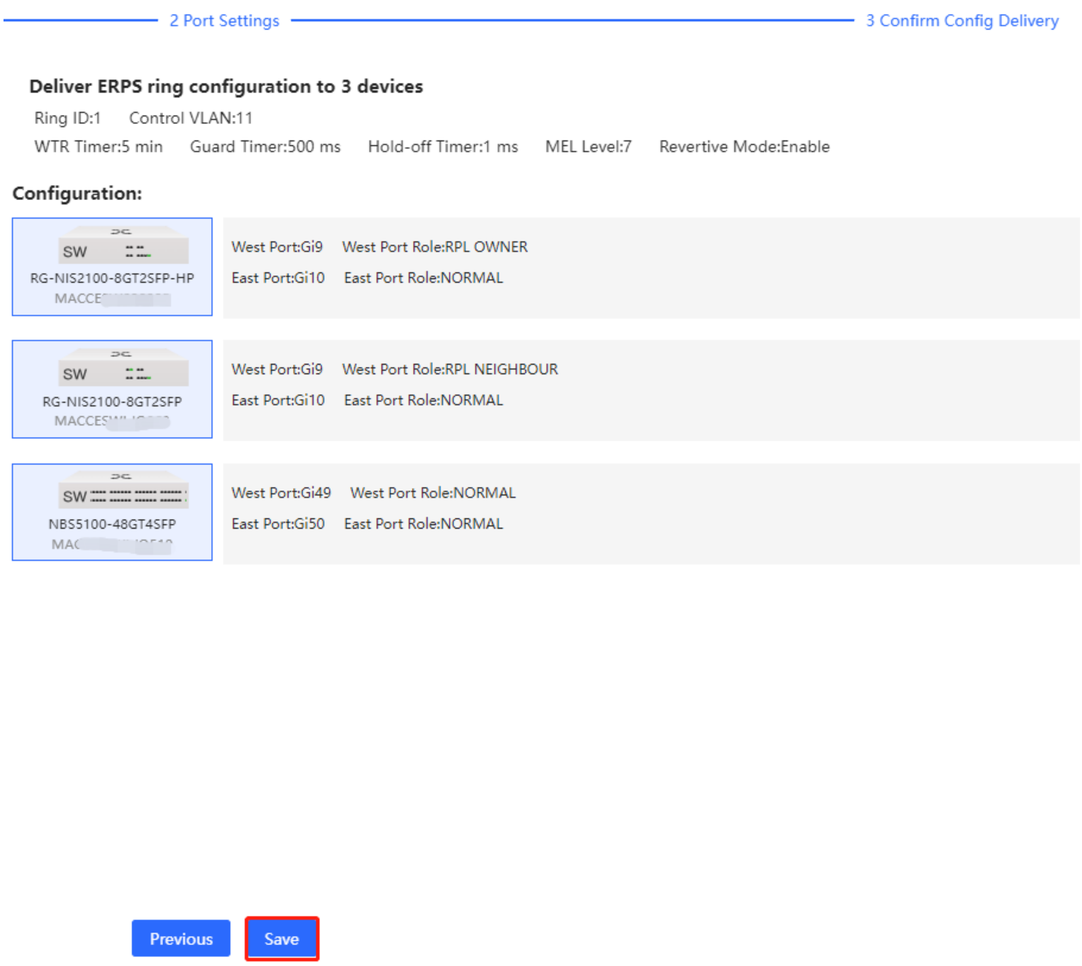
RG-NIS2100-8GT2SFP-HP — Port: Gi9 RPL OWNER; Gi10 NORMAL

RG-NIS2100-8GT2SFP — Port: Gi9 RPL NEIGHBOUF; Gi10 NORMAL

NBS5100-48GT4SFP — Port: Gi49 NORMAL; Gi50 NORMAL

(10) Click **Save** to apply all configurations.

**Figure 1-39 Delivering the Configuration**



**Deliver ERPS ring configuration to 3 devices**

Ring ID:1 Control VLAN:11

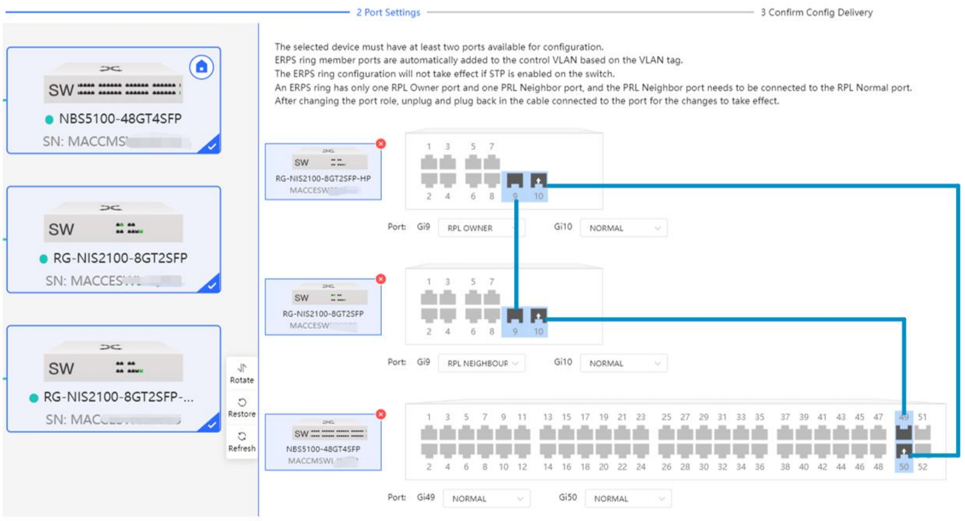
WTR Timer:5 min Guard Timer:500 ms Hold-off Timer:1 ms MEL Level:7 Revertive Mode:Enable

**Configuration:**

| | |
|---|---|
| RG-NIS2100-8GT2SFP-HP<br>MACCE[redacted] | West Port:Gi9 West Port Role:RPL OWNER<br>East Port:Gi10 East Port Role:NORMAL |
| RG-NIS2100-8GT2SFP<br>MACCES[redacted] | West Port:Gi9 West Port Role:RPL NEIGHBOUR<br>East Port:Gi10 East Port Role:NORMAL |
| NBS5100-48GT4SFP<br>MAC[redacted] | West Port:Gi49 West Port Role:NORMAL<br>East Port:Gi50 East Port Role:NORMAL |

After all cables are connected according to the topology, the devices will automatically form an ERPS ring.

**Figure 1-40 Ring Connection**



The selected device must have at least two ports available for configuration.
ERPS ring member ports are automatically added to the control VLAN based on the VLAN tag.
The ERPS ring configuration will not take effect if STP is enabled on the switch.
An ERPS ring has only one RPL Owner port and one PRL Neighbor port, and the PRL Neighbor port needs to be connected to the RPL Normal port.
After changing the port role, unplug and plug back in the cable connected to the port for the changes to take effect.

Port: Gi9 RPL OWNER Gi10 NORMAL

Port: Gi9 RPL NEIGHBOUR Gi10 NORMAL

Port: Gi49 NORMAL Gi50 NORMAL

# 8 Toolkit

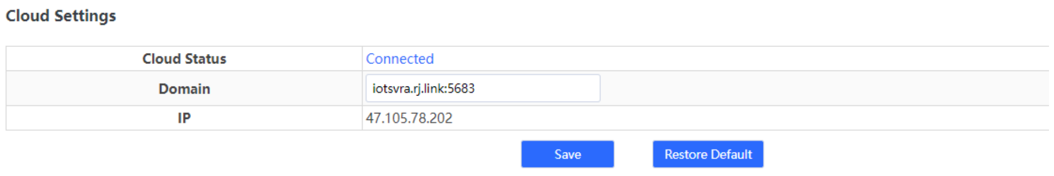
## 8.1 Cloud Settings

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

On Ruijie Cloud, you can check the status of your device, including its cloud connectivity status, reason for failure to connect, and the domain name and IP address of the cloud server.

- To change the domain name of the device, enter the new domain name in the **Domain** field, and then click **Save**.
- To restore the default domain name, click **Restore Default**, and then click **OK** on the pop-up window.

**Figure 1-41 Cloud Settings**



Cloud Settings

| | |
|---|---|
| Cloud Status | Connected |
| Domain | iotsvra.rj.link:5683 |
| IP | 47.105.78.202 |

**Table 8-1 Cloud Settings Parameters**

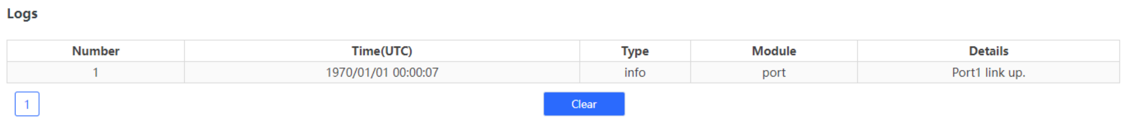
| Parameter | Description |
|---|---|
| Cloud Status | Indicates the connectivity status of the device on the cloud, including **Connected**, **Unconnected** and **Connectable**. |
| Reason | Indicates the reason for connection failure. Reasons for different cloud statuses:<br>● **Connected**: No reason is displayed.<br>● **Unconnected**:<br>○ No Internet connection or DNS resolution failure.<br>○ This device failed to connect to Ruijie Cloud.<br>● **Connectable**: This device is not registered to Ruijie Cloud. |
| Domain | Domain name of the cloud server<br>⚠ **Caution**<br>● The coap:// prefix is not required in the domain name field as it is added by default.<br>● After the domain name is changed, the page is refreshed after 5 seconds by default. |
| IP | IP address of the cloud server resolved based on the cloud address. |

## 8.2 System Logs

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

System logs record device operations, operation time, and operation modules. System logs are used by administrators to monitor the running status of the device, analyze network status, and locate faults.

**Figure 1-42 System Logs**



Logs

| Number | Time(UTC) | Type | Module | Details |
|---|---|---|---|---|
| 1 | 1970/01/01 00:00:07 | info | port | Port1 link up. |

⚠ 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.

# 9 System Settings

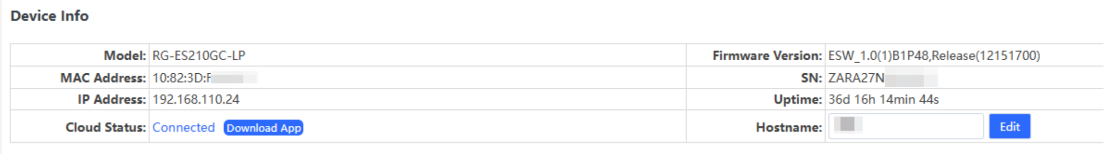
## 9.1 Managing Device Information

### 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**.

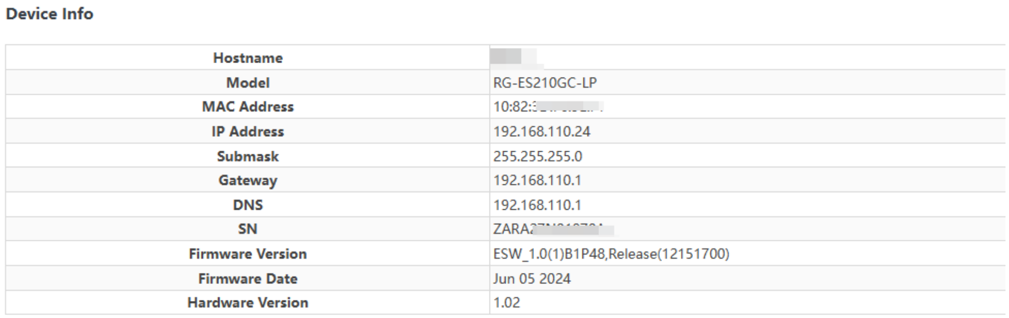
**Figure 1-43 Device Info**



Device Info

| | | | |
|---|---|---|---|
| Model: | RG-ES210GC-LP | Firmware Version: | ESW_1.0(1)B1P48,Release(12151700) |
| MAC Address: | 10:82:3D:F[redacted] | SN: | ZARA27N[redacted] |
| IP Address: | 192.168.110.24 | Uptime: | 36d 16h 14min 44s |
| Cloud Status: | Connected Download App | Hostname: | [redacted] Edit |

Figure 1-44 Viewing Device Information



Device Info

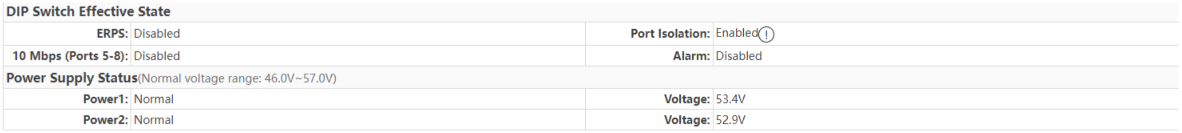
| | |
|---|---|
| Hostname | [redacted] |
| Model | RG-ES210GC-LP |
| MAC Address | 10:82:[redacted] |
| IP Address | 192.168.110.24 |
| Submask | 255.255.255.0 |
| Gateway | 192.168.110.1 |
| DNS | 192.168.110.1 |
| SN | ZARA2[redacted] |
| Firmware Version | ESW_1.0(1)B1P48,Release(12151700) |
| Firmware Date | Jun 05 2024 |
| Hardware Version | 1.02 |

**Specification**

Only the **Home** page of the RG-NIS2100 series displays the DIP switch effective state and the power supply status.

- **DIP Switch Effective State**: You can view the configuration status of ERPS, port isolation, forced 10 Mbps, and power alarm (If the configured function conflicts with the DIP switch settings, the ⓘ icon will appear next to the function. Hovering over the icon will display a prompt showing the current effective state of the DIP switch.).
- **Power Supply Status**: You can view the status and the voltage of the power supply.

Figure 1-45 Decoding/Power Status



DIP Switch Effective State

| | | | |
|---|---|---|---|
| ERPS: | Disabled | Port Isolation: | Enabled ⓘ |
| 10 Mbps (Ports 5-8): | Disabled | Alarm: | Disabled |

Power Supply Status(Normal voltage range: 46.0V~57.0V)

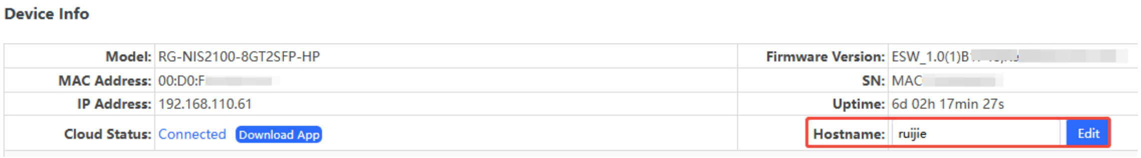
| | | | |
|---|---|---|---|
| Power1: | Normal | Voltage: | 53.4V |
| Power2: | Normal | Voltage: | 52.9V |

## 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 1-46 Editing the Hostname



Device Info

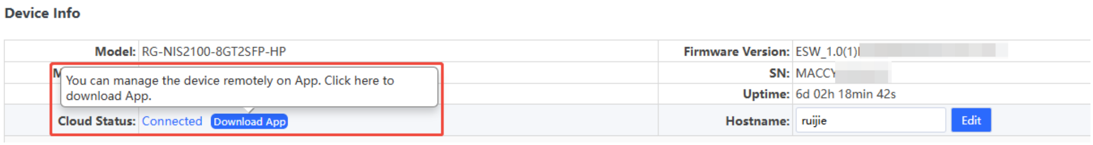
| | | | |
|---|---|---|---|
| Model: | RG-NIS2100-8GT2SFP-HP | Firmware Version: | ESW_1.0(1)B[redacted] |
| MAC Address: | 00:D0:F[redacted] | SN: | MAC[redacted] |
| IP Address: | 192.168.110.61 | Uptime: | 6d 02h 17min 27s |
| Cloud Status: | Connected Download App | Hostname: | ruijie Edit |

## 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](https://cloud-as.ruijienetworks.com)). Click **Download APP** to download Ruijie Cloud APP.

**Figure 1-47 Cloud Management**



Device Info

Model: RG-NIS2100-8GT2SFP-HP

Firmware Version: ESW_1.0(1)[redacted]

You can manage the device remotely on App. Click here to download App.

SN: MACCY[redacted]

Uptime: 6d 02h 18min 42s

Cloud Status: Connected Download App

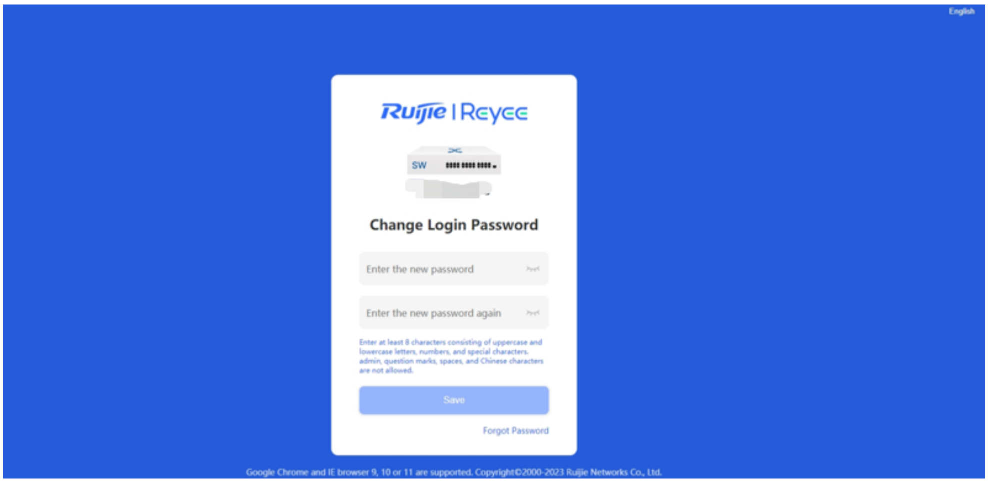
Hostname: ruijie

## 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 1-48 Setting the Login Password on the Login Page**



Change Login Password

Enter the new password

Enter the new password again

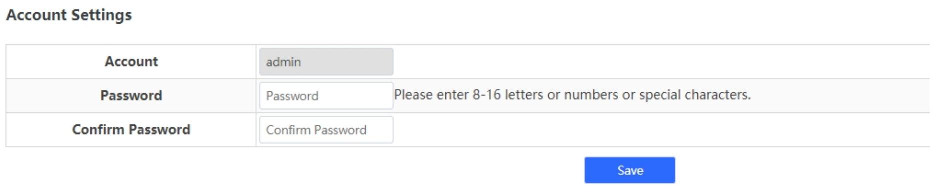
Enter at least 8 characters consisting of uppercase and lowercase letters, numbers, and special characters. admin, question marks, spaces, and Chinese characters are not allowed.

Google Chrome and IE browser 9, 10 or 11 are supported. Copyright©2000-2023 Ruijie Networks Co., Ltd.

- 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 1-49 Setting the Login Password**



Account Settings

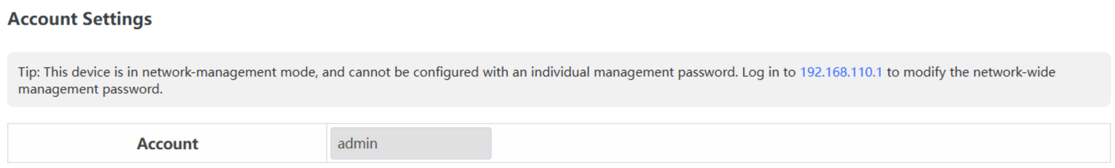
| | | |
|---|---|---|
| Account | admin | |
| Password | Password | Please enter 8-16 letters or numbers or special characters. |
| Confirm Password | Confirm Password | |

⚠ **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 1-50 Network-Management Mode**

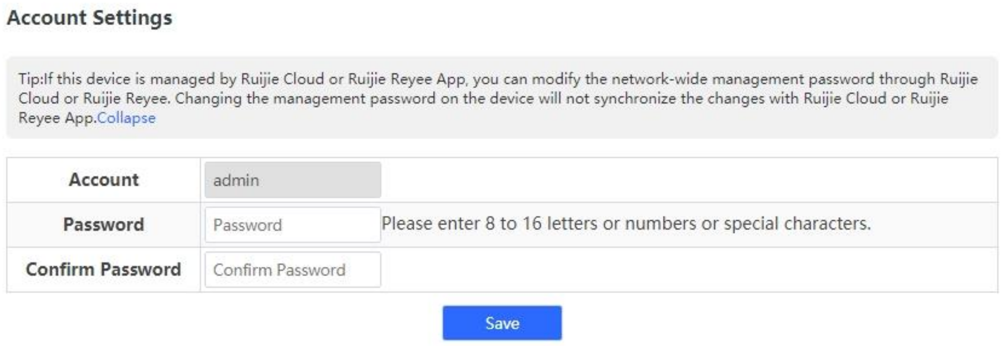


Account Settings

Tip: This device is in network-management mode, and cannot be configured with an individual management password. Log in to 192.168.110.1 to modify the network-wide management password.

| | |
|---|---|
| Account | admin |

**Figure 1-51 Management Through Ruijie Cloud or Ruijie Reyee App**



Account Settings

Tip: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. Changing the management password on the device will not synchronize the changes with Ruijie Cloud or Ruijie Reyee App.Collapse

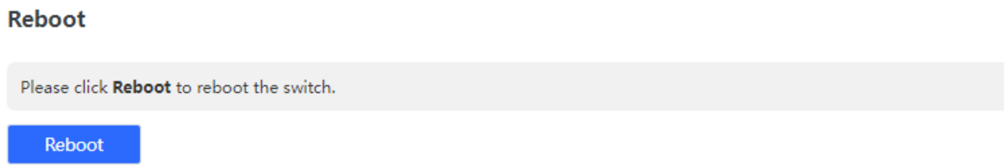
| | |
|---|---|
| Account | admin |
| Password | Password Please enter 8 to 16 letters or numbers or special characters. |
| Confirm Password | Confirm Password |

## 9.3 Device Reboot

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

Click **Reboot** to reboot the switch.

**Figure 1-52 Device Reboot**



Reboot

Please click **Reboot** to reboot the switch.

## 9.4 Setting the Maximum Power of the Power Supply

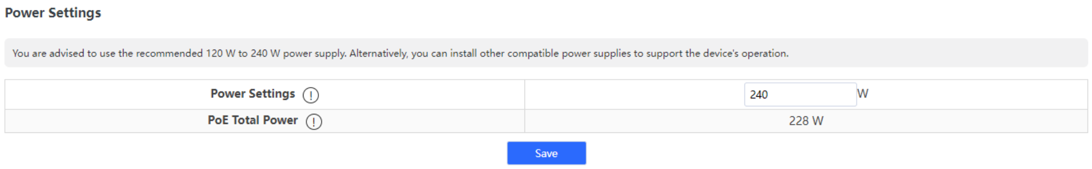
Choose **Configuration** > **Power Settings**.

If the power of the actual power supply differs significantly from the default power of the switch, adjust the power settings on the **Power Settings** page in a timely manner to avoid misoperation or unnecessary power consumption.

**Specification**

- The power value should approximate the actual output power of the power supply.
- This feature is only supported on the RG-NIS2100 series.

**Figure 1-53 Setting the Maximum Power**



Power Settings

You are advised to use the recommended 120 W to 240 W power supply. Alternatively, you can install other compatible power supplies to support the device's operation.

| | |
|---|---|
| Power Settings ⓘ | 240 W |
| PoE Total Power ⓘ | 228 W |

## 9.5 System Upgrade

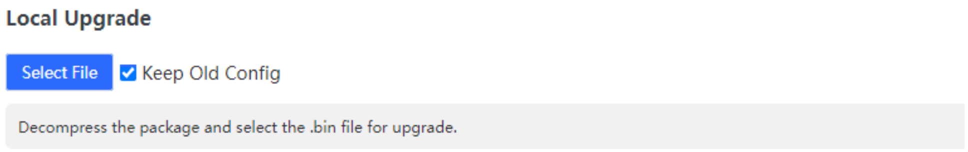
### 9.5.1 Local Upgrade

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 1-54 Local Upgrade**



Local Upgrade

☑ Keep Old Config

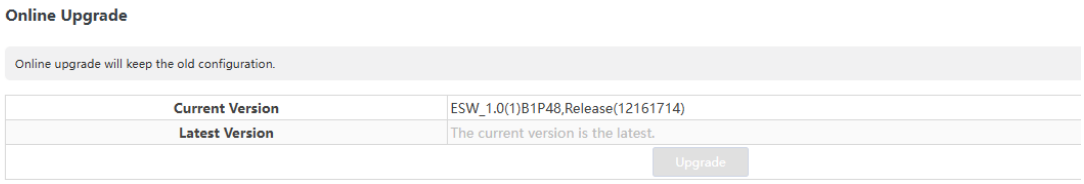
Decompress the package and select the .bin file for upgrade.

### 9.5.2 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 1-55 Online Upgrade**



**Online Upgrade**

Online upgrade will keep the old configuration.

| | |
|---|---|
| **Current Version** | ESW_1.0(1)B1P48,Release(12161714) |
| **Latest Version** | The current version is the latest. |

**Note**

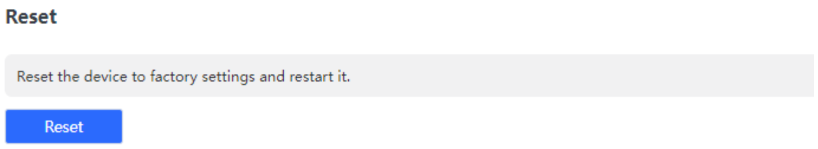
The time that online upgrade takes depends on the current network speed. It may take some time. Please be patient.

## 9.6 Restoring Factory Configuration

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

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

**Figure 1-56 Restoring Factory Configuration**



**Reset**

Reset the device to factory settings and restart it.

# 10 Monitoring

## 10.1 Cable Test

**Note**

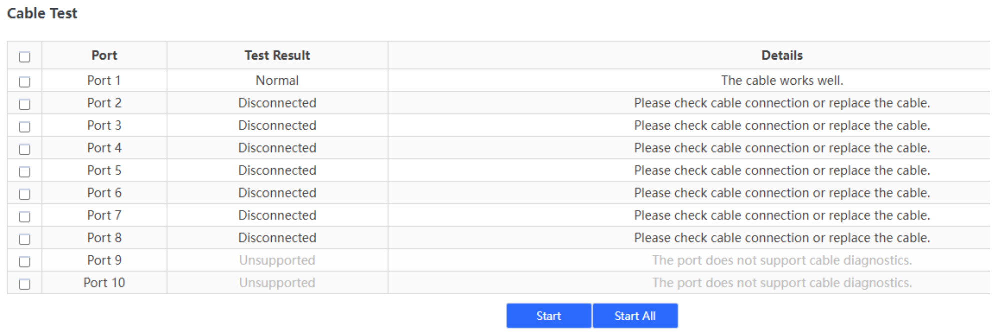
Only RJ45 ports support the cable test feature.

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 1-57 Cable Test**



Cable Test

| □ | Port | Test Result | Details |
|---|---|---|---|
| □ | Port 1 | Normal | The cable works well. |
| □ | Port 2 | Disconnected | Please check cable connection or replace the cable. |
| □ | Port 3 | Disconnected | Please check cable connection or replace the cable. |
| □ | Port 4 | Disconnected | Please check cable connection or replace the cable. |
| □ | Port 5 | Disconnected | Please check cable connection or replace the cable. |
| □ | Port 6 | Disconnected | Please check cable connection or replace the cable. |
| □ | Port 7 | Disconnected | Please check cable connection or replace the cable. |
| □ | Port 8 | Disconnected | Please check cable connection or replace the cable. |
| □ | Port 9 | Unsupported | The port does not support cable diagnostics. |
| □ | Port 10 | Unsupported | The port does not support cable diagnostics. |

⚠ **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

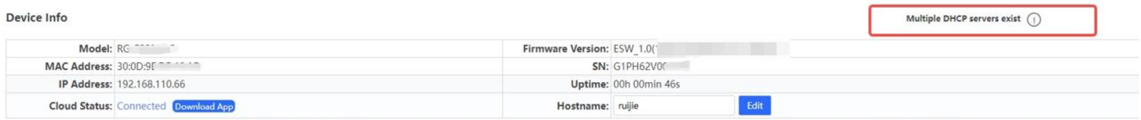
⚠ **Caution**

Multi-DHCP alarming will fail when the device IP address is not obtained dynamically. For relevant IP address configuration, see 3.6 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 1-58 Multi-DHCP Alarming**



Device Info

Multiple DHCP servers exist ⓘ

| | | | |
|---|---|---|---|
| Model: | RG [redacted] | Firmware Version: | ESW_1.0( [redacted] |
| MAC Address: | 30:0D:9E [redacted] | SN: | G1PH62V0( [redacted] |
| IP Address: | 192.168.110.66 | Uptime: | 00h 00min 46s |
| Cloud Status: | Connected Download App | Hostname: | ruijie Edit |

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

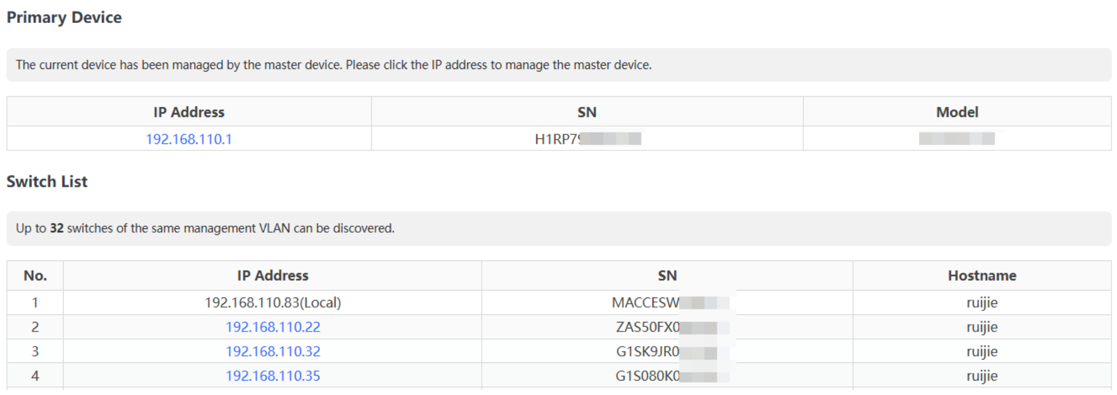
  If the switch is under uniform management, some features cannot be configured independently (such as password settings). To facilitate configuration, information of the primary device in the VLAN will be displayed on this page. Click the IP address of the primary device to access the **Primary Device** 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 1-59 Viewing Switches on the Network**



Primary Device

The current device has been managed by the master device. Please click the IP address to manage the master device.

| IP Address | SN | Model |
|---|---|---|
| 192.168.110.1 | H1RP7[redacted] | [redacted] |

Switch List

Up to **32** switches of the same management VLAN can be discovered.

| No. | IP Address | SN | Hostname |
|---|---|---|---|
| 1 | 192.168.110.83(Local) | MACCESW[redacted] | ruijie |
| 2 | 192.168.110.22 | ZAS50FX0[redacted] | ruijie |
| 3 | 192.168.110.32 | G1SK9JR0[redacted] | ruijie |
| 4 | 192.168.110.35 | G1S080K0[redacted] | ruijie |

**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.