Ruijie Reyee RG-ES220GS-LP and RG-ES228GS-LP Switches ESW_1.0(1)B1P43

Configuration Guide

Document Version: V1.0
Date: April 22, 2025
Copyright © 2025 Ruijie Networks

Copyright

Copyright © 2025 Ruijie Networks

All rights are reserved in this document and this statement.

Without the prior written consent of Ruijie Networks, any organization or individual shall not reproduce, extract, back up, modify, or propagate the content of this document in any manner or in any form, or translate it into other languages or use some or all parts of the document for commercial purposes.



and other Ruijie networks logos are trademarks of Ruijie Networks.

All other trademarks or registered trademarks mentioned in this document are owned by their respective owners.

Disclaimer

The products, services, or features that you purchase are subject to commercial contracts and terms. It is possible that some or all of the products, services, or features described in this document may not be available for purchase or use. Unless agreed upon otherwise in the contract, Ruijie Networks does not provide any explicit or implicit statements or warranties regarding 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.

The content of this document is subject to constant change due to product version upgrades or other reasons. Thus, Ruijie Networks reserves the right to modify the content of the document without prior notice or prompt.

This manual serves solely as a user guide. While Ruijie Networks endeavors to ensure the accuracy and reliability of the content when compiling this manual, it does not guarantee that the content of the manual is free of errors or omissions. All information contained in this manual does not constitute any explicit or implicit warranties.

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

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

1. Signs

The signs used in this document are described as follows:

Danger

An alert that contains important safety instructions. Before you work on any equipment, be aware of the hazards involved and be familiar with standard practices in case of accidents.

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.

2. Notes

This manual presents installation instructions, troubleshooting techniques, technical specifications, cable and connector requirements, and usage guidelines. It is intended for users who want to gain insight into the above content and have some experience in installing and maintaining network hardware. It is assumed that users are already familiar with relevant terms and concepts.

Contents

Preface.....I

1 Release Note.....1

1.1 Hardware Support.....1

1.2 New Software Features.....1

2 Login.....2

2.1 Configuration Environment Requirements.....2

2.2 Login to eWeb.....2

2.2.1 Connecting to a Device.....2

2.2.2 Login to eWeb.....2

3 Port Management.....6

3.1 Managing Port Information.....6

3.1.1 Port Status Bar.....6

3.1.2 Port Information Overview.....7

3.1.3 Port Packet Statistics.....8

3.2 Setting and Viewing Basic Port Attributes.....8

3.2.1 Port Settings.....8

3.2.2 Port Status.....10

3.3 Port Mirroring.....10

3.3.1 Overview.....10

3.3.2 Configuration Steps.....10

3.4 Port Isolation.....11

3.5 Port-based Rate Limiting.....12

3.6 Management IP Address.....13

4 Switch Management....14
4.1 Managing MAC Addresses....14
4.1.1 Overview....14
4.1.2 Viewing the MAC Address Table....14
4.1.3 Searching for MAC Addresses....15
4.1.4 Configuring Static MAC Addresses....16
4.2 VLAN Settings....16
4.2.1 Global VLAN Settings....16
4.2.2 Static VLAN Settings....17
4.2.3 Port VLAN Settings....18
5 Security Management....19
5.1 DHCP Snooping....19
5.1.1 Overview....19
5.1.2 Procedure....19
5.2 Storm Control....20
5.2.1 Overview....20
5.2.2 Procedure....20
5.3 Loop Prevention....21
6 PoE Settings....22
7 Toolkit....24
7.1 Cloud Settings....24
7.1.1 Checking the Cloud Information....24
7.1.2 Introduction to CoAP....25
7.1.3 Configuring CoAPs-based Encryption....25

7.2 System Logs 29
8 System Settings 31
8.1 Managing Device Information 31
8.1.1 Viewing Device Information 31
8.1.2 Editing the Hostname 31
8.1.3 Cloud Management 31
8.2 Login Password Settings 32
8.3 Device Reboot 33
8.4 System Upgrade 34
8.4.1 Local Upgrade 34
8.4.2 Online Upgrade 34
8.5 Restoring Factory Configuration 35
9 Monitoring Management 36
9.1 Cable Test 36
9.2 Multi-DHCP Alarming 36
9.3 Viewing Switches on the Network 37
10 FAQs 38
10.1 I failed to log in to eWeb. What can I do? 38
10.2 What can I do if I forget my password? How can I restore the factory settings? 38

1 Release Note

This section describes the hardware support and new software features in the ESW_1.0(1)B1P43 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

Model	Hardware Version Number
RG-ES220GS-LP	1.0x
RG-ES228GS-LP	1.0x

1.2 New Software Features

Note

New software features refer to those supported from ESW_1.0(1)B1P43.

Table 1-2 New Software Features

Feature Name	Description
HTTPS	Log in to eWeb using HTTPS.
Encryption mode (CoAPs)	Configure the encryption mode CoAPs to secure data transmission.

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 Login to eWeb

2.2.1 Connecting to a Device

Connect a switch port to the Ethernet port of a PC through an Ethernet cable, and configure an IP address for the PC that is on the same network segment as the default IP address of the device. Ensure 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 Settings
Device IP	10.44.77.200
Password	admin

2.2.2 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.
- Upon your first login, you may be prompted with **Your connection isn't private**. In this case, click **Advanced** and then click **Continue to xx.xx.xx.xx (unsafe)** to access the login page.

Figure 2-1 Security Prompt for First-Time Access to eWeb

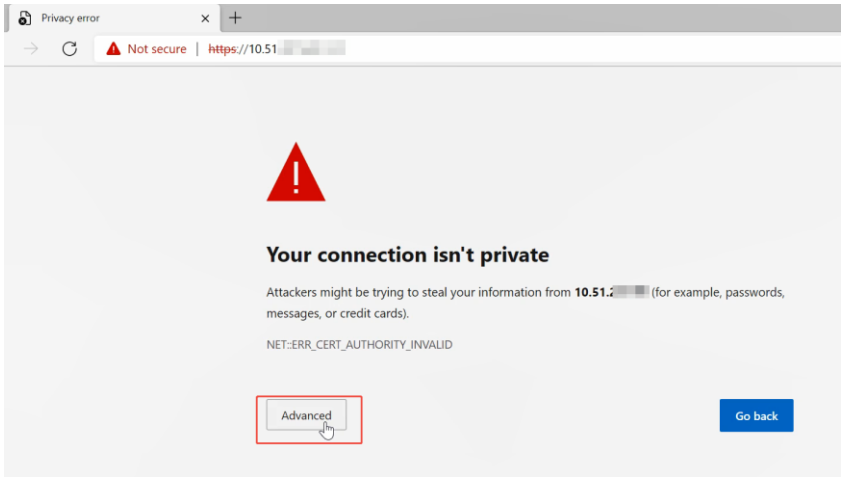
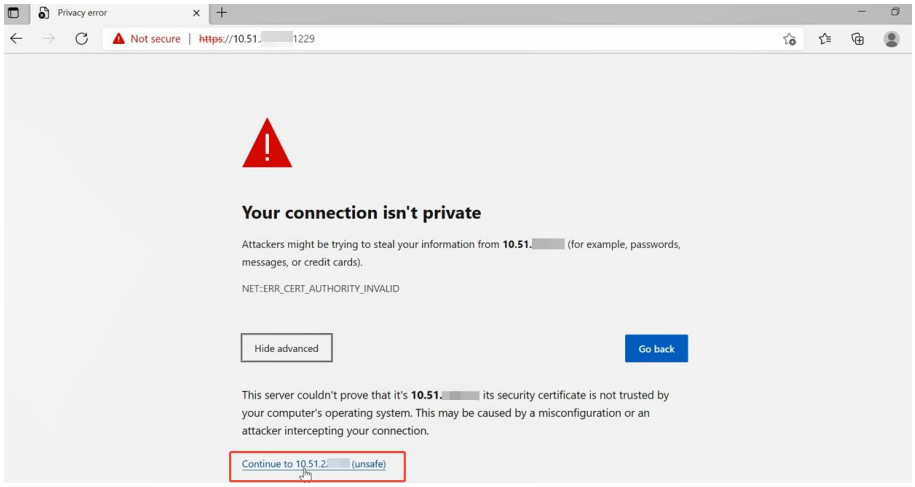
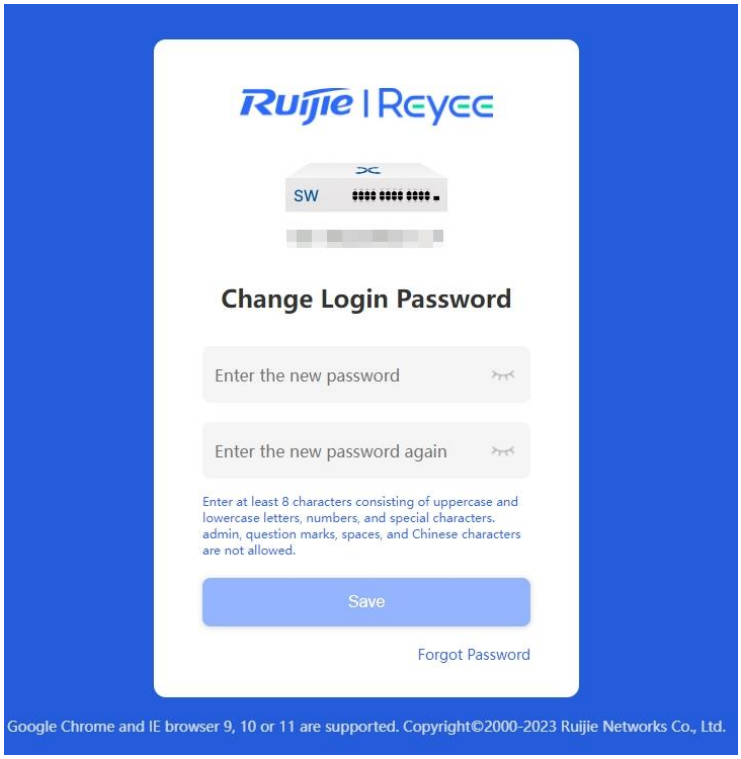


Figure 2-2 Continue Access



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

Figure 2-3 Login to eWeb Upon the First Time

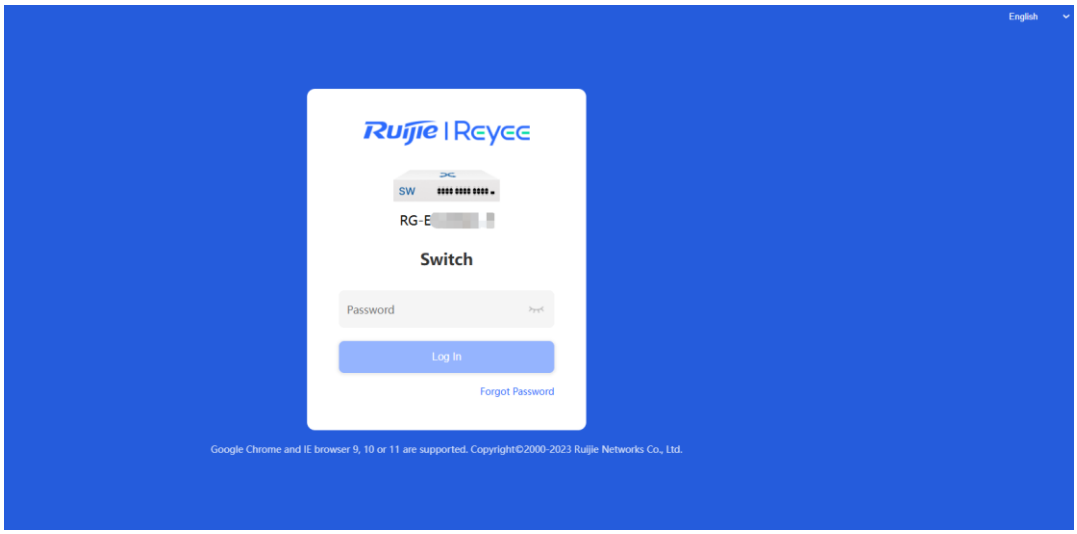


(3) On the login page, enter the password and click **Log In** to enter the homepage of eWeb.

Note

To change the login password, see 8.2 Login Password Settings.

Figure 2-4 eWeb Login Page



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

Caution

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

3 Port Management

3.1 Managing Port Information

3.1.1 Port Status Bar

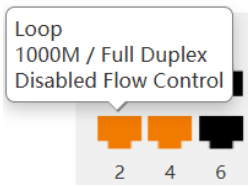
The port status bar is at the top of eWeb, showing the port ID, port attribute (uplink/downlink), connection status, and other information.

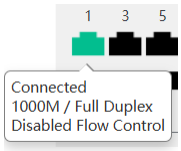
Figure 3-1 Port Status Bar



Different colors and shapes of the port icons represent different port status. 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.
	The color of the port icon is gray, showing the port is disabled and cannot receive or transmit packets.
	The color of the port icon is yellow, showing there is a loop.

Port Icon	Description
	The color of the port icon is green, showing the port is working normally.
	The number above the port icon is the port ID used to identify the device port. With the port ID, you can specify the target port.
	● The device port is classified into the uplink port and the downlink port. The uplink port is used to connect network devices in the upper layer and access the core network. The downlink port is used to connect the endpoints. ● When port isolation is enabled, the downlink ports of the device are isolated from each another, and they can only communicate with the uplink ports. For details, see 3.4 Port Isolation.

3.1.2 Port Information 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 Setting and Viewing Basic Port Attributes.
- Click **VLAN** to configure the VLANs on ports. For details, see 4.2 VLAN Settings.

Note

VLANs on ports can only be configured and viewed in the **Port Info** area after **VLAN Settings** is toggled on.

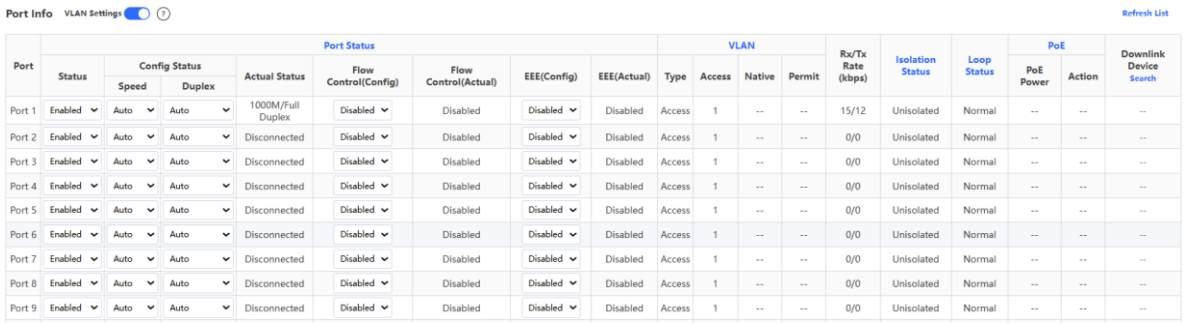
- Click **Isolation Status** to configure port isolation so that the downlink ports of the device are isolated from each other. For details, see 3.4 Port Isolation.
- Click **Loop Status** to enable the loop prevention feature. After a loop occurs, the port causing the loop will be shut down automatically. For details, see 5.3 Loop Prevention.
- Click **PoE** to view and set PoE parameters of a port. For details, see 6 PoE Settings.

Note

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

- Click **Search** in the **Downlink Device** column to search for the downlink devices of ports. After the search is done, click **View** to view the MAC addresses of the downlink devices.
- Click **Refresh List** to obtain the latest port information.

Figure 3-2 Viewing Port Information or Configuring Ports



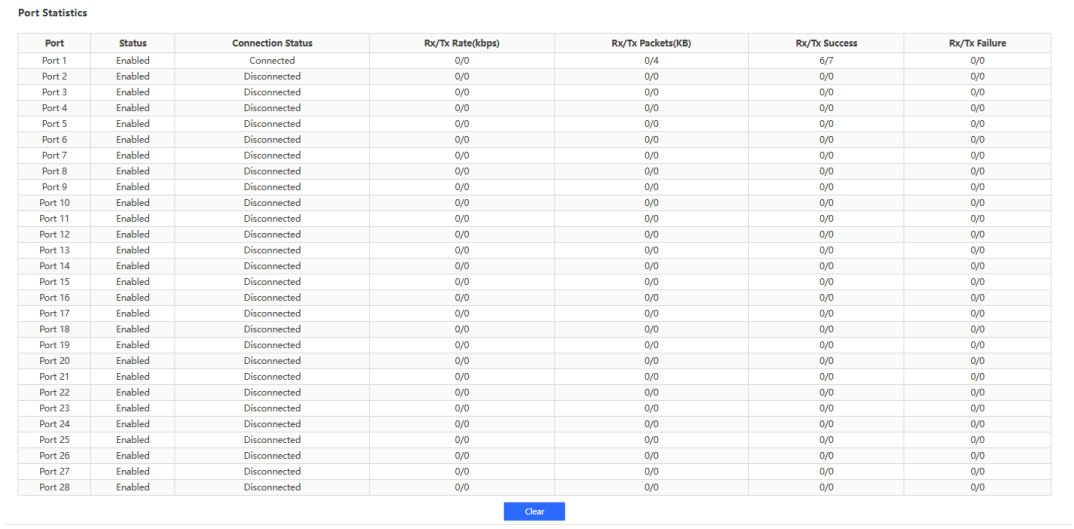
3.1.3 Port Packet Statistics

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 collection on all ports and reset the statistics.

Figure 3-3 Port Packet Statistics



3.2 Setting and Viewing Basic Port Attributes

3.2.1 Port Settings

Note

The EEE feature can be configured on RJ45 ports that operate at 100 or 1000 Mbps with auto-negotiation enabled (rate and duplex mode set to auto).

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

Procedure

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**.

Figure 3-4 Port Parameter Configuration

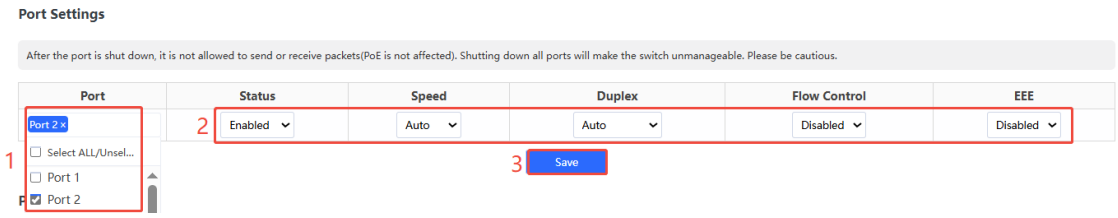


Table 3-2 Basic Port Configuration Parameters

Parameter	Description	Default
Port	Select the ports you want to configure.	No default value
Status	● **Enabled**: When the port is enabled, it can receive or transmit packets. ● **Disabled**: When the port is disabled, it cannot receive or transmit packets (PoE is not affected).	Enabled
Speed	Configure the operating speed of the Ethernet 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 rate can be any rate within the port capability	Auto
Duplex	● **Full Duplex**: The port can receive packets while sending packets. ● **Half Duplex**: The port can receive or send packets at a time. ● **Auto**: The duplex mode of a port is determined through auto-negotiation between the local port and its peer port.	Auto
Flow Control	After flow control is enabled, the port will process the received flow control frames and send them when flow congestion occurs.	Disabled
EEE	It is short for energy-efficient Ethernet, which is based on the standard IEEE 802.3az protocol. When EEE is enabled, the Ethernet port enters the Lower Power Idle (LPI) mode to save energy when the port is idle.	Disabled

Caution

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

3.2.2 Port Status

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

You can view the configuration status of the port attributes and check whether these configurations are active, including the port rate, duplex mode, flow control, and EEE status.

Figure 3-5 Port Status

Port List

Port	Status	Speed/Duplex		Flow Control		EEE	
		Config Status	Actual Status	Config Status	Actual Status	Config Status	Actual Status
Port 1	Enabled	Auto/Auto	1000M/Full Duplex	Disabled	Disabled	Disabled	Disabled
Port 2	Enabled	Auto/Auto	Disconnected	Disabled	Disabled	Disabled	Disabled
Port 3	Enabled	Auto/Auto	Disconnected	Disabled	Disabled	Disabled	Disabled
Port 4	Enabled	Auto/Auto	Disconnected	Disabled	Disabled	Disabled	Disabled
Port 5	Enabled	Auto/Auto	Disconnected	Disabled	Disabled	Disabled	Disabled
Port 6	Enabled	Auto/Auto	Disconnected	Disabled	Disabled	Disabled	Disabled
Port 7	Enabled	Auto/Auto	Disconnected	Disabled	Disabled	Disabled	Disabled
Port 8	Enabled	Auto/Auto	Disconnected	Disabled	Disabled	Disabled	Disabled
Port 9	Enabled	Auto/Auto	Disconnected	Disabled	Disabled	Disabled	Disabled
Port 10	Enabled	Auto/Auto	Disconnected	Disabled	Disabled	Disabled	Disabled
Port 11	Enabled	Auto/Auto	Disconnected	Disabled	Disabled	Disabled	Disabled
Port 12	Enabled	Auto/Auto	Disconnected	Disabled	Disabled	Disabled	Disabled
Port 13	Enabled	Auto/Auto	Disconnected	Disabled	Disabled	Disabled	Disabled
Port 14	Enabled	Auto/Auto	Disconnected	Disabled	Disabled	Disabled	Disabled

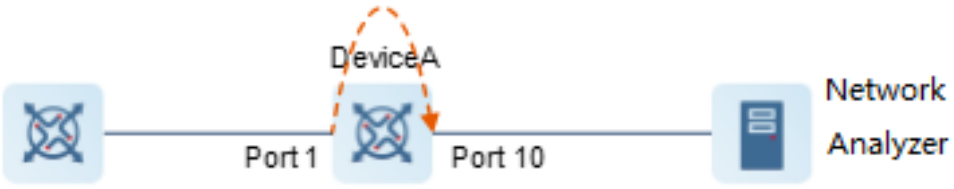
3.3 Port Mirroring

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 a network analyzer without affecting the normal data forwarding of the monitored device.

As shown in Figure 3-6, by configuring port mirroring on Device A, the packets on Port 1 are mirrored to Port 10. Though the network analyzer is not directly connected to Port 1, it can receive all packets on Port 1 and is able to monitor the data traffic on Port 1.

Figure 3-6 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**. If you want to delete the port mirroring configuration, click **Delete**.

Caution

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

Figure 3-7 Configuring Port Mirroring

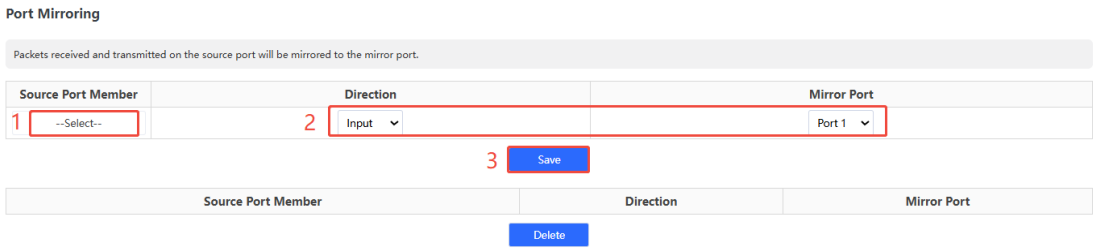


Table 3-3 Port Mirroring Parameters

Parameter	Description
Source Port Member	● The source port is also called the monitored port. Packets on the source port will be mirrored to the mirror port for network analysis or troubleshooting. ● You can select multiple source ports. Packets on these ports will be mirrored to one mirror port.
Direction	Directions of the data traffic monitored on the source port: ● Bi-directions (input & output): All packets on the source port, including the received packets and the transmitted packets, will be mirrored to the mirror port. ● Input: The packets received by the source port will be mirrored to the mirror port. ● Output: The packets transmitted from the sourced port will be mirrored to the mirror port.
Mirror Port	The mirror port is also called the monitoring port. The mirror port is connected with a monitoring device, and 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. After port isolation is enabled, downlink ports are isolated from each other and cannot forward data. Meanwhile, uplink ports are not isolated, and data can be forwarded only between uplink and downlink ports of the device.

Port isolation is disabled by default. Toggle on **Status** to enable port isolation.

Figure 3-8 Port Isolation



Note

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

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, select the rate limiting type and status, enter the rate limit, and click **Save**. The configuration will be displayed accordingly in the port rate table right below the **Save** button.

Figure 3-9 Port-based Rate Limiting

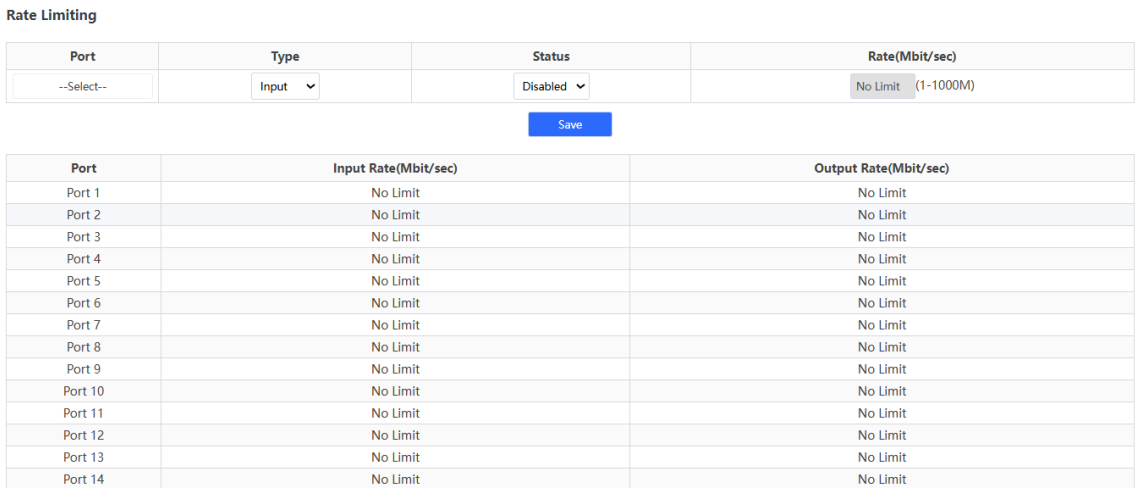


Table 3-4 Port-based Rate Limiting Parameters

Parameter	Description	Default
Port	You can select multiple ports for rate limiting configuration in batches.	No default value
Type	Direction of the rate-limited data traffic: ● All: Rate limiting all packets passing through the port, including received and sent packets. ● Input: Rate limiting packets received by the port.	No default value

Parameter	Description	Default
	● Output: Rate limiting packets transmitted from the port.	
Status	Whether to enable rate limiting on a port.	Disabled
Rate (Mbit/sec)	Indicates the maximum rate at which packets are forwarded over the port.	No Limit

Note

The port-based rate limiting range varies with the switch model.

3.6 Management IP Address

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

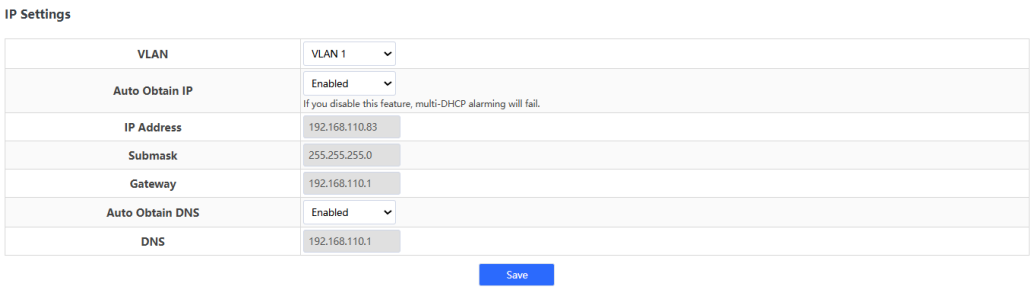
You can configure the management IP address of the device. By accessing the management IP address, you can configure and manage the device.

- Two modes of obtaining IP addresses:
  - Dynamic IP address: Enable the **Auto Obtain IP** feature to use the IP address assigned dynamically by the uplink DHCP server.

    If the **Auto Obtain IP** feature is enabled, 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 the **Auto Obtain DNS** feature is disabled, you need to configure a DNS address manually.
  - Static IP address: Disable the **Auto Obtain IP** feature to use the fixed IP address configured manually by the user.

    After disabling the **Auto Obtain IP** feature, you need to manually configure the IP address, subnet mask, gateway IP address, and DNS address. Click **Save**.
- VLAN is used for managing VLAN tag of the management packets. If the VLAN settings is disabled, the management packets will be untagged, and management VLAN configuration is not supported. The management VLAN of the device is VLAN 1 by default.

Figure 3-10 IP Settings



Note

- If the VLAN settings are disabled, 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 VLAN Settings.
- You are advised to bind a configured management VLAN to an uplink port. Otherwise, you may fail to access eWeb. For details, see 4.2.3 Port VLAN Settings.
- If you disable the **Auto Obtain IP** feature, multi-DHCP alarming will fail. For details about multi-DHCP alarming, see 9.2 Multi-DHCP Alarming.

4 Switch Management

4.1 Managing MAC Addresses

4.1.1 Overview

A 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.

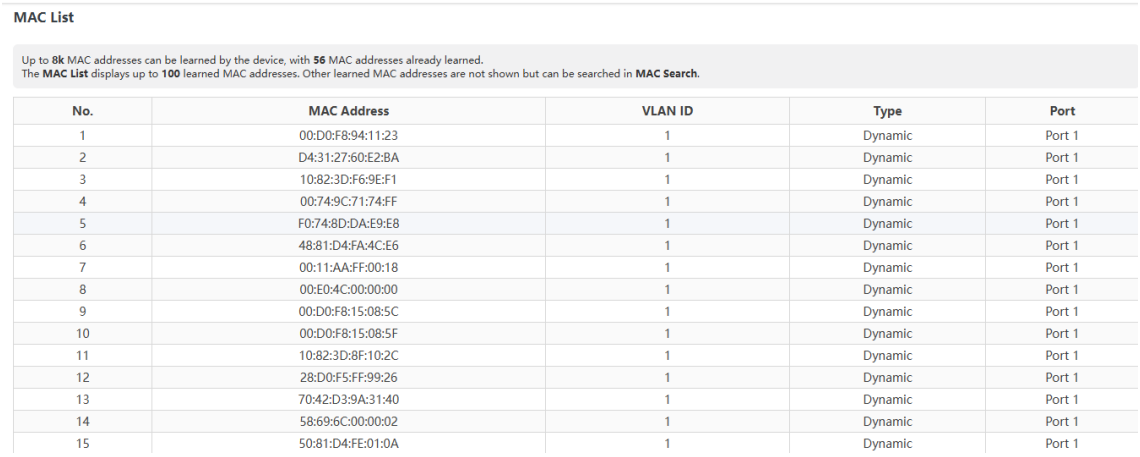
4.1.2 Viewing the MAC Address Table

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

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

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

Figure 4-1 MAC Address Table



No.	MAC Address	VLAN ID	Type	Port
1	00:D0:F8:94:11:23	1	Dynamic	Port 1
2	D4:31:27:60:E2:BA	1	Dynamic	Port 1
3	10:82:3D:F6:9E:F1	1	Dynamic	Port 1
4	00:74:9C:71:74:FF	1	Dynamic	Port 1
5	F0:74:8D:DA:E9:E8	1	Dynamic	Port 1
6	48:81:D4:FA:4C:E6	1	Dynamic	Port 1
7	00:11:AA:FF:00:18	1	Dynamic	Port 1
8	00:E0:4C:00:00:00	1	Dynamic	Port 1
9	00:D0:F8:15:08:5C	1	Dynamic	Port 1
10	00:D0:F8:15:08:5F	1	Dynamic	Port 1
11	10:82:3D:8F:10:2C	1	Dynamic	Port 1
12	28:D0:F5:FF:99:26	1	Dynamic	Port 1
13	70:42:D3:9A:31:40	1	Dynamic	Port 1
14	58:69:6C:00:00:02	1	Dynamic	Port 1
15	50:81:D4:FE:01:0A	1	Dynamic	Port 1

Note

- If you disable VLAN, the device will forward packets only according to the destination MAC addresses. The **VLAN ID** column is not displayed in the MAC address table.
- A maximum of 100 MAC address entries can be displayed.

4.1.3 Searching for MAC Addresses

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

You can search for MAC address entries by MAC address and VLAN ID.

Caution

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

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

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

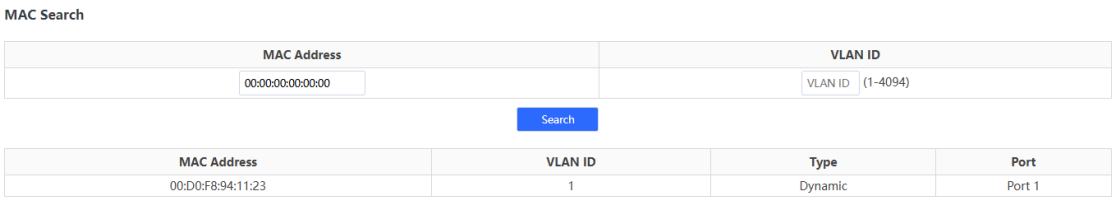
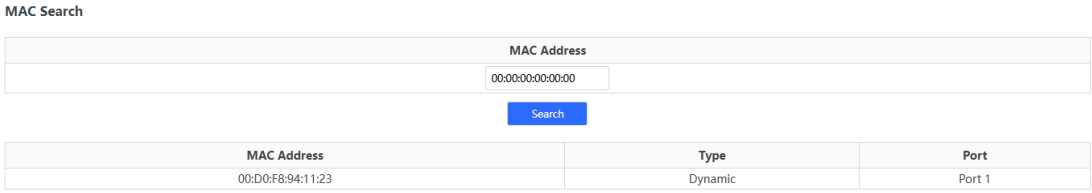


Figure 4-3 Searching for MAC Addresses (with VLAN Disabled)



4.1.4 Configuring Static MAC Addresses

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

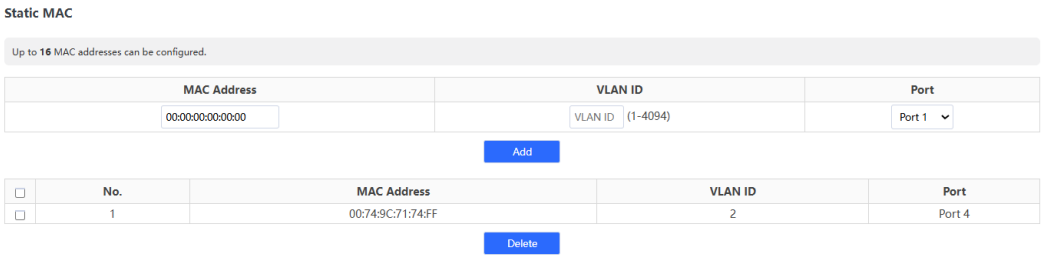
By configuring a static MAC address, you can manually bind the MAC address of another device with a port of the switch. After you add a static MAC address, when the device receives a packet destined to this address from the VLAN, it forwards the packet to the specified port.

Caution

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

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

Figure 4-4 Configuring Static MAC Addresses



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

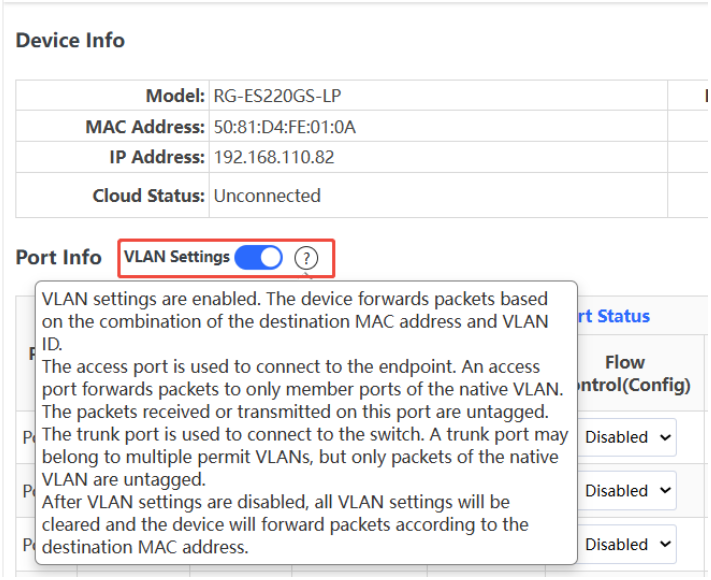
Choose **Home** from the navigation page.

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 unmanaged switch. The device forwards packets according to the destination MAC addresses, and the VLAN information of the forwarding packets remains unchanged during the forwarding process.
- When VLAN is enabled, the device operates like a managed switch. The device forwards packets according

to the destination MAC address and VLAN ID. You can configure the port mode (access or trunk) based on whether a VLAN tag is carried in packets. Besides, all device ports will be initialized to access ports.

Figure 4-5 VLAN Settings



4.2.2 Static VLAN Settings

Caution

Static VLANs can be created only when the global VLAN settings feature is enabled.

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

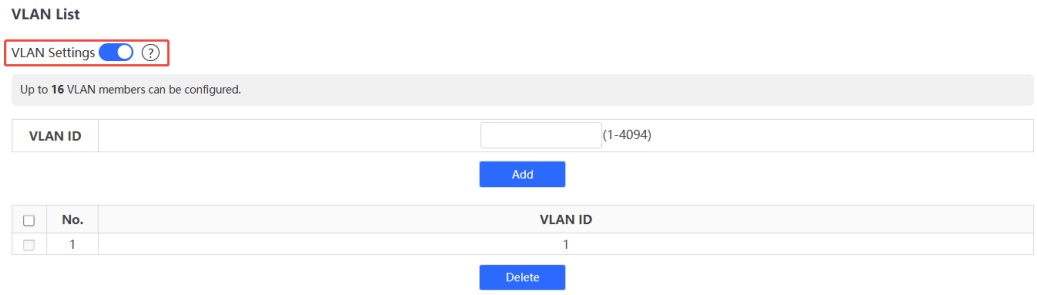
Enter a VLAN ID and click **Add** to create a static VLAN.

Note

- The VLAN ID ranges from 1 to 4094. VLAN 1 is the default VLAN.
- A maximum of 16 static VLANs can be created.
- The default VLAN (VLAN 1), management VLAN, Native VLAN, Permit VLAN, and Access VLAN cannot be deleted.
- On the **VLAN List** page, VLAN settings are the same as those on the **Home** page. The settings are globally applied and the latest configuration takes effect.

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

Figure 4-6 Static VLAN Configuration



4.2.3 Port VLAN Settings

Caution

- You can configure VLANs on ports only when **VLAN Settings** is toggled on.
- 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**.

Through configuring the port mode and VLAN members of a port, you can allow packets tagged with the VLAN IDs to pass through on the port and whether the packets forwarded by the port carry tags.

Procedure

(1) Select one or more ports on which you want to configure the VLANs.

(2) Configure the VLAN type for the ports.

- Access: If the port is an access port, set **Access VLAN** for it.
- Trunk: If the port is a trunk port, set **Native VLAN** for it, and enter the range of permitted VLAN IDs.

(3) Click **Save**.

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

Note

- You are advised to create VLAN members (refer to 4.2.2 Static VLAN Settings) before configuring the port based on VLANs. Click **VLAN List** to access the **VLAN List** page where you can add VLAN members.
- 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.

Figure 4-7 Configuring VLANs on a Port

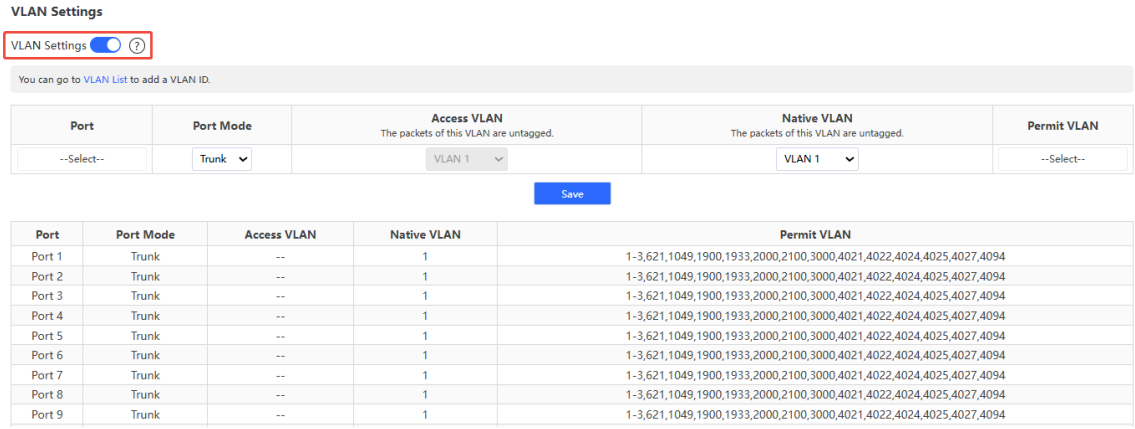


Table 4-1 Port Modes

Port Mode	Description
Access	● One access port can belong to only one VLAN and allow only frames from this VLAN to pass through. This VLAN is called an access VLAN. ● The frames from the access port do not carry VLAN tag. When the access port receives an untagged frame from a peer device, the local device determines that the frame comes from the access VLAN and adds the access VLAN ID to the frame. ● Access port is connected to the clients.
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. A trunk port is connected to switches. ● You can set the Permit VLAN range to limit VLAN frames that can be forwarded. (Note: Make sure the trunk ports at the two ends of a link are configured with the same Native VLAN.)

5 Security Management

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 Procedure

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

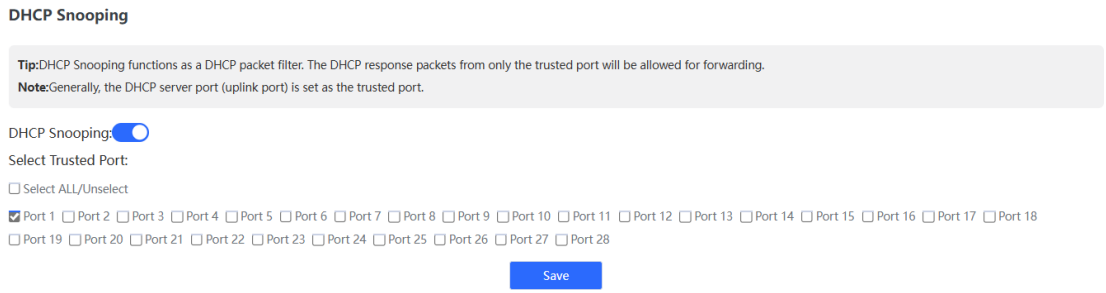
Toggle on **DHCP Snooping**, select the trusted ports, and then click **Save**.

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 typically configured as the trusted port.

Figure 5-1 DHCP Snooping Configuration



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, 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 Procedure

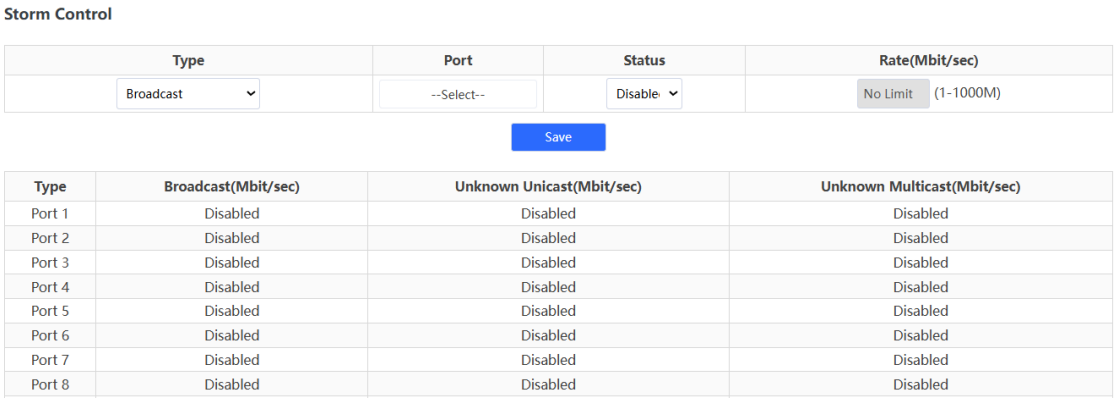
Choose **QoS** > **Storm Control**.

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

The storm control type and corresponding rate are displayed in Figure 5-2.

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

Figure 5-2 Storm Control



Note

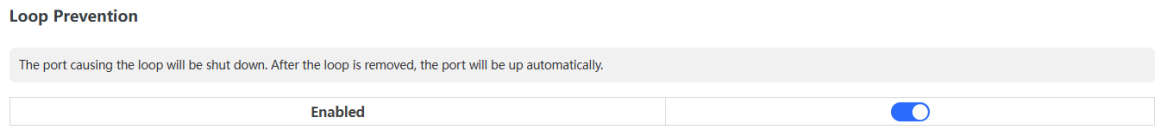
The value range of storm control varies depending on devices.

5.3 Loop Prevention

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

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

Figure 5-3 Loop Prevention



6 PoE Settings

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

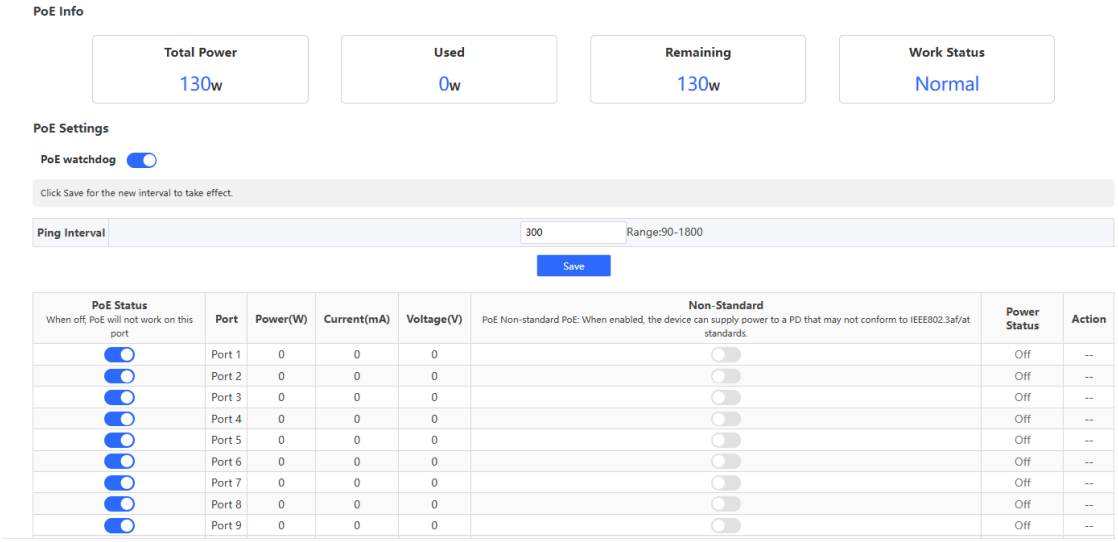
If a non-PD, such as a PC, is connected to a PoE port of this device, the PoE watchdog will not initiate any action on the non-PD even if the trigger condition is met.

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 6-2 PoE Information and Configuration



7 Toolkit

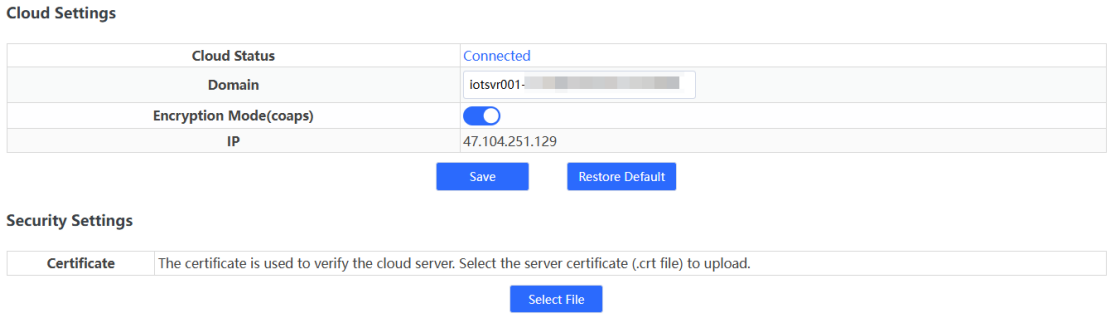
7.1 Cloud Settings

7.1.1 Checking the Cloud Information

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

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

Figure 7-1 Cloud Settings



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

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

Table 7-1 Cloud Settings Parameters

Parameter	Description
Cloud Status	Indicates the connectivity status of the device on the cloud, including **Connected**, **Unconnected**, **Connectable**, and **Certificate verification failure**.
Reason	Indicates the reason for device connection failure. The reasons for connection failure in different cloud status are as follows: ● Connected: No reason is displayed. ● Unconnected: o The network connection is down or a DNS resolution error has occurred. o This device failed to connect to Ruijie Cloud. ● Connectable: This device is not registered to Ruijie Cloud.

Parameter	Description
	● Certificate verification failure: This device failed to connect to Ruijie Cloud.
Domain	Indicates the domain name of the cloud server. **Caution** ● The coap:// prefix is not required in the domain name field as it is added by default. ● After the domain name is changed, the page is refreshed after 5 seconds by default.
Encryption Mode(coaps)	Indicate whether the encryption mode (CoAPs) is enabled on the current device. If it is enabled, **Security Settings** will be displayed below. For details, see 7.1.2 7.1.2 Introduction to CoAP.
IP	Indicates the IP address of the cloud server resolved from the cloud address.

7.1.2 Introduction to CoAP

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

7.1.3 Configuring CoAPs-based Encryption

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

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

Note

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

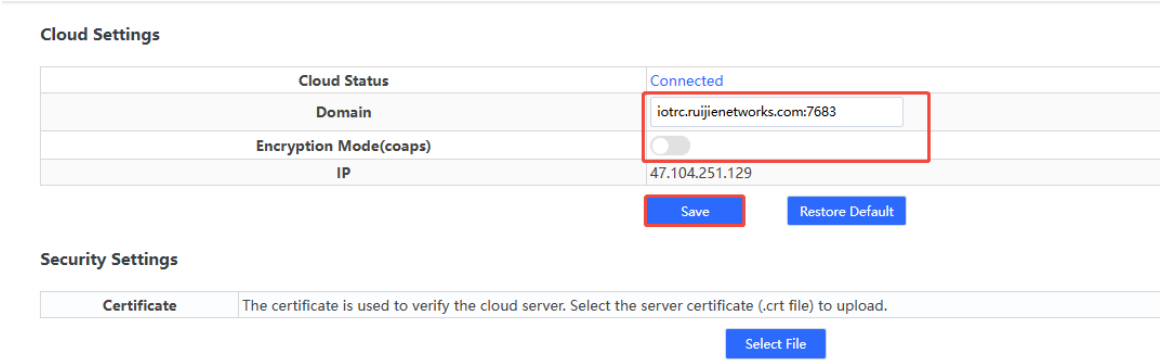
The configuration procedure in the two scenarios is described as follows.

1. Public Cloud

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

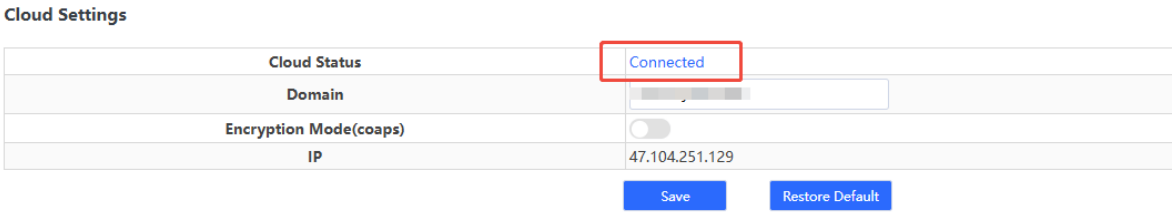
- Disable **Encryption Mode(coaps)**.
  a Toggle off **Encryption Mode(coaps)**.
  b Change the domain name to iotrc.ruijienetworks.com:7683 and click **Save**.

Figure 7-2 Disabling the Encryption Mode



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

Figure 7-3 Succeeded in Disabling the Encryption Mode

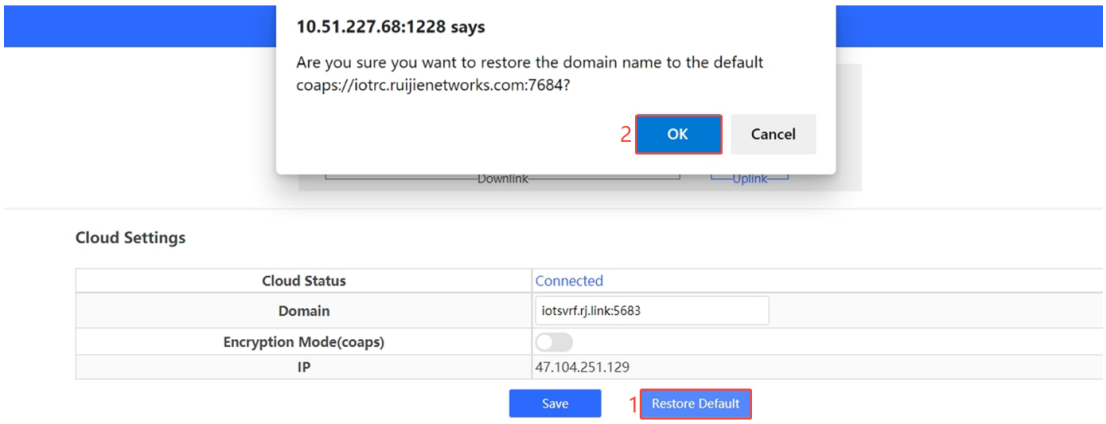


- Enable **Encryption Mode(coaps)** again.

  a Click **Restore Default**. A prompt is displayed.

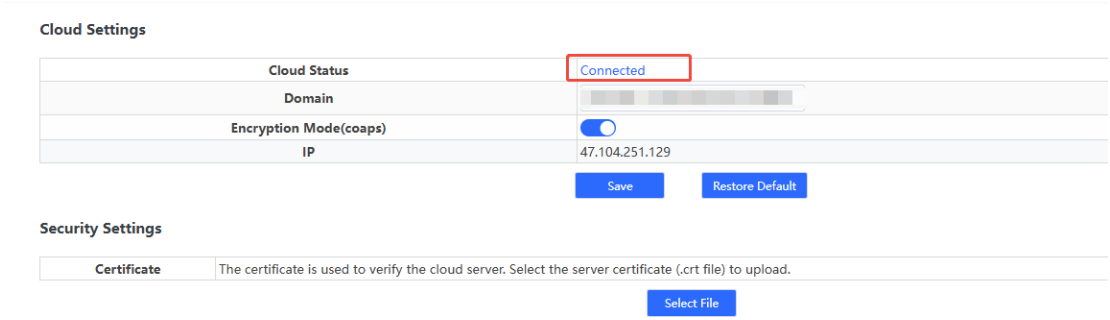
  b After confirming the prompt information, click **OK**.

Figure 7-4 Enabling the Encryption Mode



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

Figure 7-5 Succeeded in Enabling the Encryption Mode



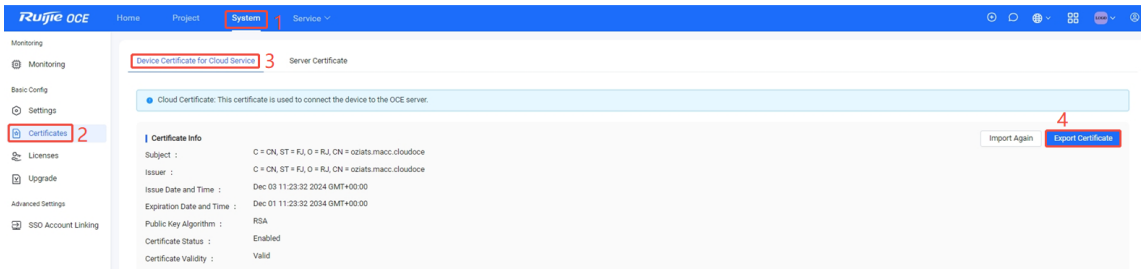
2. Private Cloud of RG-OCE Network Manager

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

(1) Obtain the certificate.

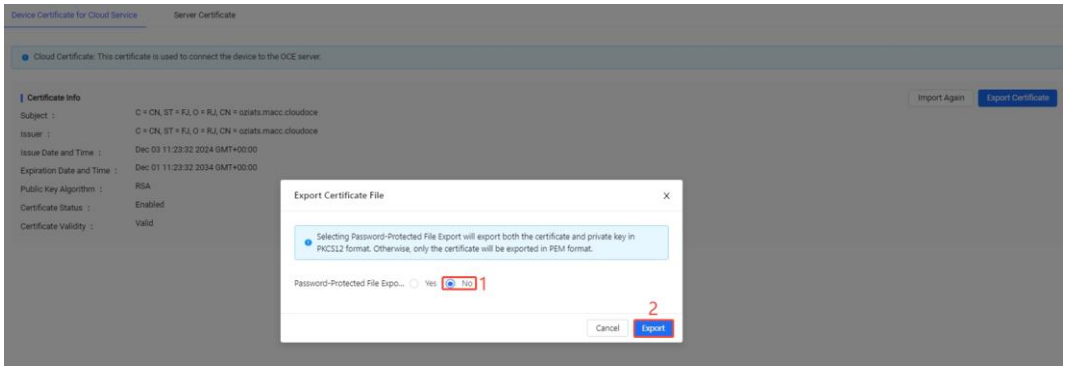
a Log in to the private cloud server of RG-OCE Network Manager, choose **System** > **Certificates** > **Device Certificate for Cloud Service**, and click **Export Certificate**.

Figure 7-6 Downloading the Private Cloud Certificate (1/2)



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

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



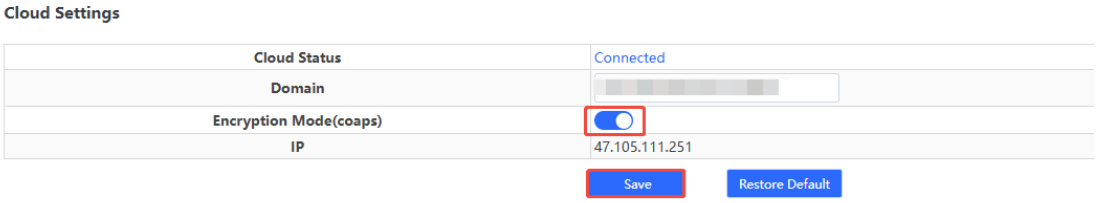
(2) Configure the domain name and port number.

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

Note

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

Figure 7-8 Toggling on the Encryption Mode

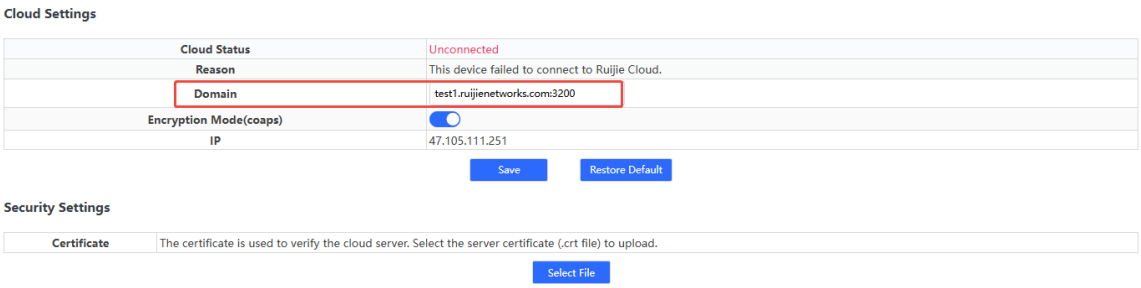


b Confirm that the domain name of a private cloud server is used and the port number is changed to the management port number for CoAPs services. Click **Save**.

Note

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

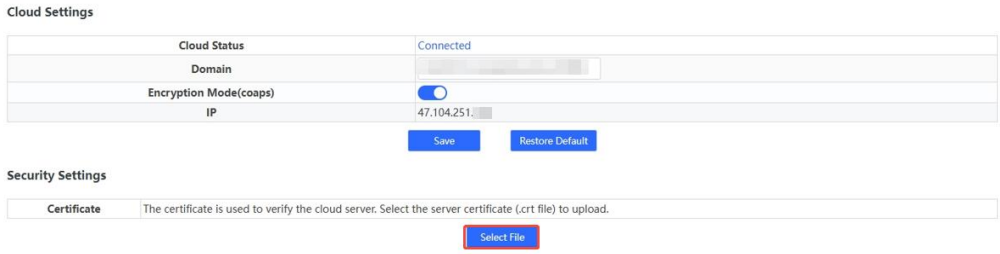
Figure 7-9 Configuring the Domain Name and Port Number for a Private Cloud Server



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

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

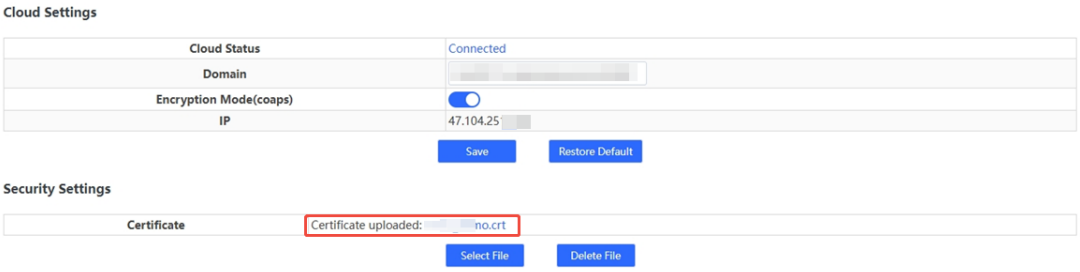
Figure 7-10 Uploading the Certificate of a Private Cloud Server



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

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

Figure 7-11 Succeeded in Uploading the Certificate



Caution

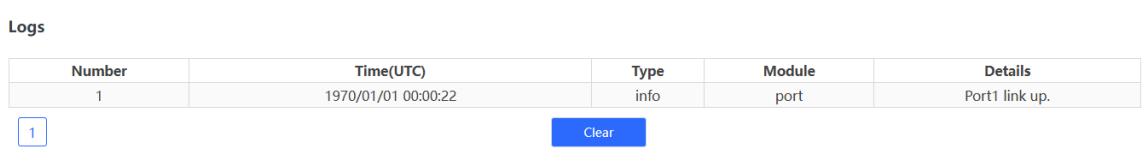
If you want to disable the encryption mode, change the port number to the management port number of the CoAP services, toggle off **Encrypted Mode(coaps)**, and click **Save**.

7.2 System Logs

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

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

Figure 7-12 System Logs



Caution

If the issue persists despite following the troubleshooting methods provided in this section, you may require remote support from a technician who will enable developer mode to resolve the issue.

8 System Settings

8.1 Managing Device Information

8.1.1 Viewing Device Information

Choose **Home** from the navigation page.

The **Device Info** area 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 choose **Monitoring** > **Device Info** to view more information about the device.

Figure 8-1 Basic Device Information

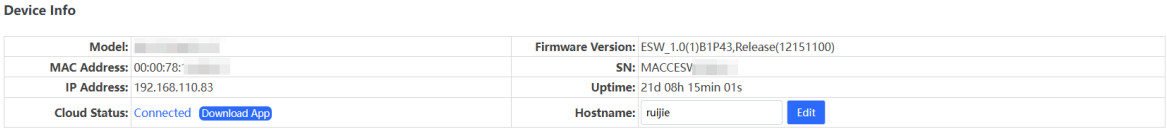
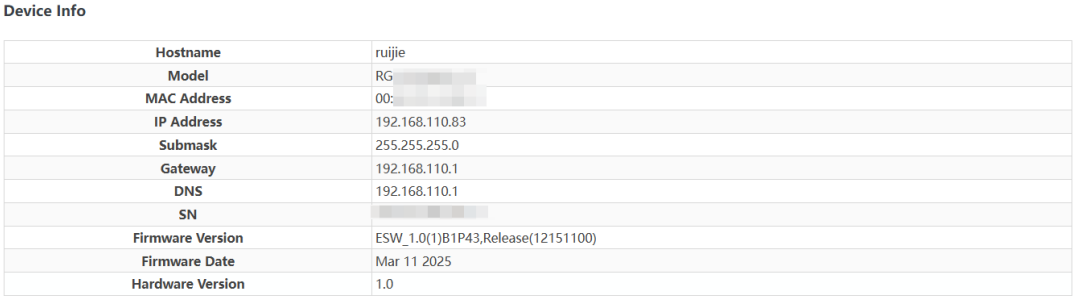


Figure 8-2 More Device Information

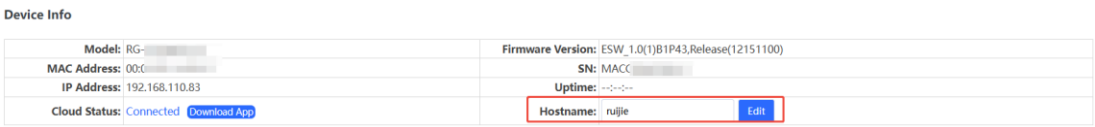


8.1.2 Editing the Hostname

Choose **Home** from the navigation page.

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

Figure 8-3 Editing the Hostname

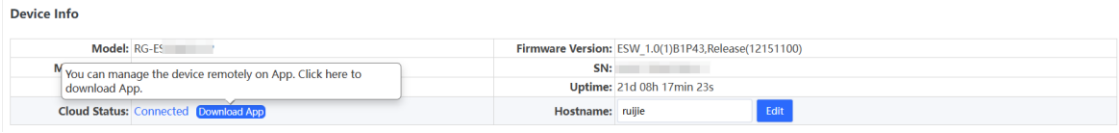


8.1.3 Cloud Management

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, **Cloud Status** changes to **Connected**, and you can manage the device remotely through Ruijie Cloud or Ruijie Reyee App. Click **Connected** to access the homepage of Ruijie Cloud (https://cloud-as.ruijienetworks.com). Click **Download App** to download Ruijie Reyee App.

Figure 8-4 Cloud Status

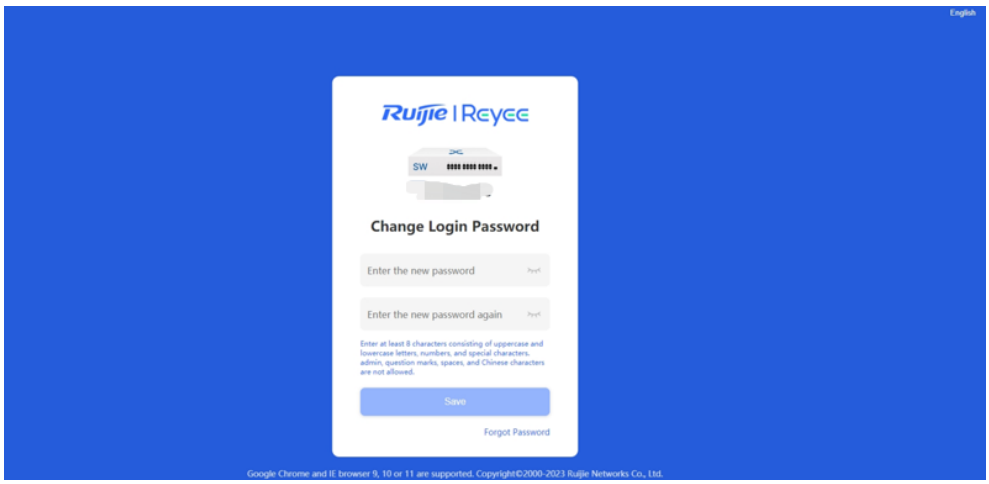


8.2 Login Password Settings

- 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.

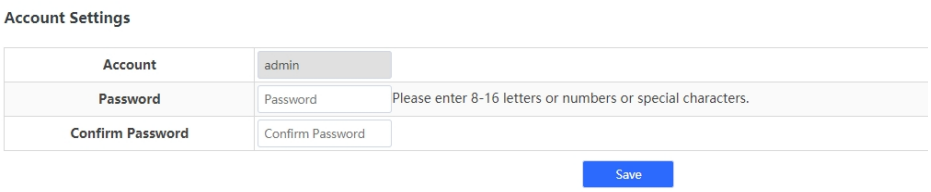
Figure 8-5 Setting the Login Password on the Login Page



- Change the login password after login.

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

Figure 8-6 Setting the Login Password



Caution

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

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

Figure 8-7 Network-Management Mode

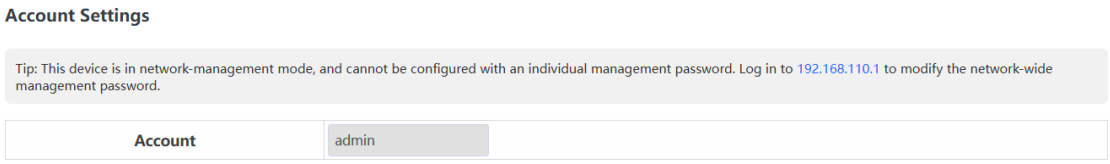
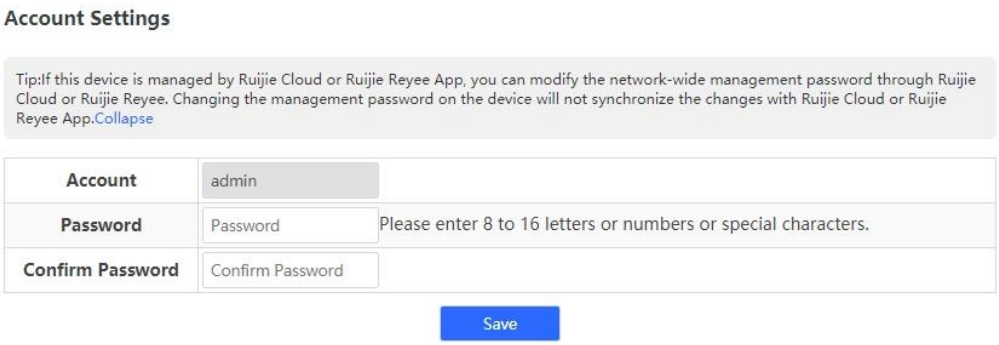


Figure 8-8 Management Through Ruijie Cloud or Ruijie Reyee App

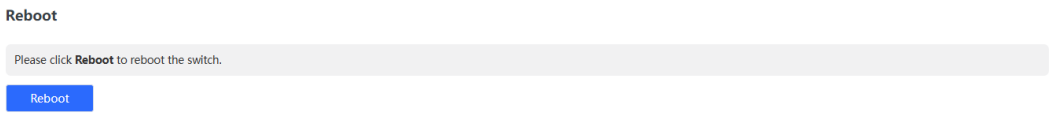


8.3 Device Reboot

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

Click **Reboot** to reboot the switch.

Figure 8-9 Device Reboot



8.4 System Upgrade

8.4.1 Local Upgrade

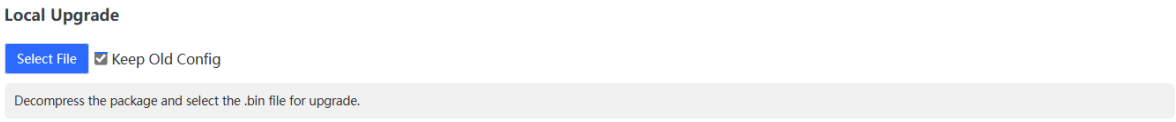
Choose **System** > **Upgrade**.

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

Note

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 8-10 Local Upgrade



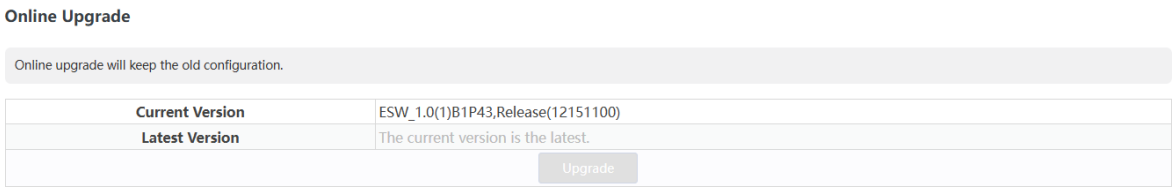
8.4.2 Online Upgrade

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

When there is a new version on Ruijie Cloud, the version number of the latest version will be displayed on this page, and the **Upgrade** button will become available.

Click **Upgrade** and confirm the upgrade. The device will download the installation package of the recommended version from Ruijie Cloud and it will be updated to the latest version. Online upgrade will keep the old configuration by default.

Figure 8-11 Online Upgrade



Note

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

8.5 Restoring Factory Configuration

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

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

Figure 8-12 Restoring Factory Configuration



9 Monitoring Management

9.1 Cable Test

Note

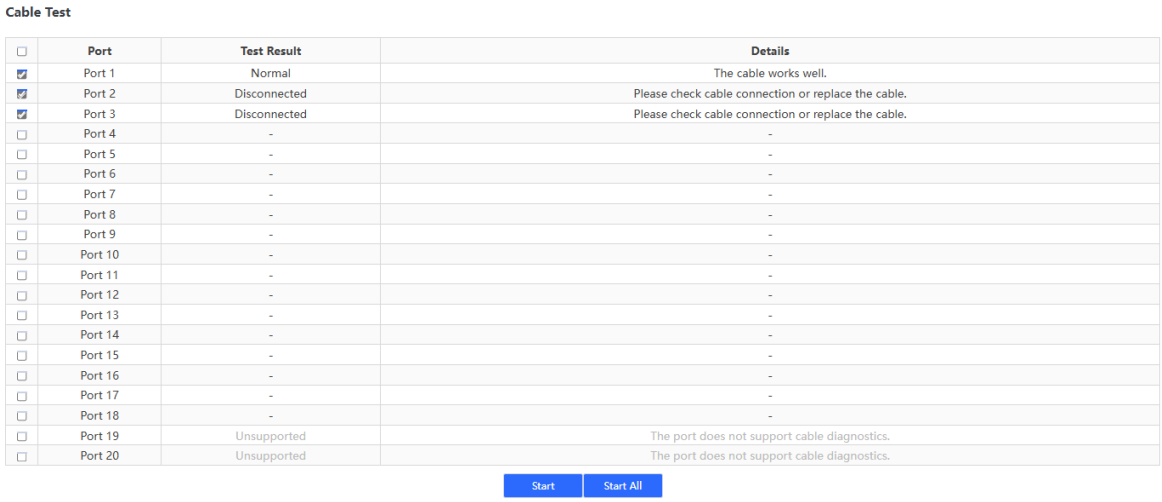
This feature is not supported on an optical port.

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

A 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 test, and then click **Start** to start a cable test. The test result will be displayed accordingly. Click **Start All** to perform a one-click cable test on all ports.

Figure 9-1 Cable Test



Caution

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

9.2 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 on the right of **Device Info**.

Figure 9-2 Multi-DHCP Alarming



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

9.3 Viewing Switches on the Network

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

- Primary device for global management

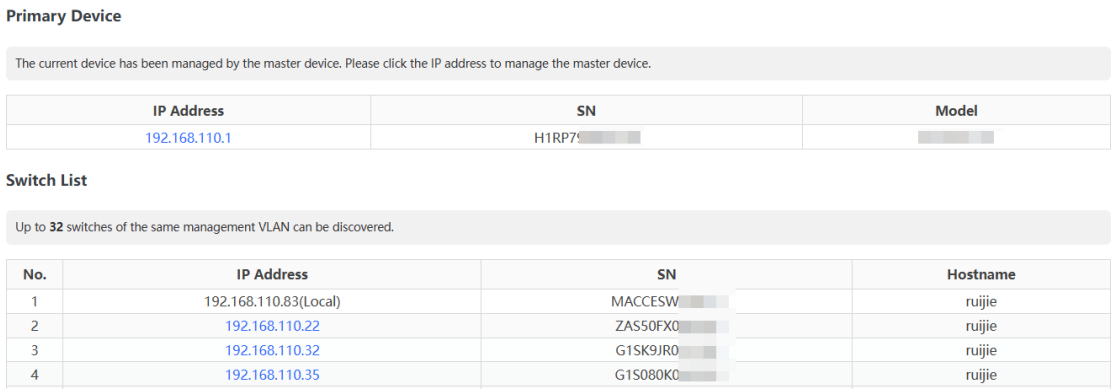
  If the switch is under uniform management, some features cannot be configured independently (such as password settings). To facilitate configuration, information of the primary device in the VLAN will be displayed on this page. Click the IP address of the primary device to access the **Primary Device** 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 9-3 Viewing Switches on the Network



10 FAQs

10.1 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.

10.2 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.