

Ruijie Reyee RG-NIS2100 Series Switches 1.0(1)B1P31

Configuration Guide



Copyright

Copyright © 2024 Ruijie Networks

All rights are reserved in this document and this statement.

Any reproduction, excerpt, backup, modification, transmission, translation or commercial use of this document or any portion of this document, in any form or by any means, without the prior written consent of Ruijie Networks is prohibited.

Trademarks including  are owned by Ruijie Networks.

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

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

- The official website of Ruijie Reyee: <https://reyee.ruijie.com>
- Technical Support Website: <https://reyee.ruijie.com/en-global/support>
- Case Portal: <https://www.ruijienetworks.com/support/caseportal>
- Community: <https://community.ruijienetworks.com>
- Technical Support Email: service_rj@ruijienetworks.com
- Online Robot/Live Chat: <https://reyee.ruijie.com/en-global/rita>

Conventions

1. GUI Symbols

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

2. Signs

The signs used in this document are described as follows:

Warning

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

Caution

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

Note

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

 **Specification**

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

3. Note

The manual offers configuration information (including model, description, port type, software interface) for indicative purpose only. In case of any discrepancy or inconsistency between the manual and the actual version, the actual version prevails.

Contents

Preface	I
1 Login.....	1
1.1 Configuration Environment Requirements	1
1.2 Login to the Web Management System	1
1.2.1 Connecting the Device.....	1
1.2.2 Login to the Web Management System	1
2 Port Settings.....	2
2.1 Managing Port Information	2
2.1.1 Port Status Bar.....	2
2.1.2 Port Info Overview	4
2.1.3 Port Packet Statistics	5
2.2 Setting and Viewing Port Attributes	5
2.2.1 Port Settings.....	5
2.2.2 Port Status	7
2.3 Port Mirroring	7
2.3.1 Overview	7
2.3.2 Configuration Steps	7
2.4 Port Isolation	8
2.5 Port-based Rate Limiting	9
2.6 Management IP Address	10
3 Switch Settings.....	11
3.1 Managing MAC Address.....	11
3.1.1 Overview	11

3.1.2 Viewing MAC Address Table.....	12
3.1.3 Searching for MAC Address	12
3.1.4 Configuring Static MAC Address	13
3.2 VLAN Settings.....	14
3.2.1 Global VLAN Settings	14
3.2.2 Static VLANs Settings.....	14
3.2.3 Port VLAN Settings	15
4 Security.....	17
4.1 DHCP Snooping.....	17
4.1.1 Overview	17
4.1.2 Configuration Steps	17
4.2 Storm Control.....	17
4.2.1 Overview	17
4.2.2 Configuration Steps	18
4.3 Loop Guard.....	18
5 PoE Settings.....	19
6 ERPS.....	20
6.1 Overview	20
6.2 Control VLAN and Data VLAN.....	20
6.3 Basic Model of an Ethernet Ring.....	21
6.3.1 Major Ring and Subring	21
6.3.2 Basic Topologies	21
6.3.3 Node.....	22
6.3.4 Ring Member Port.....	22

6.4 RPL and Nodes.....	23
6.5 ERPS Packet	24
6.6 ERPS Timer	24
6.7 Ring Protection	25
6.8 Protocols and Standards	25
6.9 Configuring ERPS.....	25
6.10 ERPS Typical Configuration Examples	28
6.10.1 Requirements.....	28
6.10.2 Topology.....	28
6.10.3 Notes.....	28
6.10.4 Procedure.....	28
7 Diagnostics.....	33
7.1 Cloud Settings.....	33
7.2 System Logs	34
8 System Settings	35
8.1 Managing Device Information.....	35
8.1.1 Viewing Device Information	35
8.1.2 Editing the Hostname.....	36
8.1.3 Cloud Management.....	36
8.2 Setting the Maximum Power of the Power Supply	36
8.3 Password Settings	37
8.4 Device Reboot	38
8.5 System Upgrade	38
8.5.1 Local Upgrade.....	38

8.5.2 Online Upgrade.....	38
8.6 Restoring Factory Configuration.....	39
9 Monitoring.....	39
9.1 Cable Diagnostics.....	39
9.2 Multi-DHCP Alarming.....	40
9.3 Viewing Switch Information.....	40
10 FAQs.....	42

1 Login

1.1 Configuration Environment Requirements

- Browser: Google Chrome, Internet Explorer 9.0, 10.0, and 11.0, and some Chromium/IE kernel-based browsers are supported. Exceptions such as messy code and format errors may occur when other browsers are used.
- Resolution: 1024 x 768 or a higher resolution is recommended. Exceptions such as font alignment error and format error may occur when other resolutions are used.

1.2 Login to the Web Management System

1.2.1 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 1-1 Default Configuration

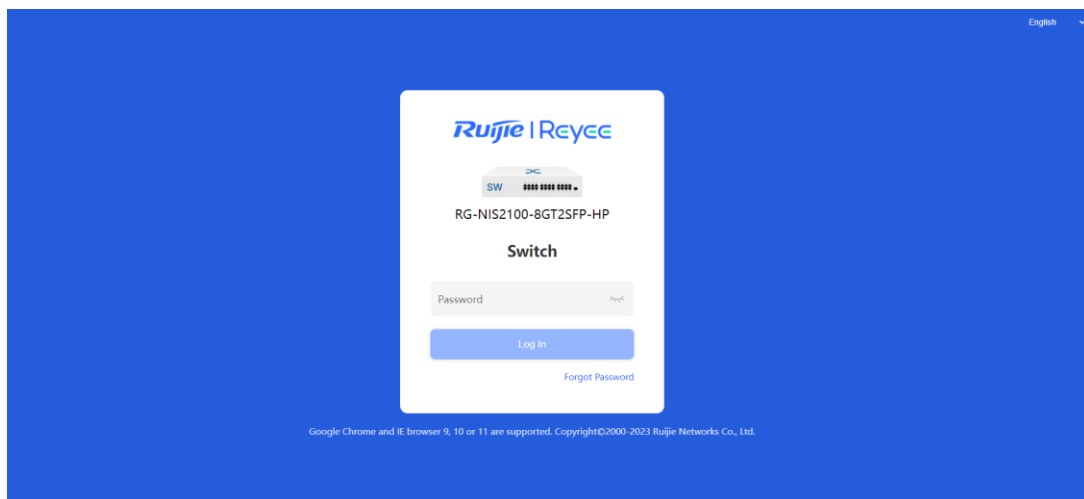
Feature	Default Setting
Device IP Address	10.44.77.200
Password	admin

1.2.2 Login to the Web Management System

- (1) Enter the IP address (10.44.77.200 by default) of the device into 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 web interface of the device as long as the PC and the device are in the same network segment of a LAN.

Figure 1-1 Login Page

(2) Enter the password (default password: admin), and then click **Log In** to enter the homepage of the web interface.

You will be prompted to reset the default password upon their first login to the web interface. If the password is the default password, you are not allowed to configure the device. You need to log in to the web interface with the reset password to configure and manage the device. For details about password settings, see [8.3](#).

If you forget the device IP address or password, press and hold the **Reset** button on the device panel for more than 5 seconds to restore factory settings. After restoration, you can use the default IP address and password to log in.

⚠ Caution

Restoring factory settings will delete the current configurations. Exercise caution when performing this operation.

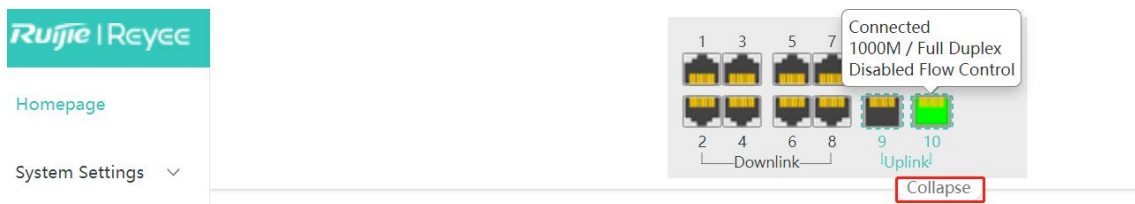
2 Port Settings

2.1 Managing Port Information

2.1.1 Port Status Bar

The port status bar is at the top of the web page, showing port ID, port attribute (uplink/downlink), and the connection status. Click **Collapse** to hide the port status bar.

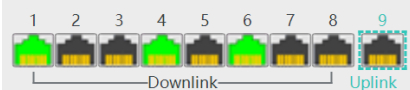
Figure 2-1 Port Status Bar



Different colors and shapes of the port icons represent different port statuses. See Table 2-1 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 2-1 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.
	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.

Port Icon	Description
	<p>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.</p> <p>When port isolation is enabled, the downlink ports of the device are isolated from each other, and they can only communicate with the uplink ports. For details, see 2.4</p>

2.1.2 Port Info Overview

Choose **Homepage**.

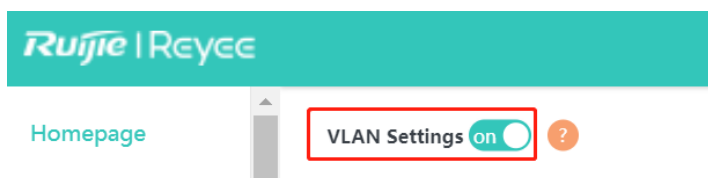
The homepage displays the global port information, including the port status, port VLAN settings, the packet receiving/transmission rate (Rx/Tx rate), port isolation status, loop detection status, and port PoE settings. Besides, it supports searching for the downlink device.

- Click **Port Status** to configure the basic port attributes. For details, see [2.2](#).
- Click **VLAN** to set the VLAN of the port. For details, see [3.2](#).

 Note

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

Figure 2-2 Enabling VLAN Settings



- Click **Isolation Status** to configure port isolation so that the downlink ports of the device are isolated from each other. For details, see [2.4](#)
- 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 [4.3](#)
- Click **PoE** to view and set PoE parameters of the port. For details, see [5](#).
- 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 2-3 Viewing or Configuring Port Settings

Port Info [Refresh List](#)

Port	Port Status						VLAN				Rx/Tx Rate (kbps)	Isolation Status	Loop Status	PoE		Downlink Device Search
	Status	Config Status		Actual Status	Flow Control(Config)	Flow Control(Actual)	Type	Access	Native	Permit				PoE Power	Action	
		Speed	Duplex													
Port 1	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	Access	2	--	--	0/0	Unisolated	Normal	--	--	View
Port 2	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	Access	1	--	--	0/0	Unisolated	Normal	--	--	View
Port 3	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	Access	1	--	--	0/0	Unisolated	Normal	--	--	View
Port 4	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	Access	1	--	--	0/0	Unisolated	Normal	--	--	View
Port 5	Enabled	Auto	Auto	Disconnected	Disabled	Disabled	Access	1	--	--	0/0	Unisolated	Normal	--	--	View

2.1.3 Port Packet Statistics

Choose **Monitoring > Packet Statistics**.

The **Packet 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 2-4 Port Packet Statistics

Packet Statistics

Port	Status	Connection Status	Rx/Tx Rate(kbps)	Rx/Tx Packets(KB)	Rx/Tx Success	Rx/Tx Failure
Port 1	Enabled	Disconnected	0/0	0/0	0/0	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	285676/192315	702667/992207	0/0
Port 10	Enabled	Connected	7/28	288974/578439	1650059/1327607	0/0

[Clear](#)

2.2 Setting and Viewing Port Attributes

Choose **Switch Settings > Port Settings**.

2.2.1 Port Settings

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

Click **Select** in the **Port** column to display options of all device ports. Select the ports you want to configure, and then select the port status, port rate, port duplex mode, flow control status, and click **Save**.

Figure 2-5 Port Parameter Configuration

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
--Select--	Enabled	Auto	Auto	Disabled

Port List

	Speed/Duplex		Flow Control	
	Config Status	Actual Status	Config Status	Actual Status
	Auto/Auto	1000M/Full Duplex	Disabled	Disabled
	Auto/Auto	Disconnected	Disabled	Disabled
	Auto/Auto	Disconnected	Disabled	Disabled
Port 4	Enabled	Auto/Auto	Disabled	Disabled
Port 5	Enabled	Auto/Auto	Disabled	Disabled
Port 6	Enabled	Auto/Auto	Disabled	Disabled
Port 7	Enabled	Auto/Auto	Disabled	Disabled
Port 8	Enabled	Auto/Auto	Disabled	Disabled
Port 9	Enabled	Auto/Auto	Disabled	Disabled

Table 2-2 Basic Port Configuration Parameters

Parameter	Description	Default
Port	Select the ports you want to configure.	NA
Status	When the port is disabled, it cannot receive or transmit packets (PoE is not affected).	Enabled
Speed	Configure the operating speed of the Ethernet physical port. When the speed is set to Auto , it means that it is determined by the auto-negotiation between the local port and the peer port. The negotiated speed can be any speed within the port capability.	Auto
Duplex	<ul style="list-style-type: none"> ● Full duplex: The port can receive packets while sending packets. ● Half duplex: The port can receive or send packets at a time. ● Auto-negotiation: The duplex mode of the port is determined by the auto-negotiation between the local port and the peer port. 	Auto
Flow Control	After enabling the flow control feature, the port will process the received flow control frames and send flow control frames when flow congestion occurs.	Disabled

⚠ Caution

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

- You can 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.

2.2.2 Port Status

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

Figure 2-6 Port Status

Port List

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

2.3 Port Mirroring

2.3.1 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 2-7](#) 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 2-7 Operating Principle of Port Mirroring



2.3.2 Configuration Steps

Choose **Switch Settings > 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 rule configured last will take effect.

Figure 2-8 Configuring Port Mirroring

Port Mirroring

Packets received and transmitted on the source port will be mirrored to the mirror port.(The image destination port can only grab packets and cannot transmit data with the switch)

Source Port Member	Direction	Mirror Port
--Select--	Input ▾	Port 1 ▾
Save		
Source Port Member	Direction	Mirror Port
Delete		

Table 2-3 Port Mirroring Parameters

Parameter	Description
Source Port Member	The source port is also called the monitored port. Packets on the source port will be mirrored to the mirror port for network analysis or troubleshooting. You can select multiple source ports. Packets on these ports will be mirrored to one mirror port.
Direction	Direction of the data traffic monitored on the source port: <ul style="list-style-type: none"> ● Bi-directions (input & output): All packets on the source port, including the received packets and the transmitted packets, will be mirrored to the mirror port. ● Input: The packets received by the source port will be mirrored to the mirror port. ● Output: The packets transmitted from the sourced port will be mirrored to the mirror port.
Mirror Port	The mirror port is also called the monitoring port. The mirror port is connected with a monitoring device, and it transmits packets on the source port to the monitoring device.

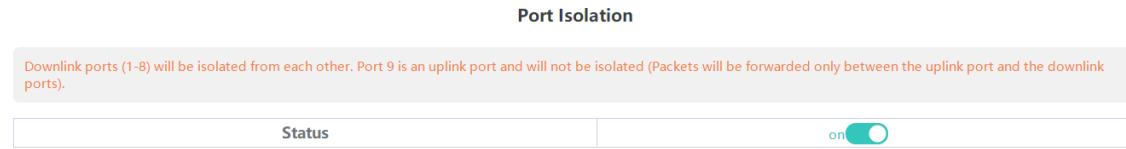
2.4 Port Isolation

Choose **Switch Settings > 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 2-9 Port Isolation



Caution

- 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 or disabled through the DIP switch on the device's front panel or through the web interface. The latest configuration takes effect.

2.5 Port-based Rate Limiting

Choose **QoS Settings > Port Rate**.

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 2-10 Port Rate

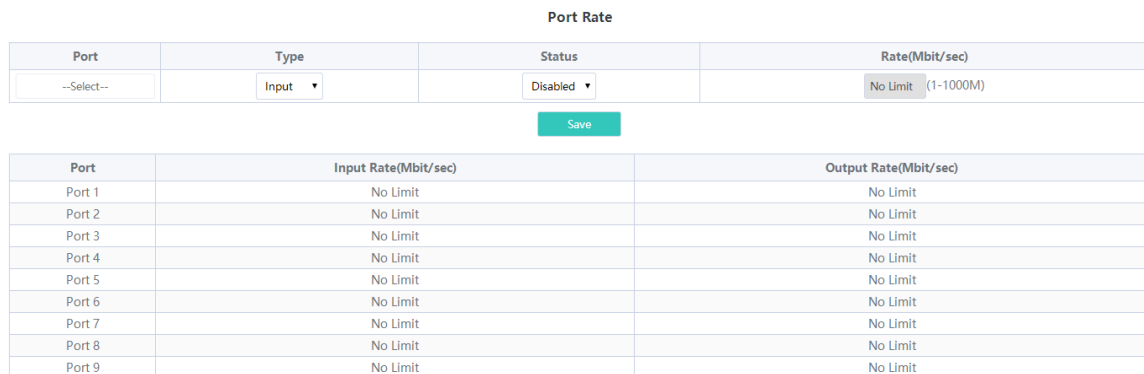


Table 2-4 Rate Limiting Parameters

Parameter	Description	Default
Port	You can select multiple ports for rate limiting configuration in batches.	NA

Parameter	Description	Default
Type	The direction of the rate-limited data traffic: <ul style="list-style-type: none"> ● Input & output: Rate limiting for all packets forwarded over the port, including the received packets and the transmitted packets. ● Input: Rate limiting for packets received by the port. ● Output: Rate limiting for packets transmitted from the port. 	NA
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.
- The port rate limit range of RG-NIS2100 series switches is from 1 Mbps to 1000 Mbps.

2.6 Management IP Address

Choose **System Settings > 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 2-11 IP Settings

IP Settings

VLAN	VLAN 1 <input type="button" value="v"/>
Auto Obtain IP	Enabled <input type="button" value="v"/> <small>If you disable this feature, multi-DHCP alarming will fail.</small>
IP Address	192.168.110.60
Submask	255.255.255.0
Gateway	192.168.110.1
Auto Obtain DNS	Enabled <input type="button" value="v"/>
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 [3.2.1](#).
 - The management VLAN must be selected from the existing VLANs. To create a static VLAN, refer to [3.2.2](#).
 - 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 [3.2.3](#).
 - If you disable **Auto Obtain IP** feature, multi-DHCP alarming will fail. For details about multi-DHCP alarming, see [7.2](#).
-

3 Switch Settings

3.1 Managing MAC Address

3.1.1 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.

3.1.2 Viewing MAC Address Table

Choose **Switch Settings > MAC Address Info**.

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 3-1 MAC Address Table

MAC Address Info

No.	MAC Address	VLAN ID	Type	Port
1	00:D0:F8:15:08:62	1	Dynamic	10
2	00:D0:F8:15:08:5F	1	Dynamic	10
3	58:69:6C:00:00:01	1	Dynamic	10
4	F8:E4:3B:3D:22:B1	1	Dynamic	10
5	70:85:C4:90:90:B5	1	Dynamic	10
6	00:D0:F8:15:33:5C	1	Dynamic	10
7	00:D0:F8:15:33:5B	1	Dynamic	10
8	10:11:22:FF:00:10	1	Dynamic	10

[Clear Dynamic MAC](#)

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.
-

3.1.3 Searching for MAC Address

Choose **Switch Settings > Search MAC**.

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 3-2 search for MAC address

MAC Address Search

MAC Address	VLAN ID
<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="VLAN ID (1-4094)"/>
<input type="button" value="Search"/>	

MAC Address	VLAN ID	Type	Port
F8:E4:3B:5A:CF:DC	1	Dynamic	Port 1

3.1.4 Configuring Static MAC Address

Choose **Switch Settings > 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 3-3 Configuring Static MAC Address

Static MAC Address

Up to 16 MAC addresses can be configured.

MAC Address	VLAN ID	Port
<input type="text" value="00:00:00:00:00:00"/>	<input type="text" value="VLAN ID (1-4094)"/>	<input type="text" value="Port 1"/>
<input type="button" value="Add"/>		

	No.	MAC Address	VLAN ID	Port
<input type="checkbox"/>	1	C8:4B:D6:06:FA:97	10	3

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

Figure 3-4 delete static MAC address

	No.	MAC Address	VLAN ID	Port
<input checked="" type="checkbox"/>	1	C8:4B:D6:06:FA:97	10	3

3.2 VLAN Settings

3.2.1 Global VLAN Settings

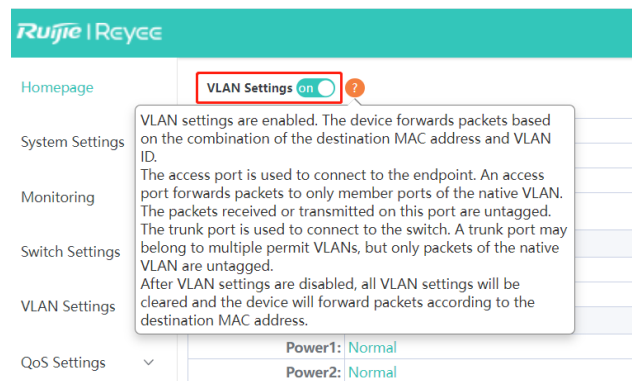
Choose **Homepage > Device Info**.

This page displays the status of VLAN settings. Toggle the **on-off** switch to enable or disable 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 3-5 VLAN Settings



3.2.2 Static VLANs Settings

Caution

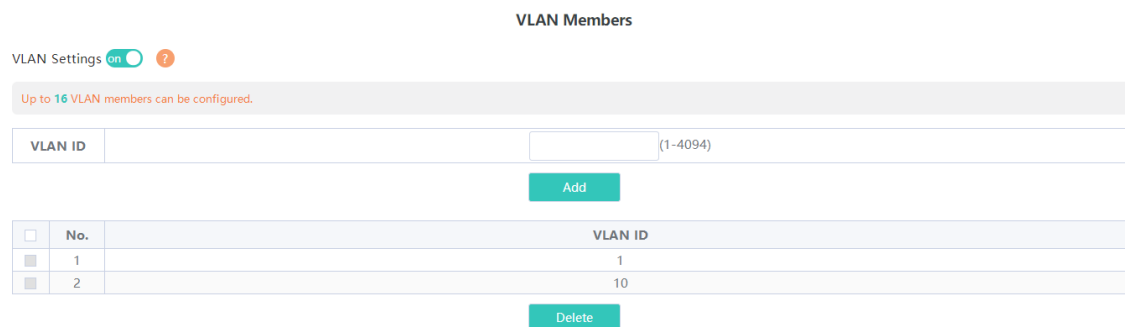
Static VLANs can be created only when the global VLAN settings feature is enabled. For details, see [3.2.1](#).

Choose **VLAN Settings > VLAN Members**.

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

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 3-6 Static VLANs Settings



- Note**
- The VLAN ID ranges from 1 to 4094. VLAN 1 is the default VLAN.
 - The Management VLAN (VLAN 1), Native VLAN, Permit VLAN, and Access VLAN cannot be deleted.

3.2.3 Port VLAN Settings

Caution

You can configure port VLAN only when the **VLAN Settings** function is enabled. For details, [see 3.2.1](#).

Choose **VLAN Settings > 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 [3.2.2](#)) before configuring the port based on VLANs. Click **VLAN Members** to access the **VLAN Members** page where you can add VLAN members.

- (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 3-7 Configuring Port VLANs

VLAN Settings

VLAN Settings on ?

You can go to [VLAN Members](#) to add a VLAN ID.

Port	VLAN Type	Permit VLAN	Native VLAN <small>The packets of this VLAN are untagged.</small>
--Select--	Access ▾	--Select--	VLAN 1 ▾

Save

Port	VLAN Type	Permit VLAN	Native VLAN
Port 1	Access	1	1
Port 2	Access	1	1
Port 3	Access	10	10
Port 4	Access	1	1
Port 5	Access	1	1
Port 6	Access	1	1
Port 7	Access	1	1
Port 8	Access	1	1

Table 3-1 Port Modes

Port Mode	Description
Access	<ul style="list-style-type: none"> ● One access port can belong to only one VLAN and allow frames from this VLAN only to pass through. This VLAN is called an access VLAN. ● The frames from the access port do not carry VLAN tag. When the access port receives an untagged frame from a peer device, the local device determines that the frame comes from the access VLAN and adds the access VLAN ID to the frame. ● Access port is connected to the endpoints.
Trunk	<ul style="list-style-type: none"> ● One trunk port supports one Native VLAN and several Permit VLANs. Native VLAN frames forwarded by a trunk port do not carry tags while Permit VLAN frames forwarded by the trunk port carry tags. Trunk port is connected to switches. ● You can set the Permit VLAN range to limit VLAN frames that can be forwarded. ● Make sure the trunk ports at the two ends of the link are configured with the same Native VLAN.

i Note

Improper configuration of VLANs on a port (especially uplink port) may cause failure to log in to the web interface. Exercise caution when configuring VLANs.

4 Security

4.1 DHCP Snooping

4.1.1 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.

4.1.2 Configuration Steps

Choose **Switch Settings > DHCP Snooping Settings**.

Toggle the switch to **On** to enable DHCP snooping, select the trusted ports, and then click **Save**. When DHCP snooping is enabled, request packets from DHCP clients are forwarded only to the trusted ports. For response packets from DHCP servers, only those from the trusted ports are forwarded.

Note

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

Figure 4-1 DHCP Snooping

DHCP Snooping Settings

Tip:DHCP Snooping functions as a DHCP packet filter. The DHCP request packets will be forwarded only to the trusted port. 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: on off

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

4.2 Storm Control

4.2.1 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.

4.2.2 Configuration Steps

Choose **QoS Settings > 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 4-2 Storm Control

Storm Control

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

Save

Type	Broadcast(Mbit/sec)	Unknown Unicast(Mbit/sec)	Unknown Broadcast(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

i Note

For RG-NIS2100 series switches, the value range of port storm control rate limit is from 1 Mbps to 1000 Mbps.

4.3 Loop Guard

Choose **Monitoring > Loop Guard**.

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 4-3 Loop Guard

Loop Guard

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

Enabled	off <input type="checkbox"/>
----------------	------------------------------

5 PoE Settings

Caution

This function is only supported on PoE-capable devices.

Choose **PoE Settings**.

The device supports PoE power supply. You can view and configure the current power status.

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

Note

- If a non-PD, such as a computer, is connected to a PoE-enabled port of this device, the PoE watchdog will not initiate any action on the non-PD even if the trigger condition is met.
- The PoE watchdog ping interval (in seconds) can be set to a value in the range of 90 to 1800.

Figure 5-1 PoE Settings

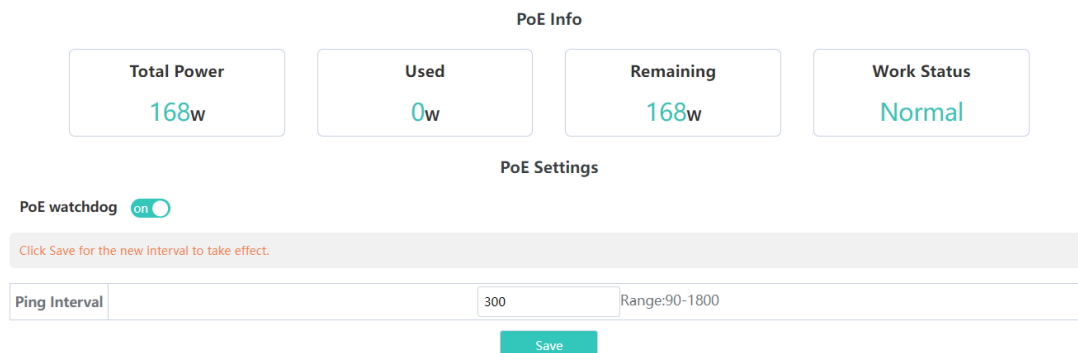


Table 5-1 PoE Watchdog Configuration Description

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

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

- Port status: The voltage, current, output power, and current power status of the device ports are displayed. You can enable or disable PoE function through the **on-off** toggle switch. When PoE is disabled, the port will not supply power to external devices.

Figure 5-2 Port Status

PoE Status <small>When off, PoE will not work on this port</small>	Port	Power(W)	Current(mA)	Voltage(V)	Non-Standard <small>PoE Non-standard PoE: When enabled, the device can supply power to a PD that may not conform to IEEE802.3af/at standards.</small>	Power Status	Action
<input checked="" type="checkbox"/>	Port 1	0	0	0	<input type="checkbox"/> No	Powered Off	--
<input checked="" type="checkbox"/>	Port 2	0	0	0	<input type="checkbox"/> No	Powered Off	--
<input checked="" type="checkbox"/>	Port 3	0	0	0	<input type="checkbox"/> No	Powered Off	--
<input checked="" type="checkbox"/>	Port 4	0	0	0	<input type="checkbox"/> No	Powered Off	--
<input checked="" type="checkbox"/>	Port 5	0	0	0	<input type="checkbox"/> No	Powered Off	--
<input checked="" type="checkbox"/>	Port 6	0	0	0	<input type="checkbox"/> No	Powered Off	--
<input checked="" type="checkbox"/>	Port 7	0	0	0	<input type="checkbox"/> No	Powered Off	--
<input checked="" type="checkbox"/>	Port 8	0	0	0	<input type="checkbox"/> No	Powered Off	--
Port 9 Unsupported							
Port 10 Unsupported							

6 ERPS

6.1 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.

6.2 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.

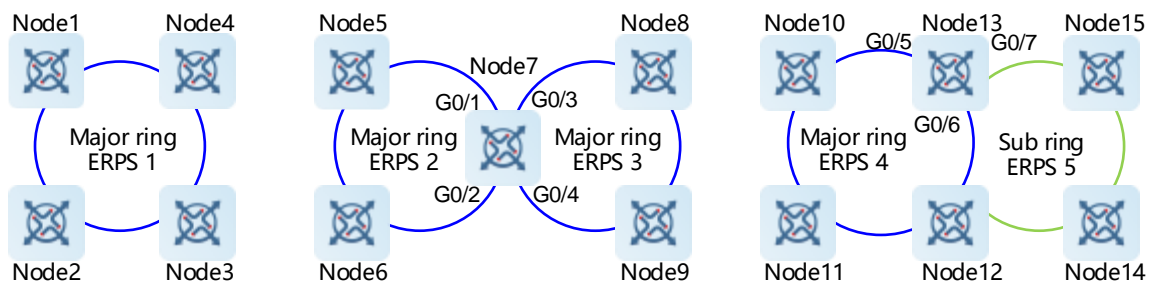
6.3 Basic Model of an Ethernet Ring

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.

6.3.1 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 6-1](#). In an ERPS ring, links that belong to and are controlled by a major ring are called major ring links.
- Subring and subring link: A subring is a topology of a non-closed network attached to a major ring, such as the green ring shown in [Figure 6-1](#). In an ERPS ring, links that belong to and are controlled by a subring are called subring links.
- R-APS virtual channel of a subring: As shown in [Figure 6-1](#), all the links on the major ring can be regarded as R-APS virtual channels of subrings, which are used to forward subring protocol packets. They belong to the major ring instead of the subring. The major ring must associate with the control VLAN of the subring and allow packets from this VLAN to pass through.

Figure 6-1 Basic Topologies of Ethernet Rings



6.3.2 Basic Topologies

Major rings, subrings, and nodes can form basic topologies with different characteristics, depending on the connection modes, as shown in [Figure 6-1](#).

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

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

6.3.3 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 6-1](#), nodes 1-4 in the single-ring topology, nodes 5, 6, 8, and 9 in the tangent-ring topology, and nodes 10, 11, 14, and 15 in the intersecting-ring topology are all single-ring nodes.
- **Tangent node:** A device shared in tangent rings is called a tangent node. Four interfaces need to be provided on each tangent node, with two added to a major ring and the other two added to another major ring. As shown in [Figure 6-1](#), node 7 in the tangent-ring topology is a tangent node.
- **Intersecting node:** The nodes in intersecting rings that belong to multiple rings are called intersecting nodes. Three interfaces need to be provided on a tangent node, with two added to a major ring and the other added to a subring. As shown in [Figure 6-1](#), nodes 12 and 13 in the intersecting-ring topology are intersecting nodes. ERPS rings can intersect with other multiple ERPS rings and share links to implement data link redundancy. Services can be quickly switched from a failed link in one ERPS ring to a normal link.

6.3.4 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 6-1](#):

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

Table 6-1 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

6.4 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.

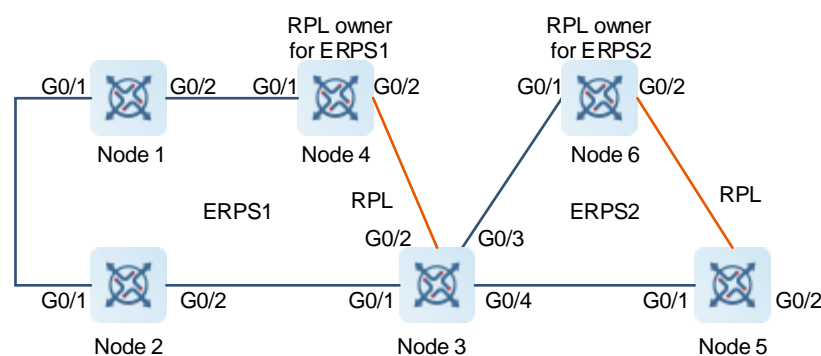
Ring protection link (RPL): When the physical links in a ring network are connected, the ERPS ring is in the idle state, and the links in the logic blocking state are RPLs. Each Ethernet ring has only one RPL. For example, the links indicated by the orange lines shown in [Figure 6-2](#) are RPLs, the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

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

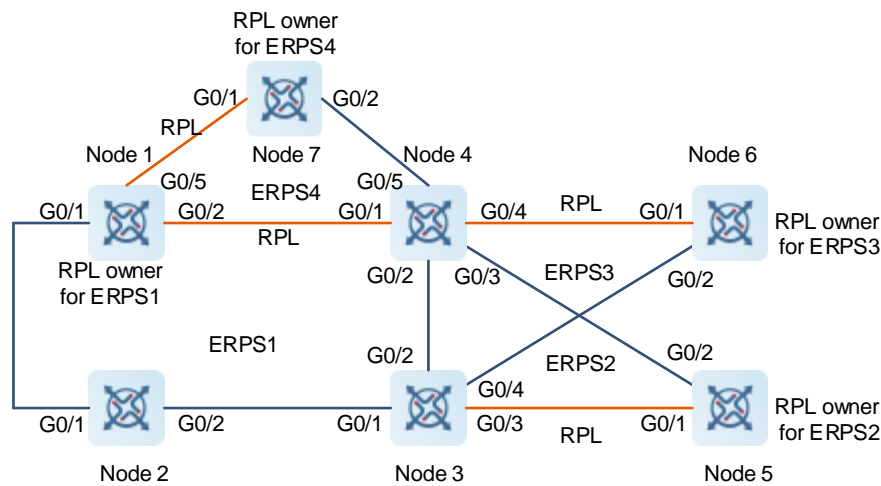
Any nodes other than the RPL owner node in an Ethernet ring are non-RPL owner nodes. As shown in [Figure 6-2](#), nodes except node 4 and node 6 are non-RPL owner nodes of the rings.

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

Figure 6-2 Typical Topology of Tangent Rings



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

Figure 6-3 Typical Topology of Intersecting Rings

As shown in [Figure 6-3](#), ERPS 1 (node 1-2-3-4) is a major ring, and ERPS 2 (node 3-4-5) is a subring. ERPS 1 and ERPS 2 share node 3 and node 4, forming an intersecting-ring topology. The links between node 4 and node 5, and between node 3 and node 5 are links of the subring ERPS 2 and are controlled by ERPS 2. The link between node 3 and node 4 belongs to the major ring not the subring, and is not controlled by the subring. However, the protocol packets of the subring are transmitted through the direct link between node 3 and node 4. This direct link is the R-APS virtual channel of the subring ERPS 2. Node 2 only belongs to the major ring ERPS 1, and is called a single-ring node. Node 6 only belongs to the subring ERPS 3, and is also called a single-ring node. Node 3 and node 4 are tangent nodes.

6.5 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.

6.6 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.

6.7 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.

6.8 Protocols and Standards

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

6.9 Configuring ERPS

Choose **ERPS**.

(1) As shown in [Figure 6-4](#), after configuring the ERPS ring parameters, click **Add** to add the ERPS ring.

Note

- The west port and the east port must be trunk ports. For details on how to configure trunk ports, see [3.2.3](#).
-

- In the permit VLANs of the west port and the east port, the native VLAN cannot be used as a control VLAN.
- 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.
- After enabling ERPS through the web interface, disable ERPS first and then re-enable it using the DIP switch on the front panel. This ensures that the ERPS ring utilizes the configuration performed through the web interface.

Figure 6-4 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	<input type="text" value="1"/> (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 ▾

Add

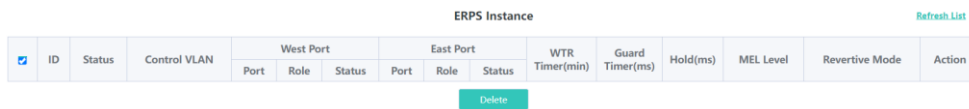
Table 6-2 Parameter Description

Parameter	Description	Default Value
ID	Specifies the ID of an ERPS instance.	N/A
Control VLAN	It is used to forward ERPS protocol packets.	N/A
West Port/Role	<ul style="list-style-type: none"> ● Specifies the west port in the ERPS ring and its role. The values of a port role include: ● NORMAL: Indicates a normal node. ● RPL OWNER: Indicates an RPL owner node. ● RPL NEIGHBOR: Indicates an RPL neighbor node. 	N/A
East Port/Role	<ul style="list-style-type: none"> ● Specifies the east port in the ERPS ring and its role. ● The values of a port role include: ● NORMAL: Indicates a normal node. ● RPL OWNER: Indicates an RPL owner node. 	N/A

Parameter	Description	Default Value
	<ul style="list-style-type: none"> RPL NEIGHBOR: Indicates an RPL neighbor node. 	
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 this switch is toggled on, once the condition causing a switch has cleared, traffic is blocked on the RPL.	Enabled.

(2) (Optional) As shown in [Figure 6-5](#), select one or more ERPS rings, and click **Delete** to delete the selected ERPS rings.

Figure 6-5 Deleting Selected ERPS Rings



(3) (Optional) As shown in [Figure 6-6](#), configure parameters as needed, and click **Confirm** to switch the link of the ERPS ring.

Figure 6-6 Link Switch

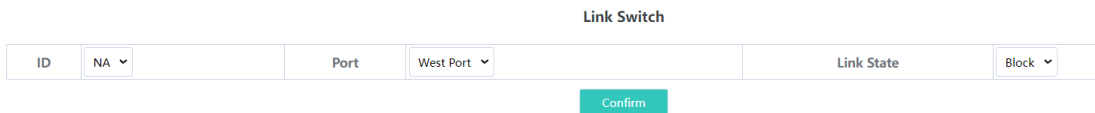


Table 6-3 Parameter Description

Parameter	Description	Default Value
ID	Specifies the ID of an ERPS instance.	N/A
Port	Specifies the port in the ERPS ring. The values include West Port and East Port.	N/A
Link State	Specifies the link state of the selected port.	N/A

Parameter	Description	Default Value
	<ul style="list-style-type: none"> ● Clear: Clears the forced switch state of the port, and allows the protocol to elect the port to be blocked. ● Block: Indicates that the port is blocked by a forced switch operation. 	

6.10 ERPS Typical Configuration Examples

i Note

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

6.10.1 Requirements

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

6.10.2 Topology



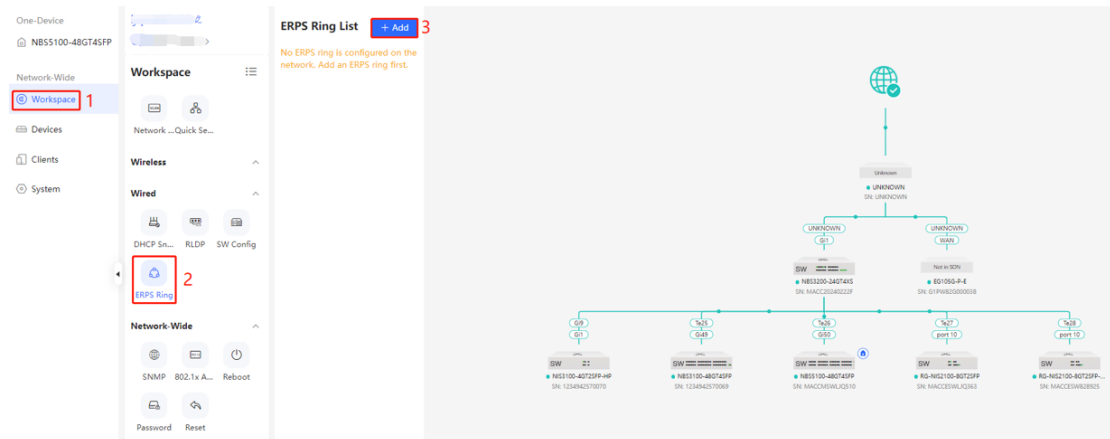
6.10.3 Notes

- 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.

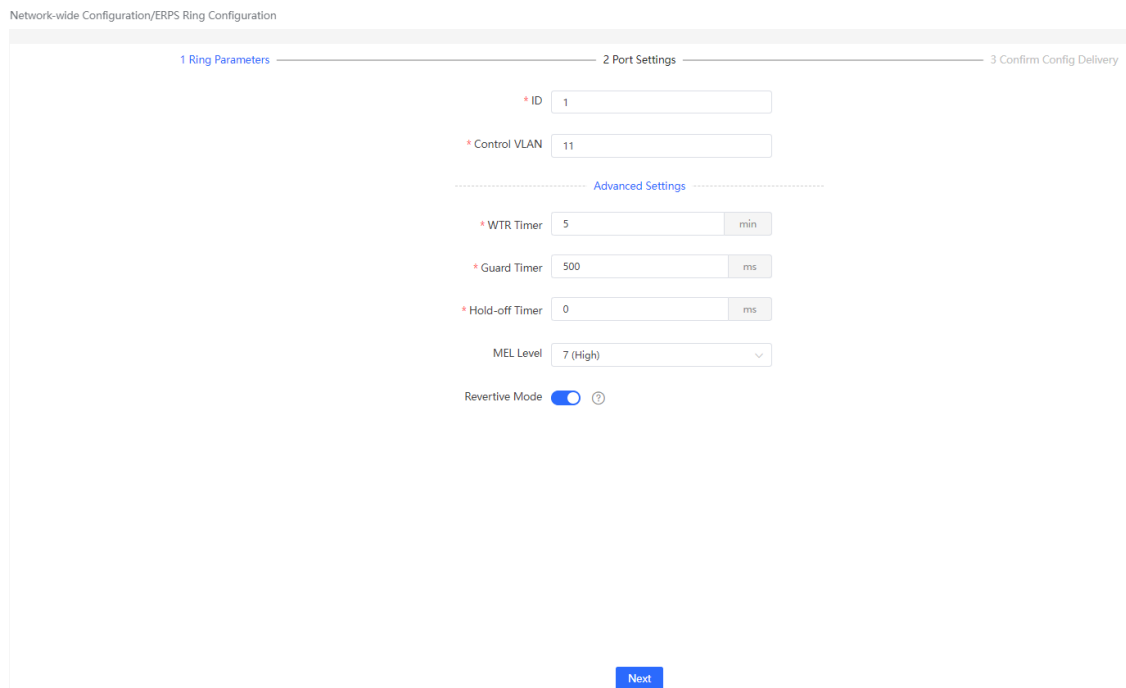
6.10.4 Procedure

- (1) Log in to the web interface of the master device.
- (2) Choose **Network-Wide > Workspace > Wired > ERPS Ring** to access the **ERPS Ring** configuration page.

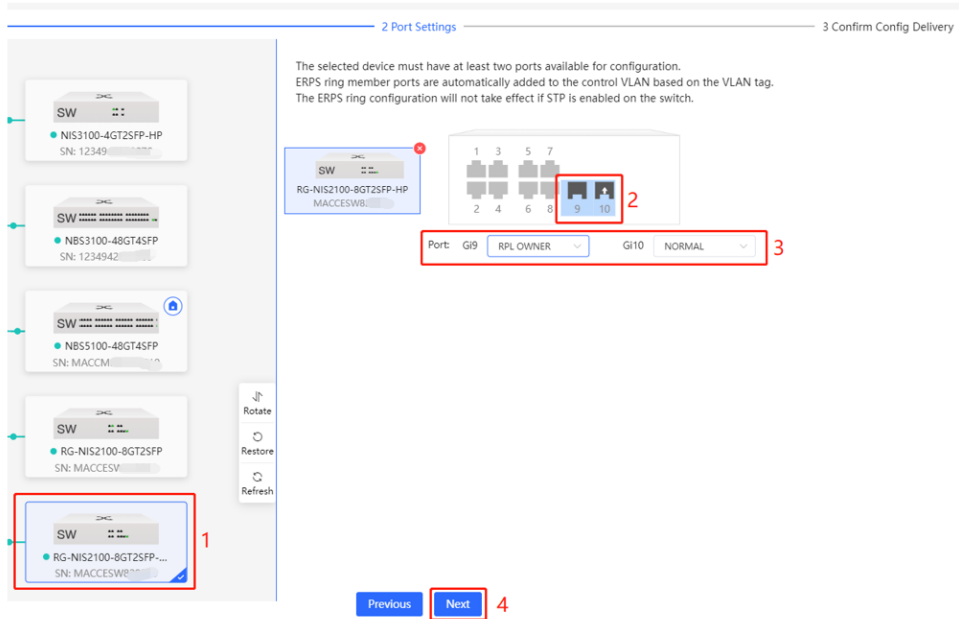
(3) Click **+Add** on the page to add an ERPS ring.



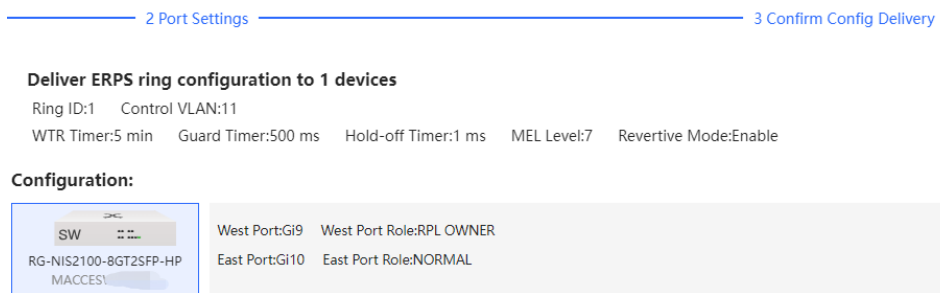
(4) As shown in the following figure, set the ERPS ring parameters (only **ID** and **Control VLAN** are mandatory, and should be configured according to the user's network setup. Other parameters can be left at their default values). Then, click **Next**.



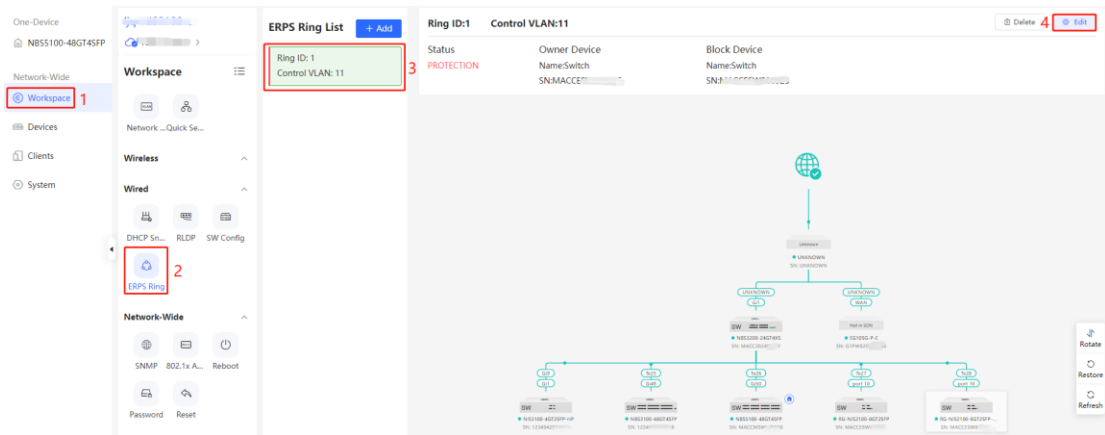
(5) As shown in the following figure, select a device for the ERPS ring, set the Gi9 to **RPL OWNER**, and Gi10 to **NORMAL**. Click **Next**.



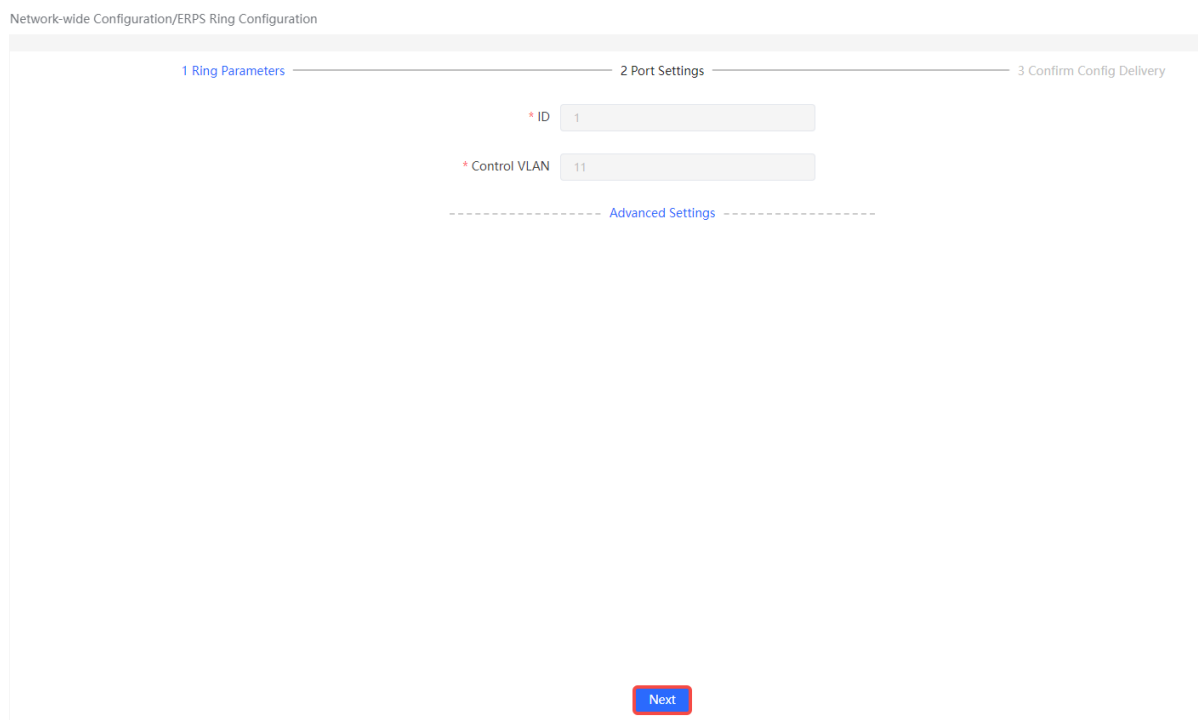
(6) As shown in the following figure, click **Save** to save the configuration.



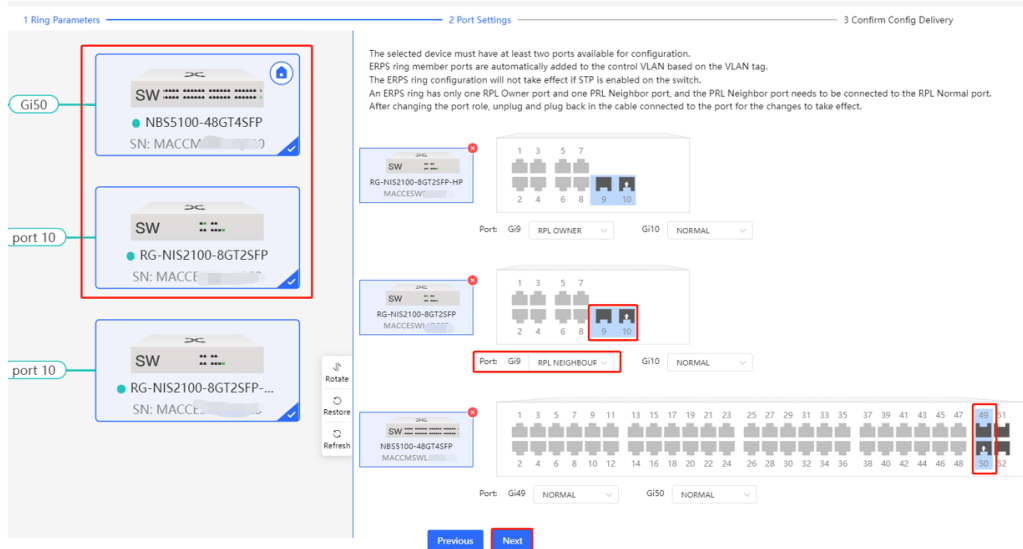
(7) As shown in the following figure, choose **Network-Wide > Workspace > Wired > ERPS Ring**. On the page that opens, click **Edit**.



(8) As shown in the following figure, click **Next** to access the **ERPS Ring Configuration** page.



(9) As shown in the following figure, 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**.



(10) As shown in the following figure, click **Save** to apply all configurations.



Deliver ERPS ring configuration to 3 devices

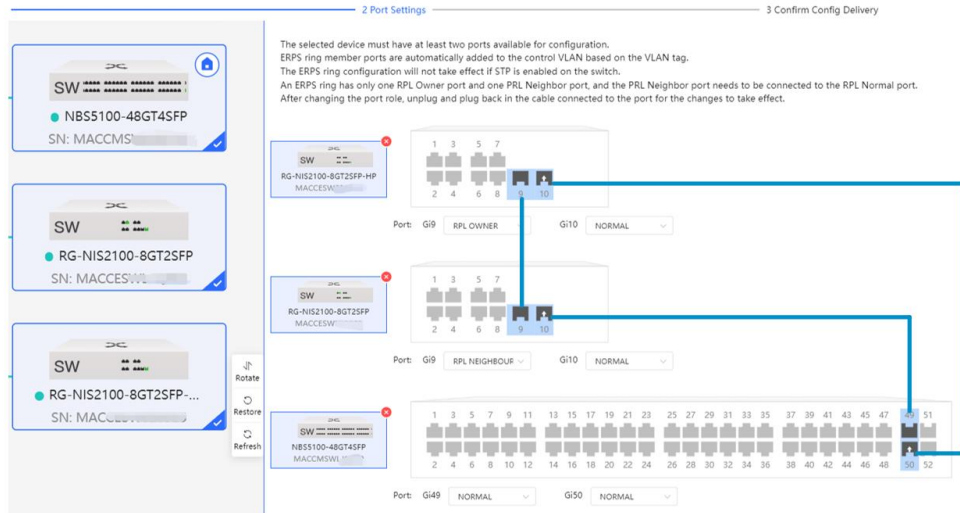
Ring ID:1 Control VLAN:11
 WTR Timer:5 min Guard Timer:500 ms Hold-off Timer:1 ms MEL Level:7 Revertive Mode:Enable

Configuration:

 SW RG-NIS2100-8GT2SFP-HP MACCE...	West Port:G9 West Port Role:RPL OWNER East Port:G10 East Port Role:NORMAL
 SW RG-NIS2100-8GT2SFP MACCES...	West Port:G9 West Port Role:RPL NEIGHBOUR East Port:G10 East Port Role:NORMAL
 SW NBS5100-48GT4SFP MAC...	West Port:G49 West Port Role:NORMAL East Port:G50 East Port Role:NORMAL



As shown in the figure below, after all cables are connected according to the topology, the devices will automatically form an ERPS ring.



7 Diagnostics

7.1 Cloud Settings

Choose **Diagnostics > 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**.

Figure 7-1 Cloud Settings

Cloud Settings

Cloud Status	Connectable
Reason	This device is not registered to Ruijie Cloud.
Domain	iotrc.ruijienetworks.com:7683
IP	47.105.111.251

Save
Restore Default

To restore the default domain name, click **Restore Default**, and then click **OK** on the pop-up window.

Figure 7-2 Restoring the Default Domain Name

Cloud Settings

Cloud Status	Connectable
Reason	This device is not registered to Ruijie Cloud.
Domain	<input type="text" value="iotrc.ruijienetworks.com:7683"/>
IP	47.105.111.251

Table 7-1 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: <ul style="list-style-type: none"> ● Connected: No reason is displayed. ● Unconnected: <ul style="list-style-type: none"> ○ No Internet connection or DNS resolution failure. ○ This device failed to connect to Ruijie Cloud. ● Connectable: This device is not registered to Ruijie Cloud.
Domain	Domain name of the cloud server <hr/> <p>⚠ Caution</p> <ul style="list-style-type: none"> ● 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. <hr/>
IP	IP address of the cloud server resolved based on the cloud address.

7.2 System Logs

Choose **Diagnostics > System 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 7-3 System Logs

System Logs

Number	Time(UTC)	Type	Module	Details
1	2024/04/24 07:47:32	info	port	Port9 link down.
2	1970/01/01 00:00:05	info	port	Port10 link up.
3	1970/01/01 00:00:05	info	port	Port9 link up.

1

⚠ Caution

If the preceding troubleshooting steps fail to resolve the issue, and remote assistance from technical support is needed, you can contact them to assist in enabling the developer mode. The technical support team can then perform diagnostics to identify and address the issue effectively.

8 System Settings

8.1 Managing Device Information

8.1.1 Viewing Device Information

Choose **Homepage**.

On this page, you can view information about the device, including basic device information, DIP switch effective state, and power supply status.

- **Device Info**

The device information is displayed on the homepage, including hostname, device model, serial number, firmware version, IP address, MAC address, cloud status, and uptime. Click **Device Info** to access the **Device Info** page (**System Settings > Device Info**) to view more detailed information.

Figure 8-1 Device Info

Model: RG-NIS2100-8GT2SFP-HP	Firmware Version: ESW_1.0(1)B1P31,Release(11161510)
MAC Address: [REDACTED]	SN: [REDACTED]
IP Address: 192.168.110.60	Uptime: 6d 19h 10min 32s
Cloud Status: Connected Download App	Hostname: <input type="text" value="ruijie"/> Edit

Figure 8-2 Viewing Device Information

System Settings

Hostname	ruijie
Model	RG-NIS2100-8GT2SFP-HP
MAC Address	[REDACTED]
IP Address	192.168.110.60
Submask	255.255.255.0
Gateway	192.168.110.1
DNS	192.168.110.1
SN	[REDACTED]
Firmware Version	ESW_1.0(1)B1P31,Release(11161510)
Firmware Date	Apr 15 2024
Hardware Version	1.00
Development mode	on <input checked="" type="checkbox"/>

- **DIP Switch Effective State:** You can view the configuration status of ERPS, port isolation, forced 10 Mbps, and power supply alarm. (When the effective status of a certain function conflicts with that of the DIP switch,



will appear next to the status. You can hover over the icon to view a tooltip.)

- **Power Supply Status:** You can view the status and the voltage of the power supply.

Figure 8-3 DIP Switch Effective State and Power Supply Status

DIP Switch Effective State	
ERPS: Enabled	Port Isolation: Disabled
10 Mbps (Ports 5-8): Disabled	Alarm: Disabled
Power Supply Status (Normal voltage range: 46.0V~57.0V)	
Power1: Normal	Voltage: 53.2V
Power2: Normal	Voltage: 53.2V

8.1.2 Editing the Hostname

Choose **Homepage > Device Info.**

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

Figure 8-4 Editing the Hostname

Device Info	
Model: RG-NIS2100-8GT2SFP-HP	Firmware Version: ESW_1.0(1)B1P31,Release(11161510)
MAC Address: 00:D0:F8:11:2D:00	SN: MACCESW828925
IP Address: 192.168.110.60	Uptime: 6d 19h 12min 48s
Cloud Status: Connected Download App	Hostname: ruijie Edit

8.1.3 Cloud Management

Choose **Homepage > Device Info.**

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

Figure 8-5 Cloud Management

Device Info	
Model: RG-NIS2100-8GT2SFP-HP	Firmware Version: ESW_1.0(1)B1P31,Release(11161510)
MAC Address: [blacked out]	SN: [blacked out]
IP Address: 192.168.110.60	Uptime: 6d 19h 14min 49s
Cloud Status: Connected Download App	Hostname: ruijie Edit

8.2 Setting the Maximum Power of the Power Supply

Choose **System Settings > Maximum Power.**

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

Note

- The power value should approximate the actual output power of the power supply.
- The default power of RG-NIS2100-8GT2SFP-HP is 240 W, and that of RG-NIS2100-4GT2SFP-HP is 120 W. For other models, see the documentation of corresponding models.

Figure 8-6 Setting the Maximum Power

Maximum Power

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.

Maximum Power ⓘ	180 W
PoE Total Power ⓘ	168 W

Save

8.3 Password Settings

When the device password is the default password, you will be prompted to reset the password when logging into the web interface. Click **Yes** to access the **Account Settings** page (or choose **System Settings > Account Settings** to access the page).

Set a new password according to the tip, and then click **Save** to save the configuration.

Figure 8-7 Password Settings

Account Settings

Tip: The current password is the default password.

Account	admin
Password	Password ⓘ The password must contain only letters, numbers and the following special characters: <=>[]!@#*\$%&.
Confirm Password	Confirm Password ⓘ

Save

If the device is under uniform management, it cannot be configured with an independent password. You need to follow the tip to log in to the master device for global password configuration.

Figure 8-8 Managing the Account

Account Settings

Tip: The device is under uniform management and cannot be configured with an independent password. Please use MACC or App to change the password of all devices. If you change the password of only this device, configuration synchronization will fail. Please enter 192.168.110.1 to change the global password.

Account	admin
----------------	-------

Caution

- Upon your initial login to the web interface, you must set the device management password first before you configuring other features.
- Please remember the device management password (default password: admin). You may need to log in again after changing the password.

- If the device has been under uniform management, please use MACC or APP to change the network-wide password. Changing the password of this device will cause failure to synchronize network-wide settings to this device.

8.4 Device Reboot

Choose **System Settings > Reboot**.

Click **Reboot** to reboot the switch.

Figure 8-9 Device Reboot

Reboot

Please click Reboot to reboot the switch.



8.5 System Upgrade

8.5.1 Local Upgrade

Choose **System Settings > 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 8-10 Local Upgrade

Local Upgrade

Select File Keep Old Config

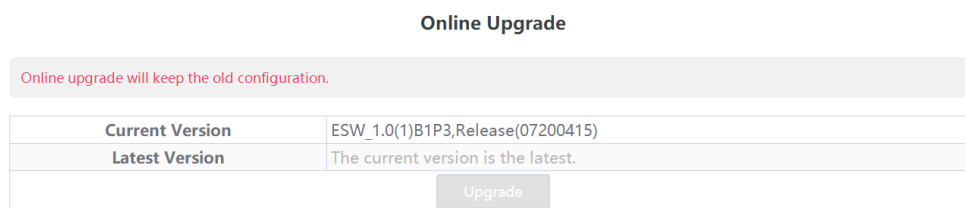
Decompress the package and select the bin file for upgrade.

8.5.2 Online Upgrade

Choose **System Settings > 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 8-11 Online Upgrade



Note

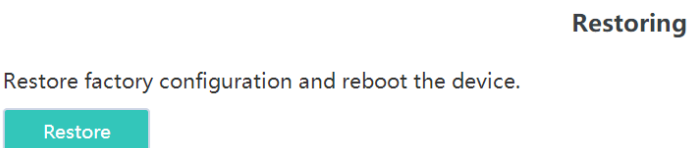
The time that online upgrade takes depends on the current network speed. It may take some time. Please be patient.

8.6 Restoring Factory Configuration

Choose **System Settings > Restore Default**.

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

Figure 8-12 Restoring Factory Configuration



9 Monitoring

9.1 Cable Diagnostics

Choose **Monitoring > Cable Diagnostics**.

Cable diagnostics 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 9-1 Cable Diagnostics

<input type="checkbox"/>	Port	Test Result	Details
<input checked="" type="checkbox"/>	Port 1	Disconnected	Please check cable connection or replace the cable.
<input checked="" type="checkbox"/>	Port 2	Disconnected	Please check cable connection or replace the cable.
<input type="checkbox"/>	Port 3	-	-
<input type="checkbox"/>	Port 4	-	-
<input type="checkbox"/>	Port 5	-	-
<input type="checkbox"/>	Port 6	-	-
<input type="checkbox"/>	Port 7	-	-
<input type="checkbox"/>	Port 8	-	-
<input type="checkbox"/>	Port 9	Unsupported	The port does not support cable diagnostics.
<input type="checkbox"/>	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.

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 [2.6](#).

Choose **Homepage**.

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 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 DHCP server, and MAC address.

9.3 Viewing Switch Information

Choose **Monitoring > Switches**.

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

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 **IP Address** of a device to access the web interface of the device (login required).

Figure 9-3 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
192.168.110.15	MACCMSV	NBS5100-48GT4SF

Switch List

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

No.	IP Address	SN	Hostname	Model
1	192.168.110.60(Local)	MACCESW8	ruijie	RG-NIS2100-8GT2SFP-HP
2	192.168.110.79	MACCESV	ruijie	RG-NIS2100-8GT2SFP

Note

- The number of switches that can be discovered varies with product models.
- A RG-NIS2100 series switch can discover up to 32 switches.

10 FAQs

Q1: I failed to log into the web interface. What can I do?

- (1) Verify that the Ethernet cable is properly connected to the LAN port of the device and the LED indicator blinks or is steady on.
- (2) Before accessing the web interface, you are advised to configure the PC with a static IP address in 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.

Q2: What can I do if I forget my password? How to restore the factory settings?

- (1) Log in with the default password (default password: admin).
- (2) If you fail to log in with the default password, restore the factory settings. To restore the factory settings, please power on the device, and press and hold the **Reset** button for 5s or more, and release the **Reset** button after the system LED indicator blinks. The device automatically restores the factory settings and restarts. After device restart, you can log into the web interface by accessing the default management IP address (10.44.77.200).