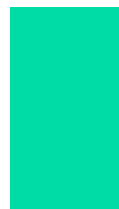
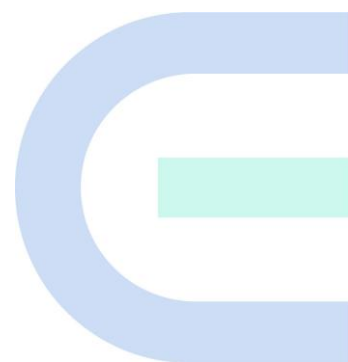


Ruijie Reyee RG-NBS Series Switches

Implementation Cookbook



Copyright

Copyright © 2024 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 you purchase are subject to commercial contracts and terms, and some or all of the products, services, or features described in this document may not be available for you to purchase or use. Except for the agreement in the contract, Ruijie Networks makes no explicit or implicit statements or warranties with respect to 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 will be updated from time to time due to product version upgrades or other reasons, Ruijie Networks reserves the right to modify the content of the document without any notice or prompt.

This manual is designed merely as a user guide. Ruijie Networks has tried its best to ensure the accuracy and reliability of the content when compiling this manual, but it does not guarantee that the content of the manual is completely free of errors or omissions, and all the information 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

- 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


This document also uses signs to indicate some important points during the operation. The meanings of these signs are 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.

 Note

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

 Instruction

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. Instruction

This manual is used to guide users to understand the product, install the product, and complete the configuration.

- The example of the port type may be different from the actual situation. Please proceed with configuration according to the port type supported by the product.
- The example of display information may contain the content of other product series (such as model and description). Please refer to the actual display information.
- The routers and router product icons involved in this manual represent common routers and layer-3 switches running routing protocols.

Ruijie Reyee RG-NBF Series Switches Implementation Cookbook

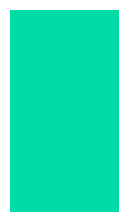
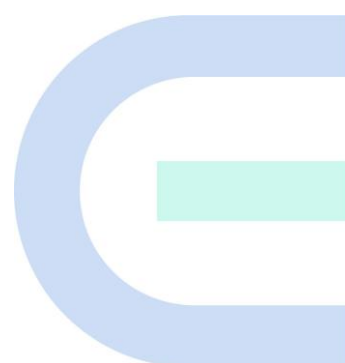
This cookbook consists of multiple independent volumes, introducing the installation, deployment, and web-based configuration of the RG-NBF Series Switches, including:

- 01- RG-NBF2100S Series e-Lighten Access Switches Installation Guide
- 02- RG-NBF5200M-8FS16GT4XS e-Lighten Core Switch Installation Guide
- 03- RG-NBF6002M e-Lighten Core Switch Installation Guide
- 04- ReyeeOS 2.290 Configuration Guide

Ruijie Reyee

RG-NBF2100S Series e-Lighten Access Switches

Installation Guide



Copyright

Copyright © 2024 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 you purchase are subject to commercial contracts and terms, and some or all of the products, services, or features described in this document may not be available for you to purchase or use. Except for the agreement in the contract, Ruijie Networks makes no explicit or implicit statements or warranties with respect to 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 will be updated from time to time due to product version upgrades or other reasons, Ruijie Networks reserves the right to modify the content of the document without any notice or prompt.

This manual is designed merely as a user guide. Ruijie Networks has tried its best to ensure the accuracy and reliability of the content when compiling this manual, but it does not guarantee that the content of the manual is completely free of errors or omissions, and all the information 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

- 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. Signs

This document also uses signs to indicate some important points during the operation. The meanings of these signs are as follows:

 Caution


An alert that calls attention to safety instruction that if not understood or followed can result in personal injury.

 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.

 Note

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

 Instruction

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. Note

This manual provides installation steps, troubleshooting, technical specifications, and usage guidelines for cables and connectors. It is intended for users who want to understand the above and have extensive experience in network deployment and management, and assume that users are familiar with related terms and concepts.

Contents

Preface	I
1 Overview	1
1.1 About the RG-NBF2100S Series Switches	1
1.2 Package Contents.....	2
1.2.1 Package Contents of the RG-NBF2100S-8GT1SC-P	2
1.2.2 Package Contents of the RG-NBF2100S-8GT1SC.....	2
1.2.3 Package Contents of the RG-NBF2100S-16GT1SC-P	3
1.3 Product Appearance	3
1.3.1 Appearance of the RG-NBF2100S-8GT1SC-P	3
1.3.2 Appearance of the RG-NBF2100S-8GT1SC.....	5
1.3.3 Appearance of the RG-NBF2100S-16GT1SC-P	6
1.4 Hardware Specifications	8
1.4.1 Hardware Specifications of the RG-NBF2100S-8GT1SC-P	8
1.4.2 Hardware Specifications of the RG-NBF2100S-8GT1SC	10
1.4.3 Hardware Specifications of the RG-NBF2100S-16GT1SC-P	11
2 Preparing for Installation	13
2.1 Safety Guidelines.....	13
2.1.1 General Precautions	13
2.1.2 Chassis-Lifting Guidelines	13
2.1.3 Electricity Safety	13
2.1.4 Preventing ESD Damage.....	14
2.1.5 Laser Safety	14
2.2 Site Requirements	15

2.2.1 Floor Loading	15
2.2.2 Airflow.....	15
2.2.3 Space	15
2.2.4 Temperature and Humidity.....	15
2.2.5 Cleanliness.....	16
2.2.6 Grounding	17
2.2.7 Anti-Electromagnetic Interference.....	17
2.2.8 Surge Protection	17
2.2.9 EMI.....	18
2.2.10 Installation Site.....	18
2.3 Rack Requirements	18
2.4 Tools	19
3 Installing the Switch	20
3.1 Precautions for Installation	20
3.2 Installation Procedure	20
3.2.1 Installing a Switch in a Rack.....	20
3.2.2 Mounting a Switch on the Wall	21
3.2.3 Mounting a Switch on the Ceiling	22
3.2.4 Installing a Switch on a Desktop.....	23
3.3 Connecting the Grounding Wire	24
3.4 Connecting the Power Cord.....	25
3.4.1 Connecting the Power Cord of the Power Adapter.....	25
3.4.2 Connecting the AC Power Cord.....	25
3.5 Verifying Installation.....	25

4 Log in to the Web UI.....	26
5 Troubleshooting.....	27
5.1 Troubleshooting Flowchart	27
5.2 Common Faults.....	27
5.2.1 Forgot or Lost the System Login Password.....	27
5.2.2 System Status LED Is Off for a Long Time.....	27
5.2.3 Only Partial PoE Ports Can Supply Power	27
6 Appendix.....	29
6.1 Ports, Connectors, and Media	29
6.1.1 1000BASE-T/100BASE-TX/10BASE-T Ports.....	29
6.1.2 PON Ports and SC Ports	30
6.2 Surge Protection	30
6.2.1 Installing an AC Power Lightning Arrester	30
6.2.2 Installing an Ethernet Port Lightning Arrester.....	32
6.3 Recommended Cabling	34
6.3.1 Requirements for the Minimum Bend Radius of an Ethernet Cable	34
6.3.2 Requirement for the Minimum Bend Radius of an Optical Cable	34
6.3.3 Precautions for Bundling up Cables	34
6.4 Site Selection	37
6.5 Cleaning the Connectors and End Faces of Optical Cables.....	38

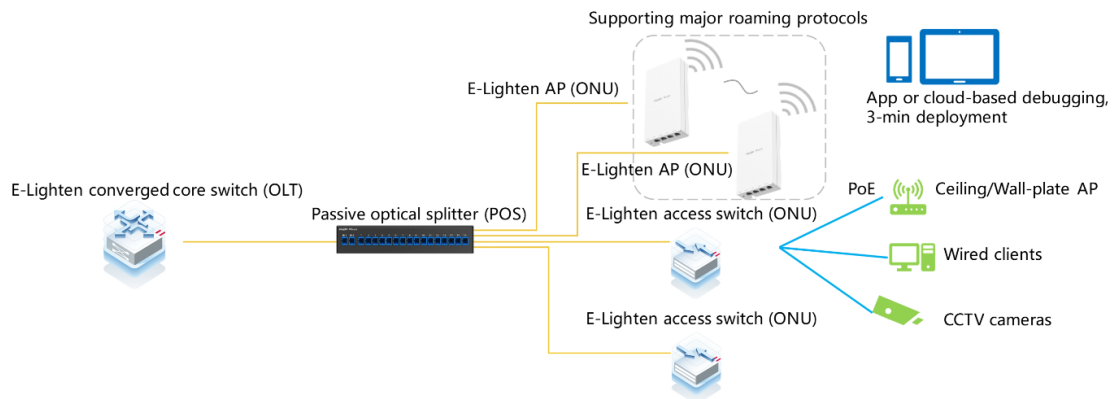
1 Overview

1.1 About the RG-NBF2100S Series Switches

The Reyee e-Lighten Solution is a network product solution based on existing Ethernet technology integrating PON technology and passive optical splitting features. The components include:

- e-Lighten core switch (OLT): As a core switch, it has the Layer 3 data forwarding capability. It provides PON ports that can be connected to e-Lighten access switches and e-Lighten access points (APs) to achieve data interconnection.
- e-Lighten access switch (ONU): As an access device, the e-Lighten access switch is connected to the PON port in the uplink direction. It can send data to the core switch through the passive optical splitter.
- e-Lighten AP (ONU): An e-Lighten AP is connected to the PON port in the uplink direction, and can send wireless users' Internet access data to the core switch through the passive optical splitter.
- Passive optical distribution network (ODN): The ODN, consisting of passive optical splitters, is connected to the core switch in the uplink direction and to e-Lighten access switches or APs in the downlink direction.

Figure 1-1 Topology Diagram of Reyee e-Lighten Solution



The RG-NBF2100S series switches serve as gigabit optical access switches (ONUs) in the Reyee e-Lighten Solution. They apply to diverse small and medium-sized business environments, and can effectively cater to the needs of ELV campus networks, office spaces, hotels, residences, and small to medium-sized enterprises.

Table 1-1 RG-NBF2100S Series Switches

Model	10/100/1000BASE-T Ethernet Ports with Auto-negotiation	SC PON Ports	PoE Ports	Power Module
RG-NBF2100S-8GT1SC-P	8	1	8	DC input
RG-NBF2100S-8GT1SC	8	1	-	DC input

Model	10/100/1000BASE-T Ethernet Ports with Auto-negotiation	SC PON Ports	PoE Ports	Power Module
RG-NBF2100S-16GT1SC-P	16	1	16	AC input

1.2 Package Contents

Note

The package contents are subject to the purchase contract, and actual delivery may vary. Please check the items carefully against the package contents or purchase contract. If you have any questions, please contact your distributor.

1.2.1 Package Contents of the RG-NBF2100S-8GT1SC-P

Table 1-2 Package Contents of the RG-NBF2100S-8GT1SC-P

No.	Item	Quantity
1	RG-NBF2100S-8GT1SC-P	1
2	Accessory bag (4 x rubber pads, 2 x mounting brackets)	1
3	DC power adapter	1
4	User Manual	1
5	Warranty card	1

1.2.2 Package Contents of the RG-NBF2100S-8GT1SC

Table 1-3 Package Contents of the RG-NBF2100S-8GT1SC

No.	Item	Quantity
1	RG-NBF2100S-8GT1SC	1
2	Accessory bag (4 x rubber pads, 2 x mounting brackets)	1
3	DC power adapter	1
4	User Manual	1
5	Warranty card	1

1.2.3 Package Contents of the RG-NBF2100S-16GT1SC-P

Table 1-4 Package Contents of the RG-NBF2100S-16GT1SC-P

No.	Item	Quantity
1	RG-NBF2100S-16GT1SC-P	1
2	Accessory bag (4 x rubber pads, 8 x mounting bracket screws)	1
3	2 x mounting brackets	1
4	AC power cord	1
5	User Manual	1
6	Warranty card	1

1.3 Product Appearance

1.3.1 Appearance of the RG-NBF2100S-8GT1SC-P

Figure 1-2 Front Panel of the RG-NBF2100S-8GT1SC-P

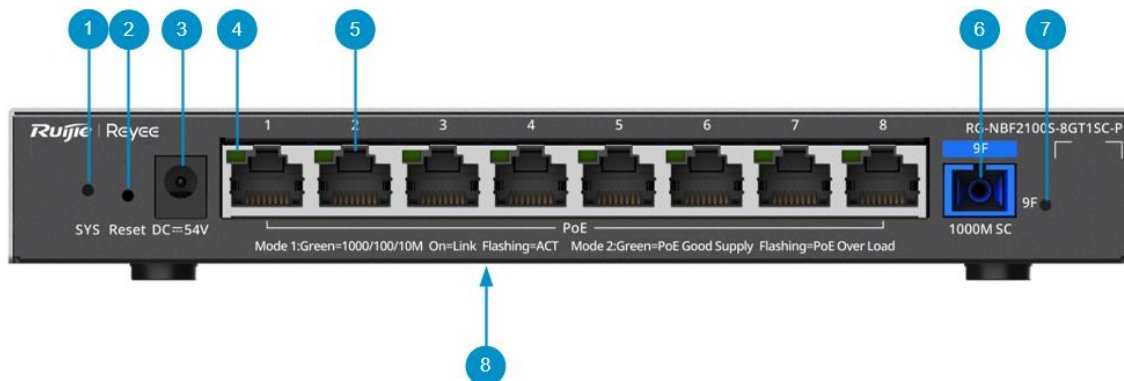


Table 1-5 Components on the Front Panel of the RG-NBF2100S-8GT1SC-P

No.	Item	Description
1	System status LED	<p>Indicates the working status of the system.</p> <ul style="list-style-type: none"> Fast blinking green: 1. The device is starting up. 2. The device is restoring factory settings. 3. The device version is being upgraded. Solid green: The device is working properly. Slow blinking green: The device is not connected to Ruijie Cloud or a loop occurs.

No.	Item	Description
2	Reset button	Used to restart the device or restore factory settings. <ul style="list-style-type: none"> ● Press and hold the button for less than 2 seconds to restart the system. ● Press and hold the button for more than 5 seconds until the system status LED blinks. The system will restore to factory settings and restart. After factory settings are restored, the default management IP address is http://10.44.77.200 (default password: admin).
3	DC power connector	Connected to the DC power adapter to supply power to the device.
4	Link/ACT status LED of Ethernet port	Indicates the working status of the port. <ul style="list-style-type: none"> ● Mode 1 <ul style="list-style-type: none"> ○ Solid green: A link is set up on the port. ○ Blinking green: The port is transmitting and receiving data. ● Mode 2 <ul style="list-style-type: none"> ○ Solid green: The PoE output is normal. ○ Blinking green: The PoE is overloaded.
5	Ethernet port	RJ45 10/100/1000BASE-T Ethernet port with auto-negotiation. The port is used to connect to the Ethernet port of a computer, switch, or AP, and supports IEEE 802.3af/at-compliant PoE.
6	SC PON port	GE SC PON uplink port.
7	SC port status LED	<ul style="list-style-type: none"> ● Slow blinking green: The device is registered successfully. ● Slow blinking red: No optical input or the optical cable is not inserted. ● Slow blinking yellow: The device is registering.
8	Nameplate	Located at the bottom of the front panel.

Figure 1-3 Rear Panel of the RG-NBF2100S-8GT1SC-P

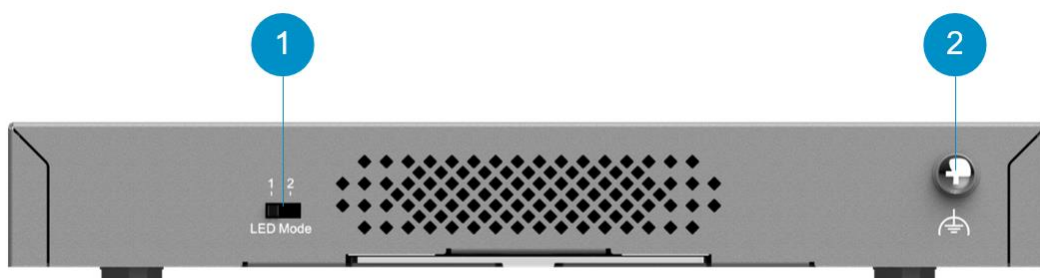


Table 1-6 Components on the Rear Panel of the RG-NBF2100S-8GT1SC-P

No.	Item	Description
1	Switch	Used to change the status LED mode of the ports on the front panel.
2	Grounding stud	Used to secure the grounding lug to connect the chassis to an earth ground.

1.3.2 Appearance of the RG-NBF2100S-8GT1SC

Figure 1-4 Front Panel of the RG-NBF2100S-8GT1SC

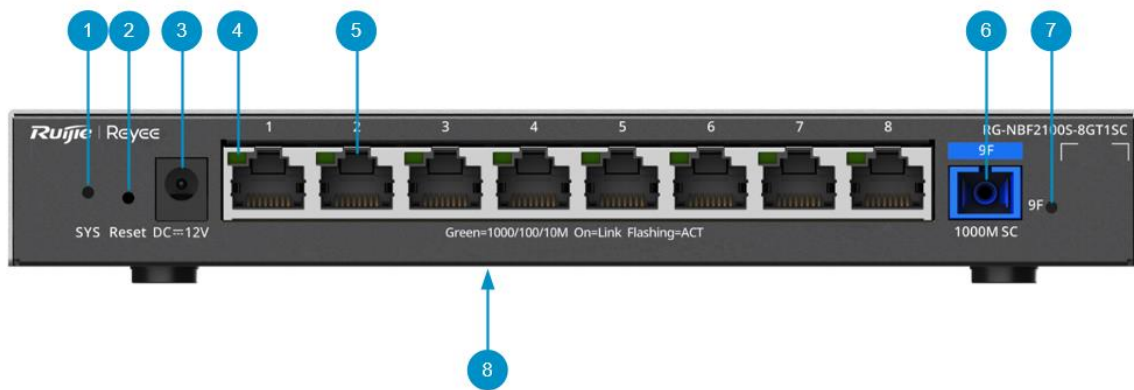


Table 1-7 Components on the Front Panel of the RG-NBF2100S-8GT1SC

No.	Item	Description
1	System status LED	Indicates the working status of the system. <ul style="list-style-type: none"> ● Fast blinking green: 1. The device is starting up. 2. The device is restoring factory settings. 3. The device version is being upgraded. ● Solid green: The device is working properly. ● Slow blinking green: The device is not connected to Ruijie Cloud or a loop occurs.
2	Reset button	Used to restart the device or restore factory settings. <ul style="list-style-type: none"> ● Press and hold the button for less than 2 seconds to restart the system. ● Press and hold the button for more than 5 seconds until the system status LED blinks. The system will restore to factory settings and restart. After factory settings are restored, the default management IP address is http://10.44.77.200 (default password: admin).
3	DC power connector	Connected to the DC power adapter to supply power to the device.
4	Link/ACT status LED of Ethernet port	Indicates the working status of the port. <ul style="list-style-type: none"> ● Solid green: A link is set up on the port. ● Blinking green: The port is transmitting and receiving data.
5	RJ45 Ethernet port	RJ45 10/100/1000BASE-T Ethernet port with auto-negotiation. The port is used to connect to the Ethernet port of a computer, switch, or AP.

No.	Item	Description
6	SC PON port	GE SC PON uplink port.
7	SC port status LED	<ul style="list-style-type: none"> ● Slow blinking green: The device is registered successfully. ● Slow blinking red: No optical input or the optical cable is not inserted. ● Slow blinking yellow: The device is registering.
8	Nameplate	Located at the bottom of the front panel.

Figure 1-5 Rear Panel of the RG-NBF2100S-8GT1SC

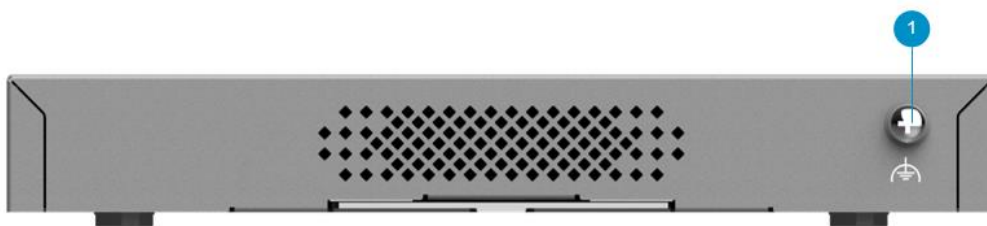


Table 1-8 Components on the Rear Panel of the RG-NBF2100S-8GT1SC

No.	Item	Description
1	Grounding stud	Used to secure the grounding lug to connect the chassis to an earth ground.

1.3.3 Appearance of the RG-NBF2100S-16GT1SC-P

Figure 1-6 Front Panel of the RG-NBF2100S-16GT1SC-P

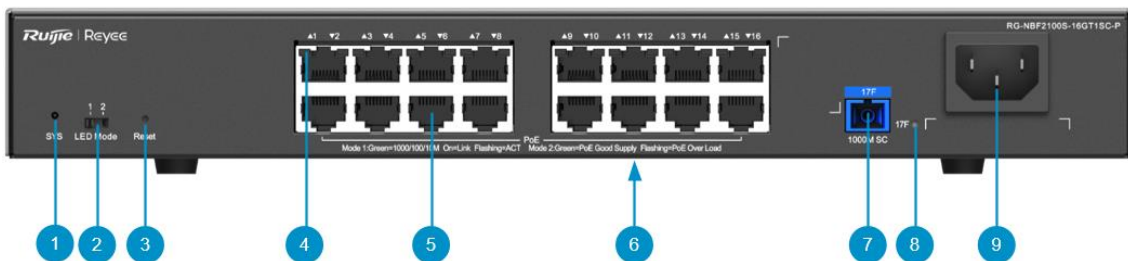


Table 1-9 Components on the Front Panel of the RG-NBF2100S-16GT1SC-P

No.	Item	Description
1	System status LED	<p>Indicates the working status of the system.</p> <ul style="list-style-type: none"> ● Fast blinking green: 1. The device is starting up. 2. The device is restoring factory settings. 3. The device version is being upgraded. ● Solid green: The device is working properly. ● Slow blinking green: The device is not connected to Ruijie Cloud or a loop occurs. ● Off: The switch is not connected to a power supply.
2	Switch	Used to change the status LED mode of the ports on the front panel.
3	Reset button	<p>Used to restart the device or restore factory settings.</p> <ul style="list-style-type: none"> ● Press and hold the button for less than 2 seconds to restart the system. ● Press and hold the button for more than 5 seconds until the system status LED blinks. The system will restore to factory settings and restart. After factory settings are restored, the default management IP address is http://10.44.77.200 (default password: admin).
4	Link/ACT status LED of Ethernet port	<p>Indicates the working status of the port:</p> <ul style="list-style-type: none"> ● Mode 1 <ul style="list-style-type: none"> ○ Solid green: A link is set up on the port. ○ Blinking green: The port is transmitting and receiving data. ○ Off: No link is set up on the port. ● Mode 2 <ul style="list-style-type: none"> ○ Solid green: The PoE output is normal. ○ Blinking green: The PoE is overloaded. ○ Off: PoE power supply is off.
5	Ethernet port	RJ45 10/100/1000BASE-T Ethernet port with auto-negotiation. The port is used to connect to the Ethernet port of a computer, switch, or AP, and supports IEEE 802.3af/at-compliant PoE.
6	Nameplate	Located at the bottom of the device.
7	SC PON port	GE SC PON uplink port.
8	SC port status LED	<ul style="list-style-type: none"> ● Off: No link is set up on the port. ● Slow blinking green: The device is registered successfully. ● Slow blinking yellow: The device is registering. ● Slow blinking red: No optical input or the optical cable is not inserted.
9	Power connector	Connected to an external AC power supply.

Figure 1-7 Rear Panel of the RG-NBF2100S-16GT1SC-P

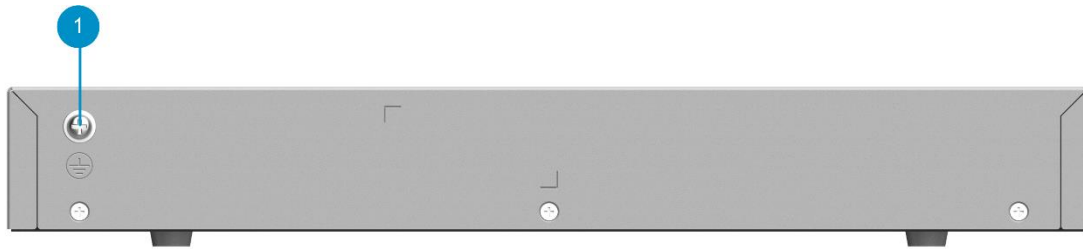


Table 1-10 Components on the Rear Panel of the RG-NBF2100S-16GT1SC-P

No.	Item	Description
1	Grounding stud	Used to secure the grounding lug to connect the chassis to an earth ground.

1.4 Hardware Specifications

1.4.1 Hardware Specifications of the RG-NBF2100S-8GT1SC-P

Table 1-11 Hardware Specifications of the RG-NBF2100S-8GT1SC-P

Model	RG-NBF2100S-8GT1SC-P
Power Range of the ONU's SC Port	<p>The optical power of the ONU's SC port should be within the range of -28 dBm to -8 dBm. If the power is out of this range, the device may have an exception or be damaged.</p> <hr/> <p>⚠ Caution</p> <p>The SC port of the ONU should not be directly connected to the PON port of the OLT. According to the optical power indicator, when short-distance single-mode fibers are used, an online optical attenuator or splitter should be added on the link to prevent device damage.</p> <hr/>
CPU	Built-in 8051 chip, 500 MHz CPU clock speed
Flash Memory	8 MB
SDRAM	N/A
Fixed Service Port	8 x RJ45 10/100/1000BASE-T Ethernet ports with auto-negotiation, 1 x gigabit SC uplink optical port, and 8 x ports supporting IEEE 802.3af/at-compliant PoE


Power Module	<p>Adapter AC input:</p> <p>Rated voltage range: 186 V AC to 240 V AC</p> <p>Maximum voltage range: 186 V AC to 240 V AC</p> <p>Frequency: 50 Hz/60 Hz</p> <p>Rated current: 1.5 A</p> <p>Power cord requirement: 10 A power cord</p>
Adapter DC Power Connector	<p>Inner diameter: 2.1 mm (0.08 in.)</p> <p>Outer diameter: 5.5 mm (0.22 in.)</p> <p>Insertion depth: 10 mm ± 0.3 mm (0.39 in. ± 0.01 in.)</p> <p>Polarity: center positive</p>
Ground-Leakage Current	≤ 3.5 mA
EEE	Supported
PoE	IEEE 802.3af/at-compliant PoE, with a maximum output power of 120 W
Overall Power Consumption	< 130 W
Operating Temperature	0°C to 40°C (32°F to 104°F)
Storage Temperature	-40°C to +70°C (-40°F to +158°F)
Operating Humidity	10% RH to 90% RH (non-condensing)
Storage Humidity	5% RH to 95% RH (non-condensing)
Fan	Fanless
Temperature Alarm	Not supported
Certification	CE
Dimensions (W x D x H)	202 mm x 108 mm x 28 mm (7.95 in. x 4.25 in. x 1.10 in.)
Weight	0.50 kg (1.10 lbs.)

 **Warning**

Operation of this equipment in a residential environment could cause radio interference.

1.4.2 Hardware Specifications of the RG-NBF2100S-8GT1SC

Table 1-12 Hardware Specifications of the RG-NBF2100S-8GT1SC

Model	RG-NBF2100S-8GT1SC
Power Range of the ONU's SC Port	<p>The optical power of the ONU's SC port should be within the range of -28 dBm to -8 dBm. If the power is out of this range, the device may have an exception or be damaged.</p> <hr/> <p> Caution</p> <p>The SC port of the ONU should not be directly connected to the PON port of the OLT. According to the optical power indicator, when short-distance single-mode fibers are used, an online optical attenuator or splitter should be added on the link to prevent device damage.</p> <hr/>
CPU	Built-in 8051 chip, 500 MHz CPU clock speed
Flash Memory	8 MB
SDRAM	N/A
Fixed Service Port	8 x RJ45 10/100/1000BASE-T Ethernet ports with auto-negotiation and 1 x gigabit SC uplink optical port
Power Module	<p>Adapter AC input:</p> <p>Rated voltage range: 100 V AC to 240 V AC</p> <p>Maximum voltage range: 90 V AC to 264 V AC</p> <p>Frequency: 50 Hz/60 Hz</p> <p>Rated current: 1 A</p>
Adapter DC Power Connector	<p>Inner diameter: 2.1 mm (0.08 in.)</p> <p>Outer diameter: 5.5 mm (0.22 in.)</p> <p>Insertion depth: 10 mm \pm 0.3 mm (0.39 in. \pm 0.01 in.)</p> <p>Polarity: center positive</p>
Ground-Leakage Current	≤ 3.5 mA
EEE	Supported
PoE	N/A
Overall Power Consumption	< 12 W
Operating Temperature	0°C to 45°C (32°F to 113°F)
Storage Temperature	-40°C to +70°C (-40°F to +158°F)


Operating Humidity	10% RH to 90% RH (non-condensing)
Storage Humidity	5% RH to 95% RH (non-condensing)
Fan	Fanless
Temperature Alarm	Not supported
Certification	CE
Dimensions (W x D x H)	202 mm x 108 mm x 28 mm (7.95 in. x 4.25 in. x 1.10 in.)
Weight	0.50 kg (1.10 lbs.)

 **Warning**

Operation of this equipment in a residential environment could cause radio interference.

1.4.3 Hardware Specifications of the RG-NBF2100S-16GT1SC-P

Table 1-13 Hardware Specifications of the RG-NBF2100S-16GT1SC-P

Model	RG-NBF2100S-16GT1SC-P
Power Range of the ONU's SC Port	<p>The optical power of the ONU's SC port should be within the range of -28 dBm to -8 dBm. If the power is out of this range, the device may have an exception or be damaged.</p> <hr/> <p> Caution</p> <p>The SC port of the ONU should not be directly connected to the PON port of the OLT. According to the optical power indicator, when short-distance single-mode fibers are used, an online optical attenuator or splitter should be added on the link to prevent device damage.</p> <hr/>
CPU	Built-in 8051 chip, 500 MHz CPU clock speed
Flash Memory	8 MB
SDRAM	N/A
Fixed Service Port	16 x RJ45 10/100/1000BASE-T Ethernet ports with auto-negotiation, 1 x gigabit SC uplink optical port, and 16 x ports supporting IEEE 802.3af/at-compliant PoE

Power Module	<p>Adapter AC input:</p> <p>Rated voltage range: 100 V AC to 240 V AC</p> <p>Maximum voltage range: 90 V AC to 264 V AC</p> <p>Frequency: 50 Hz/60 Hz</p> <p>Rated current: Vout = 54 V (4.7 A), Vout = 12 V (3 A)</p>
Ground-Leakage Current	≤ 3.5 mA
EEE	Supported
PoE	IEEE 802.3af/at-compliant PoE, with a maximum output power of 240 W
Overall Power Consumption	< 290 W
Operating Temperature	0°C to 45°C (32°F to 113°F)
Storage Temperature	-40°C to +70°C (-40°F to +158°F)
Operating Humidity	10% RH to 90% RH (non-condensing)
Storage Humidity	5% RH to 95% RH (non-condensing)
Fan	One fan
Temperature Alarm	Not supported
Certification	CE
Dimensions (W x D x H)	229 mm x 330 mm x 44 mm (9.02 in. x 12.99 in. x 1.73 in.)
Weight	3.7 kg (8.16 lbs., including the package)

 **Warning**

Operation of this equipment in a residential environment could cause radio interference.

2 Preparing for Installation

2.1 Safety Guidelines

Note

- To avoid personal injury or equipment damage, review the safety guidelines in this chapter before you begin the installation.
 - The following safety guidelines may not include all the potentially hazardous situations.
-

2.1.1 General Precautions

- Do not place the equipment in a wet area, and keep it away from liquid. Keep the chassis clean and dust-free.
- Keep the equipment away from heat sources.
- For the equipment that is installed in a cabinet, ensure that the cabinet and power distribution system are properly grounded.
- Do not place the equipment in walking areas.
- During installation and maintenance, do not wear loose clothing, jewelry, or any other objects that may hook onto the chassis.
- Do not place tools and accessories in walking areas.

2.1.2 Chassis-Lifting Guidelines

- Avoid moving the equipment frequently.
- Turn off all power supplies and disconnect all power cords before lifting or moving the equipment.
- Two or more people are required to lift the chassis. Keep balance and prevent personal injuries when lifting or moving the equipment.

2.1.3 Electricity Safety

CAUTION: DOUBLE POLE/NEUTRAL FUSING

Electric shock hazard! The fuse may be in the neutral, and that the mains shall be disconnected to de-energize the phase conductors.

- Observe local regulations and specifications when performing electrical operations. Only qualified personnel should handle these tasks.
- Any improper electrical operation can lead to accidents such as fires or electric shocks, causing severe, or even fatal damage to the human body and the equipment.
- Carefully check the work area for potential hazards, including ungrounded power system, insufficient grounding, and damp or wet ground.
- Direct or indirect touch through a wet object on high-voltage and mains supply can bring a fatal danger.

- Locate the emergency power supply switch in the room before installation. In the case of an accident, cut off the power supply immediately.
- Carefully inspect the equipment and the environment before powering on or off the equipment.
- Select the right leakage protector (also called “leakage current switch” or “leakage current breaker”) for the power supply system. This equipment automatically disconnects the power supply in the event of leakage and the risk of electric shock. A leakage protector should meet the following requirements:
 - The rated leakage action current of each leakage protector is greater than twice of the theoretical maximum leakage current of all the power supplies in the system. For example, if a system is equipped with 16 identical power supplies, and the leakage current of each power supply is equal to or less than 3.5 mA, then the leakage current of the system totals 56 mA. A leakage protector with a rated leakage action current of 30 mA supports no more than four power supplies (that is, action current of the leakage protector/2/Maximum leakage current of each power supply = $30/2/3.5 \approx 4.28$). In this case, 16 power supplies in the system require at least four leakage protectors with a rated action current of 30 mA, with each leakage protector supporting four power supplies. Although the number of power supplies in a system differs in models, the rated leakage action current of each leakage protector divided by two must be greater than the sum of the maximum leakage current of all the power supplies.
 - The rated leakage non-action current of a leakage protector should be 50% of the leakage action current. If the non-action current value is too small, the high sensitivity level can cause the circuit to break, leading to power cutoff and service interruption, even if the leakage current value is normal. For example, if a leakage protector has a rated leakage action current of 30 mA, the rated leakage non-action current should be 15 mA. The leakage protector will not activate unless the leakage current exceeds 15 mA.

 **Caution**

- To ensure personal safety, each leakage protector in the system must have a rated leakage action current equal to or below 30 mA, which is the recognized safety threshold for human body current. If the total leakage current of the system exceeds twice the 30 mA limit, the system must be equipped with two or more leakage protectors to maintain safety.
 - The leakage current values vary with products. For the leakage current value of each product model, see the product technical specifications.
-

2.1.4 Preventing ESD Damage

- Properly ground both the equipment and the installation site.
- Keep the site as dust free as possible.
- Maintain appropriate humidity conditions.
- Before installing or maintaining the equipment, wear an anti-ESD wrist strap and make sure that it is properly grounded.
- Avoid contact between the printed circuit boards and clothing. The anti-ESD wrist strap only protects the printed circuit boards from ESD voltages on the body. ESD voltages on clothing can still cause damage.

2.1.5 Laser Safety

An equipment with an optical port usually supports multiple types of optical transceivers, all of which are Class I laser products. Pay attention to the following during the use of optical transceivers:

- When an optical transceiver is in operation, ensure that its port is connected to an optical fiber or covered by

a dust cap to keep out dust and prevent it from burning your eyes.

- When an optical transceiver is in operation, do not look into its port after removing the optical fiber. Doing so may result in eye injury.

⚠ Caution

Do not approach or look directly into any optical port under any circumstances. This may cause permanent damage to your eyes.

Figure 2-1 Laser Product Warning



2.2 Site Requirements

To ensure the normal operation and prolonged service life of the equipment, it is essential to install it indoors in a location that meets the following requirements.

2.2.1 Floor Loading

Assess the combined weight of the equipment and its accessories, including the cabinet, chassis, and power supply, and verify that the installation site meets the necessary specifications.

2.2.2 Airflow

To ensure that the equipment works properly in the specified environment, a minimum clearance of 100 mm (3.94 in.) must be maintained around the equipment to ensure proper ventilation. Manage the Ethernet cables and power cords using cable ties or cable management brackets to avoid blocking air intakes. You are advised to dust the equipment at an interval of three months to avoid blocking the ventilation openings.

2.2.3 Space

Ensure that indoor pathways are at least 0.8m (31.50 in.) wide to allow for proper chassis handling and module swapping.

Maintain a minimum clearance of 0.4m (15.75 in.) around the equipment for heat dissipation and equipment maintenance.

2.2.4 Temperature and Humidity

For optimal equipment performance and extended service life, it is essential to maintain ambient temperature and humidity conditions. Prolonged exposure to excessively high or low temperature and humidity can potentially cause damage to the equipment.

- When exposed to high relative humidity, insulating materials may exhibit poor insulation capabilities, increasing the risk of electrical leakage. Furthermore, high humidity can cause mechanical changes in materials and corrosion of metallic components.
- When exposed to low relative humidity, the insulating strip may dry out and shrink, increasing the risk of static

electricity generation. This static electricity can pose a danger to the circuits inside the equipment.

- In a dry environment, static electricity is prone to occur and damage the internal circuits of the equipment.
- High temperature environments can be detrimental to the equipment, leading to reduced performance and a shorter service life. Prolonged exposure to elevated temperatures can expedite the equipment's aging process.

Note

The ambient temperature and humidity of the equipment are measured 1.5 m (59.06 in.) above the floor and 0.4 m (15.75 in.) before the equipment rack when there is no protective plate in front or at the back of the rack.

2.2.5 Cleanliness

Dust poses a major threat to the running of the equipment. The buildup of dust on the equipment can result in static electricity, causing poor contact between the metallic joints. Dust buildup is more likely to occur in environments with low relative humidity, which not only impacts the service life of the equipment but also increases the likelihood of communication failure. The following table shows the specifications for dust concentration and particle size in the equipment room.

Table 2-1 Requirements for Dust

Particle Size	Unit	Concentration
≥ 0.5 μm	Particles/m ³	≤ 3.5×10 ⁶
≥ 5 μm	Particles/m ³	≤ 3.5×10 ⁴

Apart from dust, the salt, acid, and sulfide in the air of the machine room must also meet strict requirements. These harmful substances will accelerate metal corrosion and component aging. Therefore, the machine room should be properly protected against the intrusion of harmful gases, such as sulfur dioxide, hydrogen sulfide, nitrogen dioxide, and chlorine gas. The following table lists limits for harmful gases.

Table 2-2 Requirements for Gases

Gas	Average (mg/m ³)	Maximum (mg/m ³)
Sulfur dioxide (SO ₂)	0.3	1.0
Hydrogen sulfide (H ₂ S)	0.1	0.5
Nitrogen dioxide (NO ₂)	0.5	1.0
Chlorine gas (Cl ₂)	0.1	0.3

Note


"Average" indicates the typical level of exposure over a one-week period. "Maximum" refers to the highest allowable exposure level within a week, with this level being sustainable for no more than 30 minutes per day.

2.2.6 Grounding

A proper grounding system is crucial for ensuring stable and reliable operation of the equipment, as well as preventing lightning strikes and interference. To ensure proper grounding, carefully check the grounding conditions at the installation site according to the grounding specifications, and complete grounding properly based on the actual situation.

- Safety Grounding

Ensure that the installation site and power distribution system are securely grounded if the equipment uses the AC power supply. Failure to do so may result in an increased risk of electric shock, particularly when the insulation resistance between the power module and the chassis decreases.

 **Caution**

- Adopt grounding protection connections in buildings so that the equipment can be connected to the protective grounding system.
 - Verify that the AC socket is reliably connected to the protective grounding system of the building. If not, a protective grounding wire should be used to connect the protective grounding lug of the AC socket to the protective grounding system of the building.
 - The cross-sectional area of the protective grounding wire should be at least 0.75 mm² (18 AWG).
-

- Lightning Grounding

The lightning protection system of facilities is standalone, and is composed of a lightning rod, a down conductor, and a connector connected to the grounding system. The grounding system is usually used for power reference grounding and safety grounding of the installation site. Lightning grounding is required only for facilities and is not required for the equipment.

- EMC Grounding

Grounding required for electromagnetic compatibility includes shielded grounding, filter grounding, noise and interference suppression, and level reference, which contribute to the overall grounding requirements. The grounding resistance should be smaller than 1 ohm, and the grounding terminals of the rack should be grounded before the running of the equipment.

2.2.7 Anti-Electromagnetic Interference

- Take effective measures to prevent interference from power grid to the power supply system.
- Keep the equipment away from the grounding system or lightning protection grounding system of the power facility.
- Keep the equipment far away from high-frequency current equipment such as high-power radio transmitting stations and radar launchers.
- Take electromagnetic shielding measures when necessary.

2.2.8 Surge Protection

- Ensure that the neutral point of the AC power socket is in good contact with the ground.
- Install a power arrester in front of the power input end to enhance surge protection for the power supply.
- When an AC power cord is introduced from outdoors and directly connected to the power port of the equipment, the AC power port must be connected to an external lightning protection power strip to protect the equipment against lightning strokes. Connect the mains supply AC power cord to the lightning protection

power strip, and then connect the equipment to the lightning protection power strip. This prevents high-voltage lightning from directly passing through the equipment over the mains supply AC power cord.

Note

- The lightning protection power strip is not delivered with the equipment. Purchase it as required.
 - For details on how to use the lightning protection power strip, see the related user guide.
-

2.2.9 EMI

All interference sources, either from outside or inside of the equipment or application system, affect the equipment by capacitive coupling, inductive coupling, or electromagnetic waves. Electromagnetic interference (EMI) occurs due to electromagnetic radiation or conduction, depending on the transmission path. When the energy, often RF energy, from a component arrives at a sensitive component through the space, the energy is known as radiated interference. The interference source can be either a part of the interfered system or a completely electrically isolated unit. Conduction interference occurs when interference is transferred from one unit to another unit through cables, which are usually electromagnetic wires or signal cables connected between the source and the sensitive component. Conduction interference often affects the power supply of the equipment, but can be controlled by a filter. Radiated interference may affect any signal path in the equipment, and is difficult to shield.

- Take interference prevention measures for the power supply system.
- Keep the equipment away from the grounding system or lightning protection grounding system of the power facility.
- Keep the equipment far away from high-frequency current equipment such as high-power radio transmitting stations and radar launchers.
- Take electromagnetic shielding measures when necessary.

2.2.10 Installation Site

Regardless of whether the equipment is installed in a rack, on a workbench or on a wall, the following conditions must be met:

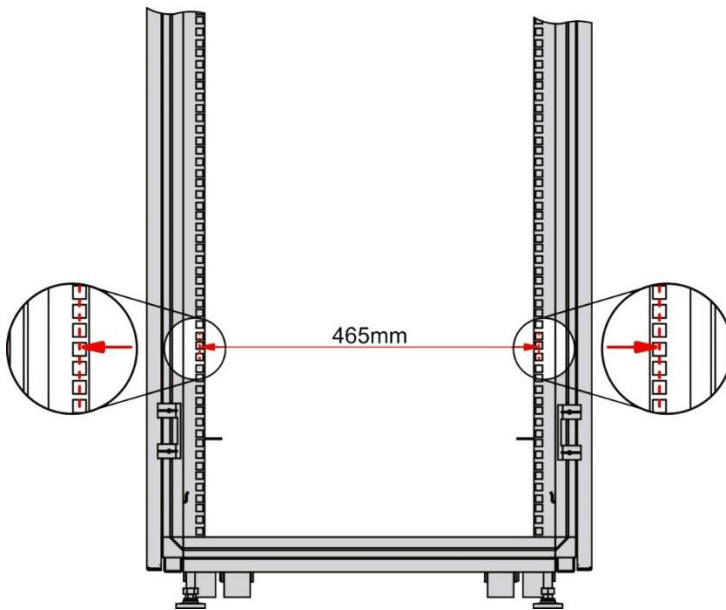
- Maintain a proper clearance around air vents for heat dissipation.
- The equipment is equipped with fans to draw air from front and left and right sides to rear. Maintain a minimum clearance of 150 mm (5.91 in.) around the ventilation openings for heat dissipation. Install the equipment in a standard 19-inch rack, or place it on a clean workbench. In hot areas, air-conditioning is recommended.
- The installation site has good cooling and ventilation.
- The installation site is sturdy enough to support the weight of the equipment and its accessories.
- The installation site is properly grounded.

2.3 Rack Requirements

If you plan to install the equipment in a rack, ensure that the rack meets the following conditions.

- (1) Use a four-post 19-inch cabinet.
- (2) The left and right square-hole rack posts are 465 mm (18.31 in.) apart.

Figure 2-2 19-Inch Rack



- (3) The square-hole rack post is at least 180 mm (7.09 in.) from the front door, and the front door is at most 25 mm (0.98 in.) thick. This ensures an available clearance of at least 155 mm (6.10 in.). The rack depth (distance between front and rear doors) is at least 1000 mm (39.37 in.).
- (4) The guide rails can bear the weight of the equipment and its accessories.
- (5) The cabinet has a reliable grounding terminal for the chassis to connect to earth ground.
- (6) The cabinet has a good ventilation system. The open area of front and rear doors is greater than 50%.

2.4 Tools

Table 2-3 Tools

Common Tools	Phillips screwdriver, power cords, Ethernet cables, cage nuts, diagonal pliers, and cable ties
Special Tools	Anti-ESD gloves, wire stripper, crimping plier, RJ45 crimping plier, and wire cutter
Meters	Multimeter

Note

The equipment is delivered without a toolkit. Prepare the preceding tools by yourself.

3 Installing the Switch

⚠ Caution

Before installing the equipment, ensure that guidelines and requirements in Chapter 2 have been met.

3.1 Precautions for Installation

Pay attention to the following points during installation:

- Connect the power cords of different colors to the corresponding cable terminals.
- Ensure that the connector of the power cord is properly seated in the power connector of the switch.
- Do not place any objects above the switch.
- Maintain a minimum clearance of 100 mm (3.94 in.) around the switch to ensure proper airflow. Do not stack switches.
- Keep the switch far away from high-frequency current equipment such as high-power radio transmitting stations and radar launchers. Take electromagnetic shielding measures when necessary, such as electromagnetic shielding for port cables.
- Keep Ethernet cables with a distance of 100 m (328.08 feet) indoors. Take surge protection measures if they need to be routed outdoors.

3.2 Installation Procedure

3.2.1 Installing a Switch in a Rack

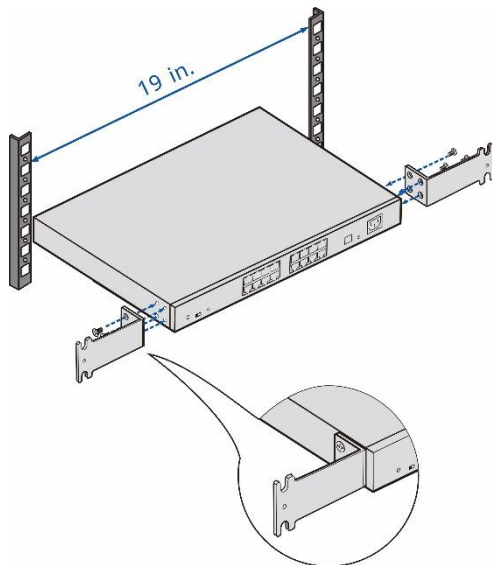
⚠ Caution

Only the RG-NBF2100S-16GT1SC-P can be installed in a rack.

The size of the RG-NBF2100S-16GT1SC-P complies with the EIA standard and can be installed in a standard 19-inch rack.

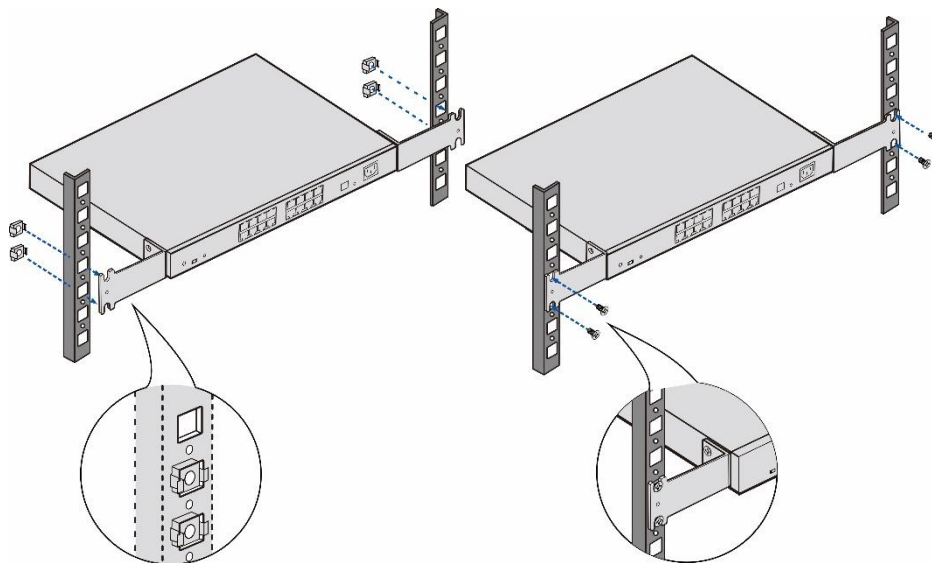
- (1) Use eight M4 x 8 mm screws to fix the mounting brackets to the left and right sides of the switch.

Figure 3-1 Installing Mounting Brackets on the RG-NBF2100S-16GT1SC-P



- (2) Place the switch horizontally in the rack and secure it to the rack using the M6 screws and matching cage nuts, which need to be prepared by yourself.

Figure 3-2 Securing the RG-NBF2100S-16GT1SC-P to the Square Holes of the Rack



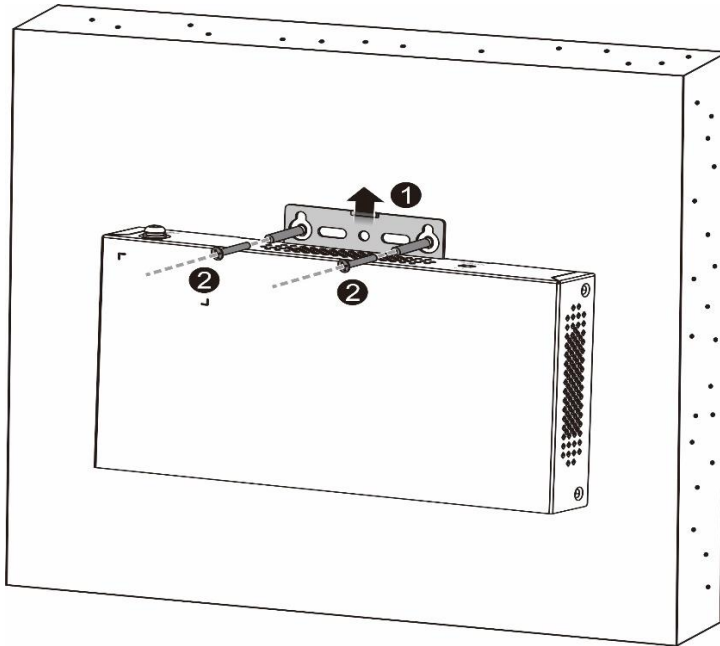
3.2.2 Mounting a Switch on the Wall

⚠ Caution

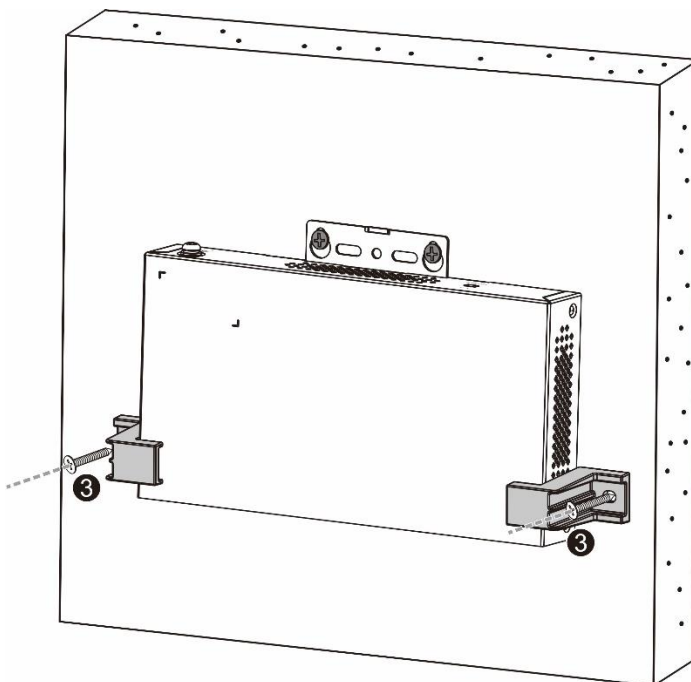
- Only RG-NBF2100S series 8-port switches support the wall-mounting mode.
- Ensure that the length of the M4 screws prepared by yourself is longer than 10 mm (0.39 in.).
- If a switch is mounted on a wall, it must be installed in a position that restricts mobility.

- **Mounting an RG-NBF2100S Series 8-Port Switch on the Wall**

- (1) Pull out the mounting plate of the switch, and use two M4 screws (which need to be prepared by yourself) to secure the switch to the wall.



- (2) Use the mounting brackets and two M4 screws (which need to be prepared by yourself) to secure the switch to the wall.



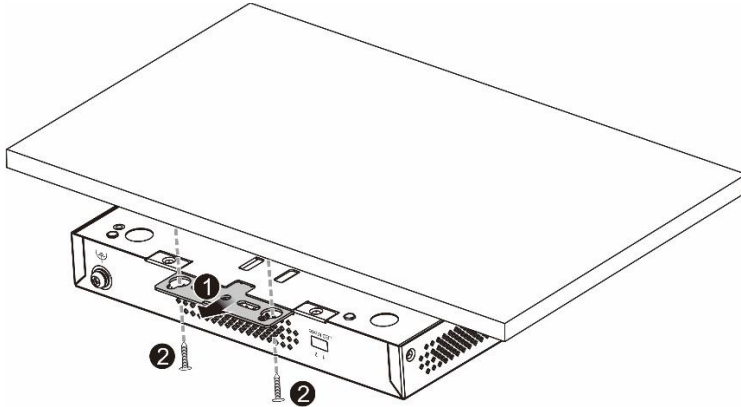
3.2.3 Mounting a Switch on the Ceiling

⚠ Caution

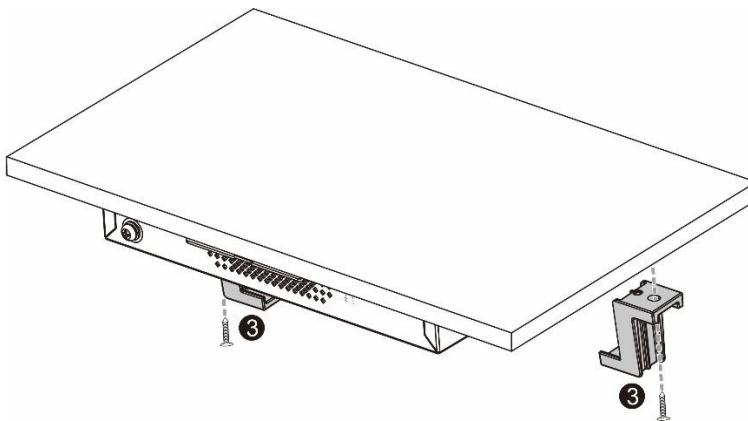
- Only RG-NBF2100S series 8-port switches support the ceiling-mounting mode.
 - If a switch is installed on a ceiling, it must be installed in a position that restricts mobility.
-

- Before mounting a switch on a ceiling, ensure that the ceiling can support the weight of the switch.
- Ensure that the length of the M4 screws prepared by yourself is longer than 10 mm (0.39 in.).

- (1) Pull out the mounting plate of the switch, and use two M4 screws (which need to be prepared by yourself) to secure the switch to the ceiling.



- (2) Use the mounting brackets and two M4 screws (which need to be prepared by yourself) to secure the switch to the ceiling.



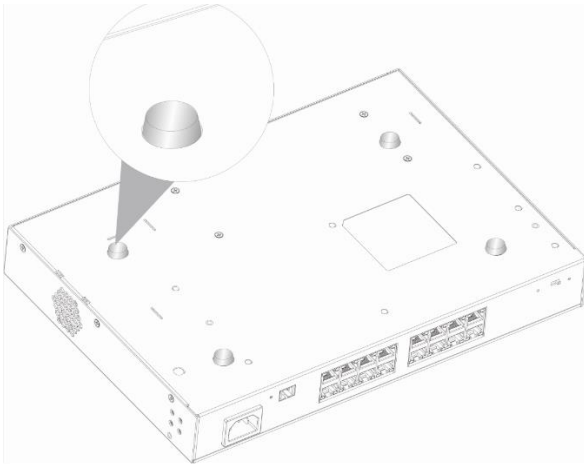
3.2.4 Installing a Switch on a Desktop

Note

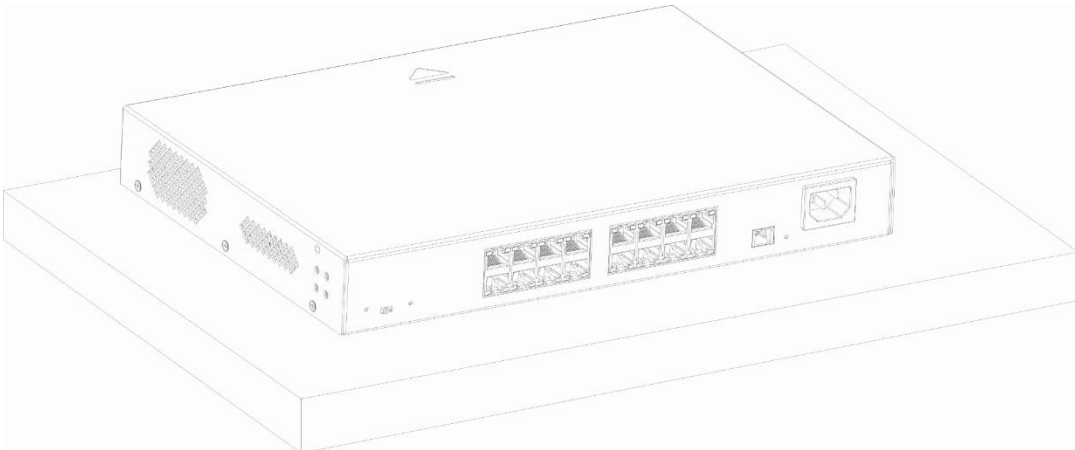
If a switch is installed on a desktop, it must be installed in a location where mobility is restricted.

In most cases, users do not have the conditions for installing a switch in a rack, on a wall, or on a ceiling. In this case, the switch can be placed on a clean workbench. The desktop installation steps of the RG-NBF2100S series switches are the same. The following uses RG-NBF2100S-16GT1SC-P as an example to describe the desktop installation procedure.

- (1) Paste the four rubber pads provided in the package to the four corners of the bottom of the device.



- (2) Place the switch on the workbench and ensure adequate airflow around the switch.



3.3 Connecting the Grounding Wire

Warning

- To avoid personal injury and device damage, connect the switch to an earth ground properly.
 - The resistance between the switch chassis and the ground must be less than 1 Ω .
 - The O&M personnel should check whether the AC outlet is properly connected to the protective ground of the building. If not, the O&M personnel should use a protective earth conductor from the AC outlet protective earth terminal to the building protective earth.
 - The power socket should be installed near the switch and easily accessible.
 - During device installation, connect the grounding wire first and disconnect it last.
 - The cross-sectional area of a protective grounding wire should be at least 2.5 mm² (12 AWG).
-

A proper grounding system is crucial for ensuring stable and reliable operation, as well as preventing lightning strikes and interference.

- The grounding wire must be a good conductor with a cross-sectional area determined by the maximum current load.
- Do not use bare wire.
- To guarantee personal and device safety, properly ground the switch. The resistance between the switch

chassis and the ground must be less than 1 Ω .

Procedure:

- (1) Remove the ground screw on the rear panel of the device.
- (2) Use the removed ground screw to secure one end of the grounding wire to the chassis. Similarly, connect the other end of the grounding wire to the rack grounding cable or the equipment room grounding bar.

3.4 Connecting the Power Cord

Caution

- Use the power adapter and power cord delivered with the device to avoid accidents.
 - The O&M personnel should check whether the AC outlet is properly connected to the protective ground of the building. If not, the O&M personnel should use a protective earth conductor from the AC outlet protective earth terminal to the building protective earth.
 - During device installation, connect the grounding wire first and disconnect it last.
 - The power socket should be installed near the switch and easily accessible.
-

3.4.1 Connecting the Power Cord of the Power Adapter

All RG-NBF2100S series models use the power cord of the power adapter except for the RG-NBF2100S-16GT1SC-P.

Connect the power cord as follows:

- (1) Insert the round end of the power adapter into the DC power connector of the device, and then plug the other end into the AC power socket.
- (2) Check whether the system status LED on the front panel is on. If so, the power supply is connected correctly. Otherwise, check the power supply connection.

3.4.2 Connecting the AC Power Cord

Only the RG-NBF2100S-16GT1SC-P uses the AC power cord.

Connect the power cord as follows:

- (1) Connect the AC power cord to the power connector of the device, and then plug the other end into the AC power socket.
- (2) Check whether the system status LED on the front panel is on. If so, the power supply is connected correctly. Otherwise, check the power supply connection.

3.5 Verifying Installation

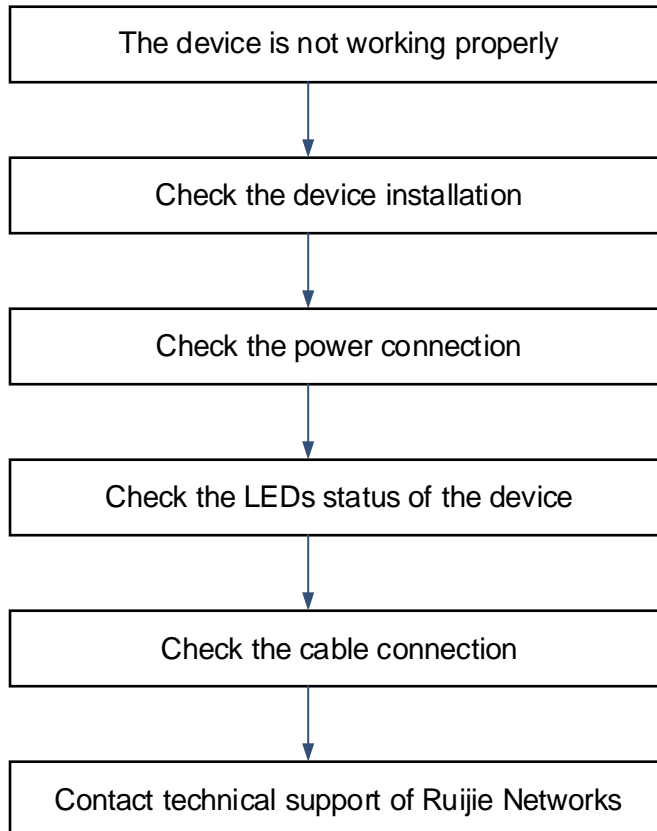
- Check whether the device is securely installed.
- The power cord meets the requirements.
- The rack is properly grounded.
- The switch is correctly connected to the terminal or other equipment.
- The power cord is long enough to avoid over-extension.

4 Log in to the Web UI

- (1) Connect the PC to the Ethernet port of the device using a cable.
- (2) Configure your PC with an IP address on the network of 10.44.77.XXX (Range of XXX: 1–255, excluding 200).
- (3) Open a browser, enter 10.44.77.200 in the address bar of the browser, and press **Enter**. (The default password is **admin** when you log in to the device for the first time. To ensure security, you are advised to change the password after login, and update the password regularly.)
- (4) Perform device commissioning based on service requirements.

5 Troubleshooting

5.1 Troubleshooting Flowchart



5.2 Common Faults

5.2.1 Forgot or Lost the System Login Password

Press and hold the reset button for more than 5 seconds to restore factory settings and reset the system login password.

5.2.2 System Status LED Is Off for a Long Time

Power off all power supplies. Check whether the cables of the rack are correctly connected, whether the power socket of the rack is normal, whether the connection between the power socket of the rack and the power cord is loose, and whether the connection of the power cord of the device is loose.

5.2.3 Only Partial PoE Ports Can Supply Power

PoE ports can be connected to PoE-powered devices. If some ports supply power and some ports do not, check whether the faulty ports are manually disabled by software and whether the power provided by the PoE power supply is insufficient. If the power is insufficient, only the ports with higher default priorities are powered on.

Fault Symptom	Possible Cause	Solution
The login password cannot be retrieved.	The login password is forgotten after being configured.	Press and hold the reset button for more than 5 seconds to reset your username and password.
The system status LED is off after the switch is powered on.	No power is supplied to the switch or the power cord is loose.	Check whether the power socket in the equipment room is normal and whether the power cord connected to the switch is loose.
An RJ45 port is disconnected or a frame sending/receiving error occurs.	<ul style="list-style-type: none"> ● The twisted pair is not connected properly. ● The cable length exceeds 100 m (328.08 feet). ● The port has special configuration and does not use the same working mode as the connected switch. 	<ul style="list-style-type: none"> ● Replace the twisted pair. ● Use optical cables or connect to an intermediate switch for relay. ● Check port configuration and ensure that the port works in the same mode as the connected switch.
Only partial PoE ports can supply power.	The PoE port is manually disabled or the output power of the PoE power supply is limited.	Enable the PoE port or remove the output power limit of the PoE power supply

6 Appendix

6.1 Ports, Connectors, and Media

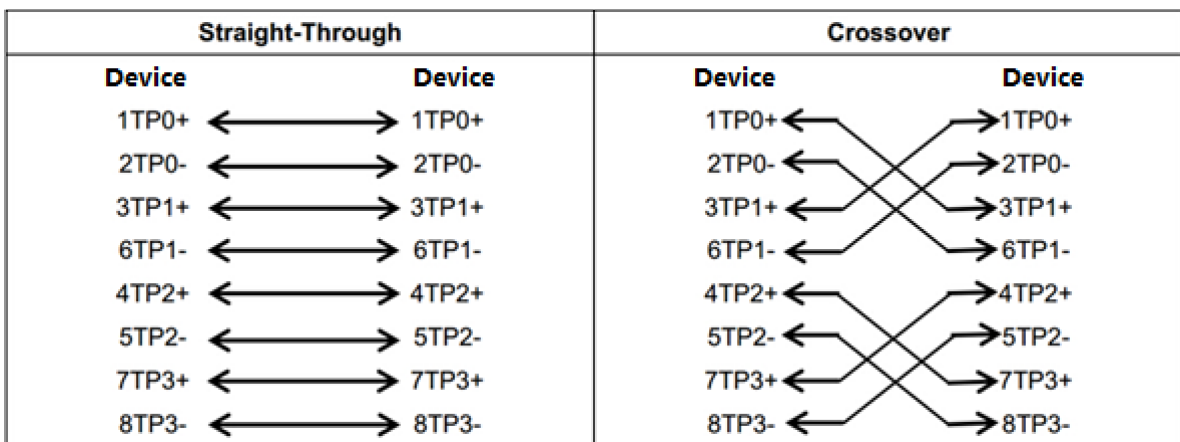
6.1.1 1000BASE-T/100BASE-TX/10BASE-T Ports

1000BASE-T/100BASE-TX/10BASE-T ports are Ethernet ports with auto-negotiation of three speeds: 10 Mbps, 100 Mbps, and 1000 Mbps. They supports auto MDI/MDIX Crossover, and use RJ 45 connectors.

Compliant with the IEEE 802.3ab standard, a 1000BASE-T port requires 100-ohm Category 5 or 5e unshielded twisted pair (UTP) or shielded twisted pair (STP) (recommended) cables, and supports a maximum distance of 100 meters (328 feet).

A 1000BASE-T port requires all four pairs of wires to be connected for data transmission. [Figure 6-1](#) shows the four pairs of wires for the 1000BASE-T port.

Figure 6-1 1000BASE-T Twisted Pair Connections



100BASE-TX/10BASE-T ports can be interconnected using cables of the preceding specifications. In addition, a 10BASE-T port can be connected using 100-ohm Category 3, Category 4, and Category 5 cables, while a 100BASE-TX port can be connected using 100-ohm Category 5 cables, and supports a maximum distance of 100 meters (328 feet). [Table 6-1](#) shows 100BASE-TX/10BASE-T pin assignments.

Table 6-1 100BASE-TX/10BASE-T Pin Assignments

Pin	Socket	Plug
1	Input Receive Data+	Output Transmit Data+
2	Input Receive Data-	Output Transmit Data-
3	Output Transmit Data+	Input Receive Data+
6	Output Transmit Data-	Input Receive Data-
4, 5, 7, 8	Not Used	Not Used

Figure 6-2 shows the connection of straight-through and crossover cables for 100BASE-TX/10BASE-T ports.

Figure 6-2 100BASE-TX/10BASE-T Twisted Pair Connections

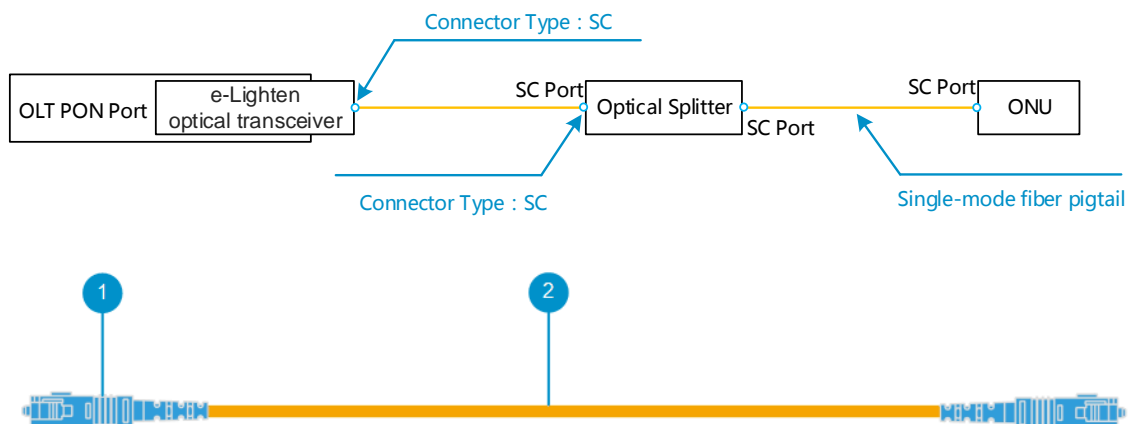
Straight-Through		Crossover	
Device	Adapter	Device	Device
1 IRD+	1 OTD+	1 IRD+	1 IRD+
2 IRD-	2 OTD-	2 IRD-	2 IRD-
3 OTD+	3 IRD+	3 OTD+	3 OTD+
6 OTD-	6 IRD-	6 OTD-	6 OTD-

6.1.2 PON Ports and SC Ports

Figure 6-3 shows the PON ports and SC ports on equipment in Ruijie Reyee e-Lighten Optical Solution.

- PON ports on the OLT require e-Lighten optical transceivers with SC connectors, which are connected to an optical splitter using single-mode pigtails.
- SC ports on optical splitters and ONUs use SC connectors, and are interconnected using single-mode pigtails.

Figure 6-3 PON Port and SC Port Connections



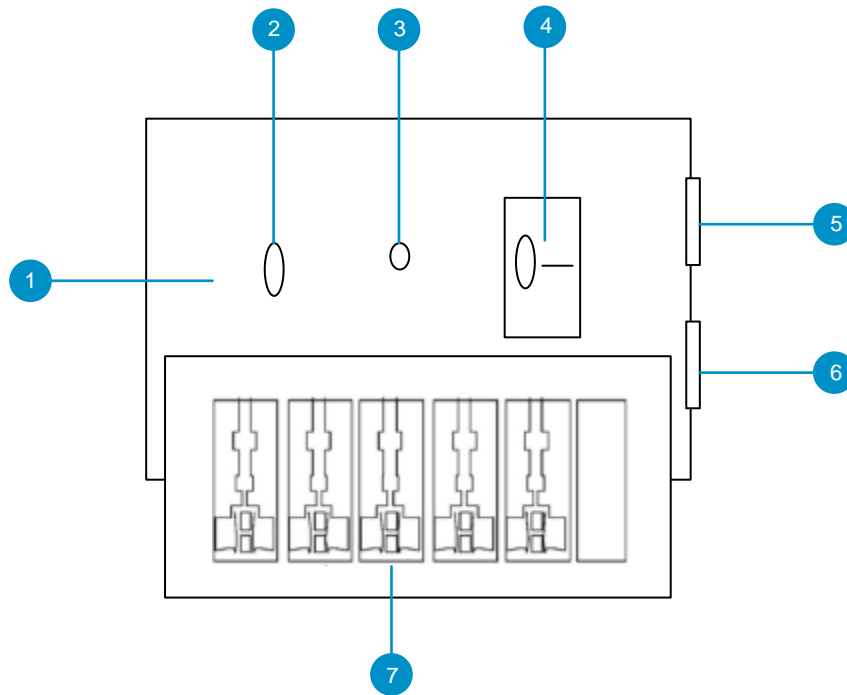
No	Description
1	SC connector
2	Single-mode pigtail

6.2 Surge Protection

6.2.1 Installing an AC Power Lightning Arrester

When an AC power cord from outdoors is directly plugged into the power port of the equipment, the AC power connector must be connected to an external surge protector power strip to protect the equipment against lightning strikes. The surge protector power strip can be fixed on the rack, workbench, or wall in the equipment room by using cable ties and screws. AC power enters the equipment through the surge protector power strip.

Figure 6-4 Installing an AC Power Lightning Arrester



No.	Description
1	Installed electronic circuit board
2	Normally running indicator: When the indicator is green, the circuit is working properly. Otherwise, the protective circuit is damaged.
3	Grounding and polarity detection indicator: If the indicator is red, cable connection is incorrect (the ground cable is not connected, or the N and L lines are reversely connected). Check your power supply line.
4	Power switch
5	IEC standard socket, which is connected to the power supply in the equipment room through the power cable
6	Overload auto-protector, which can be reset manually
7	Multi-purpose sockets (connected to the power supply of the switch)

Note

The lightning arrester is not delivered with the equipment. Please purchase it based on actual requirements.

Precautions:

- Make sure that the PE terminal of the power arrester is well grounded.
- After the AC power plug of the equipment is connected to the socket of the power arrester (lightning

resistance socket), the surge protection function is implemented only if the RUN indicator is green and the ALARM indicator is OFF.

- If the indicator on the power arrester is red, check whether it is caused by poor grounding connection or by the reversed connection of the Null and Live lines. The detection method is as follows: Use a multimeter to measure the polarity of the power socket for the arrester when the indicator is red. If the N line is on the left and the L line is on the right (facing the socket), the arrester's PE terminal is not grounded. If not, the polarity of the arrester power cord should be reversed. In this case, you should open the power arrester and rectify the polarity of the connection. If the indicator is still red, the arrester's PE terminal is not grounded.

6.2.2 Installing an Ethernet Port Lightning Arrester

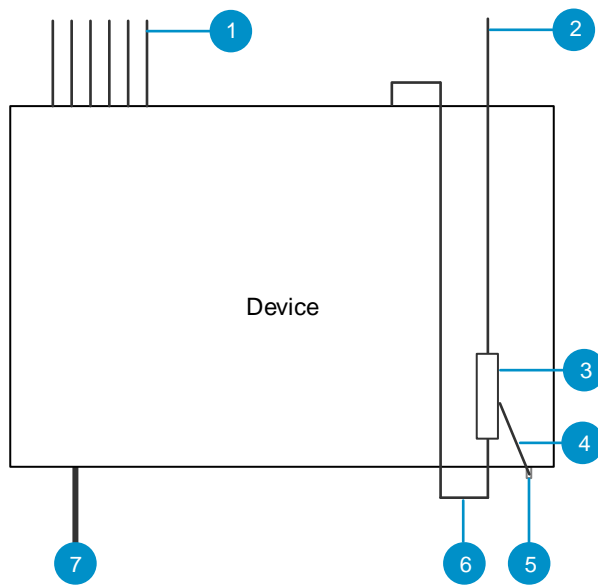
Connect an Ethernet port arrester to the equipment to prevent the damage by lightning before connecting an outdoor network cable to the device.

Tools: Phillips screwdrivers or flat-head screwdriver, multimeter, and diagonal pliers

Procedure:

- (1) Tear one side of the protective paper for the double-sided adhesive tape and paste the tape to the enclosure of the Ethernet port arrester.
- (2) Tear the other side of the protective paper for the double-sided adhesive tape and paste the Ethernet port arrester to the enclosure. The paste position for the Ethernet port arrester should be as close to the grounding terminal of the equipment as possible.
- (3) According to the distance between the equipment grounding terminal and the Ethernet port arrester, cut the grounding cable for the Ethernet port arrester and firmly crimp the grounding cable to the grounding terminal of the equipment.
- (4) Use a multimeter to check whether the grounding cable for the arrester is in good contact with the grounding terminal and the enclosure of the equipment.
- (5) Connect the arrester by using an adapter cable (note that the external network cable is connected to the IN end, while the adapter cable connected to the equipment is connected to the OUT end) and check whether the service module LED is normal.
- (6) Use a nylon cable tie to bind the power cords.

Figure 6-5 Installing an Ethernet Port Lightning Arrester



No.	Description
1	Ethernet cable for indoor connection
2	Ethernet cable connected to the outdoor
3	RJ45 port arrester (pasted on the enclosure)
4	Ground cable of the arrester
5	Grounding lug of the equipment
6	RJ45 port adapter cable
7	Power input

Note

- The Ethernet port arrester is only for Ethernet ports with an RJ45 connector.
- The Ethernet port arrester is not delivered with the equipment. Please purchase it based on actual requirements. The Ethernet port arrester user manual contains technical parameters and maintenance and installation instructions for the Ethernet port arrester. Carefully read this manual before installation.
- Pay attention to the following situations during the installation to avoid influencing the performance of the Ethernet port arrester:
 - Reversed installation direction of the arrester. Connect the external network cable to the “IN” end and connect the Ethernet port of the equipment to the “OUT” end.
 - Poor grounding of the arrester. The grounding cable of the arrester should be as short as possible to ensure that it is in good contact with the grounding terminal of the equipment. Use a multimeter to confirm the contact condition after grounding.
 - Incomplete arrester installation. If there is more than one port connected to external power cords, arresters

need to be installed on all connection ports for the purpose of surge protection.

6.3 Recommended Cabling

When the device is installed in a standard 19-inch rack, route the cables through the cable management brackets. Top cabling or bottom cabling is adopted according to the actual situation in the equipment room. All conversion connectors should be placed at the bottom of the rack instead of outside the rack that is easily accessible. Power cords are routed beside the cabinet, and top cabling or bottom cabling is adopted according to the actual situation in the equipment room, such as the locations of the DC power distribution box, AC power socket, or surge protection box.

6.3.1 Requirements for the Minimum Bend Radius of an Ethernet Cable

- The bend radius of a fixed power cord, Ethernet cable, or flat cable should be over five times greater than their respective diameters. The bend radius of these cables that are often bent or plugged should be over seven times greater than their respective diameters.
- The bend radius of a fixed common coaxial cable should be over seven times greater than its diameter. The bend radius of the common coaxial cable that is often bent or plugged should be over 10 times greater than its diameter.
- The bend radius of a fixed high-speed cable (such as SFP+ cable) should be over five times greater than its diameter. The bend radius of the fixed high-speed cable that is often bent or plugged should be over 10 times greater than its diameter.

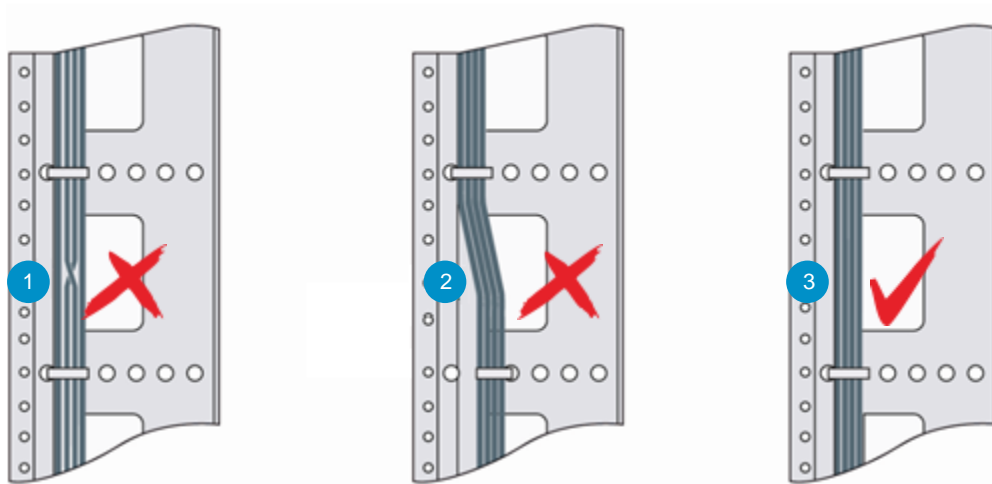
6.3.2 Requirement for the Minimum Bend Radius of an Optical Cable

- When an optical cable is coiled, the diameter of a fiber tray should be over 25 times greater than the diameter of the optical cable.
- When an optical cable is moved, the bend radius of the optical cable should be over 20 times greater than the diameter of the optical cable.
- When an optical cable is laid, the bend radius of the optical cable should be over 10 times greater than the diameter of the optical cable.

6.3.3 Precautions for Bundling up Cables

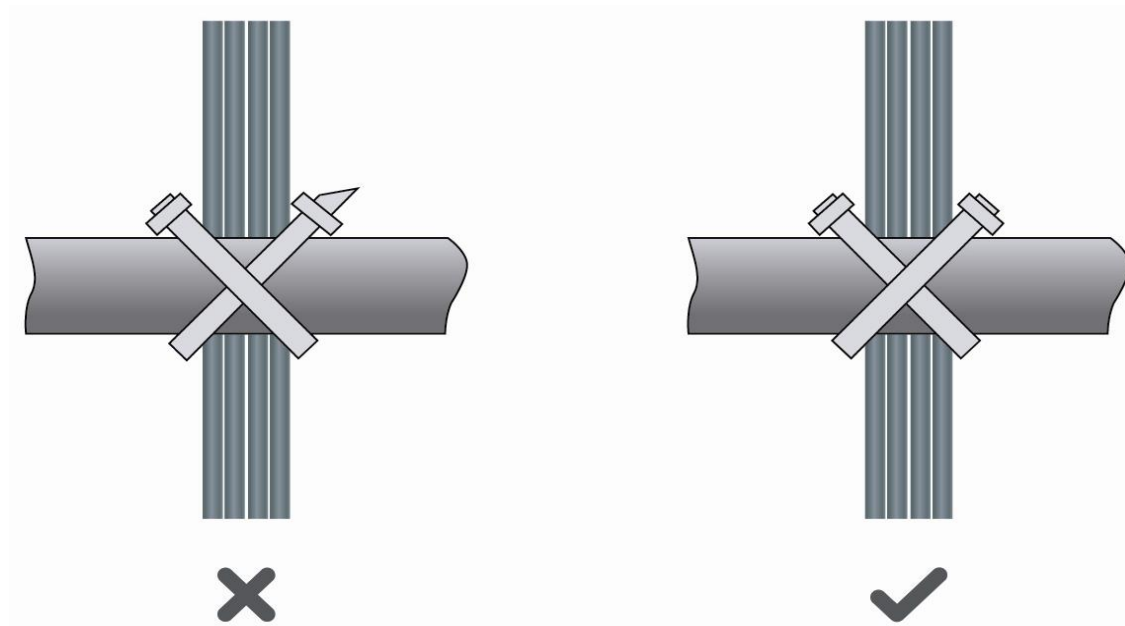
- Before cables are bundled, mark labels and stick the labels to cables wherever appropriate.
- Cables should be neatly and properly bundled in the rack without twisting or bending, as shown in [Figure 6-6](#).

Figure 6-6 Binding Cables (I)

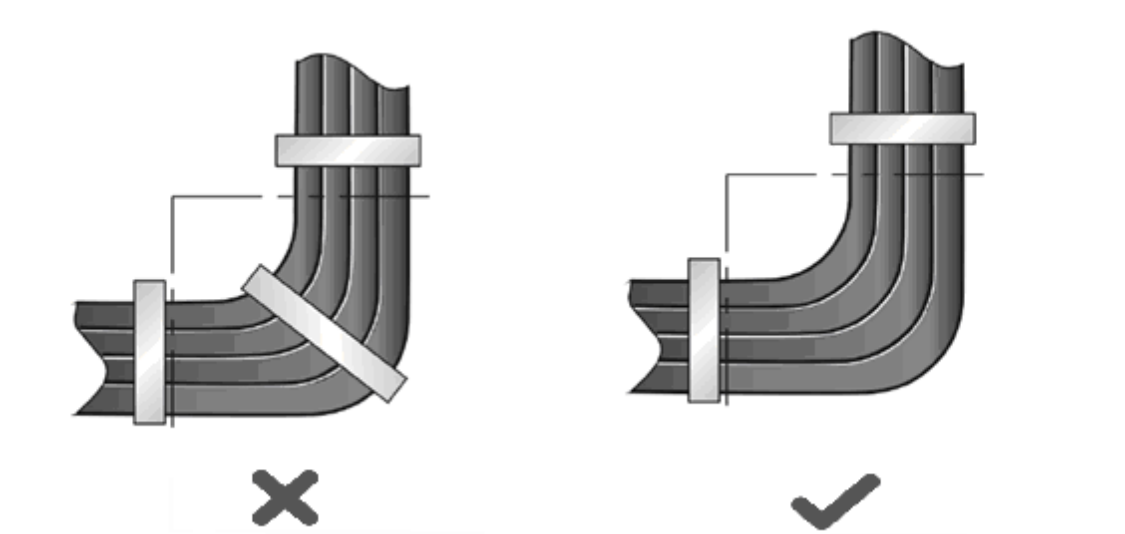


No.	Description
1	In the rack, cables should not be wound up after being bundled.
2	In the rack, cables should not bend after being bundled.
3	In the rack, cables should be neatly and straightly bundled.

- Cables of different types (such as power cords, signal cables, and ground cables) should be separated in cabling and bundling. Mixed bundling is disallowed. When they are close to each other, you are advised to adopt crossover cabling. In the case of parallel cabling, maintain a minimum distance of 30 mm (1.18 in.) between power cords and signal cables.
- The cable management brackets and cabling troughs inside and outside the rack should be smooth without sharp corners.
- The metal hole traversed by cables should have a smooth and fully rounding surface or an insulated lining.
- Use cable ties to bundle up cables properly. Please do not connect two or more cable ties to bundle up cables.
- After bundling up cables with cable ties, cut off the remaining part. The cut should be smooth and trim, without sharp corners, as shown in [Figure 6-7](#).

Figure 6-7 Binding Cables (II)

- When cables need to be bent, please bundle them up but do not tie them where the cables will be bent, as shown in [Figure 6-8](#).

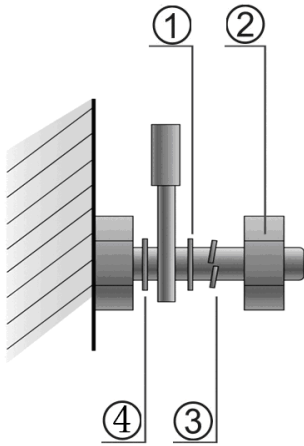
Figure 6-8 Binding Cables (III)

- Cables not to be assembled or remaining parts of cables should be folded and placed in a proper position of the rack or cable trough. The proper position refers to a position that does not affect device running or damage the device or cable.
- Do not bind power cords to the guide rails of moving parts.
- The power cords connecting moving parts such as door grounding cables should be reserved with a margin after being assembled to avoid suffering tension or stress. When the moving part is installed, the remaining cable part should not touch heat sources, sharp corners, or sharp edges. If heat sources cannot be avoided,

high-temperature cables should be used.

- When screw threads are used to fasten cable terminals, the anchor or screw must be tightly fastened, as shown in [Figure 6-9](#).

Figure 6-9 Cable Fastening



- ① Flat washer
- ② Screw nut
- ③ Spring washer
- ④ Flat washer

- Hard power cords should be fastened in the terminal connection area to prevent stress on terminal connection and cable.
- Do not use self-tapping screws to fasten terminals.
- Power cords of the same type and in the same cabling direction should be bundled up into cable bunches, with cables in cable bunches clean and straight.
- Bundle up cables by using cable ties.

Cable Bunch Diameter	Distance Between Every Binding Point
10 mm (0.39 in.)	80 mm to 150 mm (3.15 in. to 5.91 in.)
10 mm to 30 mm (0.39 in. to 1.18 in.)	150 mm to 200 mm (5.91 in. to 7.87 in.)
30 mm (1.18 in.)	200 mm to 300 mm (7.87 in. to 11.81 in.)

- Do not tie cables or bundles in a knot.
- For wiring terminal sockets (such as circuit breakers) with cord end terminals, the metal part of the cord end terminal should not be exposed outside the terminal socket when assembled.

6.4 Site Selection

- The equipment room should be at least 5 km (3.11 miles) away from heavy pollution sources, such as the smelter works, coal mine, and thermal power plant. The equipment room should be at least 3.7 km (2.30 miles) away from medium pollution sources, such as the chemical factory, rubber factory, and electroplating

factory. The equipment room should be at least 2 km (1.24 miles) away from light pollution sources, such as the food factory and leather plant. If the pollution source is unavoidable, the equipment room should be located on the windward side of the pollution source perennially with advanced protection.

- The equipment room should be at least 3.7 km (2.30 miles) away from the sea or salt lake. Otherwise, the equipment room must be sealed, with air conditioner installed for temperature control. Saline soil cannot be used for construction. Otherwise, you should select devices with advanced protection against severe environment.
- Do not build the equipment room in the proximity of livestock farms. Otherwise, the equipment room should be located on the windward side of the pollution source perennially. The previous livestock house or fertilizer warehouse cannot be used as the equipment room.
- The equipment room should be firm enough to withstand severe weather conditions such as windstorm and heavy rain as well as away from dust. If the dust is unavoidable, keep the door and window away from the pollution source.
- The equipment room should be away from the residential area. Otherwise, the equipment room should meet the construction standard in terms of noise.
- Make sure the air vent of the equipment room is away from the sewage pipe, septic tank, and sewage treatment tank. Keep the equipment room under positive pressure to prevent corrosive gas from entering the equipment room to corrode components and circuit boards.
- Keep the equipment room away from industrial boiler and heating boiler.
- The equipment room should be on the second floor. Otherwise, the equipment room floor should be 600 mm (23.62 in.) higher than the highest flood level ever recorded.
- Make sure there are no cracks or holes in the wall and floor. If there are cable entries in the wall or window, take proper sealing measures. Ensure that the wall is flat, wear-resistant, and dust-free, which should be up to the standard for flame retarding, soundproofing, heat absorption, dust reduction, and electromagnetic shielding.
- Keep the door and the window closed to make the equipment room sealed.
- The steel door is recommended for soundproofing.
- Sulfur-containing materials are forbidden.
- Keep the air conditioner from blowing wind straight toward the device or blowing water drops from the window or air vent toward the device.

6.5 Cleaning the Connectors and End Faces of Optical Cables

To ensure a good connection between a patch cable and an optical cable coupler, the cleanliness of the end face is a quite important factor, as it directly affects the communication quality of the optical network. In the daily construction of optical networks, however, improper operations or other reasons can easily contaminate the end face. When the end face accumulates dust, oil stains, and other dirt, if it is not detected and cleaned before connection, it will cause increased optical attenuation, leading to optical network failures. What's worse, it may even result in the collapse of the entire optical signal system. The following are common methods for cleaning connectors and end faces:

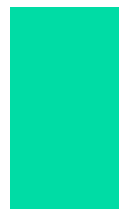
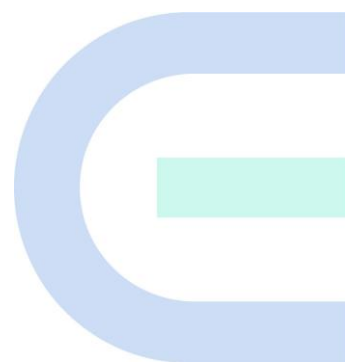
- Using fiber-optic cleaning pens

Fiber-optic cleaning pens, also known as one-click fiber-optic cleaners, typically use anti-static resin materials, lint-free cleaning tip, and cleaning solution to ensure the product remains free from dust contamination. Available in 1.25 mm and 2.5 mm sizes, these pens are suitable for cleaning SC, FC, LC connectors, and more. Select an appropriate cleaning pen for the connector to be cleaned, and gently insert the pen into the connector. To prevent ferrule damage, avoid excessive pressure when you insert the cleaning pen. Press inward gently until you hear a "click", indicating the end face has been cleaned. If necessary, repeat the process 2 to 3 times for thorough cleaning. Finally, remove the pen to complete the cleaning process.

- Using fiber-optic cleaning boxes or lint-free cloths
 - Made from high-density textile fibers, fiber-optic cleaning boxes do not need alcohol, do not produce static electricity, and are lint-free. In addition, fiber-optic cleaning boxes offer a convenient way for cleaning various optical cable connectors, including SC, FC, LC, and ST connectors.
 - To use the cleaning box, grip it with one hand and press it to reveal the clean cleaning belt core. Gently swipe the optical cable ferrule to be cleaned across the cleaning belt several times to remove dirt from the end face. To prevent ferrule damage, avoid excessive pressure when you swipe the optical cable ferrule.

Ruijie Reyee RG-NBF5200M-8FS16GT4XS e-Lighten Core Switch

Installation Guide



Copyright

Copyright © 2024 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 you purchase are subject to commercial contracts and terms, and some or all of the products, services, or features described in this document may not be available for you to purchase or use. Except for the agreement in the contract, Ruijie Networks makes no explicit or implicit statements or warranties with respect to 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 will be updated from time to time due to product version upgrades or other reasons, Ruijie Networks reserves the right to modify the content of the document without any notice or prompt.

This manual is designed merely as a user guide. Ruijie Networks has tried its best to ensure the accuracy and reliability of the content when compiling this manual, but it does not guarantee that the content of the manual is completely free of errors or omissions, and all the information 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

- 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. Signs

This document also uses signs to indicate some important points during the operation. The meanings of these signs are as follows:

 Caution


An alert that calls attention to safety instruction that if not understood or followed can result in personal injury.

 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.

 Note

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

 Instruction

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. Note

This manual provides installation steps, troubleshooting, technical specifications, and usage guidelines for cables and connectors. It is intended for users who want to understand the above and have extensive experience in network deployment and management, and assume that users are familiar with related terms and concepts.

Contents

Preface	1
1 Overview	1
1.1 About the RG-NBF5200M-8FS16GT4XS.....	1
1.2 Package Contents.....	1
1.3 Product Appearance.....	2
1.4 Hardware Specifications	4
1.5 Cooling.....	5
2 Preparing for Installation	7
2.1 Safety Guidelines.....	7
2.1.1 General Precautions	7
2.1.2 Chassis-Lifting Guidelines	7
2.1.3 Electricity Safety	7
2.1.4 Preventing ESD Damage.....	8
2.1.5 Laser Safety.....	8
2.2 Site Requirements	9
2.2.1 Floor Loading	9
2.2.2 Airflow.....	9
2.2.3 Space	9
2.2.4 Temperature and Humidity.....	9
2.2.5 Cleanliness.....	10
2.2.6 Grounding	11
2.2.7 Anti-Electromagnetic Interference.....	11

2.2.8 Surge Protection	11
2.2.9 EMI	12
2.2.10 Installation Site.....	12
2.3 Rack Requirements	12
2.4 Tools	13
3 Installing the Device	14
3.1 Installation Precautions.....	14
3.2 Installing the Device.....	14
3.2.1 Installing the Device in the Cabinet	14
3.2.2 Installing the Device on a Workbench	15
3.3 Connecting the Grounding Cable	17
3.4 Connecting the Power Cord.....	17
1.2 Checklist After Installation	17
4 Logging in to the Web Page.....	18
5 FAQs.....	19
5.1 Troubleshooting Flowchart	19
5.2 Common Faults.....	19
6 Appendix.....	21
6.1 Ports, Connectors, and Media	21
6.1.1 1000BASE-T/100BASE-TX/10BASE-T Ports.....	21
6.1.2 SFP Ports and SFP+ Ports	22
6.1.3 PON Ports and SC Ports	22
6.2 SFP and SFP+ Transceiver Modules	23
6.2.1 SFP Transceiver Modules.....	23

6.2.2 SFP+ Transceiver Modules.....	27
6.3 Surge Protection	30
6.3.1 Installing an AC Power Lightning Arrester	30
6.3.2 Installing an Ethernet Port Lightning Arrester	31
6.4 Recommended Cabling	33
6.4.1 Requirements for the Minimum Bend Radius of an Ethernet Cable	33
6.4.2 Requirement for the Minimum Bend Radius of an Optical Cable	33
6.4.3 Precautions for Bundling up Cables	33
6.5 Site Selection	36
6.6 Cleaning the Connectors and End Faces of Optical Cables.....	37

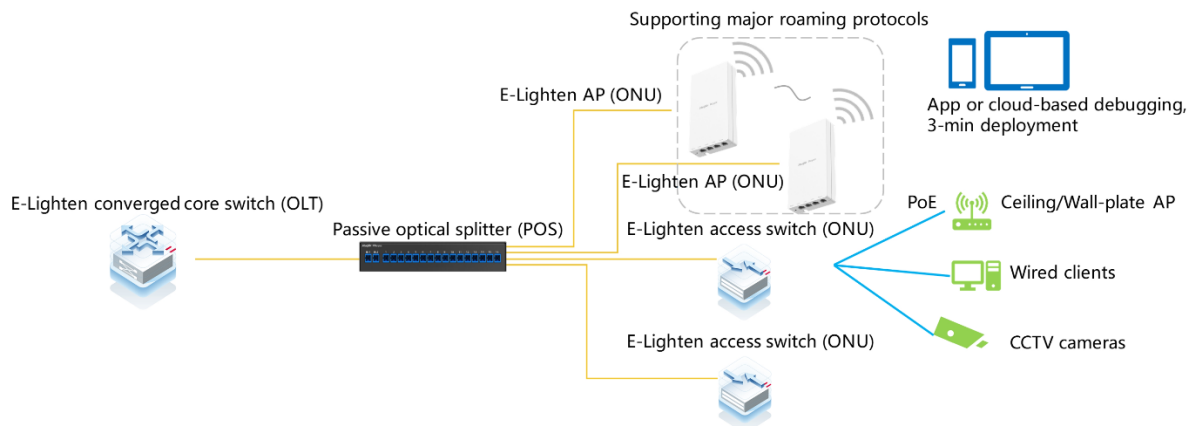
1 Overview

1.1 About the RG-NBF5200M-8FS16GT4XS

The Reyee e-Lighten Solution is a network product solution based on existing Ethernet technology integrating PON technology and passive optical splitting features. The components include:

- e-Lighten core switch (OLT): As a core switch, it has the Layer 3 data forwarding capability. It provides PON ports which can be connected to e-Lighten access switches and e-Lighten access points (APs) to achieve data interconnection.
- e-Lighten access switch (ONU): As an access device, the e-Lighten access switch is connected to the PON port at the uplink. It can send data to the core switch through the splitter.
- e-Lighten AP (ONU): An e-Lighten AP is connected to the PON port at the uplink, and can send wireless users' Internet access data to the core switch through the splitter.
- Passive optical distribution network (ODN): The ODN, consisting of splitters, is connected to the core switch at the uplink and to e-Lighten access switches or APs at the downlink.

Figure 1-1 Topology Diagram of Reyee e-Lighten Solution



The RG-NBF5200M-8FS16GT4XS switch, a core switch (OLT) launched by Ruijie Reyee, is designed for passive all-optical local area networks (LANs). The series switches adopt an efficient hardware architecture, provide larger entry specifications, faster hardware processing performance, and more convenient operation experience. It is applicable for diverse applications in small and medium-sized business environments, and can effectively cater to the needs of ELV campus networks, office spaces, hotels, residences, and small to medium-sized enterprises.

1.2 Package Contents

i Note

The package contents are subject to the purchase contract, and actual delivery may vary. Please check the items carefully against the package contents or purchase contract. If you have any questions, please contact your distributor.

Table 1-1 Package Contents

No.	Item	Quantity
1	RG-NBF5200M-8FS16GT4XS switch	1
2	Rubber pad	4
3	Mounting bracket	2
4	Black power cord (1.5 m or 4.92 ft.)	1
5	Grounding cable	1
6	M4 x 80 mm cross recessed countersunk screw	8
7	Dust plug	12
8	Power cord retainer clip	1
9	User Manual	1
10	Warranty card	1

1.3 Product Appearance

Figure 1-2 shows the product appearance.

Figure 1-2 Front View of the RG-NBF5200M-8FS16GT4XS



Figure 1-3 Front Panel of the RG-NBF5200M-8FS16GT4XS

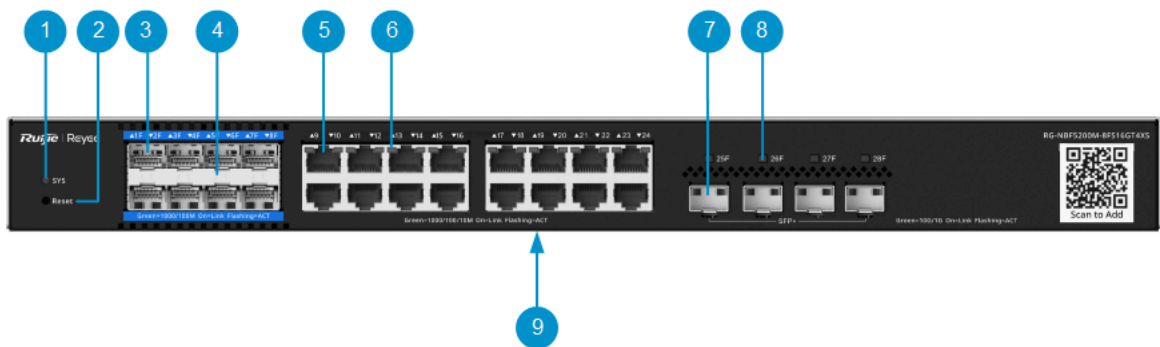


Table 1-2 Components on the Front Panel of the RG-NBF5200M-8FS16GT4XS

No.	Component	Description
1	SYS LED	<ul style="list-style-type: none"> ● Solid green: the switch is working properly. ● Blinking green (fast blinking: on for 0.0625s and off for 0.0625s): the switch is starting up. ● Blinking green (medium frequency: on for 0.25s and off for 0.25s): the device restores factory settings. ● Blinking green (slow blinking: on for 2s and off for 0.25s): the device is not connected to Ruijie Cloud. ● Blinking yellow (on for 1s and off for 1s): the temperature reaches the warning value, the temperature cannot be read, or other non-fatal problems occur, causing performance loss. ● Blinking red (one long pulse and three short pulses: on for 1s, off for 1s, on for 0.25s, off for 0.25s, on for 0.25s, off for 0.25s, on for 0.25s, and off for 1.75s, in a cycle): the main program is lost or damaged, other hardware is faulty, or a specific function is abnormal. ● Off: the device is not powered on.
2	Reset button	<ul style="list-style-type: none"> ● Press and hold for no more than two seconds: restart the switch ● Press and hold for two to five seconds: no action ● Press for more than 5s: the SYS LED blinks. Logs are collected, the username and password are reset, and the device is restarted. After the device is restarted, select whether to restore factory settings on the web page or in the app. After you restore factory settings, the default management address is http://10.44.77.200 (default password: admin).
3	SFP/PON optical port	1000BASE-X/100BASE-FX and PON optical port
4	SFP/PON optical port LED	<ul style="list-style-type: none"> ● Blinking green: the port is receiving or sending data. ● Solid green: the port is connected but not receiving or sending data. ● Off: the port is not connected or no device is successfully registered when the optical splitting function is enabled.
5	RJ45 port	10/100/1000BASE-T port
6	RJ45 port LED	<ul style="list-style-type: none"> ● Blinking green: the port is receiving or sending data. ● Solid green: the port is connected but not receiving or sending data. ● Off: the port is not connected.
7	SFP+ port LED	<ul style="list-style-type: none"> ● Blinking green: the port is receiving or sending data. ● Solid green: the port is connected but not receiving or sending data. ● Off: the port is not connected.
8	SFP+ port	10GE SFP+ and 1GE SFP transceivers, supporting hot swapping
9	Label	Bottom of the device

Figure 1-4 Rear Panel of the RG-NBF5200M-8FS16GT4XS

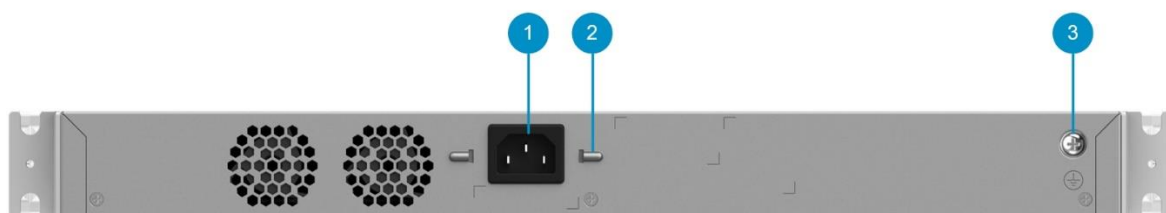


Table 1-3 Components on the Rear Panel of the RG-NBF5200M-8FS16GT4XS

No.	Component	Description
1	Power connector	Connects to an external AC power supply.
2	Power cord retention clip	Secures the power cord.
3	Grounding stud	Secures the grounding lug to connect the chassis to earth ground.

1.4 Hardware Specifications

Table 1-4 Hardware Specifications of the RG-NBF5200M-8FS16GT4XS

Model	RG-NBF5200M-8FS16GT4XS
CPU	Built-in CPU, dual-core MIPS processor, CPU clock speed of 1 GHz
Boot ROM	N/A
Flash Memory	256 MB
SDRAM	DDRIII 1 GB
Port	<ul style="list-style-type: none"> ● 8 x 100M/1000M SFP/PON combo ports ● 16 x 10/100/1000BASE-T ports ● 4 x 1GE/10GE SFP+ ports
Supported Optical Transceiver and Cable Types	See Appendix B. DAC cables are not supported. The supported module types may update without prior notification. Please contact Ruijie Networks for details.
LED	SYS LED and Link/ACT LED
Maximum Power	60 W
PoE	Not supported
EEE	Supported
Temperature Alarm	Supported

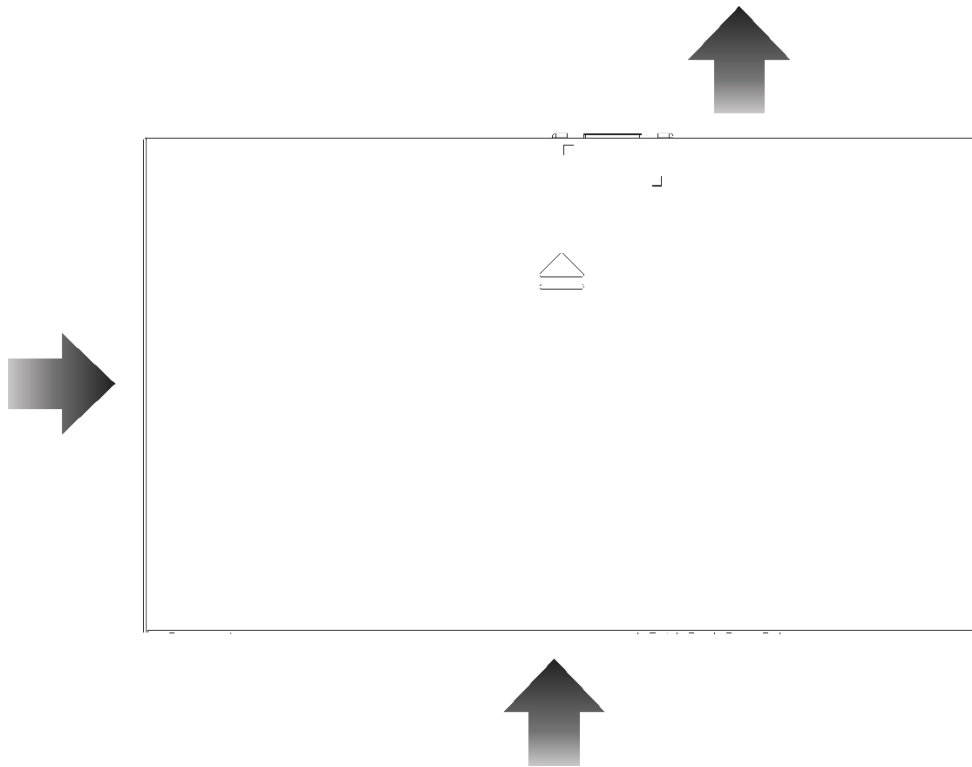
Fan	2 (automatic speed adjustment)
Power Module	AC input: <ul style="list-style-type: none"> ● Rated voltage range: 100 V AC to 240 V AC ● Max. voltage range: 90 V AC to 264 V AC ● Frequency: 50 Hz to 60 Hz ● Operating current ≤ 2 A
Leakage Current to Ground	≤ 3.5 mA
Operating Altitude	≤ 5,000 m (16,404.19 ft.)
Operating Temperature	0°C to 50°C (32°F to 122°F)
Storage Temperature	−40°C to +70°C (−40°F to +158 °F)
Operating Humidity	10% to 90% RH (non-condensing)
Storage Humidity	5% to 95% RH (non-condensing)
Port Surge Protection	6 kV
Certification	CE
Dimensions (W x D x H)	440 mm x 260 mm x 43.6 mm (17.32 in. x 10.24 in. x 1.72 in.)
Weight	4.68 kg (10.30 lbs.)

 **Warning**

Operation of this equipment in a residential environment could cause radio interference.

1.5 Cooling

The RG-NBF5200M-8FS16GT4XS adopts the cooling design of air intake from the left and front panels and air exhaust from the rear panel to ensure that the device can work properly in the specified environment. A minimum clearance of 100 mm (3.94 in.) must be maintained around the device to ensure proper ventilation. Dust the device every three months to avoid blocking the ventilation openings on the housing.



i Note

Maintain a minimum clearance of 1 RU (44.45 mm) between the switch and its neighboring device to ensure proper ventilation.

2 Preparing for Installation

2.1 Safety Guidelines



Note

- To avoid personal injury or equipment damage, review the safety guidelines in this chapter before you begin the installation.
 - The following safety guidelines may not include all the potentially hazardous situations.
-

2.1.1 General Precautions

- Do not place the equipment in a wet area, and keep it away from liquid. Keep the chassis clean and dust-free.
- Keep the equipment away from heat sources.
- For the equipment that is installed in a cabinet, ensure that the cabinet and power distribution system are properly grounded.
- Do not place the equipment in walking areas.
- During installation and maintenance, do not wear loose clothing, jewelry, or any other objects that may hook onto the chassis.
- Do not place tools and accessories in walking areas.

2.1.2 Chassis-Lifting Guidelines

- Avoid moving the equipment frequently.
- Turn off all power supplies and disconnect all power cords before lifting or moving the equipment.
- Two or more people are required to lift the chassis. Keep balance and prevent personal injuries when lifting or moving the equipment.

2.1.3 Electricity Safety



CAUTION: DOUBLE POLE/NEUTRAL FUSING

Electric shock hazard! The fuse may be in the neutral, and that the mains shall be disconnected to de-energize the phase conductors.

- Observe local regulations and specifications when performing electrical operations. Only qualified personnel should handle these tasks.
- Any improper electrical operation can lead to accidents such as fires or electric shocks, causing severe, or even fatal damage to the human body and the equipment.
- Carefully check the work area for potential hazards, including ungrounded power system, insufficient grounding, and damp or wet ground.
- Direct or indirect touch through a wet object on high-voltage and mains supply can bring a fatal danger.

- Locate the emergency power supply switch in the room before installation. In the case of an accident, cut off the power supply immediately.
- Carefully inspect the equipment and the environment before powering on or off the equipment.
- Select the right leakage protector (also called “leakage current switch” or “leakage current breaker”) for the power supply system. This equipment automatically disconnects the power supply in the event of leakage and the risk of electric shock. A leakage protector should meet the following requirements:
 - The rated leakage action current of each leakage protector is greater than twice of the theoretical maximum leakage current of all the power supplies in the system. For example, if a system is equipped with 16 identical power supplies, and the leakage current of each power supply is equal to or less than 3.5 mA, then the leakage current of the system totals 56 mA. A leakage protector with a rated leakage action current of 30 mA supports no more than four power supplies (that is, action current of the leakage protector/2/Maximum leakage current of each power supply = $30/2/3.5 \approx 4.28$). In this case, 16 power supplies in the system require at least four leakage protectors with a rated action current of 30 mA, with each leakage protector supporting four power supplies. Although the number of power supplies in a system differs in models, the rated leakage action current of each leakage protector divided by two must be greater than the sum of the maximum leakage current of all the power supplies.
 - The rated leakage non-action current of a leakage protector should be 50% of the leakage action current. If the non-action current value is too small, the high sensitivity level can cause the circuit to break, leading to power cutoff and service interruption, even if the leakage current value is normal. For example, if a leakage protector has a rated leakage action current of 30 mA, the rated leakage non-action current should be 15 mA. The leakage protector will not activate unless the leakage current exceeds 15 mA.

 **Caution**

- To ensure personal safety, each leakage protector in the system must have a rated leakage action current equal to or below 30 mA, which is the recognized safety threshold for human body current. If the total leakage current of the system exceeds twice the 30 mA limit, the system must be equipped with two or more leakage protectors to maintain safety.
 - The leakage current values vary with products. For the leakage current value of each product model, see the product technical specifications.
-

2.1.4 Preventing ESD Damage

- Properly ground both the equipment and the installation site.
- Keep the site as dust free as possible.
- Maintain appropriate humidity conditions.
- Before installing or maintaining the equipment, wear an anti-ESD wrist strap and make sure that it is properly grounded.
- Avoid contact between the printed circuit boards and clothing. The anti-ESD wrist strap only protects the printed circuit boards from ESD voltages on the body. ESD voltages on clothing can still cause damage.

2.1.5 Laser Safety

An equipment with an optical port usually supports multiple types of optical transceivers, all of which are Class I laser products. Pay attention to the following during the use of optical transceivers:

- When an optical transceiver is in operation, ensure that its port is connected to an optical fiber or covered by

a dust cap to keep out dust and prevent it from burning your eyes.

- When an optical transceiver is in operation, do not look into its port after removing the optical fiber. Doing so may result in eye injury.

⚠ Caution

Do not approach or look directly into any optical port under any circumstances. This may cause permanent damage to your eyes.

Figure 2-1 Laser Product Warning



2.2 Site Requirements

To ensure the normal operation and prolonged service life of the equipment, it is essential to install it indoors in a location that meets the following requirements.

2.2.1 Floor Loading

Assess the combined weight of the equipment and its accessories, including the cabinet, chassis, and power supply, and verify that the installation site meets the necessary specifications.

2.2.2 Airflow

To ensure that the equipment works properly in the specified environment, a minimum clearance of 100 mm (3.94 in.) must be maintained around the equipment to ensure proper ventilation. Manage the Ethernet cables and power cords using cable ties or cable management brackets to avoid blocking air intakes. You are advised to dust the equipment at an interval of three months to avoid blocking the ventilation openings.

2.2.3 Space

Ensure that indoor pathways are at least 0.8m (31.50 in.) wide to allow for proper chassis handling and module swapping.

Maintain a minimum clearance of 0.4m (15.75 in.) around the equipment for heat dissipation and equipment maintenance.

2.2.4 Temperature and Humidity

For optimal equipment performance and extended service life, it is essential to maintain ambient temperature and humidity conditions. Prolonged exposure to excessively high or low temperature and humidity can potentially cause damage to the equipment.

- When exposed to high relative humidity, insulating materials may exhibit poor insulation capabilities, increasing the risk of electrical leakage. Furthermore, high humidity can cause mechanical changes in materials and corrosion of metallic components.
- When exposed to low relative humidity, the insulating strip may dry out and shrink, increasing the risk of static

electricity generation. This static electricity can pose a danger to the circuits inside the equipment.

- In a dry environment, static electricity is prone to occur and damage the internal circuits of the equipment.
- High temperature environments can be detrimental to the equipment, leading to reduced performance and a shorter service life. Prolonged exposure to elevated temperatures can expedite the equipment's aging process.

 Note

The ambient temperature and humidity of the equipment are measured 1.5 m (59.06 in.) above the floor and 0.4 m (15.75 in.) before the equipment rack when there is no protective plate in front or at the back of the rack.

2.2.5 Cleanliness

Dust poses a major threat to the running of the equipment. The buildup of dust on the equipment can result in static electricity, causing poor contact between the metallic joints. Dust buildup is more likely to occur in environments with low relative humidity, which not only impacts the service life of the equipment but also increases the likelihood of communication failure. The following table shows the specifications for dust concentration and particle size in the equipment room.

Table 2-1 Requirements for Dust

Particle Size	Unit	Concentration
≥ 0.5 μm	Particles/m ³	≤ 3.5×10 ⁶
≥ 5 μm	Particles/m ³	≤ 3.5×10 ⁴

Apart from dust, the salt, acid, and sulfide in the air of the machine room must also meet strict requirements. These harmful substances will accelerate metal corrosion and component aging. Therefore, the machine room should be properly protected against the intrusion of harmful gases, such as sulfur dioxide, hydrogen sulfide, nitrogen dioxide, and chlorine gas. The following table lists limits for harmful gases.

Table 2-2 Requirements for Gases

Gas	Average (mg/m ³)	Maximum (mg/m ³)
Sulfur dioxide (SO ₂)	0.3	1.0
Hydrogen sulfide (H ₂ S)	0.1	0.5
Nitrogen dioxide (NO ₂)	0.5	1.0
Chlorine gas (Cl ₂)	0.1	0.3

 Note


"Average" indicates the typical level of exposure over a one-week period. "Maximum" refers to the highest allowable exposure level within a week, with this level being sustainable for no more than 30 minutes per day.

2.2.6 Grounding

A proper grounding system is crucial for ensuring stable and reliable operation of the equipment, as well as preventing lightning strikes and interference. To ensure proper grounding, carefully check the grounding conditions at the installation site according to the grounding specifications, and complete grounding properly based on the actual situation.

- Safety Grounding

Ensure that the installation site and power distribution system are securely grounded if the equipment uses the AC power supply. Failure to do so may result in an increased risk of electric shock, particularly when the insulation resistance between the power module and the chassis decreases.

 **Caution**

- Adopt grounding protection connections in buildings so that the equipment can be connected to the protective grounding system.
 - Verify that the AC socket is reliably connected to the protective grounding system of the building. If not, a protective grounding wire should be used to connect the protective grounding lug of the AC socket to the protective grounding system of the building.
 - The cross-sectional area of the protective grounding wire should be at least 0.75 mm² (18 AWG).
-

- Lightning Grounding

The lightning protection system of facilities is standalone, and is composed of a lightning rod, a down conductor, and a connector connected to the grounding system. The grounding system is usually used for power reference grounding and safety grounding of the installation site. Lightning grounding is required only for facilities and is not required for the equipment.

- EMC Grounding

Grounding required for electromagnetic compatibility includes shielded grounding, filter grounding, noise and interference suppression, and level reference, which contribute to the overall grounding requirements. The grounding resistance should be smaller than 1 ohm, and the grounding terminals of the rack should be grounded before the running of the equipment.

2.2.7 Anti-Electromagnetic Interference

- Take effective measures to prevent interference from power grid to the power supply system.
- Keep the equipment away from the grounding system or lightning protection grounding system of the power facility.
- Keep the equipment far away from high-frequency current equipment such as high-power radio transmitting stations and radar launchers.
- Take electromagnetic shielding measures when necessary.

2.2.8 Surge Protection

- Ensure that the neutral point of the AC power socket is in good contact with the ground.
- Install a power arrester in front of the power input end to enhance surge protection for the power supply.
- When an AC power cord is introduced from outdoors and directly connected to the power port of the equipment, the AC power port must be connected to an external lightning protection power strip to protect the equipment against lightning strokes. Connect the mains supply AC power cord to the lightning protection

power strip, and then connect the equipment to the lightning protection power strip. This prevents high-voltage lightning from directly passing through the equipment over the mains supply AC power cord.

Note

- The lightning protection power strip is not delivered with the equipment. Purchase it as required.
 - For details on how to use the lightning protection power strip, see the related user guide.
-

2.2.9 EMI

All interference sources, either from outside or inside of the equipment or application system, affect the equipment by capacitive coupling, inductive coupling, or electromagnetic waves. Electromagnetic interference (EMI) occurs due to electromagnetic radiation or conduction, depending on the transmission path. When the energy, often RF energy, from a component arrives at a sensitive component through the space, the energy is known as radiated interference. The interference source can be either a part of the interfered system or a completely electrically isolated unit. Conduction interference occurs when interference is transferred from one unit to another unit through cables, which are usually electromagnetic wires or signal cables connected between the source and the sensitive component. Conduction interference often affects the power supply of the equipment, but can be controlled by a filter. Radiated interference may affect any signal path in the equipment, and is difficult to shield.

- Take interference prevention measures for the power supply system.
- Keep the equipment away from the grounding system or lightning protection grounding system of the power facility.
- Keep the equipment far away from high-frequency current equipment such as high-power radio transmitting stations and radar launchers.
- Take electromagnetic shielding measures when necessary.

2.2.10 Installation Site

Regardless of whether the equipment is installed in a rack, on a workbench or on a wall, the following conditions must be met:

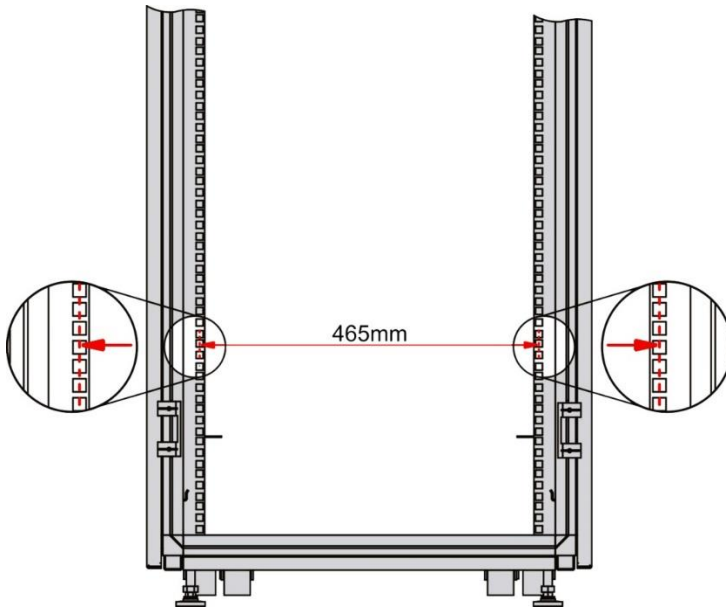
- Maintain a proper clearance around air vents for heat dissipation.
- The equipment is equipped with fans to draw air from front and left and right sides to rear. Maintain a minimum clearance of 150 mm (5.91 in.) around the ventilation openings for heat dissipation. Install the equipment in a standard 19-inch rack, or place it on a clean workbench. In hot areas, air-conditioning is recommended.
- The installation site has good cooling and ventilation.
- The installation site is sturdy enough to support the weight of the equipment and its accessories.
- The installation site is properly grounded.

2.3 Rack Requirements

If you plan to install the equipment in a rack, ensure that the rack meets the following conditions.

- (1) Use a four-post 19-inch cabinet.
- (2) The left and right square-hole rack posts are 465 mm (18.31 in.) apart.

Figure 2-2 19-Inch Rack



- (3) The square-hole rack post is at least 180 mm (7.09 in.) from the front door, and the front door is at most 25 mm (0.98 in.) thick. This ensures an available clearance of at least 155 mm (6.10 in.). The rack depth (distance between front and rear doors) is at least 1000 mm (39.37 in.).
- (4) The guide rails can bear the weight of the equipment and its accessories.
- (5) The cabinet has a reliable grounding terminal for the chassis to connect to earth ground.
- (6) The cabinet has a good ventilation system. The open area of front and rear doors is greater than 50%.

2.4 Tools

Table 2-3 Tools

Common Tools	Phillips screwdriver, power cords, Ethernet cables, cage nuts, diagonal pliers, and cable ties
Special Tools	Anti-ESD gloves, wire stripper, crimping plier, RJ45 crimping plier, and wire cutter
Meters	Multimeter

i Note

The equipment is delivered without a toolkit. Prepare the preceding tools by yourself.

3 Installing the Device

Caution

Before installing the device, ensure that guidelines and requirements in Chapter 2 have been met.

3.1 Installation Precautions

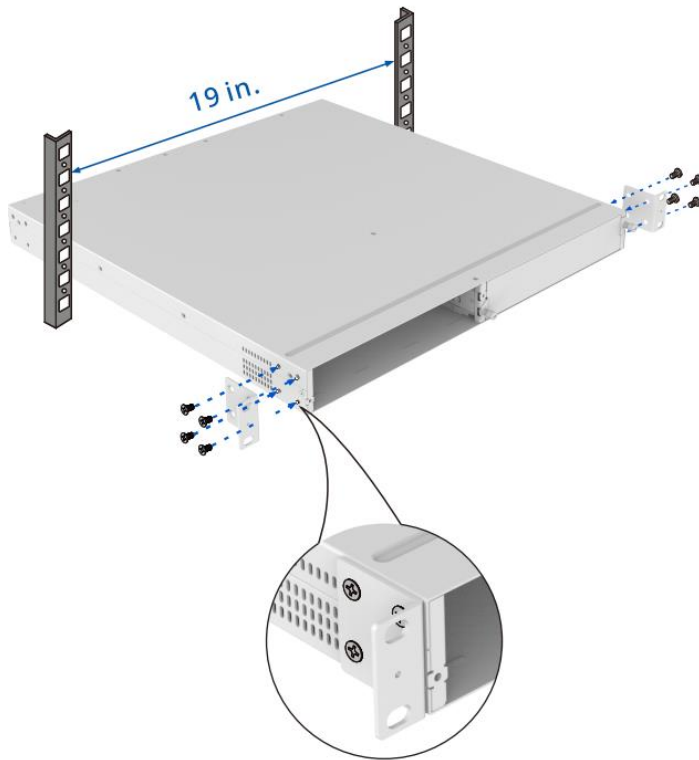
- Pay attention to the following during installation:
- Connect the power cords of different colors to the corresponding cable terminals.
- Ensure that the connector of the power cord is properly seated in the power port of the switch.
- Do not place any objects above the device.
- Maintain a minimum clearance of 100 mm (3.94 in.) around the device to ensure proper airflow. Do not stack switches.
- Keep the device away from high-power radio transmitting stations, radar transmitting stations, and high-frequency high-current devices. If necessary, use electromagnetic shielding methods, such as electromagnetic shielding for interface cables.
- Manage Ethernet cables with a distance of 100 meters (328.08 ft.) indoors. Take surge protection measures if Ethernet cables need to be routed outdoors.

3.2 Installing the Device

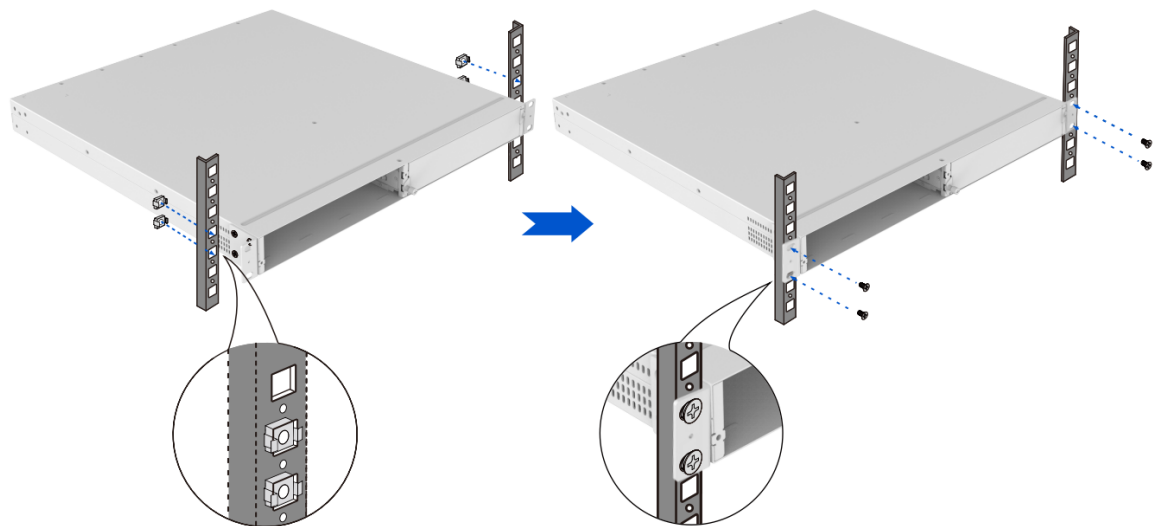
3.2.1 Installing the Device in the Cabinet

The device meets the EIA standard size and can be installed in a standard 19-inch cabinet.

- (1) Use eight M4 x 8 mm screws to fix the mounting brackets to the left and right sides of the device.



- (2) Place the device horizontally in the cabinet and secure it to the cabinet using the M6 screws and matching cage nuts.



3.2.2 Installing the Device on a Workbench

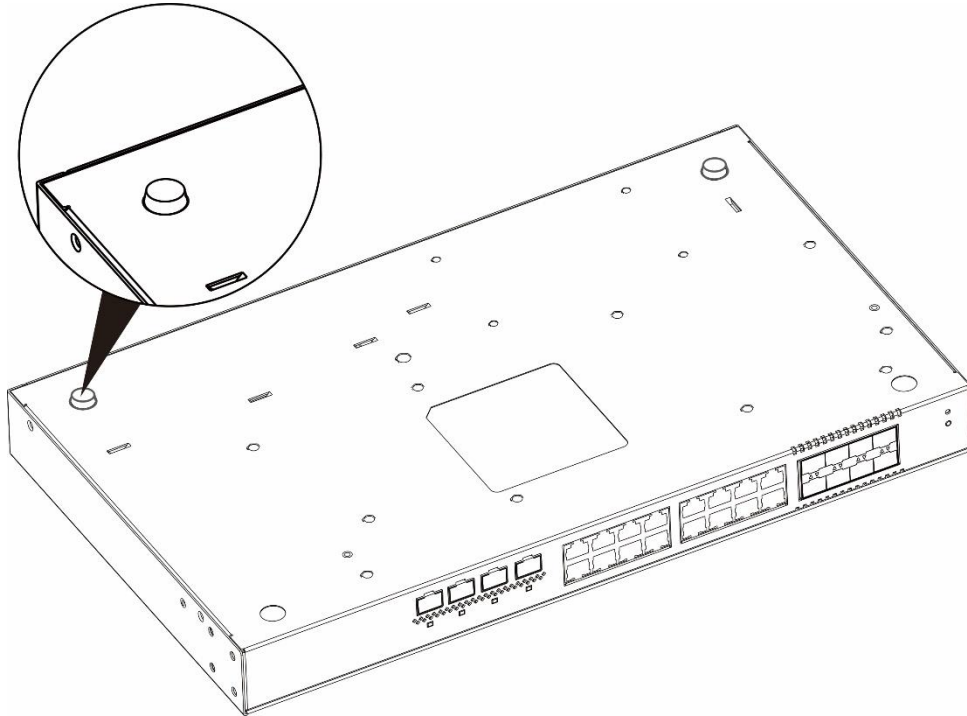
i Note

When the device is installed on a workbench, it must be installed in a location where mobility is restricted.

In many cases, users do not have the conditions for installing the device in a cabinet, on a wall, or on the ceiling. In this case, the device can be placed on a clean workbench.

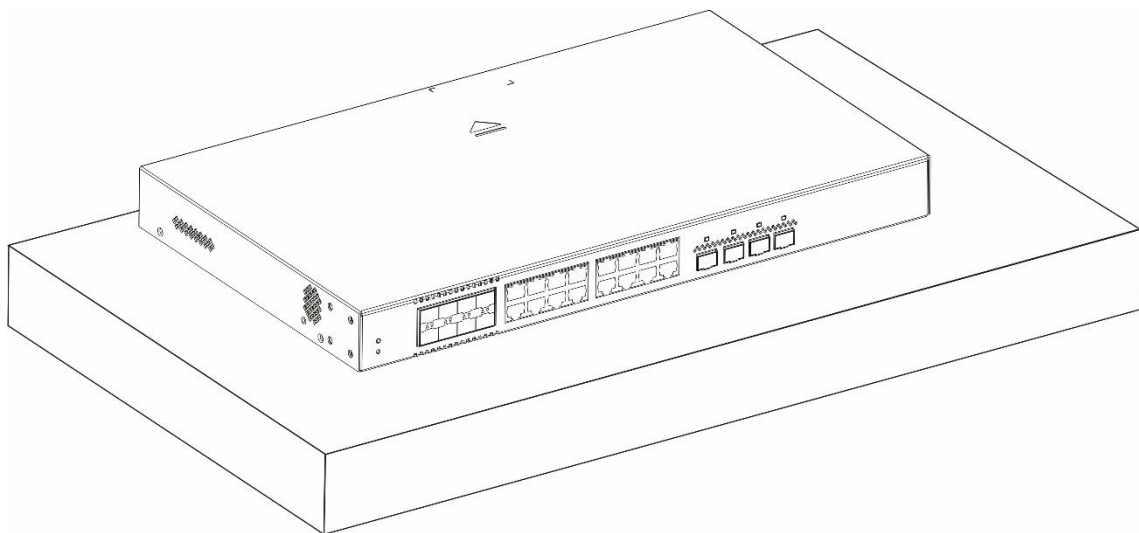
- (1) Attach the four rubber pads to the four corners at the bottom of the switch, as shown in [Figure 3-1](#).

Figure 3-1 Installing the Switch on a Workbench-1



- (2) Place the switch on the workbench and ensure adequate airflow around the switch.

Figure 3-2 Installing the Switch on a Workbench-2



Note

The location where the switch is installed must be subject to movement restrictions..

3.3 Connecting the Grounding Cable

 **Warning**

- To guarantee personal and device safety, the switch must be grounded properly.
 - The resistance between the switch chassis and the ground must be less than 1 Ω .
 - The O&M personnel should check whether the AC outlet is properly connected to the protective ground of the building. If not, the O&M personnel should use a protective earth conductor from the AC outlet protective earth lug to the building protective earth.
 - The power socket should be installed near the device and easily accessible.
 - During device installation, connect the grounding cable first and disconnect it last.
 - The cross-sectional area of a protective grounding cable should be at least 2.5 mm² (12 AWG).
-

A proper grounding system is crucial for ensuring stable and reliable operation, as well as preventing lightning strikes and interference.

- The grounding cable must be a good conductor with a cross-sectional area determined by the maximum current load.
- Do not use bare wires.

Procedure:

- (1) Remove the ground stud at the back of the device.
- (2) Use the removed grounding stud to secure one end of the grounding wire to the chassis. Similarly, connect the other end of the grounding wire to the grounding wire of the cabinet or the grounding bar of the equipment room.

3.4 Connecting the Power Cord

 **Warning**

Use the delivered power cords. Otherwise, security accidents may occur.

Procedure:

- (1) Ensure that the circuit breaker on the power supply side is turned off, plug one end of the power cord that comes with the device into the power socket on the rear panel of the chassis and the other end into the AC power socket.
- (2) Turn on the circuit breaker on the power supply side.
- (3) Check whether the power LED on the front panel of the device is on. If the LED is on, the power cord is connected correctly.

1.2 Checklist After Installation

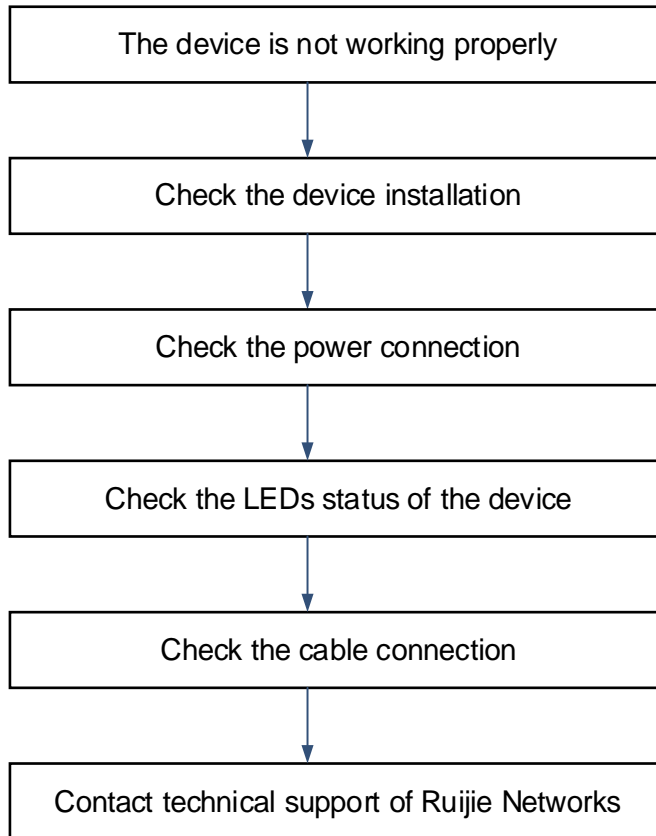
- The device is securely installed.
- The power cord meets the requirements.
- The cabinet is properly grounded.
- The device is correctly connected to terminals or other devices.
- The power cord is long enough to avoid over-extension.

4 Logging in to the Web Page

- (1) Connect your PC to the Ethernet port of the device through a cable.
- (2) Configure the PC with an IP address on the network of 10.44.77.XXX (Range: 1–255, excluding 200).
- (3) Open a browser on the PC and enter 10.44.77.200 to log in to the system configuration page. (The default password is admin when you log in to the device for the first time. To ensure security, you are advised to change the password after login, and update the password regularly.)
- (4) Perform device debugging based on service requirements.

5 FAQs

5.1 Troubleshooting Flowchart



5.2 Common Faults

Fault Symptom	Possible Cause	Solution
The login password cannot be retrieved.	The login password is forgotten after being configured.	Press and hold the reset button for over 5s to reset your username and password.
The SYS LED is off after the switch is powered on.	No power is supplied to the switch or the power cord is loose.	Check whether the power socket in the equipment room is normal and whether the power cord connected to the switch is loose.

Fault Symptom	Possible Cause	Solution
<p>An RJ45 port is disconnected or a frame sending or receiving error occurs.</p>	<p>The twisted pair cable is not connected properly.</p> <p>The cable length exceeds 100 m (328.08 ft.).</p> <p>The port is specially configured and does not use the same work mode as the interconnected switch.</p>	<p>Replace the twisted pair cable.</p> <p>Use optical cables or connect to an intermediate switch for relay.</p> <p>Make sure that the port works in the same mode as the interconnected switch.</p>
<p>An optical port cannot be connected.</p>	<p>The receiving and transmitting ends are connected incorrectly.</p> <p>The types of the interconnected optical transceivers do not match.</p> <p>The optical cable type does not meet the requirements.</p> <p>The length of the optical cable exceeds the allowed length marked on the optical transceiver.</p> <p>The optical cable or optical connector is contaminated.</p>	<p>Exchange the receiving and transmitting ends of the optical cable.</p> <p>Replace the optical transceiver with another one of the same model.</p> <p>Replace the optical cable with a qualified one.</p> <p>Use an optical cable with the allowed length.</p> <p>Use a clean cloth or a cleaning pen to clean the end face. For details, see the appendix.</p>

6 Appendix

6.1 Ports, Connectors, and Media

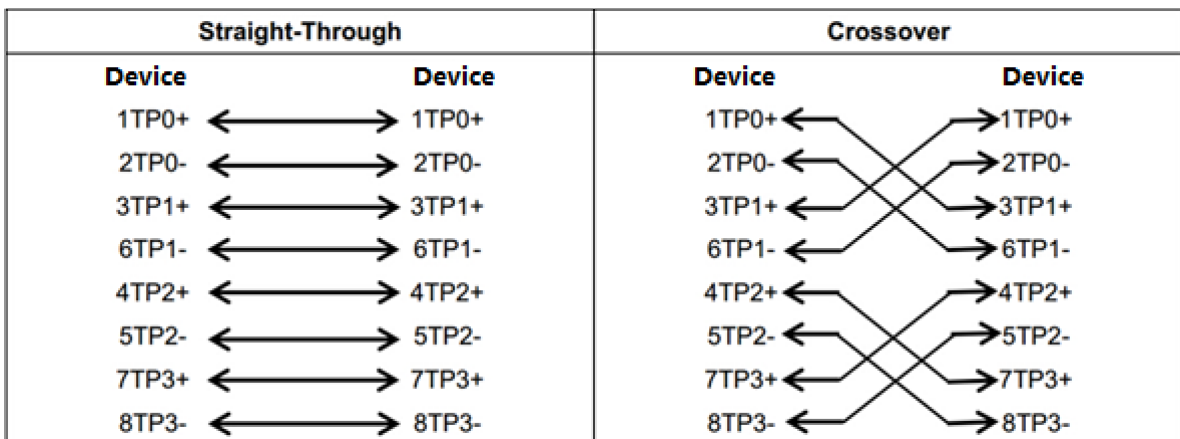
6.1.1 1000BASE-T/100BASE-TX/10BASE-T Ports

1000BASE-T/100BASE-TX/10BASE-T ports are Ethernet ports with auto-negotiation of three speeds: 10 Mbps, 100 Mbps, and 1000 Mbps. They supports auto MDI/MDIX Crossover, and use RJ 45 connectors.

Compliant with the IEEE 802.3ab standard, a 1000BASE-T port requires 100-ohm Category 5 or 5e unshielded twisted pair (UTP) or shielded twisted pair (STP) (recommended) cables, and supports a maximum distance of 100 meters (328 feet).

A 1000BASE-T port requires all four pairs of wires to be connected for data transmission. [Figure 6-1](#) shows the four pairs of wires for the 1000BASE-T port.

Figure 6-1 1000BASE-T Twisted Pair Connections



100BASE-TX/10BASE-T ports can be interconnected using cables of the preceding specifications. In addition, a 10BASE-T port can be connected using 100-ohm Category 3, Category 4, and Category 5 cables, while a 100BASE-TX port can be connected using 100-ohm Category 5 cables, and supports a maximum distance of 100 meters (328 feet). [Table 6-1](#) shows 100BASE-TX/10BASE-T pin assignments.

Table 6-1 100BASE-TX/10BASE-T Pin Assignments

Pin	Socket	Plug
1	Input Receive Data+	Output Transmit Data+
2	Input Receive Data-	Output Transmit Data-
3	Output Transmit Data+	Input Receive Data+
6	Output Transmit Data-	Input Receive Data-
4, 5, 7, 8	Not Used	Not Used

[Figure 6-2](#) shows the connection of straight-through and crossover cables for 100BASE-TX/10BASE-T ports.

Figure 6-2 100BASE-TX/10BASE-T Twisted Pair Connections

Straight-Through		Crossover	
Device	Adapter	Device	Device
1 IRD+	←→ 1 OTD+	1 IRD+ ←	→ 1 IRD+
2 IRD-	←→ 2 OTD-	2 IRD- ←	→ 2 IRD-
3 OTD+	←→ 3 IRD+	3 OTD+ ←	→ 3 OTD+
6 OTD-	←→ 6 IRD-	6 OTD- ←	→ 6 OTD-

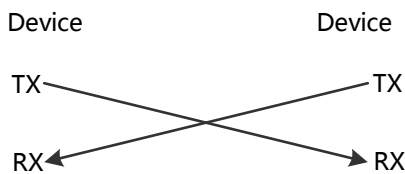
6.1.2 SFP Ports and SFP+ Ports

SFP ports and SFP+ ports require optical transceivers or Ethernet transceivers.

- Optical transceivers for SFP and SFP+ ports use LC connectors and connect to the peer end via an optical cable.
- SFP Ethernet transceivers use RJ45 connectors and connect to the remote end via an Ethernet cable.

Select either single-mode or multi-mode optical cables depending on the optical transceiver type. [Figure 6-3](#) shows the optical cable connection. Note that the TX on the local end should connect to the RX on the peer end, and the RX on the local end should connect to the TX on the peer end.

Figure 6-3 Optical Cable Connections

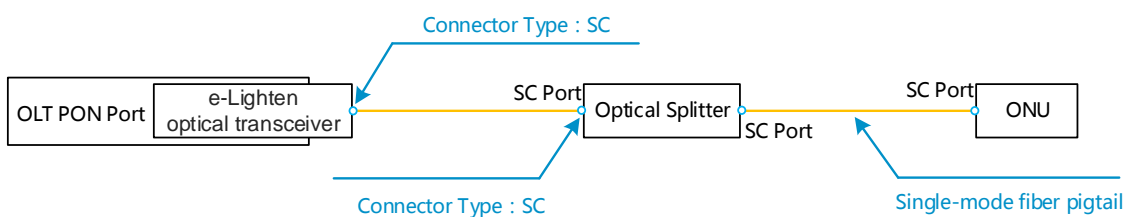


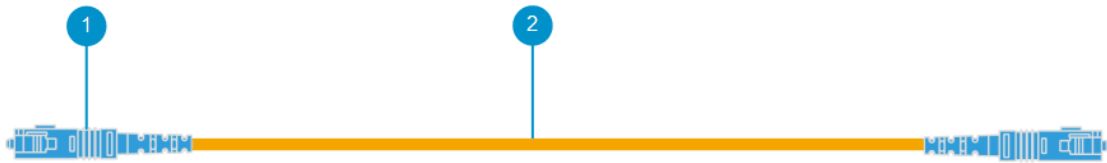
6.1.3 PON Ports and SC Ports

[Figure 6-4](#) shows the PON ports and SC ports on equipment in Ruijie Reyee e-Lighten Optical Solution.

- PON ports on the OLT require e-Lighten optical transceivers with SC connectors, which are connected to an optical splitter using single-mode pigtails.
- SC ports on optical splitters and ONUs use SC connectors, and are interconnected using single-mode pigtails.

Figure 6-4 PON Port and SC Port Connections





No	Description
1	SC connector
2	Single-mode pigtail

6.2 SFP and SFP+ Transceiver Modules

We provide SFP and SFP+ transceiver modules according to the port types. You can select the module to suit your specific needs. An SFP transceiver module can be a 1GE optical transceiver or Ethernet transceiver (Mini-GBIC-GT), while an SFP+ transceiver module is a 10GE optical transceiver. The following models and technical specifications of some SFP and SFP+ transceiver modules are listed for your reference.

6.2.1 SFP Transceiver Modules

Table 6-2 Models and Specifications of SFP Optical Transceiver Modules

Model	Wavelength (nm)	Optical Cable Type	DDM (Yes/No)	Intensity of Transmitted Light (dBm)		Intensity of Received Light (dBm)	
				Min	Max	Min	Max
MINI-GBIC-SX-MM850	850	MMF	No	-9.5	-3	-17	0
MINI-GBIC-LX-SM1310	1310	SMF	No	-9.5	-3	-20	-3
GE-eSFP-SX-MM850	850	MMF	Yes	-9.5	-3	-17	0
GE-eSFP-LX-SM1310	1310	SMF	Yes	-9.5	-3	-20	-3
GE-SFP-LX-SM1310	1310	SMF	No	-9.5	-3	-20	-3
MINI-GBIC-LH40-SM1310	1310	SMF	Yes	-2	3	-22	-3
GE-SFP-SX-SM1310-BIDI	1310	MMF	No	-10	-5	-17	-3
GE-SFP-SX-SM1550-BIDI	1550	MMF	No	-10	-5	-17	-3
GE-SFP-LX20-SM1310-BIDI	1310TX/1550RX	SMF	Yes	-9	-3	-20	-3
GE-SFP-LX20-SM1550-BIDI	1550TX/1310RX	SMF	Yes	-9	-3	-20	-3

Model	Wavelength (nm)	Optical Cable Type	DDM (Yes/No)	Intensity of Transmitted Light (dBm)		Intensity of Received Light (dBm)	
				Min	Max	Min	Max
GE-SFP-LH40-SM1310-BIDI	1310TX/1550RX	SMF	Yes	-5	0	-24	-1
GE-SFP-LH40-SM1550-BIDI	1550TX/1310RX	SMF	Yes	-5	0	-24	-1
MINI-GBIC-ZX50-SM1550	1550	SMF	Yes	-5	0	-22	-3
MINI-GBIC-ZX80-SM1550	1550	SMF	Yes	0	4.7	-22	-3
MINI-GBIC-ZX100-SM1550	1550	SMF	Yes	0	5	-30	-9
GE-SFP-SX	850	MMF	No	-9.5	-3	-17	0
GE-SFP-LX	1310	SMF	No	-9.5	-3	-20	-3
SFP-MM850	850	MMF	No	-9.5	-3	-17	0
SFP-SM1310	1310	SMF	No	-9.5	-3	-20	-3

Table 6-3 SFP Ethernet Transceiver Modules

Standard	SFP Media Converter	DDM (Yes/No)
1000BASE-T	Mini-GBIC-GT	No

Table 6-4 SFP Module Cabling Specifications

SFP Model	Connector Type	Optical Cable Type	Core Specifications (µm)	Max. Cabling Distance
MINI-GBIC-SX-MM850	LC	MMF	62.5/125	275 m (902.23 ft.)
			50/125	550 m (1804.46 ft.)
MINI-GBIC-LX-SM1310	LC	SMF	9/125	10 km (32808.40 ft.)
GE-eSFP-SX-MM850	LC	MMF	62.5/125	275 m (902.23 ft.)
			50/125	550 m (1804.46 ft.)
GE-eSFP-LX-SM1310	LC	SMF	9/125	10 km (32808.40 ft.)
GE-SFP-LX-SM1310	LC	SMF	9/125	10 km (32808.40 ft.)

SFP Model	Connector Type	Optical Cable Type	Core Specifications (µm)	Max. Cabling Distance
MINI-GBIC-LH40-SM1310	LC	SMF	9/125	40 km (131233.60 ft.)
GE-SFP-SX-SM1310-BIDI	LC	MMF	50/125	500 m (1640.42 ft.)
GE-SFP-SX-SM1550-BIDI	LC	MMF	50/125	500 m (1640.42 ft.)
GE-SFP-LX20-SM1310-BIDI	LC	SMF	9/125	20 km (65616.80 ft.)
GE-SFP-LX20-SM1550-BIDI	LC	SMF	9/125	20 km (65616.80 ft.)
GE-SFP-LH40-SM1310-BIDI	LC	SMF	9/125	40 km (131233.60 ft.)
GE-SFP-LH40-SM1550-BIDI	LC	SMF	9/125	40 km (131233.60 ft.)
MINI-GBIC-ZX50-SM1550	LC	SMF	9/125	50 km (164042.00 ft.)
MINI-GBIC-ZX80-SM1550	LC	SMF	9/125	80 km (65616.80 ft.)
MINI-GBIC-ZX100-SM1550	LC	SMF	9/125	100 km (328083.00 ft.)
GE-SFP-SX	LC	MMF	62.5/125	275 m (902.23 ft.)
			50/125	550 m (1804.46 ft.)
GE-SFP-LX	LC	SMF	9/125	10 km (32808.40 ft.)
Mini-GBIC-GT	RJ45 Ethernet cable	Cat 5 (or higher) UTP or STP		100 m (328.08 ft.)

⚠ Caution

- For optical transceivers with a cabling distance equal to or greater than 40 km (131,233.6 ft.), install an optical attenuator to avoid overload on the optical receiver when using short-distance SMF optical cables.
- An optical transceiver is a laser transmitter. Do not look directly into the optical transceiver to prevent it from burning your eyes.
- To keep the optical transceiver clean, ensure that the unused ports remain capped.

Rate/Distance	Pairing Model
1000 Mbps/500 m (1640.42 ft.)	GE-SFP-SX-SM1310-BIDI GE-SFP-SX-SM1550-BIDI
1000 Mbps/20 km (65616.80 ft.)	GE-SFP-LX20-SM1310-BIDI GE-SFP-LX20-SM1550-BIDI

1000 Mbps/40 km (131233.60 ft.)	GE-SFP-LH40-SM1310-BIDI GE-SFP-LH40-SM1550-BIDI
10000 Mbps/300 m (984.25 ft.)	XG-SFP-SR-SM1270-BIDI XG-SFP-SR-SM1330-BIDI
10000 Mbps/10 km (32808.40 ft.)	XG-SFP-LR-SM1270-BIDI XG-SFP-LR-SM1330-BIDI

⚠ Caution

The BIDI modules must be used in pairs. For example, if you install the GE-SFP-LX20-SM1310-BIDI on one end, you must install the GE-SFP-LX20-SM1550-BIDI on the other end.

6.2.2 SFP+ Transceiver Modules

Table 6-5 Models and Specifications of SFP+ Optical Transceiver Modules

Model	Wavelength (nm)	Optical Cable Type	DDM (Yes/No)	Intensity of Transmitted Light (dBm)		Intensity of Received Light (dBm)	
				Min	Max	Min	Max
XG-SFP-SR-MM850	850	Yes	MMF	-7.3	-1	-9.9	-1
XG-SFP-ZRV1	850	Yes	MMF	-7.3	-1	-9.9	-1
XG-SR-MM850	850	Yes	MMF	-7.3	-1	-9.9	-1
SFP+MM850	850	Yes	MMF	-7.3	-1	-9.9	-1
XG-SFP-SR-SM1270-BIDI	1270	No	MMF	-3	4	-9	0.5
XG-SFP-SR-SM1330-BIDI	1270	No	MMF	-3	4	-9	0.5
XG-SFP-LR-SM1270-BIDI	1270	No	SMF	-6.5	0.5	-14.4	0.5
XG-SFP-LR-SM1330-BIDI	1330	No	SMF	-6.5	0.5	-14.4	0.5
XG-LR-SM1310	1310	Yes	SMF	-8.2	0.5	-14.4	0.5
XG-SFP-LR-SM1310	1310	Yes	SMF	-8.2	0.5	-14.4	0.5
XG-eSFP-LR-SM1310	1310	Yes	SMF	-8.2	0.5	-14.4	0.5
XG-SFP-ER-SM1550	1550	Yes	SMF	-4.7	4	-11.3	-1
XG-SFP-ZR-SM1550	1550	Yes	SMF	0	4	-24	-7
XS-SFP-SR	850	Yes	MMF	-7.3	-1	-9.9	-1
XS-SFP-LR	1310	Yes	SMF	-8.2	0.5	-10.3	0.5

Table 6-6 Models of SFP+ Active Optical Cable Modules

Model	Transceiver Type	Connector Type	Copper Cable Length	Conductor Diameter (AWG)	Rate (Gb/s)	DDM (Yes/No)
XG-SFP-AOC1M	Active	SFP+	1 m (3.28 ft)	N/A	10.3125	Yes
XG-SFP-AOC3M	Active	SFP+	3 m (9.84 ft)	N/A	10.3125	Yes
XG-SFP-AOC5M	Active	SFP+	5 m (16.40 ft)	N/A	10.3125	Yes
XG-SFP-AOC10M	Active	SFP+	10 m (32.81 ft)	N/A	10.3125	Yes

i Note

- SFP+ module types and models are subject to change without prior notice. For any updates about the optical transceivers, contact Ruijie Networks marketing or technical support personnel.
- The DDM function of AOC cables does not report the transmit power. The transmit power is displayed as N/A.

Table 6-7 SFP+ Module Cabling Specifications

Model	Connector Type	Optical Cable Type	Core Specifications (μm)	Modal Bandwidth (MHz•km)	Max. Cabling Distance
XG-SFP-SR-MM850	LC	MMF	50/125	2000 (OM3)	300 m (984.25 ft.)
XG-SFP-ZRV1	LC	MMF	50/125	2000 (OM3)	300 m (984.25 ft.)
XG-SR-MM850	LC	MMF	50/125	2000 (OM3)	300 m (984.25 ft.)
SFP+MM850	LC	MMF	50/125	2000 (OM3)	300 m (984.25 ft.)
XG-SFP-SR-SM1270-BIDI	LC	MMF	50/125	2000 (OM3)	300 m (984.25 ft.)
XG-SFP-SR-SM1330-BIDI	LC	MMF	50/125	2000 (OM3)	300 m (984.25 ft.)

Model	Connector Type	Optical Cable Type	Core Specifications (μm)	Modal Bandwidth (MHz•km)	Max. Cabling Distance
XG-SFP-LR-SM1270-BIDI	LC	SMF	9/125	N/A	10 km (32808.40 ft.)
XG-SFP-LR-SM1330-BIDI	LC	SMF	9/125	N/A	10 km (32808.40 ft.)
XG-SFP-LR-SM1310	LC	SMF	9/125	N/A	10 km (32808.40 ft.)
XG-SFP-ER-SM1550	LC	SMF	9/125	N/A	40 km (131233.60 ft.)
XG-SFP-ZR-SM1550	LC	SMF	9/125	N/A	80 km (65616.80 ft.)
XS-SFP-SR	LC	MMF	62.5/125	200 (OM1) 160	33 m 108.27 ft.) 26 m (85.30 ft.)
			50/125	2000 (OM3) 500 (OM2) 400 (OM1)	300 m (984.25 ft.) 82 m (269.03 ft.) 66 m (216.54 ft.)
XS-SFP-LR	LC	SMF	9/125	N/A	10 km (32808.40 ft.)

Table 6-8 Models and Specifications of e-Lighten Optical Transceivers

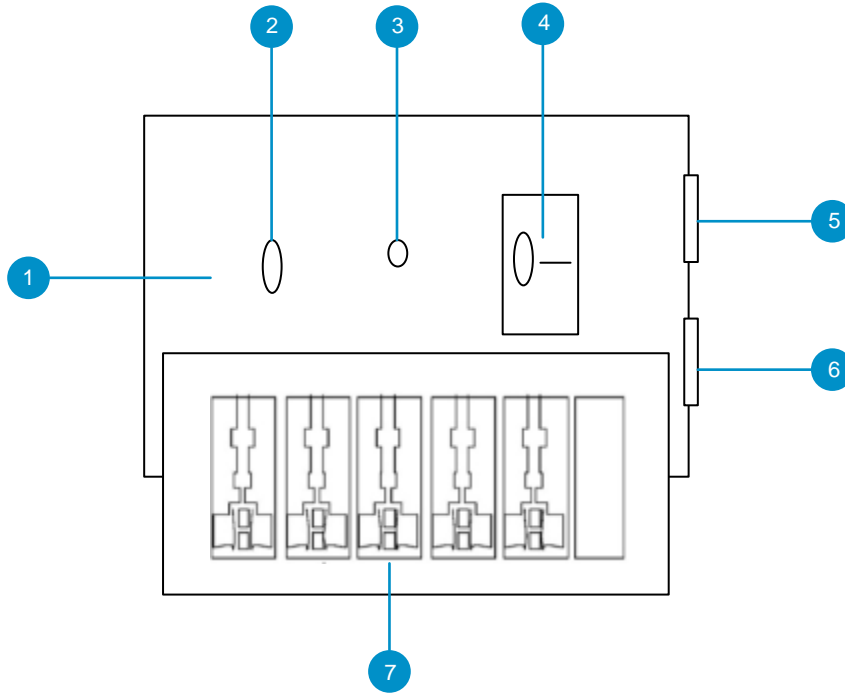
Model	Wavelength (nm)	Optical Cable Type	DDM (Yes/No)	Transmit Power (dBm)		Receive Power (dBm)	
				Min	Max	Min	Max
OM-GE-SFP-10KM-SM1490	1490/1310	Yes	SMF	3	7	-32	-12

6.3 Surge Protection

6.3.1 Installing an AC Power Lightning Arrester

When an AC power cord from outdoors is directly plugged into the power port of the equipment, the AC power connector must be connected to an external surge protector power strip to protect the equipment against lightning strikes. The surge protector power strip can be fixed on the rack, workbench, or wall in the equipment room by using cable ties and screws. AC power enters the equipment through the surge protector power strip.

Figure 6-5 Installing an AC Power Lightning Arrester



No.	Description
1	Installed electronic circuit board
2	Normally running indicator: When the indicator is green, the circuit is working properly. Otherwise, the protective circuit is damaged.
3	Grounding and polarity detection indicator: If the indicator is red, cable connection is incorrect (the ground cable is not connected, or the N and L lines are reversely connected). Check your power supply line.
4	Power switch
5	IEC standard socket, which is connected to the power supply in the equipment room through the power cable
6	Overload auto-protector, which can be reset manually
7	Multi-purpose sockets (connected to the power supply of the switch)

Note

The lightning arrester is not delivered with the equipment. Please purchase it based on actual requirements.

Precautions:

- Make sure that the PE terminal of the power arrester is well grounded.
- After the AC power plug of the equipment is connected to the socket of the power arrester (lightning resistance socket), the surge protection function is implemented only if the RUN indicator is green and the ALARM indicator is OFF.
- If the indicator on the power arrester is red, check whether it is caused by poor grounding connection or by the reversed connection of the Null and Live lines. The detection method is as follows: Use a multimeter to measure the polarity of the power socket for the arrester when the indicator is red. If the N line is on the left and the L line is on the right (facing the socket), the arrester's PE terminal is not grounded. If not, the polarity of the arrester power cord should be reversed. In this case, you should open the power arrester and rectify the polarity of the connection. If the indicator is still red, the arrester's PE terminal is not grounded.

6.3.2 Installing an Ethernet Port Lightning Arrester

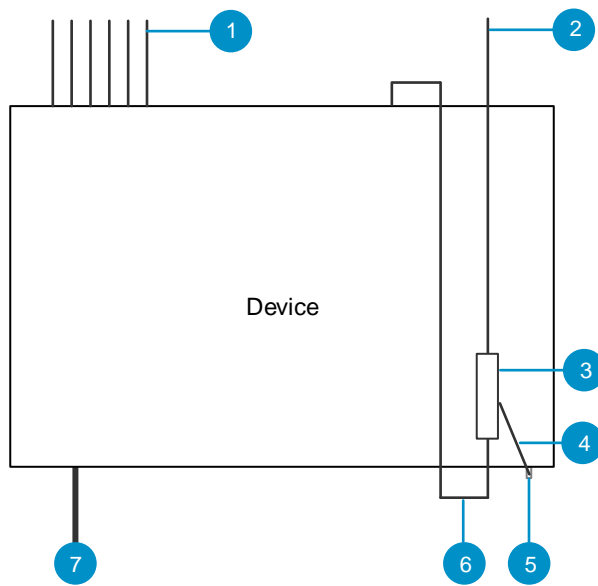
Connect an Ethernet port arrester to the equipment to prevent the damage by lightning before connecting an outdoor network cable to the device.

Tools: Phillips screwdrivers or flat-head screwdriver, multimeter, and diagonal pliers

Procedure:

- (1) Tear one side of the protective paper for the double-sided adhesive tape and paste the tape to the enclosure of the Ethernet port arrester.
- (2) Tear the other side of the protective paper for the double-sided adhesive tape and paste the Ethernet port arrester to the enclosure. The paste position for the Ethernet port arrester should be as close to the grounding terminal of the equipment as possible.
- (3) According to the distance between the equipment grounding terminal and the Ethernet port arrester, cut the grounding cable for the Ethernet port arrester and firmly crimp the grounding cable to the grounding terminal of the equipment.
- (4) Use a multimeter to check whether the grounding cable for the arrester is in good contact with the grounding terminal and the enclosure of the equipment.
- (5) Connect the arrester by using an adapter cable (note that the external network cable is connected to the IN end, while the adapter cable connected to the equipment is connected to the OUT end) and check whether the service module LED is normal.
- (6) Use a nylon cable tie to bind the power cords.

Figure 6-6 Installing an Ethernet Port Lightning Arrester



No.	Description
1	Ethernet cable for indoor connection
2	Ethernet cable connected to the outdoor
3	RJ45 port arrester (pasted on the enclosure)
4	Ground cable of the arrester
5	Grounding lug of the equipment
6	RJ45 port adapter cable
7	Power input

Note

- The Ethernet port arrester is only for Ethernet ports with an RJ45 connector.
- The Ethernet port arrester is not delivered with the equipment. Please purchase it based on actual requirements. The Ethernet port arrester user manual contains technical parameters and maintenance and installation instructions for the Ethernet port arrester. Carefully read this manual before installation.
- Pay attention to the following situations during the installation to avoid influencing the performance of the Ethernet port arrester:
 - Reversed installation direction of the arrester. Connect the external network cable to the “IN” end and connect the Ethernet port of the equipment to the “OUT” end.
 - Poor grounding of the arrester. The grounding cable of the arrester should be as short as possible to ensure that it is in good contact with the grounding terminal of the equipment. Use a multimeter to confirm the contact condition after grounding.
 - Incomplete arrester installation. If there is more than one port connected to external power cords, arresters

need to be installed on all connection ports for the purpose of surge protection.

6.4 Recommended Cabling

When the device is installed in a standard 19-inch rack, route the cables through the cable management brackets. Top cabling or bottom cabling is adopted according to the actual situation in the equipment room. All conversion connectors should be placed at the bottom of the rack instead of outside the rack that is easily accessible. Power cords are routed beside the cabinet, and top cabling or bottom cabling is adopted according to the actual situation in the equipment room, such as the locations of the DC power distribution box, AC power socket, or surge protection box.

6.4.1 Requirements for the Minimum Bend Radius of an Ethernet Cable

- The bend radius of a fixed power cord, Ethernet cable, or flat cable should be over five times greater than their respective diameters. The bend radius of these cables that are often bent or plugged should be over seven times greater than their respective diameters.
- The bend radius of a fixed common coaxial cable should be over seven times greater than its diameter. The bend radius of the common coaxial cable that is often bent or plugged should be over 10 times greater than its diameter.
- The bend radius of a fixed high-speed cable (such as SFP+ cable) should be over five times greater than its diameter. The bend radius of the fixed high-speed cable that is often bent or plugged should be over 10 times greater than its diameter.

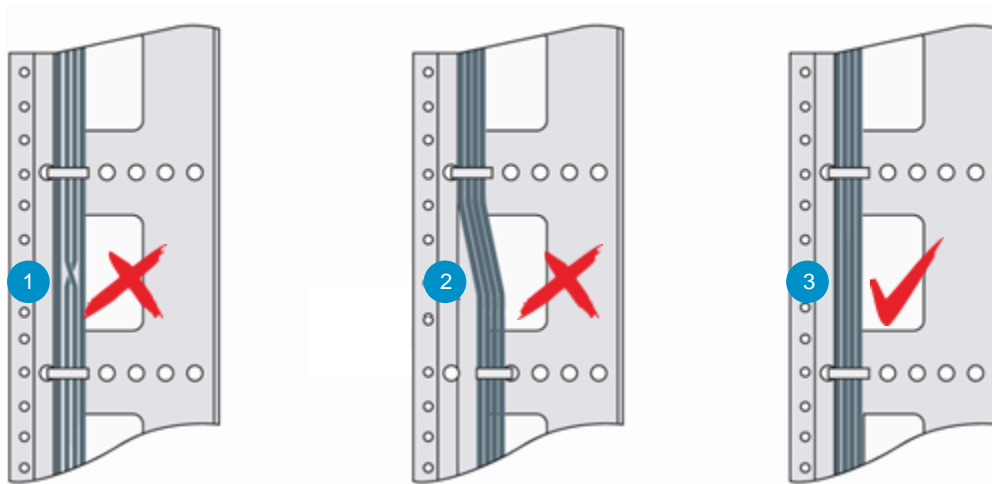
6.4.2 Requirement for the Minimum Bend Radius of an Optical Cable

- When an optical cable is coiled, the diameter of a fiber tray should be over 25 times greater than the diameter of the optical cable.
- When an optical cable is moved, the bend radius of the optical cable should be over 20 times greater than the diameter of the optical cable.
- When an optical cable is laid, the bend radius of the optical cable should be over 10 times greater than the diameter of the optical cable.

6.4.3 Precautions for Bundling up Cables

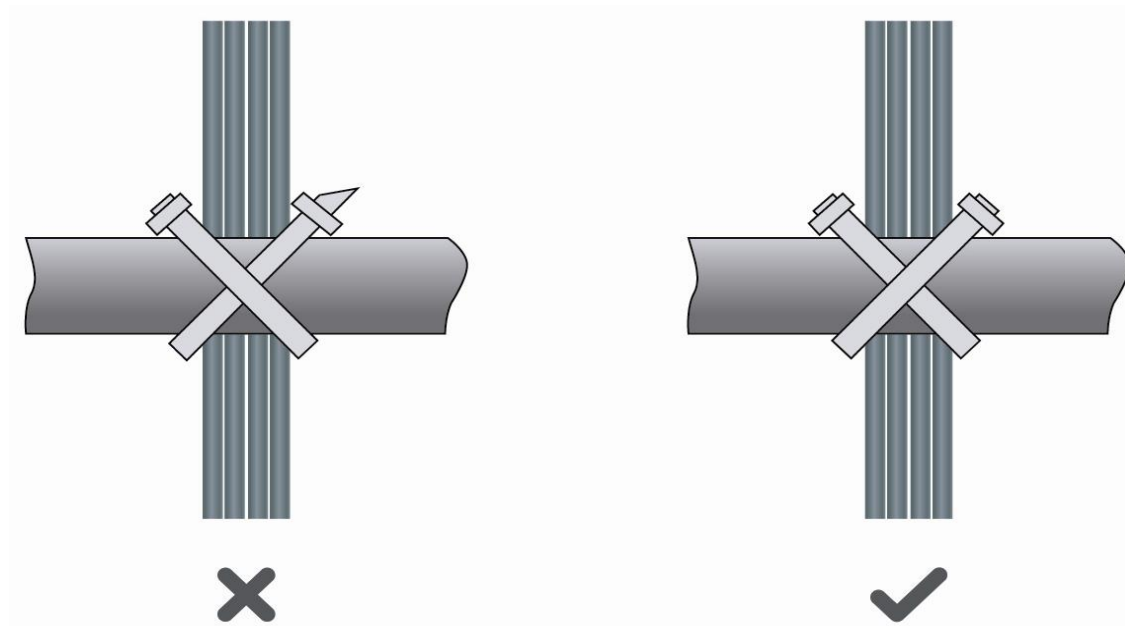
- Before cables are bundled, mark labels and stick the labels to cables wherever appropriate.
- Cables should be neatly and properly bundled in the rack without twisting or bending, as shown in [Figure 6-7](#).

Figure 6-7 Binding Cables (I)

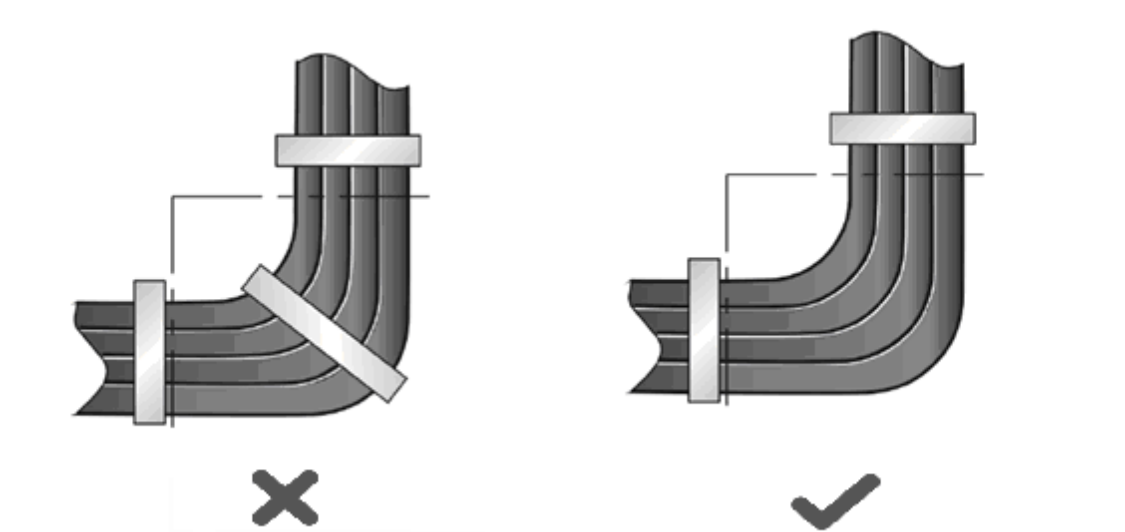


No.	Description
1	In the rack, cables should not be wound up after being bundled.
2	In the rack, cables should not bend after being bundled.
3	In the rack, cables should be neatly and straightly bundled.

- Cables of different types (such as power cords, signal cables, and ground cables) should be separated in cabling and bundling. Mixed bundling is disallowed. When they are close to each other, you are advised to adopt crossover cabling. In the case of parallel cabling, maintain a minimum distance of 30 mm (1.18 in.) between power cords and signal cables.
- The cable management brackets and cabling troughs inside and outside the rack should be smooth without sharp corners.
- The metal hole traversed by cables should have a smooth and fully rounding surface or an insulated lining.
- Use cable ties to bundle up cables properly. Please do not connect two or more cable ties to bundle up cables.
- After bundling up cables with cable ties, cut off the remaining part. The cut should be smooth and trim, without sharp corners, as shown in [Figure 6-8](#).

Figure 6-8 Binding Cables (II)

- When cables need to be bent, please bundle them up but do not tie them where the cables will be bent, as shown in [Figure 6-9](#).

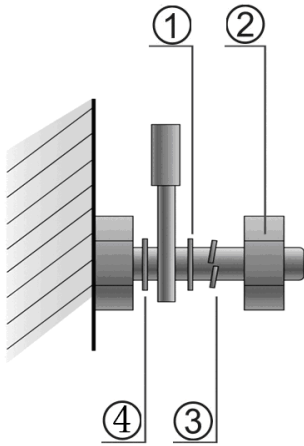
Figure 6-9 Binding Cables (III)

- Cables not to be assembled or remaining parts of cables should be folded and placed in a proper position of the rack or cable trough. The proper position refers to a position that does not affect device running or damage the device or cable.
- Do not bind power cords to the guide rails of moving parts.
- The power cords connecting moving parts such as door grounding cables should be reserved with a margin after being assembled to avoid suffering tension or stress. When the moving part is installed, the remaining cable part should not touch heat sources, sharp corners, or sharp edges. If heat sources cannot be avoided,

high-temperature cables should be used.

- When screw threads are used to fasten cable terminals, the anchor or screw must be tightly fastened, as shown in [Figure 6-10](#).

Figure 6-10 Cable Fastening



- ① Flat washer
- ② Screw nut
- ③ Spring washer
- ④ Flat washer

- Hard power cords should be fastened in the terminal connection area to prevent stress on terminal connection and cable.
- Do not use self-tapping screws to fasten terminals.
- Power cords of the same type and in the same cabling direction should be bundled up into cable bunches, with cables in cable bunches clean and straight.
- Bundle up cables by using cable ties.

Cable Bunch Diameter	Distance Between Every Binding Point
10 mm (0.39 in.)	80 mm to 150 mm (3.15 in. to 5.91 in.)
10 mm to 30 mm (0.39 in. to 1.18 in.)	150 mm to 200 mm (5.91 in. to 7.87 in.)
30 mm (1.18 in.)	200 mm to 300 mm (7.87 in. to 11.81 in.)

- Do not tie cables or bundles in a knot.
- For wiring terminal sockets (such as circuit breakers) with cord end terminals, the metal part of the cord end terminal should not be exposed outside the terminal socket when assembled.

6.5 Site Selection

- The equipment room should be at least 5 km (3.11 miles) away from heavy pollution sources, such as the smelter works, coal mine, and thermal power plant. The equipment room should be at least 3.7 km (2.30

miles) away from medium pollution sources, such as the chemical factory, rubber factory, and electroplating factory. The equipment room should be at least 2 km (1.24 miles) away from light pollution sources, such as the food factory and leather plant. If the pollution source is unavoidable, the equipment room should be located on the windward side of the pollution source perennially with advanced protection.

- The equipment room should be at least 3.7 km (2.30 miles) away from the sea or salt lake. Otherwise, the equipment room must be sealed, with air conditioner installed for temperature control. Saline soil cannot be used for construction. Otherwise, you should select devices with advanced protection against severe environment.
- Do not build the equipment room in the proximity of livestock farms. Otherwise, the equipment room should be located on the windward side of the pollution source perennially. The previous livestock house or fertilizer warehouse cannot be used as the equipment room.
- The equipment room should be firm enough to withstand severe weather conditions such as windstorm and heavy rain as well as away from dust. If the dust is unavoidable, keep the door and window away from the pollution source.
- The equipment room should be away from the residential area. Otherwise, the equipment room should meet the construction standard in terms of noise.
- Make sure the air vent of the equipment room is away from the sewage pipe, septic tank, and sewage treatment tank. Keep the equipment room under positive pressure to prevent corrosive gas from entering the equipment room to corrode components and circuit boards.
- Keep the equipment room away from industrial boiler and heating boiler.
- The equipment room should be on the second floor. Otherwise, the equipment room floor should be 600 mm (23.62 in.) higher than the highest flood level ever recorded.
- Make sure there are no cracks or holes in the wall and floor. If there are cable entries in the wall or window, take proper sealing measures. Ensure that the wall is flat, wear-resistant, and dust-free, which should be up to the standard for flame retarding, soundproofing, heat absorption, dust reduction, and electromagnetic shielding.
- Keep the door and the window closed to make the equipment room sealed.
- The steel door is recommended for soundproofing.
- Sulfur-containing materials are forbidden.
- Keep the air conditioner from blowing wind straight toward the device or blowing water drops from the window or air vent toward the device.

6.6 Cleaning the Connectors and End Faces of Optical Cables

To ensure a good connection between a patch cable and an optical cable coupler, the cleanliness of the end face is a quite important factor, as it directly affects the communication quality of the optical network. In the daily construction of optical networks, however, improper operations or other reasons can easily contaminate the end face. When the end face accumulates dust, oil stains, and other dirt, if it is not detected and cleaned before connection, it will cause increased optical attenuation, leading to optical network failures. What's worse, it may even result in the collapse of the entire optical signal system. The following are common methods for cleaning connectors and end faces:

- Using fiber-optic cleaning pens

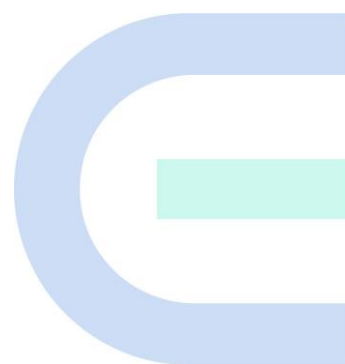
Fiber-optic cleaning pens, also known as one-click fiber-optic cleaners, typically use anti-static resin materials, lint-free cleaning tip, and cleaning solution to ensure the product remains free from dust contamination. Available in 1.25 mm and 2.5 mm sizes, these pens are suitable for cleaning SC, FC, LC connectors, and more. Select an appropriate cleaning pen for the connector to be cleaned, and gently insert the pen into the connector. To prevent ferrule damage, avoid excessive pressure when you insert the cleaning pen. Press inward gently until you hear a "click", indicating the end face has been cleaned. If necessary, repeat the process 2 to 3 times for thorough cleaning. Finally, remove the pen to complete the cleaning process.

- Using fiber-optic cleaning boxes or lint-free cloths

- Made from high-density textile fibers, fiber-optic cleaning boxes do not need alcohol, do not produce static electricity, and are lint-free. In addition, fiber-optic cleaning boxes offer a convenient way for cleaning various optical cable connectors, including SC, FC, LC, and ST connectors.
- To use the cleaning box, grip it with one hand and press it to reveal the clean cleaning belt core. Gently swipe the optical cable ferrule to be cleaned across the cleaning belt several times to remove dirt from the end face. To prevent ferrule damage, avoid excessive pressure when you swipe the optical cable ferrule.

Ruijie Reyee RG-NBF6002M e-Lighten Core Switch

Installation Guide



Copyright

Copyright © 2024 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 you purchase are subject to commercial contracts and terms, and some or all of the products, services, or features described in this document may not be available for you to purchase or use. Except for the agreement in the contract, Ruijie Networks makes no explicit or implicit statements or warranties with respect to 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 will be updated from time to time due to product version upgrades or other reasons, Ruijie Networks reserves the right to modify the content of the document without any notice or prompt.

This manual is designed merely as a user guide. Ruijie Networks has tried its best to ensure the accuracy and reliability of the content when compiling this manual, but it does not guarantee that the content of the manual is completely free of errors or omissions, and all the information 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

- 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. Signs

This document also uses signs to indicate some important points during the operation. The meanings of these signs are as follows:

 Caution


An alert that calls attention to safety instruction that if not understood or followed can result in personal injury.

 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.

 Note

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

 Instruction

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. Note

This manual provides installation steps, troubleshooting, technical specifications, and usage guidelines for cables and connectors. It is intended for users who want to understand the above and have extensive experience in network deployment and management, and assume that users are familiar with related terms and concepts.

Contents

Preface	1
1 Overview	1
1.1 About the RG-NBF6002M.....	1
1.2 RG-NBF6002M	2
1.2.1 Package Contents.....	2
1.2.2 Product Appearance	3
1.2.3 Hardware Specifications	4
1.2.4 Cooling	6
1.3 Power Module	7
1.3.1 Product Appearance	7
1.3.2 Hardware Specifications	7
1.4 Line Card.....	8
1.4.1 Package Contents.....	8
1.4.2 Product Appearance	8
1.4.3 Hardware Specifications	12
2 Preparing for Installation	15
2.1 Safety Guidelines.....	15
2.1.1 General Precautions	15
2.1.2 Chassis-Lifting Guidelines	15
2.1.3 Electricity Safety	15
2.1.4 Preventing ESD Damage.....	16
2.1.5 Laser Safety	16
2.2 Site Requirements	17

2.2.1 Floor Loading	17
2.2.2 Airflow.....	17
2.2.3 Space	17
2.2.4 Temperature and Humidity.....	17
2.2.5 Cleanliness.....	18
2.2.6 Grounding	19
2.2.7 Anti-Electromagnetic Interference.....	19
2.2.8 Surge Protection	19
2.2.9 EMI.....	20
2.2.10 Installation Site.....	20
2.3 Rack Requirements	20
2.4 Tools	21
3 Installing the Device	22
3.1 Installation Precautions.....	22
3.2 Installing the Device.....	22
3.2.1 Install the Device in the Rack	22
3.3 Installing and Removing a Power Module	23
3.3.1 Installing a Power Module.....	23
3.3.2 Removing a Power Module.....	24
3.4 Installing and Removing a Line Card.....	25
3.4.1 Installing a Line Card	25
3.4.2 Removing a Line Card	27
3.4.3 Troubleshooting a Line Card.....	28
3.4.4 Connecting the Grounding Cable	28

3.5 Connecting the Power Cable	29
3.6 Checklist After Installation	29
4 Log In to the Web Interface	30
5 Troubleshooting	31
5.1 Troubleshooting Flowchart	31
5.1 Common Faults	31
6 Appendix	33
6.1 Ports, Connectors, and Media	33
6.1.1 1000BASE-T/100BASE-TX/10BASE-T Ports	33
6.1.2 SFP Ports and SFP+ Ports	34
6.1.3 PON Ports and SC Ports	34
6.2 SFP and SFP+ Transceiver Modules	35
6.2.1 SFP Transceiver Modules	35
6.2.2 SFP+ Transceiver Modules	38
6.3 Surge Protection	41
6.3.1 Installing an AC Power Lightning Arrester	41
6.3.2 Installing an Ethernet Port Lightning Arrester	43
6.4 Recommended Cabling	45
6.4.1 Requirements for the Minimum Bend Radius of an Ethernet Cable	45
6.4.2 Requirement for the Minimum Bend Radius of an Optical Cable	45
6.4.3 Precautions for Bundling up Cables	45
6.5 Site Selection	48
6.6 Cleaning the Connectors and End Faces of Optical Cables	49

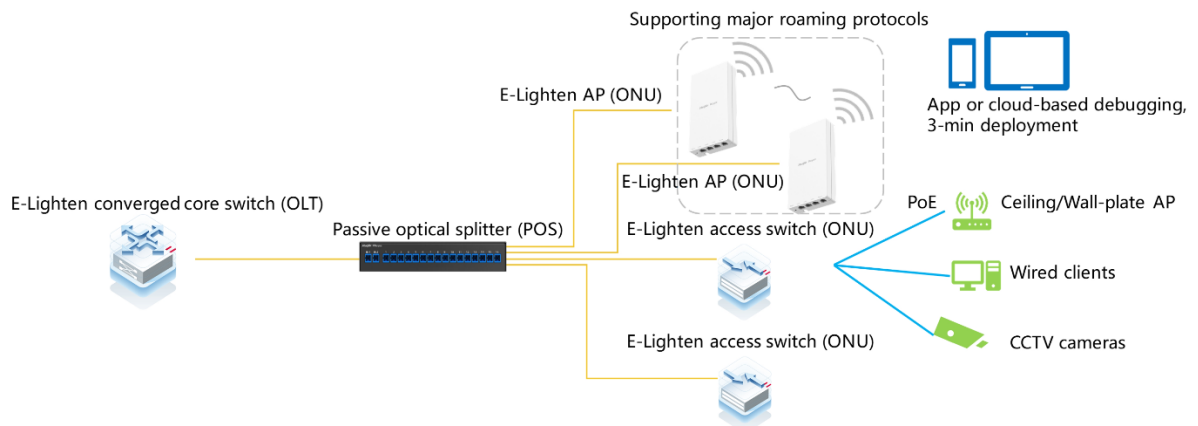
1 Overview

1.1 About the RG-NBF6002M

The Reyee e-Lighten Solution is a network product solution based on existing Ethernet technology integrating PON technology and passive optical splitting features. The components include:

- e-Lighten core switch (OLT): As a core switch, it has the Layer 3 data forwarding capability. It provides PON ports that can be connected to e-Lighten access switches and e-Lighten access points (APs) to achieve data interconnection.
- e-Lighten access switch (ONU): As an access device, the e-Lighten access switch is connected to the PON port in the uplink direction. It can send data to the core switch through the passive optical splitter.
- e-Lighten AP (ONU): An e-Lighten AP is connected to the PON port in the uplink direction, and can send wireless users' Internet access data to the core switch through the passive optical splitter.
- Passive optical distribution network (ODN): The ODN, consisting of passive optical splitters, is connected to the core switch in the uplink direction and to e-Lighten access switches or APs in the downlink direction.

Figure 1-1 Topology Diagram of Reyee e-Lighten Solution



The RG-NBF6002M switch, a core switch (OLT) launched by Ruijie Reyee, is designed for passive all-optical local area networks (LANs). It features an innovative management architecture and is compact, fitting two line cards within a 1U chassis. This switch is capable of supporting a hybrid setup, combining passive optical network (PON) line cards with traditional Ethernet line cards. Powered by Ruijie Reyee's proprietary operating system, the switch is versatile for various applications within small to medium-sized business settings. It is well-suited to meet the demands of ELV campus networks, office spaces, hotels, residential areas, and small to medium-sized enterprises.

Model	Description	Remarks
RG-NBF6002M	Chassis, purchased separately	Mandatory
MF6000M-24GT2XS	Line card, purchased separately	One or two line cards

Model	Description	Remarks
MF6000M-16GT8SFP2XS	Line card, purchased separately	can be configured on the switch.
MF6000M-16FS8GT2XS	Line card, purchased separately	
RG-PA150I-FS	Power module, purchased separately	Supports 1+1 redundancy

1.2 RG-NBF6002M

1.2.1 Package Contents

Note

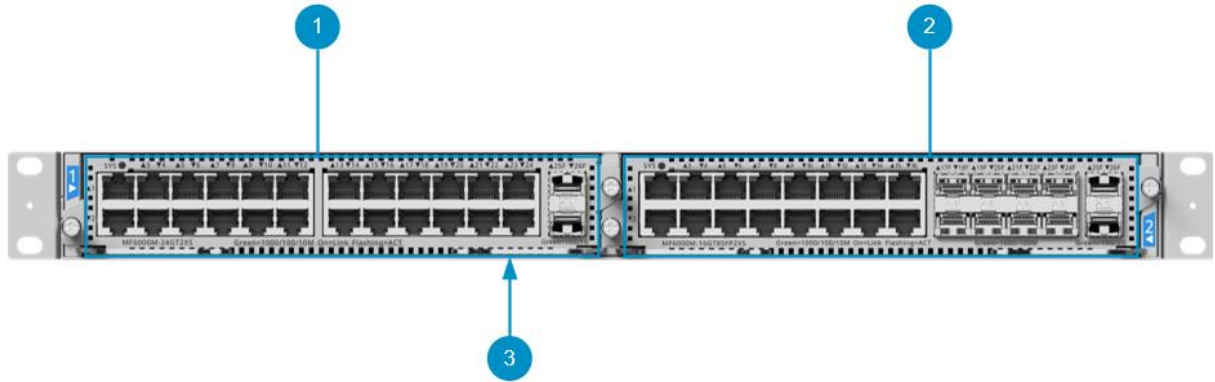
The package contents are subject to the purchase contract, and actual delivery may vary. Please check the items carefully against the package contents or purchase contract. If you have any questions, please contact your distributor.

Table 1-1 Package Contents of the RG-NBF6002M

No.	Item	Quantity
1	RG-NBF6002M switch	1
2	Power supply slot faceplate	1
3	Line card slot faceplate	1
4	M4 x 10 mm grounding screw	1
5	M4 x 8 mm screws	8
6	Rubber pads	4
7	Mounting brackets	2
8	Yellow/green grounding cable	1
9	User Manual	1
10	Warranty Card	1

1.2.2 Product Appearance

Figure 1-2 Front Panel of the RG-NBF6002M (with MF6000M-24GT2XS and MF6000M-16GT8SFP2XS Line Cards)

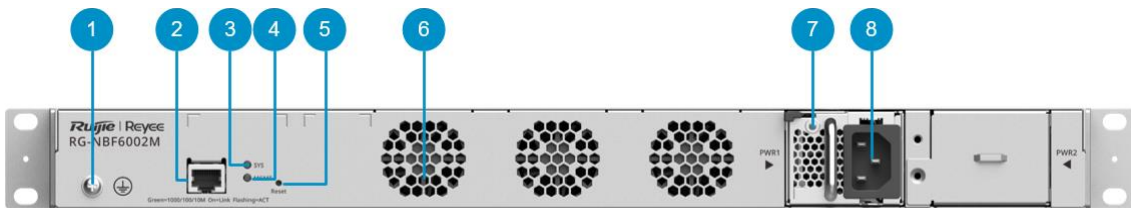


No.	Item	Description
1	Line card slot 1	For installing a line card.
2	Line card slot 1	For installing a line card.
3	Label	Located at the bottom of the device.

Warning

Before moving or transporting the chassis of the RG-NBF6002M series switches, remove the line cards and power modules from the chassis. Do not move or transport the chassis with the line cards and power modules installed.

Figure 1-3 Rear Panel of the RG-NBF6002M



No.	Item	Description
1	Grounding stud	Connects to the grounding cable.
2	Management port	A 10/100/1000BASE-T Ethernet port with an RJ45 connector. Network management port, for device configuration and firmware upgrade.
3	System LED	<ul style="list-style-type: none"> ● Solid green: The device is running properly. ● Blinking green (fast blinking: on for 0.0625s and off for 0.0625s): The

No.	Item	Description
		<p>device is starting up.</p> <ul style="list-style-type: none"> ● Blinking green (fast blinking: on for 0.25s and off for 0.25s): The device is restored to factory settings. ● Blinking green (slow blinking: on for 2s and off for 0.25s): The device is not connected to Ruijie Cloud. ● Blinking yellow (on for 1s and off for 1s): The device temperature reaches the warning threshold; the temperature cannot be read; there is another non-critical problem; or performance has deteriorated. ● Blinking red (one long blink and one short blink: on for 1s, off for 1s, on for 0.25s, and off for 1.75s): The power supply is faulty; a line card is faulty; a line card conflict occurs; or the line card is hot-swapped. ● Blinking red (one long blink, three short blinks: on for 1s, off for 1s, on for 0.25s, off for 0.25s, on for 0.25s, off for 0.25s, on for 0.25s, off for 1.75s, repeated): The main program is lost or damaged; other hardware faulty has occurred; or a specific function is abnormal. ● Off: The device is not receiving power.
4	Management port LED	<p>A 10/100/1000BASE-T port LED.</p> <ul style="list-style-type: none"> ● Solid green: A link is set up on the port at a rate of 1000 Mbps. ● Blinking green: A link is set up on the port at a rate of 1000 Mbps, and data is transmitted on the link. ● Off: No link is set up on the port.
5	Reset button	<ul style="list-style-type: none"> ● Press and hold for less than 2s: All modules will be reset. ● Press and hold for more than 5s: All modules will be reset, the initial password will be restored, and the supervisor module will be restored to factory settings and the configuration backup file will be saved. After the supervisor module is restarted, you can choose "Delete backup" or "Restore backup (with default password)" when logging in to the web interface of the device. If you do not log in to the web interface, the supervisor module is restored to factory settings. ● Press and hold for 2s to 5s: No action is triggered.
6	Fan module	Three fans for system cooling.
7	Power module status LED	<p>PWR1 and PWR2 power module status LED</p> <ul style="list-style-type: none"> ● Solid green: The power module is normal. ● Solid red: The power module is faulty. ● Off: The system has no power supply.
8	Power module	<p>Two power supply slots: PWR1 and PWR2.</p> <ul style="list-style-type: none"> ● Install the power modules before connecting the AC power cord. ● Power modules can work in 1+1 redundancy mode.

1.2.3 Hardware Specifications

Table 1-2 Hardware Specifications of the RG-NBF6002M

Model	RG-NBF6002M
CPU	Built-in CPU, single-core processor, clock speed of 1 GHz
Flash Memory	256 MB

SDRAM	DDRIII 1 GB
Number of Line Card Slots	2
Line Cards	MF6000M-24GT2XS MF6000M -16GT8SFP2XS MF6000M-16FS8GT2XS
Hot Swapping	Supported by power modules, but not by line cards.
Power Module	RG-PA150I-FS: 100 V AC to 240 V AC, 150 W
Power Module Redundancy	Supported. The power modules must be of the same model. (To improve the stability and reliability of the entire system, 1+1 power supply redundancy is recommended.)
Fan Module	Fixed fan
Certification	CE
Altitude	<ul style="list-style-type: none"> ● Long-term operating altitude: 50°C at 1800 m (5905.512 ft.). At altitudes between 1800 m (5905.512 ft.) and 5000 m (16404.2 ft.), the temperature decreases by 1°C (33.8°F) for every 220 m (721.78 ft.) increase in altitude. ● Maximum operating altitude: 5000 m (16404.2 ft.) ● Maximum storage altitude: 5000 m (16404.2 ft.)
Operating Temperature	0°C to 50°C (32°F to 122°F)
Storage Temperature	-40°C to +70°C (-40°F to +156°F)
Operating Humidity	10% to 90% RH (non-condensing)
MTBF	> 200,000 hours
Noise	≤ 60 dB at 25°C
Weight	5.4 kg (11.90 lbs.) (excluding line cards)
Dimensions (W x D x H)	442 mm x 460 mm x 44 mm (17.47 in. x 18.17 in. x 1.74 in.)

Note

The weight refers exclusively to the chassis. The overall weight of the device varies depending on the installed line cards.

Warning

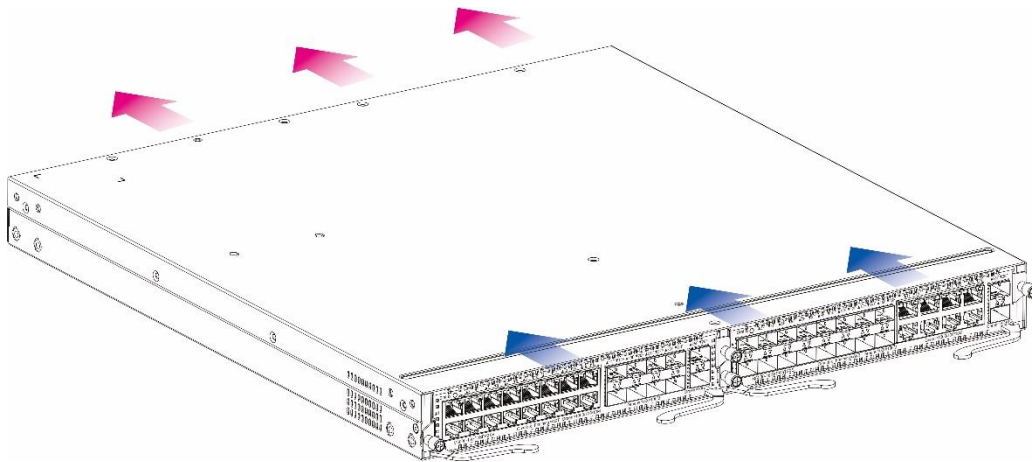
Operation of this equipment in a residential environment could cause radio interference.

⚠ Caution

- This equipment is not suitable for use in locations where children are likely to be present.
 - The switch has a built-in lithium battery to keep the real-time clock running when external power source is unavailable. To replace the lithium battery, please contact Ruijie Networks Customer Service Technical Support to have it replaced with a lithium battery of the same specifications.
 - Replacement of a battery with an incorrect type may cause fire and explosion, or compromise the safety features of the device. Replace the battery only with the same or equivalent type.
 - A battery subjected to extremely high temperature and/or low air pressure may result in an explosion or the leakage of flammable liquid or gas.
 - Disposal of a battery into a fire or by crushing or puncturing it can result in an explosion.
-

1.2.4 Cooling

The operating temperature range for the RG-NBF6002M switch is 0°C to 50°C (32°F to 122°F). Its heat dissipation design not only ensures the switch's reliability within this temperature range but also takes into account safety and ease of maintenance. The switch is equipped with fans for forced convection to maintain optimal performance and reliability in the specified operating conditions.



i Note

- Blue arrows: The air inlet direction of the line card and the power module.
 - Red arrows: The air outlet direction of the line card and the power module.
-

Line card/power module: The left, right, and front sides of the module are used for air intake, while the rear side is used for air exhaust. The fans draw air outward to create convection for heat dissipation.

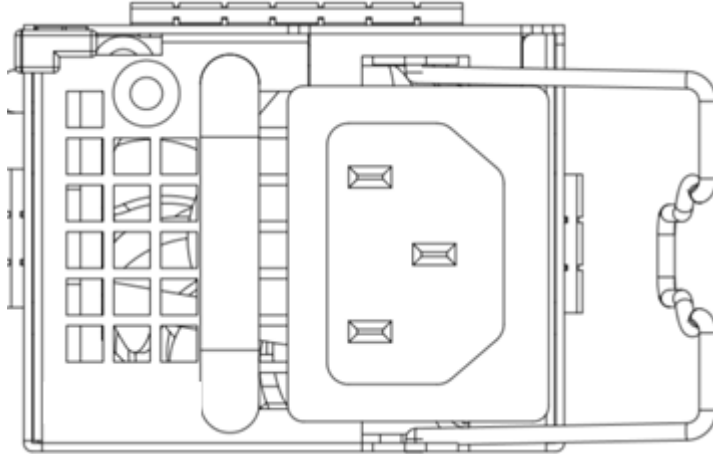
⚠ Caution

- Ensure sufficient space around the chassis for air circulation and space for the air intake vent and air exhaust (at least 10 cm). Ensure that there is adequate space around the chassis to allow for air circulation, as well as space for the air intake vent and air exhaust, with a minimum clearance of 10 cm (3.94 in.).
 - If a line card slot is not used, install a line card faceplate to the slot. If a power module slot is not used, install a power module faceplate to the slot. Faceplates should be correctly installed to the chassis slots to ensure proper airflow.
-

1.3 Power Module

1.3.1 Product Appearance

Figure 1-4 Appearance of the RG-PA150I-FS



1.3.2 Hardware Specifications

Table 1-3 Hardware Specifications of the RG-PA150I-FS

Model	RG-PA150I-FS
Rated Voltage Range	100 V to 240 V AC; 50 Hz to 60 Hz
Maximum Voltage Range	90 V to 264 V AC; 47 Hz to 63 Hz
Maximum Output Power	100 V AC to 240 V AC: 150 W
Input Current	< 3A @90 V to 264 V AC at full load
Leakage Current	< 3.5 mA @110 V AC and 220 V AC, 50 Hz to 60 Hz
Net Weight	0.55 kg (1.21 lbs.)
Power Cord Specification	10 A

⚠ Caution

- When connecting the power cord, ensure to fasten the latch securely to prevent any looseness.
- The power cord should be connected to an output socket which connects to the ground.
- Maximum operating altitude: 5000 m (16404.19 ft.); Maximum storage altitude: 5000 m (16404.19 ft.)

1.4 Line Card

1.4.1 Package Contents

Note

- This package contents applies to all line cards.
- The package contents are subject to the purchase contract, and actual delivery may vary. Please check the items carefully against the package contents or purchase contract. If you have any questions, please contact your distributor.

Table 1-4 Package Contents of a Line Card

No.	Item	Quantity
1	Line card	1
2	User Manual	1

1.4.2 Product Appearance

1. Appearance of the MF6000M-24GT2XS

Figure 1-5 Front Panel of the MF6000M-24GT2XS

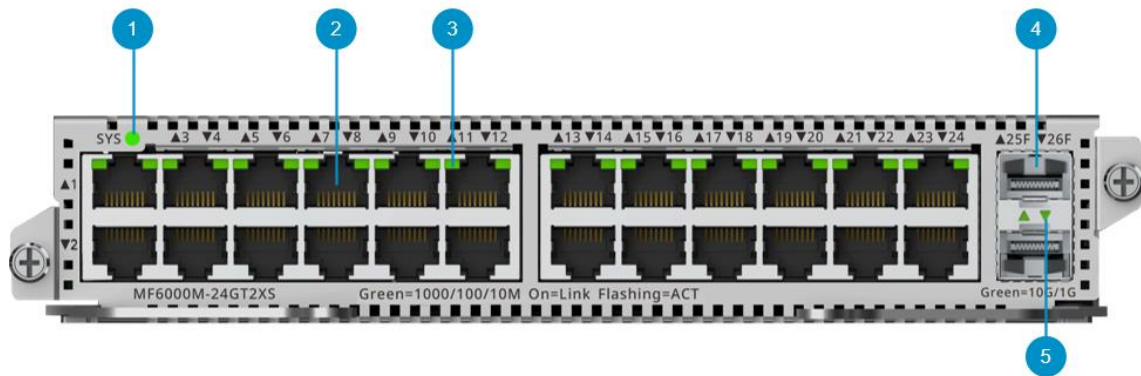


Table 1-5 Components on the Front Panel of the MF6000M-24GT2XS

No.	Component	Description
1	Line card status LED	<ul style="list-style-type: none"> ● Solid green: The line card is running normally. ● Blinking green (high frequency: on for 0.0625s and off for 0.0625s, repeated): The line card is starting up. ● Blinking green (medium frequency: on for 0.25s and off for 0.25s, repeated): The line card is resetting. ● Blinking green (medium frequency: on for 0.0625s and off for 0.0625s, repeated) with red system LED: A line card conflict or hot swapping has occurred. ● Off: The system is not receiving power, or is powered on but does not

No.	Component	Description
		run properly.
2	RJ45 port	24 x 10/100/1000BASE-T ports, with RJ45 connectors.
3	RJ45 port LED	24 x 10/100/1000BASE-T port status LEDs. <ul style="list-style-type: none"> ● Solid green: A link is set up on the port at a rate of 1000 Mbps. ● Blinking green: A link is set up on the port at a rate of 1000 Mbps, and data is transmitted on the link. ● Off: No link is set up on the port.
4	SFP+ port	2 x SFP+ ports. For supported optical transceivers, see 6.2 SFP and SFP+ Transceiver Modules .
5	SFP+ port LED	2 x SFP+ port status LEDs. <ul style="list-style-type: none"> ● Solid green: A link is set up on the port. ● Blinking green: A link is set up on the port, and data is transmitted on the link. ● Off: No link is set up on the port.

2. Appearance of the MF6000M-16GT8SFP2XS

Figure 1-6 Front Panel of the MF6000M-16GT8SFP2XS

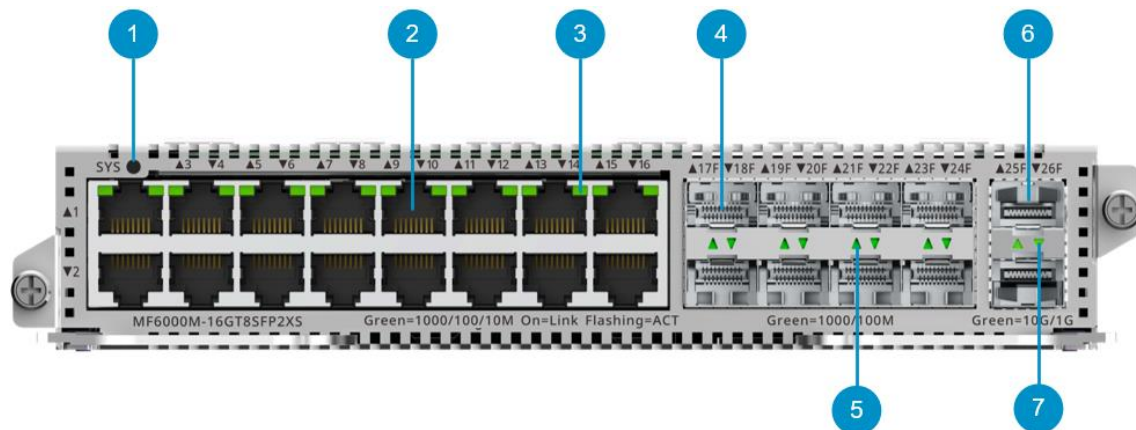


Table 1-6 Components on the Front Panel of the MF6000M-16GT8SFP2XS

No.	Component	Description
1	Line card status LED	<ul style="list-style-type: none"> ● Solid green: The line card is running normally. ● Blinking green (high frequency: on for 0.0625s and off for 0.0625s, repeated): The line card is starting up. ● Blinking green (medium frequency: on for 0.25s and off for 0.25s, repeated): The line card is resetting. ● Blinking green (medium frequency: on for 0.0625s and off for 0.0625s, repeated) with red system LED: A line card conflict or hot swapping has occurred. ● Off: The system is not receiving power, or is powered on but does not run properly.

No.	Component	Description
2	RJ45 port	16 x 10/100/1000BASE-T ports, with RJ45 connectors.
3	RJ45 port LED	16 x 10/100/1000BASE-T port status LEDs. <ul style="list-style-type: none"> ● Solid green: A link is set up on the port at a rate of 1000 Mbps. ● Blinking green: A link is set up on the port at a rate of 1000 Mbps, and data is transmitted on the link. ● Off: No link is set up on the port.
4	SFP port	8 x SFP ports. For supported optical transceivers, see 6.2 SFP and SFP+ Transceiver Modules .
5	SFP port LED	8 x SFP port status LED. <ul style="list-style-type: none"> ● Solid green: A link is set up on the port. ● Blinking green: A link is set up on the port, and data is transmitted on the link. ● Off: No link is set up on the port.
6	SFP+ port	2 x SFP+ ports. For supported optical transceivers, see 6.2 SFP and SFP+ Transceiver Modules .
7	SFP+ port LED	2 x SFP+ port status LED. <ul style="list-style-type: none"> ● Solid green: A link is set up on the port. ● Blinking green: A link is set up on the port, and data is transmitted on the link. ● Off: No link is set up on the port.

3. Appearance of the MF6000M-16FS8GT2XS

Figure 1-7 Front Panel of the MF6000M-16FS8GT2XS

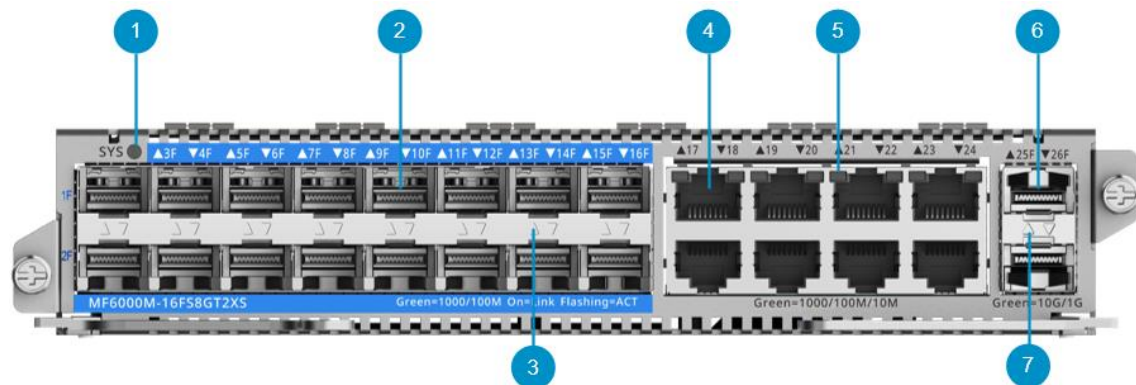


Table 1-7 Components on the Front Panel of the MF6000M-16FS8GT2XS

No.	Component	Description
1	Line card status LED	<ul style="list-style-type: none"> ● Solid green: The line card is running normally. ● Blinking green (high frequency: on for 0.0625s and off for 0.0625s, repeated): The line card is starting up.

No.	Component	Description
		<ul style="list-style-type: none"> ● Blinking green (medium frequency: on for 0.25s and off for 0.25s, repeated): The line card is resetting. ● Blinking green (medium frequency: on for 0.0625s and off for 0.0625s, repeated) with red system LED: A line card conflict or hot swapping has occurred. ● Off: The system is not receiving power, or is powered on but does not run properly.
2	SFP/PON port	16 x SFP/PON ports. For supported optical transceivers, see 6.2 SFP and SFP+ Transceiver Modules .
3	SFP/PON port LED	16 x SFP/PON port status LEDs. <ul style="list-style-type: none"> ● Solid green: A link is set up on the port. ● Blinking green: A link is set up on the port, and data is transmitted on the link. ● Off: No link is set up on the port.
4	RJ45 port	8 x 10/100/1000BASE-T ports, with RJ45 connectors.
5	RJ45 port LED	8 x 10/100/1000BASE-T port status LED. <ul style="list-style-type: none"> ● Solid green: A link is set up on the port at a rate of 1000 Mbps. ● Blinking green: A link is set up on the port at a rate of 1000 Mbps, and data is transmitted on the link. ● Off: No link is set up on the port.
6	SFP+ port	2 x SFP+ ports. For supported optical transceivers, see 6.2 SFP and SFP+ Transceiver Modules .
7	SFP+ port LED	2 x SFP+ port status LED. <ul style="list-style-type: none"> ● Solid green: A link is set up on the port. ● Blinking green: A link is set up on the port, and data is transmitted on the link. ● Off: No link is set up on the port.

1.4.3 Hardware Specifications

1. Hardware Specifications of the MF6000M-24GT2XS

Table 1-8 Hardware Specifications of the MF6000M-24GT2XS

Model	MF6000M-24GT2XS
Ports	24 x 10/100/1000BASE-T RJ45 ports, and 2 x SFP+ ports
Supported Optical Transceiver and Cable Types	<ul style="list-style-type: none"> ● See. 6.2 SFP and SFP+ Transceiver Modules Copper cables are not supported. ● The supported optical transceiver types may update without prior notification. Please contact Ruijie Networks for details.
System LED	SYS LED and Link/ACT LED
Hot Swapping	Not supported
Power Consumption	< 20.6 W
Certification	CQC
Operating Temperature	0°C to 50°C (32°F to 122°F)
Storage Temperature	-40°C to +70°C (-40°F to +158°F)
Operating Humidity	10% to 90% RH (non-condensing)
MTBF	> 200,000 hours
Net Weight	0.9 kg (1.98 lbs.)
Dimensions (W x D x H)	227 mm x 210 mm x 40.3 mm (8.94 in. x 8.27 in. x 1.59 in.)

2. Hardware Specifications of the MF6000M-16GT8SFP2XS

Table 1-9 Hardware Specifications of the MF6000M-16GT8SFP2XS

Model	MF6000M-16GT8SFP2XS
Ports	16 x 10/100/1000BASE-T RJ45 ports, 8 x SFP ports, and 2 x SFP+ ports
Supported Optical Transceiver and Cable Types	<ul style="list-style-type: none"> ● See 6.2 SFP and SFP+ Transceiver Modules. Copper cables are not supported. ● The supported module types may update without prior notification. Please contact Ruijie Networks for details.
System LED	SYS LED and Link/ACT LED
Hot Swapping	Not supported
Power Consumption	< 28.5 W
Certification	CQC
Operating Temperature	0°C to 50°C (32°F to 122°F)
Storage Temperature	-40°C to +70°C (-40°F to +158°F)
Operating Humidity	10% to 90% RH (non-condensing)
MTBF	> 200,000 hours
Net Weight	0.9 kg (1.98 lbs.)
Dimensions (W x D x H)	227 mm x 210 mm x 40.3 mm (8.94 in. x 8.27 in. x 1.59 in.)

3. Hardware Specifications of the MF6000M-16FS8GT2XS

Table 1-10 Hardware Specifications of the MF6000M-16FS8GT2XS

Model	MF6000M-16FS8GT2XS
Ports	16 x SFP/PON ports, 8 x 10/100/1000BASE-T RJ45 ports, and 2 x SFP+ ports
Supported Optical Transceiver and Cable Types	<ul style="list-style-type: none"> ● See 6.2 SFP and SFP+ Transceiver Modules. Copper cables are not supported. ● The supported module types may update without prior notification. Please contact Ruijie Networks for details.
System LED	SYS LED and Link/ACT LED
Hot Swapping	Not supported
Power Consumption	< 36.4 W
Certification	CQC
Operating Temperature	0°C to 50°C (32°F to 122°F)
Storage Temperature	-40°C to +70°C (-40°F to +158°F)
Operating Humidity	10% to 90% RH (non-condensing)
MTBF	> 200,000 hours
Net Weight	0.95 kg (2.09 lbs.)
Dimensions (W x D x H)	227 mm x 210 mm x 40.3 mm (8.94 in. x 8.27 in. x 1.59 in.)

2 Preparing for Installation

2.1 Safety Guidelines

Note

- To avoid personal injury or equipment damage, review the safety guidelines in this chapter before you begin the installation.
 - The following safety guidelines may not include all the potentially hazardous situations.
-

2.1.1 General Precautions

- Do not place the equipment in a wet area, and keep it away from liquid. Keep the chassis clean and dust-free.
- Keep the equipment away from heat sources.
- For the equipment that is installed in a cabinet, ensure that the cabinet and power distribution system are properly grounded.
- Do not place the equipment in walking areas.
- During installation and maintenance, do not wear loose clothing, jewelry, or any other objects that may hook onto the chassis.
- Do not place tools and accessories in walking areas.

2.1.2 Chassis-Lifting Guidelines

- Avoid moving the equipment frequently.
- Turn off all power supplies and disconnect all power cords before lifting or moving the equipment.
- Two or more people are required to lift the chassis. Keep balance and prevent personal injuries when lifting or moving the equipment.

2.1.3 Electricity Safety

CAUTION: DOUBLE POLE/NEUTRAL FUSING

Electric shock hazard! The fuse may be in the neutral, and that the mains shall be disconnected to de-energize the phase conductors.

- Observe local regulations and specifications when performing electrical operations. Only qualified personnel should handle these tasks.
- Any improper electrical operation can lead to accidents such as fires or electric shocks, causing severe, or even fatal damage to the human body and the equipment.
- Carefully check the work area for potential hazards, including ungrounded power system, insufficient grounding, and damp or wet ground.
- Direct or indirect touch through a wet object on high-voltage and mains supply can bring a fatal danger.

- Locate the emergency power supply switch in the room before installation. In the case of an accident, cut off the power supply immediately.
- Carefully inspect the equipment and the environment before powering on or off the equipment.
- Select the right leakage protector (also called “leakage current switch” or “leakage current breaker”) for the power supply system. This equipment automatically disconnects the power supply in the event of leakage and the risk of electric shock. A leakage protector should meet the following requirements:
 - The rated leakage action current of each leakage protector is greater than twice of the theoretical maximum leakage current of all the power supplies in the system. For example, if a system is equipped with 16 identical power supplies, and the leakage current of each power supply is equal to or less than 3.5 mA, then the leakage current of the system totals 56 mA. A leakage protector with a rated leakage action current of 30 mA supports no more than four power supplies (that is, action current of the leakage protector/2/Maximum leakage current of each power supply = $30/2/3.5 \approx 4.28$). In this case, 16 power supplies in the system require at least four leakage protectors with a rated action current of 30 mA, with each leakage protector supporting four power supplies. Although the number of power supplies in a system differs in models, the rated leakage action current of each leakage protector divided by two must be greater than the sum of the maximum leakage current of all the power supplies.
 - The rated leakage non-action current of a leakage protector should be 50% of the leakage action current. If the non-action current value is too small, the high sensitivity level can cause the circuit to break, leading to power cutoff and service interruption, even if the leakage current value is normal. For example, if a leakage protector has a rated leakage action current of 30 mA, the rated leakage non-action current should be 15 mA. The leakage protector will not activate unless the leakage current exceeds 15 mA.

 **Caution**

- To ensure personal safety, each leakage protector in the system must have a rated leakage action current equal to or below 30 mA, which is the recognized safety threshold for human body current. If the total leakage current of the system exceeds twice the 30 mA limit, the system must be equipped with two or more leakage protectors to maintain safety.
 - The leakage current values vary with products. For the leakage current value of each product model, see the product technical specifications.
-

2.1.4 Preventing ESD Damage

- Properly ground both the equipment and the installation site.
- Keep the site as dust free as possible.
- Maintain appropriate humidity conditions.
- Before installing or maintaining the equipment, wear an anti-ESD wrist strap and make sure that it is properly grounded.
- Avoid contact between the printed circuit boards and clothing. The anti-ESD wrist strap only protects the printed circuit boards from ESD voltages on the body. ESD voltages on clothing can still cause damage.

2.1.5 Laser Safety

An equipment with an optical port usually supports multiple types of optical transceivers, all of which are Class I laser products. Pay attention to the following during the use of optical transceivers:

- When an optical transceiver is in operation, ensure that its port is connected to an optical fiber or covered by

a dust cap to keep out dust and prevent it from burning your eyes.

- When an optical transceiver is in operation, do not look into its port after removing the optical fiber. Doing so may result in eye injury.

⚠ Caution

Do not approach or look directly into any optical port under any circumstances. This may cause permanent damage to your eyes.

Figure 2-1 Laser Product Warning



2.2 Site Requirements

To ensure the normal operation and prolonged service life of the equipment, it is essential to install it indoors in a location that meets the following requirements.

2.2.1 Floor Loading

Assess the combined weight of the equipment and its accessories, including the cabinet, chassis, and power supply, and verify that the installation site meets the necessary specifications.

2.2.2 Airflow

To ensure that the equipment works properly in the specified environment, a minimum clearance of 100 mm (3.94 in.) must be maintained around the equipment to ensure proper ventilation. Manage the Ethernet cables and power cords using cable ties or cable management brackets to avoid blocking air intakes. You are advised to dust the equipment at an interval of three months to avoid blocking the ventilation openings.

2.2.3 Space

Ensure that indoor pathways are at least 0.8m (31.50 in.) wide to allow for proper chassis handling and module swapping.

Maintain a minimum clearance of 0.4m (15.75 in.) around the equipment for heat dissipation and equipment maintenance.

2.2.4 Temperature and Humidity

For optimal equipment performance and extended service life, it is essential to maintain ambient temperature and humidity conditions. Prolonged exposure to excessively high or low temperature and humidity can potentially cause damage to the equipment.

- When exposed to high relative humidity, insulating materials may exhibit poor insulation capabilities, increasing the risk of electrical leakage. Furthermore, high humidity can cause mechanical changes in materials and corrosion of metallic components.
- When exposed to low relative humidity, the insulating strip may dry out and shrink, increasing the risk of static

electricity generation. This static electricity can pose a danger to the circuits inside the equipment.

- In a dry environment, static electricity is prone to occur and damage the internal circuits of the equipment.
- High temperature environments can be detrimental to the equipment, leading to reduced performance and a shorter service life. Prolonged exposure to elevated temperatures can expedite the equipment's aging process.

Note

The ambient temperature and humidity of the equipment are measured 1.5 m (59.06 in.) above the floor and 0.4 m (15.75 in.) before the equipment rack when there is no protective plate in front or at the back of the rack.

2.2.5 Cleanliness

Dust poses a major threat to the running of the equipment. The buildup of dust on the equipment can result in static electricity, causing poor contact between the metallic joints. Dust buildup is more likely to occur in environments with low relative humidity, which not only impacts the service life of the equipment but also increases the likelihood of communication failure. The following table shows the specifications for dust concentration and particle size in the equipment room.

Table 2-1 Requirements for Dust

Particle Size	Unit	Concentration
≥ 0.5 μm	Particles/m ³	≤ 3.5×10 ⁶
≥ 5 μm	Particles/m ³	≤ 3.5×10 ⁴

Apart from dust, the salt, acid, and sulfide in the air of the machine room must also meet strict requirements. These harmful substances will accelerate metal corrosion and component aging. Therefore, the machine room should be properly protected against the intrusion of harmful gases, such as sulfur dioxide, hydrogen sulfide, nitrogen dioxide, and chlorine gas. The following table lists limits for harmful gases.

Table 2-2 Requirements for Gases

Gas	Average (mg/m ³)	Maximum (mg/m ³)
Sulfur dioxide (SO ₂)	0.3	1.0
Hydrogen sulfide (H ₂ S)	0.1	0.5
Nitrogen dioxide (NO ₂)	0.5	1.0
Chlorine gas (Cl ₂)	0.1	0.3

Note

"Average" indicates the typical level of exposure over a one-week period. "Maximum" refers to the highest allowable exposure level within a week, with this level being sustainable for no more than 30 minutes per day.

2.2.6 Grounding

A proper grounding system is crucial for ensuring stable and reliable operation of the equipment, as well as preventing lightning strikes and interference. To ensure proper grounding, carefully check the grounding conditions at the installation site according to the grounding specifications, and complete grounding properly based on the actual situation.

- Safety Grounding

Ensure that the installation site and power distribution system are securely grounded if the equipment uses the AC power supply. Failure to do so may result in an increased risk of electric shock, particularly when the insulation resistance between the power module and the chassis decreases.

 **Caution**

- Adopt grounding protection connections in buildings so that the equipment can be connected to the protective grounding system.
 - Verify that the AC socket is reliably connected to the protective grounding system of the building. If not, a protective grounding wire should be used to connect the protective grounding lug of the AC socket to the protective grounding system of the building.
 - The cross-sectional area of the protective grounding wire should be at least 0.75 mm² (18 AWG).
-

- Lightning Grounding

The lightning protection system of facilities is standalone, and is composed of a lightning rod, a down conductor, and a connector connected to the grounding system. The grounding system is usually used for power reference grounding and safety grounding of the installation site. Lightning grounding is required only for facilities and is not required for the equipment.

- EMC Grounding

Grounding required for electromagnetic compatibility includes shielded grounding, filter grounding, noise and interference suppression, and level reference, which contribute to the overall grounding requirements. The grounding resistance should be smaller than 1 ohm, and the grounding terminals of the rack should be grounded before the running of the equipment.

2.2.7 Anti-Electromagnetic Interference

- Take effective measures to prevent interference from power grid to the power supply system.
- Keep the equipment away from the grounding system or lightning protection grounding system of the power facility.
- Keep the equipment far away from high-frequency current equipment such as high-power radio transmitting stations and radar launchers.
- Take electromagnetic shielding measures when necessary.

2.2.8 Surge Protection

- Ensure that the neutral point of the AC power socket is in good contact with the ground.
- Install a power arrester in front of the power input end to enhance surge protection for the power supply.
- When an AC power cord is introduced from outdoors and directly connected to the power port of the equipment, the AC power port must be connected to an external lightning protection power strip to protect the equipment against lightning strokes. Connect the mains supply AC power cord to the lightning protection

power strip, and then connect the equipment to the lightning protection power strip. This prevents high-voltage lightning from directly passing through the equipment over the mains supply AC power cord.

Note

- The lightning protection power strip is not delivered with the equipment. Purchase it as required.
 - For details on how to use the lightning protection power strip, see the related user guide.
-

2.2.9 EMI

All interference sources, either from outside or inside of the equipment or application system, affect the equipment by capacitive coupling, inductive coupling, or electromagnetic waves. Electromagnetic interference (EMI) occurs due to electromagnetic radiation or conduction, depending on the transmission path. When the energy, often RF energy, from a component arrives at a sensitive component through the space, the energy is known as radiated interference. The interference source can be either a part of the interfered system or a completely electrically isolated unit. Conduction interference occurs when interference is transferred from one unit to another unit through cables, which are usually electromagnetic wires or signal cables connected between the source and the sensitive component. Conduction interference often affects the power supply of the equipment, but can be controlled by a filter. Radiated interference may affect any signal path in the equipment, and is difficult to shield.

- Take interference prevention measures for the power supply system.
- Keep the equipment away from the grounding system or lightning protection grounding system of the power facility.
- Keep the equipment far away from high-frequency current equipment such as high-power radio transmitting stations and radar launchers.
- Take electromagnetic shielding measures when necessary.

2.2.10 Installation Site

Regardless of whether the equipment is installed in a rack, on a workbench or on a wall, the following conditions must be met:

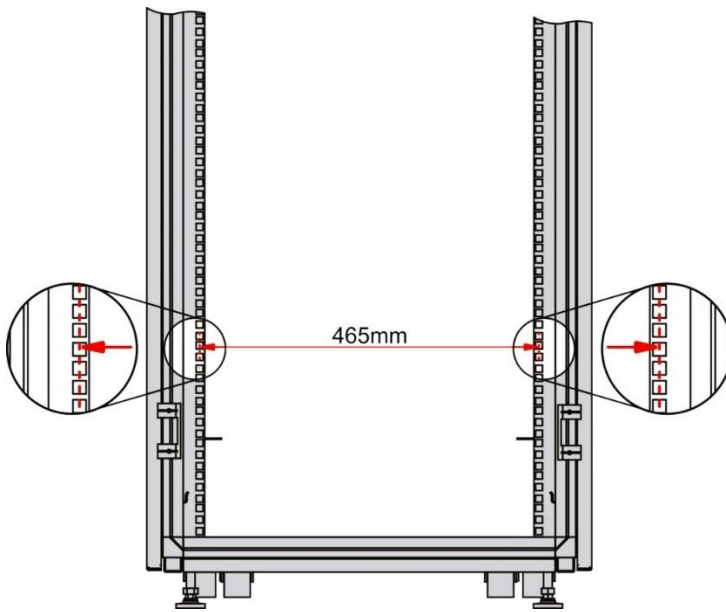
- Maintain a proper clearance around air vents for heat dissipation.
- The equipment is equipped with fans to draw air from front and left and right sides to rear. Maintain a minimum clearance of 150 mm (5.91 in.) around the ventilation openings for heat dissipation. Install the equipment in a standard 19-inch rack, or place it on a clean workbench. In hot areas, air-conditioning is recommended.
- The installation site has good cooling and ventilation.
- The installation site is sturdy enough to support the weight of the equipment and its accessories.
- The installation site is properly grounded.

2.3 Rack Requirements

If you plan to install the equipment in a rack, ensure that the rack meets the following conditions.

- (1) Use a four-post 19-inch cabinet.
- (2) The left and right square-hole rack posts are 465 mm (18.31 in.) apart.

Figure 2-2 19-Inch Rack



- (3) The square-hole rack post is at least 180 mm (7.09 in.) from the front door, and the front door is at most 25 mm (0.98 in.) thick. This ensures an available clearance of at least 155 mm (6.10 in.). The rack depth (distance between front and rear doors) is at least 1000 mm (39.37 in.).
- (4) The guide rails can bear the weight of the equipment and its accessories.
- (5) The cabinet has a reliable grounding terminal for the chassis to connect to earth ground.
- (6) The cabinet has a good ventilation system. The open area of front and rear doors is greater than 50%.

2.4 Tools

Table 2-3 Tools

Common Tools	Phillips screwdriver, power cords, Ethernet cables, cage nuts, diagonal pliers, and cable ties
Special Tools	Anti-ESD gloves, wire stripper, crimping plier, RJ45 crimping plier, and wire cutter
Meters	Multimeter

Note

The equipment is delivered without a toolkit. Prepare the preceding tools by yourself.

3 Installing the Device

Caution

Before installing the device, ensure that guidelines and requirements in Chapter 2 have been met.

3.1 Installation Precautions

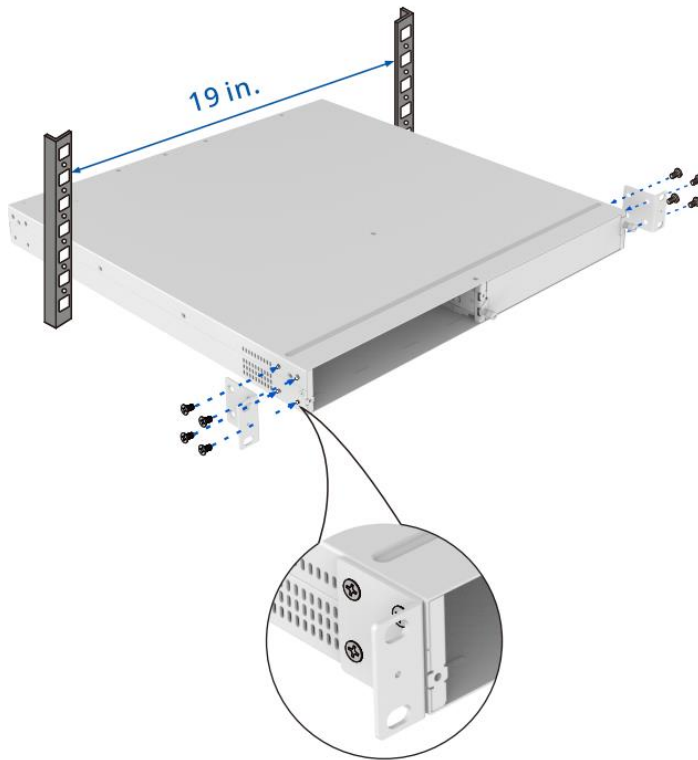
- Pay attention to the following points during installation:
- Connect the power cords of different colors to the corresponding cable terminals.
- Ensure that the connector of the power cord is properly seated in the power port of the device.
- Do not place any objects on the device.
- Maintain a minimum clearance of 100 mm (3.94 in.) around the device to ensure proper airflow. Do not stack switches.
- Keep the device away from high-power radio transmitting stations, radar transmitting stations, and high-frequency high-current devices. If necessary, use electromagnetic shielding methods, such as electromagnetic shielding for interface cables.
- Manage Ethernet cables with a distance of 100 meters (328.08 feet) indoors. Take lightning protection measures if they need to be routed outdoors.

3.2 Installing the Device

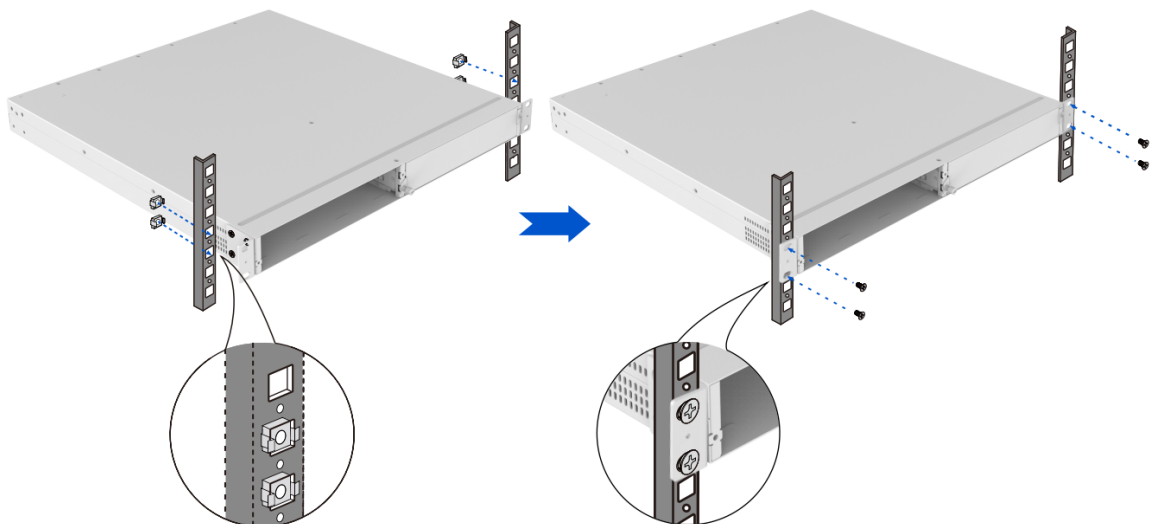
3.2.1 Install the Device in the Rack

The device meets the EIA standard, and can be installed in a standard 19-inch rack.

- (1) Use eight M4 x 8 mm screws to fix the mounting brackets to the left and right sides of the device.



- (2) Place the device horizontally in the rack, and secure it to the rack using the M6 screws and cage nuts (customer supplied).



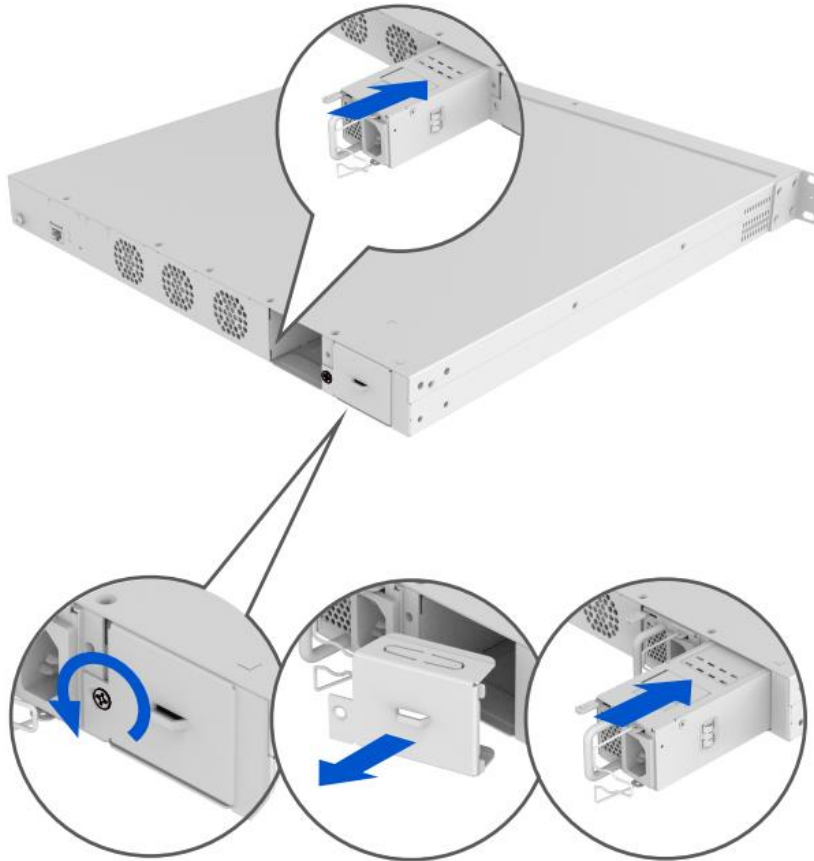
3.3 Installing and Removing a Power Module

3.3.1 Installing a Power Module

- (1) Unpack the power module, and verify that the power input specifications meet requirements.

- (2) Remove the power supply slot faceplate. The plane with the power module label is the top side. Hold the handle of the power module with one hand and hold the bottom of the power module with the other hand. Slowly insert the power module along the guide rail until it is fully inserted into the chassis and you hear a click. Ensure that the power module is in good contact with the power module slot.

Figure 3-1 Installing the RG-PA150I-FS Power Module

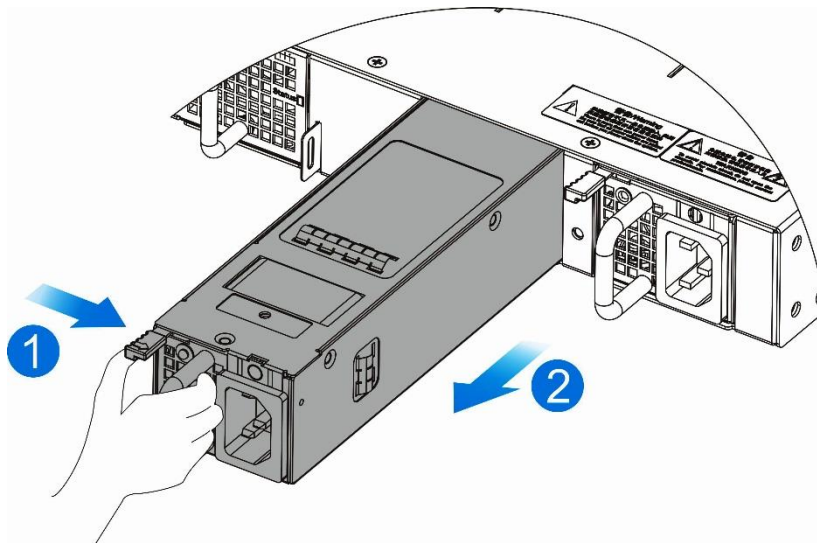


! Warning

- Before installing a power module, ensure that the power switch of the power module is off, and the power cord is not connected to the power socket of the power module. Otherwise, it may cause electric shock to the operator or damage the device.
 - When inserting the power module, apply a gentle force and insert it smoothly. If it is difficult to insert the power module in place, do not apply too much force. Instead, remove the power module, align it with the opening on the rear panel of the device, and then insert it again. Otherwise, the power module may be damaged.
-

3.3.2 Removing a Power Module

- (1) Press the latch on the power module and grasp the handle with one hand. Place your other hand under the module to support its weight. Pull the module fully out of the slot.
- (2) Install the power supply slot faceplate in the power module slot and put the removed power module into its package.

Figure 3-2 Removing the RG-PA150I-FS Power Module

Warning

- Before removing the power module, make sure that the power cord of the corresponding power module is not connected to the power outlet of the power module. Otherwise, it may cause electric shock to the operator or damage the device.
 - When removing the power module, apply a gentle force and ensure that the power module is smoothly removed. If it is difficult to remove the power module, do not apply too much force. Check whether the power module is aligned with the opening edge on the rear panel of the device. Otherwise, the power module may be damaged.
 - Install a faceplate or a power module in the unused power supply slot.
-

3.4 Installing and Removing a Line Card

For the list of supported line cards, see [Line Card](#).

Note

In this section, the line card is installed without power supply.

3.4.1 Installing a Line Card

When installing a line card, wear an ESD wrist strap. The metal part of the ESD wrist strap should be in full contact with your skin. For safety reasons, do not touch any components on the line card.

Caution

- Do not hold the edges of the printed circuit board or touch any components on the board.
 - When inserting or removing a line card, use the ejector levers on both sides of the faceplate.
-

1. Select a Line Card Slot

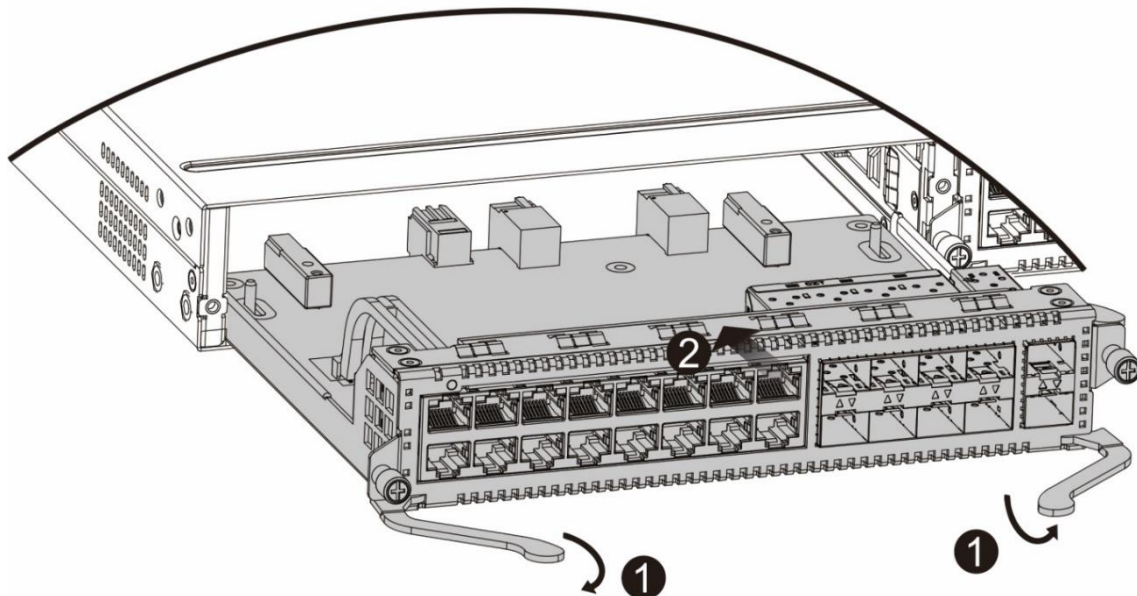
Line cards can be installed in any line card slot of the device. If you want to replace a line card or install an existing line card in another line card slot, you need to reset the device first. Before installing a line card, remove the faceplate of the corresponding slot.

2. Installing a Line Card

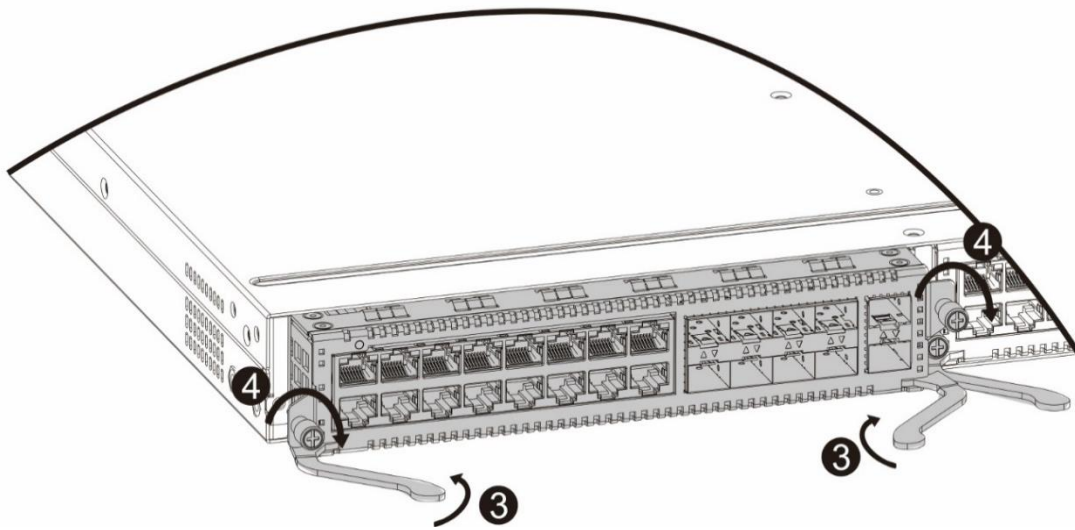
Procedure:

- (1) (Optional) Remove the faceplate.
- (2) Open the ejector lever of the line card to be installed (as marked by 1 in the following figure).
- (3) Align the line card with the guide rail in the slot, and gently push the line card into the slot horizontally (as marked by 2 in the following figure).

Figure 3-3 Installing the RG-NBF6002M Line Card — 1



- (4) Push the ejector levers inward (as marked by 3 in the following figure);
- (5) Tighten the captive screws at both ends of the faceplate (as marked by 4 in the following figure);

Figure 3-4 Installing the RG-NBF6002M Line Card — 2

! Warning

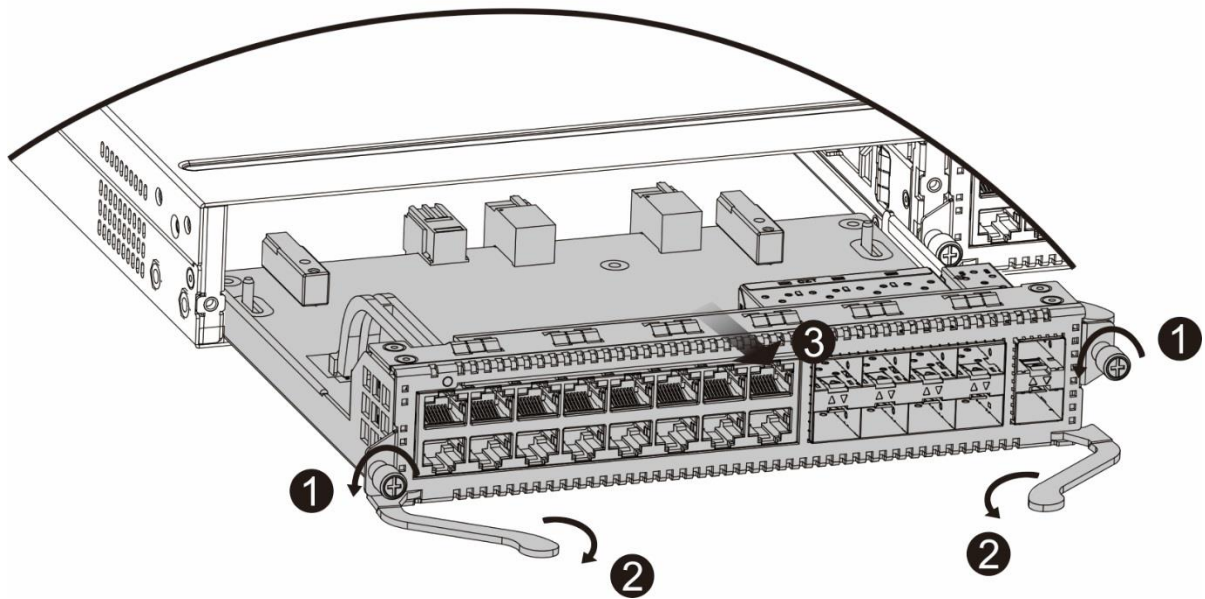
When performing steps (2), (3), and (4), apply a gentle force and insert the line card smoothly. If it is difficult to push the line card, do not apply too much force. Instead, remove the line card and check whether the line card is aligned with the opening edge of the line card slot on the front panel of the device before proceeding. Otherwise, the line card may be damaged.

3.4.2 Removing a Line Card

Procedure:

- (1) Use a screwdriver to loosen the captive screws (as marked by 1 in the following figure) of the line card.
- (2) Push the ejector levers on both sides of the line card outward (as marked by 2 in the following figure).
- (3) Remove the line card horizontally (as marked by 3 in the figure below) and place it in the line card package.

Figure 3-5 Removing the RG-NBF6002M Line Card



⚠ Caution

- Line cards do not support hot swapping. Before removing a line card, power off the device first.
 - After the line card is removed, if you do not need to install a new line card, install a faceplate to prevent dust from entering and to ensure normal ventilation of the device.
-

⚠ Warning

When removing the line card, keep a certain distance from the aisle of the work room to prevent passers-by from knocking off the removed line card or to avoid accidents due to the collision during the removal process.

3.4.3 Troubleshooting a Line Card

If the installed line card does not work properly, check the following points:

- Check whether Ethernet cables of the line card are correct.
- Observe each port LED of the line card to check whether the line card is working properly.
- Connect your PC to the MGMT port of the switch, and check whether the line card is configured correctly and works properly.

3.4.4 Connecting the Grounding Cable

⚠ Warning

- To avoid personal injury and device damage, connect the switch to earth ground properly.
 - The resistance between the switch chassis and the ground must be less than 1 Ω.
 - The O&M personnel should check whether the AC outlet is properly connected to the protective ground of the building. If not, the O&M personnel should use a protective earth conductor from the AC outlet protective earth lug to the building protective earth.
 - The power socket should be installed near the device and should be easily accessible.
-

- During device installation, connect the grounding cable first and disconnect it last.
 - The cross-sectional area of a protective grounding cable should be at least 2.5 mm² (12 AWG).
-

A proper grounding system is crucial for ensuring stable and reliable operation, as well as preventing lightning strikes and interference.

- The grounding wire must be a good conductor with a cross-sectional area determined by the maximum current load.
- Do not use bare wire.
- To ensure personal and device safety, the switch must be properly grounded. The resistance between the switch chassis and the ground must be less than 1 Ω.

Procedure:

- (1) Remove the grounding lug at the back of the device.
- (2) Use the removed grounding lug to secure one end of the grounding cable to the chassis. Similarly, connect the other end of the grounding cable to the rack grounding cable or the equipment room grounding bar.

3.5 Connecting the Power Cable

Warning

Use the delivered power cords. Otherwise, security accidents may occur.

Procedure:

- (1) Ensure that the circuit breaker switch on the power supply side is off. Plug one end of the power cord that comes with the device into the power outlet on the rear panel of the chassis and the other end into the AC power outlet.
- (2) Turn on the circuit breaker on the power supply side.
- (3) Check whether the power LED on the front panel of the device is on. If the LED is on, the power supply is connected correctly.

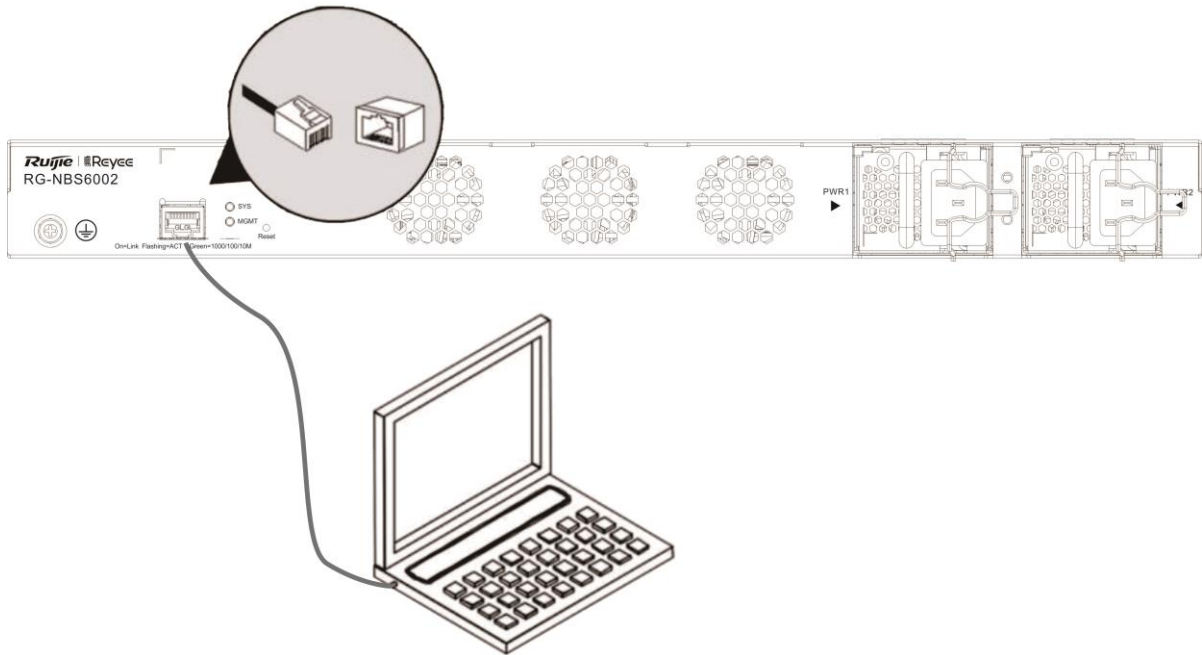
3.6 Checklist After Installation

- The device is securely installed.
- The power cord meets the requirements.
- The rack is properly grounded.
- The device is correctly connected to the terminal or other equipment.
- The power cord is long enough to avoid over-extension.

4 Log In to the Web Interface

- (1) Connect your PC to the MGMT port of the device using an Ethernet cable, as shown in the following figure.

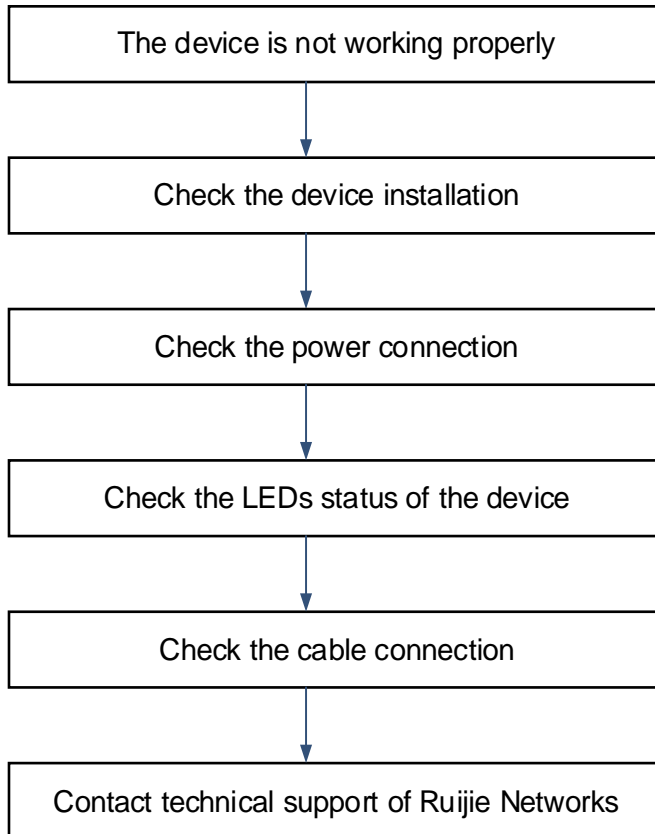
Figure 4-1 Setting Up the Configuration Environment



- (2) Configure your PC with an IP address on the network of 10.44.77.XXX (Range: 1-255, excluding 200).
- (3) Open a browser on the PC and enter 10.44.77.200 to log in to the system configuration page. (The default password is **admin** when you log in to the device for the first time. To ensure security, you are advised to change the password after login, and update the password regularly.)
- (4) Perform device debugging based on service requirements.

5 Troubleshooting

5.1 Troubleshooting Flowchart



5.1 Common Faults

Fault Symptom	Possible Cause	Solution
The login password cannot be retrieved.	The login password is forgotten after being configured.	Press and hold the reset button for over five seconds to reset your username and password.
The SYS LED is off after the switch is powered on.	No power is supplied to the switch or the power cord is loose.	Check whether the power socket in the equipment room is normal, and whether the power cord connected to the switch is loose.
An RJ45 port is disconnected or a frame sending/receiving error occurs.	The twisted pair cable is not connected properly. The cable length exceeds 100 m (328.08 feet). The port is specially configured	Replace the twisted pair cable. Use optical cables or connect to an intermediate switch for relay. Make sure that the port works in the same mode as the interconnected switch.

	<p>and does not use the same work mode as the interconnected switch.</p>	
<p>An optical port cannot be connected.</p>	<p>The receiving and transmitting ends are connected incorrectly.</p> <p>The types of the interconnected optical transceivers do not match.</p> <p>The optical cable type does not meet requirements.</p> <p>The length of the optical cable length is beyond the allowed length marked on the optical transceiver.</p> <p>The optical cable or optical connector is contaminated.</p>	<p>Exchange the transmitting and receiving ends of the optical cable.</p> <p>Replace the optical transceiver with another one of the same type.</p> <p>Replace the optical cable with a qualified one.</p> <p>Use an optical cable with the required length.</p> <p>Use a clean cloth or a cleaning pen to clean the end face.</p>

6 Appendix

6.1 Ports, Connectors, and Media

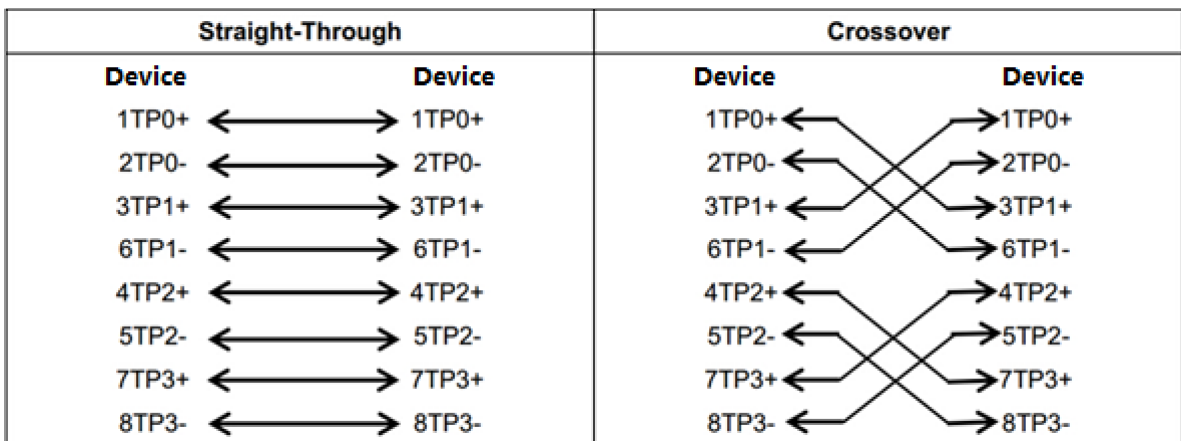
6.1.1 1000BASE-T/100BASE-TX/10BASE-T Ports

1000BASE-T/100BASE-TX/10BASE-T ports are Ethernet ports with auto-negotiation of three speeds: 10 Mbps, 100 Mbps, and 1000 Mbps. They supports auto MDI/MDIX Crossover, and use RJ 45 connectors.

Compliant with the IEEE 802.3ab standard, a 1000BASE-T port requires 100-ohm Category 5 or 5e unshielded twisted pair (UTP) or shielded twisted pair (STP) (recommended) cables, and supports a maximum distance of 100 meters (328 feet).

A 1000BASE-T port requires all four pairs of wires to be connected for data transmission. [Figure 6-1](#) shows the four pairs of wires for the 1000BASE-T port.

Figure 6-1 1000BASE-T Twisted Pair Connections



100BASE-TX/10BASE-T ports can be interconnected using cables of the preceding specifications. In addition, a 10BASE-T port can be connected using 100-ohm Category 3, Category 4, and Category 5 cables, while a 100BASE-TX port can be connected using 100-ohm Category 5 cables, and supports a maximum distance of 100 meters (328 feet). [Table 6-1](#) shows 100BASE-TX/10BASE-T pin assignments.

Table 6-1 100BASE-TX/10BASE-T Pin Assignments

Pin	Socket	Plug
1	Input Receive Data+	Output Transmit Data+
2	Input Receive Data-	Output Transmit Data-
3	Output Transmit Data+	Input Receive Data+
6	Output Transmit Data-	Input Receive Data-
4, 5, 7, 8	Not Used	Not Used

Figure 6-2 shows the connection of straight-through and crossover cables for 100BASE-TX/10BASE-T ports.

Figure 6-2 100BASE-TX/10BASE-T Twisted Pair Connections

Straight-Through		Crossover	
Device	Adapter	Device	Device
1 IRD+	1 OTD+	1 IRD+	1 IRD+
2 IRD-	2 OTD-	2 IRD-	2 IRD-
3 OTD+	3 IRD+	3 OTD+	3 OTD+
6 OTD-	6 IRD-	6 OTD-	6 OTD-

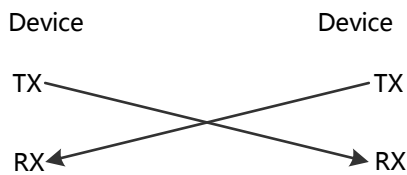
6.1.2 SFP Ports and SFP+ Ports

SFP ports and SFP+ ports require optical transceivers or Ethernet transceivers.

- Optical transceivers for SFP and SFP+ ports use LC connectors and connect to the peer end via an optical cable.
- SFP Ethernet transceivers use RJ45 connectors and connect to the remote end via an Ethernet cable.

Select either single-mode or multi-mode optical cables depending on the optical transceiver type. Figure 6-3 shows the optical cable connection. Note that the TX on the local end should connect to the RX on the peer end, and the RX on the local end should connect to the TX on the peer end.

Figure 6-3 Optical Cable Connections

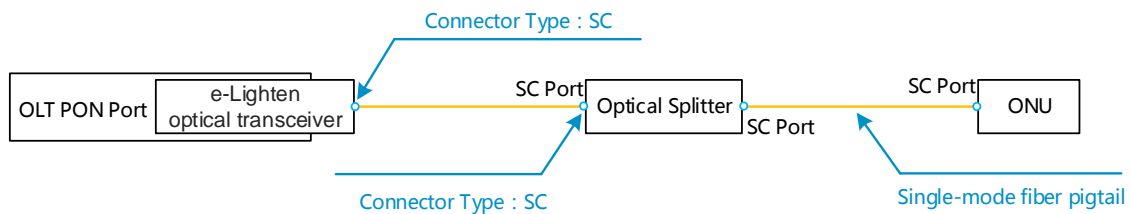


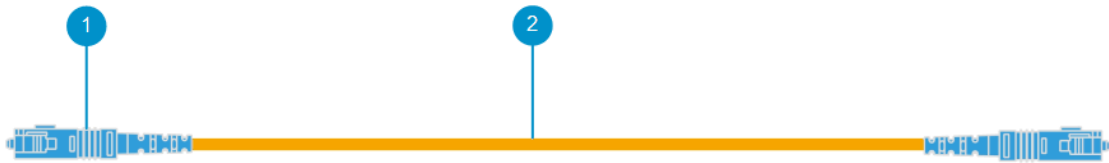
6.1.3 PON Ports and SC Ports

Figure 6-4 shows the PON ports and SC ports on equipment in Ruijie Reyee e-Lighten Optical Solution.

- PON ports on the OLT require e-Lighten optical transceivers with SC connectors, which are connected to an optical splitter using single-mode pigtails.
- SC ports on optical splitters and ONUs use SC connectors, and are interconnected using single-mode pigtails.

Figure 6-4 PON Port and SC Port Connections





No	Description
1	SC connector
2	Single-mode pigtail

6.2 SFP and SFP+ Transceiver Modules

We provide SFP and SFP+ transceiver modules according to the port types. You can select the module to suit your specific needs. An SFP transceiver module can be a 1GE optical transceiver or Ethernet transceiver (Mini-GBIC-GT), while an SFP+ transceiver module is a 10GE optical transceiver. The following models and technical specifications of some SFP and SFP+ transceiver modules are listed for your reference.

6.2.1 SFP Transceiver Modules

Table 6-2 Models and Specifications of SFP Optical Transceiver Modules

Model	Wavelength (nm)	Optical Cable Type	DDM (Yes/No)	Transmit Power (dBm)		Receive Power (dBm)	
				Min.	Max.	Min.	Max.
MINI-GBIC-SX-MM850	850	MMF	No	-9.5	-3	-17	0
MINI-GBIC-LX-SM1310	1310	SMF	No	-9.5	-3	-20	-3
MINI-GBIC-LH40-SM1310	1310	SMF	Yes	-2	3	-22	-3
GE-SFP-LX20-SM1310-BIDI	1310TX/1550RX	SMF	Yes	-9	-3	-20	-3
GE-SFP-LX20-SM1550-BIDI	1550TX/1310RX	SMF	Yes	-9	-3	-20	-3
GE-SFP-LH40-SM1310-BIDI	1310TX/1550RX	SMF	Yes	-5	0	-24	-1
GE-SFP-LH40-SM1550-BIDI	1550TX/1310RX	SMF	Yes	-5	0	-24	-1
MINI-GBIC-ZX80-SM1550	1550	SMF	Yes	0	4.7	-22	-3
MINI-GBIC-ZX100-SM1550	1550	SMF	Yes	0	5	-30	-9
SFP-MM850	850	MMF	No	-9.5	-3	-17	0

Model	Wavelength (nm)	Optical Cable Type	DDM (Yes/No)	Transmit Power (dBm)		Receive Power (dBm)	
				Min.	Max.	Min.	Max.
SFP-SM1310	1310	SMF	No	-9.5	-3	-20	-3
GE-SFP-ZX	850	MMF	Yes	-9.5	-3	-17	0
GE-SX-MM850	850	MMF	Yes	-9.5	-3	-17	0
GE-LX-SM1310	1310	SMF	Yes	-9	-3	-20	-3
SFP-S4-R1000P1 v1	1310	SMF	Yes	-9	-3	-20	-3

Table 6-3 SFP Ethernet Transceiver Modules

Standard	SFP Media Converter	DDM (Yes/No)
1000BASE-T	Mini-GBIC-GT	No

Table 6-4 SFP Module Cabling Specifications

Model	Connector Type	Optical Cable Type	Core Specifications (µm)	Max. Cabling Distance
MINI-GBIC-SX-MM850	LC	MMF	62.5/125	275 m (902.23 ft.)
			50/125	550 m (1804.46 ft.)
MINI-GBIC-LX-SM1310	LC	SMF	9/125	10 km (32,808.4 ft.)
MINI-GBIC-LH40-SM1310	LC	SMF	9/125	40 km (131,233.6 ft.)
GE-SFP-SX-SM1310-BIDI	LC	MMF	50/125	500 m (1640.42 ft.)
GE-SFP-SX-SM1550-BIDI	LC	MMF	50/125	500 m (1640.42 ft.)
GE-SFP-LX20-SM1310-BIDI	LC	SMF	9/125	20 km (65,616.8 ft.)
GE-SFP-LX20-SM1550-BIDI	LC	SMF	9/125	20 km (65,616.8 ft.)
GE-SFP-LH40-SM1310-BIDI	LC	SMF	9/125	40 km (131,233.6 ft.)
GE-SFP-LH40-SM1550-BIDI	LC	SMF	9/125	40 km (131,233.6 ft.)
MINI-GBIC-ZX80-SM1550	LC	SMF	9/125	80 km (262,467.2 ft.)
MINI-GBIC-ZX100-SM1550	LC	SMF	9/125	100 km (328,084 ft.)
SFP-MM850	LC	MMF	50/125	500 m (1640.42 ft.)

Model	Connector Type	Optical Cable Type	Core Specifications (µm)	Max. Cabling Distance
SFP-SM1310	LC	SMF	9/125	10 km (32,808.4 ft.)
GE-SFP-ZX	LC	MMF	50/125	550 m (1804.46 ft.)
GE-SX-MM850	LC	MMF	50/125	550 m (1804.46 ft.)
GE-LX-SM1310	LC	SMF	9/125	10 km (32,808.4 ft.)
SFP-S4-R1000P1 v1	LC	SMF	9/125	10 km (32,808.4 ft.)
Mini-GBIC-GT	RJ45 Ethernet cable	Cat 5 (or higher) UTP or STP		100 m (328.08 ft.)
GE-SFP-GT	RJ45 Ethernet cable	Cat 5 (or higher) UTP or STP		100 m (328.08 ft.)
SFP-GT	RJ45 Ethernet cable	Cat 5 (or higher) UTP or STP		100 m (328.08 ft.)

⚠ Caution

- For optical transceivers with a cabling distance equal to or greater than 40 km (131,233.6 ft.), install an optical attenuator to avoid overload on the optical receiver when using short-distance SMF optical cables.
- An optical transceiver is a laser transmitter. Do not look directly into the optical transceiver to prevent it from burning your eyes.
- To keep the optical transceiver clean, ensure that the unused ports remain capped.

Figure 6-5 BIDI Module Pairing Models

Rate/Distance	Pairing Model
1000 Mbps/500 m (1640.42 ft.)	GE-SFP-SX-SM1310-BIDI GE-SFP-SX-SM1550-BIDI
1000 Mbps/20 km (65616.80 ft.)	GE-SFP-LX20-SM1310-BIDI GE-SFP-LX20-SM1550-BIDI
1000 Mbps/40 km (131233.60 ft.)	GE-SFP-LH40-SM1310-BIDI GE-SFP-LH40-SM1550-BIDI
10000 Mbps/10 km (32808.4 ft.)	XG-SFP-LR-SM1270-BIDI XG-SFP-LR-SM1330-BIDI

⚠ Caution

The BIDI modules must be used in pairs. For example, if you install the GE-SFP-LX20-SM1310-BIDI on one end, you must install the GE-SFP-LX20-SM1550-BIDI on the other end.

6.2.2 SFP+ Transceiver Modules

Table 6-5 Models and Specifications of SFP+ Optical Transceiver Modules

Model	Wavelength (nm)	Optical Cable Type	DDM (Yes/No)	Transmit Power (dBm)		Receive Power (dBm)	
				Min.	Max.	Min.	Max.
XG-SFP-SR-MM850	850	Yes	MMF	-7.3	-1	-9.9	-1
XG-SR-MM850	850	Yes	MMF	-7.3	-1	-9.9	-1
SFP+MM850	850	Yes	MMF	-7.3	-1	-9.9	-1
XG-SFP-LR-SM1270-BIDI	1270	No	SMF	-6.5	0.5	-14.4	0.5
XG-SFP-LR-SM1330-BIDI	1330	No	SMF	-6.5	0.5	-14.4	0.5
XG-LR-SM1310	1310	Yes	SMF	-8.2	0.5	-14.4	0.5
SFP+SM1310	1310	Yes	SMF	-8.2	0.5	-14.4	0.5
XG-SFP-LR-SM1310	1310	Yes	SMF	-8.2	0.5	-14.4	0.5
XG-eSFP-LR-SM1310	1310	Yes	SMF	-8.2	0.5	-14.4	0.5
XG-SFP-ER-SM1550	1550	Yes	SMF	-4.7	4	-11.3	-1
XG-SFP-ZR-SM1550	1550	Yes	SMF	0	4	-24	-7
SFP-S4-R1000P1 v2	1310	Yes	SMF	-8.2	0.5	-14.4	0.5
SFP-S1-R1000P1	1310	Yes	SMF	-8.2	0.5	-14.4	0.5

Model	Wavelength (nm)	Optical Cable Type	DDM (Yes/No)	Transmit Power (dBm)		Receive Power (dBm)	
				Min.	Max.	Min.	Max.
SFP+1310	1310	Yes	SMF	-8.2	0.5	-14.4	0.5
SFP-M3-R1000P1	850	Yes	MMF	-7.3	-1	-11.1	-1
XG-LR-SM1310	1310	Yes	SMF	-8.2	0.5	-14.4	0.5
HSFP-XG-SFP-LR-SM1310	1310	Yes	SMF	-8.2	0.5	-14.4	0.5
XG-SFP-SR-MM850-I	850	Yes	MMF	-7.3	-1	-9.9	-1
XG-SFP-LR-SM1310-I	1310	Yes	SMF	-8.2	0.5	-14.4	0.5

Table 6-6 Models of SFP+ Active Optical Cable Modules

Model	Module Type	Connector Type	Copper Cable Length	Conductor Diameter (AWG)	Rate (Gbps)	DDM (Yes/No)
XG-SFP-AOC1M	Active	SFP+	1 m (3.28 ft.)	N/A	10.3125	Yes
XG-SFP-AOC3M	Active	SFP+	3 m (9.84 ft.)	N/A	10.3125	Yes
XG-SFP-AOC5M	Active	SFP+	5 m (16.40 ft.)	N/A	10.3125	Yes
XG-SFP-AOC10M	Active	SFP+	10 m (32.81 ft.)	N/A	10.3125	Yes

Note

- SFP+ module types and models are subject to change without prior notice. For any updates about the optical transceivers, contact Ruijie Networks marketing or technical support personnel.
- The DDM function of AOC cables does not report the transmit power. The transmit power is displayed as N/A.

Table 6-7 SFP+ Module Cabling Specifications

Model	Connector Type	Optical Cable Type	Core Specifications (μm)	Modal Bandwidth (MHz•km)	Max. Cabling Distance
XG-SFP-SR-MM850	LC	MMF	50/125	2000 (OM3)	300 m (984.25 ft.)
XG-SR-MM850	LC	MMF	50/125	2000 (OM3)	300 m (984.25 ft.)
SFP+MM850	LC	MMF	50/125	2000 (OM3)	300 m (984.25 ft.)
XG-SFP-LR-SM1270-BIDI	LC	SMF	9/125	N/A	10 km (32,808.4 ft.)
XG-SFP-LR-SM1330-BIDI	LC	SMF	9/125	N/A	10 km (32,808.4 ft.)
XG-SFP-LR-SM1310	LC	SMF	9/125	N/A	10 km (32,808.4 ft.)
SFP+SM1310	LC	SMF	9/125	N/A	10 km (32,808.4 ft.)
XG-SFP-ER-SM1550	LC	SMF	9/125	N/A	40 km (131,233.6 ft.)
XG-SFP-ZR-SM1550	LC	SMF	9/125	N/A	80 km (262,467.2 ft.)
SFP-S4-R1000P1 v2	LC	SMF	9/125	N/A	10 km (32,808.4 ft.)
SFP-S1-R1000P1	LC	SMF	9/125	N/A	10 km (32,808.4 ft.)
SFP+1310	LC	SMF	9/125	N/A	10 km (32,808.4 ft.)
SFP-M3-R1000P1	LC	MMF	50/125	2000 (OM3)	300 m (984.25 ft.)
XG-LR-SM1310	LC	SMF	9/125	N/A	10 km (32,808.4 ft.)
HSFP-XG-SFP-LR-SM1310	LC	SMF	9/125	N/A	10 km (32,808.4 ft.)

Model	Connector Type	Optical Cable Type	Core Specifications (μm)	Modal Bandwidth (MHz•km)	Max. Cabling Distance
XG-SFP-SR-MM850-I	LC	MMF	50/125	2000 (OM3)	300 m (984.25 ft.)
XG-SFP-LR-SM1310-I	LC	SMF	9/125	N/A	10 km (32,808.4 ft.)

Table 6-8 Models and Specifications of e-Lighten Optical Transceivers

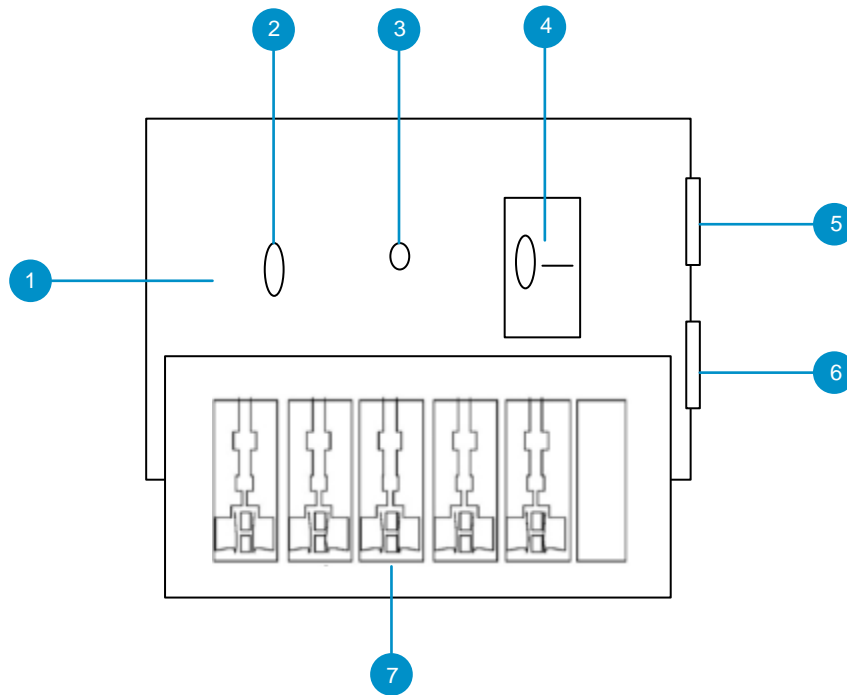
Model	Wavelength (nm)	Optical Cable Type	DDM (Yes/No)	Transmit Power (dBm)		Receive Power (dBm)	
				Min	Max	Min	Max
OM-GE-SFP-10KM-SM1490	1490/1310	Yes	SMF	3	7	-32	-12

6.3 Surge Protection

6.3.1 Installing an AC Power Lightning Arrester

When an AC power cord from outdoors is directly plugged into the power port of the equipment, the AC power connector must be connected to an external surge protector power strip to protect the equipment against lightning strikes. The surge protector power strip can be fixed on the rack, workbench, or wall in the equipment room by using cable ties and screws. AC power enters the equipment through the surge protector power strip.

Figure 6-6 Installing an AC Power Lightning Arrester



No.	Description
1	Installed electronic circuit board
2	Normally running indicator: When the indicator is green, the circuit is working properly. Otherwise, the protective circuit is damaged.
3	Grounding and polarity detection indicator: If the indicator is red, cable connection is incorrect (the ground cable is not connected, or the N and L lines are reversely connected). Check your power supply line.
4	Power switch
5	IEC standard socket, which is connected to the power supply in the equipment room through the power cable
6	Overload auto-protector, which can be reset manually
7	Multi-purpose sockets (connected to the power supply of the switch)

Note

The lightning arrester is not delivered with the equipment. Please purchase it based on actual requirements.

Precautions:

- Make sure that the PE terminal of the power arrester is well grounded.
- After the AC power plug of the equipment is connected to the socket of the power arrester (lightning

resistance socket), the surge protection function is implemented only if the RUN indicator is green and the ALARM indicator is OFF.

- If the indicator on the power arrester is red, check whether it is caused by poor grounding connection or by the reversed connection of the Null and Live lines. The detection method is as follows: Use a multimeter to measure the polarity of the power socket for the arrester when the indicator is red. If the N line is on the left and the L line is on the right (facing the socket), the arrester's PE terminal is not grounded. If not, the polarity of the arrester power cord should be reversed. In this case, you should open the power arrester and rectify the polarity of the connection. If the indicator is still red, the arrester's PE terminal is not grounded.

6.3.2 Installing an Ethernet Port Lightning Arrester

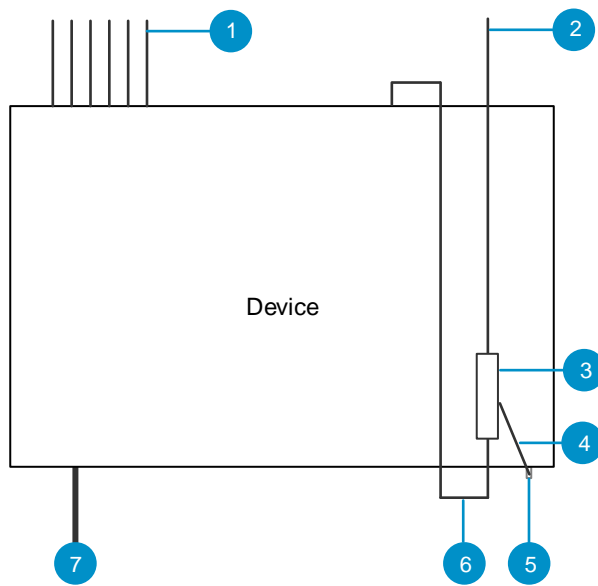
Connect an Ethernet port arrester to the equipment to prevent the damage by lightning before connecting an outdoor network cable to the device.

Tools: Phillips screwdrivers or flat-head screwdriver, multimeter, and diagonal pliers

Procedure:

- (1) Tear one side of the protective paper for the double-sided adhesive tape and paste the tape to the enclosure of the Ethernet port arrester.
- (2) Tear the other side of the protective paper for the double-sided adhesive tape and paste the Ethernet port arrester to the enclosure. The paste position for the Ethernet port arrester should be as close to the grounding terminal of the equipment as possible.
- (3) According to the distance between the equipment grounding terminal and the Ethernet port arrester, cut the grounding cable for the Ethernet port arrester and firmly crimp the grounding cable to the grounding terminal of the equipment.
- (4) Use a multimeter to check whether the grounding cable for the arrester is in good contact with the grounding terminal and the enclosure of the equipment.
- (5) Connect the arrester by using an adapter cable (note that the external network cable is connected to the IN end, while the adapter cable connected to the equipment is connected to the OUT end) and check whether the service module LED is normal.
- (6) Use a nylon cable tie to bind the power cords.

Figure 6-7 Installing an Ethernet Port Lightning Arrester



No.	Description
1	Ethernet cable for indoor connection
2	Ethernet cable connected to the outdoor
3	RJ45 port arrester (pasted on the enclosure)
4	Ground cable of the arrester
5	Grounding lug of the equipment
6	RJ45 port adapter cable
7	Power input

Note

- The Ethernet port arrester is only for Ethernet ports with an RJ45 connector.
- The Ethernet port arrester is not delivered with the equipment. Please purchase it based on actual requirements. The Ethernet port arrester user manual contains technical parameters and maintenance and installation instructions for the Ethernet port arrester. Carefully read this manual before installation.

Pay attention to the following situations during the installation to avoid influencing the performance of the Ethernet port arrester:

- Reversed installation direction of the arrester. Connect the external network cable to the “IN” end and connect the Ethernet port of the equipment to the “OUT” end.
- Poor grounding of the arrester. The grounding cable of the arrester should be as short as possible to ensure that it is in good contact with the grounding terminal of the equipment. Use a multimeter to confirm the contact condition after grounding.

- Incomplete arrester installation. If there is more than one port connected to external power cords, arresters need to be installed on all connection ports for the purpose of surge protection.

6.4 Recommended Cabling

When the device is installed in a standard 19-inch rack, route the cables through the cable management brackets. Top cabling or bottom cabling is adopted according to the actual situation in the equipment room. All conversion connectors should be placed at the bottom of the rack instead of outside the rack that is easily accessible. Power cords are routed beside the cabinet, and top cabling or bottom cabling is adopted according to the actual situation in the equipment room, such as the locations of the DC power distribution box, AC power socket, or surge protection box.

6.4.1 Requirements for the Minimum Bend Radius of an Ethernet Cable

- The bend radius of a fixed power cord, Ethernet cable, or flat cable should be over five times greater than their respective diameters. The bend radius of these cables that are often bent or plugged should be over seven times greater than their respective diameters.
- The bend radius of a fixed common coaxial cable should be over seven times greater than its diameter. The bend radius of the common coaxial cable that is often bent or plugged should be over 10 times greater than its diameter.
- The bend radius of a fixed high-speed cable (such as SFP+ cable) should be over five times greater than its diameter. The bend radius of the fixed high-speed cable that is often bent or plugged should be over 10 times greater than its diameter.

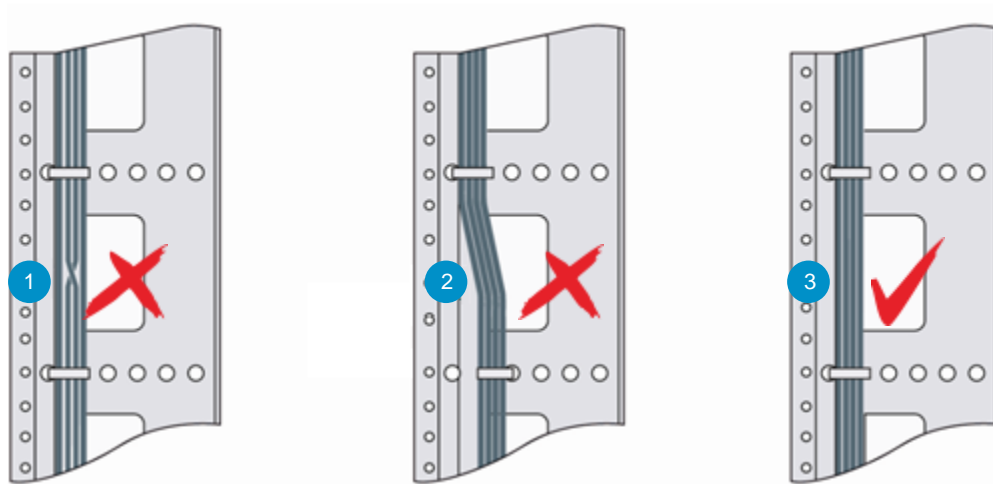
6.4.2 Requirement for the Minimum Bend Radius of an Optical Cable

- When an optical cable is coiled, the diameter of a fiber tray should be over 25 times greater than the diameter of the optical cable.
- When an optical cable is moved, the bend radius of the optical cable should be over 20 times greater than the diameter of the optical cable.
- When an optical cable is laid, the bend radius of the optical cable should be over 10 times greater than the diameter of the optical cable.

6.4.3 Precautions for Bundling up Cables

- Before cables are bundled, mark labels and stick the labels to cables wherever appropriate.
- Cables should be neatly and properly bundled in the rack without twisting or bending, as shown in [Figure 6-8](#).

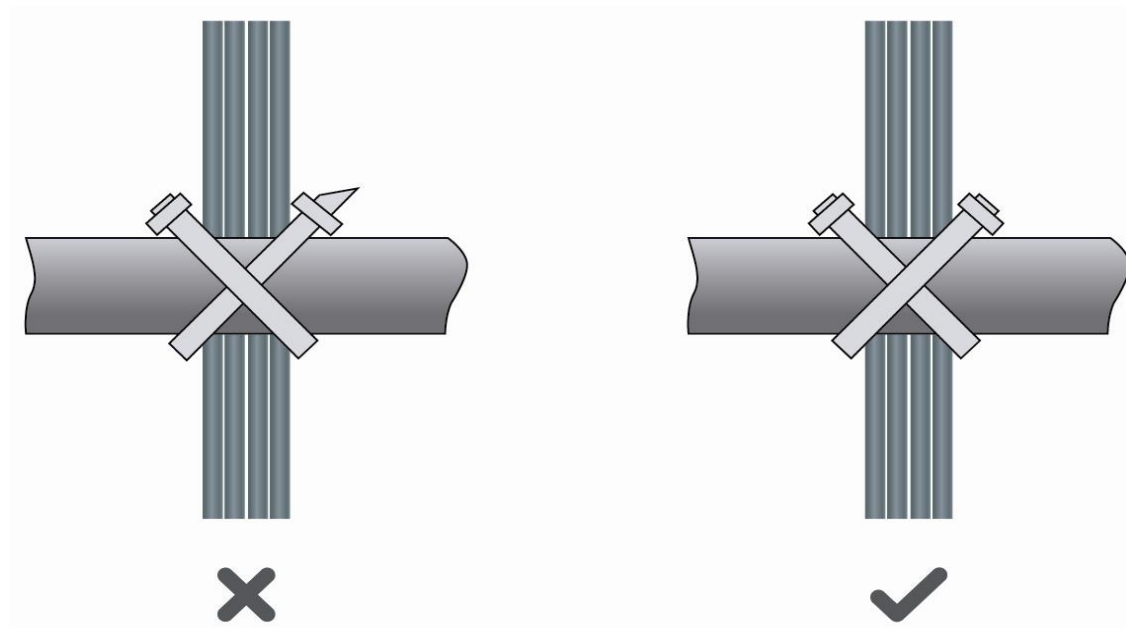
Figure 6-8 Binding Cables (I)



No.	Description
1	In the rack, cables should not be wound up after being bundled.
2	In the rack, cables should not bend after being bundled.
3	In the rack, cables should be neatly and straightly bundled.

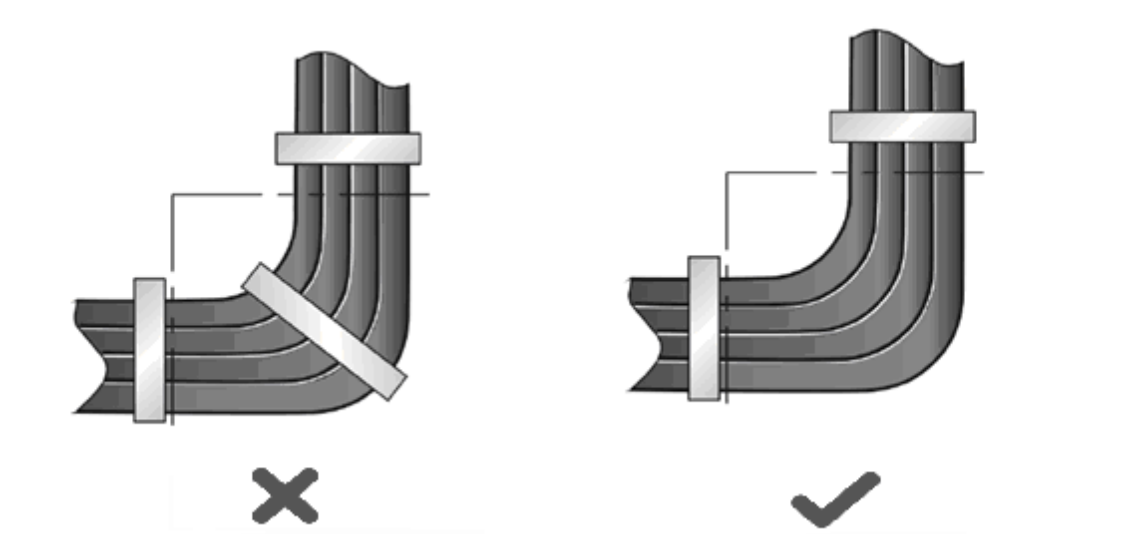
- Cables of different types (such as power cords, signal cables, and ground cables) should be separated in cabling and bundling. Mixed bundling is disallowed. When they are close to each other, you are advised to adopt crossover cabling. In the case of parallel cabling, maintain a minimum distance of 30 mm (1.18 in.) between power cords and signal cables.
- The cable management brackets and cabling troughs inside and outside the rack should be smooth without sharp corners.
- The metal hole traversed by cables should have a smooth and fully rounding surface or an insulated lining.
- Use cable ties to bundle up cables properly. Please do not connect two or more cable ties to bundle up cables.
- After bundling up cables with cable ties, cut off the remaining part. The cut should be smooth and trim, without sharp corners, as shown in [Figure 6-9](#).

Figure 6-9 Binding Cables (II)



- When cables need to be bent, please bundle them up but do not tie them where the cables will be bent, as shown in [Figure 6-10](#).

Figure 6-10 Binding Cables (III)

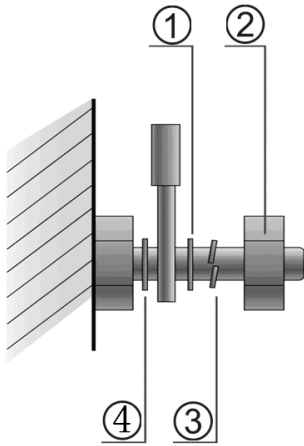


- Cables not to be assembled or remaining parts of cables should be folded and placed in a proper position of the rack or cable trough. The proper position refers to a position that does not affect device running or damage the device or cable.
- Do not bind power cords to the guide rails of moving parts.
- The power cords connecting moving parts such as door grounding cables should be reserved with a margin after being assembled to avoid suffering tension or stress. When the moving part is installed, the remaining cable part should not touch heat sources, sharp corners, or sharp edges. If heat sources cannot be avoided,

high-temperature cables should be used.

- When screw threads are used to fasten cable terminals, the anchor or screw must be tightly fastened, as shown in [Figure 6-11](#).

Figure 6-11 Cable Fastening



- ① Flat washer ③ Spring washer
- ② Screw nut ④ Flat washer

- Hard power cords should be fastened in the terminal connection area to prevent stress on terminal connection and cable.
- Do not use self-tapping screws to fasten terminals.
- Power cords of the same type and in the same cabling direction should be bundled up into cable bunches, with cables in cable bunches clean and straight.
- Bundle up cables by using cable ties.

Cable Bunch Diameter	Distance Between Every Binding Point
10 mm (0.39 in.)	80 mm to 150 mm (3.15 in. to 5.91 in.)
10 mm to 30 mm (0.39 in. to 1.18 in.)	150 mm to 200 mm (5.91 in. to 7.87 in.)
30 mm (1.18 in.)	200 mm to 300 mm (7.87 in. to 11.81 in.)

- Do not tie cables or bundles in a knot.
- For wiring terminal sockets (such as circuit breakers) with cord end terminals, the metal part of the cord end terminal should not be exposed outside the terminal socket when assembled.

6.5 Site Selection

- The equipment room should be at least 5 km (3.11 miles) away from heavy pollution sources, such as the smelter works, coal mine, and thermal power plant. The equipment room should be at least 3.7 km (2.30 miles) away from medium pollution sources, such as the chemical factory, rubber factory, and electroplating

factory. The equipment room should be at least 2 km (1.24 miles) away from light pollution sources, such as the food factory and leather plant. If the pollution source is unavoidable, the equipment room should be located on the windward side of the pollution source perennially with advanced protection.

- The equipment room should be at least 3.7 km (2.30 miles) away from the sea or salt lake. Otherwise, the equipment room must be sealed, with air conditioner installed for temperature control. Saline soil cannot be used for construction. Otherwise, you should select devices with advanced protection against severe environment.
- Do not build the equipment room in the proximity of livestock farms. Otherwise, the equipment room should be located on the windward side of the pollution source perennially. The previous livestock house or fertilizer warehouse cannot be used as the equipment room.
- The equipment room should be firm enough to withstand severe weather conditions such as windstorm and heavy rain as well as away from dust. If the dust is unavoidable, keep the door and window away from the pollution source.
- The equipment room should be away from the residential area. Otherwise, the equipment room should meet the construction standard in terms of noise.
- Make sure the air vent of the equipment room is away from the sewage pipe, septic tank, and sewage treatment tank. Keep the equipment room under positive pressure to prevent corrosive gas from entering the equipment room to corrode components and circuit boards.
- Keep the equipment room away from industrial boiler and heating boiler.
- The equipment room should be on the second floor. Otherwise, the equipment room floor should be 600 mm (23.62 in.) higher than the highest flood level ever recorded.
- Make sure there are no cracks or holes in the wall and floor. If there are cable entries in the wall or window, take proper sealing measures. Ensure that the wall is flat, wear-resistant, and dust-free, which should be up to the standard for flame retarding, soundproofing, heat absorption, dust reduction, and electromagnetic shielding.
- Keep the door and the window closed to make the equipment room sealed.
- The steel door is recommended for soundproofing.
- Sulfur-containing materials are forbidden.
- Keep the air conditioner from blowing wind straight toward the device or blowing water drops from the window or air vent toward the device.

6.6 Cleaning the Connectors and End Faces of Optical Cables

To ensure a good connection between a patch cable and an optical cable coupler, the cleanliness of the end face is a quite important factor, as it directly affects the communication quality of the optical network. In the daily construction of optical networks, however, improper operations or other reasons can easily contaminate the end face. When the end face accumulates dust, oil stains, and other dirt, if it is not detected and cleaned before connection, it will cause increased optical attenuation, leading to optical network failures. What's worse, it may even result in the collapse of the entire optical signal system. The following are common methods for cleaning connectors and end faces:

- Using fiber-optic cleaning pens

Fiber-optic cleaning pens, also known as one-click fiber-optic cleaners, typically use anti-static resin materials, lint-free cleaning tip, and cleaning solution to ensure the product remains free from dust contamination. Available in 1.25 mm and 2.5 mm sizes, these pens are suitable for cleaning SC, FC, LC connectors, and more. Select an appropriate cleaning pen for the connector to be cleaned, and gently insert the pen into the connector. To prevent ferrule damage, avoid excessive pressure when you insert the cleaning pen. Press inward gently until you hear a "click", indicating the end face has been cleaned. If necessary, repeat the process 2 to 3 times for thorough cleaning. Finally, remove the pen to complete the cleaning process.

- Using fiber-optic cleaning boxes or lint-free cloths
 - Made from high-density textile fibers, fiber-optic cleaning boxes do not need alcohol, do not produce static electricity, and are lint-free. In addition, fiber-optic cleaning boxes offer a convenient way for cleaning various optical cable connectors, including SC, FC, LC, and ST connectors.
 - To use the cleaning box, grip it with one hand and press it to reveal the clean cleaning belt core. Gently swipe the optical cable ferrule to be cleaned across the cleaning belt several times to remove dirt from the end face. To prevent ferrule damage, avoid excessive pressure when you swipe the optical cable ferrule.

Ruijie Reyee

RG-NBF Series Switches ReyeeOS 2.290

Configuration Guide



Copyright

Copyright © 2024 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 you purchase are subject to commercial contracts and terms, and some or all of the products, services, or features described in this document may not be available for you to purchase or use. Except for the agreement in the contract, Ruijie Networks makes no explicit or implicit statements or warranties with respect to 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 will be updated from time to time due to product version upgrades or other reasons, Ruijie Networks reserves the right to modify the content of the document without any notice or prompt.

This manual is designed merely as a user guide. Ruijie Networks has tried its best to ensure the accuracy and reliability of the content when compiling this manual, but it does not guarantee that the content of the manual is completely free of errors or omissions, and all the information 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

- 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	1
1 Change Description.....	1
1.1 ReyeeOS 2.290	1
1.1.1 Hardware Change.....	1
1.1.2 Software Feature Change.....	1
2 Login.....	1
2.1 Configuration Environment Requirements	1
2.1.1 PC	1
2.2 Logging in to the Web Page	1
2.2.1 Connecting to the Device.....	1
2.2.2 Logging in to the Web Page	1
2.2.3 Frequently-Used Controls on the Web Page.....	2
2.3 Quick Setup	4
2.3.1 Configuration Preparations	4
2.3.2 Procedure.....	4
2.4 Work Mode.....	5
2.5 Switching the Management Mode	6
3 Network management	8
3.1 Overviewing Network Information.....	8
3.2 Viewing Networking Information	8
3.3 Adding Networking Devices.....	11
3.3.1 Wired Connection	11
3.4 Managing Networking Devices	12

3.5 Configuring the Service Network	14
3.5.1 Configuring the Wired Network.....	15
3.5.2 Configuring the Wireless Network	17
3.6 Processing Alerts.....	19
3.7 Viewing Online Clients.....	21
3.8 Smart Device Network	22
3.8.1 Overview	22
3.8.2 Procedure.....	22
4 Basic Management	26
4.1 Overviewing Switch Information	26
4.1.1 Basic information about the Device	26
4.1.2 Port Info.....	27
4.2 Port Flow Statistics	29
4.3 MAC Address Management.....	30
4.3.1 Overview	30
4.3.2 Displaying the MAC Address Table.....	30
4.3.3 Displaying Dynamic MAC Address	31
4.3.4 Configuring Static MAC Binding	32
4.3.5 Configuring MAC Address Filtering	33
4.3.6 Configuring MAC Address Aging Time	35
4.4 Displaying ARP Information.....	35
4.5 View optical module information.....	36
4.6 Fiber Properties	36
4.7 DBA.....	37

4.7.1 Overview	37
4.7.2 Bandwidth Allocation Mechanism	37
4.7.3 Configuring DBA	38
4.8 VLAN	39
4.8.1 VLAN Overview	39
4.8.2 Creating a VLAN	39
4.8.3 Configuring Port VLAN	42
4.8.4 Batch Switch Configuration	44
4.8.5 Verifying Configuration	46
5 Port Management	47
5.1 Overview	47
5.2 Port Configuration	48
5.2.1 Basic Settings	48
5.2.2 Physical Settings	50
5.3 Aggregate Ports	53
5.3.1 Aggregate Port Overview	53
5.3.2 Overview	53
5.3.3 Aggregate Port Configuration	54
5.3.4 Configuring a Load Balancing Mode	56
5.4 Port Mirroring	56
5.4.1 Overview	56
5.4.2 Procedure	57
5.5 Rate Limiting	59
5.6 MGMT IP Configuration	61

5.6.1 Set IPv4 management address	61
5.6.2 Configuring the Management IPv6 Address	62
6 L2 Multicast	64
6.1 Multicast Overview	64
6.2 Multicast Global Settings	64
6.3 IGMP Snooping.....	65
6.3.1 Overview	65
6.3.2 Enabling Global IGMP Snooping	66
6.3.3 Configuring Protocol Packet Processing Parameters	66
6.4 Configuring MVR.....	68
6.4.1 Overview	68
6.4.2 Configuring Global MVR Parameters	68
6.4.3 Configuring the MVR Ports	69
6.5 Configuring Multicast Group	71
6.6 Configuring a Port Filter	72
6.6.1 Configuring Profile	73
6.6.2 Configuring a Range of Multicast Groups for a Profile	74
6.7 Setting an IGMP Querier	75
6.7.1 Overview	75
6.7.2 Procedure.....	75
7 L3 Management	77
7.1 Setting an L3 Interface.....	77
7.2 Configuring the IPv6 Address for the L3 Interface	78
7.3 Configuring the DHCP Service	81

7.3.1 Enable DHCP Services.....	81
7.3.2 Viewing the DHCP Client.....	82
7.3.3 Configuring Static IP Addresses Allocation.....	82
7.3.4 Configuring the DHCP Server Options	83
7.4 Configuring the DHCPv6 Server.....	85
7.4.2 Viewing DHCPv6 Clients	86
7.4.3 Configuring the Static DHCPv6 Address	86
7.5 Configuring the IPv6 Neighbor List.....	87
7.6 Configuring a Static ARP Entry	88
8 Configuring Route	90
8.1 Configuring Static Routes	90
8.2 Configuring the IPv6 Static Route	91
8.3 Configuring RIP.....	92
8.3.1 Configuring RIP Basic Functions	92
8.3.2 Configuring the RIP Port.....	94
8.3.3 Configuring the RIP Global Configuration	95
8.3.4 Configuring the RIP Route Redistribution List.....	96
8.3.5 Configuring the Passive Interface.....	97
8.3.6 Configuring the Neighbor Route	98
8.4 Configuring RIPng.....	98
8.4.1 Configuring RIPng Basic Functions	98
8.4.2 Configuring the RIPng Port.....	100
8.4.3 Configuring the RIPng Global Configuration	101
8.4.4 Configuring the RIPng Route Redistribution List.....	102

8.4.5	Configuring the RIPng Passive Interface.....	102
8.4.6	Configuring the IPv6 Aggregate Route	103
8.5	OSPFv2.....	103
8.5.1	Configuring OSPFv2 Basic Parameters	103
8.5.2	Adding an OSPFv2 Interface	109
8.5.3	Redistributing OSPFv2 Instance Routes.....	110
8.5.4	Managing OSPFv2 Neighbors.....	111
8.5.5	Viewing OSPFv2 Neighbor Information.....	112
8.6	OSPFv3.....	112
8.6.1	Configuring OSPFv3 Basic Parameters	112
8.6.2	Adding an OSPFv3 Interface	120
8.6.3	Viewing OSPFv3 Neighbor Information.....	121
8.7	Routing Table Info.....	122
9	Security.....	123
9.1	DHCP Snooping.....	123
9.1.1	Overview	123
9.1.2	Standalone Device Configuration	123
9.1.3	Batch Configuring Network Switches	123
9.2	Storm Control.....	126
9.2.1	Overview	126
9.2.2	Procedure.....	126
9.3	ACL	127
9.3.1	Overview	127
9.3.2	Creating ACL Rules.....	127

9.3.3 Applying ACL Rules.....	130
9.4 Port Protection	131
9.5 IP-MAC Binding	131
9.5.1 Overview	131
9.5.2 Procedure.....	131
9.6 IP Source Guard	133
9.6.1 Overview	133
9.6.2 Viewing Binding List.....	133
9.6.3 Enabling Port IP Source Guard	134
9.6.4 Configuring Exceptional VLAN Addresses	135
9.7 Configure 802.1x authentication.....	136
9.7.1 Function introduction.....	136
9.7.2 Configuration 802.1x.....	137
9.7.3 View the list of wired authentication users.....	143
9.8 Anti-ARP Spoofing	143
9.8.1 Overview	143
9.8.2 Procedure.....	144
10 Advanced Configuration	146
10.1 STP	146
10.1.1 STP Global Settings.....	146
10.1.2 Applying STP to a Port.....	147
10.2 LLDP	150
10.2.1 Overview	150
10.2.2 LLDP Global Settings.....	150

10.2.3	Applying LLDP to a Port.....	151
10.2.4	Displaying LLDP information	152
10.3	RLDP.....	153
10.3.1	Overview	153
10.3.2	Standalone Device Configuration	154
10.3.3	Batch Configuring Network Switches	156
10.4	Configuring the Local DNS	158
10.5	Voice VLAN.....	159
10.5.1	Overview	159
10.5.2	Voice VLAN Global Configuration.....	159
10.5.3	Configuring a Voice VLAN OUI.....	160
10.5.4	Configuring the Voice VLAN Function on a Port	161
11	Diagnostics	164
11.1	Info Center	164
11.1.1	Port Info.....	164
11.1.2	VLAN Info	165
11.1.3	Routing Info	165
11.1.4	DHCP Clients	166
11.1.5	ARP List.....	166
11.1.6	MAC Address	167
11.1.7	DHCP Snooping.....	167
11.1.8	IP-MAC Binding.....	168
11.1.9	IP Source Guard.....	168
11.1.10	CPP Info	169

11.2 Network Tools	170
11.2.1 Ping	170
11.2.2 Traceroute	170
11.2.3 DNS Lookup	171
11.3 Fault Collection	172
11.4 Cable Diagnostics	172
11.5 System Logs	173
11.6 Alerts	173
12 System Configuration	176
12.1 Setting the System Time	176
12.2 Setting the Web Login Password	177
12.3 Setting the Session Timeout Duration	177
12.4 Configuring SNMP	177
12.4.1 Overview	177
12.4.2 Global Configuration	178
12.4.3 View/Group/Community/Client Access Control	179
12.4.4 Typical Configuration Examples of SNMP Service	186
12.4.5 trap service configuration	191
12.4.6 Typical configuration examples of the trap service	195
12.5 Configure 802.1x authentication	197
12.5.1 Function introduction	197
12.5.2 Configuration 802.1x	198
12.5.3 View the list of wired authentication users	203
12.6 Anti-ARP Spoofing	203

12.6.1 Overview	203
12.6.2 Procedure.....	204
13 Diagnostics.....	206
13.1 Info Center	206
13.1.1 Port Info.....	206
13.1.2 VLAN Info.....	207
13.1.3 Routing Info.....	207
13.1.4 DHCP Clients	208
13.1.5 ARP List	208
13.1.6 MAC Address	209
13.1.7 DHCP Snooping.....	210
13.1.8 IP-MAC Binding	210
13.1.9 IP Source Guard	211
13.1.10 CPP Info.....	211
13.2 Network Tools.....	212
13.2.1 Ping.....	212
13.2.2 Traceroute.....	212
13.2.3 DNS Lookup.....	213
13.3 Fault Collection	214
13.4 Cable Diagnostics.....	214
13.5 System Logs	215
13.6 Alerts	215
14 FAQs.....	217
14.1 Failing to log in to the Eweb Management System	217

14.2 Password Lost and Restoration of Factory Settings217

1 Change Description

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

1.1 ReyeeOS 2.290

1.1.1 Hardware Change

This baseline version has no hardware change. The following table lists the applicable hardware models of this version.

Model	Hardware Version
RG-NBF6002M	1.xx
MF6000M-16GT8SFP2XS	1.xx
MF6000M-16FS8GT2XS	1.xx
MF6000M-24GT2XS	1.xx
RG-NBF5200M-8FS16GT4XS	1.xx
RG-NBF2100S-8GT1SC	1.xx
RG-NBF2100S-8GT1SC-P	1.xx
RG-NBF2100S-16GT1SC-P	1.xx

1.1.2 Software Feature Change

This baseline version has no software feature change.

2 Login

2.1 Configuration Environment Requirements

2.1.1 PC

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

2.2 Logging in to the Web Page

2.2.1 Connecting to the Device

Use a network cable to connect the switch port to the network port of the PC, and configure an IP address for the PC that is on the same network segment as the default IP of the device to ensure that the PC can ping through the switch. For example, set the IP address of the PC to 10.44.77.100.

Table 2-1 Default settings

Feature	Default Value
Device IP Address	10.44.77.200
Password	A username is not required when you log in for the first time. The default password is admin.

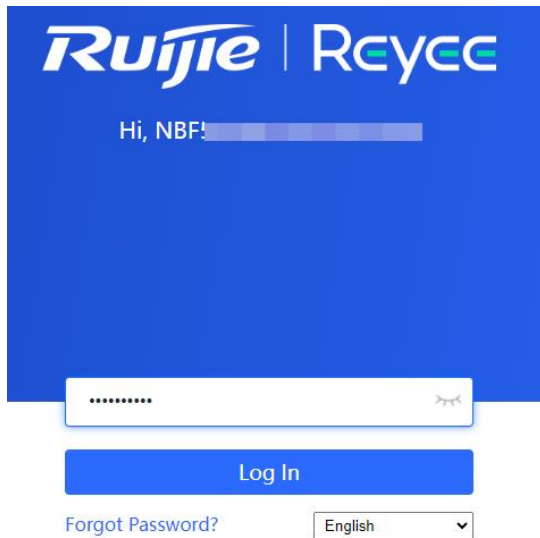
2.2.2 Logging in to the Web Page

- (1) Enter the IP address (10.44.77.254 by default) of the device in the address bar of the browser to open the login page.

 **Note**

If the static IP address of the device is changed, or the device dynamically obtains a new IP address, the new IP address can be used to access the web management system of the device as long as the PC and the device are on the same LAN, and their IP addresses are in the same network segment.

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



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

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

⚠ Caution

Restoring factory settings will delete all configurations of the device. Therefore, exercise caution when performing this operation.

2.2.3 Frequently-Used Controls on the Web Page

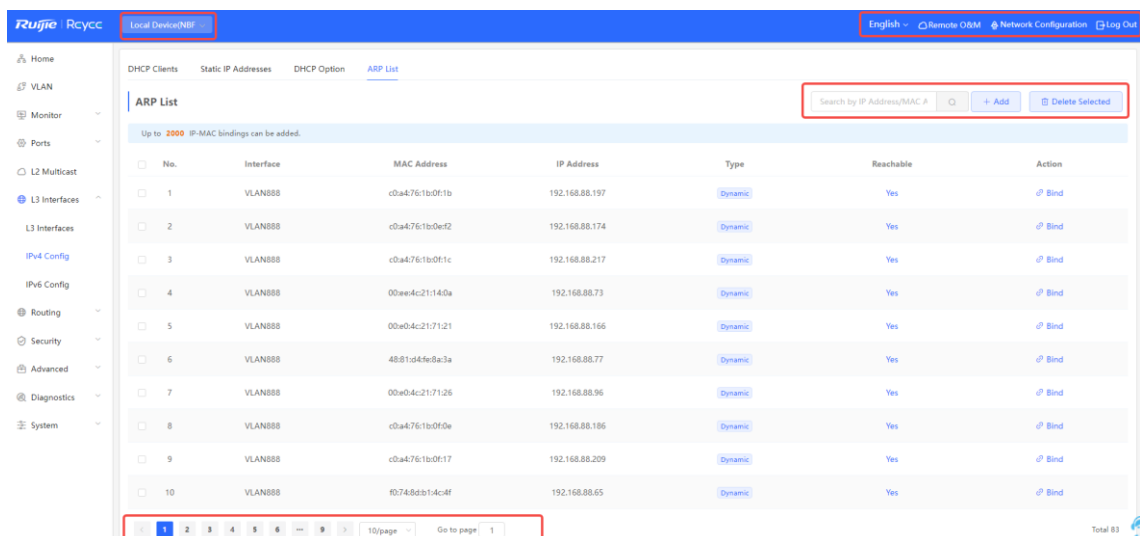
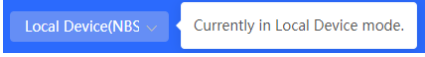
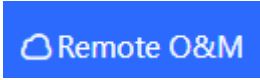


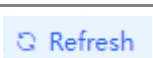


Table 2-2 Frequently-Used Controls on the Web Page

Control	Description
	<p>Local Device: Allows you to configure all functions of the local device.</p> <p>Network: Allows you to configure common functions of all wired and wireless Reyee products in batches in an ad hoc network.</p>
	<p>The navigation bar is arranged horizontally on the top when the device acts as a slave device, and vertically on the left when the device acts as a master device.</p>
	<p>Click it to change the language.</p>
	<p>Click it to log in to the MACC for remote O&M through the URL or by scanning the QR code.</p>
	<p>Click it to access the network setup wizard.</p>
	<p>Click it to log out of the web management system.</p>
	<p>Click Add or Batch Add to add one or more table entries in the dialog box that appears. After adding the table entries, you can view the added table entries on this page.</p>
	<p>Click it to delete the selected table entries in batches.</p>
	<p>Quickly locate the table entry you want to find through the drop-down list or by entering a keyword.</p>
	<p>Click them to edit, delete, or bind a table entry.</p>
	<p>If the toggle switch is displayed in gray and the button is on the left, the related function is disabled. If the toggle switch is displayed in blue and the button is on the right, the related function is enabled.</p>
	<p>Update data on the current page.</p>
	<p>Set the number of table entries displayed on a page. Click a page number or specify the page number to go to the corresponding page.</p>

2.3 Quick Setup

2.3.1 Configuration Preparations

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

2.3.2 Procedure

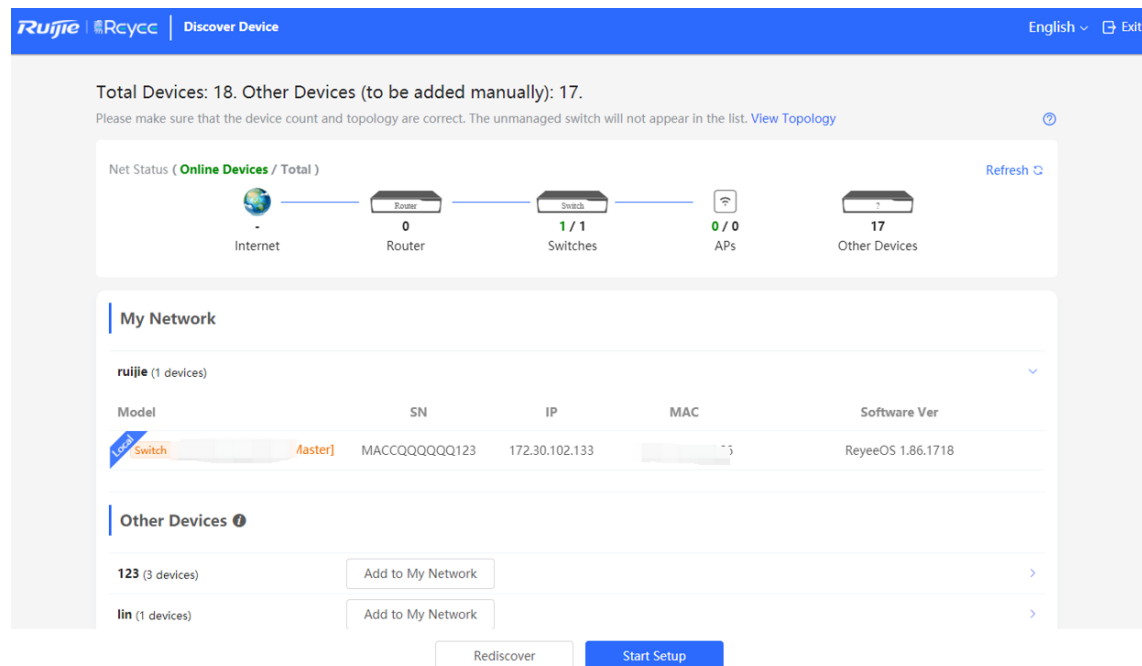
1. Adding Device to Network

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

i Note

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

If there are other devices in the network that are not added to the current network, you can click **Add to My Network** and enter the management password of the added device to manually add the corresponding device to the network where the device is located, and then start the network-wide configuration.



The screenshot displays the 'Discover Device' interface. At the top, it shows 'Total Devices: 18. Other Devices (to be added manually): 17.' Below this, a network status diagram shows connections between Internet, Router (0), Switches (1/1), APs (0/0), and Other Devices (17). The 'My Network' section lists one device: a Ruijie Switch with SN MACCQQQQ123, IP 172.30.102.133, and Software Ver ReyeeOS 1.86.1718. The 'Other Devices' section shows 123 devices and 1 device, each with an 'Add to My Network' button. At the bottom, there are 'Rediscover' and 'Start Setup' buttons.

2. Creating a Web Project

Click **Start Setup** to set the networking modes and management password of the device.

(1) **Network Name:** Identify the network where the device is located.

Internet: Select the networking mode.

- o **DHCP:** An IP address is assigned to the device by the uplink DHCP server. By default, the device detects

whether the IP address can be dynamically obtained. If the IP address is obtained successfully, there is no need to manually set the IP address.

- o **Static IP:** The user manually enter a specified IP address, subnet mask, gateway IP address, and DNS address.
- (2) **Management Password:** Set the password for logging in to the management page.
 - (3) **Country/Region:** Select the country or region where the device is located.
 - (4) **Time Zone:** Set the system time. The network time server is enabled to provide time services by default. Please select your actual time zone.

Click **Create Network & Connect** to deliver related configuration for initialization and detect the network. After completing the quick setup, the new device is connected to the Internet, and you can continue to bind the device to the cloud account for remote management. For specific operations, please refer to the instructions on the page to log in to the Noc Cloud platform for configuration.

Note

- Click **Exit** in the upper right corner and follow prompts to perform operations. Then, the device can skip quick setup to go to the Eweb management system. To configure again after exiting or completing the quick configuration, click the sign in the navigation bar at the top of the web page.
- After changing the management password, you need to re-visit the device management address and use the new password to log in to the device.

2.4 Work Mode

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

Self-Organizing Network: After the self-organizing network discovery function is enabled, the device can be discovered in the network and discover other devices in the network. Devices network with each other based on the device status and synchronize global configuration. You can log in to the Web management page of the

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

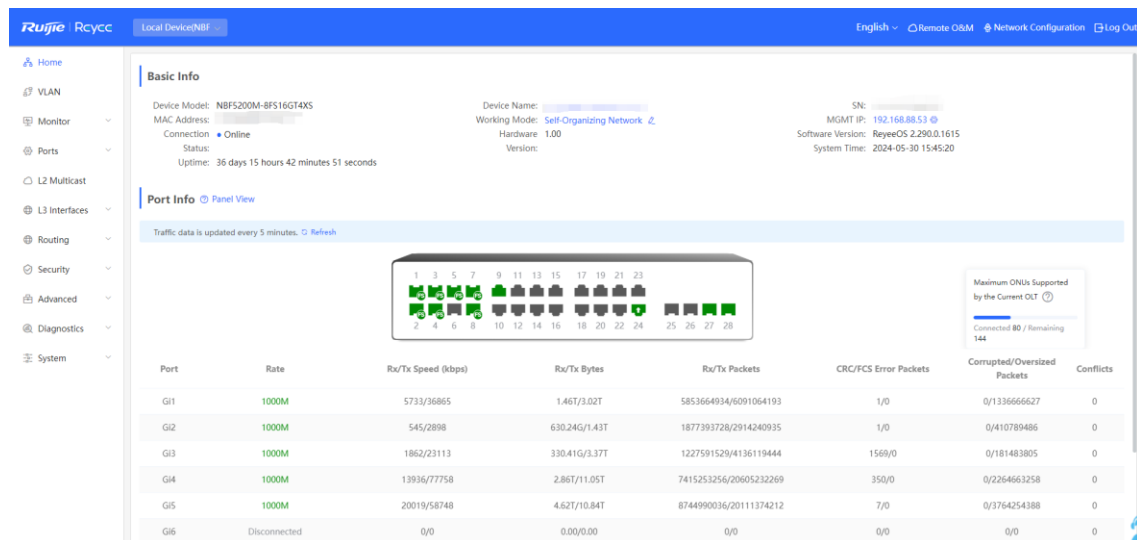
When the device is in self-organizing network mode, the Web page has two configuration modes: the network mode and the local device mode. For more information, see [Switching the Management Mode](#).

Standalone mode: If the self-organizing network discovery function is disabled, the device will not be discovered in the network. After logging in to the Web page, you can configure and manage only the currently logged in device. If only one device is configured or global configuration does not need to be synchronized to the device, you can disable the self-organizing network discovery function.

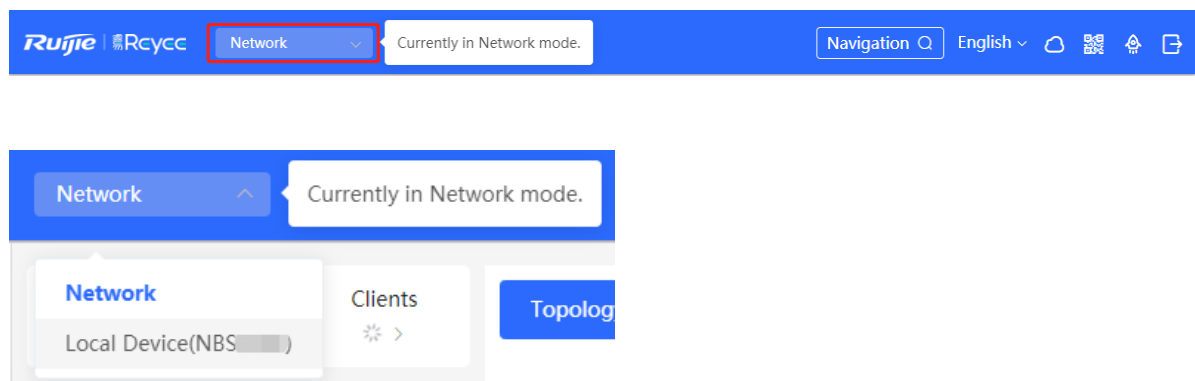
2.5 Switching the Management Mode

In standalone mode, you can configure and manage only the current logged in device without self-organizing network function. As shown in Figure 2-1.

Figure 2-1 The Web Page in Standalone Mode



In self-organizing network mode, the Web page has the network mode and the local device mode. Click the **Currently in Network** mode in the navigation bar and select the desired mode from the drop-down list box.



- The network mode: Display the management information of all devices in the network and configure all

devices in the current network from the network-wide perspective. As shown in Figure 2-2;

Figure 2-2 The local device mode: Only configure the device that you log in to. As shown in Figure 2-3. The Web Page in Network Mode in Self-Organizing Mode

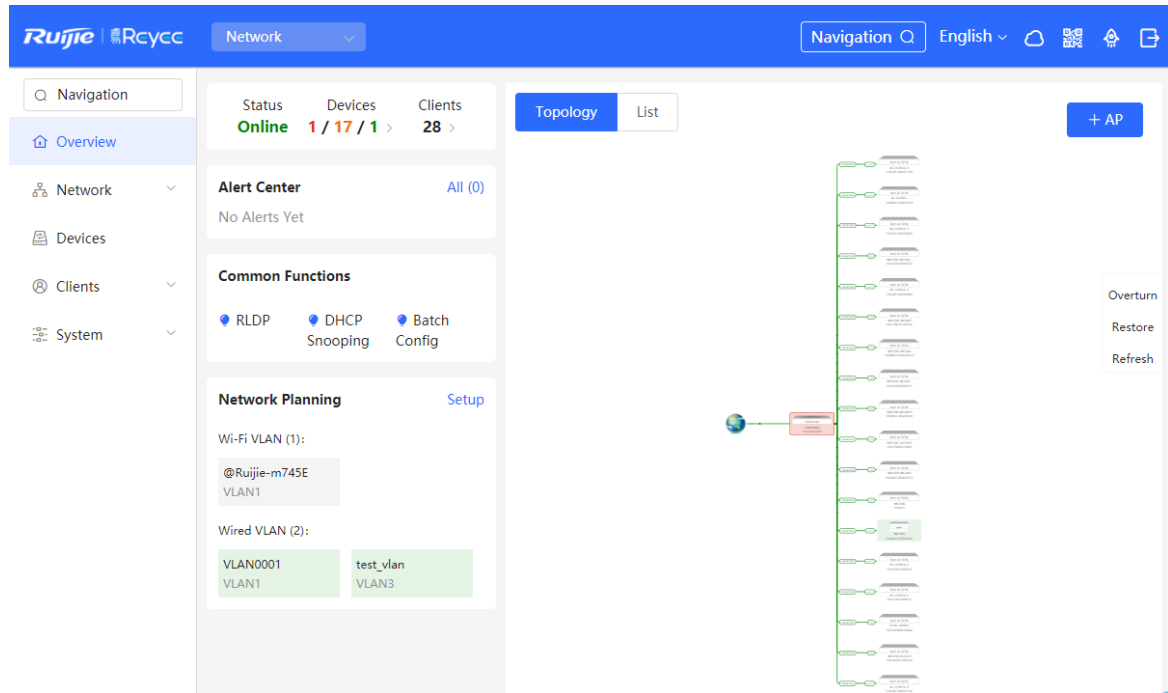
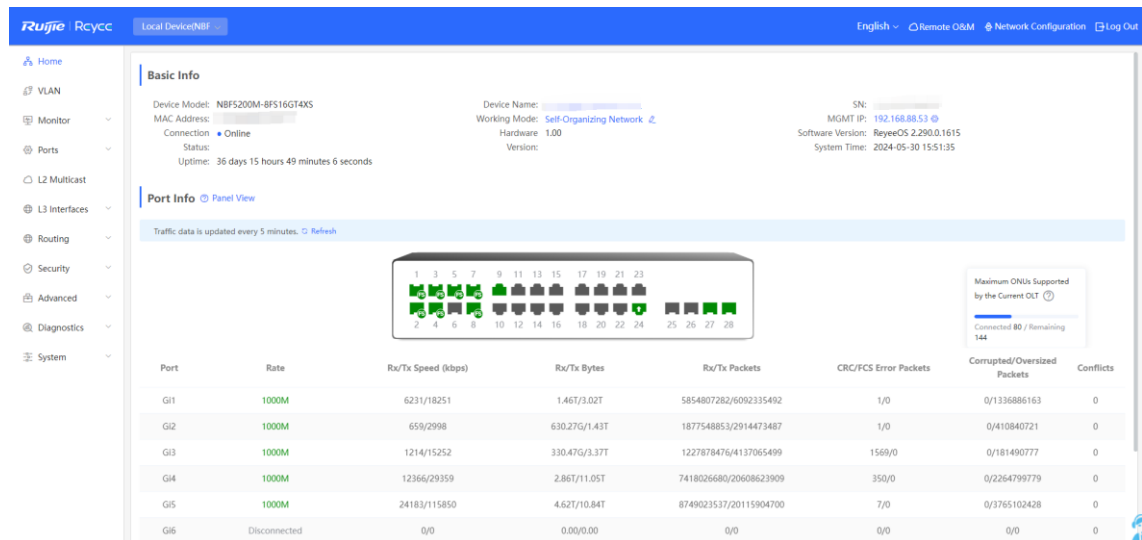


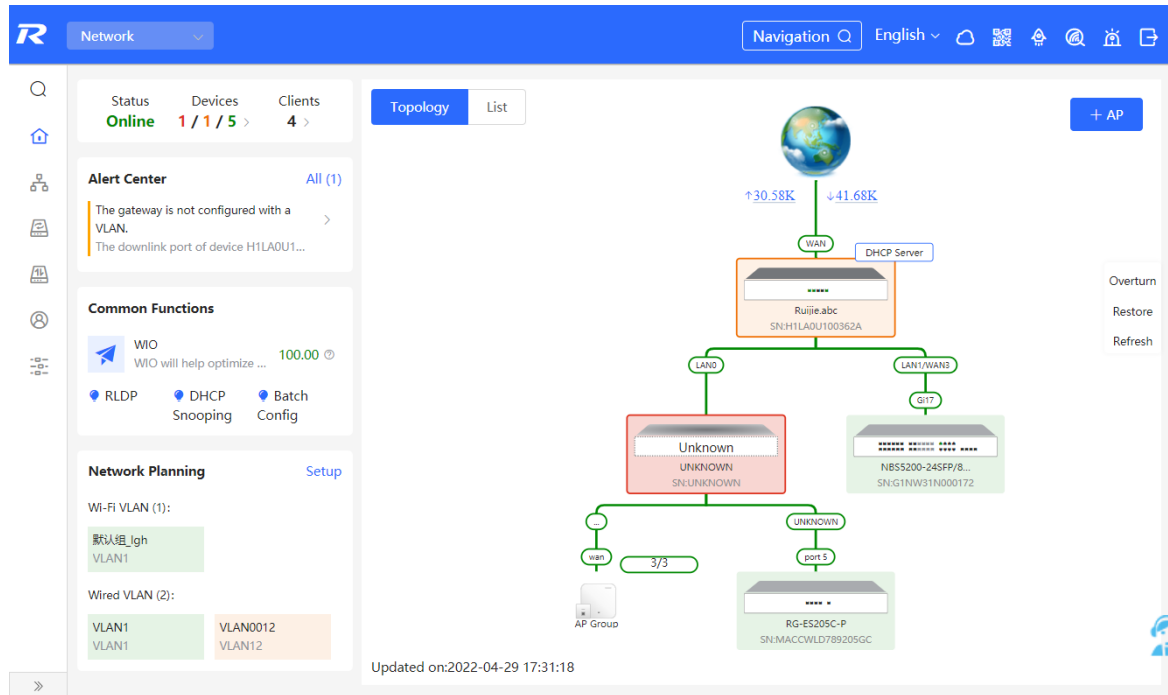
Figure 2-3 The Web Page in Local Device Mode in Self-Organizing Mode



3 Network management

3.1 Overviewing Network Information

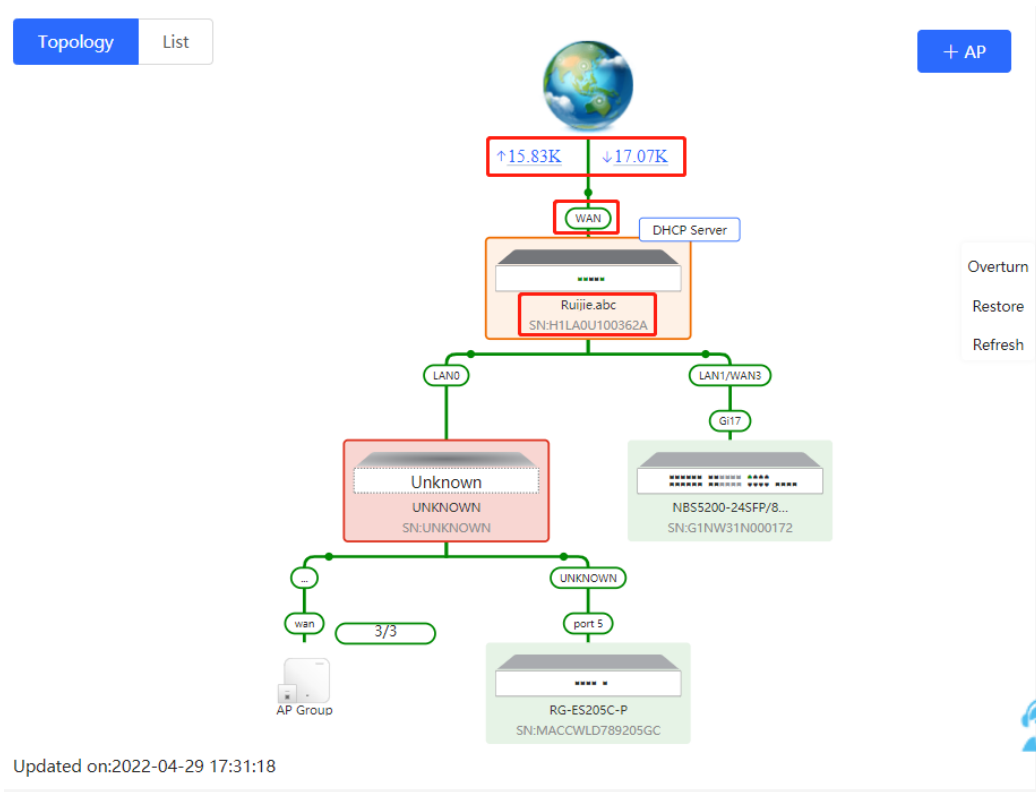
In network mode, the **Overview** page displays the current network topology, uplink and downlink real-time traffic, network connection status, and number of users and provides short-cut entries for configuring the network and devices. Users can monitor and manage the network status of the entire network on the page.



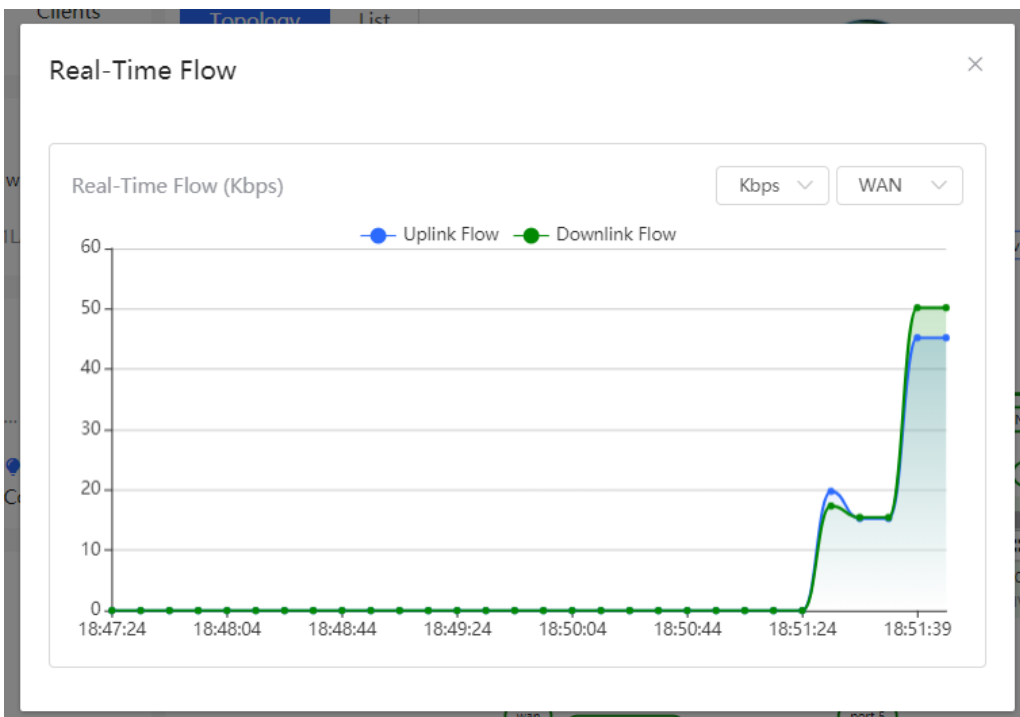
3.2 Viewing Networking Information


Choose **Network > Overview**.

The networking topology contains information about online devices, connected port numbers, device SNs, and uplink and downlink real-time traffic.



- Click a traffic data item to view the real-time total traffic information.



- Click a device in the topology to view the running status and configuration of the device and configure device functions. By default, the product model is used as the device name. Click  to modify the device name so that the description can distinguish devices from one another.

The screenshot shows the configuration page for a Ruijie EG205G device. At the top, the Hostname is 'Ruijie.abc', Model is 'EG205G', and SN is 'H1LA0U100362A'. Software version is 'ReyeeOS 1.86.1619', MGMT IP is '192.168.110.1', and MAC is '00:74:9c:87:6d:85'. On the left is a topology view with a 'Refresh' button. The main area is divided into 'Port Status' and 'VLAN' sections. The 'Port Status' section shows icons for LAN0, LAN1, LAN2, WAN1, and WAN. The 'VLAN' section has a table for 'Default VLAN':

Interface	IP	IP Range	Remark
LAN0,1	192.168.110.1	192.168.110.1-192.168.110.254	

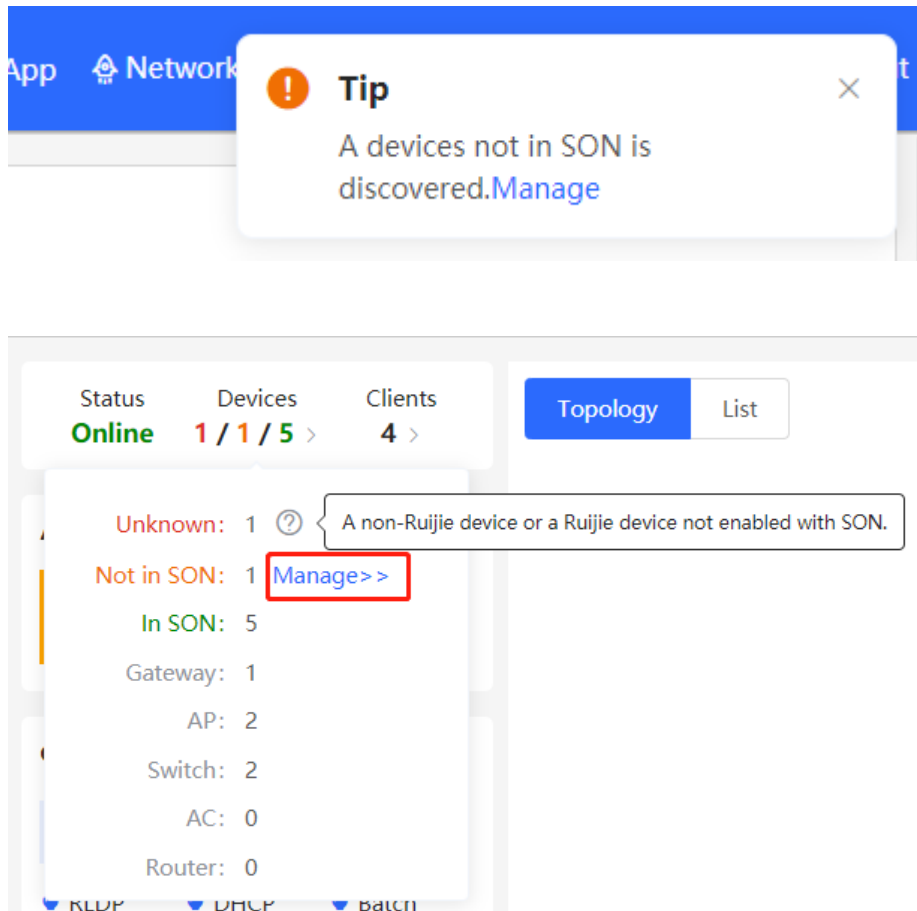
- The update time is displayed in the lower-left corner of the topology view. Click **Refresh** to update the topology to the latest state. It takes some time to update the topology data. Please wait patiently.

This screenshot shows a detailed network topology. At the top, there are traffic indicators: '+73.05K' and '-342.99K'. The central device is 'Ruijie.abc' (SN: H1LA0U100362A) with a 'DHCP Server' role. It is connected to a 'WAN' port. Below it, there are two main branches: 'LAN0' and 'LAN1/WAN3 (G1/7)'. The 'LAN0' branch leads to an 'Unknown' device (SN: UNKNOWN), which is further connected to an 'AP Group' (2/2). The 'LAN1/WAN3' branch leads to a switch (SN: G1NW31N000172), which is connected to another switch (SN: MACCWLD789205GC). On the right, there are buttons for 'Overturn', 'Restore', and 'Refresh' (highlighted with a red box). At the bottom left, the update time is 'Updated on:2022-05-19 11:06:40' (highlighted with a red box).

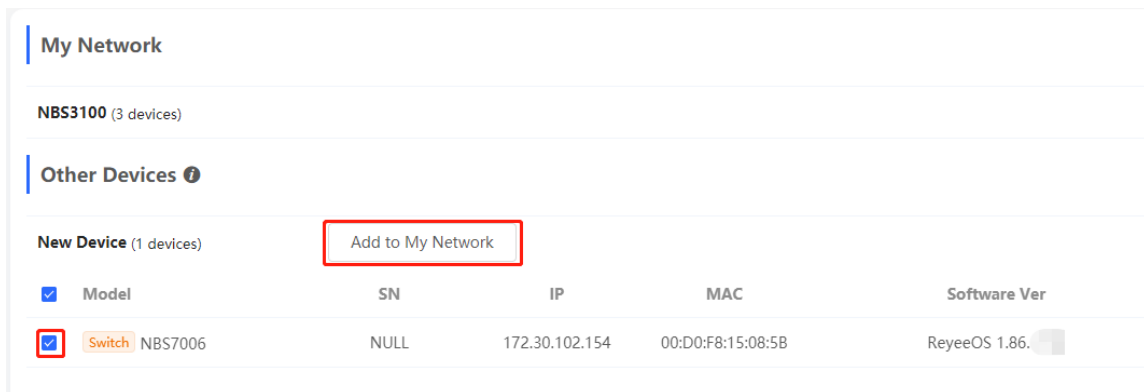
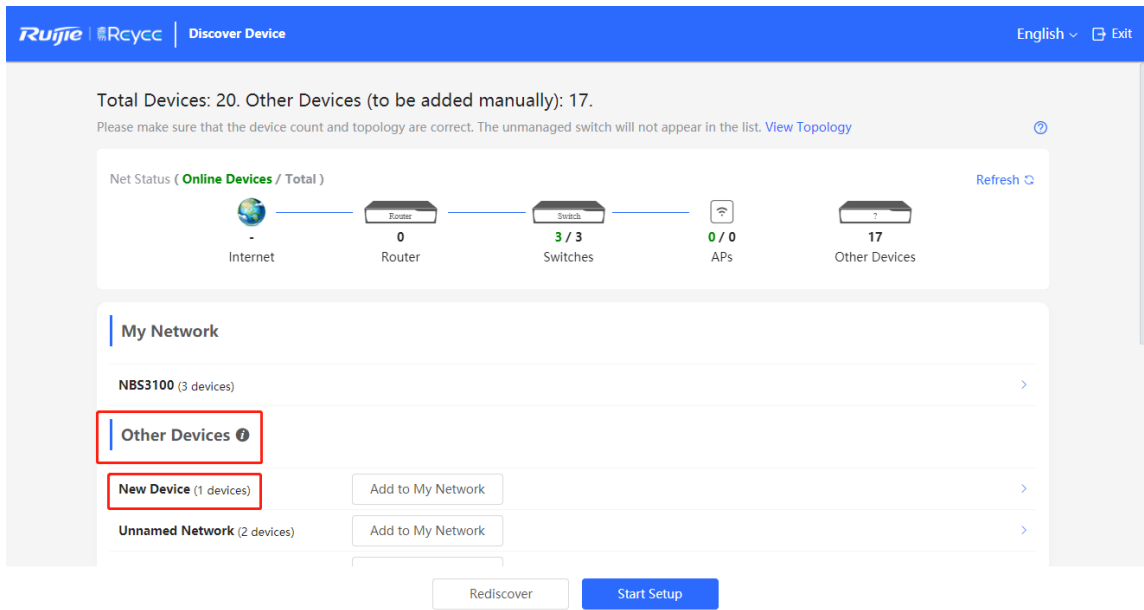
3.3 Adding Networking Devices

3.3.1 Wired Connection

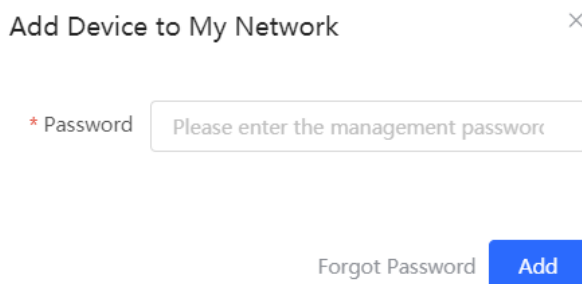
- (1) When a new device connects to an existing device on the network, the system displays the message “A device not in SON is discovered.” and the number of such devices in orange under “Devices” on the upper-left corner of the [Overview] page. You can click **Manage** to add this device to the current network.



- (2) After the system switches to the **Network List** page, click **Other Network**. In the **Other Network** section, select the device to be added to the network and click **Add to My Network**.



- (3) You do not need to enter the password if the device to add is newly delivered from factory. If the device has a password, enter the configuring password of the device. Device addition fails if the password is incorrect.



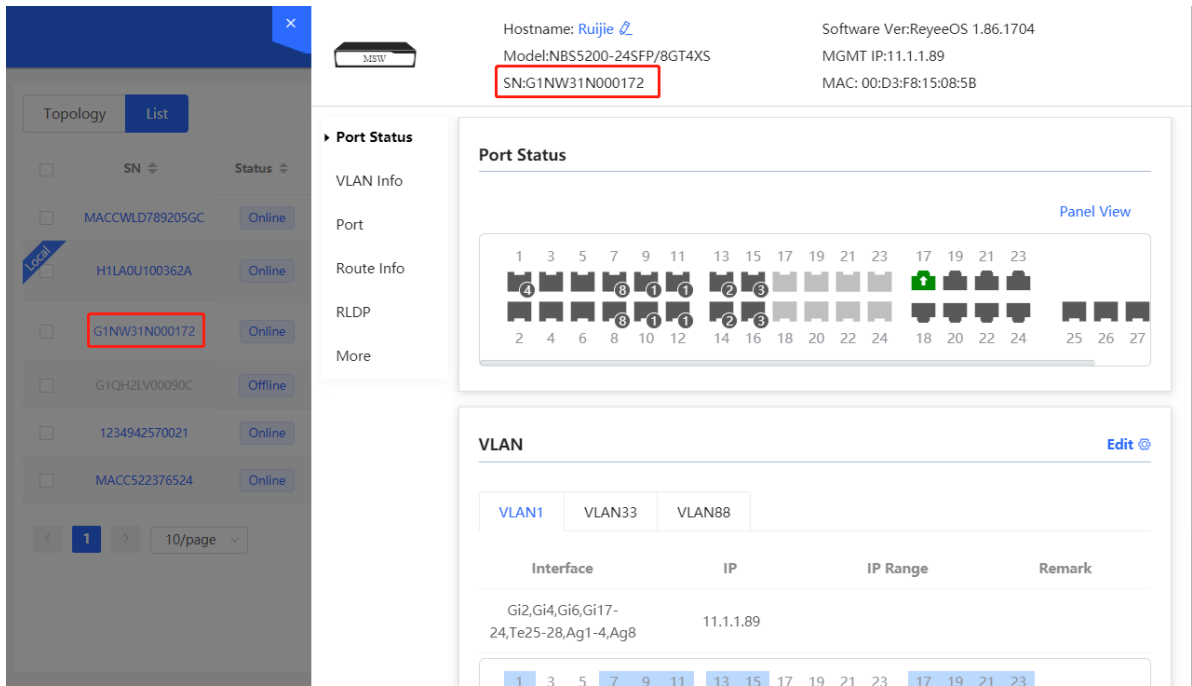
3.4 Managing Networking Devices

On the **Overview** page, click **List** in the upper-left corner of the topology or click **Devices** in the menu bar to switch to the device list view. Then, you can view all the device information in the current networking. Users only need to log in to one device in the network to configure and manage devices in the entire network.

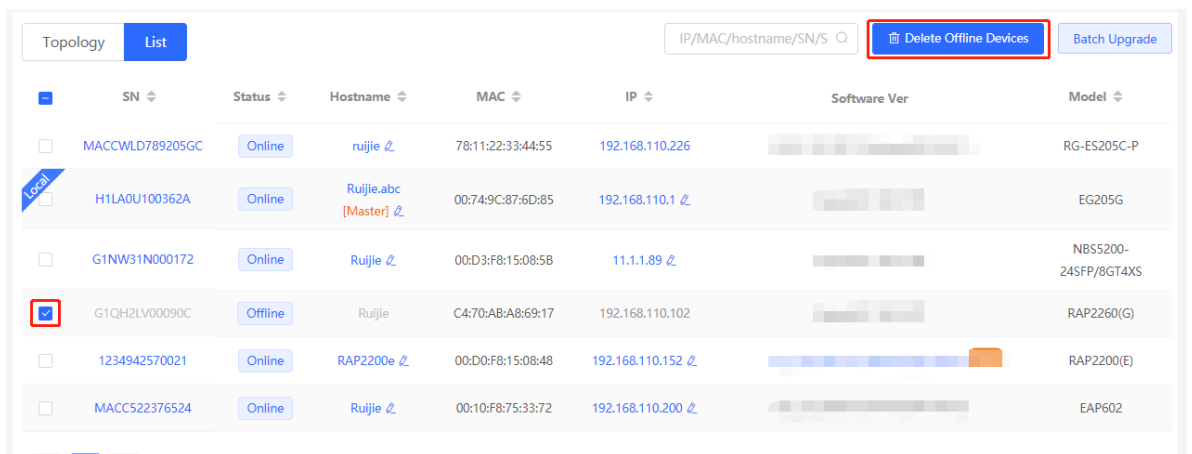
The screenshot displays the Ruijie RCloud management interface. At the top, there is a navigation bar with the Ruijie logo, a 'Network' dropdown, and a search bar. Below this, a left sidebar contains navigation options: Overview, Network, Devices (highlighted with a red box), Gateway, Clients, and System. The main content area is divided into several sections: 'Status' (Online, 1/6 devices, 3 clients), 'Alert Center' (No Alerts Yet), 'Common Functions' (WIO Disabled, RLDLP, DHCP Snooping, Batch Config), and 'Network Planning' (Setup). A network topology diagram is shown on the right, with a 'List' button highlighted in a red box. Below the topology, there is a search bar for IP/MAC/hostname/SN/S, and buttons for 'Delete Offline Devices' and 'Batch Upgrade'. A table lists the devices with columns for SN, Status, Hostname, MAC, IP, Software Ver, and Model. The table contains 5 rows of device information. At the bottom, there is a pagination control showing page 1 of 10 per page, and a 'Total 5' indicator.

SN	Status	Hostname	MAC	IP	Software Ver	Model
MACCWLD789205GC	Online	rujije	78:11:22:33:44:55	192.168.110.226	ESW_	RG-ES205C-P
H1LA0U100362A	Online	Ruijie.abc [Master]	00:74:9C:87:6D:85	192.168.110.1	ReyeeOS	EG205G
G1NW31N000172	Online	Ruijie	00:D3:F8:15:08:5B	192.168.110.89	ReyeeOS	NBS5200-24SFP/8GT4XS
1234942570021	Online	RAP2200e	00:D0:F8:15:08:48	192.168.110.152	AP_ new	RAP2200(E)
G1QH2LV00090C	Online	Ruijie	C4:70:AB:A8:69:17	192.168.110.102	ReyeeOS	RAP2260(G)

- Click the device **SN** to configure the specified device separately.

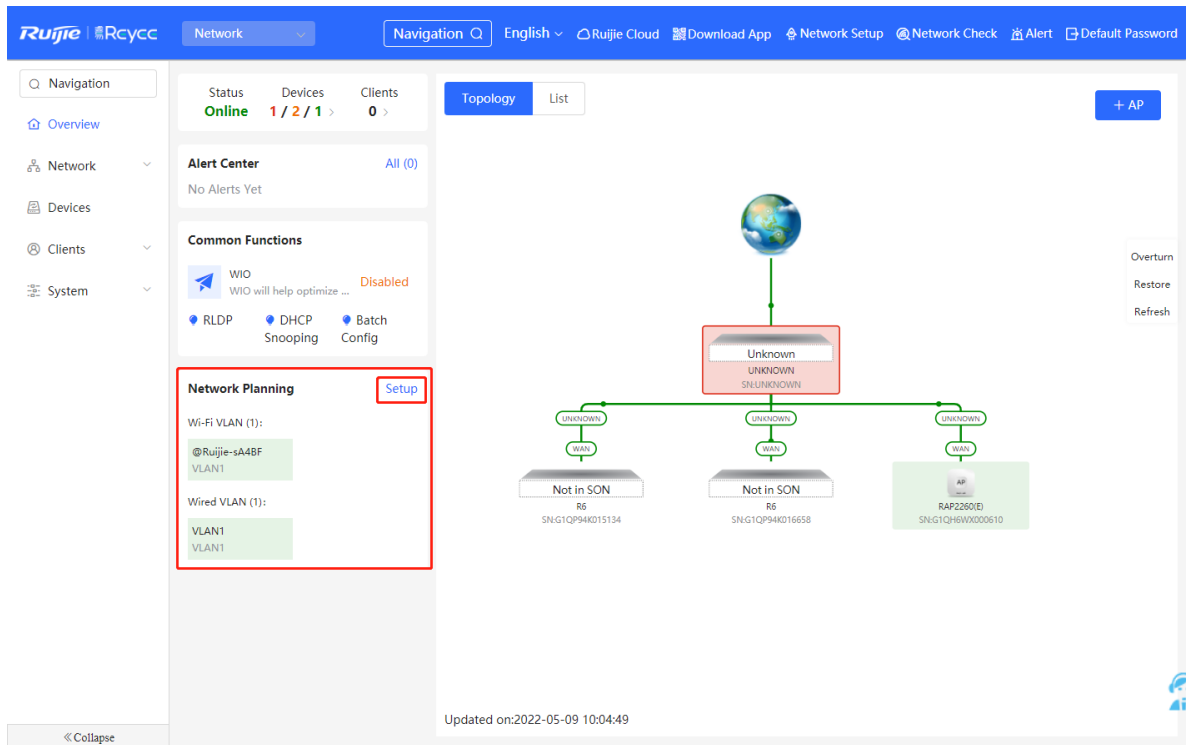


- Check offline devices and click **Delete Offline Devices** to remove them from the list and networking topology.



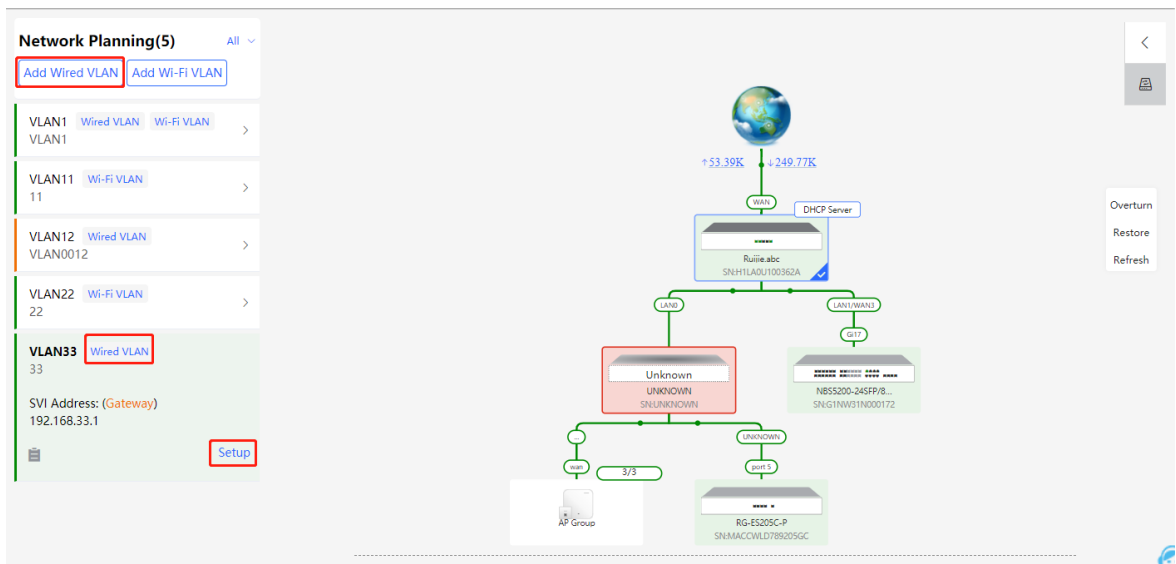
3.5 Configuring the Service Network

The wireless and wired network configurations of the current network are displayed in the lower-left of the **Overview** page. Click **Setup** to switch to the service network configuration page (or click **Network > Network Planning**).



3.5.1 Configuring the Wired Network

- (1) Click **Add Wired VLAN** to add wired network configuration, or select an existing wired VLAN and click **Setup** to modify its configuration.



- (2) Configure a VLAN for wired access, specify the address pool server for access clients in this VLAN, and determine whether to create a new DHCP address pool. A switch or gateway device can be selected as the address pool server. After setting the service parameters, click **Next**.

Configure Network Planning/Add Wired VLAN

1 Configure VLAN Parameters 2 Configure Wired Access 3 Confirm Config Delivery

Description:

* VLAN ID:

Address Pool Gateway

Server

Gateway/Mask: /

DHCP Pool:

IP Range: -

[Next](#)

(3) Select the switch to configure in the topology, select the switch ports added to this VLAN, and click **Next**.

Configure Network Planning/Add Wired VLAN

Configure VLAN Parameters **Configure Wired VLAN**

VLAN33 (33) You have selected 2 device(s) with 6 port(s). [Panel View](#)

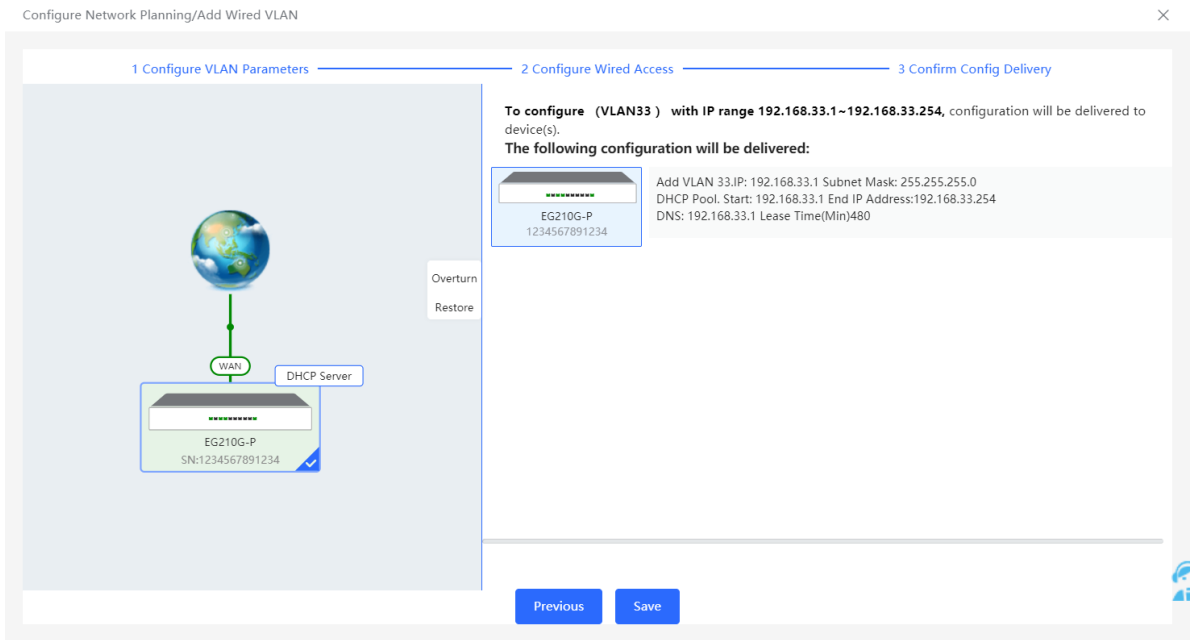
Available Unavailable Aggregate Uplink Copper Fiber

1	3	5	7	9	11	13	15	17	19	21	23		
2	4	6	8	10	12	14	16	18	20	22	24		
										25	26	27	28

Selected: Gi3, Gi5, Gi17...

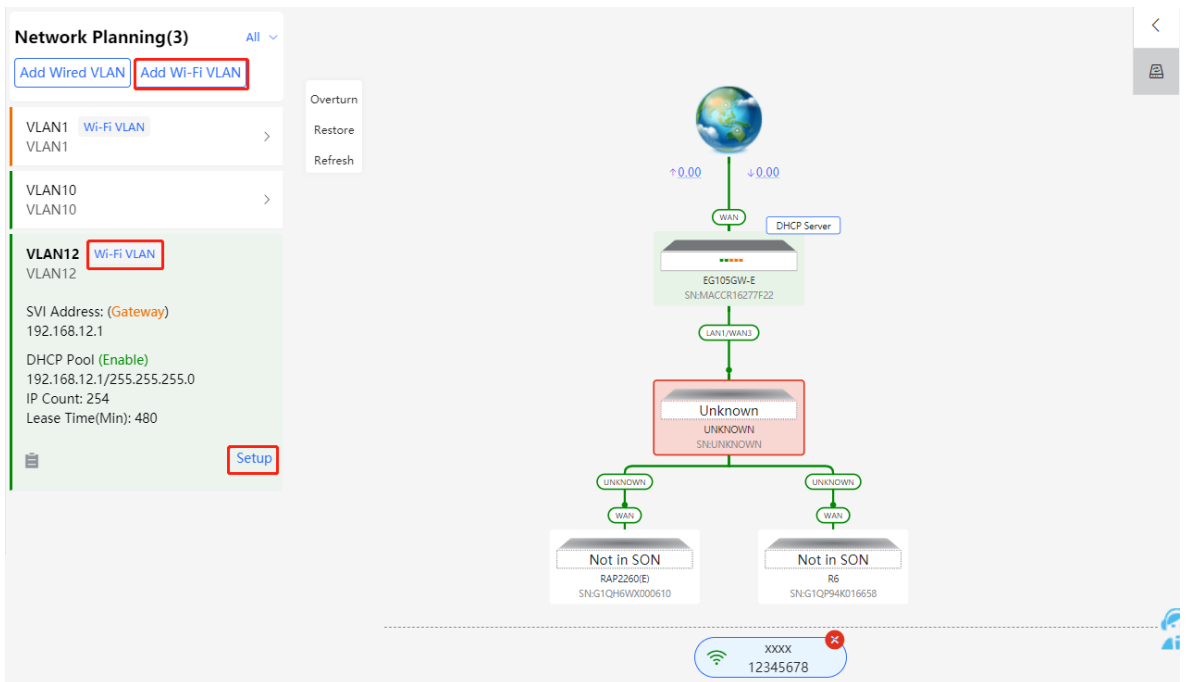
Note: You can click and drag to select one or more ports. [Select All](#) [Inverse](#) [Deselect](#)

(4) Confirm that the configuration items to be delivered are correct and then click **Save**. Wait a moment for the configuration to take effect.



3.5.2 Configuring the Wireless Network

- (1) Click **Add Wi-Fi VLAN** to add wireless network configuration, or select an existing Wi-Fi VLAN and click **Setup** to modify its configuration.



- (2) Set the Wi-Fi name, Wi-Fi password, and applicable bands. Click **Next**.

Configure Network Planning/Add Wi-Fi VLAN

1 Configure Wireless Access — 2 Configure VLAN Parameters — 3 Confirm Config Delivery

* SSID:

Security: Security Open

Band: 2.4G + 5G 2.4G 5G

- (3) Configure a VLAN for wireless access, specify the address pool server for access clients in this VLAN, and determine whether to create a new DHCP address pool. A switch or gateway device can be selected as the address pool server. After setting the service parameters, click **Next**.

Configure Network Planning/Add Wi-Fi VLAN

1 Configure Wireless Access — 2 Configure VLAN Parameters — 3 Confirm Config Delivery

Description:

* VLAN ID:

topo.addressPool Gateway

Gateway/Mask: /

DHCP Pool:

IP Range: -

- (4) Confirm that the configuration items to be delivered are correct and then click **Save**. Wait a moment for the configuration to take effect.

Configure Network Planning/Add Wi-Fi VLAN

1 Configure Wireless Access 2 Configure VLAN Parameters 3 Confirm Config Delivery

Overturn
Restore

To configure (VLAN13) with IP range 192.168.13.1~192.168.13.254, configuration will be delivered to device(s).
The following configuration will be delivered:

0

AP SSID:test Password:12345678

EG105GW-E Add VLAN 13 IP: 192.168.13.1 Subnet Mask: 255.255.255.0
MACCR16277F22 DHCP Pool: Start: 192.168.13.1 End IP Address:192.168.13.254
SN:MACCR16277F22 DNS: 192.168.13.1 Lease Time:Min:480

Previous Save

3.6 Processing Alerts

Choose **Network > Overview**.

If a network exception occurs, alert message on this exception and the corresponding solution are displayed on the **Overview** page. Click the alert message in the **Alert Center** section to view the faulty device, problem details, and its solution. Troubleshoot and process the alert according to the solution.

The screenshot shows a network management dashboard. On the left, there are navigation icons and a sidebar with sections: 'Alert Center' (highlighted with a red box), 'Common Functions' (WIO, RLDP, DHCP Snooping, Batch Config), and 'Network Planning' (Wi-Fi VLAN, Wired VLAN). The main area displays a network topology diagram with a central gateway device 'Ruijie abc' connected to various LAN and WAN ports. A red box highlights an alert in the 'Alert Center' section.

This is a partial view of the network management interface, showing the left sidebar with navigation icons and the 'Alert Center' section. The alert message is visible: 'The gateway is not configured with a VLAN. The downlink port of device H1LA0U1...'.

The 'Alerts' section displays a 'Current Alert' with the following text: 'The downlink port LAN1/WAN3 of device H1LA0U100362A is not allowed to be configured with allowed VLAN 12.' Below the alert is a 'Solution' section: 'Please configure the LAN IP address.' To the right, a detailed network topology diagram shows the gateway device connected to multiple LAN and WAN ports, with various other devices like switches and APs connected to these ports.

3.7 Viewing Online Clients

The **Clients** in the upper-left corner of the **Overview** page displays the total number of online clients in the current network; moving the cursor to the number of users will display the number of current wired users, wireless users in the 2.4GHz band, and wireless users in the 5GHz band.

Click to switch to the online clients page (or click **Clients > Online Clients**).

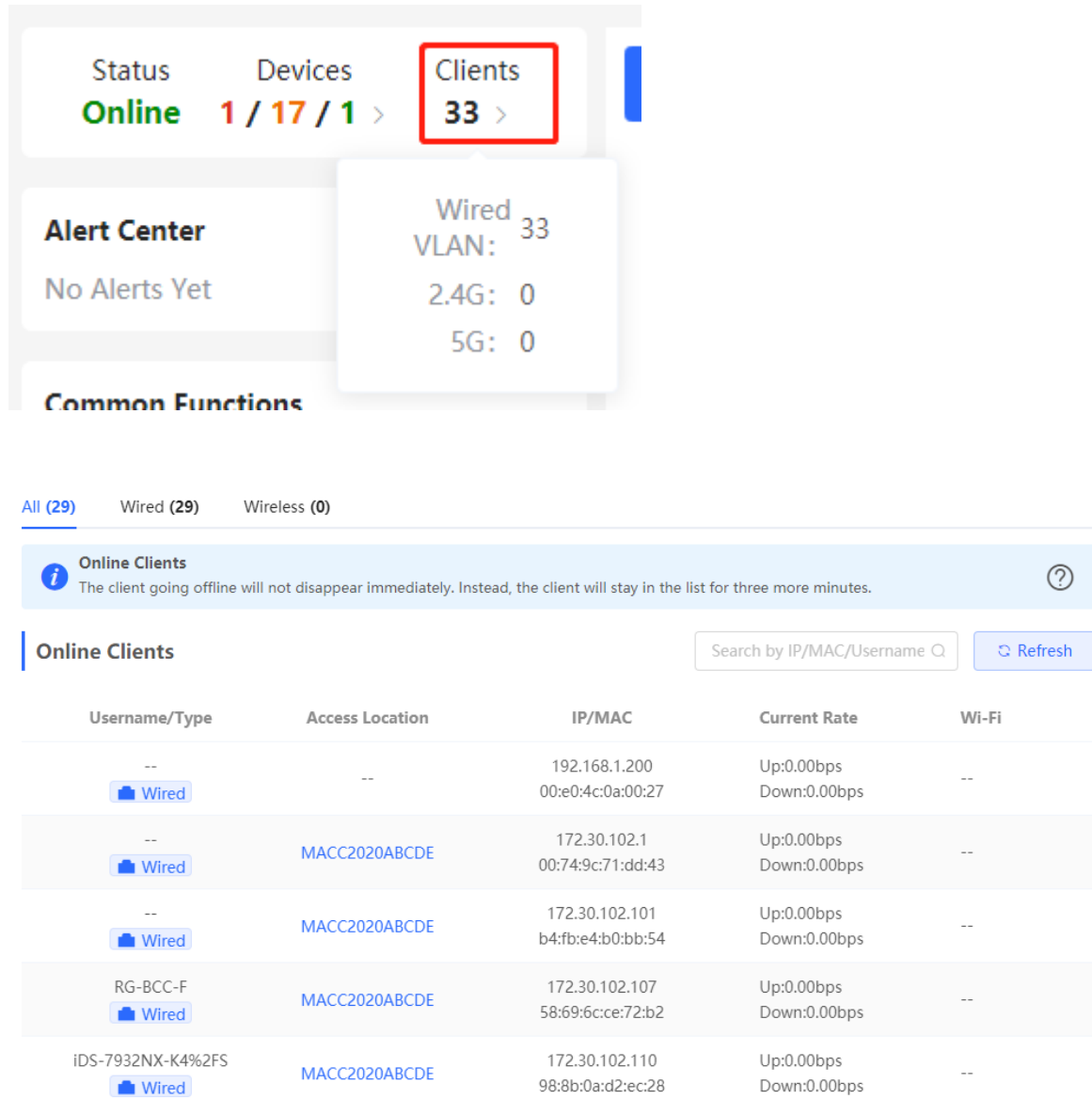


Table 3-1 Description of Online Client Information

Field	Description
Username/Type	Indicate the name and access type of the client. The access type can be wireless or wired.
Access Location	Indicate the SN of the device that the user accesses to. You can click it to view the access port during wired access.

Field	Description
IP/MAC	The IP address and the MAC address of the client.
Current Rate	Indicate the uplink and downlink data transmission rates of the client.
Wi-Fi	Wireless network information associated with wireless clients, including channel, signal strength, online time, negotiation rate, etc.

3.8 Smart Device Network

3.8.1 Overview

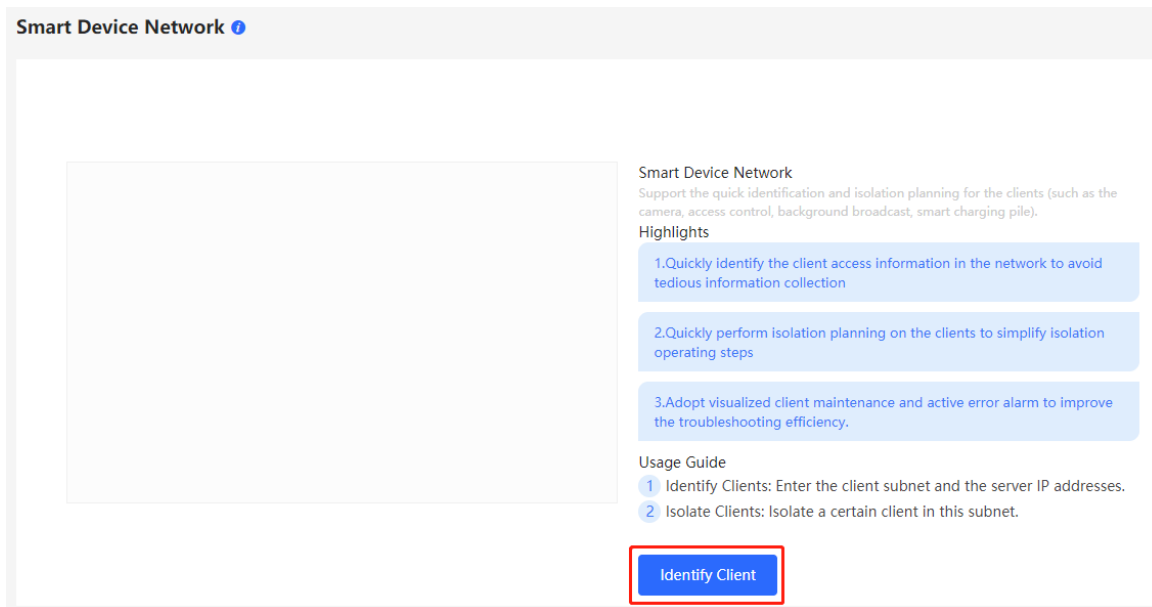
The smart device network is used to quickly plan and set up an isolation network for smart clients, so as to isolate the client network from the normal service network and other types of clients, and improve the stability of the network. The smart device network supports rapid identification of various types of clients (such as cameras, access control, background broadcasting, smart charging piles, etc.) and batch execution of isolation planning on clients. Compared with traditional client network planning and deployment steps, it eliminates the tedious process, collects information and simplifies the steps to set up client isolation.

After setting up the smart device network, the page visually displays client information, and actively alerts abnormality, which can effectively improve the efficiency of troubleshooting.

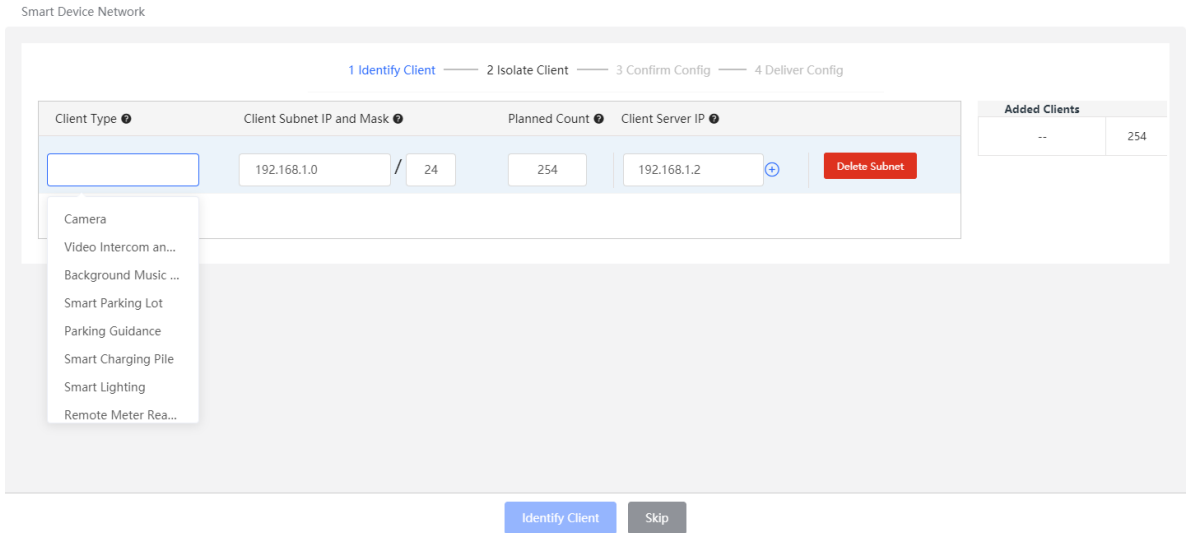
3.8.2 Procedure

Choose **Network > Clients > Smart Device Network**.

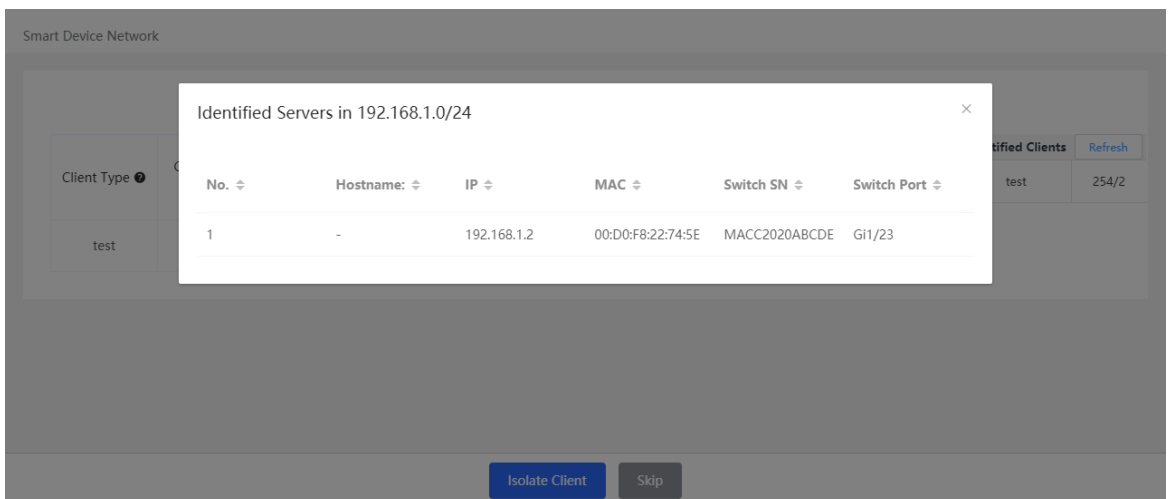
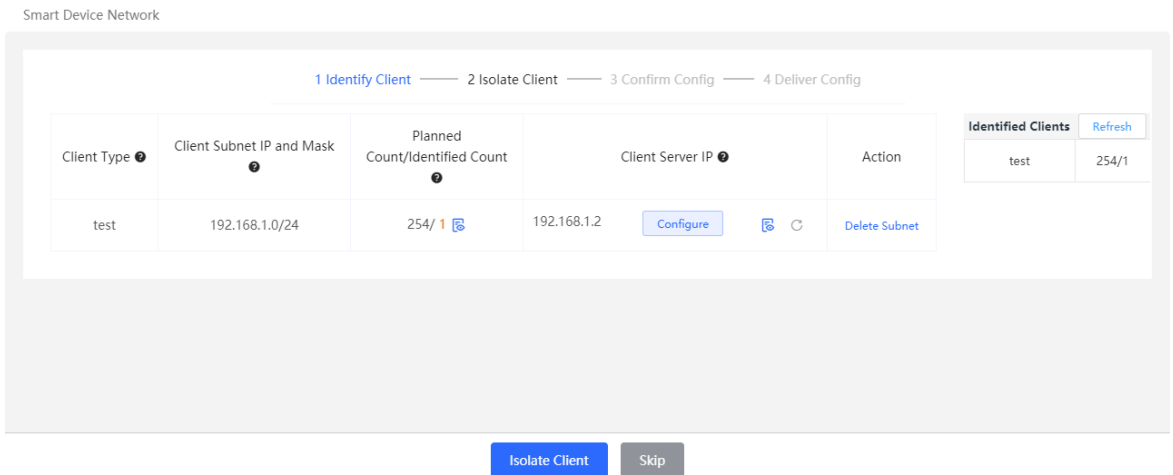
(1) Click **Identify Client**.



(2) Click **+Client Subnet**, enter the client type (which can be selected or customized in the drop-down box), the network segment of the client, the planned number and the corresponding server IP address to identify the client. Multi-type client network segments can be set. Click **Identify Client** after filling in.



- (3) Display the identified client and client server information, including IP address, MAC address, SN number of the connected switch and connection port. Click to view the detailed information. If the connection information to the client server is not identified, you need to click **Configure** and fill in the relevant information manually. After confirming that the client device information is correct, click **Isolate Client**.



- (4) Input the name of the VLAN, VLAN ID, gateway address, and subnet mask of the isolated client. Check the target network segment and click **Generate Config**.

Smart Device Network

1 Identify Client — 2 Isolate Client — 3 Confirm Config — 4 Deliver Config

<input checked="" type="checkbox"/> Subnet	Isolated VLAN Name	VLAN ID	Gateway Address	Subnet Mask	Client Isolation Planning
192.168.1.0/24 test 254 Server 1	test_vlan	3	192.168.1.240	255.255.255.0	192.168.1.0/24 VLAN3

- (5) After confirming the configuration, click **Deliver Config**. If you need to modify it, you can click **Previous** to return to the setting page.

Smart Device Network

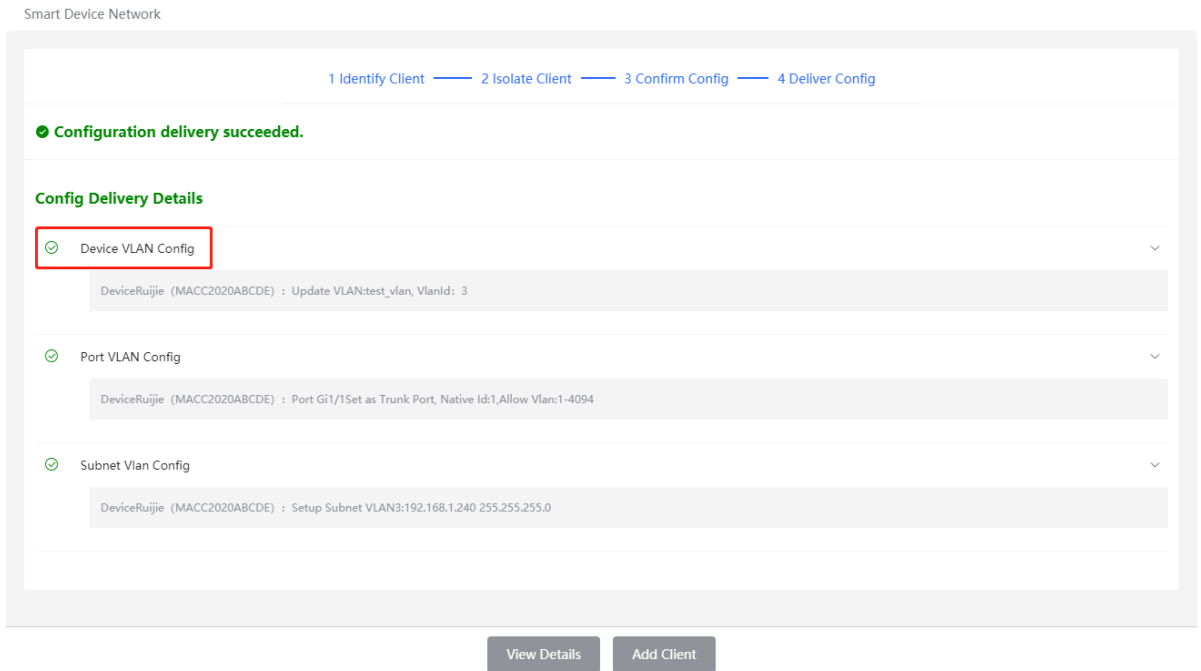
1 Identify Client — 2 Isolate Client — 3 Confirm Config — 4 Deliver Config

To ensure effective network planning, 1 devices are added autom...

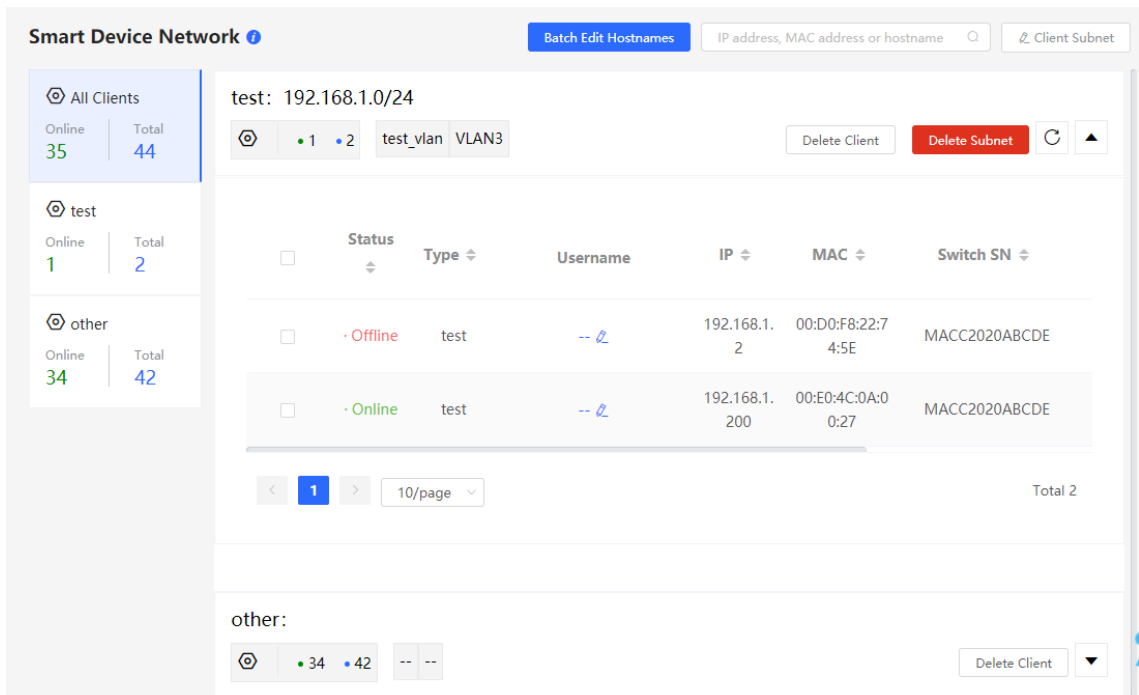
Target Devices
Ruijie(MACC2...)

Overturn
Restore

- (6) The page displays that the configuration has been delivered successfully, indicating that the settings have been completed. Click the configuration item to view the configuration delivery details. After the configuration is delivered, click **View Details** to switch to the page that displays monitoring information of the smart device network; click **Add Client** to continue setting the client network segment.



- (7) After completing the smart device network settings, you can view the client monitoring information on the page, including client online status, connection information, device information, and online and offline time. Select the client entry and click **Delete Client** to remove the specified client from the current network. Click **Batch Edit Hostnames** to import a txt file containing client IP and client name (one line for each client, each line contains an IP and a name, and the IP and the name are separated by the Tab key), and modify the client names in batches. Click **Client Subnet** to modify servers and isolate VLAN information, or add a new client network segment. Click **Delete Subnet** to delete the corresponding smart device network configuration.



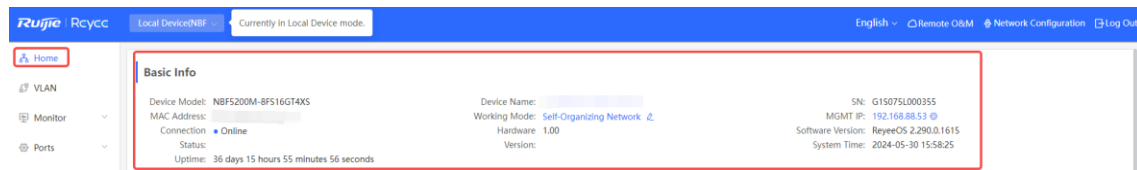
4 Basic Management

4.1 Overviewing Switch Information

4.1.1 Basic information about the Device

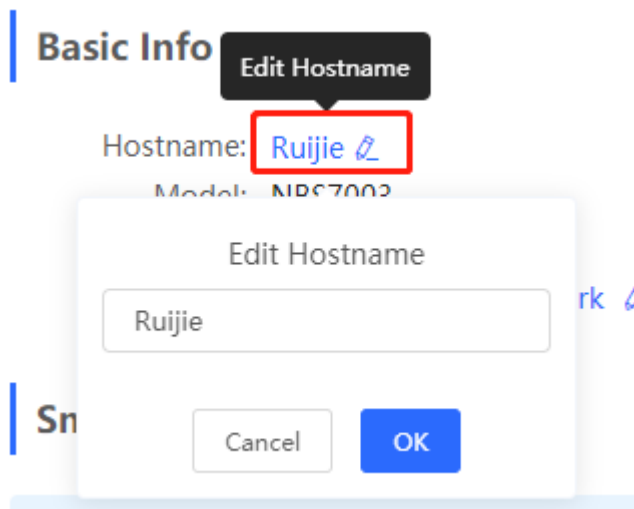
Choose **Local Device** > **Home** > **Basic Info** .

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



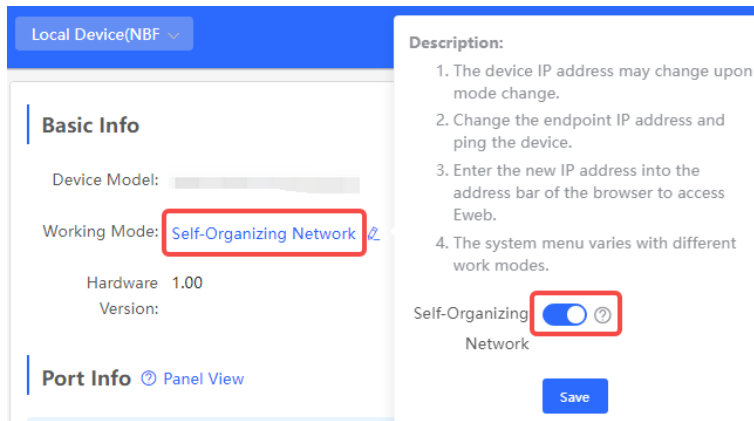
1. Setting the device name

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



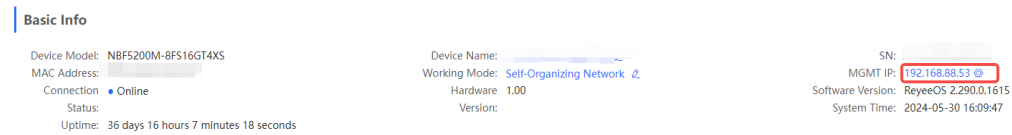
2. Switching the Work Mode

Click the current work mode to change the work mode.



3. Setting MGMT IP

Click current management IP address to jump to the management IP configuration page. For more information, see [5.6](#).



4.1.2 Port Info

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

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

The flow data will be updated every 5 minutes. Refresh

Port	Rate	Rx/Tx Speed (kbps)	Rx/Tx Bytes	Rx/Tx Packets	CRC/FCS Error Packets	Corrupted/Oversized Packets	Conflicts
Gi1	1000M	478/242	16.38G/4.03G	74718870/28166645	0/0	0/0	0
Gi2	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
Gi3	1000M	14/18	2.05G/13.88G	12265475/62920767	0/0	0/0	0
Gi4	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
Gi5	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
Gi6	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
Gi7	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
Gi8	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
Gi9	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0

Port Info Panel View

Role	Status
Copper	1G/2.5G/10G
Fiber	10M/100M
Uplink	Exception
PoE	Disconnected
PoE Error	Disable
Aggregate	

- Move the cursor to the icon of a port (for example, Gi14) on the port panel, and more information about the port will be displayed, including the port ID, port status, port rate, uplink and downlink traffic, transmission rate, and optical/electrical attribute of the port.

Port Info [Panel View](#)

The flow data will be updated every 5 minutes. [Refresh](#)

Port	Rate	Rx/Tx Speed (kbps)	Packets	CRC/FCS Error Packets	Corrupted/Oversized Packets	Conflicts
Gi1	1000M	103/85	281666	0/0	0/0	0
Gi2	Disconnected	0/0		0/0	0/0	0

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

Port Info [Panel View](#)

The flow data will be updated every 5 minutes. [Refresh](#)

Port	Rate	Rx/Tx Speed (kbps)	Rx/Tx Bytes	Rx/Tx Packets	CRC/FCS Error Packets	Corrupted/Oversized Packets	Conflicts
Gi1	1000M	206/124	16.38G/4.03G	74718870/281666 45	0/0	0/0	0

4.2 Port Flow Statistics

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

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

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

Note

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

Port Info

Clear Selected
Clear All

The flow data will be updated every 5 minutes. [Refresh](#)

<input type="checkbox"/>	Port	Rate	Rx/Tx Speed (kbps)	Rx/Tx Bytes	Rx/Tx Packets	CRC/FCS Error Packets	Corrupted/Oversized Packets	Conflicts
<input type="checkbox"/>	Gi1 ↑	1000M	342/55	16.39G/4.04G	74749819/28194 138	0/0	0/0	0
<input type="checkbox"/>	Gi2	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
<input type="checkbox"/>	Gi3	1000M	25/268	2.05G/13.88G	12270309/62929 657	0/0	0/0	0
<input type="checkbox"/>	Gi4	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
<input type="checkbox"/>	Gi5	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0
<input type="checkbox"/>	Gi6	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0

4.3 MAC Address Management

4.3.1 Overview

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

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

MAC address entries are classified into the following types:

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

i Note

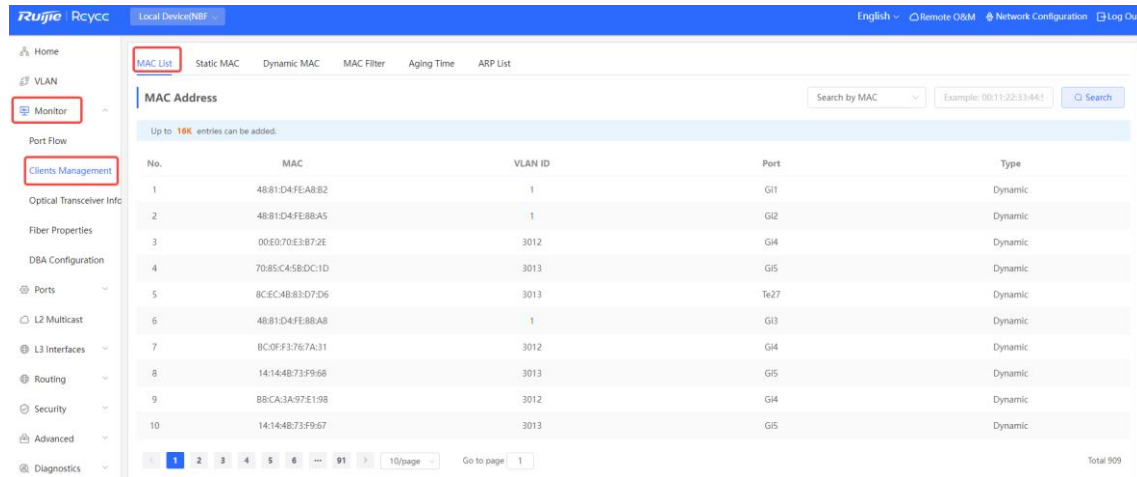
This section describes the management of static, dynamic, and filtering MAC address entries, without involving multicast MAC address entries.

4.3.2 Displaying the MAC Address Table

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

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

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



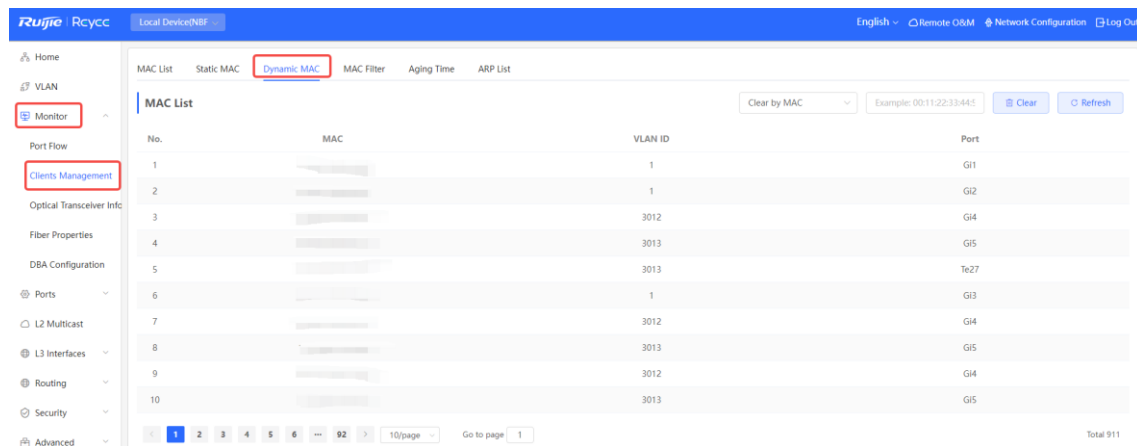
Note

The MAC address entry capacity depends on the product. For example, the MAC address entry capacity of the device shown in the figure above is 32K.

4.3.3 Displaying Dynamic MAC Address

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

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



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

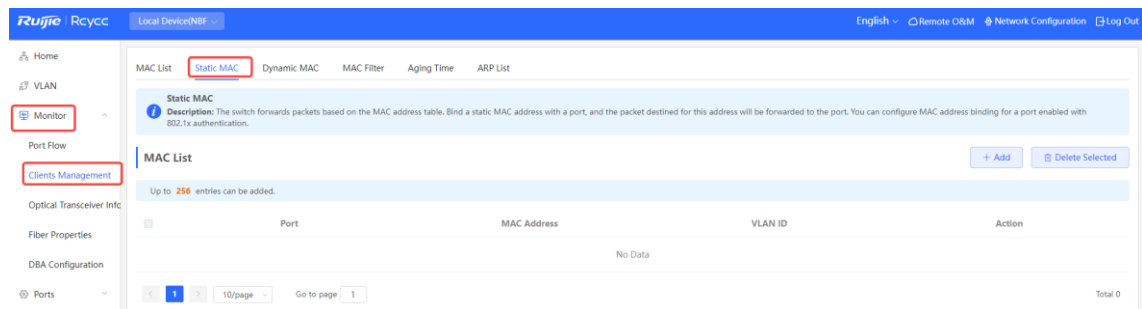
MAC List Clear by MAC Example: 00:11:22:33:44:55 Clear Refresh

No.	MAC	Port
1	54:BF:64:5C:90:5F	Gi1
2	58:69:6C:FF:1A:70	Gi1
3	8C:EC:4B:86:E3:B4	Gi1

Clear by MAC
Clear by Port
Clear by VLAN

4.3.4 Configuring Static MAC Binding

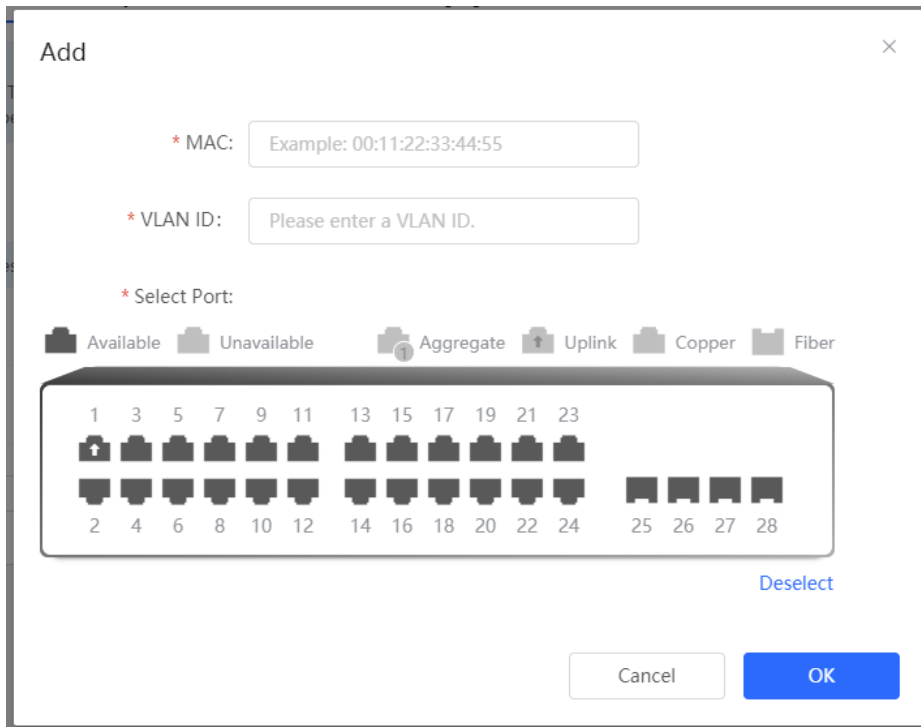
The switch forwards data based on the MAC address table. You can set a static MAC address entry to manually bind the MAC address of a downlink network device with the port of the device. After a static address entry is configured, when the device receives a packet destined to this address from the VLAN,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



1. Adding Static MAC Address Entries

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

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

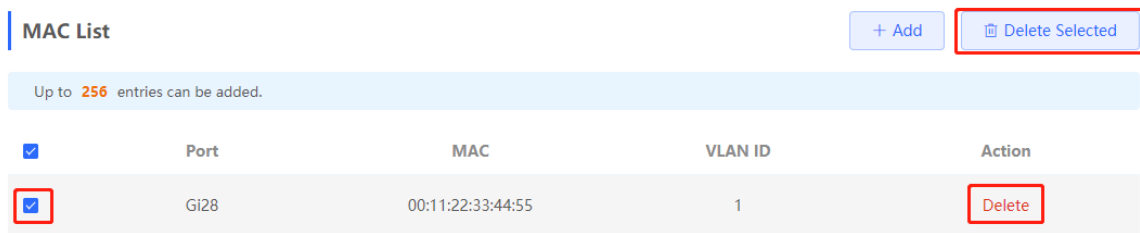


2. Deleting Static MAC Address Entries

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

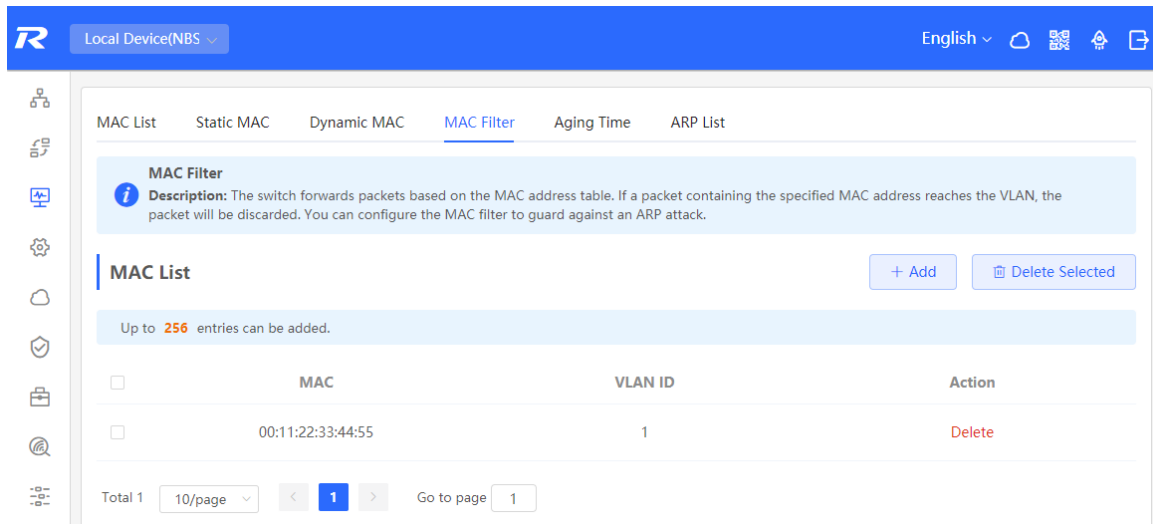
Batch delete: In **MAC List** , select the MAC address entries to be deleted and click **Delete Selected** . In the displayed dialog box, click **OK** .

Delete an entry: In **MAC List** , find the entry to be deleted, click **Delete** in the last **Action** column. In the displayed dialog box, click **OK** .



4.3.5 Configuring MAC Address Filtering

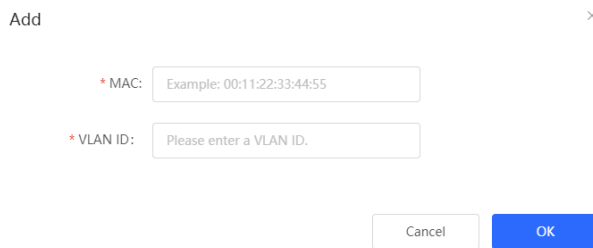
To prohibit a user from sending and receiving packets in certain scenarios, you can add the MAC address of the user to a filtering MAC address entry. After the entry is configured, packets whose source or destination MAC address matches the MAC address in the filtering MAC address entry are directly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



1. Adding Filtering MAC Address

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

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

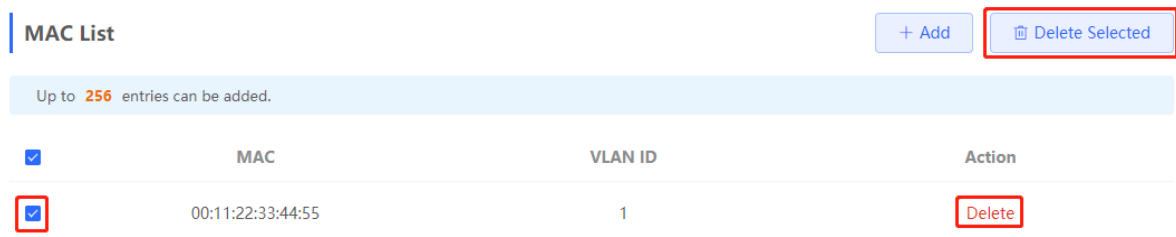


2. MAC Filter

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

Batch delete: In **MAC List** , select the MAC address entries to be deleted and click **Delete Selected** . In the displayed dialog box, click **OK** .

Delete an entry: In **MAC List** , find the entry to be deleted, click **Delete** in the last **Action** column. In the displayed dialog box, click **OK** .



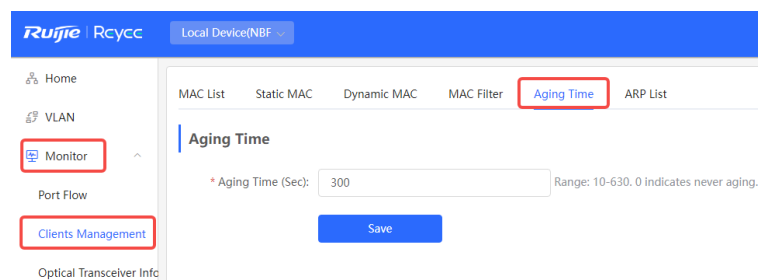
4.3.6 Configuring MAC Address Aging Time

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

The device deletes useless dynamic MAC address entries based on the aging time to save entry resources on the device. An overly long aging time may lead to untimely deletion of useless entries, whereas an overly short aging time may lead to deletion of some valid entries and repeated learning of MAC addresses by the device, which increases the packet broadcast frequency. Therefore, you are advised to configure a proper aging time of dynamic MAC address entries as required to save device resources without affecting network stability.

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

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



4.4 Displaying ARP Information

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

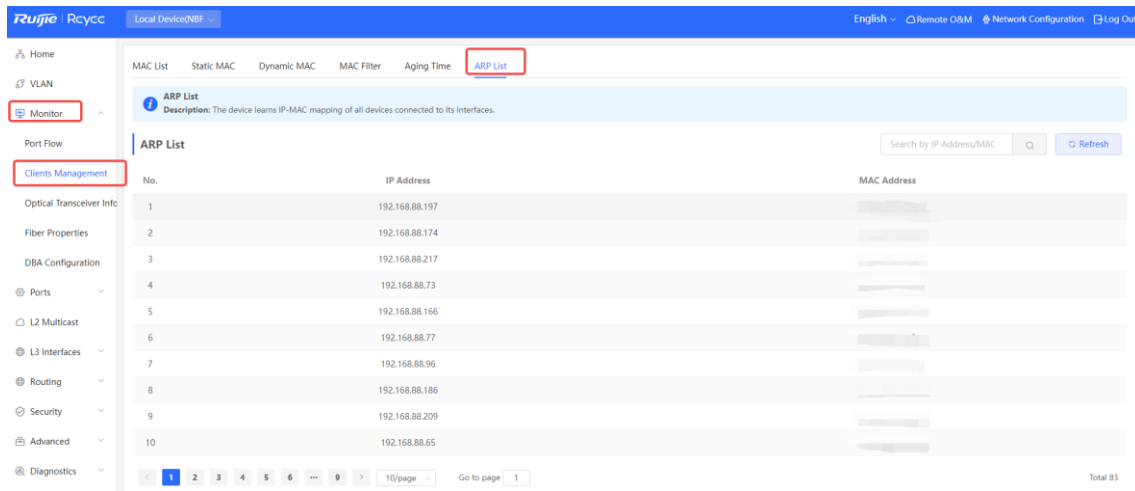
When two IP-based devices need to communicate with each other, the sender must know the IP address and MAC address of the peer. With MAC addresses, an IP-based device can encapsulate link-layer frames and then send data frames to the physical network. The process of obtaining MAC addresses based on IP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

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

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

Note

For more ARP entry function introduction, see [7.6](#).



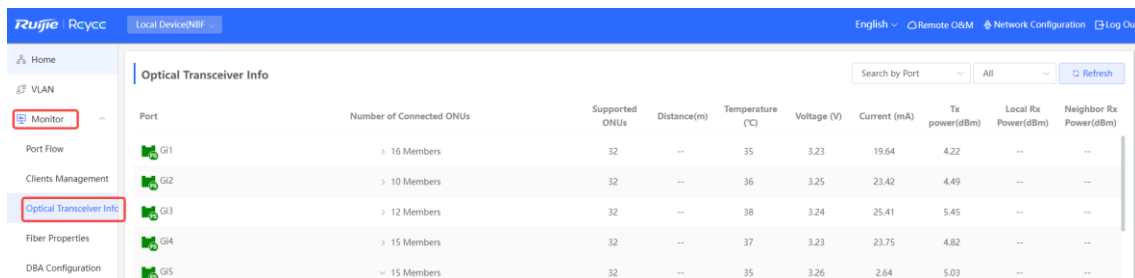
4.5 View optical module information

[Local Management-Page Wizard] Monitoring Information >> Optical module information

Displays the basic information of the optical module, including the port, whether it supports DDM , temperature, voltage, current, transmit optical power, local receive optical power, etc.

Supports querying optical module information by port.

The optical module information automatically updates the data every 5 seconds. You can also click <Refresh> to refresh the optical module information.



4.6 Fiber Properties

[Local Management-Page Wizard] Monitoring Information >> Fiber Properties

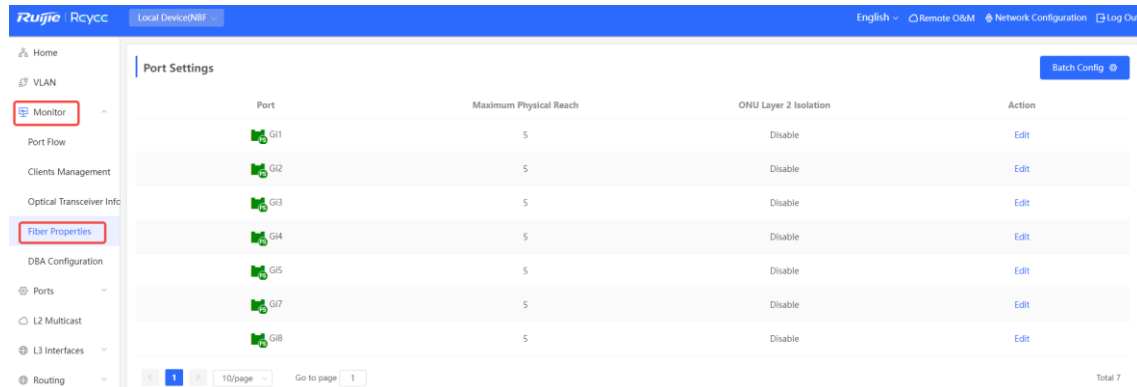
Configuring ONU Layer 2 forwarding isolation and ONU registration's maximum distance. This can only be done on connected ONU ports.

Enabling ONU Layer 2 forwarding isolation isolates communication between different ONU devices, enhancing network security and preventing unnecessary data exchange.

The default maximum ONU registration distance is 5km, but it should be adjusted based on the actual farthest ONU distance from the OLT. If the farthest ONU is 7km away, it should be set to 7km.

Setting the maximum distance accounts for the light transmission time in fibers. Large distance differences between ONUs under the same splitter port can lead to packet loss due to signal collisions. To prevent this, a discovery window time is set to compensate for the time difference between ONUs.

For example, an ONU 1m from the OLT has almost zero round-trip time, while another 20km away has a round-trip time of approximately 66.7us. If the OLT doesn't consider this delay when controlling ONU transmissions, collisions may occur, wasting bandwidth.



4.7 DBA

4.7.1 Overview

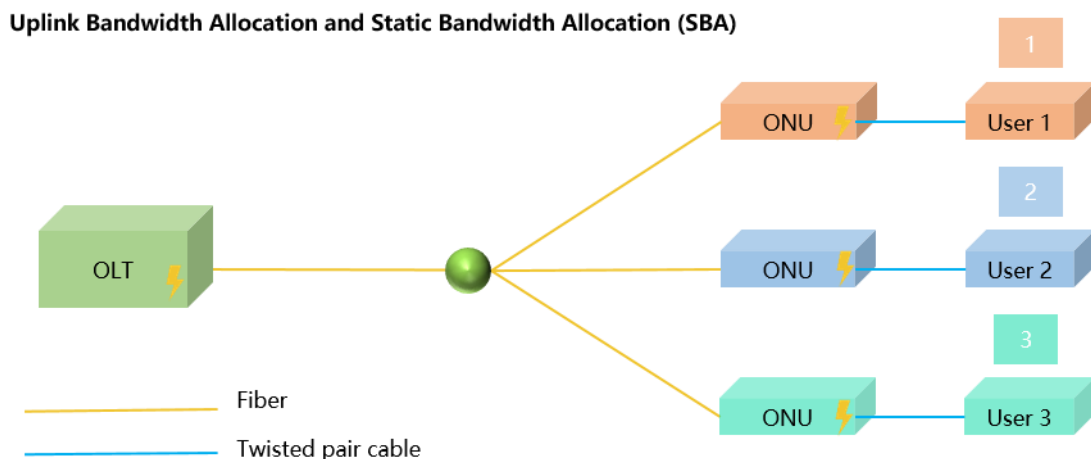
Through the DBA (Dynamic Bandwidth Assignment) function, OLT can dynamically adjust the upstream bandwidth of each ONU according to the real-time traffic conditions of each ONU, thus improving the bandwidth utilization of the PON (Passive Optical Network) system.

4.7.2 Bandwidth Allocation Mechanism

Bandwidth allocation is used to distribute network traffic to ensure the normal transmission of real-time traffic with limited bandwidth. The bandwidth allocation mechanism includes two modes: static mode and dynamic mode. By default, the static mode is used.

1. Static Mode

In the static mode, each ONU occupies an equal number of time slots for equal bandwidth allocation.



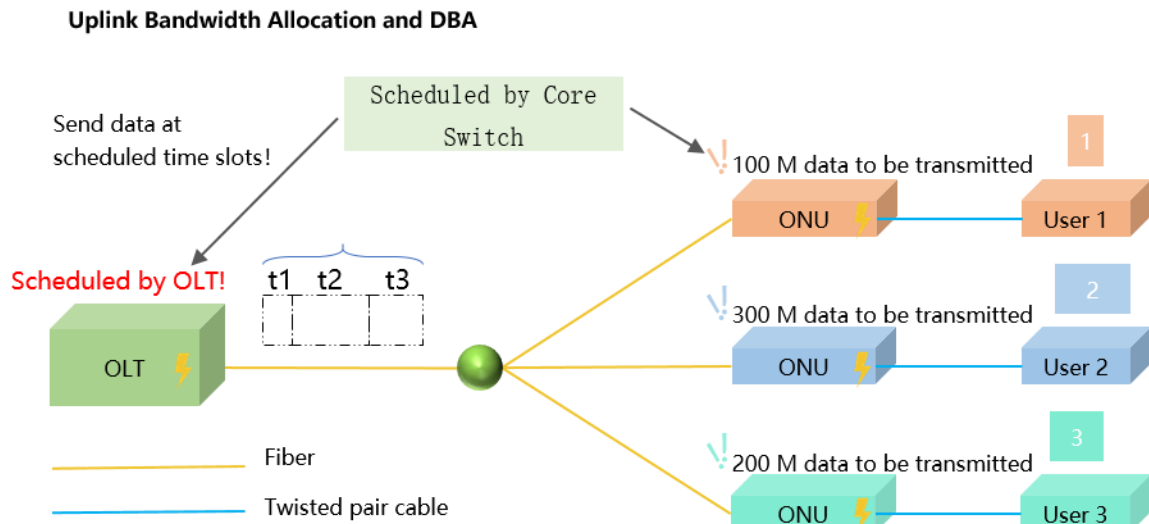
Calculation of static bandwidth allocation (SBA): Client (PC/Smartphone/Tablet) rate = PON port rate/number of split outputs

Example 1: If one FS interface is connected to 1:16 optical splitter at the downlink, and each splitter output port is connected to an ONU, then the client rate = 1000 Mbps/16 = 62.5 Mbps.

Example 2: If one FS interface is connected to 1:16 optical splitter at the downlink, and only eight output ports are connected to ONUs, then the client rate = 1000 Mbps/8=125 Mbps.

2. Dynamic Mode

In the dynamic mode, each ONU occupies an unequal number of time slots, resulting in different bandwidth allocation for each ONU.

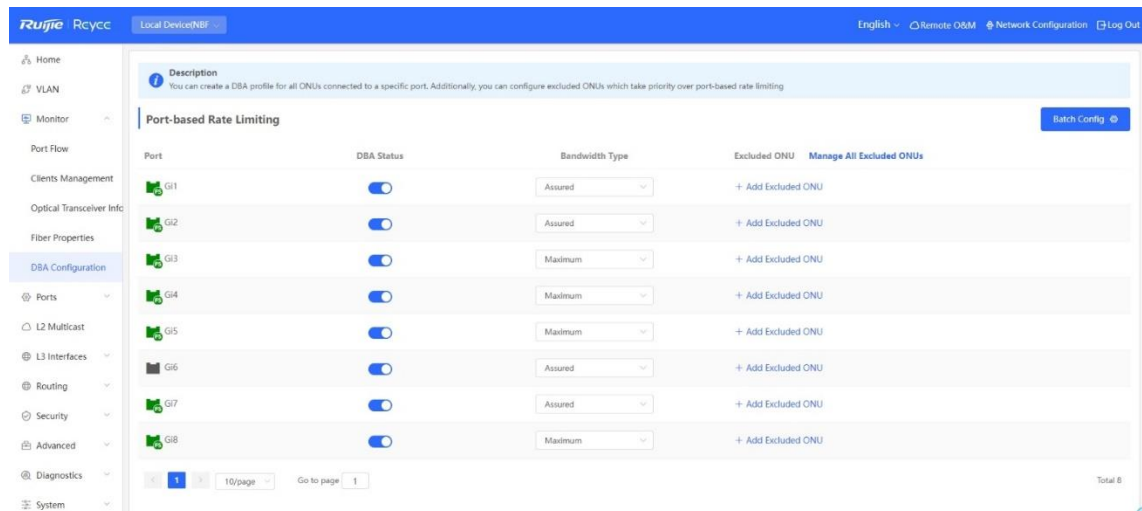


DBA Calculation:

Each ONU is assigned a default assured bandwidth (you can also set a larger assured bandwidth for a specific ONU to ensure it has a larger basic time slot). This corresponds to the initial time slot. The idle bandwidth outside the assured bandwidth is subject to dynamic allocation to handle burst traffic. If no ONU reports burst traffic, the transmission will be scheduled based on this assured bandwidth.

4.7.3 Configuring DBA

[Local Management-Page Wizard] Monitoring Information >> DBA



Parameter	Description
Port	Splitter ports on OLT devices
DBA Status	DBA switch of specified splitter ports on OLT devices
Bandwidth Type	DBA mode of specified splitter ports on OLT devices
Excluded ONU	Exception ONUs connected to the specified splitter ports on OLT devices, which are not subject to the DBA function of the splitter ports. ONU devices can be identified through the SN of the devices. After adding exception ONUs, the guaranteed bandwidth value of the devices can be specified.
Manage ALL Excluded ONUs	All exception ONU devices can be managed in batches.
Batch Config	DBA function can be enabled and DBA working mode can be adjusted in batches, etc.

4.8 VLAN

4.8.1 VLAN Overview

A virtual local area network (VLAN) is a logical network created on a physical network. A VLAN has the same properties as a normal physical network except that it is not limited by its physical location. Each VLAN has an independent broadcast domain. Different VLANs are L2-isolated. L2 unicast, broadcast, and multicast frames are forwarded and spread within one VLAN and will not be transmitted to other VLANs.

When a port is defined as a member of a VLAN, all clients connected to the port are a part of the VLAN. A network supports multiple VLANs. VLANs can make L3 communication with each other through L3 devices or L3 interfaces.

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

4.8.2 Creating a VLAN

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

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

VLAN List + Batch Add + Add Delete Selected

Up to **4094** entries can be added.(The default VLAN, management VLAN, Native VLAN, SVI VLAN, MVR VLAN, Voice VLAN and Access VLAN cannot be deleted.)

<input type="checkbox"/>	VLAN ID	Description	Port	Action
<input type="checkbox"/>	1	VLAN0001	Gi1-28	Edit Delete
<input type="checkbox"/>	10	VLAN0010	--	Edit Delete
<input type="checkbox"/>	20	VLAN0020	--	Edit Delete

Total 3 < 1 > Go to page

1. Adding a VLAN

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

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

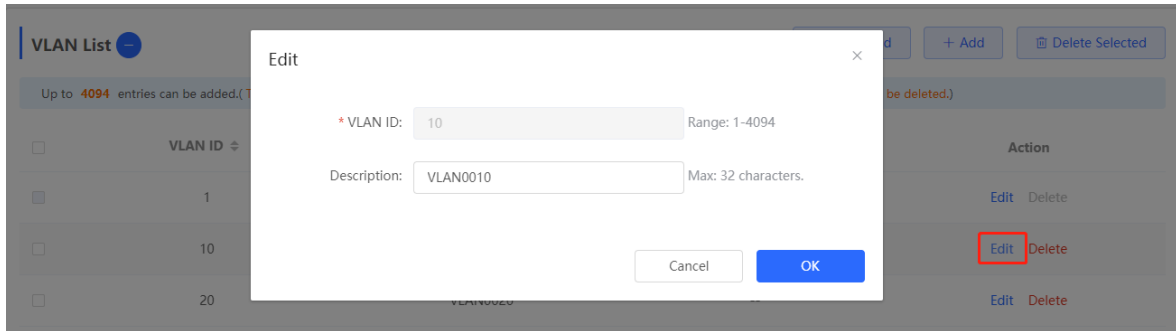
Note

- The range of a VLAN ID is from 1 to 4094.
- You can separate multiple VLANs to be added in batches with commas (,), and separate the start and end VLAN IDs of a VLAN range with a hyphen (-).

- If no VLAN description is configured when the VLAN is added, the system automatically creates a VLAN description in the specified format, for example, VLAN000XX. The VLAN descriptions of different VLANs must be unique.
- If the device supports L3 functions, VLANs, routed ports, and L3 aggregate ports (L3APs) share limited hardware resources. If resources are insufficient, a message indicating resource insufficiency for VLAN will be displayed.

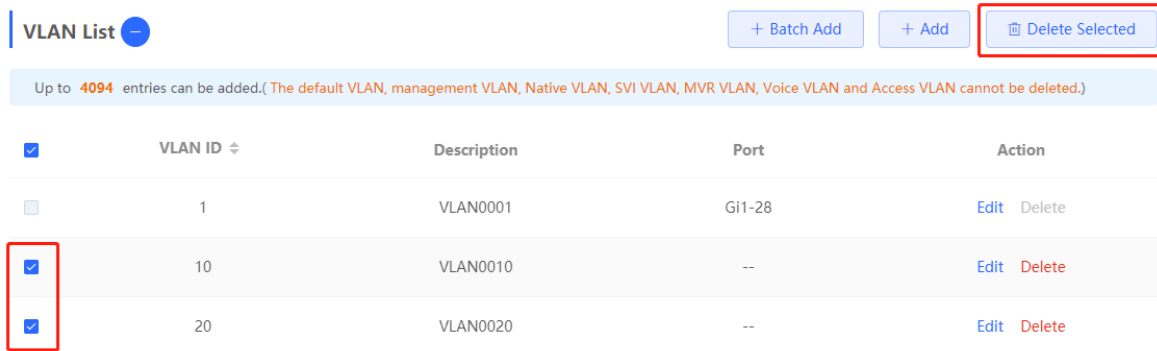
2. VLAN Description Modifying

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



3. Deleting a VLAN

Batch delete VLANs: In **VLAN List** , select the VLAN entries to be deleted and click **Delete Selected** to delete VLANs in a batch.



Delete a VLAN: In **VLAN List** , click **Delete** in the last **Action** column to delete the specified **VLAN** .



Note

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

4.8.3 Configuring Port VLAN

1. Overview

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

Port List displays the VLAN division of the current port. Create VLANs in **VLAN List** page (see [3.5.2 Creating a VLAN](#)) and then configure the port based on the VLANs.

Port List -
Batch Edit

The Permit VLAN of a hybrid port includes both the tagged VLAN and untagged VLAN.
If the Voice VLAN automatic mode is enabled on the port, the Voice VLAN will be removed from the Permit VLAN.

Port	Port Mode	Access VLAN	Native VLAN	Permit VLAN	Untag VLAN	Action
Gi1 +	ACCESS	1	--	--	--	Edit
Gi2	ACCESS	1	--	--	--	Edit
Gi3	ACCESS	1	--	--	--	Edit
Gi4	ACCESS	1	--	--	--	Edit
Gi5	ACCESS	1	--	--	--	Edit

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

Table 4-1 Port Modes Description

Port mode	Function
Access port	<p>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.</p> <p>Access VLAN has attributes of both Native VLAN and Permitted VLAN</p> <p>The frames sent from the Access port do not carry tags. When the access port receives an untagged frame from a peer device, the local device determines that the frame comes from the Access VLAN and adds the access VLAN ID to the frame.</p>
Trunk port	<p>One trunk port supports one native VLAN and several allowed VLANs. Native VLAN frames forwarded by a trunk port do not carry tags while allowed VLAN frames forwarded by the trunk port carry tags.</p> <p>A trunk port belongs to all VLANs of the device by default, and can forward frames of all VLANs. You can set the allowed VLAN range to limit VLAN frames that can be forwarded.</p>

Port mode	Function
	Note that the trunk ports on both ends of the link must be configured with the same Native VLAN.
Hybrid port	A hybrid port supports one native VLAN and several allowed VLANs. The allowed VLANs are divided into Tag VLAN and Untag VLAN. The frames forwarded by the hybrid port from a Tag VLAN carry tags, and the frames forwarded by the hybrid port from an Untag VLAN do not carry tags. The frames forwarded by the hybrid port from Native VLAN must not carry tags, therefore Native VLAN can only belong to Untag VLAN List.

Note

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

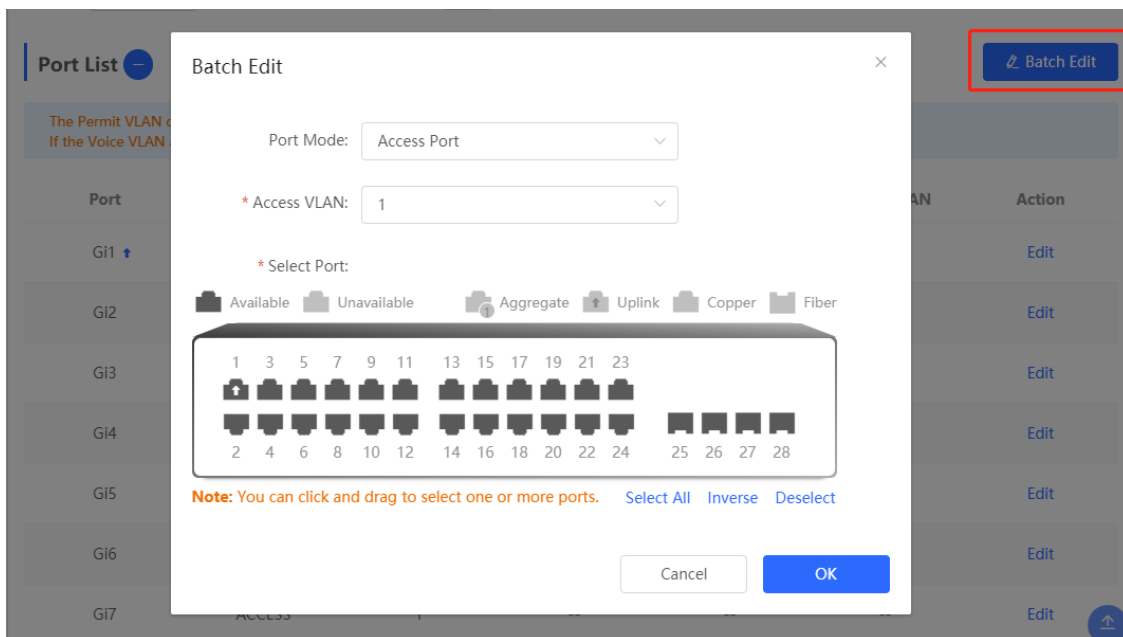
2. Procedure

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

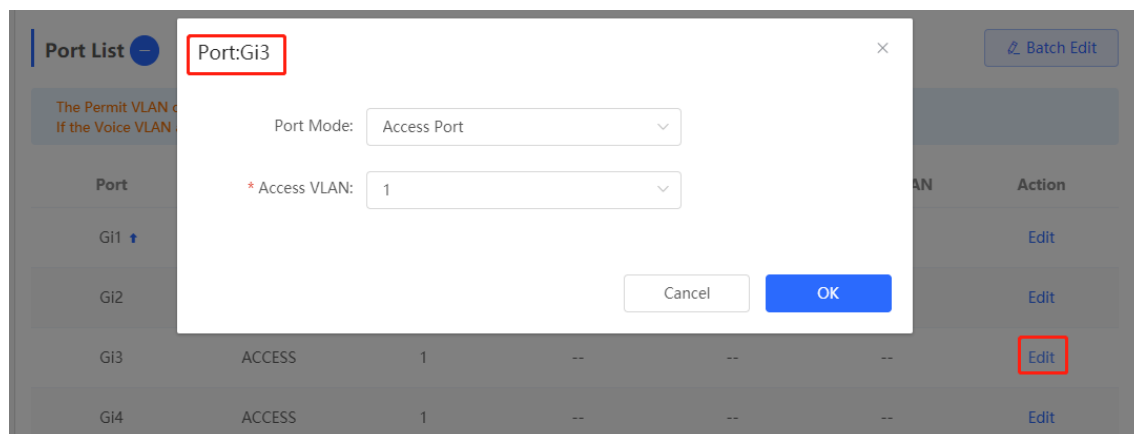
Configure port VLANs in a batch: Click **Batch Edit** , select the port to be configured on the port panel, and select the port mode. If the port mode is Access port, you need to select Access VLAN; if the port mode is Trunk port , you need to select Native VLAN and enter the allowed VLAN ID range; if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

Note

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



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



i Note

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

4.8.4 Batch Switch Configuration

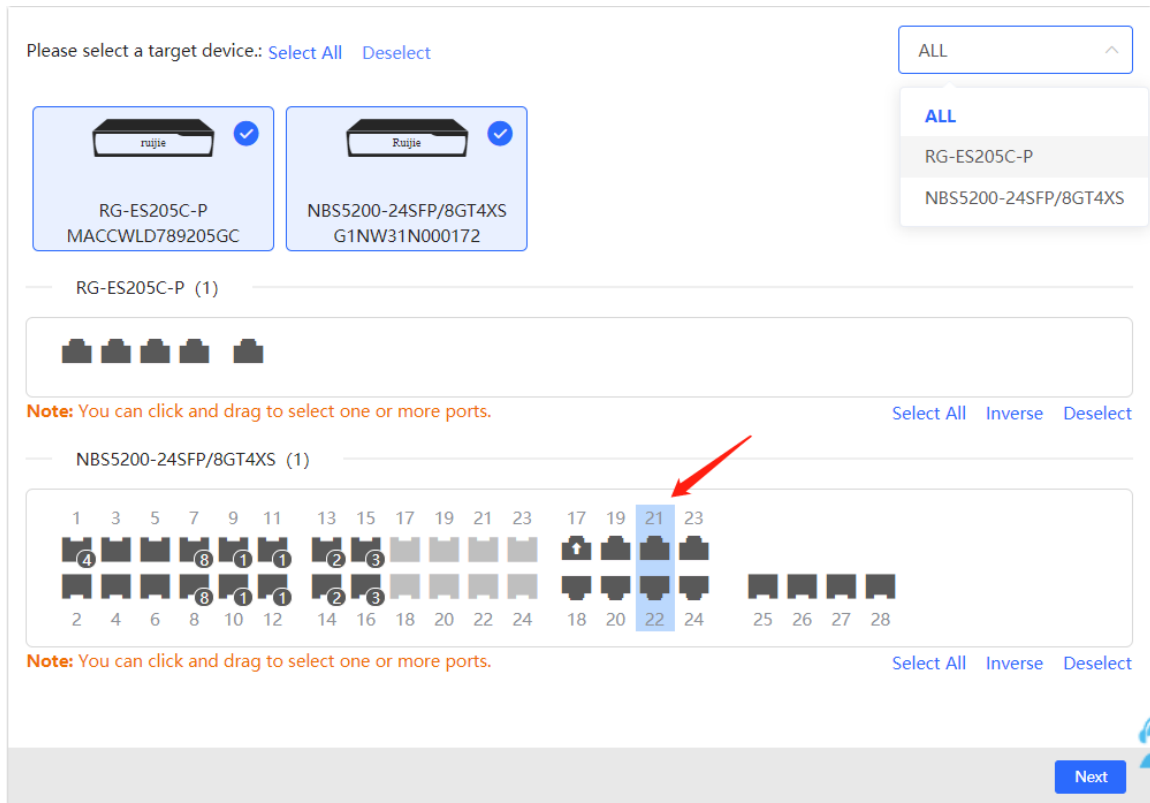
1. Overview

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

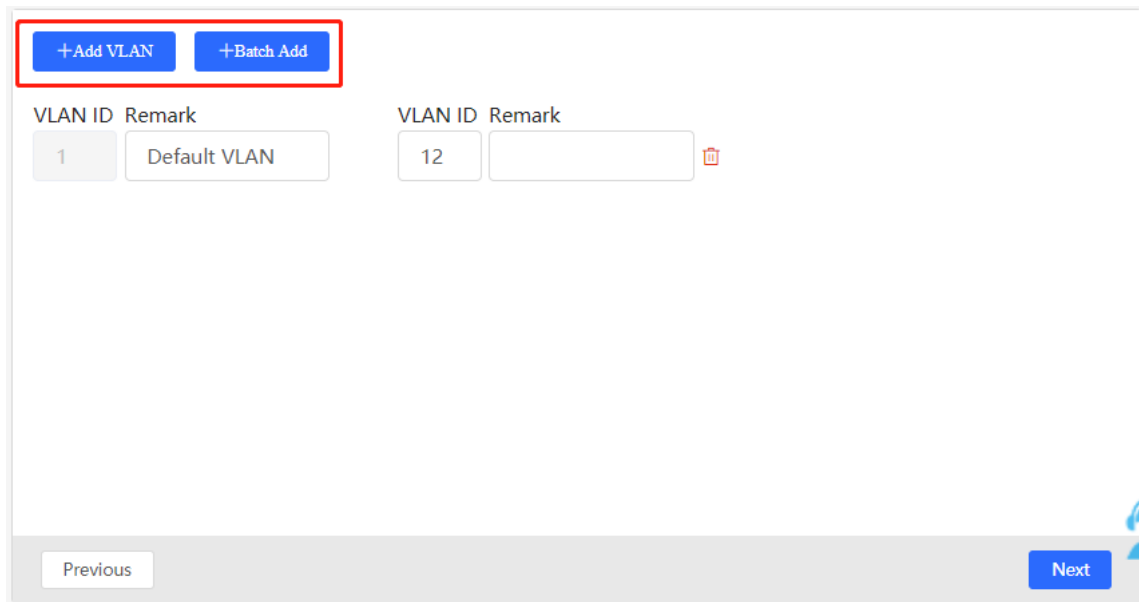
2. Procedure

Choose **Network > Batch Config** .

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



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



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

Port

Selected Port RG-ES205C-P-; NBS5200-24SFP/8GT4XS: Gi21-Gi22;

Type

* Native VLAN

Permitted VLAN

4.8.5 Verifying Configuration

View the VLAN and port information of switches to check whether the batch configurations are successfully delivered.

MSW

Hostname: [Ruijie](#) Software Ver:ReyeeOS 1.86.1619
Model:NBS5200-24SFP/8GT4XS MGMT IP:10.44.78.1
SN:G1NW31N000172 MAC: 00:d3:f8:15:08:5b

Port Status

VLAN Info

Port

Route Info

RLDP

More

VLAN [Edit](#)

VLAN1 **VLAN12**

Interface	IP	IP Range	Remark
Gi17,Gi21-22,Te27			

Port [Edit](#)

5 Port Management

5.1 Overview

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

Table 5-1 Description of Port Type

Port Type	Note	Remarks
Switch Port	A switch port consists of a single physical port on the device and provides only the L2 switching function. Switch ports are used to manage physical port and their associated L2 protocols.	Described in this section
L2 aggregate port	An Interface binds multiple physical members to form a logical link. For L2 switching, an aggregate port is like a high-bandwidth switch port. It can combine the bandwidths of multiple ports to expand link bandwidth. In addition, for frames sent through an L2 aggregate port, load balancing is performed on member ports of the L2 aggregate port. If one member link of the aggregate port fails, the L2 aggregate port automatically transfers traffic on this link to other available member links, improving connection reliability.	Described in this section
SVI Port	A switch virtual interface (SVI) serves as the management interface of the device, through which the device can be managed. You can also create an SVI as a gateway interface, which is equivalent to the virtual interface of corresponding VLAN and can be used for inter-VLAN routing on L3 devices.	For related configuration, see 6.1
Routed Port	On L3 devices, you can configure a single physical port as a routed port and use it as the gateway interface of L3 switching. Route interfaces do not have L2 switching functions and have no corresponding relationship with VLANs, but only serve as access interfaces.	For related configuration, see 6.1

Port Type	Note	Remarks
L3 Aggregate Port	<p>An L3 aggregate port is a logical aggregate port group composed of multiple physical member ports, just like an L2 aggregate port. The ports to be aggregated must be L3 ports of the same type. An aggregate port serves as the gateway interface of L3 switching. It treats multiple physical links in the same aggregate group as one logical link. It is an important way to expand link bandwidth. Multiple physical links are combined into one logical link, expanding the bandwidth of a link. Frames sent over the L3 AP are balanced among the L3 AP member ports. If one member link fails, the L3 AP automatically transfers the traffic on the faulty link to other member links, improving reliability of connections.</p> <p>L3 aggregate ports do not support the L2 switching function.</p>	For related configuration, see 6.1

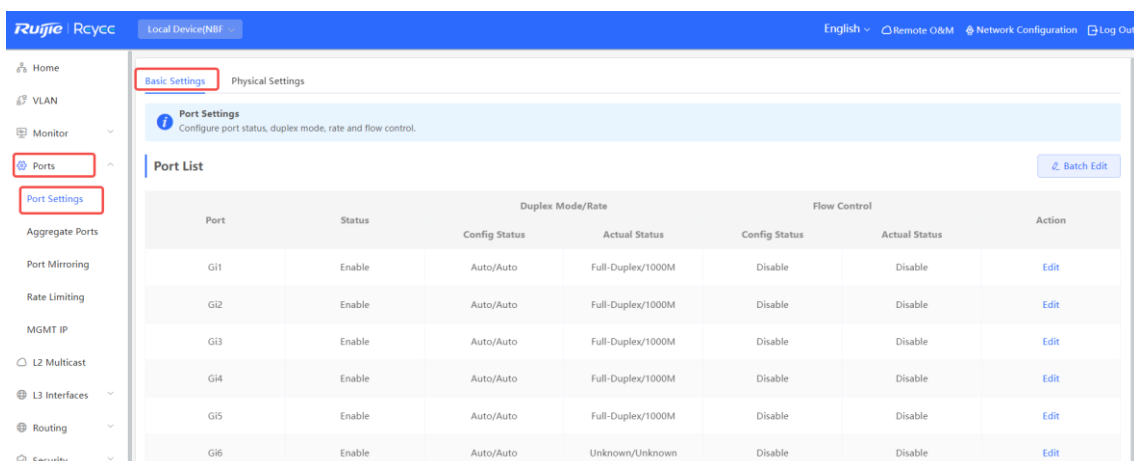
5.2 Port Configuration

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

5.2.1 Basic Settings

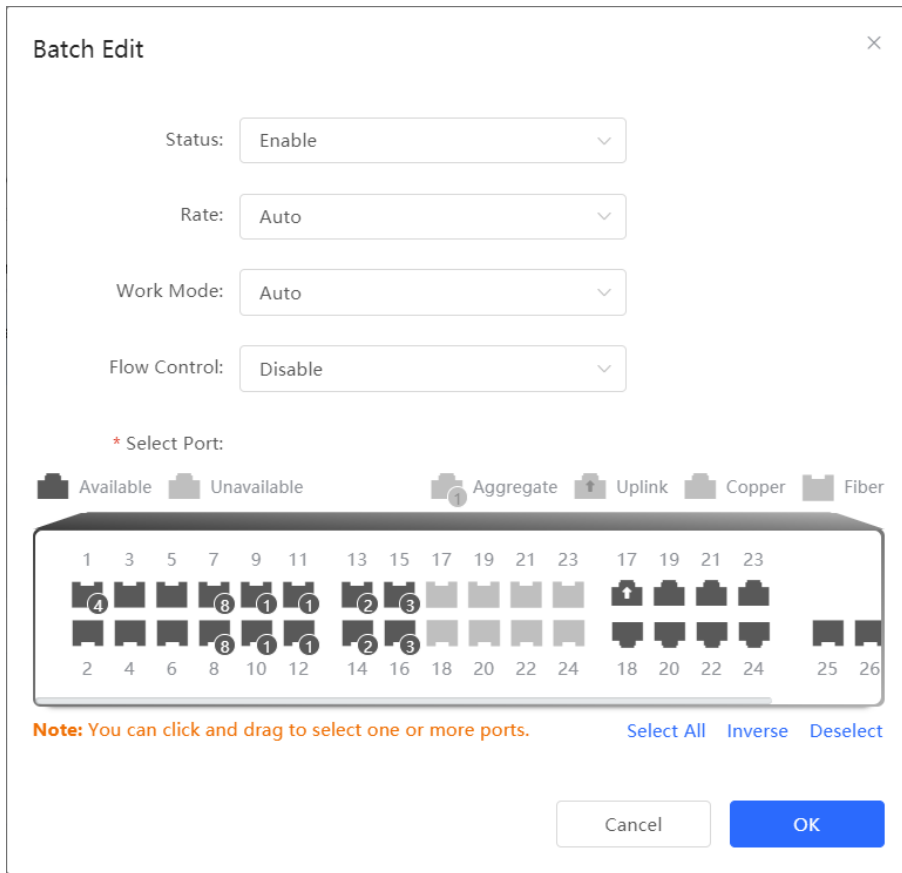
Choose **Local Device > Ports > Ports Settings > Basic Settings** .

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



Batch configure: Click **Batch Edit** , select the port to be configured In the displayed dialog box, select the port switch, rate, work mode, and flow control mode, and click **OK** to deliver the configuration. In batch configuration,

optional configuration items are a common collection of selected ports (that is, attributes supported the selected ports).



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

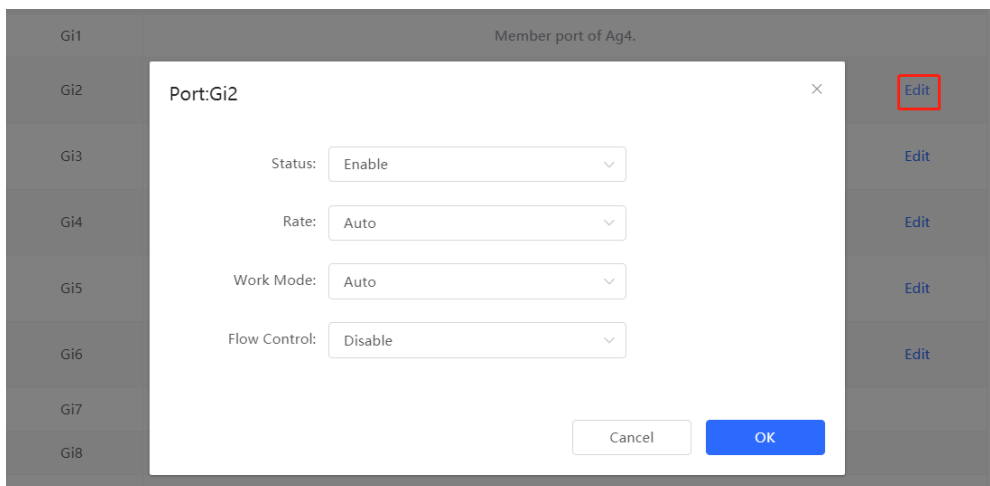


Table 5-2 Description of Basic Port Configuration Parameters

Parameter	Description	Default Value
Status	If a port is closed, no frame will be received and sent on this port, and the corresponding data processing function will be lost.	Enable
Rate	Set the rate at which the Ethernet physical interface works. Set to Auto means that the port rate is determined by the auto-negotiation between the local and peer devices. The negotiated rate can be any rate within the port capability.	Auto
Work Mode	<ul style="list-style-type: none"> ● Full duplex: realize that the port can receive packets while sending. ● Half duplex: control that the port can receive or send packets at a time. ● Auto: the duplex mode of the port is determined through auto negotiation between the local port and peer port 	Auto
Flow Control	After flow control is enabled, the port will process the received flow control frames, and send the flow control frames when congestion occurs on the port.	Disable

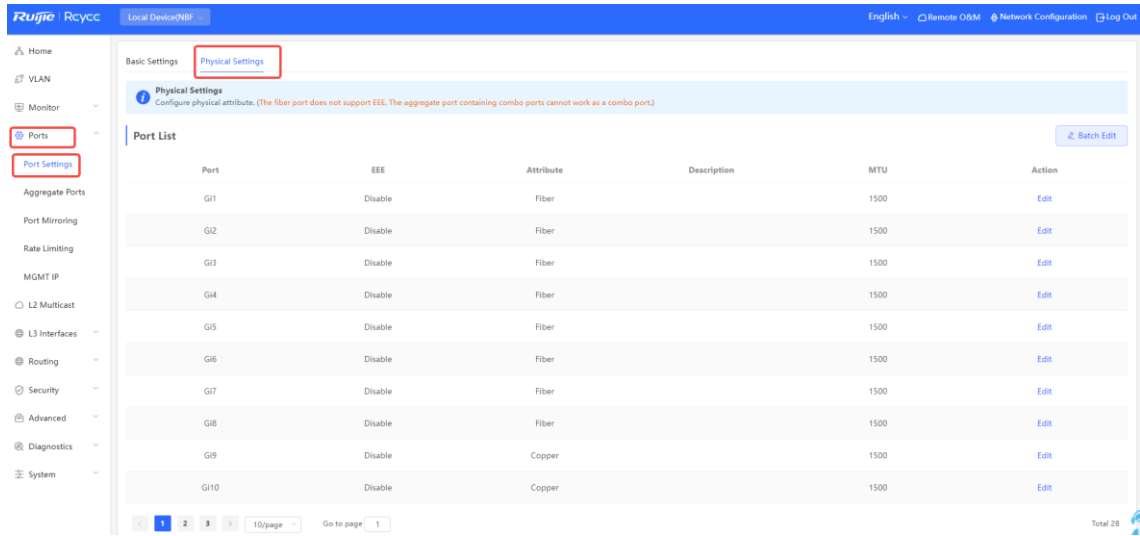
 **Note**

The rate of a GE port can be set to 1000M, 100M, or auto. The rate of a 10G port can be set to 10G, 1000M, or auto.

5.2.2 Physical Settings

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

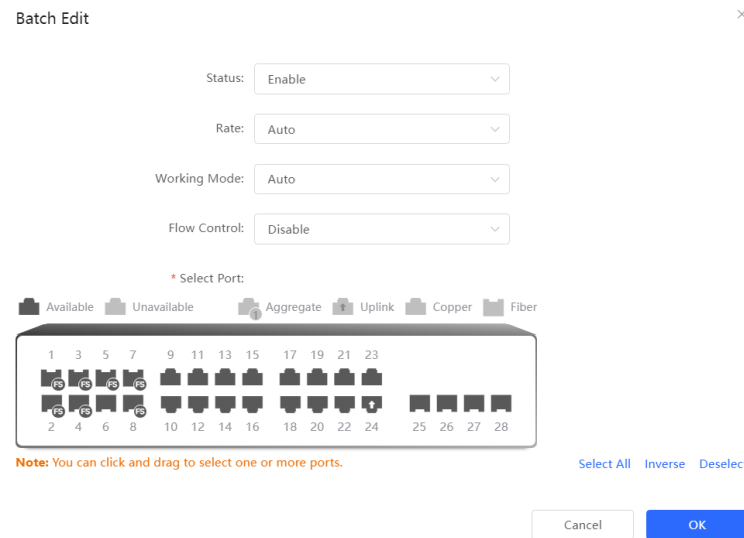
Support to enable the energy-efficient Ethernet (EEE) function of the port, and set the media type and MTU of the port.



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

Note

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



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

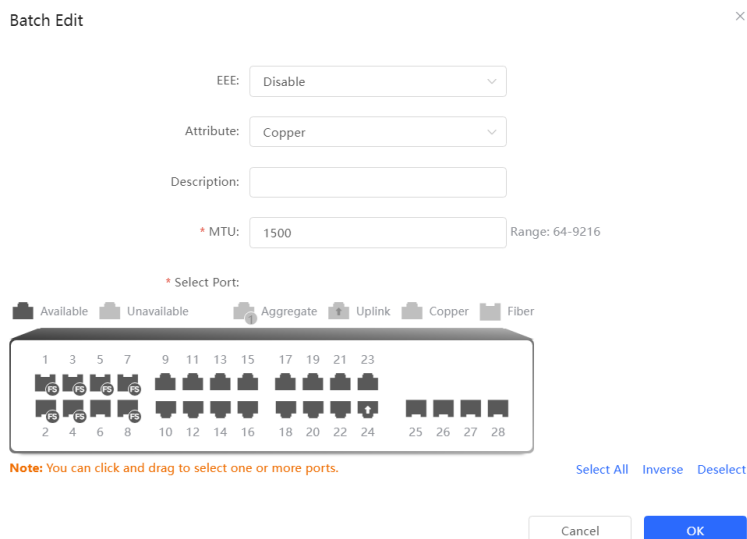


Table 5-3 Description of Physical Configuration Parameters

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

Note

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

5.3 Aggregate Ports

5.3.1 Aggregate Port Overview

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

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

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

5.3.2 Overview

1. Static AP Address

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

2. Dynamic Aggregation

Dynamic aggregation mode is a special port aggregation function developed for the WAN port of RG-MR series gateway devices. The maximum bandwidth of the WAN port of the MR device can support 2000M, but after the intranet port is connected to the switch, a single port can only support a maximum bandwidth of 1000M. In order to prevent the downlink bandwidth from being wasted, it is necessary to find a way to increase the maximum bandwidth of the port between the MR device and the switch, and the dynamic aggregation function emerged to meet the need.

After connecting the two fixed AG (aggregation) member ports on the MR gateway device to any two ports on the switch, through packet exchange, the two ports on the switch can be automatically aggregated, thereby doubling the bandwidth. The aggregate port automatically generated in This way on the switch is called a dynamic aggregate port, and the corresponding two ports are the member ports of the aggregate port.

Note

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

3. Load Balancing

An AP, based on packet characteristics such as the source MAC address, destination MAC address, source IP address, destination IP address, L4 source port ID, and L4 destination port ID of packets received by an inbound interface, differentiates packet flows according to one or several combined algorithms. It sends the same packet flow through the same member link, and evenly distributes different packet flows among member links. For example, in load balancing mode based on source MAC addresses, packets are distributed to different member links of an AP based on their source MAC addresses. Packets with different source MAC addresses are distributed to different member links; packets with a same source MAC address are forwarded along a same member link.

Currently, the AP supports the traffic balancing modes based on the following:

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

5.3.3 Aggregate Port Configuration

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

1. Adding an Aggregate Port

2. Enter an aggregate port ID, select member ports (note that ports that are already members of an aggregate port cannot be selected), and then click **Save**. The port panel will display the successfully added aggregate port.

Note

- An aggregate port contains a maximum of eight member ports.
 - The attributes of aggregate ports must be the same, and copper ports and SFP ports cannot be aggregated.
 - Dynamic aggregate ports do not support manual creation.
-

Aggregate Port Settings

Up to 16 aggregate ports can be added. An aggregate port contains up to 8 member ports.

No Data

* Aggregate Port: 1

LACP

* Select Member Ports

Available Unavailable Aggregate Uplink Copper Fiber

Note: You can click and drag to select one or more ports. [Select All](#) [Inverse](#) [Deselect](#)

Save

3. Modifying Member Ports of a Static Aggregate Port

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

Note

Dynamic aggregation ports do not support to modify member ports.

Aggregate Port Settings

Up to 16 aggregate ports can be added. An aggregate port contains up to 8 member ports.

Select All

Ag1

Delete Selected

* Aggregate Port: 1

LACP

* Select Member Ports

Available Unavailable Aggregate Uplink Copper Fiber

Note: You can click and drag to select one or more ports. [Select All](#) [Inverse](#) [Deselect](#)

Save Cancel

4. Deleting an Aggregate Port

Move the cursor over an aggregate port icon and click upper-right, or select the aggregate port to be deleted, and click **Delete Selected** to delete the selected aggregate port. After deleted, the corresponding ports become **available** on the port panel to set a new aggregate port.

Caution

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

Aggregate Port Settings

Up to **16** aggregate ports can be added. An aggregate port contains up to **8** member ports.

Select All



5.3.4 Configuring a Load Balancing Mode

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

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

Global Settings

Load Balance

Algorithm:

Save

5.4 Port Mirroring

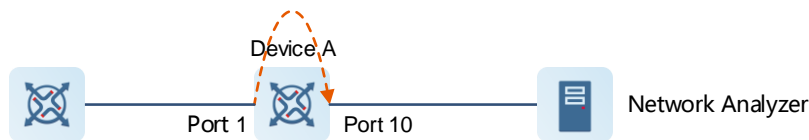
5.4.1 Overview

The switched port analyzer (SPAN) function is a function that copies packets of a specified port to another port that is connected to a network monitoring device, After port mirroring is set, the packets on the source port will be copied and forwarded to the destination port, and a packet analyzer is usually connected to the destination

port to analyze the packet status of the source port, so as to monitor all incoming and outgoing packets on source ports.

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

Figure 5-1 Port Mirroring Principles Figure



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

5.4.2 Procedure

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

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

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

⚠ Caution

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

Port Mirroring

Description: All packets on the source port will be copied to the destination port and you can analyze the traffic by using a protocol analyzer application. Traffic on more than one source port can be mirrored to one destination port.

Note: The destination port must be different from the source port.

Port Mirroring List

#	Src Port	Dest Port	Monitor Direction	Receive Pkt from Non-Src Ports	Action
1	--	--	--	--	Edit Delete
2	--	--	--	--	Edit Delete
3	--	--	--	--	Edit Delete
4	--	--	--	--	Edit Delete

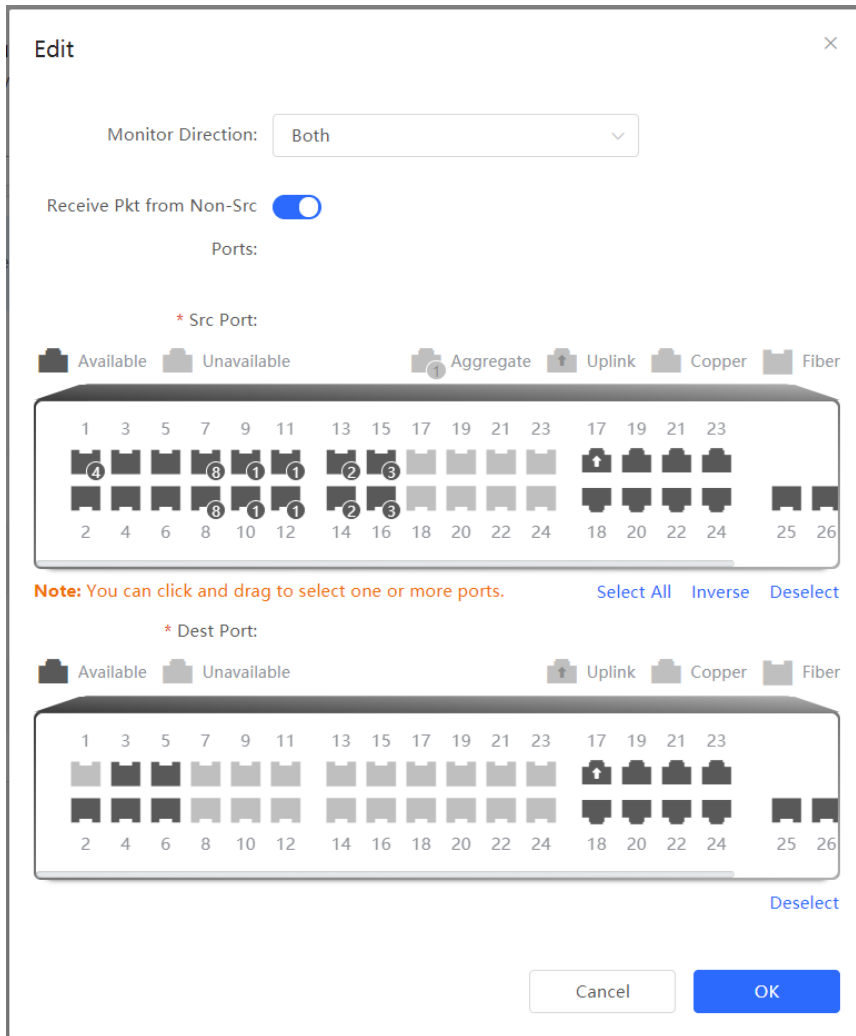


Table 5-4 Description of Port Mirroring Parameters

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

Parameter	Description	Default Value
Monitor Direction	<p>The type of packets (data flow direction) to be monitored by a source port.</p> <ul style="list-style-type: none"> ● Both: All packets passing through the port, including incoming and outgoing packets ● Incoming: All packets received by a source port are copied to the destination port ● Outcoming : All packets transmitted by a source port are copied to the destination port 	Both
Receive Pkt from Non- Src Ports	<p>It is applied to the destination port and indicates whether a destination port forwards other packets while monitoring packets.</p> <ul style="list-style-type: none"> ● Enabled: While monitoring the packets of the source port, the packets of other non-Src ports are normally forwarded ● Disabled: Only monitor source port packets 	Enable

5.5 Rate Limiting

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

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

Port List

🔗 Batch Edit
🗑 Delete Selected

	Port	Rx Rate (kbps)	Tx Rate (kbps)	Action
<input type="checkbox"/>	Gi23	10000	10000	Edit Delete

Total 1

<
1
>

Go to page

1. Rate Limiting Configuration

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

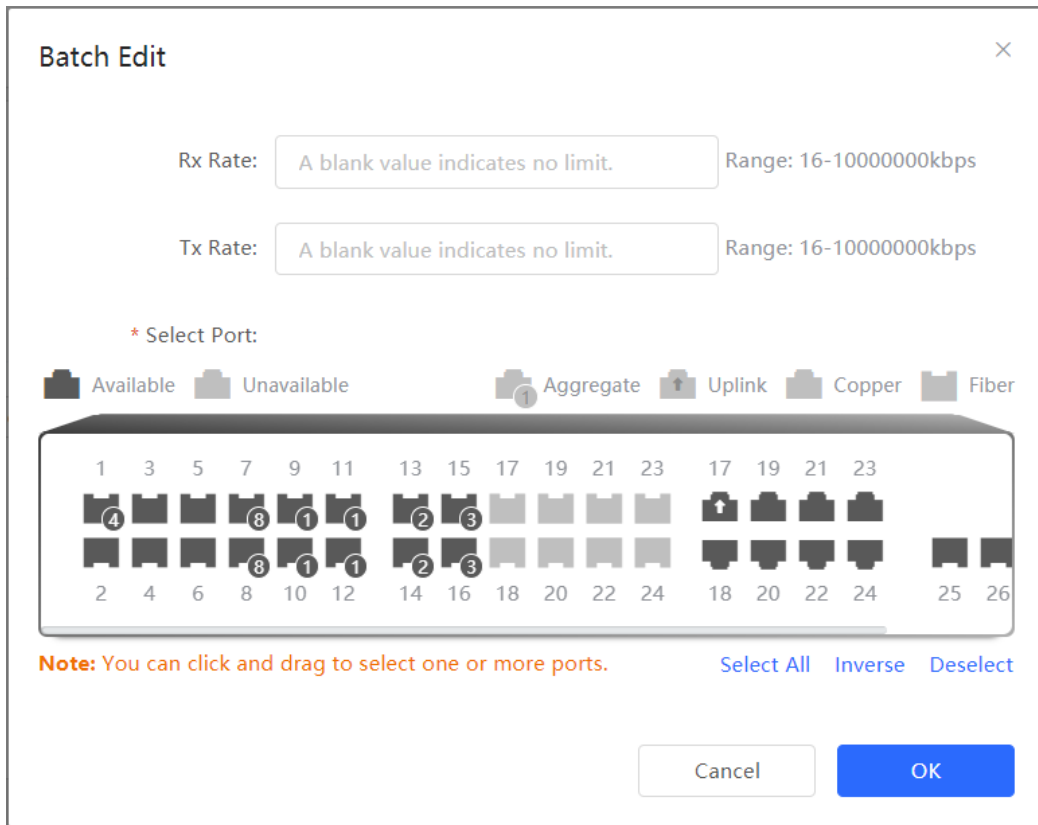


Table 5-5 Description of Rate Limiting Parameters

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

2. Changing Rate Limits of a Single Port

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

Port:Gi23 ×

Rx Rate: Range: 16-1000000kbps

Tx Rate: Range: 16-1000000kbps

3. Deleting Rate Limiting

Batch configure: Select multiple records in **Port List** , click **Delete Selected** and click **OK** in the confirmation dialog box .

Configure one port: In **Port List** , click **Delete** on the corresponding port entry, and click **OK** in the confirmation dialog box.

Port List					Batch Edit	Delete Selected
<input checked="" type="checkbox"/>	Port	Rx Rate (kbps)	Tx Rate (kbps)	Action		
<input checked="" type="checkbox"/>	Gi23	10000	10000	Edit Delete		

Note

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

5.6 MGMT IP Configuration

5.6.1 Set IPv4 management address

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

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

The screenshot shows the Ruijie Rcycc web interface for configuring the Management IP (MGMT IP) settings. The interface is in Chinese. The left sidebar contains navigation options: Home, VLAN, Monitor, Ports, Port Settings, Aggregate Ports, Port Mirroring, Rate Limiting, MGMT IP (selected), L2 Multicast, L3 Interfaces, and Routing. The main content area is titled 'MGMT IP' and 'MGMT IPv6'. Under 'MGMT IP', there is a sub-section 'MGMT IP' with the instruction 'Configure network settings.' The configuration fields are as follows:

- Internet: Static IP (selected in a dropdown menu)
- VLAN: 888
- * IP Address: 192.168.88.53
- * Subnet Mask: 255.255.248.0
- * Gateway: 192.168.88.1
- * DNS Server: 192.168.88.1
- DHCP Server:

A blue 'Save' button is located at the bottom right of the configuration area.

The device can be networked in two modes:

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

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

Note

- If the management VLAN is null or not specified, VLAN 1 takes effect by default.
- The management VLAN must be selected from existing VLANs. If no VLAN is created, go to the VLAN list to add a VLAN (for details, see [4.8.2](#)).
- You are advised to bind a configured management VLAN to an uplink port. Otherwise, you may fail to access the Eweb management system.

5.6.2 Configuring the Management IPv6 Address

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

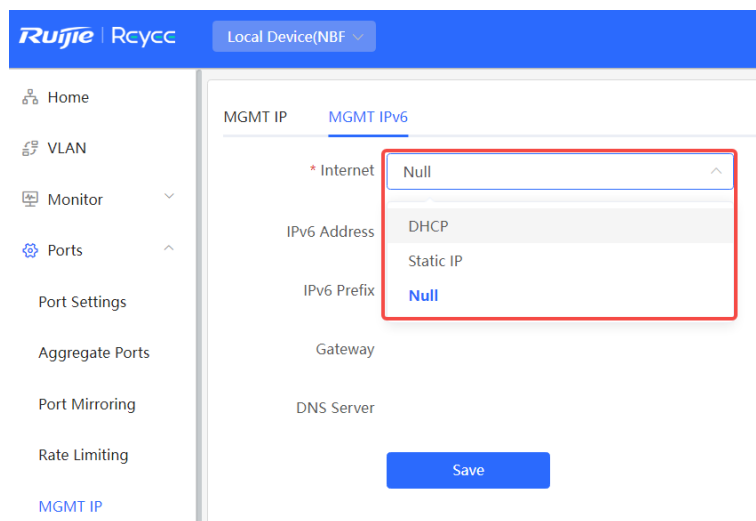
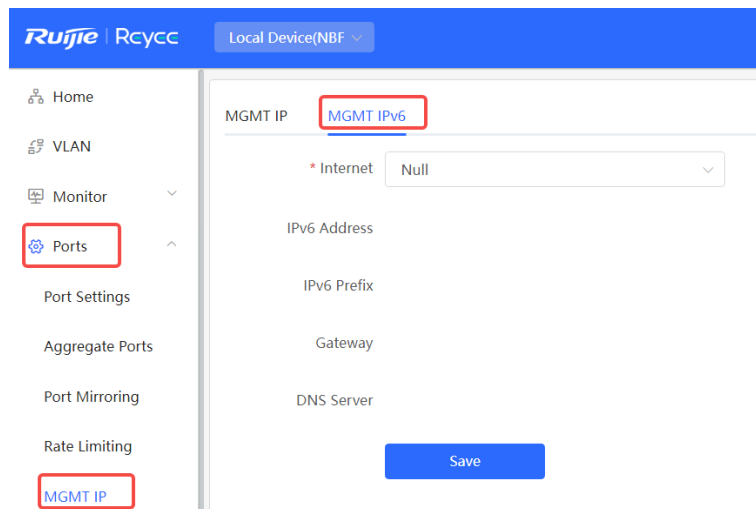
Choose **Local Device** > **Ports** > **MGMT IPv6** .

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

The device supports the following Internet connection types:

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

Click **Save** .



6 L2 Multicast

6.1 Multicast Overview


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

6.2 Multicast Global Settings

Choose **Local Device > Multicast > Global Settings**.

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

[Global Settings](#) [IGMP Snooping](#) [MVR](#) [Multicast Group](#) [IGMP Filter](#) [Querier](#)

 **Global Settings**

Version

IGMP Report Suppression

Unknown Multicast Pkt

Table 6-1 Description of Configuration Parameters of Global Multicast

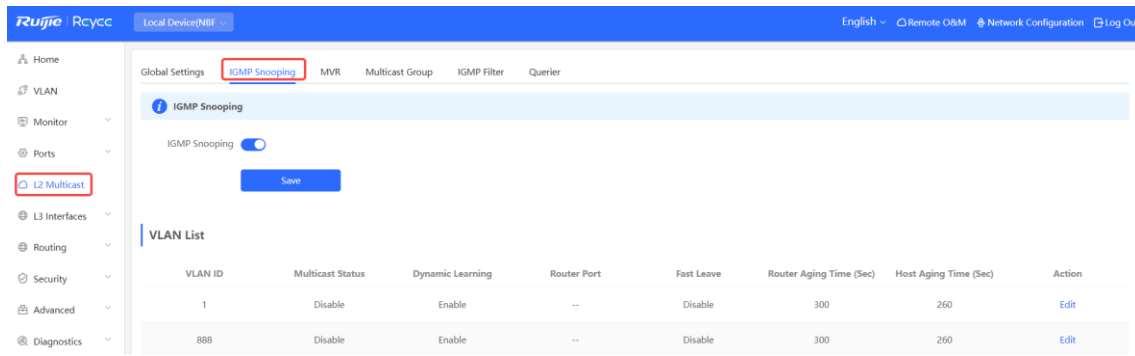
Parameter	Description	Default Value
Version	The Internet Group Management Protocol (IGMP) is a TCP/IP protocol that manages members in an IPv4 multicast group and runs on the multicast devices and hosts residing on the stub of the multicast network, creating and maintaining membership of the multicast group between the hosts and connected multicast devices. There are three versions of IGMP: IGMPv1, IGMPv2, IGMPv3. This parameter is used to set the highest version of IGMP packets that can be processed by Layer 2 multicast, and can be set to IGMPv2 or IGMPv3.	IGMPv2
IGMP Report Suppression	After this function is enabled, to reduce the number of packets in the network, save network bandwidth and ensure the performance of the IGMP multicast device, the switch forwards only one report packet to the multicast router if multiple downlink clients connected to the switch simultaneously send the report packet to demand the same multicast group.	Disable
Unknown Multicast Pkt	When both the global and VLAN multicast functions are enabled, the processing method for receiving unknown multicast packets can be set to Discard or Flood .	Discard

6.3 IGMP Snooping

6.3.1 Overview

The Internet Group Management Protocol (IGMP) snooping is an IP multicast snooping mechanism running on a VLAN to manage and control the forwarding of IP multicast traffic within the VLAN. It implements the L2 multicast function.

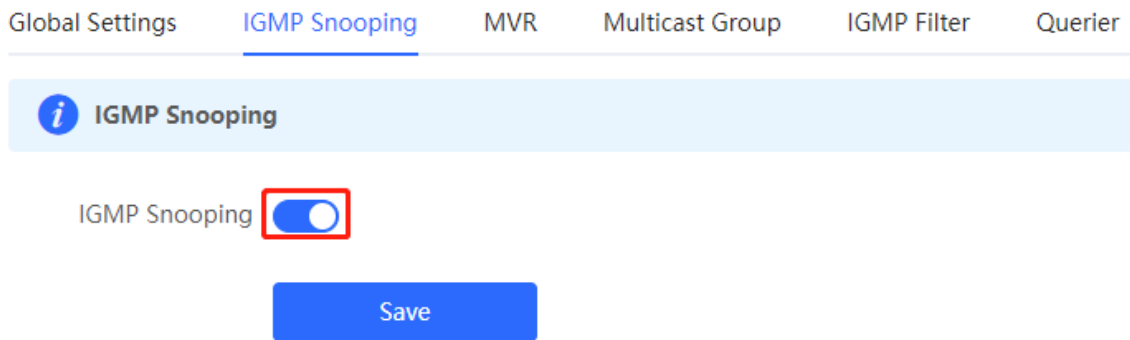
Generally, multicast packets need to pass through L2 switches, especially in some local area networks (LANs). When the Layer 2 switching device does not run IGMP Snooping, the IP multicast packets are broadcast in the VLAN; when the Layer 2 switching device runs IGMP Snooping, the Layer 2 device can snoop the IGMP protocol packets of the user host and the upstream PIM multicast device. In this way, an Layer 2 multicast entry is established, and IP multicast packets are controlled to be sent only to group member receivers, preventing multicast data from being broadcast on the Layer 2 network.



6.3.2 Enabling Global IGMP Snooping

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

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



6.3.3 Configuring Protocol Packet Processing Parameters

By controlling protocol packet processing, an L2 multicast device can establish static or dynamic multicast forwarding entries. In addition, the device can adjust parameters to refresh dynamic multicast forwarding entries and IGMP snooping membership quickly.

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

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

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

VLAN List

VLAN ID	Multicast Status	Dynamic Learning	Router Port	Fast Leave	Router Aging Time (Sec)	Host Aging Time (Sec)	Action
1	Disable	Enable	--	Disable	300	260	Edit
10	Disable	Enable	--	Disable	300	260	Edit
20	Disable	Enable	--	Disable	300	260	Edit

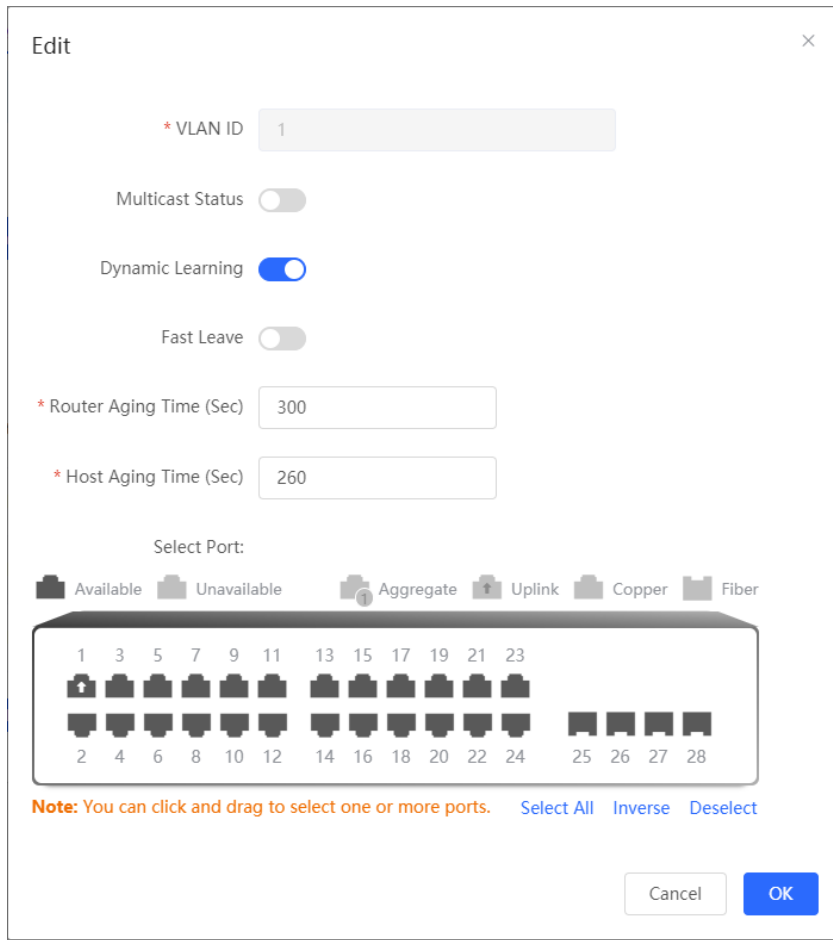


Table 6-2 Description of VLAN Configuration Parameters of IGMP Snooping

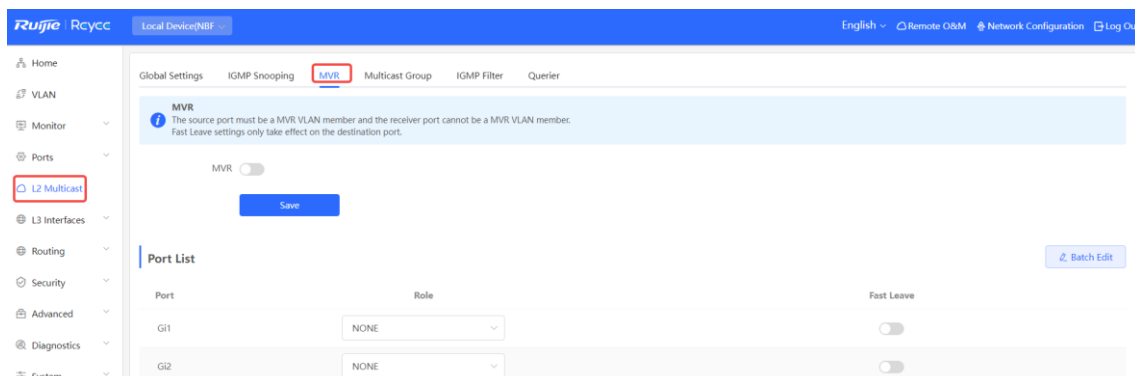
Parameter	Description	Default Value
Multicast Status	Whether to enable or disable the VLAN multicast function. The multicast function of a VLAN takes effect only when both the global IGMP snooping and VLAN multicast functions are enabled.	Disable
Dynamic Learning	The device running IGMP Snooping identifies the ports in the VLAN as router ports or member ports. The router port is the port on the Layer 2 multicast device that is connected to the Layer 3 multicast device, and the member port is the host port connected to the group on the Layer 2 multicast device. By snooping IGMP packets, the L2 multicast device can automatically discover and maintain dynamic multicast router ports.	Enable
Router Port	List of current multicast router ports includes dynamically learned routed ports (if Dynamic Learning function is enabled) and statically configured routed ports.	NA

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

6.4 Configuring MVR

6.4.1 Overview

IGMP snooping can forward multicast traffic only in the same VLAN. If multicast traffic needs to be forwarded to different VLANs, the multicast source must send multicast traffic to different VLANs. In order to save upstream bandwidth and reduce the burden of multicast sources, multicast VLAN register (MVR) comes into being. MVR can copy multicast traffic received from an MVR VLAN to the VLAN to which the user belongs and forward the traffic.




6.4.2 Configuring Global MVR Parameters

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

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

Global Settings IGMP Snooping **MVR** Multicast Group IGMP Filter Querier

MVR

 The source port must be a MVR VLAN member and the receiver port cannot be a MVR VLAN member. Fast Leave settings only take effect on the destination port.

MVR

* Multicast VLAN

* Start IP Address 

* End IP Address 

Save

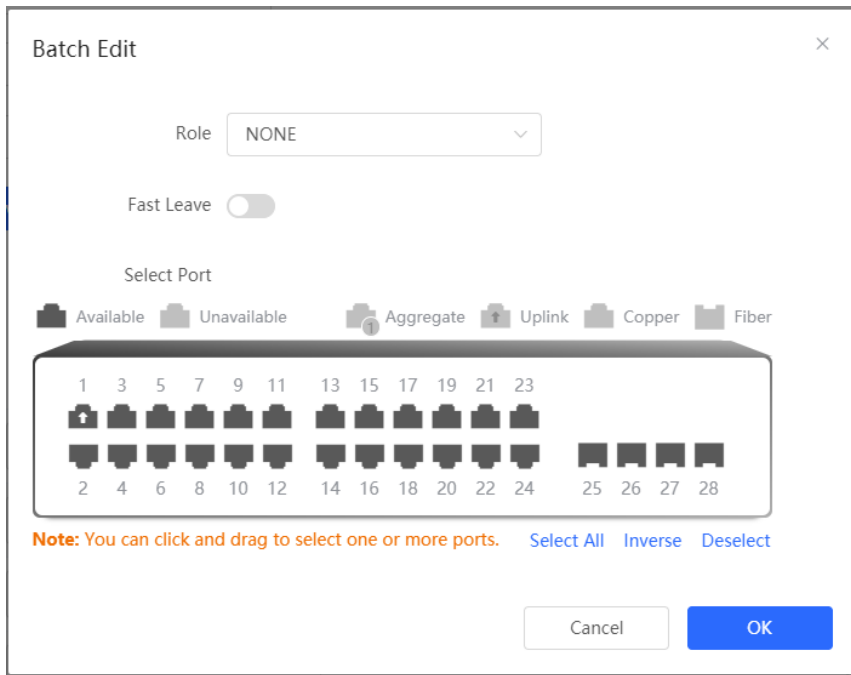
Table 6-3 Description of Configuring Global MVR Parameters

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

6.4.3 Configuring the MVR Ports

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

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



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

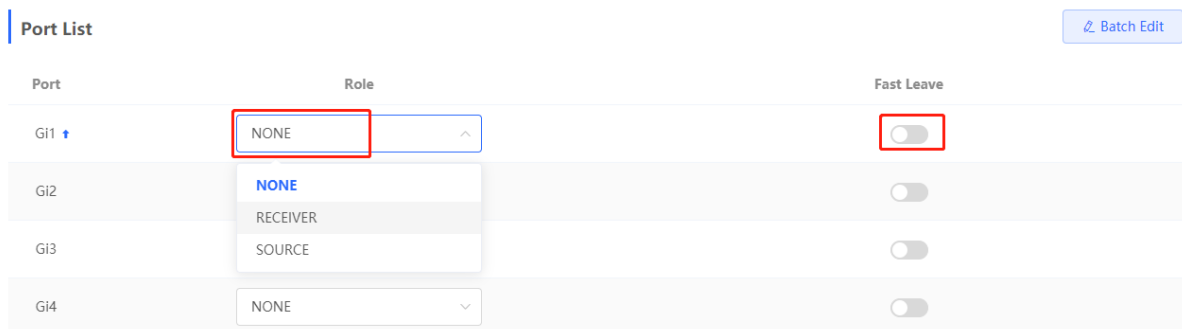


Table 6-4 Description of MVR Configuration Parameters of Ports

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

Note

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

6.5 Configuring Multicast Group

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

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

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

Click **Add** to create a multicast group.

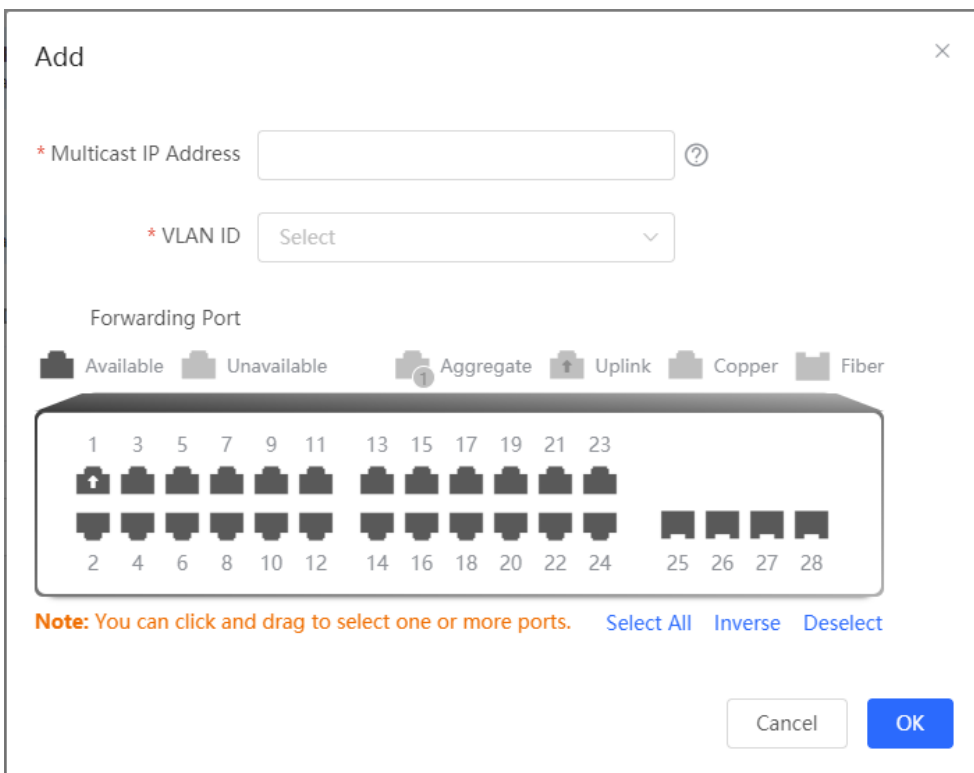
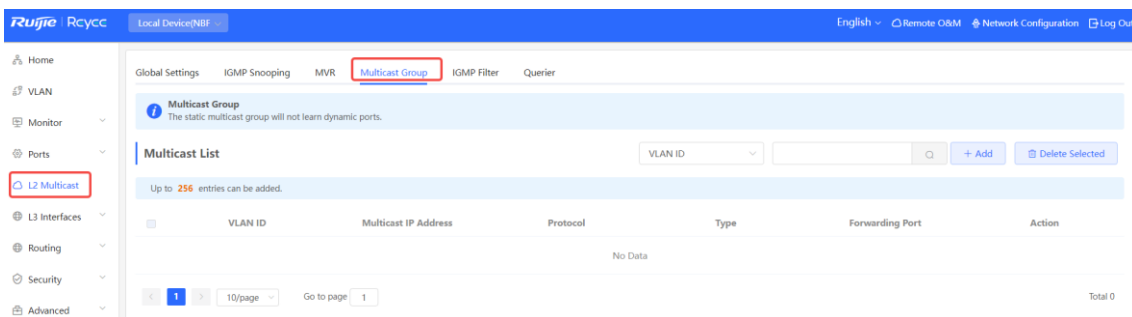


Table 6-5 Description of Multicast Group Configuration Parameters

Parameter	Description	Default Value
VLAN ID	VLAN, to which received multicast traffic belongs	NA
Multicast IP Address	On-demand multicast IP address	NA
Protocol	If the VLAN ID is a multicast VLAN and the multicast address is within the multicast IP address range of the MVR, the protocol is MVR. In other cases, the protocol is IGMP snooping.	NA
Type	Multicast group generation mode can be statically configured or dynamically learned. In normal cases, a port can join a multicast group only after the port receives an IGMP Report packet from the multicast, that is, dynamically learned mode. If you manually add a port to a group, the port can be statically added to the group and exchanges multicast group information with the PIM router without IGMP packet exchange.	NA
Forwarding Port	List of ports that forward multicast traffic	NA

 **Note**

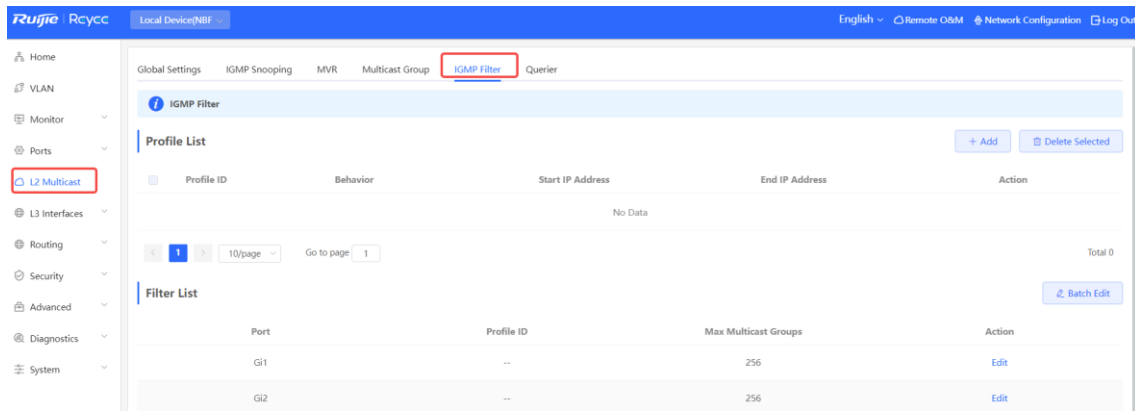
Static multicast groups cannot learn other dynamic forwarding ports.

6.6 Configuring a Port Filter

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

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

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



6.6.1 Configuring Profile

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

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

Add
✕

* Profile ID

Behavior

* Start IP Address ?

* End IP Address ?

Table 6-6 Description of Profile Configuration Parameters

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

Parameter	Description	Default Value
End IP Address	End Multicast IP address of the range of multicast group addresses	NA

6.6.2 Configuring a Range of Multicast Groups for a Profile

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

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

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

Filter List ↻ Batch Edit

Port	Profile ID	Max Multicast Groups	Action
Gi1 ↑	--	256	Edit
Gi2	--	256	Edit
Gi3	--	256	Edit
Gi4	--	256	Edit

Batch Edit ×

Profile ID

* Max Multicast Groups

Select Port

Available
 Unavailable
 Aggregate
 Uplink
 Copper
 Fiber

1	3	5	7	9	11	13	15	17	19	21	23
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	4	6	8	10	12	14	16	18	20	22	24
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Note: You can click and drag to select one or more ports. Select All Inverse Deselect

Table 6-7 Description of Port Filter Configuration Parameters

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

6.7 Setting an IGMP Querier

6.7.1 Overview

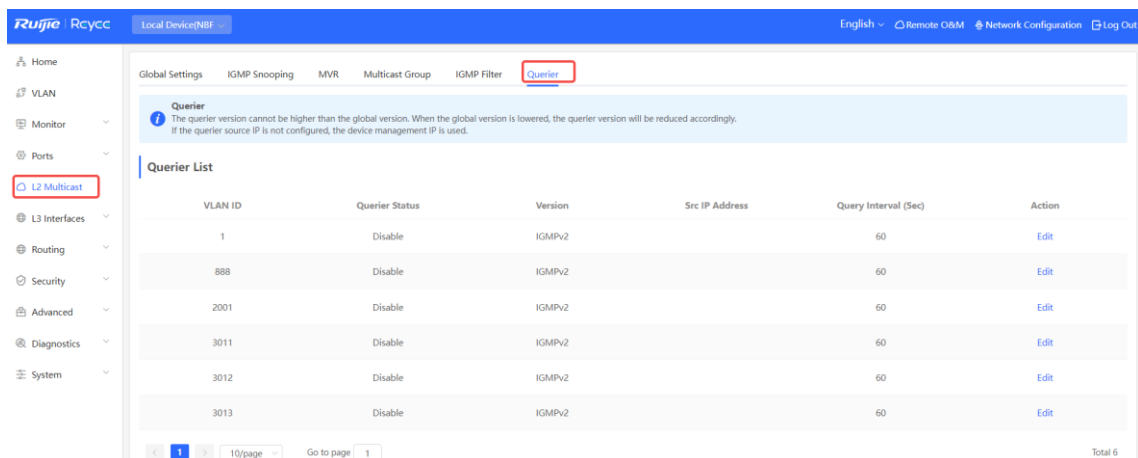
In a three-layer multicast network, the L3 multicast device serves as the querier and runs IGMP to maintain group membership. L2 multicast devices only need to listen to IGMP packets to establish and maintain forwarding entries and implement L2 multicasting. When a multicast source and user host are in the same L2 network, the query function is unavailable because the L2 device does not support IGMP. To resolve this problem, you can configure the IGMP snooping querier function on the L2 device so that the L2 device sends IGMP Query packets to user hosts on behalf of the L3 multicast device, and listens to and maintains IGMP Report packets responded by user hosts to establish L2 multicast forwarding entries.

6.7.2 Procedure

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

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

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



Edit
×

* VLAN ID

Querier Status

Version

Src IP Address

Query Interval (Sec)

Table 6-8 Description of Querier Configuration Parameters

Parameter	Description	Default Value
Querier Status	Whether to enable or disable the VLAN querier function.	Disable
Version	IGMP Protocol version of query packets sent by the querier. It can be set to IGMPv2 or IGMPv3.	IGMPv2
Src IP Address	Source IP address carried in query packets sent by the querier.	NA
Query Interval (Sec)	Packet transmission interval, of which the value range is from 30 to 18000, in seconds.	60 seconds

Note

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

7 L3 Management

Caution

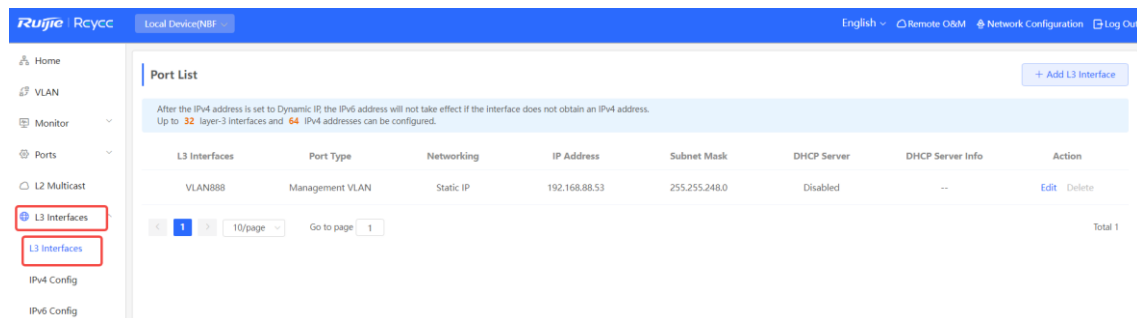
This section is applicable only to NBF Series Switches that support L3 functions. Products that do not support L3 functions such as RG-NBF2100 Series Switches, do not support the functions mentioned in this section.

7.1 Setting an L3 Interface

Choose **Local Device > L3 Interfaces > L3 Interfaces**.

The port list displays various types of L3 interfaces on the device, including SVIs, Routed Ports, and L3 Aggregate Ports.

Click **Add L3 Interfaces** to set a new L3 Interface.



Add

Port Type:

Networking:

Primary IP/Mask: [Add +](#) [?](#)

VLAN:

DHCP Mode: Disabled DHCP Server DHCP Relay

Table 7-1 Description of Configuration Parameters of L3 Interfaces

Parameter	Description
Port Type	The type of a created L3 interface. It can be an SVI, routed port, or L3 aggregate port. For details, see Table 4-1
Networking	Specifies DHCP or static mode for a port to obtain the IP address.
VLAN	Specifies the VLAN, to which an SVI belongs.
IP/Mask	When Networking is set to Static IP , you need to manually enter the IP address and subnet mask.
Select Port	Select the device port to be configured.
Aggregate	Specifies the aggregate port ID, for example, Ag1, when an L3 aggregate port is created.
DHCP Mode	Select whether to enable the DHCP service on the L3 interface. Disabled: Indicates that the DHCP service is disabled. No IP address can be assigned to clients connected to the interface. DHCP Server: Indicates that the device functions as the DHCP server to assign IP addresses to downlink devices connected to the interface. You need to set the start IP address of an address pool, number of IP addresses that can be assigned, and address lease; for more information, see 6.2 . DHCP Relay: Indicates that the device serves as a DHCP relay, obtains IP addresses from an external server, and assigns the IP addresses to downlink devices. The interface IP address and DHCP server IP address need to be configured. The interface IP address must be in the same network segment as the address pool of the DHCP server.
Excluded IP Address (Range)	When the device acts as a DHCP server, set the IP address in the address pool that is not used for assignment

Note

- VLAN 1 is the default SVI of the device. It can be neither modified nor deleted.
- The management VLAN is only displayed on the **L3 Interfaces** page but cannot be modified. To modify it, choose **Ports > MGMT IP**. For details, see [5.6](#).
- The DHCP relay and DHCP server functions of an L3 interface are mutually exclusive and cannot be configured at the same time.
- The member ports of an L3 aggregated interface must be configured as routed ports.

7.2 Configuring the IPv6 Address for the L3 Interface

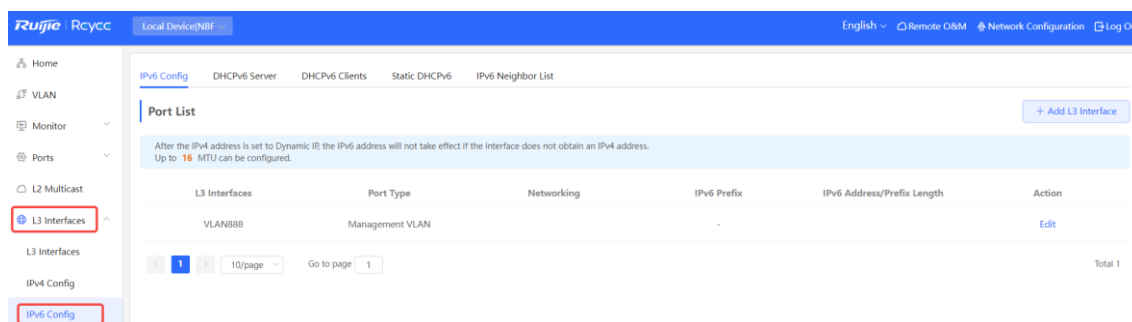
IPv6 is a suite of standard protocols for the network layer of the Internet. IPv6 solves the following problems of IPv4:

- Address depletion:

NAT must be enabled on the gateway to convert multiple private network addresses into a public network address. This results in an extra delay caused by address translation, and may interrupt the connection between devices inside and outside the gateway. In addition, you need to add a mapping to enable access to the intranet devices from the Internet.

- Design defect:
IP addresses cannot be formed using network topology mapping, and a large-scale routing table is needed.
- Lack of built-in authentication and confidentiality:
IPv4 itself does not require encryption. It is difficult to trace the source after address translation. As the number of addresses in a network segment is limited, it is easy for attackers to scan all hosts in the LAN. IPv6 integrates IPSec by default. End-to-end connections can be established without address translation, and it is easy to trace the source. IPv6 has a huge address space. A 64-bit prefix address supports 64 host bits, which increases the difficulty and cost of scanning and therefore prevents attacks.

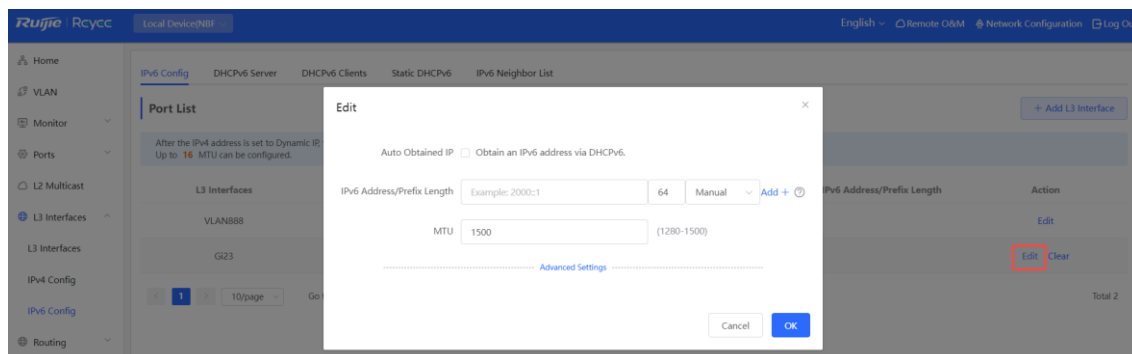
Choose Local Device > L3 Interfaces > IPv6 Config.



Caution

- Add an IPv4 L3 interface first. Then, select the interface on the IPv6 L3 interface configuration page, and click **Edit**.
- If the IPv4 address of an interface is set to **DHCP** and no IPv4 address is obtained, the IPv6 address of this interface will not take effect.

- If an upstream DHCPv6 server is available, select **Auto Obtained IP** and specify the MTU. The default MTU is **1500**. You are advised to retain the default value. Then, click **OK**.



- If no upstream DHCPv6 server is available to assign the IP address, configure the IPv6 information as follows:

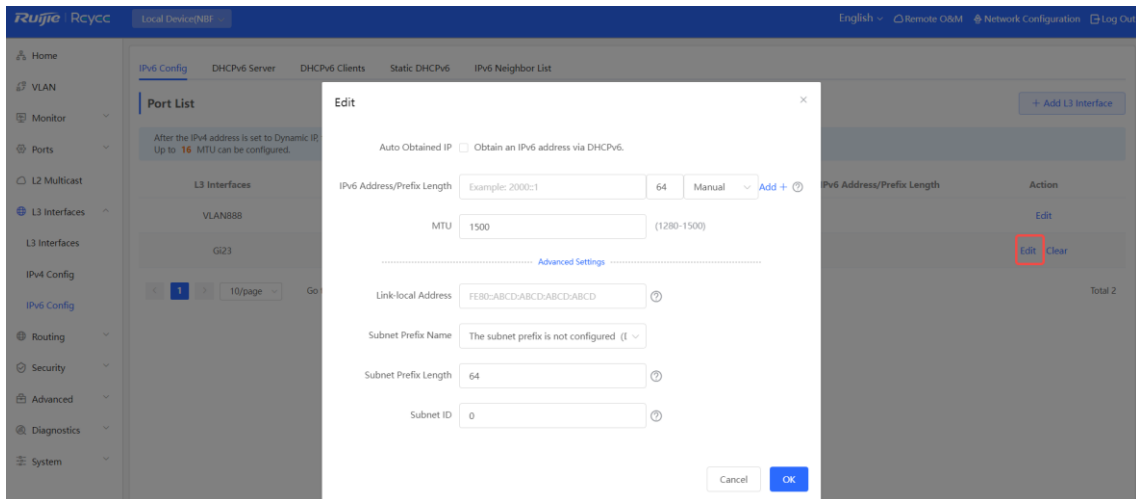


Table 7-2 IPv6 Address Configuration Parameters of the L3 Interface

Parameter	Description
Obtain an IPv6 address via DHCPv6	If no upstream DHCPv6 server is available, do not select Auto Obtained IP . Instead, manually add the IPv6 address.
IPv6 Address/Prefix Length	Configure the IPv6 address and prefix length. You can click Add to add multiple IPv6 addresses. If the primary IP address is empty, the configured secondary IP address is invalid. For manual configuration, the prefix length ranges from 1 to 128. For auto configuration, the prefix length ranges from 1 to 64. If the IPv6 prefix length of the L3 interface is between 48 and 64, this address can be assigned.
MTU	Configure the MTU. The default MTU is 1500 .
Advanced Settings	Click Advanced Settings to configure the link local address, subnet prefix name, subnet prefix length, and subnet ID.
Link-local Address	The link local address is used to number hosts on a single network link. The first 10 bits of link address in binary notation must be '1111111010'.
Subnet Prefix Name	It identifies a specified link (subnet).
Subnet Prefix Length	It indicates the length (in bits) of the subnet prefix in the address. The value ranges from 48 to 64 (The subnet prefix length must be greater than the length of the prefix assigned by the server).
Subnet ID	Configure the subnet ID of the interface in hexadecimal notation. The number of available subnet IDs is $(2^N - 1)$, where N is equal to (Subnet prefix length of the interface - Length of the prefix assigned by the server).

7.3 Configuring the DHCP Service

After the DHCP server function is enabled on the L3 interface, the device can assign IP addresses to downlink devices connected to the port.

7.3.1 Enable DHCP Services

Choose **Local Device > L3 Interfaces > L3 Interfaces**.

Click **Edit** on the designated port, or click **Add L3 Interface** to add a Layer 3 interface, select DHCP mode for local allocation, and enter the starting IP of the address pool, the number of allocated IPs, the excluded IP address range, and the address lease time.

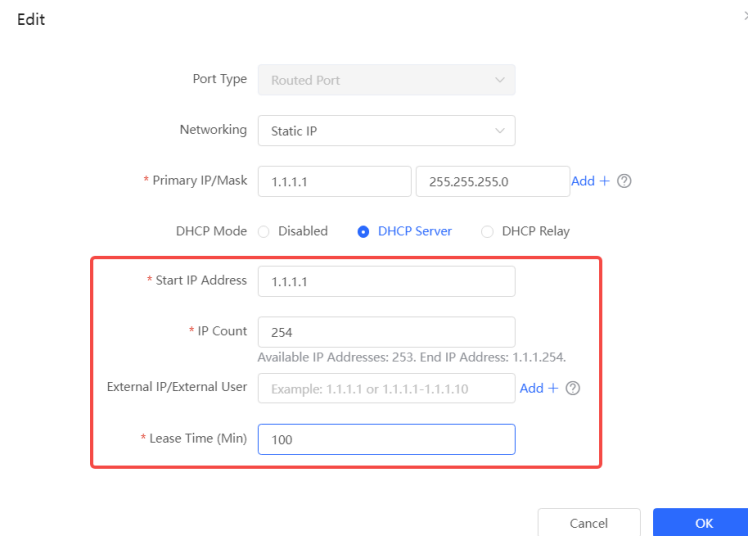
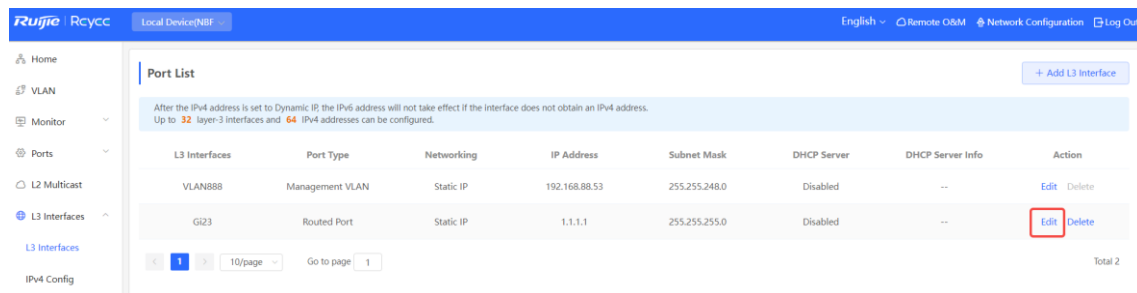


Table 7-3 Description of DHCP Server Configuration Parameters

Parameter	Description
DHCP Mode	To choose DHCP server
Start	The DHCP server assigns the Start IP address automatically, which is the Start IP address of the DHCP address pool. A client obtains an IP address from the address pool. If all the addresses in the address pool are used up, no IP address can be obtained from the address pool.
IP Count	The number of IP addresses in the address pool

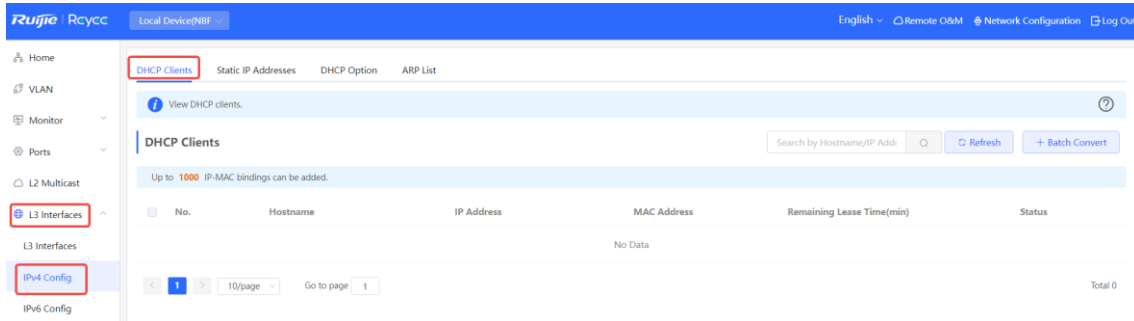
Parameter	Description
Excluded IP Address (Range)	IP addresses in the address pool that are not used for allocation, support inputting a single IP address or IP network segment, and add up to 20 address segments.
Lease Time(Min)	The lease of the address, in minutes. Lease Time(Min) : When a downlink client is connected, the leased IP address is automatically renewed. If a leased IP address is not renewed due to client disconnection or network instability, the IP address will be reclaimed after the lease term expires. After the downlink client connection is restored, the client can request an IP address again

7.3.2 Viewing the DHCP Client

Choose **Local Device > L3 Interfaces > IPv4 Config > DHCP Clients**.

View the addresses automatically allocated to downlink clients after the L3 Interfaces enable DHCP services. You can find the client information based on the MAC address, IP address, or username.

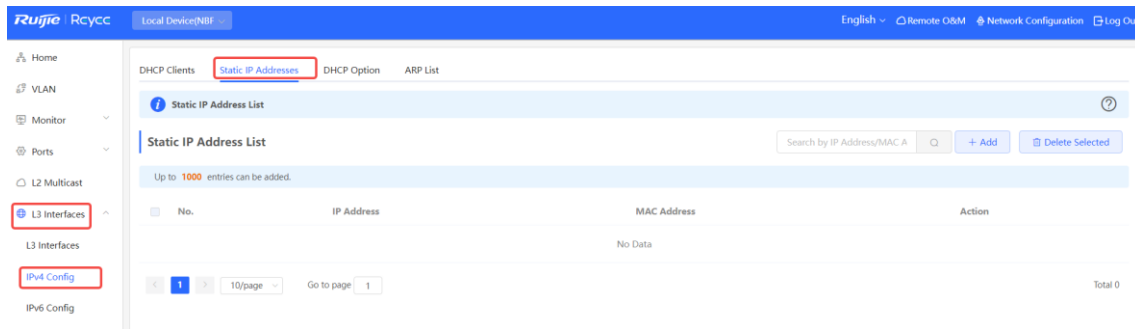
Find the target client and click **Convert to Static IP** in the **Status** column, or select desired clients and click **Batch Convert**. The dynamic address allocation relationship is added to the static address allocation list, so that the host can obtain the bound IP address for each connection. For details on how to view the static address allocation list, see [7.3.3](#).



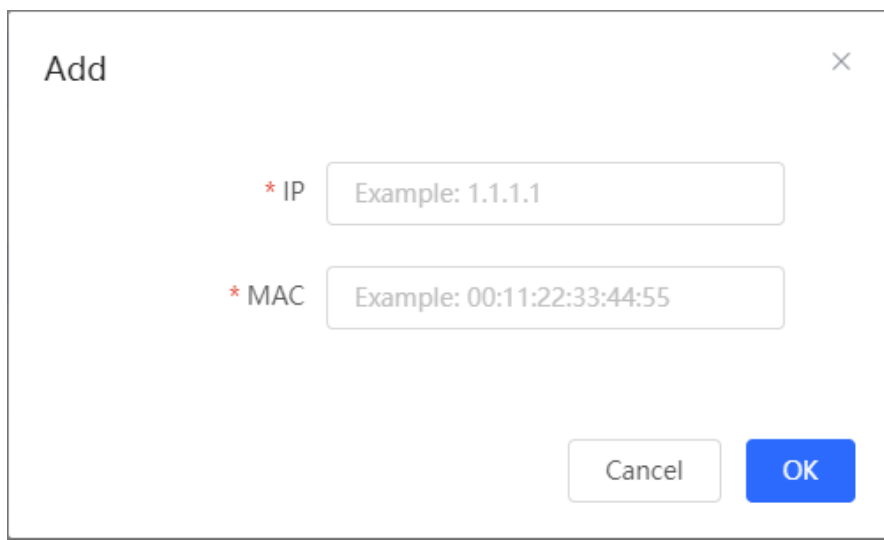
7.3.3 Configuring Static IP Addresses Allocation

Choose **Local Device > L3 Interfaces > IPv4 Config > Static IP Addresses**.

Displays the client entries which are converted into static addresses in the client list as well as manually added static address entries. The upper-right search box supports searching for corresponding entries based on the assigned IP address or the Device MAC Address



Click **Add**. In the displayed static IP address binding dialog box, enter the MAC address and IP address of the client to be bound, and click **OK**. After a static IP address is bound, the bound IP address will be obtained each time the corresponding downlink client connects to the network.



To delete a static address, select the static entry to be deleted in **Static IP Address List**, and click **Delete Selected**; or click **Delete** in the last **Action** column of the corresponding entry.

7.3.4 Configuring the DHCP Server Options

Choose **Local Device** > **L3 Interfaces** > **IPv4 Config** > **DHCP Option**.

The configuration delivered to the downlink devices is optional and takes effect globally when the L3 interface serves as the DHCP server.

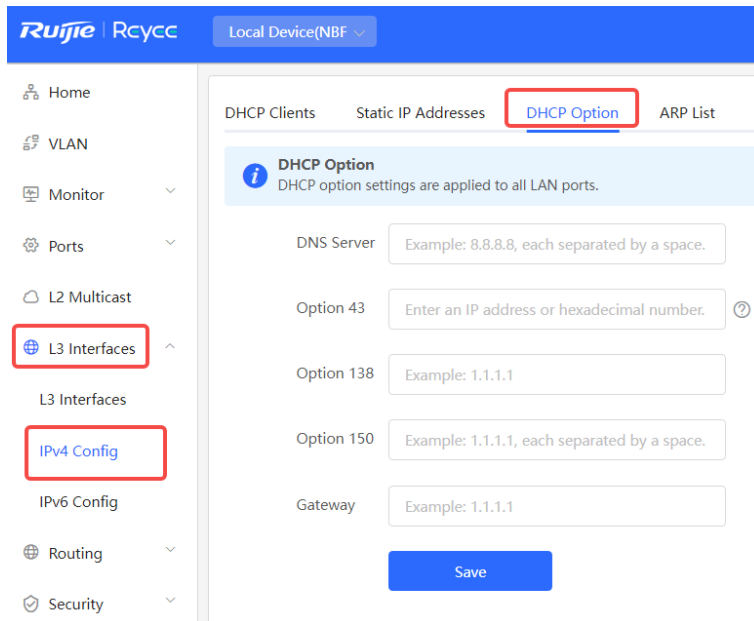


Table 7-4 Description of the DHCP Server Options Configuration Parameters

Parameter	Description
DNS Server	DNS server address provided by an ISP. Multiple IP addresses can be entered and separated by spaces.
Option 43	When the AC (wireless controller) and the AP are not in the same LAN, the AP cannot discover the AC through broadcast after obtaining an IP address from the DHCP server. To enable the AP to discover the AC, you need to configure Option 43 carried in the DHCP response packet on the DHCP server.
Option 138	Enter the IP address of the AC. Similar to Option 43, when the AC and AP are not in the same LAN, you can configure Option 138 to enable the AP to obtain the IPv4 address of the AC.
Option 150	Enter the IP address of the TFTP server. Enter the IP address of the TFTP server to specify the TFTP server address assigned to the client. Multiple IP addresses can be entered and separated by spaces.

Note

DHCP options are optional configuration when the device functions as an L3 DHCP server. The configuration takes effect globally and does not need to be configured by default. If no DNS server address is specified, the DNS address assigned to a downlink port is the gateway IP address by default.

7.4 Configuring the DHCPv6 Server

Dynamic Host Configuration Protocol for IPv6 (DHCPv6) is a protocol that allows the DHCP server to pass configuration information (such as the IPv6 network address) to IPv6 nodes.

Compared with other IPv6 address assignment methods (such as manual configuration and stateless address autoconfiguration), DHCPv6 provides the functions of address assignment, Prefix Delegation (PD), and configuration parameter assignment.

- DHCPv6 is both a stateful address autoconfiguration protocol and a stateless address configuration protocol. It supports flexible addition and reuse of network addresses, and can record the assigned addresses, thus enhancing network management.
- The configuration parameter assignment function of DHCPv6 can solve the problem that parameters cannot be obtained under the stateless address autoconfiguration protocol, and provide the host with configuration information, such as the DNS server address and domain name.

Choose **Local Device > L3 Interfaces > IPv6 Config > DHCPv6 Server** .

- (1) Click **Add**, select a L3 interface and IP address assignment method, and enter the address lease term and DNS server address. The address lease term is 30 minutes by default. You are advised to retain the default value. Then, click **OK**.

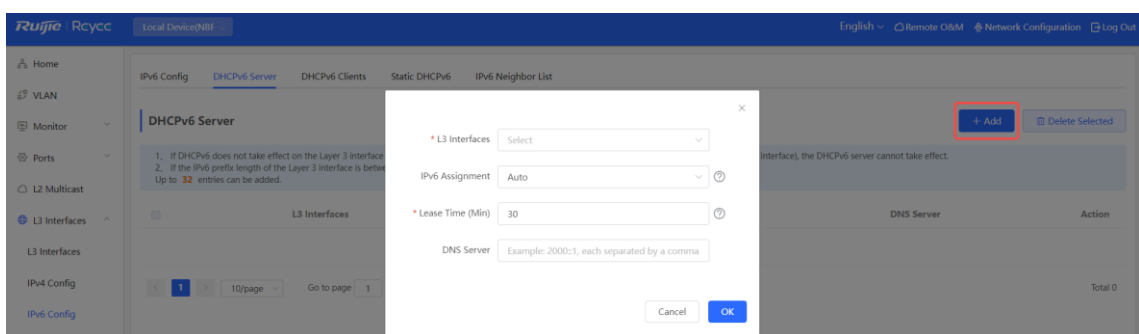


Table 7-5 IPv6 Address Configuration Parameters of the L3 Interface

Parameter	Description
L3 Interfaces	Select the L3 interface for which the DHCPv6 server needs to be added.
IPv6 Assignment	If this parameter is set to Auto , both DHCPv6 and SLAAC are used to assign

Parameter	Description
	IPv6 addresses.
Lease Time	The default value is 30 minutes. The value ranges from 30 to 2880 minutes. When the device stays online and the network is normal, this parameter is periodically updated (reset to 0).
DNS Server	Enter the DNS server address.

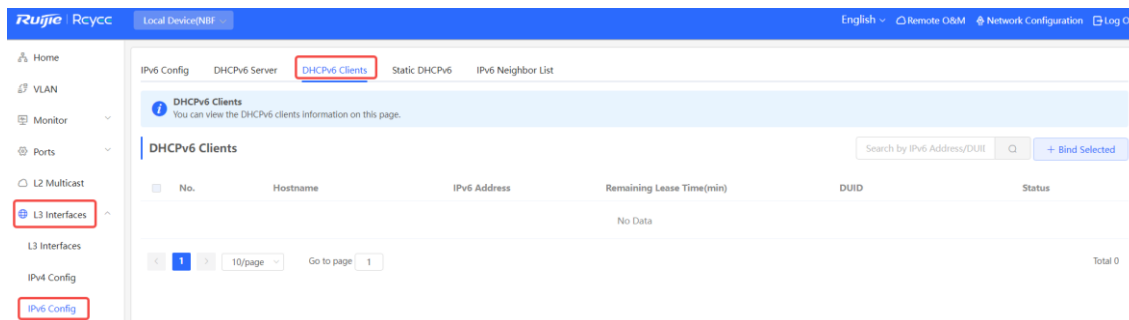
7.4.2 Viewing DHCPv6 Clients

Choose **Local Device > L3 Interfaces > IPv6 Config > DHCPv6 Clients**.

View the information of the client that obtains the IPv6 address from the device, including the host name, IPv6 address, remaining lease term, DHCPv6 Unique Identifier (DUID), and status. Click + Bind Selected to bind the IP addresses and hosts in batches, so that the IP addresses obtained by the hosts from the switch remain unchanged.

Note

Each server or client has only one DUID for identification.



7.4.3 Configuring the Static DHCPv6 Address

Configure the IPv6 address statically bound to the DUID of a client so that the client can obtain the specified address each time.

Choose **Local Device > L3 Interfaces > IPv6 Config > Static DHCPv6**.

Click **Add**, and enter the IPv6 address and DUID. You are advised to bind the IPv6 address and DUID in the client list. You can run the `ipconfig /all` command on the Command Prompt in Windows to view the DUID.

```
Command Prompt
Microsoft Windows [Version 10.0.17763.1577]
(c) 2018 Microsoft Corporation. All rights reserved.

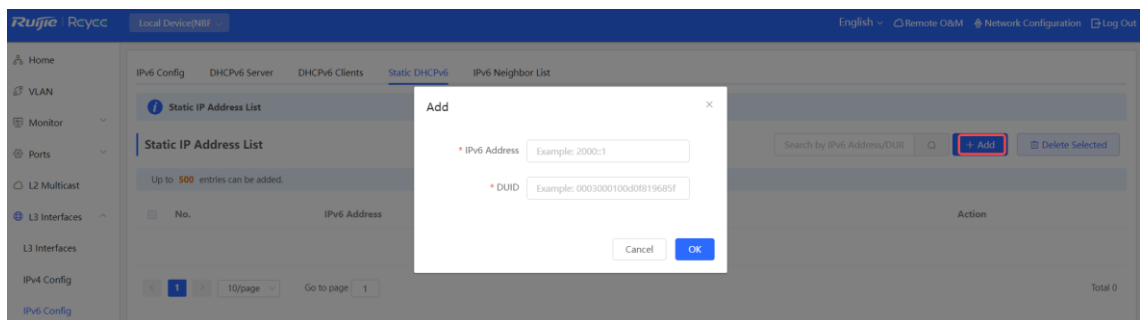
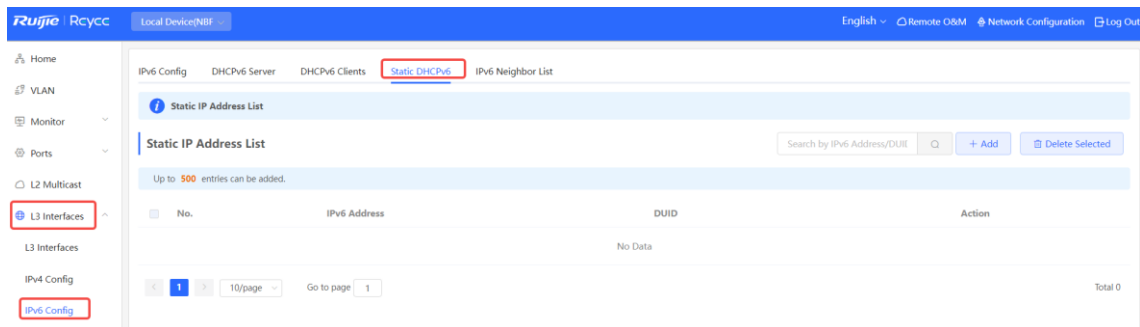
C:\Users\admin>ipconfig /all

Windows IP Configuration

Host Name . . . . . : PC-
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter

Connection-specific DNS Suffix . . . :
Description . . . . . : Ruijie VirtIO Ethernet Adapter
Physical Address. . . . . :
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::6dd5:266f:b695:55df%12(Preferred)
IPv4 Address. . . . . : 172.26.1.123(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Thursday, December 22, 2022 5:29:03 PM
Lease Expires . . . . . : Friday, December 30, 2022 5:28:57 PM
Default Gateway . . . . . : 172.26.1.1
DHCP Server . . . . . : 172.26.1.1
DHCPv6 IAID . . . . . : 340939776
DHCPv6 Client DUID. . . . . : 00-01-00-01-27-C7-77-50-52-54-00-3C-D6-BE
DNS Servers . . . . . : 192.168.58.94
```



7.5 Configuring the IPv6 Neighbor List

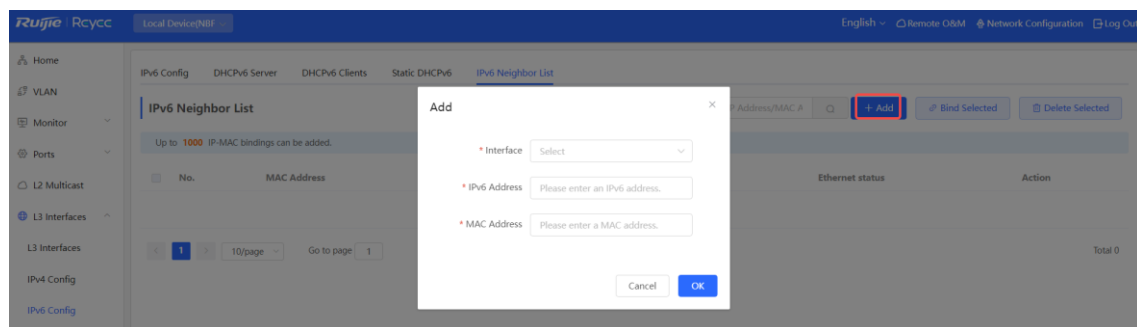
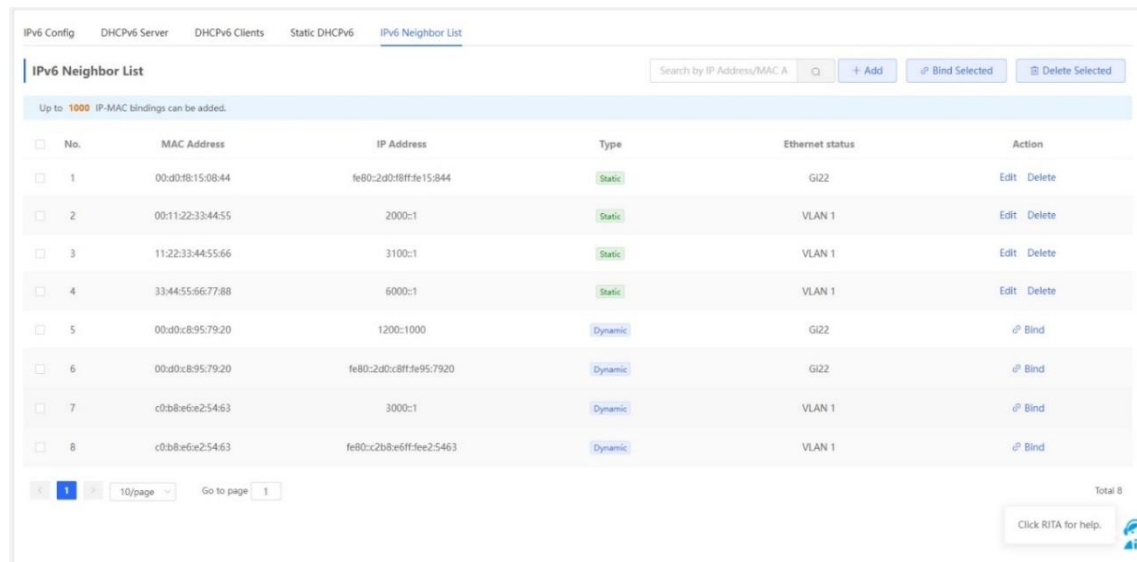
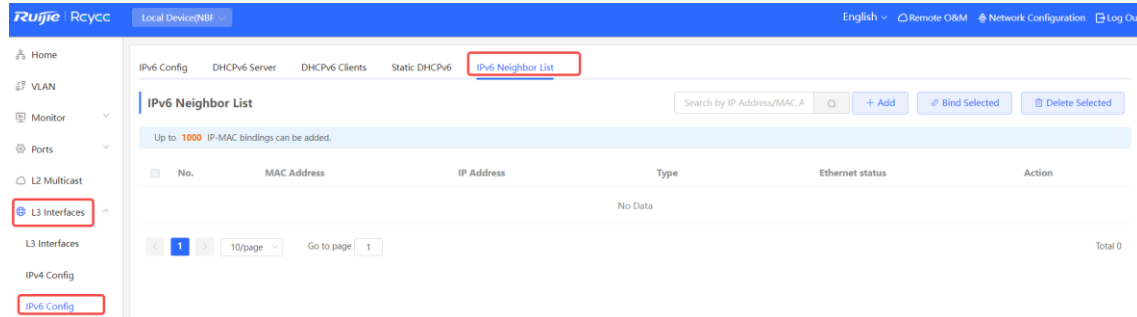
In IPv6, Neighbor Discovery Protocol (NDP) is an important basic protocol. NDP replaces the ARP and ICMP route discovery protocols of IPv4, and supports the following functions: address resolution, neighbor status tracking, duplicate address detection, router discovery, and redirection.

Choose **Local Device > L3 Interfaces > IPv6 Config > IPv6 Neighbor List**.

Click **Add** and manually add the interface, IPv6 address and MAC address of the neighbor.

Click **Bind Selected** to bind the IPv6 address and MAC address in the list to prevent ND attacks.

You can also modify, delete, batch delete, or search neighbors (by IP address or MAC address).



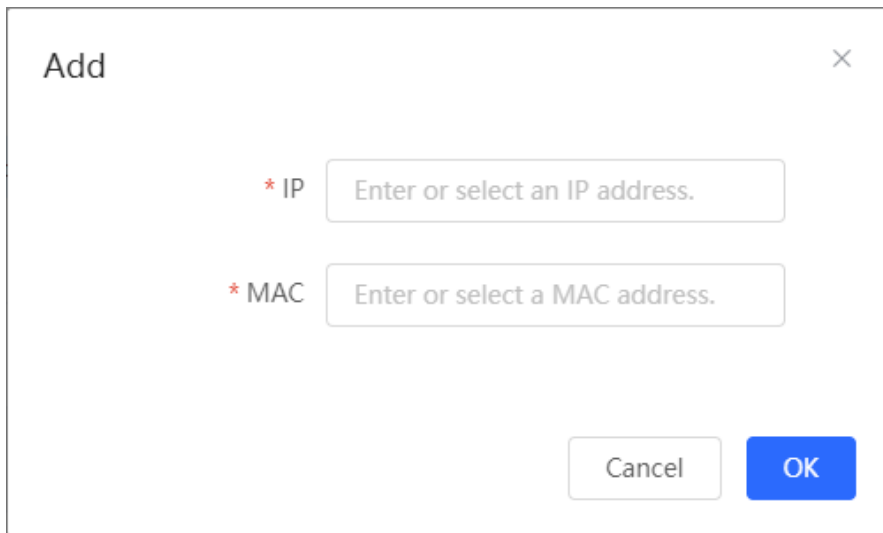
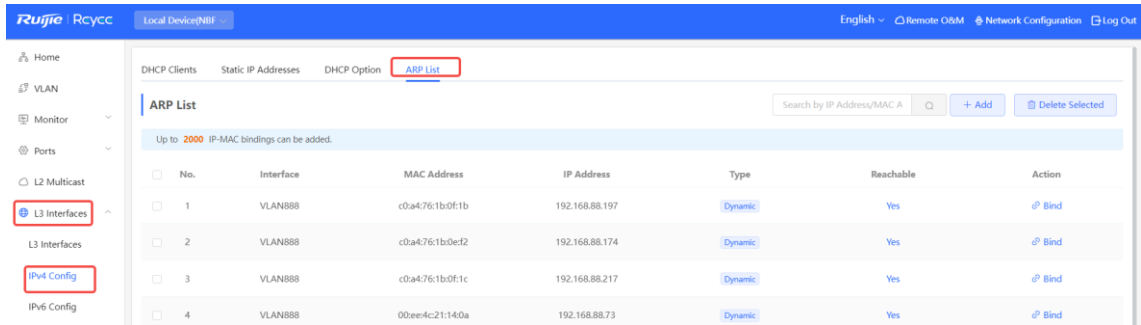
7.6 Configuring a Static ARP Entry

Choose **Local Device > L3 Interfaces > IPv4 Config > ARP List**.

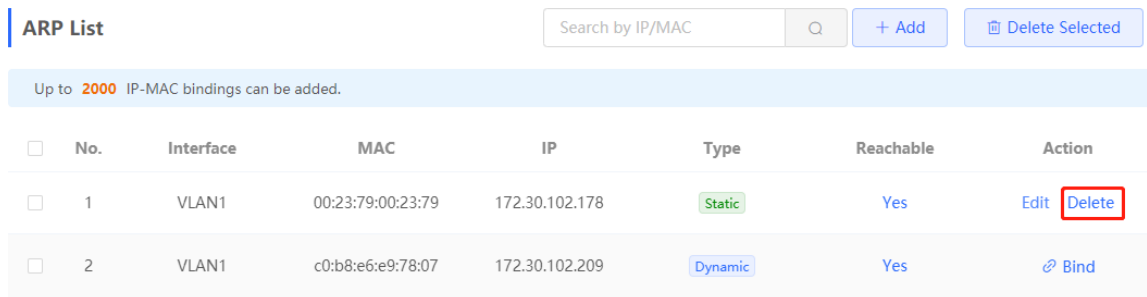
The device learns the IP address and MAC address of the network devices connected to its interfaces and generates the corresponding ARP entries. Supports binding ARP mappings or manually specifying the IP

address and MAC address mapping to prevent devices from learning wrong ARP entries and improve network security.

- To bind a dynamic ARP entry to a static entry: Select the ARP mapping entry dynamically obtained in the **ARP List**, and click **Bind** to complete the binding.
- To manually configure a static ARP entry: Click **Add**, enter the IP address and MAC address to be bound, and click **OK**.



To remove the binding between a static IP address and a MAC address, click **Delete** in the **Action** column.



8 Configuring Route

Notice

This section is applicable only to NBF Series Switches that support L3 functions. Products that do not support L3 functions such as RG-NBF2100 Series Switches, do not support the functions mentioned in this section.

8.1 Configuring Static Routes

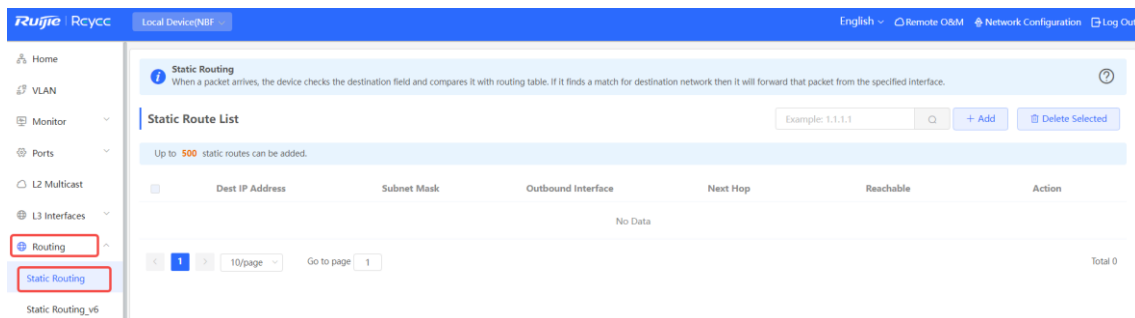
Choose **Local Device > L3 Interfaces > Static Routing** .

Static routes are manually configured by the user. When a data packet matches a static route, the packet will be forwarded according to the specified forwarding mode.

Caution

Static routes cannot automatically adapt to changes of the network topology. When the network topology changes, you need to reconfigure the static routes.

Click **Add** . In the dialog box that appears, enter the destination address, subnet mask, outbound interface, and next-hop IP address to create a static route.



Edit ✕

* Dest IP Address

* Subnet Mask

Outbound Interface ▾

* Next Hop

Table 8-1 Description of Static Routes Configuration Parameters

Parameter	Description
Dest IP Address	Specify the destination network to which the data packet is to be sent. The device matches the data packet based on the destination address and subnet mask.
Subnet Mask	Specify the subnet mask of the destination network. The device matches the data packet based on the destination address and subnet mask.
Outbound Interface	Specify the interface that forwards the data packet.
Next Hop	Specify the IP address of the next hop in the route for the data packet

After a static route is created, you can find the relevant route configuration and reachability status in the static route list. The **Reachable** parameter specifies whether the next hop is reachable, based on which you can determine whether the route takes effect. If the value is **No**, check whether the outbound interface in the current route can ping the next-hop address.

Static Route List Example: 1.1.1.1

Up to 500 static routes can be added.

<input type="checkbox"/>	Dest IP Address	Subnet Mask	Outbound Int	Next Hop	Reachable	Action
<input type="checkbox"/>	2.1.1.0	255.255.255.0	Gi9	3.1.1.1	No	Edit Delete

The route is unreachable. Please initiate a Ping test from the outbound interface to the next hop.

To delete or modify a static route, in **Static Route List**, you can click **Delete** or **Edit** in the last **Action** column; or select the static route entry to be deleted, click **Delete Selected** to delete multiple static route entries.

8.2 Configuring the IPv6 Static Route

Choose **Local Device > Routing > Static Routing_v6**.

You need to manually configure an IPv6 static route. When the packet matches the static route, the packet will be forwarded according to the specified forwarding method.

Caution

The static route cannot automatically adapt to changes in the network topology. When the network topology changes, you need to manually reconfigure the static route.

Click **Add**, and enter the destination IPv6 address, length, outbound interface, and next-hop IP address to create a static route.

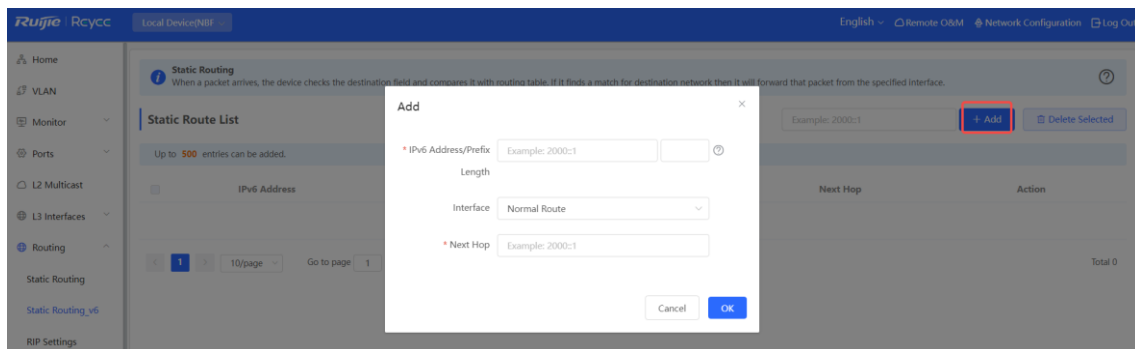
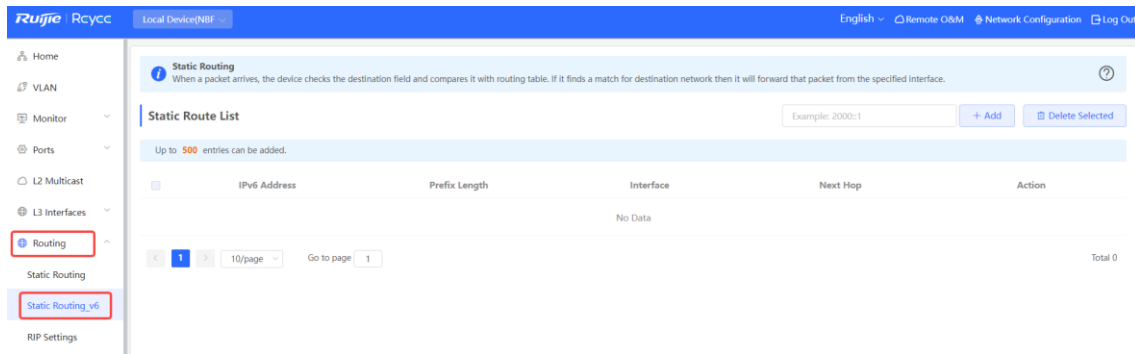


Table 8-2 IPv6 Static Route Configuration Parameters

Parameter	Description
IPv6 Address/Prefix Length	Destination network of the packet. The destination address of the packet is matched according to the IPv6 address and prefix length.
Outbound Interface	Interface that forwards the packet.
Next Hop	IP address of the next routing node to which the packet is sent.

8.3 Configuring RIP

Routing Information Protocol (RIP) is applicable to small and medium-sized networks and is a dynamic routing protocol that is easy to configure. RIP measures the network distance based on the number of hops and selects a route based on the distance. RIP uses UDP port 520 to exchange the routing information.

8.3.1 Configuring RIP Basic Functions

Choose **Local Device > Routing > RIP Settings** .

Click **Add** and configure the network segment and interface.

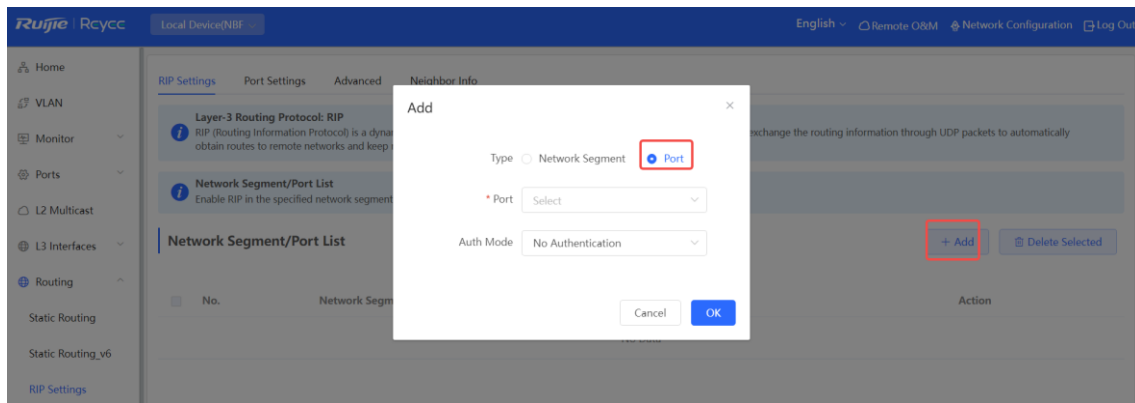
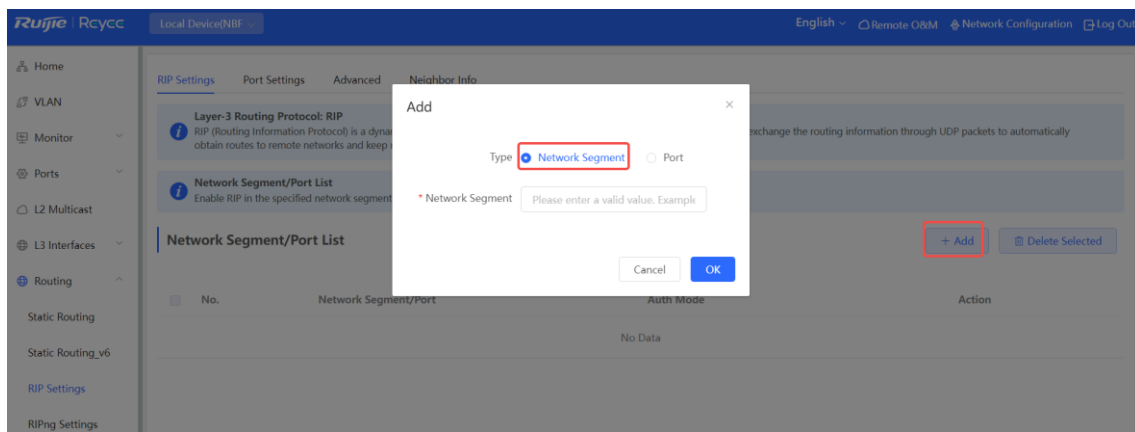
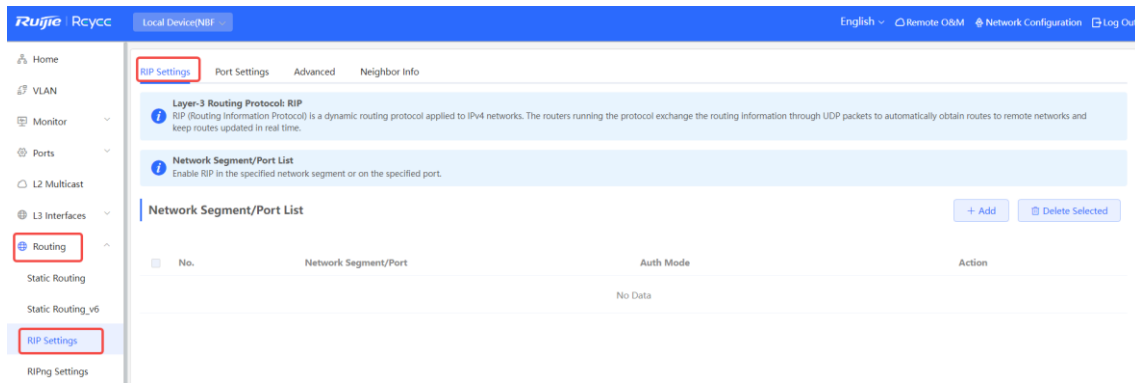


Table 8-3 RIP Configuration Parameters

Parameter	Description
Type	<p>Network Segment : Enable RIP in the specified network segment. The IP addresses of this network segment are added to the RIP routing table. The device and its RIP-enabled neighbor devices learn the routing table from each other.</p> <p>Port : Enable RIP on the specified port. All the IP addresses of this port are added to the RIP routing table. The device and its RIP-enabled neighbor devices learn the routing table from each other.</p>
Network Segment	Enter the network segment, for example, 10.1.0.0/24 , when Type is set to Network

Parameter	Description
	Segment . RIP will be enabled on all interfaces of the device covered by this network segment.
Port	Select a VLAN interface or physical port when Type is set to Port .
Auth Mode	No Authentication : The protocol packets are not authenticated. Encrypted Text : The protocol packets are authenticated, and the authentication key is transmitted with the protocol packets in the form of encrypted text. Plain Text : The protocol packets are authenticated, and the authentication key is transmitted with the protocol packets in the form of plain text.
Auth Key	Enter the authentication key to authenticate protocol packets when Auth Mode is set to Encrypted Text or Plain Text .

8.3.2 Configuring the RIP Port

Choose **Local Device > Routing > RIP Settings > Port Settings** .

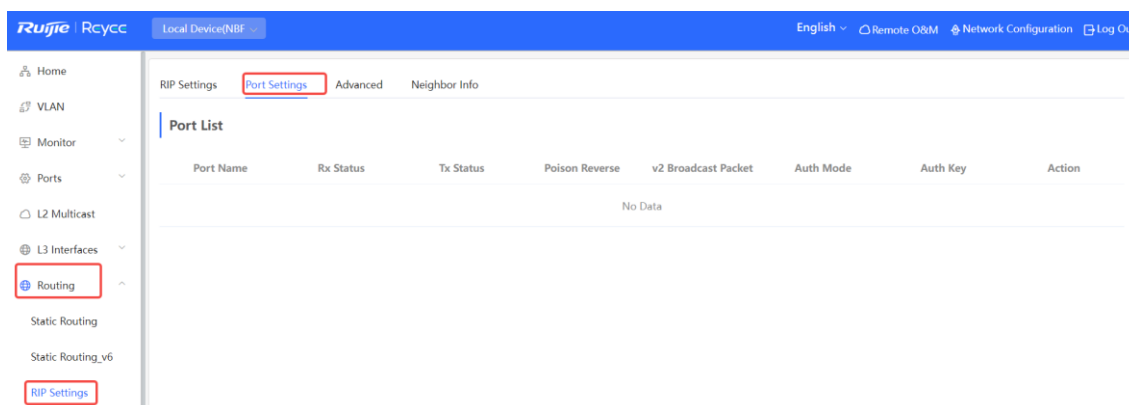


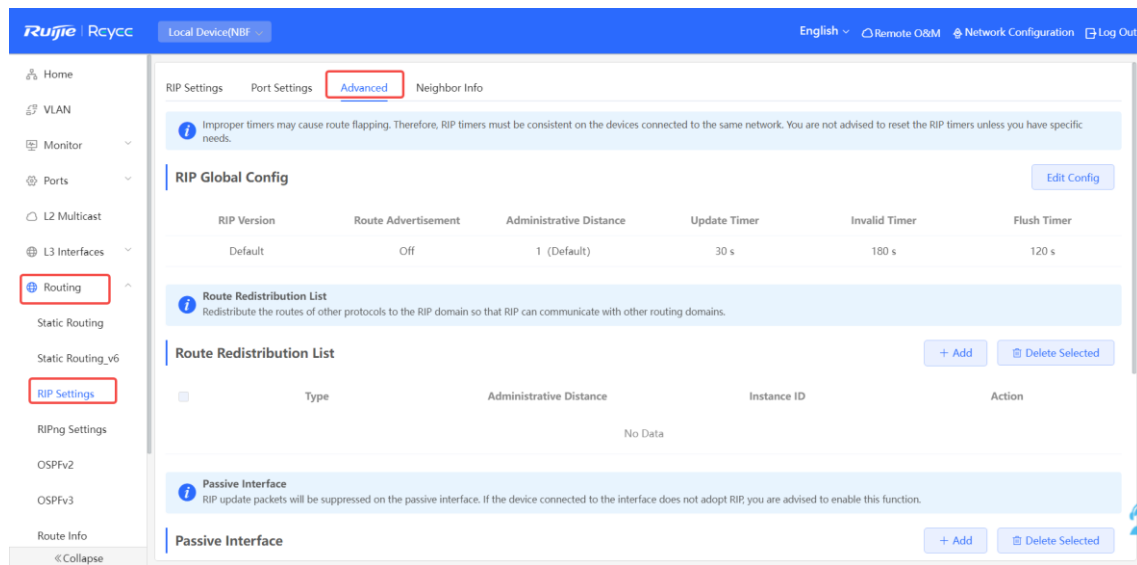
Table 8-4 Configuration Parameters in the Port List

Parameter	Description
Port Name	Name of the port where RIP is enabled.
RxStatus	RIP version of packets currently received.
Tx Status	RIP version of packets currently transmitted.
Poison Reverse	After the port learns the route, the route overhead is set to 16 (indicating that the route is unreachable), and the route is sent back to the neighbor from the original port to avoid a loop.
v2 Broadcast Packet	When a neighbor does not support multicast, broadcast packets can be sent. You are advised to disable RIPv2 broadcast packets to improve network

Parameter	Description
	performance.
Auth Mode	<p>No Authentication : The protocol packets are not authenticated.</p> <p>Encrypted Text : The protocol packets are authenticated, and the authentication key is transmitted with the protocol packets in the form of encrypted text.</p> <p>Plain Text : The protocol packets are authenticated, and the authentication key is transmitted with the protocol packets in the form of plain text.</p>
Auth Key	Enter the authentication key to authenticate protocol packets when Auth Mode is set to Encrypted Text or Plain Text .
Action	Click Edit to modify RIP settings of the port.

8.3.3 Configuring the RIP Global Configuration

Choose **Local Device > Routing > RIP Settings > Advanced** , click **Edit Config** , and configure RIP global configuration parameters.



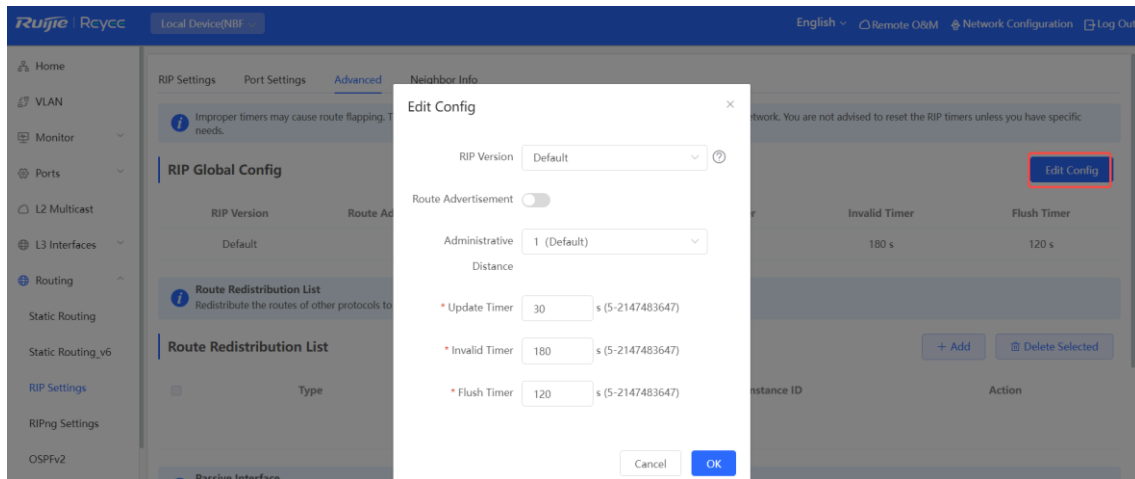


Table 8-5 RIP Global Configuration Parameters

Parameter	Description
RIP Version	<p>Default : Select RIPv2 for sending packets and RIPv1/v2 for receiving packets.</p> <p>V1 : Select RIPv1 for sending and receiving packets.</p> <p>V2 : Select RIPv2 for sending and receiving packets.</p>
Route Advertisement	After route advertisement is enabled, the current device generates a default route and sends it to the neighbor.
Administrative Distance	Redistribute routes of other protocols to the RIP domain so that RIP can interwork with other routing domains.
Update Timer	RIP update cycle. The routing information is updated every 30 seconds by default.
Invalid Timer	If no update is received before a route becomes invalid, the route is considered unreachable. The default value is 180 seconds.
Flush Timer	If no update is received before the flush timer of an invalid route expires, the route is completely deleted from the RIP routing table. The default value is 120 seconds.

8.3.4 Configuring the RIP Route Redistribution List

Redistribute routes of other protocols to the RIP domain so that RIP can interwork with other routing domains.

Choose **Local Device** > **Routing** > **RIP Settings** > **Advanced** > **Route Redistribution List** , click **Add** , and select the type and administrative distance.

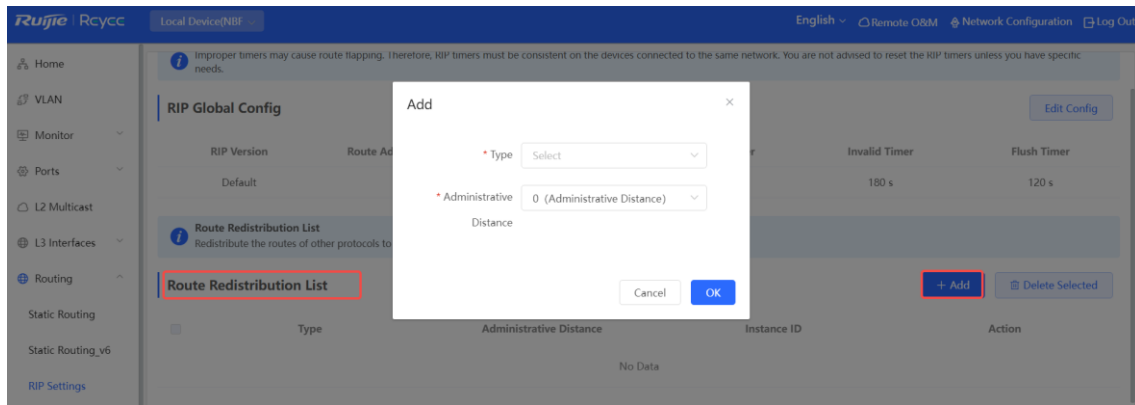
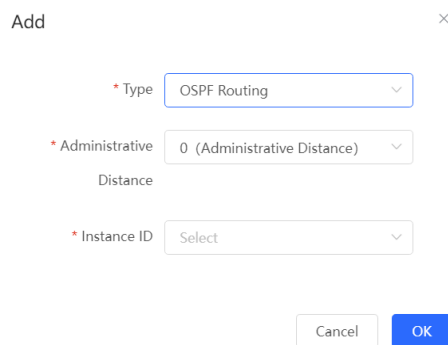


Table 8-6 RIP Route Redistribution on Parameters

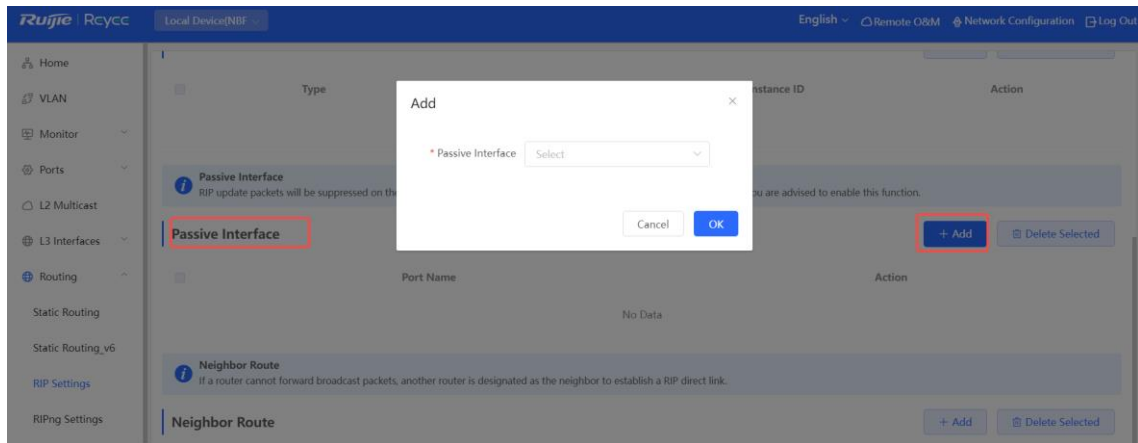
Parameter	Description
Type	Direct Routing OSPF Routing Static Routing
Administrative Distance	A smaller administrative distance indicates a higher priority. The default value is 0 . The value ranges from 0 to 16.
Instance ID	Select the instance ID of OSPF that needs to be redistributed. OSPFv2 needs to be enabled on the local device.



8.3.5 Configuring the Passive Interface

If an interface is configured as a passive interface, it will suppress RIP update packets. If the connected peer device does not run RIP, you are advised to enable the passive interface.

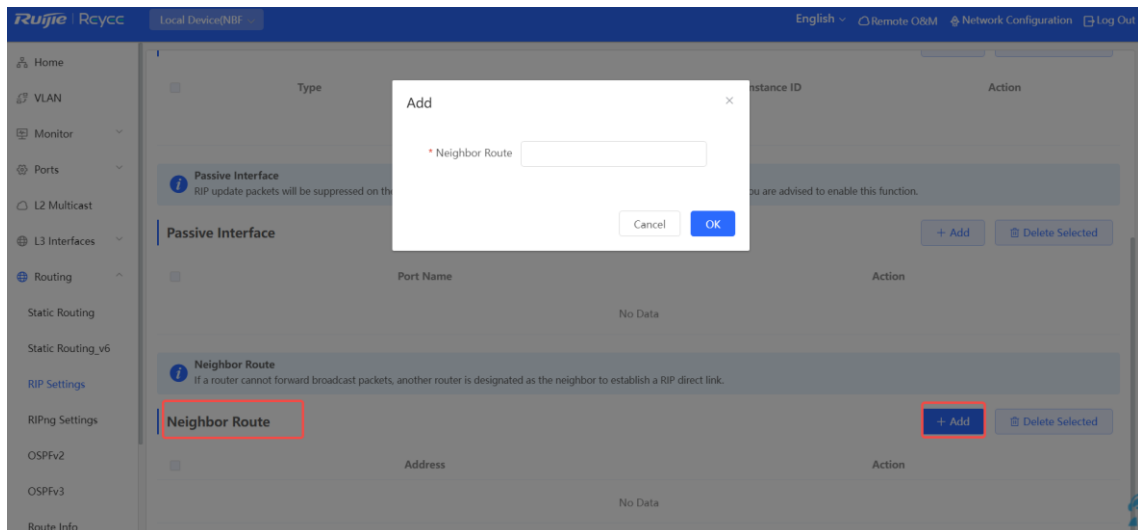
Choose **Local Device > Routing > RIP Settings > Advanced > Passive Interface** , click **Add** , and select a passive interface.



8.3.6 Configuring the Neighbor Route

When the router cannot process broadcast packets, another router can be designated as the neighbor to establish a RIP direct link.

Choose **Local Device > Routing > RIP Settings > Advanced > Neighbor Route**, click **Add**, and enter the IP address of the neighbor router.



8.4 Configuring RIPng

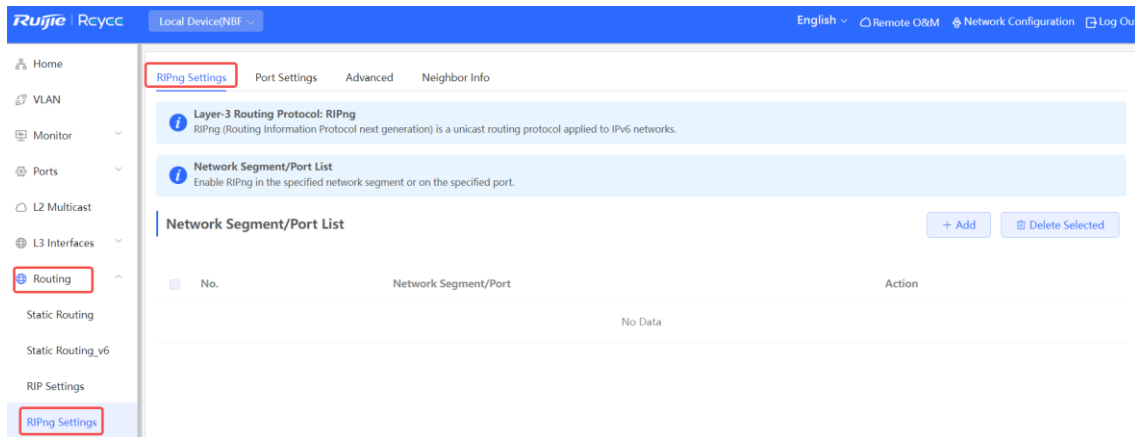
8.4.1 Configuring RIPng Basic Functions

RIP Next Generation (RIPng) provides the routing function for IPv6 networks.

RIPng uses UDP port 512 to exchange the routing information.

Choose **Local Device > Routing > RIPng Settings**.

Click **Add**, set **Type** to **Network Segment** or **Port**, and specify the network segment or port accordingly.

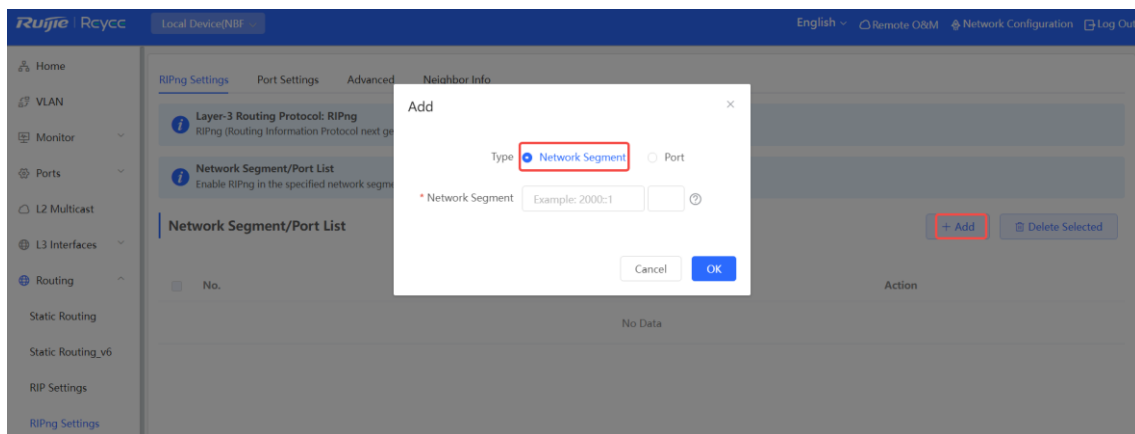


rip.protong

RIPng (Routing Information Protocol next generation) is a unicast routing protocol applied to IPv6 networks.

Network Segment/Port List

Enable RIPng in the specified network segment or on the specified port.



If the address length is between 48 and 64, the address will be used as a prefix.

Alternatively, enable RIPng on a specified port:

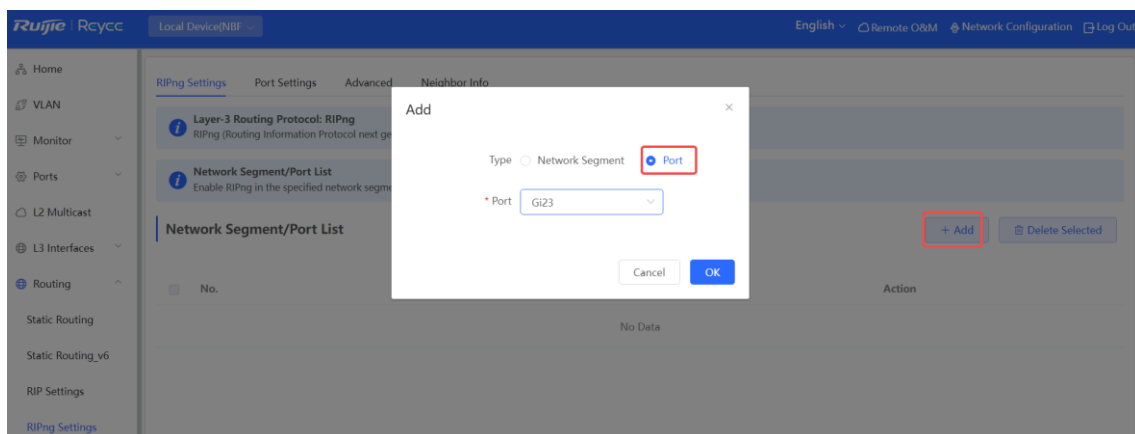


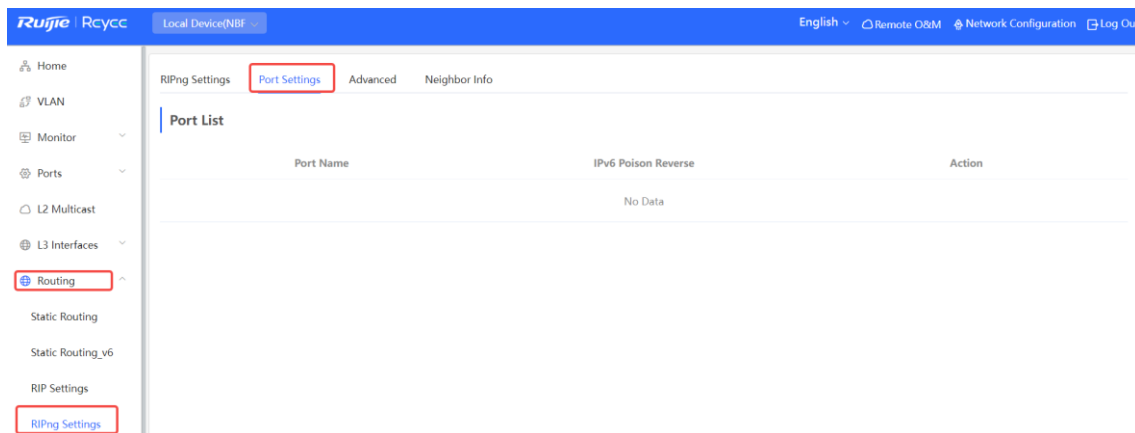
Table 8-7 RIPng Configuration Parameters

Parameter	Description
Type	<p>Network Segment : Enable RIP in the specified network segment. The IP addresses of this network segment are added to the RIP routing table, and the device and its RIP-enabled neighbor devices learn the routing table from each other.</p> <p>Port : Enable RIP on the specified port. All the IP addresses of this port are added to the RIP routing table, and the device and its RIP-enabled neighbor devices learn the routing table from each other.</p>
Network Segment	Enter the IPv6 address and prefix length when Type is set to Network Segment . RIPng will be enabled on all interfaces of the device covered by this network segment.
Port	Select a VLAN interface or physical port when Type is set to Port .

8.4.2 Configuring the RIPng Port

RIPng poison reverse: After the port learns the route, the route overhead is set to **16** (indicating that the route is unreachable), and the route is sent back to the neighbor from the original port to avoid a loop.

Choose **Local Device > Routing > RIPng Settings > Port Settings** , click Edit, and enable IPv6 poison reverse.



Edit ×

* Port Name VLAN 1

IPv6 Poison Reverse

Cancel
OK

8.4.3 Configuring the RIPng Global Configuration

Choose **Local Device > Routing > RIPng Settings > Advanced > RIPng Global Configuration** , and click **Edit Config** .

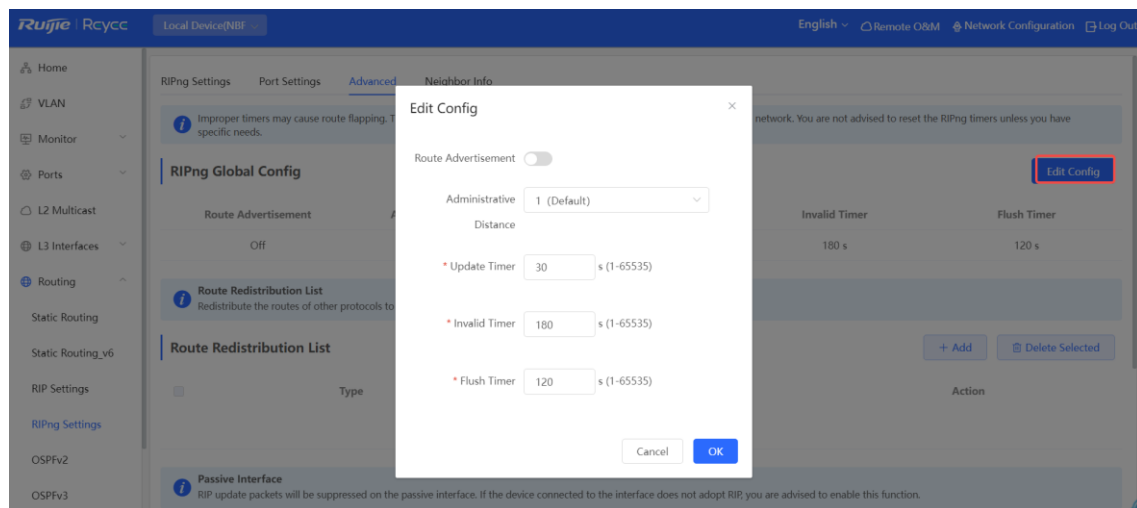
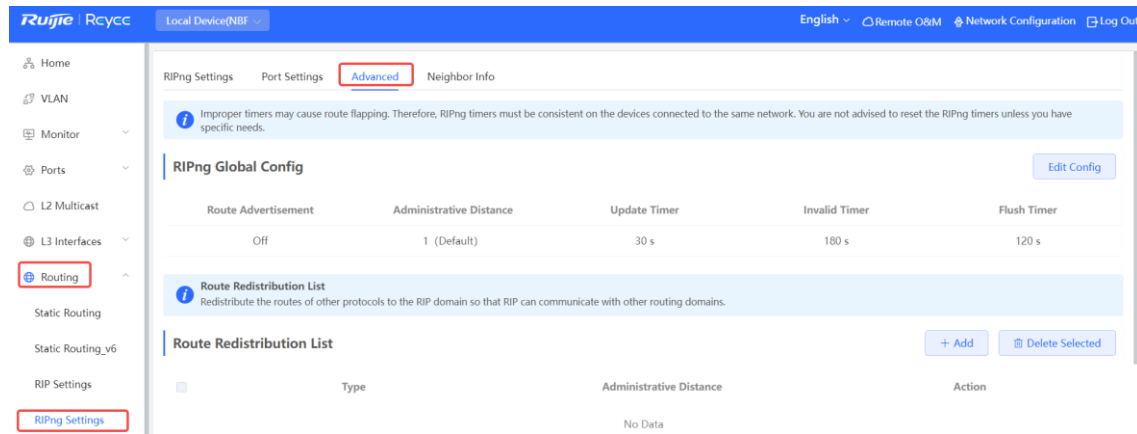


Table 8-8 RIPng Global Configuration Parameters

Parameter	Description
Route Advertisement	After route advertisement is enabled, the current device generates a default route and sends it to the neighbor.
Administrative Distance	Redistribute routes of other protocols to the RIP domain so that RIP can interwork with other routing domains.
Update Timer	RIP update cycle. The routing information is updated every 30 seconds by default.
Invalid Timer	If no update is received before a route becomes invalid, the route is considered unreachable. The default value is 180 seconds.
Flush Timer	If no update is received before the flush timer of an invalid route expires, the

Parameter	Description
	route is completely deleted from the RIP routing table. The default value is 120 seconds.

8.4.4 Configuring the RIPng Route Redistribution List

Redistribute routes of other protocols to the RIPng domain to interwork with other routing domains.

Choose **Local Device > Routing > RIPng Settings > Advanced > Route Redistribution List** , and click **+ Add** .

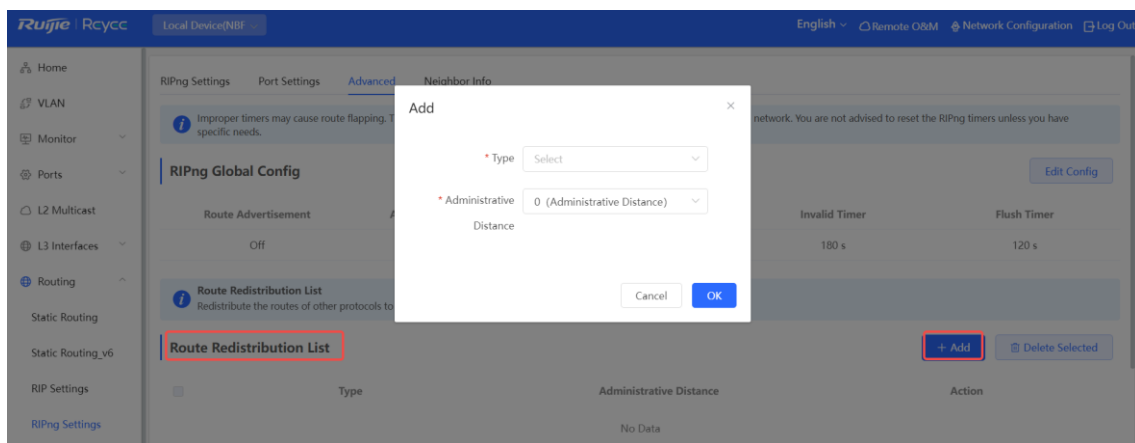


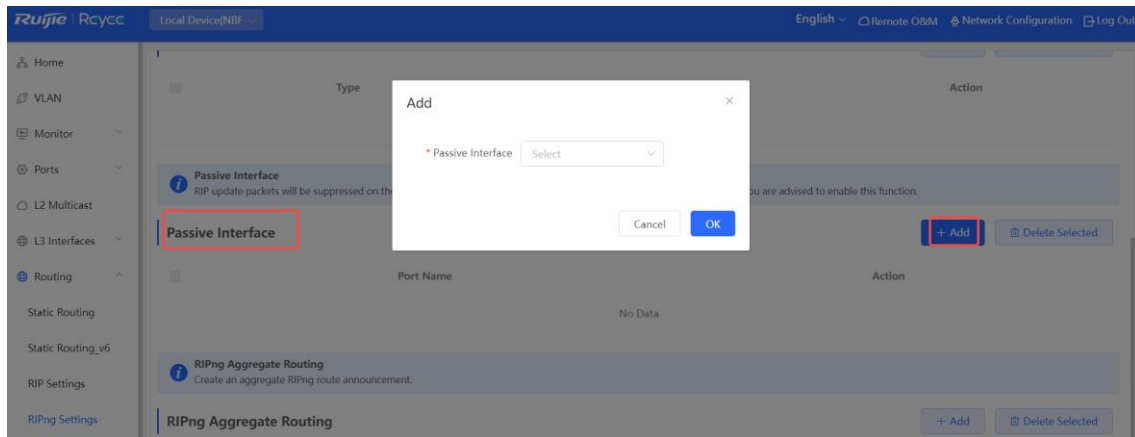
Table 8-9 RIP Route Redistribution Parameters

Parameter	Description
Type	Direct Routing OSPF Routing Static Routing
Administrative Distance	Value range: 0-16. The default value is 0 .

8.4.5 Configuring the RIPng Passive Interface

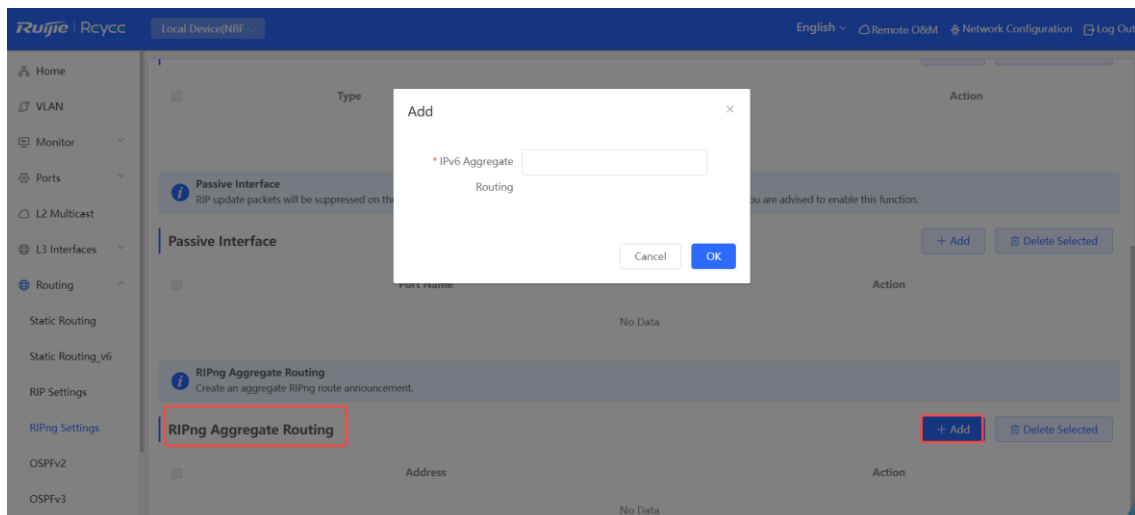
If an interface is configured as a passive interface, it will suppress RIPng update packets. If the connected peer device does not run RIP, you are advised to enable the passive interface.

Choose **Local Device > Routing > RIPng Settings > Advanced > Passive Interface**, click **Add** , and enter the IP address of the neighbor router.



8.4.6 Configuring the IPv6 Aggregate Route

Choose **Local Device > Routing > RIP Settings > Advanced > RIPng Aggregate Route**, click **Add**, and enter the IPv6 address and prefix length (value range: 0–128).



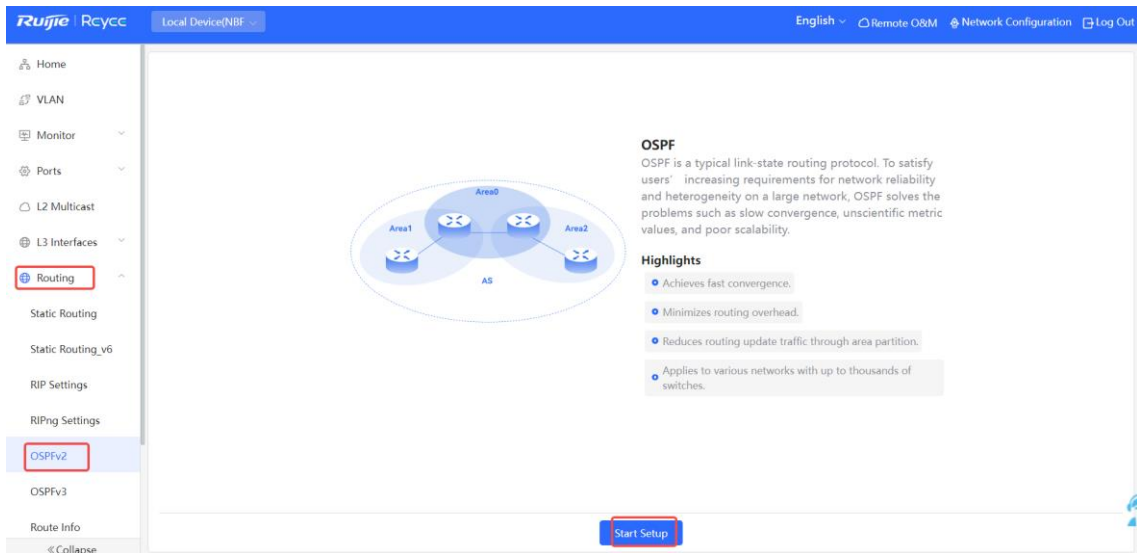
8.5 OSPFv2

Open Shortest Path First (OSPF) can be applied to large-scale networks. IPv4 uses OSPFv2, and IPv6 uses OSPFv3.

OSPF is a typical link-state routing protocol, which can solve the problems of slow route update, inaccurate measurement, and poor scalability in large networks. It is suitable for networks of various sizes, and even a network with up to thousands of devices.

8.5.1 Configuring OSPFv2 Basic Parameters

Choose **Local Device > Routing > OSPFv2**, click **Start Setup**, and then configure an instance and an interface respectively.



(1) Configure an instance.

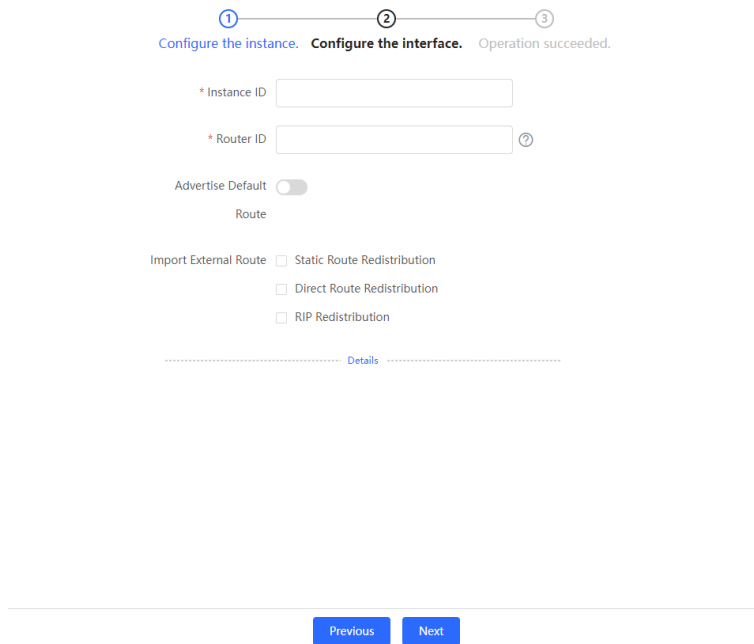


Table 8-10 Instance Configuration Parameters

Parameter	Description
Instance ID	Create an OSPF instance based on the service type. The instance only takes effect locally, and does not affect packet exchange with other devices .
Router ID	It identifies a router in an OSPF domain. <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <p>Caution</p> <p>Router IDs within the same domain must be unique. The same</p> </div>

Parameter	Description
	configuration may cause neighbor discovery failures.
Advertise Default Route	<p>Generate a default route and send it to the neighbor.</p> <p>After this function is enabled, you need to enter the metric and select a type. The default metric is 1 .</p> <p>Type 1: The metrics displayed on different routers vary.</p> <p>Type 2: The metrics displayed on all routers are the same.</p>
Import External Route	<p>Redistribute routes of other protocols to the OSPF domain to interwork with other routing domains.</p> <p>If Static Route Redistribution is selected, enter the metric, which is 20 by default.</p> <p>If Direct Route Redistribution is selected, enter the metric, which is 20 by default.</p> <p>If RIP Redistribution is selected, enter the metric, which is 20 by default.</p>
Details	Expand the detailed configuration.

----- Details -----

Distance

Intra-Area Optional.Default:110

Inter-Area Optional.Default:110

External Optional.Default:110

LSA

Generation Delay Optional.Default

Received Delay Optional.Default

SPF Calculation

Waiting Interval Optional.Default

Min Interval Optional.Default:50

Max Interval Optional.Default:50

Graceful Restart Graceful Restart

Helper

LSA Check

* Max Wait Time 1800

Table 8-11 Parameters in the Instance Detailed Configuration

Parameter	Description
Distance	It is used for protocol selection. By default, the intra-area, inter-area, and external distances are all 110 .
LSA	Frequent network changes and route flapping may occupy too much network bandwidth and device resources. The LSA generation and reception delays are specified in OSPF by default. The default value is 1000 ms.
SPF Calculation	When the link state database (LSDB) changes, OSPF recalculates the shortest path, and sets the interval to prevent frequent network changes from occupying a large number of resources Waiting Interval : When the state changes, the timer is triggered. The delay is calculated for the first time after the timer expires. The default value is 0 ms. Min Interval : As the number of changes increases, the time of each interval will increase according to the algorithm, and the default value is 50 ms. Max Interval : When the calculated interval reaches the maximum interval, the subsequent interval is always equal to the maximum interval. If the time from the last calculation exceeds the maximum interval and the LSDB is not updated, the timer is disabled.
Graceful Restart	Graceful Restart (GR) can avoid route flapping caused by traffic interruption and active/standby board switchover, thus ensuring the stability of key services. Graceful Restart Helper : The Graceful Restart Helper function is enabled when this switch is turned on. LSA Check : LSA packets outside the domain are checked when this switch is turned on. Max Wait Time : Timing starts after the device receives the GR packet from the peer device. If the peer device does not complete GR within Max Wait Time , the device exits the GR Helper mode. The default value is 1800 seconds.

(2) Configure an interface.

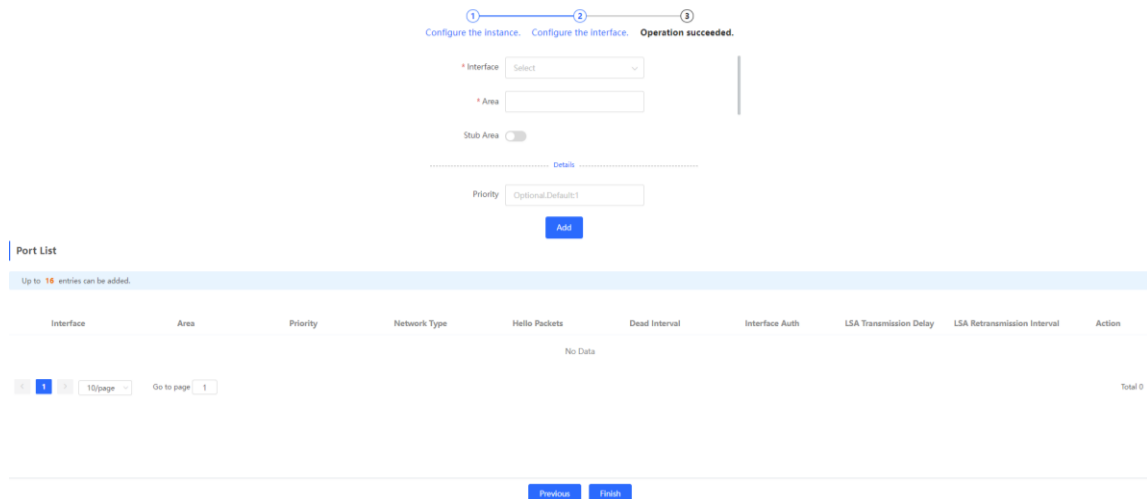
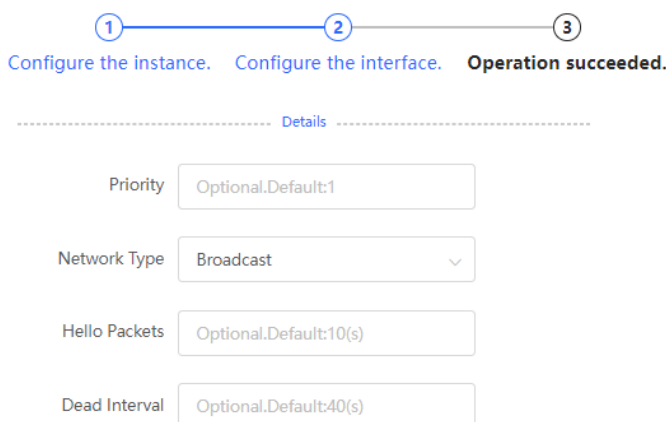


Table 8-12 Interface Configuration Parameters

Parameter	Description
Interface	Select the OSPF-enabled L3 interface.
Area	Configure the area ID. Value range: 0-4294967295
Stub Area	<p>If Stub Area is enabled, you need to configure the area type and inter-area route isolation.</p> <p>Stub area: Routers at the edge of the area do not advertise routes outside the area, and the routing table in the area is small.</p> <p>Not-So-Stubby Area (NSSA): A few external routes can be imported.</p> <p>Inter-area route isolation: After this function is enabled, inter-area routes will not be imported to this area.</p>
Details	Expand the detailed configuration.



LSA Transmission
Delay

LSA Retransmission
Interval

Interface Auth
▼

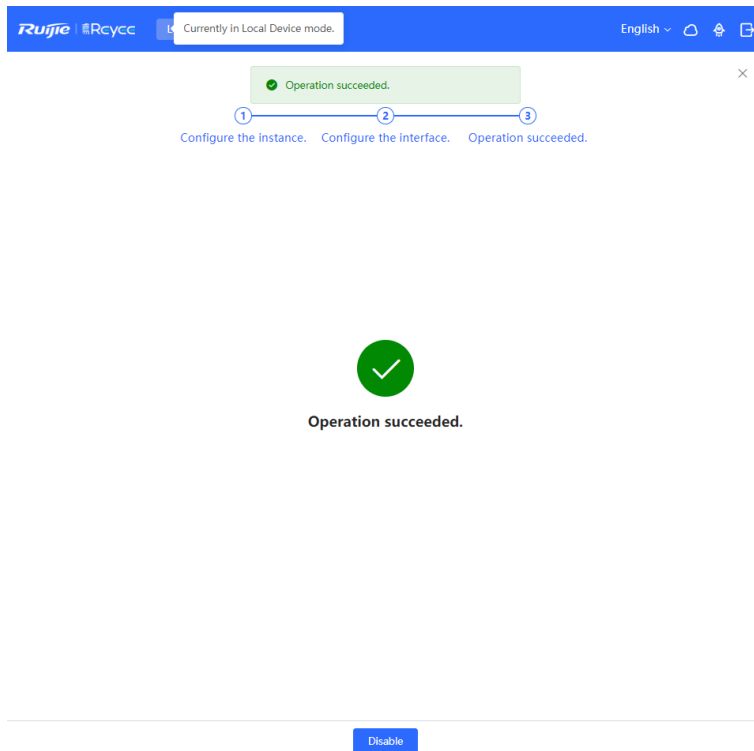
Ignore MTU Check

Table 8-13 Parameters in the Interface Detailed Configuration

Parameter	Description
Priority	It is 1 by default.
Network Type	Broadcast Unicast Multicast Non-Broadcast Multiple Access
Hello Packets	Interval for periodic transmission, which is used to discover and maintain OSPF neighbor relationship. The default value is 10 seconds.
Dead Interval	Time after which the neighbor becomes invalid. The default value is 40 seconds.
LSA Transmission Delay	LSA transmission delay of the interface. The default value is 1 second.
LSA Retransmission Interval	Time after which LSA is retransmitted after LSA is lost. The default value is 5 seconds.
Interface Auth	No Auth : The protocol packets are not authenticated. It is the default value. Plain Text : The protocol packets are authenticated, and the authentication key is transmitted with the protocol packets in the form of plain text. MD5 : The protocol packets are authenticated, and the authentication key is MD5 encrypted and then transmitted with the protocol packets.
Ignore MTU Check	Enabled by default.

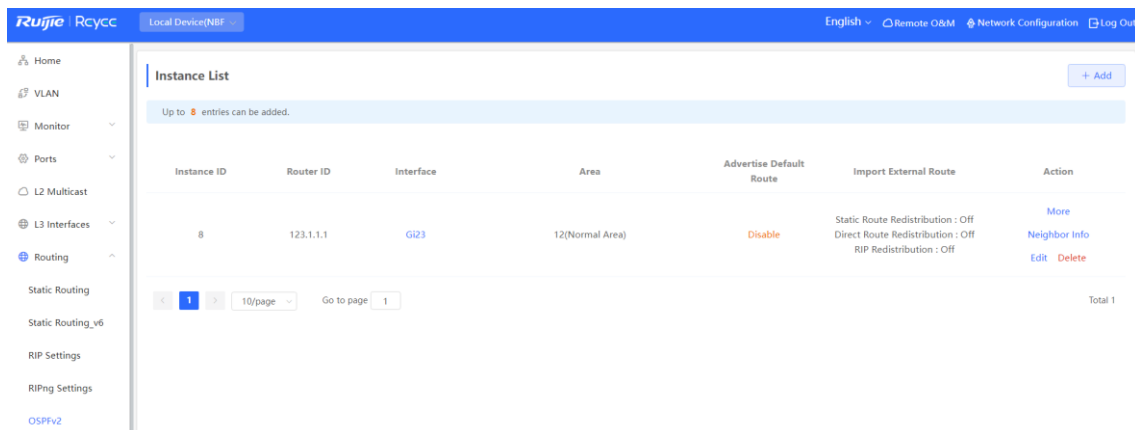
(2) Complete the configuration.

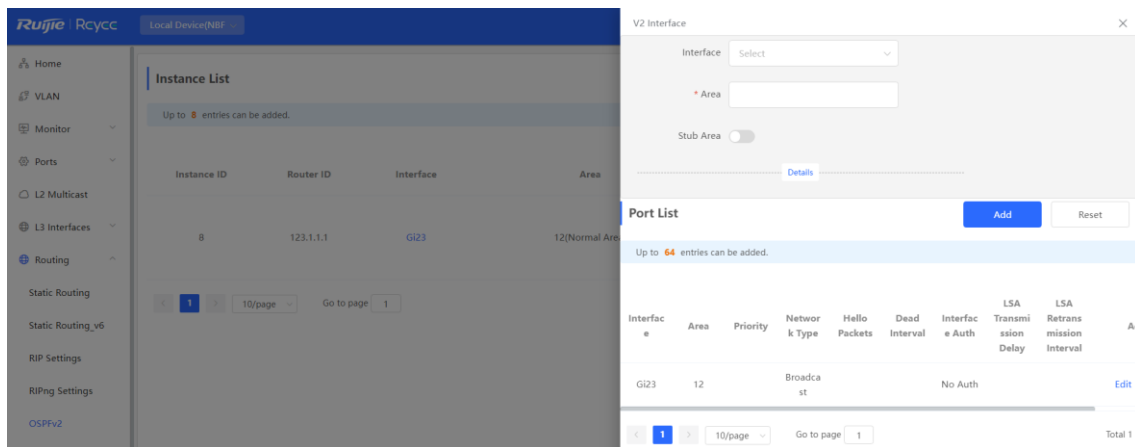
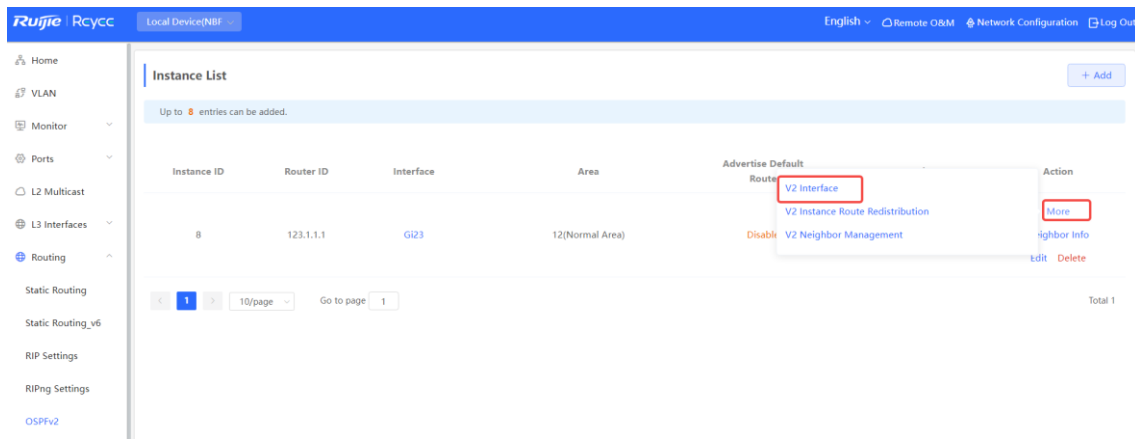
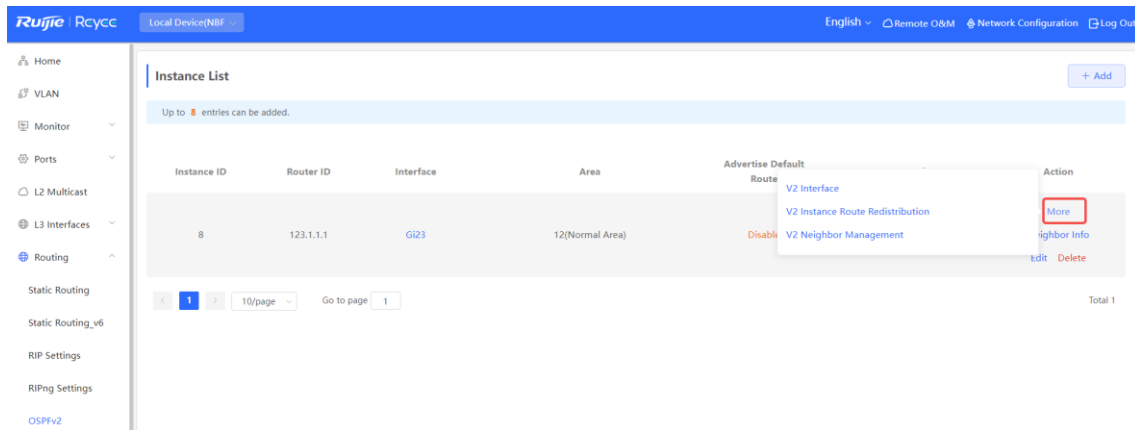
After completing the configuration, you can choose **Local Device > Routing > OSPFv2** and view the instance list.



8.5.2 Adding an OSPFv2 Interface

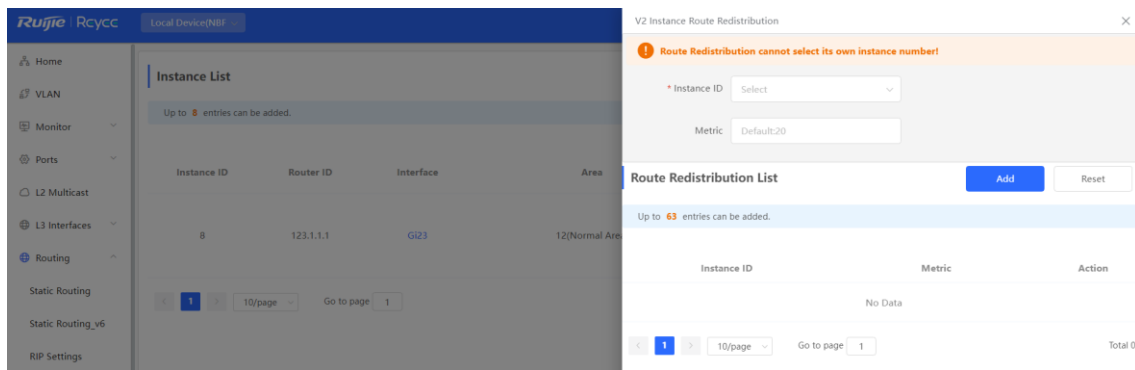
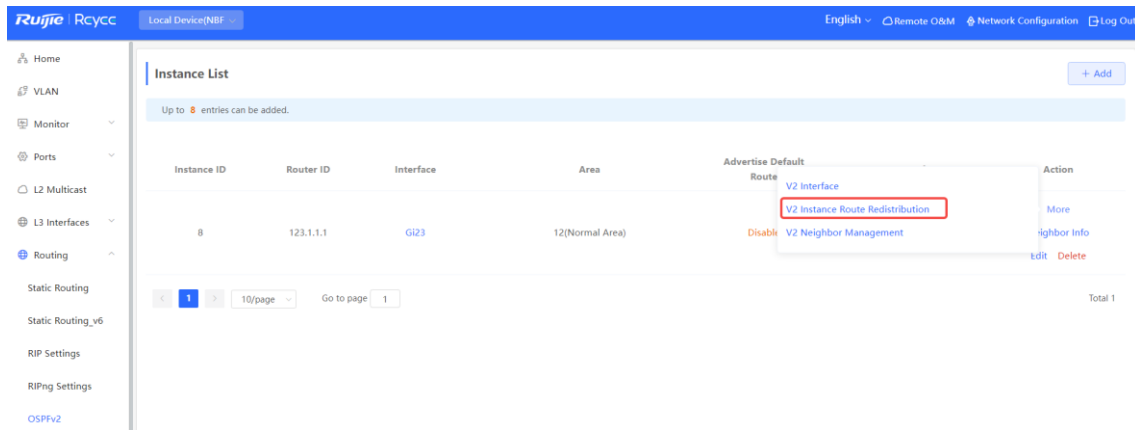
Choose **Local Device > Routing > OSPFv2** , click **More** in the **Action** column, and select **V2 Interface** .





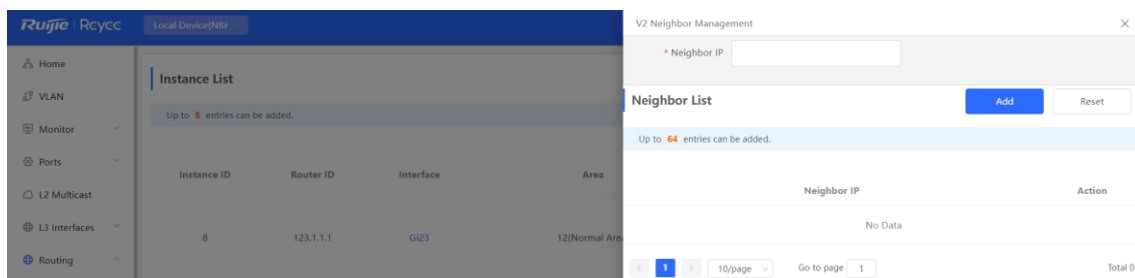
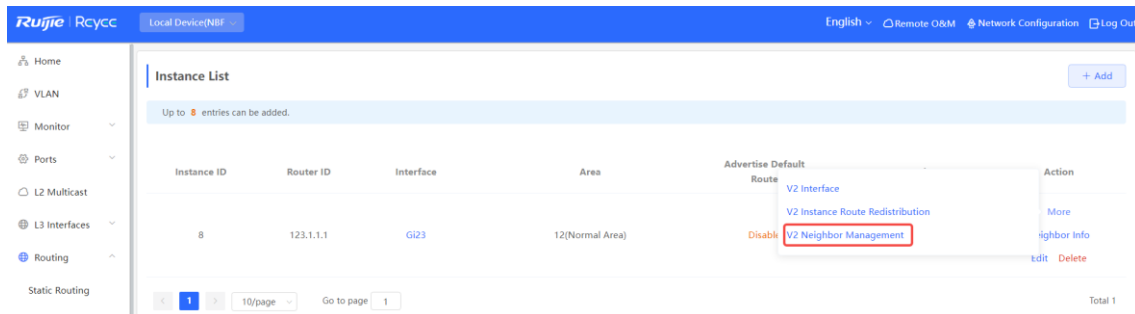
8.5.3 Redistributing OSPFv2 Instance Routes

Choose **Local Device > Routing > OSPFv2** , click **More** in the **Action** column, and select **V2 Instance Route Redistribution** .



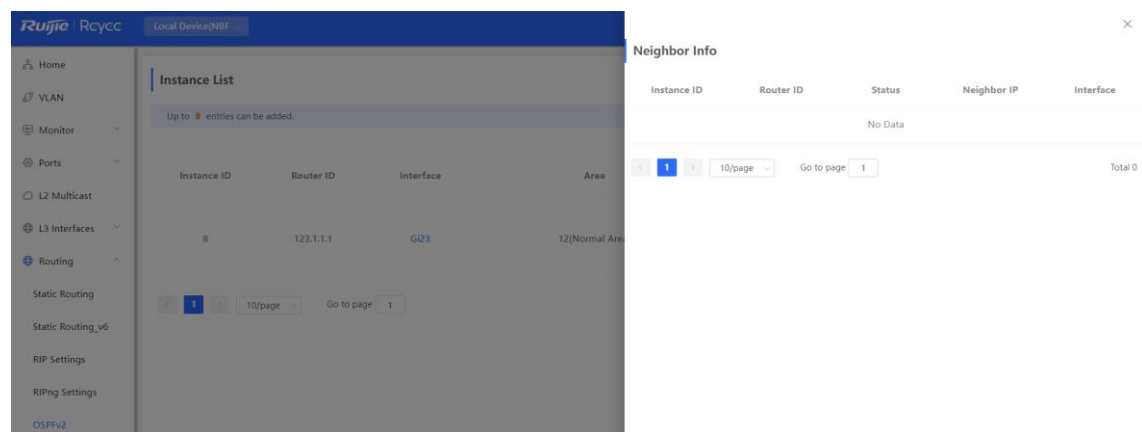
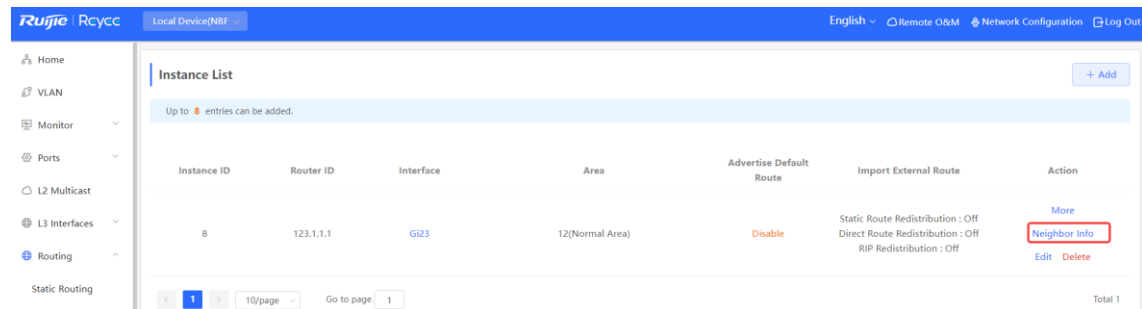
8.5.4 Managing OSPFv2 Neighbors

Choose **Local Device > Routing > OSPFv2** , click **More** in the **Action** column, and select **V2 Neighbor Management** .



8.5.5 Viewing OSPFv2 Neighbor Information

Choose **Local Device > Routing > OSPFv2** , and click **Neighbor Info** in the **Action** column.



8.6 OSPFv3

Open Shortest Path First (OSPF) can be applied to large-scale networks. IPv4 uses OSPFv2, and IPv6 uses OSPFv3.

8.6.1 Configuring OSPFv3 Basic Parameters

Choose **Local Device > Routing > OSPFv3** , click **Start Setup** , and then configure an instance and an interface respectively.

1. Configure an instance.

The screenshot displays the Ruijie Reycs web-based configuration interface. The top navigation bar includes the Ruijie Reycs logo, the device name 'Local Device(NBF)', and options for language (English), remote O&M, network configuration, and log out. The left sidebar contains a navigation menu with categories like Home, VLAN, Monitor, Ports, L2 Multicast, L3 Interfaces, Routing, Static Routing, Static Routing_v6, RIP Settings, RIPng Settings, OSPFv2, and OSPFv3. The 'Routing' and 'OSPFv3' items are highlighted with red boxes. The main content area shows a network diagram of an AS with three areas (Area0, Area1, Area2) and a 'Start Setup' button. Text on the right explains OSPF and lists its highlights.

OSPF
OSPF is a typical link-state routing protocol. To satisfy users' increasing requirements for network reliability and heterogeneity on a large network, OSPF solves the problems such as slow convergence, unscientific metric values, and poor scalability.

Highlights

- Achieves fast convergence.
- Minimizes routing overhead.
- Reduces routing update traffic through area partition.
- Applies to various networks with up to thousands of switches.

- **OSPF**

OSPF is a typical link-state routing protocol. To satisfy users' increasing requirements for network reliability and heterogeneity on a large network, OSPF solves the problems such as slow convergence, unscientific metric values, and poor scalability.

- **Highlights**

Achieves fast convergence.

Minimizes routing overhead.

Reduces routing update traffic through area partition.

Applies to various networks with up to thousands of switches.

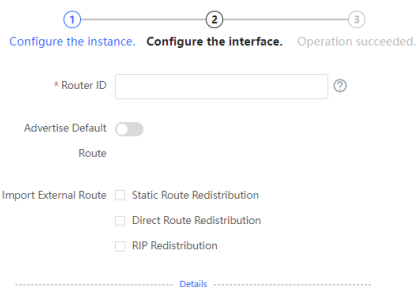


Table 8-14 Instance Configuration Parameters

Parameter	Description
Instance ID	Create an OSPF instance based on the service type. The instance only takes effect locally, and does not affect packet exchange with other devices.
Router ID	It identifies a router in an OSPF domain. <div style="border: 1px solid black; padding: 5px;"> <p> Caution Router IDs within the same domain must be unique. The same configuration may cause neighbor discovery failures.</p> </div>
Advertise Default Route	Generate a default route and send it to the neighbor. After this function is enabled, you need to enter the metric and select a type. The default metric is 1 . Type 1: The metrics displayed on different routers vary. Type 2: The metrics displayed on all routers are the same.
Import External Route	Redistribute routes of other protocols to the OSPF domain to interwork with other routing domains. If Static Route Redistribution is selected, enter the metric, which is 20 by default. If Direct Route Redistribution is selected, enter the metric, which is 20 by default. If RIP Redistribution is selected, enter the metric, which is 20 by default.

Parameter	Description
Details	Expand the detailed configuration.

×

① ————— ② ————— ③

Configure the instance. **Configure the interface.** Operation succeeded.

* Router ID

Advertise Default

Route Metric Type 2

Import External Route Static Route Redistribution
 Metric

Direct Route Redistribution
 Metric

RIP Redistribution
 Metric

----- Details -----

Distance Intra-Area
 Inter-Area
 External

LSA Generation Delay
 Received Delay

Previous Next

×

① ————— ② ————— ③

Configure the instance. **Configure the interface.** Operation succeeded.

Metric

RIP Redistribution
 Metric

----- Details -----

Distance Intra-Area
 Inter-Area
 External

LSA Generation Delay
 Received Delay

SPF Calculation Waiting Interval
 Min Interval
 Max Interval

Graceful Restart Graceful Restart
 Helper
 LSA Check
 * Max Wait Time

Previous Next

Table 8-15 Parameters in the Instance Detailed Configuration

Parameter	Description
Distance	It is used for protocol selection. By default, the intra-area, inter-area, and external distances are all 110 .
LSA	<p>Frequent network changes and route flapping may occupy too much network bandwidth and device resources. The LSA generation and reception delays are specified in OSPF by default.</p> <p>The default value is 1000 ms.</p>
SPF Calculation	<p>When the link state database (LSDB) changes, OSPF recalculates the shortest path, and sets the interval to prevent frequent network changes from occupying a large number of resources</p> <p>Waiting Interval : When the state changes, the timer is triggered. The delay is calculated for the first time after the timer expires. The default value is 0 ms.</p> <p>Min Interval : As the number of changes increases, the time of each interval will increase according to the algorithm, and the default value is 50 ms.</p> <p>Max Interval : When the calculated interval reaches the maximum interval, the subsequent interval is always equal to the maximum interval. If the time from the last calculation exceeds the maximum interval and the LSDB is not updated, the timer is disabled.</p>
Graceful Restart	<p>Graceful Restart (GR) can avoid route flapping caused by traffic interruption and active/standby board switchover, thus ensuring the stability of key services.</p> <p>Graceful Restart Helper : The Graceful Restart Helper function is enabled when this switch is turned on.</p> <p>LSA Check : LSA packets outside the domain are checked when this switch is turned on.</p> <p>Max Wait Time : Timing starts after the device receives the GR packet from the peer device. If the peer device does not complete GR within Max Wait Time , the device exits the GR Helper mode. The default value is 1800 seconds.</p>

2. Configure an interface.

Table 8-16 Interface Configuration Parameters

Parameter	Description
Interface	Select the OSPF-enabled L3 interface.
Area	Configure the area ID. Value range: 0-4294967295
Stub Area	<p>If Stub Area is enabled, you need to configure the area type and inter-area route isolation.</p> <p>Stub area: Routers at the edge of the area do not advertise routes outside the area, and the routing table in the area is small.</p> <p>Not-So-Stubby Area (NSSA): A few external routes can be imported.</p>
Details	Expand the detailed configuration.

×

① ————— ② ————— ③
Configure the instance. Configure the interface. **Operation succeeded.**

..... Details

Priority

Network Type

Hello Packets

Dead Interval

Add

Port List

Up to 16 entries can be added.

Interface	Area	Priority	Network Type	Hello Packets	Dead Interval	LSA Transmission Delay	LSA Retransmission Interval	Action
No Data								

< **1** > 10/page Go to page 1 Total 0

Previous **Finish**

×

① ————— ② ————— ③
Configure the instance. Configure the interface. **Operation succeeded.**

..... Details

LSA Transmission Delay

LSA Retransmission Interval

Ignore MTU Check

Add

Port List

Up to 16 entries can be added.

Interface	Area	Priority	Network Type	Hello Packets	Dead Interval	LSA Transmission Delay	LSA Retransmission Interval	Action
No Data								

< **1** > 10/page Go to page 1 Total 0

Previous **Finish**

×

① — ② — ③
 Configure the instance. Configure the interface. **Operation succeeded.**

LSA Transmission Delay

LSA Retransmission Interval

Ignore MTU Check

Port List

Up to 16 entries can be added.

Interface	Area	Priority	Network Type	Hello Packets	Dead Interval	LSA Transmission Delay	LSA Retransmission Interval	Action
G12/14	12		Broadcast					Delete

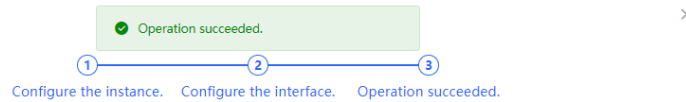
< 1 >
10/page
Go to page 1
Total 1

Table 8-17 Parameters in the Interface Detailed Configuration

Parameter	Description
Priority	It is 1 by default.
Network Type	Broadcast Unicast Multicast Non-Broadcast Multiple Access
Hello Packets	Interval for periodic transmission, which is used to discover and maintain OSPF neighbor relationship. The default value is 10 seconds.
Dead Interval	Time after which the neighbor becomes invalid. The default value is 40 seconds.
LSA Transmission Delay	LSA transmission delay of the interface. The default value is 1 second.
LSA Retransmission Interval	Time after which LSA is retransmitted after LSA is lost. The default value is 5 seconds.
Interface Auth	No Auth : The protocol packets are not authenticated. It is the default value. Plain Text : The protocol packets are authenticated, and the authentication

Parameter	Description
	key is transmitted with the protocol packets in the form of plain text. MD5 : The protocol packets are authenticated, and the authentication key is MD5 encrypted and then transmitted with the protocol packets.
Ignore MTU Check	Enabled by default.

3. Complete the configuration.



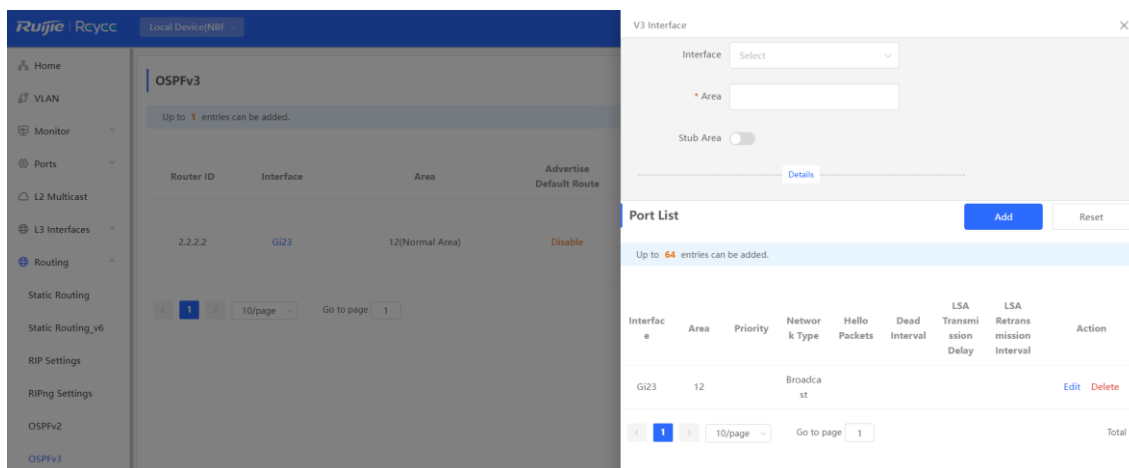
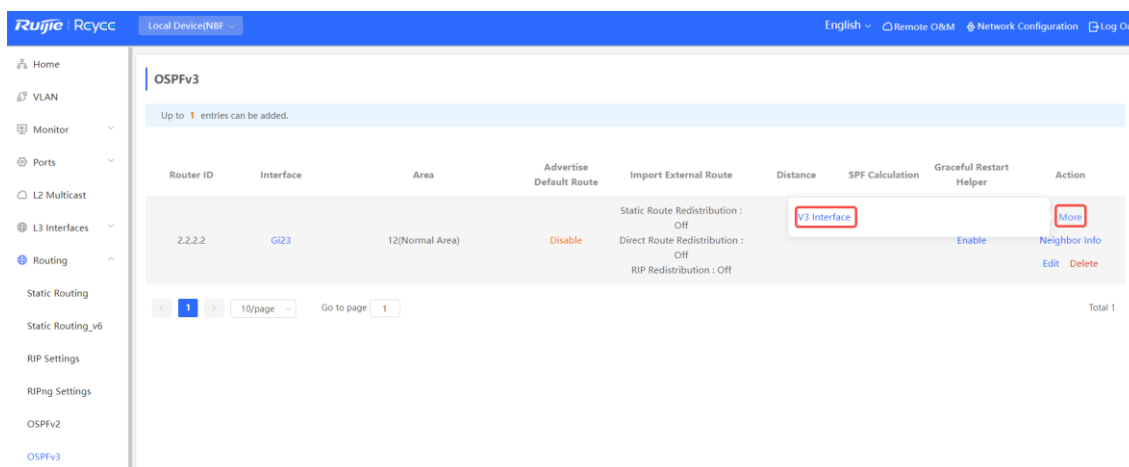
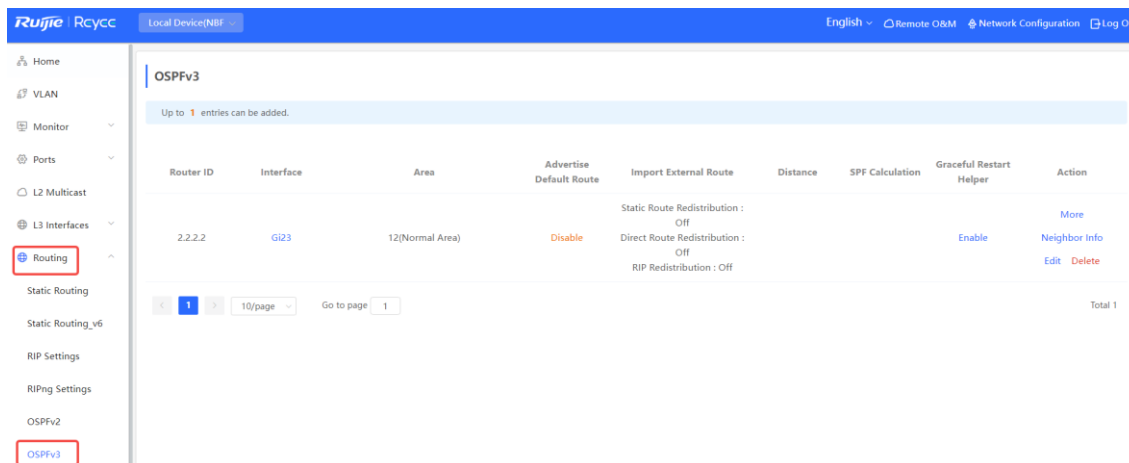
Operation succeeded.

Disable

After completing the configuration, you can choose **Local Device > Routing > OSPFv 3** and view the instance list.

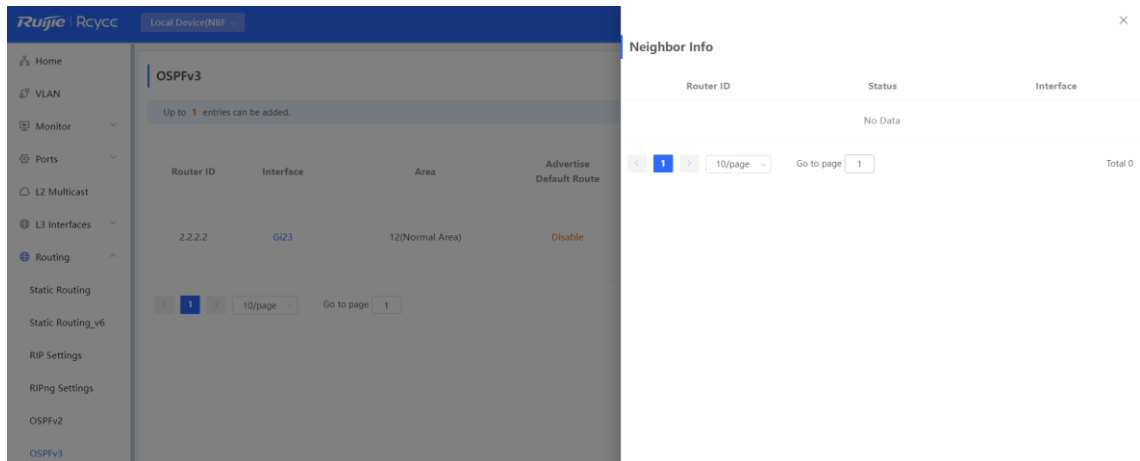
8.6.2 Adding an OSPFv3 Interface

Choose **Local Device > Routing > OSPFv3** , click **More** in the **Action** column, and select **V3 Interface** .



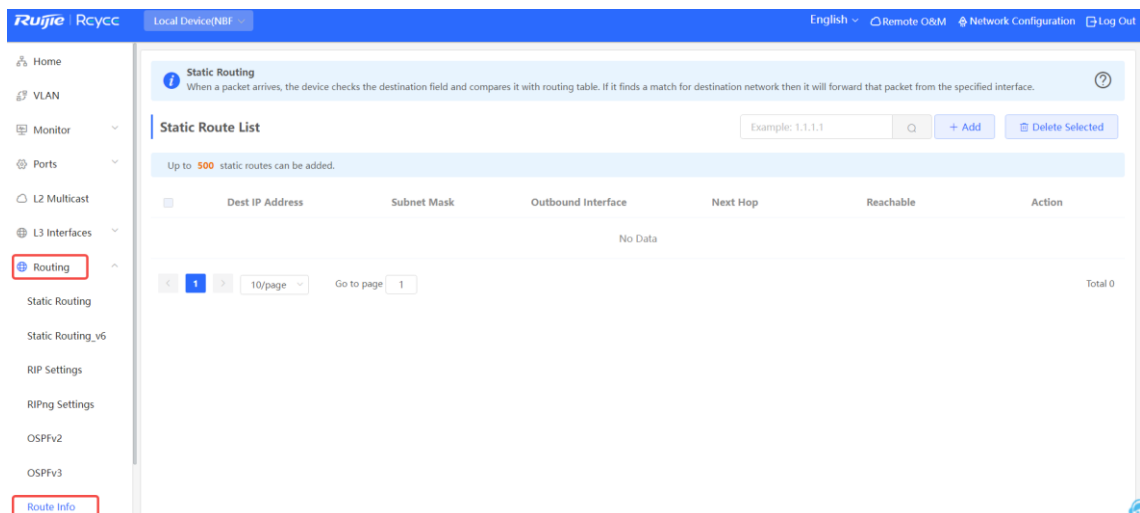
8.6.3 Viewing OSPFv3 Neighbor Information

Choose **Local Device > Routing > OSPFv3** , and click **Neighbor Info** in the **Action** column.



8.7 Routing Table Info

Choose **Local Device > Routing > Route Info**, you can view Static Route List details.



9 Security

9.1 DHCP Snooping

9.1.1 Overview

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

9.1.2 Standalone Device Configuration

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

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

Note

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

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

DHCP Snooping

Description: Enabling DHCP Snooping helps filter DHCP packets. The device only forwards DHCP request packets to the trusted port and DHCP response packets from the trusted port.

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

DHCP Snooping:

Option 82:

Select Trusted Port:

Available Unavailable

Aggregate Uplink Copper Fiber

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49	51
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38	40	42	44	46	48	50	52

Note: You can click and drag to select one or more ports. [Select All](#) [Inverse](#) [Deselect](#)

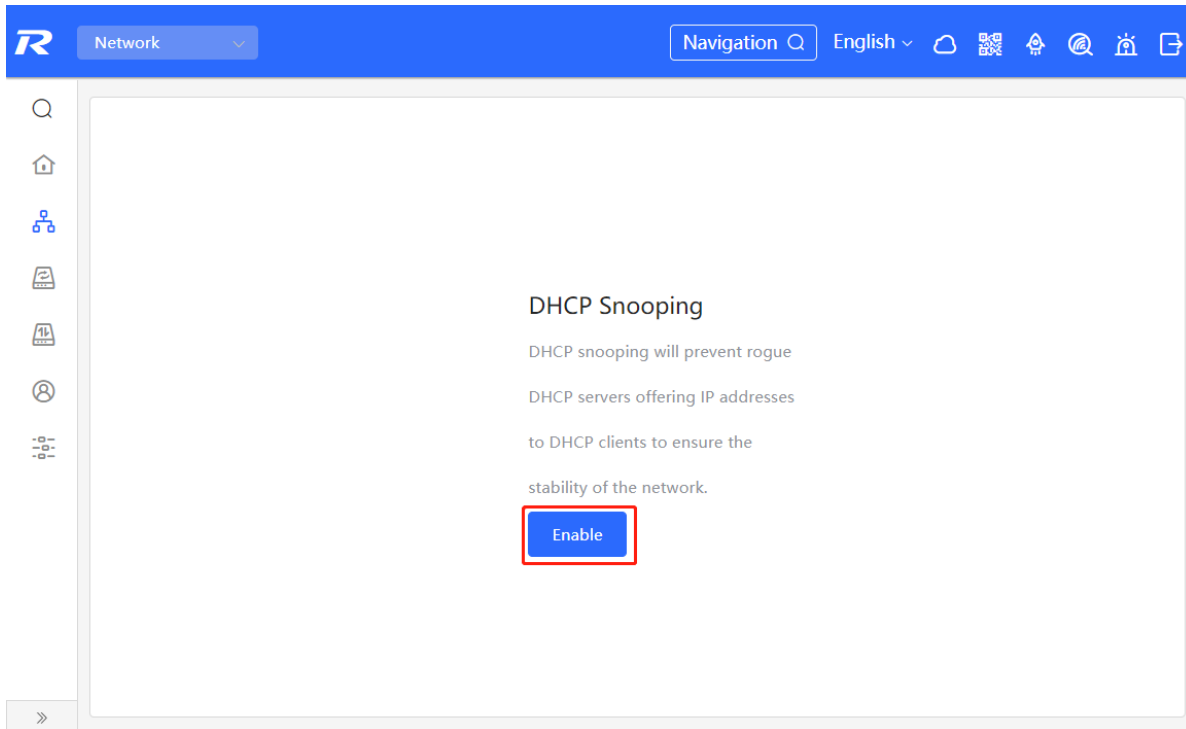
[Save](#)

9.1.3 Batch Configuring Network Switches

Choose **Network > DHCP Snooping** .

Enabling DHCP Snooping on network switches can ensure that users can only obtain network configuration parameters from the DHCP server within the control range, and avoid the occurrence of “the Internet terminal in the original network obtains the IP address assigned by the privately accessed router”, to guarantee the stability of the network.

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



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

← DHCP Snooping Config

Please select the target switch:

Recommended
All Switches

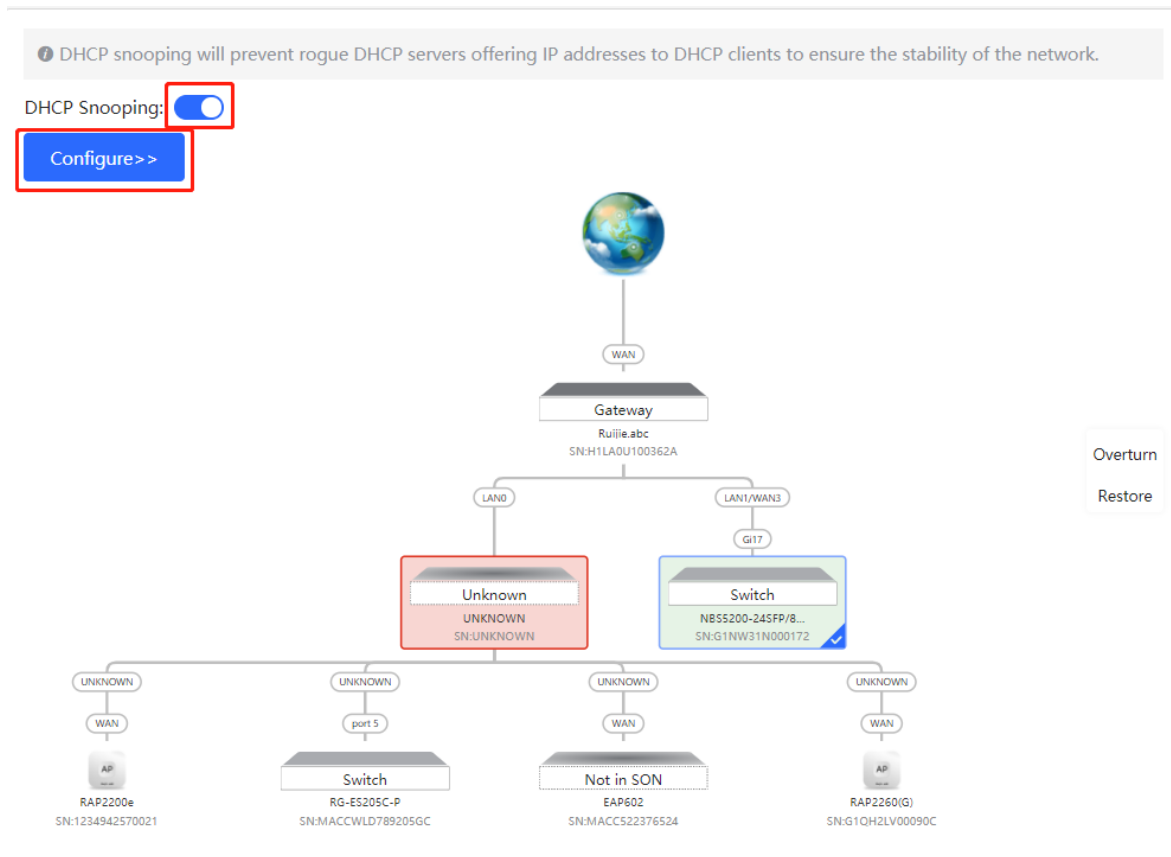
Custom
Specified Switches

Overturn
Restore

1 switches are selected.

Deliver Config Cancel Config

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



9.2 Storm Control

9.2.1 Overview

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

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

9.2.2 Procedure

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

Click **Batch Edit** . In the displayed dialog box, select configuration types and ports, enter the rate limits of broadcast, unknown multicast, and unknown unicast, and click **OK** . To modify or delete the rate limit rules after completing the configuration, you can click **Edit** or **Delete** in the **Action** column.

There are two configuration types:

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

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

Port List					
<input type="checkbox"/>	Port	Broadcast	Unknown Multicast	Unknown Unicast	Action
<input type="checkbox"/>	Gi35	1000pps	1000pps	1000pps	Edit Delete

Batch Edit ×

Broadcast: kbps Range: 16-1000000 (1000M)

Unknown Multicast: kbps Range: 16-1000000 (1000M)

Unknown Unicast: kbps Range: 16-1000000 (1000M)

* Select Port:

Available
 Unavailable
 Aggregate
 Uplink
 Copper
 Fiber

1	3	5	7	9	11
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	4	6	8	10	12
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Note: You can click and drag to select one or more ports. [Select All](#) [Inverse](#) [Deselect](#)

9.3 ACL

9.3.1 Overview

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

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

9.3.2 Creating ACL Rules

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

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

Based on MAC address: To control the L2 packets entering/leaving the port, and deny or permit specific L2 packets destined to a network.

Based on IP address: To control the Ipv4 packets entering/leaving a port, and deny or permit specific Ipv4 packets destined to a network.

- MAC address- based control : Control the incoming and outgoing Layer 2 packets on the port, prohibiting or allowing specific Layer 2 packets to enter the network
- Based on IPv4 address control : Control the incoming and outgoing IPv4 packets on the port, prohibit or allow specific IPv4 packets to enter the network
- Based on IPv6 address control : Control the incoming and outgoing IPv6 packets on the port , prohibit or allow specific IPv6 packets to enter the network

[ACL List](#) [ACL Binding](#)

ACL + Add Delete Selected

Up to **512** entries can be added.

<input type="checkbox"/>	ACL Name	ACL Type	Status	Action
No Data				

Add ×

* ACL Name:

ACL Type: Based on MAC Based on IPv4 Address Based on IPv6 Address

Cancel **OK**

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

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

[ACL List](#) [ACL Binding](#)

ACL + Add Delete Selected

Up to **512** entries can be added.

<input type="checkbox"/>	ACL Name	ACL Type	Status	Action
<input type="checkbox"/>	test	Based on MAC	Inactive	Details Edit Delete

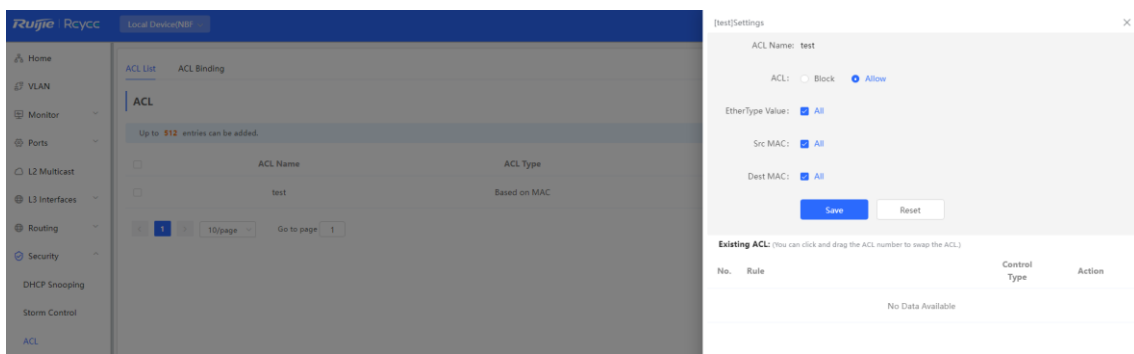


Table 9-1 Description of ACL Rule Configuration Parameters

Parameter	Description
ACL	Configuring ACL Rules Action Block: If packets match this rule, the packets are denied. Allow: If packets match this rule, the packets are permitted.
IP Protocol Number	Match IP protocol number The value ranges from 0 to 255. Check All to match all IP protocols. Applicable to A CL based on "IPv4 address control" and "IPv6 address control" .
Src IP Address	Match the source IP address of the packet. Check All to match all source IP addresses. Applicable to "IPv4 address-based control" and "IPv6 address-based control" A CL.
Dest IP Address	Match the destination IP address of the packet. Check All to match all destination IP addresses applies to ACLs based on "IPv4 address control" and "IPv6 address control" .
EtherType Value	Match Ethernet protocol type. The value range is 0x600~0xFFFF. Check All to match all protocol type numbers. Applicable to A CL based on " MAC address control" .
SrcMac	Match the MAC address of the source host. Check All to match all source MAC addresses applies to A CL based on " MAC address control" .
DEST MAC	Match the MAC address of the destination host. Check All to match all destination MAC addresses applies to A CL based on " MAC address control" .

Note

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

9.3.3 Applying ACL Rules

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

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

Note

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

ACL List ACL Binding

ACL Binding
The device only filters incoming packets.

ACL Binding
+ Batch Add
Unbind Selected

	Port	MAC-based ACL	IP-based ACL	Action
<input type="checkbox"/>	Gi1	--	--	Edit Unbind
<input type="checkbox"/>	Gi2	--	--	Edit Unbind
<input type="checkbox"/>	Gi3	--	--	Edit Unbind
<input type="checkbox"/>	Gi4	--	--	Edit Unbind

Add ×

MAC-based ACL:

IPv4-based ACL:

IPv6-based ACL:

* Select Port:

Available
Unavailable
Aggregate
Uplink
Copper
Fiber

1	3	5	7	9	11
2	4	6	8	10	12

Note: You can click and drag to select one or more ports.

Select All
Inverse
Deselect

Cancel
OK

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

ACL List [ACL Binding](#)

ACL Binding
The device only filters incoming packets.

ACL Binding + Batch Add Unbind Selected

<input type="checkbox"/>	Port	MAC-based ACL	IP-based ACL	Action
<input type="checkbox"/>	Gi1	test	--	Edit Unbind
<input type="checkbox"/>	Gi2	--	--	Edit Unbind

9.4 Port Protection

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

In some scenarios, it is required that communication be disabled between some ports on the device. For this purpose, you can configure some ports as protected ports. Ports that enable port protection (protected ports) cannot communicate with each other, users on different ports are L2-isolated. The protected ports can communicate with non-protected ports.

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

Port Protection
The protected ports are isolated from each other.

Port List Batch Edit

Port	Action
Gi1	☑
Gi2	☐
Gi3	☐
Gi4	☐
Gi5	☐

9.5 IP-MAC Binding

9.5.1 Overview

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

9.5.2 Procedure

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

1. Adding an IP-MAC Binding Entry

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

Caution

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

IP-MAC Binding

Description: IP-MAC Binding checks both the source IP addresses and MAC addresses of IP packets, and packets not matching any entry in the address binding list will be filtered.

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

IP-MAC Binding Search by IP Address

Up to **500** entries can be added.

<input type="checkbox"/>	IP	MAC	Port	Action
<input type="checkbox"/>	192.168.1.1	00:11:22:33:44:55	Gi29	Edit Delete

Add ×

IPv4 Address: ⓘ

MAC Address:

* Select Port:

Available
Unavailable
Aggregate
Uplink
Copper
Fiber

1	3	5	7	9	11
2	4	6	8	10	12

Note: You can click and drag to select one or more ports.

[Select All](#) [Inverse](#) [Deselect](#)

2. Searching Binding Entries

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

Search by IPv4 Address

Search by IPv6 Address
Search by IPv4 Address
 Search by MAC
 Search by Port

Port	Action
------	--------

3. Deleting an IP-MAC Binding Entry

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

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

IP-MAC Binding Search by IP Address

Up to 500 entries can be added.

<input checked="" type="checkbox"/>	IP	MAC	Port	Action
<input checked="" type="checkbox"/>	192.168.1.1	00:11:22:33:44:55	Gi29	Edit <input type="button" value="Delete"/>

9.6 IP Source Guard

9.6.1 Overview

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

Caution

IP Source Guard should be enabled together with DHCP snooping. Otherwise, IP packet forwarding may be affected. To configure DHCP Snooping function, see [7.1](#) for details.

9.6.2 Viewing Binding List

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

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

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

Basic Settings Excluded VLAN **Binding List**

Binding List
 Description: The entries come from dynamic learning of DHCP Snooping.

Search by IP Address

Up to **1900** entries can be added.

IP	MAC	Port	VLAN ID	Status	Rule
No Data					

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

Search by IP Address

- Search by IP Address
- Search by MAC
- Search by VLAN
- Search by Port

IP	MAC	Port	VLAN ID	Status	Rule
No Data					

9.6.3 Enabling Port IP Source Guard

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

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

There are two match rules:

- IP address: The source IP addresses of all IP packets passing through the port are checked. Packets are allowed to pass through the port only when the source IP addresses of these packets match those in the binding list.
- IP address+ MAC address: The source IP addresses and MAC addresses of IP packets passing through the port are checked. Packets are allowed to pass through the port only when both the L2 source MAC addresses and L3 source IP addresses of these packets match an entry in the binding list.

Caution

- IP Source Guard is not supported to be enabled on a DHCP Snooping trusted port.
- Only on an L2 interface is IP Source Guard supported to be enabled.

Basic Settings Excluded VLAN Binding List

Basic Settings
Description: Enable IP Source Guard to check the IP fields or both IP and MAC fields of packets from untrusted ports. Packets not matching any entry in the address binding list will be filtered. It can prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.
Note: IP Source Guard should be enabled together with DHCP Snooping. Otherwise, IP packet forwarding may be affected.

Port List [Batch Edit](#)

Port	Enable	Rule	Action
Gi1	Disabled	IP	Edit
Gi2	Disabled	IP	Edit
Gi3	Disabled	IP	Edit

Edit ×

Enable

Rule

IP

IP+MAC

9.6.4 Configuring Exceptional VLAN Addresses

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

When IP Source Guard is enabled on an interface, it is effective to all the virtual local area networks (VLANs) under the interface by default. Users can specify excluded VLANs, within which IP packets are not checked or filtered, that is, such IP packets are not controlled by IP Source Guard.

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

⚠ Caution

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

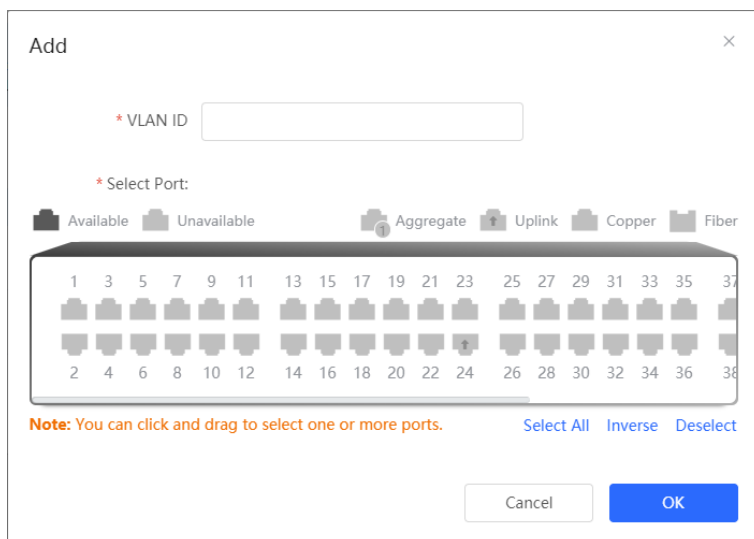
Basic Settings Excluded VLAN Binding List

Excluded VLAN
Description: Packets within this VLAN are allowed to pass the port without checking or filtering.
Note: Excluded VLAN can be specified only after IP Source Guard is enabled on a port.

VLAN List [+ Add](#) [Delete Selected](#)

Up to **64** entries can be added.

<input type="checkbox"/>	VLAN ID	Port	Action
No Data			



9.7 Configure 802.1x authentication

9.7.1 Function introduction

IEEE802.1x (Port -Based Network Access Control) is a port-based network access control standard that provides secure access services for LANs.

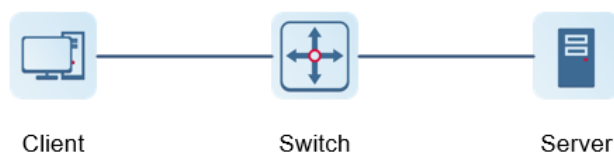
IEEE 802 LAN , as long as users can connect to network devices, they can directly access network resources without authentication and authorization. This uncontrolled behavior will bring security risks to the network. The IEEE 802.1x protocol was proposed to solve the security problem of 802 LAN.

802.1x supports Authentication , Authorization , and Accounting three security applications, referred to as AAA .

- Authentication : Authentication, used to determine whether users can obtain access rights and restrict illegal users;
- Authorization : Authorization, which services authorized users can use, and control the rights of legitimate users;
- Accounting : Accounting, recording the use of network resources by users, and providing a basis for charging.

802.1x can be deployed in a network that controls access users to implement authentication and authorization services for access users.

802.1x system is a typical Client/Server structure, including three entities: client, access device and authentication server. A typical architecture diagram is shown in the figure.



- The client is generally a user terminal device, and the user can initiate 802.1X authentication by starting the

client software. The client must support the Extensible Authentication Protocol over LANs (EAPoL).

- AP or switching device) that supports the 802.1x protocol . It provides a port for the client to access the LAN. The port can be a physical port or a logical port.
- The authentication server is used to implement user authentication, authorization, and accounting, and it is usually a RADIUS server.

Note

RG- NBF switching devices only support the authentication function.

9.7.2 Configuration 802.1x

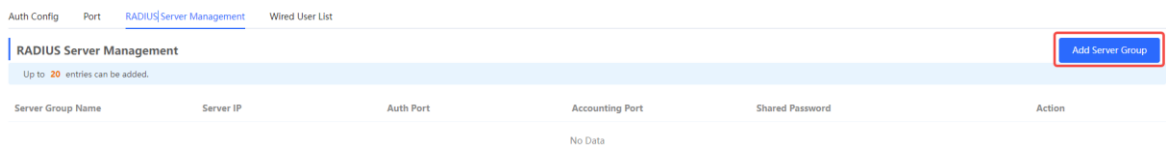
1. Configure Radius server

[Local Management - Page Wizard] Security Management >> 802.1x Certification >> Radius server management

Before configuration, please confirm :

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

(1) Click <Add New Server Group> to add a server group.



Add
×

* Server Group Name

Server 1

* Server IP

* Server Name

* Auth Port

* Accounting Port ?

* Shared Password

* Match Order ?

Add Server

parameter	Reference without translation	illustrate
Server group name		<p>The name of the server group. Multiple servers can be added to each group. If the server with high priority does not respond, it will switch to other servers in matching order.</p> <hr/> <p>i Note</p> <p>This function requires the server detection function to be turned on . See (2) .</p>
Server IP	server address	Radius server address.
Auth Port	authentication port	The port number used for accessing user authentication on the Radius server.
Accounting Port	billing port	The port number used to access the accounting process on the Radius server.
Shared Password	shared password	Radius server shared key.
Match Order	matching order	<p>The system supports adding up to 5 Radius servers.</p> <p>The higher the matching order value is, the higher the priority is.</p>

(2) Set server global configuration and click <Save> .

Server global configuration

* Packet Retransmission Interval s

* Packet Retransmission Count time

Server Detection

MAC Address Format ?

parameter	reference - do not translate	illustrate
Packet Retransmission Interval	packet retransmission interval	Configure the interval for the device to send request packets before confirming that there is no response from RADIUS
Packet Retransmission Count	Packet retransmission times	Configure the number of times the device sends request packets before confirming that there is no response from RADIUS
Server Detection	server detection	If this function is enabled, you need to set "Server Detection Period", "Server Detection Times" and "Server Detection Username". It is used to determine the status of the server, so as to decide whether to enable functions such as escape .
MAC Address Format	M AC address format	Configure the MAC address format of RADIUS attribute No. 31 (Calling- Stationg -ID). The following formats are supported: <ul style="list-style-type: none"> ● Dotted hexadecimal format, such as 00d0.f8aa.bbcc ● IETF format, such as 00-D0-F8-AA-BB-CC ● No format (default) , eg 00d0f8aabbcc

2. Configuration 8 02. 1x Global Configuration

【Local Management - Page Wizard】 Security > 8 02.1x Authentication > Auth Config

(1) Click the " Global 802.1x " switch, the system prompts to confirm whether to enable it, click <Configure>.

[Auth Config](#) Port RADIUS Server Management Wired User List

Global Config

Global 802.1x

Authentication

Auth Server [Edit](#)

[Advanced Settings](#)

Configure

(2) Select a server group.

Global Config

Global 802.1x

Authentication

Server Group [Edit](#)

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

[Auth Config](#) Port RADIUS Server Management Wired User List

Guest Vlan

* EAP-Request Packet

Retransmission Count

* Quiet Period s

Client Packet
* Timeout Duration s

Client Packet
* Timeout Duration s

* EAP-Request Packet s

Interval

parameter	illustrate
Server Escape	If the server disconnection is detected, all users will be allowed to access the Internet
Re-authentication	Require clients to re-authenticate at certain intervals to ensure network security
Guest VLAN	Provide a VLAN for unauthenticated clients to restrict their access
EAP-Request Packet Retransmission Count	Define the number of times the EAP request message will be retransmitted when no response is received, value range: 1- 10 times
Quiet Period	During the authentication process, the idle time between the client and the server does not exchange authentication messages, value range: 0- 65535 seconds
Client Packet Timeout Duration	The time limit for the server to wait for the response from the client. Exceeding this time will be regarded as an authentication failure. Value range: 1-65535 seconds
Client Packet Timeout Duration	The time limit for the client to wait for the server to respond, exceeding this time will be considered as an authentication failure, value range: 1- 65535 seconds
EAP-Request Packet Interval	Define the time interval between sending EAP request messages to control the rate of the authentication process, value range: 1-65535 seconds

3. Configure the effective interface

[Local Management - Page Wizard] Security Management >> 8 02.1x Certification >> Interface configuration
 click interface configuration , click modify or batch configuration after a single interface , and edit the authentication parameters of the interface .

Auth Config Port RADIUS Server Management Wired User List

Port List Batch Config

Interface	Port Authentication	Auth Method	Auth Mode	Action
Gi1	Off	disable	multi-auth	Edit
Gi2	Off	disable	multi-auth	Edit

Edit
×

802.1x Authentication

Auth Method disable ▾


Auth Mode multi-auth ▾

Guest Vlan

* User Count Limit per
Port

Cancel OK

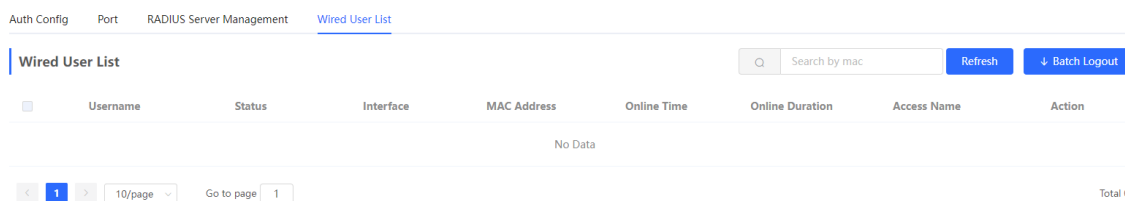
parameter	reference - do not translate	illustrate
802.1x Authentication	802.1x certification	When enabled, the selected interface will enable 8.02.1x authentication .
Auth Method	authentication method	<p>disable : Turn off the authentication method , which has the same effect as turning off the 802.1x authentication switch</p> <p>force- auth : Mandatory authentication , the client can directly access the Internet without a password</p> <p>force- unauth : force no authentication, the client cannot authenticate and cannot access the Internet</p> <p>auto : automatic authentication, the device needs to be authenticated, and can access the Internet after passing the authentication</p> <p>It is recommended to select the auto authentication method .</p>
Auth Mode	authentication mode	<p>multi- auth : Supports multiple devices using the same port for authentication, but each device needs to be authenticated independently</p> <p>multi- host : Multiple devices are allowed to share the same port. As long as one user passes the authentication, subsequent users can access the Internet</p> <p>single-host : Each port only allows one device to be authenticated, and can access the Internet after successful authentication</p>

parameter	reference - do not translate	illustrate
Guest Vlan	Guest VLAN	<p>When enabled, devices that fail authentication will be dynamically assigned to the specified Guest VLAN</p> <hr/> <p> Notice You need to create a VLAN ID first and apply it to the interface , then in Security Management >> 802.1x Authentication >> Advanced settings in the authentication configuration enable Guest VLAN and enter the ID</p> <hr/>
User Count Limit per Port	Maximum number of users per port	Limit the number of users under the interface

9.7.3 View the list of wired authentication users

8.02.1x function is configured on the entire network and a terminal is authenticated and connected to the network, you can view the list of authenticated users.

【Local Management - Page Wizard】 Security Management >> 802.1x Authentication to obtain specific user information.



Click <Refresh> to get the latest user list information.

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

9.8 Anti-ARP Spoofing

9.8.1 Overview

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

9.8.2 Procedure

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

1. Enabling Anti-ARP Spoofing

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

Note

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

Anti-ARP Spoofing

Description: Anti-ARP Spoofing prevents hosts from spoofing the source IP address of the ARP packets to be the IP address of the gateway.
Note: Anti-ARP Spoofing is generally configured on a downlink port.

Anti-ARP Spoofing

Up to **256** entries can be added.

	IP	Port	Action
No Data			

Add ×

* IP

* Select Port:

Available
Unavailable
Aggregate
Uplink
Copper
Fiber

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38

Note: You can click and drag to select one or more ports.
[Select All](#)
[Inverse](#)
[Deselect](#)

2. Disabling Anti-ARP Spoofing

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

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

Anti-ARP Spoofing
Description: Anti-ARP Spoofing prevents hosts from spoofing the source IP address of the ARP packets to be the IP address of the gateway.
Note: Anti-ARP Spoofing is generally configured on a downlink port.

Anti-ARP Spoofing Add Delete Selected

Up to 256 entries can be added.

<input checked="" type="checkbox"/>	IP	Port	Action
<input checked="" type="checkbox"/>	172.30.102.1	Gi15	Edit Delete

10 Advanced Configuration

10.1 STP

STP (Spanning Tree Protocol) is an L2 management protocol that eliminates L2 loops by selectively blocking redundant links in the network. It also provides the link backup function.

[STP Settings](#) STP Management

Note: Enabling STP or changing the STP mode will initiate a new session. Please do not refresh the page.

STP:

* Priority: * Hello Time: seconds

* Max Age: seconds * Forward Delay: seconds

* Recovery Time: seconds STP Mode:

i

10.1.1 STP Global Settings

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

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

⚠ Caution

Enabling the STP or changing the STP mode will initiate a new session. Do not refresh the page during the configuration.

[STP Settings](#) STP Management

Note: Enabling STP or changing the STP mode will initiate a new session. Please do not refresh the page.

STP:

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

Note: Enabling STP or changing the STP mode will initiate a new session. Please do not refresh the page.

STP:

* Priority: seconds

* Hello Time: seconds

* Max Age: seconds

* Forward Delay: seconds

* Recovery Time: seconds

STP Mode:

Save

Table 10-1 Description of STP Global Configuration Parameters

Parameter	Description	Default Value
STP	Whether to enable the STP function. It takes effect globally. STP attributes can be configured only after STP is enabled.	Disable
Priority	Bridge priority. The device compares the bridge priority first during root bridge selection. A smaller value indicates a higher priority.	32768
Max Age	The maximum expiration time of BPDUs. The packets expiring will be discarded. If a non-root bridge fails to receive a BPDU from the root bridge before the aging time expires, the root bridge or the link to the root bridge is deemed as faulty.	20 seconds
Recovery Time	Network recovery time when redundant links occur on the network.	30 seconds
Hello Time	Interval for sending two adjacent BPDUs	2 seconds
Forward Delay	The interval at which the port status changes, that is, the interval for the port to change from Listening to Learning, or from Learning to Forwarding.	15 seconds
STP Mode	The versions of Spanning Tree Protocol. Currently the device supports STP (Spanning Tree Protocol) and RSTP (Rapid Spanning Tree Protocol).	RSTP

10.1.2 Applying STP to a Port

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

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

STP Port Settings
 Tip: It is recommended to enable the port connected to a PC with Port Fast.

Port List Refresh Batch Edit

Port	Role	Status	Priority	Link Status		BPDU Guard	Port Fast	Action
				Config Status	Actual Status			
Gi1	disable	disable	128	Auto	Shared	Disable	Disable	Edit
Gi2	disable	disable	128	Auto	Shared	Disable	Disable	Edit
Gi3	disable	disable	128	Auto	Shared	Disable	Disable	Edit

Port:Gi1 ✕

Port Fast:

BPDU Guard:

Link Status:

* Priority:

Cancel

Table 10-2 Description of STP Configuration Parameters of Ports

Parameter	Description	Default Value
Role	<ul style="list-style-type: none"> ● Root: A port with the shortest path to the root ● Alternate: A backup port of a root port. Once the root port fails, the alternate port becomes the root port immediately. ● Designated (designated ports): A port that connects a root bridge or an upstream bridge to a downstream device. ● Disable (blocked ports): Ports that have no effect in the spanning tree. 	NA

Parameter	Description	Default Value
Status	<ul style="list-style-type: none"> ● Disable: The port is closed manually or due to a fault, does not participate in spanning tree and does not forward data, and can be turned into a blocking state after initialization or opening. ● Blocking: A port in the blocking state cannot forward data packets or learn addresses, but can send or receive configuration BPDUs and send them to the CPU. ● Listening: If a port can become the root port or designated port, the port will enter the listening state. Listening : A port in the listening state does not forward data or learn addresses, but can receive and send configuration BPDUs. ● Learning : A port in the learning state cannot forward data, but starts to learn addresses, and can receive, process, and send configuration BPDUs. ● Forwarding : Once a port enters the state, it can forward any data, learn addresses, and receive, process, and send configuration BPDUs. 	NA
Priority	The priority of the port is used to elect the port role, and the port with high priority is preferentially selected to enter the forwarding state	128
Link Status Config Status	Configure the link type, the options include: Shared, Point-to-Point and Auto. In auto mode, the interface type is determined based on the duplex mode. For full-duplex ports, the interface type is point-to-point, and for half-duplex ports, the interface type is shared.	Auto
Link Status Actual Status	Actual link type: Shared, Point-to-Point	NA
BPDU Guard	Whether to enable the BPDU guard function. After the function is enabled, if Port Fast is enabled on a port or the port is automatically identified as an edge port connected to an endpoint, but the port receives BPDUs, the port will be disabled and enters the Error-disabled state. This indicates that an unauthorized user may add a network device to the network, resulting in network topology change.	Disable
Port Fast	Whether to enable the Port Fast function. After Port Fast is enabled on a port, the port will neither receive nor send BPDUs. In this case, the host directly connected to the port cannot receive BPDUs. If a port, on which Port Fast is enabled exits the Port Fast state automatically when it receives BPDUs, the BPDU filter feature is automatically disabled. Generally, the port connected to a PC is enabled with Port Fast.	Disable

Note

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

10.2 LLDP

10.2.1 Overview

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

10.2.2 LLDP Global Settings

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

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

LLDP Settings LLDP Management LLDP Info



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

LLDP Settings LLDP Management LLDP Info

LLDP:

* Hold Multiplier: * Reinitialization Delay: seconds

* Transmit Interval: seconds * Forward Delay: seconds

* Fast Count:

Table 10-3 Description of LLDP Global Configuration Parameters

Parameter	Description	Default Value
LLDP	Indicates whether the LLDP function is enabled.	Enable

Parameter	Description	Default Value
Hold Multiplier	TTL multiplier of LLDP In LLDP packets, TTL TLV indicates the TTL of local information on a neighbor. The value of TTL TLV is calculated using the following formula: $TTL\ TLV = TTL\ multiplier \times Packet\ transmission\ interval + 1$. The TTL TLV value can be modified by configuring the TTL multiplier and LLDP packet transmission interval.	4
Transmit Interval	Transmission interval of LLDP packets, in seconds The value of TTL TLV is calculated using the following formula: $TTL\ TLV = TTL\ multiplier \times Packet\ transmission\ interval + 1$. The TTL TLV value can be modified by configuring the TTL multiplier and LLDP packet transmission interval.	30 seconds
Fast Count	Number of packets that are transmitted rapidly When a new neighbor is discovered, or the LLDP working mode is changed, the device will start the fast transmission mechanism in order to let the neighboring devices learn the information of the device as soon as possible. The fast transmission mechanism shortens the LLDP packet transmission interval to 1s, sends a certain number of LLDP packets continuously, and then restores the normal transmission interval. You can configure the number of LLDP packets that can be transmitted rapidly for the fast transmission mechanism.	3
Reinitialization Delay	Port initialization delay, in seconds You can configure an initialization delay to prevent frequent initialization of the state machine caused by frequent changes of the port work mode.	2 seconds
Forward Delay	Delay for sending LLDP packets, in seconds. When local information of a device changes, the device immediately transmits LLDP packets to its neighbors. You can configure a transmission delay to prevent frequent transmission of LLDP packets caused by frequent changes of local information. If the delay is set to a very small value, frequent change of the local information will cause frequent transmission of LLDP packets. If the delay is set to a very large value, no LLDP packet may be transmitted even if local information is changed. Set an appropriate delay according to actual conditions.	2 seconds

10.2.3 Applying LLDP to a Port

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

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

Send LLDPDU : After **Send LLDPDU** is enabled on a port, the port can send LLDPDUs.

Receive LLDPDU : After **Receive LLDPDU** is enabled on a port, the port can receive LLDPDUs.

LLDPMED : After **LLDPMED** is enabled, the device is capable of discovering neighbors when its peer endpoint supports LLDP-MED (the Link Layer Discovery Protocol-Media Endpoint Discovery).

LLDP Settings [LLDP Management](#) LLDP Info

Port List ↶ Batch Edit				
Port	Send LLDPDU	Receive LLDPDU	LLDP-MED	Action
Gi1	Enable	Enable	Enable	Edit
Gi2	Enable	Enable	Enable	Edit
Gi3	Enable	Enable	Enable	Edit

Batch Edit ✕

Send LLDPDU:

Receive LLDPDU:

LLDP-MED:

* Select Port:

Available Unavailable
Uplink Copper Fiber

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38
<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Note: You can click and drag to select one or more ports. [Select All](#) [Inverse](#) [Deselect](#)

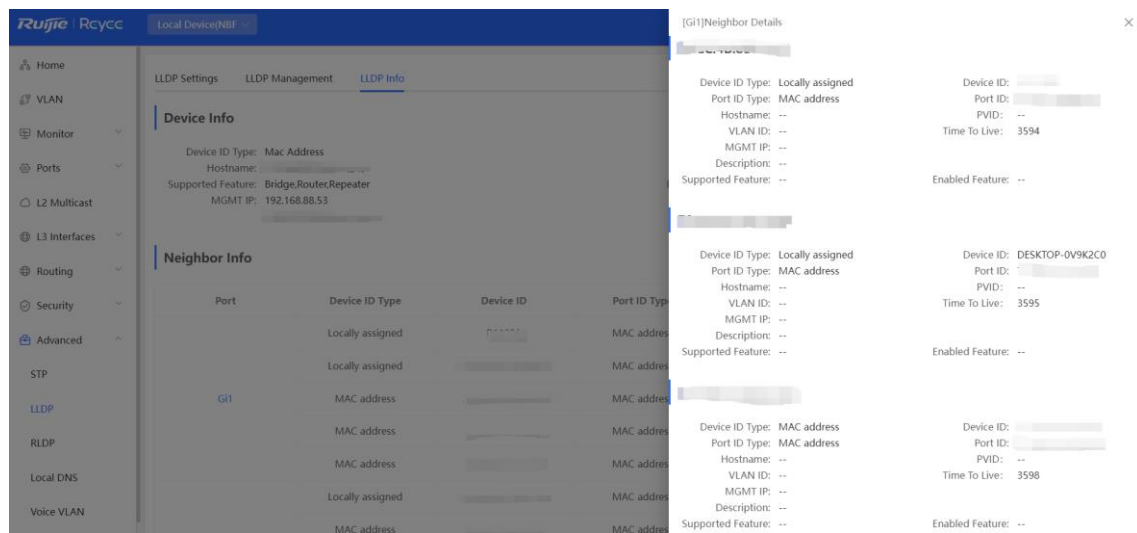
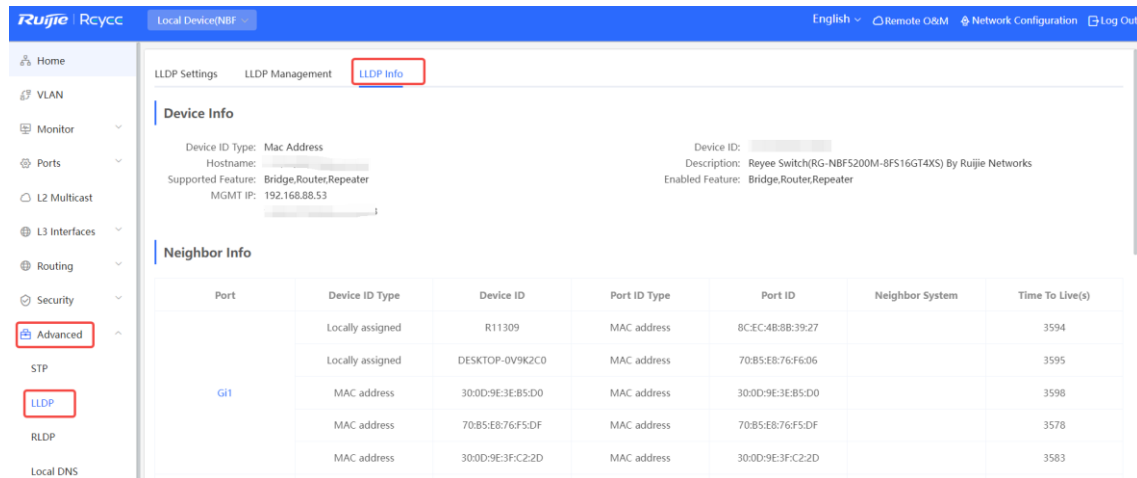
10.2.4 Displaying LLDP information

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

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

You can check the topology connection through LLDP information, or use LLDP to detect errors. For example, if two switch devices are directly connected in the network topology. When an administrator configures the VLAN,

port rate, duplex mode, an error will be prompted if the configurations do not match those on the connected neighbor.



10.3 RLDP

10.3.1 Overview

The Rapid Link Detection Protocol (RLDP) is an Ethernet link failure detection protocol, which is used to rapidly detect unidirectional link failures, bidirectional link failures, and downlink loop failures. When a failure is found, RLDP automatically shuts down relevant ports or asks users to manually shut down the ports according to the configured failure handling methods, to avoid wrong forwarding of traffic or Ethernet L2 loops.

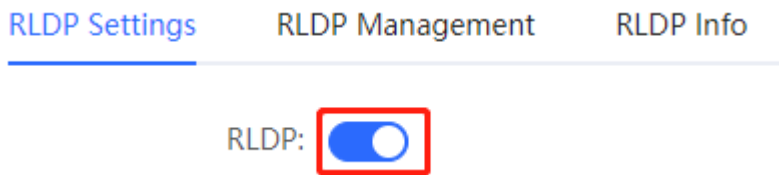
Supports enabling the RLDP function of the access switches in the network in a batch. By default, the switch ports will be automatically shut down when a loop occurs. You can also set a single switch to configure whether loop detection is enabled on each port and the handling methods after a link fault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

10.3.2 Standalone Device Configuration

1. RLDP Global Settings

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

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



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

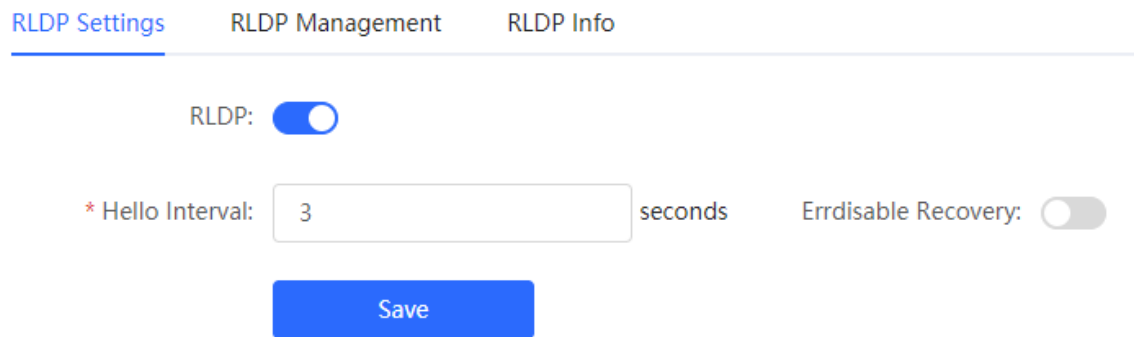


Table 10-4 Description of RLDP Global Configuration Parameters

Parameter	Description	Default Value
RLDP	Indicates whether the RLDP function is enabled.	Disable
Hello Interval	Interval for RLDP to send detection packets, in seconds	3 seconds
Errdisable Recovery	After it is enabled, a port automatically recovers to the initialized state after a loop occurs.	Disable
Errdisable Recovery Interval	The interval at which the failed ports recover to the initialized state regularly and link detection is restarted, in seconds.	30 seconds

2. Applying RLDP to a Port

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

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

There are three methods to handle port failures:

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

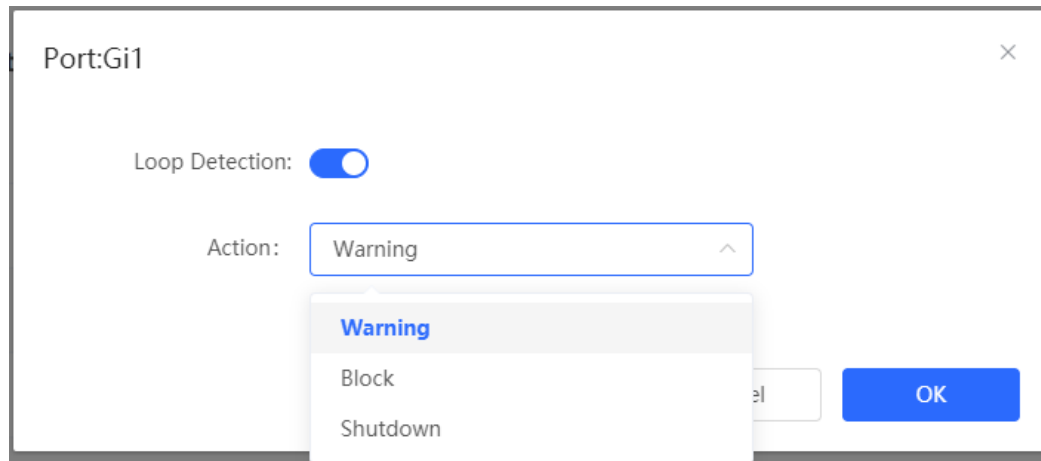
Caution

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

RLDP Settings RLDP Management RLDP Info

Port List Batch Edit

Port	Loop Detection	Action	Action
Gi1	Disable	--	Edit
Gi2	Disable	--	Edit
Gi3	Disable	--	Edit



3. Displaying RLDP information

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

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

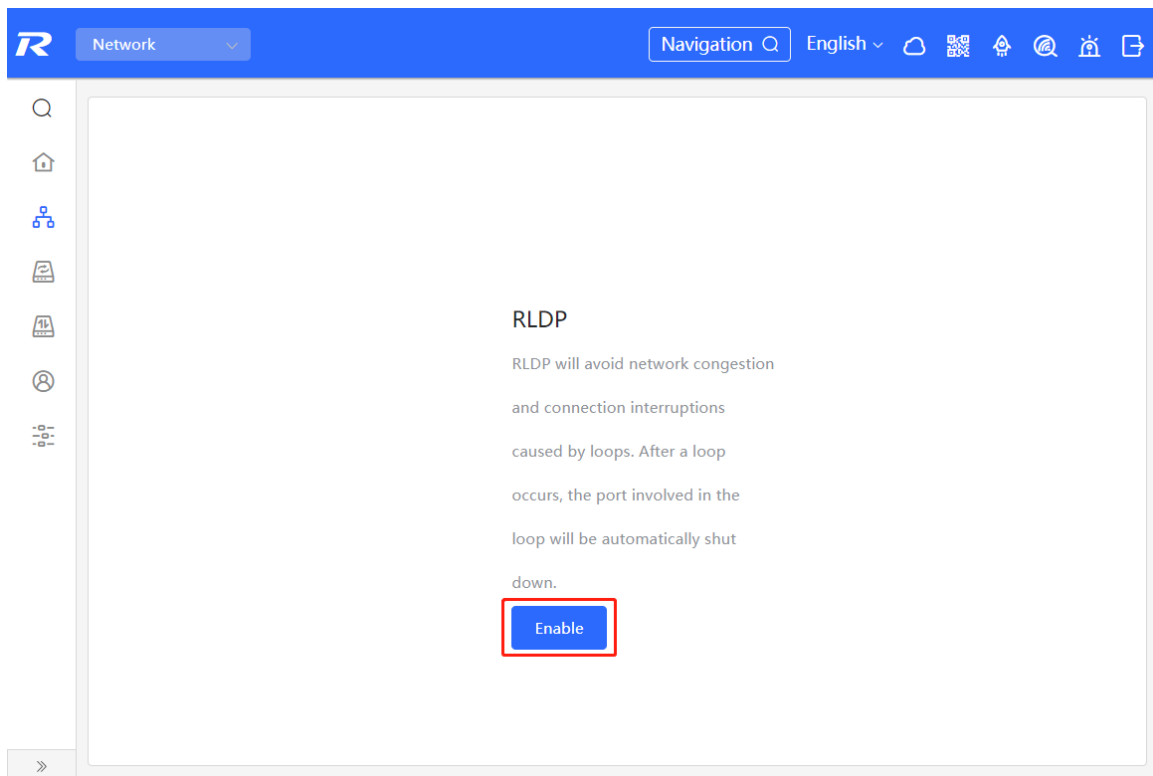
The screenshot shows the 'RLDP Info' page with a 'Port List' table. The table has four columns: Port, Status, Action, and Neighbor Port. A 'Reset' button is located in the top right corner of the table area.

Port	Status	Action	Neighbor Port
Gi1	OK	--	--
Gi2	OK	--	--
Gi3	OK	--	--
Gi4	OK	--	--
Gi5	OK	--	--
Gi6	OK	--	--
Gi7	OK	--	--

10.3.3 Batch Configuring Network Switches

Choose **Network > RLDP** .

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



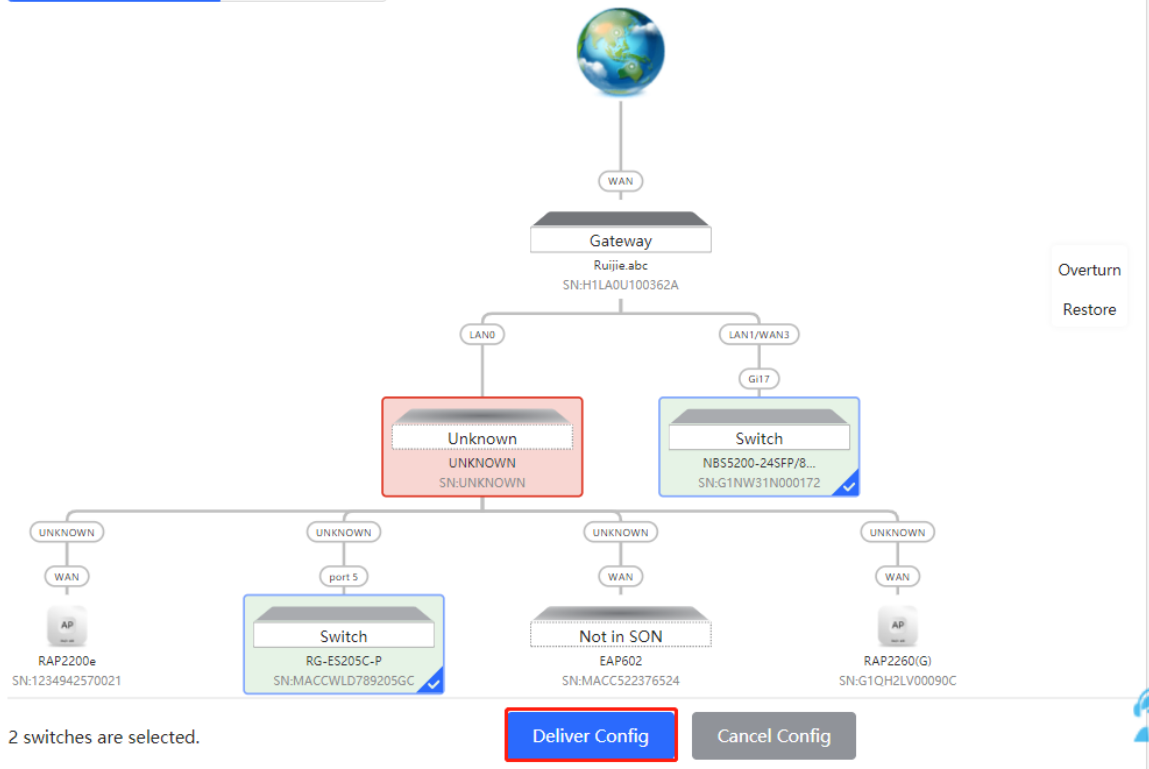
(2) In the networking topology, you can select the access switches on which you want to enable RLDP in either recommended or custom mode. If you select the recommended mode, all access switches in the network are selected automatically. If you select the custom mode, you can manually select the desired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

← RLDP Config

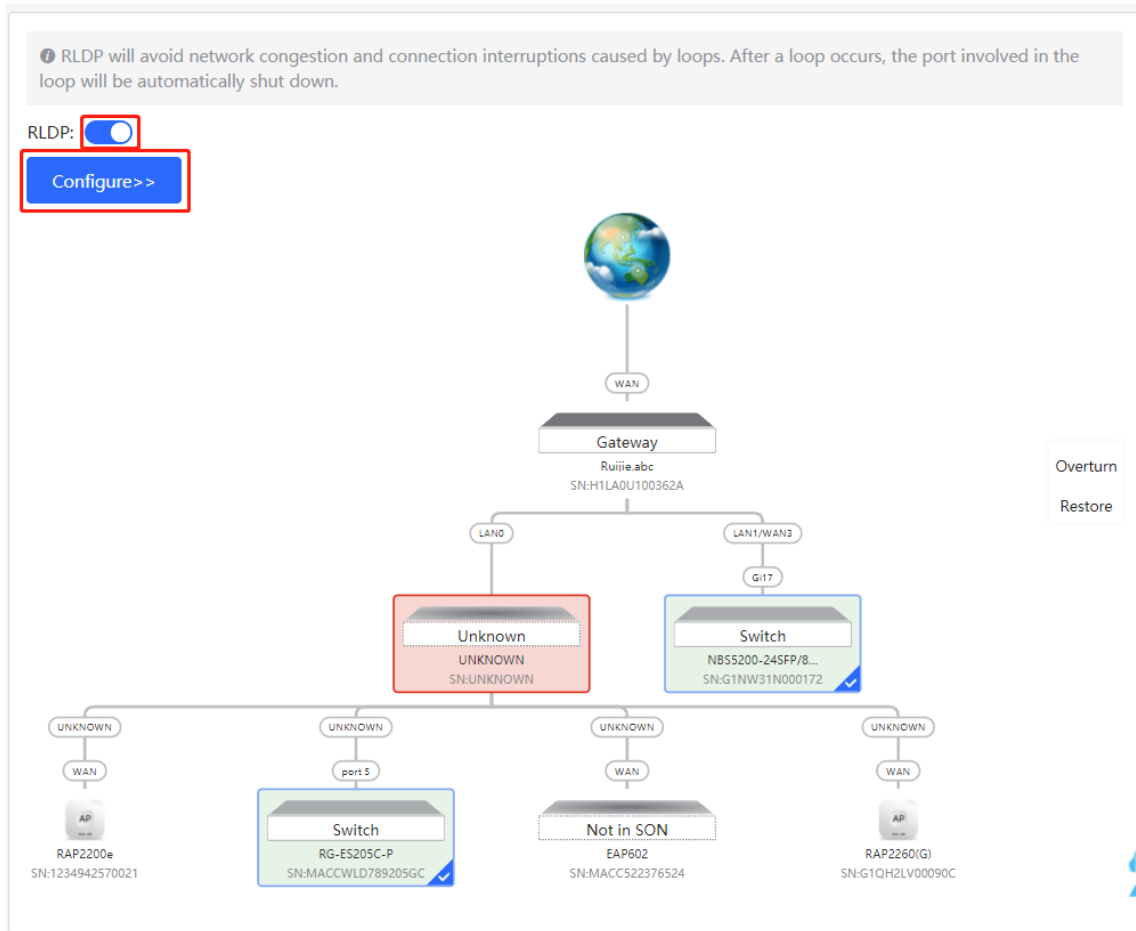
Please select the target switch:

Recommended
 Auto-Identified Switches

Custom
 Specified Switches



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



10.4 Configuring the Local DNS

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

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

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

The device will get the DNS server address from the uplink device.

Local DNS server

[Save](#)

10.5 Voice VLAN

Caution

The support of this function differs among different products, and the NBF2100M series does not support this function.

10.5.1 Overview

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

10.5.2 Voice VLAN Global Configuration

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

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

Global Settings OUI Port Settings

i Global Settings

Voice VLAN

* VLAN Range: 2-4094

* Max Age minute Range: 1-43200

CoS Priority

Save

Table 10-5 Description of VLAN Global Configuration Parameters

Parameter	Description	Default Value
Voice VLAN	Whether to enable the Voice VLAN function	Disable
VLAN	VLAN ID as Voice VLAN	NA

Parameter	Description	Default Value
Max Age	Aging time of voice VLAN, in minutes. In automatic mode, after the MAC address in a voice packet ages, if the port does not receive any more voice packets within the aging time, the device removes this port from the voice VLAN	1440 minutes
CoS Priority	The L2 Priority of voice stream packets in a Voice VLAN. The value range is from 0 to 7. A greater value indicates a higher priority. You can modify the priority of the voice traffic to improve the call quality.	6

10.5.3 Configuring a Voice VLAN OUI

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

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

Note

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

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

Global Settings
OUI
Port Settings

OUI List
The enabled globally port will automatically add the corresponding OUI when receiving an LLDP packet that is identified as telephone.

OUI List + Add Delete Selected

Up to **32** entries can be added.

	MAC Address	OUI Mask	Description	Type	Action
<input type="checkbox"/>					

No Data

Add
×

* MAC Address

OUI Mask

Description

10.5.4 Configuring the Voice VLAN Function on a Port

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

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

Global Settings
OUI
Port Settings

Port List

The port can be set to the automatic mode only when the port VLAN is in the trunk or hybrid mode. When the port is in the automatic mode, the port will exit the voice VLAN first, and automatically join the voice VLAN until it receives voice data again.

i To ensure the normal operation of voice VLAN on port, please do not switch the port mode (hybrid/trunk/access mode). To switch the mode, please disable the voice VLAN first.

Voice VLAN does not support layer 3 ports and aggregation ports.

Port List ↻ Batch Edit

Port	Enable	Voice VLAN Mode	Security Mode	Action
Gi1	Disabled	Auto Mode	Enabled	Edit
Gi2	Disabled	Auto Mode	Enabled	Edit
Gi3	Disabled	Auto Mode	Enabled	Edit
Gi4	Disabled	Auto Mode	Enabled	Edit

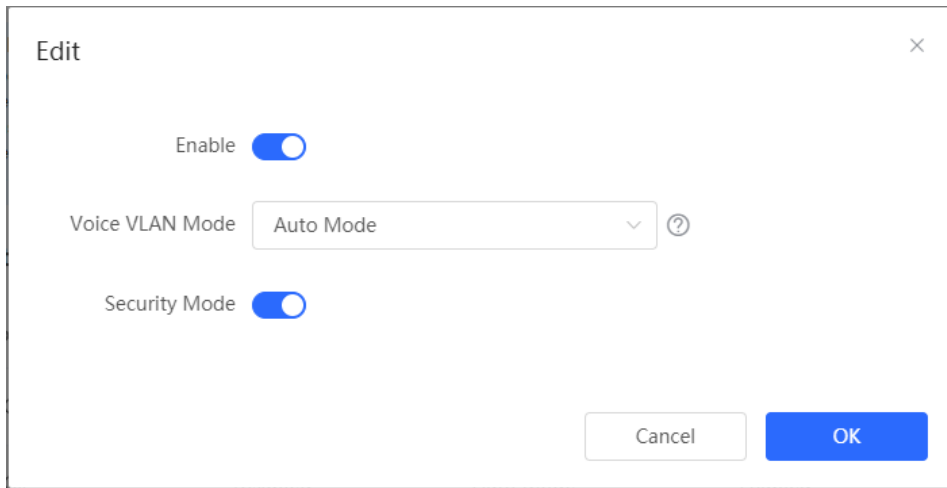


Table 10-6 Description of the Voice VLAN Configuration Parameters on a Port

Parameter	Description	Default Value
Voice VLAN Mode	<p>Based on different ways the Voice VLAN function is enabled on the port, the Voice VLAN Mode can be Auto Mode or Manual Mode:</p> <ul style="list-style-type: none"> ● Auto Mode : In this mode, the device checks whether the permit VLANs of a port contain the voice VLAN after the voice VLAN function is enabled on the port. If yes, the device deletes the voice VLAN from the permit VLANs of the port until the port receives a voice packet containing a specified OUI. Then, the device automatically adds the voice VLAN to the port's permit VLANs. If the port does not receive a voice packet containing the specified OUI within the global aging time, the device removes the Voice VLAN from the permit VLANs of the port. ● Manual Mode : If the permit VLANs of a port contains the voice VLAN, voice packets can be transmitted in the voice VLAN. 	Auto Mode
Security Mode	<p>When the security mode is enabled, only voice traffic can be transmitted in the voice VLAN. The device checks the source MAC address in each packet. When the source MAC address in the packet matches the voice VLAN OUI, the packet can be transmitted in the voice VLAN. Otherwise, the device discards the packet.</p> <p>When the security mode is disabled, the source MAC addresses of packets are not checked and all packets can be transmitted in the voice VLAN.</p>	Enable

⚠ Caution

- The voice VLAN mode of the port can be set as the auto mode only when the VLAN mode of the port is Trunk mode. When the voice VLAN mode of the port work in the auto mode, the port exits the voice VLAN first and is automatically added to the voice VLAN only after receiving voice data.

- After the voice VLAN function is enabled on a port, do not switch the L2 mode (trunk or access mode) of the port to ensure normal operation of the function. If you need to switch the L2 mode of the port, disable the voice VLAN function on the port first.
 - It is not recommended that both voice data and service data be transmitted over the voice VLAN. If you want to transmit both voice data and service data over the voice VLAN, disable the voice VLAN function in security mode.
 - The voice VLAN function is unavailable on L3 ports or aggregate ports.
-

11 Diagnostics

11.1 Info Center

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

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

The screenshot shows the Ruijie Rcycc web interface. The left sidebar contains navigation options: VLAN, Monitor, Ports, L2 Multicast, L3 Interfaces, Routing, Security, Advanced, Diagnostics (highlighted), Info Center (highlighted), Network Tools, Fault Collection, Cable Diagnostics, System Logs, and Alarms. The main content area is titled 'Info Center' and shows 'Port Info' for G11. The port status is 'Connected'. Below the port info, there is a table for 'VLAN Info (SVI&Routed Port)' with columns for Interface, IP Address, DHCP Address Pool, and Remarks. The table lists VLAN1, VLAN888, VLAN2001, VLAN3011, VLAN3012, VLAN3013, and Routed Port Gi23.

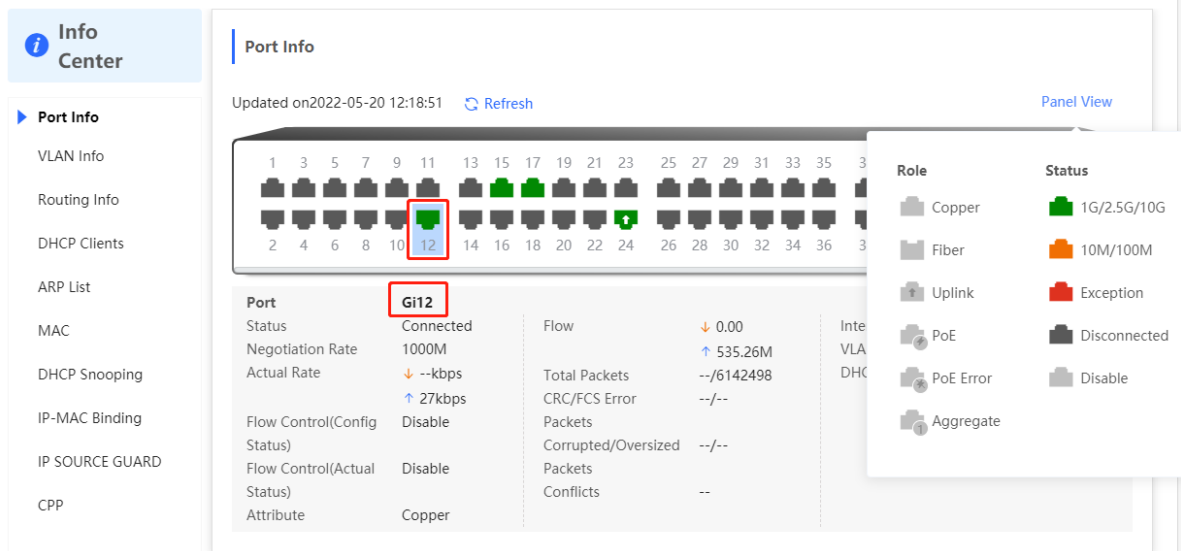
11.1.1 Port Info

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

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

Note

- To configure the flow control of the port or the optical/electrical attribute of a combo port, see [4.2](#) .
- To configure the L2 mode of the port and the VLAN to which it belongs, see [3.5.3](#) .



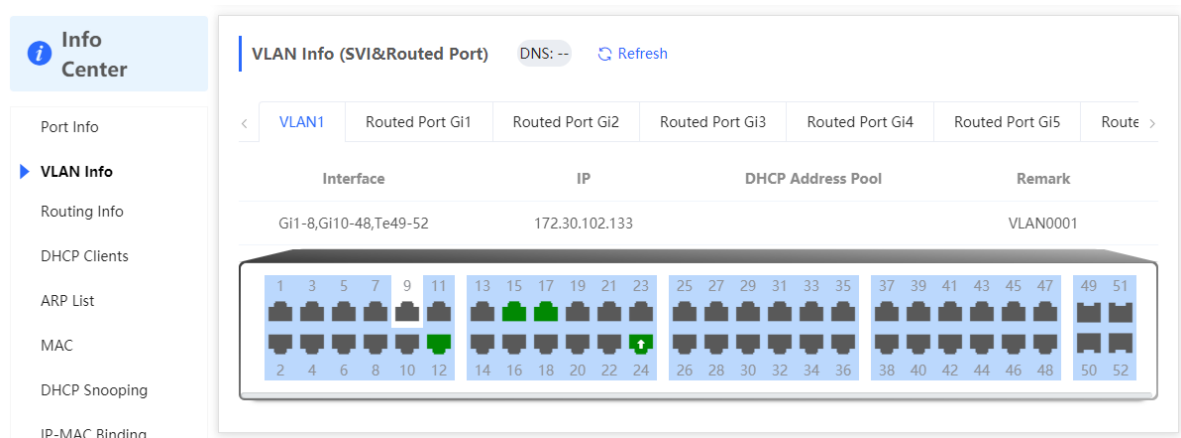
11.1.2 VLAN Info

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

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

Note

- To configure VLAN, see [0](#).
- To configure SVI ports and routed ports, see [6.1](#).



11.1.3 Routing Info

Caution

If the device does not support L3 functions (such as RG-NBF2100 Series), this type of information is not displayed.

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

Displays the routing information on the device. The search box in the upper-right corner supports finding route entries based on IP addresses.

Note

To set up static routes, see [6.3](#).

The screenshot shows the 'Routing Info' section of the 'Info Center'. On the left, there is a navigation menu with options: Port Info, VLAN Info, Routing Info (selected), and DHCP Clients. The main content area has a title 'Routing Info' and a tip: 'Tip: Up to 500 entries can be added.' Below the tip is a search box labeled 'Search by IP Address' with a magnifying glass icon and a 'Refresh' button. A table displays routing information:

Interface	IP	Subnet Mask	Next Hop
Gi9	2.1.1.0	255.255.255.0	3.1.1.1

11.1.4 DHCP Clients

Caution

If the device does not support L3 functions (such as RG-NBF2100 Series), this type of information is not displayed.

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

Displays the IP address information assigned to endpoints by the device as a DHCP server.

Note

To configure DHCP server related functions, see [6.2](#).

The screenshot shows the 'DHCP Clients' section of the 'Info Center'. On the left, there is a navigation menu with options: Port Info, VLAN Info, Routing Info, DHCP Clients (selected), ARP List, and MAC. The main content area has a title 'DHCP Clients' and a tip: 'Tip: Up to 1000 entries can be added.' Below the tip is a search box labeled 'Search by Hostname/IP/MAC' with a magnifying glass icon and a 'Refresh' button. A table displays DHCP client information:

Hostname	IP	MAC	Lease Time(Min)	Status
No Data				

11.1.5 ARP List

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

Displays ARP information on the device, including dynamically learned and statically configured ARP mapping entries.

Note

To bind dynamic ARP or manually configure static ARP, see [6.4](#).

Info Center

ARP List

Tip: Up to 1000 entries can be added.

Search by IP Address/MAC A Refresh

Interface	IP Address	MAC Address	Type	Reachable
VLAN0001	10.52.48.179	00:d0:f8:15:08:bb	Dynamic	Yes
VLAN0001	10.52.49.124	00:d0:f9:15:08:61	Dynamic	Yes
VLAN0001	10.52.48.138	00:e0:4c:00:21:2d	Dynamic	Yes
VLAN0001	10.52.48.43	00:d0:88:88:08:60	Dynamic	Yes
VLAN0001	10.52.48.182	00:d0:f8:12:08:5a	Dynamic	Yes
VLAN0001	10.52.48.73	30:0d:9ec4:1a:35	Dynamic	Yes
VLAN0001	10.52.48.117	64:00:6a:06:23:43	Dynamic	Yes
VLAN0001	10.52.48.128	30:0d:9e:94:0e:aa	Dynamic	Yes
VLAN0001	10.52.49.13	58:69:6c:fb:22:d6	Dynamic	Yes
VLAN0001	10.52.48.226	00:d0:f8:15:17:62	Dynamic	Yes

1 2 3 4 10/page Go to page 1 Total 33

11.1.6 MAC Address

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

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

Note

To configure and manage the MAC address, see [3.3](#).

Info Center

MAC

Tip: Up to 16K entries can be added.

Search by MAC Refresh

Interface	MAC	Type	VLAN ID
Gi24	70:B5:E8:5F:FD:29	Dynamic	1
Gi24	50:9A:4C:42:C9:50	Dynamic	1
Gi24	30:0D:9E:6F:C2:3C	Dynamic	1
Gi24	30:0D:9E:6F:C2:3D	Dynamic	1
Gi24	C0:B8:E6:E9:78:07	Dynamic	1
Gi24	30:B4:9E:8F:85:E5	Dynamic	1
Gi24	58:69:6C:CE:72:B2	Dynamic	1
Gi24	70:B5:E8:78:B7:8D	Dynamic	1

11.1.7 DHCP Snooping

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

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

Note

To modify DHCP Snooping related configuration, see [7.1](#).

The screenshot shows the 'Info Center' sidebar on the left with 'DHCP Snooping' selected. The main content area is divided into two sections:

- DHCP Snooping:** Shows 'DHCP Snooping: Enabled', 'Option82: Disabled', and 'Trusted Port: Gi24'. Below this is a table titled 'DHCP Snooping Binding Entries from the Trusted Port':

Interface	IP	MAC	VLAN ID	Lease Time(Min)
Gi15	172.30.102.17	08:00:27:62:F0:53	1	240
- IP-MAC Binding:** Shows a tip 'Up to 500 entries can be added.' and a search bar 'Search by IP Address'. Below is a table with columns 'Port', 'IP', and 'MAC':

Port	IP	MAC

11.1.8 IP-MAC Binding

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

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

Note

To add or modify the IP-MAC binding, see [7.5](#).

The screenshot shows the 'Info Center' sidebar on the left with 'IP-MAC Binding' selected. The main content area is divided into two sections:

- IP-MAC Binding:** Shows a tip 'Up to 500 entries can be added.' and a search bar 'Search by IP Address'. Below is a table with columns 'Port', 'IP', and 'MAC':

Port	IP	MAC
Gi29	192.168.1.1	00:11:22:33:44:55
- IP SOURCE GUARD:** Shows a tip 'Up to 1900 entries can be added.' and a search bar 'Search by IP Address'. Below is a table with columns 'Interface', 'Rule', 'IP', 'MAC', 'VLAN ID', and 'Status':

Interface	Rule	IP	MAC	VLAN ID	Status
Gi15	IP	172.30.102.17	08:00:27:62:F0:53	1	Inactive

11.1.9 IP Source Guard

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

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

Note

To configure IP Source Guard function, see [7.6](#).

IP SOURCE GUARD

Tip: Up to **1900** entries can be added. Search by IP Address

Interface	Rule	IP	MAC	VLAN ID	Status
Gi15	IP	172.30.102.17	08:00:27:62:F0:53	1	Inactive

CPP

Total CPU bandwidth: 2000pps

EtherType Value	Rate	Current Rate	Total messages
bodu	60pps	0pps	0

11.1.10 CPP Info

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

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

Info Center

CPP

Total CPU bandwidth: 2000pps

EtherType Value	Rate	Current Rate	Total messages
bodu	60pps	0pps	0
lldp	50pps	0pps	5328
rldp	50pps	0pps	0
lacp	600pps	0pps	0
arp	400pps	2pps	426731
dhcp	600pps	5pps	622
icmp	600pps	0pps	3708
macc	600pps	11pps	190569
mqtt	600pps	0pps	0
http/https	1600pps	4pps	105864

Total 26 < 1 2 3 > Go to page

11.2 Network Tools

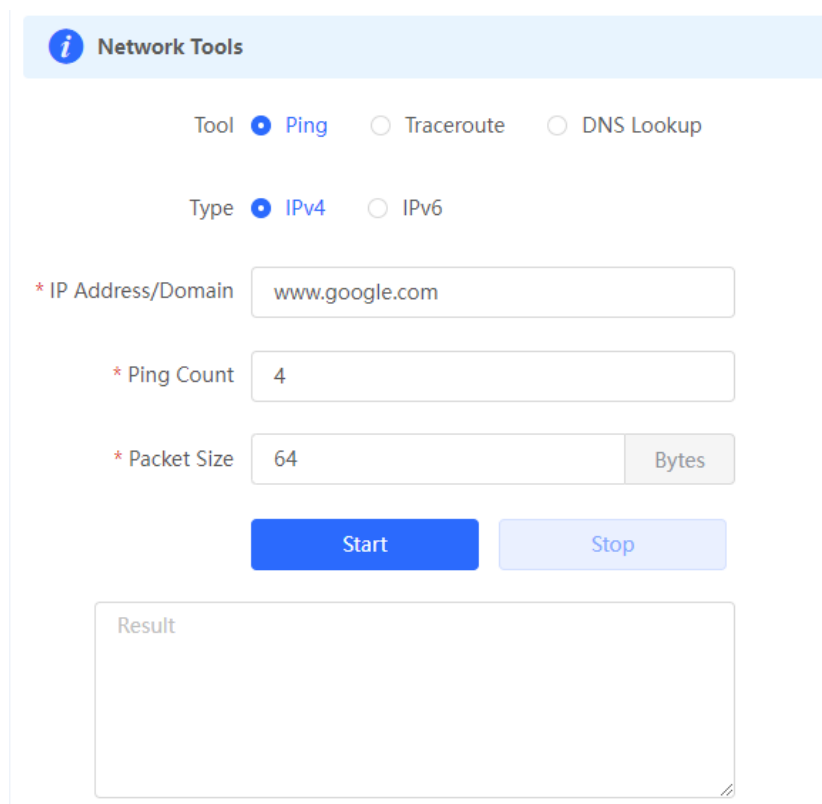
The **Network Tools** page provides three tools to detect the network status: **Ping** , **Traceroute** , and **DNS Lookup** .

11.2.1 Ping

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

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

Select **Ping** as the diagnosis mode, select the IP address type (IPv4 or IPv6), enter the destination IP address or domain name , configure the ping count and packet size, and click **Start** to test the network connectivity between the device and the IP address or website. If "Ping failed" is displayed, the device is not reachable to the IP address or website.



The screenshot shows the 'Network Tools' configuration page. At the top, there is a header 'Network Tools' with an information icon. Below the header, there are three radio buttons for 'Tool': 'Ping' (selected), 'Traceroute', and 'DNS Lookup'. Underneath, there are two radio buttons for 'Type': 'IPv4' (selected) and 'IPv6'. The main configuration area includes three input fields: '* IP Address/Domain' with the value 'www.google.com', '* Ping Count' with the value '4', and '* Packet Size' with the value '64' and a 'Bytes' label. Below these fields are two buttons: a blue 'Start' button and a light blue 'Stop' button. At the bottom, there is a large empty text area labeled 'Result'.

11.2.2 Traceroute

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

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

Select **Traceroute** as the diagnosis mode, select IP address type (IPv4 or IPv6), enter a destination IP address or the maximum TTL value used by the URL and traceroute , and click **Start** .

i Network Tools

Tool Ping Traceroute DNS Lookup

Type IPv4 IPv6

* IP Address/Domain

* Max TTL

Result

11.2.3 DNS Lookup

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

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

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

i Network Tools

Tool Ping Traceroute DNS Lookup

* IP Address/Domain

* DNS

Result

11.3 Fault Collection

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

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

i Fault Collection
Compress the configuration file for engineers to identify fault.

11.4 Cable Diagnostics

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

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

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

Port Panel

Available Unavailable Uplink Copper Fiber

Note: You can click and drag to select one or more ports. [Select All](#) [Inverse](#) [Deselect](#)

Start

Result

Port	Cable Length (cm)	Result
Gi15	700	OK

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

11.5 System Logs

Choose **Local Device > 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. You can search for specified logs by fault type, faulty module, and keyword in fault information.

System Logs
View system logs.

Log List

Time	Type	Module	Details
May 18 18:52:37	kern.crit	kernel	%Port-2: GigabitEthernet12 link up
May 18 18:52:37	local.info	syslog	%L3-6: Manage VLAN 1 change to UP
May 18 18:52:37	kern.crit	kernel	%Port-2: GigabitEthernet13 link up
May 18 18:52:37	kern.crit	kernel	%Port-2: GigabitEthernet17 link up
May 18 18:52:38	kern.crit	kernel	%Port-2: GigabitEthernet22 link up

Search [] Q

- local.info
- syslog
- kernel
- kern.crit

11.6 Alerts

Choose **Local Device > Diagnostics > Alarms** .

Note

Choose **Network > Alerts** to view the alert information of other devices in the network.

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

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

 **Caution**

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

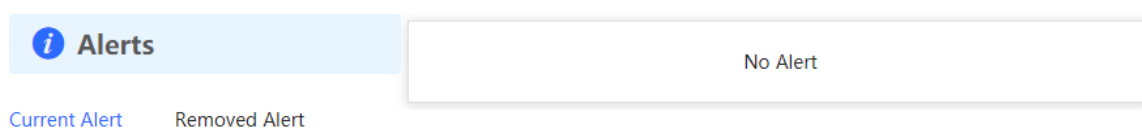


Table 11-1 Alert Types and Product Support

Alert Type	Description	Support Description
Addresses in the DHCP address pool are to be exhausted.	The device acts as a DHCP server, and the number of allocated addresses is about to reach the maximum number of addresses that can be allocated in the address pool.	It is applicable only to devices that support L3 functions. Products that do not support L3 functions such as RG-NBF2100 Series do not support this type of alert.
The IP address of the local device conflicts with that of another device.	The IP address of the local device conflicts with that of another client on the LAN.	NA
An IP address conflict occurs on downlink devices connected to the device.	Among the devices connected to the current device on the LAN, an IP address conflict occurs on one or more devices.	NA
The MAC address table is full of entries.	The number of L2 MAC address entries is about to reach the hardware capacity limit of the product.	NA
The ARP table is full of ARP entries.	The number of ARP entries on the network exceeds the ARP capacity of the device.	NA



Alert Type	Description	Support Description
The device has a loop alarm.	A network loop occurs on the LAN.	NA

12 System Configuration

12.1 Setting the System Time

[Whole Network Management-Page Wizard] System Management >> System Time

You can view the current system time. If the time is incorrect, check and select the local time zone. If the time zone is correct but time is still incorrect, click Edit to manually set the time. In addition, the device supports **Network** Time Protocol (NTP) servers. By default, multiple servers serve as the backup of each other. You can add or delete the local server as required.

 Configure and view system time (The device has no RTC module. The time settings will not be saved upon reboot). 

Current Time 2022-05-20 14:32:29

* Time Zone (GMT+8:00)Asia/Shanghai

* NTP Server

0.cn.pool.ntp.org	<input type="button" value="Add"/>
1.cn.pool.ntp.org	<input type="button" value="Delete"/>
2.cn.pool.ntp.org	<input type="button" value="Delete"/>
3.cn.pool.ntp.org	<input type="button" value="Delete"/>
0.asia.pool.ntp.org	<input type="button" value="Delete"/>
3.asia.pool.ntp.org	<input type="button" value="Delete"/>
0.pool.ntp.org	<input type="button" value="Delete"/>
1.pool.ntp.org	<input type="button" value="Delete"/>
rdate.darkorb.net	<input type="button" value="Delete"/>

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

Edit ×

* Time  2022-05-20 14:32:25

12.2 Setting the Web Login Password

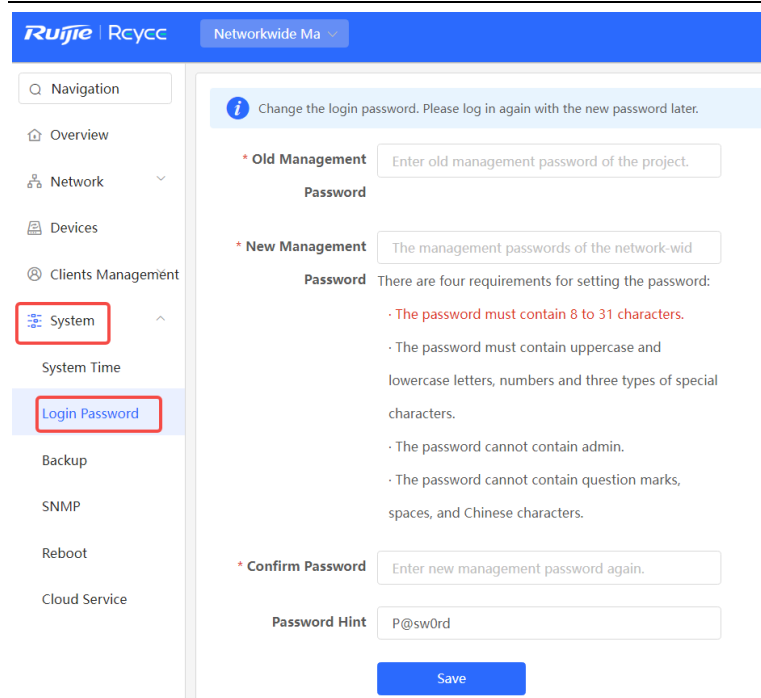
[Local Management-Page Wizard] System Settings>> Login Management >>Login Password

[Whole Network Management-Page Wizard] System Management >> Login Password

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

Caution

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



The screenshot shows the Ruijie Rcycc web management interface. The top navigation bar includes the Ruijie logo and 'Rcycc' text. A dropdown menu shows 'Networkwide Ma'. The left sidebar contains a navigation menu with items: Overview, Network, Devices, Clients Management, System (highlighted with a red box), System Time, Login Password (highlighted with a red box), Backup, SNMP, Reboot, and Cloud Service. The main content area displays a message: 'Change the login password. Please log in again with the new password later.' Below this are three password input fields: 'Old Management Password' (with placeholder 'Enter old management password of the project.'), 'New Management Password' (with placeholder 'The management passwords of the network-wid'), and 'Confirm Password' (with placeholder 'Enter new management password again.'). A 'Password Hint' field contains 'P@sw0rd'. A list of requirements for the new password is shown: 'There are four requirements for setting the password: · The password must contain 8 to 31 characters. · The password must contain uppercase and lowercase letters, numbers and three types of special characters. · The password cannot contain admin. · The password cannot contain question marks, spaces, and Chinese characters.' A blue 'Save' button is at the bottom.

12.3 Setting the Session Timeout Duration

[Local Management-Page Wizard] System Settings>> Login Management >> Login Timeout

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

12.4 Configuring SNMP

12.4.1 Overview

SNMP (Simple Network Management Protocol) is a protocol used for managing network devices. It is based on the client/server model and can remotely monitor and control network devices.

SNMP consists of a management station and agents, with the management station communicating with agents through the SNMP protocol to obtain information such as device status, configuration information, performance data, etc., while also being able to configure and manage devices.

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

12.4.2 Global Configuration

1. Overview

The purpose of global configuration is to enable SNMP services and implement basic configurations such as SNMP protocol version (v1/v2c/v3), local port settings, device location settings, contact information settings.

SNMPv1: v1 is the earliest version of SNMP with poor security that only supports simple community string authentication. The v1 version has some defects such as plaintext transmission of community strings which makes it vulnerable to attacks; therefore it is not recommended for use in modern networks .

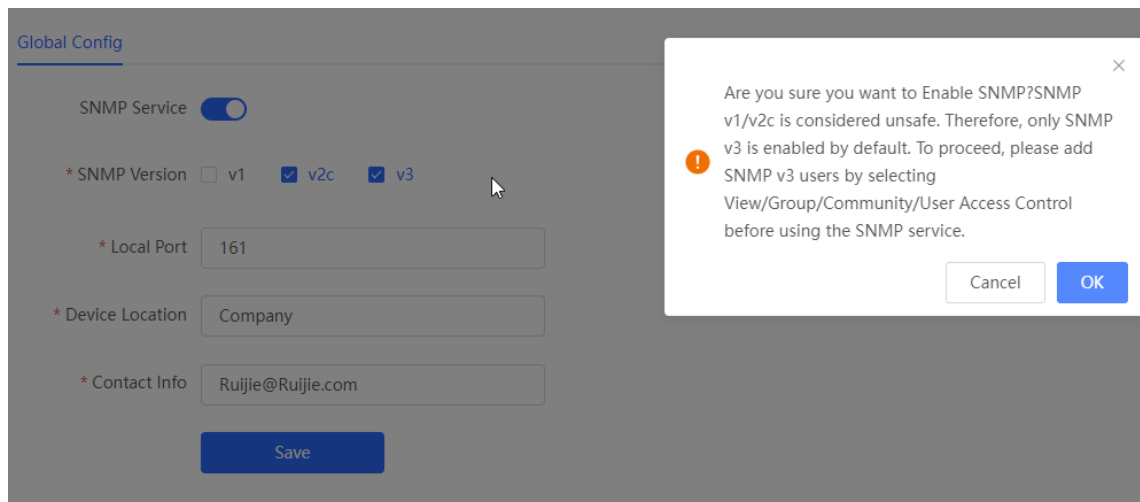
SNMPv2c: v2c is an improved version over v1 that supports richer functionality and more complex data types while enhancing security measures compared to its predecessor. The v2c version provides better security features than v1 along with greater flexibility allowing users to configure according to their specific needs.

SNMPv3: This latest version of the SNMP protocol includes additional security mechanisms like message authentication encryption compared to its predecessors - V1 & V2C - resulting in significant improvements in terms of access control & overall safety measures implemented by this standard.

2. Configuration Steps:

[Network-wide Management-Page Wizard] System>>SNMP>>Global Config

(1) Enable SNMP services.



When first opened, the system prompts to enable SNMPv3 by default. Click < OK >.

(2) Set global configuration parameters for SNMP service.

Global Config View/Group/Community/Client Access Control Trap Settings

SNMP Service

* SNMP Version v1 v2c v3

* Local Port

* Device Location

* Contact Info

Table 12-1 Global Configuration Description Table

Parameter	Parameter
SNMP Service	Whether the SNMP service is enabled or not.
SNMP Protocol Version	SNMP protocol version number includes v1 version, v2c version, and v3 version.
Local Port	[1, 65535]
Device Location	Cannot contain Chinese characters, full-width characters, question marks and spaces. Character length: 1-64.
Contact Information	Cannot contain Chinese characters, full-width characters, question marks and spaces. Character length: 1-64.

(3) Click <Save>.

After enabling the SNMP service takes effect, click <Save> to make basic configurations such as SNMP protocol version number take effect .

12.4.3 View/Group/Community/Client Access Control

1. View/Group/Community/Client Access Control

MIB (Management Information Base) can be regarded as a database of different status information and performance data of network devices containing a large number of OID (Object Identifiers), which are used to identify different status information and performance data of network devices in snmp .

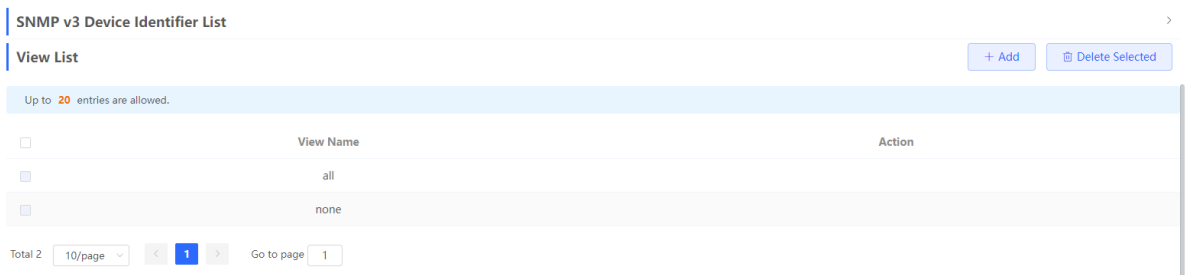
The role of views in snmp is to limit the node range that management systems can access in MIBs so as to improve network management security and reliability. Views are an indispensable part of SNMP management that needs to be configured and customized according to specific management requirements.

Views can define multiple subtrees according to requirements limiting the MIB nodes that management systems can only access within these subtrees while unauthorized MIB nodes cannot be accessed by unauthenticated system administrators thus protecting network device security. At the same time views also optimize network management efficiency improving response speed for managing systems.

Configuration Steps:

[Network-wide Management - Page Wizard] System >> SNMP >> View/Group/Community/Client Access Control >> View List

(1) Click <Add> to create a view.



(2) Configure the basic information of the view.

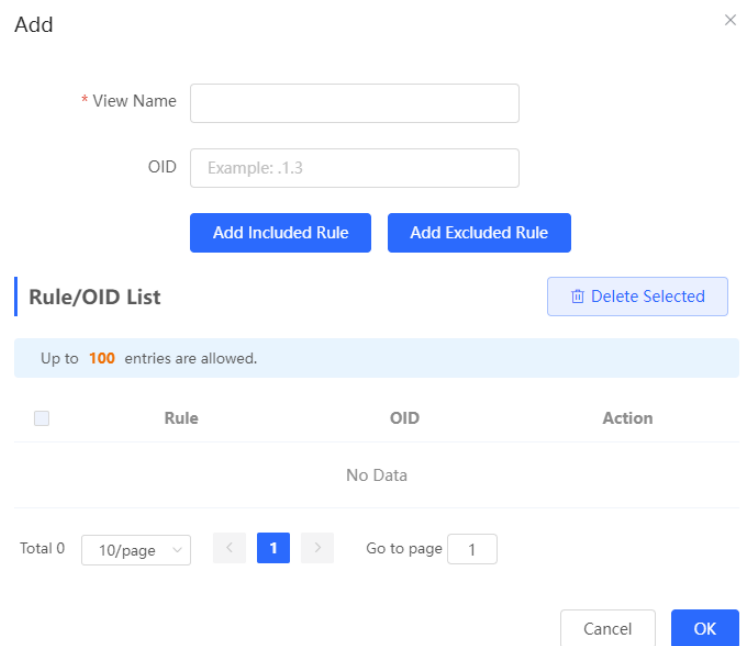


Table 12-2 Create a view

parameter	illustrate
View Name	The name used to identify the view.

parameter	illustrate
	The length is 1 to 32 characters, and cannot contain Chinese and full-width characters.
OIDs	Define the range of OIDs included in the view, which can be a single OID or a subtree of OIDs
Add Included Rule or Excluded Rule <div style="display: flex; justify-content: space-around; margin-top: 10px;"> Add Included Rule Add Excluded Rule </div>	Divided into inclusion rules and exclusion rules <ul style="list-style-type: none"> ● Include rules allow access only to OIDs within the OID range . Click <Add Inclusion Rule> to set up this type of view. ● Exclusion rules allow access to all OIDs except the OID range . Click <Add Exclusion Rule> to set up this type of view.

Notice

For the created view, add at least one OID rule , otherwise a warning message will appear .

(3) Click <OK> .

1. v1 /v2c user configuration

Introduction

- When the SNMP protocol version is set to v1/v2c, user configuration needs to be completed.

[Global Config](#)
[View/Group/Community/Client Access Control](#)
[Trap Settings](#)

SNMP Service

* SNMP Version v1 v2c v3

* Local Port

* Device Location

* Contact Info

Save

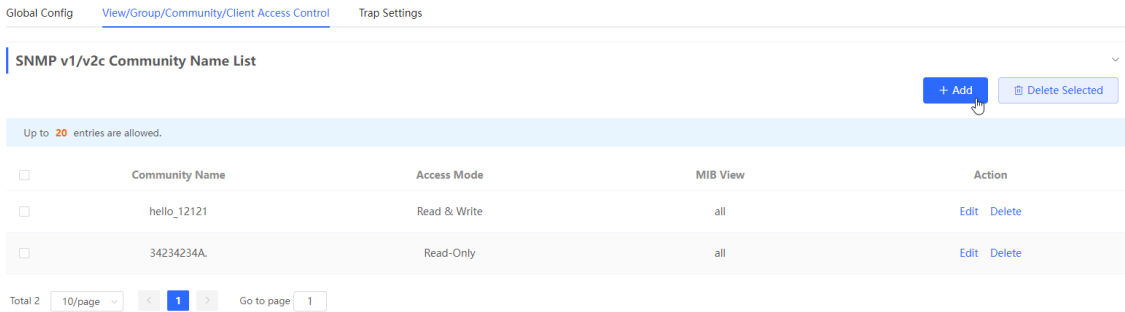
Note

Select the SNMP protocol version, click <Save>, and the corresponding configuration options will appear on the view/group/group/user access control interface.

- configuration steps

【 Entire Network Management-Page Wizard 】 System>>SNMP>> View/Group/Community/Client Access Control

(1) In the " SNMP v1/v2c Community Name List " area, click <Add>.



(2) Create v1/v2c users.

Add ×

* Community Name

* Access Mode

* MIB View [Add View +](#)

Table 4-1 v1 / v2c user information description table

parameter	illustrate
Community Name	at least 8 characters Contains three types of uppercase letters, lowercase letters, numbers, and special characters Does not contain admin/public/private Do not contain question marks, spaces and Chinese
Access Mode	Access rights of the community name (read-only, read-write) Read & Write Read-Only
MIB View	The options in the drop-down box are configured views (default views all , none)

⚠ Notice

- Among v1/v2c users, the community name cannot be repeated .
- Click <Add View> to add a view .

2. v3 group configuration

- Introduction

SNMPv3 introduces the concept of grouping for better security and access control. A group is a group of SNMP users with the same security policy and access control settings. Using SNMPv3 , multiple groups can be configured, each group can have its own security policy and access control settings, and each group can also have one or more users.

- prerequisite

When the SNMP protocol version is set to v3 , the v3 group configuration needs to be completed.

Note

Select the SNMP protocol version, click <Save>, and the corresponding configuration options will appear on the view/group/group/user access control interface.

- configuration steps

[Entire Network Management - Page Wizard] Setting >> SNMP >> View/Group/Group/User Access Control.

(1) Click <Add> in the " SNMP v3 Group List " area to create a v3 group .

Global Config View/Group/Community/Client Access Control Trap Settings

SNMP Service

* SNMP Version v1 v2c v3

* Local Port

* Device Location

* Contact Info

(2) Set v3 groups of related parameters.

Global Config View/Group/Community/Client Access Control Trap Settings

SNMP v3 Group List + Add Delete Selected

Up to 20 entries are allowed.

<input type="checkbox"/>	Group Name	Security Level	Read-Only View	Read & Write View	Notification View	Action
<input type="checkbox"/>	default_group	Auth & Security	all	none	none	Edit Delete

Total 1 10/page < 1 > Go to page 1

Add
×

* Group Name

* Security Level Allowlist & Security ▾

* Read-Only View all ▾ [Add View +](#)

* Read & Write View all ▾ [Add View +](#)

* Notification View none ▾ [Add View +](#)

Cancel
OK

Table 4-1 V3 group configuration parameters

parameter	illustrate
Group Name	rule group name 1-32 characters, a single Chinese accounted for three characters Cannot contain Chinese, full-width characters, question marks and spaces
Security Level	The minimum security level of the rule group (Auth & Security Auth &Open Allowlist & Security authentication with encryption, authentication without encryption, no authentication encryption)
Read-Only View	The options in the drop-down box are configured views (default views all , none)
Read & Write View	The options in the drop-down box are configured views (default views all , none)
Notification View	The options in the drop-down box are configured views (default views all , none)

Notice

- Groups limit the minimum security level, read and write permissions and scope of users in the group.
- The group name cannot be repeated . If you need to add a view, click < Add View >.

(3) Click <OK> .

3. v 3 user configuration

- Introduction
- prerequisite

When the SNMP protocol version is set to v3 , the v3 group configuration needs to be completed.

Global Config View/Group/Community/Client Access Control Trap Settings

SNMP Service

* SNMP Version v1 v2c v3

* Local Port

* Device Location

* Contact Info

i illustrate

Select the SNMP protocol version, click <Save>, and the corresponding configuration options will appear on the view/group/group/user access control interface.

● configuration steps

[Entire Network Management - Page Wizard] Setting >> SNMP >> View/Group/Group/User Access Control >>.

(1) In the "SNMP v3 Client List" area, click <Add> to create a v3 user .

Global Config View/Group/Community/Client Access Control Trap Settings

SNMP v3 Client List

Up to 50 entries are allowed.

<input type="checkbox"/>	Username	Group Name	Security Level	Auth Protocol	Auth Password	Encryption Protocol	Encrypted Password	Action
No Data								

Total 0

(2) Set v3 user related parameters.

Add

* Username

* Group Name

* Security Level


* Auth Protocol * Auth Password

* Encryption Protocol * Encrypted Password

Table 12-3 v3 user configuration parameters

parameter	illustrate
Username	username

parameter	illustrate
	<p>at least 8 characters</p> <p>Contains three types of uppercase letters, lowercase letters, numbers, and special characters</p> <p>Does not contain admin/public/private</p> <p>Do not contain question marks, spaces and Chinese</p>
Group Name	user's group
Security Level	User security level (authentication and encryption, authentication without encryption, no authentication and encryption)
Auth Protocol , Auth Password	<p>Authentication protocols include: MD5/SHA/SHA224/SHA256/SHA384/SHA512</p> <p>Authentication password: 8~31 characters in length, cannot contain Chinese characters, full-width characters, question marks, and spaces , and must contain at least 3 types of uppercase and lowercase letters, numbers, or special characters.</p> <p>Note: This parameter needs to be set when the "Security Level" is "authentication and encryption" or "authentication without encryption".</p>
Encryption Protocol , Encrypted Password	<p>Encryption protocols include: DES/AES/AES192/AES256</p> <p>Encrypted password: the length is 8~ 31 characters, and cannot contain Chinese, full-width characters, question marks and spaces format , containing at least 3 types of uppercase and lowercase letters, numbers, or special characters.</p> <p>Note: When the "Security Level" is "Authentication and Encryption", this parameter needs to be set.</p>

 Notice

- The security level of the v3 user must be greater than or equal to the security level of this group.
- There are three security levels. For authentication and encryption, you need to configure the authentication protocol, authentication password, encryption protocol, and encryption password. For authentication without encryption, you only need to configure the authentication protocol and encryption protocol. Without authentication and encryption , no configuration is required.

12.4.4 Typical Configuration Examples of SNMP Service

1. v2c version SNMP service configuration

- scenes to be used

The user only needs to monitor the information of the device, and does not need to set and send it. The data information of nodes such as 1.3.6.1.2.1.1 is monitored through the third-party software using the v2c version.

- configuration list

According to the analysis of the user's usage scenario, the requirements are shown in the table:

Table 12-4 User Requirements Description Form

description item	illustrate
view range	Inclusion rule: OID is .1.3.6.1.2.1.1 , custom view named " system "
use version number	v2c version The custom community name is " public ", and the default port number is 161
Read and write permissions	Read permission

- configuration steps
- (1) On the global configuration interface, select the v2c version, and leave other settings as default. After the operation is complete, click <Save> .

Global Config View/Group/Community/Client Access Control Trap Settings

SNMP Service

* SNMP Version v1 v2c v3

* Local Port

* Device Location

* Contact Info

- (2) On the view/group/group/user access control interface, click <Add> in the view list, fill in the view name and O ID in the pop-up window and click <Add inclusion rule>, and click <OK> after the operation is complete .

View List

Up to 20 entries are allowed.

<input type="checkbox"/>	View Name	Action

Add
×

* View Name

OID

Add Included Rule
Add Excluded Rule

Rule/OID List
Delete Selected

Up to **100** entries are allowed.

<input type="checkbox"/>	Rule	OID	Action
No Data			

Total 0 < **1** > Go to page

Cancel
OK

(3) view /group/group/user access control interface, click <Add> in the SNMP v1/v2c community name list , fill in the community name, access mode and view in the pop-up window, and click <OK> after the operation is completed.

Global Config
View/Group/Community/Client Access Control
Trap Settings

SNMP v1/v2c Community Name List
Delete Selected

Up to **20** entries are allowed.

<input type="checkbox"/>	Community Name	Access Mode	MIB View	Action
--------------------------	----------------	-------------	----------	--------

Add
×

* Community Name

* Access Mode

* MIB View [Add View +](#)

Cancel
OK

2. v 3 version SNMP service configuration

- scenes to be used

Users need to monitor and control the equipment, and use the v3 version of the third-party software to monitor and send data to the public node (1.3.6.1.2.1) node. The security level of the v3 version adopts authentication and encryption.

- configuration list

According to the analysis of the user's usage scenario, the requirements are shown in the table:

Table 12-5 User Requirements Description Form

description item	illustrate
view range	Inclusion rule: OID is .1.3.6.1.2.1 and custom view is named " public_view "
group configuration	Group name: group Security level: authenticated and encrypted Readable view select " public_view " Writable view select " public_view " Notification view select " none "
v3 user configuration	Username: v3_user Group name: group Security level: authenticated and encrypted Authentication protocol / authentication password: MD5/Ruijie123 Encryption protocol / encryption password: AES/ Ruijie123
use version number	v3 version, default port 161

- configuration steps

- (1) Select the v3 version on the global configuration interface , change the port to 161, and set other settings to default. After the operation is complete, click <Save>.

Global Config View/Group/Community/Client Access Control Trap Settings

SNMP Service

* SNMP Version v1 v2c v3

* Local Port

* Device Location

* Contact Info

- (2) On the view/group/group/user access control interface, click <Add> in the view list, fill in the view name and OID in the pop-up window, click <Add Inclusion Rule>, and click <OK> after the operation is complete.

Add ×

* View Name

OID

Rule/OID List

Up to 100 entries are allowed.

<input type="checkbox"/>	Rule	OID	Action
No Data			

Total 0

(3) Click <Add> in the SNMP v3 group list, fill in the group name and security level in the pop-up window, the user has read and write permissions, select "public _view" for the readable view and read and write view, and set the notification view to none , click <OK>.

SNMP v3 Group List

Up to 20 entries are allowed.

<input type="checkbox"/>	Group Name	Security Level	Read-Only View	Read & Write View	Notification View	Action
<input type="checkbox"/>	default_group	Auth & Security	all	none	none	Edit Delete

Total 1

Add ×

* Group Name

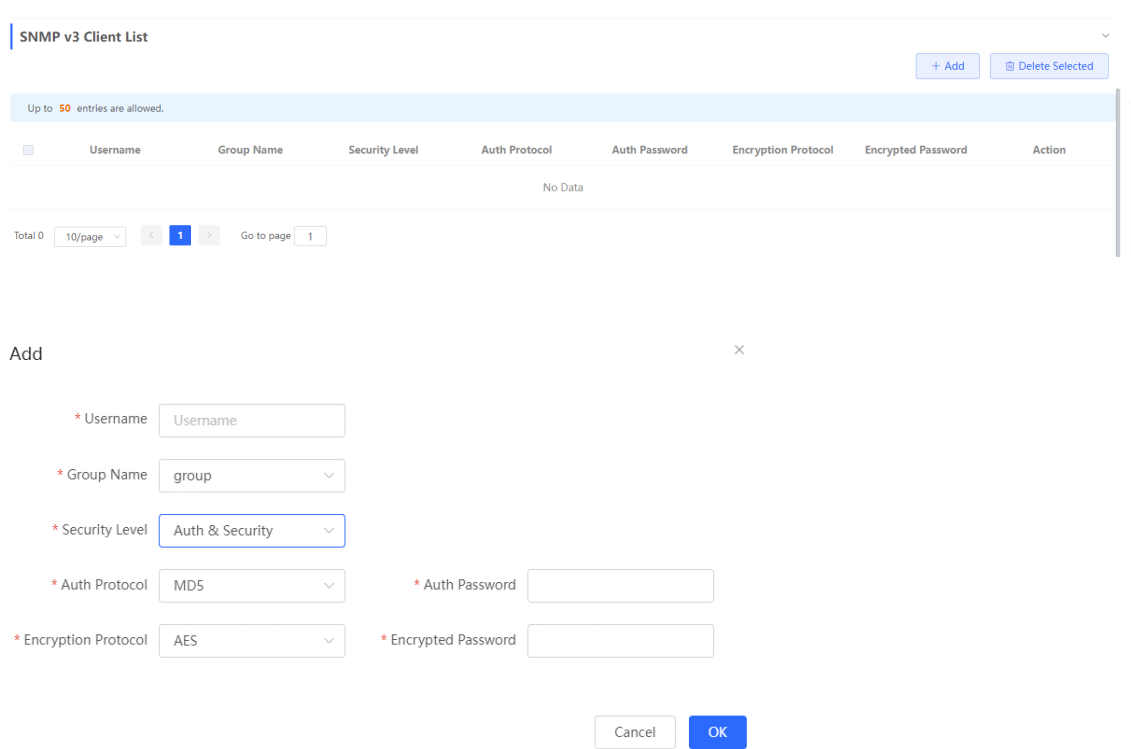
* Security Level

* Read-Only View [Add View +](#)

* Read & Write View [Add View +](#)

* Notification View [Add View +](#)

- (4) Click <Add> in the SNMP v3 user list , fill in the user name and group name in the pop-up window, the user security level adopts authentication and encryption mode, fill in the corresponding authentication protocol, authentication password, encryption protocol, and encryption password, and click <OK>.



12.4.5 trap service configuration

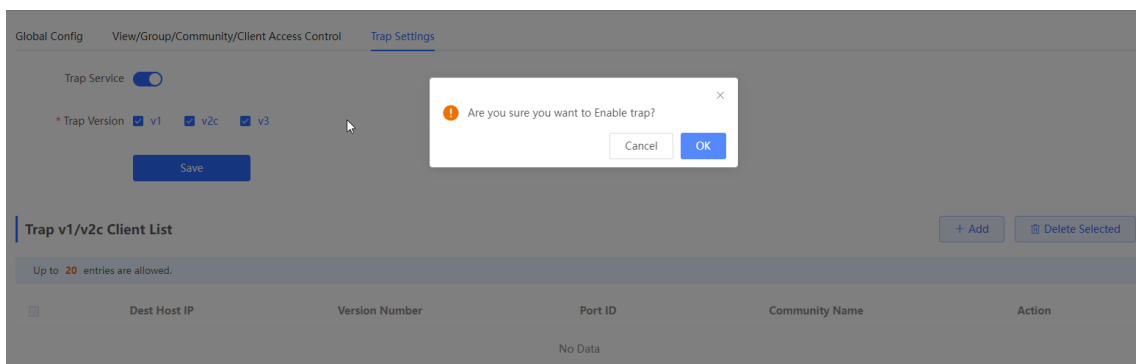
trap is a notification mechanism of SNMP (Simple Network Management Protocol) protocol, which is used to report the status and events of network devices to managers, including device status reports, fault reports, performance reports, configuration reports and security management. Trap can provide real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

1. trap open settings

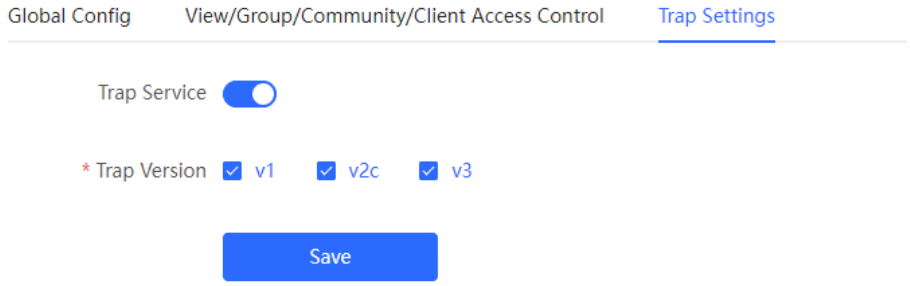
Enable the trap service and select the effective trap protocol version, including v1, v2c , and v3 .

[Entire Network Management - Page Wizard] Setting >> SNMP >> trap setting

- (1) Enable the trap service switch.



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



(2) Set the trap version.

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

(3) Click <OK>.

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

2. trap v1/v2c user configuration

- Introduction

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

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

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

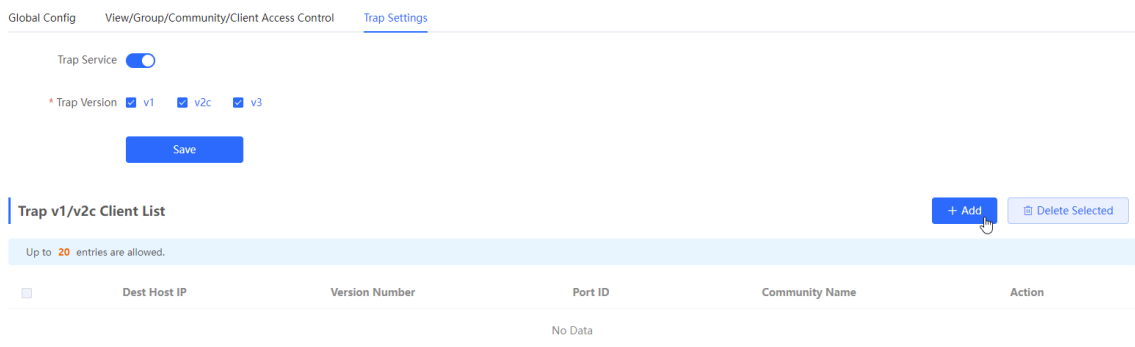
- prerequisite

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

- configuration operation

[Entire Network Management - Page Wizard] Setting >> SNMP >> trap setting

(1) Click <Add> in the Trap v1v2c User list to create a trap v1v2c user.



(2) Configure trap v1v2c user-related parameters.
set up

Add
×

* Dest Host IP

* Version Number ▾

* Port ID

* Community
Name/Username

Table 12-6 t rap v1/v2c user information description table

parameter	illustrate
destination ip	Trap peer device IP, support IPv4 / IPv6 address
version number	Trap version number, including v1 v2c
The port number	trap peer device port [1, 65535]
Group Name/User Name	The community name of the trap user at least 8 characters Contains three types of uppercase letters, lowercase letters, numbers, and special characters Does not contain admin/public/private Do not contain question marks, spaces and Chinese

Notice

- IP address of trap v1/v2c /v3 users cannot be repeated .
- Trap v1/v2c user names cannot be repeated.

(3) Click <OK>.

3. trap v 3 user configuration

- Introduction

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

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

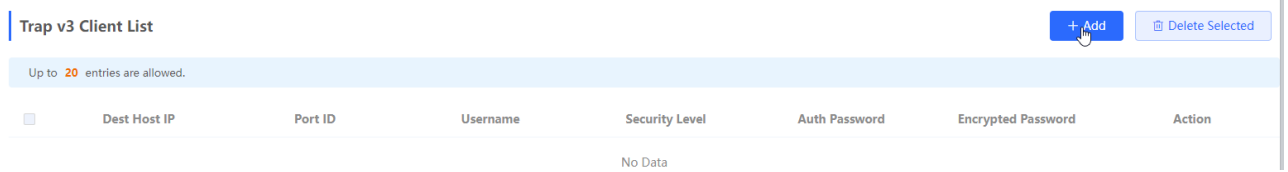
- prerequisite

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

- configuration steps

[Entire Network Management - Page Wizard] Setting >> SNMP >> trap setting

(1) Click <Add> in the "trap v3 user " list to create a trap v3 user .



(2) Configure parameters related to t rap v3 users.

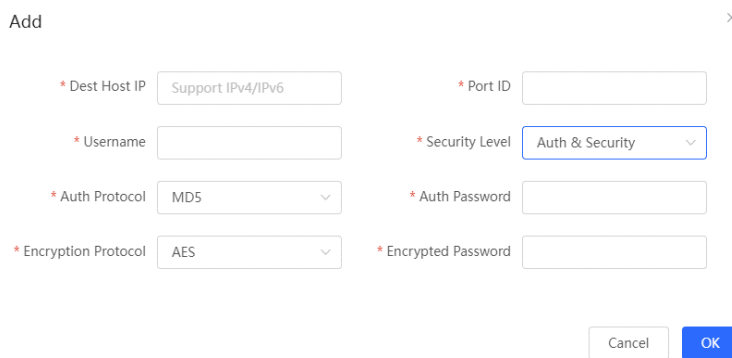


Table 12-7 trap v3 user information description table

parameter	illustrate
target host ip	trap peer device IP , support IPv4/IPv6 address
The port number	trap peer device port [1, 65535]
username	username of the trap v3 user at least 8 characters Contains three types of uppercase letters, lowercase letters, numbers, and special characters Does not contain admin/public/private Do not contain question marks, spaces and Chinese
Security Level	Trap user security level, including three levels of authentication and encryption, authentication and encryption, and authentication and no encryption
Authentication protocol, authentication password	Authentication protocols include: MD5/SHA/SHA224/SHA256/SHA384/SHA512 Authentication password: 8~ 31 characters in length, cannot contain Chinese characters, full-width characters, question marks, and spaces, and must contain at least 3 types of uppercase and lowercase letters, numbers, or special characters.

parameter	illustrate
	Note: This parameter needs to be set when the "Security Level" is "authentication and encryption" or "authentication without encryption".
encryption protocol, encryption password	Encryption protocols include: DES/AES/AES192/AES256 Encrypted password: the length is 8~ 31 characters, and cannot contain Chinese, full-width characters, question marks and spaces format , containing at least 3 types of uppercase and lowercase letters, numbers, or special characters. Note: When the "Security Level" is "Authentication and Encryption", this parameter needs to be set.

 Notice
IP of trap v1/v2c/v3 users cannot be repeated.

12.4.6 Typical configuration examples of the trap service

1. v2c version trap configuration

- scenes to be used

When the user is monitoring the device, if the device is suddenly interrupted or abnormal, the third-party monitoring software cannot detect and deal with the abnormal situation in time, so configure the device with the destination ip 192.168.110.85 and port number 166 , so that the device sends a trap of the v2c version in case of an exception.

- configuration list

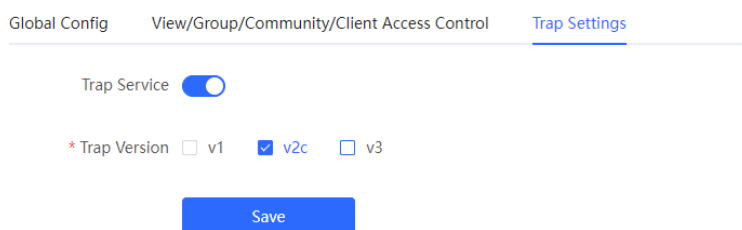
According to the analysis of the user's usage scenario, the requirements are shown in the table:

Table 12-8 User Requirements Description Form

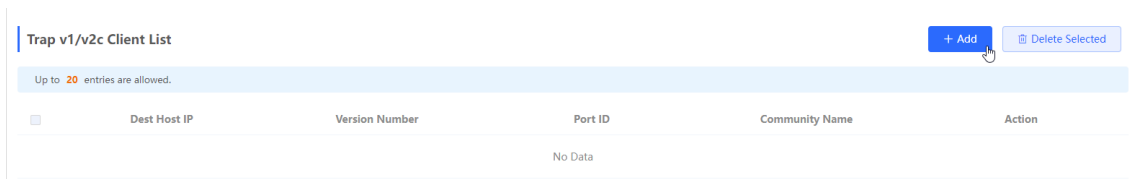
description item	illustrate
IP and port number	The target host IP is "192.168.110.85" , and the port number is "166" .
use version number	Select v2 version
Group Name / User Name	Trap_public

- configuration steps

(1) Select the v2c version on the trap setting interface , click <Save> ,



(2) Click <Add> in the " trap v1 / v2c user list " .



(3) Fill in the target host IP, version number, port number, user name and other information, and click <OK> after the configuration is complete .

Add
×

* Dest Host IP

* Version Number

* Port ID

* Community

Name/Username

2. V3 version trap configuration

- scenes to be used

When the user is monitoring the device, if the device is suddenly interrupted or abnormal, the third-party monitoring software cannot detect and deal with the abnormal situation in time, so configure the device with the destination ip 1 92. 1 68.110.87 and the port number 1 67 , and use the more secure v3 version to send traps.

- configuration list

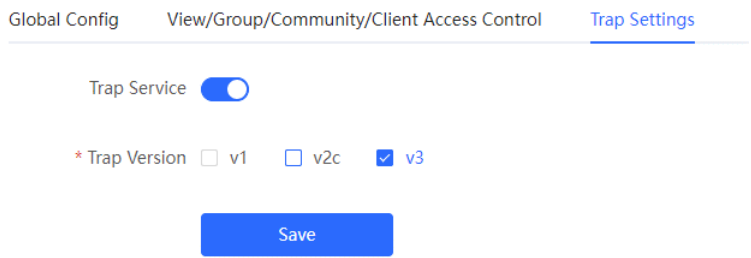
According to the analysis of the user's usage scenario, the requirements are shown in the table:

Table 12-9 User Requirements Description Form

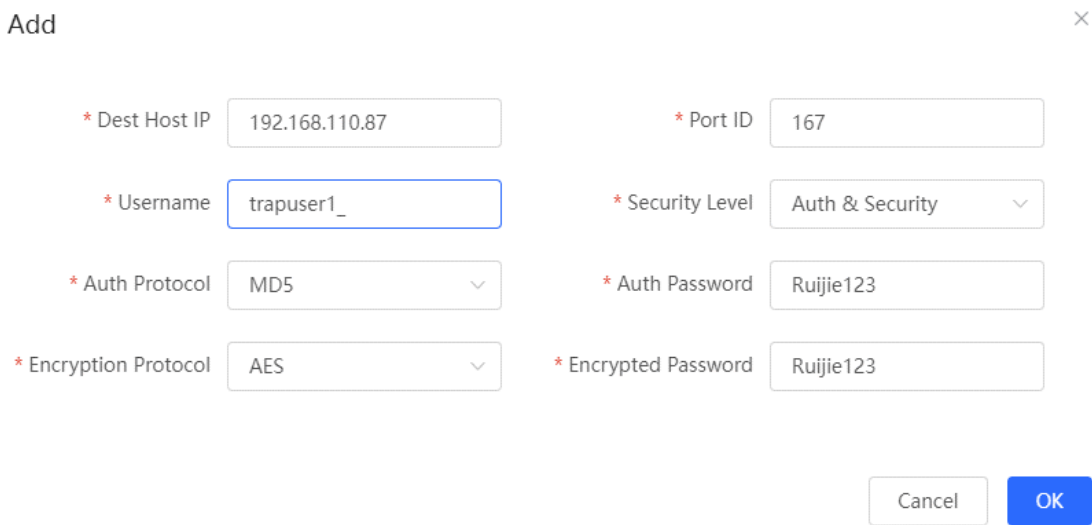
description item	illustrate
IP and port number	The target host IP is "192.168.110.87 " , and the port number is "167" .
Use version number, username	Select the v3 version, the user name is "trapv3_public"
Authentication Protocol / Encryption Protocol	Authentication protocol / authentication password: MD5/Ruijie123
Encryption Protocol / Encryption Cipher	Encryption protocol / encryption password: AES/ Ruijie123

- configuration steps

(1) Select the v3 version on the trap setting interface , and click <Save> .



- (2) Click <Add> in the trap v3 user list .
- (3) Fill in the target host IP , port number, user name and other information, and click <OK> after the configuration is complete.



12.5 Configure 802.1x authentication

12.5.1 Function introduction

IEEE802.1x (Port -Based Network Access Control) is a port-based network access control standard that provides secure access services for LANs.

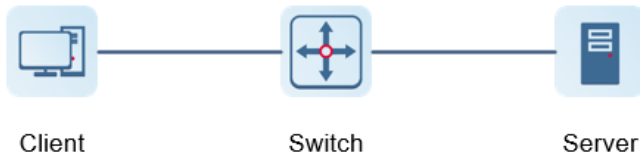
IEEE 802 LAN , as long as users can connect to network devices, they can directly access network resources without authentication and authorization. This uncontrolled behavior will bring security risks to the network. The IEEE 802.1x protocol was proposed to solve the security problem of 802 LAN.

802.1x supports Authentication , Authorization , and Accounting three security applications, referred to as AAA .

- Authentication : Authentication, used to determine whether users can obtain access rights and restrict illegal users;
- Authorization : Authorization, which services authorized users can use, and control the rights of legitimate users;
- Accounting : Accounting, recording the use of network resources by users, and providing a basis for charging.

802.1x can be deployed in a network that controls access users to implement authentication and authorization services for access users.

802.1x system is a typical Client/Server structure, including three entities: client, access device and authentication server. A typical architecture diagram is shown in the figure.



- The client is generally a user terminal device, and the user can initiate 802.1X authentication by starting the client software. The client must support the Extensible Authentication Protocol over LANs (EAPoL).
- AP or switching device) that supports the 802.1x protocol . It provides a port for the client to access the LAN. The port can be a physical port or a logical port.
- The authentication server is used to implement user authentication, authorization, and accounting, and it is usually a RADIUS server.

12.5.2 Configuration 802.1x

【Local Management - Page Wizard】 Security > 802.1x Authentication > Auth _Config _

(1) Click the " Global 802.1x " switch, the system prompts to confirm whether to enable it, click <Configure>.

The screenshot shows a web-based configuration page for 802.1x authentication. At the top, there are four tabs: 'Auth Config' (selected), 'Port', 'RADIUS Server Management', and 'Wired User List'. Below the tabs is a section titled 'Global Config'. Under 'Global Config', there is a toggle switch for 'Global 802.1x' which is currently turned on. Below the toggle is the text 'Authentication'. Under 'Authentication', there is a text input field labeled 'Auth Server' containing the text 'Add a server to be authenticated.' and a blue link labeled 'Edit' with a pencil icon. Below the input field is a dashed line with the text 'Advanced Settings' in blue. At the bottom of the configuration area is a large blue button labeled 'Configure'.

Click Advanced Settings to configure parameters such as Guest VLAN .

Auth Config Port RADIUS Server Management Wired User List

Guest Vlan

* EAP-Request Packet

Retransmission Count

* Quiet Period s

Client Packet
* Timeout Duration s

Client Packet
* Timeout Duration s

* EAP-Request Packet s

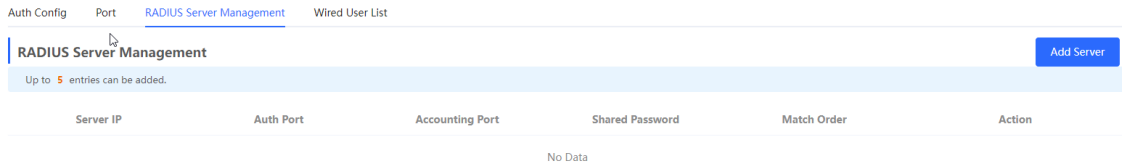
Interval

parameter	illustrate
Server Escape	If the server disconnection is detected, all users will be allowed to access the Internet
Re-authentication	Require clients to re-authenticate at certain intervals to ensure network security
Guest VLAN	Provide a VLAN for unauthenticated clients to restrict their access
EAP-Request Packet Retransmission Count	Define the number of times the EAP request message will be retransmitted when no response is received, value range: 1- 10 times
Quiet Period	During the authentication process, the idle time between the client and the server does not exchange authentication messages, value range: 0- 65535 seconds
Client Packet Timeout Duration	The time limit for the server to wait for the response from the client, exceeding this time will be considered as an authentication failure, value range: 1-65535 seconds
Client Packet Timeout Duration	The time limit for the client to wait for the server to respond, exceeding this time will be considered as an authentication failure, value range: 1- 65535 seconds
EAP-Request Packet Interval	Define the time interval between sending EAP request messages to control the rate of the authentication process, value range: 1-65535 seconds

(2) add server

Before configuration, please confirm :

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



Add ×

* Server IP

* Auth Port

* Accounting Port ?

* Shared Password

* Match Order ?

parameter	Reference without translation	illustrate
Server IP	server address	Radius server address.
Auth Port	authentication port	The port number used for accessing user authentication on the Radius server.
Accounting Port	billing port	The port number used to access the accounting process on the Radius server.
Shared Password	shared password	Radius server shared key.
Match Order	matching order	The system supports adding up to 5 Radius servers. The higher the matching order value is, the higher the priority is.

(3) Set up the server and click <Save> .

Server global configuration

* Packet Retransmission Interval s

* Packet Retransmission Count time

Server Detection

MAC Address Format ⓘ

[Save](#)

parameter	reference - do not translate	illustrate
Packet Retransmission Interval	packet retransmission interval	Configure the interval for the device to send request packets before confirming that there is no response from RADIUS
Packet Retransmission Count	Packet retransmission times	Configure the number of times the device sends request packets before confirming that there is no response from RADIUS
Server Detection	server detection	If this function is enabled, you need to set "Server Detection Period", "Server Detection Times" and "Server Detection Username". It is used to determine the status of the server, so as to decide whether to enable functions such as escape .
MAC Address Format	M AC address format	the MAC address format of RADIUS attribute No. 31 (Calling- Stationg -ID). The following formats are supported: <ul style="list-style-type: none"> ● Dotted hexadecimal format, such as 00d0.f8aa.bbcc ● IETF format, such as 00-D0-F8-AA-BB-CC ● No format (default) , eg 00d0f8aabbcc

(4) Configure the effective interface , click interface configuration , click modify or batch configuration after a single interface , and edit the authentication parameters of the interface .

Auth Config [Port](#) RADIUS Server Management Wired User List

Port List [Batch Config](#)

Interface	Port Authentication	Auth Method	Auth Mode	Action
Gi1	Off	disable	multi-auth	Edit
Gi2	Off	disable	multi-auth	Edit

Edit
×

802.1x Authentication

Auth Method

Auth Mode

Guest Vlan

* User Count Limit per
Port

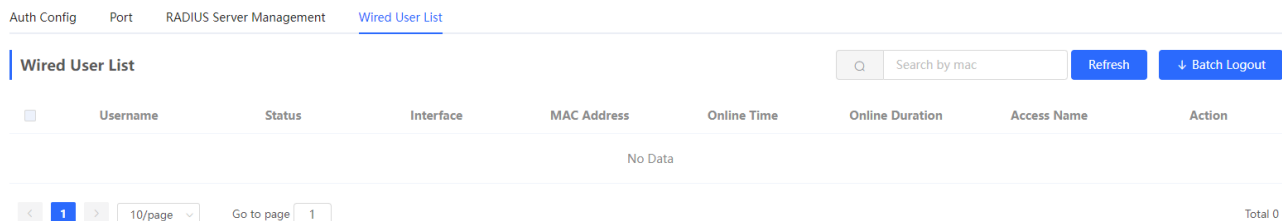
parameter	reference - do not translate	illustrate
802.1x Authentication	802.1x certification	When enabled, the selected interface will enable 8.02.1x authentication .
Auth Method	authentication method	<p>disable : Turn off the authentication method , which has the same effect as turning off the 802.1x authentication switch</p> <p>force- auth : Mandatory authentication , the client can directly access the Internet without a password</p> <p>force- unauth : Force no authentication, the client cannot be authenticated, nor can it access the Internet</p> <p>auto : automatic authentication, the device needs to be authenticated, and can access the Internet after passing the authentication</p> <p>It is recommended to select the auto authentication method .</p>
Auth Mode	authentication mode	<p>multi- auth : supports multiple devices using the same port for authentication, but each device needs to be authenticated independently</p> <p>multi- host : Multiple devices are allowed to share the same port. As long as one user passes the authentication, subsequent users can access the Internet</p> <p>single-host : Each port only allows one device to be authenticated, and can access the Internet after successful authentication</p>

parameter	reference - do not translate	illustrate
Guest Vlan	Guest VLAN	<p>When enabled, devices that fail authentication will be dynamically assigned to the specified Guest VLAN</p> <p>Notice</p> <p>You need to create a VLAN ID first and apply it to the interface , then in Security Management >> 802.1x Authentication >> Advanced settings in the authentication configuration enable Guest VLAN and enter the ID</p>
User Count Limit per Port	Maximum number of users per port	<p>Limit the number of users under the interface</p> <p>Product Difference Description</p>

12.5.3 View the list of wired authentication users

8.02.1x function is configured on the entire network and a terminal is authenticated and connected to the network, you can view the list of authenticated users.

【Local Management - Page Wizard】 Security Management >> 802.1x Authentication to obtain specific user information.



Click <Refresh> to get the latest user list information.

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

12.6 Anti-ARP Spoofing

12.6.1 Overview

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

12.6.2 Procedure

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

1. Enabling Anti-ARP Spoofing

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

i note

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

Anti-ARP Spoofing

Description: Anti-ARP Spoofing prevents hosts from spoofing the source IP address of the ARP packets to be the IP address of the gateway.
Note: Anti-ARP Spoofing is generally configured on a downlink port.

Anti-ARP Spoofing Add Delete Selected

Up to **256** entries can be added.

<input type="checkbox"/>	IP	Port	Action
No Data			

Add ×

* IP

* Select Port:

Available Unavailable Aggregate Uplink Copper Fiber

1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37
2	4	6	8	10	12	14	16	18	20	22	24	26	28	30	32	34	36	38

Note: You can click and drag to select one or more ports. [Select All](#) [Inverse](#) [Deselect](#)

2. Disabling Anti-ARP Spoofing

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

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

Anti-ARP Spoofing
Description: Anti-ARP Spoofing prevents hosts from spoofing the source IP address of the ARP packets to be the IP address of the gateway.
Note: Anti-ARP Spoofing is generally configured on a downlink port.

Anti-ARP Spoofing Add Delete Selected

Up to 256 entries can be added.

<input checked="" type="checkbox"/>	IP	Port	Action
<input checked="" type="checkbox"/>	172.30.102.1	Gi15	Edit Delete

13 Diagnostics

13.1 Info Center

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

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

The screenshot shows the Ruijie Rcycc web interface. The 'Info Center' is selected in the left sidebar. The main content area displays 'Port Info' for interface Gi1. The port status is 'Connected'. The actual rate is 4957kbps, and the negotiation rate is 1000M. The flow control is set to 'Disable'. The interface mode is 'Trunk Port'. Below the port info, there is a 'VLAN Info (SVI&Routed Port)' section with a table showing VLAN configurations.

VLAN ID	Interface	IP Address	DHCP Address Pool	Remarks
VLAN1				
VLAN888				
VLAN2001				
VLAN3011				
VLAN3012				
VLAN3013				
Routed Port Gi23				

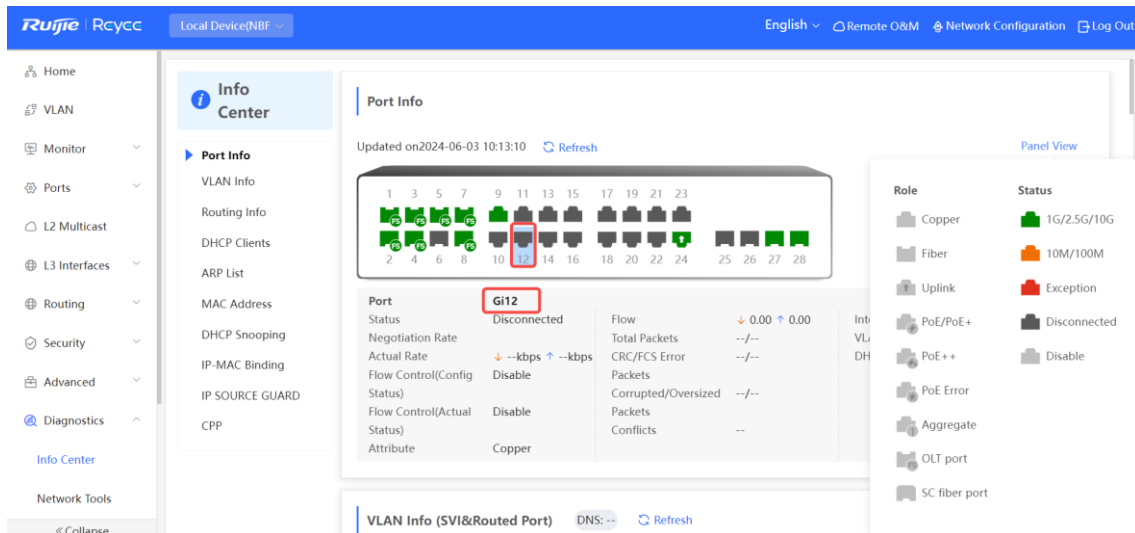
13.1.1 Port Info

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

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

i note

- To configure the flow control of the port or the optical/electrical attribute of a combo port, see [Port Configuration4.2 Port Configuration](#).
- To configure the L2 mode of the port and the VLAN to which it belongs, see [Configuring Port VLAN3.5.3 Configuring Port VLAN](#).



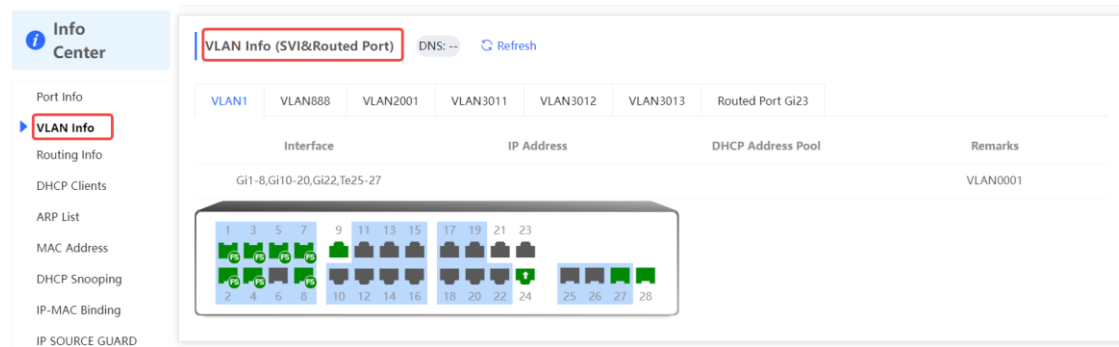
13.1.2 VLAN Info

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

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

i **note**

- To configure VLAN, see [0](#).
- To configure SVI ports and routed ports, see [Setting an L36.1](#) [Setting an L3](#).



13.1.3 Routing Info

⚠ **Caution**

If the device does not support L3 functions (such as RG-NBF2100 Series), this type of information is not displayed.

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

Displays the routing information on the device. The search box in the upper-right corner supports finding route entries based on IP addresses.

i note

To set up static routes, see [Configuring Static Routes](#).

The screenshot shows the 'Info Center' sidebar on the left with 'Routing Info' and 'DHCP Clients' highlighted. The main content area is divided into two sections:

- Routing Info:** A table with columns 'Interface', 'IP Address', 'Subnet Mask', and 'Next Hop'. It contains 'No Data' and has a search bar for 'IP Address' and a 'Refresh' button.
- DHCP Clients:** A table with columns 'Hostname', 'IP Address', 'MAC Address', 'Lease Time (Min)', and 'Status'. It contains 'No Data' and has a search bar for 'Hostname/IP Add.' and a 'Refresh' button.

13.1.4 DHCP Clients

⚠ Caution

If the device does not support L3 functions (such as RG-NBF2100 Series Switches), this type of information is not displayed.

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

Displays the IP address information assigned to endpoints by the device as a DHCP server.

i note

To configure DHCP server related functions, see [Configuring the DHCP](#).

The screenshot shows the 'Info Center' sidebar on the left with 'DHCP Clients' and 'ARP List' highlighted. The main content area is divided into two sections:

- DHCP Clients:** A table with columns 'Hostname', 'IP Address', 'MAC Address', 'Lease Time (Min)', and 'Status'. It contains 'No Data' and has a search bar for 'Hostname/IP Add.' and a 'Refresh' button.
- ARP List:** A table with columns 'Interface', 'IP Address', 'MAC Address', 'Type', and 'Reachable'. It contains one entry:

Interface	IP Address	MAC Address	Type	Reachable
VLAN888	192.168.88.197	c0:a4:76:1b:0f:1b	Dynamic	Yes

 It also has a search bar for 'IP Address/MAC A' and a 'Refresh' button.

13.1.5 ARP List

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

Displays ARP information on the device, including dynamically learned and statically configured ARP mapping entries.

note

To bind dynamic ARP or manually configure static ARP, see [Configuring a Static6.4](#) [Configuring a Static](#).

The screenshot shows the 'ARP List' page in the 'Info Center'. The left sidebar has 'ARP List' highlighted. The main content area has a search bar and a table of ARP entries. The table has the following data:

Interface	IP Address	MAC Address	Type	Reachable
VLAN888	192.168.88.197	c0:a4:76:1b:0f:1b	Dynamic	Yes
VLAN888	192.168.88.174	c0:a4:76:1b:0e:f2	Dynamic	Yes
VLAN888	192.168.88.217	c0:a4:76:1b:0f:1c	Dynamic	Yes
VLAN888	192.168.88.73	00:ee:4c:21:14:0a	Dynamic	Yes
VLAN888	192.168.88.166	00:e0:4c:21:71:21	Dynamic	Yes
VLAN888	192.168.88.77	48:81:d4:fe:8a:3a	Dynamic	Yes
VLAN888	192.168.88.96	00:e0:4c:21:71:26	Dynamic	Yes
VLAN888	192.168.88.186	c0:a4:76:1b:0f:0e	Dynamic	Yes
VLAN888	192.168.88.209	c0:a4:76:1b:0f:17	Dynamic	Yes
VLAN888	192.168.88.65	f0:74:8db1:4c:4f	Dynamic	Yes

13.1.6 MAC Address

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

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

note

To configure and manage the MAC address, see [MAC Address Management3.3](#) [MAC Address Management](#).

The screenshot shows the 'MAC Address' page in the 'Info Center'. The left sidebar has 'MAC Address' highlighted. The main content area has a search bar and a table of MAC addresses. The table has the following data:

Interface	MAC Address	Type	VLAN ID
Gi1	48:81:D4:FE:A8:B2	Dynamic	1
Gi2	48:81:D4:FE:88:A5	Dynamic	1
Gi4	00:E0:70:E3:B7:2E	Dynamic	3012
Gi5	70:85:C4:5B:DC:1D	Dynamic	3013
Gi3	48:81:D4:FE:88:A8	Dynamic	1
Gi4	BC:0F:F3:76:7A:31	Dynamic	3012
Te28	52:4B:ED:7F:8B:EF	Dynamic	2001
Gi5	14:14:4B:73:F9:68	Dynamic	3013
Gi4	B8:CA:3A:97:E1:98	Dynamic	3012
Gi5	14:14:4B:73:F9:67	Dynamic	3013

13.1.7 DHCP Snooping

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

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

i **note**

To modify DHCP Snooping related configuration, see [_DHCP Snooping7.1 DHCP Snooping_](#).

Info Center

DHCP Snooping

DHCP Snooping: **Enabled** Option82: **Disabled** Trusted Port: Gi24,Te27,Te28 Refresh

DHCP Snooping Binding Entries from the Trusted Port

Interface	IP Address	MAC Address	VLAN ID	Lease Time (Min)
Gi4	192.168.89.92	00:0E:C6:04:A0:EC	888	480
Gi9	192.168.88.167	00:D0:F5:20:08:97	888	480
Gi5	192.168.88.119	00:D0:FA:A1:00:23	888	480
Gi5	192.168.88.164	00:E0:4C:21:70:03	888	480
Gi5	192.168.88.89	00:E0:4C:21:71:12	888	480
Gi5	192.168.88.137	00:E0:4C:21:71:13	888	480
Gi5	192.168.88.70	00:E0:4C:21:71:14	888	480
Gi5	192.168.88.142	00:E0:4C:21:71:15	888	480
Gi5	192.168.88.110	00:E0:4C:21:71:17	888	480
Gi5	192.168.88.123	00:E0:4C:21:71:18	888	480

1 2 3 4 5 6 ... 62 > 10/page Go to page 1 Total 618

13.1.8 IP-MAC Binding

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

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

i **note**

To add or modify the IP-MAC binding, see [_IP-MAC Binding7.5 IP-MAC Binding_](#).

Info Center

IP-MAC Binding

Tips: Up to **500** entries can be added. Search by IP Address Refresh

Port	IP Address	MAC Address
No Data		

IP SOURCE GUARD

Tips: Up to **1900** entries can be added. Search by IP Address Refresh

Interface	Rule	IP Address	MAC Address	VLAN ID	Status
Gi9	IP Address	192.168.88.167	00:D0:F5:20:08:97	888	Inactive
Gi4	IP Address	10.52.40.70	28:D0:F5:72:A9:5D	3012	Inactive
Gi5	IP Address	192.168.88.166	00:E0:4C:21:71:21	888	Inactive

13.1.9 IP Source Guard

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

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

Note

To configure IP Source Guard function, see [IP Source Guard7.6 IP Source Guard](#).

Interface	Rule	IP Address	MAC Address	VLAN ID	Status
Gi9	IP Address	192.168.88.167	00:D0:F5:20:08:97	888	Inactive
Gi4	IP Address	10.52.40.70	28:D0:F5:72:A9:5D	3012	Inactive
Gi5	IP Address	192.168.88.166	00:E0:4C:21:71:21	888	Inactive
Gi5	IP Address	10.52.48.30	C0:88:E6:1D:89:51	3013	Inactive
Gi4	IP Address	192.168.89.125	80:05:88:99:BC:FD	888	Inactive
Gi5	IP Address	192.168.88.132	00:E0:4C:21:76:66	888	Inactive
Gi5	IP Address	10.52.48.90	44:6E:55:22:44:66	3013	Inactive
Gi5	IP Address	10.52.48.172	00:74:9C:D8:92:19	3013	Inactive
Gi3	IP Address	192.168.88.88	48:81:D4:FE:88:E4	888	Inactive
Gi2	IP Address	192.168.88.101	48:81:D4:FE:A8:D1	888	Inactive

13.1.10 CPP Info

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

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

EtherType Value	Rate	Current Rate	Total messages
bpdu	60pps	0pps	0
lldp	50pps	2pps	5124000
rldp	50pps	0pps	0
lacp	600pps	0pps	0
rdla	600pps	0pps	0
arp	400pps	14pps	84656427
dhcp	600pps	3pps	4350407
icmp	600pps	0pps	121
macc	600pps	24pps	86588720
mqtt	600pps	2pps	4540492

13.2 Network Tools

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

13.2.1 Ping

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

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

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

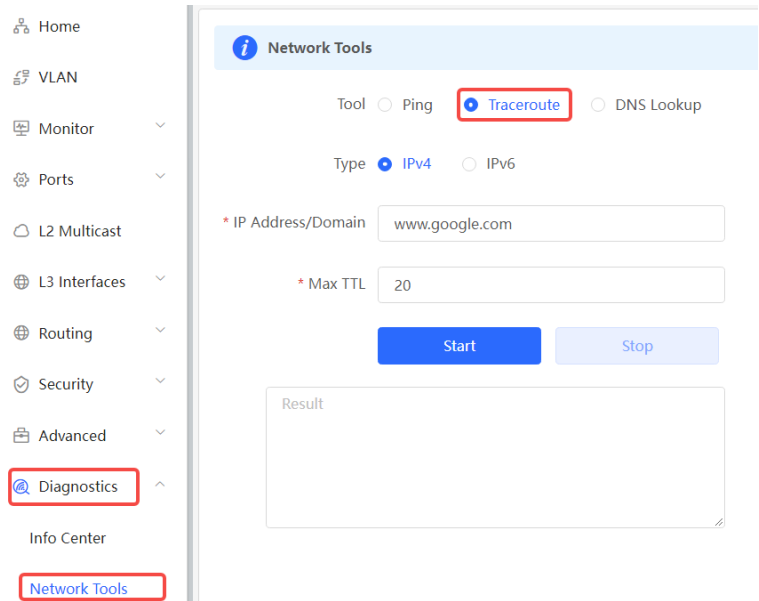
The screenshot shows the Ruijie Rcycc web interface. The left sidebar contains navigation options: Home, VLAN, Monitor, Ports, L2 Multicast, L3 Interfaces, Routing, Security, Advanced, Diagnostics (highlighted with a red box), and Info Center. Below the sidebar is a 'Network Tools' button (also highlighted with a red box). The main content area is titled 'Network Tools' and features three radio buttons for 'Tool': 'Ping' (selected and highlighted with a red box), 'Traceroute', and 'DNS Lookup'. Below these are radio buttons for 'Type': 'IPv4' (selected) and 'IPv6'. The configuration fields include: '* IP Address/Domain' with the value 'www.google.com', '* Ping Count' with the value '4', and '* Packet Size' with the value '64' and a 'Bytes' label. There are 'Start' and 'Stop' buttons. At the bottom, there is a 'Result' text area.

13.2.2 Traceroute

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

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

Select **Traceroute** as the diagnosis mode, enter a destination IP address or the maximum TTL value used by the URL and traceroute , and click **Start** .

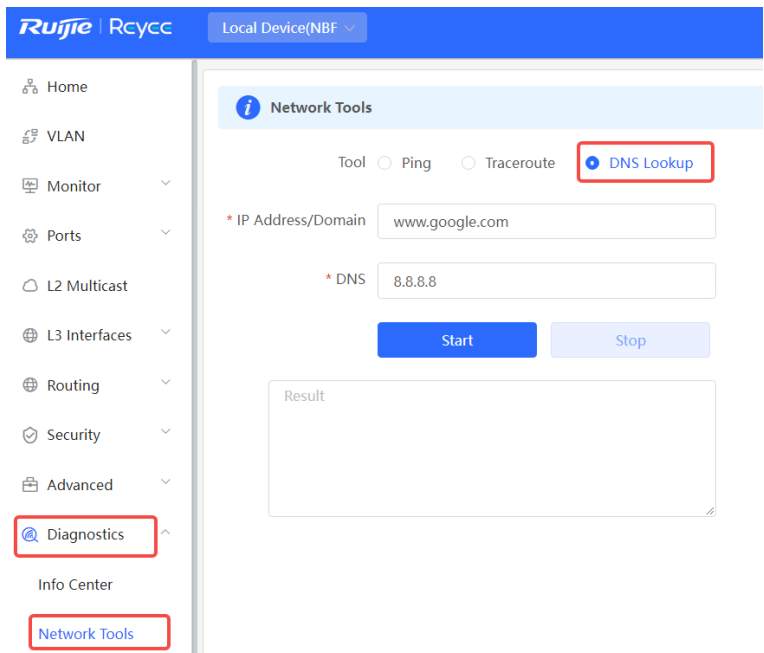


13.2.3 DNS Lookup

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

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

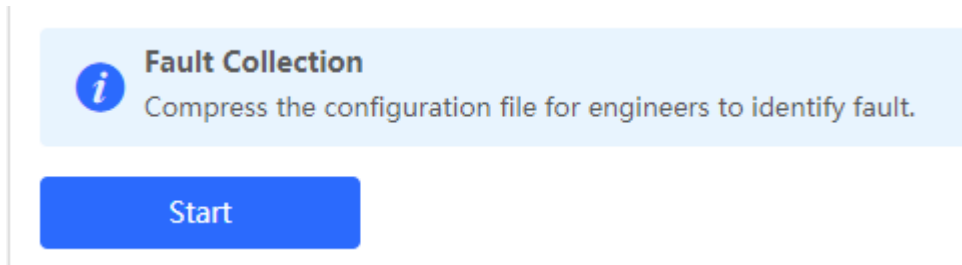
Select **DNS Lookup** as the diagnosis mode, enter a destination IP address or URL, and click **Start** .



13.3 Fault Collection

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

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

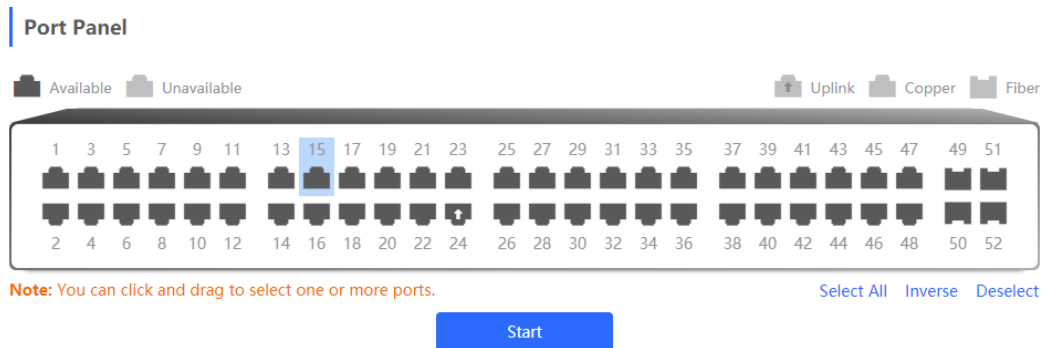


13.4 Cable Diagnostics

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

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

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



Result

Port	Cable Length (cm)	Result
GI15	700	OK

⚠ Caution

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

13.5 System Logs

Choose **Local Device > 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. You can search for specified logs by fault type, faulty module, and keyword in fault information.

i **System Logs**
View system logs.

Log List

Time	Type	Module	Details
May 18 18:52:37	kern.crit	kernel	%Port-2: GigabitEthernet12 link up
May 18 18:52:37	local.info	syslog	%L3-6: Manage VLAN 1 change to UP
May 18 18:52:37	kern.crit	kernel	%Port-2: GigabitEthernet13 link up
May 18 18:52:37	kern.crit	kernel	%Port-2: GigabitEthernet17 link up
May 18 18:52:38	kern.crit	kernel	%Port-2: GigabitEthernet22 link up

13.6 Alerts

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

i **note**

Choose **Network > Alerts** to view the alert information of other devices in the network.

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

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

⚠ **Caution**

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

i **Alerts**

No Alert

Current Alert
Removed Alert

Table 13-1 Alert Types and Product Support

Alert Type	Description	Support Description
Addresses in the DHCP address pool are to be exhausted.	The device acts as a DHCP server, and the number of allocated addresses is about to reach the maximum number of addresses that can be allocated in the address pool.	It is applicable only to devices that support L3 functions. Products that do not support L3 functions such as RG-NBF2100 Series Switches do not support this type of alert.
The IP address of the local device conflicts with that of another device.	The IP address of the local device conflicts with that of another client on the LAN.	NA
An IP address conflict occurs on downlink devices connected to the device.	Among the devices connected to the current device on the LAN, an IP address conflict occurs on one or more devices.	NA
The MAC address table is full of entries.	The number of L2 MAC address entries is about to reach the hardware capacity limit of the product.	NA
The ARP table is full of ARP entries.	The number of ARP entries on the network exceeds the ARP capacity of the device.	NA
The device has a loop alarm.	A network loop occurs on the LAN.	NA

14 FAQs

14.1 Failing to log in to the Eweb Management System

- (1) Confirm that the network cable is correctly connected to the port of the device, and the corresponding indicator is flashing or steady on.
- (2) Before accessing the Web management system, it is recommended to set the PC to use a static IP address and set the IP of the computer to be in the same network segment as the IP of the device (the default IP of the device is 10.44.77.200 and the subnet mask is 255.255.255.0) For example, set the IP address of the computer to 10.44.77.100 and the subnet mask to 255.255.255.0.
- (3) Run the ping command to check the connectivity between the PC and the device.
- (4) If you still cannot log in to the **Device Management** page after the preceding steps, restore the device to factory settings.

14.2 Password Lost and Restoration of Factory Settings

If you forget the password, hold down the **Reset** button on the device panel for more than 5s when the device is powered on, release the button after the system indicator blinks, and the device will be restored to factory settings. The device reboot can use the default management IP (10.44.77.200) to log into the device Web and select whether to restore the backup configuration according to the prompt message.

Select **Reset Backup**: The configuration will be restored to a backup status and only the login password will be restored to the default password.

Select **Delete Backup**: To restore factory settings, that is, passwords and configurations will be deleted.

