

Ruijie Reyee RG-NBF Series Switches ReyeeOS 2.290

Configuration Guide



Document Version: V1.0 Date: July 8, 2024 Copyright © 2024 Ruijie Networks

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.



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: <u>https://reyee.ruijie.com/en-global/support</u>
- Case Portal: https://www.ruijienetworks.com/support/caseportal
- Community: <u>https://community.ruijienetworks.com</u>
- Technical Support Email: service rj@ruijienetworks.com
- Online Robot/Live Chat: <u>https://reyee.ruijie.com/en-global/rita</u>

Conventions

1. GUI Symbols

Interface symbol	Description	Example
Boldface	 Button names Window names, tab name, field name and menu items Link 	 Click OK. Select Config Wizard. 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

PrefaceI
1 Change Description1
1.1 ReyeeOS 2.2901
1.1.1 Hardware Change1
1.1.2 Software Feature Change1
2 Login1
2.1 Configuration Environment Requirements1
2.1.1 PC1
2.2 Logging in to the Web Page1
2.2.1 Connecting to the Device1
2.2.2 Logging in to the Web Page1
2.2.3 Frequently-Used Controls on the Web Page2
2.3 Quick Setup4
2.3.1 Configuration Preparations4
2.3.2 Procedure
2.4 Work Mode5
2.5 Switching the Management Mode6
3 Network management
3.1 Overviewing Network Information8
3.2 Viewing Networking Information8
3.3 Adding Networking Devices11
3.3.1 Wired Connection11
3.4 Managing Networking Devices12

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	
4.3.1 Overview	
4.3.2 Displaying the MAC Address Table	
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	
4.7 DBA	37

4.7.1 Overview	37
4.7.2 Bandwidth Allocation Mechanism	37
4.7.3 Configuring DBA	
4.8 VLAN	
4.8.1 VLAN Overview	
4.8.2 Creating a VLAN	
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 Services87	1
7.3.2 Viewing the DHCP Client82	2
7.3.3 Configuring Static IP Addresses Allocation82	2
7.3.4 Configuring the DHCP Server Options83	3
7.4 Configuring the DHCPv6 Server85	5
7.4.2 Viewing DHCPv6 Clients86	3
7.4.3 Configuring the Static DHCPv6 Address86	3
7.5 Configuring the IPv6 Neighbor List87	7
7.6 Configuring a Static ARP Entry88	3
8 Configuring Route)
8.1 Configuring Static Routes90)
8.2 Configuring the IPv6 Static Route9 ²	1
8.3 Configuring RIP92	2
8.3.1 Configuring RIP Basic Functions92	2
8.3.2 Configuring the RIP Port94	4
8.3.3 Configuring the RIP Global Configuration98	5
8.3.4 Configuring the RIP Route Redistribution List	3
8.3.5 Configuring the Passive Interface97	7
8.3.6 Configuring the Neighbor Route98	3
8.4 Configuring RIPng98	3
8.4.1 Configuring RIPng Basic Functions	3
8.4.2 Configuring the RIPng Port100)
8.4.3 Configuring the RIPng Global Configuration107	1
8.4.4 Configuring the RIPng Route Redistribution List102	2

8.4.5 Configuring the RIPng Passive Interface	102
8.4.6 Configuring the IPv6 Aggregate Route	103
8.5 OSPFv2	
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
8.7 Routing Table Info	
	123
9 Security	123
9 Security 9.1 DHCP Snooping	123 123 123
9 Security 9.1 DHCP Snooping 9.1.1 Overview	
9 Security 9.1 DHCP Snooping 9.1.1 Overview 9.1.2 Standalone Device Configuration	
9 Security 9.1 DHCP Snooping 9.1.1 Overview 9.1.2 Standalone Device Configuration 9.1.3 Batch Configuring Network Switches	
9 Security 9.1 DHCP Snooping 9.1.1 Overview 9.1.2 Standalone Device Configuration 9.1.3 Batch Configuring Network Switches 9.2 Storm Control	
 9 Security 9.1 DHCP Snooping 9.1.1 Overview 9.1.2 Standalone Device Configuration 9.1.3 Batch Configuring Network Switches 9.2 Storm Control 9.2.1 Overview 	
9 Security 9.1 DHCP Snooping 9.1.1 Overview 9.1.2 Standalone Device Configuration 9.1.3 Batch Configuring Network Switches 9.2 Storm Control 9.2.1 Overview 9.2.2 Procedure	

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 Diagnostics	
	164
11.1 Info Center	164 164
11.1 Info Center	164 164 165
11.1 Info Center 11.1.1 Port Info 11.1.2 VLAN Info	164 164 165 165
11.1 Info Center 11.1.1 Port Info 11.1.2 VLAN Info 11.1.3 Routing Info	164 164 165 165 166
11.1 Info Center 11.1.1 Port Info 11.1.2 VLAN Info 11.1.3 Routing Info 11.1.4 DHCP Clients	164 164 165 165 166 166
11.1 Info Center 11.1.1 Port Info 11.1.2 VLAN Info 11.1.3 Routing Info 11.1.4 DHCP Clients 11.1.5 ARP List	164 164 165 165 166 166 167
11.1 Info Center 11.1.1 Port Info 11.1.2 VLAN Info 11.1.3 Routing Info 11.1.4 DHCP Clients 11.1.5 ARP List 11.1.6 MAC Address	164 164 165 165 166 166 167 167
11.1 Info Center 11.1.1 Port Info 11.1.2 VLAN Info 11.1.3 Routing Info 11.1.4 DHCP Clients 11.1.5 ARP List 11.1.6 MAC Address 11.1.7 DHCP Snooping	164 164 165 165 166 167 167 167 168

	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	2 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	
	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	
12.6.2 Procedure	
13 Diagnostics	
13.1 Info Center	
13.1.1 Port Info	
13.1.2 VLAN Info	
13.1.3 Routing Info	
13.1.4 DHCP Clients	
13.1.5 ARP List	
13.1.6 MAC Address	
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 Settings
--

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.

2.1 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.

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.

1 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.

	Reyce	
	*	
Log	j In	
Forgot Password?	English 🗸	

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.

Home	HCP	Sente	Static IP Addresses DHCP O	ption ARP List				
VLAN			static in Addresses Differ o			ſ		
Monitor ~	ARP	List					Search by IP Address/MAC A Q	+ Add 🗈 Delete Selected
Ports	Up	o 2000 I	P-MAC bindings can be added.					
L2 Multicast		No.	Interface	MAC Address	IP Address	Туре	Reachable	Action
L3 Interfaces		1	VLAN888	c0:a4:76:1b:0f:1b	192.168.88.197	Dynamic	Yes	∂ Bind
L3 Interfaces		2	VLAN888	c0:a4:76:1b:0e:f2	192.168.88.174	Dynamic	Yes	∂ Bind
Pv4 Config		3	VLAN888	c0:a4:76:1b:0f:1c	192.168.88.217	Dynamic	Yes	<i>∂</i> Bind
IPv6 Config		4	VLAN888	00:ee:4c:21:14:0a	192.168.88.73	Dynamic	Yes	් Bind
Routing		5	VLAN888	00:e0:4c:21:71:21	192.168.88.166	Dynamic	Yes	∂ Bind
Security ~		6	VLAN888	48:81:d4:fe:8a:3a	192.168.88.77	Dynamic	Yes	∂ Bind
Diagnostics		7	VLAN888	00:e0:4c:21:71:26	192.168.88.96	Dynamic	Yes	<i>∂</i> Bind
System ~		8	VLAN888	c0:a4:76:1b:0f:0e	192.168.88.186	Dynamic	Yes	ළු Bind
		9	VLAN888	c0ta4:76:1b:0f:17	192.168.88.209	Dynamic	Yes	∂ Bind
		10	VLAN888	f0:74:8d:b1:4c:4f	192.168.88.65	Dynamic	Yes	& Bind

2.2.3 Frequently-Used Controls on the Web Page

Control	Description
Local Device(NBS < Currently in Local Device mode.	Local Device: Allows you to configure all functions of the local device. Network: Allows you to configure common functions of all wired and wireless Reyee products in batches in an ad hoc network.
Home VLAN Monitor Y Ports Y L2 Multicast L3 Interfaces Y	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.
English ~	Click it to change the language.
C Remote O&M	Click it to log in to the MACC for remote O&M through the URL or by scanning the QR code.
	Click it to access the network setup wizard.
🔁 Log Out	Click it to log out of the web management system.
+ Add + Batch Add	Click Add or Batch Add to add one or more table entries in the dialog box that appears. After adding the table entries, yo can view the added table entries on this page.
i Delete Selected	Click it to delete the selected table entries in batches.
Search by MAC V Example: 00:11:22:33:44:5 Q Search	Quickly locate the table entry you want to find through the drop-down list or by entering a keyword.
Edit Delete 🖉 Bind	Click them to edit, delete, or bind a table entry.
	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.
Q Refresh	Update data on the current page.
< 1 2 3 4 5 6 > 10/page ~ Go to page 1	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.

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

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.

🚺 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.

Rujje	[€] Rcycc	Discover Device					English 🗸 🕞 E	kit
		vices: 18. Other Device			not appear in the list. View T	opology	0	
	Net Status	(Online Devices / Total)	Router	Switch 1/1 Switches	ি 0 / 0 APs	17 Other Devices	Refresh O	
	My Ne	twork						
	ruijie (1 d Model	ievices) Aaster]	SN MACCQQQQQQ123	IP 172.30.102.133	MAC	Software Ver ReyeeOS 1.86.1718	×	
	Other	Devices 0						
	123 (3 de	vices)	Add to My Network				>	
	lin (1 devi	ces)	Add to My Network				>	
			Red	iscover	Start Setup			

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.

- 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.

	English 🗸 🕞 Exit
* Network Name Example: XX hotel.	
Network Settings	
Internet o DHCP O Static IP	
Management Password (Please remember the password.)	
* Management Please remember the management pass ** Password	
Country/Region/Time Zone	
* Country/Region China (CN) ~	
* Time Zone (GMT+8:00)Asia/Shanghai V	
Previous Create Network & Connect	

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 <u>Switching the Work Mode</u>.

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.

Ruíjie Rcy	cc	Local Device(NBF ~					English ∽	M 😔 Network Configuratio	in (⊟Log Ou
ം Home		Basic Info							
∯ VLAN			NBF5200M-8FS16GT4XS	Davice	Name:		SN:		
🕾 Monitor	~	MAC Address: Connection		Working	Mode: Self-Organizing Network &		MGMT IP: 192.168.88.53 Software Version: ReyeeOS 2.290.0.1615		
Ø Ports		Status:	36 days 15 hours 42 minutes 51 seconds		Version:		System Time: 2024-05-30 15:45:20		
L2 Multicast		1							
L3 Interfaces	~	Port Info 💿 Pa	anel View						
Routing	~	Traffic data is upd	lated every 5 minutes. 🔾 Refresh						
⊘ Security	~			1 3 5 7 9	11 13 15 17 19 21 23			Maximum ONUs Supported	
🖻 Advanced								by the Current OLT ②	
② Diagnostics				8 8 1 0	12 14 16 18 20 22 24	25 26 27 28		Connected 80 / Remaining 144	
🐵 System		Port	Rate	Rx/Tx Speed (kbps)	Rx/Tx Bytes	Rx/Tx Packets	CRC/FCS Error Packets	Corrupted/Oversized Packets	Conflicts
		Gi1	1000M	5733/36865	1.46T/3.02T	5853664934/6091064193	1/0	0/1336666627	0
		GI2	1000M	545/2898	630.24G/1.43T	1877393728/2914240935	1/0	0/410789486	0
		GI3	1000M	1862/23113	330.41G/3.37T	1227591529/4136119444	1569/0	0/181483805	0
		G14	1000M	13936/77758	2.86T/11.05T	7415253256/20605232269	350/0	0/2264663258	0
		GI5	1000M	20019/58748	4.62T/10.84T	8744990036/20111374212	7/0	0/3764254388	0
		GI6	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0

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.

Rujje	Network	Currently i	n Network mode.
Network	~ < c	Currently in Net	work mode.
Network		Clients	Topolog
Local Device(NBS)	$z_{\mu\nu}^{\rm sig}$ >	ropolog

• 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

Rujje	Network 🗸	Navigation Q English 🗸 🛆 🎇 🔶 📑
Q Navigation	Status Devices Clients	Topology List
1 Overview	Online 1 / 17 / 1 > 28 >	+ AP
P. Network	Alert Center All (0)	
Devices	No Alerts Yet	
Olients V	Common Functions	Contraction of the second seco
-a- System V	RLDP OHCP Batch Snooping Config	Restore
		Refresh
	Network Planning Setup	
	Wi-Fi VLAN (1):	
	@Ruijie-m745E VLAN1	
	Wired VLAN (2):	
	VLAN0001 test_vlan	
	VLAN1 VLAN3	

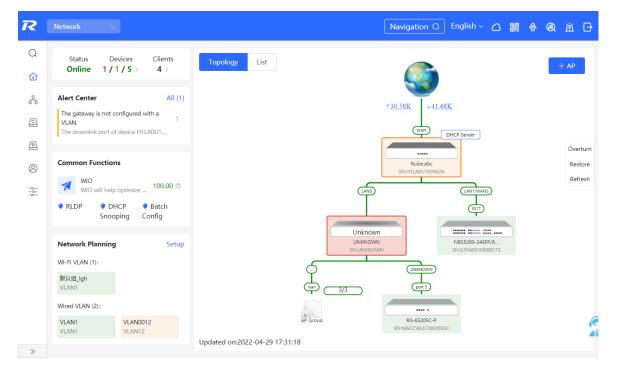
Figure 2-3 The Web Page in Local Device Mode in Self-Organizing Mode

Ruijie Rey	усс	Local Device(NBF ~					English ∨ Remote 08	M 👌 Network Configurat	
ൿ Home		Basic Info							
😚 VLAN		·	4BF5200M-8FS16GT4XS	Device	Name:		SN:		
图 Monitor		MAC Address: Connection		Working	Node: Self-Organizing Network 2 rdware 1.00		MGMT IP: 192.168.88.53 Software Version: ReyeeOS 2.290.0.1615		
Ports		Status:	6 days 15 hours 49 minutes 6 seconds		fersion:		System Time: 2024-05-30 15:51:35		
L2 Multicast									
L3 Interfaces	~	Port Info 💿 Pa	inel View						
Routing	~	Traffic data is upd	ated every 5 minutes. C Refresh						
Security	~			1 3 5 7 9	11 13 15 17 19 21 23				
🗄 Advanced								Maximum ONUs Supported by the Current OLT ⑦	
@ Diagnostics				B B B B 2 4 6 8 10	12 14 16 18 20 22 24	25 26 27 28		Connected 80 / Remaining 144	
臺 System		Port	Rate	Rx/Tx Speed (kbps)	Rx/Tx Bytes	Rx/Tx Packets	CRC/FCS Error Packets	Corrupted/Oversized Packets	Conflicts
		Gi1	1000M	6231/18251	1.46T/3.02T	5854807282/6092335492	1/0	0/1336886163	0
		GI2	1000M	659/2998	630.27G/1.43T	1877548853/2914473487	1/0	0/410840721	0
		GI3	1000M	1214/15252	330.47G/3.37T	1227878476/4137065499	1569/0	0/181490777	0
		GI4	1000M	12366/29359	2.86T/11.05T	7418026680/20608623909	350/0	0/2264799779	0
		GI5	1000M	24183/115850	4.62T/10.84T	8749023537/20115904700	7/0	0/3765102428	0

3 Network management

3.1 Overviewing Network Information

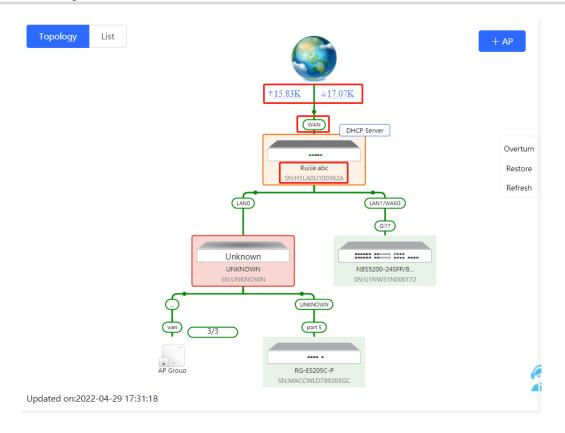
In network mode, the **Overview** page displays the current network topology, uplink and downlink real-time traffic, network connection status, and number of users and provides short-cut entries for configuring the network and devices. Users can monitor and manage the network status of the entire network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



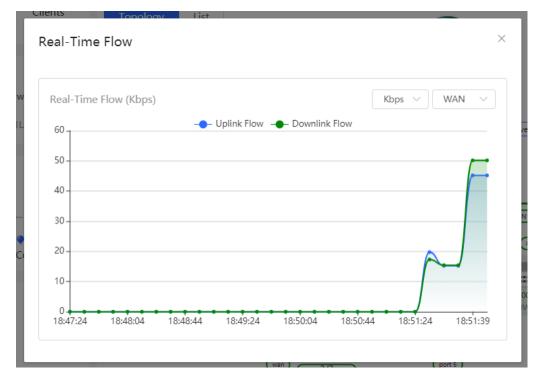
3.2 Viewing Networking Information

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.

Topology List ×	EGW	Hostname <mark>: Ruijie.abc</mark> Model:EG205G S N :H1LA0U100362A	Ø	Software Ver:ReyeeOS 1.86 MGMT IP:192.168.110.1 MAC: 00:74:9c:87:6d:85	.1619
viewen vie viewen vie vie vie viewen viewen vie vie vie vie vie vie vie vie vie vie	Port Status VLAN Info Port More	Port Status	LANO LANI L	LANZ WANI WAN	
		VLAN			Edit ©
RE EDEC-P SHARE/WLDTHORDE		Default VLAN			
		Interface	IP	IP Range	Remark
		LAN0,1	192.168.110.1	192.168.110.1- 192.168.110.254	
Updated on:2022-04-29 17:31:18					

• 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.



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.

Арр		•	Tip A devices discovered	not in SON is d.Manage		×
	Status D Online 1 / Unknown:	ſ		Topology evice or a Ruijie device	List	with SON
1	Not in SON: In SON:	1 Mana		,		
	Gateway: AP:					
•	Switch: AC:	_				
Ļ	Router:	-	🛓 Batch			

(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**.

Ruffe RCycc Discover Device					English 🗸 🕒 Exi
Total Devices: 20. Other D Please make sure that the device cou			not appear in the list. <mark>View T</mark> o	ppology	Ø
Net Status (Online Devices / Tota	N) Romer O Router	Switch 3 / 3 Switches		2 17 Other Devices	Refresh O
My Network					
NBS3100 (3 devices)					>
Other Devices 0					
New Device (1 devices)	Add to My Network				>
Unnamed Network (2 devices)	Add to My Network				>
	Red	iscover Star	t Setup		
My Network					
NBS3100 (3 devices)					
Other Devices ()					
New Device (1 devices)	Add to My Network	:			
✓ Model	SN	IP	MAC		Software Ver
Switch NBS7006	NULL	172.30.102.154	00:D0:F8:15:08:5B	Re	yeeOS 1.86.

(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.

Add Device	to My Network	×
* Password	Please enter the management password	
	Forgot Password Add	

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.

Rujje	Network	~			Navigation Q English ~ 🛆 🖁	🖁 🔶 🎯 🖄 🖯
Q Navigation		evices Clients	Topology	List	_	+ AP
A Network	Alert Center No Alerts Yet	All (0)			+ <u>84.26K</u> 4 <u>40.67K</u>	
Clients System	Common Function WIO WIO will help RLDP OF Snoo	optimize Disabled			Printers Printers Detribution	Overturn Restore Refresh
	Network Planning Wi-Fi VLAN (3):			ے م	Unknown UNNXOWN SR.UNRXOWN Gameran Gam	
	默认组_lgh VLAN1 22 VLAN22	11 VLAN11		AP Group	2/2 (pert) 	
« Collapse	Wired VLAN (7):		Updated on:2022	-05-09 04:00:15		2
Topology List				IP/MAC	/hostname/SN/S Q	es Batch Upgrade
SN \$	Status ≑	Hostname 🌲	MAC \$	IP ≑	Software Ver	Model ≑
MACCWLD789205G	C Online	ruijie 🖉	78:11:22:33:44:55	192.168.110.226	ESW_	RG-ES205C-P
H1LAOU100362A	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.	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.

Network management

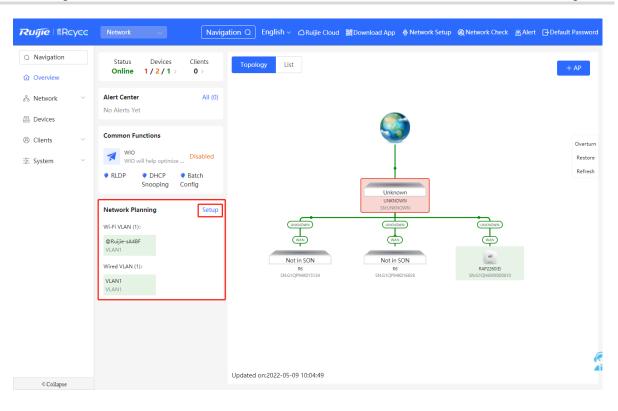
		×	MSW	Hostnam Model:N SN:G1NV	BS5200-2	24SFP/	/8GT4X	(S			MGM	vare Ve IT IP:11 00:D3	1.1.1.8	9		.1704			
Тор	ology List	Status ≑	Port Status VLAN Info	Port Status	S														
	MACCWLD789205GC	Online	Port														Panel	Vie	N
Local	H1LA0U100362A	Online	Route Info	1 3	57	9 8 (1	11	13	15 1 3	7 1	9 21	23	17	19	21	23			
	G1NW31N000172	Online	RLDP	2 4	68	8-1	- 1 12	-2 14	3 16 1	8 2	0 22	24	18	20	22	24	25	26	27
		Offline																	
	1234942570021	Online		VLAN														Ed	lit ©
	MACC522376524	Online		VLAN1	VLAN	122		N88											
	1 > 10/page				rface	100	VLA	IP				IP Ra	ange				Remark		
				Gi2,Gi4,0 24,Te25-28				11.1.1	.89										
				1 3	5 7	9	11	13	15 1	7 1	9 21	23	17	19	21	23			

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

	ogy List				IP/MAC,	hostname/SN/S Q	Batch Upgrade
	SN \$	Status ≑	Hostname 🌲	MAC \$	IP \$	Software Ver	Model ≑
<u> </u>	MACCWLD789205GC	Online	ruijie 🖉	78:11:22:33:44:55	192.168.110.226		RG-ES205C-P
Local	H1LA0U100362A	Online	Ruijie.abc [Master] 🖉	00:74:9C:87:6D:85	192.168.110.1 🖉		EG205G
	G1NW31N000172	Online	Ruijie 🖉	00:D3:F8:15:08:5B	11.1.1.89 🖉		NBS5200- 24SFP/8GT4XS
	G1QH2LV00090C	Offline	Ruijie	C4:70:AB:A8:69:17	192.168.110.102	Constitution of Constitution	RAP2260(G)
	1234942570021	Online	RAP2200e 🖉	00:D0:F8:15:08:48	192.168.110.152 🖉		RAP2200(E)
	MACC522376524	Online	Ruijie 🖉	00:10:F8:75:33:72	192.168.110.200 🖉		EAP602

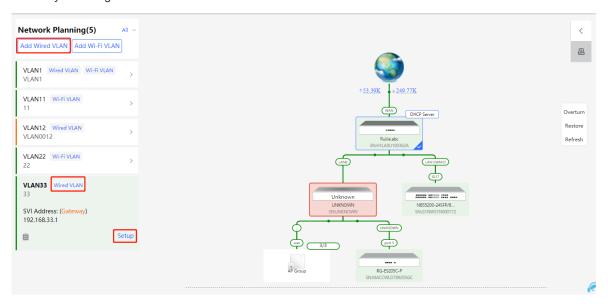
3.5 Configuring the Service Network

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

 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			\times
1 Configure VLAN Parameters	2 Configure Wired Access	3 Confirm Config Delivery	
Description			
* VLAN ID:	33		
Address Poo	• Gateway		
Server			
Gateway/Mask	192.168.33.1 / 255.255.255.0		
DHCP Pool			
IP Range	192.168.33.1 - 192.168.33.254		
	_		e
	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		×
<	gure VLAN Parameters Configure Wired VLAN	>
UKA DHCP Server	VLAN33 (33) You have selected 2 device(s) with 6 port(s). Pane	View Apprepate Im Uplink Im Copper Fiber 23 177 19 21 23 10<
Unknown Unknown Skulinkriciwn Skulinkriciwn		
AP Group		

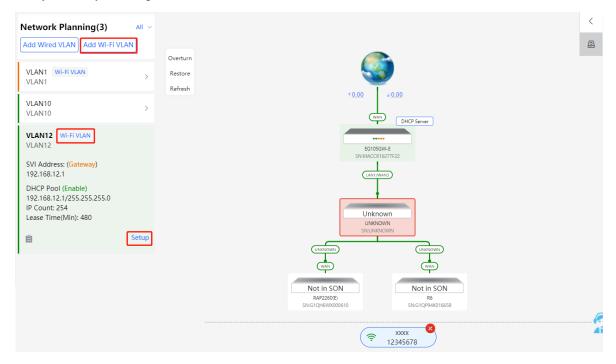
(4) Confirm that the configuration items to be delivered are correct and then click Save. Wait a moment for the configuration to take effect.

Network management

Configure Network Planning/Add Wired VLAN		\times
1 Configure VLAN Parameters	2 Configure Wired Access 3 Confirm Config Delivery	
Overt WAN DHCP Server EG210G-P SN:1234557891234		
		-
	Previous Save	(e

3.5.2 Configuring the Wireless Network

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



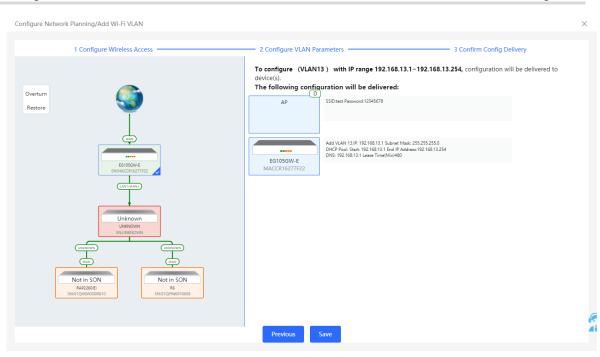
(2) Set the Wi-Fi name, Wi-Fi password, and applicable bands. Click Next.

Configure Network Planning/Add W	/i-Fi VLAN			×
1 Configure Wireless	s Access	— 2 Configure VLAN Parameters —	3 Confirm Config De	livery
	* SSID:			
	Security: 🔿 Secur	rity 💽 Open		
	Band: O 2.4G	+ 5G 0 2.4G 0 5G		
		Next		

(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 Dellvery
Description:		
* VLAN ID:	13	
topo.addressPool	• Gateway	
Gateway/Mask	192.168.13.1 / 255.255.255.0	
DHCP Pool		
IP Range	192.168.13.1 - 192.168.13.254	
	Previous Next	

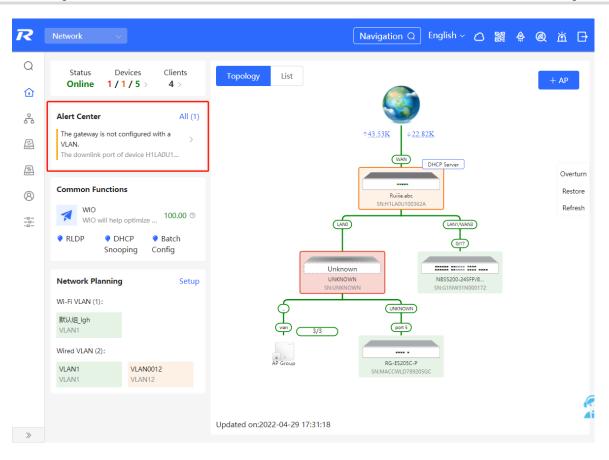
(4) Confirm that the configuration items to be delivered are correct and then click **Save**. Wait a moment for the configuration to take effect.

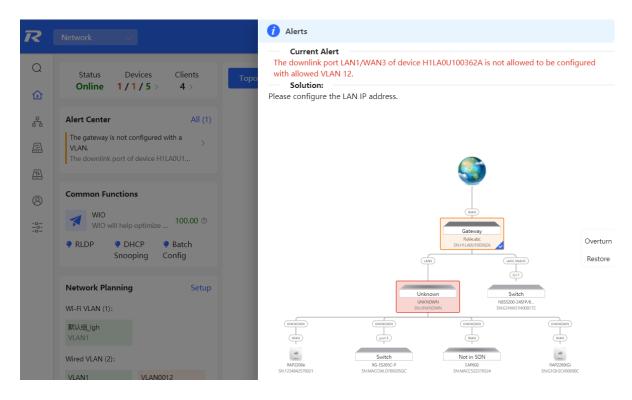


3.6 Processing Alerts

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.





20

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**).

Status Online	Devices	Clients 33 >
Alert Center		Wired 33 VLAN:
No Alerts Yet		2.4G: 0
		5G: 0
Common Fun	ctions	

All (29) Wired (29) Wireless (0)

<i>Online Clients</i> The client going offline will not disappear immediately. Instead, the client will stay in the list for three more minutes.							
Online Clients			Search by IP/MAC/Username	Q C Refresh			
Username/Type	Access Location	IP/MAC	Current Rate	Wi-Fi			
 Wired		192.168.1.200 00:e0:4c:0a:00:27	Up:0.00bps Down:0.00bps				
 Wired	MACC2020ABCDE	172.30.102.1 00:74:9c:71:dd:43	Up:0.00bps Down:0.00bps				
 Wired	MACC2020ABCDE	172.30.102.101 b4:fb:e4:b0:bb:54	Up:0.00bps Down:0.00bps				
RG-BCC-F	MACC2020ABCDE	172.30.102.107 58:69:6c:ce:72:b2	Up:0.00bps Down:0.00bps				
iDS-7932NX-K4%2FS	MACC2020ABCDE	172.30.102.110 98:8b:0a:d2:ec:28	Up:0.00bps Down:0.00bps				

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**.

Smart Device Network 0	
	Smart Device Network Support the quick identification and isolation planning for the clients (such as the camera, access control, background broadcast, smart charging pile). Highlights
	1.Quickly identify the client access information in the network to avoid tedious information collection
	2.Quickly perform isolation planning on the clients to simplify isolation operating steps
	3.Adopt visualized client maintenance and active error alarm to improve the troubleshooting efficiency.
	Usage Guide Identify Clients: Enter the client subnet and the server IP addresses. Isolate Clients: Isolate a certain client in this subnet.
	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.

nart Device Network							
	1 Identify	Client — 2 Isolate Clien	nt —— 3 Confirm Config	— 4 Deliver Confi	g		
Client Type 🛛	Client Subnet IP and Mask Ø	Planned (Count 🛛 Client Server IP 🖉			Added Clients	
	192.168.1.0	24 254	192.168.1.2	÷	Delete Subnet		254
Camera							
Video Intercom an							
Background Music							
Smart Parking Lot							
Parking Guidance							
Smart Charging Pile							
Smart Lighting							
Remote Meter Rea							
		Identif	y Client Skip				

(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**.

lient Type 🛿	Client Subnet IP and Mask	Planned Count/Identified Count	C	Client Server IP 🛿		Action	Identified Clients	Refr 254
test	192.168.1.0/24	254/ 1 🐻	192.168.1.2	Configure	5 J	Delete Subnet		
	192.168.1.0/24	254/ 1 🐻	192.168.1.2	Configure	J 🛃	Delete Subnet		

Smar	t Device Network									
		Identified Serve	ers in 192.168.1.0,	/24				×		
									tified Clients	Refresh
	Client Type 🔞	No. ≑	Hostname: ≑	IP ÷	MAC \$	Switch SN \Leftrightarrow	Switch Port $\mbox{$\ddagger$}$		test	254/2
	test	1	-	192.168.1.2	00:D0:F8:22:74:5E	MACC2020ABCDE	Gi1/23			
				Isolate Clier	nt Skip					

(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 De	liver Config		
Subnet 🛛	Isolated VLAN Name 🛛	VLAN ID Ø	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	VLAN
	P	Previous Genera	ate Config Skip			

(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 Overturn Restore	Target Devices Ruijie(MACC2					
Previous Deliver Config Skip						

(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.

Smart I	Device Network	
	1 Identify Client —— 2 Isolate Client —— 3 Confirm Config —— 4 Deliver Config	
© Co	onfiguration delivery succeeded.	
Cont	fig Delivery Details	
⊘	Device VLAN Config	\sim
	DeviceRuijie (MACC2020A8CDE) : Update VLAN:test_vlan, Vlanld: 3	
\odot	Port VLAN Config	~
	DeviceRuijie (MACC2020A8CDE) : Port Gi1/1Set as Trunk Port, Native Id:1,Allow Vlan:1-4094	
\odot	Subnet Vlan Config	~
	DeviceRuijie (MACC2020ABCDE) : Setup Subnet VLAN3:192.168.1.240 255.255.255.0	
	View Details Add Client	

(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.

Smart Device Netw	vork 🕖	Batch Edit Hostnames	IP address,	MAC address or hos	tname Q
Image: OnlineTotal3544	test: 192.168.1.0/24			Delete Client	Delete Subnet C
⊘ test Online Total 1 2	Status	Username	IP ≑	MAC \$	Switch SN 💠
other Total	• Offline test	&	192.168.1. 2	00:D0:F8:22:7 4:5E	MACC2020ABCDE
34 42	• Online test	Ø	192.168.1. 200	00:E0:4C:0A:0 0:27	MACC2020ABCDE
	< 1 > 10/page >				Total 2
	other:				
	• 34 • 42				Delete Client 🔻

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.

Revijie Rev	ycc	Local Device(NBF		English 🗸 🛆 Remote O&M 🔮 Network Configuration 📑 Lo
🖧 Home		Basic Info		
🖉 VLAN				
		Device Model: NBF5200M-8FS16GT4XS	Device Name:	SN: G1S075L000355
Monitor		MAC Address:	Working Mode: Self-Organizing Network &	MGMT IP: 192.168.88.53 @
		Connection • Online	Hardware 1.00	Software Version: ReyeeOS 2.290.0.1615
Ports	~	Status:	Version:	System Time: 2024-05-30 15:58:25
		Uptime: 36 days 15 hours 55 minutes 56 seconds		

1. Setting the device name

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

Bas	ic Info	
	Hostname: Ruijie 🖉	
	Edit Hostname	
	Ruijie	rk 🥼
Sn	Cancel	

2. Switching the Work Mode

Click the current work mode to change the work mode.

Local Device(NBF ~	Description:
	 The device IP address may change upon mode change.
Basic Info	Change the endpoint IP address and ping the device.
Device Model:	3. Enter the new IP address into the address bar of the browser to access
Working Mode: Self-Organizing Network	Eweb. 4. The system menu varies with different
Hardware 1.00	work modes.
Version:	Self-Organizing 🔵 🕜
1	Network
Port Info ⑦ Panel View	Save

3. Setting MGMT IP

Click current management IP address to jump to the management IP configuration page. For more information, see <u>5.6</u>.

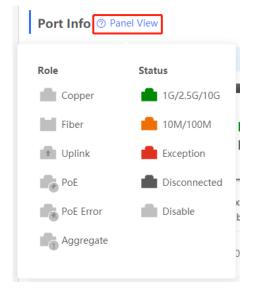
Basic Info					
Device Model:	NBF5200M-8FS16GT4XS	Device Name:	~	SN:	
MAC Address:		Working Mode:	Self-Organizing Network &	MGMT IP:	192.168.88.53 @
Connection	Online	Hardware	1.00	Software Version:	ReyeeOS 2.290.0.1615
Status:		Version:		System Time:	2024-05-30 16:09:47
Uptime:	36 days 16 hours 7 minutes 18 seconds				

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.

R	Local Device(NBS	~					English 🗸 🛆	1 e C
ጽ	Port Info	⑦ Panel View						
40 10 10	The flow data	will be updated every	5 minutes. 🔉 Refresh					
쑷				_				
<u>چ</u>			1 3 5 7	9 11 13 15	17 19 21 23			
\bigcirc								
\bigcirc			2 4 6 8	10 12 14 16	18 20 22 24	25 26 27 28		
Ē	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	74718870/281666 45	0/0	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	12265475/629207 67	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
>>	GIQ	Disconnected	0./0	0.00/0.00	0./0	0/0	n <i>/</i> n	0



• 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	⑦ Panel View							
The flow data	will be updated every	5 minutes. 🔾 Refres	h					
			7 9 1 8 10 1		21 23 21 23 22 24	25 26 27 28		
Port	Rate	Rx/Tx Speed (kbps)	Port: Status: Rate:	Gi14 Connected 1000M	ckets	CRC/FCS Error Packets	Corrupted/Oversized Packets	Conflicts
Gi1 🕇	1000M	103/85	Flow: Rate: Attribute:	 ↓ 1.70G ↑ 18.42G ↓ 167kbps ↑ 205kbps Copper 	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 ⑦) Panel View						
The flow data v	will be updated every	5 minutes. 🔉 Refresh					
		1 3 5 7 2 4 6 8		17 19 21 23 18 20 22 24	25 26 27 28		
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 I	nfo						Clear Selected	🖻 Clear All	
The flo	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 1	1000M	342/55	16.39G/4.04G	74749819/28194 138	0/0	0/0	0	
	Gi2	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0	
	Gi3	1000M	25/268	2.05G/13.88G	12270309/62929 657	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	

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.

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 .

lome	MAC List Star	tic MAC Dynamic MAC MAC Filter A	iging Time ARP List		
LAN	MAC Addres	ss		Search by N	MAC - Example: 00:11:22:33:44:5 Q Search
Aonitor					
rt Flow	Up to 16K ent	tries can be added.			
ents Management	No.	MAC	VLAN ID	Port	Туре
tical Transceiver Info	1	48:81:D4:FE:A8:82	1	GI1	Dynamic
er Properties	2	48:81:D4:FE:88:A5	3	GIZ	Dynamic
	3	00:E0:70:E3:B7:2E	3012	G14	Dynamic
A Configuration	4	70:85:C4:58:DC:1D	3013	GI5	Dynamic
orts	5	8C:EC:48:83:D7:D6	3013	Te27	Dynamic
2 Multicast	6	48:81:D4:FE:88:A8	1	GI3	Dynamic
3 Interfaces	7	8C:0F:F3:76:7A:31	3012	G14	Dynamic
outing ~	8	14:14:48:73:F9:68	3013	GIS	Dynamic
ecurity ~	9	B8:CA:3A:97:E1:98	3012	Gi4	Dynamic
dvanced ~	10	14:14:48:73:F9:67	3013	GIS	Dynamic

🚺 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**.

Ruíjie Reyce	Local Device(NBF \vee			English ∽ Remote O&M _ €	Network Configuration 🕞 Log C
🖧 Home	MAC List Static MAC	Dynamic MAC MAC Filter Aging Time	ARP List		
🗊 VLAN	MAC List			Clear by MAC V Example: 00:11:22:33:44:5	Clear C Refresh
Port Flow	No.	MAC	VLAN ID	Port	
Clients Management	1		1	Gi1	
Optical Transceiver Info	2		1	Gi2	
	3		3012	Gi4	
Fiber Properties	4		3013	GI5	
DBA Configuration	5		3013	Te27	
Ports ~	6		1	GI3	
L2 Multicast	7		3012	Gi4	
L3 Interfaces ~	8		3013	GI5	
Routing ~	9		3012	GI4	
Security	10		3013	GI5	
Advanced	< 1 2 3	4 5 6 ··· 92 > 10/page ~ Go	to page 1		Total 911

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: 00:11:22:33:44:5	🔟 Clear	C Refresh
No.	MAC	Clear by MAC		Port	
1	54:BF:64:5C:90:5F	Clear by Port Clear by VLAN		Gi1	
2	58:69:6C:FF:1A:70			Gi1	
3	8C:EC:4B:86:E3:B4	1		Gi1	

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.

Reyce	Local Device(NBF \vee		English ~	CRemote O&M 👲 Network Configuration	n ⊡Log O
중 Home	MAC List Static MAC Dynamic MAC MAC Filter	Aging Time ARP List			
Monitor	Static MAC Description: The switch forwards packets based on the MAC ad 802.1x authentication.	dress table. Bind a static MAC address with a port, and the packet des	tined for this address will be forwarded to the port. You can config	ure MAC address binding for a port enabled with	h
Port Flow Clients Management	MAC List			+ Add 🗄 Delete	Selected
Optical Transceiver Info	Up to 256 entries can be added.				
Fiber Properties	Port	MAC Address	VLAN ID	Action	
DBA Configuration		No Data			
Ø Ports	< 1 → 10/page ∨ Go to page 1				Total 0

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.

Add		×
* MAC:	Example: 00:11:22:33:44:55	
* VLAN ID:	Please enter a VLAN ID.	1
* Select Port:		
Available Una	9 11 13 15 17 19 21 23	
2 4 6 8	10 12 14 16 18 20 22 24 25 26 27 28	
	Deselect	
	Cancel	

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**.

MAC List				+ Add
Up to 256	entries can be added.			
	Port	MAC	VLAN ID	Action
	Gi28	00:11:22:33:44:55	1	Delete

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.

R	Local Device(NBS V		English - 🛆 🎇 🖨 🗗
	MAC List Static MAC Dynamic MAC MAC F	Iter Aging Time ARP List	
₽°	MAC Filter Description: The switch forwards packets based on the packet will be discarded. You can configure the MAC fil		he specified MAC address reaches the VLAN, the
⊕	MAC List		+ Add 🗇 Delete Selected
\bigcirc	Up to 256 entries can be added.		
Ē	MAC	VLAN ID	Action
<u> </u>	00:11:22:33:44:55	1	Delete
-0-	Total 1 10/page \checkmark (1 \Rightarrow Go to page	1	

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 .

Add			×
* MAC:	Example: 00:11:22:33:44:55		
* VLAN ID:	Please enter a VLAN ID.		
		Cancel	ОК

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**.

MAC List		+ Add Delete Selected	
Up to 256	entries can be added.		
~	MAC	VLAN ID	Action
	00:11:22:33:44:55	1	Delete

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.

Ruíjie Rcycc	Local Device(NBF \vee
器 Home	MAC List Static MAC Dynamic MAC MAC Filter Aging Time ARP List
≝ ^p VLAN	
Monitor	Aging Time
Port Flow	* Aging Time (Sec): 300 Range: 10-630. 0 indicates never aging.
Clients Management	Save
Optical Transceiver Info	

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.

Ruíjie Reyce	Local Device(NBF \sim		English ~ △Remote O&M ♦ Network Configuration 🕒Log Out
$\delta_0^{\mathcal{D}_0}$ Home	MAC List Static MAC Dynamic MAC MAC Filter Aging 1	ime ARP List	
VLAN Monitor	ARP List Description: The device learns IP-MAC mapping of all devices connected	to its interfaces.	
Port Flow	ARP List		Search by IP Address/MAC Q Refresh
Clients Management	No. IP Address		MAC Address
Optical Transceiver Info	1 192.168.88.19	,	
Fiber Properties	2 192.168.88.17	1	
DBA Configuration	3 192.168.88.21	,	
Ø Ports	4 192.168.88.73		
L2 Multicast	5 192.168.88.16	5	
L3 Interfaces	6 192.168.88.77		
	7 192.168.88.96		
Routing	8 192.168.88.18	õ	
Security ~	9 192.168.88.20		
🖹 Advanced 🗸 🗸	10 192.168.88.65		
Diagnostics	2 3 4 5 6 ··· 9 > 10/page ~	Go to page 1	Total 83

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.

Ruíjie Reyce	Local Device(NBF ~						English ~F	Remote O&M	Network Config	uration 🕞 Log C
🖧 Home	Optical Transceiver Info						Search by Port		All v	C Refresh
€ ⁹ VLAN	optical manaceiver milo									
🗄 Monitor	Port	Number of Connected ONUs	Supported ONUs	Distance(m)	Temperature (°C)	Voltage (V)	Current (mA)	Tx power(dBm)	Local Rx Power(dBm)	Neighbor Rx Power(dBm)
Port Flow	Gi1	> 16 Members	32		35	3.23	19.64	4.22		
Clients Management	Gi2	> 10 Members	32		36	3.25	23.42	4.49		
Optical Transceiver Infc	Gi3	> 12 Members	32		38	3.24	25.41	5.45		
Fiber Properties	Gi4	> 15 Members	32		37	3.23	23.75	4.82		
DBA Configuration	GI5	 15 Members 	32		35	3.26	2.64	5.03		

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.

Rujjie Royco	Local Device(NBF \vee		English ~ 🛆	Remote O&M 🔮 Network Configuration 📑 Log Ou
🖧 Home	Port Settings			Batch Config 🛽 🕹
S VLAN	Port	Maximum Physical Reach	ONU Layer 2 Isolation	Action
Port Flow	Gi1	5	Disable	Edit
Clients Management	G12	5	Disable	Edit
Optical Transceiver Info	Gr3	5	Disable	Edit
Fiber Properties	Gi4	5	Disable	Edit
DBA Configuration	GIS	5	Disable	Edit
Ports	GI7	5	Disable	Edit
L3 Interfaces	GI8	5	Disable	Edit
Routing ~	< 1 → 10/page ∨ Go to page 1			Total 7

4.7 DBA

4.7.1 Overview

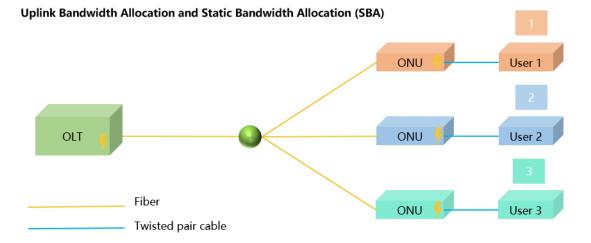
Through the DBA (Dynamic Bandwidth Assignment) function, OLT can dynamically adjust the upstream bandwidth of each ONU according to the real-time traffic conditions of each ONU, thus improving the bandwidth utilization of the PON (Passive Optical Network) system.

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.



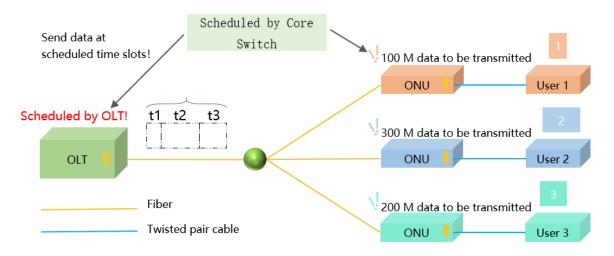
Calculation of static bandwidth allocation (SBA): Client (PC/Smartphone/Tablet) rate = PON port rate/number of split outputs

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.



Uplink Bandwidth Allocation and DBA

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

	O Description				
VLAN	You can create a DBA profile for	r all ONUs connected to a specific port. Additionally	, you can configure excluded ONUs which take priority ove	port-based rate limiting	
Monitor	Port-based Rate Limiting				Batch Config
Port Flow	Port	DBA Status	Bandwidth Type	Excluded ONU Manage All Excluded ONUs	
Clients Management	Gi1		Assured	+ Add Excluded ONU	
Optical Transceiver Infc	Gi2		Assured	+ Add Excluded ONU	
Fiber Properties					
DBA Configuration	GI3		Maximum	+ Add Excluded ONU	
Ports	Gi4		Maximum	+ Add Excluded ONU	
L2 Multicast	GI5		Maximum	+ Add Excluded ONU	
L3 Interfaces	Gi6		Assured	+ Add Excluded ONU	
Routing ~					
Security 🗸	GI7		Assured ~	+ Add Excluded ONU	
Advanced 💛	Gi8		Maximum	+ Add Excluded ONU	
Diagnostics	< 1 > 10/page ~	Go to page 1			

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.

o-based Confi	guration Guide			Basic Managem
VLAN L	ist 😑		+ Batch Add	+ Add 🗎 🖻 Delete Selected
Up to 40 deleted.)		efault VLAN, management VLAN, Native VLA	N, SVI VLAN, MVR VLAN, Voice VLA	N and Access VLAN cannot be
	VLAN ID \$	Description	Port	Action
	1	VLAN0001	Gi1-28	Edit Delete
	10	VLAN0010		Edit Delete
	20	VLAN0020		Edit Delete
Total 3	10/page \checkmark (1 $>$	Go to page 1		

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** .

VLAN List	•		+ Batch Add	+ Add 💼 Delete Selected
Up to 4094 deleted.)	entries can be added.(The	e default VI AN management VI AN Batch Add	Native VLAN SVLVLAN MVR VLAN, Voice V	/LAN and Access VLAN cannot be
	VLAN ID ≑	Example: 3-5 and 20.		Action
	1		Cancel OK	Edit Delete
	10	VEANOUTO		Edit Delete
	20	VLAN0020		Edit Delete

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 .

VLAN List	•	Add		×	d + Add 🗈 Delete Selected
Up to 4094 e	entries can be added.(1				be deleted.)
		* VLAN ID:	Range: 1-4094	Range: 1-4094	
	VLAN ID 💠	Description		Maria 22 alternations	Action
	1	Description:	Description	Max: 32 characters.	Edit Delete
	10			Cancel	Edit Delete
	20		VEANOUZU		Edit Delete

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.

VLAN List	•	Edit			×	d + Add 🗊 Delete Selected
Up to 4094 e	ntries can be added.(T					be deleted.)
	VLAN ID \$	* VLAN ID:	10	Range: 1-4094		Action
	1	Description:	VLAN0010	Max: 32 characters.		Edit Delete
	10			Cancel	ж	Edit Delete
	20		VERINUUZU			Edit Delete

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.

VLAN Lis	st 😑		+ Batch Add	+ Add
Up to 409	4 entries can be added.(The defau	lt VLAN, management VLAN, Native VLAN, S	VI VLAN, MVR VLAN, Voice VLAN and A	ccess VLAN cannot be deleted.)
	VLAN ID \$	Description	Port	Action
	1	VLAN0001	Gi1-28	Edit Delete
	10	VLAN0010		Edit Delete
	20	VLAN0020		Edit Delete

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

VLAN Lis	t 😑		+ Batch Add	+ Add 🗈 Delete Selected
Up to 409 4	4 entries can be added.(The de	fault VLAN, management VLAN, Native VLAN, SVI	VLAN, MVR VLAN, Voice VLAN and A	ccess VLAN cannot be deleted.)
	VLAN ID \$	Description	Port	Action
	1	VLAN0001	Gi1-28	Edit Delete
	10	VLAN0010		Edit Delete

1 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 <u>3.5.2</u> <u>Creating a VLANCreating Creating a VLANa VLAN</u>) and then configure the port based on the VLANs.

Port List 😑						🖉 Batch Edit
		both the tagged VLAN ar ad on the port, the Voice		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	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. Access VLAN has attributes of both Native VLAN and Permitted VLAN 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.
Trunk port	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. 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.

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.

1 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**.

1 Note

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

Port List	Batch Edit	×		🖉 Batch Edit
The Permit VLAN o If the Voice VLAN	Port Mode: Access Port			
Port	* Access VLAN: 1		AN	Action
Gi1 🕇	* Select Port:			Edit
Gi2	Available 💼 Unavailable 👘 Aggregate ท Uplink 💼 Copper 🔛 Fiber			Edit
Gi3	1 3 5 7 9 11 13 15 17 19 21 23			Edit
Gi4	2 4 6 8 10 12 14 16 18 20 22 24 25 26 27 28			Edit
GI5	Note: You can click and drag to select one or more ports. Select All Inverse Deselect			Edit
Gi6	Cancel			Edit
Gi7	ACCESS I			Edit 🔔

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**.

Port List	Port:Gi3			×		∠ Batch Edit
The Permit VLAN c If the Voice VLAN	Port Mode:	Access Port	~			
Port	* Access VLAN:	1	~		AN	Action
Gi1 🕇						Edit
Gi2			Cancel	ОК		Edit
Gi3	ACCESS	1	 			Edit
Gi4	ACCESS	1	 			Edit

🚺 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**.

RG-ES205C-P NBS5200-24SFP/8GT4XS G1NW31N000172 RG-ES205C-P (1) RG-ES205C-P (1) Dete: You can click and drag to select one or more ports. Select All Inverse Desel NBS5200-24SFP/8GT4XS (1) 1 3 5 7 9 11 13 15 17 19 21 23 24 26 27 28																				ALL			
RG-ES205C-P (1) RG-ES205C-P (1) Dete: You can click and drag to select one or more ports. Select All Inverse Desel NBS5200-24SFP/8GT4XS (1) 2 1 3 5 7 9 11 13 15 17 19 21 23 17 19 21 23 2 4 6 8 10 12 14 16 18 20 22 24 25 26 27 28		ruijie						Ruijie												RG-ES	S205C-P		
Image: Select one or more ports. Select All Inverse Desel NBS5200-24SFP/8GT4XS (1) Image: Select one or more ports. 1 3 5 7 9 11 13 15 17 19 21 23 17 19 21 23 2 4 6 8 10 12 14 16 18 20 22 24 25 26 27 28				GC																NBS5	200-2451	P/8GT	4X
NBS5200-24\$FP/8GT4XS (1) 1 3 5 7 9 11 13 15 17 19 21 23 1 3 5 7 9 11 13 15 17 19 21 23 1 1 16 16 16 10 10 10 10 10 10 10 2 4 6 8 10 12 14 16 18 20 22 24 25 26 27 28	RG-I	ES205C-	P (1)																				
NBS5200-24SFP/8GT4XS (1) 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																							
1 3 5 7 9 11 13 15 17 19 21 23 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 																							
2 4 6 8 10 12 14 16 18 20 22 24 18 20 22 24 25 26 27 28	te: You	can clic	k and	drag	to se	elect c	one or	r moi	re poi	rts.									Sele	ect All	Inverse	e Des	ele
2 4 6 8 10 12 14 16 18 20 22 24 18 20 22 24 25 26 27 28							one or	r moi	re poi	rts.									Sele	ect All	Inverse	e Des	ele
	NBS	5200-24	ISFP/8	3GT4)	XS (1)					23	17	19	21	23				Sele	ect All	Inverse	e Des	ele
	NBS	5200-24 3 5	ISFP/8	9 9	XS (1)) -	15	17			23	_	_	21	23	_			Sele	ect All	Inverse	e Des	ele
	NBS	3 5	7 7 8	9 9	xs (1) 11 1) 13	15 3	17	19	21						25	26	27		ect All	Inverse	e Des	ele
	1 4 2	3 5 3 4 4 6	7 7 8 8	9 9 10 10	XS (1) 11 1 1 12	13 2 -2 14	15 3 -3 16	17 18	19 20	21						25	26	27	28				

(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.

+Add VLAN +Batch Add		
VLAN ID Remark	VLAN ID Remark	
1 Default VLAN	12	till and the second sec
Previous		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.

Selected Port			
Selected Port	RG-ES205C-P:; NBS	200-24SFP/8GT4XS: Gi21-Gi22;	
Туре	Trunk Port	~	
* Native VLAN	Default VLAN	\sim	
Permitted VLAN	1,12		

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 🖉 Model:NBS5200-24SFP/8G SN:G1NW31N000172	T4XS	Software Ver:ReyeeOS 1.8 MGMT IP:10.44.78.1 MAC: 00:d3:f8:15:08:5b	36.1619
Port Status VLAN Info	VLAN			Edit 🕲
Port	VLAN1 VLAN12			
Route Info	Interface	IP	IP Range	Remark
RLDP	Gi17,Gi21-22,Te27		_	
More	1 3 5 7 9 1			1 23
		1 2 3 1 2 3		
	2 4 6 8 10 1	2 14 16 18	20 22 24 18 20 2	2 24 25 26 27
	Port			Edit Ø

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.

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 <u>6.1</u>
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 <u>6.1</u>

 Table 5-1
 Description of Port Type

Port Type	Note	Remarks
L3 Aggregate Port	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. L3 aggregate ports do not support the L2 switching function.	For related configuration, see <u>6.1</u>

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.

Ruíjie Rcycc	Local Device(NBF >				English	 	♦ Network Configuration 🕒 Log C
ಕೆ Home	Basic Settings Physical Sett	ings					
<pre></pre>							
🖭 Monitor 🗸 🗸	Configure port status, dup	lex mode, rate and flow control.					
Ports	Port List						🖉 Batch Edit
Port Settings	Port	Status	Duplex N	lode/Rate	Flow Contr	ol	Action
Aggregate Ports	Port	Status	Config Status	Actual Status	Config Status	Actual Status	Action
Port Mirroring	Gi1	Enable	Auto/Auto	Full-Duplex/1000M	Disable	Disable	Edit
Rate Limiting	Gi2	Enable	Auto/Auto	Full-Duplex/1000M	Disable	Disable	Edit
MGMT IP	Gi3	Enable	Auto/Auto	Full-Duplex/1000M	Disable	Disable	Edit
L2 Multicast L3 Interfaces	Gi4	Enable	Auto/Auto	Full-Duplex/1000M	Disable	Disable	Edit
Routing	Gi5	Enable	Auto/Auto	Full-Duplex/1000M	Disable	Disable	Edit
Security	Gi6	Enable	Auto/Auto	Unknown/Unknown	Disable	Disable	Edit

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).

Batch Edit		×
Status:	Enable v	
Rate:	Auto	
Work Mode:	Auto	
Flow Control:	Disable	
* Select Port:	available 🛛 🗖 Aggregate 🕇 Uplink	Copper Fiber
1 3 5 7	9 11 13 15 17 19 21 23 17 19	9 21 23
	1 1	0 22 24 25 26
Note: You can click and	drag to select one or more ports. Selec	t All Inverse Deselect
	Cancel	ОК

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**.

Gi1			Member port	of Ag4.			
Gi2	Port:Gi2					×	Edit
Gi3	Status:	Enable		~			Edit
Gi4	Rate:	Auto		~			Edit
Gi5	Work Mode:	Auto		~			Edit
Gi6	Flow Control:	Disable		~			Edit
Gi7							
Gi8				Cancel	ОК		

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	 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

 Table 5-2
 Description of Basic Port Configuration Parameters

1 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.

Ruíjie Reyce	Local Device(NBF \vee				English ~ 🛆 Remote (08M 🔞 Network Configuration 🕞 Log O
충 Home 중 VLAN	Basic Settings Physical Settings					
🗄 Monitor	Configure physical attribute. (The fiber port	does not support EEE. The aggregate por	t containing combo ports cannot work as a combo	s port.)		
Ports	Port List					🖉 Batch Edit
Port Settings	Port	EEE	Attribute	Description	мти	Action
Aggregate Ports	Gi1	Disable	Fiber		1500	Edit
Port Mirroring	GI2	Disable	Fiber		1500	Edit
Rate Limiting	Gi3	Disable	Fiber		1500	Edit
L2 Multicast	Gi4	Disable	Fiber		1500	Edit
L3 Interfaces ~	GI5	Disable	Fiber		1500	Edit
Routing	Gi6	Disable	Fiber		1500	Edit
Security ~	GI7	Disable	Fiber		1500	Edit
🖻 Advanced 🗸 🗸	GIB	Disable	Fiber		1500	Edit
Oliagnostics `` `	Gi9	Disable	Copper		1500	Edit
± System √	GI10	Disable	Copper		1500	Edit
	< 1 2 3 > 10/page ~	Go to page 1				Total 28

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** .

Not	e				
opper p	orts and SFP	ports cannot be	e both configu	ured during batch configurati	on.
atch Edit				×	
	Status:	Enable			
	Rate:	Auto			
	Working Mode:	Auto	~		
	Flow Control:	Disable			
	* Select Port:				
Available	Unavailable	Aggregate 🚹 Uplink	Copper Fiber		
1 3	5 7 9 11 13 1	5 17 19 21 23			
66	66				
		6 18 20 22 24	25 26 27 28		

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**.

Batch Edit		×
EEE:	Disable \lor	
Attribute:	Copper 🗸	
Description:		
* MTU:	1500 Range: 64-9216	
* Select Port:		
Available 💼 Unavailable	Aggregate Uplink Copper	
	5 17 19 21 23	
6 6 8 10 12 14 10	5 18 20 22 24 25 26 27 28	
Note: You can click and drag to select one	or more ports. Select All Inverse	Deselect
	Cancel	ок

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

1 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 Mbps × *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.

F	Aggregate Port Settings
	Up to 16 aggregate ports can be added. An aggregate port contains up to 8 member ports.
	Select All
	Ag1 Ag2 Ag3 Ag8 Ag4

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	Src & Dest MAC	~
Algorithm:		
	Save	

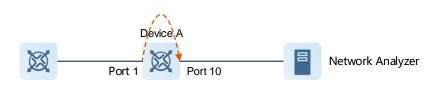
5.4 Port Mirroring

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.

A 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.

🕖 ana	alyzer application. Traffic o		ed to the destination port and y ort can be mirrored to one dest source port.		using a protocol
Port N	lirroring List				
	Src Port	Dest Port	Monitor Direction	Receive Pkt from Non-Src Ports	Action
					Edit Delete
					Edit Delete
					Edit Delete
					Edit Delete

Edit ×
Monitor Direction: Both ~
Receive Pkt from Non-Src Ports:
* Src Port:
1 3 5 7 9 11 13 15 17 19 21 23 17 19 21 23 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1
2 4 6 8 10 12 14 16 18 20 22 24 18 20 22 24 25 26 Note: You can click and drag to select one or more ports. Select All Inverse Deselect
* Dest Port:
1 3 5 7 9 11 13 15 17 19 21 23 17 19 21 23
2 4 6 8 10 12 14 16 18 20 22 24 18 20 22 24 25 26
Deselect Cancel OK
Cancer

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	 The type of packets (data flow direction) to be monitored by a source port. 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	 It is applied to the destination port and indicates whether a destination port forwards other packets while monitoring packets. 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 Ed	it 🗇 Delete Selected
	Port	Rx Rate (kbps)	Tx Rate (kbps)	Action
	Gi23	10000	10000	Edit Delete
Total 1 10/p	bage 🗸 < 🚺	> Go to page 1		

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.

Batch Edit		×
Rx Rate:	A blank value indicates no limit.	Range: 16-10000000kbps
Tx Rate:	A blank value indicates no limit.	Range: 16-10000000kbps
* Select Port:		
Available 💼 Una	available Aggregate	Uplink Copper Fiber
1 3 5 7		17 19 21 23
4 8		
2 4 6 8	10 12 14 16 18 20 22 24	18 20 22 24 25 26
Note: You can click and	drag to select one or more ports.	Select All Inverse Deselect
		Cancel OK

 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:	10000		Range: 16	-1000000kbps	
Тх	Rate:	10000		Range: 16	-1000000kbps	
			Cá	ancel	ОК	

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 Rx Rate (kbps) Tx Rate (kbps)	Action
Gi23 10000 10000	Edit Delete

1 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.

Ruíjie Rcycc	Local Device(NBF 🗸	
器 Home	MGMT IP MGMT IPv6	
≟≓ VLAN	MGMT IP	
뚶 Monitor 🗸	Configure network settings.	
🐼 Ports 🛛 🔿	Internet: Static IP	~
Port Settings	VLAN: 888	
Aggregate Ports	* IP Address: 192.168.88.53	
Port Mirroring		
Rate Limiting	* Subnet Mask: 255.255.248.0	
MGMT IP	* Gateway: 192.168.88.1	
🛆 L2 Multicast	* DNS Server: 192.168.88.1	
L3 Interfaces `` ` ` `	DHCP Server:	
\oplus Routing \checkmark	Save	

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 <u>4.8.2</u>).
- 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 .

Ruíjie Rcycc	Local Device(NBF V	
윰 Home	MGMT IP MGMT IPv6	
≝ [₽] VLAN	* Internet Null	
🖞 Monitor 🗸	IPv6 Address	
🚱 Ports 🔷 🔿		
Port Settings	IPv6 Prefix	
Aggregate Ports	Gateway	
Port Mirroring	DNS Server	
Rate Limiting	Save	
MGMT IP		
Rujje Royco	Local Device(NBF >>	
Ruífie Rcycc	Local Device(NBF >	
	MGMT IP MGMT IPv6	1
🖧 Home	MGMT IP MGMT IPv6 * Internet Null	
చిం Home హె VLAN	MGMT IP MGMT IPv6	
යි Home 중 VLAN 몇 Monitor ✓	MGMT IP MGMT IPv6 * Internet Null IPv6 Address DHCP	
☆ Home 같 ⁹ VLAN 딸 Monitor ~ ঔ Ports ^	MGMT IP MGMT IPv6 * Internet IPv6 Address DHCP Static IP	
☆ Home ☆ VLAN ☆ Monitor × ☆ Ports ^ Port Settings	MGMT IP MGMT IPv6 * Internet IPv6 Address DHCP Static IP IPv6 Prefix Null	
² → Home ^{2→} VLAN ^{2→} Monitor ^{2→} Ports Port Settings Aggregate Ports	MGMT IP MGMT IPv6 * Internet IPv6 Address IPv6 Prefix Gateway	

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 Sn	ooping	MVR	Multicast	Group	IGMP Filter	Querier
i Global Settir	ngs						
	Version	IGMPv2			~		
IGMP Report Supp	oression						
Unknown Multi	cast Pkt	Discard			~		
		Sa	ive				

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

 Table 6-1
 Description of Configuration Parameters of Global Multicast

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.

Ruíjie Rcycc	Local Device(NBF ~					English ~	C Remote O&M	Network Configuration	🕒 Log Ou
and Home	Global Settings IGMP S	nooping MVR Multic	ast Group IGMP Filter	Querier					
🖗 VLAN	() IGMP Snooping								
🗄 Monitor 🗸 🗸	IGMP Snooping								
Ports		Save							
L2 Multicast L3 Interfaces	-	3090							
Routing	VLAN List								
⊘ Security ~	VLAN ID	Multicast Status	Dynamic Learning	Router Port	Fast Leave	Router Aging Time (Sec)	Host Aging Time	(Sec) Action	
🖻 Advanced	1	Disable	Enable		Disable	300	260	Edit	
@ Diagnostics	888	Disable	Enable		Disable	300	260	Edit	

6.3.2 Enabling Global IGMP Snooping

Choose Local Device > Multicast > IGMP Snooping.

Turn on IGMP Snoo	ping and click Save.				
Global Settings	IGMP Snooping	MVR	Multicast Group	IGMP Filter	Querier
iGMP Sno	oping				
IGMP Snoop	ping 🚺				
	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

Edit		×
* VLAN ID	1	
Multicast Status		
Dynamic Learning		
Fast Leave (
* Router Aging Time (Sec)	300	
* Host Aging Time (Sec)	260	
Select Port:		
Available 💼 Unavailab	le Aggregate 🖬 Uplink 💼 Copper 🔛 Fiber	
	1 13 15 17 19 21 23	
2 4 6 8 10 1	2 14 16 18 20 22 24 25 26 27 28	
Note: You can click and drag	to select one or more ports. Select All Inverse Deselect	
	Cancel	ĸ

 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.

Ruijie Rcy	cc	Local Device(NBF <			English ∽ @Remote O&M	A Network Configuration	🕞 Log O
🖧 Home		Global Settings IGMP Snooping MVR Mu	lticast Group IGMP Filter	Querier			
🕄 VLAN		MVR					
🗄 Monitor	ř	The source port must be a MVR VLAN member and t Fast Leave settings only take effect on the destination	he receiver port cannot be a MVR VL n port.	AN member.			
Ports	ř	MVR					
L2 Multicast		Save					
L3 Interfaces	č						
 Routing Security 		Port List				2 Batc	h Edit
 Security Advanced 	Ĵ	Port	Role		Fast Leave		
 Advanced Diagnostics 	÷	Gi1 NONE					
		Gi2 NONE					

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 Se	ettings	IGMP Snooping	MVR	Multicast Grou	p IGMP	Filter Querier	
() т		rt must be a MVR VLAN tings only take effect or			ort cannot be	a MVR VLAN membe	er.
	MV	R 🚺					
* M	ulticast VLAI	N VLAN0001		~			
* Sta	rt IP Addres	SS			0		
* Er	nd IP Addres	ss			0		
		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**.

3at	ch [Edit																×
			I	Role	N	IONE						\sim						
		Fá	ast Le	eave														
		Se	lect	Port														
	Ava	ailable		Ur	navail	able		1	Aggr	egate	I	Uplir	nk	Cop	oper	ы	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		
lot	e: Yo	ou ca	n clic	k an	d dra	g to s	elect	one	or mo	ore p	orts.	Sel	ect All	Inv	erse	De	select	
													Canc	ol			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.

Port List			🖉 Batch Edit
Port	Role		Fast Leave
Gi1 🕇	NONE	^	
Gi2	NONE		
	RECEIVER		
Gi3	SOURCE		
Gi4	NONE	×	

Table 6-4 Description of MVR Configuration Parameters of Ports

Parameter	Description	Default Value
Role	 NONE: Indicates that the MVR function is disabled. SOURCE: Indicates the source port that receives multicast data streams. RECEIVER: Indicates the receiver port connected to a client. 	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

1 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.

Ruíjie Rcycc			English	✓ △ Remote O&M	
🖧 Home	Global Settings IGMP Snooping MVR Multicast Group	IGMP Filter Querier			
🕫 VLAN	Multicast Group The static multicast group will not learn dynamic ports.				
Monitor Monitor Ports	Multicast List	VLAN ID		Q + Add 🗊 Delete Sel	lected
C L2 Multicast	Up to 256 entries can be added.				
⊕ L3 Interfaces ~	VLAN ID Multicast IP Addre	ss Protocol	Type Forwa	arding Port Action	
Routing ~		No Data			
⊘ Security ~	< 1 > 10/page < Go to page 1				Total 0
🖹 Advanced 🗸 🗸					

Add		×
* Multicast IP Address	0	
* VLAN ID	Select ~	
Forwarding Port	available 🔓 Aggregate 🖬 Uplink 💼 Copper 🔛 Fiber	
	9 11 13 15 17 19 21 23	
2 4 6 8	10 12 14 16 18 20 22 24 25 26 27 28	
Note: You can click and	drag to select one or more ports. Select All Inverse Deselect	
	Cancel	

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
Туре	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

 Table 6-5
 Description of Multicast Group Configuration Parameters

1 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.

Ruíjie Reyco	c	Local Device(NBF ~			Eng	jlish ~ Remote O&M Network Config	juration 🕞 Log (
🖧 Home		Global Settings IGMP Snooping MVR	Multicast Group	Querier			
🖗 VLAN		() IGMP Filter					
Monitor	×	Profile List				+ Add 🗈 🗈	elete Selected
 Ports L2 Multicast 		Profile ID B	ehavior	Start IP Address	End IP Address	Action	
B L3 Interfaces <	~			No Data			
Routing	~	< 1 > 10/page > Go to pag	e 1				Total 0
Security		Filter List					& Batch Edit
Advanced ~		Port	Profile	ID.	Max Multicast Groups	Action	
② Diagnostics ~ ② System ~		Gi1			256	Edit	
≓ system		Gi2			256	Edit	

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	PERMIT ~	
* Start IP Address		0
* End IP Address		0
		Cancel

Table 6-6 Description of Profile Configuration Pa	² arameters
---	------------------------

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	Unbound ~	
* Max Multicast Groups	256	
Select Port		
Available 💼 Unavail	lable 👖 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	
Note: You can click and dra	ag to select one or more ports. Select All Inverse Deselect	
	Cancel	ок

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

 Table 6-7
 Description of Port Filter Configuration Parameters

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**.

Ruíjie Ro	усс	Local Device(NBF ~				English ~ 🛆 Remote O&M	♣ Network Configuration ┣ Log O
🖁 Home		Global Settings IGMP Snooping	MVR Multicast Group IGM	P Filter Querier			
₽ VLAN							
🗄 Monitor	~		er than the global version. When the globa jured, the device management IP is used.	I version is lowered, the querier version	will be reduced accordingly.		
Orts	~	Ourseling Lint					
L2 Multicast	ר	Querier List					
		VLAN ID	Querier Status	Version	Src IP Address	Query Interval (Sec)	Action
L3 Interfaces	Ť	1	Disable	IGMPv2		60	Edit
Routing	~						
⊘ Security	~	888	Disable	IGMPv2		60	Edit
Advanced		2001	Disable	IGMPv2		60	Edit
Diagnostics Diagno	~	3011	Disable	IGMPv2		60	Edit
壶 System	×	3012	Disable	IGMPv2		60	Edit
		3013	Disable	IGMPv2		60	Edit
		< 1 > 10/page >	Go to page 1				Total 6

Edit		×
* VLAN ID	1	
Querier Status		
Version	IGMPv2 ~	
Src IP Address		
Query Interval (Sec)	60	
		Cancel
		Cancel

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

1 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

A 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.

Ruíjie Reyce	Local Device(NBF \sim					English ~	🛆 Remote O&M 🔒 No	etwork Configuration 🕒 Log Out
옹 Home	Port List							+ Add L3 Interface
🖉 VLAN	rore list							
🖭 Monitor		to Dynamic IP, the IPv6 address w and 64 IPv4 addresses can be c		e does not obtain an IPv4 addre	55.			
Ports ~	L3 Interfaces	Port Type	Networking	IP Address	Subnet Mask	DHCP Server	DHCP Server Info	Action
L2 Multicast	VLAN888	Management VLAN	Static IP	192.168.88.53	255.255.248.0	Disabled		Edit Delete
L3 Interfaces	< 1 > 10/page	 Go to page 1 						Total 1
L3 Interfaces								
IPv4 Config								
IPv6 Config								

Add		×
Port Type	SVI v	
Networking	Static IP V	
Primary IP/Mask	192.168.1.1 255.255.255.0 Add + ⑦	
VLAN	Select ~	
DHCP Mode	Disabled OHCP Server OHCP Relay	
	Cancel OK	

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 <u>Table 4-1</u>
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 <u>6.2</u>. 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

 Table 7-1
 Description of Configuration Parameters of L3 Interfaces

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 <u>5.6</u>.
- 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.

Ruijie Reyce	Local Device(NBF >				English 🗸 🛆 Remote O&M 💧	Network Configuration 📑 Log C
🖧 Home	IPv6 Config DHCPv6 Server	DHCPv6 Clients Static DHCPv6 I	Pv6 Neighbor List			
^{d®} ₅ VLAN	Port List					+ Add L3 Interface
E Monitor V	After the IPv4 address is set to Dynam	ic IP, the IPv6 address will not take effect if th	e interface does not obtain an IPv4 addre	155.		
Ports ~	Up to 16 MTU can be configured.					
L2 Multicast	L3 Interfaces	Port Type	Networking	IPv6 Prefix	IPv6 Address/Prefix Length	Action
L3 Interfaces ^	VLAN888	Management VLAN				Edit
L3 Interfaces	< 1 > 10/page ~	Go to page 1				Total 1
IPv4 Config						
1996 Conlig						

🛕 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.

Ruijie Rcyc									
and Home	Config DHCPv6 Server DHC	Pv6 Clients Static DHCPv6	IPv6 Neighbor List						
🖉 VLAN	ort List	Edit	n to theighten ent			×		+ Add L3 Ir	nterface
Monitor Ports	fter the IPv4 address is set to Dynamic IP, Ip to 16 MTU can be configured.	Auto Obtained IP	Obtain an IPv6 address via DHCPv6.						
C L2 Multicast	L3 Interfaces	IPv6 Address/Prefix Length	Example: 2000::1	64	Manual \sim	Add + 🕐	Pv6 Address/Prefix Length	Action	
L3 Interfaces	VLAN888	MTU	1500	(1280-1	500)			Edit	
L3 Interfaces	Gi23		Advanced Settings					Edit Clear	
IPv6 Config	1 > 10/page > Go								Total 2
Routing					Cancel	ОК			

• If no upstream DHCPv6 server is available to assign the IP address, configure the IPv6 information as follows:

Ruijie Rcy										
着 Home		IPv6 Config DHCPv6 Server DHC	Pv6 Clients Static DHCPv6	IPv6 Neighbor List						
VLAN Monitor		Port List	Edit				×		+ Add L3 In	iterface
Ø Ports		After the IPv4 address is set to Dynamic IP, Up to 16 MTU can be configured.	Auto Obtained IP	Obtain an IPv6 address via DHCPv6.						
L2 Multicast		L3 Interfaces	IPv6 Address/Prefix Length	Example: 2000::1	64	Manual	Add + 💿	Pv6 Address/Prefix Length	Action	
L3 Interfaces		VLAN888	MTU	1500	(1280-	1500)			Edit	
L3 Interfaces				Advanced Settings					Edit Clear	
IPv4 Config		Go 10/page Go	Link-local Address	FE80::ABCD:ABCD:ABCD:ABCD	0					Total 2
Routing			Subnet Prefix Name	The subnet prefix is not configured $~(I ~ \vee$						
Security			Subnet Prefix Length	64	0					
🖻 Advanced			Subnet ID	0	0					
② Diagnostics					0					
≆ System	>					Cancel	ОК			

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.

Ruijie Rcy	ycc u	ocal Device(NBF 🗸					English ~	🛆 Remote O&M 🛛 🐣 Net	twork Configuration 🕞 Log Out
දී Home ද [®] VLAN	I	Port List	et to Dynamic IP, the IPv6 address will n	ot take effect if the interface	does not obtain an IPv4 address				+ Add L3 Interface
문 Monitor	~	Up to 32 layer-3 interfac	es and 64 IPv4 addresses can be confi	igured.					
Ø Ports	~	L3 Interfaces	Port Type	Networking	IP Address	Subnet Mask	DHCP Server	DHCP Server Info	Action
L2 Multicast		VLAN888	Management VLAN	Static IP	192.168.88.53	255.255.248.0	Disabled		Edit Delete
L3 Interfaces	^	Gi23	Routed Port	Static IP	1.1.1.1	255.255.255.0	Disabled		Edit Delete
L3 Interfaces		< 1 > 10/pag	ge v Go to page 1						Total 2
Edit						×			
		Port Type	Routed Port						
		Networking	Static IP	~					
	*	Primary IP/Mask	1.1.1.1	255.255.255.0	Add + ②				
		DHCP Mode	O Disabled O DHCF	Server ODH	ICP Relay				
		* Start IP Address	1.1.1.1						
		* IP Count	254 Available IP Addresses: 253	3. End IP Address: 1	.1.1.254.				
	Externa	al IP/External User	Example: 1.1.1.1 or 1.1.1	.1-1.1.10	Add + ⑦				
	*	Lease Time (Min)	100						
					Cancel	ОК			

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 <u>7.3.3</u>.

Ruíjie Reyce	Local Device[NBF ~		English 🗸 🛆 Remote O&M 👲 Net	work Configuration 🕞 Log Out
en Home	DHCP Clients Static IP Addresses DHCP Option ARP List			
S VLAN	View DHCP clients.			0
Monitor	DHCP Clients		Search by Hostname/IP Addi Q Q Refresh	+ Batch Convert
 L2 Multicast 	Up to 1000 IP-MAC bindings can be added.			
L3 Interfaces ^	No. Hostname IP A	ddress MAC Address	Remaining Lease Time(min)	Status
L3 Interfaces		No Data		
IPv4 Config	< 1 > 10/page ~ Go to page 1			Total 0
IPv6 Config				

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

Ruíjie Reyce	Local Device(NBF ~			English 🗸 🛆 Remote O&M 🔌 Netwo	rk Configuration 📑 Log Out
and Home	DHCP Clients Static	IP Addresses DHCP Option ARP List			
S [®] VLAN	Static IP Address	List			0
Monitor Monitor Ports	Static IP Address	List	Sean	ch by IP Address/MAC A Q + Add	Delete Selected
 L2 Multicast 	Up to 1000 entries car	n be added.			
L3 Interfaces ^	No.	IP Address	MAC Address	Action	
L3 Interfaces			No Data		
IPv4 Config	< 1 > 10/;	age v Go to page 1			Total 0
IPv6 Config					

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.

Add		×
* IP	Example: 1.1.1.1	
* MAC	Example: 00:11:22:33:44:55	
	Cancel	ОК

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.

Ruijie Rcy	/CC	Local Device(NBF \vee	
음 Home		DHCP Clients Statio	c IP Addresses DHCP Option ARP List
€ [₽] VLAN			
🕾 Monitor	~	<i>i</i> DHCP Option DHCP option sett	ings are applied to all LAN ports.
Ports	~	DNS Server	Example: 8.8.8.8, each separated by a space.
🛆 L2 Multicast		Option 43	Enter an IP address or hexadecimal number.
L3 Interfaces	^	Option 138	Example: 1.1.1.1
L3 Interfaces			
IPv4 Config	ר ו	Option 150	Example: 1.1.1.1, each separated by a space.
IPv6 Config		Gateway	Example: 1.1.1.1
Routing	~		Save
😔 Security	~		

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.

i 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 .

 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.

Reyce					English 🗸 🛆	⊇Remote O&M	Network Configuration	🕞 Log Out
දී Home	IPv6 Config DHCPv6 Server DHCPv6 Clients	Static DHCPv6 IPv6 N	Neighbor List					
🖉 VLAN								
🐑 Monitor 🗸 👋	DHCPv6 Server						+ Add 🗇 Delete S	Selected
⊕ Ports ~	1, If DHCPv6 does not take effect on the Layer 3 interface 2, If the IPv6 prefix length of the Layer 3 interface is betwee	(including but not limited to i een 48 and 64, the address car	invalid IPv6 address and incorrect IPv6 address pref n be assigned.	ix of the Layer 3	interface), the DHCPv6 server cannot	ot take effect.		
 L2 Multicast 	Up to 32 entries can be added.							
L3 Interfaces ^	L3 Interfaces		IPv6 Assignment		Dħ	NS Server		Action
L3 Interfaces			No Data					
IPv4 Config	< 1 > 10/page > Go to page 1							Total 0
IPv6 Config								
IPv6 Config	Local Device(N8F				English ~	⊇ Remote O&M	😤 Network Configuration	⊡ Log Out
		_			English v – C	े Remote O&M	Network Configuration	⊨ []-Log Out
ரபரா Rcycc ஃ Home	Local Device (MIF > IPv6 Config DHCPv6 Server DHCPv6 Clients	Static DHCPv6 IPv6 I	Neighbor List	_	English	⊖Remote O&M	Network Configuration	i ⊡Log Out
Ruíjie Royco				×	English ~	-	Network Configuration + Add	
Ruffe Rcycc & Home Ø VLAN	Pv6 Config DHCPv6 Server DHCPv6 Clients DHCPv6 Server 1. If DHCPv6 does not take effect on the Layer 3 Interface	* L3 Interfaces		~	English - C			
Ruffe Rcycc	IPv6 Config DHCPv6 Server DHCPv6 Clients DHCPv6 Server	* L3 Interfaces	Select	~				
Ruffe : Rcycc A Home VLAN Monitor Ports	IPv6 Config DHCPv6 Server DHCPv6 Clients DHCPv6 Server 1. If DHCPv6 does not take effect on the Layer 3 interface is betwee	* L3 Interfaces	Select	- -	interface), the DHCPy6 server canno		+ Add Delete	
Ruffie Rcycc Home VLAN Monitor × Ports × L2 Multicast	PVG Config DHCPvG Server DHCPvG Clients DHCPvG Server I. If DHCPvG does not take effect on the Layer 3 interface 2. If the IPvG prefix length of the Layer 3 interface is betwe Up to 32 entries can be added.	* L3 Interfaces IPv6 Assignment	Select Auto		interface), the DHCPy6 server canno	ot take effect.	+ Add Delete	Selected
Ruffe Rcycc Anne VIAN Monitor * Monitor * Noritor * Iz Multicast * B L3 Interfaces *	PVG Config DHCPvG Server DHCPvG Clients DHCPvG Server I. If DHCPvG does not take effect on the Layer 3 interface 2. If the IPvG prefix length of the Layer 3 interface is betwe Up to 32 entries can be added.	* L3 Interfaces IPv6 Assignment * Lease Time (Min)	Select Auto		interface), the DHCPy6 server canno	ot take effect.	+ Add Delete	Selected

 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.

Ruíjie Reyce	Local Device(HBF >	English - 🛆 Remote O&M 🔶 N	etwork Configuration 🕒 Log O		
å Home ♂ VLAN	IPv6 Config DHCPv6 Server DHCPv6 Clients Static DHCPv6 IPv6 Neighbor List				
🗄 Monitor 🗸	DHCPv6 Clients You can view the DHCPv6 clients Information on this page.				
Ø Ports	DHCPv6 Clients	Search by IPv6 Address/DUII	Q + Bind Selected		
C L2 Multicast	No. Hostname IPv6 Address Remaining Lease Time(min)	DUID	Status		
L3 Interfaces ^	No Data				
L3 Interfaces	< 1 > 10/page < Go to page 1		Total 0		
IPv4 Config					
IPv6 Config					

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. (c) 2018 Microsoft Corporation. All ri	
C:\Users\admin <mark>></mark> ipconfig /all	
Windows IP Configuration	
Host Name	Hybrid No
Ethernet adapter	
Connection-specific DNS Suffix . : Description	Yes
	fe80::6dd5:266f:b695:55df%12(Preferred) 172.26.1.123(Preferred)
Lease Obtained	Thursday, December 22, 2022 5:29:03 PM Friday, December 30, 2022 5:28:57 PM
DHCPv6 IAID	172. 26. 1. 1 340939776
DHCFv6 Client DUID	00-01-00-01-27-C7-77-50-52-54-00-3C-D6-BE 192. 168. 58. 94

Ruíjie Rcycc	Local Device(NBF >			English ~	~ 🛆 Remote O&M	k Configuration 🕒 Log Out
B Home	IPv6 Config DHCPv6 Server	DHCPv6 Clients Static DHCPv6	Рvб Neighbor List			
문 VLAN 또 Monitor ·	🥖 Static IP Address List					
Ø Ports	Static IP Address List			Search by IPv6 Address	s/DUII Q + Add	Delete Selected
L2 Multicast	Up to 500 entries can be added					
L3 Interfaces ^	No.	IPv6 Address	DUID		Action	
L3 Interfaces			No Data			
IPv4 Config	< 1 > 10/page ~	Go to page 1				Total 0
IPv6 Config						

Rcycc	Local Device(NBF <		English 🗸 🛆 Remote O&M 🛛 🔮 Network Configuration 🕞 Log Out
🖧 Home	IPv6 Config DHCPv6 Server DHCPv6 Clients St	atic DHCPv6 IPv6 Neighbor List	
🖗 VLAN	Static IP Address List	Add ×	
Monitor	Static IP Address List	* IPv6 Address Example: 2000::1	Search by IPv6 Address/DUII Q + Add Delete Selected
 L2 Multicast 	Up to 500 entries can be added.	DUID Example: 0003000100d0f819685f	
L3 Interfaces ^	No. IPv6 Address		Action
L3 Interfaces		Салсеі Ок	
IPv4 Config	Control to the second s		Total 0
IPv6 Config			

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).

Reyce	Local Device(NBF ~			English 🗸 🛆 Remote O8	M 🔮 Network Configuration 🕒 Log Out
en Home	IPv6 Config DHCPv6 Server DHCPv6 Clients St	atic DHCPv6 IPv6 Neighbor List			
É [®] VLAN	IPv6 Neighbor List		Search by IP Addres	iss/MAC A Q + Add @ Bin	d Selected
E Monitor	Up to 1000 IP-MAC bindings can be added.				
Ports	No. MAC Address	IP Address	Туре	Ethernet status	Action
L2 Multicast L3 Interfaces			No Data		
L3 Interfaces					
IPv4 Config	< 1 > 10/page < Go to page 1				Total 0
IPv6 Config					

Pv6 Neighb	or List		Search by	IP Address/MAC A Q + Add @	Bind Selected Delete Selected
Up to 1000 IP	MAC bindings can be added.				
No.	MAC Address	IP Address	Туре	Ethernet status	Action
1	00:d0:f8:15:08:44	fe80::2d0:f8ff:fe15:844	Static	G122	Edit Delete
2	00:11:22:33:44:55	2000::1	Static	VLAN 1	Edit Delete
3	11:22:33:44:55:66	3100::1	Static	VLAN 1	Edit Delete
4	33:44:55:66:77:88	6000::1	Static	VLAN 1	Edit Delete
5	00:d0:c8:95:79:20	1200::1000	Dynamic	GI22	@ Bind
6	00:d0:c8:95:79:20	fe80::2d0:c8ff:fe95:7920	Dynamic	Gi22	d ^p Bind
7	c0:b8:e6:e2:54:63	3000::1	Dynamic	VLAN 1	@ Bind
8	c0:b8:e6:e2:54:63	fe80::c2b8:e6ff:fee2:5463	Dynamic	VLAN 1	∂ Bind
1 2	10/page Go to page 1				Tot
					Click RITA for help

Ruijie Reyce	Local Device(NBF \sim			English 🗸 🛆 Remo	ote O&M Network Configuration 🕞 Log Out
ക Home	IPvő Config DHCPvő Server DHCPvő Clients Stati	c DHCPv6 IPv6 Neighbor List			
🖗 VLAN	IPv6 Neighbor List	Add	×	Address/MAC A Q + Add	P Bind Selected
图 Monitor ~	Up to 1000 IP-MAC bindings can be added.	* Interface Select		,	
 Ports L2 Multicast 	No. MAC Address		~	Ethernet status	Action
L3 Interfaces		IPv6 Address Please enter an IPv6 address.			
L3 Interfaces	< 1 > 10/page < Go to page 1	* MAC Address Please enter a MAC address.			Total 0
IPv4 Config		Cancel	ОК		
IPv6 Config					

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**.

Ruíjie Reyce	Local Device(NBF \	e.				English 🗸 🛆 Remote O&M 🚽	🕆 Network Configuration 🛛 🕞 Log
🖧 Home	DHCP Clients	Static IP Addresses DHCI	Option ARP List				
왕 VLAN	ARP List				Search b	y IP Address/MAC A Q + a	Add 📋 Delete Selected
Ports	Up to 2000 IP-#	/IAC bindings can be added.					
 L2 Multicast 	No.	Interface	MAC Address	IP Address	Туре	Reachable	Action
L3 Interfaces ^	. 1	VLAN888	c0:a4:76:1b:0f:1b	192.168.88.197	Dynamic	Yes	∂ Bind
L3 Interfaces	2	VLAN888	c0:a4:76:1b:0e:f2	192.168.88.174	Dynamic	Yes	
IPv4 Config	. 3	VLAN888	c0:a4:76:1b:0f:1c	192.168.88.217	Dynamic	Yes	@ Bind
IPv6 Config	. 4	VLAN888	00:ee:4c:21:14:0a	192.168.88.73	Dynamic	Yes	∂ ⁹ Bind

Add		×
* IP	Enter or select an IP address.	
* MAC	Enter or select a MAC address.	
	Cancel	ОК

To remove the binding between a static IP address and a MAC address, click **Delete** in the **Action** column.

ARP	List			Search by IF	Y/MAC	Q + Add	Delete Selected
Up t	to 2000 I	P-MAC bindings can	be added.				
	No.	Interface	MAC	IP	Туре	Reachable	Action
	1	VLAN1	00:23:79:00:23:79	172.30.102.178	Static	Yes	Edit Delete
	2	VLAN1	c0:b8:e6:e9:78:07	172.30.102.209	Dynamic	Yes	

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.

Rujje Reyce	Local Device(NBF \vee				English 🗸 🛆 Remote O&M	A Network Configuration 🕒 Log O
충 Home 중 VLAN	Static Routing When a packet arrives, the device checks the device	tination field and compares it wit	h routing table. If it finds a match for destination	n network then it will forward t	hat packet from the specified interface.	0
图 Monitor V	Static Route List			Ð	cample: 1.1.1.1 Q	+ Add 🗇 Delete Selected
Ports	Up to 500 static routes can be added.					
L2 Multicast	Dest IP Address	Subnet Mask	Outbound Interface	Next Hop	Reachable	Action
L3 Interfaces ~			No Data			
Routing Static Routing_v6	< 1 ⊃ 10/page ∨ Go to page	1				Total 0
Edit				×		
* Dest IP	Address					
* Subi	net Mask 255.255.255.0					
Outbound	Interface Select	~				
۱ * ۱	Next Hop					
			Cancel	ОК		

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				ple: 1.1.1.1	Q	+ Add	Delete Selected
Up to	500 static routes can be	added.					
	Dest IP Address	Subnet Mask	Outbound Internet	ute is unreachable. Please init	iate a Ping	test from the out	bound interface to the next hop.
	2.1.1.0	255.255.255.0	Gi9	3.1.1.1		No 🕑	Edit Delete

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.

A 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.

Ruijie Rcycc	Local Device(NBF ~					English \sim	CRemote O&M A Network Configuration 🕒 Log Out
å Home	Static Routing When a packet arrives, the device checks the destination fit	ield and compares it with r	oution table. If it finds a mat	rh for dectination netwo	rk then it will forw	and that nacket from the snee	ified interface
🖗 VLAN		ield and compares it with i	outing table. If it finds a filat	ch for deschauor netwo	IK CHETTIC WILL TOTW		
图 Monitor Y	Static Route List					Example: 2000::1	+ Add 🖹 Delete Selected
Ø Ports	Up to 500 entries can be added.						
 L2 Multicast 	IPv6 Address	Prefix Length		Interface		Next Hop	Action
L3 Interfaces				No Data			
Routing Static Routing	< 1 > 10/page > Go to page 1						Total 0
Static Routing_v6							
RIP Settings							
Ruíjie Royco						Feedbala	△Remote O8M · 총 Network Configuration □ Hog Out
	Local Device(NBF ~					Liigiisii ×	Chemite Osoni & Network Configuration (\$100 Out
A Home	Static Routing When a packet arrives, the device checks the destination fi					ard that packet from the spec	ified interface.
🖉 VLAN		Add			×		
	Static Route List						+ Add 🗈 Delete Selected
Ports	Up to 500 entries can be added.	* IPv6 Address/Prefix Length	Example: 2000::1		0		
L2 Multicast	IPv6 Address					Next Hop	Action
L3 Interfaces ×		Interface	Normal Route				
Routing ^	Go to page 1	* Next Hop	Example: 2000::1				Total 0
Static Routing					_ 1		
Static Routing_v6				Cancel	ОК		
RIP Settings							

 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

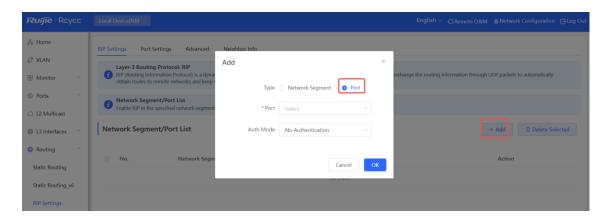
Routing Information Protocol (RIP) is ap plicable to small and medium-sized networks and is a dynamic routing protocol that is easy to configure. RIP measures the network distance based on the number of hops and selects a route based on the distance. RIP uses UDP port 520 to exchange the routing information.

8.3.1 Configuring RIP Basic Functions

Choose Local Device > Routing > RIP Settings .

Click Add and configure the network segment and interface.

Ruíjie Reyce	Local Device(NBF -> English -> @Remote ObM	Network Configuration 🕞 Log Out
ஃ Home	RIP Settings Port Settings Advanced Neighbor Info	
É [#] VLAN	Layer-3 Routing Protocol: RIP	
🖳 Monitor	() RIP (Routing Information Protocol) is a dynamic routing protocol applied to IPv4 networks. The routers running the protocol exchange the routing information through UDP packets to automatically obtain keep routes updated in real time.	n routes to remote networks and
Ø Ports	Network Segment/Port List Enable RP In the specified network segment or on the specified port.	
L2 Multicast L3 Interfaces	Network Segment/Port List	+ Add 🗇 Delete Selected
Routing		
Static Routing	No. Network Segment/Port Auth Mode A	Action
Static Routing_v6	No Data	
RIP Settings		
RIPng Settings		
Ruíjie Rcycc	Local Device(NBF ~	Network Configuration 🕞 Log Out
	English - ORemote O&M &	Network Configuration 🕒 Log Out
යි Home	RIP Settings Port Settings Advanced Neighbor Info	Network Configuration 🕒 Log Out
နံ Home တ VLAN	RIP Settings Port Settings Advanced Neighbor Info Layer-3 Routing Protocol: RIP Add ×	
යි Home	RIP Settings Port Settings Advanced Neighbor info	
နံ Home တ VLAN	RIP Settings Port Settings Advanced Neilabbor Info Layer-3 Routing Protocol: RIP Add × RIP (Routing Information Protocol) is a dyna obtain routes to remote networks and keep Add × Network Segment/Port List Type • Network Segment Port	
ී Home ඒ VLAN ම Monitor	RIP Settings Port Settings Advanced Neinhbor Info Lyer-3 Routing Protocol: RIP Add × RIP (Routing Information Protocol) is a dynar Add × RIP Routing Information Protocol: RIP Network Segment Port Network Segment/Port List * Network Segment Port * Network Segment Please enter a valid value. Example	
 ♣ Home Ø VLAN ⊕ Monitor ~ ⊗ Ports ~ 	RIP Settings Port Settings Advanced Neishbor Info Layer-3 Routing Protocol: RIP Add × Pipe Polating Information Protocol: Bip Routing Info	packets to automatically
eis Home Ø VLAN Ø Monitor ~ Ø Ports ~ O L2 Multicast	RIP Settings Port Settings Advanced Neishbor info Image: Advanced Layer-3 Routing Protocol: RIP Add × Image: Rip Coulting Information Protocol: Bit RIP in the specified network same keep Add × Image: Rip Rip in the specified network segment Port Port Image: Network Segment/Port List *Network Segment Port Image: Rip Rip in the specified network segment Please enter a valid value. Example + Add Image: Rip Rip in the specified network segment Please enter a valid value. Example + Add	packets to automatically
Home U VLAN Monitor Ports L3 interfaces X	RIP Settings Port Settings Advanced Neithboor Info Image: Approximation Protocol: RIP Add × Ref Politing Information Protocol: Bit Protocol: RIP Add × Image: Ref Politing Information Protocol: Bit Protocol: RIP Add × Image: Ref Politing Information Protocol: Bit Protocol: RIP Add × Image: Ref Politing Information Protocol: Bit Protoco	packets to automatically
 A Home Ø VLAN Ø Monitor > Ø Ports > □ L2 Multicast ⊕ L3 Interfaces ♥ Routing 	RIP Settings Port Settings Advanced Neishbor info Image: Advanced Layer-3 Routing Protocol: RIP Add × Image: Rip Coulting Information Protocol: Bit RIP in the specified network same keep Add × Image: Rip Rip in the specified network segment Port Port Image: Network Segment/Port List *Network Segment Port Image: Rip Rip in the specified network segment Please enter a valid value. Example + Add Image: Rip Rip in the specified network segment Please enter a valid value. Example + Add	packets to automatically
Home Home Home Home Home Home Home Home	RIP Settings Port Settings Advanced Neithboor Info Image: Approximation Protocol: RIP Add × Ref Politing Information Protocol: Bit Protocol: RIP Add × Image: Ref Politing Information Protocol: Bit Protocol: RIP Add × Image: Ref Politing Information Protocol: Bit Protocol: RIP Add × Image: Ref Politing Information Protocol: Bit Protoco	packets to automatically



Parameter	Description
Туре	 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. 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.
Network Segment	Enter the ne twork 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 .				
	No Authentication : The protocol packets are not authenticated.			
	Encrypted Text : The protocol packets are authenticated, and the authentication			
Auth Mode	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 .

Ruijie Rcycc		English ~ Remote O&M � Network Configuration 금 Log Ou
နိုး Home	RIP Settings Port Settings Advanced Neighbor Info	
台 VLAN	Port List	
🕾 Monitor 🗸		
Ports ~	Port Name Rx Status Tx Status Poison Reverse v2 Broadcast Packet	Auth Mode Auth Key Action
 L2 Multicast 	No Data	
⊕ L3 Interfaces ∨		
Routing		
Static Routing		
Static Routing_v6		
RIP Settings		

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

 Table 8-4
 Configuration Parameters in the Port List

Parameter	Description
	performance.
	No Authentication : The protocol packets are not authenticated.
	Encrypted Text : The protocol packets are authenticated, and the authentication
Auth Mode	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
Aduit Key	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.

Ruíjie Rcycc				Er	nglish ~ 🛆 Remote O&M	A Network Configuration	🕞 Log Out
🖧 Home	RIP Settings Port Settings	Advanced Neighbor Info					
≟ [₽] VLAN	Improper timers may cause re	oute flapping. Therefore, RIP timer	s must be consistent on the devices co	nnected to the same network. You a	re not advised to reset the PI	P timers unless you have snerific	
🖞 Monitor 🗸 🗸	needs.						
Ø Ports	RIP Global Config					Edit Co	nfig
L2 Multicast	RIP Version	Route Advertisement	Administrative Distance	Update Timer	Invalid Timer	Flush Timer	
⊕ L3 Interfaces ∨	Default	Off	1 (Default)	30 s	180 s	120 s	
Routing Static Routing	Route Redistribution List Redistribute the routes of oth	er protocols to the RIP domain so	that RIP can communicate with other n	outing domains.			
Static Routing_v6	Route Redistribution List	t				+ Add 🗊 Delete Selee	ted
RIP Settings	Туре		Administrative Distance	Instance ID		Action	
RIPng Settings			No Da	ta			
OSPFv2							
OSPFv3	RIP update packets will be su	ppressed on the passive interface.	If the device connected to the interface	e does not adopt RIP, you are advise	d to enable this function.		
Route Info	Passive Interface					+ Add 🗇 Delete Selee	ted
«Collapse							

Ruijie Rcycc	Local Device(NBF ~					English ~	C Remote O&A	세 🔮 Network Configuration 🕞 Log Out
🖧 Home	RIP Settings Port Settings Advanced	Neighbor Info						
∄ VLAN	Improper timers may cause route flapping. T needs.	Edit Config			×	twork. You are not adv	ised to reset the R	IP timers unless you have specific
Monitor Monitor	RIP Global Config	RIP Version	Default		~ (?)			Edit Config
 L2 Multicast 	RIP Version Route Ad	Route Advertisement				e 1	nvalid Timer	Flush Timer
⊕ L3 Interfaces	Default	Administrative	1 (Default)				180 s	120 s
Routing	Route Redistribution List Redistribute the routes of other protocols to	Distance						
Static Routing	Route Redistribution List	* Update Timer	30	s (5-2147483647)				+ Add 🕅 Delete Selected
Static Routing_v6	1	* Invalid Timer	180	s (5-2147483647)		nstance ID		Action
RIPng Settings	Туре	* Flush Timer	120	s (5-2147483647)		nstance ID		Action
OSPFv2	 Passive Interface 			Cancel	ОК			

Parameter	Description
	Default : Select RIPv2 for sending packets and RIPv1/v2 for receiving packets.
RIP Version	V1 : Select RIPv1 for sending and receiving packets.
	V2 : Select RIPv2 for sending and receiving packets.
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.
	If no update is received before the flush timer of an invalid route expires, the
Flush Timer	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.

Ruíjie Rcycc	Local Device(NBF ~		English - 스 Remote O&M 🔮 Network Configuration 금 Log Out
ക Home	Improper timers may cause route flapping. Th needs.	nerefore, RIP timers must be consistent on the devices connected to the same network	work. You are not advised to reset the RIP timers unless you have specific
🖇 VLAN	RIP Global Config	Add ×	Edit Config
문 Monitor 🗸	RIP Version Route Ad	* Type Select V	Invalid Timer Flush Timer
Ports	Default		180 s 120 s
L2 Multicast		* Administrative 0 (Administrative Distance)	
	Redistribute the routes of other protocols to	Distance	
Routing	Route Redistribution List	Cancel	+ Add 🔯 Delete Selected
Static Routing	Туре	Administrative Distance Ins	tance ID Action
Static Routing_v6		No Data	
RIP Settings			

Table 8-6 RIP Route Redistribution on Parameters

Parameter	Description
	Direct Routing
Туре	OSPF Routing
	Static Routing
Administrative Distance	A smaller administrative distance indicates a higher priority. The default value is ${f 0}$. 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.

Add
* Type OSPF Routing

* Administrative	0 (Administrative Distance)	~
Distance		
* Instance ID	Select	~
	Cancel	ОК

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.

Ruíjie Royco	Local Device(NBF > English > ORemote ORM Network Configuration Elog Out
ea Home	
🖉 VLAN	Type Add × Action
倒 Monitor 👋	* Passive Interface Select
Ø Ports	Passive Interface
L2 Multicast	un dome faves un se adhiezaie er or
🕀 L3 Interfaces 👋	Passive Interface Cancel OK + Add @ Delete Selected
Routing	Port Name Action
Static Routing	No Deta
Static Routing_v6	
RIP Settings	If a route cannot forward broadcast packets, another router is designated as the neighbor to establish a RIP direct link.
RIPng Settings	Neighbor Route + Add Delete Selected

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.

Reyce					
🖧 Home	- 1				
🖉 VLAN	Туре	Add	nstance ID		Action
🖭 Monitor		* Neighbor Route			
Ø Ports	Passive Interface	* Neighbor Koute			
L2 Multicast	RIP update packets will be suppressed on the .			I to enable this function.	
L3 Interfaces	Passive Interface		Cancel	+ Ad	d 🗇 Delete Selected
Routing		Port Name		Action	
Static Routing			No Data		
Static Routing_v6	Malakhar Barda				
RIP Settings	Neighbor Route If a router cannot forward broadcast packets	, another router is designated as the neighbor to o	establish a RIP direct link.		
RIPng Settings	Neighbor Route			+ Ad	d 🗇 Delete Selected
OSPFv2		Address		Action	
OSPFv3			No Data		
Route Info					

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.

Ruijie Rcycc	Local Device(NBF 😔	English ~	C Remote O&M	A Network Configuration	🕞 Log Out
යි Home	RIPng Settings Port Settings Advanced Neighbor Info				
≝ ^p VLAN	- Laver-3 Routing Protocol- BIDog				
딸 Monitor ~	RIPng (Routing Information Protocol next generation) is a unicast routing protocol applied to IPv6 networks.				
Ports	Network Segment/Port List Enable RIPing in the specified network segment or on the specified port.				
L2 Multicast	Network Segment/Port List			+ Add 🗇 Delete Sel	acted
L3 Interfaces	Network Stylinery for List			E Delete Sel	Rector
Routing	No. Network Segment/Port		Action		
Static Routing	No Data				
Static Routing_v6					
RIP Settings					
RIPng Settings					

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.

Rcycc		
🖧 Home	RIPng Settings Port Settings Advanced Neichbor Info	_
🔗 VLAN	Layer-3 Routing Protocol: RIPng Diport Bradient Information Protocol and as	
문 Monitor 🗸	Type • Network Segment • Port	
Ports	Network Segment/Port List Enable RIPng in the specified network segm Network Segment Example: 2000:1	
L2 Multicast	Network Segment/Port List	+ Add 🔹 Delete Selected
L3 Interfaces ×		
Routing ^	Cancel OK	Action
Static Routing	No Data	
Static Routing_v6		
RIP Settings		
RIPng Settings		

If the address length is between 48 and 64, the address will be used as a prefix.

Ruíjie Rcycc			
🐣 Home	RIPng Settings Port Settings Advanced	Neighbor Info	
🕼 VLAN	A Rayer-3 Routing Protocol: RIPng RIPng (Routing Information Protocol next ge	dd ×	
Ports	Network Segment/Port List Enable RIPng in the specified network segment	Type O Network Segment O Port	
L2 Multicast L3 Interfaces	Network Segment/Port List		+ Add 🖄 Delete Selected
Routing	No.	Cancel	Action
Static Routing		No Data	
Static Routing_v6			
RIP Settings			
RIPng Settings			

Alternatively, enable RIPng on a specified port:

Parameter	Description
Туре	 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. 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.
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 .

 Table 8-7
 RIPng Configuration Parameters

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.

Ruíjie Reyce			English ~ @Remote O&M & Network Configuration 🕒 Log Out
ී Home ි VLAN	RIPng Settings Port Settings Advanced Ne Port List	ghbor Info	
፼ Monitor ~ ⊗ Ports ~	Port Name	IPv6 Poison Reverse	Action
L2 Multicast		No Data	
⊕ L3 Interfaces ∨			
Routing ^			
Static Routing			
Static Routing_v6			
RIP Settings			
RIPng Settings			
Edit		×	
* Port	Name VLAN 1	\sim	
IPv6 Poison R	everse		
	Car	cel OK	

8.4.3 Configuring the RIPng Global Configuration

Choose Local Device > Routing > RIPng Settings > Advanced > RIPng Global Configuration , and click Edit Config .

Rujje Rcycc	Local Device(NBF ~			English ∽ Remote O&M	। 🐣 Network Configuration 🕞 Log Ou
🖧 Home	RIPng Settings Port Settings	Advanced Neighbor Info			
🔄 VLAN	Improper timers may cause route f	lapping. Therefore, RIPng timers must be c	onsistent on the devices connected to the same	e network. You are not advised to reset the	RIPng timers unless you have
🐑 Monitor 🗸 👋	specific needs.				
Ports ` `	RIPng Global Config				Edit Config
 L2 Multicast 	Route Advertisement	Administrative Distance	Update Timer	Invalid Timer	Flush Timer
⊕ L3 Interfaces ∨	Off	1 (Default)	30 s	180 s	120 s
Routing Static Routing	Route Redistribution List Redistribute the routes of other pre-	otocols to the RIP domain so that RIP can c	ommunicate with other routing domains.		
Static Routing_v6	Route Redistribution List				+ Add 🗇 Delete Selected
RIP Settings	Ту	pe	Administrative Distance		Action
RIPng Settings			No Data		
Ruíjie Rcycc					
ి Home					

ှိ Home	RIPng Settings Port Settings Advanced	Neighbor Info					
E VLAN	Improper timers may cause route flapping. T specific needs.	Edit Config			×	network. You are not advised to reset the	RIPng timers unless you have
🐏 Monitor 🛛 👋	specific needs.	Route Advertisement					
Ports	RIPng Global Config						Edit Config
L2 Multicast	Route Advertisement	Administrative Distance	1 (Default)		Invalid Timer	Flush Timer
L3 Interfaces	Off	Distance				180 s	120 s
Routing ^	Dente De l'articultur	* Update Timer	30	s (1-65535)			
Static Routing	Redistribute the routes of other protocols to			(4.05520)			
Static Routing v6	Route Redistribution List	* Invalid Timer	180	s (1-65535)			+ Add 🗇 Delete Selected
	1	* Flush Timer	120	s (1-65535)			
RIP Settings	Туре						Action
RIPng Settings							
OSPFv2	Passive Interface			Cancel	ОК		
OSPFv3	RIP update packets will be suppressed on the	e passive interface. If the dev	ice connected	to the interface does no	ot adopt RIP	you are advised to enable this function.	

Table 8-8 RIPng Global Config	uration 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.

 $\label{eq:choose Local Device > Routing > RIPng Settings > Advanced > Route Redistribution List \ , \ and \ click + Add \ .$

Ruíjie Rcycc	Local Device(NBF >		English ∽ Remote O&M	Network Configuration 🕒 Log Out
🖧 Home	RIPng Settings Port Settings Advanced	Neighbor Info		
	Improper timers may cause route flapping. T specific needs.	Add ×	c network. You are not advised to reset the RI	Png timers unless you have
Ports ~	RIPng Global Config	* Type Select ~		Edit Config
L2 Multicast	Route Advertisement 4	Administrative 0 (Administrative Distance)	Invalid Timer	Flush Timer
L3 Interfaces ~	Off		180 s	120 s
Routing ^ Static Routing	Route Redistribution List Redistribute the routes of other protocols to	Cancel OK		
Static Routing_v6	Route Redistribution List			Add 🗊 Delete Selected
RIP Settings	Туре	Administrative Distance		Action
RIPng Settings		No Data		

 Table 8-9
 RIP Route Redistribution Parameters

Parameter	Description	
	Direct Routing	
Туре	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 adv ised 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.

Rujjie Rcycc	Local Device(NBF			English 🗸 🛆 Remote Oð	dM . ♠ Network Configuration [] Log Ou
🖧 Home	1			(a	
్లి VLAN	Туре	Add	×		Action
🗐 Monitor 👘		* Passive Interface Select	~		
Ports	Passive Interface RIP update packets will be suppressed on the			advised to enable this function.	
L2 Multicast	KOP update packets will be suppressed on the			advised to enable this function.	
L3 Interfaces ×	Passive Interface		Cancel		+ Add Delete Selected
Routing		Port Name		Action	
Static Routing			No Data		
Static Routing_v6					
RIP Settings	RIPng Aggregate Routing Create an aggregate RIPng route announcen	ient.			
RIPng Settings	RIPng Aggregate Routing				+ Add

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).

Ruíjie Rcycc		
ಕಿ Home		
^{2⊕} ∋ ² VLAN	Add ×	Action
😰 Monitor 🛛 👋	* IPv6 Aggregate	
Ø Ports	Passive Interface Ref update packets will be suppressed on the	ou are advised to enable this function.
L2 Multicast		
⊕ L3 Interfaces ~	Passive Interface Cancel OK	+ Add 🖹 Delete Selected
Routing ^	POLINAR	Action
Static Routing	No Data	
Static Routing_v6	RIPng Aggregate Routing	
RIP Settings	Create an aggregate RIPng route announcement.	
RIPng Settings	RIPng Aggregate Routing	+ Add
OSPFv2	Address	Action
OSPFv3	No Data	

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.

Ruijie Reyce	Local Device(NBF ~	Network Configuration	🕞 Log Out
പ്പ് Home			
중 VLAN			
딸 Monitor 🗸	OSPF		
Ø Ports	OSPF is a typical link-state routing protocol. To satisfy users' increasing requirements for network reliability		
C L2 Multicast	Aread and heterogeneity on a large network, OSPF solves the problems such as slow convergence, unscientific metric		
L3 Interfaces	Areal Area2 values, and poor scalability. Highlights		
Routing	A5 • Achieves fast convergence.		
Static Routing	Minimizes routing overhead.		
Static Routing_v6	• Reduces routing update traffic through area partition.		
RIP Settings	 Applies to various networks with up to thousands of switches. 		
RIPng Settings			
OSPFv2			
OSPFv3			e
Route Info	Start Setup		Ai
« Collapse			

(1) Configure an instance.

① Configure the insta	2 ance. Configure the interface.	(3) Operation succeeded.
* Instance ID		
* Router ID		0
Advertise Default Route		
Import External Route	Static Route Redistribution Direct Route Redistribution RIP Redistribution	
	Details	



Table 8-10 Instance Configuration Parameters

Parameter	Description	
Create an OSPF instance based on the service type.		
Instance ID	The instance only takes effect locally, and does not affect packet exchange with other devices .	
	It identifies a router in an OSPF domain.	
Router ID	A Caution	
	Router IDs within the same domain must be unique. The same	

Parameter	Description
	configuration may cause neighbor discovery failures.
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.
Details	Expand the detailed configuration.

Details

Distance	Intra-Area	Op	Optional.Default:110	
	Inter-Area	Opt	tional.Default:110	
	External	Optio	onal.Default:110	
LSA	Genaration [Delay	Optional.Defau	
	Received De	lay	Optional.Default	
SPF Calculation	Waiting Inte	rval	Optional.Defaul	
	Min Interval	C	ptional.Default:50	
	Max Interval	0	Optional.Default:50	
Graceful Restart	Graceful Res	tart		
	He	per		
	LSA Ch	eck (
	* Max Wait T	ime	1800	

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.
	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.
SPF Calculation	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 (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.
Graceful Restart	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.

Table 8-11 Parameters in the Instance Detailed Configura	tion
--	------

(2) Configure an interface.

			(1)- Configure the in	2 nstance. Configure the int	3 erface. Operation succee	ded.			
			* Interfa	ace Select					
			* A	rea					
			Stub A	rea 🕥					
				Details					
			Prio	rity Optional.Default:1					
Port List				Add					
Up to 16 entries can be added.									
Interface	Area	Priority	Network Type	Hello Packets	Dead Interval	Interface Auth	LSA Transmission Delay	LSA Retransmission Interval	Action
				No Data					
< 1 > 10/page >	Go to page 1								Total 0
				Previous	Finish				

 Table 8-12
 Interface Configuration Parameters

Parameter	Description
Interface	Select the OSPF-enabled L3 interface.
Area	Configure the area ID. Value range: 0-4294967295
	If Stub Area is enabled, you need to configure the area type and inter-area route isolation.
Stub Area	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.
	Not-So-Stubby Area (NSSA): A few external routes can be imported.
	Inter-area route isolation: After this function is enabled, inter-area routes will not be
	imported to this area.
Details	Expand the detailed configuration.

1 Configure the insta	2 nce. Configure the interface.	(3) Operation succeeded
	Details	
Priority	Optional.Default:1	
Network Type	Broadcast v	
Hello Packets	Optional.Default:10(s)	
Dead Interval	Optional.Default:40(s)	

LSA Transmission	Optional.Default:1(s)	
Delay		
LSA Retransmission	Optional.Default:5(s)	
Interval		
Interface Auth	No Auth \sim	
Ignore MTU Check		
	Add	

Table 8-13 Parameters in the Interface Detailed Configuration

Parameter	Description
Priority	It is 1 by default.
	Broadcast
Network Type	Unicast
	Multicast
	Non-Broadcast Multiple Access
Hello Packets	Interval for periodic transmission, which is used to discover and maintain OSPF
Tiello Fackets	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	Time after which LSA is retransmitted after LSA is lost. The default value is 5
Interval	seconds.
	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
Interface Auth	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.

Ruijie	Currently in Local Device mode.	English ~	٥	٩	₽
	Operation succeeded.				×
	13				
	Configure the instance. Configure the interface. Operation succeeded				
	\checkmark				
	Operation succeeded.				
	Disable				

8.5.2 Adding an OSPFv2 Interface

 $\label{eq:choose Local Device > Routing > OSPFv2} \ , \ click \ More \ in the \ Action \ column, \ and \ select \ V2 \ Interface \ .$

Ruíjie Rcycc	Local Device(NBF \vee					English 🗸 🛆 Remote O&M 👲 Netv	vork Configuration 🕒 Log Out
응 Home	Instance List						+ Add
🗄 Monitor 🗸	Up to 8 entries can be ac	ided.					
Ports	Instance ID	Router ID	Interface	Area	Advertise Default Route	Import External Route	Action
L3 Interfaces	8	123.1.1.1	Gi23	12(Normal Area)	Disable	Static Route Redistribution : Off Direct Route Redistribution : Off RIP Redistribution : Off	More Neighbor Info Edit Delete
Static Routing Static Routing_v6	< 1 > 10/pag	e v Go to page	• 1				Total 1
RIP Settings							
RIPng Settings							
OSPFv2							

Ruíjie Reyce	Local Device(NBF <	English - 🛆 Remote O&M 🛭 🖨 Network Configuration 🕞 Log Out
ී Home	Instance List	+ Add
🖉 VLAN		T AUU
🖳 Monitor 🗸	Up to 8 entries can be added.	
Ports		Advertise Default
L2 Multicast	Instance ID Router ID Interface Area	Route V2 Interface
L3 Interfaces ~		V2 Instance Route Redistribution More
Routing ^	8 123.1.1.1 Gi23 12(Normal /	Area) Disable V2 Neighbor Management ighbor Info Edit Delete
Static Routing		
Static Routing_v6	< 1 > 10/page v Go to page 1	Total 1
RIP Settings		
RIPng Settings		
OSPFv2		
03FTV2		
Ruíjie Reyce	Local Device(NBF	English 🗸 🛆 Remote O&M 🔞 Network Configuration 🕒 Log Out
and Home	Instance List	+ Add
É ⁹ VLAN	Up to 8 entries can be added.	
🗄 Monitor 🗸	op to o chines can be added.	
OPorts	Instance ID Router ID Interface Area	Advertise Default Action
L2 Multicast		Koute V2 Interface
⊕ L3 Interfaces ∨	8 123.1.1.1 Gi23 12(Normal A	V2 Instance Route Redistribution More Ivrea) Disable V2 Neighbor Management ighbor Info
Routing ^		Edit Delete
Static Routing	< 1 > 10/page < Go to page 1	Total 1
Static Routing_v6	toppage - corcepage 1	
RIP Settings		
RIPng Settings		
OSPFv2		
Ruíjie Rcycc	Local Device(NBF 😒	V2 Interface X
ిం Home	Instance List	Interface Select
🔗 VLAN	Up to 8 entries can be added.	* Area
🐑 Monitor 🗠	up to o entries can be abbed.	Stub Area
Ports	Instance ID Router ID Interface Area	Details
L2 Multicast		
⊕ L3 Interfaces ~	8 123.1.1.1 Gi23 12(Normal	Port List Add Reset
Routing		Up to 64 entries can be added.
Static Routing	< 1 > 10/page > Go to page 1	LSA LSA
Static Routing_v6		Interfac Area Priority Networ Hello Dead Interfac Transmi Retrans Ac e Area Priority kType Packets Interval e Auth ssion mission
RIP Settings		e k type rackets interval e Auth salon mission Delay interval
RIPng Settings		Gi23 12 Broadca No Auth Edit
OSPFv2		
		< 1 → 10/page ∨ Go to page 1 Total 1

8.5.3 Redistributing OSPFv2 Instance Routes

Choose Local Device > Routing > OSPFv2 , click More in the Action column, and select V2 Instance Route Redistribution .

Ruijie Rcycc	Local Device(NBF 🗸	English 🗸 🛆 Remote O&M 🛭 🕭 Network Conf	guration 🕞 Log Out
å Home	Instance List		+ Add
ấ ⁹ VLAN			+ Add
🗄 Monitor 🗸 🗸	Up to 8 entries can be added.		
Ports	Instance ID Router ID Interface	Area Route	Action
 L2 Multicast 		V2 Interface V2 Instance Route Redistribution	More
L3 Interfaces ~	8 123.1.1.1 Gi23		ighbor Info
Routing ^		te	lit Delete
Static Routing	< 1 > 10/page < Go to page 1		Total 1
Static Routing_v6			
RIP Settings			
RIPng Settings			
OSPFv2			
		V2 Instance Route Redistribution	
ເດັນເບັນເ Revec	Local Device(NBF 🗸	Route Redistribution Route Redistribution	×
🖧 Home	Instance List	Koute Redistribution cannot select its own instance number	
🜮 VLAN	-	* Instance ID Select V	
🖳 Monitor 🛛 👋	Up to 8 entries can be added.	Metric Default:20	
Ports ~	Instance ID Router ID Interface	Area Deute Dedistribution List	
L2 Multicast	instance iD Router iD interface	Area Route Redistribution List Add	Reset
L3 Interfaces ` ` ` ` ` ` ` ` ` ` ` ` ` ` ` ` ` ` ` ` ` `	8 123.1.1.1 Gi23	Up to 63 entries can be added. #2(Normal Are	
Routing	8 123,1.1.1 0123	rzywormał Are Instance ID Metric	Action
Static Routing	C 1 > 10/page ~ Go to page 1	No Data	
Static Routing_v6			
RIP Settings		< 1 > 10/page ~ Go to page 1	Total 0

8.5.4 Managing OSPFv2 Neighbors

Choose Local Device > Routing > OSPFv2 , click More in the Action column, and select V2 Neighbor Management .

Ruíjie Rcycc					English 🗸 🛆 Remote O&M 🔮 Netw	ork Configuration 🕞 Log O
සි Home හි VLAN	Instance List					+ Add
🗄 Monitor 🗸	Up to 8 entries can be	added.				
Ports	Instance ID	Router ID	Interface	Area	Advertise Default Route V2 Interface	Action
B L3 Interfaces ∨ B Routing ∧	8	123.1.1.1	Gi23	12(Normal Area)	V2 Instance Route Redistribution Disable V2 Neighbor Management	More Highbor Info Edit Delete
Static Routing	< 1 > 10/p	age 🧹 Go to pag	e 1			Total 1
Static Routing	C 1 > 10/p	age ∨ Go to pag	e 1	V2 Neigi	Nor Management	Total 1
Ruíjíe Rcycc	Local Device(NBF >	age ∨ Go to pag	• 1	· · · ·	nbor Management Neighbor IP	
ரைம் Rcycc ஃ Home லீ VLAN		-	•	· · · ·	Neighbor IP	
	Local Device(NBF >	-	Interface	Neight Up to 6	Neighbor IP	×
Ruffie Rcycc & Home & VLAN ⊕ Monitor ~ ⊕ Ports ~	Local Device(NBF Instance List Up to 8 entries can be	t added.		Neighb	Neighbor IP	×
Ruífie Reyce À Home Ø VLAN B Monitor	Local Device(NBF Instance List Up to 8 entries can be	t added.		Neight Up to 6	Neighbor IP Or List A 4 entries can be added.	xdd Reset

8.5.5 Viewing OSPFv2 Neighbor Information

Choose Local Device > Routing > OSPFv2 , and click Neighbor Info in the Action column.

Reyce	Local Device(NBF \vee					English 🗸 🛆 Remote O&M Net	work Configuration 🕒 Log
🖧 Home	Instance List						+ Add
🖇 VLAN							
된 Monitor 🗸	Up to 8 entries can be a	idded.					
Ports	Instance ID	Router ID	Interface	Area	Advertise Default Route	Import External Route	Action
L2 Multicast L3 Interfaces Routing	8	123.1.1.1	GiZ3	12(Normal Area)	Disable	Static Route Redistribution : Off Direct Route Redistribution : Off RIP Redistribution : Off	More Neighbor Info Edit Delete
Static Routing	< 1 > 10/pa	ge 🗸 Go to page					Total 1
Rcycc	Local Device(NBF V			Naiakha	r Info		
Ruராச Rcycc	Local Device(NBF		_	Neighbo			
		added.	-	Neighbo		Status Neighb	
home VLAN	Instance List	sdded.				Status Neighb No Data	or IP Interface
5 Home 7 VLAN 9 Monitor ~ 9 Ports ~	Instance List	ndded. Router ID	Interface		e ID Router ID		
5 Home 7 VLAN 9 Monitor ~ 9 Ports ~ 3 L2 Multicast	Up to 8 entries can be a		Interface	Instanc	e ID Router ID	No Data	or IP Interface
5 Home 7 VLAN 8 Monitor × 9 Ports × 3 L2 Multicast 4 L3 Interfaces ×	Up to 8 entries can be a		interface Gi23	Instanc	e ID Router ID	No Data	
5 Home 7 VLAN 8 Monitor × 9 Ports × 3 L2 Multicast 4 L3 Interfaces ×	Instance List Up to ® entities can be a Instance ID	Router ID 123.1.1.1		Instanc	e ID Router ID	No Data	
§ Home Ø VLAN Ø Ports × Ø L2 Multicast Ø El Interfaces × Ø Routing ∧	Instance List Up to 8 entries can be a Instance ID	Router ID 123.1.1.1		Instanc	e ID Router ID	No Data	
5 Home 7 VLAN 9 Ports × 9 Ports × 9 Datas 1 L2 Multicust 9 L3 Interfaces × 9 L3 Interfaces × 9 L3 Interfaces × 9 Routing <	Instance List Up to ® entities can be a Instance ID	Router ID 123.1.1.1		Instanc	e ID Router ID	No Data	
Home VLAN Nonitor VLAN Nonitor La Multicast La Multicast La Interfaces Static Routing Static Routing_v6	Instance List Up to ® entities can be a Instance ID	Router ID 123.1.1.1		Instanc	e ID Router ID	No Data	

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.

Ruíjie Rcycc	Local Device(NEF > CRemote ORM
🖧 Home	
27 VLAN	
찦 Monitor 🗸	OSPF
Ø Ports ~	OSPF is a typical link-state routing protocol. To satisfy users' increasing requirements for network reliability
 L2 Multicast 	and neterogeneity on a large network. USPr solves the problem such as allow convergence, unscientific metric
L3 Interfaces ~ ~	Area1 Area2 values, and poor scalability.
Routing	AS • Achieves fast convergence.
Static Routing	Minimizes routing overhead.
Static Routing_v6	 Reduces routing update traffic through area partition.
RIP Settings	 Applies to various networks with up to thousands of switches.
RIPng Settings	
OSPFv2	
OSPFv3	e e e e e e e e e e e e e e e e e e e
Route Info	Start Setup
Collapse	

• 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.

(1)	(3)
Configure the insta	ance. Configure the interface. Operation succeeded.
* Router ID	0
Advertise Default Route	
Import External Route	Static Route Redistribution Direct Route Redistribution RIP Redistribution
	Details



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. A Caution Router IDs within the same domain must be unique. The same configuration may cause neighbor discovery failures.				
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)	ace. Configure the interface. Operation succeeded.	
configure the firsta	Compute the interface. Operation succeeded.	
* Router ID	0	
Advertise Default		
Route	Metric Optional.Default1	
	Type 2 \checkmark ⑦	
mport External Route	Static Route Redistribution	
	Metric Optional.Default:20 Direct Route Redistribution	
	Metric Optional.Default:20	
	RIP Redistribution	
	Metric Optional.Default20	
	Details	
Distance	Intra-Area Optional.Default:110	
	Inter-Area Optional.Default:110	
	External Optional.Default:110	
LSA	Genaration Delay Optional.Defat	
	Received Delay Optional.Default Previous Next	
0	Previous Next	
<u> </u>	Previous Next	
Configure the insta	Previous Next 2 3 nce. Configure the interface. Operation succeeded.	
Configure the insta	Previous Next 2 3 nce. Configure the interface. Operation succeeded. Metric Optional.Default:20	
Configure the insta	Previous Next a a a a a a a a a a a a a a a a a a	
Configure the insta	Previous Next	
Configure the insta	Previous Next Image: Configure the interface. Operation succeeded. Metric Optional.Default:20 Image: Redistribution Details Details Optional.Default:110	
Configure the insta	Previous Next Ince. Configure the Interface. Operation succeeded. Metric Optional.Default20 Intra-Area Optional.Default110 Inter-Area Optional.Default110	
Configure the insta	Previous Next Image: Configure the interface. Operation succeeded. Metric Optional.Default:20 Image: Redistribution Details Details Optional.Default:110	
Configure the insta	Previous Next Ince. Configure the Interface. Operation succeeded. Metric Optional.Default20 Intra-Area Optional.Default110 Inter-Area Optional.Default110	
Configure the insta	Previous Next Image: Configure the interface. Operation succeeded. Metric Optional.Default20 Image: Redistribution Details Details Details Intra-Area Optional.Default110 Inter-Area Optional.Default110 External Optional.Default110	
Configure the insta	Previous Next 2 3 Rec. Configure the interface. Operation succeeded. Metric Optional.Default20 2 RIP Redistribution Metric Optional.Default20 Details Optional.Default110 Inter-Area Optional.Default110 External Optional.Default110 Genaration Delay Optional.Default Received Delay Optional.Default	
Configure the insta	Previous Next Image: Configure the interface. Operation succeeded. Metric Optional.Default20 Intra-Area Optional.Default10 Inter-Area Optional.Default10 External Optional.Default10 External Optional.Default10 External Optional.Default10 Optional.Default10 Optional.Default10	
Configure the insta	Previous Next 2 3 Rec. Configure the interface. Operation succeeded. Metric Optional.Default20 2 RIP Redistribution Metric Optional.Default20 Details Optional.Default110 Inter-Area Optional.Default110 External Optional.Default110 Genaration Delay Optional.Default Received Delay Optional.Default	

Previous Next

Helper LSA Check * Max Wait Time 1800

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.
	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.
SPF Calculation	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 (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.
Graceful Restart	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.

Table 8-15 Parameters in the Instance Detailed Configuration

2. Configure an interface.

								×
		1		2		3		
		Configure the in	istance. C	onfigure the in	terface. O	peration succeed	led.	
		* Interfa	ce Gi2/14		~			
		* Ar	ea 12					
		Stub Ar	ea 🔵					
				Details				
				Add				
Port List								
Up to 16 entri	es can be added.							
Interface	Area	Priority	Network Type	Hello Packets	Dead Interval	LSA Transmission Delay	LSA Retransmissi on Interval	Action
				No Data				
< 1 →	10/page 🗸	Go to page	1					Total 0
			_	Previous	Finish			

 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	If Stub Area is enabled, you need to configure the area type and inter-area route isolation. 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. Not-So-Stubby Area (NSSA): A few external routes can be imported.
Details	Expand the detailed configuration.

		(1)	(2)		(3)		
		Configure the insta	nce. Configure the in	terface. Op	peration succeed	led.	
			Details				
		Priority	Optional.Default:1				
		Network Type	Broadcast	~			
		Hello Packets	Optional.Default:10(s)				
		Dead Interval	Optional.Default:40(s)				
			Add				
Port List							
Up to 16 entri	es can be added.						
Interface	Area	Priority	work Hello pe Packets	Dead Interval	LSA Transmission Delay	LSA Retransmissi on Interval	Action
			No Data		,		
< 1 S	10/2222	Go to page 1					Total
	10/page 🗸	do to page					Iotai
			Previous	Finish			
							×
		1	2				
		Configure the instal	nce. Configure the in	terrace. Op	peration succeed	led.	
		LSA Transmission	Optional.Default:1(s)				
		LSA Transmission Delay	Optional.Default:1(s)				
		Delay LSA Retransmission	Optional.Default:1(s) Optional.Default:5(s)			1	
		Delay					
		Delay LSA Retransmission	Optional.Default5(s)				
		Delay LSA Retransmission Interval	Optional.Default5(s)				
Port List		Delay LSA Retransmission Interval	Optional.Default5(s)				
	es can be added.	Delay LSA Retransmission Interval	Optional.Default5(s)				
	es can be added.	Delay LSA Retransmission Interval	Optional.Default5(s)				
	es can be added. Area	Delay LSA Retransmission Interval Ignore MTU Check Priority Net	Optional.Default5(s)	Dead	LSA Transmission	LSA Retransmissi	Action
Up to 16 entrie		Delay LSA Retransmission Interval Ignore MTU Check Priority Net	Optional.Default5(s) Add work Hello pe Packets				Action
Up to 16 entrie	Area	Delay LSA Retransmission Interval Ignore MTU Check Priority Net	Optional.Default:5(s)		Transmission	Retransmissi	
Up to 16 entrie		Delay LSA Retransmission Interval Ignore MTU Check Priority Net	Optional.Default5(s) Add work Hello pe Packets		Transmission	Retransmissi	Action
Up to 16 entri	Area	Delay LSA Retransmission Interval Ignore MTU Check Priority Net	Optional.Default5(s) Add work Hello pe Packets		Transmission	Retransmissi	
Up to 16 entri	Area	Delay LSA Retransmission Interval Ignore MTU Check Priority Net	Optional.Default5(s) Add work Hello pe Packets		Transmission	Retransmissi	

									×
LSA Transmission Optional.Default:1(s) Delay LSA Retransmission Optional.Default:5(s) Interval Ignore MTU Check C Add Port List Up to 16 entries can be added. Interface Area Priority Network Hello Dead Interval Collay Retransmissi Action G12/14 12 Broadcast Delete C 1 10/page Go to page 1 Total 1			\bigcirc		\smile		0		
Delay USA Retransmission Optional.Default:5(s) Interval Ignore MTU Check Add Port List Up to 16 entries can be added. Interval Interface Area Priority Network Type Packets Dead Interval Delay Colored Color			Configure the in:	stance.	Configure the ir	nterface. Op	eration succeed	led.	
Delay USA Retransmission Optional.Default:5(s) Interval Ignore MTU Check Add Port List Up to 16 entries can be added. Interval Interface Area Priority Network Type Packets Dead Interval Delay Colored Color									
LSA Retransmission Optional.Default=S(s) Interval Ignore MTU Check Add Port List Up to 16 entries can be added. Interface Area Priority Network Hello Dead Interval So Ketransmissi Action Gi2/14 12 Broadcast Delete Gi2/14 12 Go to page 1 Total 1					onal.Default:1(s)				
Interval Ignore MTU Check Area Priority Network Hello Dead Interval Search Retransmissi Action Gi2/14 12 Broadcast Delete Go to page 1 Total 1			Dela	У					
Interface Area Priority Network Hello Dead LSA LSA Action Gi2/14 12 Broadcast Delete Delete Color Total 1			LSA Retransmissio	n Opti	onal.Default:5(s)				
Add Port List Up to 16 entries can be added. Interface Area Priority Network Hello Dead LSA LSA Gi2/14 12 Broadcast Delete Image: Image			Interv	al					
Port List Up to 16 entries can be added. Interface Area Priority Network Type Hello Packets Dead Interval LSA Transmission Delay LSA Retransmissi on Interval Action GI2/14 12 Broadcast Delete Image:			Ignore MTU Chec	k 🚺					
Port List Up to 16 entries can be added. Interface Area Priority Network Type Hello Packets Dead Interval LSA Transmission Delay LSA Retransmissi on Interval Action GI2/14 12 Broadcast Delete Image:					Add				
Up to 16 entries can be added. Interface Area Priority Network Type Hello Packets Dead Interval LSA Transmission Delay LSA Retransmissi on Interval Action Gi2/14 12 Broadcast Delete Delete Total 1	PortList				Aud				
Interface Area Priority Network Type Hello Packets Dead Interval LSA Transmission Delay LSA Retransmissi on Interval LSA Retransmissi on Interval Gi2/14 12 Broadcast Delete 1 > 10/page ~ Go to page 1 Total 1									
Interface Area Priority Network Type Hello Packets Dead Interval Transmission Delay Retransmissi on Interval Action Gi2/14 12 Broadcast Delete < 1	Up to 16 entr	ies can be added.							
Interface Area Priority Type Packets Interval Transmission Delay Retransmissi on Interval Gi2/14 12 Broadcast Delete <							LSA	LSA	
< 1 > 10/page > Go to page 1 Total 1	Interface	Area	Priority						Action
	Gi2/14	12	В	roadcast					Delete
Previous Finish	< 1 →	10/page 🗸	Go to page 1						Total 1
Previous Finish									
Previous Finish									
					Previous	Finish			

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 prot ocol 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.

1 Configure the instance. Configure the interface.	③ Operation succeeded.
	Operation succeeded.
Operation succeeded.	
Operation succeeded.	
Disable	
pleting the configuration, you can choose L	

nce list.

8.6.2 Adding an OSPFv3 Interface

Choose Local Device > Routing > OSPFv3 , click More in the Action column, and select V3 Interface .

uíjie Rcycc	Local Device(NBF \vee					E	nglish 🗸 🛆 Remot	e O&M 🔶 Network	Configuration 🕒
Home									
VLAN	OSPFv3								
Monitor ~	Up to 1 entries can be add	ied.							
Ports ~	Router ID Inte	terface	Area	Advertise Default Route	Import External Route	Distance	SPF Calculation	Graceful Restart Helper	Action
L2 Multicast				Delaurt Route	Static Route Redistribution			Helper	More
L3 Interfaces 🗸 🗸	2.2.2.2	Gi23	12(Normal Area)	Disable	Off Direct Route Redistribution			Enable	Neighbor Info
Routing					Off RIP Redistribution : Off				Edit Delete
atic Routing	< 1 > 10/page	e 🗸 Go to page	1						Tot
atic Routing_vб Р Settings									
Png Settings									
SPFv2									
ISPFv3									
ijjie Rcycc	Local Device(NBF >>					E	nglish ~ 🛆 Remot	e O&M 🚷 Network (Configuration 🕞 I
lome	OSPFv3								
/LAN	Up to 1 entries can be add	ded.							
Monitor ~									
Ports ~	Router ID Inte	terface	Area	Advertise Default Route	Import External Route	Distance	SPF Calculation	Graceful Restart Helper	Action
.2 Multicast .3 Interfaces					Static Route Redistribution Off	: V3 Inter	face		More
Routing ^	2.2.2.2	Gi23	12(Normal Area)	Disable	Direct Route Redistribution Off			Enable	Neighbor Info Edit Delete
atic Routing					RIP Redistribution : Off				
atic Routing_v6	< 1 > 10/page	e 🗸 Go to page	1						Tota
P Settings									
Png Settings									
SPFv2									
SPFv3									
					V3 Interface				
ijjie Rcycc	Local Device(NBF \vee					Select			
Home	OSPFv3				* Area				
(1 A NI									
	Up to 1 entries can be add	ded.							
Monitor 🗸		ded.		Advertice	Stub Area				
Monitor × Ports ×		ded. terface	Area	Advertise Default Route	Stub Area	Details			
Monitor × Ports × L2 Multicast	Router ID Int	terface		Default Route	Stub Area			Add	Reset
VLAN Monitor × Ports × L2 Multicast L3 Interfaces × Routing ^	Router ID Int		Area 12(Normal Area)			Details		Add	Reset
Monitor × Ports × L2 Multicast L3 Interfaces ×	Router ID Int	Gi23	12(Normal Area)	Default Route	Port List Up to 64 entries can be	Details		LSA LSA	
Monitor × Ports × L2 Multicast L3 Interfaces × Routing ^	Router ID Int	Gi23	12(Normal Area)	Default Route	Port List Up to 64 entries can be	Details	Hello Dead Packets Interva	LSA LSA Transmi Retra ssion missi	ns Actior
Monitor × Ports × L2 Multicas × L3 Interfaces × I3 Interfaces × L3 Couting × pr Settings	Router ID Int	Gi23	12(Normal Area)	Default Route	Port List Up to 64 entries can be Interfac e Area F	Details added.		LSA LSA Transmi Retra	ns Actior ral
donitor > Aorts > 2 Multicast = 3 Interfaces > atic Routing > atic Routing v =	Router ID Int	Gi23	12(Normal Area)	Default Route	Port List Up to 64 entries can be Interfac	added. Priority Networ k Type		LSA LSA Transmi Retra ssion missi	ns Action

8.6.3 Viewing OSPFv3 Neighbor Information

Choose Local Device > Routing > OSPFv3 , and click Neighbor Info in the Action column.

Rujjie Rcycc	Local Device(NBF \sim							\times
ී Home ඒ VLAN	OSPFv3				Neighbor Info	Status	Interface	
E Monitor	Up to 1 entries can b	e added.				No Data		
Ports	Router ID	Interface	Area	Advertise Default Route	< 1 > 10/page >	Go to page 1		Total 0
L2 Multicast L3 Interfaces			12(Normal Area)					
Routing								
Static Routing Static Routing_v6	< 1 > 10/	/page v Go	to page 1					
RIP Settings								
RIPng Settings								
OSPFv2 OSPFv3								

8.7 Routing Table Info

Choose Local Device > Routing > Route Info, you can view Static Route List details.

Ruíjie Rcycc	Local Device(NBF >			E	nglish 🗸 🛆 Remote O&M 😭 No	twork Configuration 🕞 Log Out
€ Home	Static Routing When a packet arrives, the device cher	cks the destination field and comp	pares it with routing table. If it finds a matcl	h for destination network then it v	will forward that packet from the specif	ed interface.
🖳 Monitor 🛛 👋	Static Route List			Example: 1.1.1	.1 Q + Add	Delete Selected
Ports	Up to 500 static routes can be added.					
L2 Multicast	Dest IP Address	Subnet Mask	Outbound Interface	Next Hop	Reachable	Action
⊕ L3 Interfaces ∨			No Data			
Routing Static Routing	< 1 > 10/page > Go	to page 1				Total 0
Static Routing_v6						
RIP Settings						
RIPng Settings						
OSPFv2						
OSPFv3						
Route Info						e

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.

packets	Snoopin otion: Ena from the he port o	abling e trust	ed por	rt.												HCP re	ques	t pac	kets t	to the	e truste	ed por	rt and DHCP
DHCP	Snoopin	.g: 🌔	0																				
O	ption 82	: (
Select Tru	usted Po	rt:																					
Available	un Un	availa	ıble	_		_				_				1	Ag	gregat	te 🖠	t U	plink	-	Сор	per	Fiber
	F 7	0				_		24															
1 3		9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49	51
		9	11	13	15	17	19			25	27	29	31	33	35	37	39	41	43	45	47	49	51
1 3 2 4	5 7 6 8	9 10	11 11 12	13	15	17	19 20	21	23	25	27	29	31 31 32	33	35	37	39 40	41 41 42	43	45	47	49	51 52

9.1.3 Batch Configuring Network Switches

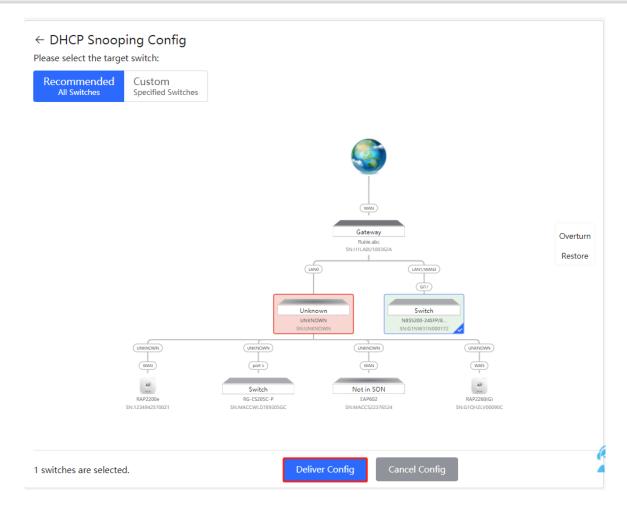
Choose Network > DHCP Snooping .

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.

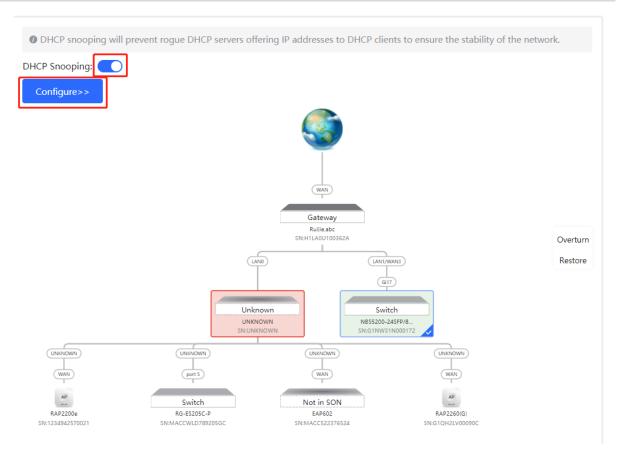
R	Network 🗸 🗸				Navigation Q	English ~	۵	٩	@	Щ	₿
Q											
î											
ጽ											
				o Snoop	ing						
11					ll prevent rogue						
8			DHCP se	ervers offer	ing IP addresses						
-0-			to DHCI	P clients to	ensure the						
			stability	v of the netw	vork.						
>>											

(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.



(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 Snoo ping 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.

Port List				🖉 Batch Edit	🔟 Delete Selecte
	Port	Broadcast	Unknown Multicast	Unknown Unicast	Action
	Gi35	1000pps	1000pps	1000pps	Edit Delete
atch Edit				×	
Broadcas	t: A blank value	ndicates no limit.	kbps Range: 16-1000	000 (1000M)	
Unknown Multicas	t: A blank value	ndicates no limit.	kbps Range: 16-1000	000 (1000M)	
Unknown Unicas	t: A blank value	ndicates no limit.	kbps Range: 16-1000	000 (1000M)	
* Select Por	_	regate 🚹 Uplink	Copper Fiber		
1 3 5 7					
2 4 6 8	3 10 12				
ote: You can click a	nd drag to select or	e or more ports.	Select	All Inverse Deselect	
			Cancel	ОК	

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			+ Ac	Id Delete Selected					
Up to	512 entries can be added.								
	ACL Name	ACL Type	Status	Action					
		No Data							
Add			×						
* 4	ACL Name: Example: Server ACL.								
	ACL Type: • Based on MAC O Based on IPv4 Address O Based on IPv6 Address								
		Cancel	ок						

(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 51	2 entries can be added.			
	ACL Name	ACL Type	Status	Action
	test	Based on MAC	Inactive	Details Edit Delete

Ruíjie Rcycc	Local Device(NBF ~			[test]Settings			×
🖧 Home				ACL Name: test			
∯ VLAN	ACL List ACL Binding			ACL: O Block O Allow	v		
및 Monitor 🌱	ACL			EtherType Value : 🔽 All			
Ports ~	Up to 512 entries can b	se added.		Src MAC: 🗾 All			
 L2 Multicast 		ACL Name	ACL Type	Dest MAC: 🗾 All			
L3 Interfaces ~		test	Based on MAC				
Routing ~	< 1 > 10/p	age 🗸 Go to page 1		Save	Reset		
Security ^				Existing ACL: (You can click and drag the ACL m	umber to swap the ACL)		
DHCP Snooping				No. Rule		Control Type	Action
Storm Control					No Data Available		
ACL							

Table 9-1	Description of ACL Rule Configuration Parameters
-----------	--

Parameter	Description
	Configuring ACL Rules Action
ACL	Block: If packets match this rule, the packets are denied.
	Allow: If packets match this rule, the packets are permitted.
	Match IP protocol number The value ranges from 0 to 255. Check All to
IP Protocol Number	match all IP protocols. Applicable to A CL based on "IPv4 address control" and "IPv6 address control".
	Match the source IP address of the packet. Check All to match all source IP
Src IP Address	addresses. Applicable to "IPv4 address-based control" and "IPv6 address- based control" A CL.
	Match the destination IP address of the packet. Check All to match all
Dest IP Address	destination IP addresses applies to ACLs based on "IPv4 address control" and
	"IPv6 address control " .
	Match Ethernet protocol type. The value range is 0x600~0xFFFF. Check All to
EtherType Value	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" .

1 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 .

1 Note

Currently, ACLs can be applied only in the inbound direction of ports, that is, to filter incoming packets.

ACL List	ACL Binding			
	Binding levice only filters incomi	ing packets.		
ACL Bin	ding		+ Batch Add	The Unbind Selected
	Port	MAC-based ACL	IP-based ACL	Action
	Gi1			Edit Unbind
	Gi2			Edit Unbind
	GI3			Edit Unbind
	Gi4			Edit Unbind
Add				×
	MAC-based ACL:	No Data V		
	IPV4-based ACL:	No Data v		
	IPV6-based ACL:	No Data ~		
Available	* Select Port:	egate 📭 Uplink 💼 Copper 🛄 Fiber		
	5 7 9 11 6 8 10 12			
Note: You can o	lick and drag to select one	e or more ports.	Select All Inverse De	select
			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 Bir	nding		+ Batch Add	Dubind Selected		
	Port	MAC-based ACL	IP-based ACL	Action		
	Gi1	test		Edit Unbind		
	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**.

<i>i</i> 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.

ist will be filtered	IAC Binding check	is both the source IP addresses and MAC address prior to ACL, but it has the same privilege with IP		
IP-MAC Binding	Search by	IP Address 🗸	Q Search	Add Delete Selected
Up to 500 entries ca	n be added.			
	IP	MAC	Port	Action
19	2.168.1.1	00:11:22:33:44:55	Gi29	Edit Delete
Add	IPv4 Addı > MAC Address	192.168.1.1 00:11:22:33:44:55	×	
Available Unav	* Select Port: vailable Aggree 9 11	egate 💼 Uplink 💼 Copper 🔛 Fiber		
2 4 6 8 Note: You can click and c	10 12	e or more ports.	Select All Inverse Deselect	
			Cancel OK	

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 <		Q Search	🖉 Add	Delete Selected
Search by IPv6 Address				
Search by IPv4 Address Search by MAC	Port		Action	
Search by Port				

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 Ac	idress v	Q Search	
Up to 500	entries can be added.			
~	IP	MAC	Port	Action
~	192.168.1.1	00:11:22:33:44:55	Gi29	Edit 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 <u>7.1</u> 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					
	<i>i</i> Binding List Description: The entries come from dynamic learning of DHCP Snooping.						
Binding List	t		Search by IP Address 🛛 🗸		QS	earch C Refresh	
Up to 1900 e	ntries can be added.						
IP	n	/IAC	Port	VLAN ID	Status	Rule	
			No E	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		Q Search
Search by IP Address		
Search by MAC		
Search by VLAN	VLAN ID	Status
Search by Port	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.

A 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	Enabled ~]
Rule	IP ^]
	IP	
	IP+MAC	ncel OK

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 ${\bf Edit}$, enter the Excluded VLAN ID and the desired port, and click ${\bf OK}$.

🛕 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		
	on: Packets within this		the port without checking or filtering. e Guard is enabled on a port.	
VLAN List				+ Add 🗇 Delete Selected
Up to <mark>64</mark> entr	ries can be added.			
	VLAN II	D	Port	Action
			No Data	

Add			×
* VLAN ID			
* Select Port:			
Available 💼 Una	vailable Aggregat	te 💼 Uplink 💼 Copper	Fiber
1 3 5 7	9 11 13 15 17 19 21 2	23 25 27 29 31 33	35 37
2 4 6 8	10 12 14 16 18 20 22 2	24 26 28 30 32 34	36 38
Note: You can click and	drag to select one or more ports.	Select All Inverse	Deselect
		Cancel	к

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.

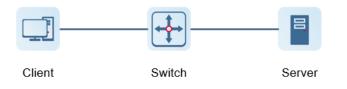
IEEE 802 LAN, as long as users can connect to network devices, they can directly access network resources without authentication and authorization. This uncontrolled behavior will bring security risks to the network. The IEEE 802.1x protocol was proposed to solve the security problem of 802 LAN.

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.
 - o Add username and password for client login.
 - Close the firewall, otherwise the authentication message may be intercepted, resulting in authentication failure.
 - o 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.

Auth Config Port RADI	US Server Management Wired Use	er List			
RADIUS Server Manage	ment				Add Server Group
Up to 20 entries can be added.					
Server Group Name	Server IP	Auth Port	Accounting Port	Shared Password	Action
			No Data		

Add			×
* Server Group Name			
* Server IP	👜 Server 1		
* Server Name			
* Auth Port	1812		
* Accounting Port	1813	0	
* Shared Password			
* Match Order		0	
	↔ Add Server		
		Cancel	ОК

parameter	Reference without translation	illustrate	
Server group name		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.	
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.	

(2) Set server global configuration and click <Save> .

Server global configuration	
* Packet Retransmission Interval	3 5
* Packet Retransmission Count	3 time
Server Detection	
MAC Address Format	xxxxxxxxxx ~) Ø
	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	 Configure the MAC address format of RADIUS attribute No. 31 (Calling- Stationg -ID). The following formats are supported: 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 Po	ort	RADIUS Server Management	Wired U	Jser List		
Global Config	9					
Global 8	802.1x					
Authentic	ation					
Auth S	Server	Add a server to be authenticated	ł.	🖉 Edit		
		Advanced Settings				
		Configure				
Select a server gr	oup.					
Global Config						
		Select	~ 2	Edit		
	Global Config Global & Authentic Auth S Gelect a server gr Global Config Global 80 Authentica	Global Config Global 802.1x Authentication Auth Server	Global Config Global 802.1x Authentication Auth Server Add a server to be authenticated Advanced Settings Configure Global Config Global 802.1x Authentication	Global Config Global 802.1x Authentication Auth Server Add a server to be authenticated. Advanced Settings Configure Global Config Global 802.1x Authentication	Global Config Global 802.1x Authentication Auth Server Add a server to be authenticated. Ledit Auth Server Add a server to be authenticated. Ledit Configure Global Config Global 802.1x Authentication	Global Config Global 802.1x Authentication Auth Server Add a server to be authenticated. Advanced Settings Configure Select a server group. Global Config Global 802.1x Authentication

(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	2	
Retransmission Count		
* Quiet Period	60	s
Client Packet * Timeout Duration	30	S
Client Packet * Timeout Duration	30	S
* EAP-Request Packet	30	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	Define the number of times the EAP request message will be
Retransmission Count	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	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
Timeout Duration	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 Manageme	nt 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 Aut	hentication			
Au	uth Method	disable \vee		
	Auth Mode	multi-auth \vee		
	Guest Vlan			
* User Cour	nt Limit per	1000		
	Port			

Cancel	ОК

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	disable : Turn off the authentication method , which has the same effect as turning off the 802.1x authentication switch force- auth : Mandatory authentication , the client can directly access the Internet without a password force- unauth : force no authentication, the client cannot authenticate and cannot access the Internet auto : automatic authentication, the device needs to be authenticated, and can access the Internet after passing the authentication It is recommended to select the auto authentication method .
Auth Mode	authentication mode	multi- auth : Supports multiple devices using the same port for authentication, but each device needs to be authenticated independently 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 single-host : Each port only allows one device to be authenticated, and can access the Internet after successful authentication

parameter	reference - do not translate	illustrate
Guest Vlan	Guest VLAN	When enabled, devices that fail authentication will be dynamically assigned to the specified Guest VLAN 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
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.

Auth Config		S Server Management	Vired User List					
Wired U	Jser List					Q Search by mac	Refresh	↓ Batch Logout
	Username	Status	Interface	MAC Address	Online Time	Online Duration	Access Name	Action
				No Data	1			
< 1	> 10/page >	Go to page 1						Total 0

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 \mathbf{Add} , select the desired port and enter the gateway IP, click \mathbf{OK} .

Note

Generally, the anti-ARP spoofing function is enabled on the downlink ports of the device.

1	Anti-ARP Spoofing Description: Anti-ARP Spoofing prevents hosts fr Note: Anti-ARP Spoofing is generally configured	rom spoofing the source IP address of the ARP pack on a downlink port.	ets to be the IP address of the gateway.
Ant	i-ARP Spoofing		🖉 Add 🗇 Delete Selected
Up	to 256 entries can be added.		
	IP	Port	Action
		No Data	

Add				×
* Ib	192.168.1.1			
* Select Port:	available	Aggregate	t Uplink	opper Fiber
1 3 5 7	9 11 13 15	17 19 21 23		33 35 37
2 4 6 8	10 12 14 16	18 20 22 24	26 28 30 32	2 34 36 38
Note: You can click and	drag to select one o	or more ports.	Select All In	verse Deselect
			Cancel	OK

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.

1	Anti-ARP Spoofing Description: Anti-ARP Spoofing prevents hosts from s Note: Anti-ARP Spoofing is generally configured on a		packets to be the IP address of the gateway.
An	ti-ARP Spoofing		2 Add
Up	to 256 entries can be added.		
~	IP	Port	Action
	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 S	STP N	lanagement						
i Note: Enabli	ing ST	P or changing the STP mode	will initiate	a new sessio	n. Please do not refresh ti	he page.		
S	TP:							
* Prior	ity:	32768	~		* Hello Time:	2		seconds
* Max A	ge:	20		seconds	* Forward Delay:	15		seconds
* Recovery Tir	me:	30		seconds	STP Mode:	RSTP	~	
		0						
		Save						

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: Er	nabling STP or changing the STP mode will initiate a new session. Please do not refresh the page.



(2) Configure the STP global parameters, and click Save .

STP Settings STF	Management			
i Note: Enabling	STP or changing the STP mode will initiate	a new session. Please do not refresh t	the page.	
STP				
* Priority	: 32768 ~	* Hello Time:	2	seconds
* Max Age	20	seconds * Forward Delay:	15	seconds
* Recovery Time	30	seconds STP Mode:	RSTP ~	
	0			
	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 Settings	P Settings STP Management								
 STP Port Settings Tip: It is recommended to enable the port connected to a PC with Port Fast. 									
Port List						C	Refresh	🖉 Batch Edit	
Port	Role	Status	Priority		Status	BPDU	Port Fast	Action	
TOR	Roie	Juius	monty	Config Status	Actual Status	Guard	Foretase	Action	
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:	Auto ~		
* Priority:	128 ~		
		Canad	OK
		Cancel	ОК

Table 10-2 Description of STP Configuration Parameters of Ports

Parameter	Description	Default Value
Role	 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
	 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 	
Status	 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. 	NA
	 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.	
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 BPDU.s. 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

1 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

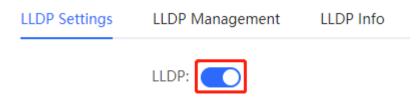
10.2.1 Overview

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 .

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.



(2) Configure the global LLDP parameters and click Save .

LLDP Settings	LLDP M	lanagement	LLDP Info				
	LLDP:						
* Hold M	lultiplier:	4			* Reinitialization Delay:	2	seconds
* Transmit	Interval:	30		seconds	* Forward Delay:	2	seconds
* Fas	st Count:	3					
		Save					

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 × 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 × 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	LDP Management	LLDP Info			
Port List					🖉 Batch Edit
Port	S	end 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 💼 Unavai	ilable		1 Uplink	с 💼 Сорр	er 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	1 24 26 28	30 32	3 4 3 6 3 8
Note: You can click and dr	ag to select one c	or more ports.	Sele	ct All Inver	se Deselect
			Cancel		ОК

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.

Ruíjie Rcyc	C Local Device(NBF >				English	ି 🗠 🛆 Remote ଠିଷ୍ଠM 🛛 💩 Ne	twork Configuration 🛛 🕞 Log
음 Home	LLDP Settings LLDP Man	agement LLDP Info					
문 VLAN							
∑ Monitor	Device Info						
Ports	Device ID Type: Mac A Hostname:				vice ID: ription: Reyee Switch(RG-NBF	5200M-8FS16GT4XS) By Ruijie	Networks
L2 Multicast	Supported Feature: Bridge MGMT IP: 192.16			Enabled F	eature: Bridge,Router,Repeate	ſ	
L3 Interfaces	~						
Routing	Neighbor Info						
Security	~ Port	Device ID Type	Device ID	Port ID Type	Port ID	Neighbor System	Time To Live(s)
Advanced	~	Locally assigned	R11309	MAC address	8C:EC:4B:8B:39:27		3594
STP		Locally assigned	DESKTOP-0V9K2C0	MAC address	70:85:E8:76:F6:06		3595
LLDP	Gi1	MAC address	30:0D:9E:3E:B5:D0	MAC address	30:0D:9E:3E:B5:D0		3598
		MAC address	70:B5:E8:76:F5:DF	MAC address	70:B5:E8:76:F5:DF		3578
RLDP							

					[Gi1]Neighbor Deta	ils		
a ⁶ a Home								
	LLDP Settings LLDP M	anagement LLDP Info				Locally assigned	Device ID:	
S VLAN	10					MAC address	Port ID:	
	Device Info				Hostname:		PVID:	
E Monitor					VLAN ID:		Time To Live:	3594
	Device ID Type: Mac	: Address			MGMT IP:			
Ports	Hostname:				Description:			
	Supported Feature: Brid	lge.Router,Repeater		9	Supported Feature:	CT	Enabled Feature:	C
C L2 Multicast	MGMT IP: 192	.168.88.53						
L3 Interfaces								
	Neighbor Info				Device ID Type:	Locally assigned	Device ID:	DESKTOP-0V9K2C0
Routing	Neighbor Into					MAC address		-
- or mouning				_	Hostname:		PVID:	
Security	Port	Device ID Type	Device ID	Port ID Typ	VLAN ID:		Time To Live:	
Security					MGMT IP:	**		
Advanced		Locally assigned		MAC addres	Description:			
- Nuvanceu					Supported Feature:	-	Enabled Feature:	
STP		Locally assigned		MAC addres				
SIP								
		MAC address		MAC addres				
LLDP								
		MAC address		MAC addres	Device ID Type:		Device ID:	
RLDP						MAC address		
		MAC address		MAC addres	Hostname:		PVID:	
Local DNS					VLAN ID:		Time To Live:	3598
		Locally assigned		MAC addres	MGMT IP:			
Voice VLAN					Description:			
		MAC address		MAC addres	Supported Feature:	**	Enabled Feature:	**

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.

RLDP Settings	RLDP Management	RLDP Info	
	RLDP:		

(2) Configure RLDP global parameters and click Save .

RLDP Settings	RLDP Manageme	nt RLDP Inf	o	
	RLDP:			
* Hello In	terval: 3		seconds	Errdisable Recovery:
	Save	e		

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.

A 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
F	Port	Loop Detection	Action	Action
(Gi1	Disable		Edit
(Gi2	Disable		Edit
(GI3	Disable		Edit

Port:Gi1				×
Loop Detection:				
Action:	Warning]		
	Warning			
	Block	el	ОК	
	Shutdown			

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.

*	RLDP Settings RLDP Managemen	nt RLDP Info				
금문 Port List 딸						
<u>چ</u>	Port	Status	Action	Neighbor Port		
0	Gi1	ОК				
	Gi2	ОК				
	Gi3	ОК				
\bigcirc	Gi4	ОК				
e	Gi5	ОК				
Q	Gi6	ОК				
-0-	Gi7	ОК				

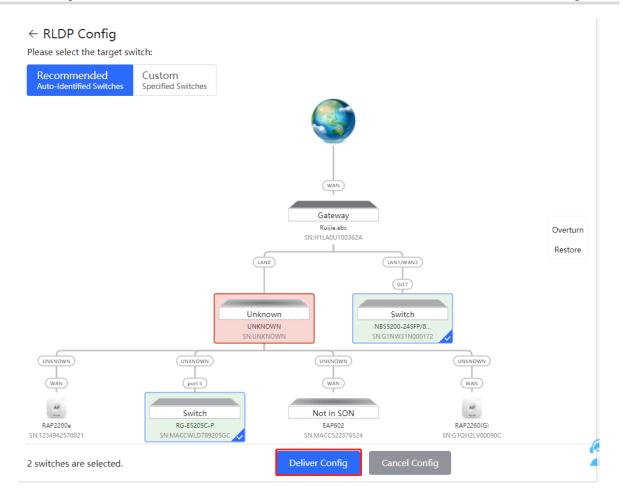
10.3.3 Batch Configuring Network Switches

Choose Network > RLDP .

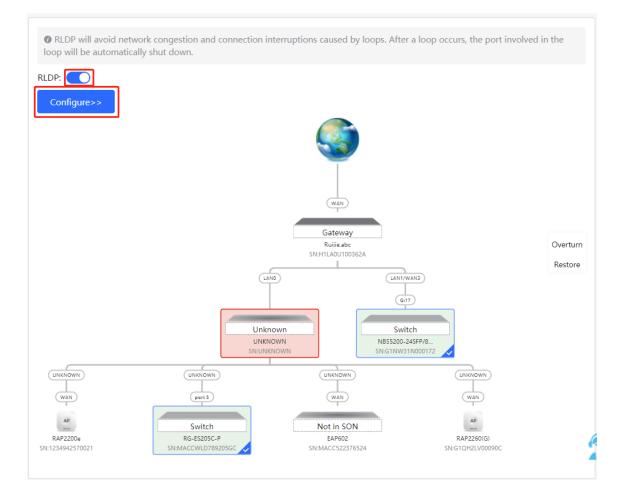
(1) Click **Enable** to access the **RLDP Config** page.

R	Network 🗸	Navigation Q English	~ ¢	援	۵	@	بو	₿
Q								
î								
ጽ								
(1) 								
11	F	LDP						
8		DP will avoid network congestion						
-0-		nd connection interruptions nused by loops. After a loop						
		ccurs, the port involved in the						
	le	op will be automatically shut						
	d	Enable						
>>								

(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.



(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.

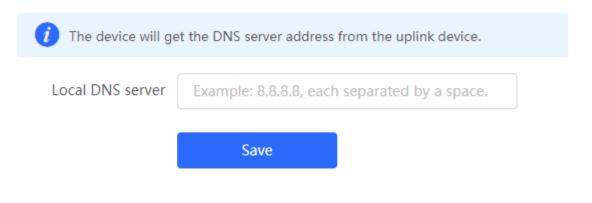


10.4 Configuring the Local DNS

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.



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 $\ensuremath{\textbf{Save}}$.

Global Settings	OUI	Port Settings		
i Global	Settings			
	Voice VLAN			
	* VLAN	2		Range: 2-4094
	* Max Age	1440		minute Range: 1-43200
	CoS Priority	6	~	
		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

$\label{eq:choose} Choose \ \textbf{Local Device} > \textbf{Advanced} > \textbf{Voice VLAN} > \textbf{OUI} \ .$

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 \mathbf{Add} . In the displayed dialog box, enter an MAC address and OUI, and click \mathbf{OK} .

Global Settings	OUI	Port Settings			
<i>i</i> OUI List The enable	d globally po	rt will automatically add the corre	esponding OUI when receiving an LLD	P packet that is identified as teleph	none.
OUI List				+ Add	Delete Selected
Up to 32 entr	es can be ado	ded.			
M	AC Address	OUI Mask	Description	Туре	Action

No Data

Add			×
* MAC Address	00:11:22:33:44:55		
OUI Mask	Select		
Description			
		Cancel	OK

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. 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			

Edit			×
Enable			
Voice VLAN Mode	Auto Mode	~ ?	
Security Mode			
		Cancel	ОК

Table 10-6 Description of the Voice VLAN Configuration Parameters on a Port

Parameter	arameter Description		
Voice VLAN Mode	 Based on different ways the Voice VLAN function is enabled on the port, the Voice VLAN Mode can be Auto Mode or Manual Mode: 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	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. 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.	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.

uijie Rcycc				Eng	jlish ∽ Remote O&M	A Network Configuration	
VLAN							
Monitor ~	 Info Center 	Port Info					
Ports ~		Updated on2024-05-31 18:01:23				Panel View	
2 Multicast	Port Info VLAN Info					Fallel View	Ň
3 Interfaces	Routing Info		17 19 21 23				
outing	DHCP Clients		18 20 22 24 25 26 2	27 28			
curity ~	ARP List						
	MAC Address	Port Gi1 Status Connected	Flow	↓ 1.51T ↑ 3.16T	Interface Mode	Trunk Port	
dvanced ~	DHCP Snooping	Negotiation Rate 1000M	Total Packets	1806299871/6398519981	Native Id	1	
iagnostics	IP-MAC Binding	Actual Rate Flow Control(Config Disable	359kbps CRC/FCS Error Packets	64/	Allowed VLAN	1-4094 Effective VLAN 1,888,2001,3011-3013	
o Center	IP SOURCE GUARD	Status)	Corrupted/Oversized	d/1393949662	DHCP Address Pool		
	CPP	Flow Control(Actual Disable Status)	Packets Conflicts				
twork Tools		Attribute OLT port					
It Collection							
ble Diagnostics		VLAN Info (SVI&Routed Port) DM	IS: C Refresh				
stem Logs		VLAN1 VLAN888 VLAN2001	VLAN3011 VLAN3012	VLAN3013 Routed Port G	i23		
irms							
«Collapse		Interface	IP Address	DHCP Address	Pool	Remarks	

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.

Info Center	Port Info						
Port Info	Updated on2022-05-20	12:18:51 😋 Refres	h				Panel View
VLAN Info	1 3 5 7	9 11 13 15	17 19 21 23 25	27 29 31 33 3	53	Role	Status
Routing Info					н.	Copper	1G/2.5G/10
DHCP Clients	2 4 6 8	10 12 14 16	18 20 22 24 26	28 30 32 34 3	63	Fiber	🛑 10M/100M
ARP List	Port	Gi12				1 Uplink	Exception
MAC	Status Negotiation Rate	Connected 1000M	Flow	↓ 0.00 ↑ 535.26M	Inte VLA	PoE	Disconnecte
DHCP Snooping	Actual Rate	↓kbps	Total Packets	/6142498	DHC	PoE Error	Disable
P-MAC Binding	Flow Control(Config	↑ 27kbps Disable	CRC/FCS Error Packets	/		Aggregate	
P SOURCE GUARD	Status) Flow Control(Actual	Disable	Corrupted/Oversized Packets	/			
CPP	Status) Attribute	Copper	Conflicts				

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 <u>0</u>.
- To configure SVI ports and routed ports, see <u>6.1</u>.

info Center	VLAN Info	(SVI&Routed Port)	DNS: 😋 Ref	resh			
Port Info	< VLAN1	Routed Port Gi1	Routed Port Gi2	Routed Port Gi3	Routed Port Gi4	Routed Port Gi5	Route
VLAN Info	In	terface	IP	DHC	P Address Pool	Remark	
Routing Info	Gi1-8,Gi	10-48,Te49-52	172.30.102.133			VLAN0001	
DHCP Clients							
ARP List	1 3	5 7 9 11 13	3 15 17 19 21 2	3 25 27 29 3	1 33 35 37 39	41 43 45 47	49 51
MAC							
DHCP Snooping	2 4	6 8 10 12 14	16 18 20 22 2	4 26 28 30 3	2 34 36 38 40	42 44 46 48	50 52
IP-MAC Binding							

11.1.3 Routing Info

A 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.

1 Note	
To set up static route	es, see <u>6.3</u> .
 Info Center 	Routing Info

Port Info				
VLAN Info	Interface	IP	Subnet Mask	Next Hop
Routing Info	Gi9	2.1.1.0	255.255.255.0	3.1.1.1

11.1.4 DHCP Clients

A 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.

 Info Center 	Gi9	2.1.1.0		255.255.255.0	3.1.1.1
Port Info	DHCP Clients				
VLAN Info	Tip: Up to 1000 entries can be	added.		Search by Hostname/IP/MAC	Q Refresh
Routing Info	Hostname	IP	MAC	Lease Time(Min)	Status
DHCP Clients ARP List			No Data		
MAC					

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.

1 Note

To bind dynamic ARP or manually configure static ARP, see 6.4.

Info Center	ARP List				
ort Info	Tips: Up to 1000 entries can be added.			Search by I	P Address/MAC A Q Refresh
LAN Info	Interface	IP Address	MAC Address	Туре	Reachable
RP List	VLAN0001	10.52.48.179	00:d0:f8:15:08:bb	Dynamic	Yes
HCP Snooping	VLAN0001	10.52.49.124	00:d0:f9:15:08:61	Dynamic	Yes
-MAC Binding	VLAN0001	10.52.48.138	00:e0:4c:00:21:2d	Dynamic	Yes
SOURCE GUARD	VLAN0001	10.52.48.43	00:d0:88:88:08:60	Dynamic	Yes
ЭE	VLAN0001	10.52.48.182	00:d0:f8:12:08:5a	Dynamic	Yes
PP	VLAN0001	10.52.48.73	30:0d:9e:c4:1a: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

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.

1 Note

To configure and manage the MAC address, see 3.3.

info Center	МАС			
Port Info	Tip: Up to 16K entries can be added.	Search by MAC	×]	Q C Refresh
VLAN Info	Interface	MAC	Туре	VLAN ID
	Gi24	70:B5:E8:5F:FD:29	Dynamic	1
Routing Info	Gi24	50:9A:4C:42:C9:50	Dynamic	1
DHCP Clients	Gi24	30:0D:9E:6F:C2:3C		1
ARP List			Dynamic	I
MAC	Gi24	30:0D:9E:6F:C2:3D	Dynamic	1
DHCP Snooping	Gi24	C0:B8:E6:E9:78:07	Dynamic	1
	Gi24	30:B4:9E:8F:85:E5	Dynamic	1
IP-MAC Binding	Gi24	58:69:6C:CE:72:B2	Dynamic	1
IP SOURCE GUARD	Gi24	70:B5:E8:78:B7:8D	Dynamic	1
СРР				

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.

1 Note

To modify DHCP Snooping related configuration, see <u>7.1</u>.

info Center	DHCP Snooping				
Port Info	DHCP Snooping: Enabled	Option82: D	isabled	Trusted Port: Gi24 ORefr	esh
POILINIO	DHCP Snooping Binding Entri	es from the Trusted Po	rt		
VLAN Info	Interface	IP	MAC	VLAN ID	Lease Time(Min)
Routing Info	Gi15	172.30.102.17	08:00:27:62:F0:53	1	240
DHCP Clients					
ARP List	IP-MAC Binding				
MAC	[·· ·····]				
	Tip: Up to 500 entries can be	e added. Searcl	n by IP Address 🛛 🗸		Q C Refresh
DHCP Snooping					
IP-MAC Binding	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.

1 Note

To add or modify the IP-MAC binding, see 7.5.

info Center	IP-MAC Binding]				
Port Info	Tip: Up to 500 entries of	an be added.	Search by IP Address	~	Q	C Refresh
VLAN Info	Por	t	1	Р	M	AC
Routing Info	Gi2	9	192.1	68.1.1	00:11:22:	33:44:55
DHCP Clients						
ARP List	IP SOURCE GUARD					
MAC	Tip: Up to 1900 entries	can be added.	Search by IP Address	~	Q	C Refresh
DHCP Snooping	Interface	Rule	IP	MAC	VLAN ID	Status
IP-MAC Binding	Gi15	IP	172.30.102.17	08:00:27:62:F0:53	1	Inactive
IP SOURCE GUARD						

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 $\underline{7.6}$.

Port Info	IP SOURCE GUARE					
VLAN Info	IP SOURCE GUARL	,				
Routing Info	Tip: Up to 1900 entries	s can be added.	Search by IP Address	~	Q	C Refresh
DHCP Clients	Interface	Rule	IP	MAC	VLAN ID	Status
ARP List	Gi15	IP	172.30.102.17	08:00:27:62:F0:53	1	Inactive
MAC						
DHCP Snooping	СРР					
IP-MAC Binding	Total CPU bandwidth: 2	000pps 😋 Refre	esh			
IP SOURCE GUARD	EtherType Val	ue	Rate	Current Rate	Т	otal messages

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.

<i>i</i> Info Center	СРР			
Center	Total CPU bandwidth: 2000pps	G Refresh		
Port Info	EtherType Value	Rate	Current Rate	Total messages
VLAN Info	bpdu	60pps	0pps	0
Routing Info	lldp	50pps	Opps	5328
DHCP Clients	rldp	50pps	Opps	0
ARP List	lacp	600pps	0pps	0
MAC	arp	400pps	2pps	426731
DHCP Snooping	dhcp	600pps	5pps	622
IP-MAC Binding	icmp	600pps	Opps	3708
IP SOURCE GUARD	macc	600pps	11pps	190569
• СРР	mqtt	600pps	Opps	0
	http/https	1600pps	4pps	105864
	Total 26 10/page 🗸 🤇 1	2 3 → Go to page	1	

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.

i Network Tools				
Tool	Ping	 Traceroute 	O DNS	Lookup
Туре	O IPv4	O IPv6		
* IP Address/Domain	www.go	oogle.com		
* Ping Count	4			
* Packet Size	64			Bytes
		Start	Sto	p
Result				
				li li

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>i</i> Network Tools	;			
Tool	🔿 Ping 💿 Tr	aceroute	O DNS Lookup	
Туре	● IPv4 ○ IPv	vб		
P Address/Domain	www.google.com	m		
* Max TTL	20			
	Start		Stop	
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.

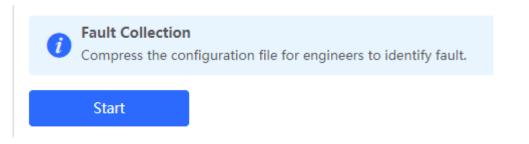
Select **DNS Lookup** as the diagnosis mode, enter a destination IP address or URL, and DNS server address , and click **Start** .

O Ping O Traceroute	DNS Lookup
www.google.com	
8.8.8.8	
Start	Stop
	www.google.com 8.8.8.8

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.



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 Cable Length (cm) Re	ort Panel				
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 te: You can click and drag to select one or more ports. Select All Inverse Deselect Result Port Cable Length (cm)	Available 💼 Un	available		t Uplink Copper	Fiber
te: You can click and drag to select one or more ports. Select All Inverse Deselect Start Port Cable Length (cm) Re	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 5	1
esult Port Cable Length (cm) Re	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	2
Result Port Cable Length (cm) Re	te: You can click and	drag to select one or more p		Select All Inverse De	select
<i>u</i> · · ·			Start		
	esult				
Gi15 700		Port	Cable	e Length (cm)	Resu
		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.

<i>System Logs</i> View system logs.						
Log List					Search	Q
Time	Туре	Module		Details	local.info	
May 18 18:52:37	kern.crit	kernel	%Port-2: GigabitEthernet12 link up		syslog	
May 18 18:52:37	local.info	syslog	%L3-6: Manage VLAN 1 change to UP		kern.crit	
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			

11.6 Alerts

Choose Local Device > Diagnostics > Alarms .

1 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.

A 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.



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

Table 11-1 Alert Types and Product Support

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.

<i>i</i> Configure and vi	ew system time (The device ha	as no RTC mo	odule. The time settings will not be saved upon reboot).	?
Current Time	2022-05-20 14:32:29 Ed	it		
* Time Zone	(GMT+8:00)Asia/Shangha	ai ~		
* NTP Server	0.cn.pool.ntp.org	Add		
	1.cn.pool.ntp.org	Delete		
	2.cn.pool.ntp.org	Delete		
	3.cn.pool.ntp.org	Delete		
	0.asia.pool.ntp.org	Delete		
	3.asia.pool.ntp.org	Delete		
	0.pool.ntp.org	Delete		
	1.pool.ntp.org	Delete		
	rdate.darkorb.net	Delete		
	Save			

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	Current Time
		Cancel

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.

A Caution

When self-organizing network discovery is enabled, the login password of all devices in the network will be changed synchronously.

Ruíjie Rcycc	Networkwide Ma \vee	
Q Navigation	<i>i</i> Change the login pa	assword. Please log in again with the new password later.
Overview		
	* Old Management	Enter old management password of the project.
움 Network 🌱	Password	
Devices		
	* New Management	The management passwords of the network-wid
8 Clients Management	Password	There are four requirements for setting the password:
System ^		• The password must contain 8 to 31 characters.
		\cdot The password must contain uppercase and
System Time		lowercase letters, numbers and three types of special
Login Password		characters.
Backup		· The password cannot contain admin.
		 The password cannot contain question marks,
SNMP		spaces, and Chinese characters.
Reboot	* Confirm Password	Enter new management password again.
Cloud Service		
	Password Hint	P@sw0rd
		Save

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.

Global Config		_
SNMP Service		× Are you sure you want to Enable SNMP?SNMP v1/v2c is considered unsafe. Therefore, only SNMP
* SNMP Version	🗆 v1 🗹 v2c 🗹 v3 😽	v3 is enabled by default. To proceed, please add SNMP v3 users by selecting View/Group/Community/User Access Control
* Local Port	161	before using the SNMP service.
* Device Location	Company	
* Contact Info	Ruijie@Ruijie.com	
	Save	

When first opened, the system prompts to enable SNMPv3 by default. Click < OK >.

(2) Set global configuration parameters for SNMP service.

Global Config V	iew/Group/Community/Client Access Control	Trap Settings
SNMP Servic	e 🚺	
* SNMP Versio	n 🗌 v1 🔽 v2c 🔽 v3	
* Local Po	rt 161	
* Device Locatio	n Company	
* Contact Inf	o Ruijie@Ruijie.com	
	Save	

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.

SNMP v3 Device Identifier List				
View List			+ Add Delete Selected	
Up to 20 entries are allowed.				
	View Name	Action		
	all			
	none			
Total 2 10/page V 1	> Go to page 1			

(2) Configure the basic information of the view.

Add			×
* View Name			
OID	Example: .1.3		
	Add Included Rule	Add Excluded Rule	
Rule/OID List			Delete Selected
Up to 100 entries an	e allowed.		
Rul	e	OID	Action
	No [Data	
Total 0 10/page \vee	< 1 > G	o to page 1	
			Cancel

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 Add Included Rule Add Excluded Rule	 Divided into inclusion rules and exclusion rules Include rules allow access only to OIDs within the OID range . Click <add inclusion="" rule=""> to set up this type of view.</add> Exclusion rules allow access to all OIDs except the OID range . Click <add exclusion="" rule=""> to set up this type of view.</add> 		

🛕 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 Se	ervice	
* SNMP Ve	ersion 🗌 v1 🔽 v2c 🔽 v3	
* Local	I Port 161	
* Device Loc	Company	
* Contac	t Info Ruijie@Ruijie.com	
	Save	

1 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>.

SNMP v1/v	2c Community I	Name List				+ Add 🗈 Delete Selected
Up to 20 entr	ies are allowed.					
	Community	Name	Access Mode		MIB View	Action
	hello_121	21	Read & Write		all	Edit Delete
	34234234	4A.	Read-Only		all	Edit Delete
) Create v Add	1/v2c use	rs.			×	
* Comm	unity Name					
* A	ccess Mode	Read-Only	\sim			
	* MIB View	all	~	Add View +		
				Cancel	ОК	

Table 4-1v1 / 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 Servi	ce 💽	
* SNMP Versio	on 🗌 v1 🗹 v2c 🗹 v3	
* Local Po	ort 161	
* Device Location	Company	
* Contact In	fo Ruijie@Ruijie.com	
	Save	

(2) Set v3 groups of related parameters.

Global Config	View/Group/Commun	ity/Client Access Control Trap Setting	gs			
SNMP v3 G	Group List				4	• Add h
Up to 20 ent	tries are allowed.					
	Group Name	Security Level	Read-Only View	Read & Write View	Notification View	Action
	default_group	Auth & Security	all	none	none	Edit Delete
Total 1 10/pa	ige 🗸 < 1 🗦	Go to page 1				

Add		×
* Group Name		
* Security Level	Allowlist & Security \lor	
* Read-Only View	all V	Add View +
* Read & Write View	all \vee	Add View +
* Notification View	none 🗸	Add View +
		Cancel

Table 4-1V3 group configuration parameters

parameter	illustrate
Group Name 1-32 characters, a single Chinese accounted for three characters Cannot contain Chinese, full-width characters, question marks and single	
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 vie 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)

A 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 Vie	ew/Group/Community/Client Access Control	Trap Settings
SNMP Service		ß
* SNMP Version	🗌 v1 🔽 v2c 🗹 v3	
* Local Port	161	
* Device Location	Company	
* Contact Info	Ruijie@Ruijie.com	
	Save	

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 .

SNMP v3 Client List							
						+ Add	🗊 Delete Se
Up to 50 entries are allowed	L						
Username	Group Name	Security Level	Auth Protocol	Auth Password	Encryption Protocol	Encrypted Password	Action
			No Data				
Total 0 10/page V	1 > Go to page 1						
Set v3 user rel:	ated narameters						
	ated parameters.						
Set v3 user rela	ated parameters.				×		
Add					×		
	ated parameters.			Ç.	×		
Add * Username	123sdf!@			ß	×		
Add	123sdf!@				×		
Add * Username	123sdf!@			L ₂	×		
Add * Username * Group Name * Security Level	123sdf!@ default_group ~ Auth & Security ~		uugd	Ş	×		
Add * Username * Group Name	123sdf!@ default_group ~		word	ß	×		

Table 12-3 v3 user configuration parameters

parameter	illustrate
Username	username

Cancel

parameter	illustrate			
	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			
Group Name	user's group			
Security Level	User security level (authentication and encryption, authentication without encryption, no authentication and encryption)			
	Authentication protocols include:			
	MD5/SHA/SHA224/SHA256/SHA384/SHA512			
	Authentication password: 8~31 characters in length, cannot contain			
Auth Protocol , Auth Password	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.			
	Note: This parameter needs to be set when the "Security Level" is			
	"authentication and encryption" or "authentication without encryption".			
	Encryption protocols include: DES/AES/AES192/AES256			
	Encrypted password: the length is 8~ 31 characters, and cannot contain			
Enerytics Distance Enerytad	Chinese, full-width characters, question marks and spaces			
Encryption Protocol , Encrypted Password	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

- 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 D	escription Form
	obor noquironito b	

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
- On the global configuration interface, select the v2c version, and leave other settings as default. After the operation is complete, click <Save> .

Global Config Vi	ew/Group/Community/Client Access Control	Trap Settings
SNMP Service		
* SNMP Versior	n 🗌 v1 🗹 v2c 🗌 v3	
* Local Port	t 161	
* Device Location	Company	
* Contact Info	Ruijie@Ruijie.com	
	Save	

(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			+ Add	Delete Selected
Up to 20 entries are allowed.				
	View Name	Action		

Add			×
* View Name	system		
OID	.1.3.6.1.2.1		
		Add Excluded Rule	
Rule/OID List			Delete Selected
Up to 100 entries ar	e allowed.		
Rul	e	OID	Action
	No E	Data	
Total 0 10/page 🗸	< 1 > Go	to page 1	
			Cancel

(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	w/Group/Community/Client Access Co	ntrol Trap Settings			
SNMP v1/v2c Co	ommunity Name List				+ Att
Up to 20 entries are	allowed.				
	Community Name	Access Mode		MIB View	Action
Add				×	
* Community	y Name texttrtd1@				
* Acces	s Mode Read-Only	~			
* M	IB View system	~	Add View +		
			Cancel	ОК	

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 For	n
--	---

description item	illustrate
view range	Inclusion rule: OID is .1.3.6.1.2.1 and custom view is named " public_view "
	Group name: group
	Security level: authenticated and encrypted
group configuration	Readable view select " public_view "
	Writable view select " public_view "
	Notification view select " none "
	Username: v3_user
	Group name: group
v3 user configuration	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
- 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	/iew/Group/Community/Client Access Control	Trap Settings
SNMP Servi	ce 💽	
* SNMP Versio	on 🗌 v1 🔲 v2c 🗹 v3	
* Local Po	rt 161	
* Device Locatio	Company	
* Contact In	fo Ruijie@Ruijie.com	
	Save	

(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	view23		
OID	.1.6654		
	Add Included Rule	Add Excluded Rule	
Rule/OID List		[Delete Selected
Up to 100 entries ar	e allowed.		
Rul	e	OID	Action
	No [Data	
Total 0 10/page \vee	< 1 > G	o to page 1	
			Cancel

(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					Add Im Delete Selected
Up to 20 entries are allowed.					
Group Name	Security Level	Read-Only View	Read & Write View	Notification View	Action
default_group	Auth & Security	all	none	none	Edit Delete
Total 1 10/page < 1	> Go to page 1				
Add			×		
* Group Name	group				
* Security Level	Allowlist & Security	~			
* Read-Only View	all	 ✓ Add View + 	-		
* Read & Write View	all	 ✓ Add View + 	-		
* Notification View	none	✓ Add View +	-		
		Can			
		Can	Icel OK		

(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>.

Up to 50 entries are allowed	d.						
Username	Group Name	Security Level	Auth Protocol	Auth Password	Encryption Protocol	Encrypted Password	Action
			No Data				
otal 0 10/page 🗸 🤇	1 > Go to page 1						
dd					×		
* Username							
Osername	Username						
* Group Name	group ~						
	Auth & Security ~						
* Security Level							
			word				
* Security Level * Auth Protocol	MD5 ~	* Auth Pass					

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.

Global Config	View/Group/Community/Client Access Con	ntrol Trap Settings					
Trap Ser	vice 💽			×			
* Trap Ver	sion 🗹 v1 💟 v2c 💟 v3		Are you sure you want to Enable trap?				
	Save		Cancel	ОК			
Trap v1/v2c	Client List					+ Add	Delete Selected
Up to 20 entri	es are allowed.						
	Dest Host IP	Version Number	Port ID		Community Name		Action
			No Data				

When the first open is turned on, the system pops up a prompt message. Click <OK>.

Global Config	View/Group	/Community	//Client Acce	ss Control	Trap Settings
Trap Ser	vice 🔵				
* Trap Vers	sion 🔽 v1	✓ v2c	✓ v3		
		Save			

(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.

Global Config	View/Group/Community/Client Access Contro	Trap Settings			
Trap Se	rvice 🚺				
* Trap Ve	rsion 🗹 v1 🗹 v2c 🗹 v3				
	Save				
Trap v1/v2o	: Client List				+ Add
Up to 20 entr	ries are allowed.				
	Dest Host IP	Version Number	Port ID	Community Name	Action
			No Data		

(2) Configure trap v1v2c user-related parameters.

set up

Add		×
* Dest Host IP	Support IPv4/IPv6	
* Version Number	v1 ~	
* Port ID		
* Community Name/Username	Community Name/Username	

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]
	The community name of the trap user
	at least 8 characters
Group Name/User Name	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

Cancel

Table 12-6 t rap v1/v2c user information description table

A 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 .

Trap v	3 Client List					+ Add	Delete Selected
Up to 2	o entries are allowed.						
	Dest Host IP	Port ID	Username	Security Level	Auth Password	Encrypted Password	Action
				No Data			

(2) Configure parameters related to t rap v3 users.

Add					×
* Dest Host IP	Support IPv4/IPv6		* Port ID		
* Username			* Security Level	Auth & Security	~
* Auth Protocol	MD5	~	* Auth Password		
* Encryption Protocol	AES	~	* Encrypted Password		
				Cancel	ОК

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 of the trap v3 user at least 8 characters				
username	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 protocols include: MD5/SHA/SHA224/SHA256/SHA384/SHA512				
Authentication protocol, authentication password	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 t rap 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 1 92.1 68.110.85 and port number 1 66, 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:

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> ,

Global Config	View/Group,	/Communit	y/Client Access Control	Trap Settings
Trap Ser	vice 🔵			
* Trap Ver	sion 🗌 v1	✓ v2c	v 3	
		Save		

(2) Click <Add> in the " trap v1 / v2c user list " .

Trap v1/v	v2c Client List				+ Add
Up to 20	entries are allowed.				
	Dest Host IP	Version Number	Port ID	Community Name	Action
			No Data		

(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	192.168.110.77		
* Version Number	v1 ~		
* Port ID	123		
* Community	123e#dfd		
Name/Username			
		Cancel	ОК

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 $^{\rm "}$, 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> .

Global Config	View/Group	/Communit	y/Client Access Co	ontrol	Trap Settings
Trap Se	rvice 🔵				
* Trap Ve	rsion 🗌 v1	v2c	✓ v3		
		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.

* Dest Host IP	192.168.110.87		* Port ID	167
* Username	trapuser1_		* Security Level	Auth & Security \lor
* Auth Protocol	MD5	~	* Auth Password	Ruijie123
Encryption Protocol	AES	~	* Encrypted Password	Ruijie123

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.

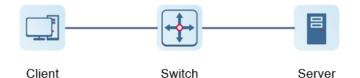
IEEE 802 LAN, as long as users can connect to network devices, they can directly access network resources without authentication and authorization. This uncontrolled behavior will bring security risks to the network. The IEEE 802.1x protocol was proposed to solve the security problem of 802 LAN.

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>.

Auth Config	Port	RADIUS Server Management	Wired Us	ser List
Global Co	onfig			
Glo	bal 802.1x			
Auth	nentication			
A	uth Server	Add a server to be authenticated	d.	ℓ_ Edit
		Advanced Settings		
		Configure		

Click Advanced Settings to configure parameters such as Guest VLAN .

Auth Config	Port	RADIUS Server Management	Wired User List
	Guest Vlan		
* EAP-Requ	uest Packet	2	
Retransmis	sion Count		
* Q	uiet Period	60	S
	ient Packet ut Duration	30	S
	ient Packet ut Duration	30	S
* EAP-Requ	uest Packet	30	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.
 - o Add username and password for client login.
 - Close the firewall, otherwise the authentication message may be intercepted, resulting in authentication failure.
 - o 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.

Up to 5 entries can be added.					
Server IP	Auth Port	Accounting Port	Shared Password	Match Order	Action
			No Data		
				×	
Add				^	
* Server IP					
* Auth Port	1812				
* Accounting Port	1813	0			
Accounting Fort	1015	0			
* Shared Password					
* Match Order		\bigcirc			

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	3 S	
* Packet Retransmission Count	3 time	
Server Detection		
MAC Address Format	XXXXXXXXXXX ~	?
	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: 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 Manageme	nt 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 \vee
Auth Mode	multi-auth \vee
Guest Vlan	
* User Count Limit per Port	1000

Cancel	ОК
--------	----

 \times

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	disable : Turn off the authentication method , which has the same effect as turning off the 802.1x authentication switch force- auth : Mandatory authentication , the client can directly access the Internet without a password force- unauth : Force no authentication, the client cannot be authenticated, nor can it access the Internet auto : automatic authentication, the device needs to be authenticated, and can access the Internet after passing the authentication It is recommended to select the auto authentication method .
Auth Mode	authentication mode	multi- auth : supports multiple devices using the same port for authentication, but each device needs to be authenticated independently 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 single-host : Each port only allows one device to be authenticated, and can access the Internet after successful authentication

parameter	reference - do not translate	illustrate
Guest Vlan	Guest VLAN	When enabled, devices that fail authentication will be dynamically assigned to the specified Guest VLAN 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
User Count Limit per Port	Maximum number of users per port	Limit the number of users under the interface Product Difference Description

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

Auth Config	Port RADIUS	Server Management	red User List					
Wired U	Jser List					Q Search by mac	Refresh	↓ Batch Logout
	Username	Status	Interface	MAC Address	Online Time	Online Duration	Access Name	Action
				No Data	3			
< 1	> 10/page >	Go to page 1						Total 0

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

information.

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 \mathbf{Add} , select the desired port and enter the gateway IP, click \mathbf{OK} .

🚺 note

Generally, the anti-ARP spoofing function is enabled on the downlink ports of the device.

1	Anti-ARP Spoofing Description: Anti-ARP Spoofing prevents hosts f Note: Anti-ARP Spoofing is generally configured	rom spoofing the source IP address of the ARP pac on a downlink port.	kets to be the IP address of the gateway.					
Ant	Anti-ARP Spoofing							
Up	to 256 entries can be added.							
	IP	Port	Action					
		No Data						

Add			×
* IP	192.168.1.1		
* Select Port:	available 💼 Aggreg.	ate 🕇 Uplink	Copper Fiber
1 3 5 7	9 11 13 15 17 19 21	23 25 27 29	9 31 33 35 37
2 4 6 8	10 12 14 16 18 20 22	1 2 2 2 3) 32 34 36 38
Note: You can click and	drag to select one or more ports.	Select Al	I Inverse Deselect
		Cancel	ОК

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.

i	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.							
An	ti-ARP Spoofing		∠ Add in Delete Selected					
Up	to 256 entries can be added.							
~	IP	Port	Action					
	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.

Ruíjie Reyce	Local Device(NBF >>			English ~ 🛆 Remote O&M	A Network Configuration 🕞 Log C
중 Home 중 VLAN	info Center	Port Info			
图 Monitor V	Port Info	Updated on2024-06-03 10:13:10 😋 Refresh			Panel View
Ports	VLAN Info	1 3 5 7 9 11 13 15 17 19	21 23		
 L2 Multicast L3 Interfaces 	Routing Info DHCP Clients		22 24 25 26 27 28		
Routing	ARP List MAC Address	Port Gi1			
Security	DHCP Snooping	Status Connected Negotiation Rate 1000M	Flow 4 1.62T 1 3.34T Total Packets 2229366192/67932003		Trunk Port 1
🖻 Advanced	IP-MAC Binding	Actual Rate U 4957kbps † 16545kbps Flow Control(Config Disable Status)	CRC/FCS Error 64/ Packets Corrupted/Oversized/1470506354	Allowed VLAN	1-4094 Effective VLAN 1,888,2001,3011-3013
Diagnostics	CPP	Flow Control(Actual Disable Status)	Packets Conflicts		
Info Center		Attribute OLT port			
Network Tools		1			
Fault Collection		VLAN Info (SVI&Routed Port) DNS: C	Refresh		
Cable Diagnostics		VLAN1 VLAN888 VLAN2001 VLAN3	011 VLAN3012 VLAN3013 Routed	Port Gi23	
«Collapse		Interface	IP Address DHCP Ad	ldress Pool	Remarks

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 L2 mode of the port and the VLAN to which it belongs, see <u>Configuring Port VLAN3.5.3 Configuring Port VLAN</u>.

Ruijie Rcycc	Local Device(NBF >		English ~	△ Remote O&M	। 👌 Network Confi	guration 🕞 Log Ou
음 Home 등 VLAN	info Center	Port Info				
🕾 Monitor 🗸 🗸	Port Info	Updated on2024-06-03 10:13:10 😋 Refresh				Panel View
Ports	VLAN Info	1 3 5 7 9 11 13 15	17 19 21 23	Role		Status
L2 Multicast	Routing Info			1.1.4	Copper	1G/2.5G/10G
⊕ L3 Interfaces ∨	ARP List		18 20 22 24 25 26 27 28] –	Fiber	10M/100M
B Routing	MAC Address	Port Gi12 Status Disconnected	Flow ↓ 0.00 ↑ 0.00		Uplink	Exception
Security ~	DHCP Snooping	Negotiation Rate	Total Packets/	VL	PoE/PoE+	Disconnected
🖹 Advanced 🛛 🗸	IP-MAC Binding	Actual Rate ↓kbps ↑kbps Flow Control(Config Disable	CRC/FCS Error/ Packets		PoE++	Disable
Diagnostics	IP SOURCE GUARD	Status) Flow Control(Actual Disable	Corrupted/Oversized/ Packets Conflicts		PoE Error Aggregate	
Info Center		Status) Attribute Copper	Connicts		OLT port	
Network Tools		1			SC fiber port	
«Collapse		VLAN Info (SVI&Routed Port) DNS	i: 😋 Refresh			

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.

🚺 note

- To configure VLAN, see <u>0</u>.
- To configure SVI ports and routed ports, see <u>Setting an L36.1 Setting an L3</u>.

Info Center	VLAN Info (SVI&Routed Port) DNS: C Refresh	
Port Info	VLAN1 VLAN888 VLAN2001 VLAN3011 VLAN3012 VLAN3013 Routed Port Gi23	
VLAN Info Routing Info	Interface IP Address DHCP Address Pool	Remarks
DHCP Clients	Gi1-8,Gi10-20,Gi22,Te25-27	VLAN0001
ARP List		
MAC Address		
DHCP Snooping		
IP-MAC Binding	2 4 6 8 10 12 14 16 18 20 22 24 25 26 27 28	
IP SOURCE GUARD		

13.1.3 Routing Info

A 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 <u>Configuring Static Routes6.3 Configuring Static Routes</u>.

InfoCenter	Routing Info						
Port Info	Tips: Up to 500 entries can be added.				Search by IP Addr	ess Q	C Refresh
VLAN Info	Interface	IP Addre	55	Subnet	Mask	Next	Нор
Routing Info DHCP Clients ARP List MAC Address	DHCP Clients		No Da	ta			
DHCP Snooping IP-MAC Binding	Tips: Up to 1000 entries can be added.				Search by Hostnar	me/IP Addı Q	C Refresh
IP SOURCE GUARD	Hostname	IP Address	MAC Ad	dress	Lease Time (Min)		Status
CPP			No Da	ta			

13.1.4 DHCP Clients

A 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.

1 note

To configure DHCP server related functions, see <u>Configuring the DHCP6.2</u> <u>Configuring the DHCP</u>.

InfoCenter	DHCP Clients				
Port Info	Tips: Up to 1000 entries can be a	dded.		Search by Hostname/IP Add	Q Q Refresh
VLAN Info	Hostname	IP Address	MAC Address	Lease Time (Min)	Status
Routing Info			No Data		
DHCP Clients			No Duta		
ARP List					
MAC Address	ARP List				
DHCP Snooping	1 ·				
IP-MAC Binding	Tips: Up to 2000 entries can be a	dded.		Search by IP Address/MAC	A Q C Refresh
IP SOURCE GUARD	Interface	IP Address	MAC Address	Туре	Reachable
II JOOKEL OOARD					

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.

1 note

To bind dynamic ARP or manually configure static ARP, see <u>Configuring a Static6.4 Configuring a Static</u>.

Info Center	ARP List				
Port Info	Tips: Up to 2000 entries can be a	dded.		Search by IP Address/MA	C A Q C Refresh
VLAN Info	Interface	IP Address	MAC Address	Туре	Reachable
Routing Info	VLAN888	192.168.88.197	c0:a4:76:1b:0f:1b	Dynamic	Yes
DHCP Clients	VLAN888	192.168.88.174	c0:a4:76:1b:0e:f2	Dynamic	Yes
ARP List	VLAN888	192.168.88.217	c0:a4:76:1b:0f:1c	Dynamic	Yes
MAC Address	VLAN888	192.168.88.73	00:ee:4c:21:14:0a	Dynamic	Yes
DHCP Snooping	VLAN888	192.168.88.166	00:e0:4c:21:71:21	Dynamic	Yes
IP-MAC Binding	VLAN888	192.168.88.77	48:81:d4:fe:8a:3a	Dynamic	Yes
IP SOURCE GUARD	VLAN888	192.168.88.96	00:e0:4c:21:71:26	Dynamic	Yes
Crr	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	f0:74:8d:b1:4c: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.

1 note

To configure and manage the MAC address, see <u>_MAC_Address_Management3.3</u>

MAC Address Management.

Info Center	MAC Address			
Port Info	Tips: Up to 16K entries can be added.	Sea	rch by MAC \vee	Q Refresh
VLAN Info	Interface	MAC Address	Туре	VLAN ID
Routing Info	Gi1	48:81:D4:FE:A8:B2	Dynamic	1
DHCP Clients	Gi2	48:81:D4:FE:88:A5	Dynamic	1
ARP List	Gi4	00:E0:70:E3:B7:2E	Dynamic	3012
MAC Address DHCP Snooping	Gi5	70:85:C4:5B:DC:1D	Dynamic	3013
IP-MAC Binding	Gi3	48:81:D4:FE:88:A8	Dynamic	1
IP SOURCE GUARD	Gi4	BC:0F:F3:76:7A:31	Dynamic	3012
CPP	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.

note

To modify DHCP Snooping related configuration, see <u>DHCP_Snooping7.1_DHCP_Snooping</u>.

Center	DHCP Snooping				
t Info	DHCP Snooping: Enabled	Option82: Disable	d	Trusted Port: Gi24,Te27,Te28 QR	efresh
AN Info	DHCP Snooping Binding Entries fro	m the Trusted Port			
uting Info	Interface	IP Address	MAC Address	VLAN ID	Lease Time (Min)
CP Clients	Gi4	192.168.89.92	00:0E:C6:04:A0:EC	888	480
P List	Gi9	192.168.88.167	00:D0:F5:20:08:97	888	480
C Address	Gi5	192.168.88.119	00:D0:FA:A1:00:23	888	480
CP Snooping	Gi5	192.168.88.164	00:E0:4C:21:70:03	888	480
MAC Binding	Gi5	192.168.88.89	00:E0:4C:21:71:12	888	480
OURCE GUARD	Gi5	192.168.88.137	00:E0:4C:21:71:13	888	480
5	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

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.

1 note

To add or modify the IP-MAC binding, see <u>IP-MAC Binding7.5 IP-MAC Binding</u>.

 Info Center 	IP-MAC Binding										
Port Info	Tips: Up to 500 entries can be a	dded.		Search by IP Address $ \lor$		Q C Refresh					
VLAN Info	Po	rt	IP Ad	ldress	MAC	Address					
Routing Info		No Data									
ARP List MAC Address	ARP List										
DHCP Snooping	Tips: Up to 1900 entries can be	added.		Search by IP Address \sim		Q C Refresh					
IP-MAC Binding	Interface	Rule	IP Address	MAC Address	VLAN ID	Status					
	Gi9	IP Address	192.168.88.167	00:D0:F5:20:08:97	888	Inactive					
CPP	0.0										
СРР	Gi4	IP Address	10.52.40.70	28:D0:F5:72:A9:5D	3012	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.

1 Note

To configure IP Source Guard function, see IP Source Guard7.6 IP Source Guard.

info Center	IP SOURCE GUARD					
Port Info	Tips: Up to 1900 entries can be	added.		Search by IP Address \sim		Q Refresh
VLAN Info	Interface	Rule	IP Address	MAC Address	VLAN ID	Status
Routing Info	Gi9	IP Address	192.168.88.167	00:D0:F5:20:08:97	888	Inactive
DHCP Clients	Gi4	IP Address	10.52.40.70	28:D0:F5:72:A9:5D	3012	Inactive
ARP List	Gi5	IP Address	192.168.88.166	00:E0:4C:21:71:21	888	Inactive
MAC Address	Gi5	IP Address	10.52.48.30	C0:B8:E6:1D:89:51	3013	Inactive
DHCP Snooping IP-MAC Binding	Gi4	IP Address	192.168.89.125	80:05:88:99:BC:FD	888	Inactive
IP SOURCE GUARD	Gi5	IP Address	192.168.88.132	00:E0:4C:21:76:66	888	Inactive
CPP	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
	< 1 2 3 4	5 6 … 62 → 10	/page v Go to page 1			Total 618

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.

info Center	СРР			
Port Info	Total CPU bandwidth: 2000pps 🛛 📿 Refresh			
VLAN Info	EtherType Value	Rate	Current Rate	Total messages
Routing Info	bpdu	60pps	Opps	0
DHCP Clients	lldp	50pps	2pps	5124000
ARP List	rldp	50pps	Opps	0
MAC Address	lacp	600pps	Opps	0
DHCP Snooping	rdla	600pps	Opps	0
IP-MAC Binding	arp	400pps	14pps	84656427
IP SOURCE GUARD	dhcp	600pps	3pps	4350407
	icmp	600pps	Opps	121
	macc	600pps	24pps	86588720
	mqtt	600pps	2pps	4540492
	< 1 2 3 4 5 > 10/pi	age \vee Go to page 1		Total 4

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.

Ruíjie Rcy	/CC	Local Device(NBF >>
🖧 Home		1 Network Tools
≝ VLAN		
🕾 Monitor	~	Tool • Ping Traceroute ONS Lookup
Ports	~	Type 💿 IPv4 💿 IPv6
L2 Multicast		* IP Address/Domain www.google.com
L3 Interfaces	~	* Ping Count 4
Routing	~	* Packet Size 64 Bytes
⊘ Security	~	Start Stop
🗄 Advanced	~	
Ø Diagnostics	^	Result
Info Center		
Network Tools]	A.

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** .

🖧 Home		0	Network Tools			
음 ^므 VLAN			Tool	O Ping	• Traceroute	O DNS Lookup
🖞 Monitor	~		1001	- Filig	• naceroute	
🔅 Ports	~		Туре	IPv4	○ IPv6	
L2 Multicast		* IP Ac	ldress/Domain	www.go	oogle.com	
L3 Interfaces	~		* Max TTL	20		
Routing	~				Start	Stop
😔 Security	~		Result			
🗄 Advanced	~					
Ø Diagnostics	^					
Info Center						k
Network Tools						

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.

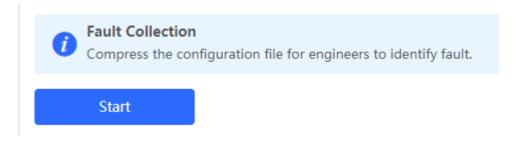
Select DNS Lookup as the diagnosis mode, enter a destination IP address or URL, and click Start .

Ruijie R	cycc	Local Device(NBF \vee		
ය Home		i Network Tools		
<i>≝</i> VLAN				
😤 Monitor	~	Tool	O Ping O Traceroute	DNS Lookup
Ports	~	* IP Address/Domain	www.google.com	
L2 Multicas	st	* DNS	8.8.8.8	
L3 Interface	es ~		Start	Stop
Routing	~	Result		
⊘ Security	~			
🗄 Advanced	~			
Ø Diagnostics	s ^			10
Info Center				
Network Too	ols			

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.

Port Panel																				
Available	Unavailable												l	r u	lplink		Сор	per	Fiber	
1 3 5 2 4 6	7 9 11 8 10 12	13 15 13 15 14 16	18	20 2	22 24	25 26		29	31	33	35	37	39	41	43	45	47 48	49	52	
te: You can click	and drag to s	select one	or mo	re por	ts.	St	tart								Selec	t All	Inve	erse	Deselect	
lesult																				
	Port								Cab	le Le	ngth	(cm)								Res

🛕 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.

View system logs.						
Log List					Search	Q
Time	Туре	Module		Details	local.info	
May 18 18:52:37	kern.crit	kernel	%Port-2: GigabitEthernet12 link up		syslog	
May 18 18:52:37	local.info	syslog	%L3-6: Manage VLAN 1 change to UP		kern.crit	
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 .

🚺 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.

A 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 13-1	Alert Types and Product Support
	, all i spool and i sou dot ouppoit

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 to10.44.77.100 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.

