

Ruijie Reyee ES, NBS, NIS Series Switch

Cookbook



Document Version: V1.7 Date: 2023.12.20 Copyright © 2023 Ruijie Networks

Copyright

Copyright © 2023 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 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: <u>https://www.ruijienetworks.com/products/reyee</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

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

Warning

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



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



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

Specification

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

3. Instruction

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

The example of the port type may be different from the actual situation. Please proceed with configuration according to the port type supported by the product.

The example of display information may contain the content of other product series (such as model and description). Please refer to the actual display information.

The routers and router product icons involved in this manual represent common routers and layer-3 switches running routing protocols.

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 Product Introduction
1.1 Reyee ES2 Series Switch1
1.1.1 Product List
1.1.2 LED Indicator2
1.1.3 Button
1.2 Reyee NBS Series Switch
1.2.1 Product List4
1.2.2 LED Indicator9
1.2.3 Button9
1.3 Reyee NIS Series Switch9
1.3.1 Product List9
1.3.2 LED Indicator10
1.3.3 Bottom Panel13
1.3.4 Cooling14
2 Device Management
2.1 Logging in15
2.1.1 Case Demonstration15
2.2 Configuring Password16
2.3 Upgrading16
2.4 Backing up and Resetting17
2.5 Restoring Factory Settings

3 Getting Start	19
3.1 Preparing for Installation	19
3.1.1 Safety Suggestions	19
3.1.2 Installation Site Requirement	20
3.1.3 Network Planning	21
3.2 Quick Provisioning	23
3.2.1 Quick provisioning via Ruijie Cloud APP	23
3.2.2 Quick provisioning via Reyee EWeb	33
4 ES Series Switches Port Settings	37
4.1 Managing Port Information	37
4.1.1 Port Status Bar	37
4.1.2 Port Info Overview	
4.1.3 Port Packet Statistics	
4.2 Setting and Viewing Port Attributes	39
4.2.1 Port Settings	39
4.2.2 Port Status	41
4.3 Port Mirroring	41
4.3.1 Overview	41
4.3.2 Configuration Steps	41
4.4 Port Isolation	42
4.5 Port-based Rate Limiting	43
4.6 Management IP Address	43
4.7 DC Port Reboot	44
5 ES Series Switches Switch Settings	46

5.1 Managing MAC Address	46
5.1.1 Overview	46
5.1.2 Viewing MAC Address Table	46
5.1.3 Searching for MAC Address	46
5.1.4 Configuring Static MAC Address	47
5.2 VLAN Settings	47
5.2.1 Global VLAN Settings	47
5.2.2 Static VLANs Settings	48
5.2.3 Port VLAN Settubgs	49
6 ES Series Switches Security	51
6.1 DHCP Snooping	51
6.1.1 Overview	51
6.1.2 Configuration Steps	51
6.2 Storm Control	51
6.2.1 Overview	51
6.2.2 Configuration Steps	52
6.3 Loop Guard	52
7 ES Series Switches PoE Settings	53
8 ES Series Switches System Settings	54
8.1 Managing Device Information	54
8.1.1 Viewing Device Information	54
8.1.2 Editing the Hostname	54
8.1.3 Cloud Management	55
8.2 Password Settings	55

8.3 Device Reboot	55
8.4 System Upgrade	56
8.4.1 Local Upgrade	56
8.4.2 Online Upgrade	56
8.5 Restoring Factory Configuration	56
9 ES Series Switches Monitoring	58
9.1 Cable Diagnostics	58
9.2 Multi-DHCP Alarming	58
9.3 Viewing Switch Information	59
10 NBS and NIS Series Switches Network management	60
10.1 Overviewing Network Information	60
10.2 Viewing Networking Information	60
10.3 Adding Networking Devices	63
10.3.1 Wired Connection	63
10.3.2 AP Mesh	65
10.4 Managing Networking Devices	65
10.5 Configuring the Service Network	67
10.5.1 Configuring the Wired Network	68
10.5.2 Configuring the Wireless Network	70
10.6 Processing Alerts	72
10.7 Viewing Online Clients	73
10.8 Smart Device Network	74
10.8.1 Overview	75
10.8.2 Procedure	75

11 NBS and NIS Series Switches Basic Management	80
11.1 Overviewing Switch Information	80
11.1.1 Basic information about the Device	80
11.1.2 Hardware Monitor Information	81
11.1.3 Port Info	82
11.2 Port Flow Statistics	84
11.3 MAC Address Management	84
11.3.1 Overview	84
11.3.2 Displaying the MAC Address Table	85
11.3.3 Displaying Dynamic MAC Address	86
11.3.4 Configuring Static MAC Binding	86
11.3.5 Configuring MAC Address Filtering	
11.3.6 Configuring MAC Address Aging Time	90
11.4 Displaying ARP Information	90
11.5 IPv6 Neighbor List	91
11.6 VLAN	92
11.6.1 VLAN Overview	92
11.6.2 Creating a VLAN	93
11.6.3 Configuring Port VLAN	95
11.6.4 Batch Switch Configuration	
11.6.5 Verifying Configuration	100
11.7 Viewing Optical Transceiver Info	100
12 NBS and NIS Series Switches Port Management	101
12.1 Overview	101

12.2 Port Configuration	102
12.2.1 Basic Settings	102
12.2.2 Physical Settings	104
12.3 Aggregate Ports	106
12.3.1 Aggregate Port Overview	106
12.3.2 Overview	107
12.3.3 Aggregate Port Configuration	108
12.3.4 Configuring a Load Balancing Mode	111
12.4 Port Mirroring	111
12.4.1 Overview	111
12.4.2 Procedure	112
12.5 Rate Limiting	114
12.6 MGMT IP Configuration	116
12.6.1 Configuring the Management IPv4 Address	116
12.6.2 Configuring the Management IPv6 Address	117
12.7 Out-of-Band IP Configuration	119
12.8 PoE Configuration	121
12.8.1 Viewing Global PoE Info	121
12.8.2 PoE Global Settings	121
12.8.3 Power Supply Configuration of Ports	122
12.8.4 Displaying the Port PoE Information	124
13 NBS and NIS Series Switches L2 Multicast	126
13.1 Multicast Overview	126
13.2 Multicast Global Settings	

13.3 IGMP Snooping127
13.3.1 Overview
13.3.2 Enabling Global IGMP Snooping128
13.3.3 Configuring Protocol Packet Processing Parameters
13.4 Configuring MVR131
13.4.1 Overview
13.4.2 Configuring Global MVR Parameters131
13.4.3 Configuring the MVR Ports132
13.5 Configuring Multicast Group134
13.6 Configuring a Port Filter136
13.6.1 Configuring Profile136
13.6.2 Configuring a Range of Multicast Groups for a Profile
13.7 Setting an IGMP Querier139
13.7.1 Overview
13.7.2 Procedure
14 NBS and NIS Series Switches L3 Multicast141
14.1 Overview
14.2 Multicast Routing Table141
14.3 Configuring PIM142
14.3.1 Overview
14.3.2 Enabling PIM142
14.3.3 Viewing PIM Neighbor Table143
14.4 Configuring RP143
14.4.1 Overview

14.4.2 Configuring a Static RP	144
14.4.3 Configuring a Candidate RP	144
14.5 Configuring BSR	145
14.5.1 Overview	145
14.5.2 Configuring BSR	145
14.5.3 Viewing BSR Routing Info	146
14.6 Configuring IGMP	146
14.6.1 Overview	146
14.6.2 Enabling IGMP	146
14.6.3 Viewing IGMP Multicast Group	147
15 NBS and NIS Series Switches L3 Management	148
15.1 Setting an L3 Interface	148
15.2 Configuring the IPv6 Address for the L3 Interface	150
15.3 Configuring the DHCP Service	153
15.3.1 Enable DHCP Services	153
15.3.2 Viewing the DHCP Client	155
15.3.3 Configuring Static IP Addresses Allocation	155
15.3.4 Configuring the DHCP Server Options	156
15.4 Configuring the DHCPv6 Server	158
15.4.1 Viewing DHCPv6 Clients	159
15.4.2 Configuring the Static DHCPv6 Address	160
15.5 Configuring the IPv6 Neighbor List	163
15.6 Configuring a Static ARP Entry	164
16 NBS and NIS Series Switches Configuring Route	166

16.1 Configuring Static Routes	166
16.2 Configuring the IPv6 Static Route	168
16.3 Configuring RIP	169
16.3.1 Configuring RIP Basic Functions	.170
16.3.2 Configuring the RIP Port	172
16.3.3 Configuring the RIP Global Configuration	174
16.3.4 Configuring the RIP Route Redistribution List	176
16.3.5 Configuring the Passive Interface	.177
16.3.6 Configuring the Neighbor Route	.179
16.4 Configuring RIPng	.181
16.4.1 Configuring RIPng Basic Functions	.181
16.4.2 Configuring the RIPng Port	183
16.4.3 Configuring the RIPng Global Configuration	184
16.4.4 Configuring the RIPng Route Redistribution List	185
16.4.5 Configuring the RIPng Passive Interface	.187
16.4.6 Configuring the IPv6 Aggregate Route	.188
16.5 OSPFv2	189
16.5.1 Configuring OSPFv2 Basic Parameters	.189
16.5.2 Adding an OSPFv2 Interface	198
16.5.3 Redistributing OSPFv2 Instance Routes	201
16.5.4 Managing OSPFv2 Neighbors	201
16.5.5 Viewing OSPFv2 Neighbor Information	202
16.6 OSPFv3	203
16.6.1 Configuring OSPFv3 Basic Parameters	203

16.6.2 Adding an OSPFv3 Interface	215
16.6.3 Viewing OSPFv3 Neighbor Information	218
16.7 Routing Table Info	219
17 NBS and NIS Series Switches Security	
17.1 DHCP Snooping	
17.1.1 Overview	
17.1.2 Standalone Device Configuration	
17.1.3 Batch Configuring Network Switches	
17.2 Storm Control	
17.2.1 Overview	
17.2.2 Procedure	
17.3 ACL	224
17.3.1 Overview	224
17.3.2 Creating ACL Rules	
17.3.3 Applying ACL Rules	
17.4 Port Protection	
17.5 IP-MAC Binding	
17.5.1 Overview	
17.5.2 Procedure	230
17.6 IP Source Guard	231
17.6.1 Overview	231
17.6.2 Viewing Binding List	231
17.6.3 Enabling Port IP Source Guard	232
17.6.4 Configuring Exceptional VLAN Addresses	

17.7 Configure 802.1x authentication	
17.7.1 Function introduction	
17.7.2 Configuration 802.1x	
17.7.3 View the list of wired authentication users	
17.8 Anti-ARP Spoofing	
17.8.1 Overview	
17.8.2 Procedure	
18 NBS and NIS Series Switches Advanced Configuration	
18.1 STP	
18.1.1 STP Global Settings	
18.1.2 Applying STP to a Port	
18.2 LLDP	
18.2.1 Overview	
18.2.2 LLDP Global Settings	
18.2.3 Applying LLDP to a Port	
18.2.4 Displaying LLDP information	
18.3 RLDP	
18.3.1 Overview	
18.3.2 Standalone Device Configuration	
18.3.3 Batch Configuring Network Switches	
18.4 Configuring the Local DNS	
18.5 Voice VLAN	
18.5.1 Overview	
18.5.2 Voice VLAN Global Configuration	

18.5.3 Configuring a Voice VLAN OUI	259
18.5.4 Configuring the Voice VLAN Function on a Port	
18.6 Configuring Smart Hot Standby (VCS)	
18.6.1 Configuring Hot Standby	
18.6.2 Configuring DAD Interfaces	
18.6.3 Active/Standby Switchover	
19 NBS and NIS Series Switches Diagnostics	
19.1 Info Center	
19.1.1 Port Info	
19.1.2 VLAN Info	
19.1.3 Routing Info	
19.1.4 DHCP Clients	
19.1.5 ARP List	
19.1.6 MAC Address	
19.1.7 DHCP Snooping	
19.1.8 IP-MAC Binding	
19.1.9 IP Source Guard	
19.1.10 CPP Info	
19.2 Network Tools	
19.2.1 Ping	270
19.2.2 Traceroute	270
19.2.3 DNS Lookup	271
19.3 Fault Collection	272
19.4 Cable Diagnostics	272

19.	5 System Logs	273
19.	6 Alerts	273
20 NB	S and NIS Series Switches System Configuration	276
20.	1 Setting the System Time	276
20.	2 Setting the Web Login Password	277
20.	3 Setting the Session Timeout Duration	277
20.	4 Configuring SNMP	278
	20.4.1 Overview	278
	20.4.2 Global Configuration	278
	20.4.3 View/Group/Community/Client Access Control	280
	20.4.4 Typical Configuration Examples of SNMP Service	
	20.4.5 trap service configuration	294
	20.4.6 Typical configuration examples of the trap service	299
20.	5 Configuration Backup and Import	301
20.	6 Reset	
	20.6.1 Resetting the Device	
	20.6.2 Resetting the Devices in the Network	
20.	7 Rebooting the Device	
	20.7.1 Rebooting the Device	
	20.7.2 Rebooting the Devices in the Network	
	20.7.3 Rebooting Specified Devices in the Network	
20.	20.7.3 Rebooting Specified Devices in the Network	
20. 20.	20.7.3 Rebooting Specified Devices in the Network	

20.9.2 Local Upgrade	
20.10 LED	
20.11 Switching the System Language	
21 NBS and NIS Series Switches Wi-Fi Network Setup	
21.1 Configuring AP Groups	
21.1.1 Overview	
21.1.2 Procedure	
21.2 Configuring Wi-Fi	310
21.3 Configuring Guest Wi-Fi	312
21.4 Adding a Wi-Fi	313
21.5 Healthy Mode	314
21.6 RF Settings	315
21.7 Configuring Wi-Fi Blocklist or Allowlist	
21.7.1 Overview	
21.7.2 Configuring a Global Blocklist/Allowlist	
21.7.3 Configuring an SSID-based Blocklist/Allowlist	318
21.8 Wireless Network Optimization with One Click	319
21.8.1 Network Optimization	319
21.8.1 Scheduled Wireless Optimization	
21.8.2 Wi-Fi Roaming Optimization (802.11k/v)	323
21.9 Enabling the Reyee Mesh Function	324
21.10 Configuring the AP Ports	325
22 Reyee FAQ	326
22.1 Reyee Password FAQ ((collection))	

22.2 Reyee Flow Control FAQ((collection))	326
22.3 Reyee Self-Organizing Network (SON) FAQ ((collection))	326
22.4 Reyee series Devices Parameters Tables	326
22.5 Reyee Parameter Consultation FAQ ((collection))	326

1 Product Introduction

1.1 Reyee ES2 Series Switch

Ruijie Reyee smart surveillance switches offer a variety of port options to meet the needs of video surveillance networks of different scales. Ruijie Reyee smart surveillance switches support full-power PoE output to ensure that all cameras can be powered simultaneously when connected to the switch at maximum capacity. In addition, Ruijie Real-easy Series smart surveillance switches provide simple and easy-to-use management features while offering plug and play with default factory configuration, which can quickly locate the surveillance network faults, initiate PoE port restart, perform VLAN configuration, etc. Ruijie Cloud app and Ruijie Cloud platform remote management is also supported, making the operation and maintenance of the surveillance network easier and more convenient, while reducing operation and maintenance costs.



1.1.1 Product List

Model	10/100 Base-T Auto- sensing Ethernet Port	10/100/1000 Base-T Auto- sensing Ethernet Port	1000Base-X SFP Port	Console Port
RG- ES205GC-P	N/A	5 (Ports 1-4 support PoE+/PoE)	N/A	N/A
RG- ES209GC-P	N/A	9 (Ports 1-8 support PoE+/PoE)	N/A	N/A
RG- ES218GC-P	N/A	16 (Support PoE+/PoE)	2	N/A
RG- ES226GC-P	N/A	24 (Support PoE+/PoE)	2	N/A

Model	10/100 Base-T Auto- sensing Ethernet Port	10/100/1000 Base-T Auto- sensing Ethernet Port	1000Base-X SFP Port	Console Port
RG-ES224GC	N/A	24	N/A	N/A
RG-ES216GC	N/A	16	N/A	N/A
RG-ES106D- P V2	6	N/A	N/A	N/A
RG-ES126S- LP V2	24	1	1 combo port	N/A
RG-ES126S-P V2	24	1	1 combo port	N/A

The SPF ports cannot be downward compatible with 100Base-FX.

1000Base-T is compatible with 100Base-TX and 10Base-T in the downlink direction.

1.1.2 LED Indicator

LED	State	Meaning
	Off	The switch is not receiving power.
System status LED	Blinking green	The PoE power exceeds the power of the entire device (370 W). The new connected PD cannot be powered up due to insufficient power. The switching function is operational.
	Solid green	The switch is operational.
	Off	PoE is not enabled.
LED	Solid green	PoE is enabled. The port is operational.
	Blinking green	Indicates PoE overload.
	Off	The port is not connected.
1000Mbps RJ-45 port	Solid green	The port is connected at 10/100/1000 Mbps.
status LED	Blinking green	The port is receiving or transmitting traffic at 10/100/1000 Mbps.
	Off	The port is not connected.
SFP port status LED	Solid green	The port is connected at 1000 Mbps.
	Blinking green	The port is receiving or transmitting traffic at 1000 Mbps.

1.1.3 Button

Botton	Description
Port mode LED Switch-Over button	 When the button is turned to the left position (Mode 1), the LED indicates the switching status of the port: when the LED is solid green, it indicates that the link is up; when the LED blinks green, data is being transmitted or received. When the button is turned to the right position (Mode 2), the LED indicates the PoE status of ports: when the LED is solid green, it indicates that the PoE-supported ports are supplying power; when the LED blinks green, the power of the ports is overloaded.
System reset The switch reboots after the reset button is pressed for less than 2 second button The switch restores the default factory settings after the reset button is pressed for less than 2 second more than 5 seconds (until the status LED blinks).	

1.2 Reyee NBS Series Switch

Reyee RG-NBS3100 series of managed switches are Reyee's 4 switches tailored for SME customer applications, which can meet the different levels of network access needs of SME customers. Covering basic VLAN division and advanced security features such as ACL,etc. The model with the suffix '-P' is a model that supports PoE output, and can meet the PoE power supply requirements of wireless APs, digital cameras and other devices in various occasions.

RG-NBS3200 series switch is a new generation of high-performance, strong security and integrated multiservice layer 2 Ethernet switch launched by Reyee. This series of switches adopts an efficient hardware architecture design, providing larger entry specifications and faster Hardware processing performance, more convenient operation experience. The RG-NBS3200 series provides flexible Gigabit access to 10 Gigabit uplink ports. The entire series of switches all have 4-port 10 Gigabit optical and high-performance port uplink capabilities.

Ruijie RG-NBS5100&5200 Series Switches are the next-generation high-performance, high-security and multiservice Layer 3 Ethernet switches. Adopting an efficient hardware architecture design, this switch series provides larger MAC address table size, faster hardware processing performance, and more convenient operating experience. RG-NBS5100 series provides Gigabit access and Gigabit uplink, while RG-NBS5200 series provides Gigabit access and 10G uplink ports. Every switch of this series offers 4 fixed 10G fiber ports with high-performance uplink capability.

RG-NBS5100&5200 series switches provide comprehensive end-to-end QoS as well as flexible and rich security settings for small and medium-sized networks at an extremely high price-performance ratio to meet the needs of high-speed, secure and smart enterprise networks.

RG-NBS6002 switch is 1U swappable box-type network switch independently developed by Ruijie Networks. It provides two line card slots for four types of line cards and two power supply module slots for 1+1 power redundancy. The following table describes components of an RG-NBS6002 switch.

The RG-NBS7000 series switches are next-generation switches launched by Ruijie independently. The switch comes into two models: RG-NBS7006 and RG-NBS7006. RG-NBS7003: Any line card can work as a supervisor

engine in slot 1 (slot 1 must be occupied). The switch provides three line card slots. RG-NBS7006: The switch provides two supervisor engine slots and six line card slots.



1.2.1 Product List

Model	10/100/1000 Base-T Ethernet Port	1000Base-X SFP Port	10G SFP+ Port	Console Port	Power Suppl y
RG- NBS3100- 24GT4SFP	24	4	N/A	N/A	Single
RG- NBS3100- 24GT4SFP-P	24 (Support PoE+)	4	N/A	N/A	Single
RG- NBS3100- 8GT2SFP	8	2	N/A	N/A	Power adapte r
RG- NBS3100- 8GT2SFP-P	8 (Support PoE+)	2	N/A	N/A	Single
RG- NBS3200- 24GT4XS	24	N/A	4	N/A	Single

Model	10/100/1000 Base-T Ethernet Port	1000Base-X SFP Port	10G SFP+ Port	Console Port	Power Suppl y
RG- NBS3200- 24SFP/8GT4 XS	8 (combo)	24	4	N/A	Single
RG- NBS3200- 24GT4XS-P	24 (Support PoE+)	N/A	4	N/A	Single
RG- NBS3200- 48GT4XS	48	N/A	4	N/A	Single
RG- NBS3200- 48GT4XS-P	48 (Support PoE+)	N/A	4	N/A	Single
RG- NBS5100- 24GT4SFP	24	4	N/A	N/A	Single
RG- NBS5100- 48GT4SFP	48	4	N/A	N/A	Single
RG- NBS5200- 24GT4XS	24	N/A	4	N/A	Single
RG- NBS5200- 24SFP/8GT4 XS	8 (combo)	24	4	N/A	Single
RG- NBS5200- 48GT4XS	48	N/A	4	N/A	Single
RG- NBS3100- 48GT4SFP-P	48	4	N/A	N/A	Single

Model	10/100/1000 Base-T Ethernet Port	1000Base-X SFP Port	10G SFP+ Port	Console Port	Power Suppl y
RG- NBS5100- 24GT4SFP-P	24	4	N/A	N/A	Single
RG- NBS5200- 24GT4XS-P	24	N/A	4	N/A	Single
RG- NBS5200- 48GT4XS-UP	48	N/A	4	N/A	Single
RG-NBS6002 Two service module slots	N/A	N/A	N/A	N/A	2, 1+1 power redund ancy is suppor ted
M6000- 24GT2XS	24	N/A	2	N/A	N/A
M6000- 24SFP2XS	N/A	24	2	N/A	N/A
M6000- 16GT8SFP2 XS	16	8	2	N/A	N/A
M6000- 16SFP8GT2 XS	8	16	2	N/A	N/A

Model	10/100/1000 Base-T Ethernet Port	1000Base-X SFP Port	10G SFP+ Port	Console Port	Power Suppl y
RG-NBS7003 Three line card slots Any line card can work as a supervisor engine in slot 1 (slot 1 must be occupied).	N/A	N/A	N/A	No console but has one manageme nt port	2, 1+1 power supply redund ancy
RG-NBS7006 Two supervisor engine slots and six line card slots Supervisor Engine M7006-CM	N/A	N/A	N/A	N/A	4, Suppor ts 1+1 and 2+2 power supply redund ancy
M7006-CM The supervisor engine of the RG-NBS7006 switch	N/A	N/A	N/A	10/100 Mbps MGMT port	N/A
M7000-16XS- EA	N/A	N/A	16	N/A	N/A
M7000- 24GT24SFP2 XS-EA	24	24	2	N/A	N/A
M7000- 48GT2XS-EA	48	N/A	2	N/A	N/A
M7000- 24GT2XS-EA	24	N/A	2	N/A	N/A

Model	10/100/1000 Base-T Ethernet Port	1000Base-X SFP Port	10G SFP+ Port	Console Port	Power Suppl y
M7000- 48SFP2XS- EA	N/A	48	2	N/A	N/A
M7000- 24SFP2XS- EA	N/A	24	2	N/A	N/A
M7000-8XS- EA	N/A	N/A	8	N/A	N/A

SFP port is downward compatible with 100Base-FX.

1000Base-T is downward compatible with 100Base-TX and 10Base-T.

Combo port consists of one 1000Base-X SFP port and one 10/100/1000Base-T Ethernet port. That is, only one port of them is available at a particular time.

Line Cards for 7K Series	10/100/1000 Base-T Ethernet Port	1000Base-X SFP Port	10G SFP+ Port
M7000-16XS-EA	-	-	16
M7000-24GT24SFP2XS- EA	24	24	2
M7000-48GT2XS-EA	48	-	2
M7000-48SFP2XS-EA	-	48	2
M7000-24SFP2XS-EA	-	24	2
M7000-8XS-EA	-	-	8

RG-NBS6002 switch is 1U swappable box-type network switch independently developed by Ruijie Networks. It provides two line card slots for four types of line cards and two power supply module slots for 1+1 power redundancy. The following table describes components of an RG-NBS6002 switch.

The RG-NBS7000 series switches are next-generation switches launched by Ruijie independently. The switch comes into two models: RG-NBS7006 and RG-NBS7006. RG-NBS7003: Any line card can work as a supervisor engine in slot 1 (slot 1 must be occupied). The switch provides three line card slots. RG-NBS7006: The switch provides two supervisor engine slots and six line card slots.

1.2.2 LED Indicator

LED	State	Meaning
	Off	The switch is not receiving power.
System status LED	Blinking green (0.5 Hz)	The switch is running, but the alarm of insufficient PoE power prompts.
	Blinking green (10Hz)	The switch is being upgraded or initialized.
	Solid green	The switch is connected to Ruijie Cloud.
	Off	The port is not connected.
10/100/1000Base-T	Solid green	The port is connected at 10/100/1000 Mbps.
Ethernet port status LED	Blinking green	The port is receiving or transmitting traffic at 10/100/1000 Mbps.
	Off	PoE is not enabled.
RJ45 port PoE status	Solid green	PoE is enabled. The port is operational.
	Blinking green	The port has a PoE fault of overload.
	Off	The port is not connected.
SFP port status LED	Solid green	The port is connected.
	Blinking green	The port is receiving or transmitting traffic.
	Off	The port is not connected.
SFP+ port status LED	Solid green	The port is connected.
	Blinking green	The port is receiving or transmitting traffic.

1.2.3 Button

Botton	Description
PoE mode switch- over button	Press PoE Mode Switch-Over Button for above 3 seconds to switch the display mode between PoE mode and port rate mode.
Reset button	The switch reboots after the reset button is pressed for less than 2 seconds. The switch restores the default factory settings after the reset button is pressed for more than 5 seconds (until the status LED blinks).

1.3 Reyee NIS Series Switch

1.3.1 Product List

Model	10/100/1000BASE-T Ethernet Port with Auto-Negotiation	1000BASE-X SFP Port	Console Port	10GE SFP+ Port	Power Supply
RG-NIS3100- 8GT4SFP-HP	8	4	N/A	N/A	1+1 redundancy

RG-NIS3100- 8GT2SFP-HP	8	2	N/A	N/A	1+1 redundancy
RG-NIS3100- 4GT2SFP-HP	4	2	N/A	N/A	1+1 redundancy

Note

1000BASE-T ports are downward compatible with 100BASE-T and 10BASE-T.

1.3.2 LED Indicator

1. Front Panel



Figure 1-1 Front Panel of RG-NIS3100-8GT4SFP-HP

Reset button: Press and hold the button for less than 2 seconds to restart the system. Press and hold the button for over 5 seconds until the system status LED starts blinking to restore factory settings and restart the system.

2. LEDs

LED	Silkscreen Label	Status	Description
· · · · · · · · · · · · · · · · · · ·			

		Off	The switch is not powered on.
		Fast blinking green (8–10 Hz)	The switch is starting up.
		Solid green	The switch is running properly.
System status LED		Slow blinking green (0.5 Hz)	The switch is not connected to the cloud.
	SYS	Blinking green (2 Hz)	The switch is restoring factory settings and will be powered off or is being upgraded.
		Blinking green at different time points (cycle: 1s on and 1s off, 0.25s on and 0.25s off, 0.25s on and 0.25s off, 0.25s on and 1.75s off)	The main program is lost or damaged, or specific functions are abnormal.
	LINK/ACT	Off	The port is Down.
		Solid green	The port is Up.
Electrical port and optical port LEDs		Blinking green	The port is Up and is receiving or sending data.
	PoF/PoF+	Off	PoE power supply is off.
	POE/POE+	Solid yellow	PoE power supply is on.
	P1	Off	PWR1 power supply is off.
Power status		Solid on	PWR1 power supply is on.
LEDs	P2	Off	PWR2 power supply is off.
		Solid on	PWR2 power supply is on.

3. Top Panel



Figure 1-2 Top Panel of NIS3100-8GT4SFP-HP

3. Alarm port

- 2. DC power connector PWR2
- 4. DC power connector PWR1

4. Rear Panel

The switch supports two installation modes: DIN rail mounting and wall mounting.









2. Mounting holes

1.3.3 Bottom Panel

ff ={

ff _____

(T



Figure 1-5 Bottom Panel of NIS3100-8GT4SFP-HP

1. Nameplate

1.3.4 Cooling

The RG-NIS3100-8GT4SFP-HP adopts natural cooling to ensure that it works properly in a specified environment. Maintain a minimum clearance of 100 mm (3.94 in.) around the device to ensure proper ventilation.

2 Device Management

2.1 Logging in

Web is a Web-based network management system used to manage or configure devices. You can access eWeb via browsers such as Google Chrome.Web-based management involves a Web server and a Web client. The Web server is integrated in a device, and is used to receive and process requests from the client, and return processing results to the client. The Web client usually refers to a browser, such as Google Chrome IE, or Firefox.

The Reyee managed switches not only support Web interface management, but also support life-time-free Ruijie Cloud App and Ruijie Cloud platform remote management. Users can view the network status, modify the configuration, and troubleshooting at home.

2.1.1 Case Demonstration

Network Topology

As shown in the figure below, you can access the eWeb management system of an access or aggregation switch via PC browser to manage and configure the device.



Set PC's IP assignment mode to obtain the IP address automatically.

Visit http://192.168.110.1 by Chrome browser.

Enter the password on the login page and click "Login".

Default Password: admin

RUJJE Hi, EG205G	
Password Login Forgot Password? English	

For the Reyee EG device, you may use either 192.168.110.1 or 10.44.77.254 to access the device.

For the **Reyee switches**, you may use 10.44.77.200 to access the device.

For the Reyee AP, you may use either 192.168.120.1 or 10.44.77.254 to access the device.

For the **EST**, you may use 10.44.77.254 to access the device.

The default login password for all Reyee devices is admin.

You may visit https://10.44.77.253 to login to the master device of Reyee network.

2.2 Configuring Password

Ruíjie l ® Rcycc	test123 > AP1 [Slave] 🕖
[®] Online Clients	<i>i</i> Change the login password. Please log in again with the new password later.
🖽 Router	* Old Password
♥ Wireless	* New Password
A Switches	
-e-Network ^	* Confirm Password
Time	Save
Password	
Scheduled Reboot	

2.3 Upgrading

Login to the eWeb of the device and choose Local Device > System > Upgrade.

Ruíjie Rcycc	Local Device(NBS \vee	English ~	٥	⋳
\oplus Routing \vee	Online Upgrade Local Upgrade			
 ⊘ Security 	Online upgrade will keep the current configuration.			
🗄 Advanced 🗸 🗸	Current Version			
② Diagnostics ~				
System				
Login				
Backup				
Upgrade				
Reboot				
Cloud Service				4
« Collapse				

2.4 Backing up and Resetting

Login in the eWeb of the device and choose Local Device > System > Backup.

Ruíjie Rcycc	Local Device(NBS V	English ~	٥	٩	G
Routing ~	Backup & Import Reset				
⊘ Security ~	If the target version is much later than the current version some configuration may be mission			0	
🗄 Advanced 🛛 🗸	You are advised to choose Reset before importing the configuration. The device will restart automatically later.			0	
Oiagnostics Second	Backup Config				
😤 System 🔷	Backup Config Backup				
Login	Import Config				
Backup	File Path Please select a file. Browse Import				
Upgrade					
Reboot					6
Cloud Service					A
« Collapse					

Login in the eWeb of the device and click Local Device > System > Reboot, then you can reset your devices.
Reyee Cookbook

Ruíjie Rcycc	Local Device(NBS	English \sim	٥	٩	
\oplus Routing \checkmark	() Please keep the device powered on during reboot.			?	
🛇 Security 🗸	Reboot				
🖶 Advanced 🗸 🗸					
Ø Diagnostics ~					
System					
Login					
Backup					
Upgrade					
Reboot					
Cloud Service					4
≪ Collapse					

2.5 Restoring Factory Settings

Login in the eWeb of the device Reset all device in the network.

Ruíjie Rcycc	Local Device(NBS > English >		₿
\oplus Routing \checkmark	Backup & Import Reset		
⊘ Security ∨	Resetting the device will clear the current settings. To retain the configuration, back up the profile.	?	
🖹 Advanced 🛛 👋	Keep Smart Hot Obsconnect the links between the member devices in the hot standby group after factory reset. Otherwise, a loop	may	
Diagnostics `	Standby Config		
System ^	Reset		
Login			
Backup			
Upgrade			
Reboot			
Cloud Service			4
« Collapse			

3 Getting Start

3.1 Preparing for Installation

3.1.1 Safety Suggestions

To avoid personal injury and equipment damage, please carefully read the safety suggestions before you install each device. The following safety suggestions do not cover all possible dangers

1. Installation

a) Keep the chassis clean and free from any dust.

b) Do not place devices in a walking area.

c) Do not wear loose clothes or accessories that may be hooked or caught by devices during installation and maintenance

2. Movement

a) Do not frequently move devices.

b) When moving devices, note the balance and avoid hurting legs and feet or straining the back.

c) Before moving devices, turn off all power supplies and dismantle all power modules.

3. Electricity

a) Observe local regulations and specifications when performing electric operations. Relevant operators must be qualified.

b) Before installing the device, carefully check any potential danger in the surroundings, such as ungrounded power supply, and damp/wet ground or floor.

c) Before installing the device, find out the location of the emergency power supply switch in the room. First cut off the power supply in the case of an accident.

d) Try to avoid maintaining the switch that is powered-on alone.

e) Be sure to make a careful check before you shut down the power supply.

f) Do not place the equipment in a damp location. Do not let any liquid enter the chassis

4. Static Discharge Damage Prevention

To prevent damage from static electricity, pay attention to the following:

a) Proper grounding of grounding screws on the back panel of the device. Use of a three-wire single-phase socket with protective earth wire (PE) as the AC power socket.

b) Indoor dust prevention

c) Proper humidity conditions

5. Laser

Some devices support varying models of optical modules sold on the market which are Class I laser products. Improper use of optical modules may cause damage. Therefore, pay attention to the following when you use them:

a) When a fiber transceiver works, ensure that the port has been connected with an optical fiber or is covered with a dust cap, to keep out dust and avoid burning your eyes.

b) When the optical module is working, do not pull out the fiber cable and stare into the transceiver interface or you may hurt your eyes.

3.1.2 Installation Site Requirement

To ensure the normal working and a prolonged durable life of the equipment, the installation site must meet the following requirements

1. Ventilation

For installing devices, a sufficient space (at least 10 cm distances from both sides and the back plane of the cabinet) should be reserved at the ventilation openings to ensure the normal ventilation. After various cables have been connected, they should be arranged into bundles or placed on the cabling rack to avoid blocking the air inlets. It is recommended to clean the switch at regular intervals (like once every 3 months). Especially, avoid dust from blocking the screen mesh on the back of the cabinet.

2. Temperature and Humidity

To ensure the normal operation and prolong the service life of router, you should keep proper temperature and humidity in the equipment room.

If the equipment room has temperature and humidity that do not meet the requirements for a long time, the equipment may be damaged.

In an environment with relatively high humidity, the insulating material may have bad insulation or even leak electricity. Sometimes the materials may suffer from mechanical performance change and metallic parts may get rusted.

In an environment with relatively low humidity, however, the insulating strip may dry and shrink. Static electricity may occur easily and endanger the circuit on the equipment.

In an environment with high temperature, the equipment is subject to even greater harm, as its performance may degrade significantly and various hardware faults may occur.

3. Cleanness

Dust poses a severe threat to the running of the equipment. The indoor dust falling on the equipment may be adhered by the static electricity, causing bad contact of the metallic joint. Such electrostatic adherence may occur more easily when the relative humidity is low, not only affecting the useful life of the equipment, but also causing communication faults.

4. Grounding

A good grounding system is the basis for the stable and reliable operation of devices. It is the chief condition to prevent lightning stroke and resist interference. Please carefully check the grounding conditions on the installation site according to the grounding requirements, and perform grounding operations properly as required

Lightning Grounding

The lightning protection system of a facility is an independent system that consists of the lightning rod, download conductor and the connector to the grounding system, which usually shares the power reference ground and yellow/green safety cable ground. The lightning discharge ground is for the facility only, irrelevant to the equipment.

EMC Grounding

The grounding required for EMC design includes shielding ground, filter ground, noise and interference suppression, and level reference. All the above constitute the comprehensive grounding requirements. The resistance of earth wires should be less than 1Ω

5. EMI

Electro-Magnetic Interference (EMI), from either outside or inside the equipment or application system, affects the system in the conductive ways such as capacitive coupling, inductive coupling, and electromagnetic radiation. There are two types of electromagnetic interference: radiated interference and conducted interference,

depending on the type of the transmission path.

When the energy, often RF energy, from a component arrives at a sensitive component via the space, the energy is known as radiated interference. The interference source can be either a part of the interfered system or a completely electrically isolated unit. Conducted interference results from the electromagnetic wire or signal cable connection between the source and the sensitive component, along which cable the interference conducts from one unit to another. Conducted interference often affects the power supply of the equipment, but can be controlled by a filter. Radiated interference may affect any signal path in the equipment and is difficult to shield.

a) For the AC power supply system TN, single-phase three-core power socket with protective earthing conductors (PE) should be adopted to effectively filter out interference from the power grid through the filtering circuit.

b) The grounding device of the switch must not be used as the grounding device of the electrical equipment or anti-lightning grounding device. In addition, the grounding device of the switch must be deployed far away from the grounding device of the electrical equipment and anti-lightning grounding device.

c) Keep the equipment away from high-power radio transmitter, radar transmitting station, and high-frequency large-current device.

d) Measures must be taken to shield static electricity.

e) Interface cables should be laid inside the equipment room. Outdoor cabling is prohibited, avoiding damages to device signal interfaces caused by over-voltage or over-current of lightning

3.1.3 Network Planning

The DHCP server has two address pools on the egress gateway: 192.168.110.0/24 in VLAN 1 for devices of this network 192.168.10.0/24 in VLAN 10 for clients of this network



Following ports are used for Ruijie Cloud management. To let devices go online on Ruijie Cloud, ensure these ports are available and the data stream is permitted in this network.

Domain name (Cloud-as)	DST.IP	Domain name (Cloud-eu, Cloud-me)	DST.IP	DST.TCP	DST.UDP
Device Online Related:		Device Online Related:			
devicereg.ruijienetworks.com	35.197.150.240	devicereg.ruijienetworks.com	35.190.10.141	80,443	
ryrc.ruijienetworks.com	35.197.150.240	ryrc.ruijienetworks.com	35.234.108.108	80,443	
stunrc.ruijienetworks.com	35.197.150.240	stunrc.ruijienetworks.com	35.234.108.108		34,783,479
stunsvr-as.ruijienetworks.com	34.126.80.150	stunsvr-eu.ruijienetworks.com	35.246.237.78		34,783,479
stunb-as.ruijienetworks.com	34.126.80.150	cwmpsvr-eu.ruijienetworks.com	34.159.112.239		34,783,479
stunc-as.ruijienetworks.com	34.87.169.209	cwmpcp-eu.ruijienetworks.com	34.120.73.71		34,783,479
cwmpsvr-as.ruijienetworks.com	35.197.136.171	cwmpb-eu.ruijienetworks.com	34.159.112.239	80, 443	
cwmpcp-as.ruijienetworks.com	34.160.143.162				
cwmpb-as.ruijienetworks.com	35.197.136.171				
Log Upload:		Log Upload:			
34.87.93.12	34.87.93.12	cloudlog-eu.ruijienetworks.com	35.246.247.49	80,443	
Advanced Service:		Advanced Service:			
firmware.ruijienetworks.com	34.87.32.36	firmware.ruijienetworks.com	34.89.153.55	80,443	
cloudweb.ruijienetworks.com	34.87.32.36	cloudweb.ruijienetworks.com	34.89.153.55	80,443	
fastonline.ruijienetworks.com	34.87.32.36	fastonline.ruijienetworks.com	34.89.153.55	80,443	
cloudapi.ruijienetworks.com	35.197.150.240	cloudapi.ruijienetworks.com	35.234.108.108	80,443	
cdn.ruijienetworks.com	35.201.94.110	cdn.ruijienetworks.com	35.190.93.193	80,443	
ES Series Switch		ES Series Switch			
iotrc.ruijienetworks.com	34.87.101.31	iotrc.ruijienetworks.com	34.107.106.56		7683
iotsvr-as.ruijienetworks.com	35.247.161.22	iotsvr-eu.ruijienetworks.com	35.242.228.40		5683
iotlog-as.ruijienetworks.com	35.240.167.168	iotlog-eu.ruijienetworks.com	35.198.144.180		6683
iotdl-as.ruijienetworks.com	34.87.141.45	iotdl-eu.ruijienetworks.com	35.234.118.145		8683
MQTT Devices with P206 version		MQTT Devices with P206 version			
ryrcmq.ruijienetworks.com	34.120.84.165	ryrcmq.ruijienetworks.com	34.149.186.87	25857	
ehrrcmq.ruijienetworks.com	34.120.84.165	ehrrcmq.ruijienetworks.com	34.149.186.87	25857	
mqclt001-as.rj.link	34.160.191.165	mqclt001-eu.rj.link	34.120.138.185	25857	

3.2 Quick Provisioning

3.2.1 Quick provisioning via Ruijie Cloud APP

The network topology shown in the below picture includes the Reyee gateway, Reyee POE switch and Reyee RAP.



1. Create a project

Open Ruijie Cloud App and Click Create a Project, then select Connect to Wi-Fi.



After click Yes, then Cloud App will prompt you to connect @Ruijie-mxxxx SSID.

Note:

@Ruijie-mxxxx is generated after network self-organization established successfully, while @Ruijie-sxxxx is generated on a standalone device, xxxx is the last four letters of mac address of device.



Connect the @Ruijie-mxxxx SSID on your phone.



After connected the @Ruijie-mxxxx SSID, the Cloud App will prompt to generate topology and detect all devices in this SON.



After all devices were detected, Cloud App will display them and show the topology, shown in the below picture. Click **Start Config** to perform the basic configuration of this project.

17:54 🛛 🖸 🖬 ··· 8.5KB/s 🚀 ලි කnl .ස් කු යො < Detect Device
Detect 3 devices The devices that support SON are displayed below.
EGIOSG-P EGIOSG-P TRAPI200(F) RAPI200(E)
Topo is incomplete?~
Detect Again Start Config

2. Configure the project

Input the Project Name and Management Password.

17:55 🚨 🖸 🖸 ···· 2.8KB/s 🕼 🎯 ၱ배 艘 🎅 🚳
< Basic Config
Project Config Internet Config Wi-Fi Config
Project Name * Reyee123
Management Password *
·····
For project safety, please ensure the password: has at least 8 characters contains 3 of these character types: lowercase letters: abcd uppercase letters: ABCD numbers: 0123 special characters: <=>[]!@#\$*(). can not contain "admin" can not contain spaces or question marks
Scenario *
Next

Then select the scenario of this project based on your requirement.



For configuring WAN, you can chose PPPoE, DHCP and Static IP.

17:55 🗳 🤷 🕻	0.5KB/s 🗐	° 🖓 📲 📲 🗢 🐠
Project Conf	ig Internet Config	─── ○ Wi-Fi Config
Single ISP Lin	nk: WANO	
Internet Connecti	ion of Link 1 (conne	ct to WAN0)
PPPoE	DHCP	Static IP
Network param assigned. You o	neters are automa don't need to con	itically figure.
802.1Q Tag		
O Dual ISP Link	s: WAN0 and WAN1	
	Next	
-		-

4. Configure the SSID

For SSID settings, input the name of SSID and configure it as open or configure password for this SSID. Select the region code.

	17:55 😫 🔼 🖸 🚥 1.1KB/s 🚀	° C III. II ? @ 160
<	Basic Config	
	Project Config Internet Config	Wi-Fi Config
Name/ Reyee1	ISSID *	8
Open		
Radio (Country/Region Code *	
China	3	
Tip: Plea	ase select your country or region.	

The configuration will be synchronized to the network

	17:55 🗳 🎦 🖸 ··· 0.2KB/s 🌾 🞯 ଜ୍ମା 🛒 😤 🚳
<	Add succeeded
	•
	15
	•
	Please wait
	Configuring Wi-Fi
	Configuring Device
	Configuring Network

After about 3s, Ruijie Cloud App will prompt that the configuration is delivery succeed.



Connect to the SSID created just now to manage the whole network on Cloud App.

17:56 🚨 🖸 🖸 ··· 0.0KB/s 🚀 🎯 🖬 .	ati 🔶 45)
\leftarrow	5
WLAN	
WLAN	
WLAN assistant	>
ଙ୍କ Reyce123 ହୁଏସ/୨୦ Connected	٠
	>

3.2.2 Quick provisioning via Reyee EWeb

The network topology shown in the below picture includes the Reyee gateway, Reyee POE switch and Reyee RAP.

17:56 🖪 🕒 🗖	··· 9.7KB/s	\$\$ 0 \$11; \$ 45
<	Reyee123	QG
Hotel Basic Enabled	CCTV Sr Disabled	Disabled IP
Project Sta		Uptime 0 d 0 h
Online Devices:3 Offline Devices:0		
	RAP1200(F) RAP1200	(E)
User Experience		
	No Data	
Egress Bandwidth		
C	~	
Tool Kit		



Connect PC to POE switch, set the ip address of PC as static ip address 192.168.110.x, then input 192.168.110.1 on the browser to login the EWEB of EG. All devices in this networks will display in EWEB. Click the Start Setup to perform the quick start of this network.

					English
Total Devices: 3. Please make sure that the device count and	d topology are correct. The unmanaged swit	ch will not appear in the lis	t.		Ø
Net Status (Online Devices / Total)	DHCP Internet	Router	Switch 1/1 Switches	令 1/1 APs	Refresh O
My Network					
New Device (3 devices)					~
Model	SN	IP	MAC	Softw	rare Ver
Router EG105G-P-V2 [Master]		192.168.110.1		1	914
AP RAP1200(E)		192.168.110.203	3		14
Switch RG-ES209GC-P	0	192.168.110.44	175	r,	1se(07200415)
	R	ediscover	Start Setup		

Show in the below picture, to finish the quick start of this network, you need to input the network name, configure the manner to access internet of this network and input the password of SSID or set the SSID as open. After select the Country/Region and click **Create Network & Connect**, the configuration will be delivery and activated, shown as the below two picture.

* Netv	work Name Re	eyeeNetwork
Networ	rk Settings	
	Internet	PPPoF DHCP Static IP Ourrent IP
	# a	hecking IP assignment
	* IP 17	72.26.6.162
• 51	ubnet Mask 25	55.255.252.0
	* Gateway 1	72.26.4.1
		E-EUR1
	DNS Server 19	92.168.58.94 192.168.58.110
	* SSID @	Ruijie-m0843
W.	-Fi Password	Security D Open
vvi-		ocony 🚽 Open
Country	y/Region/Tim	ie Zone
	Previous	Create Network & Connect
		syceNetwork
		Delivering configuration

After the configuration has been delivery and activated, you can enter the overview interface to manage the SON of Reyee devices.

त्याग्रह । बिRcycc Create Network		h ~ 🕞 Exit
* N Netwo * Subnet Mask * Gateway * DNS Server	Operation succeeded. Project Name: RoyseNetwork SSID: @Ruijie=m0843 Redirecting 255.255.252.0 172.26.4.1 192.168.58.94 192.158.58.110	
* SSID	@Ruijie-m0843	
Wi-Fi Password	🔿 Security 🔹 Open	
Country/Region/1	/Time Zone V	
Prev	evious Create Network & Connect	

Reyee Cookbook

Ruijie Rcycc	ReyeeNetwork > Ruijie (Master) 0		English 🗸 🛆 Ruijie Cloud	證Download App	work Setup @Network Check	<u>ṁ</u> Warn 🕞 Log Out
&Overview	Device Info	Setup> Wi-Fi				Setup>
(Online Clients	Hostname: Ruijie					
Router	SN: 119 Ip: 172.26.6.162 • EG105G-P-V2 Mac ⁻ :0843	Primary Wi-Fi: Re Security: No	veeNetwork	Guest Wi-Fi: Security:	No	
	Software Ver: 1 .55.1914					
☑ Switches						
	Net Status (Online Devices / Total)			_		Refresh 🗅
	() ↑ 3.71Kbps	Router ↓ 3.09Kbps (Switch		1	
	Internet	Router	Switches	APs	Online Clients	
	Real-Time Flow (Kbps)				Кыр	s 🗸 🤍 WAN 🗸
	8	Uplink Flov	Downlink Flow			
	7					
	5- 5-					
	4					
	3-					
	2					2
«Collapse						

4 ES Series Switches Port Settings

4.1 Managing Port Information

4.1.1 Port Status Bar

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



Different colors and shapes of the port icons represent different port statuses. See <u>Table 4-1 Port Icons</u> for details. Move the cursor over a port icon and the port status will be displayed, including the connection status, port rate, duplex mode, and flow control status.





Port Icon	Description
	The port icon is in the shape of a square, showing the port is a fiber port.
-	The port icon is in the shape of an RJ-45 connector, showing the port is a copper port.
Disconnected 4 5 6	The color of the port icon is black, showing the port is disconnected.

Disabled 3 4 5	The color of the port icon is gray, showing the port is disabled and cannot receive or transmit packets.
6 7 8 9 Loop 1000M / Full Duplex Disabled Flow Control	The color of the port icon is yellow, showing there is a loop.
Connected 1000M / Full Duplex Disabled Flow Control	The color of the port icon is green, showing the port is working normally.
	The number above the port icon is the port ID used to identify the device port. With the port ID, users can specify the port they want to configure.
1 2 3 4 5 6 7 8 9 Downlink Uplink	The device port is classified into the uplink port and the downlink port. The uplink port is used to connect network devices in the upper layer and access the core network. The downlink port is used to connect the endpoints.
	are isolated from each another, and they can only communicate with the uplink ports. For details, see Chapter <u>4.4 Port</u> <u>Isolation</u> .

4.1.2 Port Info Overview

Choose Homepage.

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

Click **Port Status** to configure the basic port attributes. For details, see Chapter <u>4.2</u> <u>Setting and Viewing Port</u> <u>Attributes</u>.

Click **Isolation Status** to configure port isolation so that the downlink ports of the device are isolated from each other. For details, see Chapter<u>4.4 Port Isolation</u>.

Click **Loop Status** to enable loop guard function. After a loop occurs, the port causing the loop will be shut down automatically. For details, see <u>6.3 Loop Guard</u>.

Click **Search** in the **Downlink Device** column to search for the downlink device of the selected port. After the search is done, click **View** to view the MAC address of the downlink device.

Click **Refresh List** to fetch the latest port information.

	Port Info Refresh List											
	Port Status								PoE			
Port	Status	Con	fig Status	Actual Status	Flow Control(Config)	Flow Control(Actual)	Rx/Tx Rate (kbps)	Isolation Status	Loop Status	PoF Power	Action	Downlink Device
		Speed	Duplex									
Port 1	Enabled •	Auto •	Auto •	1000M/Full Duplex	Disabled •	Disabled	8/58	Unisolated	Normal	- MAC:F	8:E4:3B:5A	CF:DC View
Port 2	Enabled •	Auto •	Auto •	Disconnected	Disabled •	Disabled	0/0	Unisolated	Normal			View
Port 3	Enabled •	Auto •	Auto •	Disconnected	Disabled •	Disabled	0/0	Unisolated	Normal			View
Port 4	Enabled •	Auto •	Auto •	Disconnected	Disabled •	Disabled	0/0	Unisolated	Normal			View
Port 5	Enabled •	Auto •	Auto •	Disconnected	Disabled •	Disabled	0/0	Unisolated	Normal			View
Port 6	Enabled •	Auto •	Auto •	Disconnected	Disabled •	Disabled	0/0	Unisolated	Normal			View
Port 7	Enabled •	Auto •	Auto •	Disconnected	Disabled •	Disabled	1/0	Unisolated	Normal			View
Port 8	Enabled •	Auto •	Auto •	Disconnected	Disabled 🔹	Disabled	0/0	Unisolated	Normal			View
Port 9	Enabled •	Auto •	Auto •	Disconnected	Disabled •	Disabled	0/0	Unisolated	Normal	PoE Unsup	ported	View

4.1.3 Port Packet Statistics

Choose Monitoring > Packet Statistics.

The **Packet Statistics** page displays the port status, the connection status, Rx/Tx rate (kbps), Rx/Tx packets (KB), Rx/Tx success, and Rx/Tx failure.

Click Clear to clear current packet statistics of all ports and reset the statistics.

Port	Status	Connection Status	Rx/Tx Rate(kbps)	Rx/Tx Packets(KB)	Rx/Tx Success	Rx/Tx Failure
Port 1	Enabled	Connected	3/5	349/1246	2778/2247	0/0
Port 2	Enabled	Disconnected	0/0	0/0	0/0	0/0
Port 3	Enabled	Disconnected	0/0	0/0	0/0	0/0
Port 4	Enabled	Disconnected	0/0	6/6	21/22	0/0
Port 5	Enabled	Disconnected	0/0	0/0	0/0	0/0
Port 6	Enabled	Disconnected	0/0	6/6	21/21	0/0
Port 7	Enabled	Disconnected	0/0	6/3	21/21	0/0
Port 8	Enabled	Disconnected	0/0	0/0	0/0	0/0
Port 9	Enabled	Disconnected	0/0	0/0	0/0	0/0
TOILS	Enabled	Disconnected	5,0	5,0	570	0,0

Packet Statistics

4.2 Setting and Viewing Port Attributes

Choose Switch Settings > Port Settings.

4.2.1 Port Settings

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

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

Port Settings

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

Ро	Port Status Speed Duplex		Duplex	Flow Control			
Sele	ect	Enabled 🔻	Auto 🔻	Auto 🔻	Disabled 🔻		
Select ALL	/Unse		Cours				
Port 1	<u>^</u>		Save				
Port 2			Port List				
Port 3							
Port 4		Spe	ed/Duplex	Flov	Flow Control		
Port 5		Config Status	Actual Status	Config Status	Actual Status		
Port 6	1	Auto/Auto	1000M/Full Duplex	Disabled	Disabled		
Port 7	1	Auto/Auto	Disconnected	Disabled	Disabled		
. 0		Auto/Auto	Disconnected	Disabled	Disabled		
Port 4	Enabled	Auto/Auto	Disconnected	Disabled	Disabled		
Port 5	Enabled	Auto/Auto	Disconnected	Disabled	Disabled		
Port 6	Enabled	Auto/Auto	Disconnected	Disabled	Disabled		
Port 7	Enabled	Auto/Auto	Disconnected	Disabled	Disabled		
Port 8	Enabled	Auto/Auto	Disconnected	Disabled	Disabled		
Port 9	Enabled	Auto/Auto	Disconnected	Disabled	Disabled		

Table 4-2 Basic Port Configuration Parameters

Parameter	Description	Default
Port	Select the ports you want to configure.	NA
Status	When the port is disabled, it cannot receive or transmit packets (PoE is not affected).	Enabled
Speed	Configure the operating speed of the Ethernet physical port. When the speed is set to Auto , it means that it is determined by the auto-negotiation between the local port and the peer port. The negotiated speed can be any speed within the port capability.	Auto
Duplex	 Full duplex: The port can receive packets while sending packets. Half duplex: The port can receive or send packets at a time. Auto-negotiation: The duplex mode of the port is determined by the auto-negotiation between the local port and the peer port. 	Auto
Flow Control	After enabling the flow control feature, the port will process the received flow control frames and send flow control frames when flow congestion occurs.	Disabled

A Caution

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

4.2.2 Port Status

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

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

Port List

4.3 Port Mirroring

4.3.1 Overview

In network monitoring and troubleshooting scenarios, users need to analyze data traffic on suspicious network nodes or device ports. When port mirroring is enabled, packets received and transmitted on the source port will be mirrored to the mirror port (destination port). Users can monitor and analyze the packets on the mirror port through network analyzer without affecting the normal data forwarding of the monitored device.

As <u>Figure 4-1</u> shows, by configuring port mirroring on Device A, the packets on Port 1 are mirrored to Port 10. Though the network analyzer is not directly connected to Port 1, it can receive all packets on Port 1 and is able to monitor the data traffic on Port 1.

Figure 4-1 Operating Principle of Port Mirroring



4.3.2 Configuration Steps

Choose Switch Settings > Port Mirroring.

Select the source port, the monitoring direction, and the mirror port, and click **Save**. The device supports configuring one port mirroring rule.

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

A Caution

- You can select multiple source ports but only one mirror port. The source ports cannot contain the mirror port.
- For RG-ES205C-P, RG-ES205GC-P, RG-ES209C-P, RG-ES209GC-P switches, the mirror port only supports packet capture and cannot transmit data with switches.

Port Mirroring

Parameter	Description		
Source Port Member	The source port is also called the monitored port. Packets on the source port will be mirrored to the mirror port for network analysis or troubleshooting. Users can select multiple source ports. Packets on these ports will be mirrored to one mirror port.		
Direction	 Direction of the data traffic monitored on the source port: Bi-directions (input & output): All packets on the source port, including the received packets and the transmitted packets, will be mirrored to the mirror port. Input: The packets received by the source port will be mirrored to the mirror port. Output: The packets transmitted from the sourced port will be mirrored to the mirror port. 		
Mirror Port	The mirror port is also called the monitoring port. The mirror port is connected with a monitoring device, and it transmits packets on the source port to the monitoring device.		

Table 4-3 Port Mirroring Parameters

4.4 Port Isolation

Choose Switch Settings > Port Isolation.

Port isolation is used for isolating layer-2 packets. When port isolation is enabled, the downlink ports are isolated from each other but can communicate with uplink ports.

Port isolation is disabled by default. Toggle the switch to **On** to enable port isolation.

Port Isolation					
Downlink ports (1-8) will be isolated from each other. Port 9 is an uplink port and will not be isolated (Packets will be forwarded only between the uplink port and the downlink ports).					
Status on					

🛕 Caution

The number of the uplink/downlink ports and port IDs of different devices vary. Please refer to the actual information of the device.

4.5 Port-based Rate Limiting

Choose QoS Settings > Port Rate.

Users can configure rate limiting rules for packets in the input direction and the output direction of ports. There is no rate limiting on ports by default.

Select the port you want to configure, then select the rate limiting type and status, and enter the rate limit. Click **Save** to save the configuration. The configuration will be displayed accordingly in the **Port Rate** table right below the **Save** button.

Port Rate					
Port	Туре	Status	Rate(Mbit/sec)		
Select	Input 🔹	Disabled •	No Limit (1-1000M)		

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

Table 4-4 Rate Limiting Parameters

Parameter	Description	Default
Port	Users can select multiple ports for rate limiting configuration in batches.	NA
Туре	 The direction of the rate-limited data traffic: Input & output: Rate limiting for all packets forwarded over the port, including the received packets and the transmitted packets. Input: Rate limiting for packets received by the port. Output: Rate limiting for packets transmitted from the port. 	NA
Status	Users can decide whether to enable or disable rate limiting.	Disabled
Rate (Mbit/sec)	The maximum rate at which packets are forwarded over the port.	No limit

🚺 Note

- The rate limiting range for RG-ES205C-P switch ports is from 1 to 100M.
- The maximum rate supported by port 1 to port 8 of RG-ES209C-P switch is 100M. If the configured rate exceeds 100M, the effective rate will still be 100M. The rate limiting range for port 9 is from 1 to 1000M.
- The rate limiting range for RG-ES226GC-P, RG-ES218GC-P, RG-ES205GC-P, RG-ES209GC-P, RG-FS303AB, RG-FS306-P, RG-FS306-D switches ports is from 1 to 1000M.

4.6 Management IP Address

Choose System Settings > IP Settings.

Users can configure the management IP address of the device. By accessing the management IP address, users can configure and manage the device.

There are two Internet types available:

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

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

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

VLAN is used for managing VLAN tag of the management packets. Disable VLAN settings, and the management packets will be untagged, and management VLAN configuration is not supported. The management VLAN of the device is VLAN 1 by default.

VIAN	1	(1-4094)
VEAN	Disable VLAN Settings, ar	nd the management packets will be untagged. If you want to tag packets, please enable VLAN Settings.
Auto Obtain IP	Enabled •	
	If you disable this feature	e, multi-DHCP alarming will fail.
IP Address	0.0.0.0	
Submask	0.0.0.0	
Gateway	0.0.0.0	
Auto Obtain DNS	Enabled •	
DNS	0.0.0.0	
		Save

IP Settings

🚺 Note

- Disable VLAN settings, and the management packets will be untagged. If you want to tag packets, please enable VLAN settings. For details, see Chapter 5.2.1 Global VLAN Settings_ .
- The management VLAN must be selected from the existing VLANs. To create a static VLAN, refer to Chapter 5.2.2 Static VLANs Settings.
- You are advised to bind a configured management VLAN to an uplink port. Otherwise, you may fail to
 access the web management system. For details, see Chapter <u>5.2.3 Port VLAN Settubgs</u>.
- If you disable Auto Obtain IP feature, multi-DHCP alarming will fail. For details about multi-DHCP alarming, see Chapter <u>9.2 Multi-DHCP Alarming</u>.

4.7 DC Port Reboot

🛕 Caution

Only RG-FS306-D switch supports this feature.

Choose DC Settings.

Select the DC port you want to reboot, and click **Reboot** to reboot the selected DC port. Click **Reboot all** to reboot all DC ports of the device.

DC Settings

Port	DC Reboot		
DC 1	Reboot		
DC 2	Reboot		
DC 3	Reboot		
DC 4	Reboot		
Reboot all			

5 ES Series Switches Switch Settings

5.1 Managing MAC Address

5.1.1 Overview

The MAC address table records mappings of MAC addresses and ports to VLANs.

The device queries the MAC address table based on the destination MAC address in a received packet. If the device finds an entry that is consistent with the destination MAC address in the packet, the device forwards the packet through the port specified by the entry in unicast mode. If the device does not find such an entry, it forwards the packet through all ports other than the receiving port in broadcast mode.

MAC address entries are classified into the following types:

- Static MAC address entries: Static MAC address entries are manually configured by the users. Packets whose destination MAC address matches the one in such an entry are forwarded through the corresponding port.
- Dynamic MAC address entries: Dynamic MAC address entries are learned dynamically by the device. They are generated automatically by the device.

5.1.2 Viewing MAC Address Table

Choose Switch Settings > MAC Address Info.

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

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

	MAC Address Info		
No.	MAC Address	Туре	Port
1	F8:E4:3B:5A:CF:DC	Dynamic	1
2	C8:4B:D6:06:FA:97	Dynamic	3
	Clear Dynamic MAC		

) Note

- If you disable VLAN, the device will forward packets according to only the destination MAC address.
 VLAN ID is not displayed in the MAC address table.
- Up to 100 MAC addresses are displayed.

5.1.3 Searching for MAC Address

Choose Switch Settings > Search MAC.

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

A Caution

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

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

MAC Address Search					
MAC Address VLAN ID					
00:00:00:00:00:00		VLAN ID (1	-4094)		
	Search				
MAC Address	VLAN ID	Туре	Port		
F8:E4:3B:5A:CF:DC	1	Dynamic	Port 1		

5.1.4 Configuring Static MAC Address

Choose Switch Settings > Static MAC.

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

A Caution

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

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

Up to 16 MAC addresses can be configured.				
I	MAC Address		VLAN ID	Port
00:0	0:00:00:00:00	VLAN	Port 1 🔻	
		Add		
No.	MAC Address	5	VLAN ID	Port
□ 1	C8:4B:D6:06:FA:	97	10	3
		Delete		

Static MAC Address

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

No.	MAC Address	VLAN ID	Port
1	C8:4B:D6:06:FA:97	10	3
	Delete		

5.2 VLAN Settings

5.2.1 Global VLAN Settings

Choose Homepage > Device Info.

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

When VLAN is disabled, the device operates like an un-managed switch. The device forwards packets according to the destination MAC address, and the VLAN information of the forwarding packets remains unchanged during the forwarding process.

When VLAN is enabled, the device operates like a managed switch. The device forwards packets according to the destination MAC address and VLAN ID. Users can configure the port mode (access or trunk) based on whether a VLAN tag is carried in packets. Besides, all device ports will be initialized to access ports.

Ruíjie I ®Re	yee														
Homepage									2	4 5 6 Downlink	7	89	i k		
System Settings	\sim										Collap	se)—			
Monitoring	~	VLA	N Settings on	0						I	Device I	nfo			
	VLAN	AN settings are enabled. The device forwards packets based n the combination of the destination MAC address and VLAN 0.			Firmware Version: ESW 1.0(1)B1P3,Release(07200415)										
Switch Settings	ID.				SN: CAR10UP013138										
	The a	access po	access port is used to connect to the endpoint. An access forwards packets to only member ports of the native I. The packets received or transmitted on this port are used			Uptime: 00h 38min 05s									
VLAN Settings	VLAN	N. The pa				e				Hostname:	ruijie			Edit	
QoS Settings	The t may nativ	trunk por belong t	yeu. runk port is used to connect to the switch. A trunk port belong to multiple permit VLANs, but only packets of the e VIAN are untagged								Port In	fo			
	After	After VLAN settings are disabled, all VLAN settings will be		Status				VLAN							
PoE Settings	desti	red and t ination N	ne device will IAC address.	forward paci	kets according to	Actua	il Status	Flow	onfig)	Flow	tual)	Туре	Permit	Native	Rx/Tx Rate (kbps)
				Speed	Duplex			control(cc	shing)	Control(AC	lual)				× 1 /

5.2.2 Static VLANs Settings

🛕 Caution

Static VLANs can be created only when the global VLAN settings feature is enabled. For details, see Chapter 5.2.1 Global VLAN Settings.

Choose VLAN Settings > VLAN Members.

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

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

		VLAN Members			
VLAN	Settings				
Up to	Up to 16 VLAN members can be configured.				
VL	VLAN ID (1-4094)				
		Add			
	No.	VLAN ID			
	1	1			
	2	10			
	Delete				

🚺 Note

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

5.2.3 Port VLAN Settubgs

🛕 Caution

Users can configure port VLAN only when the global VLAN settings feature is enabled. For details, see Chapter <u>5.2.1 Global VLAN Settings</u>.

Choose VLAN Settings > VLAN Settings.

Configure the port mode and VLAN members of a port, and you will know the allowed VLANs of the port and whether the packets forwarded by the port carry tags.

1 Note

You are advised to create VLAN members (refer to Chapter <u>5.2.2</u> <u>Static VLANs Settings</u>) before configuring the port based on VLANs. Click **VLAN Members** to access **VLAN Members** page where you can add VLAN members.

Select the port you want to configure and the port mode. If you select the access mode, select **Access VLAN** for the port and click **Save**. If you select the trunk mode, select **Native VLAN** for the port and enter the VLAN ID range allowed by the port and click **Save**.

VLAN Settings VLAN Settings 🐽 👔 You can go to VLAN Me rs to add a VLAN ID. Native VLAN Permit VLAN VLAN Type Port The packets of this VLAN are -Select--Select Access • VLAN 1 T Permit VLAN Port VLAN Type Native VLAN Port 1 Access Port 2 Access

Port 3	Access	10	10
Port 4	Access	1	1
Port 5	Access	1	1
Port 6	Access	1	1
Port 7	Access	1	1
Port 8	Access	1	1

Table 5-1 Port Modes

Port Mode	Description
Access	One access port can belong to only one VLAN and allow frames from this VLAN only to pass through. This VLAN is called an access VLAN.
	The frames from the access port do not carry VLAN tag. When the access port receives an untagged frame from a peer device, the local device determines that the frame comes from the access VLAN and adds the access VLAN ID to the frame. Access port is connected to the endpoints.

Port Mode	Description
Trunk	One trunk port supports one Native VLAN and several Permit VLANs. Native VLAN frames forwarded by a trunk port do not carry tags while Permit VLAN frames forwarded by the trunk port carry tags. Trunk port is connected to switches. Users can set the Permit VLAN range to limit VLAN frames that can be forwarded. Make sure the trunk ports at the two ends of the link are configured with the same Native VLAN.

Note

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

6 ES Series Switches Security

6.1 DHCP Snooping

6.1.1 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.

6.1.2 Configuration Steps

Choose Switch Settings > DHCP Snooping Settings.

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

🚺 Note

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

DHCP Snooping Settings

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

 Select ALL/Unselect

 ✓ Port 1
 Port 2
 Port 3
 Port 5
 Port 6
 Port 7
 Port 9
 Port 10
 Port 11
 Port 12
 Port 14
 Port 15
 Port 16
 Port 17

 Port 18
 Port 19
 Port 20
 Port 22
 Port 24
 Port 25
 Port 26

6.2 Storm Control

Select Trusted Port:

6.2.1 Overview

When a local area network (LAN) has excess broadcast, multicast, or unknown unicast data flows, the network speed will slow down and packet transmission will have an increased timeout probability. This situation is called a LAN storm, which may be caused by topology protocol execution errors or incorrect network configuration.

Users can perform storm control separately for the broadcast, unknown multicast, and unknown unicast data flows. When the rate of broadcast, unknown multicast, or unknown unicast data flows received over a device port exceeds the specified range, the device transmits only packets in the specified range and discards packets beyond the range until the packet rate falls within the range. This prevents flooded data from entering the LAN and causing a storm.

6.2.2 Configuration Steps

Choose QoS Settings > Storm Control.

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

The storm control type and corresponding rate are displayed in the table right below the **Save** button. When storm control is disabled, the rate of broadcast, unknown multicast, and unknown unicast data flows is not limited. The corresponding status is displayed **Disabled**. When storm control is enabled, the corresponding rate limits will be displayed.

Storm Control							
Туре		Port	Status	Rate(Mbit/sec)			
	Broadcast 🔹	Select	Disable 🔻	No Limit (1-1000M)			
			Save				
Turne	Broadcast/Mhit/coc)	Unknown Unic	act(Mhit/coc)	Unknown Broadcast/Mhit/cos)			
Type Deat 1	Disabled	Dial	ast(wbrysec)	onknown broadcast(mbr/sec)			
Port I	Disabled	Disa	bled	Disabled			
Port 2	Disabled	Disabled		Disabled			
Port 3	Disabled	Disal	oled	Disabled			
Port 4	Disabled	Disabled		Disabled			
Port 5	Disabled Disabled		Disabled				
Port 6	Disabled	Disabled		Disabled			
Port 7	Disabled	Disabled		Disabled			
Port 8	Disabled	Disal	oled	Disabled			
Port 9	Disabled	Disabled		Disabled			

1 Note

- The rate limit for the ports of RG-ES205C-P switch ranges from 1Mpbs to 100Mbps.
- The maximum rate supported by ports 1 to 8 of RG-ES209C-P switch is 100Mbps. If the configured rate exceeds 100Mbps, the effective rate will still be 100Mbps. The rate limit for port 9 ranges from 1Mbps to 1000Mbps.
- The rate limit for the ports of RG-ES226GC-P, RG-ES218GC-P, RG-ES205GC-P, RG-ES209GC-P, RG-FS303AB, RG-FS306-P, RG-FS306-D switches ranges from 1Mbps to 1000Mbps.

6.3 Loop Guard

Choose Monitoring > Loop Guard.

When loop guard feature is enabled, the port causing the loop will be shut down automatically. After the loop is removed, the port will be up automatically. Loop guard function is disabled by default.

100	n Gi	lard
LUU	p Gi	Jaru

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

7 ES Series Switches PoE Settings

A Caution

Only RG-ES226GC-P, RG-ES218GC-P, RG-ES209GC-P, RG-ES209C-P, RG-ES205GC-P, RG-ES205C-P, and RG-FS306-P switches support the PoE function.

Choose PoE Settings.

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

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



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

If a PD device fails, please power on the port connected to the PD device again to reboot it.

PoE Status When off, PoE will not work on this port	Port	Power(W)	Current(mA)	Voltage(V)	Power Status	Act
on 🔵	Port 1	0	0	0	Powered Off	-
on 🔵	Port 2	0	0	0	Powered Off	-
on	Port 3	0	0	0	Powered Off	-
on 🔵	Port 4	0	0	0	Powered Off	-
on	Port 5	0	0	0	Powered Off	-
on	Port 6	0	0	0	Powered Off	-
on	Port 7	0	0	0	Powered Off	-
on 🔵	Port 8	0	0	0	Powered Off	-

PoE Settings

🚺 Note

The fiber ports of RG-ES226GC-P, RG-ES218GC-P, and RG-FS306-P switches do not support the PoE function.
8 ES Series Switches System Settings

8.1 Managing Device Information

8.1.1 Viewing Device Information

Choose Homepage > Device Info.

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

Ruíjie i ®Reyee					English 🔻 Logout
Homepage			4 5 6 7 8 Downlink	9 Uplink	
System Settings $~~$			Collapse	e ,	
Monitoring \lor	VLAN Settings on	8	Device In	fo	
	Model:	RG-ES209GC-P	Firmware Version:	ESW_1.0(1)B1P3,Release(07200415)	
Switch Settings 🛛 🗸	MAC Address:	54:16:51:25:F6:1E	SN:	CAR10UP013138	
	IP Address:	0.0.0.0	Uptime:	00h 45min 50s	
VLAN Settings 🛛 🗸	Cloud Status:	Unconnected	Hostname:	ruijie Edit	
System Settings A			Downlink Co System	uplink ollapse	
IP Settings				5	
A		Hostname	ruijie		
Account Settings		MAC Addross	KG-ES209GC-P	-	
Deheet		IR Address	0.0.0.0		
Keboot		Submask	0.0.0.0		
the second s		Gateway	0.0.0.0		
Upgrade		DNS	0.0.0.0		
Bastava Dafavilt		SN	CAR10UP013138	8	
Restore Detault		Firmware Version	ESW 1.0(1)B1P3	.Release(07200415)	
		Firmware Date	Aug 04 2020		
Monitoring ~		Hardware Version	1.20		

8.1.2 Editing the Hostname

Choose Homepage > Device Info.

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

VLAN Settings on	•	Device In	fo
Model:	RG-ES209GC-P	Firmware Version:	ESW_1.0(1)B1P3,Release(07200415)
MAC Address:	54:16:51:25:F6:1E	SN:	CAR10UP013138
IP Address:	0.0.0.0	Uptime:	00h 47min 35s
Cloud Status:	Unconnected	Hostname:	ruijie

8.1.3 Cloud Management

Choose Homepage > Device Info.

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

VLAN Settings on 🔿 🕜		Device Info		
Model:	RG-ES209GC-P	Firmware Version:	ESW_1.0(1)B1P3,Release(07200415)	
MAC Address:	54:16:51:25:F6:1E	SN:	CAR10UP013138	
IP Address:	192.168.110.223	Uptime:	00h 12min 19s	
Cloud Status:	Connected Download App	Hostname:	ruijie Edit	

8.2 Password Settings

When the device password is the default password, users will be prompted to reset the password when they log into the Eweb management system. Click **Yes** to access the **Account Settings** page (or choose **System Settings** > **Account Settings** to access the page).

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

Account Settings			
Tip: The current password is the default password.			
Account	admin		
Password	Password Image: The password must contain only letters, numbers and the following special characters: <=>[]!@#\$*().		
Confirm Password	Confirm Password		

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

Account	Settings
---------	----------

Tip: The device is under uniform management and cannot be configured with an independent password. Please use MACC or App to change the password of all devices. If you change the password of only this device, configuration synch #zation will fail. Please enter <u>192.168.110.1</u> to change the global password.				
Account	admin			

🛕 Caution

- Upon your initial login to the Eweb management system, you must set the device management password first before you configuring other features.
- Please remember the device management password (default username/password: admin/admin). You
 may need to log in again after changing the password.
- If the device has been under uniform management, please use MACC or APP to change the networkwide password. Changing the password of this device will cause failure to synchronize network-wide settings to this device.

8.3 Device Reboot

Choose System Settings > Reboot.

Click **Reboot** to reboot the switch.

Reboot

Please click Reboot to reboot the switch.

Reboot

8.4 System Upgrade

8.4.1 Local Upgrade

Choose System Settings > Upgrade.

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

Keep Old Config is selected by default. That means the current configuration will be saved after device upgrade. If there is a huge difference between the current version and the upgrade version, you are advised not to select **Keep Old Config**.

Local Upgrade

Select File 🗹 Keep Old Config

Decompress the package and select the bin file for upgrade.

8.4.2 Online Upgrade

Choose System Settings > Upgrade.

When there is a new version in the cloud, the version number of the latest version will be displayed on this page, and the **Upgrade** button will become available. The device will download the installation package of the recommended version from the cloud and it will be updated to the latest version. Online upgrade will keep the old configuration by default.

Online Upgrade

ograde will keep the old configu	uration.
Current Version	ESW_1.0(1)B1P3,Release(07200415)
Latest Version The current version is the latest.	

🚺 Note

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

8.5 Restoring Factory Configuration

Choose System Settings > Restore Default.

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

Restoring

Restore factory configuration and reboot the device.

Restore

9 ES Series Switches Monitoring

9.1 Cable Diagnostics

Choose Monitoring > Cable Diagnostics.

Cable diagnostics allows users to check the status of Ethernet cables. For example, users can check whether the cables are short-circuited or disconnected.

Select the ports you want to detect, and then click **Start** to start cable diagnostics. The test result will be displayed accordingly. Click **Start All** to perform one-click cable diagnostics on all ports.

Port	Test Result	Details		
Port 1	Normal	The cable works well.		
Port 2	Disconnected	Please check cable connection or replace the cable.		
Port 3	Disconnected	Please check cable connection or replace the cable.		
Port 4	Disconnected	Please check cable connection or replace the cable.		
Port 5	Disconnected	Please check cable connection or replace the cable.		
Port 6	Disconnected	Please check cable connection or replace the cable.		
Port 7	Disconnected	Please check cable connection or replace the cable.		
Port 8	Normal	The cable works well.		
Port 9	Disconnected	Please check cable connection or replace the cable.		

Cable Diagnostics

Caution

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

9.2 Multi-DHCP Alarming

A Caution

- Only RG-ES226GC-P, RG-ES218GC-P, RG-ES224GC, RG-ES216GC switches support multi-DHCP alarming.
- Multi-DHCP alarming will fail when the device IP address is not obtained dynamically. For relevant IP address configuration, see Chapter <u>4.6 Management IP Address</u>.

Choose Homepage.

When there are multiple DHCP servers in a LAN, the system will send a conflicting alarm. An alarming message will be displayed in the **Device Info** column.

		compse	
N Settings Off	0	Device Info	Multiple DHCP servers exist 👔
Model:	RG-ES218GC-P	Firmware Version:	n: ESW_1.0(1)B1P20,Release(09182117)
MAC Address:	00:E0:4C:11:35:3D	SN:	N: CAQ71M1006444
IP Address:	192.168.110.190	Uptime:	e: 00h 00min 27s
Cloud Status:	Connectable Download App	Hostname:	e: ruijie Edit

Move the cursor to ¹ to view the alarm details, including the VLAN where the conflicts occur, port, IP address of DHCP server, and MAC address.

9.3 Viewing Switch Information

Choose Monitoring > Switches.

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

Primary	Device
rilliary	Device

The current device has been managed by the master device. Please click the IP address to manage the master device.					
IP Address SN Model					
<u>192.168.110.1</u>	H1RP4HH076624	EG105GW-E			

The device is able to automatically discover other switches in the same management VLAN. Information of these switches will be displayed in **Switch List**.

The first row of **Switch List** displays information of the current device, and the following rows display information of other devices. Click **IP Address** of a device to access the Eweb management system of the device (login required).

Switch List						
Up to 16 switches of the same management VLAN can be discovered.						
No.	IP Address	SN	Hostname	Model		
1	192.168.110.209(Local)	CARL542000171	ruijie	RG-ES205C-P		
2	<u>192.168.110.39</u>	MACCLLES226GC	ruijie	RG-ES226GC-P		
3	<u>192.168.110.102</u>	CAQB1AW047292	ruijie	New Model		

🚺 Note

The number of switches that can be discovered varies with product modes:

- RG-ES226GC-P, RG-ES218GC-P and RG-FS303-AB can discover 32 switches.
- RG-ES205C-P, RG-ES205GC-P, RG-ES209C-P, RG-ES209GC-P, RG-FS306-P and RG-FS306-D can discover 16 switches.

10 NBS and NIS Series Switches Network management

10.1 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.



10.2 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 SN:H1LA0U100362A	2	Software Ver:ReyeeOS 1.86 MGMT IP:192.168.110.1 MAC: 00:74:9c:87:6d:85	.1619
viscant viscast viscast viscast viscast restore viscast viscas	Port Status VLAN Info Port More	Port Status	LANO LAN1 L	anz wani wan	
		VLAN			Edit 🕲
M ² Coup M ² Coup 91 Marcon Composed		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.



10.3 Adding Networking Devices

10.3.1 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	A Network	•	Tip A devices r discovered	not in SON is I.Manage		×
	Status D Online 1/	evices 1/5>	Clients 4 >	Topology	List	
4	Unknown:	1 ⑦ {	A non-Ruijie de	vice or a Ruijie device	e not enabled	with SON.
11	Not in SON:	1 Mana	ge>>			
	In SON:	5				
	Gateway:	1				
	AP:	2				
•	Switch:	2				
	AC:	0				
Ļ	Router:	0 нсг	🝷 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**.

Rujje RCycc Discover Device					English 🗸 🕞 Exit
Total Devices: 20. Other De Please make sure that the device court	evices (to be added r at and topology are correct. T	nanually): 17.	not appear in the list. View	r Topology	0
Net Status (Online Devices / Total) Router	Switches	ি 0 / 0 APs	2 17 Other Devices	Refresh O
My Network					
NBS3100 (3 devices)					>
Other Devices 🕖					
New Device (1 devices)	Add to My Network				>
Unnamed Network (2 devices)	Add to My Network				>
	Re	discover Sta	rt Setup		
My Network					
NBS3100 (3 devices)					
Other Devices 🕖					
New Device (1 devices)	Add to My Networ	k			
✓ 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.

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

10.3.2 AP Mesh

If the AP supports the AP Mesh (Reyee Mesh) function, you do not need to connect cables after powering on the AP. The AP can be added to the current network in Reyee Mesh mode, establish a mesh networking with other wireless devices, and automatically synchronize Wi-Fi configuration.

\rm A Caution

To scan the AP, the Reyee Mesh function must be enabled on the current network. (For details, see <u>21.9</u> <u>Enabling the Reyee Mesh Function</u>.) The AP should be powered on nearby. It may fail to be scanned in case of long distance or obstacle blocking.

(1) Place the powered new AP near an existing AP, where the new AP can receive Wi-Fi signals from the existing AP. Log in to a device in the network. On the **Overview** page, click +AP in the upper-right corner of the topology to scan nearby APs that do not belong to the current network and are not connected to a network cable.



(2) Select the target AP to add it to the current network. You do not need to enter the password if the device to add is new. If the device has a password, enter the management password of the device.

10.4 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.

Ruij	jie @Rcycc					Navigation Q	English - 🛆 🎇	<u>e</u> @	ر ق
Q N	lavigation	Status D Online 1	evices Clients / 6 > 3 >	Topology	List			+	- AP
A N ₽ D	letwork ~	Alert Center No Alerts Yet	All (0)			↑ <u>84.26K</u> ↓ 40.	<u>67K</u>		
₿ G ⊗ C	iateway lients	Common Function WIO WIO will help RLDP O	ns o optimize Disabled HCP • Batch			Ruije abc SNHTLADU0036	DHCP Server		Overturn Restore Refresh
-a- 5)	ystem	Snoc Network Planning Wi-Fi VLAN (3):	pping Config g Setup		م م		N855200-245F/8 SNG1NW31N000172		
		默认组_lgh VLAN1 22 VLAN22	11 VLAN11		AP Group	2/2 (pert.) RG-E5205C-P SN-MACCWLD78920	500		(
	«Collapse	Wired VLAN (7):		Updated on:2022	2-05-09 04:00:15				
Тор	ology List				IP/MAG	C/hostname/SN/S [,] Q	🗇 Delete Offline Devices	Batch	Upgrade
	SN ≑	Status ≑	Hostname ≑	MAC ≑	IP ≑	Software	Ver	Model	*
	MACCWLD789205G	Online	ruijie 🖉	78:11:22:33:44:55	192.168.110.226	ESW_		RG-ES20)5C-P
Local	H1LA0U100362A	Online	Ruijie.abc [Master] 🖉	00:74:9C:87:6D:85	192.168.110.1 🖉	ReyeeOS		EG20	5G
	G1NW31N000172	Online	Ruijie 🖉	00:D3:F8:15:08:5B	192.168.110.89 🖉	ReyeeOS		NBS52 24SFP/80	:00- 3T4XS
	1234942570021	Online	RAP2200e 🖉	00:D0:F8:15:08:48	192.168.110.152 🖉	AP.	new	RAP220)O(E)
	G1QH2LV00090C	Online	Ruijie 🖉	C4:70:AB:A8:69:17	192.168.110.102 🖉	ReyeeOS		RAP226	i0(G)
	1 > 10/pa	ge 🗸							Total 5

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

NBS and NIS Series Switches Network management

		×	MSW	Hostname: Ruijie 2Software Ver:ReyeeOS 1.86.170Model:NBS5200-24SFP/8GT4XSMGMT IP:11.1.1.89SN:G1NW31N000172MAC: 00:D3:F8:15:08:58	4
Тор	ology List		▶ Port Status	Port Statue	
	SN \$	Status ≑	VLAN Info		
	MACCWLD789205GC	Online	Port		Panel View
Local	H1LA0U100362A	Online	Route Info	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	I
	G1NW31N000172	Online	RLDP	2 4 6 8 10 12 14 16 18 20 22 24 18 20 22 24	25 26 27
		Offline			
	1234942570021	Online		VLAN	Edit 🛇
	MACC522376524	Online			
	1			VLAN1 VLAN33 VLAN88	
	TU/page			Interface IP IP Range	Remark
				Gi2,Gi4,Gi6,Gi17- 24,Te25-28,Ag1-4,Ag8	
				1 3 5 7 9 11 13 15 17 19 21 23 17 19 21 23	

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

Тор	ology List				IP/MA	C/hostname/SN/S	Batch Upgrade
•	SN \$	Status ≑	Hostname 🌲	MAC ≑	IP \$	Software Ver	Model 🌲
	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	Sector State	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

10.5 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 **manage** to switch to the service network configuration page (or click **Network > Network Planning**).

Ruíjie Reyce	Networkwide Ma	Currently in Netw	rork mode.	Navigation	Q English ~	≙ ⊡
Q Navigation	No uplink port is not	configured as a t	Topology List		_	+ AP
Overview	Device WIACC500547	oro is enabled wit				
🖧 Network 🗸 🗸	Common Function	s				
Devices	RLDP OH Snoop	CP		t		
8 Clients Management						Overturn
*** C · · · · · · · · · · · · · · · · · · ·	Network Planning	manage		Unknown		Restore
-a- System	Wi-Fi VLAN (3):	Add		SN:UNKNOWN		Refresh
	@Ruijie-qqt VLAN1	@Ruijie-guest-2268 VLAN1				
	test VLAN130		Not in SON	Hot Standby Group	Not in SON	
	Wired VLAN (2):	Add	SN:1234942570069	SN:MACC506347678	SN:G1NW30B000041	
	VLAN0001 VLAN1	test VLAN130	Updated on:2023-10-16 04:00:08			4
« Collapse						

10.5.1 Configuring the Wired Network

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



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

1 Configure VLAN Parameters —		2 Configure Wire	d Acc	ess	3 Confirm Config Delivery	
	Description:					
	* VLAN ID:	33				
	Address Pool	Gateway				
	Server					
(Gateway/Mask:	192.168.33.1	/	255.255.255.0		
	DHCP Pool:					
	IP Range:	192.168.33.1] -	192.168.33.254		

(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	\times
✓ gre VLAN Parmeters Configure VLAN ✓ gre VLAN Parmeters Configure VLAN ✓ gre VLAN Parmeters Configure VLAN ✓ Unit of the second configure VLAN of the second configure (second configure vLand) ✓ Unit of the second configure VLAN of the second configure vLand of the second c	

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

Configure Network Planning/Add Wired VLAN		\times
1 Configure VLAN Parameters	2 Configure Wired Access 3 Confirm Config Delivery	
Overturn Restore	To configure (VLAN33) with IP range 192.168.33.1~192.168.33.254, configuration will be delivered to device(s). The following configuration will be delivered: Image: Confi	
	Previous Save	

10.5.2 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 Wi-Fi VLAN	×
1 Configure Wireless Access — 2 Configure VLAN Parameters 3 Confirm Config	Delivery
* SSID:	
Security: O Security O Open	
Band: • 2.4G + 5G 2.4G 5G	
	e
Next	A i

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

Configure Network Planning/Add Wi-Fi VLAN		×
1 Configure Wireless Access	2 Configure VLAN Parameters	3 Confirm Config Delivery
Description	:	
* VLAN ID:	13	
topo.addressPoo	Gateway	
Gateway/Masi	: 192.168.13.1 / 255.255.255.0	
DHCP Poo		
ir Kalığı	192.108.13.1	
	Previous Next	(e Ai

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

Configure Netwo	rk Planning/Add Wi-Fi VLAN		×
	1 Configure Wireless Access	2 Configure VLAN Parameters	
Overturn		To configure (VLAN13) with IP range 192.168.13.1~192.168.13.254, configuration will be deliver device(s). The following configuration will be delivered:	red to
Restore	2	др SSID:test Password:12345678	
	E01050V/E SHIMACCINE27722	Add VIAN 13.1P. 192.168.13.1 Subnet Mark: 255.255.255.0 DHCP Pool. Saart 192.168.13.1 End IP Address: 192.168.13.254 DNS: 192.168.13.1 Lease TimeMiniH80	
	Not in SON RAZ22000 85		
	SNG1QP94K016658		e.
		Previous Save	A i

10.6 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.





10.7 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 1 / 17 / 1 >	Clients 33 >
Alert Center		Wired 33
No Alerts Yet		2.4G: 0
		5G: 0
Common Fun	ctions	

All (29)	Wired (29)	Wireless (0)			
i Onl The	l ine Clients client going offline	e will not disappear immediately. Ins	tead, the client will stay in the li	st for three more minutes.	?
Online	Clients			Search by IP/MAC/Username Q	C Refresh
U	sername/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 10-1 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.
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.

10.8 Smart Device Network

A Caution

Currently, the function is supported by RG-NBS6002 Series, RG-NBS7003 Series and RG-NBS7006 Series devices.

10.8.1 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.

10.8.2 Procedure

Choose Network > Clients > Smart Device Network.

(1) Click Identify Client.



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

I Identify (Client Type Client Subnet IP and Mask 192.168.1.0	Client — 2 Isolate Client — Planned Count @	3 Confirm Config — 4 Deliver Co Client Server IP	Added Clie	nts
Client Type Client Subnet IP and Mask Client Subnet IP and Mask	Planned Count 🖉	Client Server IP	Added Clie	nts
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				

(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**.

1

Sma	rt Device Network									
		Identified Se	rvers in 192.168.1.0/	/24				×		
	Client Type 🕑 🤇	No. ÷	Hostname: ≑	IP ≑	MAC \$	Switch SN $\ensuremath{\hat{\Rightarrow}}$	Switch Port $\mbox{$\stackrel{\diamond}{=}$}$		tified Clients	Refresh 254/2
	test	1	-	192.168.1.2	00:D0:F8:22:74:5E	MACC2020ABCDE	Gi1/23			
				Isolate Clier	t 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**.

mart Device Network						
	1 Identify Client	- 2 Isolate Client	- 3 Confirm Config 4 De	liver Config		
Subnet 🛛	Isolated VLAN Name Ø	VLAN ID Ø	Gateway Address 🛛	Subnet Mask 🛛	Client Isolation Planning	
100 100 1 0/01					192.168.1.0/24	VLAN3
192.168.1.0/24	test_vlan	3	192.168.1.240	255.255.255.0		
test 254 Server 1 🐻						
		Previous Genera	te 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 Target Devices Ruijie(MACC2
Over Rest	um
Previous	veliver 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.

mart Device Network					
	1 Identify Client	- 2 Isolate Client	– 3 Confirm Config –	- 4 Deliver Config	
Configuration de	livery succeeded.				
Config Delivery Del	ails				
 Device VLAN Cor 	fig				\sim
DeviceRuijie (/ACC2020ABCDE) : Update VLAN:test_vlan, VlanId: :	3			
 Port VLAN Config 	1				~
DeviceRuijie (//ACC2020ABCDE) : Port Gi1/1Set as Trunk Port, Nati	ve Id:1,Allow Vlan:1-4094			
Subnet Vlan Con	ig				~
DeviceRuijie (/ACC2020ABCDE) : Setup Subnet VLAN3:192.168.1.2	40 255.255.255.0			
		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	ork 0	Batch Edit Hostnames	IP address, MAC address or hos	tname Q
Ill Clients Online Total 35	test: 192.168.1.0/24		Delete Client	Delete Subnet C
	Status	Username	$IP \Leftrightarrow MAC \Leftrightarrow$	Switch SN ≑
other Total	• Offline test	Ø	192.168.1. 00:D0:F8:22:7 2 4:5E	MACC2020ABCDE
34 42	Online test	Ø_	192.168.1. 00:E0:4C:0A:0 200 0:27	MACC2020ABCDE
	< 1 > 10/page ~			Total 2
	other: (a) • 34 • 42			Delete Client 🔻

11 NBS and NIS Series Switches Basic Management

11.1 Overviewing Switch Information

11.1.1 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, power supply status, etc.

Ruffe RCyCC Local Device(NIS: >		English 🗸 🛆 Remote O&M 👌 Network Configuratio	n 🕞 Log Ou
Hostname: Rujje SN: 01CH1EH002222 • NIS3100- Software Wision: ReyeeOS 2.248.0.2114 Hardware Version: 1.00 BGT4SFP-HP Home VLAN Monitor ~ Ports ~ L2 Multicast Security ~ Advanced ~	IP Address: 10.524288 MAC Address: 00.0078.150866 DHS: 172.30.44.20,192.166.528 Diagnostics Y System Y		ල Reboot
Basic Info Device Model: NIS MAC Address: 0020/5781508:56 Connection • Online Status: Software Version: ReyeeOS 2:248:	Device Name: Ruijie 2, Working Mode: Self-Organizing Network 2, Master Device IP: 10.52.46.213 System Time: 2023-09-18 1451:30	SN: G1QH1EH002322 MGNT IP: 10.52.49.89 Hardware 1.00 Version: Uptime: 3 days 22 hours 51 minutes 1 second	
Port Info © Panel View Traffic data is updated every 5 minutes. © Refeeti			
	1 3 5 7 9 11 2 4 6 8 10 12		

1. Setting the device name

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

Bas	ic Info Edit Hostname	
	Model: NP\$7002	
	Edit Hostname	
	Ruijie	rk 🧟
Sn	Cancel	

2. Switching the Work Mode

Click the current work mode to change the work mode.

	Description:
Basic Info	 The device IP address may change upon mode change.
Hostname: Ruiile Ø	2. Change the endpoint IP address and ping the device.
Model: NBS Status: • Online	 Enter the new IP address into the address bar of the browser to access EWEB.
Work Mode: Self-Organizing Network 🍭	4. The system menu varies with different work modes.
Smart Monitoring	Self-Organizing
PS is short for power supply.	Network
Temperature: OK Fan 1 Presence: Present	Save

3. Setting MGMT IP

Click current management IP address to jump to the management IP configuration page. For more information, see <u>12.6 MGMT IP Configuration</u>.

Basic Info					
Device Model:	NIS	Device Name:	Ruijie 🖉	SN:	G1QH1EH002322
MAC Address:	00:D0:F8:15:08:66	Working Mode:	Self-Organizing Network 🖉	MGMT IP:	10.52.49.88 🕲
Connection	Online	Master Device IP:	10.52.48.213	Hardware	1.00
Status:				Version:	
Software Version:	ReyeeOS 2.248	System Time:	2023-09-18 14:52:01	Uptime:	3 days 22 hours 51 minutes 32 seconds

11.1.2 Hardware Monitor Information

A Caution

Only RG-NBS6002 Series, RG-NBS7003 Series and RG-NBS7006 Series devices support displaying this type of information.

Choose Local Device > Home > Smart Monitoring.

Display the current hardware operating status of the device, such as the device temperature and power supply status, etc.

R	Local Device(NBS ~						English \sim	٥	٩	₿
에 Na SH 양	Basic Info Hostname: Model: Status: Work Mode:	Ruijie & NBS7003 • Online Self-Organizing Network &	MGMT IP: MAC: SN:	172.30.102.84 @ 00:D0:F8:22:74:5E MACC2020ABCDE	Software Ver: Systime: Uptime:	ReyeeOS 1.50 2022-05-19 1 3 days 2 hour	0.1706 9:44:36 rs 38 minutes			
•	Smart Moni	toring								
\bigcirc	PS is short for	power supply.								
	Temperature: Fan 1 Presence: Fan Type: PS1 Presence: PS1 Pype: PS2 Presence:	OK Present Absent	Fan Version: Fan Speed: Power: PS Status: Power:	0.64 1650rmp 	Fan SN: Fan Status: PS SN: PS Version: PS SN:	OK 				
	PS2 Presence: PS Type: Port Info ③ The flow data w	Absent Panel View ill be updated every 5 minutes. © 1	Power: PS Status: Refresh		PS SN: PS Version:				_	
>>	M	7000-24GT2XS-EA/MACCZZZFFf 1 3 5 7 9 11 13	F123 <mark>Online</mark> 15 17 19 2	21 23						

11.1.3 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 🗸 🔿	談 合	G
ጽ	Port Info	⑦ Panel View							
	The flow data	will be updated every	/ 5 minutes. 😋 Refresh						
<u>+</u>									
谷			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			
÷	Port	Rate	Rx/Tx Speed (kbps)	Rx/Tx Bytes	Rx/Tx Packets	CRC/FCS Error Packets	Corrupted/Oversized Packets	Conflicts	
۵.	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	6
	Gi8	Disconnected	0/0	0.00/0.00	0/0	0/0	0/0	0	
>>	Gi9	Disconnected	0./0	0.00/0.00	0./0	0./0	0./0	Ο	



• 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	Port Info @ Panel View							
The flow data	will be updated every	5 minutes. 🔾 Refresh	n					
		1 3 5 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	7 9 ·	11 13 15 17 19 2 12 14 16 18 20 2	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 📀	Panel View						
The flow data w	vill be updated every	5 minutes. 🛇 Refresh					
			_				
			9 11 13 15	17 19 21 23			
		2 4 6 8	10 12 14 16	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

11.2 Port Flow Statistics

Choose Local Device > Monitor > Port Flow.

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

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

Note

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

Port	Info						Clear Selected	i Clear All
The fl	ow data will be	updated every 5 minu	tes. 🔉 Refresh					
	Port	Rate	Rx/Tx Speed (kbps)	Rx/Tx Bytes	Rx/Tx Packets	CRC/FCS Error Packets	Corrupted/Oversized Packets	Conflicts
	Gi1 🕇	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

11.3 MAC Address Management

11.3.1 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.

11.3.2 Displaying the MAC Address Table

Choose Local Device > Monitor > Clients Management > 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.

Ruíjie Rcycc	Local Device(N	IBS 🗸			English 🗸 🛆 🧟 🗗
움 Home	MAC List	Static MAC Dynamic MAC	MAC Filter Aging Ti	me ARP List	
^f [□] / _J VLAN					
😤 Monitor 🔷	MAC Add	ress	Search by	MAC V Example: 00	:11:22:33:44:5 Q Search
Port Flow	Up to 32K	entries can be added.			
FORTHOW	No.	MAC	VLAN ID	Port	Туре
Clients Management	1	4A:AA:43:6A:FA:7E	1	Ag2	Dynamic
Optical Transceiver Info	2	20.70.25.50.52.45	1	Ag2	Dynamic
Ports	2	5C:/C:5F:F0.E2:4F	1	Agz	Dynamic
<u></u>	3	00:11:22:33:44:55	10		Filter
L2 Multicast	4	34:73:5A:A3:1B:B8	1	Ag2	Dynamic
🛆 L3 Multicast	5	3A:D0:86:C7:3E:8A	1	Ag2	Dynamic
L3 Interfaces ~	6	00:E0:4C:B0:4D:87	1	Ag2	Dynamic
« Collapse	7	40:B0:76:90:D9:79	1	Ag2	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.

11.3.3 Displaying Dynamic MAC Address

Choose Local Device > Monitor > Clients Management > 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 Rcycc	Local Device			English 🗸 🛆 🚔 🕞
🖧 Home	MAC List	Static MAC Dynamic MAC	MAC Filter Aging Time ARP List	
≝ [□] VLAN				
Manitar ^	MAC Lis	t	Clear by MAC \checkmark Example: 00:11:22:33:44:5	🗇 Clear C Refresh
	Na	MAG	VI AN ID	David
Port Flow	NO.	MAC	VLAN ID	Port
Clients Management	1	4A:AA:43:6A:FA:7E	1	Ag2
chents Management	2	3C:7C:3F:F0:E2:4F	1	Ag2
Optical Transceiver Info	3	34:73:5A:A3:1B:B8	1	Ag2
Ports	4	3A:D0:86:C7:3E:8A	1	Ag2
🛆 L2 Multicast	5	00:E0:4C:B0:4D:87	1	Ag2
L3 Multicast	6	40:B0:76:90:D9:79	1	Ag2
L3 Interfaces	7	04:92:26:B7:F3:0E	1	Ag2
« Collapse	8	00:11:22:33:88:9A	1	Ag2

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

11.3.4 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.

R	Local Device(NBS 🗸 C) 📓 🍐 🗗
	MAC List Static MAC Dynamic MAC MAC Filter Aging Time ARP List
쑫	Static MAC Description: The switch forwards packets based on the MAC address table. Bind a static MAC address with a port, and the packet destined for this address will be forwarded to the port. You can configure MAC address binding for a port enabled with 802.1x authentication.
\$ ₽	MAC List + Add Delete Selected
\bigcirc	Up to 256 entries can be added.
Ð	Port MAC VLAN ID Action
Q	No Data
•0- -0- •0-	Total 0 10/page \checkmark < 1 \Rightarrow Go to page 1

1. Adding Static MAC Address Entries

Choose Local Device > Monitor > Clients Management > 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.

Ruíjie Rcycc	Local Device(NBS 🗸				English 🗸 🔿	ê 🗗
Å Home	MAC List Static MAC	Dynamic MAC MAC	Filter Aging Time	ARP List		
E [□] VLAN	Static MAC					
🖞 Monitor 🔷	<i>i</i> Description: The switch this address will be forv	forwards packets based on th arded to the port. You can co	e MAC address table. Bind nfigure MAC address bind	d a static MAC address with ing for a port enabled with	a port, and the packet destined for 802.1x authentication.	r -
Port Flow	MAC List				+ Add 🗇 Delete Sele	ected
Clients Management	Up to 256 entries can be a	dded.				
Optical Transceiver Info						
Ports	Port	MA	Address	VLAN ID	Action	
L2 Multicast			No Data			
□ L3 Multicast				٦	lotal 0	
\oplus L3 Interfaces \checkmark						
«Collapse						

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

2. Deleting Static MAC Address Entries

Choose Local Device > Monitor > Clients Management > 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					Delete Selected
Up to 256 entries	can be added.				
	Port	MAC	VLAN ID		Action
	Gi28	00:11:22:33:44:55	1		Delete

11.3.5 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.

Ruíjie Rcycc	English 🗸 🛆 🤮 📑	
🖧 Home	MAC List Static MAC Dynamic MAC MAC Filter Aging T	ime ARP List
É [₽] VLAN	MAC Filter	
🖞 Monitor 🔷	Description: The switch forwards packets based on the MAC address table the packet will be discarded. You can configure the MAC filter to guard ag	e. If a packet containing the specified MAC address reaches the VLAN, ainst an ARP attack.
Port Flow	MAC List	+ Add 🗇 Delete Selected
Clients Management	lin to 256 entries can be added	
Optical Transceiver Info	op to 250 entries can be added.	
Ports	MAC Address VL	AN ID Action
 L2 Multicast 	00:11:22:33:44:55	10 Delete
L3 Multicast	< 1 > 10/page < Go to page 1	Total 1
L3 Interfaces		
« Collapse		

1. Adding Filtering MAC Address

Choose Local Device > Monitor > Clients Management > 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 Management > 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	t		+ Add	Delete Selected
Up to 256	entries can be added.			
<u>~</u>	MAC	VLAN ID	Act	tion
	00:11:22:33:44:55	1	De	lete

11.3.6 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 Management > 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.

Ruijie Rcycc	Local Device(NBS 🗸	English 🗸 🛆 🦂	ê ⊡
🖧 Home	MAC List Static MAC Dynamic MAC MAC Filter Aging Time ARP List		
^E [□] / ₂ VLAN			
🖞 Monitor 🔷	Aging Time		
Port Flow	* Aging Time (Sec): 300 Range: 10-630. 0 indicates never aging.		
Clients Management	Save		
Optical Transceiver Info			
② Ports			
 L2 Multicast 			
A L3 Multicast			
\oplus L3 Interfaces \checkmark			4
« Collapse			

11.4 Displaying ARP Information

Choose Local Device > Monitor > Clients Management > 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.

1 Note

For more ARP entry function introduction, see <u>15.6 Configuring a Static ARP Entry</u>.

R	Local Device(NBS \vee						English ~	٥		٩	₿
동 등	MAC List Static	MAC Dynamic MAC	MAC Filter	Aging Time	ARP Lis	t					
쑫	<i>i</i> ARP List Description:	The device learns IP-MAC mappi	ng of all devices	connected to its int	erfaces.						
發	ARP List					Search by IP/MAC	Q	5	Refre	sh	
	No.	IP				MAC					
\bigcirc	1	172.30.102.1	33			00:11:22:33:4	14:67				
÷	2	172.30.102.	1			00:74:9c:71:c	ld:43				
Ø	3	172.30.102.1	57			00:23:79:00:2	23:79				
-0-	4	172.30.102.1	16			00:d0:fa:15:0)9:5c				
	5	172.30.102.2	09			c0:b8:e6:e9:7	78:07				
	6	172.30.102.1	43			00:d0:f8:45:0	08:90				

11.5 IPv6 Neighbor List

In the IPv6 protocol system, the Neighbor Discovery Protocol (NDP) is an essential foundational protocol. NDP replaces the ARP and ICMP router discovery protocols used in IPv4 and supports various functions such as address resolution, neighbor state tracking, duplicate address detection, router discovery, and redirection.

Choose Local Device > L3 Interfaces > IPv6 Config > IPv6 Neighbor List.

Click Add to manually add the interface, IPv6 address, and MAC address of the neighbor.

Click Bind Selected to bind IPv6 and MAC addresses in the list to prevent ND attacks.

You can also edit, delete, batch delete and search a neighbor by its IP address or MAC address.

Ruíjie Rcycc	Local Device(NBS 🗸	English -> 🛆 🏩 🗗
Ports	IPv6 Config DHCPv6 Server DHCPv6 Clients Static DHCPv6 IPv6 Neighbor List	
 L2 Multicast L3 Multicast 	IPv6 Neighbor List Search by IP Address/MAC A Q + Add Ø Bind Selected	Delete Selected
L3 Interfaces	Up to 4000 IP-MAC bindings can be added.	
L3 Interfaces	No. MAC Address IP Address Type Ethernet status	Action
IPv4 Config	1 04:d4:c4:5c:ed:9b b Dynamic VLAN 1	
IPv6 Config	fe80::4d4:c400:15c:ee4	
\oplus Routing \checkmark		7.410
⊘ Security ~	Go to page 1	Iotal 2
Advanced V		2
« Collapse		
Ruíjie Rcycc	Local Device(NBS 🗸	English 🗸 🛆 🔮 🕞
Rcycc	Local Device(NBS \vee)	English -> 🛆 🔶 🕞
Ports CL2 Multicast	Local Device(NBS V IPv6 Config DHC Add × ist IPv6 Neighbor Ø Bind Selected	English ~ 🛆 🔮 🕞
Ports Construction Ports Construction L2 Multicast L3 Multicast L3 Interfaces	Local Device(NBS IPv6 Config DHC Add × ist IPv6 Neighbor • Interface Select · ·	English ~ 🛆 🔮 🕞
Ports Ports L2 Multicast L3 Multicast L3 Interfaces L3 Interfaces	Local Device(NBS IPv6 Config DHC Add × ist @ Bind Selected * Interface Select * IPv6 Address Please enter an IPv6 address. Ethernet status	English V 🛆 🏩 🕞
Ports × 12 Multicast × 13 Multicast × 13 Interfaces × IPv4 Config ×	IPv6 Config DHc Add × ist IPv6 Neighbor * Interface Select ✓ Up to 4000 IP-MA * IPv6 Address Please enter an IPv6 address. Ethernet status No. * MAC Address Please enter a MAC address. VLAN 1	English > A A F
Ports > L2 Multicast	IPv6 Config DHc Add × ist IPv6 Neighbor • Interface Select ✓ Up to 4000 IP-MA • IPv6 Address Please enter an IPv6 address. Ethernet status No. • MAC Address Please enter a MAC address. VLAN 1	English ~ A A T
Ruffie Rcycc Ports × L2 Multicast L3 Multicast L3 Interfaces IPv4 Config IPv6 Config Routing ×	IPv6 Config DHc Add × ist IPv6 Neighbor • Interface Select ✓ Up to 4000 IP-MA • IPv6 Address Please enter an IPv6 address. Ethernet status No. • MAC Address Please enter a MAC address. VLAN 1 2 04 Cancel OK VLAN 1	English > A A T
Ruffie Rcycc Ports × L2 Multicast L3 Multicast L3 Interfaces IPv4 Config IPv6 Config Routing × Routing × Security ×	IPv6 Config DHc Add int IPv6 Neighbor • Interface Select • Bind Selected Up to 4000 IP-Ma • IPv6 Address Please enter an IPv6 address. Ethernet status No. • MAC Address Please enter a MAC address. VLAN 1 2 04 Cancel OK VLAN 1	English > A A Cion Delete Selected Action Bind Bind Bind Total 2
Ruffie Rcycc Ports × L2 Multicast L3 Multicast L3 Interfaces IPv4 Config IPv6 Config × Routing × Security × Advanced ×	IPv6 Config DHc Add ist IPv6 Neighbor • Interface Select • Bind Selected Up to 4000 IP-Ma • IPv6 Address Please enter an IPv6 address. Ethernet status No. • MAC Address Please enter a MAC address. VLAN 1 2 04 Cancel OK 1 10/page × Go to page 1 Interface	English <

11.6 VLAN

11.6.1 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.

11.6.2 Creating a VLAN

Choose Local Device > VLAN > VLAN List.

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

VLAN L	ist 😑		+ Batch Add +	- Add 🗇 Delete Selected
Up to 4 deleted.)	094 entries can be added.(The d	efault VLAN, management VLAN, Native VI	LAN, SVI VLAN, MVR VLAN, Voice VLAN	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 🗸 🤇 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 Lis	t 😑		+ Batch Add + /	Add Delete Selected
Up to 409 deleted.)	4 entries can be added.(Th	e default VI AN management VI AN Batch Add	Native VLAN, SVI VLAN, MIVR VLAN, Voice VLAN ar	d Access VLAN cannot be
	VLAN ID ≑	Example: 3-5 and 20.		Action
	1		Cancel	Edit Delete
	10	VEXINOUTO		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 entries can be added	a _			be deleted.)
ULAN ID	* VLAN ID:	Range: 1-4094	e: 1-4094	Action
. 1	Description:	Description Max: 3	32 characters.	Edit Delete
. 10		Cancel	ОК	Edit Delete
20		VLANUUZU		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 entrie	s can be added.(T					be deleted.)	
		* VLAN ID:	10	Ra	ange: 1-4094		
	VLAN ID 🗢					Action	
	1	Description:	VLAN0010	M	ax: 32 characters.	Edit Delete	
	10			Canc	el OK	Edit Delete	
	20		VEANOUZU			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 🗇 Delete Selected
Up to 409	94 entries can be added.(The defa	ult VLAN, management VLAN, Native VLAN, SV	/I VLAN, MVR VLAN, Voice VLAN and Acce	ess 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 List			+ Batch Add +	Add 🗇 Delete Selected
Up to 4094 er	ntries can be added.(<mark>The de</mark>	fault VLAN, management VLAN, Native VLAN, SVI	VLAN, MVR VLAN, Voice VLAN and Access	VLAN cannot be deleted.)
	VLAN ID \$	Description	Port	Action
	1	VLAN0001	Gi1-28	Edit Delete
	10	VLAN0010		Edit Delete

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.

11.6.3 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>11.6.2</u> <u>Creating</u> <u>a VLAN</u>) and then configure the port based on the VLANs.

Port List 😑						🖉 Batch Edit
The Permit VLAN of If the Voice VLAN a	f a hybrid port includes b utomatic mode is enable	ooth the tagged VLAN ar d on the port, the Voice	nd untagged VLAN. VLAN will be removed	from the Permit VLAN.		
Port	Port Mode	Access VLAN	Native VLAN	Permit VLAN	Untag VLAN	Action
Gi1 🕇	ACCESS	1				Edit
Gi2	ACCESS	1				Edit
Gi3	ACCESS	1				Edit
Gi4	ACCESS	1				Edit
Gi5	ACCESS	1				Edit

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

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. 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 Untagged VLAN. The frames forwarded by the hybrid port from a Tag VLAN carry tags, and the frames forwarded by the hybrid port from an Untagged 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 Untagged VLAN List.

Table 11-1 Port Modes Description

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 Untagged VLAN range. Click **OK** to complete the batch configuration.

Note

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

Port List	Batch Edit ×	∠ Batch Edit
The Permit VLAN of If the Voice VLAN	Port Mode: Access Port	
Port	* Access VLAN: 1 ~	Action
Gi1 🕇	* Select Port:	Edit
Gi2	Available Unavailable Aggregate 🕇 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 1	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 of 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.

11.6.4 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**.

Please select a target device.: Select All Deselect	ALL		
	ALL		
ruijie Ruijie	RG-ES205C-P		
RG-ES205C-P NBS5200-24SFP/8GT4XS	NBS5200-24SFP/8GT4XS		
MACCWLD789205GC G1NW31N000172			
RG-ES205C-P (1)			
Note: You can click and drag to select one or more ports.	elect All Inverse Deselect		
NBS5200-24SFP/8GT4XS (1)			
1 3 5 7 9 11 13 15 17 19 21 23 17 19 21 23			
Note: You can click and drag to select one or more ports.	elect All Inverse Deselect		
	Next		

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

+Add VLAN +Batch Add			
LAN ID Remark	VLAN ID Remark		
1 Default VLAN	12	Ū	

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

Port			
Selected Port	RG-ES205C-P:; NBS5200)-24SFP/8GT4XS: Gi21-Gi22;	
Туре	Trunk Port \vee		
* Native VLAN	Default VLAN \vee		
Permitted VLAN	1,12		
Previous			Override

11.6.5 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/8 SN:G1NW31N000172	BGT4XS	Software Ver:ReyeeOS 1.86 MGMT IP:10.44.78.1 MAC: 00:d3:f8:15:08:5b	5.1619
Port Status VLAN Info	VLAN			Edit 💿
Route Info RLDP	VLAN1 VLAN12 Interface Gi17,Gi21-22,Te27	IP	IP Range	Remark
More				23 ••• •••
	2 4 6 8 10	12 14 16 18 2	20 22 24 18 20 22	24 25 26 27

11.7 Viewing Optical Transceiver Info

Choose Local Device > Monitoring > Optical Transceiver Info.

The **Optical Transceiver Info** page displays the basic information of an optical transceiver, including the port to which it is connected, DDM, temperature, voltage, current, Tx power, local Rx power, and so on.

You can query the information of an optical transceiver by entering the port to which it is connected in the search box.

The data on this page is automatically updated every 5 seconds. You can also click **Refresh** to refresh the optical transceiver information.

Optical Transcei	ver Info												Search	h by Port		All		C Refresh
Port	DDM	Temperatu re("C)	Voltage (V)	Current (mA)	Tx power(dB m)	Local Rx Power(dB m)	Vendor	Vendor Oui	Vendor P/N	Vendor Revision Number	Transceiver SN	Date of Manufactu re	Decoding Mode	Transceiver Type	Conne Typ	ector pe	Wavelengt h(nm)	Max Transmissi on Range(m)

12 NBS and NIS Series Switches Port Management

12.1 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>15.1</u> <u>Setting an L3 Interface</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>15.1</u> <u>Setting an L3 Interface</u>

Table 12-1 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>15.1</u> <u>Setting an L3 Interface</u>

12.2 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, port media type and MTU, etc.

12.2.1 Basic Settings

Choose Local Device > Ports > Port 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 Reyce	Local Device(NBS \sim					Eng	lish -> 🛆 🖕	⋳
ి Home	Basic Settings Ph	ysical Settings						
걁 VLAN 쭏 Monitor ~	<i>Port Settings</i> Configure port	status, duplex mode	, rate and flow control.					
Ports ^	Port List						🖉 Batch Edit	
Port Settings			Duplex N	lode/Rate	Flow C	ontrol		
Aggregate Ports	Port	Status	Config Status	Actual Status	Config Status	Actual Status	Action	
Port Mirroring	Gi1/1/1 †			Member po	ort of Ag2.			
Rate Limiting	Gi1/1/2	Enable	Auto/Auto	Unknown/Unkno wn	Disable	Disable	Edit	
MGMT IP	Gi1/1/3			Member po	ort of Ag1.			
Out-of-Band IP	Gi1/1/4	Disable	Auto/Auto	Unknown/Unkno wn	Disable	Disable	Edit	4

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	~	
Rate:	Auto	~	
Work Mode:	Auto	~	
Flow Control:	Disable	~	
* Select Port:	available	Aggregate Uplink	Copper Fiber
1 3 5 7	9 11 13	3 15 17 19 21 23 17 19 21	23
2 4 6 8	10 12 14	4 16 18 20 22 24 18 20 22	24 25 26
	drag to select		Inverse Descrect
		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 po	ort of Ag4.		
Gi2	Port:Gi2			×	Edit
Gi3	Status:	Enable	~		Edit
Gi4	Rate:	Auto	~		Edit
Gi5	Work Mode:	Auto	\sim		Edit
Gi6	Flow Control:	Disable	~		Edit
Gi7					
Gi8			Cancel OK		

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, but the PoE power supply function of the port will not be affected.	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

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.

12.2.2 Physical Settings

Choose Local Device > Ports > Port Settings > Physical Settings.

On this page, you can enable the energy-efficient Ethernet (EEE) function, and set the media type and MTU on the port.

Note

 Maximum Transmission Unit (MTU) is used to notify the peer of the acceptable maximum size of a data service unit. It indicates the size of the payload acceptable to the sender. You can configure the MTU of a port to limit the length of a frame that can be received or forwarded through this port. The default value for MTU is 1500 bytes.

• MTU is configured globally.

Ruíjie Rcycc	Local Device(NBS >>				English ∽ Remote O&M →	✿ Network Configuration ☐ Log Out
ം Home	Basic Settings Physical Settings					
dr VLAN	- Dhysical Settings					
🔄 Monitor	Configure physical attribute. (T	ne fiber port does not support l	EEE. The aggregate port containing co	ombo ports cannot work as a com	bo port.)	
🛞 Ports 🔷	Port List					🖉 Batch Edit
Port Settings	Port	EEE	Attribute	Description	MTU	Action
Aggregate Ports	Gi1/1/1 †			Member port of Ag2.		
Port Mirroring	Gi1/1/2	Disable	Copper		1500	Edit
Rate Limiting	Gi1/1/3			Member port of Ag1.		
MGMT IP	Gi1/1/4	Disable	Copper		1500	Edit
Out-of-Band IP	Gi1/1/5	Disable	Copper		1500	Edit
L2 Multicast	Gi1/1/6	Disable	Copper		1500	Edit
L3 Multicast	Gi1/1/7			Member port of Ag2.		
⊕ L3 Interfaces ∨	Gi1/1/8			Member port of Ag2.		4
«Collapse	Gi1/1/9			Member port of Aa2		

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**.

1 Note

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

Batch Edit		×
EEE:	Disable	
Attribute:	Copper ~	
Description:		
* MTU:	1500	Range: 64-9216
* Select Port:	Aggregate 📭 Uplink 💼 Copper	Fiber
M7000-24GT2XS-EA/1234942 1 3 5 7 9 11 1 5 7 9 11 1 5 7 9 11 1 5 7 9 11	570068 Online 13 15 17 19 21 23	(e) <u>M</u>
2 4 6 6 10 12	Sorry, the board is offline.	2
3 💿	Sorry, the board is offline.	6 3
Note: You can click and drag to select or	e or more ports.	Select All Inverse Deselect
		Cancel OK

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**.

Port:Gi1/1/2			×
EEE:	Disable		
Attribute:	Copper ~		
Description:			
* MTU:	1500	Range: 64-9216	
			_
		Cancel OK	

Table 4-3 Description of Physical Configuration Parameters

Paramete r	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

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.

12.3 Aggregate Ports

12.3.1 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.

12.3.2 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

12.3.3 Aggregate Port Configuration

Choose Local Device > Ports > Aggregate Ports > Aggregate Port Settings.

Ruíjie Rcycc	Local Device(NBS V	English ~	0	e E	}
😤 Home	Aggregate Port Settings LACP Settings LACP Details				
음 ^프 VLAN					
쭏 Monitor 🗸	Global Settings				
😨 Ports 🔷	Load Balance Algorithm: Src & Dest MAC				
Port Settings	Save				
Aggregate Ports					
Port Mirroring	Aggregate Port Settings				
Rate Limiting	Up to 16 aggregate ports can be added. An aggregate port contains up to 8 member ports.				
MGMT IP	Select All				
Out-of-Band IP	Ag2 Ag1 Delete Selected				(. 4 i
«Collapse					

1. Adding a Static Aggregate Port

Enter an aggregate port ID, select member ports (ports that have been added to an aggregate port cannot be selected), and click **Save**. The port panel displays a 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.	
Select All	
X X Ag2 Ag1 Delete Selected	
* Aggregate Port: 6	
* Select Member Ports	
Available Unavailable Aggregate 1 Uplink Copper Fiber	
M7000-24GT2XS-EA/12349427.558 Online 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	
2 Sorry, the board is offline.	
3 Sorry, the board is offline.	
Note: You can click and drag to select one or more ports.	Select All Inverse Deselect
Save	

2. 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.

1 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 X X X Ag2 Ag1 Ag6	
* Aggregate Port: 1 LACP ⑦	
* Select Member Ports	
Available Unavailable Aggregate 🗈 Uplink 💼 Copper 🔛 Fiber	
M7000-24GT2XS-EA/1234942570068 Online 1 3 5 7 9 11 13 15 17 19 21 23 M 2 4 6 8 10 12 14 16 18 20 22 24 25 26 M	
2 Sorry, the board is offline.	
3 Sorry, the board is offline.	
Note: You can click and drag to select one or more ports. Save Cancel	Select All Inverse Deselect

3. 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.

A Caution

After an aggregate port is deleted, its member ports are restored to the default settings and are disabled.

Aggregate Port Settings					
Up to 16 ag	igregate ports can b	be added. An ag	ggregate port contains up to 8 member ports.		
Select All					
Ag2	× Ag1	× Ag6	Delete Selected		

12.3.4 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	

12.4 Port Mirroring

12.4.1 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 12-1 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.

12.4.2 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

Port Mirroring

- 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.

 Description: All packets on the source port will be copied to the destination port and you can analyze the traffic by using a protocol analyzer application. Traffic on more than one source port can be mirrored to one destination port. Note: The destination port must be different from the source port. 								
Port M	Port Mirroring List							
#	Src Port	Dest Port	Monitor Direction	Receive Pkt from Non-Src Ports	Action			
1					Edit Delete			
2					Edit Delete			
3					Edit Delete			
4					Edit Delete			

Edit ×
Monitor Direction: Both \lor
Receive Pkt from Non-Src Ports:
* Src 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
Note: You can click and drag to select one or more ports. Select All Inverse Deselect * Dest Port:
Available Unavailable
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

Table 4-4 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

12.5 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 E	dit 🗇 Delete Selected
	Port	Rx Rate (kbps)	Tx Rate (kbps)	Action
	Gi23	10000	10000	Edit Delete
Total 1 10/p	age 🗸 🔇 1	> 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	vailable Aggregate	Uplink Copper Fiber
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
Note: You can click and	drag to select one or more ports.	Select All Inverse Deselect
		Cancel OK

Table 1 C	Deceription			
Table 4-5	Description	or 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**.

×
Range: 16-100000kbps
Range: 16-100000kbps
Cancel

3. Deleting Rate Limiting

Batch configure: Select multiple records in **Port List**, click **Delete Selected** and click **OK** in the confirmation dialog box.

Configure one port: In **Port List**, click **Delete** on the corresponding port entry, and click **OK** in the confirmation dialog box.

Port List		🖉 Batch	Edit 📋 Delete Selected
Port	Rx Rate (kbps)	Tx Rate (kbps)	Action
Gi23	10000	10000	Edit Delete

Note

- When configuring rate limits for a port, you must configure at least the ingress rate or egress rate.
- When the ingress rate or egress rate is not set, the port rate is not limited.

12.6 MGMT IP Configuration

12.6.1 Configuring the Management IPv4 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.

R Local Device(N	BS V Currently in Local Device mode.	English ~	△ 🏾 🗗
• NBS6002 s Home VLAN M Diagnostics ~ Sys	Hostname: Ruijie SN: MACCNBS6000HQ IP Address: 192.168.110.62 MAC Address: 00:D0:F8:95:68:5E Software Ver: ReyeeOS 1.218.2421 Hardware Ver: 1.00 DNS: 192.168.110.1 Ionitor \checkmark Ports \checkmark L2 Multicast L3 Interfaces \checkmark Routing \checkmark Security \checkmark stem \checkmark	Advanced	(¹) Reboot
MGMT IP MGMT	IPv6		
<i>MGMT IP</i> Configure netwo	ork settings.		0
Internet:	DHCP ~		
VLAN:			
IP Address:	192.168.110.62		
Subnet Mask:	255.255.255.0		
Gateway:	192.168.110.1		
DNS Server:	192.168.110.1		
	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 take effect.

1 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>11.6.2 Creating a VLAN</u>).
- You are advised to bind a configured management VLAN to an uplink port. Otherwise, you may fail to
 access the Eweb management system.

12.6.2 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.

R Local Device(NE	S V Currently in Local Device mode.	English -> 🛆 🌸 🗗
• NBS6002 s Home VLAN Mo Diagnostics ~ Syst	Hostname: Ruijie SN: MACCNBS6000HQ IP Address: 192.168.110.62 MAC Address: 00:D0:F8:95:68:5E oftware Ver: ReyeeOS 1.218.2421 Hardware Ver: 1.00 DNS: 192.168.110.1 Initor Y Ports Y L2 Multicast L3 Interfaces Y Routing Y Security Y tem Y	() Reboot Advanced ~
MGMT IP MGMT I	2v6	
* Internet	Null ~	
IPv6 Address		
IPv6 Prefix		
Gateway		
DNS Server		
	Save	

R Local Device(NB	S < Currently in Local Device mode.	English 🗸 🖌) 🌸 🗗
Switch • NBS6002 So Home VLAN Mo Diagnostics ~ Syst	Hostname: Ruijie SN: MACCNBS6000HQ IP Address: 192.168.110.62 MAC Address: 00:D0:F8:95:68:5E oftware Ver: ReyeeOS 1.218.2421 Hardware Ver: 1.00 DNS: 192.168.110.1 unitor \checkmark Ports \checkmark L2 Multicast L3 Interfaces \checkmark Routing \checkmark Security \checkmark em \checkmark	C Advanced ~) Reboot
MGMT IP MGMT II	246		
* Internet	Null		
IPv6 Address	DHCP		
IPv6 Prefix	Static IP Null		
Gateway			
DNS Server			
	Save		

12.7 Out-of-Band IP Configuration

A Caution

Only the RG-NBS6002 Series, RG-NBS7003 Series and RG-NBS7006 Series support this function.

Choose Local Device > Ports > Out-of-Band IP.

Set the MGMT management port IP of the chassis to centrally manage the modules in multiple slots of the device.

Currently in Local Device mode.	English 🗸 🛆 🛕 📑
Image: Switch Switch Switch Structure Hostname: Ruijie SN: MACCNBS6000HQ IP Address: 192.168.110.62 MAC Address: 00:D0:F8:95:68:5E Software Ver: ReyeeOS 1.218.2421 Hardware Ver: 1.00 DNS Home VLAN Monitor \checkmark Ports \checkmark L2 Multicast L3 Interfaces \checkmark Routing \checkmark Diagnostics \checkmark System \checkmark	() Reboot 5: 192.168.110.1 Security × Advanced ×
i Out-of-Band IP	
IPV4 IPV6	
IP Address: Example: 1.1.1.1	
Subnet Mask: 255.255.255.0	
Save	
Currently in Local Device mode.	English ~ 🛆 🔮
Hostname: Ruijie SN: MACCNBS6000HQ IP Address: 192.168.110.62 MAC Address: 00:D0:F8:95:68:5E NBS6002 Software Ver: ReyeeOS 1.218.2421 Hardware Ver: 1.00	() Reboot DNS: 192.168.110.1
Home VLAN Monitor × Ports × L2 Multicast L3 Interfaces × Routi Diagnostics × System ×	ng \checkmark Security \checkmark Advanced \checkmark
i Out-of-Band IP	
IPV4 IPV6	
IPv6 Address/Prefix Length: Example: 2000::1	0
Sava	
save	

1 Note

No IP address is configured for the MGMT port by default. Currently, only a static IP address can be configured for the MGMT port but DHCP is not supported.

12.8 PoE Configuration

A Caution

Only PoE switches (The device models are marked with -P) support this function.

Choose Local Device > Ports > PoE.

The device supplies power to PoE powered devices through ports. Users can view the current power supply status, and set the system power supply and port power supply policies respectively to achieve flexible power distribution.

R	Local Device(NBS 🗸						English ~	
	PoE Overview							
뙆 않	Total Transr 370	nit Power W	Used Transmit <mark>0</mark> w	Power	Reserved Trans <mark>0</mark> w	smit Power	Free Transr 370	nit Power W
0	Peak Transr <mark>0</mark> w	nit Power /	Powered Po 0	rts				
Ē	PoE Settings							
-0-	Transmit Power Mode:	Energy Saving						
	* Reserved Transmit Power:	0 Save	Range:	0-50%				
	Port List						C Refresh	🖉 Batch Edit
	Port	PoE Status	Transmit Power Status	Priority	Current Transmit Power (W)	Non-Standard	Work Status	Action
>>	> Gi1	Enable	Off	Low	0	No	PD Disconnected	Edit Repower

12.8.1 Viewing Global PoE Info

Choose Local Device > Ports > PoE > PoE Overview.

The **PoE Overview** page displays global PoE power supply, including total power, used power, reserved power, free power, peak power, and powered ports.

PoE Overview							
60w Total	Used Power Ow Reserved Power Ow Free Power 60w	Input Voltage ⊚ 11 v	Used Power O W	Reserved Power O w	Free Power 60w	Peak Power O w	Powered Ports 0

12.8.2 PoE Global Settings

Choose Local Device > Ports > PoE > PoE Settings.

PoE Transmit Power Mode refers to the way that a device allocates power to a connected PD (Powered Device). It supports Auto mode and Energy-saving mode.

In Auto mode, the system allocates power based on the classes of PDs detected on ports. The device allocates power to PD devices of Class 0~4 based on a fixed value: Class 0 is 15.4W, Class 1 is 4W, Class 2 is 7W, Class 3 is 15.4W, Class 4 Type 1 is 15.4W, and Class 4 Type 2 is 30W. In this mode, if the port is connected to a device of Class 3, even if the actual power consumption is only 11W, the PoE power supply device will allocate power to the port based on the power of 15.4W.

In energy-saving mode, the PoE device dynamically adjusts allocated power based on actual consumption of PDs. In this mode, in order to prevent the power supply of the port from fluctuating due to the fluctuation of the actual power consumption of the PD when the power is fully loaded, you can set the Reserved Transmit Power, and the reserved power will not be used for power supply, so as to ensure that the total power consumed by the current system does not exceed the limit of the PoE device. The size of the reserved power is expressed as a percentage of the total PoE power. The value ranges from 0 to 50.

PoE watchdog: By enabling **PoE watchdog**, you can monitor the status of connected PDs. When the Powered Device (PD) does not respond or ceases to function properly, the PoE watchdog feature automatically restarts the PoE function of the port to restore the PD's operation.

PoE Settings

Power Mode:	Energy Saving	~	0
* Reserved Power:	0		Range: 0-50%
PoE watchdog:			
	Save		

12.8.3 Power Supply Configuration of Ports

Choose Local Device > Ports > PoE > Port List.

Click Edit in the port entry or click Batch Edit to set the PoE power supply function of the port.

Port Lis	st						Q Refresh	🖉 Batch Edit
	Port	PoE Status	Transmit Power Status	Priority	Current Transmit Power (W)	Non-Standard	Work Status	Action
>	Gi1	Enable	Off	Low	0	No	PD Disconnected	Edit Repower
>	Gi2	Enable	Off	Low	0	No	PD Disconnected	Edit Repower
>	Gi3	Enable	Off	Low	0	No	PD Disconnected	Edit Repower
>	Gi4	Enable	Off	Low	0	No	PD Disconnected	Edit Repower

Port:Gi1		×
PoE:	Enable	~
Non-Standard:	Disable	~
Priority:	Low	~
Max Transmit Power:	A blank value indicates no limit.	Range: 0-30W
		Cancel OK

Table 4-6 Description of Parameters for Power Supply Configuration of Ports

Parameter	Description	Default Value
PoE	Whether to enable the power supply function on the ports	Enable
Non- Standard	By default, the device only supplies power to PDs that comply with the standard IEEE 802.3af and 802.3at protocols. In practical applications, there may be PDs that do not conform to the standard. After the non-standard mode is enabled, the device port can supply power to some non-standard PD devices.	Disable
Priority	The power supply priority of the port is divided into three levels: High, Medium, and Low In auto and energy-saving modes, ports with high priorities are powered first. When the system power of the PoE device is insufficient, ports with low priorities are powered off first. Ports with the same priority are sorted by the port number. A smaller port number indicates a higher priority.	Low

Parameter	Description	Default Value
Max Transmit Power	The maximum power that the port can transmit, ranging from 0 to 30, in watts (W). A blank value indicates no limit	Not limit

12.8.4 **Displaying the Port PoE Information**

Choose Local Device > PoE > Port List.

The **Port List** displays the PoE configuration and status information of each port. Click to expand the detailed information.

When the PD device connected to the port needs to be restarted, for example, when the AP connected to the port is abnormal, you can click **Repower** to make the port power off briefly and then power on again to restart the device connected to the power supply port.

Port	List						C Refresh	🖉 Batch Edit
	Port	PoE Status	Transmit Power Status	Priority	Current Transmit Power (W)	Non-Standard	Work Status	Action
\sim	Gi1	Enable	Off	Low	0	No	PD Disconnected	Edit Repower
	Current: OmA Max Transmit Power: 2D Type: Failed to fe	No Limit etch the PD type.	Voltage: 0\ PD Request PD Class: N	/ ed Transmit Power: IA	0W	Avg Transmit Powe PSE Allocated Trans	r: 0W smit Power: 0W	
>	Gi2	Enable	Off	Low	0	No	PD Disconnected	Edit Repower
>	Gi3	Enable	Off	Low	0	No	PD Disconnected	Edit Repower

Table 4-7	Description	of Port	Power	Supply	Info
	Description		1 0 10 1	Ouppiy	millo

Field	Description
Port	Device Port ID
PoE Status	Whether to enable the PoE function on the ports.
Transmit Power Status	Whether the port supplies power for Pds currently.
Priority	The power supply priority of the port is divided into three levels: High, Medium, and Low.

Field	Description
Current Transmit Power	Indicates the power output by the current port, in watts (W).
Non-Standard	Indicates whether the non-standard compatibility mode is enabled.
Work Status	Current work status of PoE ports.
Current	Indicates the present current of the port in milliamps (mA).
Voltage	Indicates the present current of the port in volts (V).
Avg Transmit Power	Indicates the current average power of the port, namely, the sampling average of current power after the port is powered on, in watts (W).
Max Transmit Power	The maximum output power of the port in watts (W).
PD Requested Transmit Power	The power requested by the PD to the PSE (Power Sourcing Equipment, power supply equipment), in watts (W).
PSE Allocated Transmit Power	Indicates the power allocated to a PD by PSE in watts (W).
РD Туре	Information of PD type obtained through LLDP classification are divided into Type 1 and Type 2.
PD Class	The classification level of the PD connected to the port is divided into Class 0~4, based on the IEEE 802.3af/802.3at standard.
13 NBS and NIS Series Switches L2 Multicast

13.1 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.

13.2 Multicast Global Settings

Choose Local Device > L2 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.

Ruijie Rcycc	Local Device(NBS 🗸	English \sim	0	ê 🗗
🖧 Home	Global Settings IGMP Snooping MVR Multicast Group IGMP Filter Querier			
EP VLAN				
至 Monitor ~	() Global Settings			
Ports	Version IGMPv2 ~			
L2 Multicast	IGMP Report Suppression			
L3 Multicast	Unknown Multicast Pkt \Box Discard \sim			
⊕ L3 Interfaces ∨	Save			
Routing ` ` ` `				
Security 🗸				
🗄 Advanced 🗸 🗸				
« Collapse				

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 5-1 Description of Configuration Parameters of Global Multicast

13.3 IGMP Snooping

13.3.1 **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.

Reyee Cookbook

Ruíjie Rcycc	Local Device(NBS						English	~ 🛆 🏩	G
Home	Global Settings	IGMP Snooping	MVR	Multicast Group	IGMP Filter	Querier			
^f ≘ ^p VLAN	iGMP Snoo	ping							- 1
또 Monitor 🗸									- 1
Ports	IGMP Snoopi	ng							
L2 Multicast		Save							
L3 Multicast									. 1
L3 Interfaces	VLAN List								
\oplus Routing \checkmark	VLAN ID	Multicast Status	Dynamic Learning	Router Port	Fast Leave	Router Aging Time (Sec)	Host Aging Time (Sec)	Action	
⊘ Security ~	1	Disable	Enable		Disable	300	260	Edit	
🗄 Advanced 🗸 🗸	10	Disable	Enable		Disable	300	260	Edit	Ai
« Collapse									

13.3.2 Enabling Global IGMP Snooping

Choose Local Device > L2 Multicast > IGMP Snooping.

Turn on IGMP Snooping and click Save.

Global Settings	IGMP Snooping	MVR	Multicast Group	IGMP Filter	Querier
iGMP Snoo	oping				
IGMP Snoop	ing 🚺				
	Save				

13.3.3 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 > L2 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**.

۷	LAN 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:	
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 drag to select one or more ports. Select All Inverse Deselect	
Cancel	DK

Table 5-2 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

Parameter	Description	Default Value
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
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

13.4 Configuring MVR

13.4.1 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.

Global Settings	IGMP Snooping	MVR M	Multicast Group	IGMP Filter	Querier		
<i>MVR</i> The source Fast Leave	e port must be a MVR VLA settings only take effect (N member an on the destinat	d the receiver port ca tion port.	nnot be a MVR VI	AN member.		
	MVR						
	Save						
Port List							🖉 Batch Edit
Port							
		R	ole			Fast Leave	
Gi1 1	NC	R DNE	Role ~			Fast Leave	
Gi1 🕇		R DNE DNE	tole ~			Fast Leave	
Gi1 t Gi2			kole ~			Fast Leave	

13.4.2 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.

Reyee Cookbo	ook			NBS	S and NIS Series Sv	vitches L2 Multicast
Glob	al Settings	IGMP Snooping	MVR	Multicast Grou	p IGMP Filter	Querier
6	MVR The source p Fast Leave se	ort must be a MVR VL ettings only take effect	.AN membe t on the des	r and the receiver p tination port.	oort cannot be a MV	R VLAN member.
	M	VR				
	* Multicast VL/	AN VLAN0001		~		
	* Start IP Addre	ess			0	
	* End IP Addre	ess			0	
		Save				

Table 5-3 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

13.4.3 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**.

Batch Edit		×
Role NONE	~	
Fast Leave		
Select Port		
Available 💼 Unavailable	Aggregate 🚺 Uplink 💼 Copper 🚺 Fiber	
1 3 5 7 9 11	13 15 17 19 21 23	

2 4 6 8 10 12	14 16 18 20 22 24 25 26 27 28	
Note: You can click and drag to s	select one or more ports. Select All Inverse Deselect	
	Cancel 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 5-4 Description of MVR Configuration Parameters of Ports

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

Parameter	Description	Default Value
Fast Leave	Configures the fast leave function for a port. After the function is enabled, if the port receives the leave packet, it is directly deleted from the multicast group.	Disable

Note

- If a source port or a receiver port is configured, the source port must belong to the MVR VLAN and the receiver port must not belong to the MVR VLAN.
- The fast leave function takes effect only on the receiver port.

13.5 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.

Global Settings	IGMP Snooping	MVR	Multicast Group	IGMP Filter	Querier		
<i>i</i> Multicast The static	: Group multicast group will not	t learn dynamic	ports.				
Multicast Li	st	VLAN	1 ID	~		Q + Add	Delete Selected
Up to 256 en	tries can be added.						
. V	LAN ID Mu	lticast IP Add	ress Proto	ocol	Туре	Forwarding Port	Action
	20	224.10.10.10	IGMP Sn	ooping	Static	Gi28	Edit Delete

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	Cancel OK	

Table 5-5	Description of Multicast Group	Configuration Parameters

Parameter	Description	Default Value
VLAN ID	VLAN, to which received multicast traffic belongs	NA
Multicast IP Address	On-demand multicast IP address	NA
Protocol	If the VLAN ID is a multicast VLAN and the multicast address is within the multicast IP address range of the MVR, the protocol is MVR. In other cases, the protocol is IGMP snooping.	NA
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

Parameter	Description	Default Value
Forwarding Port	List of ports that forward multicast traffic	NA

1 Note

Static multicast groups cannot learn other dynamic forwarding ports.

13.6 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.

Global Settings	IGMP Snooping	MVR N	Multicast Group	IGMP Filter	Querier		
iGMP Filte	er						
Profile List						+ Add	i Delete Selected
Profile	ID Be	havior	Start IP	Address	End IP Address		Action
				No Data			
Total 0 10/pag	e ~ 1	> Go to p	page 1				
Filter List							🖉 Batch Edit
	Port		Profile ID		Max Multicast Groups		Action
	Gi1 🕇				256		Edit
	Gi2				256		Edit
	Gi3				256		Edit

13.6.1 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
		Cancel

Table 5-6 Description of Profile Configuration Parameters

Parameter	Description	Default Value
Profile ID	Profile ID	NA
Behavior	DENY : Forbids demanding multicast IP addresses in a specified range. PERMIT : Only allows demanding multicast IP addresses in a specified range.	NA
Start IP Address	Start Multicast IP address of the range of multicast group addresses	NA
End IP Address	End Multicast IP address of the range of multicast group addresses	NA

13.6.2 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		Х
Profile ID	Unbound \lor	
* Max Multicast Groups	256	
Select Port		
Available 💼 Unavai	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 OK

Table 5-7	Description	of Port Fi	ilter Configurat	ion Parameters
			men eenigenen	

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

Parameter	Description	Default Value
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

13.7 Setting an IGMP Querier

13.7.1 **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.

13.7.2 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**.

Global	Settings	IGMP Snooping	MVR	Multicast Group	IGMP Filter	Querier		
1	Querier The querier If the querier	version cannot be high r source IP is not confiç	er than the g gured, the de	global version. When the evice management IP is	e global version is lo used.	owered, the querier	version will be reduced accord	ingly.
Que	erier List							
	VLAN ID	Querie	r Status	Version	Src I	P Address	Query Interval (Sec)	Action
	1	Dis	able	IGMPv2			60	Edit
	10	Dis	able	IGMPv2			60	Edit
	20	Dis	able	IGMPv2			60	Edit

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

Table 5-8 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.

14 NBS and NIS Series Switches L3 Multicast

14.1 Overview

Layer 3 multicast is a communication method that uses multicast addressing at the network layer for sending data. Multicast enables a sender to send packets to a group of receivers simultaneously, which reduces the network bandwidth consumption and lowers the network load. Layer 3 multicast is extensively used in applications such as video conferencing, streaming media, VoIP, and others.

In Layer 3 multicast, each multicast group address corresponds to a specific multicast group, and the members of a multicast group share the same multicast group address. The sender sends data packets to the multicast group address, and routers on the network forward the packets to all members of the multicast group based on the multicast group address and the routing protocols used.

14.2 Multicast Routing Table

Choose Local Device > L3 Multicast > Multicast Routing Table.

The **Multicast Routing Table** page displays the information of the Layer 3 multicast routing table, including the source IP address, multicast group address, incoming interface, outgoing interface, and time to live (TTL). You can search the routing information based on either the source IP address or the multicast group address. You can click **Refresh** to view the up-to-date multicast routing table information.

Multicast Routing Table PIM RF	P BSR IGMP				
Multicast Routing Table				Enter source IP address or multicast group address Q	Refresh
Source IP Address	Multicast Group Address	Incoming Interface	Outgoing Interface	TTL	
		No Data			
< 1 > 10/page > G	o to page 1				Total 0

Parameter	Description	Default Value
Source IP Address	IP address of the source device sending the multicast packet.	N/A
Multicast Group Address	A special IP address that identifies a multicast group. In the routing table, the multicast group address is the IP address of the destination multicast group.	N/A
Incoming Interface	Interface receiving the multicast packets	N/A
Outgoing Interface	When the router receives a multicast packet, it forwards the multicast packet to the appropriate outgoing interface according to the value in the Outgoing Interface field in the routing table.	N/A

 Table 14-1
 Description of Multicast Routing Table Parameters

Parameter	Description	Default Value
TTL	The TTL value is the duration for which a routing table entry remains valid. Once this time expires, the routing table entry is considered expired and is no longer utilized.	N/A

14.3 Configuring PIM

14.3.1 **Overview**

Protocol Independent Multicast (PIM) is a protocol-independent intra-domain multicast routing protocol. PIM allows multicast communication to be implemented using various unicast routing protocols, including static routing, RIP, OSPF, and others. Through the implementation of the PIM protocol, routers can exchange multicast routing information, which enables the establishment and maintenance of multicast trees, thus efficiently delivering multicast data packets from the source to the receivers within the multicast group.

The PIM protocol features two widely used modes:

• PIM Dense Mode (PIM-DM)

This mode is applicable to small-scale networks or scenarios with dense multicast traffic. In PIM-DM, multicast packets are transmitted along all available paths, which results in higher network bandwidth and resource consumption.

• PIM Sparse Mode (PIM-SM)

This mode is applicable to large-scale networks or scenarios with sparse multicast traffic. In PIM-SM, routers only forward multicast packets along the required paths, effectively reducing the utilization of network bandwidth.

14.3.2 Enabling PIM

Choose Local Device > L3 Multicast > PIM > PIM-enabled Interface List.

Click **Add**. A pop-up window is displayed. On the pop-up window, select the interface on which PIM is to be enabled, and click **OK**. Multicast packet forwarding can be implemented on the selected interface. The PMI mode is PIM-SM by default.

PIM-enabled Interface List				Add	Delete Selected
Interface	PIM Mode			Action	
VLAN 1	PIM-SM			Ē	
< 1 > 10/page < Go to page 1					Total 1
Select Interfaces		×			
Select	Cancel	ОК			

14.3.3 Viewing PIM Neighbor Table

In the PIM protocol, routers discover neighboring routers and establish neighbor relationships through the exchange of Hello messages. Once a neighbor relationship is established between two PIM-enabled routers, they can exchange multicast information, including multicast group memberships and multicast forwarding states. By continuously updating and maintaining the PIM neighbor table, PIM-enabled routers are able to efficiently forward and process multicast packets based on the neighbor information, thereby achieving effective multicast communication.

Choose Local Device > L3 Multicast > PIM > PIM Neighbor Table.

The **PIM Neighbor Table** page displays information about PIM neighbors, such as interface, PIM neighbor, TTL, and aging time. You can search for PIM neighbor table information by entering either the interface or the PIM neighbor in the search box. You can click **Refresh** to view the up-to-date PIM neighbor table information.

PIM Neighbor Table			Enter interface or PIM neighbor O Refresh
Interface	PIM Neighbor	TTL	Aging Time
		No Data	
< 1 > 10/page ~ Go to pag	e 1		Total 0

Table 14-2 Description of PIM Neighbor Table Parameters

Parameter	Description	Default Value
Interface	Interface connecting the neighbor router to the local router.	N/A
PIM Neighbor	IP address of the neighbor router.	N/A
TTL	The TTL value indicates the duration in which Hello messages sent by neighboring routers remain valid. If the local router does not receive any new Hello messages from a neighbor within the TTL time, it will consider the neighboring router as inactive or expired.	N/A
Aging Time	If a neighboring router becomes inactive or ceases to send Hello messages, the respective entry in the PIM Neighbor Table will be deleted after the specified aging time is exceeded.	105 seconds

14.4 Configuring RP

14.4.1 Overview

The Rendezvous Point (RP) is a crucial concept in the PIM protocol. In multicast communication, when a sender sends a multicast data packet, it needs to identify a specific point as the rendezvous point, from which multiple receivers can receive the multicast packet. The RP is the rendezvous point router in the multicast tree. An RP can be manually configured or dynamically elected through the BSR (Bootstrap Router) mechanism.

Note

An RP can provide services for multiple or all multicast groups. However, only one RP can forward multicast traffic for a multicast group at a time.

14.4.2 Configuring a Static RP

Choose Local Device > L3 Multicast > RP > Static RP.

Click Add. On the pop-up window that is displayed, enter the multicast group range covered by the RP and the RP address, then click **OK**.

Static RP			Add	Delete Selected
Multicast Group Range	RP Address		Action	
		No Data		
< 1 → 10/page ∨ Go to p	Age 1			Total 0
Add		×		
* Multicast Group	Example: 224.0.0.0/4			
Range				
* RP Address	Example: 1.1.1.1			
	Cancel	ЭК		

14.4.3 Configuring a Candidate RP

On a PIM network, a Candidate RP refers to a router that is eligible to become an RP. You can configure several PIM-enabled routers in the PIM domain as Candidate RPs, so that a suitable RP is eventually elected. This process aims to enhance the efficiency and reliability of multicast communication.

Choose Local Device > L3 Multicast > RP > Candidate RP.

Toggle on **Local routing device as candidate RP:** to designate the local device as the candidate RP. Enter the priority, advertisement interval, source IP address, and the designated multicast group. Then, click **Save**.

Candidate RP		
Local routing device as candidate RP:		
Priority:	192	(0-255. A lower value indicates a higher priority.)
Advertisement interval:	60	s
* Source IP Address	Interface V Select V	0
Designated multicast group	Example: 224.0.0.0/4 Add	0
	Save	

Parameter	Description	Default Value
Priority	The priority determines which candidate RP will become the RP during the election process. The priority value ranges from 0 to 255, where a smaller value indicates a higher priority. A candidate RP with a higher priority has a greater chance of being elected as the RP.	192
Advertisement Interval	A candidate RP announces its presence and availability by sending PIM messages. The advertisement interval determines the frequency at which a candidate RP sends these messages. A shorter advertisement interval can notify other routers about the presence of candidate RP more quickly, but it will also increase the network load.	60 seconds
Source IP Address	The source IP address of the PIM messages sent by the candidate RP, which can be either an interface or an IP address.	N/A
Designated multicast group	The PIM messages sent by the candidate RP must contain a multicast group address, which falls within the range of 224.0.0.0/4 to 239.255.255.255/32. Candidate RPs typically send multiple messages, each specifying a different multicast group address, in order to notify other routers that they can become the RP for these multicast groups. You can click Add to configure multiple multicast group addresses.	N/A

Table 4-1 Description of Candidate RP Configuration Paramete	on Parameters	Description of Candidate RP Configuration	Table 4-1
--	---------------	---	-----------

14.5 Configuring BSR

14.5.1 **Overview**

In PIM-SM mode, RP needs to be manually configured, which is a tedious task for large-scale networks. The BSR (Bootstrap Router) mechanism can automatically select the RP, simplifying the RP configuration process. BSR serves as the management core of the PIM-SM domain, responsible for collecting and advertising RP information within the domain. BSR is elected by candidate BSRs.

Note

A PIM-SM domain can have only one BSR, but can have multiple candidate BSRs.

14.5.2 Configuring BSR

Choose Local Device > L3 Multicast > BSR > Local Routing Device as Candidate BSR.

Toggle on **Local routing device as candidate BSR:** to designate the local device as the candidate BSR. Enter the priority and the source IP address. Then, click **Save**.

Local	routing device as candidate I	BSR:
Local rout	ing device as candidate BSR: 🚺	
Priority:	192	(0-255. A higher value indicates a higher priority.)
* Source I	P Address Interfaci V Select	~ 💿
	Save	

Table 4-2 Description of Candidate BSR Configuration Parameters

Parameter	Description	Default Value
Priority	Higher-priority candidate BSRs have a greater chance of being elected as the BSR. The priority value ranges from 0 to 255, where a smaller value indicates a higher priority.	192
Source IP Address	The source IP address of the PIM messages sent by the candidate BSR, which can be either an interface or an IP address.	N/A

14.5.3 Viewing BSR Routing Info

Choose Local Device > L3 Multicast > BSR > BSR Routing Info.

The **BSR Routing Info** page displays BSR routing information, including BSR address, priority, status, online duration and aging time. You can click **Refresh** to view the up-to-date BSR routing information.

BSR Routing Info					Refresh
BSR address	Priority	Status	Online Duration	Aging Time	
0.0.0.0	0	ACCEPT ANY	00:00:00		

14.6 Configuring IGMP

14.6.1 Overview

Internet Group Management Protocol (IGMP) is used to enable multicast communication on IPv4 networks. IGMP is responsible for managing the membership of multicast groups and facilitating communication between hosts and multicast routers. With IGMP, hosts can join or leave a specific multicast group and advertise its membership to multicast routers. Multicast routers use IGMP to determine which hosts are members of a multicast group, enabling efficient forwarding of multicast traffic.

14.6.2 Enabling IGMP

Choose Local Device > L3 Multicast > IGMP > IGMP-enabled Interface List.

The **IGMP-enabled Interface List** page displays basic information of IGMP-enabled interfaces, including the interface and the IGMP version.

IGN	IP-enabled Interface List		Add	🖉 Batch Edit	Delete Selected
	Interface	IGMP Version		Action	
	VLAN 1	IGMPv3 ~		۵.	
	1 > 10/page < Go to page 1				Total 1

Add: Click **Add**. The **Select Interfaces** pop-up window is displayed. On the pop-up window, select an interface on which IGMP will be enabled. Then, Click **OK**. IGMP is enabled on the corresponding VLAN.

Select Interfaces			×
Select	~		
		Cancel	ОК

Batch edit: Select the interfaces, and click **Batch Edit**. On the pop-up window that is displayed, select the IGMP version, then click **OK**.

IGMPv3 has improved functionality and flexibility compared to IGMPv2. It supports more multicast group management features, provides finer control over membership and query methods, and introduces security mechanisms. With these enhancements, IGMPv3 can be applied in scenarios that require a higher level of multicast management and security.

Batch Edit		×
Select the IGMP version:		
• IGMPv2 O IGMPv3		
	Cancel	ОК

Batch delete: Select the interfaces, and click Batch Delete. IGMP is disabled on the selected interfaces.

14.6.3 Viewing IGMP Multicast Group

Choose Local Device > L3 Multicast > IGMP > IGMP Multicast Group.

The **IGMP Multicast Group** page displays information about IGMP multicast groups, including the number of multicast groups, source IP addresses, TTL, and aging time. You can click to expand a multicast group to view the detailed IP addresses associated with the multicast group on that interface.

You can search IGMP multicast group information by entering the interface in the search box. You can click **Refresh** to view the up-to-date IGMP multicast group information.

IGMP Multicast Group					Enter interface	Refresh
Interface	Multicast Group	Source IP Address	TTL	Aging Time		
VLAN 1						
	239.255.255.250	*	00:52:34	00:02:20		
< 1 > 10/	'page \vee Go to page	1				Total 1

15 NBS and NIS Series Switches L3 Management

A Caution

This section is applicable only to NBS Series Switches that support L3 functions. Products that do not support L3 functions such as RG-NBS3100 Series Switches, RG-NBS3200 Series Switches, do not support the functions mentioned in this section.

15.1 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.

R Local Dev	rice(NBS 🗸 🗸 🗸	urrently in Local	Device mode.			English		٩	Ð
Switch • NBS6002	Hostname IP Address Software Ver:	Ruijie 192.168.110.62 ReyeeOS 1.218.2	SN: MA MAC Address: 421 Hardware	CCNBS6000HQ 00:D0:F8:95:68:5E Ver: 1.00	DNS: 192.16	3.110.1	U	Reboot	t
Home VLAN Diagnostics ~	Home VLAN Monitor × Ports × L2 Multicast L3 Interfaces × Routing × Security × Advanced × Diagnostics × System ×								
Port List						+ Ad	d L3 In	terface	
After the IPv4 a Up to 64 laye	address is set to Dy er-3 interfaces and	namic IP, the IPv6 64 IPv4 address	5 address will not t es can be configur	ake effect if the int ed.	terface does not ol	otain an IPv4 addre	iss.		
L3 Interfaces	Port Type	Networking	IP Address	Subnet Mask	DHCP Server	DHCP Server Info	A	tion	
VLAN1	Management VLAN	DHCP	192.168.110.6 2	255.255.255.0	Disabled		Edit	Delete	9
Gi2/14	Routed Port	Static IP	12.12.12.12	255.255.255.0	Disabled		Edit	Delete	e
< 1 >	10/page 🗸	Go to page	1					Total 2	2

Add		×
r Port Type	SVI v	
Networking	Static IP 🗸 🗸	
Primary IP/Mask	192.168.1.1 255.255.2 Add + ⑦	
VLAN	Select ~	
DHCP Mode	Disabled OHCP Server OHCP Relay	
	Cancel	ОК

Table 6-1 Description of Configuration Parameters of L3 Interfaces

Parameter	Description
Port Type	The type of a created L3 interface. It can be an SVI, routed port, or L3 aggregate port. For details, see <u>Table 12-1</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 15.2 Configuring the IPv6 Address for the L3 Interface. 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.

Parameter	Description
Excluded IP	When the device acts as a DHCP server, set the IP address in the address pool that is not used
Address (Range)	for assignment

Note

- VLAN 1 is the default SVI of the device. It can be neither modified nor deleted.
- The management VLAN is only displayed on the L3 Interfaces page but cannot be modified. To modify it, choose Ports > MGMT IP. For details, see <u>12.6</u> <u>MGMT IP Configuration</u>.
- The DHCP relay and DHCP server functions of an L3 interface are mutually exclusive and cannot be configured at the same time.
- Member ports of an L3 interface must be routed ports.

15.2 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.

Rcy	'CC	Local Device(NBS 🗸					nglish 🗸 🛆 🧁	Ð
Ports	~							
L2 Multicast		IPv6 Config DHCP	v6 Server DHCPv6 Cli	ents Static DHCP	Pv6 IPv6 Neighbor Lis	st		
L3 Multicast		Port List					+ Add L3 Interface	9
4 L3 Interfaces	~	After the IPv4 address Up to 16 MTU can b	s is set to Dynamic IP, the IPv e configured.	6 address will not take e	effect if the interface does n	ot obtain an IPv4 address.		
L3 Interfaces						IPv6 Address/Prefix		
IPv4 Config		L3 Interfaces	Port Type	Networking	IPv6 Prefix	Length	Action	
IPv6 Config		VLAN1	Management VLAN		-		Edit	
Routing	×	VLAN130	SVI	Static IP	-		Edit Clear	
Security	~	< 1 > 10	/page 🗸 Go to page	e 1			Total	2
🖶 Advanced	~							6
Collapse								

A 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.

R	Local Devic	e(NBS 🗸 🔹 Curren	tly in Local Devic	e mode.		English 🗸 🛆 🧁 🕞
•	Switch	Hostname: Ruiji IP Address: 192. Software Ver: Reye	e 68.110.62 M/ eOS 1.218.2421	SN: MACCNBS AC Address: 00:D0:F Hardware Ver: 1.0	5000HQ 8:95:68:5E 00 DNS: 192.168.110.1	(1) Reboot
Hon Diag	ne VIAN gn Edit	Monitor Y Port	s ⊻ I 2 Multic ✔ Obtain an IF	ast 13 Interface	s × Routina × Security × CPv6.	Advanced ×
Por	rt	MTU	1500		(1280-1500)	rface
					Can	Cel
	VLAN1	Manager	nent VLAN			Edit
	Gi2/14	Route	ed Port	Static IP		Edit Clear
<	1	10/page \vee	Go to page 1			Total 2

Local Device(NBS > Current	ly in Local Device mode.		English 🗸 🛆 🛕 🕞
Hostname: Ruijie iP Address: 192.1 • NB56002 Software Ver: Reyet HomeVLANMonitor ≤Onthe	SN: MACCN856000HQ 68:110.62 MAC Address: 00:D0:F8:95:68:5E OS 1.218:2421 Hardware Ver: 1.00	DNS: 192.168.110.1	() Reboot
Diagn Edit			×
IPv6 Co Auto Obtained IP	Obtain an IPv6 address via DHCPv6.		
Port IPv6 Address/Prefix Length	Example: 2000::1	64 Manual	✓ Add + ⑦ rface
After MTU	1500	(1280-1500)	
L	Advanced Settings		
Link-local Address	FE80::ABCD:ABCD:ABCD:ABCD	0	
Subnet Prefix Name	The subnet prefix is not configured ([$ \lor $		
Subnet Prefix Length	64	0	lotal 2
Subnet ID	0	0	
		Cance	el OK

Table 6-2 IPv6 Address Configuration Parameters of the L3 Interface

Parameter	Description
Obtain an IPv6 address via DHCPv6	If no upstream DHCPv6 server is available, do not select Auto Obtained IP . Instead, manually add the IPv6 address.
	Configure the IPv6 address and prefix length. You can click Add to add multiple IPv6 addresses.
IPv6	If the primary IP address is empty, the configured secondary IP address is invalid.
Address/Prefix Length	For manual configuration, the prefix length ranges from 1 to 128.
U U	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 .

Parameter	Description
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).

15.3 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.

15.3.1 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.

Ruíji	e Rcy	cc	Local Device	e(NBS 🗸					En	glish ~ 🛆 🧁	Đ
掛 Mor	nitor	~	Port Lis	t						+ Add L3 Interface	•
Port	s Iulticast	~	After the Up to 50	IPv4 address is set to Dynami IPv4 address is set to Dynami IPv4 address interfaces and 500	c IP, the IPv6 address IPv4 addresses can	s will not take effect if the be configured.	interface does not ob	tain an IPv4 address.			
🛆 L3 N	Iulticast		L3 Inter	faces Port Type	Networking	J IP Address	Subnet Mask	DHCP Server	DHCP Server Info	Action	
) L3 Ir	nterfaces	^	VLAN	Management VLAN	Static IP	10.51.227.7	255.255.255.0	Disabled	-	Edit Delete	
IPv4 0	Config		VLAN	130 SVI	Static IP	192.168.130.1	255.255.255.0	DHCP Server	View Details	Edit Delete	
IPv6 0	Config		< 1	10/page v	Go to page 1					Total	2
Rout	ting	×									
⊘ Sect	anced	~									e
«	Collapse										
Edit							×				
			Port Type	SVI							
			Networking	Static IP	~						
		* Pri	mary IP/Mask	192.168.130.1	255.255.255.0	Add + ⑦					
			VLAN	test	~		_				
		* C+	DHCP Mode	Disabled O DHCI	P Server O DI	HCP Relay					
		31	* IP Count	254							
	Exte	ernal IP.	/External User	Available IP Addresses: 25	3. End IP Address:	192.168.130.254.					
		* Lea	ise Time (Min)	480							
l											
						Cancel	ОК				

Table 6-3	Description of DHCP	Server Configuration	Parameters
	200000000000000000000000000000000000000	een een galaden	

Parameter	Description
DHCP Server	To choose DHCP server
Start IP Address	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.

Parameter	Description
IP Count	The number of IP addresses in the address pool
External IP/External User	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

15.3.2 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>15.3.3</u> Configuring Static IP Addresses Allocation.

Ruíjie Rcycc	Local Device(NBS 🗸				English 🗸 🛆	۵ 🗗
🔄 Monitor	DHCP Clients Static IP Addresses	DHCP Option ARP List				
Ports	<i>i</i> View DHCP clients.					?
L2 Multicast	DHCP Clients		Search by Hostname/I	P Addı 🔾 😋 Refresh	+ Batch Conv	vert
🛆 L3 Multicast						
L3 Interfaces	Up to 4000 IP-MAC bindings can be adde	:d.				
L3 Interfaces	No. Device Name	IP Address	MAC Address	Remaining Lease Time(min)	Status	
IPv4 Config			No Data			
IPv6 Config						Code L O
Routing	To/page V Go	to page 1				
⊘ Security ∨						
🗄 Advanced 🛛 🗸						
«Collapse						

15.3.3 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 Rcycc		English 🗸 🛆 🤮 🕞
껲 Monitor 🗸	DHCP Clients Static IP Addresses DHCP Option ARP List	
Ports ✓	1 Static IP Address List	0
L2 Multicast	Static IP Address List Search by IP Address/MAC A Q Batch Import Batch Export + Add	Delete Selected
L3 Multicast		
🕀 L3 Interfaces	Up to 4000 entries can be added.	
L3 Interfaces	No. Device Name IP Address MAC Address	Action
IPv4 Config	No Data	
IPv6 Config	< 1 > 10/page < Go to page 1	Total 0
⊕ Routing ~		
😔 Security 🗸 🗸		
🖹 Advanced 🗸 🗸		
Collapse		

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		×
Device Name	Optional	
* IP Address	Example: 1.1.1.1	
* MAC Address	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.

15.3.4 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.

Reyee Cookbook

Ruíjie Rcycc	Local Device(NBS V	English ~ 🛆 🛔 🗗
Monitor >	DHCP Clients Static IP Addresses DHCP Option ARP List	
Ports	DHCP Option DHCP option settings are applied to all LAN ports.	0
L2 Multicast		
L3 Multicast	DNS Server Example: 8.8.8.8, each separated by a space.	
🜐 L3 Interfaces 🗠	Option 43 Enter an IP address or hexadecimal number.	
L3 Interfaces	Option 138 Example: 1.1.1.1	
IPv4 Config		
IPv6 Config	Option 150 Example: 1.1.1.1, each separated by a space.	
\oplus Routing \checkmark	Gateway Example: 1.1.1.1	
\oslash Security \checkmark	Save	
🖹 Advanced 🗸 🗸		(* 41
«Collapse		

Table 6-4 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.
Gateway	Specifies the default gateway address that client devices use to access networks outside of their local subnet, typically the IP address of a router or other networking device that connects to other networks or the internet.

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.

15.4 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.

 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.

R Local De	evice(NBS 🗸 🔹 Cu	urrently in Local Device mode.				English ~	٥		
Switch • NBS6002 Home VLAI Diagnostics ~	Hostname: IP Address: Software Ver: N Monitor ~ System ~	Ruijie SN: M 192.168.110.62 MAC Address ReyeeOS 1.218.2421 Hardwai Ports × L2 Multicast L3 I	ACCNBS60001 : 00:D0:F8:95: re Ver: 1.00 nterfaces ~	HQ 668:5E DNS Routing ~	: 192.168.110.1 Security ~	Advanced	() Re	boot	
IPv6 Config DHCPv6 Se	DHCPv6 Server	DHCPv6 Clients Static	DHCPv6	IPv6 Neighbo	r List + Add	🔟 Dele	te Sele	cted	
1、 If DHCPvi prefix of the I 2、 If the IPvi Up to 64 en	5 does not take effec ayer 3 interface), the 5 prefix length of the tries can be added.	t on the Layer 3 interface (includii e DHCPv6 server cannot take effec Layer 3 interface is between 48 a	ng but not lim .t. nd 64, the ado	iited to invalid IP dress can be assi	ν6 address and gned.	incorrect IPv6	addres	S	
	L3 Interfaces	IPv6 Assig	nment		DNS Server		Act	ion	
		No	Data						
< 1 >	10/page V	Go to page 1					Т	otal O	

R Local Device(NBS	Currently in Loca	I Device mode.		English ~ 🛆 🗗
Switch II • NB56002 Sof	Hostname: Ruijie P Address: 192.168.110.62 tware Ver: ReyeeOS 1.218.	SN: MACCNBS6000HQ MAC Address: 00:D0:F8:95:68:5E 2421 Hardware Ver: 1.00 DNS: 192.	168.110.1	() Reboot
Home VLAN Mor Diagnostics × Sys	itor ⊻ Ports ⊻ 12	Multicast I 3 Interfaces × Routino × Se	curitv × ×	Advanced Y
IPv6 Config DHCF	* L3 Interfaces	Select ~		
	IPv6 Assignment	Auto ~	?	
DHCPv6 Server	* Lease Time (Min)	30	(?)	Delete Selected
1、 If DHCPv6 does r prefix of the Layer 3 2、 If the IPv6 prefix Up to 64 entries ca	DNS Server	Example: 2000::1, each separated by a comma		rrect IPv6 address
		Cancel	ОК	Action
	page \vee Go to page	9 1		Total 0

Table 6-5 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 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.

15.4.1 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.

1 Note

Each server or client has only one DUID for identification.

Ruíjie Rcycc	Local Device(NBS >	English ~ 🛆 Remote O&M 🚷 Network Configuration 🕒 Log Out
∂ ² δ Home	IPv6 Config DHCPv6 Server DHCPv6 Clients Static DHCPv6 IPv6 Neighbor List	
응 VLAN	DHCPv6 Clients	
🗄 Monitor	Vou can view the DHCPv6 clients information on this page.	
Ø Ports ~	DHCPv6 Clients	Search by IPv6 Address/DUIE Q + Bind Selected
L2 Multicast	No. Hostname IPv6 Address Remaining Lease Time(min)	DUID Status
L3 Multicast	No Data	
L3 Interfaces ^		Tetel 0
L3 Interfaces	C V 10/page V 0010 page 1	total U
IPv4 Config		
IPv6 Config		
Routing		
⊘ Security ~		
🖻 Advanced		
«Collapse		

15.4.2 Configuring the Static DHCPv6 Address

Configure the IPv6 address statically bound to the DUID of a client so that the client can obtain the specified address each time.

Choose Local Device > L3 Interfaces > IPv6 Config > Static DHCPv6.

Click **Add**, and enter the IPv6 address and DUID. You are advised to bind the IPv6 address and DUID in the client list. You can run the **ipconfig /all** command on the Command Prompt in Windows to view the DUID.

Command Prompt
Microsoft Windows [Version 10.0.17763.1577] (c) 2018 Microsoft Corporation. All rights reserved.
C:\Users\admin>ipconfig /all
Windows IP Configuration
Host Name : PC- Primary Dns Suffix : Node Type : Hybrid IP Routing Enabled : No WINS Proxy Enabled : No
Ethernet adapter
Connection-specific DNS Suffix . : Description : RuiJie VirtIO Ethernet Adapter Physical Address : Yes DHCP Enabled : Yes Autoconfiguration Enabled : Yes Link-local IPv6 Address : fe80::6dd5:266f:b695:55df%12(Preferred) IPv4 Address : 172.26.1.123(Preferred) Subnet Mask : 255.255.255.0 Lease Obtained : Thursday, December 22, 2022 5:29:03 PM Lease Expires : : 172.26.1.1 DHCPv6 IAID DHCPv6 IAID DHCP 6 GUILD DHCP
DHCPvb Client DUID

Currently in Local Device mode.	inglish -> 🛆 🛕 🗗
Hostname: Ruijie SN: MACCNBS6000HQ IP Address: 192.168.110.62 MAC Address: 00:D0:F8:95:68:5E Software Ver: ReyeeOS 1.218.2421 Hardware Ver: 1.00	
Home VLAN Monitor ~ Ports ~ L2 Multicast L3 Interfaces ~ Routing ~ Security ~ Advanced ~ Diagnostics ~ System ~	
IPv6 Config DHCPv6 Server DHCPv6 Clients Static DHCPv6 IPv6 Neighbor List DHCPv6 Clients Variantian on this page	
DHCPv6 Clients Search by IPv6 Address/DUII Q	+ Batch Convert
No. Hostname IPv6 Address Remaining Lease DUID Time(min)	Status
No Data	
C 1 > 10/page > Go to page 1	Total 0

You can view the DHCPv6 clients information on this page.
	mode.	English -> 🛆 🖨 🗗
Hostname: Ruijie MAC Address: 00:D0:F8:95:68:5E • NBS6002 DNS: 192.168.110.1	SN: MACCNBS6000HQ IP Addres Software Ver: ReyeeOS 1.218.2421 Harc	is: 192.168.110.62 Iware Ver: 1.00
Home VLAN Monitor ^v Ports ^v L2 Multica Diagnostics ^v System ^v	st <u>L3 Interfaces</u> Routing × Se	curity \checkmark Advanced \checkmark
IPv6 Config DHCPv6 Server DHCPv6 Clients	Static DHCPv6 IPv6 Neighbor List	:
🥡 Static IP Address List		
Static IP Address List	Search by IPv6 Address/DUIE Q	+ Add Delete Selected
Up to 1000 entries can be added.		
No. IPv6 Address	DUID	Action
	No Data	
Control to the second s		Total 0

Rujje Rcycc	Currently in Local Device mode			English -> 🛆 🏩 🗗				
Image: Switch Hostname: Ruijie SN: MACCNBS6000HQ IP Address: 192.168.110.62 Image: Switch MAC Address: 00:D0:F8:95:68:5E Software Ver: ReyeeOS 1.218.2421 Hardware Ver: 1.00 Image: NBS6002 DNS: 192.168.110.1 Image: SN: Macconstant Image: SN: Macconstant								
Home VLAN Monitor ~ Diagnostics ~ System ~	Ports ⊻ 12 Multicast I Add	3 Interfaces × Routing × S	Security × Adv	ranced Y				
IPv6 Config DHCPv6 Server	* IPv6 Address	xample: 2000::1						
i Static IP Address List	* DUID	xample: 0003000100d0f819685f						
Static IP Address List		Cancel	ок	Delete Selected				
🗌 No. IPvé	Address	DUID		Action				
No Data								
Image Image Go to page Image Total 0								

15.5 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).

Ruíjie I Rcycc 🛛 🖳	Currently in Local Device mode.			English -> 🛆 🔮 📑	
Switch Hostnam MAC Addres NBS6002 DN	e: Ruijie SN: MAC s: 00:D0:F8:95:68:5E Software Ve S: 192.168.110.1	CCNBS6000HQ r: ReyeeOS 1.218.2421	IP Address: 192.168.110.62 Hardware Ver: 1.00	() Reboot	
Home VLAN Monitor $^{\sim}$ Diagnostics $^{\sim}$ System $^{\sim}$	Ports Y L2 Multicast L3 Inte	erfaces \vee Routing	∼ Security ∼ Adva	anced ~	
IPv6 Config DHCPv6 Server	DHCPv6 Clients Static DH	ICPv6 IPv6 Neig	hbor List		
IPv6 Neighbor List	Search by IP Address/MAC A	Q + Add	Bind Selected	Delete Selected	
Up to 2000 IP-MAC bindings ca	an be added.				
No. MAC Address	IP Address	Туре	Ethernet status	Action	
No Data					
< 1 > 10/page >	Go to page 1			Total 0	

v6 Config D	HCPv6 Server DHCPv6 Clients S	tatic DHCPv6 IPv6 Neighbor List			
IPv6 Neighb	or List		Search by	y IP Address/MAC A Q + Add	P Bind 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	Gi22	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	e ^o Bind
6	00:d0:c8:95:79:20	fe80::2d0:c8ff:fe95:7920	Dynamic	Gi22	& Bind
7	c0:b8:e6:e2:54:63	3000::1	Dynamic	VLAN 1	e ^p Bind
8	c0:b8:e6:e2:54:63	fe80::c2b8:e6ff:fee2:5463	Dynamic	VLAN 1	e ^p Bind
1	10/page v Go to page 1				Tot
					Click RITA for help.

Rujje l Rcycc	Currently in Local Device mode.		English -> 🛆 🛕 🕞
Switch Hostnam MAC Addre • NBS6002 DN	ne: Ruijie SN: M ss: 00:D0:F8:95:68:5E Software 45: 192.168.110.1	ACCNBS6000HQ IP Address: 192. /er: ReyeeOS 1.218.2421 Hardware \	168.110.62 /er: 1.00
Home VLAN Monitor ~ Diagnostics ~ System ~	Ports Y 12 Multicast 13 In Add	nterfaces × Routing × Security. ×	✓. Advanced ✓
IPv6 Config DHCPv6 Server	* Interface Sele	ct ~	
IPv6 Neighbor List	* IPv6 Address Plea	se enter an IPv6 address.	ed 🗇 Delete Selected
Up to 2000 IP-MAC bindings of	* MAC Address Plea	se enter a MAC address.	
No. MAC Addres		Cancel OK	tus Action
10/page V	Go to page 1		Total 0

15.6 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**.

L3 Inter	rfaces	DHCP Clients	Static IP Addresses	DHCP Option Stat	ic Routing ARP Li	st	
ARP	List			Search by	IP/MAC	Q + Add	Delete Selected
Up t	to 2000	IP-MAC bindings can	be added.				
	No.	Interface	MAC	IP	Туре	Reachable	Action
	1	VLAN1	00:23:79:00:23:79	172.30.102.178	Dynamic	Yes	
	2			172.30.102.174	Dynamic	No 🕑	
	3	VLAN1	c0:b8:e6:e9:78:07	172.30.102.209	Dynamic	Yes	
	4	VLAN1	c0:b8:e6:ec:a1:5c	172.30.102.118	Dynamic	Yes	



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

ARP	List			Search by IF	P/MAC	Q + Add	Delete Selected
Up t	o 2000 IF	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	

16 NBS and NIS Series Switches Configuring Route

A Caution

The content covered in this chapter is applicable solely to NBS series switches with Layer 3 capabilities. Switches from the RG-NIS series, RG-NBS3100 series, and RG-NBS3200 series do not support the features described in this section.

16.1 Configuring Static Routes

Choose Local Device > Routing > 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.

A 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.

Ruíjie Rcycc						English 🗸 🛆 🤮	
Orts							
🛆 L2 Multicast	 Static Routing When a packet arrives, the depacket from the specified int 	evice checks the destination erface.	field and compares it with	routing table. If it finds a mate	h for destination network the	en it will forward that 🥐	
L3 Multicast							
\oplus L3 Interfaces \checkmark	Static Route List			Example: 1.1.1.1	Q + Add	Delete Selected	
Routing	Up to 500 static routes can be a	dded.					
Static Routing	Dest IP Address	Subnet Mask	Outbound Interface	Next Hop	Reachable	Action	
Static Routing_v6	2.1.1.0	255.255.255.0	Normal Route	3.1.1.1	No 🔞	Edit Delete	
RIP Settings	< 1 > 10/page ~	Go to page 1				Total 1	
RIPng Settings							
OSPFv2							
OSPFv3							
Route Info							4
«Collapse							

Edit		×
* Dest IP Address	2.1.1.0	
* Subnet Mask	255.255.255.0	
Outbound Interface	Normal Route	\sim
* Next Hop	3.1.1.1	
	C	ancel OK

 Table 16-1
 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.

Statio	Route List		Exa	mple: 1.1.1.1	Q	+ Add	Delete Selected
Up to	500 static routes can be	added.					
	Dest IP Address	Subnet Mask	Outbound Inte	route is unreachable. Please in	itiate 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.

16.2 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.

R Local Device(NBS >	Currently in Local Device m	ode.		English 🗸 🛆 🛕 🕞
Switch IP Addr NB56002 Software	me: Ruijie ess: 192.168.110.62 MAC A _{/er:} ReyeeOS 1.218.2421 _H	N: MACCNBS6000HQ ddress: 00:D0:F8:95:68:5E ardware Ver: 1.00	DNS: 192.168.110.1	(1) Reboot
Home VLAN Monitor · Diagnostics · System ·	Y Ports ∀ L2 Multicast	L3 Interfaces Y Rou	uting \checkmark Security \checkmark	Advanced 🗠
Static Routing When a packet arrives, th network then it will forwa	e device checks the destination rd that packet from the specifie	field and compares it with d interface.	routing table. If it finds a r	match for destination (?)
Static Route List	Exam	ole: 2000::1	+ Add	Delete Selected
Up to 500 entries can be ad	ded.			
IPv6 Address	Prefix Length	Outbound Interface	Next Hop	Action
		No Data		
< 1 > 10/page	Go to page 1			Total 0

R Local Device(NE	S ~ Currently in Loca	l Device mode.		English -> 🛆 🔮 📑
Switch • NBS6002 S	Hostname: Ruijie IP Address: 192.168.110.62 oftware Ver: ReyeeOS 1.218.	SN: MACCNBS6000HQ MAC Address: 00:D0:F8:95:68:5E 2421 Hardware Ver: 1.00	DNS: 192.168.110	(¹) Reboot
Home VLAN M Diagnostics Y Sys	Add	Multicast 13 Interfaces Y Ro	outina 👋 Security)	× Advanced ×
Static Routing When a packet a network then it a	* IPv6 Address/Prefix Length	Example: 2000::1	0	ch for destination 🥐
Static Route Lis	Outbound Interface	Normal Route	~	Delete Selected
Up to 500 entries c	* Next Hop	Example: 2000::1		
IPv6 Add			Cancel	Action
)/page	e 1		Total 0

Table 16-2 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.

16.3 Configuring RIP

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

16.3.1 Configuring RIP Basic Functions

Choose Local Device > Routing > RIP Settings.

Click Add and configure the network segment and interface.

R Local Device(NBS ~	Currently in Local Device m	ode.	E	inglish ~ 🛆 🧟		
Hostr IP Ad • NBS6002 Softwar Home VLAN Monitor Diagnostics × System ×	name: Ruijie	SN: MACCNBS6000HQ ddress: 00:D0:F8:95:68:5E ardware Ver: 1.00 DN L3 Interfaces × Routing ×	s: 192.168.110.1	() Reboot Advanced ~		
RIP Settings Port Settings Advanced Neighbor Info Image: Layer-3 Routing Protocol: RIP 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 routes to remote networks and keep routes updated in real time.						
<i>i</i> Network Segment/P Enable RIP in the specif	ort List ied network segment or on the sp	pecified port.				
Network Segment/P	ort List		+ Add	Delete Selected		
No. Netwo	rk Segment/Port	Auth Mode		Action		
□ 1	VLAN 1	No Authentication	E	dit Delete		

Reyee Cookbook

Local Device(NBS >	Currently in Local Devic	te mode.	English 🗸 🛆 🔮 🗗
Hostn IP Add • NBS6002 Software Home VLAN Monitor Diagnostics × System ×	ame: Ruijie Iress: 192.168.110.62 M/ _{2 Ver:} ReyeeOS 1.218.2421 × Ports × 1.2 Multic Add	SN: MACCNBS6000HQ AC Address: 00:D0:F8:95:68:5E Hardware Ver: 1.00 DNS: 1 Past 13 Interfaces × Routing ×	92.168.110.1 Security × Advanced × ×
RIP Settings Port Settings Layer-3 Routing Proto RIP (Routing Information exchange the routing intrupdated in real time.	Type * Network Segment	Network Segment Port Please enter a valid value. Example	inning the protocol ks and keep routes
Network Segment/Po Enable RIP in the specific Network Segment/Po	ort List	Auth Mode	+ Add Delete Selected
		Auto Mode	
R Local Device(NBS ~	Currently in Local Devic	e mode. SN: MACCNBS6000HQ	English ~ 🔿 🔮 📑
C Local Device(NBS Hostn IP Add • NBS6002 Software	Currently in Local Devic ame: Ruijie iress: 192.168.110.62 MA Ver: ReyeeOS 1.218.2421	e mode. SN: MACCNBS6000HQ AC Address: 00:D0:F8:95:68:5E Hardware Ver: 1.00 DNS: 1	English ~ 🛆 🏩 🗗 (*) Reboot 92.168.110.1
Cocal Device(NBS) Hostn IP Add • NBS6002 Software Home VLAN Monitor Diagnostics Y System Y	Currently in Local Devic ame: Ruijie ress: 192.168.110.62 MA . Ver: ReyeeOS 1.218.2421 Y Ports Y 1.2 Multic Add	sn; MACCNBS6000HQ SN; MACCNBS6000HQ AC Address: 00:D0:F8:95:68:5E Hardware Ver: 1.00 DNS: 1 ast 13 Interfaces × Routing ×	English ~ 🛆 ಿ 🕞 92.168.110.1 Security ~ Advanced ~ ×
Clocal Device(NBS) Hostning NBS6002 Software Home VLAN Monitor Diagnostics Y System Y RIP Settings Port Settings	Currently in Local Devic ame: Ruijie ress: 192.168.110.62 MA Ver: ReyeeOS 1.218.2421 Ports × 1.2 Multic Add	se mode. SN: MACCNBS6000HQ AC Address: 00:D0:F8:95:68:5E Hardware Ver: 1.00 DNS: 1 ast 1.3 Interfaces × Routing ×	English ~ () &) () Reboot 92.168.110.1 Security × Advanced × ×
Clocal Device(NBS Clock Constraints) Switch Hosting Switch IP Add • NB56002 Software Home VLAN Monitor Diagnostics System System RIP Settings Port Settings RIP (Routing Information exchange the routing intugated in real time.	Currently in Local Devic ame: Ruijie ress: 192.168.110.62 MA . Ver: ReyeeOS 1.218.2421 Y Ports Y 1.2 Multice Add Type * Port Auth Mode	se mode. SN: MACCNBS6000HQ AC Address: 00:D0:F8:95:68:5E Hardware Ver: 1.00 DNS: 1 ast 1.3 Interfaces × Routino × Network Segment • Port Select × No Authentication ×	English ~ () Reboot 92.168.110.1 Security × Advanced × × inning the protocol ks and keep routes
 Local Device(NBS Hostming NBS6002 Software Home VLAN Monitor Diagnostics Y System Y RIP Settings Port Settings RIP Setting Port Settings RIP (Routing Information exchange the routing information updated in real time. Network Segment/Portion Network Segment/Portion 	Currently in Local Device ame: Ruijie ress: 192.168.110.62 MA .Ver; ReyeeOS 1.218.2421 Y Ports Y 1.2 Multice Add Type * Port Auth Mode	se mode. SN: MACCNBS6000HQ AC Address: 00:D0:F8:95:68:5E Hardware Ver: 1.00 DNS: 1 ast 1.3 Interfaces × Routing × ONetwork Segment • Port Select × No Authentication × Cancel	English ~ () Reboot 92.168.110.1 Security ~ Advanced ~ X inning the protocol is and keep routes OK IDelete Selected
 Local Device(NBS Hostmanner NBS56002 Software Home VLAN Monitor Diagnostics System RIP Settings Port Settings RIP Settings Port Settings RIP (Routing Information exchange the routing information Network Segment/Pool Network Segment/Pool No. Network	Currently in Local Device ame: Ruijie ress: 192.168.110.62 MA Ver: ReyeeOS 1.218.2421 × Ports × 1.2 Multice Add Type * Port Auth Mode	se mode. SN: MACCNBS6000HQ AC Address: 00:D0:F8:95:68:5E Hardware Ver: 1.00 DNS: 1 ast 13 Interfaces × Routino × Network Segment • Port Select × No Authentication × Cancel •	English ~ () Reboot 92.168.110.1 Security ~ Advanced ~ × inning the protocol is and keep routes OK DK DC Action

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 network segment, for example, 10.1.0.0/24 , when Type is set to Network Segment . RIP will be enabled on all interfaces of the device covered by this network segment.
Port	Select a VLAN interface or physical port when Type is set to Port .
Auth Mode	No Authentication: The protocol packets are not authenticated. Encrypted Text: The protocol packets are authenticated, and the authentication key is transmitted with the protocol packets in the form of encrypted text. Plain Text: The protocol packets are authenticated, and the authentication key is transmitted with the protocol packets in the form of plain text.
Auth Key	Enter the authentication key to authenticate protocol packets when Auth Mode is set to Encrypted Text or Plain Text .

Table 16-3 RIP Configuration Parameters

16.3.2 Configuring the RIP Port

Choose Local Device > Routing > RIP Settings > Port Settings.

Local Dev	vice(NBS 🗸 🔨	Currently in Loca	l Device mode.			English ~		<u>۾</u>
Switch • NB56002 Home VLAN Diagnostics ~	Hostname IP Address Software Ver Monitor ~ System ~	e: Ruijie s: 192.168.110.62 r: ReyeeOS 1.218.2 Ports × L2	SN: MA MAC Address: 2421 Hardware Multicast L3 Ir	CCNBS6000HQ 00:D0:F8:95:68:5E 9 Ver: 1.00 hterfaces ~ Ro	DNS: 192.16 uting Y Secu	8.110.1 rity [∨] Advance	() Reb	oot
NP Settings Port List	Port Settings	Advanced	Neighbor Info					
Port Name	Rx Status	Tx Status	Poison Reverse	v2 Broadcast Packet	Auth Mode	Auth Key	Actio	n

Table 16-4 Configuration Parameters in the Port List

Parameter	Description
Port Name	Name of the port where RIP is enabled.
Rx Status	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 performance.

Auth Mode	No Authentication: The protocol packets are not authenticated. Encrypted Text: The protocol packets are authenticated, and the authentication key is transmitted with the protocol packets in the form of encrypted text.
Auth Mode	authenticated, and the authentication key is transmitted with the protocol packets in the form of encrypted text. Plain Text : The protocol packets are
	authenticated, and the authentication key is
	transmitted with the protocol packets in the form of plain text.
Auth Key	Enter the authentication key to authenticate protocol packets when Auth Mode is set to Encrypted Text or Plain Text .
Action	Click Edit to modify RIP settings of the port.

16.3.3 Configuring the RIP Global Configuration

Choose Local Device > Routing > RIP Settings > Advanced, click Edit Config, and configure RIP global configuration parameters.

Ruíjie Rcycc						English -> 🛆 🔮 🗗
L3 Multicast	(
⊕ L3 Interfaces ∨	RIP Settings Port Sett	ings Advanced Neig	hbor Info			
Routing	<i>i</i> Improper timers may RIP timers unless you	/ cause route flapping. Therefore u have specific needs.	, RIP timers must be consistent	on the devices connected to the	e same network. You are n	ot advised to reset the
Static Routing	RIP Global Config					Edit Config
Static Routing_v6	· ·					
RIP Settings	RIP Version	Route Advertisement	Administrative Distance	Update Timer	Invalid Timer	Flush Timer
RIPng Settings	Default	Off	1 (Default)	30 s	180 s	120 s
OSPFv2						
	Redistribute the rout	on List ies of other protocols to the RIP (domain so that RIP can commu	inicate with other routing domai	ns.	
OSPFv3						
Route Info	Route Redistributi	on List			+ Add	Delete Selected
⊘ Security ~	Т	/pe A	dministrative Distance	Instance ID		Action
🗄 Advanced 🛛 🗸			No Da	ita		4
«Collapse						

NBS and NIS Series Switches Configuring Route

Reyee Cookbook

Ruíjie Rcycc	Local Device(NBS \vee							Er	nglish ~ 🛆 🧔	· G
🛆 L3 Multicast		Edit Config				×				
L3 Interfaces `` ` ``	RIP Settings Port Settings	g								
Routing ^	Improper timers may cause RIP timers unless you have	RIP Version	Default		v Ø)	ted to the same network.	You are not ac	dvised to reset the	
Static Routing	RIP Global Config	Route Advertisement							Edit Config	
Static Routing_v6		Administrative	1 (Default))						
RIP Settings	RIP Version F	Distance					Invalid Time	er	Flush Timer	
RIPng Settings	Default	* Update Timer	30	s (5-2147483647)			180 s		120 s	
OSPFv2	<i>Route Redistribution L</i> Redistribute the routes of	* Invalid Timer	180	s (5-2147483647)			ng domains.			
OSPFv3		* Flush Timer	120	s (5-2147483647)						
Route Info	Route Redistribution I						+	Add	Delete Selected	
⊘ Security	Туре			Cancel	ОК		ince ID		Action	6
🗄 Advanced 🛛 👋				Ho Data						4
«Collapse										

 Table 16-5
 RIP Global Configuration Parameters

Parameter	Description
RIP Version	 Default: Select RIPv2 for sending packets and RIPv1/v2 for receiving packets. 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.

Parameter	Description
Flush Timer	If no update is received before the flush timer of an invalid route expires, the route is completely deleted from the RIP routing table. The default value is 120 seconds.

16.3.4 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, click Add, and select the type and administrative distance.

R Local Device	e(NBS 🗸 🗸	Currently in Local Device	mode.				English ~	△ 🖗	₽
Switch • NBS6002	Hostnam IP Addres Software Ve	ne: Ruijie ss: 192.168.110.62 MA(er: ReyeeOS 1.218.2421	SN: MA C Address: Hardware	ACCNBS600 00:D0:F8:99 e Ver: 1.00	DHQ 5:68:5E D	NS: 192.168.110.	.1	() Rebo	ot
Home VLAN Diagnostics ~	Monitor × System ×	Ports Y 12 Multica Add	st I3lr	nterfaces 🔌	Routina	✓ Security `	 Advanced 		
RIP Global Co	onfig	* Type	Select			~	Ed	it Config	
RIP Version	Adv	Distance	U (Adm	inistrative	Distance)	1e	r Flus	h Timer	
Default	stribution				Cancel	ок		120 s	
Route Redistribute	the routes of c	other protocols to the RIP c	lomain so	that RIP car	i communicate	+ Add	ng domains.	Selected	
	Туре	Administrative	Distance	2	Instance I	D	Actio	n	
			No	Data					
Passive Inte	e rface ackets will be o enable this t	suppressed on the passive function.	interface.	If the device	connected to	the interface do	es not adopt RII	⁹ , you	
Passive Interf	face					+ Add	i Delete	Selected	
		Port Name				Action			

Table 16-6 RIP Route Redistribution Parameters

Parameter	Description
Туре	Direct Routing OSPF Routing Static Routing
Administrative Distance	A smaller administrative distance indicates a higher priority. The default value is 0 . The value ranges from 0 to 16.
Instance ID	Select the instance ID of OSPF that needs to be redistributed. OSPFv2 needs to be enabled on the local device.

 \times

Add

* Туре	OSPF Routing	\sim	
* Administrative	0 (Administrative Distance)	~	
Distance			
* Instance ID	Select	^	
	3		
	Cancel	0	к

16.3.5 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, click Add, and select a passive interface.

Currently in Local Device mode.	English 🗸 🛆 🔮 🗗
Hostname: Ruijie SN: MACCNBS6000HQ IP Address: 192.168.110.62 MAC Address: 00:D0:F8:95:68:5E • NBS6002 Software Ver: ReyeeOS 1.218.2421 Hardware Ver: 1.00 DNS: 192	(1) Reboot
Home VLAN Monitor Ports L2 Multicast L3 Interfaces Routing Set Diagnostics ✓ System ✓	iecurity \checkmark Advanced \checkmark
Type Administrative Distance ID	Action
No Data	
 Passive Interface RIP update packets will be suppressed on the passive interface. If the device connected to the interface are advised to enable this function. 	erface does not adopt RIP, you
Passive Interface +	- Add 🔲 🗇 Delete Selected
Port Name	Action
No Data	
<i>i</i> Neighbor Route If a router cannot forward broadcast packets, another router is designated as the neighbor to establish	ablish a RIP direct link.
Neighbor Route +	- Add 🔟 Delete Selected
Address	Action
No Data	

R Local Device(NBS ~	Currently in Local Devic	e mode.		English 🗸 🛆 🧟 🗗
Switch IP Add • NB56002 Software	ame: Ruijie ress: 192.168.110.62 MA Ver: ReyeeOS 1.218.2421	SN: MACCNBS600 C Address: 00:D0:F8:9 Hardware Ver: 1.00	0HQ 5:68:5E DNS: 192.168.110.1	(1) Reboot
Home VLAN Monitor	Y Ports Y 12 Multica	ast 1.3 Interfaces `	Routina Security Security	Advanced Y
Diagnostics × System ×	Add		×	
Route Redistribution	* Passive Interface	Select	~]	Delete Selected
П Туре			Cancel	Action
Passive Interface RIP update packets will b are advised to enable th	be suppressed on the passive is function.	interface. If the device	e connected to the interface doe	s not adopt RIP, you
Passive Interface			+ Add	Delete Selected
	Port Name		Action	
		No Data		
Neighbor Route If a router cannot forward	d broadcast packets, anothe	r router is designated -	as the neighbor to establish a RI	P direct link.
Neighbor Route			+ Add	Delete Selected
	Address		Action	

16.3.6 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, click Add, and enter the IP address of the neighbor router.

R Local Device(NBS V	Currently in Local Device mode.		English -> 🛆 🛕 🕞
Swech Hostname IP Address IP Address • NBS6002 Software Ver	: Ruijie SN: M/ : 192.168.110.62 MAC Address: : ReyeeOS 1.218.2421 Hardwan	CCN856000HQ 00:D0:F8:95:68:5E 9 Ver: 1.00 DNS: 192.168.110.	() Reboot
Home VLAN Monitor Y Diagnostics Y System Y	Ports Y 12 Multicast 13 Ir Add	nterfaces <u>× Routino × Security</u> × ×	Advanced Y
Туре	* Neighbor Route		Action
Passive Interface RIP update packets will I are advised to enable this to	nction.	Cancel OK	es not adopt RIP, you
Passive Interface		+ Add	Delete Selected
0	Port Name	Action	
	No	Data	
Neighbor Route If a router cannot forward b	roadcast packets, another router is c	lesignated as the neighbor to establish a RI	P direct link.
Neighbor Route		+ Add	Delete Selected
	Address	Action	
	No	Data	

Cur	rently in Local Device mode.		Enç	glish ~ 🛆	ê 🗗
Hostname: R IP Address: 19 • NBS6002 Software Ver: R Home VI AN Monitor × P	uijie SN: MA 32.168.110.62 MAC Address: 3yeeOS 1.218.2421 Hardware	ACCNBS6000HQ 00:D0:F8:95:68:5E e Ver: 1.00	DNS: 192.168.110.1	() Re	eboot
Diagnostics × System ×					
RIP Settings Port Settings Neighbor Info	Advanced Neighbor Info				
Neighbor Address Version	otocol Local Address	Connected Interface	Rx Error Packets	Rx Error Ro	outes
	No	Data			
< 1 > 10/page >	Go to page 1			I	lotal 0

16.4 Configuring RIPng

16.4.1 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.

Ruíjie Rcycc	Local Device/NBS 👳	English ~ _ ORemote O&M _
പ്പം Home	RIP Settings Port Settings Advanced Neighbor Info	
≝ [₽] VLAN	Laver-3 Routing Protocol: RIP	
Monitor	() RP(Routing information Protocol) is a dynamic routing protocol applied to IPv4 networks. The routers running the obtain routes to remote networks and keep routes updated in real time.	e protocol exchange the routing information through UDP packets to automatically
Ports	Network Segment/Port List	
 L2 Multicast 	Enable RIP in the specified network segment or on the specified port.	
L3 Multicast	Network Segment/Port List	+ Add Delete Selected
L3 Interfaces		
Routing	No. Network Segment/Port Auth Mod	e Action
Static Routing	1 VLAN 1 No Authentice	ition Edit Delete
Static Routing_v6		
RIP Settings		
RIPng Settings		
OSPFv2		
«Collapse		

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.

Ruíjie Royco		English 🗸 🛆 🔮 🕞
🖧 Home	RIP Settings Port Se	v l
≝ VLAN	Add	^
Monitor 🗸	RIP (Routing Inform information throug Type • Network Segment	Port ers running the protocol exchange the routing es updated in real time.
Ports	Network Segmen * Network Segment Please enter a valid value.	Example
L2 Multicast	Enable KIP in the s	
L3 Multicast	Network Segmen	cel OK + Add Delete Selected
L3 Interfaces	No. Notwark Sourcest/Best	uth Made
Routing	No. Network segment/Port A	Action
Static Routing	I VLAN 1 No A	uthentication Edit Delete
Static Routing_v6		
«Collapse		

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

Reycc	Local Device(NBS V			English 🗸 🛆 🔮 🕞
🖧 Home	RIP Settings Port Se		~	
^{£⊕} ∋ [≠] VLAN	Laver-3 Routing	Add	×	
🐏 Monitor 🛛 👋	<i>information throug</i>	Туре	Network Segment • Port	ters running the protocol exchange the routing es updated in real time.
Ports	Network Segmen	* Port	Select ~	
L2 Multicast	Enable RIP in the s	Auth Mode	No Authentication	
L3 Multicast	Network Segmen			+ Add 🗇 Delete Selected
L3 Interfaces `` ` ``	No		Cancel	Action
Routing				Action
Static Routing	- 1	VLAN 1	No Authentication	Edit Delete
Static Routing_v6				
«Collapse				

Alternatively, enable RIPng on a specified port:

Table 16-7 RIPng Configuration Parameters

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 .

16.4.2 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.

Rujje	Local Device(NBS >>					English ~ 🛆 Re	mote O&M 🛛 👲 Network Co	onfiguration 🕒 Log Out
🖧 Home	RIP Settings Port Settin	gs Advanced	Neighbor Info					
ar VLAN								
🔄 Monitor	Port List							
Ø Ports	Port Name	Rx Status	Tx Status	Poison Reverse	v2 Broadcast Packet	Auth Mode	Auth Key	Action
L2 Multicast	VLAN 1	v2	v2	Off	On	No Authentication	No Authentication	Edit
🛆 L3 Multicast								
L3 Interfaces `` ` ` `								
Routing								
Static Routing								
Static Routing_v6								
RIP Settings								
RIPng Settings								
OSPFv2								
«Collapse								

Edit		×
* Port Name	VLAN 1 ~	
Rx Status	 Disable v1 v2 	
Tx Status	 Disable v1 v2 	
Poison Reverse		
v2 Broadcast Packet		
Auth Mode	No Authentication \sim	
	Cancel	OK

16.4.3 Configuring the RIPng Global Configuration

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

Ruíjie Rcycc	Local Device(NBS V	English 🗸 🛆 🛕 🗄	€
A Home	RIP Settings Port Settings Advanced Neighbor Info		1
≟ [□] ∕ VLAN			
쭏 Monitor 🗸	Improper timers may cause route happing. Inerefore, KIP timers must be consistent on the devices connected to the same netw advised to reset the RIP timers unless you have specific needs.	work. You are not	
Ports	RIP Global Config	Edit Config	
 L2 Multicast 	RIP Version Route Advertisement Administrative Update Timer Invalid Timer	Flush Timer	l
L3 Multicast	Default On 1 (Default) 30 s 180 s	120 s	
L3 Interfaces			
Routing	Route Redistribution List Redistribute the routes of other protocols to the RIP domain so that RIP can communicate with other routing domains.		
Static Routing	Route Redistribution List + Add	Delete Selected	
Static Routing_v6	Type Administrative Distance Instance ID	Action	4
«Collapse			2

R Local Device(NBS V	Currently in Local Device mode		English 🗸 🛆 🛕 🕞
Hostna IP Add • NBS6002 Software Home VLAN Monitor I Diagnostics ~ System ~	ame: Ruijie SN: ress: 192.168.110.62 MAC Addin Ver: ReyeeOS 1.218.2421 Hardv ≤ Ports ≤ 1.2 Multicast L Edit Config	MACCNBS6000HQ ess: 00:D0:F8:95:68:5E eare Ver: 1.00 DNS: 192.168.* 3 Interfaces × Routino × Securit ×	() Reboot 110.1 N × Advanced ×
RIPng Settings Port Settin	Route Advertisement		
<i>improper timers may can</i> network. You are not ad	Administrative 1 (E	efault) ~	nnected to the same
RIPng Global Config	* Update Timer 30	s (1-65535)	Edit Config
Route Advertisement	* Invalid Timer 180	s (1-65535)	Flush Timer
Off			120 s
Route Redistribution Redistribute the routes of	* Flush Timer 120	s (1-65535)	ting domains.
Route Redistribution		Cancel	Delete Selected
Туре	e Admi	nistrative Distance	Action
	4	lo Data	
Passive Interface RIP update packets will b are advised to enable thi	e suppressed on the passive interfaces in the suppressed on the passive interfaces in the superscript of the	e. If the device connected to the interface	o does not adopt RIP, you

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 route is completely deleted from the RIP routing table. The default value is 120 seconds.

Table 16-8 RIPng Global Configuration Parameters

16.4.4 Configuring the RIPng Route Redistribution List

Redistribute routes of other protocols to the RIPng domain to interwork with other routing domains.

Choose Local Device > Routing > RIPng Settings > Advanced, and click + Add.

R Local Device(NBS ~	Currently in Local Devic	e mode.		English -> 🛆 🔮 🕞
Hostna Switch IP Addr • NB56002 Software V	me: Ruijie ess: 192.168.110.62 MA _{Ver:} ReyeeOS 1.218.2421	SN: MACCNBS6000HQ C Address: 00:D0:F8:95:68:5E Hardware Ver: 1.00	DNS: 192.168.110.1	() Reboot
Home VLAN Monitor - Diagnostics - System -	Add	ast 1.3 Interfaces Y Routin	a × Security × ×	Advanced ~
RIPng Settings Port Setting	* Туре	Select	~	
Improper timers may car network. You are not ad	* Administrative Distance	0 (Administrative Distance)	nnec	ted to the same Edit Config
Route Advertisement		Cancel	ОК	Flush Timer
Off	1 (Default)	30 s	180 s	120 s
Route Redistribution L Redistribute the routes of	Route Redistribution List Redistribute the routes of other protocols to the RIP domain so that RIP can communicate with other routing domains.			
Route Redistribution	List		+ Add	Delete Selected
П Туре		Administrative Distance		Action
		No Data		
Passive Interface (i) RIP update packets will be are advised to enable this	e suppressed on the passive function.	interface. If the device connected	to the interface does i	not adopt RIP, you

Table 16-9 RIP Route Redistribution Parameters

Parameter	Description
	Direct Routing
Туре	OSPF Routing
	Static Routing
Administrative Distance	Value range: 0-16. The default value is 0 .

16.4.5 Configuring the RIPng Passive Interface

If an interface is configured as a passive interface, it will suppress RIPng update packets. If the connected peer device does not run RIP, you are advised to enable the passive interface.

Choose Local Device > Routing > RIPng Settings > Advanced, click Add, and enter the IP address of the neighbor router.

Currently in L	ocal Device mode.	English ~ 🛆 🔮 🕒
Hostname: Ruijie IP Address: 192.168.110 Software Ver: ReyeeOS 1.2 Home VLAN Monitor \checkmark Ports \checkmark	SN: MACCNBS6000HQ 1.62 MAC Address: 00:D0:F8:95:68:5E 218.2421 Hardware Ver: 1.00 L2 Multicast L3 Interfaces Y Routing	U Reboot
Diagnostics 🐃 System 🐃		
Туре	Administrative Distance	Action
	No Data	
 RIP update packets will be suppressed on are advised to enable this function. Passive Interface 	the passive interface. If the device connected t	to the interface does not adopt RIP, you + Add
Port Name		Action
	No Data	
<i>RIPng Aggregate Routing</i> Create an aggregate RIPng route announce	cement.	
RIPng Aggregate Routing		+ Add Delete Selected
Address		Action
	No Data	

Reyee Cookbook

R Local Device(NBS >	Currently in Local Device mode.		English 🗸 🛆 🧁	₿
Switch IP Addr NBS6002 Software	me: Ruijie SN: M ess: 192.168.110.62 MAC Address Ver: ReyeeOS 1.218.2421 Hardwa	ACCNBS6000HQ : 00:D0:F8:95:68:5E re Ver: 1.00 DNS: 1	92.168.110.1	t
Home VLAN Monitor S Diagnostics × System ×	Add	ntertaces × Routing ×	× Advanced ×	
Тур	* Passive Interface Select	~	Action	
RIP update packets will are advised to enable this	function.	Cancel	DK oes not adopt RIP, you	
Passive Interface			+ Add 🗇 Delete Selected	
	Port Name		Action	
	No	Data		
Create an aggregate RIP	ing g route announcement.			
RIPng Aggregate Rou	ting		+ Add 🗇 Delete Selected	
	Address		Action	
	No	Data		

16.4.6 Configuring the IPv6 Aggregate Route

Choose Local Device > Routing > RIP Settings > Advanced, click Add, and enter the IPv6 address and prefix length (value range: 0–128).

Local Device(NBS ~	Currently in Local Device mode			English -> 🛆 🔮 🗗
Switch IP Add • NBS6002 Software	ame: Ruijie SN: Iress: 192.168.110.62 MAC Addro Ver: ReyeeOS 1.218.2421 Hardv	MACCNBS6000HQ ss: 00:D0:F8:95:68:5E rare Ver: 1.00 DN:	_{S:} 192.168.110.1	() Reboot
Home VLAN Monitor Diagnostics ~ System ~	Add	3 Interfaces × Routing ×	Security, ~ ×	Advanced 🗡
Тур	* IPv6 Aggregate Routing			Action
Passive Interface RIP update packets will I are advised to enable th		Cancel	ОК	s not adopt RIP, you
Passive Interface			+ Add	Delete Selected
	Port Name		Action	
	٨	o Data		
Create an aggregate RIP	i ting Ing route announcement.			
RIPng Aggregate Roo	uting		+ Add	Delete Selected
	Address		Action	
	М	o Data		

16.5 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.

16.5.1 Configuring OSPFv2 Basic Parameters

Choose Local Device > Routing > OSPFv2, click Start Setup, and then configure an instance and an interface respectively.

Reyee Cookbook

Local Device(NBS Currently in Local Device mod	e. English ~ 🔿 🔮 🕞
Hostname: Ruijie SN: IP Address: 192.168.110.62 MAC Addr • NB56002 Software Ver: ReyeeOS 1.218.2421 Hard Home VLAN Monitor × Ports × L2 Multicast I Diagnostics × System ×	: MACCNBS6000HQ ress: 00:DD:F8:95:68:5E ware Ver: 1.00 DNS: 192.168.110.1 L3 Interfaces × Routing × Security × Advanced ×
	 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 protenses such as slow convergence, unscientific metric values, and poor scalability. Displication of the solution of t

(1) Configure an instance.

Currently in Local Device mode.	English ~	٥	٩	₿
				×
1 3 Configure the instance. Configure the interface. Operation succeeded	ed.			
* Instance ID				
* Router ID				
Advertise Default				
Route				
Import External Route Static Route Redistribution				
Direct Route Redistribution RIP Redistribution				
Details				
Previous Next				

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 configuration may cause neighbor discovery failures.
	Generate a default route and send it to the neighbor.
Advertise Default Route	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.
	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.
Import External Koute	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.

Table 16-10 Instance Configuration Parameters

Details			
Distance	Intra-Area	Optional.Default:110	
	Inter-Area	Optional.Default:110	
	External	Optional.Default:110	
LSA	Genaration D	Optional.Defa	
	Received Dela	ay Optional.Default	
SPF Calculation	Waiting Inter	val Optional.Defaul	
	Min Interval Optional.Default:50		
	Max Interval	Optional.Default:50	
Graceful Restart	Graceful Rest	tart 🚺	
	Hel	per	
	LSA Che	eck	
	* Max Wait Ti	me 1800	

Table 16-11 Parameters in the Instance Detailed Configuration

Parameter	Description
Distance	It is used for protocol selection. By default, the intra-area, inter-area, and external distances are all 110 .

Parameter	Description
LSA	Frequent network changes and route flapping may occupy too much network bandwidth and device resources. The LSA generation and reception delays are specified in OSPF by default. The default value is 1000 ms.
SPF Calculation	 When the link state database (LSDB) changes, OSPF recalculates the shortest path, and sets the interval to prevent frequent network changes from occupying a large number of resources Waiting Interval: When the state changes, the timer is triggered. The delay is calculated for the first time after the timer expires. The default value is 0 ms. Min Interval: As the number of changes increases, the time of each interval will increase according to the algorithm, and the default value is 50 ms. Max Interval: When the calculated interval reaches the maximum interval, the subsequent interval is always equal to the maximum interval. If the time from the last calculation exceeds the maximum interval and the LSDB is not updated, the timer is disabled.

Parameter	Description
	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.

(2) Configure an interface.

					Englist		Network Setup	
								×
	Configure the inst	2 ance. Configure the interface.						
	* Interface	Select v						
	* Area							
	Stub Area							
		Detail:						
	Priority	Optional.Default1						
		Add						
Port List								
Up to 16 entries can be added.								
Interface Area	Priority Network Type	Hello Packets De	ad Interval	Interface Auth	LSA Transmission Delay	LSA Retransmission	Interval	Action
		No Data						
< 1 > T0/page < Go to page 1								Total 0

Table 16-12 Interface Configuration Parameters

Parameter	Description
Interface	Select the OSPF-enabled L3 interface.

Parameter	Description	
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.	
	Inter-area route isolation: After this function is enabled, inter-area routes will not be imported to this area.	
Details	Expand the detailed configuration.	



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

Table 16-13 Parameters in the Interface Detailed Configuration

Parameter	Description
Priority	It is 1 by default.
	Broadcast
Network Type	Unicast
Network Type	Multicast
	Non-Broadcast Multiple Access
	Interval for periodic transmission, which is used to discover and maintain OSPF
Hello Packets	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.

Parameter	Description
LSA Retransmission Interval	Time after which LSA is retransmitted after LSA is lost. The default value is 5 seconds.
Interface Auth	No Auth: The protocol packets are not authenticated. It is the default value. Plain Text: The protocol packets are authenticated, and the authentication key is transmitted with the protocol packets in the form of plain text. MD5: The protocol packets are authenticated, and the authentication key is MD5 encrypted and then transmitted with the protocol packets.
Ignore MTU Check	Enabled by default.

(2) Complete the configuration.

After completing the configuration, you can choose **Local Device** > **Routing** > **OSPFv2** and view the instance list.
Ruíjie Rcycc	Currently in Local Device mode.	English ~	٥	٩	₽
	Operation succeeded.				×
	Image: Configure the instance. Image: Configure the interface. Image: Operation succeeded.				



Operation succeeded.

Disable

16.5.2 Adding an OSPFv2 Interface

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

ιλαί μ ε β		Currently in Local De	evice mode.		Englis	sh ~ 🛆 🔮 🗗
Switch • NBS6002	Hostnar MAC Addre DI	me: Ruijie ess: 00:D0:F8:95:68:5E NS: 192.168.110.1	SN: MACCNBS6000 Software Ver: ReyeeOS	HQ IP Address: 1 1.218.2421 Hardwar	92.168.110.62 e Ver: 1.00	(U) Reboot
Home VLAN System ~	Monitor ~	Ports 🐃 L2 Mu	lticast L3 Interfaces ~	Routing ~ Securit	y 🎽 Advanced 🎽 Dia	gnostics ~
Instance List	:					+ Add
Up to 16 entrie	es can be added.					
Instance ID	Router ID	Interface	Area	Advertise Default Route	Import External Route	Action
12	123.1.1.1	VLAN 1	23(stub)	Enable	Static Route Redistribution : On Direct Route Redistribution : On RIP Redistribution : On	More Neighbor Info Edit Delete
	10/page 🗸	Go to page	1			Total 1

Ruijie I ®Rcy		Currently in Local Dev	vice mode.		English ~ 🛆 🧟	Ð
Switch • NBS6002	Hostnar MAC Addre Di	ne: Ruijie ess: 00:D0:F8:95:68:5E NS: 192.168.110.1	SN: MACCNBS Software Ver: Reye	6000HQ IP Address: 192.168.110.62 eeOS 1.218.2421 Hardware Ver: 1.00	(U) Rebo	ot
Home VLAN System ~	Monitor ~	Ports 🐃 L2 Mult	ticast L3 Interfaces	Conting Security Advanced Continues	Diagnostics 🗡	
Instance List	:				+ Ad	ld
Up to 16 entrie	es can be added.					
Instance ID	Router ID	Interface	Area	Advertise V2 Interface	Action	
12	123.1.1.1	VLAN 1	23(stub)	V2 Instance Route Redistribution V2 Stub Area Management V2 Neighbor Management	More eighbor Inf dit Delete	io e
< 1 >	10/page 🗸	Go to page	1		Tota	d 1

Rujje SRcycc L a	irrently in Local Device m	iode.					Englis	sh ~ 🖒	@ (3
Hostname	V2 Interface								×	<
Switch MAC Addres NBS6002 DN	Interface	Select		· · · · · · · · · · · · · · · · · · ·	~					
Home VLAN Monitor ~	* Area									
System ~	Priority	Optional D)efault:1							
Instance List			ordard I							
Up to 16 entries can be added.	Network Type	Broadcast			~					
	Hello Packets	Optional.D	efault:10(s)						
Instance ID Router ID	Dead Interval	Ontional D	efault:40(s			_				
	Port List						Add	Re	eset	
12 123.1.1.1	Up to 64 entries can	be added.								
	Interfac		Networ	Hello	Dead	Interfac	LSA Transmi	LSA Retrans		
< 1 > 10/page ~	Area e	Priority	k Type	Packets	Interval	e Auth	ssion Delay	mission Interval		Act
	VLAN 1 23		Broadca st			No Auth			Ed	lit
	< 1 > 10/	/page ∨	Go to pa	ge 1					Total	1
Hostname: Ruijie • NB55100- 24GT45FP-P Home VLAN Monitor * Ports * L2 Multicast	SN: G15K375000148 IP Address: Jardware Version: 1.19 DNS: 1 L3 Multicast L3 Interfaces Y Routin	192.168.110.5 MA 92.168.110.1 g <u> </u>	V2 Interfac	e Interface Select		~			×	
Instance List				tub Area						
up to a chines can be auded.			Port List	300			Add	Reset		
Instance ID Router ID	Intelface	Area	Up to 64	entries can be added.						
4 4323	VLAN 1	3(Normal Area)	Interfac	Area Priority	Networ k Type	Hello Dead Packets Interval	LSA Interfac Transmi e Auth ssion	LSA Retrans mission	Act	
Go to page 1			VLAN 1	3	Broadca st		Delay No Auth	Interval	Edit	
			< 1	> 10/page v	Go to page	e 1		To	otal 1	

16.5.3 Redistributing OSPFv2 Instance Routes

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

Rujje		rrently in Local Device m	ode.				English	~ O		G
Switch	Hostname MAC Addrese	V2 Instance Route Rec	listribution		• •					×
NBS6002 Home VLAN	DNS Monitor 🗡	* Instance ID	ution cannot Select	select its own	instance nu	mber!				
System ~		Metric	Optional.De	efault:20						
Up to 16 entrie	s can be added.	Route Redistribu	tion List				Add	R	eset	
		Up to 63 entries can	pe added.							
Instance ID	Router ID	Instance ID Metric				Metric		Ac	tion	
					No Data					
12	123.1.1.1	< 1 → 10/	page 🗸	Go to page	1				To	otal 0
< 1 >	10/page v									

16.5.4 Managing OSPFv2 Neighbors

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

Ruíjie l Rcycc L	Currently in Local Device mode.		English	× 🛆 🔮 🗗
Switch Hostn MAC Add • NBS6002	V2 Neighbor Management			×
Home VLAN Monitor ~ System ~	Neighbor List		Add	Reset
1	Up to 64 entries can be add	ed.		
Up to 16 entries can be adde	d.	Neighbor IP		Action
		No Data	à	
Instance ID Router ID	< 1 > 10/page	 Go to page 1 		Total 0
12 123.1.1.1				
< 1 > 10/page >				

16.5.5 Viewing OSPFv2 Neighbor Information

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

Ruíjie \$Rcycc	Currently in Local Device mode.			English ~	∕ △ 🔮 🗗
Switch Hostna Switch MAC Add • NBS6002	nes Neighbor Info				×
Home VLAN Monitor ~	Instance ID	Router ID	Status	Neighbor IP	Interface
System ~			No Data		
Instance List	< 1 > 10/page	✓ Go to page	1		Total 0
Up to 16 entries can be added	ł				
Instance ID Router ID					
12 123.1.1.1					
< 1 > 10/page <					

16.6 OSPFv3

Open Shortest Path First (OSPF) can be applied to large-scale networks. IPv4 uses OSPFv2, and IPv6 uses OSPFv3.

16.6.1 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.



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.

Rujje	Local Device(NBS 🗸	Currently in Local Device mode.		English ~	٥	٩	₽
							×
	1 Configure the insta	(2) ance. Configure the interface.					
	* Router ID	_	0				
	Advertise Default						
	Route						
	import External Route	 Static Route Redistribution Direct Route Redistribution 					
		RIP Redistribution					
	Advertise Default Route Import External Route	 Static Route Redistribution Direct Route Redistribution RIP Redistribution Details 					



Table 16-14 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.

Reyee Cookbook

Parameter	Description
Router ID	It identifies a router in an OSPF domain. 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.
Details	Expand the detailed configuration.

Ruíjie ®Rcycc	Local Device(NBS >	Currently in Lo	cal Device mode.			English ~	٥	٩	₽
									×
	1		2		3				
	Configure the insta	ance. Configu	ure the interfac	e. Oper	ation succeeded.				[
	* Router ID				0				
	Advertise Default								
	Route	Metric	Optional.Default:1						
		Type 2		\sim	0				
	Import External Route	Static Route	Redistribution						
		Metric	Optional.Default:20)					
		Direct Route	e Redistribution						
		Metric	Optional.Default:20)					
		RIP Redistri	Oution						
		Metric	Optional.Delauti.20	J					
		De	etails						
	Distance	Intra-Area	Optional.Defau	lt:110					
		Inter-Area	Optional.Defau	lt:110					
		External	Optional.Default:	110					
	LSA	Genaration [Delay Optiona	ıl.Defaı					
		Received De	lay Optional.[Default					
		Previ	ous Next						

Ruíjie	Local Device(NBS 🗸	Currently in Loo	al Device mode.	English ~	۵	٩	G
							×
	1		3				
	Configure the insta	ance. Configu	re the interface. Operation succeeded.				
		RIP Redistrib	ution				
		Metric C	Optional.Default:20				
		De	tair				
	Distance	Intra-Area	Optional.Default:110				
		Inter-Area	Optional.Default:110				
		External	Optional.Default:110				
	LSA	Genaration D	Pelay Optional.Defa				
		Received Del	ay Optional.Default				
	SPF Calculation	Waiting Inter	val Optional.Defaul				
		Min Interval	Optional.Default:50				
		Max Interval	Optional.Default:50				
	Graceful Restart	Graceful Rest	art 🔵				
		Hel	per				
		LSA Che	eck				
		* Max Wait Ti	me 1800				
		Previo	ous Next				

Table 16-15 Parameters in the Instance Detailed Configuration

Parameter	Description
Distance	It is used for protocol selection. By default, the intra-area, inter-area, and external distances are all 110 .

Parameter	Description
LSA	Frequent network changes and route flapping may occupy too much network bandwidth and device resources. The LSA generation and reception delays are specified in OSPF by default. The default value is 1000 ms.
SPF Calculation	 When the link state database (LSDB) changes, OSPF recalculates the shortest path, and sets the interval to prevent frequent network changes from occupying a large number of resources Waiting Interval: When the state changes, the timer is triggered. The delay is calculated for the first time after the timer expires. The default value is 0 ms. Min Interval: As the number of changes increases, the time of each interval will increase according to the algorithm, and the default value is 50 ms. Max Interval: When the calculated interval reaches the maximum interval, the subsequent interval is always equal to the maximum interval. If the time from the last calculation exceeds the maximum interval and the LSDB is not updated, the timer is disabled.

Parameter	Description
Parameter Graceful Restart	Description Graceful Restart (GR) can avoid route flapping caused by traffic interruption and active/standby board switchover, thus ensuring the stability of key services. Graceful Restart Helper: The Graceful Restart Helper function is enabled when this switch is turned on. LSA Check: LSA packets outside the domain are checked when this switch is turned on.
	Max Wait Time: Timing starts after the device receives the GR packet from the peer device.
	If the peer device does not complete GR
	within Max Wait Time, the device exits the
	GR Helper mode. The default value is 1800
	seconds.

2. Configure an interface.

Ruíjie	#Rcycc	Local Device(NBS 🗸	Currently in Local	I Device mode.			English ~	٥	٩	₽
										×
		1				3				
		Configure the inst	ance. Configur	e the interfac	e. Op	peration succeeded	Ι.			
		* Interface	Gi2/14		~					
		* Area	12							
		Stub Area								
			Deta	ils						
De ut Lint			Add	d						
Port List										
Up to 16 e	ntries can be adde	ed.								
Interface	Area	Priority Ne	twork He Type Pack	llo D kets Int)ead terval	LSA Transmission R Delay	LSA etransmissi on Interval	Act	ion	
			١	No Data						
< 1	> 10/page	✓ Go to page 1							То	tal 0
					_					
			Previous	s Finish						

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.

Table 16-16 Interface Configuration Parameters

Ruijie l Rcy	/CC Local		Currently	in Local Device	mode.		English	0	۵
	Cc	1 onfigure the ins	stance. C	2 onfigure the in	iterface. O	3 peration succeed	led.		×
				Details					
		Priorit	by Option	al.Default:1			1		
		Network Typ	Broadd	ast					
		Hello Packet	ts Option	al.Default:10(s)			1		
		Dead Interv	al Option	al.Default:40(s)					
Port List				Add					
Up to 16 entries ca	n be added.								
Interface	Area F	Priority P	Vetwork Type	Hello Packets	Dead Interval	LSA Transmission Delay	LSA Retransmissi on Interval	Act	ion
				No Data					
	0/page \vee	Go to page 1							Total 0
				Previous	Finish				

Rujje	Local Device(NBS >	Currently in Local Device	mode.		English ~	0	e 1	
	1) Configure the insta	2 ance. Configure the ir	nterface. Op		ed.)	×
	LSA Transmission Delay	Optional.Default:1(s)						
	LSA Retransmission Interval	Optional.Default:5(s)						
1	Ignore MTU Check	Add						
Port List								
Up to 16 entries can be added	ł.							
Interface Area	Ne Priority 1	twork Hello Type Packets	Dead Interval	LSA Transmission Delay	LSA Retransmissi on Interval	Actio	n	
		No Data						
< 1 > 10/page >	Go to page 1						Tota	ы O
		Previous	Finish					

Ruijie	Rcycc	Local Device(NBS \sim	Curren	tly in Local Device mode			English ~	٥		Ð
		(1) Configure the in	stance.	2 Configure the interfa	ce. O	3 Operation succeeded	I.			×
		LSA Transmissio Del	on Opti	onal.Default:1(s)						
		LSA Retransmissio	on Opti	onal.Default:5(s)						
		Ignore MTU Che	ck 🚺	Add						
Port List										
Up to 16	entries can be adde	d.								
Interface	Area	Priority	Network Type	Hello Packets II	Dead nterval	LSA Transmission R Delay o	LSA etransmissi on Interval	Acti	on	
Gi2/14	12	E	Broadcast					Dele	ete	
< 1	> 10/page	Go to page 1							To	tal 1
			l	Previous Finisl	h					

Table 16-17 Parameters in the Interface Detailed Configuration

Parameter	Description
Priority	It is 1 by default.

Parameter	Description
Network Type	Broadcast Unicast Multicast Non-Broadcast Multiple Access
Hello Packets	Interval for periodic transmission, which is used to discover and maintain OSPF neighbor relationship. The default value is 10 seconds.
Dead Interval	Time after which the neighbor becomes invalid. The default value is 40 seconds.
LSA Transmission Delay	LSA transmission delay of the interface. The default value is 1 second.
LSA Retransmission Interval	Time after which LSA is retransmitted after LSA is lost. The default value is 5 seconds.
Interface Auth	 No Auth: The protocol packets are not authenticated. It is the default value. Plain Text: The protocol packets are authenticated, and the authentication key is transmitted with the protocol packets in the form of plain text. MD5: The protocol packets are authenticated, and the authentication key is MD5 encrypted and then transmitted with the protocol packets.
Ignore MTU Check	Enabled by default.

3. Complete the configuration.

Rujje	Local Device(NBS 🗸	Currently in Local Device mode.		English ~	۵	٩	₿
	•	Operation succeeded.					×
	1	2	3				
	Configure the inst	ance. Configure the interface.	Operation succeeded.				





After completing the configuration, you can choose **Local Device** > **Routing** > **OSPFv**3 and view the instance list.

16.6.2 Adding an OSPFv3 Interface

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

Ruíjie	#Rcycc	Loca	I Device(NBS 🗸	Currently in Loca	l Device mode.			English ~	0	\$\]
• NBS	ich 6002	Hostnan MAC Addre Df	ne: Ruijie Iss: 00:D0:F8:95:68:51 NS: 192.168.110.1	SN: MACC	NBS6000HQ IP ReyeeOS 1.218.2421	Address: 192.168 Hardware Ver:	8.110.62 1.00	× Diagnor	(U) Re	eboot
System		onitor				Security	Auvanceu	Diagnos	ues.	
OSPFv	3									
Up to 1	l entries can	be added.								
Router I	D Interf	ace	Area	Advertise Default Route	Import External Route	Distance	SPF Calculatio n	Graceful Restart Helper	Acti	on
2.2.2.2	Gi2/	14	12(Normal Area)	Disable	S V3 Interface Redis D V3 Stub Area Redistribution : Off	a Management			Ma eighb Edit [ore or Info Delete
< 1	> 1	0/page 🗸	Go to page	1					-	Total 1

Rujje sRcycc Local	Device(NBS 🗸 Curre	ently in Local Device mo	ode.		English ~) 🔒 🕞
Hostnam	V3 Interface					×
Switch MAC Addres NBS6002 DN:	Interface	Select	~			
Home VLAN Monitor ~	* Area					
System ~	Priority	Optional.Default:1				
OSPFv3						l
Up to 1 entries can be added.	Network Type	Broadcast	~			
	Hello Packets	Optional.Default:10(s)			
Router ID Interface	Dead Interval	Ontional Default:40(s)			
	PortList			Add		Reset
2.2.2.2 Gi2/14	Up to 64 entries can	be added.				
< 1 > 10/page <	Interfac Area e	Priority Networ k Type	Hello Dead Packets Interva	LSA L: Transmi Ret I ssion mis Delay Inte	SA rrans ssion erval	Action
	Gi2/14 12	Broadca st			Edi	t Delete
	< 1 > 10,	′page ∨ Go to p	age 1			Total 1
Hostname: Ruijie NBS5100- Software Version: ReverOS 2.248.0.2305	SN: G15K37500014B IP Ad	V Idress: 192.168.110.5 MAC Ac	3 Interface			×
24GT4SFP-P Home VLAN Monitor Y Ports Y L2 Multicast	: L3 Multicast L3 Interfaces ~ F	Routing Y Security Y Adv	* Area			
OSPFv3			Stub Area 🗾			
Up to 1 entries can be added.			Area Type stub	~		la contra con
Router ID Interface	Area Ac	dvertise Default Import Route	Ip to 64 entries can be added.		Add	Reset
T.S.L.F. VLAN 1	34(Normal Area)	Static Route Disable Direct Route RIP Red In	terfac Area Priority N e k	ietwor Hello Dead Type Packets Interval	LSA LSA Transmi Retrans ssion mission Delay Interval	Action
T0/page Go to page 1		V	AN 1 34 B	roadca st		Edit Delete
			1 > 10/page v	Go to page 1		Total 1

16.6.3 Viewing OSPFv3 Neighbor Information

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

Rujje SRcycc Loca	I Device(NBS 🗸	Currently in Local I	Device mode.		English ~	0	è ⊡
Bwitch Hostnam Switch MAC Addre • NBS6002 DN	^{s:} Neighbor I	nfo					×
Home VLAN Monitor ~	R	outer ID		Status	Interfa	ce	
System ~				No Data			
OSPFv3	< 1 >	10/page 🗸	Go to page	1			Total 0
Up to 1 entries can be added. Router ID Interface							
2.2.2.2 Gi2/14							
1 > 10/page							

16.7 Routing Table Info

	/CC Local De	evice(NBS 🗸 🗸 🗸	Currently in Local Device mode.			English \sim	0 🖗 🗗
Switch • NBS6002	Hostname: F MAC Address: 0 DNS: 1	Ruijie 00:D0:F8:95:68:5E 192.168.110.1	SN: MACCNBS6000HQ Software Ver: ReyeeOS 1.218.2	IP Address 421 Hards	s: 192.168.110.62 ware Ver: 1.00		() Reboot
Home VLAN System ~	Monitor 🎽 Po	orts 🎽 L2 Multic	ast L3 Interfaces × Routi	ng Y Seci	urity ~ Advance	ed 🌱 Diagnostic	cs ~
IPv4 IPv6							
Route Info				Entry Type	Global Data	د ~	Re-fetch
Dest IP Add	dress	Route Type	Distance/Metric		Interface	Next H	юр
0.0.0.0/	0	System routing	[0/5]		VLAN 1	192.168.	110.1
192.168.110	0.0/24	Direct Routing	[0/0]		VLAN 1	*	
< 1 >	10/page \vee	Go to page 1					Total 2
Rujje	/CC Local De	evice(NBS 🗸 🗸	Currently in Local Device mode.			English ~	△ 🏾 🗗
Ruffe Rcy Switch • NBS6002	Acc Local De Hostname: R MAC Address: C DNS: 1	evice(NBS > C Ruijie 00:D0:F8:95:68:5E 192.168.110.1	SN: MACCNBS6000HQ Software Ver: ReyeeOS 1.218.2	IP Address 421 Hards	s: 192.168.110.62 ware Ver: 1.00	English ~	 △ ♠ ➡ △ № (¹) Reboot
NBS6002 Home VLAN System ~	Hostname: F MAC Address: C DNS: 1 Monitor Y Po	evice(NBS > C Ruijie 00:D0:F8:95:68:5E 192.168.110.1 rrts > L2 Multic	SN: MACCNBS6000HQ SN: MACCNBS6000HQ Software Ver: ReyeeOS 1.218.2 ast L3 Interfaces × <u>Routi</u>	IP Address 421 Hard ng V Sect	s: 192.168.110.62 ware Ver: 1.00 urity ~ Advance	English ~	 △ ♠ ➡ ○ Reboot cs ×
NBS6002 Home VLAN System ~	CC Local De Hostname: F MAC Address: 0 DNS: 1 Monitor ⊻ Po	evice(NBS >) Ruijie 00:D0:F8:95:68:55 192.168.110.1 orts > L2 Multic	SN: MACCNBS6000HQ Software Ver: ReyeeOS 1.218.2 ast L3 Interfaces × <u>Routi</u>	IP Address 421 Hardn ng ⊻ Sect	s: 192.168.110.62 ware Ver: 1.00 urity ~ Advance	English ~	C ♠ ➡ () Reboot cs ×
NBS6002 Home VLAN System ~	Acc Local De Hostname: F MAC Address: 0 DNS: 1 Monitor ∨ Po	evice(NBS > C Ruijie 00:D0:F8:95:68:5E 192.168.110.1 orts > L2 Multic	Currently in Local Device mode. SN: MACCNBS6000HQ Software Ver: ReyeeOS 1.218.2 ast L3 Interfaces × <u>Routi</u>	IP Address 421 Hard ng <u>Sec</u> Entry Type	s: 192.168.110.62 ware Ver: 1.00 urity ~ Advance Global Data	English ~	C ♠ C () Reboot Cs →
Switch • NBS6002 Home VLAN System V IPv4 IPv6 Route Info Dest IP Add	CC Local De Hostname: F MAC Address: C DNS: 1 Monitor ∨ Po	evice(NBS > C Ruijie 00:D0:F8:95:68:5E 192.168.110.1 orts > L2 Multic	Currently in Local Device mode. SN: MACCNBS6000HQ Software Ver: ReyeeOS 1.218.2 ast L3 Interfaces Y Routi	IP Address 421 Hard ng Y Sect Entry Type	s: 192.168.110.62 ware Ver: 1.00 urity ~ Advance Global Data Interface	English ~	C ♠ C Reboot CS → Re-fetch
Switch • NBS6002 Home VLAN System IPv4 IPv6 Route Info Dest IP Add	VCC Local De Hostname: F MAC Address: O DNS: 1 Monitor \checkmark Po	evice(NBS > C Ruijie D0:D0:F8:95:68:5E 192.168.110.1 orts > L2 Multic Route Type	Currently in Local Device mode. SN: MACCNBS6000HQ Software Ver: ReyeeOS 1.218.2 ast L3 Interfaces Y <u>Routi</u> Distance/Metric No Data	IP Address 421 Hard ng <u>~</u> Sect	s: 192.168.110.62 ware Ver: 1.00 urity ~ Advance Global Data Interface	English ~	C A C

17 NBS and NIS Series Switches Security

17.1 DHCP Snooping

17.1.1 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.

17.1.2 Standalone Device Configuration

Choose Local Device > Security > DHCP Snooping.

Turn on the DHCP snooping function, select the port to be set as trusted ports on the port panel and click **Save**. After DHCP Snooping is enabled, request packets from DHCP clients are forwarded only to trusted ports; for response packets from DHCP servers, only those from trusted ports are forwarded.

🚺 Note

Generally, the uplink port connected to the DHCP server is configured as a trusted port.

Option 82 is used to enhance the DHCP server security and optimize the IP address assignment policy. Option 82 information will be carried in the DHCP request packet when Option 82 is turned on.

DHCP	Snoopir	ng: (
_																								
O	ption 82	: (
Select Tru	usted Po	ort:																						
Select Tru Available	rusted Po	ort: navaila	able												Ag	gregat	e	U	plink	-	Copp	oer	Fi	ber
Select Tru Available 1 3	usted Po	ort: navaila 9	able 11	13	15	17	19	21	23	25	27	29	31	33	Ag 35	gregat 37	e 1	41	plink 43	45	Copr 47	ber 49	51	ber
Select Tru Available	Ur Ur 5 7	ort: navaila 9	able 11	13	15	17	19	21	23	25	27	29	31	33	1 Ag	gregat 37	e 1	41	plink 43	45	Copr 47	der 49	51	ber

17.1.3 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	82	٩	@	١	Ð
Q													
ⓓ													
ጽ													
					Snoor	aing							
11				DHCP sr	nooping v	vill prevent rogue							
8				DHCP se	ervers offe	ering IP addresses							
-0-				to DHCF	P clients to	o ensure the							
			[stability Enab	of the ne	twork.							
>>													

(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. After the configuration is delivered, if you want to modify the effective range of the DHCP Snooping function, click **Configure** to select desired switches in the topology again. Turn off **DHCP Snooping** to disable DHCP Snooping on all switches with one click.



17.2 Storm Control

17.2.1 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.

17.2.2 Procedure

Choose Local Device > Security > Storm Control.

Click **Batch Edit**. In the displayed dialog box, select configuration types and ports, enter the rate limits of broadcast, unknown multicast, and unknown unicast, and click **OK**. To modify or delete the rate limit rules after completing the configuration, you can click **Edit** or **Delete** in the **Action** column.

There are two configuration types:

• Storm control based on packets per second: If the rate of data flows received over a device port exceeds the configured packets-per-second threshold, excess data flows are discarded until the rate falls within the threshold.

Storm control based on kilobytes per second: If the rate of data flows received over a device port exceeds the configured kilobytes-per-second threshold, excess data flows are discarded until the rate falls within the threshold.

Port List				🖉 Batch Edit	🗇 Delete S	elected	
	Port	Broadcast	Unknown Multicast	Unknown Unicast	Actio	on	
	Gi35	1000pps	1000pps	1000pps	Edit De	elete	
Batch Ec	lit						×
	Broadcast:	A blank value ind	icates no limit.	kbps Range: 16	5-1000000 (1000M)	
						,	
Unknow	n Multicast:	A blank value ind	icates no limit.	kbps Range: 16	5-1000000 (1000M)	
Unkno	wn Unicast:	A blank value ind	icates no limit.	kbps Range: 16	5-1000000 (1000M)	
*	Select Port:						
Availa	able 💼 Un	available 💼 Aggreg	ate 💼 Uplink 💼	Copper Fiber			
1	357	9 11					
2	4 6 8	10 12					
Note: You	can click and	l drag to select one c	or more ports.		Select All	Inverse	Deselect
				Cal	ncel	C	эк

17.3 ACL

17.3.1 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.

17.3.2 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-based access control: Regulates the flow of Layer 2 packets entering and exiting ports, allowing or denying specific packets based on their Layer 2 addresses.
- IPv4-based access control: Regulates the flow of IPv4 packets entering and exiting ports, allowing or denying specific packets based on their IPv4 addresses.
- IPv6-based access control: Regulates the flow of IPv4 packets entering and exiting ports, allowing or denying specific packets based on their IPv4 addresses.

ACL List	ACL Binding	9				
ACL					+ Add	i Delete Selected
Up to	512 entries can	be added.				
	ACL Na	me	ACL Type	Status		Action
			No Data	1		
Add						×
	* ACL Name:	Example: Server A	CL.			
	ACL Type:	• Based on MAC	Based on IPv4	Address 🔿 Base	ed on IPv6 Addre	255
				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			+ 4	Add Delete Selected
Up to 5	12 entries can be added.			
	ACL Name	ACL Type	Status	Action
	test	Based on MAC	Inactive	Details Edit Delete

RUTTE RCYCC Local Device(NIS: < Currently in Local Device mode.		English ∽ Remote O&M	음 Network Configuratio	on 🕞 Log Out
Hostname Ruije SN: G1QH1EH002322 NIS3100- Software Version: Reyer05 2.239.02118 Hardware Version: 1.00 Gottage Version: Reyer05 2.239.02118 Hardware Version: 1.00 Gottage Version: Reyer05 2.239.02118 Hardware Version: 1.00	IP Address: 10.52.49.88 MAC Address: 00.00/E150866 DNS: 172.30.44.20.192.168.528	(test)Settings ACL Name: test ACL: O Block O Allow		×
ACL List ACL Binding		EtherType Value : 🗹 All		
ACL		Src MAC: Z All Dest MAC: Z All		
Up to 512 entries can be added.	ACL Type	Save Reset		
□ test	Based on MAC	Existing ACL: (You can click and drag the ACL number to swap the ACL)	Control	
Co to page 1		No. Rufe No Data Available	Туре	lation

 Table 7-1
 Description of ACL Rule Configuration Parameters

Parameter	Description
ACL	Configuring ACL Rules Action Block: If packets match this rule, the packets are denied. Allow: If packets match this rule, the packets are permitted.
IP Protocol Number	Match IP protocol number The value ranges from 0 to 255. Check All to match all IP protocols. This applies to IPv4-based access control and IPv6-based access control.
Src IP Address	Match the source IP address of the packet. Check All to match all source IP addresses. This applies to IPv4-based access control and IPv6-based access control.

Parameter	Description
Dest IP Address	Match the destination IP address of the packet. Check All to match all destination IP addresses. This applies to IPv4-based access control and IPv6-based access control.
EtherType Value	Match Ethernet protocol type. The value range is 0x600~0xFFFF. Check All to match all protocol type numbers. This applies to MAC- based access control.
Src Mac	Match the MAC address of the source host. Check All to match all source MAC addresses. This applies to MAC-based access control.
Dest MAC	Match the MAC address of the destination host. Check All to match all destination MAC addresses. This applies to MAC-based access control.

Note

- ACLs cannot have the same name. Only the name of a created ACL can be edited.
- An ACL applied by a port cannot be edited or deleted. To edit, unbind the ACL from the port first.
- There is one default ACL rule that denies all packets hidden at the end of an ACL.

17.3.3 Applying ACL Rules

Choose Local Device > Security > ACL > ACL List.

Click Batch Add or Edit in the Action column, select the desired ACL for ports, and click OK.

Note

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

ACL Bindi	ing		+ Batch Add	🗇 Unbind Sel	ected
	Port	MAC-based ACL	IP-based ACL	Action	
	Gi1			Edit Unbind	
	Gi2			Edit Unbind	
	Gi3			Edit Unbind	
	Gi4			Edit Unbind	
	MAC-based ACL:	No Data No Data	~		
	IPV4-based ACL:	No Data	 		
		No Dete			
	IPV6-based ACL:	No Data	~		
	IPV6-based ACL: * Select Port:	NO Data			
Available	IPV6-based ACL: * Select Port:	igate 👥 Uplink 💼 Co	opper Fiber		
Available	IPV6-based ACL: * Select Port: Unavailable Aggree 5 7 9 11 6 8 10 12	egate	ppper Fiber		

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 Bi	nding		+ Batch Add	Dubind Selected		
	Port	MAC-based ACL	IP-based ACL	Action		
	Port Gi1	MAC-based ACL	IP-based ACL	Action Edit Unbind		

17.4 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>Port Protection</i> The protected ports are isolated from each other.	
Port List	🖉 Batch Edit
Port	Action
Gi1	
Gi2	
Gi3	
Gi4	
Gi5	

17.5 **IP-MAC Binding**

17.5.1 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.

 \times

17.5.2 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.

A Caution

IP-MAC Binding take effects prior to ACL, but it has the same privilege with IP Source Guard. The packet matching either configuration will be allowed to pass through.

iP-MA Descrip list will Note: II pass the	 IP-MAC Binding Description: IP-MAC Binding checks both the source IP addresses and MAC addresses of IP packets, and packets not matching any entry in the address binding Ist will be filtered. Note: IP-MAC Binding takes effect prior to ACL, but it has the same privilege with IP Source Guard. The packet matching either configuration will be allowed to pass through. 						
IP-MAC B	entries can be added.	ress v	Q Search	🖉 Add 👘 Delete Selected			
	IP	MAC	Port	Action			
	192.168.1.1	00:11:22:33:44:55	Gi29	Edit Delete			

Add

	IPv4 Addı 🗸	192.168.1.1	0	
	MAC Address	00:11:22:33:44:55		
	* Select Port:			
Available 💼 Una	available 💼 Aggr	egate 💼 Uplink 💼 Copper 🔛 Fiber		
1 2 5 7	0 11	1		
	9 11			
2 4 6 8	9 11 10 12			
2 4 6 8 : You can click and	9 11 10 12 drag to select on	e or more ports.	Select All	Inverse Desele

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 I	Binding Search by IP Ad	dress 🗸	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

17.6 IP Source Guard

17.6.1 **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.

A 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>17.1</u> DHCP Snooping for details.

17.6.2 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 L Descriptio	<i>i</i> Binding List Description: The entries come from dynamic learning of DHCP Snooping.							
Binding List			Search by IP Address \sim		Q Sear	ch C Refresh		
Up to 1900 er	ntries can be added.							
IP	,	/IAC	Port	VLAN ID	Status	Rule		
			No [Data				

The search box in the upper-right corner supports finding the specified entry in **Binding List** based on IP addresses, MAC addresses, VLANs or ports. Click the drop-down list box to select the search type, enter the search string, and click **Search**.

Search by IP Address		Q Search
Search by IP Address		
Search by MAC Search by VLAN	VLAN ID	Status
Search by Port	Data	

17.6.3 Enabling Port IP Source Guard

Choose Local Device > Security > IP Source Guard > Basic Settings.

In Port List, click Edit in the Action column. Select Enabled and select the match rule, and click OK.

There are two match rules:

- IP address: The source IP addresses of all IP packets passing through the port are checked. Packets are allowed to pass through the port only when the source IP addresses of these packets match those in the binding list.
- IP address+ MAC address: The source IP addresses and MAC addresses of IP packets passing through the port are checked. Packets are allowed to pass through the port only when both the L2 source MAC addresses and L3 source IP addresses of these packets match an entry in the binding list.

Caution

- IP Source Guard is not supported to be enabled on a DHCP Snooping trusted port.
- Only on an L2 interface is IP Source Guard supported to be enabled.

Reyee Cookbook

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	Ib	Edit	
	Gi3	Disabled	IP	Edit	

Edit			×
Enable	Enabled	~	
Rule	IP	^	
	IP		
	IP+MAC	ncel	ОК

17.6.4 Configuring Exceptional VLAN Addresses

Choose Local Device > Security > IP Source Guard > Excluded VLAN.

When IP Source Guard is enabled on an interface, it is effective to all the virtual local area networks (VLANs) under the interface by default. Users can specify excluded VLANs, within which IP packets are not checked or filtered, that is, such IP packets are not controlled by IP Source Guard.

Click Edit, enter the Excluded VLAN ID and the desired port, and click OK.

A 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.
Reyee Cookbook

Basic Settings	Excluded VLAN	Binding List						
i Excluded Descripti Note: Exc	1 VLAN on: Packets within this \ luded VLAN can be spec	/LAN are allowed to pass cified only after IP Source	the port without che Guard is enabled on	cking or filteri 1 a port.	ng.			
VLAN List						+	Add	Delete Selected
Up to <mark>64</mark> ent	tries can be added.							
	VLAN ID			Port			Actio	on
			Nol	Data				
Add								×
	* VLAN ID							
;	* Select Port:							
Avai	lable 💼 Unav	ailable	Agg	regate	t Uplink	Copper	Fi	ber
1	3 5 7 9 6 8 1	9 11 13 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1 1	5 17 19 2 6 18 20 2	21 23 1 1 1 1 1 1 1 1	25 27 2 1 1 1 1 1 1 1 1	9 31 33 1 1 1 1 1 1 1 1 1 1	35 36	37 38
Note: You	u can click and o	Irag to select on	e or more por	ts.	Select A	II Inverse	Desel	ect
					Cancel		ОК	

17.7 Configure 802.1x authentication

17.7.1 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- NBS switching devices only support the authentication function.

17.7.2 Configuration 802.1x

1. Configuring RADIUS Server

Choose Local Device > Security > 802.1x Authentication > 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 Server Group to add a server group.

Auth Config Port RADIU	IS Server Management Wired U	ser 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. 2010		

		×
道 Server 1]	
1812		
1813	0	
	0	
⊕ Add Server		
	 Berver 1 1812 1813 O Add Server 	1812 1813 ②

parameter	Description		
Server Group Name	Name of the server group. Multiple servers can be added to a server group. If the server with a higher priority does not respond, the system switches to other servers in the matching order. Note This function requires the server detection function to be enabled.		
Server IP	Radius server address.		
Auth Port	The port number used for accessing user authentication on the Radius server.		
Accounting Port	The port number used to access the accounting process on the Radius server.		
Shared Password	Radius server shared key.		

Cancel

parameter	Description
Match Order	The system supports adding up to 5 Radius servers. The higher the matching order value is, the higher the priority is.

(2) Configure server global settings and click Save..

Server global configuration		
* Packet Retransmission Interval	3 s	
* Packet Retransmission Count	3 time	
Server Detection		
MAC Address Format	XXXXXXXXXXX ~ ~]	0
	Save	

Parameter	Description
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	Configure the number of times the device sends request packets before confirming that there is no response from RADIUS
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	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. Configuring 802.1x Global Settings

Choose Local Device > 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 User List
Global Cor	nfig	
Glob	al 802.1x	
Authe	entication	
Au	th Server	Add a server to be authenticated.
		Advanced Settings
		Configure
Select the serv	er group	
Global Conf	ig	
		_
Global	802.1x	
Global Authen	tication	

(3) Click Advanced Settings to configure parameters such as Guest VLAN.

Auth Config	Port	RADIUS Server Management	Wired User List
(Guest Vlan		
* EAP-Requ	est Packet	2	
Retransmiss	ion Count		
* Qu	iiet Period	60	S
Clie * Timeou	ent Packet t Duration	30	S
Clie * Timeou	ent Packet t Duration	30	S
* EAP-Requ	est Packet	30	S
	Interval		

Parameter	Description
Server Escape	If the server disconnection is detected, all users will be allowed to access the Internet
Re-authentication	Require clients to re-authenticate at certain intervals to ensure network security
Guest VLAN	Provide a VLAN for unauthenticated clients to restrict their access
EAP-Request Packet Retransmission Count	Define the number of times the EAP request message will be retransmitted when no response is received, value range: 1-10 times
Quiet Period	During the authentication process, the idle time between the client and the server does not exchange authentication messages, value range: 0-65535 seconds
Client Packet Timeout Duration	The time limit for the server to wait for the response from the client. Exceeding this time will be regarded as an authentication failure. Value range: 1-65535 seconds

Parameter	Description
Client Packet	The time limit for the client to wait for the server to respond, exceeding this time will be considered as an authentication
Timeout Duration	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

Choose Local Device > Security > 802.1x authentication > Port.

(1) 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 Manag	ement 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					×
802.1	Ix Authentication				
	Auth Method	disable \lor			
	Auth Mode	multi-auth \vee			
	Guest Vlan				
* Use	r Count Limit per Port	1000			
				Cancel	ОК

Parameter	Description
802.1x Authentication	When enabled, the selected interface will enable 8.02.1x authentication.

Parameter	Description
	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
Auth Method	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.
	multi-auth: Supports multiple devices using the same port for authentication, but each device needs to be authenticated independently
Auth Mode	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
	When enabled, devices that fail authentication will be dynamically assigned to the specified Guest VLAN
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
	Limit the number of users under the interface
User Count Limit per Port	Product Difference Description
	The value range of NBS3100 series switches is 1-256, and other switches are 1-1000

17.7.3 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.

Choose Local Device > Security Management > 802.1x Authentication to obtain specific user information.

Auth Config	Port R	ADIUS Server Management	Wired User List						
Wired User List Q Search by mac Refresh				↓ Batch Logout					
	Username	Status	Interface	MAC Address	Online Time	Onlin	e 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>.

17.8 Anti-ARP Spoofing

17.8.1 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 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.

17.8.2 Procedure

Choose Local Device > Security > IP Source Guard > Excluded VLAN.

1. Enabling Anti-ARP Spoofing

Click Add, select the desired port and enter the gateway IP, click OK.

Note

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

I	Anti-ARP Spoofing Description: Anti-ARP Spoofing prevents hosts Note: Anti-ARP Spoofing is generally configure	s from spoofing the source IP address of the ARP packed on a downlink port.	tets to be the IP address of the gateway.
An	ti-ARP Spoofing		🖉 Add 🗇 Delete Selected
Up	to 256 entries can be added.		
	IP	Port	Action
		No Data	

Add			×
* IP	192.168.1.1		
* Select Port:	available Aggregate	e 🚹 Uplink 💼 Cr	opper Fiber
1 3 5 7	9 11 13 15 17 19 21 2	3 25 27 29 31	1 33 35 37
2 4 6 8	10 12 14 16 18 20 22 2	4 26 28 30 37	2 34 36 38
Note: You can click and	l drag to select one or more ports.	Select All In	nverse 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.

Anti- Desci Note	•ARP Spoofing ription: Anti-ARP Spoofing prevents hosts fro : Anti-ARP Spoofing is generally configured o	om spoofing the source IP address of the ARP pack on a downlink port.	tets to be the IP address of the gateway.
Anti-AR	P Spoofing		🖄 Add 👘 Delete Selected
Up to 25	6 entries can be added.		
	IP	Port	Action
	172.30.102.1	Gi15	Edit Delete

18 NBS and NIS Series Switches Advanced Configuration

18.1 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	IP or changing the STP mode will initiate	a new sessio	on. 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	ne:	30	seconds	STP Mode:	RSTP	~	
		0					
		Save					

18.1.1 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.

A 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
i Note: En	abling STP or changing the STP mode will initiate a new session. Please do not refresh the page.
	STP:

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

STP Settings STP N	/lanagement			
i Note: Enabling S	TP 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

Parameter	Description	Default Value
STP Mode	The versions of Spanning Tree Protocol. Currently the device supports STP (Spanning Tree Protocol) and RSTP (Rapid Spanning Tree Protocol).	RSTP

18.1.2 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	STP Managem	nent						
STP Por Tip: It is	t Settings recommended to	enable the port c	onnected to a PC	with Port Fast.				
Port List						0	Refresh	🖉 Batch Edit
				Link	Status	RDDU		
Port	Role	Status	Priority	Config Status	Actual Status	Guard	Port Fast	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 ~			
		Cancel	OK	

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
Status	 Disable: The port is closed manually or due to a fault, does not participate in spanning tree and does not forward data, and can be turned into a blocking state after initialization or opening. Blocking: A port in the blocking state cannot forward data packets or learn addresses, but can send or receive configuration BPDUs and send them to the CPU. Listening: If a port can become the root port or designated port, the port will enter the listening state. Listening: A port in the listening state does not forward data or learn addresses, but can receive and send configuration BPDUs. Learning: A port in the learning state cannot forward data, but starts to learn addresses, and can receive, process, and send configuration BPDUs. Forwarding: Once a port enters the state, it can forward any data, learn addresses, and receive, process, and send configuration BPDUs. 	NA
priority	The priority of the port is used to elect the port role, and the port with high priority is preferentially selected to enter the forwarding state	128
Link Status Config Status	Configure the link type, the options include: Shared, Point-to- Point and Auto. In auto mode, the interface type is determined based on the duplex mode. For full-duplex ports, the interface type is point-to-point, and for half-duplex ports, the interface type is shared.	Auto

Table 18-1 Description of STP Configuration Parameters of Ports

Parameter	Description	Default Value
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.

18.2 LLDP

18.2.1 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 M Can Learn The Topology 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.

18.2.2 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.

LLDP Settings	LLDP Management	LLDP Info
	LLDP:	

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

LLDP Settings LLC	DP Management LLDP Info			
LLC	DP:			
* Hold Multipli	er: 4	* Reinitialization Delay:	2	seconds
* Transmit Interv	val: 30	seconds * Forward Delay:	2	seconds
* Fast Cou	nt: 3			
	Save			

Table 18-2 Description of LLDP Global Configuration Parameters

Parameter	Description	Default Value
LLDP	Indicates whether the LLDP function is enabled.	enable
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

Parameter	Description	Default Value
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

18.2.3 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).

LDP Settings LLDP Ma	nagement LLDP Info			
Port List				🖉 Batch E
Port	Send LLDPDU	Receive LLDPDU	LLDP-MED	Action
Gi1	Enable	Enable	Enable	Edit
Gi2	Enable	Enable	Enable	Edit
Gi3	Enable	Enable	Enable	Edit
Patch Edit				×
Dalch Euli				
Send LLDPE	DU:			
Receive LLDPE	DU:			
LLDP-MI	ED:			
* Select I	Port: Unavailable	t Up	link Copper	Fiber
	7 9 11 13 15 17	7 19 21 23 25	27 29 31 33	35 37
2 4 0 8	D IU IZ 14 16 18	0 20 22 24 20	20 30 32 34	50 58
Note: You can click a	and drag to select one or n	nore ports. Se	elect All Inverse	Deselect
		Can	cel O	ж

18.2.4 **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 ted If the configurations do not match those on the connected neighbor.

LLDP Settings	LLDP Management	LLDP Info
Device Info		

Device ID Type:	Mac Address	Device ID:	00:11:22:33:44:67
Hostname:	Ruijie	Description:	RG-NBS5200-48GT4XS
Supported Feature:	Bridge,Router,Repeater	Enabled Feature:	Bridge,Router,Repeater
MGMT IP:	172.30.102.133		

Neighbor Info

Port	Device ID Type	Device ID	Port ID Type	Port ID	Neighbor System	Time To Live(s)
Gi15	MAC address	30:0D:9E:3E:B4:62	MAC address	30:0D:9E:3E:B4:62		3559
Gi17	MAC address	30:0D:9E:3E:AC:1A	MAC address	30:0D:9E:3E:AC:1A		2743
Gi24	MAC address	30:0D:9E:6F:C2:3C	Locally assigned	Gi3	NBS3100	117



18.3 RLDP

18.3.1 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 ask 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

18.3.2 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 Manager	nent	RLDP Info		
		RLDP:				
(2) Config	gure RLDP global par RLDP Settings	rameters and click Save. RLDP Management	RLDP Inf	ō		
	RL	.DP:				
	* Hello Inter	rval: 3		seconds	Errdisable Recovery:	

Table 18-3	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

Save

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, shut down 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
	Port	Loop Detection	Action	Action
	Gi1	Disable		Edit
	Gi2	Disable		Edit
	Gi3	Disable		Edit



3. Displaying RLDP information

Choose Local Device > Advanced > RLDP > RLDP Info.

You can view the detection status, failure handling methods, and ports that connect the neighbor device to the local device. You can click **Reset** to restore the faulty RLDP status triggered by a port to the normal state.

R	Local Device(NBS >			English 🗸 🛆	题 👌	₽
	RLDP Settings RLDP Management	RLDP Info				
*	Port List				Reset	:
⇔	Port	Status	Action	Neighbor I	Port	
0	Gi1	ОК				
A	Gi2	ОК				
•	Gi3	ОК				
\odot	Gi4	ОК				
Ē	Gi5	ОК				
Q	Gi6	ОК				
-0-	GI7	ОК				

18.3.3 Batch Configuring Network Switches

Choose Network > RLDP.

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

R		Navigation Q	English ~	۵	.	٩	@	Ņ	₿
Q									
ⓓ									
ጽ									
11	RLDP								
8	RLDP will avoid net	work congestion							
-0-	and connection inte	erruptions							
	occurs, the port inv	olved in the							
	loop will be automa	atically shut							
	down. 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.



18.4 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 resolving domain names. If the device fail To parse domain names, then use this DNS address instead.



18.5 Voice VLAN

\rm **Caution**

The Voice VLAN function is supported by RG-NBS3100 Series, RG-NBS3200 Series, RG-NBS5100 Series and RG-NBS5200 Series Switches.

18.5.1 **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.

18.5.2 Voice VLAN Global Configuration

Choose Local Device > Advanced > Voice VLAN > Global Settings.

Turn on the voice VLAN function, configure global parameters, and click Save.

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

Table 18-4 Description of VLAN Global Configuration Parameters

Parameter	Description	Default Value
Voice VLAN	Whether to enable the Voice VLAN function	Disable

Parameter	Description	Default Value
VLAN	VLAN ID as Voice VLAN	NA
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

18.5.3 Configuring a Voice VLAN OUI

Choose Local Device > Advanced > Voice VLAN > OUI.

The source MAC address of a voice packet contains the organizationally unique identifier (OUI) of the voice device manufacturer. After the voice VLAN OUI is configured, the device compares the voice VLAN OUI with the source MAC address in a received packet to identify voice data packets, and send 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.

 Global Settings
 OUI
 Port Settings

 Image: OUI List
 The enabled globally port will automatically add the corresponding OUI when receiving an LLDP packet that is identified as telephone.

 OUI List
 + Add

 Up to 32 entries can be added.

 MAC Address
 OUI Mask

 Description
 Type

No Data

Click Add. In the displayed dialog box, enter an MAC address and OUI, and click OK.

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

18.5.4 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 \checkmark ⑦	
Security Mode		
	Cancel OK	

Table 18-5 Description of the Voice VLAN Configuration Parameters on a Port

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

A 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.

18.6 Configuring Smart Hot Standby (VCS)

Smart hot standby enables multiple switches to act as a hot standby device for each other, ensuring uninterrupted data forwarding in the event of a single point failure.

18.6.1 Configuring Hot Standby

View or modify selected hot standby interfaces, device IDs and priorities. The switch with a higher priority is selected as the active switch in a hot standby group.

Caution

The devices in a hot standby group must have unique device IDs and priorities configured.

Choose Local Device > Advanced > Smart Hot Standby.

Ruíjie Rcycc	Local Device(NBS 🗸 Configuration Configurat
den vlan	
Monitor 🗸	Hot Standby Config DAD Port Config Active/Standby Switchover
Ports	🕖 The switches in the same smart hot standby group must have different switch IDs and priorities. The switch with a higher priority acts as the active device in the hot standby group.
L3 Interfaces	NB57006 (MACC567890326) Active NB57006 (MACC567897006)
Routing	Device ID Device1 V Device ID Device2 V
🛇 Security 🗸	Device Priority150 Device Priority100
😫 Advanced 🛛 🔿	Hot Standby Interface Config
STP	Selected Ports:Te1/2/1, Te1/2/3, Te1/2/4
LLDP	Available Turavailable Connected
RLDP	M7000-24GT245FP2XS-EA/GTRL307000065 Online 1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47
Local DNS	2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 49 50
Smart Hot Standby	M7000-8XS-EA/1234942570069 Online
Diagnostics	
-a- -a- System V	Delete Save
«Collapse	

18.6.2 Configuring DAD Interfaces

After selecting the DAD interfaces of both the active and standby switches, connect these DAD interfaces with a network cable to prevent network failures caused by dual active devices.

Ruíjie Rcycc	Local Device(NBS Configuration								
S VLAN									
受 Monitor 🗸	Hot Standby Config DAD Port Config Active/Standby Switchover								
Ø Ports	() Dual Active Detection (DAD) detects the health status of VSU members in real time through private protocol packets to avoid dual active devices, thereby enhancing system stability and connectivity.								
⊕ L3 Interfaces ∨	NB57006 (MACC567890326) Active NB57006 (MACC567897006)								
Routing	Device ID Device I Device ID Device 2								
🛇 Security 🗸	Device Priority 150 Device Priority 100								
🗄 Advanced 🔷 🔿	DAD Port Config								
STP	Selected Ports:GI1/4/11								
LLDP	Available 🛄 Unavailable 📥 Connected								
RLDP	1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47								
Local DNS	2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38 40 42 44 46 48 49 50								
Smart Hot Standby	M7000-8XS-EA/1234942570069 Online								
Diagnostics `									
😳 System 🗸	Save								
«Collapse									

18.6.3 Active/Standby Switchover

Active/Standby Switchover allow manual switching between the active and standby supervisor engines. Clicking the **Switch** button will restart the supervisor engine. Please exercise caution.

Ruíjie Rcycc	Local Device(NBS - Configuration] Local
≦ [₽] VLAN	
🕾 Monitor 🗸 🖉	Hot Standby Config DAD Port Config Active/Standby Switchover
Ø Ports	O You can manually perform mandatory active/standby wiltchover to switch the active supervisor engine to the standby supervisor engine. After the switchover, the active supervisor engine is forcibly restarted and becomes a candidate or standby supervisor engine. The standby supervisor engine assumes the active role to manage the members in the hot standby group.
L3 Interfaces V	Switch
Routing ~	
⊘ Security ∨	
🖆 Advanced 🛛 🔿	
STP	
LLDP	4
RLDP	
Local DNS	
Smart Hot Standby	
Diagnostics	
🗄 System 🗸	

19 NBS and NIS Series Switches Diagnostics

19.1 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.

R	Local Device(NBS 🗸	English - 🔿 🎇 🚖
ጽ		
£⊒ ₽	Center	Port Info
<u>+</u>	Port Info	Updated on2022-05-20 12:18:51 🙄 Refresh Panel View
₩	VLAN Info	1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37 39 41 43 45 47 49 51
\bigcirc	Routing Info	
	DHCP Clients	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
\bigcirc	ARP List	Port Gi1
Ð	MAC	Status Disconnected Flow ↓ 0.00 ↑ 0.00 Interface Mode Access Port Negotiation Rate Total Packets / VLAN 1
Q	DHCP Snooping	Actual Rate
-0-	IP-MAC Binding	Flow Control(Config Disable Corrupted/Oversized/
-0-	IP SOURCE GUARD	Flow Control(Actual Disable Conflicts
	CPP	Status) Attribute Copper

19.1.1 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 <u>12.2</u> Port Configuration.
- To configure the L2 mode of the port and the VLAN to which it belongs, see <u>11.6.3</u> Configuring Port VLAN.

Info Center	Port Info						
Port Info	Updated on2022-05-20 12	2:18:51 😋 Refres	h				Panel View
VLAN Info	1 3 5 7 9	9 11 13 15	17 19 21 23 25	27 29 31 33	35 3	Role	Status
Routing Info					11	Copper	1 G/2.5G/100
DHCP Clients	2 4 6 8 10	0 12 14 16	18 20 22 24 26	28 30 32 34	36 3	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)	Copper	Conflicts				

19.1.2 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>11.6 VLAN</u>.
- To configure SVI ports and routed ports, see <u>15.1 Setting an L3 Interface</u>.

info Center	VLAN Info (SVI&Routed Port) DNS: 🕃 Refresh							
Port Info	< VLAN1	Routed Port Gi1	Routed Port Gi2	Routed Port Gi3 Routed Port Gi4	Routed Port Gi5 Rout			
VLAN Info	In	terface	IP	DHCP 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	15 17 19 21 2	3 25 27 29 31 33 35 37 39	41 43 45 47 49 51			
MAC								
DHCP Snooping	2 4	6 8 10 12 14	16 18 20 22 24	4 26 28 30 32 34 36 38 40	42 44 46 48 50 52			
IP-MAC Binding								

19.1.3 Routing Info

A Caution

If the device does not support L3 functions (such as RG-NBS3100 Series and RG-NBS3200 Series Switches), 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 15.4 Configuring the DHCPv6 Server .

info Center	Routing Info			
Port Info	Tip: Up to 500 entries can be adde	d.	Search by IP Address	Q Refresh
VIANInfo	Interface	IP	Subnet Mask	Next Hop
Routing Info	Gi9	2.1.1.0	255.255.255.0	3.1.1.1
DHCP Clients				

19.1.4 DHCP Clients

🔺 Caution

If the device does not support L3 functions (such as RG-NBS3100 Series and RG-NBS3200 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>15.4</u> Configuring the DHCPv6 Server.

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	e added.		Search by Hostname/IP/MAC	Q Refresh			
Routing Info	Hostname	IP	MAC	Lease Time(Min)	Status			
ARP List		No Data						
MAC	APD List							

19.1.5 ARP List

Choose Local Device > Diagnostics > Info Center > ARP List.

Displays ARP information on the device, including dynamically learned and statically configured ARP mapping entries.

Note

To bind dynamic ARP or manually configure static ARP, see <u>15.6 Configuring a Static ARP Entry</u>.

Info	ARP List					
Center	Tip: Up to 2000 entries car	n be added.	5	Search by IP/MAC	Q © Refresh	
Port Info	Interface	IP	MAC	Туре	Reachable	
VLAN Info	VLAN1	172.30.102.209	c0:b8:e6:e9:78:07	Dynamic	Yes	
Routing Info	VLAN1	172.30.102.118	c0:b8:e6:ec:a1:5c	Dynamic	Yes	
DHCP Clients	VLAN1	172.30.102.94	c0:b8:e6:e9:e3:04	Dynamic	Yes	
ARP List	VLAN1	172.30.102.84	00:d0:f8:22:74:5f	Dynamic	Yes	
MAC	VLAN1	172.30.102.40	c0:b8:e6:e3:3e:38	Dynamic	Yes	
DHCP Snooping	VLAN1	172.30.102.139	30:0d:9e:3e:b4:62	Dynamic	Yes	
IP-MAC Binding	VLAN1	172.30.102.179	00:d0:f8:15:08:5c	Dynamic	Yes	
IP SOURCE GUARD	VLAN1	172.30.102.90	c0:b8:e6:7c:f2:7c	Dynamic	Yes	
СРР	VLAN1	172.30.102.121	30:0d:9e:6f:c2:3d	Dynamic	Yes	
	VLAN1	172.30.102.116	00:d0:fa:15:09:5c	Dynamic	Yes	

19.1.6 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 11.3 MAC Address Management

Info Center	МАС			
Port Info	Tip: Up to 16K entries can be added.	Search by MAC	~	Q C Refresh
VIANInfo	Interface	MAC	Туре	VLAN ID
Pouting lafe	Gi24	70:B5:E8:5F:FD:29	Dynamic	1
Routing into	Gi24	50:9A:4C:42:C9:50	Dynamic	1
DHCP Clients	Gi24	30:0D:9E:6F:C2:3C	Dynamic	1
ARP List	Gi24	30:0D:9E:6F:C2:3D	Dynamic	1
MAC	Gi24	C0:B8:E6:E9:78:07	Dynamic	1
DHCP Snooping	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:F8:78:B7:8D	Dynamic	1
CPP			- <i>j</i>	

19.1.7 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>17.1 DHCP Snooping</u>.

info Center	DHCP Snooping				
Dest Infe	DHCP Snooping: Enabled	Option82: D	sabled	Trusted Port: Gi24 ORefi	resh
Port Into	DHCP Snooping Binding Entri	es from the Trusted Po	t		
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. Search	by IP Address 🗸 🗸		Q Q Refresh
DHCP Snooping	Port		ID		MAC
IP-MAC Binding	FOIL		IF		MAG

19.1.8 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>17.5</u> IP-MAC Binding.

Info Center	IP-MAC Binding]				
Port Info	Tip: Up to 500 entries c	an be added.	Search by IP Address	×	Q	C Refresh
VI AN Info	Port		IP		MAC	
Routing Info	Gi29		192.168.1.1		00:11:22:33:44:55	
DUCD Cliants						
ARP List	IP SOURCE GUARD					
ARP List	IP SOURCE GUARD	can be added.	Search by IP Address	~] [۵	C Refresh
ARP List MAC DHCP Snooping	IP SOURCE GUARD Tip: Up to 1900 entries Interface	can be added. Rule	Search by IP Address	∽) [MAC	Q VLAN ID	C Refresh Status

19.1.9 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 <u>17.6 IP Source Guard</u>.

Port Info	IP SOURCE GUARE	>				
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: 20	000pps 😋 Refre	sh			
IP SOURCE GUARD	EtherType Val	ue	Rate	Current Rate		Total messages
CPP	bodu		60000	0		0

19.1.10 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	СРР							
ecinter	Total CPU bandwidth: 2000pps 😋 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					

19.2 Network Tools

The **Network Tools** page provides three tools to detect the network status: **Ping, Traceroute,** and **DNS Lookup.**
19.2.1 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.

<i>i</i> Network Tools				
Tool	Ping	O Tracerout	e 🔿 DNS	S Lookup
IP Address/Domain	172.30.	102.1		
* Ping Count	4			
* Packet Size	64			Bytes
		Start	Sto	р
PING 172.30.1 72 bytes from 72 bytes from 72 bytes from 72 bytes from	02.1 (172 172.30.10 172.30.10 172.30.10 172.30.10	.30.102.1): 64 dat 02.1: seq=0 ttl=6 02.1: seq=1 ttl=6 02.1: seq=2 ttl=6 02.1: seq=3 ttl=6	ta bytes 4 time=0.000 4 time=0.000 4 time=0.000 4 time=0.000) ms) ms) ms) ms
172.30.102 4 packets tran round-trip mi	2.1 ping st ismitted, 4 n/avg/ma	atistics 4 packets receive x = 0.000/0.000/	d, 0% packet 0.000 ms	loss

19.2.2 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.**

i Network Tools		
Tool	O Ping • Traceroute	e 🔿 DNS Lookup
P Address/Domain	172.30.102.30	
* Max TTL	20	
	Start	Stop
traceroute to byte packets 1 172.30.102	172.30.102.30 (172.30.102.3 2.133 (172.30.102.133) 2999	30), 20 hops max, 38 9.863 ms !H

19.2.3 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.

i Network Tools								
Tool	O Ping	 Traceroute 	DNS Lookup					
* IP Address/Domain	IP Address/Domain www.google.com							
		Start	Stop					
Server: 127. Address 1: 12	0.0.1 7.0.0.1 loca	alhost						
Name: ww Address 1: 20 Address 2: 10	Name: www.google.com Address 1: 2001::67f0:b475 Address 2: 104.244.46.85							
			1.					

19.3 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.



19.4 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.

				-		-	-	-	-		-						-									
1	3	5	7	9	11	13	15	17	19	21	23	25	27	29	31	33	35	37	39	41	43	45	47	49	51	
Ţ	Ţ	Ţ	Ţ	Ţ	Ţ.	Ţ	Ŧ	Ţ	Ţ	Ţ	Ū.	Ţ	ī.		Ţ	Ţ	÷.	Ţ	Ţ	Ţ	Ę.	Ţ	Ţ.			
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	
ote: Y	ou ca	n clio	k an	d dra	g to se	elect	one c	or mo	ore po	orts.											Selec	t All	Inve	erse	Deselect	
ote: Y	ou ca	n clio	ck and	d dra	g to se	elect	one o	or mo	ore po	orts.		Sta	art								Selec	t All	Inve	erse	Deselect	
ote: Y	ou ca	n clia	ck and	d dra	g to se	elect	one c	or mo	ore po	orts.		St	art								Selec	t All	Inve	erse	Deselect	
ote: Ye Resu	bu ca	n clio	ck and	d dra	g to se	elect	one d	or mo	ore po	orts.		St	art								Selec	t All	Inve	erse	Deselect	
ote: Ye	bu ca	n clia	ck and	d dra	g to se Port	elect	one d	or mo	ore po	orts.		St	art		Cabl	e Le	ngth (cm)			Selec	t All	Inve	erse	Deselect	Re

A 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.

19.5 System Logs

Choose Local Device > Diagnostics > System Logs.

System logs record device operations, operation time, and operation modules. System logs are used by administrators to monitor the running status of the device, analyze network status, and locate faults. You can search for specified logs by fault type, faulty module, and keyword in fault information.

I	System Logs View system logs.						
Log	y List					Search	Q
	Time	Туре	Module	D	etails	local.info	
Ma	ay 18 18:52:37	kern.crit	kernel	%Port-2: GigabitEthernet12 link up		syslog	
Ma	ay 18 18:52:37	local.info	syslog	%L3-6: Manage VLAN 1 change to UP		kern.crit	
Ma	ay 18 18:52:37	kern.crit	kernel	%Port-2: GigabitEthernet13 link up			
Ma	ay 18 18:52:37	kern.crit	kernel	%Port-2: GigabitEthernet17 link up			
Ma	ay 18 18:52:38	kern.crit	kernel	%Port-2: GigabitEthernet22 link up			

19.6 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.

🔺 Caution

After unfollowing an alert, the system will not issue an alert prompt for this type of fault, and users cannot find and deal with the fault in time. Exercise caution when performing this operation.



Table 11-1 Alert Types and Product Support

Alert Type	Description	Support Description
Addresses in the DHCP address pool are to be exhausted.	The device acts as a DHCP server, and the number of allocated addresses is about to reach the maximum number of addresses that can be allocated in the address pool.	It is applicable only to devices that support L3 functions. Products that do not support L3 functions such as RG-NBS3100 Series, RG-NBS3200 Series Switches do not support this type of alert.

Alert Type	Description	Support Description
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 PoE process is not running.	The PoE service of the device fails and no power can be supplied.	It is applicable only to NBS Series Switches that support the PoE function. (The device models are marked with "-P".)
The total PoE power is overloaded.	The total PoE power of the device is overloaded, and the new connected PD cannot be powered properly.	It is applicable only to NBS Series Switches that support the PoE function. (The device models are marked with "-P".)
The device has a loop alarm.	A network loop occurs on the LAN.	NA

20 NBS and NIS Series Switches System Configuration

20.1 Setting the System Time

Choose Networkwide Management > System > 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 vie	ew system time (The device ha	is no RTC mo	dule. 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

20.2 Setting the Web Login Password

Choose Networkwide Management > System > 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 $ imes $	
Q Navigation	<i>i</i> Change the login pa	ssword. Please log in again with the new password later.
 Overview ♣ Network 	* Old Management Password	Enter old management password of the project.
Devices	* New Management	The management passwords of the network-wid
 Clients Management System ^ 	Password	There are four requirements for setting the password: • The password must contain 8 to 31 characters.
System Time		The password must contain uppercase and lowercase letters, numbers and three types of special
Backup		The password cannot contain admin. The password cannot contain question marks
SNMP		spaces, and Chinese characters.
Reboot Cloud Service	* Confirm Password	Enter new management password again.
	Password Hint	ruijie
		Save

20.3 Setting the Session Timeout Duration

Choose Local Device > System > Login > Session 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.

Login Password	Session Timeout	
<i>i</i> Session Time	out	
* Session Timeou	t 3600	seconds
	Save	

20.4 Configuring SNMP

20.4.1 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.

20.4.2 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 re 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 ity 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 im plemented by this standard.

2. Configuration Steps:

Network Management > 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 v3 is enabled by default. To proceed, please add
* SNMP Version	🗌 v1 🗹 v2c 🗹 v3 🔓	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** >. (1) 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 Por	rt 161	
* Device Locatio	n Company]
* Contact Inf	o Ruijie@Ruijie.com]
	Save	

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.

Table 20-1 Global Configuration Description Table

(2) Click <Save>.

After enabling the SNMP service takes effect, click <**Save**> to make basic configurations such as SNMP protocol version number take effect.

20.4.3 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 rements.

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 Management > System > SNMP > View/Group/Community/Client Access Control > View List

(1) Click <**Add**> to create a view.

Reyee Cookbook

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 🗸 🚺	> 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			1 Delete Sele	cted
Up to 100 entries are	e allowed.			
Rule	e	OID	Action	
	No D	Data		
Total 0 10/page \vee	< 1 > Go	o to page 1		
			Cancel	ОК

Table 20-2 View configuration information description table

parameter	Description
View Name	The name used to identify the view. The length is 1 to 32 characters, and cannot contain Chinese and full-width characters.

parameter	Description
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.

(1) Click <**OK**>.

2. v1 /v2c user configuration

Introduction

When the SNMP protocol version is set to v1/v2c, user configuration needs to be completed.

SNMP Service	
* SNMP Version □ v1 🗹 v2c 🗹 v3	
* Local Port 161	
* Device Location Company	
* Contact Info Ruijie@Ruijie.com	
Save	

Note

Select the SNMP protocol version, click **Save**>, and the corresponding configuration options will appear on the view/group/group/user access control interface.

configuration steps

Choose Networkwide Management > System >SNMP> View/Group/Community/Client Access Control

Global Config	/iew/Group/Community/Cli	ent Access Control Trap Settings		
SNMP v1/v2c	Community Name L	ist		+ Add 💿 Delete Selected
Up to 20 entries a	are allowed.			- U
	Community Name	Access Mode	MIB View	Action
	hello_12121	Read & Write	all	Edit Delete
	34234234A.	Read-Only	all	Edit Delete
Add * Comm	nunity Name	ls.		×
* A	Access Mode	Read-Only	\sim	
	* MIB View	all	 ✓ Add View + 	
			Cancel	ОК

Table 20-3	v1 / v2c use	r information	description	table
------------	--------------	---------------	-------------	-------

Parameter	Description
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)

A Notice

- Among v1/v2c users, the community name cannot be repeated.
- Click <Add View> to add a view.

3. 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

Network Management > System > 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 Serv	ice 🔵	
* SNMP Versi	ion 🗌 v1 🗹 v2c 🗹 v3	
* Local P	ort 161	
* Device Locati	Company	
* Contact Ir	nfo Ruijie@Ruijie.com	
	Save	

(2) Set v 3 groups of related parameters.

Revee	Cookbook
-------	----------

IMP v3 Group List					I	+ Add	I Delete Selected
to 20 entries are allowed.							
Group Name	Security Level	Read-Only View	Read & Wr	ite View	Notification View		Action
default_group	Auth & Security	all	non	e	none	Edi	t Delete
1 10/page > < 1 > Got	to page 1						
Add						\times	
t Carrie Name							
* Group Mame							
* Security Level	Allowlist & S	Security	\sim				
* Read-Only View	all		\sim	Add View	<i>ı</i> +		
* Read & Write View	all		~	Add View	ı +		
* Notification View	2020			Add View	· _		
Nouncation view	none		~	Add view	/ +		
				0	ancel)K	

Table 20-4 V3 group configuration parameters

Parameter	Description
Group Name	rule group name 1-32 characters, a single Chinese accounted for three characters Cannot contain Chinese, full-width characters, question marks and spaces
Security Level	The minimum security level of the rule group (Auth & Security Auth & Open Allowlist & Security authentication with encryption, authentication without encryption, no authentication encryption)
Read-Only View	The options in the drop-down box are configured views (default views all, none)

Parameter	Description
Read & Write View	The options in the drop-down box are configured views (default views all, none)
Notification View	The options in the drop-down box are configured views (default views all, none)

🛕 Notice

- Groups limit the minimum security level, read and write permissions and scope of users in the group.
- The group name cannot be repeated. If you need to add a view, click < Add View >.

(3) Click <**OK**>.

- 4. v 3 user configuration
- Introduction
- prerequisite

When the SNMP protocol version is set to v3, the v3 group configuration needs to be completed.

Global Config	View/Group/Community/Client Access Control	Trap Settings
SNMP Serv	vice 💽	ß
* SNMP Vers	ion 🗌 v1 🔽 v2c 🔽 v3	
* Local F	Port 161	
* Device Locat	ion Company	
* Contact I	nfo Ruijie@Ruijie.com	
	Save	
i Note		

Select the SNMP protocol version, click **Save**, and the corresponding configuration options will appear on the view/group/group/user access control interface.

		Tran Settings		create a vo t	1501.		
otar i otpage		hap settings					
SNMP v3 Client List							
						+ Add	Delete Selected
Up to 50 entries are allowed.							
Username G	roup Name S	Security Level	Auth Protocol	Auth Password	Encryption Protocol	Encrypted Password	Action
ıtal 0 10/page ∨ < 1 >	Go to page 1						
 Set v3 user relate 	ed paramete	ers.					
e) Set v3 user relate	ed paramete	ers.					×
2) Set v3 user relate Add	ed paramete	ers.					×
2) Set v3 user relate Add * Username	ed paramete 123sdf!@	ers.				ß	×
2) Set v3 user relate Add * Username * Group Name	ed paramete 123sdf!@ default_gro	oup	~			ß	×
2) Set v3 user relate Add * Username * Group Name * Security Level	ed paramete 123sdf!@ default_gro Auth & Se	oup curity				<u>₹</u>	×
2) Set v3 user relate Add * Username * Group Name * Security Level * Auth Protocol	ed paramete 123sdf!@ default_gro Auth & Se MD5	oup curity	~ ~	* Auth Pass	word	ß	×

Table 20-5	v3 user	configuration	parameters
------------	---------	---------------	------------

parameter	Description
	username
	at least 8 characters
Username	Contains three types of uppercase letters, lowercase letters, numbers, and special characters
	Does not contain admin/public/private
	Does not contain question marks, spaces and Chinese

parameter	Description
Group Name	user's group
Security Level	User security level (authentication and encryption, authentication without encryption, no authentication and encryption)
Auth Protocol, Auth Password	Authentication protocols include: MD5/SHA/SHA224/SHA256/SHA384/SHA512 Authentication password: 8~31 characters in length, cannot contain Chinese characters, full-width characters, question marks, and spaces, and must contain at least 3 types of uppercase and lowercase letters, numbers, or special characters. Note: This parameter needs to be set when the "Security Level" is "authentication and encryption" or "authentication without encryption".
Encryption Protocol, Encrypted 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

- 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.

20.4.4 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 issue, and uses the v2c version to monitor the data information of nodes such as 1.3.6.1.2.1.1 through the third-party software.

• configuration list

According to the analysis of the user's usage scenario, the requirements are shown in the table:

Table 20-6	User Requirements D	escription Form
		-

description item	Description
view range	Inclusion rule: OID is.1.3.6.1.2.1.1, custom view named " system "
use version number	v2c version The custom community name is " public ", and the default port number is 161
Read and write permissions	Read permission

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

Global Config	View/Group/Community/Client Access Control	Trap Settings
SNMP Serv	rice 🚺	
* SNMP Vers	ion 🗌 v1 🔽 v2c 🔲 v3	
* Local P	ort 161	
* Device Locat	ion Company	
* Contact li	nfo Ruijie@Ruijie.com	
	Save	

(1) 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		

А	d	d

Add				×
* View Name	system			
OID	.1.3.6.1.2.1			
		Add Excluded Rule		
Rule/OID List		(Delete Selected	
Up to 100 entries ar	re allowed.			
Ru	le	OID	Action	
	No	Data		
Total 0 10/page 🗸		Go to page 1		
			Cancel	к

(2) view /group/group/user access control interface, click <**Add**> in the SNMP v1/v2c community name list, fill in the community name, access mode and view in the pop-up window, and click <**OK**> after the operation is completed.

Global Config View/Group/Community	/Client Access Control Trap Settings				
SNMP v1/v2c Community Nam	e List				+ Aud Delete Selected
Up to 20 entries are allowed.					
Community Name	e Access Mode	2	MIB View		Action
Add				×	
* Community Name	texttrtd1@				
* Access Mode	Read-Only	~			
* MIB 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:

Parameter	Description
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

Table 20-7 User Requirements Description Form

• configuration steps

(2) 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 V	iew/Group/Community/Client Access Control	Trap Settings
SNMP Service	e 🚺	
* SNMP Version	n 🗌 v1 🔲 v2c 🗹 v3	
* Local Por	t 161	
* Device Location	Company	
* Contact Info	Ruijie@Ruijie.com	
	Save	

(1) 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	re allowed.			
Rul	le	OID	Action	
	No D	Data		
Total 0 10/page 🗸	C 1 C Go	to page 1		
			Cancel	(

(2) 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. After the operation is complete, click < **OK**>.

SNMP v3 Group List					
					+ Add
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		\sim	Add View +	
* Read & Write View	all		~	Add View +	
* Notification View	none		\sim	Add View +	
				Cancel	ОК

(3) 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>.

SNM	v3 Client List							~
							+ Add	Delete Selected
Up to	50 entries are allowed.							
	Username	Group Name	Security Level	Auth Protocol	Auth Password	Encryption Protocol	Encrypted Password	Action
				No Data				
Total 0	10/page 🗸 🤇 1	> Go to page 1						

Add					×
* Username	Username				
* Group Name	group	~			
* Security Level	Auth & Security	\sim			
* Auth Protocol	MD5	~	* Auth Password		
* Encryption Protocol	AES	~	* Encrypted Password		
				Cancel	ОК

20.4.5 trap service configuration

trap is a notification mechanism of the 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.

Network Management > System > SNMP > trap setting

(1) Enable the trap service switch.

Global Config	View/Group/Community/Client Access Con	trol Trap Settings				
Trap Servi	ce 💽			×		
* Trap Versio	on 🗹 v1 🗹 v2c 🗹 v3	b	Are you sure you want to Enable trap?			
	Save		Cancel	OK		
1	11					
	lient List					
Up to 20 entries	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 Access	Control	Trap Settings	
Trap Ser	vice 🔵					
* Trap Ver	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

Network Management >System > SNMP > trap setting

(1) Click <Add> in the Trap v1v2c User list to create a trap v1v2c user.

Global Config	View/Group/Community/Clie	nt Access Control Trap Settings			
Trap	Service 🚺				
* Trap	Version 🗹 v1 🗹 v2c 🗹	v3			
	Save				
Trap v1/v	2c Client List				+ Add
Up to 20 e	entries are allowed.				
	Dest Host IP	Version Number	Port ID	Community Name	Action
			No Data		

(2) Configure trap v1v2c user-related parameters.

set up

 \times

•	_	_
~	α	$^{\prime}$
~	u	u
	ч	ч

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



Table 20-8 t rap v1/v2c user information description table

Parameter	Description
destination ip	Trap peer device IP, support IPv4 / IPv6 address
version number	Trap version number, including v1 v2c
The port number	trap peer device port [1, 65535]
Group Name/User Name	The community name of the trap user at least 8 characters Contains three types of uppercase letters, lowercase letters, numbers, and special characters Does not contain admin/public/private Do not contain question marks, spaces and Chinese

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

[Network Management] System > 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	20 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 \lor	
* Auth Protocol	MD5	\sim	* Auth Password		
* Encryption Protocol	AES	~	* Encrypted Password		
				Cancel	

Table 20-9 trap v3 user information description table

Parameter	Description
target host ip	trap peer device IP, support IPv4/IPv6 address
The port number	trap peer device port [1, 65535]

Parameter	Description
username	username of the trap v3 user at least 8 characters Contains three types of uppercase letters, lowercase letters, numbers, and special characters Does not contain admin/public/private Do not contain question marks, spaces and Chinese
Security Level	Trap user security level, including three levels of authentication and encryption, authentication and encryption, and authentication and no encryption
Authentication protocol, authentication password	Authentication protocols include: MD5/SHA/SHA224/SHA256/SHA384/SHA512 Authentication password: 8~ 31 characters in length, cannot contain Chinese characters, full-width characters, question marks, and spaces, and must contain at least 3 types of uppercase and lowercase letters, numbers, or special characters. 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.

A Notice

IP of t rap v1/v2c/v3 users cannot be repeated.

20.4.6 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:

Table 4-1 User Requirements Description Form

description item	Description
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
- (3) Select the v2c version on the trap setting interface, click **Save**>.

Global Config	View/Group/Community/Client Access Control	Trap Settings
Trap Se	ervice 🚺	
* Trap Ve	ersion 🗌 v1 🗹 v2c 🔲 v3	
	Save	
2) Click < Add > ii	n the " trap v1 / v2c user list ".	

Trap v1/	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.

 \times

Add

* Dest Host IP	192.168.110.77
* Version Number	v1 ~
* Port ID	123
* Community	123e#dfd
Name/Username	



2. V3 version trap configuration

scenes to be used

When the user is monitoring the device, if the device is suddenly interrupted or abnormal, the third-party monitoring software cannot detect and deal with the abnormal situation in time, and the device with the destination ip of 1 92.1 68.110.87 and the port number of 1 67 is configured, 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 4-1 User Requirements Description Form

description item	Description
IP and port number	The target host IP is "192.168.110.87", and the port number is "167".
Use version number, username	Select the v3 version, the user name is "trapv3_public"
Authentication Protocol / Encryption Protocol	Authentication protocol / authentication password: MD5/Ruijie123
Encryption Protocol / Encryption Cipher	Encryption protocol / encryption password: AES/ Ruijie123

• configuration steps

(4) Select the v3 version on the trap setting interface, and click <Save>.

Global Config	View/Group/Commun	ity/Client Access Contro	Trap Settings
Trap Ser	vice 🔵		
* Trap Ver	sion 🗌 v1 🗌 v2c	✓ v3	
	Save		
(2) Click <Add> in the(3) Fill in the target ho configuration is configuration is configuration.	e trap v3 user list. st IP, port number, user na mplete.	me and other information,	and click < OK > after the
Add			×
* Dest Host IP	192.168.110.87	* Port ID	167
* Username	trapuser1_	* Security Level	Auth & Security \vee
* Auth Protocol	MD5 \sim	* Auth Password	Ruijie123

20.5 Configuration Backup and Import

AES

* Encryption Protocol

Choose Local Device > System > Backup > Backup&Import.

Configure backup: Click Backup to generate the backup configuration and download it locally.

Configure import: Click **Browse**, select a backup configuration file locally, and click **Import** to apply the configuration specified by the file to the device After importing the configuration, the device will restart.

* Encrypted Password

Ruijie123

OK

Cancel

Backup & Import	leset
<i>i</i> If the target version If the target version It is recommende	on is much later than the current version, some configuration may be missing. d to choose Reset before importing the configuration. The device will be rebooted automatically later.
Backup Config	
Backup Config	Backup
Import Config	
File Path	Please select a file. Browse Import

20.6 Reset

20.6.1 Resetting the Device

Choose Local Device > System > Backup > Reset.

Click **Reset**, and click **OK** to restore factory settings.

Backup	& Import Reset	
I	Resetting the device will clear the current settings. If you want to keep the configuration, please Backup Config first.	
	Reset	
Tip) ×	
Resetting the device will clear the current settings and reboot the device. Do you want to continue?		
	Cancel	

A Caution

Resetting the device will clear current settings and reboot the device. If a useful configuration exists in the current system, you can export the current configuration (see <u>20.4</u> <u>Configuring SNMP</u>) before restoring the factory settings. Exercise caution when performing this operation.

20.6.2 Resetting the Devices in the Network

Choose Network Management > System > Backup > Reset.

Select **All Devices** and choose whether to **Unbind Account**, click **Reset All Devices** and all devices in the current network will be restored to their factory settings.

Backup & Import	Reset	
<i>i</i> Resetting the d	device will clear the current settings. If you want to keep the configuration, please Backup Config first.	?
Select	Local All Devices	
Option	Unbind Account (The devices of this account will be removed from Ruijie Cloud and will not be managed by this a	account).
	Reset All Devices	

A Caution

Resetting the network will clear current settings of all devices in the network and reboot the devices. Exercise caution when performing this operation.

20.7 Rebooting the Device

20.7.1 Rebooting the Device

Choose Self-Organizing Mode > Network Management > System > Reboot

Choose Standalone Mode > System > Reboot.

Select **Local** and click **All Devices**. The device will restart. Do not refresh the page or close the browser during the reboot. After the device is successfully rebooted and the Web service becomes available, the device automatically jumps to the login page.

eboot Scheduled Reboot	
<i>i</i> Please keep the device powered on during reboot.	?
Select O Local O All Devices O Specified Devices	
Reboot	

20.7.2 Rebooting the Devices in the Network

Choose Network Management > System > Reboot > Reboot.

Select **All Devices**, and click **Reboot All Device** to reboot all devices in the current network.

Reboot Scheduled Reboot	
<i>i</i> Please keep the device powered on during reboot.	?
Select Cocal Specified Devices	
Reboot All Device	

A Caution

It will take some time for the network to reboot, please be patient. The network operation will affect the entire network. Therefore, exercise caution when performing this operation.

20.7.3 Rebooting Specified Devices in the Network

Choose Network Management > System > Reboot > Reboot.

Click **Specified Devices**, select desired devices from the **Available Devices** list, and click **Add** to add devices to the **Selected Devices** list on the right. Click **Reboot**. Specified devices in the **Selected Devices** list will be rebooted.

Reboot Schee	duled Reboot				
<i>i</i> Please keep	the device powered on during rel	boot.			?
Select	O Local O All Devi	ces	Specified Devic	tes	
	✓ Available Devices	1/1		Selected Devices	0/0
	Q Search by SN/Model			Q Search by SN/Model	
	MACCQQQQQQ123 - NBS	5200-48GT4	< Delete	No data	
			Add >		
	Reboot				

20.8 Configuring Scheduled Reboot

Confirm that the system time is accurate. For details about how to configure the system time, see <u>20.1</u> Setting the System Time. To avoid network interruption caused by device reboot at wrong time.

Choose Self-Organizing Mode > Network Management > System> Reboot > Scheduled Reboot.

Choose Standalone Mode > System > Reboot > Scheduled Reboot.

Click **Enable**, and select the date and time of scheduled reboot every week. Click **Save**. When the system time matches the scheduled reboot time, the device will restart.

🔺 Caution

Once enable scheduled reboot in the network mode, all devices in the network will reboot when the system time matches to the timed time. Therefore, exercise caution when performing this operation.

Reboot	Scheduled Reboot
i It is The	recommended to set the scheduled time to a network idle time, e.g., 2 A.M downlink device will also be rebooted as scheduled.
	Enable
	Day 🗹 Mon 🗹 Tue 🔽 Wed 🗹 Thu 🔽 Fri 🗹 Sat 🗹 Sun
	Time 03 ~ : 00 ~
	Save

20.9 Upgrade

A Caution

- It is recommended to backup the configuration before software upgrade.
- Version upgrade will restart the device. Do not refresh or close the browser during the upgrade process.

20.9.1 Online Upgrade

Choose Local Device > System > Upgrade > Online Upgrade.

The current page displays the current system version and allows you to detect whether a later version is available. If a new version is available, click **Upgrade Now** to perform online upgrade. If the network environment does not support online upgrade, click **Download File** to download the upgrade installation package locally and then perform local upgrade.
	Û	Note	
,		Online upg	rade will retain the current configuration.
,	•	Do not refr	esh the page or close the browser during the upgrade process. After successful upgrade, you
		will be redi	rected to the login page automatically.
	Onli	ine Upgrade	Local Upgrade
	_		
		i) Online up	grade will keep the current configuration. Please do not refresh the page or close th
	Cur	rent Version	ReveeOS 1.86
	Cui	Tent version	
	I	New Version	ReyeeOS 1.
		Description	1.
			2.
		Tip	1. If your device cannot access the Internet, please click Download File.
			2 Choose Local Ungrade to unload the file for local ungrade
			2. choose cour opgrade to upload the file for local upgrade.
			Upgrade Now

20.9.2 Local Upgrade

Choose Local Device > System > Upgrade > Local Upgrade.

Displays the device model and current software version. You can choose whether to keep the configuration upgrade or not. Click **Browse** to select the local software installation package, click **Upload** to upload the installation package and upgrade.

Online Upgrade	Local Upgrade						
•							
1 Please do	not refresh the page or close t	the browser.					(?)
Model	NBS						
Current Version	ReyeeOS						
Keep Config	(If the target version is)	much later th	nan the current	version, it is re-	commended not	to keep the config	uration.)
File Path	Please select a file.	Browse	Upload				

20.10 LED

Choose Network Management> Network > LED.

Click the button to control the LED status of the downlink AP. Click **Save** to deliver the configuration and make it take effect.

1	LED Status Cor Control the LED	ntrol status of the downlink AP.	
	Enable		
		Save	

20.11 Switching the System Language

Click English ~

in the upper-right corner of the Web page.

Click a required language to switch the system language.

Ruijie Rcycc	Networkwide Ma 🗸	tion Q English ∨ △Remote O&M
Q Navigation	Reboot Scheduled Reboot	简体中文
Overview	Please keen the device powered on during reboot	English
A Network		繁彊中又 Español
Devices	Select Master device All Devices Specified Devic	Bahasa Indonesia
③ Clients Management	Reboot	Русский
		Türkçe
System Time		Tiếng Việt
Login Password		اللغه العربية
Backup		
SNMP		
Reboot		6
Cloud Service «Collapse		

21 NBS and NIS Series Switches Wi-Fi Network Setup

Note

- To manage other devices in the self-organizing network, enable the self-organizing network discovery function. (See <u>11.1.1</u> <u>2</u>. Switching the Work Mode) The wireless settings are synchronized to all wireless devices in the network by default. You can configure groups to limit the device scope under wireless management. For details, see <u>21.1</u> <u>Configuring AP Groups</u>.
- The device itself does not support transmitting wireless Wi-Fi signals, and the wireless settings need to be synchronized to the wireless devices in the network to take effect.

21.1 Configuring AP Groups

21.1.1 Overview

After self-organizing network discovery is enabled, the device can function as the master AP/AC to batch configure and manage its downlink APs by group. Before you configure the APs, divide them to different groups.

🚺 Note

If you specify groups when configuring the wireless network, the configuration takes effect on wireless devices in the specified groups.

21.1.2 Procedure

Choose Network > Devices > AP.

(1) View the information of all APs in the current network, including the basic information, RF information, and model. Click the SN of an AP to configure the AP separately.

All (1)	Gateway (0)	AP (1)	Switch (0)	AC (0)	Router (0)						
0	Device List A devices not in SON is	s discovered.	Manage								
Dev	ice List 🕃 Group:	All Groups	Expand	Change Group	Basic Info	RF Information	Model				
						IP/M.	AC/hostname/	SN/S Q	🗎 Delete Off	fline Devices	Batch Upgrade
	SN 🜩	Status 🌲	Hostname	\$	MAC ≑	IP 🔶	Clients ≑	Device	Group	Relay Informatio \$	n
Jeed	SN \$	Status 🗢 Online	Hostname Ruijie (Mast	e ♦ I er] & EC:B:	MAC \$ 9:70:23:A4:BF	IP ≑ 172.26.1.32 &	Clients \$	Device defaultNe	e Group etwork/默认	Relay Informatio	n

(2) Click Expand. Information of all the current groups is displayed to the left of the list. Click + to create a group. You can create a maximum of eight groups. Select the target group and click / to modify the group

name or click it to delete the group. You cannot modify the name of the default group or delete the default group.

Devic	e List Group	: All Groups	Expand Change	e Group
	SN 🔶	Status ≑	Hostname 🔶	MAC
Local	G1QH6WX000610	Online	Ruijie [Master] 🖉	EC:B9:70:
Devi	ce List Gro	up: All Group	5 Collapse	
Search	by Group		SN 🔶	
 All G Defat 	Groups	+	G1QH6WX00061	

(3) Click a group name in the left. All APs in the group are displayed. One AP can belong to only one group. By default, all APs belong to the default group. Select a record in the device list and click Change Group to migrate the selected device to the specified group. After a device is moved to the specified group, the device will use the configuration for the new group. Click Delete Offline Devices to remove offline devices from the list.

Device List 😳 Group: All Groups	Collapse Ch	nange Group	Basic Info RF In	nformation Model	IP/MAC/hostna	me/SN/S Q	🖻 Delete Offline Devic	Batch Upgrade
Search by Group	sn \$	Status ≑	Hostname 🔶	MAC ≑	IP \$	Clients ≑	Device Group	Relay Information \$
Default (2) (2) (2) (3) (4) (4) (4) (4) (4) (4) (4) (4) (4) (4	61QH6WX000610	Online	Ruijie [Master] 🖉	EC:B9:70:23:A4:BF	172.26.1.32 🖉	0	test/默认组	Wired View Details

Change Group		×
Select Group	Select ^	
	Default test	el

21.2 Configuring Wi-Fi

Choose Network > Wi-Fi > Wi-Fi Settings.

Enter the Wi-Fi name and Wi-Fi password, select the frequency band used by the Wi-Fi signal, and click Save.

Click Advanced Settings to configure more Wi-Fi parameters.

A Caution

Modification will cause restart of the wireless configuration, resulting in logout of connected clients. Exercise caution when performing this operation.

Rujje Rcycc	Networked& Ma	ut
Navigation Overview	WI-Fi Settings WI-Fi List Healthy Mode Load Balancing	
A Network	Trg: Changing configuration requires a reboot and clients will be reconnected.	
Network Planning	Wi-Fi Settings Device Groups: Detual:	
Wi-Fi	Up to 8 SSIDs can be added.	
LimitSpeed	Octivul @Ruije:m0DAF Octivul + Add Guest WI-FI I cellul VLAN + Add WI-FI	
RLDP	RANG ZAL+50	
DHCP Snooping WIO	* SSID @&uije-mDDAF	
Radio Frequency	Band 🛿 2.46 🖾 56	
Reyee Mesh	Encryption 🕐 Open 💿 Security 💿 802.1x (Enterprine) 👁	
LAN Ports	* Security OPEN(Open) V	
LED	College	
Alarms	Wi-Fi Standard 802.11ac(Wi-Fi6)	
Batch Config		
Devices	www.subware	
🖻 Gateway	VLAN Default VLAN v	
Clients Management	Hide SSID 💿 (The SSID is hidden and must be manually entered.)	
🗄 System 🗸	Client Isolation () (Prevent wireless clients of this WI-Fi from communicating with one another.)	
	Band Steering Om (The SG-supported client will access SG radio preferentially.)	
	XPress () (The client will experience faster speed.)	
	Layer 3 Roaming 💿 (The client will keep the IP address unchanged on the WI-Fi network.) 💿	
	UmitSpeed 🕕	
	Do you want to edit RF parameters? Navigate to Radio Frequency for configuration.	
	Save	
< Collapse		

Table 11-1 Wireless Network Configuration

Parameter	Description
SSID	Enter the name displayed when a wireless client searches for a wireless network.
SSID Encoding	If the SSID does not contain Chinese, this item will be hidden. If the SSID contains Chinese, this item will be displayed. You can select UTF-8 or GBK.

Parameter	Description
Band	Set the band used by the Wi-Fi signal. The options are 2.4 GHz and 5 GHz. The 5 GHz band provides faster network transmission rate and less interference than the 2.4 GHz band, but is inferior to the 2.4 GHz band in terms of signal coverage range and wall penetration performance. Select a proper band based on actual needs. The default value is 2.4G + 5G , indicating that the device provides signals at both 2.4 GHz and 5 GHz bands.
Security	Select an encryption mode for the wireless network connection. The options are as follows: Open: The device can associate with Wi-Fi without a password. WPA-PSK/WPA2-PSK: Wi-Fi Protected Access (WPA) or WPA2 is used for encryption. WPA_WPA2-PSK (recommended): WPA2-PSK or WPA-PSK is used for encryption.
Wi-Fi Password	Specify the password for connection to the wireless network. The password is a string of 8 to 16 characters.
Wi-Fi Standard	Refers to the wireless communication protocol version, such as Wi-Fi 4 (802.11n), Wi-Fi 5 (802.11ac), Wi-Fi 6 (802.11ax), determining speed, frequency, and other wireless features.
Wireless Schedule	Specify the time periods during which Wi-Fi is enabled. After you set this parameter, users cannot connect to Wi-Fi in other periods.
VLAN	Set the VLAN to which the Wi-Fi signal belongs.
Hide SSID	Enabling the hide SSID function can prevent unauthorized user access to Wi- Fi, improving security. However, mobile phones or computers cannot find the Wi-Fi name after this function is enabled. You must manually enter the correct name and password to connect to Wi-Fi. Record the current Wi-Fi name before you enable this function.
Client Isolation	After you enable this parameter, clients associated with the Wi-Fi are isolated from one other, and end users connected to the same AP (in the same network segment) cannot access each other. This improves security.

Parameter	Description
Band Steering	After this function is enabled, 5G-capable clients select 5G Wi-Fi preferentially. You can enable this function only when Band is set to 2.4G + 5G .
XPress	After this function is enabled, the device sends game packets preferentially, providing more stable wireless network for games.
Layer-3 Roaming	After this function is enabled, clients keep their IP addresses unchanged when associating with the same Wi-Fi. This function improves the roaming experience of users in the cross-VLAN scenario.
Wi-Fi6	After this function is enabled, wireless users can have faster network access speed and optimized network access experience. This function is valid only on APs and routers supporting 802.11ax. Clients must also support 802.11ax to experience high-speed network access empowered by Wi-Fi 6. If clients do not support Wi-Fi 6, disable this function.
LimitSpeed	Specifies the maximum data transfer rate allowed for a device or user on the Wi-Fi network, often set to manage bandwidth allocation or ensure fair usage among connected devices.

21.3 Configuring Guest Wi-Fi

Choose Network > Wi-Fi > Guest Wi-Fi.

Guest Wi-Fi is a wireless network provided for guests, and is disabled by default. **Client Isolation** is enabled for guest Wi-Fi by default, and it cannot be disabled. In this case, users associating with guest Wi-Fi are mutually isolated, and they can only access the Internet through Wi-Fi. This improves network access security. You can configure a wireless schedule for the guest network. After the specified schedule expires, the guest network will become unreachable.

Click **+Add Guest Wi-Fi** and set the guest Wi-Fi name and password. Click **Expand** to configure the wireless schedule of the guest Wi-Fi and more Wi-Fi parameters. (For details, see <u>21.2</u> <u>Configuring Wi-Fi</u>.) Click **Save**. Guests can access the Internet through Wi-Fi after entering the Wi-Fi name and password.

Ruíjie Rcycc Na	etworkwide Ma 😞	Navigation	Q Eng	lish ~ 🛆	٩	Q	<u>بة</u> (
Q Navigation [™]	-Fi Settings WI-Fi List Healthy Mode Load Balancing Tip: Changing configuration requires a reboot and clients will be reconnected. Wi-Fi Settings Device Group: Default </th <th></th> <th></th> <th></th> <th></th> <th></th> <th>0</th>						0
WI-Fi LimitSpeed RLDP	Up to 8 SSIDs can be added. Pefault @Ruijie-mDDAF Default VLAN Band:2.4G+5G + Add Guest Wi-Fi + Add Wi-Fi						
* SSID Band	©Ruijie-guest-DDAF ☑ 2.4G ☑ 5G	ĸ					
Encryption * Security	Open Security 802.1x (Enterprise) OPEN(Open) Collapse						
Wi-Fi Standard	802.11ax(Wi-Fi6)						
Effective Time	Never Disable \lor						
VLAN	Default VLAN ~						
Hide SSID Client Isolation	 (The SSID is hidden and must be manually entered.) (Prevent wireless clients of this Wi-Fi from communicating with one another.) 						
Band Steering	ing (The 5G-supported client will access 5G radio preferentially.)						
XPress Layer 3 Roaming	(The client will experience faster speed.) (The client will keep the IP address unchanged on the Wi-Fi network.) ②						
LimitSpeed	Do you want to edit RF parameters? Navigate to Radio Frequency for configuration.						
	Cancel OK						

21.4 Adding a Wi-Fi

Choose Network > Wi-Fi > Wi-Fi List.

Click **Add**, enter the Wi-Fi name and password, and click **OK** to create a Wi-Fi. Click **Expand** to configure more Wi-Fi parameters. For details, see <u>21.2</u> <u>Configuring Wi-Fi</u>. After a Wi-Fi is added, clients can find this Wi-Fi, and the Wi-Fi information is displayed in the Wi-Fi list.

Ruíjie Reyce	Networkwide Ma \vee		Navigation	Q English ∽ △Remote O&/V	🛛 💩 Network Configuration	@ Network Check 拙 Alert 금 Log Out
Navigation Overview Network Network Planning	Wi-Fi Settings Wi-Fi Lis Tip: Changing configur Wi-Fi List Device Grou	Healthy Mode Load Balancing ation requires a reboot and clients will be re	3 connected.			() + Add Wi-Fi
Wi-Fi LimitSpeed	SSID	Band	Security	Hidden	VLAN ID	Action
RLDP	@Ruijie-mDDAF	2.4G 5G	OPEN(Open)	No	Default VLAN	Edit Delete
DHCP Snooping						
WIO						
Add	euration will take o	fact they being delivery	ite AD	×		
	* SSID Band 💟 2.4G	Z 5G				
Enc	cryption 💿 Open	O Security 🔵 802.1	Ix (Enterprise) 🜖			
* (Security OPEN(Op	pen)	\sim			
	Ε	xpand	Canc	el OK		

21.5 Healthy Mode

Choose Network > Wi-Fi > Healthy Mode.

Turn on healthy mode and select a wireless schedule for the mode.

After the healthy mode is enabled, the RF transmit power and Wi-Fi coverage range of the wireless device are reduced in the schedule. This may lead to weak signals and network freezing. You are advised to disable healthy mode or set the wireless schedule to the idle periods.

Ruíjie Rcycc	Networkwide Ma	🕞 Log Out
Q Navigation	Wi-Fi Settings Wi-Fi List Healthy Mode Load Balancing	
Overview Network ^	Trable the healthy mode. The device will decrease its transmit power to reduce radiation. Tp: Changing configuration requires a reboot and clients will be reconnected.	0
Network Planning	Healthy Mode Device Group: Default v	
Wi-Fi	Enable 💽	
LimitSpeed	Effective Time All Time V	
RLDP DHCP Snooping	Save	
WIO		

21.6 RF Settings

Choose Networkwide Management > Network > Radio Frequency.

The wireless device can detect the surrounding wireless environment upon power-on and select proper configuration. However, network freezing caused by wireless environment changes cannot be prevented. You can analyze the wireless environment around the APs and routers and manually select proper parameters.

A Caution

Modification will cause restart of the wireless configuration, resulting in logout of connected clients. Exercise caution when performing this operation.

Ruíjie Rcycc	Networkwide Ma		Navigation O English ~ Q Remote O&M A Network Configuration G Log Out
Q Navigation	🧃 Tip: Changir	g configuration requires a reboot and clients will be reconnected.	
Network Planning	Radio Frequ	Iency Device Group: Default 🗸	Not solved yet? Click here to access the Network Optimization page for automatic optimization.
Wi-Fi	Radio Parameters		
LimitSpeed	Country/Reg	ion China (CN) \vee	
RLDP	Radio Parameters		
DHCP Snooping	2.4G	Global Radio Settings	
WIO		Channel Width Auto ~	
Wireless Auth	5G	Multicast Rate (Mbns)	
802.1x Authentication		0	
Radio Frequency		Client Count Limit 64	
Reyee Mesh		Disconnection	
LAN Ports		Threshold Disable -85dBm -65dBm	
LED		0	
Alarms		for a	
«Collapse		Save	

Table 11-2 RF Configuration

Parameter	Description
Country/Region	The Wi-Fi channels stipulated by each country may be different. To ensure that clients can find the Wi-Fi signal, select the country or region where the device is located.
2.4G/5G	A lower bandwidth indicates more stable network, and a higher bandwidth indicates easier interference. In case of severe interference, select a relatively low bandwidth to prevent network freezing to certain extent. The 2.4 GHz band supports the 20 MHz and 40 MHz bandwidths. The 5 GHz band supports the 20 MHz, 40 MHz, and 80 MHz bandwidths. By default, the value is Auto , indicating that the bandwidth is selected automatically based on the environment.
Client Count Limit	If a large number of users access the AP or router, the wireless network performance of the AP or router may be degraded, affecting users' Internet access experience. After you set this parameter, new user access is prohibited when the number of access users reaches the specified value. If the clients require high bandwidth, you can adjust this parameter to a smaller value. You are advised to keep the default value unless otherwise specified.
Disconnection Threshold	When multiple Wi-Fi signals are available, you can set this parameter to optimize the wireless signal quality to some extent. When a client is far away from the wireless device, the Wi-Fi connection is disconnected when the wireless signal strength of the end user is lower than the kick-off threshold. In this case, the client has to select a nearer wireless signal. The client is prone to be kicked off if the kick-off threshold is high. To ensure that the client can normally access the Internet, you are advised to set this parameter to Disable or a value smaller than -75 dBm.

1 Note

- Wireless channels available for your selection are determined by the country code. Select the country code based on the country or region of your device.
- Channel, transmit power, and roaming sensitivity cannot be set globally, and the devices should be configured separately.

21.7 Configuring Wi-Fi Blocklist or Allowlist

21.7.1 Overview

You can configure the global or SSID-based blocklist and allowlist. The MAC address supports full match and OUI match.

Wi-Fi blocklist: Clients in the Wi-Fi blocklist are prevented from accessing the Internet. Clients that are not added to the Wi-Fi blocklist are free to access the Internet.

Wi-Fi allowlist: Only clients in the Wi-Fi allowlist can access the Internet. Clients that are not added to the Wi-Fi allowlist are prevented from accessing the Internet.

A Caution

If the allowlist is empty, the allowlist does not take effect. In this case, all clients are allowed to access the Internet.

21.7.2 Configuring a Global Blocklist/Allowlist

Choose Clients Management > Blocklist/Allowlist > Global Blocklist/Allowlist.

Select the blocklist or allowlist mode and click **Add** to configure a blocklist or allowlist client. In the **Add** window, enter the MAC address and remark of the target client and click **OK**. If a client is already associated with the access point, its MAC address will pop up automatically. Click the MAC address directly for automatic input. All clients in the blocklist will be forced offline and not allowed to access the Wi-Fi network. The global blocklist and allowlist settings take effect on all Wi-Fi networks of the access point.

Ruíjie Royco	Networkwide Ma 🗸		Navigation Q English ~ A 🛕 🗗
Q Navigation	Global Blocklist/Allowlist SSID-Based Blocklist/Allowlist		
Overview			
🖇 Network	• All STAs except blocklisted STAs are allowed to access Wi-Fi.	 Only the allowlisted STAs are allowed 	I to access Wi-Fi.
Devices	Blocked WLAN Clients		+ Add 🗎 Delete Selected
8 Clients Management	Up to 256 members can be added.		
Clients	Device Name	MAC Address	Action
Blocklist/Allowlist	□ 11 <i>ℓ</i> _	11:11:33:22:44:22	Edit Delete
System 🗸	< 1 > 10/page < Go to page 1		Total 1
«Collapse			1

Add		×
Match Type	• Full O Prefix (OUI)	
* MAC	Example: 00:11:22:33:44:55	
Remark		
	Cancel	ОК

If you click **Delete** in black list mode, the corresponding client can reconnect to Wi-Fi; if you click **Delete** in allowlist mode and the allowlist list is not empty after deletion, the corresponding client will be disconnected and prohibited from connecting to Wi-Fi.

• All STAs except blacklisted STAs are allowed to access Wi-Fi.		Vi-Fi. Only the v	Only the whitelisted STAs are allowed to access Wi-Fi.		
Blocked WL	AN Clients		+ Add 🗇 Delete Selected		
Up to 64 mer	nbers can be added.				
	MAC	Remark	Action		
	AE:4E:11 OUI		Edit Delete		
	11:22:33:44:55:66		Edit Delete		

21.7.3 Configuring an SSID-based Blocklist/Allowlist

Choose Clients > Blocklist/Allowlist > SSID-Based Blocklist/Allowlist.

Select a target Wi-Fi network from the left column, select the blocklist or allowlist mode, and click Add to configure a blocklist or allowlist client. The SSID-based blocklist and allowlist will restrict the client access to the specified Wi-Fi.

Ruíjie Rcycc	Networkwide Ma 🗸		Navigation O	English - 🛆 🤮
Q Navigation	Global Blocklist/Allowlist SSID-Base	d Blocklist/Allowlist		
Overview	Blocklist/Allowlist is used to allow o	r reject a client's request to connect to the Wi-Fi network.		
🖧 Network 🗸 🗸	Note: OUI matching rule and SSID- Rule: 1. In the Blocklist mode, the L In the Allowlist mode on	based blocklist/allowlist are supported by only RAP Net and P32 (and late clients in the blocklist are not allowed to connect to the Wi-Fi network. by the clients in the allowlist are allowed to connect to the Wi-Fi network.	er versions).	
Devices				
8 Clients Management	Device Group: Default ~	• All STAs except blocklisted STAs are allowed to access Wi-Fi.		
Clients	@Ruijie-qqt	Only the allowlisted STAs are allowed to access Wi-Fi.		
Blocklist/Allowlist	test	Blocked WLAN Clients	+ Add	Delete Selected
°− °°- System ∨	@Ruijie-guest-2268	Up to 256 members can be added.		
		Device Name MAC Ac	ldress	Action
		No Data		
		< 1 > 10/page ~ Go to page 1		Total 0
Collapse				

21.8 Wireless Network Optimization with One Click

🛕 Caution

- WIO is supported only in the self-organizing network mode.
- The client may be offline during the optimization process. The configuration cannot be rolled back once optimization starts. Therefore, exercise caution when performing this operation.

21.8.1 Network Optimization

Choose Networkwide Management > Network > WIO > Network Optimization.

(1) Select the optimization mode. Then, click **OK** to optimize the wireless network.

Ruíjie Rcycc	Networkwide Ma English < @Remote O&M @Network Configuration
Q Navigation	Network Optimization Scheduled Optimization Optimization Record 802.11k/v Roaming Optimization
☆ Overview	In a networking environment, WIO can help maximize wireless performance by optimizing your network.
A Network	Optimization
Network Planning	Optimization Ouick optimization Deep optimization
Wi-Fi	mode:
LimitSpeed	Advanced Settings
RLDP	Estimated Time
DHCP Snooping	Environment scan
WIO	
Wireless Auth	Upgrade all APs to the latest version for optimal network optimization.
802.1x Authentication	WIO only supports 20 MHz, 40 MHz, and 80 MHz channel bandwidths at the moment.
Radio Frequency	• Please perform optimization after all APs in the target area are online.
Reyee Mesh	ОК
«Collapse	

Parameter	Description		
Quick optimization	In this mode, external interference and bandwidth are not considered. A quick optimization is performed to optimize channel, power, and management frame power		
optimization Deep optimization	 is performed to optimize channel, power, and management frame power. In this mode, external interference and bandwidth are considered. A deep optimization is performed to optimize channel, power, and management frame power. Click to expand Advanced Settings to configure the scanning time, channel bandwidth and channels. Scan time: Indicates the time for scanning channels during the optimization. Roaming Sensitivity: The roam sensitivity can be optimized based on the actual environment to ensure fast roaming of wireless devices. Transmit power: Increasing the transmit power enhances both the strength and coverage of the wireless signal, but it may also introduce interference to surrounding wireless networks. With this feature enabled, the AP will automatically adjust the transmit power based on the environment. 2.4G Channel bandwidth: Indicates the channel bandwidth. The channel bandwidth will be calculated by the system if Default is selected. Selected channels: Indicates the channels to be optimized. 		
	• 5G		
	 Channel bandwidth: Indicates the channel bandwidth. The channel bandwidth will be calculated by the system if Default is selected. 		
	 Selected channels: Indicates the channels to be optimized. 		

Table 21-1 Description of Optimization Mode

When the **Optimization mode** is configured as **Deep optimization**, expand the **Advanced Settings** to set the scanning time, channel bandwidth and selected channels.

Optimization					
Optimization	Quick optimization	 Deep optimization 			
mode:					
	Advanced Settings				
Scan time	10s	\sim			
Poaming					
Koaming					
Sensitivity					
Tana and A Damag					
fransmit Power					
	2.45				
	2.4G				
Channel Width	Default	~			
* Calaatad	1 (2 /12GHz) Q 2	(2 417GHz)			
* Selected	3 (2 422GHz) (2 4	(2.427GHz)			
channels	5 (2.432GHz) @ 6	(2.437GHz)			
	7 (2.442GHz) 🛞 8	(2.447GHz) 🛞 🗸			
	9 (2.452GHz) 🛞 10	(2.457GHz) 🛞			
	11 (2.462GHz) 🛞 1	2 (2.467GHz) 🛞			
	13 (2.472GHz) 🛞				
	5G				
Channel Width	Default	~			
	(
* Selected	36 (5.18GHz)	(5.2GHz) 🛞			
channels	44 (5.22GHZ) (Badar ch	(5.24GHZ)			
	52 (5.26GHz) (Radar channel)				
	60 (5.3GHz) (Radar cha	nnel) 🛞 🗸			
	64 (5.32GHz) (Radar ch	annel) 🛞			
	149 (5.745GHz) 🛞	153 (5.765GHz) 🛞			
	157 (5.785GHz) 🛞	161 (5.805GHz) 🛞			
	165 (5.825GHz) 🛞				

(2) Confirm the tips, and Click **OK**.

Tips

During optimization, the APs may switch channels and collect data, which may result in temporary disconnection and affect user experience. This situation may last for some time. You are advised to enable scheduled optimization if you require an Internet connection for the time being.

 \times

OK

321

After optimization starts, please wait patiently until optimization is complete. After optimization ends, click **Cancel Optimization** to restore optimized RF parameters to default values.

Network Optimization	Scheduled Optimization	Optimization Record 80	02.11k/v Roaming Optimiza	ation		
\bigcirc	Finish Completion time: 2023-11-1 Optimization mode: Quick of Time consumed: 39 seconds and improved user experience	7 15:17:10 ptimization . Optimized 1 APs, resolved sev ce by 0.00%.	ere interference of 0 APs, re	educed channel interference by (Cancel Op 0.00%, Back t	o Home
Optimization De	tails				Enter AP name/SN Q	5G 2.4G
Hostname 💠	Band 💠	SN \$	Channel Width (Before/After)	Channel (Before/After)	Transmit Power (Before/After)	Sensitivity (Before/After)
Ruijie	5G	G1RP6P8183248	80	52	auto->100	0
< 1 > 10/	/page \vee					Total 1

21.8.1 Scheduled Wireless Optimization

You can configure scheduled optimization to optimize the network at the specified time. You are advised to set the scheduled optimization time to daybreak or the idle periods.

A Caution

Clients may be kicked offline during optimization and the configuration cannot be rolled back after optimization starts. Exercise caution when performing this operation.

Ruíjie Rcycc	Networkwide Ma 🗸			Navigation Q	English ~	△ 🏾	Ð
Q Navigation	Network Optimization	Scheduled Optimization	Optimization Record	802.11k/v Roaming Optimization			
Overview	Scheduled Optim	ization					
🖧 Network 🗠	Optimize the netwo	ork performance at a scheduled	time for a better user experie	nce.			
Network Planning	Enable 🦲)					
Wi-Fi	Day Su	n ~					
LimitSpeed	Time 04	~ : 49 ~					
RLDP	Optimization 🔘 Q	uick optimization 📀 Dee	p optimization				
DHCP Snooping	mode:						
WIO	Ad	vanced Settings					e
Wireless Auth		Save					Ai
«Collapse							

Choose Networkwide Management > Network > WIO > Scheduled Optimization.

- (1) Configure the scheduled time.
- (2) Select the optimization mode.

(3) (Optional) When the Optimization Mode is configured as Deep optimization, expand the Advanced Settings to set the scanning time, channel bandwidth and selected channels.

Optimization C	Quick optimizatio	n 💿 Deep optimiz	ation		
	Advanced Settings				
Scan time	10c				
Scantine	105				
Roaming					
Sensitivity					
Transmit Power	D				
	2.4G				
Channel Width	Default		~		
* Selected	1 (2.412GHz)	2 (2 417GHz)			
Selected	3 (2.422GHz)	4 (2.427GHz)			
channels	5 (2.432GHz) 🛞	6 (2.437GHz)			
	7 (2.442GHz) 🛞	8 (2.447GHz) 🛞	\sim		
	9 (2.452GHz) 🛞	10 (2.457GHz) 🛞			
	11 (2.462GHz) 🛞	12 (2.467GHz) 🛞			
	13 (2.472GHz) 🛞				
	5G				
Channel Width	Default		~		
* Selected	36 (5.18GHz) 🛞	40 (5.2GHz) 🛞			
channels	44 (5.22GHz) 🛞	48 (5.24GHz) 🛞			
	52 (5.26GHz) (Rada	ir channel) 🛞			
	56 (5.28GHz) (Radar channel) 🛞				
	64 (E 22CU-) (B-1-	channel)	~		
	140 (5.32GHZ) (Kada				
	157 (5.785GHz)	161 (5 805GHz)			
	165 (5.825GHz)				

(4) Click Save.

21.8.2 Wi-Fi Roaming Optimization (802.11k/v)

Wi-Fi roaming is further optimized through the 802.11k/802.11v protocol. Smart endpoints compliant with IEEE 802.11k/v can switch association to the access points with better signal and faster speed, thereby ensuring high-speed wireless connectivity.

To ensure high quality of smart roaming service, the WLAN environment will be automatically scanned when Wi-Fi roaming optimization is first enabled.

Choose Networkwide Management > Network > WIO > Wi-Fi Roaming Optimization (802.11k/v).

Ruíjie Rcycc	Networkwide Ma $ imes $		Navigation	Q English ~ 🛆 🔮 🕞
Q Navigation	Network Optimization	Scheduled Optimization Optimization Record	802.11k/v Roaming Optimization	
Overview				
🖧 Network	⊘ Start	Q Scanning	Optimizing	Finish
Network Planning		Description		
Wi-Fi		The Wi-Fi roaming is further optimized through the 802 better signal and faster speed during the roaming proc	2.11k/v protocol. Smart clients compliant with 802 ess, ensuring high-speed wireless connectivity.	2.11k/v can switch to the APs with
LimitSpeed		To ensure smart roaming effect, the WLAN environmen	t will be auto scanned when Wi-Fi roaming optim	ization is first enabled.
RLDP		Notes: During the WLAN environment scanning, the APs will so	witch channels, forcing the clients to go offline. T	he process will last for 2 minutes.
DHCP Snooping		Optimization Mode O Performance-prior O Roa	ming-prior	
WIO		Enable		
Wireless Auth				
802.1x Authentication				
Radio Frequency «Collapse				

🛕 Caution

During the optimization, the clients may be forced offline. Please proceed with caution.

Select the Optimization Mode. Click Enable and the optimization starts.

21.9 Enabling the Reyee Mesh Function

Choose Network > Reyee Mesh.

After the Reyee Mesh function is enabled, the devices that support EasyLink can be paired to form a mesh network. Devices can automatically search for new routers around them and pair with each other via the **Mesh** button, or log in to the router management page to search and select a new router for pairing.

i	After enabling Re Mesh.	eyee Mesh, you can set up	p a Mesh network through Mesh pairing between the devices that support	Reyee
	Enable			
		Save		

21.10 Configuring the AP Ports

A Caution

The configuration takes effect only on APs having wired LAN ports.

Choose Network > LAN Ports.

Choose Network > LAN Ports.

Enter the VLAN ID and click **Save** to configure the VLAN, to which the AP wired ports belong. If the VLAN ID is null, the wired ports and WAN port belong to the same VLAN.

In self-organizing network mode, the AP wired port configuration applies to all APs having wired LAN ports on the current network. The configuration applied to APs in **LAN Port Settings** takes effect preferentially. Click **Add** to add the AP wired port configuration. For APs, to which no configuration is applied in **LAN Port Settings**, the default configuration of the AP wired ports will take effect on them.

 LAN Port Settings The configuration takes effect only for the AP with a LAN port, e.g., EAP101. Note: The configured LAN port settings prevail. The AP device with no LAN port settings will be enabled with default settings. 						
Default Settings						
VLAN ID		Add VLAN				
(Range: 2-232 and 234-4090. A blank value indicates the same VLAN as WAN port.) Applied to AP device with no LAN port settings						
LAN Port Settin	gs		+ Add			
Up to 8 VLAN IDs or	32 APs can be added (1 APs have been added).					
VLAN	ID \$ Ap	plied to		Action		
2		Ruijie		Edit Delete		

22 Reyee FAQ

- 22.1 <u>Reyee Password FAQ ((collection))</u>
- 22.2 <u>Reyee Flow Control FAQ((collection))</u>
- 22.3 <u>Reyee Self-Organizing Network (SON) FAQ ((collection))</u>
- 22.4 <u>Reyee series Devices Parameters Tables</u>
- 22.5 <u>Reyee Parameter Consultation FAQ ((collection))</u>