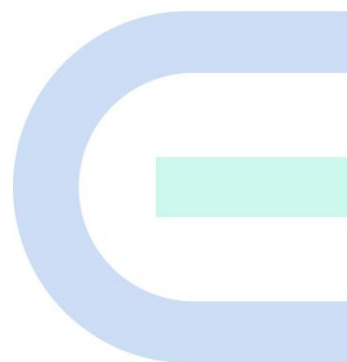


Ruijie Reyee RG-NBS, NIS3100 Series Switches

ReyeeOS 2.280[260] Configuration Guide



Copyright

Copyright © 2025 Ruijie Networks

All rights are reserved in this document and this statement.

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



and other Ruijie networks logos are trademarks of Ruijie Networks.

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

Disclaimer

The products, services, or features you purchase are subject to commercial contracts and terms, and some or all of the products, services, or features described in this document may not be available for you to purchase or use. Except for the agreement in the contract, Ruijie Networks makes no explicit or implicit statements or warranties with respect to the content of this document.

The names, links, descriptions, screenshots, and any other information regarding third-party software mentioned in this document are provided for your reference only. Ruijie Networks does not explicitly or implicitly endorse or recommend the use of any third-party software and does not make any assurances or guarantees concerning the applicability, security, or legality of such software. You should choose and use third-party software based on your business requirements and obtain proper authorization. Ruijie Networks assumes no liability for any risks or damages arising from your use of third-party software.

The content of this document will be updated from time to time due to product version upgrades or other reasons, Ruijie Networks reserves the right to modify the content of the document without any notice or prompt.

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

Preface

Intended Audience

This document is intended for:

- Network engineers
- Technical support and servicing engineers
- Network administrators

Technical Support

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




Conventions

1. GUI Symbols

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

2. Signs

The signs used in this document are described as follows:

| |
|--|
|  Warning |
| An alert that calls attention to important rules and information that if not understood or followed can result in data loss or equipment damage. |
|  Caution |
| An alert that calls attention to essential information that if not understood or followed can result in function failure or performance degradation. |
|  Note |
| An alert that contains additional or supplementary information that if not understood or followed will not lead to serious consequences. |

 **Specification**

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

3. Note

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

Contents

| | |
|---|----|
| Preface | I |
| 1 Change Description..... | 1 |
| 1.1 ReyeeOS 2.280.0.1718;SWITCH_3.0(1)B11P280,Release(11171809) | 1 |
| 1.1.1 Hardware Change..... | 1 |
| 1.1.2 Software Feature Change..... | 1 |
| 1.2 ReyeeOS 2.280.0.1621;SWITCH_3.0(1)B11P280,Release(11162101) | 1 |
| 1.2.1 Hardware Change..... | 1 |
| 1.2.2 Software Feature Change..... | 1 |
| 1.3 ReyeeOS 2.260 | 2 |
| 1.3.1 Hardware Change..... | 2 |
| 1.3.2 Software Feature Change..... | 3 |
| 2 Login..... | 4 |
| 2.1 Configuration Environment Requirements | 4 |
| 2.2 Logging in to the Web Interface..... | 4 |
| 2.2.1 Connecting to the Device..... | 4 |
| 2.2.2 Logging in to the Web Interface..... | 4 |
| 2.2.3 Layout Configuration..... | 6 |
| 2.3 Quick Setup | 7 |
| 2.3.1 Configuration Preparations | 7 |
| 2.3.2 Procedure..... | 7 |
| 2.3.3 Procedure for Configuring Hot Standby (VCS)..... | 10 |
| 2.4 Work Mode..... | 14 |

| | |
|---|----|
| 2.5 Switching the Management Mode | 14 |
| 3 Network-Wide Management | 16 |
| 3.1 Viewing Networking Information | 16 |
| 3.2 Adding Devices | 18 |
| 3.2.1 Adding a Device Through Wired Connection..... | 18 |
| 3.2.2 AP Mesh..... | 20 |
| 3.3 Configuring VLANs | 28 |
| 3.3.1 Configuring a Wired VLAN..... | 28 |
| 3.3.2 Configuring a Wi-Fi VLAN..... | 31 |
| 3.4 Network-wide Wireless Management..... | 33 |
| 3.5 Device Management..... | 34 |
| 3.6 Online Client Management | 35 |
| 3.6.1 Configuring Client IP Binding..... | 37 |
| 3.6.2 Configuring Client Access Control | 38 |
| 3.6.3 Blocking Clients | 39 |
| 3.6.4 Configuring Client Rate Limiting | 40 |
| 3.7 Firewall Management | 41 |
| 3.7.1 Viewing Firewall Information..... | 41 |
| 3.7.2 Configuring Firewall Port | 42 |
| 3.8 Alerts | 42 |
| 3.9 Smart Device Network | 44 |
| 3.9.1 Overview | 44 |
| 3.9.2 Procedure..... | 44 |
| 4 One-Device Information | 48 |

| | |
|--|----|
| 4.1 Basic information about the One-Device | 48 |
| 4.2 Smart Monitoring..... | 49 |
| 4.3 Port Info..... | 50 |
| 5 VLAN | 52 |
| 5.1 VLAN Overview..... | 52 |
| 5.2 Configuring a VLAN | 52 |
| 5.2.1 Adding a VLAN..... | 52 |
| 5.2.2 Modifying VLAN Description | 53 |
| 5.2.3 Deleting a VLAN | 54 |
| 5.3 Configuring Port VLAN | 54 |
| 5.4 Batch Switch Configuration..... | 57 |
| 6 Monitoring..... | 60 |
| 6.1 Port Flow | 60 |
| 6.2 Client Management..... | 60 |
| 6.2.1 Overview | 60 |
| 6.2.2 Displaying the MAC Address Table..... | 61 |
| 6.2.3 Configuring Static MAC Binding | 62 |
| 6.2.4 Displaying Dynamic MAC Address | 63 |
| 6.2.5 Configuring MAC Address Filtering | 64 |
| 6.2.6 Configuring MAC Address Aging Time | 66 |
| 6.2.7 Displaying ARP Information | 66 |
| 6.3 Viewing Optical Transceiver Info | 67 |
| 7 Ports | 69 |
| 7.1 Overview | 69 |

| | |
|--|----|
| 7.2 Port Configuration | 70 |
| 7.2.1 Basic Settings | 70 |
| 7.2.2 Physical Settings..... | 73 |
| 7.3 Aggregate Ports | 76 |
| 7.3.1 Aggregate Port Overview | 76 |
| 7.3.2 Overview | 77 |
| 7.3.3 Aggregate Port Configuration | 78 |
| 7.3.4 Configuring a Load Balancing Mode | 80 |
| 7.3.5 Configuring LACP Settings | 80 |
| 7.4 Port Mirroring | 82 |
| 7.4.1 Overview | 82 |
| 7.4.2 Procedure..... | 83 |
| 7.5 Rate Limiting | 85 |
| 7.6 MGMT IP Configuration | 87 |
| 7.7 Configuring the Management IPv6 Address..... | 88 |
| 7.8 Out-of-Band IP Configuration | 89 |
| 7.9 PoE Configuration..... | 90 |
| 7.9.1 PoE Global Settings..... | 91 |
| 7.9.2 Power Supply Configuration of Ports..... | 92 |
| 7.9.3 Displaying Global PoE Information | 94 |
| 7.9.4 Displaying the Port PoE Information..... | 94 |
| 8 L2 Multicast | 96 |
| 8.1 Multicast Overview..... | 96 |
| 8.2 Multicast Global Settings | 96 |

| | |
|---|-----|
| 8.3 IGMP Snooping..... | 97 |
| 8.3.1 Overview | 97 |
| 8.3.2 Enabling Global IGMP Snooping | 97 |
| 8.3.3 Configuring Protocol Packet Processing Parameters | 98 |
| 8.4 Configuring MVR..... | 100 |
| 8.4.1 Overview | 100 |
| 8.4.2 Configuring Global MVR Parameters | 101 |
| 8.4.3 Configuring the MVR Ports | 101 |
| 8.5 Configuring Multicast Group | 103 |
| 8.6 Configuring a Port Filter | 104 |
| 8.6.1 Configuring Profile | 105 |
| 8.6.2 Configuring a Range of Multicast Groups for a Profile | 106 |
| 8.7 Setting an IGMP Querier | 107 |
| 8.7.1 Overview | 107 |
| 8.7.2 Procedure..... | 108 |
| 9 L3 Multicast | 110 |
| 9.1 Overview | 110 |
| 9.2 Multicast Routing Table | 110 |
| 9.3 Configuring PIM | 111 |
| 9.3.1 Overview | 111 |
| 9.3.2 Enabling PIM..... | 111 |
| 9.3.3 Viewing PIM Neighbor Table..... | 112 |
| 9.4 Configuring RP..... | 113 |
| 9.4.1 Overview | 113 |

| | |
|--|-----|
| 9.4.2 Configuring a Static RP | 113 |
| 9.4.3 Configuring a Candidate RP | 113 |
| 9.5 Configuring BSR | 114 |
| 9.5.1 Overview | 114 |
| 9.5.2 Configuring BSR | 115 |
| 9.5.3 Viewing BSR Routing Info..... | 115 |
| 9.6 Configuring IGMP | 115 |
| 9.6.1 Overview | 115 |
| 9.6.2 Enabling IGMP | 116 |
| 9.6.3 Viewing IGMP Multicast Group..... | 116 |
| 10 L3 Management | 118 |
| 10.1 Setting an L3 Interface..... | 118 |
| 10.2 Configuring the IPv6 Address for the L3 Interface | 119 |
| 10.3 Configuring the DHCP Service | 122 |
| 10.3.1 Enable DHCP Services..... | 122 |
| 10.3.2 Viewing the DHCP Client | 124 |
| 10.3.3 Configuring Static IP Addresses Allocation..... | 124 |
| 10.3.4 Configuring the DHCP Server Options | 125 |
| 10.4 Configuring the DHCPv6 Server..... | 126 |
| 10.4.1 Viewing DHCPv6 Clients | 128 |
| 10.4.2 Configuring the Static DHCPv6 Address | 128 |
| 10.5 Configuring the IPv6 Neighbor List..... | 130 |
| 10.6 Configuring a Static ARP Entry | 131 |
| 11 Configuring Route..... | 133 |

| | |
|--|-----|
| 11.1 Configuring Static Routes | 133 |
| 11.2 Configuring the IPv6 Static Route | 135 |
| 11.3 Configuring RIP..... | 136 |
| 11.3.1 Configuring RIP Basic Functions | 136 |
| 11.3.2 Configuring the RIP Port | 138 |
| 11.3.3 Configuring the RIP Global Configuration..... | 140 |
| 11.3.4 Configuring the RIP Route Redistribution List | 141 |
| 11.3.5 Configuring the Passive Interface | 143 |
| 11.3.6 Configuring the Neighbor Route | 144 |
| 11.4 Configuring RIPng | 145 |
| 11.4.1 Configuring RIPng Basic Functions | 145 |
| 11.4.2 Configuring the RIPng Port | 147 |
| 11.4.3 Configuring the RIPng Global Configuration..... | 148 |
| 11.4.4 Configuring the RIPng Route Redistribution List | 149 |
| 11.4.5 Configuring the RIPng Passive Interface..... | 150 |
| 11.4.6 Configuring the RIPng Aggregate Route | 152 |
| 11.5 OSPFv2..... | 152 |
| 11.5.1 Configuring OSPFv2 Basic Parameters | 152 |
| 11.5.2 Adding an OSPFv2 Interface | 159 |
| 11.5.3 Redistributing OSPFv2 Instance Routes | 161 |
| 11.5.4 Managing OSPFv2 Stub Areas | 162 |
| 11.5.5 Managing OSPFv2 Neighbors | 162 |
| 11.5.6 Viewing OSPFv2 Neighbor Information | 163 |
| 11.6 OSPFv3..... | 163 |

| | |
|--|-----|
| 11.6.1 Configuring OSPFv3 Basic Parameters | 163 |
| 11.6.2 Adding an OSPFv3 Interface | 173 |
| 11.6.3 Managing OSPFv3 Stub Areas | 174 |
| 11.6.4 Viewing OSPFv3 Neighbor Information | 175 |
| 11.7 Routing Table Info | 175 |
| 12 Security | 176 |
| 12.1 DHCP Snooping..... | 176 |
| 12.1.1 Overview | 176 |
| 12.1.2 Standalone Device Configuration | 176 |
| 12.1.3 Batch Configuring Network Switches | 176 |
| 12.2 Storm Control..... | 179 |
| 12.2.1 Overview | 179 |
| 12.2.2 Procedure..... | 179 |
| 12.3 ACL | 180 |
| 12.3.1 Overview | 180 |
| 12.3.2 Creating ACL Rules | 180 |
| 12.3.3 Applying ACL Rules | 183 |
| 12.4 Port Protection | 184 |
| 12.5 IP-MAC Binding | 184 |
| 12.5.1 Overview | 184 |
| 12.5.2 Procedure..... | 185 |
| 12.6 IP Source Guard | 186 |
| 12.6.1 Overview | 186 |
| 12.6.2 Viewing Binding List..... | 186 |

| | |
|---|-----|
| 12.6.3 Enabling Port IP Source Guard | 187 |
| 12.6.4 Configuring Exceptional VLAN Addresses | 188 |
| 12.7 Configure 802.1x authentication..... | 189 |
| 12.7.1 Function introduction..... | 189 |
| 12.7.2 Configuration 802.1x..... | 190 |
| 12.7.3 View the list of wired authentication users..... | 195 |
| 12.8 Anti-ARP Spoofing..... | 195 |
| 12.8.1 Overview | 195 |
| 12.8.2 Procedure..... | 195 |
| 13 Advanced Configuration | 197 |
| 13.1 STP | 197 |
| 13.1.1 STP Global Settings..... | 197 |
| 13.1.2 Applying STP to a Port..... | 198 |
| 13.2 LLDP | 201 |
| 13.2.1 Overview | 201 |
| 13.2.2 LLDP Global Settings..... | 201 |
| 13.2.3 Applying LLDP to a Port..... | 202 |
| 13.2.4 Displaying LLDP information | 203 |
| 13.3 RLDP..... | 204 |
| 13.3.1 Overview | 204 |
| 13.3.2 Standalone Device Configuration | 205 |
| 13.3.3 Batch Configuring Network Switches | 207 |
| 13.4 ERPS | 209 |
| 13.4.1 Overview | 209 |

| | |
|--|-----|
| 13.4.2 Control VLAN and Data VLAN | 209 |
| 13.4.3 Basic Model of an Ethernet Ring | 210 |
| 13.4.4 RPL and Nodes | 212 |
| 13.4.5 ERPS Packet | 213 |
| 13.4.6 ERPS Timer | 213 |
| 13.4.7 Ring Protection | 214 |
| 13.4.8 Protocols and Standards | 214 |
| 13.4.9 Configuring ERPS | 214 |
| 13.4.10 ERPS Typical Configuration Examples | 217 |
| 13.5 QoS | 223 |
| 13.5.1 Overview | 223 |
| 13.5.2 Principles | 224 |
| 1.1.2 Configuring QoS | 227 |
| 13.6 Configuring the Local DNS | 232 |
| 13.7 Voice VLAN | 233 |
| 13.7.1 Overview | 233 |
| 13.7.2 Voice VLAN Global Configuration | 233 |
| 13.7.3 Configuring a Voice VLAN OUI | 234 |
| 13.7.4 Configuring the Voice VLAN Function on a Port | 235 |
| 13.8 Configuring Smart Hot Standby (VCS) | 237 |
| 13.8.1 Configuring Hot Standby | 237 |
| 13.8.2 Configuring DAD Interfaces | 237 |
| 13.8.3 Active/Standby Switchover | 238 |
| 14 Diagnostics | 239 |

| | |
|---|-----|
| 14.1 Info Center | 239 |
| 14.1.1 Port Info..... | 239 |
| 14.1.2 VLAN Info..... | 240 |
| 14.1.3 Routing Info..... | 240 |
| 14.1.4 DHCP Clients | 241 |
| 14.1.5 ARP List | 241 |
| 14.1.6 MAC Address | 242 |
| 14.1.7 DHCP Snooping..... | 242 |
| 14.1.8 IP-MAC Binding | 243 |
| 14.1.9 IP Source Guard | 243 |
| 14.1.10 PoE | 244 |
| 14.1.11 CPP Info | 244 |
| 14.2 Network Tools | 245 |
| 14.2.1 Ping | 245 |
| 14.2.2 Traceroute | 246 |
| 14.2.3 DNS Lookup..... | 247 |
| 14.3 Fault Collection | 248 |
| 14.4 Cable Diagnostics | 248 |
| 14.5 System Logs | 249 |
| 14.6 Alerts | 249 |
| 15 System Configuration..... | 252 |
| 15.1 Setting the System Time..... | 252 |
| 15.2 Setting the Web Login Password | 252 |
| 15.3 Setting the Session Timeout Duration | 253 |

| | |
|--|-----|
| 15.4 Configuring SNMP | 253 |
| 15.4.1 Overview | 253 |
| 15.4.2 Global Configuration | 254 |
| 15.4.3 View/Group/Community/Client Access Control | 255 |
| 15.4.4 SNMP Service Typical Configuration Examples | 262 |
| 15.4.5 Trap service configuration..... | 267 |
| 15.4.6 Typical configuration examples of the trap service..... | 271 |
| 15.5 Configuration Backup and Import..... | 274 |
| 15.6 Reset..... | 275 |
| 15.6.1 Resetting the Device..... | 275 |
| 15.6.2 Resetting the Devices on the network..... | 275 |
| 15.7 Rebooting the Device | 276 |
| 15.7.1 Rebooting the Device..... | 276 |
| 15.7.2 Rebooting the Devices on the Network | 276 |
| 15.7.3 Rebooting Specified Devices on the Network | 277 |
| 15.8 Configuring Scheduled Reboot..... | 277 |
| 15.9 Upgrade | 278 |
| 15.9.1 Online Upgrade..... | 278 |
| 15.9.2 Local Upgrade..... | 279 |
| 15.10 Cloud Service..... | 279 |
| 15.10.1 Overview | 279 |
| 15.10.2 Configuration Steps | 280 |
| 15.10.3 Unbinding Cloud Service | 281 |

1 Change Description

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

1.1 ReyeeOS 2.280.0.1718;SWITCH_3.0(1)B11P280,Release(11171809)

1.1.1 Hardware Change

The following table lists the applicable hardware models of this version.

| Model | Hardware Version |
|------------|------------------|
| RG-NBS6002 | 1.0x, 2.0x |
| RG-NBS7003 | 1.0x, 2.0x |
| RG-NBS7006 | 1.0x, 2.0x |

1.1.2 Software Feature Change

- Before the change: RG-NIS3100, RG-NBS3100, RG-NBS3200, RG-NBS5100, RG-NBS5200, and RG-NBS5300 series switches running ReyeeOS 2.280.0.1621 or later support QoS.
- After the change:
 - RG-NIS3100, RG-NBS3100, RG-NBS3200, RG-NBS5100, RG-NBS5200, and RG-NBS5300 series switches running ReyeeOS 2.280.0.1621 or later support QoS.
 - RG-NBS6000 and RG-NBS7000 series switches running ReyeeOS 2.280.0.1718 or later support QoS.

1.2 ReyeeOS 2.280.0.1621;SWITCH_3.0(1)B11P280,Release(11162101)

1.2.1 Hardware Change

This version has no hardware change.

1.2.2 Software Feature Change

1. New Feature: ERPS

This version supports ERPS. RG-NIS3100, RG-NBS3100, RG-NBS3200, and RG-NBS5100 series switches running ReyeeOS 2.280.0.1621 or later support ERPS and QoS. For details, see [13.4 ERPS](#).

2. New Feature: QoS

This version supports QoS. RG-NIS3100, RG-NBS3100, RG-NBS3200, RG-NBS5100, RG-NBS5200, and RG-NBS5300 series switches running ReyeeOS 2.280.0.1621 or later support QoS. For details, see [13.5 QoS](#).

1.3 ReyeeOS 2.260

1.3.1 Hardware Change

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

| Model | Hardware Version |
|--------------------------|--|
| RG-NBS3100-8GT2SFP | 1.0x, 1.1x, 1.2x |
| RG-NBS3100-8GT2SFP-P | 1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 1.5x |
| RG-NBS3100-24GT4SFP | 1.0x, 1.1x, 1.2x, 2.0x, 2.1x, 2.2x, 3.0x, 3.1x, 3.2x |
| RG-NBS3100-24GT4SFP-P | 1.0x, 2.0x, 2.1x, 2.2x, 2.3x, 3.0x, 3.1x |
| RG-NBS3100-48GT4SFP | 1.0x, 1.1x |
| RG-NBS3100-24GT4SFP-P V2 | 1.0x, 1.1x |
| RG-NBS3100-24GT4SFP V2 | 1.0x |
| RG-NBS3100-8GT2SFP-P V2 | 1.0x |
| RG-NIS3100-8GT4SFP-HP | 1.0x |
| RG-NIS3100-8GT2SFP-HP | 1.0x |
| RG-NIS3100-4GT2SFP-HP | 1.0x |
| RG-NBS3200-24GT4XS | 1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 1.5x, 1.6x, 1.7x, 2.0x, 2.1x, 2.2x, 2.3x |
| RG-NBS3200-24GT4XS-P | 1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 1.5x, 1.6x, 2.0x, 2.1x, 2.2x, 2.3x |
| RG-NBS3200-48GT4XS | 1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 2.0x, 2.1x, 2.2x, 2.3x |
| RG-NBS3200-48GT4XS-P | 1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 1.5x, 1.6x, 2.0x, 2.1x, 2.2x, 2.3x |
| RG-NBS3200-24SFP/8GT4XS | 1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 2.0x, 2.1x, 2.2x, 2.3x |
| RG-NBS5100-48GT4SFP | 1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 2.0x, 2.1x, 2.2x, 2.3x |
| RG-NBS5100-24GT4SFP | 1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 2.0x, 2.1x, 2.2x, 2.3x |
| RG-NBS5200-48GT4XS | 1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 2.0x, 2.1x, 2.2x, 2.3x |
| RG-NBS5200-24GT4XS | 1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 2.0x, 2.1x, 2.2x, 2.3x |
| RG-NBS5200-24SFP/8GT4XS | 1.0x, 1.1x, 1.2x, 1.3x, 1.4x, 2.0x, 2.1x, 2.2x, 2.3x |
| RG-NBS5300-48MG6XS | 1.0x, 1.1x, 1.2x |
| RG-NBS5300-8MG2XS-UP | 1.0x |

1.3.2 Software Feature Change

This baseline version has no software feature change.

2 Login

2.1 Configuration Environment Requirements

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

2.2 Logging in to the Web Interface

2.2.1 Connecting to the Device

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

Table 2-1 Default Settings

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

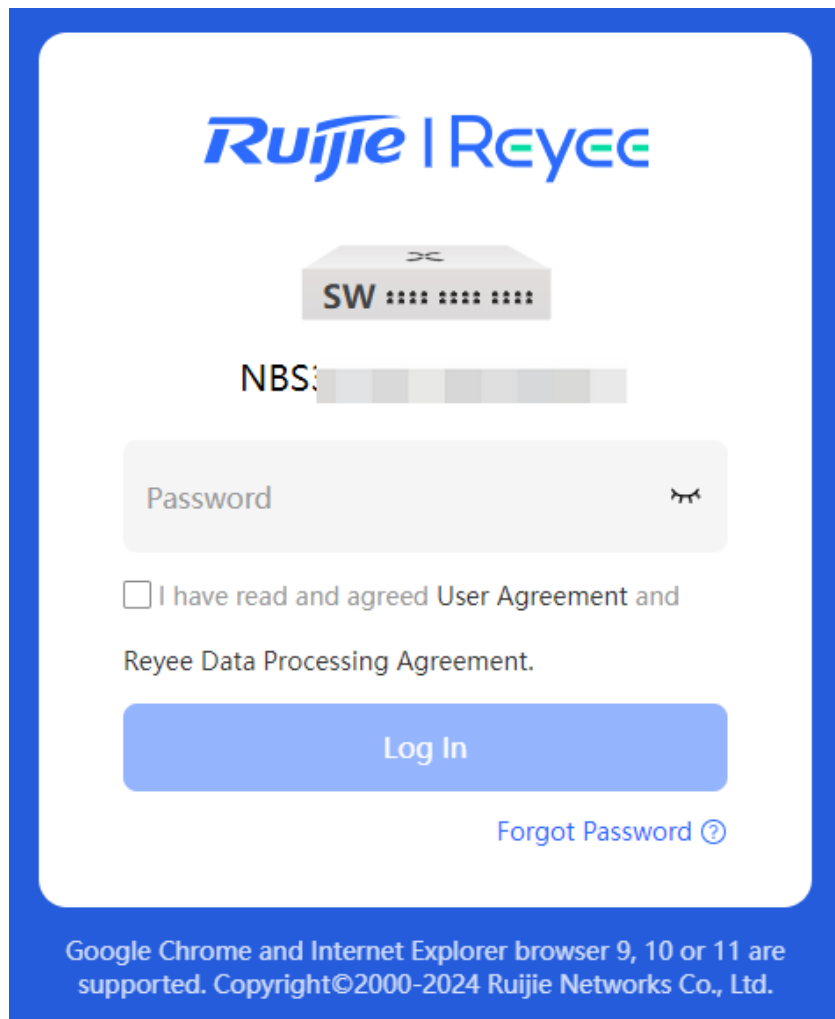
2.2.2 Logging in to the Web Interface

- (1) Enter the IP address (10.44.77.200 by default) of the device in the address bar of the browser to access the login page.

 **Note**

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

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



The login interface features the Ruijie | Reyee logo at the top. Below it is a graphic of a network switch with 'SW' and a series of dots. Underneath is a graphic of a network switch with 'NBS' and a series of dots. A password input field is labeled 'Password' and has an eye icon. Below the password field is a checkbox with the text 'I have read and agreed User Agreement and Reyee Data Processing Agreement.' A blue 'Log In' button is centered below the checkbox. To the right of the button is a link 'Forgot Password ?'. At the bottom, a footer states: 'Google Chrome and Internet Explorer browser 9, 10 or 11 are supported. Copyright©2000-2024 Ruijie Networks Co., Ltd.'

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

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

 **Caution**

- Restoring factory settings will delete all configurations of the device. Therefore, exercise caution when performing this operation.
 - The method to restore factory settings may vary with devices. For details, see the installation guide for specific instructions.
-

2.2.3 Layout Configuration

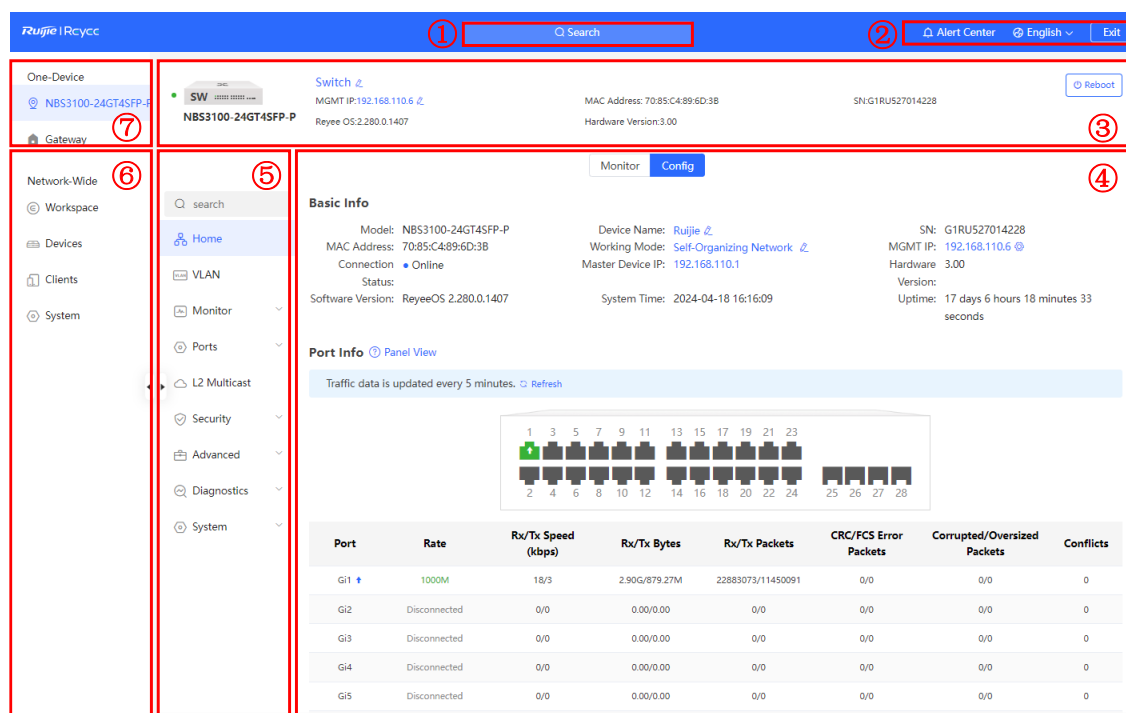


Table 2-2 Layout Configuration

| No. | Description |
|-----|--|
| 1 | Search for frequently used device functions, including network-wide management, egress gateway, and device and system related functionalities. |
| 2 | Quick view of device alarms, change the web interface language, and exit the web interface. |
| 3 | Device information and device restart button. |
| 4 | Device function configuration and display area. Click Monitor to display the interface traffic and PoE power usage of the device (only PoE switches with model names containing -P, -LP, -HP, and -UP support this function). Click Config to view the device's configuration and running status. |
| 5 | The navigation bar, which is vertically arranged on the left side when the device is a primary device on the network, and is horizontally arranged on the top when the device is a secondary device. |
| 6 | Frequently used functions of all wired and wireless Reyee products on self-organizing network, which can be configured in batch. |
| 7 | In this pane, you can configure all functions of the local device, as well as rapid setup of the egress gateway. |

2.3 Quick Setup

2.3.1 Configuration Preparations

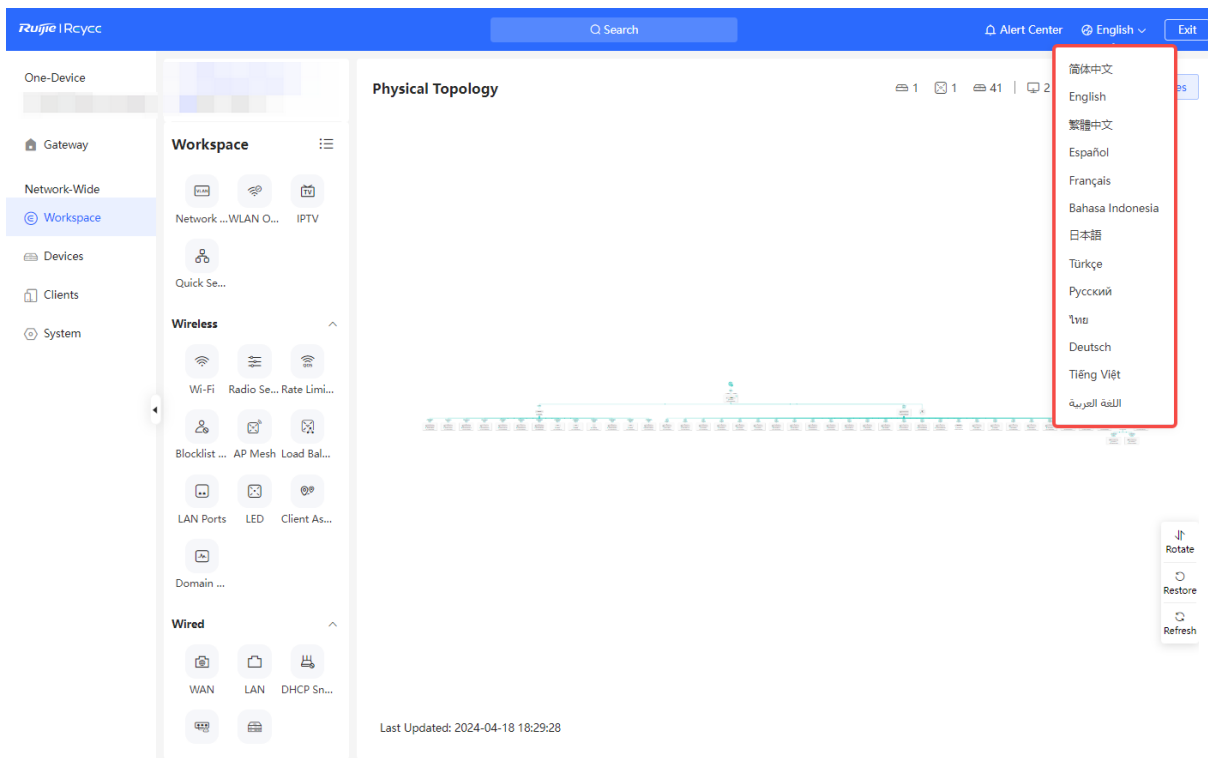
Connect the device to the power supply, and connect the device port to an uplink device with an Ethernet cable.

2.3.2 Procedure

1. Change the Web Interface Language

Click **English** in the top right corner of the web interface.

Select the desired language from the drop-down list to change the language of the web interface.



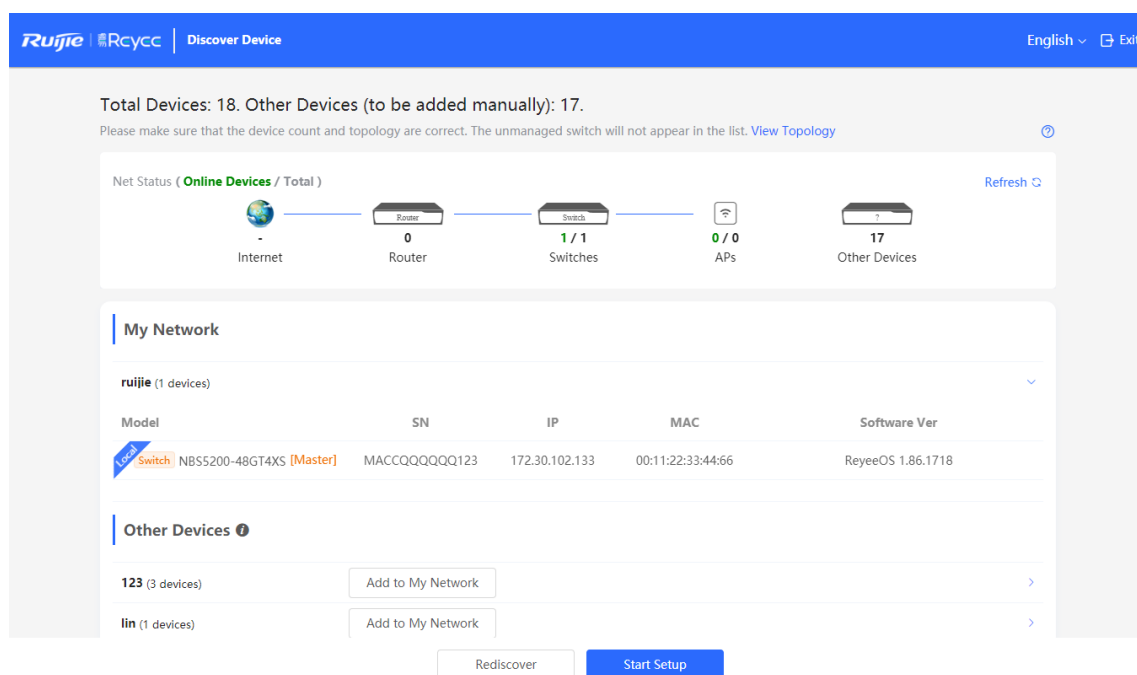
2. Adding a Device to the Network

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

Note

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

If there are other devices on the network that are not added to the current network, you can manually add them by choosing **Workspace > Quick Setup > Add to My Network** on the network-wide section and entering the management password of each device. This will incorporate the respective devices into the appropriate network, allowing you to proceed with the network-wide configuration.



3. Creating a Web Project

(1) Click **Start Setup** to configure the Internet connection type.

- **Internet:** Configure the Internet connection type according to requirements of the local Internet Service Provider (ISP).
 - PPPoE: Click **PPPoE**, and enter the username, password, and service name. Click **Next**.
 - DHCP: The device detects whether it can obtain an IP address via DHCP by default. If the device connects to the Internet successfully, you can click **Next** without entering an account.
 - Static IP: Enter the IP address, subnet mask, gateway, and DNS server, and click **Next**.
- **Wi-Fi Settings:** Select the Wi-Fi mode. This configuration option is unavailable for a new project.
 - Use old settings: Use the Wi-Fi settings of an existing project.
 - Use new settings: Configure the Wi-Fi network using new settings.
- **SSID and Wi-Fi Password:** The device has no Wi-Fi password by default, indicating that the Wi-Fi network is an open network. You are advised to configure a complex password to enhance the network security.
- **Country/Region:** The Wi-Fi channel may vary from country to country. To ensure that a client searches for a Wi-Fi network successfully, you are advised to select the actual country or region.
- **Time Zone:** Set the system time. The network time server is enabled by default to provide the time service. You are advised to select the actual time zone.

Ruijie RCycc | Network Settings

Internet ☐ PPPoE ☒ DHCP ☐ Static IP

Wi-Fi Settings ☐ Use old settings ☒ Use new settings

Dual-Band Single ☒

SSID

2.4G+5G

* SSID @Ruijie-s0477

Encryption ☒ Open ☐ Security

Security OPEN(Open)

No available frequency band? Log in to Ruijie Cloud to add or re-identify the target frequency band. [Re-identify](#) [View Causes](#)

Country/Region/Time Zone

* Country/Region China (CN)

* Time Zone (GMT+8:00)Asia/Shanghai

Previous Next

(2) Click **Next**. On the page that is displayed, set the project name and management password.

- **Project Name:** Identifies the network project where the device is located.
- **Management Password:** The password is used for logging in to the web interface.

Ruijie RCycc | Project Settings

1 Network Settings 2 Project Settings

* Project Name test

Password ☐ Use Old Management Password ☒ Edit

* Management The management passwords of the network-wide de

Password There are four requirements for setting the password:

- The password must contain 8 to 31 characters.
- The password must contain uppercase and lowercase letters, numbers and three types of special characters.
- The password cannot contain admin.
- The password cannot contain question marks, spaces, and Chinese characters.

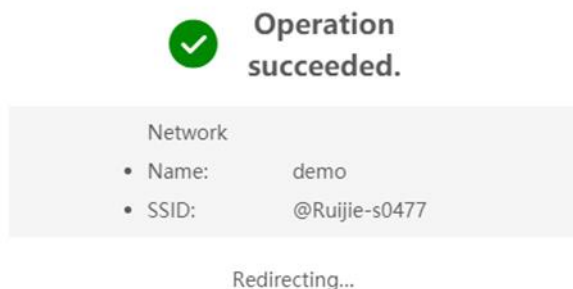
* Confirm Enter new management password again.

Confirm Password

Password Hint Enter a hint that can help you remember the manage-

Previous Finish

Click **Finish**. The system will deliver the initialization settings to the device and check the network connectivity.



The device can access the Internet now. Bind the device to a Ruijie Cloud account for remote management. Follow the instruction to log in to Ruijie Cloud for further configuration.

Note

- If your device is not connected to the Internet, click **Exit** to exit the configuration wizard.
 - Log in again with the new password if you change the management password.
-

2.3.3 Procedure for Configuring Hot Standby (VCS)

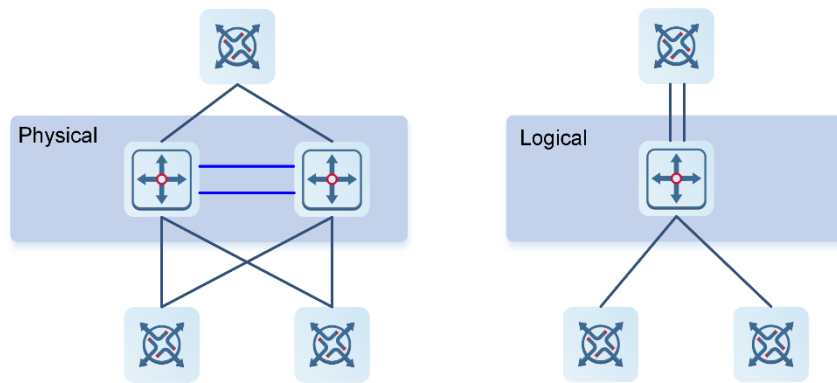
The VCS (Virtual Chassis System) is a feature that provides virtualization and clustering capabilities for switches. VCS technology allows multiple physical switches to form a logically unified device, creating a virtual switch stack. This stack is treated as a single entity with shared management and data planes.

Hot standby can improve data forwarding reliability when an NBS switch is used as the core switch. By stacking two switches and automatically switching to the standby switch when the active switch fails, hot standby ensures uninterrupted data forwarding in the event of a single point of failure.

Caution

- Hot standby is supported only on NBS7006 Series, NBS7003 Series, NBS6002 Series, NBS5300 Series, and NBS5200 Series switches.
 - Only two switches are supported to form a hot standby group.
 - When multiple switches are configured, select 10GE interfaces as hot standby interfaces to connect the member switches.
 - VCS is only supported on switches of the same series. For instance, an NBS7003 switch can only form a VCS group with another NBS7003 switch, but not with an NBS6002 switch. It should be noted that the NBS7003 and the NBS7006, which belong to different series, cannot form a VCS group.
 - Switches of different models in the same series can form a VCS group, for example, the RG-NBS5200-24GT4XS can form a VCS group with the RG-NBS5200-48GT4XS. However, if the switches in the VCS group have different switching capacities, the capacity of the VCS group is subject to the switch with the lower capacity.
 - In a VCS group, only the management port of the active switch or active supervisor module is available.
-

Stacking: refers to physically connecting multiple switches with stack cables, allowing them to operate as a single logical unit for data forwarding.

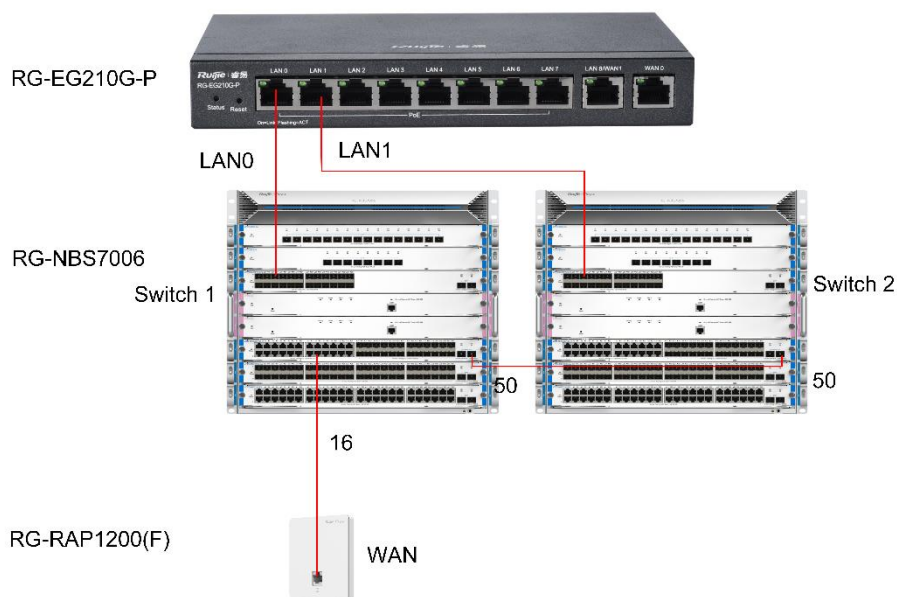


- (1) Connect two switches with cables to form a VCS group.

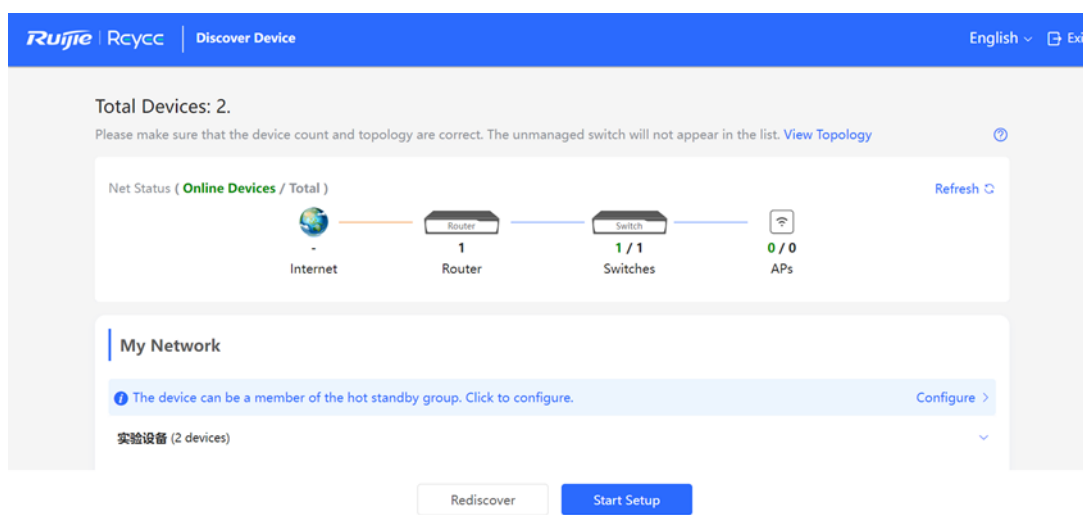
Caution

Only one link is required between devices before VCS is configured, for example, connect Port 50 of Device 1 to Port 50 of Device 2, as shown in [Figure 2-1](#). Otherwise, a loop may occur.

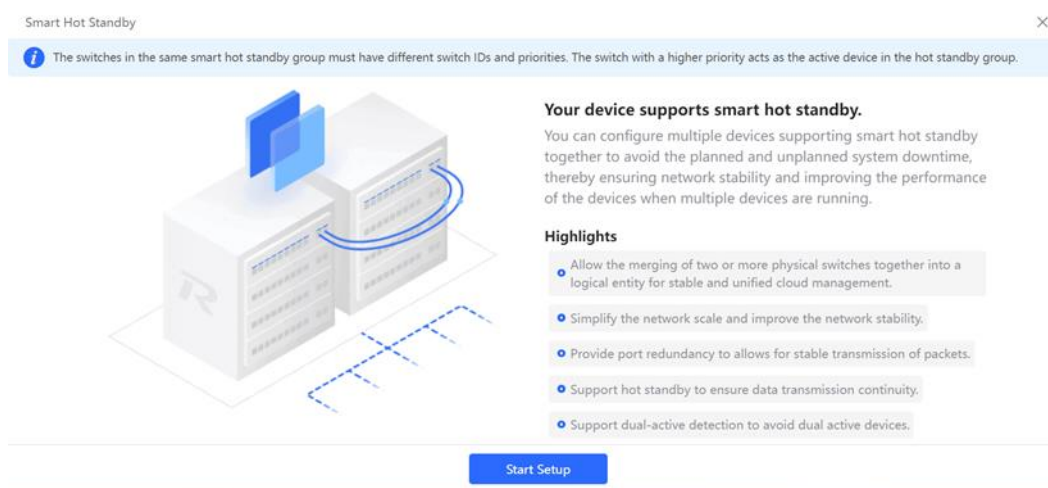
Figure 2-1 Connecting Switches Before Configuring VCS



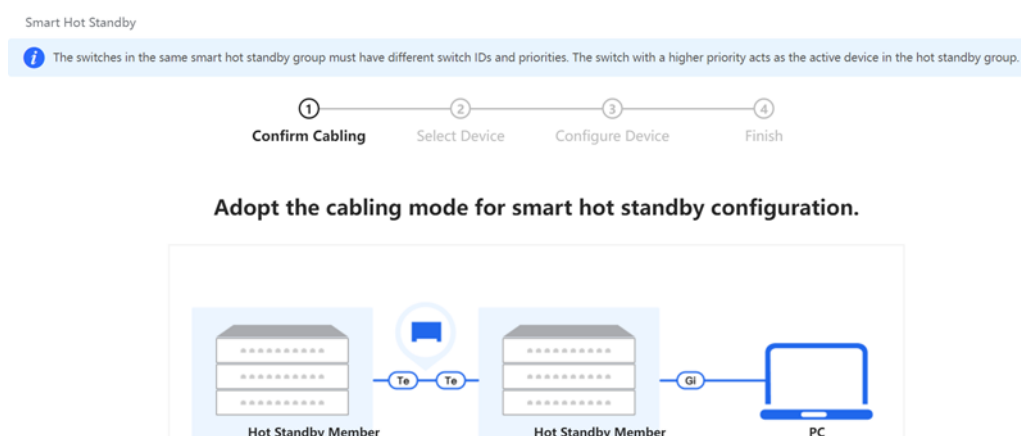
- (2) Enter the default IP address 10.44.77.200 in the address bar of your browser to access the web interface of an NBS switch. Click **Configure**.



(3) Click **Start Setup**.



(4) Connect the 10GE interfaces of the two switches using a cable (for example, connect Interface 50 of Device 1 to Interface 50 of Device 2, as shown in [Figure 2-1](#)). Then, choose **Dual-Device Config**, and click **Next**.



Dual-Device Cabling Diagram

☒ Dual-Device Config **Recommended**
☐ Single-Device Config

You are advised to only keep the members of the hot standby group on the network to prevent device loops.
When multiple switches are configured, select 10GE ports as hot standby interfaces to connect the member switches.

Previous
Next

(5) Select the standby switch.

(6) Select another VCS interface (Interface 49 in the following figure), or multiple VCS interfaces. You are advised to select two adjacent interfaces on a switch. Up to four VCS interfaces on a switch can be selected. These VCS interfaces must be 10GE interfaces. By default, the active switch has a priority of 200, while the standby switch has a priority of 100. If the priority is changed, a switch with a higher priority will become the active device.

Smart Hot Standby
Confirm Cabling Select Device Configure Device Finish

Select a hot standby interface.

You are advised to select two adjacent 10GE ports. You can configure the device priority to change the active/standby relationship. The one with a higher priority is elected as the active device.

Device1/ NBS7003/ MACC567890328

Device Priority:
Standby 50 100 150 200 Active

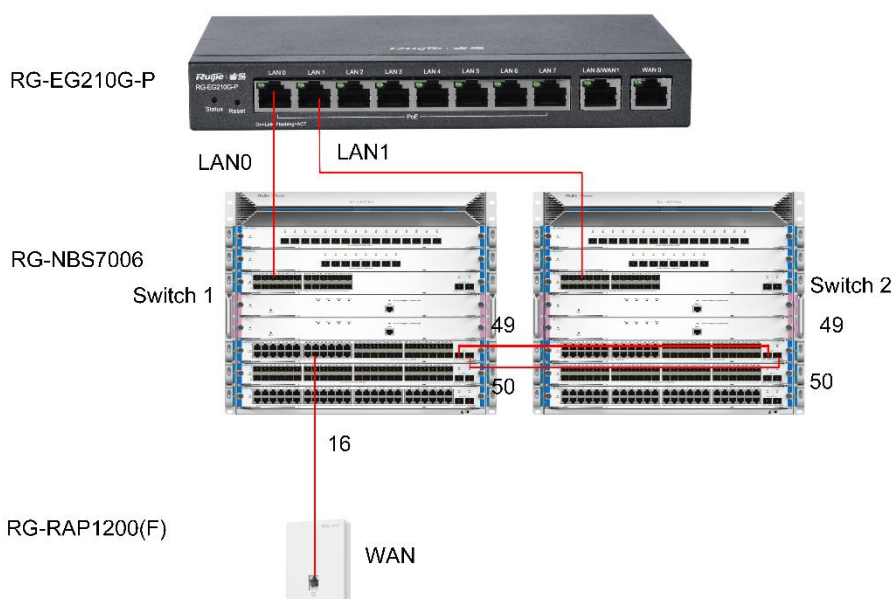
Available
 Unavailable
 Connected

M7000-24GT24SFP2XS-EA/1234942570069 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 | |
| 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 |

Previous
Save

(7) Click **Next**. Use a 10GE cable to connect the VCS interfaces that you have selected. (The following figure shows an example of connecting Interface 49 of Device 1 to Interface 49 of Device 2.)



(8) After the cables are connected, proceed as prompted, and wait for the device to reboot successfully.

⚠ Caution

To delete the hot standby configuration, ensure that the network cable connecting the hot standby interfaces is disconnected. Failure to do so may result in a loop that can cause network disconnection.

2.4 Work Mode

The device supports two work modes: **Standalone** and **Self-Organizing Network**. It works in **Self-Organizing Network** mode by default. The system presents different menu items based on the work mode. To modify the work mode, see [2.5 Switching the Management Mode](#).

Self-Organizing Network: After the self-organizing network discovery function is enabled, the device can be discovered on the network and discover other devices on the network. Devices network with each other based on the device status and synchronize global configuration. You can log in to the Web management page of the device to check management information about all devices on the network. After self-organizing network discovery is enabled, users can maintain and manage the current network more efficiently. You are advised to keep this function enabled.

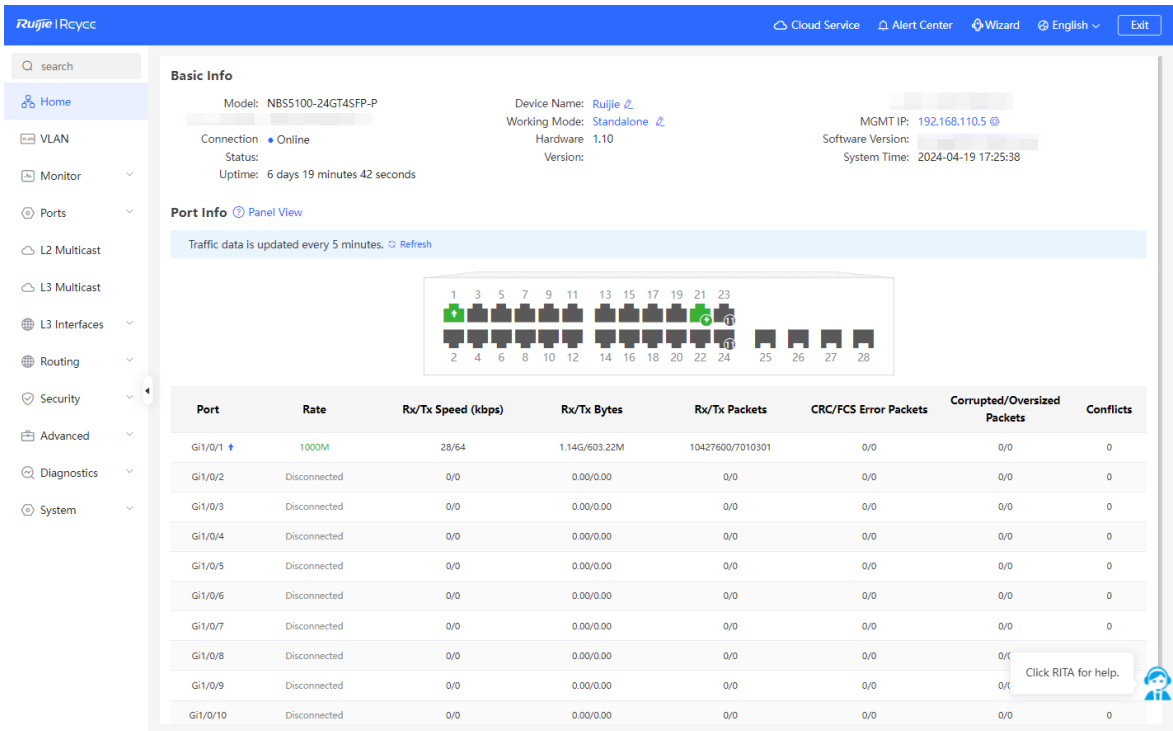
When the device is in self-organizing network mode, the web interface has two configuration modes: the networkwide management mode and the local device mode. For more information, see [2.5 Switching the Management Mode](#).

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

2.5 Switching the Management Mode

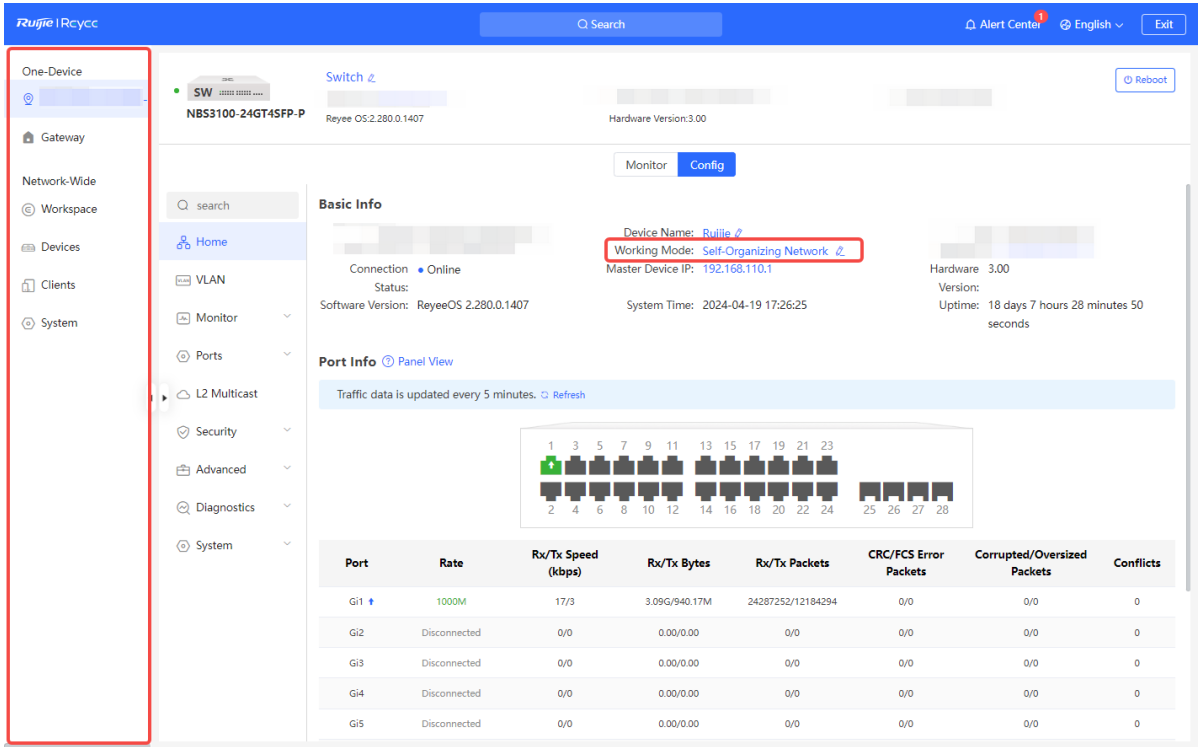
In standalone mode, you can configure and manage only the current logged in device without self-organizing network function, as shown in [Figure 2-2](#).

Figure 2-2 Web Interface in Standalone Mode



In SON mode, you can batch set the commonly used functions of all wired and wireless Reyee products on the self-organizing network, including the currently logged-in device, as shown in [Figure 2-3](#).

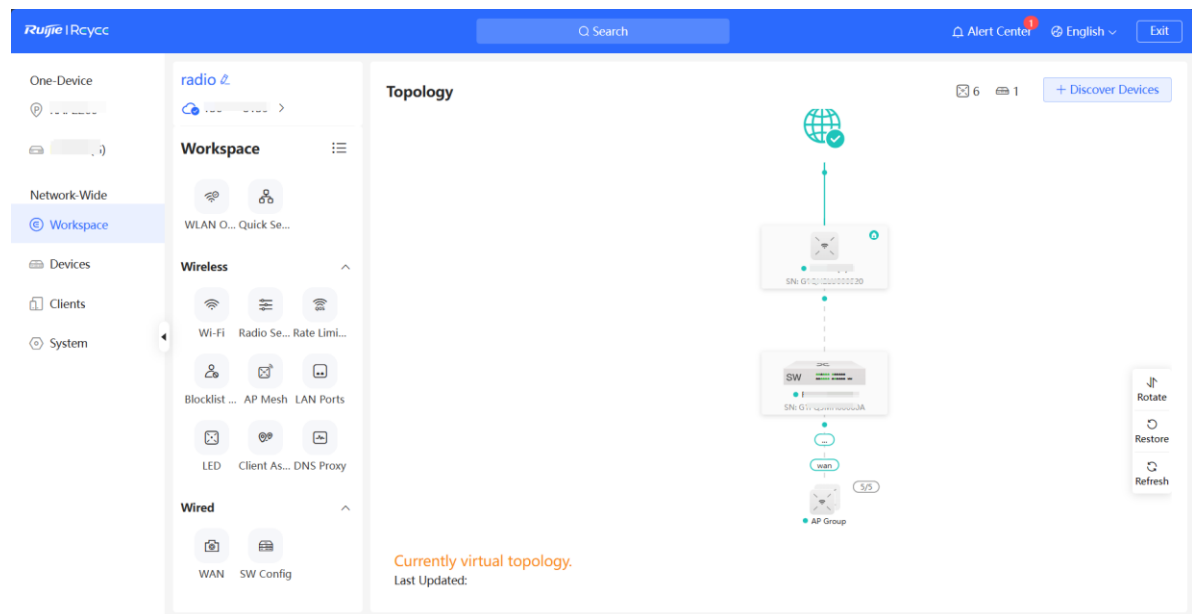
Figure 2-3 Web Interface in Self-Organizing Mode



3 Network-Wide Management

Choose **Network-Wide > Workspace > Topology**.

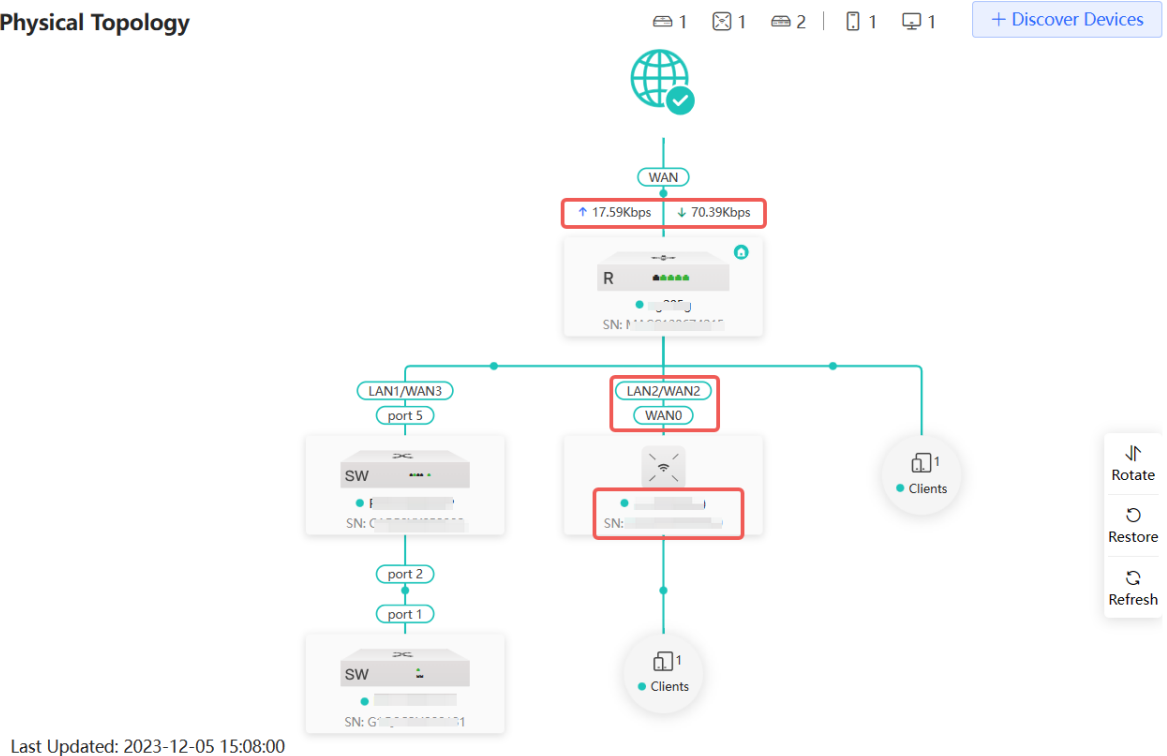
The **Topology** page displays the current network topology, real-time uplink and downlink traffic, connection status, and number of clients on the current network. It also provides quick actions for network and device setup. On the current page, you can monitor, configure, and manage the entire network.



3.1 Viewing Networking Information

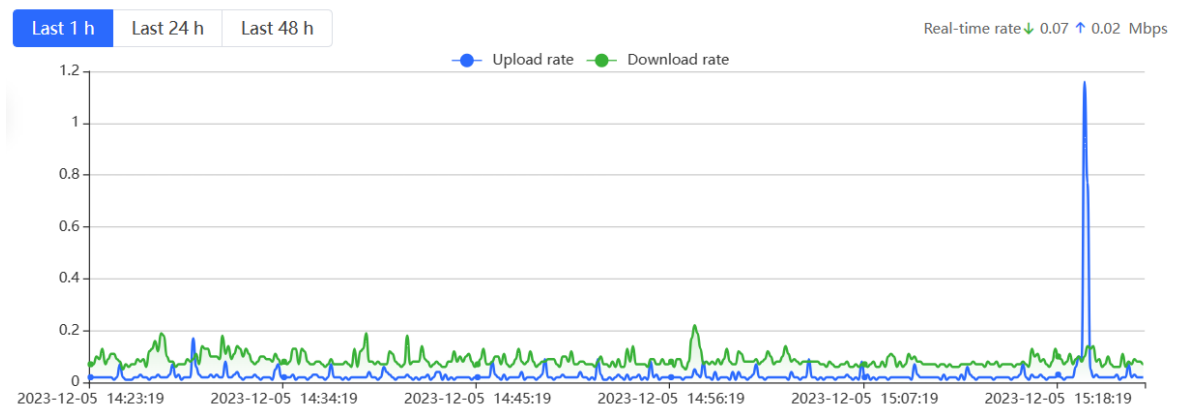
In SON mode, the topology displays information about online devices, connected ports, device SNs, and uplink and downlink real-time traffic.


Physical Topology

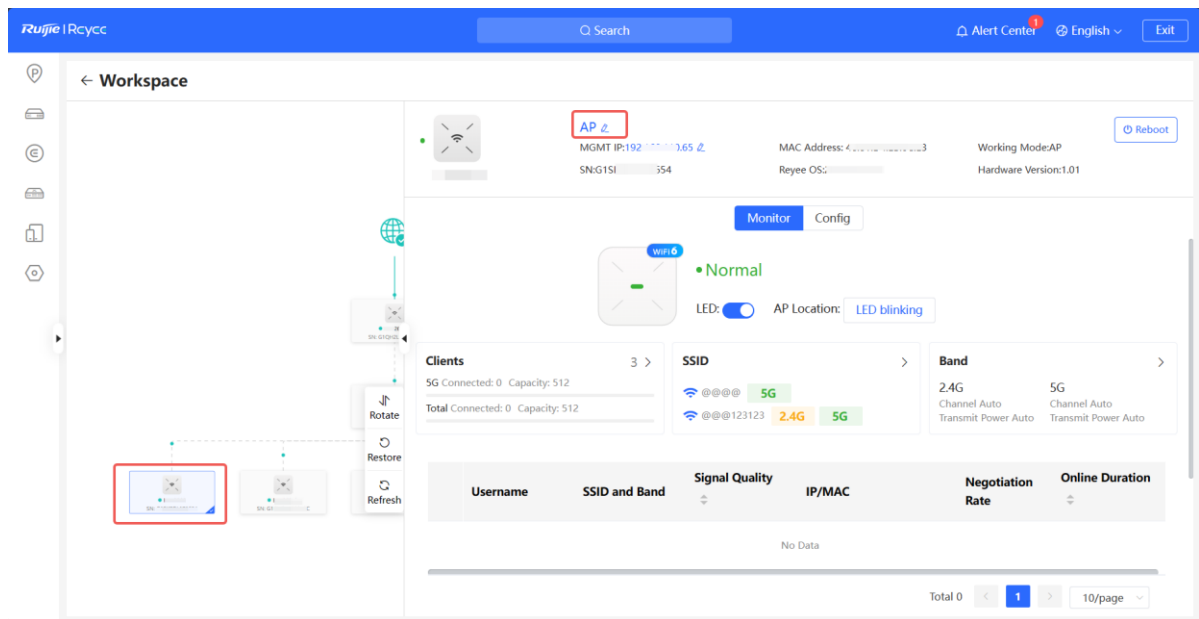


- Click the egress gateway to view real-time traffic information of the device.

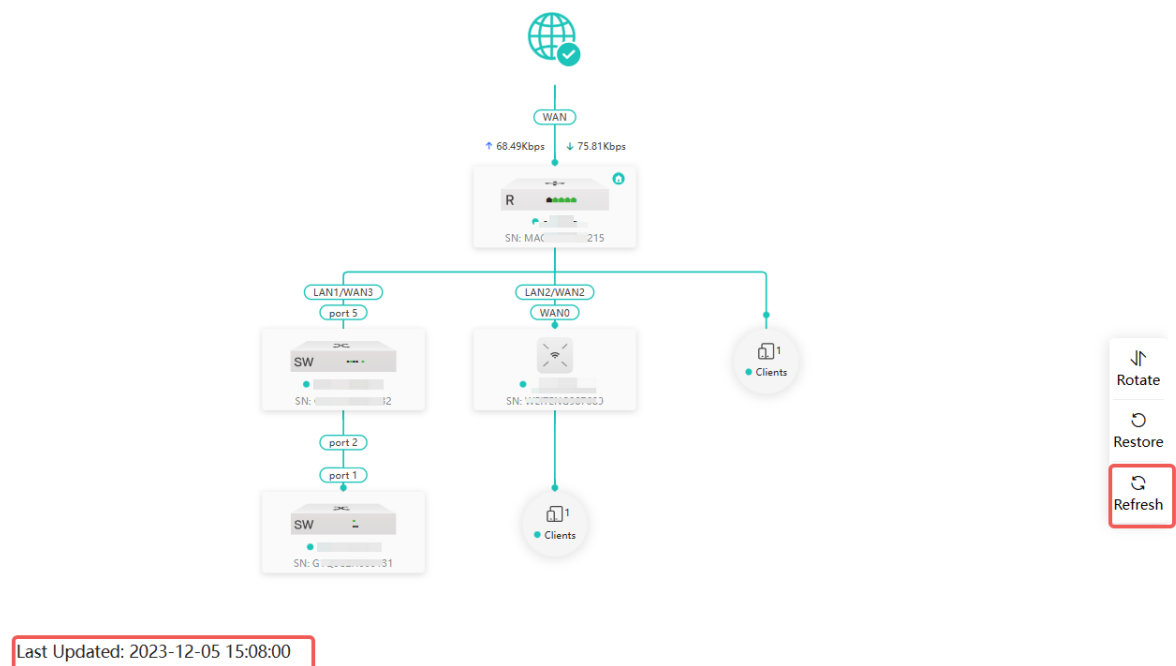
Traffic Trend



- Click a device in the topology to view the running status and configuration of the device, and to configure functions on the device. The device name is the product model by default. You can click  to change the device name.



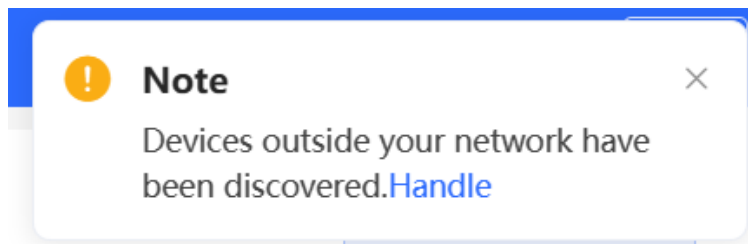
- The update time is displayed in the lower left corner of the topology page. Click **Refresh** to refresh the topology. It takes some time to refresh the topology.



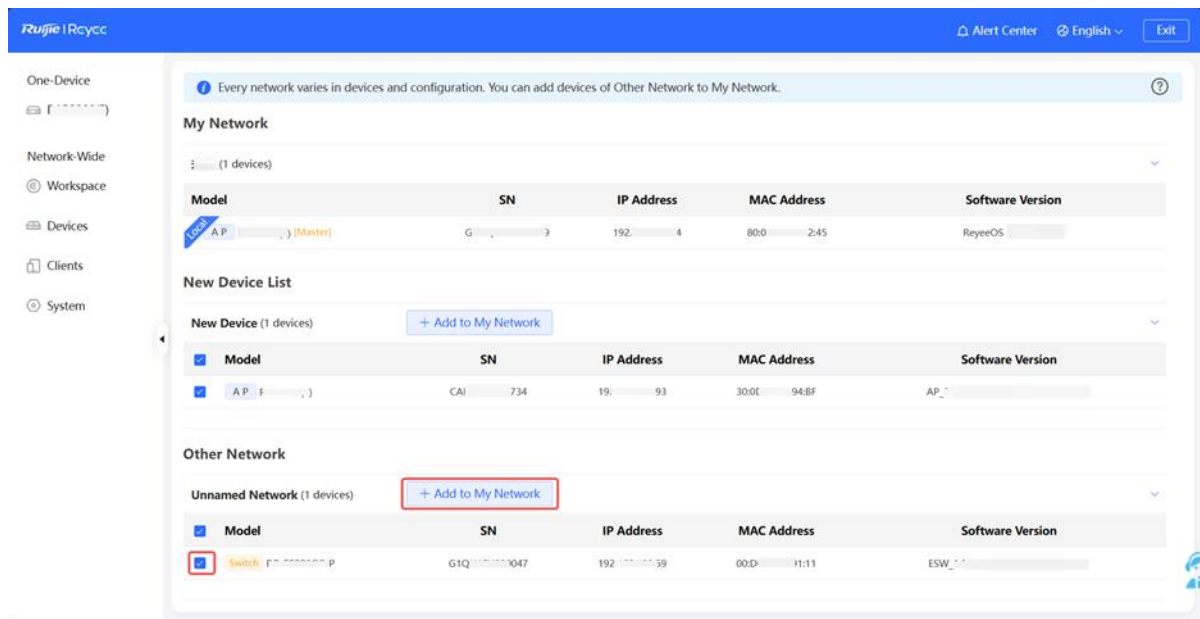
3.2 Adding Devices

3.2.1 Adding a Device Through Wired Connection

- (1) When a new device joins the network through a wired connection, the system displays a prompt that a device not in SON is detected. Click **Handle** to add the device to the current network.



- (2) On the **Network List** page, click the downward arrow next to **Other Network** to expand this list. Select the desired device(s) and click **Add to My Network**.



You do not need to enter the password if the device to be added has not been configured before. If a password is required, enter the management password of the device. The device cannot be added if the entered management password is incorrect.

Add Device to My Network

* Password

[Forgot Password](#) [Add](#)

3.2.2 AP Mesh

Note

This function is only supported on Reyee APs that support AP Mesh function.

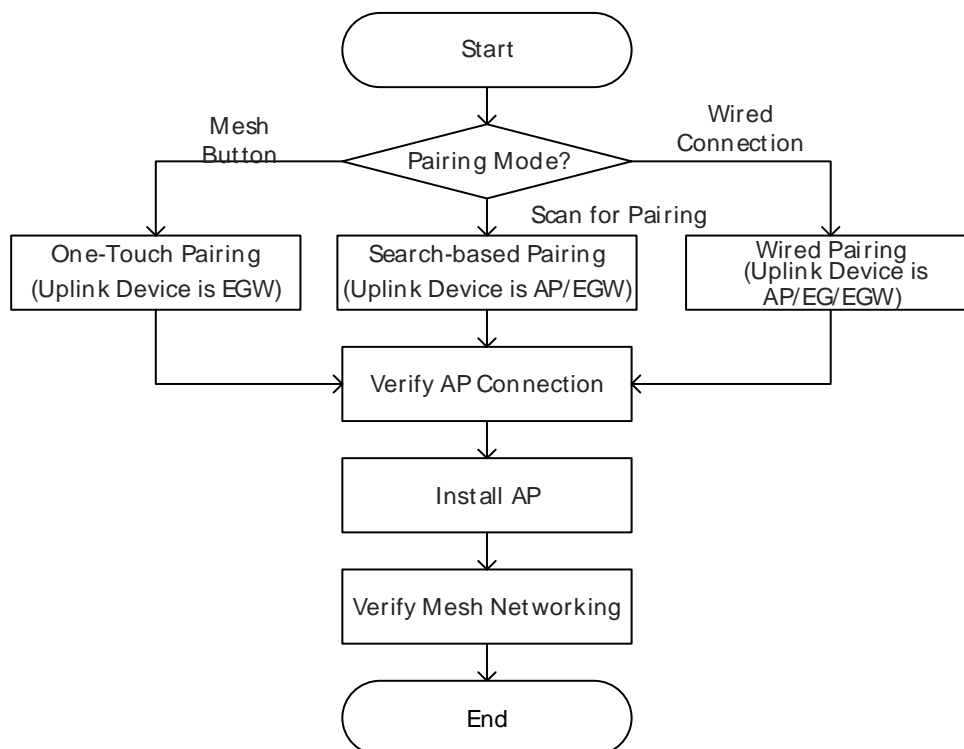
1. Overview

After being powered on and enabled with the AP Mesh feature, a Mesh-capable new AP can be paired with other Mesh-capable wireless devices on the target network through multiple ways. Then the AP will synchronize its Wi-Fi configuration with other devices automatically. Mesh networking addresses pain points such as complex wireless networking and cabling. A new AP can be connected to any uplink wireless device among AP, EG router, and EGW router in the following ways:

- One-touch pairing: Short press the Mesh button on the EGW router on the target network to implement fast pairing of the AP with the EGW router.
- Search-based pairing: Log in to the web interface of a device on the target network. Search and add APs to be paired.
- Wired pairing: Connect the new AP to a wireless device on the target network using an Ethernet cable. The new AP will go online on the target network.

Once the pairing process is complete, the new AP acquires wireless backhaul information from neighboring APs within the network. After the new AP is installed, it will automatically connect to the most suitable neighboring AP.

2. Configuration Steps




3. One-Touch Pairing

Caution

- The uplink device must be an EGW router.
- The new AP must be in factory-reset configuration.
- It can be scanned only when the network is enabled with AP Mesh.
- Place the new AP no more than 2 meters away from the uplink device to ensure that the new AP can receive the Wi-Fi signal from the uplink device. The new AP may fail to be scanned due to the long distance or obstacles between it and the uplink device.

(1) Power on the new AP and place it near the EGW router on the target network.


(2) Press and hold the Mesh button  on the EGW router for no more than two seconds to start pairing. The pairing process takes about one minute.

(3) Check the topology on the **Physical Topology** page to make sure that the new AP has connected to the uplink device in wireless mode.



(4) Power off the new AP and install it to a planned location.

(5) Log in to the web interface of a device on the target network. In SON mode, choose **Devices > AP**. Make

sure that the new AP is online and the icon  appears in the **Relay Information** column. The icon indicates that wireless backhaul is performed through the 5 GHz radio.

All (54) Gateway (1) **AP (50)** Switch (2) AC (1) Router (0)

Select Reboot Batch Upgrade Delete Offline IP/MAC/hostname/SN/S:

Devices outside your network have been discovered. [Handle](#)

Group: **All Groups** [Expand](#) [Change Group](#) **Basic Info** ☐ RF Information ☐ Model

| | Username | Model | Clients | Device Group | Relay Information | Software Version | Action |
|--|----------|-------|---------|--------------|------------------------------|------------------|---|
| | AP | | 0 | Default | View Details | ReyeeOS | Manage Reboot |
| | AP | | 0 | Default | View Details | ReyeeOS | Manage Reboot |
| | AP | | 7 | Default | View Details | ReyeeOS | Manage Reboot |
| | AP | | 0 | Default | View Details | ReyeeOS | Manage Reboot |
| | AP | | 0 | Default | View Details | ReyeeOS | Manage Reboot |

(6) Click **View Details** next to the



icon to obtain information about the uplink device and RSSI.

| | | | | | | |
|--|----|--|---|---------|------------------------------|--|
| | AP | | 0 | Default | View Details | <div> <p>Noise Floor: -82 dBm Channel Utilization: 16 % RSSI: -26 dBm Good Negotiation Rate: 173 Mbps Uptime: 13 minutes 18 seconds</p> <p>Uplink Local</p> <p>AP </p> <p>Model: Model: SN: ZASI 923 SN: G1NC 79 IP: 192 155 IP: 192 0.31</p> </div> |
| | AP | | 0 | Default | View Details | |
| | AP | | 0 | Default | View Details | |
| | AP | | 0 | Default | View Details | |
| | AP | | 0 | Default | View Details | |
| | AP | | 0 | Default | View Details | |

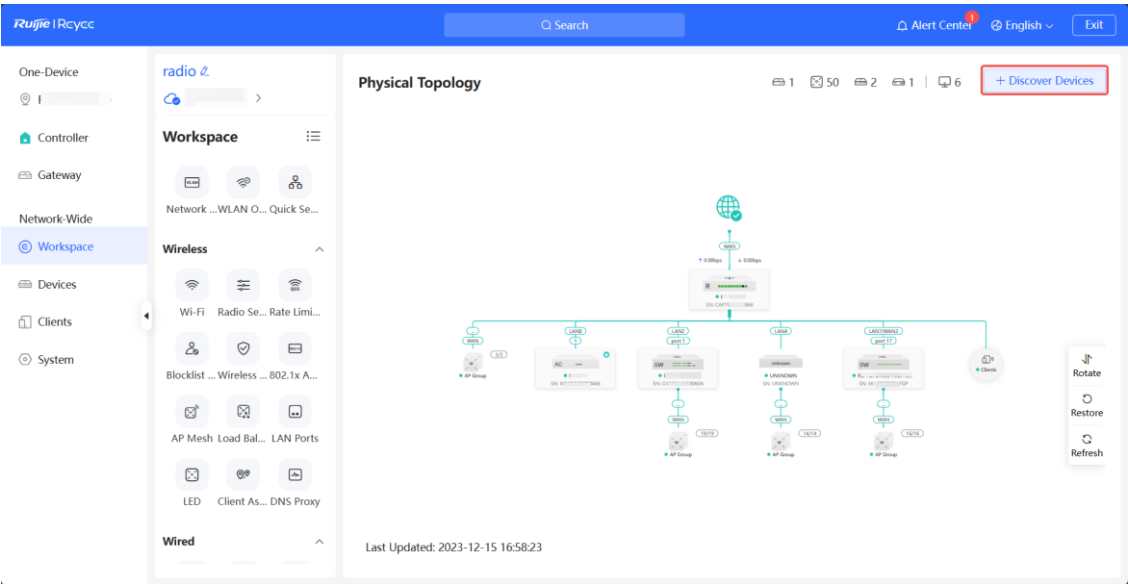
4. Search-based Pairing

Caution

- The uplink device must be an EGW router.
- The new AP must be in factory-reset configuration.
- It can be scanned only when the network is enabled with AP Mesh.
- Place the new AP no more than 2 meters away from the uplink device to ensure that the new AP can receive the Wi-Fi signal from the uplink device. The new AP may fail to be scanned due to the long distance or obstacles between it and the uplink device.

(1) Power on the new AP and place it near the AP or EGW router on the target network.

(2) Log in to the web interface of a device on the target network. In SON mode, click **+Discover Devices** in the upper right corner of the **Physical Topology** page to scan the APs in other networks not connected with Ethernet cables.



- (3) On the **AP Mesh** page, click **Scan** to scan devices that are not connected to the network via an Ethernet cable.

Device Networking [AP Mesh](#)

i Every network varies in devices and configuration. You can add devices of Other Network to My Network.

My Network

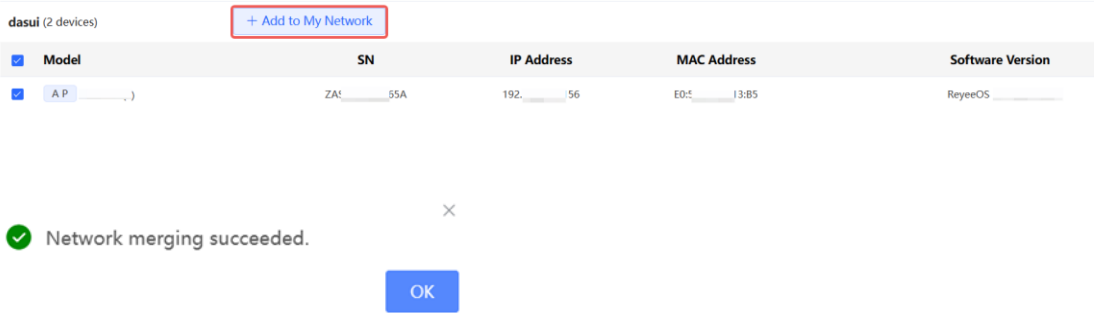
radio (53 devices)

Other Device

No data

Scan


- (4) Select the APs to be added and click **Add to My Network**. Up to eight APs can be added at a time. Wait until the mesh process finishes.



- (5) Check the topology on the **Physical Topology** page to make sure that the new AP has connected to the uplink device in wireless mode.



- (6) Power off the new AP and install it to the planned location.
- (7) Log in to the web interface of a device on the target network. In SON mode, choose **Devices > AP**. Make

sure that the new AP is online and the icon  appears in the **Relay Information** column. The icon indicates that wireless backhaul is performed through the 5 GHz radio.


[All \(54\)](#)
[Gateway \(1\)](#)
[AP \(50\)](#)
[Switch \(2\)](#)
[AC \(1\)](#)
[Router \(0\)](#)

[Select](#)
[Reboot](#)
[Batch Upgrade](#)
[Delete Offline](#)
[IP/MAC/hostname/SN/S...](#)

Devices outside your network have been discovered. [Handle](#)

Group: [All Groups](#)
[Expand](#)
[Change Group](#)
[Basic Info](#)
[RF Information](#)
[Model](#)

| | Username | Model | Clients | Device Group | Relay Information | Software Version | Action |
|--|----------|-------|---------|--------------|---------------------------------------|------------------|---|
| | AP 2 | | 0 | Default | Wired View Details | ReyeeOS | Manage Reboot |
| | AP 2 | | 0 | Default | Wired View Details | ReyeeOS | Manage Reboot |
| | AP 2 | | 0 | Default | Wired View Details | ReyeeOS | Manage Reboot |
| | AP 2 | | 0 | Default | Wired View Details | ReyeeOS | Manage Reboot |
| | AP 2 | | 0 | Default | View Details | ReyeeOS | Manage Reboot |

- (8) Click **View Details** next to the  icon to obtain information about the uplink device and RSSI.

The screenshot shows a table of APs with columns for status, name, model, SN, IP, and actions. A red box highlights a detailed view of an AP's status, showing:

- Noise Floor: -82 dBm
- Channel Utilization: 16 %
- RSSI: -26 dBm **Good**
- Negotiation Rate: 173 Mbps
- Uptime: 13 minutes 18 seconds

Below the status box, there are icons for 'Uplink' and 'Local' connections, and a diagram showing the AP's connection to a 5G network. At the bottom, there are fields for Model, SN, and IP for both the AP and the uplink device.

5. Wired Pairing


⚠ Caution

- The uplink device can be an AP, EG router, or EGW router.
- The new AP must be in factory-reset configuration.
- It can be scanned only when the live network is enabled with AP Mesh.

- (1) Plug one end of the Ethernet cable to the uplink port of the new AP, and the other end to the downlink port of an AP, EG router, or EGW router on the target network. The Mesh process takes one to three minutes. When the system status LED is steady on, it indicates that the Mesh process finishes.
- (2) Log in to the web interface of a device on the target network. In SON mode, choose **Devices** and make sure that the new AP is online.

The screenshot shows a network management interface with a top navigation bar containing tabs for All (54), Gateway (1), AP (50), Switch (2), AC (1), and Router (0). Below the tabs, there are buttons for Select, Reboot, Batch Upgrade, Delete Offline, and a search field. A yellow banner indicates that devices outside the network have been discovered. Below the banner, there are tabs for Group, All Groups, Expand, Change Group, Basic Info, RF Information, and Model. A table lists the devices with columns for Username, Model, SN, IP Address, MAC Address, Clients, Device Group, and Action. The table shows three devices, with the first one highlighted by a red box. The first device is an AP with SN G1N14233, IP 192.15.15, and MAC 10:81:E8. The second device is an AP with SN ZAS0170, No IP Address Available, and MAC E0:12:F1. The third device is an AP with SN G1N00379, IP 192.31.31, and MAC 80:12:45.

- (3) Unplug the Ethernet cable, power off the new AP, and install it to a planned location.
- (4) Log in to the web interface of a device on the target network. In SON mode, choose **Devices > AP**. Make

sure that the new AP is online and the icon  appears in the **Relay Information** column. The icon indicates that wireless backhaul is performed through the 5 GHz radio.

All (54) Gateway (1) **AP (50)** Switch (2) AC (1) Router (0)

Select Reboot Batch Upgrade Delete Offline IP/MAC/hostname/SN/Sr

Devices outside your network have been discovered. [Handle](#)

Group: **All Groups** [Expand](#) [Change Group](#) **Basic Info** ☐ RF Information ☐ Model

| | Username | Model | Clients | Device Group | Relay Information | Software Version | Action |
|--|----------------------|-------|---------|--------------|---------------------------------------|------------------|---|
| | AP 🔗 | | 0 | Default | Wired View Details | ReyeeOS | Manage Reboot |
| | AP 🔗 | | 0 | Default | Wired View Details | ReyeeOS | Manage Reboot |
| | AP 🔗 | | 0 | Default | Wired View Details | ReyeeOS | Manage Reboot |
| | AP 🔗 | | 0 | Default | Wired View Details | ReyeeOS | Manage Reboot |
| | AP 🔗 | | 0 | Default | 5G View Details | ReyeeOS | Manage Reboot |

(5) Click **View Details** next to the icon to obtain information about the uplink device and RSSI.

| | | | | | |
|--|----------------------|--|---|---------|---------------------------------------|
| | AP 🔗 | | 0 | Default | Wired View Details |
| | AP 🔗 | | 0 | Default | Wired View Details |
| | AP 🔗 | | 0 | Default | Wired View Details |
| | AP 🔗 | | 0 | Default | 5G View Details |
| | AP 🔗 | | 0 | Default | Wired View Details |
| | AP 🔗 | | 0 | Default | Wired View Details |

Noise Floor: -82 dBm
Channel Utilization: 16 %
RSSI: -26 dBm **Good**
Negotiation Rate: 173 Mbps
Uptime: 13 minutes 18 seconds

Uplink **Local**

AP AP

Model: Model:
SN: ZASL 923 SN: G1NC 79
IP: 192 155 IP: 192 131

6. Enabling WAN Port

The WAN port works as the wired uplink port of the AP by default. For the AP added to the target network through Mesh pairing, the WAN port is disabled by default. If you want to connect the Mesh AP to other downlink device in wired mode to expand the network, enable this port.

- Log in to the web interface of the network project. Choose **Network-Wide > Devices > AP**, and click **Manage** next to a device in the AP list.

All (54) Gateway (1) **AP (50)** Switch (2) AC (1) Router (0)

Select Reboot Batch Upgrade Delete Offline IP/MAC/hostname/SN/Sr

Devices outside your network have been discovered. [Handle](#)

Group: **All Groups** [Expand](#) [Change Group](#) **Basic Info** ☐ RF Information ☐ Model

| | Username | Model | SN | IP Address | MAC Address | Clients | Device Group | Action |
|--|----------------------|-------|--------------|---------------------------------|-------------|---------|--------------|---|
| | AP 🔗 | | G1SK3 04233 | 192. 0.45 🔗 | 10:82 :E8 | 0 | Default | Manage Reboot |
| | AP | | ZASLA 170 | No IP Address Available | E0:5D 2:F1 | 0 | - | Manage Reboot |
| | AP 🔗 | | G1NQCA 79 | 192.11 10.31 🔗 | 80: 2:45 | 0 | Default | Manage Reboot |

- (2) Choose **Config > Advanced > Enable WAN**, toggle on **Enable**, and click **Save**.

i The WAN port is used as an uplink port of the AP by default. When the device works in the wireless repeater mode, the WAN port is disabled by default. If you want to extend network coverage through connecting the WAN port of the AP to a switch, enable the WAN port first.

Enable ☒

Save


7. Viewing Mesh APs and Mesh Details

- (1) Log in to the web interface of a device on the target network.

- (2) View Mesh APs.

- Method 1: In SON mode, check the topology on the **Physical Topology** page. The AP that connects to the uplink device in wireless mode is a Mesh AP.



- Method 2: In SON mode, choose **Devices > AP**. If the icon  appears in the **Relay Information** column, the corresponding AP is a Mesh AP.

All (54)

Gateway (1)

AP (50)

Switch (2)

AC (1)

Router (0)

Select

Reboot

Batch Upgrade ?

Delete Offline

IP/MAC/hostname/SN/S...

Devices outside your network have been discovered. [Handle](#)

Group: All Groups

Expand ?

Change Group ?

Basic Info

RF Information

Model

| | Username ? | Model | Clients | Device Group | Relay Information | Software Version ? | Action |
|--|---------------------------------|-------------|---------|--------------|--|-----------------------|---|
| | AP View Details | <div></div> | 0 | Default | <div>Wired</div> <div>View Details</div> | ReyeeOS <div></div> | Manage Reboot |
| | AP View Details | <div></div> | 0 | Default | <div>Wired</div> <div>View Details</div> | ReyeeOS ; <div></div> | Manage Reboot |
| | AP View Details | <div></div> | 0 | Default | <div>Wired</div> <div>View Details</div> | ReyeeOS ; <div></div> | Manage Reboot |
| | AP View Details | <div></div> | 0 | Default | <div>Wired</div> <div>View Details</div> | ReyeeOS ; <div></div> | Manage Reboot |
| | AP View Details | <div></div> | 0 | Default | <div>5G View Details</div> | ReyeeOS <div></div> | Manage Reboot |

(3) View Mesh details.

In SON mode, choose **Devices > AP**. Select the target AP, and click **View Details** in the **Relay Information** column to view the Mesh details.

| AP Icon | AP Name | Relay Information | Action |
|-----------|---------|-------------------|--------------|
| [AP Icon] | AP 1 | Wired | View Details |
| [AP Icon] | AP 2 | Wired | View Details |
| [AP Icon] | AP 3 | Wired | View Details |
| [AP Icon] | AP 4 | 5G | View Details |
| [AP Icon] | AP 5 | Wired | View Details |
| [AP Icon] | AP 6 | Wired | View Details |

Noise Floor: -82 dBm
 Channel Utilization: 16 %
 RSSI: -26 dBm Good
 Negotiation Rate: 173 Mbps
 Uptime: 13 minutes 18 seconds

Uplink 5G Local

AP AP

Model: I SN: ZASI923 IP: 192.155
 Model: SN: G1NC79 IP: 192.131

3.3 Configuring VLANs

Choose **Network-Wide > Workspace > Network Planning**.

Ruijie RCloud | Search | Alert Center | English | Exit

One-Device | Workspace | Network-Wide | **Workspace** | Devices | Clients | System

radio 1

Workspace

Network | WLAN | Quick Se...

Wireless

Wi-Fi | Radio Se... | Rate Limi...

Blocklist ... | AP Mesh | LAN Ports

LED | Client As... | DNS Proxy

Wired

WAN | DHCP Sn... | RLDP

Physical Topology

6 | 1 | + Discover Devices

Rotate | Restore | Refresh

Last Updated: 2023-12-06 04:00:12

3.3.1 Configuring a Wired VLAN

Choose **Network-Wide > Workspace > Network Planning**.

On the **Network Planning** page, click **Add Wired VLAN**.

Network Planning(1) All ▾

Add Wired VLAN Add Wi-Fi VLAN

VLAN1 Wi-Fi VLAN
VLAN1

SVI Address: (Gateway)
192.168.110.1

DHCP Pool (Enable)
192.168.110.1/255.255.255.0
IP Count: 254
Lease Time (Min): 30

Rotate
Restore
Refresh

Alternatively, you can select an existing wired VLAN and click **Setup** to edit the VLAN.

Network Planning(2) All ▾

Add Wired VLAN Add Wi-Fi VLAN

VLAN1 Wi-Fi VLAN
VLAN1

VLAN10 test

SVI Address: (Gateway)
192.168.10.1

DHCP Pool (Enable)
192.168.10.1/255.255.255.0
IP Count: 254
Lease Time (Min): 480

Setup

Rotate
Restore
Refresh

- (1) Configure the VLAN ID, address pool server, and DHCP pool. The gateway is configured as the address pool server by default to assign IP addresses to clients. If an access switch exists on the network, you can select the access switch as the address pool server. Click **Next** after VLAN parameters are configured.

Configure Network Planning/Add Wired VLAN

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

Description:

* VLAN ID:

Address Pool ☒ Gateway

Server

Gateway/Mask: /

DHCP Pool: ☒

IP Range: -

[Next](#)

(2) Select the target switch in the topology and all member ports in the VLAN, and click **Next**.

Configure Network Planning/Add Wired VLAN

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

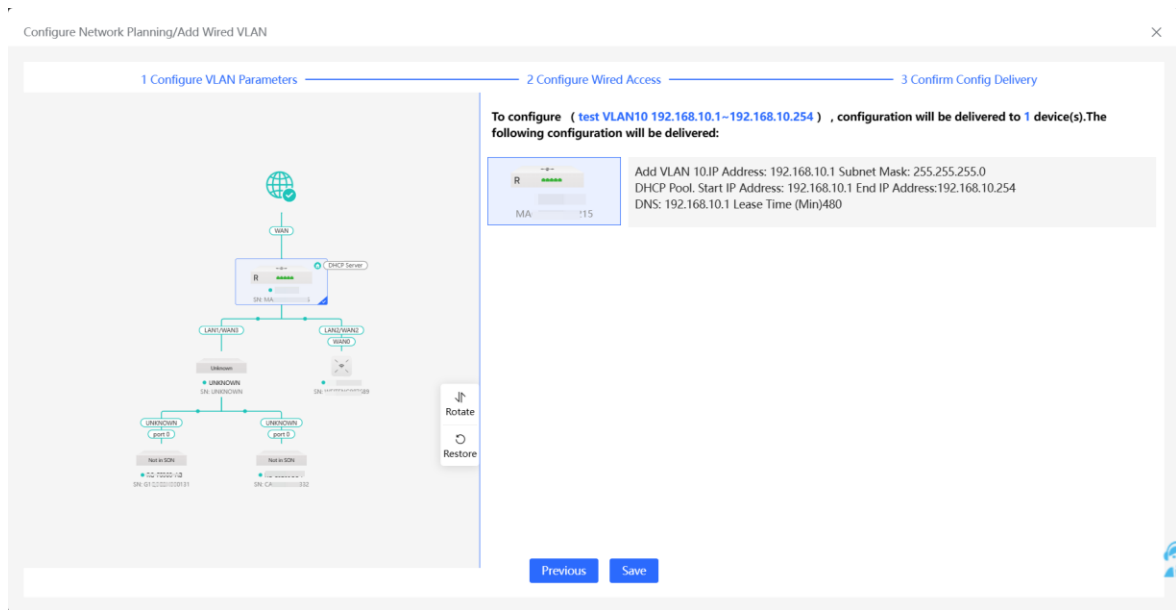
VLAN20 (1) 192.168.20.1~192.168.20.254 You have selected 0 device(s) with 0 port(s). [Panel View](#)

No Device and Port Selected

Step 1: Click to select the device in the topology.
Step 2: Click or drag to select the port.

[Previous](#) [Next](#)

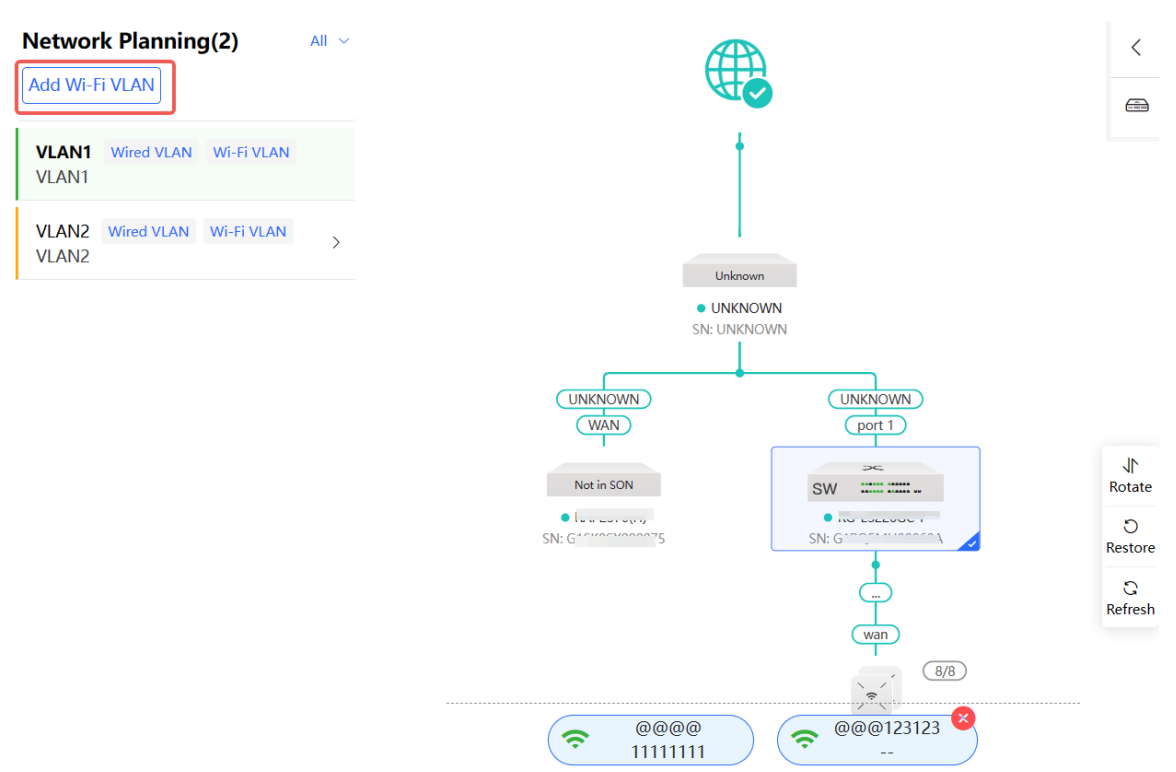
(3) Confirm the configurations and click **Save**. The configurations will take effect in a few minutes.



3.3.2 Configuring a Wi-Fi VLAN

Choose **Network-Wide** > **Workspace** > **Network Planning**.

On the **Network Planning** page, click **Add Wi-Fi LAN**.



Alternatively, you can select an existing wireless VLAN and click **Setup** to edit the VLAN.

- (1) Configure the SSID, Wi-Fi password and band. Click **Expand** to expand the advanced settings and set the parameters. Then, click **Next**.

Configure Network Planning/Add Wi-Fi VLAN

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

i The configuration will take effect after being delivered to AP.

* SSID

Band ☒ 2.4G + 5G ☐ 2.4G ☐ 5G

Security

[Collapse](#)

Wireless Schedule

Hide SSID ☐ (The SSID is hidden and must be manually entered.)

Client Isolation ☐ Prevent wireless clients of this Wi-Fi from communicating with one another.

Band Steering ☐ (The 5G-supported client will access 5G radio preferentially.)

XPress ☐ (The client will faster speed.)

[Next](#)

- (2) Configure the VLAN ID, address pool server and DHCP pool. The gateway is configured as the address pool server by default to assign IP addresses to clients. If an access switch exists on the network, you can select the access switch as the address pool server. Click **Next** after VLAN parameters are configured.

Configure Network Planning/Add Wi-Fi VLAN

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

* Description:

VLAN:

* VLAN ID:

Address Pool ☒ Gateway

Server ⓘ

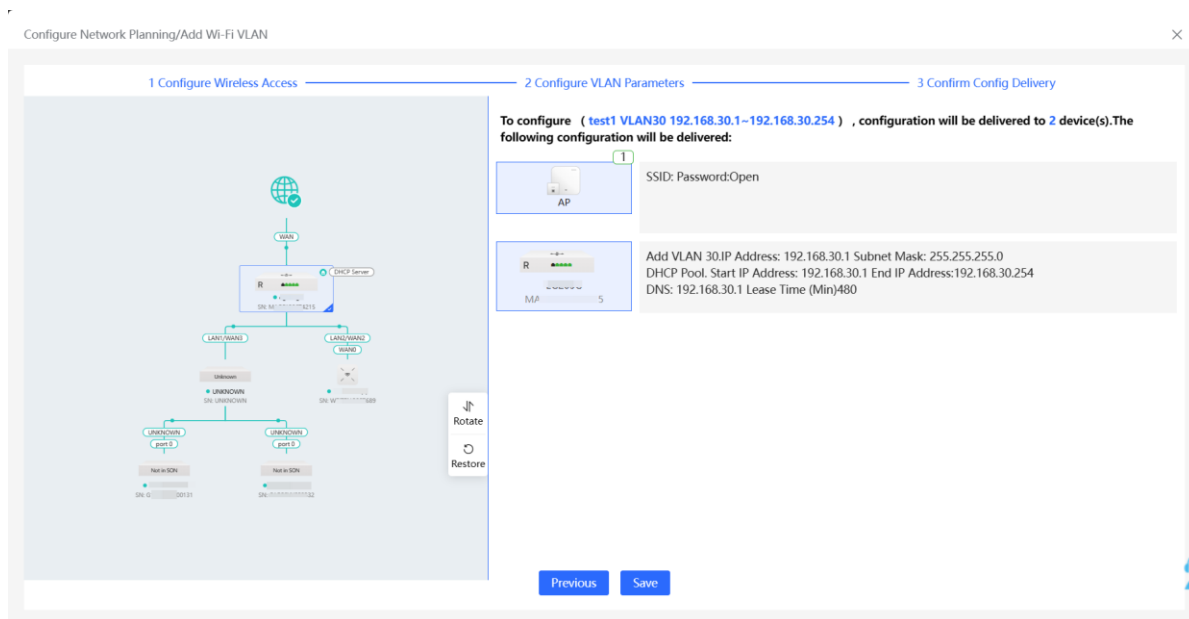
Gateway/Mask: /

DHCP Pool: ☒

IP Range: -

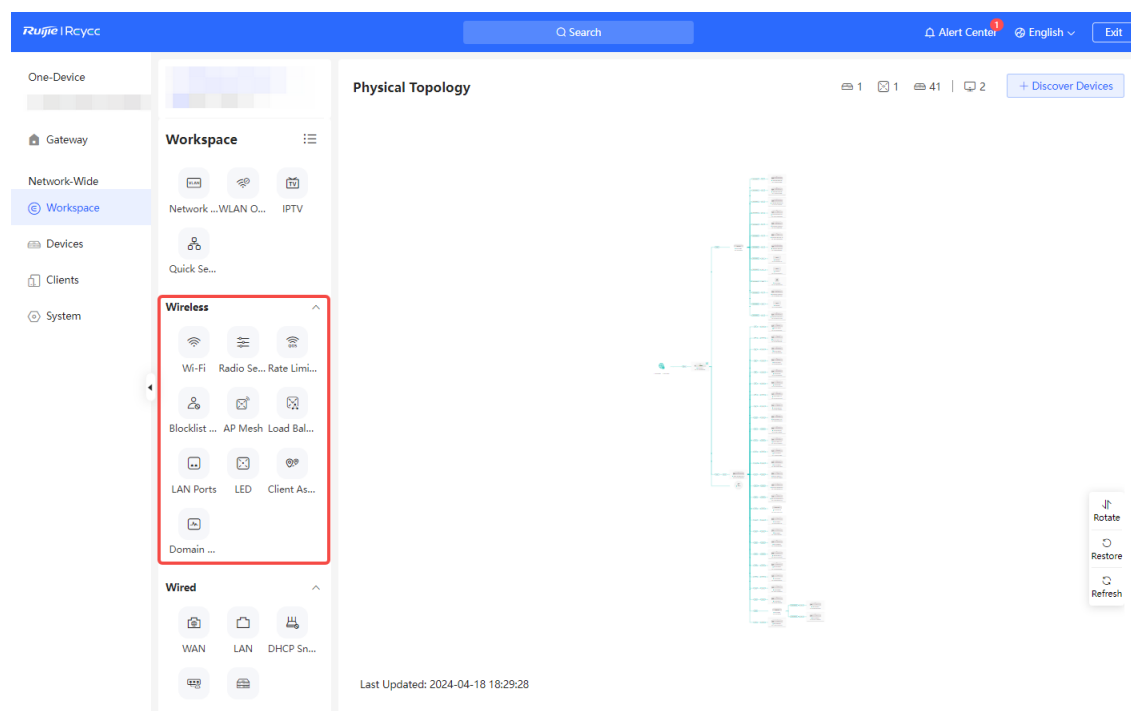
[Previous](#) [Next](#)

- (3) Confirm the delivered configurations and click **Save**. The configurations will take effect in a few minutes.



3.4 Network-wide Wireless Management

Choose **Network-Wide > Workspace > Wireless**.

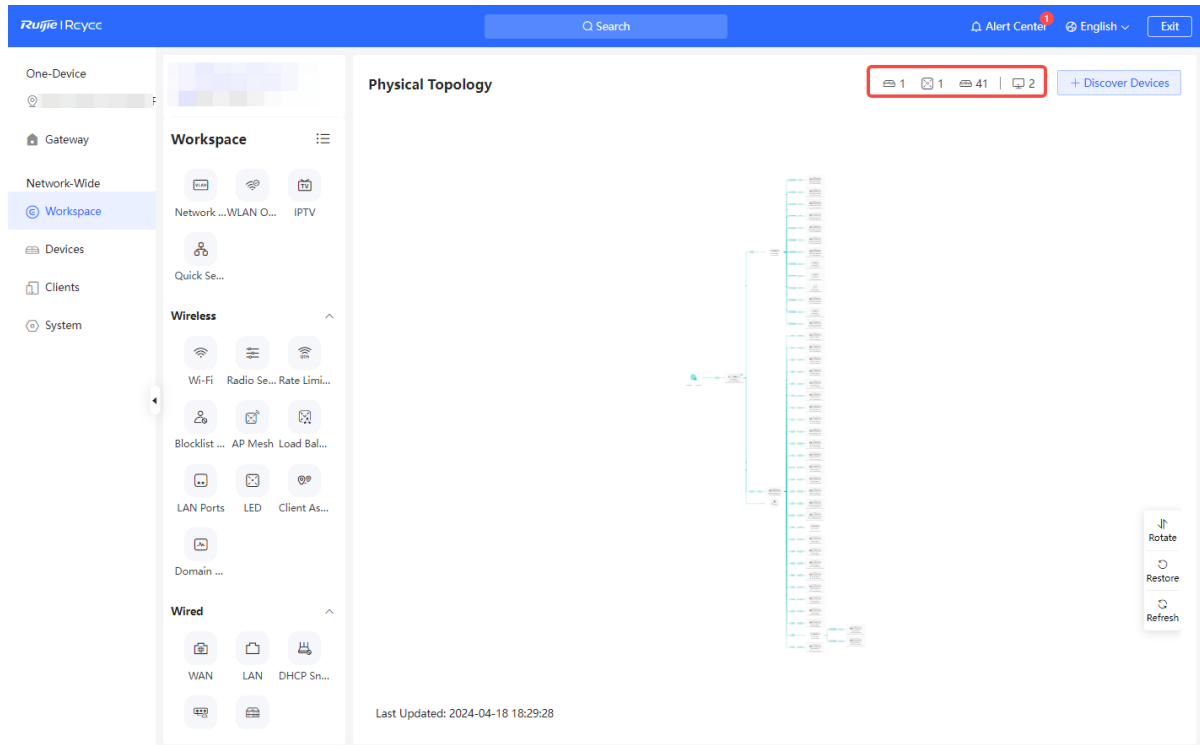


The functions supported by Network-wide Wireless Management depend on the APs on the network. Detailed information on the supported functions can be found in the Web-based Configuration Guide of RG-RAP and RG-EAP devices. For example, if the software version of the AP device is ReyyeOS 2.280, the functions supported by Network-wide Wireless Management can be referenced in the RG-RAP and RG-EAP Web-based Configuration Guide for ReyyeOS 2.280 version.

3.5 Device Management

View all devices on the current network. You can configure and manage the devices simply by logging into one device on the network. The methods to access device management are as follows:

Method 1: Click the device icon in the top right corner of the **Physical Topology** to switch to the device list view.



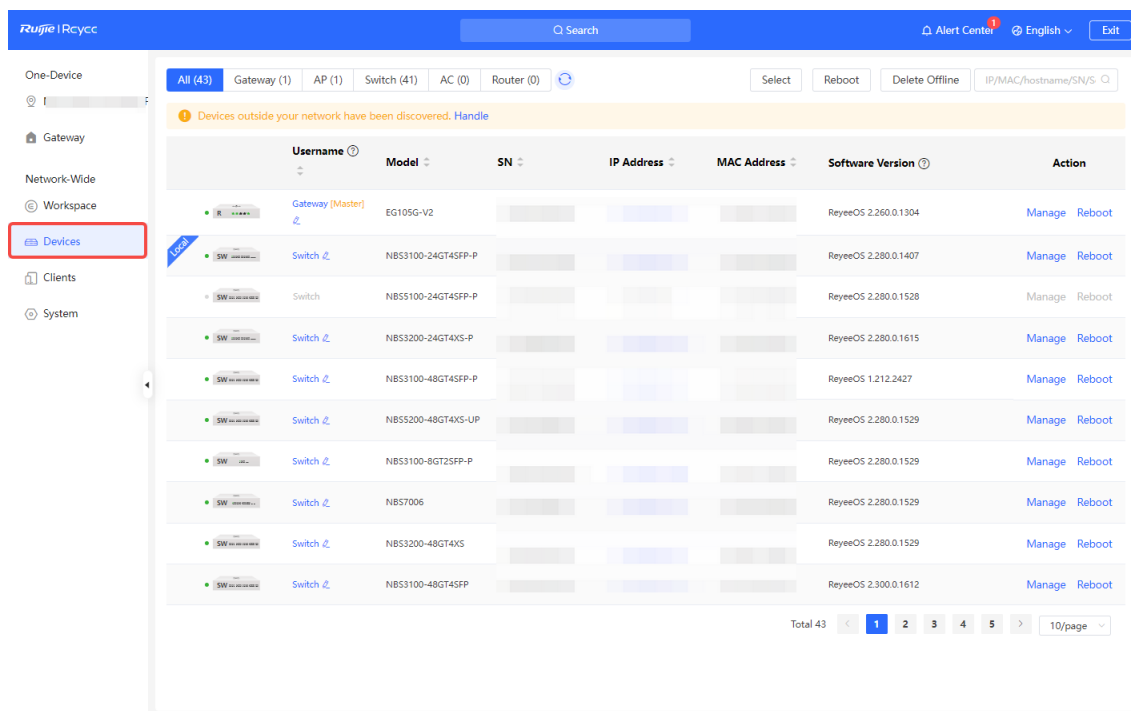
Method 2: Choose **Network-Wide** > Devices

Click Handle to add a device to the current network.

Click Manage to configure a specific device.

Click Reboot to restart a specific device.

Click Select to select offline devices. Then, click Delete Offline. The selected devices will be removed from the list and network topology.



3.6 Online Client Management

Choose **Network-Wide > Clients**.

The client list displays wired, wireless, and users not connected on the current network, including the username, connection mode, associated device, IP/MAC address, IP address binding status, rate, and related operations.





| All (1) Wired (0) Wireless (1) User not connected (0) | | | | | | | | |
|--|---------------|------------------|------------------|---|------------------|---------------------|------------|-----------------|
| The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes. | | | | | | | | |
| Username | SSID and Band | Signal Quality | Connected To | IP/MAC | Negotiation Rate | Online Duration | LimitSpeed | Action |
| Xiaomi-13 | 5G 132 | -40db Channel:56 | AP ZASLASQ000170 | 192.168.120.89 86ee0e1c9ca6 Not bound | 2401M | 5 minutes 5 seconds | No Limit | Associate Block |
| Total 1 | | | | | | | | |

- Click **Not Bound** in the **IP/MAC** column to bind the client to a static IP address.
- Click a button in the **Action** column to perform the corresponding operation on the online client.
 - Wired: Only access control can be configured.
 - Wireless: Access control, associate, and block can be configured.

Note










IP binding and access control are supported only in router mode.

Table 3-1 Online Client Management Configuration Parameters

| Parameter | Description |
|-----------------|--|
| Username | Name of the connected client. |
| SSID and Band | Indicates the access mode of the client, which can be wireless or wired. The SSID and frequency band is displayed when a client is connected wirelessly. |
| Signal Quality | <p>The Wi-Fi signal strength of the client and the associated channel.</p> <hr/> <p> Note</p> <p>This information is displayed only in the wireless online client list.</p> <hr/> |
| Connected To | Indicates wired or wireless connection, the associated device and SN. |
| IP/MAC | Indicates the IP address and MAC address of the client. |
| Negotiated Rate | <p>The uplink data rate and downlink data rate of the client.</p> <hr/> <p> Note</p> <p>This information is displayed only in the wireless online client list.</p> <hr/> |
| Online Duration | <p>Client access duration.</p> <hr/> <p> Note</p> <p>This information is displayed only in the wireless online client list.</p> <hr/> |
| LimitSpeed | <p>Implement wireless speed limiting for clients to prevent certain clients from consuming large amounts of bandwidth resources. For details, see 3.6.4 Configuring Client Rate Limiting.</p> <hr/> <p> Note</p> <p>This information is displayed only in the wireless online client list.</p> <hr/> |
| Action | You can click the corresponding button to perform access control, association, and block operations on online clients. |

Wired Clients

Click the **Wired** tab to see details about wired clients.

| <div> All (24) Wired (23) Wireless (1) User not connected (6)  </div> <div> Select  Block  Bind IP <input type="text" value="Search by IP/MAC/Username"/>  </div> | | | | | | |
|--|---|----------------------|----------------------------------|---|----------------------------|--------------------------------|
|  The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes. | | | | | | |
| Username | SSID and Band | Connected To | IP/MAC | | Rate | Action |
| Click to edit |  Wired G1/18 | NBS6000 NBS6000Q | 192.168.120.1 : : : : : |  Not bound | ↑ 0.00bps ↓ 0.00bps | Access Control |
| PC-4277ac |  Wired G1/21 | NBS6000I MBS6000Q | 192.168.110.3 3C : : : : : ac |  Bound | ↑ 40.18Kbps ↓ 21.28Kbps | Access Control |

Wireless Clients

Click the **Wireless** tab to see details about wireless clients.

All (4)
Wired (1)
Wireless (3)
User not connected (0)

Select
Block
Bind IP
Search by IP/MAC/Username

The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes.

| Username | SSID and Band | Signal Quality | Connected To | IP/MAC | Rate | Negotiation Rate | Online Duration | LimitSpeed | Action |
|-----------------------------|----------------------------|----------------|--------------|----------------------------|--------------------------|------------------|-----------------------|------------|---|
| * 🔗 | 5G Channel:149 ***** | -42db | AP 89 | 192.168.110.6 Not bound | ↑ 0.00kbps ↓ 0.00kbps | 866M | 44 minutes 47 seconds | No Limit | Access Control Associate Block |
| M2102J25C 🔗 | 5G Channel:149 ***** | -33db | AP W***** | 192.168.110.7 Not bound | ↑ 1.20kbps ↓ 5.90kbps | 585M | 8 seconds | No Limit | Access Control Associate Block |

User not connected

Click the **User not connected tab** to see details about clients waiting to connect. This list includes clients tagged manually or recognized as devices previously connected to the network but not currently listed in device management or online client lists. To remove a client device, click **Delete**.

All (24)
Wired (23)
Wireless (1)

User not connected (6)

Bind IP
Search by IP/MAC/Username

The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes.

| Username | MAC Address | Action |
|-------------------|-------------------|--------|
| 00:11:22:33:44:55 | 00:11:22:33:44:55 | Delete |
| 00:11:22:33:44:66 | 00:11:22:33:44:66 | Delete |

3.6.1 Configuring Client IP Binding

Note

This function is supported only in router mode.

Choose **Network-Wide** > **Clients**.

IP address binding is a security and access control policy that associates a specific IP address with a specific device or user to achieve identity authentication, access control, monitoring, and accounting.

- Single client IP address binding
Select the client to be bound with an IP address in the list, click **Not bound**, and click **OK** in the pop-up box to bind the client to a static IP address.

All (1)

Wired (0)

Wireless (1)

User not connected (0)

Select

Block

Bind IP

Search by IP/MAC/Username

The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes.

| Username | SSID and Band | Signal Quality | Connected To | IP/MAC | Negotiation Rate | Online Duration | LimitSpeed | Action |
|-----------|---------------|--------------------|---------------------|---------------------------------|--------------------|---------------------|------------|---------------------------------|
| Xiaomi-13 | 5G 132 | -40db Channel56 | AP ZASLASQ000170 | 192.168.120.89 86ae0e1c39ca6 | Not bound 2401M | 5 minutes 5 seconds | No Limit | Associate Block |

Total 1

1

10/page

Are you sure you want to convert the dynamic IP address to a static IP address?

Cancel

OK

- Batch IP binding
Click **Select**.

Select Block Bind IP Search by IP/MAC/Username

Select the clients to be bound, click **Bind IP**, and click **OK** in the pop-up box to bind the selected clients to a static IP address.

All (1)

Wired (0)

Wireless (1)

User not connected (0)

Deselect

Block

Bind IP

Search by IP/MAC/Username

The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes.

| <input checked="" type="checkbox"/> | Username | SSID and Band | Signal Quality | Connected To | IP/MAC | Negotiation Rate | Online Duration | LimitSpeed | Action |
|-------------------------------------|-----------|---------------|---------------------|---------------------|---|------------------|---------------------|------------|-----------------|
| <input checked="" type="checkbox"/> | Xiaomi-13 | 5G 132 | -40db Channel:56 | AP ZASLASQ000170 | 192.168.120.89 86ee0e1c9ca6 Not bound | 2401M | 5 minutes 5 seconds | No Limit | Associate Block |

Total 1

1

10/page

- Unbind an IP address

Select the client to be unbound from the list, click **Bound**, and click **OK** in the pop-up box.

All (1)

Wired (0)

Wireless (1)

User not connected (0)

Select

Block

Bind IP

Search by IP/MAC/Username

The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes.

| Username | SSID and Band | Signal Quality | Connected To | IP/MAC | Negotiation Rate | Online Duration | LimitSpeed | Action |
|-----------|---------------|---------------------|---------------------|---|------------------|---------------------|---|---|
| Xiaomi-13 | 132 | -40db Channel:56 | AP ZASLASQ000170 | 192.168.120.89 86ee0e1c9ca6 <div> Bound</div> | 2401M | 5 minutes 5 seconds | No Limit | Associate Block |
| Total 1 | | | | | | | <div><div><</div><div>1</div><div>></div></div> | 10/page |

3.6.2 Configuring Client Access Control

Note

This function is supported only in router mode.

Choose **Network-Wide > Clients**.

Select a client in the list and click **Access Control** in the **Action** column. You will be redirected to the **Edit Rule** page, where a MAC-based access control rule is automatically generated. The name and MAC address are automatically generated based on the selected client. After selecting the control type and effective time, click **OK** to create an access control rule for the client.

Edit Rule

Status ☒

Name

Based on ☒ MAC Address ☐ IP Address

* MAC Address

Control Type

Effective Time

Cancel

OK

3.6.3 Blocking Clients

Choose **Network-Wide > Clients**.

An unauthorized client may occupy network bandwidth and pose security risks. You can block specified clients to solve the unauthorized access problem.



Note

Client block is available only for wireless clients.

- Block a single client

Select a client to block in the list, click **Block** in the **Action** column, and click **OK** in the pop-up box to block the selected client.

All (1)
Wired (0)
Wireless (1)
User not connected (0)
⌂
Select
⚙️ Block
⇌ Bind IP
Search by IP/MAC/Username

The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes.

| Username | SSID and Band | Signal Quality | Connected To | IP/MAC | | Negotiation Rate | Online Duration | LimitSpeed | Action |
|-----------|---------------|--------------------|---------------------|--------------------------------|-------|------------------|----------------------|------------|------------------------|
| Xiaomi-13 | 5G 132 | -40db Channel56 | AP ZASLASQ000170 | 192.168.120.89 86ee0e1c9ca6 | Bound | 2401M | 10 minutes 5 seconds | No Limit | Associate Block |

Total 1 < 1 > 10/page

Do you want to add 86:ee:0e:1c:9c:a6 to the blocklist?

Cancel

OK

- Batch block clients

a Click **Select**.

Select
⚙️ Block
⇌ Bind IP
Search by IP/MAC/Username

b Select the target clients, click **Block**, and click **OK** in the pop-up box to block the selected clients.

All (1)
Wired (0)
Wireless (1)
User not connected (0)
⌂
Deselect
⚙️ Block
⇌ Bind IP
Search by IP/MAC/Username

The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes.

| <input checked="" type="checkbox"/> | Username | SSID and Band | Signal Quality | Connected To | IP/MAC | | Negotiation Rate | Online Duration | LimitSpeed | Action |
|-------------------------------------|-----------|---------------|--------------------|---------------------|--------------------------------|-------|------------------|----------------------|------------|------------------------|
| <input checked="" type="checkbox"/> | Xiaomi-13 | 5G 132 | -40db Channel56 | AP ZASLASQ000170 | 192.168.120.89 86ee0e1c9ca6 | Bound | 2401M | 10 minutes 5 seconds | No Limit | Associate Block |

Total 1 < 1 > 10/page

- Cancel block

Choose **Network-Wide > Workspace > Wireless > Blocklist/Allowlist > Global Blocklist/Allowlist**.

Select the client to be removed from the blocklist in the wireless blocklist and click **Delete**.

[Global Blocklist/Allowlist](#) [SSID-Based Blocklist/Allowlist](#)

☒ All STAs except blocklisted STAs are allowed to access Wi-Fi. ☐ Only the allowlisted STAs are allowed to access Wi-Fi.

Blocked WLAN Clients + Add Delete Selected

| <input type="checkbox"/> | Device Name | MAC Address | Action |
|--------------------------|-----------------------------|-------------|---|
| <input type="checkbox"/> | M2102J2SC ? | 8i:_____f | Edit Delete |

Up to 512 members can be added. Total 1 1 10/page

3.6.4 Configuring Client Rate Limiting

Choose **Network-Wide > Clients > Wireless**.

To ensure fair resource allocation, the network administrator can implement wireless rate limiting to prevent some users or devices from occupying a large amount of bandwidth and affecting the network experience of other users.



Note

Rate limiting applies only to wireless clients.

- Configure rate limits for clients

Click the **Wireless** tab, click the **LimitSpeed** column in the table, set the uplink rate limit and downlink rate limit, and click **OK**.

All (1) Wired (0) Wireless (1) User not connected (0) Refresh Deselect Block Bind IP Search by IP/MAC/Username

The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes.

| <input checked="" type="checkbox"/> | Username | SSID and Band | Signal Quality | Connected To | IP/MAC | Negotiation Rate | Online Duration | LimitSpeed | Action |
|-------------------------------------|-----------------------------|---------------|---------------------|---------------------|--|------------------|----------------------|--------------------------|---|
| <input checked="" type="checkbox"/> | Xiaomi-13 ? | 5G 132 | -40db Channel:56 | AP ZASLASQ000170 | 192.168.120.89 86:ee:0e:1c:9ca6 Bound | 2401M | 10 minutes 5 seconds | No Limit | Associate Block |

Total 1 1 10/page

LimitSpeed

Uplink Rate

No Limit by Default. R Kbps

Limit Current: Kbps. Range: 1-1700000 Kbps

Downlink Rate

No Limit by Default. R Kbps

Limit Current: Kbps. Range: 1-1700000 Kbps

[Disable](#)[Cancel](#)[OK](#)

- Cancel rate limits

Click the **Wireless** tab, click the **LimitSpeed** column in the table, and click **Disable**.

All (1) Wired (0) Wireless (1) User not connected (0)

Deselect Block Bind IP Search by IP/MAC/Username

The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes.

| <input checked="" type="checkbox"/> | Username | SSID and Band | Signal Quality | Connected To | IP/MAC | Negotiation Rate | Online Duration | LimitSpeed | Action |
|-------------------------------------|-----------|---------------|--------------------|---------------------|------------------------------------|------------------|----------------------|------------|-----------------|
| <input checked="" type="checkbox"/> | Xiaomi-13 | 5G 132 | -40db Channel56 | AP ZASLASQ000170 | 192.168.120.89 86ee0e1c9ca6 | 2401M | 10 minutes 5 seconds | | Associate Block |

Total 1 10/page

LimitSpeed

Uplink Rate Kbps

Limit Current: **10000** Kbps. Range: 1-1700000 Kbps

Downlink Rate Kbps

Limit Current: **10000** Kbps. Range: 1-1700000 Kbps

Disable

Cancel

OK

3.7 Firewall Management

After a firewall is added to the network, you can manage and configure the firewall on the Web management system.

3.7.1 Viewing Firewall Information

You can view the basic information and license of the firewall on the Web management system.

Choose **Network-Wide > Network > Firewall**.

- (1) If the password of the firewall is inconsistent with that of the gateway, please enter the management password of the firewall and click **OK**.

Tip

A firewall exists in the current network. The password of the firewall is inconsistent with that of the device. Please enter the password of the firewall admin.

Forgot Password

OK

- (2) The basic information, capacity, and security service license of the firewall are displayed on the Web management system.

Firewall Info

Hostname: RG-WALL
 Model: ZS100-S
 IP: 192.168.110.4
 SN: 1234942571039
 MAC: 00:d0:18:91:ab:ab
 Software Ver: NGFW_NTOS 1.0R3, Release(02211502)

[Manage Firewall](#)

License

Activated Licenses: 1.

Capacity

Available Capacity: 3G (Default Capacity: 3G + Licensed Capacity: 0G)
 Remaining Capacity: 7G

Security Service License

| No. | Security Service Name | Description | License Type | Status |
|-----|-----------------------------------|---|------------------|--------------------------------------|
| 1 | App Identification (APP) | Provide the upgrade of the firewall app identification library. | Official License | Activated Expiry Date: 2023-07-26 |
| 2 | Intrusion Prevention System (IPS) | Provide the upgrade of the firewall IPS application library. | - | Not Activated |
| 3 | Anti-Virus (AV) | Provide the upgrade of the firewall AV library. | - | Not Activated |

Click **Manage Firewall** to go to the Web management interface of the firewall. Configure the security policy and license activation for the firewall. For details, see the Web-based configuration guide of the firewall.

3.7.2 Configuring Firewall Port

If the firewall is set to transparent mode, the **Firewall Port Config** page appears. You can select the WAN port connected to the gateway or the LAN port connected to the switch and enable **Security Guard**.

Firewall Port Config

WAN Port: The port connected to the gateway.

LAN Port: The port connected to the switch.

☒ Enable Security Guard
 The security policy of the firewall between the LAN and the WAN is enabled by default.

[Save](#)

3.8 Alerts

When a network exception occurs, the network overview page will display an alert and provide a suggestion. Click an alert in the **Alert Center** to view the faulty device, problem details, and description. You can troubleshoot the fault based on the suggestion.

Ruijie iRcycc

Search

[Alert Center](#) English Exit

The **Alert List** page displays possible problems on the network environment and device. All types of alarms are followed by default. You can click **Unfollow** in the **Action** column to unfollow this type of alarm.

 **Caution**

After unfollowing a specified alert type, you will not discover and process all alerts of this type promptly. Therefore, exercise caution when performing this operation.

View and manage alarms.

Alert List

View Unfollowed Alert

| Expand | Alerts | Suggestion | Action | | | | | | | | | | | |
|--------------|--|--|---------------------------------------|--|-------------------|---------|--------|--------|---------------|--------------|---------------------|--|-------------------|--|
| <div>▼</div> | Power supply is insufficient. | Under voltage may affect device performance or cause device reboot. Please check the power supply of device. | <div>Delete</div> <div>Unfollow</div> | | | | | | | | | | | |
| | <table><thead><tr><th>Device Name</th><th>SN</th><th>Type</th><th>Time</th><th>Details</th><th>Action</th></tr></thead><tbody><tr><td>Ruijie</td><td>G1SK34H004233</td><td>RAP6260(H)-D</td><td>2023-12-06 15:33:10</td><td>Currently, 802.3at PoE power supply is used. A PoE switch or power supply module compliant with IEEE 802.3bt standard is needed to provide power for the device.</td><td><div>Delete</div></td></tr></tbody></table> | Device Name | SN | Type | Time | Details | Action | Ruijie | G1SK34H004233 | RAP6260(H)-D | 2023-12-06 15:33:10 | Currently, 802.3at PoE power supply is used. A PoE switch or power supply module compliant with IEEE 802.3bt standard is needed to provide power for the device. | <div>Delete</div> | |
| Device Name | SN | Type | Time | Details | Action | | | | | | | | | |
| Ruijie | G1SK34H004233 | RAP6260(H)-D | 2023-12-06 15:33:10 | Currently, 802.3at PoE power supply is used. A PoE switch or power supply module compliant with IEEE 802.3bt standard is needed to provide power for the device. | <div>Delete</div> | | | | | | | | | |

Total 1

<1>

10/page

Are you sure you want to unfollow the alarm and delete it from the alarm list?

1. After being unfollowed, an alarm will not appear again.
2. You can click [View Unfollowed Alert](#) to re-follow an unfollowed alarm.

Cancel

OK

Click **View Unfollowed Alert** to view the unfollowed alert. You can follow the alert again in the pop-up window.

View and manage alarms.

Alert List

View Unfollowed Alert

| Expand | Alerts | Suggestion | Action |
|--------|--------|------------|--------|
| | | No Data | |

Total 0

<1>

10/page

View Unfollowed Alert



Power supply is insufficient.

Re-follow

Cancel

3.9 Smart Device Network

Caution

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

3.9.1 Overview

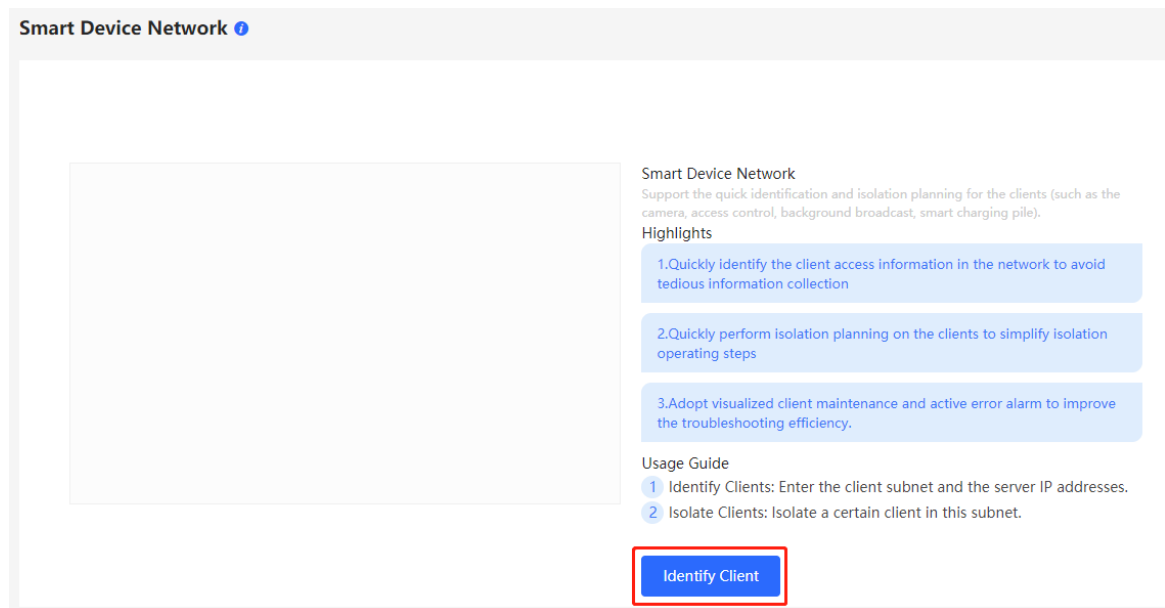
The smart device network is used to quickly plan and set up an isolation network for smart clients, so as to isolate the client network from the normal service network and other types of clients, and improve the stability of the network. The smart device network supports rapid identification of various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

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

3.9.2 Procedure

Choose **Network-Wide > 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.

Smart Device Network

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

| Client Type | Client Subnet IP and Mask | Planned Count | Client Server IP | |
|---|---------------------------|---------------|------------------|--|
| <div> <input type="text"/> <ul style="list-style-type: none"> Camera Video Intercom an... Background Music ... Smart Parking Lot Parking Guidance Smart Charging Pile Smart Lighting Remote Meter Rea... </div> | 192.168.1.0 / 24 | 254 | 192.168.1.2 | <input type="button" value="Delete Subnet"/> |

Added Clients

| -- | 254 |
|----|-----|

- (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**.

Smart Device Network

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

| Client Type | Client Subnet IP and Mask | Planned Count/Identified Count | Client Server IP | Action |
|-------------|---------------------------|--------------------------------|------------------|---|
| test | 192.168.1.0/24 | 254/ 1 | 192.168.1.2 | <input type="button" value="Configure"/> <input type="button" value="Delete Subnet"/> |

Identified Clients

| test | 254/1 |
|------|-------|

Smart Device Network

Identified Servers in 192.168.1.0/24

| No. | Hostname | IP | MAC | Switch SN | Switch Port |
|-----|----------|-------------|-------------------|---------------|-------------|
| 1 | - | 192.168.1.2 | 00:D0:F8:22:74:5E | MACC2020ABCDE | Gi1/23 |

Identified Clients

| test | 254/2 |
|------|-------|

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

Smart Device Network

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

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

| | |
|----------------|-------|
| 192.168.1.0/24 | VLAN3 |
|----------------|-------|

Previous **Generate 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

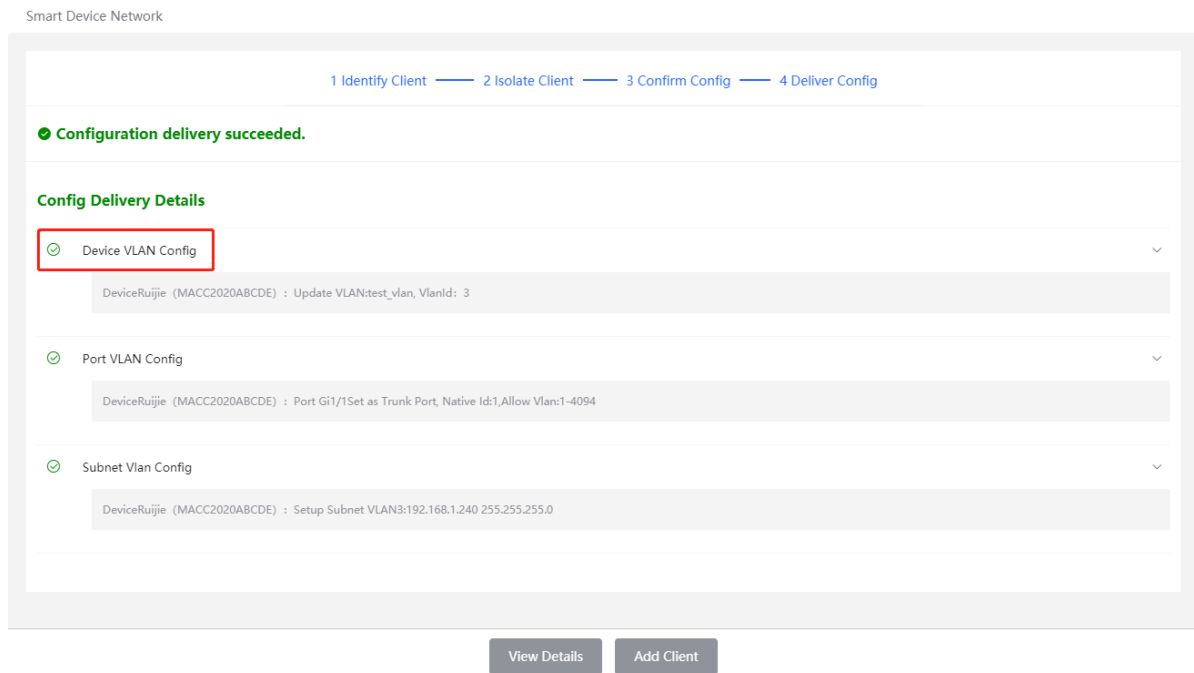
To ensure effective network planning, 1 devices are added autom...

Target Devices
Ruijie(MACC2...

Overtun
Restore

Previous **Deliver Config** Skip

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



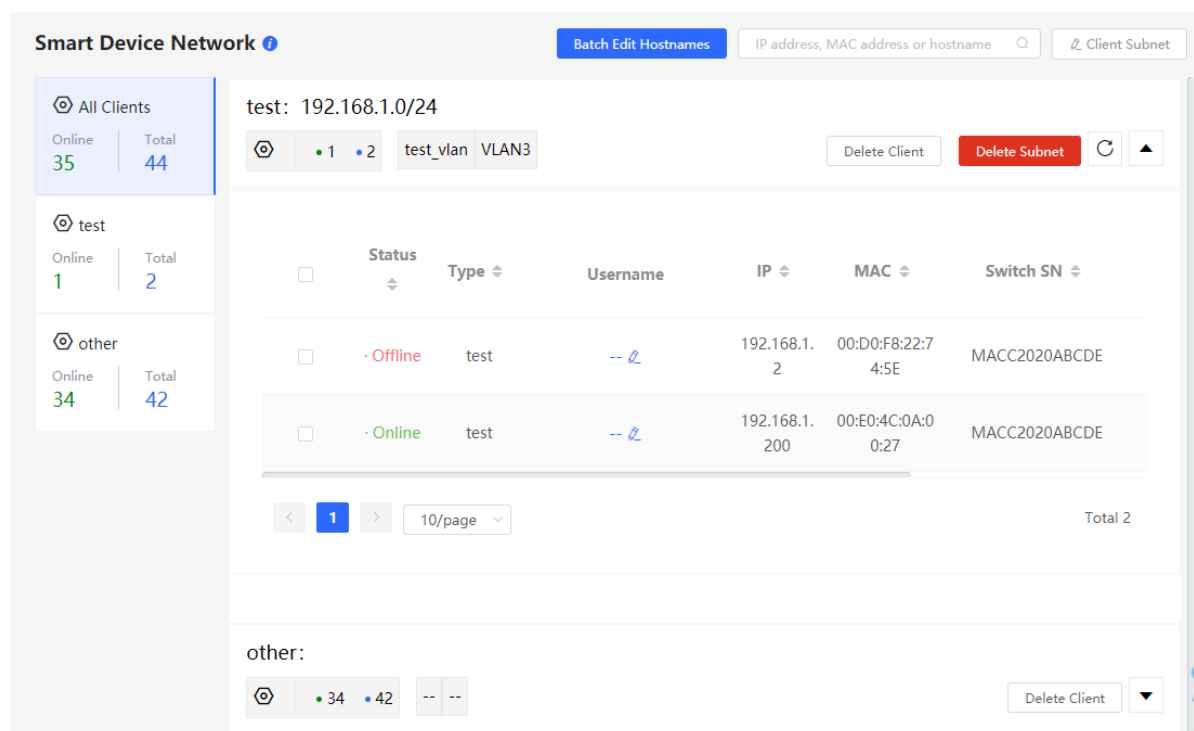
- (7) After completing the smart device network settings, you can view the client monitoring information on the page, including client online status, connection information, device information, and online and offline time.

Select the client entry and click **Delete Client** to remove the specified client from the current network.

Click **Batch Edit Hostnames** to import a txt file containing client IP and client name (one line for each client, each line contains an IP and a name, and the IP and the name are separated by the Tab key), and modify the client names in batches.

Click **Client Subnet** to modify servers and isolate VLAN information, or add a new client network segment.

Click **Delete Subnet** to delete the corresponding smart device network configuration.



4 One-Device Information

4.1 Basic information about the One-Device

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

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

The screenshot displays the Ruijie One-Device management interface. The left sidebar shows the navigation menu with 'One-Device' selected. The main content area is divided into 'Basic Info' and 'Port Info' sections.

Basic Info:

- Model: NBS3100-24GT4SFP-P
- Device Name: [Editable]
- Working Mode: Self-Organizing Network
- MGMT IP: 192.168.110.6
- Connection: Online
- Status: [Online]
- Software Version: ReyeeOS 2.280.0.1407
- System Time: 2024-04-19 19:10:40
- Hardware Version: 3.00
- Uptime: 18 days 9 hours 13 minutes 4 seconds

Port Info:

Traffic data is updated every 5 minutes. Refresh

| Port | Rate | Rx/Tx Speed (kbps) | Rx/Tx Bytes | Rx/Tx Packets | CRC/FCS Error Packets | Corrupted/Oversized Packets | Conflicts |
|------|--------------|--------------------|---------------|-------------------|-----------------------|-----------------------------|-----------|
| Gi1 | 1000M | 18/3 | 3.10G/946.72M | 24382890/12235766 | 0/0 | 0/0 | 0 |
| Gi2 | Disconnected | 0/0 | 0.00/0.00 | 0/0 | 0/0 | 0/0 | 0 |
| Gi3 | Disconnected | 0/0 | 0.00/0.00 | 0/0 | 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 |

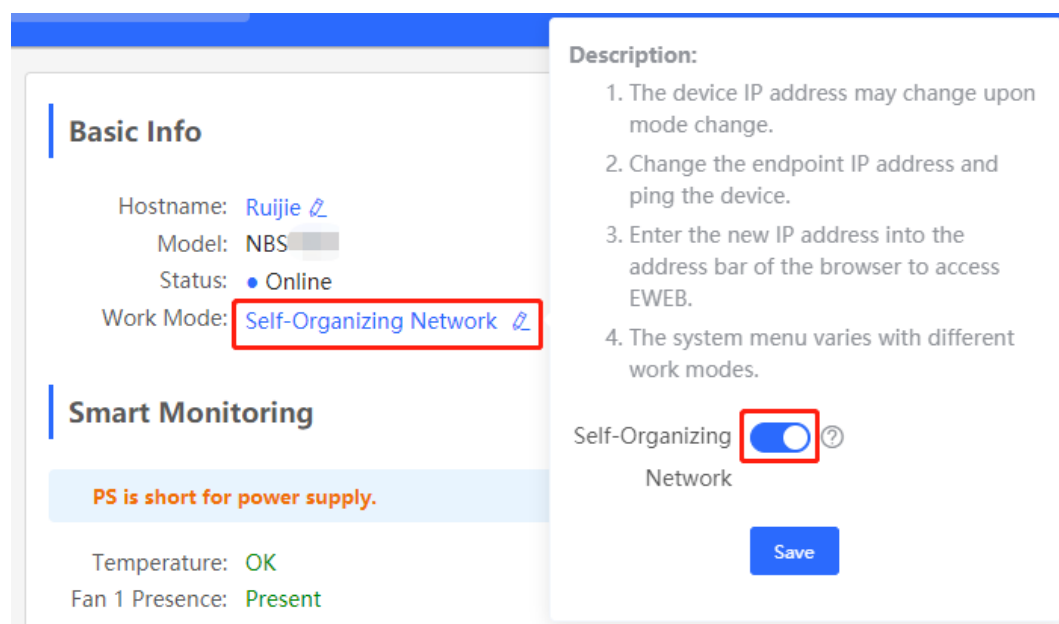
1. Setting the device name

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

The screenshot shows the 'Basic Info' section of the device configuration page. The 'Hostname' field is highlighted with a red box, and a tooltip 'Edit Hostname' is visible. Below it, a modal dialog box titled 'Edit Hostname' is open, showing the current hostname 'Ruijie' in a text input field. The dialog has 'Cancel' and 'OK' buttons.

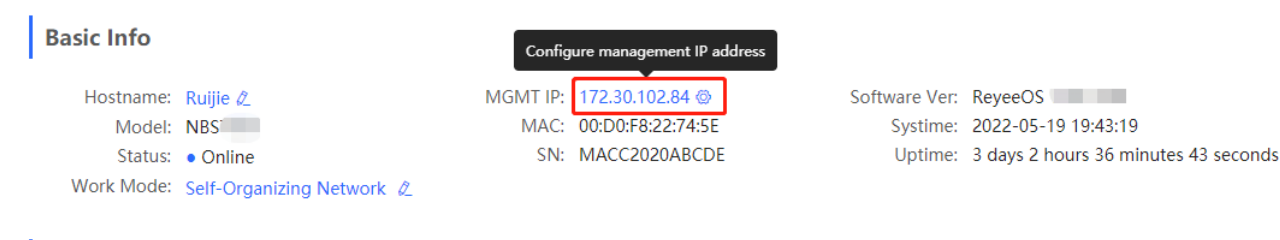
2. Switching the Work Mode

Click the current work mode to change the work mode.



3. Setting MGMT IP

Click current management IP address to jump to the management IP configuration page. For more information, see [7.6](#).



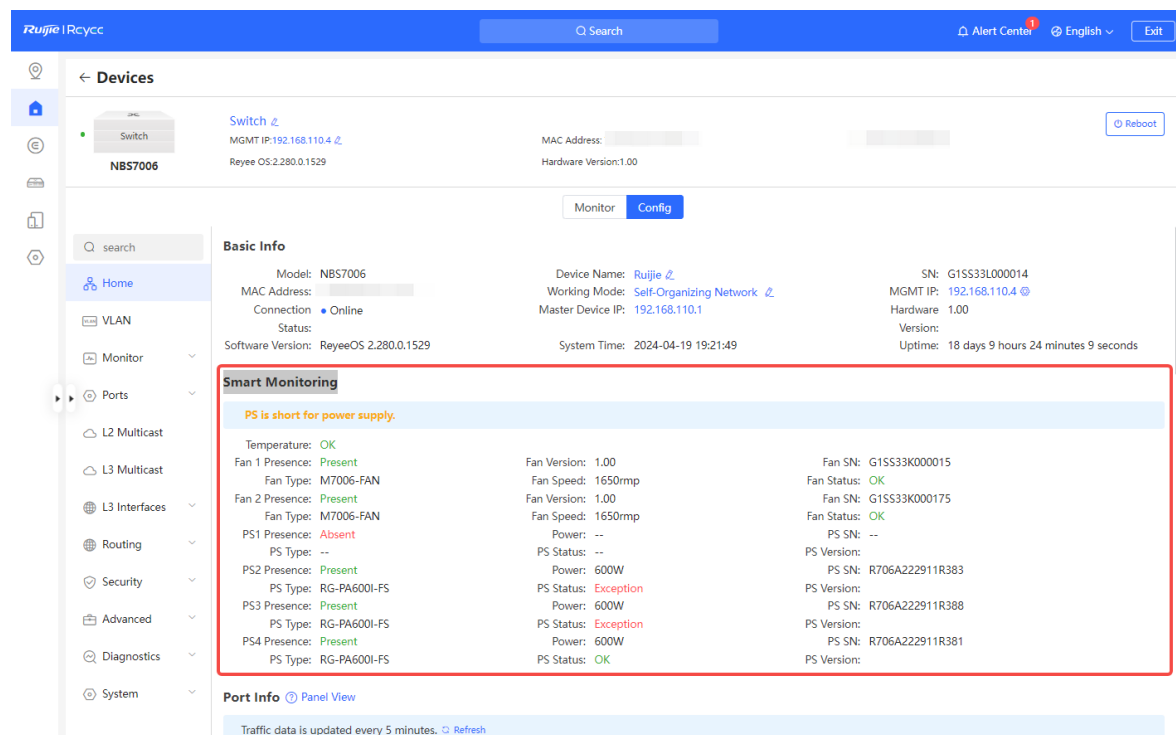
4.2 Smart Monitoring

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**.

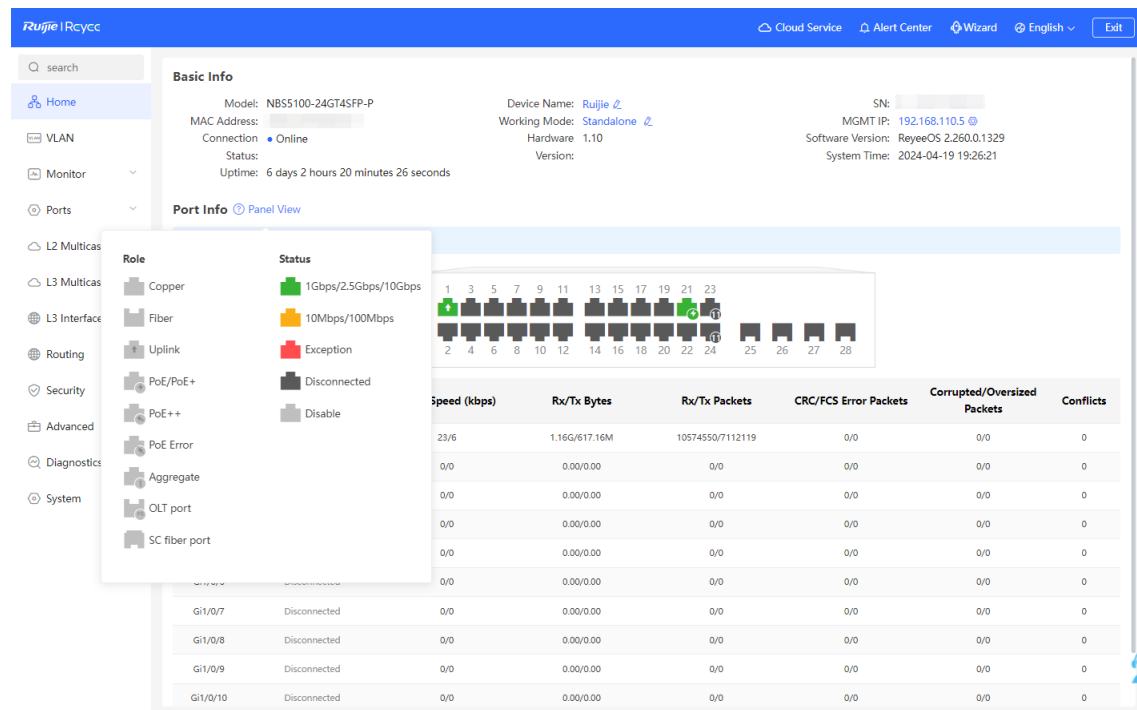
Display the current hardware operating status of the device, such as the device temperature and power supply status, etc.



4.3 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.



- Move the cursor to the icon of a port (for example, Gi14) on the port panel, and more information about the

port will be displayed, including the port ID, port status, port rate, uplink and downlink traffic, transmission rate, and optical/electrical attribute of the port.

Port Info [Panel View](#)

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

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

Port: Gi14

Status: Connected

Rate: 1000M

Flow: ↓ 1.70G ↑ 18.42G

Rate: ↓ 167kbps ↑ 205kbps

Attribute: Copper

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

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

Port Info [Panel View](#)

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

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

| 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 | 74718870/28166645 | 0/0 | 0/0 | 0 |

51

5 VLAN

5.1 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.

5.2 Configuring a VLAN

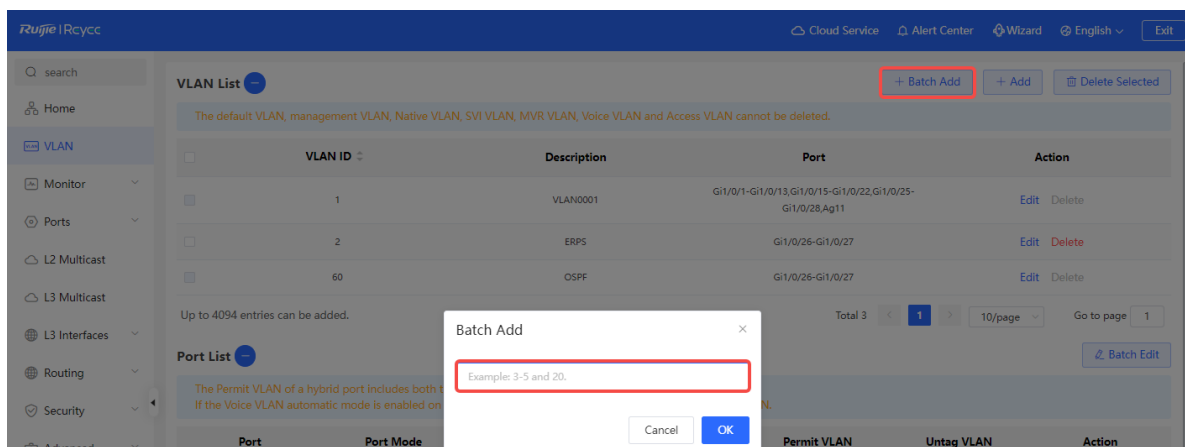
Choose **Local Device > VLAN > VLAN List**.

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

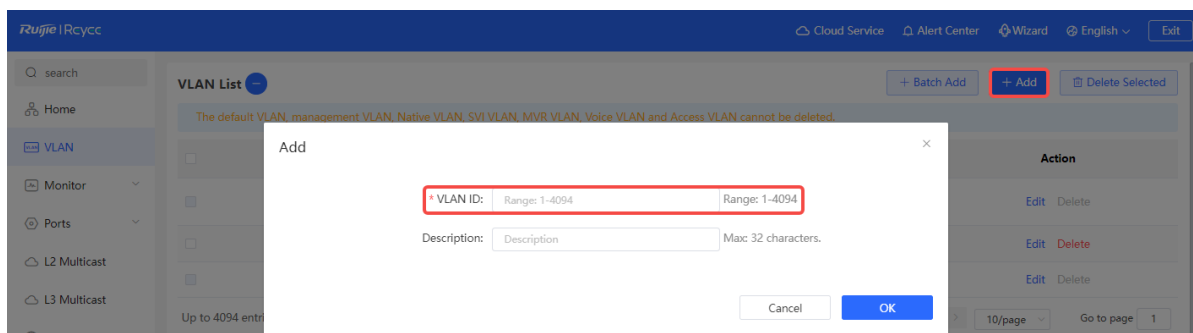
| VLAN ID | Description | Port | Action |
|---------|-------------|--|-------------|
| 1 | VLAN0001 | Gi1/0/1-Gi1/0/13, Gi1/0/15-Gi1/0/22, Gi1/0/25-Gi1/0/28, Ag11 | Edit Delete |
| 2 | ERPS | Gi1/0/26-Gi1/0/27 | Edit Delete |
| 60 | OSPF | Gi1/0/26-Gi1/0/27 | Edit Delete |

5.2.1 Adding a VLAN

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



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

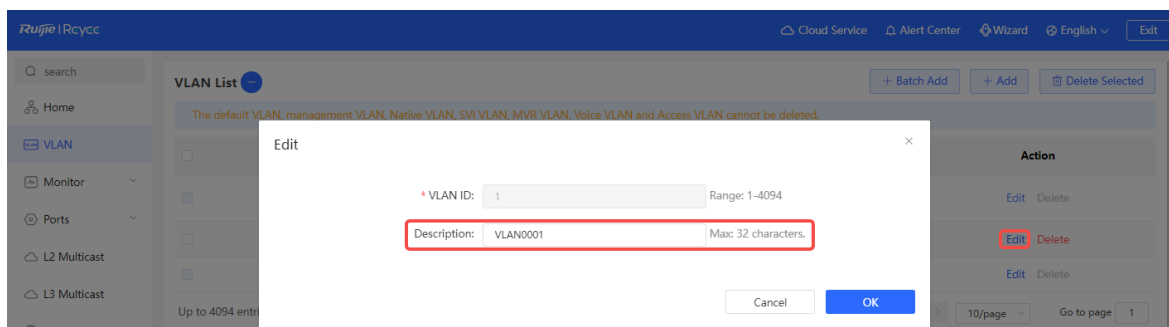


Note

- The range of a VLAN ID is from 1 to 4094.
- You can separate multiple VLANs to be added in batches with commas (,), and separate the start and end VLAN IDs of a VLAN range with a hyphen (-).
- If no VLAN description is configured when the VLAN is added, the system automatically creates a VLAN description in the specified format, for example, VLAN000XX. The VLAN descriptions of different VLANs must be unique.
- If the device supports L3 functions, VLANs, routed ports, and L3 aggregate ports (L3APs) share limited hardware resources. If resources are insufficient, a message indicating resource insufficiency for VLAN will be displayed.

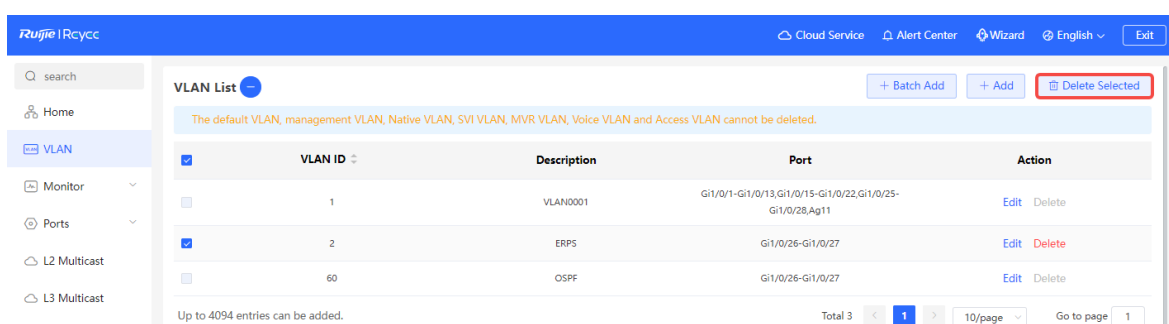
5.2.2 Modifying VLAN Description

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

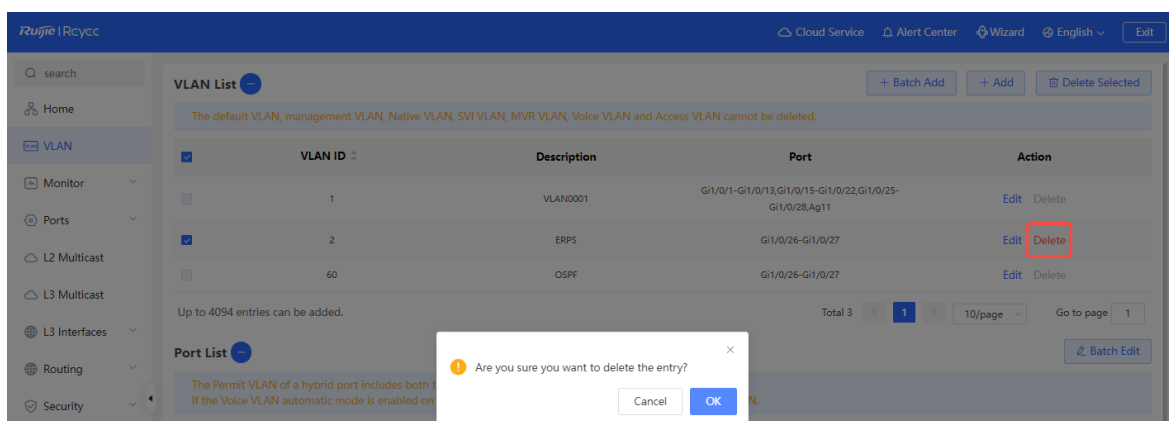


5.2.3 Deleting a VLAN

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



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



Note

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

5.3 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 [5.2 Configuring a VLAN](#)) and then configure the port based on the VLANs.

Up to 4094 entries can be added. Total 3 < 1 > 10/page Go to page 1

Port List [Batch Edit](#)

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

| Port | Port Mode | Access VLAN | Native VLAN | Permit VLAN | Untag VLAN | Action |
|----------|-----------|-------------|-------------|-------------|------------|----------------------|
| Gi1/0/1 | ACCESS | 1 | -- | -- | -- | Edit |
| Gi1/0/2 | ACCESS | 1 | -- | -- | -- | Edit |
| Gi1/0/3 | ACCESS | 1 | -- | -- | -- | Edit |
| Gi1/0/4 | ACCESS | 1 | -- | -- | -- | Edit |
| Gi1/0/5 | ACCESS | 1 | -- | -- | -- | Edit |
| Gi1/0/6 | ACCESS | 1 | -- | -- | -- | Edit |
| Gi1/0/7 | ACCESS | 1 | -- | -- | -- | Edit |
| Gi1/0/8 | ACCESS | 1 | -- | -- | -- | Edit |
| Gi1/0/9 | ACCESS | 1 | -- | -- | -- | Edit |
| Gi1/0/10 | ACCESS | 1 | -- | -- | -- | Edit |

Total 29 < 1 2 3 > 10/page Go to page 1

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

Table 5-1 Port Modes Description

| Port mode | Function |
|-------------|---|
| Access port | <p>One access port can belong to only one VLAN and allow only frames from this VLAN to pass through. This VLAN is called an access VLAN.</p> <p>Access VLAN has attributes of both Native VLAN and Permitted VLAN</p> <p>The frames sent from the Access port do not carry tags. When the access port receives an untagged frame from a peer device, the local device determines that the frame comes from the Access VLAN and adds the access VLAN ID to the frame.</p> |
| Trunk port | <p>One trunk port supports one native VLAN and several allowed VLANs. Native VLAN frames forwarded by a trunk port do not carry tags while allowed VLAN frames forwarded by the trunk port carry tags.</p> <p>A trunk port belongs to all VLANs of the device by default, and can forward frames of all VLANs. You can set the allowed VLAN range to limit VLAN frames that can be forwarded.</p> <p>Note that the trunk ports on both ends of the link must be configured with the same Native VLAN.</p> |
| Hybrid port | <p>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</p> |

| Port mode | Function |
|-----------|--|
| | 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. |

Note

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

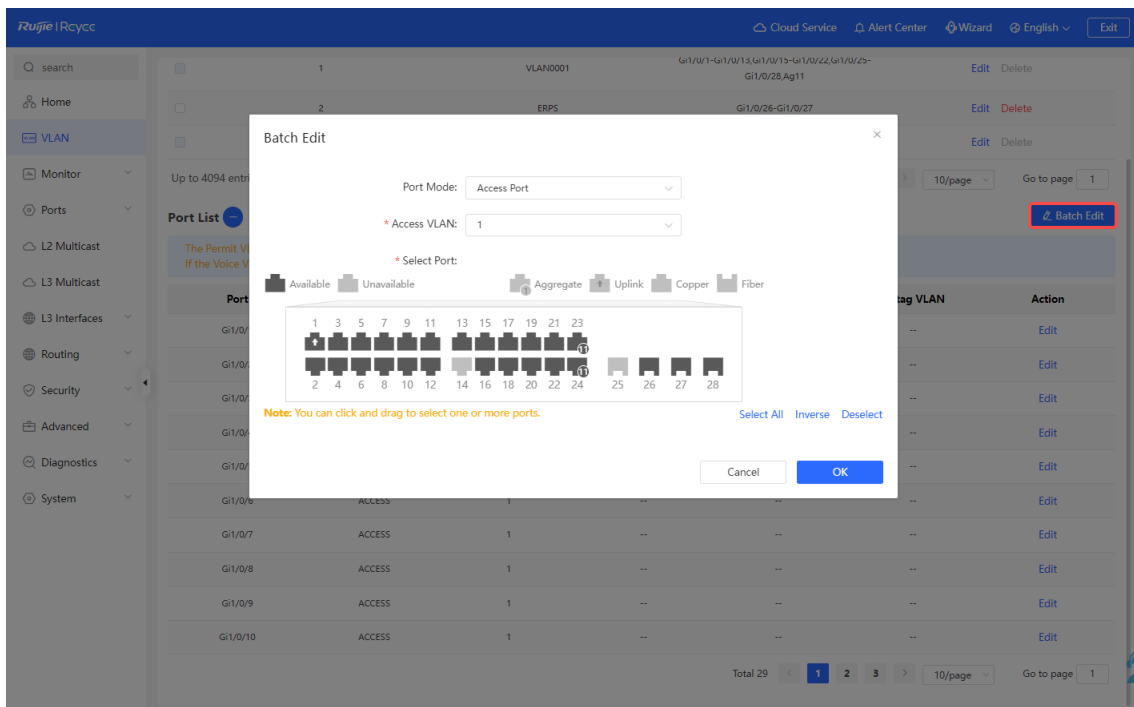
2. Procedure

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

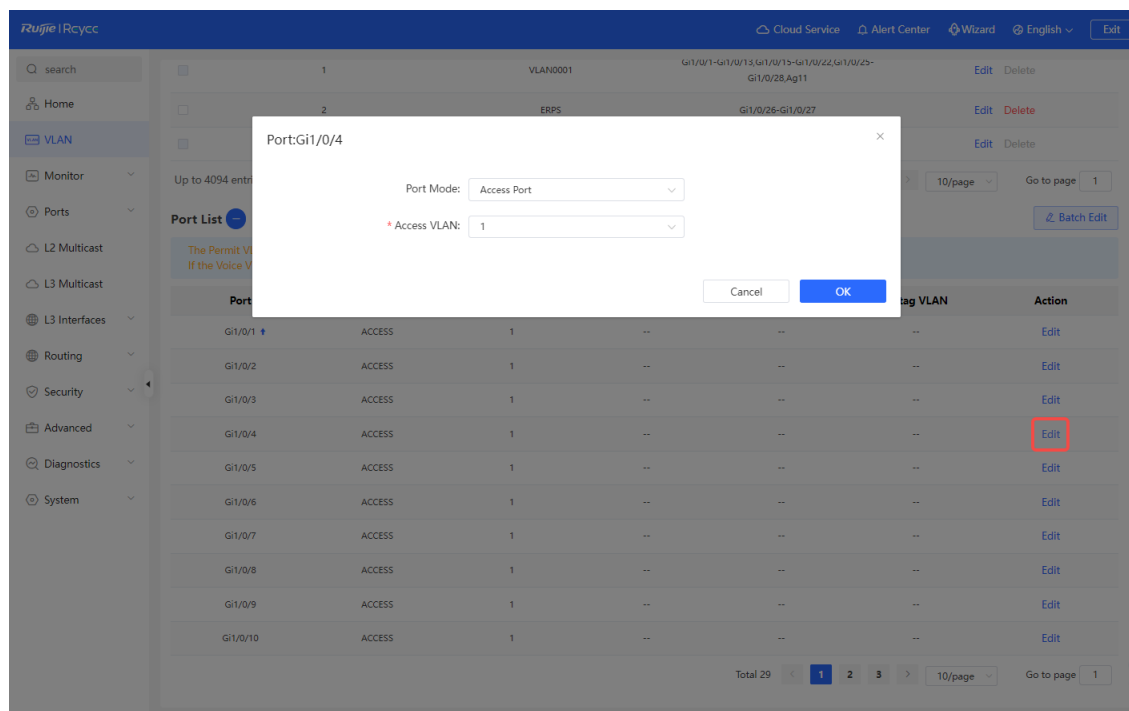
Configure port VLANs in a batch: Click **Batch Edit**, select the port to be configured on the port panel, and select the port mode. If the port mode is Access port, you need to select Access VLAN; if the port mode is Trunk port, you need to select Native VLAN and enter the allowed VLAN ID range; if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



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



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 web interface. Therefore, exercise caution when configuring VLANs.

5.4 Batch Switch Configuration

Caution

Functions in this section are not supported on the NBS6000, and NBS7000 series switches.

1. Overview


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

2. Procedure


Choose **Network > Batch Config**. Choose **Network-Wide > Workspace > Wired > SW 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](#)



RG-ES205C-P
MACCWLD789205GC



NBS5200-24SFP/8GT4XS
G1NW31N000172

RG-ES205C-P (1)

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

NBS5200-24SFP/8GT4XS (1)

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

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

| VLAN ID | Remark | VLAN ID | Remark |
|---------|--------------|---------|--------|
| 1 | Default VLAN | 12 | |

[Previous](#)
[Next](#)

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

Port

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

Type

Trunk Port

* Native VLAN

Default VLAN

Permitted VLAN

1,12

Previous

Override

3. 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/8GT4XS

SN:G1NW31N000172

Software Ver:ReyeeOS 1.86.1619

MGMT IP:10.44.78.1

MAC: 00:d3:f8:15:08:5b

Port Status

VLAN Info

Port

Route Info

RLDP

More

VLAN

VLAN1

VLAN12

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

1 3 5 7 9 11 13 15 17 19 21 23

4

8

1

1

2

3

17

19

21

23

2 4 6 8 10 12 14 16 18 20 22 24

8

1

1

2

3

18

20

22

24

25 26 27

Port

Edit

59

6 Monitoring

6.1 Port Flow

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

This page displays 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 interfaces can be configured. Traffic of an aggregate interface is the sum of traffic of all member ports.

| Port | Rate | Rx/Tx Speed (kbps) | Rx/Tx Bytes | Rx/Tx Packets | CRC/FCS Error Packets | Corrupted/Oversized Packets | Conflicts |
|----------|--------------|--------------------|---------------|------------------|-----------------------|-----------------------------|-----------|
| Gi1/0/1 | 1000M | 14/19 | 1.16G/620.11M | 10617025/7141105 | 0/0 | 0/0 | 0 |
| Gi1/0/2 | Disconnected | 0/0 | 0.00/0.00 | 0/0 | 0/0 | 0/0 | 0 |
| Gi1/0/3 | Disconnected | 0/0 | 0.00/0.00 | 0/0 | 0/0 | 0/0 | 0 |
| Gi1/0/4 | Disconnected | 0/0 | 0.00/0.00 | 0/0 | 0/0 | 0/0 | 0 |
| Gi1/0/5 | Disconnected | 0/0 | 0.00/0.00 | 0/0 | 0/0 | 0/0 | 0 |
| Gi1/0/6 | Disconnected | 0/0 | 0.00/0.00 | 0/0 | 0/0 | 0/0 | 0 |
| Gi1/0/7 | Disconnected | 0/0 | 0.00/0.00 | 0/0 | 0/0 | 0/0 | 0 |
| Gi1/0/8 | Disconnected | 0/0 | 0.00/0.00 | 0/0 | 0/0 | 0/0 | 0 |
| Gi1/0/9 | Disconnected | 0/0 | 0.00/0.00 | 0/0 | 0/0 | 0/0 | 0 |
| Gi1/0/10 | Disconnected | 0/0 | 0.00/0.00 | 0/0 | 0/0 | 0/0 | 0 |

6.2 Client Management

6.2.1 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

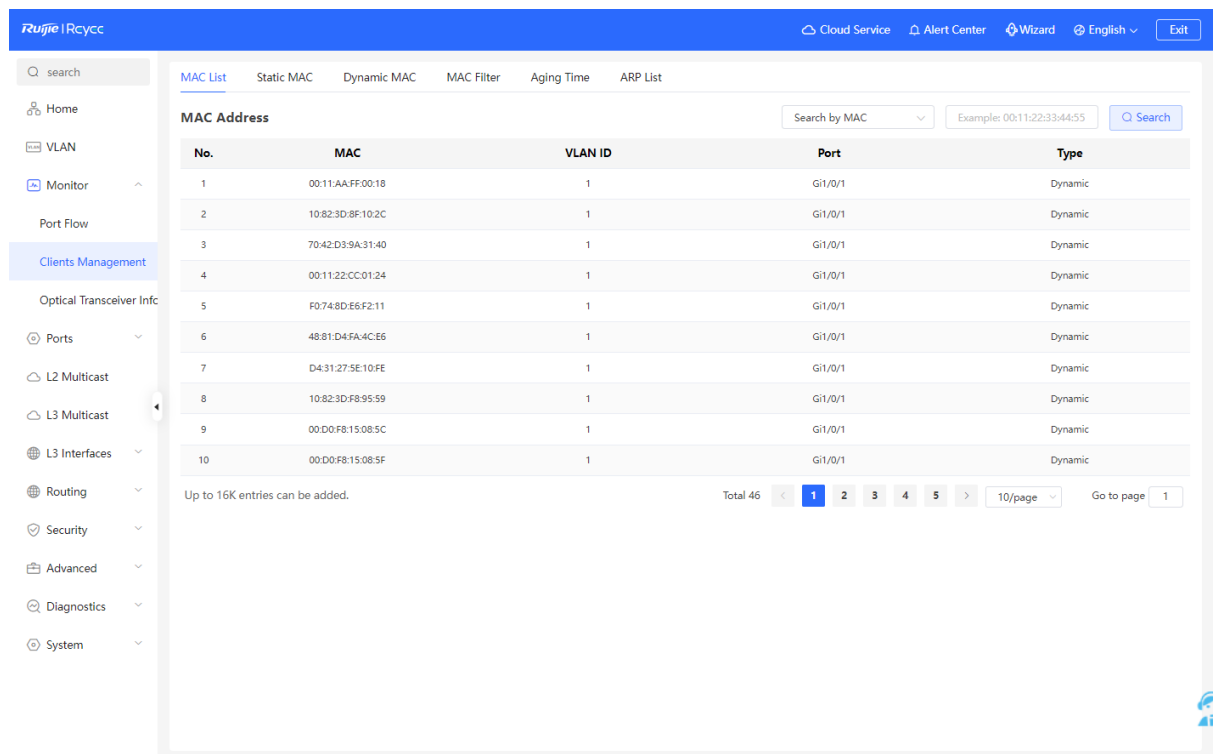
This section describes the management of static, dynamic, and filtering MAC address entries, and does not cover multicast MAC address entries.

6.2.2 Displaying the MAC Address Table

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

This page 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: Query 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. Fuzzy search is supported.



The screenshot displays the Ruijie iRcycs web interface. The top navigation bar includes links for Cloud Service, Alert Center, Wizard, English, and an Exit button. The left sidebar contains a search bar and a list of navigation items: Home, VLAN, Monitor, Port Flow, Clients Management (highlighted), Optical Transceiver Info, Ports, L2 Multicast, L3 Multicast, L3 Interfaces, Routing, Security, Advanced, Diagnostics, and System. The main content area is titled 'MAC List' and includes tabs for Static MAC, Dynamic MAC, MAC Filter, Aging Time, and ARP List. Below these tabs is a 'MAC Address' section with a search bar (Search by MAC) and a search button. The search bar contains the example text 'Example: 00:11:22:33:44:55'. Below the search bar is a table with the following columns: No., MAC, VLAN ID, Port, and Type. The table lists 10 entries, all with VLAN ID 1 and Port Gi1/0/1. The entries are as follows:

| No. | MAC | VLAN ID | Port | Type |
|-----|-------------------|---------|---------|---------|
| 1 | 00:11:AA:FF:00:18 | 1 | Gi1/0/1 | Dynamic |
| 2 | 10:82:3D:8F:10:2C | 1 | Gi1/0/1 | Dynamic |
| 3 | 70:42:D3:9A:31:40 | 1 | Gi1/0/1 | Dynamic |
| 4 | 00:11:22:CC:01:24 | 1 | Gi1/0/1 | Dynamic |
| 5 | F0:74:8D:E6:F2:11 | 1 | Gi1/0/1 | Dynamic |
| 6 | 48:81:D4:FA:4C:E6 | 1 | Gi1/0/1 | Dynamic |
| 7 | D4:31:27:5E:10:FE | 1 | Gi1/0/1 | Dynamic |
| 8 | 10:82:3D:F8:95:59 | 1 | Gi1/0/1 | Dynamic |
| 9 | 00:D0:F8:15:08:5C | 1 | Gi1/0/1 | Dynamic |
| 10 | 00:D0:F8:15:08:5F | 1 | Gi1/0/1 | Dynamic |

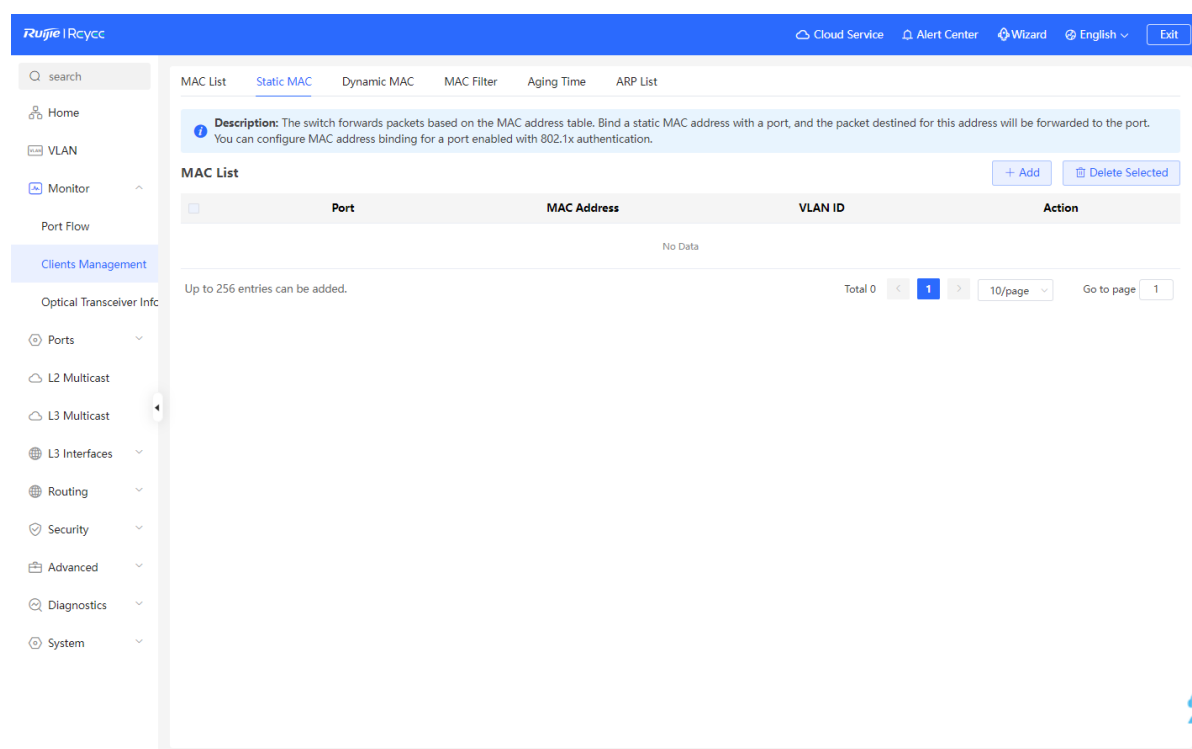
Below the table, it states 'Up to 16K entries can be added.' and 'Total 46' entries. The pagination bar shows '10/page' and 'Go to page 1'.

Note

The MAC address entry capacity depends on the product. For example, the MAC address entry capacity of the device shown in the preceding figure is 32000.

6.2.3 Configuring Static MAC Binding

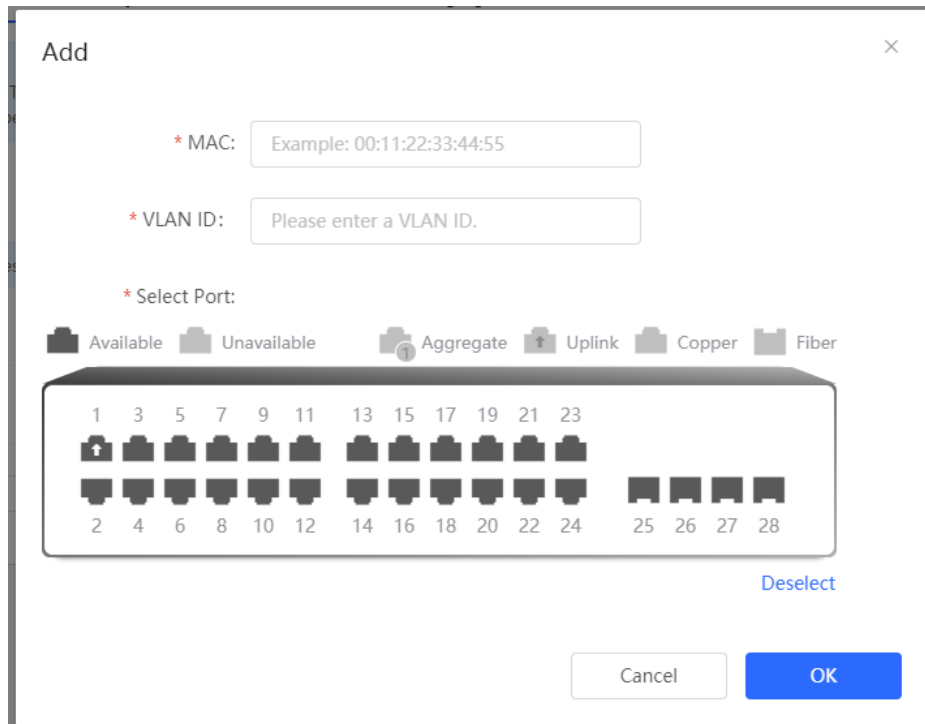
The switch forwards data based on the MAC address table. You can set a static MAC address entry to manually bind the MAC address of a downlink network device to the port of the device. After a static address entry is configured, when the device receives a packet destined to this address from the VLAN,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



1. Adding Static MAC Address Entries

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

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



Add

* MAC:

* VLAN ID:

* 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

Deselect

Cancel OK

2. Deleting Static MAC Address Entries

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

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

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

| MAC List | | | | |
|-------------------------------------|------|-------------------|---------|--------|
| Up to 256 entries can be added. | | | | |
| <input checked="" type="checkbox"/> | Port | MAC | VLAN ID | Action |
| <input checked="" type="checkbox"/> | Gi28 | 00:11:22:33:44:55 | 1 | Delete |

6.2.4 Displaying Dynamic MAC Address

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

After receiving a 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.

MAC List Static MAC **Dynamic MAC** MAC Filter Aging Time ARP List

MAC List

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

| No. | MAC | VLAN ID | Port |
|-----|-------------------|---------|---------|
| 1 | 00:11:AA:FF:00:18 | 1 | Gi1/0/1 |
| 2 | 10:82:3D:8F:10:2C | 1 | Gi1/0/1 |
| 3 | 70:42:D3:9A:31:40 | 1 | Gi1/0/1 |
| 4 | 00:11:22:CC:01:24 | 1 | Gi1/0/1 |
| 5 | F0:74:8D:E6:F2:11 | 1 | Gi1/0/1 |
| 6 | 48:81:D4:FA:4C:E6 | 1 | Gi1/0/1 |
| 7 | D4:31:27:5E:10:FE | 1 | Gi1/0/1 |
| 8 | 10:82:3D:F8:95:59 | 1 | Gi1/0/1 |
| 9 | 00:D0:F8:15:08:5C | 1 | Gi1/0/1 |
| 10 | 00:D0:F8:15:08:5F | 1 | Gi1/0/1 |

Total 46 1 2 3 4 5 10/page Go to page 1

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

MAC List

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

Clear by MAC

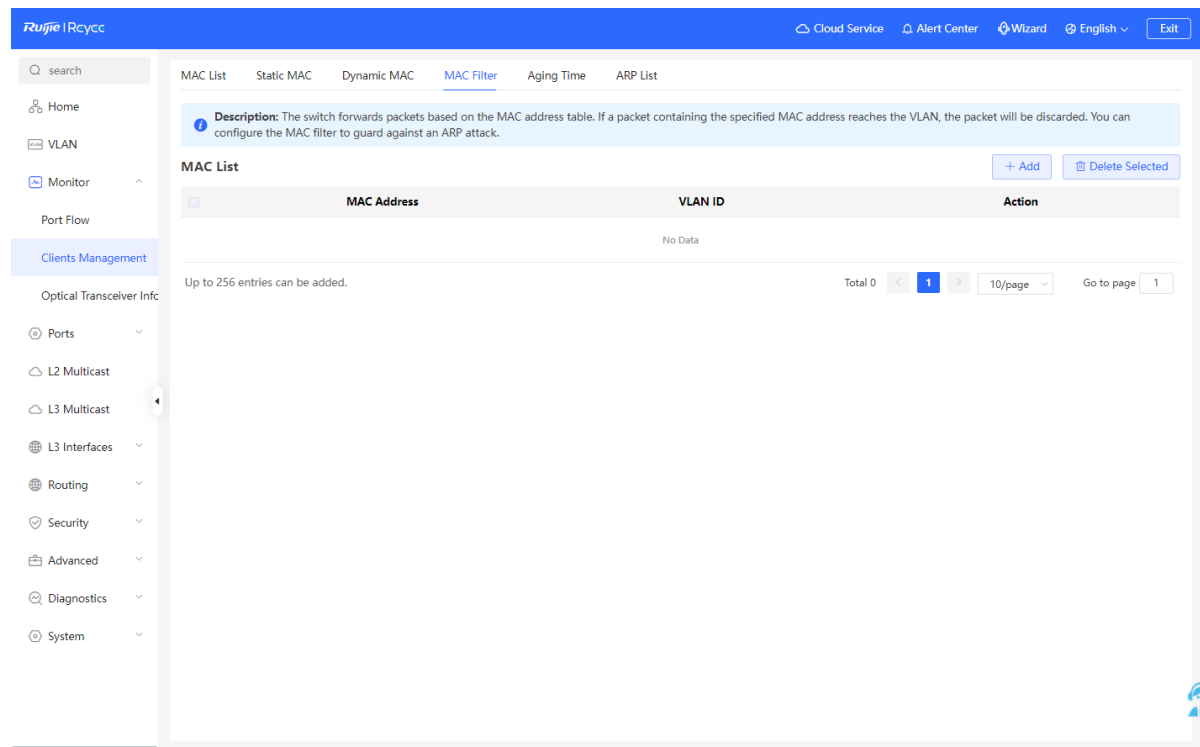
Clear by Port

Clear by VLAN

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

6.2.5 Configuring MAC Address Filtering

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



1. Adding Filtering MAC Address

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

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

2. MAC Filter

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

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

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

| MAC List | | | |
|-------------------------------------|-------------------|---------|--------|
| Up to 256 entries can be added. | | | |
| <input checked="" type="checkbox"/> | MAC | VLAN ID | Action |
| <input checked="" type="checkbox"/> | 00:11:22:33:44:55 | 1 | Delete |

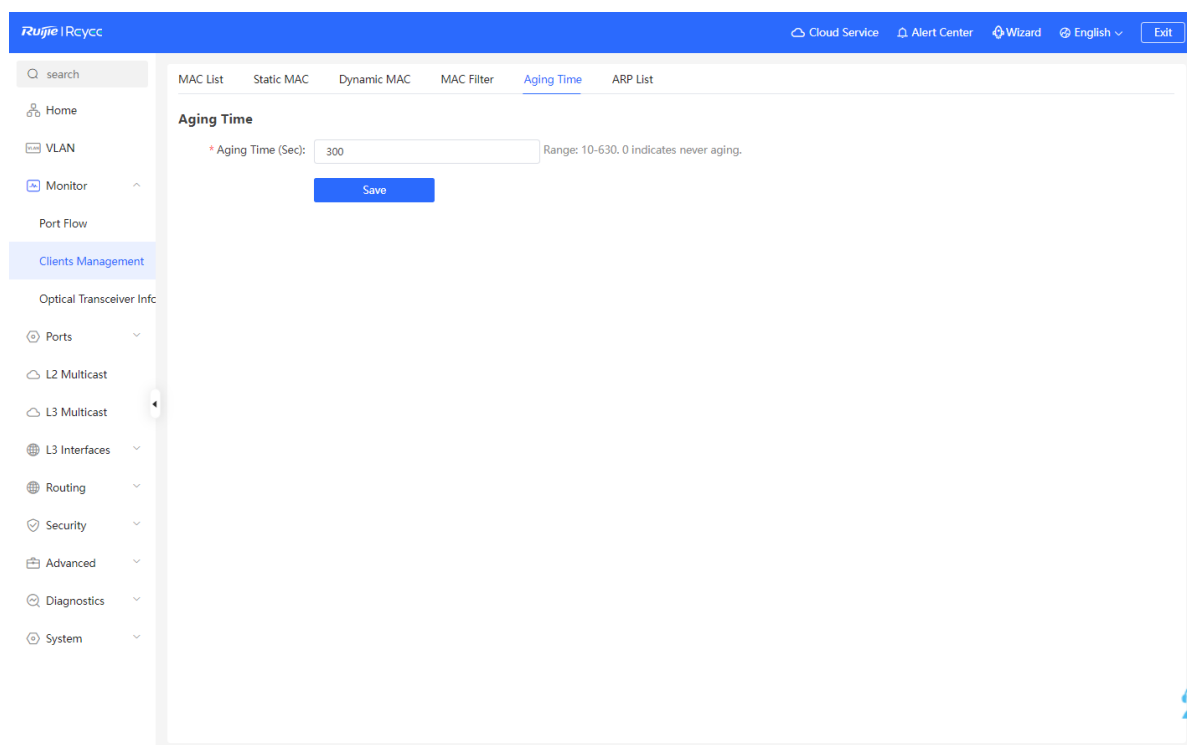
6.2.6 Configuring MAC Address Aging Time

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

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

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

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



6.2.7 Displaying ARP Information

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

When two IP-based devices need to communicate with each other, the sender must know the IP address and MAC address of the peer. With MAC addresses, an IP-based device can encapsulate link-layer frames and then

send data frames to the physical network. The process of obtaining MAC addresses based on IP addresses is called address resolution.

The Address Resolution Protocol (ARP) is used to resolve IP addresses into MAC addresses. ARP can obtain the MAC address associated with an IP address. The 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 an IP or MAC address. Click **Refresh** to obtain the latest ARP entries.

Note

For details about the ARP function, see [10.6](#).

The screenshot shows the Ruijie iRcycs web interface. The left sidebar contains navigation options: Home, VLAN, Monitor, Port Flow, Clients Management (selected), Optical Transceiver Info, Ports, L2 Multicast, L3 Multicast, L3 Interfaces, Routing, Security, Advanced, Diagnostics, and System. The main content area is titled 'ARP List' and includes a description: 'The device learns IP-MAC mapping of all devices connected to its interfaces.' Below the description is a table with the following data:

| No. | IP Address | MAC Address |
|-----|----------------|-------------------|
| 1 | 192.168.110.8 | 00:d0:f8:15:08:5f |
| 2 | 192.168.110.14 | 70:42:d3:9a:31:40 |
| 3 | 192.168.110.17 | 10:82:3d:59:32:34 |
| 4 | 192.168.110.12 | 48:81:d4:fa:4c:e6 |
| 5 | 192.168.110.2 | 10:82:3d:31:05:f9 |
| 6 | 192.168.110.6 | 70:85:c4:89:6d:3c |
| 7 | 192.168.110.4 | 70:42:d3:9a:3b:a0 |
| 8 | 192.168.110.48 | 54:16:51:21:a9:ab |
| 9 | 192.168.110.11 | 00:d0:f8:35:28:51 |
| 10 | 192.168.110.18 | 28:d0:f5:ff:99:26 |

At the bottom of the table, there is a pagination bar showing 'Total 15' entries, with page 1 selected out of 2 pages. There is also a search bar and a 'Refresh' button.

6.3 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, transmit power, local receive 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 Transceiver Info

Search by Port

All

Refresh

| Port | DDM | Temperature(°C) | Voltage(V) | Current(mA) | Tx power(dBm) | Local Rx Power(dBm) | Vendor | Vendor Oui | Vendor P/N | Vendor Revision Number | Transceiver SN | Date of Manufacture | Decoding Mode | Transceiver Type | Connector Type | Wavelength(nm) | Max Transmission Range(m) |
|------|-----|-----------------|------------|-------------|---------------|---------------------|--------|------------|------------|------------------------|----------------|---------------------|---------------|------------------|----------------|----------------|---------------------------|
| | | | | | | | | | | | | | | | | | |

7 Ports

7.1 Overview

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

Table 7-1 Description of Port Type

| Port Type | Note | Remarks |
|-------------------|---|---|
| Switch Port | A switch port consists of a single physical port on the device and provides only the L2 switching function. Switch ports are used to manage physical port and their associated L2 protocols. | Described in this section |
| L2 aggregate port | An Interface binds multiple physical members to form a logical link. For L2 switching, an aggregate port is like a high-bandwidth switch port. It can combine the bandwidths of multiple ports to expand link bandwidth. In addition, for frames sent through an L2 aggregate port, load balancing is performed on member ports of the L2 aggregate port. If one member link of the aggregate port fails, the L2 aggregate port automatically transfers traffic on this link to other available member links, improving connection reliability. | Described in this section |
| SVI Port | A switch virtual interface (SVI) serves as the management interface of the device, through which the device can be managed. You can also create an SVI as a gateway interface, which is equivalent to the virtual interface of corresponding VLAN and can be used for inter-VLAN routing on L3 devices. | For related configuration, see 10.1 Setting an L3 Interface |
| 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 10.1 Setting an L3 Interface |

| Port Type | Note | Remarks |
|-------------------|---|--|
| L3 Aggregate Port | <p>An L3 aggregate port is a logical aggregate port group composed of multiple physical member ports, just like an L2 aggregate port. The ports to be aggregated must be L3 ports of the same type. An aggregate port serves as the gateway interface of L3 switching. It treats multiple physical links in the same aggregate group as one logical link. It is an important way to expand link bandwidth. Multiple physical links are combined into one logical link, expanding the bandwidth of a link. Frames sent over the L3 AP are balanced among the L3 AP member ports. If one member link fails, the L3 AP automatically transfers the traffic on the faulty link to other member links, improving reliability of connections.</p> <p>L3 aggregate ports do not support the L2 switching function.</p> | <p>For related configuration, see 10.1 Setting an L3 Interface</p> |

7.2 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.

7.2.1 Basic Settings

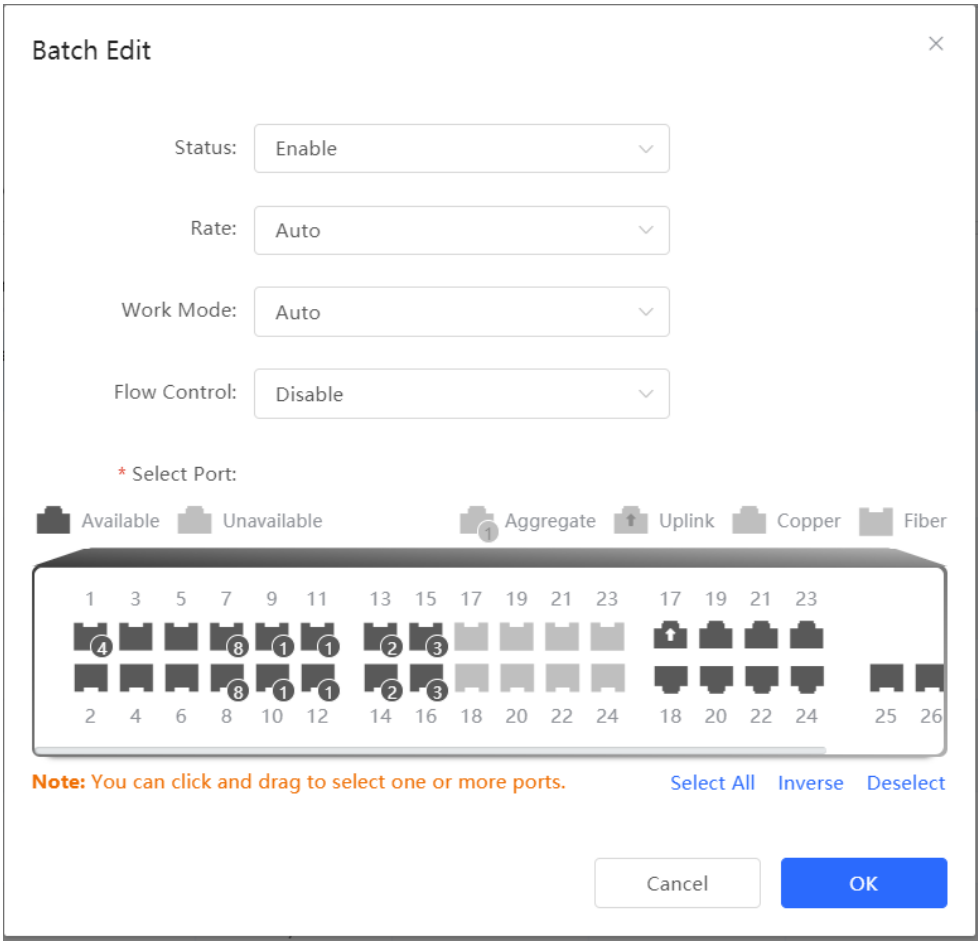
Choose **Local Device > Ports > Basic Settings > Basic Settings**.

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.

The screenshot shows the Ruijie iRcyc web interface. The top navigation bar includes links for Cloud Service, Alert Center, Wizard, English, and an Exit button. The left sidebar contains a search bar and a menu with options: Home, VLAN, Monitor, Ports (expanded), Port Settings (selected), Aggregate Ports, Port Mirroring, Rate Limiting, PoE, MGMT IP, L2 Multicast, L3 Multicast, L3 Interfaces, Routing, Security, Advanced, and Diagnostics. The main content area is titled 'Basic Settings' and 'Physical Settings'. A blue banner at the top of the main area says 'Configure port status, duplex mode, rate and flow control.' Below this is the 'Port List' section with a 'Batch Edit' button. The table below shows the configuration for 10 ports (Gi1/0/1 to Gi1/0/10). Each row has columns for Port, Status, Duplex Mode/Rate (Config Status and Actual Status), Flow Control (Config Status and Actual Status), and an Action button (Edit). The Status for all ports is 'Enable'. The Duplex Mode/Rate for Gi1/0/1 is 'Auto/Auto' and 'Full-Duplex/1000M', while for the others it is 'Auto/Auto' and 'Unknown/Unknown'. The Flow Control for all ports is 'Disable' for both Config and Actual Status. The bottom of the table shows 'Total 29' rows, with pagination controls for pages 1, 2, and 3, and a 'Go to page' field set to 1.

| Port | Status | Duplex Mode/Rate | | Flow Control | | Action |
|----------|--------|------------------|-------------------|---------------|---------------|--------|
| | | Config Status | Actual Status | Config Status | Actual Status | |
| Gi1/0/1 | Enable | Auto/Auto | Full-Duplex/1000M | Disable | Disable | Edit |
| Gi1/0/2 | Enable | Auto/Auto | Unknown/Unknown | Disable | Disable | Edit |
| Gi1/0/3 | Enable | Auto/Auto | Unknown/Unknown | Disable | Disable | Edit |
| Gi1/0/4 | Enable | Auto/Auto | Unknown/Unknown | Disable | Disable | Edit |
| Gi1/0/5 | Enable | Auto/Auto | Unknown/Unknown | Disable | Disable | Edit |
| Gi1/0/6 | Enable | Auto/Auto | Unknown/Unknown | Disable | Disable | Edit |
| Gi1/0/7 | Enable | Auto/Auto | Unknown/Unknown | Disable | Disable | Edit |
| Gi1/0/8 | Enable | Auto/Auto | Unknown/Unknown | Disable | Disable | Edit |
| Gi1/0/9 | Enable | Auto/Auto | Unknown/Unknown | Disable | Disable | Edit |
| Gi1/0/10 | Enable | Auto/Auto | Unknown/Unknown | Disable | Disable | Edit |

Batch configure: Click **Batch Edit**, select the port to be configured. In the displayed dialog box, select the port switch, rate, work mode, and flow control mode, and click **OK** to deliver the configuration. In batch configuration, optional configuration items are a common collection of selected ports (that is, attributes supported the selected ports).



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

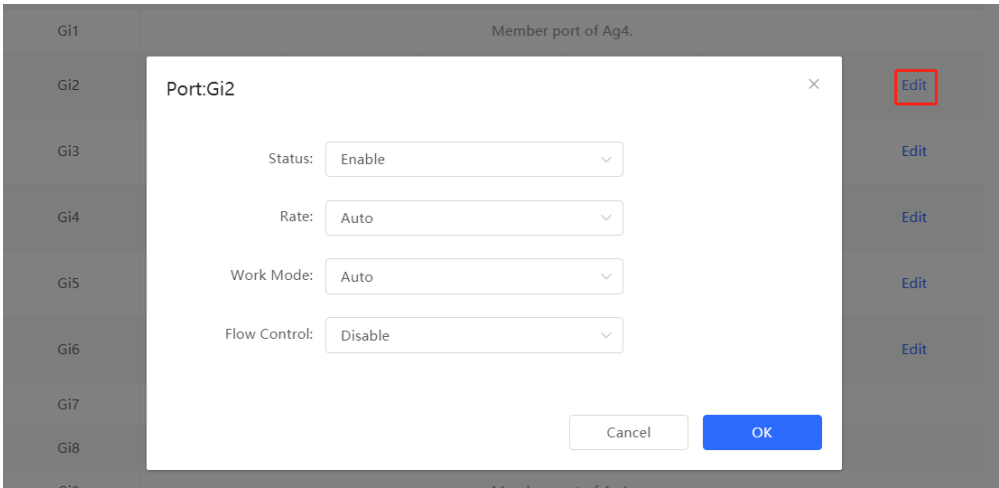


Table 7-2 Description of Basic Port Configuration Parameters

| Parameter | Description | Default Value |
|-----------|--|---------------|
| Status | If a port is closed, no frame will be received and sent on this port, and the corresponding data processing function will be | Enable |

| Parameter | Description | Default Value |
|--------------|---|---------------|
| | lost, but the PoE power supply function of the port will not be affected. | |
| Rate | Set the rate at which the Ethernet physical interface works. Set to Auto means that the port rate is determined by the auto-negotiation between the local and peer devices. The negotiated rate can be any rate within the port capability. | Auto |
| Work Mode | <ul style="list-style-type: none">● Full duplex: realize that the port can receive packets while sending.● Half duplex: control that the port can receive or send packets at a time.● Auto: the duplex mode of the port is determined through auto negotiation between the local port and peer port | Auto |
| Flow Control | After flow control is enabled, the port will process the received flow control frames, and send the flow control frames when congestion occurs on the port. | Disable |

Note

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

7.2.2 Physical Settings

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

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

Basic Settings **Physical Settings**

Configure physical attribute. (The fiber port does not support EEE. The aggregate port containing combo ports cannot work as a combo port.)

Port List [Batch Edit](#)

| Port | EEE | Attribute | Description | MTU | Action |
|----------|---------|-----------|-------------|------|----------------------|
| Gi1/0/1 | Disable | Copper | | 1500 | Edit |
| Gi1/0/2 | Disable | Copper | | 1500 | Edit |
| Gi1/0/3 | Disable | Copper | | 1500 | Edit |
| Gi1/0/4 | Disable | Copper | | 1500 | Edit |
| Gi1/0/5 | Disable | Copper | | 1500 | Edit |
| Gi1/0/6 | Disable | Copper | | 1500 | Edit |
| Gi1/0/7 | Disable | Copper | | 1500 | Edit |
| Gi1/0/8 | Disable | Copper | | 1500 | Edit |
| Gi1/0/9 | Disable | Copper | | 1500 | Edit |
| Gi1/0/10 | Disable | Copper | | 1500 | Edit |

Total 29 [1](#) [2](#) [3](#) > 10/page Go to page [1](#)

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

Note

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

Batch Edit

EEE:

Disable

Attribute:

Copper

Description:

* MTU:

1500

Range: 64-9216

* Select Port:

Available

Unavailable

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

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:Gi18

EEE:

Disable

Attribute:

Copper

Description:

* MTU:

1500

Range: 64-9216

Cancel

OK

Table 7-3 Description of Physical Configuration Parameters

| Parameter | Description | Default Value |
|-----------|--|---------------|
| EEE | It is short for energy-efficient Ethernet, which is based on the | Disable |

75

| Parameter | Description | Default Value |
|-------------|--|---------------------------------|
| | 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 | |
| Attribute | The port attribute indicates whether the port is a copper port or an SFP port. Copper 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. | N/A |
| MTU | MTU (Maximum Transmission Unit) 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. | 1500 |

 **Note**

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

7.3 Aggregate Ports

7.3.1 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 $\times n$.
- If two devices are connected through a single cable, when the link between the two interfaces is disconnected, services carried on this link are interrupted. After multiple interconnected interfaces are bound, as long as there is one link available, services carried on these interfaces will not be interrupted.

7.3.2 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. Automatic Aggregation

Automatic 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 automatic 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 an automatic aggregate port, and the corresponding two ports are the member ports of the aggregate port.

Note

- Automatic 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.
 - Only the RG-NBS3100, RG-NBS3200, and RG-NBS5000 series products support automatic aggregation, and the peer device for automatic aggregation must be RG-EG310G-E.
-

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

4. LACP

Link Aggregation Control Protocol (LACP) is a standardized protocol for dynamically aggregating multiple physical links into a single logical link to enhance network bandwidth and reliability. LACP defines the negotiation process and parameters of link aggregation, which enables the exchange of link aggregation information and the negotiation of link aggregation parameters among network devices and ensures the reliability and stability of the link aggregation. LACP supports dynamic addition and deletion of links, achieving dynamic link adjustment and optimization.

In LACP, two roles are defined: the actor and the partner. The actor sends a link aggregation request, while the partner responds to the request and joins the link aggregation group.

7.3.3 Aggregate Port Configuration

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

1. Adding an Aggregate Port

Enter an aggregate port ID, select member ports (ports that are already a member of an aggregate port cannot be selected), toggle on **LACP**, and click **Save**. You can enable **LACP** to dynamically aggregate links to enhance network reliability and flexibility. 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.
- The LACP state cannot be modified once a static aggregate port is created.

Aggregate Port Settings

Up to 16 aggregate ports can be added. An aggregate port contains up to 8 member ports.

No Data

* Aggregate Port: 1

LACP

* Select Member Ports

Available Unavailable Aggregate Uplink Copper Fiber

1 3 5 7

2 4 6 8 9 10

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.

Note

Dynamic aggregation ports do not support to modify member ports.

Aggregate Port Settings

Up to **16** aggregate ports can be added. An aggregate port contains up to **8** member ports.

☐ Select All

Ag1

Delete Selected

* Aggregate Port:

LACP ☐

* Select Member Ports

Available

Unavailable

Aggregate

Uplink

Copper

Fiber

1

3

5

7

2

4

6

8

9

10

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.

Caution

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

Aggregate Port Settings

Up to **16** aggregate ports can be added. An aggregate port contains up to **8** member ports.

☒ Select All

Ag1

Ag2

Ag3

Ag8

Ag4

Delete Selected

7.3.4 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

7.3.5 Configuring LACP Settings

1. LACP System Priority

>>>Choose **Local Device > Ports > Aggregate Port > LACP Settings > Global Settings**.

In LACP, the device with a higher system priority becomes the actor in the link aggregation group and controls the working state and parameters of the link aggregation group. The value of system priority ranges from 1 to 65535, and the default value is 32768. The lower the value of system priority, the higher the device priority. When two devices have the same system priority, their MAC addresses are compared, and the device with the smaller MAC address becomes the actor in the link aggregation group.

Aggregate Port Settings

LACP Settings

LACP Details

Global Settings

* LACP System Priority

32768

Save

2. LACP Port List

Choose **Local Device > Ports > Aggregate Port > LACP Settings > LACP Port List**. The **LACP Port List** page shows the port ID, priority, mode, and timeout mode of each LACP-enabled port. You can view the member port details of the corresponding link aggregation group by selecting an aggregate port.

LACP Port List

Select an aggregate port.

Search

Batch Edit

| <input type="checkbox"/> | Port | Aggregated Port | Priority | Mode | Timeout | Action |
|--------------------------|---------|-----------------|----------|--------|---------|----------------------|
| <input type="checkbox"/> | Mt1/0/3 | 1 | 1 | Active | Long | Edit |
| <input type="checkbox"/> | Mt1/0/5 | 1 | 1 | Active | Long | Edit |

<

1

>

10/page

Go to page

1

Total 2

You can select a specific port and click **Edit**, or select multiple ports and click **Batch Edit** to modify the port priority, mode, and timeout mode in the pop-up window. Then, click **OK** to confirm and apply the changes.

Edit

×

* Priority

Mode

Active

▼

Timeout

Long

▼

Table 7-4 Description of LACP Port List Configuration Parameters

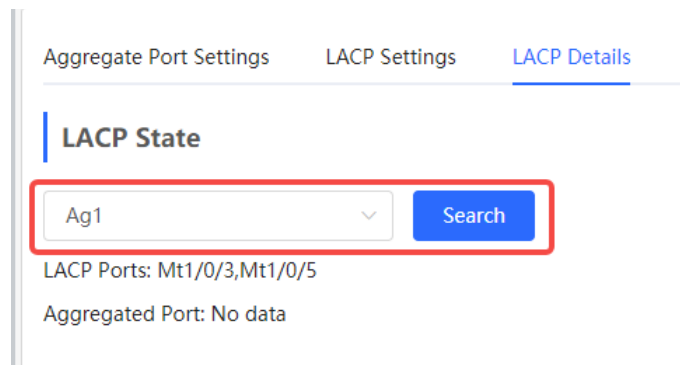
| Parameter | Description | Default Value |
|-----------|--|---------------|
| Priority | Priority is used to determine which port is the master, with the highest-priority port being selected as the active port. The priority value ranges from 1 to 65535, and a lower priority value indicates a higher priority. If multiple ports have the same priority, their priority ranking is determined by evaluating their port IDs, and the port with the lower port ID will be given a higher priority. | 32768 |
| Mode | Mode refers to the method by which two devices within a link aggregation group negotiate their operating mode. <ul style="list-style-type: none"> ● Active: In active mode, the device assumes the role of the actor and sends requests to establish link aggregation. ● Passive: In passive mode, the device assumes the role of the partner and waits for the peer device to send a request. | Active |

| Parameter | Description | Default Value |
|-----------|---|---------------|
| Timeout | <p>The purpose of the timeout mode is to determine the timeout period and mechanism for LACP link aggregation. When no LACP frames are received from the peer device within the specified timeout duration, it is assumed that the peer device has experienced a failure. As a result, the failure detection and recovery mechanism of the link aggregation is triggered.</p> <ul style="list-style-type: none"> ● Long: In long timeout mode, LACP frames are sent every 30 seconds, and the timeout duration is set to 90 seconds. This mode enhances the reliability and stability of link aggregation, but it can potentially lead to delayed detection of faults. ● Short: In short timeout mode, LACP frames are sent every second, and the timeout duration is set to 3 seconds. This mode enhances the response speed of link aggregation and ensures timely fault detection, but it may impose additional network load and resource consumption. | Long |

3. Viewing LACP State

Choose **Local Device** > **Ports** > **Aggregate Port** > **LACP Details**.

You can select an LACP-enabled aggregate port and click **Search** to view the LACP-enabled member ports and the aggregate port information on this page.



7.4 Port Mirroring

7.4.1 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 7-1 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.

7.4.2 Procedure

Choose **Local Device** > **Ports** > **Port Mirroring**.

Click **Edit**, select the source port, destination port, monitor direction, and whether to receive packets from non-source ports, and click **OK**. A maximum of four SPAN entries can be configured.

To delete the port mirroring configuration, click **Delete** in the corresponding **Action** column.

Caution

- You can select multiple source traffic monitoring ports but only one destination port. Moreover, the source traffic monitoring ports cannot contain the destination port.
- An aggregate port cannot be used as the destination port.
- A maximum of four SPAN entries can be configured. SPAN cannot be configured for ports that have been used for SPAN.

Description: All packets on the source port will be copied to the destination port and you can analyze the traffic by using a protocol analyzer application. Traffic on more than one source port can be mirrored to one destination port.
Note: The destination port must be different from the source port.

Port Mirroring List

| # | Src Port | Dest Port | Monitor Direction | Receive Pkt from Non-Src Ports | Action |
|---|----------|-----------|-------------------|--------------------------------|---|
| 1 | -- | -- | -- | -- | Edit Delete |
| 2 | -- | -- | -- | -- | Edit Delete |
| 3 | -- | -- | -- | -- | Edit Delete |
| 4 | -- | -- | -- | -- | Edit Delete |

Edit

Monitor Direction: Both

Receive Pkt from Non-Src

Ports:

* Src Port:

Available

Unavailable

Aggregate

Uplink

Copper

Fiber

1 3 5 7 9 11 13 15 17 19 21 23 17 19 21 23

4

8

1

1

2

3

8

1

1

2

3

18

20

22

24

25

26

2 4 6 8 10 12 14 16 18 20 22 24

Note: You can click and drag to select one or more ports.

Select All

Inverse

Deselect

* Dest Port:

Available

Unavailable

Uplink

Copper

Fiber

1 3 5 7 9 11 13 15 17 19 21 23 17 19 21 23

18

20

22

24

25

26

Deselect

Cancel

OK

Table 7-5 Description of Port Mirroring Parameters

| Parameter | Description | Default Value |
|-----------|--|---------------|
| Src Port | <p>A source port is also called a monitored port. Data flows on the source port are monitored for network analysis or troubleshooting.</p> <p>Support selecting multiple source ports and mirroring multiple ports to one destination port</p> | N/A |
| Dest Port | <p>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.</p> | N/A |

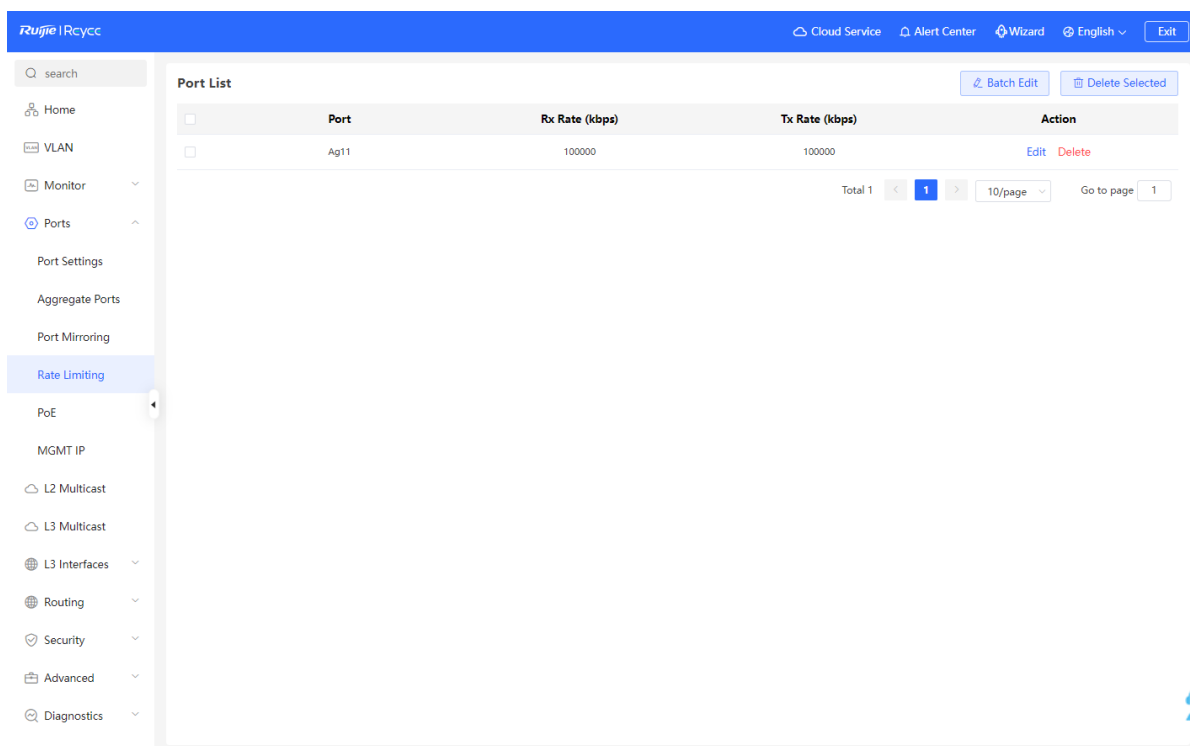
84

| Parameter | Description | Default Value |
|--------------------------------|---|---------------|
| Monitor Direction | <p>The type of packets (data flow direction) to be monitored by a source port.</p> <ul style="list-style-type: none"> Both: All packets passing through the port, including incoming and outgoing packets Incoming: All packets received by a source port are copied to the destination port Outgoing: All packets transmitted by a source port are copied to the destination port | Both |
| Receive Pkt from Non-Src Ports | <p>It is applied to the destination port and indicates whether a destination port forwards other packets while monitoring packets.</p> <ul style="list-style-type: none"> Enabled: While monitoring the packets of the source port, the packets of other non-source ports are normally forwarded Disabled: Only monitor source port packets | Enable |

7.5 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.



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: Range: 16-10000000kbps

Tx Rate: Range: 16-10000000kbps

* Select Port:

Available Unavailable Aggregate Uplink Copper Fiber

1 3 5 7 9 11 13 15 17 19 21 23 17 19 21 23

4 8 1 1 2 3 1 1 2 3 1 1 2 3 1 1 2 3 1 1 2 3 1 1 2 3

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 7-6 Description of Rate Limiting Parameters

| Parameter | Description | Default Value |
|-----------|---|---------------|
| Rx Rate | Max Rate at which packets are sent from a port to a switch, in kbps. | Not limited |
| Tx Rate | Max Rate at which packets are sent out of a switch through a port, in kbps. | Not limited |

2. Changing Rate Limits of a Single Port

In the port list for which the rate limit has been set, click **Edit** on the corresponding port entry, enter the ingress rate and egress rate in the displayed dialog box, and click **OK**.

Port:Gi23

Rx Rate:

10000

Range: 16-1000000kbps

Tx Rate:

10000

Range: 16-1000000kbps

Cancel

OK

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 |
| <input checked="" type="checkbox"/> | Gi23 | 10000 | 10000 | Edit Delete |

Note

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

7.6 MGMT IP Configuration

Choose **Local Device** > **Ports** > **MGMT IP**.

The **MGMT IP** page allows you to configure the management IP address for the device. Users can configure and manage the device by accessing the management IP.

The 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.

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 [5.2](#)).
- You are advised to bind a configured management VLAN to an uplink port. Otherwise, you may fail to access the web interface.

7.7 Configuring the Management IPv6 Address

Configure the IPv6 address used to log in to the device management page.

Choose **Local Device > Ports > MGMT IP > 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**.

The screenshot shows the Ruijie iReycs web interface. The left sidebar has a search bar and various navigation icons. The main area is for 'MGMT IP' configuration, specifically the 'MGMT IPv6' tab. It features a dropdown for 'Internet' set to 'Null', a dropdown for 'IPv6 Address' with 'DHCP' selected, a dropdown for 'IPv6 Prefix' with 'Static IP' selected, a text field for 'Gateway' set to 'Null', and a text field for 'DNS Server'. A blue 'Save' button is located at the bottom of the configuration area.

7.8 Out-of-Band IP Configuration

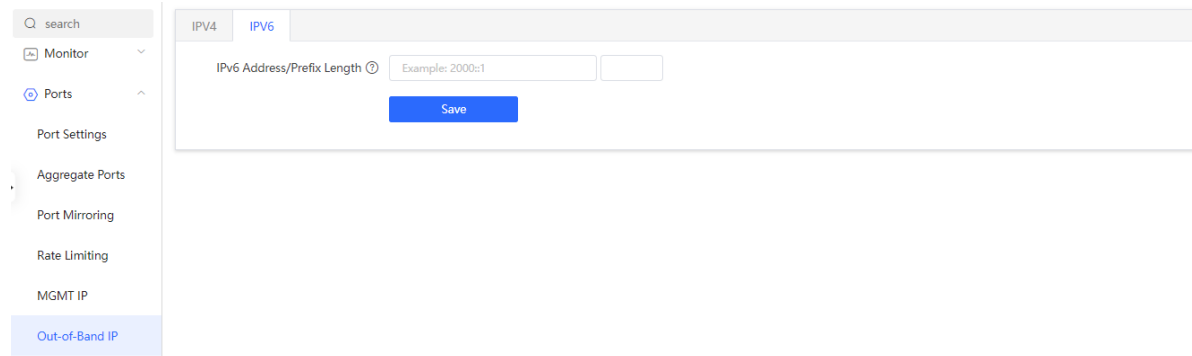
Caution

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.

The screenshot shows the 'Out-of-Band IP' configuration page in the Ruijie iReycs web interface. The left sidebar is consistent with the previous image. The main area has tabs for 'IPv4' and 'IPv6'. The 'IPv4' tab is selected, displaying input fields for 'IP Address' (with the example '1.1.1.1') and 'Subnet Mask' (with the example '255.255.255.0'). A blue 'Save' button is positioned below these fields.



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.

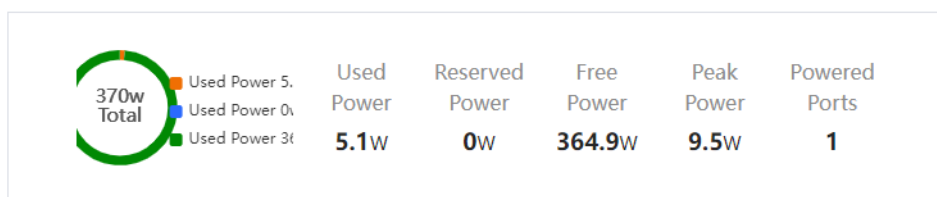
7.9 PoE Configuration

Caution

Only PoE switches (model name containing -P, -LP, -HP, and -UP) 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.

PoE Overview**PoE Settings**

Power Mode: ? Energy Saving ▼

* Reserved Power: Range: 0-50%

PoE watchdog: ☐

[Save](#)

Port List[Refresh](#)[Batch Edit](#)

| | Port | PoE Status | Power Status | Priority | Current 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 |

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



Table 7-7 PoE Watchdog Configuration Description

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

Note

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

PoE Settings

Power Mode:  Energy Saving 

* Reserved Power: Range: 0-50%

PoE watchdog: ☒

* Ping Interval: Range: 90-1800s

Save

7.9.2 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 List | | | | | | | | |
|-----------|------|------------|-----------------------|----------|----------------------------|--------------|-------------------------|------------------------------|
| | | | | | | | 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:

Non-Standard:

Priority:

Max Transmit Power:

Range: 0-30W

Cancel

OK

Table 7-8 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 | <p>The power supply priority of the port is divided into three levels: High, Medium, and Low</p> <p>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.</p> <p>Ports with the same priority are sorted by the port number. A smaller port number indicates a higher priority.</p> | 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 |

7.9.3 Displaying Global PoE Information

Choose **Local Device > Ports > PoE > PoE Overview**.

Displays the global power supply information of the PoE function, including the total system power, used power, reserved power, remaining available power, peak maximum power, and the number of ports currently powered.

PoE Overview

| | | | |
|-------------------------------------|----------------------------------|--------------------------------------|------------------------------------|
| Total Transmit Power 370W | Used Transmit Power 0W | Reserved Transmit Power 0W | Free Transmit Power 370W |
| Peak Transmit Power 0W | Powered Ports 0 | | |

7.9.4 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

[Refresh](#)
[Batch Edit](#)

| | Port | PoE Status | Transmit Power Status | Priority | Current Transmit Power (W) | Non-Standard | Work Status | Action |
|---|------|------------|-----------------------|----------|----------------------------|--------------|-----------------|--|
| <input checked="" type="checkbox"/> | Gi1 | Enable | Off | Low | 0 | No | PD Disconnected | Edit Repower |
| Current: 0mA Max Transmit Power: No Limit PD Type: Failed to fetch the PD type. Voltage: 0V PD Requested Transmit Power: 0W PD Class: NA Avg Transmit Power: 0W PSE Allocated Transmit Power: 0W | | | | | | | | |
| > | Gi2 | Enable | Off | Low | 0 | No | PD Disconnected | Edit Repower |
| > | Gi3 | Enable | Off | Low | 0 | No | PD Disconnected | Edit Repower |

Table 7-9 Description of Port Power Supply Info

| 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. |

| Field | Description |
|------------------------------|--|
| Priority | The power supply priority of the port is divided into three levels: High, Medium, and Low. |
| 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). |
| PD Type | 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. |

8 L2 Multicast

8.1 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.

8.2 Multicast Global Settings

Choose **Local Device > Multicast > Global Settings**.

Global Settings allow you to specify the version of the IGMP protocol, whether to enable report packet suppression, and the behavior for processing unknown multicast packets.

[Global Settings](#)
[IGMP Snooping](#)
[MVR](#)
[Multicast Group](#)
[IGMP Filter](#)
[Querier](#)

 **Global Settings**

Version

IGMP Report Suppression ☐

Unknown Multicast Pkt

Save

Table 8-1 Description of Configuration Parameters of Global Multicast

| Parameter | Description | Default Value |
|-----------|---|---------------|
| Version | <p>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, and IGMPv3.</p> <p>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.</p> | IGMPv2 |

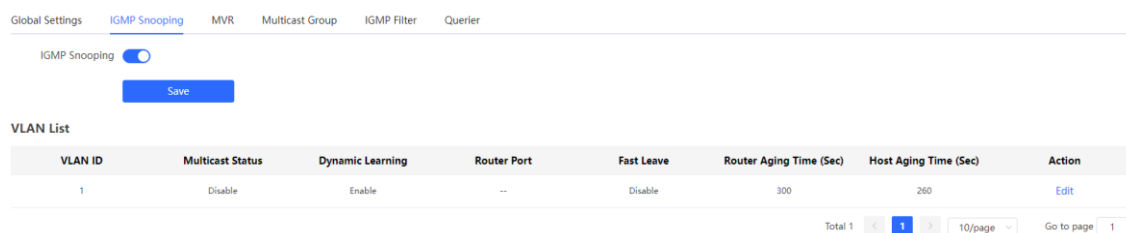
| Parameter | Description | Default Value |
|-------------------------|---|---------------|
| IGMP Report Suppression | After this function is enabled, to reduce the number of packets on the network, save network bandwidth and ensure the performance of the IGMP multicast device, the switch forwards only 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 |

8.3 IGMP Snooping

8.3.1 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, a 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.




8.3.2 Enabling Global IGMP Snooping

Choose **Local Device > Multicast > IGMP Snooping**.

Turn on **IGMP Snooping** and click **Save**.

Global Settings IGMP Snooping MVR Multicast Group IGMP Filter Querier

IGMP Snooping

IGMP Snooping 

Save

8.3.3 Configuring Protocol Packet Processing Parameters

By controlling protocol packet processing, an L2 multicast device can establish static or dynamic multicast forwarding entries. In addition, the device can adjust parameters to refresh dynamic multicast forwarding entries and IGMP snooping membership quickly.

Choose **Local Device** > **Multicast** > **IGMP Snooping**.

The IGMP Snooping function is implemented based on VLANs. Therefore, each VLAN corresponds to an IGMP Snooping setting entry. There are as many IGMP Snooping entries as VLANs on the device.

Click **Edit** in the VLAN entry. In the displayed dialog box enable/disable the VLAN multicast function, dynamic learning function, fast leave function and static route connection port, and set the router aging time and the host aging time, and click **OK**.

VLAN List

| VLAN ID | Multicast Status | Dynamic Learning | Router Port | Fast Leave | Router Aging Time (Sec) | Host Aging Time (Sec) | Action |
|---------|------------------|------------------|-------------|------------|-------------------------|-----------------------|----------------------|
| 1 | Disable | Enable | -- | Disable | 300 | 260 | Edit |
| 10 | Disable | Enable | -- | Disable | 300 | 260 | Edit |
| 20 | Disable | Enable | -- | Disable | 300 | 260 | Edit |

Edit

* VLAN ID
1

Multicast Status

Dynamic Learning

Fast Leave

* Router Aging Time (Sec)
300

* Host Aging Time (Sec)
260

Select Port:

Available
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 select one or more ports.
Select All
Inverse
Deselect

Cancel
OK

Table 8-2 Description of VLAN Configuration Parameters of IGMP Snooping

| Parameter | Description | Default Value |
|------------------|---|---------------|
| Multicast Status | Whether to enable or disable the VLAN multicast function. The multicast function of a VLAN takes effect only when both the global IGMP snooping and VLAN multicast functions are enabled. | Disable |
| Dynamic Learning | The device running IGMP Snooping identifies the ports in the VLAN as router ports or member ports. The router port is the port on the Layer 2 multicast device that is connected to the Layer 3 multicast device, and the member port is the host port connected to the group on the Layer 2 multicast device. By snooping IGMP packets, the L2 multicast device can automatically discover and maintain dynamic multicast router ports. | Enable |
| Router Port | List of current multicast router ports includes dynamically learned routed ports (if Dynamic Learning function is enabled) and statically configured routed ports. | N/A |

| Parameter | Description | Default Value |
|-------------------------|--|---------------|
| Fast Leave | After it is enabled, when the port receives the Leave packets, it will immediately delete the port from the multicast group without waiting for the aging timeout. After that, when the device receives the corresponding specific group query packets and multicast data packets, the device will no longer forward it to the port. This function is applicable when only one host is connected to one port of the device, and is generally enabled on the access switch directly connected to the endpoint. | Disable |
| Router Aging Time (Sec) | Aging time of dynamically learned multicast router ports ranges from 30 to 3600, in seconds. | 300 seconds |
| Host Aging Time (Sec) | Aging time of dynamically learned member ports of a multicast group, in seconds. | 260 seconds |
| Select Port | In the displayed dialog box, select a port and set it as the static router port. When a port is configured as a static router port, the port will not age out | N/A |

8.4 Configuring MVR

8.4.1 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
Multicast Group
IGMP Filter
Querier

MVR
The source port must be a MVR VLAN member and the receiver port cannot be a MVR VLAN member. Fast Leave settings only take effect on the destination port.

MVR ☐

Save

Port List
[Batch Edit](#)

| Port | Role | Fast Leave |
|------|------|--------------------------|
| Gi1 | NONE | <input type="checkbox"/> |
| Gi2 | NONE | <input type="checkbox"/> |
| Gi3 | NONE | <input type="checkbox"/> |

8.4.2 Configuring Global MVR Parameters

Choose **Local Device > L2 Multicast > MVR**.

Click to enable the MVR, select the MVR VLAN, set the multicast group supported by the VLAN, and click **Save**. Multiple multicast groups can be specified by entering the start and end multicast IP addresses.

Global Settings
IGMP Snooping
MVR
Multicast Group
IGMP Filter
Querier

MVR
i The source port must be a MVR VLAN member and the receiver port cannot be a MVR VLAN member. Fast Leave settings only take effect on the destination port.

MVR ☒

* Multicast VLAN

* Start IP Address ?

* End IP Address ?

Save

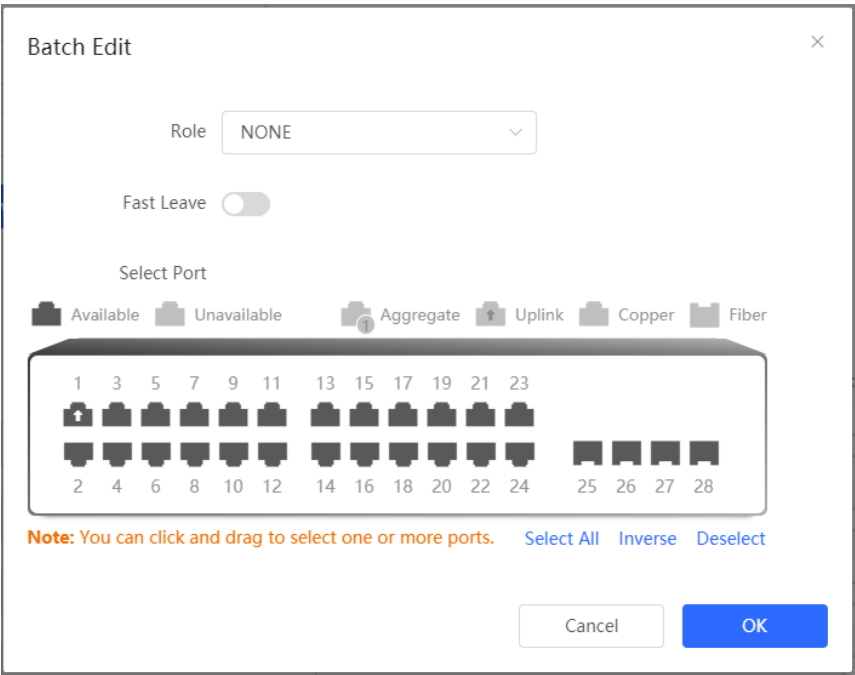
Table 8-3 Description of Configuring Global MVR Parameters

| 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. | N/A |
| End IP Address | Learned or configured end multicast IP address of an MVR multicast group. | N/A |

8.4.3 Configuring the MVR Ports

Choose **Local Device > L2 Multicast > MVR**.

Batch configure: Click **Batch Edit**, select the port role, the port to be set, and whether to enable the Fast Leave function on the port, and click **OK**.



Configure one port: Click the drop-down list box to select the MVR role type of the port. Click the switch in the **Fast Leave** column to set whether the port enables the fast leave function.

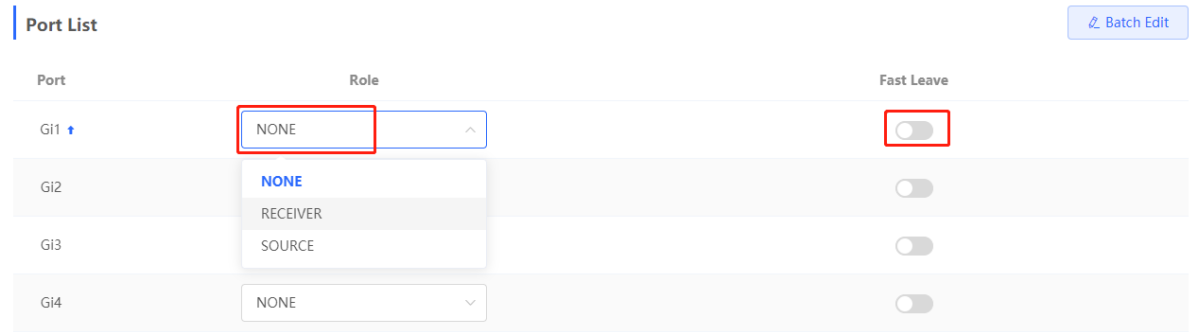


Table 8-4 Description of MVR Configuration Parameters of Ports

| Parameter | Description | Default Value |
|------------|--|---------------|
| Role | NONE: Indicates that the MVR function is disabled. SOURCE: Indicates the source port that receives multicast data streams. RECEIVER: Indicates the receiver port connected to a client. | NONE |
| Fast Leave | Configures the fast leave function for a port. After the function is enabled, if the port receives the leave packet, it is directly deleted from the multicast group. | Disable |

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.

8.5 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

Multicast Group
The static multicast group will not learn dynamic ports.

Multicast List VLAN ID

Up to **256** entries can be added.

| <input type="checkbox"/> | VLAN ID | Multicast IP Address | Protocol | Type | Forwarding Port | Action |
|--------------------------|---------|----------------------|---------------|--------|-----------------|---|
| <input type="checkbox"/> | 20 | 224.10.10.10 | IGMP Snooping | Static | Gi28 | Edit Delete |



Add ×


* Multicast IP Address

* VLAN ID

Forwarding 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 select one or more ports. [Select All](#) [Inverse](#) [Deselect](#)

Table 8-5 Description of Multicast Group Configuration Parameters

| Parameter | Description | Default Value |
|-----------|---|---------------|
| VLAN ID | VLAN, to which received multicast traffic belongs | N/A |

| Parameter | Description | Default Value |
|----------------------|--|---------------|
| Multicast IP Address | On-demand multicast IP address | N/A |
| 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. | N/A |
| Type | Multicast group generation mode can be statically configured or dynamically learned. In normal cases, a port can join a multicast group only after the port receives an IGMP Report packet from the multicast, that is, dynamically learned mode. If you manually add a port to a group, the port can be statically added to the group and exchanges multicast group information with the PIM router without IGMP packet exchange. | N/A |
| Forwarding Port | List of ports that forward multicast traffic | N/A |

Note

Static multicast groups cannot learn other dynamic forwarding ports.

8.6 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 Multicast Group **IGMP Filter** Querier

IGMP Filter

Profile List [+ Add](#) [Delete Selected](#)

| Profile ID | Behavior | Start IP Address | End IP Address | Action |
|------------|----------|------------------|----------------|--------|
| No Data | | | | |

Total 0 10/page < 1 > Go to page 1

Filter List [Batch Edit](#)

| Port | Profile ID | Max Multicast Groups | Action |
|-------|------------|----------------------|----------------------|
| Gi1 ↑ | -- | 256 | Edit |
| Gi2 | -- | 256 | Edit |
| Gi3 | -- | 256 | Edit |

8.6.1 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

?

* End IP Address

?

Cancel

OK

Table 8-6 Description of Profile Configuration Parameters

| Parameter | Description | Default Value |
|------------|-------------|---------------|
| Profile ID | Profile ID | N/A |

| Parameter | Description | Default Value |
|------------------|--|---------------|
| Behavior | DENY: Forbids demanding multicast IP addresses in a specified range. PERMIT: Only allows demanding multicast IP addresses in a specified range. | N/A |
| Start IP Address | Start Multicast IP address of the range of multicast group addresses | N/A |
| End IP Address | End Multicast IP address of the range of multicast group addresses | N/A |

8.6.2 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 |

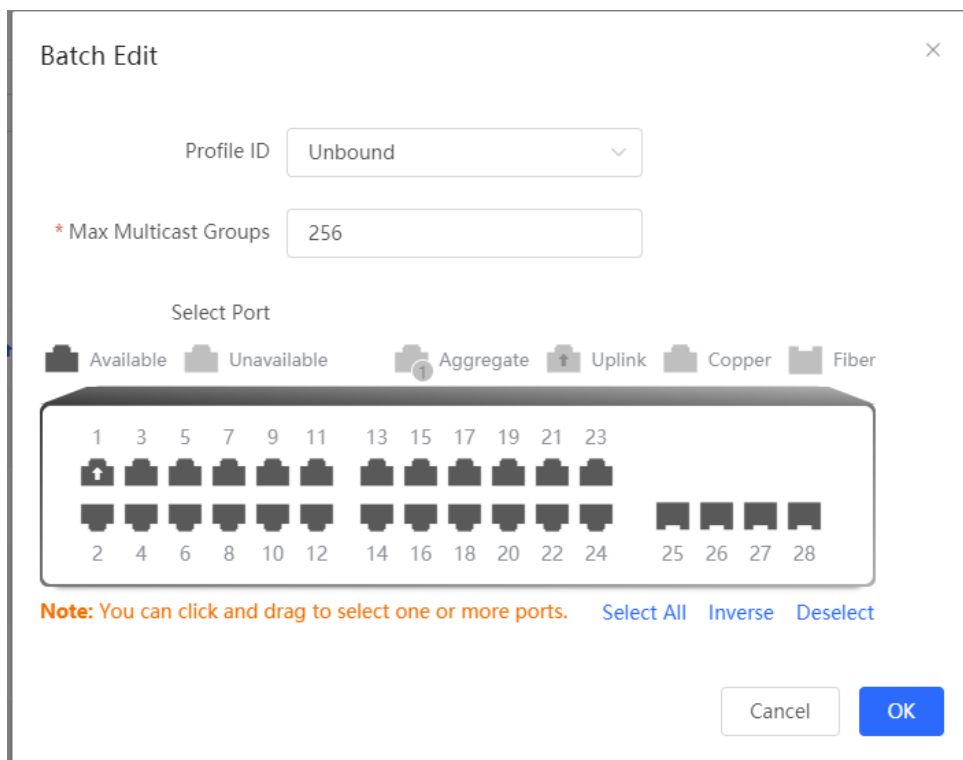


Table 8-7 Description of Port Filter Configuration Parameters

| Parameter | Description | Default Value |
|----------------------|--|---------------|
| Profile ID | Profile that takes effect on a port. If it is not set, no profile rule is bound to the port. | N/A |
| 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 |

8.7 Setting an IGMP Querier

8.7.1 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.

8.7.2 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 **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

Querier

 The querier version cannot be higher than the global version. When the global version is lowered, the querier version will be reduced accordingly.
If the querier source IP is not configured, the device management IP is used.

Querier List

| VLAN ID | Querier Status | Version | Src IP Address | Query Interval (Sec) | Action |
|---------|----------------|---------|----------------|----------------------|--|
| 1 | Disable | IGMPv2 | | 60 | Edit |
| 10 | Disable | IGMPv2 | | 60 | Edit |
| 20 | Disable | IGMPv2 | | 60 | Edit |

Edit
×

* VLAN ID

Querier Status ☐

Version

Src IP Address

Query Interval (Sec)

Table 8-8 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. | N/A |

| Parameter | Description | Default Value |
|-------------------------|---|---------------|
| Query Interval (Sec) | Packet transmission interval, of which the value range is from 30 to 18000, in seconds. | 60 seconds |

**Note**

- The querier version cannot be higher than the global IGMP version. When the global IGMP version is lowered, the querier version is lowered accordingly.
- If no querier source IP is configured, the device management IP is used as the source IP address of the querier.

9 L3 Multicast

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.

9.1 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.

9.2 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.

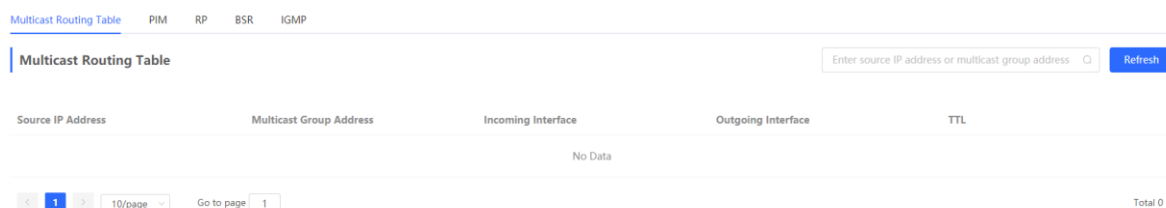


Table 9-1 Description of Multicast Routing Table Parameters

| 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 |

| Parameter | Description | Default Value |
|--------------------|---|---------------|
| 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 |
| 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 |

9.3 Configuring PIM

Caution

The current product does not yet support PIM-DM. PIM-SM is exclusively supported by the NBS5100, NBS5200, NBS5300, NBS6000, and NBS7000 series of switches.

9.3.1 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.

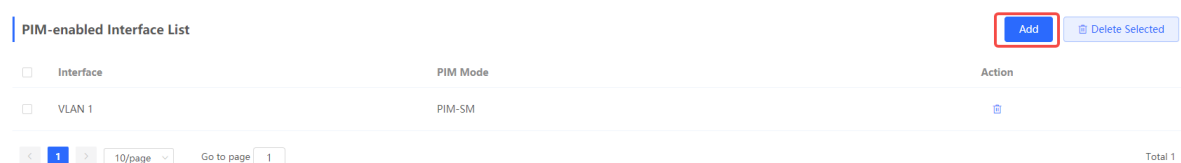
The PIM protocol features two widely used modes:


- **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.

9.3.2 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 PIM mode is PIM-SM by default.



| Interface | PIM Mode | Action |
|-----------|----------|---|
| VLAN 1 | PIM-SM |  |

1 10/page Go to page 1 Total 1

Select Interfaces



Select



Cancel

OK

9.3.3 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

| Interface | PIM Neighbor | TTL | Aging Time |
|-----------|--------------|-----|------------|
| No Data | | | |

< 1 > 10/page Go to page 1 Total 0

Table 9-2 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 |

9.4 Configuring RP

9.4.1 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.

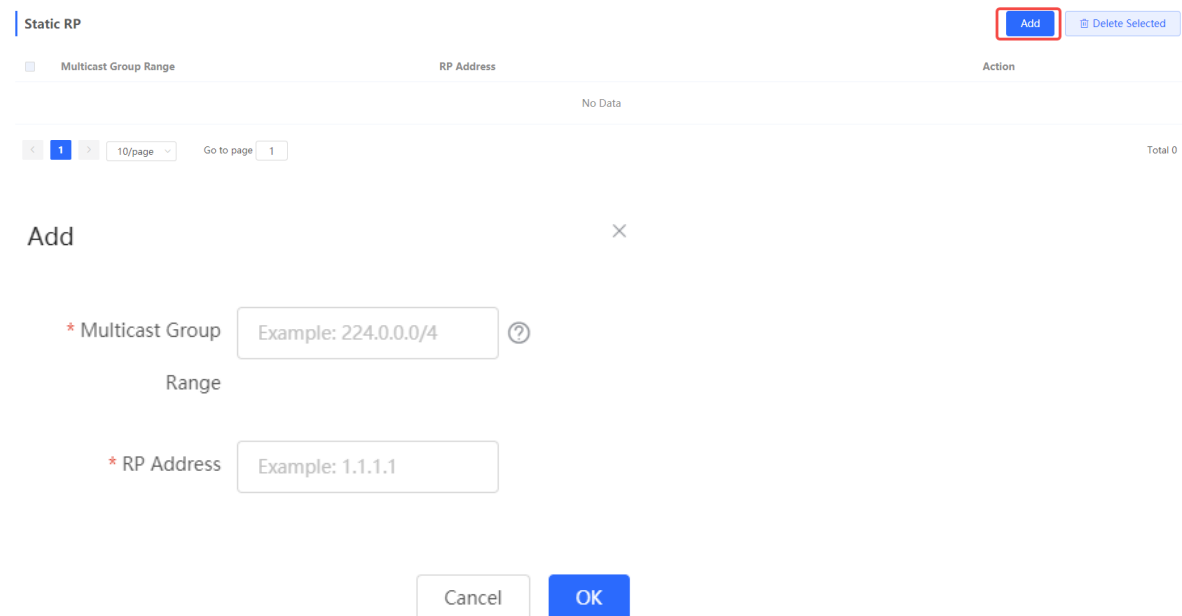
Note

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.

9.4.2 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**.



9.4.3 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: (0-255. A lower value indicates a higher priority.)Advertisement interval: s* Source IP Address ?Designated multicast group ?

Table 9-3 Description of Candidate RP Configuration Parameters

| 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 |

9.5 Configuring BSR

9.5.1 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.

9.5.2 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 BSR:

Local routing device as candidate BSR: ☒

Priority: (0-255. A higher value indicates a higher priority.)

* Source IP Address 

Save


Table 9-4 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 |

9.5.3 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  | | | | |
|--|----------|------------|-----------------|------------|
| BSR address | Priority | Status | Online Duration | Aging Time |
| 0.0.0.0 | 0 | ACCEPT_ANY | 00:00:00 | --:--:-- |

9.6 Configuring IGMP

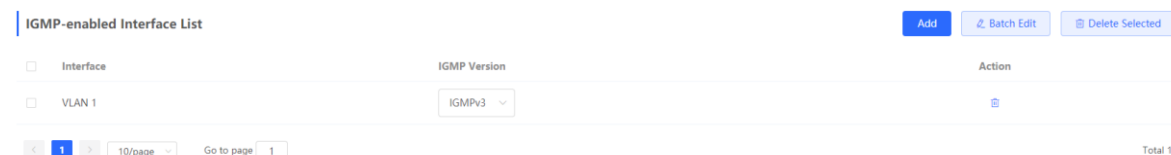
9.6.1 Overview

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.

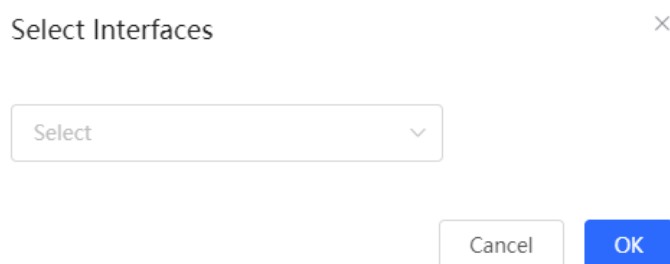
9.6.2 Enabling IGMP

>>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.

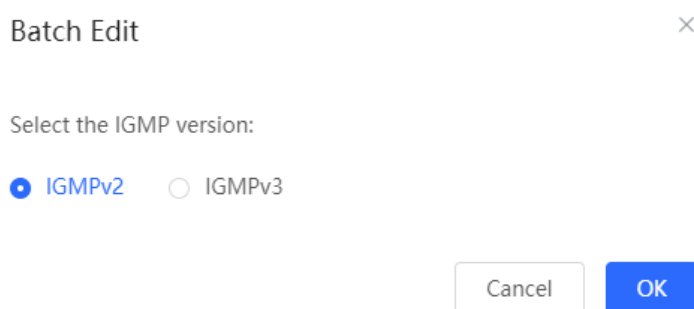


Add: Click **Add**. The **Select Interfaces** pop-up window is displayed. On the pop-up window, select an interface on which IGMP will be enabled. Then, Click **OK**. IGMP is enabled on the corresponding VLAN.



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

9.6.3 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 | <div><div></div></div> | 239.255.255.250 * | 00:52:34 | 00:02:20 |

< 1 >

10/page

Go to page 1

Total 1

10 L3 Management

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.

10.1 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.

Port List

+ Add L3 Interface

After the IPv4 address is set to Dynamic IP, the IPv6 address will not take effect if the interface does not obtain an IPv4 address.
Up to 64 layer-3 interfaces and 64 IPv4 addresses can be configured.

| L3 Interfaces | Port Type | Networking | IP Address | Subnet Mask | DHCP Server | DHCP Server Info | Action |
|---------------|-----------------|------------|--------------------|---------------|-------------|------------------|---|
| VLAN1 | Management VLAN | DHCP | 192.168.110.6 2 | 255.255.255.0 | Disabled | -- | Edit Delete |
| Gi2/14 | Routed Port | Static IP | 12.12.12.12 | 255.255.255.0 | Disabled | -- | Edit Delete |

< 1 >

10/page

Go to page 1

Total 2

Add

×

Port Type

SVI

Networking

Static IP

Primary IP/Mask

192.168.1.1

255.255.255.0

Add + ?

VLAN

Select

DHCP Mode

☒ Disabled

☐ DHCP Server

☐ DHCP Relay

Cancel

OK

Table 10-1 Description of Configuration Parameters of L3 Interfaces

| Parameter | Description |
|-----------------------------|---|
| Port Type | The type of a created L3 interface. It can be an SVI, routed port, or L3 aggregate port. For details, see Table 7-1 . |
| Networking | Specifies DHCP or static mode for a port to obtain the IP address. |
| VLAN | Specifies the VLAN, to which an SVI belongs. |
| IP/Mask | When Networking is set to Static IP , you need to manually enter the IP address and subnet mask. |
| Select Port | Select the device port to be configured. |
| Aggregate | Specifies the aggregate port ID, for example, Ag1, when an L3 aggregate port is created. |
| DHCP Mode | <p>Select whether to enable the DHCP service on the L3 interface.</p> <p>Disabled: Indicates that the DHCP service is disabled. No IP address can be assigned to clients connected to the interface.</p> <p>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 10.2 Configuring the IPv6 Address for the L3 Interface.</p> <p>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.</p> |
| Excluded IP Address (Range) | When the device acts as a DHCP server, set the IP address in the address pool that is not used for assignment |

Note

- VLAN 1 is the default SVI of the device. It can be neither modified nor deleted.
- The management VLAN is only displayed on the **L3 Interfaces** page but cannot be modified. To modify it, choose **Ports > MGMT IP**. For details, see [7.6 MGMT IP Configuration](#).
- 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.

10.2 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**.

IPv6 Config DHCPv6 Server DHCPv6 Clients Static DHCPv6 IPv6 Neighbor List

Port List [+ Add L3 Interface](#)

After the IPv4 address is set to Dynamic IP, the IPv6 address will not take effect if the interface does not obtain an IPv4 address.

| L3 Interfaces | Port Type | Networking | IPv6 Address/Prefix Length | Action |
|---------------|-----------------|------------|----------------------------|--|
| VLAN1 | Management VLAN | | | Edit |
| Gi2/14 | Routed Port | Static IP | | Edit Clear |

< 1 > 10/page Go to page 1 Total 2

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**.

Diagn Edit

Auto Obtained IP ☒ Obtain an IPv6 address via DHCPv6.

MTU (1280-1500)

Cancel OK

VLAN1 Management VLAN Edit

Gi2/14 Routed Port Static IP Edit Clear

< 1 > 10/page Go to page 1 Total 2

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

Diagn Edit

Auto Obtained IP ☐ Obtain an IPv6 address via DHCPv6.

IPv6 Address/Prefix Length 64 Manual Add + ?

MTU (1280-1500)

Advanced Settings

Link-local Address ?

Subnet Prefix Name ?

Subnet Prefix Length ?

Subnet ID ?

Cancel OK

VLAN1 Management VLAN Edit

Gi2/14 Routed Port Static IP Edit Clear

< 1 > 10/page Go to page 1 Total 2

Table 10-2 IPv6 Address Configuration Parameters of the L3 Interface

| Parameter | Description |
|-----------------------------------|--|
| Obtain an IPv6 address via DHCPv6 | If no upstream DHCPv6 server is available, do not select Auto Obtained IP . Instead, manually add the IPv6 address. |
| IPv6 Address/Prefix | Configure the IPv6 address and prefix length. You can click Add to add multiple |

| Parameter | Description |
|----------------------|--|
| Length | IPv6 addresses. If the primary IP address is empty, the configured secondary IP address is invalid. For manual configuration, the prefix length ranges from 1 to 128. For auto configuration, the prefix length ranges from 1 to 64. If the IPv6 prefix length of the L3 interface is between 48 and 64, this address can be assigned. |
| MTU | Configure the MTU. The default MTU is 1500 . |
| Advanced Settings | Click Advanced Settings to configure the link local address, subnet prefix name, subnet prefix length, and subnet ID. |
| Link-local Address | The link local address is used to number hosts on a single network link. The first 10 bits of link address in binary notation must be '1111111010'. |
| Subnet Prefix Name | It identifies a specified link (subnet). |
| Subnet Prefix Length | It indicates the length (in bits) of the subnet prefix in the address. The value ranges from 48 to 64 (The subnet prefix length must be greater than the length of the prefix assigned by the server). |
| Subnet ID | Configure the subnet ID of the interface in hexadecimal notation. The number of available subnet IDs is $(2^N - 1)$, where N is equal to (Subnet prefix length of the interface - Length of the prefix assigned by the server). |

10.3 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.

10.3.1 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.

| | | | | | |
|-------------------------------|------------------------------|-------------------------------------|-----------------------------|--------------------------------|--------------------------|
| L3 Interfaces | DHCP Clients | Static IP Addresses | DHCP Option | Static Routing | ARP List |
|-------------------------------|------------------------------|-------------------------------------|-----------------------------|--------------------------------|--------------------------|

Port List
[+ Add L3 Interface](#)

Up to **16** layer-3 interfaces and **32** IPv4 addresses can be configured.

| L3 Interfaces | Port Type | Networking | IP | Subnet Mask | DHCP Server | DHCP Server Info | Action |
|---------------|-----------------|------------|----------------|---------------|-------------|------------------------------|---|
| VLAN1 | Management VLAN | DHCP | 172.30.102.133 | 255.255.255.0 | Disabled | -- | Edit Delete |
| Gi9 | Routed Port | Static IP | 1.1.1.1 | 255.255.255.0 | DHCP Server | View Details | Edit Delete |

Edit

Port Type

Routed Port

Networking

Static IP

* Primary IP/Mask

1.1.1.1

255.255.255.0

Add + ?

DHCP Mode

☐ Disabled
 ☒ DHCP Server
 ☐ DHCP Relay

* Start

1.1.1.1

* IP Count

254

Available IP Addresses: 244. End IP Address: 1.1.1.254.

Excluded IP Address

1.1.1.1-1.1.1.10

Add + ?

(Range).

* Lease Time(Min)

100

Cancel

OK

Table 10-3 Description of DHCP Server Configuration Parameters

| Parameter | Description |
|-----------------------------|--|
| DHCP Mode | To choose DHCP server |
| Start | The DHCP server assigns the Start IP address automatically, which is the Start IP address of the DHCP address pool. A client obtains an IP address from the address pool. If all the addresses in the address pool are used up, no IP address can be obtained from the address pool. |
| IP Count | The number of IP addresses in the address pool |
| Excluded IP Address (Range) | IP addresses in the address pool that are not used for allocation, support |

| Parameter | Description |
|-----------------|---|
| | 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 |

10.3.2 Viewing the DHCP Client

Choose **Local Device > L3 Interfaces > 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 [10.3.3](#).

L3 Interfaces
DHCP Clients
Static IP Addresses
DHCP Option
Static Routing
ARP List

i View DHCP clients.

DHCP Clients
Search by Hostname/IP/MAC
Refresh
+ Batch Convert

Up to 1000 IP-MAC bindings can be added.

| <input type="checkbox"/> | No. | Hostname | IP | MAC | Remaining Lease Time(min) | Status |
|--------------------------|-----|----------|----|-----|---------------------------|--------|
| No Data | | | | | | |

10.3.3 Configuring Static IP Addresses Allocation

Choose **Local Device > L3 Interfaces > 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

L3 Interfaces DHCP Clients **Static IP Addresses** DHCP Option Static Routing ARP List

Static IP Address List ⓘ

Static IP Address List Search by IP/MAC Q + Add Delete Selected

Up to **1000** entries can be added.

| <input type="checkbox"/> | No. | IP | MAC | Action |
|--------------------------|-----|-----------|-------------------|---|
| <input type="checkbox"/> | 1 | 1.1.1.200 | 00:11:22:33:44:55 | Edit Delete |

Click **Add**. In the displayed static IP address binding dialog box, enter the MAC address and IP address of the client to be bound, and click **OK**. After a static IP address is bound, the bound IP address will be obtained each time the corresponding downlink client connects to the network.

Add

* IP

Example: 1.1.1.1

* MAC

Example: 00:11:22:33:44:55

Cancel

OK

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 **Action** column of the corresponding entry.

10.3.4 Configuring the DHCP Server Options

Choose **Local Device** > **L3 Interfaces** > **DHCP Option**.

The configuration delivered to the downlink devices is optional and takes effect globally when the L3 interface serves as the DHCP server.

L3 Interfaces
DHCP Clients
Static IP Addresses
DHCP Option
Static Routing
ARP List

DHCP Option
DHCP option settings are applied to all LAN ports.

DNS Server

Option 43

?

Option 138

Option 150

Save

Table 10-4 Description of the DHCP Server Options Configuration Parameters

| Parameter | Description |
|------------|--|
| DNS Server | DNS server address provided by an ISP. Multiple IP addresses can be entered and separated by spaces. |
| Option 43 | When the AC (wireless controller) and the AP are not in the same LAN, the AP cannot discover the AC through broadcast after obtaining an IP address from the DHCP server. To enable the AP to discover the AC, you need to configure Option 43 carried in the DHCP response packet on the DHCP server. |
| Option 138 | Enter the IP address of the AC. Similar to Option 43, when the AC and AP are not in the same LAN, you can configure Option 138 to enable the AP to obtain the IPv4 address of the AC. |
| Option 150 | Enter the IP address of the TFTP server. Enter the IP address of the TFTP server to specify the TFTP server address assigned to the client. Multiple IP addresses can be entered and separated by spaces. |

Note

DHCP options are optional configuration when the device functions as an L3 DHCP server. The configuration takes effect globally and does not need to be configured by default. If no DNS server address is specified, the DNS address assigned to a downlink port is the gateway IP address by default.

10.4 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**.

- (1) Click **Add**, select a L3 interface and IP address assignment method, and enter the address lease term and DNS server address. The address lease term is 30 minutes by default. You are advised to retain the default value. Then, click **OK**.

The screenshot displays the 'DHCPv6 Server' configuration page. At the top, there are tabs for 'IPv6 Config', 'DHCPv6 Server' (selected), 'DHCPv6 Clients', 'Static DHCPv6', and 'IPv6 Neighbor List'. Below the tabs, there are '+ Add' and 'Delete Selected' buttons. A light blue box contains two instructions: '1、 If DHCPv6 does not take effect on the Layer 3 interface (including but not limited to invalid IPv6 address and incorrect IPv6 address prefix of the Layer 3 interface), the DHCPv6 server cannot take effect.' and '2、 If the IPv6 prefix length of the Layer 3 interface is between 48 and 64, the address can be assigned. Up to 64 entries can be added.' Below this is a table with columns: 'L3 Interfaces', 'IPv6 Assignment', 'DNS Server', and 'Action'. The table is currently empty, showing 'No Data'. At the bottom, there is a pagination bar with '10/page', 'Go to page 1', and 'Total 0'.

A modal dialog is open in the foreground, allowing the user to add a new DHCPv6 server entry. The dialog contains the following fields:

- * L3 Interfaces:** A dropdown menu with 'Select' as the current value.
- IPv6 Assignment:** A dropdown menu with 'Auto' as the current value, accompanied by a help icon (?).
- * Lease Time (Min):** A text input field with '30' as the value, accompanied by a help icon (?).
- DNS Server:** A text input field with the placeholder text 'Example: 2000::1, each separated by a comma'.

At the bottom of the dialog are 'Cancel' and 'OK' buttons.

Table 10-5 IPv6 Address Configuration Parameters of the L3 Interface

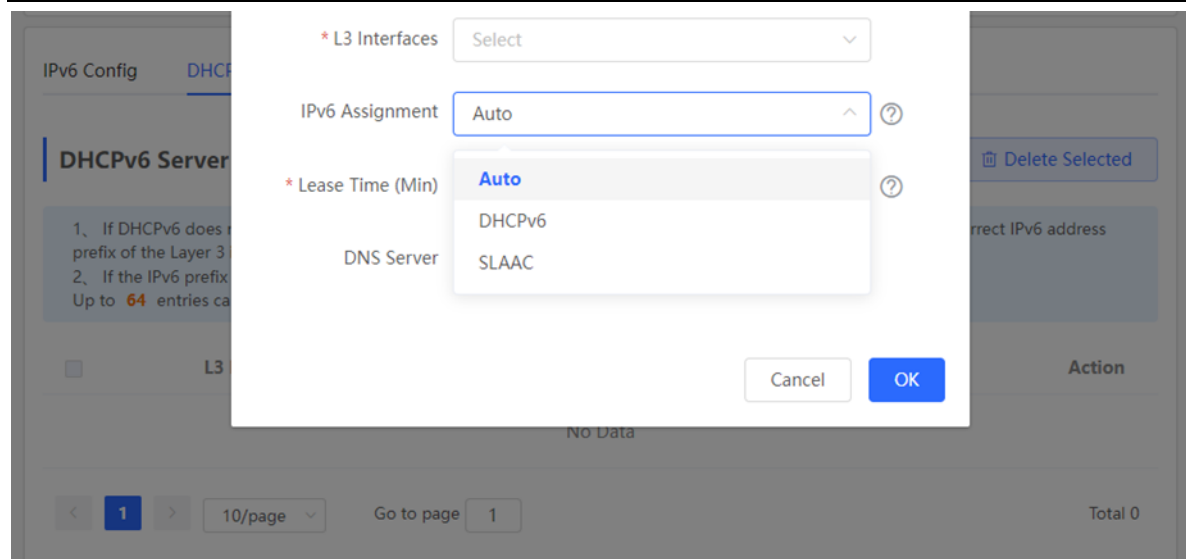
| Parameter | Description |
|-----------------|---|
| L3 Interfaces | Select the L3 interface for which the DHCPv6 server needs to be added. |
| IPv6 Assignment | If this parameter is set to Auto , both DHCPv6 and SLAAC are used to assign IPv6 addresses. |
| Lease Time | The default value is 30 minutes. 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. |

10.4.1 Viewing 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 [+ Batch Convert](#) to bind the IP addresses and hosts in batches, so that the IP addresses obtained by the hosts from the switch remain unchanged.

Note

Each server or client has only one DUID for identification.



10.4.2 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.

```

C:\Users\admin>ipconfig /all

Windows IP Configuration

Host Name . . . . . : PC-
Primary Dns Suffix . . . . . :
Node Type . . . . . : Hybrid
IP Routing Enabled. . . . . : No
WINS Proxy Enabled. . . . . : No

Ethernet adapter :

Connection-specific DNS Suffix . :
Description . . . . . : Ruijie VirtIO Ethernet Adapter
Physical Address. . . . . :
DHCP Enabled. . . . . : Yes
Autoconfiguration Enabled . . . . : Yes
Link-local IPv6 Address . . . . . : fe80::6dd5:266f:b695:55df%12(Preferred)
IPv4 Address. . . . . : 172.26.1.123(Preferred)
Subnet Mask . . . . . : 255.255.255.0
Lease Obtained. . . . . : Thursday, December 22, 2022 5:29:03 PM
Lease Expires . . . . . : Friday, December 30, 2022 5:28:57 PM
Default Gateway . . . . . : 172.26.1.1
DHCP Server . . . . . : 172.26.1.1
DHCPv6 IAID . . . . . : 340939776
DHCPv6 Client DUID. . . . . : 00-01-00-01-27-C7-77-50-52-54-00-3C-D6-BE
DNS Servers . . . . . : 192.168.58.94

```

IPv6 Config DHCPv6 Server **DHCPv6 Clients** Static DHCPv6 IPv6 Neighbor List

DHCPv6 Clients
You can view the DHCPv6 clients information on this page.

DHCPv6 Clients Search by IPv6 Address/DUID

| No. | Hostname | IPv6 Address | Remaining Lease Time(min) | DUID | Status |
|---------|----------|--------------|---------------------------|------|--------|
| No Data | | | | | |

< 1 > 10/page Go to page 1 Total 0

You can view the DHCPv6 client information on this page.

IPv6 Config DHCPv6 Server DHCPv6 Clients **Static DHCPv6** IPv6 Neighbor List

Static IP Address List
Up to 1000 entries can be added.

Static IP Address List Search by IPv6 Address/DUID

| No. | IPv6 Address | DUID | Action |
|---------|--------------|------|--------|
| No Data | | | |

< 1 > 10/page Go to page 1 Total 0

Add

* IPv6 Address

* DUID

Cancel OK

Static IP Address List

Up to 1000 entries can be added.

| No. | IPv6 Address | DUID | Action |
|---------|--------------|------|--------|
| No Data | | | |

< 1 > 10/page Go to page 1 Total 0

10.5 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).

IPv6 Config DHCPv6 Server DHCPv6 Clients Static DHCPv6 **IPv6 Neighbor List**

IPv6 Neighbor List Search by IP Address/MAC A

Up to 2000 IP-MAC bindings can be added.

| No. | MAC Address | IP Address | Type | Ethernet status | Action |
|---------|-------------|------------|------|-----------------|--------|
| No Data | | | | | |

< 1 > 10/page Go to page 1 Total 0

IPv6 Config DHCPv6 Server DHCPv6 Clients Static DHCPv6 **IPv6 Neighbor List**

Search by IP Address/MAC A + Add

Up to 1000 IP-MAC bindings can be added.

| No. | MAC Address | IP Address | Type | Ethernet status | Action |
|-----|-------------------|---------------------------|---------|-----------------|-------------|
| 1 | 00:d0:18:15:08:44 | fe80::2d0:18ff: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 | 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 | Bind |
| 8 | c0:b8:e6:e2:54:63 | fe80::c2b8:e6ff:fee2:5463 | Dynamic | VLAN 1 | Bind |

10/page Go to page 1 Total 8

[Click RITA for help.](#)

Add

* Interface

* IPv6 Address

* MAC Address

Cancel OK

10.6 Configuring a Static ARP Entry

Choose **Local Device > L3 Interfaces > 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 Interfaces DHCP Clients Static IP Addresses DHCP Option Static Routing ARP List

ARP List

Up to **2000** IP-MAC bindings can be added.

| <input type="checkbox"/> | No. | Interface | MAC | IP | Type | Reachable | Action |
|--------------------------|-----|-----------|-------------------|----------------|---------|-----------|----------------------|
| <input type="checkbox"/> | 1 | VLAN1 | 00:23:79:00:23:79 | 172.30.102.178 | Dynamic | Yes | Bind |
| <input type="checkbox"/> | 2 | -- | -- | 172.30.102.174 | Dynamic | No | Bind |
| <input type="checkbox"/> | 3 | VLAN1 | c0:b8:e6:e9:78:07 | 172.30.102.209 | Dynamic | Yes | Bind |
| <input type="checkbox"/> | 4 | VLAN1 | c0:b8:e6:ec:a1:5c | 172.30.102.118 | Dynamic | Yes | Bind |

Add ×

*

IP

*

MAC

Cancel

OK

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

ARP List

Up to **2000** IP-MAC bindings can be added.

| <input type="checkbox"/> | No. | Interface | MAC | IP | Type | Reachable | Action |
|--------------------------|-----|-----------|-------------------|----------------|---------|-----------|---|
| <input type="checkbox"/> | 1 | VLAN1 | 00:23:79:00:23:79 | 172.30.102.178 | Static | Yes | Edit Delete |
| <input type="checkbox"/> | 2 | VLAN1 | c0:b8:e6:e9:78:07 | 172.30.102.209 | Dynamic | Yes | Bind |

11 Configuring Route

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.

11.1 Configuring Static Routes

Choose **Local Device** > **L3 Interfaces** > **Static Routing**.

Static routes are manually configured by the user. When a data packet matches a static route, the packet will be forwarded according to the specified forwarding mode.



Caution

Static routes cannot automatically adapt to changes of the network topology. When the network topology changes, you need to reconfigure the static routes.

Click **Add**. In the dialog box that appears, enter the destination address, subnet mask, outbound interface, and next-hop IP address to create a static route.

L3 Interfaces
DHCP Clients
Static IP Addresses
DHCP Option
Static Routing
ARP List


Static Routing

 When a packet arrives, the device checks the destination field and compares it with routing table. If it finds a match for destination network then it will forward that packet from the specified interface. 

Static Route List

Example: 1.1.1.1

Up to **500** static routes can be added.

| <input type="checkbox"/> | Dest IP Address | Subnet Mask | Outbound Interface | Next Hop | Reachable | Action |
|--------------------------|-----------------|---------------|--------------------|----------|--|---|
| <input type="checkbox"/> | 2.1.1.0 | 255.255.255.0 | Gi9 | 3.1.1.1 | No  | Edit Delete |

Edit
×

* Dest IP Address

* Subnet Mask

255.255.255.0

Outbound Interface

Select

* Next Hop

Cancel

OK

Table 11-1 Description of Static Routes Configuration Parameters

| Parameter | Description |
|--------------------|--|
| Dest IP Address | Specify the destination network to which the data packet is to be sent. The device matches the data packet based on the destination address and subnet mask. |
| Subnet Mask | Specify the subnet mask of the destination network. The device matches the data packet based on the destination address and subnet mask. |
| Outbound Interface | Specify the interface that forwards the data packet. |
| Next Hop | Specify the IP address of the next hop in the route for the data packet |

After a static route is created, you can find the relevant route configuration and reachability status in the static route list. The **Reachable** parameter specifies whether the next hop is reachable, based on which you can determine whether the route takes effect. If the value is **No**, check whether the outbound interface in the current route can ping the next-hop address.

Static Route List

Example: 1.1.1.1

Q

+ Add

Delete Selected

Up to 500 static routes can be added.

| | Dest IP Address | Subnet Mask | Outbound Int | | | | |
|--------------------------|-----------------|---------------|--------------|---------|----|--|-------------|
| <input type="checkbox"/> | 2.1.1.0 | 255.255.255.0 | Gi9 | 3.1.1.1 | No | | Edit Delete |

The route is unreachable. Please initiate a Ping test from the outbound interface to the next hop.

To delete or modify a static route, in **Static Route List**, you can click **Delete** or **Edit** in the **Action** column; or select the static route entry to be deleted, click **Delete Selected** to delete multiple static route entries.

11.2 Configuring the IPv6 Static Route

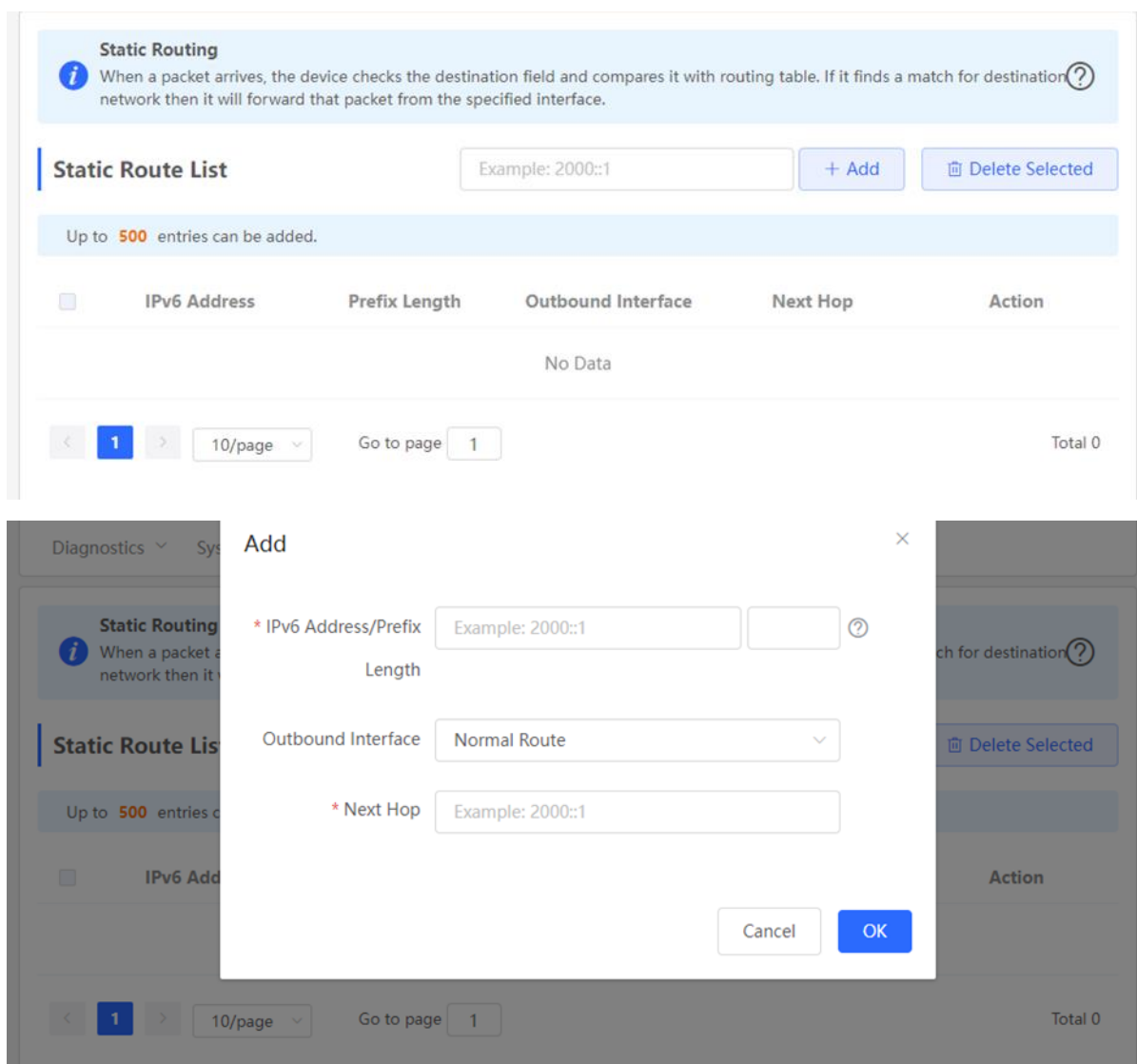
Choose **Local Device > Routing > IPv6 Static Routing**.

You need to manually configure an IPv6 static route. When the packet matches the static route, the packet will be forwarded according to the specified forwarding method.

Caution

The static route cannot automatically adapt to changes on 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.



Static Routing

When a packet arrives, the device checks the destination field and compares it with routing table. If it finds a match for destination network then it will forward that packet from the specified interface.

Static Route List

Example: 2000::1 + Add Delete Selected

Up to 500 entries can be added.

| IPv6 Address | Prefix Length | Outbound Interface | Next Hop | Action |
|--------------|---------------|--------------------|----------|--------|
| No Data | | | | |

< 1 > 10/page Go to page 1 Total 0

Add

* IPv6 Address/Prefix Length Example: 2000::1

Outbound Interface Normal Route

* Next Hop Example: 2000::1

Cancel OK

Table 11-2 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 |

| Parameter | Description |
|--------------------|--|
| | 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. |

11.3 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.

11.3.1 Configuring RIP Basic Functions

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

Click **Add** and configure the network segment and interface.

Local Device(NBS) Currently in Local Device mode. English

Switch
● NBS6002
Hostname: Ruijie
IP Address: 192.168.110.62
Software Ver: ReyeeOS 1.218.2421
SN: MACCNBS6000HQ
MAC Address: 00:D0:F8:95:68:5E
Hardware Ver: 1.00
DNS: 192.168.110.1
Reboot

Home VLAN Monitor Ports L2 Multicast L3 Interfaces Routing Security Advanced

Diagnostics System

RIP Settings Port Settings Advanced Neighbor Info

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.

Network Segment/Port List
Enable RIP in the specified network segment or on the specified port.

Network Segment/Port List + Add Delete Selected

| No. | Network Segment/Port | Auth Mode | Action |
|-----|----------------------|-------------------|-------------|
| 1 | VLAN 1 | No Authentication | Edit Delete |

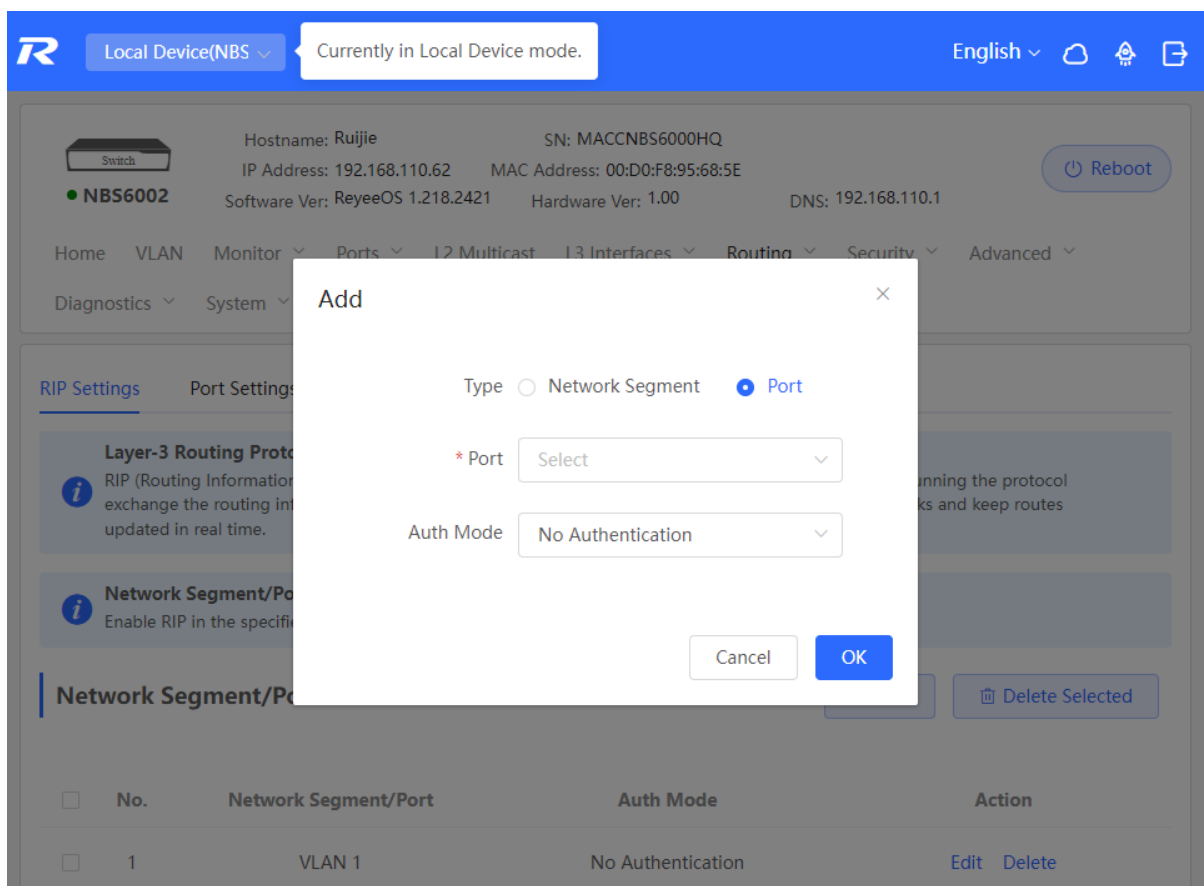
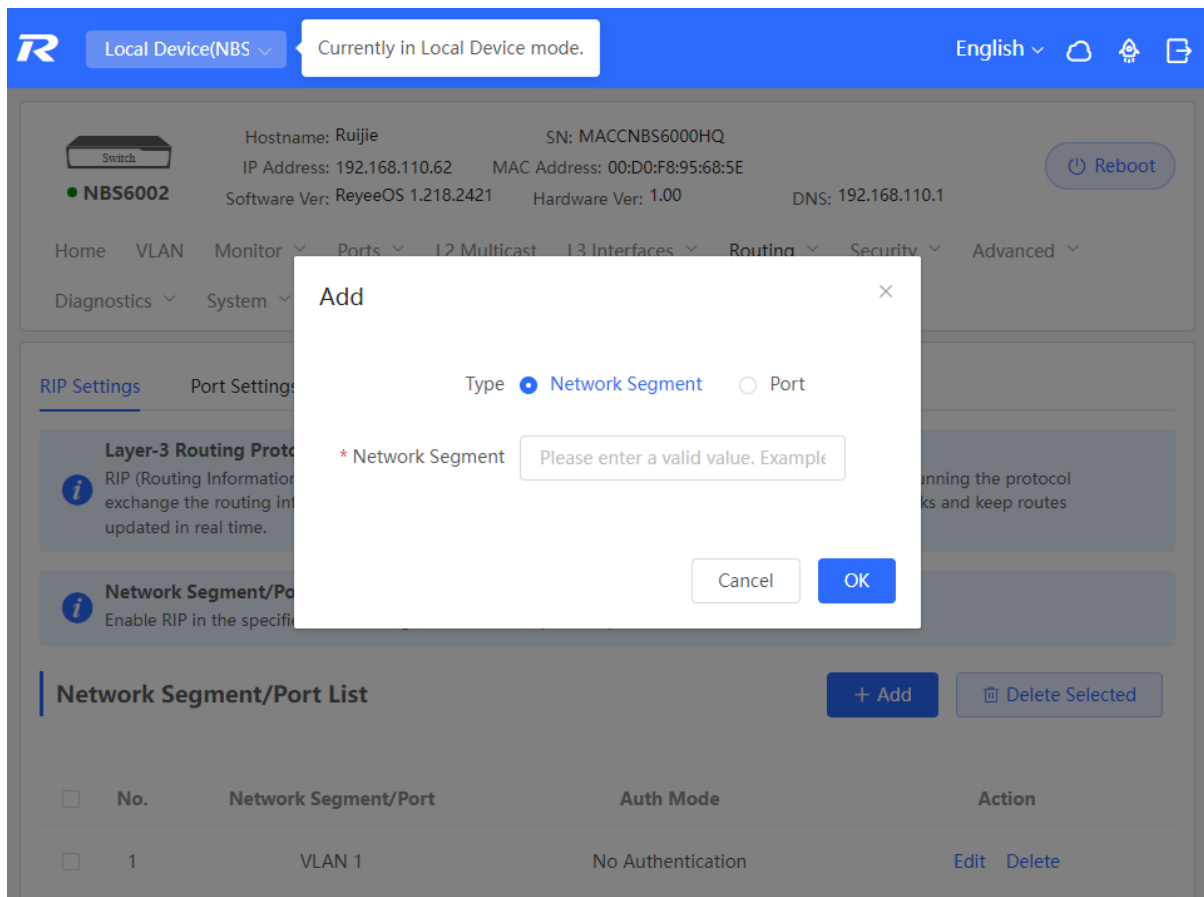


Table 11-3 RIP Configuration Parameters

| Parameter | Description |
|-----------------|--|
| Type | <p>Network Segment: Enable RIP in the specified network segment. The IP addresses of this network segment are added to the RIP routing table. The device and its RIP-enabled neighbor devices learn the routing table from each other.</p> <p>Port: Enable RIP on the specified port. All the IP addresses of this port are added to the RIP routing table. The device and its RIP-enabled neighbor devices learn the routing table from each other.</p> |
| Network Segment | <p>Enter the network segment, for example, 10.1.0.0/24, when Type is set to Network Segment.</p> <p>RIP will be enabled on all interfaces of the device covered by this network segment.</p> |
| Port | Select a VLAN interface or physical port when Type is set to Port . |
| Auth Mode | <p>No Authentication: The protocol packets are not authenticated.</p> <p>Encrypted Text: The protocol packets are authenticated, and the authentication key is transmitted with the protocol packets in the form of encrypted text.</p> <p>Plain Text: The protocol packets are authenticated, and the authentication key is transmitted with the protocol packets in the form of plain text.</p> |
| Auth Key | Enter the authentication key to authenticate protocol packets when Auth Mode is set to Encrypted Text or Plain Text . |

11.3.2 Configuring the RIP Port

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

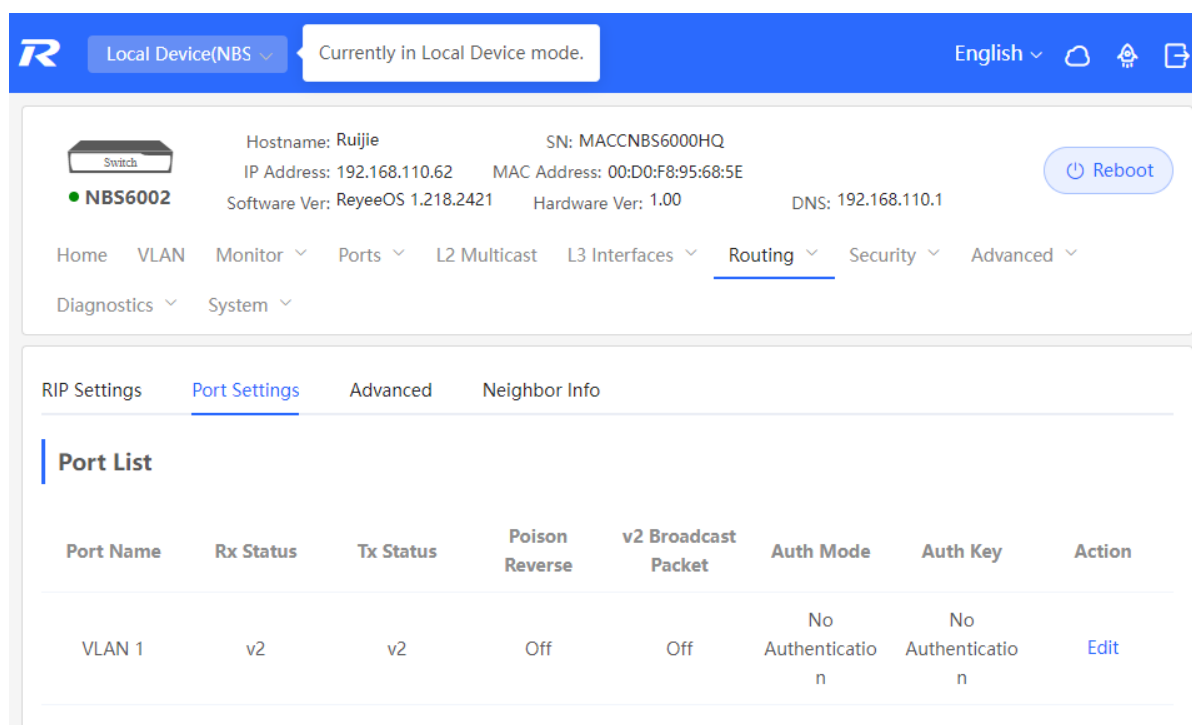


Table 11-4 Configuration Parameters in the Port List

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

11.3.3 Configuring the RIP Global Configuration

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

search

Ports

L2 Multicast

L3 Multicast

L3 Interfaces

Routing

- Static Routing
- IPv6 Static Routing
- RIP Settings**
- RIPng Settings
- OSPFv2
- OSPFv3
- Route Info

Security

RIP Settings

Port Settings

Advanced

Neighbor Info

RIP Global Config

Edit Config

| RIP Version | Route Advertisement | Administrative Distance | Update Timer | Invalid Timer | Flush Timer |
|-------------|---------------------|-------------------------|--------------|---------------|-------------|
| Default | Off | 1 (Default) | 30 s | 180 s | 120 s |

Route Redistribution List

+ Add

Delete Selected

| Type | Administrative Distance | Instance ID | Action |
|---------|-------------------------|-------------|--------|
| No Data | | | |

Passive Interface

Edit Config

RIP Version

- Default

Route Advertisement

- Off

Administrative Distance

- 1 (Default)

* Update Timer

- 30 s (5-2147483647)

* Invalid Timer

- 180 s (5-2147483647)

* Flush Timer

- 120 s (5-2147483647)

Cancel

OK

RIP Settings

Port Settings

Advanced

Neighbor Info

Improper timers may cause route flapping. Therefore, RIP timers must be consistent on the devices connected to the same network. You are not advised to reset the RIP timers unless you have specific needs.

RIP Global Config

Edit Config

| RIP Version | Route Advertisement | Administrative Distance | Update Timer | Invalid Timer | Flush Timer |
|-------------|---------------------|-------------------------|--------------|---------------|-------------|
| Default | Off | 1 (Default) | 30 s | 180 s | 120 s |

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

| Type | Administrative Distance | Instance ID | Action |
|---------|-------------------------|-------------|--------|
| No Data | | | |

Passive Interface

RIP update packets will be suppressed on the passive interface. If the device connected to the interface does not adopt RIP, you are advised to enable this function.

140

Table 11-5 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. |
| 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. |

11.3.4 Configuring the RIP Route Redistribution List

Redistribute routes of other protocols to the RIP domain so that RIP can interwork with other routing domains.

Choose **Local Device > Routing > RIP Settings > Advanced > Route Redistribution List**, click **Add**, and select the type and administrative distance.

The screenshot shows a configuration interface for RIP. An 'Add' dialog box is open in the foreground, allowing the user to add a new route redistribution entry. The dialog contains two required fields: '* Type' and '* Administrative Distance'. The '* Type' field has a dropdown menu currently set to 'Select'. The '* Administrative Distance' field has a dropdown menu currently set to '0 (Administrative Distance)'. Below these fields are 'Cancel' and 'OK' buttons. In the background, the 'RIP Global Config' page is visible, showing a 'Route Redistribution List' table with columns for Type, Administrative Distance, Instance ID, and Action. The table currently contains no data. Below the table is a 'Passive Interface' section with a note about suppressing RIP update packets on passive interfaces.

Table 11-6 RIP Route Redistribution Parameters

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

Add ×

* Type

OSPF Routing

* Administrative Distance

0 (Administrative Distance)

* Instance ID

Select

3

Cancel

OK

11.3.5 Configuring the Passive Interface

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

Choose **Local Device > Routing > RIP Settings > Advanced > Passive Interface**, click **Add**, and select a passive interface.

| <input type="checkbox"/> | Type | Administrative Distance | Instance ID | Action |
|--------------------------|------|-------------------------|-------------|--------|
| No Data | | | | |

Passive Interface

RIP update packets will be suppressed on the passive interface. If the device connected to the interface does not adopt RIP, you are advised to enable this function.

Passive Interface

+ Add

Delete Selected

| <input type="checkbox"/> | Port Name | Action |
|--------------------------|-----------|--------|
| No Data | | |

Neighbor Route

If a router cannot forward broadcast packets, another router is designated as the neighbor to establish a RIP direct link.

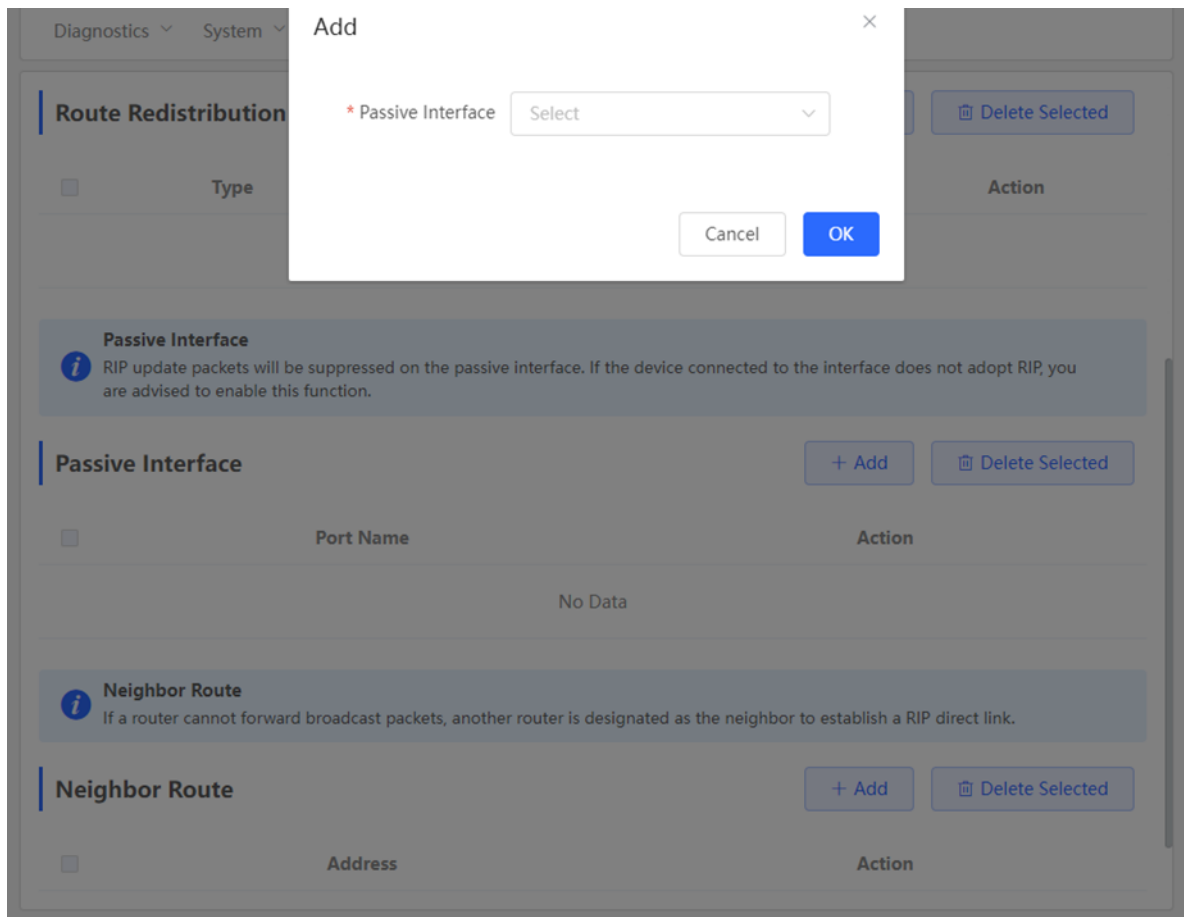
Neighbor Route

+ Add

Delete Selected

| <input type="checkbox"/> | Address | Action |
|--------------------------|---------|--------|
| No Data | | |

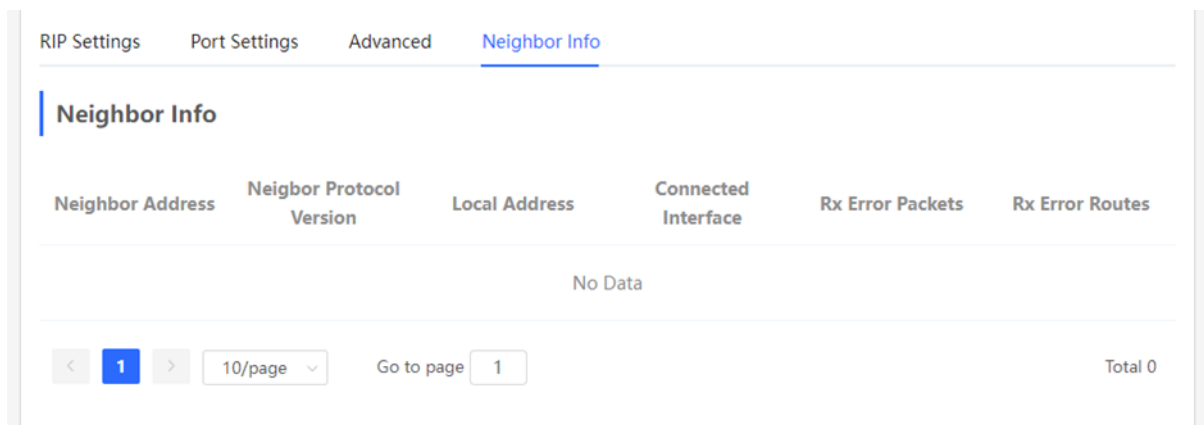
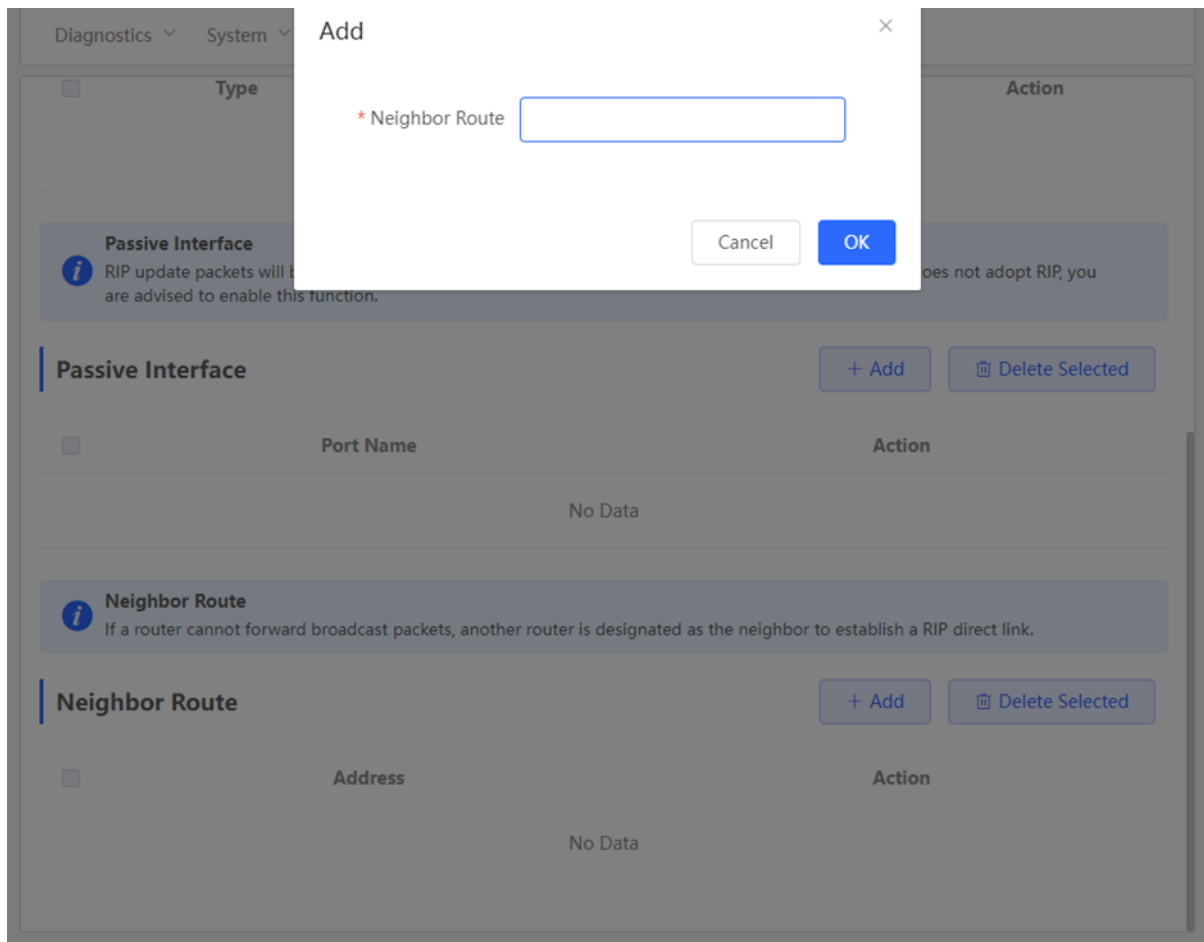
143



11.3.6 Configuring the Neighbor Route

When the router cannot process broadcast packets, another router can be designated as the neighbor to establish a RIP direct link.

Choose **Local Device > Routing > RIP Settings > Advanced > Neighbor Route**, click **Add**, and enter the IP address of the neighbor router.



11.4 Configuring RIPng

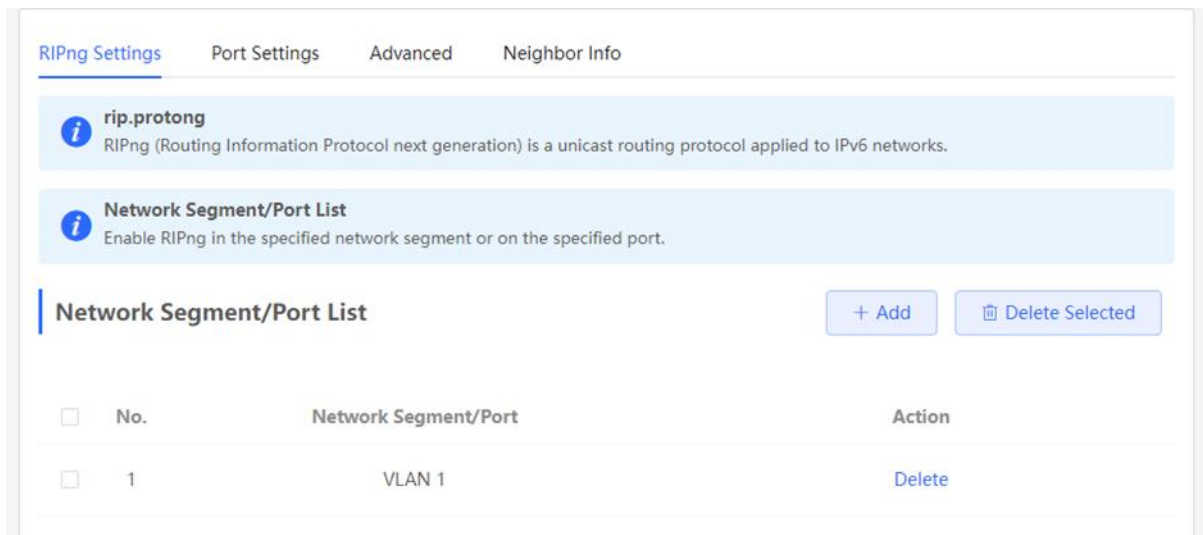
11.4.1 Configuring RIPng Basic Functions

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**.

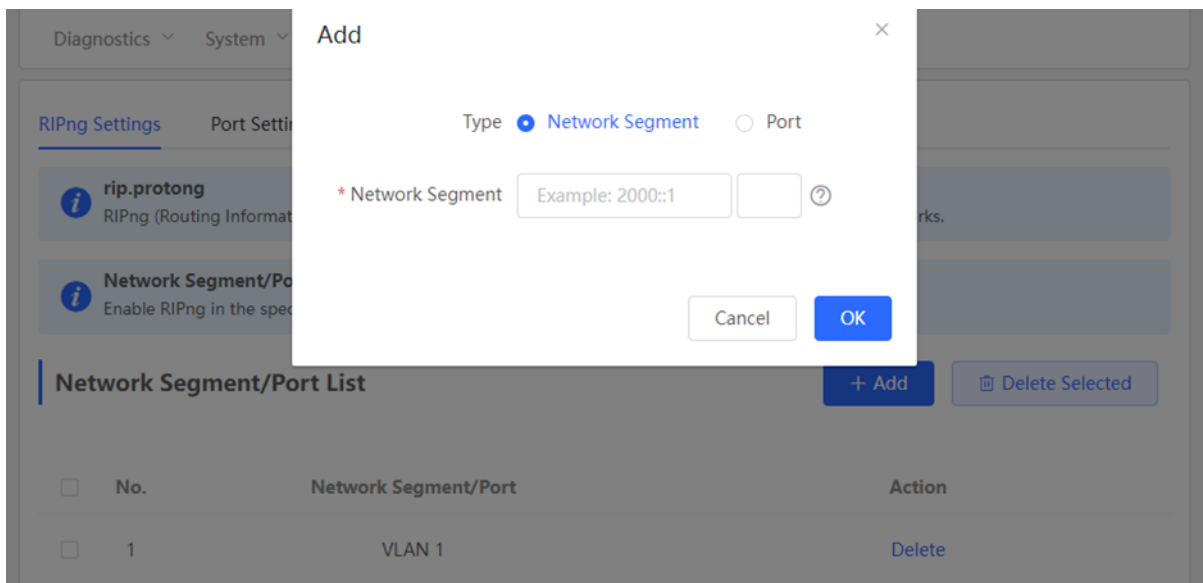
Click **Add**, set **Type** to **Network Segment** or **Port**, and specify the network segment or port accordingly.



RIPng (Routing Information Protocol next generation) is a unicast routing protocol applied to IPv6 networks.

Network Segment/Port List

Enable RIPng in the specified network segment or on the specified port.



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

Alternatively, enable RIPng on a specified port:

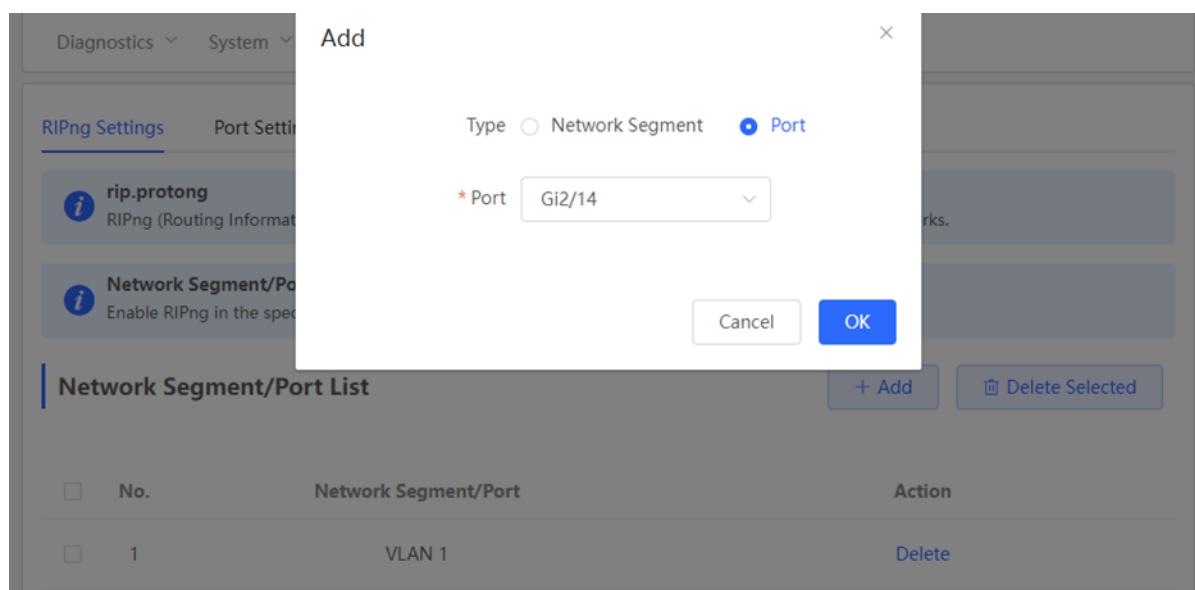


Table 11-7 RIPng Configuration Parameters

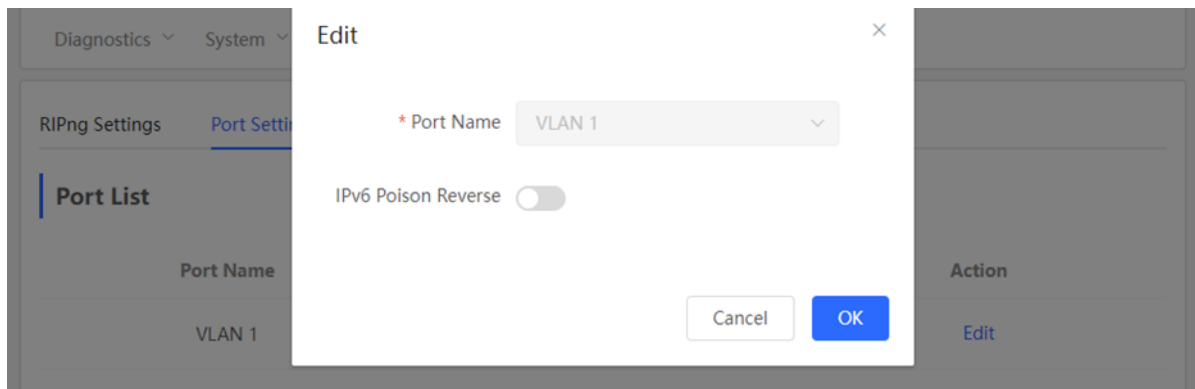
| Parameter | Description |
|-----------------|--|
| Type | <p>Network Segment: Enable RIP in the specified network segment. The IP addresses of this network segment are added to the RIP routing table, and the device and its RIP-enabled neighbor devices learn the routing table from each other.</p> <p>Port: Enable RIP on the specified port. All the IP addresses of this port are added to the RIP routing table, and the device and its RIP-enabled neighbor devices learn the routing table from each other.</p> |
| Network Segment | Enter the IPv6 address and prefix length when Type is set to Network Segment . RIPng will be enabled on all interfaces of the device covered by this network segment. |
| Port | Select a VLAN interface or physical port when Type is set to Port . |

11.4.2 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.

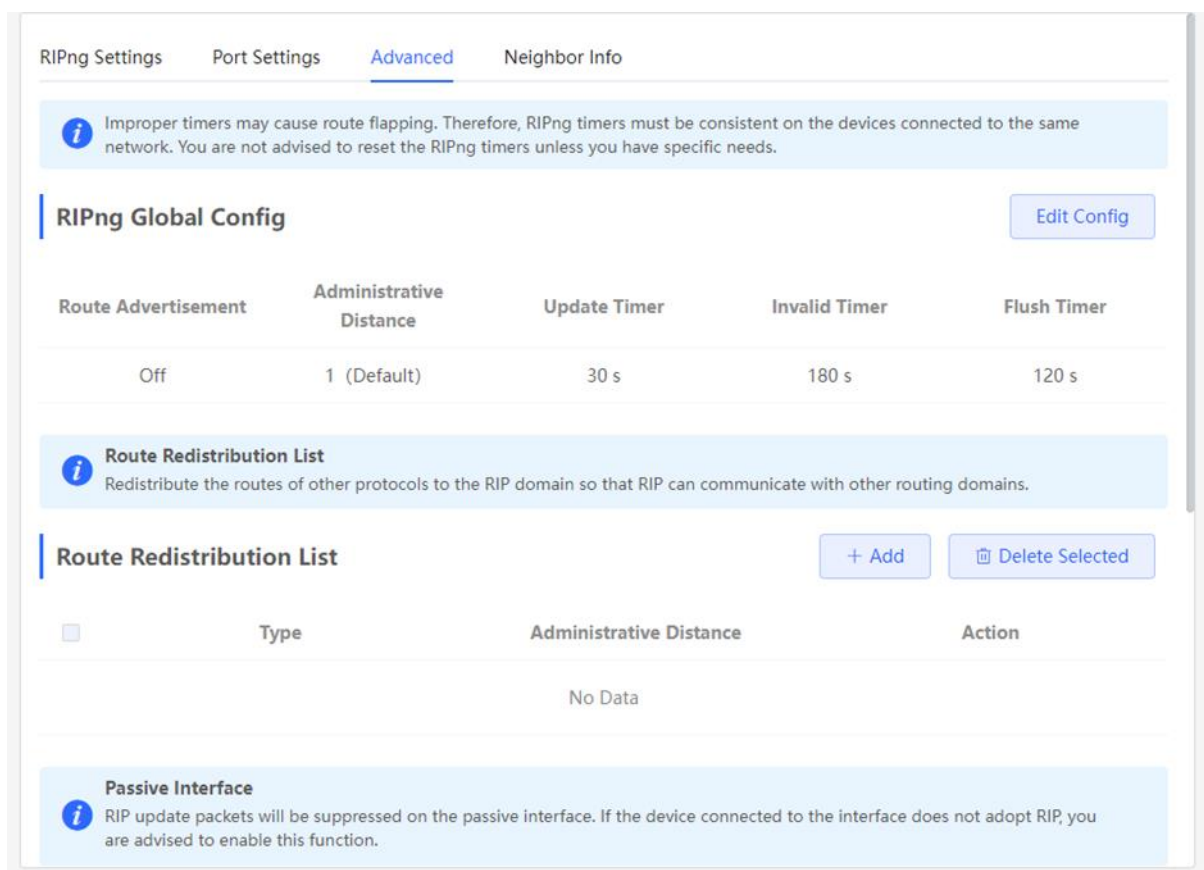
Choose **Local Device** > **Routing** > **RIPng Settings** > **Port Settings**, click Edit, and enable IPv6 poison reverse.





11.4.3 Configuring the RIPng Global Configuration

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



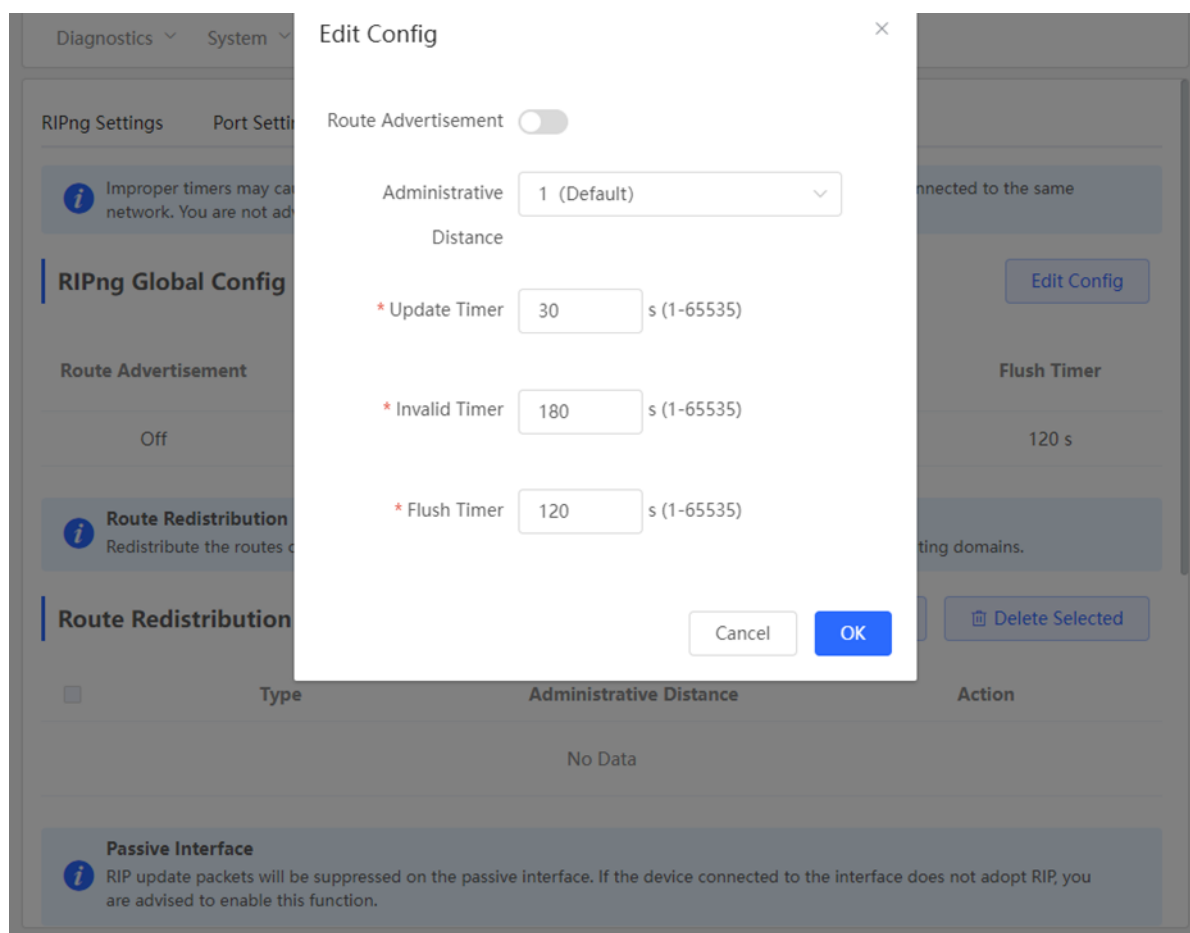


Table 11-8 RIPng Global Configuration Parameters

| Parameter | Description |
|-------------------------|--|
| Route Advertisement | After route advertisement is enabled, the current device generates a default route and sends it to the neighbor. |
| Administrative Distance | Redistribute routes of other protocols to the RIP domain so that RIP can interwork with other routing domains. |
| Update Timer | RIP update cycle. The routing information is updated every 30 seconds by default. |
| Invalid Timer | If no update is received before a route becomes invalid, the route is considered unreachable. The default value is 180 seconds. |
| Flush Timer | If no update is received before the flush timer of an invalid route expires, the route is completely deleted from the RIP routing table. The default value is 120 seconds. |

11.4.4 Configuring the RIPng Route Redistribution List

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

Choose **Local Device > Routing > RIPng Settings > Advanced > Route Redistribution List**, and click **+ Add**.

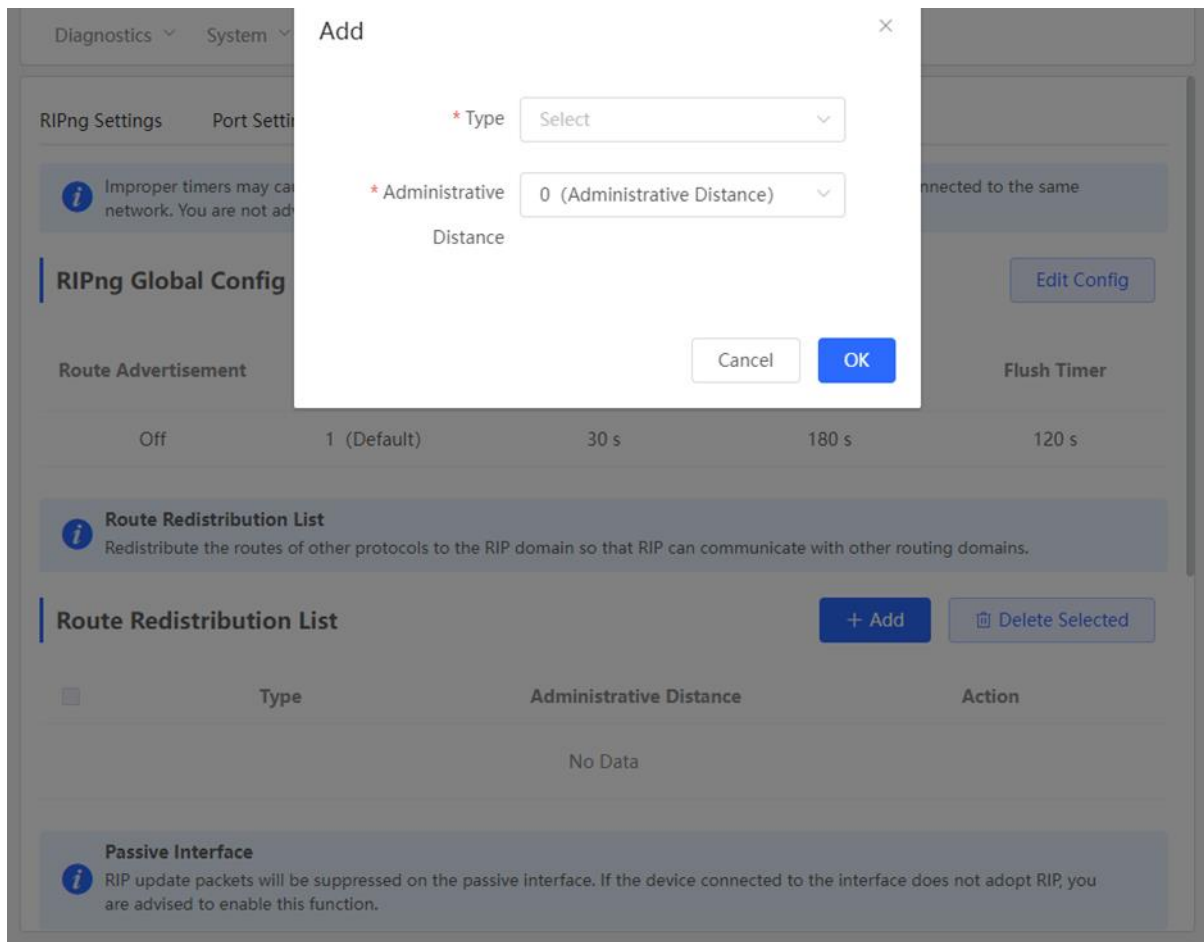


Table 11-9 RIP Route Redistribution Parameters

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

11.4.5 Configuring the RIPng Passive Interface

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

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

☐

Type

Administrative Distance

Action

No Data

Passive Interface

RIP update packets will be suppressed on the passive interface. If the device connected to the interface does not adopt RIP, you are advised to enable this function.

Passive Interface

+ Add

Delete Selected

☐

Port Name

Action

No Data

RIPng Aggregate Routing

Create an aggregate RIPng route announcement.

RIPng Aggregate Routing

+ Add

Delete Selected

☐

Address

Action

No Data

Diagnostics

System

Add

* Passive Interface

Select

Cancel

OK

Passive Interface

RIP update packets will be suppressed on the passive interface. If the device connected to the interface does not adopt RIP, you are advised to enable this function.

Passive Interface

+ Add

Delete Selected

☐

Port Name

Action

No Data

RIPng Aggregate Routing

Create an aggregate RIPng route announcement.

RIPng Aggregate Routing

+ Add

Delete Selected

☐

Address

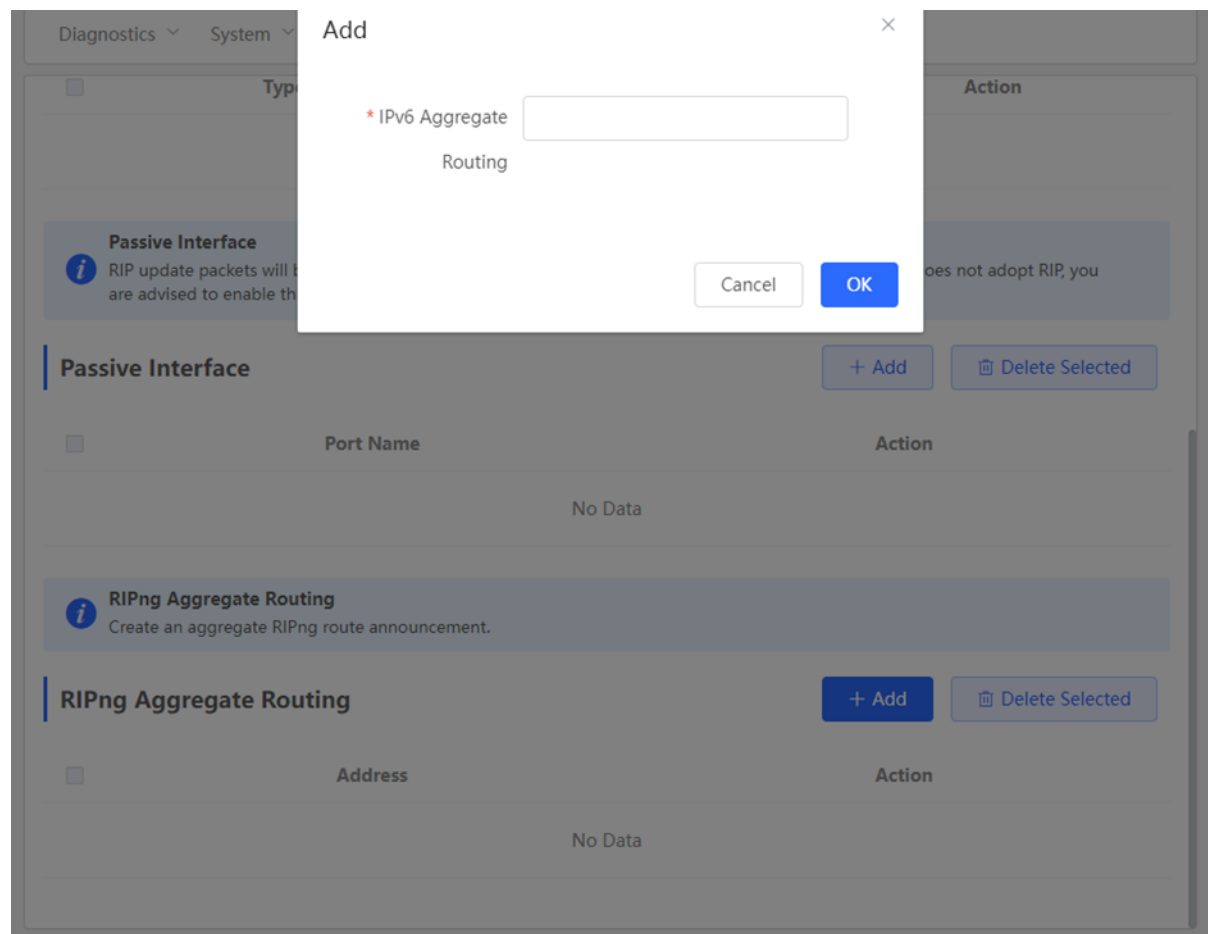
Action

No Data

151

11.4.6 Configuring the RIPng Aggregate Route

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



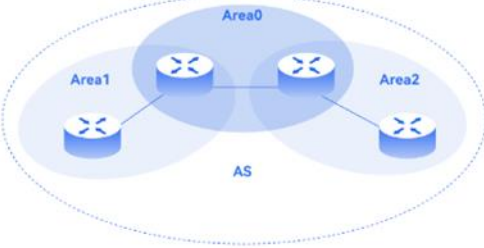
11.5 OSPFv2

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.

11.5.1 Configuring OSPFv2 Basic Parameters

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



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.

[Start Setup](#)

(1) Configure an instance.

① ————— ② ————— ③
 Configure the instance. **Configure the interface.** Operation succeeded.

* Instance ID

* Router ID ?

Advertise Default ☐

Route

Import External Route ☐ Static Route Redistribution

☐ Direct Route Redistribution


☐ RIP Redistribution

[Details](#)

[Previous](#)

[Next](#)

Table 11-10 Instance Configuration Parameters

| Parameter | Description |
|-------------------------|---|
| Instance ID | Create an OSPF instance based on the service type. The instance only takes effect locally, and does not affect packet exchange with other devices. |
| Router ID | It identifies a router in an OSPF domain. <div>  Caution Router IDs within the same domain must be unique. The same configuration may cause neighbor discovery failures. </div> |
| Advertise Default Route | Generate a default route and send it to the neighbor. After this function is enabled, you need to enter the metric and select a type. The default metric is 1. Type 1: The metrics displayed on different routers vary. Type 2: The metrics displayed on all routers are the same. |

| Parameter | Description |
|-----------------------|---|
| Import External Route | <p>Redistribute routes of other protocols to the OSPF domain to interwork with other routing domains.</p> <p>If Static Route Redistribution is selected, enter the metric, which is 20 by default.</p> <p>If Direct Route Redistribution is selected, enter the metric, which is 20 by default.</p> <p>If RIP Redistribution is selected, enter the metric, which is 20 by default.</p> |
| Details | Expand the detailed configuration. |

----- Details -----

Distance

Intra-Area
Optional.Default:110

Inter-Area
Optional.Default:110

External
Optional.Default:110

LSA

Generation Delay
Optional.Default:

Received Delay
Optional.Default:

SPF Calculation

Waiting Interval
Optional.Default:

Min Interval
Optional.Default:50

Max Interval
Optional.Default:50

Graceful Restart
Graceful Restart ☒

Helper
LSA Check ☐

* Max Wait Time

Table 11-11 Parameters in the Instance Detailed Configuration

| Parameter | Description |
|------------------|--|
| Distance | It is used for protocol selection. By default, the intra-area, inter-area, and external distances are all 110 . |
| LSA | Frequent network changes and route flapping may occupy too much network bandwidth and device resources. The LSA generation and reception delays are specified in OSPF by default. The default value is 1000 ms. |
| SPF Calculation | When the link state database (LSDB) changes, OSPF recalculates the shortest path, and sets the interval to prevent frequent network changes from occupying a large number of resources Waiting Interval: When the state changes, the timer is triggered. The delay is calculated for the first time after the timer expires. The default value is 0 ms. Min Interval: As the number of changes increases, the time of each interval will increase according to the algorithm, and the default value is 50 ms. Max Interval: When the calculated interval reaches the maximum interval, the subsequent interval is always equal to the maximum interval. If the time from the last calculation exceeds the maximum interval and the LSDB is not updated, the timer is disabled. |
| Graceful Restart | Graceful Restart (GR) can avoid route flapping caused by traffic interruption and active/standby board switchover, thus ensuring the stability of key services. Graceful Restart Helper: The Graceful Restart Helper function is enabled when this switch is turned on. LSA Check: LSA packets outside the domain are checked when this switch is turned on. Max Wait Time: Timing starts after the device receives the GR packet from the peer device. If the peer device does not complete GR within Max Wait Time , the device exits the GR Helper mode. The default value is 1800 seconds. |

(2) Configure an interface.

1 2 3
Configure the instance. Configure the interface. Operation succeeded.

* Interface:

* Area:

Stub Area: ☐

Details

Priority:

Port List

Up to 16 entries can be added.

| Interface | Area | Priority | Network Type | Hello Packets | Dead Interval | Interface Auth | LSA Transmission Delay | LSA Retransmission Interval | Action |
|-----------|------|----------|--------------|---------------|---------------|----------------|------------------------|-----------------------------|--------|
| No Data | | | | | | | | | |

1 10/page Go to page: 1 Total: 0

Table 11-12 Interface Configuration Parameters

| Parameter | Description |
|-----------|---|
| Interface | Select the OSPF-enabled L3 interface. |
| Area | Configure the area ID. Value range: 0-4294967295 |
| Stub Area | <p>If Stub Area is enabled, you need to configure the area type and inter-area route isolation.</p> <p>Stub area: Routers at the edge of the area do not advertise routes outside the area, and the routing table in the area is small.</p> <p>Not-So-Stubby Area (NSSA): A few external routes can be imported.</p> <p>Inter-area route isolation: After this function is enabled, inter-area routes will not be imported to this area.</p> |
| Details | Expand the detailed configuration. |

1

2

3

Configure the instance. Configure the interface. **Operation succeeded.**

Details

Priority

Optional.Default:1

Network Type

Broadcast

Hello Packets

Optional.Default:10(s)

Dead Interval

Optional.Default:40(s)

LSA Transmission Delay

Optional.Default:1(s)

LSA Retransmission Interval

Optional.Default:5(s)

Interface Auth

No Auth

Ignore MTU Check

☒

Add

Table 11-13 Parameters in the Interface Detailed Configuration

| Parameter | Description |
|--------------|--|
| Priority | It is 1 by default. |
| Network Type | Broadcast Unicast Multicast Non-Broadcast Multiple Access |

| Parameter | Description |
|-----------------------------|---|
| 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 | <p>No Auth: The protocol packets are not authenticated. It is the default value.</p> <p>Plain Text: The protocol packets are authenticated, and the authentication key is transmitted with the protocol packets in the form of plain text.</p> <p>MD5: The protocol packets are authenticated, and the authentication key is MD5 encrypted and then transmitted with the protocol packets.</p> |
| 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.



Disable

11.5.2 Adding an OSPFv2 Interface

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

Instance List

+ Add

Up to 16 entries 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 |

< 1 >

10/page

Go to page 1

Total 1

Instance List

+ Add

Up to 16 entries can be added.

| Instance ID | Router ID | Interface | Area | Advertise | Action |
|-------------|-----------|-----------|----------|---|--|
| 12 | 123.1.1.1 | VLAN 1 | 23(stub) | <div>V2 Interface V2 Instance Route Redistribution V2 Stub Area Management V2 Neighbor Management</div> | More Neighbor Info Edit Delete |

< 1 >

10/page

Go to page 1

Total 1

V2 Interface

Interface

Select

* Area

Priority

Optional.Default:1

Network Type

Broadcast

Hello Packets

Optional.Default:10(s)

Dead Interval

Optional.Default:40(s)

Port List

Add

Reset

Up to 64 entries can be added.

| Interface | Area | Priority | Network Type | Hello Packets | Dead Interval | Interface Auth | LSA Transmission Delay | LSA Retransmission Interval | Action |
|-----------|------|----------|--------------|---------------|---------------|----------------|------------------------|-----------------------------|----------------------|
| VLAN 1 | 23 | | Broadcast | | | No Auth | | | Edit |

<

1

>

10/page

Go to page

1

Total 1

11.5.3 Redistributing OSPFv2 Instance Routes

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

V2 Instance Route Redistribution
×

!

Route Redistribution cannot select its own instance number!

* Instance ID
Select

Metric
Optional.Default:20

Route Redistribution List
Add
Reset

Up to 63 entries can be added.

| Instance ID | Metric | Action |
|-------------|--------|--------|
| No Data | | |

<
1
>

10/page

Go to page
1

Total 0

11.5.4 Managing OSPFv2 Stub Areas

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

V2 Stub Area Management
×

* Area ID

Area Type
stub

Inter-Route Isolation
☐

Area List
Add
Reset

Up to 64 entries can be added.

| Area ID | Area Type | Inter-Route Isolation | Action |
|---------|-----------|-----------------------|---|
| 23 | stub | Enable | Edit Delete |

<
1
>

10/page

Go to page
1

Total 1

11.5.5 Managing OSPFv2 Neighbors

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

V2 Neighbor Management ×

* Neighbor IP

Neighbor List Add Reset

Up to 64 entries can be added.

| Neighbor IP | Action |
|-------------|--------|
| No Data | |

< 1 > 10/page Go to page 1 Total 0

11.5.6 Viewing OSPFv2 Neighbor Information

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

Neighbor Info ×

| Instance ID | Router ID | Status | Neighbor IP | Interface |
|-------------|-----------|--------|-------------|-----------|
| No Data | | | | |

< 1 > 10/page Go to page 1 Total 0

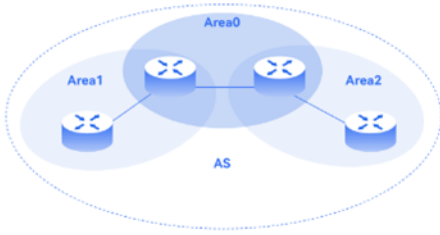
11.6 OSPFv3

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

11.6.1 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.

[Start Setup](#)

OSPF

OSPF is a typical link-state routing protocol. To satisfy users' increasing requirements for network reliability and heterogeneity on a large network, OSPF solves the problems such as slow convergence, unscientific metric values, and poor scalability.

Highlights

Achieves fast convergence.

Minimizes routing overhead.

Reduces routing update traffic through area partition.

Applies to various networks with up to thousands of switches.

① — ② — ③
 Configure the instance. **Configure the interface.** Operation succeeded.

* Router ID ?


Advertise Default ☐ Route

Import External Route ☐ Static Route Redistribution
☐ Direct Route Redistribution
☐ RIP Redistribution

..... [Details](#)

[Previous](#)
[Next](#)

Table 11-14 Instance Configuration Parameters

| Parameter | Description |
|-------------------------|---|
| Instance ID | Create an OSPF instance based on the service type. The instance only takes effect locally, and does not affect packet exchange with other devices. |
| Router ID | It identifies a router in an OSPF domain. <div>  Caution Router IDs within the same domain must be unique. The same configuration may cause neighbor discovery failures. </div> |
| Advertise Default Route | Generate a default route and send it to the neighbor. After this function is enabled, you need to enter the metric and select a type. The default metric is 1 . Type 1: The metrics displayed on different routers vary. Type 2: The metrics displayed on all routers are the same. |
| Import External Route | Redistribute routes of other protocols to the OSPF domain to interwork with other routing domains. If Static Route Redistribution is selected, enter the metric, which is 20 by default. If Direct Route Redistribution is selected, enter the metric, which is 20 by |

| Parameter | Description |
|-----------|--|
| | default. If RIP Redistribution is selected, enter the metric, which is 20 by default. |
| Details | Expand the detailed configuration. |

① ————— ② ————— ③
 Configure the instance. **Configure the interface.** Operation succeeded.

* Router ID ?

Advertise Default ☒

Route Metric Optional.Default:1
 Type 2 ?

Import External Route ☒ Static Route Redistribution

Metric Optional.Default:20

☒ Direct Route Redistribution

Metric Optional.Default:20

☒ RIP Redistribution

Metric Optional.Default:20

Details

Distance Intra-Area Optional.Default:110

Inter-Area Optional.Default:110

External Optional.Default:110

LSA Generation Delay Optional.Default

Received Delay Optional.Default

Previous

Next

1 —
 2 —
 3

Configure the instance. **Configure the interface.** Operation succeeded.

Metric
Optional.Default:20

☒ RIP Redistribution

Metric
Optional.Default:20

Details

Distance
Intra-Area
Optional.Default:110

Inter-Area
Optional.Default:110

External
Optional.Default:110

LSA
Generation Delay
Optional.Default

Received Delay
Optional.Default

SPF Calculation
Waiting Interval
Optional.Default

Min Interval
Optional.Default:50

Max Interval
Optional.Default:50

Graceful Restart
Graceful Restart ☒

Helper

LSA Check
☐

* Max Wait Time
1800

Previous

Next

Table 11-15 Parameters in the Instance Detailed Configuration

| Parameter | Description |
|-----------------|--|
| Distance | It is used for protocol selection. By default, the intra-area, inter-area, and external distances are all 110 . |
| LSA | <p>Frequent network changes and route flapping may occupy too much network bandwidth and device resources. The LSA generation and reception delays are specified in OSPF by default.</p> <p>The default value is 1000 ms.</p> |
| SPF Calculation | <p>When the link state database (LSDB) changes, OSPF recalculates the shortest path, and sets the interval to prevent frequent network changes from occupying a large number of resources</p> <p>Waiting Interval: When the state changes, the timer is triggered. The delay is calculated for the first time after the timer expires. The default value is 0 ms.</p> <p>Min Interval: As the number of changes increases, the time of each interval will increase according to the algorithm, and the default value is 50 ms.</p> |

| Parameter | Description |
|------------------|---|
| | <p>Max Interval: When the calculated interval reaches the maximum interval, the subsequent interval is always equal to the maximum interval. If the time from the last calculation exceeds the maximum interval and the LSDB is not updated, the timer is disabled.</p> |
| Graceful Restart | <p>Graceful Restart (GR) can avoid route flapping caused by traffic interruption and active/standby board switchover, thus ensuring the stability of key services.</p> <p>Graceful Restart Helper: The Graceful Restart Helper function is enabled when this switch is turned on.</p> <p>LSA Check: LSA packets outside the domain are checked when this switch is turned on.</p> <p>Max Wait Time: Timing starts after the device receives the GR packet from the peer device. If the peer device does not complete GR within Max Wait Time, the device exits the GR Helper mode. The default value is 1800 seconds.</p> |

2. Configure an interface.

① — ② — ③
 Configure the instance. Configure the interface. **Operation succeeded.**

* Interface

* Area

Stub Area ☐

[Details](#)

Port List

Up to **16** entries can be added.

| Interface | Area | Priority | Network Type | Hello Packets | Dead Interval | LSA Transmission Delay | LSA Retransmission Interval | Action |
|-----------|------|----------|--------------|---------------|---------------|------------------------|-----------------------------|--------|
| No Data | | | | | | | | |

< 1 >

10/page

Go to page

Total 0

Table 11-16 Interface Configuration Parameters

| Parameter | Description |
|-----------|---|
| Interface | Select the OSPF-enabled L3 interface. |
| Area | Configure the area ID. Value range: 0-4294967295 |
| Stub Area | <p>If Stub Area is enabled, you need to configure the area type and inter-area route isolation.</p> <p>Stub area: Routers at the edge of the area do not advertise routes outside the area, and the routing table in the area is small.</p> <p>Not-So-Stubby Area (NSSA): A few external routes can be imported.</p> |
| Details | Expand the detailed configuration. |

① — ② — ③
 Configure the instance. Configure the interface. **Operation succeeded.**

Details

Priority

Network Type

Hello Packets

Dead Interval

[Add](#)

Port List

Up to **16** entries can be added.

| Interface | Area | Priority | Network Type | Hello Packets | Dead Interval | LSA Transmission Delay | LSA Retransmission Interval | Action |
|-----------|------|----------|--------------|---------------|---------------|------------------------|-----------------------------|--------|
| No Data | | | | | | | | |

[<](#) 1 [>](#)

10/page

Go to page

Total 0

[Previous](#)
[Finish](#)

1

2

3

Configure the instance. Configure the interface. **Operation succeeded.**

LSA Transmission Delay

Optional.Default:1(s)

LSA Retransmission Interval

Optional.Default:5(s)

Ignore MTU Check

☒

Add

Port List

Up to 16 entries can be added.

| Interface | Area | Priority | Network Type | Hello Packets | Dead Interval | LSA Transmission Delay | LSA Retransmission Interval | Action |
|-----------|------|----------|--------------|---------------|---------------|------------------------|-----------------------------|--------|
| No Data | | | | | | | | |

<1>

10/page

Go to page 1

Total 0

Previous

Finish

① — ② — ③
 Configure the instance. Configure the interface. **Operation succeeded.**

LSA Transmission Delay

Optional.Default:1(s)

LSA Retransmission Interval

Optional.Default:5(s)

Ignore MTU Check

☒

[Add](#)

Port List

Up to **16** entries can be added.

| Interface | Area | Priority | Network Type | Hello Packets | Dead Interval | LSA Transmission Delay | LSA Retransmission Interval | Action |
|-----------|------|----------|--------------|---------------|---------------|------------------------|-----------------------------|--|
| Gi2/14 | 12 | | Broadcast | | | | | Delete |

[<](#) 1 [>](#)

10/page Go to page 1

Total 1

[Previous](#)
[Finish](#)

Table 11-17 Parameters in the Interface Detailed Configuration

| Parameter | Description |
|-----------------------------|---|
| Priority | It is 1 by default. |
| Network Type | Broadcast Unicast Multicast Non-Broadcast Multiple Access |
| Hello Packets | Interval for periodic transmission, which is used to discover and maintain OSPF neighbor relationship. The default value is 10 seconds. |
| Dead Interval | Time after which the neighbor becomes invalid. The default value is 40 seconds. |
| LSA Transmission Delay | LSA transmission delay of the interface. The default value is 1 second. |
| LSA Retransmission Interval | Time after which LSA is retransmitted after LSA is lost. The default value is 5 seconds. |
| Header Certification | No auth: Default without verification. MD5 auth: Verifies the protocol message. The authentication secret |

| Parameter | Description |
|--------------------|--|
| | <p>key is encrypted through MD5 and transmitted together with the protocol message.</p> <p>SHA1 auth: Verifies the protocol message. The authentication secret key is encrypted through SHA1 and transmitted together with the protocol message.</p> <p>SHA256 auth: Verifies the protocol message. The authentication secret key is encrypted through SHA256 and transmitted together with the protocol message.</p> <p>After selecting MD5, SHA1, or SHA256 authentication, you need to enter Kid and Key. Among them, Kid is the key identifier, and Key is the actual secret key used.</p> |
| Tail Certification | <p>No auth: Default without verification.</p> <p>MD5 auth: Verifies the protocol message. The authentication secret key is encrypted through MD5 and transmitted together with the protocol message.</p> <p>SHA256 auth: Verifies the protocol message. The authentication secret key is encrypted through SHA256 and transmitted together with the protocol message.</p> <p>After selecting MD5, SHA1, or SHA256 authentication, you need to enter Kid and Key. Among them, Kid is the key identifier, and Key is the actual secret key used.</p> |
| Interface Auth | <p>No Auth: The protocol packets are not authenticated. It is the default value.</p> <p>Plain Text: The protocol packets are authenticated, and the authentication key is transmitted with the protocol packets in the form of plain text.</p> <p>MD5: The protocol packets are authenticated, and the authentication key is MD5 encrypted and then transmitted with the protocol packets.</p> |
| Ignore MTU Check | Enabled by default. |

3. Complete the configuration.

Operation succeeded.

1

2

3

Configure the instance. Configure the interface. Operation succeeded.

✓

Operation succeeded.

Disable

After completing the configuration, you can choose **Local Device > Routing > OSPFv3** and view the instance list.

11.6.2 Adding an OSPFv3 Interface

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

OSPFv3

Up to 1 entries can be added.

| Router ID | Interface | Area | Advertise Default Route | Import External Route | Distance | SPF Calculation | Graceful Restart Helper | Action |
|-----------|-----------|-----------------|-------------------------|---|----------|-----------------|-------------------------|--|
| 2.2.2.2 | Gi2/14 | 12(Normal Area) | Disable | <div><div>S</div><div>Redis</div><div>D</div><div>Redis</div><div>Redistribution</div><div>RIP Redistribution</div><div>: Off</div></div> | | | | <div><div>More</div><div>Neighbor Info</div><div>Edit</div><div>Delete</div></div> |

< 1 >

10/page

Go to page 1

Total 1

V3 Interface
×

Interface

* Area

Priority

Network Type

Hello Packets

Dead Interval

Port List
Add
Reset

Up to 64 entries can be added.

| Interface | Area | Priority | Network Type | Hello Packets | Dead Interval | LSA Transmission Delay | LSA Retransmission Interval | Action |
|-----------|------|----------|--------------|---------------|---------------|------------------------|-----------------------------|---|
| Gi2/14 | 12 | | Broadcast | | | | | Edit Delete |

<
1
>
10/page
Go to page

Total 1

11.6.3 Managing OSPFv3 Stub Areas

Choose **Local Device** > **Routing** > **OSPFv3**, click **More** in the **Action** column, and select **V3 Stub Area Management**.

V3 Stub Area Management
×

* Area ID

Area Type

Inter-Route Isolation ☐

Area List
Add
Reset

Up to 64 entries can be added.

| Area ID | Area Type | Inter-Route Isolation | Action |
|---------|-----------|-----------------------|--------|
| No Data | | | |

<
1
>
10/page
Go to page

Total 0

11.6.4 Viewing OSPFv3 Neighbor Information

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

×

Neighbor Info

| Router ID | Status | Interface |
|-----------|--------|-----------|
| No Data | | |

< 1 >

10/page

Go to page 1

Total 0

11.7 Routing Table Info

IPv4 IPv6

Route Info

Entry Type Global Data

Re-fetch

| Dest IP Address | Route Type | Distance/Metric | Interface | Next Hop |
|------------------|----------------|-----------------|-----------|---------------|
| 0.0.0.0/0 | System routing | [0/5] | VLAN 1 | 192.168.110.1 |
| 192.168.110.0/24 | Direct Routing | [0/0] | VLAN 1 | * |

< 1 >

10/page

Go to page 1

Total 2

IPv4 IPv6

Route Info

Entry Type Global Data

Re-fetch

| Dest IP Address | Route Type | Distance/Metric | Interface | Next Hop |
|-----------------|------------|-----------------|-----------|----------|
| No Data | | | | |

< 1 >

10/page

Go to page 1

Total 0

12 Security

12.1 DHCP Snooping

12.1.1 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.

12.1.2 Standalone Device Configuration

Choose **Local Device > Security > DHCP Snooping**.

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

Note

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

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

DHCP Snooping

Description: Enabling DHCP Snooping helps filter DHCP packets. The device only forwards DHCP request packets to the trusted port and DHCP response packets from the trusted port.

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

DHCP Snooping: ☒

Option 82: ☐

Select Trusted Port:

Available

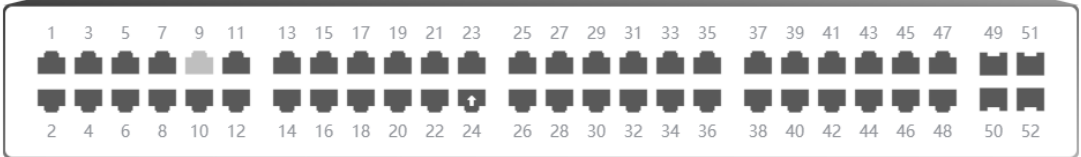
Unavailable

Aggregate

Uplink

Copper

Fiber



Note: You can click and drag to select one or more ports.

[Select All](#) [Inverse](#) [Deselect](#)

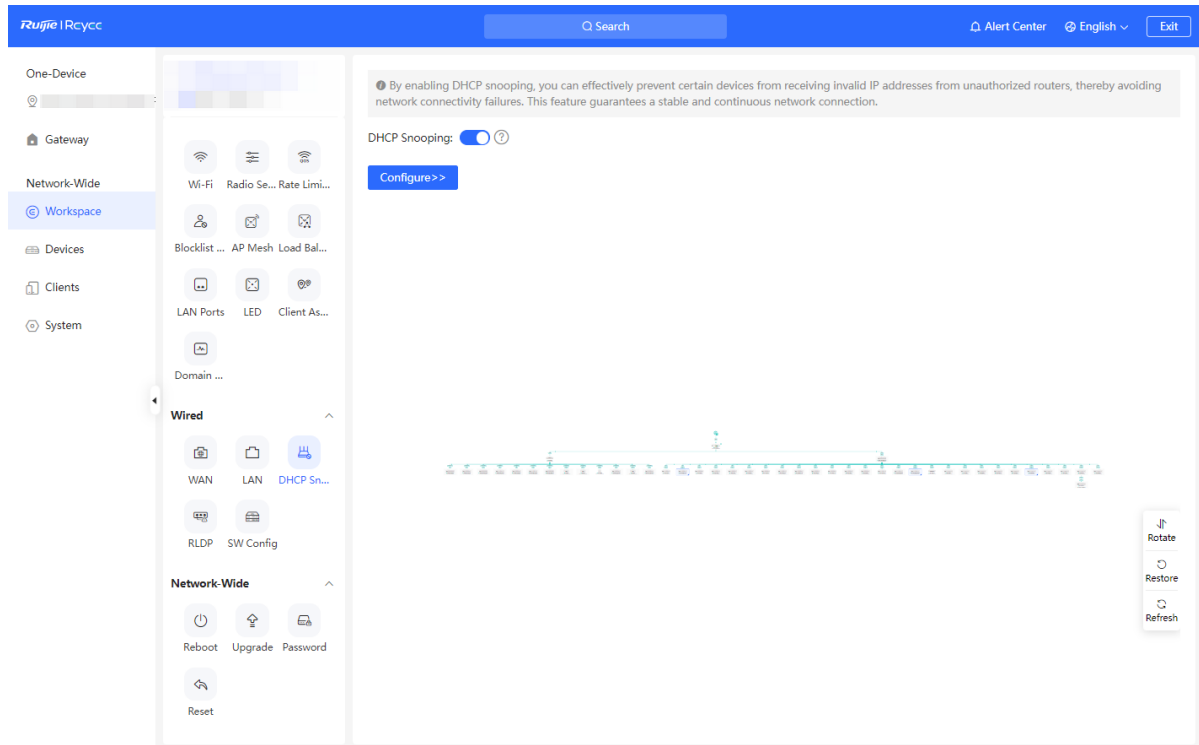
[Save](#)

12.1.3 Batch Configuring Network Switches

Choose **Network-Wide > Workspace > Wired > 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 a host on the original network obtaining an IP address assigned by an unauthorized router, so as to guarantee the stability of the network.

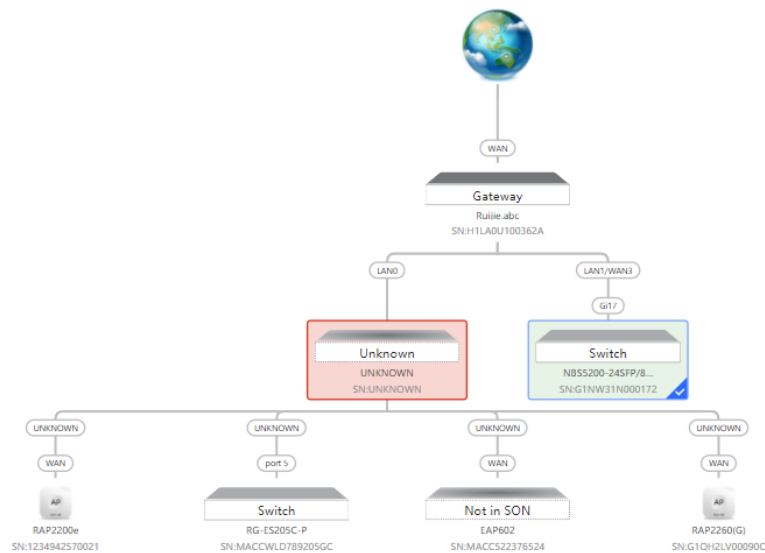
- (1) Click **Enable** to access the **DHCP Snooping Config** page.



- (2) On 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 on the network are selected automatically. If you select the custom mode, you can manually select the desired switches. Click **Deliver Config**. DHCP Snooping is enabled on the selected switches.

← DHCP Snooping Config

Please select the target switch:

Recommended
All SwitchesCustom
Specified Switches

Overturn

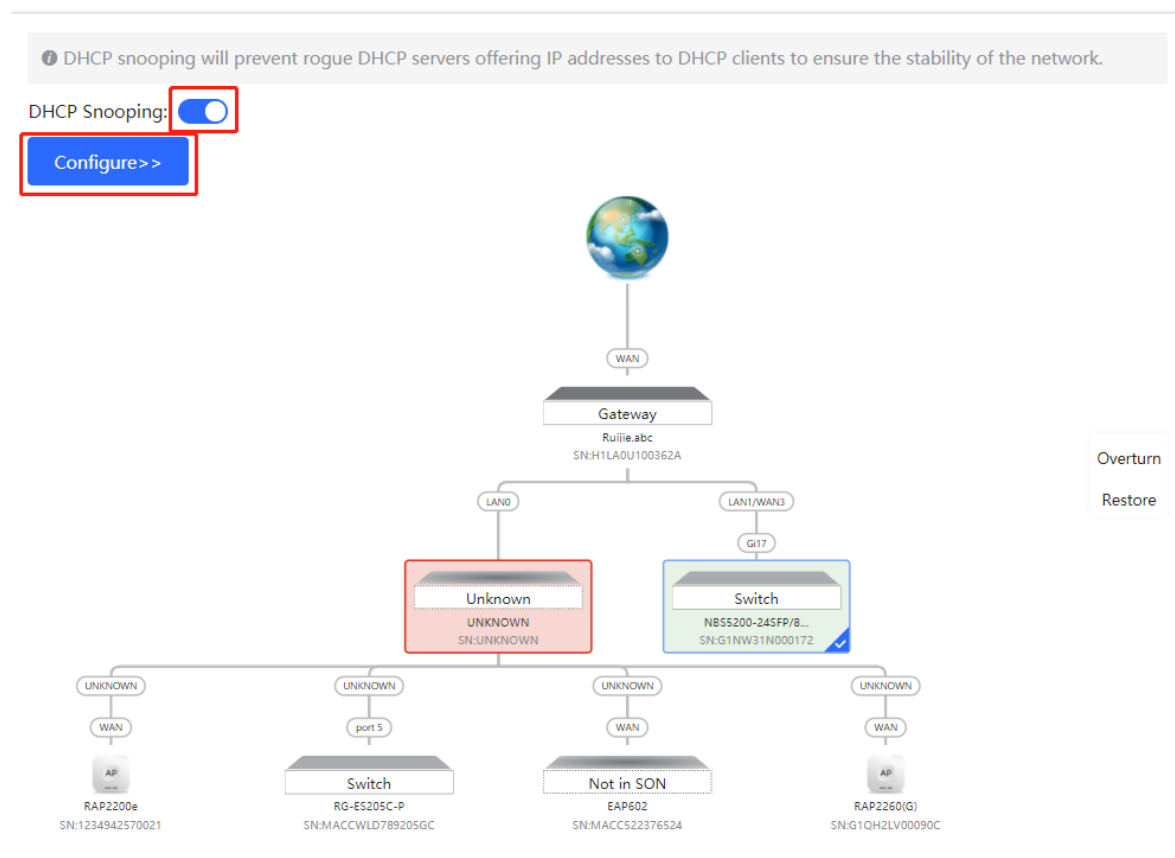
Restore

1 switches are selected.

Deliver Config

Cancel Config

- (3) After the configuration is delivered, if you need to modify the effective range of the anti-private connection function, click **Configure** to reselect the switch that enables the anti-private connection in the topology. 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.



12.2 Storm Control

12.2.1 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.

12.2.2 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 Selected](#)

| <input type="checkbox"/> | Port | Broadcast | Unknown Multicast | Unknown Unicast | Action |
|--------------------------|------|-----------|-------------------|-----------------|---|
| <input type="checkbox"/> | Gi35 | 1000pps | 1000pps | 1000pps | Edit Delete |

Batch Edit ×

Config Type: ☒ By Packet Count ☐ By Traffic Volume

Broadcast: pps Range: 1-14880952

Unknown Multicast: pps Range: 1-14880952

Unknown Unicast: pps Range: 1-14880952

* Select Port:

Available

Unavailable

Aggregate

Uplink

Copper

Fiber

1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37

2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38

Note: You can click and drag to select one or more ports.

[Select All](#)
[Inverse](#)
[Deselect](#)

Cancel

OK

12.3 ACL

12.3.1 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.

12.3.2 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**.

180

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.

[ACL List](#)
[ACL Binding](#)

ACL

[+ Add](#)
[Delete Selected](#)

Up to **512** entries can be added.

| | ACL Name | ACL Type | Status | Action |
|--|----------|----------|--------|--------|
|--|----------|----------|--------|--------|

No Data

Add

* ACL Name:

ACL Type:

☒ Based on MAC
 ☐ Based on IP Address

Cancel

OK

- (2) Click **Details** in the **Action** column of the ACL entry, set the filtering rules in the pop-up sidebar, and click **Save** to add rules for the ACL. Multiple rules can be added.

The rules include two actions of **Allow** or **Block**, and the matching rules of packets. The sequence of a Rule in an ACL determines the matching priority of the Rule in the ACL. When processing packets, the network device matches packets with ACEs based on the Rule sequence numbers. Click **Move** in the rule list to adjust the matching order.

[ACL List](#)
[ACL Binding](#)

ACL

[+ Add](#)
[Delete Selected](#)

Up to **512** entries can be added.

| | ACL Name | ACL Type | Status | Action |
|--------------------------|----------|--------------|----------|---|
| <input type="checkbox"/> | test | Based on MAC | Inactive | Details Edit Delete |

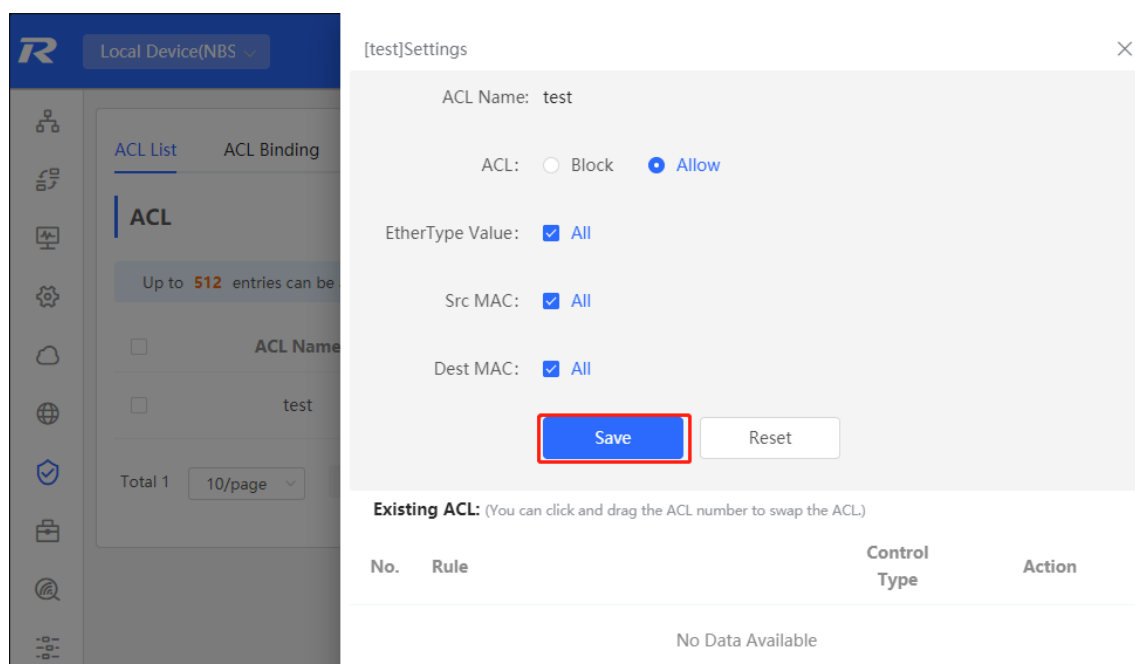


Table 12-1 Description of ACL Rule Configuration Parameters

| 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. |
| Src IP Address | Match the source IP address of the packet. Check All to match all source IP addresses. |
| Dest IP Address | Match the destination IP address of the packet. Check All to match all destination IP addresses |
| EtherType Value | Match Ethernet protocol type. The value range is 0x600~0xFFFF. Check All to match all protocol type numbers. |
| Src Mac | Match the MAC address of the source host. Check All to match all source MAC addresses |
| Dest MAC | Match the MAC address of the destination host. Check All to match all destination MAC addresses |

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.

12.3.3 Applying ACL Rules


Choose **Local Device** > **Security** > **ACL** > **ACL List**.

Click **Batch Add** or **Edit** in the **Action** column, select the desired MAC ACL and IP 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 List ACL Binding

 **ACL Binding**
 The device only filters incoming packets.

ACL Binding

+ Batch Add

Unbind Selected

| | Port | MAC-based ACL | IP-based ACL | Action |
|--------------------------|------|---------------|--------------|---|
| <input type="checkbox"/> | Gi1 | -- | -- | Edit Unbind |
| <input type="checkbox"/> | Gi2 | -- | -- | Edit Unbind |
| <input type="checkbox"/> | Gi3 | -- | -- | Edit Unbind |
| <input type="checkbox"/> | Gi4 | -- | -- | Edit Unbind |

Add
×

MAC-based ACL: No Data

IP-based ACL: No Data

*** Select Port:**

Available
 Unavailable
 Aggregate
 Uplink
 Copper
 Fiber

1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37

2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38

Note: You can click and drag to select one or more ports.

Select All
Inverse
Deselect

Cancel
OK

After an ACL is applied to a port, you can click **Unbind** in the **Action** column, or check the port entry and click **Delete Selected** to unbind the ACL from the port.

ACL List [ACL Binding](#)

ACL Binding
The device only filters incoming packets.

ACL Binding + Batch Add Unbind Selected

| <input type="checkbox"/> | Port | MAC-based ACL | IP-based ACL | Action |
|--------------------------|------|---------------|--------------|---|
| <input type="checkbox"/> | Gi1 | test | -- | Edit Unbind |
| <input type="checkbox"/> | Gi2 | -- | -- | Edit Unbind |

12.4 Port Protection

Choose **Local Device** > **Security** > **Port Protection**.

In some scenarios, it is required that communication be disabled between some ports on the device. For this purpose, you can configure some ports as protected ports. Ports that enable port protection (protected ports) cannot communicate with each other, users on different ports are L2-isolated. The protected ports can communicate with non-protected ports.

Port protection is disabled by default, which can be enabled by clicking to batch enable port protection for multiple ports, you can click **Batch Edit** to enable port protection, select desired port and click **OK**.

Port Protection
The protected ports are isolated from each other.

Port List Batch Edit

| Port | Action |
|------|-------------------------------------|
| Gi1 | <input checked="" type="checkbox"/> |
| Gi2 | <input type="checkbox"/> |
| Gi3 | <input type="checkbox"/> |
| Gi4 | <input type="checkbox"/> |
| Gi5 | <input type="checkbox"/> |

12.5 IP-MAC Binding

12.5.1 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.

12.5.2 Procedure

Choose **Local Device** > **Security** > **IP-MAC Binding**.

1. Adding an IP-MAC Binding Entry

Click **Add**, select the desired port, enter the IP address and MAC address to be bound, and click **OK**. At least one of the IP address and MAC address needs to be entered. To modify the binding, you can click **Edit** in the **Action** column.

Caution

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

IP-MAC Binding

Description: IP-MAC Binding checks both the source IP addresses and MAC addresses of IP packets, and packets not matching any entry in the address binding list will be filtered.

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

IP-MAC Binding Search by IP Address

Up to **500** entries can be added.

| | IP | MAC | Port | Action |
|--------------------------|-------------|-------------------|------|---|
| <input type="checkbox"/> | 192.168.1.1 | 00:11:22:33:44:55 | Gi29 | Edit Delete |

Add ×

IP ?

MAC

*** Select Port:**

☒ Available ☐ Unavailable
☒ Aggregate ☐ Uplink ☐ Copper ☐ Fiber

| | | | | | | | | | | | | | | | | | | |
|---|---|---|---|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|
| 1 | 3 | 5 | 7 | 9 | 11 | 13 | 15 | 17 | 19 | 21 | 23 | 25 | 27 | 29 | 31 | 33 | 35 | 37 |
| 2 | 4 | 6 | 8 | 10 | 12 | 14 | 16 | 18 | 20 | 22 | 24 | 26 | 28 | 30 | 32 | 34 | 36 | 38 |

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

2. 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.

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 **Action** column of the entry in the list. In the displayed dialog box, click **OK**.

12.6 IP Source Guard

12.6.1 Overview

After the IP Source Guard function is enabled, the device checks IP packets from DHCP non-trusted ports. You can configure the device to check only the IP field or IP+MAC field to filter out IP packets not matching the binding list. It can prevent users from setting private IP addresses and forging IP packets.

Caution

IP Source Guard should be enabled together with DHCP snooping. Otherwise, IP packet forwarding may be affected. To configure DHCP Snooping function, see [12.1 DHCP Snooping](#) for details.


12.6.2 Viewing Binding List

Choose **Local Device** > **Security** > **IP Source Guard** > **Binding List**.

The binding list is the basis for IP Source Guard. Currently, data in **Binding List** is sourced from dynamic learning results of DHCP snooping binding database. When IP Source Guard is enabled, data of the DHCP Snooping binding database is synchronized to the binding list of IP Source Guard. In this case, IP packets are filtered strictly through IP Source Guard on devices with DHCP Snooping enabled.

Click **Refresh** to obtain the latest data in **Binding List**.

Basic Settings Excluded VLAN Binding List


Binding List
 Description: The entries come from dynamic learning of DHCP Snooping.

Binding List

Search by IP Address ▾

Up to **1900** entries can be added.

| IP | MAC | Port | VLAN ID | Status | Rule |
|---------|-----|------|---------|--------|------|
| No Data | | | | | |

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

Search by IP Address ▴

Search by IP Address
 Search by MAC
 Search by VLAN
 Search by Port

| VLAN ID | Status |
|---------|--------|
| Data | |

12.6.3 Enabling Port IP Source Guard

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

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

There are two match rules:

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

Caution

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

Basic Settings Excluded VLAN Binding List

Basic Settings

Description: Enable IP Source Guard to check the IP fields or both IP and MAC fields of packets from untrusted ports. Packets not matching any entry in the address binding list will be filtered. It can prevent IP spoofing attacks when a host tries to spoof and use the IP address of another host.
Note: IP Source Guard should be enabled together with DHCP Snooping. Otherwise, IP packet forwarding may be affected.

Port List

[Batch Edit](#)

| Port | Enable | Rule | Action |
|------|----------|------|----------------------|
| Gi1 | Disabled | IP | Edit |
| Gi2 | Disabled | IP | Edit |
| Gi3 | Disabled | IP | Edit |

Edit

Enable

Enabled

Rule

IP

IP

IP+MAC

Cancel

OK

12.6.4 Configuring Exceptional VLAN Addresses

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

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

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

Caution

Excluded VLANs can be specified on a port only after IP Source Guard is enabled on the port. Specified excluded VLANs will be deleted automatically when IP Source Guard is disabled on the port.

Basic Settings Excluded VLAN Binding List

Excluded VLAN

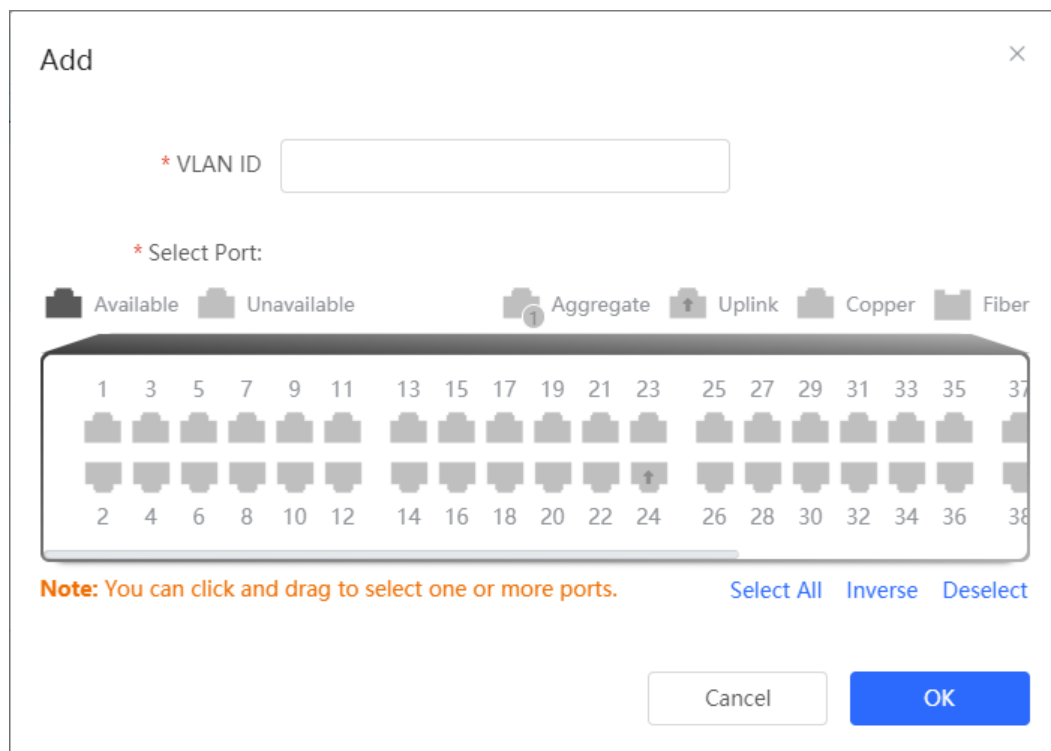
Description: Packets within this VLAN are allowed to pass the port without checking or filtering.
Note: Excluded VLAN can be specified only after IP Source Guard is enabled on a port.

VLAN List

[+ Add](#)
[Delete Selected](#)

Up to 64 entries can be added.

| | VLAN ID | Port | Action |
|--|---------|------|--------|
| | No Data | | |



12.7 Configure 802.1x authentication

12.7.1 Function introduction

IEEE802.1x (Port-Based Network Access Control) is a port-based network access control standard that provides secure access services for LANs.

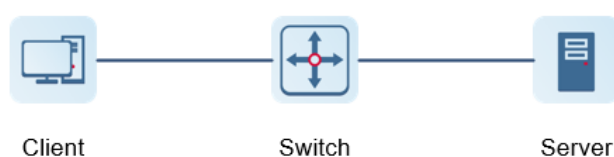
IEEE 802 LAN, as long as users can connect to network devices, they can directly access network resources without authentication and authorization. This uncontrolled behavior will bring security risks to the network. The IEEE 802.1x protocol was proposed to solve the security problem of 802 LAN.

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.

12.7.2 Configuration 802.1x

Choose **Local Device > Security > 802.1x Authentication > Auth Config**

Toggle on **Global 802.1x**, the system prompts to confirm whether to enable it, click **Configure**.

[Auth Config](#) [Port](#) [RADIUS Server Management](#) [Wired User List](#)

Global Config

Global 802.1x ☒

Authentication

Auth Server [Edit](#)

[Advanced Settings](#)

Configure

Click Advanced Settings to configure parameters such as Guest VLAN.

[Auth Config](#) [Port](#) [RADIUS Server Management](#) [Wired User List](#)

Guest Vlan ☐

* EAP-Request Packet

Retransmission Count

* Quiet Period s

Client Packet
* Timeout Duration s

Client Packet
* Timeout Duration s

* EAP-Request Packet s

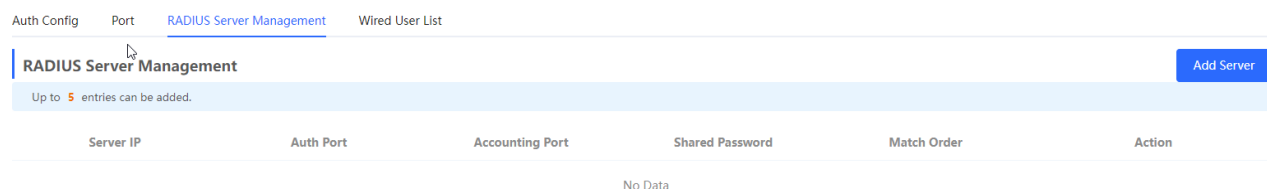
Interval

| parameter | 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 |
| Client Packet Timeout Duration | The time limit for the client to wait for the server to respond, exceeding this time will be considered as an authentication failure, value range: 1-65535 seconds |
| EAP-Request Packet Interval | Define the time interval between sending EAP request messages to control the rate of the authentication process, value range: 1-65535 seconds |

(1) add server

Before configuration, please confirm:

- The Radius server is fully built and configured as follows.
 - Add username and password for client login.
 - Close the firewall, otherwise the authentication message may be intercepted, resulting in authentication failure.
 - A trusted IP on the Radius server.
- The network connection between the authentication device and the Radius server.
- IP addresses of the Radius server and the authentication device have been obtained.



×

Add

* Server group name

----- ☐ Server 1 -----

* Server IP

* Server name

* Auth Port

* Accounting Port ?

* Shared Password

* Match Order ?

----- ⦿ Add Server -----

| parameter | Reference without translation | Description |
|-------------------|-------------------------------|--|
| Server group name | | Server group name |
| Server IP | server address | Radius server address. |
| Auth Port | authentication port | The port number used for accessing user authentication on the Radius server. |
| Accounting Port | billing port | The port number used to access the accounting process on the Radius server. |
| Shared Password | shared password | Radius server shared key. |
| Match Order | matching order | The system supports adding up to 5 Radius servers. The higher the matching order value is, the higher the priority is. |

(3) Set up the server and click **Save**.

Server global configuration

* Packet Retransmission Interval

3

s

* Packet Retransmission Count

3

time

Server Detection

☐

MAC Address Format

XXXXXXXXXXXX

?

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-Station-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), e.g. 00d0f8aabbcc |

- (4) Configure the effective interface, click interface configuration, click modify or batch configuration after a single interface, and edit the authentication parameters of the interface.

Auth Config

Port

RADIUS Server Management

Wired User List

Port List

Batch Config

| Interface | Port Authentication | Auth Method | Auth Mode | Action |
|-----------|---------------------|-------------|------------|--------|
| Gi1 | Off | disable | multi-auth | Edit |
| Gi2 | Off | disable | multi-auth | Edit |

Edit

✕

802.1x Authentication ☒Auth Method disable ▾Auth Mode multi-auth ▾Guest Vlan ☐* User Count Limit per 1000

Port

Cancel

OK

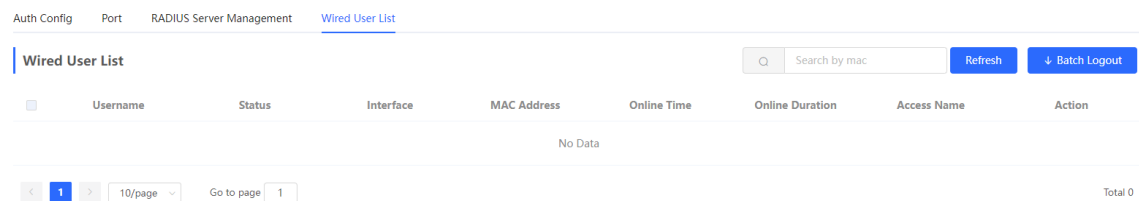
| parameter | Description |
|---------------------------|--|
| 802.1x Authentication | When enabled, the selected interface will enable 802.1x authentication. |
| Auth Method | <p>disable: Turn off the authentication method, which has the same effect as turning off the 802.1x authentication switch</p> <p>force-auth: Mandatory authentication, the client can directly access the Internet without a password</p> <p>force-unauth: force no authentication, the client cannot authenticate and cannot access the Internet</p> <p>auto: automatic authentication, the device needs to be authenticated, and can access the Internet after passing the authentication</p> <p>It is recommended to select the auto authentication method.</p> |
| Auth Mode | <p>multi-auth: Supports multiple devices using the same port for authentication, but each device needs to be authenticated independently</p> <p>multi-host: Multiple devices are allowed to share the same port. As long as one user passes the authentication, subsequent users can access the Internet</p> <p>single-host: Each port only allows one device to be authenticated, and can access the Internet after successful authentication</p> |
| Guest Vlan | <p>When enabled, devices that fail authentication will be dynamically assigned to the specified Guest VLAN</p> <p>Notice</p> <p>You need to create a VLAN ID first and apply it to the interface, then in Security Management > 802.1x Authentication > Advanced settings in the authentication configuration enable Guest VLAN and enter the ID</p> |
| User Count Limit per Port | Limit the number of users under the interface |

| parameter | Description |
|-----------|--|
| | Product Difference Description The value range of NBS3100 series switches is 1-256, and other switches are 1-1000 |

12.7.3 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.



Click <Refresh> to get the latest user list information.

If you want to disconnect a certain user from the network, you can select the user and click <Offline> in the "Operation" column; you can also select multiple users and click <Batch Offline>.

12.8 Anti-ARP Spoofing

12.8.1 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.

12.8.2 Procedure

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

1. Enabling Anti-ARP Spoofing

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

Note

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

Anti-ARP Spoofing

Description: Anti-ARP Spoofing prevents hosts from spoofing the source IP address of the ARP packets to be the IP address of the gateway.
Note: Anti-ARP Spoofing is generally configured on a downlink port.

Anti-ARP Spoofing

Add

Delete Selected

Up to 256 entries can be added.

| | IP | Port | Action |
|---------|----|------|--------|
| No Data | | | |

Add

* IP

192.168.1.1

* Select Port:

AvailableUnavailableAggregateUplinkCopperFiber

135791113151719212325272931333537

2468101214161820222426283032343638

Note: You can click and drag to select one or more ports.

Select AllInverseDeselect

Cancel

OK

2. Disabling Anti-ARP Spoofing

Batch disable: Select an entry to be deleted in the list and click **Delete Selected**.

Disable one port: click **Delete** in the **Action** column of the corresponding entry.

Anti-ARP Spoofing

Description: Anti-ARP Spoofing prevents hosts from spoofing the source IP address of the ARP packets to be the IP address of the gateway.
Note: Anti-ARP Spoofing is generally configured on a downlink port.

Anti-ARP Spoofing

Add

Delete Selected

Up to 256 entries can be added.

| | IP | Port | Action |
|-------------------------------------|--------------|------|---|
| <input checked="" type="checkbox"/> | 172.30.102.1 | Gi15 | <div><div>Edit</div><div>Delete</div></div> |

196

13 Advanced Configuration

13.1 STP

STP (Spanning Tree Protocol) is an L2 management protocol that eliminates L2 loops by selectively blocking redundant links on the network. It also provides the link backup function.

[STP Settings](#) [STP Management](#)

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

STP: ☒

| | | | | | |
|------------------|------------------------------------|---------|------------------|-----------------------------------|---------|
| * Priority: | <input type="text" value="32768"/> | | * Hello Time: | <input type="text" value="2"/> | seconds |
| * Max Age: | <input type="text" value="20"/> | seconds | * Forward Delay: | <input type="text" value="15"/> | seconds |
| * Recovery Time: | <input type="text" value="30"/> | seconds | STP Mode: | <input type="text" value="RSTP"/> | |

Save

13.1.1 STP Global Settings

Choose **Local Device** > **Advanced** > **STP** > **STP**.

(1) Click to enable the STP function, and click OK in the displayed box. The STP function is disabled by default.

Caution

- After enabling the STP configuration of the device, the ERPS configuration cannot take effect normally.
- Enabling the STP or changing the STP mode will initiate a new session. Do not refresh the page during the configuration.

[STP Settings](#) [STP Management](#)

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

STP: ☒

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

STP Settings

STP Management

**Note:** Enabling STP or changing the STP mode will initiate a new session. Please do not refresh the page.STP: ☒* Priority: * Hello Time: seconds* Max Age: seconds* Forward Delay: seconds* Recovery Time: secondsSTP Mode: **Table 13-1 Description of STP Global Configuration Parameters**

| Parameter | Description | Default Value |
|---------------|--|---------------|
| STP | Whether to enable the STP function. It takes effect globally. STP attributes can be configured only after STP is enabled. | Disable |
| Priority | Bridge priority. The device compares the bridge priority first during root bridge selection. A smaller value indicates a higher priority. | 32768 |
| Max Age | The maximum expiration time of BPDUs. The packets expiring will be discarded. If a non-root bridge fails to receive a BPDU from the root bridge before the aging time expires, the root bridge or the link to the root bridge is deemed as faulty. | 20 seconds |
| Recovery Time | Network recovery time when redundant links occur on the network. | 30 seconds |
| Hello Time | Interval for sending two adjacent BPDUs. | 2 seconds |
| Forward Delay | The interval at which the port status changes, that is, the interval for the port to change from Listening to Learning, or from Learning to Forwarding. | 15 seconds |
| STP Mode | The versions of Spanning Tree Protocol. Currently the device supports STP (Spanning Tree Protocol) and RSTP (Rapid Spanning Tree Protocol). | RSTP |

13.1.2 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 Management](#)**STP Port Settings****Tip:** It is recommended to enable the port connected to a PC with Port Fast.**Port List**[Refresh](#)[Batch Edit](#)

| Port | Role | Status | Priority | Link Status | | BPDU Guard | Port Fast | Action |
|------|---------|---------|----------|---------------|---------------|------------|-----------|----------------------|
| | | | | Config Status | Actual Status | | | |
| Gi1 | disable | disable | 128 | Auto | Shared | Disable | Disable | Edit |
| Gi2 | disable | disable | 128 | Auto | Shared | Disable | Disable | Edit |
| Gi3 | disable | disable | 128 | Auto | Shared | Disable | Disable | Edit |

Port:Gi1

Port Fast: ☐

BPDU Guard: ☐

Link Status:

* Priority:

Cancel

OK

Table 13-2 Description of STP Configuration Parameters of Ports

| Parameter | Description | Default Value |
|-----------|--|---------------|
| Role | <ul style="list-style-type: none"> Root: A port with the shortest path to the root Alternate: A backup port of a root port. Once the root port fails, the alternate port becomes the root port immediately. Designated (designated ports): A port that connects a root bridge or an upstream bridge to a downstream device. Disable (blocked ports): Ports that have no effect in the spanning tree. | N/A |

| Parameter | Description | Default Value |
|------------------------------|--|---------------|
| Status | <ul style="list-style-type: none"> ● Disable: The port is closed manually or due to a fault, does not participate in spanning tree and does not forward data, and can be turned into a blocking state after initialization or opening. ● Blocking: A port in the blocking state cannot forward data packets or learn addresses, but can send or receive configuration BPDUs and send them to the CPU. ● Listening: If a port can become the root port or designated port, the port will enter the listening state. Listening: A port in the listening state does not forward data or learn addresses, but can receive and send configuration BPDUs. ● Learning: A port in the learning state cannot forward data, but starts to learn addresses, and can receive, process, and send configuration BPDUs. ● Forwarding: Once a port enters the state, it can forward any data, learn addresses, and receive, process, and send configuration BPDUs. | N/A |
| Priority | The priority of the port is used to elect the port role, and the port with high priority is preferentially selected to enter the forwarding state | 128 |
| Link Status Config Status | Configure the link type, the options include: Shared, Point-to-Point and Auto. In auto mode, the interface type is determined based on the duplex mode. For full-duplex ports, the interface type is point-to-point, and for half-duplex ports, the interface type is shared. | Auto |
| Link Status Actual Status | Actual link type: Shared, Point-to-Point | N/A |
| BPDU Guard | Whether to enable the BPDU guard function. After the function is enabled, if Port Fast is enabled on a port or the port is automatically identified as an edge port connected to an endpoint, but the port receives BPDUs, the port will be disabled and enters the Error-disabled state. This indicates that an unauthorized user may add a network device to the network, resulting in network topology change. | Disable |
| Port Fast | Whether to enable the Port Fast function. After Port Fast is enabled on a port, the port will neither receive nor send BPDUs. In this case, the host directly connected to the port cannot receive BPDUs. If a port, on which Port Fast is enabled exits the Port Fast state automatically when it receives BPDUs, the BPDU filter feature is automatically disabled. Generally, the port connected to a PC is enabled with Port Fast. | Disable |

Note

- It is recommended to enable Port Fast on the port connected to a PC.
- A port switches to the forwarding state after STP is enabled more than 30 seconds. Therefore transient disconnection may occur and packets cannot be forwarded.

13.2 LLDP

13.2.1 Overview

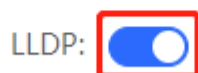
LLDP (Link Layer Discovery Protocol) is defined by IEEE 802.1AB. LLDP can discover devices and detect topology changes. With LLDP, the web interface can learn the topological connection status, for example, ports of the device that are connected to other devices, port rates at both ends of a link, and duplex mode matching status. An administrator can locate and troubleshoot faults quickly based on the preceding information.

13.2.2 LLDP Global Settings

Choose **Local Device** > **Advanced** > **LLDP** > **LLDP Settings**.

- (1) Click to enable the LLDP function, and click **OK** in the displayed box. The STP function is enabled by default. When the LLDP is enabled, this step can be skipped.

[LLDP Settings](#) [LLDP Management](#) [LLDP Info](#)



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

[LLDP Settings](#) [LLDP Management](#) [LLDP Info](#)

LLDP: ☒

* Hold Multiplier: * Reinitialization Delay: seconds

* Transmit Interval: seconds * Forward Delay: seconds

* Fast Count:

Table 13-3 Description of LLDP Global Configuration Parameters

| Parameter | Description | Default Value |
|-----------|---|---------------|
| LLDP | Indicates whether the LLDP function is enabled. | Enable |

| Parameter | Description | Default Value |
|------------------------|--|---------------|
| Hold Multiplier | TTL multiplier of LLDP In LLDP packets, TTL TLV indicates the TTL of local information on a neighbor. The value of TTL TLV is calculated using the following formula: $TTL\ TLV = TTL\ multiplier \times Packet\ transmission\ interval + 1$. The TTL TLV value can be modified by configuring the TTL multiplier and LLDP packet transmission interval. | 4 |
| Transmit Interval | Transmission interval of LLDP packets, in seconds The value of TTL TLV is calculated using the following formula: $TTL\ TLV = TTL\ multiplier \times Packet\ transmission\ interval + 1$. The TTL TLV value can be modified by configuring the TTL multiplier and LLDP packet transmission interval. | 30 seconds |
| Fast Count | Number of packets that are transmitted rapidly When a new neighbor is discovered, or the LLDP working mode is changed, the device will start the fast transmission mechanism in order to let the neighboring devices learn the information of the device as soon as possible. The fast transmission mechanism shortens the LLDP packet transmission interval to 1s, sends a certain number of LLDP packets continuously, and then restores the normal transmission interval. You can configure the number of LLDP packets that can be transmitted rapidly for the fast transmission mechanism. | 3 |
| Reinitialization Delay | Port initialization delay, in seconds You can configure an initialization delay to prevent frequent initialization of the state machine caused by frequent changes of the port work mode. | 2 seconds |
| Forward Delay | Delay for sending LLDP packets, in seconds. When local information of a device changes, the device immediately transmits LLDP packets to its neighbors. You can configure a transmission delay to prevent frequent transmission of LLDP packets caused by frequent changes of local information. If the delay is set to a very small value, frequent change of the local information will cause frequent transmission of LLDP packets. If the delay is set to a very large value, no LLDP packet may be transmitted even if local information is changed. Set an appropriate delay according to actual conditions. | 2 seconds |

13.2.3 Applying LLDP to a Port

Choose **Local Device > Advanced > LLDP > LLDP Management**.

In **Port List**, Click **Edit** in the **Action** column, or click **Batch Edit**, select the desired port, configure the LLDP working mode on the port and whether to enable LLDP-MED, and click **OK**.

Send LLDPDU: After **Send LLDPDU** is enabled on a port, the port can send LLDPDUs.

Receive LLDPDU: After **Receive LLDPDU** is enabled on a port, the port can receive LLDPDUs.

LLDPMED: After **LLDPMED** is enabled, the device is capable of discovering neighbors when its peer endpoint supports LLDP-MED (the Link Layer Discovery Protocol-Media Endpoint Discovery).

LLDP Settings [LLDP Management](#) LLDP Info

| Port List Batch Edit | | | | |
|---|-------------|----------------|----------|----------------------|
| Port | Send LLDPDU | Receive LLDPDU | LLDP-MED | Action |
| Gi1 | Enable | Enable | Enable | Edit |
| Gi2 | Enable | Enable | Enable | Edit |
| Gi3 | Enable | Enable | Enable | Edit |

Batch Edit ×

Send LLDPDU: ☐

Receive LLDPDU: ☐

LLDP-MED: ☐

* Select Port:

Available Unavailable

Uplink Copper Fiber

1 3 5 7 9 11 13 15 17 19 21 23 25 27 29 31 33 35 37

2 4 6 8 10 12 14 16 18 20 22 24 26 28 30 32 34 36 38

↑

Note: You can click and drag to select one or more ports.

[Select All](#)
[Inverse](#)
[Deselect](#)

Cancel

OK

13.2.4 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 on the network topology. When an administrator configures the VLAN, port rate, duplex mode, an error will be prompted if the configurations do not match those on the connected neighbor.

203

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 |

The screenshot shows the Ruijie Cloud management interface. On the left, the 'Local Device(NBS)' is selected. The main panel displays 'LLDP Settings' and 'LLDP Management' tabs, with 'LLDP Info' active. Under 'Device Info', the device is identified as 'Ruijie' with MAC address '00:11:22:33:44:67' and MGMT IP '172.30.102.133'. Under 'Neighbor Info', a table lists neighbors. The neighbor for 'Gi24' is highlighted with a red box. To the right, a pop-up window titled '[Gi24]Neighbor Details' shows the specific neighbor information for 'Gi3'.

[Gi24]Neighbor Details

Gi3

Device ID Type: MAC address Device ID: 30:0D:9E:6F:C2:3C
 Port ID Type: Locally assigned Port ID: Gi3
 Hostname: NBS3100 PVID: 1
 VLAN ID: 1(VLAN0001) Time To Live: 117
 MGMT IP: 172.30.102.121
 Description: RG-NBS3100-24GT4SFP-P
 Supported Feature: Bridge Enabled Feature: Bridge

13.3 RLDP

13.3.1 Overview

The Rapid Link Detection Protocol (RLDP) is an Ethernet link failure detection protocol, which is used to rapidly detect unidirectional link failures, bidirectional link failures, and downlink loop failures. When a failure is found, RLDP automatically shuts down relevant ports or asks users to manually shut down the ports according to the configured failure handling methods, to avoid wrong forwarding of traffic or Ethernet L2 loops.

Supports enabling the RLDP function of the access switches on 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

13.3.2 Standalone Device Configuration

1. RLDP Global Settings

Choose **Local Device** > **Advanced** > **RLDP** > **RLDP Settings**.


(1) Enable the RLDP function and click **OK** in the displayed dialog box. The RLDP function is disabled by default.

RLDP Settings RLDP Management RLDP Info

RLDP: 

(2) Configure RLDP global parameters and click **Save**.

RLDP Settings RLDP Management RLDP Info

RLDP: 

* Hello Interval:

3

seconds

Errdisable Recovery:



Save

Table 13-4 Description of RLDP Global Configuration Parameters

| Parameter | Description | Default Value |
|------------------------------|--|---------------|
| RLDP | Indicates whether the RLDP function is enabled. | Disable |
| Hello Interval | Interval for RLDP to send detection packets, in seconds | 3 seconds |
| Errdisable Recovery | After it is enabled, a port automatically recovers to the initialized state after a loop occurs. | Disable |
| Errdisable Recovery Interval | The interval at which the failed ports recover to the initialized state regularly and link detection is restarted, in seconds. | 30 seconds |

2. Applying RLDP to a Port

Choose **Local Device** > **Advanced** > **RLDP** > **RLDP Management**.

In **Port List**, click **Edit** in the Action column or click **Batch Edit**, select the desired port, configure whether to enable loop detection on the port and the handling method after a fault is detected, and click **OK**.

There are three methods to handle port failures:

- Warning: Only the relevant information is prompted to indicate the failed port and the failure type.

- Block: After alerting the fault, set the faulty port not to forward the received packets
- Shutdown port: After alerting the fault, shutdown the port.

Caution

- When RLDLP is applied to an aggregate port, the **Action** can only be set to **Warning** and **Shutdown**.
- When performing RLDLP 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 |

Port:Gi1

Loop Detection: ☒

Action: Warning

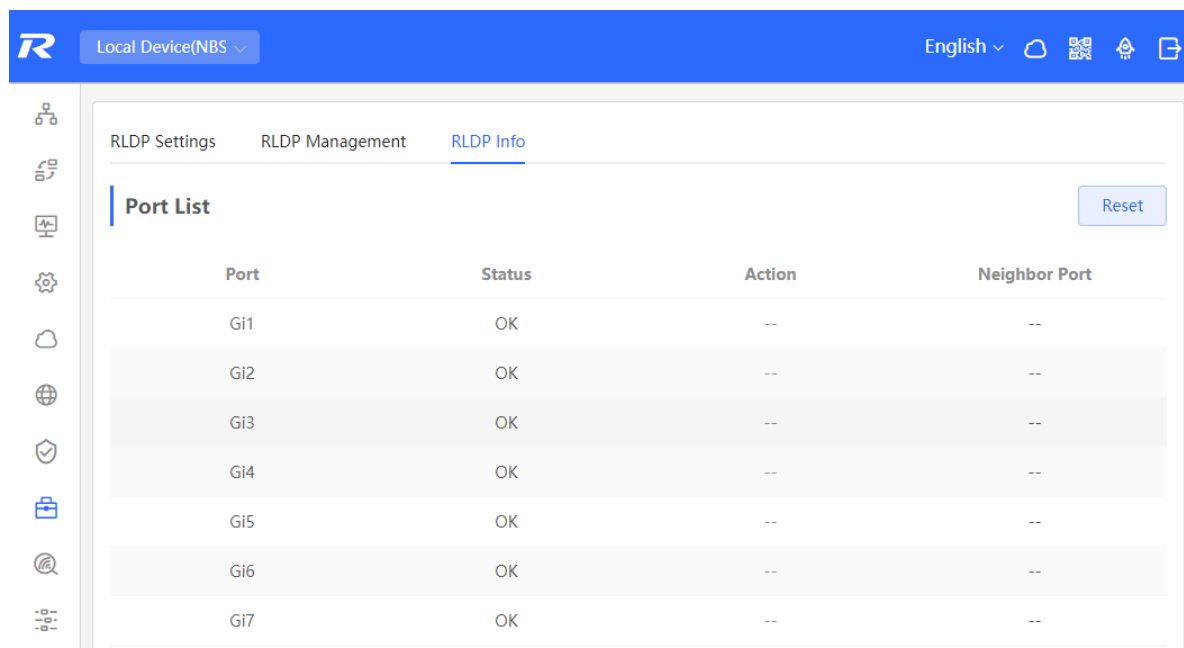
Warning
Block
Shutdown

OK

3. Displaying RLDLP information

Choose **Local Device** > **Advanced** > **RLDP** > **RLDP Info**.

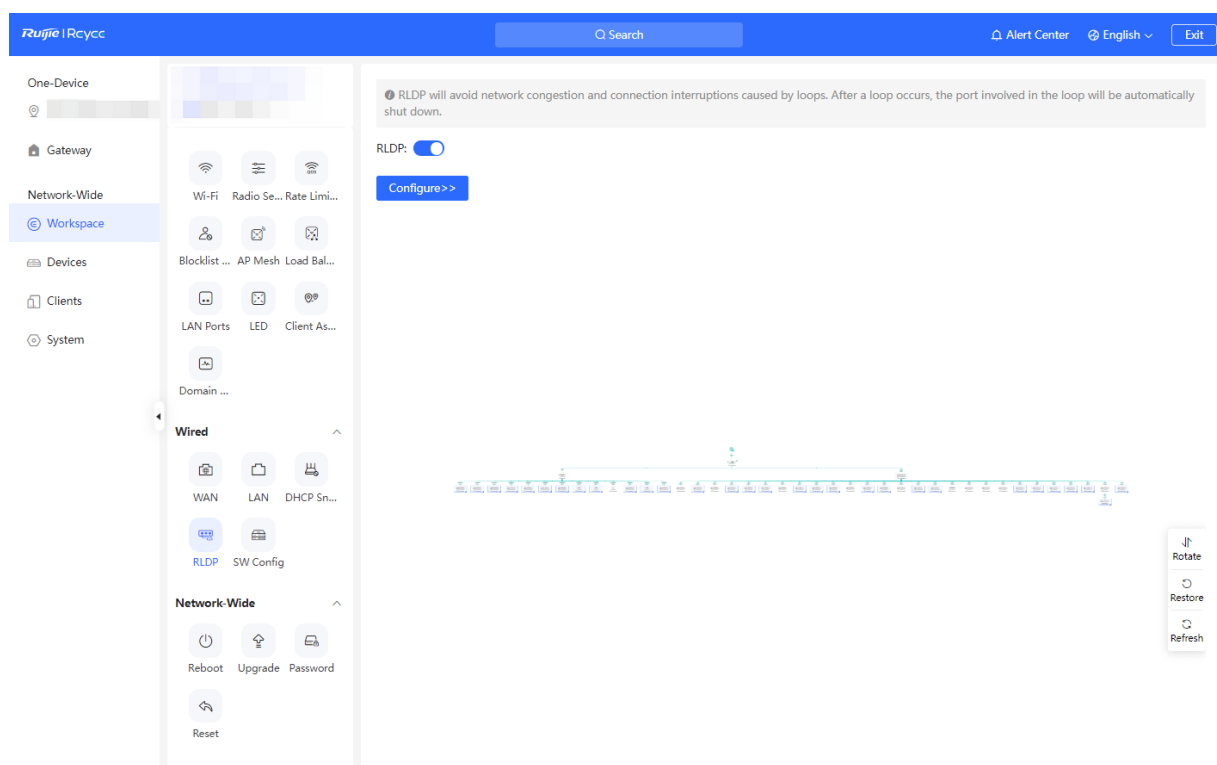
You can view the detection status, failure handling methods, and ports that connect the neighbor device to the local device. You can click **Reset** to restore the faulty RLDLP status triggered by a port to the normal state.



13.3.3 Batch Configuring Network Switches

Choose **Network-Wide > Workspace > Wired > RLDP**

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



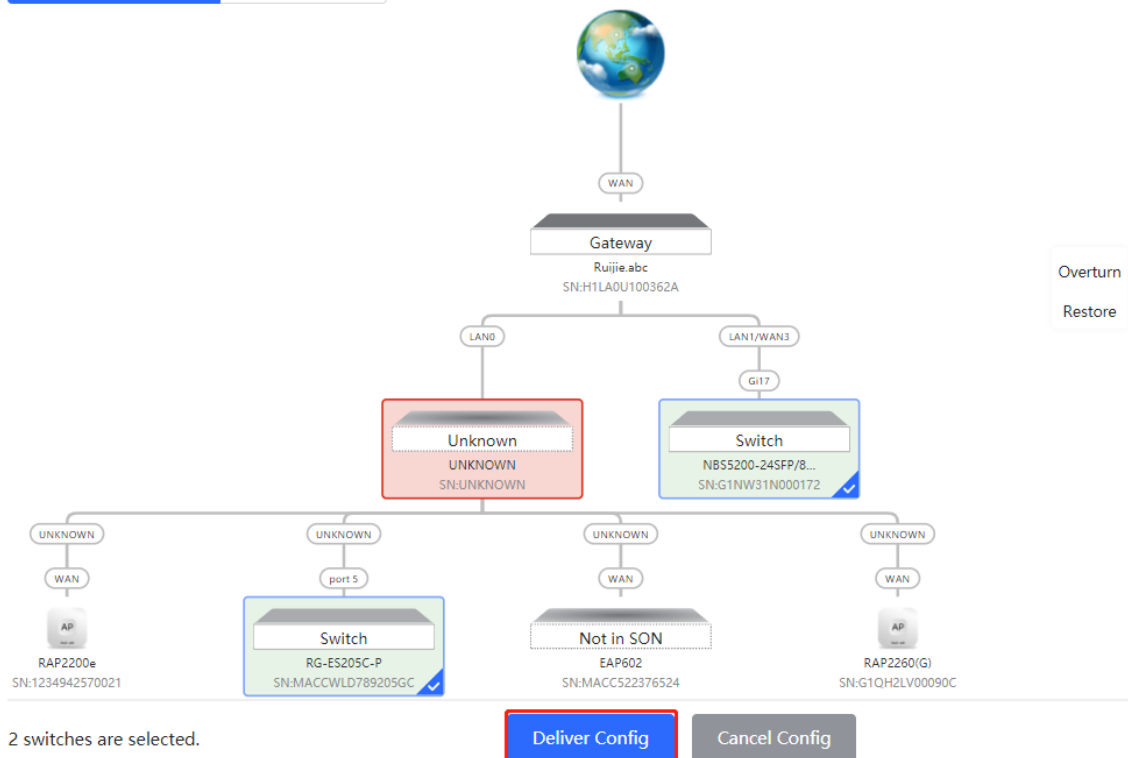
(2) On the networking topology, you can select the access switches on which you want to enable RLDP in either recommended or custom mode. If you select the recommended mode, all access switches on the network are selected automatically. If you select the custom mode, you can manually select the desired access switches. Click **Deliver Config**. RLDP is enabled on the selected switches.

← RLDP Config

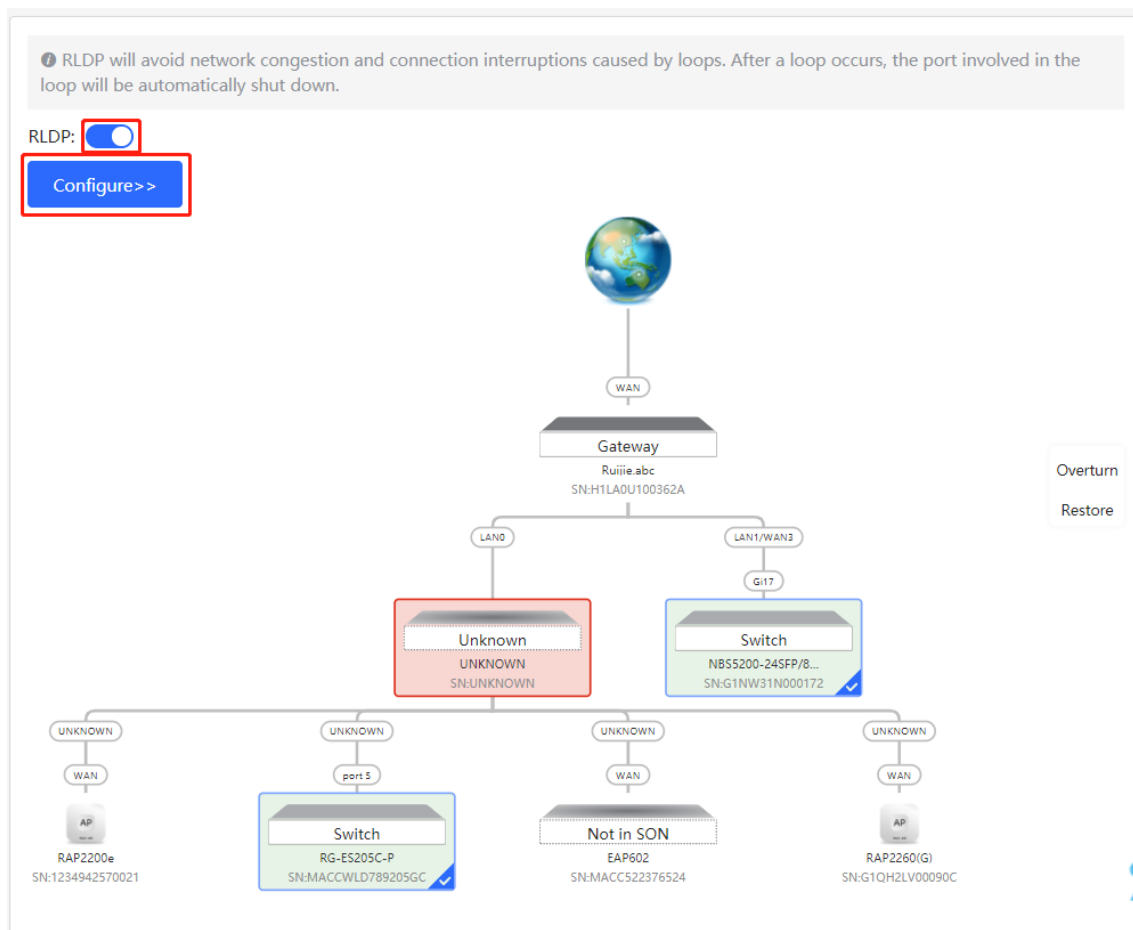
Please select the target switch:

Recommended
Auto-Identified Switches

Custom
Specified Switches



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



13.4 ERPS

✓ Specification

RG-NIS3100, RG-NBS3100, RG-NBS3200, and RG-NBS5100 series switches running ReyeeOS 2.280 or later support ERPS.

13.4.1 Overview

Ethernet Ring Protection Switching (ERPS), also known as G.8032, is a ring protection protocol developed by the International Telecommunication Union (ITU). It is a data link layer protocol specially designed for Ethernet rings. ERPS prevents broadcast storms caused by data loops when an Ethernet ring network is intact, and can rapidly perform link switching and recover the communication between nodes when a link is disconnected in the Ethernet ring, so as to implement data link redundancy.

Currently, the Spanning Tree Protocol (STP) is another solution to the Layer 2 network loop problem. STP is at mature application stage but requires a relatively long (within seconds) convergence time. Compared with STP, ERPS provides faster convergence, with the Layer 2 convergence time less than 50 ms.

13.4.2 Control VLAN and Data VLAN

ERPS supports two types of virtual local area networks (VLANs): control VLANs and data VLANs.

- **Control VLAN:** Also known as the Ring Auto Protection Switching VLAN (R-APS VLAN) for transmitting ERPS protocol packets. On a device, the ports connecting to an ERPS ring belong to a control VLAN, and only such ports can be added to a control VLAN.
- **Data VLAN:** A data VLAN is used to transmit data packets. Both ERPS ports and non-ERPS ports can be assigned to a data VLAN. A data VLAN is also known as a protected VLAN.

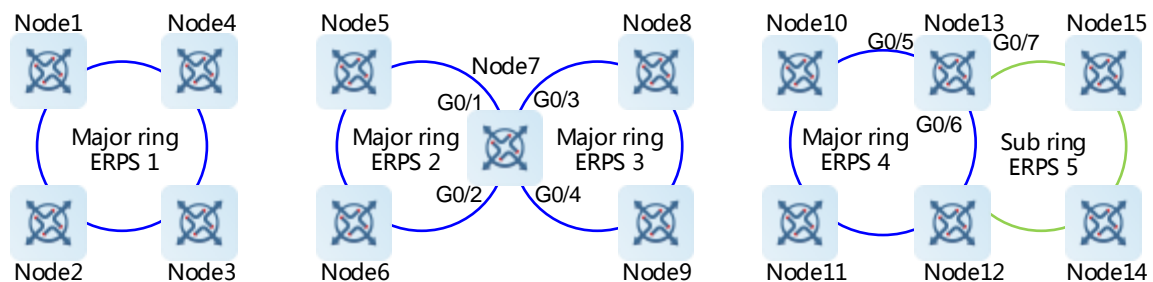
13.4.3 Basic Model of an Ethernet Ring

A group of interconnected devices in the same control VLAN (R-APS VLAN) constitute an Ethernet ring (ERPS ring), in which each device is called a node. ERPS rings can be classified into major rings and subrings based on whether a ring is closed.

1. Major Ring and Subring

- **Major ring and major ring link:** A major ring is a topology of a closed network connected in a ring, such as the blue rings shown in [Figure 13-1](#). In an ERPS ring, links that belong to and are controlled by a major ring are called major ring links.
- **Subring and subring link:** A subring is a topology of a non-closed network attached to a major ring, such as the green ring shown in [Figure 13-1](#). In an ERPS ring, links that belong to and are controlled by a subring are called subring links.
- **R-APS virtual channel of a subring:** As shown in Figure 13-1, all the links on the major ring can be regarded as R-APS virtual channels of subrings, which are used to forward subring protocol packets. They belong to the major ring instead of the subring. The major ring must associate with the control VLAN of the subring and allow packets from this VLAN to pass through.

Figure 13-1 Basic Topologies of Ethernet Rings



2. Basic Topologies

Major rings, subrings, and nodes can form basic topologies with different characteristics, depending on the connection modes, as shown in [Figure 13-1](#).

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

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

3. Node

According to the different topological relationships between nodes and Ethernet rings, nodes are classified into single-ring nodes, tangent nodes, and intersecting nodes by role.

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

4. Ring Member Port

An Ethernet ring has two ring member ports on each node that it passes through: the **west** and **east** ports. As shown in [Figure 13-1](#):

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

There are two states for a port running the ERPS protocol: forwarding and block. Their functions are listed in [Table 13-5](#).

Table 13-5 ERPS Protocol Port States

| Port State | Receiving Protocol Packets | Sending Protocol Packets | Address Learning | Receiving Data Packets | Sending Data Packets |
|------------|----------------------------|--------------------------|------------------|------------------------|----------------------|
| Block | Yes | Yes | No | No | No |
| Forwarding | Yes | Yes | Yes | Yes | Yes |

13.4.4 RPL and Nodes

An Ethernet ring can be in either of the following two states regardless of whether it is a major ring or subring:

- **Idle** state: The physical links in the entire ring network are connected.
- **Protection** state: A physical link in the ring network is disconnected.

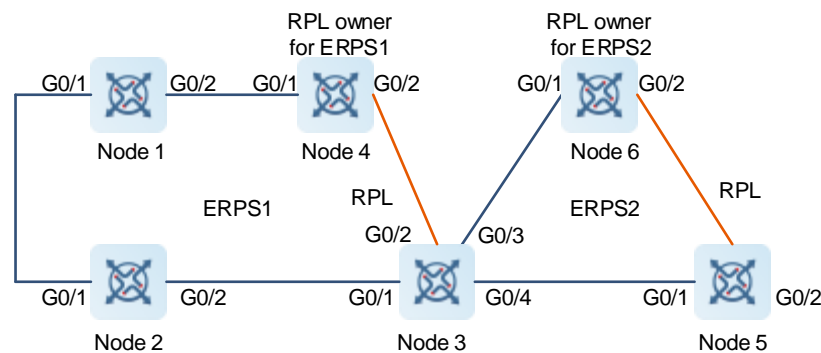
Ring protection link (RPL): When the physical links in a ring network are connected, the ERPS ring is in the idle state, and the links in the logic blocking state are RPLs. Each Ethernet ring has only one RPL. For example, the links indicated by the orange lines shown in [Figure 13-2](#) are RPLs, the link between node 3 and node 4 is the RPL of the Ethernet ring ERPS 1 (node 1-2-3-4), and the link between node 5 and node 6 is the RPL of the Ethernet ring ERPS 2 (node 3-5-6).

A node that is adjacent to an RPL and is used to block the RPL to prevent loops when the Ethernet ring is free of faults is called an RPL **owner** node. As shown in [Figure 13-2](#), node 4 is the RPL owner node of the Ethernet ring ERPS 1 (node 1-2-3-4) and node 6 is the RPL owner node of the ERPS 2 (node 3-5-6).

Any nodes other than the RPL owner node in an Ethernet ring are non-RPL owner nodes. As shown in [Figure 13-2](#), nodes except node 4 and node 6 are non-RPL owner nodes of the rings.

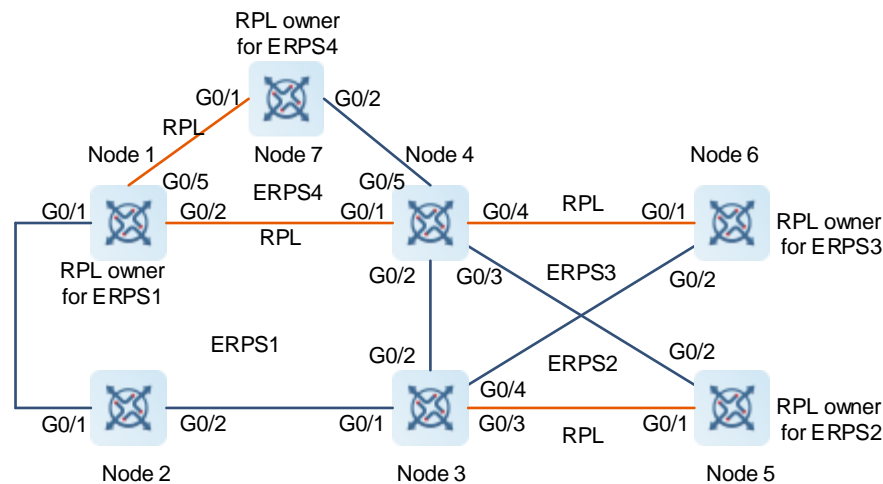
Blocked ports on RPLs are RPL ports, and RPL ports do not forward data packets to prevent loops. RPL ports are on RPL owner nodes, and the RPL owner nodes block the RPL ports. Each Ethernet ring has only one RPL owner node.

Figure 13-2 Typical Topology of Tangent Rings



As shown in [Figure 13-2](#), the link between node 3 and node 4 is the RPL of the Ethernet ring ERPS 1. As the RPL owner node of ERPS 1, node 4 blocks the RPL port. The link between node 5 and node 6 is the RPL of the Ethernet ring ERPS 2. As the RPL owner node of ERPS 2, node 6 blocks the RPL port. ERPS 1 (node 1-2-3-4) and ERPS 2 (node 3-5-6) share node 3, forming a tangent-ring topology. Node 3 is the tangent node.

Figure 13-3 Typical Topology of Intersecting Rings



As shown in [Figure 13-3](#), ERPS 1 (node 1-2-3-4) is a major ring, and ERPS 2 (node 3-4-5) is a subring. ERPS 1 and ERPS 2 share node 3 and node 4, forming an intersecting-ring topology. The links between node 4 and node 5, and between node 3 and node 5 are links of the subring ERPS 2 and are controlled by ERPS 2. The link between node 3 and node 4 belongs to the major ring not the subring, and is not controlled by the subring. However, the protocol packets of the subring are transmitted through the direct link between node 3 and node 4. This direct link is the R-APS virtual channel of the subring ERPS 2. Node 2 only belongs to the major ring ERPS 1, and is called a single-ring node. Node 6 only belongs to the subring ERPS 3, and is also called a single-ring node. Node 3 and node 4 are tangent nodes.

13.4.5 ERPS Packet

ERPS packets (also called R-APS packets) are classified into Signal Fail (SF) packets, No Request (NR) packets, No Requests-RPL Blocked (NR-RB) packets, and Flush packets.

- SF packet: When the link of a node is down, the node sends an SF packet to notify other nodes of its link failure.
- NR packet: When the failed link is restored, the node sends an NR packet to notify the RPL owner node of its link recovery.
- NR-RB packet: When all nodes in an ERPS ring function properly, the RPL owner node sends NR-RB packets periodically.
- Flush packet: In intersecting rings, when a topology change occurs in a subring, the intersecting nodes send flush packets to notify other devices in the Ethernet ring to which the subring is connected.

13.4.6 ERPS Timer

ERPS supports three timers: Holdoff timer, Guard timer, and **Wait-To-Restore (WTR)** timer.

- **Holdoff** timer: The timer is used to minimize frequent ERPS topology switching due to intermittent link failures. After you configure the Holdoff timer, ERPS performs topology switching only if the link failure still persists after the timer times out.
- **Guard** timer: The timer is used to prevent a device from receiving expired R-APS PMDU packets. When a

device detects that a link failure is cleared, it sends link recovery packets and starts the **Guard** timer. Before the timer expires, all packets except Flush packets indicating a subring topology change will be discarded.

- **WTR timer:** The timer is effective only for RPL owner nodes. It is used to avoid ring status misjudgment by the RPL owner node. When an RPL owner node detects that a failure is cleared, it will not perform topology switching immediately but only if the Ethernet ring is recovered after the WTR timer times out. If a ring failure is detected again before the timer expires, the RPL owner node cancels the timer and does not perform topology switching.

13.4.7 Ring Protection

The ring protection function prevents broadcast storms caused by data loops and can rapidly recover the communication between nodes when a link is disconnected in the Ethernet ring.

- **Normal state**
 - All nodes in the physical topology are connected in ring mode.
 - ERPS blocks the RPL to prevent loops.
 - ERPS detects failures on each link between adjacent nodes.

- **Link fault**

A node adjacent to a failed node detects the fault.

The node adjacent to the failed link blocks the failed link and sends SF packets to notify other nodes in the same ring.

An SF packet triggers the RPL owner node to enable the RPL port, and also triggers all nodes to update their MAC address entries and ARP/ND entries and enter the protection state.

- **Link recovery**

When a failed link is restored, an adjacent node still blocks the link and sends NR packets indicating that no local fault exists.

When the RPL owner node receives the first NR packet, it starts the WTR timer.

When the WTR timer times out, the RPL owner node blocks the RPL and sends an NR-RB packet.

After receiving this NR-RB packet, other nodes update their MAC address entries and ARP/ND entries, and the node that sends the NR packet stops sending the NR packet and enables the blocked ports.

- The ring network is restored to the normal state.

13.4.8 Protocols and Standards

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

13.4.9 Configuring ERPS

1. Adding and Deleting an ERPS Ring

Choose **Local Device** > **Advanced** > **ERPS**

- (1) Click **Add** on the **ERPS Ring List** page.
- (2) As shown in Figure 13-4, configure the parameters on the page based on the service requirements.

Figure 13-4 Adding an ERPS Ring

Add
×

* ID

* Control VLAN

Select ▼

Type

☒ Major Ring
☐ Sub Ring

* West Port/Role

Select ▼

NORMAL ▼

* East Port/Role

Select ▼

NORMAL ▼

Sub Ring VLAN

Select ▼

Advanced Settings

* WTR Timer

min

* Guard Timer

ms

* Hold-off Timer

ms

MEL Level

7 (High) ▼

Revertive Mode

☒

?

Cancel

OK

Table 13-6 Parameter Description

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

| | | |
|----------------|---|---|
| | The values of a port role include: <ul style="list-style-type: none"> ● NORMAL: Indicates a normal node. ● RPL OWNER: Indicates an RPL owner node. ● RPL NEIGHBOR: Indicates an RPL neighbor node. | |
| Sub Ring VLAN | Specifies the control VLAN of a sub ring. | N/A |
| WTR Timer | Specifies the interval of the WTR timer. | 5 min |
| Guard Timer | Specifies the interval of the Guard timer. | 500 ms |
| Hold-off Timer | Specifies the interval of the Hold-off timer. | 0 ms, indicating a topology switch is performed immediately after a link failure is detected. |
| MEL Level | Indicates the maintenance entity group (MEG) level. The MEL level of devices in the same ERPS ring must be consistent. | 7 |
| Revertive Mode | When this switch is toggled on, once the condition causing a switch has cleared, traffic is blocked on the RPL. | Enabled. |

- (3) (Optional) As shown in Figure 13-5, select existing ERPS rings, and then click **Delete Selected** to delete selected ERPS rings.

Figure 13-5 Deleting Selected ERPS Rings

ERPS Ring List
+ Add
↕ Link Switch
🗑 Delete Selected

Up to **20** entries can be added.
 Remove any associated sub rings before deleting the major ring.

| <input checked="" type="checkbox"/> | ID | Type | Status | Control VLAN | West Port | East Port | Major Ring |
|-------------------------------------|----|------------|---------|--------------|---|---|------------|
| <input checked="" type="checkbox"/> | 2 | Major Ring | PENDING | 3 | Port: Gi5 Role: RPL NEIGHBOUR Status: BLOCKED | Port: Gi6 Role: NORMAL Status: FORWARDING | -- |

2. Link Switch

Choose **Local Device > Advanced > ERPS**

- Click **Link Switch** on the **ERPS Ring List** page.
- As shown in Figure 13-6, configure the parameters on the page based on the service requirements.

Figure 13-6 Link Switch

Link Switch ×

* ID

2

▼

* Port

West Port

▼

* Link State

Block

▼

Cancel

OK

Table 13-7 Parameter Description

| Parameter | Description | Default Value |
|------------|---|---------------|
| ID | Specifies the ID of an ERPS instance. | N/A |
| Port | Specifies the port in the ERPS ring. The values include West Port and East Port. | N/A |
| Link State | <div>Specifies the link state of the selected port. The values include Clear and Block.</div> <ul style="list-style-type: none">● Clear: Indicates that the port is blocked by a forced switch operation.● Block: Indicates that the port is blocked by a manual switch operation. | N/A |

13.4.10 ERPS Typical Configuration Examples

1. Requirements

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

2. Topology



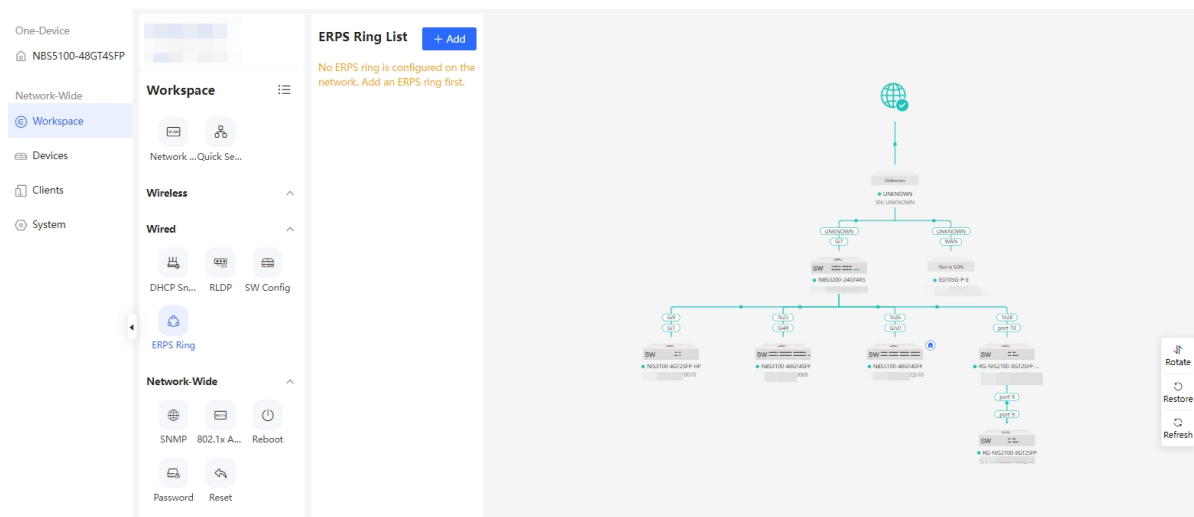
3. Notes

To prevent loops, configure ERPS before performing cable connections.

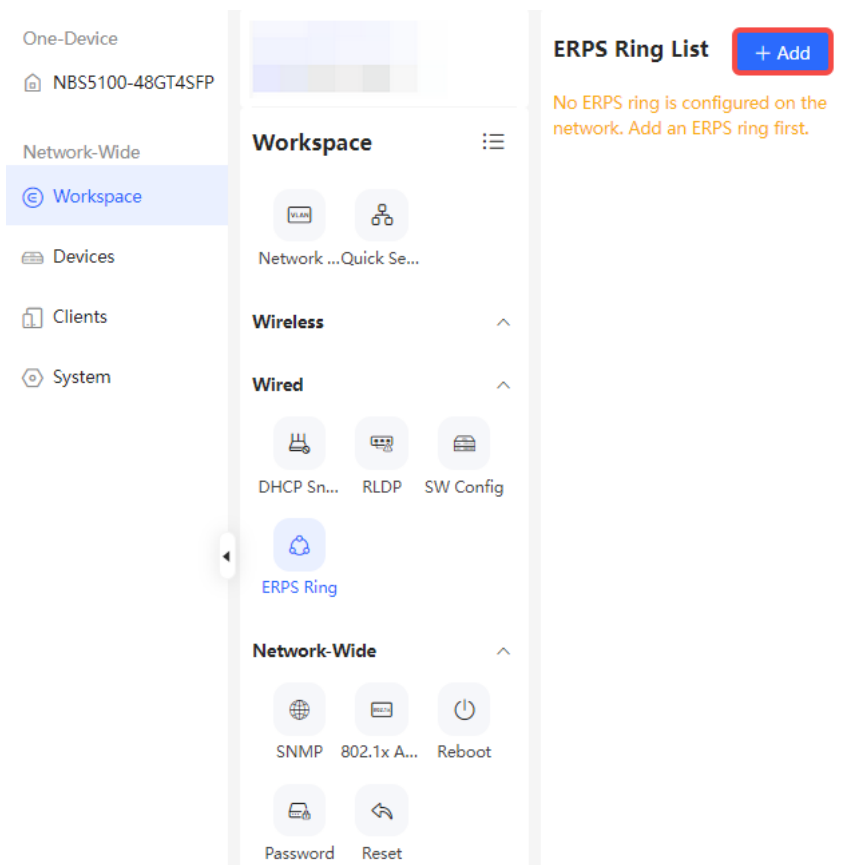
For an ERPS ring, only one interface can be the RPL Owner, and its peer interface must be the RPL Neighbor.

4. Procedure

(1) Choose **Network-Wide > Workspace > Wired > ERPS Ring** to access the **ERPS Ring** configuration page.



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



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

Network-wide Configuration/ERPS Ring Configuration

1 Ring Parameters

2 Port Settings

3 Confirm Config Delivery

* ID

1

* Control VLAN

11

Advanced Settings

* WTR Timer

5

min

* Guard Timer

500

ms

* Hold-off Timer

0

ms

MEL Level

7 (High)

▼

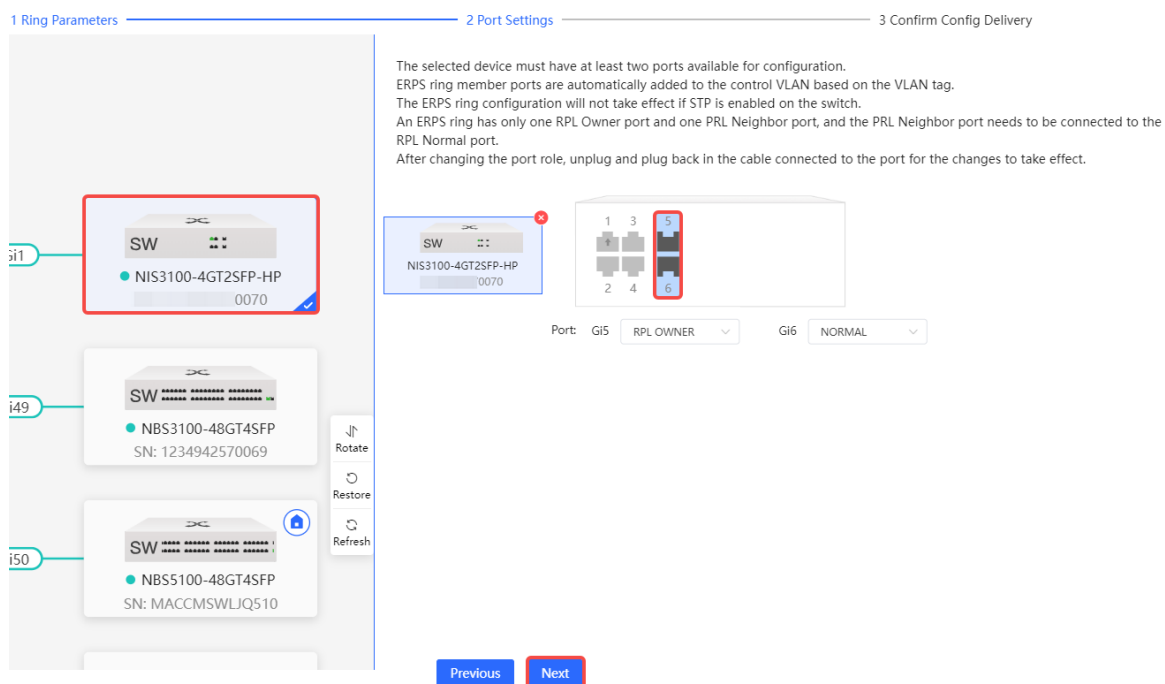
Revertive Mode

☒

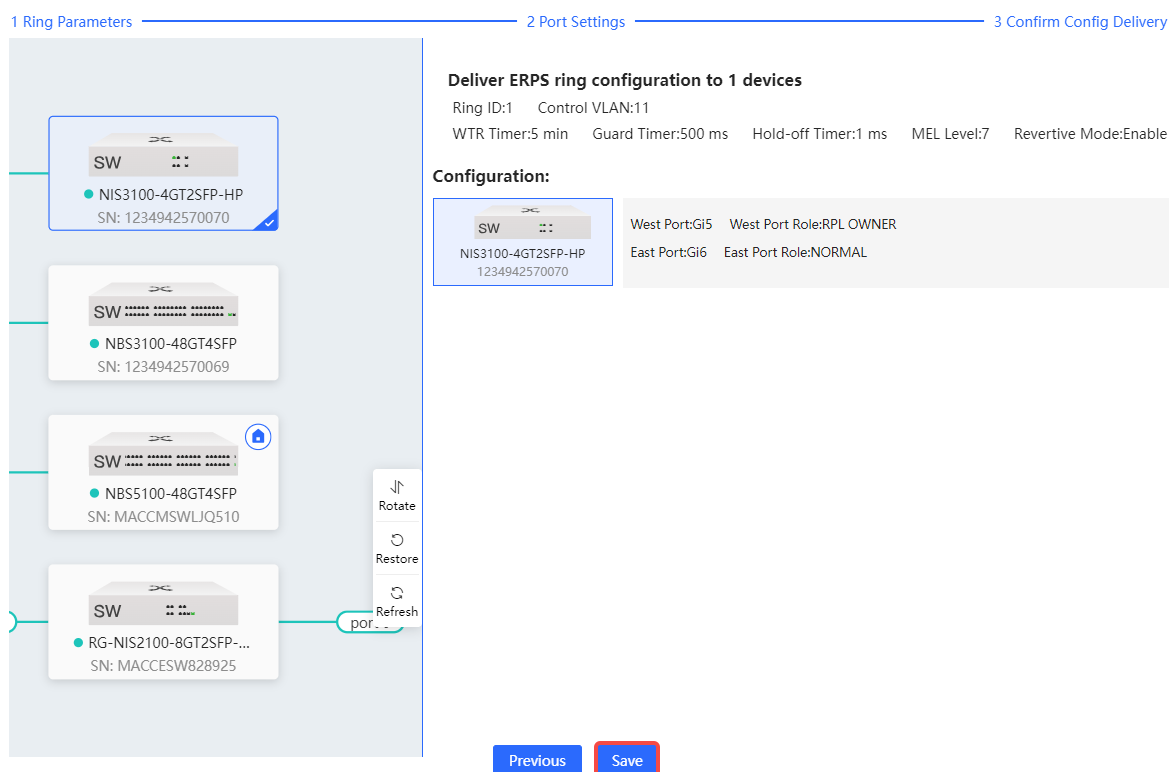
?

Next

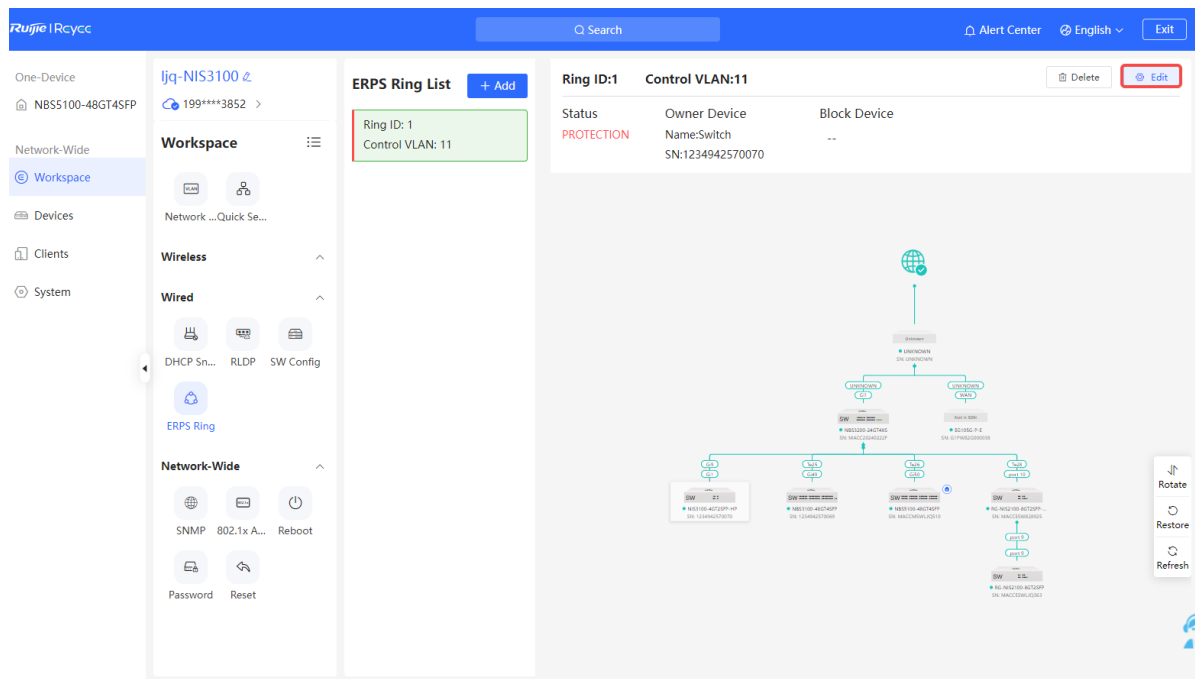
- (4) As shown in the following figure, select a device for the ERPS ring, set the Gi5 to **RPL OWNER**, and Gi6 to **NORMAL**. Click **Next**.



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



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



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

Network-wide Configuration/ERPS Ring Configuration

1 Ring Parameters — 2 Port Settings — 3 Confirm Config Delivery

* ID 1

* Control VLAN 11

----- Advanced Settings -----

Next

(8) As shown in the following figure, add the remaining devices on the **ERPS Ring Configuration** page. Select the optical ports on the devices and configure the interfaces connected to the RPL OWNER as RPL NEIGHBOR, following the example of Gi52 in the figure below. Configure other interfaces as NORMAL. After completing the configuration, click **Next**.

The selected device must have at least two ports available for configuration.
 ERPS ring member ports are automatically added to the control VLAN based on the VLAN tag.
 The ERPS ring configuration will not take effect if STP is enabled on the switch.
 An ERPS ring has only one RPL Owner port and one RPL Neighbor port, and the RPL Neighbor port needs to be connected to the RPL Normal port.
 After changing the port role, unplug and plug back in the cable connected to the port for the changes to take effect.

Previous Next

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

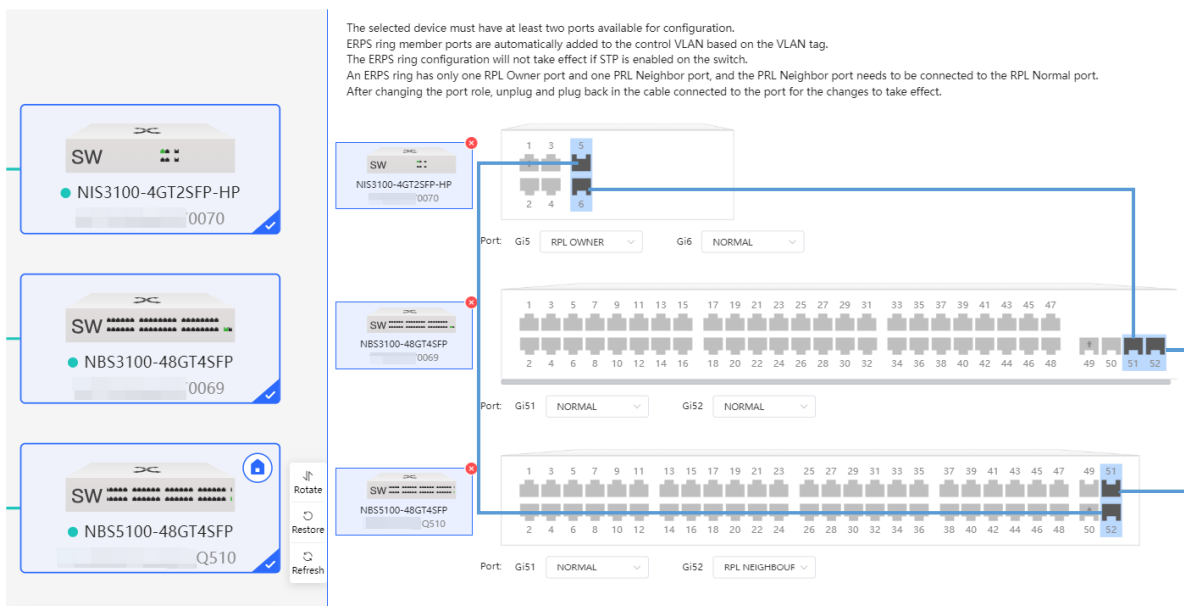
Deliver ERPS ring configuration to 3 devices
 Ring ID:1 Control VLAN:11
 WTR Timer:5 min Guard Timer:500 ms Hold-off Timer:1 ms MEL Level:7 Revertive Mode:Enable

Configuration:

| | |
|----------------------------------|---|
| SW NIS3100-4GT2SFP-HP 0070 | West Port:Gi5 West Port Role:RPL OWNER East Port:Gi6 East Port Role:NORMAL |
| SW NBS3100-48GT4SFP 0069 | West Port:Gi51 West Port Role:NORMAL East Port:Gi52 East Port Role:NORMAL |
| SW NBS5100-48GT4SFP Q510 | West Port:Gi51 West Port Role:NORMAL East Port:Gi52 East Port Role:RPL NEIGHBOUR |

Previous Save

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



13.5 QoS

✓ Specification

QoS can be viewed or set only on devices running ReyeeOS 2.280 or later versions.

13.5.1 Overview

Quality of service (QoS) can meet users' requirements for different applications and different levels of service quality. It allocates and schedules resources based on users' requirements and provides different levels of service quality for different packets.

On a traditional IP network, a device treats all the packets in the same way, in which the device processes packets based on their arrival time according to the queuing strategy of first in first out (FIFO), and transmits the packets to the destination on a best-effort basis. When the network bandwidth is abundant, all the packets are properly processed; when the network is congested, all the packets may be discarded.

QoS assigns a transmission priority to the packets of a type to highlight the importance of the packets. Then, the devices provide special transmission services for these packets according to forwarding policies for different priorities, congestion avoidance, and other mechanisms. With QoS, a device processes real-time and important packets preferentially, processes non-real-time and common packets with lower priorities and even discards the packets upon network congestion.

QoS enhances the network performance predictability, effectively allocates network bandwidth, and reasonably utilizes network resources.

13.5.2 Principles

1. Basic Concepts

- DiffServ model

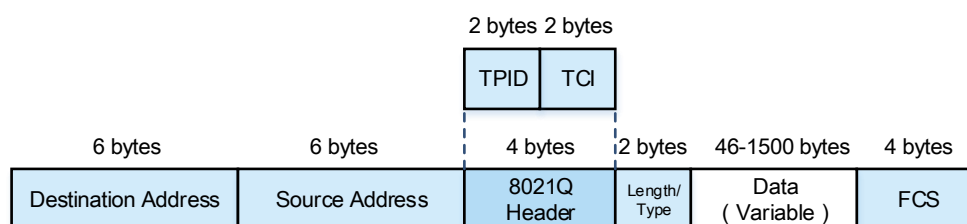
The differentiated services (DiffServ) model classifies all packets transmitted on a network into different types. The classification information related to QoS priority marking is recorded in some fields of L2 or L3 packets, for example, the PRI field of IEEE 802.1Q frames, type of service (ToS) field of IPv4 packets, traffic class (TC) field of IPv6 packets, and the MPLS experimental bits (EXP) field of multiprotocol label switching (MPLS) packets.

On the network of DiffServ model, the classification information of packets can be assigned by hosts or other network devices or based on different application policies or different packet contents. A device applies the same transmission service policy to packets containing the same classification information and applies different transmission service policies to packets containing different classification information. Based on the classification information carried by packets, a device may provide different transmission priorities for different packets, reserve bandwidth for a kind of packets, discard certain packets with lower priorities, or take some other actions.

- PRI field of the IEEE 802.1q frames

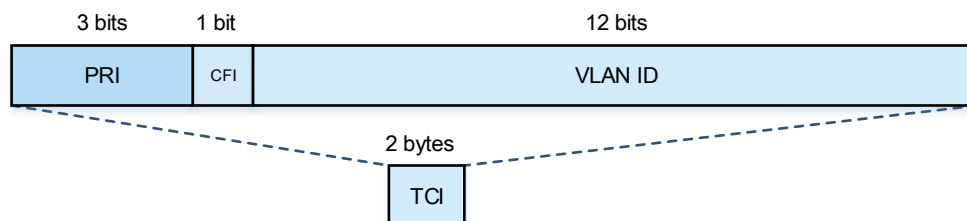
The PRI field of IEEE 802.1Q frames (namely, the IEEE 802.1p priority) is located in the header of an L2 packet containing an IEEE 802.1Q tag header, as shown in [Figure 13-7](#).

Figure 13-7 Format of an L2 Frame with an IEEE 802.1Q Tag Header



The 4-byte IEEE 802.1Q tag header contains the 2-byte tag protocol identifier (TPID) and 2-byte tag control information (TCI). TCI contains the 3-bit PRI field, as shown in [Figure 13-8](#).

Figure 13-8 PRI Field of the IEEE 802.1q Frames

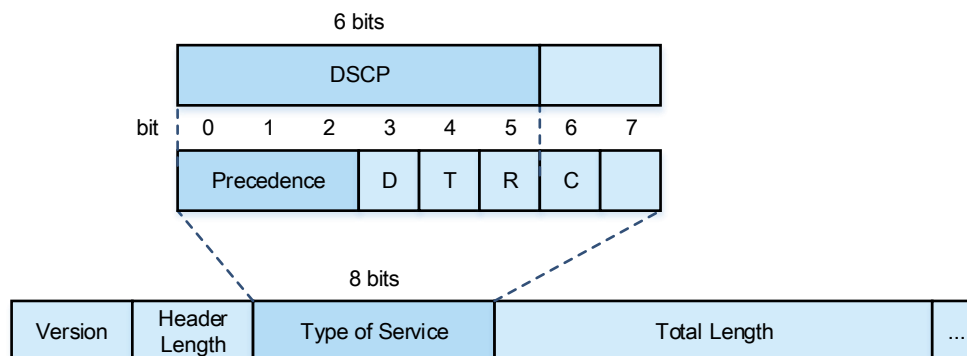


The PRI field represents eight priorities for packet transmission, and the priority values from high to low are 7, 6, ..., 1, and 0. The IEEE 802.1p priority is applicable to scenarios where L3 headers do not need to be analyzed and QoS needs to be implemented only at L2.

- ToS field of the IPv4 packets

IPv4 packets use the ToS field in the IP header to indicate the priority of the packets, as shown in [Figure 13-9](#).

Figure 13-9 ToS Field in the IP Header



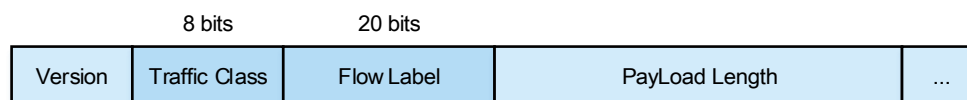
The ToS field contains eight bits, of which the first three bits are the IP PRE (precedence) field and represent eight priorities for packet transmission, with the priority values from high to low being 7, 6, ..., 1, and 0.

RFC 2474 redefines the ToS field of the IP header, in which the first 6 bits (bits 0 to 5) represent the differentiated services code point (DSCP). DSCP is used to classify packets into a maximum of 64 different categories.

- ToS field of the IPv6 packets

IPv6 packets use the TC field in the IPv6 header to indicate the packet priority, as shown in [Figure 13-10](#) Figure 13-10.

Figure 13-10 TC Field in the IPv6 Header



The TC field contains eight bits and provides the same function as the ToS field of IPv4 packets. The first six bits of the TC field indicate DSCP.

2. Priority Mapping

Priorities are used to identify the scheduling weights or forwarding priority of packets. Different priority types are defined for different packet types: IEEE 802.1q frames use the IEEE 802.1p priority, IP packets use the DSCP, and so on.

After a packet enters a device interface, the packet priority is mapped to the CoS according to the trust mode configured for the interface. [Table 13-8](#) shows the mappings between trust modes configured for an interface and the priorities.

Table 13-8 Interface Trust Mode and Priority Mapping

| Trust Mode | Priority Mapping |
|------------|--|
| Untrusted | <ul style="list-style-type: none"> ● The device does not trust any priority information carried in the packet. ● A packet received by the interface is assigned to a queue based on the 802.1p-queue mapping table using the 802.1p value (interface priority) configured for the interface. ● For a packet with a VLAN tag sent by the interface, the device re-marks the 802.1p value of the packet based on the queue-802.1p mapping table. ● For a packet without a VLAN tag sent by the interface, the device does not re-mark the 802.1p value of the packet. ● If the packet sent by the interface is an IP packet, the device re-marks the DSCP value of the packet based on the queue-DSCP mapping table. |
| 802.1p | <ul style="list-style-type: none"> ● After an interface receives a packet: <ul style="list-style-type: none"> ○ If the packet carries a VLAN tag, the 802.1p value carried by the packet will be used as the input for mapping, and the packet will be assigned to a queue based on the 802.1p-queue mapping table. ○ If the packet does not carry any VLAN tag, it will be processed by the device in the same way as that in untrusted mode. ● For a packet with a VLAN tag sent by the interface, the device re-marks the 802.1p value of the packet based on the queue-802.1p mapping table. ● For a packet without a VLAN tag sent by the interface, the device does not re-mark the 802.1p value of the packet. ● If the packet sent by the interface is an IP packet, the device re-marks the DSCP value of the packet based on the queue-DSCP mapping table. |
| DSCP | <ul style="list-style-type: none"> ● After an interface receives a packet: <ul style="list-style-type: none"> ○ If the packet is not an IP packet, it will be processed by the device in the same way as that in 802.1p mode. ○ If the packet is an IP packet, the DSCP value of the packet will be used as the input for mapping, and the packet will be assigned to a queue based on the DSCP-queue mapping table. ● If the packet sent by the interface is an IP packet, the device re-marks the DSCP value of the packet based on the queue-DSCP mapping table. ● If the packet sent by the interface is not an IP packet, the packet is processed depending on whether it carries a VLAN tag: <ul style="list-style-type: none"> ○ If the packet carries a VLAN tag, the device re-marks the 802.1p value of the packets based on the queue-802.1p mapping table. ○ If the packet does not carry a VLAN tag, the device does not re-mark the 802.1p value of the packet. |

3. Congestion Management

When the receiving rate of packets exceeds the sending rate, congestion occurs on the sending interface. If no sufficient buffer is provided to store these packets, packet loss may occur. The congestion management mechanism determines the sending order of packets based on their local priorities. The congestion management function controls congestion and improves the local priorities of packets for some important data. When congestion occurs, the packets of higher priorities are sent first to ensure that key services are provided in time.

Congestion management adopts the queue scheduling mechanism. The processing is as follows:

- (1) Each packet is assigned to a queue based on priority-to-queue mappings.
- (2) The outbound interface selects the packets in a queue for sending according to various queue scheduling policies (such as SP, WRR, and SP+WRR).

- SP scheduling policy

In strict-priority (SP) scheduling, packets are scheduled strictly based on their queue priorities from high to low (a larger queue ID indicates a higher priority). Before sending a packet, check whether there is a packet to be sent in a high-priority queue. If there is, send it. If not, check whether there is a packet to be sent in the next-level queue, and so on.

The weakness of SP scheduling is that, when congestion occurs, if the packets in a higher priority queue exist for a long time, the packets in a lower priority queue have no opportunity of being scheduled.

- WRR scheduling policy

Weighted Round Robin (WRR) ensures that all queues are scheduled in turn. Taking eight output queues as an example, the device allocates bandwidth resources based on the weight of each queue. For example, if the WRR weights of a 1000 Mbps port are set to 50, 50, 30, 30, 10, 10, 10, and 10, WRR ensures that at least 50 Mbps of bandwidth is allocated to the queue with the lowest priority. WRR also allows for efficient use of bandwidth by immediately switching to the next queue when a queue is empty.

- SP+WRR scheduling policy

SP scheduling is configured for one or more sending queues, and the other queues are scheduled in the WRR mode. Among SP queues, only after all the packets in an SP queue with a higher priority are sent, can the packets in an SP queue with a next higher priority be sent. Among SP and WRR queues, only after the packets in all SP queues are sent, can the packets in WRR queues be sent.

1.1.2 Configuring QoS

1. Global Configuration

In local device mode, choose **Advanced > QoS > Global Config**.

In the **Global Config** page, you can configure the trust mode, modify the 802.1p-Queue Mapping Table for inbound packets, modify the DSCP-Queue Mapping Table for inbound packets, modify the Queue-802.1p Mapping Table for outbound packets, and modify the Queue-DSCP Mapping Table for outbound packets.

Click **Batch Config** to batch configure these mapping tables.

Click **Reset** to restore a mapping table to default values.

The screenshot shows the 'Global Config' page for QoS. The '802.1p-Queue Mapping Table' is selected. The table has three columns: '802.1p', 'Queue ID', and 'Action'. The 'Action' column contains 'Edit' links for each row. The 'Batch Config' and 'Reset' buttons are located at the top right of the table.

| 802.1p | Queue ID | Action |
|--------|----------|----------------------|
| 0 | 0 | Edit |
| 1 | 1 | Edit |
| 2 | 2 | Edit |
| 3 | 3 | Edit |
| 4 | 4 | Edit |
| 5 | 5 | Edit |

Table 13-9 Global Configuration Parameter Description

| Parameter | Description | Default Value |
|----------------------------|---|------------------------|
| Trusted Mode | <p>Priority designations of an inbound packet:</p> <p>Untrusted Mode: The device does not trust any priority information carried in the packet, and uses the interface priority as the 802.1p value of the packet. The device assigns the packet into a queue based on the 802.1p-queue mapping table. If Untrusted Mode is selected, any packets received by any interface on the device will be assigned to queues based on the interface priority regardless of the trust mode status configured in the Port Settings page.</p> <p>802.1p: The device trusts the 802.1p value carried in the packet, and use the 802.1p value to assign the packet to a queue based on the 802.1p-queue mapping table. If the packet does not carry an 802.1p value, that is, the packet does not carry a VLAN tag, the device will process the packet in the same way as that in untrusted mode. If 802.1p is selected, and the designated interface is in untrusted mode in the Port Settings page, the device will process the packet in the same way as that in untrusted mode.</p> <p>802.1p-DSCP: The device trusts the 802.1p value (for non-IP packets) or DSCP value (for IP packets) of the packet, and assigns the packet to a queue based on the 802.1p-queue mapping table or the DSCP-queue mapping table depending on the 802.1p value or DSCP value of the packet. If 802.1p-DSCP is selected, and the designated interface is in untrusted mode in the Port Settings page, the device will process the packet in the same way as that in untrusted mode.</p> | Untrusted Mode |
| 802.1p-Queue Mapping Table | An input queue mapping table, which contains the mappings between the 802.1p value and the queue ID. For example, if the 802.1p value is 0, and the queue ID is 1, packets with the 802.1p value 0 will be assigned to queue 1. | As shown inTable 13-10 |
| DSCP-Queue Mapping Table | An input queue mapping table, which contains the mappings between the DSCP value and the queue ID. For example, if the DSCP value falls within 0 to 7, and the queue ID is 0, packets with a DSCP value between 0 and 7 will be assigned to queue 0. | As shown inTable 13-11 |
| Queue-802.1p Mapping Table | An output queue mapping table, which contains the mappings between the queue ID and the 802.1p value. The 802.1p value of an outgoing packet in a queue is re-marked based on the mapping. For example, if the queue ID is 0, and the packets carrying a VLAN tag in queue 0 have an 802.1p value, then the 802.1p value of the packets in queue 0 are re-marked to 2. If a packet does not carry any 802.1p value, that is, the packet does not carry any VLAN tag, the device does not re-mark the 802.1p value of the packet. | As shown inTable 13-12 |

| Parameter | Description | Default Value |
|--------------------------|--|-------------------------|
| Queue-DSCP Mapping Table | An output queue mapping table, which contains the mappings between the queue ID and the DSCP value. The DSCP value of packets in the output queue is re-marked based on the mapping. For example, if the queue ID is 0, and the mapped DSCP value is 8, then the DSCP value of packets in queue 0 is re-marked to 8. | As shown in Table 13-13 |

Table 13-10 Default 802.1p-Queue Mapping Table of the Device

| 802.1p Value | Queue ID |
|--------------|----------|
| 0 | 0 |
| 1 | 1 |
| 2 | 2 |
| 3 | 3 |
| 4 | 4 |
| 5 | 5 |
| 6 | 6 |
| 7 | 7 |

Table 13-11 Default DSCP-Queue Mapping Table of the Device

| DSCP Value | Queue ID |
|------------|----------|
| 0–7 | 0 |
| 8–15 | 1 |
| 16–23 | 2 |
| 24–31 | 3 |
| 32–39 | 4 |
| 40–47 | 5 |
| 48–55 | 6 |

| DSCP Value | Queue ID |
|------------|----------|
| 56–63 | 7 |

Table 13-12 Default Queue–802.1p Mapping Table of the Device

| Queue ID | 802.1p Value After Remarking |
|----------|------------------------------|
| 0 | 0 |
| 1 | 1 |
| 2 | 2 |
| 3 | 3 |
| 4 | 4 |
| 5 | 5 |
| 6 | 6 |
| 7 | 7 |

Table 13-13 Default Queue-DSCP Mapping Table of the Device

| Queue ID | DSCP Value After Re-marking |
|----------|-----------------------------|
| 0 | 0 |
| 1 | 8 |
| 2 | 16 |
| 3 | 24 |
| 4 | 32 |
| 5 | 40 |
| 6 | 48 |
| 7 | 56 |

2. Port Settings

In local device mode, choose **Advanced > QoS > Port Settings**.

In the **Port Settings** page, you can set the priority, trust mode, 802.1p remarking, DSCP remarking, queue algorithm, and queue ID/weight for a designated interface.

Q search

Security

Advanced

STP

LLDP

RLDP

ERPS

QoS

Voice VLAN

Local DNS

Diagnostics

Global Config

Port Settings

Batch Config

Port List

| Interface | Priority | Trusted Mode | 802.1p Remarki ng | DSCP Remarki ng | Queue Algorith m | Queue ID/Weight | | | | | |
|-----------|----------|--------------|-------------------|-----------------|------------------|-----------------|---|---|---|---|---|
| | | | | | | 0 | 1 | 2 | 3 | 4 | 5 |
| Gi1 | 0 | Disable | Disable | Disable | SP + WRR | 1 | 2 | 3 | 4 | 5 | 9 |
| Gi2 | 0 | Disable | Disable | Disable | SP + WRR | 1 | 2 | 3 | 4 | 5 | 9 |
| Gi3 | 0 | Disable | Disable | Disable | SP + WRR | 1 | 2 | 3 | 4 | 5 | 9 |
| Gi4 | 0 | Disable | Disable | Disable | SP + WRR | 1 | 2 | 3 | 4 | 5 | 9 |
| Gi5 | 0 | Disable | Disable | Disable | SP + WRR | 1 | 2 | 3 | 4 | 5 | 9 |
| Gi6 | 0 | Disable | Disable | Disable | SP + WRR | 1 | 2 | 3 | 4 | 5 | 9 |
| Gi7 | 0 | Disable | Disable | Disable | SP + WRR | 1 | 2 | 3 | 4 | 5 | 9 |

Table 13-14 Port Configuration Parameter Description

| Parameter | Description | Default Value |
|--------------|--|---------------|
| Priority | Interface priority. When the device is in untrusted mode, packets are assigned to a queue based on this priority, which is equivalent to the 802.1p value of a packet. | 0 |
| Trusted Mode | <p>Priority designations of an inbound packet:</p> <p>Disable: The device does not trust any priority information carried in the packet, and uses the interface priority as the 802.1p value of the packet. The device assigns the packet into a queue based on the 802.1p-queue mapping table.</p> <p>Enable: The device trusts the 802.1p value (for non-IP packets) or DSCP value (for IP packets) of the packet, and assigns the packet to a queue based on the 802.1p-queue mapping table or the DSCP-queue mapping table depending on the 802.1p value or DSCP value of the packet.</p> <p>If Untrusted Mode is selected in the Global Config page, any packets received by any interface on the device will be assigned to queues based on the interface priority regardless of the trust mode status configured in the Port Settings page.</p> <p>If 802.1p or 802.1p-DSCP is selected in the Global Config page, the device will only process packets received by the specified interface in the same way as that in trusted mode when the Trusted Mode of the designated interface is set to Enable in the Port Settings page.</p> | Disable |

| | | |
|------------------|--|------------------------|
| 802.1p Remarking | <p>Enable: The 802.1p value of packets in the queue is re-marked based on the Queue-802.1p Mapping Table.</p> <p>Disable: The device does not re-mark the 802.1p value of packets in the queue based on the Queue-802.1p Mapping Table, and marks the priority of the outgoing packets based on the priority of the input queue.</p> | Enable |
| DSCP Remarking | <p>Enable: The DSCP value of packets in the queue is re-marked based on the DSCP-802.1p Mapping Table.</p> <p>Disable: The device does not re-mark the DSCP value of packets in the queue based on the Queue-802.1p Mapping Table, and marks the priority of the outgoing packets based on the priority of the input queue.</p> | Enable |
| Queue Algorithm | The queue algorithm adopted by the interface. | SP+WRR |
| Queue ID/Weight | WRR weight of a queue. The value 0 indicates that the SP algorithm is adopted for the queue. After all packets in all SP queues are sent, the device will send packets in WRR queues. Among SP queues, the queue with a larger ID is scheduled first. | As shown in Table 13-5 |

Table 13-15 Default Interface Queue ID/Weight of the Device

| Queue ID | WRR Weight |
|----------|------------|
| 0 | 1 |
| 1 | 2 |
| 2 | 3 |
| 3 | 4 |
| 4 | 5 |
| 5 | 9 |
| 6 | 13 |
| 7 | 15 |

13.6 Configuring the Local DNS

The local DNS server is optional. The device obtains the DNS server address from the connected uplink device by default.

Choose **Local Device > Advanced > Local DNS**.

Enter the DNS server address used by the local device. If multiple addresses exist, separate them with spaces. Click **Save**. After configuring the local DNS, the device first use the DNS of the management IP address for parsing domain names. If the device fail to parse domain names, then use this DNS address instead.



The device will get the DNS server address from the uplink device.

Local DNS server

Example: 8.8.8.8, each separated by a space.

Save

13.7 Voice VLAN

13.7.1 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.

13.7.2 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



Global Settings

Voice VLAN ☒

* VLAN

2



Range: 2-4094

* Max Age

1440

minute Range: 1-43200

CoS Priority

6



Save

Table 13-16 Description of VLAN Global Configuration Parameters

| Parameter | Description | Default Value |
|--------------|--|---------------|
| Voice VLAN | Whether to enable the Voice VLAN function | Disable |
| VLAN | VLAN ID as Voice VLAN | N/A |
| 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 |

13.7.3 Configuring a Voice VLAN OUI

Choose **Local Device > Advanced > Voice VLAN > OUI**.

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

Note

After the voice VLAN function is enabled on a port, when the port receives LLDP packets sent by IP phones, it can identify the device capability fields in the packets, and identify the devices with the capability of **Telephone** as voice devices. It also extracts the source MAC address of a protocol packet and processes it as the MAC address of the voice device. In this way, the OUI can be added automatically.

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

Global Settings OUI Port Settings



OUI List

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

OUI List

[+ Add](#)

[Delete Selected](#)

Up to **32** entries can be added.

| <input type="checkbox"/> | MAC Address | OUI Mask | Description | Type | Action |
|--------------------------|-------------|----------|-------------|------|--------|
|--------------------------|-------------|----------|-------------|------|--------|

No Data

Add
×

* MAC Address
00:11:22:33:44:55

OUI Mask
Select

Description

Cancel
OK

13.7.4 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 |

Table 13-17 Description of the Voice VLAN Configuration Parameters on a Port

| Parameter | Description | Default Value |
|-----------------|---|---------------|
| Voice VLAN Mode | <p>Based on different ways the Voice VLAN function is enabled on the port, the Voice VLAN Mode can be Auto Mode or Manual Mode:</p> <ul style="list-style-type: none"> ● Auto Mode: In this mode, the device checks whether the permit VLANs of a port contain the voice VLAN after the voice VLAN function is enabled on the port. If yes, the device deletes the voice VLAN from the permit VLANs of the port until the port receives a voice packet containing a specified OUI. Then, the device automatically adds the voice VLAN to the port's permit VLANs. If the port does not receive a voice packet containing the specified OUI within the global aging time, the device removes the Voice VLAN from the permit VLANs of the port. ● Manual Mode: If the permit VLANs of a port contains the voice VLAN, voice packets can be transmitted in the voice VLAN. | Auto Mode |
| Security Mode | <p>When the security mode is enabled, only voice traffic can be transmitted in the voice VLAN. The device checks the source MAC address in each packet. When the source MAC address in the packet matches the voice VLAN OUI, the packet can be transmitted in the voice VLAN. Otherwise, the device discards the packet.</p> <p>When the security mode is disabled, the source MAC addresses of packets are not checked and all packets can be transmitted in the voice VLAN.</p> | Enable |

 **Caution**

- The voice VLAN mode of the port can be set as the auto mode only when the VLAN mode of the port is Trunk mode. When the voice VLAN mode of the port work in the auto mode, the port exits the voice VLAN first and is automatically added to the voice VLAN only after receiving voice data.

- After the voice VLAN function is enabled on a port, do not switch the L2 mode (trunk or access mode) of the port to ensure normal operation of the function. If you need to switch the L2 mode of the port, disable the voice VLAN function on the port first.
- It is not recommended that both voice data and service data be transmitted over the voice VLAN. If you want to transmit both voice data and service data over the voice VLAN, disable the voice VLAN function in security mode.
- The voice VLAN function is unavailable on L3 ports or aggregate ports.

13.8 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.

Note

Smart hot standby is supported only on NBS7006 Series, NBS7003 Series, NBS5300 Series, and NBS5200 Series switches.

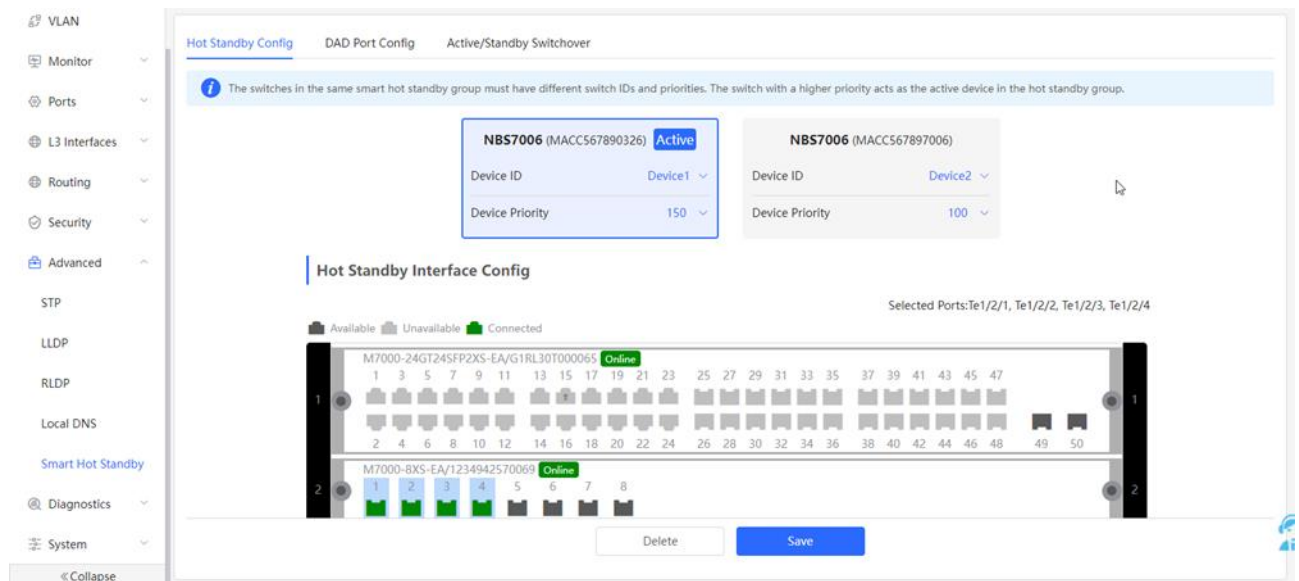
13.8.1 Configuring Hot Standby

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

Caution

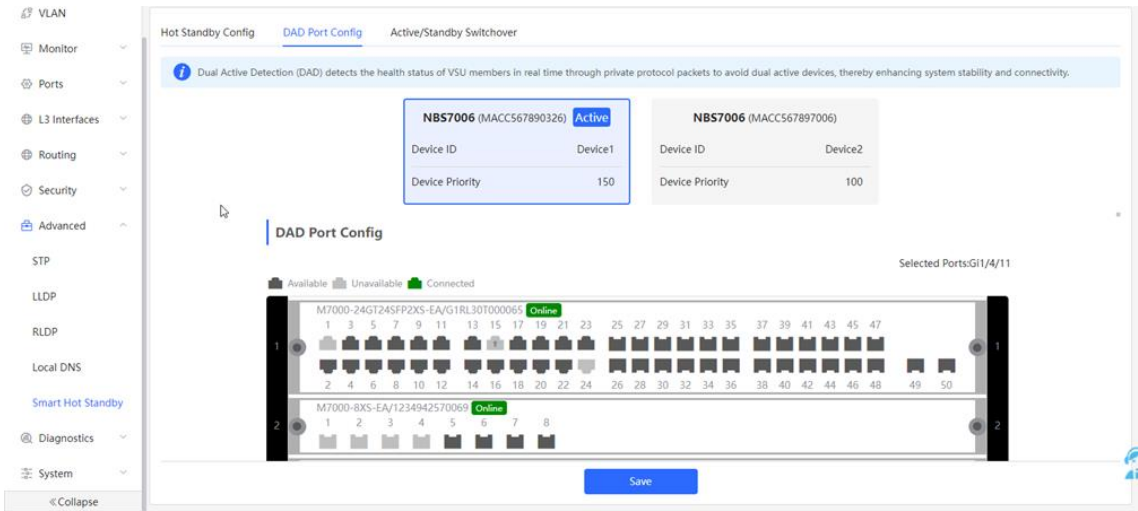
The devices in a hot standby group must have unique device IDs and priorities configured.

Choose **Local Device > Advanced > Smart Hot Standby**.



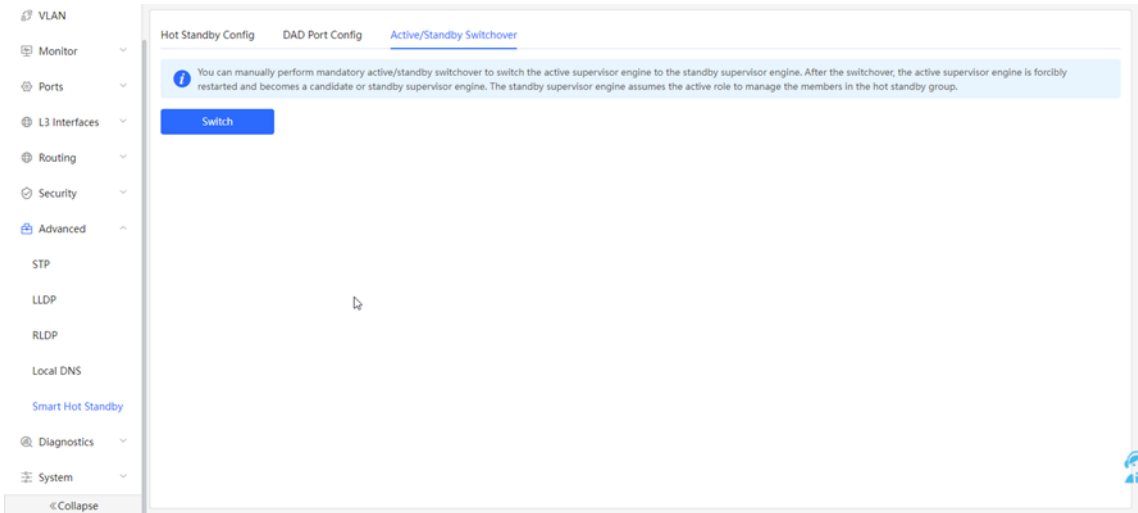
13.8.2 Configuring DAD Interfaces

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



13.8.3 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.

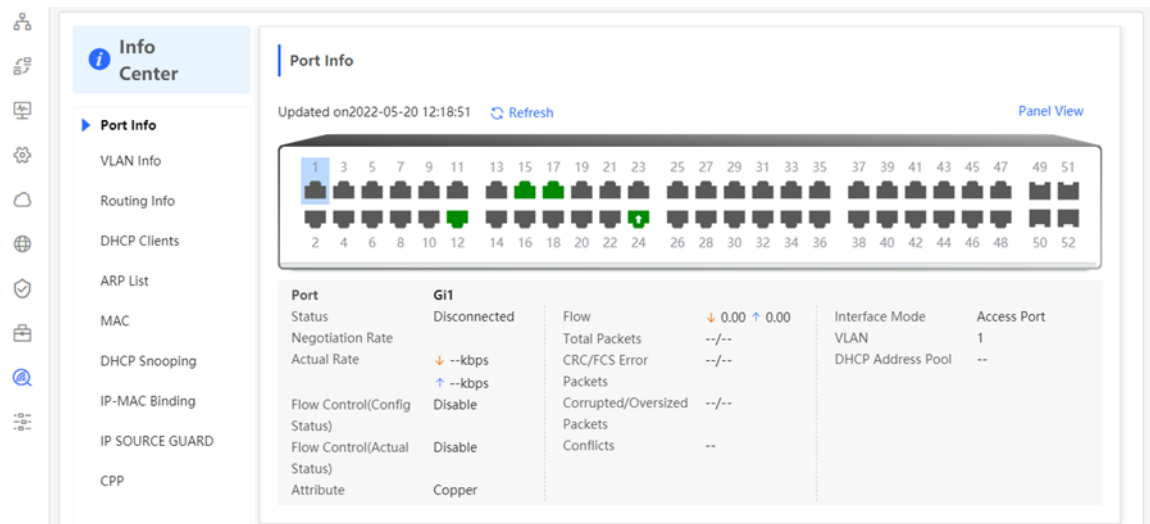


14 Diagnostics

14.1 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.



14.1.1 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 [7.2 Port Configuration](#).
- To configure the L2 mode of the port and the VLAN to which it belongs, see [5.3 Configuring Port VLAN](#).

Port Info

Updated on 2022-05-20 12:18:51 [Refresh](#) [Panel View](#)

Port **Gi12**

| | | | |
|-----------------------------|-----------|-----------------------------|---------|
| Status | Connected | Flow | 0.00 |
| Negotiation Rate | 1000M | Total Packets | 535.26M |
| Actual Rate | 27kbps | CRC/FCS Error | --/-- |
| Flow Control(Config Status) | Disable | Packets | --/-- |
| Flow Control(Actual Status) | Disable | Corrupted/Oversized Packets | --/-- |
| Attribute | Copper | Conflicts | -- |

Role

- Copper
- Fiber
- Uplink
- PoE
- PoE Error
- Aggregate

Status

- 1G/2.5G/10G
- 10M/100M
- Exception
- Disconnected
- Disable

14.1.2 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 [5 VLAN](#).
- To configure SVI ports and routed ports, see [10.1 Setting an L3 Interface](#).

VLAN Info (SVI&Routed Port) [DNS: --](#) [Refresh](#)

VLAN1 **Routed Port Gi1** **Routed Port Gi2** **Routed Port Gi3** **Routed Port Gi4** **Routed Port Gi5** **Route**

| Interface | IP | DHCP Address Pool | Remark |
|-------------------------|----------------|-------------------|----------|
| Gi1-8, Gi10-48, Te49-52 | 172.30.102.133 | | VLAN0001 |

14.1.3 Routing Info



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 [11.1 Configuring Static Routes](#).

14.1.4 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.

Note

To configure DHCP server related functions, see [10.3.2 Viewing the DHCP Client](#).

14.1.5 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 [10.6 Configuring a Static ARP Entry](#).

Info Center

- Port Info
- VLAN Info
- Routing Info
- DHCP Clients
- ARP List**
- MAC
- DHCP Snooping
- IP-MAC Binding
- IP SOURCE GUARD
- CPP

ARP List

Tip: Up to **2000** entries can be added.

Search by IP/MAC

| Interface | IP | MAC | Type | Reachable |
|-----------|----------------|-------------------|---------|-----------|
| VLAN1 | 172.30.102.209 | c0:b8:e6:e9:78:07 | Dynamic | Yes |
| VLAN1 | 172.30.102.118 | c0:b8:e6:ec:a1:5c | Dynamic | Yes |
| VLAN1 | 172.30.102.94 | c0:b8:e6:e9:e3:04 | Dynamic | Yes |
| VLAN1 | 172.30.102.84 | 00:d0:f8:22:74:5f | Dynamic | Yes |
| VLAN1 | 172.30.102.40 | c0:b8:e6:e3:3e:38 | Dynamic | Yes |
| VLAN1 | 172.30.102.139 | 30:0d:9e:3e:b4:62 | Dynamic | Yes |
| VLAN1 | 172.30.102.179 | 00:d0:f8:15:08:5c | Dynamic | Yes |
| VLAN1 | 172.30.102.90 | c0:b8:e6:7c:f2:7c | Dynamic | Yes |
| 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 |

14.1.6 MAC Address

Choose **Local Device > Diagnostics > Info Center > MAC**.

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

Note

To configure and manage the MAC address, see [6.2 Client Management](#).

Info Center

- Port Info
- VLAN Info
- Routing Info
- DHCP Clients
- ARP List
- MAC**
- DHCP Snooping
- IP-MAC Binding
- IP SOURCE GUARD
- CPP

MAC

Tip: Up to **16K** entries can be added.

Search by MAC

| Interface | MAC | Type | VLAN ID |
|-----------|-------------------|---------|---------|
| Gi24 | 70:B5:E8:5F:FD:29 | Dynamic | 1 |
| Gi24 | 50:9A:4C:42:C9:50 | Dynamic | 1 |
| Gi24 | 30:0D:9E:6F:C2:3C | Dynamic | 1 |
| Gi24 | 30:0D:9E:6F:C2:3D | Dynamic | 1 |
| Gi24 | C0:B8:E6:E9:78:07 | Dynamic | 1 |
| Gi24 | 30:B4:9E:8F:85:E5 | Dynamic | 1 |
| Gi24 | 58:69:6C:CE:72:B2 | Dynamic | 1 |
| Gi24 | 70:B5:E8:78:B7:8D | Dynamic | 1 |

14.1.7 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 [12.1 DHCP Snooping](#).

Info Center

- Port Info
- VLAN Info
- Routing Info
- DHCP Clients
- ARP List
- MAC
- DHCP Snooping**
- IP-MAC Binding

DHCP Snooping

DHCP Snooping: [Enabled](#) Option82: [Disabled](#) Trusted Port: [Gi24](#) [Refresh](#)

DHCP Snooping Binding Entries from the Trusted Port

| Interface | IP | MAC | VLAN ID | Lease Time(Min) |
|-----------|---------------|-------------------|---------|-----------------|
| Gi15 | 172.30.102.17 | 08:00:27:62:F0:53 | 1 | 240 |

IP-MAC Binding

Tip: Up to **500** entries can be added. Search by IP Address [Refresh](#)

| Port | IP | MAC |
|------|----|-----|
|------|----|-----|

14.1.8 IP-MAC Binding

Choose **Local Device > Diagnostics > Info Center > IP-MAC Binding**.

Displays the configured IP-MAC binding entries. The device checks whether the source IP addresses and source MAC addresses of IP packets match those configured for the device and filters out IP packets not matching the binding.

Note

To add or modify the IP-MAC binding, see [12.5 IP-MAC Binding](#).

Info Center

- Port Info
- VLAN Info
- Routing Info
- DHCP Clients
- ARP List
- MAC
- DHCP Snooping
- IP-MAC Binding**
- IP SOURCE GUARD

IP-MAC Binding

Tip: Up to **500** entries can be added. Search by IP Address [Refresh](#)

| Port | IP | MAC |
|------|-------------|-------------------|
| Gi29 | 192.168.1.1 | 00:11:22:33:44:55 |

IP SOURCE GUARD

Tip: Up to **1900** entries can be added. Search by IP Address [Refresh](#)

| Interface | Rule | IP | MAC | VLAN ID | Status |
|-----------|------|---------------|-------------------|---------|----------|
| Gi15 | IP | 172.30.102.17 | 08:00:27:62:F0:53 | 1 | Inactive |

14.1.9 IP Source Guard

Choose **Local Device > Diagnostics > Info Center > Source Guard**.

Displays the binding list of the IP Source Guard function. The IP Source Guard function will check the IP packets from non-DHCP trusted ports according to the list, and filter out the IP packets that are not in the binding list.

Note

To configure IP Source Guard function, see [12.5 IP-MAC Binding](#).

Port Info
VLAN Info
Routing Info
DHCP Clients
ARP List
MAC
DHCP Snooping
IP-MAC Binding
IP SOURCE GUARD
CPP

IP SOURCE GUARD

Tip: Up to **1900** entries can be added.
Search by IP Address

| Interface | Rule | IP | MAC | VLAN ID | Status |
|-----------|------|---------------|-------------------|---------|----------|
| Gi15 | IP | 172.30.102.17 | 08:00:27:62:F0:53 | 1 | Inactive |

CPP

Total CPU bandwidth: **2000pps**

| EtherType Value | Rate | Current Rate | Total messages |
|-----------------|-------|--------------|----------------|
| bodu | 60pps | 0pps | 0 |

14.1.10 PoE

Caution


Only PoE switches (model name containing -P, -LP, -HP, and -UP) support this function.

Choose **Local Device > Diagnostics > Info Center > PoE**.

Info Center
Port Info
VLAN Info
Routing Info
DHCP Clients
ARP List
MAC Address
DHCP Snooping
IP-MAC Binding
IP SOURCE GUARD
PoE
CPP

PoE

G1SK37500014B
Device1



Used Power 5.6w
Used Power 0w
Used Power 364.4w

Used Power **5.6W**
Reserved Power **0W**
Free Power **364.4W**
Peak Power **11.9W**
Powered Ports **1**

| | Port | PoE Status | Power Status | Priority | Current Power (W) | Non-Standard | Work Status |
|---|----------|------------|--------------|----------|-------------------|--------------|-----------------|
| > | Gi1/0/1 | Enable | Off | Low | 0 | No | PD Disconnected |
| > | Gi1/0/2 | Enable | Off | Low | 0 | No | PD Disconnected |
| > | Gi1/0/3 | Enable | Off | Low | 0 | No | PD Disconnected |
| > | Gi1/0/4 | Enable | Off | Low | 0 | No | PD Disconnected |
| > | Gi1/0/5 | Enable | Off | Low | 0 | No | PD Disconnected |
| > | Gi1/0/6 | Enable | Off | Low | 0 | No | PD Disconnected |
| > | Gi1/0/7 | Enable | Off | Low | 0 | No | PD Disconnected |
| > | Gi1/0/8 | Enable | Off | Low | 0 | No | PD Disconnected |
| > | Gi1/0/9 | Enable | Off | Low | 0 | No | PD Disconnected |
| > | Gi1/0/10 | Enable | Off | Low | 0 | No | PD Disconnected |

Total 24 < 1 2 3 > 10/page Go to page 1

14.1.11 CPP Info

Choose **Local Device > Diagnostics > Info Center > CPP**.

Displays the current total CPU bandwidth and statistics of various packet types, including the bandwidth, current rate, and total number of packets.

Info Center

Port Info

VLAN Info

Routing Info

DHCP Clients

ARP List

MAC

DHCP Snooping

IP-MAC Binding

IP SOURCE GUARD

CPP

CPP

Total CPU bandwidth: 2000pps

Refresh

| EtherType Value | Rate | Current Rate | Total messages |
|-----------------|---------|--------------|----------------|
| b pdu | 60pps | 0pps | 0 |
| lldp | 50pps | 0pps | 5328 |
| rldp | 50pps | 0pps | 0 |
| larp | 600pps | 0pps | 0 |
| arp | 400pps | 2pps | 426731 |
| dhcp | 600pps | 5pps | 622 |
| icmp | 600pps | 0pps | 3708 |
| macc | 600pps | 11pps | 190569 |
| mqtt | 600pps | 0pps | 0 |
| http/https | 1600pps | 4pps | 105864 |

Total 26

10/page

<

1

2

3

>

Go to page

1

14.2 Network Tools


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

14.2.1 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.

 **Network Tools**

Tool ☒ Ping ☐ Traceroute ☐ DNS Lookup

* IP Address/Domain

* Ping Count

* Packet Size Bytes

Start Stop

```
PING 172.30.102.1 (172.30.102.1): 64 data bytes
72 bytes from 172.30.102.1: seq=0 ttl=64 time=0.000 ms
72 bytes from 172.30.102.1: seq=1 ttl=64 time=0.000 ms
72 bytes from 172.30.102.1: seq=2 ttl=64 time=0.000 ms
72 bytes from 172.30.102.1: seq=3 ttl=64 time=0.000 ms


--- 172.30.102.1 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.000/0.000/0.000 ms
```

14.2.2 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**.

 **Network Tools**

Tool ☐ Ping ☒ Traceroute ☐ DNS Lookup

* IP Address/Domain

* Max TTL


```
traceroute to 172.30.102.30 (172.30.102.30), 20 hops max, 38
byte packets
1 172.30.102.133 (172.30.102.133) 2999.863 ms !H
```

14.2.3 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**.

 **Network Tools**

Tool ☐ Ping ☐ Traceroute ☒ **DNS Lookup**

* IP Address/Domain


Server: 127.0.0.1
Address 1: 127.0.0.1 localhost

Name: www.google.com
Address 1: 2001::67f0:b475
Address 2: 104.244.46.85

14.3 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.

 **Fault Collection**
Compress the configuration file for engineers to identify fault.

14.4 Cable Diagnostics

Choose **Local Device** > **Diagnostics** > **Cable Diagnostics**.

The cable diagnostics function can detect the approximate length of a cable connected to a port and whether the cable is faulty.

Select the port to be detected on the port panel and click **Start**. The detection results will be displayed below.

Port Panel

Available

Unavailable

Uplink

Copper

Fiber

13

15

17

19

21

23

25

27

29

31

33

35

37

39

41

43

45

47

49

51

2

4

6

8

10

12

14

16

18

20

22

24

26

28

30

32

34

36

38

40

42

44

46

48

50

52

Note: You can click and drag to select one or more ports.

Select AllInverseDeselect

Start

Result

| Port | Cable Length (cm) | Result |
|------|-------------------|--------|
| Gi15 | 700 | OK |

Caution

The SPF port does not support the function.

If a detected port contains an uplink port, the network may be intermittently disconnected. Exercise caution when performing this operation.

14.5 System Logs

Choose **Local Device > Diagnostics > System Logs**.

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

System Logs

View system logs.

Log List

Search

Q

local.info

syslog

kernel

kern.crit

| Time | Type | Module | Details |
|-----------------|------------|--------|------------------------------------|
| May 18 18:52:37 | kern.crit | kernel | %Port-2: GigabitEthernet12 link up |
| May 18 18:52:37 | local.info | syslog | %L3-6: Manage VLAN 1 change to UP |
| May 18 18:52:37 | kern.crit | kernel | %Port-2: GigabitEthernet13 link up |
| May 18 18:52:37 | kern.crit | kernel | %Port-2: GigabitEthernet17 link up |
| May 18 18:52:38 | kern.crit | kernel | %Port-2: GigabitEthernet22 link up |

14.6 Alerts

Choose **Local Device > Diagnostics > Alerts**.

Note

Click an alert in the **Alert Center** to view the faulty device, problem details, and description.

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.

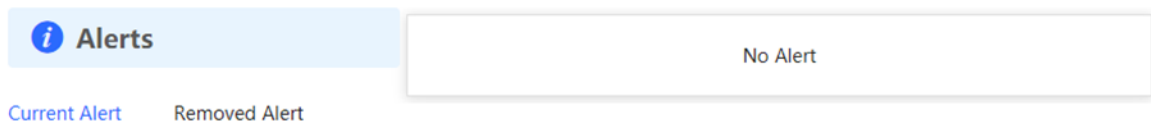


Table 14-1 Alert Types and Product Support

| 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. |
| 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. | N/A |
| 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. | N/A |
| 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. | N/A |
| The ARP table is full of ARP entries. | The number of ARP entries on the network exceeds the ARP capacity of the device. | N/A |
| 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 |

| Alert Type | Description | Support Description |
|------------------------------------|---|--|
| | | 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. | N/A |

 Caution



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


15 System Configuration


15.1 Setting the System Time


Choose **Local Device** > **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.


 Configure and view system time (The device has no RTC module. The time settings will not be saved upon reboot). 


Current Time 2022-05-20 14:32:29 


* Time Zone (GMT+8:00)Asia/Shanghai 


* NTP Server 0.cn.pool.ntp.org 


1.cn.pool.ntp.org 


2.cn.pool.ntp.org 


3.cn.pool.ntp.org 

0.asia.pool.ntp.org 

3.asia.pool.ntp.org 


0.pool.ntp.org 



1.pool.ntp.org 

rdate.darkorb.net 

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 

Cancel

OK

15.2 Setting the Web Login Password

Choose **Local Device** > **System** > **Login** > **Login Password**.

252

Enter the old password and new password. After saving the configuration, use the new password to log in.

 **Caution**

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



Change the login password. Please log in again with the new password later.

* Old Password

* New Password

* Confirm Password

Save

15.3 Setting the Session Timeout Duration

Choose **Local Device > System > Login > Session Timeout**.

If you do not log out after login, the web interface allows you to continue the access without authentication on the current browser within one hour by default. After one hour, the web interface automatically refreshes the page and you need to log in again before continuing your operations. You can change the session timeout duration.

15.4 Configuring SNMP

15.4.1 Overview

The Simple Network Management Protocol (SNMP) is a protocol for managing network devices. Based on the client/server model, it can achieve remote monitoring and control of network devices.

SNMP uses a manager and agent architecture. The manager communicates with agents through the SNMP protocol to retrieve information such as device status, configuration details, and performance data. It can also be used to configure and manage devices.

SNMP can be used to manage various network devices, including routers, switches, servers, firewalls, etc. You can achieve user management through the SNMP configuration interface and monitor and control devices through the third-party software.

15.4.2 Global Configuration

1. Overview

The purpose of global configuration is to enable the SNMP service and make the SNMP protocol version (v1/v2c/v3) take effect, so as to achieve basic configuration of local port, device location, and contact information.

SNMP v1: As the earliest version of SNMP, SNMP v1 has poor security, and only supports simple community string authentication. SNMP v1 has certain flaws, such as plaintext transmission of community strings and vulnerability to attacks. Therefore, SNMP v1 is not recommended for modern networks.

SNMP v2c: As an improved version of SNMP v1, SNMP v2c supports richer functions and more complex data types, with enhanced security. SNMP v2c performs better than SNMP v1 in terms of security and functionality, and is more flexible. It can be configured according to different needs.

SNMP v3: As the newest version, SNMP v3 supports security mechanisms such as message authentication and encryption compared to SNMP v1 and SNMP v2c. SNMP v3 has achieved significant improvements in security and access control.

2. Configuration Steps

Choose **Local Device > System > SNMP > Global Config**

(1) Enable the SNMP service.

Global Config

SNMP Service ☒

* SNMP Version ☐ v1 ☒ v2c ☒ v3

* Local Port

* Device Location

* Contact Info

Save

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 v3 users by selecting View/Group/Community/User Access Control before using the SNMP service.

Cancel OK

When it is enabled for the first time, SNMP v3 is enabled by default. Click **OK**.

(2) Set SNMP service global configuration parameters.

[Global Config](#) [View/Group/Community/Client Access Control](#) [Trap Settings](#)

SNMP Service ☒

* SNMP Version

☐ v1 ☒ v2c ☒ v3

* Local Port

* Device Location

* Contact Info

Save

Table 15-1 Global Configuration Parameters

| Parameter | Description |
|-----------------|---|
| SNMP Server | Indicates whether SNMP service is enabled. |
| SNMP Version | Indicates the SNMP protocol version, including v1, v2c, and v3 versions. |
| Local Port | The port range is 1 to 65535. |
| Device Location | 1-64 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. |
| Contact Info | 1-64 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. |

(3) Click **Save**.

After the SNMP service is enabled, click **Save** to make basic configurations such as the SNMP protocol version number take effect.

15.4.3 View/Group/Community/Client Access Control

1. View/Group/Community/Client Access Control

Management Information Base (MIB) can be regarded as a database storing the status information and performance data of network devices. It contains a large number of object identifiers (OIDs) to identify the status information and performance data of these network devices.

Views in SNMP can limit the range of MIB nodes that the management system can access, thereby improving the security and reliability of network management. Views are an indispensable part of SNMP and need to be configured or customized according to specific management requirements.

A view can have multiple subtrees. The management system can only access MIB nodes in these subtrees, and cannot access other unauthorized MIB nodes. This can prevent unauthorized system administrators from accessing sensitive MIB nodes, thereby protecting the security of network devices. Moreover, views can also improve the efficiency of network management and speed up the response from the management system.

- Configuration Steps

Choose **Local Device > System > SNMP > View/Group/Community/Client Access Control**.

(1) Click **Add** under the **View List** to add a view.

(2) Configure basic information of a view.

Table 15-2 View Configuration Parameters

| Parameter | Description |
|-----------|--|
| View Name | Indicates the name of the view. 1-32 characters. Chinese or full width characters are not allowed. |
| OID | Indicates the range of OIDs included in the view, which can be a single OID or a subtree of OIDs. |
| Type | There are two types of rules: included and excluded rules. <ul style="list-style-type: none"> ● The included rule only allows access to OIDs within the OID range. Click Add Included Rule to set this type of view. |

| Parameter | Description |
|-----------|---|
| | <ul style="list-style-type: none"> Excluded rules allow access to all OIDs except those in the OID range. Click Add Excluded Rule to configure this type of view. |

Note

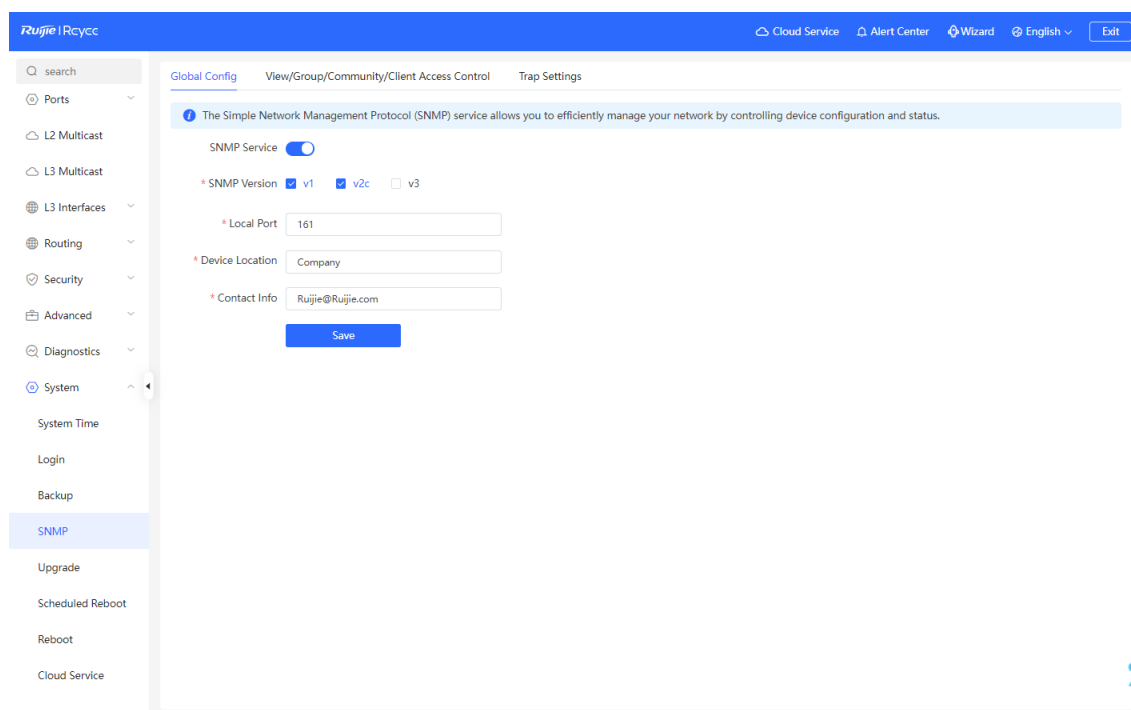
At least one OID rule must be configured for a view. Otherwise, an alarm message will appear.

(1) Click **OK**.

2. Configuring v1/v2c Users

● Overview

When the SNMP version is set to v1/v2c, user configuration is required.



The screenshot shows the Ruijie Rcycc web interface. The left sidebar contains a search bar and a list of navigation items: Ports, L2 Multicast, L3 Multicast, L3 Interfaces, Routing, Security, Advanced, Diagnostics, System (selected), System Time, Login, Backup, SNMP (highlighted), Upgrade, Scheduled Reboot, Reboot, and Cloud Service. The main content area is titled 'Global Config' and 'View/Group/Community/Client Access Control'. It features a blue header with the Ruijie logo and navigation links for Cloud Service, Alert Center, Wizard, English, and Exit. Below the header, a blue banner states: 'The Simple Network Management Protocol (SNMP) service allows you to efficiently manage your network by controlling device configuration and status.' The configuration section includes a toggle for 'SNMP Service' which is turned on. Under 'SNMP Version', there are checkboxes for v1, v2c (checked), and v3. Below this, there are input fields for 'Local Port' (161), 'Device Location' (Company), and 'Contact Info' (Ruijie@Ruijie.com). A blue 'Save' button is located at the bottom of the configuration section.

Note

Select the SNMP protocol version, and click **Save**. The corresponding configuration options will appear on the **View/Group/Community/User Access Control** page.

● Configuration Steps

Choose **Local Device** > **System** > **SNMP** > **View/Group/Community/Client Access Control**.

(1) Click **Add** in the SNMP v1/v2c Community Name List pane.

Global Config

View/Group/Community/Client Access Control

Trap Settings

SNMP v1/v2c Community Name List

+ Add

Delete Selected

Up to 20 entries are allowed.

| <input type="checkbox"/> | Community Name | Access Mode | MIB View | Action |
|--------------------------|----------------|--------------|----------|---|
| <input type="checkbox"/> | hello_12121 | Read & Write | all | Edit Delete |
| <input type="checkbox"/> | 34234234A. | Read-Only | all | Edit Delete |

Total 2

10/page

< 1 >

Go to page 1

(2) Add a v1/v2c user.

Add

×

* Community Name

* Access Mode

Read-Only

▼

* MIB View

all

▼

Add View +

Cancel

OK

Table 15-3 v1/v2c User Configuration Parameters

| Parameter | Description |
|----------------|---|
| Community Name | At least 8 characters. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Admin, public or private community names are not allowed. Question marks, spaces, and Chinese characters are not allowed. |
| Access Mode | Indicates the access permission (read-only or read & write) for the community name. |
| MIB View | The options under the drop-down box are configured views (default: all, none). |

 Note

- Community names cannot be the same among v1/v2c users.
- Click **Add View** to add a view.

3. Configuring v3 Groups

- Overview

SNMP v3 introduces the concept of grouping to achieve better security and access control. A group is a group of SNMP users with the same security policies and access control settings. With SNMP v3, multiple groups can be configured, each with its own security policies and access control settings. Each group can have one or more users.

- Prerequisites

When the SNMP version is set to v3, the v3 group configuration is required.



Note

Select the SNMP protocol version, and click **Save**. The corresponding configuration options will appear on the **View/Group/Community/User Access Control** page.

- Configuration Steps

Choose **Local Device > System > SNMP > View/Group/Community/Client Access Control**.

(1) Click **Add** in the SNMP v3 Group List pane to create a group.

| Group Name | Security Level | Read-Only View | Read & Write View | Notification View | Action |
|---------------|-----------------|----------------|-------------------|-------------------|-------------|
| default_group | Auth & Security | all | none | none | Edit Delete |

(2) Configure v3 group parameters.

Add



* Group Name

* Security Level

* Read-Only View [Add View +](#)

* Read & Write View [Add View +](#)

* Notification View [Add View +](#)

Cancel

OK

Table 15-4 v3 Group Configuration Parameters

| Parameter | Description |
|-------------------|--|
| Group Name | Indicates the name of the group. 1-32 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. |
| Security Level | Indicates the minimum security level (authentication and encryption, authentication but no encryption, no authentication and encryption) of the group. |
| Read-Only View | The options under the drop-down box are configured views (default: all, none). |
| Read & Write View | The options under the drop-down box are configured views (default: all, none). |
| Notify View | The options under the drop-down box are configured views (default: all, none). |

 **Note**

- A group defines the minimum security level, read and write permissions, and scope for users within the group.
- The group name must be unique. To add a view, click **Add View**.

(3) Click **OK**.

4. Configuring v3 Users

- Prerequisites

When the SNMP version is set to v3, the v3 group configuration is required.

Global Config View/Group/Community/Client Access Control Trap Settings

SNMP Service ☒

* SNMP Version ☐ v1 ☒ v2c ☒ v3

* Local Port

* Device Location

* Contact Info

Save



Note

Select the SNMP protocol version, and click **Save**. The corresponding configuration options will appear on the **View/Group/Community/User Access Control** page.

● Configuration Steps

Choose **Local Device > System > SNMP > View/Group/Community/Client Access Control**

(2) Click **Add** in the **SNMP v3 Client List** pane to add a v3 user.

Global Config

View/Group/Community/Client Access Control

Trap Settings

1/2 page

1

1

SNMP v3 Client List

+ Add

Delete Selected

Up to 50 entries are allowed.

| <input type="checkbox"/> | Username | Group Name | Security Level | Auth Protocol | Auth Password | Encryption Protocol | Encrypted Password | Action |
|--------------------------|----------|------------|----------------|---------------|---------------|---------------------|--------------------|--------|
| No Data | | | | | | | | |

Total 0

10/page

< 1 >

Go to page 1

(3) Configure v3 user parameters.

Add

* Username

123sdf!@

* Group Name

default_group

* Security Level

Auth & Security

* Auth Protocol

MD5

* Auth Password

* Encryption Protocol

AES

* Encrypted Password

Cancel

OK

Table 15-5 v3 User Configuration Parameters

| Parameter | Description |
|-----------|---|
| Username | Username At least 8 characters. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters. Admin, public or private community names are not allowed. Question marks, spaces, and Chinese characters are not allowed. |

| Parameter | Description |
|--|---|
| Group Name | Indicates the group to which the user belongs. |
| Security Level | Indicates the security level (authentication and encryption, authentication but no encryption, and no authentication and encryption) of the user. |
| Auth Protocol, Auth Password | <p>Authentication protocols supported: MD5/SHA/SHA224/SHA256/SHA384/SHA512.</p> <p>Authentication password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters.</p> <p>Note: This parameter is mandatory when the security level is authentication and encryption, or authentication but no encryption.</p> |
| Encryption Protocol, Encryption Password | <p>Encryption protocols supported: DES/AES/AES192/AES256.</p> <p>Encryption password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed.</p> <p>It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters.</p> <p>Note: This parameter is mandatory when the security level is authentication and encryption.</p> |

 **Note**

- The security level of v3 users must be greater than or equal to that of the group.
- There are three security levels, among which authentication and encryption requires the configuration of authentication protocol, authentication password, encryption protocol, and encryption password. Authentication but no encryption only requires the configuration of authentication protocol and encryption protocol, while no authentication and encryption does not require any configuration.

15.4.4 SNMP Service Typical Configuration Examples

1. Configuring SNMP v2c

- Application Scenario

You only need to monitor the device information, but do not need to set and deliver it. A third-party software can be used to monitor the data of nodes like 1.3.6.1.2.1.1 if v2c version is configured.

- Configuration Specification

According to the user's application scenario, the requirements are shown in the following table:

Table 15-6 User Requirement Specification

| Item | Description |
|------------|---|
| View range | Included rule: the OID is .1.3.6.1.2.1.1, and the custom view name is |

| Item | Description |
|-------------------------|--|
| | "system". |
| Version | For SNMP v2c, the custom community name is "public", and the default port number is 161. |
| Read & write permission | Read-only permission. |

- Configuration Steps

- (1) Choose **Local Device > System > SNMP > Global Config**, select v2c and set other settings as default. Then, click **Save**.

Global Config View/Group/Community/Client Access Control Trap Settings

SNMP Service ☒

* SNMP Version ☐ v1 ☒ v2c ☐ v3

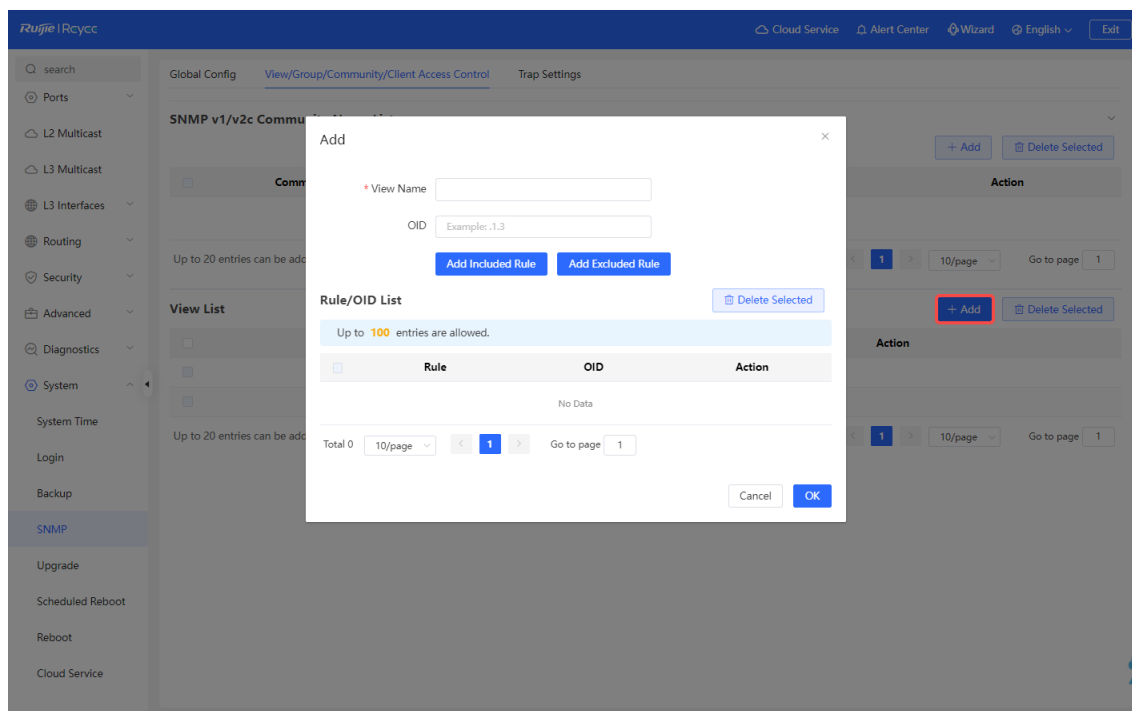
* Local Port

* Device Location

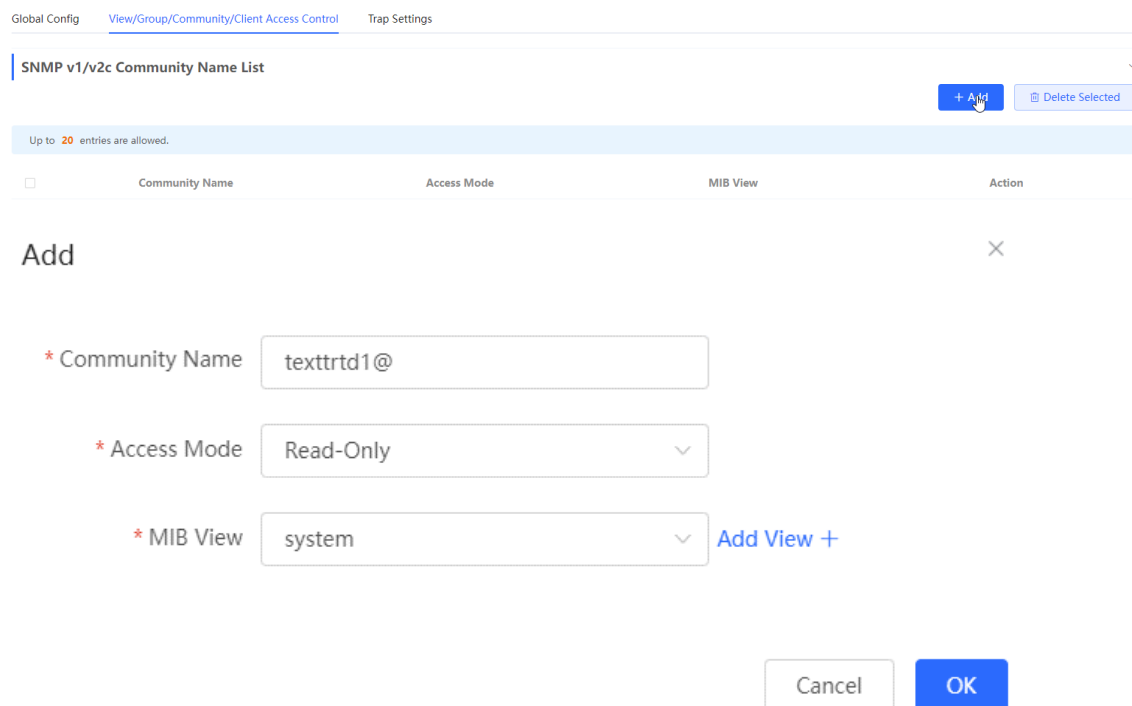
* Contact Info

Save

- (2) Choose **Local Device > System > SNMP > View/Group/Community/Client Access Control**, Add a view on the View/Group/Community/Client Access Control interface.
 - a Click **Add** in the **View List** pane.
 - b Enter the view name and OID in the pop-up window, and click **Add Included Rule**.
 - c Click **OK**.



- (2) 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.



2. v3 version SNMP service configuration

● Application Scenario

You need to monitor and control devices, and use the third-party software to monitor and deliver device information to public nodes (1.3.6.1.2.1). The security level of v3 is authentication and encryption.

● Configuration Specification

According to the user's application scenario, the requirements are shown in the following table:

Table 15-7 User Requirements Description Form

| Item | Description |
|----------------------|---|
| View range | Included rule: the OID is .1.3.6.1.2.1, and the custom view name is "public_view". |
| Group configuration | Group name: group Security level: authentication and encryption Select public_view for a read-only view. Select public_view for a read & write view. Select none for a notify view. |
| Configuring v3 Users | User name: v3_user Group name: group Security level: authentication and encryption Authentication protocol/password: MD5/Ruijie123 Encryption protocol/password: AES/Ruijie123 |
| Version | For SNMP v3, the default port number is 161. |

- Configuration Steps

- (2) Choose **Local Device > System > SNMP > Global Config**, select v3, and change the port number to 161. Set other settings to defaults. Then, click **Save**.

[Global Config](#)
[View/Group/Community/Client Access Control](#)
[Trap Settings](#)

SNMP Service ☒

* SNMP Version ☐ v1 ☐ v2c ☒ v3

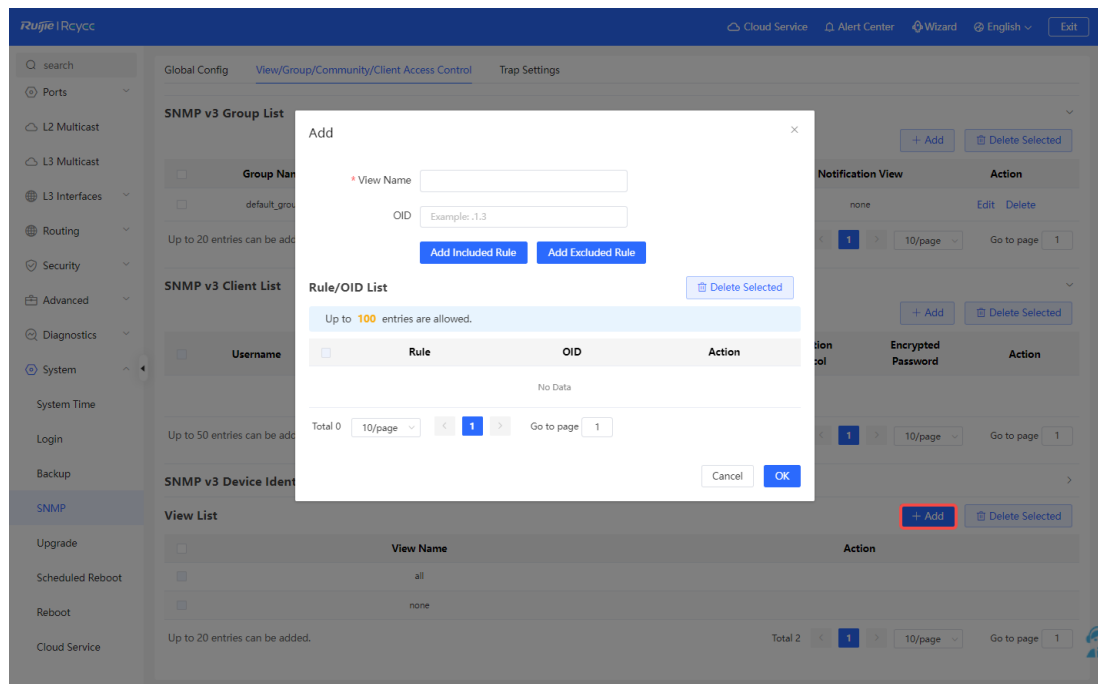
* Local Port

* Device Location

* Contact Info

- (2) Choose **Local Device > System > SNMP > View/Group/Community/Client Access Control**. Add a view on the View/Group/Community/Client Access Control interface.

- a Click **Add** in the **View List** pane.
- b Enter the view name and OID in the pop-up window, and click **Add Included Rule**.
- c Click **OK**.



- (3) Click **Add** in the SNMP v3 group list, fill in the group name and security level in the pop-up window, the user has read and write permissions, select "public _view" for the readable view and read and write view, and set the notification view to none. After the operation is complete, click **OK**.

| SNMP v3 Group List | | | | | | |
|---|---------------|-----------------|----------------|-------------------|-------------------|---|
| | | | | | | + Add Delete Selected |
| Up to 20 entries are allowed. | | | | | | |
| <input type="checkbox"/> | Group Name | Security Level | Read-Only View | Read & Write View | Notification View | Action |
| <input type="checkbox"/> | default_group | Auth & Security | all | none | none | Edit Delete |
| Total 1 10/page < 1 > Go to page 1 | | | | | | |

×

Add

* Group Name

* Security Level

* Read-Only View [Add View +](#)

* Read & Write View [Add View +](#)

* Notification View [Add View +](#)

- (4) Click Add in the SNMP v3 user list, fill in the user name and group name in the pop-up window, the user security level adopts authentication and encryption mode, fill in the corresponding authentication protocol, authentication password, encryption protocol, and encryption password, and click **OK**.

| SNMP v3 Client List | | | | | | | | |
|---|----------|------------|----------------|---------------|---------------|---------------------|--------------------|--------|
| Up to 50 entries are allowed. | | | | | | | | |
| <input type="checkbox"/> | Username | Group Name | Security Level | Auth Protocol | Auth Password | Encryption Protocol | Encrypted Password | Action |
| No Data | | | | | | | | |
| Total 0 10/page < 1 > Go to page 1 | | | | | | | | |

×

Add

* Username

* Group Name

* Security Level

* Auth Protocol * Auth Password

* Encryption Protocol * Encrypted Password

15.4.5 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,

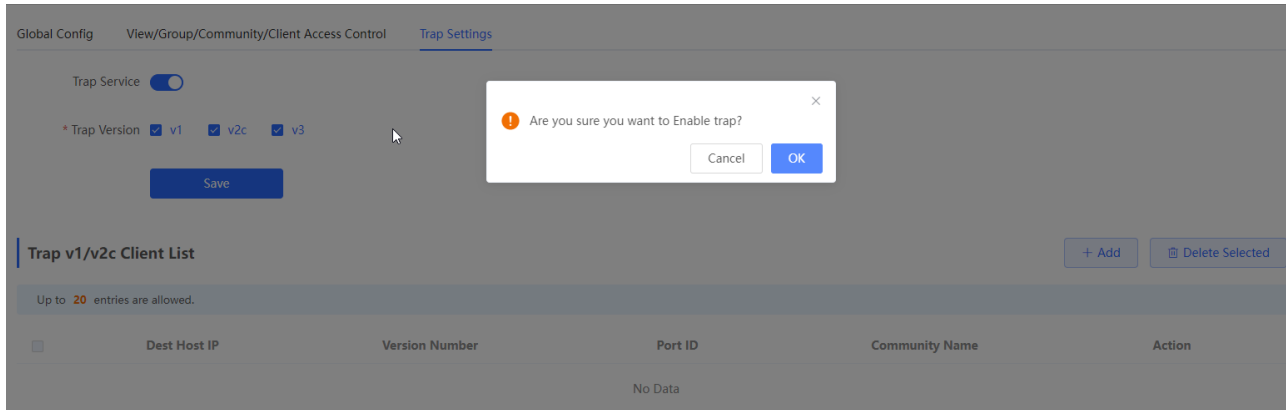
performance reports, configuration reports and security management. Trap can provide real-time network monitoring and fault diagnosis to help administrators find and solve network problems in time.

1. Trap open settings

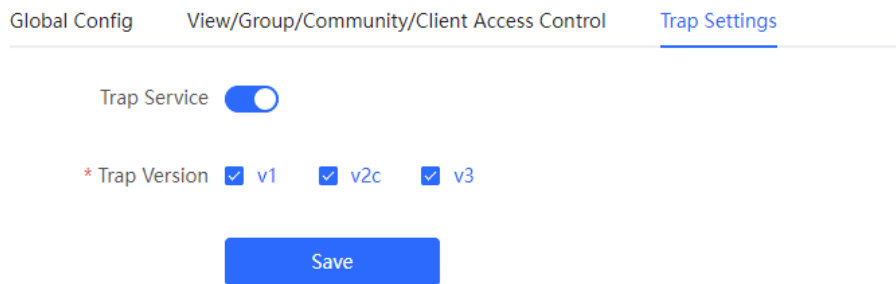
Enable the trap service and select the effective trap protocol version, including v1, v2c, and v3.

Choose **Local Device > System > SNMP > Trap setting**

(1) Enable the trap service switch.



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



(2) Set the trap version.

The trap protocol version number includes v1 version, v2c version, and v3 version.

(3) Click **OK**.

After the trap service is enabled, you need to click **Save**, and the configuration of the trap protocol version number will take effect.

2. Trap v1/v2c user configuration

● Introduction

A trap is a notification mechanism used to send an alert to administrators when important events or failures occur on a device or service. Trap v1/v2c are two versions of SNMP protocol, used for network management and monitoring.

Trap v1 is the first version in the SNMP protocol, which supports basic alarm notification functions. trap v2c is the second version in the SNMP protocol, which supports more alarm notification options and more advanced security.

By using trap v1/v2c, the administrator can know the problems on the network in time and take corresponding measures.

- Prerequisites

When the trap service version selects v1 or v2c, a trap v1v2c user needs to be created.

- Configuration Steps

Choose **Local Device > System > SNMP > Trap setting**.

(1) Click Add in the Trap v1v2c User list to create a trap v1v2c user.

Global Config View/Group/Community/Client Access Control **Trap Settings**

Trap Service ☒

* Trap Version ☒ v1 ☒ v2c ☒ v3

Save

Trap v1/v2c Client List + Add Delete Selected

Up to 20 entries are allowed.

| | Dest Host IP | Version Number | Port ID | Community Name | Action |
|--|--------------|----------------|---------|----------------|--------|
| | No Data | | | | |

(2) Configure trap v1v2c user-related parameters.

Add

×

* Dest Host IP

* Version Number

* Port ID

* Community

Name/Username

Cancel

OK

Table 15-8 Trap v1/v2c user information description table

| Parameter | Description |
|--------------------------|---|
| Dest Host IP | IP address of the trap peer device. An IPv4 or IPv6 address is supported. |
| Version Number | Trap version, including v1 and v2c. |
| Port ID | The port range of the trap peer device is 1 to 65535. |
| Community name/User name | <p>Community name of the trap user.</p> <p>At least 8 characters.</p> <p>It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters.</p> <p>Admin, public or private community names are not allowed.</p> |

| Parameter | Description |
|-----------|---|
| | Question marks, spaces, and Chinese characters are not allowed. |

Note

- The destination host IP address of trap v1/ v1/v2c users cannot be the same.
- Community names of trap v1/ v1/v2c users cannot be the same.

(3) Click OK.

3. trap v3 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.

• Prerequisites

When v3 is selected as the trap service version, a trap v3 user needs to be created.

• Configuration Steps

Choose **Local Device > System > SNMP > Trap setting**.

(1) Click Add in the "Trap v3 user" list to create a trap v3 user.

Trap v3 Client List

+ Add

Delete Selected

Up to 20 entries are allowed.

| <input type="checkbox"/> | Dest Host IP | Port ID | Username | Security Level | Auth Password | Encrypted Password | Action |
|--------------------------|--------------|---------|----------|----------------|---------------|--------------------|--------|
| No Data | | | | | | | |

(2) Configure parameters related to trap v3 users.

Add
×

* Dest Host IP

Support IPv4/IPv6

* Port ID

* Username

* Security Level

Auth & Security

* Auth Protocol

MD5

* Auth Password

* Encryption Protocol

AES

* Encrypted Password

Cancel

OK

Table 15-9 trap v3 user information description table

| Parameter | Description |
|--|---|
| Dest Host IP | IP address of the trap peer device. An IPv4 or IPv6 address is supported. |
| Port ID | The port range of the trap peer device is 1 to 65535. |
| Username | <p>Name of the trap v3 user.</p> <p>At least 8 characters.</p> <p>It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters.</p> <p>Admin, public or private community names are not allowed.</p> <p>Question marks, spaces, and Chinese characters are not allowed.</p> |
| Security Level | Indicates the security level of the trap v3 user. The security levels include authentication and encryption, authentication but no encryption, and no authentication and encryption. |
| Auth Protocol, Auth Password | <p>Authentication protocols supported: MD5/SHA/SHA224/SHA256/SHA384/SHA512.</p> <p>Authentication password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed. It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters.</p> <p>Note: This parameter is mandatory when the security level is authentication and encryption, or authentication but no encryption.</p> |
| Encryption Protocol, Encryption Password | <p>Encryption protocols supported: DES/AES/AES192/AES256.</p> <p>Encryption password: 8-31 characters. Chinese characters, full-width characters, question marks, and spaces are not allowed.</p> <p>It must contain at least three character categories, including uppercase and lowercase letters, digits, and special characters.</p> <p>Note: This parameter is mandatory when the security level is authentication and encryption.</p> |

**Note**

IP of trap v1/v2c/v3 users cannot be repeated.

15.4.6 Typical configuration examples of the trap service

1. v2c version trap configuration

- Application Scenarios

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 Specification

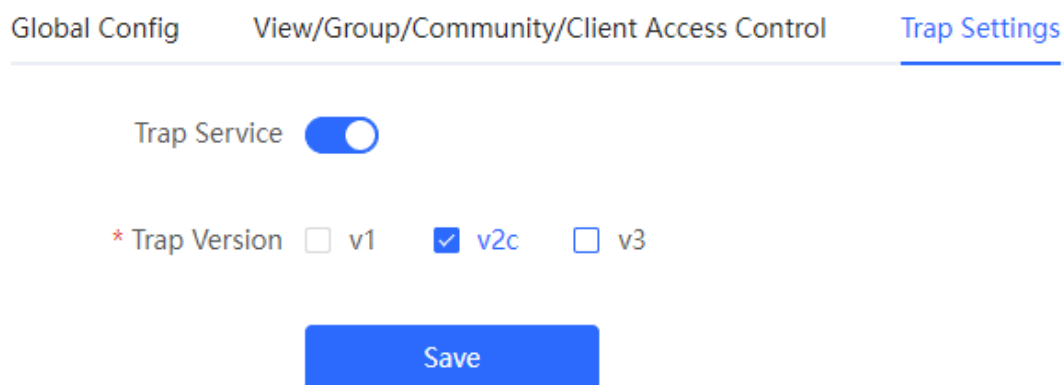
According to the analysis of the user's usage scenario, the requirements are shown in the table:

Table 15-10 User Requirements Description Form

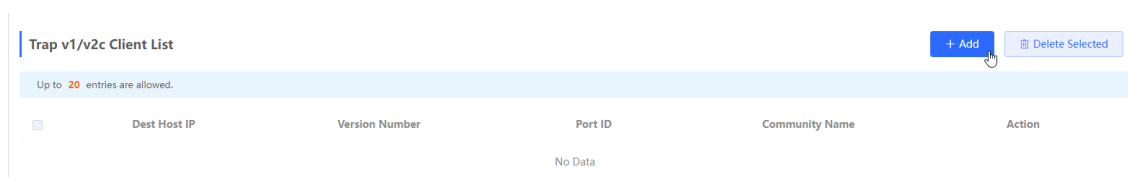
| Item | Description |
|----------------------------|--|
| IP address and port number | The destination host IP is 192.168.110.85, and the port number is 166. |
| Version | Select the v2 version. |
| Community name/User name | Trap_user |

- Configuration Steps

- (1) Choose **Local Device > System > SNMP > Trap setting**. Select the v2c version on the trap setting interface, click **Save**,



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



- (3) Fill in the target host IP, version number, port number, user name and other information, and click OK after the configuration is complete.

Add ×

* Dest Host IP

192.168.110.77

* Version Number

v1

* Port ID

123

* Community

123e#dfd

Name/Username

Cancel

OK

2. V3 version trap configuration

- Application Scenarios

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 Specification

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

Table 15-11 User Requirements Description Form

| Item | Description |
|--|--|
| IP address and port number | The destination host IP is 192.168.110.87, and the port number is 167. |
| Version and user name | Select the v3 version and trapv3_user for the user name. |
| Authentication protocol/authentication password | Authentication protocol/password: MD5/Ruijie123 |
| Encryption protocol/encryption password | Encryption protocol/password: AES/Ruijie123 |

- Configuration Steps

- (1) Select the v3 version on the trap setting interface, and click **Save**.

[Global Config](#)[View/Group/Community/Client Access Control](#)[Trap Settings](#)Trap Service ☒* Trap Version ☐ v1 ☐ v2c ☒ v3[Save](#)

- (2) Click Add in the trap v3 user list.
- (3) Fill in the target host IP, port number, user name and other information, and click OK after the configuration is complete.

Add ×

| | | | |
|-----------------------|---|----------------------|--|
| * Dest Host IP | <input type="text" value="192.168.110.87"/> | * Port ID | <input type="text" value="167"/> |
| * Username | <input type="text" value="trapuser1_"/> | * Security Level | <input type="text" value="Auth & Security"/> |
| * Auth Protocol | <input type="text" value="MD5"/> | * Auth Password | <input type="text" value="Ruijie123"/> |
| * Encryption Protocol | <input type="text" value="AES"/> | * Encrypted Password | <input type="text" value="Ruijie123"/> |

[Cancel](#) [OK](#)


15.5 Configuration Backup and Import

Choose **Local Device** > **System** > **Management** > **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.

[Backup & Import](#)[Reset](#)

 If the target version is much later than the current version, some configuration may be missing. It is recommended 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](#)


15.6 Reset

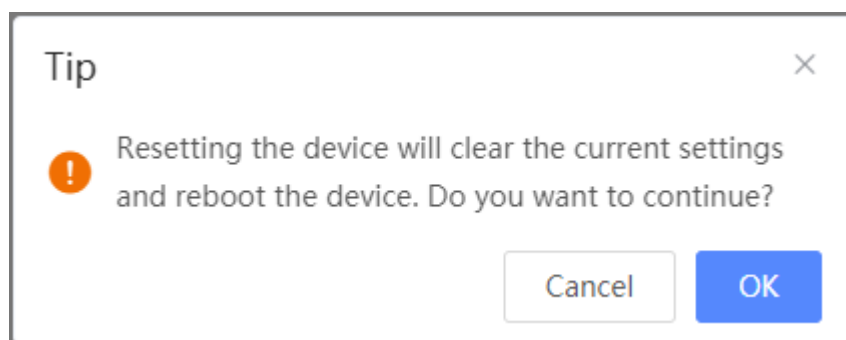
15.6.1 Resetting the Device

Choose **Local Device** > **System** > **Management** > **Reset**.

Click **Reset**, and click **OK** to restore factory settings.

[Backup & Import](#)[Reset](#)

 Resetting the device will clear the current settings. If you want to keep the configuration, please [Backup Config](#) first.

[Reset](#)

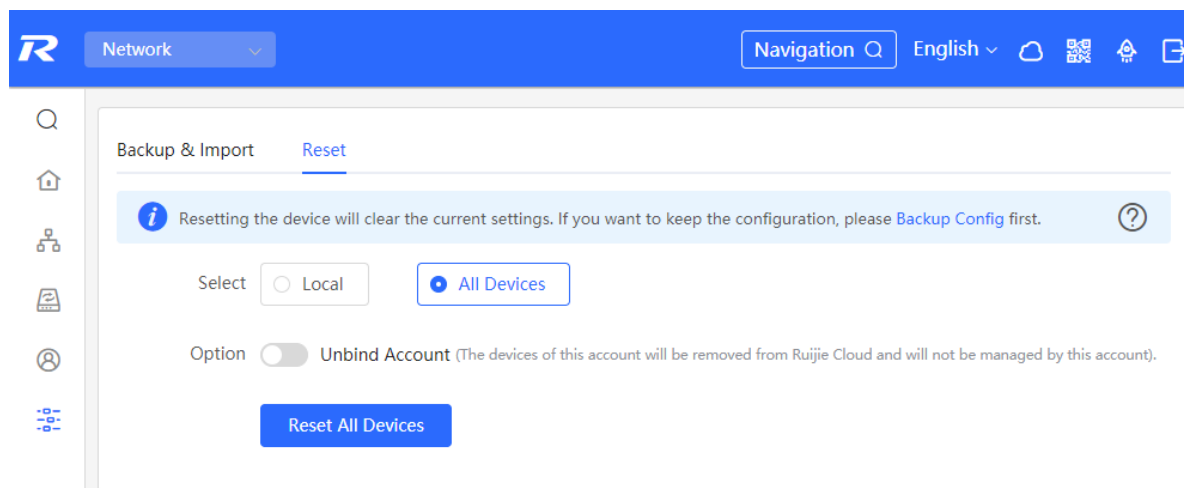
Caution

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 [15.5 Configuration Backup and Import](#)) before restoring the factory settings. Exercise caution when performing this operation.

15.6.2 Resetting the Devices on the network

Choose **Network-Wide** > **System** > **Management** > **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.



Caution

Resetting the network will clear current settings of all devices on the network and reboot the devices. Exercise caution when performing this operation.

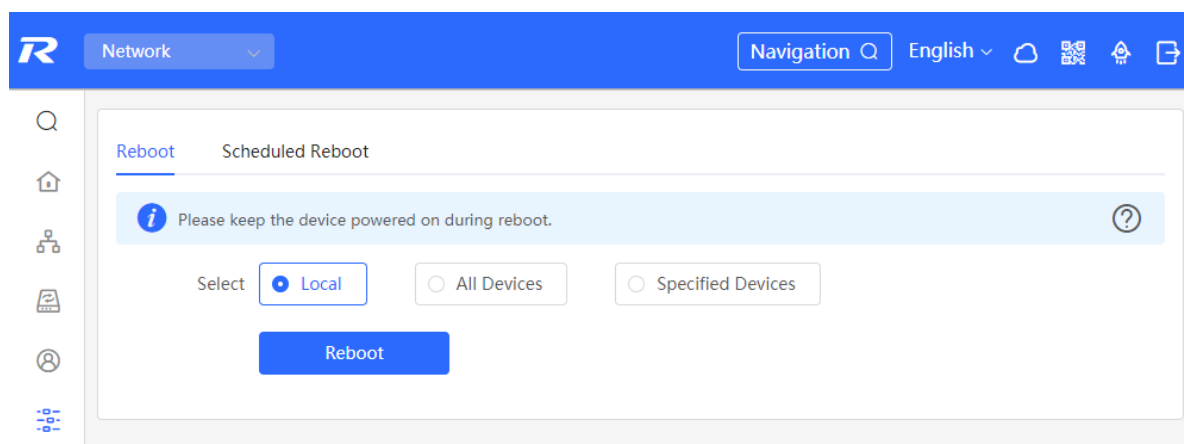
15.7 Rebooting the Device

15.7.1 Rebooting the Device

Choose **Self-Organizing Mode** > **Network** > **System** > **Management** > **Reset**.

Choose **Standalone Mode** > **System** > **Reboot**.

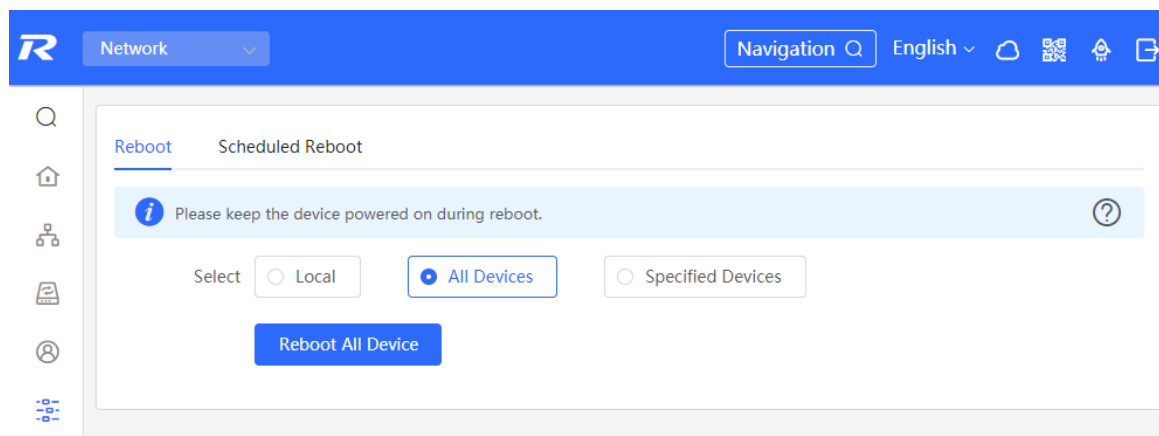
Select **Local** and click **All Devices**. The device will restart. Do not refresh the page or close the browser during the reboot. After the device is successfully rebooted and the Web service becomes available, the device automatically jumps to the login page.



15.7.2 Rebooting the Devices on the Network

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

Select **All Devices**, and click **Reboot All Device** to reboot all devices in the current network.



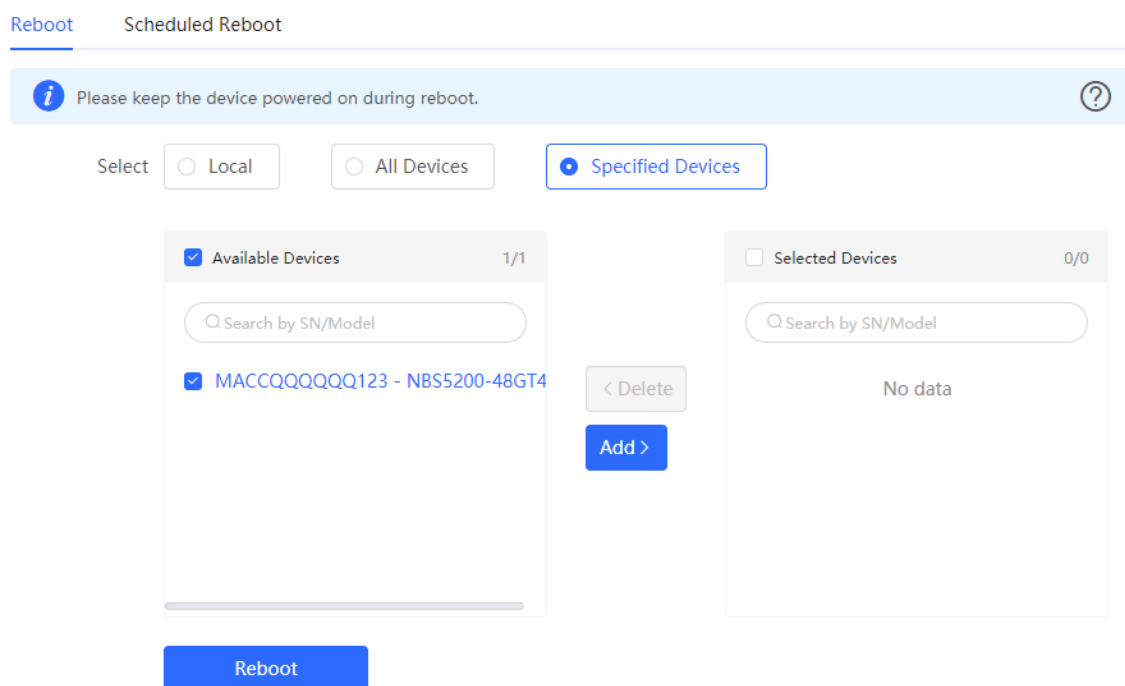
Caution

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.

15.7.3 Rebooting Specified Devices on the Network

Choose **Network > 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.



15.8 Configuring Scheduled Reboot

Confirm that the system time is accurate. For details about how to configure the system time, see [15.1](#). To avoid network interruption caused by device reboot at wrong time.

Choose **Self-Organizing Mode** > **Network** > **System** > **Scheduled Reboot**.

Choose **Standalone Mode** > **System** > **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 on the network mode, all devices on the network will reboot when the system time matches to the timed time. Therefore, exercise caution when performing this operation.

Reboot Scheduled Reboot



It is recommended to set the scheduled time to a network idle time, e.g., 2 A.M..
The downlink device will also be rebooted as scheduled.

Enable ☒

Day ☒ Mon ☒ Tue ☒ Wed ☒ Thu ☒ Fri ☒ Sat ☒ Sun

Time :

Save

15.9 Upgrade

 **Caution**

- It is recommended to back up the configuration before software upgrade.
 - Version upgrade will restart the device. Do not refresh or close the browser during the upgrade process.
-

15.9.1 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.




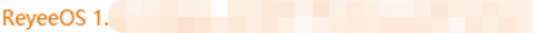
Note



- Online upgrade will retain the current configuration.
 - Do not refresh the page or close the browser during the upgrade process. After successful upgrade, you will be redirected to the login page automatically.
-

[Online Upgrade](#) [Local Upgrade](#)

 Online upgrade will keep the current configuration. Please do not refresh the page or close th

Current Version 

New Version 

Description 1. 
2. 

Tip 1. If your device cannot access the Internet, please click [Download File](#).
2. Choose [Local Upgrade](#) to upload the file for local upgrade.



[Upgrade Now](#)


15.9.2 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](#)

 Please do not refresh the page or close the browser. 

Model 

Current Version 

Keep Config ☒ (If the target version is much later than the current version, it is recommended not to keep the configuration.)

File Path [Browse](#) [Upload](#)

15.10 Cloud Service

15.10.1 Overview

The Cloud Service feature provides powerful remote network management and operation capabilities, making it convenient and efficient to manage geographically dispersed networks with diverse device types. This feature supports wireless devices, switches, and gateways, enabling unified network management and visualized monitoring and operation. Additionally, it also offers various components such as real-name authentication, dedicated Wi-Fi, and passenger flow analysis, allowing for flexible expansion of network services.

By configuring Cloud Service, you can conveniently manage networks through Ruijie Cloud or the Ruijie Reyee app.

15.10.2 Configuration Steps

Choose **One-Device > Config > System > Cloud Service**.

If the device is not currently associated with a cloud account, simply follow the on-screen instructions to add it to the network. Open up the Ruijie Reyee app, click the scan icon at the upper left corner on the **Project** page, and enter the device's management password.



Once the device is associated with a cloud account, it will automatically be bound to a cloud server based on its geographic location.

⚠ Caution

Exercise caution when modifying cloud service configurations as improper modifications may lead to connectivity issues between the device and the cloud service.

Cloud Server

☒ China CloudConnected [Cancel](#)

This device is connected to Ruijie Cloud. The IP is 120.27.22.80, Exercise caution when modifying the cloud service configuration to ensure uninterrupted device connectivity.

Cloud Server [Reset](#)

* Domain Name [Configure IP](#)

IP Address

[Save](#)

To change the Cloud Service configurations, select the cloud server from the **Cloud Server** drop-down list, enter the domain name and IP address, and click **Save**.

Note

If the server selected is not **Other Cloud**, the system automatically fills in the domain name and IP address of the cloud server. When **Other Cloud** is selected, you need to manually configure the domain name and IP address and upload the cloud server certificate.

Table 15-12 Cloud Server Description

| Parameter | Description |
|--------------|---|
| Cloud Server | Geographic location of the cloud server, including China Cloud, Asia Cloud, Europe Cloud, America Cloud, and Other. |
| Domain Name | Domain name of the cloud server. |
| IP Address | IP address of the cloud server. |

15.10.3 Unbinding Cloud Service

Choose **One-Device > Config > System > Cloud Service**

You can click **Unbind** to unbind the account if you no longer wish to manage this project remotely.

Project Name:radio

Account:

Unbind the account if you no longer wish to manage this project remotely.

It is used to unbind all devices throughout the network. To unbind a single device, remove the device from the network and restore its default settings.

[Unbind](#)