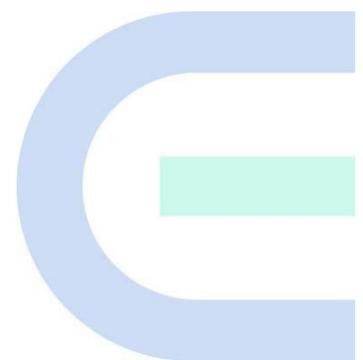


Ruijie Reyee RG-EG-W Series Wireless Routers

ReyeeOS 2.340[320] Configuration Guide



Copyright

Copyright © 2025 Ruijie Networks

All rights are reserved in this document and this statement.

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



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

- Official website of Ruijie Reye: <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 | <ol style="list-style-type: none">1. Button names2. Window names, tab name, field name and menu items3. Link | <ol style="list-style-type: none">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

This manual introduces the product model, port type and CLI for your reference. 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 2.340 | 1 |
| 1.1.1 Hardware Change..... | 1 |
| 1.1.2 Software Feature Change..... | 1 |
| 1.2 ReyeeOS 2.320 | 4 |
| 1.2.1 Hardware Change..... | 4 |
| 1.2.2 Software Feature Change..... | 4 |
| 2 Login..... | 6 |
| 2.1 Configuration Environment Requirements | 6 |
| 2.1.1 PC | 6 |
| 2.2 Default Configuration | 6 |
| 2.3 Login to the Web Interface | 6 |
| 2.3.1 Connecting to the Router..... | 6 |
| 2.3.2 Configuring the IP Address of the Management Client | 6 |
| 2.3.3 Login | 7 |
| 2.3.4 Frequently-Used Controls on the Web Page..... | 8 |
| 2.4 Work Mode..... | 9 |
| 2.4.1 Router Mode | 9 |
| 2.4.2 AP Mode..... | 9 |
| 2.4.3 Wireless Repeater | 9 |
| 2.4.4 WISP | 9 |
| 2.5 Configuration Wizard (Router Mode)..... | 10 |

| | |
|---|----|
| 2.5.1 Getting Started..... | 10 |
| 2.5.2 Configuration Steps | 10 |
| 2.5.3 Forgetting the PPPoE Account | 12 |
| 2.6 Configuration Wizard (AP Mode)..... | 13 |
| 2.6.1 Getting Started..... | 13 |
| 2.6.2 Configuration Steps | 13 |
| 2.7 Configuration Wizard (Wireless Repeater)..... | 13 |
| 2.7.1 Getting Started..... | 13 |
| 2.7.2 Configuration Steps | 14 |
| 2.8 Configuration Wizard (WISP) | 16 |
| 2.8.1 Getting Started..... | 16 |
| 2.8.2 Configuration Steps | 16 |
| 2.9 Switching the Work Mode..... | 18 |
| 3 Network-Wide Monitoring..... | 21 |
| 3.1 Viewing Networking Information..... | 21 |
| 3.2 Adding Networking Devices..... | 23 |
| 3.2.1 Wired Connection | 23 |
| 3.2.2 AP Mesh..... | 24 |
| 3.3 Configuring the Service Network..... | 27 |
| 3.3.1 Configuring the Wired Network..... | 27 |
| 3.3.2 Configuring the Wireless Network | 29 |
| 3.4 Supporting Traffic Monitoring | 32 |
| 3.4.1 Viewing Real-Time Traffic..... | 32 |
| 3.4.2 Viewing Historical Traffic..... | 36 |

| | |
|--|----|
| 3.5 Supporting the URL Logging Function | 39 |
| 3.6 Processing Alerts | 40 |
| 4 Network Settings | 42 |
| 4.1 Switching the Work Mode | 42 |
| 4.1.1 Work Mode | 42 |
| 4.1.2 Self-Organizing Network Discovery | 42 |
| 4.1.3 Configuration Steps | 42 |
| 4.2 Port Settings | 43 |
| 4.2.1 Setting the Port Parameters | 43 |
| 4.2.2 Viewing the Port Information | 44 |
| 4.3 Configuring the WAN Ports | 45 |
| 4.3.1 Configuring the Internet Access Mode | 45 |
| 4.3.2 Modifying the MAC Address | 46 |
| 4.3.3 Modifying the MTU | 47 |
| 4.3.4 Configuring the Private Line | 48 |
| 4.3.5 Configuring the VLAN Tag | 49 |
| 4.3.6 Configuring NAT Mode | 49 |
| 4.3.7 Configuring the Multi-Line Load Balancing Mode | 50 |
| 4.3.8 Configuring Line Detection | 55 |
| 4.4 Configuring the LAN Ports | 58 |
| 4.4.1 Modifying the LAN Port IP Address | 58 |
| 4.4.2 Modifying the MAC Address | 59 |
| 4.5 Configuring VLAN | 60 |
| 4.5.1 VLAN Overview | 60 |

| | |
|--|----|
| 4.5.2 Creating a VLAN | 61 |
| 4.5.3 Configuring a Port VLAN | 62 |
| 4.6 Configuring Repeater Mode | 63 |
| 4.6.1 Wired Repeater..... | 63 |
| 4.6.2 Wireless Repeater | 63 |
| 4.7 Configuring WISP | 65 |
| 4.8 Configuring DNS..... | 67 |
| 4.8.1 Local DNS..... | 67 |
| 4.8.2 DNS Policy..... | 67 |
| 4.8.3 DNS Proxy | 69 |
| 4.9 Configuring IPv6 | 69 |
| 4.9.1 IPv6 Overview..... | 69 |
| 4.9.2 IPv6 Basics | 70 |
| 4.9.3 IPv6 Address Allocation Modes | 70 |
| 4.9.4 Enabling the IPv6 Function..... | 71 |
| 4.9.5 Configuring an IPv6 Address for the WAN Port..... | 71 |
| 4.9.6 Configuring an IPv6 Address for the LAN Port | 73 |
| 4.9.7 Viewing the DHCPv6 Client..... | 75 |
| 4.9.8 Configuring the Static DHCPv6 Address | 75 |
| 4.9.9 Configuring the IPv6 Neighbor List..... | 76 |
| 4.10 Configuring a DHCP Server | 77 |
| 4.10.1 DHCP Server Overview | 77 |
| 4.10.2 Address Allocation Mechanism..... | 77 |
| 4.10.3 Configuring the DHCP Server..... | 78 |

| | |
|--|-----|
| 4.10.4 Viewing the DHCP Client..... | 80 |
| 4.10.5 Configuring Static IP Addresses | 80 |
| 4.11 Configuring Routes | 82 |
| 4.11.1 PBR | 82 |
| 4.11.2 Configuring Static Routes | 90 |
| 4.11.3 Configuring the IPv6 Static Route..... | 92 |
| 4.11.4 Set URL Route | 94 |
| 4.12 Configuring ARP Binding and ARP Guard | 95 |
| 4.12.1 Overview | 95 |
| 4.12.2 Configuring ARP Binding | 95 |
| 4.12.3 Configuring ARP Guard | 96 |
| 4.13 Configuring MAC Address Filtering | 97 |
| 4.13.1 Overview | 97 |
| 4.13.2 Configuration Steps | 97 |
| 4.14 Port Mapping..... | 98 |
| 4.14.1 Overview | 98 |
| 4.14.2 Getting Started..... | 98 |
| 4.14.3 Configuration Steps | 98 |
| 4.14.4 Verification and Test..... | 100 |
| 4.14.5 Solution to Test Failure | 100 |
| 4.14.6 Configuration Steps (DMZ)..... | 100 |
| 4.15 UPnP..... | 102 |
| 4.15.1 Overview | 102 |
| 4.15.2 Configuring UPnP | 102 |

| | |
|--|-----|
| 4.15.3 Verifying Configuration..... | 103 |
| 4.16 Dynamic DNS | 103 |
| 4.16.1 Overview | 103 |
| 4.16.2 Getting Started..... | 103 |
| 4.16.3 Configuring DDNS | 103 |
| 4.17 Connecting to IPTV..... | 105 |
| 4.17.1 Getting Started..... | 105 |
| 4.17.2 Configuration Steps (VLAN Type) | 105 |
| 4.17.3 Configuration Steps (IGMP Type)..... | 106 |
| 4.18 Limiting the Number of Connections | 107 |
| 4.19 Configuring Local Security..... | 108 |
| 4.19.1 Configuring an Admin IP Address..... | 108 |
| 4.19.2 Configuring Security Zones | 111 |
| 4.19.3 Configuring Session Attack Prevention | 113 |
| 4.19.4 Checking the Security Log..... | 115 |
| 4.20 Configuring TTL Rules..... | 116 |
| 4.20.1 Overview | 116 |
| 4.20.2 Configuring TTL Rules..... | 116 |
| 4.21 Configuring USB Settings..... | 119 |
| 4.22 Configuring Self-Healing Mesh..... | 120 |
| 4.23 Hardware Acceleration | 120 |
| 4.24 Configuring Audit Log | 121 |
| 4.25 Other Settings..... | 122 |
| 5 Wireless Management | 124 |

| | |
|---|-----|
| 5.1 Configuring AP Groups..... | 124 |
| 5.1.1 Overview | 124 |
| 5.1.2 Configuration Steps | 124 |
| 5.2 Configuring Wi-Fi..... | 125 |
| 5.2.1 Adding a Wi-Fi Network | 125 |
| 5.2.2 Configuring Guest Wi-Fi | 130 |
| 5.2.3 Managing Wi-Fi Networks..... | 131 |
| 5.3 Healthy Mode..... | 132 |
| 5.4 RF Settings | 133 |
| 5.4.1 Configuring Global Radio Settings | 133 |
| 5.4.2 Configuring Standalone Radio Settings | 135 |
| 5.5 Configuring Wi-Fi Blocklist or Allowlist | 136 |
| 5.5.1 Overview | 136 |
| 5.5.2 Configuring a Global Blocklist/Allowlist | 136 |
| 5.5.3 Configuring an SSID-based Blocklist/Allowlist | 137 |
| 5.6 Configuring AP Load Balancing..... | 138 |
| 5.6.1 Overview | 138 |
| 5.6.2 Configuring Client Load Balancing | 138 |
| 5.6.3 Configuring Traffic Load Balancing..... | 140 |
| 5.7 Configuring Wireless Rate Limiting | 141 |
| 5.7.1 Overview | 141 |
| 5.7.2 Configuration Steps | 142 |
| 5.8 Wireless Network Optimization..... | 145 |
| 5.8.1 Wireless Network Optimization 2.0 Version | 145 |

| | |
|---|-----|
| 5.8.2 Wireless Network Optimization 1.0 Version | 150 |
| 5.8.3 Wi-Fi Roaming Optimization (802.11k/v) | 152 |
| 5.8.4 Configuring IGMP Snooping | 153 |
| 5.9 Reye Mesh Settings..... | 154 |
| 5.9.1 Configuring Mesh Wi-Fi | 155 |
| 5.9.2 Adding Mesh Devices | 156 |
| 5.10 Configuring the LAN Port of Downlink Access Point..... | 158 |
| 5.11 Configure IEEE 802.1X authentication..... | 159 |
| 5.11.1 Overview | 159 |
| 5.11.2 Configuring 802.1X Globally | 160 |
| 5.11.3 Configuring the RADIUS Server | 163 |
| 5.11.4 Checking Authentication User List..... | 165 |
| 5.12 Configuring Domain Proxy..... | 166 |
| 5.13 Client Association | 167 |
| 5.13.1 Configuring Intelligent Association..... | 167 |
| 5.13.2 Configuring Client Association..... | 167 |
| 6 Switch Management..... | 169 |
| 6.1 Configuring RLDP | 169 |
| 6.1.1 Overview | 169 |
| 6.1.2 Configuration Steps | 169 |
| 6.2 Configuring DHCP Snooping..... | 170 |
| 6.2.1 Overview | 170 |
| 6.2.2 Configuration Steps | 171 |
| 6.3 Batch Configuring Switches..... | 172 |

| | |
|--|-----|
| 6.3.1 Overview | 172 |
| 6.3.2 Configuration Steps | 172 |
| 6.3.3 Verifying Configuration..... | 174 |
| 7 Authentication Management | 175 |
| 7.1 Web Authentication..... | 175 |
| 7.1.1 Overview | 175 |
| 7.1.2 Getting Started..... | 175 |
| 7.1.3 WiFiDog Authentication | 175 |
| 7.1.4 Configuring Third-Party Authentication..... | 177 |
| 7.1.5 Local Account Authentication..... | 183 |
| 7.1.6 Authorized Guest Authentication | 189 |
| 7.1.7 Guest Authentication through QR Code Scanning..... | 191 |
| 7.1.8 Authentication-Free..... | 193 |
| 7.1.9 Custom Portal Page..... | 196 |
| 7.1.10 Global Configuration | 197 |
| 7.2 Configuring the PPPoE Server | 198 |
| 7.2.1 Overview | 198 |
| 7.2.2 Global Settings..... | 198 |
| 7.2.3 Configuring the PPPoE User Groups | 199 |
| 7.2.4 Configuring a PPPoE User Account | 200 |
| 7.2.5 Configuring Exceptional IP Addresses | 202 |
| 7.3 Online User Management..... | 203 |
| 8 Online Behavior Management | 204 |
| 8.1 Overview | 204 |

| | |
|---|-----|
| 8.2 User Management | 204 |
| 8.2.1 Overview | 204 |
| 8.2.2 User Group | 204 |
| 8.2.3 Authentication Group | 207 |
| 8.3 Time Management..... | 209 |
| 8.3.1 Configuring a Schedule by Week | 209 |
| 8.3.2 Configuring a Schedule by Date..... | 210 |
| 8.4 App Control..... | 211 |
| 8.4.1 Overview | 211 |
| 8.4.2 Configuring App Control..... | 211 |
| 8.4.3 Custom App | 213 |
| 8.4.4 Custom Application Group | 215 |
| 8.5 Website Management..... | 216 |
| 8.5.1 Overview | 216 |
| 8.5.2 Configuration Steps | 217 |
| 8.6 QoS..... | 220 |
| 8.6.1 Overview | 220 |
| 8.6.2 Intelligence QoS..... | 220 |
| 8.6.3 Custom Policies | 221 |
| 8.6.4 Application Priority | 230 |
| 8.7 Access Control..... | 232 |
| 8.7.1 Overview | 232 |
| 8.7.2 Configuration Steps | 232 |
| 8.8 Upgrading the Application Library | 238 |

| | |
|---|-----|
| 8.8.1 Overview | 238 |
| 8.8.2 Local Upgrade..... | 238 |
| 8.8.3 Online Upgrade..... | 239 |
| 8.9 Network Behavior Settings | 239 |
| 8.9.1 Internet Alert..... | 239 |
| 8.9.2 Online Time Control | 240 |
| 8.9.3 Internet Block Policy | 241 |
| 9 Online Client Management | 242 |
| 9.1 Overview | 242 |
| 9.2 Configuring Client IP Binding..... | 244 |
| 9.3 Configuring Client Access Control..... | 245 |
| 9.4 Configuring Client Association..... | 245 |
| 9.5 Blocking Clients | 246 |
| 9.6 Configuring Client Rate Limiting | 247 |
| 10 VPN | 249 |
| 10.1 Configuring IPsec VPN | 249 |
| 10.1.1 Overview | 249 |
| 10.1.2 Configuring the IPsec Server..... | 250 |
| 10.1.3 Configuring the IPsec Client | 256 |
| 10.1.4 Viewing the IPsec Connection Status..... | 258 |
| 10.1.5 Typical Configuration Example | 259 |
| 10.1.6 Solution to IPsec VPN Connection Failure | 263 |
| 10.2 Configuring L2TP VPN | 264 |
| 10.2.1 Overview | 264 |

| | | |
|--------|---|-----|
| 10.2.2 | Configuring the L2TP Server | 264 |
| 10.2.3 | Configuring the L2TP Client..... | 271 |
| 10.2.4 | Viewing the L2TP Tunnel Information..... | 273 |
| 10.2.5 | Typical Configuration Example | 274 |
| 10.2.6 | Solution to L2TP VPN Connection Failure | 284 |
| 10.3 | Configuring PPTP VPN | 285 |
| 10.3.1 | Overview | 285 |
| 10.3.2 | Configuring the PPTP Service | 285 |
| 10.3.3 | Configuring the PPTP Client..... | 288 |
| 10.3.4 | Viewing the PPTP Tunnel Information..... | 290 |
| 10.3.5 | Typical Configuration Example | 291 |
| 10.3.6 | Solution to PPTP VPN Connection Failure | 300 |
| 10.4 | OpenVPN..... | 301 |
| 10.4.1 | Overview | 301 |
| 10.4.2 | Configuring the OpenVPN Server | 301 |
| 10.4.3 | Configuring the OpenVPN Client..... | 306 |
| 10.4.4 | Viewing the OpenVPN Tunnel Information..... | 311 |
| 10.4.5 | Typical Configuration Example | 311 |
| 10.5 | Configuring WireGuard VPN | 319 |
| 10.5.1 | Overview | 319 |
| 10.5.2 | Configuring a WireGuard VPN Server..... | 319 |
| 10.5.3 | Configuring a WireGuard VPN Client | 324 |
| 10.5.4 | Checking the Status of a WireGuard VPN Connection | 327 |
| 11 | SD-WAN | 329 |

| | |
|--|-----|
| 12 System Management | 330 |
| 12.1 System Logs | 330 |
| 12.1.1 Viewing System Logs..... | 330 |
| 12.1.2 Configuring System Logs..... | 332 |
| 12.2 Setting the Login Password..... | 337 |
| 12.3 Setting the Session Timeout Duration..... | 337 |
| 12.4 Restoring Factory Settings | 338 |
| 12.4.1 Restoring the Current Device to Factory Settings..... | 338 |
| 12.4.2 Restoring All Devices to Factory Settings | 338 |
| 12.5 Configuring SNMP | 339 |
| 12.5.1 Overview | 339 |
| 12.5.2 Global Configuration | 339 |
| 12.5.3 View/Group/Community/User Access Control..... | 341 |
| 12.5.4 SNMP Service Typical Configuration Examples..... | 349 |
| 12.5.5 Configuring Trap Service | 354 |
| 12.5.6 Trap Service Typical Configuration Examples..... | 358 |
| 12.6 Configuring Reboot..... | 361 |
| 12.6.1 Rebooting the Current Device | 361 |
| 12.6.2 Rebooting All Devices in the Network | 361 |
| 12.6.3 Rebooting the Specified Device | 362 |
| 12.7 Configuring Scheduled Reboot..... | 362 |
| 12.8 Setting and Displaying System Time..... | 363 |
| 12.9 Configuring Backup and Import..... | 364 |
| 12.10 Configuring LEDs..... | 364 |

| | |
|--|-----|
| 12.11 Configuring Diagnostics..... | 366 |
| 12.11.1 Network Check..... | 366 |
| 12.11.2 Alerts | 367 |
| 12.11.3 Network Tools..... | 367 |
| 12.11.4 Packet Capture | 370 |
| 12.11.5 Fault Collection | 371 |
| 12.11.6 Viewing Flow Statistics..... | 371 |
| 12.12 Performing Upgrade and Checking System Version | 372 |
| 12.12.1 Online Upgrade..... | 372 |
| 12.12.2 Local Upgrade..... | 372 |
| 12.13 Switching System Language | 373 |
| 12.14 Configuring Cloud Service..... | 373 |
| 12.14.1 Overview | 373 |
| 12.14.2 Configuration Steps | 373 |
| 12.14.3 Unbinding Cloud Service | 375 |
| 13 FAQ | 376 |
| 13.1 What Can I Do If I Fail to Log In to the Web Page? | 376 |
| 13.2 How Do I Restore Factory Settings? | 376 |
| 13.3 What Can I Do If I Forget the Device Login Password? | 376 |
| 13.4 What Can I Do If Internet Access Through PPPoE Dial-Up Fails? | 376 |

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 2.340

1.1.1 Hardware Change

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

| Model | Hardware Version |
|---------------|------------------|
| RG-EG105GW(T) | 1.xx |
| RG-EG105GW-X | 1.xx |

1.1.2 Software Feature Change

Compared to ReyeeOS 2.320, the software feature changes in this version are as follows:

1. New Feature: WireGuard VPN

This version supports the configuration of WireGuard VPN. For details, see Section [10.5 Configuring WireGuard VPN](#).

2. Changed Feature: Authentication

- Before the change:
 - Authentication settings are under the **Advance** menu.
 - The account expiration reminder is not supported.
- After the change:
 - The web-based authentication, PPPoE authentication, and their related functions are included in the independent **Authentication** menu.
 - The account expiration reminder is supported. For details, see Section [7 Authentication Management](#).

3. Changed feature: QoS

- Before the change:
 - On versions earlier than ReyeeOS 2.340, this feature is called flow control.
 - When the **Type** of a QoS policy is set to **Custom**, and the **Bandwidth Type** is set to **Independent**, you can only configure the bandwidth limit for designated interfaces.

Add
×

* Policy Name

Type User Group Custom

* User Group

Application All Applications App Group Custom

Bandwidth Type Shared Independent

Bandwidth Limit Limit No Limit

Uplink Bandwidth Mbps Mbps

Downlink Bandwidth Mbps Mbps

Max-Limit per User
 Uplink Mbps
 Downlink Mbps

* Interface

Enabled

----- [Advanced Settings](#) -----

- After the change:
 - On ReyeOS 2.340 and later versions, this feature is renamed as quality of service (QoS).
 - When the **Type** of a traffic control policy is set to **Custom**, and the **Bandwidth Type** is set to **Independent**, you can apply the policy at device level, limiting the maximum bandwidth for all users. For details, see Section [8.6.3 Custom Policies](#).

Add ×

* Policy Name

Type User Group Custom

* User Group

Application All Applications App Group Custom

Bandwidth Type Shared Independent

Bandwidth Limit Limit No Limit

Uplink Bandwidth Mbps Mbps

Downlink Bandwidth Mbps Mbps

Max-Limit per User Uplink Mbps Downlink Mbps

Apply To Designated interfaces ALL-WAN

* Interface

Enabled

----- Advanced Settings -----

4. Changed Feature — DHCP Option

- Before the change: **Domain Name** cannot be configured in **DHCP Option**.

DNS Server

Option 43 i

Option 138

Option 150

Gateway

- After the change: **Domain Name** can be configured in **DHCP Option**. For details, see Section [4.10.3 2. Configuring DHCP Option](#).

DNS Server ?

Option 43 ? i

Option 138 ?

Option 150 ?

Gateway

Domain Name

1.2 ReyeeOS 2.320

1.2.1 Hardware Change

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

| Model | Hardware Version |
|---------------|------------------|
| RG-EG105GW(T) | 1.xx |
| RG-EG105GW-X | 1.xx |

1.2.2 Software Feature Change

Compared to ReyeeOS 2.300, the software feature changes in this version are as follows:

1. Changed Feature — Software Security Reinforcement

This version fixes known security vulnerabilities, with no changes to functionality.

2. New Feature — System Log

This version supports the System Log function. For details, see Section [12.1 System Logs](#).

3. Changed Feature — AP Mesh

- Before the change: Configuring Mesh Wi-Fi is not supported.

After Reyee Mesh is enabled, the devices that support Reyee Mesh can be paired through wireless or wired connection to set up a Mesh network. Auto link optimization is supported in the Mesh network.

i Mesh link optimization algorithm: The algorithm not only covers signal strength, wireless mode, antenna streams and bandwidth parameters, but also considers the attenuation of Mesh hops. The Mesh system will select the optimal uplink automatically for the AP based on the link optimization algorithm.

Enable

- After the change: Configuring Mesh Wi-Fi and device scanning are supported. For details, see Section [5.9](#)

[Reyee Mesh Settings.](#)

AP Mesh



When AP Mesh is enabled, Devices that support the AP Mesh function can form a network either wirelessly or through a wired connection. The system will automatically optimize mesh links by considering factors such as signal strength, wireless mode, number of antenna streams, channel width, and signal loss across mesh hops to choose the optimal uplink.

Mesh Networking

Old Device Compatibility



Mesh Devices List

[Configure Mesh Wi-Fi](#)

[Scan to Add Devices](#)

| Username | Model | SN | IP/MAC | Uplink | Status | Connectivity Quality |
|----------|---------|--------------|--------------------------------|--------|---------|----------------------|
| AP | EG205GW | f[redacted]3 | 192.168.110.91 e[redacted]3 | - | Offline | - |

Total 1 **1** 10/page

2 Login

2.1 Configuration Environment Requirements

2.1.1 PC

- Browser: 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 or format error may occur if an unsupported browser is used.
- Resolution: 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 Default Configuration

Table 2-1 Default Web Configuration

| Item | Default |
|------------|----------------------------------|
| IP address | 192.168.110.1 |
| Password | The default password is "admin". |

2.3 Login to the Web Interface

2.3.1 Connecting to the Router

You can open the management page and complete Internet access configuration only after connecting a client to the router in either of the following ways:

- Wired Connection

Connect a local area network (LAN) port of the router to the network port of the PC, and set the IP address of the PC. See Section [2.3.2 Configuring the IP Address of the Management Client](#) for details.

- Wireless Connection

On a mobile phone or laptop, search for wireless network @Ruijie-mXXXX (XXXX is the last four digits of the MAC address of each device). In this mode, you do not need to set the IP address of the management client, and you can skip the operation in Section [2.3.2 Configuring the IP Address of the Management Client](#).

2.3.2 Configuring the IP Address of the Management Client

Configure an IP address for the management client in the same network segment as the default IP address of the device (The default device IP address is 192.168.110.1, and the subnet mask is 255.255.255.0.) so that the management client can access the device. For example, set the IP address of the management client to 192.168.110.200.

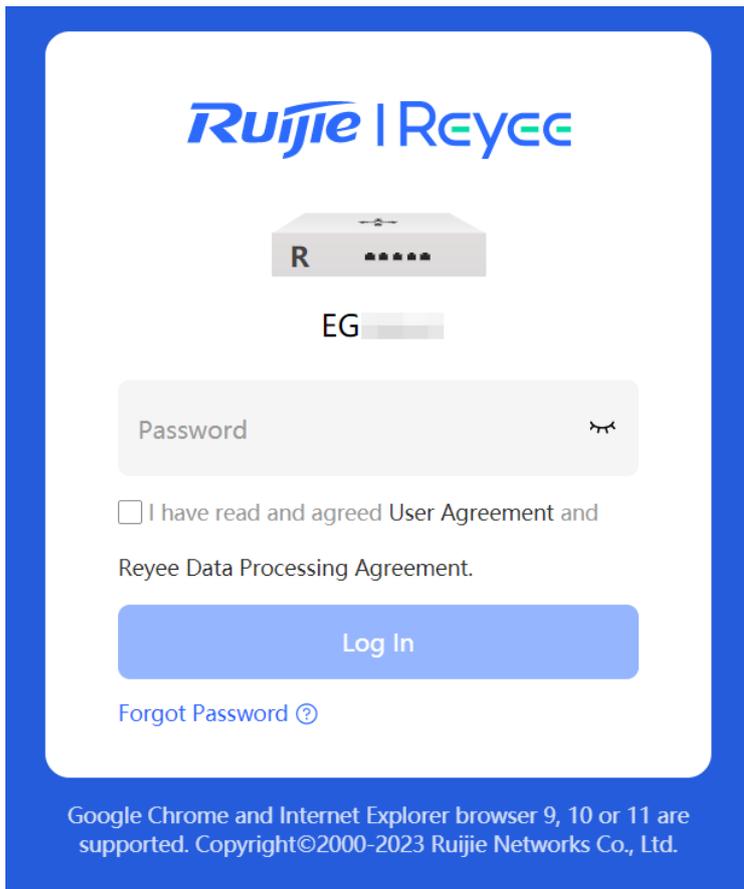
2.3.3 Login

- (1) Enter the IP address (192.168.110.1 by default) of the router in the address bar of the browser to open the login page.

Note

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

- (2) On the web page, enter the password and click **Log In** to enter the web management system.



You can use the default password **admin** to log in to the device for the first time.

For security purposes, you are advised to change the default password as soon as possible after logging in, and to regularly update your password thereafter.

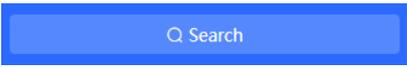
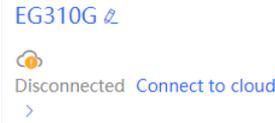
If you forget the IP address or password, hold down the **Reset** button on the device panel for more than 5 seconds when the device is connected to the power supply to restore factory settings. After restoration, you can use the default IP address and password to log in.

Caution

Restoring factory settings will delete the existing configuration and you are required to configure the device again at your next login. Therefore, exercise caution when performing this operation.

2.3.4 Frequently-Used Controls on the Web Page

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

| Control | Description |
|---|---|
|  | <p>Monitor: Click it to view the topology of the self-organizing network and monitor device traffic trend, client traffic usage, device port status, and so on.</p> <p>Config: Click it to configure all functions available on the local device.</p> |
|  | <p>Click it to search or select features for quick configuration.</p> |
|  | <p>The navigation bar is arranged horizontally on the top when the device acts as the slave device, and vertically on the left when the device acts as the master device.</p> |
|  | <p>Click it to access the alert list.</p> |
|  | <p>Click it to change the language.</p> |
|  | <p>Click it to log out of the web management system.</p> |
|  | <p>Click it to connect the device to the cloud by scanning the QR code for remote management.</p> |
|  | <p>Click Add or Batch Add to add one or more table entries in the dialog box that appears. After adding the table entries, you can view the added table entries on this page.</p> |
|  | <p>Click it to delete the selected table entries in batches.</p> |
|  | <p>Quickly locate the table entry you want to find through the drop-down list or by entering a keyword.</p> |
|  | <p>Click them to edit, delete, or bind a table entry.</p> |
|  | <p>If the toggle switch is displayed in gray and the button is on the left, the related function is disabled. If the toggle switch is displayed in blue and the button is on the right, the related function is enabled.</p> |
|  | <p>Update data on the current page.</p> |

| Control | Description |
|---|---|
|  | Set the number of table entries displayed on a page. Click a page number or specify the page number to access the corresponding page. |

2.4 Work Mode

The device can work in router mode, AP mode, or wireless repeater mode. The system menu pages and configuration function scope vary depending on the work mode. By default, the RG-EG-W router works in router mode. To modify the work mode, see [4.1 Switching the Work Mode](#).

2.4.1 Router Mode

The device supports routing functions such as route-based forwarding and network address translation (NAT), VPN, and behavior management. It can allocate addresses to downlink devices, forward network data based on routes, and perform NAT operations.

In the router mode, the device can access the network through Point-to-Point Protocol over Ethernet (PPPoE) dialing, dynamic IP address, and static IP address. It can also directly connect to a fiber-to-the-home (FTTH) network cable or an uplink device to provide network access and manage downlink devices.

2.4.2 AP Mode

After the AP mode is enabled, the device serves as a fit AP and supports Layer 2 forwarding only. In AP mode, the device does not provide the routing and Dynamic Host Configuration Protocol (DHCP) server functions. By default, the device obtains IP addresses through DHCP and uniformly allocates and manages IP addresses to downlink devices connected to it through the DHCP address pool. In this mode, the AP only transmits data transparently.

Generally, the RG-EG-W router cooperates with devices providing the routing function. On a normally working network, the RG-EG-W router connects to an uplink router through a network cable to convert wired signals into wireless signals, extending the wireless network coverage range.

2.4.3 Wireless Repeater

Similar to the AP mode, the device does not provide the routing and DHCP server functions in wireless repeater mode. The addresses of end users are allocated and managed by the primary router. This mode is applicable to a normally working network, where the device connects to the primary router in wireless mode to expand the Wi-Fi coverage range and increase the number of network cable ports and wireless access devices.

2.4.4 WISP

This device provides wireless Internet access through a Wireless Internet Service Provider (WISP). The supported Internet connection types include PPPoE, DHCP, and static IP.

This device supports routing functions such as NAT forwarding, VPN, and behavior management. It can assign IP addresses to downlink devices, route traffic between networks, and supports NAT.

2.5 Configuration Wizard (Router Mode)

2.5.1 Getting Started

- (1) Power on the device. Connect the WAN port of the device to an uplink device using an Ethernet cable, or connect the device to the optical modem directly.
- (2) Configure the Internet connection type according to requirements of the local Internet Service Provider (ISP). Otherwise, the Internet access may fail due to improper configuration. You are advised to contact your local ISP to confirm the Internet connection type:
 - o Figure out whether the Internet connection type is PPPoE, DHCP mode, or static IP address mode.
 - o In the PPPoE mode, a username, a password, and possibly a service name are needed.
 - o In the static IP address mode, an IP address, a subnet mask, a gateway, and a DNS server need to be configured.

2.5.2 Configuration Steps

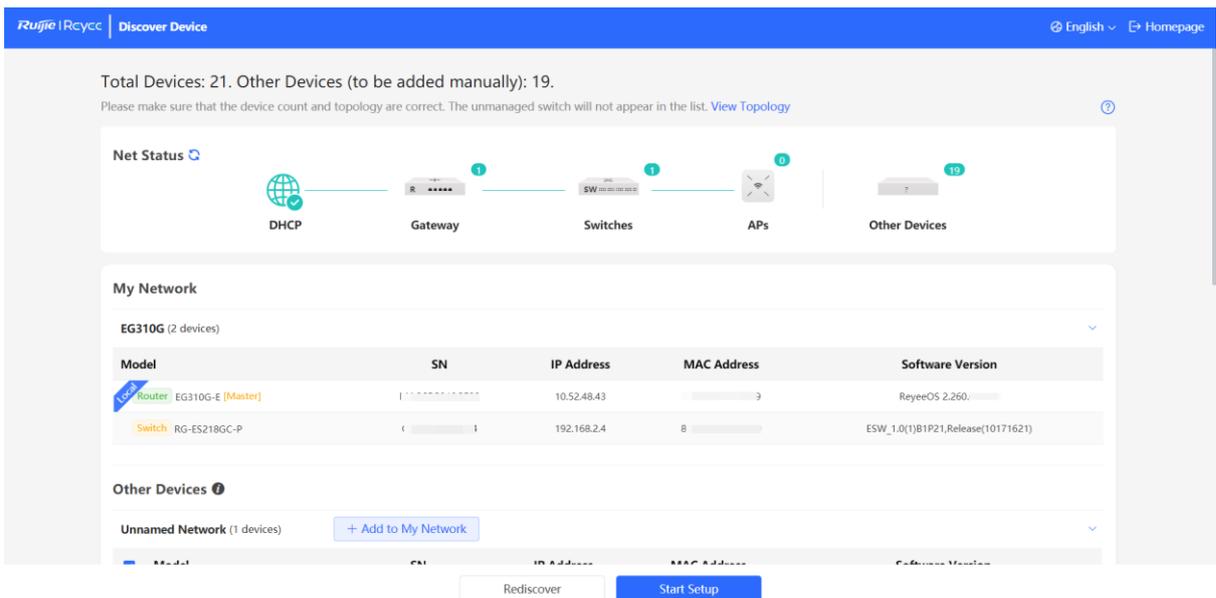
1. Adding a Device to Network

You can manage and configure all devices in the network in batches by default. Please verify the device count and network status before configuration.

Note

New devices will join in a network automatically after being powered on. You only need to verify the device count.

If a new device is detected not in the network, click **Add to My Network** and enter its management password to add the device manually.



Total Devices: 21. Other Devices (to be added manually): 19.
Please make sure that the device count and topology are correct. The unmanaged switch will not appear in the list. [View Topology](#)

Net Status

DHCP Gateway Switches APs Other Devices

My Network

EG310G (2 devices)

| Model | SN | IP Address | MAC Address | Software Version |
|--|------------------|-------------|-------------------|-----------------------------------|
|  Router EG310G-E [Master] | 1111111111111111 | 10.52.48.43 | 11:11:11:11:11:11 | ReyeeOS 2.260. |
|  Switch RG-ES218GC-P | 1111111111111111 | 192.168.2.4 | 88:88:88:88:88:88 | ESW_1.0(1)B1P21,Release(10171621) |

Other Devices

Unnamed Network (1 devices) [+ Add to My Network](#)

Rediscover Start Setup

2. Creating a Network Project

Click **Start Setup** to configure the Internet connection type, Wi-Fi network and management password.

- (1) **Internet:** Configure the Internet connection type according to requirements of the local ISP.
 - o **DHCP:** The router detects whether it can obtain an IP address via DHCP by default. If the router connects to the Internet successfully, you can click **Next** without entering an account.
 - o **PPPoE:** Click **PPPoE**, and enter the username, password, and service name. Click **Next**.
 - o **Static IP:** Enter the IP address, subnet mask, gateway, and DNS server, and click **Next**.
- (2) **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.
- (3) **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.
- (4) **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.
- (5) **Network Name:** Identify the network where the device is located.
- (6) **Management Password:** The password is used for logging in to the management page.

The first screenshot shows the 'Network Settings' step (1) of the configuration process. It features a progress bar at the top with three steps: 'Network Settings' (1), 'Project Settings' (2), and 'Project Binding' (3). Below the progress bar, there are radio buttons for 'Internet' connection types: 'PPPoE', 'DHCP' (selected), and 'Static IP'. Below this, it says 'Current Settings: DHCP'. A dashed line separates this from the 'Country/Region/Time Zone' section. There are two dropdown menus: '* Country/Region' set to 'United States (US)' and '* Time Zone' set to '(GMT-5:00)America/New_York'.

The second screenshot shows the 'Project Settings' step (2). The progress bar at the top now has 'Network Settings' (1) in blue, 'Project Settings' (2) in bold, and 'Project Binding' (3). Below the progress bar, there is a text input field for '* Project Name' containing 'EG310G'. Below that, there are radio buttons for 'Password': 'Use Old Management Password' (selected) and 'Edit'.

Click **Create Network & Connect**. The device will deliver the initialization and check the network connectivity.

The device can access the Internet now. Bind the device with a Ruijie Cloud account for remote management.

Follow the instruction to log in to Ruijie Cloud for further configuration.



Network

- Name: ruijie
- SSID: ruijie

Management

- Password: Ruijie123

Redirecting...

Note

If your device is not connected to the Internet, click **Exit** to exit the configuration wizard.

Please log in again with the new password if you change the management password.

2.5.3 Forgetting the PPPoE Account

- (1) Consult your local ISP.
- (2) If you replace the old router with a new one, click **Obtain Account from Old Device**. Connect the old and new routers to a power supply and start them. Insert one end of an Ethernet cable into the WAN port of the old router and connect the other end to a LAN port of the new router, and click **Obtain**. The new router automatically fetches the PPPoE account of the old router. Click **Save** to make the configuration take effect.

Obtain PPPoE Account from Old Router ×

Internet PPPoE DHCP Static IP

☼ Checking IP assignment

* Username

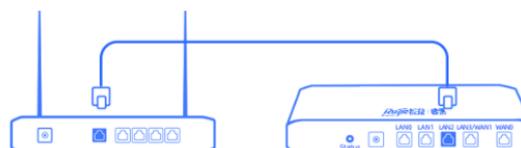
* Password

Service Name

🔍 Forgot Account? Obtain Account from Old Device

* SSID

Wi-Fi Password Security Open



Steps:

1. Transmit Power on the old router and new router.
2. Connect one end of a cable to the WAN port of the old router and connect the other end to the LAN port of the new router.
3. Click "Obtain".

Obtain

2.6 Configuration Wizard (AP Mode)

2.6.1 Getting Started

- Power on the device and connect the device to an uplink device.
- Make sure that the device can access the Internet.

2.6.2 Configuration Steps

- (1) On the work mode setting page, change the work mode from router mode to AP mode. For details, see Section [4.1 Switching the Work Mode](#).

Working Mode ×

Description:

1. The device IP address may change upon mode change.
2. Change the endpoint IP address and ping the device.
3. Enter the new IP address into the address bar of the browser to access Eweb.
4. The system menu varies with different work modes.

Working Mode ? AP ▼

Self-Organizing Network ?

Cancel

Save

- (2) After mode switching, the device will restart. After restart, the WAN port on the device obtains an IP address through DHCP and accesses the network by using a dynamic IP address. Set the SSID, Wi-Fi password, and management password. The default Internet connection type is DHCP mode. You can use the default value or manually configure a static IP address for the WAN port. For details, see Section [2.5.2 Configuration Steps](#).

2.7 Configuration Wizard (Wireless Repeater)

2.7.1 Getting Started

⚠ Caution

The device does not need to connect to a network cable when working in wireless repeater mode. However, wireless stability is affected by many factors. You are advised to select a wired mode (AP mode).

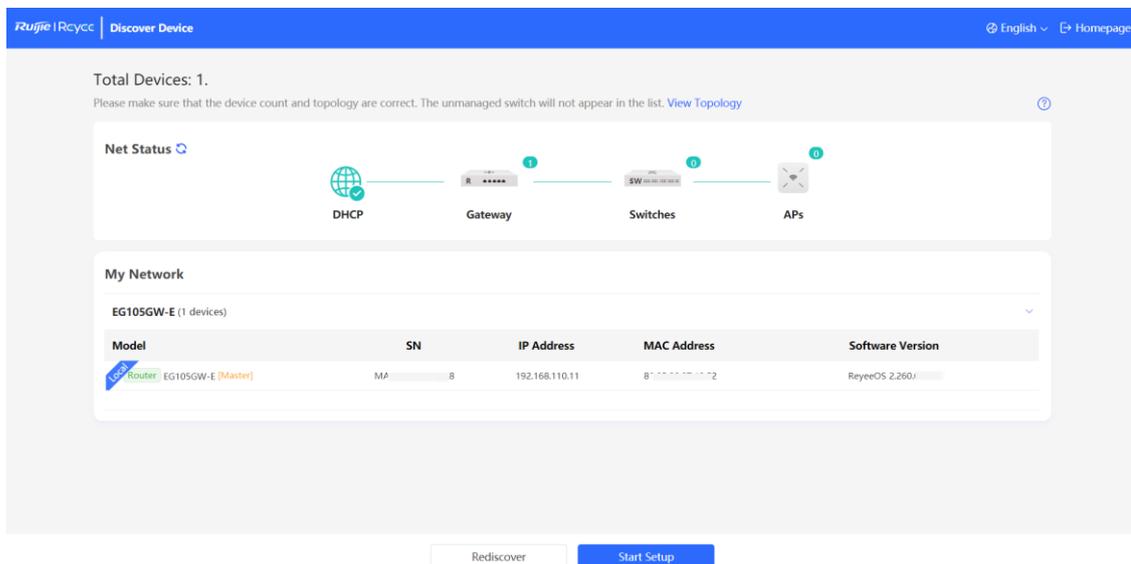
- Before setting the wireless repeater mode, configure the primary router and test that the primary router can

normally access the Internet.

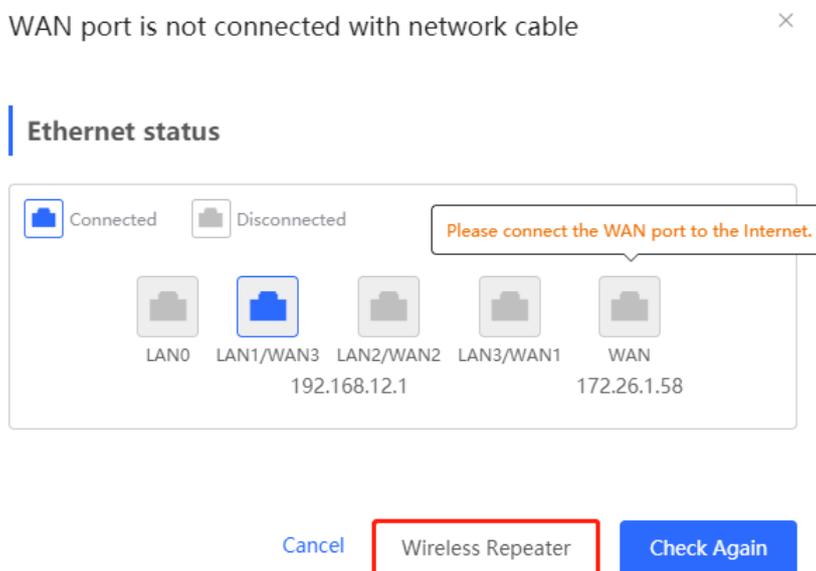
- Place the device in a location where Wi-Fi signal of the primary router can be searched and the signal has two or more cells.

2.7.2 Configuration Steps

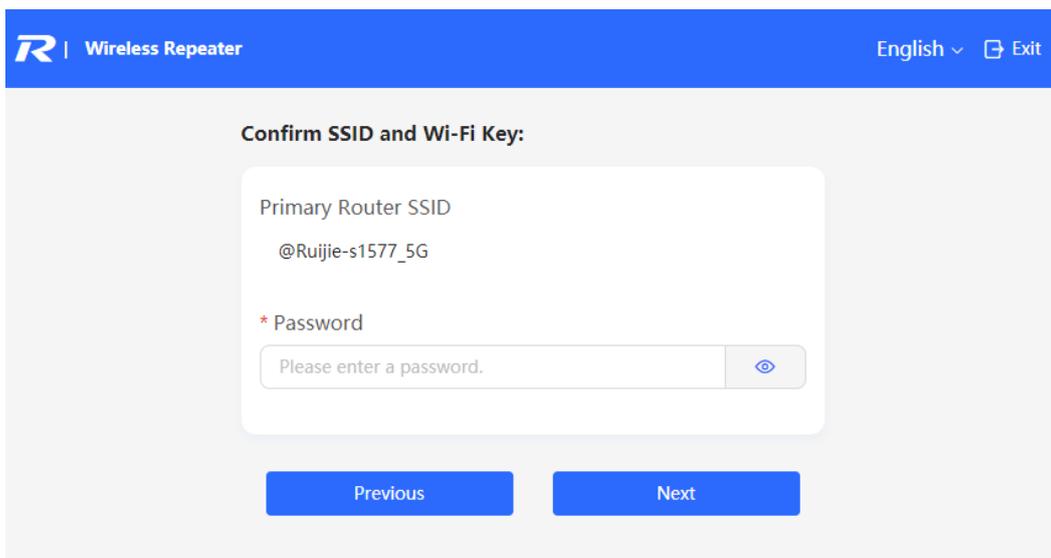
- (1) Connect the device to a power supply but not a network cable. Then, click **Start Setup**.



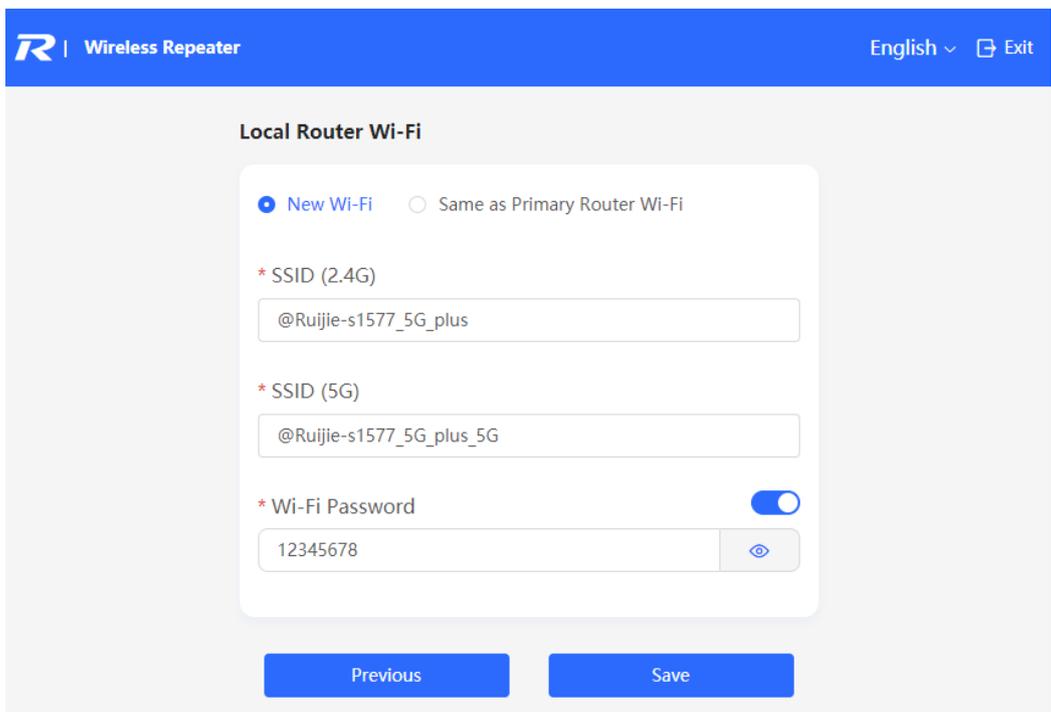
- (2) On the page showing the WAN port is not connected with network cable message, click **Wireless Repeater**.



- (3) Select the primary router whose Wi-Fi signal needs to be extended, enter the Wi-Fi password of the primary router, and click **Next**.



(4) Set the SSID and password and click **Save**. Wi-Fi will restart.



2.8 Configuration Wizard (WISP)

2.8.1 Getting Started

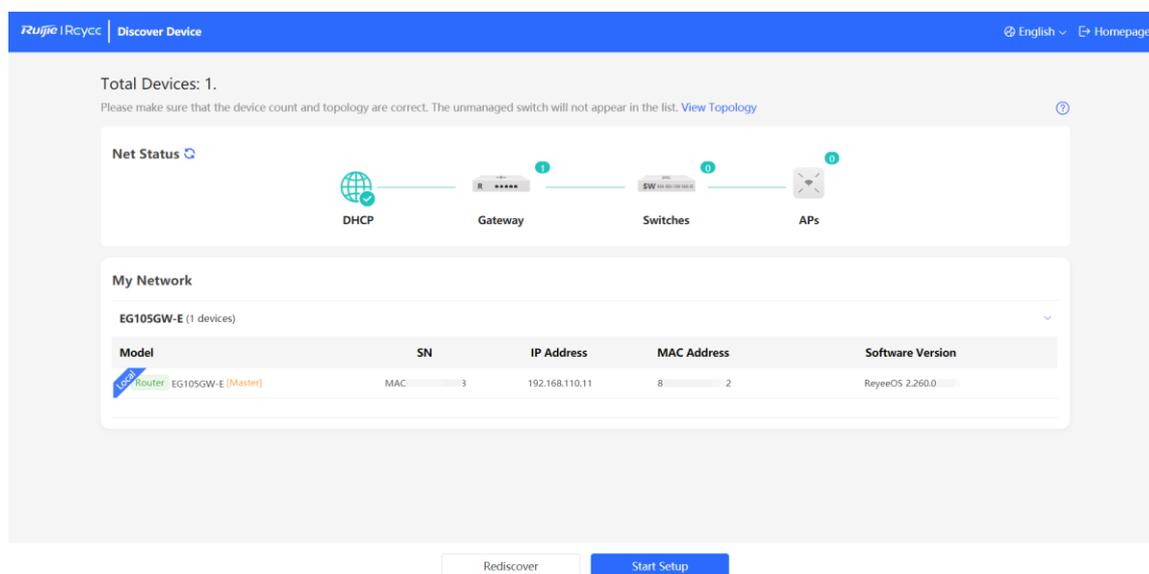
- Configure the Internet connection type: DHCP, PPPoE, or static IP.
- Obtain the necessary wireless access information for the WISP network, including the network name (SSID) and security settings, such as encryption mode (for example, WPA2-PSK) and password.

Note

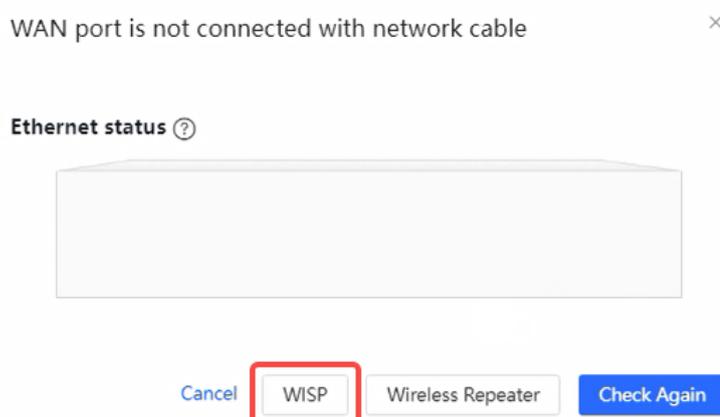
WISP enables users to access the Internet wirelessly, eliminating the need for Ethernet cable connections on their devices.

2.8.2 Configuration Steps

- (1) Connect the router to a power source. Once the router is powered on, open a web browser and log in to the web interface. On the page that is displayed, click **Start Setup**.



- (2) On the pop-up window displaying "WAN port is not connected with network cable", click **WISP**.



- (3) Select the Wi-Fi network provided by WISP, enter the Wi-Fi password, choose the connection type (PPPoE, DHCP, or static IP), and click **Next**.

Search SSID

- 5G @YDGL-IOTIOT-1
- 5G @YDGL-IOTIOT-3
- 5G @YDGL-IOTIOT-5
- 5G @YDGL-IOTIOT-2
- 5G @Ruijie-m68D8
- 5G 213213213**
- 5G @Ruijie-m9DD6
- 5G 222222222222
- 5G r214wq41243
- 5G qweqwrwqe

Please enter the Wi-Fi password

Primary Router SSID
213213213

Password
Open

Please select an Internet

Internet:
DHCP

Dynamically Assigned IP Address

Previous Next

- (4) Set the Wi-Fi name and password for the router, configure the device management password, and click **Next**.

Local Router Wi-Fi

Same as Primary Router Wi-Fi
 New Wi-Fi

* SSID(2.4G)

* SSID(5G)

Wi-Fi Password

Length: 8-31 characters.

Management Password

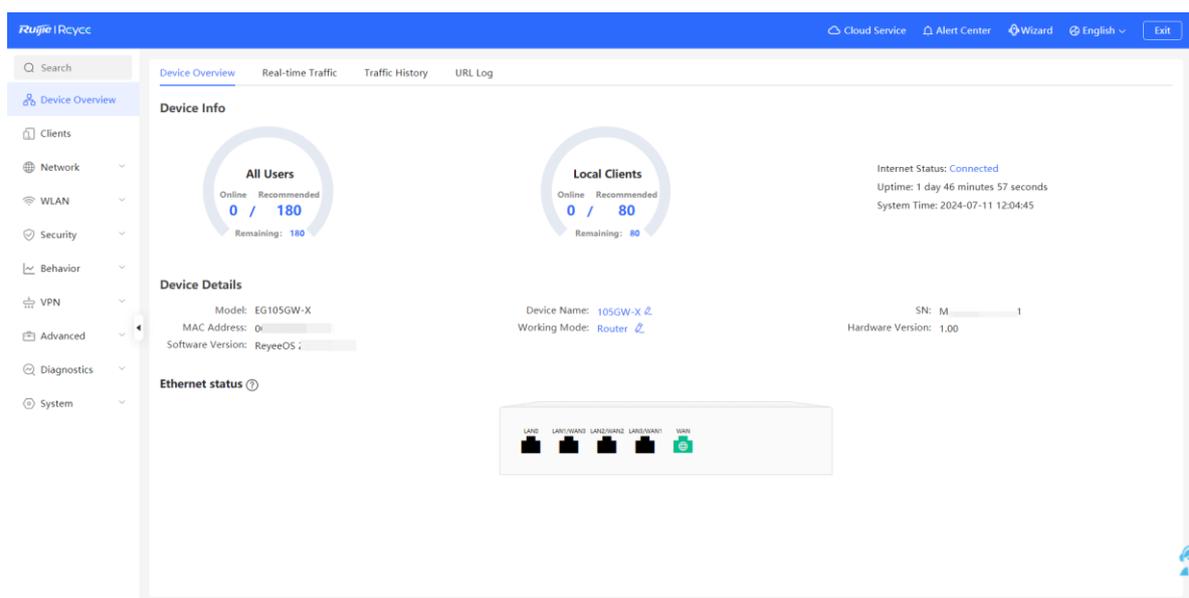
* Management Password

(Please remember the password.)

(5) Select the country/region code and time zone, and click **Save**.

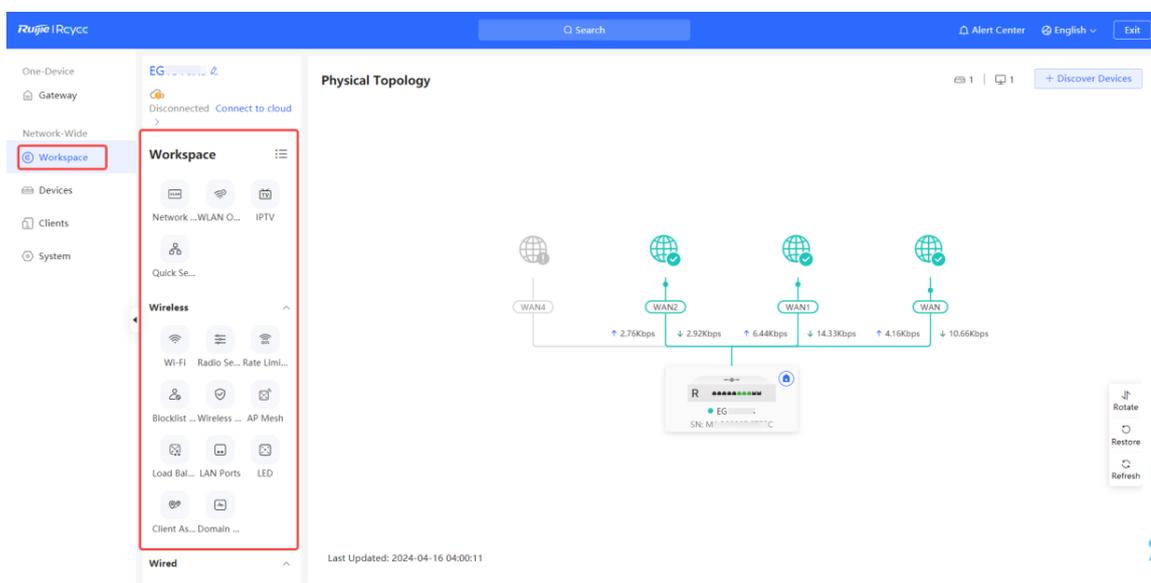
2.9 Switching the Work Mode

When the self-organizing network discovery function is disabled, which is enabled by default, the web interface will switch to the local device mode. For details, see Section [4.1 Switching the Work Mode](#).

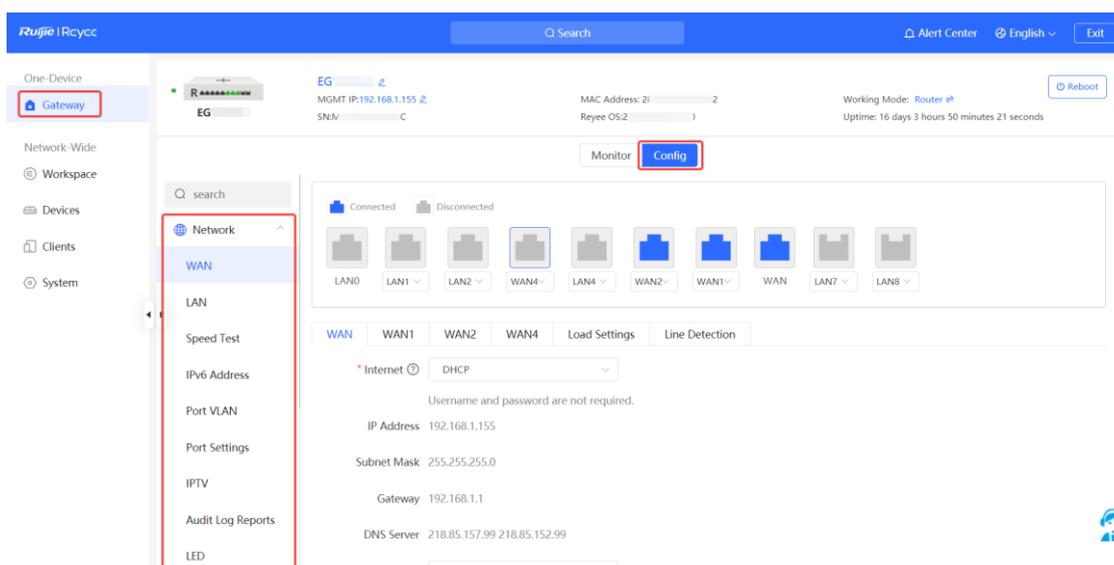


When the self-organizing network discovery function is enabled, you can switch the web interface between network-wide mode and local device mode.

- Network-wide mode: You can view and configure all devices on the network from a network perspective.
Click **Workspace** in the left navigation bar to access the corresponding functions for network-wide configuration in the secondary menu.



- Local device mode: You can configure only one device on the network. The configuration and management of an individual device can be accessed as follows:
 - Method 1: Choose **Gateway > Config** under the **One-Device** menu. On the displayed page, you can access the corresponding functions for single-device configuration in the secondary menu. This method only supports configuring gateway devices on the network.



- Method 2: Choose **Network-Wide > Devices**. In the device list, click the **Manage** button next to the target device. This method supports configuring any type of device on the network.

The screenshot shows the Ruijie iReycc management interface. On the left, a navigation menu includes 'One-Device', 'Gateway', 'Network-Wide', 'Workspace', 'Devices' (highlighted with a red box), 'Clients', and 'System'. The main content area displays a table of devices. At the top, there are filters for 'All (2)', 'Gateway (1)', 'AP (0)', 'Switch (1)', 'AC (0)', and 'Router (0)'. Action buttons for 'Select', 'Reboot', and 'Delete Offline' are visible. The table has the following data:

| Username | Model | SN | IP/MAC | Software Version | Action |
|------------------|-------|----|---------------------|------------------|---------------|
| Gateway [Master] | EC | M | 10.51.216.153 48 | ReyeeOS | Manage Reboot |
| NBS6002 | NR | M | 192.168.110.2 00 | ReyeeOS 2 | Manage Reboot |

At the bottom right of the table, it shows 'Total 2' and a pagination control for page 1 of 10.

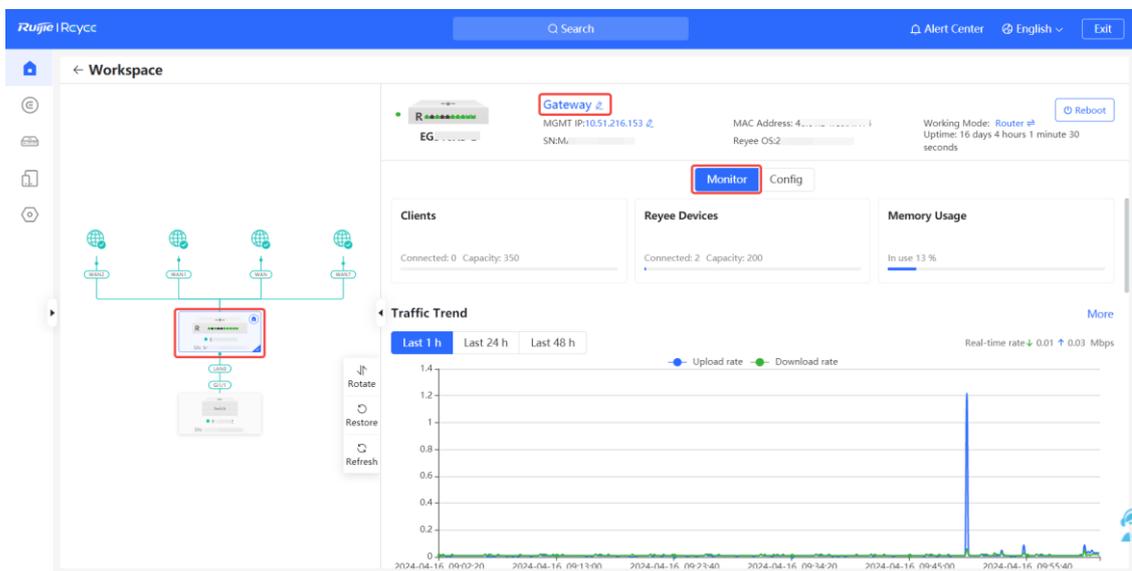
• WAN

Rate : 1000M

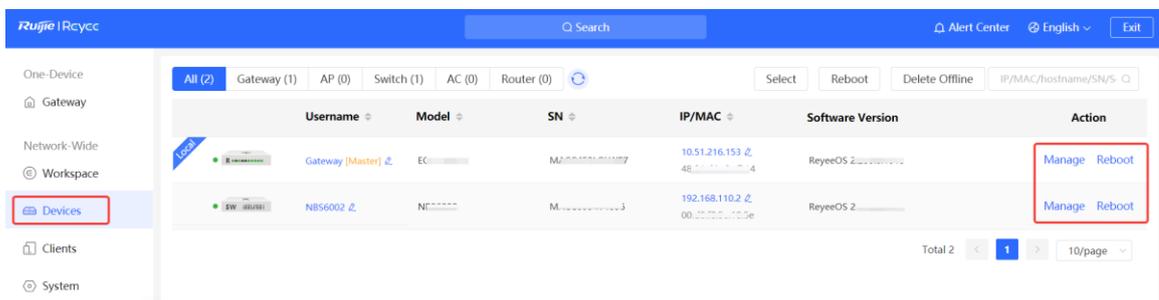
Real-time rate : ↑ 29.14Kbps ↓

140.87Kbps

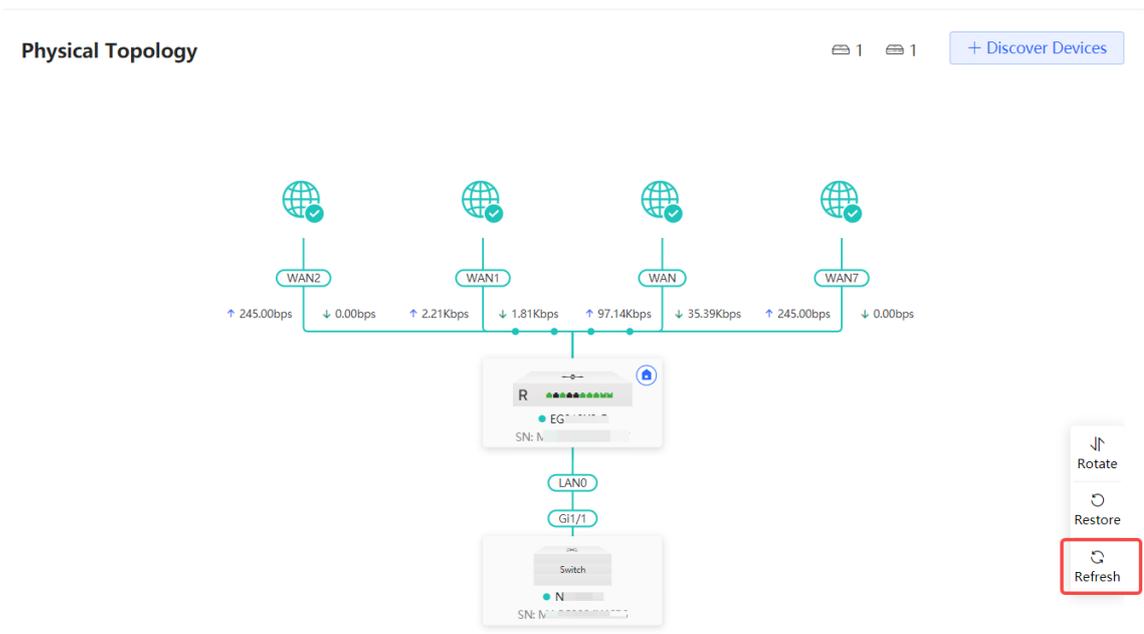
- Click a device in the topology to view the running status and configuration of the device and configure device functions. By default, the product model is used as the device name. Click  to modify the device name so that the description can distinguish devices from one another.



- Choose **Network-Wide > Devices** to view the devices on the current network. Click **Manage** to monitor the device status and perform configuration. Click **Reboot** to reboot the device.



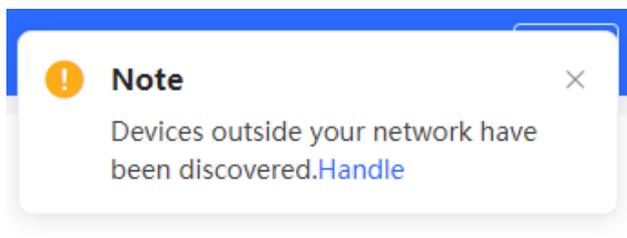
- The update time is displayed in the lower-left corner of the topology view. Click **Refresh** to update the topology to the latest state. It takes some time to update the topology data. Please wait patiently.



3.2 Adding Networking Devices

3.2.1 Wired Connection

- (1) When a new device is connected to the network via a wired connection, the system will display a prompt message indicating the presence of a new device and other unconnected devices. You can click **Handle** to add the new device and other unconnected devices to the network.



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

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

My Network

EG310G (1 devices)

| Model | SN | IP Address | MAC Address | Software Version |
|--------------------------|-------------|-------------|--------------|----------------------|
| Router EG310G-E (Master) | WXXXXXXXXXX | 10.52.48.43 | 0CXXXXXXXXXX | ReyeeOS 2.260.0.2316 |

New Device List

New Device (1 devices) [+ Add to My Network](#)

Other Network

xxxx (2 devices) [+ Add to My Network](#)

| Model | SN | IP Address | MAC Address | Software Version |
|------------------------|---------------|--------------|--------------|----------------------|
| Switch NBS3100-8GT25FP | MXXXXXXXXXX | 10.52.49.145 | 5EXXXXXXXXXX | ReyeeOS 1.230.1604 |
| Switch NBS3200-48GT4XS | 12D1012070100 | 10.52.48.155 | 0XXXXXXXXXX | ReyeeOS 2.248.0.2213 |

123 (1 devices) [+ Add to My Network](#)

R11088_tingxin (1 devices) [+ Add to My Network](#)

yihang (1 devices) [+ Add to My Network](#)

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

×

Add Device to My Network

* Password

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

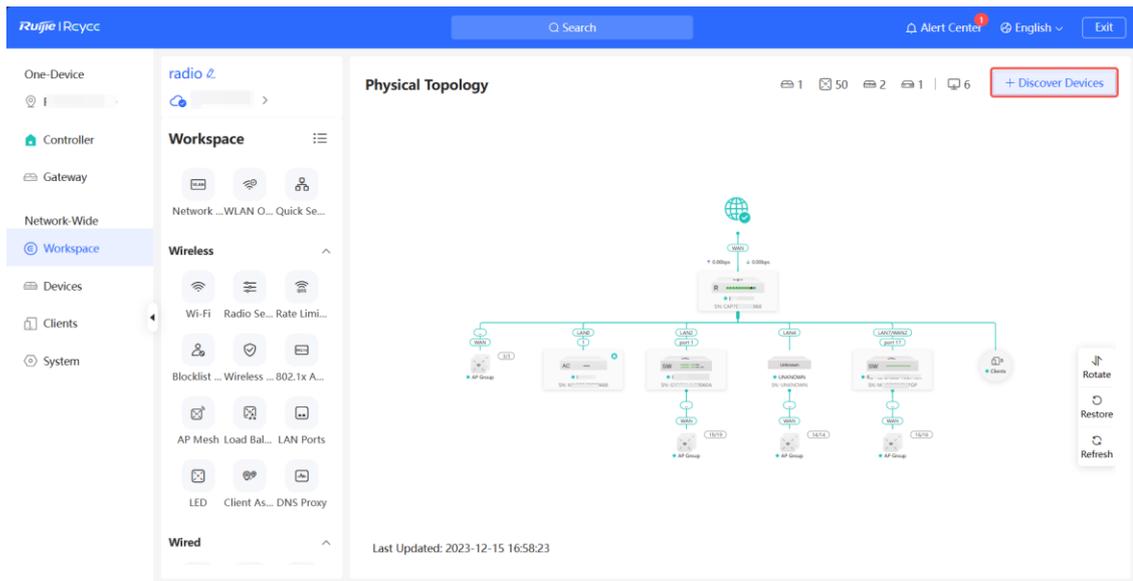
3.2.2 AP Mesh

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

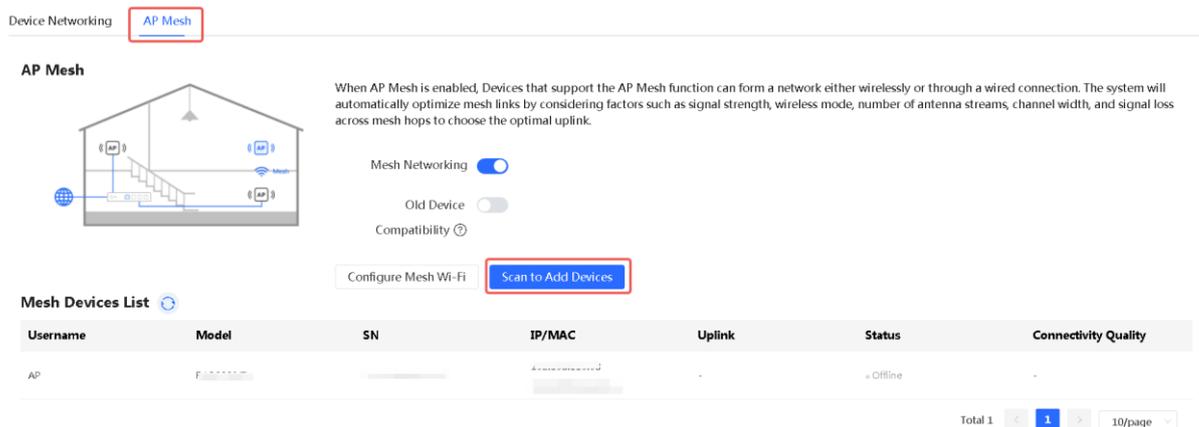
⚠ Caution

- To scan the AP, the Reyee Mesh function must be enabled on the current network. (For details, see Section [5.9 Reyee Mesh Settings](#).) The AP should be powered on nearby. It may fail to be scanned in case of long distance or obstacle blocking.
- You can scan to discover new APs on the AP Mesh page only when there are APs supporting the AP Mesh function on the network.

- (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 **Network-Wide** mode, click **+Discover Devices** in the upper right corner of the **Physical Topology** page to scan the APs in other networks not plugged in with Ethernet cables.



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



- (4) Select the APs to be added and click **Mesh Networking**. Up to eight APs can be selected at a time. Wait until network merging finishes.

← Back



1 old devices are detected. You can enable Old Device Compatibility, or upgrade their firmware to the latest version.



Total Devices: 2.

| <input checked="" type="checkbox"/> Model | MAC |
|--|------------|
| <input checked="" type="checkbox"/> RAP73HD | XXXXXXXXXX |
| <input type="checkbox"/> RAP73HD Old Version | XXXXXXXXXX |

Up to 8 devices can be selected.

Cannot find the desired device. ⓘ

Re-scan Mesh Networking

← Back



Finish

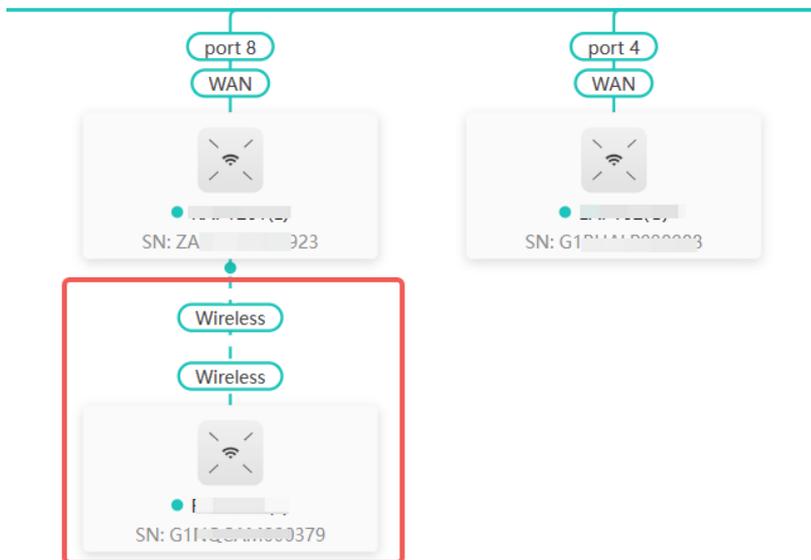
| Model | MAC |
|--|------------|
| <input checked="" type="checkbox"/> RAP73HD | XXXXXXXXXX |
| <input type="checkbox"/> RAP73HD Old Version | XXXXXXXXXX |

Up to 8 devices can be selected.

Cannot find the desired device. ⓘ

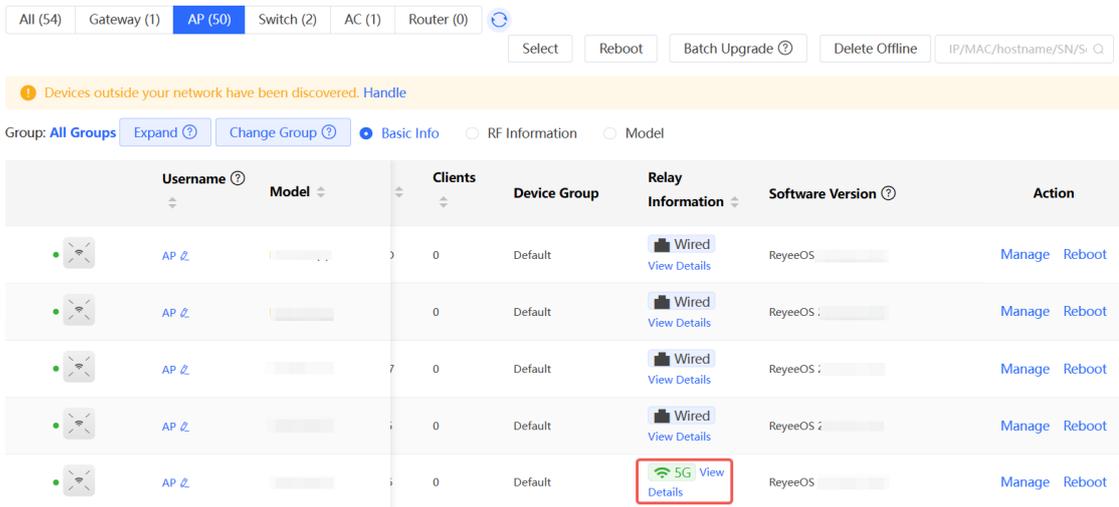
Finish

- (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.

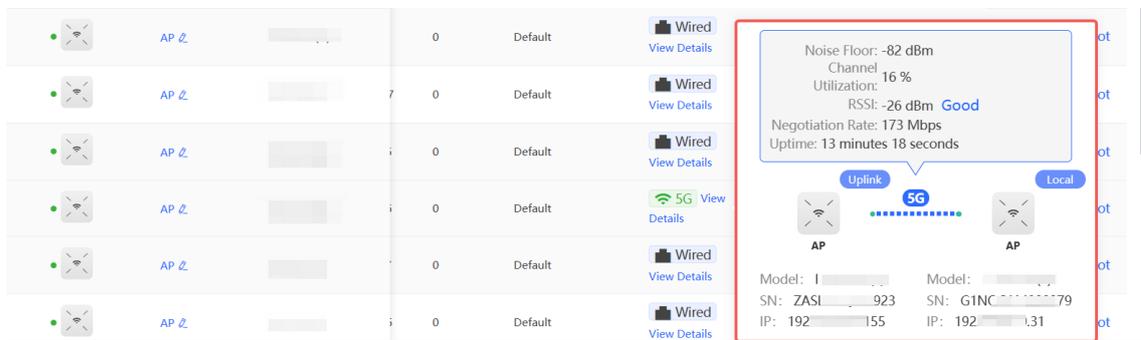


- (6) Power off the new AP and install it as planned.
- (7) Log in to the web interface of a device on the target network. In **Network-Wide** mode, choose **Devices > AP**.

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



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



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

3.3 Configuring the Service Network

3.3.1 Configuring the Wired Network

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

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



- (2) Configure a VLAN for wired access, specify the address pool server for access clients in this VLAN, and determine whether to create a new DHCP address pool. By default, the gateway is used as the address pool server to allocate addresses to access clients. If an access switch is available in this networking, you can select this switch as the address pool server. After setting the service parameters, click **Next**.

* Description:

VLAN: ▾

* VLAN ID:

Address Pool Gateway

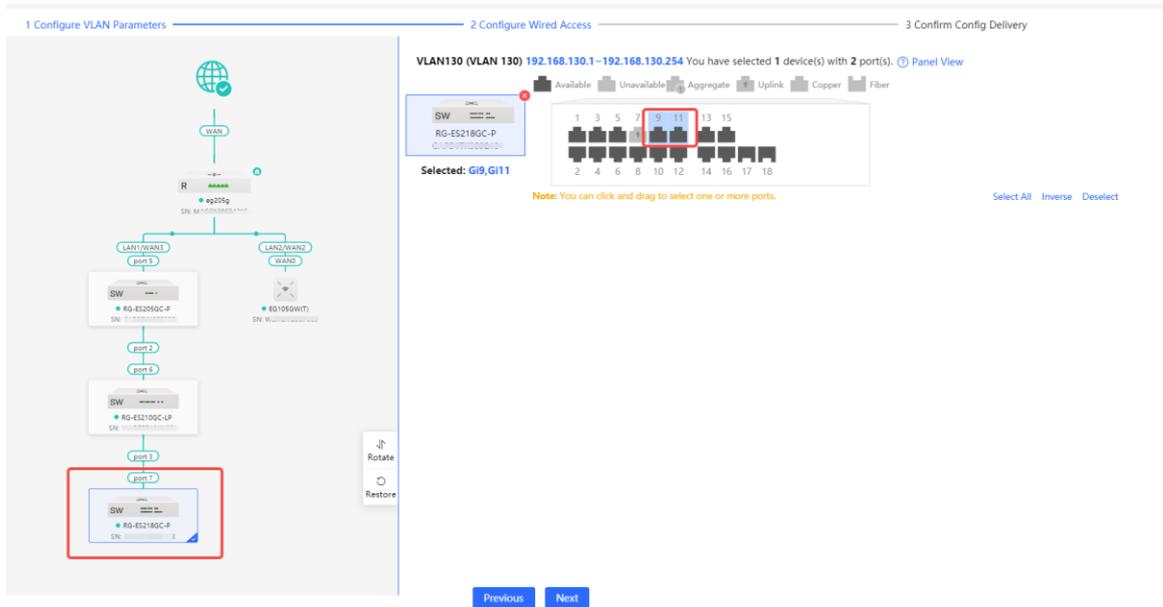
Server

Gateway/Mask: /

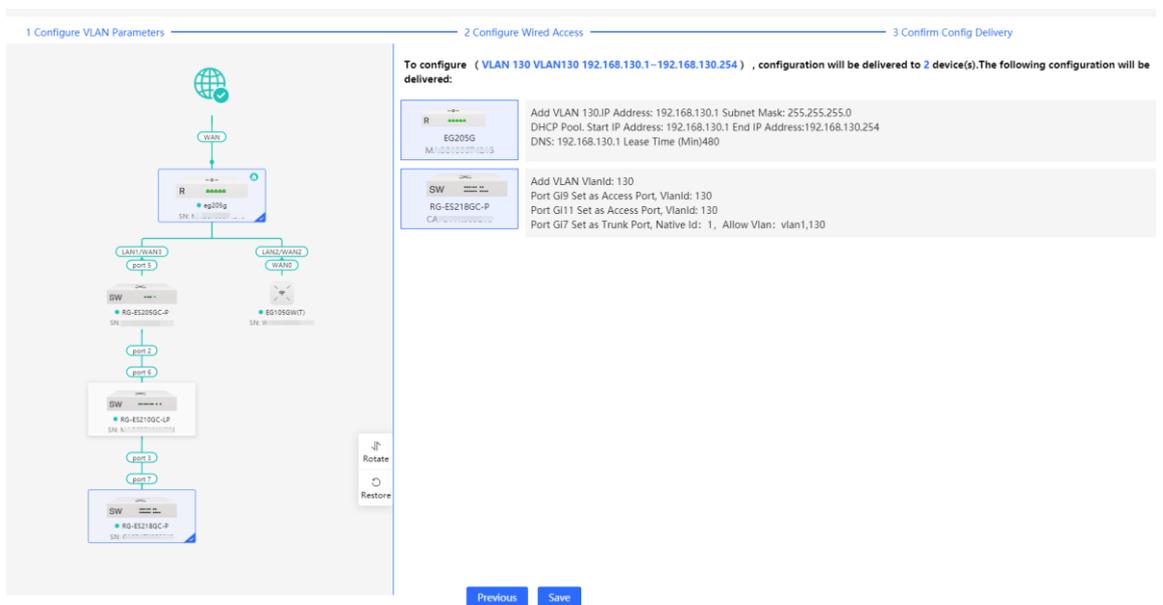
DHCP Pool:

IP Range: -

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



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



3.3.2 Configuring the Wireless Network

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

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

Network Planning(3) All ▾

[Add Wired VLAN](#) [Add Wi-Fi VLAN](#)

VLAN1 Wi-Fi VLAN >

VLAN1

VLAN120 Wi-Fi VLAN

VLAN 120

SVI Address: (**Gateway**)
192.168.120.1

DHCP Pool (**Enable**)
192.168.120.1/255.255.255.0
IP Count: 254
Lease Time (Min): 480

 [Setup](#)

VLAN130 >

VLAN 130

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

Add ×

* SSID ?

Purpose ? General | IoT | Guest

Band ? 2.4G 5G

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

Encryption Open Security 802.1x (Enterprise) !

* Security ?

* Wi-Fi Password

----- [Advanced Settings](#) -----

----- [Advanced Settings](#) -----

SSID Encoding

Wi-Fi Standard

Schedule

VLAN

Hide SSID The SSID is hidden and must be manually entered.

Client Isolation Prevent mutual access between clients connected to this SSID on this AP.

Layer 2 Isolation Prevent mutual access between clients connected to this SSID on all APs.

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

XPress The client will experience faster speed.

Layer 3 Roaming The client will keep the IP address unchanged on the Wi-Fi network.

802.11r After this feature is enabled, roaming time is reduced to achieve fast transition.

LimitSpeed

[Do you want to edit RF parameters? Navigate to Radio Frequency for configuration.](#)

Applicable bands include 2.4 GHz, 5 GHz, and 2.4 GHz + 5 GHz.

Encryption modes include: **Open**, **Security**, and **802.1x (Enterprise)**. When the encryption mode is set to **Security**, you need to set the Wi-Fi password.

Click **Advanced Settings** to configure the advanced parameters, including Wi-Fi Standard, Wireless Schedule, Hide SSID, Client Isolation and so on.

- (3) Configure a VLAN for wireless access, specify the address pool server for access clients in this VLAN, and determine whether to create a new DHCP address pool. By default, the gateway is used as the address pool server to allocate addresses to access clients. If an access switch is available in this networking, you can select this switch as the address pool server. After setting the service parameters, click **Next**.

* Description:

VLAN: ▾

* VLAN ID:

Address Pool Gateway

Server ?

Gateway/Mask: /

DHCP Pool:

IP Range: -

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

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

To configure (VLAN 120 VLAN120 192.168.120.1-192.168.120.254) , configuration will be delivered to 3 device(s).The following configuration will be delivered:

- AP SSID:Test Password:Open
- R Add VLAN 120.IP Address: 192.168.120.1 Subnet Mask: 255.255.255.0
 DHCP Pool. Start IP Address: 192.168.120.1 End IP Address:192.168.120.254
 DNS: 192.168.120.1 Lease Time (Min):480
- SW Add VLAN VlanId: 120
 Port Gi7 Set as Trunk Port, Native Id: 1, Allow Vlan: vlan1,120

Previous
Save

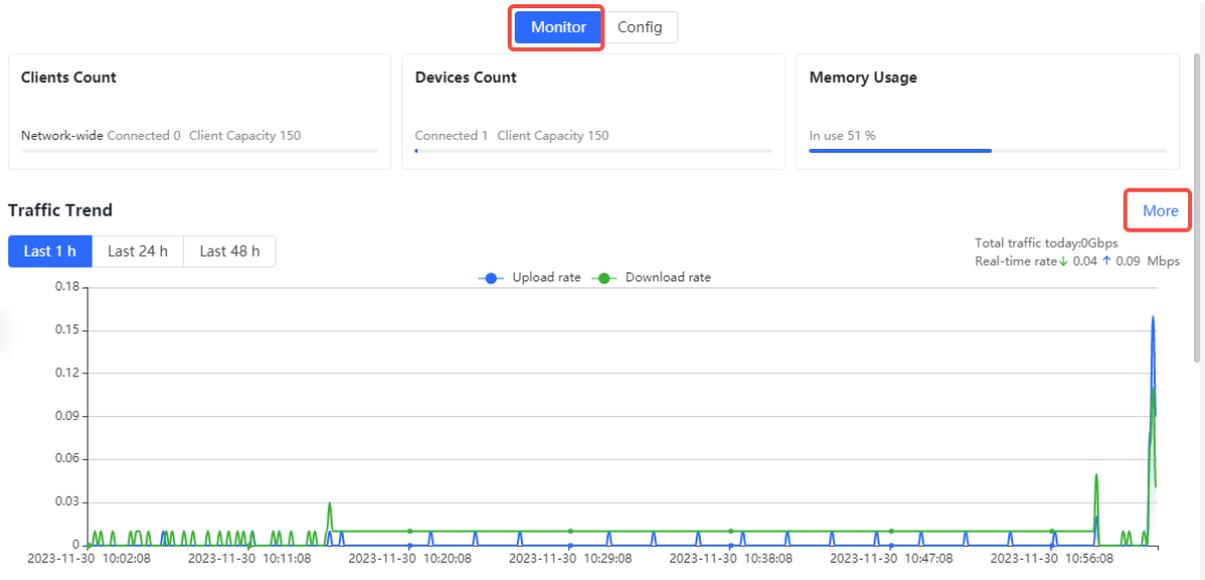
3.4 Supporting Traffic Monitoring

Traffic monitoring can be carried out based on ports, users, and applications. The real-time or historical uplink traffic, downlink traffic, and number of sessions can be displayed.

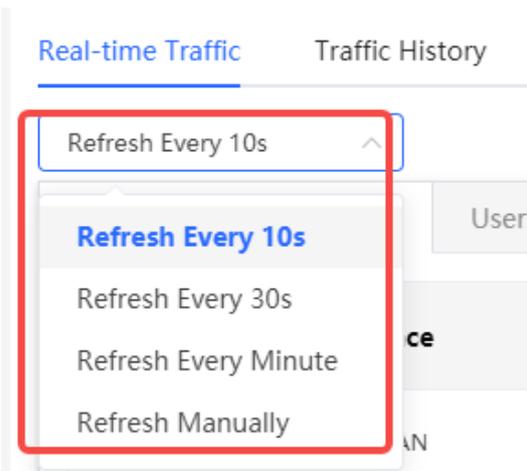
3.4.1 Viewing Real-Time Traffic

Choose **One-Device > Gateway > Monitor**.

Click **More** to the right of **Traffic Trend** to access the gateway's monitoring details page. On the page that is displayed, click the **Real-time Traffic** tab.



Select a refresh frequency to set the frequency of real-time traffic refresh.



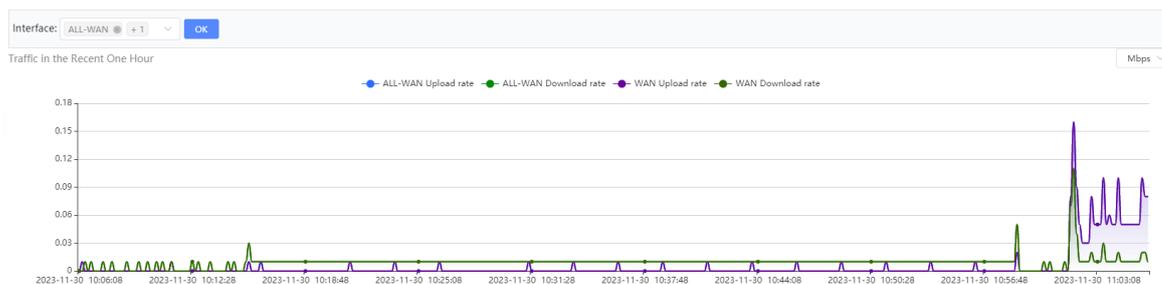
1. Viewing Real-time Traffic of an Interface

Click the **Interface Real-Time Traffic** tab to view the uplink or downlink traffic of an interface or the entire device.

| Interface | Traffic Rate | Downlink | Uplink | Mbps |
|-----------|---|----------|----------|------|
| ALL-WAN | <div style="width: 100%;"><div style="width: 10%; background-color: green;"></div><div style="width: 90%; background-color: blue;"></div></div> | 0.02Mbps | 0.10Mbps | |
| WAN | <div style="width: 100%;"><div style="width: 10%; background-color: green;"></div><div style="width: 90%; background-color: blue;"></div></div> | 0.02Mbps | 0.10Mbps | |

- View traffic in the recent one hour

Select an interface or **ALL-WAN** in the **Interface** drop-down menu. You can view the traffic and sessions of the interface or device in the last one hour, including the sessions of the excluded WAN port.

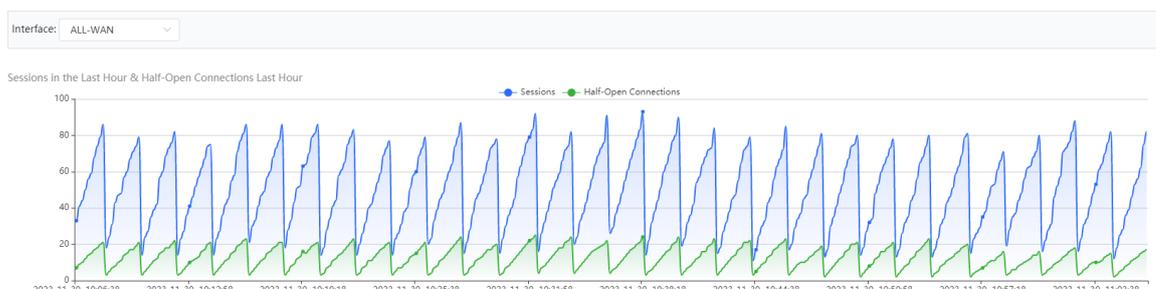


Note

Uplink traffic and downlink traffic are color-coded in the figure. You can move the cursor over a curve to view uplink traffic and downlink traffic at a certain time.

- View the number of sessions and half-open connections in the last one hour

Select an interface or **ALL-WAN** in the **Interface** drop-down menu to check the number of sessions and half-open connections in the last one hour (including the session information of the excluded WAN port).



2. Viewing Real-time Traffic of a Client

Click the **User Real-Time Traffic** tab to view the IP address, name, online duration, number of sessions, and uplink and downlink traffic of each client.

If there are multiple clients, the system displays traffic data by downlink traffic in descending order by default. The sorting mode can be switched based on uplink traffic or downlink traffic. You can set the traffic unit, number of items to be displayed on the current page, paging display, and other functions based on service requirements.

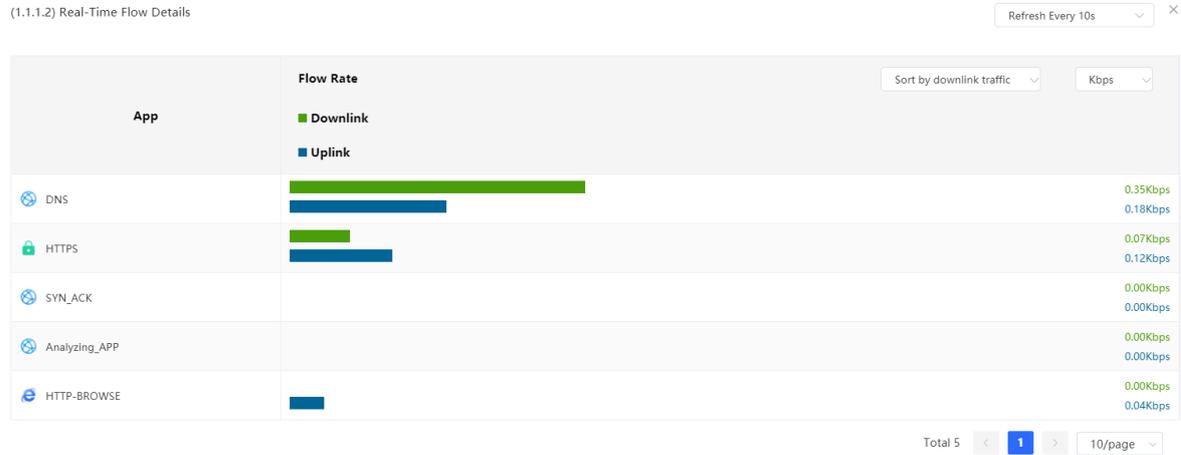
| No. | IP | Name | Online Duration | Sessions | Flow Rate | | Detailed |
|-----|---------|---------|---------------------------------------|----------|-----------|----------|--------------------------|
| | | | | | Downlink | Uplink | |
| 1 | 1.1.1.2 | 1.1.1.2 | 15 days 7 hours 19 minutes 21 seconds | 38 | 0.00Mbps | 0.00Mbps | Detailed |

Total 1 1 /page

Click **Detailed**. The system displays the uplink and downlink traffic rates of various applications used by the current client. You can set the sorting mode (by downlink traffic or uplink traffic), unit, and other parameters based on service requirements.

Note

To view real-time traffic of a client, ensure that the **Traffic Audit** function is enabled on the **App Real-time Traffic** page.



3. Viewing Real-time Traffic of an App

Click the **App Real-Time Traffic** tab and enable **Traffic Audit**. You can view the name, application group, uplink traffic, and downlink traffic of each app.

If there are multiple apps, the system displays traffic data by downlink traffic in descending order by default. The sorting mode can be switched based on uplink traffic or downlink traffic. You can set the traffic unit, number of items to be displayed on the current page, paging display, and other functions based on service requirements.

Traffic Audit

| No. | App | App Group | Flow Rate | Action |
|-----|---------------|-----------|----------------------|----------------|
| 1 | DNS | Other | 0.00Mbps 0.00Mbps | Block Detailed |
| 2 | HTTPS | Other | 0.00Mbps 0.00Mbps | Block Detailed |
| 3 | Analyzing_APP | Other | 0.00Mbps 0.00Mbps | Block Detailed |
| 4 | SYN_ACK | Other | 0.00Mbps 0.00Mbps | Block Detailed |
| 5 | HTTP-BROWSE | Other | 0.00Mbps 0.00Mbps | Block Detailed |

Total 5 | 10/page

Click **Detailed**. The details of the traffic used by each user of the current application are displayed in the pop-up dialog box. You can set the sorting mode (by downlink traffic or uplink traffic), unit, and other parameters based on service requirements.

(DNS) Real-Time Flow Details Refresh Every 10s ×

| ip | Name | Flow Rate | | Sort by downlink traffic | Kbps |
|---------|---------|--|---|--------------------------|----------------------|
| | | Downlink | Uplink | | |
| 1.1.1.2 | 1.1.1.2 | <div style="width: 80%; height: 10px; background-color: green;"></div> | <div style="width: 20%; height: 10px; background-color: blue;"></div> | | 0.69Kbps 0.37Kbps |

Total 1 < 1 > 10/page

Click **Block**. In the displayed message, click **OK** to block the corresponding application.

Tips ×

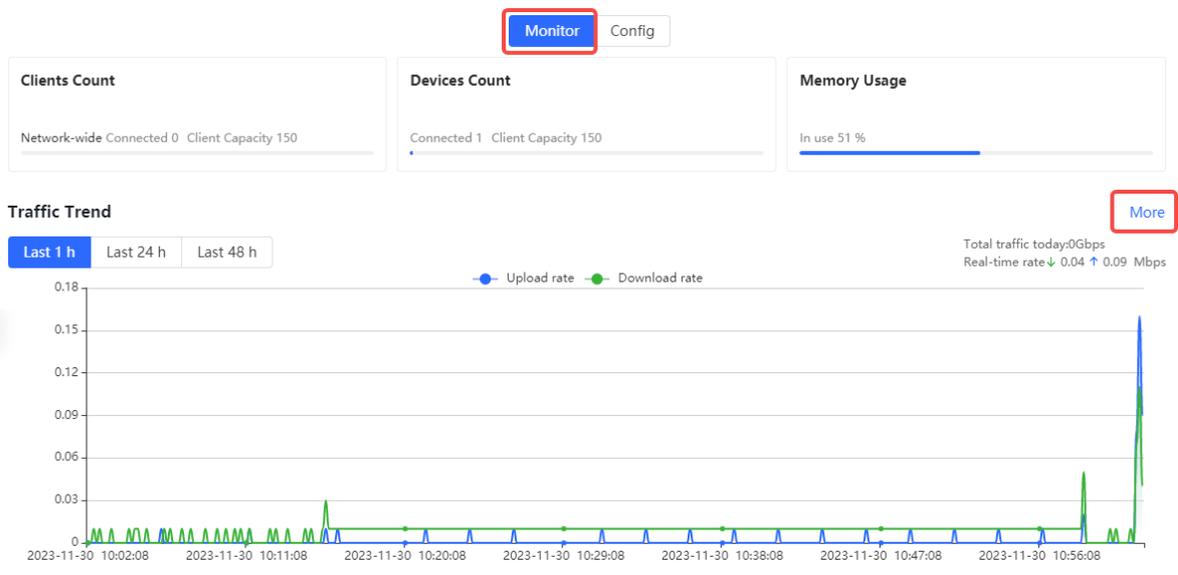
! Are you sure you want to block the current application?

Cancel **OK**

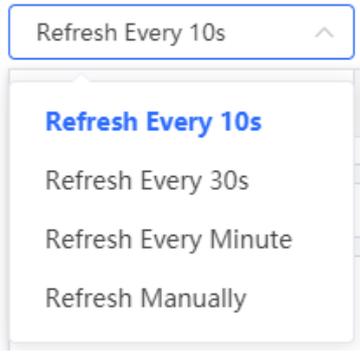
3.4.2 Viewing Historical Traffic

Choose **One-Device > Gateway > Monitor**.

Click **More** to the right of the **Traffic Trend** tab. On the gateway monitoring details page, click the **Traffic History** tab.



Select a refresh frequency to set the frequency of historical traffic refresh.



1. Viewing Historical Traffic of an Interface

- (1) Click the **Traffic History** tab.
- (2) Select an interface or ALL-WAN in the Interface drop-down menu.
- (3) Select a time range.
- (4) The system displays historical traffic, session, and half-open connection statistics of an interface or the device within a specified period.



Note

Uplink traffic and downlink traffic are color-coded in the figure. You can move the cursor over a curve to view uplink traffic and downlink traffic at a certain time.

2. View Historical Traffic of a Client

Click the **User Traffic History** tab. Select a time range. You can view historical traffic data of clients today or this week on the **User Traffic History** page.

If there are multiple clients, the system displays the traffic data by downlink traffic in descending order by default. You can view the online duration, uplink traffic, and downlink traffic of each client in the time span. The sorting mode can be switched based on the uplink traffic or downlink traffic. You can set the traffic unit, number of items to be displayed on the current page, paging display, and other functions based on service requirements.

Period: Day Week Month The time range of current flow: Today

| No. | IP | Name | Online Duration | Traffic History | Detailed |
|-----|---------|---------|-------------------------------|--|--------------------------|
| 1 | 1.1.1.2 | 1.1.1.2 | 10 hours 9 minutes 10 seconds | Sort by downlink traffic Downlink: 2.59MB Uplink: 1.49MB | Detailed |

Total 1 1 10/page

Click **Detailed**. The details of the current client's app usage, including the traffic size and online duration, are displayed in a pop-up dialog box. You can set the sorting mode (by downlink traffic or uplink traffic), unit, and other parameters based on service requirements.

Note

To view historical traffic of a client, ensure that the **Traffic Audit** function is enabled on the **App Real-Time Traffic** page.

(1.1.1.2) Today Flow Details Refresh Every 10s

| App | Online Duration | Traffic History | Detailed |
|---------------|--------------------------------|------------------------------------|----------|
| DNS | 10 hours 36 minutes 36 seconds | Downlink: 2.59MB Uplink: 1.41MB | |
| HTTPS | 10 hours 36 minutes 36 seconds | Downlink: 0.06MB Uplink: 0.09MB | |
| HTTP-BROWSE | 2 hours 50 minutes 36 seconds | Downlink: 0.05MB Uplink: 0.04MB | |
| SYN_ACK | 2 hours 18 minutes 4 seconds | Downlink: 0.01MB Uplink: 0.01MB | |
| Analyzing_APP | 2 hours 12 minutes 16 seconds | Downlink: 0.01MB Uplink: 0.00MB | |

Total 6 1 10/page

3. View Historical Traffic of an App

Click the **Traffic History** tab, enable the **Traffic Audit** function, and view the application historical traffic.

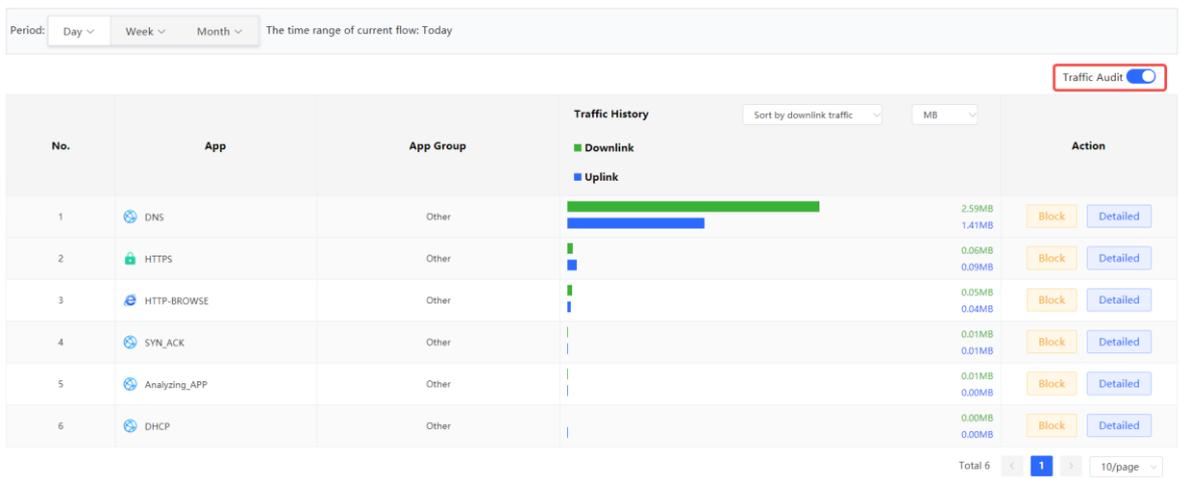
Note

The status of **Traffic Audit** switch is consistent with that on the **App Real-Time Traffic** page. After it is enabled, the **App Real-Time Traffic** function and **App History Traffic** function are enabled.

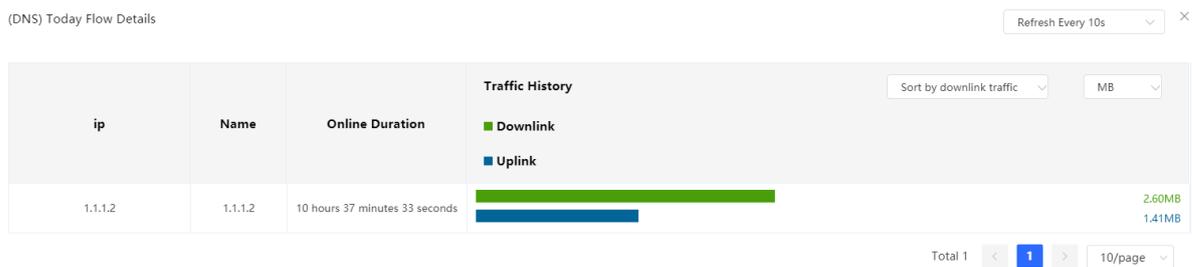
On the **App History Traffic** page, you can view historical traffic of an application today or this week.

If there are multiple applications, the system displays traffic data by downlink traffic in descending order by default. You can view the name, application group, uplink traffic, and downlink traffic of each application in the time span.

The sorting mode can be switched based on uplink traffic or downlink traffic. You can set the traffic unit, number of items to be displayed on the current page, paging display, and other functions based on service requirements.



Click **Detailed**. The system displays details about the traffic used by each client of the current application in a pop-up dialog box. You can set the sorting mode (by downlink traffic or uplink traffic), unit, and other parameters based on service requirements.



Click **Block**. In the displayed message, click **OK** to block the corresponding application.

Tips

Are you sure you want to block the current application?

Cancel OK

3.5 Supporting the URL Logging Function

URL logs record and display website domain names accessed by devices connected to LAN ports within a certain minute, access count, and audit results.

Choose **One-Device > Gateway > Monitor**.

- (1) Click **More** to the right of the **Traffic Trend** tab. On the page that is displayed, click the **URL Log** tab.

- (2) Toggle on the **Enable** switch. On the pop-up dialog box, click **OK**.



Tips ×

! Are you sure you want to enable the URL Log?

- (3) (Optional) Configure **record IP**.

The system records access records of all devices connected to LAN ports by default. If you need to view access records of a single device, set **record IP**.

Enter the device IP address in **record IP** and click **Save**.

Enable

Record IP Only ⓘ

| Time | IP | Access Count | URL | Action |
|------------------|----------------|--------------|------------------------|--------|
| 2023-11-30 15:17 | 192.168.110.11 | 2 | http://conf.wsm.360.cn | Allow |
| 2023-11-30 15:17 | 192.168.110.11 | 2 | http://qup.f.360.cn | Allow |

Note

If you need to restore access records of all devices connected to LAN ports, clear information in **Record IP Only** and click **Save**.

- (4) Check access records.

The system displays detailed access records, including the time, IP address.

You can search for access records by IP address or URL.

Enable Record IP Only ⓘ

| Time | IP | Access Count | URL | Action |
|------------------|----------------|--------------|------------------------|--------|
| 2023-11-30 15:20 | 192.168.110.11 | 2 | http://conf.wsm.360.cn | Allow |
| 2023-11-30 15:20 | 192.168.110.11 | 2 | http://qup.f.360.cn | Allow |
| 2023-11-30 15:20 | 192.168.110.11 | 1 | https://msgmq.rj.link | Allow |

3.6 Processing Alerts

When a network exception occurs, the system generates an alert and provides suggested actions. Click **Alert Center** in the navigation bar to view the faulty device, alert details, and suggested actions. You can troubleshoot the fault based on the suggested actions.

The screenshot shows the Rujie | Reycc Alert Center interface. At the top, there is a blue header with the logo, a search bar, and an 'Alert Center' notification with a red badge showing '1'. Below the header is a sidebar with navigation options: One-Device, Controller, Gateway, Network-Wide, Workspace, Devices, Clients, and System. The main content area is titled 'View and manage alarms.' and contains an 'Alert List' section. The alert list has columns for 'Expand', 'Alerts', 'Suggestion', and 'Action'. One alert is visible: 'The IP address of the downlink device is already in use.' with a suggestion to check the IP address and change it if static. Below this is a detailed table for the alert.

| Device Name | SN | Type | Time | Details | Action |
|-------------|---------------|--------|---------------------|--|--------|
| | H11A0U100362A | EG205G | 2023-12-11 14:38:55 | An IP address conflict occurs, IP address: 10.52.48.25. Conflicting MAC address: 00:d0:f8:15:92:66 and f0:74:8d:b1:9d:e3 | Delete |

Total 1 | 1 | 10/page

4 Network Settings

4.1 Switching the Work Mode

4.1.1 Work Mode

For details, see Section [2.4 Work Mode](#).

4.1.2 Self-Organizing Network Discovery

When setting the work mode, you can set whether to enable the self-organizing network discovery function. This function is enabled by default.

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

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

Note

- In AC mode, the self-organizing network discovery function is enabled by default.
 - After the self-organizing network discovery function is enabled, you can view the self-organizing role of the device on the Device Details page.
 - The menus on the Web page vary depending on whether the self-organizing network discovery function is enabled. (For details, see Section [2.9 Switching the Work Mode](#).) Find the configuration entry for this function according to the instructions in Configuration Steps below.
-

4.1.3 Configuration Steps

Note

To modify the work mode to wireless repeater, see Section [4.6.2 Wireless Repeater](#).

Choose **One-Device > Gateway**.

Click the current work mode to change the work mode.

Caution

After you switch the work mode, the device will restore factory settings and the device IP address may change. You need to access the Web system again using the new IP address. Exercise caution when performing this operation.

EG205G | eg205g | MGMT IP: 10.80.12.19 | SN: M15 | MAC Address: 0k...7 | Reboot | Working Mode: Router | Hardware Version: 1.00

AC function switch: If a device works in the router mode and the self-organizing network discovery function is enabled, you can enable or disable the AC function. After the AC function is enabled, the device in the router mode supports the virtual AC function and can manage downlink devices. If this function is disabled, the device needs to be elected as an AC in self-organizing network mode and then manage downlink devices.

Working Mode ×

Description:

1. The device IP address may change upon mode change.
2. Change the endpoint IP address and ping the device.
3. Enter the new IP address into the address bar of the browser to access Eweb.
4. The system menu varies with different work modes.

Working Mode ? ▼

Self-Organizing Network ? ? Tips

AC ?

4.2 Port Settings

You can choose **Port Settings** to set port parameters and view the port information.

4.2.1 Setting the Port Parameters

Choose **One-Device > Gateway > Config > Network > Port Settings > Basic Settings**.

[Basic Settings](#) | [Port Info](#)

? Configure port status, duplex mode, rate and flow control.

| Port | Status | Duplex Mode/Rate | | Flow Control | | Action |
|-----------|--------|------------------|-------------------|---------------|---------------|----------------------|
| | | Config Status | Actual Status | Config Status | Actual Status | |
| LAN0 | Enable | Auto/Auto | Unknown/Unknown | Disable | Unknown | Edit |
| LAN1/WAN3 | Enable | Auto/Auto | Full-Duplex/1000M | Disable | Disable | Edit |
| LAN2/WAN2 | Enable | Auto/Auto | Full-Duplex/1000M | Disable | Disable | Edit |
| LAN3/WAN1 | Enable | Auto/Auto | Full-Duplex/1000M | Disable | Disable | Edit |
| WAN | Enable | Auto/Auto | Full-Duplex/1000M | Disable | Disable | Edit |

- (1) Choose the target port and click **Edit**.

Port:LAN0
×

Status:

Rate:

Working Mode:

Flow Control:

Table 4-1 Port Configuration Parameters

| Parameter | Description |
|--------------|---|
| Status | Enable or disable the port. |
| Rate | Set the data transmission rate of the port. The options are Auto , 10M , 100M , and 1000M . When selecting the port rate, ensure that the connected device can communicate at the same rate. If a device only supports a rate of 100 Mbps, but the port rate is set to 1000 Mbps, communication may fail due to rate mismatch. |
| Working Mode | Set the working mode of the port: <ul style="list-style-type: none"> ● Auto: The port automatically detects the working mode of the connected device and automatically selects the full-duplex or half-duplex mode based on the connected device. ● Full-duplex: In full-duplex mode, a port can send and receive data simultaneously, achieving bidirectional communication. ● Half-duplex: In half-duplex mode, a port can only send or receive data, but not both. |
| Flow Control | When wired ports of the device work in different rates, data blocking may occur, leading to slow network speed. Enabling port flow control helps relieve the data congestion. |

(2) Set the port parameters and click **OK**.

4.2.2 Viewing the Port Information

Choose **One-Device > Gateway > Config > Network > Port Settings > Port Info**.

Basic Settings [Port Info](#)

Traffic data is updated every 5 minutes. [Refresh](#) [Clear All](#)

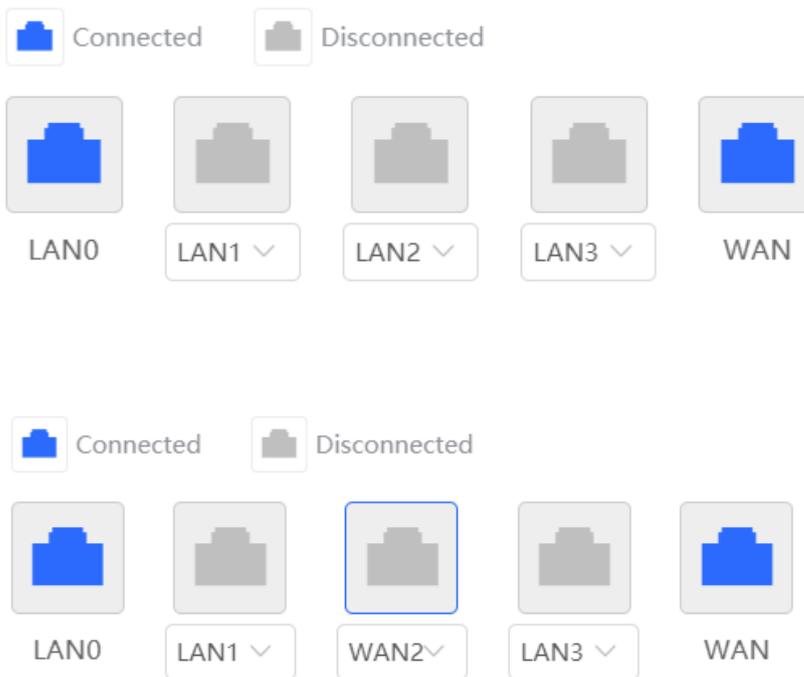
| Port | Rate | Rx/Tx Speed (kbps) | Rx/Tx Bytes | Rx/Tx Packets | CRC/FCS Error Packets | Corrupted/Oversized Packets | Conflicts |
|-----------|--------------|--------------------|-----------------|------------------|-----------------------|-----------------------------|-----------|
| LAN0 | Disconnected | 0/0 | 1.09G/1.73G | 8386170/7207651 | 0/0 | 0/0 | 0 |
| LAN1/WAN3 | 1000M | 0/0 | 93.37M/34.26M | 256091/173024 | 0/0 | 0/0 | 0 |
| LAN2/WAN2 | 1000M | 0/0 | 49.28M/34.04M | 240416/239703 | 0/0 | 0/0 | 0 |
| LAN3/WAN1 | 1000M | 0/8 | 364.87M/615.33M | 1046197/1163807 | 0/0 | 0/0 | 0 |
| WAN | 1000M | 48/8 | 2.95G/1.54G | 12632449/9913297 | 0/0 | 0/0 | 0 |

4.3 Configuring the WAN Ports

Choose **One-Device > Gateway > Config > Network > WAN**.

You can configure multi-line access for the device to allow multiple lines to work simultaneously. After you switch to multi-line access, you need to specify the egress provider of the lines and set the load balancing mode, in addition to setting basic network parameters for the WAN ports.

- The number of lines supported varies with the product. The actual configuration prevails.
- If the LAN/WAN switchover can be configured, click the port to switch between the LAN and WAN modes.



The number of the WAN ports and lines will change through LAN/WAN switchover. The actual number prevails,

4.3.1 Configuring the Internet Access Mode

Choose **One-Device > Gateway > Config > Network > WAN**.

The device can access the WAN in one of the following three methods: static IP, DHCP, and PPPoE dialing. Select a proper method based on the actual broadband line type. For details, see Section [2.5 Configuration Wizard \(Router Mode\)](#).

Select the target WAN port and configure **Internet** by selecting PPPoE, DHCP or Static IP from the drop-down list box.

When the Internet access mode is not **DHCP** or **PPPoE**, you can specify a DNS server to ensure that the device can correctly parse domain names and access Internet resources, thereby improving the access speed and security.

Single Line Dual-Line Three Lines Four Lines

WAN Line Detection

* Internet (?) DHCP

Username and password are not required.

IP Address 10.52.48.172

Subnet Mask 255.255.248.0

Gateway 10.52.48.1

DNS Server 172.30.44.20 192.168.5.28

Dedicated DNS Server (?) Optional

----- Advanced Settings -----

Save

4.3.2 Modifying the MAC Address

Choose **One-Device > Gateway > Config > Network > WAN**.

Sometimes, the provider restricts Internet access of devices with unknown MAC addresses out of security considerations. In this case, you can change the MAC addresses of the WAN ports to valid MAC addresses.

Select the target WAN port. Click **Advanced Settings**, enter a MAC address, and click **Save**. You do not need to modify the default MAC address unless otherwise specified.

----- Advanced Settings -----

* MTU (?) MTU Detection

* MAC Address (?)

802.1Q Tag

Private Line (?)

NAT Mode (?)

Save

4.3.3 Modifying the MTU

Choose **One-Device > Gateway > Config > Network > WAN**.

1. Modifying the MTU

MTU specifies the maximum transmission unit allowed to pass a WAN port. By default, the MTU of a WAN port is 1500 bytes. Sometimes, large data packets are limited in transmission speed or prohibited in the ISP network, leading to slow network speed or even network disconnection. If this occurs, you can click **Advanced Settings**, set the MTU to a smaller value.

----- Advanced Settings -----

* MTU (?) MTU Detection

* MAC Address (?)

802.1Q Tag

Private Line (?)

NAT Mode (?)

Save

If the MTU value is unknown, click **MTU Detection** to configure the one-click MTU detection, and adjust the MTU settings based on the results obtained from MTU detection.

2. Detecting the MTU

Click **MTU Detection** to configure the one-click MTU detection to determine the MTU between two communication devices.

Enter the destination IP/domain name, retry count, ICMP echo request timeout, minimum MTU, maximum MTU, and click **Start** to start the detection.

MTU Detection



| | |
|---|--|
| * IP Address/Domain | <input type="text" value="www.google.com"/> |
| * Retry Count | <input type="text" value="1"/> |
| * ICMP Echo Request Timeout | <input type="text" value="1"/> s |
| * Min. MTU | <input type="text" value="576"/> |
| * Max. MTU | <input type="text" value="1500"/> |
| | <input type="button" value="Start"/> <input type="button" value="Stop"/> |
| <div style="border: 1px solid #ccc; padding: 5px; min-height: 80px;">Result</div> | |

4.3.4 Configuring the Private Line

Choose **One-Device > Gateway > Config > Network > WAN**.

Click **Advanced Settings**, turn on **Private Line** and determine whether to set the current WAN line as a private line. Generally, private lines are used for access to specific internal networks but not the Internet. Private lines provide higher network security.

----- Advanced Settings -----

* MTU (?) MTU Detection

* MAC Address (?)

802.1Q Tag

Private Line (?)

NAT Mode (?)

4.3.5 Configuring the VLAN Tag

Choose **One-Device > Gateway > Config > Network > WAN**.

Some ISPs require that packets transmitted to their networks carry VLAN IDs. In this case, you can click **Advanced Settings**, enable the **802.1Q Tag** function and set a **VLAN ID** and **Priority** for the WAN port. By default, the VLAN tag function is disabled. You are advised to keep the VLAN tag function disabled unless otherwise specified.

----- Advanced Settings -----

* MTU (?) MTU Detection

* MAC Address (?)

802.1Q Tag

*** VLAN ID**

Private Line (?)

NAT Mode (?)

4.3.6 Configuring NAT Mode

Choose **One-Device > Gateway > Config > Network > WAN**.

When an intranet needs to communicate with an extranet, Network Address Translation (NAT) must be configured to convert the private IP address into a globally unique IP address, so that the private network can access the public network.

Click **Advanced Settings**, toggle on **NAT Mode** to enable the NAT mode. When the NAT mode is disabled, this router operates in router mode to forward data packets, enabling mutual access between hosts connected to the LAN and the WAN ports of this router.

----- Advanced Settings -----

* MTU (?) MTU Detection

* MAC Address (?)

802.1Q Tag

Private Line (?)

NAT Mode (?)

⚠ Caution
 Disabling NAT mode may potentially impact the functionality of the self-organizing network (SON) feature.

4.3.7 Configuring the Multi-Line Load Balancing Mode

Choose **One-Device > Gateway > Config > Network > WAN > Load Settings**.

When multiple lines are available, some traffic is forwarded along the line selected based on the address library and the remaining traffic is distributed to other lines in load balancing mode.

Table 4-2 Load balancing modes

| Load Balancing Mode | Description |
|---------------------|---|
| Load balancing | <p>The traffic will be spread across multiple links according to the weight of each WAN port. Larger traffic will be distributed to the WAN port with a higher weight.</p> <p>When you select this mode, you must specify the weight of each WAN port. For example, if WAN and WAN 1 weight are set to 3 and 2 respectively, 60% of the total traffic will be routed over WAN and 40% over WAN 1.</p> |
| Active/Secondary | <p>All traffic is routed over the primary interface. Once the primary interface fails, traffic will be switched over to the secondary interface.</p> <p>If there are multiple primary or secondary interfaces, please configure their weight. (See balanced mode.)</p> |

| Load Balancing Mode | Description |
|---------------------|--|
| Forced Switch | <p>With Load Mode switched from Load balancing to Active/Secondary, if Forced Switch is not selected, traffic of new connections will be routed through the specified primary interface, while the egress for the traffic of existing connections remains unchanged.</p> <p>When Forced Switch is selected, traffic of both new and existing connections will be routed to the primary interface.</p> |

The system supports IPv4 and IPv6 multi-link load balancing. IPv4 multi-link load balancing is enabled by default, while IPv6 multi-link load balancing needs to be enabled manually.

1. Configuring IPv4 Multi-Link Balancing

Load Balancing Settings v4

Load Mode (?) Loading balancing ▼

Load Balancing Policy Smart Load Balancing ▼

WAN Rate

* Uplink 1000 Mbps * Downlink 1000 Mbps

WAN1 Rate

* Uplink 1000 Mbps * Downlink 1000 Mbps

Load Balancing Settings v4

Load Mode (?) Active/Secondary ▾ (?) Forced Switch

Load Balancing Policy Smart Load Balancing ▾

WAN0 Set as Primary Interface ▾

* Uplink 1000 Mbps * Downlink 1000 Mbps

WAN1 Set as Secondary Interface ▾

* Uplink 1000 Mbps * Downlink 1000 Mbps

- (1) Select a load balancing mode from the **Load Mode** drop-down list.
- (2) Select a loading balancing policy from the **Load Balancing Policy** drop-down list.

Table 4-3 Description of Load Balancing Policies (IPv4)

| Load Balancing Policy | Description |
|----------------------------------|--|
| Based on Connections | After you enable this policy, the traffic is routed over multiple links based on the links. Packets with the same source IP address, destination IP address, source port, destination port, and protocol are routed over the same link. |
| Based on Src IP Address | After you enable this policy, the traffic is routed over multiple links based on the source IP address. The traffic from the same user (same source IP address) will be routed to the same interface. This policy prevents traffic from the same user from being routed to different links, lowering the risks of network access exceptions. |
| Based on Src and Dest IP Address | After you enable this policy, the traffic is routed over multiple links based on the source IP address and destination. The traffic of the same source IP address and destination IP address will be routed to the same interface. |
| Smart Load Balancing | After you enable this feature, the traffic is routed over multiple links based on the link bandwidth, the actual loads of the links, application recognition and traffic prediction. |

- (3) Set the uplink and downlink bandwidths or the weight for each WAN port.

- When the load balancing policy is set to **Based on Connections**, **Based on Src IP Address**, or **Based on Src and Dest IP Address**, a weight must be set for each WAN port.

Load Balancing Settings v4

Load Mode  Loading balancing 

Load Balancing Policy Based on Src IP Addresses 

* WAN Weight 1

* WAN1 Weight 1

Note

The higher the value of the weight, the more traffic is directed to the WAN port.

- When the load balancing policy is set to **Smart Load Balancing**, the uplink and downlink bandwidths must be set for each WAN port.

Load Mode Loading balancing 

Load Balancing Policy Smart Load Balancing 

WAN0 Rate

* Uplink 1000 Mbps

* Downlink 1000 Mbps

WAN1 Rate

* Uplink 1000 Mbps

* Downlink 1000 Mbps

- (4) Click **Save**.

2. Configuring IPv6 Multi-Link Balancing

Load Balancing Settings v6

Enable

Load Mode ?

Load Balancing Policy

If you fail to access online bank service, please select Based on Src IP Address.

* WAN Weight

* WAN1 Weight

- (1) Toggle on **Enable** to enable the IPv6 multi-link load balancing mode.
- (2) Select a load balancing mode from the **Load Mode** drop-down list.
- (3) Select a loading balancing policy from the **Load Balancing Policy** drop-down list.

Table 4-4 Description of Load Balancing Policies (IPv6)

| Load Balancing Policy | Description |
|----------------------------------|--|
| Based on Connections | After you enable this policy, the traffic is routed over multiple links based on the links. Packets with the same source IP address, destination IP address, source port, destination port, and protocol are routed over the same link. |
| Based on Src IP Address | After you enable this policy, the traffic is routed over multiple links based on the source IP address. The traffic from the same user (same source IP address) will be routed to the same interface. This policy prevents traffic from the same user from being routed to different links, lowering the risks of network access exceptions. |
| Based on Src and Dest IP Address | After you enable this policy, the traffic is routed over multiple links based on the source IP address and destination. The traffic of the same source IP address and destination IP address will be routed to the same interface. |

- (4) Set a weight for each WAN port.
The valid range of weight is 1 to 100000.

Note

The higher the value of the weight, the more traffic is directed to the WAN port.

- (5) Click **Save**.

4.3.8 Configuring Line Detection

Choose **One-Device > Gateway > Config > Network > WAN > Line Detection**.

After configuring multiple WAN ports, use the line detection function to check whether lines are connected to the external network. If the network is down, the system does not select a route based on the interface, such as load balancing, policy-based routing, and ISP routing.

The system supports IPv4 and IPv6 WAN link detection, which can be enabled separately.

1. Configuring IPv4 WAN Link Detection

- (1) On the **IPv4 WAN Link Probe** page, select a WAN interface, and toggle on **Enable** to enable IPv4 WAN link detection.

IPv4 WAN Link Probe

| Interface | Enable | Destination IP | Latency/ms | Packet loss/% | Status | Action |
|-----------|-------------------------------------|---------------------------|------------|---------------|--------|----------------------|
| WAN0 | <input checked="" type="checkbox"/> | 8.8.8.8 www.google.com | 23.49 | 0.00 | Online | Edit |
| WAN1 | <input checked="" type="checkbox"/> | 8.8.8.8 www.google.com | 0.00 | 0.00 | Online | Edit |

- (2) In the WAN port list, select a WAN port for line detection, and click **Edit**.
- (3) Configure the parameters of the line detection function.

Edit
×

Destination IP Add

Delete

Advanced Settings

* Probe Interval (s)

* Timeout (s)

* Number of Consecutive Probe Successes

* Probe Rounds for Going Offline

Cancel
OK

Table 4-5 Description of Link Detection (IPv4)

| Parameter | Description |
|---------------------------------------|---|
| Destination IP | The destination IP address to which the system sends ping messages. You can set up to three destination IP addresses. The system sends ping messages to one of the IP addresses randomly during detection. |
| Probe Interval (s) | Interval for the system to perform connectivity detection. The default value is 1 second. |
| Timeout (s) | The maximum timeout period during which the device waits for a response after sending a ping message to the destination IP address. If no response is received within this time, the probe packet is marked as timed out. The default value is 3 seconds. |
| Number of Consecutive Probe Successes | The system periodically sends a ping message to a detection destination IP address at the specified interval. If the ping succeeds and the number of consecutive successful pings reaches the set number of Number of Consecutive Probe Successes , the WAN interface is set to be online. |
| Probe Rounds for Going Offline | The system periodically sends a ping message to a detection destination IP address at the specified interval. If the ping fails and the number of consecutive unsuccessful pings reaches the set number of Probe Rounds for Going Offline , the WAN interface is set to be offline. |

(4) Click **OK**.

2. Configuring IPv6 WAN Link Detection

(1) On the **IPv6 WAN Link Detection** page, toggle on **Enable** to enable IPv6 WAN link detection.

IPv6 WAN Link Probe

| Interface | Enable | Destination IP | Latency/ms | Packet loss/% | Status | Action |
|----------------------|--------------------------|---------------------|------------|---------------|---------|----------------------|
| WAN0 | <input type="checkbox"/> | 2001:4860:4860::888 | 0.00 | 0.00 | Offline | Edit |
| | | 8 | | | | |
| | | 2001:4860:4860::884 | | | | |
| WAN1 | <input type="checkbox"/> | 2001:4860:4860::888 | 0.00 | 0.00 | Online | Edit |
| | | 8 | | | | |
| | | 2001:4860:4860::884 | | | | |
| Save | | | | | | |

(2) In the WAN port list, select a WAN port for link detection, and click **Edit**.

(3) Configure the link detection parameters.

Edit

×

Destination IP

----- Advanced Settings -----

* Probe Interval (s)

* Timeout (s)

* Number of Consecutive Probe Successes

* Probe Rounds for Going Offline

Table 4-6 Description of Link Detection (IPv6)

| Parameter | Description |
|---------------------------------------|---|
| Destination IP | The destination IP address (IPv6) to which the system sends ping messages. You can set up to three destination IP addresses. The system sends ping messages to one of the IP addresses randomly during detection. |
| Probe Interval (s) | Interval for the system to perform connectivity detection. The default value is 1 second. |
| Timeout (s) | The maximum timeout period during which the device waits for a response after sending a ping message to the destination IP address. If no response is received within this time, the probe packet is marked as timed out. The default value is 3 seconds. |
| Number of Consecutive Probe Successes | The system periodically sends a ping message to a detection destination IP address at the specified interval. If the ping succeeds and the number of consecutive successful pings reaches the set number of Number of Consecutive Probe Successes , the WAN interface is set to be online. |

| Parameter | Description |
|--------------------------------|--|
| Probe Rounds for Going Offline | The system periodically sends a ping message to a detection destination IP address at the specified interval. If the ping fails and the number of consecutive unsuccessful pings reaches the set number of Probe Rounds for Going Offline , the WAN interface is set to be offline. |

(4) Click **OK**.

4.4 Configuring the LAN Ports

4.4.1 Modifying the LAN Port IP Address

Choose **One-Device > Gateway > Config > Network > LAN > LAN Settings**.

Click **Edit**. In the dialog box that appears, enter the IP address and subnet mask, and then click **OK**. After you modify the LAN port IP address, you need to enter the new IP address in the browser to log in to the device again before you can configure and manage this device.

LAN Settings + Add Delete Selected

| <input type="checkbox"/> | IP Address [?] | Subnet Ma... [?] | VLAN ID [?] | Remarks | DHCP Serv... [?] | Start IP Address [?] | IP Count [?] | Lease Time (Min) [?] | Action |
|--------------------------|-------------------------|---------------------------|----------------------|---------|---------------------------|-------------------------------|-----------------------|-------------------------------|---|
| <input type="checkbox"/> | 192.168.2.1 | 255.255.255.0 | Default VLAN | - | Enabled | 192.168.2.1 | 254 | 8 | Edit Delete |

Edit

✕

| | |
|--------------------|--|
| * IP Address | <input type="text" value="192.168.2.1"/> |
| * Subnet Mask | <input type="text" value="255.255.255.0"/> |
| Remarks | <input type="text" value="Remarks"/> |
| MAC Address | <input type="text" value="00:11:22:33:44:55"/> |
| DHCP Server | <input checked="" type="checkbox"/> |
| * Start IP Address | <input type="text" value="192.168.2.1"/> |
| * IP Count | <input type="text" value="254"/> |
| * Lease Time (Min) | <input type="text" value="8"/> |
| DNS Server | 192.168.2.1 ⓘ |

Cancel

OK

4.4.2 Modifying the MAC Address

Choose **One-Device > Gateway > Config > Network > LAN > LAN Settings**.

If a static Address Resolution Protocol (ARP) entry (binding between IP address and MAC address of the gateway) is configured to prevent ARP attacks to clients in the LAN, the gateway IP address remains unchanged but its MAC address changes when the gateway is replaced. As a result, the client may fail to learn the gateway MAC address. You can modify the static ARP entry of the client to prevent this problem. You can also change the LAN port MAC address of the new device to the MAC address of the original device to allow clients in the LAN to access the Internet normally.

Click **Edit**. In the dialog box that appears, enter the MAC address, and then click **OK**. You do not need to modify the default LAN port MAC address unless otherwise specified.

Edit ×

* IP Address

* Subnet Mask

Remarks

MAC Address

DHCP Server

* Start IP Address

* IP Count

* Lease Time (Min)

DNS Server 192.168.2.1 ⓘ

4.5 Configuring VLAN

4.5.1 VLAN Overview

Virtual Local Area Network (VLAN) is a communication technology that divides a physical LAN into multiple logical broadcast domains. Each VLAN has independent broadcast domains. Hosts in the same VLAN can directly communicate with each other, while hosts in different VLANs cannot as they are isolated at Layer 2. Compared with traditional Ethernet, VLAN has the following advantages:

- Control broadcast storms: Broadcast packets can only be forwarded inside a VLAN. This saves bandwidth as the performance of a VLAN is not affected by broadcast storms of other VLANs.
- Enhance LAN security: As a VLAN is divided into multiple broadcast domains, packets of different VLANs in a LAN are isolated. Different VLAN users cannot directly communicate, enhancing network security.
- Simplify network management: The VLAN technology can be used to divide the same physical network into different logical networks. When the network topology changes, you only need to modify the VLAN configuration, simplifying network management.

4.5.2 Creating a VLAN

Note

RG-EG105GW(T) and RG-EG105GW-X support a maximum of 16 VLANs.

Choose **One-Device > Gateway > Config > Network > LAN > LAN Settings**.

A LAN can be divided into multiple VLANs. Click **Add** and create a VLAN.

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

| <input type="checkbox"/> | IP Address [?] | Subnet Ma... [?] | VLAN ID [?] | Remarks | DHCP Serv... [?] | Start IP Address [?] | IP Count [?] | Lease Time (Min) [?] | Action |
|-------------------------------------|-------------------------|---------------------------|----------------------|---------|---------------------------|-------------------------------|-----------------------|-------------------------------|---|
| <input checked="" type="checkbox"/> | 192.168.2.1 | 255.255.255.0 | Default VLAN | - | Enabled | 192.168.2.1 | 254 | 8 | Edit Delete |
| <input type="checkbox"/> | 5.5.5.5 | 255.255.255.0 | 55 | - | Enabled | 5.5.5.1 | 254 | 30 | Edit Delete |

Up to 8 entries can be added.

Add



* IP Address

* Subnet Mask

* VLAN ID

Remarks

MAC Address

DHCP Server

* Start IP Address

* IP Count

* Lease Time (Min)

DNS Server - [?]

Cancel

OK

Table 4-7 VLAN configuration

| Parameter | Description |
|-------------|--|
| IP Address | Configure an IP address for the VLAN interface. This IP address is used as the default gateway for the LAN devices that need to access the Internet. |
| Subnet Mask | Configure an IP address subnet mask for the VLAN interface. |
| VLAN ID | Configure the VLAN ID. |
| Remark | Enter the VLAN description. |
| MAC Address | Configure an MAC address for the VLAN interface. |
| DHCP Server | Enable the DHCP server function. After this function is enabled, devices in the LAN can automatically obtain IP addresses. You also need to specify the start address for IP address allocation by the DHCP server, the number of IP addresses that can be allocated, and the address lease. You can also configure DHCP Options. For details, see Section 4.10.3 Configuring the DHCP . |

Caution

The VLAN configuration is associated with the uplink configuration. Exercise caution when you perform this operation.

4.5.3 Configuring a Port VLAN

Choose **One-Device > Gateway > Config > Network > Port VLAN**.

This page displays the VLAN division of the current port. Create VLANs on the **LAN Settings** page and then configure the port based on the VLANs on this page. For details, see Section [4.5.2 Creating a VLAN](#).

Click the check box under a port and select the relationship between VLAN and port from the drop-down list box.

i Please choose [LAN Settings](#) to create a VLAN first and configure port settings based on the VLAN.

Connected
 Disconnected

AG

AG

LAN0

LAN1

LAN2

LAN3

LAN4/WAN3

LAN5/WAN2

| | | | | | | | | |
|--------------|----------|-----------|----------|----------|-----------|-----------|-----------|-----------|
| Default VLAN | Untagged | Untagged | Untagged | Untagged | Non-addec | Non-addec | Non-addec | Non-addec |
| VLAN 55 | Tagged | Non-added | Tagged | Tagged | Tagged | Tagged | Tagged | Non-addec |

Tagged
Untagged

- **Untagged:** Configure the VLAN as the native VLAN of the port. When the port receives packets from the

specified VLAN, the port removes the VLAN ID before forwarding the packets. When the port receives packets without a VLAN ID, the port adds this VLAN ID to the packets before forwarding them. You can set only one VLAN of the port to **Untagged**.

- **Tagged:** Configure the port to allow packets with this VLAN ID to pass. This VLAN is not the native VLAN. When the port receives packets from the specified VLAN, it forwards the packets with the original VLAN ID.
- **Non-added:** Configure the port to deny packets with this VLAN ID to pass. For example, if you set VLAN 10 and VLAN 20 to **Non-added** for port 2, port 2 will not receive packets from VLAN 10 and VLAN 20.

4.6 Configuring Repeater Mode

4.6.1 Wired Repeater

Choose **Local Device** > **Basics** > **Repeater Mode**.

Connect a network cable from the WAN port (uplink LAN port) of the device to the upper-layer device.

Select **Access Point**, click **Check**, confirm the Wi-Fi settings of the AP, and then click **Save** to expand the network coverage.

Caution

After the configuration is saved, connected clients will be disconnected from the network for a short period of time. You can reconnect the clients to the Wi-Fi network for restoration.

The device is working in **Router** mode.

Router
 Access Point
 Wireless Repeater



This mode allows you to establish a wired connection between a primary router and a secondary router, extending network coverage.
Cable Connection: Please connect the WAN port of the local router to the LAN port of the primary router.

Wired Repeater

Check

4.6.2 Wireless Repeater

The wireless repeater mode extends the Wi-Fi coverage range of the primary device. The device supports the dual-link wireless repeater mode and can extend both 2.4 GHz and 5 GHz signals of the primary device.



Note

To avoid loops in wireless repeater mode, remove the network cable from the WAN port.

Obtain the SSID and Wi-Fi password of the upper-layer router.

Choose **One-Device** > **Gateway** > **Config** > **Network** > **Repeater Mode**.

- Click **Wireless Repeater** and then click **Select**. A list of surrounding Wi-Fi signals pops up. A list of nearby 5 GHz Wi-Fi networks is displayed by default. You can switch from 5 GHz to 2.4 GHz band by selecting **2.4G** from the drop-down list box. You are advised to select a strong 5 GHz Wi-Fi network signal.

The device is working in **Access Point** mode.

Router
 Access Point
 Wireless Repeater

- This mode allows you to establish a wireless connection between a primary device and a secondary device, extending network coverage.
- The local device will work as a secondary device.
- It is recommended to select a 5G Wi-Fi of the primary device.

To avoid loops, wireless repeater is not allowed to be configured.

Wireless Repeater

Primary Device

* SSID

×

5G Wi-Fi List Select a target Wi-Fi.

| SSID | BSSSID | Security | Channel | RSSI |
|-------------------|-------------------|----------|---------|-----------------|
| damo | ec:b9:70:68:3b:86 | OPEN | 161 | -18 dBm High |
| HUAWEI-11111111 | 4c:50:77:42:61:58 | WPA2PSK | 36 | -34 dBm High |
| @ew1800 | c6:70:ab:8c:bf:b5 | OPEN | 36 | -34 dBm High |
| HUAWEI-11111111 | 4c:50:77:42:61:5e | WPA2PSK | 149 | -36 dBm High |
| @Ruijie-ew1800_5G | 82:05:88:90:20:12 | OPEN | 64 | -37 dBm High |

- Select the Wi-Fi signal of the primary router that you want to extend. The configuration items of the local device are displayed. If the signal of the upper-layer device is encrypted, enter the Wi-Fi password of the upper-layer device.
- Configure **Local Router Wi-Fi**. You can select **New Wi-Fi** or **Same as Primary Router Wi-Fi**.
 - If you select **Same as Primary Router Wi-Fi**, the Wi-Fi settings of the router are automatically synchronized with those on the primary router. Generally, clients merge Wi-Fi signals with the same name into one Wi-Fi signal, and they can search out only the Wi-Fi signal of the primary router.

- o If **New Wi-Fi** is selected, you can set a local SSID and password. Clients will search out different Wi-Fi signals.

The device is working in **Access Point** mode.

Router
 Access Point
 Wireless Repeater

i

- This mode allows you to establish a wireless connection between a primary device and a secondary device, extending network coverage.
- The local device will work as a secondary device.
- It is recommended to select a 5G Wi-Fi of the primary device.

To avoid loops, wireless repeater is not allowed to be configured.

Wireless Repeater

Primary Device

* SSID @ew1800

Local Device

Local Router Wi-Fi **New Wi-Fi** Same as Primary Router Wi-Fi

* SSID(2.4G)

* SSID(5G)

Wi-Fi Password

⚠ Caution

After the configuration is saved, the AP will be disconnected from the Wi-Fi network and needs to connect to the new Wi-Fi network. Exercise caution when performing this operation. Record the new SSID and password.

You are advised to install the AP in a position where the RSSI is greater than two bars of signal to prevent signal loss. If the signal at the installation position is too weak, the Wi-Fi extension may fail or the quality of the extended signal may be poor.

4.7 Configuring WISP

The WISP feature enables users to utilize the WAN port of the router for wireless access, empowering them to easily create their own wireless network and offer wireless Internet service in various public venues like cafes, hotels, airports, restaurants, and more.

Choose **One-Device > Gateway > Config > Network > WISP**.

- (1) Click **WISP**, choose the Internet connection type (DHCP, PPPoE, or static IP) from the **Internet** drop-down menu, and click **Next**.

The device is working in **Router** mode.

Router
 Access Point
 Wireless Repeater
 WISP

- WISP configures the WAN port of router to wireless access. Please first select the access type (DHCP, PPPoE or Static IP), and
- WISP allows users to establish their own WLAN for Internet access in public spaces, including coffee, hotel, airport or resta

WAN

* Internet

Username and password are not required.

Next

- Click the **Select** button next to **SSID** and choose the Wi-Fi network of the primary router. If the Wi-Fi network of the primary router is encrypted, enter the Wi-Fi password for the selected Wi-Fi network.

Wireless Repeater

Primary Router

* SSID

5G Wi-Fi List **Select a target Wi-Fi.**

| SSID | BSSID | Security | Channe l | RSSI | MLO |
|-----------|-----------------------|----------|-------------|-------------------|---------------|
| 213213213 | 02:d0:32:a0:05:12 | OPEN | 56 | -62 dBm Medium | Not supported |
| 213213213 | 02:d0:f8:a5:10:02 | OPEN | 56 | -67 dBm Medium | Not supported |
| 213213213 | 02:e0:32:a0:02:55 | OPEN | 60 | -58 dBm High | Not supported |
| 1 | 10:82:3d:34:48:7 d | WPA2PSK | 60 | -61 dBm Medium | Not supported |
| 1 | 56:16:51:86:3b:0e | OPEN | 64 | -84 dBm Low | Not |

- Configure the Wi-Fi network for the local router. You can choose **New Wi-Fi** or **Same as Primary Router Wi-Fi**.

Wireless Repeater

— **Primary Router** _____

* SSID @@@s58vlan130

— **Local Router** _____

Local Router Wi-Fi **New Wi-Fi** Same as Primary Router Wi-Fi

* SSID(2.4G) @@@s58vlan130_plus

* SSID(5G) @@@s58vlan130_plus_5G

Wi-Fi Password

4.8 Configuring DNS

4.8.1 Local DNS

When the WAN interface runs DHCP or PPPoE protocol, the device automatically obtains the DNS server address. If the upper-layer device does not deliver the DNS server address or the DNS server needs to be changed, you can manually configure a new DNS server.

Choose **One-Device > Gateway > Config > Advanced > DNS > Local DNS**.

Local DNS server: Configure the DNS server address used by the local device. If multiple addresses exist, separate them with spaces.

 The device will get the DNS server address from the uplink device.

Local DNS server

4.8.2 DNS Policy

Choose **One-Device > Gateway > Config > Advanced > DNS > DNS Policy**.

1. Static Domain Name Resolution

By configuring a DNS policy, you can resolve a specified domain name to the corresponding IP address, without relying on an external DNS server to perform domain name resolution. This can accelerate domain name resolution and mitigate security risks such as DNS hijacking.

(1) In the **Static Domain Resolution** section, click **+Add**.

The screenshot shows the 'Static Domain Resolution' section. At the top right, there is a search box labeled 'Search by Domain Name' and a blue '+ Add' button, which is highlighted with a red rectangle. To its right is a 'Delete Selected' button. Below this is a table with the following columns: Domain Name, IP Address, Remarks, Status, and Action. One entry is visible with 'getRealIndex' as the domain name and '[IPv4] 1.1.1.1' as the IP address. The status is 'Enable'. At the bottom right, there is a pagination control showing 'Total 1' and '10/page'.

(2) In the pop-up window that is displayed, enter the domain name and IP address.

The screenshot shows a pop-up window titled 'Add' with a close button (X) in the top right corner. It contains several input fields: a required 'Domain Name' field with a question mark icon, an 'IP Address' field with a plus sign, an 'IPv6 Address' field with a plus sign, and an 'Remarks' field with the placeholder text 'Optional'. Below these fields is an 'Enable' toggle switch that is currently turned on. At the bottom right, there are 'Cancel' and 'OK' buttons.

(3) Toggle on **Enable**, and click **OK**.

2. Dynamic Domain Name Resolution

After a DNS server is configured, the specified interface uses the configured DNS server to resolve domain names.

In the **Dynamic Domain Resolution** section, click **+Add**. In the pop-up window that is displayed, enter the domain name, and select the interface. Enter the DNS server IP address and remarks if necessary, toggle on **Enable**, and click **OK**.

Caution

If an intranet server is configured for resolving specific domains, you are advised to not use the local gateway as the DNS server to prevent potential problems like recursive queries or other domain resolution issues.

The screenshot shows the 'Dynamic Domain Resolution' section. At the top right, there is a search box labeled 'Search by Domain Name' and a blue '+ Add' button, which is highlighted with a red rectangle. To its right is a 'Delete Selected' button. Below this is a light blue informational banner with the text: 'If an intranet server is configured for resolving specific domains, you are advised to not use the local gateway as the DNS server to prevent potential problems like recursive queries or other domain resolution issues.' Below the banner is a table with the following columns: Domain Name, Interface, Server IP, Remarks, Status, and Action. The table is currently empty, showing 'No Data'. At the bottom right, there is a pagination control showing 'Total 0' and '10/page'.

Add
×

* Domain Name ?

Interface ?

Server IP +

Server IPv6 +

Remarks

Enable

4.8.3 DNS Proxy

DNS proxy is optional configuration. By default, the device obtains the DNS server address from the upper-layer device.

Choose **One-Device > Gateway > Config > Advanced > DNS > DNS Proxy**.

DNS Proxy: By default, the DNS proxy is disabled, and the DNS address delivered by the ISP is used. If the DNS configuration is incorrect, the device may fail to parse domain names and network access will fail. It is recommended to keep the DNS proxy disabled.

DNS Server: Enable clients to access the Internet by using the DNS server address delivered by the upper-layer device. The default settings are recommended. After the DNS proxy is enabled, you need to enter the DNS server IP address. The DNS settings vary with the region. Consult the local ISP for details.

Enable ?

* DNS Server ?

4.9 Configuring IPv6

4.9.1 IPv6 Overview

Internet Protocol Version 6 (IPv6) is the next-generation IP protocol designed by Internet Engineering Task Force (IETF) to substitute IPv4. It is used to compensate insufficient IPv4 network addresses.

4.9.2 IPv6 Basics

1. IPv6 Address Format

IPv6 extends 32-bit IPv4 address into 128 bits, providing wider address space than IPv4.

The basic format of an IPv6 address is X:X:X:X:X:X:X. It is represented as eight groups of four hexadecimal digits (0-9, A-F), each group representing 16 bits. The groups are separated by colons (:). In this format, each X represents a group of four hexadecimal digits.

Samples of IPv6 addresses are 2001:ABCD:1234:5678:AAAA:BBBB:1200:2100, 800:0:0:0:0:0:0:1, and 1080:0:0:0:8:800:200C:417A.

The digit 0 in an IPv6 address can be suppressed as follows:

- Leading zeros in each 16-bit field are suppressed. For example, 2001:00CD:0034:0078:000A:000B:1200:2100 can be suppressed to 2001:CD:34:78:A:B:1200:2100.
- The long sequence of consecutive all-zero fields in some IPv6 addresses can be replaced with two colons (::). For example, 800:0:0:0:0:0:0:1 can be represented as 800::1. The two colons (::) can be used only when all the 16 bits in a group are 0s, and it can appear only once in an IPv6 address.

2. IPv6 Prefix

IPv6 addresses are typically composed of two logical parts:

- Network prefix: n bits, corresponding to the network ID in IPv4 addresses
- interface ID: $(128 - n)$ bits, corresponding to the host ID in IPv4 addresses

A slash (/) is used to separate the length of network prefix from an IPv6 address. For example, 12AB::CD30:0:0:0:0/60 indicates that the 60-bit network prefix in the address is used for route selection. IPv6 prefixes can be obtained from the IPv6 DHCP server, along with IPv6 addresses. A downlink DHCP server can also automatically obtain IPv6 prefixes from its uplink DHCP server.

3. Special IPv6 Addresses

There are some special IPv6 addresses:

fe80::/8: loopback address, similar to the IPv4 address 169.254.0.0/16

fc00::/7: local address, similar to IPv4 addresses 10.0.0.0/8, 172.16.0.0/16, and 192.168.0.0/16

ff00::/12: multicast address, similar to the IPv4 address 224.0.0.0/8

4. NAT66

IPv6-to-IPv6 Network Address Translation (NAT66) is a process of converting the IPv6 address in the IPv6 data packet header into another IPv6 address. NAT66 can be implemented by converting the prefix in an IPv6 address in an IPv6 data packet header into another IPv6 address prefix. NAT66 enables mutual access between an internal network and an external public network.

4.9.3 IPv6 Address Allocation Modes

- Manual configuration: IPv6 addresses, prefixes, and other network parameters are configured manually.
- Stateless Address Autoconfiguration (SLAAC): The link-local address is generated based on the interface ID, and the IPv6 address is automatically allocated based on the prefix information in the Router Advertisement

(RA) packet.

- Stateful address allocation (DHCPv6): Two DHCPv6 allocation methods are as follows:
 - Automatic DHCPv6 allocation: The DHCPv6 server automatically allocates IPv6 addresses, prefixes, and other network parameters.
 - Automatic allocation of DHCPv6 Prefix Delegations (PDs): The lower-layer network device submits a prefix allocation application to the upper-layer network device. The upper-layer network device allocates an appropriate address prefix to the lower-layer device. The lower-layer device further divides the obtained prefix (usually less than 64 bits) into 64-bit prefixed subnet segments and advertises the address prefixes to the user link directly connected to the IPv6 host through the RA packet, implementing automatic address configuration for hosts.

4.9.4 Enabling the IPv6 Function

Choose **One-Device > Gateway > Config > Network > IPv6 Address**.

Turn on **Enable** to enable the IPv6 function.

Enable  

4.9.5 Configuring an IPv6 Address for the WAN Port

Choose **One-Device > Gateway > Config > Network > IPv6 Address > WAN Settings**.

Caution

- When IPv6 is enabled, the MTU of the IPv4 WAN port must be greater than 1280.
 - If NAT66 is disabled, a public IPv6 address can access clients using the public IPv6 address on the intranet.
-

After you enable the IPv6 function, you can set related parameters on the **WAN Settings** tab. The number of **WAN** tabs indicates the number of WAN ports on the current device.

[WAN Settings](#) LAN Settings DHCPv6 Clients Static DHCPv6

WAN0 WAN1

* Internet DHCP/PPPoE

IPv6 Address

IPv6 Prefix

Gateway

DNS Server

NAT66 ?

[Advanced Settings](#)

Save

Table 4-8 IPv6 address configuration for WAN port

| Parameter | Description |
|--------------|---|
| Internet | Configure a method for the WAN port to obtain an IPv6 address. <ul style="list-style-type: none"> ● DHCP/PPPoE: The current device functions as the DHCPv6 client, and it applies for an IPv6 address and prefix from the uplink network device. ● Static IP: You need to manually configure a static IPv6 address, gateway address, and DNS server. ● Null: The IPv6 function is disabled on the WAN port. |
| IPv6 Address | When Internet is set to DHCP/PPPoE , the automatically obtained IPv6 address is displayed. When Internet is set to Static IP , you need to configure this parameter manually. |
| IPv6 Prefix | When Internet is set to DHCP/PPPoE , the IPv6 address prefix automatically obtained by the current device is displayed. |
| Gateway | When Internet is set to DHCP/PPPoE , the automatically obtained gateway address is displayed. When Internet is set to Static IP , you need to configure this parameter manually. |
| DNS Server | When Internet is set to DHCP/PPPoE , the automatically obtained DNS server address is displayed. When Internet is set to Static IP , you need to configure this parameter manually. |

| Parameter | Description |
|--------------------|---|
| NAT66 | If the current device cannot access the Internet through DHCP/PPPoE or cannot obtain the IPv6 prefix, you need to enable the NAT66 function to allocate IPv6 addresses to clients on the internal network. |
| Default Preference | Set the default route preference for the current line. A smaller value indicates a higher preference. For the same destination address, the route with the highest preference is selected as the optimal route. |

4.9.6 Configuring an IPv6 Address for the LAN Port

Choose **One-Device > Gateway > Config > Network > IPv6 Address > LAN Settings**.

When the device accesses the Internet through DHCP, it can obtain LAN port IPv6 addresses from the uplink device and allocate IPv6 addresses to the clients in the LAN based on the IPv6 address prefix. If the uplink device cannot allocate an IPv6 address prefix to the device, you need to manually configure an IPv6 address prefix for the LAN port and enable the NAT66 function to allocate IPv6 addresses to the clients in the LAN. For details, see Section [4.9.5 Configuring an IPv6 Address for the WAN Port](#).

Click **Add** and configure a rule for assigning IPv6 addresses to clients in the VLAN.

LAN Settings ⓘ + Add Delete Selected

| <input type="checkbox"/> | VLAN ID | IPv6 Assignment | Subnet Prefix Name | Subnet ID | Subnet Prefix Length | IPv6 Address/Prefix Length | Action |
|--------------------------|---------|-----------------|--------------------|-----------|----------------------|----------------------------|--------|
| No Data | | | | | | | |

Up to 64 entries can be added.

Add
×

* VLAN ID

IPv6 Assignment

IPv6 Address/Prefix Length

----- Advanced Settings -----

Subnet Prefix Name

* Subnet Prefix Length

* Subnet ID

* Lease Time (Min)

DNS Server

Table 4-9 IPv6 address configuration for LAN port

| Parameter | Description |
|----------------------------|---|
| VLAN ID | Configure a VLAN to which the rule applies. You can click the drop-down list box and select an existing VLAN. For details about how to create a VLAN, see Section 4.5 Configuring VLAN . |
| IPv6 Assignment | <p>You can use either of the following methods to allocate IPv6 addresses to clients:</p> <ul style="list-style-type: none"> ● Auto: Allocate IPv6 addresses to clients in DHCPv6 or SLAAC mode. ● DHCPv6: Allocate IPv6 addresses to clients through DHCPv6. ● SLAAC: Allocate IPv6 addresses to clients through SLAAC. ● Null: Do not allocate addresses to clients. <p>You should select an allocation method based on the protocol supported by clients on the internal network. If you are not sure about the supported protocol, select Auto.</p> |
| IPv6 Address/Prefix Length | Configure the IPv6 address and length for the VLAN. If the address length ranges from 48 to 64 bits, the address will also be used as the IPv6 address prefix. |

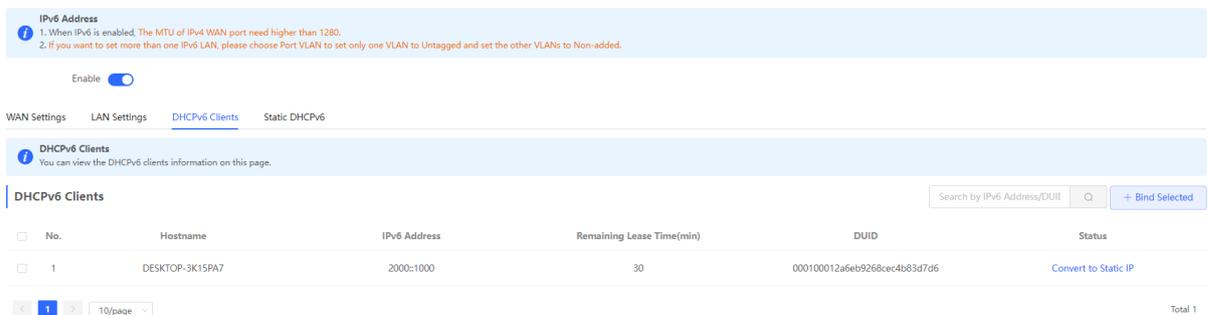
| Parameter | Description |
|----------------------|--|
| Subnet Prefix Name | Configure the interface from which the prefix is obtained, for example, WAN_V6. The default value is all interfaces. If Disable is selected, the IPv6 Address/Prefix Length field must be configured to assign IP addresses to hosts on the LAN. |
| Subnet Prefix Length | Specify the length of the subnet prefix. The value is in the range of 48 to 64. |
| Subnet ID | Configure the subnet ID in the hexadecimal format. The value 0 indicates auto increment. |
| Lease Time(Min) | Set the lease of the IPv6 address, in minutes. |
| DNS Server | Configure the IPv6 DNS server address. |

4.9.7 Viewing the DHCPv6 Client

Choose **One-Device > Gateway > Config > Network > IPv6 Address > DHCPv6 Clients**.

When the device functions as a DHCPv6 server to allocate IPv6 addresses to clients, you can view the information about the client that obtains an IPv6 address from the device on the current page. The client information includes the host name, IPv6 address, remaining lease time, and DHCPv6 Unique Identifier (DUID).

Enter the DUID in the search bar and click  to quickly find relative information of the specified DHCPv6 client.



IPv6 Address
 1. When IPv6 is enabled, The MTU of IPv4 WAN port need higher than 1280.
 2. If you want to set more than one IPv6 LAN, please choose Port VLAN to set only one VLAN to Untagged and set the other VLANs to Non-added.

Enable

WAN Settings LAN Settings **DHCPv6 Clients** Static DHCPv6

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

DHCPv6 Clients

| No. | Hostname | IPv6 Address | Remaining Lease Time(min) | DUID | Status |
|----------------------------|-----------------|--------------|---------------------------|------------------------------|--------------------------------------|
| <input type="checkbox"/> 1 | DESKTOP-3K15PA7 | 2000:1000 | 30 | 000100012a6eb9268cec4b83d7d6 | Convert to Static IP |

1 / 10/page Total 1

4.9.8 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 **One-Device > Gateway > Config > Network > IPv6 Address > Static DHCPv6**.

Static IP Address List Search by IPv6 Address/DUID Q [+ Add](#) [Delete Selected](#)

| <input type="checkbox"/> | No. | IPv6 Address | DUID | Action |
|--------------------------|-----|--------------|------|--------|
| No Data | | | | |

Up to 200 entries can be added. Total 0 < 1 > 10/page v

(1) Click **Add**.

Add
×

* IPv6 Address

* DUID

Cancel
OK

(2) Enter the IPv6 address and DUID.

(3) Click **OK**.

4.9.9 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 **One-Device > Gateway > Config > Security > IPv6 Neighbor List**.

IPv6 Neighbor List Search by IP Address/MAC Addr Q [+ Add](#) [Bind Selected](#) [Delete Selected](#)

| <input type="checkbox"/> | No. | IPv6 Address | MAC Address | Type | Ethernet status | Action |
|--------------------------|-----|---------------------------|-------------|---------|-----------------|----------------------|
| <input type="checkbox"/> | 1 | fe80::139:bf7:aa4f:dcc1 | 7C:.....ic | Dynamic | WAN | Bind |
| <input type="checkbox"/> | 2 | fe80::79e8:e7c0:9949:45a2 | 3:.....1 | Dynamic | WAN | Bind |
| <input type="checkbox"/> | 3 | fe80::1c92:b8af:ceaa:e921 | 7C:.....f | Dynamic | WAN | Bind |
| <input type="checkbox"/> | 4 | fe80::dc82:d321:7d3b:94f7 | 3C:.....lf | Dynamic | WAN | Bind |
| <input type="checkbox"/> | 5 | fe80::2941:1186:1ee4:563e | 7:.....01 | Dynamic | WAN | Bind |

(1) Click **Add** and manually add the interface, IPv6 address and MAC address of the neighbor.

×

Add

* Interface Select ▼

* IPv6 Address Please enter an IPv6 address.

* MAC Address Please enter a MAC address.

Cancel
OK

- (2) Select the MAC address and IP address to be bound, and click **Bind** in the **Action** column to bind the IP address to the MAC address to prevent ND attacks.

IPv6 Neighbor List

+ Add
 Bind Selected
Delete Selected

| <input type="checkbox"/> | No. | IPv6 Address | MAC Address | Type | Ethernet status | Action |
|--------------------------|-----|---------------------------|-------------|---------|-----------------|--------|
| <input type="checkbox"/> | 1 | fe80::139:bfb7:aa4f:dcc1 | 7C:.....:lc | Dynamic | WAN | Bind |
| <input type="checkbox"/> | 2 | fe80::79e8:e7c0:9949:45a2 | 3C:.....:01 | Dynamic | WAN | Bind |

4.10 Configuring a DHCP Server

4.10.1 DHCP Server Overview

After the DHCP server function is enabled in the LAN, the device can automatically deliver IP addresses to clients, so that clients connected to the LAN ports of the device or connected to Wi-Fi can access the Internet using the obtained addresses.

See Section [4.9.6 Configuring an IPv6 Address for the LAN Port](#) for more information about the DHCPv6 server function.

4.10.2 Address Allocation Mechanism

The DHCP server allocates an IP address to a client in the following way:

- (1) When the device receives an IP address request from a DHCP client, the device searches the DHCP static address allocation list. If the MAC address of the DHCP client is in the DHCP static address allocation list, the device allocates the corresponding IP address to the DHCP client.

- (2) If the MAC address of the DHCP client is not in the DHCP static address allocation list or the IP address that the DHCP client applies is not in the same network segment as the LAN port IP address, the device selects an IP address not used from the address pool and allocates the address to the DHCP client.
- (3) If no IP address in the address pool is allocable, the client will fail to obtain an IP address.

4.10.3 Configuring the DHCP Server

1. Configuring Basic Parameters

Choose **One-Device > Gateway > Config > Network > LAN > LAN Settings**.

Select the VLAN to which the DHCP function needs to be configured and click **Edit**.

LAN Settings + Add Delete Selected

| <input type="checkbox"/> | IP Address <small>?</small> | Subnet Ma... <small>?</small> | VLAN ID <small>?</small> | Remarks | DHCP Serv... <small>?</small> | Start IP Address <small>?</small> | IP Count <small>?</small> | Lease Time (Min) <small>?</small> | Action |
|--------------------------|-----------------------------|-------------------------------|--------------------------|---------|-------------------------------|-----------------------------------|---------------------------|-----------------------------------|--|
| <input type="checkbox"/> | 192.168.2.1 | 255.255.255.0 | Default VLAN | - | Enabled | 192.168.2.1 | 254 | 8 | Edit Delete |
| <input type="checkbox"/> | 5.5.5.5 | 255.255.255.0 | 55 | - | Enabled | 5.5.5.1 | 254 | 30 | Edit Delete |

Up to 8 entries can be added.

Edit ×

* IP Address

* Subnet Mask

Remarks

MAC Address

DHCP Server

* Start IP Address

* IP Count

* Lease Time (Min)

DNS Server 192.168.2.1 ?

DHCP Server: The DHCP server function is enabled by default in the router mode. You are advised to enable the function if the device is used as the sole router in the network. When multiple routers are connected to the upper-layer device through LAN ports, disable this function.

⚠ Caution

If the DHCP server function is disabled on all devices in the network, clients cannot automatically obtain IP addresses. You need to enable the DHCP server function on one device or manually configure a static IP address for each client for Internet access.

Start IP Address: Enter 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: Enter the number of IP addresses in the address pool.

Lease Time (Min): Enter the address lease term. When a 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 client connection is restored, the client can request an IP address again. The default lease term is 30 minutes.

2. Configuring DHCP Option

Choose **One-Device > Gateway > Config > Network > LAN > DHCP**.

The DHCP Option configuration is shared by all LAN ports. You can configure DHCP Option based on actual needs.

DNS Server ?

Option 43 ? i

Option 138 ?

Option 150 ?

Gateway

Domain Name

Save

Table 4-10 DHCP Option configuration

| Parameter | Description |
|------------|---|
| DNS Server | Enter the DNS server address provided by the ISP. |

| Parameter | Description |
|-------------|--|
| 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. The TFTP server allocates addresses to clients. |
| Gateway | Configure the IP address of the default gateway or default route that the DHCP server assigns to clients. The default gateway is the next hop address used by a client to send data packets to an external network. It is responsible for forwarding the data packets to the target network. |
| Domain Name | When deploying a server on the internal network, you can set a domain name to allow intranet clients to access the server. After the configuration is completed, intranet clients can access the server by using the host name and domain name, thereby avoiding access failure due to changes in the server's IP address. |

4.10.4 Viewing the DHCP Client

Choose **One-Device > Gateway > Config > Network > LAN > DHCP Clients**.

View the client addresses automatically allocated by thorough DHCP. Find the target client and click **Convert to Static IP** in the **Status** column, or select desired clients and click **Batch Add**. 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 Section [4.10.5 Configuring Static IP Addresses](#).

DHCP Clients

| <input type="checkbox"/> | No. | Device Name | IP Address | MAC Address | Remaining Lease Time(min) | Status |
|--------------------------|-----|-----------------------------------|-------------|-------------------|---------------------------|--------------------------------------|
| <input type="checkbox"/> | 1 | DESKTOP-PJE70H1 ℹ | 192.168.2.2 | f8-01-11-11-11-11 | 6 | Convert to Static IP |

Up to 500 static binding entries are supported. Total 1 < 1 > 10/page v

4.10.5 Configuring Static IP Addresses

Choose **One-Device > Gateway > Config > Network > LAN Static IP Addresses**.

The page displays all configured static IP addresses.

Click **Add**. In the pop-up window, 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 client connects to the network.

Static IP Address List

Batch Import Batch Export **+ Add** Delete Selected Search by IP Address/MAC Addr Q

| No. | Device Name | IP Address | MAC Address | Action |
|-----|--------------------------------|-------------|-------------|-------------|
| 1 | Xiaomi10s111 🔗 | 192.168.2.8 | 86:_____b | Edit Delete |

Up to 500 entries can be added. Total 1 < 1 > 10/page

Add ×

Device Name

* IP Address

* MAC Address

Cancel OK

Click **Batch Export** to export all existing static IP addresses.

Click **Batch Import** to import static IP addresses in the file to the device. The entries with the same MAC address as those in the list will be overwritten by the configurations in the file, and the other configurations in the list will not be changed. The other configurations in the file will be added to the list in the form of new entries.

Preview of Configuration ×

- 1. When the existing configuration has the same MAC address or IP address as the uploaded data, the existing configuration will be changed.
- 2. The uploaded data has the same MAC address or IP address, and the data configured later will be imported.
- 3. Configurations that do not meet the validation rules will not be imported.

| Username | MAC Address | IP Address | Is It Possible to Import |
|----------|-------------|-----------------|--------------------------|
| 0 | a | 192.168.110.249 | Passed |
| 5 | 0 | 192.168.110.220 | Passed |
| 0 | a | 192.168.110.61 | Passed |
| c | 4 | 192.168.110.77 | Passed |
| 8 | 8 | 192.168.110.29 | Passed |
| 3 | 6 | 192.168.110.14 | Passed |
| c | c | 192.168.110.178 | Passed |
| c | 3 | 192.168.110.232 | Passed |
| e | 2 | 192.168.110.165 | Passed |
| c | 7 | 192.168.110.102 | Passed |

Total 30 < 1 2 3 > 10/page

Cancel **OK**

4.11 Configuring Routes

4.11.1 PBR

1. Overview

Policy-based routing (PBR) is a mechanism for routing and forwarding based on user-specified policies. When a router forwards data packets, it filters the packets according to the configured rules, and then forwards the matched packets according to the specified forwarding policy. The PBR feature enables the device to formulate rules according to specific fields (source or destination IP address and protocol type) in the data packets, and forward the data packets from a specific interface.

In a multi-line scenario, if the device is connected to the Internet and the internal network through different lines, the traffic will be evenly routed over the lines if no routing settings are available. In this case, access data to the internal network may be sent to the external network, or access data to the external network may be sent to the internal network, resulting in network exceptions. To prevent these exceptions, you need to configure PBR to control data isolation and forwarding on the internal and external networks.

The device can forward data packets using either of the following three policies: PBR, address-based routing, and static routing. When all the policies exist, PBR, static routing, and address-based routing have descending order in priority. For details on address-based routing, see Section [4.3.7 Configuring the Multi-Line Load Balancing Mode](#).

2. Configuring IPv4 PBR

Choose **One-Device > Gateway > Config > Advanced > Routing > PBR**.

Click **Add** to add a PBR rule.

Route Priority: PBR > > URL > Static Routing > ISP Routing.

PBR List ⊕ + Add 🗑️ Delete Selected

| <input type="checkbox"/> | Name ⊕ | Protocol Type ? | Src IP Address ? | Dest IP Address ? | Src Port Range ? | Dest Port Range ? | Outbound Interface ? | Traffic Assurance | Effective State | Action |
|--------------------------|---------------------|------------------------------|-------------------------------|--------------------------------|-------------------------------|--------------------------------|-----------------------------------|-------------------|-----------------|--------|
| No Data | | | | | | | | | | |

Up to 30 entries can be added. Total 0 < 1 > 10/page

Add PBR ×

* Name ?

Protocol Type ?

Src IP/IP Range ?

Dest IP/IP Range ?

Outbound Interface ?

Traffic Assurance ?

Effective State

Table 4-11 PBR configuration

| Parameter | Description |
|-----------------|---|
| Name | Specify the name of the PBR rule, which uniquely identifies a PBR rule. The name must be unique for each rule. |
| Protocol Type | Specify the protocol to which the PBR rule is effective. You can set this parameter to IP , ICMP , UDP , TCP , or Custom . |
| Protocol Number | When Protocol Type is set to Custom , you need to enter the protocol number. |

| Parameter | Description |
|--------------------|--|
| Src IP/IP Range | Configure the source IP address or IP address range for matching PBR entries. The default value is All IP Addresses. <ul style="list-style-type: none"> ● All IP Addresses: Match all the source IP addresses. ● Custom: Match the source IP addresses in the specified IP range. |
| Custom Src IP | When Src IP/IP Range is set to Custom , you need to enter a single source IP address or a source IP range. |
| Dest IP/IP Range | Configure the destination IP address or IP address range for matching PBR entries. The default value is All IP Addresses. <ul style="list-style-type: none"> ● All IP Addresses: Match all the destination IP addresses. ● Custom: Match the destination IP addresses in the specified IP range. |
| Custom Dest IP | When Dest IP/IP Range is set to Custom, you need to enter a destination source IP address or a destination IP range. |
| Src Port Range | This parameter is available only when Protocol Type is set to TCP or UDP. This parameter specifies the source port range for packet matching using PBR. |
| Dest Port Range | This parameter is available only when Protocol Type is set to TCP or UDP. This parameter specifies the destination port range for packet matching using PBR. |
| Outbound Interface | Specify the interface that forwards the data packet based on the hit PBR rule. |
| Traffic Assurance | When an outbound interface is unreachable, the traffic will be automatically routed to other reachable outbound interfaces. |
| Effective State | Turn on Effective State to specify whether to enable the PBR rule. If Effective State is turned off, this rule does not take effect. |

 **Note**

If you want to restrict the access device to access only the specified internal network, you can set the outbound interface in the corresponding route to the WAN port in the private line network. For details on how to set the private line network, see Section [4.3.4 Configuring the Private Line](#).

All the created PBR policies are displayed in the PBR list, with the latest policy listed on the top. The device matches the policies according to their sorting in the list. You can manually adjust the policy matching sequence by clicking  or  in the **Match Order** column.

PBR List ? + Add Delete Selected

| <input type="checkbox"/> | Name ? | Protocol Type ? | Src IP Address ? | Dest IP Address ? | Src Port Range ? | Dest Port Range ? | Outbound Interface ? | Traffic Assurance | Effective State ? | Match Order ? | Action |
|--------------------------|---------------------|------------------------------|-------------------------------|--------------------------------|-------------------------------|--------------------------------|-----------------------------------|-------------------|--------------------------------|----------------------------|----------------|
| <input type="checkbox"/> | test2 | IP | 1.1.1.1 | 2.2.2.2 | - | - | WAN0 | Enable | Enable ? | ↓ | Edit Delete |
| <input type="checkbox"/> | test1 | IP | All IP Addresses | All IP Addresses | - | - | WAN0 | Enable | Enable ? | ↑ | Edit Delete |

Up to 30 entries can be added. Total 2 < 1 > 10/page

3. Configuring IPv6 PBR

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **IPv6 PBR**.

PBR List ? + Add Delete Selected

| <input type="checkbox"/> | Name ? | Protocol Type ? | Src IP Address | Dest IP Address | Src Port Range ? | Dest Port Range ? | Outbound Interface ? | Traffic Assurance | Effective State | Action |
|--------------------------|---------------------|------------------------------|----------------|-----------------|-------------------------------|--------------------------------|-----------------------------------|-------------------|-----------------|--------|
| No Data | | | | | | | | | | |

Up to 30 entries can be added. Total 0 < 1 > 10/page

Click **Add** to add a PBR rule.

Add PBR

* Name ?

Protocol Type ?

Src IP/IP Range ?

Dest IP/IP Range ?

Outbound Interface ?

Traffic Assurance ?

Effective State

Table 4-12 Description of IPv6 PBR Configuration Parameters

| Parameter | Description |
|-----------|--|
| Name | Specify the name of the PBR rule, which uniquely identifies a PBR rule. The name must be unique for each rule. |

| Parameter | Description |
|--------------------|--|
| Protocol Type | Specify the protocol to which the PBR rule is effective. You can set this parameter to IP , ICMPv6 , UDP , TCP , or Custom . |
| Protocol Number | When Protocol Type is set to Custom , you need to enter the protocol number. |
| Src IP/IP Range | Configure the source IP address or IP address range for matching PBR entries. The default value is All IP Addresses. <ul style="list-style-type: none"> ● All IP Addresses: Match all the source IP addresses. ● Custom: Match the source IP addresses in the specified IP range. |
| Custom Src IP | When Src IP/IP Range is set to Custom , you need to enter a single source IP address or a source IP range. |
| Dest IP/IP Range | Configure the destination IP address or IP address range for matching PBR entries. The default value is All IP Addresses. <ul style="list-style-type: none"> ● All IP Addresses: Match all the destination IP addresses. ● Custom: Match the destination IP addresses in the specified IP range. |
| Custom Dest IP | When Dest IP/IP Range is set to Custom, you need to enter a destination source IP address or a destination IP range. |
| Src Port Range | This parameter is available only when Protocol Type is set to TCP or UDP. This parameter specifies the source port range for packet matching using PBR. |
| Dest Port Range | This parameter is available only when Protocol Type is set to TCP or UDP. This parameter specifies the destination port range for packet matching using PBR. |
| Outbound Interface | Specify the interface that forwards the data packet based on the hit PBR rule. |
| Traffic Assurance | When an outbound interface is unreachable, the traffic will be automatically routed to other reachable outbound interfaces. |
| Effective State | Turn on Effective State to specify whether to enable the PBR rule. If Effective State is turned off, this rule does not take effect. |

Note

If you want to restrict the access device to access only the specified internal network, you can set the outbound interface in the corresponding route to the WAN port in the private line network. For details on how to set the private line network, see Section [4.3.4 Configuring the Private Line](#).

All the created PBR policies are displayed in the PBR list, with the latest policy listed on the top. The device matches the policies according to their sorting in the list. You can manually adjust the policy matching sequence by clicking  or  in the **Match Order** column.

PBR List ? + Add Delete Selected

| <input type="checkbox"/> | Name ? | Protocol Type ? | Src IP Address | Dest IP Address | Src Port Range ? | Dest Port Range ? | Outbound Interface ? | Traffic Assurance | Effective State | Match Order | Action |
|--------------------------|---------------------|------------------------------|------------------|------------------|-------------------------------|--------------------------------|-----------------------------------|-------------------|-----------------------|-------------|----------------|
| <input type="checkbox"/> | test2 | IP | 2000::1 | All IP Addresses | - | - | WAN0 | Enable | Enable ? | ↓ | Edit Delete |
| <input type="checkbox"/> | test1 | IP | All IP Addresses | All IP Addresses | - | - | WAN0 | Enable | Enable ? | ↑ | Edit Delete |

Up to 30 entries can be added. Total 2 1 10/page

4. Typical Configuration Example

- Networking Requirements

Two lines with different bandwidths are deployed for an enterprise. Line A (WAN 1) is used for access to the Internet and Line B (WAN 2) is used for access to the specific internal network (10.1.1.0/24). The enterprise wants to configure PBR to guarantee correct data flows between the internal and external networks, isolate devices in the specified address range (172.26.31.1 to 172.26.31.200) from the external network, and allow these devices to access the specific internal network only.

- Configuration Roadmap

- Configure the private line.
- Add a PBR policy for access to the internal network.
- Add a PBR policy for access to the external network.
- Add a PBR policy to restrict specific devices to access the internal network only.

- Configuration Steps

(1) Configure WAN 2 as the private line for the internal network.

When you configure networking parameters for WAN 2 port, click **Advanced Settings**, turn on **Private Line**, and click **Save**. For details, see Section [4.3.4 Configuring the Private Line](#).

----- Advanced Settings -----

* MTU ? MTU Detection

* MAC Address ?

802.1Q Tag

Private Line ?

NAT Mode ?

(2) Add a PBR policy to forward data packets destined to the external network through WAN 1 port.

Choose **One-Device > Gateway > Config > Advanced > Routing > PBR** and click **Add**. In the dialog box that appears, create a PBR policy and set **Outbound Interface** to **WAN1**.

Add PBR ×

* Name ?

Protocol Type ?

Src IP/IP Range ?

Dest IP/IP Range ?

Outbound Interface ?

Traffic Assurance ?

Effective State

- (3) Add a PBR policy to forward data packets destined to the internal network through WAN 2 port. In this policy, set **Custom Dest IP** to 10.1.1.1-10.1.1.254 and **Outbound Interface** to WAN2.

×

Add PBR

* Name ?

Protocol Type ? ▾

Src IP/IP Range ? ▾

Dest IP/IP Range ? ▾

* Custom Dest IP

Outbound Interface ? ▾

Traffic Assurance ?

Effective State

- (4) Add a PBR policy to restrict devices in the IP range 172.26.31.1 to 172.26.31.200 to access the internal private line only.

In this policy, set **Src IP/IP Range** to **Custom**, **Custom Src IP** to 172.26.31.1-172.26.31.200, and **Outbound Interface** to WAN2.

Add PBR
×

* Name ?

Protocol Type ?

Src IP/IP Range ?

* Custom Src IP

Dest IP/IP Range ?

Outbound Interface ?

Traffic Assurance ?

Effective State

4.11.2 Configuring Static Routes

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.

1. Configuring IPv4 Static Routing

Choose **One-Device > Gateway > Config > Advanced > Routing > Static Routing**.

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.

Static Route List ?
+ Add
Delete Selected

| | Dest IP Address ? | Subnet Mask ? | Outbound Interface ? | Next Hop ? | Reachable ? | Action |
|--------------------------|--------------------------------|----------------------------|-----------------------------------|-------------------------|--------------------------|---|
| <input type="checkbox"/> | 10.52.48.0 | 255.255.255.0 | WAN0 | 10.52.48.43 | Yes | Edit Delete |

Up to 100 entries can be added.

Total 1 1 10/page

Add
×

* Dest IP Address

* Subnet Mask

* Outbound Interface ▾

* Next Hop

Table 4-13 Static route configuration

| 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. If the outbound interface accesses the Internet through PPPoE dialing, you do not need to configure the next-hop address. |

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 ?

| | Dest IP Address ? | Subnet Mask ? | Outbound Interface ? | Next Hop ? | Reachable ? | Action |
|--------------------------|--|--|---|---|--|---|
| <input type="checkbox"/> | 10.52.48.0 | 255.255.255.0 | WAN0 | | | |
| <input type="checkbox"/> | 192.168.110.0 | 255.255.255.0 | WAN0 | 192.168.10.1 | No ? | Edit Delete |

Up to 100 entries can be added.
Total 2 < 1 > 10/page ▾

2. Configuring the IPv6 Static Route

Choose **One-Device** > **Gateway** > **Config** > **Advanced** > **Routing** > **IPv6 Static Routing**.

Static Route List ? + Add 🗑️ Delete Selected

| <input type="checkbox"/> | IPv6 Address | Prefix Length | Interface ? | Next Hop ? | Action |
|--------------------------|--------------|---------------|--------------------------|-------------------------|--------|
| No Data | | | | | |

Up to 100 entries can be added. Total 0 < **1** > 10/page ▾

(1) Click **Add**.

Add ×

* IPv6 Address/Prefix

Length ?

* Interface ? ▾

* Next Hop ?

(2) Configure an IPv6 static route of the device.

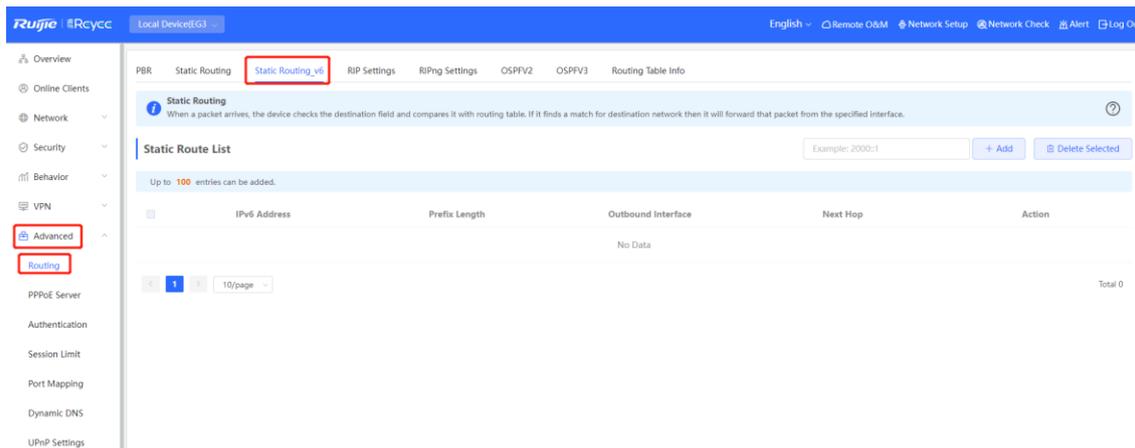
Table 4-14 Description of IPv6 Static Routing Configuration Parameters

| Parameter | Description |
|----------------------------|--|
| IPv6 Address/Prefix Length | Destination network of the packet. The destination address of the packet is matched according to the IPv6 address and prefix length. |
| Outbound Interface | Interface that forwards the packet. |
| Next Hop | IP address of the next routing node to which the packet is sent. |

(3) Click **OK**.

4.11.3 Configuring the IPv6 Static Route

Choose **Local Device** > **Advanced** > **Routing** > **Static Routing_v6**.



(1) Click **Add**.

Add
✕

* IPv6 Address/Prefix Length

* Outbound Interface

* Next Hop

(2) Configure an IPv6 static route of the device.

Table 4-15 Description of IPv6 Static Routing Configuration Parameters

| Parameter | Description |
|----------------------------|--|
| IPv6 Address/Prefix Length | Destination network of the packet. The destination address of the packet is matched according to the IPv6 address and prefix length. |
| Outbound Interface | Interface that forwards the packet. |
| Next Hop | IP address of the next routing node to which the packet is sent. |

(3) Click **OK**.

4.11.4 Set URL Route

Choose **Local Device > Config > Advanced > Routing Settings > URL Routing**.

Configure the outbound interface for accessing a website URL. When a data packet matches the URL route, the data packet is forwarded in the specified mode.

URL Routing When a packet successfully matches a URL route, the packet is forwarded based on the defined routing rules.

URL Routing Table + Add Delete Selected

| <input type="checkbox"/> | User Group | Website Group | Time | Outbound Interface | Traffic Assurance | Effective State | Remarks | Action |
|--------------------------|------------|---------------|------|--------------------|-------------------|-----------------|---------|--------|
| No Data | | | | | | | | |

Up to 30 entries can be added. Total 0 1 10/page

Click **Add**. In the dialog box that appears, set the type, website group, outbound interface, and managed time range, and then click Add to create a URL route.

Add ×

Type **User Group** Custom

* User Group (?)

* Website Group

Time

Outbound Interface

Remarks

Traffic Assurance

Effective State

Table 4-16 URL Routing Configuration Parameters

| Parameter | Description |
|-----------|-------------------------------|
| Type | URL route type, which can be: |

| Parameter | Description |
|----------------------------------|--|
| | <ul style="list-style-type: none"> ● User group: select the user group to which the route-policy applies. ● Custom: apply the route to users with IP addresses in the specified IP address range. You need to manually enter the IP address range. |
| User group | <p>This parameter is required when type is set to user group.</p> <p>Select users to which the URL route applies from the user group list. The user group list is available in 8.2 User Management. If all members in a user group are selected, the configuration takes effect for the entire user group (including members added to the user group later).</p> |
| IP Address Group | <p>Configure this information when type is set to custom.</p> <p>Enter the IP address range managed by URL routing.</p> |
| Website group | <p>Set the website type for which URL routes need to be configured. Select a website group from the created website groups. For details on how to create or modify a website group, see Section 8.5 Website Management.</p> |
| Managed time period | <p>During the controlled period, when the managed client accesses the application in the website group, the packets are forwarded through the outbound interface. Select from the drop-down list. Time range defined in 8.3 Time Management, or select custom and manually configure a time range.</p> |
| Outgoing interface | <p>Specify the interface that forwards the data packet based on the hit PBR rule.</p> |
| Remarks | <p>Configuring the description of a URL route</p> |
| Network disconnection protection | <p>After this function is enabled, if the outbound interface is unreachable, traffic is automatically switched to another reachable outbound interface.</p> |
| Effective status | <p>Turn on status to specify whether to enable the PBR rule. If status is turned off, this rule does not take effect.</p> |

4.12 Configuring ARP Binding and ARP Guard

4.12.1 Overview

The device learns the IP address and MAC address of the network devices connected to its interfaces and generates the corresponding ARP entries. You can enable ARP guard and configure IP-MAC binding to restrict Internet access of LAN hosts and improve network security.

4.12.2 Configuring ARP Binding

Choose **One-Device > Gateway > Config > Security > ARP List**.

Before you enable ARP guard, you must configure the binding between IP addresses and MAC addresses in either of the following ways:

- (1) Select a dynamic ARP entry in the ARP list and click **Bind**. You can select multiple entries to be bound at one time and click **Bind Selected** to bind them.

| No. | Device Name | MAC Address | IP Address | Type | Action |
|-------------------------------------|-------------|-------------|--------------|---------|----------------------|
| <input checked="" type="checkbox"/> | 1 | ec.....98 | 10.52.48.1 | Dynamic | Bind |
| <input checked="" type="checkbox"/> | 2 | cC.....5 | 10.52.49.26 | Dynamic | Bind |
| <input type="checkbox"/> | 3 | 0.....79 | 10.52.48.53 | Dynamic | Bind |
| <input type="checkbox"/> | 4 | 00.....3c | 10.52.48.110 | Dynamic | Bind |
| <input type="checkbox"/> | 5 | 00.....36 | 10.52.50.239 | Dynamic | Bind |

- (2) Click **Add**, enter the IP address and MAC address to be bound, and click **OK**. The input box can display existing address mappings in the ARP list. You can click a mapping to automatically enter the address mapping.

Add ×

Device Name ?

* IP Address

* MAC Address

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

| No. | Device Name | MAC Address | IP Address | Type | Action |
|-------------------------------------|-------------|-------------|--------------|---------|----------------------|
| <input checked="" type="checkbox"/> | 1 | e..... | 10.52.48.1 | Dynamic | Bind |
| <input checked="" type="checkbox"/> | 2 | c.....5 | 10.52.49.26 | Dynamic | Bind |
| <input type="checkbox"/> | 3 | 0C.....79 | 10.52.48.53 | Dynamic | Bind |
| <input type="checkbox"/> | 4 | 0C.....3c | 10.52.48.110 | Dynamic | Bind |

4.12.3 Configuring ARP Guard

Choose **One-Device > Gateway > Config > Security > ARP List**.

Turn on **Enable** in the **ARP Guard** section to enable ARP guard. After ARP guard is enabled, only LAN hosts with IP-MAC binding can access the external network. For details on how to configure ARP binding, see Section [4.12.2 Configuring ARP Binding](#).

ARP Guard

Enable ? Only the devices configured with IP-MAC binding are allowed to access the Internet.

Interface Select All

Default VLAN
 VLAN 55
 VLAN 555

Keep Config

4.13 Configuring MAC Address Filtering

4.13.1 Overview

You can enable MAC address filtering and configure a whitelist or blacklist to effectively control Internet access from LAN hosts.

- **Allowlist:** Allow only hosts whose MAC addresses are in the filter rule list to access the Internet.
- **Blocklist:** Deny hosts whose MAC addresses are in the filter rule list from accessing the Internet.

4.13.2 Configuration Steps

Choose **One-Device > Gateway > Config > Security > MAC Filtering**.

- (1) In the Filtering Rule List pane, click **Add**. In the dialog box that appears, enter the MAC address and remarks. The input box can display existing address mappings in the ARP list. You can click a mapping to automatically enter the MAC address. Click **OK**. A filter rule is created.

Filtering Rule List Search by mac + Add Delete Selected

| | Device Name | MAC Address | Action |
|--------------------------|-------------|-------------|--------|
| <input type="checkbox"/> | | | |

No Data

Up to 512 entries can be added. Total 0 < 1 > 10/page ▾

Add
×

Device Name ?

* MAC Address

Cancel
OK

- (2) Turn on **MAC Filtering**, set Filtering Type, and click Save.

MAC Filtering

MAC Filtering

The following hosts are not allowed to access the Internet.

Filtering Type: Blocklist

Save

4.14 Port Mapping

4.14.1 Overview

1. Port Mapping

The port mapping function can establish a mapping relationship between the IP address and port number of a WAN port and the IP address and port number of a server in the LAN, so that all access traffic to a service port of the WAN port will be redirected to the corresponding port of the specified LAN server. This function enables external users to actively access the service host in the LAN through the IP address and port number of the specified WAN port.

Application scenario: Port mapping enables users to access the cameras or computers in their home network when they are in the enterprise or on a business trip.

2. NAT-DMZ

When an incoming data packet does not hit any port mapping entry, the packet is redirected to the LAN server according to the Demilitarized Zone (DMZ) rule. All data packets actively sent from the Internet to the device are forwarded to the designated DMZ host, thus realizing LAN server access of external network users. DMZ not only realizes the external network access service, but also ensures the security of other hosts in the LAN.

Application scenario: Configure port mapping or DMZ when an external network user wants to access the LAN server, for example, access a server deployed in the home network when the user is in the enterprise or on a business trip.

4.14.2 Getting Started

- Confirm the intranet IP address of the mapping device on the LAN and the port number used by the service.
- Confirm that the mapped service can be normally used on the LAN.

4.14.3 Configuration Steps

Choose **One-Device > Gateway > Config > Advanced > Port Mapping > Port Mapping**.

Click **Add**. In the dialog box that appears, enter the rule name, service type, protocol type, external port/range, internal server IP address, and internal port/range. You can create a maximum of 50 port mapping rules.

Port Mapping List + Add Delete Selected

| | Name ? | Protocol ? | External IP Address ? | External Port ? | Internal IP Address ? | Internal Port ? | Action |
|---------|--------|------------|-----------------------|-----------------|-----------------------|-----------------|--------|
| No Data | | | | | | | |

Up to 512 entries can be added. Total 0 < 1 > 10/page

Add ×

* Name ?

Preferred Server

Protocol ?

External IP Address ? Outbound Interface Enter or select an IP address.

* External Port/Range ?

* Internal IP Address ?

* Internal Port/Range ?

Table 4-17 Port mapping configuration

| Parameter | Description |
|------------------|---|
| Name | Enter the description of the port mapping rule, which is used to identify the rule. |
| Preferred Server | Select the type of service to be mapped, such as HTTP or FTP. The internal port number commonly used by the service is automatically entered. If you are not sure about the service type, select Custom. |
| Protocol | Select the transmission layer protocol type used by the service, such as TCP or UDP. The value ALL indicates that the rule applies to both protocols. The value must comply with the client configuration of the service. |

| Parameter | Description |
|---------------------|--|
| External IP Address | Specify the host address used for Internet access. The default value is the IP address of the WAN port. |
| External Port/Range | Specify the port number used for Internet access. You need to confirm the port number in the client software, such as the camera monitoring software. You can enter a port number or a port range, such as 1050-1060. If you enter a port range, the value of Internal Port/Range must also be a port range. |
| Internal IP Address | Specify the IP address of the internal server to be mapped to the WAN port, that is, the IP address of the LAN device that provides Internet access, such as the IP address of the network camera. |
| Internal Port/Range | Specify the service port number of the internal server to be mapped to the WAN port, that is, the port number of the application that provides Internet access, such as port 8080 of the Web service. You can enter a port number or a port range, such as 1050-1060. If you enter a port range, the number of ports must be the same as that specified in External Port/Range. |

4.14.4 Verification and Test

Check whether the external network device can access services on the destination host using the external IP address and external port number.

4.14.5 Solution to Test Failure

- (1) Modify the value of **External Port/Range** and use the new external port number to perform the test again. The possible cause is that the port is blocked by the firewall.
- (2) Enable the remote access permission on the server. The possible cause is that remote access is displayed on the server, resulting in normal internal access but abnormal access across network segments.
- (3) Configure DMZ rules. For details, see Section [4.14.6 Configuration Steps \(DMZ\)](#). The possible cause is that the specified ports are incorrect or incomplete.

4.14.6 Configuration Steps (DMZ)

Choose **One-Device > Gateway > Config > Advanced > Port Mapping > NAT-DMZ**.

Click **Add**. Enter the rule name and internal server IP address, select the interface to which the rule applies, specify the rule status, and click **OK**. You can configure only one DMZ rule for an outbound interface.

? You can view NAT-DMZ settings and edit or delete the rule.

NAT-DMZ Rule List + Add Delete Selected

| | Name ? | Outbound Interface ? | Dest IP Address ? | Status ? | Action |
|---------|---|---|--|---|--------|
| No Data | | | | | |

There are 2 outbound interfaces. Up to 2 rules can be added.

Add Rule ×

* Name

* Dest IP Address

Outbound Interface

Status

Table 4-18 DMZ rule configuration

| Parameter | Description |
|--------------------|--|
| Name | Enter the description of the mapping rule, which is identify the DMZ rule. |
| Dest IP Address | Specify the IP address of the DMZ host to which packets are redirected, that is, the IP address of the internal server that can be accessed from the Internet. |
| Outbound Interface | Specify the WAN port in the DMZ rule. You can configure only one rule for a WAN port. |
| Status | Specify whether the rule is effective. The rule is effective after you turn on Status . |

4.15 UPnP

4.15.1 Overview

After the Universal Plug and Play (UPnP) function is enabled, the device can change the port used by the Internet access service according to the client request, implementing NAT. When a client on the Internet wants to access the internal resources on the LAN device, the device can automatically add port mapping entries to realize traversal of some services between internal and external networks. The following commonly used programs support the UPnP protocol: MSN Messenger, Thunder, BT, and PPLive.

Before you use the UPnP service, note that clients (PCs and mobile phones) used in combination also support UPnP.

Note

To implement automatic port mapping using UPnP, the following conditions must be met:

- UPnP is enabled on the device.
- The operating system of the LAN host supports UPnP and has UPnP enabled.
- The programs support UPnP and have UPnP enabled.

4.15.2 Configuring UPnP

Choose **One-Device > Gateway > Config > Advanced > UPnP**.

Turn on Enable to enable the UPnP function. Select a port from the drop-down list box of **Default Interface**. Click **Save** to make the configuration take effect.

If any relevant program converts the port automatically, the information is displayed in the **UPnP List** section.

UPnP (Universal Plug and Play) is a new Internet protocol aimed at improving communication between devices.

Enable

Default Interface: WAN0

Save

UPnP List

| Protocol | App | Client IP Address | Internal Port | External Port |
|----------------|-----|-------------------|---------------|---------------|
| No UPnP Device | | | | |

Table 4-19 UPnP configuration

| Parameter | Description |
|-----------|---|
| Enable | Specify whether to enable UPnP. By default, UPnP is disabled. |

| Parameter | Description |
|-------------------|--|
| Default Interface | Specify the WAN port address bound to the UPnP service. By default, the default interface is a WAN port. On the device with multiple WAN ports, you can manually select the WAN port to bind or set this parameter to Auto to allow the device to select a WAN port automatically. |

4.15.3 Verifying Configuration

After the UPnP service is enabled, open a program that supports the UPnP protocol (such as Thunder or BitComet) on the client used with the device, and refresh the Web page on the device. If a UPnP entry is displayed in the UPnP list, a UPnP tunnel is created successfully.

4.16 Dynamic DNS

4.16.1 Overview

After the Dynamic Domain Name Server (DDNS) service is enabled, external users can use a fixed domain name to access service resources on the device over the Internet at any time, without the need to search for the WAN port IP address. You need to register an account and a domain name on the third-party DDNS service provider for this service. The device supports DynDNS and No-IP DNS.

4.16.2 Getting Started

Before you use the DDNS service, register an account and a domain name on the No-IP or DynDNS official website.

4.16.3 Configuring DDNS

1. Configuration Steps

The device supports No-IP DNS and DynDNS. DynDNS can be used by International users only, and No-IP DNS can be used by both Chinese and International users.

Choose **One-Device > Gateway > Config > Advanced > Dynamic DNS**.

Enter the registered username and password and click Log In to initiate a connection request to the server. The binding between the domain name and WAN port IP address of the device takes effect.

Click Delete to clear all the entered information and remove the server connection relationship.

The Link Status parameter specifies whether the server connection is established successfully. If you do not specify the domain name upon login, the domain name list of the current account is displayed after successful connection. All the domain names of this account are parsed to the WAN port IP address.

No-IP DNS

Other DNS

* Service Interface

* Username [Register](#)

* Password

Domain

IPv6 Disable Enable

Link Status -

Domain -

Note

- Both No-IP DNS and other DNS support IPv6 connectivity.
- To ensure compatibility with the IPsec VPN functionality, you are advised to enable IPv6 when IPv6 is used for IPsec VPN connection.

Table 4-20 DDNS login information

| Parameter | Description |
|---------------------|--|
| Service Interface | One domain name can be parsed to only one IP address. Therefore, you need to specify the WAN port bound to the domain name when multiple WAN ports are available. By default, the service interface is a WAN port. |
| Username / Password | Enter the username and password of the account registered on the official website. If no registered account is available, click Register to switch to the official website and create a new account. |

| Parameter | Description |
|-----------|--|
| Domain | <p>Specify the domain name bound to the service interface IP address.</p> <p>This parameter is optional for No-IP DNS. One account can be bound to multiple domain names. You can choose to bind only one domain name to the IP address of the current service interface. Only the selected domain name is parsed to the WAN port IP address. If no domain name is specified, all the domain names of the current account are parsed to the WAN port IP address.</p> <p>This parameter is optional for DynDNS, and the value is provided by the DynDNS service provider.</p> |

2. Verifying Configuration

If **Link Status** is displayed as **Connected**, the server connection is established successfully. After the configuration is completed, ping the domain name from the Internet. The ping succeeds and the domain name is parsed to the WAN port IP address.

4.17 Connecting to IPTV

Caution

IPTV connection is not supported only in the Chinese environment. To connect to IPTV in the Chinese environment, switch the system language. For details, see Section [12.13 Switching System Language](#).

IPTV is a network television service provided by the ISP.

4.17.1 Getting Started

- Confirm that the IPTV service is activated.
- Check the local IPTV type: VLAN or IGMP. If the type is VLAN, confirm the VLAN ID. If you cannot confirm the type or VLAN ID, contact the local ISP.

4.17.2 Configuration Steps (VLAN Type)

Choose **One-Device > Gateway > Config > Network > IPTV > IPTV/VLAN**.

Select a proper mode based on your region, click the drop-down list box next to the interface to connect and select **IPTV**, and enter the VLAN ID provided by the ISP. For example, when you want to connect the IPTV set top box to LAN 3 port of the device and the VLAN ID is 20, the configuration UI is as follows.

Internet VLAN: If you need to set a VLAN ID for the Internet access service, turn on this parameter, and enter the VLAN ID.

By default, the VLAN tag function is disabled. You are advised to keep the VLAN tag function disabled unless otherwise specified.

After the configuration is completed, confirm that the IPTV set top box is connected to the correct port, for example, LAN 3 in the example.

⚠ Caution

Enabling this function may lead to network disconnection. Exercise caution when performing this operation.

* Mode ▾

* AG ▾

* AG ▾

* LAN0 ▾

* LAN1 ▾

* LAN2 ▾

* LAN3 ▾

* LAN4/WAN3 ▾

* LAN5/WAN2 ▾

Internet VLAN (WAN) 802.1Q Tag

4.17.3 Configuration Steps (IGMP Type)

Choose **One-Device > Gateway > Config > Network > IPTV > IPTV/IGMP**.

The IGMP type is applicable to the ISP FPT. After you enable IPTV connection, connect the IPTV set top box to any LAN port on the router.

Enable

4.18 Limiting the Number of Connections

Choose **One-Device > Gateway > Config > Advanced > Session Limit**.

This function is used to control the maximum number of connections per IP address.

Click **Add** to add an IP session limit rule.

Rule List ↻ + Add Delete Selected

| <input type="checkbox"/> | Name ? | User Group | Application List | Time | Total Connections | Total Connections per IP | Connected ? | Status ? | Match Order | Action |
|--------------------------|---------------------|------------|------------------|------|-------------------|--------------------------|--------------------------|-----------------------|-------------|--------|
| No Data | | | | | | | | | | |

Up to 20 entries can be added.

Add ×

* Name ?

Type User Group Custom

* User Group ?

Total Connections

Total Connections per IP

Status ?

----- Advanced Settings -----

Application All Applications App Group Custom

Time ?

Apply To Total Specified port

Table 4-21 IP session limit rule information

| Parameter | Description |
|-----------|---|
| Name | Enter the name of the IP session limit rule. |
| Type | Select the rule type: <ul style="list-style-type: none"> ● User Group: The rule takes effect on the specified user group. ● Custom: The rule takes effect on the custom IP address range. |

| Parameter | Description |
|--------------------------|--|
| User Group | <p>Select the user group from the list. For details about the user group list, see Section 8.2 User Management.</p> <p>If all members of the user group are selected, the rule applies to the entire user group, including future members added to the group.</p> <p>Note: This field is required only when the rule Type is set to User Group.</p> |
| Start IP Address | Enter the start IP address for session matching in the rule. |
| End IP Address | Enter the end IP address for session matching in the rule. |
| Total Connections | Specify the total number of sessions for all IP addresses matching this rule. |
| Total Connections per IP | Specify the maximum number of sessions per IP address for all IP addresses matching this rule. |
| Status | Specify whether the rule is effective. The rule takes effect after you turn on this parameter. |
| Application | <p>After an application is selected, the rule will take effect on the specified application.</p> <ul style="list-style-type: none"> ● All Applications: The rule takes effect on all applications. ● App Group: Select an application group defined in 8.4.4 Custom Application Group from the drop-down list box. The rule takes effect on applications in the selected application group. ● Custom: The rule takes effect on specified applications in the application list. |
| Time | The rule is effective in the selected time period. Select a time period from the time periods defined in 8.3 Time Management from the drop-down list, or select Custom to manually configure a time period. |
| Apply To | <p>Set the application scope of the rule:</p> <ul style="list-style-type: none"> ● Total: The rule applies to the entire device. ● Specified port: Select the interfaces to which the session count limit will be applied. The rule will be applied to the selected interfaces only. |

4.19 Configuring Local Security

4.19.1 Configuring an Admin IP Address

Admin IP addresses are exempt from the ping prohibition function. Packets sent from admin IP addresses can pass through and will not be discarded.

Choose **One-Device > Gateway > Config > Security > Local Security > Security Zone**.

Click **Add**. Then, you can configure admin IP address information.

Up to 8 entries can be added.

Admin IP Address

| <input type="checkbox"/> | Username | IP Range/Interface | Action |
|--------------------------|----------|--------------------|---|
| <input type="checkbox"/> | admin | WAN0 | Edit Delete |

Up to 32 entries can be added. Total 1

1. Configuring an Admin IP Address (Based on an IP Address)

Add ×

* Username

Specified Mode IP Range Interface

Please enter an IP address or range.

- (1) Configure a name for the admin IP address.
The name is a string of 1–32 characters.
- (2) Set **Specific Mode** to **IP Range**.
- (3) Configure an IP address.
You can specify a single IP address or an IP address range.

2. Configuring an Admin IP Address (Based on a Port)

Add
×

* Username

Specified Mode IP Range **Interface**

Cancel
OK

- (1) Configure a name for the admin IP address.
The name is a string of 1–32 characters.
- (2) Set **Specific Mode** to **Interface**.
- (3) Specify the port.
You can select a LAN port or WAN port as the interface.

3. Deleting an Admin IP Address

- Select an entry and click **Delete** to delete information about the admin IP address.
- Select multiple entries and click **Delete Selected** to bulk delete selected entries.

| Admin IP Address | | | |
|--------------------------|----------|--------------------|---|
| | Username | IP Range/Interface | Action |
| <input type="checkbox"/> | admin | WAN0 | Edit Delete |
| <input type="checkbox"/> | test | WAN1 | Edit Delete |

Up to 32 entries can be added.

Total 2 1 10/page

4. Editing Information About an Admin IP Address

You cannot modify the name and specified mode of an admin IP address but modify the IP address range or port in the specified mode.

Edit

✕

* Username

test

Specified Mode IP Range Interface

192.168.10.1

Cancel

OK

Edit

✕

* Username

admin

Specified Mode IP Range Interface

WAN0

Cancel

OK

4.19.2 Configuring Security Zones

Note

For devices that do not support SNMP, the SNMP service cannot be disabled in a LAN zone.

A security zone is a logical zone consisting of a group of systems that trust each other and share the same security protection requirements. Generally, a security zone consists of a group of interfaces. Networks formed by interfaces in the same security zone share the same security attributes. Each interface can only belong to one security zone.

- Up to eight security zones can be added.
- Pre-defined security zones include:

- o Pre-defined LAN zone: By default, all VLANs are mapped to the pre-defined LAN zone.
- o Pre-defined WAN zone: By default, all WAN interfaces are mapped to the pre-defined WAN zone.

Choose **One-Device > Gateway > Config > Security > Local Security > Security Zone**.

Security Zone ? + Add Delete Selected

| <input type="checkbox"/> | Name | Network Interface | Accessible Security Zones | Authorized Security Zones | Disabled Service | Action |
|--------------------------|--------------------|--|--|---------------------------|------------------|---|
| <input type="checkbox"/> | Default LAN Zone | LAN <small>Default VLAN</small> VLAN 555 VLAN 55 | Default WAN Zone Default Route Zone | | | Edit Delete |
| <input type="checkbox"/> | Default WAN Zone | WAN <small>WAN1</small> WAN0 | | Default LAN Zone | | Edit Delete |
| <input type="checkbox"/> | Default Route Zone | WAN | Default LAN Zone | Default LAN Zone | | Edit Delete |

Up to 8 entries can be added.

- (1) Click **Add**.
- (2) Configure parameters for the security zone.

×

Add

* Name

* Network Interface LAN WAN

Accessible Security Zones

Authorized Security Zones

Disabled Service ? WEB PING DNS
 DHCP SNMP

Table 4-22 Description of Security Zone Configuration Parameters

| Parameter | Description |
|---------------------------|---|
| Name | Name of the security zone. |
| Network Interface | Interfaces mapped to the security zone, including LAN and WAN. LAN refers to VLAN, and WAN refers to WAN interfaces. Note: After a new security zone is created and VLANs or WAN interfaces are mapped to this new security zone, the VLANs or WAN interfaces will be removed from the pre-defined LAN zone or pre-defined WAN zone. |
| Accessible Security Zones | Other security zones to which this security zone can access. |
| Authorized Security Zones | Other security zones that can access this security zone. |
| Disabled Service | Services prohibited in this security zone: <ul style="list-style-type: none"> ● If PING is selected, clients in the security zone cannot ping the local device. ● If Web is selected: clients in the security zone cannot access the local web page. ● If DNS is selected, the address of the DNS server used by clients in the security zone is the local IP address, and web pages cannot be accessed normally. ● If DHCP is selected, clients in the security zone cannot obtain IP addresses. ● If SNMP is selected, clients in the security zone cannot use the SNMP service of the device. |

(3) Click **OK**.

4.19.3 Configuring Session Attack Prevention

1. Overview

- Session Attack Prevention

In a session attack, an attacker sends heavy traffic to the device. In this case, the device has to consume many resources when creating connections. To reduce the impact of the attack, you can limit the rate of creating sessions.

- DDoS Attack Prevention

In a DDoS Attack, an attacker sends tremendous abnormal packets to a device. As a result, the device uses a large amount of resources to handle the packets. This causes the device performance to deteriorate or the system to break down.

If the value of TCP SYN and other TCP Flood parameters is too small, the authentication function and access to local web pages will be affected.

If the value of UDP Flood parameter is too small, the DHCP address allocation, DNS domain name resolution, and VPN functionalities will be affected.

You are advised to set the value to be greater than the load capacity of the local device.

- Suspicious Packet Attack Prevention

- In a suspicious packet attack, an attacker sends tremendous error packets to the device. When the host or server handles the error packets, its system will crash.

2. Configuring Session Attack Prevention

Choose **One-Device > Gateway > Config > Security > Local Security > Attack Defense**.

- (1) Enable Anti Session Attack.

- (2) Configure the session creation rate limit, including global and per-IP values.
- (3) Click **Save**.

3. Configuring DDoS Attack Prevention

Choose **One-Device > Gateway > Config > Security > Local Security > Attack Defense**.

- (1) Select required attack prevention types and enable this feature.

- (2) Configure rate limiting.
- (3) Click **Save**.

4. Configuring Suspicious Packet Attack Prevention

Choose **One-Device > Gateway > Config > Security > Local Security > Attack Defense**.

- (1) Select required attack prevention types and validity check types to enable this feature.

- (2) To enable large ping attack prevention, enter the packet length.
- (3) Click **Save**.

5. Configuring Packet Receiving and Sending Control

Choose **One-Device > Gateway > Config > Security > Local Security > Attack Defense**.

- (1) Select the packet types that are prohibited from being sent by the device. Select at least one packet type.

Disable ICMP Error Message ICMP Timeout (type:11) x 0 packets blocked Details
ICMP Packet Management ⓘ
 Disable ICMPv6 Error Mess Time Exceeded x 0 packets blocked Details

- o Enable **Disable ICMP Error Messages**. You can select **ICMP Timeout**, **Destination Unreachable**, **Redirection**, and **Parameter**.

Anti Large Ping Attack Packet Length 4000
 Anti Fraggle Attack
Anti Malformed Packet Attack medium ⓘ
 ICMP Validity Check ⓘ 0 packets blocked
 IP Protocol Validity Check ⓘ
 Disable ICMP Error Messages ⓘ ICMP Timeout (type:11) x 0 packets blocked Details
 Disable ICMPv6 Error Messages Time Exceeded x 0 packets blocked Details

Destination Unreachable (type:3)
 Redirection (type:5)
 ICMP Timeout (type:11)
 Parameter (type:12)

- o Enable **Disable ICMPv6 Error Message**. You can select **Destination Unreachable**, **Datagram too Big**, **Time Exceeded**, and **Parameter Problem**.

Disable ICMP Error Messages ⓘ
 Disable ICMPv6 Error Messages Time Exceeded x 0 packets blocked Details

Destination Unreachable
 Datagram Too Big
 Time Exceeded
 Parameter Problem

(2) Click **Save**.

4.19.4 Checking the Security Log

Choose **One-Device > Gateway > Config > Security > Local Security > Security Log**.

Check defense results of the device against various attacks on the **Security Log** page.

Refresh Every 10s v

Security Log Search Q Last 1 week v

| Timestamp v | Attack Type ⓘ | Severity ⓘ | Description |
|---|---------------|------------|-------------|
| The device has been running safely for 3 days | | | |

Total 0 < 1 > 10/page v

4.20 Configuring TTL Rules

4.20.1 Overview

Time to live (TTL) aims to prevent unauthorized connections. It limits the number of devices that can transmit data packets in the network by limiting the existence time of the data packets in the computer network, so as to prevent infinite transmission of data packets in the network and the waste of resources.

When TTL is set to 1 and is valid for LANs, packets are directly discarded when passing through the next router. If a user connects a router to Ruijie device without permission and connects a client to the router, packets cannot pass through the client, either. This restriction prevents users from connecting routers without permission.

Note

- Changing the TTL affects packet forwarding on the network.
- The following data packets are not affected by this function: data packets forwarded by the express forwarding function of the device, data packets used by Wi-Fi cracking software (Cheetah Wi-Fi) to implement hotspot sharing, data packets forwarded at L2, and data packets passing through devices with TTL changed.

4.20.2 Configuring TTL Rules

Choose **One-Device > Gateway > Config > Advanced > TTL Rule**.

This operation allows you to change the TTL value in packets forwarded to a specified IP address range or a specified port.

TTL Rule

+ Add
Delete Selected

| <input type="checkbox"/> | Rule Name | Dest IP Address | Outbound Interface | TTL Config Mode | Value | Action |
|--------------------------|-----------|-----------------|--------------------|-----------------|-------|--------|
| No Data | | | | | | |

Up to 10 entries can be added.

Total 0
<
1
>
10/page

1. Configuring a TTL Rule

Add
×

* Rule Name

Specified Mode Dest IP Address Outbound Interface

Please enter an IP address or range.

TTL Config Mode TTL Value TTL Increment
 TTL Decrement

* Value

Table 4-23 Description of TTL Rule Configuration

| Parameter | Description |
|-----------------|--|
| Rule Name | Specify the name of a TTL rule. |
| Specified Mode | Specify the range for the rule to take effect: <ul style="list-style-type: none"> ● Dest IP Range: Indicates that the TTL rule takes effect on a specified IP address or range. ● Outbound Interface: Indicates that the TTL rule takes effect on a specified outbound interface. |
| TTL Config Mode | Configure a rule for TTL values in packets. <ul style="list-style-type: none"> ● TTL Value: Specifies the value, to which the TTL value is changed, after a data packet passes through the device. ● TTL Increment: Specifies the increment of the TTL value on the basis of the original value after a data packet passes through the device. ● TTL Decrement: Specifies the decrement of the TTL value on the basis of the original value after a data packet passes through the device. |
| Value | Configure the TTL value in packets. The value range is from 1 to 255. |

2. Deleting a TTL Rule

- Click Delete to delete the configuration of a specified entry.
- Select multiple entries and click Delete Selected to bulk delete selected entries.

TTL Rule + Add Delete Selected

| <input type="checkbox"/> | Rule Name | Dest IP Address | Outbound Interface | TTL Config Mode | Value | Match Order | Action |
|-------------------------------------|-----------|-----------------|--------------------|-----------------|-------|-------------|---|
| <input checked="" type="checkbox"/> | test1 | | WAN | TTL Value | 64 | ↓ | Edit Delete |
| <input type="checkbox"/> | test2 | | WAN1 | TTL Value | 64 | ↑ | Edit Delete |

Up to 10 entries can be added. Total 2 1 10/page

3. Editing a TTL Rule

Click **Edit**. Change the TTL rule configuration mode and TTL value.

Edit ×

* Rule Name

Specified Mode Dest IP Address Outbound Interface

TTL Config Mode TTL Value TTL Increment
 TTL Decrement

* Value

4. Adjusting the Sequence of TTL Rules

After configuring multiple TTL rules, you can adjust their sequence to specify the rule matching sequence. TTL rules in front rows are matched first, and those in back rows are matched later. If the ranges of rules overlap, the final effect is the superposition of multiple matching results.

TTL Rule + Add Delete Selected

| <input type="checkbox"/> | Rule Name | Dest IP Address | Outbound Interface | TTL Config Mode | Value | Match Order | Action |
|--------------------------|-----------|-----------------|--------------------|-----------------|-------|---|-------------|
| <input type="checkbox"/> | test1 | | WAN | TTL Value | 64 | ↓ ↓ | Edit Delete |
| <input type="checkbox"/> | test2 | | WAN1 | TTL Value | 64 | ↑ ↑ | Edit Delete |

Up to 10 entries can be added. Total 2 1 10/page

4.21 Configuring USB Settings

The Samba protocol is a network file-sharing protocol used to provide shared access to files, printers, and other resources. It allows Linux/Unix-based systems to share files, folders, printers, and other resources with Windows-based systems and vice versa.

When a USB storage device is connected to the USB port of the gateway, Samba allows other devices on the network to access and share files and data stored on the connected USB storage device.

Choose **Local Device > Advanced > USB Application**.

Caution

- Prior to configuration, ensure that the USB storage device is connected to the designated USB port.
 - Samba Filesharing is supported on RG-EG105GW-X only.
-

1. Enabling Samba Filesharing

Toggle on the **Samba Filesharing** switch. After this feature is enabled, devices on the Local Area Network (LAN) can access files stored on the USB flash drive through the Samba protocol.

Samba Sharing

 After Samba Sharing is enabled, the devices on the LAN can access the files stored in the USB drive. In Windows, you can access the file server by entering \\ device IP address in the address bar of the file manager, such as \\192.168.110.1 Only an empty folder can be deleted.

Samba Sharing

2. Adding Users

Click **Add User**. Enter the username and password, and then click **OK** to create and manage filesharing users.

Samba Sharing

+ Add User



Guest

Add ×

* Username

* Password

You can click the three horizontal dots on the right side of the user to edit or delete the user.

Samba Sharing

+ Add User

Guest

test ⋮ Edit Delete

4.22 Configuring Self-Healing Mesh

Choose **One-Device > Gateway > Config > Advanced > Self-Healing Mesh**.

After Reye Mesh is enabled, Self-Healing Mesh is automatically switched to Wireless Repeater mode to ensure normal service operation if a fault occurs on the wired link.

 After Reye Mesh is enabled, Self-Healing Mesh is automatically switched to Wireless Repeater mode to ensure normal service operation if a fault occurs on the wired link.

Enable

4.23 Hardware Acceleration

Note

This feature is supported by only the RG-EG105GW-X.

Choose **One-Device > Gateway > Config > Advanced > Hardware Acceleration**.

After Hardware acceleration is enabled, the Internet access speed will be improved.

i After Hardware Acceleration is enabled, the Internet access speed will be improved and clients will not be rate-limited.

Enable

Save

⚠ Caution

- The Hardware Acceleration feature conflicts with the **WLAN Rate Limiting**, **IPv6**, and **Smart Flow Control** feature. If **WLAN Rate Limiting**, **IPv6**, or **Smart Flow Control** is configured, enabling Hardware Acceleration will cause the **WLAN Rate Limiting**, **IPv6**, or **Smart Flow Control** to become ineffective.
- The Hardware Acceleration feature conflicts with the Wireless Authentication function. If Wireless Authentication is configured, Hardware Acceleration cannot be enabled.

4.24 Configuring Audit Log

Choose **One-Device > Gateway > Config > Advanced > Audit Log**.

After the **Audit Log** function is enabled and configured, the system uploads audit logs of the selected log type to the specified server.

(1) Toggle on **Enable** to enable the **Audit Log** function.

i The port ID of the device must be consistent with that of the peer server. The server logs can be divided into three levels: high, medium and low.

Enable

* Server Type

* Server Address

* Port 1-65535

* Log Sending Rate (log/s)

Log Type **DHCP Log** **NAT Log**

URL Log **Auth User Log**

Save

Show Log Status

(2) Configure parameters of the **Audit Log** function.

Table 4-24 Audit Log Configuration Parameters

| Parameter | Description |
|------------------|--|
| Server Type | Server type. The device supports the following three server types: <ul style="list-style-type: none"> ● Default: Default server type. ● turkiye-5651: Local server in Türkiye. ● Thailand: Local server in Thailand. |
| Server Address | Address of the log server. It can be a domain name and an IPv4 address. |
| Port | Port number of the server, which can be a custom port number. The default port number is 514. |
| Log Sending Rate | Rate at which the device sends audit logs to the server. The default rate is 5000 logs per second. The value ranges from 1 log per second to 10000 logs per second. |
| Log Type | Types of logs to be sent to the server, including DHCP logs, NAT logs, URL logs, and authentication user logs. Priority of sending audit logs: High, Medium, and Low. When the device resources are limited, audit logs with higher priority are sent to the server first. |

(3) Click **Save**.

Click **Show Log Status** to view the status of the **Audit Log** function, including the server address, server connection status, and the sending history of each log type (including received, sent, and discarded logs).

Log Status



Server: 10.52.40.204:514
 Server Type: default
 Server Status: Connected
 Log Sending Rate: 5000 (log/s)

| | | | |
|----------------|--------------------|----------------|------------------|
| NAT Log: | Received: 19223869 | Sent: 19223869 | Discarded: 51562 |
| DHCP Log: | Received: 222 | Sent: 222 | Discarded: 0 |
| URL Log: | Received: 11900136 | Sent: 11900136 | Discarded: 526 |
| Auth User Log: | Received: 0 | Sent: 0 | Discarded: 0 |

Refresh

Cancel

4.25 Other Settings

Choose **Local Device > Advanced > Other Settings**.

You can set some functions not frequently used on the Other Settings page. By default, all the functions on this page are disabled.

Enable RIP&RIPng: After this function is enabled, LAN and WAN ports support dynamic routing protocols Routing Information Protocol (RIP) and RIP next generation (RIPng) and can automatically synchronize route information from other RIP-enabled routers in the network.

Enable Advanced Firewall: After this function is enabled, enhanced attack defense and packet protocol check will degrade the forwarding performance of the device.

Enable SIP ALG: Some voice communication uses the Session Initiation Protocol (SIP) protocol. If the server is connected to a WAN port, SIP packets may become unavailable after NAT. After you enable this function, SIP packets are converted by the application-level gateway (ALG). You can enable or disable this function based on actual needs.

Disable ICMPv6 Error Messages: In normal cases, when the device receives an ICMPv6 anomaly packet, it sends an ICMPv6 error packet to the packet source. If you do not want the device to send these packets due to security considerations, enable this function.

 **Other Settings**

Enable RIP&RIPng

Enable Advanced 

Firewall

Enable SIP ALG

Disable ICMPv6 Error

Messages

5 Wireless Management

Note

Wireless management includes wireless function settings of the device and management of downlink wireless devices of the device. When self-organizing network discovery is enabled, the wireless settings are synchronized to all wireless devices in the network. You can configure groups to limit the device scope under wireless management. For details, see Section [5.1 Configuring AP Groups](#).

5.1 Configuring AP Groups

5.1.1 Overview

After self-organizing network discovery is enabled, the device can function as the master AP/AC to batch configure and manage its downlink APs by group. Before you configure the APs, divide them to different groups.

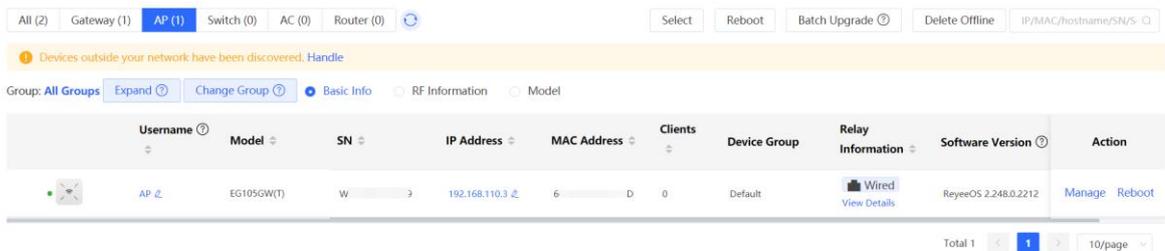
Note

If you specify groups when configuring the wireless network, the configuration takes effect on wireless devices in the specified groups.

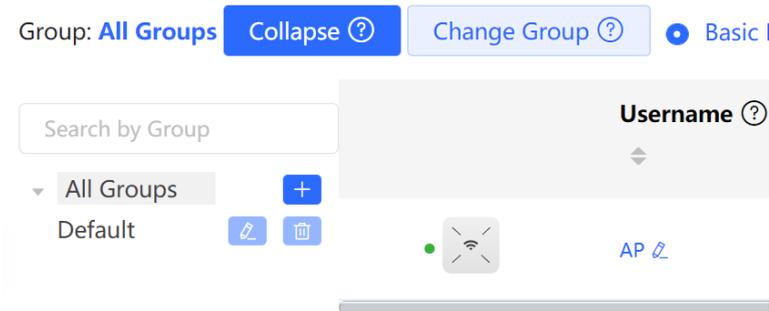
5.1.2 Configuration Steps

Choose **Network > Devices > AP**.

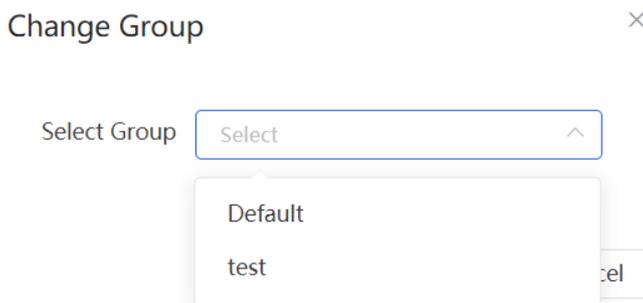
- (1) View the information of all APs in the current network, including the basic information, RF information, and model. Click the SN of an AP to configure the AP separately.



- (2) Click **Expand**. Information of all the current groups is displayed to the left of the list. Click **+** to create a group. You can create a maximum of eight groups. Select the target group and click **✎** to modify the group name or click **🗑** to delete the group. You cannot modify the name of the default group or delete the default group.



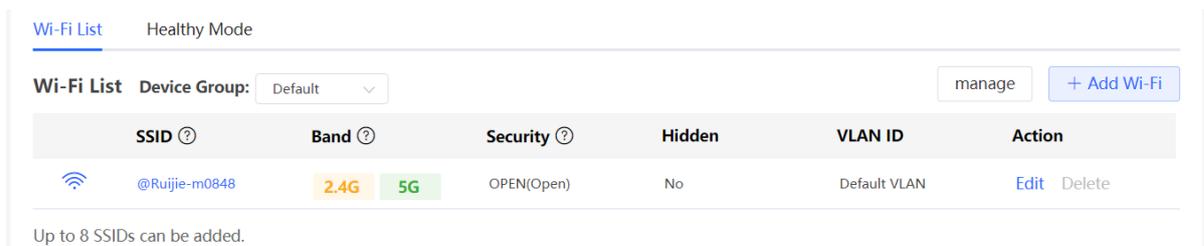
- Click a group name in the left. All devices in the group are displayed. One device can belong to only one group. By default, all devices belong to the default group. Select a record in the device list and click **Change Group** to migrate the selected device to the specified group. After a device is moved to the specified group, the device will use the configuration for the new group. Click **Delete Offline Devices** to remove offline devices from the list.



5.2 Configuring Wi-Fi

5.2.1 Adding a Wi-Fi Network

Choose **Network-Wide > Workspace > Wireless > Wi-Fi > Wi-Fi List**.



(1) Click **Add Wi-Fi**, enter the SSID and Wi-Fi password, select purpose and a frequency band.

×

Add

* SSID ?

Purpose ? General | IoT | Guest

Band ? 2.4G 5G 6G

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

Encryption Open Security 802.1x (Enterprise)

* Security ?

* Wi-Fi Password 👁

Advanced Settings

Cancel OK

(2) Click **Advanced Settings** to configure more Wi-Fi parameters.

----- Advanced Settings -----

SSID Encoding

Wi-Fi Standard

MLO When enabled, MLO-capable clients can connect to multiple frequency bands simultaneously, enhancing the user experience.

802.11r After this feature is enabled, roaming time is reduced to achieve fast transition.

Schedule

VLAN

Hide SSID The SSID is hidden and must be manually entered.

Client Isolation Prevent mutual access between clients connected to this SSID on this AP.

Layer 2 Isolation Prevent mutual access between clients connected to this SSID on all APs.

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

XPress The client will experience faster speed.

Layer 3 Roaming The client will keep the IP address unchanged on the Wi-Fi network.

LimitSpeed

[Do you want to edit RF parameters? Navigate to Radio Frequency for configuration.](#)

(3) Click **OK**.

 **Caution**

Modification will cause restart of the wireless configuration, resulting in logout of connected clients. Exercise caution when performing this operation.

Table 5-1 Wireless network configuration

| Parameter | Description |
|---------------------|---|
| SSID | Enter the name displayed when a wireless client searches for a wireless network. |
| Purpose | Set the Wi-Fi usage scenario. The options include General , IoT , and Guest . The system will recommend different Wi-Fi parameter combinations based on the selected purpose. |
| Band | <p>Set the band used by the Wi-Fi signal. The options are 2.4 GHz and 5 GHz. The 5 GHz band provides faster network transmission rate and less interference than the 2.4 GHz band, but is inferior to the 2.4 GHz band in terms of signal coverage range and wall penetration performance. Select a proper band based on actual needs. The default value is 2.4G + 5G, indicating that the device provides signals at both 2.4 GHz and 5 GHz bands.</p> <p>Compared with the 2.4 GHz and 5 GHz bands, the 6 GHz band supports a higher network transmission rate and is less susceptible to interference, but is inferior in signal coverage and through-wall penetration.</p> <hr/> <p> Note</p> <p>Only in networks with APs supporting the 6 GHz frequency band, you'll see an additional '6G' option in the frequency settings. The 6 GHz band provides faster data transmission rates, but it's worth noting that not all access devices may fully support this band. The RG-RAP73(HD) supports 6 GHz band.</p> <hr/> |
| Encryption | The encryption options for a Wi-Fi network include Open , Security , and 802.1x (Enterprise) . |
| Wi-Fi Password | When the Encryption is set to Security , you need to set the password for connecting to the wireless network. The password is a string of 8 to 63 characters. |
| Select server group | When the Encryption is set to 802.1x (Enterprise) , you need to configure a remote server set for authentication and authorization. |
| SSID Encoding | The SSID encoding standard is set to "UTF-8" by default when Chinese characters are included in the SSID. If the Chinese characters are garbled, you can choose GB2312 as the SSID encoding standard. |

| Parameter | Description |
|-------------------|--|
| Wi-Fi Standard | <p>The Wi-Fi standards include 802.11be (Wi-Fi 7), 802.11ax (Wi-Fi 6), Compatibility Mode or Auto. The final effective Wi-Fi standard depends on the support of Wi-Fi standards on each device. The latest standard is recommended. If there is a compatibility issue, try use an older standard. However, an old standard setting will affect the bandwidth.</p> |
| MLO | <p>When enabled, MLO-capable clients can connect to multiple frequency bands simultaneously, enhancing the user experience.</p> <hr/> <p> Specification</p> <ul style="list-style-type: none"> ● This feature is supported only when there are Wi-Fi 7 Aps running on ReyeeOS 2.230 or later version on the network. ● MLO and 802.11r are mutually exclusive features. Enabling MLO will automatically disable 802.11r. <hr/> |
| Wireless Schedule | <p>Specify the time periods during which Wi-Fi is enabled. After you set this parameter, users cannot connect to Wi-Fi in other periods.</p> |
| VLAN | <p>Set the VLAN to which the Wi-Fi signal belongs. You can choose from the available VLANs or click Add New VLAN, and go to the LAN Settings page to add a VLAN.</p> |
| Hide SSID | <p>Enabling the hide SSID function can prevent unauthorized user access to Wi-Fi, improving security. However, mobile phones or computers cannot find the SSID after this function is enabled. You must manually enter the correct name and password to connect to Wi-Fi. Record the current SSID before you enable this function.</p> |
| Client Isolation | <p>When enabled, devices connected to this Wi-Fi network under the same access point (AP) will be isolated from each other. This prevents end users from accessing other users on the same subnet, thereby enhancing security.</p> |
| Layer 2 Isolation | <p>When enabled, clients connected to this SSID are isolated from each other, and cannot access other clients connected to this SSID on all APs on Layer 2, thereby improving security.</p> <hr/> <p> Specification</p> <p>This feature is supported only in ReyeeOS 2.300 or later.</p> <hr/> |

| Parameter | Description |
|-----------------|--|
| Band Steering | After this function is enabled, 5G-capable clients select 5G Wi-Fi preferentially. You can enable this function only when Band is set to 2.4G + 5G . |
| XPress | After this function is enabled, the device sends game packets preferentially, providing more stable wireless network for games. |
| Layer-3 Roaming | After this function is enabled, clients keep their IP addresses unchanged when associating with the same Wi-Fi. This function improves the roaming experience of users in the cross-VLAN scenario. |
| 802.11r | Enabling the 802.11r function can shorten the roaming handover time. The 802.11r function is supported only when Encryption is set to Security or 802.1x (Enterprise) . Once 802.11r is enabled, the encryption type can only be WPA2-PSK or WPA2-802.1X. |
| LimitSpeed | After enabling Wi-Fi rate limiting, you can set the uplink and downlink rate limits for users. <ul style="list-style-type: none"> ● Rate Limit Per User: The rate limit applies to all clients connected to the SSID. ● Rate Limit All Users: All clients connected to the SSID share the configured rate limit equally. The rate limit of each client changes dynamically with the number of clients connected to the SSID. |

5.2.2 Configuring Guest Wi-Fi

Guest Wi-Fi, the Wi-Fi service provided for guests, is disabled by default. By default, user isolation is enabled for the guest Wi-Fi. That is, users connected to the guest Wi-Fi are isolated from each other and can only access the Internet through the Wi-Fi network, which improves security. Guest Wi-Fi can be disabled at a scheduled time. When the scheduled time arrives, the guest Wi-Fi is automatically disabled.

Choose **Network-Wide > Workspace > Wireless > Wi-Fi > Wi-Fi List**.

Click **Add Wi-Fi**, set the **Purpose** to **Guest**, and configure the Wi-Fi name and password. Click **Advanced Settings** to configure the effective time of the guest Wi-Fi and other Wi-Fi parameters. After the settings are saved, guests can connect to the Internet through the SSID and password. For details, see Section [5.2.1 Adding a Wi-Fi Network](#).

Add



* SSID ?

Purpose ? General | IoT | Guest

Band ? 2.4G 5G 6G

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

Encryption Open Security 802.1x (Enterprise)

* Security ?

* Wi-Fi Password

5.2.3 Managing Wi-Fi Networks

Choose **Network-Wide > Workspace > Wireless > Wi-Fi > Wi-Fi List**.

(1) Click **manage** to batch manage Wi-Fi networks.

Wi-Fi List Healthy Mode

Wi-Fi List Device Group: manage + Add Wi-Fi

| SSID ? | Band ? | Security ? | Hidden | VLAN ID | Action |
|---------------------|---|-------------------------|--------|--------------|---|
| @Ruijie-m0848 | 2.4G 5G | OPEN(Open) | No | Default VLAN | Edit Delete |
| test | 2.4G 5G | OPEN(Open) | No | Default VLAN | Edit Delete |

Up to 8 SSIDs can be added.

(2) Batch manage Wi-Fi networks.

- o Batch enable Wi-Fi networks: Select the desired Wi-Fi networks, and click **Enable**.

Wi-Fi List Device Group: Enable Disable Delete Exit + Add Wi-Fi

| <input type="checkbox"/> | SSID ? | Band ? | Security ? | Hidden | VLAN ID |
|-------------------------------------|---------------------|---|-------------------------|--------|--------------|
| <input checked="" type="checkbox"/> | @Ruijie-m0848 | 2.4G 5G | OPEN(Open) | No | Default VLAN |
| <input type="checkbox"/> | test | 2.4G 5G | OPEN(Open) | No | Default VLAN |

Up to 8 SSIDs can be added.

- o Batch disable Wi-Fi networks: Select the desired Wi-Fi networks, and click **Disable**.

Wi-Fi List Device Group: Default Enable Disable Delete Exit + Add Wi-Fi

| <input checked="" type="checkbox"/> | SSID | Band | Security | Hidden | VLAN ID |
|-------------------------------------|---------------|---------|------------|--------|--------------|
| <input checked="" type="checkbox"/> | @Ruijie-m0848 | 2.4G 5G | OPEN(Open) | No | Default VLAN |
| <input checked="" type="checkbox"/> | test | 2.4G 5G | OPEN(Open) | No | Default VLAN |

Up to 8 SSIDs can be added.

- o Batch delete Wi-Fi networks: Select the desired Wi-Fi networks, and click **Delete**.

Wi-Fi List Device Group: Default Enable Disable Delete Exit + Add Wi-Fi

| <input checked="" type="checkbox"/> | SSID | Band | Security | Hidden | VLAN ID |
|-------------------------------------|---------------|---------|------------|--------|--------------|
| <input checked="" type="checkbox"/> | @Ruijie-m0848 | 2.4G 5G | OPEN(Open) | No | Default VLAN |
| <input checked="" type="checkbox"/> | test | 2.4G 5G | OPEN(Open) | No | Default VLAN |

Up to 8 SSIDs can be added.

- (3) Click **Exit** to exit Wi-Fi network batch management.

Wi-Fi List Healthy Mode

Wi-Fi List Device Group: Default Enable Disable Delete Exit + Add Wi-Fi

| <input type="checkbox"/> | SSID | Band | Security | Hidden | VLAN ID |
|--------------------------|--------|---------|------------|--------|---------------------|
| <input type="checkbox"/> | LJW_55 | 2.4G | WPA2-PSK | No | The same VLAN as AP |
| <input type="checkbox"/> | 1 | 2.4G 5G | OPEN(Open) | No | The same VLAN as AP |
| <input type="checkbox"/> | TEST | 2.4G 5G | OPEN(Open) | No | The same VLAN as AP |

Up to 8 SSIDs can be added.

5.3 Healthy Mode

Choose **Network-Wide > Workspace > Wireless > Wi-Fi > Healthy Mode**.

Turn on healthy mode and select a wireless schedule for the mode.

After the healthy mode is enabled, the RF transmit power and Wi-Fi coverage range of the device are reduced in the schedule. This may lead to weak signals and network freezing. You are advised to disable healthy mode or set the wireless schedule to the idle periods.

Healthy Mode Device Group: Default

Enable

Effective Time ? All Time

Save

5.4 RF Settings

5.4.1 Configuring Global Radio Settings

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

The device can detect the surrounding wireless environment upon power-on and select proper configuration. However, network freezing caused by wireless environment changes cannot be prevented. You can analyze the wireless environment around the APs and routers and manually select proper parameters.

Caution

Modification will cause restart of the wireless configuration, resulting in logout of connected clients. Exercise caution when performing this operation.

Radio Setting Device Group: Default [Not solved yet? Click here to access the Network Optimization page for automatic optimization.](#)

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

Country/Region United States (US)

Radio Parameters

2.4G

5G

6G

Global Radio Settings

Channel Width ? Auto

Multicast Rate (Mbps) ? Auto

Client Count Limit

Disconnection Threshold ? Disable -85dBm -65dBm

Save

Table 5-2 RF configuration

| Parameter | Description |
|--------------------------|--|
| Country/Region | The Wi-Fi channels stipulated by each country may be different. To ensure that clients can find the Wi-Fi signal, select the country or region where the device is located. |
| 2.4G/5G/6G Channel Width | <p>A lower bandwidth indicates more stable network, and a higher bandwidth indicates easier interference. In case of severe interference, select a relatively low bandwidth to prevent network freezing to certain extent.</p> <ul style="list-style-type: none"> ● The 2.4 GHz band supports the 20 MHz and 40 MHz bandwidths. ● The 5 GHz band supports the 20 MHz, 40 MHz, 80 MHz and 160MHz bandwidths. ● The 6 GHz band supports the 20 MHz, 40 MHz, 80 MHz, 160MHz and 320 MHz bandwidths. <p>By default, the value is Auto, indicating that the bandwidth is selected automatically based on the environment.</p> |
| Multicast Rate (Mbps) | If the multicast rate is too high, the packet loss rate of multicast packets may increase. If the multicast rate is too low, the radio interface may become busy. When network stalling is serious, you are advised to configure a high multicast rate. When network stalling is minor, configure a medium multicast rate. |
| Client Count Limit | If a large number of users access the AP or router, the wireless network performance of the AP or router may be degraded, affecting users' Internet access experience. You can toggle on the Client Count Limit toggle switch to set a client limit. After you set this parameter, new user access is prohibited when the number of access users reaches the specified value. If the clients require high bandwidth, you can adjust this parameter to a smaller value. You are advised to keep the default value unless otherwise specified. |
| Disconnection Threshold | <p>When multiple Wi-Fi signals are available, you can set this parameter to optimize the wireless signal quality to some extent. When a client is far away from the wireless device, the Wi-Fi connection is disconnected when the wireless signal strength of the end user is lower than the kick-off threshold. In this case, the client has to select a nearer wireless signal.</p> <p>The client is prone to be kicked off if the kick-off threshold is high. To ensure that the client can normally access the Internet, you are advised to set this parameter to Disable or a value smaller than -75 dBm.</p> |

Note

- Wireless channels available for your selection are determined by the country code. Select the country code based on the country or region of your device.
- Channel, transmit power, and roaming sensitivity cannot be set globally, and the configuration is valid only on the current device. To modify related configuration for other devices, configure these devices separately.

5.4.2 Configuring Standalone Radio Settings

Choose **One-Device > Gateway > Config > WLAN > Radio Setting**.

In high-density client environments, you can fine-tune radio settings to alleviate radio frequency interference resulting from too many access points in close proximity. This include disabling the radio of neighboring APs that are causing significant interference, aiming to minimize signal conflicts and enhance the overall quality and stability of wireless communication.

In environments like conference rooms, offices, and smart homes, disabling the 2.4GHz radio of specific APs can enhance the performance of wireless devices such as mice, keyboards, Bluetooth and Zigbee devices when they experience signal interference or operational lag.

The **Radio Switch** is enabled by default, and can be disabled as required.

Radio Setting

Radio Parameters

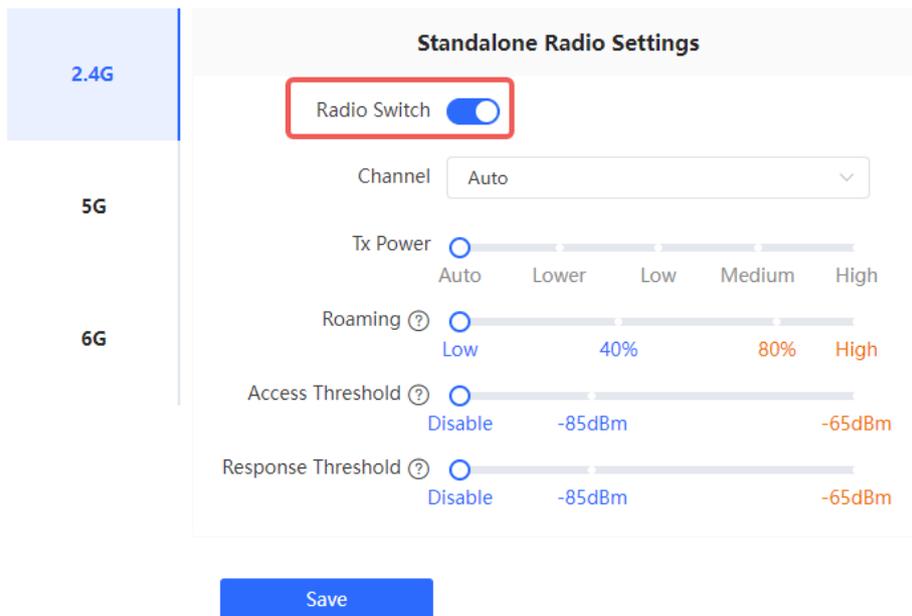


Table 5-3 Standalone Radio Settings configuration

| Parameter | Description |
|--------------------|---|
| 2.4G/5G/6G Channel | <p>Before you set the channel, install WiFi Moho or another app with the Wi-Fi scan function on your mobile phone to view the interference analysis result and find the optimal channel.</p> <p>Select the optimal channel according to the analysis result. More wireless devices in the channel indicate larger interference.</p> |

| Parameter | Description |
|--------------------|---|
| Tx Power | Larger transmit power indicates stronger wireless signal strength, wider coverage range, and larger interference to the surrounding wireless network. When a large number of APs or routers are deployed, you can appropriately adjust the transmit power to a lower value. By default, the wireless transmit power is automatically adjusted according to the environment. You are advised to retain the default configuration. |
| Roaming | Roaming sensitivity specifies the speed at which a moving wireless client connects to the optimal wireless signal. A high roaming sensitivity indicates a narrow coverage range of the wireless signal. When the client is moving and multiple Wi-Fi signals are available, you can increase the roaming sensitivity to improve the wireless signal quality. You are advised to retain the default configuration. |
| Access Threshold | When the wireless signal of the end user is lower than the access threshold set on the device, the client cannot detect the wireless signal of the device. |
| Response Threshold | When the wireless signal of the end user is lower than the response RSSI threshold configured on the device, the client cannot detect the wireless signal of the device. The smaller the response RSSI threshold is configured, the less the environmental factors interfere with the AP. |

5.5 Configuring Wi-Fi Blocklist or Allowlist

5.5.1 Overview

You can configure the global or SSID-based blocklist and allowlist. The MAC address supports full match and OUI match.

Wi-Fi blocklist: Clients in the Wi-Fi blocklist are prevented from accessing the Internet. Clients that are not added to the Wi-Fi blocklist are free to access the Internet.

Wi-Fi allowlist: Only clients in the Wi-Fi allowlist can access the Internet. Clients that are not added to the Wi-Fi allowlist are prevented from accessing the Internet.

Caution

If the allowlist is empty, the allowlist does not take effect. In this case, all clients are allowed to access the Internet.

5.5.2 Configuring a Global Blocklist/Allowlist

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

Select the blocklist or allowlist mode and click **Add** to configure a blocklist or allowlist client. In the **Add** dialog box, enter the **Device Name**, **Match Type** and **MAC Address** of the target client and click **OK**. If a client is already

associated with the router, its MAC address will pop up automatically. Click the MAC address directly for automatic input. All clients in the blocklist will be forced offline and not allowed to access the Wi-Fi network. The global blocklist and allowlist settings take effect on all Wi-Fi networks of the router.

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"/> | test ↗ | 06:ea:65:38:23:11 | Edit Delete |

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

Add ×

Device Name ?

Match Type Full Prefix (OUI)

* MAC Address

If you delete a client from the blocklist, the client will be allowed to connect to the Wi-Fi network.

If you delete a client from the allowlist, the client will be forced offline and denied access to the Wi-Fi network.

Blocked WLAN Clients + Add Delete Selected

| <input type="checkbox"/> | Device Name | MAC Address | Action |
|--------------------------|------------------------|-------------------|--------------------|
| <input type="checkbox"/> | test ↗ | 06:ea:65:38:23:11 | Edit Delete |

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

5.5.3 Configuring an SSID-based Blocklist/Allowlist

Choose **Network-Wide > Workspace > Wireless > Blocklist and Allowlist > SSID-Based Blocklist/ Allowlist**.

Select a target Wi-Fi network from the left column, select the blocklist or allowlist mode, and click **Add** to configure a blocklist or allowlist client. The SSID-based blocklist and allowlist will restrict the client access to the specified Wi-Fi.

Blocklist/Allowlist is used to allow or reject a client's request to connect to the Wi-Fi network.

Note: OUI matching rule and SSID-based blocklist/allowlist are supported by only RAP Net and P32 (and later versions).

Rule:

- In the Blocklist mode, the clients in the blocklist are not allowed to connect to the Wi-Fi network.
- In the Allowlist mode, only the clients in the allowlist are allowed to connect to the Wi-Fi network.

Device Group: Default ▾

SSID-Based Blocklist/Allowlist

@Ruijie-m6649

test

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

| | Device Name | MAC Address | Action |
|---------|-------------|-------------|--------|
| ❑ | | | |
| No Data | | | |

Up to 512 members can be added. Total 0 < 1 > 10/page ▾

5.6 Configuring AP Load Balancing

5.6.1 Overview

The AP load balancing function is used to balance the load of APs in the wireless network. When APs are added to a load balancing group, clients will automatically associate with the APs with light load when the APs in the group are not load balanced. AP load balancing supports two modes:

- **Client Load Balancing:** The load is balanced according to the number of associated clients. When a large number of clients have been associated with an AP and the count difference to the AP with the lightest load has reached the specified value, the client can only associate with another AP in the group.
- **Traffic Load Balancing:** The load is balanced according to the traffic on the APs. When the traffic on an AP is large and the traffic difference to the AP with the lightest load has reached the specified value, the client can only associate with another AP in the group.

Example: Add AP1 and AP2 into a group and select client load balancing. Set both the client count threshold and difference to 3. AP1 is associated with 5 clients and AP2 is associated with 2 clients, triggering load balancing. New clients' attempt to associate to AP1 will be denied, and therefore they can associate only with AP2.

After a client request is denied by an AP and it fails to associate with another AP in the group, the client will keep trying to associate with this AP. If the client attempts reach the specified value, the AP will permit connection of this client, ensuring that the user can normally access the Internet.

5.6.2 Configuring Client Load Balancing

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

Click **Add**. In the dialog box that appears, set **Type** to **Client Load Balancing**, and configure **Group Name**, **Members**, and **Rule**.

Load Balancing

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

By grouping APs in the same area into a load balancing group, they can collaborate to control the access of wireless clients and to achieve optimal traffic distribution.
 For example, when AP1 and AP2 are added to the same load balancing group, with the load balancing type set to Client Load Balancing and a strategy to trigger load balancing when one AP has 3 clients and the load-balancing threshold is 3, if AP1 has 5 clients and AP2 has 2 clients, any new client trying to connect to AP1 will be denied access and redirected to AP2, achieving load balancing between the two APs.

| <input type="checkbox"/> | Group Name | Type | Rule | Members | Action |
|--------------------------|------------|------|------|---------|--------|
| No Data | | | | | |

Up to 32 entries can be added.

Add



* Group Name

* Type

* Rule
 Load balancing is triggered when the number of clients connected to an AP in a group reaches and the client count difference between the AP and other APs in the group exceeds . Once a client has been denied access to an AP in the group for a total of 10 attempts, it will be allowed to connect to that AP again upon the next attempt.

* Members

Table 5-4 Client load balancing configuration

| Parameter | Description |
|------------|--|
| Group Name | Enter the name of the AP load balancing group. |
| Type | Select Client Load Balancing . |

| Parameter | Description |
|-----------|---|
| Rule | <p>Configure a detailed load balancing rule, including the maximum number of clients allowed to associate with an AP, the difference between the currently associated client count and client count on the AP with the lightest load, and the number of attempts to the AP with full load.</p> <p>By default, when an AP is associated with 3 clients and the difference between the currently associated client count and client count on the AP with the lightest load reaches 3, clients can associate only to another AP in the group. After a client association is denied by an AP for 10 times, the client will be allowed to associate to the AP upon the next attempt.</p> |
| Members | Specify the APs to be added to the AP load balancing group. |

5.6.3 Configuring Traffic Load Balancing

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

Click **Add**. In the dialog box that appears, set **Type** to **Traffic Load Balancing**, and configure **Group Name**, **Members**, and **Rule**.

Add ×

* Group Name

* Type Traffic Load Balancing ▼

* Rule

Load balancing is triggered when the traffic on an AP in a group reaches *100Kbps, and the traffic difference between the AP and other APs in the group exceeds x 100Kbps. Once a client has been denied access to an AP in the group for a total of 10 attempts, it will be allowed to connect to that AP again upon the next attempt.

* Members Enter an AP name or SN. ▼

Cancel
OK

Table 5-5 Traffic load balancing configuration

| Parameter | Description |
|------------|---|
| Group Name | Enter the name of the AP load balancing group. |
| Type | Select Traffic Load Balancing . |
| Rule | <p>Configure a detailed load balancing rule, including the maximum traffic allowed on an AP, the difference between the current traffic and the traffic on the AP with the lightest load, and the number of attempts to the AP with full load.</p> <p>By default, when the traffic load on an AP reaches 500 Kbit/s and the difference between the current traffic and the traffic on the AP with the lightest load reaches 500 Kbps, clients can associate only to another AP in the group. After a client association is denied by an AP for 10 times, the client will be allowed to associate to the AP upon the next attempt.</p> |
| Members | Specify the APs to be added to the AP load balancing group. |

5.7 Configuring Wireless Rate Limiting

5.7.1 Overview

The device supports four rate limiting modes: client-based rate limiting, SSID-based rate limiting, AP-based rate limiting, and packet-based rate limiting. For the same client, if multiple rate limiting modes are configured, the priority order is as follows: client-based rate limiting > SSID-based rate limiting > AP-based rate limiting.

- Client-based rate limiting: This function allows you to limit the rate based on the MAC address of the client, so as to limit or guarantee the bandwidth required by specific clients.
- SSID-based rate limiting: This function provides two rate limiting modes for a specified SSID: **Rate Limit Per User** and **Rate Limit All Users**. **Rate Limit Per User** means that all clients connected to the SSID use the same rate limit. **Rate Limit All Users** means that the configured rate limit value is evenly allocated to all clients connected to the SSID. The rate limit value of each client dynamically changes with the number of clients connected to the SSID.
- AP-based rate limiting: This function limits the client rates based on the whole network. All clients connected to the network will work according to the configured rate limit value.
- Packet-based rate limiting: This function limits the client rates based on the downlink broadcast and multicast packets. The device supports rate limiting for specific broadcast packets (such as ARP and DHCP), multicast packets (such as MDNS and SSDP), or all types of broadcast and multicast packets. If network stalling remains during network access and there is no client with large traffic, you are advised to adjust the rate between 1 kbps and 512 Kbps.

5.7.2 Configuration Steps

1. Configuring Client-based Rate Limiting

Choose **Network-Wide > Workspace > Wireless > Rate Limiting > Client-based Rate Limiting**.

- (1) Enable Wireless Rate Limiting.
- (2) Click **Add**. In the dialog box that appears, set the MAC address and uplink and downlink rate limit values of the client, and click **OK**.

Wireless Rate Limiting

[Client-based Rate Limiting](#) SSID-based Rate Limiting AP-based Rate Limiting Packet-based Rate Limiting

i The rate limiting mode based on wireless clients can limit or provide the bandwidth for specific clients.

Client-based Rate Limiting [+ Add](#) [Delete Selected](#)

| <input type="checkbox"/> | Client MAC | Uplink Rate Limit | Downlink Rate Limit | Remarks | Action |
|--------------------------|------------|-------------------|---------------------|---------|--------|
| No Data | | | | | |

Up to 512 entries can be added. Total 0 [1](#) 10/page

Add ×

* Client MAC

Uplink Rate
Limit Current: Kbps. Range: 1-1700000 Kbps

Downlink Rate
Limit Current: Kbps. Range: 1-1700000 Kbps

Remarks

2. Configuring SSID-based Rate Limiting

Choose **Network-Wide > Workspace > Wireless > Rate Limiting > SSID-based Rate Limiting**.

- (1) Enable Wireless Rate Limiting.

- (2) Click **Edit** in the **Action** column of the target SSID. In the dialog box that appears, set the uplink and downlink rate limit modes and values, and click **OK**.

Wireless Rate Limiting

Client-based Rate Limiting SSID-based Rate Limiting AP-based Rate Limiting Packet-based Rate Limiting

i This function provides rate limit per user and dynamic rate limiting for a specified SSID. Rate Limit per User indicates that all clients connected to the SSID use the same rate limit. Rate Limit All Users indicates that all clients connected to the SSID share the rate limit in average. The priority of this function is lower than that of client-based rate limiting.

SSID-based Rate Limiting Device Group: [Are you sure you want to add a Wi-Fi? Click to go.](#)

| SSID | Uplink Rate Limit | Downlink Rate Limit | Action |
|---------------|-------------------|---------------------|--|
| @Ruijie-m6649 | No Limit | No Limit | Edit Disable |
| test | No Limit | No Limit | Edit Disable |

Edit



Uplink Rate Limit (?) Rate Limit Per User Rate Limit All Users

Rate Limit
Current: Kbps. Range: 1-1700000 Kbps

Downlink Rate Limit (?) Rate Limit Per User Rate Limit All Users

Rate Limit
Current: Kbps. Range: 1-1700000 Kbps

3. Configuring AP-based Rate Limiting

Choose **Network-Wide > Workspace > Wireless > Rate Limiting > AP-based Rate Limiting**.

- (1) Enable Wireless Rate Limiting.
- (2) Set the uplink and downlink rate limit modes to **Rate Limit Per User**, configure the rate limit values, and click **OK**.

Wireless Rate Limiting

Client-based Rate Limiting SSID-based Rate Limiting AP-based Rate Limiting Packet-based Rate Limiting

i This function provides client rate limiting based on the whole network. All devices connected to the network use the preset rate limiting value.
The priority of this function is lower than that of client-based rate limiting and SSID-based rate limit per user.

AP-based Rate Limiting

Uplink Rate Limit [?] No Limit Rate Limit Per User

Kbps
Current: Kbps. Range: 1-1700000 Kbps

Downlink Rate Limit No Limit Rate Limit Per User

Kbps
Current: Kbps. Range: 1-1700000 Kbps

4. Configuring Packet-based Rate Limiting

Choose **Network-Wide > Workspace > Wireless > Rate Limiting > Packet-based Rate Limiting**.

- (1) Enable Wireless Rate Limiting.
- (2) Select the specific type of packets for rate limiting, configure the rate limit value, and click **Save**.

Wireless Rate Limiting

Client-based Rate Limiting SSID-based Rate Limiting AP-based Rate Limiting Packet-based Rate Limiting

i This function allows users to limit the downlink rate for broadcast and multicast packets. If the internet access is still slow and unstable when no client needs large amounts of traffic, you are advised to set the rate ranging from 1 Kbps to 512 Kbps. Smaller rate brings better network improvement.
Tip: A lower rate limit brings better network improvement but may affect client services. A higher rate limit indicates poorer network improvement.

Packet-based Rate Limiting

Broadcast Rate Limiting Disable Limit All Limit Part

ARP Packet DHCP Packet

Multicast Rate Limiting Disable Limit All Limit Part

MDNS Packet SSDP Packet

* Rate Limit Kbps
Current: 0 Kbps. Range: 1-1700000 Kbps

5.8 Wireless Network Optimization

5.8.1 Wireless Network Optimization 2.0 Version

 **Specification**

This feature is supported only on RG-EG105GW-X.

1. One-Click Wireless Optimization

Select the optimization mode, the system automatically optimize the wireless network.

 **Caution**

- WIO is supported only in the self-organizing network mode.
- The client may be offline during the optimization process. The configuration cannot be rolled back once optimization starts. Therefore, exercise caution when performing this operation.

Choose **Network-Wide > Workspace > WLAN Optimization > Network Optimization**.

(1) Select the optimization mode. Then, click **OK** to optimize the wireless network.



Wireless Intelligent Optimization

In a networking environment, WIO can help maximize wireless performance by optimizing your network.

Optimization

Optimization Quick optimization Deep optimization mode

Estimated Time

180s Environment scan + 3 minute Optimization

Instructions

- Upgrade all APs to the latest version for optimal network optimization.
- WIO is not supported on APs without an IP address.
- WIO only supports 20 MHz, 40 MHz, and 80 MHz channel bandwidths at the moment.
- Please perform optimization after all APs in the target area are online.

OK

Table 5-6 Description of Tuning Mode

| Parameter | Description |
|--------------|---|
| Quick tuning | In this mode, external interference and bandwidth are not considered. A quick optimization is performed to optimize channel, power, and management frame power. |

| Parameter | Description |
|-------------|---|
| Deep tuning | <p>In this mode, external interference and bandwidth are considered. A deep optimization is performed to optimize channel, power, and management frame power. Click to expand Advanced Settings to configure the Scan Time, Roaming Sensitivity, Transmit Power, Channel Width and channels.</p> <ul style="list-style-type: none"> ● Scan Time: Indicates the time for scanning channels during the optimization. ● Roaming Sensitivity: You can adjust the roaming sensitivity to balance the roaming performance and connection stability of the device during roaming. ● Transmit Power: You can adjust the transmit power of wireless devices to optimize the performance and coverage of the Wi-Fi network. ● 2.4G <ul style="list-style-type: none"> ○ Channel Width: Indicates the channel bandwidth. The channel bandwidth will be calculated by the system if Default is selected. ○ Selected channels: Indicates the channels to be optimized. ● 5G <ul style="list-style-type: none"> ○ Channel Width: Indicates the channel bandwidth. The channel bandwidth will be calculated by the system if Default is selected. ○ Selected channels: Indicates the channels to be optimized. |

(2) (Optional) When the **Optimization Mode** is configured as **Deep tuning**, expand the **Advanced Settings** to set the Scan Time, Roaming Sensitivity, Transmit Power, Channel Width and channels.

----- Advanced Settings -----

Scan time ▾

Roaming

Sensitivity

Transmit Power

2.4G

Channel Width ▾

Selected channels

| | | | |
|------|-------|-------|------|
| CH.1 | CH.2 | CH.3 | CH.4 |
| CH.5 | CH.6 | CH.7 | CH.8 |
| CH.9 | CH.10 | CH.11 | |

[Restore to Default](#)

5G

Channel Width ▾

Selected channels

| | | | |
|-----------------------|--------|--------|-------|
| CH.36 | CH.40 | CH.44 | CH.48 |
| CH.52(Radar channel) | | | |
| CH.56(Radar channel) | | | |
| CH.60(Radar channel) | | | |
| CH.64(Radar channel) | | | |
| CH.100(Radar channel) | | | |
| CH.104(Radar channel) | | | |
| CH.108(Radar channel) | | | |
| CH.112(Radar channel) | | | |
| CH.116(Radar channel) | | | |
| CH.120(Radar channel) | | | |
| CH.124(Radar channel) | | | |
| CH.128(Radar channel) | | | |
| CH.132(Radar channel) | | | |
| CH.136(Radar channel) | | | |
| CH.140(Radar channel) | CH.149 | | |
| CH.153 | CH.157 | CH.161 | |
| CH.165 | | | |

[Restore to Default](#)

There are devices supporting multiple 5 GHz radios on the network, each with its own channel range. You are advised to optimize at least one channel for each 5 GHz radio. Otherwise, optimization for that radio will be skipped.

(3) Confirm the tips, and Click **OK**.

Tips ×

During optimization, the APs may switch channels and collect data, which may result in temporary disconnection and affect user experience. This situation may last for some time. You are advised to enable scheduled optimization if you require an Internet connection for the time being.

- (4) After optimization starts, please wait patiently until optimization is complete. After optimization is complete, you can click **Cancel Optimization** to restore the radio parameters to the default values.

Click **Optimization Record** to view the changes in channel width, channel, and transmit power of the APs before and after the optimization.

Finish

Completion time: 2024-09-30 14:11:11
 Optimization mode Quick optimization
 Time consumed: 2 minutes 40 seconds. Optimized 14 APs, resolved severe interference of 14 APs, reduced channel interference by 52.69%, and improved user experience by 48.72%.

- (5) Click **Optimization Record** Tab to view details of the latest optimization.

? Last Optimized:2024-09-30 14:11:11
 Time consumed: 2 minutes 40 seconds. Optimized 14 APs, resolved severe interference of 14 APs, reduced channel interference by 52.69%, and improved user experience by 48.72%.

Optimization Details Enter AP name/SN 2.4G **5G** 5G-2

| Hostname | Band | SN | Channel Width (Before/After) | Channel (Before/After) | Transmit Power (Before/After) | Sensitivity (Before/After) |
|----------|------|----|------------------------------|------------------------|-------------------------------|----------------------------|
| RAP2261E | 5G | | 40 | 149->116 | 100 | 90 |
| Ruijie | 5G | | 40 | 36->60 | 100 | 90 |
| Ruijie | 5G | | 40 | 157 | 100 | 84 |
| Ruijie | 5G | | 40 | 116->36 | 100 | 90 |
| Ruijie | 5G | | 40 | 44->132 | 100 | 80 |
| Ruijie | 5G | | 40 | 153->100 | 100 | 74 |
| Ruijie | 5G | | 40 | 100 | 100 | 90 |
| Ruijie | 5G | | 160->40 | 60->44 | 100 | 90 |
| Ruijie | 5G | | 40 | 157 | 100 | 90 |
| Ruijie | 5G | | 40 | 132->52 | 100 | 90 |

Total 14 1 2 10/page

2. Scheduled Wireless Optimization

You can configure scheduled optimization to optimize the network at the specified time. You are advised to set the scheduled optimization time to daybreak or the idle periods.

Caution

Clients may be kicked offline during optimization and the configuration cannot be rolled back after optimization starts. Exercise caution when performing this operation.

Choose **Network-Wide > Workspace > WLAN Optimization > Scheduled Optimization**.

 Optimize the network performance at a scheduled time for a better user experience.

Enable

Day

Time :

Schedule Weekly One time

Optimization mode Quick optimization Deep optimization

----- [Advanced Settings](#) -----

- (1) Configure the scheduled time.
- (2) Select the optimization mode.
- (3) (Optional) When the **Optimization Mode** is configured as **Deep tuning**, expand the **Advanced Settings** to set the scanning time, roaming sensitivity, transmit power, channel bandwidth and selected channels.

----- Advanced Settings -----

Scan time

Roaming

Sensitivity

Transmit Power

2.4G

Channel Width

Selected channels

| | | | |
|-------------------------------|--------------------------------|--------------------------------|-------------------------------|
| <input type="checkbox"/> CH.1 | <input type="checkbox"/> CH.2 | <input type="checkbox"/> CH.3 | <input type="checkbox"/> CH.4 |
| <input type="checkbox"/> CH.5 | <input type="checkbox"/> CH.6 | <input type="checkbox"/> CH.7 | <input type="checkbox"/> CH.8 |
| <input type="checkbox"/> CH.9 | <input type="checkbox"/> CH.10 | <input type="checkbox"/> CH.11 | |

[Restore to Default](#)

5G

Channel Width

Selected channels

| | | | |
|--|---------------------------------|---------------------------------|--------------------------------|
| <input type="checkbox"/> CH.36 | <input type="checkbox"/> CH.40 | <input type="checkbox"/> CH.44 | <input type="checkbox"/> CH.48 |
| <input type="checkbox"/> CH.52(Radar channel) | | | |
| <input type="checkbox"/> CH.56(Radar channel) | | | |
| <input type="checkbox"/> CH.60(Radar channel) | | | |
| <input type="checkbox"/> CH.64(Radar channel) | | | |
| <input type="checkbox"/> CH.100(Radar channel) | | | |
| <input type="checkbox"/> CH.104(Radar channel) | | | |
| <input type="checkbox"/> CH.108(Radar channel) | | | |
| <input type="checkbox"/> CH.112(Radar channel) | | | |
| <input type="checkbox"/> CH.116(Radar channel) | | | |
| <input type="checkbox"/> CH.120(Radar channel) | | | |
| <input type="checkbox"/> CH.124(Radar channel) | | | |
| <input type="checkbox"/> CH.128(Radar channel) | | | |
| <input type="checkbox"/> CH.132(Radar channel) | | | |
| <input type="checkbox"/> CH.136(Radar channel) | | | |
| <input type="checkbox"/> CH.140(Radar channel) | <input type="checkbox"/> CH.149 | | |
| <input type="checkbox"/> CH.153 | <input type="checkbox"/> CH.157 | <input type="checkbox"/> CH.161 | |
| <input type="checkbox"/> CH.165 | | | |

[Restore to Default](#)

There are devices supporting multiple 5 GHz radios on the network, each with its own channel range. You are advised to optimize at least one channel for each 5 GHz radio. Otherwise, optimization for that radio will be skipped.

(4) Click **Save**.

5.8.2 Wireless Network Optimization 1.0 Version

Specification

This feature is supported only on RG-EG105GW(T).

Choose **Network-Wide > Workspace > WLAN Optimization > Network Optimization**.

Tick **I have read the notes** and click **Network Optimization** to optimize the wireless network. You can configure scheduled optimization to optimize the network at the specified time. You are advised to set the scheduled optimization time to midnight or other idle periods.

Caution

- This feature is supported only in the self-organizing network mode.
- The client may be offline during the optimization process. The configuration cannot be rolled back once optimization starts. Therefore, exercise caution when performing this operation.

Network Optimization Optimization Record 802.11k/v Roaming Optimization

Start Scanning Optimizing Finish

Description:
This feature will optimize the self-organizing network to maximize the WLAN performance. Please make sure that all APs have been online.
If WIO is enabled on the device supporting Wi-Fi roaming optimization (802.11k/v), this feature is enabled at the same time.

Notes:
1. During network optimization, the APs will switch channels, forcing the clients to go offline. The process will last for a while, subject to the quantity of devices. It is recommended you enable network optimization at night.
2. If dynamic channel allocation is running in the backend, network optimization will fail. Please try again later.
3. Network Optimization is not supported by the device without an IP address.
4. The configuration cannot be rolled back once optimization starts.

I have read the notes.

[Network Optimization](#)

After the optimization starts, please wait patiently until the optimization is complete.

Network Optimization Optimization Record 802.11k/v Roaming Optimization

Start Scanning Optimizing Finish

Finish

Optimization finished on 2023-12-12 09:32:17
Time: 41 seconds

[View Details](#) [Back](#) [Cancel Optimization](#)

Click **Optimization Record** to view details of the latest optimization.

i Last Optimized:2023-12-12 09:32:17
 You have optimized 2 APs and improved the performance by 85.83%!

[Details](#)

| Hostname | Band | SN | Channel (Before/After) | Channel Width (Before/After) | Transmit Power (Before/After) | Sensitivity (Before/After) | CCI (Before/After) | ACI (Before/After) | Interference (Before/After) |
|----------|------|-------------------|------------------------|------------------------------|-------------------------------|----------------------------|--------------------|--------------------|-----------------------------|
| Ruijie | 2.4G | G1PQ5AM05 3417 | 11/1 | 20 | auto/75 | 0/98 | 1/0 | 0 | 1/0 |
| Ruijie | 5G | G1PQ5AM05 3417 | 36/149 | 80 | auto/100 | 0/94 | 1/0 | 0 | 1/0 |
| Ruijie | 2.4G | G1PQ5AM06 3877 | 11 | 20 | 100/75 | 0/98 | 1/0 | 0 | 1/0 |
| Ruijie | 5G | G1PQ5AM06 3877 | 44/36 | 80 | 100 | 0/94 | 1/0 | 0 | 1/0 |

Total 4 < **1** > 10/page

The wireless optimization function supports scheduled network optimization, which optimizes the network at a specified time. You are advised to set the scheduled optimization time to midnight or other idle periods.

Scheduled Optimization

i Optimize the network performance at a scheduled time for a better user experience.

Enable

Day Mon ▼

Time 17 ▼ : 20 ▼

Save

5.8.3 Wi-Fi Roaming Optimization (802.11k/v)

Wi-Fi roaming is further optimized through the 802.11k/802.11v protocol. Smart endpoints compliant with IEEE 802.11k/v can switch association to the access points with better signal and faster speed, thereby ensuring high-speed wireless connectivity.

To ensure high quality of smart roaming service, the WLAN environment will be automatically scanned when Wi-Fi roaming optimization is first enabled.

Choose **Network-Wide > Workspace > WLAN Optimization > 802.11k/v Roaming Optimization**.

Start Scanning Optimizing Finish

Description:
The Wi-Fi roaming is further optimized through the 802.11k/v protocol. Smart clients compliant with 802.11k/v can switch to the APs with better signal and faster speed during the roaming process, ensuring high-speed wireless connectivity.
To ensure smart roaming effect, the WLAN environment will be auto scanned when Wi-Fi roaming optimization is first enabled.

Notes:
During the WLAN environment scanning, the APs will switch channels, forcing the clients to go offline. The process will last for 2 minutes.

Optimization Mode Performance-prior Roaming-prior

Enable

Caution

During the optimization, the clients may be forced offline. Please proceed with caution.

Select **Optimization Mode** and click **Enable**, then the optimization starts.

Start Scanning Optimizing Finish

Optimization is enabled.

Optimization finished on 2023-12-08 13:32:29
Time: 36 seconds
To ensure smart roaming effect, please [Click Here](#) to scan the WLAN environment again if the topology changes.

Disable

5.8.4 Configuring IGMP Snooping

1. IGMP Snooping

IGMP snooping allows switches to listen for and analyze IGMP (Internet Group Management Protocol) messages in order to determine which switch ports are connected to hosts that are interested in specific multicast groups. By forwarding multicast traffic only to these ports, IGMP snooping helps to prevent unnecessary flooding of multicast traffic to all ports on the network, thereby improving network efficiency and security.

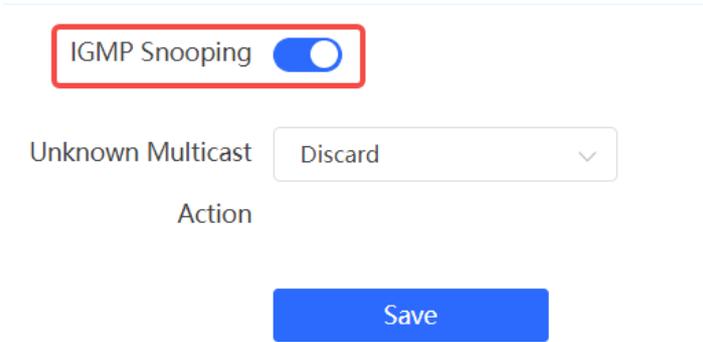
2. Unknown Multicast Packet

Unknown multicast packets are multicast packets transmitted on a network, whose destination addresses are multicast group addresses that are not learned or identified by the switch.

3. Configuration Steps

Choose **Network-Wide > Workspace > WLAN Optimization > Advanced**.

Enable **IGMP Snooping**, select the action for unknown multicast packets, and click **Save**.



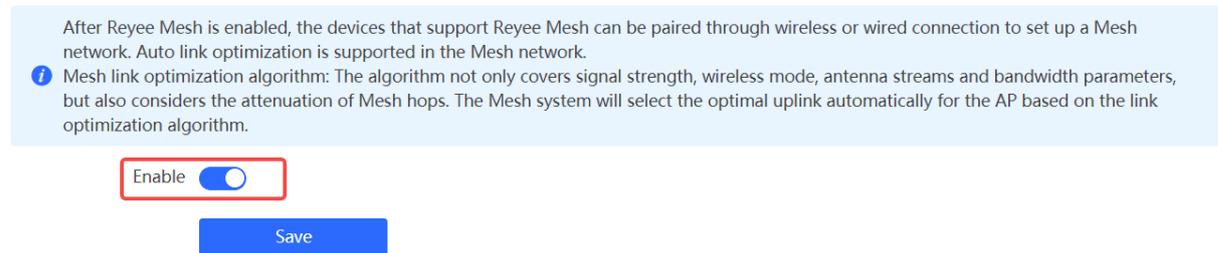
Caution

- You are advised to enable this function when a large number of multicast packets are transmitted and the network is congested to improve the user experience.
- If you set the action for unknown multicast packets to **Discard**, multicast packets sent by certain clients may be discarded. Therefore, exercise caution when performing this configuration.

5.9 Reyee Mesh Settings

Specification

This feature is supported only in ReyeeOS version 2.320 and later. The following figure shows the configuration page for versions prior to ReyeeOS 2.320.



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

After Reyee Mesh is enabled, you can set up a Mesh network through Mesh pairing between the devices that support Reyee Mesh. You can press the **Mesh** button on the device to automatically discover a new device for Mesh pairing or log in to the management page to select a new device for Mesh pairing. Reyee Mesh is enabled on the device by default.

Old Device Compatibility: If there are devices running software versions older than ReyeeOS 2.320 in the environment to form a Mesh network, you are advised to enable **Old Device Compatibility**. When this feature is enabled, devices with software versions prior to ReyeeOS 2.320 can join the mesh network through the fixed Mesh Wi-Fi network.

AP Mesh



When AP Mesh is enabled, Devices that support the AP Mesh function can form a network either wirelessly or through a wired connection. The system will automatically optimize mesh links by considering factors such as signal strength, wireless mode, number of antenna streams, channel width, and signal loss across mesh hops to choose the optimal uplink.

Mesh Networking

Old Device Compatibility

Configure Mesh Wi-Fi

Mesh Devices List

| Username | Model | SN | IP/MAC | Uplink | Status | Connectivity Quality |
|----------|---------|----|----------------|--------|---------|----------------------|
| AP | EG205GW | 68 | 192.168.110.91 | - | Offline | - |

Total 1 < 1 > 10/page

5.9.1 Configuring Mesh Wi-Fi

Specification

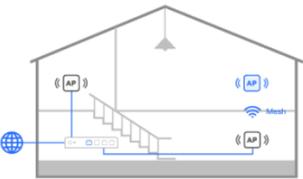
Devices running ReyeeOS 2.320 or later can be paired through the configured Mesh Wi-Fi network.

(1) Click **Configure Mesh Wi-Fi**, modify the SSID and Wi-Fi password, and click **OK**.

Note

Modifying the Mesh Wi-Fi configuration may lead to disconnections of paired devices, which will need to be reset to factory settings and re-paired.

AP Mesh



When AP Mesh is enabled, Devices that support the AP Mesh function can form a network either wirelessly or through a wired connection. The system will automatically optimize mesh links by considering factors such as signal strength, wireless mode, number of antenna streams, channel width, and signal loss across mesh hops to choose the optimal uplink.

Mesh Networking

Old Device Compatibility

Configure Mesh Wi-Fi

Mesh Devices List

| Username | Model | SN | IP/MAC | Uplink | Status | Connectivity Quality |
|----------|-------|----|----------------|--------|---------|----------------------|
| AP | | | 192.168.110.98 | - | Offline | - |

Total 1 < 1 > 10/page

Edit ✕

* SSID

* Wi-Fi Password 👁

(2) Click **OK** in the pop-up window.

Edit ✕

* SSID

* Wi-Fi Password 👁

Tips ✕

⚠ Modifying configurations may cause existing devices on the mesh network to disconnect. If this occurs, you can reset them to factory settings and then re-connect them through wireless mesh connection.

5.9.2 Adding Mesh Devices

(1) Click **Scan to Add Devices** to scan for nearby APs that are not on the network and are not connected via an Ethernet cable.

AP Mesh



When AP Mesh is enabled, Devices that support the AP Mesh function can form a network either wirelessly or through a wired connection. The system will automatically optimize mesh links by considering factors such as signal strength, wireless mode, number of antenna streams, channel width, and signal loss across mesh hops to choose the optimal uplink.

Mesh Networking

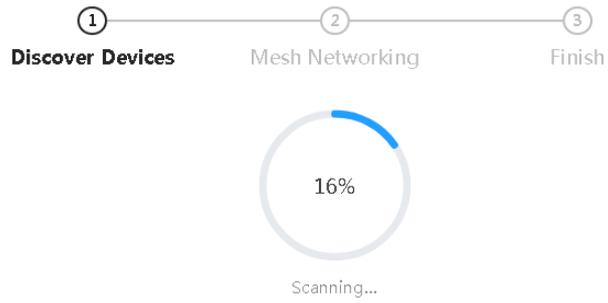
Old Device Compatibility ?

Mesh Devices List 🔄

| Username | Model | SN | IP/MAC | Uplink | Status | Connectivity Quality |
|----------|-------|----|----------------|--------|---------|----------------------|
| AP | | | 192.168.110.98 | - | Offline | - |

Total 1 < **1** > 10/page ▾

← Back



- (2) Select the desired APs (up to eight APs can be selected at a time), then click **Mesh Networking**. Wait for the mesh process to complete.

Note

If devices with a software version older than R320 are detected, you can toggle on **Old Device Compatibility** or upgrade the device's software version to R320 or later for Mesh networking.

← Back

The screenshot shows the Mesh Networking configuration interface. At the top, a progress bar indicates the current step is 2, Mesh Networking. A blue box contains a warning: "1 old devices are detected. You can enable Old Device Compatibility, or upgrade their firmware to the latest version." Below this, a circular progress indicator shows 100% completion with the text "Total Devices: 2." A table lists detected devices:

| Model | MAC |
|---|------------|
| <input checked="" type="checkbox"/> RAP73HD | XXXXXXXXXX |
| <input type="checkbox"/> F044550000 Old Version | XXXXXXXXXX |

Below the table, it says "Up to 8 devices can be selected." and "Cannot find the desired device. (?)". There are "Re-scan" and "Mesh Networking" buttons. The "Mesh Networking" button is highlighted with a red box. Below this, the progress bar shows step 2, Mesh Networking, is active. A circular progress indicator shows 3% completion with the text "Creating a mesh network...". The table below shows:

| Model | MAC |
|---|------------|
| <input checked="" type="checkbox"/> RAP73HD | XXXXXXXXXX |
| <input type="checkbox"/> Old Version | XXXXXXXXXX |

It also includes the same "Up to 8 devices can be selected." and "Cannot find the desired device. (?)" text, along with "Re-scan" and "Mesh Networking" buttons.

(3) Once the mesh networking process is complete, click **Finish** to return to the main interface.

← Back

| Model | MAC |
|-------------|-------|
| ✓ RAP73HD | |
| Old Version | |

Up to 8 devices can be selected. Cannot find the desired device. ?

Finish

(4) View the list of devices successfully joining the Mesh network.

AP Mesh

When AP Mesh is enabled, Devices that support the AP Mesh function can form a network either wirelessly or through a wired connection. The system will automatically optimize mesh links by considering factors such as signal strength, wireless mode, number of antenna streams, channel width, and signal loss across mesh hops to choose the optimal uplink.

Mesh Networking

Old Device Compatibility

[Configure Mesh Wi-Fi](#) [Scan to Add Devices](#)

Mesh Devices List

| Username | Model | SN | IP/MAC | Uplink | Status | Connectivity Quality |
|----------|---------|-------|-----------------|---------|--------|----------------------|
| AP | RAP73HD | | 192.168.110.236 | No data | Online | Good |

Total 1 1 10/page

5.10 Configuring the LAN Port of Downlink Access Point

Caution

The configuration takes effect only for a downlink access point with a wired LAN port.

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

Enter the VLAN ID and click **Save** to configure the VLAN, to which the AP wired ports belong. If the VLAN ID is null, the wired ports and WAN port belong to the same VLAN.

In self-organizing network mode, the AP wired port configuration applies to all APs having wired LAN ports on the current network. The configuration applied to APs in **LAN Port Settings** takes effect preferentially. Click **Add** to add the AP wired port configuration. For APs, to which no configuration is applied in **LAN Port Settings**, the default configuration of the AP wired ports will take effect on them.

i This profile takes effect only on APs with wired LAN ports, and is subject to the actual device. For example, the AP wired port profile takes effect on the RG-EAP101 AP.
Note: This profile takes effect on APs on the AP Wired Port Profile List. The AP Wired Profile Default Profile takes effect on other APs on the network.

Default Settings

VLAN ID [Add VLAN](#)

(Range: 2-232, 234-4090. If this field is left blank, it indicates that the VLAN corresponding to the WAN port is used.)

Apply to APs not on the AP Wired Port Profile List **i**

[Save](#)

LAN Port Settings [+ Add](#) [Delete Selected](#)

| <input type="checkbox"/> | VLAN ID ↕ | Apply to | Action |
|--------------------------|-----------|----------|---|
| <input type="checkbox"/> | 20 | Ruijie | Edit Delete |

Up to 8 VLAN IDs or 32 APs can be added (1 APs have been added).

5.11 Configure IEEE 802.1X authentication

i **Note**

This feature is only supported on RG-EG105GW-X.

5.11.1 Overview

IEEE 802.1X is a port-based network access control standard that provides secure access services for LANs.

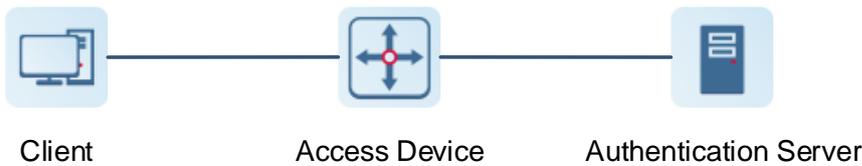
On an IEEE 802 LAN, a user can directly access network resources without authentication and authorization as long as it can connect to a network device. This uncontrolled behavior can bring security risks to the network. The IEEE 802.1X protocol was proposed to address the security issues on an IEEE 802 LAN.

The IEEE 802.1X protocol supports three security applications: Authentication, Authorization, and Accounting, abbreviated as AAA.

- **Authentication:** Determines whether a user can obtain access, and restricts unauthorized users.
- **Authorization:** Authorizes services available for authorized users, and controls the permissions of unauthorized users.
- **Accounting:** Records the usage of network resources by users, and provides a basis for traffic billing.

The 802.1X feature can be deployed on networks to control user authentication, authorization, and more.

An 802.1X network uses a typical client/server architecture, consisting of three entities: client, access device, and authentication server. A typical architecture is shown here.

Figure 5-1 Typical Architecture of 802.1X Network

- The client is usually an endpoint device which can initiate 802.1X authentication through the client software. The client must support the Extensible Authentication Protocol over LANs (EAPoL) on the local area network.
- The access device is usually a network device (AP or switching device) that supports the IEEE 802.1X protocol. It provides an interface for clients to access the local area network, which can be a physical or a logical interface.

Note

- The RG-EG-W gateway device itself does not support the IEEE 802.1X authentication, and can only serve as the primary device to support 802.1X global configuration and deliver the configuration to APs and switching devices on the entire network.
 - To achieve IEEE 802.1X authentication, ensure that the network includes an AP or switching device.
-
- The authentication server can realize user authentication, authorization, and accounting. Usually a RADIUS server is used as the authentication server.

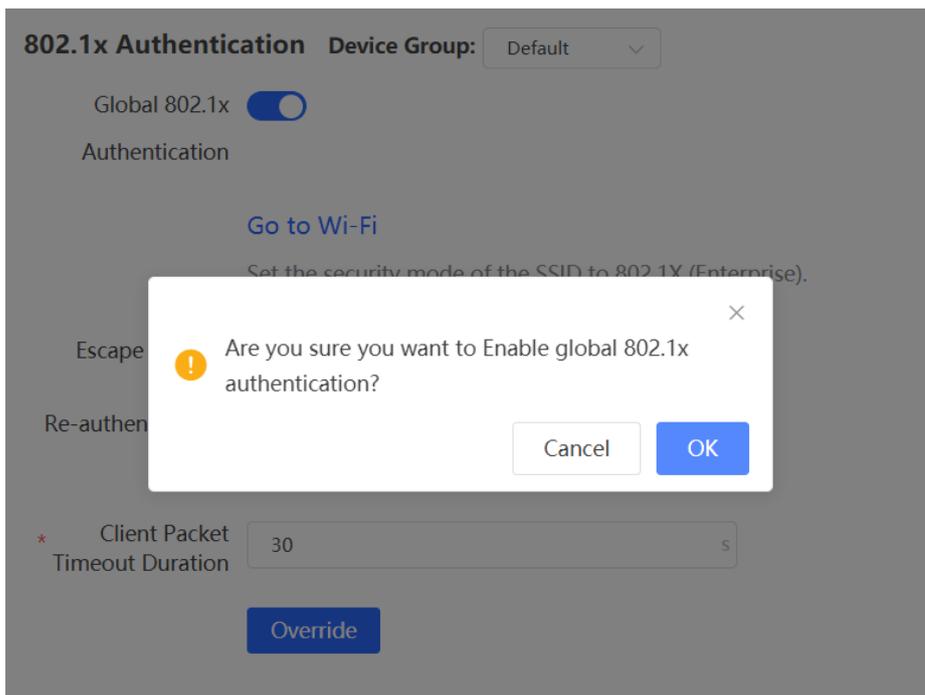
5.11.2 Configuring 802.1X Globally

The gateway device supports the 802.1X global configuration, and can synchronously deliver the configuration to APs and switching devices on the network.

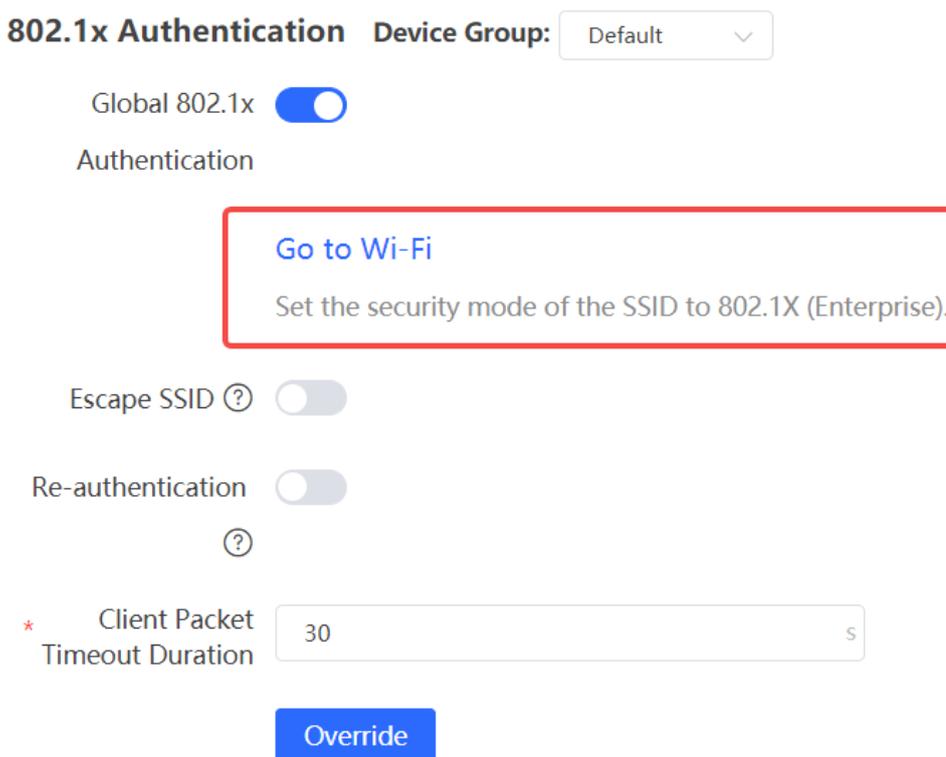
Choose **Network-Wide > Workspace > Wireless > 802.1x Authentication**.

- (1) Click the **802.1x Authentication** tab to configure global configuration for 802.1x wireless authentication.
- (2) Select the authentication device group, and enable the global 802.1x authentication.

You will be prompted to enable this feature or not. Click **OK**.



- (3) Click **Go to Wi-Fi**, and set the encryption method of SSID to **802.1x (Enterprise)**.



Edit



* SSID ?

Purpose ? **General** | IoT | Guest

Band ? 2.4G 5G

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

Encryption Open Security 802.1x (Enterprise)

* Security ?

Server Group [Edit](#)

----- advanced Setting -----

(4) Configure global parameters.

802.1x Authentication Device Group:

Global 802.1x Authentication

[Go to Wi-Fi](#)

Set the security mode of the SSID to 802.1X (Enterprise).

Escape SSID ?

Re-authentication ?

* Client Packet Timeout Duration s

Table 5-7 Description of Global 802.1x Authentication Configuration

| Parameter | Description |
|--------------------------------|--|
| Escape SSID | Once this feature is enabled, when the authentication server is unavailable, the system will create a temporary Wi-Fi network for users. If this function is enabled, it is necessary to set the Escape SSID, encryption type, and Wi-Fi password. |
| Re-authentication | Once this feature is enabled, the system regularly re-authenticates users. Users who do not match the information on the server will be automatically disconnected. If this function is enabled, it is necessary to set the re-authentication cycle, which is 21600 seconds by default. |
| Client Packet Timeout Duration | The timeout period during which the client waits for a response from the authentication server. If this timer expires, authentication is considered failed. The value range is 10 seconds to 60 seconds. The default value is 30 seconds. |

(5) Click **Override**.

5.11.3 Configuring the RADIUS Server

1. Prerequisites

Before configuration, ensure that the RADIUS server is ready, and that the IP address and shared key of the RADIUS server are configured.

2. Configuration Steps

Choose **Network-Wide > Workspace > Wireless > 802.1x Authentication**

- (1) Click the **RADIUS Server Management** tab.
- (2) Click **Add Server Group** to configure related server parameters.

RADIUS Server Management Add Server Group

| Server Group Name | Server IP | Auth Port | Accounting Port | Shared Password | Action |
|-------------------|-----------|-----------|-----------------|-----------------|--------|
| No Data | | | | | |

Up to 20 entries can be added.

Add
×

* Server Group Name

🗑 Server 1

* Server IP

* Server Name

* Auth Port

* Accounting Port

* Shared Password

* Match Order

⊕ Add Server

Table 5-8 Description of RADIUS Server Management Configuration

| Parameter | Description |
|-----------------|--|
| Server IP | IP address of the RADIUS server. |
| Auth Port | The port number for the RADIUS server to perform user authentication. |
| Accounting Port | The port number for the RADIUS server to perform user accounting. |
| Shared Password | Shared key of the RADIUS server. |
| Match Order | The system supports up to five RADIUS servers. A larger value indicates a higher priority. |

(3) Enter the server global configuration parameters, and click **Save**.

Server global configuration

Proxy Server

* Packet Retransmission Interval s

* Packet Retransmission Count time

Server Detection

MAC Address Format

Save

Table 5-9 Description of Server Global Configuration

| Parameter | Description |
|--------------------------------|---|
| Proxy Server | After this function is enabled, local device will act as a proxy for the RADIUS server to send RADIUS messages. |
| Packet Retransmission Interval | Configure the interval during which the device sends a request to a RADIUS server before confirming that the RADIUS server is unreachable. |
| Packet Retransmission Count | Configure the number of times that the device sends requests to a RADIUS server before confirming that the RADIUS server is unreachable. |
| Server Detection | If this function is enabled, it is necessary to set the server detection cycle, server detection times, and server detection username. Determines the server status and whether to enable functions such as the escape function. |
| MAC Address Format | Configure the format of the MAC address used in attribute 31 (Calling-Station-ID) of a RADIUS message. The following formats are supported: <ul style="list-style-type: none"> ● Dotted hexadecimal format. For example, 00d0.f8aa.bbcc. ● IETF format. For example: 00-D0-F8-AA-BB-CC. ● Unformatted (default). For example: 00d0f8aabbcc |

5.11.4 Checking Authentication User List

When the 802.1x feature 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 **Network-Wide > Workspace > Wireless > 802.1x Authentication**

Click **Wireless User List** or **Wired User List** to view specific user information.

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

Wireless User List [Refresh](#) [↓ Batch Logout](#)

| <input type="checkbox"/> | Name | IP | MAC Address | Online Time | Connect SSID | Access Name | Action |
|--------------------------|------|----|-------------|-------------|--------------|-------------|--------|
| No Data | | | | | | | |

Total 0 [<](#) [1](#) [>](#)

Click **Refresh** to view the latest user list.

If you want to disconnect a user from the network, select the user and click **Logout** under the **Action** column. You can also select multiple users and click **Batch Logout** to disconnect selected users.

5.12 Configuring Domain Proxy

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

When a client accesses a Wi-Fi network, the message "No Internet connection" or "The Wi-Fi is not connected to the Internet" may be displayed. The possible cause is that the client's operating system introduces an Internet detection mechanism. Generally, the detection mechanism sends a probe packet to a specified domain name and evaluates whether the wireless network can access the Internet based on the detection result. If the DNS server takes a long time to parse a domain name or returns a probe node with a long delay, the probe may be deemed unreachable, causing a false network unavailability.

After the **Domain Proxy** function is enabled, the device returns the preset domain name node to the client, reducing the misjudgment of network unavailability of the client.

Domain Proxy

Enable

Click **+Add**, enter the preset domain name and IP address, and click **OK**.

User Configuration List [+ Add](#) [Delete Selected](#)

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

Up to 32 entries can be added. Total 0 [<](#) [1](#) [>](#)

×

* Domain Name

* IP

5.13 Client Association

5.13.1 Configuring Intelligent Association

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

Note

Intelligent association is not supported by Wi-Fi 5 APs. Enabling it on Wi-Fi 5 APs may lead to suboptimal performance.

After certain smart home devices are associated with a remote AP, they are unable to re-associate with a nearby AP, resulting in poor user experience and significant delays.

With the Intelligent Association feature enabled, clients can dynamically select the access point for association, eliminating issues related to poor user experience caused by remote associations.

Toggle on the **Intelligent Association** switch, select the association mode, and click **Save**.

- Signal First
Associate with the AP with the best signal.
- Experience First
Associate with the AP with the best wireless experience.

Intelligent Association ?

Intelligent Association

Association Mode **Signal First** RSSI Threshold Experience First
Associate with the AP with the best signal Associate with the AP with the best wireless experience

5.13.2 Configuring Client Association

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

Client Association

Enter MAC

| <input type="checkbox"/> | Client | IP/MAC | Associated Device | Signal Strength | Action |
|--------------------------|--------|-------------|---|-----------------------|---|
| <input type="checkbox"/> | - | 9c:.....:ie | AP @Ruijie-m6649 5G | -42dBm Channel: 36 | Edit Delete |

Up to 128 entries can be added. Total 1 **1** 10/page

Click **Add Association**. Select the client and the associated device. You can associate the client with a specified AP on the network to reduce remote association and improve the wireless experience.

Add Association ✕

* Client

* Associated Device

[Advanced Settings](#)

Click **Advanced Settings** to configure the SSID for client association and to enable **Forced Association**.

[Advanced Settings](#)

SSID

Forced Association

Enabling this feature will forcefully associate the client with a specific AP. However, since the client cannot initiate automatic association, this may cause disconnection and unsuccessful association attempts.

Caution

The **Forced Association** feature may cause the client to go offline or fail to associate with the AP. Therefore, exercise caution when performing this configuration.

6 Switch Management

6.1 Configuring RLDP

6.1.1 Overview

Rapid Link Detection Protocol (RLDP) is an Ethernet link fault detection protocol used to quickly detect link faults and downlink loop faults. RLDP can prevent network congestion and connection interruptions caused by loops. After a loop occurs, the port on the access switch involved in the loop will shut down automatically.

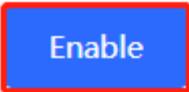
6.1.2 Configuration Steps

Choose **Network-Wide > Workspace > Wired > RLDP**.

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

RLDP

RLDP will avoid network congestion and connection interruptions caused by loops. After a loop occurs, the port involved in the loop will be automatically shut down.



Enable

(2) In the networking topology, you can select the access switches on which you want to enable RLDP in either recommended or custom mode. If you select the recommended mode, all access switches in the network are selected automatically. If you select the custom mode, you can manually select the desired access switches. Click **Deliver Config**. RLDP is enabled on the selected switches.

← RLDP Config

Please select the target switch:

Recommended Custom
Auto-Identified Switches Specified Switches

1 switches are selected.

Deliver Config Cancel Config

Rotate
Restore
Refresh

- (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.



6.2 Configuring DHCP Snooping

6.2.1 Overview

DHCP Snooping implements recording and monitoring the usage of client IP addresses through exchange of DHCP packets between the server and client. In addition, this function can filter invalid DHCP packets to ensure that clients can obtain network configuration parameters only from the DHCP server in the controlled range. DHCP Snooping will prevent rogue DHCP servers offering IP addresses to DHCP clients to ensure the stability of the network.

Caution

After DHCP Snooping is enabled on the switch, the switch does not forward invalid DHCP packets. However, if a client directly connects to a rogue DHCP server, it cannot access the Internet as the obtained IP address is incorrect. In this case, you need to find the rogue router and disable DHCP on it, or use the WAN port for uplink connection.

6.2.2 Configuration Steps

Choose **Network-Wide > Workspace > Wired > DHCP Snooping**.

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

DHCP Snooping

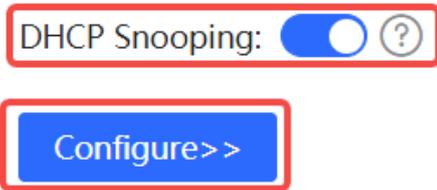
By enabling DHCP snooping, you can effectively prevent certain devices from receiving invalid IP addresses from unauthorized routers, thereby avoiding network connectivity failures.

This feature guarantees a stable and continuous network connection.



- (2) In the networking topology, you can select the access switches on which you want to enable DHCP Snooping in either recommended or custom mode. If you select the recommended mode, all switches in the network are selected automatically. If you select the custom mode, you can manually select the desired switches. Click **Deliver Config**. DHCP Snooping is enabled on the selected switches.

- (3) After the configuration is delivered, if you 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.



6.3 Batch Configuring Switches

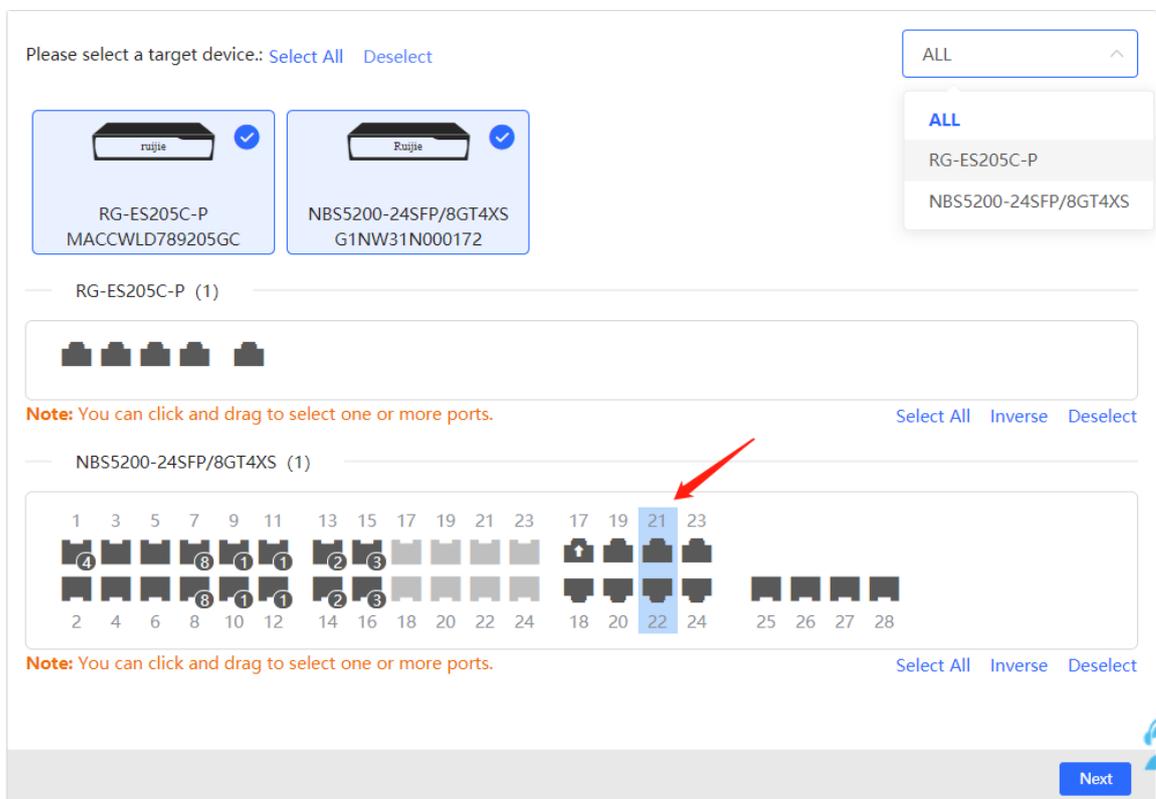
6.3.1 Overview

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

6.3.2 Configuration Steps

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**.



- (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**.

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

- (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

6.3.3 Verifying Configuration

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

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

Port Status
▶ **VLAN Info**
Port
Route Info
RLDP
More

VLAN [Edit](#)

VLAN1 **VLAN12**

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

1 3 5 7 9 11 13 15 17 19 21 23 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 18 20 22 24 25 26 27

Port [Edit](#)

7 Authentication Management

7.1 Web Authentication

7.1.1 Overview

With the popularity of wireless networks, Wi-Fi has become one of the marketing means for merchants. Customers can connect to the Wi-Fi provided by the merchants to surf the Internet after watching advertisements. In addition, to defend against security vulnerabilities, the wireless office network usually allows only employees to associate with Wi-Fi, so the identity of the clients needs to be verified.

The Wi-Fi authentication function of the device uses the Portal authentication technology to implement information display and user management. After users connect to Wi-Fi, the traffic will not be directly routed to the Internet. Wi-Fi users must pass authentication on the Portal authentication website, and only authenticated users are allowed to use network resources. Merchants or enterprises can customize Portal pages for identity authentication and advertisement display.

7.1.2 Getting Started

- (1) Before you enable Wi-Fi authentication, ensure that the wireless signal is stable and users can connect to Wi-Fi and surf the Internet normally. The wireless SSID used for authentication in the network should be set to the open state.
- (2) If the IP address of an AP in the network is within the authentication scope, add the AP as the authentication-free user. For details, see Section [7.1.8 Authentication-Free](#).
 - o In a Layer 2 network, add the MAC address of the AP to the authentication-free MAC address allowlist.
 - o In a Layer 3 network, add the IP address of the AP to the authentication-free IP address Allowlist.

7.1.3 WiFiDog Authentication

1. Overview

The EG device is connected to the MACC authentication server on the cloud. After Wi-Fi users connect to Wi-Fi, a Portal page pops up. The users need to enter the account and password to pass authentication before they can access the Internet. According to the authentication configuration on the MACC authentication server, you can set the authentication mode to SMS authentication, fixed account authentication, or account-free one-click login.

2. Getting Started

- (1) WiFiDog is a Layer 2 protocol. Ensure that the authentication device can obtain the MAC addresses of the wireless users.
 - o The gateway address of the wireless users to be authenticated is deployed on the authentication device.
 - o If the gateway address is not deployed on the authentication device, the device functions as a DHCP server to allocate IP addresses to the wireless users and obtain MAC addresses of the wireless users. In this scenario, you need to set Network Type to Layer-3 Network.

- (2) Complete the corresponding configuration on the Ruijie Cloud platform before you enable the authentication function on the device. If SMS authentication is used, you also need to configure the SMS gateway.

3. Configuration Steps

Choose **One-Device > Gateway > Config > Authentication > Web Authentication > Cloud Auth**.

- (1) Turn on **Authentication**.
- (2) Set **Server Type** to **Cloud Integration**, configure Network Type, Auth Server URL, Client Escape and HTTPS Redirection, and click **Save**.

Ruijie Cloud supports voucher authentication, local account authentication, SMS authentication and one-click authentication. Please log into Ruijie Cloud to enable authentication. [View](#)

i In a layer-2 network, if the IP address of the EAP device is in the authentication IP range, please add its MAC address to the MAC address allowlist of [Allowlist](#).
 In a layer-3 network, if the IP address of the EAP device is in the authentication IP range, please add its IP address to the IP address allowlist of [Allowlist](#).

Authentication

* Network Type

* Server Type

* Auth Server URL

Client Escape Enable

HTTPS Redirection Enable

- (3) In the **Net List** area, click **Add**. In the displayed dialog box, enter the **VLAN** name and the **Auth IP / IP Range** to be authenticated and click **OK**.

Add ×

* VLAN

* Auth IP / IP Range

Table 7-1 Description of WiFiDog Authentication Configuration

| Parameter | Description |
|-----------------|--|
| Network Type | The default value is Layer-2 Network . Set the parameter based on the actual network environment. |
| Server Type | Select Cloud Integration from the drop-down list. |
| Auth Server URL | After completing the configuration at the server end, the Ruijie Cloud authentication server returns a URL. The device sends authentication requests to the URL during authentication. |

| Parameter | Description |
|--------------------|--|
| Client Escape | After the client escape function is enabled, if an exception occurs on the authentication server, the device disables authentication to allow all clients to directly access the Internet. After the server recovers, the device automatically enables authentication. |
| HTTPS Redirection | Enabling HTTPS redirection ensures that user data transmission during the authentication process is encrypted, thereby enhancing the security of the authentication process. When HTTPS redirection is disabled, authentication requests can only be sent to HTTP pages. |
| VLAN | Specify the name of a Wi-Fi network, to which clients connect. A maximum of eight VLAN names can be configured. |
| Auth IP / IP Range | Specify the IP address range to be authenticated. You can enter a single IP address (such as 192.168.112.2) or an IP address range (such as 192.168.112.2–192.168.112.254). A maximum of five IP address ranges can be configured. |

4. Verifying Configuration

After a mobile phone connects to a specific Wi-Fi, the Portal authentication page pops up automatically.

If the authentication mode configured on the Ruijie Cloud authentication server is SMS authentication, the user needs to enter the mobile number to obtain an Internet access password and enter the password to complete authentication.

If the authentication mode configured on the Ruijie Cloud authentication server is account-free one-click authentication, the user can directly access the Internet after clicking the corresponding button on the page.

If the authentication mode configured on the Ruijie Cloud authentication server is fixed account login, the user can access the Internet after entering the account and password configured on the cloud.

After successful connection, you can choose **One-Device > Gateway > Config > Authentication > Online Clients** to view information about this authenticated user. For details, see Section [7.3 Online User Management](#).

7.1.4 Configuring Third-Party Authentication

 Note

This feature is supported on RG-EG105GW-X running ReyeeOS 2.237 or later.

1. Overview

Reyee EG series gateway devices can interwork with WISPr-compliant external authentication servers. After a wireless client is connected to the Wi-Fi network, a Portal page pops up. The wireless client needs to be authenticated before it can access the Internet. Based on the services provided by different authentication servers, you can choose RADIUS authentication, local account authentication, or no authentication for third-party authentication.

2. Getting Started

- Ensure that the authentication server can obtain the MAC address of the wireless client:
 - The gateway address of the wireless client to be authenticated is deployed on the authentication server.
 - If the gateway address of the wireless client to be authenticated is not deployed on the authentication server, then the device must act as a DHCP server to assign an IP address to the wireless client in order to obtain its MAC address. In this scenario, the **Network Type** must be set to **Layer 3 Network**.
- Complete relevant configurations on the third-party authentication platform, and then enable the Wi-Fi authentication feature on the device. For specific configurations, see the configuration manual of relevant third-party authentication platforms.

3. Configuration Steps

Choose **One-Device > Gateway > Config > Authentication > Web Authentication > Cloud Auth**.

Authentication

* Network Type

* Server Type [Customized Parameter](#)

* Auth Server URL

Client Escape Enable

HTTPS Redirection Enable

Authentication type RADIUS Local account None

To make the RADIUS flow control effective, please go to the Flow Control for configuration. [View](#)

RADIUS Encryption PAP CHAP MS-CHAP MS-CHAP-V2

Authentication server [Edit](#)
group

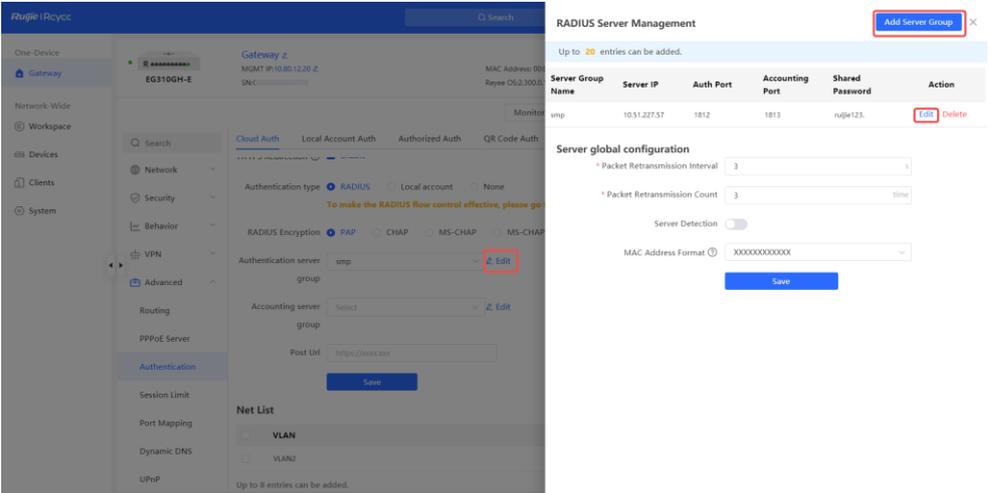
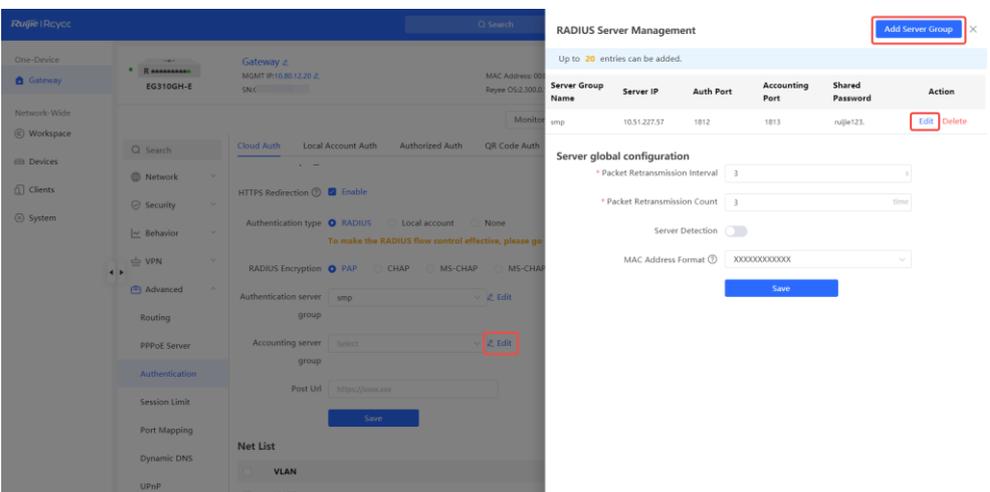
Accounting server [Edit](#)
group

Post Url

- (1) Toggle on **Authentication**.
- (2) Set **Server Type** to **Third-party Authentication**, configure Network Type, Auth Server URL, Client Escape, HTTPS Redirection, Authentication Type, Auth Server Group and Accounting Server Group, and click Save.

Table 7-2 Description of Third-Party Authentication Configuration Parameters

| Parameter | Description |
|---------------------|---|
| Network Type | The default value is Layer-2 Network. Set the parameter based on the actual network environment. |
| Server Type | Select Third-party authentication from the drop-down list. |
| Auth Server URL | After completing the configuration on the third-party authentication server, the third-party authentication server returns a URL. The device sends authentication requests to the URL during authentication. |
| Client Escape | After the client escape function is enabled, if an exception occurs on the authentication server or the RADIUS server, the device disables authentication to allow all clients to directly access the Internet. After the server recovers, the device automatically enables authentication. |
| HTTPS Redirection | Enabling HTTPS Redirection ensures that data is encrypted during user authentication, thus improving the security of the authentication process. When HTTPS Redirection is disabled, you will be redirected to HTTP pages only. |
| Authentication type | Types of third-party authentication, which include: <ul style="list-style-type: none"> ● RADIUS: The wireless client is authenticated by the RADIUS server. ● Local account: The wireless client is authenticated based on local username and password. ● None: No authentication is required for the wireless client. |
| RADIUS Encryption | When Authentication Type is set to RADIUS, you need to configure the encryption mode for RADIUS authentication: <ul style="list-style-type: none"> ● RAP: This mode has low security. Passwords are transmitted in plain text, posing a risk of interception. ● CHAP: The server sends a random CHAP challenge to the client, and the client uses the password to calculate and returns a response. ● MS-CHAP: Functions such as password change and failed attempt count are supported. This mode is more secure and flexible than CHAP. ● MS-CHAPv2: As an improved version of MS-CHAP, this mode provides higher security and better encryption. |

| Parameter | Description |
|------------------------------------|---|
| <p>Authentication server group</p> | <p>Select a RADIUS authentication server group from the drop-down list box.</p> <p>This parameter is mandatory when the Authentication Type is set to RADIUS.</p> <p>You can click Edit next to the input box to create or modify a RADIUS authentication server group in the pop-up box. For details, see Section 5.11.3 Configuring the RADIUS Server.</p>  |
| <p>Accounting server group</p> | <p>Select a RADIUS accounting server group from the drop-down list box.</p> <p>This parameter is mandatory when the Authentication Type is set to RADIUS.</p> <p>You can click Edit next to the input box to create or modify a RADIUS accounting server group in the pop-up box. For details, see Section 5.11.3 Configuring the RADIUS Server.</p>  |
| <p>Post URL</p> | <p>The URL to which the user will be redirected after authentication.</p> |
| <p>VLAN</p> | <p>Specify the name of a Wi-Fi network, to which clients connect. A maximum of eight VLAN names can be configured.</p> |
| <p>Auth IP / IP Range</p> | <p>Specify the IP address range to be authenticated. You can enter a single IP address (such as 192.168.112.2) or an IP address range (such as 192.168.112.2–192.168.112.254). A maximum of five IP address ranges can be configured.</p> |

- (3) (Optional) Considering the different HTTP parameters and request methods required by different third-party authentication platforms. To configure custom third-party authentication parameters, you can click **Customized Parameter** next to **Server Type** and set **Parameter template** to **Custom**.

Authentication

* Network Type

* Server Type **Customized Parameter**

* Auth Server URL

Client Escape **Enable**

HTTPS Redirection **Enable**

Authentication type **RADIUS** Local account None

To make the RADIUS flow control effective, please go to the Flow Control for configuration. [View](#)

Customized Parameter ×

Parameter template Ruijie Ruijie-CHAP **Custom**

Request Parameters

Request method **get** post

Parameter Type Key Val

Login Parameters

Name

Password

Post Url

Table 7-3 Description of Custom Third-Party Authentication Parameters

| Parameter | Description |
|--------------------|--|
| Parameter template | The built-in parameter template. Default parameters are used when the Parameter Template is set to Ruijie or Ruijie-CHAP . When the Parameter Template is set to Custom , the parameters can be customized. |
| Request method | The HTTP request methods used for requesting the portal page. |

| Parameter | Description |
|------------------|---|
| Parameter | <p>Parameters in the parameter template for requesting the portal page:</p> <ul style="list-style-type: none"> ● When the parameter type is not other, the Val field is invalid, and the default value NULL can be used. The Reyee EG gateway device will automatically populate the value of this parameter. ● When the parameter type is other, you need to enter a value in the Val field. <p>Parameters include:</p> <ul style="list-style-type: none"> ● nas_ip: IP address of the Reyee EG series gateway device. Example: 10.52.48.7. ● nas_mac: MAC address of the Reyee EG series gateway device. Example: 11:22:33:44:55:66. ● client_ip: IP address of the wireless client to be authenticated. Example: 192.168.110.5. ● client_mac: MAC address of the wireless client to be authenticated. Example: 11:22:33:44:55:66. ● orig_url: Original URL accessed by the wireless client to be authenticated. Example: https://www.baidu.com. ● login_url: Login interface received by the Reyee EG series gateway device from the third-party authentication platform. Example: http://192.168.110.1:2060/ext_login. ● logout_url: Logout interface received by the Reyee EG series gateway device from the third-party authentication platform. Example: http://192.168.110.1:2060/ext_logout. ● ssid: SSID or VLAN name associated with the wireless client to be authenticated. Example: VLAN233. ● sn: SN of the gateway. ● identity: ID of the gateway. ● chap_id: Identifier or session ID stored during CHAP authentication. ● chap_challenge: The challenge string used in the CHAP authentication process. ● interface_name: Name of the interface through which the wireless client accesses the network. ● login_host: IP address of the login interface on the Reyee EG series gateway device. Example: 192.168.110.1:2060. ● other: other custom field. Multiple custom fields are supported. |
| Login Parameters | <p>Custom fields of the login interface received by the Reyee EG series gateway devices from the third-party authentication platform, including:</p> <ul style="list-style-type: none"> ● Name: username. ● Password: password. ● Post Url: URL to which the wireless client is redirected after successful authentication. |

(4) In the **Net List** area, click **Add**. In the displayed dialog box, enter the **VLAN** name and the **Auth IP / IP Range** to be authenticated and click **OK**.



Add×

* VLAN

* Auth IP / IP Range

?

4. Verifying Configuration

Connect your smartphone to the specific Wi-Fi network to verify that the portal page pops up automatically.

Connect to different authentication platforms to view services provided by these authentication platforms.

After successful connection, you can choose **One-Device > Gateway > Config > Authentication > Online Clients** to view information about this authenticated user. For details, see Section [7.3 Online User Management](#).

7.1.5 Local Account Authentication

1. Overview

The device is connected to the local authentication server, and user identity is verified based on the account and password. Local account authentication is applicable to the wireless office network environment.

2. Getting Started

Ensure that the device with the authentication function enabled has been connected to the Internet. Otherwise, the authentication page does not pop up when a client associates with Wi-Fi.

3. Configuration Steps

Choose **One-Device > Gateway > Config > Authentication > Web Authentication > Local Account Auth**.

(1) Enable account authentication.

Turn on **Local Account Auth**, enter the IP address range of clients to be authenticated, and click **Save**. After account authentication is enabled, clients in the specified IP address range can access the Internet only after passing authentication.

Local Account Auth

Auth Integration with
Cloud

Accounts 0

* Network Type

Auth IP / IP Range

Seamless Online Period

* Custom Time days

HTTPS Redirection Enable

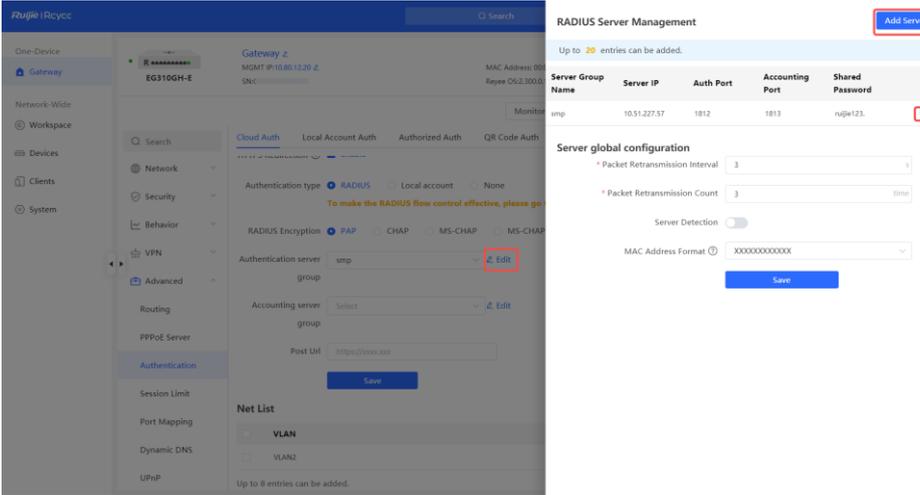
Expiration Reminder

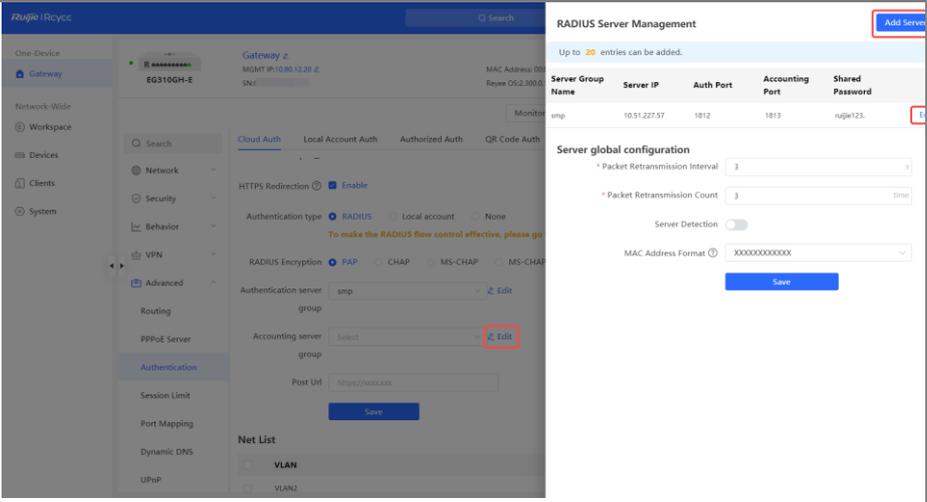
A reminder portal page will appear when a user's account is nearing expiration. The user can continue browsing only after confirmation.

* Authentication type RADIUS Local account

Table 7-4 Description of Local Account Authentication Configuration Parameters

| Parameter | Description |
|-----------------------------|---|
| Auth Integration with Cloud | Use the authentication service integrated in Ruijie Cloud. |
| Accounts | The number of created authentication accounts. |
| Network Type | The default value is Layer-2 Network. Set the parameter based on the actual network environment. |
| Auth IP / IP Range | Specify the IP address range to be authenticated. You can enter a single IP address (such as 192.168.112.2) or an IP address range (such as 192.168.112.2–192.168.112.254). A maximum of five IP address ranges can be configured. After setting the IP address or IP address range, select the portal page for this IP address or IP address range from the drop-down list box on the right. For details about the configuration of the portal page, see Section 7.1.9 Custom Portal Page . |
| Seamless Online Period | Set the validity period of seamless authentication. After a user is authenticated successfully for the first time, the user will be automatically authenticated when connecting to the Wi-Fi network within the validity period. |
| HTTPS Redirection | Enabling HTTPS Redirection ensures that data is encrypted during user authentication, thus improving the security of the authentication process. When HTTPS Redirection is disabled, you will be redirected to HTTP pages only. |
| Expiration Reminder | When an account is about to expire, a reminder portal page will appear. The user can continue to access the Internet only after confirmation. |
| Authentication type | Types of local account authentication, which include: |

| Parameter | Description |
|-----------------------------|---|
| | <ul style="list-style-type: none"> ● RADIUS: The wireless client is authenticated by the RADIUS server. ● Local account: The wireless client is authenticated based on local username and password. |
| RADIUS Encryption | <p>When Authentication Type is set to RADIUS, you need to configure the encryption mode for RADIUS authentication:</p> <ul style="list-style-type: none"> ● RAP: This mode has low security. Passwords are transmitted in plain text, posing a risk of interception. ● CHAP: The server sends a random CHAP challenge to the client, and the client uses the password to calculate and returns a response. ● MS-CHAP: Functions such as password change and failed attempt count are supported. This mode is more secure and flexible than CHAP. ● MS-CHAP-V2: As an improved version of MS-CHAP, this mode provides higher security and better encryption. |
| Authentication server group | <p>Select a RADIUS authentication server group from the drop-down list box.</p> <p>This parameter is mandatory when the Authentication Type is set to RADIUS.</p> <p>You can click Edit next to the input box to create or modify a RADIUS authentication server group in the pop-up box. For details, see Section 5.11.3 Configuring the RADIUS Server.</p>  |
| Authentication server group | <p>Select a RADIUS accounting server group from the drop-down list box.</p> <p>This parameter is mandatory when the Authentication Type is set to RADIUS.</p> <p>You can click Edit next to the input box to create or modify a RADIUS accounting server group in the pop-up box. For details, see Section 5.11.3 Configuring the RADIUS Server.</p> |

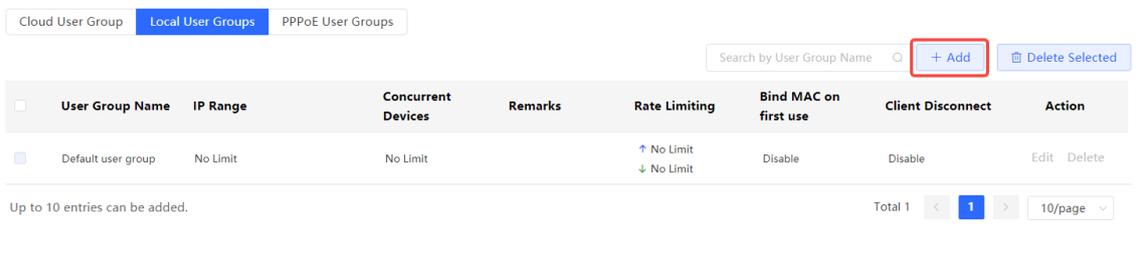
| Parameter | Description |
|-----------|--|
| |  |

(2) Configure local user groups.

Choose **One-Device > Gateway > Config > Authentication > Account > User Groups**.

Configuring local user groups can limit the network segment for user authentication and Internet access rate. For example, on a campus network, you can configure different local user groups for teachers and students, which limits network segments for their authentication and isolates users.

Click the **Local User Groups** tab and click **Add** to set parameters. After the configuration is complete, the user group can be associated with a local authentication account.



| ☐ | User Group Name | IP Range | Concurrent Devices | Remarks | Rate Limiting | Bind MAC on first use | Client Disconnect | Action |
|---|--------------------|----------|--------------------|---------|--------------------------|-----------------------|-------------------|-------------|
| ☐ | Default user group | No Limit | No Limit | | ↑ No Limit ↓ No Limit | Disable | Disable | Edit Delete |

×

* User Group Name

IP Range ?

Concurrent Devices No Limit Custom

Remarks

Maximum Uplink Rate No Limit Custom

Maximum Downlink Rate No Limit Custom

Bind MAC on first use

Client Disconnect ?

Table 7-5 Configuration of Local User Groups

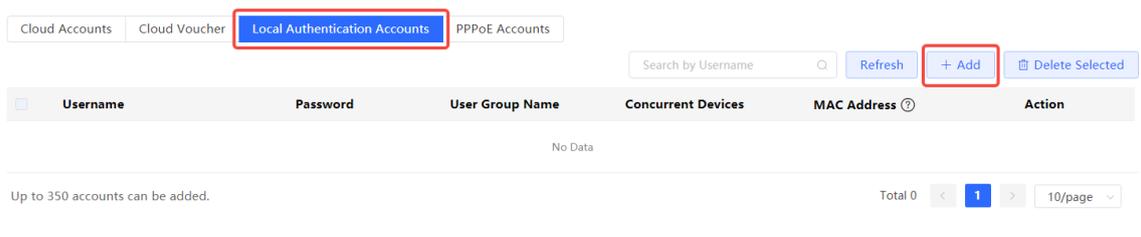
| Parameter | Description |
|------------------------------|--|
| User Group Name | Specify the name of a user group. You can associate a local user group based on the name when configuring a local authentication account. |
| IP Range | Specify the IP address segment used to limit the local account authentication. An account associated with a user group can pass Internet access authentication only when the account initiates an authentication request from the corresponding network segment. Multiple associated network segments can be configured. |
| Concurrent Devices | <p>Multiple clients can access the Internet using the same username and password. You can set the parameter to limit the maximum number of clients that can access the Internet using the account associated with a user group. You can set Concurrent Devices to Custom and enter the maximum number of allowed online clients.</p> <hr/> <p>⚠ Caution</p> <p>If this parameter is also configured for an authentication account, the configuration takes effect preferentially.</p> <hr/> |
| Remarks | Enter the user group description. |
| Maximum Uplink/Downlink Rate | Configure the uplink and downlink bandwidth limits for users associated with the user group. |
| Bind MAC on first use | After this parameter is toggled on and a client logs in for the first time, the local authentication server records the MAC address of the client. |

| Parameter | Description |
|----------------------|--|
| Client Disconnection | <p>When the number of online clients using an account associated with a user group exceeds the configured Concurrent Devices, new clients cannot be onboarded. After the parameter is toggled on, new clients can choose to disconnect other clients, thereby gaining access to the Internet.</p> <p>You are advised not to toggle on the parameter when Bind MAC on first use is toggled on. Otherwise, the bound MAC address may become invalid.</p> |

(3) Configure an authentication account.

Choose **One-Device > Gateway > Config > Authentication > Account > Accounts**.

Click the **Local Authentication Accounts** tab, and click **Add** to create a local account for web-based authentication. Set **Username** and **Password**. Multiple devices can access the Internet using the same username and password. You can set **Concurrent Users** to configure the maximum number of users who can access the Internet using the same account. To limit the network segment or bandwidth for user login, you can set **Plan** to a user group.



Add Account ✕

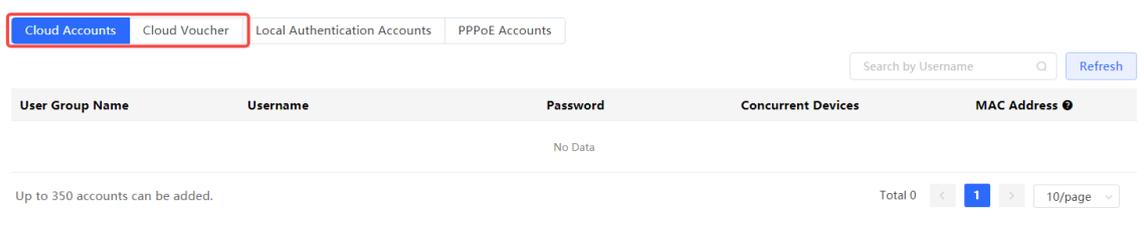
* Username

* Password

Concurrent Devices
(?)

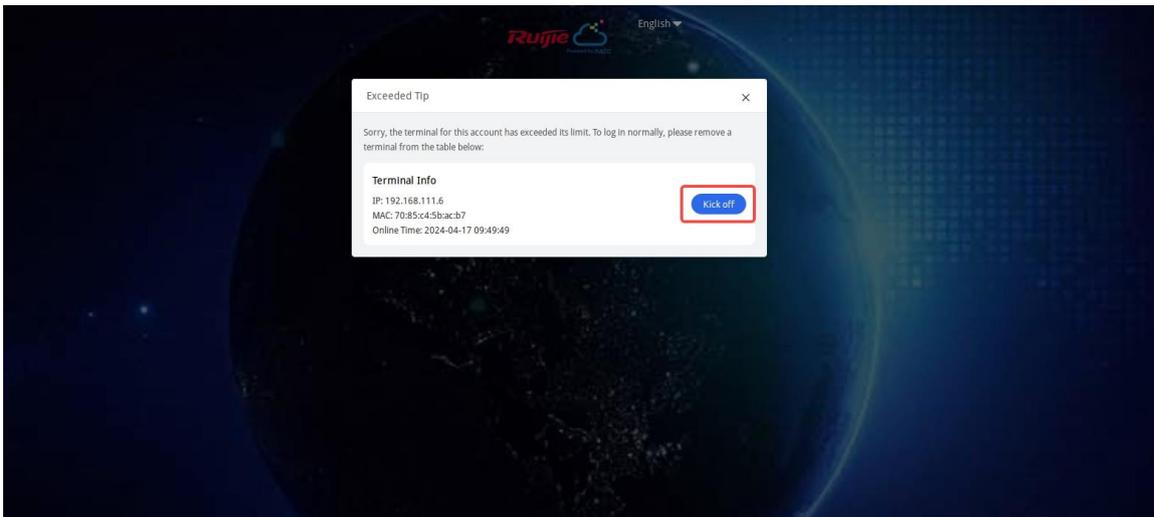
Plan

Click **Cloud Accounts** or **Cloud Voucher** to view the account and voucher information synchronized from Ruijie Cloud.



(4) Disconnect an online user.

When the number of concurrent users in a single account exceeds the limit, a prompt will appear when a new user attempts to connect. You can then choose to disconnect a specific user by clicking the Kick off button. After re-logging in, the user can access the network.



4. Verifying Configuration

After a client connects to the specific Wi-Fi, the authentication page pops up automatically. The user can normally access the Internet only after entering the account and password configured on the local server on the authentication page. You can choose **One-Device > Gateway > Config > Advanced > Authentication > Online Clients** to view information about the successfully connected user. For details, see Section [7.3 Online User Management](#).

7.1.6 Authorized Guest Authentication

1. Overview

The device is connected to the local authentication server. After a guest connects to Wi-Fi, the guest can access the Internet after the specified authorization IP user or account and password authentication user scans the QR code that pops up for guest authentication. For example, in the wireless office network, users in the employee network segment are authorized to scan the guest authentication QR code for users in the guest network segment.

2. Getting Started

Ensure that the device with the authentication function enabled has been connected to the Internet. Otherwise, the authentication page does not pop up when a client associates with Wi-Fi.

3. Configuration Steps

Choose **One-Device > Gateway > Config > Authentication > Web Authentication > Authorized Auth**.

Turn on **Authorized Auth**, configure **Popup Message**, **Auth IP / IP Range**, **Authorization IP/IP Range**, **Limit Online Duration**, **HTTPS Redirection**, and click **Save**.

Authorized Auth

Popup Message

* Auth IP / IP Range

Limit Online Duration

* Authorization IP/IP Range

HTTPS Redirection **Enable**

Table 7-6 Authorized guest authentication configuration

| Parameter | Description |
|-----------------------|--|
| Popup Message | Specify the text to be displayed on the pop-up QR code page. |
| Auth IP / IP Range | Specify the IP address range for users to be authenticated. The value can be a single IP address (such as 192.168.110.2) or an IP address range (such as 192.168.110.2-192.168.110.254). Users in the specified IP address range can access the Internet only after passing authentication. |
| Limit Online Duration | Specify whether to limit the online duration of guests. After you enable this function, you need to configure Duration Limit. If the online duration of a guest exceeds the specified value, the guest can continue Internet access only after re-authorization. By default, this function is disabled, indicating that guests can use Wi-Fi without limit on the online duration. |
| Duration Limit | Specify the maximum online duration of authorized guests. If the online duration of an authorized guest exceeds the specified value, the guest goes offline automatically and needs to be re-authorized for login again. |

| Parameter | Description |
|---------------------------|--|
| Authorization IP/IP Range | Specify the IP address range of authorization users. Users in this range can scan the QR code to authorize guests. |
| HTTPS Redirection | Enabling HTTPS redirection ensures that user data transmission during the authentication process is encrypted, thereby enhancing the security of the authentication process. When HTTPS redirection is disabled, authentication requests can only be sent to HTTP pages. |

4. Verifying Configuration

After a guest connects to Wi-Fi, the QR code authentication page pops up. The guest can access the Internet after the specified authorization user scans this QR code. After successful connection, you can choose **One-Device > Gateway > Config > Authentication > Online Clients** to view information about this authenticated user. For details, see Section [7.3 Online User Management](#).

7.1.7 Guest Authentication through QR Code Scanning

1. Overview

Guests scan the specified QR code to access the Internet. For example, in the wireless office network, guests scan the pasted QR code to access the Internet after they connect to Wi-Fi.

2. Getting Started

Ensure that the device with the authentication function enabled has been connected to the Internet. Otherwise, the authentication page does not pop up when a client associates with Wi-Fi.

3. Configuration Steps

Choose **One-Device > Gateway > Config > Authentication > Web Authentication > QR Code Auth**.

Turn on **QR Code Auth**, configure **Auth IP / IP Range**, **Limit Online Duration**, and **QR Code Generator**, and click **Save**.

QR Code Auth

* Auth IP / IP Range

Limit Online Duration

QR Code Generator

* Dynamic QR Code

Popup Message


Please print and paste the QR code for guests to scan.

Table 7-7 Guest authentication through QR code scanning configuration

| Parameter | Description |
|-----------------------|---|
| Auth IP / IP Range | Specify the IP address range for users to be authenticated. The value can be a single IP address (such as 192.168.110.2) or an IP address range (such as 192.168.110.2-192.168.110.254). Users in the specified IP address range can access the Internet only after passing authentication. |
| Limit Online Duration | Specify whether to limit the online duration of guests. After you enable this function, you need to configure Duration Limit. If the online duration of a guest exceeds the specified value, the guest needs to scan the QR code again before continuing Internet access. By default, this function is disabled, indicating that guests can use Wi-Fi without limit on the online duration. |
| Duration Limit | Specify the maximum online duration of authorized guests. If the online duration of an authorized guest exceeds the specified value, the guest goes offline automatically and needs to be re-authenticated. |
| Dynamic QR Code | The dynamic QR code is used to generate a QR code image. After the dynamic QR code is updated, the QR code image changes and the previous image becomes invalid. You can print and paste the generated QR code image, which can be scanned by guests to access the Internet. |

| Parameter | Description |
|---------------|---|
| Popup Message | Specify the QR code prompt message displayed on the page after a guest scans the QR code. |

4. Verifying Configuration

After a client connects to Wi-Fi, the guest can scan the QR code to pass authentication and access the Internet. You can choose **One-Device > Gateway > Config > Authentication > Online Clients** to view information about the successfully connected user. For details, see Section [7.3 Online User Management](#).

7.1.8 Authentication-Free

1. Overview

After IP addresses or MAC addresses are configured for authentication-free users, they can directly access the Internet without passing authentication. Traffic from all the users in the blocklist is blocked.

2. Configuring an Authentication-Free Intranet User

Choose **One-Device > Gateway > Config > Authentication > Web Authentication > Allowlist**.

Intranet User Allowlist: Users in the specified IP address range can directly access the Internet without passing authentication.

Click **Add** to configure the IP address range for authentication-free users. The value can be a single IP address (such as 192.168.110.2) or an IP address range (such as 192.168.110.2-192.168.110.254). A maximum of 50 entries are supported.

Intranet User Allowlist + Add Delete Selected

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

Up to 50 entries can be added. Total 0 < 1 > 10/page

Add ×

* IP / IP Range

Cancel
OK

3. Configuring Destination IP Addresses for Authentication-Free

Choose **One-Device > Gateway > Config > Authentication > Web Authentication > Allowlist**.

Destination IP Allowlist: Specify the IP addresses that can be accessed by all users including unauthenticated users.

Click **Add** to configure extranet IP addresses that can be assessed by users without authentication. A maximum of 50 entries are supported.

Destination IP Allowlist [+ Add](#) [Delete Selected](#)

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

Up to 50 entries can be added. Total 0 < 1 > 10/page

Add ×

* IP / IP Range

4. Configuring a Domain Allowlist

Choose **One-Device > Gateway > Config > Advanced > Authentication > Allowlist > Domain Allowlist**.

Domain Allowlist: Specify the URLs that can be accessed without authentication.

Click **Add**. In the dialog box that appears, enter the authentication-free URLs, and then click OK. When the destination URL of the user is in the **Domain Allowlist** traffic from the user will be permitted directly, regardless of whether the user passes authentication. A maximum of 100 entries are supported.

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

| <input type="checkbox"/> | URL | Action |
|--------------------------|--------------------|---|
| <input type="checkbox"/> | ruijienetworks.com | Edit Delete |

Up to 100 entries can be added. Total 1 < 1 > 10/page

Add ×

* URL

5. Configuring a User MAC Allowlist

Choose **One-Device > Gateway > Config > Advanced > Authentication > Allowlist > MAC Allowlist.**

MAC Allowlist: Clients whose MAC addresses are in the **Allowlist** can access the Internet through Wi-Fi without the need for authentication.

Click **Add**. In the dialog box that appears, enter the MAC addresses of authentication-free users, and then click **OK**. A maximum of 250 entries are supported.

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

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

Up to 250 entries can be added. Total 1 < **1** > 10/page ▾

Add ×

* MAC Address

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

6. Configuring a User MAC Blocklist

Choose **One-Device > Gateway > Config > Advanced > Authentication > Allowlist > MAC Blocklist.**

User MAC Blocklist Clients whose MAC addresses are in the blocklist are prohibited from accessing the Internet.

Click **Add**. In the dialog box that appears, enter the MAC addresses of users in the blocklist, and then click **OK**. A maximum of 250 entries are supported.

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

| <input type="checkbox"/> | MAC Address | Action |
|--------------------------|-------------------|---|
| <input type="checkbox"/> | 0A:2B:3C:4D:5F:6E | Edit Delete |

Up to 250 entries can be added. Total 1 < **1** > 10/page ▾

Add ×

* MAC Address

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

7.1.9 Custom Portal Page

Choose **One-Device > Gateway > Config > Authentication > Web Authentication > Customized Portal**.

1. Customized Portal

(1) On the **Customized Portal** page, click **Add**.

Customized Portal + Add

Up to 5 entries can be added.

| ID | Name | Action |
|----|----------------|-------------|
| 0 | Default Portal | Edit Delete |
| 1 | portal_1 | Edit Delete |
| 11 | portal_3 | Edit Delete |

Total 3 < 1 > 10/page

(2) Enter the portal page name and customize its content. The preview page will update in real-time as you enter the values.

Add

Name

Login Options Account

Post Url

Logo Image

Background Background Image Solid Color

Background Image

Languages English

Welcome Message

Marketing Message

Terms & Conditions

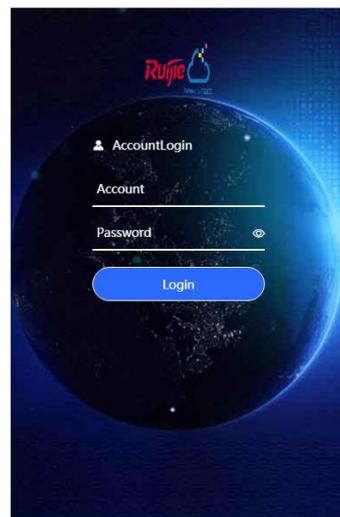
Copyright

title

Account Placeholder

Password Placeholder

Login Button



(3) Click **OK**.

2. Cloud Portal

In the **Cloud Portal** pane, the portal page configured in Ruijie Cloud is displayed. Click **View** to preview the page content.

Cloud Portal

| ID | Name | Action |
|----|------|----------------------|
| 2 | zyh | View |

Total 1 < 1 > 10/page

7.1.10 Global Configuration

Choose **One-Device > Gateway > Config > Authentication > Web Authentication > Global Config.**

1. Authentication Configuration

 Specification

Personal Status Page is only supported on the RG-EG105GW-X and RG-EG105GW(T) running ReyeeOS 2.340 or later.

You can configure the timeout period for an idle client. The default value is 15 minutes. If no traffic from an online user passes through the device within the specified period, the device will log out the user. The user can continue Internet access only after re-authentication.

You can set **Personal Status Page** to a domain name and **Protocol** to **http** or **https**. When a user accesses the domain name, you can view the online client information using the current account, including the IP address, MAC address, and uplink and downlink traffic of the client.

Auth Settings

* Idle Client Timeout: Min (Range: 5-65535)

Personal Status Page:  Accessing will automatically redirect the user to the personal status page.

Protocol:  http https

2. Account Expiration Reminder Settings

If a web-based authentication account is associated with a user group, you can configure the expiration reminder. The system will remind the user of renewal when the account is about to expire.

Account Expiration Reminder

* Reminder Time: Remind the user days before expiration

* Repeat Reminder Interval: Every hours

7.2 Configuring the PPPoE Server

7.2.1 Overview

Point-to-Point Protocol over Ethernet (PPPoE) is a network tunneling protocol that encapsulates PPP frames inside Ethernet frames. When the router functions as a PPPoE server, it provides the access service to LAN users and supports bandwidth management.

7.2.2 Global Settings

Choose **One-Device > Gateway > Config > Authentication > PPPoE Server > Global Settings**.

Set **PPPoE Server** to **Enable** and configure PPPoE server parameters.

PPPoE Server Enable Disabled

Mandatory PPPoE Dialup Enable Disable

* Local Tunnel IP

* IP Range

VLAN

Primary DNS Server

Secondary DNS Server

* Unanswered LCP Packet Limit Range: 1-60

Auth Mode PAP CHAP MSCHAP MSCHAP2

Expiration Reminder

A reminder portal page will appear when a user's account is nearing expiration. The user can continue browsing only after confirmation.

Save

Table 7-8 PPPoE server configuration

| Parameter | Description |
|------------------------------|--|
| PPPoE Server | Specify whether to enable the PPPoE server function. |
| Mandatory PPPoE Dialup | Specify whether LAN users must access the Internet through dialing. |
| Local Tunnel IP | Set the point-to-point address of the PPPoE server. |
| IP Range | Specify the IP address range that can be allocated by the PPPoE server to authenticated users. |
| VLAN | Set the VLAN of the current PPPoE server. |
| Primary/Secondary DNS Server | Specify the DNS server address delivered to authenticated users. |

| Parameter | Description |
|-----------------------------|---|
| Unanswered LCP Packet Limit | When the number of LCP packets not answered in one link exceeds the specified value, the PPPoE server automatically disconnects the link. |
| Auth Mode | Select at least one authentication mode from the following: PAP, CHAP, MSCHAP, and MSCHAP2. |
| Expiration Reminder | When an account is about to expire, a reminder portal page will appear. The user can continue to access the Internet only after confirmation. |

7.2.3 Configuring the PPPoE User Groups

Choose **One-Device > Gateway > Config > Authentication > Account > User Groups**.

If smart flow control is disabled, the configuration of the PPPoE user groups does not take effect. Before you configure a PPPoE user group, enable smart flow control first. For details on how to set smart flow control, see Section [8.6.2 Intelligence QoS](#).

Click the **PPPoE User Groups** tab and click **Add** to create a PPPoE user group. The currently created user groups for flow control are displayed in the user group list. You can modify or delete the user groups.

Cloud User Group Local User Groups **PPPoE User Groups** + Add Delete Selected

| <input type="checkbox"/> | User Group Name | Uplink Bandwidth | Downlink Bandwidth | Interface | Action |
|--------------------------|--------------------|--|--|-----------|-------------|
| <input type="checkbox"/> | Default user group | Limit-at 1000Mbps Max-Limit 1000Mbps Max-Limit per User No Limit | Limit-at 1000Mbps Max-Limit 1000Mbps Max-Limit per User No Limit | Each-WAN | Edit Delete |

Up to 10 entries can be added.

Add

* User Group Name

Uplink Bandwidth * Limit-at Mbps * Max-Limit Mbps ?

Downlink Bandwidth * Limit-at Mbps * Max-Limit Mbps ?

Max-Limit per User Uplink Mbps Downlink Mbps
Bandwidth Bandwidth

Apply To ? Designated interfaces ALL Interface

* Interface

Cancel **OK**

Table 7-9 PPPoE user flow control package configuration

| Parameter | Description |
|--------------------|---|
| Account Name | Set the name of the flow control package. When you configure an authentication account, you can select a flow control package based on the name. |
| Uplink Bandwidth | <p>The following uplink bandwidth options can be configured, all measured in Mbps.</p> <ul style="list-style-type: none"> ● Limit-at: Guaranteed available uplink bandwidth for authenticated users when bandwidth resources are limited. ● Max-Limit: Maximum available uplink bandwidth for authenticated users when bandwidth resources are sufficient. ● Max-Limit per User: Maximum available uplink bandwidth for each user. This parameter is optional and the default value is no limit. |
| Downlink Bandwidth | <p>The following downlink bandwidth options can be configured, all measured in Mbps.</p> <ul style="list-style-type: none"> ● Limit-at: Guaranteed available downlink bandwidth for authenticated users when bandwidth resources are limited. ● Max-Limit: Maximum available downlink bandwidth for authenticated users when bandwidth resources are sufficient. ● Max-Limit per User: Maximum available downlink bandwidth for each user. This parameter is optional and the default value is no limit. |
| Apply To | <ul style="list-style-type: none"> ● Designated interfaces: You need to select a specified interface or interfaces. Assume that a device has three outbound interfaces, if each user is allowed to use up to 10 Mbps upstream bandwidth and Interface is set to Each-WAN, the bandwidth is limited to 10 Mbps per WAN port and a maximum of 30 Mbps bandwidth is available to the user. ● ALL Interface: The flow control policy applies to the entire device. Regardless of the number of WAN ports on the device, the maximum bandwidths available to each user are the values specified in the Max-Limit per User fields. |
| Interface | Specify the interface to which the flow control package applies. |

7.2.4 Configuring a PPPoE User Account

Choose **One-Device > Gateway > Config > Authentication > Account > Accounts**.

Click **PPPoE Accounts** and click **Add** to create a PPPoE authentication user account. The currently created PPPoE authentication user accounts are displayed in the **Account List** section. Find the target account and click **Edit** to modify the account information. Find the target account and click **Delete** to delete the account.

Cloud Accounts Cloud Voucher Local Authentication Accounts **PPPoE Accounts**

i If you want to use the Batch Config or Backup Config feature, Office 2019 or a later version is required. Otherwise, invalid format and garbled text may occur.
 Concurrent Devices 128 Clients 0

Search by Username Batch Config Backup Config **+ Add** Delete Selected

| <input type="checkbox"/> | Username | Password | Expire Date | Status | Account Management | Remarks | Action |
|--------------------------|----------|----------|-------------|--------|--------------------|---------|--------|
| No Data | | | | | | | |

Up to 300 entries can be added. Total 0 < 1 > 10/page

Add ×

* Username

* Password

Expire Date

Remarks

Status

Rate Limiting

* Account Management

Table 7-10 PPPoE user account configuration

| Parameter | Description |
|-------------------|--|
| Username/Password | Set the username and password of the authentication account for Internet access through PPPoE dialing. |
| Expire Date | Set the expiration date of the authentication account. After the account expires, it can no longer be used for Internet access through PPPoE authentication. |
| Remark | Enter the account description. |

| Parameter | Description |
|--------------------|--|
| Status | Specify whether to enable this user account. If the account is disabled, the account is invalid and cannot be used for Internet access through PPPoE authentication. |
| Rate Limiting | Specify whether to apply flow control on the account. If flow control is enabled, you need to configure flow control policies for the PPPoE authentication user. If smart flow control is disabled, Rate Limiting must be turned off. To turn on Rate Limiting, enable smart flow control first. |
| Account Management | After Rate Limiting is toggled on, you need to associate a PPPoE user group with the current account to restrict the user bandwidth according to the user group. For details about the configuration of a PPPoE user group, see Section 7.2.3 Configuring the PPPoE User Groups . |

7.2.5 Configuring Exceptional IP Addresses

Choose **One-Device > Gateway > Config > Advanced > PPPoE Server > Exceptional IP Address**.

When the PPPoE server is enabled, if you want to allow some IP addresses in a specific VLAN to access the Internet without passing account and password authentication, you can configure these IP addresses as exceptional IP addresses.

The currently created exceptional IP addresses are displayed in the **Exceptional IP Address List** section. Click **Edit** to modify the exceptional IP address. Click **Delete** to delete the exceptional IP address.

Exceptional IP Address List + Add Delete Selected

| | Start IP Address ? | End IP Address ? | Remarks ? | Status ? | Action |
|--------------------------|--------------------|------------------|-----------|----------|---|
| <input type="checkbox"/> | 192.168.2.3 | 192.168.2.4 | | Enable | Edit Delete |

Up to 5 entries can be added.

Add ×

* Start IP Address ?

* End IP Address ?

Remarks ?

Status ?

Cancel
OK

- **Start IP Address/End IP Address:** Start and end of exceptional IP addresses.
- **Remark:** Description of an exceptional IP address.
- **Status:** Whether the exceptional IP address is effective.

7.3 Online User Management

Choose **One-Device > Gateway > Config > Authentication > Online Clients**.

The online client list displays information about all the current online clients, including the client IP addresses, client MAC addresses, login time, and authentication modes. You can locate a client based on the IP address, MAC address, or username.

Online Clients

Search by IP Address

| <input type="checkbox"/> | Username | IP | Device Name | MAC Address | Online Time | Duration(Sec) | Auth Type | Status | Action |
|--------------------------|----------|----|-------------|-------------|-------------|---------------|-----------|--------|--------|
| No Data | | | | | | | | | |

Total 0

8 Online Behavior Management

8.1 Overview

Online behavior management aims to block or prohibit specific Internet access behaviors of LAN users. Online behavior management functions are classified into five categories: app control, website filtering, QQ management, flow control, and access control. The effective range of each behavior management policy is flexibly controlled by the specified client IP address and effective time.

8.2 User Management

8.2.1 Overview

The management policy of online behavior needs to flexibly match with specific user groups. Please manage and classify users before the behavior management policy is configured, ensuring efficient configuration and management. User management is used to maintain user information based on IP addresses. When managing online behaviors, you can limit the effective scope of application blocking, traffic auditing, flow control and other services by specifying created or authenticated users.

User groups contain three default root user groups: User Group, Authentication Group and VPN Group. You can create and configure users and user groups under the root user group.

i 400 of entries that can be added in a user group. Current User Groups: 1; Current Users: 1.

+ Add
Delete Selected

| | Username | IP Range | MAC | Action | |
|--|--------------------------|---------------|-------------------------|--------|---------------------------------------|
| <ul style="list-style-type: none"> User Group + ▼ Authentication Group <ul style="list-style-type: none"> Local Authentication ... VPN Group | <input type="checkbox"/> | All Addresses | 1.1.1.1-255.255.255.255 | - | Edit Delete |

Total 1
<
1
>
10/page

i **Note**

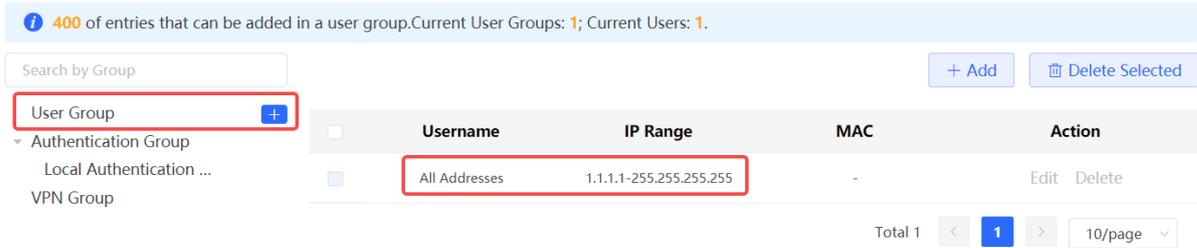
The system creates a VPN user group by default. The VPN accounts added in the system are automatically added to a VPN user group. You can select a VPN user group to control VPN accounts when you create a policy of application control, network management or flow control.

8.2.2 User Group

Choose **One-Device > Gateway > Config > Behavior > User Management**.

You can add new user groups or users below the first-level user group. Up to three levels of grouping is supported. If a user is a leaf node, no users or user groups can be created below this leaf node. A created user group can be used as a configuration item in a behavior management policy and is directly referenced by the user group name.

All Addresses client exists in the user group list by default. The IP range is from 1.1.1.1 to 255.255.255.255. This client cannot be edited or deleted.



1. Creating a User Group

Click  near **User Group** or click **Add** at the upper right of the page. Select the type of **User Group** and enter the group name, and click **OK**. You can create a sub-user group below this user group.

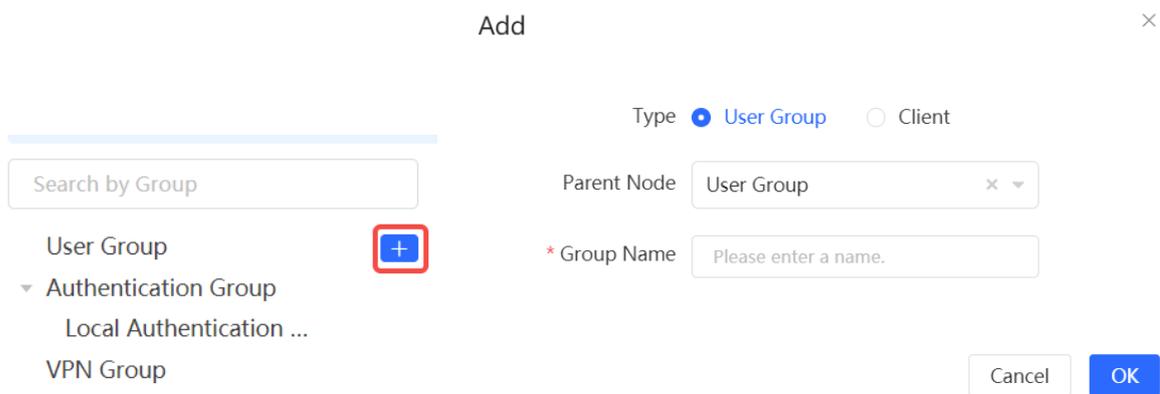


Table 8-1 Parameter Descriptions of User Group

| Parameter | Description |
|-------------|---|
| Parent Node | Configure the parent group to which the created user group belongs. Up to three levels of groups are allowed below a user group currently (such as Root Node/R&D Center/R&D Section 1). No user groups are allowed below the third-level group. |
| Group Name | Configure the name of the user group. |

2. Creating a User

Click **User Group** to display the users in the current group. Click  or click **Add** at the upper right of the page. Select the type of **Client** and enter the user name and IP range, and click **OK**. You can create a user under the user group.

Search by Group + Add Delete Selected

- ▼ User Group
 - ruijie + -
- ▼ Authentication Group
 - Local Authentication ...
 - VPN Group

| | Username | IP Range | MAC | Action |
|--------------------------|---------------|-------------------------|-----|-------------|
| <input type="checkbox"/> | All Addresses | 1.1.1.1-255.255.255.255 | - | Edit Delete |

Total 1 1 10/page

Add

Type User Group Client

Parent Node x ▼

* Username

Type IP MAC

* IP / IP Range

Cancel
OK

Table 8-2 Parameter Descriptions of User

| Parameter | Description |
|--------------|---|
| Parent Node | Configure the group to which the created user belongs, Click the drop-down list box to display all the currently created user groups and click to select one group. |
| Username | Configure the name of the user. |
| IP /IP Range | Configure the IP address of the user. You can enter an IP address or IP range. If a rule is valid to this user, the rule takes effect in this IP range. |

3. Deleting a User Group or a User

Click - near **User Group** to delete the user group and its members. Click **Delete** in the **Action** bar in the user list to delete the specified user.

Search by Group + Add Delete Selected

- ▼ User Group
 - ruijie + -
- ▼ Authentication Group
 - Local Authentication ...
 - VPN Group

| | Username | IP Range | MAC | Action |
|--------------------------|----------|--------------|-----|---|
| <input type="checkbox"/> | user1 | 192.168.11.1 | - | Edit Delete |

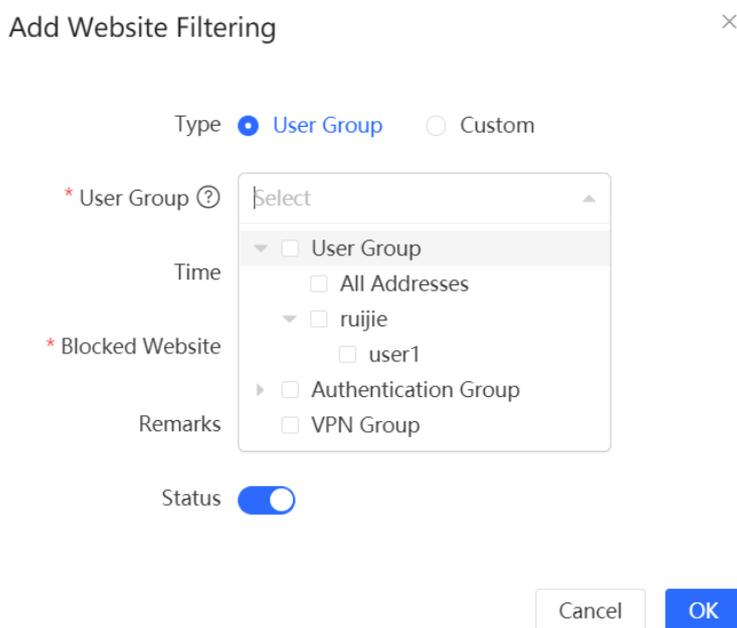
Total 1 1 10/page

4. Verifying Configuration

- (1) You can view the created user groups on the left part of the page after user groups and users are configured. Click **User Group** to view user details in this group.



- (2) When configuring the behavior management policy (such as adding an application control rule), you can view and select the created user groups and the members.



8.2.3 Authentication Group

Choose **One-Device > Gateway > Config > Behavior > User Management**.

The users in the **Authentication Group** are synchronized from the authentication server to the **Authentication Group**. The local authentication account set by the device (See Section [7.1.5 Local Account Authentication](#) for details.) is automatically synchronized to the **Local Authentication Group**.

Cloud Auth Local Account Auth Authorized Auth QR Code Auth Allowlist Online Clients

* Auth IP / IP Range Add

MAB validity period

* Custom Time days

Save

Account Settings

| <input type="checkbox"/> | Username | Password | At most of Concurrent Users | MAC Address | Action |
|--------------------------|----------|----------|-----------------------------|-------------|-------------|
| <input type="checkbox"/> | test | ***** | 5 | | Edit Delete |

Up to 200 accounts can be added. Total 1

- ▼ User Group
 - ruijie
- ▼ Authentication Group
 - ▼ Local Authentication ...
 - test**
- VPN Group

When configuring the behavior management policy (such as adding an application control rule), you can configure a policy to take effect in the specified authentication group. After an authenticated user goes online, the user automatically matches with the authentication group and then associates with the behavior management policy, enabling online behavior control over the authenticated user.

Add Website Filtering

Type User Group Custom

* User Group

Time

* Blocked Website

Remarks

Status

- ▼ User Group
 - All Addresses
- ▼ ruijie
 - user1
- ▼ Authentication Group
 - ▼ Local Authentication Gro...
 - test
- VPN Group

8.3 Time Management

Choose **One-Device > Gateway > Config > Behavior > Time Management**.

You can create time entries to classify time information. A created time entry can be used as a configuration item in a behavior management policy and is directly referenced by the time entry name.

All the created time entries are displayed in the time entry list. In the list, find the target time entry and click **Edit** to modify the time span. Find the target time entry and click **Delete** to delete it. By default, the time entries named **All Time**, **Weekdays**, and **Weekends** are available and they cannot be modified or deleted.

⚠ Caution

If a time entry is referenced in any policy, it cannot be deleted on the **Time Management** page. To delete the time entry, remove the reference relationship first.

| Time List | | + Add | Delete Selected |
|--------------------------|--------------------------|-----------------------|---|
| <input type="checkbox"/> | Schedule Name | Time Span | Action ? |
| <input type="checkbox"/> | app_6BD100B822B681658CE0 | | Edit Delete |
| <input type="checkbox"/> | app_84581586C3D5FDF2FF15 | | Edit Delete |
| <input type="checkbox"/> | Weekends | | Edit Delete |
| <input type="checkbox"/> | Weekdays | | Edit Delete |
| <input type="checkbox"/> | All Time | | Edit Delete |

Up to 20 entries can be added.

8.3.1 Configuring a Schedule by Week

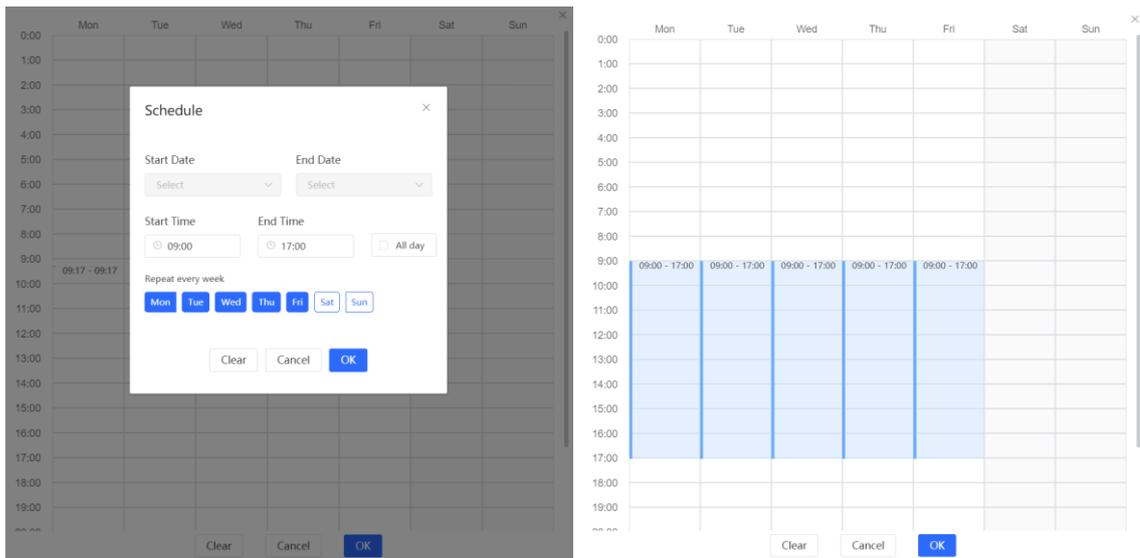
Add Schedule ×

* Schedule Name

System Time **Week** Day

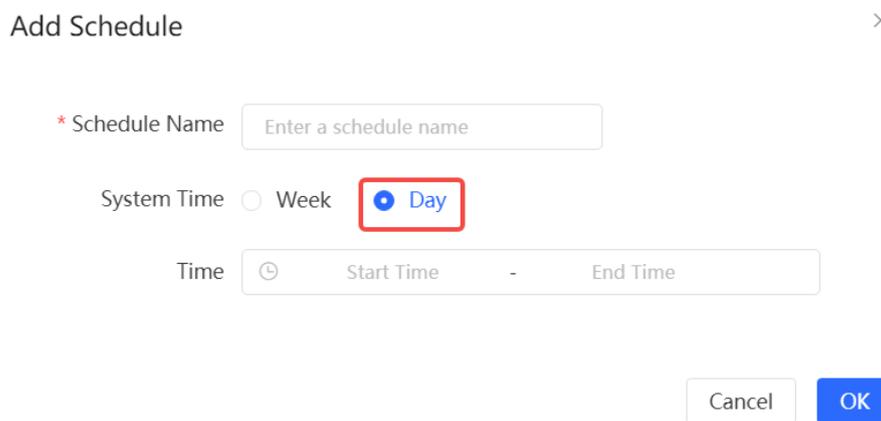
* Time [Schedule](#)

- (1) Click **+Add**. On the **Add Schedule** page that is displayed, enter the name of the schedule.
- (2) Set **System Time** to **Week**.
- (3) Click **Wireless Schedule** to set the time period. On the **Schedule** pop-up box, set the time period to be repeated every week and click **OK**.



(4) Click **OK**.

8.3.2 Configuring a Schedule by Date



- (1) Click **+Add**. On the **Add Schedule** page that is displayed, enter the name of the schedule.
- (2) Set **System Time** to **Day**.
- (3) Choose the start and end dates, and click **OK**.

2024-03-22

10:00

>

2024-04-21

00:00

2024 March

| Sun | Mon | Tue | Wed | Thu | Fri | Sat |
|-----|-----|-----|-----|-----|-----|-----|
| 25 | 26 | 27 | 28 | 29 | 1 | 2 |
| 3 | 4 | 5 | 6 | 7 | 8 | 9 |
| 10 | 11 | 12 | 13 | 14 | 15 | 16 |
| 17 | 18 | 19 | 20 | 21 | 22 | 23 |
| 24 | 25 | 26 | 27 | 28 | 29 | 30 |
| 31 | 1 | 2 | 3 | 4 | 5 | 6 |

2024 April

| Sun | Mon | Tue | Wed | Thu | Fri | Sat |
|-----|-----|-----|-----|-----|-----|-----|
| 31 | 1 | 2 | 3 | 4 | 5 | 6 |
| 7 | 8 | 9 | 10 | 11 | 12 | 13 |
| 14 | 15 | 16 | 17 | 18 | 19 | 20 |
| 21 | 22 | 23 | 24 | 25 | 26 | 27 |
| 28 | 29 | 30 | 1 | 2 | 3 | 4 |
| 5 | 6 | 7 | 8 | 9 | 10 | 11 |

Clear OK

(4) Click **OK**.

8.4 App Control

8.4.1 Overview

App control aims at controlling the range of specific apps that can be accessed by users. By default, users can access any app. After an app control policy is configured, users in the current network cannot access prohibited apps. App access can be prohibited based on the specified client IP address and time range. For example, employees in the office network are prohibited from accessing entertainment and game software during work periods to improve network security.

8.4.2 Configuring App Control

Choose **One-Device > Gateway > Config > Behavior > App Block > App Control**.

1. Switching the Application Library

The application lists vary in different regions. The Chinese and International versions of the application library are provided. Please select the version based on the regions.

Click to select **Application Library Version** and click **OK**. The version is switched after a few minutes.

⚠ Caution

- It takes about one minute to switch the application library version. Please wait.
- If you switch the application library, the old application control policy may be inactive. Please proceed with caution.

🔍 Application Library Version:

International

▼
+ Add
🗑 Delete Selected

2. Configuring App Control

Click **Add** to create an app control policy.

App Control + Add Delete Selected

| <input type="checkbox"/> | User Group | Time ? | Blocked applications ? | Status ? | Remarks ? | Action |
|--------------------------|--|----------|------------------------|----------|--------------------------------|-------------|
| <input type="checkbox"/> | User Group | All Time | ██████████ | Enable | | Edit Delete |
| <input type="checkbox"/> | User Group/3dbbuser Unknown | All Time | ... More | Enable | BLOCK_7708EBC4CF4490C 55D68 | Edit Delete |

Up to 50 entries can be added.

Add ×

Type User Group Custom

* User Group ?

Time ?

Application Blocked applications Blocked Application Group

* Application List

Remarks ?

Status ?

Table 8-3 App control policy configuration

| Parameter | Description |
|------------------|--|
| Type | <ul style="list-style-type: none"> ● User Group: The policy is applicable to users in the specified user group. Please select the target user group. ● Custom: The policy is applicable to users in the specified IP range. Please manually enter the managed IP range. |
| User Group | <p>Select the users managed by the policy from the list of user groups. For the configuration of the user group list, see Section 8.2 User Management.</p> <p>If all members in the user group are selected, the policy takes effect for the user group and is also valid for new members added to this group.</p> |
| IP Address Group | <p>If the IP range is restricted by the APP control policy and the type of the policy is set to Custom, please enter the IP range manually.</p> |

| Parameter | Description |
|------------------|---|
| Time | Specify the time range under app control. In the specified time range, managed clients cannot access the selected apps in the list of prohibited apps. You can select a time range defined in Section 8.3 Time Management from the drop-down list box, or select Custom and manually enter the specific time range. |
| Application | Specify the applications or application groups to block. |
| Application List | When Blocked applications is selected, you can select the applications that need to be blocked. |
| App Group | When Blocked Application Group is selected, you can select the application groups that need to be blocked. |
| Remarks | Enter the policy description. |
| Status | Specify whether to enable the app control policy. |

8.4.3 Custom App

1. Overview

Based on traffic packets of certain websites or apps that are captured by the device, users can analyze and extract 5-tuple information characteristics (protocol, source IP address, source port, destination IP address, and destination port) of the packets. You can define apps that are not in the default application list.

After custom apps are configured successfully, you can configure control policies for custom apps on the app control page to block users from accessing the custom apps on the current network.

2. Procedure

Choose **One-Device > Gateway > Config > Behavior > App Block > Custom**.

(1) Switch the application library.

The supported app list varies with regions. There are the application library of the Chinese version and the application library of the international version. Select an application library version based on the actual region.

Click **Application Library Version** and select a version. In the displayed dialog box, click **OK**. Wait a period of time for the system to complete switching.

Caution

Switching the application library version takes about 1 minute to take effect.

After the application library version is switched, the original app control policy may become invalid.

Therefore, exercise caution when performing this operation.

(2) Click **Add**. Enter information about a custom app.

Custom

| <input type="checkbox"/> | App | Protocol Type | Source IP | Destination IP | Source Port | Destination Port | Action |
|--------------------------|-----|---------------|-------------|----------------|-------------|------------------|---|
| <input type="checkbox"/> | APP | TCP | Auto Assign | 192.168.10.1 | Auto Assign | 80 | Edit Delete |

Up to 500 entries can be added. Total 1

Add ×

* App

Protocol Type

Control Type

* Destination IP Enter Manually Auto Assign

* Destination Port Enter Manually Auto Assign

Table 8-4 Description of Custom App Configuration

| Parameter | Description |
|---------------|---|
| App | Configure the app name (the name cannot be duplicated with a name in the app list). |
| Protocol Type | Select a protocol type based on the protocol used by captured packets. It can be set to TCP , UDP , or IP . |
| Control Type | Select a rule type based on 5-tuple information characteristics of extracted packets. It can be set to the following: <ul style="list-style-type: none"> ● Src IP + Src Port ● Dest IP + Dest Port ● Src IP+ Dest IP |

| Parameter | Description |
|-------------------------|-------------------------------------|
| Source/Destination IP | Enter a characteristic IP address. |
| Source/Destination Port | Enter a characteristic port number. |

Note

- If **Control Type** is set to **Src IP + Src Port**, you need to set the source IP address and source port.
- If **Control Type** is set to **Dest IP + Dest Port**, you need to set the destination IP address and destination port.
- If **Control Type** is set to **Src IP + Dest IP**, you need to set the source and destination IP addresses. The source IP address can be also to **Auto Assign**.

(3) Click **OK**.

Custom

| | App | Protocol Type | Source IP | Destination IP | Source Port | Destination Port | Action |
|--------------------------|------|---------------|-------------|----------------|-------------|------------------|---|
| <input type="checkbox"/> | APP | TCP | Auto Assign | 192.168.10.1 | Auto Assign | 80 | Edit Delete |
| <input type="checkbox"/> | test | IP | Auto Assign | 192.168.1.1 | Auto Assign | Auto Assign | Edit Delete |

Up to 500 entries can be added.
Total 2

8.4.4 Custom Application Group

1. Overview

You can add multiple applications with the same features into a customer application group, which is a logical group. The custom application group can be used for policy.

The system has a default blocking group to block applications. (The blocking group is associated with relevant applications by default.) The applications added to the blocking group are directly blocked.

2. Procedure

Choose **One-Device > Gateway > Config > Behavior > App Block > Custom Application Group**.

(1) Switch the application library version.

The supported application list varies with regions. The application library version falls into the Chinese version and the international version. Select an application library version based on the actual region.

Click **Application Library Version** and select a version. In the displayed dialog box, click **OK**. Wait a moment for the system to complete switching.

Caution

Switching the application library version takes about one minute. Please wait for the configuration to take effect.

The existing custom application group is invalid after the application library version is switched. Therefore, exercise caution when performing this operation.

Application Library Version: International + Add Delete Selected

(2) Click **Add** to configure the parameters for an application group.

Custom Application Group App

| <input type="checkbox"/> | Group Name | Application List | Citation Count | Remarks | Action <input type="button" value="ⓘ"/> |
|--------------------------|--|------------------|----------------|---------|---|
| <input type="checkbox"/> | Block Group <input type="button" value="ⓘ"/> | - | 1 | - | <input type="button" value="Edit"/> <input type="button" value="Delete"/> |

Up to 20 entries can be added. Total 1 1

Add



* Group Name

Application List

Remarks

Table 8-5 Custom Application Group

| Parameter | Description |
|------------------|---|
| Group Name | The application group name customized by a user. (The group name must differ from the application names in the group list.) |
| Application List | Multiple applications involved in an application group. |
| Remark | Description of an application group. |

(3) Click **OK**.

8.5 Website Management

8.5.1 Overview

Website management consists of website grouping and website filtering. Website grouping refers to the classification of website URLs. You can modify existing website groups or create new website groups. Website

filtering refers to access control to existing website groups to prohibit user access to websites in specific groups. Website filtering can be applied based on the specified client IP address and time range. For example, employees in the office network are prohibited from accessing game websites during work periods to improve network security.

8.5.2 Configuration Steps

Choose **One-Device > Gateway > Config > Behavior > Website Management**.

1. Configuring Website Groups

Choose **One-Device > Gateway > Config > Behavior > Website Management > Website Group**.

Click the **Website Group** tab. On the page that appears, all the created website groups are displayed in the list. Find the target group and click **More** in the **Member** column to view all the website URLs in the group. Find the target group and click **Edit** in the **Action** column to modify the member website URLs in the group. Find the target group and click **Delete** in the **Action** column to delete the group.

Click **Add** to create a new website group.

 **Caution**

If a website filtering rule in a website group is being referenced, the group cannot be deleted from the website group list. To delete this group, modify the website filtering configuration to remove the reference relationship first.

| Website Group | | Website Filtering | + Add | Delete Selected |
|--------------------------|------------|---|-----------------------|---------------------------------|
| <input type="checkbox"/> | Group Name | Member | Action | |
| <input type="checkbox"/> | Games | duowan.com... More | Edit | Delete |
| <input type="checkbox"/> | Finance | *.10jqka.com.cn... More | Edit | Delete |
| <input type="checkbox"/> | Social | *.baihe.com... More | Edit | Delete |
| <input type="checkbox"/> | Shopping | *.taobao.com... More | Edit | Delete |
| <input type="checkbox"/> | Life | *.55bbs.com... More | Edit | Delete |
| <input type="checkbox"/> | Music | *.1ting.com... More | Edit | Delete |

Add Group

×

*** Group Name**

*** Member**

Set group members. The group member can be a complete URL (example: www.baidu.com) or a domain (example: *.56.com). If you want to add a domain, please make sure that the domain starts with *.

Cancel
OK

Table 8-6 Website group configuration

| Parameter | Description |
|------------|--|
| Group Name | Configure a unique name for the website group. The name can be a string of 1 to 64 characters. |
| Member | Specify members in the website group. You can enter multiple websites in a batch. The group member can be complete URL (such as www.baidu.com) or keywords in the URL (domain name with a wildcard in front, such as *.baidu.com). The wildcard can only appear at the beginning of a URL, and it cannot be in the middle or end of the domain name. |

2. Configuring Website Filtering

Choose **One-Device > Gateway > Config > Behavior > Website Management > Website Filtering**.

Click the **Website Filtering** tab. On the page that appears, all the created website filtering rules are displayed in the list. Click Edit to modify the rule information. Click Delete to delete the specific filtering rule.

Click **Add** to create a website filtering rule.

Website Filtering

+ Add
Delete Selected

| <input type="checkbox"/> | User Group | Control Type | Blocked Website | Time | Status | Remarks | Action |
|--------------------------|------------|--------------|-----------------|------|--------|---------|--------|
| No Data | | | | | | | |

Up to 20 entries can be added.

Add Website Filtering
×

Type User Group Custom

* User Group (?)

Time

* Blocked Website

Remarks

Status

Table 8-7 Website filtering rule configuration

| Parameter | Description |
|------------------|---|
| Type | <ul style="list-style-type: none"> ● User Group: The policy is applicable to users in the specified user group. Please select the target user group. ● Custom: The policy is applicable to users in the specified IP range. Please manually enter the managed IP range. |
| User Group | <p>Select the users managed by the policy from the list of user groups. For the configuration of the user group list, see Section 8.2.2 User Group.</p> <p>If all members in the user group are selected, the policy takes effect for the user group and is also valid for new members added to this group.</p> |
| IP Address Group | <p>If the IP range is restricted by the APP control policy and the type of the policy is set to Custom, please enter the IP range manually.</p> |
| Time | <p>Specify the time range under website filtering control. In the specified time range, managed clients cannot access the prohibited websites. You can select a time range defined in Section 8.3 Time Management from the drop-down list box, or select Custom and manually enter the specific time range.</p> |
| Blocked Website | <p>Configure the type of websites to block. You can select an existing website group. After a website group is selected, users are prohibited from accessing all websites in this group. For details on how to create or modify a website group, see Configuring Website Groups.</p> |
| Remarks | <p>Enter the rule description.</p> |

| Parameter | Description |
|-----------|---|
| Status | Specify whether to enable the website filtering rule. |

8.6 QoS

8.6.1 Overview

QoS is a mechanism that classifies flows based on certain rules and processes flows using different policies based on their categories. You can configure QoS to guarantee key flows and suppress malicious flows. You can enable QoS when the bandwidth is insufficient or flows need to be distributed properly.

8.6.2 Intelligence QoS

1. Overview

When you need to limit the uplink traffic and downlink traffic bandwidth of the device ports (such as WAN and WAN 1), you can enable the smart QoS function. After the line bandwidth is configured for a port, the uplink and downlink traffic of the port will be limited within the specified range. In addition, the per user bandwidth should be intelligently adjusted according to the number of users to ensure that users fairly share the bandwidth.

2. Configuration Steps

Choose **One-Device > Gateway > Config > Behavior > QoS > Smart QoS**.

Enable  If you want to test the WAN rate, please disable smart flow control first.

WAN0 Bandwidth  * Uplink Mbps * Downlink Mbps

WAN1 Bandwidth  * Uplink Mbps * Downlink Mbps

Turn on **Enable** on the **Smart QoS** tab and set the line bandwidth based on the bandwidth actually allocated by the ISP. If the device has multiple lines, you can set the bandwidth for these WAN ports separately. For details on the multi-line configuration, see Section [4.2 Port Settings](#).

Click **Save** to make the configuration take effect.

Caution

Enabling QoS will affect network speed testing. If you want to test the network speed, disable QoS first.

Table 8-8 Smart QoS configuration

| Parameter | Description |
|---------------|--|
| Enable | Specify whether to enable the smart QoS function. By default, smart QoS is disabled. |
| WAN Bandwidth | Set the uplink and downlink bandwidth limits for the WAN ports, in Mbit/s. |

Note

Smart QoS can be used to control the line traffic in different networking modes, including bandwidth-based, static IP address, and dynamic IP address.

8.6.3 Custom Policies

1. Overview

Custom policies are used to restrict the traffic with specific IP addresses based on the smart QoS function, thereby meeting the bandwidth requirements of specific users or servers. When you create a custom QoS policy, you can flexibly configure the limited IP address range, the bandwidth limit, the limited application traffic, and the rate limit mode. When a custom policy is enabled, it takes precedence over the smart QoS configuration.

2. Getting Started

Before you configure a custom policy, enable smart QoS first. For details, see Section [8.6.2 Intelligence QoS](#).

3. Configuring a Normal Policy

Choose **One-Device > Gateway > Config > Behavior > QoS > Custom Policy**.

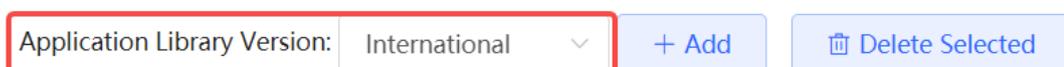
Note

The QoS policies configured on Ruijie Cloud and the web interface are displayed in the **Normal Policy** list. The QoS policies for authentication accounts configured on Ruijie Cloud cannot be edited or deleted on the web interface. You can only enable or disable these policies and change the priority of them.

(1) (Optional) Switch the application library

The application lists vary in different regions. The Chinese and International versions of the application library are provided. Please select the version based on the regions.

Click to select **Application Library Version** and click **OK**. The version is switched after a few minutes.



⚠ Caution

- It takes about one minute to switch the application library version. Please wait.
- If you switch the application library, the template of the application priority will be reset (See Section [8.6.4 Application Priority](#) for details.), and the old application control policy may be inactive (See Section [8.4 App Control](#) for details.). Please proceed with caution.

(2) Set **Policy Type** to **Normal Policy** and click **Add** to create a custom QoS policy.

You can set up to 30 custom common policies, including the custom policies configured on the web interface and Ruijie Cloud.

You can set up to 20 QoS policies for authentication accounts on Ruijie Cloud. The web interface only displays these policies.

Add ×

* Policy Name

Type User Group Custom

* User Group

Application All Applications App Group Custom

Bandwidth Type Shared Independent

Bandwidth Limit Limit No Limit

Uplink Bandwidth Mbps Mbps

Downlink Bandwidth Mbps Mbps

* Interface

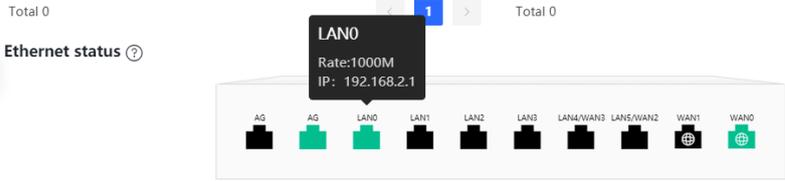
Enabled

----- Advanced Settings -----

IP/DSCP Priority

Channel Priority

Time

| Parameter | Description |
|-------------------|---|
| User Group | <p>Select a user to be managed by the policy from the user group list. For details about how to set the user group list, see Section 8.2 User Management.</p> <p>If you select all members of a user group, the policy takes effect on the entire user group (it also takes effect on members added to the user group later).</p> <p>This parameter is required when Type is set to User Group.</p> |
| IP/IP Range | <p>Specify the IP address range for the QoS policy to take effect. When Type is set to Custom, enter the IP address manually. You can enter a single IP address or an IP address segment.</p> <p>This parameter is required when Type is set to Client.</p> <p>The IP address range must be within a LAN segment. You can choose One-Device > Gateway > Monitor > Ethernet status to check the network segment of the current LAN port. For example, the network segment of the LAN port shown in the figure below is 192.168.2.0/24.</p>  <p>The screenshot shows a network interface configuration page. At the top, there are navigation buttons and 'Total 0' indicators. Below that, the 'Ethernet status' section is active, displaying a list of network ports: AG, AG, LAN0, LAN1, LAN2, LAN3, LAN4/WAN3, LAN5/WAN2, WAN1, and WAN0. The LAN0 port is highlighted with a tooltip that shows 'LAN0', 'Rate:1000M', and 'IP: 192.168.2.1'.</p> |
| Application | <p>When Bandwidth Type is set to Shared, the QoS policy can be configured to take effect only on specified applications.</p> <ul style="list-style-type: none"> ● All Applications: Indicates that the QoS policy takes effect on all applications in the current application library. ● Application Group: Indicates that the QoS policy takes effect only on specified applications in the application list. For details about how to set the application group list, see Section 8.4.4 Custom Application Group. ● Custom: Indicates that the QoS policy takes effect only on specified applications in the application list. <p>When Bandwidth Type is set to Independent, some models do not support application selection and the QoS policy takes effect on all applications in the current application library by default.</p> <p>For the models, contact technical support engineers.</p> |
| Application List | <p>When Application is set to Custom, it specifies the applications, on which the policy takes effect. The traffic of the selected applications is subject to the policy.</p> |
| Application Group | <p>When Application is set to Application Group, it specifies the application groups, on which the policy takes effect. The traffic of the selected application group is subject to the policy.</p> |
| Bandwidth Type | <ul style="list-style-type: none"> ● Shared: Indicates that all users in a user group (all IP addresses in an address range) share the configured uplink and downlink bandwidths, and the bandwidth of a single user is not limited. ● Independent: Indicates that all users in a user group (all IP addresses in an address range) share the configured uplink and downlink bandwidths, and the maximum bandwidth of a single user can be limited. |

| Parameter | Description |
|---------------------------|---|
| Bandwidth Limit | <p>Configure whether to limit the bandwidth.</p> <ul style="list-style-type: none"> ● Limit: You can set the uplink and downlink bandwidth limits as needed. ● No Limit: When the bandwidth is sufficient, the maximum bandwidth is not limited. When the bandwidth is insufficient, the minimum bandwidth cannot be guaranteed. |
| Uplink/Downlink Bandwidth | <p>Configure the data transmission rate in uploading and downloading, in Mbps. It includes Limit-at, Max-Limit, and Max-Limit per User.</p> <ul style="list-style-type: none"> ● Limit-at: Specifies the minimum bandwidth that can be shared by all users when the bandwidth is insufficient. ● Max-Limit: Specifies the total maximum bandwidth that can be occupied by all users when the bandwidth is sufficient. ● Max-Limit per User: Specifies the maximum bandwidth that can be occupied by each user when multiple users share the bandwidth. It is optional and can be configured only when Bandwidth Type is set to Independent. The rate is not limited by default. |
| Apply To | <p>In ReyeeOS 2.340 and later, when the Bandwidth Type is set to Independent, you can select the scope of application for the traffic policy.</p> <ul style="list-style-type: none"> ● Designated interfaces: You need to select specific interfaces. For example, if the device has three WAN ports and each user is limited to a maximum of 10 Mbps upload bandwidth, selecting Each-WAN means the total available bandwidth will add up to 30 Mbps for the user. ● ALL Interface: The traffic control policy applies at device level. Each user's maximum bandwidth is limited to the value specified in Max-Limit per User, regardless of the number of WAN ports. |
| Interface | <p>Specify the WAN port, on which the policy takes effect. When it is set to All WAN Ports, the policy will be applied to all WAN ports.</p> |
| Enabled | <p>Set whether to enable the QoS policy. If it is disabled, the policy does not take effect.</p> |
| IP/DSCP Priority | <p>Specifies the priority of packets to differentiate various types of traffic and allocate different levels of service quality. QoS policies are applied based on the IP/DSCP field in the packet.</p> |
| Channel Priority | <p>Specify the traffic guarantee level. The value range is from 0 to 7. A smaller value indicates a higher priority and the value 0 indicates the highest priority.</p> <p>Different traffic priority values correspond to different application groups in an application template. 2 indicates the key group, 4 indicates the normal group, and 6 indicates the suppression group. For the description of application groups in a priority template, see 8.6.4 Application Priority.</p> |
| Time | <p>Specifies the time period during which the rule takes effect. You can choose from existing time rules or create custom ones.</p> |

 **Caution**

After switching the application library version, you may need to reconfigure the application list.

(4) Click **OK**.

4. Configuring a VPN policy

Choose **One-Device > Gateway > Config > Behavior > QoS > Custom Policy**.

Note

The QoS policies configured on Ruijie Cloud and the web interface are displayed in the **Normal Policy** list. The QoS policies for authentication accounts configured on Ruijie Cloud cannot be edited or deleted on the web interface. You can only enable or disable these policies and change the priority of them.

(1) (Optional) Switch the application library

The application lists vary in different regions. The Chinese and International versions of the application library are provided. Please select the version based on the regions.

Click to select **Application Library Version** and click **OK**. The version is switched after a few minutes.



Caution

- It takes about one minute to switch the application library version. Please wait.
- If you switch the application library, the template of the application priority will be reset (See Section [8.6.4 Application Priority](#) for details.), and the old application control policy may be inactive (See Section [8.4 App Control](#) for details.). Please proceed with caution.

(2) Set **Policy Type** to **VPN Policy** and click **Add** to create a custom VPN QoS policy.

A maximum of 10 VPN policies can be configured.

Policy Type Normal Policy **VPN Policy**

Policy List ⓘ + Add Delete Selected

| <input type="checkbox"/> | Policy Name ⓘ | User Group | Time | IP/DSCP Priority | Application List ⓘ | Uplink Bandwidth ⓘ |
|--------------------------|---------------|----------------------|--------------|------------------|--------------------|---|
| <input type="checkbox"/> | 11 | Authentication Group | All Time | -- | All Applications | Max-Limit 110Mbps Max-Limit per User 100Mbps |

Up to 10 entries can be added. The Ruijie Cloud policy cannot be edited. 1 entries are already added.

(3) Configure items related to a VPN policy.

Add
×

* Policy Name

Type User Group Custom

* User Group

Effective User Internal IP/User External IP/External User

Application All Applications App Group Custom

Bandwidth Limit Limit No Limit

Uplink Bandwidth Mbps Mbps per User

Downlink Bandwidth Mbps Mbps per User

* Interface

Enabled

----- Advanced Settings -----

IP/DSCP Priority

Time

Table 8-10 Configuration of a Custom VPN Policy

| Parameter | Description |
|-------------|--|
| Policy Name | A policy name uniquely identifies a custom QoS policy. It cannot be modified. |
| Type | The type of a QoS policy can be set to the following: <ul style="list-style-type: none"> ● User Group: Indicates that the policy is applied to users in a specified user group. You need to select a user group to be managed. ● Custom: Indicates that the policy is applied to users in a specified IP address segment. You need to manually enter the IP address range to be managed. |

| Parameter | Description |
|-------------------|---|
| User Group | <p>Select a user to be managed by the policy from the user group list. For details about how to set the user group list, see Section 8.2 User Management.</p> <p>If you select all members of a user group, the policy takes effect on the entire user group (it also takes effect on members added to the user group later).</p> <p>This parameter is required when Type is set to User Group.</p> |
| IP/IP Range | <p>Enter an IP address or IP range manually.</p> <p>This parameter is required when Type is set to Client.</p> |
| Effective User | <p>Specify the type of effective users. It can be set to the following:</p> <ul style="list-style-type: none"> ● Internal IP/User: For a gateway, IP addresses of clients connected to the gateway are internal IP addresses. ● External IP/External User: For a gateway, non-gateway internal IP addresses are external IP addresses. <p>The configuration suggestions are as follows:</p> <ul style="list-style-type: none"> ● When clients are configured to control VPN traffic, select Internal IP/ User to control the traffic of internal network users. When the VPN server is configured to control the VPN traffic, select External IP/External User to control the traffic of external network users. ● For the VPN of the NAT model, the external IP address of the server must be in the IP address segment of the VPN address pool. ● For the VPN in router mode, the IP address segment must be set to IP addresses of restricted users. For the VPN in router mode, to configure QoS on internal IP addresses of clients, set internal IP addresses to the IP addresses of the QoS objects. <p>Note: The external IP address configured by the Open VPN server is the IP address of the address pool. The internal IP address configured by the client is the actual IP address of the client.</p> |
| Application | <p>When Bandwidth Type is set to Shared, the QoS policy can be configured to take effect only on specified applications.</p> <ul style="list-style-type: none"> ● All Applications: Indicates that the QoS policy takes effect on all applications in the current application library. ● Custom: Indicates that the QoS policy takes effect only on specified applications in the application list. ● Application Group: Indicates that the QoS policy takes effect only on specified application groups. The traffic of applications involved in the application group is subject to the policy. For details about how to set the application group list, see Section 8.4.4 Custom Application Group. |
| Application List | <p>When Application is set to Custom, it specifies the applications, on which the policy takes effect. The traffic of the selected applications is subject to the policy.</p> |
| Application Group | <p>When Application is set to Application Group, it specifies the application group, on which the policy takes effect. The traffic of the selected application group is subject to the policy.</p> |
| Bandwidth Limit | <p>Configure whether to limit the bandwidth.</p> <ul style="list-style-type: none"> ● Limit: You can set uplink and downlink bandwidth limits as needed. ● No Limit: When the bandwidth is sufficient, the maximum bandwidth is not limited. When the bandwidth is insufficient, the minimum bandwidth is not guaranteed. |

| Parameter | Description |
|---------------------------|---|
| Uplink/Downlink Bandwidth | Configure the maximum uplink/downlink bandwidth shared by VPN users matching the policy in Mbps. When the bandwidth is shared by multiple users, you can also set the maximum uplink/downlink bandwidth per user in Mbps. The uplink/downlink bandwidth is not limited by default. Note: The parameter is valid when Bandwidth Limit is set to Limit . |
| Interface | Specify the VPN port, on which the policy takes effect. When it is set to All VPN Ports , the policy will be applied to all VPN ports. |
| Enabled | Set whether to enable the QoS policy. If it is disabled, the policy does not take effect. |
| IP/DSCP Priority | Specifies the priority of packets to differentiate various types of traffic and allocate different levels of service quality. QoS policies are applied based on the IP/DSCP field in the packet. |
| Time | Specifies the time period during which the rule takes effect. You can choose from existing time rules or create custom ones. |

(4) Click **OK**.

5. View Custom Policies

The current custom policies are displayed in the **Policy List** section. You can modify and delete a custom policy. To delete multiple custom policies in a batch, select the desired policies and click **Delete Selected**.

- Normal policy list

Policy Type Normal Policy VPN Policy

Policy List ? + Add Delete Selected

| <input type="checkbox"/> | Policy Name ? | User Group | Bandwidth Type ? | Channel Priority | Application List ? | Uplink Bandwidth ? |
|--------------------------|----------------------------|------------|-------------------------------|------------------|---------------------------------|--------------------------------------|
| <input type="checkbox"/> | test | User Group | Shared | 4 | All Applications | Limit-at 2Mbps Max-Limit 1000Mbps |

Up to 30 entries can be added. 1 entries are already added.

- VPN policy list

Policy Type Normal Policy VPN Policy

Policy List ? + Add Delete Selected

| <input type="checkbox"/> | Policy Name ? | User Group | Application List ? | Uplink Bandwidth ? | Downlink Bandwidth ? |
|--------------------------|----------------------------|------------|---------------------------------|--|--|
| <input type="checkbox"/> | L2TP | VPN Group | All Applications | Max-Limit 1000Mbps Max-Limit per User 100Mbps | Max-Limit 1000Mbps Max-Limit per User 100Mbps |
| <input type="checkbox"/> | IPSec | VPN Group | All Applications | Max-Limit 1000Mbps Max-Limit per User 100Mbps | Max-Limit 1000Mbps Max-Limit per User 100Mbps |

Up to 10 entries can be added. The Ruijie Cloud policy cannot be edited. 2 entries are already added.

Table 8-11 Policy list information

| Parameter | Description |
|------------------|---|
| Application List | The Application List contains the applications to which the policy is valid. If the Application Library matches with the Application that is set to Custom and supported by the policy,  is displayed in the Application List . If not,  is displayed. |
| Status | Indicate whether the current policy is enabled. You can click to edit the status. If the Application Library does not match with the Application that is set to Custom and supported by the policy, you cannot edit the Status directly. Please click Edit in the action bar to edit the policy or switch the application library. |
| Effective State | Indicate whether the policy is effective in the current system. If Inactive is displayed, check whether the policy is enabled, whether the policy-enabled port exists, and whether the Application Library matches with the Application to which the policy is valid. |
| Match Order | All the created custom policies are displayed in the policy list, with the latest policy listed on the top. The device matches the policies according to their sorting in the list. You can manually adjust the policy matching sequence by clicking  or  in the list. |
| Action | You can modify and delete the custom policy. |

8.6.4 Application Priority

1. Overview

After smart QoS is enabled, you can set the application priority to provide guaranteed bandwidth to applications with high priority and suppress the bandwidth for applications with low priority. You can predefine a list of applications whose bandwidth needs to be guaranteed preferentially and a list of applications whose bandwidth needs to be suppressed based on actual needs.

 **Caution**

If one application exists in both the custom policy list and the application priority list, the custom policy prevails.

2. Getting Started

Before you configure application priority, enable smart QoS first. For details, see Section [8.6.2 Intelligence QoS](#).

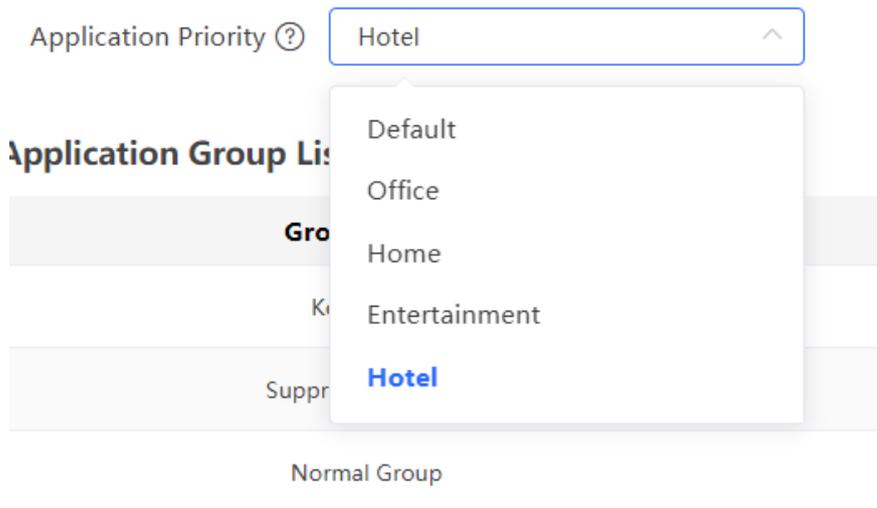
3. Configuration Steps

Choose **One-Device > Gateway > Config > Behavior > QoS > Application Priority**.

(1) Create an application priority template.

Select a template from the **Application Priority** drop-down list box.

Five application priority templates are predefined to meet the needs in different scenarios. You can switch among the templates based on actual needs.



The application priority templates are as follows:

- **Default:** This template is used during device initialization. The traffic bandwidth is not guaranteed or suppressed for any application.
 - **Office:** This template is designed for the office scenario, where the application traffic from the office network is guaranteed preferentially.
 - **Home:** This template is designed for the home scenario, where the application traffic from the home network is guaranteed preferentially.
 - **Entertainment:** This template is designed for the entertainment scenario, where the application traffic from the entertainment network is guaranteed preferentially.
 - **Hotel:** This template is designed for the hotel scenario, where the application traffic from the hotel network is guaranteed preferentially.
- (2) Create an application group list.

Each default template has three application groups: key group, block group, and normal group. The application priority of the three groups decreases in the following order: key group, normal group, and block group.

- **Key Group:** The traffic from applications in the application list for this group is guaranteed preferentially.
- **Block Group:** The traffic from applications in the application list for this group is suppressed to preferentially guarantee the traffic from applications with higher priority.
- **Normal Group:** All the applications beyond the key group and block group are in this group. The traffic from applications in this group are guaranteed after that from the key group.

After you select a template, three application groups **Key Group**, **Block Group**, and **Normal Group** and the application list for each group in the current template are displayed. You can click **More** to view the details of each application list.

You can click **Edit** in the **Action** column next to the key group and block group to edit the application list for the groups, allowing the traffic from these applications to be guaranteed or suppressed.

Application Group List

| Group Name | Application List | Action |
|-------------------|----------------------------------|----------------------|
| Key Group | Video... More | Edit |
| Suppression Group | Databank... More | Edit |
| Normal Group | Other | Edit |

Application List(2)

Databank P2PSoftware

Edit ×

Group Name: Suppression Group

Application List: Databank × P2PSoftware ×

- ▶ Communication
- ▶ Shopping
- ▶ Play
- ▶ Databank
- ▶ P2PSoftware
- ▶ Payment
- ▶ NetworkService

Cancel OK

⚠ Caution

The application list will be reset after you switch the application priority template.

8.7 Access Control

8.7.1 Overview

The access control function matches data packets passing through the device based on specific rules and permits or drops data packets in the specified time range. This function controls whether to permit LAN user access to the Internet and whether to block a specific data flow. The device matches packets based on the MAC address or IP address.

8.7.2 Configuration Steps

Choose **One-Device > Gateway > Config > Behavior > Access Control**.

The access control rule list displays the created access control rules. Click **Add** to add an access control rule.

Configure ACL based on IP addresses. **Default reverse flow mismatches** .
 The L2TP/PPTP/OpenVPN VPN only supports the IP-based ACL. The dest networks must be configured in the internal network.
 Example: **Configure a deny ACL entry containing source IP address 192.168.1.0/24 and destination IP address 192.168.2.0/24.** Device configured with IP address 192.168.1.x will fail to access device 192.168.2.x. **But device 192.168.2.x will be allowed to access device 192.168.1.x.**
 Tips: **Configure one more deny ACL entry containing source IP address 192.168.2.0/24 and destination IP address 192.168.1.0/24.** The two devices will be mutually unreachable.

ACL List + Add Delete Selected

| <input type="checkbox"/> | Username <small>?</small> | Rule <small>?</small> | Control Type <small>?</small> | Effective Time <small>?</small> | Src Networks | Dest Networks | Status | Effective Sta... <small>?</small> |
|--------------------------|---------------------------|-----------------------|-------------------------------|---------------------------------|--------------|---------------|--------|-----------------------------------|
| No Data | | | | | | | | |

Up to 50 entries can be added. Total 0 1 10/page

Table 8-12 Access control rule information

| Parameter | Description |
|----------------|---|
| Username | Identify the purpose of the rule. |
| Rule | Display a summary of the control information. MAC-based: Display the MAC address matching the rule. IP-based: Display the connection type, source IP address, destination IP address, and protocol type of packets matching the rule. |
| Control Type | Indicate how packets that match the rule are processed. <ul style="list-style-type: none"> Allow: Permit the packets that match the rule. Block: Discard the packets that match the rule. |
| Effective Time | Indicate the time period during which the rule takes effect. |
| Src Networks | Indicate the source interface that matches the rule. If the rule is based on the MAC address, then this field is set to "All Intranets" by default. If the rule is based on IP addresses, then this field can be set to "All Networks", "All Extranets", "All Intranets", or a specific network. |
| Dest Networks | Indicate the destination interface that matches the rule. If the rule is based on the MAC address, then this field is set to "All Extranets" by default. If the rule is based on IP addresses, then this field can be set to "All Networks", "All Extranets", "All Intranets", or a specific network. |
| Status | Indicate whether the rule is enabled. You can click to switch the status. When this toggle switch is off, the rule will not take effect. |

| | |
|-----------------|---|
| Effective State | Indicate whether the rule takes effect. If Inactive is displayed, the current system time may not in the effective time range. Move the cursor to  to view the detailed cause. |
| Match Order | All the created ACL rules are displayed in the ACL list, with the latest rule listed on the top. The device matches the rules according to their sorting in the list. You can manually adjust the rule matching sequence by clicking  or  in the list. |
| Action | You can modify and delete a rule. |

1. Configuring a MAC Address-based ACL Rule

MAC address-based ACL rules enable the device to match data packets based on the source MAC address, and are generally used to control Internet access from online users or specific clients.

Set **Based on** to **MAC**, enter the MAC address of the client, select a rule type, set the effective time range, and click **OK**.

 **Note**

MAC address-based ACL rules are valid on WAN ports by default.

Add Rule ×

Status

Name

Based on **MAC Address** IP Address

* MAC Address

Control Type  

Effective Time  

Table 8-13 MAC address-based ACL configuration

| Parameter | Description |
|----------------|--|
| Status | Indicate whether the rule is enabled. You can click to switch the status. When this toggle switch is off, the rule will not take effect. |
| Name | Identify the rule. This field can be customized by the user. |
| MAC Address | Enter the client MAC address to be controlled by the ACL rule. After you click the input field, the current client information is displayed. You can click to automatically enter the corresponding MAC address. |
| Control Type | Specify the method for processing data packets matching the conditions. <ul style="list-style-type: none"> ● Allow: Permit the data packets matching the conditions. ● Block: Drop the data packets matching the conditions. |
| Effective Time | You can select a time range defined in 8.3 Time Management from the drop-down list box, or select Custom and manually enter the specific time range. |

2. Configuring an IP Address-based ACL Rule

IP address-based ACL rules enable the device to match data flows according to the source IP address, destination IP address, and protocol number.

Set **Based on** to **IP**, enter the source IP address and port and destination IP address and port of the data flow, select the protocol type, rule type, effective time range, and effective port, and click **OK**.

Caution

- IP address-based ACL rules are effective in only one direction. For example, in a block rule, the source IP address segment is 192.168.1.0/24 and the destination IP address segment is 192.168.2.0/24. According to this rule, the device with the IP address 192.168.1.x cannot access the device with the IP address 192.168.2.x, but the device with the IP address 192.168.2.x can access the device with the IP address 192.168.1.x. To block bidirectional access in this network segment, you need to configure another block rule with the source IP address segment 192.168.2.0/24 and destination IP address segment 192.168.1.0/24.
- L2TP/PPTP VPN supports only IP address-based access control and the effective ports must be in the LAN.

Add Rule
×

Status

Name

Based on MAC Address IP Address

Internet IPv4 IPv6

Enable User Groups

Src IP Address

Dest IP Address

Protocol Type

Control Type

Effective Time

Src Networks

Dest Networks

----- [Advanced Settings](#) -----

Table 8-14 IP address-based ACL configuration

| Parameter | Description |
|-----------|--|
| Status | Indicate whether the rule is enabled. You can click to switch the status. When this toggle switch is off, the rule will not take effect. |
| Name | Identify the purpose of the rule, which can be customized by the user. |

| Parameter | Description |
|-----------------|---|
| Internet | <p>The source IP address and port of the packet. If this parameter is left empty, it means all IP addresses and ports.</p> <p>If the Internet is set to IPv4, then the format of the IP address is IPv4. Example: 192.168.1.1/24.</p> <p>If the Internet is set to IPv6, then the format of the IP address is IPv6. Example: 2000::1.</p> |
| Src IP Address | Enter the source IP address and port number for data packet matching. If this parameter is not specified, the device matches all the IP addresses and port numbers. The source IP address can be a single IP address (such as 192.168.1.1) or an IP address range (such as 192.168.1.1/24). |
| Dest IP Address | Enter the destination IP address and port number for data packet matching. If this parameter is not specified, the device matches all the IP addresses and port numbers. The destination IP address can be a single IP address (such as 192.168.1.1) or an IP address range (such as 192.168.1.1/24). |
| Protocol Type | Specify the protocol type for data packet matching. The options are TCP, UDP, and ICMP. |
| Control Type | <p>Specify the method for processing data packets matching the conditions.</p> <p>Allow: Permit the data packets matching the conditions.</p> <p>Block: Drop the data packets matching the conditions. This rule is valid only in one direction, and does not block the reverse flow.</p> |
| Effective Time | You can select a time range defined in Section 8.3 Time Management from the drop-down list box, or select Custom and manually enter the specific time range. |
| Src Networks | Indicate the source interface that matches the rule. If the rule is based on the MAC address, then this field is set to "All Intranets" by default. If the rule is based on IP addresses, then this field can be set to "All Networks", "All Extranets", "All Intranets", or a specific network. |
| Dest Networks | Indicate the destination interface that matches the rule. If the rule is based on the MAC address, then this field is set to "All Extranets" by default. If the rule is based on IP addresses, then this field can be set to "All Networks", "All Extranets", "All Intranets", or a specific network. |

To limit the session state of packets matching the rule, you can click **Advanced Settings** and select one or more session states as required. These session states include New, Established, Related, and Invalid. Then, click **OK**.

Note

If no session state is selected, the rule matches all sessions by default.

----- Advanced Settings -----

* Session State All

New Established Related

Invalid

8.8 Upgrading the Application Library

8.8.1 Overview

The app control function relies on the accuracy of the application library, and the application library is updated with the app version. You can upgrade the application library to the latest version on the **Application Library Update** page.

8.8.2 Local Upgrade

Choose **One-Device > Gateway > Config > Behavior > Application Library Update > Local Application Library Update**.

Caution

- Upgrading the application library version takes about one minute to take effect. Do not cut off power during the upgrade. You can view the current application library version on the page.
- Perform subsequent operations based on the memory information displayed on the page. If the memory is insufficient, you are advised to restart the device and then upgrade the application library.
- After the application library is upgraded, the original app control policy may become invalid. Therefore, exercise caution when performing this operation.

- (1) Click **Browse**. Select an application library upgrade file.
- (2) Click **Upload** to upload the upgrade file.
- (3) Click **OK**. Wait for the system to automatically complete the upgrade.

Current Version 2023.12.01.23.12.01(V2.0)

File Path

8.8.3 Online Upgrade

Choose **One-Device > Gateway > Config > Behavior > Application Library Management > Application Library Management.**

Enable **Auto Update Version.** When the system identifies the latest version, the application library is automatically upgraded.

Auto Update Version

Application Recognition 2023.12.01.23.12.01(V2.0) New version is not found. Please check the network connection.
Library

8.9 Network Behavior Settings

8.9.1 Internet Alert

Choose **One-Device > Gateway > Config > Behavior > Network Settings > Internet Alert.**

Click **Add** to create a network access notification policy and notify users of their online behaviors or application usage.

i 1.VPN connections are not supported. 2.The Alerts and Notifications feature is not supported on PPPoE clients.

| <input type="checkbox"/> | User Group | Notification Type | Status | Action |
|--------------------------|---|---|--|-------------|
| <input type="checkbox"/> | Authentication Group | Network Activity Notification; App Use Notification: Game | Enable ⊙ | Edit Delete |
| <input type="checkbox"/> | VPN Group | App Use Notification: Video | Enable ⊙ | Edit Delete |
| <input type="checkbox"/> | User Group/3dbbuser Unknown | Network Activity Notification; | Enable ⊙ | Edit Delete |
| <input type="checkbox"/> | User Group/c3f4user Unknown | Network Activity Notification; | Enable ⊙ | Edit Delete |

Up to 20 entries can be added.

Add
×

* User Group (?)

App Alert (?) Select All
 Game Video Payment

Data Usage Alert

Status

Table 8-15 Internet Access Notification Configuration Parameters

| Parameter | Description |
|------------------|---|
| User group | Select a user group managed by the policy from the user group list. For details about how to set the user group list, see Section 8.2 User Management . If you select all members of a user group, the policy takes effect on the entire user group (and members added to the user group later). |
| App Alert | To enable the App Alert function, enable Traffic Audit first. For details, see Section 3.4 Supporting Traffic Monitoring . |
| App category | When App Alert is enabled, you need to select the application category for the policy. When a user uses an application in the corresponding application category, a notification will be received. |
| Data Usage Alert | After the Data Usage Alert function is enabled, you will receive a notification when a specified user accesses the Internet. |
| Status | Enable/disable the Data Usage Alert function. If it is disabled, the policy does not take effect. |

8.9.2 Online Time Control

Note

The **Online Time Control** feature can only be configured on the app, and the web interface only displays the synchronization status.

Choose **One-Device > Gateway > Config > Behavior > Network Settings > Online Time Control**.

The **Online Time Control** list displays the type, schedule, accounting status, status, and operation information.

Online Time Control

| Type | Schedule | Accounting Status | Status | Action |
|---------|----------|-------------------|--------|--------|
| No Data | | | | |

8.9.3 Internet Block Policy

 **Note**

The Internet block policy can be configured only on the app, and the web interface only displays the synchronization status.

Choose **One-Device > Gateway > Config > Behavior > Network Settings > Internet Block Policy**.

The **Policy List** displays the user group, start time of network disconnection, end time of network disconnection, start time of temporary access, and end time of temporary access.

Policy List

| User Group | Start Time | End Time  | Temporary Access Start Time | Temporary Access End Time  |
|------------|------------|--|-----------------------------|---|
| No Data | | | | |

9 Online Client Management

9.1 Overview

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.

The screenshot shows a web interface for managing online clients. At the top, there are filters for 'All (5)', 'Wired (2)', 'Wireless (3)', and 'User not connected (0)'. There are also buttons for 'Select', 'Block', and 'Bind IP', and a search bar. A notification states: 'The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes.' Below this is a table with the following data:

| Username | SSID and Band | Connected To | IP/MAC | Rate | Action |
|---------------------------------|---------------------|-------------------|---------------------------|-----------------------------|-----------------------------------|
| Click to edit | 5G @@@@zzzzzzzzzz | AP W.....9 | 192.168.110.6 1.....a | ↑ 0.00bps ↓ 0.00bps | Access Control Associate Block |
| M2102J2SC | 5G @@@@zzzzzzzzzz | AP V.....9 | 192.168.110.7 E..... | ↑ 571.00bps ↓ 1.35Kbps | Access Control Associate Block |
| DESKTOP-DTUM8V | Wired LAN3/WAN1 | eg205g M.....5 | 192.168.110.9 7.....5 | ↑ 0.00bps ↓ 475.00bps | Access Control |
| DESKTOP-IPV6G6R | Wired LAN1/WAN3 | eg205g V.....5 | 192.168.110.14 c.....4 | ↑ 295.54Kbps ↓ 79.64Kbps | Access Control |
| zhuyihan | 2.4G @@@@zzzzzzzzzz | AP V.....9 | 192.168.110.16 0C..... | ↑ 132.00bps ↓ 43.00bps | Access Control Associate Block |

At the bottom right of the table, it shows 'Total 5' and a pagination control for '1' out of '10/page'.

- 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.

Table 9-1 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. |
| Connected To | Indicates wired or wireless connection, the associated device and SN. |
| IP/MAC | Indicates the IP address and MAC address of the client. |
| Rate | Indicates the uplink and downlink rates of the client. |
| Action | You can click the corresponding button to perform access control, association, and block operations on online clients. |
| Signal Quality | The Wi-Fi signal strength of the client and the associated channel. |

| Parameter | Description |
|------------------|---|
| | Note: This information is displayed only in the wireless online client list. |
| Negotiation Rate | Negotiation rate between the client and the AP. Note: This information is displayed only in the wireless online client list. |
| Online Duration | Online duration of the client. Note: This information is displayed only in the wireless online client list. |
| Limit Speed | Indicates the wireless rate limiting of the current client. For details, see Section 9.6 Configuring Client Rate Limiting . Note: This information is displayed only in the wireless online client list. |

1. Wired Clients

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

| Username | SSID and Band | Connected To | IP/MAC | Rate | Action |
|-------------------------------|---------------|--------------|---------------|----------------------------|----------------|
| Click to edit | Wired G1/18 | NBS6000 | 192.168.120.1 | ↑ 0.00bps ↓ 0.00bps | Access Control |
| PC-4277ac | Wired G1/21 | NBS60001 | 192.168.110.3 | ↑ 40.18Kbps ↓ 21.28Kbps | Access Control |

2. Wireless Clients

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

| Username | SSID and Band | Signal Quality | Connected To | IP/MAC | Rate | Negotiation Rate | Online Duration | LimitSpeed | Action |
|---------------------------|------------------------------|----------------|--------------|---------------|--------------------------|------------------|-----------------------|------------|-----------------------------------|
| * | 5G @@@@zzzzzzzzzz Channel149 | -42db | AP | 192.168.110.6 | ↑ 0.00bps ↓ 0.00bps | 866M | 44 minutes 47 seconds | No Limit | Access Control Associate Block |
| M2102J25C | 5G @@@@zzzzzzzzzz Channel149 | -33db | AP | 192.168.110.7 | ↑ 1.20Kbps ↓ 3.90Kbps | 585M | 8 seconds | No Limit | Access Control Associate Block |

3. 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**.

| 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 |

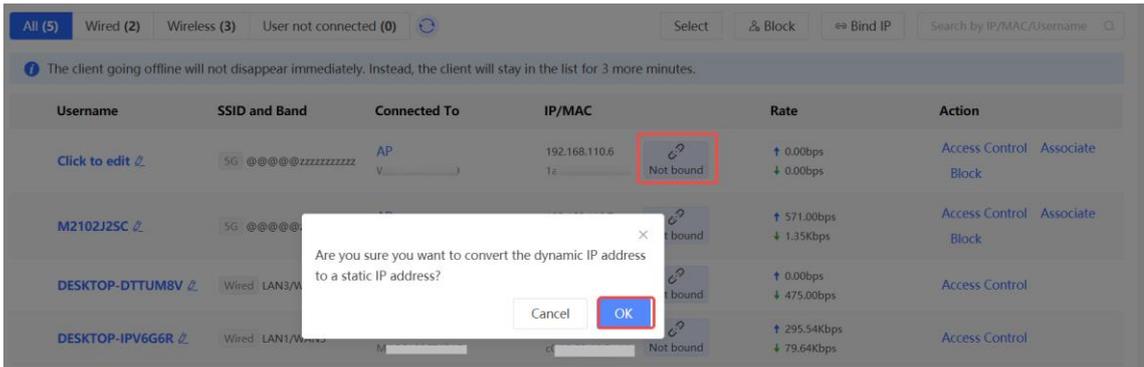
9.2 Configuring Client IP Binding

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.

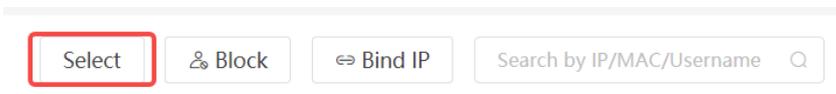
- Single client IP address binding

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.

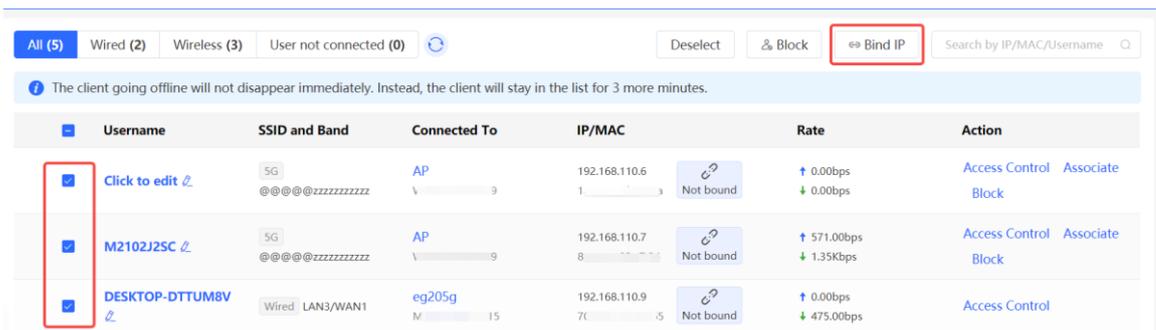


- Batch IP binding

Click **Select**.

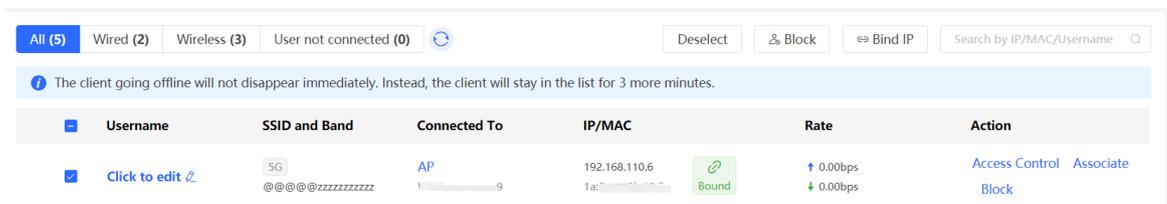


Select the clients to be bound, click **Bind IP**, and click **OK** in the pop-up box to bind the selected clients to a static IP address.



- Unbind IP address

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



9.3 Configuring Client Access Control

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. For details, see [Configuring a MAC Address-based ACL Rule](#).

Edit Rule ×

Status

Name

Based on MAC Address IP Address

* MAC Address

Control Type

Effective Time

9.4 Configuring Client Association

Choose **Network-Wide > Clients**.

Note

The Client Association feature applies only to wireless clients.

Select a client in the list and click **Associate** in the **Action** column. You will be redirected to the **Edit Association** page. The **Client** field is populated with the MAC address of the selected client and cannot be modified. The **Associated Device** field is populated with the associated device of the client by default. Set the SSID and the Forced Association feature as required, and click **OK**. For details, see Section [5.13 Client Association](#).

All (4) | Wired (1) | Wireless (3) | 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 | Connected To | IP/MAC | Rate | Action |
|-----------|---------------------|--------------|-----------------------|--------------------------|---|
| * | 5G @@@@ @zzzzzzzzzz | AP W | 192.168.110.6 1: a | ↑ 0.00bps ↓ 0.00bps | Access Control Associate Block |
| M2102J25C | 5G @@@@ @zzzzzzzzzz | AP V | 192.168.110.7 8: 4 | ↑ 2.95Kbps ↓ 5.79Kbps | Access Control Associate Block |

Edit Association
×

* Client

* Associated Device ?

Advanced Settings

SSID

Forced Association

Enabling this feature will forcefully associate the client with a specific AP. However, since the client cannot initiate automatic association, this may cause disconnection and unsuccessful association attempts.

9.5 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.

i **Note**

Client Block is available only for wireless clients.

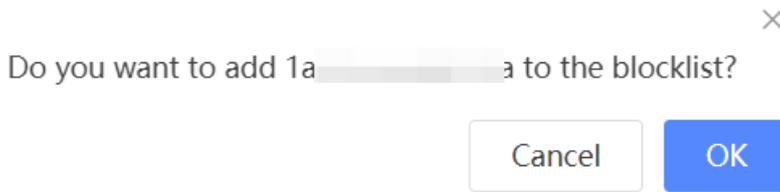
- Block a single client

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 (4) | Wired (1) | Wireless (3) | User not connected (0) ↻
Select
⚙️ Block
↔️ Bind IP
Search by IP/MAC/Username

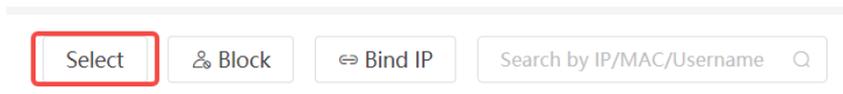
ⓘ The client going offline will not disappear immediately. Instead, the client will stay in the list for 3 more minutes.

| Username | SSID and Band | Connected To | IP/MAC | Rate | Action |
|--------------------------|-------------------|--|-------------------------------|--|---|
| * 🔗 | 5G @@@@zzzzzzzzzz | AP V <input type="text" value="9"/> | 192.168.110.6 1c- - - - -a | ↑ 0.00bps ↓ 0.00bps | Access Control Associate Block |
| M2102J2SC 🔗 | 5G @@@@zzzzzzzzzz | AP V <input type="text" value="j"/> | 192.168.110.7 8- - - - -4 | ↑ 2.95Kbps ↓ 5.79Kbps | Access Control Associate Block |

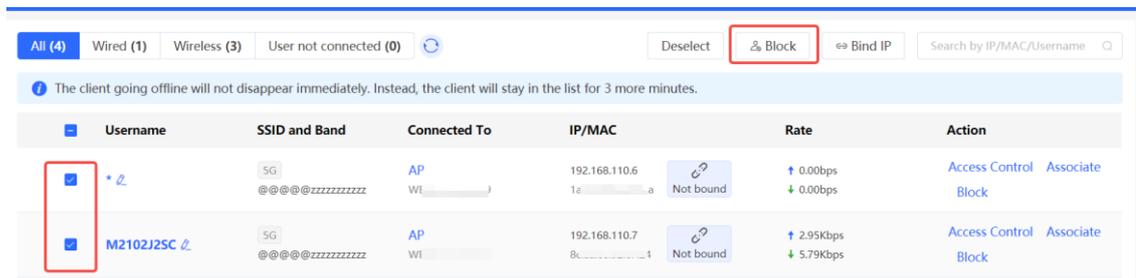


- Batch block clients

Click **Select**.



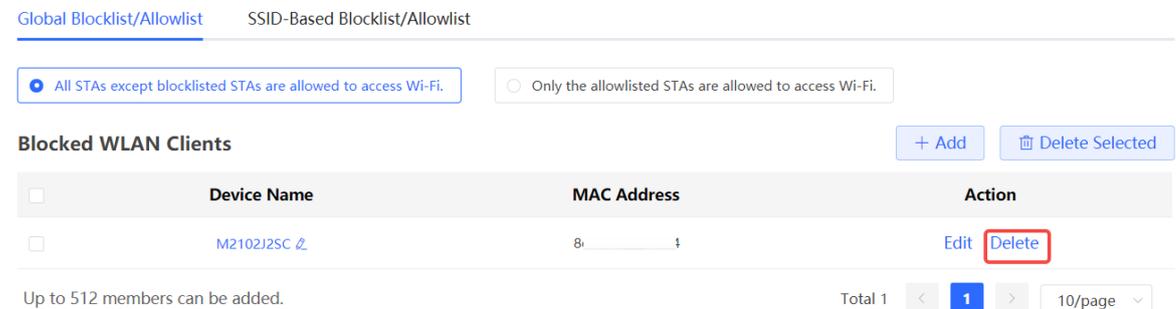
Select the target clients, click **Block**, and click **OK** in the pop-up box to block the selected clients.



- 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**.



9.6 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**.

| Username | SSID and Band | Signal Quality | Connected To | IP/MAC | Rate | Negotiation Rate | Online Duration | LimitSpeed | Action |
|--------------------|---------------|----------------------|--------------|---------------|--------------------------|------------------|-----------------------|------------|-----------------------------------|
| + [client] | 5G [SSID] | -42db Channel:149 | AP | 192.168.110.6 | ↑ 0.00bps ↓ 0.00bps | 866M | 44 minutes 47 seconds | No Limit | Access Control Associate Block |
| M2102J25C [client] | 5G [SSID] | -33db Channel:149 | AP | 192.168.110.7 | ↑ 1.20Kbps ↓ 5.90Kbps | 585M | 8 seconds | No Limit | Access Control Associate Block |

LimitSpeed

Uplink Rate Kbps
Limit Current: Kbps. Range: 1-1700000 Kbps

Downlink Rate Kbps
Limit Current: Kbps. Range: 1-1700000 Kbps

- Cancel rate limits

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

| Username | SSID and Band | Signal Quality | Connected To | IP/MAC | Rate | Negotiation Rate | Online Duration | LimitSpeed | Action |
|--------------------|---------------|----------------------|--------------|---------------|--------------------------|------------------|-----------------------|------------------------|-----------------------------------|
| + [client] | 5G [SSID] | -42db Channel:149 | AP | 192.168.110.6 | ↑ 0.00bps ↓ 0.00bps | 866M | 44 minutes 47 seconds | ↑ 100Mbps ↓ 100Mbps | Access Control Associate Block |
| M2102J25C [client] | 5G [SSID] | -33db Channel:149 | AP | 192.168.110.7 | ↑ 1.20Kbps ↓ 5.90Kbps | 585M | 8 seconds | No Limit | Access Control Associate Block |

LimitSpeed

Uplink Rate Mbps
Limit Current: **102400** Kbps. Range: 1-1700000 Kbps

Downlink Rate Mbps
Limit Current: **102400** Kbps. Range: 1-1700000 Kbps

10 VPN

10.1 Configuring IPsec VPN

10.1.1 Overview

1. IPsec Overview

IP Security (IPsec) is a Layer 3 tunnel encryption protocol defined by the IETF. IPsec is used to provide end-to-end encryption and verification services in the network to provide high quality and interoperability for data transmission over the network and ensure transmission security by using cryptographic algorithms. The communicating parties obtain the following security services at the IP layer through encryption and data source authentication:

- Confidentiality: The IPsec sender encrypts packets before transmitting the packets over the network.
- Data integrity: The IPsec receiver authenticates packets received from the sender to ensure that data is not tampered with during the transmission.
- Data authentication: The IPsec receiver authenticates whether the sender of IPsec packets is valid.
- Anti-replay: The IPsec receiver detects and denies expired or repeated packets.

The IPsec protocol is widely used for communication between the HQ and branches of an organization. Currently, the device can be deployed as the IPsec server or client. A secure tunnel is established between the HQ and each branch based on the IPsec protocol to ensure the confidentiality of data transmission and improve network security.

2. IKE Overview

IPsec provides secure communication between two endpoints, which are called IPsec peers. Security Association (SA) is the establishment of shared security attributes between the peers to support secure communication. An SA may include attributes such as: security protocol used by the peers, characteristics of data flows to be protected, encapsulation mode of data transmitted between the peers, encryption and authentication algorithms, keys for secure data conversion and transmission, and the SA lifetime. When you configure IPsec, you can use the Internet Key Exchange (IKE) protocol to establish an SA. IKE provides automatically negotiated keys for establishing and maintaining SAs, simplifying IPsec usage and management.

3. IPsec Security Policy

IPsec security policies define security proposals (equivalent to SA) for data flows. You can configure matching security policies on both parties engaged in the communication to establish IPsec tunnels between the IPsec client and the IPsec server, protecting the communication data. An IPsec security policy consists of two parts: basic settings and advanced settings. Advanced settings are optional and include the specific IKE policy and connection policy. You can keep the default settings unless otherwise specified. For details, see the configuration steps below.

10.1.2 Configuring the IPsec Server

Choose **One-Device > Gateway > Config > VPN > IPsec > IPsec Security Policy**.

1. Basic Settings

Click **Add**. In the dialog box that appears, set **Policy Type** to **Server**, enter the policy name and local subnet range, set the pre-shared key, and click **OK**.

Note: Example: IP address/number of subnet mask bits.
Tips: If it is set to 192.168.110.x/24, the address range is from 192.168.110.1 to 192.168.110.254.
 Up to **3** entries with the policy type of client can be configured.
 Up to **1** entry with the policy type of server can be configured.
 The server and client cannot be configured at the same time.

Policy List + Add

| Policy Type ? | Policy Name ? | Peer Gateway ? | Key Exchange Version | Local Subnet ? | Peer Subnet ? | Status | Action |
|---------------|---------------|----------------|----------------------|----------------|-----------------|----------|-------------|
| Client | test | 10.52.50.239 | IKEv1 | 192.168.2.0/24 | 192.168.68.0/24 | Enable ☺ | Edit Delete |

Total 1 < 1 > 10/page

Add ×

i If clients want to access from different WAN ports, please set Local ID Type to Name. Otherwise, all clients will access from the same one WAN port.

Policy Type ? Client **Server**

Internet ? IPv4 IPv6

* Policy Name ?

Interface ?

Key Exchange Version IKEv1 IKEv2

* Subnets

+ Local Subnets

* Pre-shared Key ?

Status

- 1. Set IKE Policy -----
- 2. Connection Policy -----

Cancel OK

Table 10-1 IPsec server basic settings

| Parameter | Description |
|----------------------|--|
| Policy Name | Specify the name of the IPsec security policy. The name must be a string of 1 to 28 characters. |
| Internet | Format of the IP address. Both IPv4 and IPv6 address formats are supported. |
| Interface | Select a local WAN port from the drop-down list box. The Peer Gateway parameter set for the communication peer (IPsec client) must use the IP address of the WAN port specified here. In the multi-line scenario, you are advised to set this parameter to Auto . |
| Key Exchange Version | Select the IKE version for SA negotiation. There are two options available: <ul style="list-style-type: none"> ● IKEv1: The negotiation of SA in IKEv1 primarily consists of two phases. <ul style="list-style-type: none"> ○ Phase 1: The purpose is to establish an IKE SA using one of two negotiation modes: Main Mode and Aggressive Mode. Main Mode requires six ISAKMP (Internet Security Association and Key Management Protocol) messages to complete the negotiation, while Aggressive Mode only requires three ISAKMP messages. Aggressive Mode offers faster IKE SA establishment. However, it combines key exchange and identity authentication, which means it does not provide identity protection. ○ Phase 2: The purpose is to establish an IPsec SA for data transmission, utilizing a fast exchange mode that requires only three ISAKMP messages to complete the negotiation. ● IKEv2: In IKEv2, the negotiation process for SA is simplified. The establishment of one IKE SA and one pair of IPsec SAs can be accomplished using two exchanges with four messages. If there is a need to establish more than one pair of IPsec SAs, only one additional exchange is needed for each pair. This enables the negotiation to be completed with just two messages per pair. |
| Subnets | Specify the local subnet address range for the data flows to be protected, that is, the LAN port network segment of the server. The value is the combination of IP address and subnet mask. |
| Pre-shared Key | Specify the same pre-shared key as the credential for authentication between communicating parties. For higher security, different peers must be configured with different pre-shared keys. That is, a pair of interface bound to the IPsec server and peer gateway of the IPsec client must be configured with the same unique pre-shared key. |
| Status | Specify whether to enable the security policy. |

2. Advanced Settings (Phase 1)

- The key exchange version in the basic setting is IKEv1:

Click **1. Set IKE Policy** to expand the configuration items. Keep the default settings unless otherwise specified.

1. Set IKE Policy

Authentication-Encryption-DH Group

| | | |
|--------------|--|---|
| IKE Policy 1 | <input type="text" value="sha1-3des-dh1"/> | ▼ |
| IKE Policy 2 | <input type="text" value="sha1-des-dh1"/> | ▼ |
| IKE Policy 3 | <input type="text" value="sha1-3des-dh2"/> | ▼ |
| IKE Policy 4 | <input type="text" value="md5-des-dh1"/> | ▼ |
| IKE Policy 5 | <input type="text" value="md5-3des-dh2"/> | ▼ |

Negotiation Mode Main Mode Aggressive Mode

Local ID Type IP Name

Peer ID Type IP Name

* Lifetime

DPD Enable Disable

* DPD Interval

seconds

- The key exchange version in the basic setting is IKEv2:

Click **IKE Policy** to expand the configuration items. Keep the default settings unless otherwise specified.

----- IKE Policy -----

Authentication-Encryption-DH Group

IKE Policy 1 IKE Policy 2 IKE Policy 3 IKE Policy 4 IKE Policy 5 Local ID Type IP NamePeer ID Type IP Name* Lifetime DPD Enable Disable* DPD Interval

seconds

Table 10-2 IPsec server IKEv2 policy configuration

| Parameter | Description |
|--------------------|---|
| IKE Policy | <p>Select the hash algorithm, encryption algorithm, and Diffie-Hellman (DH) group ID used by the IKE protocol. An IKE policy is composed of the three parameters. You can set five sets of IKE policies. To ensure successful IKE negotiation, the two parties engaged in IKE negotiation must have at least one set of consistent IKE policy.</p> <ul style="list-style-type: none"> ● Hash algorithm: <ul style="list-style-type: none"> ○ sha1: SHA-1 algorithm ○ md5: MD5 algorithm ● Encryption algorithm: <ul style="list-style-type: none"> ○ des: DES algorithm using 56-bit keys ○ 3des: 3DES algorithm using 168-bit keys ○ aes-128: AES algorithm using 128-bit keys ○ aes-192: AES algorithm using 192-bit keys ○ aes-256: AES algorithm using 256-bit keys ● DH group ID: <ul style="list-style-type: none"> ○ dh1: 768-bit DH group ○ dh2: 1024-bit DH group ○ dh5: 1536-bit DH group |
| Negotiation Mode | <p>Select Main Mode or Aggressive Mode. The negotiation mode on the IPsec server and IPsec client must be the same.</p> <ul style="list-style-type: none"> ● Main Mode: Generally, this mode is applicable to communication between fixed public network IP addresses and point-to-point communication between devices. In this mode, the peer identity is authenticated to provide high security. ● Aggressive Mode: The public network IP addresses obtained by ADSL dial-up users are not fixed and an NAT device may exist. Therefore, the aggressive mode is used to implement NAT traversal. In this mode, you need to set the local and peer ID type to NAME as the IP address is not fixed. The aggressive mode does not authenticate the peer identity, so it has low security. |
| Local/Peer ID Type | <p>Specify the ID type of the local or peer device. The local ID type of the peer device must be the same as the peer ID type of the local device.</p> <ul style="list-style-type: none"> ● IP: The IP address is used as the identity ID. The IDs of the local and peer devices are generated automatically. ● NAME: The host character string is used as the identity ID. The IDs of the local and peer devices are generated automatically. When the IP address is not fixed, you need to set Local ID Type to NAME and modify the peer device settings accordingly. In this case, you also need to configure the host character string that is used as the identity ID. |
| Local/Peer ID | <p>When the local or peer ID type is set to NAME, you also need to host character string that is used as the identity ID. The local ID of the peer device must be the same as peer ID of the local device.</p> |

| Parameter | Description |
|--------------|---|
| Lifetime | Specify the lifetime of the IKE SA. (The negotiated IKE SA lifetime prevails.) You are advised to use the default value. |
| DPD | Specify whether to enable Dead Peer Detection (DPD) to detect the IPsec neighbor status. After DPD is enabled, if the receiver does not receive IPsec encrypted packets from the peer within the DPD detection interval, DPD query will be triggered and the receiver actively sends a request packet to detect whether the IKE peer exists. You are advised to configure DPD when links are unstable. |
| DPD Interval | Specify the DPD detection interval. That is, the interval for triggering DPD query. You are advised to keep the default setting. |

3. Advanced Settings (Phase 2)

Click **2. Connection Policy** to expand the configuration items. Keep the default settings unless otherwise specified.

----- [Connection Policy](#) -----

Protocol Type-Authentication-Encryption

Transform 1

Transform 2

Perfect Forward

Secrecy

* Lifetime

Table 10-3 IPsec server connection policy configuration

| Parameter | Description |
|-------------------------|---|
| Transform Set | <p>Specify the set of security protocol and algorithms. During IPsec SA negotiation, the two parties use the same transform set to protect specific data flow. The transform set on the IPsec server and IPsec client must be the same.</p> <ul style="list-style-type: none"> ● Security protocol: The Encapsulating Security Payload (ESP) protocol provides data source authentication, data integrity check, and anti-replay functions for IPsec connections and guarantees data confidentiality. ● Verification algorithm: <ul style="list-style-type: none"> ○ sha1: SHA-1 HMAC ○ md5: MD5 HMAC ● Encryption algorithm: <ul style="list-style-type: none"> ○ des: DES algorithm using 56-bit keys ○ 3des: 3DES algorithm using 168-bit keys ○ aes-128: AES algorithm using 128-bit keys ○ aes-192: AES algorithm using 192-bit keys ○ aes-256: AES algorithm using 256-bit keys |
| Perfect Forward Secrecy | <p>Perfect Forward Secrecy (PFS) is a security feature that can guarantee the security of other keys when one key is cracked, because there is no derivative relationship among the keys. After PFS is enabled, temporary private key exchange is performed when an IKE negotiation is initiated using a security policy. If PFS is configured on the local device, it must also be configured on the peer device that initiates negotiation and the DH group specified on the local and peer devices must be the same. Otherwise, negotiation will fail.</p> <ul style="list-style-type: none"> ● none: Disable PFS. ● d1: 768-bit DH group ● d2: 1024-bit DH group ● d5: 1536-bit DH group <p>By default, PFS is disabled.</p> |

10.1.3 Configuring the IPsec Client

Choose **One-Device > Gateway > Config > VPN > IPsec > IPsec Security Policy**.

Click **Add**. In the dialog box that appears, set **Policy Type** to **Client**, enter the policy name, peer gateway, local subnet range, and peer subnet range, set the pre-shared key, and click **OK**.

Note: Example: IP address/number of subnet mask bits.
Tips: If it is set to 192.168.110.x/24, the address range is from 192.168.110.1 to 192.168.110.254.
 Up to 3 entries with the policy type of client can be configured.
 Up to 1 entry with the policy type of server can be configured.
 The server and client cannot be configured at the same time.

Policy List + Add

| Policy Type ? | Policy Name ? | Peer Gateway ? | Key Exchange Version | Local Subnet ? | Peer Subnet ? | Status | Action |
|---------------|---------------|----------------|----------------------|----------------|---------------|--------|--------|
| No Data | | | | | | | |

Total 0 < 1 > 10/page

Add ×

Policy Type ? Client Server

Internet ? IPv4 IPv6

* Policy Name ?

* Peer Gateway ? +

Interface ? ▾

Key Exchange Version IKEv1 IKEv2
 ?

* Subnets

Local Subnets + Peer Subnets

* Pre-shared Key ?

Status

Table 10-4 IPsec client basic settings

| Parameter | Description |
|-------------|---|
| Policy Name | Specify the name of the IPsec security policy. The name must be a string of 1 to 28 characters. |
| Internet | Format of the IP address. Both IPv4 and IPv6 address formats are supported. |

| Parameter | Description |
|----------------------|---|
| Peer Gateway | Enter the IP address or domain name of the peer device. |
| Interface | Select a WAN port used locally from the drop-down list box. In the multi-line scenario, you are advised to set this parameter to Auto . |
| Key Exchange Version | <p>Select the IKE version for SA negotiation. There are two options available:</p> <ul style="list-style-type: none"> ● IKEv1: The negotiation of SA in IKEv1 primarily consists of two phases. <ul style="list-style-type: none"> ○ Phase 1: The purpose is to establish an IKE SA using one of two negotiation modes: Main Mode and Aggressive Mode. Main Mode requires six ISAKMP (Internet Security Association and Key Management Protocol) messages to complete the negotiation, while Aggressive Mode only requires three ISAKMP messages. Aggressive Mode offers faster IKE SA establishment. However, it combines key exchange and identity authentication, which means it does not provide identity protection. ○ Phase 2: The purpose is to establish an IPsec SA for data transmission, utilizing a fast exchange mode that requires only three ISAKMP messages to complete the negotiation. ● IKEv2: In IKEv2, the negotiation process for SA is simplified. The establishment of one IKE SA and one pair of IPsec SAs can be accomplished using two exchanges with four messages. If there is a need to establish more than one pair of IPsec SAs, only one additional exchange is needed for each pair. This enables the negotiation to be completed with just two messages per pair. |
| Local Subnets | Specify the local subnet address range for the data flows to be protected, that is, the LAN port network segment of the server. The value is the combination of IP address and subnet mask. |
| Peer Subnets | Specify the peer subnet address range for the data flows to be protected, that is, the LAN port network segment of the client. The value is the combination of IP address and subnet mask. |
| Pre-shared Key | Configure the pre-shared key the same as that on the IPsec server. |
| Status | Specify whether to enable the security policy. |

You can configure advanced parameters by referring to the corresponding settings on the IPsec server. For details, see [Advanced Settings \(Phase 1\)](#) and [Advanced Settings \(Phase 2\)](#).

10.1.4 Viewing the IPsec Connection Status

Choose **One-Device > Gateway > Config > VPN > IPsec > IPsec Connection Status**.

You can view the IPsec tunnel connection status on the current page.

IPSec Security Policy [IPSec Connection Status](#)

IPSec Connection Status Refresh

| Name | SPI | Direction | Tunnel Endpoint | Flow | Status | Security Protocol | Algorithm |
|------|----------------|-----------|------------------------------|---------------------------------------|--------|-------------------|--|
| test | 32569111 34 | in | 172.26.1.200<--172.26.30.192 | 192.168.120.0/24 <-- 192.168.110.0/24 | OK | ESP | AH Authentication: -- ESP Authentication: SHA1 ESP Security: AES-128 |
| test | 32874839 13 | out | 172.26.1.200-->172.26.30.192 | 192.168.120.0/24 --> 192.168.110.0/24 | OK | ESP | AH Authentication: -- ESP Authentication: SHA1 ESP Security: AES-128 |

Table 10-5 IPsec tunnel connection status information

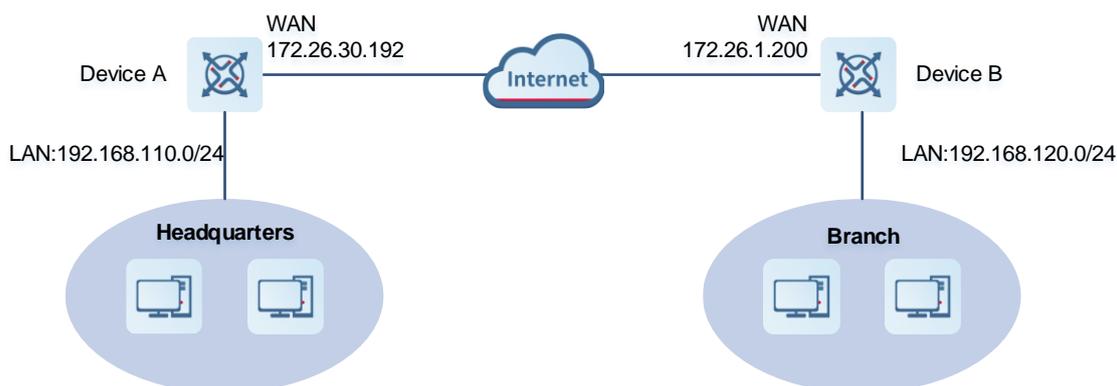
| Parameter | Description |
|-------------------|--|
| Name | Indicate the security policy name on the IPsec server or client. |
| SPI | Indicate the Security Parameter Index (SPI) of the IPsec connection, used to associate the received IPsec data packets with the corresponding SA. The SPI of each IPsec connection must be unique. |
| Direction | Indicate the direction of the IPsec connection. The value in indicates inbound, and the value out indicates outbound. |
| Tunnel Client | Indicate the gateway addresses on two ends of the IPsec connection. The arrow indicates the direction of data flows to be protected by the current tunnel. |
| Flow | Indicate the subnet range on two ends of the IPsec connection. The arrow indicates the direction of data flows to be protected by the current tunnel. |
| Status | Indicate the IPsec tunnel connection status. |
| Security Protocol | Indicate the security protocol used by the IPsec connection. |
| Algorithm | Indicate the encryption algorithm and authentication algorithm used by the IPsec connection. |

10.1.5 Typical Configuration Example

1. Networking Requirements

The HQ and branch of an enterprise are connected through the Internet. An IPsec tunnel needs to be established between the HQ gateway and branch gateway to ensure the confidentiality of transmitted data.

2. Networking Diagram



3. Configuration Roadmap

- Configure the HQ gateway Device A as the IPsec server.
- Configure the branch gateway Device B as the IPsec client.

4. Configuration Steps

- Configure the HQ gateway.

- (1) Log in to the web management system and choose **One-Device > Gateway > Config > VPN > IPsec > IPsec Security Policy** to access the IPsec Security Policy page.

Note: Example: IP address/number of subnet mask bits.
Tip: If it is set to 192.168.110.x/24, the address range is from 192.168.110.1 to 192.168.110.254.
 Up to 3 entries with the policy type of client can be configured.
 Up to 1 entry with the policy type of server can be configured.
 The server and client cannot be configured at the same time.

Policy List + Add

| Policy Type ? | Policy Name ? | Peer Gateway ? | Key Exchange Version | Local Subnet ? | Peer Subnet ? | Status | Action |
|---------------|---------------|----------------|----------------------|----------------|---------------|--------|--------|
| No Data | | | | | | | |

Total 0 < 1 > 10/page

- (2) Click **Add**. In the dialog box that appears, set Policy Type to Server, enter the policy name, select the bound interface, and configure the local subnet to be accessed through IPsec and the pre-shared key.

If the device connects to other EG devices in the Reyee network, you are advised to keep the default settings in IKE phase 1 and phase 2. If the device connects to devices from another vendor, keep the parameter settings consistent on the connected devices.

Add



i If clients want to access from different WAN ports, please set Local ID Type to Name. Otherwise, all clients will access from the same one WAN port.

Policy Type Client Server

Internet IPv4 IPv6

* Policy Name

Interface

Key Exchange Version IKEv1 IKEv2



* Subnets

[+ Local Subnets](#)

* Pre-shared Key

Status

- Configure the branch gateway.
 - (1) Log in to the web management system and access the IPsec Security Policy page.
 - (2) Click **Add**. In the dialog box that appears, set Policy Type to Client, enter the policy name, select the peer gateway (WAN port address or domain name of the HQ gateway), and configure the local subnet that needs to access the peer subnet and the pre-shared key the same as that on the HQ gateway. Keep the other phase 1 and phase 2 parameters consistent with those on the IPsec server.

Add×

Policy Type ? Client Server

Internet ? IPv4 IPv6

* Policy Name ?

* Peer Gateway ? +

Interface ? ▾

Key Exchange Version IKEv1 IKEv2 ?

* Subnets

Local Subnets + Peer Subnets

* Pre-shared Key ? 👁

Status

----- 1. Set IKE Policy -----

----- 2. Connection Policy -----

5. Verifying Configuration

- (1) Log in to the web management system of the HQ or branch gateway and choose **One-Device > Gateway > Config > VPN > IPsec > IPsec Connection Status**. You can view the IPsec connection status between the HQ and branch.

IPSec Security Policy [IPSec Connection Status](#)

IPSec Connection Status Refresh

| Name | SPI | Direction | Tunnel Client | Flow | Status | Security Protocol | Algorithm |
|------|------------|-----------|------------------------------|---------------------------------------|--------|-------------------|--|
| test | 3483169338 | in | 172.26.30.192<--172.26.1.200 | 192.168.110.0/24 <-- 192.168.120.0/24 | OK | ESP | AH Authentication: -- ESP Authentication: SHA1 ESP Security: AES-128 |
| test | 3281459512 | out | 172.26.30.192-->172.26.1.200 | 192.168.110.0/24 --> 192.168.120.0/24 | OK | ESP | AH Authentication: -- ESP Authentication: SHA1 ESP Security: AES-128 |

- (2) Perform ping test between clients on the two ends that need to access each other. The clients can successfully ping and access each other.

10.1.6 Solution to IPsec VPN Connection Failure

- (1) Run the ping command to test the connectivity between the client and server. For details, see Section [12.11.1 Network Check](#). If the ping fails, check the network connection settings. Check whether the branch EG can ping to HQ EG. If the ping fails, check the network connection between the two EGs.

Click **One-Device > Gateway > Config > Diagnostics > Network Tools**. Then, you can start the ping operation. For details, see Section [12.11.1 Network Check](#).

- (2) Confirm that the configurations on the IPsec server and IPsec client are correct.

Choose **One-Device > Gateway > Config > VPN > IPsec > IPsec Security Policy** and confirm that the security policies configured on the two ends are matching.

Policy List + Add

Up to 1 entries can be added.

| Policy Type | Policy Name | Peer Gateway | Local Subnet | Peer Subnet | Status | Action |
|-------------|-------------|--------------|------------------|-------------|----------|-------------|
| Server | test | 0.0.0.0 | 192.168.110.0/24 | 0.0.0.0/0 | Enable ☺ | Edit Delete |

Policy List + Add

Up to 1 entries can be added.

| Policy Type | Policy Name | Peer Gateway | Local Subnet | Peer Subnet | Status | Action |
|-------------|-------------|---------------|------------------|------------------|----------|-------------|
| Client | test | 172.26.30.192 | 192.168.120.0/24 | 192.168.110.0/24 | Enable ☺ | Edit Delete |

- (3) Check whether the WAN IP address of your HQ EG is a public IP address. If not, you need to configure DMZ or port mapping (UDP 500 and 4500 used as IPsec VPN port) on your egress gateway and set **Local ID Type** to **NAME** on HQ and branch gateways.

1. Set IKE Policy

Authentication-Encryption-DH Group

IKE Policy 1

IKE Policy 2

IKE Policy 3

IKE Policy 4

IKE Policy 5

Negotiation Mode Main Mode Aggressive Mode

Local ID Type IP Name

* Local ID

Peer ID Type IP Name

* Peer ID

* Lifetime

DPD Enable Disable

* DPD Interval
seconds

1. Set IKE Policy

Authentication-Encryption-DH Group

IKE Policy 1

IKE Policy 2

IKE Policy 3

IKE Policy 4

IKE Policy 5

Negotiation Mode Main Mode Aggressive Mode

Local ID Type IP Name

* Local ID

Peer ID Type IP Name

* Peer ID

* Lifetime

DPD Enable Disable

* DPD Interval
seconds

10.2 Configuring L2TP VPN

10.2.1 Overview

Layer Two Tunneling Protocol (L2TP) is a virtual tunneling protocol, usually used in virtual private networks.

The L2TP protocol does not provide encryption and reliability verification functions, but it can work with a security protocol to implement encrypted data transmission. L2TP is frequently used with IPsec to encapsulate packets using L2TP before encapsulating packets using IPsec. This combination implements user verification and address allocation through L2TP and ensures communication security through IPsec.

L2TP VPN can be used to establish secure tunnels between the enterprise HQ and branches and allow traveling employees to access the HQ. Currently, the device can be deployed as the L2TP server or client.

10.2.2 Configuring the L2TP Server

1. Basic Settings of L2TP Server

Choose **One-Device > Gateway > Config > VPN > L2TP > L2TP Settings**.

Turn on the L2TP function, set **L2TP Type** to **Server**, set L2TP server parameters, and click **Save**.

Enable Disable

L2TP Type Server Client

* Local Tunnel IP

* IP Range

* DNS Server

Tunnel Authentication Disable Enable

IPSec Security Open Security

Flow Control Disable Enable

* PPP Hello Interval seconds

Table 10-6 L2TP server configuration

| Parameter | Description |
|-----------------|--|
| Local Tunnel IP | Specify the local virtual IP address of the L2TP server. Clients can dial up to access the L2TP server through this address. |
| IP Range | Specify the address pool used by the L2TP server to allocate IP addresses to clients. |
| DNS Server | Specify the DNS server address pushed by the L2TP server to clients. |

| Parameter | Description |
|-----------------------|---|
| Tunnel Authentication | <p>Specify whether to enable L2TP tunnel authentication. If you enable this function, you need to configure a tunnel authentication key. By default, tunnel authentication is disabled.</p> <p>The tunnel authentication request can be initiated by clients. If tunnel authentication is enabled on one end, a tunnel to the peer can be established only when tunnel authentication is also enabled on the peer and consistent keys are configured on the two ends. Otherwise, the local end will automatically shut down the tunnel connection. If tunnel authentication is disabled on both ends, no authentication key is required for tunnel establishment.</p> <p>When a PC functions as the client to access the L2TP server, you are advised not to enable tunnel authentication on the L2TP server.</p> |
| IPsec Security | <p>Specify whether to encrypt the tunnel. If you select Security, the device encrypts the L2TP tunnel using IPsec, indicating the L2TP over IPsec mode.</p> <p>If an IPsec security policy is enabled on the current device, you cannot enable IPsec encryption for the L2TP tunnel. If you want to configure L2TP over IPsec, disable the IPsec security policy first.</p> <p>The IPsec encryption configuration on the L2TP server and client must be consistent. For details, see Configuring the L2TP Server.</p> |
| Flow Control | <p>The VPN server has a lower priority to control the traffic of the client than the custom policy. The VPN server can only limit the maximum uplink and downlink bandwidth per user for the client. For details, see Section 8.6.2 Intelligence QoS.</p> |
| PPP Hello Interval | <p>Specify the interval for sending PPP Hello packets after L2TP VPN is deployed. You are advised to retain the default configuration.</p> |

 **Caution**

The local tunnel address and IP address range of the address pool cannot overlap the network segment of the LAN port on the device.

2. Configuring the L2TP over IPsec Server

Choose **Local Device > VPN > L2TP > L2TP Settings**.

After you complete [Basic Settings of L2TP Server](#), enable IPsec encryption on the L2TP server to guarantee communication security. For details on the IPsec configuration, see Section [10.1 Configuring IPsec VPN](#).

* DNS Server

Tunnel Authentication Disable Enable

IPSec Security Open Security

* Pre-shared Key

IKE Policy

Transform Set

Negotiation Mode Main Mode Aggressive Mode

Local ID Type IP Address NAME

Flow Control Disable Enable

* PPP Hello Interval seconds

Table 10-7 L2TP over IPsec server configuration

| Parameter | Description |
|----------------|---|
| Pre-shared Key | Specify the same unique pre-shared key as the credential for mutual authentication between the server and client. |

| Parameter | Description |
|---------------|--|
| IKE Policy | <p>Select the encryption algorithm, hash algorithm, and DH group ID used by the IKE protocol. To ensure successful IKE negotiation, the two parties engaged in IKE negotiation must have at least one set of consistent IKE policy. The IKE policies on the server and client must be consistent.</p> <ul style="list-style-type: none"> ● Hash algorithm: <ul style="list-style-type: none"> ○ sha1: SHA-1 algorithm ○ md5: MD5 algorithm ● Encryption algorithm: <ul style="list-style-type: none"> ○ des: DES algorithm using 56-bit keys ○ 3des: 3DES algorithm using 168-bit keys ○ aes-128: AES algorithm using 128-bit keys ○ aes-192: AES algorithm using 192-bit keys ○ aes-256: AES algorithm using 256-bit keys ● DH group ID: <ul style="list-style-type: none"> ○ dh1: 768-bit DH group ○ dh2: 1024-bit DH group ○ dh5: 1536-bit DH group |
| Transform Set | <p>Specify the set of security protocol and algorithms. During IPsec SA negotiation, the two parties use the same transform set to protect specific data flow. The transform set on the server and client must be the same.</p> <ul style="list-style-type: none"> ● Security protocol: The Encapsulating Security Payload (ESP) protocol provides data source authentication, data integrity check, and anti-replay functions for IPsec connections and guarantees data confidentiality. ● Verification algorithm: <ul style="list-style-type: none"> ○ sha1: SHA-1 HMAC ○ md5: MD5 HMAC ● Encryption algorithm: <ul style="list-style-type: none"> ○ des: DES algorithm using 56-bit keys ○ 3des: 3DES algorithm using 168-bit keys ○ aes-128: AES algorithm using 128-bit keys ○ aes-192: AES algorithm using 192-bit keys ○ aes-256: AES algorithm using 256-bit keys |

| Parameter | Description |
|------------------|---|
| Negotiation Mode | <p>Select Main Mode or Aggressive Mode. The negotiation mode on the server and client must be the same.</p> <ul style="list-style-type: none"> ● Main Mode: This mode is applicable to communication between fixed public network IP addresses and point-to-point communication between devices. In this mode, the peer identity is authenticated to provide high security. ● Aggressive Mode: The public network IP addresses obtained by ADSL dial-up users are not fixed and an NAT device may exist. Therefore, the aggressive mode is used to implement NAT traversal. In this mode, you need to set the local and peer ID type to NAME as the IP address is not fixed. The aggressive mode does not authenticate the peer identity, so it has low security. |
| Local ID Type | <p>Specify the ID type of the local device. The peer ID of the client must be the same as local ID of the server.</p> <ul style="list-style-type: none"> ● IP: The IP address is used as the identity ID. The ID of the local device is generated automatically. ● NAME: The host character string is used as the identity ID. The ID of the local device is generated automatically. In this case, you also need to configure the host character string that is used as the identity ID. <p>When the WAN port IP address of the server is a private network address, you need to set Local ID Type to NAME and configure DMZ on the external device.</p> <p>When the IP address is not fixed, you need to set Local ID Type to NAME and modify the peer device settings accordingly.</p> |
| Local ID | <p>When Local ID Type is set to NAME, the host character string is used as the identity ID. The peer ID of the client must be the same as local ID of the server.</p> |

3. Configuring L2TP User

Choose **One-Device > Gateway > Config > VPN > VPN Account**

Only user accounts added to the VPN client list are allowed to dial up to connect to the L2TP server. Therefore, you need to manually configure user accounts for clients to access the L2TP server.

Click **Add**. In the dialog box that appears, set **Service Type** to **L2TP** or **ALL**. (If you select **ALL**, the created account can be used to establish all types of VPN tunnels.) Enter the username, password, and peer subnet, select a network mode, and click **OK**.

VPN User List Username/Password + Add Delete All Delete Selected

| <input type="checkbox"/> | Username | Password | Service Type | Network Mode | Client Subnet | Status | Action |
|--------------------------|--------------|----------|--------------|------------------|-----------------|--------|---|
| <input type="checkbox"/> | pptp@branch | **** | PPTP | Router to Router | 192.168.12.0/24 | Enable | Edit Delete |
| <input type="checkbox"/> | pptp@pc | **** | PPTP | PC to Router | - | Enable | Edit Delete |
| <input type="checkbox"/> | OpenVpnUser1 | **** | OpenVpn | - | - | Enable | Edit Delete |

Up to 300 entries can be added. Total 3 < 1 > 10/page

Add User

Service Type  L2TP 

* Username L2TP

* Password Network Mode  PC to Router Status

Cancel

OK

Table 10-8 L2TP user configuration

| Parameter | Description |
|-------------------|---|
| Username/Password | Specify the name and password of the L2TP user allowed to dial up to connect to the L2TP server. The username and password are used to establish a connection between the server and client. |
| Network Mode | <ul style="list-style-type: none"> ● PC to Router: The dial-up client is an individual. Select this mode when a PC wants to dial up to communicate with the remote PC through the LAN. ● Router to Router: The dial-up client is a user in a network segment. Select this mode when the LANs on two ends of the tunnel need to communicate through router dial-up. |
| Client Subnet | <p>Specify the IP address range used by the LAN on the peer end of the L2TP tunnel. Generally, the Client Subnet is the IP address network segment of the LAN port on the device. (The LAN network segments of the server and client cannot overlap.)</p> <p>For example, when a branch dials up to connect to the HQ, enter the LAN network segment of the router.</p> <p>Note: When the Network Mode is set to Router to Router, you can click  to set multiple pairs of peer subnets for scenarios where multiple clients are connected to the same server.</p> |
| Status | Specify whether to enable the user account. |

10.2.3 Configuring the L2TP Client

1. Basic Settings of L2TP Client

Choose **One-Device > Gateway > Config > VPN > L2TP > L2TP Settings**.

Turn on the L2TP function, set **L2TP Type** to **Client**, set L2TP client parameters, and click **Save**.

Enable

L2TP Type Server Client

* Username

* Password

Interface

Tunnel IP Dynamic Static

* Server Address

* Server Subnet +

Route All Traffic over VPN

Tunnel Authentication Disable Enable

IPSec Security Open Security

Working Mode NAT Router

* PPP Hello Interval seconds

Table 10-9 L2TP client configuration

| Parameter | Description |
|----------------------------|---|
| Username/Password | Specify the username and password for identity authentication for communication over the L2TP tunnel. The values must be the same as those configured on the L2TP server. |
| Interface | Specify the WAN port used by the client. |
| Tunnel IP | Specify the virtual IP address of the VPN tunnel client. If you select Dynamic , the client obtains an IP address from the server address pool. If you select Static , manually configure an idle static address within the range of the server address pool as the local tunnel IP address. |
| Server Address | Enter the WAN port IP address or domain name of the server. This address must be a public network IP address. |
| Server Subnet | Enter the LAN network segment in which clients want to access the server. The value cannot overlap with the LAN network segment of the client. |
| Route ALL Traffic over VPN | Once this feature is enabled, all traffic will be directed through the VPN connection, that is, VPN is configured as the default route. |
| Tunnel Authentication | Specify whether to enable L2TP tunnel authentication. If you enable this function, you need to enter tunnel authentication key the same as that configured on the server. By default, tunnel authentication is disabled. To protect tunnel security, you are advised to enable tunnel authentication. |
| IPsec Security | Specify whether to encrypt the tunnel. If you select Security, the device Enable the L2TP tunnel using IPsec, indicating the L2TP over IPsec mode. The IPsec encryption configuration on the server and client must be consistent. For details, see Configuring the L2TP Client . |
| Working Mode | <ul style="list-style-type: none"> ● NAT: Perform NAT traversal on the data packet passing through the L2TP tunnel. That is, replace the source IP address of the data packet with the local virtual IP address of the L2TP tunnel. In NAT mode, the server cannot access the LAN where the client resides. ● Router: Only route the data packet passing through the L2TP tunnel. In router mode, the server can access the LAN where the client resides. |
| PPP Hello Interval | Specify the interval for sending PPP Hello packets after L2TP VPN is deployed. You are advised to retain the default configuration. |

2. Configuring the L2TP over IPsec Client

Choose **One-Device > Gateway > Config > VPN > L2TP > L2TP Settings**.

After you complete [Basic Settings of L2TP Client](#), enable IPsec encryption on the L2TP client to guarantee communication security. The IPsec encryption configuration on the server and client must be consistent. For details, see [Configuring the L2TP Server](#).

Tunnel Authentication Disable Enable

IPSec Security Open Security

* Pre-shared Key

IKE Policy

Transform Set

Negotiation Mode Main Mode Aggressive Mode

Peer ID Type IP Address NAME

Working Mode NAT Router

* PPP Hello Interval seconds

Save

10.2.4 Viewing the L2TP Tunnel Information

Choose **One-Device > Gateway > Config > VPN > L2TP > Tunnel List**.

It takes some time to establish a VPN connection between the server and client. After the configuration of the server and client is completed, wait for 1 to 2 minutes to refresh the page and view the L2TP tunnel establishment status.

Export Log File Delete Selected

| <input type="checkbox"/> | Username | Server/Client | Tunnel Name | Virtual Local IP | Access Server IP | Peer Virtual IP | DNS | Status | Action |
|--------------------------|----------|---------------|-------------|------------------|------------------|-----------------|-----|--------|--------|
| No Data | | | | | | | | | |

Total 0 < 1 > 10/page

Table 10-10 L2TP tunnel information

| Parameter | Description |
|------------------|---|
| Username | Indicate the username used by the client for identity authentication. |
| Server/Client | Indicate the role of the current device, which is client or server. |
| Tunnel Name | Indicate the name of the vNIC generated by L2TP. |
| Virtual Local IP | Indicate the local virtual IP address of the tunnel. The virtual IP address of the L2TP client is allocated by the L2TP server. |
| Access Server IP | Indicate the real IP address of the peer connecting to the L2TP tunnel. |
| Peer Virtual IP | Indicate the peer virtual IP address of the tunnel. The virtual IP address of the L2TP client is allocated by the L2TP server. |
| DNS | Indicate the DNS server address allocated by the L2TP server. |

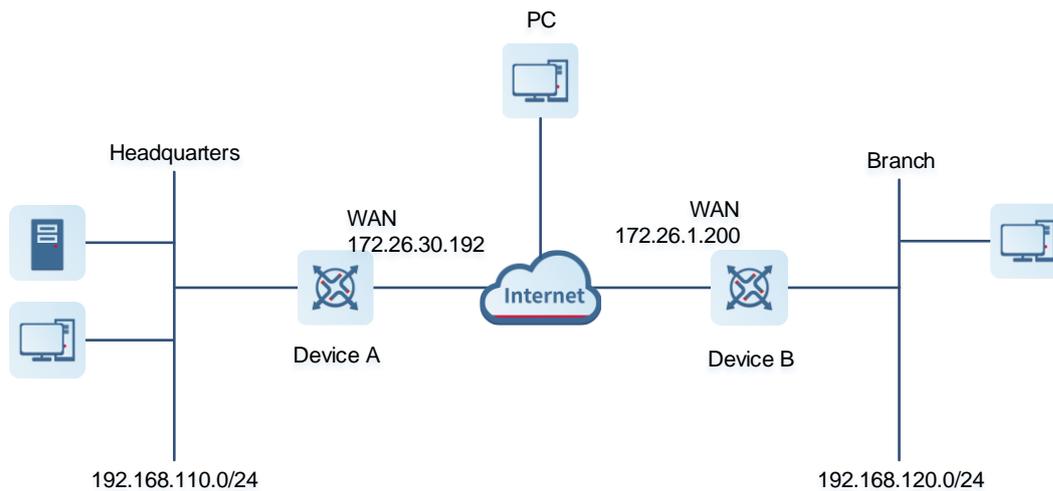
10.2.5 Typical Configuration Example

1. Networking Requirements

An enterprise wants to establish an L2TP tunnel to allow its traveling employees and branch employees to access the servers deployed in the HQ LAN.

- Traveling employees want to access the HQ servers from their PCs through L2TP VPN.
- Branch employees need to frequently access documents on the HQ servers. The enterprise wants to deploy the branch router (Device B) as the L2TP client, so that branch employees can dial up to transparently and directly access documents on the HQ servers, as if they are accessing servers inside the branch.

2. Networking Diagram



3. Configuration Roadmap

- Configure the HQ gateway Device A as the L2TP server.
- Configure the branch gateway Device B as the L2TP client.
- Configure the PC of the traveling employee as the L2TP client.

4. Configuration Steps

- Configure the HQ gateway.

Note

The LAN address of the HQ cannot conflict with that of the branch. Otherwise, resource access will fail.

- (1) Log in to the web management system and choose **One-Device > Gateway > Config > VPN > L2TP > L2TP Settings** to access the L2TP Settings page.
- (2) Turn on the L2TP function, set L2TP Type to **Server**, enter the local tunnel IP, IP Range, and DNS Server address, specify whether to enable IPsec encryption and tunnel authentication, and click **Save**.

Enable

L2TP Type Server Client

* Local Tunnel IP

IP Range

* DNS Server

Tunnel Authentication Disable Enable

IPSec Security Open Security

* Pre-shared Key

IKE Policy

Transform Set

Negotiation Mode Main Mode Aggressive Mode

Local ID Type IP Address NAME

Flow Control Disable Enable

* PPP Hello Interval seconds

Table 10-11 L2TP server configuration

| Parameter | Description |
|-----------------|--|
| Local Tunnel IP | Enter an IP address not in the LAN network segment. The PC can dial up to access the server through this IP address. |
| IP Range | Enter an IP address range not in the LAN network segment, which is used to allocate IP addresses to clients. |
| DNS Server | Enter an available DNS server address. |

| Parameter | Description |
|--|---|
| Tunnel Authentication | By default, tunnel authentication is disabled. After this function is enabled, the server and client can be connected only when they use the same tunnel key. You can keep tunnel authentication disabled. |
| IPsec Security | Specify whether to encrypt the L2TP tunnel using the IPsec protocol. You are advised to select Security to guarantee data security. If an IPsec security policy is enabled on the current device, you cannot enable IPsec encryption for the L2TP tunnel. If you want to configure L2TP over IPsec, disable the IPsec security policy first. |
| Pre-shared Key | Enter the key for IPsec authentication. The client can access the server only when the same pre-shared key is configured on the client. |
| IKE Policy Transform Set Negotiation Mode Local ID Type Local ID | Keep the default settings unless otherwise specified. |
| Flow Control | The VPN server has a lower priority to control the traffic of the client than the custom policy. The VPN server can only limit the maximum uplink and downlink bandwidth per user for the client. For details, see Section 8.6.2 Intelligence QoS . |
| PPP Hello Interval | Keep the default settings unless otherwise specified. |

- (3) Choose **One-Device > Gateway > Config > VPN > VPN Account** and add L2TP user accounts for the traveling employee and branch employee to access the HQ.

For the traveling employee account, set **Network Mode** to **PC to Router**.

For the branch employee account, set **Network Mode** to **Router to Router** and **Peer Subnet** to the LAN network segment of the branch gateway, which is 192.168.120.0/24.

 **Caution**

The LAN network segments of the server and client cannot overlap.

Add User ×

Service Type ⓘ

* Username

* Password

Network Mode ⓘ

* Client Subnet +

Status

Add User ×

Service Type ⓘ

* Username

* Password

Network Mode ⓘ

Status

VPN User List Username/Password

| <input type="checkbox"/> | Username | Password ↕ | Service Type ⓘ | Network Mode ⓘ | Client Subnet ⓘ | Status | Action |
|--------------------------|--------------|-------------------------|-----------------------------|-----------------------------|------------------------------|--------|---|
| <input type="checkbox"/> | pptp@branch | **** | PPTP | Router to Router | 192.168.12.0/24 | Enable | Edit Delete |
| <input type="checkbox"/> | pptp@pc | **** | PPTP | PC to Router | - | Enable | Edit Delete |
| <input type="checkbox"/> | OpenVpnUser1 | **** | OpenVpn | - | - | Enable | Edit Delete |
| <input type="checkbox"/> | branch | ***** | L2TP | Router to Router | 192.168.120.0/24 | Enable | Edit Delete |
| <input type="checkbox"/> | pc@l2tp | ***** | L2TP | PC to Router | - | Enable | Edit Delete |

Up to 300 entries can be added. Total 5

● Configure the branch gateway.

- (1) Log in to the web management system and access the L2TP Settings page.
- (2) Turn on the L2TP function, set L2TP Type to Client, enter the username and password configured on the server, server address, and LAN network segment of the peer, configure IPsec encryption parameters the same as those on the server, and click Save.

Enable

L2TP Type Server Client

* Username

* Password

Interface

Tunnel IP Dynamic Static

* Server Address

* Server Subnet +

Route All Traffic over VPN

Tunnel Authentication Disable Enable

IPSec Security Open Security

* Pre-shared Key

IKE Policy

Transform Set

Negotiation Mode Main Mode Aggressive Mode

Peer ID Type IP Address NAME

Working Mode NAT Router

* PPP Hello Interval seconds

Table 10-12 L2TP client configuration

| Parameter | Description |
|--|---|
| Username/Password | Enter the username and password configured on the server. |
| Interface | Select the WAN port on the client to establish a tunnel with the server. |
| Tunnel IP | Select Dynamic to automatically obtain the tunnel IP address. You can also select Static and enter an IP address in the address pool of the server. |
| Server Address | Enter the WAN port address of the server, which is 172.26.30.192. |
| Server Subnet | Enter the LAN network segment (LAN port IP address range) of the server, which is 192.168.110.0/24. |
| Route ALL Traffic over VPN | Once this feature is enabled, all traffic will be directed through the VPN connection, that is, VPN is configured as the default route. |
| Tunnel Authentication | The value must be the same as that on the server. In this example, you need to disable tunnel authentication. |
| IPsec Security | The value must be the same as that on the server. In this example, you need to set this parameter to Security. |
| Pre-shared Key | Enter the pre-shared key configured on the server. |
| IKE Policy Transform Set Negotiation Mode Peer ID Type Peer ID | The settings must be the same as those on the server. Set Peer ID Type to the same value as that of Local ID Type on the server. |
| Work Mode | If the HQ wants to access the LAN of the branch, set this parameter to Router. |
| PPP Hello Interval | Specify the interval for sending PPP Hello packets after L2TP VPN is deployed. Keep the default settings. |

- Configure the PC of the traveling employee.

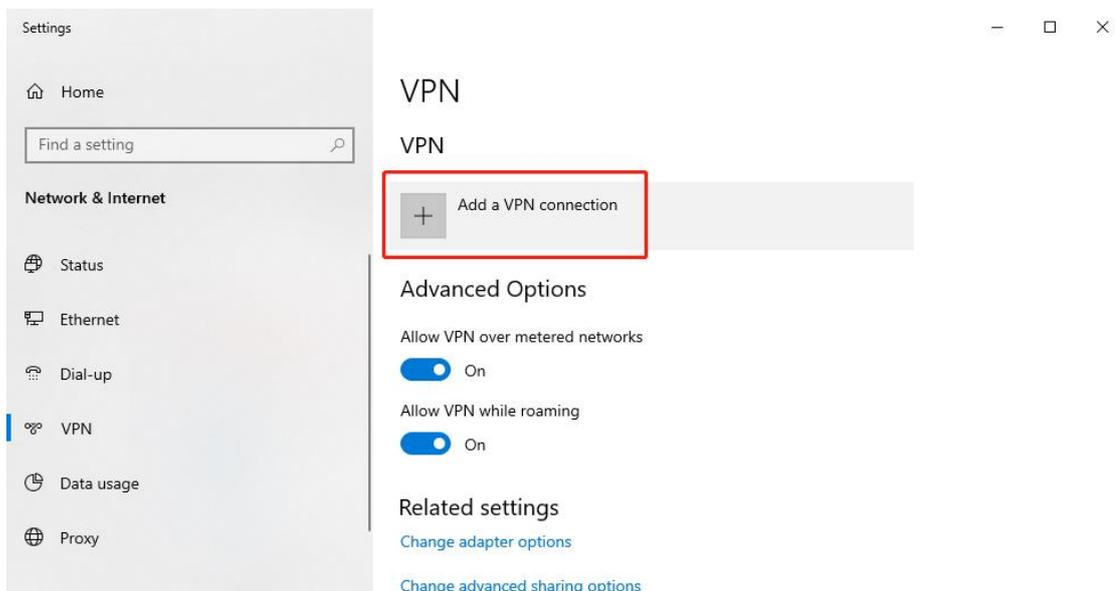
Note

- Configure the PC of a traveling employee as the L2TP client. The following uses the PC running Windows 10 operating system as an example.
- The Windows XP (shorted as XP) system and Windows 7/Windows 10 (shorted as Win7/10) system differ in their support for L2TP VPN: To enable L2TP VPN in the XP system, you need to modify the

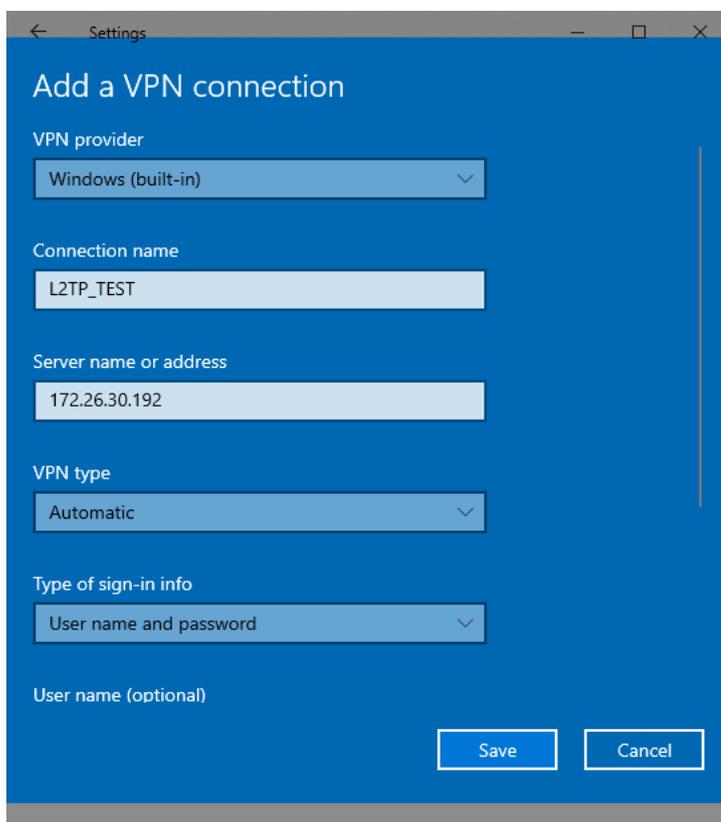
service registries. L2TP is supported in the Win7/10 system by default, without the need to modify registries.

- Neither the Win7/Win10 system nor the XP system supports L2TP tunnel authentication. Therefore, tunnel authentication must be disabled on the server.
- Apple mobile phones support L2TP over IPsec but do not support IPsec encryption for L2TP dial-up.

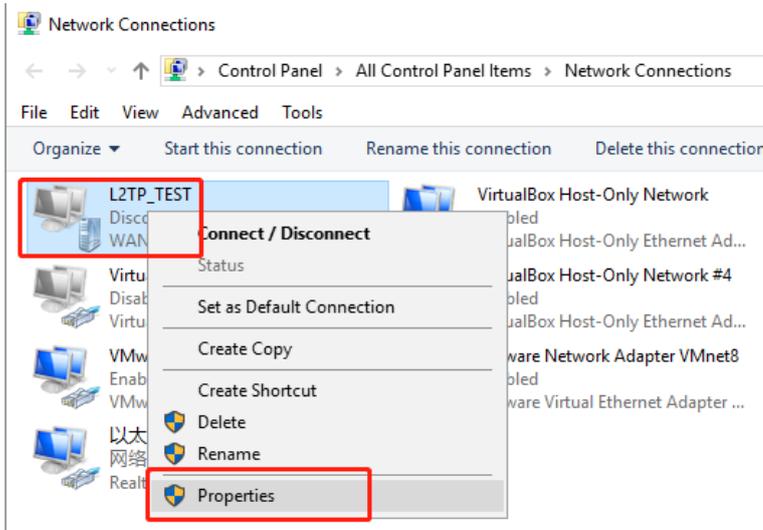
- (1) Choose **Settings > Network & Internet > VPN** to access the VPN page.



- (2) Click **Add a VPN connection**. In the dialog box that appears, set VPN provider to **Windows**, enter the connection name and server address or domain name, and click **Save**.



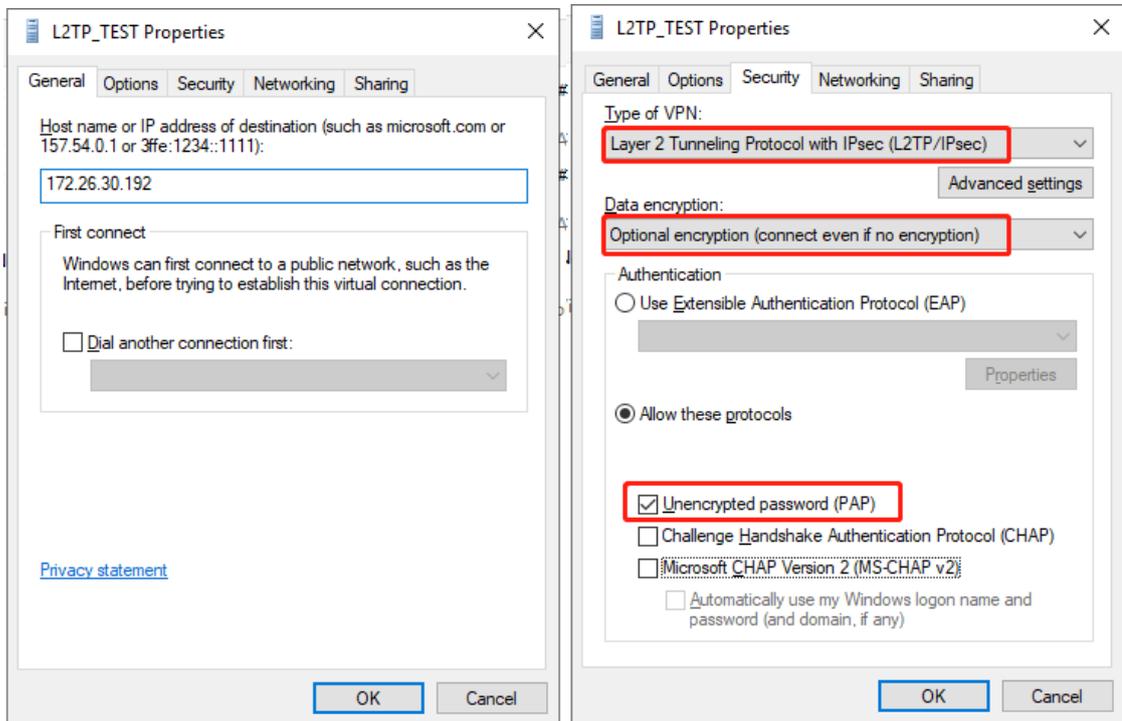
- Right-click the created VPN connection named **L2TP_TEST** and select Properties to view the properties of the network connection.



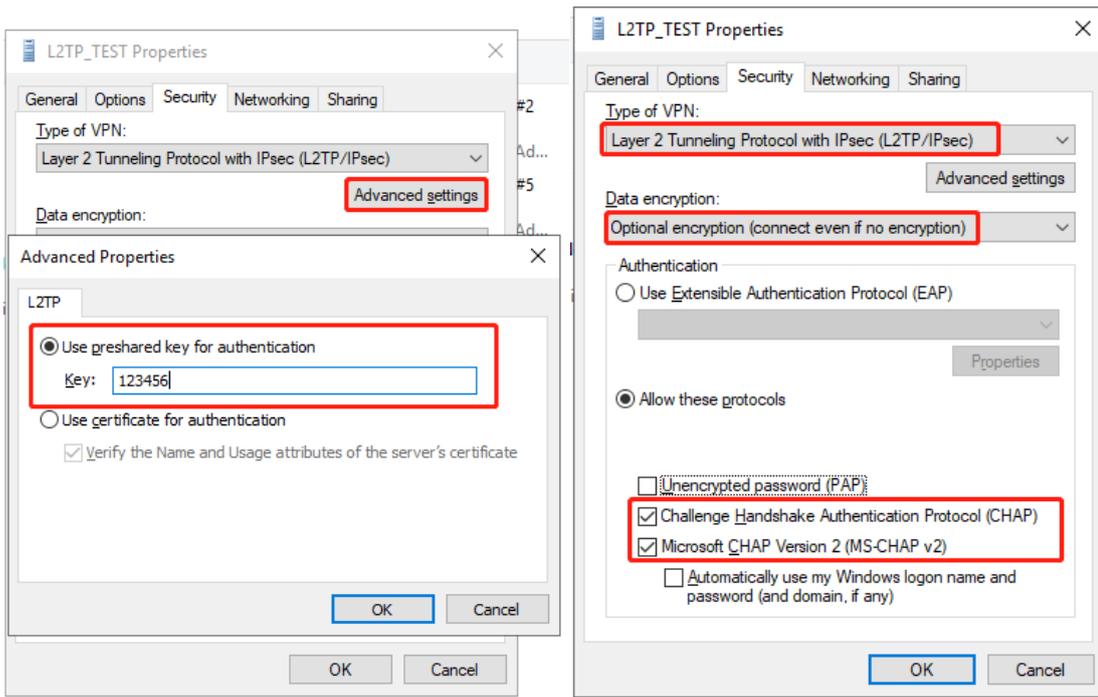
- In the dialog box that appears, click the Security tab, and set Type of VPN to Layer 2 Tunneling Protocol with IPsec (L2TP/IPsec) and Data encryption to Optional encryption (connect even if no encryption).

If IPsec encryption is not enabled on the L2TP server, select **Unencrypted password (PAP)** and click **OK**. Skip Step (5) .

If IPsec encryption is enabled on the L2TP server, perform Step (5) .



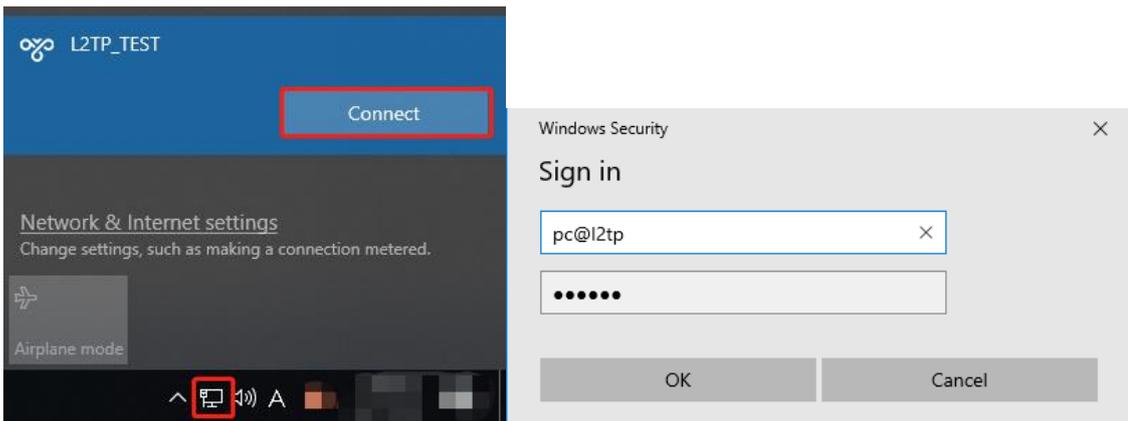
- If IPsec encryption is enabled on the server, select **CHAP** and **MS-CHAP v2** as the identity authentication protocols and click **Advanced settings**. In the dialog box that appears, configure the pre-shared key the same as that on the server. After completing the configuration, click **OK**.



Note

The device does not support EAP for identity authentication. Therefore, you cannot select EAP-related identity authentication options in the Windows client. Otherwise, the VPN connection fails.

- After the L2TP client configuration is completed on the PC, initiate a VPN connection on the PC. Click the network icon  in the task bar, select the created L2TP VPN connection, and click Connect. In the dialog box that appears, enter the username and password configured on the server.



5. Verifying Configuration

- After the server and client are configured, wait for about 1 minute. If you can view the L2TP tunnel connection information on the HQ server and branch client, the connection is successful.

HQ:

L2TP Settings [Tunnel List](#)

| Tunnel List | | | | | | | | |
|--------------------------|----------|---------------|-------------|------------------|------------------|-----------------|-----------------|------------------------|
| <input type="checkbox"/> | Username | Server/Client | Tunnel Name | Virtual Local IP | Access Server IP | Peer Virtual IP | DNS | Action |
| <input type="checkbox"/> | pc@l2tp | Server | ppp2 | 20.0.0.1 | 172.26.1.200 | 20.1.1.3 | 114.114.114.114 | Delete |
| <input type="checkbox"/> | branch | Server | ppp0 | 20.0.0.1 | 172.26.1.200 | 20.1.1.2 | 114.114.114.114 | Delete |

Branch:

| Tunnel List | | | | | | | | |
|-------------------------------------|----------|---------------|-------------|------------------|------------------|-----------------|-----------------|------------------------|
| <input type="checkbox"/> | Username | Server/Client | Tunnel Name | Virtual Local IP | Access Server IP | Peer Virtual IP | DNS | Action |
| <input checked="" type="checkbox"/> | branch | Client | l2tp | 20.1.1.2 | 172.26.30.192 | 20.0.0.1 | 114.114.114.114 | Delete |

- Ping the LAN address of the peer from the HQ or branch. The HQ and branch can successfully communicate. The PC of the traveling employee and the PC of the branch employee can access the HQ server.

```

Administrator: C:\Windows\system32\cmd.exe

C:\Users\Administrator>ping 192.168.110.1

Pinging 192.168.110.1 with 32 bytes of data:
Reply from 192.168.110.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.110.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
    
```

10.2.6 Solution to L2TP VPN Connection Failure

- Run the ping command to test the connectivity between the client and server. For details, see Section [12.11.1 Network Check](#). If the ping fails, check the network connection settings. Check whether the branch EG can ping to HQ EG. If the ping fails, check the network connection between the two EGs.
Choose **One-Device > Gateway > Config > Diagnostics > Network Tools**. Then, you can start the ping operation. For details, see Section [12.11.1 Network Check](#).
- Check whether the username and password used by the client are the same as those configured on the server.
- Check whether the WAN port IP address of your HQ EG is a public network IP address. If not, you need to configure DMZ on your egress gateway.

10.3 Configuring PPTP VPN

10.3.1 Overview

Point-to-Point Tunneling Protocol (PPTP) is an enhanced security protocol designed based on the Point-to-Point Protocol (PPP). It allows an enterprise to use private tunnels to expand its enterprise network over the public network. PPTP relies on the PPP protocol to implement security functions such as encryption and identity authentication. Generally, PPTP works with Password Authentication Protocol (PAP), Challenge Handshake Authentication Protocol (CHAP), Microsoft Challenge Handshake Authentication Protocol (MS-CHAPv1/v2), or Extensible Authentication Protocol-Transport Layer Security (EAP-TLS) for identity authentication and Microsoft Point-to-Point Encryption (MPPE) for encryption to improve security.

Currently, the device can be deployed as the PPTP server or client. It supports MPPE for encryption MSCHAP-v2 for identity authentication, and does not support EAP authentication.

10.3.2 Configuring the PPTP Service

1. Configuring the PPTP Server

Choose **One-Device > Gateway > Config > VPN > PPTP > PPTP Settings**.

Turn on the PPTP function, set **PPTP Type** to **Server**, configure PPTP server parameters, and click **Save**.

Enable

PPTP Type Server Client

* Local Tunnel IP

* IP Range (?)

* DNS Server

MPPE Disable Enable

Flow Control Disable Enable

* PPP Hello Interval (?) seconds

Table 10-13 PPTP server configuration

| Parameter | Description |
|--------------------|--|
| Local Tunnel IP | Specify the local virtual IP address of the L2TP server. Clients can dial up to access the L2TP server through this address. |
| IP Range | Specify the address pool used by the PPTP server to allocate IP addresses to clients. |
| DNS Server | Specify the DNS server address pushed by the PPTP server to clients. |
| MPPE | <p>Specify whether to use MPPE to encrypt the PPTP tunnel.</p> <p>After MPPE is enabled on the server: If Data encryption is set to Optional encryption on the client, the server and client can be connected but the server does not encrypt packets. If Data encryption is set to Require encryption on the client, the server and client can be connected and the server encrypts packets. If Data encryption is set to No encryption allowed on the client, the server and client cannot be connected.</p> <p>If MPPE is disabled on the server but the client requires encryption, the server and client connection fails.</p> <p>By default, MPPE is disabled on the server. After you enable MPPE, the bandwidth performance of the device degrades. You are advised to keep MPPE disabled if there are no special security requirements.</p> |
| Flow Control | The VPN server has a lower priority to control the traffic of the client than the custom policy. The VPN server can only limit the maximum uplink and downlink bandwidth per user for the client. For details, see Section 8.6.2 Intelligence QoS |
| PPP Hello Interval | Specify the interval for sending PPP Hello packets after PPTP VPN is deployed. |

 **Caution**

The local tunnel address and IP address range of the address pool cannot overlap the network segment of the LAN port on the device.

2. Configuring PPTP User

Choose **One-Device > Gateway > Config > VPN > VPN Account**.

Only user accounts added to the VPN client list are allowed to dial up to connect to the PPTP server. Therefore, you need to manually configure user accounts for clients to access the PPTP server.

Click **Add**. In the dialog box that appears, set **Service Type** to **PPTP** or **ALL**. (If you select **ALL**, the created account can be used to establish all types of VPN tunnels.) Enter the username, password, and peer subnet, select a network mode, and click **OK**.

VPN User List Username/Password **+ Add**

| <input type="checkbox"/> | Username | Password | Service Type | Network Mode | Client Subnet | Status | Action |
|--------------------------|-------------|----------|--------------|------------------|-----------------|--------|---|
| <input type="checkbox"/> | pptp@branch | **** | PPTP | Router to Router | 192.168.12.0/24 | Enable | Edit Delete |
| <input type="checkbox"/> | pptp@pc | **** | PPTP | PC to Router | - | Enable | Edit Delete |

Add User ✕

Service Type

* Username

* Password

Network Mode

Status

Table 10-14 PPTP user configuration

| Parameter | Description |
|-------------------|--|
| Username/Password | Specify the name and password of the PPTP user allowed to dial up to connect to the PPTP server. The username and password are used to establish a connection between the server and client. |
| Network Mode | <ul style="list-style-type: none"> ● PC to Router: The dial-up client is an individual. Select this mode when a PC wants to dial up to communicate with the remote PC through the LAN. ● Router to Router: The dial-up client is a user in a network segment. Select this mode when the LANs on two ends of the tunnel need to communicate through router dial-up. |

| Parameter | Description |
|---------------|---|
| Client Subnet | <p>Specify the IP address range used by the LAN on the peer end of the PPTP tunnel. Generally, the peer subnet is the IP address network segment of the LAN port on the device. (The LAN network segments of the server and client cannot overlap.)</p> <p>For example, when a branch dials up to connect to the HQ, enter the LAN network segment of the router.</p> <p>Note: When the Network Mode is set to Router to Router, you can click  to set multiple pairs of peer subnets for scenarios where multiple clients are connected to the same server.</p> |
| Status | Specify whether to enable the user account. |

10.3.3 Configuring the PPTP Client

Choose **One-Device** > **Gateway** > **Config** > **VPN** > **PPTP** > **PPTP Settings**.

Turn on the PPTP function, set **PPTP Type** to **Client**, configure PPTP client parameters, and click **Save**.

Enable

PPTP Type Server Client

* Username

* Password

Interface

Tunnel IP Dynamic Static

* Server Address

* Server Subnet +

Route All Traffic over VPN

MPPE Disable Enable

Working Mode NAT Router

* PPP Hello Interval seconds

Table 10-15 PPTP client configuration

| Parameter | Description |
|-------------------|---|
| Username/Password | Specify the username and password for identity authentication for communication over the PPTP tunnel. The values must be the same as those configured on the PPTP server. |
| Interface | Specify the WAN port used by the client. |

| Parameter | Description |
|----------------------------|--|
| Tunnel IP | Specify the virtual IP address of the VPN tunnel client. If you select Dynamic, the client obtains an IP address from the server address pool. If you select Static, manually configure an idle static address within the range of the server address pool as the local tunnel IP address. |
| Server Address | Enter the WAN port IP address or domain name of the server. This address must be a public network IP address. |
| Server Subnet | Enter the LAN network segment in which clients want to access the server. The value cannot overlap with the LAN network segment of the client. |
| Route All Traffic over VPN | Once this feature is enabled, all traffic will be directed through the VPN connection, that is, VPN is configured as the default route. |
| MPPE | Specify whether to use MPPE to encrypt the PPTP tunnel. The value must be the same as that on the server. |
| Work Mode | <ul style="list-style-type: none"> ● NAT: The client can access the server network, but the server cannot access the client network. ● Router: The server can access the client network. |
| PPP Hello Interval | Specify the interval for sending PPP Hello packets after a PPTP tunnel is established. You are advised to retain the default configuration. |

10.3.4 Viewing the PPTP Tunnel Information

Choose **One-Device > Gateway > Config > VPN > PPTP > Tunnel List**.

It takes some time to establish a VPN connection between the server and client. After the configuration of the server and client is completed, wait for 1 to 2 minutes to refresh the page and view the PPTP tunnel establishment status.

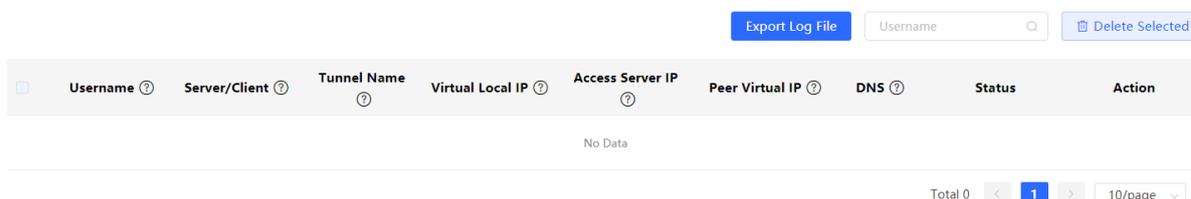


Table 10-16 PPTP tunnel information

| Parameter | Description |
|-----------|---|
| Username | Indicate the username used by the client for identity authentication. |

| Parameter | Description |
|------------------|---|
| Server/Client | Indicate the role of the current device, which is client or server. |
| Tunnel Name | Indicate the name of the vNIC generated by PPTP. |
| Virtual Local IP | Indicate the local virtual IP address of the tunnel. The virtual IP address of the PPTP client is allocated by the PPTP server. |
| Access Server IP | Indicate the real IP address of the peer connecting to the PPTP tunnel. |
| Peer Virtual IP | Indicate the peer virtual IP address of the tunnel. The virtual IP address of the PPTP client is allocated by the PPTP server. |
| DNS | Indicate the DNS server address allocated by the PPTP server. |

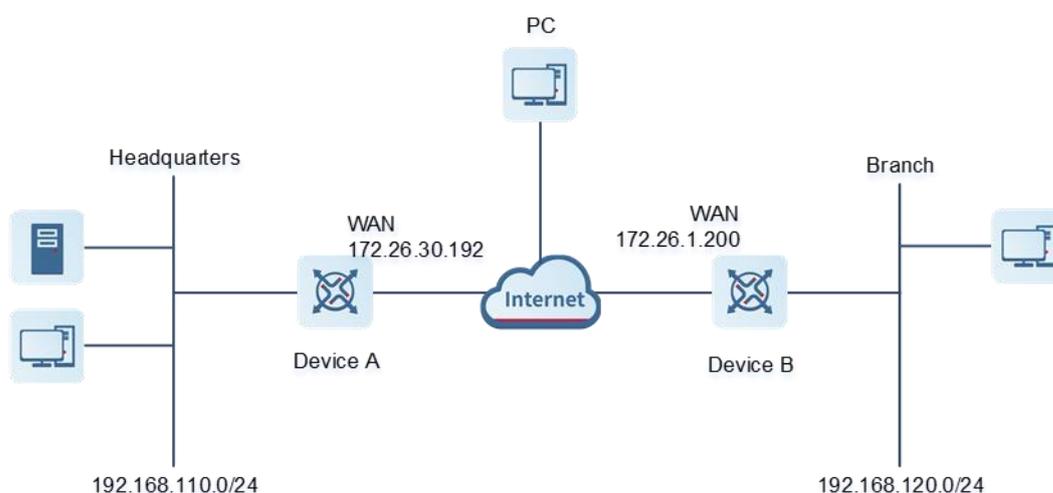
10.3.5 Typical Configuration Example

1. Networking Requirements

An enterprise wants to establish a PPTP tunnel to allow its traveling employees and branch employees to access the servers deployed in the HQ LAN.

- Traveling employees want to access the HQ servers from their PCs through PPTP dial-up.
- Branch employees need to frequently access documents on the HQ servers. The enterprise wants to deploy the branch router (Device B) as the PPTP client, so that branch employees can dial up to transparently and directly access documents on the HQ servers, as if they are accessing servers inside the branch.

2. Networking Diagram



3. Configuration Roadmap

- Configure the HQ gateway Device A as the PPTP server.
- Configure the branch gateway Device B as the PPTP client.
- Configure the PC of the traveling employee as the PPTP client.

4. Configuration Steps

- Configure the HQ gateway.

Note

The LAN address of the HQ cannot conflict with that of the branch. Otherwise, resource access will fail.

- (1) Log in to the web management system and choose **One-Device > Gateway > Config > VPN > PPTP > PPTP Settings** to access the PPTP Settings page.
- (2) Turn on the PPTP function, set PPTP Type to Server, enter the local tunnel address, address pool IP address range, and DNS server address, specify whether to enable MPPE encryption, and click Save.

Enable

PPTP Type Server Client

* Local Tunnel IP

* IP Range (?)

* DNS Server

MPPE Disable Enable

Flow Control Disable Enable

* PPP Hello Interval (?) seconds

Table 10-17 PPTP server configuration

| Parameter | Description |
|-----------------|--|
| Local Tunnel IP | Enter an IP address not in the LAN network segment. The PC can dial up to access the server through this IP address. |

| Parameter | Description |
|--------------------|--|
| IP Range | Enter an IP address range not in the LAN network segment, which is used to allocate IP addresses to clients. |
| DNS Server | Enter an available DNS server address. |
| MPPE | Specify whether to use MPPE to encrypt the PPTP tunnel. The value must be the same as that on the client. After you enable MPPE, the device security is improved but the bandwidth performance of the device degrades. You are advised to keep MPPE disabled if there are no special security requirements. |
| Flow Control | Flow control is disabled by default. |
| PPP Hello Interval | Keep the default settings unless otherwise specified. |

(3) Choose **One-Device > Gateway > Config > VPN > VPN Account** and add PPTP user accounts for the traveling employee and branch employee to access the HQ.

For the traveling employee account, set **Network Mode to PC to Router**.

For the branch employee account, set **Network Mode to Router to Router** and **Client Subnet** to the LAN network segment of the branch gateway.

⚠ Caution

The LAN network segments of the server and client cannot overlap.

Add User



Service Type ?

* Username

* Password

Network Mode ?

* Client Subnet +

Status

Cancel

Add User ×

Service Type ?

* Username

* Password

Network Mode ?

Status

VPN User List

Username/Password

| <input type="checkbox"/> | Username | Password ↕ | Service Type ? | Network Mode ? | Client Subnet ? | Status | Action |
|--------------------------|----------|-------------------------|-----------------------------|-----------------------------|------------------------------|--------|---|
| <input type="checkbox"/> | branch | ***** | L2TP | Router to Router | 192.168.120.0/24 | Enable | Edit Delete |
| <input type="checkbox"/> | pc@l2tp | ***** | L2TP | PC to Router | - | Enable | Edit Delete |
| <input type="checkbox"/> | branch | ***** | PPTP | Router to Router | 192.168.120.0/24 | Enable | Edit Delete |
| <input type="checkbox"/> | pc@pptp | ***** | PPTP | PC to Router | - | Enable | Edit Delete |

Up to 300 entries can be added.

Total 4

- Configure the branch gateway.
 - (1) Log in to the web management system and access the PPTP Settings page.
 - (2) Turn on the PPTP function, set PPTP Type to Client, enter the username and password configured on the server, server address, and LAN network segment of the peer, configure IPsec encryption parameters the same as those on the server, and click Save.

Enable

PPTP Type Server Client

* Username

* Password

Interface

Tunnel IP Dynamic Static

* Server Address

* Server Subnet +

Route All Traffic over VPN

MPPE Disable Enable

Working Mode NAT Router

* PPP Hello Interval seconds

Table 10-18 PPTP client configuration

| Parameter | Description |
|-------------------|---|
| Username/Password | Enter the username and password configured on the server. |
| Interface | Select the WAN port on the client to establish a tunnel with the server. |
| Tunnel IP | Select Dynamic to automatically obtain the tunnel IP address. You can also select Static and enter an IP address in the address pool of the server. |
| Server Address | Enter the WAN port address of the server. |
| Server Subnet | Enter the LAN network segment (LAN port IP address range) of the server. |

| Parameter | Description |
|----------------------------|---|
| Route All Traffic over VPN | Once this feature is enabled, all traffic will be directed through the VPN connection, that is, VPN is configured as the default route. |
| MPPE | The value must be the same as that on the server. |
| Working Mode | If the HQ wants to access the LAN of the branch, set this parameter to Router. |
| PPP Hello Interval | Specify the interval for sending PPP Hello packets after PPTP VPN is deployed. Keep the default settings. |

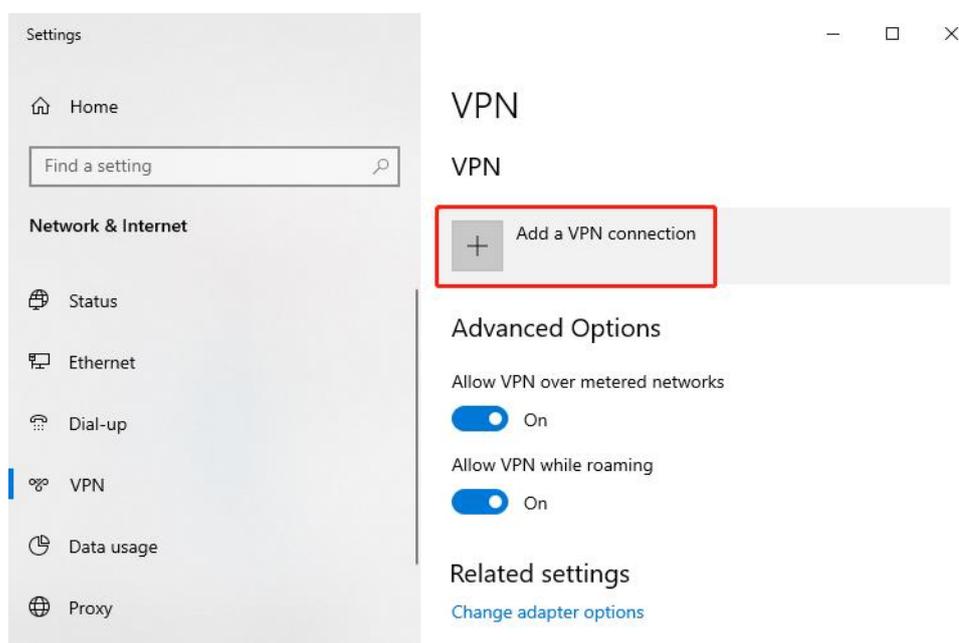
- Configure the PC of the traveling employee.

Note

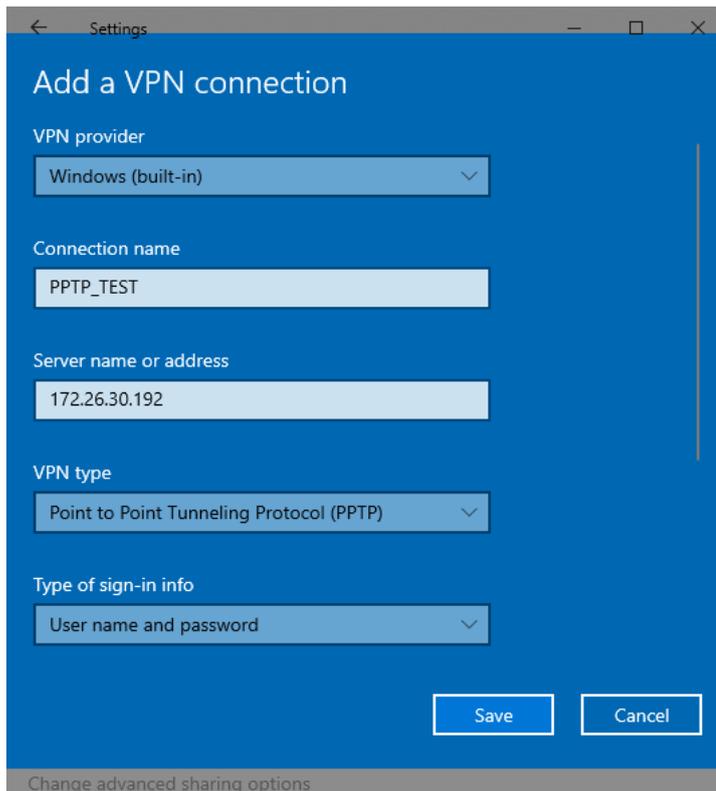
Configure the PC of a traveling employee as the PPTP client. The following uses the PC running Windows 10 operating system as an example.

Enable ports 1723 (PPTP) and 47 (GRE) on the PC firewall.

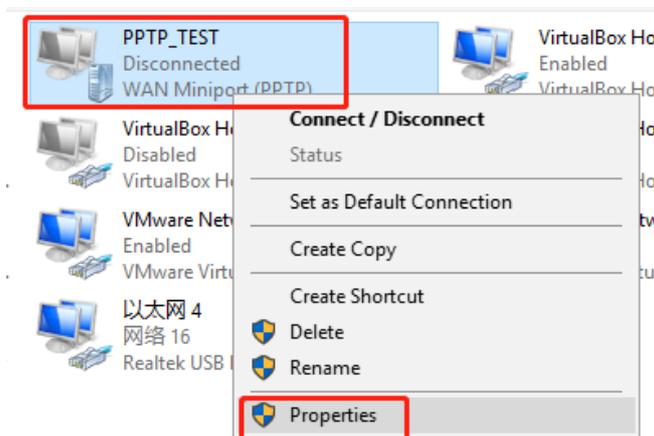
- (1) Choose **Settings > Network & Internet > VPN** to access the VPN page.



- (2) Click **Add a VPN connection**. In the dialog box that appears, set VPN provider to **Windows** and VPN type to **Point to Point Tunneling Protocol (PPTP)**, enter the connection name and server address or domain name, and click **Save**.



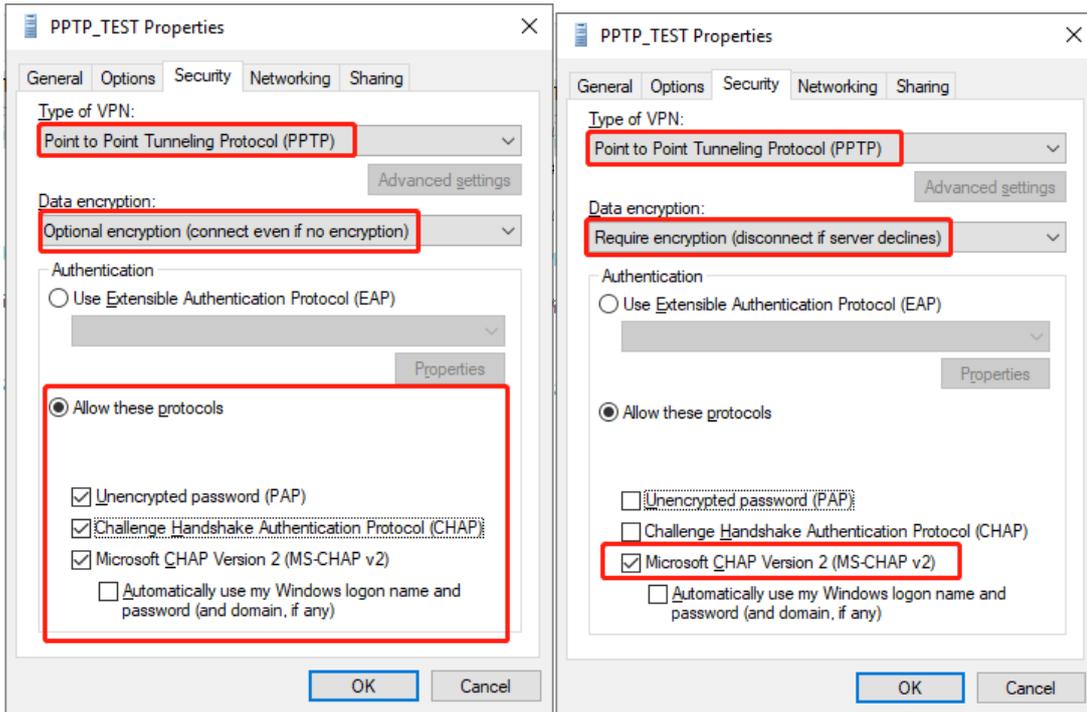
- (3) Right-click the created VPN connection named **PPTP_TEST** and select Properties to view the properties of the network connection.



- (4) In the dialog box that appears, click the **Security** tab.

If MPPE is not enabled on the PPTP server, set **Data encryption** to **Optional encryption** or **No encryption allowed** and use PAP, CHAP, or MS-CHAP v2 for identity authentication, as shown in the following figure on the left.

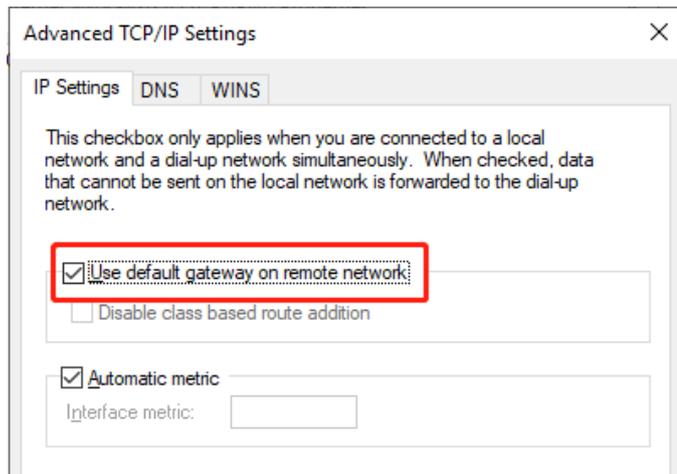
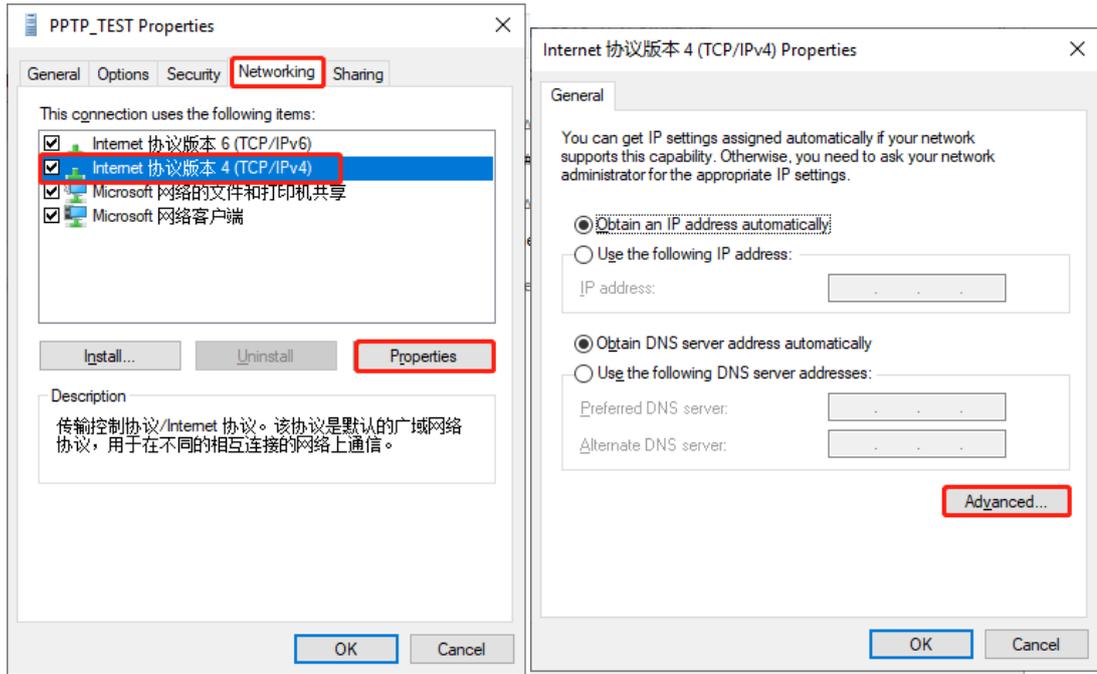
If MPPE is enabled on the PPTP server, set **Data encryption** to **Require encryption** or **Maximum strength encryption** and use MS-CHAP v2 for identity authentication, as shown in the following figure on the right.



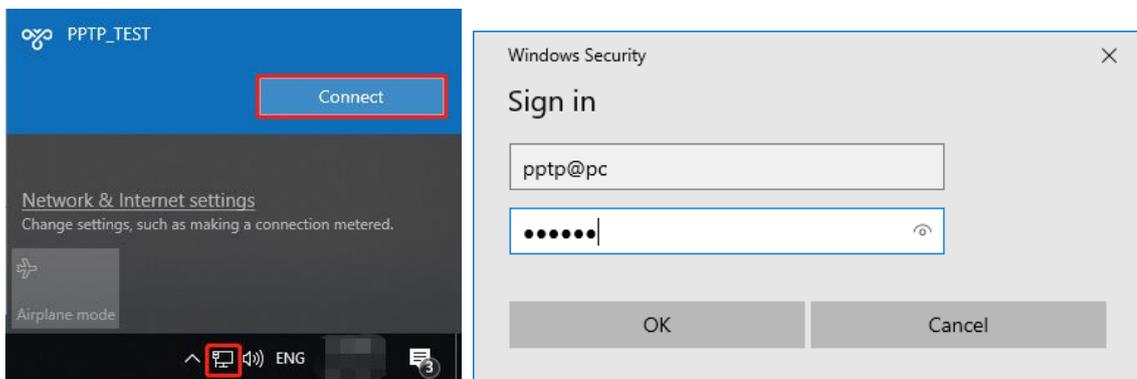
Note

The device does not support EAP for identity authentication. Therefore, you cannot select EAP-related identity authentication options in the Windows client. Otherwise, the VPN connection fails.

- (5) When the PC functions as a dial-up client, configure the PC by using either of the following methods:
 - o Add a route to the VPN peer network segment on the PC as the administrator.
 - o In the **Properties** dialog box of the local VPN connection, select **Use default gateway on remote network**. After the VPN connection is successful, all data flows from the PC to the Internet are routed to the VPN tunnel. The following figures show the detailed configuration.



- (6) After the PPTP client configuration is completed on the PC, initiate a VPN connection on the PC. Click the network icon  in the task bar, select the PPTP VPN connection, and click **Connect**. In the dialog box that appears, enter the username and password configured on the server.



5. Verifying Configuration

- (1) After the server and client are configured, wait for about 1 minute. If you can view the PPTP tunnel connection information on the HQ server and branch client, the connection is successful.

HQ:

PPTP Settings [Tunnel List](#)

| Tunnel List | | | | | | | | |
|--------------------------|----------|---------------|-------------|------------------|------------------|-----------------|-----------------|--------|
| <input type="checkbox"/> | Username | Server/Client | Tunnel Name | Virtual Local IP | Access Server IP | Peer Virtual IP | DNS | Action |
| <input type="checkbox"/> | pc@pptp | Server | ppp2 | 10.1.1.1 | 172.26.1.200 | 10.2.2.3 | 114.114.114.114 | Delete |
| <input type="checkbox"/> | branch | Server | ppp1 | 10.1.1.1 | 172.26.1.200 | 10.2.2.2 | 114.114.114.114 | Delete |

Branch:

| Tunnel List | | | | | | | | |
|-------------------------------------|----------|---------------|-------------|------------------|------------------|-----------------|-----------------|--------|
| <input type="checkbox"/> | Username | Server/Client | Tunnel Name | Virtual Local IP | Access Server IP | Peer Virtual IP | DNS | Action |
| <input checked="" type="checkbox"/> | branch | Client | pptp | 10.2.2.2 | 172.26.30.192 | 10.1.1.1 | 114.114.114.114 | Delete |

- (2) Ping the LAN address of the peer from the HQ or branch. The HQ and branch can successfully communicate. The PC of the traveling employee and the PC of the branch employee can access the HQ server.

```
Administrator: C:\Windows\system32\cmd.exe
C:\Users\Administrator>ping 192.168.110.1
Pinging 192.168.110.1 with 32 bytes of data:
Reply from 192.168.110.1: bytes=32 time=2ms TTL=64

Ping statistics for 192.168.110.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 2ms, Maximum = 2ms, Average = 2ms
```

10.3.6 Solution to PPTP VPN Connection Failure

- (1) iPhones and other IOS devices do not support PPTP VPN. Please use L2TP VPN instead
- (2) Run the ping command to test the connectivity between the client and server. For details, see Section [12.11.1 Network Check](#). If the ping fails, check the network connection settings. Check whether the branch EG can ping to HQ EG. If the ping fails. Check the network connection between the two EGs.
Choose **One-Device > Gateway > Config > Diagnostics > Network Tools**. Then, you can start the ping operation. For details, see Section [12.11.1 Network Check](#).
- (3) Check whether the username and password used by the client are the same as those configured on the server.

- (4) Check whether the WAN port IP address of your HQ EG is a public network IP address. If not, please configure DMZ on your egress gateway.

10.4 OpenVPN

10.4.1 Overview

1. OpenVPN Overview

Due to security considerations or cross-NAT communication needs, private channels need to be established between enterprises or between individual and enterprise. OpenVPN is used to establish Layer 2 or Layer 3 VPN tunnels by using the vNIC. OpenVPN supports flexible client authorization modes, supports authentication through certificate or username and password, and allows users to connect to VPN virtual interfaces through the firewall. It is easier to use than other types of VPN technologies. OpenVPN can run in the Linux, xBSD, Mac OS X, and Windows 2000/XP systems. The device can establish VPN connections to PCs, Android/Apple mobile phones, routers, and Linux devices, and it is compatible with most OpenVPN products in the market.

OpenVPN connections can traverse most proxy servers and can function well in the NAT environment. The OpenVPN server can push the following network configuration to clients: IP address, routes, and DNS settings.

2. Certificate Overview

The major advantage of OpenVPN lies in its high security, but OpenVPN security requires the support of certificates.

The OpenVPN client supports certificates **ca.crt**, **ca.key**, **client.crt**, and **client.key** and the OpenVPN server supports certificates **ca.crt**, **ca.key**, **server.crt**, and **server.key**.

10.4.2 Configuring the OpenVPN Server

Choose **One-Device > Gateway > Config > VPN > OpenVPN**.

1. Basic Settings

Turn on **Enable** to enable the OpenVPN function, set **OpenVPN Type** to **Server**, set other parameters, and click **Save**. After the basic settings are completed, you can view the tunnel information of the server in the tunnel list.

Enable

OpenVPN Type Server Client

Server Mode

Protocol

* Server Address

* Port ID 1-65535

* IP Range

* Deliver Route +

Flow Control Disable Enable

[Advanced Settings](#)

Client Config

Table 10-19 OpenVPN server basic settings

| Parameter | Description |
|-------------|--|
| Server Mode | <p>Select a server authentication mode. The options are Account, Certificate, and Account & Certificate.</p> <ul style="list-style-type: none"> ● Account: Enter the correct username and password and upload the CA certificate on the client to connect to the server. The configuration is simple. ● Certificate: Upload the CA certificate and client certificate and enter the correct private key on the client to connect to the server. ● Account & Certificate: Upload the CA certificate and client certificate and enter the correct username, password, and private key. This mode is applicable to scenarios with high security requirements. |
| Protocol | <p>Select a protocol for all OpenVPN communications based on a single IP port. The options are UDP and TCP.</p> <p>The default value is UDP, which is recommended. When you select a protocol, pay attention to the network status between two encrypted tunnel ends. If high latency or heavy packet loss occurs, select TCP as the underlying protocol.</p> |

| Parameter | Description |
|----------------|---|
| Server Address | Specify the server address for client connection. You can set this parameter to a domain name. |
| Port ID | Specify the port used by the OpenVPN service process. Internet Assigned Numbers Authority (IANA) specifies port 1194 as the official port for the OpenVPN service. If the port is in use or disabled in the local network, the server log prompts port binding failure and you are asked to change the port number. |
| IP Range | Specify the network segment of the OpenVPN address pool. The first available in the address pool is allocated to the server, and the other addresses are allocated to clients. For example, if this parameter is set to 10.80.12.0/24, the VPN virtual address of the server is 10.80.12.1. |
| Deliver Route | Specify the VPN dial-up line for clients to access the LAN network segment of the server. The server informs clients that want to access the server LAN of the route information. You can configure a maximum of three routes. |
| Flow Control | The VPN server has a lower priority to control the traffic of the client than the custom policy. The VPN server can only limit the maximum uplink and downlink bandwidth per user for the client. For details, see Section 8.6.2 Intelligence QoS . |
| Client Config | <p>Click Export to export the parameter configuration of the client connected to the server in the .tar compressed package. The decompressed information is used for setting the OpenVPN client.</p> <p>In account mode, the compressed package contains the configuration file client.ovpn, CA certificate ca.crt, and CA private key ca.key.</p> <p>If certificate authentication is configured, the compressed package contains the configuration file client.ovpn, CA certificate ca.crt, CA private key ca.key, client certificate client.cart, and client private key client.key.</p> <p>If TLS authentication is enabled, the compressed package contains the TLS identity authentication key tls.key apart from the preceding files. For details on TLS authentication, see Advanced Settings.</p> |
| Server Log | Click Export to export server log files, including the server start time and client dial-up logs. |

 **Caution**

The IP address range of the device cannot overlap the network segment of the LAN port on the device.

2. Advanced Settings

Click **Advanced Settings** to configure the advanced parameters. Keep the default settings unless otherwise specified.

TLS Authentication ?

Allow Data Compression ?

Route All Traffic over VPN ?

Cipher ?

Deliver DNS ? +

Auth

Table 10-20 OpenVPN server advanced settings

| Parameter | Description |
|----------------------------|--|
| TLS Authentication | Specify the TLS key for enhanced OpenVPN security by allowing the communicating parties to possess the shared key before TLS handshake. After TLS authentication is enabled, you must import the TLS key on the client. (The version of the peer OpenVPN client must be higher than 2.40.) |
| Allow Data Compression | Specify whether to enable data compression. If this function is enabled, transmitted data is compressed using the LZO algorithm. Data compression saves bandwidth but consumes certain CPU resources. The setting on the client must be the same as that on the server. Otherwise, the connection fails. |
| Route All Traffic over VPN | Specify whether to route all traffic over VPN. After this function is enabled, all the traffic is routed over the VPN tunnel. This means that the VPN tunnel is the default route. |

| Parameter | Description |
|-------------|---|
| Cipher | Select the data encryption mode before data transmission to ensure that even data packets are intercepted during transmission, the leaked data cannot be interpreted. If this parameter is set to Auto on the server, you can set this parameter to any option on the client. If a specific encryption algorithm is configured on the server, you must select the same encryption algorithm on the client. Otherwise, the connection fails. |
| Deliver DNS | Specify the DNS server address pushed by the server to clients. Currently, the device can push the DNS server address to Windows clients only. |
| Auth | Specify the MD5 algorithm used by the server. The server will inform the clients of this information. The default value is SHA1. |

3. Configuring OpenVPN User

Choose **One-Device > Gateway > Config > VPN > VPN Account**.

Only user accounts added to the VPN client list are allowed to dial up to connect to the OpenVPN server. Therefore, you need to manually configure user accounts for clients to access the OpenVPN server.

Click **Add**. In the dialog box that appears, set **Service Type** to **OpenVpn**, enter the username and password, and click **OK**. The **Status** parameter specifies whether to enable the user account.

VPN User List Username/Password 🔍 + Add Delete All Delete Selected

| <input type="checkbox"/> | Username | Password 🔒 | Service Type ? | Network Mode ? | Client Subnet ? | Status | Action |
|--------------------------|----------|------------|----------------|------------------|------------------|--------|---|
| <input type="checkbox"/> | branch | ***** | L2TP | Router to Router | 192.168.120.0/24 | Enable | Edit Delete |
| <input type="checkbox"/> | pc@l2tp | ***** | L2TP | PC to Router | - | Enable | Edit Delete |

Add User ✕

Service Type ?

* Username

* Password

Status

10.4.3 Configuring the OpenVPN Client

Choose **One-Device > Gateway > Config > VPN > OpenVPN**.

Currently, you can configure the device as the OpenVPN client in either of the following methods:

Web Settings: Configure OpenVPN client on the web page. This method is used when the device is connected to a non-EG server.

Import Config: Manually import the configuration file. This method is used when the device is connected to a similar device. The client configuration file **client.ovpn** can be directly exported from the connected OpenVPN server.

Enable

OpenVPN Type Server Client

Client Config Import Config Web Settings

1. Import Config

Turn on **Enable** to enable the OpenVPN function, set **OpenVPN Type** to **Client** and **Client Config** to **Import Config**, select a server mode, set relevant parameters, and click **Browse** to import the client configuration file. Then, click **Save** to make the configuration take effect.

Enable

OpenVPN Type Server Client

Client Config Import Config Web Settings

Server Mode

* Username

* Password

Client Config It already exists.

Table 10-21 OpenVPN client configuration in Import Config method

| Parameter | Description |
|-------------------|--|
| Server Mode | <p>Select a server authentication mode. The options are Account, Certificate, Account & Certificate and Pre-Shared Key.</p> <ul style="list-style-type: none"> ● Account: Enter the correct username and password and upload the CA certificate on the client. The CA certificate information is embedded in the client configuration file. ● Certificate: Upload the CA certificate and client certificate and enter the correct private key on the client. All the information is embedded in the client configuration file. ● Account & Certificate: Enter the correct username, password, and private key and upload the CA certificate, and client certificate on the client. The information of the CA certificate, client certificate, and private key is embedded in the client configuration file. ● Static Key: Upload the pre-shared key file apart from the client configuration file. |
| Username/Password | Enter the username and password configured on the server. |
| Client Config | Click Browse , select the client configuration file exported from the server, and upload the file. |
| Pre-Shared Key | <p>This parameter is available only when Server Mode is set to Static Key.</p> <p>Click Browse, select the pre-shared key file, and upload the file.</p> |
| Working Mode | <p>This parameter is available only when Server Mode is set to Static Key.</p> <ul style="list-style-type: none"> ● NAT: The client can access the server network, but the server cannot access the client network. ● Router: The server can access the client network. |

2. Web Settings

Turn on **Enable** to enable the OpenVPN function, set **OpenVPN Type** to **Client** and **Client Config** to **Web Settings**, configure parameters such as **Device Mode** and **Device Mode**, and click **Save** to make the configuration take effect.

(1) Basic Settings

Enable

OpenVPN Type Server Client

Client Config Import Config Web Settings

Device Mode

Server Mode

* Username

* Password

Protocol

* Server Address

* Server Port ID 1-65535

----- Advanced Settings -----

CA Certificate

Table 10-22 OpenVPN client configuration in Web Settings method

| Parameter | Description |
|-------------|---|
| Device Mode | Specify the mode of the EG device that functions as a client. The options are TUN and TAP . The value must be the same as that configured on the server. When the EG device works as a server, it supports the TUN mode only. |

| Parameter | Description |
|------------------------|---|
| Server Mode | <p>Select a client authentication mode. The options are Account, Certificate, and Account & Certificate.</p> <ul style="list-style-type: none"> ● Account: Enter the correct username and password and upload the CA certificate on the client. ● Certificate: Upload the correct CA certificate, client certificate, and private key file on the client. ● Account & Certificate: Enter the correct username and password, and upload the CA certificate, client certificate, and private key file on the client. |
| Username/Password | Enter the username and password configured on the server. |
| Protocol | Select the protocol running on the device. The options are UDP and TCP. The value must be the same as that configured on the server. |
| Server Address | Enter the address or domain name of the server to be connected. |
| Server Port ID | Enter the port number of the server to be connected. |
| CA Certificate | Click Browse , select the CA certificate file with the file name extension .ca, and upload the file. |
| Client Key | Click Browse , select the client private file with the file name extension .key, and upload the file. |
| Client Certificate | Click Browse , select the client certificate file with the file name extension .crt, and upload the file. |
| Client Certificate Key | Specify the client certificate key if the client certificate provided by the server (such as the MikroTik server) is encrypted twice. |

(2) Advanced Settings

Click **Advanced Settings** to configure the advanced parameters. Keep the default settings unless otherwise specified.

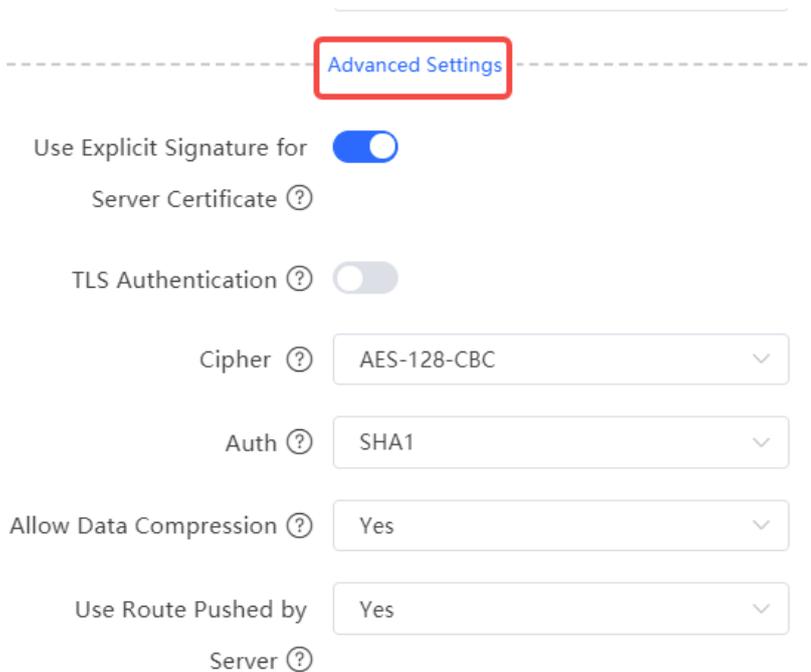


Table 10-23 OpenVPN client configuration in Web Settings method

| Parameter | Description |
|---|--|
| Use Explicit Signature for Server Certificate | Specify whether to verify the server certificate using explicit signature. By default, this function is enabled. If the server certificate does not use explicit signature, for example, the MikroTik server, you need to disable this function. Otherwise, the connection fails. |
| TLS Authentication | Specify whether to enable TLS authentication for the server. If this function is enabled, you need to upload the TLS certificate file. |
| Cipher | Select a data compression algorithm. The value must be the same as that configured on the server. Otherwise, the connection fails. |
| Auth | Select an MD5 algorithm for data packet verification. The options are SHA1 , MD5 , SHA256 , and NULL . The value must be the same as that configured on the server. Otherwise, the connection fails. |
| Allow Data Compression | Specify whether to allow data compression. After this function is enabled, the transmitted data can be compressed by using the LZO algorithm. The value must be the same as that configured on the server. |
| Use Route Pushed by Server | Specify whether to use the routes pushed by the server. If this function is disabled, the device cannot accept the routes pushed by the server. If the server needs to access LAN devices, you must set this parameter to Yes . |

10.4.4 Viewing the OpenVPN Tunnel Information

Choose **One-Device > Gateway > Config > VPN > OpenVPN > Tunnel List**.

After the server and client are configured, you can view the OpenVPN tunnel connection status. If the tunnel is established successfully, the client tunnel information is displayed in the tunnel list of the server.

| <input type="checkbox"/> | Username | Server/Client | Status | Real IP Address | Virtual IP Address |
|--------------------------|----------|---------------|--------|-----------------|--------------------|
| <input type="checkbox"/> | openvpn | Server | OK | 10.52.48.43 | 10.80.12.1 |

Total 1 < 1 > 10/page

Table 10-24 OpenVPN tunnel information

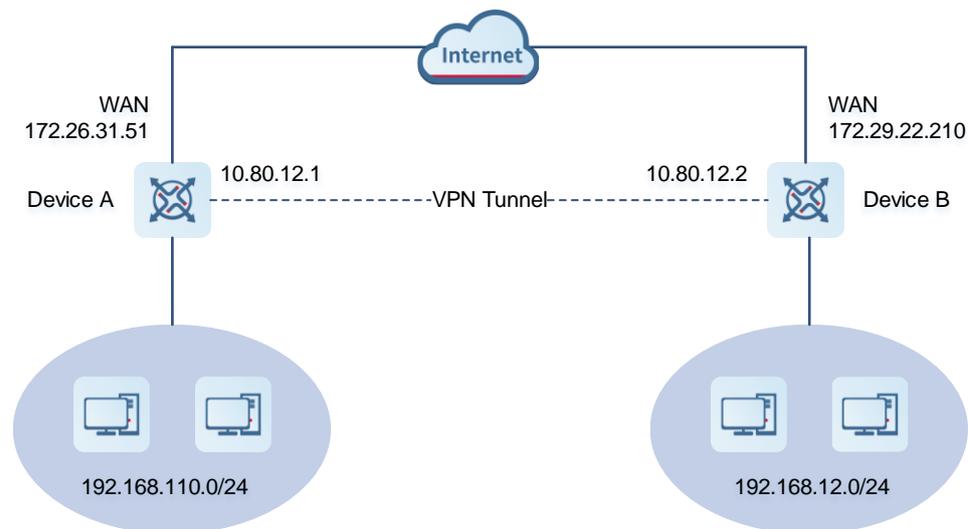
| Parameter | Description |
|--------------------|--|
| Username | Indicate the username used by the client for identity authentication. By default, the username displayed on the server is openvpn . |
| Server/Client | Indicate the role of the local end of the tunnel, which can be client or server. |
| Status | Indicate the tunnel establishment status. |
| Real IP Address | Indicate the real IP address used by the local end to connect to the VPN. |
| Virtual IP Address | Indicate the local virtual IP address of the tunnel. The virtual IP address of the OpenVPN client is allocated by the OpenVPN server. |

10.4.5 Typical Configuration Example

1. Networking Requirements

The enterprise wants to allow the client network to dial up to the server through OpenVPN, implementing mutual access between the server and client.

2. Networking Diagram



3. Configuration Roadmap

- Configure Device A as the OpenVPN server.
- Configure Device B as the OpenVPN client.
- The server needs to push the local LAN network segment to the client to allow the client to access the server in the LAN.

4. Configuration Steps

- Configure Device A.
 - (1) Log in to the web management system and choose **One-Device > Gateway > Config > VPN > OpenVPN > OpenVPN** to access the OpenVPN page.
 - (2) Turn on Enable to enable the OpenVPN function, set OpenVPN Type to Server, select a server mode and protocol, enter the port number (1194 by default) and server address (external IP address of the local device), and click Save.

Enable

OpenVPN Type Server Client

Server Mode

Protocol

* Server Address

* Port ID 1-65535

* IP Range

* Deliver Route +

Flow Control Disable Enable

[Advanced Settings](#)

Client Config

Table 10-25 OpenVPN server configuration

| Parameter | Description |
|----------------|---|
| Server Mode | Select an authentication mode. In this example, select Account . In scenarios with high security requirements, select Account & Certificate . |
| Protocol | Select UDP unless otherwise specified. When the network status between two encrypted tunnel ends is poor, such as high latency or heavy packet loss, select TCP . |
| Server Address | Enter the WAN port address of the server, which is 172.26.31.51 . |
| Port ID | The default value is 1194 . Keep the default value unless otherwise specified. If the port is in use or disabled in the current network, change to an available port number. |

| Parameter | Description |
|---------------|---|
| IP Range | Specify the network segment of the OpenVPN address pool. The first available in the address pool is allocated to the server, and the other addresses are allocated to clients. For example, if this parameter is set to 10.80.12.0/24 , the VPN virtual address of the server is 10.80.12.1. |
| Deliver Route | Add routes to the corresponding network segment if the client wants to the LAN network segment where the server resides. |

- (3) Click **Advanced settings** to configure more advanced parameters. If the device connects to other EG devices in the Reye network, you are advised to keep the default values for advanced settings. If the device connects to devices from another vendor, keep the parameter settings consistent on the connected devices.

TLS Authentication

Allow Data Compression

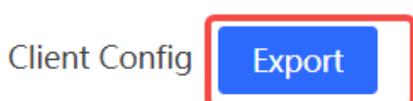
Route All Traffic over VPN

Cipher

Deliver DNS +

Auth

- (4) Click **Export** to export the compressed package of the client parameter configuration. Download the compressed package to the local device and decompress it for setting the OpenVPN client in subsequent steps.



- (5) Choose **One-Device > Gateway > Config > VPN > VPN Account** and add an OpenVPN user account.

×

Add User

Service Type ?

* Username

* Password ?

Status

- Configure Device B.
 - (1) Log in to the web management system and access the OpenVPN page.
 - (2) Turn on Enable to enable the OpenVPN function and set OpenVPN Type to Client. Two methods are available for configuring the client. The Import Config method is recommended.
 - **Import Config:**

Enable

OpenVPN Type Server Client

Client Config Import Config Web Settings

Server Mode

* Username ?

* Password ? ?

Client Config It already exists.

OpenVPN client configuration in Import Config method

| Parameter | Description |
|---------------|-------------------------------|
| Client Config | Select Import Config . |

| Parameter | Description |
|---------------------|---|
| Server Mode | The value must be the same as that on the server. In this example, select Account . |
| Username & Password | Enter the username and password configured on the server. |
| Client Config | Click Browse , select the client configuration file exported from the server, and upload the file. |

o **Web Settings:**

Enable

OpenVPN Type Server Client

Client Config Import Config Web Settings

Device Mode

Server Mode

* Username

* Password

Protocol

* Server Address

* Server Port ID 1-65535

----- Advanced Settings -----

CA Certificate

OpenVPN client configuration in Web Settings method

| Parameter | Description |
|---------------|--|
| Client Config | Select Web Settings . |
| Device Mode | The value must be the same as that on the server. In this example, select TUN . |

| Parameter | Description |
|---------------------|--|
| Server Mode | The value must be the same as that on the server. In this example, select Account . |
| Username & Password | Enter the username and password configured on the server. |
| Protocol | The value must be the same as that on the server. In this example, select UDP . |
| Server Address | Enter the public network IP address of the server, which is 172.26.31.51 . |
| Server Port ID | Enter the port number used by the server, such as 1194 . |

Import the corresponding files according to the value of **Server Mode**.

If **Server Mode** is set to **Certificate** or **Account & Certificate**, you need to import the CA certificate file, client certificate file, and client private key file. If **Server Mode** is set to **Account**, you only need to import the CA certificate file. If the client certificate is encrypted, you also need to enter the pre-shared key specified by **Client Certificate Key**.

| | | |
|------------------------|------------------------------------|---|
| CA Certificate | <input type="text" value=".cert"/> | <input type="button" value="Browse"/> |
| Client Key | <input type="text" value=".key"/> | <input type="button" value="Browse"/> |
| Client Certificate | <input type="text" value=".cert"/> | <input type="button" value="Browse"/> |
| Client Certificate Key | <input type="text"/> | <input style="border: none; background-color: #ccc; padding: 2px 5px; font-size: 12px; border-radius: 3px; vertical-align: middle;" type="button" value="?"/> |

Click **Advanced Settings** to configure more parameters. Configure **Use Route Pushed by Server** to specify whether to accept routes pushed by the server. The value must be the same as that on the server. If the client is connected to a non-EG device, such as MikroTik server outside China, you need to turn off **Use Explicit Signature for Server Certificate**.

Advanced Settings

Use Explicit Signature for Server Certificate

TLS Authentication

Cipher

Auth

Allow Data Compression

Use Route Pushed by Server

CA Certificate

(3) After the configuration is completed, click Save to make the configuration take effect.

5. Verifying Configuration

After the server and client are configured, view the two tunnel end information in the tunnel list.

- Client:

| Username | Server/Client | Status | Real IP Address | Virtual IP Address |
|--------------|---------------|---------------|-----------------|--------------------|
| OpenVpnUser1 | Client | Connecting... | 10.52.48.43 | |

Total 1 < 1 >

- Server:

| Username | Server/Client | Status | Real IP Address | Virtual IP Address |
|----------|---------------|--------|-----------------|--------------------|
| openvpn | Server | OK | 10.52.48.43 | 10.80.12.1 |

Total 1 < 1 >

10.5 Configuring WireGuard VPN

10.5.1 Overview

1. WireGuard VPN Overview

Conventional VPN protocols such as OpenVPN and IPsec have certain limitations, such as slow connection speed due to the complexity of the encryption and encapsulation processes. This is where WireGuard VPN comes in. It is a new OpenVPN protocol and is widely recognized for its high efficiency, security, and ease of use. WireGuard operates at Layer 3 of the Open System Interconnection (OSI) model and supports IPv4 and IPv6. Simplified design and encryption technologies of WireGuard minimize system overhead, delivering high-speed connections and resulting in lower latency.

WireGuard follows the principles of simplicity and uses modern encryption technologies. Its working principle is as follows:

- (1) **Key exchange and handshake:** When a client initiates a connection request to the remote server, key exchange is performed. Public and private key pairs are generated for each of the client and server, which exchange public keys to establish a secure communication channel.
- (2) **Tunnel creation:** WireGuard creates a virtual network interface on each of the client and server and establishes an encrypted tunnel to transmit data packets.
- (3) **Data packet transmission:** The sender uses the public key of the receiver to encrypt data packets.
- (4) **Decryption:** After receiving encrypted data packets, the receiver uses its own private key to decrypt the data packets.

2. Applicable Scenarios

WireGuard VPN on the Ruijie Reyee RG-EG-W series gateways supports client and server configurations and displays the tunnel link after a successful connection. WireGuard VPN is applicable to the following scenarios:

- End-to-end VPN: connects two or more network nodes to enable communication, data sharing, and resource access between networks. In this scenario, an RG-EG-W gateway can function as the server or client of WireGuard VPN and interconnect with another RG-EG-W gateway or a third-party device.
- Mobile access VPN: allows mobile users to securely access specified network resources from anywhere. In this scenario, the RG-EG-W gateway can serve as the WireGuard VPN server, and mobile devices connect to the VPN through the configuration of the WireGuard VPN client.

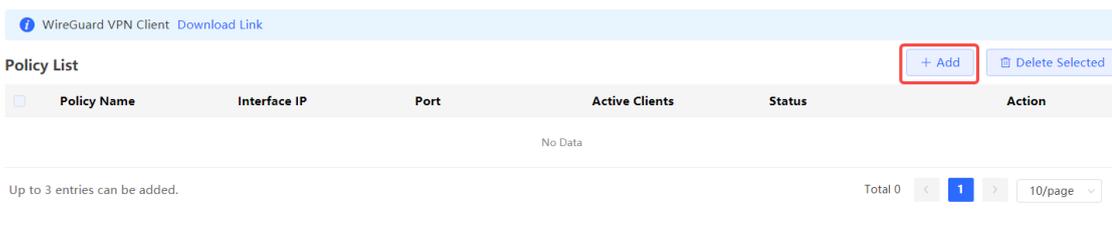
10.5.2 Configuring a WireGuard VPN Server

 **Caution**

- A WireGuard VPN server must have a public IP address. Otherwise, a VPN tunnel cannot be established.
 - Intranet access supports only IPv4.
-

Choose **One-Device > Gateway > Config > VPN > WireGuard VPN > WireGuard VPN Server**.

- (1) Click **Add** on the right of **Policy List**.



(2) Set **Policy Name** and toggle on **Status**.

* Policy Name

Status

(3) Set related parameters of the server.

Local Configuration

* Server IP

* Port

* Public Key

* Private Key

* Interface IP

* DNS Server

Table 10-26 Local Configuration Parameters of a WireGuard VPN Server

| Parameter | Description |
|-----------|--|
| Server IP | Specify a public IP address or a domain name of a VPN server to establish a connection with a VPN client. |
| Port | Specify the port number on which a VPN server listens. The port number is used to receive connection requests from a VPN client. WireGuard uses UDP by default and the default port number is 51820. |

| Parameter | Description |
|--------------|--|
| Public Key | <p>Specify the public key of a server. The public key is used to encrypt data packets transmitted in a VPN tunnel. During the exchange of WireGuard keys, the public key of a server will be sent to a client so that the client can securely send information to the server. The public and private keys are automatically generated by the system. You can click the copy icon to copy the public key of the server, and click the refresh icon to generate a new public and private key pair.</p> <p>* Public Key <input type="text" value="q' ivoz"/>  </p> <p>* Private Key <input "="" type="text" value="C ZvmA="/></p> |
| Private Key | Specify the private key of a server. The private key is used to decrypt encrypted information received from a client and encrypt information to be sent to the client. |
| Interface IP | Specify the IP address of a tunnel interface on a server, which is used to identify the server connected to a VPN tunnel. A client will communicate with the server with this IP address. |
| DNS Server | Specify the DNS server for resolving a domain name when Server IP is set to the domain name. |

(4) In the **Client** area, click **Add** to add a client.

Client  

| <input type="checkbox"/> | Username | Interface IP | Action |
|--------------------------|----------|--------------|--------|
| No Data | | | |

Cancel OK

×

* Username

* Interface IP

* Public Key

Accessible IP Range Interface IP only Custom



Pre-Shared Key

Download Config File

File



To connect to the client automatically, download the VPN configuration file and upload it to the client for VPN setup.



Multiple WireGuard clients should not share the same VPN configuration file.



Click **OK** to save the configuration. A prompt is displayed. After a client is added, the **Download Config File** function is unavailable.

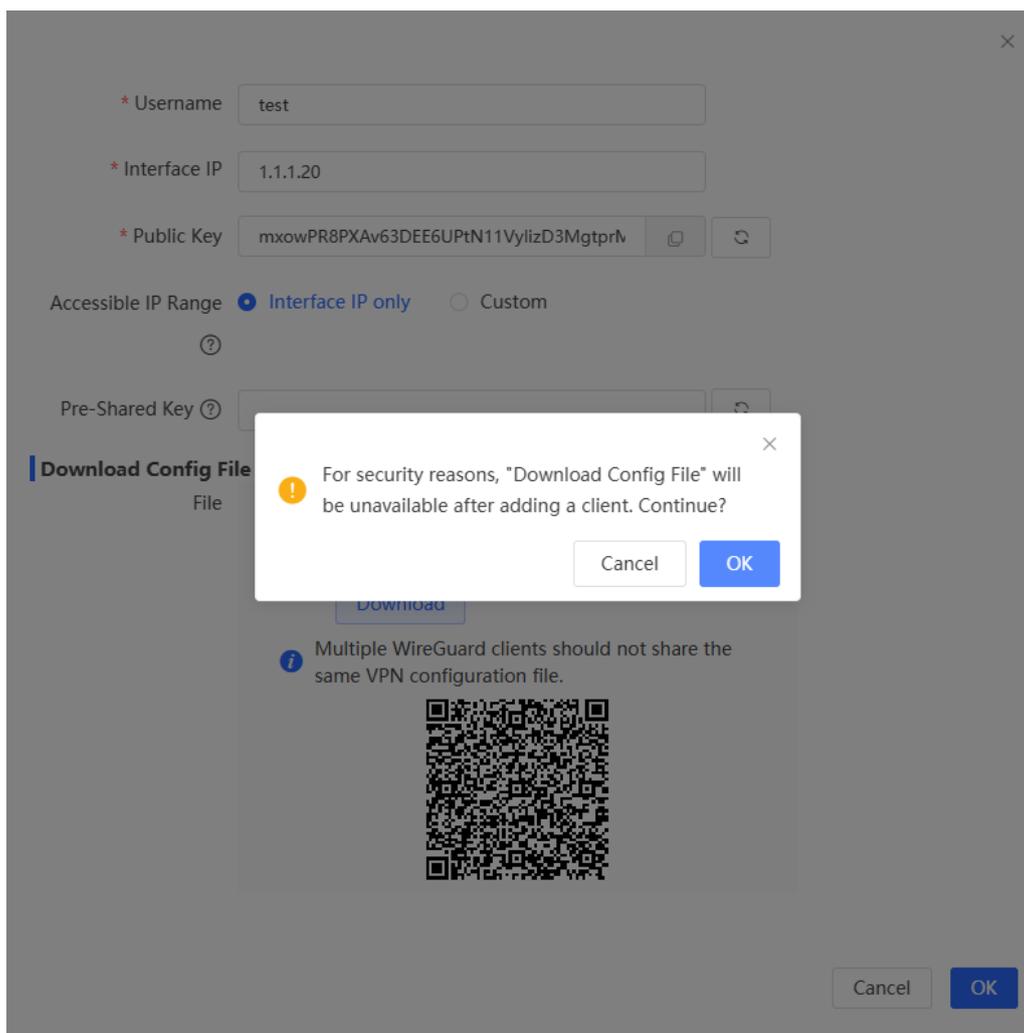


Table 10-27 Parameters of Adding a Client on a WireGuard VPN Server

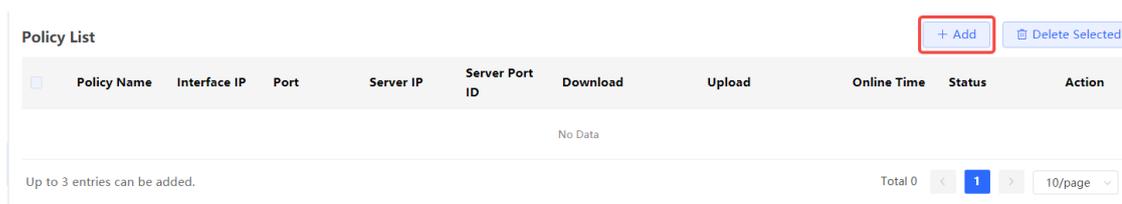
| Parameter | Description |
|---------------------|--|
| Username | Specify the client identifier, which is used to identify a client during the authentication. A username is typically unique to identify a client. |
| Interface IP | Specify the IP address of a tunnel interface on a client. The IP address is used to identify the client connected to a VPN tunnel. |
| Public Key | Specify the public key of a client, which is used to encrypt data packets transmitted in a VPN tunnel. |
| Accessible IP Range | Specify the client IP address range that is allowed to access a server. Interface IP only: Access is allowed only through the interface IP address, that is, only the client with the interface IP address can access the server. Custom: You can add the intranet addresses of the clients so that they can also access the server. |

| Parameter | Description |
|----------------------|---|
| Pre-Shared Key | Specify a pre-shared key, which improves link security. The keys on the client and server must be consistent. |
| Download Config File | <p>Click Download to download the configuration file. After the configuration file is uploaded to the clients, the configuration is automatically complete.</p> <p>After the configuration is complete on the clients, the QR code is displayed. The content of the QR code is the same as that of the exported configuration file, which facilitates the configuration of mobile clients by scanning the QR code.</p> <p>Multiple WireGuard clients should not share the same VPN configuration file.</p> |

10.5.3 Configuring a WireGuard VPN Client

Choose **One-Device > Gateway > Config > VPN > WireGuard VPN > WireGuard VPN Client**.

(1) Click **Add** on the right of **Policy List**.



(2) Set **Policy Name** and toggle on **Status**.

* Policy Name

Status

(3) Set **Configuration Mode**.

- Manual: Manually enter the configuration parameters related to the client and server.

Configuration Mode Manual File

- File: Click **Select**, select the configuration file downloaded from the server, and complete the configuration automatically.

Configuration Mode Manual File

(4) Configure the client parameters.

| Parameter | Description |
|---------------------|--|
| Bound Interface | In the scenario of multiple WAN ports, you can configure this parameter to specify the outbound interface of VPN traffic. You are advised to set this parameter to Auto . |
| DNS Server | Specify the DNS server for resolving a domain name when Server IP is set to the domain name. |
| Accessible IP Range | Specify the IP address range of a server to be accessed by a client. <ul style="list-style-type: none"> ● All: Force the client-generated IPv4 traffic to be routed through the VPN tunnel. ● Custom: You can add the intranet address of the server so that data is transmitted through a VPN tunnel only when the client accesses the corresponding network segment. |

(5) Set related parameters of the server.

Server Config

* Server IP 

* Port

* Public Key 

Table 10-29 Server Config Parameters on a WireGuard VPN Client

| Parameter | Description |
|------------|--|
| Server IP | Specify a public IP address or a domain name of a VPN server to establish a connection with a VPN client. |
| Port | Specify the port number on which a VPN server listens. The port number is used to receive connection requests from a VPN client. The value must be the same as that on the server. |
| Public Key | Specify the public key of a server. The public key is used to encrypt data packets transmitted in a VPN tunnel. The value must be the same as that on the server. |

(6) (Optional) Click **Advanced Settings** to set advanced parameters.

----- Advanced Settings -----

Pre-Shared Key (?) ↻

* Heartbeat Interval s (?)

Table 10-30 Advanced Settings Parameters on a WireGuard VPN Client

| Parameter | Description |
|--------------------|--|
| Pre-Shared Key | Specify the key shared by both communication parties for authentication and encrypted communication in advance. The key is used to enhance the security of the handshake process. The value must be the same as that configured on the server. |
| Heartbeat Interval | Specify the interval at which a client sends heartbeat packets to a server, which is used to detect the connection liveliness. If the server does not receive any heartbeat signal from the client within the specified interval, the connection is considered to be disconnected and is closed. |

(7) Click **OK**.

10.5.4 Checking the Status of a WireGuard VPN Connection

1. Checking the Server Connection Status

Choose **One-Device > Gateway > Config > VPN > WireGuard VPN > WireGuard VPN Server**.

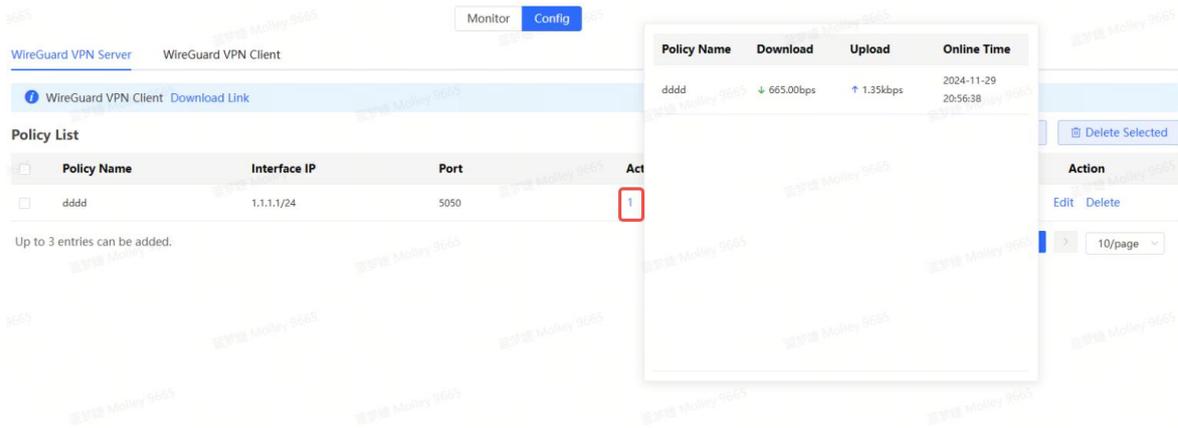
WireGuard VPN Client [Download Link](#)

Policy List + Add Delete Selected

| Policy Name | Interface IP | Port | Active Clients | Status | Action |
|-------------|--------------|------|----------------|--------|--------|
| No Data | | | | | |

Up to 3 entries can be added. Total 0 < 1 > 10/page

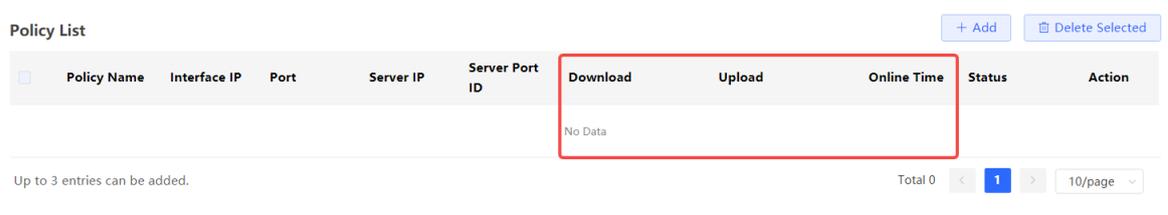
Active Clients indicates the number of clients that have successfully connected to the server. Click the number in the **Active Clients** column to display the real-time upload and download rates of a client. **Online Time** indicates the last time of a successful handshake between the server and client.



2. Checking the Client Connection Status

Choose **One-Device > Gateway > Config > VPN > WireGuard VPN > WireGuard VPN Client**.

If a client successfully connects to a server, upload and download rates as well as the onboarding time are displayed in the policy list.



11 SD-WAN

✔ Specification

- This feature is only supported on RG-105GW(T) and RG-EG105GW-X running ReyeeOS 2.300 or later version.
 - This feature can only be configured in Ruijie Cloud.
-

Small and medium-sized chain businesses usually require service interconnectivity between their headquarters and branch offices for purposes such as supervision, information tracking, and video conferencing. These services demand high real-time performance and reliability. Moreover, pre-configuration and batch configuration features are often necessary during project deployment, in order to improve network deployment efficiency. Ruijie Cloud's SD-WAN solution can effectively meet the above requirements and has the following advantages compared with traditional WAN solutions:

- (1) **Networking without public IP addresses:** Networking without public IP addresses enables remote connectivity across any broadband connection. For details, see <https://cloud.ruijienetworks.com/help/#/ArticleList?id=017d4b240fbc443c9b383d63c35c5aac>.
- (2) **Visualized monitoring:** Map-based network monitoring provides a clear, intuitive overview of the entire network, projects, and links, with one-click alarm analysis. For details, see <https://cloud.ruijienetworks.com/help/#/ArticleList?id=d48a89fb844a4795bf0f3967245597fd>.
- (3) **Batch configuration:** A template can be applied across multiple projects, eliminating the need for repetitive operations. For details, see <https://cloud.ruijienetworks.com/help/#/ArticleList?id=586ede226ec04f0f9fe32ce1fdb34f56>.
- (4) **Pre-configuration deployment:** Templates can be created beforehand, which are automatically delivered to devices upon network connection, facilitating zero-touch provisioning onsite. For details, see <https://cloud.ruijienetworks.com/help/#/ArticleList?id=6436c96a5cf94b9c97b92f863ff8bf06>.

12 System Management

12.1 System Logs

 **Specification**

This feature is only supported on RG-EG105GW-X running ReyeeOS 2.320 or later version.

For medium to large-scale network projects, network administrators often use third-party software to interface with all devices, monitoring system metrics and identifying any abnormal behavior to ensure system health and security. Devices usually support network management protocols such as SNMP and Syslog for seamless integration.

12.1.1 Viewing System Logs

Go to the configuration page.

- In SON mode:
 - Choose **Network-Wide** > **System** > **Syslog**.
 - Choose **One-Device** > **Config** > **System** > **Syslog**.
- In standalone mode: Choose **System** > **Syslog**.

The **Log List** displays the operation logs of the local device. You can filter the logs by specific dates or modules on the **View Log** page. You can also export the log list and log files to your local system for storage, viewing, or backup.

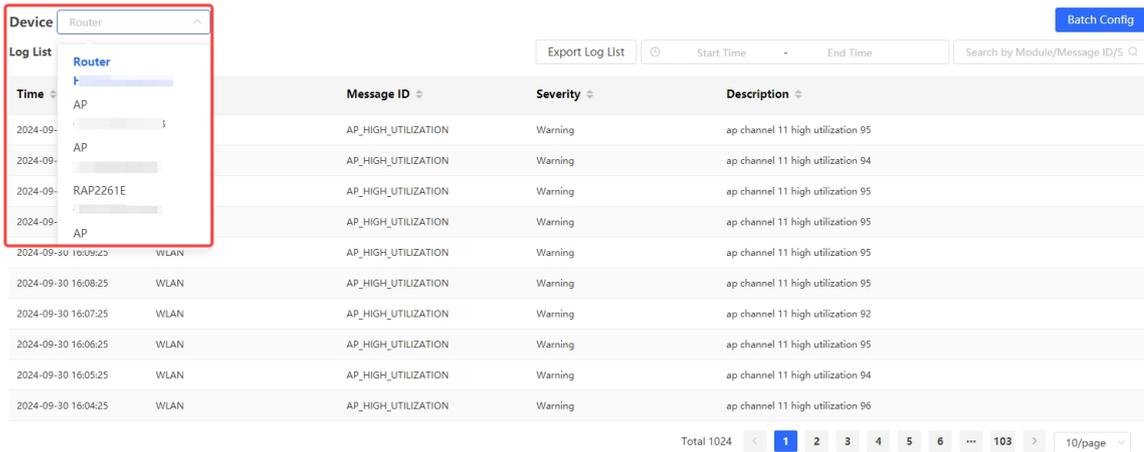
Device [Batch Config](#)

Log List [Export Log List](#) -

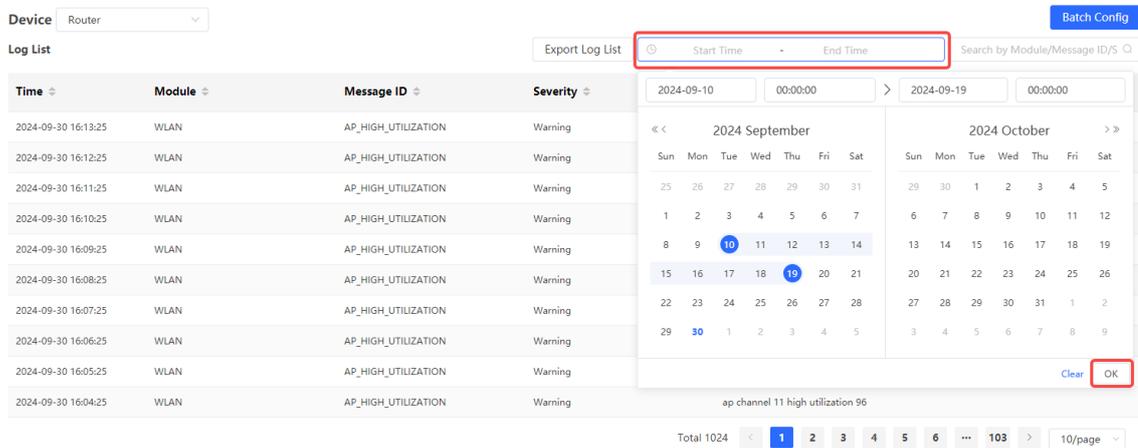
| Time | Module | Message ID | Severity | Description |
|---------------------|--------|---------------------|----------|-----------------------------------|
| 2024-09-30 16:13:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 95 |
| 2024-09-30 16:12:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 94 |
| 2024-09-30 16:11:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 95 |
| 2024-09-30 16:10:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 95 |
| 2024-09-30 16:09:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 95 |
| 2024-09-30 16:08:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 95 |
| 2024-09-30 16:07:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 92 |
| 2024-09-30 16:06:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 95 |
| 2024-09-30 16:05:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 94 |
| 2024-09-30 16:04:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 96 |

Total 1024 1 2 3 4 5 6 ... 103 10/page

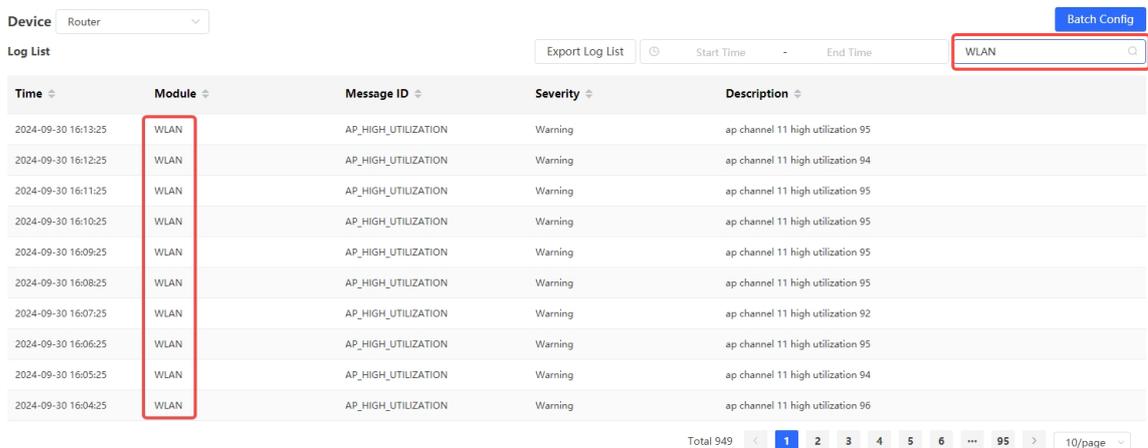
- On the **Syslog** page in Network-Wide mode, you can view the logs of specific devices.



- To view logs for a specific date, click **Start Time**, select the start and end time, and then click **OK** to filter the logs accordingly.



- To view the logs of a specific module, enter the module name in the search box to access its operation logs.



- To download the log files, click **Download Local Log File** to save the compressed log file to your local device for storage and backup. To export the log list, click **Export Log List** to download the log list in .csv format for

viewing on your computer.

- o Syslog page in Network-Wide mode.

✔ Specification

Only **Export Log list** is supported on the syslog page in Network-Wide mode, but **Download Local Log File** is not supported. To download the log file, click **One-Device > Config > System > Syslog** to access the device configuration page.

Device: Router

Log List

Export Log List

| Time | Module | Message ID | Severity | Description |
|---------------------|--------|---------------------|----------|-----------------------------------|
| 2024-09-30 16:13:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 95 |
| 2024-09-30 16:12:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 94 |
| 2024-09-30 16:11:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 95 |
| 2024-09-30 16:10:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 95 |
| 2024-09-30 16:09:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 95 |
| 2024-09-30 16:08:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 95 |
| 2024-09-30 16:07:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 92 |
| 2024-09-30 16:06:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 95 |
| 2024-09-30 16:05:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 94 |
| 2024-09-30 16:04:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 96 |

Total 1024

- o Syslog page in Standalone mode.

View Log Log Settings

Log List

Download Local Log File

Export Log List

| Time | Module | Message ID | Severity | Description |
|---------------------|--------|---------------------|----------|-----------------------------------|
| 2024-09-30 16:21:26 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 96 |
| 2024-09-30 16:20:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 93 |
| 2024-09-30 16:19:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 94 |
| 2024-09-30 16:18:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 94 |
| 2024-09-30 16:17:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 95 |
| 2024-09-30 16:16:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 95 |
| 2024-09-30 16:15:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 94 |
| 2024-09-30 16:14:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 94 |
| 2024-09-30 16:13:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 95 |
| 2024-09-30 16:12:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 94 |

Total 1024

12.1.2 Configuring System Logs

Go to the configuration page.

- In SON mode:
 - o Choose **Network-Wide > System > Syslog**. Click **Batch Config**.

Device: Router Batch Config

Log List Export Log List Start Time End Time Search by Module/Message ID/S

| Time | Module | Message ID | Severity | Description |
|---------------------|--------|---------------------|----------|-----------------------------------|
| 2024-09-30 16:28:26 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 93 |
| 2024-09-30 16:27:26 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 92 |
| 2024-09-30 16:26:26 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 91 |
| 2024-09-30 16:25:26 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 95 |
| 2024-09-30 16:24:26 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 93 |
| 2024-09-30 16:23:26 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 93 |
| 2024-09-30 16:22:26 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 93 |
| 2024-09-30 16:21:26 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 96 |
| 2024-09-30 16:20:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 93 |
| 2024-09-30 16:19:25 | WLAN | AP_HIGH_UTILIZATION | Warning | ap channel 11 high utilization 94 |

Total 1024 1 2 3 4 5 6 ... 103 10/page

o Choose **One-Device > Config > System > Syslog**. Click **Log Settings**.

View Log [Log Settings](#)

SYSLOG

Save Log Local device Enable
Filter Rule default [Edit](#)

Remote log server Up to 4 entries can be added. Add

| Enable | Protocol | IP/Domain | Port | Rate Limiting | Log Format | Filter Rule | Action |
|---------|----------|-----------|------|---------------|------------|-------------|--------|
| No Data | | | | | | | |

[Save](#)

● In standalone mode, choose **System > Syslog**. Click **Log Settings**.

1. Enabling Syslog

Toggle on **SYSLOG** to enable the SYSLOG protocol. When enabled, the device can connect with a remote log server to send log information over the network.

SYSLOG

Save Log Local device Enable
Filter Rule default [Edit](#)

Remote log server Up to 4 entries can be added. Add

| Enable | Protocol | IP/Domain | Port | Rate Limiting | Log Format | Filter Rule | Action |
|---------|----------|-----------|------|---------------|------------|-------------|--------|
| No Data | | | | | | | |

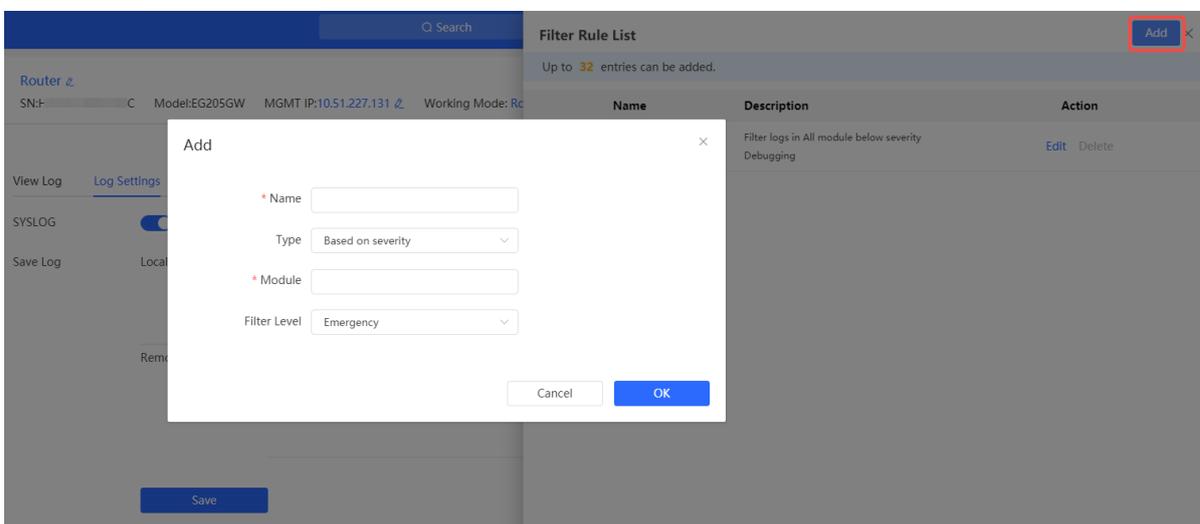
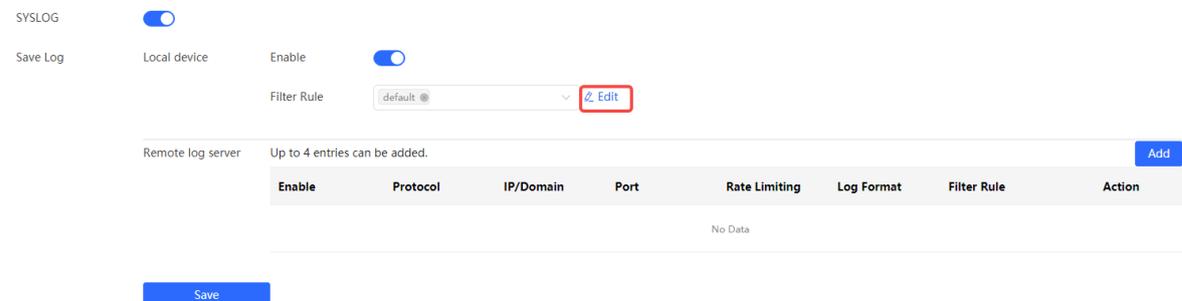
[Save](#)

2. Configuring Local Logs

Local log saving is enabled by default. Click **Edit**, and then **Add** to create filtering rules for device operation logs, allowing you to exclude certain operation logs (like debug messages from all modules) from being displayed in the log list.

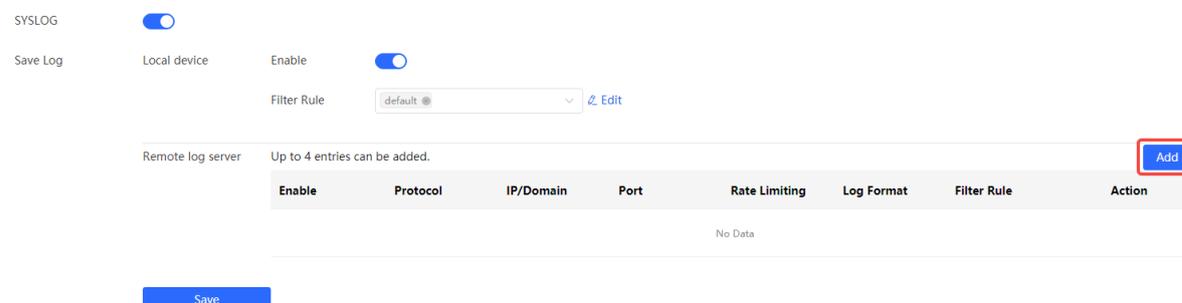
Caution

When local log saving is disabled, all actions performed on the device will no longer be displayed in the log list. Please exercise caution.



3. Configuring Remote Log Server

Click **Add** next to the **Remote log server** to add basic information of the remote log server.



Add
×

Enable

* IP/Domain IPv4

* Port

Protocol UDP

Rate Limiting No Limit by Default

* Log Format ? RFC3164 RFC5424

Filter Rule default

[Edit](#)

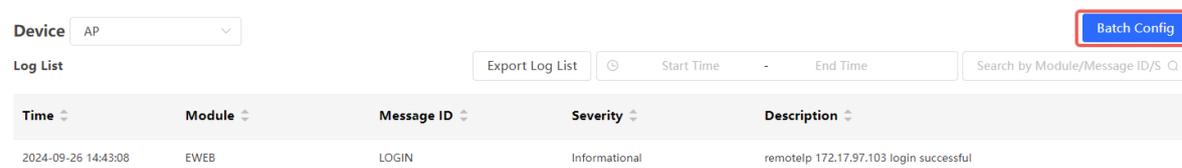
Table 12-1 Remote Log Server Configuration Parameters

| Parameter | Description | Default Value |
|---------------|---|---------------|
| Enable | Enable or disable the remote log server. When enabled, the device will send its operation logs to the remote log server. | Enabled |
| IP/Domain | IP address or domain name of the remote log server. The IP address can be an IPv4 or IPv6 address. | N/A |
| Port | Port number of the remote log server. | 514 |
| Protocol | Protocol for communication between the device and the remote log server. Currently only UDP is supported. | UDP |
| Rate Limiting | The highest rate at which the device can send log data to the remote log server. | No limit |
| Log Format | The format of logs sent to the remote log server. RFC3164: <Priority> second-level local time Hostname Module Name % Message Identifier: Log Message. RFC5424: <Priority> microsecond-level UTC time Hostname Module % Process ID Message Identifier - Log Message. | RFC3164 |
| Filter Rule | Rules for filtering device operation logs. Any logs that are filtered out will not be sent to the remote log server. | default |

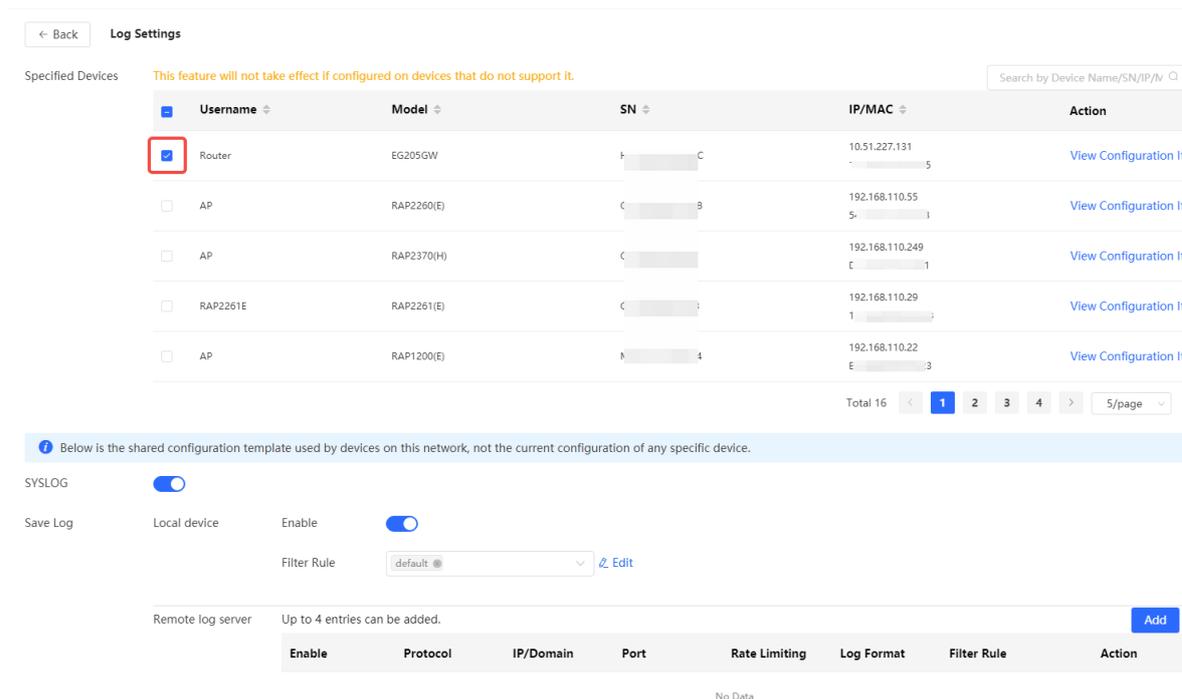
4. Batch Configuration

Go to the configuration page.

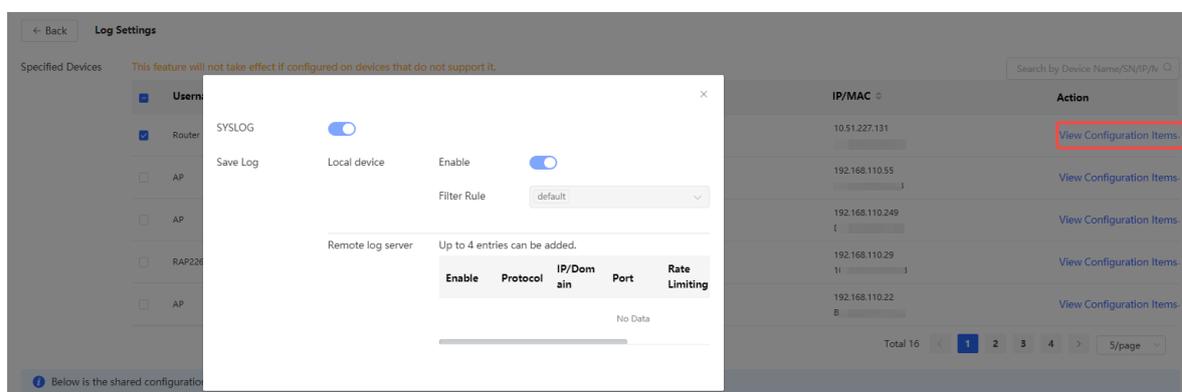
Choose **Network-Wide > System > Syslog**. Click **Batch Config**.



On the **Log Settings** page in Network-Wide mode, select the targeted devices and configure the log settings. Then, click **Save** to apply the settings to the selected devices.



After the log settings are successfully applied, click **View Configuration** to view the log settings of individual devices.



12.2 Setting the Login Password

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

Enter the old password and new password. After saving the configuration, log in again using the new password.

 **Caution**

In the self-organizing network mode, the login password of all devices in the network will be changed synchronously.

 Change the login password. Please log in again with the new password later.

* **Old Management Password**

* **New Management 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 Password**

Password Hint

12.3 Setting the Session Timeout Duration

Choose **One-Device > Gateway > Config > System > Login > Session Timeout**.

If no operation is performed on the Web page within a period of time, the session is automatically disconnected. When you need to perform operations again, enter the password to log in again. The default timeout duration is 3600 seconds, that is, 1 hour.

* Session Timeout  seconds

Save

12.4 Restoring Factory Settings

12.4.1 Restoring the Current Device to Factory Settings

Choose **One-Device** > **Gateway** > **Config** > **System** > **Backup** > **Reset**.

Click **Reset** to restore the current device to the factory settings.

 You can reset the device to factory settings by clicking the Factory Reset button below. If you want to retain the current configuration while performing a factory reset, then [back up the profile](#) the configuration file prior to the reset. 

Reset

Tips



Resetting the device will clear the current settings and reboot the device. Do you want to continue?

Cancel

OK

Caution

The operation will clear all configuration of the current device. If you want to retain the current configuration, back up the configuration first. (For details, see Section [12.9 Configuring Backup and Import](#).) Therefore, exercise caution when performing this operation.

12.4.2 Restoring All Devices to Factory Settings

Choose **Network-Wide** > **System** > **Reset**.

Click **All Devices**, select whether to enable **Unbind Account**, and click **Reset All Devices**. All devices in the network will be restored to factory settings.

 You can reset the device to factory settings by clicking the Factory Reset button below. If you want to retain the current configuration while performing a factory reset, then [back up the profile](#) the configuration file prior to the reset. 

Select master device All Devices

Retain bound Selecting this checkbox will allow the cloud account to maintain its project management privileges without requiring you to rebind your account.
account

Reset All Devices

 **Caution**

The operation will clear all configuration of all devices in the network. Therefore, exercise caution when performing this operation.

12.5 Configuring SNMP

 **Note**

This feature is only supported on RG-EG105GW-X and RG-EG105GW(T).

12.5.1 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.

12.5.2 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.

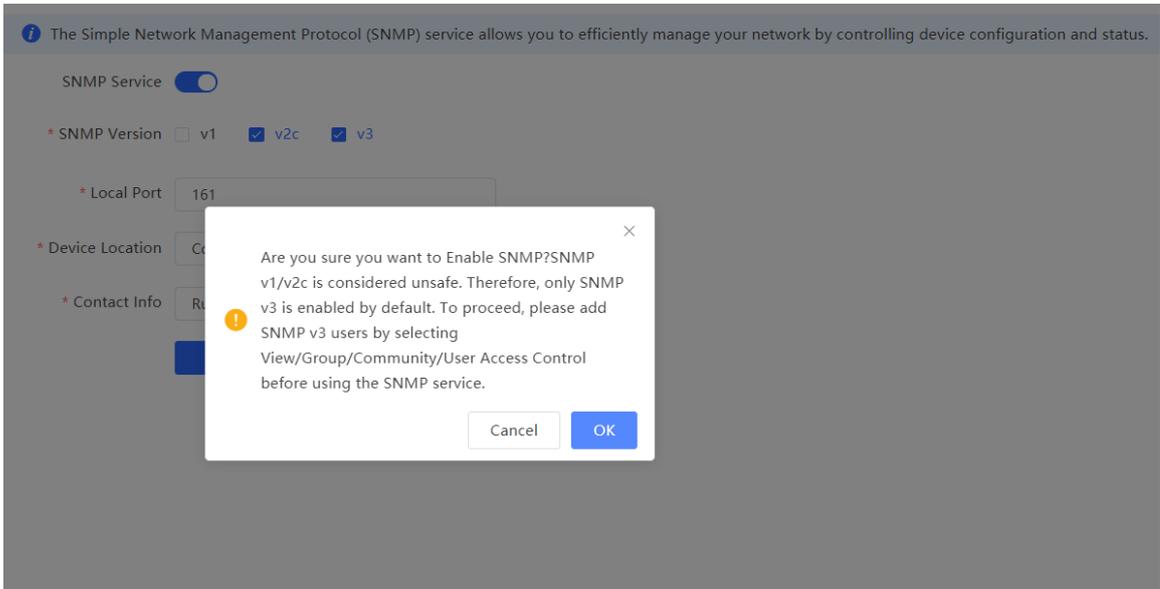
SNMP v2c: As an improved version of SNMP v1, SNMP v2c supports richer functions and more complex data types, with enhanced security. SNMP v2c performs better than SNMP v1 in terms of security and functionality, and is more flexible. It can be configured according to different needs.

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 **Network-Wide > Workspace > Network-Wide > SNMP > Global Config**

(1) Enable the SNMP service.



When it is enabled for the first time, SNMP v3 is enabled by default. Click **OK**.

(2) Set SNMP service global configuration parameters.

SNMP Service

* SNMP Version v1 v2c v3

* Local Port

* Device Location

* Contact Info

Table 12-2 Global Configuration Parameters

| Parameter | Description |
|-------------|--|
| SNMP Server | Indicates whether SNMP service is enabled. |

| Parameter | Description |
|-----------------|---|
| 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) After the SNMP service is enabled, click **Save** to make basic configurations such as the SNMP protocol version number take effect.

12.5.3 View/Group/Community/User Access Control

1. Configuring Views

- Overview

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 **Network-Wide > Workspace > Network-Wide > 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.

×

Add

* View Name

OID

Add Included Rule
Add Excluded Rule

Rule/OID List
Delete Selected

Up to **100** entries are allowed.

| | Rule | OID | Action |
|---------|------|-----|--------|
| No Data | | | |

Total 0

<
1
>

Go to page

Cancel
OK

Table 12-3 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. ● Excluded rules allow access to all OIDs except those in the OID range. Click Add Excluded Rule to configure this type of view. |

⚠ Note

A least one OID rule must be configured for a view. Otherwise, an alarm message will appear.

(3) Click **OK**.

2. Configuring v1/v2c Users

- Overview

When the SNMP version is set to v1/v2c, user configuration is required.

SNMP Service

* SNMP Version v1 v2c v3

* Local Port

* Device Location

* Contact Info

 **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 **Network-Wide > Workspace > Network-Wide > SNMP > View/Group/Community/Client Access Control**

(1) Click **Add** in the **SNMP v1/v2c Community Name List** pane.

SNMP v1/v2c Community Name List

| <input type="checkbox"/> | Community Name | Access Mode | MIB View | Action |
|--------------------------|----------------|-------------|----------|---|
| <input type="checkbox"/> | snmp_v2c_group | Read-Only | all | Edit Delete |

Up to 20 entries can be added.

Total 1

(2) Add a v1/v2c user.

Add
×

* Community Name

* Access Mode Read-Only ▼

* MIB View all ▼ [Add View +](#)

Cancel
OK

Table 12-4 v1/v2c User Configuration Parameters

| Parameter | Description |
|----------------|---|
| Community Name | <ul style="list-style-type: none"> ● 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.

SNMP Service

* SNMP Version v1 v2c v3

* Local Port

* Device Location

* Contact Info

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 **Network-Wide > Workspace > Network-Wide > SNMP > View/Group/Community/Client Access Control**.

(1) Click **Add** in the **SNMP v3 Group List** pane to create a group.

SNMP v3 Group List

| <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 |

Up to 20 entries can be added. Total 1

(2) Configure v3 group parameters.

Add
×

* Group Name

* Security Level Allowlist & Security ▼

* Read-Only View all ▼ [Add View +](#)

* Read & Write View all ▼ [Add View +](#)

* Notification View none ▼ [Add View +](#)

Cancel
OK

Table 12-5 v3 Group Configuration Parameters

| Parameter | Description |
|-------------------|---|
| Group Name | Indicates the name of the group. <ul style="list-style-type: none"> ● 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.

SNMP Service

* SNMP Version v1 v2c v3

* Local Port

* Device Location

* Contact Info

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 **Network-Wide > Workspace > Network-Wide > SNMP > View/Group/Community/Client Access Control**

(1) Click **Add** in the **SNMP v3 Client List** pane to add a v3 user.

SNMP v3 Client List

| <input type="checkbox"/> | Username | Group Name | Security Level | Auth Protocol | Auth Password | Encryption Protocol | Encrypted Password | Action |
|--------------------------|----------|------------|----------------|---------------|---------------|---------------------|--------------------|--------|
| No Data | | | | | | | | |

Up to 50 entries can be added. Total 0 < **1** > 10/page

(2) Configure v3 user parameters.

Add
×

* Username

* Group Name ▾

* Security Level ▾

* Auth Protocol ▾

* Encryption Protocol ▾

* Auth Password

* Encrypted Password

Table 12-6 v3 User Configuration Parameters

| Parameter | Description |
|------------------------------|---|
| Username | <ul style="list-style-type: none"> ● 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. |
| 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> |

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

12.5.4 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 12-7 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 “system”. |
| Version | For SNMP v2c, the custom community name is “snmp_v2c_group”, and the default port number is 161. |
| Read & write permission | Read-only permission. |

- Configuration Steps

(1) In the global configuration interface, select v2c and set other settings as default. Then, click **Save**.

SNMP Service

* SNMP Version v1 v2c v3

* Local Port

* Device Location

* Contact Info

- (2) Add a view on the View/Group/Community/Client Access Control interface.
 - a Click **Add** in the **View List** pane to add a view.
 - b Enter the view name and OID in the pop-up window, and click **Add Included Rule**.

Add ×

* View Name

OID

Rule/OID List

Up to **100** entries are allowed.

| <input type="checkbox"/> | Rule | OID | Action |
|--------------------------|----------|----------------|------------------------|
| <input type="checkbox"/> | Included | .1.3.6.1.2.1.1 | Delete |

Total 1 < 1 > Go to page

- c Click **OK**.
- (3) On the View/Group/Community/Client Access Control interface, enter the SNMP v1/v2c community name.
 - a Click **Add** in the **SNMP v1/v2c Community Name List** pane.
 - b Enter the group name, access mode, and view in the pop-up window.

×

Add

* Community Name

* Access Mode

* MIB View [Add View +](#)

c Click **OK**.

2. Configuring SNMP v3

- 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 12-8 User Requirement Specification

| 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

(1) On the global configuration interface, select v3, and change the port number to 161. Set other settings to defaults. Then, click **Save**.

SNMP Service

* SNMP Version v1 v2c v3

* Local Port

* Device Location

* Contact Info

Save

(2) 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**.

Add ×

* View Name

OID

Add Included Rule **Add Excluded Rule**

Rule/OID List Delete Selected

Up to **100** entries are allowed.

| <input type="checkbox"/> | Rule | OID | Action |
|--------------------------|----------|----------------|--------|
| <input type="checkbox"/> | Included | .1.3.2.6.1.2.1 | Delete |

Total 1 Go to page

Cancel **OK**

- a Click **OK**.
- (3) On the View/Group/Community/Client Access Control interface, add an SNMP v3 group.
- a Click **Add** in the **SNMP v3 Group List** pane.
 - b Enter the group name and security level on the pop-up window. As this user has read and write permissions, select `public_view` for read-only and read & write views, and select `none` for notify views.

Add ×

| | | |
|---------------------|--|------------------------------|
| * Group Name | <input type="text" value="default_group"/> | |
| * Security Level | <input type="text" value="Auth & Security"/> | ▼ |
| * Read-Only View | <input type="text" value="public_view"/> | ▼ Add View + |
| * Read & Write View | <input type="text" value="public_view"/> | ▼ Add View + |
| * Notification View | <input type="text" value="none"/> | ▼ Add View + |

- c Click **OK**.
- (4) On the View/Group/Community/Client Access Control interface, add an SNMP v3 user.
- a Click **Add** in the **SNMP v3 Client List** pane.
 - b Enter the user name and group name in the pop-up window. As the user's security level is authentication and encryption, enter the authentication protocol, authentication password, encryption protocol, and encryption password.

Add ×

* Username

* Group Name

* Security Level

* Auth Protocol * Auth Password

* Encryption Protocol * Encrypted Password

c Click **OK**.

12.5.5 Configuring Trap Service

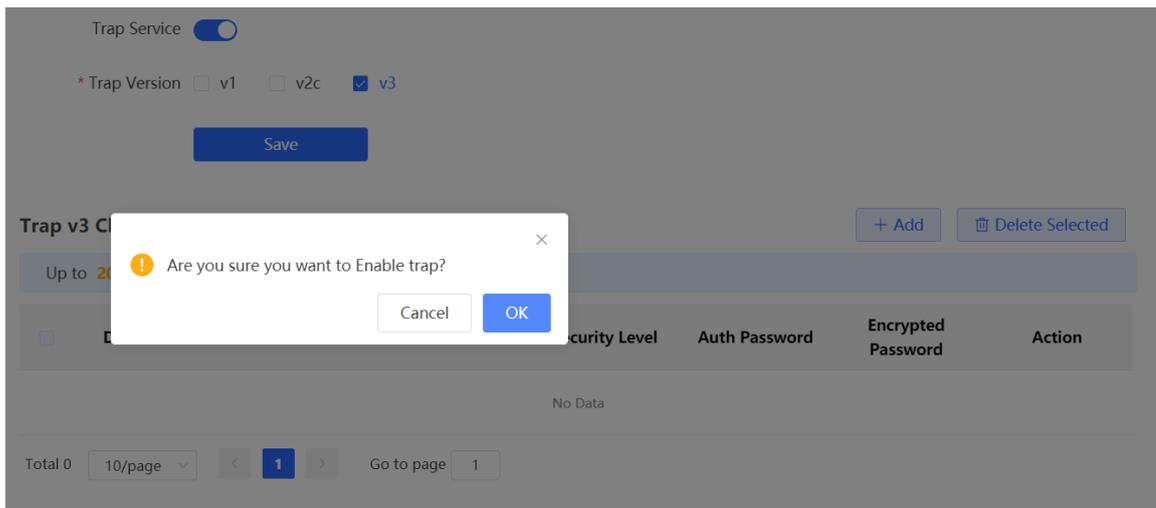
Trap is a notification mechanism of the Simple Network Management Protocol (SNMP) protocol. It is used to report the status and events of network devices to administrators, including device status, faults, performance, configuration, and security management. Trap provides real-time network monitoring and fault diagnosis services, helping administrators discover and solve network problems in a timely manner.

1. Enabling Trap Service

Enable the trap service and select the effective trap version, including v1, v2c, and v3 versions.

Choose **Network-Wide > Workspace > Network-Wide > SNMP > Trap Setting**

(1) Enable the trap service. When the trap service is enabled for the first time, the system will pop up a prompt message. Click **OK**.



When the trap service is enabled for the first time, the system will pop up a prompt message. Click **OK**.

(2) Set the trap version. The trap versions include v1, v2c, and v3.

Trap Service

* Trap Version v1 v2c v3

Save

(3) After the trap service is enabled, click **Save** for the configuration to take effect.

2. Configuring Trap v1/v2c Users

- Overview

Trap is a notification mechanism that is used to send alerts to administrators when important events or failures occur on devices or services. Trap v1/v2c are two versions in the SNMP protocol for network management and monitoring.

Trap v1 is the first version that supports basic alert notification functionality. Trap v2c is the second version, which supports more alert notification options and advanced security features.

By using trap v1/v2c, administrators can promptly understand problems on the network and take corresponding measures.

- Prerequisites

Once trap v1 and v2c versions are selected, it is necessary to add trap v1/v2c users.

- Procedure

- Choose **Network-Wide > Workspace > Network-Wide > SNMP > Trap Setting**

(1) Click **Add** in the **Trap v1/v2c Client List** pane to add a trap v1/v2c user.

Trap v1/v2c Client List + Add Delete Selected

Up to 20 entries are allowed.

| <input type="checkbox"/> | Dest Host IP | Version Number | Port ID | Community Name | Action |
|--------------------------|--------------|----------------|---------|----------------|--------|
| No Data | | | | | |

Total 0 < 1 > Go to page

(2) Configure trap v1/v2c user parameters.

Add
×

* Dest Host IP

* Version Number

* Port ID

* Community
Name/Username

Table 12-9 Trap v1/v2c User Configuration Parameters

| 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 | Community name of the trap user. <ul style="list-style-type: none"> ● 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. |

⚠ 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**.

2. Configuring Trap v3 Users

- Overview

Trap v3 is a network management mechanism based on the SNMP protocol. It is used to send alert notifications to administrators. Unlike previous versions, trap v3 provides more secure and flexible configuration options, including authentication and encryption features.

Trap v3 offers custom conditions and methods for sending alerts, as well as the recipients and notification methods for receiving alerts. This enables administrators to have a more accurate understanding of the status of network devices and to take timely measures to ensure the security and reliability of the network.

- Prerequisites

When the v3 version is selected for the trap service, it is necessary to add a trap v3 user.

- Configuration Steps

Choose **Network-Wide > Workspace > Network-Wide > SNMP > Trap Setting**

(1) Click **Add** in the **Trap v3 User** pane to add a trap v3 user.

Trap Service

* Trap Version v1 v2c v3

Save

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 | | | | | | | |

Total 0 Go to page

(2) Configure trap v3 user parameters.

Add ×

* Dest Host IP * Port ID

* Username * Security Level

* Auth Protocol * Auth Password

* Encryption Protocol * Encrypted Password

Table 12-10 Trap v3 User Configuration Parameters

| 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 | Name of the trap v3 user. <ul style="list-style-type: none"> ● 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 |
|--|---|
| 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**

The destination host IP address of trap v1/ v1/v2c users cannot be the same.

12.5.6 Trap Service Typical Configuration Examples

1. Configuring Trap v2c

- Application Scenarios

During device monitoring, if the device is suddenly disconnected or encounters an abnormality, and the third-party monitoring software cannot detect and handle the abnormal situation in a timely manner, you can configure the device with a destination IP address of 192.168.110.85 and a port number of 166 to enable the device to send a v2c trap in case of an abnormality.

- Configuration Specification

According to the user’s application scenario, the requirements are shown in the following table:

Table 12-11 User Requirement Specification

| Item | Description |
|----------------------------|--|
| IP address and port number | The destination host IP is 192.168.110.85, and the port number is 166. |

| Item | Description |
|--------------------------|------------------------|
| Version | Select the v2 version. |
| Community name/User name | Trap_user |

● Configuration Steps

(1) Select the v2c version in the **Trap Setting** interface and click **Save**.

Trap Service

* Trap Version v1 v2c v3

Save

Trap v1/v2c Client List **+ Add** **Delete Selected**

Up to 20 entries are allowed.

| <input type="checkbox"/> | Dest Host IP | Version Number | Port ID | Community Name | Action |
|--------------------------|--------------|----------------|---------|----------------|--------|
| No Data | | | | | |

Total 0

(2) Click **Add** in the Trap v1/v2c Client List to add a trap v2c user.

(3) Enter the destination host IP address, version, port number, user name, and other information. Then, click **OK**.

Add ×

* Dest Host IP

* Version Number

* Port ID

* Community Name/Username

2. Configuring Trap v3

● Application Scenarios

During device monitoring, if the device is suddenly disconnected or encounters an abnormality, and the third-party monitoring software cannot detect and handle the abnormal situation in a timely manner, you can configure the

device with a destination IP address of 192.168.110.87 and a port number of 167 to enable the device to send a v3 trap, which is a safer trap compared with v1/v2c traps.

● Configuration Specification

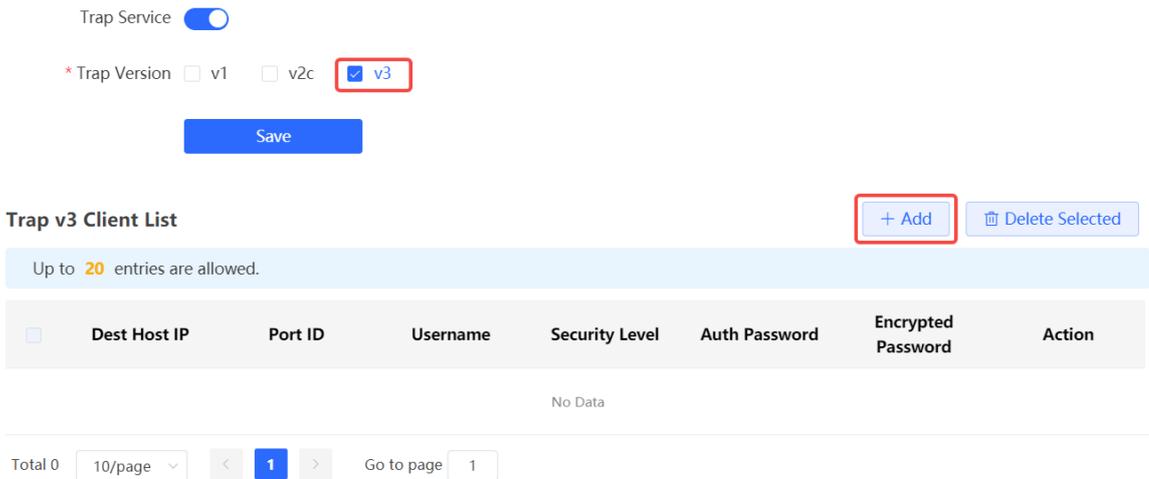
According to the user’s application scenario, the requirements are shown in the following table:

Table 12-12 User Requirement Specification

| 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 in the **Trap Setting** interface and click **Save**.



(2) Click **Add** in the Trap v3 Client List to add a trap v3 user.

(3) Enter the destination host IP address, port number, user name, and other information. Then, click **OK**.

Add
×

| | |
|--|---|
| * Dest Host IP <input style="width: 90%;" type="text" value="192.168.110.87"/> | * Port ID <input style="width: 90%;" type="text" value="167"/> |
| * Username <input style="width: 90%;" type="text" value="trap_v3_user"/> | * Security Level <input style="width: 90%;" type="text" value="Auth & Security"/> |
| * Auth Protocol <input style="width: 90%;" type="text" value="MD5"/> | * Auth Password <input style="width: 90%;" type="text" value="Ruijie123"/> |
| * Encryption Protocol <input style="width: 90%;" type="text" value="AES"/> | * Encrypted Password <input style="width: 90%;" type="text" value="Ruijie123"/> |

12.6 Configuring Reboot

12.6.1 Rebooting the Current Device

Choose **One-Device > Gateway > Config > System > Reboot > Reboot**.

Click **Reboot**, and the device will be restarted. Please do not refresh or close the page during the reboot process. After the device is rebooted, the browser will be redirected to the login page.

Do not power off the device during reboot.

12.6.2 Rebooting All Devices in the Network

Choose **Network-wide > System > Reboot > Reboot**.

Select **All Devices**, and click **Reboot All Device** to reboot all devices in the current network.

Do not power off the device during reboot.

Select

master device

All Devices

Specified Devices

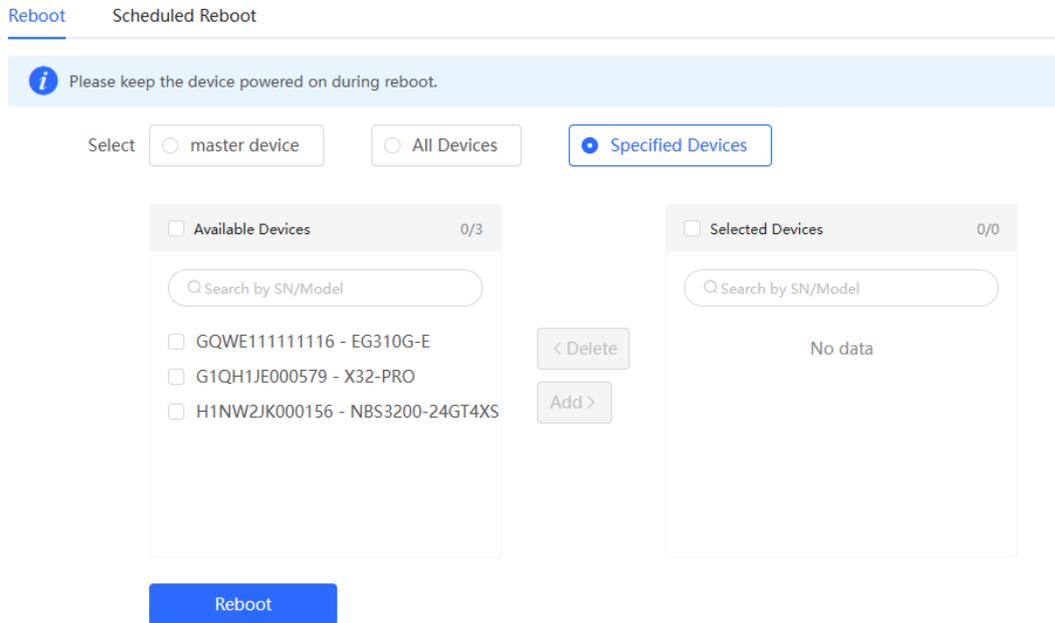
Caution

The operation takes some time and affects the whole network. Therefore, exercise caution when performing this operation.

12.6.3 Rebooting the Specified Device

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

Click **Specified Devices**, select required 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.



12.7 Configuring Scheduled Reboot

Confirm that the system time is accurate to avoid network interruption caused by device reboot at wrong time. For details about how to configure the system time, see Section [12.8 Setting and Displaying System Time](#).

Choose **Network-Wide > Workspace > Network-Wide > Reboot > Scheduled Reboot**.

Turn on **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. You are advised to set scheduled reboot time to off-peak hours.

⚠ Caution

The operation affects the whole network. Therefore, exercise caution when performing this operation.

1. After this feature is enabled, the device will reboot at the scheduled time.
2. You are advised to set the scheduled reboot time in the early morning or other service idle time.
Note: When the upstream device is rebooted at the scheduled time, all downstream devices connected to it will also be rebooted.

Scheduled Reboot

Repeats on Mon Tue Wed Thu Fri Sat Sun

Reboot Time 05 : 18

Save

12.8 Setting and Displaying System Time

Choose **Network-Wide > 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, and time settings are not saved upon restart).

Current Time

* Time Zone

* NTP Server

Save

Click **Current Time**, and the current system time will be filled in automatically.

Edit×

* Time

12.9 Configuring Backup and Import

Choose **Network-Wide > System > Backup & Import**.

Configuration backup: Click **Backup** to download a configuration file locally.

Configuration import: Click **Browse**, select a backup file on the local PC, and click **Import** to import the configuration file. The device will restart.

- i** If the target version is much later than the current version, some configuration may be missing.

 1. Before importing the configuration file, you are advised to [Reset](#) the device.
 2. After the configuration file is imported, the device will reboot automatically.

Backup Config ?

Backup Config

Import Config ?

File Path

12.10 Configuring LEDs

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

- Configuring the LED status of network-wide APs

Click **Open All** or **Close All** to enable or disable the LEDs of all APs on the network.

LED ? Batch Operation ✓ Open All Close all IP/MAC/hostname/SN/S Q

| | Username | Model | SN | IP Address | Action |
|--|----------|------------|----|-----------------|--------------------------|
| | AP | RAP73HD | G | 192.168.110.113 | <input type="checkbox"/> |
| | R260AP | RAP2260(G) | G | 192.168.110.48 | <input type="checkbox"/> |
| | 2261E | RAP2261(E) | M | 192.168.110.41 | <input type="checkbox"/> |
| | 2260G | RAP2260(G) | M | 192.168.110.76 | <input type="checkbox"/> |

Total 4 < 1 > 10/page

● Configuring the LED status of selected APs

Click **Batch Operation**, select the desired APs, and click **Open Selected** or **Close Selected** to enable or disable the LED status of the selected APs.

LED ? Batch Operation ✓ Open All Close all IP/MAC/hostname/SN/S Q

| | Username | Model | SN | IP Address | Action |
|--|----------|------------|---------------|-----------------|--------------------------|
| | AP | RAP73HD | G1SK48F000415 | 192.168.110.113 | <input type="checkbox"/> |
| | R260AP | RAP2260(G) | C | 192.168.110.48 | <input type="checkbox"/> |
| | 2261E | RAP2261(E) | M | 192.168.110.41 | <input type="checkbox"/> |

LED ? Exit Batch Operation Open Selected Close Selected IP/MAC/hostname/SN/S Q

| | Username | Model | SN | IP Address | Action | |
|-------------------------------------|----------|--------|------------|------------|-----------------|--------------------------|
| <input type="checkbox"/> | | AP | RAP73HD | C | 192.168.110.113 | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> | | R260AP | RAP2260(G) | M | 192.168.110.48 | <input type="checkbox"/> |
| <input checked="" type="checkbox"/> | | 2261E | RAP2261(E) | M | 192.168.110.41 | <input type="checkbox"/> |

● Configuring the LED status of a single AP

Toggle on or off the switch in the **Action** column to enable or disable the LED status of the corresponding AP.

LED ? Batch Operation ✓ Open All Close all IP/MAC/hostname/SN/S Q

| | Username | Model | SN | IP Address | Action |
|--|----------|------------|----|-----------------|-------------------------------------|
| | AP | RAP73HD | C | 192.168.110.113 | <input type="checkbox"/> |
| | R260AP | RAP2260(G) | C | 192.168.110.48 | <input checked="" type="checkbox"/> |
| | 2261E | RAP2261(E) | M | 192.168.110.41 | <input type="checkbox"/> |

12.11 Configuring Diagnostics

Caution

If the issue persists despite following the troubleshooting methods provided in this section, you may require remote support from a technician who will enable developer mode to resolve the issue. We will ensure your data is protected during this process.

12.11.1 Network Check

When a network error occurs, perform **Network Check** to identify the fault and take the suggested action.

Choose **One-Device > Gateway > Config > Diagnostics > Network Check**.

Click **Start** to perform the network check and show the result.



The interface displays a 'Start' button in blue. Below it is a 'Recheck' button in blue. A progress bar is shown at 100%. Below the progress bar is a list of 13 diagnostic items, each with a checkmark icon on the right:

- WAN/LAN Cable Connection
- Negotiation Speed
- WAN Port Configuration
- DHCP IP Address Allocation
- WAN and LAN IP Conflicts
- Loop Detection
- DHCP Server Conflict
- IP Conflicts
- Routing Configuration
- Next-Hop Connectivity
- DNS Configuration
- IP Session Count

If a network error occurs, its symptom and suggested action will be displayed.

Cloud Service Configuration !

Check Cloud Service

Result : The device is not enabled with cloud service. Cloud service may fail to start.

Suggestion : Please restore the device to factory settings or contact Ruijie technical support.

12.11.2 Alerts

Click **Alert Center** in the navigation bar.

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

⚠ 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 |
|--------|--|---|-----------------|
| ▼ | The IP address of the downlink device is already in use. | Please check the IP address of the downlink device. If it is a static IP address, please change the IP address. | Delete Unfollow |

| Device Name | SN | Type | Time | Details | Action |
|-------------|------|----------|---------------------|---|--------|
| RG310G-E | N-99 | EG310G-E | 2023-12-12 14:32:05 | An IP address conflict occurs. IP address: 10.52.48.106. Conflicting MAC address: f0:74:8d:b1:9d:e3 and 00:d0:f8:12:5a:2c | Delete |

Total 1 < 1 > 10/page

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

View Unfollowed Alert ×

The IP address of the downlink device is already in use.

[Re-follow](#)

Cancel

12.11.3 Network Tools

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

1. Ping

Choose **One-Device > Gateway > Config > Diagnostics > Network Tools**.

The **Ping** command is used to detect the network connectivity.

Select **Ping** as the diagnosis mode, select the IP type, 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.

Tool ? Ping Traceroute DNS Lookup

Type IPv4 IPv6

* IP Address/Domain

* Ping Count

* Packet Size

Result

2. Traceroute

Choose **One-Device > Gateway > Config > Diagnostics > Network Tools**.

The **Traceroute** function is used to identify the network path from one device to another. On a simple network, the network path may pass through only one routing node or none at all. On a complex network, packets may pass through dozens of routing nodes before reaching their destination. The traceroute function can be used to judge the transmission path of data packets during communication.

Select **Traceroute** as the diagnosis mode, select the IP type, and enter a destination IP address or the maximum TTL value used by the URL and traceroute, and click **Start**.

Tool Ping Traceroute DNS Lookup

Type IPv4 IPv6

* IP Address/Domain

* Max TTL

Result

3. DNS Lookup

Choose **One-Device > Gateway > Config > 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**.

Tool Ping Traceroute DNS Lookup

* IP Address/Domain

DNS

```
Server:      8.8.8.8
Address: 8.8.8.8#53

Name: www.google.com
Address 1: 159.138.20.20
Address 2: 2a03:2880:f11a:83:face:b00c:0:25de
```

12.11.4 Packet Capture

Choose **One-Device > Gateway > Config > Diagnostics > Packet Capture**.

If the device fails and troubleshooting is required, the packet capture result can be analyzed to locate and rectify the fault.

Select an interface and a protocol and specify the host IP address to capture the content in data packets. Select the file size limit and packet count limit to determine the conditions for automatically stopping packet capture. (If the file size or number of packets reaches the specified threshold, packet capture stops and a diagnostic package download link is generated.) Click **Start** to execute the packet capture command.

Caution

The packet capture operation may occupy many system resources, causing network freezing. Therefore, exercise caution when performing this operation.

| | | |
|----------------------|----------------------------------|----------------------------------|
| Interface ? | <input type="text" value="ALL"/> | |
| Protocol ? | <input type="text" value="ALL"/> | |
| IP Address ? | <input type="text"/> | |
| File Size Limit ? | <input type="text" value="2M"/> | Available Memory 776.54 M |
| Packet Count Limit ? | <input type="text" value="500"/> | |

PCAP file [Click to download the PCAP file.](#) 

[Click to delete the file.](#)

Packet capture can be stopped at any time. After that, a download link is generated. Click this link to save the packet capture result in the PCAP format locally. Use analysis software such as Wireshark to view and analyze the result.

Interface ?

Protocol ?

IP Address ?

File Size Limit ? Available Memory **776.54 M**

Packet Count Limit ? **File Size: 106.77K**
Captured on: 2023-12-07 19:02:45

PCAP file [Click to download the PCAP file](#) i
[Click to delete the file.](#)

12.11.5 Fault Collection

Choose **One-Device > Gateway > Config > Diagnostics > Fault Collection.**

When the device fails, you need to collect the fault information. Click **Start**. The configuration files of the device will be packed into a compressed file. Download the compressed file locally and provide it to R&D personnel for fault locating.

i Compress the configuration file for engineers to identify fault.

12.11.6 Viewing Flow Statistics

Choose **One-Device > Gateway > Config > Diagnostics > Flow Statistic.**

On the **Flow Table Packet Counters Page**, you can view the details of packets received by the device, including protocol, aging time, state, source IP address, destination IP address, source port, destination port, and so on.

Flow Table Packet Counters Page Fuzzy search by Src IP/Dest IP/Src port/Dest port

| protocol | aging_time | state1 | src | dst | sport | dport | packets | bytes | state2 | src_down | dst_down | sport_down | dport_down | packets_down | bytes_down | mark | use |
|----------|------------|--------|--------------|--------------|------------------|----------|---------|-------|--------|--------------|--------------|------------------|------------|--------------|------------|------|-----|
| udp | 3 | - | 127.0.0.1 | 127.0.0.1 | 45982 | 53 | 1 | 71 | - | 127.0.0.1 | 127.0.0.1 | 53 | 45982 | 1 | 71 | 0 | 2 |
| udp | 1 | - | 192.168.2.5 | 192.168.2.1 | 39498 | 53 | 1 | 59 | - | 192.168.2.1 | 192.168.2.5 | 53 | 39498 | 1 | 169 | 1 | 2 |
| udp | 5 | - | 10.52.48.4.3 | 192.168.5.28 | 49271 | 53 | 1 | 58 | - | 192.168.5.28 | 10.52.48.4.3 | 53 | 49271 | 1 | 166 | 1 | 2 |
| icmp | 2 | - | 10.52.48.4.3 | 223.5.5.5 | type=8 code=0 | id=16145 | 1 | 84 | - | 223.5.5.5 | 10.52.48.4.3 | type=0 code=0 | id=16145 | 1 | 84 | 1 | 2 |
| udp | 4 | - | 192.168.2.2 | 192.168.2.1 | 59258 | 53 | 1 | 63 | - | 192.168.2.1 | 192.168.2.2 | 53 | 59258 | 1 | 430 | 1 | 2 |
| udp | 4 | - | 10.52.48.4.3 | 172.30.44.20 | 40322 | 53 | 1 | 63 | - | 172.30.44.20 | 10.52.48.4.3 | 53 | 40322 | 1 | 430 | 1 | 2 |
| udp | 2 | - | 127.0.0.1 | 127.0.0.1 | 36339 | 53 | 2 | 118 | - | 127.0.0.1 | 127.0.0.1 | 53 | 36339 | 2 | 260 | 0 | 2 |

12.12 Performing Upgrade and Checking System Version

Caution

You are advised to back up the configuration before upgrading the router.

Version upgrade will restart the device. Do not refresh or close the browser during the upgrade process.

12.12.1 Online Upgrade

Choose **One-Device > Gateway > Config > 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.
systool.upgradeWarningTip

Current Version ReyeeOS 2.0000.0000.0000 (Latest version)

12.12.2 Local Upgrade

Choose **One-Device > Gateway > Config > System > Upgrade > Local Upgrade**.

You can view the current software version and device model. If you want to upgrade the device with the configuration retained, select **Keep Config**. Click **Browse**, select an upgrade package on the local PC, and click **Upload** to upload the file. The device will be upgraded.

 systool.upgradeWarningTip

Model E

Current Version  ReyeeOS 2 4

Development Mode (It is recommended to be disabled after use.)

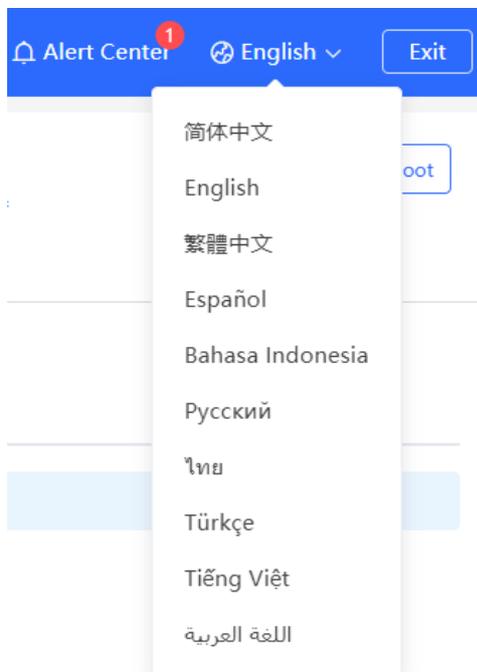
Retain Configuration  (If the target version is much later than the current version, you are advised not to retain the configuration.)

File Path 

12.13 Switching System Language

Click  in the upper-right corner of the Web page.

Click a required language to switch the system language.



12.14 Configuring Cloud Service

12.14.1 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.

12.14.2 Configuration Steps

Choose **One-Device > Gateway > 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.



If the device cannot connect to Ruijie Cloud through QR code scanning, you can click the Configure Cloud Service button to connect the device to Ruijie Cloud.

[Configure Cloud Service](#)

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.

Project Name:lg [blurred]

Account: 18 [blurred]

Unbind the account if you no longer wish to manage this project remotely.

[Unbind](#)

Cloud Server

On-Premises Private Cloud Connected [Configure Cloud Service](#)

13 FAQ

13.1 What Can I Do If I Fail to Log In to the Web Page?

- (1) Confirm that the network cable is correctly connected to the LAN port of the device, and the corresponding indicator is flashing or steady on.
- (2) Before you access the Settings page, you are advised to configure the PC to automatically obtain an IP address, so the DHCP-enabled device automatically allocates an IP address to the PC. If you want to specify a static IP address to the PC, ensure that the IP address of the PC and the IP address of the device's LAN port are in the same network segment. For example, if the LAN port IP address is 192.168.110.1 and subnet mask is 255.255.255.0, set the PC IP address to 192.168.110.X (X representing any integer in the range of 2 to 254) and the subnet mask to 255.255.255.0.
- (3) Run the ping command to test the connectivity between the PC and device. If ping fails, check the network settings.
- (4) If you still cannot log in to the **Device Management** page after the preceding steps, restore the device to factory settings.

13.2 How Do I Restore Factory Settings?

When the device is powered, press and hold the **Reset** button on the panel for 5 seconds. The device will restore factory settings after restart. Then, you can log in to the Web page of the device using the default IP address 192.168.110.1.

13.3 What Can I Do If I Forget the Device Login Password?

Try to log in using the Wi-Fi password. If the fault persists, restore the factory settings.

13.4 What Can I Do If Internet Access Through PPPoE Dial-Up Fails?

- (1) Check whether the PPPoE account is correct. Please see Section [2.5.3 Forgetting the PPPoE Account](#) for details.
- (2) Check whether the IP address allocated by the ISP conflicts with the IP address existing on the router.
- (3) Check whether the MTU setting of the device meets the requirements of the ISP. The default MTU is 1500. Please see Section [4.3.3 Modifying the MTU](#) for details.
- (4) Check whether VLAN tagging should be configured for PPPoE. VLAN tagging is disabled by default. Please see Section [4.3.5 Configuring the VLAN Tag](#) for details.