YF355 Series Router User Manual

2G/3G/4G/5G Cellular Router
1x WAN/LAN, 1 x LAN, 1 x RS232, 1 x RS485, 1 x DI, 1 x DO

The user manual is suitable for the following models:

Model No.	Description
YF355-L	CAT4 4G LTE Router, Dual SIM
YF355-L1	CAT1 4G LTE Router, Dual SIM
YF355-LA	CAT6 4G LTE Router, Dual SIM
YF355-5R	5G Redcap Router, Dual SIM

Xiamen Yifan Communication Technology Co., Ltd.
Add：14th Floor, No.370, Chengyi Street, Jimei,
Xiamen, China Zip Code: 361000
Tel：+86 592-6101492
Fax: +86 592-5222813
http://www.yifanwireless.com

Revision History

Date	Version	Declaration	Author
2025-5-30	V1.0.0	Initial version	Jonas
2025-9-3	V1.0.1	Adding Installation Chapter	Jonas

Note: There may be differences between models of accessories and interfaces, actual products shall prevail.

Copyright Notice

All materials or content contained in this document are protected by copyright law. All copyrights are owned by Xiamen Yifan Communication Technology Co., Ltd., except for content attributed to other parties. Without written permission from Yifan, no one may copy, distribute, reprint, link, transmit, or use any content on this document for any commercial purpose. However, downloading or printing for non-commercial, personal use is permitted (provided that the material is not modified, and the copyright notice or other ownership notices are retained).

Trademark Statement

Yifan, Yeacomm both are registered trademarks of Xiamen Yifan Communication Technology Co., Ltd. Without prior written permission, no one is allowed to use the Yifan name and Yifan trademarks and symbols in any way.

Product Applicability Statement

This user manual explains how to configure the following devices:

- YF355-5R
- YF355-LA
- YF355-L
- YF355-L1

CE Warning

- An adapter shall be installed near the equipment and shall be easily accessible.
- Supply by specified adapter the operating temperature of the device, can't exceed 40℃ and should not be lower than -10℃. Supply by other power supply the operating temperature of the device, can't exceed 75℃ and shouldn't be lower than -40℃.
- The plug considered as disconnect device of adapter.
- The device complies with RF specifications when the device used at 20cm from the body.

Hereby, Yifan Corporation declares that this product is in compliance with essential requirements and other relevant provisions of Directive 2014/53/EU. This product is allowed to be used in all EU member states.

Contents

Chapter 1 Parameter Configuration.....1

1.1 Configuration Connection Diagram 1

1.2 Login to the Configuration Page 1

1.2.1 PC IP Address Configuration (Three Methods) 1

1.2.2 Login to the Configuration Page 2

Chapter 2 Configuration and Management.....4

2.1 WEBUI header.....4

2.2 HOME.....5

2.2.1 Operating Performance.....5

2.2.2 Device Info 6

2.2.3 Internet 7

2.2.4 Wireless.....7

2.2.5 LAN Port.....8

2.2.6 4G/5G Cellular Network 9

2.2.7 Console 10

2.3 Network.....11

2.3.1 WAN 11

2.3.1.1 WAN Configure 11

2.3.1.2 Global Setting 14

2.3.1.3 Operator Limit 14

2.3.1.4 Topology.....15

2.3.2 LAN 15

2.3.3 WIFI.....18

2.3.3.1 WIFI Configure.....18

2.3.3.2 Virtual Interface.....21

2.3.3.3 Chillispot.....22

2.3.4 VPN 24

2.3.4.1 PPTP.....24

2.3.4.2 L2TP.....26

2.3.4.3 OPENVPN.....30

2.3.4.4 IPSEC 34

2.3.4.5 GRE 38

2.3.4.6 EOIP.....40

2.3.4.7 FRP 41
2.3.4.8 ZeroTier 43
2.3.4.9 L2tpv3 45
2.3.4.10 WireGuard 46
2.3.5 NAT 51
2.3.5.1 Port Forward 51
2.3.5.2 DMZ 53
2.3.5.3 Virtual IP Setting 53
2.3.6 IPV6 54
2.3.7 VLAN 58
2.3.8 Bridge 58
2.3.8.1 Bridge Configure 58
2.3.8.2 Port Setup 59
2.3.9 Routing 61
2.3.10 DDNS 62
2.3.11 MAC Clone 62
2.4 Data Acquisition 63
2.4.1 Child Device 63
2.4.2 Cloud 64
2.4.3 I/F Setting 65
2.4.4 Proto Conv 65
2.4.4.1 Modbus TCP 65
2.4.4.2 Modbus RTU 66
2.5 Application 67
2.5.1 Active Policy 67
2.5.1.1 Schedule Reboot 67
2.5.1.2 Timed Tasks 68
2.5.2 Security 68
2.5.2.1 IP Restrictions 68
2.5.2.2 URL Restrictions 70
2.5.2.3 MAC Restrictions 70
2.5.2.4 Firewall 71
2.5.2.5 Cert Management 72
2.5.2.6 Web Access 73
2.5.3 QOS 73
2.5.3.1 QOS Basic 73
2.5.3.2 QOS Classify 75

2.6 Serial Applications 77
2.6.1 Serial Applications 77
2.6.2 SMS App 78
2.7 Maintenance 83
2.7.1 Diagnosiss 83
2.7.2 Network Tools 83
2.7.3 Commands 84
2.7.4 Log 84
2.7.5 Firewall 85
2.7.6 Traffic 86
2.7.7 Storage 87
2.7.8 Remote MGT 87
2.8 Maintenance 91
2.8.1 Platform 91
2.9 System 91
2.9.1 System Settings 91
2.9.2 Login MGT 94
2.9.3 Restore 94
2.9.4 Backup 94
2.9.5 Upgrade 95
2.9.6 Module Upgrade 95

Chapter 3 LEDs 97

Chapter 4 Installations 100

4.1 Din Rail Kit Installation 1 (Back Side) 100
4.2 Din Rail Kit Installation 2 (Side Panel) 101
4.3 DI/DO Connection Cable Installation 103

Chapter 1 Parameter Configuration

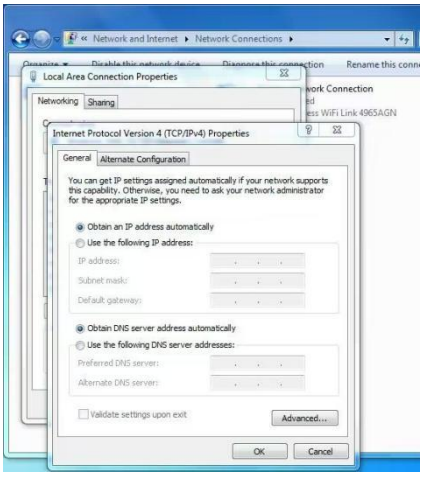
1.1 Configuration Connection Diagram

Before configuring the router, ensure that it is properly connected to the PC used for configuration using the factory-supplied network cable. To establish the connection, insert one end of the network cable into the Ethernet interface labeled "ETH" on the router (referred to as the LAN port below) and connect the other end to the Ethernet port on the PC. This connection is essential for accessing the router's configuration interface.

1.2 Login to the Configuration Page

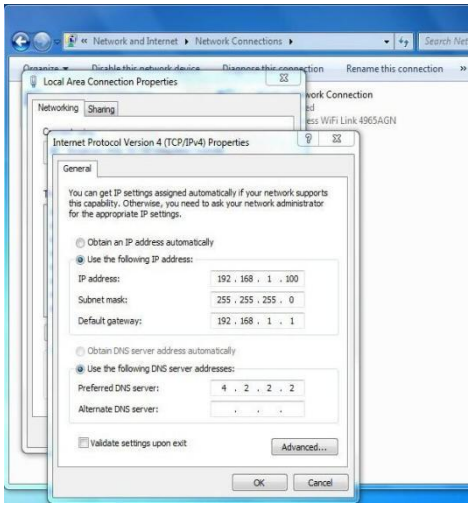
1.2.1 PC IP Address Configuration (Three Methods)

Method 1: Automatically Obtain an IP Address
As illustrated in the figure below, configure the PC to obtain an IP address automatically. Once the PC successfully acquires an IP address within the 192.168.1.1 subnet, you can access the router’s web configuration page by entering 192.168.1.1 in your browser's address bar.



Method 2: Specify an IP Address

Configure the PC's network settings as follows: set the IP address to 192.168.1.100 (or any other available IP within the 192.168.1 subnet), the subnet mask to 255.255.255.0, the default gateway to 192.168.1.1, and the DNS server to a locally available DNS. Once configured, open a web browser and enter 192.168.1.1 in the address bar to access the router's web configuration page.



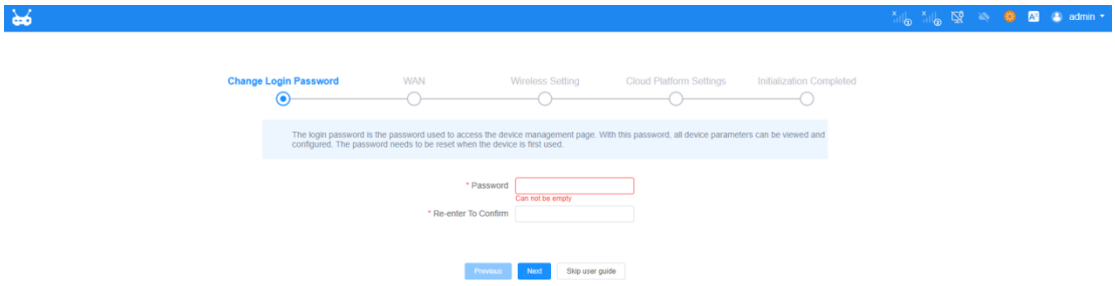
Method 3:

Set the router's connection mode to Static IP or Auto-DHCP, ensuring that both the PC and the router are connected to the same network segment as the upstream router. Once properly configured, you can access the router's web interface by entering its WAN IP:8088 in a web browser.

1.2.2 Login to the Configuration Page

To access the router's web-based management interface, open Internet Explorer or any other web browser. Based on the access method outlined in Section 2.2.1, enter the appropriate URL in the address bar to log in. By default, both the username and password are set to admin.

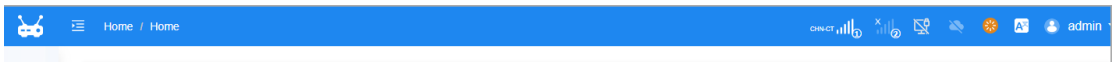
To access the router's web-based management interface, launch Internet Explorer or any other web browser. Refer to Section 2.2.1 for the appropriate access method, then enter the corresponding URL in the address bar. Use the default username and password, both set to admin, to log in and configure the router's settings.



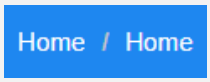
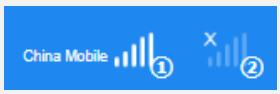
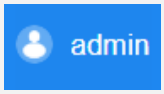
Chapter 2 Configuration and Management

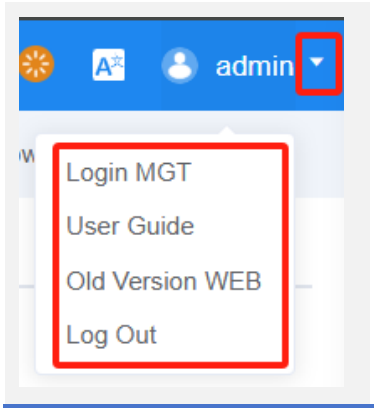
2.1 WEB UI Header

Each device includes a web header. In this chapter, we will explore the key features and functionalities of the web header in detail.



WEB UI Header Description

	Click on the retractable menu bar
	Displays the current page menu path
	Connection status of SIM1 and SIM2
	Wired network connection status
	Manage the platform connection status
	Reboot
	Language switching
	Displays the current login user



Login MGT: change password

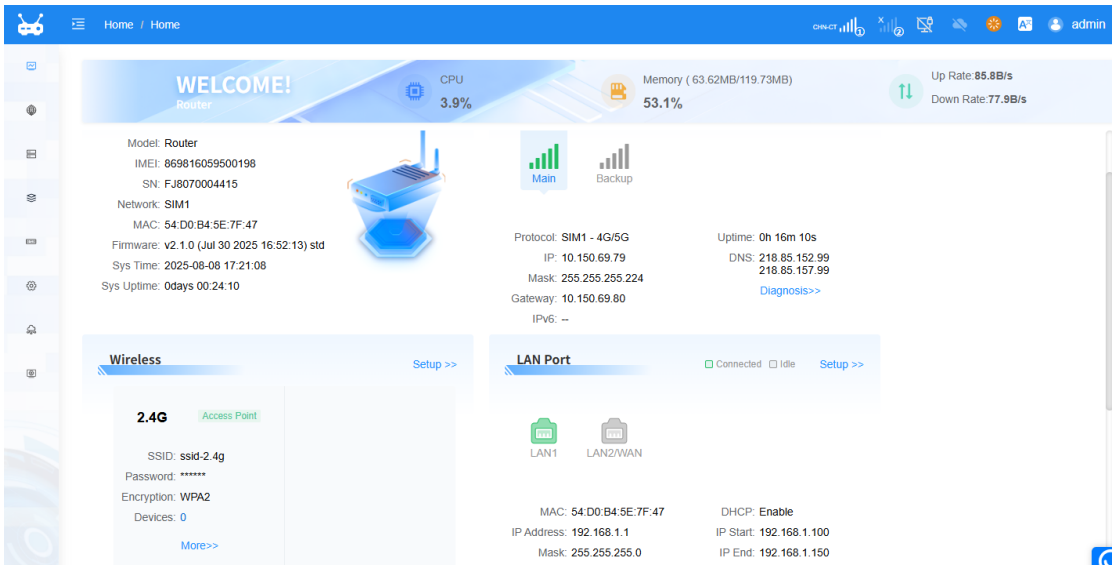
User Guide: enter the boot page settings.

Old Version WEB: The previous version of the web page

Log Out: Users log out

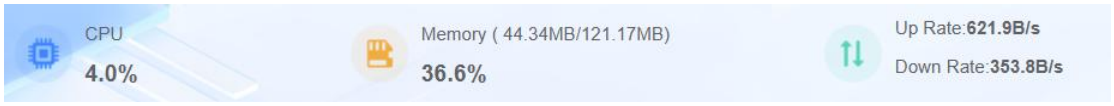
2.2 HOME

The Home page serves as the main dashboard of the WEB UI, providing an overview of key information summaries along with quick access shortcuts to various other pages for streamlined navigation.



2.2.1 Operating Performance

This section provides an overview of the device's current performance, displaying key metrics such as CPU usage, memory status, and the real-time data upload and download rates. These indicators help monitor the device's operational efficiency and performance.

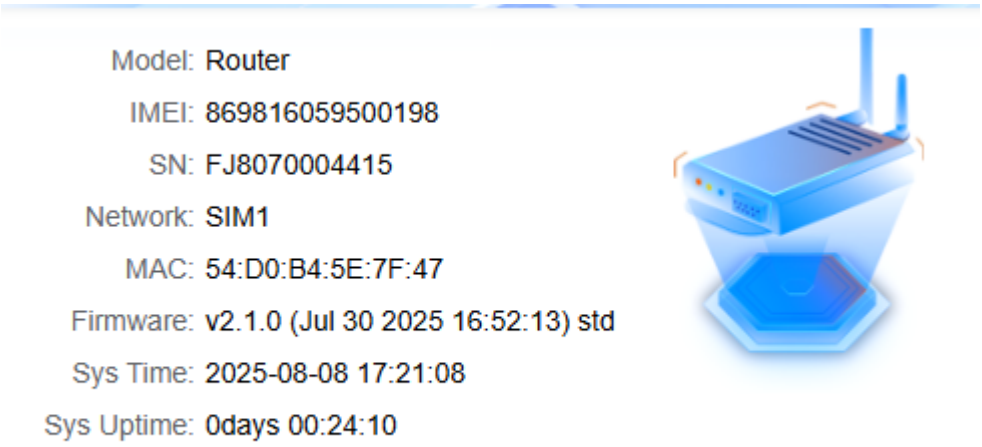


Field Name	Description

CPU	Percentage of CPU utilization
Memory	Percentage of memory usage
Up Rate	Instantaneous upload rate
Down Rate	Instantaneous download rate

2.2.2 Device Info

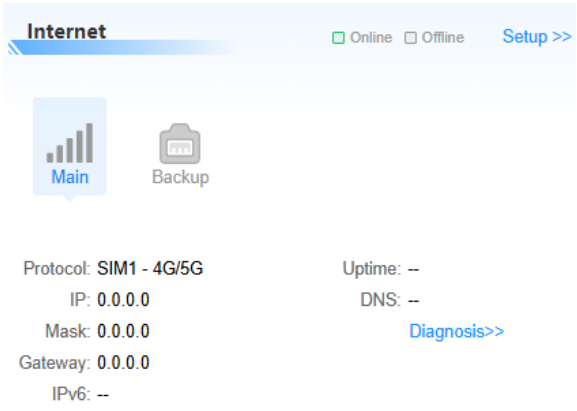
This section is dedicated to presenting the essential information about the equipment, including key details such as its model, serial number, firmware version, and other vital specifications. This provides a clear overview of the device's identity and configuration.



Field Name	Description
Name	Device name
Model	Device mode
SN	Unique device identifier
Network	Network connection method
MAC	Device's MAC address
Firmware	Device's firmware version
Sys Time	System time of the device
Sys Uptime	Duration since device startup

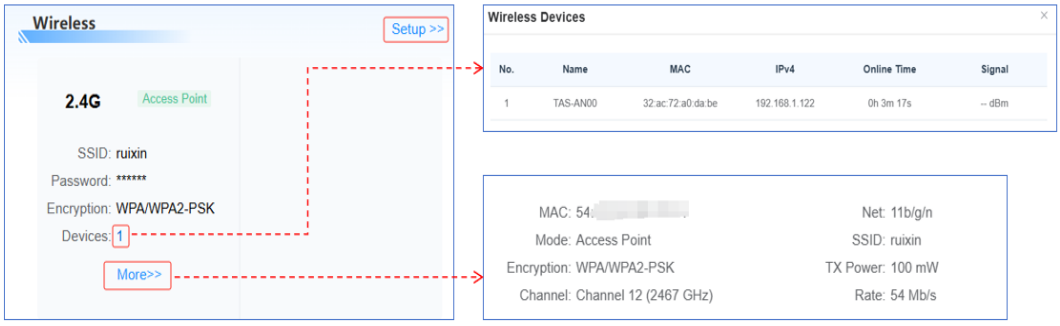
2.2.3 Internet

This section allows you to view detailed Internet connection information. To access the Internet configuration page, simply click "Setup". For more specific details, click on the wireless icon or wired icon to switch between and view the corresponding Internet information. Additionally, by clicking "Diagnosis", you will be redirected to the network diagnostic page for troubleshooting and analysis.



2.2.4 Wireless

This section provides detailed information about the wireless network. To access the wireless network configuration page, click "Setup". The "Devices" field shows the number of users currently connected to the wireless network. For more details, click on "Digital" to view basic information about Wi-Fi users. Additionally, by clicking "More", you can access further details about the wireless network, including signal strength, security settings, and connected devices.

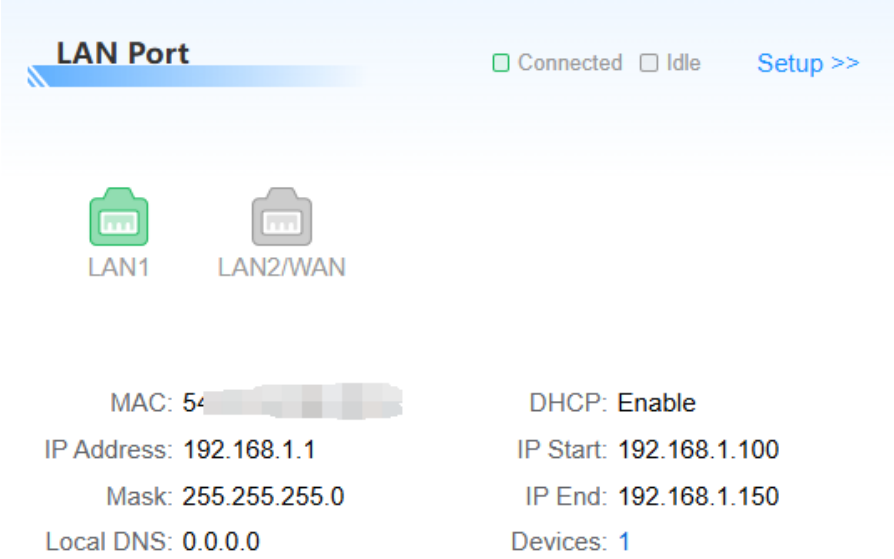


Field Name	Description
SSID	Name of the wireless network

Password	Wireless network password
Encryption	Wireless network encryption type
Devices	Number of devices connected to the network
MAC	MAC address of the device
Mode	Equipment working mode
Channel	Wireless channel in use
Net	Supported network standards
TX Power	Transmit power of the wireless signal
Rate	Wireless network transmission rate

2.2.5 LAN Port

This section provides essential information about the LAN and LAN/WAN ports, helping you monitor the network connections. To configure the LAN port settings, click "Setup" to be redirected to the LAN Port configuration page. The network port icon visually indicates the connection status: if the icon is green, it means the port is actively connected, whereas if it appears gray, the port is not currently connected. This provides a clear and intuitive way to check and manage the port connections.

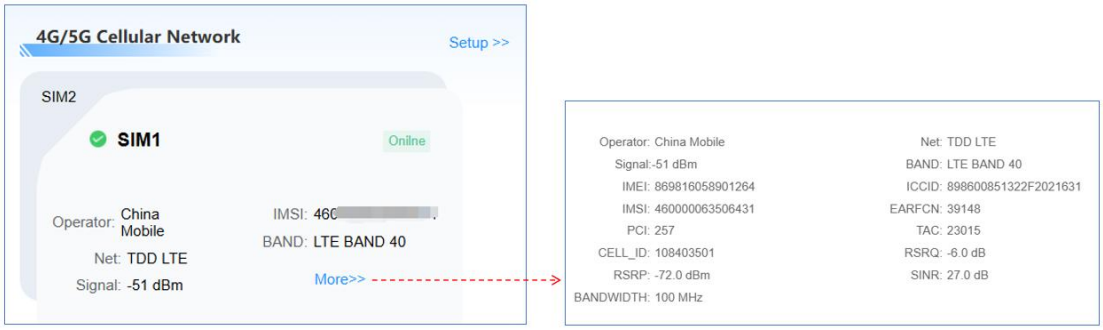


Field Name	Description
MAC	MAC address of the device

IP Address	Router's address on the network
Mask	Netmask for the interface, used to separate network and host parts of the IP address
Local DNS	DNS services for domain name resolution in the local network
DHCP	Status of Dynamic Host Configuration Protocol (DHCP). When enabled, the device automatically assigns IP addresses to connected clients
IP Start	Starting IP address available for DHCP assignment
IP End	Ending IP address available for DHCP assignment
Devices	Number of devices connected to the port

2.2.6 4G/5G Cellular Network

This section allows you to view detailed information about the cellular network connection. To configure the WAN settings, click "Setup" to be directed to the WAN configuration page. You can switch between the two SIM cards by clicking "SIM1" or "SIM2" to view the specific details related to each SIM card. For more in-depth information about the cellular network, click "More" to access further details, such as signal strength, network status, and connection parameters.

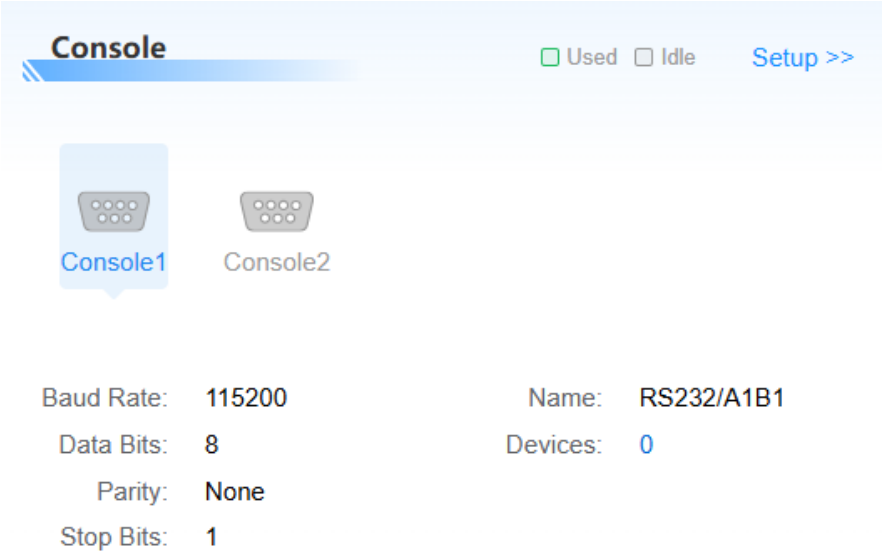


Field Name	Description
Operator	Telecommunications service provider
Net	Network system indicating technical standards and communication mode
Signal	Signal strength received by the device
BAND	Communication frequency band of the device

IMEI	Unique International Mobile Equipment Identity (IMEI) code for mobile devices
ICCID	Unique SIM card identifier for ownership and authentication
IMSI	Unique mobile subscriber identity for distinguishing users in a network
EARFCN	LTE wireless channel identifier (Evolved Absolute Radio Frequency Channel Number)
PCI	Physical Cell Identity, distinguishing LTE base station cells
TAC	Tracking Area Code for mobility management in LTE networks
CELL_ID	Unique identifier for a specific base station cell
RSRQ	Reference Signal Received Quality, measuring signal quality
RSRP	Reference Signal Received Power, indicating received signal strength
SINR	Signal-to-Interference-plus-Noise Ratio, reflecting signal clarity
BANDWIDTH	Frequency range for data transmission in a communication network

2.2.7 Console

This section provides detailed information about the console, allowing you to manage and monitor console-related settings. To view information specific to a particular console, click "Console1" or "Console2" to switch to the details of the corresponding console. For configuring the serial port settings, click "Setup" to be directed to the serial port configuration page, where you can adjust settings such as baud rate, data bits, and other serial communication parameters.



Field Name	Description
Baud Rate	Data transmission rate. It can be adjusted according to the connected device, but must match the baud rate of the connected equipment.
Data Bits	Number of binary bits in transmitted data. The default is usually 8 bits, but it can be modified if required by the connected device.
Devices	Number of currently connected devices.
Parity	Displays the parity mode in use.
Stop Bits	Number of stop bits marking the end of transmitted data.

2.3 Network

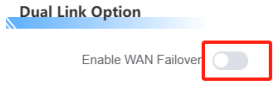
2.3.1 WAN

2.3.1.1 WAN Configure

The WAN Configure page is designed to set up the WAN network interfaces, allowing the device to connect to external networks. This configuration ensures the device can establish communication with wider networks, enabling internet access or connections to other remote systems.

- **Dual Link Option**

The Dual Link Option is used to configure the double-link switch settings. This feature allows the device to manage and switch between two network connections, providing enhanced reliability and failover support for uninterrupted connectivity. It ensures the device can automatically switch to an alternate link if one fails, maintaining continuous network service.



Field Name	Description
Enable WAN Failover	**ON:** When enabled, the router automatically switches to the standby link if the main link fails. **OFF:** When disabled, the router will not switch to the standby link if the main link fails.
Dual Both Online	**ON:** Both links (e.g., 4G and wired) remain active simultaneously, supporting high-bandwidth applications or multi-link collaboration. **OFF:** Only one link remains active at a time, preventing simultaneous connectivity.
Load Balancer	**ON:** The router dynamically distributes network traffic across available links to optimize performance and prevent congestion. **OFF:** Traffic is not automatically distributed, and load balancing is disabled.

- **Main**

This page Is used to set up the relevant parameters of the main link.

Field Name	Description
Connection Type	Selects the primary link connection method (SIM1 or SIM2).
Username	Enter the network authentication username if required.
Password	Enter the password for network authentication.
APN	Specifies the access point name for the mobile network.
PIN Code	The SIM card's personal identification number.
DNN Enable	Toggle to enable or disable the Dedicated Network Name (DNN) function.
Keep Online Detection	Selects the method for monitoring and maintaining network connectivity.
Detection Interval	Sets the interval (in seconds) for connectivity checks.
Main Detection IP	The primary server IP is used for network status detection.
Backup Detection IP	The backup server IP is used for network status detection.

- **Backup**

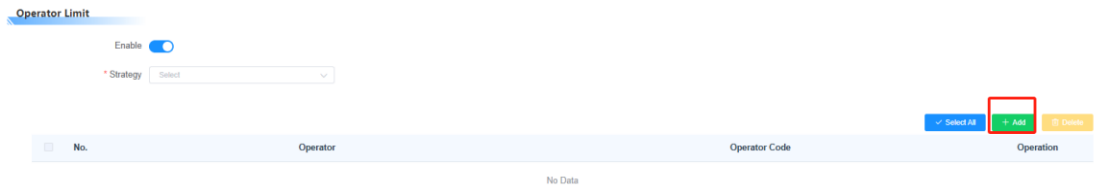
Field Name	Description
Connection Type	Selects the primary link connection method (SIM1 or SIM2).
Keep Online Detection	Chooses the method for monitoring and maintaining network connectivity.
Detection Interval	Sets the time interval (in seconds) for connectivity checks.
Main Detection IP	IP address of the primary server for network status detection.

Backup Detection IP	IP address of the backup server for network status detection.

2.3.1.2 Global Setting

Field Name	Description
Force Net Card Mode	Sets the network card's operating mode. "Auto" allows the system to automatically detect and select the optimal mode.
MTU	Defines the maximum data packet size (in bytes) for network transmission.
Assign WAN Port to Switch	A toggle option. When enabled, the WAN port functions as a switch port, allowing multiple device connections. When disabled, it operates as a standard WAN port.

2.3.1.3 Operator Limit

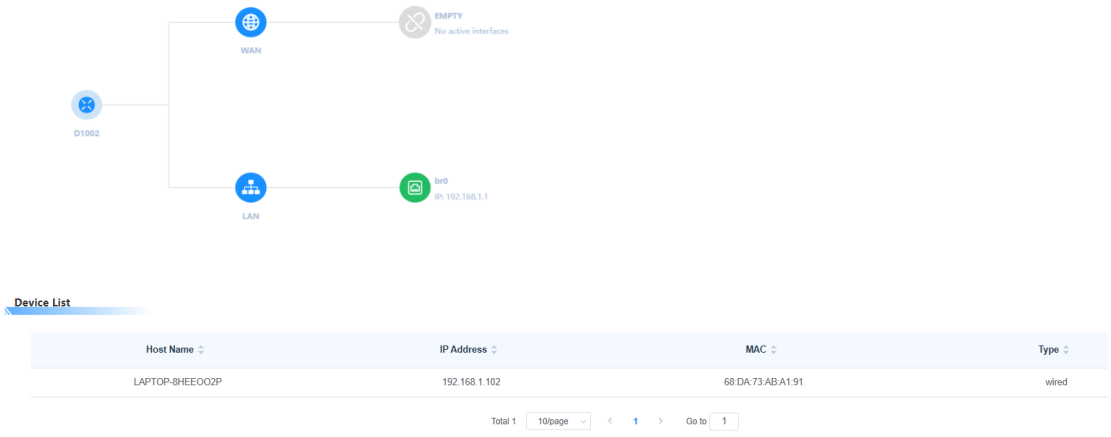


Click the Add button to add the corresponding carrier information.

Field Name	Description
Enable	A toggle option. When enabled, the operator restriction function manages network access based on the defined strategy. When disabled, no restrictions are applied.
Strategy	Defines the operator restriction method. In "Blacklist" mode, blocked operators cannot access the network. In "Whitelist" mode, only approved operators are allowed access.

2.3.1.4 Topology

Supports viewing the device network topology and list of connected devices.



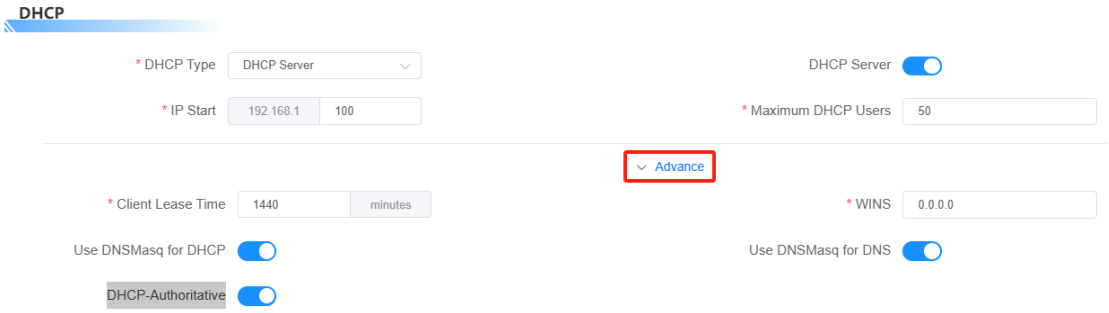
2.3.2 LAN

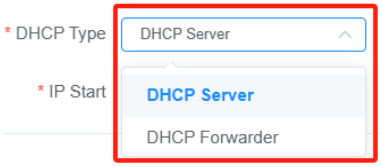
This page is used to configure LAN network interfaces, enabling devices to connect to the local area network.

- **Router IP**

Field Name	Description
LAN IP	The router's IP address within the local network (LAN), allowing devices to access the router's management interface.
Mask	The subnet mask for this interface, distinguishing between the network and host portions of the IP address.
Gateway	The exit IP address for LAN devices accessing the external network; ensure the correct gateway address is set for proper external access.
Local DNS	Used to resolve domain names to IP addresses, requiring a valid DNS server address for correct resolution.

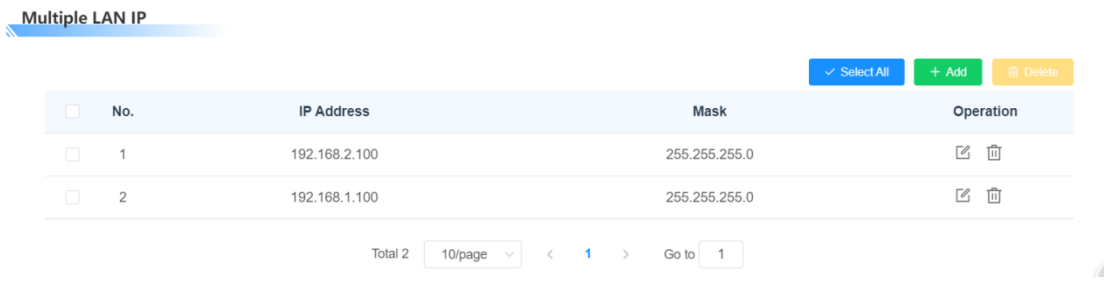
- **DHCP**



Field Name	Description
DHCP Type	 Select the router's DHCP service type. "DHCP Server" allows the router to automatically assign network parameters such as IP address to connected devices. "DHCP Forwarder" acts as a relay agent to forward DHCP messages. When selected, you must manually enter the destination DHCP server address.
DHCP Server	**ON（default）:** The router acts as a DHCP server, automatically allocating IP addresses, subnet masks, gateways, and other network settings to connected devices. **OFF:** The router does not assign network configuration parameters to devices.
IP Start	The starting IP address for the DHCP server to assign to devices.
Maximum DHCP Users	The maximum number of devices that the DHCP server can assign IP addresses to.
Client Lease Time	The duration for which a device can use the IP address assigned by the DHCP server, after which the lease must be renewed.
WINS	Used to resolve NetBIOS names within the local network.
Use DNSMasq for DHCP	**ON:** Uses DNSMasq to manage DHCP services, providing enhanced flexibility and configuration options. **OFF:** Disables DNSMasq and uses the default system

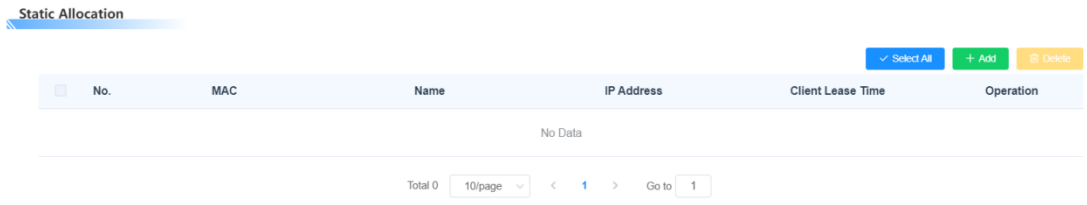
Use DNSMasq for DNS	DHCP management mode. **ON:** Uses DNSMasq for domain name resolution, enabling local domain name caching and faster resolution speeds. **OFF:** Disables DNSMasq and uses the default system DNS resolution method.
DHCP-Authoritative	When enabled, the router is authoritative for IP address assignments, and any non-authoritative DHCP servers will be ignored.

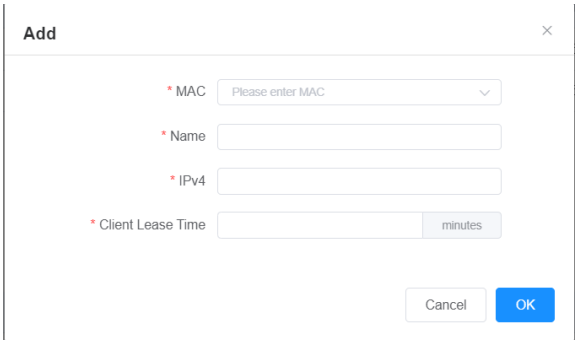
- **Multiple LAN IP**



Allows you to add and manage multiple LAN IP addresses and subnet masks, enabling devices within corresponding IP segments to connect to the network.

- **Static Allocation**





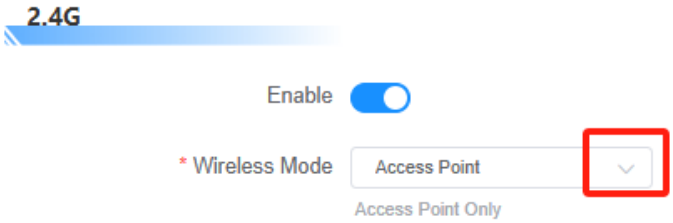
Enables selection of the MAC address of a connected device, with options to customize its name, IP address, and the duration for which the assigned IP is valid.

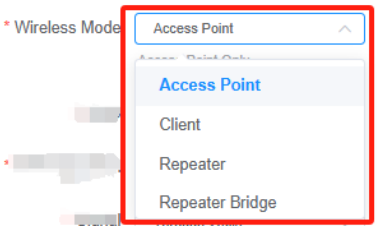
2.3.3 WIFI

The Wi-Fi Configuration page allows you to set up wireless settings for device interconnection and internet access via Wi-Fi.

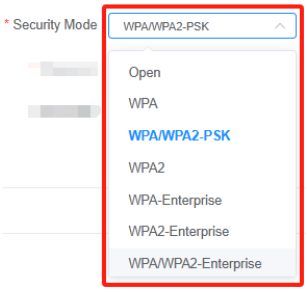
2.3.3.1 WIFI Configure

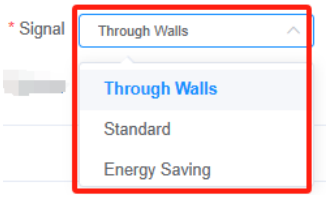
Set up WIFI mode.

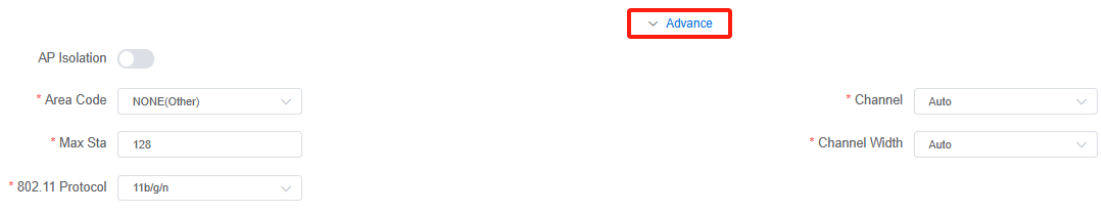


Field Name	Description
Enable	**ON:** Activates the 2.4G wireless network, allowing the device to transmit signals in the 2.4G frequency band for other devices to connect. **OFF:** Disables the 2.4G wireless network, stopping the device from transmitting signals in the 2.4G frequency band.
Wireless Mode	 **Access Point**: Allows other devices (e.g., mobile phones, computers) to connect to the router's wireless network for internet access. **Client**: The device acts as a wireless client, connecting to other WiFi networks and accessing the internet through them. **Repeater**: Receives an existing WiFi signal and retransmits it, extending the coverage of the current wireless network. **Repeater Bridge**: Expands WiFi coverage and creates a bridge

	between multiple network devices, enabling communication across different regions within the same local area network.

Field Name	Description
SSID	The name of the wireless network.
Security Mode	Used to set the security protection type of the 4G router's wireless network.  **Open:** No encryption, allowing open access to the wireless network. **WPA**: Wi-Fi Protected Access, a wireless security standard using dynamic key generation. **WPA/WPA2-PSK**: A common encryption method for home networks where a shared password is required for devices to connect. **WPA2**: An upgraded version of WPA, providing stronger security with advanced encryption protocols (e.g., AES). **WPA-Enterprise**: Used in large-scale networks, it requires a RADIUS server for user authentication, offering robust security but more complex settings. **WPA2-Enterprise**: Combines WPA2 encryption with enterprise-level authentication via a RADIUS server, suitable for high-security environments. **WPA/WPA2-Enterprise**: A combination of WPA/WPA2

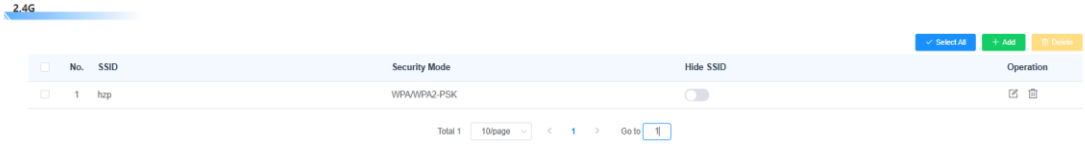
	encryption with enterprise-level authentication, requiring a RADIUS server for user verification.
WPA Algorithm	The encryption algorithms used for securing wireless network data.
Password	The WiFi password used for authentication when connecting to the wireless network.
Signal	The related setting options of WiFi signal are used to adjust the output mode of WiFi signal.  **Through Walls**: Enhances transmission power to improve signal penetration through obstacles like walls, expanding coverage but potentially increasing power consumption. **Standard**: Default transmission power, balancing signal strength, coverage, and power consumption. **Energy Saving**: Reduces transmission power to conserve energy, which may reduce signal strength and coverage area.
Hide SSID	**ON:** Disables broadcasting the wireless network name (SSID), requiring manual entry of the SSID for connection, enhancing security and network concealment. **OFF:** The SSID is actively broadcasted, making it easy for users to find and connect to the network.
MAC Filtering	When disabled, any device can attempt to connect to the network. When enabled, devices with specific MAC addresses can be allowed or denied access, improving network access control.



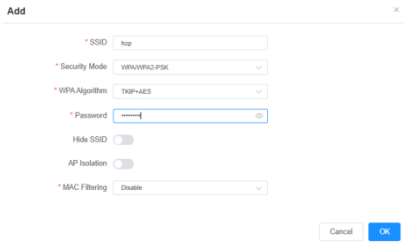
Field Name	Description
AP Isolation	**ON:** The 2.4G wireless network operates independently, without interference from other frequency bands or functions. **OFF:** The 2.4G wireless network may work in coordination with other frequency bands or functions, depending on the overall device configuration.
Area Code	Specifies the regional standard applicable to the wireless network.
Channel	Represents the path for wireless network data transmission. In automatic mode, the router selects the least interfered channel for optimal data transmission based on the surrounding network environment.
Max Sta	The maximum number of devices that can simultaneously connect to this 2.4G wireless network.
Channel Width	Referring to the transmission bandwidth of the channel. In automatic mode, the router adjusts the channel bandwidth based on the network environment and device capabilities to enhance network performance.
802.11 Protocol	Defines the communication standards for wireless networking.

2.3.3.2 Virtual Interface

Multiple virtual interfaces can be created, with each one representing a distinct subnetwork or network service.

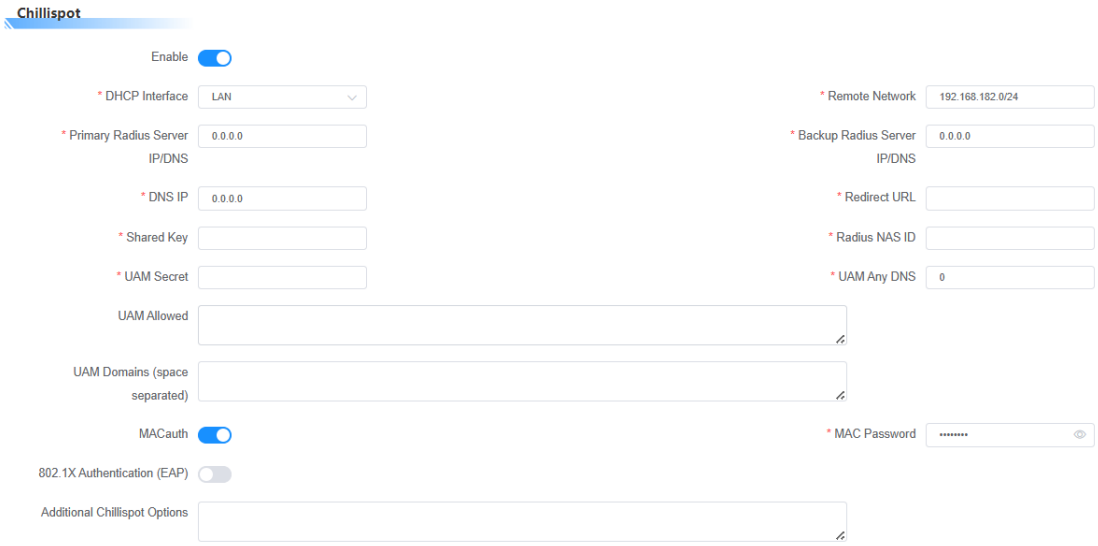


Field Name	Description
+ Add	Used to add virtual interface, See for content settings ("WiFi" page)

	
Select All	One click all choice
Delete	Delete the selected entry

2.3.3.3 Chillispot

It is an open-source hotspot management system for managing and controlling wireless network access. This page provides its configuration interface.



Field Name	Description
Enable	**ON:** Activates the Chillispot function, enabling user management and authentication for the router's wireless network. **OFF:** Disables Chillispot, and network access management will not be handled through it.
DHCP Interface	Defines the network interface used for Dynamic Host Configuration Protocol (DHCP).

Remote Network	Specifies the address range of a remote network, allowing control over device access within a specific range.
Primary Radius Server IP/DNS	Sets the IP or DNS address of the primary RADIUS server, which handles user authentication, authorization, and accounting. The default 0.0.0.0 indicates it is not configured.
Backup Radius Server IP/DNS	Defines the IP or DNS address of the backup RADIUS server. If the primary server fails, authentication switches to the backup. The default 0.0.0.0 indicates it is not configured.
DNS IP	Specifies the IP address of the DNS server for domain name resolution, enabling devices to access internet resources.
Redirect URL	Redirects users to this URL when authentication fails or access to specific resources is restricted, typically an authentication or notification page.
Shared Key	A security key for encrypted communication with the RADIUS server, ensuring secure and consistent data transmission.
Radius NAS ID	A unique identifier for the Network Access Server (NAS) in the RADIUS system, used for device recognition and management.
UAM Secret	A security key associated with the User Access Manager (UAM) to enhance user access protection.
UAM Any DNS	Defines whether UAM permits the use of any DNS server.
UAM Allowed	Enables or disables the User Access Manager (UAM) function, with configuration options available in the input field.
UAM Domains (Space separated)	Specifies a space-separated list of domains permitted by UAM for network access.
MACauth	**ON:** Enables MAC address-based authentication, allowing only pre-approved devices to connect. **OFF:** Disables MAC-based authentication, allowing alternative connection methods.
MAC Password	The authentication password used when MACauth is enabled.
802.1X Authentication (EAP)	**ON:** Activates 802.1X and EAP authentication for port-based network access control, improving security.

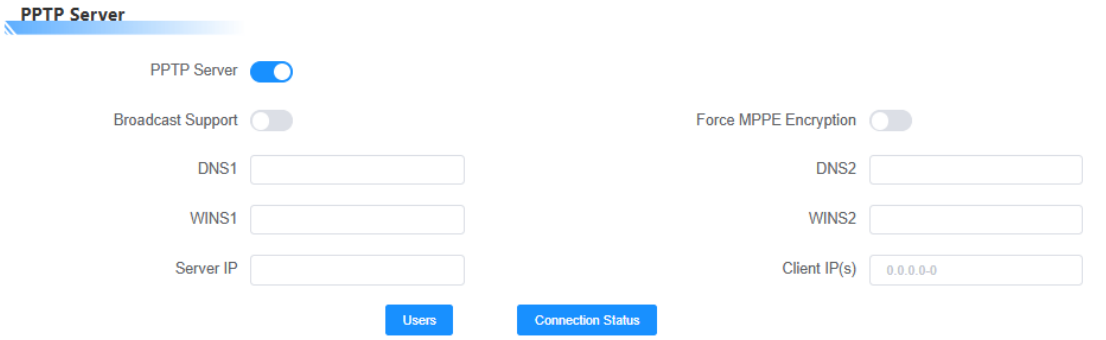
	OFF: Disables 802.1X and EAP authentication.
Additional Chillispot Options	Allows input of additional Chillispot configuration parameters as required by the system.

2.3.4 VPN

The VPN Configuration page is used to set up a Virtual Private Network (VPN), creating a secure private network over a public network. It enables encrypted communication for remote access and secure data transmission.

2.3.4.1 PPTP

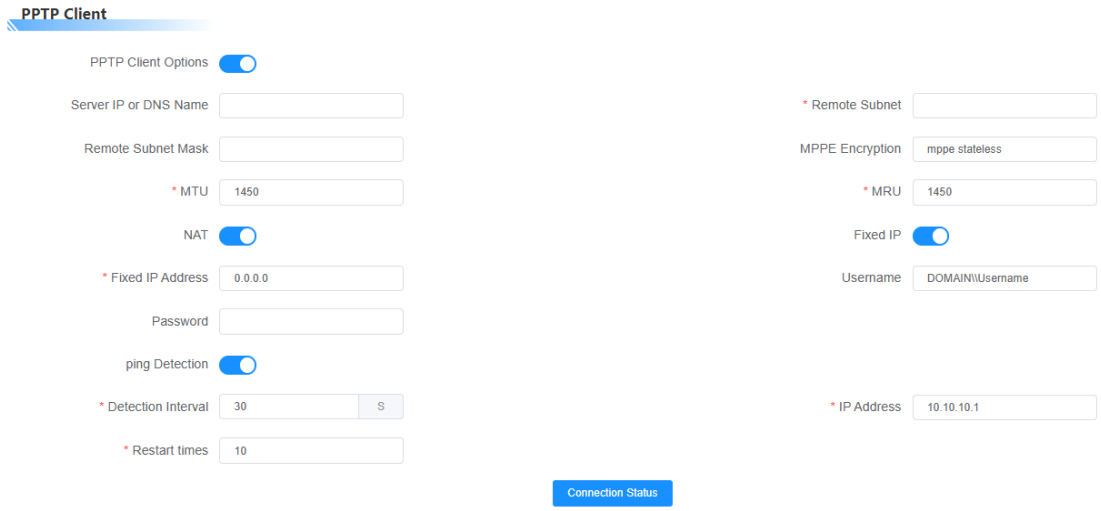
- **PPTP Server**



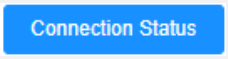
Field Name	Description
PPTP Server	Enable or disable the PPTP server.
Broadcast Support	Enable or disable broadcast support for the PPTP server.
Force MPP Encryption	Select whether to enforce MPPE encryption for PPTP data.
DNS1 and DNS2	Set the primary and secondary DNS servers.
WINS1 and WINS2	Set the primary and secondary WINS server addresses.
Server IP	Enter the IP address of the router acting as the PPTP server. This must be different from the LAN address.
Client IP(s)	Specify the range of IP addresses assigned to PPTP clients in the format xxx.xxx.xxx.xxx-xxx.

Users	Click to access the user management interface, where you can add, delete, or manage PPTP user accounts.
Connection Status	Click to view the current PPTP server connection status, including connected clients, connection duration, and other details.

- **PPTP Client**

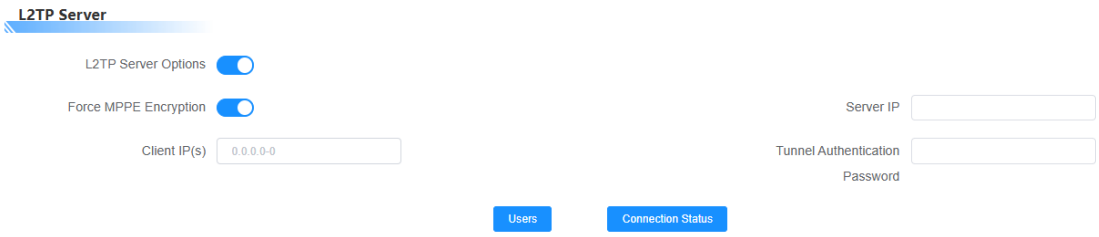


Field Name	Description
PPTP Client Options	**ON:** Enables the PPTP client, allowing the router to connect to a remote VPN server via the PPTP protocol. **OFF:** Disables the PPTP client, preventing the router from establishing a VPN connection via PPTP.
Server IP or DNS Name	Enter the WAN IP address or DNS name of the PPTP server.
Remote Subnet	Specify the local IP address of the remote PPTP server.
Remote Subnet Mask	Define the subnet mask of the remote PPTP server.
MPPE Encryption	Enable or disable MPPE encryption for secure communication.
MTU	Set the MTU value (range: 0-1500).
MRU	Set the MRU value (range: 0-1500).
NAT	**ON:** Enables NAT, allowing multiple internal devices to

	share a public IP for VPN access. **OFF:** Disables NAT, requiring internal devices to have their own public IPs for VPN access.
Fixed IP	**ON:** Uses a fixed IP address to connect to the VPN server. The IP must be specified in Fixed IP Address. **OFF:** The VPN server dynamically assigns an IP address.
Fixed IP Address	Enter the fixed IP address to be used when Fixed IP is enabled. A value of 0.0.0.0 indicates no fixed IP is set.
Username	Enter the username authorized by the PPTP server.
Password	Enter the corresponding password for the PPTP server username.
Ping Detection	**ON:** Enables periodic ping detection, allowing the router to monitor VPN connection status. **OFF:** Disables ping detection.
Detection Interval	Set the time interval for ping detection (e.g., 30 seconds means a ping request is sent every 30 seconds).
IP Address	Displays the IP address assigned to the router by the VPN server.
Restart Times	Specifies the number of automatic reconnection attempts if the VPN connection is interrupted (e.g., 10 attempts).
	Click to view the current PPTP client connection details.

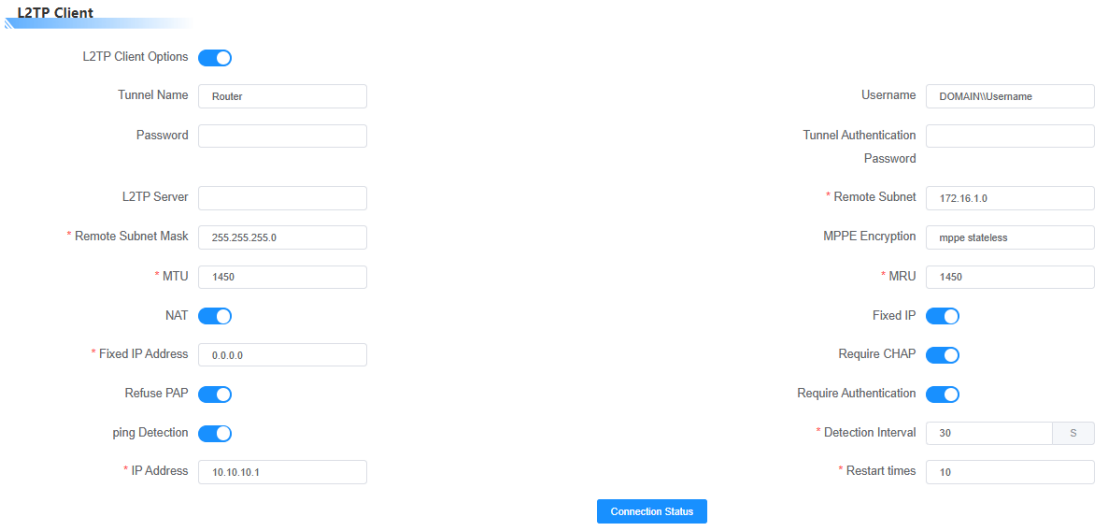
2.3.4.2 L2TP

- **L2TP Server**



Field Name	Description
L2TP Server Options	**ON:** Enables the L2TP server, allowing clients to connect to the router's VPN service via the L2TP protocol. **OFF:** Disables the L2TP server, preventing clients from connecting via L2TP.
Force MPPE Encryption	**ON:** Enforces MPPE (Microsoft Point-to-Point Encryption) for L2TP connections, enhancing security by preventing data theft or tampering. **OFF:** Does not enforce MPPE encryption, allowing data to be transmitted unencrypted or using other encryption methods.
Server IP	Set the IP address of the L2TP server. Clients use this address to connect. Leaving it blank may prevent the server from functioning properly.
Client IP(s)	Specify the range of IP addresses assigned to L2TP clients (format: xxx.xxx.xxx.xxx-xxx).
Tunnel Authentication Password	Set the password required for L2TP tunnel authentication. Clients must provide this password to establish a secure connection with the server.
Users	Click to access the user management interface, where you can add, delete, or manage L2TP user accounts, including usernames and passwords.
Connection Status	Click to view the current L2TP server connection details.

- **L2TP Client**



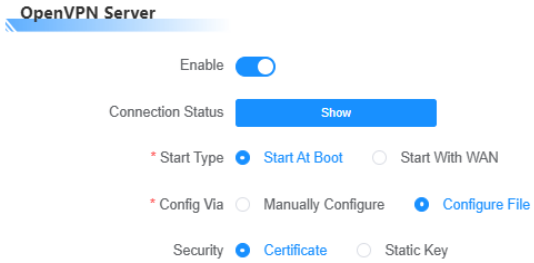
Field Name	Description
L2TP Client Options	**ON:** Enables the L2TP client, allowing the router to connect to a remote VPN server via the L2TP protocol. **OFF:** Disables the L2TP client, preventing the router from establishing an L2TP VPN connection.
Tunnel Name	Specify a name for the L2TP tunnel to identify this VPN connection.
Username	Enter the username for connecting to the remote L2TP server, in the format DOMAIN\username, where "DOMAIN" is the domain name and "username" is the account name.
Password	Enter the password corresponding to the username for authentication with the remote L2TP server.
Tunnel Authentication Password	An additional password required to establish the L2TP tunnel, enhancing connection security.
L2TP Server	Enter the IP address or domain name of the remote L2TP server.
Remote Subnet	Specify the IP address of the remote L2TP server.
Remote Subnet Mask	Specify the subnet mask of the remote L2TP server.
MPPE Encryption	Choose whether to enable MPPE encryption for secure data transmission.
MTU	Set the Maximum Transmission Unit (MTU) (range: 0-1500).

MRU	Set the Maximum Receive Unit (MRU) (range: 0-1500).
NAT	**ON:** Enables NAT, allowing multiple internal devices to share a public IP for VPN access. **OFF:** Disables NAT, requiring internal devices to use their own public IPs for VPN access.
Fixed IP	**ON:** Uses a fixed IP address for VPN connection. Specify the IP in Fixed IP Address. **OFF:** The VPN server dynamically assigns an IP address.
Fixed IP Address	Enter the fixed IP address if Fixed IP is enabled. 0.0.0.0 indicates no IP is set.
Require CHAP	**ON:** Enforces CHAP (Challenge-Handshake Authentication Protocol) for secure authentication. **OFF:** Does not enforce CHAP.
Refuse PAP	**ON:** Rejects PAP (Password Authentication Protocol) due to its lower security (plaintext password transmission). **OFF:** Allows PAP authentication.
Require Authentication	**ON:** Requires authentication when connecting to the L2TP server. **OFF:** Does not enforce authentication (may pose security risks).
Ping Detection	**ON:** Enables periodic ping requests to monitor VPN connection status. **OFF:** Disables ping detection.
Detection Interval	Set the interval for ping detection (default: 30 seconds).

IP Address	Displays the IP address obtained from the VPN connection.
Restart times	Set the number of automatic reconnection attempts when the VPN disconnects (default: 10 times).
Connection Status	Click to check the L2TP client's current connection status.

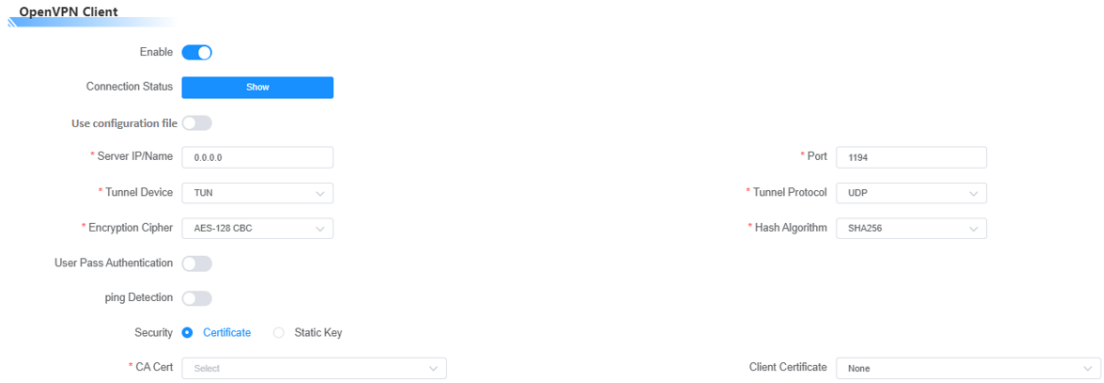
2.3.4.3 OPENVPN

- **OpenVPN Server**



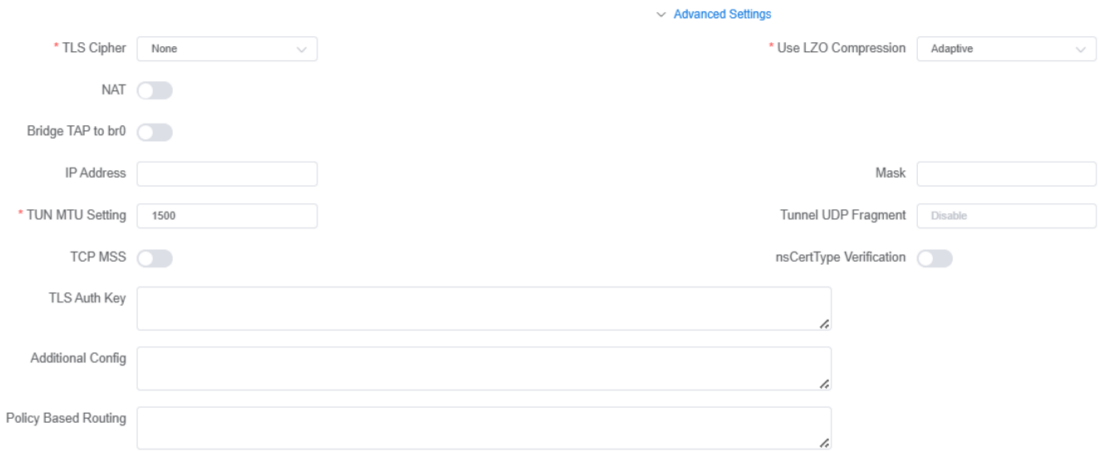
Field Name	Description
Enable	**ON:** Activates the OpenVPN server, allowing clients to connect via the OpenVPN protocol. **OFF:** Disables the OpenVPN server, preventing client connections.
Connection Status	Click "Show" to view the current OpenVPN server connection status.
Start Type	**Start at Boot**: Automatically starts the OpenVPN server when the router boots. **Start with WAN**: Starts the OpenVPN server when the WAN connection is established.
Config Via	**Manual Configure**: Manually set OpenVPN server parameters. **Configure File**: Upload a pre-configured file for easier setup, ideal when a configuration template is available.
Security	**Certificate**: Uses Certificate Authority (CA)-issued certificates for authentication, ensuring high security. **Static Key**: Uses a static key for authentication, offering simpler configuration but lower security compared to certificates.

- **OpenVPN Client**



Field Name	Description
Enable	**ON:** Activates the OpenVPN client, allowing the router to connect to a remote server via OpenVPN. **OFF:** Disables the OpenVPN client, preventing connections.
Connection Status	Click "Show" to view the current OpenVPN client connection status.
Use Configuration File	**ON:** Import a pre-configured file for easier setup. **OFF:** Manually configure each parameter.
Server IP/Name	Enter the IP address or domain name of the remote OpenVPN server. A value of "0.0.0.0" indicates it is not set.
Port	Specify the port for connecting to the OpenVPN server. The default is **1194**, commonly used by OpenVPN.
Tunnel Device	**TUN**: Uses a virtual IP-layer tunnel, suitable for most IP-based applications. **TAP**: Uses a virtual Ethernet tunnel, simulating an Ethernet interface.
Tunnel Protocol	**UDP**: Fast and low-overhead, ideal for real-time applications. Commonly used with OpenVPN. **TCP**: Reliable and connection-oriented, suitable for scenarios requiring high data accuracy.
Encryption Cipher	Specifies the algorithm for encrypting data.
Hash Algorithm	Defines the algorithm for data integrity verification and

	authentication.
User Pass Authentication	**ON:** Requires a username and password for authentication. **OFF:** Disables username-password authentication, using other methods like certificates.
Ping Detection	**ON:** Enables periodic ping requests to monitor connection status. **OFF:** Disables ping detection.
Security	**Certificate**: Uses CA-issued certificates for authentication, ensuring high security. **Static Key**: Uses a static key for authentication, simpler but less secure than certificates.
CA Cert	Required when using Certificate mode. Select an existing CA certificate to verify the server and client credentials.
Client Certificate	A digital certificate used for client authentication and encrypted communication.



Field Name	Description
TLS Cipher	Specifies the encryption algorithm used for TLS (Transport Layer Security) protocol.
Use LZO Compression	**Adaptive:** Automatically adjusts LZO compression based on network conditions to optimize data transmission. **YES:** Forces the use of LZO compression for data transmission.

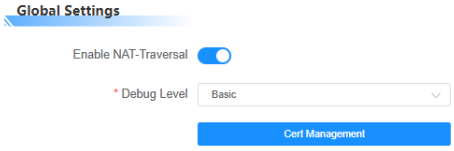
	Disable: Disables LZO compression. **NO:** Disables LZO compression (same as "Disable").
NAT	**ON:** Enables NAT, allowing internal devices to share a public IP for VPN access. **OFF:** Disables NAT, requiring internal devices to have their own public IPs for VPN access.
Bridge TAP to br0	**ON:** Bridges the TAP virtual Ethernet device to the br0 bridge, enabling flexible network connections and data forwarding. **OFF:** Disables TAP-to-br0 bridging.
IP Address	Manually set the IP address for the OpenVPN connection.
Mask	Defines the subnet mask for the assigned IP address, determining network and host address segmentation.
TUN MTU Setting	Sets the Maximum Transmission Unit (MTU) for the TUN virtual network device. The default value is 1500 bytes. Proper MTU settings help avoid packet fragmentation and improve transmission efficiency.
Tunnel UDP Fragment	**Enable:** Allows UDP fragmentation when necessary. **Disable:** Disables UDP fragmentation.
TCP MSS	**ON:** Sets the Maximum Segment Size (MSS) for TCP connections to optimize performance. **OFF:** Disables TCP MSS configuration.
nsCertType Verification	**ON:** Enables certificate type verification to enhance connection security. **OFF:** Disables certificate type verification.
TLS Auth Key	Enter the TLS authentication key for protocol authentication and encryption.
Additional Config	Allows entering custom OpenVPN client configuration parameters based on specific requirements.

Policy Based Routing	Define policy-based routing rules to control network traffic based on specified policies.

2.3.4.4 IPSEC

- **Global Settings**

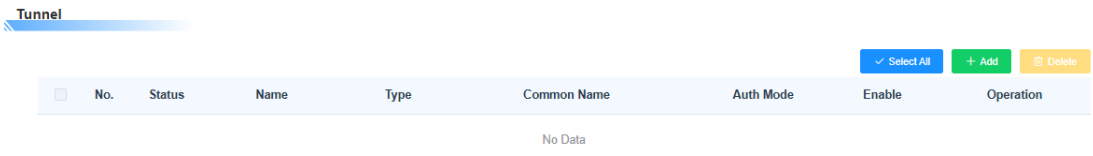
Configure general parameters affecting the overall IPsec



Field Name	Description
Enable NAT-Traversal	**ON:** Enables NAT-Traversal, allowing IPsec to function properly in networks with Network Address Translation (NAT), ensuring compatibility. **OFF:** Disables NAT-Traversal. IPsec connections may fail if a NAT device is present in the network.
Debug Level	**Basic**: Records key debug information for initial troubleshooting. **Close:** Captures more detailed logs for in-depth debugging.
Cert Management	Click to access the certificate management interface, where you can import, export, view, or delete IPsec-related certificates to ensure connection security.

- **Tunnel**

Manage IPsec tunnel configurations.

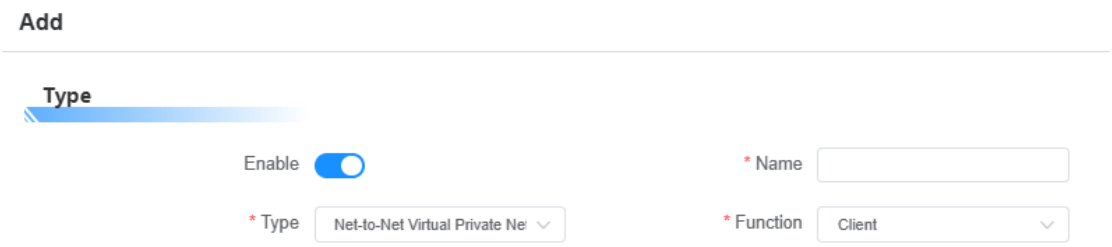


Field Name	Description
Select All	Selects all IPsec tunnel entries on the current page for batch operations.
Add	Opens the interface to create a new IPsec tunnel configuration.

Delete	Deletes the selected IPsec tunnel configurations.

- **Add**

Adding IPsec tunnel configurations



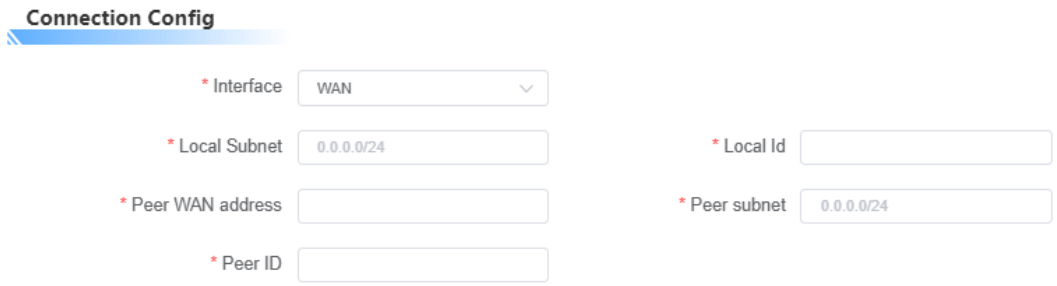
- **Type**

Type configurations

Field Name	Description
Enable	**ON:** Activates the IPsec tunnel, allowing secure connections to be established. **OFF:** Disables the tunnel, preventing it from being used even if configured.
Name	Assign a unique name to identify and manage the IPsec tunnel.
Type	**Net-to-Net VPN**: Connects two separate networks, enabling site-to-site VPN communication. **Host-to-Host VPN (RoadWarrior):** Establishes a secure connection between a single device and another host, typically a corporate VPN server.
Function	**Client**: The tunnel operates as a client, initiating connections to a remote VPN server **Server:** The tunnel acts as a server, handling incoming client connections for secure communication.

- **Connection Config**

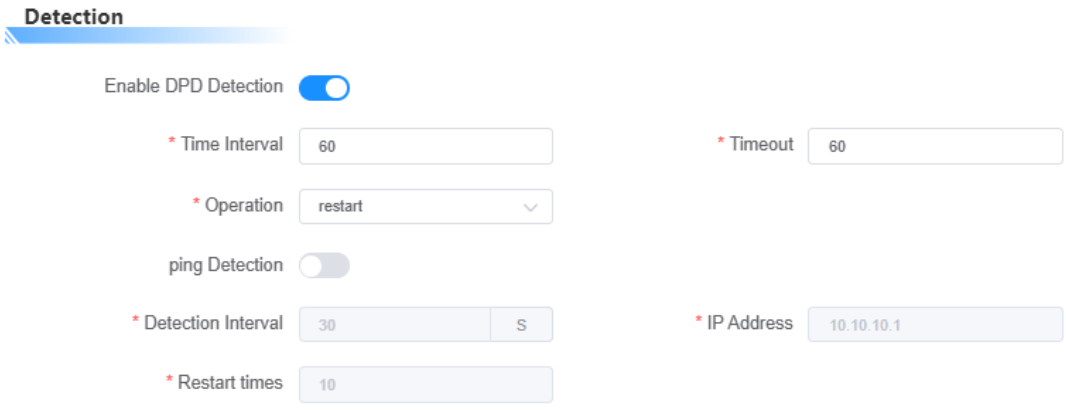
For the connection configuration



Field Name	Description
Interface	Select the network interface used for the IPsec connection.
Local Subnet	Define the subnet address and mask of the local network.
Local ID	Identifies the local device in the IPsec connection for authentication and communication.
Peer WAN address	Enter the public IP address of the remote device (e.g., VPN server) to establish the IPsec connection.
Peer Subnet	Specify the subnet address and mask of the remote network.
Peer ID	Identifies the remote device in the IPsec connection for authentication and communication.

- **Detection**

Detection configuration

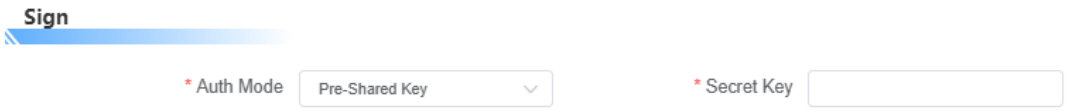


Field Name	Description
Enable DPD Detection	**ON:** Activates Dead Peer Detection (DPD) to monitor the availability of the remote device. **OFF:** Disables DPD detection.

Time Interval	Defines the interval between DPD detection attempts.
Timeout	Sets the maximum wait time before marking the peer as unreachable.
Operation	**Hold**: Maintains the current connection status when an issue is detected, requiring manual intervention or further detection. **Restart**: Automatically attempts to restart the IPsec tunnel upon connection failure. **Clear**: Clears the current connection status to prepare for re-establishing the connection. **Restart by Peer**: Requests the remote device to restart the connection when an issue is detected.
Ping Detection	**ON:** Enables ping detection, allowing the router to send regular ping requests to monitor connectivity. **OFF:** Disables ping detection.
Detection Interval	Sets the frequency of ping detection.
IP Address	Specifies the target IP address for ping requests.
Restart times	Defines the number of automatic reconnection attempts after a connection failure.

- **Sign**

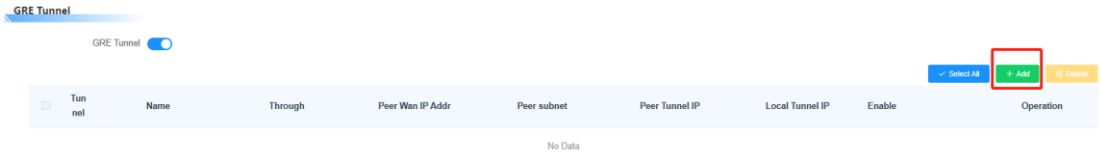
Sign configuration



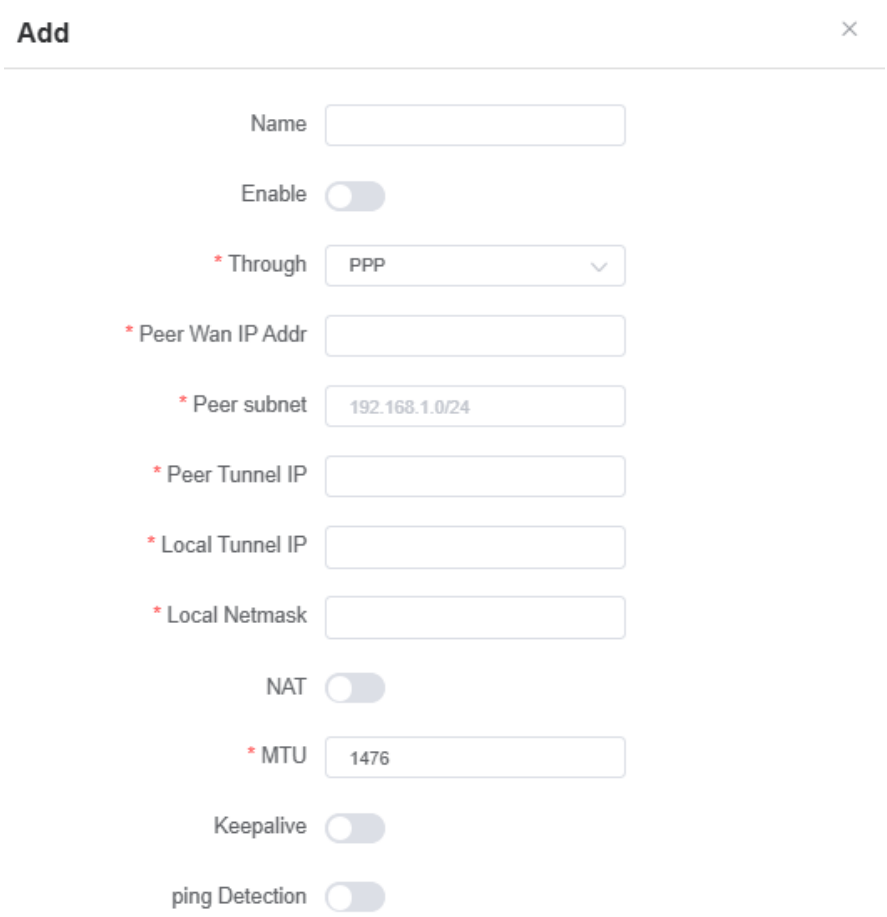
Field Name	Description
Auth Mode	**Pre-Shared Key**: Uses a shared secret key for authentication. Both parties must configure the same key to establish a secure connection. **X.509 Certificate:** Utilizes X.509 digital certificates for authentication, ensuring identity verification through certificates issued by a Certificate Authority (CA).

2.3.4.5 GRE

Add the GRE Tunnel



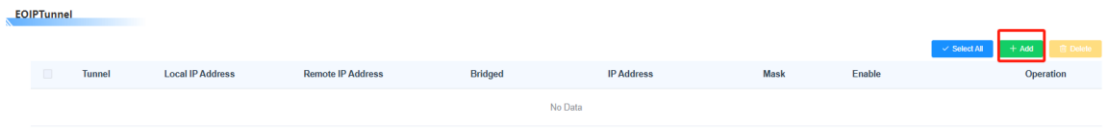
Field Name	Description
GRE Tunnel	**ON:** Activates the GRE tunnel function. **OFF:** Disables the GRE tunnel function.
Select All	Selects all displayed GRE tunnel configuration entries for batch operations.
+ Add	Opens the interface to create a new GRE tunnel configuration.
Delete	Removes the selected GRE tunnel configuration entries.



Field Name	Description
Name	Assign a unique name to the GRE tunnel for easy identification and management.
Enable	**ON:** Activates the GRE tunnel, allowing data transmission. **OFF:** Disables the tunnel, preventing data transmission even if other parameters are configured.
Through	**PPP**: Encapsulates and transmits GRE tunnel data via the Point-to-Point Protocol (PPP). **LAN**: Uses the local area network (LAN) for data transmission, suitable for connecting different subnets or devices within the same network. **WAN**: Establishes GRE tunnels over a wide-area network (WAN) to enable cross-regional network interconnection.
Peer Wan IP Addr	Enter the remote device's WAN IP (e.g., a router) to establish a

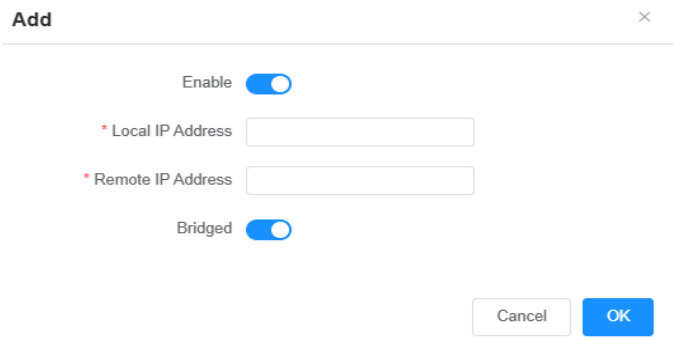
	GRE tunnel connection.
Peer subnet	Define the subnet and mask of the remote network.
Peer Tunnel IP	Set the IP address of the remote device within the GRE tunnel.
Local Tunnel IP	Configure the local device's IP address within the GRE tunnel.
Local Netmask	Specify the subnet mask for the local tunnel IP to define the network range.
NAT	**ON:** Enables NAT, allowing multiple internal devices to share a public IP for communication through the GRE tunnel. **OFF:** Disables NAT, requiring internal devices to have individual public IPs for GRE tunnel communication.
MTU	Set the maximum transmission unit (packet size) for data in the GRE tunnel.
Keepalive	**ON:** Enables periodic keepalive messages to monitor and maintain the tunnel connection. **OFF:** Disables the keepalive mechanism.
Ping Detection	**ON:** Sends periodic ping requests to a target to verify the GRE tunnel's connection status. **OFF:** Disables ping detection.

2.3.4.6 EOIP



Field Name	Description
Select All	Click to select all EOIP tunnel configuration entries on the current page for batch operations.
+ Add	Click to open the interface for creating a new EOIP tunnel configuration.

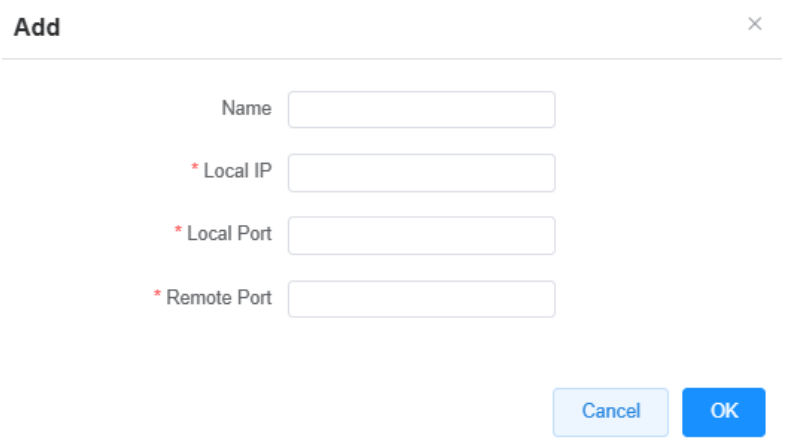
Delete	Click to remove the selected EOIP tunnel configuration entries.



Field Name	Description
Enable	**ON:** Activates the EOIP tunnel, allowing Ethernet data transmission over an IP network. **OFF:** Disables the EOIP tunnel. Even if other parameters are set, Ethernet data transmission will not occur.
Local IP Address	Specifies the local device's IP address in the EOIP tunnel, used for identification within the tunnel.
Remote IP Address	Enter the remote device's IP address in the EOIP tunnel to establish communication with the local device.
Bridged	**ON:** Bridges the EOIP tunnel with the local network, enabling seamless data forwarding and interaction. **OFF:** Disables bridging, keeping the EOIP tunnel independent from the local network. Additional routing configurations may be required for data interaction.

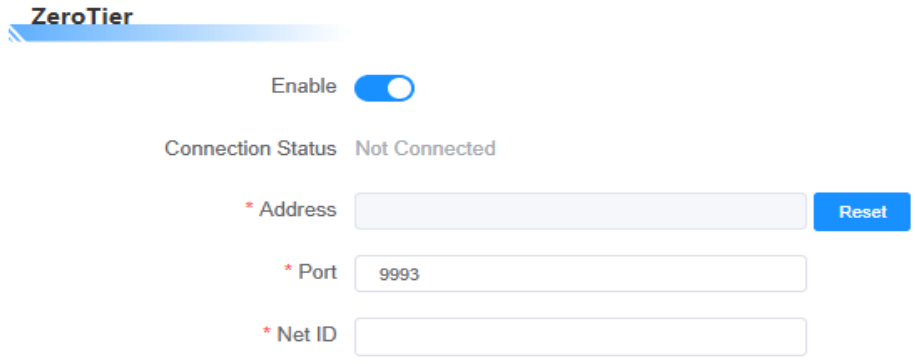
2.3.4.7 FRP

Field Name	Description
Enable	**ON:** Activates the FRPC (Fast Reverse Proxy Client) function, allowing the router to communicate with the FRP server as a client and perform reverse proxy-related services. **OFF:** Disables the FRPC function. The router will no longer act as an FRP client and cannot perform FRP-based reverse proxy operations.
FRP Server Addr	Enter the IP address or domain name of the FRP server. This address enables the router to establish a connection with the FRP server for communication.
FRP Server Port	Specifies the port number on which the FRP server listens. The router will use this port for communication, matching the listening port configured on the server.
FRP Remote Token	The authentication key between the FRP client and server. The correct token is required for the FRPC to successfully connect to the FRP server and perform subsequent operations.
✓ Select All	Clicking this button selects all FRP-related configuration entries on the current page for batch actions.
+ Add	Clicking this button opens the interface for adding new FRP-related configurations.
Delete	Clicking this button deletes the selected FRP-related configuration entries.

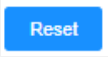


Field Name	Description
Name	Assigns a name to the current FRP configuration item for easier identification.
Local IP	Specifies the IP address of the local device (e.g., server or host). This address identifies the local service within the local network and allows FRP to forward external requests to the correct device.
Local Port	Sets the port number on which the local service listens. FRP forwards incoming external requests to this port, directing them to the appropriate local service.
Remote Port	Defines the port number on the FRP server used to map the local service. External users can access the local service by connecting to this port on the FRP server.

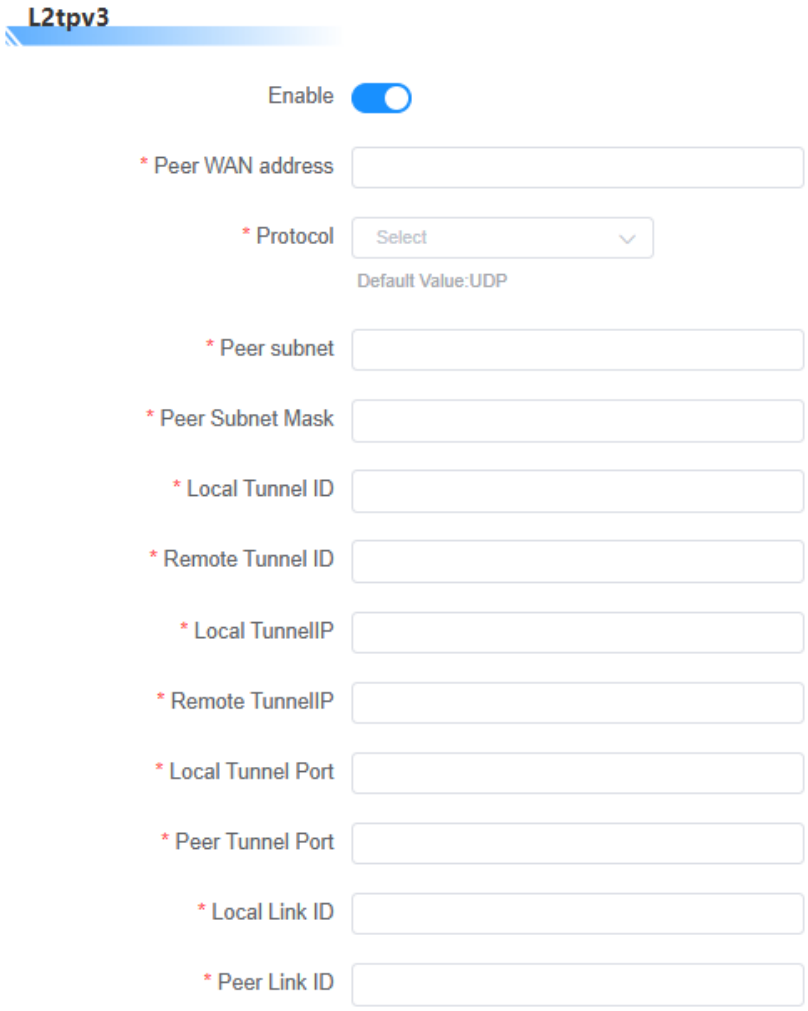
2.3.4.8 Zero Tier



Field Name	Description

Enable	**ON:** Activates the ZeroTier function, allowing the router to connect and communicate through the ZeroTier network. **OFF:** Deactivates the ZeroTier function, preventing the router from participating in any ZeroTier network operations.
Connection Status	Displays the current connection status between the router and the ZeroTier network.
Address	Specifies the address associated with the ZeroTier network.
	Clicking this button resets the "Address" field to its default unfilled state.
Port	Defines the port number used for communication with the ZeroTier network.
Net ID	The unique identifier for the ZeroTier network, used to distinguish between different ZeroTier virtual networks. Enter the correct Net ID when joining a specific network.

2.3.4.9 L2tpv3

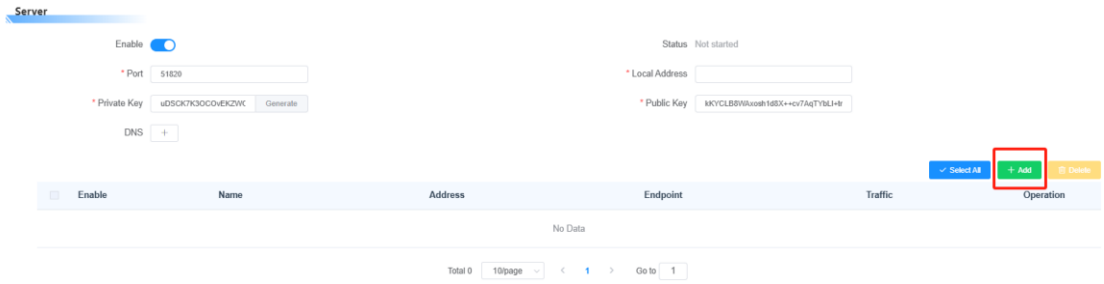


Field Name	Description
Enable	**ON:** Activates the L2TPv3 (Layer 2 Tunneling Protocol version 3) function, enabling the router to establish secure tunnel connections for data transmission. **OFF:** Deactivates the L2TPv3 function, preventing the router from performing tunnel connections or related data transmission.
Peer WAN address	Enter the wide-area network (WAN) IP address of the peer device (e.g., a remote router) to establish the L2TPv3 tunnel, which is necessary for communication between the two devices.
Protocol	Select the transmission protocol for the L2TPv3 tunnel, with UDP

	as the default option.
Peer subnet	Specifies the subnet address of the peer network, defining which peer devices can communicate through this tunnel and the scope of the peer network.
Peer Subnet Mask	Works with the "Peer Subnet" to define the network mask, further clarifying the structure and range of the peer network.
Local Tunnel ID	The IP address used by the local device in the L2TPv3 tunnel, serving as the device's identification during data transmission within the tunnel.
Remote Tunnel ID	The unique identifier for the peer device in the L2TPv3 tunnel, used alongside the local tunnel ID to manage connections and control data transmission.
Local Tunnel IP	The IP address used by the local device within the L2TPv3 tunnel, identifying the device during data transmission within the tunnel.
Remote Tunnel IP	The IP address used by the peer device within the L2TPv3 tunnel, facilitating communication with the local device.
Local Tunnel Port	The port number used by the local device to receive and transmit data in the L2TPv3 tunnel.
Peer Tunnel Port	The port number used by the peer device for L2TPv3 tunnel connections, which works with the local tunnel port to enable data interaction between both devices.
Local Link ID	The identifier for the local device at the link layer of the L2TPv3 tunnel, used for link-layer management and controlling data forwarding.
Peer Link ID	The identifier for the peer device at the link layer of the L2TPv3 tunnel, working with the local link ID to ensure proper link-layer data transmission.

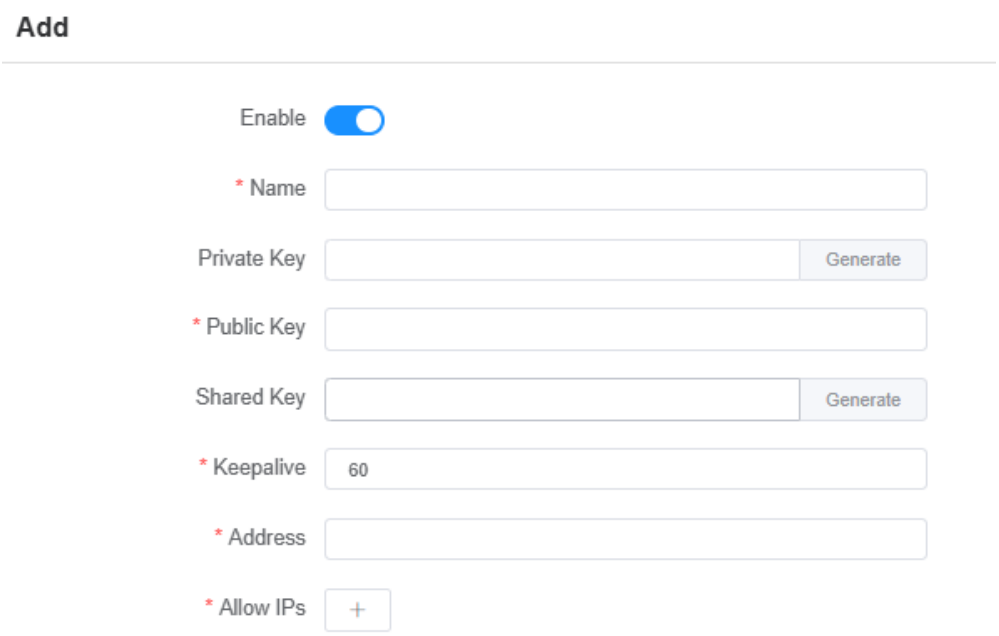
2.3.4.10 WireGuard

- **Server**



Field Name	Description
Enable	**ON:** Activates the WireGuard server function, allowing the router to operate as a WireGuard server, accept client connections, and establish secure tunnels. **OFF:** Deactivates the WireGuard server function, preventing it from accepting client connections.
Status	Displays the current operating status of the WireGuard server.
Port	Sets the port number on which the WireGuard server listens for incoming client connections.
Local Address	Specifies the WireGuard server's IP address within the local network, used to identify its location.
Private Key	The WireGuard server's private key, used for encrypting and decrypting data during communication with clients. It should be securely stored. Clicking the "Generate" button will create a new private key.
Public Key	The public key derived from the private key, used for authentication and secure key exchange with clients.
DNS	Allows specifying a DNS server address for domain name resolution within the WireGuard tunnel, facilitating access to services by domain name.
Select All	Clicking this button selects all client configuration items in the list for batch operations.
Add	Clicking this button opens the interface for adding new client configurations.
Delete	Clicking this button deletes the selected client configuration items.

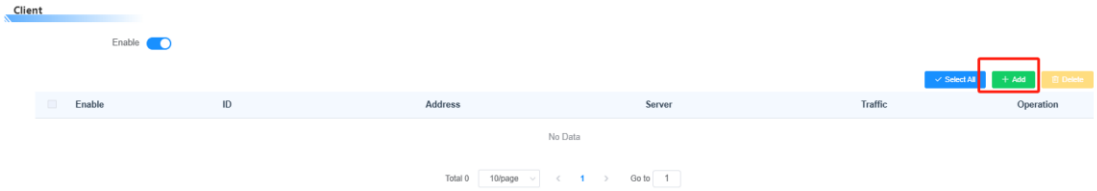
Add relevant information about the WireGuard .



Field Name	Description
Enable	**ON:** Activates the WireGuard client configuration, allowing it to establish a connection with the server. **OFF:** Deactivates the client configuration, preventing connection to the server.
Name	Sets a name for the WireGuard client configuration to facilitate identification and management of multiple connections.
Private Key	The client's private key, used for encrypting and decrypting data during communication with the server. Clicking the "Generate" button will create a new private key.
Public Key	The client’s public key, used for authentication and key exchange with the server. It must match the corresponding configuration on the server.
Shared Key	A shared key for additional encryption or authentication scenarios. Clicking the "Generate" button will create a new shared key.
Keepalive	Sets the interval for sending keepalive messages between the client and server to maintain a stable connection.
Address	Specifies the client’s IP address or domain name, used by the

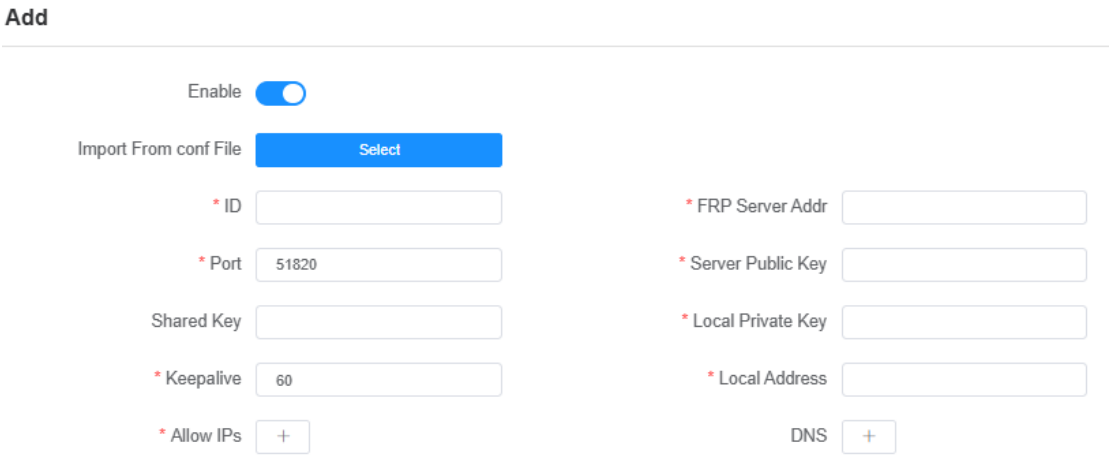
Allow IPs	server for identification and connection. Defines the IP addresses or network segments that the client is permitted to access, controlling its network reach.

- **Client**



Field Name	Description
Enable	**ON:** Activates the WireGuard client function, allowing the router to establish a secure connection with the server. **OFF:** Deactivates the WireGuard client function, preventing connection to the server.
Select All	Click this button to select all entries in the current list for batch operations.
+ Add	Click this button to open the interface for adding WireGuard server configurations.
Delete	Click this button to delete the selected entry.

Add relevant information about the WireGuard



Field Name	Description
Enable	**ON:** Activates the WireGuard server configuration. **OFF:** Deactivates the server configuration.
Import From conf File	Click "Select" to upload and import a pre-configured WireGuard server profile.
ID	Assigns a unique identifier to the WireGuard server configuration.
FRP Server Addr	Specifies the address of the FRP (Fast Reverse Proxy) server used to establish a connection.
Port	Sets the communication port for the WireGuard client to connect to the server.
Server Public Key	Enter the WireGuard server's public key for key exchange and authentication.
Shared Key	Sets a shared key for additional encryption or authentication. Click "Generate" to create a new key.
Local Private Key	The WireGuard client's private key for encrypting and decrypting data. Click "Generate" to generate a new key.
Keepalive	Defines the interval for sending keepalive messages between the client and server.
Local Address	Specifies the WireGuard client's IP address in the local network.

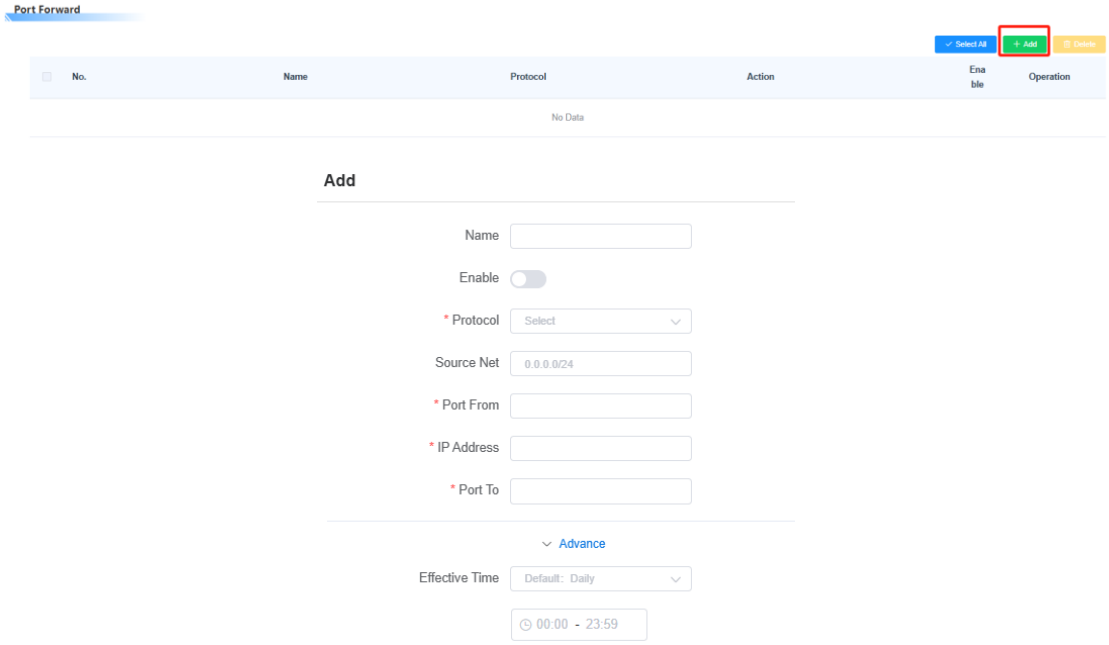
Allow IPs	Adds IP addresses or network segments that the client is permitted to access.
DNS	Configures a DNS server for domain name resolution within the WireGuard tunnel.

2.3.5 NAT

2.3.5.1 Port Forward

- **Port Forward**

Port forwarding is used to configure public network services, such as web servers, FTP servers, or other internet-based applications that require external access.

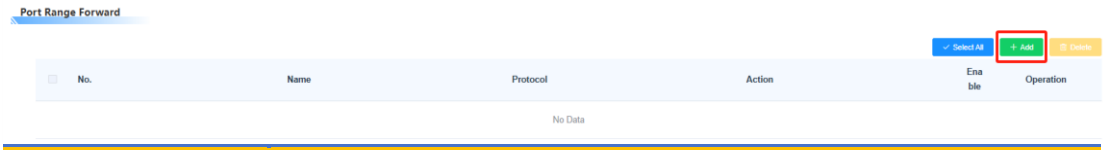


Field Name	Description
Name	Enter the application's name.
Enable	Toggle port forwarding on or off.
Protocol	Select UDP, TCP, or both for the application.
Source Net	Specify the IP addresses of internet users. For an IP range, use formats like 172.168.2.0/24, where 172.168.2.0 is the network address and 24 is the subnet mask length.
Port From	Enter the external port number used by the service.

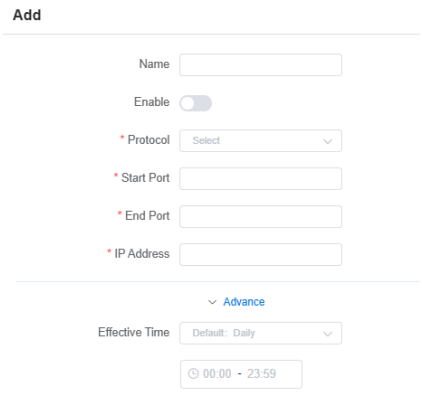
IP Address	Specify the internal IP address of the server to be accessed by internet users.
Port To	Enter the internal port number used by the service.
Effective Time	Set the time period during which the rule is active.

- **Port Range Forward**

Certain applications require a specific range of ports to be forwarded for proper functionality. When an external request targets a specified port range, the router forwards the data to the designated device. For security reasons, restrict port forwarding to only necessary ports. If a configuration is no longer needed, unchecking the "Enable" option temporarily disables the forwarding rule.

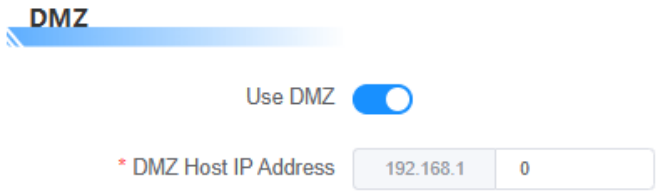


Field Name	Description
Name	Enter a name for the application.
Enable	Enable or disable port range forwarding.
Protocol	Select UDP, TCP, or both as needed.
Start Port	Specify the starting port of the forwarding range.
End Port	Specify the ending port of the forwarding range.
IP Address	Enter the internal IP address of the target server.
Effective Time	Set the active time for the forwarding rule.



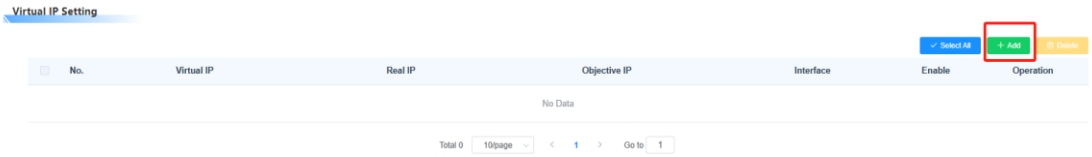
2.3.5.2 DMZ

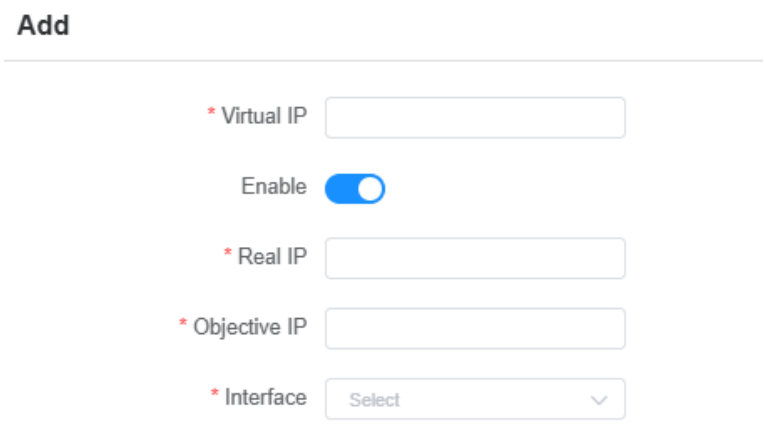
The DMZ feature allows a designated device on the network to be exposed to the Internet for specific services. A DMZ host forwards all ports to a single computer, making it accessible from the Internet. While port forwarding is a more secure option as it only opens necessary ports, enabling DMZ exposes the device to all incoming connections, increasing security risks.



Field Name	Description
Use DMZ	**ON:** Enables DMZ, exposing the specified host to the Internet. **OFF:** Disables DMZ, keeping the network more secure.
DMZ Host IP Address	Specifies the IP address of the device designated as the DMZ host, placing it between the internal and external networks for direct Internet access.

2.3.5.3 Virtual IP Setting





Field Name	Description
Virtual IP	Specifies the IP address exposed to the external network during the NAT process. It maps to the internal server's real IP, allowing external access to internal services.
Enable	**ON:** Activates DMZ functionality. **OFF:** Disables DMZ.
Real IP	The internal server's actual IP address. During NAT, it is mapped to the virtual IP, enabling the external network to access the internal server.
Objective IP	The target IP address of a server or device in the external network that needs to be accessed. NAT settings can route internal requests to this target via the virtual IP.
Interface	Select the network interface used for address translation: **lo**: Loopback interface, mainly for internal device communication and testing. **br0**: Bridging interface, used to connect multiple networks within a local area network. **wan**: Wide-area network interface, connecting to the external network (e.g., the Internet), facilitating communication between internal and external networks.

2.3.6 IPV6

- **IPV6 Support**

Field Name	Description
Enable	**ON:** Activates IPv6 support, allowing the router to process and transmit IPv6 network data. **OFF:** Disables IPv6 support, limiting the router to IPv4 networks or excluding IPv6-related services.
IPv6 Type	**Native IPv6 from ISP:** Obtains native IPv6 addresses directly from the Internet Service Provider (ISP) for network communication. **6in4 Static Tunnel:** Encapsulates IPv6 packets in IPv4 packets, enabling IPv6 communication over IPv4 networks.
Prefix Length	Defines the length of the IPv6 address prefix.
Static DNS1	Specifies the address of the primary static IPv6 DNS server for domain name resolution in the IPv6 network.
Static DNS2	Specifies the address of the secondary static IPv6 DNS server, used as a backup for domain name resolution if the first server is unavailable.
Router IPv6 Address	Sets the IPv6 address of the router itself.
Assigned / Routed Prefix	Enter the IPv6 address prefix assigned by the ISP or used for routing, essential for address management and network configuration.
MTU	Sets the maximum data packet size allowed for transmission in the IPv6 network. A typical value is 1452 bytes, which helps prevent packet fragmentation and optimize transmission efficiency.

- **Wan IPV6 address conf**

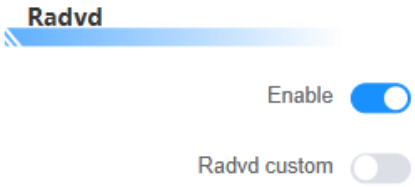
Field Name	Description
Wan IPV6 address conf	**Use Autoconf**: Automatically obtains the WAN IPv6 address through the IPv6 protocol. The router will retrieve address information from the ISP without manual configuration. **Use Autoconf (SLAAC)**: The router utilizes Stateless Address Auto-Configuration (SLAAC) to obtain network prefix information and generate an IPv6 address, typically by combining the device's MAC address. This eliminates the need for manual address configuration.
The method of getting WAN IPV6	**Use DHCPv6 Client**: Configures the router as a DHCPv6 client to dynamically receive the WAN IPv6 address and related settings from the DHCPv6 server. This method is fast and works in networks that support DHCPv6, similar to obtaining an IPv4 address via DHCP. **Use RS (Router Solicitation)**: The router sends Router Solicitation messages to request network prefix and configuration information from other routers in the network. It then generates its IPv6 address using the obtained information, as part of the stateless address autoconfiguration process.

- **Dhcp6s**

Field Name	Description
Enable	**ON:** Activates the DHCPv6 server, allowing the 4G industrial router to assign IPv6 addresses and network parameters to devices in the LAN. **OFF:** Disables the DHCPv6 server, preventing the router from allocating IPv6 addresses.

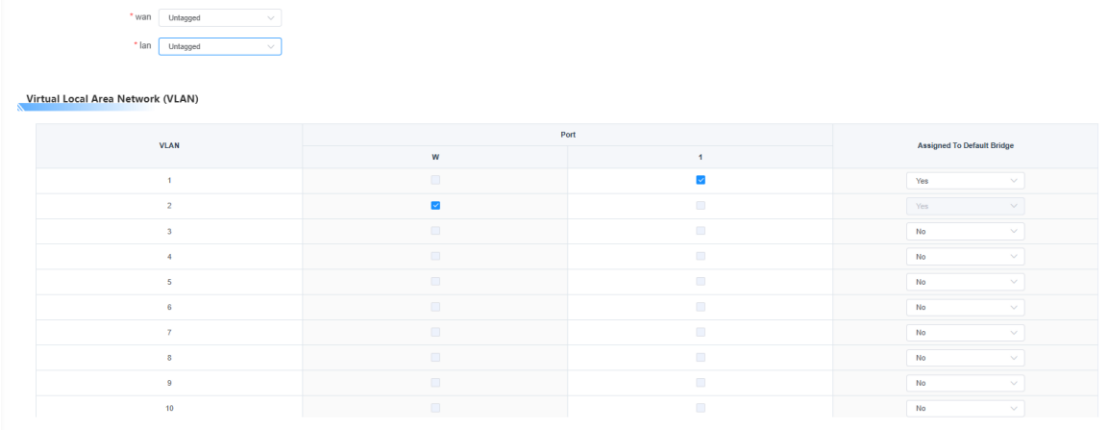
Sequential IPs	**ON:** Enables sequential allocation of IPv6 addresses for better management and planning. **OFF:** Disables sequential allocation; addresses may be assigned based on other rules.
Custom hosts	Allows specifying custom hostname-to-IPv6 address mappings for fixed address allocation or device identification.
Dhcp6s custom	**ON:** Enables custom DHCPv6 settings, allowing personalized parameter configurations. **OFF:** Uses the default DHCPv6 configuration.

- **Radvd**



Field Name	Description
Enable	**ON:** Activates the Radvd (Router Advertisement Daemon), allowing the router to send router advertisement messages in the IPv6 network, informing devices of network prefixes and routing information. **OFF:** Disables the Radvd function, and the router stops sending advertisement messages.
Dhcp6s custom	**ON:** Enables custom Radvd settings, allowing personalized adjustments for parameters like advertisement frequency and content. **OFF:** Uses the default Radvd configuration without customization.

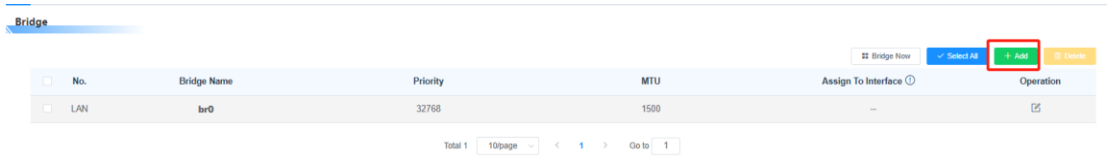
2.3.7 VLAN



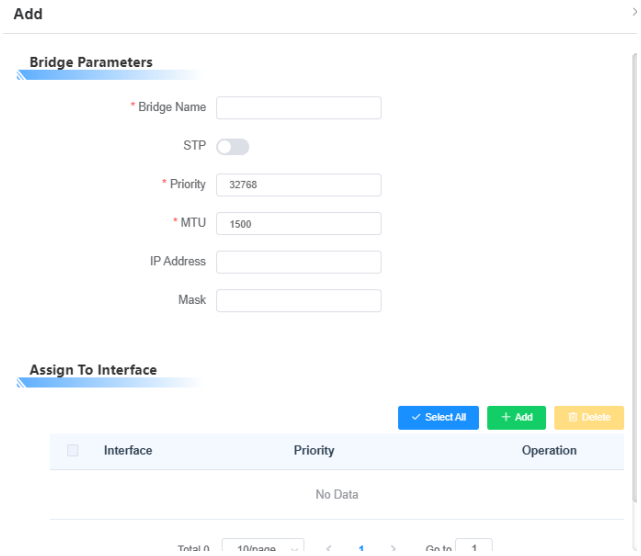
The VLAN feature enables users to segment ports based on their preferences. The system supports up to 15 VLAN ports (VLAN1 to VLAN15), but only two ports can be configured: one for WAN and one for LAN. These ports can be assigned to different VLANs as needed, but the LAN and WAN ports cannot belong to the same VLAN.

2.3.8 Bridge

2.3.8.1 Bridge Configure

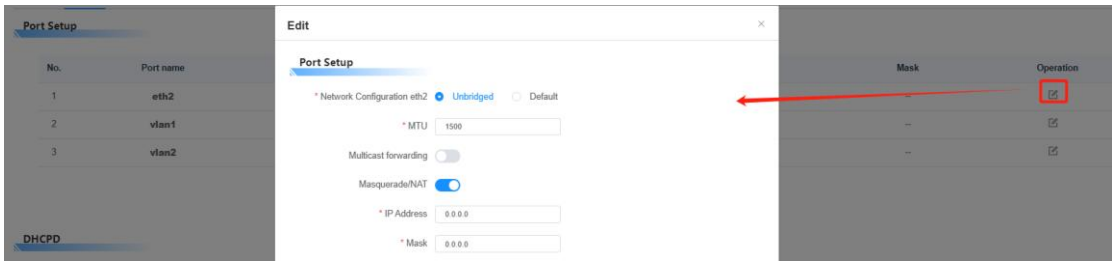


Clicking the “ADD” button will open the interface for adding a new bridge configuration, allowing you to create a bridge and set the relevant parameters.



Field Name	Description
Bridge Name	Sets a name for the new bridge.
STP	**ON:** Enables Spanning Tree Protocol (STP) to prevent network loops by blocking certain ports, ensuring a loop-free topology for stable network communication. **OFF:** Disables STP, which may lead to issues such as broadcast storms if physical loops exist in the network.
Priority	Sets the priority of the bridge, with a range of 0-65535. A lower value gives the bridge higher priority in the network topology calculation.
MTU	Specifies the maximum data packet size allowed in the bridge, optimizing network performance and preventing fragmentation from overly large packets.
IP Address	Defines the IP address for the bridge, enabling its identification within the network.
Mask	Works with the IP address to define the network and host ranges, specifying the subnet the bridge belongs to.
Assign To Interface	Allows assigning existing interfaces to the created bridge.

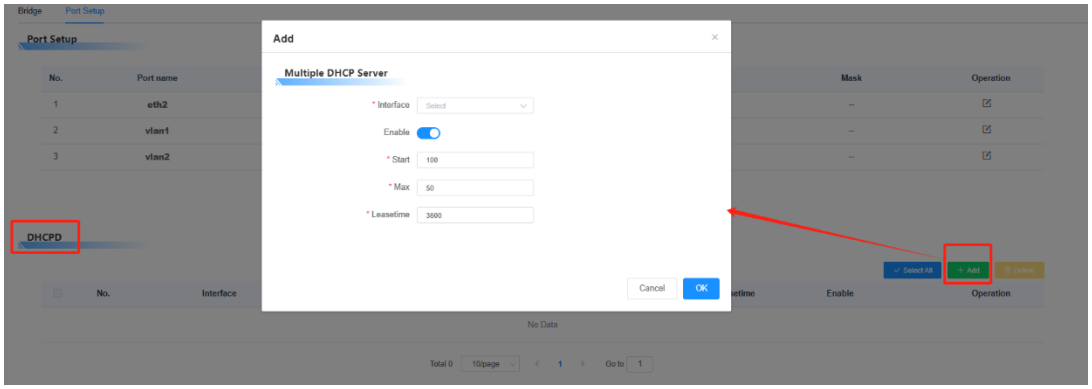
2.3.8.2 Port Setup



Field Name	Description
Network Configuration eth2	**Unbridged**: The interface operates in unbridged mode, transmitting network data independently without bridging with other interfaces. This is ideal for scenarios requiring separate management or isolation of network connections.

	Default: The interface uses the default network configuration.
MTU	Specifies the Maximum Transmission Unit, which defines the largest packet size that can be transmitted.
Multicast forwarding	Enables or disables multicast forwarding functionality.
Masquerade/NAT	Enables or disables Masquerade/NAT for network address translation.
IP Address	Set the IP address for the ra0 interface, ensuring no conflicts with other ports or bridges.
Mask	Configures the subnet mask for the port.

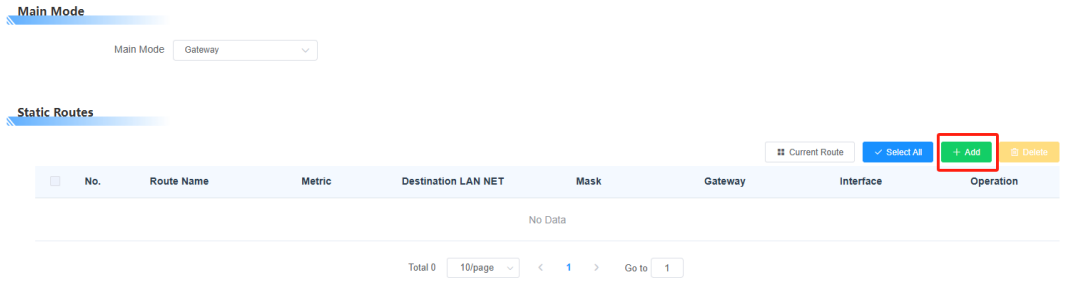
- **DHCPD**



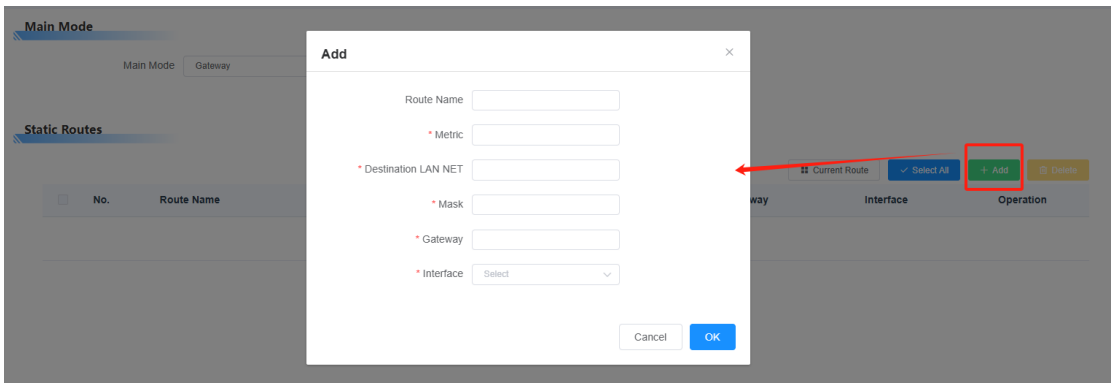
Field Name	Description
Interface	Select the network interface for enabling the multiple DHCP server function. The correct interface must be chosen to allow the DHCP server to assign IP addresses to devices connected to this interface.
Enable	**ON:** Activates the current multiple DHCP server configuration, allowing the router to assign network parameters (such as IP addresses) to devices on the selected interface. **OFF:** Disables this configuration, stopping the router from providing DHCP services through this interface.
Start	Defines the starting IP address for the DHCP range.
Max	Specifies the maximum number of DHCP clients that can be assigned IP addresses.
Lease Time	Sets the lease time (in minutes) for DHCP clients.

2.3.9 Routing

On the "Advanced Routing" page, you can configure the operating mode and static routing. For most users, it is recommended to use the default gateway mode.



Click "Add" to add a static routing-related configuration



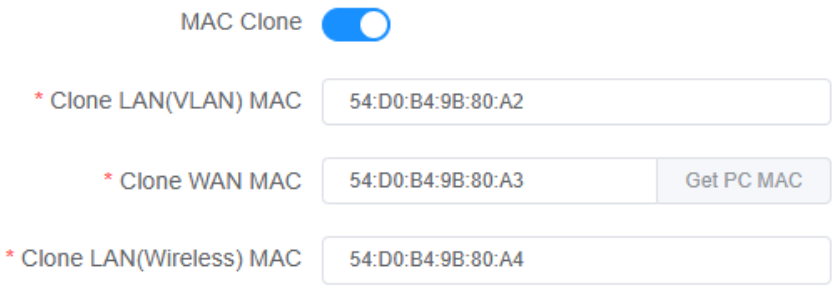
Field Name	Description
Route Name	User-defined name for the route (up to 25 characters).
Metric	Specifies the number of hops from the source to the destination (range: 0-9999).
Destination LAN NET	The destination network or host IP address for the static route.
Mask	The subnet mask that defines the network and host portions of the destination IP.
Gateway	The IP address of the gateway device enabling communication with the destination.
Interface	Select the appropriate interface (LAN, wireless, WAN, or other ports) based on the destination IP location.

2.3.10 DDNS

Field Name	Description
DDNS Service	Supports various DDNS providers, including DynDNS, FreeDNS, ZoneEdit, No-IP, 3322, easyDNS, TZO, and DynSIP. Custom DDNS servers can also be configured.
Username	The registered username for the DDNS service (max 64 characters).
Password	The password is associated with the DDNS account (max 32 characters).
Host Name	The hostname is assigned by the DDNS provider (no specific length limit).
Type	DDNS service type, varying by provider.
Wildcard	Enables wildcard support (default: OFF). When ON, *.host.3322.org is treated as host.3322.org.
Do not use external IP check	Enables or disables external IP detection.
Force Update Interval	Forces a DDNS update within the specified number of days.

2.3.11 MAC Clone

Some ISPs require MAC address registration. To avoid re-registration, you can clone your router's MAC address to match the one already registered with your ISP.



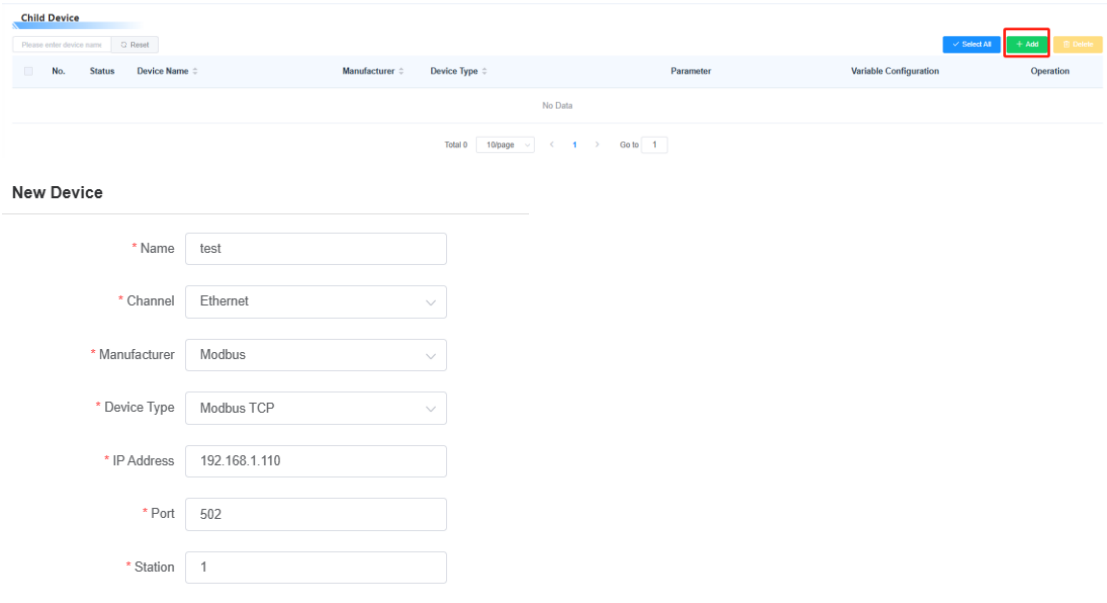
MAC address cloning can be applied to both the LAN and WAN ports. Key considerations:

1. A MAC address is 48 bits and cannot be a multicast address, meaning the first byte must be even.
2. The MAC address must be valid and cannot be arbitrarily assigned.

2.4 Data Acquisition

D1002 supports operation data acquisition from various industrial equipment. This chapter provides an overview of data acquisition and configuration for industrial devices.

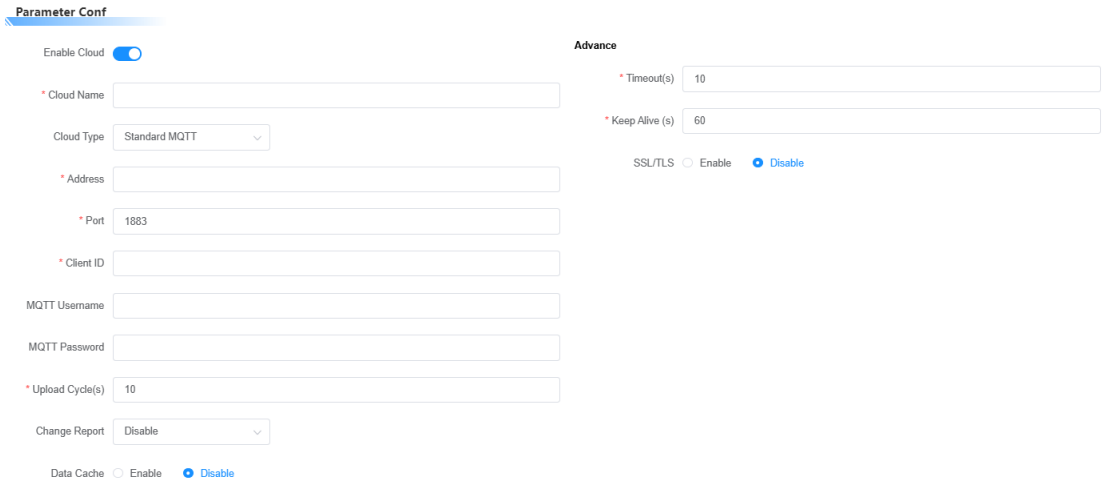
2.4.1 Child Device



Field Name	Description
Name	Customizable name for the added subdevice (typically industrial equipment).

Channel	Selects the connection type, including Ethernet, RS232/A1B1, or TTL232.
Manufacturer	Choose the equipment manufacturer or protocol.
Device Type	Specifies the device's communication protocol.
IP Address	Enter the device's IP address for network identification.
Port	Specify the port number for device communication.
Station	In Modbus communication, this identifies the device number. Devices are distinguished by station numbers, with "1" as the default setting.

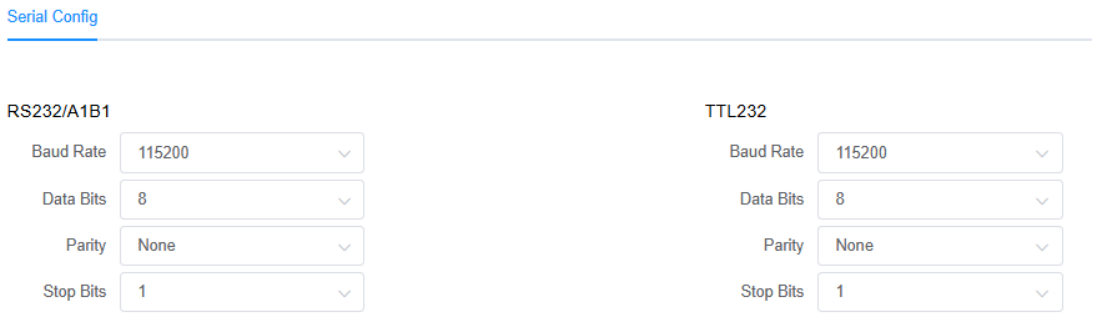
2.4.2 Cloud



Field Name	Description
Cloud Name	Enter the name of the cloud service.
Cloud Type	Select the cloud platform type, including MQTT, HTTP, TCP/UDP, or third-party platforms. Currently set to "Standard MQTT."
Address	Enter the cloud platform's network address.
Port	Specify the port number for cloud communication.
Client ID	A unique identifier for the device on the cloud platform, used for device management.
MQTT Username	The account used to log in to the cloud platform.
MQTT Password	The corresponding password for MQTT authentication.
Upload Cycle(s)	Defines the data upload interval to the cloud, in seconds.

Change Report	When enabled, the device reports data changes to the cloud; when disabled, it does not.
Data Cache	When enabled, the device temporarily stores data; when disabled, caching is turned off.
Timeout(s)	Sets the timeout period for cloud connection.
Keep Alive (s)	Defines the MQTT heartbeat interval to maintain connection stability.
SSL/TLS	When enabled, activates SSL/TLS encryption for secure data transmission; when disabled, encryption is not used.

2.4.3 I/F Setting



Field Name	Description
Baud Rate	Defines the data transmission rate in serial communication, measured in baud. Set to 115200, meaning 115200 symbols are transmitted per second. Both communication devices must use the same baud rate for proper communication.
Data Bits	Specifies the number of valid data bits in each data frame.
Parity	Error detection method in data transmission. "None" means no parity check is performed.
Stop Bits	Indicates the end of a data frame in serial communication.

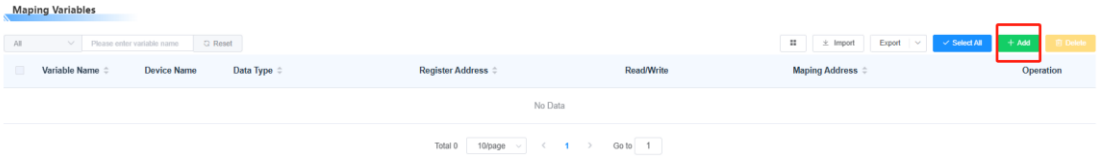
2.4.4 Proto Conv

2.4.4.1 Modbus TCP

- **Slave Config**

Field Name	Description
TCP Mode	Defines the device's role in Modbus TCP communication. In "TCP Server" mode, the device listens for incoming connection requests. In "TCP Client" mode, the device actively initiates a connection to a specified server.
Listen Port	When operating in "TCP Server" mode, this sets the port number for listening to connection requests. Default is 502, the standard port for Modbus TCP.
Server Key	Identifies the slave device in Modbus communication. Each slave has a unique station number, allowing the master device to recognize and communicate with it properly.

- **Maping Variables**



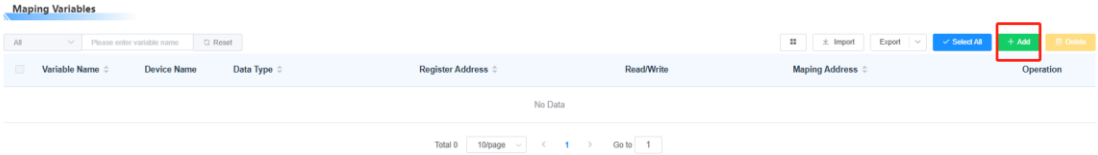
Click "Add" to configure Mapping Variables.

2.4.4.2 Modbus RTU

- **Slave Config**

Field Name	Description
Channel	Selects the physical channel for device communication.
Server Key	A configuration parameter used for device identification, security verification, or enabling specific functions.

- **Maping Variables**

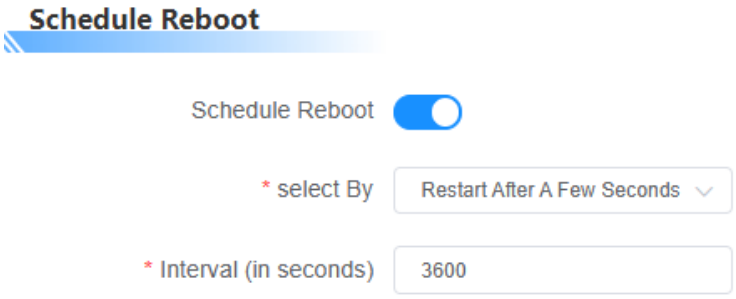


Clicking "Add" allows you to configure the Mapping Variables.

2.5 Application

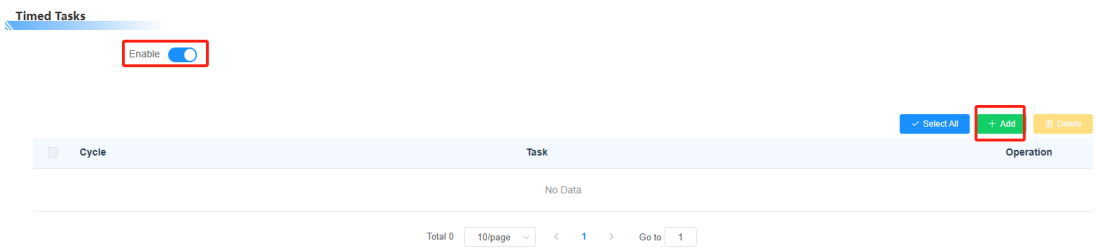
2.5.1 Active Policy

2.5.1.1 Schedule Reboot



Field Name	Description
Schedule Reboot	A toggle to enable or disable the router's scheduled reboot function. When enabled, the router will reboot according to the specified schedule; when disabled, the router will not reboot automatically.
Select by	Choose the trigger method for the scheduled reboot. Various trigger options are available in the drop-down menu: **Restart After A Few Seconds Interval**: Select this option to have the router reboot cyclically at the specified interval in seconds. **Schedule Reboot:** Set a specific day and time for the router to reboot.

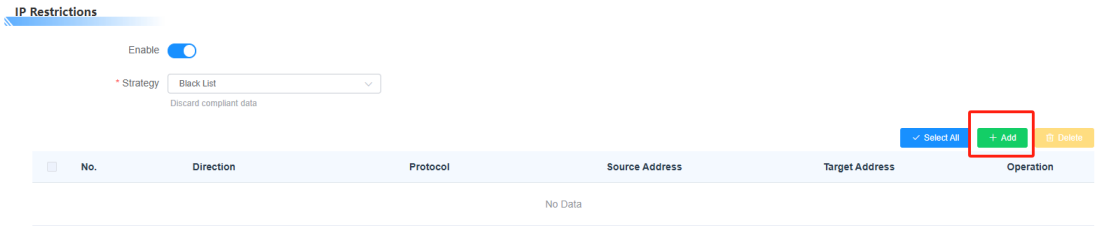
2.5.1.2 Timed Tasks

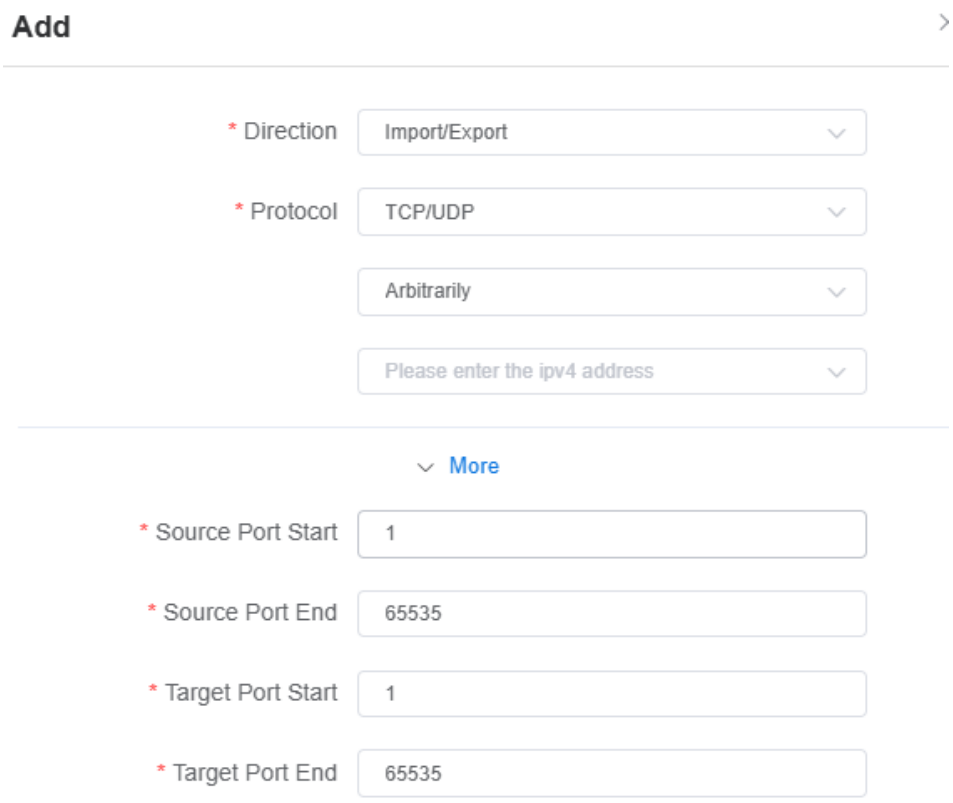


Users can add scheduled tasks here, such as automatic reboot tasks.

2.5.2 Security

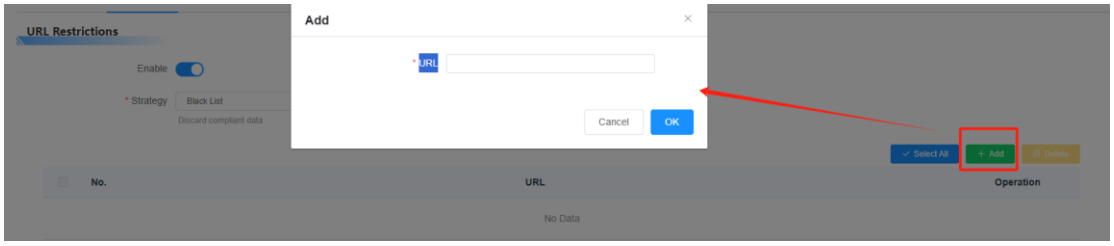
2.5.2.1 IP Restrictions





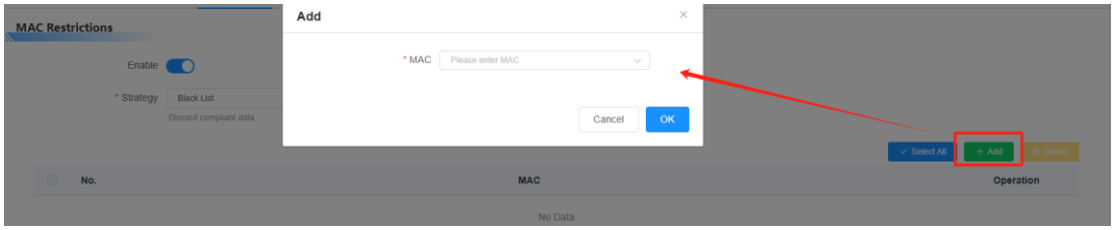
Field Name	Description
Enable	A switch option. When enabled, the IP restriction function is activated, restricting IP-related access based on the configured rules. When disabled, IP restrictions are turned off, and no restriction rules are applied.
Strategy	Select the strategy mode for IP restrictions.
Add	Click this button to open the interface for adding new IP restriction rules.
Direction	Defines the direction of data transmission.
Protocol	Select the network protocol to which the restriction rules apply.
Source Port Start	Set the starting port number for the source port range.
Source Port End	Set the ending port number for the source port range.
Target Port Start	Set the starting port number for the target port range.
Target Port End	Set the ending port number for the target port range.

2.5.2.2 URL Restrictions



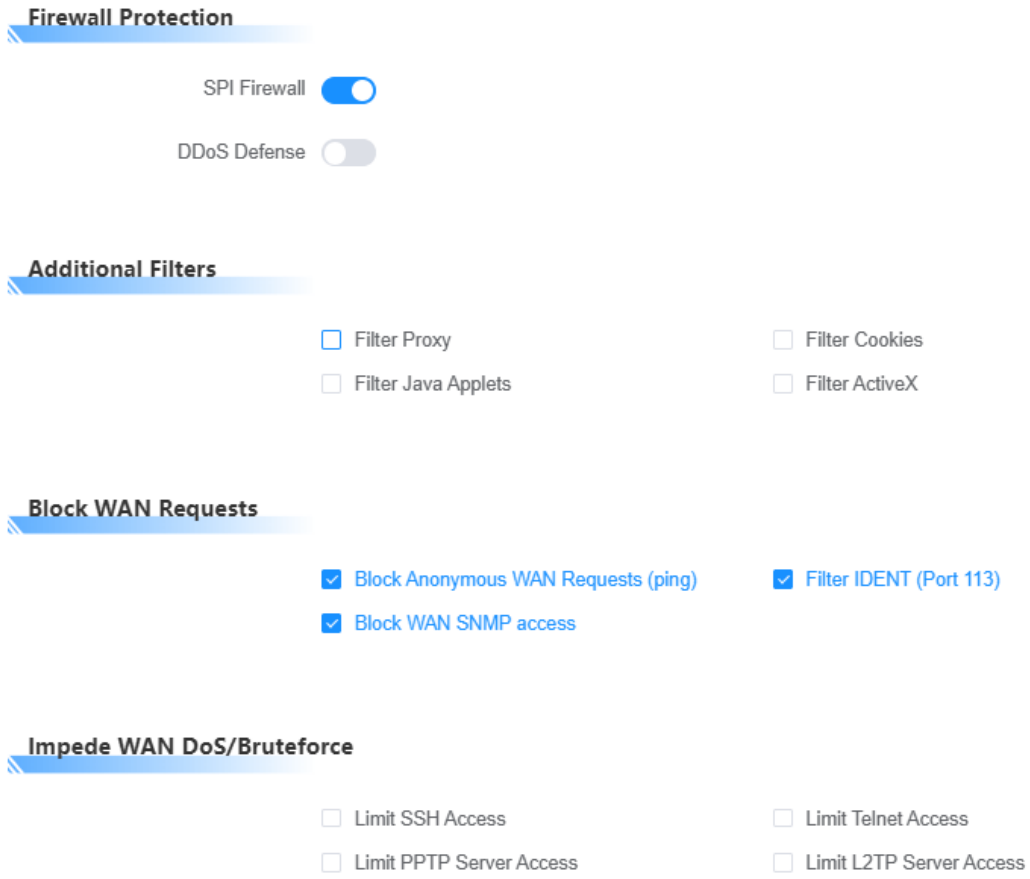
Field Name	Description
Enable	A switch option. When enabled, the URL Restrictions function is activated. When disabled, URL Restrictions are turned off.
Strategy	Select the strategy mode for URL restrictions.
Add	Click this button to open the interface for adding new URL restriction rules.
URL	Enter the URL or policy link for the restriction.

2.5.2.3 MAC Restrictions



Field Name	Description
Enable	A switch option. When enabled, the MAC Restrictions function is activated. When disabled, MAC Restrictions are turned off.
Strategy	Select the strategy mode for MAC restrictions.
Add	Click this button to open the interface for adding new MAC restriction rules.
MAC	Enter the MAC address to which the policy applies.

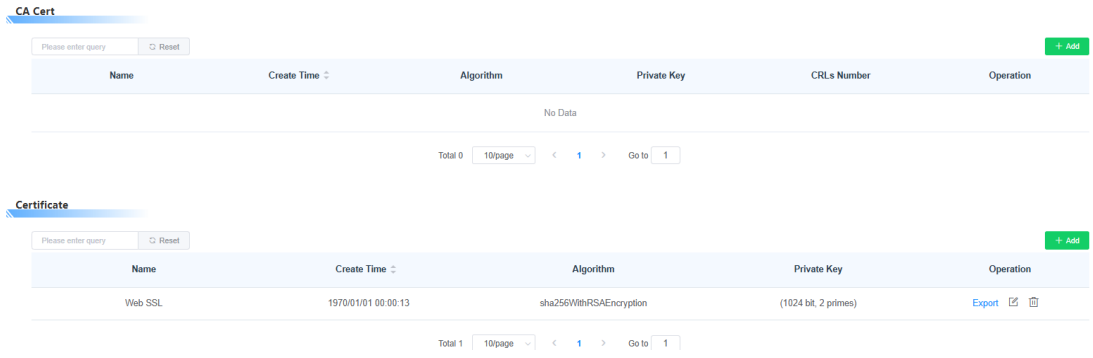
2.5.2.4 Firewall



Field Name	Description
SPI Firewall	A switch option. When enabled, the SPI (Stateful Packet Inspection) Firewall is activated. When disabled, the firewall function is turned off.
DDoS Defense	Select the strategy mode for DDoS (Distributed Denial of Service) defense to protect against potential DDoS attacks.
Filter Proxy	Click to open the interface for adding new MAC restriction rules, allowing the addition of new MAC restrictions.
Filter Cookies	When enabled, the router will block network traffic containing cookies to protect against privacy breaches or malicious tracking.
Filter Java Applets	When enabled, the router blocks network traffic containing Java applets to prevent potential security risks, such as malicious code execution.
Filter ActiveX	When enabled, the router blocks network traffic containing ActiveX controls to prevent security issues like unauthorized system access.
Block Anonymous WAN Requests	When enabled, the router blocks anonymous ping requests from the wide-area network, preventing network probing and potential

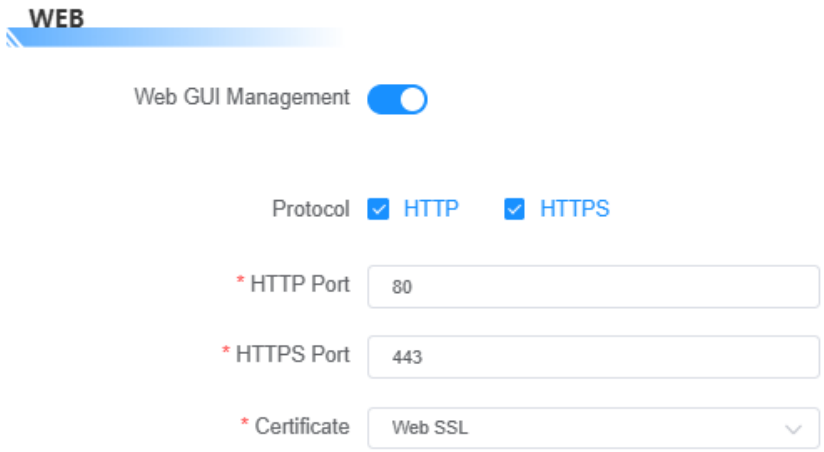
(ping)	attacks.
Filter IDENT (Port 113)	When enabled, the router filters traffic related to the IDENT protocol through port 113 to prevent security threats, such as unauthorized user identity queries.
Block WAN SNMP access	When enabled, the router blocks wide-area network access to the Simple Network Management Protocol (SNMP), preventing unauthorized access or tampering with network management information.
Limit SSH Access	When enabled, the router restricts SSH (Secure Shell Protocol) access. You can set rules, such as limiting access to specific IPs or restricting connection frequencies, to prevent brute-force SSH attacks.
Limit Telnet Access	When enabled, the router restricts Telnet (Remote Login Protocol) access, and you can set rules to prevent unauthorized remote logins, as Telnet is less secure due to its unencrypted data transmission.
Limit PPTP Server Access	When enabled, the router restricts access to the PPTP (Point-to-Point Tunneling Protocol) server to prevent unauthorized users from establishing tunnel connections.
Limit L2TP Server Access	When enabled, the router restricts access to the L2TP (Layer 2 Tunneling Protocol) server, preventing unauthorized users from establishing tunnel connections and enhancing network security.

2.5.2.5 Cert Management



This section is primarily for managing certificates and configuring related parameters.

2.5.2.6 Web Access



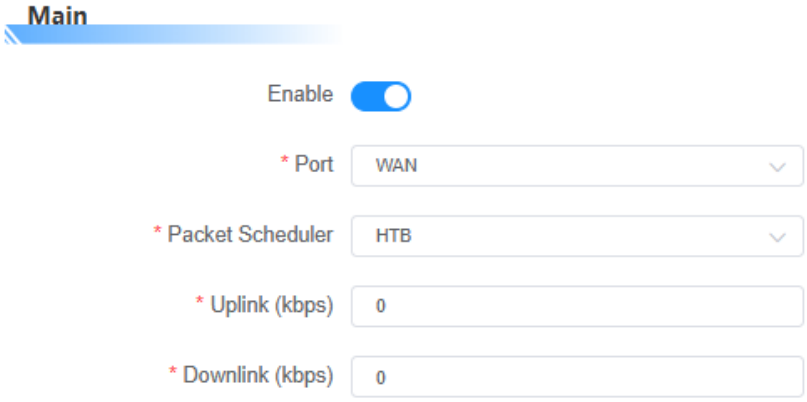
Field Name	Description
Web GUI Management	Enables or disables router management via the web interface. When enabled, the router can be managed through its web page; when disabled, web-based management is unavailable.
Protocol	Selects the protocol for accessing the router's web management page. "HTTP" is the standard protocol, while "HTTPS" provides a secure connection using SSL/TLS encryption. If HTTPS is selected, a valid certificate must be chosen (can be managed in the certificate section).
HTTP Port	Configures the port for accessing the router's web page via HTTP, typically set to port 80 by default.
HTTPS Port	Configures the port for accessing the router's web page via HTTPS, typically set to port 443 by default.
Certificate	Selects the HTTPS certificate for secure web access.

2.5.3 QOS

2.5.3.1 QOS Basic

- **Main**

Represents the main link configuration



Field Name	Description
Enable	Turns the main link's QoS function on or off. When enabled, it manages network traffic based on the set parameters. When disabled, the QoS function is inactive.
Port	Select the port for the main link. The default option is "WAN" (Wide Area Network).
Packet Scheduler	Choose the algorithm for managing and scheduling data packets. "HTB" (Hierarchical Token Bucket) is commonly used for hierarchical traffic control.
Uplink (kbps)	Enter the uplink bandwidth value, typically 80% to 90% of the maximum available bandwidth.
Downlink (kbps)	Enter the downlink bandwidth value, generally 80% to 90% of the maximum bandwidth.

- **Backup**

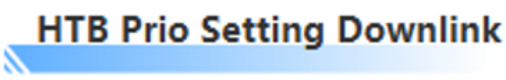
Represents the backup link configuration

- **HTB Prio Setting Uplink**

Sets the priority for uplink traffic using the HTB algorithm.

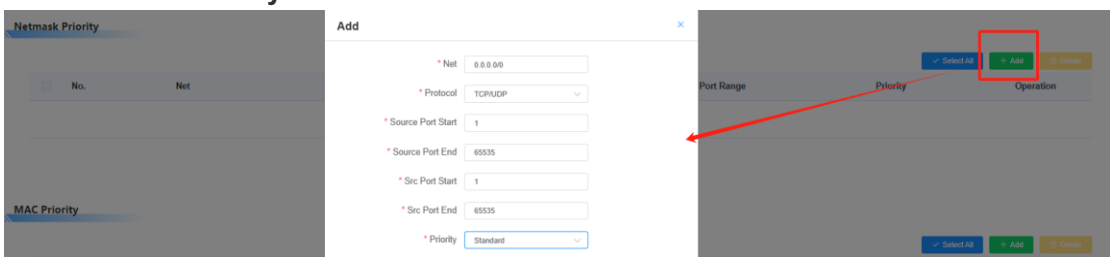
- **HTB Prio Setting Downlink**

Sets the priority for downlink traffic using the HTB algorithm.



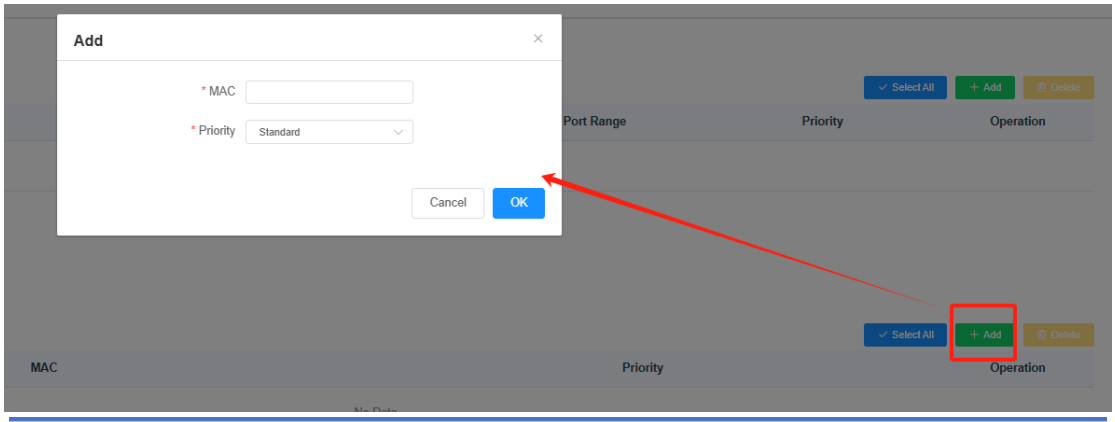
2.5.3.2 QOS Classify

- **Netmask Priority**



Field Name	Description
Net	Specifies the IP address range. "0.0.0.0/0" matches all IP addresses.
Protocol	Selects the network protocol for applying QoS rules.
Source Port Start	Sets the starting port number of the source port range (1 - 65535).
Source Port End	Sets the ending port number of the source port range (1 - 65535).
Src Port Start	Sets the starting port number of the source port range (1 - 65535).
Src Port End	Sets the ending port number of the source port range (1 - 65535).
Priority	Sets the priority of the network traffic.

- **MAC Priority**



Field Name	Description
MAC	Specify the MAC address.
Priority	Sets the priority for network traffic.

- **Priority Description:**

This system offers five priority levels. The "Exempt" priority operates independently from the other four, which are: Premium (High Priority), Express (Priority), Standard, and Bulk (Low Priority).

- **Exempt**:

Data streams at the Exempt priority are limited only by hardware capabilities. The relationship between Exempt bandwidth and the other four priorities is as follows:

- **Max_Up:** Total upload bandwidth
- **Max_Down:** Total download bandwidth
- **Uplink:** Upload limit in "QoS Settings"
- **Downlink:** Download limit in "QoS Settings"
- **Exempt_Rate_Up:** Upload traffic rate of the Exempt data stream
- **Exempt_Rate_Do:** Download traffic rate of the Exempt data stream

Then the total upload bandwidth for other priorities is:
min(Max_Up - Exempt_Rate_Up, Uplink)
The total download bandwidth for other priorities is:
min(Max_Down - Exempt_Rate_Do, Downlink)

After the Exempt data stream is allocated, the remaining bandwidth is distributed among the other priorities. For example, if the remaining upload and download bandwidths are 1000 kbps, and four data streams with priorities Premium, Express, Standard, and Bulk exist, the allocation would be as follows:

- **Premium**: (75/100) * Uplink, (75/100) * Downlink
- **Express**: (15/100) * Uplink, (15/100) * Downlink
- **Standard**: (10/100) * Uplink, (10/100) * Downlink
- **Bulk**: 1000 bits (nearly 0); 1000 bits (nearly 0)

For the Bulk priority, its upload and download rates are minimal, serving only after the other priority data streams have been processed. When only one data stream is active, its bandwidth is governed solely by the upload and download limits in the "QoS Settings."

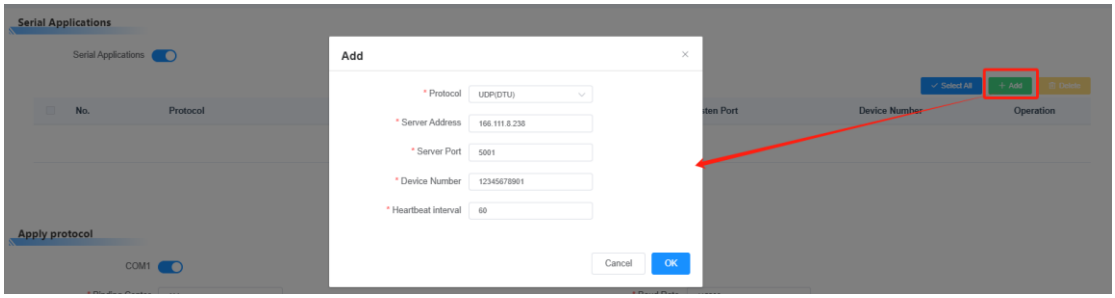
Note: If a connection meets the control conditions for both MAC priority and netmask priority, the rule added first takes precedence.

2.6 Serial Applications

2.6.1 Serial Applications

The device features one RS-485 serial port and one RS-232 serial port, both used for data transmission. It includes a built-in serial-to-TCP/IP program and supports multi-server center functionality, enabling data from COM1 and COM2 to be directed to any specified data center.

- **Serial Applications**



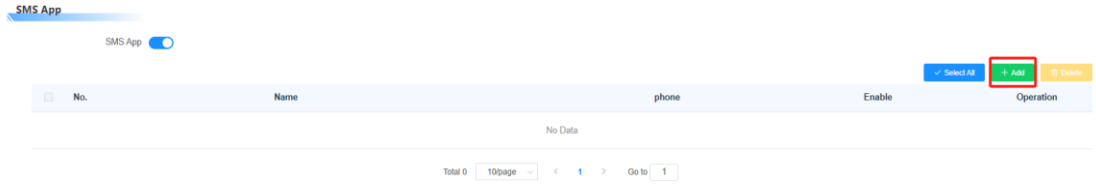
Field Name	Description
Protocol	Select the protocol type.
Server Address	Enter the IP address or domain name of the data service center for communication with the router's serial-to-TCP program.
Server Port	Specify the port the data service center program listens on.
Device Number	Set the device's 11-byte ID number. This option is only applicable when the protocol type is set to "UDP (DTU)" or "TCP (DTU)".
Heartbeat interval	Set the time interval for sending heartbeat packets. This option is only applicable when the protocol type is set to "UDP (DTU)" or "TCP (DTU)".

- **Apply Protocol**

Field Name	Description
Binding Center	Links the communication center, corresponding to the one set in Serial Applications.
Baud Rate	Specifies the data transmission speed in bytes per second. Common baud rates include 115200, 57600, 38400, 19200, etc.
Data Bits	Defines the number of bits in each character, typically 7 or 8. It is usually represented in ASCII and transmitted starting with the least significant bit, synchronized by the clock.
Stop Bits	Indicates the end of a character's data, typically set to 1 or 2 high-level bits.
Parity	Refers to the error-checking method for the data set. Options include odd or even parity.
Flow Control	Encompasses both hardware and software methods to manage data flow.

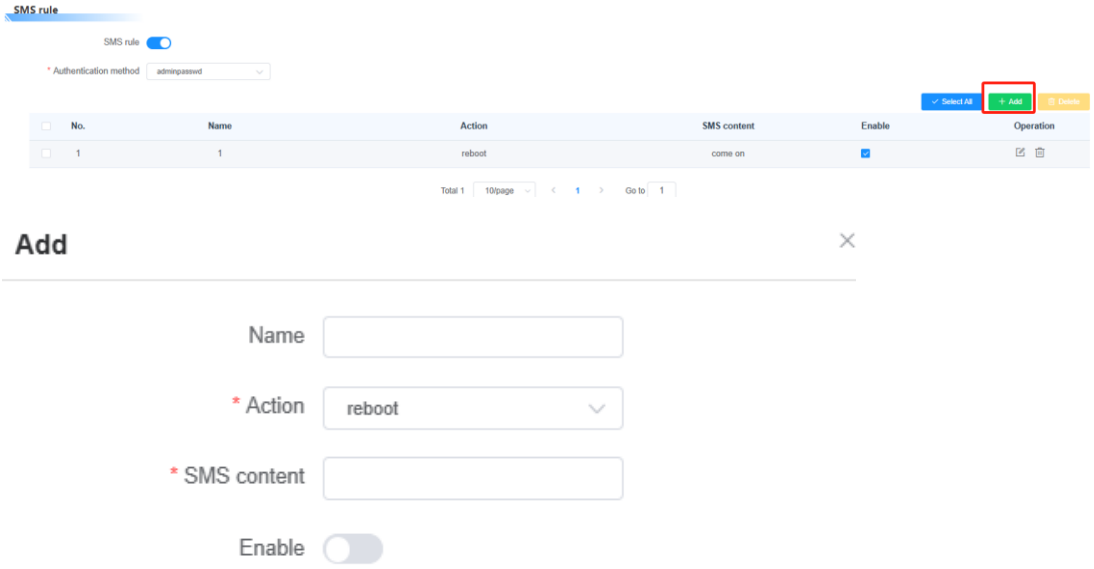
2.6.2 SMS App

- **SMS App**



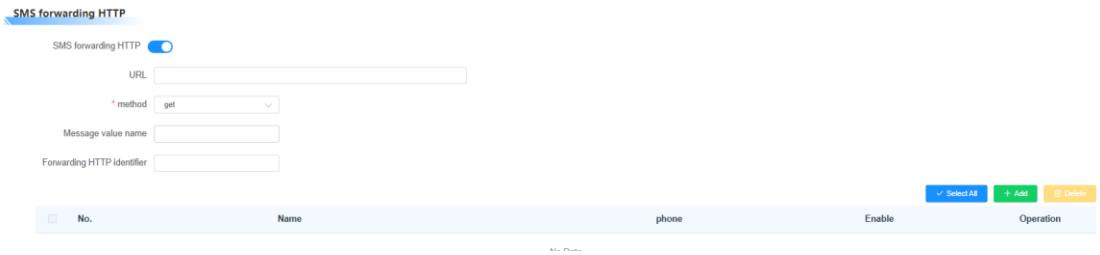
Click "Add" to include the phone numbers that should receive SMS.

- **SMS Rule**



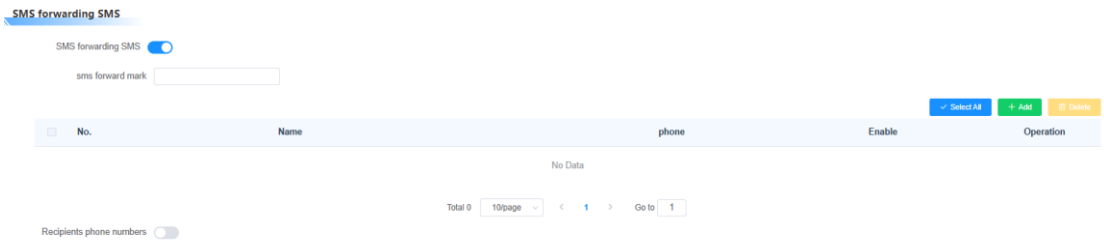
Field Name	Description
Authentication Method	Select the authentication method for the SMS function:- **Adminpasswd:** Authentication is performed using the administrator password. **SN:** Authentication is performed using the device's serial number. **NONE:** No authentication method is applied.
Action	Select the events that will trigger SMS notifications.
SMS content	Enter the content for the SMS message.
Enable	Toggle to enable or disable the SMS function.

- **SMS Forwarding HTTP**



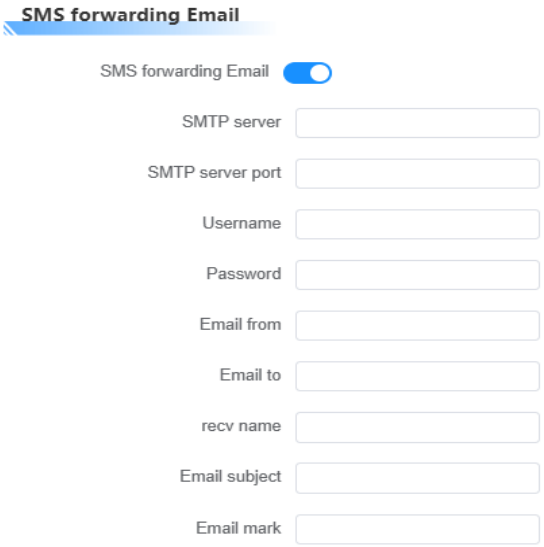
Field Name	Description
SMS forwarding HTTP	A toggle option to enable or disable SMS forwarding via the HTTP protocol. When enabled, the router forwards SMS content to the target server based on the settings; when disabled, the SMS forwarding function is turned off.
URL	Enter the URL of the target server that will receive the forwarded SMS content.
method	Select the HTTP request method for SMS forwarding.
Message value name	Define a custom parameter name for the SMS content, helping the receiving server identify and process the SMS-related data.
Forwarding HTTP identifier	Specify an identifier for the HTTP request used in SMS forwarding. This can be used to distinguish different forwarding tasks or manage them effectively.

- **SMS Forwarding SMS**



Field Name	Description
SMS forwarding SMS	A toggle option to enable or disable SMS forwarding. When enabled, the router forwards received SMS messages to specified numbers based on the settings; when disabled, SMS forwarding is turned off.
SMS forward Mark	Enter a custom identifier to distinguish specific SMS forwarding tasks, aiding in management and identification.
Recipients Phone Numbers	A toggle option to enable or disable the recipient phone number settings. When enabled, recipients can be specified; when disabled, this setting is inactive.

- **SMS Forwarding Email**



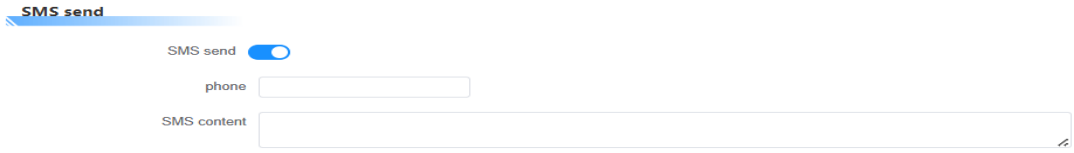
Field Name	Description
SMTP server	Enter the SMTP server address for sending emails, required for the SMS-to-email forwarding function.
SMTP server port	Specify the port number for the SMTP server.
Username	The login username for the SMTP server.
Password	The password corresponding to the username for SMTP login, ensuring secure email transmission.

Email from	Specify the sender's email address for forwarding SMS messages.
Email to	Enter the recipient's email address where the forwarded SMS message will be sent.
recv name	(Optional) Enter the recipient’s name to display in the email.
Email subject	Specify the subject line of the email to summarize its content for the recipient.
Email mark	(Optional) Enter a custom identifier to distinguish specific SMS-to-email forwarding tasks.

- **SMS Timing Management**

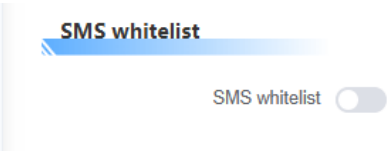
Field Name	Description
Interval(s)	Set the time interval (in seconds) for sending SMS messages, determining the frequency of scheduled SMS transmissions.
Scheduled SMS content	Enter the text content for the scheduled SMS message to be sent at the defined intervals.

- **SMS Send**



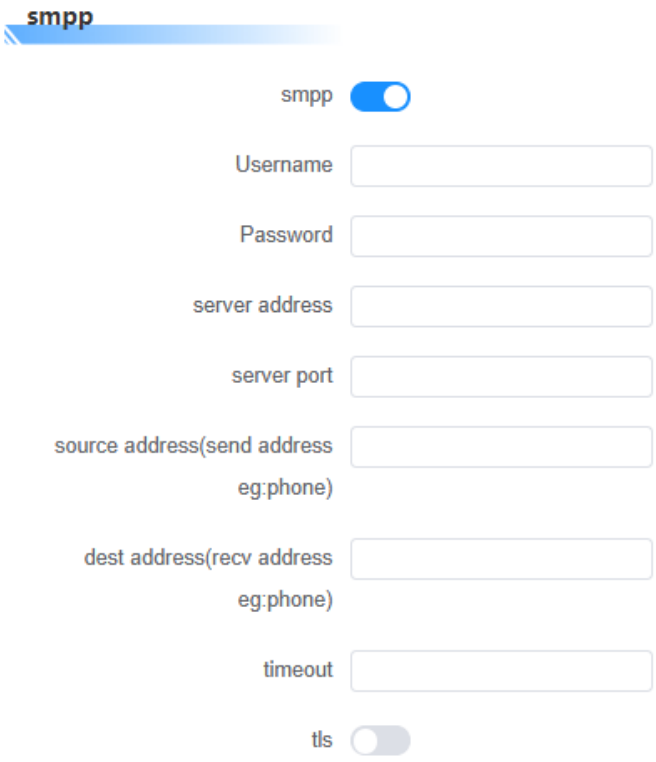
Field Name	Description
Phone	Enter the recipient's mobile phone number for the SMS.
SMS content	Enter the text message to be sent.

- **SMS whitelist**



Field Name	Description
SMS whitelist	A toggle option. When enabled, only numbers on the whitelist can perform SMS-related operations (such as sending and receiving messages). When disabled, SMS operations are unrestricted.

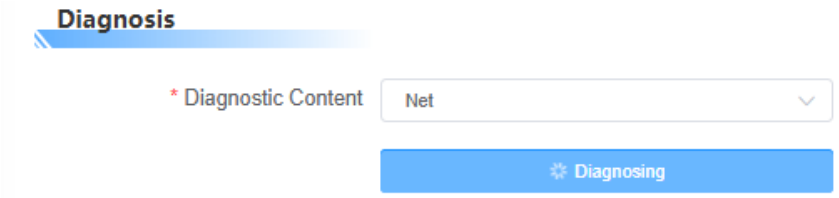
- **Smpp**



Field Name	Description
Username	The login username for the SMPP server, used for identity verification.
Password	The corresponding password for logging into the SMPP server, ensuring authentication.
Server Address	Enter the IP address or domain name of the SMPP server to establish a connection.
Server Port	Specify the port number for connecting to the SMPP server.
Source address (send address eg:phone)	The phone number used as the sender of SMS messages.
Dest address (recv address eg:phone)	The phone number designated to receive SMS messages.
Timeout	Set the maximum waiting time for a response from the SMPP server before considering the request as timed out.
TLS	A toggle option. When enabled, TLS encryption secures communication with the SMPP server; when disabled, encryption is not applied.

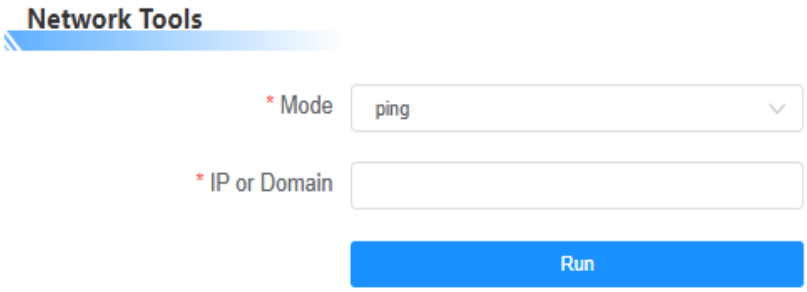
2.7 Maintenance

2.7.1 Diagnosiss



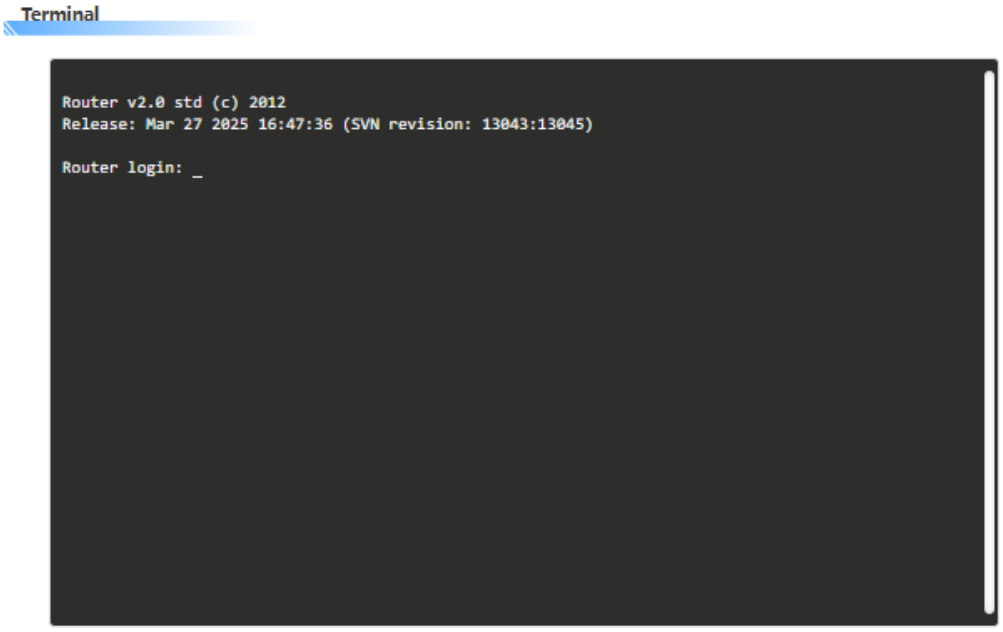
Field Name	Description
Diagnostic Content	Click "Start Diagnostic" to analyze the device's relevant information. Once the diagnosis is complete, you can export the diagnostic report.

2.7.2 Network Tools



Field Name	Description
Mode	Select the network testing mode, including Ping, Traceroute, and NSLookup.
IP or Domain	Enter the target IP address or domain name.

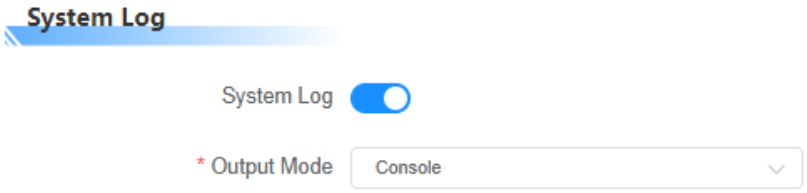
2.7.3 Commands



Field Name	Description
Terminal	Execute commands on the Terminal page for device maintenance.
Start Command	Save command-line instructions to execute automatically when the router starts.
Shutdown Command	Save command-line instructions to execute automatically when the router shuts down.
Firewall Command	Run custom iptables commands each time the firewall starts.

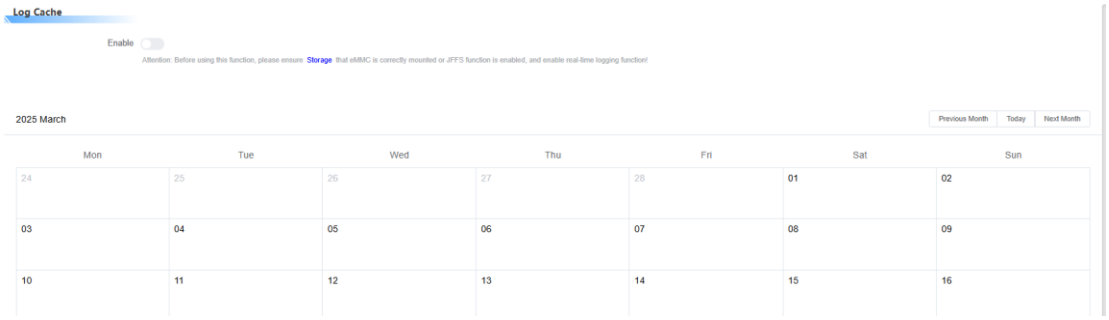
2.7.4 Log

- **Realtime Log**



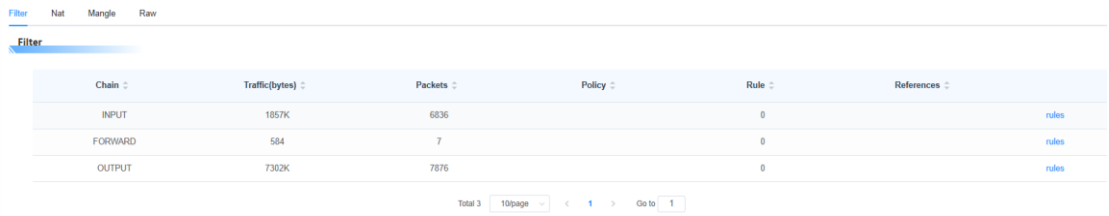
Field Name	Description
System Log	A switch option. When enabled, the system records operational events and logs; when disabled, logging stops.
Output Mode	Selects how system logs are output: **Console:** Logs are displayed on the device's console for local viewing. **NET:** Logs are transmitted over the network to a designated log server for remote management. **Web Page:** Logs are accessible via a web interface, allowing users to view them through a browser.

- **History Log**



You can view historical logs by selecting the corresponding date.

2.7.5 Firewall

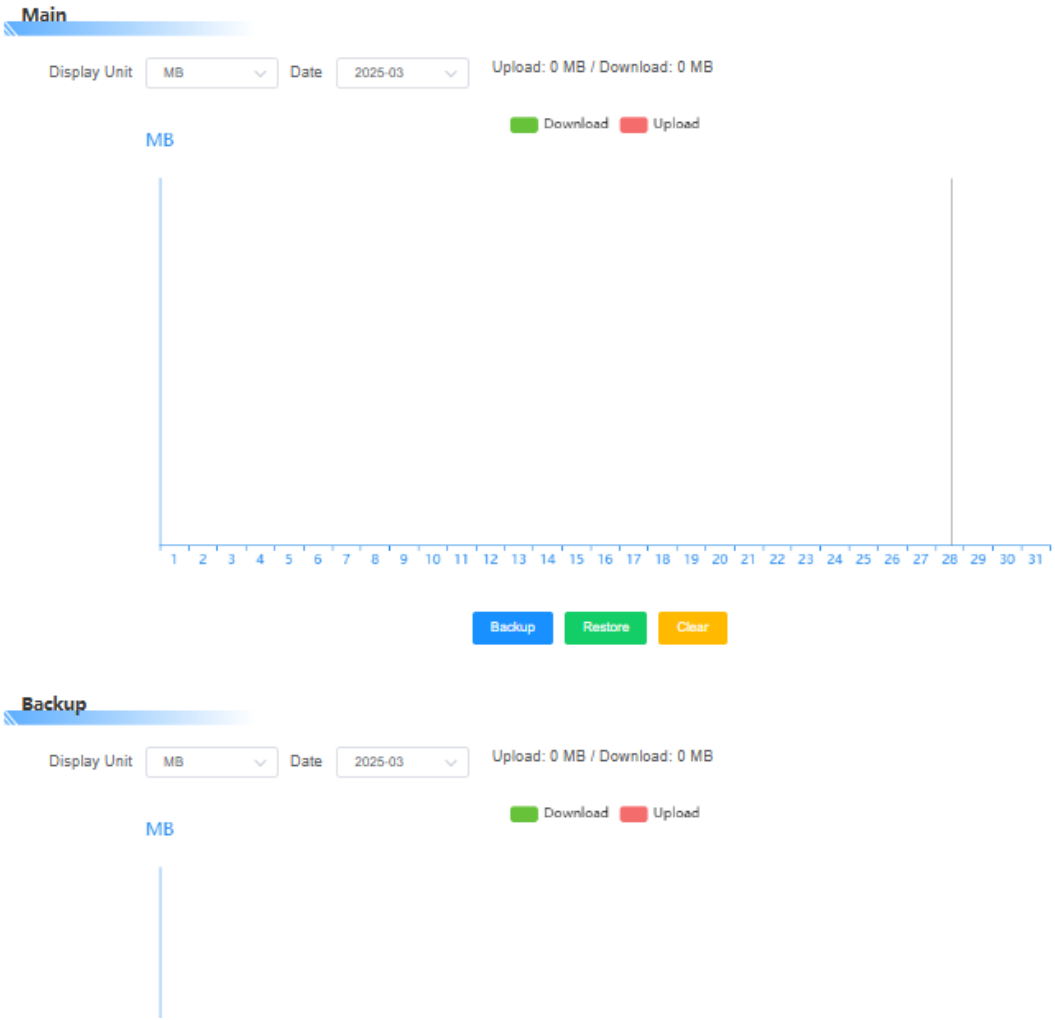


Use to view related data for several firewall rule table types like Filter, Nat, Mangle, Raw.

Field Name	Description
Chain	Represents the different chains organizing firewall rules.

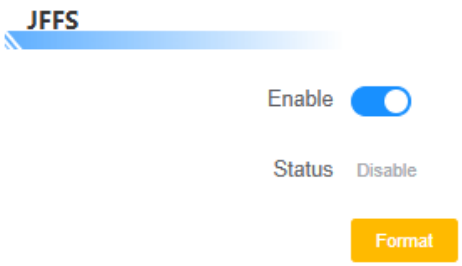
Traffic(bytes)	Displays the size of network traffic passing through the corresponding chain, measured in bytes, indicating the bandwidth used by data packets in the chain.
Packets	Counts the number of data packets passing through the corresponding chain.
Policy	Specifies the default processing policy for the corresponding chain.
Rule	Indicates the number of active rules within the current chain.

2.7.6 Traffic



View the traffic of the primary and backup links in a visual chart.

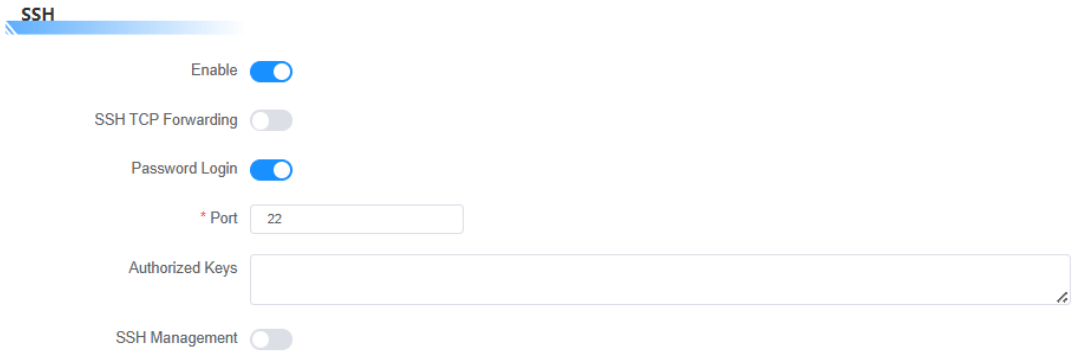
2.7.7 Storage



Format the JFFS file system to erase all data and reinitialize it.

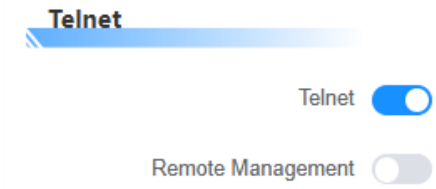
2.7.8 Remote MGT

- **SSH**



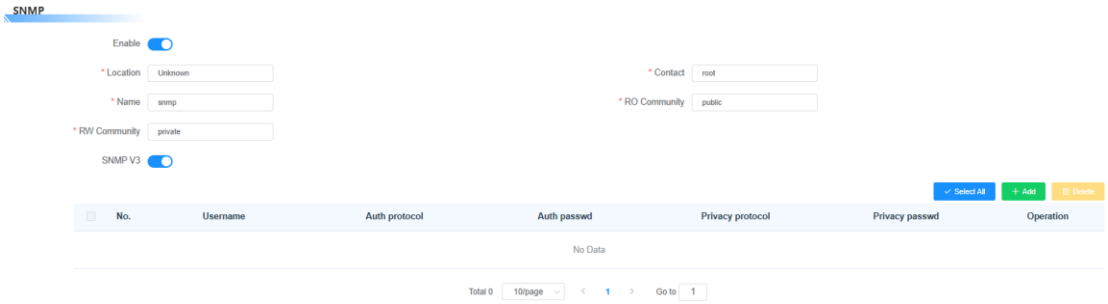
Field Name	Description
SSH TCP Forwarding	A switch option that enables or disables SSH TCP forwarding. When enabled, TCP traffic can be forwarded through an SSH tunnel; when disabled, SSH-based TCP forwarding is not allowed.
Password Login	A switch option that allows or restricts SSH login using a username and password. When disabled, alternative authentication methods, such as key-based login, may be required.
Port	Specifies the port number for the SSH service. The default is typically 22, but it can be modified for security purposes.
Authorized Keys	Allows adding public keys for SSH authentication.
SSH Management	Enables SSH-related management functions, including remote port configuration.

- **TELNET**



Field Name	Description
Telnet	Enables the Telnet service for the device.
Remote Management	Allows remote management via Telnet.

- **SNMP**

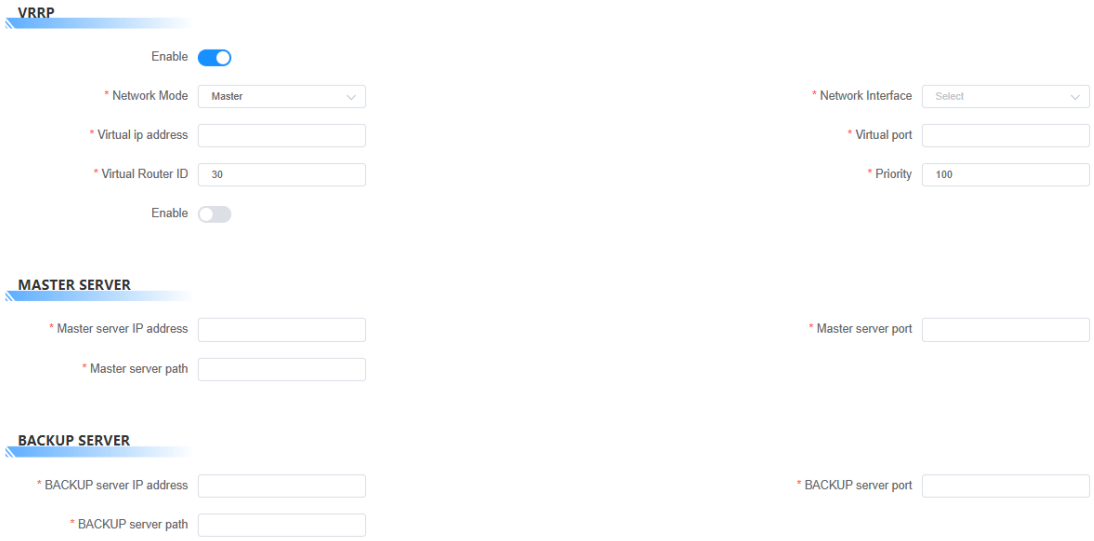


Field Name	Description
Location	Specifies the device's physical location to help administrators identify its placement.
Contact	Defines the device's contact information, defaulting to "root."
Name	Customizes the device name for SNMP management, defaulting to "snmp."
RO Community	The read-only authentication string for SNMP. Management stations with this community name can only view device information but cannot modify it. Default: "public."
RW Community	The read-write authentication string for SNMP. Management stations with this community name can read and modify device information. Default: "private."
SNMP V3	A switch option. When enabled, activates SNMP version 3 features.
+ Add	Allows adding SNMP-related details.

- **TR069**

Field Name	Description
TR069 Mode	Selects the working mode of the TR069 protocol. "Production" is for formal operational environments, while "Staging" is for testing and pre-deployment.
Heartbeat enables switching	A switch option. When enabled, the router periodically sends heartbeat messages to the management server to maintain the connection and report its status. When disabled, this function stops.
The account used for FTP diagnosis in TR143	Specifies the login account for FTP-related diagnostic operations under TR143.
The password used for FTP diagnostics in TR143	Specifies the login password for FTP diagnostics under TR143, used alongside the account for authentication.

- **VRRP**



Field Name	Description
Network Mode	Defines the VRRP device's role in the network.

Network Interface	Selects the network interface for VRRP operation.
Virtual IP Address	Sets the shared IP address for the VRRP virtual router, used by both primary and backup routers to provide external services.
Virtual Port	Specifies the port associated with the virtual IP address for network communication.
Virtual Router ID	Identifies the VRRP virtual router, typically ranging from 0 to 255. Devices in the same VRRP group must have the same ID.
Priority	Determines the device's priority within the VRRP group. A higher value increases the likelihood of becoming the master router (range: 1–254, default: 150).
Master Server IP Address	Specifies the IP address of the master server.
Master Server Port	Sets the port number for connecting to the master server.
Master Server Path	Defines the path related to the master server.
Backup Server IP Address	Specifies the IP address of the backup server, which takes over if the master server fails.
Backup Server Port	Sets the port number for connecting to the backup server.
Backup Server Path	Defines the path related to the backup server.

- **IO Set**

Field Name	Description
DO(level)	A switch option that controls the digital output function. When enabled, it allows control of the output level state. The current DI state is displayed as "high level." When disabled, the digital output function is turned off.
HTTP	A switch option that enables or disables IO management and access via the HTTP protocol. When enabled, IO settings can be managed through HTTP; when disabled, HTTP-based operations are not available.
Time	Used to configure time-related parameters for IO operations.

DI Function Control	A switch option that enables or disables digital input function control. When enabled, it allows monitoring and managing input signals; when disabled, digital input control is turned off.

2.8 Maintenance

2.8.1 Platform

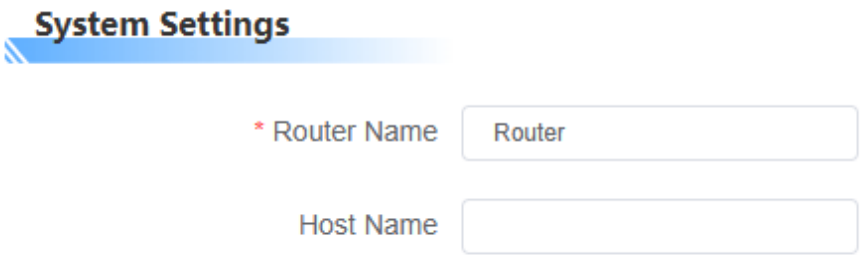
Field Name	Description
Remote Login Server IP	Enter the IP address of the remote login server.
Remote Login Server Port	Enter the port number for the remote login server.
Heart Interval	Sets the time interval (in seconds) for sending heartbeat messages between the router and the remote management platform.
3G Flow Upload Interval	Defines the time interval (in seconds) for uploading 3G network traffic data to the remote management platform.
Device Code	A unique identifier assigned to the device.
Device Type Description	Enter a description of the device type.
Customized Local Domian	Allows you to specify a custom local domain name for network access or identification.

2.9 System

2.9.1 System Settings

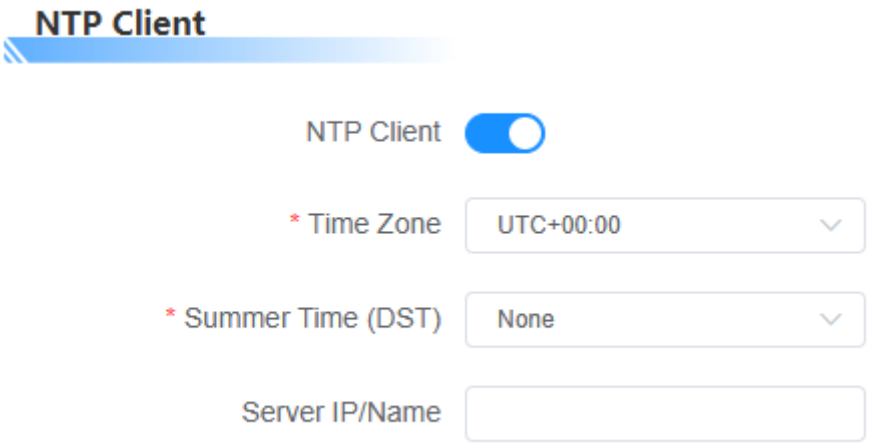
- **System Settings**

You can modify both the router's name and the host name in the system settings.



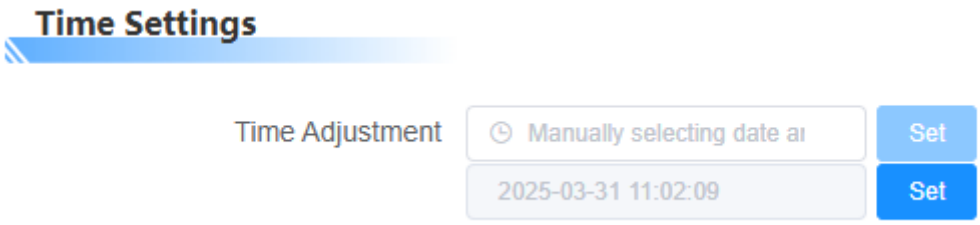
- **NTP Client**

Enabling the NTP Client lets you configure the Time Zone, Daylight Saving Time, and Server IP/Name.

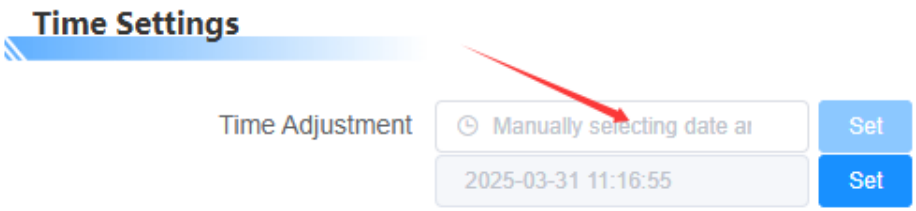


- **Time Settings**

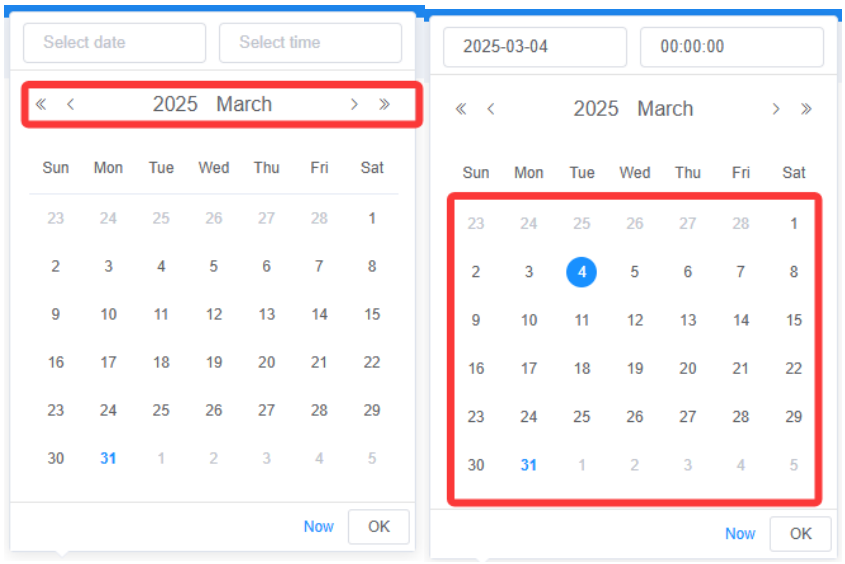
You can configure the router's system time by selecting the correct month, date, and time to ensure accurate synchronization.



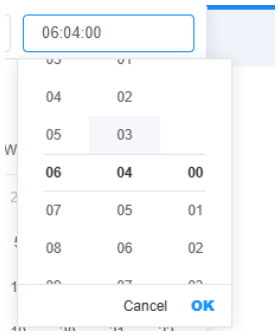
Click the box.



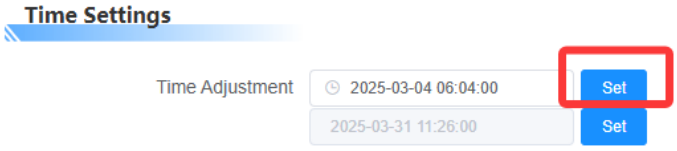
Select the month and date, choose the desired time.



Choose the desired time, and click "OK."



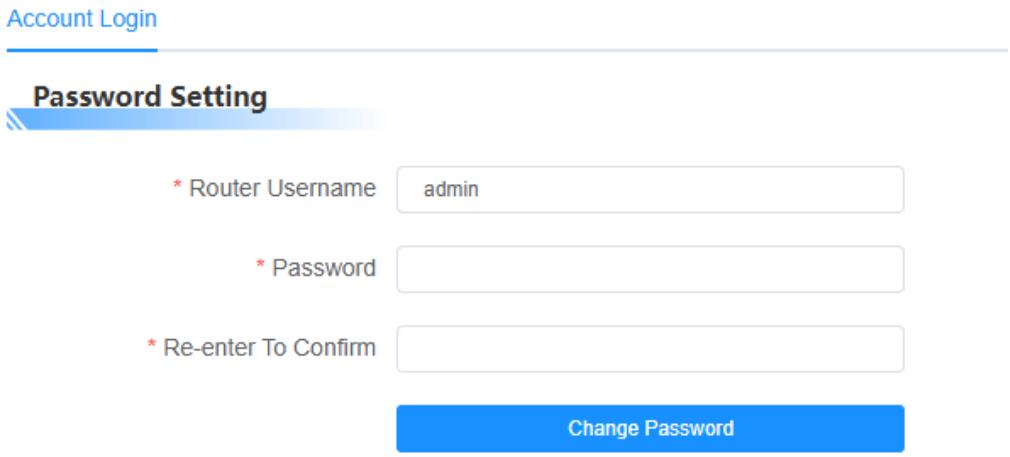
Then, click the "Set" button to apply the selected date and time.



2.9.2 Login MGT

- **Account Login**

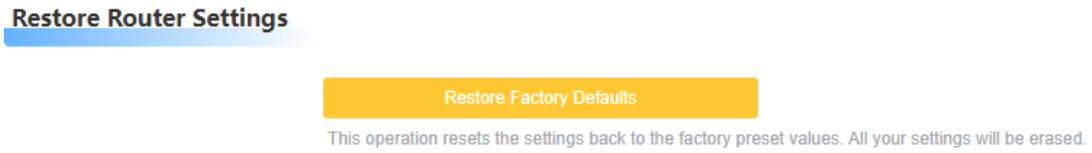
You can modify the router's username and password. This allows you to enhance security by setting a strong password and managing user access. It is recommended to use a combination of letters, numbers, and special characters for better protection.



2.9.3 Restore

- **Restore Router Settings**

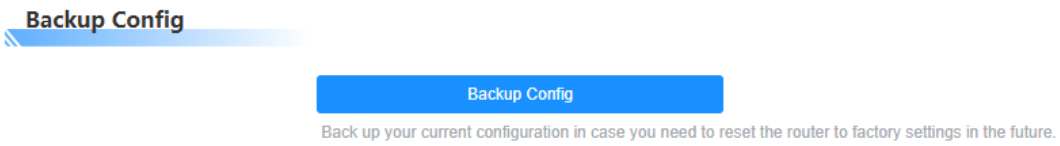
This operation will restore the router to its factory default settings, erasing all custom configurations, including network settings, passwords, and user preferences. It is recommended to back up important settings before proceeding.



2.9.4 Backup

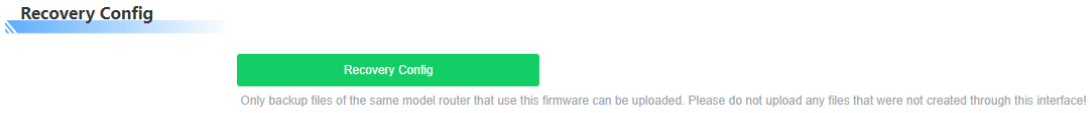
- **Backup Config**

Create a backup of your current router configuration to safeguard your settings. This ensures you can quickly restore them if the router is reset to factory defaults or experiences unexpected issues.



- **Recovery Config**

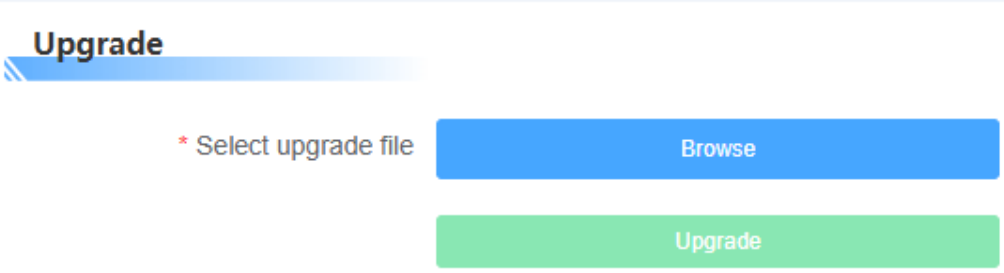
Only configuration backup files from the same router model and firmware version can be uploaded for restoration. Uploading incompatible files or those not created through this interface may cause errors or system instability. Please ensure you use the correct backup file to avoid potential issues.



2.9.5 Upgrade

- **Upgrade**

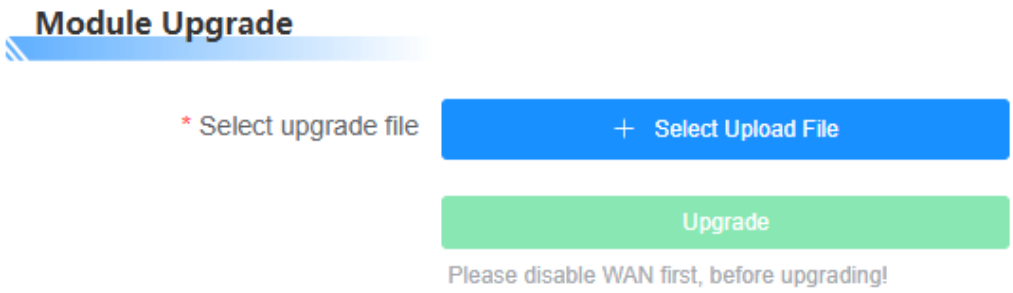
To upgrade the router's firmware, first obtain the corresponding software file from your local storage. Once the file is selected, click the "Upgrade" button to begin the upgrade process. The system will automatically initiate the upgrade, and the router will restart once the process is complete. Ensure that the router is not powered off during the upgrade to avoid potential issues. It’s recommended to back up the current configuration before upgrading to prevent data loss.



2.9.6 Module Upgrade

- **Module Upgrade**

To upgrade the communication module's firmware, first obtain the appropriate software file from local storage. After selecting the file, click the "Upgrade" button to initiate the upgrade process. The system will then begin updating the module's firmware.


Module Upgrade
* Select upgrade file
+ Select Upload File
Upgrade
Please disable WAN first, before upgrading!

Chapter 3 LEDs

- **WIFI LED**

The WiFi LED is located in the LED indicator area on the right side of the front panel, positioned at the upper left.

Action	Description
LED turned ON	WIFI is enabled, and the WIFI function is available.
LED turned OFF	WIFI is disabled.

- **Online LED**

The Online LED is located in the LED indicator area on the right side of the front panel, positioned at the lower left.

Action	Description
LED turned ON	Connected to 3G/4G cellular network
LED turned OFF	No SIM card or bad PIN

- **LAN LED**

The LAN LED is located in the LED indicator area on the right side of the front panel, positioned at the middle up.

Action	Description
LED turned ON	Operating as a 10/100 Mbps connection for LAN
LED blinking	Connection established and there is activity on this port (data being transferred)
LED turned OFF	No link established

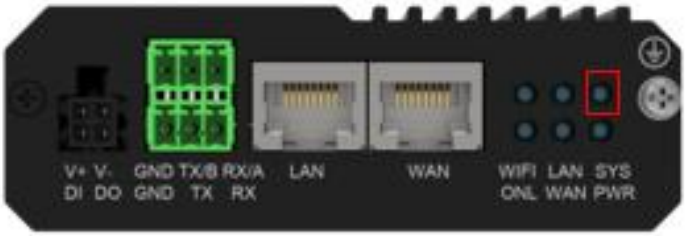
- **WAN LED**

The WAN LED is located in the LED indicator area on the right side of the front panel, positioned at the middle down.

Action	Description
LED turned ON	Operating as a 10/100 Mbps connection for WAN
LED blinking	Connection established and there is activity on this port (data being transferred)
LED turned OFF	No link established

- **System LED**

The system LED is located in the LED indicator area on the right side of the front panel, positioned at the right up.



Action	Description
LED blinking every 1 sec	The device is operating normally.
LED turned OFF	The device is not powered on or has been turned off.

- **Power LED**

The system LED is located in the LED indicator area on the right side of the front panel, positioned at the right down.

Action	Description
LED turned ON	Router is powered up
LED turned OFF	Router is not powered up

Chapter 4 Installation

4.1 Din Rail Kit Installation 1 (Back Side)

Step 1: Flip the YF355 to its back side and take out the DIN rail bracket and two screws from the rail tool kit.

Step 2: Align the two mounting holes of the DIN rail bracket with the slots on the back of the main unit and position it in place.

Step 3: Secure the bracket with the supplied screws and tighten them to complete the installation.

4.2 Din Rail Kit Installation 2 (Side Panel)

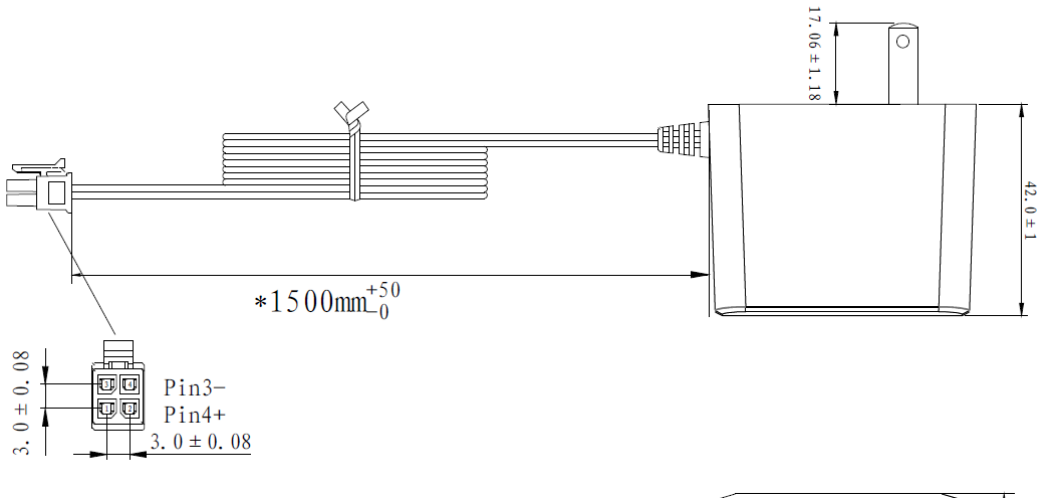
Step 1: Prepare the router and the DIN rail tool kit, and take out the DIN rail bracket and two screws from the kit.

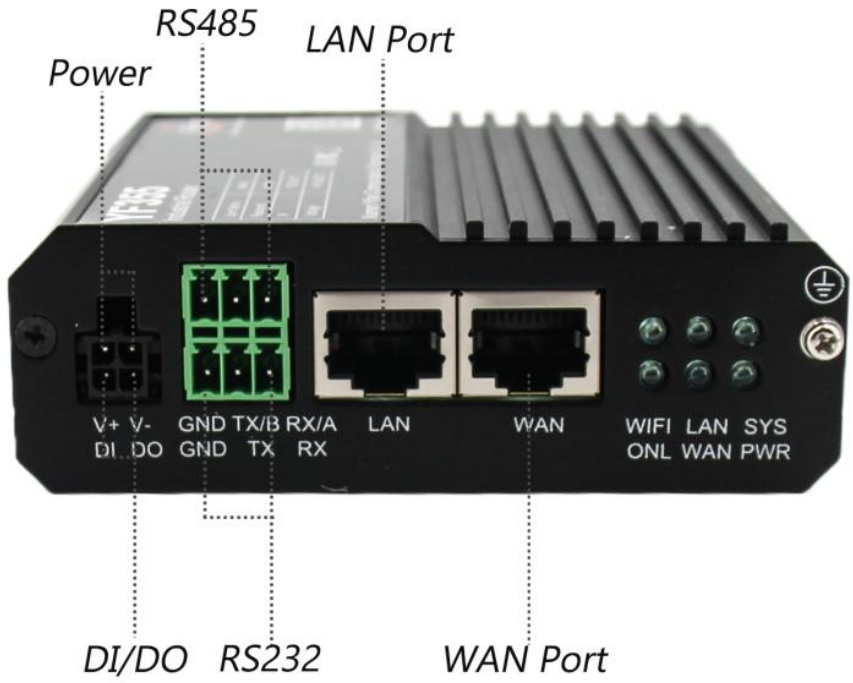
Step 2: Both sides of the router have DIN rail slots; choose one slot for installation as needed.

Step 3: Align the mounting holes of the DIN rail bracket with the selected slot and position it in place.

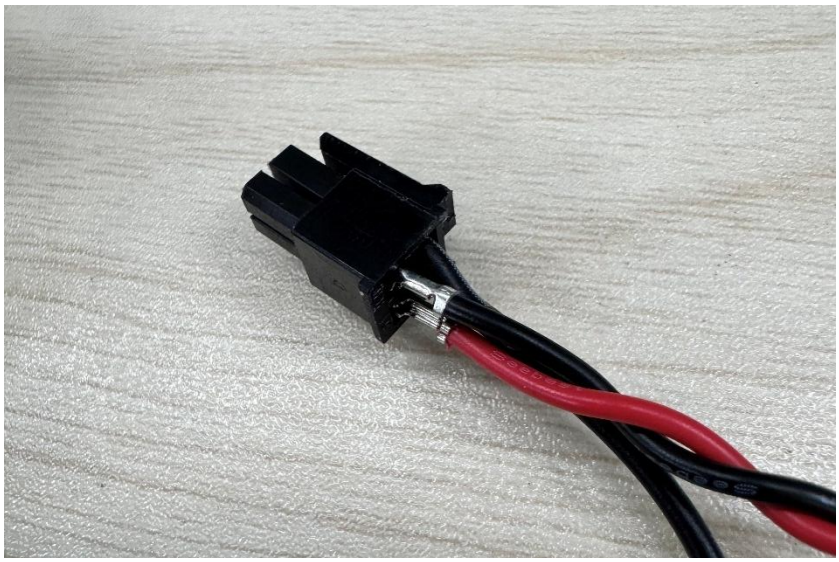
Step 4: Secure the bracket with the supplied screws and tighten them to complete the installation.

4.3 DI/DO Connection Cable Installation





Step 1: Before installation, prepare the power cable, DI/DO signal cables, and the host device. Make sure all cables and connectors are in good condition.



Step2: Insert the red wire as the DO signal into the lower right terminal of the power connector and insert the black wire as the DI signal into the lower left terminal. After insertion, gently pull the wires to ensure they are firmly secured.

Step 3: Connect the power terminal with the attached DI/DO cables to the corresponding power port on the host device, and check that the connection is tight and not loose. Finally, verify that all connections are correct and secure. Then power on the device, and the DI/DO function will be ready for use.