Industrial Router Pro Series

UR32

User Guide

Preface

Thanks for choosing Milesight UR32 industrial cellular router. The UR32 industrial cellular router delivers tenacious connection over network with full-featured design such as automated failover/failback, extended operating temperature, dual SIM cards, hardware watchdog, VPN, Fast Ethernet and beyond.

This guide describes how to configure and operate the UR32 industrial cellular router. You can refer to it for detailed functionality and router configuration.

Readers

This guide is mainly intended for the following users:
- Network Planners
- On-site technical support and maintenance personnel
- Network administrators responsible for network configuration and maintenance

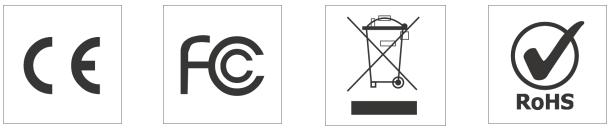
Safety Precautions

Milesight will not shoulder responsibility for any loss or damage resulting from not following the instructions of this operating guide.

- The device must not be disassembled or remodeled in any way.
- To avoid risk of fire and electric shock, do keep the product away from rain and moisture before installation.
- Do not place the device where the temperature or humidity is below/above the operating range.
- The device must never be subjected to drops, shocks or impacts.
- Make sure the device is firmly fixed when installing.
- Make sure the plug is firmly inserted into the power socket.
- Do not pull the antenna or power supply cable, detach them by holding the connectors.

Declaration of Conformity

UR32 is in conformity with the essential requirements and other relevant provisions of the CE, FCC, and RoHS.



For assistance, please contact
Milesight technical support:
Email: iot.support@milesight.com
Support Portal: support.milesight-iot.com
Tel: 86-592-5085280
Fax: 86-592-5023065
Address: Building C09, Software Park III, Xiamen 361024, China

Revision History

Date	Doc Version	Description
May. 16, 2019	V 1.1	Initial version
Nov. 14, 2019	V 1.2	Add Python, SMS, IP passthrough functions
May 11, 2020	V 1.3	Web interfaces upgrade
Dec. 9, 2020	V 2.0	Layout replace
Sept. 17, 2021	V 2.1	1. Cellular and ping detection support IPv6 2. Add WAN connection type: DHCPv6 client, DS-Lite 3. Add DHCPv6 Server feature 4. Add IPv6 static routing feature 5. Add Expert Option box in IPsec settings 6. Support SMS inbox and outbox record clear
June 30, 2023	V 2.2	1. Add high priority link revert feature; 2. Add MQTT and TR069 feature; 3. Support customized cellular MTU and IMS; 4. Support to import openVPN file configurations, add tls-crypt mode and authentication mode; 5. Update Modbus Master/Slave to Modbus Client/Server; 6. Support to configure L2TP hostname.
July 5, 2024	V 2.3	1. Add Wireguard VPN feature; 2. Add cellular band selection and subnet mask customization; 3. Support to sync time with cellular operator; 4. Support to show Ethernet port connection status and configure PoE settings; 5. Support MQTT feature on DI and serial DTU mode downlink; 6. Update default secondary ICMP and DNS server

		address; 7. Add WPA/WPA2-Enterprise encryption mode of WLAN client mode; 8. IPsec setting web GUI optimization.
April 11, 2025	V 2.4	1. Add ZeroTier VPN. 2. Compatible with DeviceHub 2.0 and Milesight Development Platform. 3. Support 802.1x protocol to connect to Radius servers. 4. Add cellular custom DNS server option. 5. Optimize the configuration modes of Email groups and phone groups. 6. Support to configure username, test email address in SMTP client settings. 7. Add byte order on Modbus channel settings.
Sep.19, 2025	V 2.5	1. Add DLMS feature. 2. Support cellular interface IP passthrough 3. Support multiple VPN 4. Support policy routing function 5. Switch setting web GUI optimization. 6. Support to configure IP, reporting interval in DDNS settings. 7. Support to configure service name, VLAN ID in PPPoE client settings. 8. Support to configure IPv6 address in Switch setting. 9. Support multiple local & remote subnets on IPsec.
Dec. 30, 2025	V 2.6	1. Modbus Client function optimization. 2. Add web password limitation and change prompt. 3. Add partial backup. 4. Add auto APN. 5. Add level change trigger mode and SNMP Trap reporting in DI setting. 6. Add Autp DST function in system time setting. 7. Support automatic IP address acquisition via interface in DMVPN setting. 8. Add multiple encryption and authentication algorithms for DMVPN.

Contents

Chapter 1 Product Introduction

1.1 Overview

UR32 is an industrial cellular router with embedded intelligent software features that are designed for multifarious M2M/IoT applications. Supporting global WCDMA and 4G LTE, UR32 provides drop-in connectivity for operators and makes a giant leap in maximizing uptime.

Adopting high-performance and low-power consumption industrial grade CPU and wireless module, the UR32 is capable of providing wire-speed network with low power consumption and ultra-small package to ensure the extremely safe and reliable connection to the wireless network.

Meanwhile, the UR32 also supports Fast Ethernet ports, serial port (RS232/RS485) and I/O (input/output), which enables you to scale up M2M application combining data and video in limited time and budget.

UR32 is particularly ideal for smart grid, digital media installations, industrial automation, telemetry equipment, medical device, digital factory, finance, payment device, environment protection, water conservancy and so on.

For details of hardware and installation, please check UR32 Quick Start Guide.

1.2 Advantages

Benefits

- Built-in high-performance NXP industrial CPU with large memory
- Fast Ethernet for fast data transmission
- Dual SIM cards for backup between multiple carrier networks, with global 2G/3G/LTE options for easy connectivity
- Multiple APN interfaces for simultaneous access to different network services
- Equipped with Ethernet, I/O, serial port, Wi-Fi, GPS for connecting diverse field assets
- Embedded Python SDK for second development
- Rugged enclosure, optimized for DIN rail or shelf mounting
- 3-year warranty included

Security & Reliability

- Automated failover/failback between Ethernet and Cellular (dual SIM)
- Enable unit with security frameworks like IPsec/OpenVPN/GRE/L2TP/PPTP/DMVPN/WireGuard/ZeroTier VPN
- Embed hardware watchdog, automatically recovering from various failure, and ensuring highest level of availability

- Establish a secured mechanism on centralized authentication and authorization of device access by supporting AAA (TACACS+, Radius, LDAP, local authentication) and multiple levels of user authority

Easy Maintenance

- Milesight DeviceHub/Development Platform provide easy setup, mass configuration, and centralized management of remote devices
- The user-friendly web interface design and more than one option of upgrade help administrator to manage the device as easy as pie
- Web GUI and CLI enable the admin to achieve simple management and quick configuration among a large quantity of devices
- Efficiently manage the remote routers on the existing platform through the industrial standard SNMP and TR069

Capabilities

- Link remote devices in an environment where communication technologies are constantly changing
- Industrial 32-bit ARM Cortex-A7 processor, high-performance operating up to 528MHz and 128 MB memory available to support more applications
- Support rich protocols like SNMP, TR069, MQTT, Modbus bridging, RIP, OSPF, etc
- Support wide operating temperature ranging from -40°C to 70°C/-40°F to 158°F

Chapter 2 Access to Web GUI

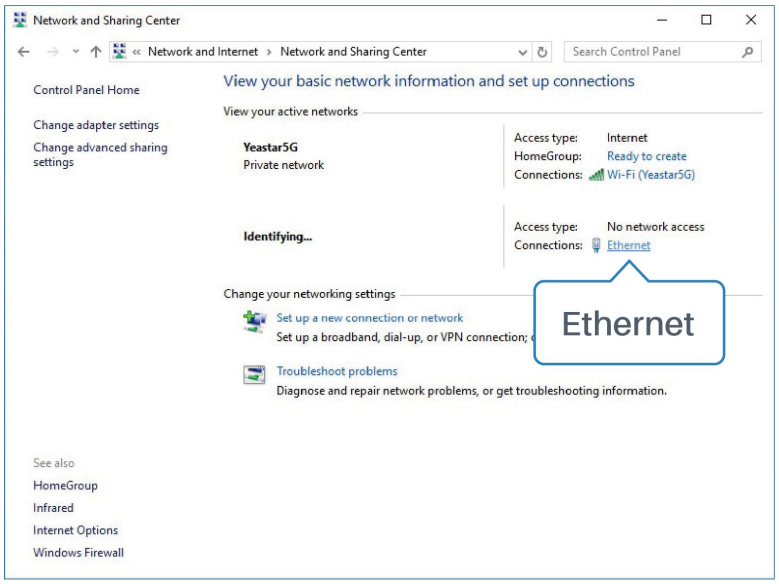
This chapter explains how to access to Web GUI of the UR32 router. Connect PC to LAN port of UR32 router directly. The following steps are based on Windows 10 operating system for your reference.

Username: **admin**

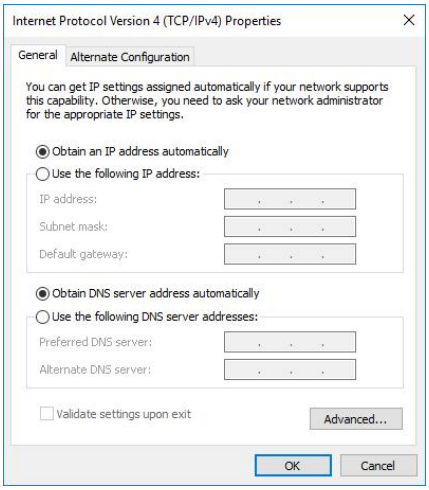
Password: **password**

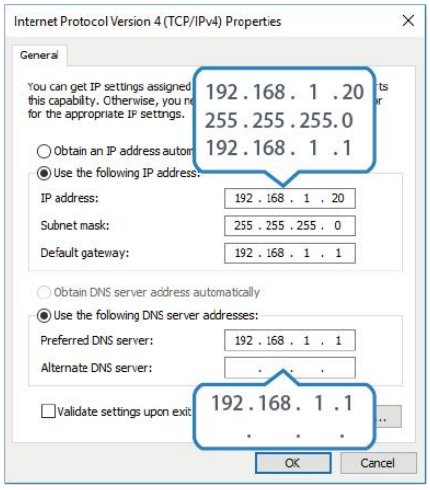
IP Address: **192.168.1.1**

1. Go to “Control Panel” → “Network and Internet” → “Network and Sharing Center”, then click “Ethernet” (May have different names).



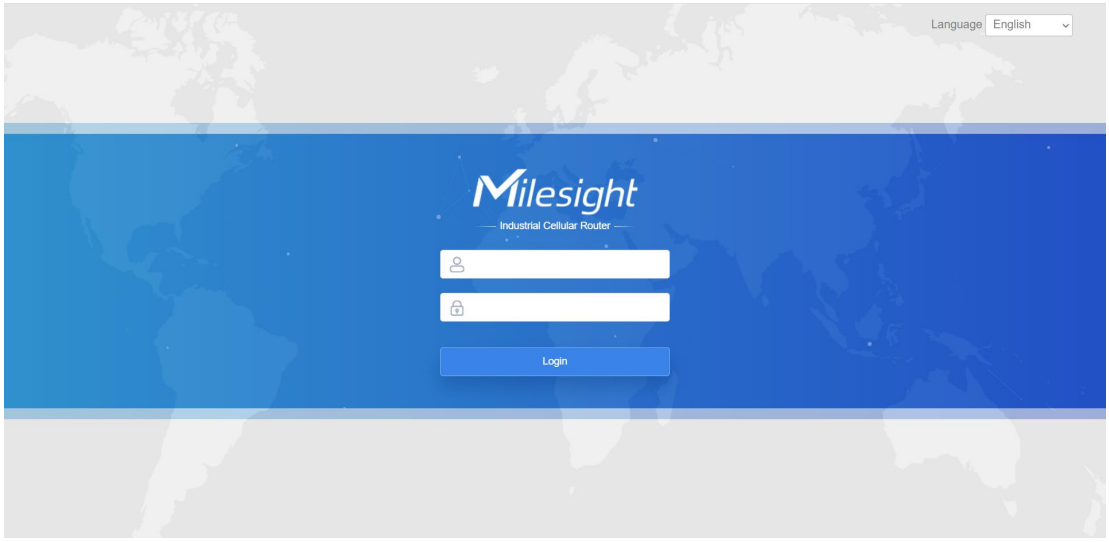
2. Go to “Properties” → “Internet Protocol Version 4(TCP/IPv4) ”, select “Obtain an IP address automatically” or “Use the following IP address”, then assign a static IP manually within the same subnet of the device.





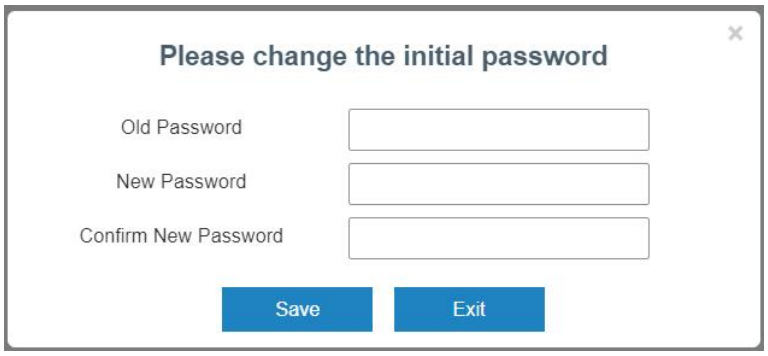
3. Open a Web browser on your PC (Chrome is recommended), type in the IP address https://192.168.1.1, and press Enter on your keyboard.

4. Enter the username, password, and click "Login".



If you enter the username or password incorrectly more than 5 times, the login page will be locked for 10 minutes.

5. After logging the web GUI, it is necessary to change the web GUI password for the first time. The password must contain at least one letter and one number.



6. Use the new password to log in to the web GUI again. After logging the web GUI, you can view system information.

Chapter 3 Web Configuration

3.1 Status

3.1.1 Overview

You can view the system information of the router on this page.

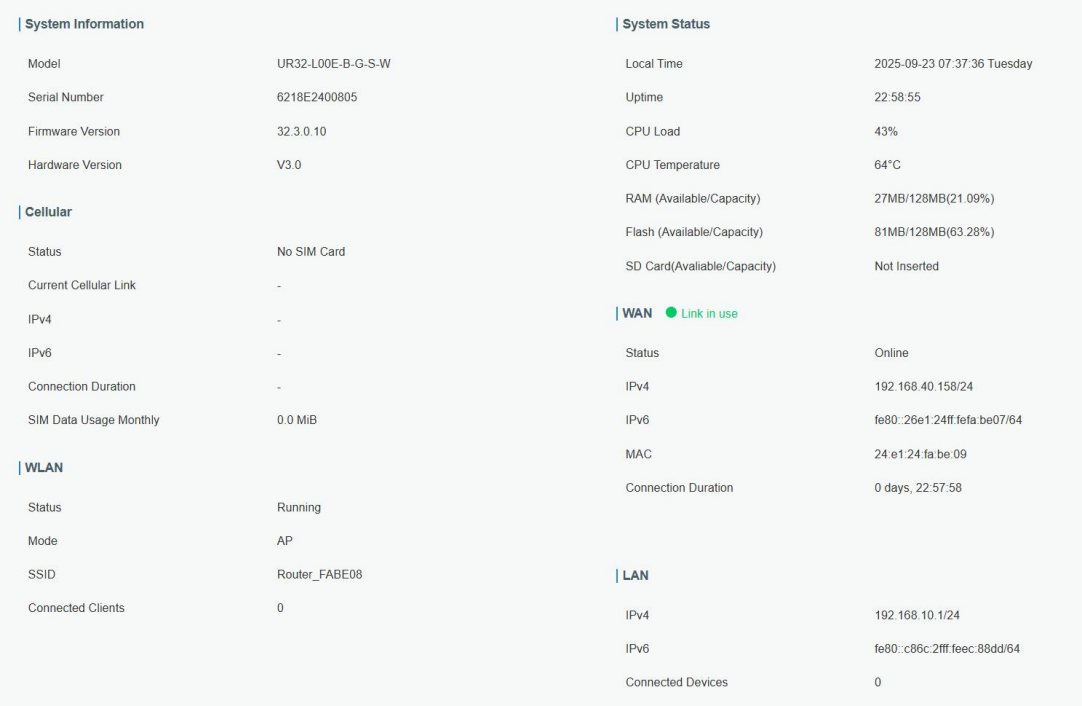


Figure 3-1-1-1

System Information	
Item	**Description**
Model	Show the model name of router.
Serial Number	Show the serial number of router.
Firmware Version	Show the currently firmware version of router.
Hardware Version	Show the currently hardware version of router.

Table 3-1-1-1 System Information

System Status	
Item	**Description**
Local Time	Show the currently local time of system.
Uptime	Show the information on how long the router has been running.
CPU Load	Show the current CPU utilization of the router.
CPU Temperature	Show current CPU temperature.
RAM (Available/Capacity)	Show the RAM capacity and the available RAM memory.
Flash (Available/Capacity)	Show the Flash capacity and the available Flash memory.
SD Card (Available/Capacity)	Show the capacity and the available memory of micro SD card if it is inserted.

Table 3-1-1-2 System Status

Cellular	
Item	**Description**
Status	Show the real-time status of the currently SIM card
Current Cellular Link	Show the cellular network currently used for the data connection.
IPv4/IPv6	Show the IPv4/IPv6 address obtained from the mobile carrier. **Note:** UR3x-L0GEU only supports IPv4.
Connection Duration	Show the connection duration of the currently SIM card.
SIM Data Usage Monthly	Show the monthly data usage statistics of currently used SIM card.

Table 3-1-1-3 Cellular Status

WAN	
Item	**Description**
Status	Show the currently status of WAN port.
IPv4/IPv6	The IPv4/IPv6 address configured WAN port.
MAC	The MAC address of the Ethernet port.
Connection Duration	Show the connection duration of the WAN port.

Table 3-1-1-4 WAN Status

WLAN (Only applicable for Wi-Fi model)	
Item	**Description**
Status	Show the currently status of WLAN.
IP	Show the WLAN mode (AP or client).
SSID	Show the SSID of the WLAN AP or client.
Connected Clients	Show the amount of connected devices when mode is AP.

Table 3-1-1-5 WLAN Status

LAN	
Item	**Description**
IP4/IPv6	Show the IP4/IPv6 address of the LAN port.
Connected Devices	Number of devices that connected to the router's LAN.

Table 3-1-1-6 LAN Status

3.1.2 Cellular

You can view the cellular network status of router on this page.

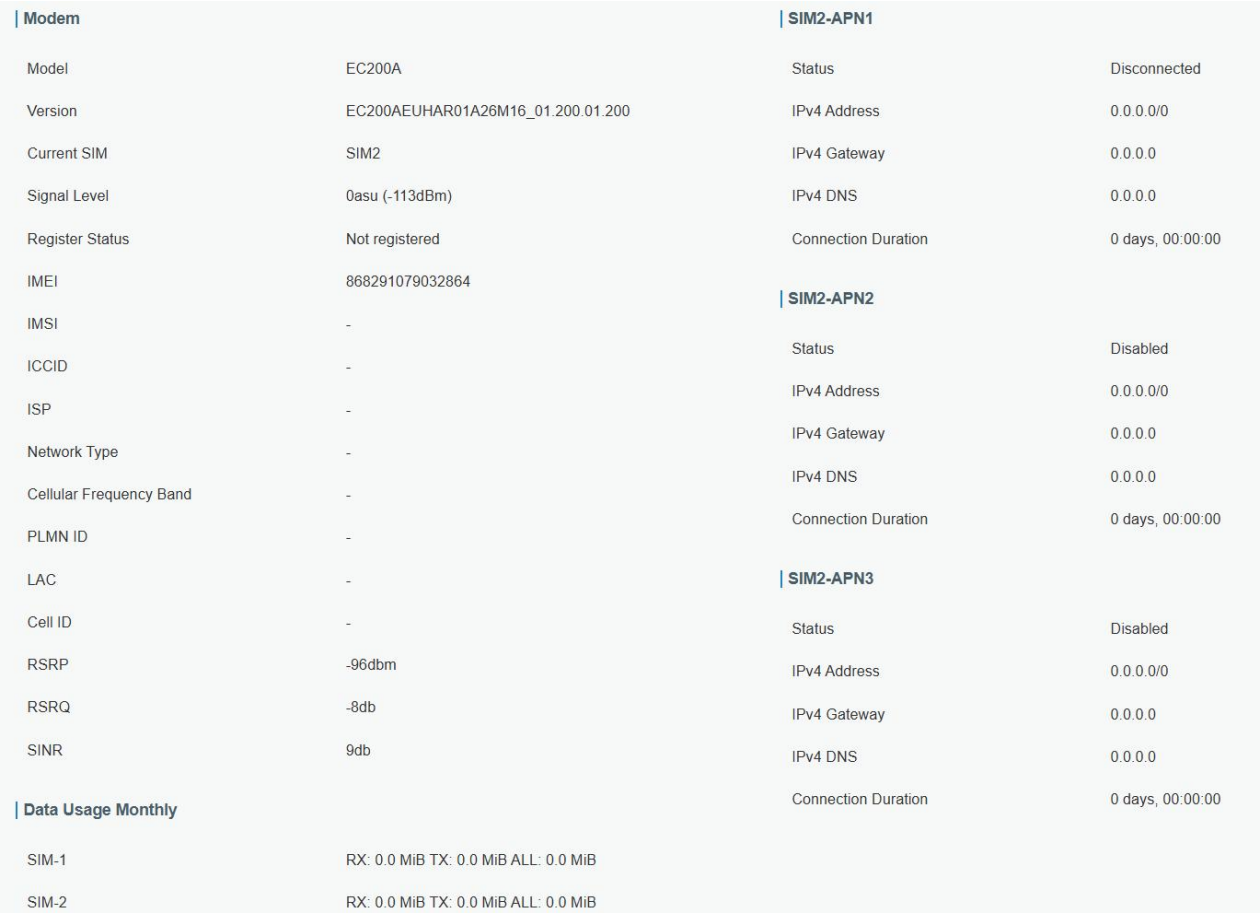


Figure 3-1-2-1

Modem Information	
Item	**Description**
Status	Show corresponding detection status of module and SIM card.
Version	Show the cellular module firmware version.
Current SIM	Show the current SIM card used.
Signal Level	Show the cellular signal level.
Register Status	Show the registration status of SIM card.
IMEI	Show the IMEI of the module.
IMSI	Show IMSI of the SIM card.
ICCID	Show ICCID of the SIM card.
ISP	Show the network provider which the SIM card registers on.
Network Type	Show the connected network type, such as LTE, 3G, etc.
PLMN ID	Show the current PLMN ID, including MCC, MNC, LAC and Cell ID.
LAC	Show the location area code of the SIM card.
Cell ID	Show the Cell ID of the SIM card location.

Table 3-1-2-1 Modem Information

SIM-APN	
Item	**Description**
Status	Show the connection status of cellular network.

IPv4/IPv6 Address	Show the IPv4/IPv6 address and netmask of cellular network. **Note:** UR3x-L0GEU only supports IPv4.
IPv4/IPv6 Geteway	Show the IPv4/IPv6 gateway and netmask of cellular network. **Note:** UR3x-L0GEU only supports IPv4.
IPv4/IPv6 DNS	Show the IPv4/IPv6 DNS of cellular network. **Note:** UR3x-L0GEU only supports IPv4.
Connection Duration	Show information on how long the cellular network has been connected.

Table 3-1-2-2 Network Status

Data Usage Monthly	
Item	**Description**
SIM-1	Show the monthly data usage statistics of SIM-1.
SIM-2	Show the monthly data usage statistics of SIM-2.

Table 3-1-2-3 Data Usage Information

3.1.3 Network

On this page you can check the WAN and LAN status of the router.

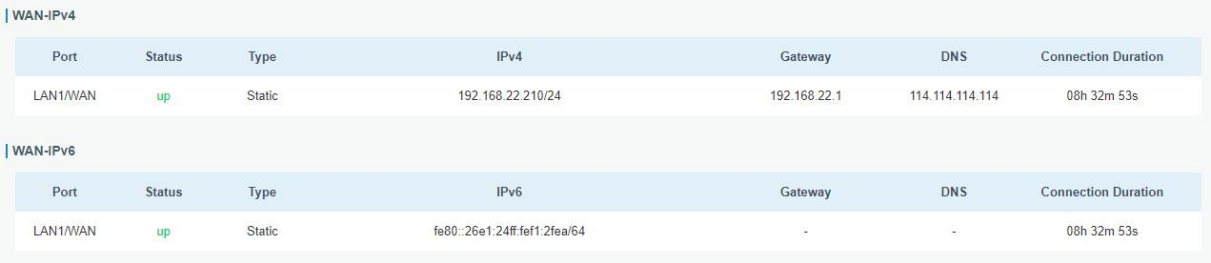


Figure 3-1-3-1

WAN Status	
Item	**Description**
Port	Show the name of WAN port.
Status	Show the status of WAN port. "up" refers to a status that WAN is enabled and Ethernet cable is connected. "down" means Ethernet cable is disconnected or WAN function is disabled.
Type	Show the dial-up connection type of WAN port.
IPv4/IPv6	Show the IPv4 address with netmask or IPv6 address with prefix-length of WAN port.
Gateway	Show the gateway of WAN port.
DNS	Show the DNS of WAN port.
Connection Duration	Show the information on how long the Ethernet cable has been connected on WAN port when WAN function is enabled. Once WAN function is disabled or Ethernet connection is disconnected, the duration will stop.

Table 3-1-3-1 WAN Status

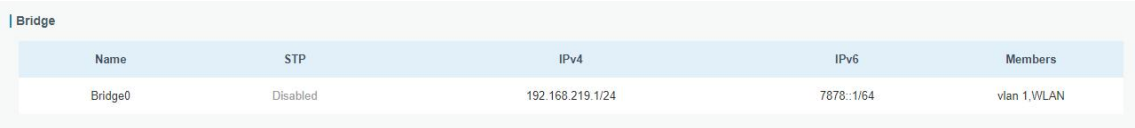


Figure 3-1-3-2

Bridge	
Item	**Description**
Name	Show the name of the bridge interface.
STP	Show if STP is enabled.
IPv4/IPv6	Show the IPv4/IPv6 address and netmask of the bridge interface.
Netmask	Show the Netmask of the bridge interface.
Members	Show the members of the bridge interface.

Table 3-1-3-2 Bridge Status

3.1.4 WLAN (Only Applicable to Wi-Fi Version)

You can check Wi-Fi status on this page, including the information of access point and client.

Figure 3-1-4-1

WLAN Status	
Item	**Description**
WLAN Status	
Name	Show the name of the Wi-Fi interface .
Status	Show the status of the Wi-Fi interface.
Type	Show the Wi-Fi interface type.
SSID	Show the SSID of the router when the interface type is AP. Show the SSID of AP which the router connected to when the interface type is Client.
IP Address	Show the IP address of the router when the interface type is AP. Show the IP address of AP which the router connected to when the interface type is Client.
Netmask	Show the netmask of the router when the interface type is AP. Show the netmask of AP which the router connected to when the interface type is Client.
Associated Stations	
SSID	Show the SSID of the router when the interface type is AP. Show the SSID of AP which the router connected to when the interface type is Client.

MAC Address	Show the MAC address of the client which connected to the router when the interface type is AP. Show the MAC address of the AP which the router connected to when the interface type is Client.
IP Address	Show the IP address of the client which connected to the router when the interface type is AP. Show the IP address of the AP which the router connected to when the interface type is Client.
Connection Duration	Show the connection duration between client device and router when the interface type is AP. Show the connection duration between router and the AP when the interface type is Client.

Table 3-1-4-1 WLAN Status

3.1.5 VPN

You can check VPN status on this page, including PPTP, L2TP, IPsec, OpenVPN and DMVPN.

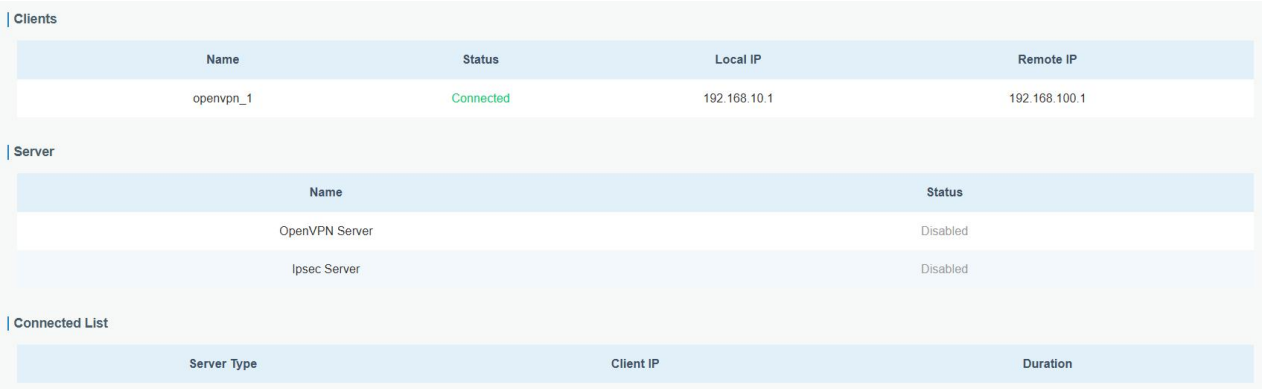


Figure 3-1-5-1

VPN Status	
Item	**Description**
Clients	
Name	Show the name of the enabled VPN clients.
Status	Show the status of client. "Connected" refers to a status that client is connected to the server. "Disconnected" means client is disconnected to the server.
Local IP	Show the local IP address of the tunnel.
Remote IP	Show the real remote IP address of the tunnel.
Server	
Name	Show the name of the enabled VPN Server.
Status	Show the status of Server.
Connected List	
Server Type	Show the type of the server.
Client IP	Show the IP address of the client which connected to the server.
Duration	Show the information about how long the client has been connected to this server when the server is enabled. Once the server is disabled or connection is disconnected, the

	duration will stop counting.

Table 3-1-5-1 VPN Status

3.1.6 Routing

You can check routing status on this page, including the routing table and ARP cache.

Figure 3-1-6-1

Item	Description
Routing Table	
Destination	Show the IP address of destination host or destination network.
Netmask/Prefix Length	Show the netmask or prefix length of destination host or destination network.
Gateway	Show the IP address of the gateway.
Interface	Show the outbound interface of the route.
Metric	Show the metric of the route.
ARP Cache	
IP	Show the IP address of ARP pool.
MAC	Show the IP address's corresponding MAC address.
Interface	Show the binding interface of ARP.

Table 3-1-6-1 Routing Information

3.1.7 Host List

You can view the host information on this page.

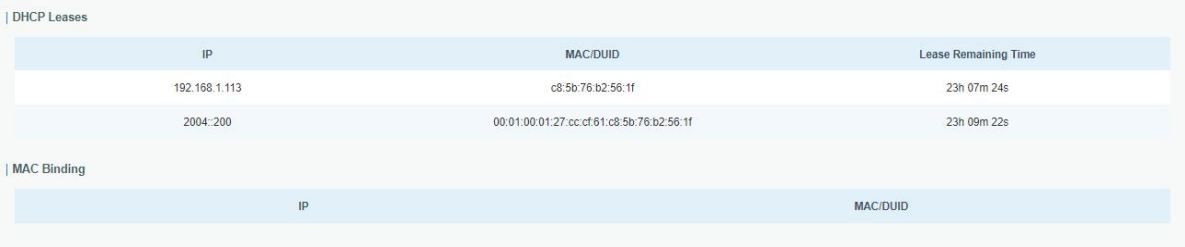


Figure 3-1-7-1

Host List	
Item	**Description**
DHCP Leases	
IP Address	Show IP address of DHCP client
MAC/DUID	Show MAC address of DHCPv4 client or DUID of DHCPv6 client.
Lease Time Remaining	Show the remaining lease time of DHCP client.
MAC Binding	
IP & MAC	Show the IP address and MAC address set in the Static IP list of DHCP service.

Table 3-1-7-1 Host List Description

3.1.8 GPS (Only Applicable to GPS Version)

When GPS function is enabled and the GPS information is obtained successfully, you can view the latest GPS information including GPS Time, Latitude, Longitude and Speed on this page.

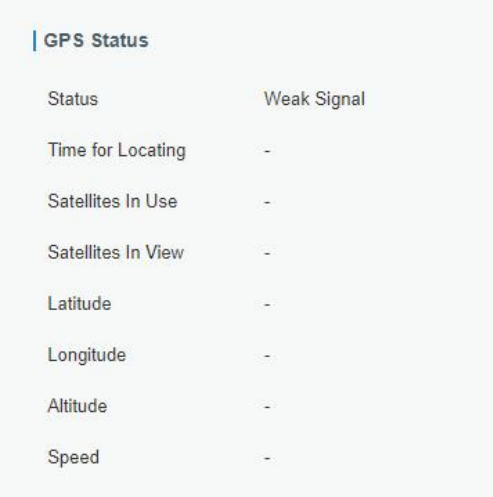


Figure 3-1-8-1

GPS Status	
Item	**Description**
Status	Show the status of GPS.
Time for Locating	Show the time for locating.
Satellites In Use	Show the quantity of satellites in use.
Satellites In View	Show the quantity of satellites in view.
Latitude	Show the Latitude of the location.
Longitude	Show the Longitude of the location.
Altitude	Show the Altitude of the location.

Speed	Show the speed of movement.

Table 3-1-8-1 GPS Status Description

3.2 Network

3.2.1 Interface

3.2.1.1 Link Failover

This section describes how to configure link failover strategies, their priority and the ping settings, each rule owns its own ping rules by default. Router will follow the priority to choose the next available interface to access the internet, make sure you have enable the full interface that you need to use here. If priority 1 can only use IPv4, UR32 will select a second link which IPv6 works as main IPv6 link and vice versa.

Note: If the priority of one SIM is higher than the other, the device will switch the APN links among the high priority SIM first. **Example:** The configuration order is SIM1-APN1, SIM2-APN1, SIM1-APN2, the real switch order is SIM1-APN1, SIM1-APN2, SIM2-APN1.

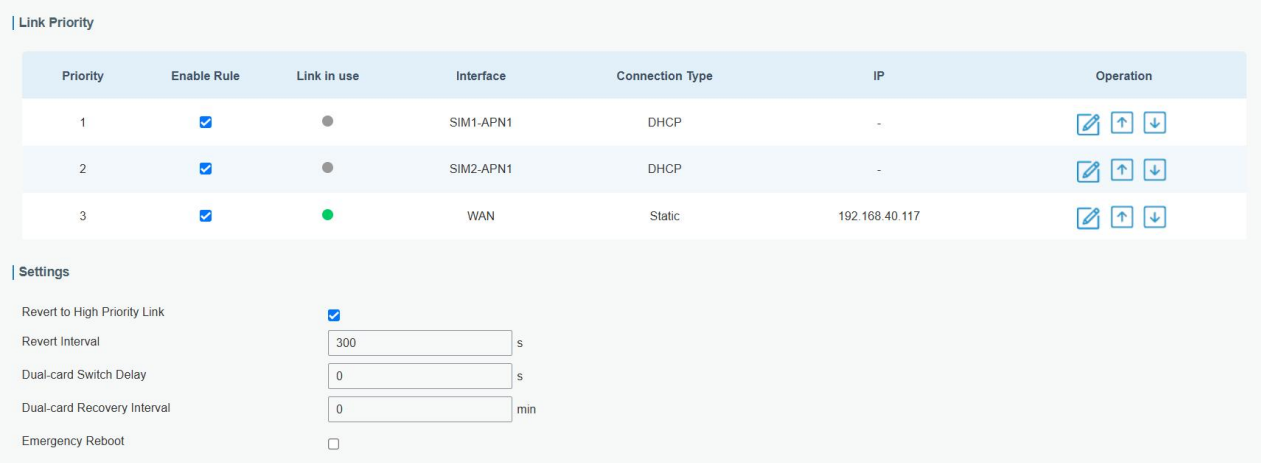


Figure 3-2-1-1

Link Failover	
Item	**Description**
Link Priority	
Priority	Display the priority of each interface, you can modify it by the operation's up and down button.
Enable Rule	If enabled, the router will put this interface into its switching rule. For the Cellular interface, if it's not enabled here, the interface will be disabled as well.
Link In Use	Mark whether this interface is in use with Green color
Interface	Display the name of the interface.
Connection type	Display how to obtain the IP address in this interface, like static IP or DHCP.
IP	Display the IP address of the interface.
Operation	You can change the priority of the rules and configure the ping detection rules here.
Settings	

Revert to High Priority Link	When the connection of high priority link returns back, reverting back to high priority link.
Revert Interval	Specify the number of seconds to waiting for switching to the link with higher priority, 0 means disable the function.
Dual-card Switch Delay	The delay time to switch to low priority card when high priority cellular connection is failed. 0 means switching immediately.
Dual-card Recovery Interval	The interval to detect high priority cellular connection. If the connection recovers, switching back to high priority cellular link.
Emergency Reboot	Enable to reboot the device if no link is available.

Table 3-2-1-1 Link Failover Parameters

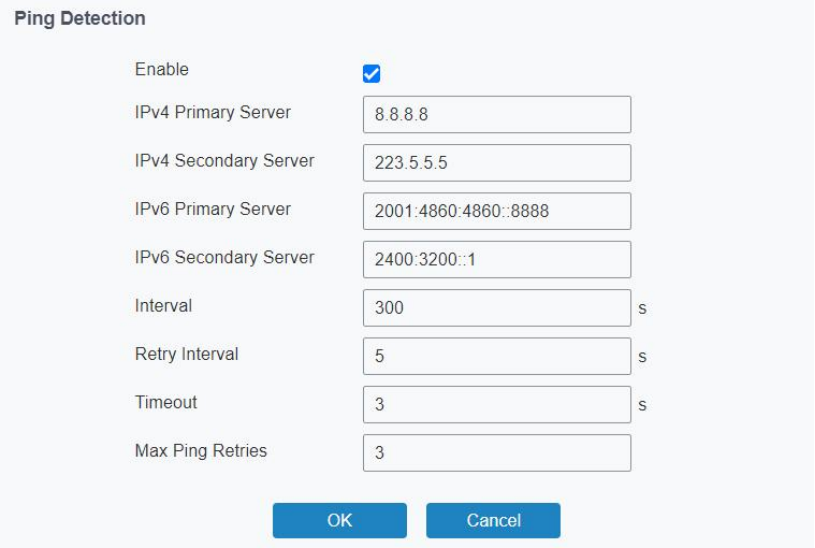


Figure 3-2-1-2

Ping Detection	
Item	**Description**
Enable	If enabled, the router will periodically detect the connection status of the link.
IPv4/IPv6 Primary Server	The router will send ICMP packet to the IPv4/IPv6 address or hostname to determine whether the Internet connection is still available or not.
IPv4/IPv6 Secondary Server	The router will try to ping the secondary server name if primary server is not available.
Interval	Time interval (in seconds) between two Pings.
Retry Interval	Set the ping retry interval. When ping failed, the router will ping again in every retry interval.
Timeout	The maximum amount of time the router will wait for a response to a ping request. If it does not receive a response for the amount of time defined in this field, the ping request will be considered to have failed.
Max Ping Retries	The retry times of the router sending ping request until determining that the connection has failed.

Table 3-2-1-2 Ping Detection Parameters

3.2.1.2 Cellular

This section explains how to set the related parameters for the cellular network. The UR32 cellular router has two cellular interfaces, namely SIM1 and SIM2. Each cellular interface is configured to establish three cellular network sub-interfaces, each supporting the configuration of one APN. The three sub-cellular network interfaces under the same cellular network interface can be active at one time, enabling different network services to be accessed simultaneously through multiple APNs when the cellular network is registered. Only one cellular interface is active at one time. If both cellular interfaces are enabled, it will follow the priority rule configured in the **Link Failover** page.

Note:

- To use the multi-APN feature for the first time, a device reboot is required.
- After enabling multi-APN, different sub-interfaces on the same SIM card cannot add the same APN.

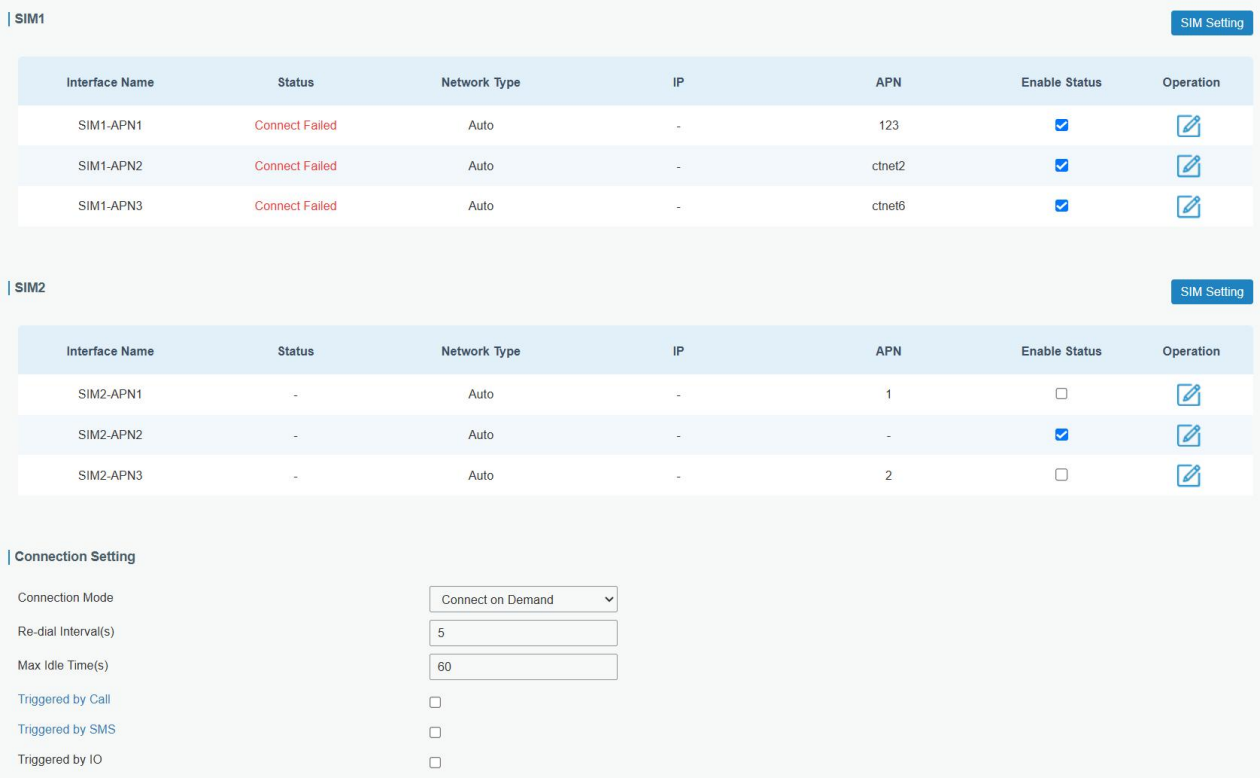


Figure 3-2-1-3

Cellular Setting	
Item	**Description**
Interface Name	Display cellular network interface names.
Status	Show the cellular network connection status.
Network Type	Select from "Auto", "4G Only", "3G Only", and "2G Only". Auto: connect to the network with the strongest signal automatically. 4G Only: connect to 4G network only. And so on.
IP	IP address corresponding to this cellular network interface.

APN	Enter the Access Point Name for the cellular dial-up connection provided by the local ISP.
Enable Status	Show the enable status of this interface.
Operation	You can edit the configuration items for this cellular network interface.
Connection Setting	
Item	**Description**
Connection Mode	Select "Always Online" and "Connect on Demand".
Re-dial Interval(s)	Set the interval to dial into ISP when it loses connection. The default value is 5s.
Max Idle Times	Set the maximum duration of the router when the current link is under idle status. Range: 10-3600
Triggered by Call	The router will automatically switch from offline mode to cellular network mod e upon receiving a call from a specific phone number.
Call Group	Select a call group for the call trigger. Go to **System > Phone&SMS > Phone** to set up phone group.
Triggered by SMS	The router will switch from offline mode to cellular network mode automatically when it receives a specific SMS from the specific mobile phone.
SMS Group	Select an SMS group for the trigger. Go to **System > Phone&SMS > SMS** to set up an SMS group.
SMS Text	Fill in the SMS content for triggering.
Triggered by IO	The router will switch from offline mode to cellular network mode automatically when the DI status is changed. Go to **Industrial > I/O > DI** to configure the trigger condition.

Table 3-2-1-3 Cellular Status

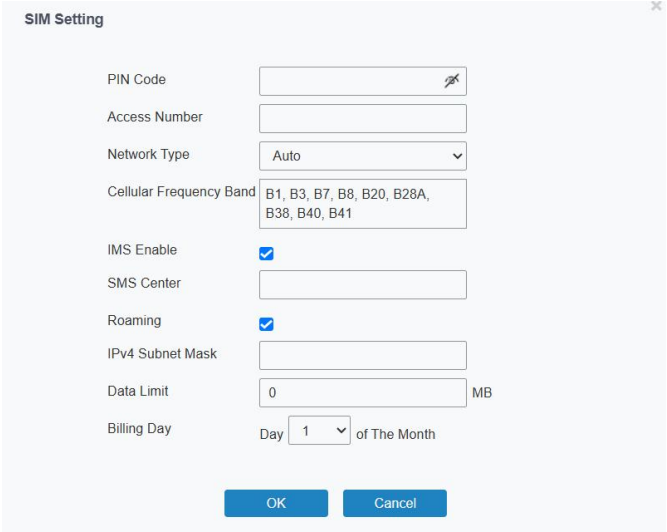


Figure 3-2-1-4

SIM Setting	
Item	**Description**
PIN Code	Enter a 4-8 characters PIN code to unlock the SIM.
Access Number	Enter the dial-up center NO. For cellular dial-up connection provided by local ISP.

Network Type	Select from "Auto", "4G Only", "3G Only", and "2G Only". Auto: connect to the network with the strongest signal automatically. 4G Only: connect to 4G network only. And so on.
Cellular Frequency Band	Select the cellular bands used to register the cellular network. It can be used to optimize cellular speeds by selecting specific bands.
IMS Enable	Enable or disable IMS function.
SMS Center	Enter the local SMS center number for storing, forwarding, converting and delivering SMS message.
Roaming	Enable or disable roaming.
IPv4 Subnet Mask	Customize the cellular subnet mask. If blank, the device will use the subnet mask provided by the cellular base station.
Data Limit	When you reach the specified data usage limit, the data connection of the currently used SIM card will be disabled. 0 means disable the function.
Billing Day	Choose the billing day of the SIM card, then the router will reset the data used to 0.

Table 3-2-1-4 SIM Parameters

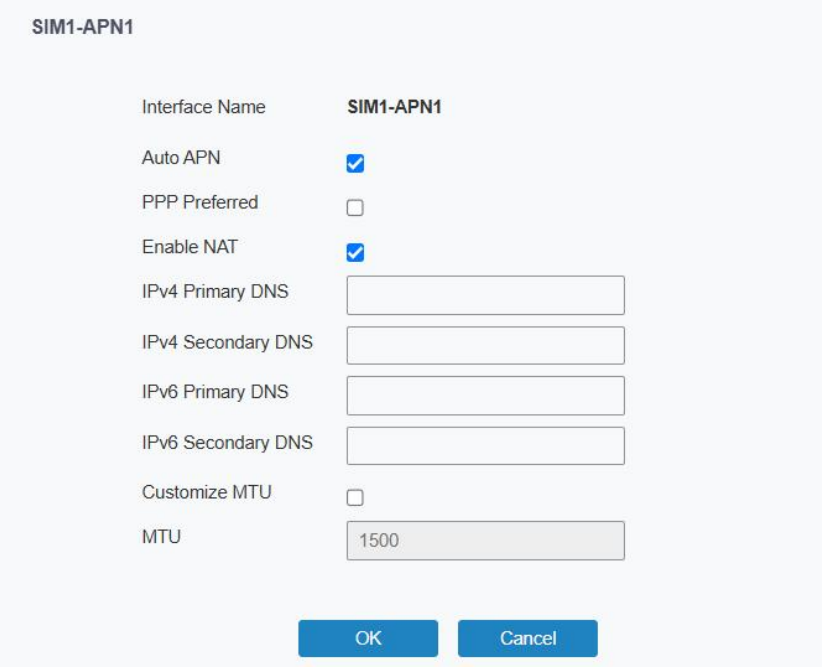


Figure 3-2-1-5

SIM-APN	
Item	**Description**
Interface Name	Display the name of the currently configured interface.
Auto APN	Enable to automatically detect the carrier and use the built-in APN database for automatic connection. When using Auto APN, there is no need to fill in protocol type, APN, username, password, and authentication method. **Note:**

	• Only the APN1 of each SIM card can use Auto APN. • On the same SIM card, Auto APN and Multi-APN cannot be enabled simultaneously.
Protocol Type	Select from "IPv4", "IPv6" and "IPv4/IPv6". **Note:** UR3x-L0GEU only supports IPv4.
APN	Enter the Access Point Name for the cellular dial-up connection provided by the local ISP.
Username	Enter the username for the cellular dial-up connection provided by the local ISP.
Password	Enter the password for the cellular dial-up connection provided by the local ISP.
Authentication Type	Select from "None", "PAP", or "CHAP".
PPP Preferred	The PPP dial-up method is preferred.
Enable NAT	Enable or disable NAT function.
IPv4/IPv6 Primary DNS	IPv4/IPv6 address of the preferred DNS server.
IPv4/IPv6 Secondary DNS	IPv4/IPv6 address of the secondary DNS server.
Customize MTU	Enable or disable to customize the maximum transmission units. When disabled, the device will use the operator's MTU settings.
MTU	Customize the maximum transmission units.

Table 3-2-1-5 APN Parameters

Related Topics

Cellular Network Connection

Phone Group

DI Setting

3.2.1.3 Port

This section describes how to configure the Ethernet port parameters.

UR32 cellular router supports 2 Fast Ethernet ports.

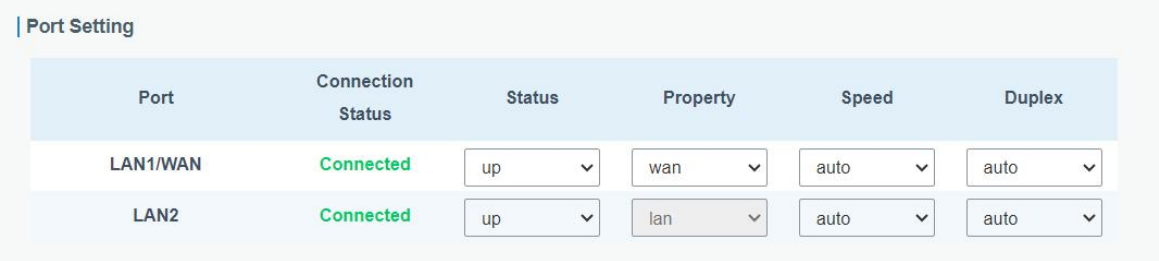


Figure 3-2-1-6

Port Setting	
Item	**Description**
Port	Users can define the Ethernet ports according to their needs.
Connection Status	Show the connection status of this Ethernet port.
Status	Set the status of the Ethernet port; select "up" to enable and "down"

	to disable.
Property	Show the Ethernet port's type, as a WAN port or a LAN port.
Speed	Set the Ethernet port's speed. The options are "auto", "100 Mbps", and "10 Mbps".
Duplex	Set the Ethernet port's mode. The options are "auto", "full", and "half".

Table 3-2-1-7 Port Parameters

Note:

- **Only the PoE version (model name included "-P") supports the below settings.**
- **These settings only work when this router is powered by 48V.**
- **Only the devices with hardware version 3.0 and later support these features.**
- **Only when the port property of LAN1/WAN is set to LAN port, the PoE setting will work.**

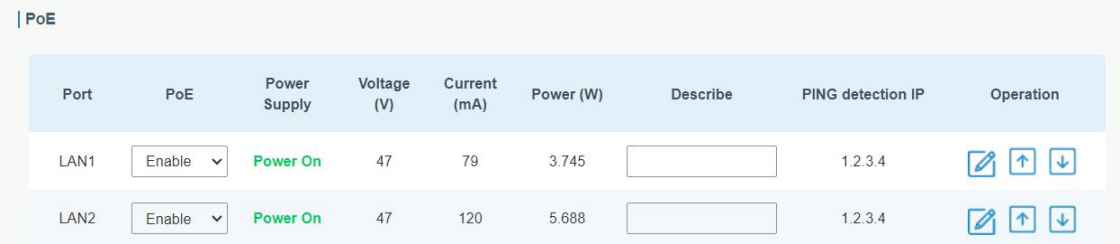


Figure 3-2-1-7

PoE Setting	
Item	**Description**
Port	Users can define the Ethernet ports according to their needs.
PoE	Enable or disable this Ethernet port to supply power.
Power Supply	Show the power supply status of this Ethernet port.
Voltage	Show the current output voltage of this Ethernet port.
Current	Show the current output current of this Ethernet port.
Power	Show the current output power of this Ethernet port.
Describe	Add the description of this Ethernet port.
Ping Detection IP	Show the IP address to send ICMP packet to detect the connection status.
Operation	You can change the power supply priority of the ports and configure the ping detection rules here.

Table 3-2-1-8 PoE Parameters

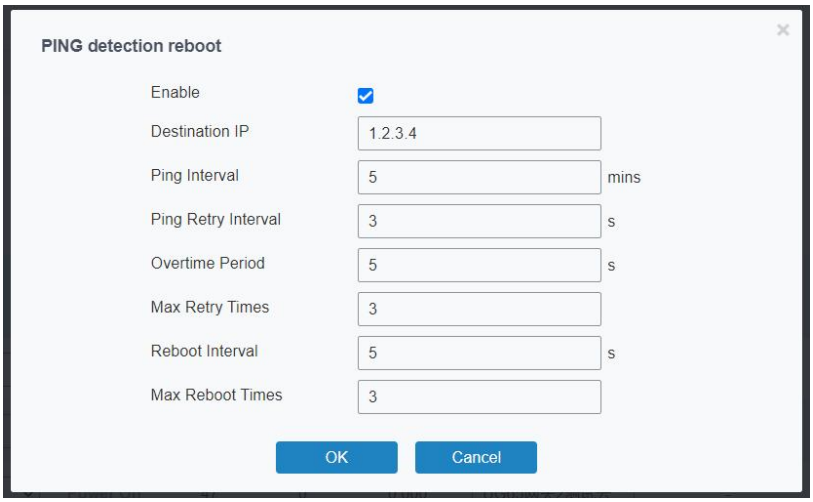


Figure 3-2-1-8

Ping Detection reboot	
Item	**Description**
Enable	If enabled, the router will periodically detect the connection status of the port. If detection fails, the router will reboot this port.
Destination IP	The router will send an ICMP packet to the IPv4 address to determine whether the connection is still available or not.
Interval	Time interval (in seconds) between two Pings.
Ping Retry Interval	Set the ping retry interval. When ping fails, the router will ping again in every retry interval.
Overtime Period	The maximum amount of time the router will wait for a response to a ping request. If it does not receive a response for the amount of time defined in this field, the ping request will be considered to have failed.
Max Ping Retries	The retry times of the router sending ping request until determining that the connection has failed.
Reboot Interval	The power-off interval of this Ethernet port.
Max Reboot Times	The retry times of the router rebooting this port. 0 means no limits.

Table 3-2-1-9 Ping Detection Parameters

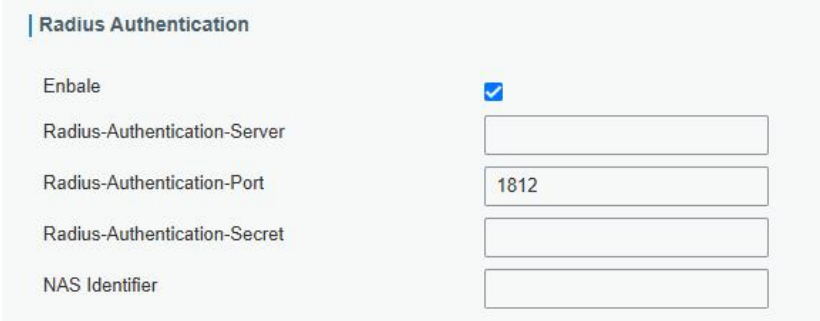


Figure 3-2-1-9

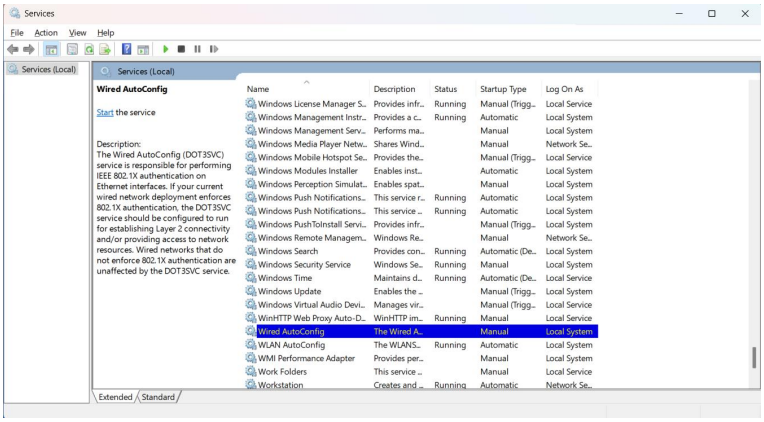
Radius Authentication	
Item	**Description**

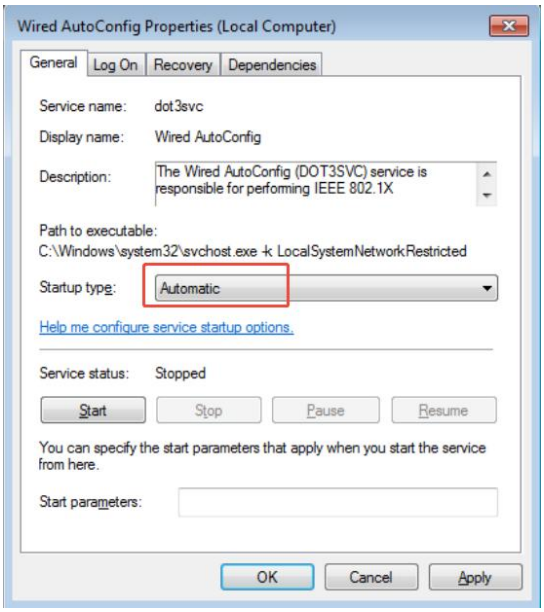
Enable	Enable or disable Radius authentication for the wired portion of the LAN port.
Radius-Authentication-Server	Enter the IP address of the Radius authentication server.
Radius-Authentication-Port	Enter the port of the Radius authentication server. Default: 1812
Radius-Authentication-Secret	Enter the shared secret for the Radius authentication server.
NAS Identifier	Unique identifier, used to identify the access device, can help the RADIUS server distinguish authentication requests from different access devices.

Table 3-2-1-10

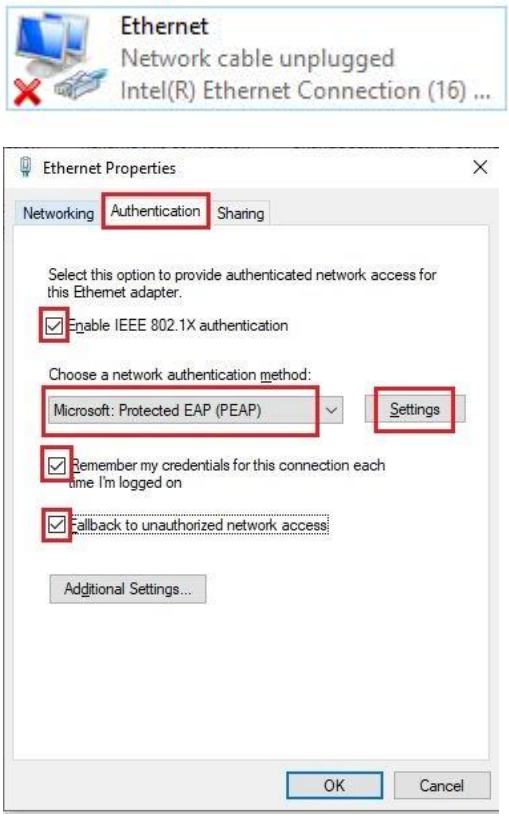
Note: Please refer to below steps to turn on the 802.1x authentication on a Windows computer

1. Enable the **Wired Autoconfig** and set it to start automatically.





2. Go to **Control Panel > Network and Internet > Network and Sharing Center** to select **Ethernet** connection to enable 802.1x authentication, and configure according to the authentication method provided by the authentication server.



3.2.1.4 WAN

The WAN port can be connected with an Ethernet cable to get Internet access.

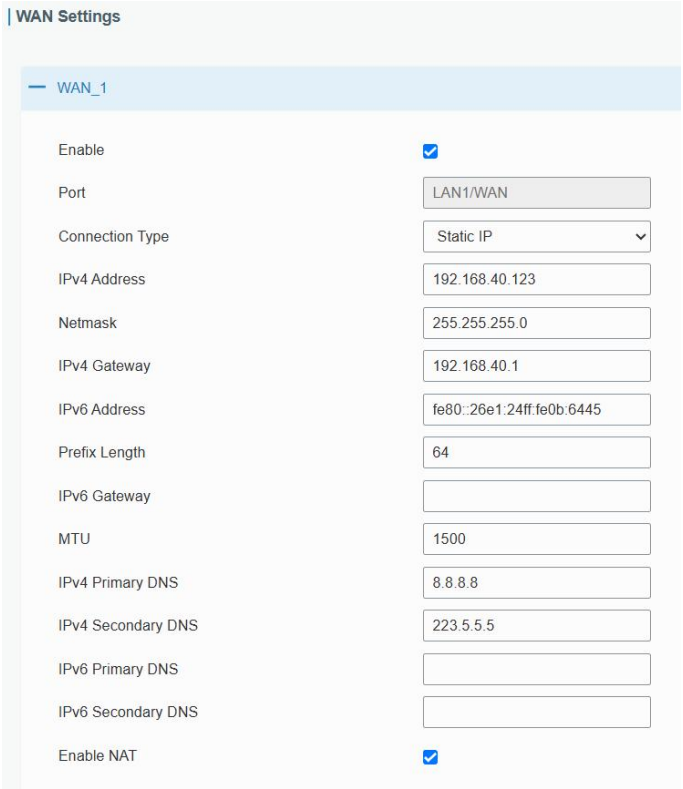


Figure 3-2-1-10

WAN Setting		
Item	**Description**	**Default**
Enable	Enable WAN function.	Enable
Port	The port that is currently set as a WAN port.	WAN
Connection Type	Select connection type as required. **Static IP**: assign a static IP address, netmask and gateway for Ethernet WAN interface. **DHCP Client**: configure Ethernet WAN interface as DHCP Client to obtain the IP address automatically. **PPPoE**: configure Ethernet WAN interface as PPPoE Client. -**DHCPv6 Client**: configure Ethernet WAN interface as DHCP Client to obtain IPv6 address automatically. **Dual-Stack Lite**: use IPv4-in-IPv6 tunneling to send terminal device's IPv4 packet through a tunnel on the IPv6 access network to the ISP.	Static IP
MTU	Set the maximum transmission unit.	1500
IPv4 Primary DNS	Set the primary IPv4 DNS server.	8.8.8.8
IPv4 Secondary DNS	Set the secondary IPv4 DNS server.	-- --
IPv6 Primary DNS	Set the primary IPv6 DNS server.	-- --
IPv6 Secondary DNS	Set the secondary IPv6 DNS server.	-- --
Enable NAT	Enable or disable NAT function. When enabled, a private IP can be translated to a public IP.	Enable

Table 3-2-1-11 WAN Parameters

1. Static IP Configuration

If the external network assigns a fixed IP for the WAN interface, select Static IP mode.

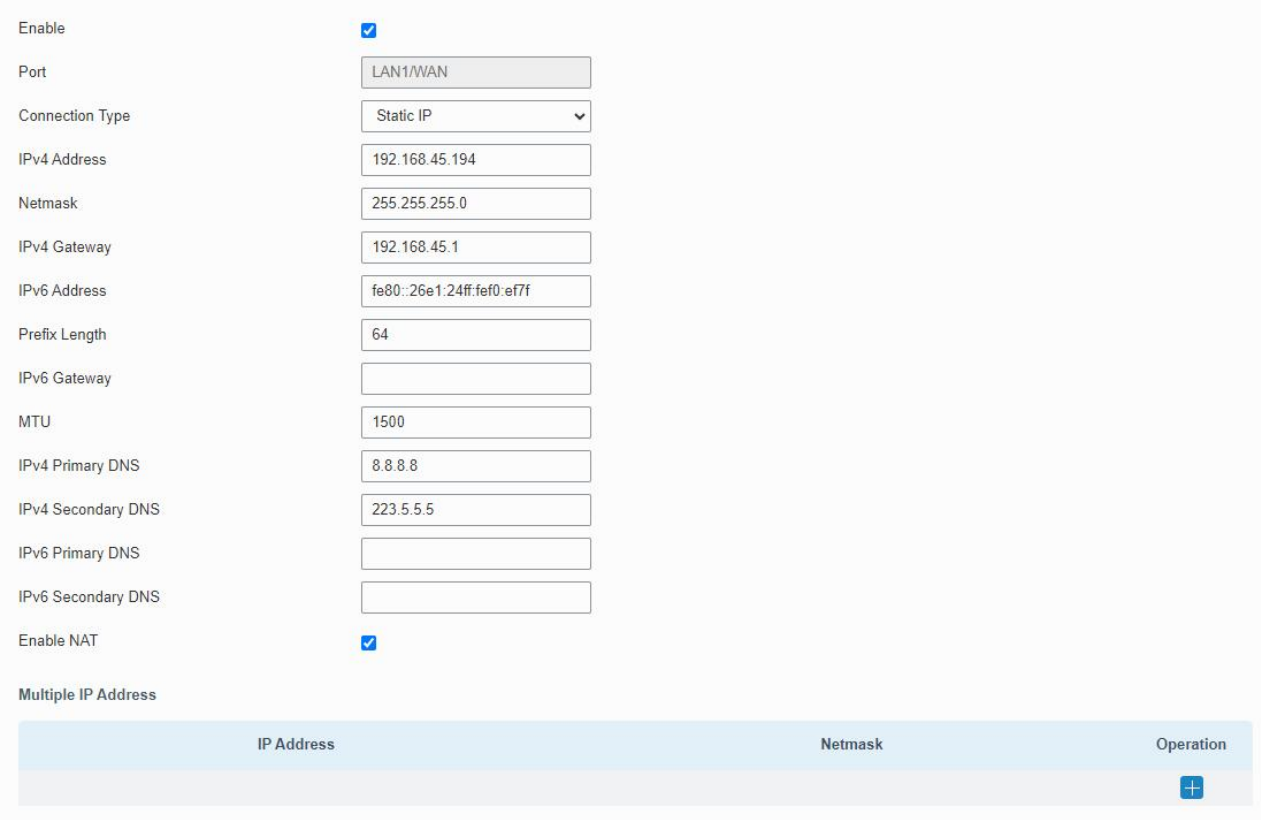


Figure 3-2-1-11

Static IP		
Item	**Description**	**Default**
IPv4 Address	Set the IPv4 address of the WAN port.	192.168.0.1
Netmask	Set the Netmask for WAN port.	255.255.255.0
IPv4 Gateway	Set the gateway for WAN port's IPv4 address.	192.168.0.2
IPv6 Address	Set the IPv6 address which can access Internet.	Generated from Mac address
Prefix-length	Set the IPv6 prefix length to identify how many bits of a Global Unicast IPv6 address are there in network part. For example, in 2001:0DB8:0000:000b::/64, the number 64 is used to identify that the first 64 bits are in network part.	64
IPv6 Gateway	Set the gateway for WAN port's IPv6 address. E.g.2001:DB8:ACAD:4::2.	--
Multiple IP Address	Set the multiple IP addresses for WAN port.	Null

Table 3-2-1-12 Static Parameters

2. DHCP Client/DHCPv6 Client

If the external network has DHCP server enabled and has assigned IP addresses to the Ethernet WAN interface, select DHCP/DHCPv6 client mode to obtain IP address automatically.

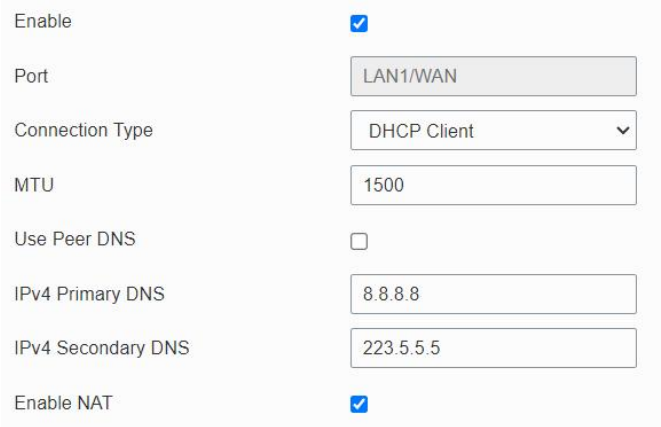


Figure 3-2-1-12

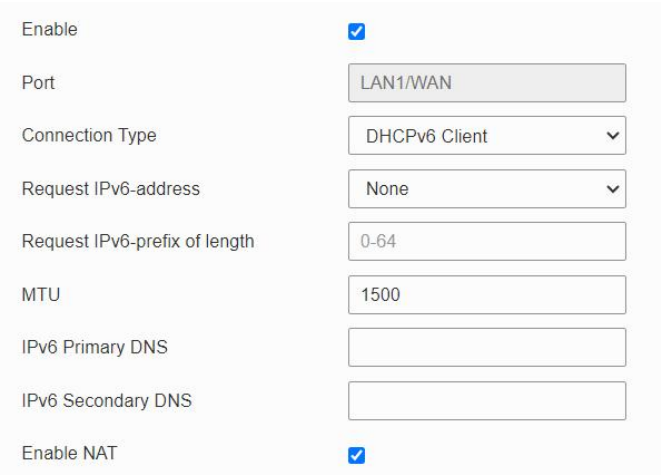


Figure 3-2-1-13

DHCP Client	
Item	**Description**
Use Peer DNS	Obtain peer DNS automatically during PPP dialing. DNS is necessary when visiting domain name.
DHCPv6 Client	
Request IPv6-address	Choose the ways to obtain the IPv6 address from the DHCP Server. Select from try, force, none. Try: The DHCP Server will assign specific address in priority. Force: The DHCP Server assigns specific address only. None: The DHCP Server will randomly assign address.The specific address is relevant to the prefix length of IPv6 address you set.
Request prefix length of IPv6	Set the prefix length of IPv6 address which router is expected to obtain from DHCP Server.

Table 3-2-1-13 DHCP Client Parameters

3. PPPoE

PPPoE refers to a point to point protocol over Ethernet. User has to install a PPPoE client on the basis

of the original connection way. With PPPoE, remote access devices can get control of each user.

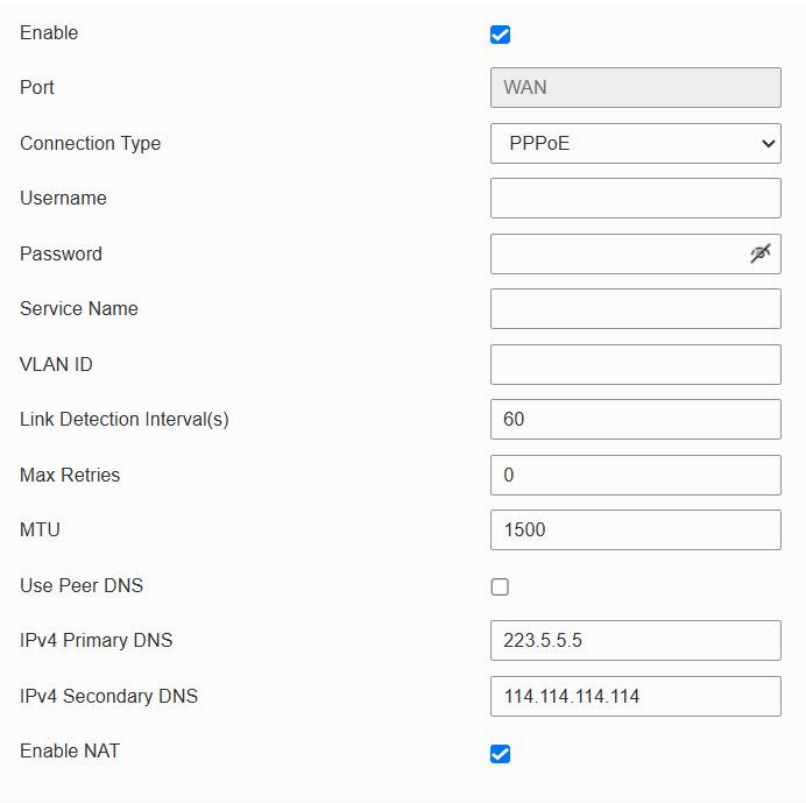


Figure 3-2-1-14

PPPoE	
Item	**Description**
Username	Enter the username provided by your Internet Service Provider (ISP).
Password	Enter the password provided by your Internet Service Provider (ISP).
Service Name	Configure the service name that the client will request.
VLAN ID	Configure the VLAN ID to identify and isolate network traffic for different services.
Link Detection Interval (s)	Set the heartbeat interval for link detection. Range: 1-600.
Max Retries	Set the maximum retry times after it fails to dial up. Range: 0-9.
Use Peer DNS	Obtain peer DNS automatically during PPP dialing. DNS is required when accessing domain names.

Table 3-2-1-14 PPPoE Parameters

4. Dual-Stack Lite

Dual-Stack Lite (DS-Lite) uses IPv4-in-IPv6 tunneling to send a subscriber's IPv4 packet through a tunnel on the IPv6 access network to the ISP. The IPv6 packet is decapsulated to recover the subscriber's IPv4 packet and is then sent to the Internet after NAT address and port translation and other LSN-related processing. The response packets traverse through the same path to the

subscriber.

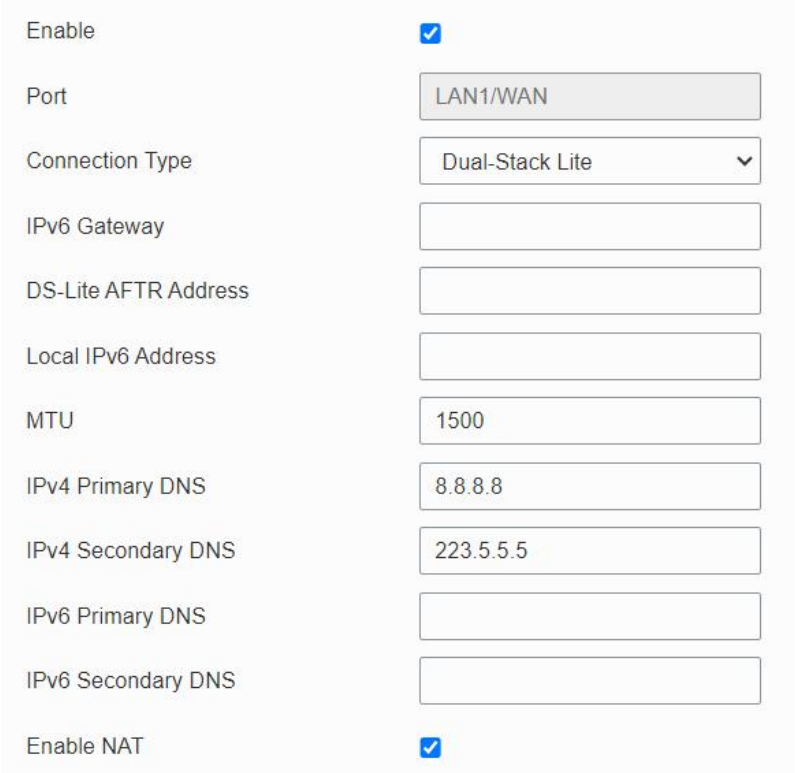


Figure 3-2-1-15

Dual-Stack Lite	
Item	**Description**
IPv6 Gateway	Set the gateway for WAN port's IPv6 address.
DS-Lite AFTR Address	Set the DS-Lite AFTR server address.
Local IPv6 Address	Set the WAN port IPv6 address which use the same subnet as IPv6 gateway.

Table 3-2-1-15 Dual-Stack Lite Parameters

Related Configuration Example

Ethernet WAN Connection

3.2.1.5 Bridge

Bridge setting is used for managing local area network devices which are connected to LAN ports of the UR32, allowing each of them to access the Internet.

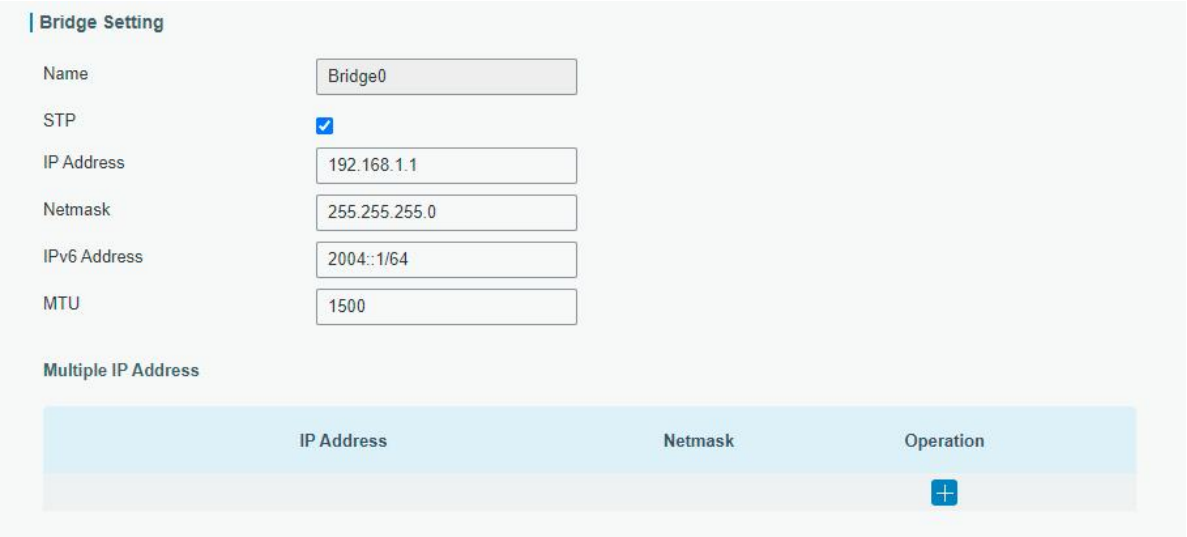


Figure 3-2-1-16

Bridge		
Item	**Description**	**Default**
Name	Show the name of bridge. "Bridge0" is set by default and cannot be changed.	Bridge0
STP	Enable/disable STP.	Disable
IP Address	Set the IP address for bridge.	192.168.1.1
Netmask	Set the Netmask for bridge.	255.255.255.0
IPv6 Address	Set the IPv6 address for bridge.	2004::1/64
MTU	Set the maximum transmission unit. Range: 68-1500.	1500
Multiple IP Address	Set the multiple IP addresses for bridge.	Null

Table 3-2-1-16 Bridge Settings

3.2.1.6 WLAN (Only Applicable to Wi-Fi Version)

This section explains how to set the related parameters for Wi-Fi network. UR32 supports 802.11 b/g/n, as AP or client mode.

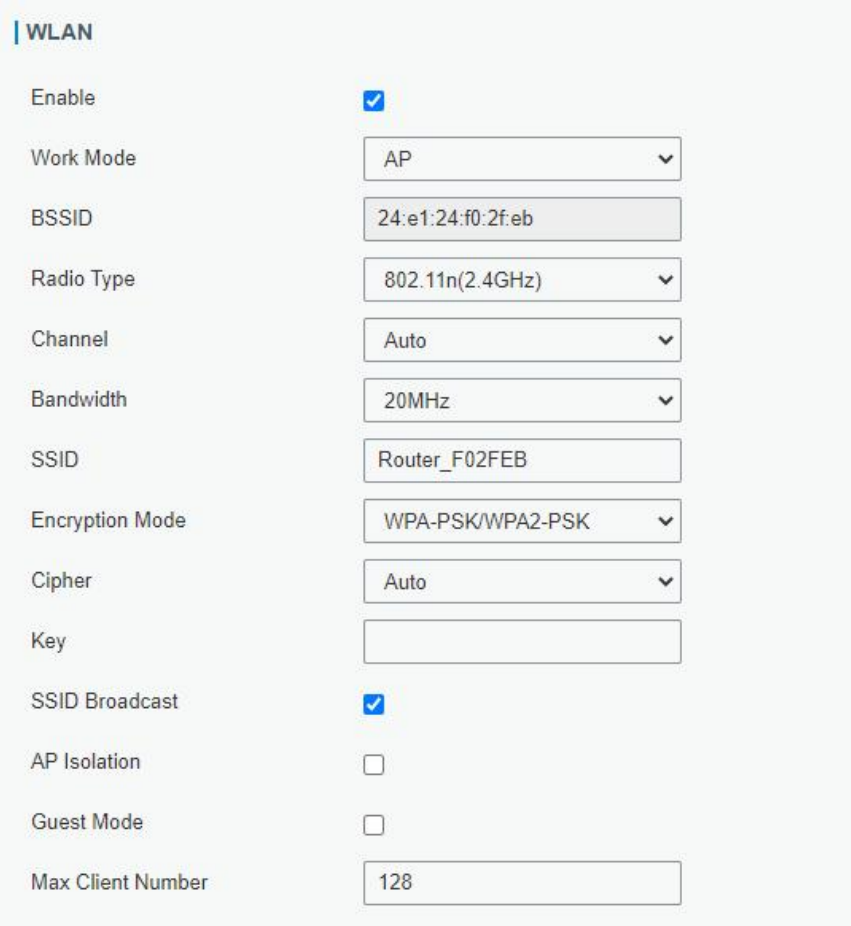


Figure 3-2-1-17

WLAN	
Item	**Description**
Enable	Enable/disable WLAN.
Work Mode	Select router's work mode. The options are "Client" or "AP".
AP Mode	
BSSID	Show the MAC address of this WLAN interface.
Radio Type	Select Radio type. The options are “802.11b (2.4 GHz)", “802.11g (2.4 GHz)", “802.11n (2.4 GHz)”.
Channel	Select wireless channel. The options are "Auto", "1", "2"....."11".
Bandwidth	Select bandwidth. The options are "20MHz" and "40MHz".
SSID	Fill in the SSID of the access point.
Encryption Mode	Select encryption mode. The options are “No Encryption", “WEP Open System", “WEP Shared Key", “WPA-PSK", “WPA2-PSK", “WPA-PSK/WPA2-PSK", “WPA-EAP” and “WPA2-EAP”..
Cipher	Select cipher of WPA encryption. The options are “Auto", “AES", “TKIP" and “AES/TKIP".
Key	Fill the key to connect to this access point. The default key is **iotpassword**.
Radius-Authentication-Server	Enter the IP address of the Radius authentication server.

Radius-Authentication-Port	Enter the Radius authentication server port number.
Radius-Authentication-Secret	Enter the shared key for the Radius Authentication Server.
Radius-Accounting-Server	Enter the IP address of the Radius accounting server.
Radius-Accounting-Port	Enter the port number of the Radius accounting server.
Radius-Accounting-Secret	Enter the shared key for the Radius accounting server.
NAS Identifier	Unique identifier, used to identify the access device, can help the RADIUS server distinguish authentication requests from different access devices.
SSID Broadcast	When SSID broadcast is disabled, other wireless devices can't not find the SSID, and users have to enter the SSID manually to access to the wireless network.
AP Isolation	When AP isolation is enabled, all users who access to the AP are isolated without communication with each other.
Guest Mode	The internal network is not allowed to visit if the guest mode is enabled.
Max Client Number	Set the maximum number of clients to access when the router is configured as AP.
MAC Filtering	
Type	Choose the filter type of devices connected to this router's wireless access point. **Disable:** allow all users to connect to this access point. **Allow and Block the Rest:** Only the listed MAC addresses are allowed to connect to the router's wireless access point. **Block and allow the rest:** The listed MAC addresses are not allowed to connect to the router's wireless access point.
MAC Address	The device MAC addresses which need to block or allow.
Description	The description of this MAC address.
Client Mode	
Scan	Click to scan the access points around this device.
SSID	Fill in the SSID of the access point.
BSSID	Fill in the MAC address of the access point. Either SSID or BSSID can be filled to join the network.
Encryption Mode	Select encryption mode. The options are "No Encryption", "WEP Open System", "WEP Shared Key", "WPA-PSK", "WPA2-PSK", "WPA-PSK/WPA2-PSK", "WPA-Enterprise", "WPA2-Enterprise" and "WPA-Enterprise/WPA2-Enterprise".
Cipher	Select cipher of WPA encryption. The options are "Auto", "AES", "TKIP" and "AES/TKIP".
Key	Fill the key to connect to this access point.
Xsupplicant Type	Select from "Peap", "Leap", "TLS" and "TTLS".

Username	Fill the username of WPA/WPA2-Enterprise.
Password	Fill the password of WPA/WPA2-Enterprise.
Anonymous Identity	Fill the anonymous identity of WPA/WPA2-Enterprise.
Phase 1/2	Fill the phase of WPA/WPA2-Enterprise.
CA Certificate	The public server certificate used for verifying with WPA/WPA2-Enterprise access point.
Public Key	When Xsupplicant type is "TLS", import the public key used for verifying with WPA/WPA2-Enterprise access point.
Private Key	When Xsupplicant type is "TLS", import the private key used for verifying with WPA/WPA2-Enterprise access point.
Private Key Decryption	Set the decryption password of private key.
IP Setting	
Protocol	Set the protocol to get the WLAN IP address.
IP Address	Set the IP address in wireless network when protocol is Static IP.
Netmask	Set the netmask in wireless network when protocol is Static IP.
Gateway	Set the gateway in wireless network when protocol is Static IP.

Table 3-2-1-17 WLAN Parameters

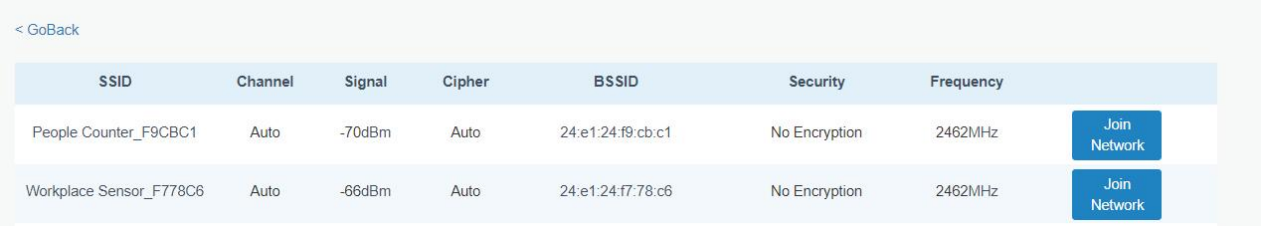


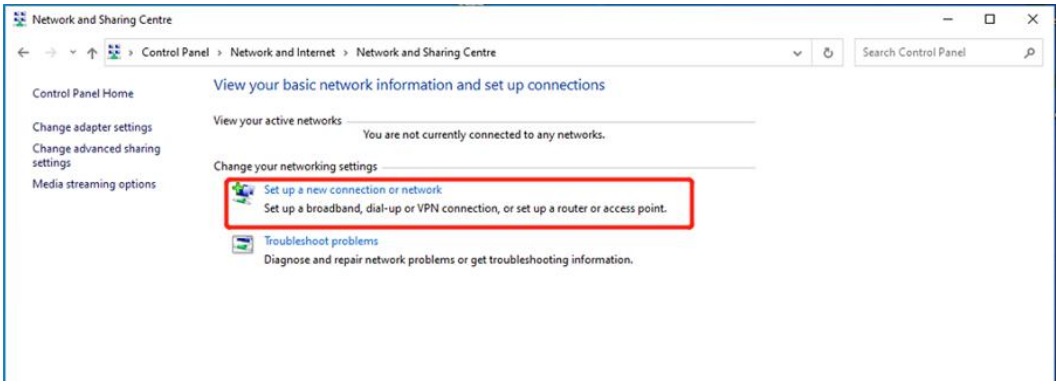
Figure 3-2-1-18

WLAN-Scan	
Item	**Description**
SSID	Show SSID.
Channel	Show wireless channel.
Signal	Show wireless signal.
BSSID	Show the MAC address of the access point.
Cipher	Show the cipher of the access point.
Security	Show the encryption mode.
Frequency	Show the frequency of radio.
Join Network	Click the button to join the wireless network.

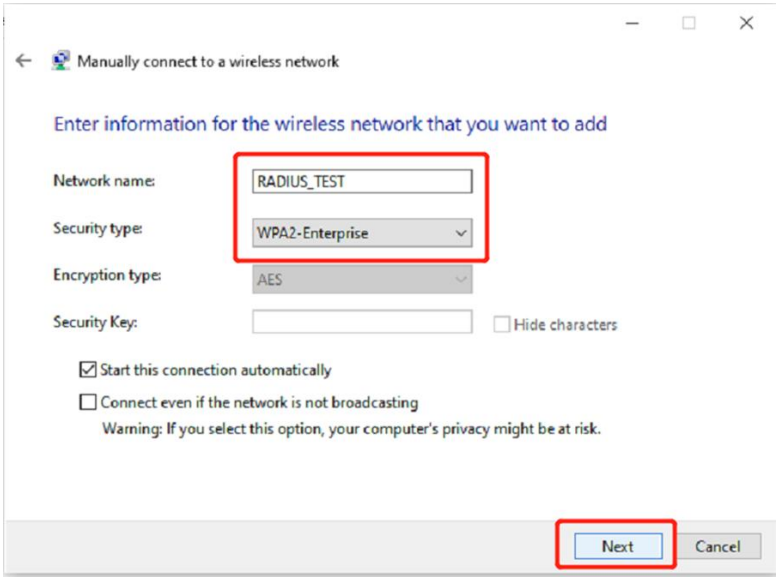
Table 3-2-1-18 WLAN-Scan Parameters

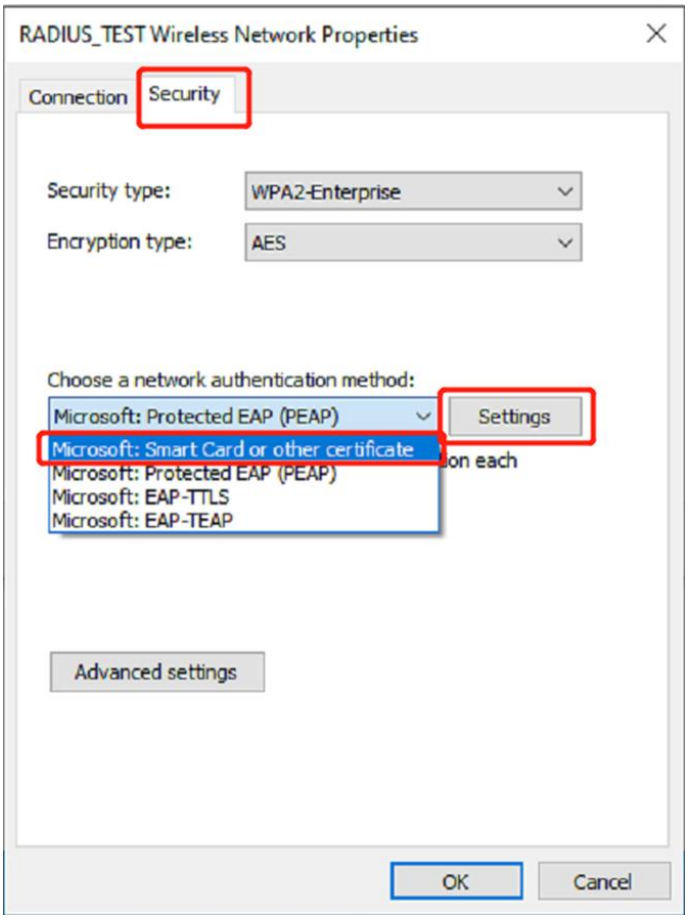
Note: Please refer to below steps to turn on the 802.1x authentication on a Windows computer:

1. Set up a wireless network.

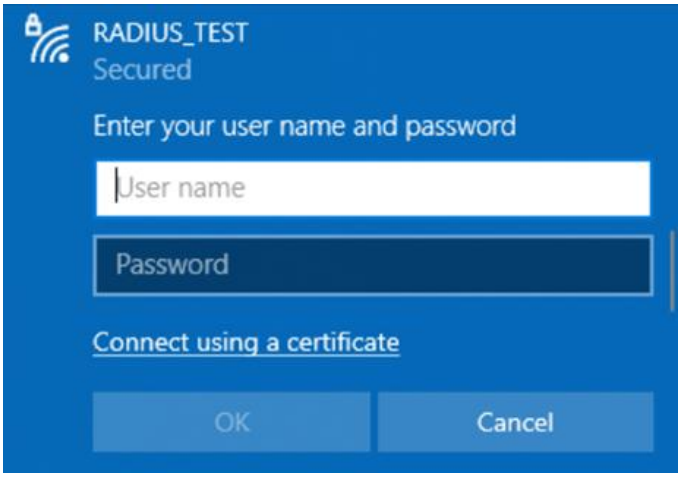


2. Manually add the wireless network and select the security type. Choose a network authentication method in **Security** by the authentication server.





3. Connect to Wi-Fi.



Related Topic

Wi-Fi Application Example

3.2.1.7 Switch

VLAN is a kind of new data exchange technology that realizes virtual work groups by logically dividing

the LAN device into network segments.

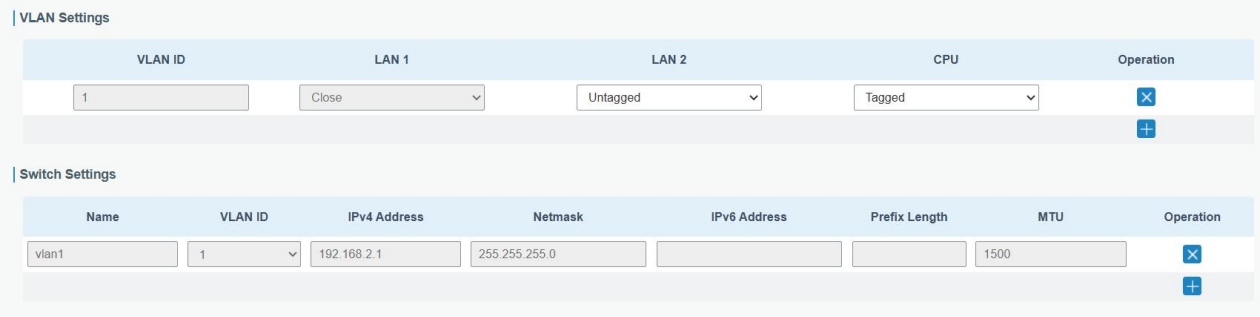


Figure 3-2-1-19

Switch	
Item	**Description**
VLAN Settings	
VLAN ID	Set the label ID of the VLAN. Range: 1-4094.
LAN 1/2	Make the VLAN bind with the corresponding ports and select status from "Tagged", "Untagged" and "Close" for Ethernet frame on trunk link.
CPU	Control communication between VLAN and other networks.
Switch Settings	
Name	Set interface name of VLAN.
VLAN ID	Select VLAN ID of the interface.
IPv4 Address	Set IPv4 address of LAN port.
Netmask	Set Netmask of LAN port.
IPv6 Address	Set IPv6 address of LAN port.
Prefix Length	Set the IPv6 prefix length of VLAN.
MTU	Set the maximum transmission unit of LAN port. Range: 68-1500.

Table 3-2-1-19 VLAN Trunk Parameters

3.2.1.8 Loopback

Loopback interface is used for replacing router's ID as long as it is activated. When the interface is DOWN, the ID of the router has to be selected again which leads to long convergence time of OSPF. Therefore, Loopback interface is generally recommended as the ID of the router.

Loopback interface is a logic and virtual interface on router. Under default conditions, there's no loopback interface on router, but it can be created as required.

Figure 3-2-1-20

Loopback		
Item	**Description**	**Default**
IP Address	Unalterable	127.0.0.1
Netmask	Unalterable	255.0.0.0
Multiple IP Addresses	Apart from the IP above, user can configure other IP addresses.	Null

Table 3-2-1-20 Loopback Parameters

3.2.2 DHCP

DHCP adopts Client/Server communication mode. The Client sends configuration request to the Server which feeds back corresponding configuration information and distributes IP address to the Client so as to achieve the dynamic configuration of IP address and other information.

3.2.2.1 DHCP Server/DHCPv6 Server

UR32 can be set as a DHCP server or DHCPv6 server to distribute IP address when a host logs on and ensures each host is supplied with different IP addresses. DHCP Server has simplified some previous network management tasks requiring manual operations to the largest extent. UR32 only supports stateful DHCPv6 when working as DHCPv6 server.

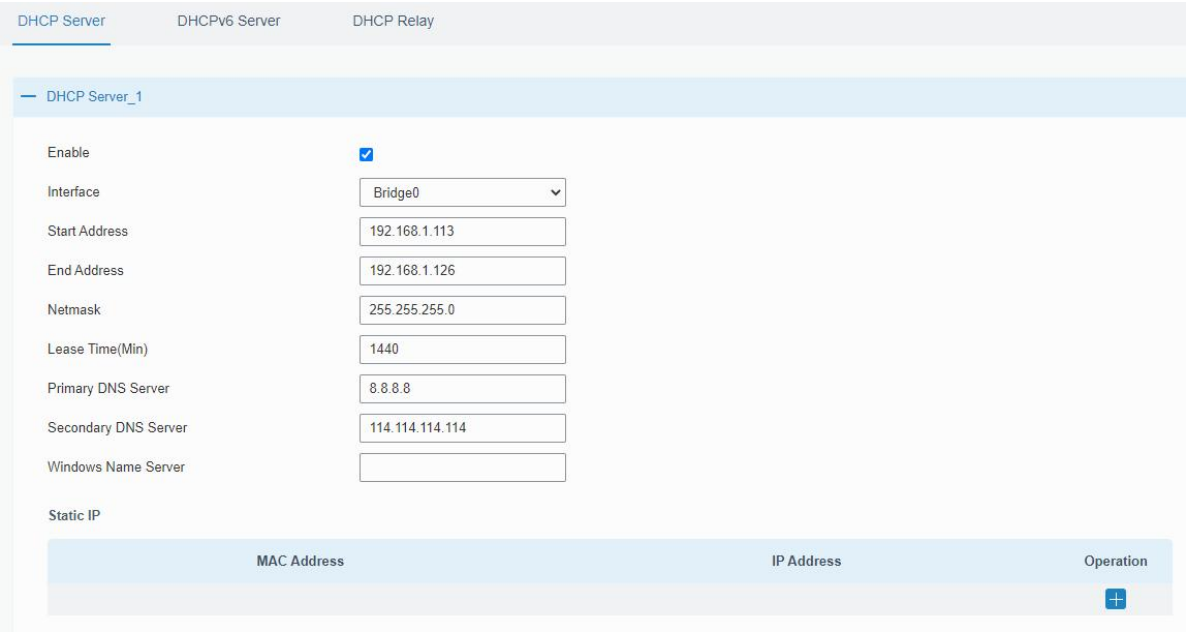


Figure 3-2-2-1

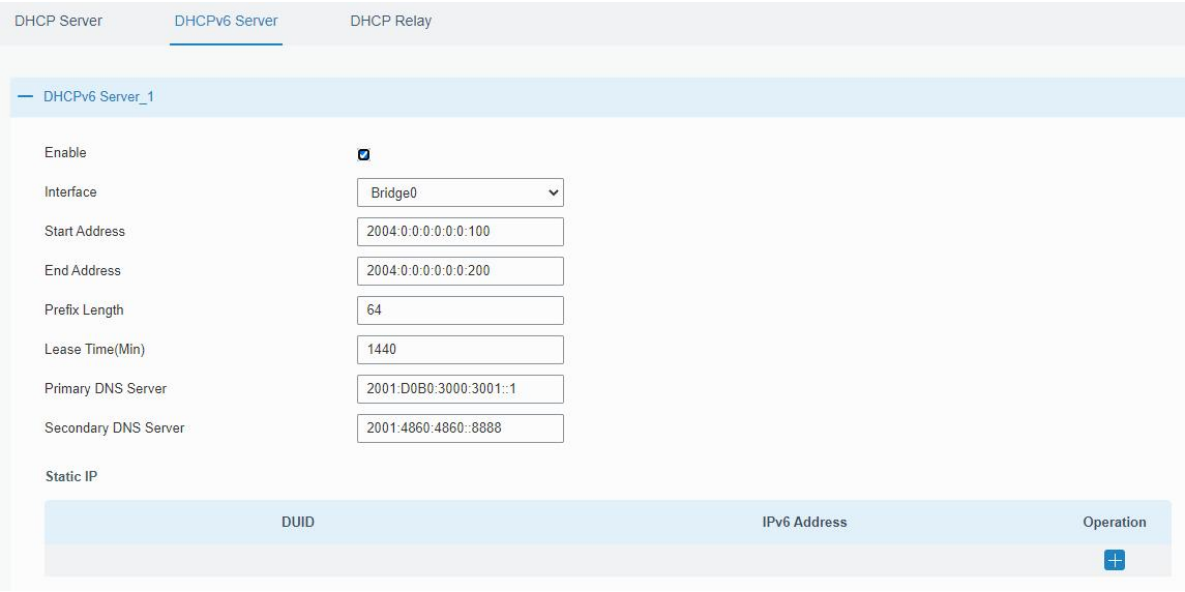


Figure 3-2-2-2

DHCP/DHCPv6 Server		
Item	**Description**	**Default**
Enable	Enable or disable DHCP server.	Enable
Interface	Select interface.	Bridge0
Start Address	Define the beginning of the pool of IP addresses which will be leased to DHCP clients.	192.168.1.00
End Address	Define the end of the pool of IP addresses which will be leased to DHCP clients.	192.168.1.99
Netmask	Define the subnet mask of IPv4 address obtained by DHCP clients from DHCP server.	255.255.255.0
Prefix Length	Set the IPv6 prefix length of IPv6 address obtained by DHCP clients from DHCP server.	64
Lease Time (Min)	Set the lease time on which the client can use the IP address obtained from DHCP server. Range: 1-10080.	1440
Primary DNS Server	Set the primary DNS server.	192.168.1.1
Secondary DNS Server	Set the secondary DNS server.	Null
Windows Name Server	Define the Windows Internet Naming Service obtained by DHCP clients from DHCP sever. Generally you can leave it blank.	Null
Static IP		
MAC Address	Set a static and specific MAC address for the DHCP client (it should be different from other MACs so as to avoid conflict).	Null
DUID	Set a static and specific DUID for the DHCPv6 client (it should be different from other DUID so as to avoid conflict).	Null
IP Address	Set a static and specific IP address for the DHCP client (it	Null

	should be outside of the DHCP range).	

Table 3-2-2-1 DHCP Server Parameters

3.2.2.2 DHCP Relay

UR32 can be set as DHCP Relay to provide a relay tunnel to solve the problem that DHCP Client and DHCP Server are not in the same subnet.

Figure 3-2-2-3

DHCP Relay	
Item	**Description**
Enable	Enable or disable DHCP relay.
DHCP Server	Set DHCP server, up to 10 servers can be configured; separate them by blank space or ",".

Table 3-2-2-2 DHCP Relay Parameters

3.2.3 Firewall

This section describes how to set the firewall parameters, including security, ACL, DMZ, Port Mapping, MAC Binding and SPI.

The firewall implements corresponding control of data flow at entry direction (from Internet to local area network) and exit direction (from local area network to Internet) according to the content features of packets, such as protocol style, source/destination IP address, etc. It ensures that the router operate in a safe environment and host in local area network.

3.2.3.1 Security

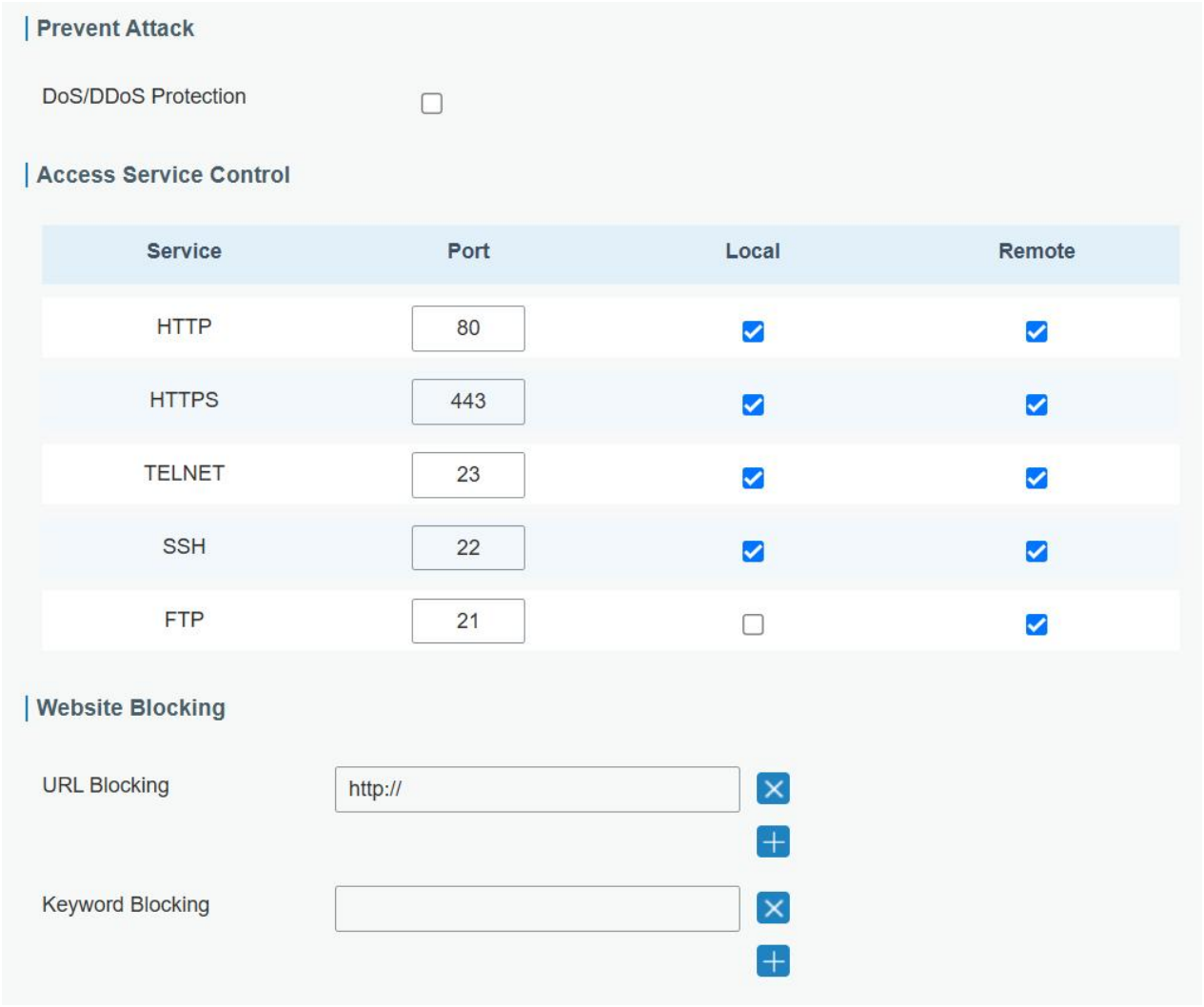


Figure 3-2-3-1

Item	Description	Default
Prevent Attack		
DoS/DDoS Protection	Enable/disable Prevent DoS/DDoS Attack.	Disable
Access Service Control		
Port	Set port number of the services. Range: 1-65535.	--
Local	Access the router locally.	Enable
Remote	Access the router remotely.	Disable
HTTP	Users can log in the device locally via HTTP to access and control it through Web after the option is checked.	80
HTTPS	Users can log in the device locally and remotely via HTTPS to access and control it through Web after option is checked.	443
TELNET	Users can log in the device locally and remotely via Telnet after the option is checked.	23
SSH	Users can log in the device locally and remotely	22

	via SSH after the option is checked.	
FTP	Users can log in the device locally and remotely via FTP after the option is checked.	21
Website Blocking		
URL Blocking	Enter the HTTP address which you want to block.	
Keyword Blocking	You can block specific website by entering keyword. The maximum number of character allowed is 64.	

Table 3-2-3-1 Security Parameters

3.2.3.2 ACL

Access control list, also called ACL, implements permission or prohibition of access for specified network traffic (such as the source IP address) by configuring a series of matching rules so as to filter the network interface traffic. When router receives packet, the field will be analyzed according to the ACL rule applied to the current interface. After the special packet is identified, the permission or prohibition of corresponding packet will be implemented according to preset strategy.

The data package matching rules defined by ACL can also be used by other functions requiring flow distinction.

Figure 3-2-3-2

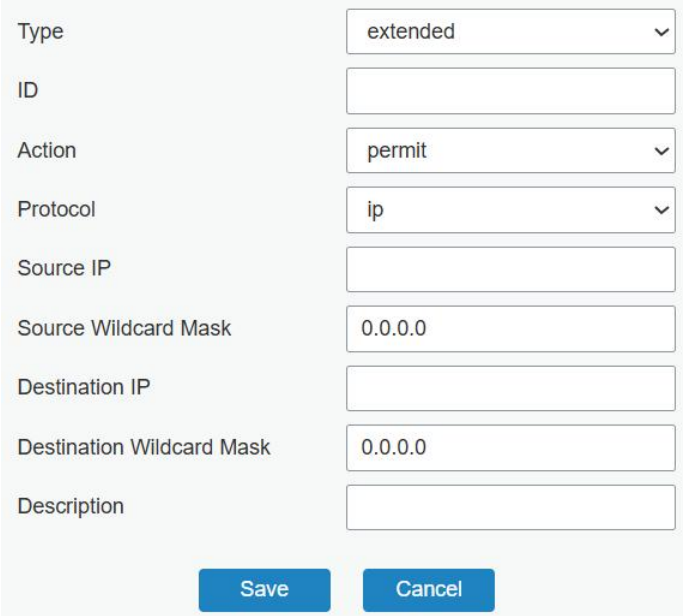


Figure 3-2-3-3

Item	Description
ACL Setting	
Default Filter Policy	Select from "Accept" and "Deny". The packets which are not included in the access control list will be processed by the default filter policy.
Access Control List	
Type	Select type from "Extended" and "Standard".
ID	User-defined ACL number. Range: 1-199.
Action	Select from "Permit" and "Deny".
Protocol	Select protocol from "ip", "icmp", "tcp", "udp", and "1-255".
Source IP	Source network address (leaving it blank means all).
Source Wildcard Mask	Wildcard mask of the source network address.
Destination IP	Destination network address (0.0.0.0 means all).
Destination Wildcard Mask	Wildcard mask of destination address.
Description	Fill in a description for the groups with the same ID.
ICMP Type	Enter the type of ICMP packet. Range: 0-255.
ICMP Code	Enter the code of ICMP packet. Range: 0-255.
Source Port Type	Select source port type, such as specified port, port range, etc.
Source Port	Set source port number. Range: 1-65535.
Start Source Port	Set start source port number. Range: 1-65535.
End Source Port	Set end source port number. Range: 1-65535.
Destination Port Type	Select destination port type, such as specified port, port range, etc.
Destination Port	Set destination port number. Range: 1-65535.
Start Destination Port	Set start destination port number. Range: 1-65535.
End Destination Port	Set end destination port number. Range: 1-65535.
More Details	Show information of the port.
Interface List	
Interface	Select network interface for access control.
In ACL	Select a rule for incoming traffic from ACL ID.
Out ACL	Select a rule for outgoing traffic from ACL ID.

Table 3-2-3-2 ACL Parameters

3.2.3.3 Port Mapping (DNAT)

When external services are needed internally (for example, when a website is published externally), the external address initiates an active connection. And, the router or the gateway on the firewall receives the connection. Then it will convert the connection into the an internal connection. This conversion is called DNAT, which is mainly used for external and internal services.

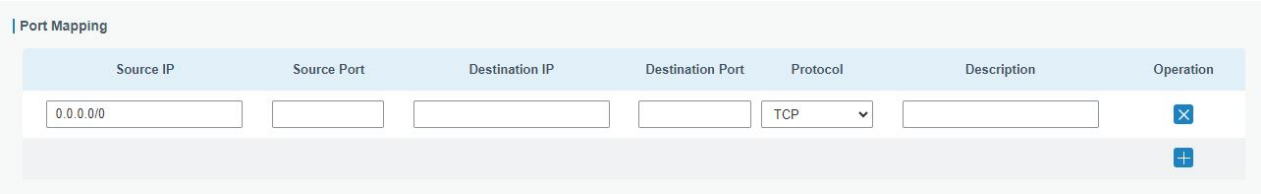


Figure 3-2-3-3

Port Mapping	
Item	**Description**
Source IP	Specify the host or network which can access local IP address. 0.0.0.0/0 means all.
Source Port	Enter the TCP or UDP port from which incoming packets are forwarded. Range: 1-65535.
Destination IP	Enter the IP address that packets are forwarded to after being received on the incoming interface.
Destination Port	Enter the TCP or UDP port that packets are forwarded to after being received on the incoming port(s). Range: 1-65535.
Protocol	Select from "TCP" and "UDP" as your application required.
Description	The description of this rule.

Table 3-2-3-3 Port Mapping Parameters

Related Configuration Example

NAT Application Example

3.2.3.4 DMZ

DMZ is a host within the internal network that has all ports exposed, except those forwarded ports in port mapping.

Figure 3-2-3-4

DMZ	
Item	**Description**
Enable	Enable or disable DMZ.
DMZ Host	Enter the IP address of the DMZ host on the internal network.
Source Address	Set the source IP address which can access to DMZ host. "0.0.0.0/0" means any address.

Table 3-2-3-4 DMZ Parameters

3.2.3.5 MAC Binding

MAC Binding is used for specifying hosts by matching MAC addresses and IP addresses that are in the list of allowed outer network access.

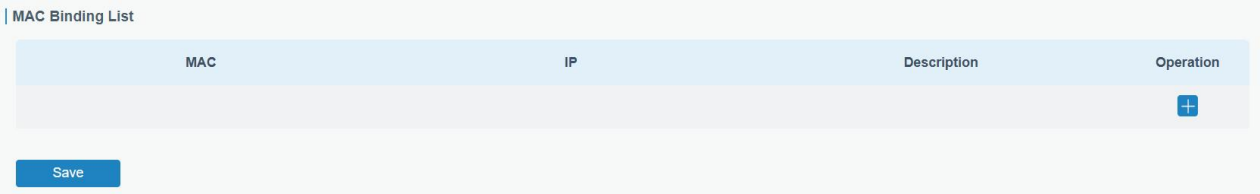


Figure 3-2-3-5

MAC Binding List	
Item	**Description**
MAC Address	Set the binding MAC address.
IP Address	Set the binding IP address.
Description	Fill in a description for convenience of recording the meaning of the binding rule for each piece of MAC-IP.

Table 3-2-3-5 MAC Binding Parameters

3.2.3.6 Custom Rules

In this page, you can configure your own custom firewall iptables rules.

Figure 3-2-3-6

Custom Rules	
Item	**Description**
Rule	Specify an iptables rule like the example shows. Tips: You must reboot the device to take effect after modifying or deleting the iptables rules.
Description	Enter the description of the rule.

Table 3-2-3-6 Custom Rules Parameters

3.2.3.7 SPI

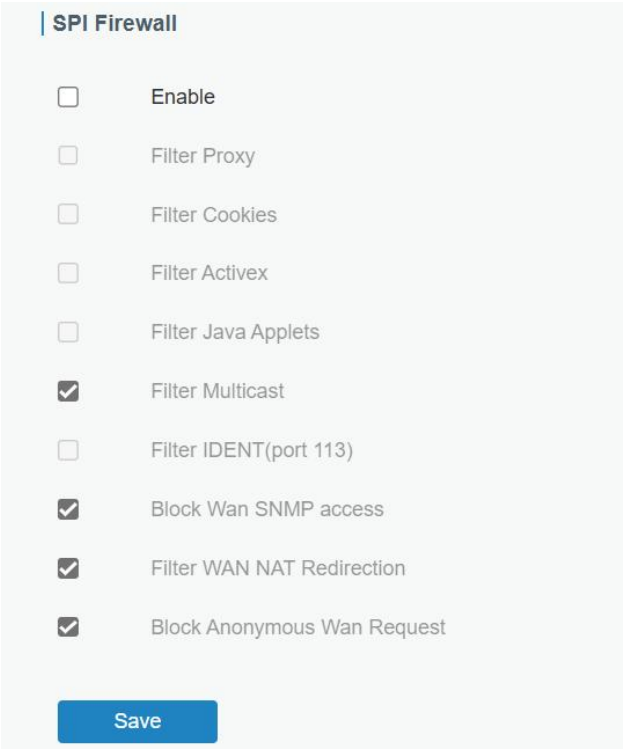


Figure 3-2-3-7

SPI Firewall	
Item	**Description**
Enable	Enable/disable SPI firewall.
Filter Proxy	Blocks HTTP requests containing the "Host": string.
Filter Cookies	Identifies HTTP requests that contain "Cookie": String and mangle the cookie. Attempts to stop cookies from being used.
Filter ActiveX	Blocks HTTP requests of the URL that ends in ".ocx" or ".cab".
Filter Java Applets	Blocks HTTP requests of the URL that ends in ".js" or ".class".
Filter Multicast	Prevent multicast packets from reaching the LAN.
Filter IDENT(port 113)	Prevent WAN access to Port 113.
Block WAN SNMP access	Block SNMP requests from the WAN.
Filter WAN NAT Redirection	Prevent hosts on LAN from using WAN address of router to connect servers on the LAN (which have been configured using port redirection).
Block Anonymous WAN Requests	Stop the router from responding to "pings" from the WAN.

Table 3-2-3-7 SPI Parameters

3.2.4 QoS

Quality of service (QoS) refers to traffic prioritization and resource reservation control mechanisms rather than the achieved service quality. QoS is engineered to provide different priority for different applications, users, data flows, or to guarantee a certain level of performance to a data flow.

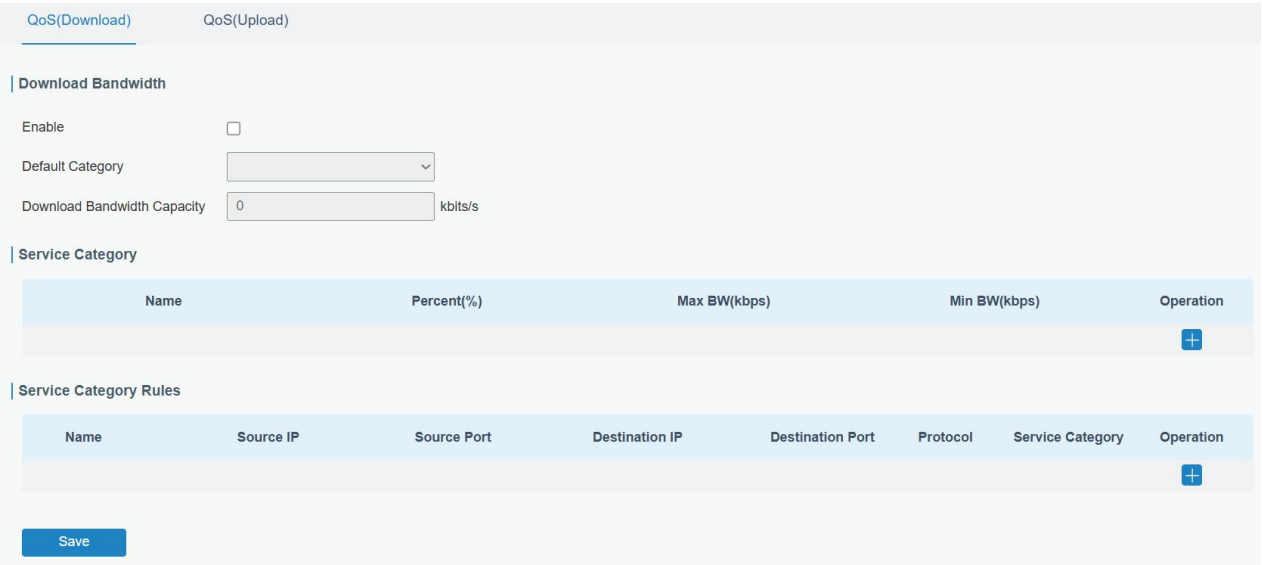


Figure 3-2-4-1

QoS	
Item	**Description**
Download/Upload	
Enable	Enable or disable QoS.
Default Category	Select the default category from Service Category list.
Download/Upload Bandwidth Capacity	The download/upload bandwidth capacity of the network that the router is connected with, in kbps. Range: 1-8000000.
Service Category	
Name	You can use characters such digits, letters and "-".
Percent (%)	Set percent for the service category. Range: 0-100.
Max BW(kbps)	The maximum bandwidth that this category is allowed to consume, in kbps. The value should be less than the "Download/Upload Bandwidth Capacity" when the traffic is blocked.
Min BW(kbps)	The minimum bandwidth that can be guaranteed for the category, in kbps.The value should be less than the "MAX BW" value.
Service Category Rules	
Item	**Description**
Name	Give the rule a descriptive name.
Source IP	Source address of flow control (leaving it blank means any).
Source Port	Source port of flow control. Range: 0-65535 (leaving it blank means any).
Destination IP	Destination address of flow control (leaving it blank means any).
Destination Port	Destination port of flow control. Range: 0-65535 (leaving it blank means any).
Protocol	Select protocol from "ANY", "TCP", "UDP", "ICMP", and "GRE".

Service Category	Set service category for the rule.

Table 3-2-4-1 QoS (Download/Upload) Parameters

Related Configuration Example

QoS Application Example

3.2.5 VPN

Virtual Private Networks, also called VPNs, are used to securely connect two private networks together so that devices can connect from one network to the other network via secure channels.
The UR32 supports DMVPN, IPsec, GRE, L2TP, PPTP, OpenVPN, as well as GRE over IPsec and L2TP over IPsec.

3.2.5.1 DMVPN

A dynamic multi-point virtual private network (DMVPN), combining mGRE and IPsec, is a secure network that exchanges data between sites without passing traffic through an organization's headquarter VPN server or router.

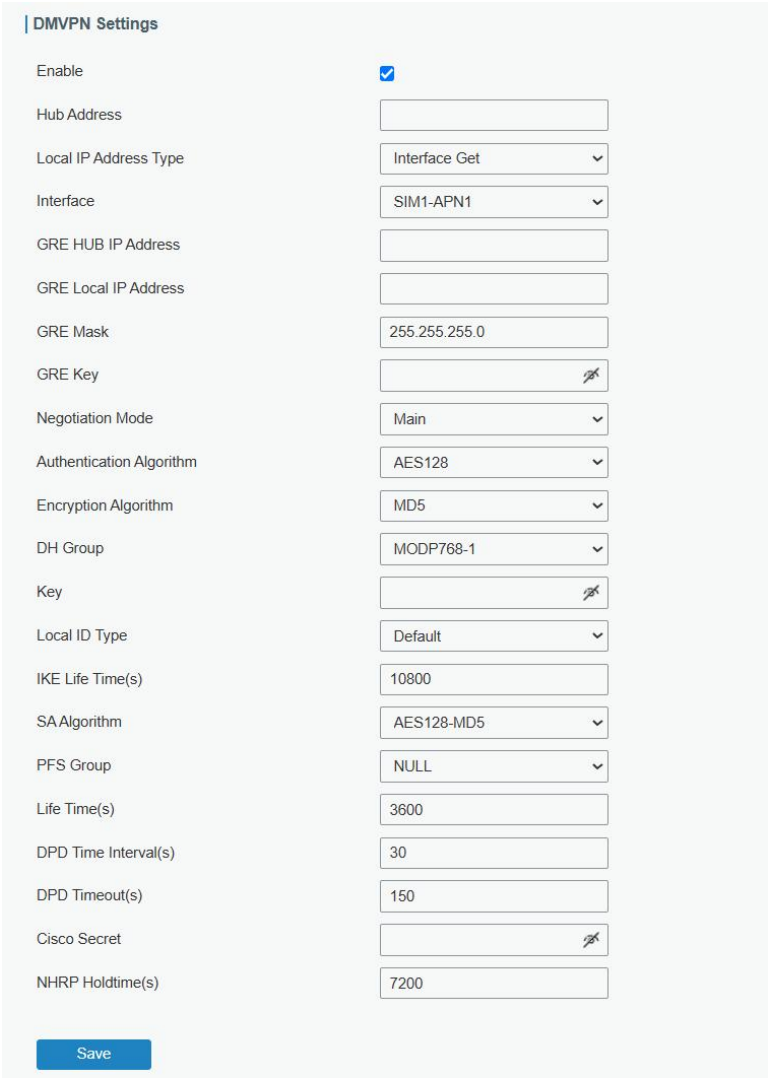


Figure 3-2-5-1

DMVPN	
Item	**Description**
Enable	Enable or disable DMVPN.
Hub Address	The IP address or domain name of DMVPN Hub.
Local IP Address Type	Local IP address obtaining method. Select from "Manual Input" and "Interface Get".
Local IP address	DMVPN local tunnel IP address.
Interface	Select the interface IP address to be used.
GRE Hub IP Address	GRE Hub tunnel IP address.
GRE Local IP Address	GRE local tunnel IP address.
GRE Netmask	GRE local tunnel netmask.
GRE Key	GRE tunnel key.
Negotiation Mode	Select from "Main" and "Aggressive".
Authentication Algorithm	Select from "DES", "3DES", "AES128", "AES192" and "AES256".
Encryption Algorithm	Select from "MD5", "SHA1" and “SHA2-256”.
DH Group	Select from "MODP768_1", "MODP1024_2", "MODP1536_5", “MODP2048-14” and “MODP3072-15”.
Key	Enter the preshared key.
Local ID Type	Select from "Default", "ID", "FQDN", and "User FQDN"
IKE Life Time (s)	Set the lifetime in IKE negotiation. Range: 60-86400.
SA Algorithm	Select from "DES_MD5", "DES_SHA1", “AES128-SHA256”, "3DES_MD5", "3DES_SHA1", "AES128_MD5", "AES128_SHA1", "AES192_MD5", "AES192_SHA1", “AES192-SHA256”, "AES256_MD5", “AES256-SHA256” and "AES256_SHA1".
PFS Group	Select from "NULL", "MODP768_1", "MODP1024_2" and "MODP1536-5".
Life Time (s)	Set the lifetime of IPsec SA. Range: 60-86400.
DPD Interval Time (s)	Set DPD interval time
DPD Timeout (s)	Set DPD timeout.
Cisco Secret	Cisco Nhrp key.
NHRP Holdtime (s)	The holdtime of NHRP protocol.

Table 3-2-5-1 DMVPN Parameters

3.2.5.2 IPSec Server

IPsec is especially useful for implementing virtual private networks and for remote user access through dial-up connection to private networks. A big advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers.

IPsec provides three choices of security service: Authentication Header (AH), Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE). AH essentially allows authentication of the senders' data. ESP supports both authentication of the sender and data encryption. IKE is used for cipher code exchange. All of them can protect one and more data flows between hosts, between host and

gateway, and between gateways.

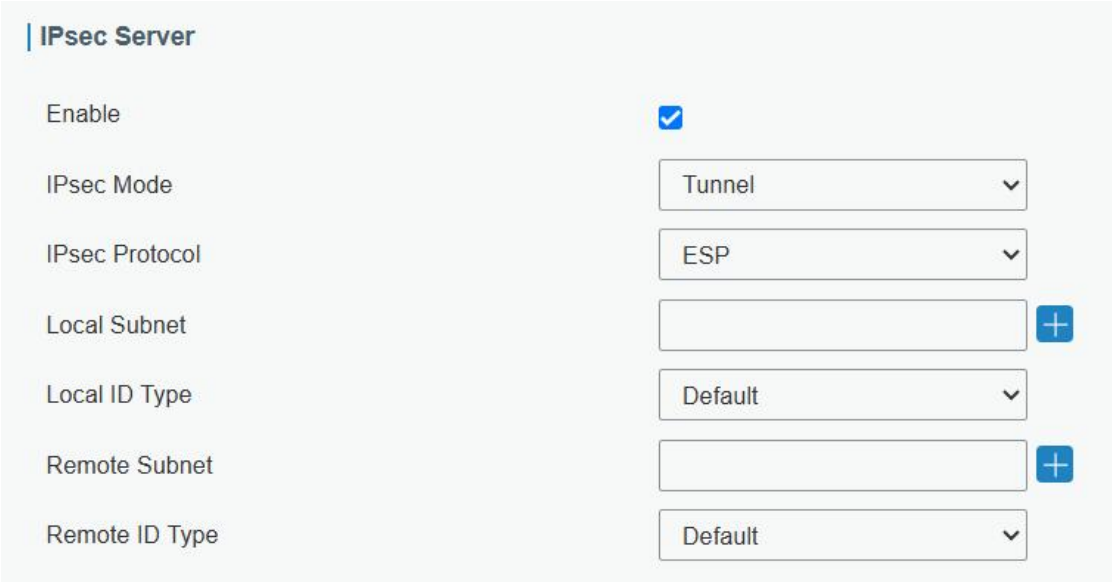


Figure 3-2-5-2

IPsec Server	
Item	**Description**
Enable	Enable or disable IPsec server mode.
IPsec Mode	Select Tunnel or Transport.
IPsec Protocol	Select from ESP or AH.
Local Subnet	Enter the local LAN subnet IP address on the IPsec tunnel. **Note:** Only when IKE version = IKEv2, is it supported to add multiple local subnets.
Local ID Type	Select the identifier type, and send it to remote peer. **Default:** None **ID:** use local subnet IP address as ID **FQDN:** fully qualified domain name, example: test.user.com **User FQDN:** fully qualified username string with email address format, example: test@user.com
Remote Subnet	Set the remote LAN subnet on the IPsec tunnel. **Note:** Only when IKE version = IKEv2, is it supported to add multiple remote subnets.
Remote ID type	Select the identifier type that is the same as remote peer local ID. **Default:** None **ID:** use remote subnet IP address as ID **FQDN:** fully qualified domain name, example: test.user.com **User FQDN:** fully qualified username string with email address format, example: test@user.com

Table 3-2-5-2 IPsec Server Parameters

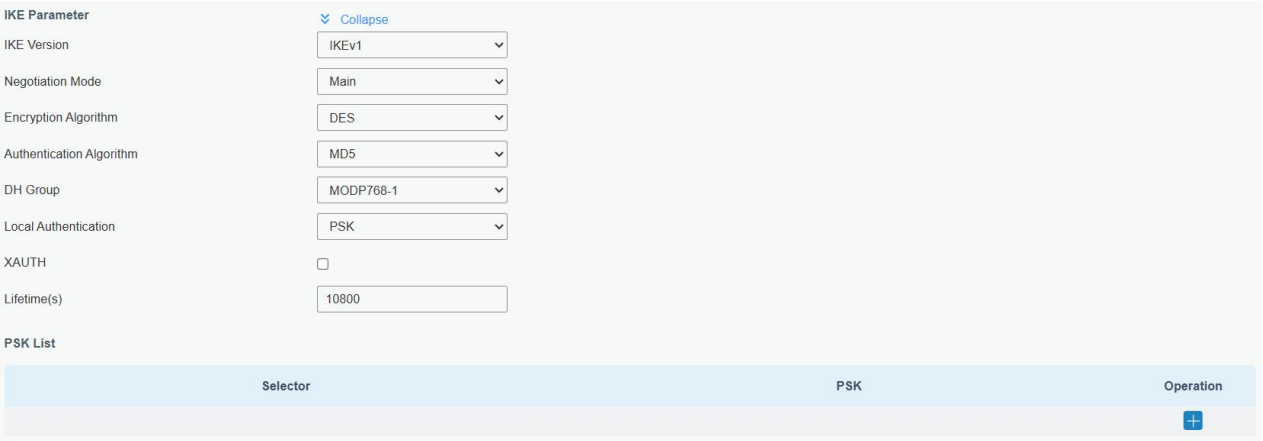


Figure 3-2-5-3

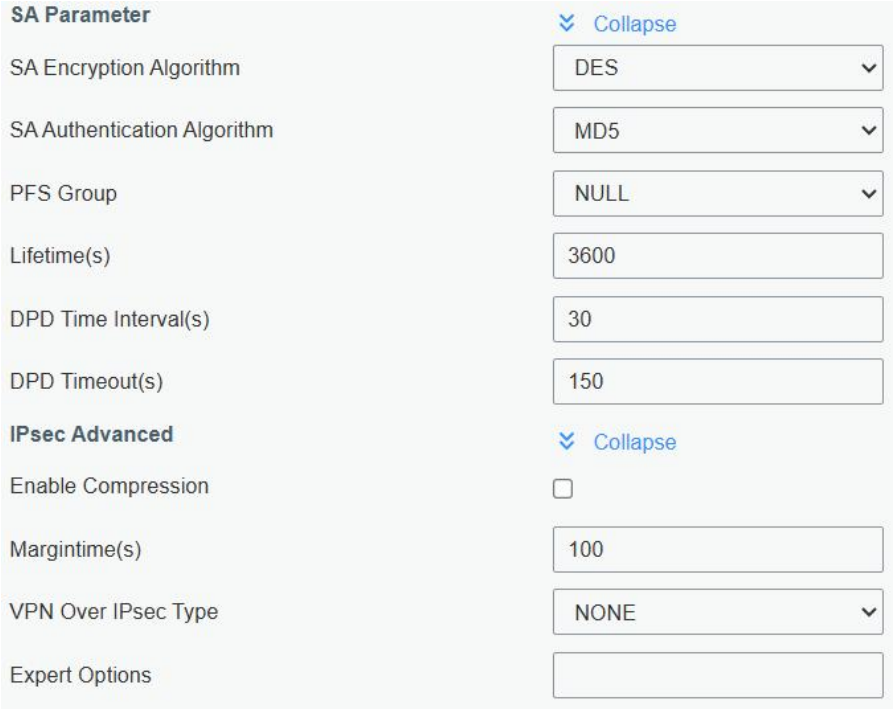


Figure 3-2-5-4

IKE Parameter	
Item	**Description**
IKE Version	Select the method of key exchange from IKEv1 and IKEv2.
Negotiation Mode	When using IKEv1, select Main or Aggressive.
Encryption Algorithm	Select DES, 3DES, AES128, AES192 or AES256.
Authentication Algorithm	Select MD5, SHA1 or SHA2-256.
DH Group	Select MODP768-1, MODP1024-2, MODP1536-5, MODP2048-14 or MODP3072-15.
Local Authentication	Select PSK or CA. **PSK:** use pre-shared key to complete the authentication. **CA:** use certificate to complete the authentication. After selecting, go to **Network > VPN > Certifications** page to import CA certificate, local certificate and private key to corresponding fields.
Remote Authentication	When using IKEv2, select PSK or CA.

	PSK: use pre-shared key to complete the authentication. **CA:** use certificate to complete the authentication. After selecting, go to **Network > VPN > Certifications** page to import remote certificate to corresponding fields.
XAUTH	When using IKEv1, define XAUTH username and password after XAUTH is enabled.
Lifetime (s)	Set the lifetime in IKE negotiation. Range: 60-86400.
XAUTH List	
Username	Enter the username used for the xauth authentication.
Password	Enter the password used for the xauth authentication.
PSK List	
Selector	Enter the corresponding identification number for PSK authentication.
PSK	Enter the pre-shared key.
SA Parameter	
SA Encryption Algorithm	Select DES, 3DES, AES128, AES192 or AES256.
SA Authentication Algorithm	Select MD5, SHA1 or SHA2-256.
PFS Group	Select NULL, MODP768-1 , MODP1024-2 or MODP1536-5.
Lifetime (s)	Set the lifetime of IPsec SA. Range: 60-86400 s.
DPD Time Interval(s)	Set DPD retry interval to send DPD requests. Range: 1-86400 s
DPD Timeout(s)	Set DPD timeout to detect the remote side fails. Range: 10-86400 s.
IPsec Advanced	
Enable Compression	The head of IP packet will be compressed after it's enabled.
Margintime	Set advanced time before the lifetime expires to begin the re-negotiation.
VPN Over IPsec Type	Select from NONE, GRE and L2TP.
Expert Options	User can enter some other initialization strings in this field and separate the strings with semicolon.

Table 3-2-5-3 IPsec Server Parameters

3.2.5.3 IPSec

UR32 supports running at most 3 IPsec clients at the same time.

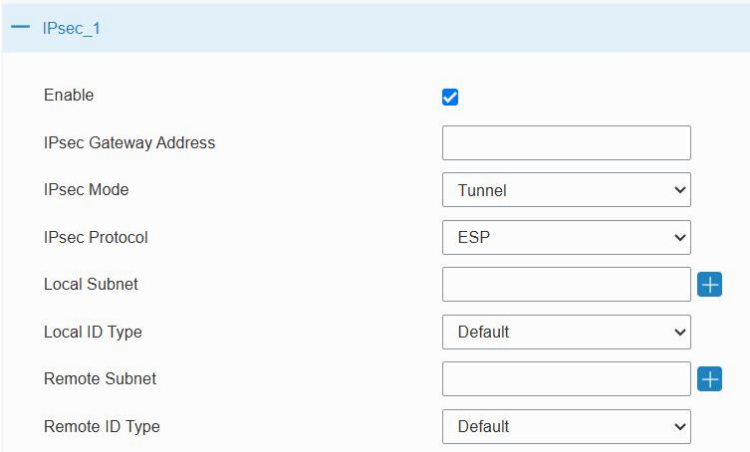


Figure 3-2-5-5

IPsec	
Item	**Description**
Enable	Enable or disable IPsec client mode. A maximum of 3 tunnels is allowed.
IP Gateway Address	Enter the remote IPsec server address.
IPsec Mode	Select Tunnel or Transport.
IPsec Protocol	Select from ESP or AH.
Local Subnet	Enter the local LAN subnet IP address on the IPsec tunnel. **Note:** Only when IKE version = IKEv2, is it supported to add multiple local subnets for connection.
Local ID Type	Select the identifier type, and send it to remote peer. **Default:** None **ID:** use local subnet IP address as ID **FQDN:** fully qualified domain name, example: test.user.com **User FQDN:** fully qualified username string with email address format, example: test@user.com
Remote Subnet	Set the remote LAN subnet on the IPsec tunnel. **Note:** Only when IKE version = IKEv2, is it supported to add multiple remote subnets for connection.
Remote ID type	Select the identifier type that is the same as remote peer local ID. **Default:** None **ID:** use remote subnet IP address as ID **FQDN:** fully qualified domain name, example: test.user.com **User FQDN:** fully qualified username string with email address format, example: test@user.com

Table 3-2-5-4 IPsec Parameters

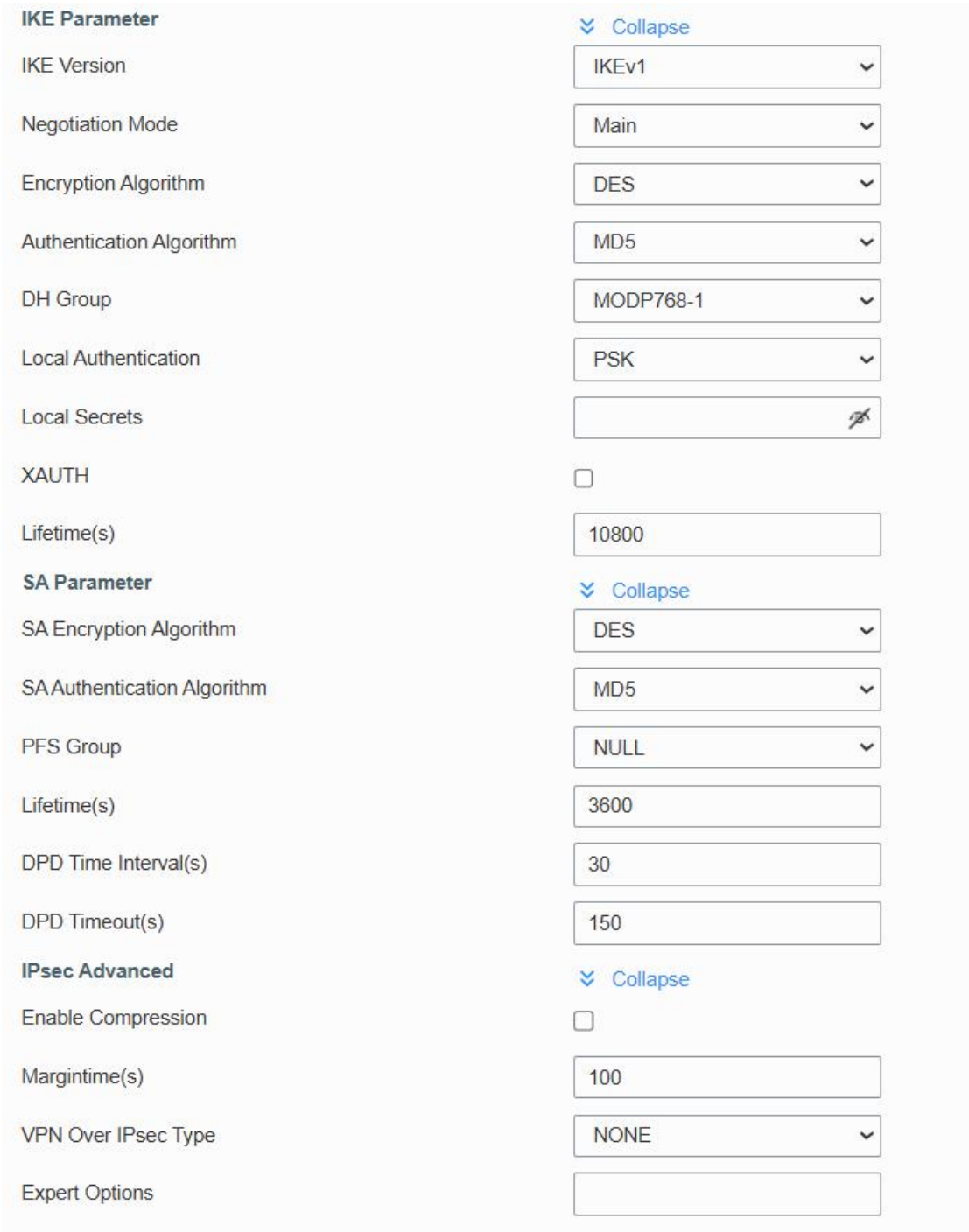


Figure 3-2-5-6

IKE Parameter	
Item	**Description**
IKE Version	Select the method of key exchange from IKEv1 and IKEv2.
Negotiation Mode	When using IKEv1, select Main or Aggressive.
Encryption Algorithm	Select DES, 3DES, AES128, AES192 or AES256.
Authentication Algorithm	Select MD5, SHA1 or SHA2-256.
DH Group	Select MODP768-1, MODP1024-2, MODP1536-5, MODP2048-14 or MODP3072-15.
Local Authentication	Select PSK or CA.

	PSK: use pre-shared key to complete the authentication. **CA:** use certificate to complete the authentication. After selecting, go to **Network > VPN > Certifications** page to import CA certificate, local certificate and private key to corresponding fields.
Local Secrets	Enter the pre-shared key which is defined on serer side.
Remote Authentication	When using IKEv2, select PSK or CA. **PSK:** use pre-shared key to complete the authentication. **CA:** use certificate to complete the authentication. After selecting, go to **Network > VPN > Certifications** page to import remote certificate to corresponding fields.
Remote Secrets	Enter the pre-shared key which is defined on server side.
XAUTH	Enter XAUTH username and password which is defined on server side.
Lifetime (s)	Set the lifetime in IKE negotiation. Range: 60-86400.
SA Parameter	
SA Encryption Algorithm	Select DES, 3DES, AES128, AES192 or AES256.
SA Authentication Algorithm	Select MD5, SHA1 or SHA2-256.
PFS Group	Select NULL, MODP768-1 , MODP1024-2 or MODP1536-5.
Lifetime (s)	Set the lifetime of IPsec SA. Range: 60-86400 s.
DPD Time Interval(s)	Set DPD retry interval to send DPD requests. Range: 1-86400 s
DPD Timeout(s)	Set DPD timeout to detect the remote side fails. Range: 10-86400 s.
IPsec Advanced	
Enable Compression	The head of IP packet will be compressed after it's enabled.
Margintime	Set advanced time before the lifetime expires to begin the re-negotiation.
VPN Over IPsec Type	Select from NONE, GRE and L2TP.
Expert Options	User can enter some other initialization strings in this field and separate the strings with semicolon.

Table 3-2-5-5 IPsec Parameters

3.2.5.4 GRE

Generic Routing Encapsulation (GRE) is a protocol that encapsulates packets in order to route other protocols over IP networks. It's a tunneling technology that provides a channel through which encapsulated data message could be transmitted and encapsulation and decapsulation could be realized at both ends.

In the following circumstances the GRE tunnel transmission can be applied:

- GRE tunnel could transmit multicast data packets as if it were a true network interface. Single use of IPSec cannot achieve the encryption of multicast.
- A certain protocol adopted cannot be routed.
- A network of different IP addresses shall be required to connect other two similar networks.

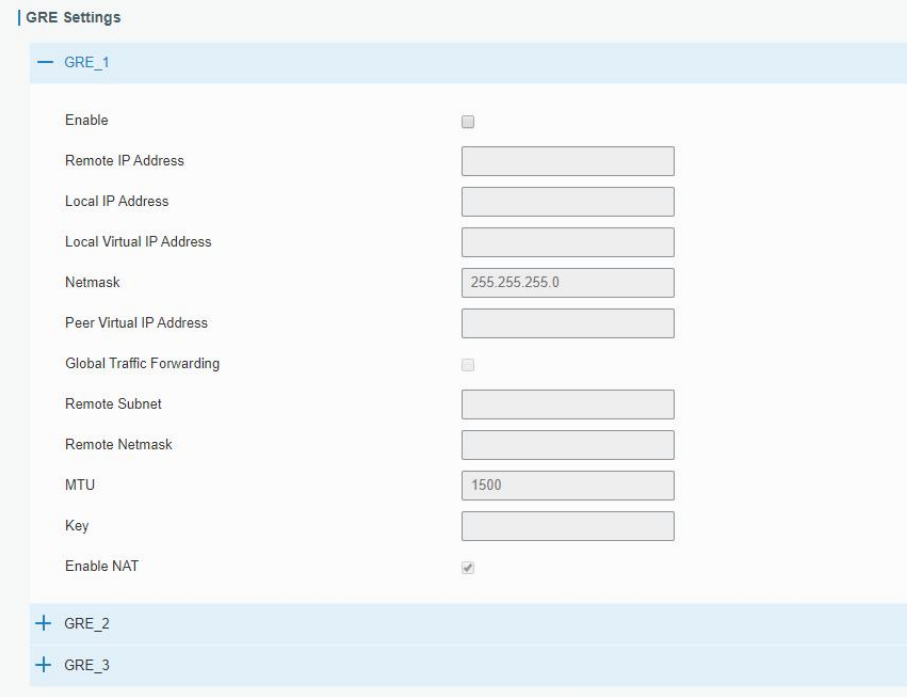


Figure 3-2-5-7

GRE	
Item	**Description**
Enable	Check to enable GRE function.
Remote IP Address	Enter the real remote IP address of GRE tunnel.
Local IP Address	Set the local IP address.
Local Virtual IP Address	Set the local tunnel IP address of GRE tunnel.
Netmask	Set the local netmask.
Peer Virtual IP Address	Enter remote tunnel IP address of GRE tunnel.
Global Traffic Forwarding	All the data traffic will be sent out via GRE tunnel when this function is enabled.
Remote Subnet	Enter the remote subnet IP address of GRE tunnel.
Remote Netmask	Enter the remote netmask of GRE tunnel.
MTU	Enter the maximum transmission unit. Range: 64-1500.
Key	Set GRE tunnel key.
Enable NAT	Enable NAT traversal function.

Table 3-2-5-6 GRE Parameters

3.2.5.5 L2TP

Layer Two Tunneling Protocol (L2TP) is an extension of the Point-to-Point Tunneling Protocol (PPTP) used by an Internet service provider (ISP) to enable the operation of a virtual private network (VPN) over the Internet.

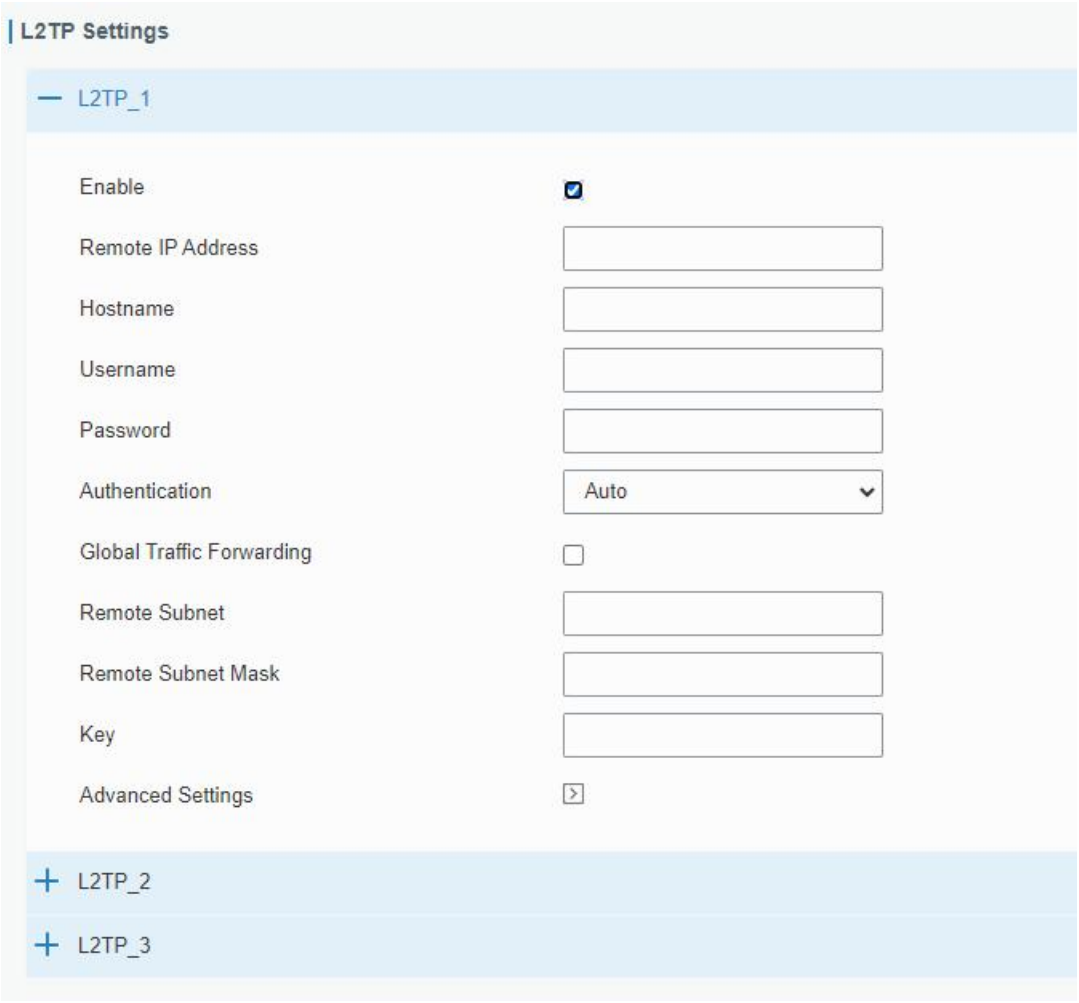


Figure 3-2-5-8

L2TP	
Item	**Description**
Enable	Check to enable L2TP function.
Remote IP Address	Enter the public IP address or domain name of L2TP server.
Hostname	Enter the hostname to verify with L2TP server.
Username	Enter the username that L2TP server provides.
Password	Enter the password that L2TP server provides.
Authentication	Select from "Auto", "PAP", "CHAP", "MS-CHAPv1" and "MS-CHAPv2".
Global Traffic Forwarding	All of the data traffic will be sent out via L2TP tunnel after this function is enabled.
Remote Subnet	Enter the remote IP address that L2TP protects.
Remote Subnet Mask	Enter the remote netmask that L2TP protects.
Key	Enter the password of L2TP tunnel.

Table 3-2-5-7 L2TP Parameters

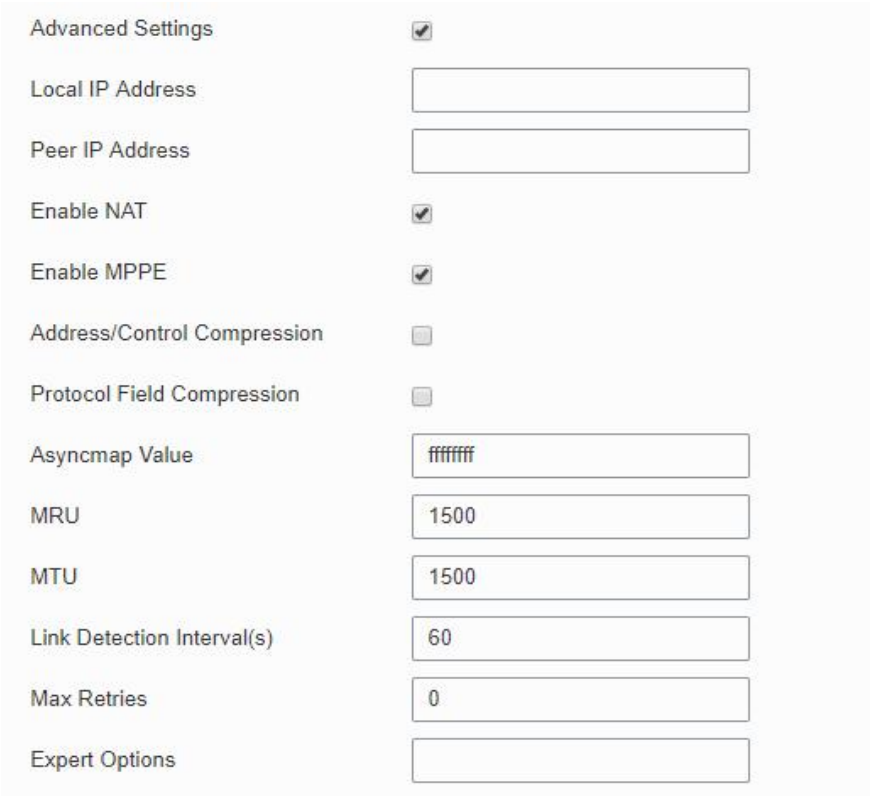


Figure 3-2-5-9

Advanced Settings	
Item	**Description**
Local IP Address	Set tunnel IP address of L2TP client. Client will obtain tunnel IP address automatically from the server when it's null.
Peer IP Address	Enter tunnel IP address of L2TP server.
Enable NAT	Enable NAT traversal function.
Enable MPPE	Enable MPPE encryption.
Address/Control Compression	For PPP initialization. User can keep the default option.
Protocol Field Compression	For PPP initialization. User can keep the default option.
Asyncmap Value	One of the PPP protocol initialization strings. User can keep the default value. Range: 0-ffffffff.
MRU	Set the maximum receive unit. Range: 64-1500.
MTU	Set the maximum transmission unit. Range: 64-1500
Link Detection Interval (s)	Set the link detection interval time to ensure tunnel connection. Range: 0-600.
Max Retries	Set the maximum times of retry to detect the L2TP connection failure. Range: 0-10.
Expert Options	User can enter some other PPP initialization strings in this field and separate the strings with blank space.

Table 3-2-5-8 L2TP Parameters

3.2.5.6 PPTP

Point-to-Point Tunneling Protocol (PPTP) is a protocol that allows corporations to extend their own corporate network through private "tunnels" over the public Internet. Effectively, a corporation uses a wide-area network as a single large local area network.

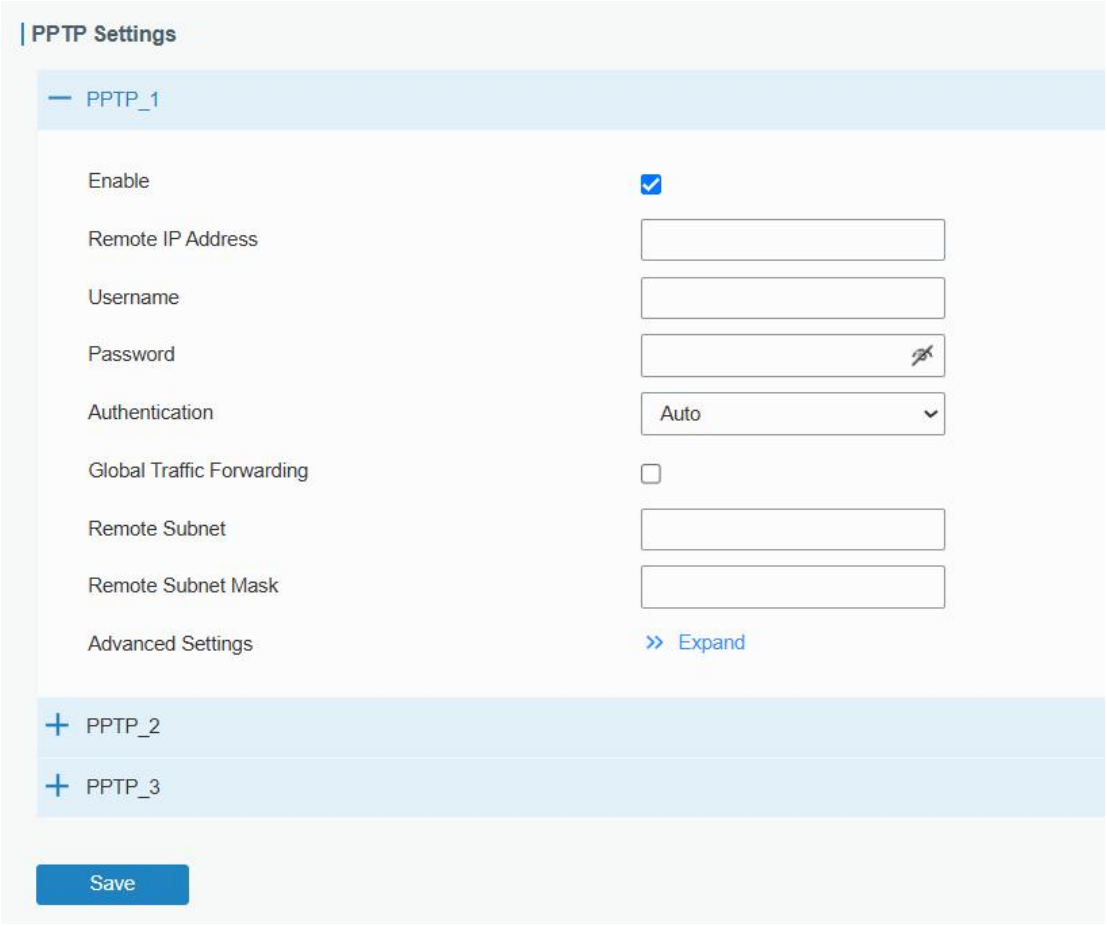


Figure 3-2-5-10

PPTP	
Item	**Description**
Enable	Enable PPTP client. A maximum of 3 tunnels is allowed.
Remote IP Address	Enter the public IP address or domain name of PPTP server.
Username	Enter the username that PPTP server provides.
Password	Enter the password that PPTP server provides.
Authentication	Select from "Auto", "PAP", "CHAP", "MS-CHAPv1", and "MS-CHAPv2".
Global Traffic Forwarding	All of the data traffic will be sent out via PPTP tunnel once enable this function.
Remote Subnet	Set the peer subnet of PPTP.
Remote Subnet Mask	Set the netmask of peer PPTP server.

Table 3-2-5-9 PPTP Parameters

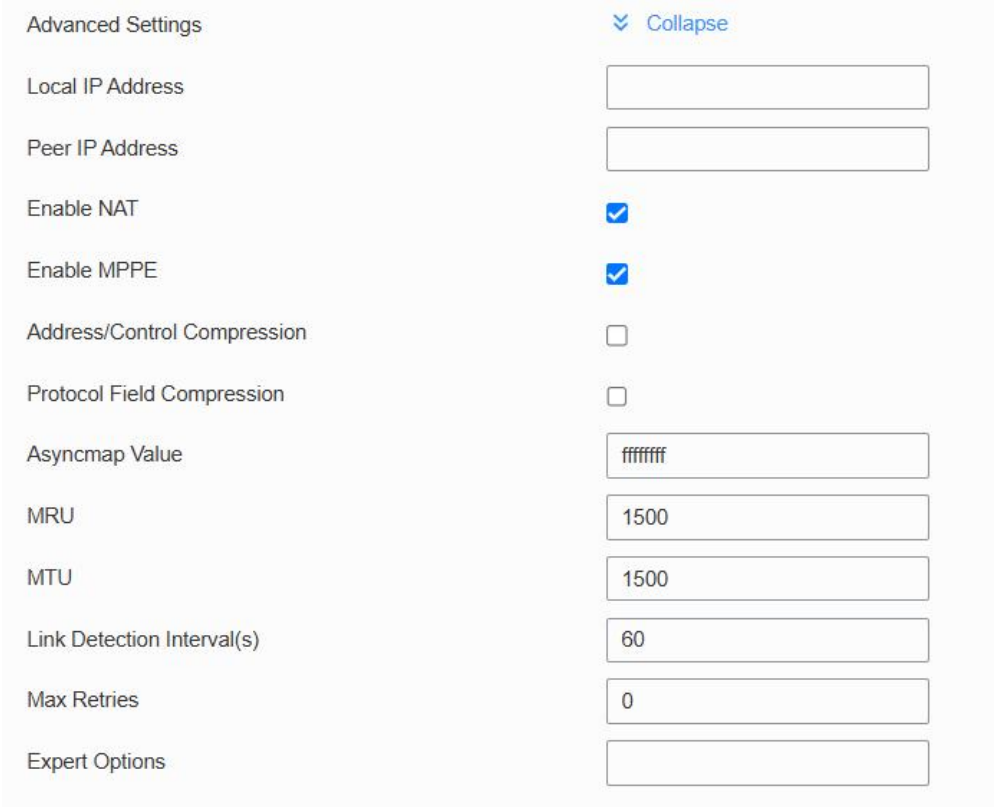


Figure 3-2-5-11

PPTP Advanced Settings	
Item	**Description**
Local IP Address	Set IP address of PPTP client.
Peer IP Address	Enter tunnel IP address of PPTP server.
Enable NAT	Enable the NAT faction of PPTP.
Enable MPPE	Enable MPPE encryption.
Address/Control Compression	For PPP initialization. User can keep the default option.
Protocol Field Compression	For PPP initialization. User can keep the default option.
Asyncmap Value	One of the PPP protocol initialization strings. User can keep the default value. Range: 0-ffffffff.
MRU	Enter the maximum receive unit. Range: 0-1500.
MTU	Enter the maximum transmission unit. Range: 0-1500.
Link Detection Interval (s)	Set the link detection interval time to ensure tunnel connection. Range: 0-600.
Max Retries	Set the maximum times of retrying to detect the PPTP connection failure. Range: 0-10.
Expert Options	User can enter some other PPP initialization strings in this field and separate the strings with blank space.

Table 3-2-5-10 PPTP Parameters

3.2.5.7 OpenVPN Client

OpenVPN is an open source virtual private network (VPN) product that offers a simplified security framework, modular network design, and cross-platform portability. The default OpenVPN version of UR32 is 2.4.9.

UR32 supports running at most 3 OpenVPN clients at the same time. You can import the ovpn file directly or configure the parameters on this page to set clients.

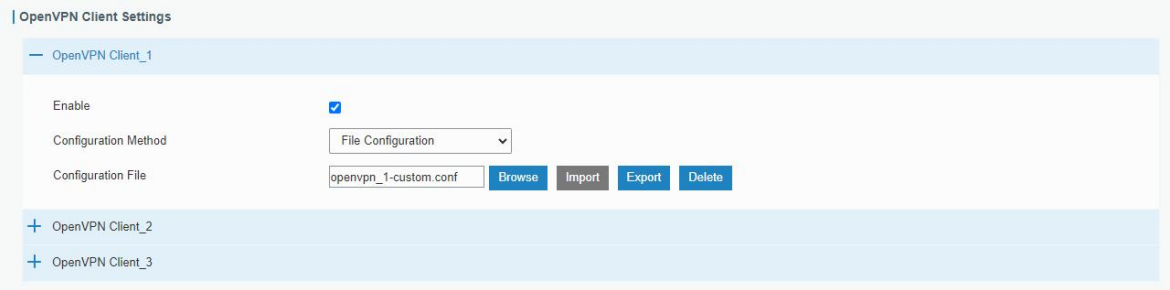


Figure 3-2-5-12

OpenVPN Client - File Configuration	
Item	**Description**
Browse	Click to browse the client configuration ovpn format file including the settings and certificate contents. Please refer to the client configuration file according to sample: client.conf
Edit	Click to edit the imported file.
Export	Export the server configuration file.
Delete	Click to delete the configuration file.

Table 3-2-5-11 OpenVPN Client Parameters

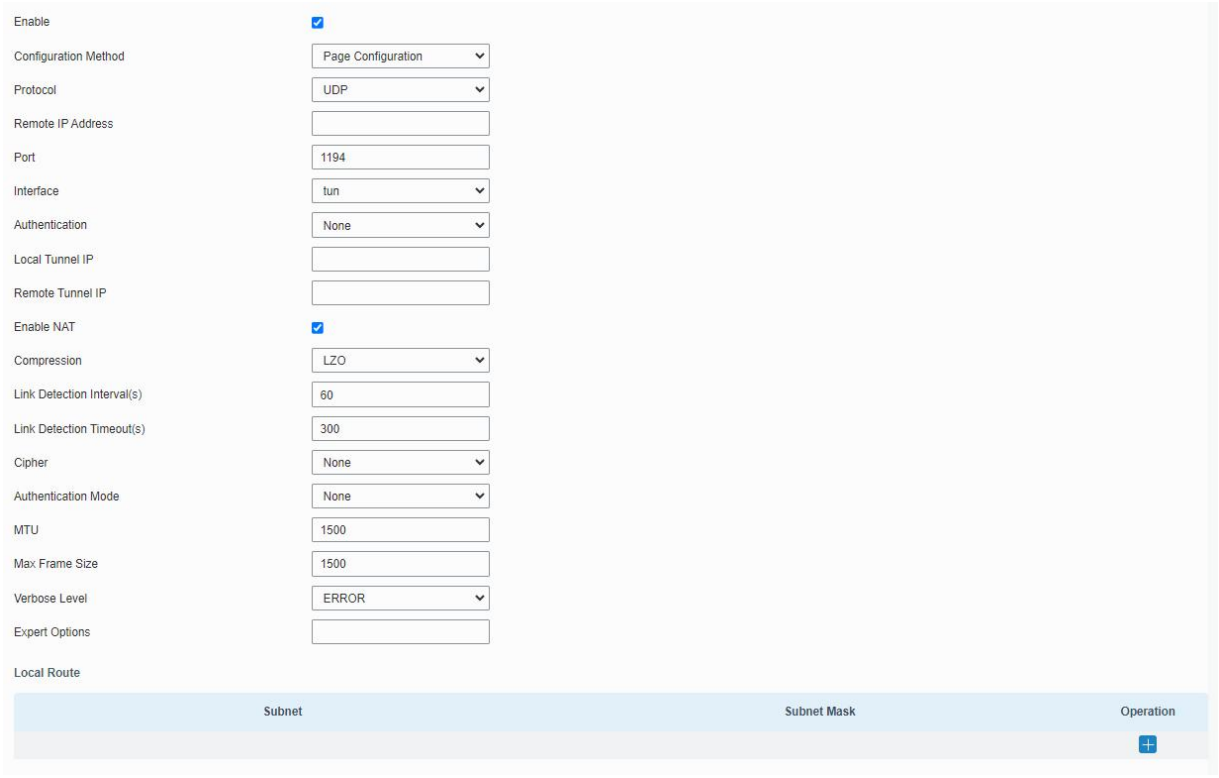


Figure 3-2-5-13

OpenVPN Client - Page Configuration	
Item	**Description**
Protocol	Select a transport protocol used by connecting UDP and TCP.
Remote IP Address	Enter remote OpenVPN server's IP address or domain name.
Port	Enter the TCP/UCP service number of remote OpenVPN server. Range: 1-65535.
Interface	Select virtual VPN network interface type from TUN and TAP. TUN devices encapsulate IPv4 or IPv6 (OSI Layer 3) while TAP devices encapsulate Ethernet 802.3 (OSI Layer 2).
Authentication Type	Select authentication type used to secure data sessions. **Pre-shared:** use the same secret key as server to complete the authentication. After selecting, go to **Network > VPN > Certifications** page to import a static.key to **PSK** field. **Username/Password:** use username/password which is preset in server side to complete the authentication. **X.509 cert:** use X.509 type certificate to complete the authentication. After selecting, go to **Network > VPN > Certifications** page to import CA certificate, client certificate and client private key to corresponding fields. **X.509 cert + user:** use both username/password and X.509 cert authentication type.
Local Virtual IP	Set local tunnel address when authentication type is **None** or **Pre-shared**.
Remote Virtual IP	Set remote tunnel address when authentication type is **None** or **Pre-shared**.
Global Traffic Forwarding	All the data traffic will be sent out via OpenVPN tunnel when this function is enabled.
Enable TLS Authentication	Select from None, TLS Auth and TLS Crypt. When selecting TLS Auth or TLS Crypt, go to **Network > VPN > Certifications** page to import a ta.key.
Compression	Select to enable or disable LZO to compress data.
Link Detection Interval (s)	Set link detection interval time to ensure tunnel connection. If this is set on both server and client, the value pushed from server will override the client local values. Range: 10-1800 s.
Link Detection Timeout (s)	OpenVPN will be reestablished after timeout. If this is set on both server and client, the value pushed from server will override the client local values. Range: 60-3600 s.
Cipher	Select from NONE, BF-CBC, DES-CBC, DES-EDE3-CBC, AES-128-CBC, AES-192-CBC and AES-256-CBC. **Note:** The BF-CBC, DES-CBC, DES-EDE3-CBC algorithm has security risks; it is recommended to use AES.
Authentication Mode	Select from NONE, MD5, SHA1, SHA256, and SHA512.
MTU	Enter the maximum transmission unit. Range: 128-1500.
Max Frame Size	Set the maximum frame size. Range: 128-1500.
Verbose Level	Select from ERROR, WARING, NOTICE and DEBUG.
Expert Options	User can enter some initialization strings in this field and separate the strings with semicolon.

	Example: ncp-ciphers AES-128-GCM; key direction 1
Local Route	
Subnet	Set the local route's IP address.
Subnet Mask	Set the local route's netmask.

Table 3-2-5-12 OpenVPN Client Parameters

Related Topic

OpenVPN Client Application Example

3.2.5.8 OpenVPN Server

The UR32 supports OpenVPN server to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. You can import the ovpn file directly or configure the parameters on this page to set this server. UR32 supports at most 20 openVPN clients connections.

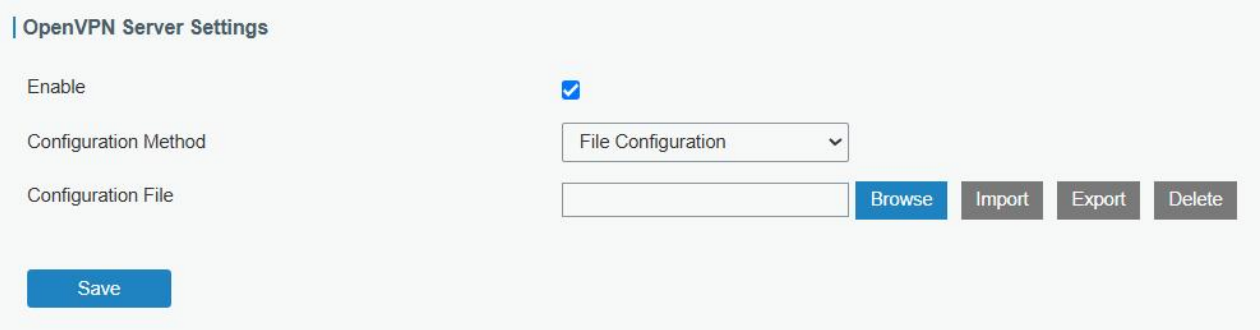


Figure 3-2-5-14

OpenVPN Server - File Configuration	
Item	**Description**
Browse	Click to browse the server configuration ovpn format file including the settings and certificate contents. Please refer to the server configuration file according to sample: server.conf
Edit	Click to edit the imported file.
Export	Export the server configuration file.
Delete	Click to delete the configuration file.

Table 3-2-5-13 OpenVPN Server Parameters

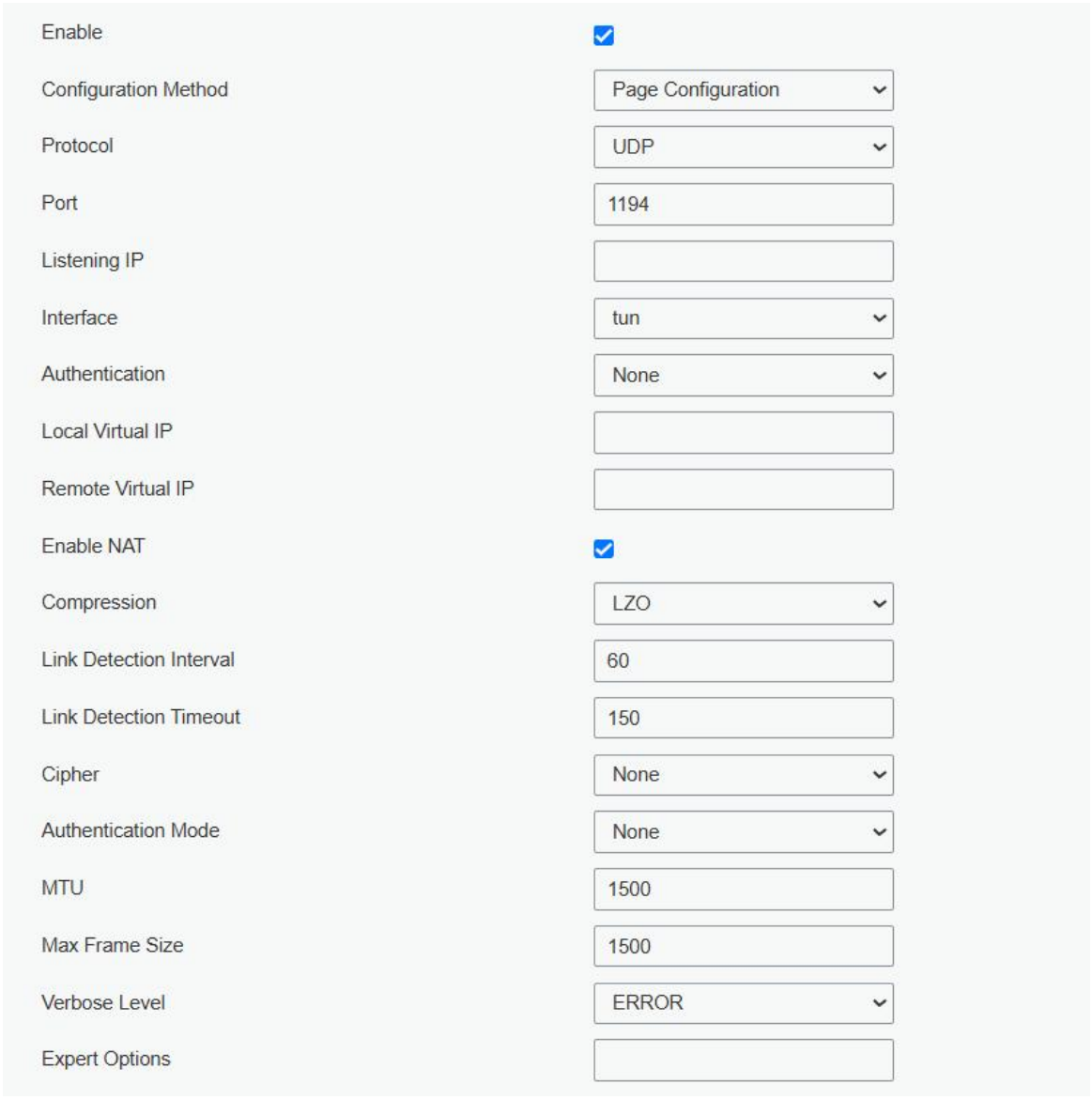


Figure 3-2-5-15

Figure 3-2-5-16

OpenVPN Server - Page Configuration	
Item	**Description**
Protocol	Select a transport protocol used by connection from UDP and TCP.
Listening IP	Enter the local hostname or IP address for bind. If left blank, OpenVPN server will bind to all interfaces.

Port	Enter the TCP/UCP service number for OpenVPN client connection. Range: 1-65535.
Interface	Select virtual VPN network interface type from TUN and TAP. TUN devices encapsulate IPv4 or IPv6 (OSI Layer 3) while TAP devices encapsulate Ethernet 802.3 (OSI Layer 2).
Authentication Type	Select authentication type used to secure data sessions. **Pre-shared:** use the same secret key as server to complete the authentication. After select, go to **Network > VPN > Certifications** page to import a static.key to **PSK** field. **Username/Password:** use username/password which is preset in server side to complete the authentication. **X.509 cert:** use X.509 type certificate to complete the authentication. After select, go to **Network > VPN > Certifications** page to import CA certificate, client certificate and client private key to corresponding fields. **X.509 cert + user:** use both username/password and X.509 cert authentication type.
Local Virtual IP	Set local tunnel address when authentication type is **None** or **Pre-shared**.
Remote Virtual IP	Set remote tunnel address when authentication type is **None** or **Pre-shared**.
Client Subnet	Define an IP address pool for openVPN client.
Client Netmask	Set the client subnet netmask to limit the IP address range.
Renegotiation Interval	Renegotiate data channel key after this interval. 0 means disable.
Max Clients	Limit server to a maximum of concurrent clients, range: 1-20. **Note:** please adjust log severity to Info if you need to connect many clients.
Enable CRL	Enable or disable CRL verify.
Enable Client to Client	When enabled, openVPN clients can communicate with each other.
Enable Dup Client	Allow multiple clients to connect with the same common name or certification.
Enable TLS Authentication	Select from None, TLS Auth and TLS Crypt. When selecting TLS Auth or TLS Crypt, go to **Network > VPN > Certifications** page to import a ta.key.
Compression	Select to enable or disable LZO to compress data.
Link Detection Interval (s)	Set link detection interval time to ensure tunnel connection. If this is set on both server and client, the value pushed from server will override the client local values. Range: 10-1800 s.
Link Detection Timeout (s)	OpenVPN will be reestablished after timeout. If this is set on both server and client, the value pushed from server will override the client local values. Range: 60-3600 s.
Cipher	Select from NONE, BF-CBC, DES-CBC, DES-EDE3-CBC, AES-128-CBC, AES-192-CBC and AES-256-CBC. **Note:** The BF-CBC, DES-CBC, DES-EDE3-CBC algorithm has security risks; it is recommended to use AES.
Authentication Mode	Select from NONE, MD5, SHA1, SHA256, and SHA512.
MTU	Enter the maximum transmission unit. Range: 64-1500.

Max Frame Size	Set the maximum frame size. Range: 64-1500.
Verbose Level	Select from ERROR, WARING, NOTICE and DEBUG.
Expert Options	User can enter some initialization strings in this field and separate the strings with semicolon. **Example:** ncp-ciphers AES-128-GCM; key direction 1
Account	
Username & Password	Set username and password for OpenVPN client when authentication type is username/password.
Local Route	
Subnet	Set the local route's IP address.
Subnet Mask	Set the local route's netmask.
Client Subnet	
Name	Set the name as OpenVPN client certificate common name.
Subnet	Set the subnet of OpenVPN client.
Subnet Mask	Set the subnet netmask of OpenVPN client.

Table 3-2-5-14 OpenVPN Server Parameters

3.2.5.9 WireGuard

WireGuard is an extremely simple yet fast and modern VPN that utilizes state-of-the-art cryptography. WireGuard passes traffic over UDP protocol.

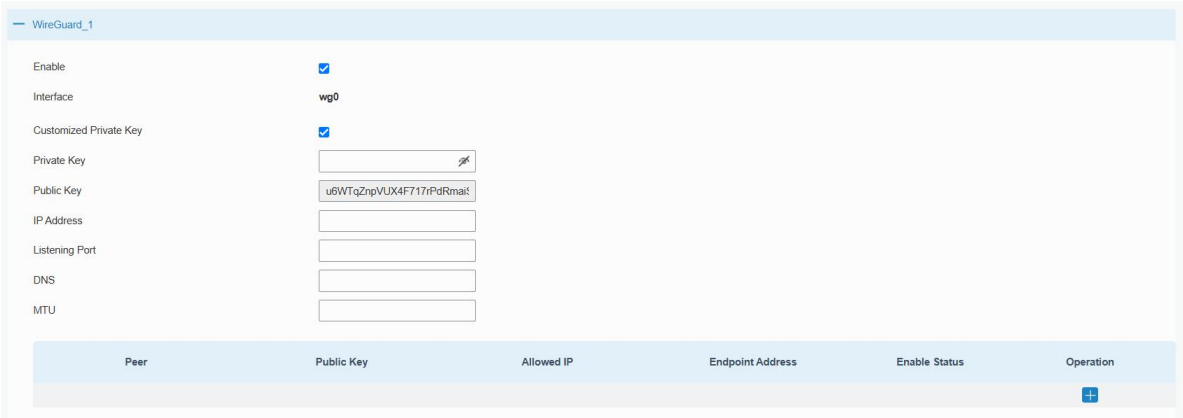


Figure 3-2-5-21

WireGuard	
Item	**Description**
Enable	Enable WireGuard interface. A maximum of 3 WireGaurd interfaces is allowed.
Interface	Show the WireGuard interface name.
Customized Private Key	Enable or disable to customize the private key of this WireGuard interface. If disabled, the client will use the private key generated by this router.
Public Key	Show the public key generated by the private key.
IP Address	Set the local virtual IP address and netmask. Example: 10.8.0.2/24
Listening Port	Set the port to send or receive WireGuard packets. The port numbers of different WireGuard interfaces should be different.
DNS	Set the DNS server address of this WireGuard interface. If left blank,

	the router will use DNS server address of common network interfaces (WAN, cellular, etc.).
MTU	Set the maximum transmission unit of this WireGuard interface. If left blank, the router will use MTU of common network interfaces (WAN, cellular, etc.).
Peer Table	Click "+" to add WireGuard peers of this WireGuard interface. One WireGuard interface can add 20 peers at most.

Table 3-2-5-15 WireGuard Parameters

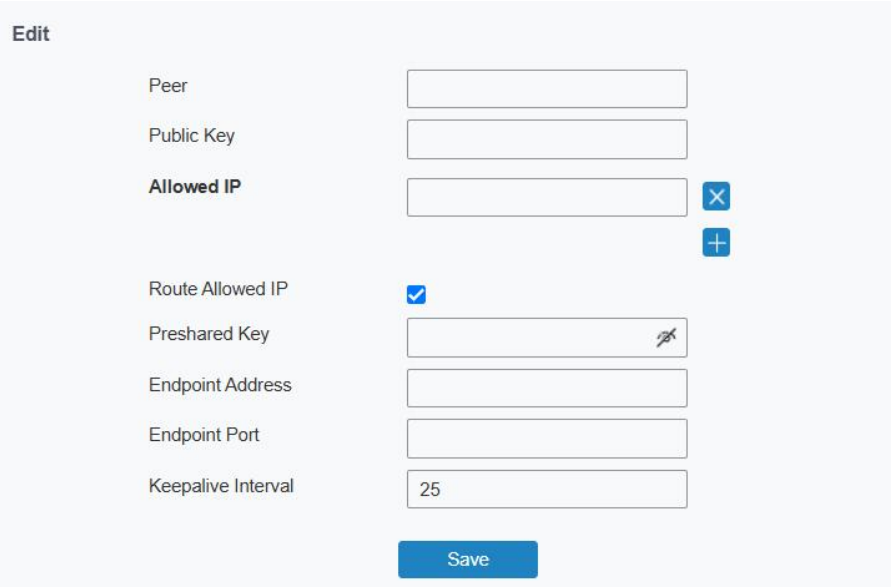


Figure 3-2-5-22

WireGuard-Peer	
Item	**Description**
Peer	Set a WireGuard peer name. This name should be unique in this WireGuard client.
Public Key	Set the public key of WireGuard peer server/client.
Allowed IP	Set the real IP address and netmask of WireGuard peer's LAN network. Example: 192.168.1.0/24 One WireGuard peer supports to add 8 allowed IP addresses.
Route Allowed IP	Enable or disable to add static routings of allowed IP addresses.
Preshared Key	Set the presahred key and both this interface and peer interface should set the same key value.
Endpoint Address	Set IP address or domain name of WireGuard peer server/client.
Endpoint Port	Set the destination port of WireGuard peer server/client.
Keepalive Interval	After the connection is established, this WireGuard interface will send heartbeat packet regularly to keep alive. 0 means disabled.

Table 3-2-5-16 WireGuard-Peer Parameters

3.2.5.10 ZeroTier

ZeroTier is a way to connect devices over your own private network anywhere in the world. You do this by creating a network and then joining two or more devices to that network.

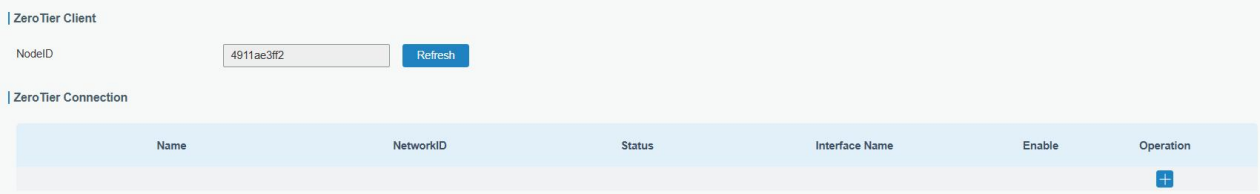


Figure 3-2-5-23

ZeroTier	
Item	**Description**
ZeroTier Client	
NodeID	The router's own automatically generated ID.
Refresh	Click to regenerate a new Node ID.
ZeroTier Connection	
Name	Customize the name of the connection.
NetworkID	The ZeroTier virtual Ethernet network that the router will join.
Status	Display the status of the connection between the router and the ZeroTier virtual Ethernet network.
Interface Name	Display the name of the virtualized network interface to which the router is added.
Enable	Check to enable this function.

Table 3-2-5-17

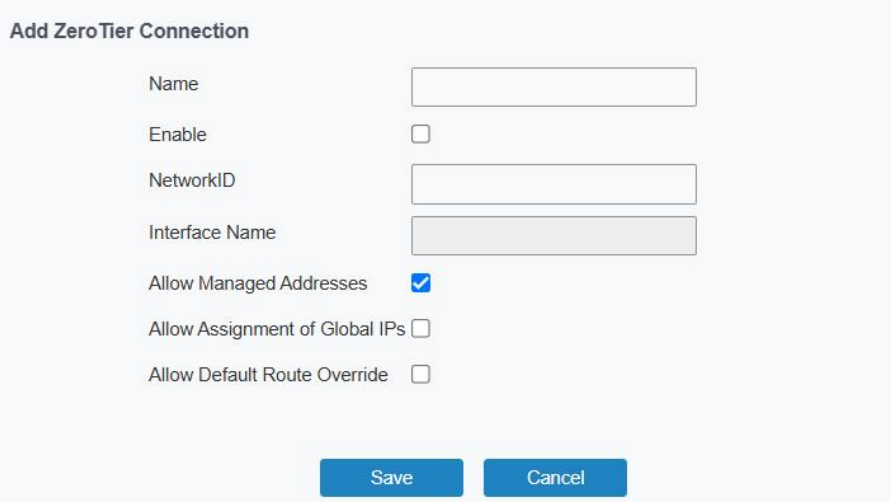


Figure 3-2-5-24

Add ZeroTier Connection	
Item	**Description**
Name	Customize the name of the connection.
Enable	Check to enable this function
NetworkID	The ZeroTier virtual Ethernet network that the device will join.
Interface Name	Display the name of the virtualized network interface to which the

	router is added.
Allow Managed Addresses	Allow or disables the ZeroTier controller to dynamically assign IP addresses and configure routing information when the router joins the network.
Allow Assignment of Global IPs	Allow or disallow ZeroTier network controllers to assign worldwide IPv6 addresses.
Allow Default Route Override	Allow or disallow the router to override the default route settings when connecting to the ZeroTier network.

Table 3-2-5-18

3.2.5.11 Certifications

User can import/export certificate and key files for OpenVPN and IPsec on this page.

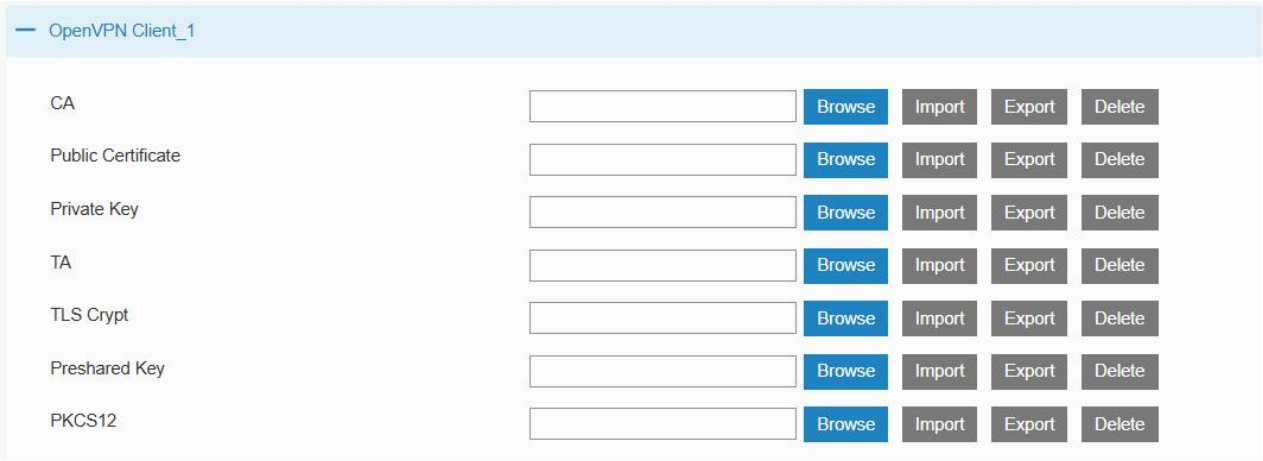


Figure 3-2-5-17

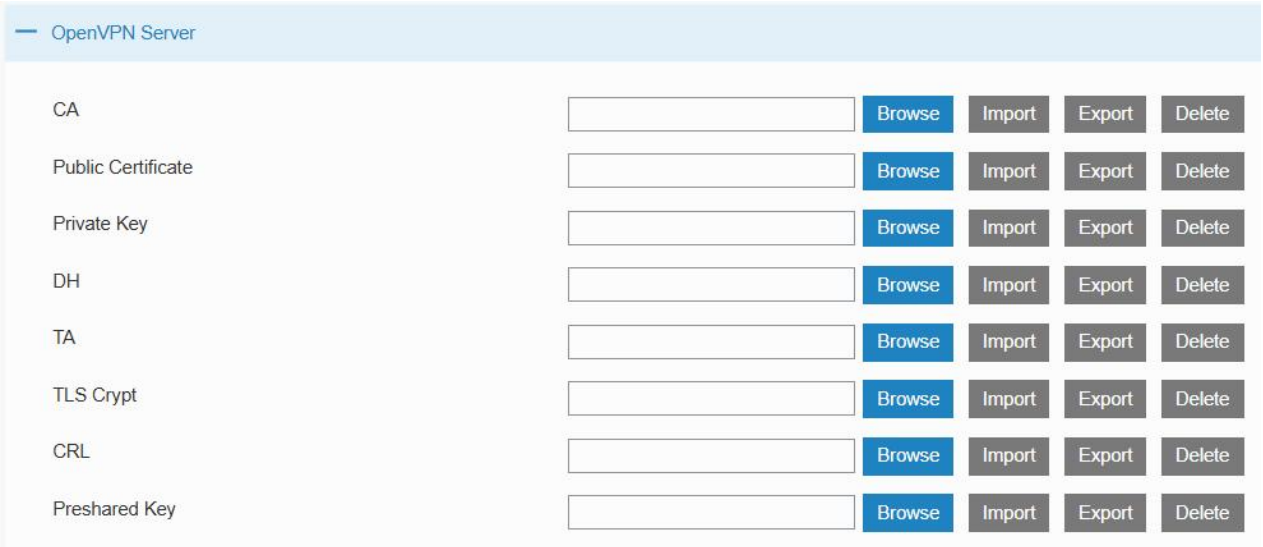


Figure 3-2-5-18

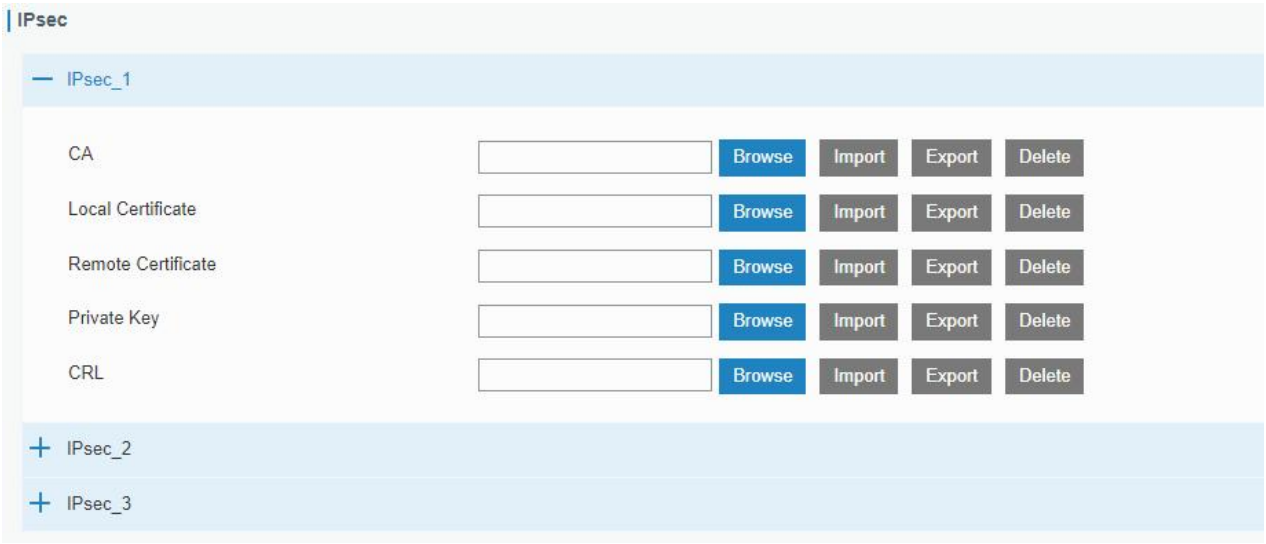


Figure 3-2-5-19

Figure 3-2-5-20

3.2.6 IP Passthrough

IP Passthrough mode shares or "passes" the Internet providers assigned IP address to a single LAN client device connected to the router.

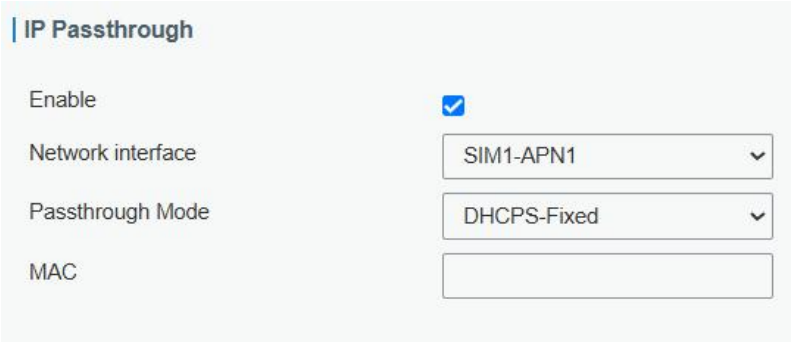


Figure 3-2-6-1

IP Passthrough	
Item	**Description**
Enable	Enable or disable IP Passthrough.

Network Interface	Select network interface from SIM1-APN1, SIM1-APN2, SIM1-APN3, SIM2-APN1, SIM2-APN2 and SIM2-APN3.
Passthrough Mode	Select passthrough mode from DHCPS-Fixed and DHCPS-Dynamic.
MAC	Set MAC address when mode is DHCPS-Fixed.

Table 3-2-6-1 IP Passthrough Parameters

3.2.7 Routing

3.2.7.1 Static Routing

A static routing is a manually configured routing entry. Information about the routing is manually entered rather than obtained from dynamic routing traffic. After setting static routing, the package for the specified destination will be forwarded to the path designated by user.

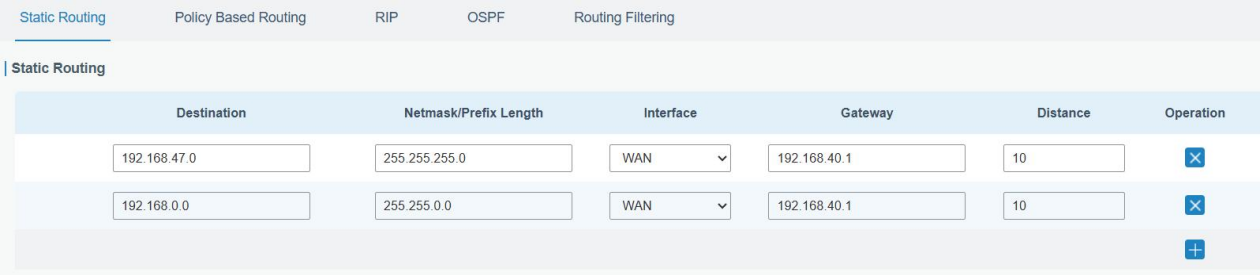


Figure 3-2-7-1

Static Routing	
Item	**Description**
Destination	Enter the destination IP address.
Netmask/Prefix Length	Enter the subnet mask or prefix length of destination address.
Interface	The interface through which the data can reach the destination address.
Gateway	IP address of the next router that will be passed by before the input data reaches the destination address.
Distance	Priority, smaller value refers to higher priority. Range: 1-255.

Table 3-2-7-1 Static Routing Parameters

3.2.7.2 Priority Based Routing

Policy-based routing (PBR) is a technique used in computer networks to direct network packets based on defined criteria beyond the standard destination-based routing. Unlike traditional routing, which forwards packets solely based on their destination address, PBR allows to customize routing decisions according to various factors. **Policy-based routing takes precedence over static routing.**
With policy-based routing you can implement specific rules or policies to dictate the path that packets should take through the network. This flexibility enables organizations to optimize traffic flow, prioritize certain types of traffic, enforce security measures, and manage network resources more efficiently.

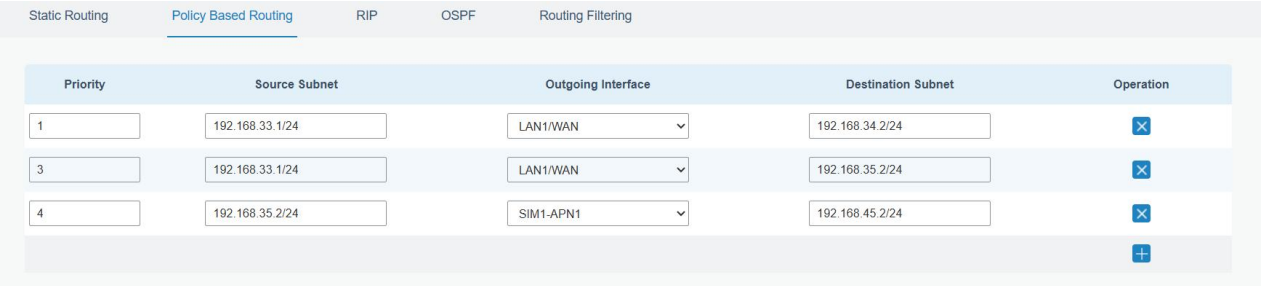


Figure 3-2-7-2

Priority-Based Routing	
Item	**Description**
Priority	Set the priority of this policy. The smaller the number, the higher the priority. Valid range: 1–255.
Source Subnet	Traffic that matches the specified source subnet will be applied to this policy. Leave blank if no source subnet matching is required.
Outgoing Interface	Traffic that matches both the source and destination subnets will be forwarded through the selected interface. Policy routing has higher priority than static routing.
Destination Subnet	Traffic that matches the specified destination subnet will be applied to this policy.
Operation	You can add or delete the policy routing configuration.

Table 3-2-7-2 Priority-Based Routing Parameters

Related Topics

Cellular

3.2.7.3 PIR

RIP is mainly designed for small networks. RIP uses Hop Count to measure the distance to the destination address, which is called Metric. In RIP, the hop count from the router to its directly connected network is 0 and the hop count of network to be reached through a router is 1 and so on. In order to limit the convergence time, the specified metric of RIP is an integer in the range of 0 - 15 and the hop count larger than or equal to 16 is defined as infinity, which means that the destination network or host is unreachable. Because of this limitation, the RIP is not suitable for large-scale networks. To improve performance and prevent routing loops, RIP supports split horizon function. RIP also introduces routing obtained by other routing protocols.

Each router that runs RIP manages a routing database, which contains routing entries to reach all reachable destinations.

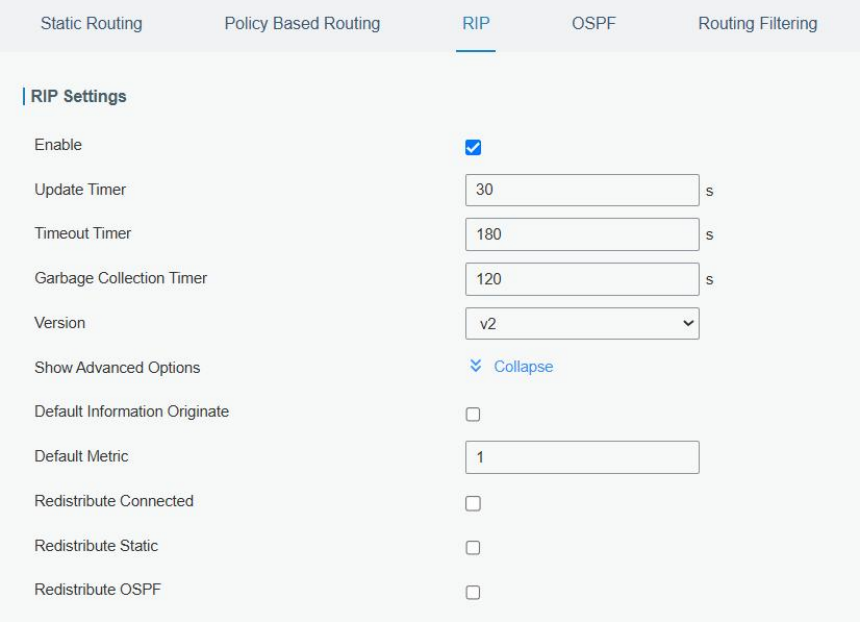


Figure 3-2-7-3

RIP	
Item	**Description**
Enable	Enable or disable RIP.
Update Timer	It defines the interval to send routing updates. Range: 5-2147483647, in seconds.
Timeout Timer	It defines the routing aging time. If no update package on a routing is received within the aging time, the routing's Routing Cost in the routing table will be set to 16. Range: 5-2147483647, in seconds.
Garbage Collection Timer	It defines the period from the routing cost of a routing becomes 16 to it is deleted from the routing table. In the time of Garbage-Collection, RIP uses 16 as the routing cost for sending routing updates. If Garbage Collection times out and the routing still has not been updated, the routing will be completely removed from the routing table. Range: 5-2147483647, in seconds.
Version	RIP version. The options are v1 and v2.
Advanced Settings	
Default Information Originate	Default information will be released when this function is enabled.
Default Metric	The default cost for the router to reach destination. Range: 0-16
Redistribute Connected	Check to enable.
Metric	Set metric after "Redistribute Connected" is enabled. Range: 0-16.
Redistribute Static	Check to enable.
Metric	Set metric after "Redistribute Static" is enabled. Range: 0-16.
Redistribute OSPF	Check to enable.
Metric	Set metric after "Redistribute OSPF" is enabled. Range: 0-16.

Table 3-2-7-3 RIP Parameters

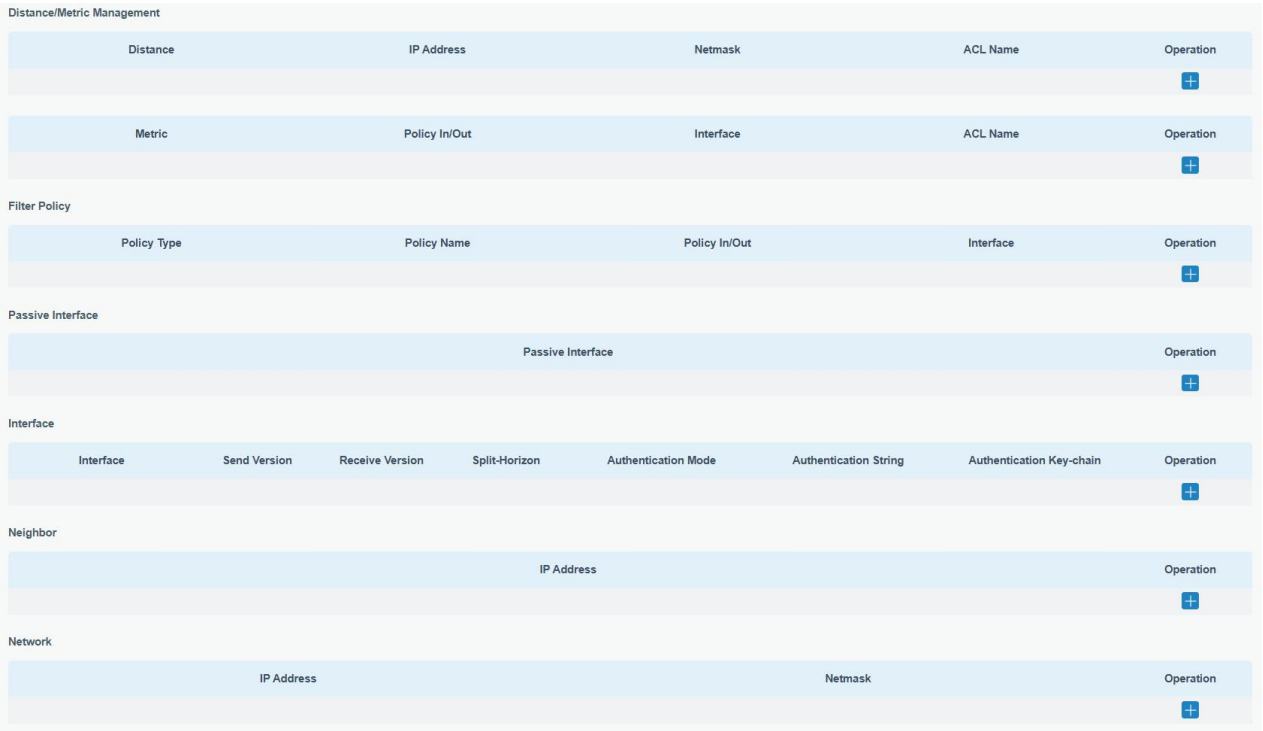


Figure 3-2-7-4

Item	Description
Distance/Metric Management	
Distance	Set the administrative distance that a RIP route learns. Range: 1-255.
IP Address	Set the IP address of RIP route.
Netmask	Set the netmask of RIP route.
ACL Name	Set ACL name of RIP route.
Metric	The metric of received route or sent route from the interface. Range: 0-16.
Policy in/out	Select from "in" and "out".
Interface	Select interface of the route.
ACL Name	Access control list name of the route strategy.
Filter Policy	
Policy Type	Select from "access-list" and "prefix-list".
Policy Name	User-defined prefix-list name.
Policy in/out	Select from "in" and "out".
Interface	Select interface from "cellular0", "LAN1/WAN" and "Bridge0".
Passive Interface	
Passive Interface	Select interface from "cellular0" and "LAN1/WAN", "Bridge0".
Interface	
Interface	Select interface from "cellular0", "LAN1/WAN" and "Bridge0".

Send Version	Select from "default", "v1" and "v2".
Receive Version	Select from "default", "v1" and "v2".
Split-Horizon	Select from "enable" and "disable".
Authentication Mode	Select from "text" and "md5".
Authentication String	The authentication key for package interaction in RIPV2.
Authentication Key-chain	The authentication key-chain for package interaction in RIPV2.
Neighbor	
IP Address	Set RIP neighbor's IP address manually.
Network	
IP Address	The IP address of interface for RIP publishing.
Netmask	The netmask of interface for RIP publishing.

Table 3-2-7-4

3.2.7.4 OSPF

OSPF, short for Open Shortest Path First, is a link status based on interior gateway protocol developed by IETF.

If a router wants to run the OSPF protocol, there should be a Router ID that can be manually configured. If no Router ID configured, the system will automatically select an IP address of interface as the Router ID. The selection order is as follows:

- If a Loopback interface address is configured, then the last configured IP address of Loopback interface will be used as the Router ID;
- If no Loopback interface address is configured, the system will choose the interface with the biggest IP address as the Router ID.

Five types of packets of OSPF:

- **Hello packet**
- **DD packet** (Database Description Packet)
- **LSR packet** (Link-State Request Packet)
- **LSU packet** (Link-State Update Packet)
- **LSAck packet** (Link-Sate Acknowledgment Packet)

Neighbor and Neighboring

After OSPF router starts up, it will send out Hello Packets through the OSPF interface. Upon receipt of Hello packet, OSPF router will check the parameters defined in the packet. If it's consistent, a neighbor relationship will be formed. Not all matched sides in neighbor relationship can form the adjacency relationship. It is determined by the network type. Only when both sides successfully exchange DD packets and LSDB synchronization is achieved, the adjacency in the true sense can be formed. LSA describes the network topology around a router, LSDB describes entire network topology.

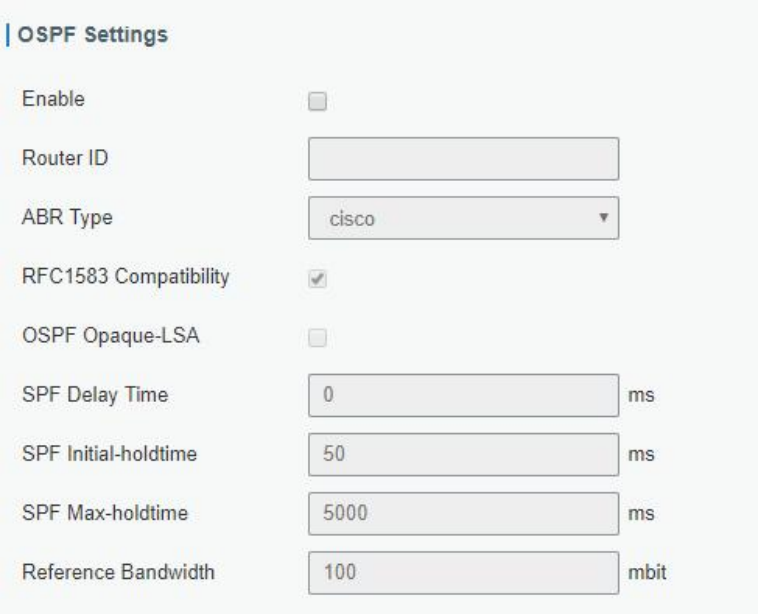


Figure 3-2-7-5

OSPF	
Item	**Description**
Enable	Enable or disable OSPF.
Router ID	Router ID (IP address) of the originating LSA.
ABR Type	Select from cisco, ibm, standard and shortcut.
RFC1583 Compatibility	Enable/Disable.
OSPF Opaque-LSA	Enable/Disable LSA: a basic communication means of the OSPF routing protocol for the Internet Protocol (IP).
SPF Delay Time	Set the delay time for OSPF SPF calculations. Range: 0-6000000, in milliseconds.
SPF Initial-holdtime	Set the initialization time of OSPF SPF. Range: 0-6000000, in milliseconds.
SPF Max-holdtime	Set the maximum time of OSPF SPF. Range: 0-6000000, in milliseconds.
Reference Bandwidth	Range: 1-4294967, in Mbit.

Table 3-2-7-5 OSPF Parameters

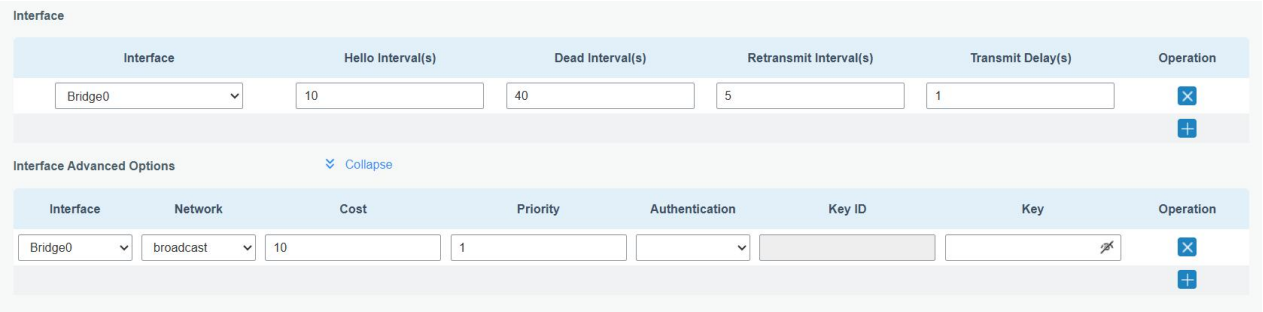


Figure 3-2-7-6

Item	Description
Interface	
Interface	Select interface from "cellular0","WAN"and "Bridge0".
Hello Interval (s)	Send interval of Hello packet. If the Hello time between two adjacent routers is different, the neighbour relationship cannot be established. Range: 1-65535.
Dead Interval (s)	Dead Time. If no Hello packet is received from the neighbours within the dead time, then the neighbour is considered failed. If dead times of two adjacent routers are different, the neighbour relationship cannot be established.
Retransmit Interval (s)	When the router notifies an LSA to its neighbour, it is required to make acknowledgement. If no acknowledgement packet is received within the retransmission interval, this LSA will be retransmitted to the neighbour. Range: 3-65535.
Transmit Delay (s)	It will take time to transmit OSPF packets on the link. So a certain delay time should be increased before transmission the aging time of LSA. This configuration needs to be further considered on the low-speed link. Range: 1-65535.
Interface Advanced Options	
Interface	Select interface.
Network	Select OSPF network type.
Cost	Set the cost of running OSPF on an interface. Range: 1-65535.
Priority	Set the OSPF priority of interface. Range: 0-255.
Authentication	Set the authentication mode that will be used by the OSPF area. Simple: a simple authentication password should be configured and confirmed again. MD5: MD5 key & password should be configured and confirmed again.
Key ID	It only takes effect when MD5 is selected. Range 1-255.
Key	The authentication key for OSPF packet interaction.

Table 3-2-7-6 OSPF Parameters

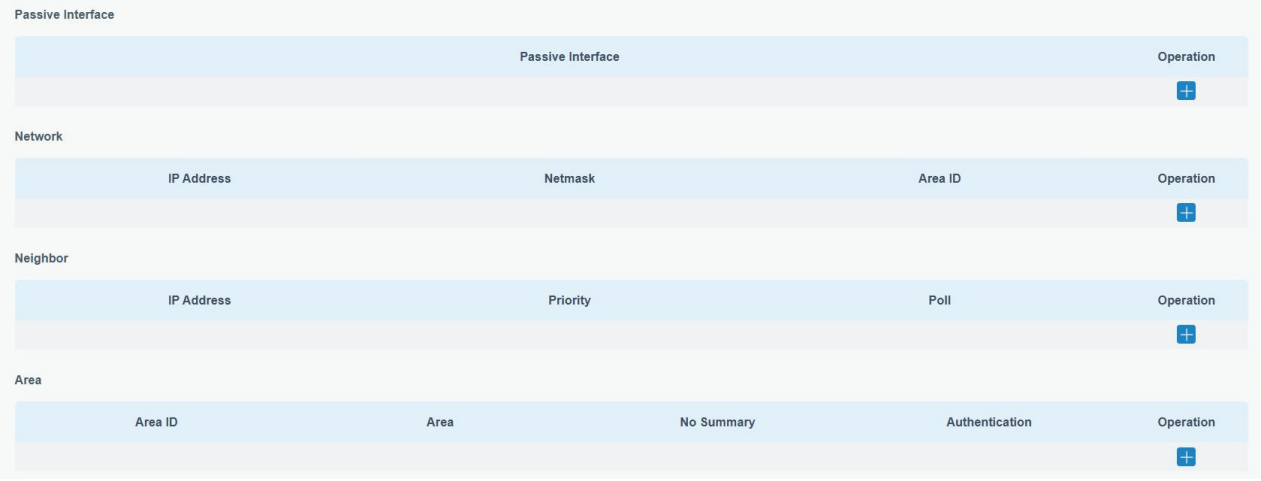


Figure 3-2-7-7

Item	Description
Passive Interface	
Passive Interface	Select interface from "cellular0", "LAN1/WAN" and "Bridge0".
Network	
IP Address	The IP address of local network.
Netmask	The netmask of local network.
Area ID	The area ID of original LSA's router.
Area	
Area ID	Set the ID of the OSPF area (IP address).
Area	Select from "Stub" and "NSSA". The backbone area (area ID 0.0.0.0) cannot be set as "Stub" or "NSSA".
No Summary	Forbid route summarization.
Authentication	Select authentication from "simple" and "md5".

Table 3-2--7-7 OSPF Parameters

Figure 3-2-7-8

Area Advanced Options	
Item	**Description**
Area Range	
Area ID	The area ID of the interface when it runs OSPF (IP address).
IP Address	Set the IP address.
Netmask	Set the netmask.
No Advertise	Forbid the route information to be advertised among different areas.
Cost	Range: 0-16777215
Area Filter	
Area ID	Select an Area ID for Area Filter.
Filter Type	Select from "import", "export", "filter-in", and "filter-out".
ACL Name	Enter an ACL name which is set on **Routing > Routing Filtering** webpage.
Area Virtual Link	
Area ID	Set the ID number of OSPF area.
ABR Address	ABR is the router connected to multiple outer areas.
Authentication	Select from "simple" and "md5".
Key ID	It only takes effect when MD5 is selected. Range 1-15.

Key	The authentication key for OSPF packet interaction.
Hello Interval	Set the interval time for sending Hello packets through the interface. Range: 1-65535.
Dead Interval	The dead interval time for sending Hello packets through the interface. Range: 1-65535.
Retransmit Interval	The retransmission interval time for re-sending LSA. Range: 1-65535.
Transmit Delay	The delay time for LSA transmission. Range: 1-65535.

Table 3-2-7-8 OSPF Parameters

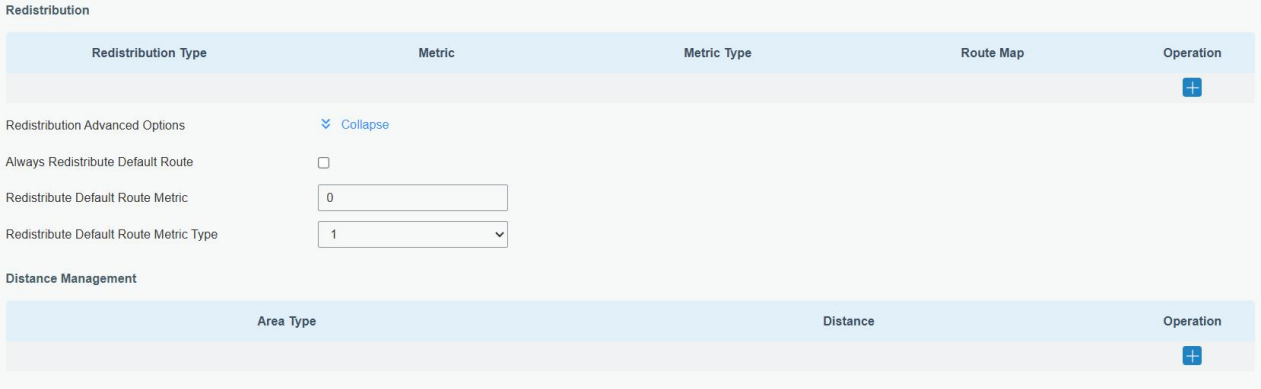


Figure 3-2-7-9

Item	Description
Redistribution	
Redistribution Type	Select from "connected", "static" and "rip".
Metric	The metric of redistribution router. Range: 0-16777214.
Metric Type	Select Metric type from "1" and "2".
Route Map	Mainly used to manage route for redistribution.
Redistribution Advanced Options	
Always Redistribute Default Route	Send redistribution default route after starting up.
Redistribute Default Route Metric	Send redistribution default route metric. Range: 0-16777214.
Redistribute Default Route Metric Type	Select from "0", "1" and "2".
Distance Management	
Area Type	Select from "intra-area", "inter-area" and "external".
Distance	Set the OSPF routing distance for area learning. Range: 1-255.

Table 3-2-7-9 OSPF Parameters

3.2.7.5 Routing Filtering

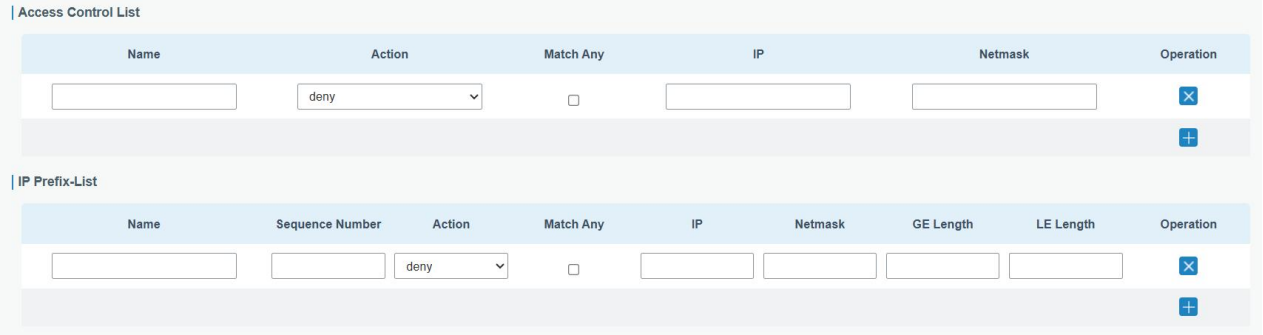


Figure 3-2-7-10

Routing Filtering	
Item	**Description**
Access Control List	
Name	User-defined name, need to start with a letter. Only letters, digits and underline (_) are allowed.
Action	Select from "permit" and "deny".
Match Any	No need to set IP address and subnet mask.
IP Address	User-defined.
Netmask	User-defined.
IP Prefix-List	
Name	User-defined name, need to start with a letter. Only letters, digits and underline (_) are allowed.
Sequence Number	A prefix name list can be matched with multiple rules. One rule is matched with one sequence number. Range: 1-4294967295.
Action	Select from "permit" and "deny".
Match Any	No need to set IP address, subnet mask, FE Length, and LE Length.
IP Address	User-defined.
Netmask	User-defined.
FE Length	Specify the minimum number of mask bits that must be matched. Range: 0-32.
LE Length	Specify the maximum number of mask bits that must be matched. Range: 0-32.

Table 3-2-7-10 Routing Filtering Parameters

3.2.8 VRRP

The Virtual Router Redundancy Protocol (VRRP) is a computer networking protocol that provides automatic assignment of available Internet Protocol (IP) routers for participating hosts. This increases the availability and reliability of routing paths via automatic default gateway selections in an IP sub-network.

Increasing the number of exit gateway is a common method for improving system reliability. VRRP adds a group of routers that undertake gateway function into a backup group so as to form a virtual router. The election mechanism of VRRP will decide which router undertakes the forwarding task, and the host in LAN is only required to configure the default gateway for the virtual router.

In VRRP, routers need to be aware of failures in the virtual master router. To achieve this, the virtual

master router sends out multicast “alive” announcements to the virtual backup routers in the same VRRP group.

The VRRP router who has the highest number will become the virtual master router. The VRRP router number ranges from 1 to 255 and usually we use 255 for the highest priority and 100 for backup.

If the current virtual master router receives an announcement from a group member (Router ID) with a higher priority, then the latter will pre-empt and become the virtual master router.

VRRP has the following characteristics:

- The virtual router with an IP address is known as the Virtual IP address. For the host in LAN, it is only required to know the IP address of virtual router, and set it as the address of the next hop of the default route.
- The network Host communicates with the external network through this virtual router.
- A router will be selected from the set of routers based on its priority to undertake the gateway function. Other routers will be used as backup routers to perform the duties of gateway for the gateway router in the case of any malfunction, so as to guarantee uninterrupted communication between the host and external network.

When interface connected with the uplink is at the state of Down or Removed, the router actively lowers its priority so that priority of other routers in the backup group will be higher. Thus the router with the highest priority becomes the gateway for the transmission task.

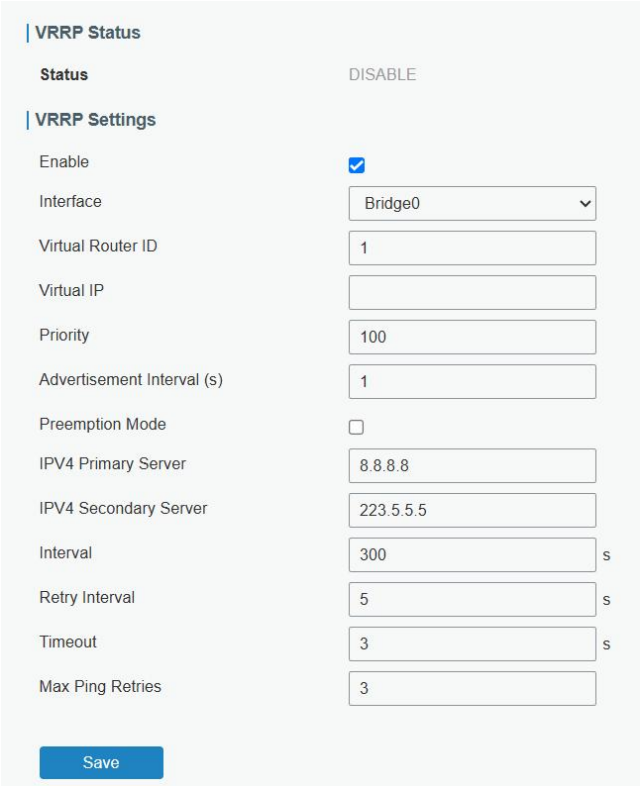


Figure 3-2-8-1

VRRP		
Item	**Description**	**Default**
Enable	Enable or disable VRRP.	Disable
Interface	Select the interface of Virtual Router.	None
Virtual Router ID	User-defined Virtual Router ID. Range: 1-255.	None
Virtual IP	Set the IP address of Virtual Router.	None

Priority	The VRRP priority range is 1-254 (a bigger number indicates a higher priority). The router with higher priority will be more likely to become the gateway router.	100
Advertisement Interval (s)	Heartbeat package transmission time interval between routers in the virtual ip group. Range: 1-255.	1
Preemption Mode	If the router works in the preemption mode, once it finds that its own priority is higher than that of the current gateway router, it will send VRRP notification package, resulting in re-election of gateway router and eventually replacing the original gateway router. Accordingly, the original gateway router will become a Backup router.	Disable
IPV4 Primary Server	The router will send ICMP packet to the IP address or hostn ame to determine whether the Internet connection is still av ailable or not.	8.8.8.8
IPV4 Secondary Server	The router will try to ping the secondary server name if prim ary server is not available.	223.5.5.5
Interval	Time interval (in seconds) between two Pings.	300
Retry Interval	Set the ping retry interval. When ping failed, the router will pi ng again every retry interval.	5
Timeout	The maximum amount of time the router will wait for a resp onse to a ping request. If it does not receive a response for the amount of time defined in this field, the ping request will be considered as failure.	3
Max Ping Retries	The retry times of the router sending ping request until dete rmining that the connection has failed.	3

Table 3-2-8-1 VRRP Parameters

Related Configuration Example

VRRP Application Example

3.2.9 DDNS

Dynamic DNS (DDNS) is a method that automatically updates a name server in the Domain Name System, which allows user to alias a dynamic IP address to a static domain name.

DDNS serves as a client tool and needs to coordinate with DDNS server. Before starting configuration, user shall register on a website of proper domain name provider and apply for a domain name.

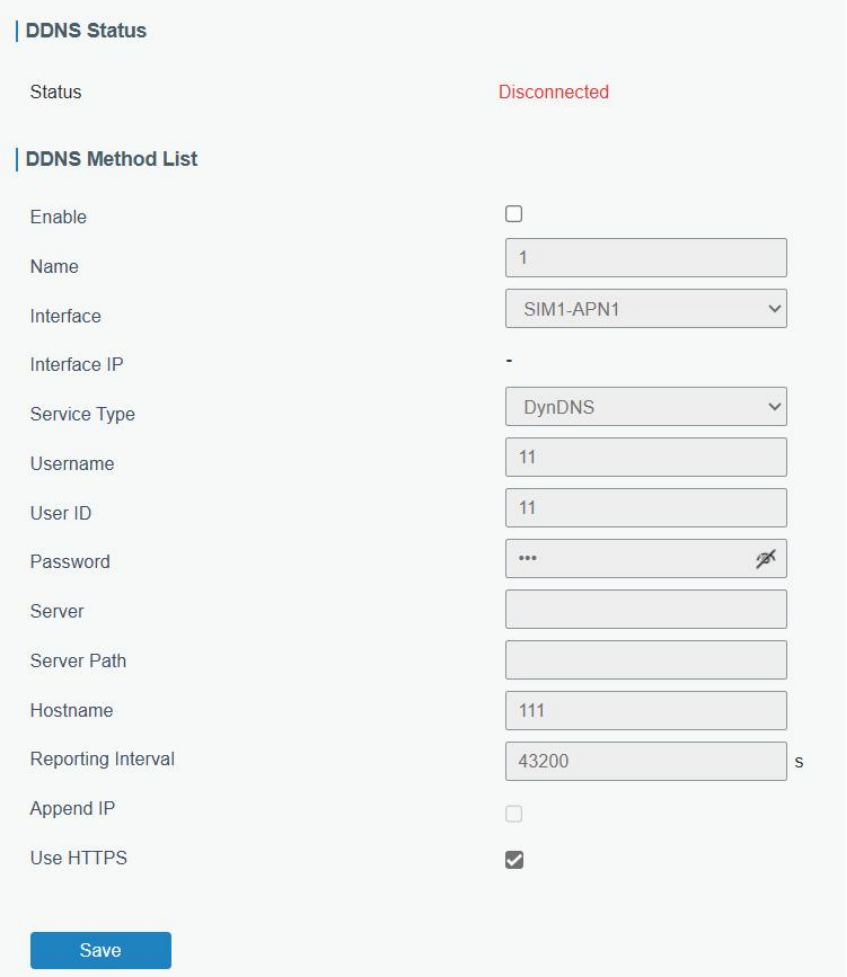


Figure 3-2-9-1

DDNS	
Item	**Description**
Enable	Enable/disable DDNS.
Name	Give the DDNS a descriptive name.
Interface	Set interface bundled with the DDNS.
Interface IP	Display the IP address of the selected interface.
Service Type	Select the DDNS service provider.
Username	Enter the username for DDNS register.
User ID	Enter User ID of the custom DDNS server.
Password	Enter the password for DDNS register.
Server	Enter the name of DDNS server.
Server Path	By default the hostname is appended to the path.
Hostname	Enter the hostname for DDNS.
Reporting Interval	Set the IP reporting interval for the DDNS.
Append IP	Append your current IP to the DDNS server update path.
Use HTTPS	Enable HTTPS for some DDNS providers.

Table 3-2-9-1 DDNS Parameters

3.3 System

3.3.1 General Settings

3.3.1.1 General

General settings include system info and HTTPS certificates.

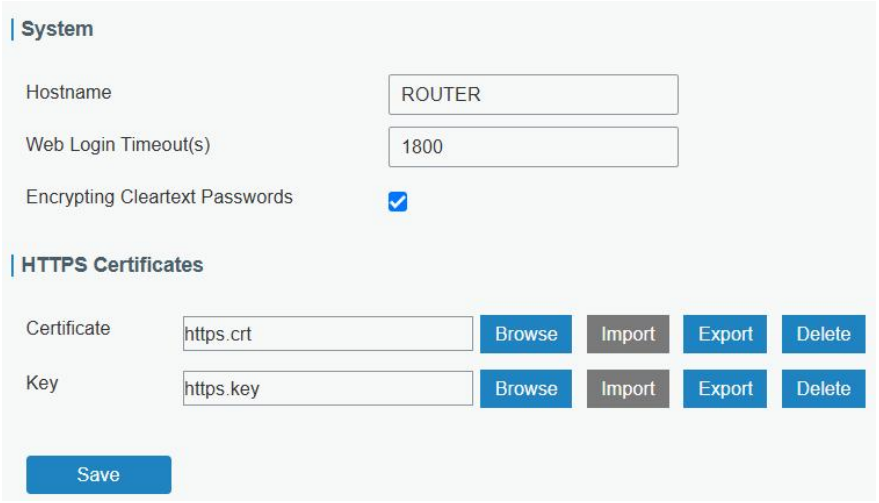


Figure 3-3-1-1

General		
Item	**Description**	**Default**
System		
Hostname	User-defined router name, needs to start with a letter.	ROUTER
Web Login Timeout (s)	You need to log in again if it times out. Range: 100-3600.	1800
Encrypting Cleartext Passwords	This function will encrypt all of cleartext passwords into ciphertext passwords.	Enable
HTTPS Certificates		
Certificate	Click "Browse" button, choose certificate file on the PC, and then click "Import" button to upload the file into router. Click "Export" button will export the file to the PC. Click "Delete" button will delete the file.	--
Key	Click "Browse" button, choose key file on the PC, and then click "Import" button to upload the file into router. Click "Export" button will export file to the PC. Click "Delete" button will delete the file.	--

Table 3-3-1-1 General Setting Parameters

3.3.1.2 System Time

This section explains how to set the system time including time zone and time synchronization type.

Note: to ensure that the router runs with the correct time, it's recommended that you set the system time when configuring the router.

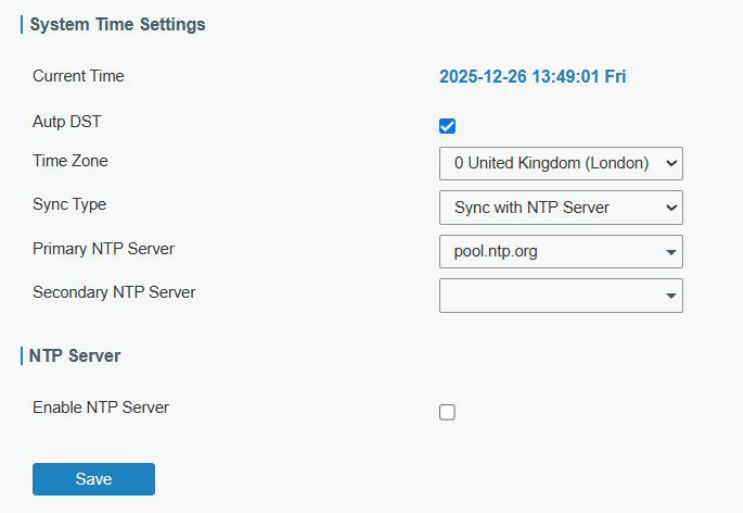


Figure 3-3-1-2

System Time	
Item	**Description**
Current Time	Show the current system time.
Autp DST	Enable to use the daylight saving time.
Time Zone	Click the drop down list to select the time zone you are in.
Sync Type	Click the drop down list to select the time synchronization type. **Sync with Browser:** Synchronize time with browser. **Sync with NTP Server:** Synchronize time with NTP Server. **Set up Manually:** configure the time manually. **GPS Time Synchronization:** Synchronize time with GPS per hour. This is only applicable with GPS version and ensure that GPS is enabled on **Service > GPS > GPS**. **Sync with Cellular Operator:** Synchronize time with cellular operator. This only works when the device has registered to cellular network.
Sync with Browser	Synchronize time with browser.
Browser Time	Show the current time of browser.
Set up Manually	Manually configure the system time.
GPS Time Synchronization	Synchronize time with GPS.
Primary NTP Server	Enter primary NTP Server's IP address or domain name.
Secondary NTP Server	Enter secondary NTP Server's IP address or domain name.
NTP Server	
Enable NTP Server	NTP client on the network can achieve time synchronization with router after this option is checked.

Table 3-3-1-2 System Time Parameters

3.3.1.3 Email

SMTP, short for Simple Mail Transfer Protocol, is a TCP/IP protocol used in sending and receiving e-mail. This section describes how to configure email settings and add email groups for alarms and events.

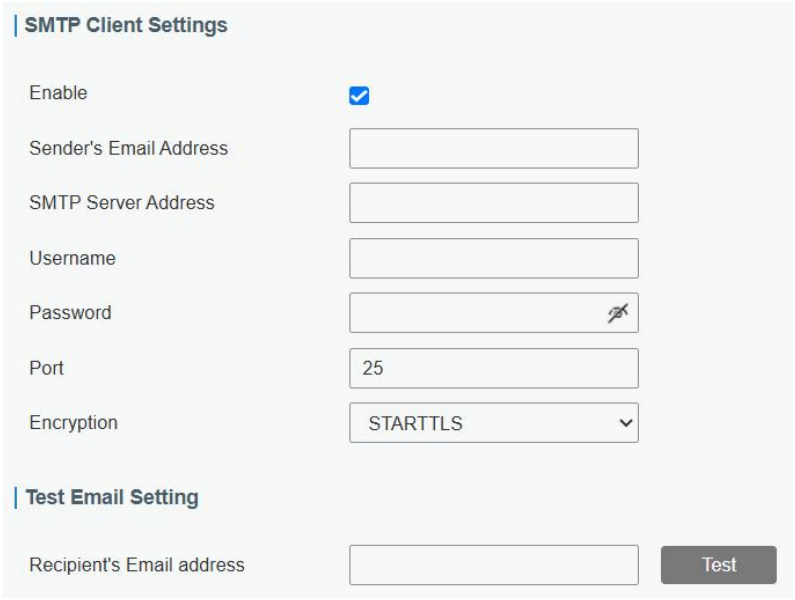


Figure 3-3-1-3

SMTP Client Settings	
Item	**Description**
Enable	Enable or disable SMTP client function.
Sender's Email Address	Enter the sender's email account.
SMTP Server Address	Enter SMTP server's domain name.
Username	Enter the sender's email username.
Password	Enter the sender's email password.
Port	Enter SMTP server port. Range: 1-65535.
Encryption	Select from: None, TLS/SSL, STARTTLS. **None:** No encryption. The default port is 25. **STARTTLS:** STARTTLS is a way to take an existing insecure connection and upgrade it to a secure connection by using SSL/TLS. The default port is 587. **TLS/SSL:** SSL and TLS both provide a way to encrypt a communication channel between two computers (e.g. your computer and our server). TLS is the successor to SSL and the terms SSL and TLS are used interchangeably unless you're referring to a specific version of the protocol.The default port is 465.
Test Email Setting	
Recipient's Email address	Enter the recipient's email account. Click **Test**, the test email will be sent to this address.

Table 3-3-1-3 SMTP Setting

Figure 3-3-1-4

Item	Description
Email List	
Recipient's Email Address	Enter the recipient's Email address.
Description	The description of the Email address.
Email Group List	
Group ID	Set number for email group. Range: 1-100.
Description	The description of the Email group.
Recipient's Email address	Select the Email addresses.

Table 3-3-1-4 Email Settings

Related Topics

DI Setting

Events Setting

3.3.1.4 Storage

You can view Micro SD card information on this page.

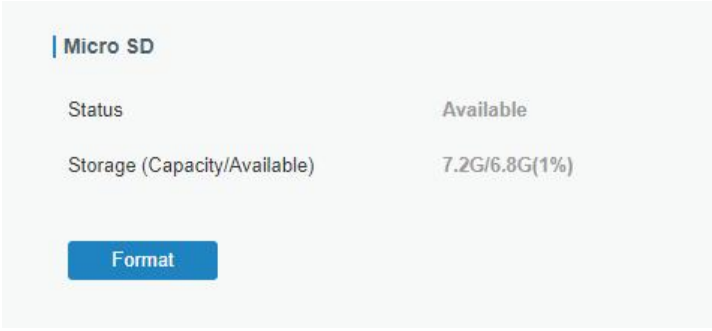


Figure 3-3-1-5

Storage	
Item	**Description**
Status	Show the status of Micro SD card, such as “Available” or “Not Inserted”.
Storage (Capacity/Available)	The total capacity of the Micro SD Card.
Format	Format the Micro SD card.

Table 3-3-1-5 Storage Information

3.3.2 Phone&SMS

3.3.2.1 Phone

Phone settings involve in call/SMS trigger, SMS control and SMS alarm for events.

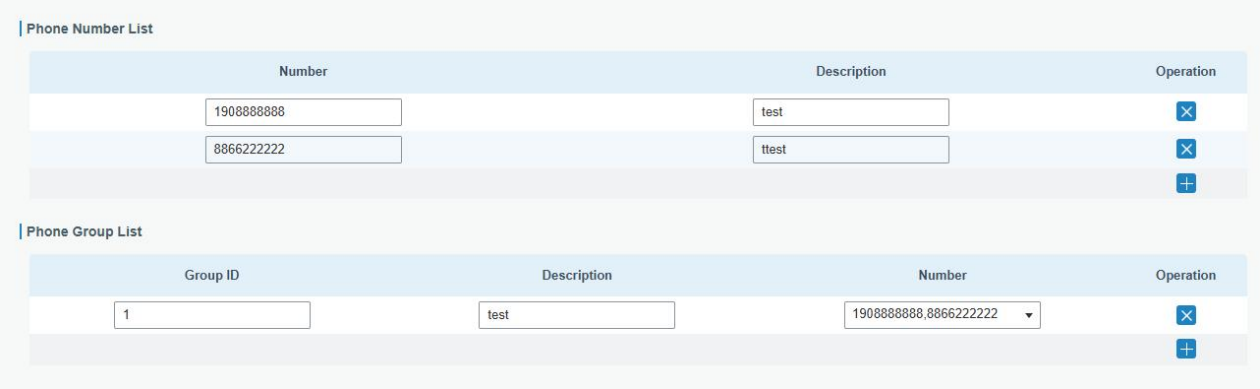


Figure 3-3-2-1

Phone	
Item	**Description**
Phone Number List	
Number	Enter the telephone number. Digits, "+" and "-" are allowed.
Description	The description of the telephone number.
Phone Group List	
Group ID	Set number for phone group. Range: 1-100.
Description	The description of the phone group.
Number	Select the phone numbers.

Table 3-3-2-1 Phone Settings

Related Topic

Connect on Demand

3.3.2.2 SMS

SMS settings involve in remote SMS control, sending SMS and SMS receiving and sending status. Ensure the SMS center number is typed on **Network > Interface > Cellular** page before using SMS features.

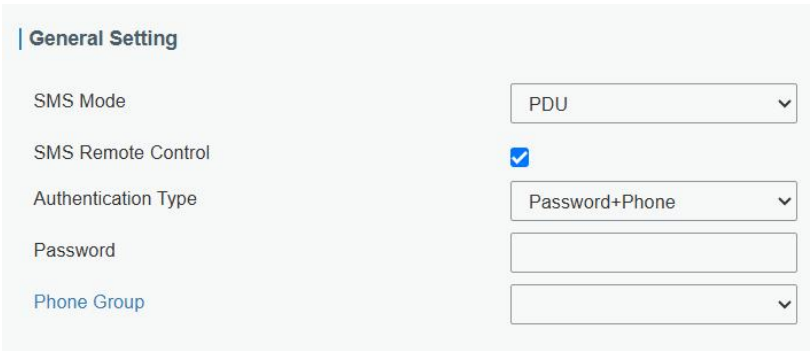


Figure 3-3-2-2

SMS Settings	
Item	**Description**
SMS Mode	Select SMS mode: **Text:** Pure text mode, mainly used in Europe and America. Technically, it can also be used to send Short Messages in Chinese. When CLI commands will be sent to control the router, Text mode is recommended to choose. **PDU:** It;s the default encoding Mode for mobile phones, which conform to all mobile phones SMS format and can use any character.
SMS Remote Control	Enable/disable SMS Remote Control to send SMS to control the router.
Authentication Type	You can choose “phone number” or ”password + phone number”. Phone number: only the phone numbers on phone groups support remote control. Password + phone number: only the phone numbers on phone groups support remote control; besides, control SMS should be sent as format password+”;”+command content.
Password	Set password for authentication.
Phone Group	Select the Phone group which used for remote control. User can click the Phone Group and set phone number.

Table 3-3-2-2 SMS Remote Control Parameters

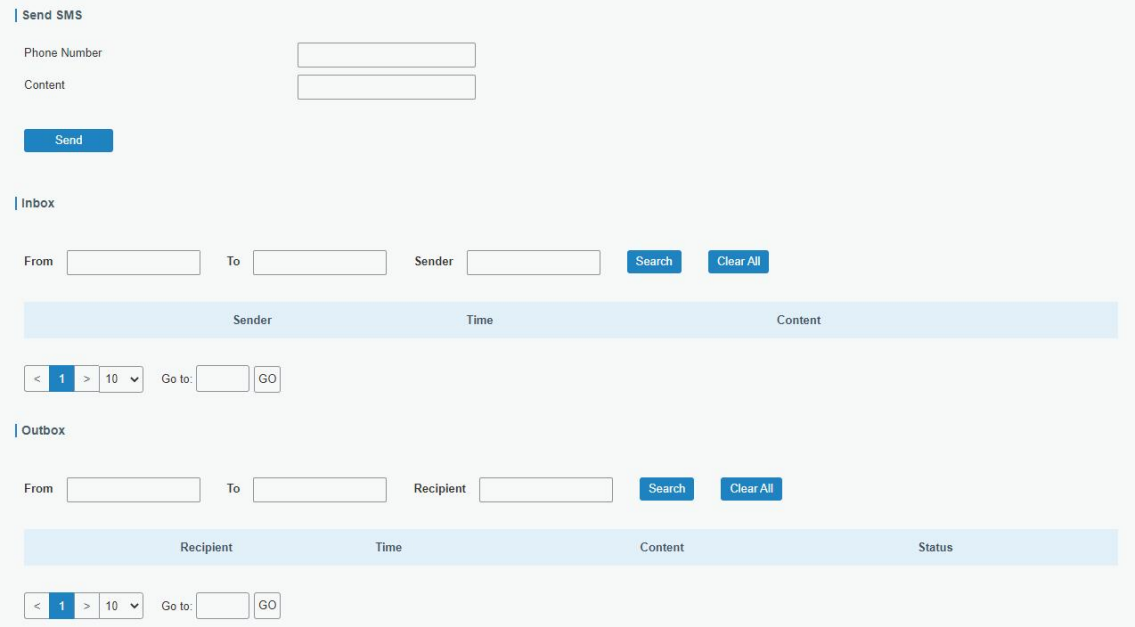


Figure 3-3-2-3

SMS	
Item	**Description**
Send SMS	
Phone Number	Enter the number to receive the SMS.
Content	SMS content.

Inbox/Outbox	
Sender	SMS sender from outside.
Recipient	SMS recipient which UR32 send to.
From	Select the start date.
To	Select the end date.
Search	Search for SMS record.
Clear All	Clear all SMS records in web GUI.

Table 3-3-2-3 SMS Settings

3.3.3 User Management

3.3.3.1 Account

Here you can change the login username and password of the administrator.

Note: it is strongly recommended that you modify them for the sake of security.

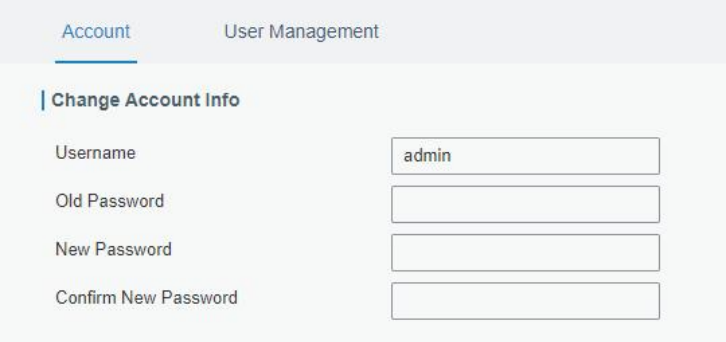


Figure 3-3-3-1

Account	
Item	**Description**
Username	Enter a new username. You can use characters such as a-z, 0-9, "_", "-". The first character can't be a digit.
Old Password	Enter the old password.
New Password	Enter a new password. You can use any ASCII characters except blank. The password must contain at least one letter and one number, with a length of 5-31 characters.
Confirm New Password	Enter the new password again.

Table 3-3-3-1 Account Settings

3.3.3.2 User Management

This section describes how to create common user accounts. The common user permission includes Read-Only and Read-Write.

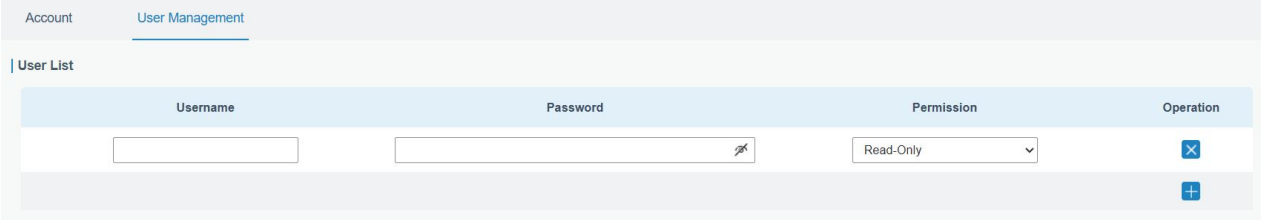


Figure 3-3-3-2

User Management	
Item	**Description**
Username	Enter a new username. You can use characters such as a-z, 0-9, "_", "-". The first character can't be a digit.
Password	Set password. You can use any ASCII characters except blank. The password must contain at least one letter and one number, with a length of 5-31 characters.
Permission	Select user permission from "Read-Only" and "Read-Write". **Read-Only:** users can only view the configuration of router in this level. **Read-Write:** users can view and set the configuration of router in this level.

Table 3-3-3-2 User Management

3.3.4 AAA

AAA access control is used for visitors control and the available corresponding services once access is allowed. It adopts the same method to configure three independent safety functions. It provides modularization methods for following services:

- Authentication: verify if the user is qualified to access to the network.
- Authorization: authorize related services available for the user.
- Charging: record the utilization of network resources.

3.3.4.1 Radius

Using UDP for its transport, Radius is generally applied in various network environments with higher requirements of security and permission of remote user access.

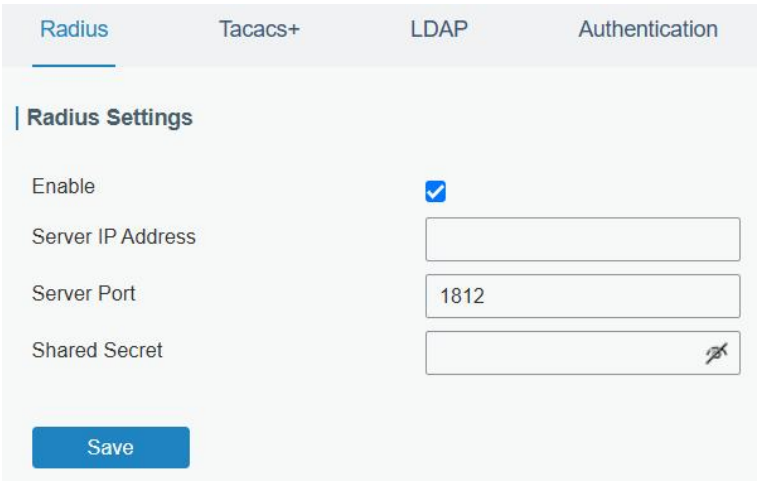


Figure 3-3-4-1

Radius	
Item	**Description**
Enable	Enable or disable Radius.
Server IP Address	Fill in the Radius server IP address/domain name.
Server Port	Fill in the Radius server port. Range: 1-65535.
Key	Fill in the key consistent with that of Radius server in order to get connected with Radius server.

Table 3-3-4-1 Radius Parameters

3.3.4.2 TACACS+

Using TCP for its transport, TACACS+ is mainly used for authentication, authorization and charging of the access users and terminal users by adopting PPP and VPDN.

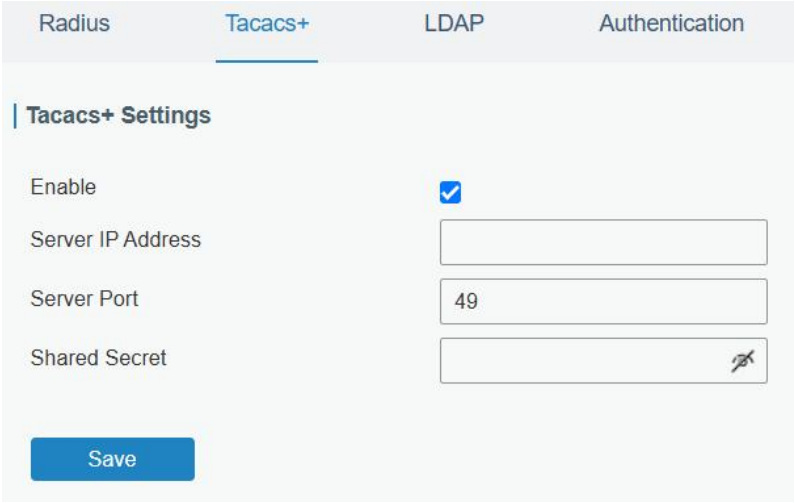


Figure 3-3-4-2

TACACS+	
Item	**Description**
Enable	Enable or disable TACACS+.
Server IP Address	Fill in the TACACS+ server IP address/domain name.
Server Port	Fill in the TACACS+ server port. Range: 1-65535.
Key	Fill in the key consistent with that of TACACS+ server in order to get connected with TACACS+ server.

Table 3-3-4-2 TACACS+ Parameters

3.3.4.3 LDAP

A common usage of LDAP is to provide a central place to store usernames and passwords. This allows many different applications and services to connect the LDAP server to validate users.

LDAP is based on a simpler subset of the standards contained within the X.500 standard. Because of this relationship, LDAP is sometimes called X.500-lite as well.

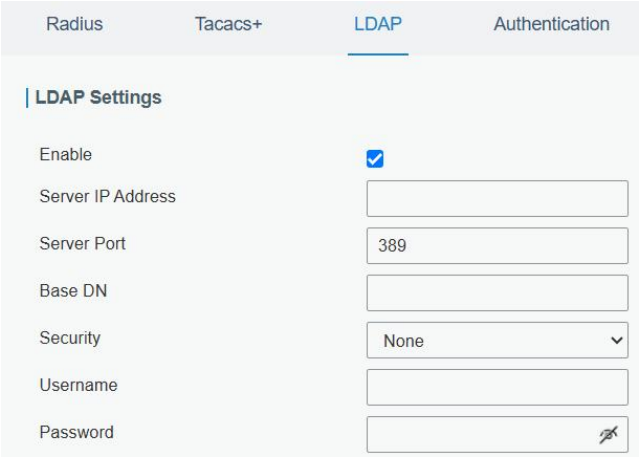


Figure 3-3-4-3

LDAP	
Item	**Description**
Enable	Enable or Disable LDAP.
Server IP Address	Fill in the LDAP server's IP address/domain name. The maximum count is 10.
Server Port	Fill in the LDAP server's port. Range: 1-65535
Base DN	The top of LDAP directory tree.
Security	Select secure method from "None", "StartTLS" and "SSL".
Username	Enter the username to access the server.
Password	Enter the password to access the server.

Table 3-3-5-3 LDAP Parameters

3.3.4.4 Authentication

AAA supports the following authentication ways:

- None: uses no authentication, generally not recommended.
- Local: uses the local username database for authentication.
  - Advantages: rapidness, cost reduction.
  - Disadvantages: storage capacity limited by hardware.
- Remote: has user's information stored on authentication server. Radius, TACACS+ and LDAP supported for remote authentication.

When radius, TACACS+, and local are configured at the same time, the priority level is: 1 >2 >3.

Figure 3-3-4-4

Authentication	
Item	**Description**
Console	Select authentication for Console access.
Web	Select authentication for Web access.
Telnet	Select authentication for Telnet access.
SSH	Select authentication for SSH access.

Table 3-3-4-4 Authentication Parameters

3.3.5 Device Management

3.3.5.1 Auto Provision

When Auto Provision is enabled and the device is connected to Internet, the device will receive the configuration profile to achieve initial configuration by Milesight Development Platform. This feature will work even the device does not configure to connect Milesight Development Platform.

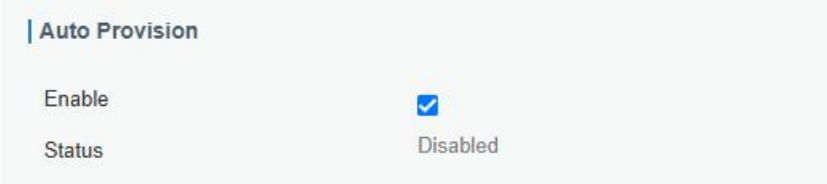


Figure 3-3-5-1

3.3.5.2 Device Management

You can choose which platform you want to connect on this page so as to manage the router centrally and remotely: Milesight DeviceHub, Milesight DeviceHub 2.0, and Milesight Development Platform. For more details please refer to corresponding platform manuals.

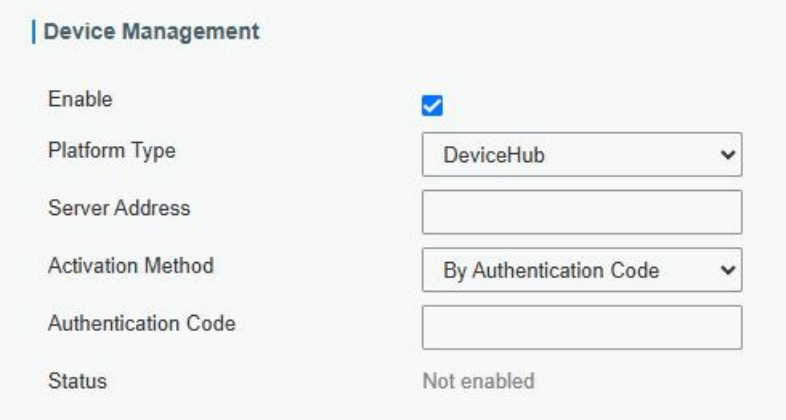


Figure 3-3-5-2

Device Management	
Item	**Description**
Enable	Enable or disable to connect router to management platform.
Platform Type	DeviceHub, DeviceHub 2.0, and Milesight Development Platform are optional.
Status	Show the connection status between the router and the platform.
DeviceHub	
Server Address	IP address or domain of the device management server.
Activation Method	Select activation method to connect the router to the DeviceHub server, options are "By Authentication Code" and

	"By Account name".
Authentication Code	Fill in the authentication code generated from the DeviceHub.
Account name	Fill in the registered DeviceHub account (email) and password.
Password	
DeviceHub 2.0	
Server Address	IP address or domain of the device management server.

Table 3-3-5-1

3.3.5.3 Milesight VPN

You can connect the device to the Milesight VPN on this page so as to manage the router and connected devices centrally and remotely. For more details please refer to ***MilesightVPN User Guide***.

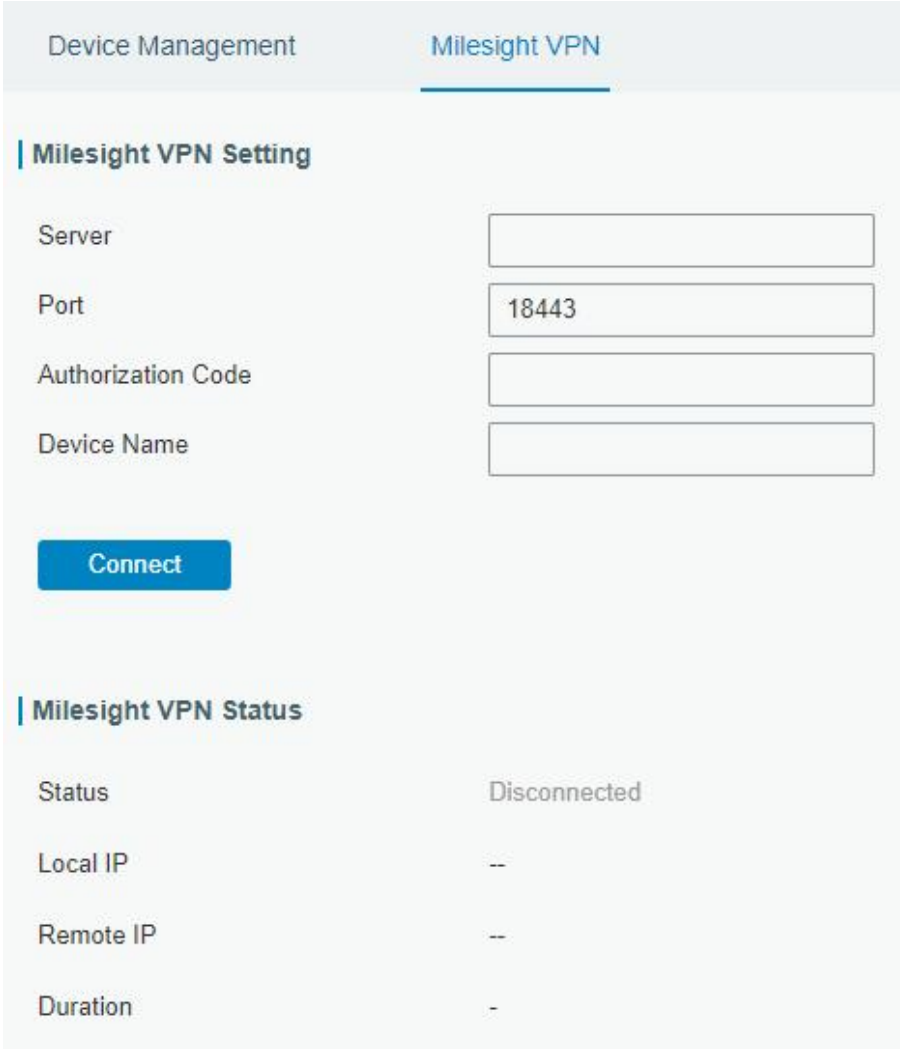


Figure 3-3-5-3

Milesight VPN	
Item	**Description**
Milesight VPN Settings	
Server	Enter the IP address or domain name of Milesight VPN.

Port	Enter the HTTPS port number.
Authorization code	Enter the authorization code which generated by Milesight VPN.
Device Name	Enter the name of the device.
Milesight VPN Status	
Status	Show the connection information about whether the router is connected to the Milesight VPN.
Local IP	Show the virtual IP of the router.
Remote IP	Show the virtual IP of the Milesight VPN.
Duration	Show the information on how long the router has been connected to the Milesight VPN.

Table 3-3-5-2

3.3.6 Events

Event feature is capable of sending alerts by Email when certain system events occur.

3.3.6.1 Events

You can view alarm messages on this page.

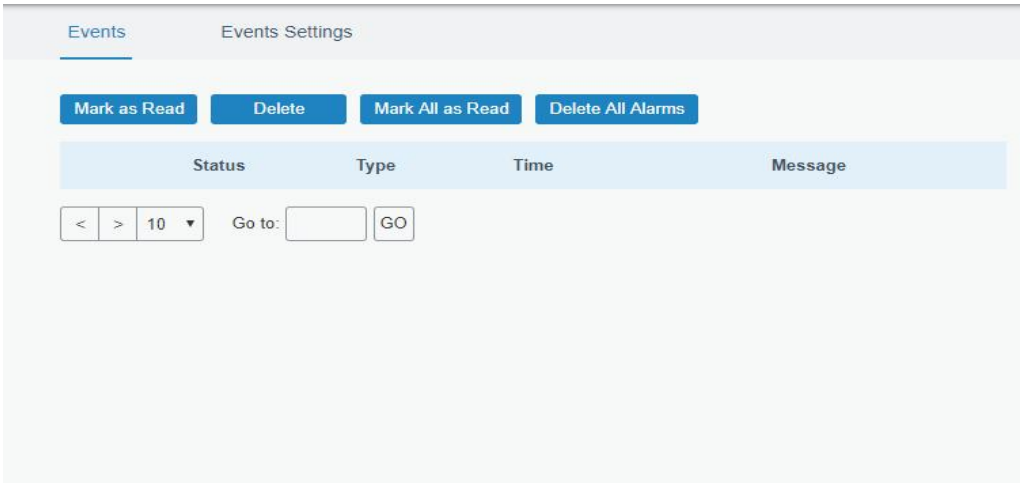


Figure 3-3-6-1

Events	
Item	**Description**
Mark as Read	Mark the selected event alarm as read.
Delete	Delete the selected event alarm.
Mark All as Read	Mark all event alarms as read.
Delete All Alarms	Delete all event alarms.
Status	Show the reading status of the event alarms, such as “Read” and “Unread”.
Type	Show the event type that should be alarmed.
Time	Show the alarm time.
Message	Show the alarm content.

Table 3-3-6-1 Events Parameters

3.3.6.2 Events Settings

In this section, you can decide what events to record and whether you want to receive email and SMS notifications when any change occurs.

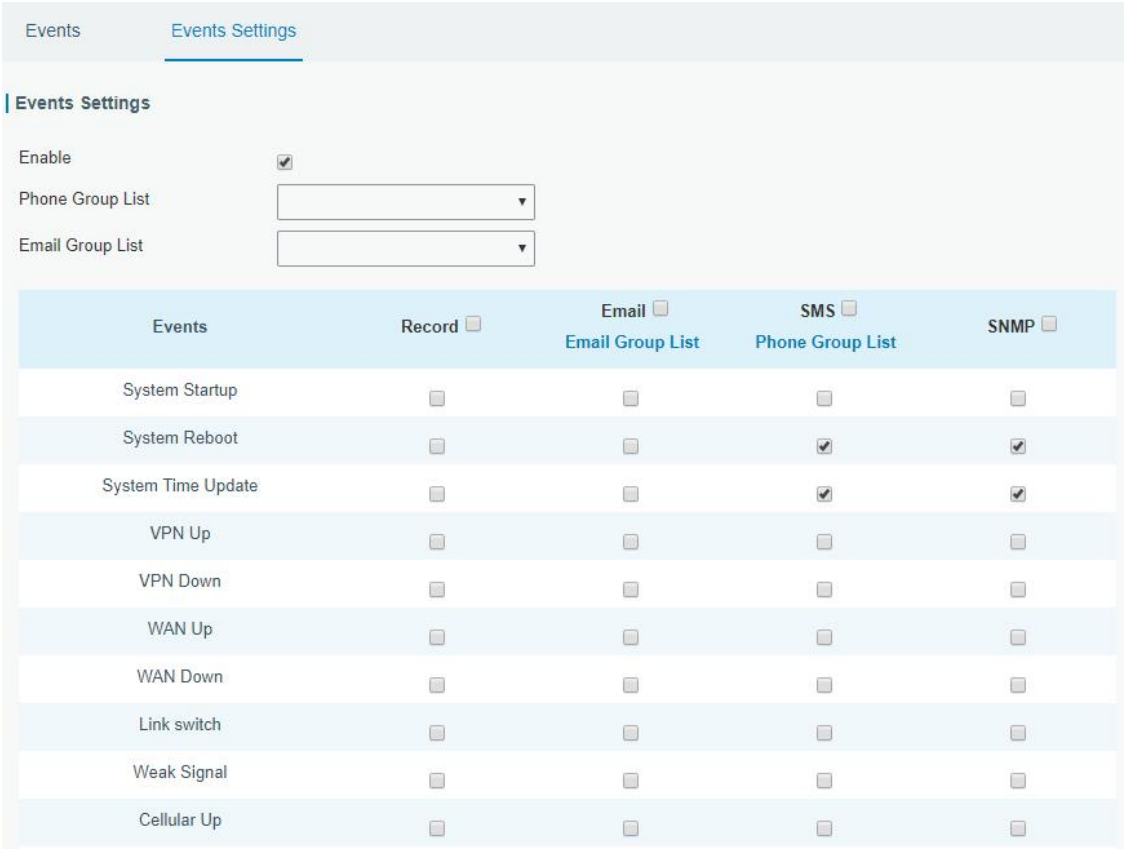


Figure 3-3-6-2

Figure 3-3-6-3

Event Settings	
Item	**Description**
Enable	Check to enable "Events Settings".
Phone Group List	Select phone group to receive SMS alarm.
Email Group List	Select email group to receive alarm.
Record	The relevant content of event alarm will be recorded on "Event" page if this option is checked.

Email	The relevant content of event alarm will be sent out via email if this option is checked.
Email Setting	Click and you will be redirected to the page "Email" to configure email group list.
SMS	The relevant content of event alarm will be sent out via SMS if this option is checked.
SMS Setting	Click and you will be redirected to the page of "Phone" to configure phone group list.
VPN Up	VPN is connected.
VPN Down	VPN is disconnected.
WAN Up	Ethernet cable is connected to WAN port.
WAN Down	Ethernet cable is disconnected to WAN port.
Link Switch	Switch to use other interface for Internet access.
Weak Signal	The signal level of cellular is low (RSSI < 11 or ≥ 99).
Cellular Up	Cellular network is connected.
Cellular Down	Cellular network is disconnected.
Cellular Data Stats Clear	Zero out the data usage of the main SIM card.
Cellular Data Traffic is running out	The main SIM card is reaching the data usage limit.
Cellular Data Traffic Over Flow	The main SIM card has exceeded the data usage plan.
WLAN Up(AP)	The WLAN(AP) is enabled.
WLAN Down(AP)	The WLAN(AP) has stopped working.
WLAN Up(Client)	The WLAN(Client) is enabled.
WLAN Down(Client)	The WLAN(Client) has stopped working.

Table 3-3-6-2 Events Parameters

Related Topics

Email Setting

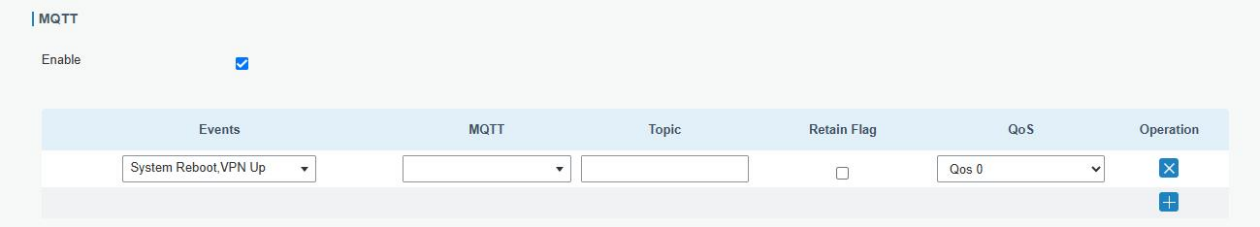


Figure 3-3-6-4

MQTT	
Item	**Description**
Enable	If enabled, MQTT forwarding is performed when an event is triggered.
Events	Select the type of event that needs to be MQTT forwarded.
MQTT	Select the MQTT connection used for forwarding the current event type.

Topic	Define the topic name of the forwarding event, which is used by the router to forward data when the event is triggered.
Retain Flag	Enable to set the latest message of this topic as retain message.
QoS	**QoS 0** – Only Once This is the fastest method and requires only 1 message. It is also the most unreliable transfer mode. **QoS 1** – At Least Once This level guarantees that the message will be delivered at least once, but may be delivered more than once. **QoS 2** – Exactly Once QoS 2 is the highest level of service in MQTT. This level guarantees that each message is received only once by the intended recipients. QoS 2 is the safest and slowest quality of service level.

Table 3-3-6-3

3.4 Service

3.4.1 I/O

3.4.1.1 DI

This section explains how to configure monitoring condition on digital input, and take certain actions once the condition is reached.

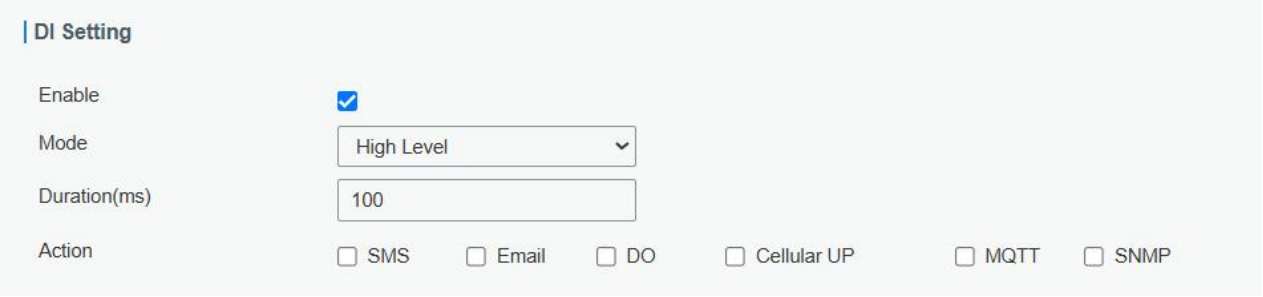


Figure 3-4-1-1

DI	
Item	**Description**
Enable	Enable or disable DI.
Mode	Options are High Level, Low Level, Counter and Level Change.
Duration (ms)	Set the duration of high/low level in digital input. Range: 1-10000.
Condition	Select the condition to trigger the counter. **Low->High:** The counter value will increase by 1 if digital input's status changes from low level to high level. **High->Low:** The counter value will increase by 1 if digital input's status changes from high level to low level.
Counter	The system will take actions accordingly when the counter value reach the preset one, and then reset the counter value to 0. Range: 1-100.
Action	Select the corresponding actions that the system will take when digital input mode meets the preset condition or duration.

	SMS: enable to send SMS alarms. **Email:** enable to send Email alarms. **DO:** control the DO status as settings on **Service > I/O > DO page**. **Cellular UP:** Trigger the router to switch from offline to register to cellular network. **MQTT**: enable to send message to MQTT broker. The MQTT connection is set up on **Service > MQTT** page. **SNMP:** enable to report DI events via SNMP Trap. The SNMP parameters is set up on **Service > SNMP** page.

Table 3-4-1-1 DI Parameters

Related Topics

DO Setting

Email Setting

Connect on Demand

3.4.1.2 DO

This section describes how to configure digital output mode.

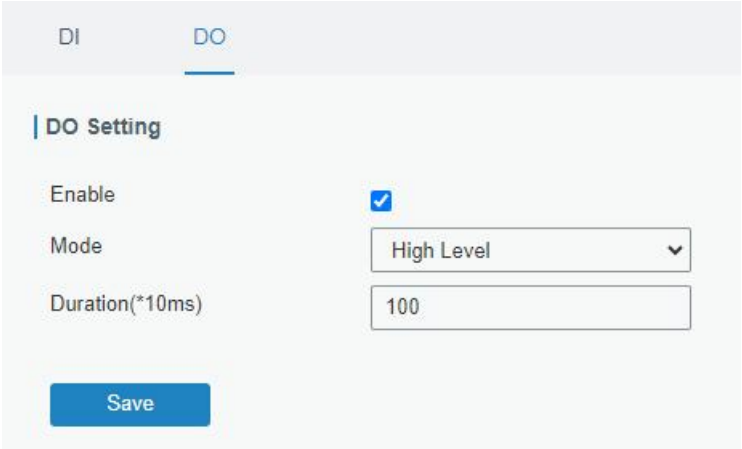


Figure 3-4-1-2

DO	
Item	**Description**
Enable	Enable or disable DO.
Mode	Select the working mode of DO. **High Level:** trigger the DO to send high level signal. **Low Level:** trigger the DO to send low level signal. **Pulse:** trigger the DO to send pulses. **Custom:** trigger the DO via SMS on the phone group.
Initial Status	Select the initial status of DO when mode is Custom or Pulse. It is also the initial status when the router restarts.
Duration (*10ms)	When mode is high level or low level, set duration of high/low level on digital output. Range: 1-10000.
Duration of High Level	Set the duration of pulse's high level. Range: 1-10000.

(*10ms)	
Duration of Low Level (*10ms)	Set the duration of pulse's low level. Range: 1-10000.
The Number of Pulse	Set the quantity of pulse. Range: 1-100.
Phone Group	Select phone group which will be used for I/O configuration. User can click the Phone Group and set phone number.

Table 3-4-1-2 DO Settings

Related Topics

DI Setting

3.4.2 Serial Port

This section explains how to configure serial port parameters to achieve communication with serial terminals, and configure work mode to achieve communication with the remote data center, so as to achieve two-way communication between serial terminals and remote data center.

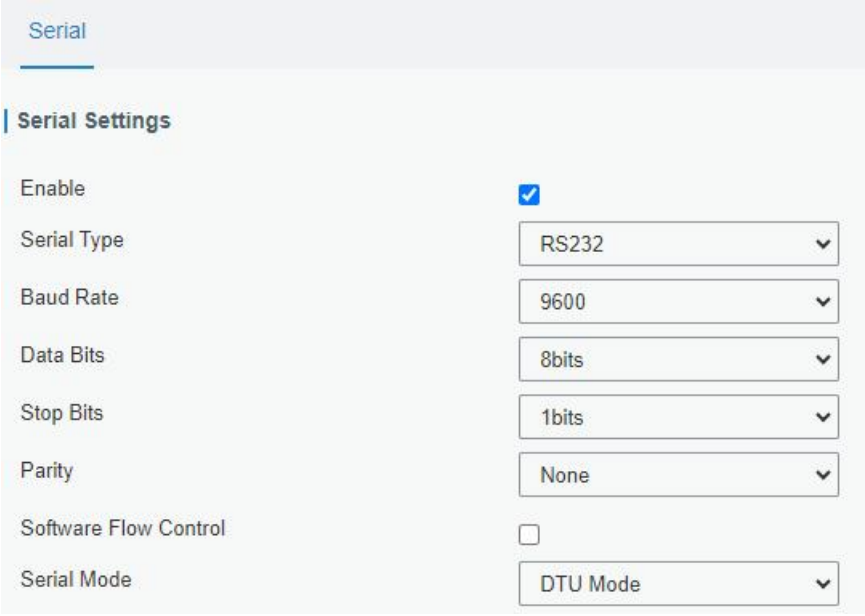


Figure 3-4-2-1

Serial Settings	
Item	**Description**
Enable	Enable or disable serial port function.
Serial Type	For normal model, it's fixed as RS232; for -485 model, select the serial type as RS232 or RS485.
Baud Rate	The range is 300-230400. Same with the baud rate of the connected terminal device.
Data Bits	Options are 8 and 7. Same with the data bits of the connected terminal device.
Stop Bits	Options are 1 and 2. Same with the stop bits of the connected terminal device.
Parity	Options are None, Odd and Even. Same with the parity of the connected

	terminal device.
Software Flow Control	Enable or disable software flow control.
Serial Mode	Select work mode of the serial port. **DTU Mode:** the serial port can establish communication with the remote server/client. **GPS:** go to **Service > GPS > GPS Serial Forwarding** to configure basic parameters to send GPS data to serial port. **Modbus Client:** go to **Service > Modbus Client** to configure basic parameters and channels. **Modbus Server:** go to **Service > Modbus Server** to configure basic parameters. **DLMS Connection:** go to **Service > DLMS** to configure basic parameters.

Table 3-4-2-1 Serial Parameters

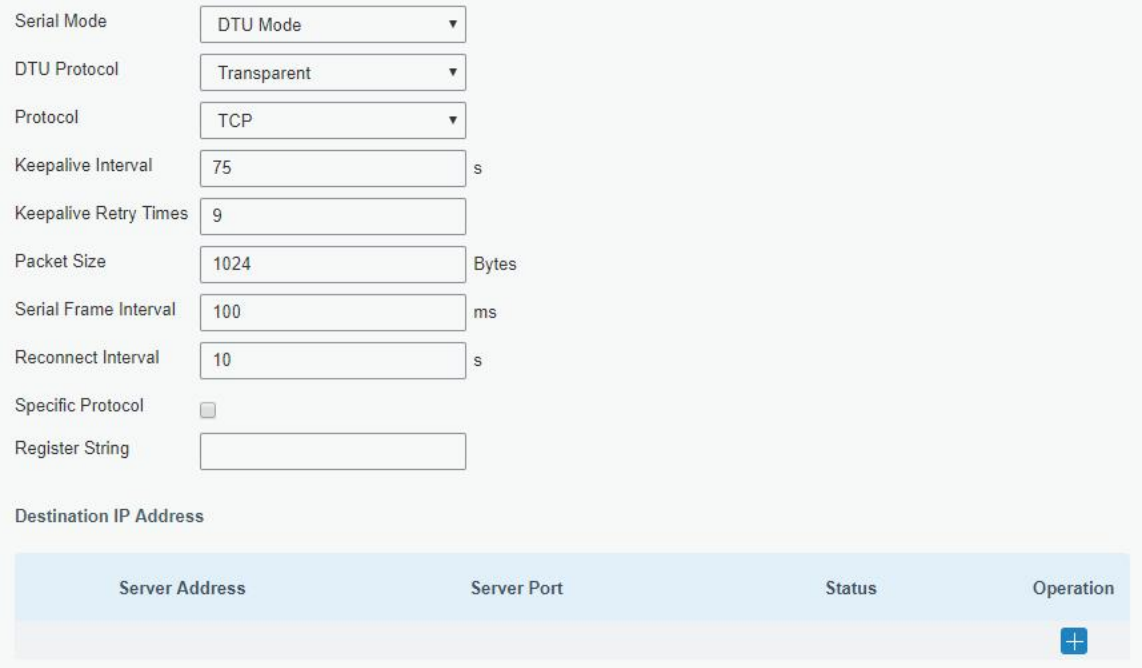


Figure 3-4-2-2

DTU Mode		
Item	**Description**	**Default**
DTU Protocol	Select from below protocols: **Transparent:** the router is used as TCP/UDP client and transmits data to server transparently. **TCP server:** the router is used as TCP server to wait for polling data. **UDP server:** the router is used as UDP server to wait for polling data. **Modbus:** the router will be used as Modbus gateway, which can achieve conversion between Modbus RTU and Modbus TCP. **MQTT:** the router will be used as MQTT client to forward data to MQTT broker or forward downlink to serial port.	--
TCP/UDP Server		

Listening port	Set the router listening port. Range: 1-65535.	502
Keepalive Interval	After TCP connection is established, client will send heartbeat packet regularly by TCP to keep alive. The interval range is 1-3600s.	75
Keepalive Retry Times	When TCP heartbeat times out, router will resend heartbeat. After it reaches the preset retry times, TCP connection will be reestablished. The retry times range is 1-16.	9
Packet Size	Set the size of the serial data frame. Packet will be sent out when preset frame size is reached. The size range is 1-1024 bytes.	1024
Serial Frame Interval	The interval that the router sends out real serial data stored in the buffer area to public network. The range is 10-65535 ms. **Note:** data will be sent out to public network when real serial data size reaches the preset packet size, even though it's within the serial frame interval.	100

Table 3-4-2-2 DTU Parameters

Item	Description	Default
Transparent		
Protocol	Select TCP or UDP protocol.	TCP
Keepalive Interval (s)	After TCP client is connected with TCP server, the client will send heartbeat packet by TCP regularly to keep alive. The interval range is 1-3600 s.	75
Keepalive Retry Times	When TCP heartbeat times out, the router will resend heartbeat. After it reaches the preset retry times, router will reconnect to TCP server. The range is 1-16.	9
Packet Size	Set the size of the serial data frame. Packet will be sent out when preset frame size is reached. The range is 1-1024 bytes.	1024
Serial Frame Interval	The interval that the router sends out real serial data stored in the buffer area to public network. The range is 10-65535 ms. **Note:** data will be sent out to public network when real serial data size reaches the preset packet size, even though it's within the serial frame interval.	100
Reconnect Interval	After connection failure, router will reconnect to the server at the preset interval. The range is 10-60 s.	10
Specific Protocol	By Specific Protocol, the router will be able to connect to the TCP2COM software.	--
Heartbeat Interval	By Specific Protocol, the router will send heartbeat packet to the server regularly to keep alive. The interval range is 1-3600 s.	30
ID	Define unique ID of each router. No longer than 63 characters without space character.	--
Register String	Define register string for connection with the server.	Null
Server Address	Fill in the TCP or UDP server address (IP/domain name).	Null
Server Port	Fill in the TCP or UDP server port. Range: 1-65535.	Null
Status	Show the connection status between the router and the server.	--
Modbus		

Local Port	Set the router listening port. Range: 1-65535.	502
Maximum TCP Clients	Specify the maximum number of TCP clients allowed to connect th e router which act as a TCP server.	32
Connection Timeout	If the TCP server does not receive any data from the slave device w ithin the connection timeout period, the TCP connection will be bro ken.	60
Reading Interval	Set the interval for reading remote channels. When a read cycle end s, the new read cycle begins until this interval expires. If it is set to 0, the device will restart the new read cycle after all channels have been read.	100
Response Timeout	Set the maximum response time that the router waits for the respo nse to the command. If the device does not get a response after th e maximum response time, it's determined that the command has ti med out.	3000
Maximum Retries	Set the maximum retry times after it fails to read.	3
MQTT		
Packet Size	Set the size of the serial data frame. Packet will be sent out when preset frame size is reached. The range is 1-1024 bytes.	1024
Serial Frame Interval	The interval that the router sends out real serial data stored in the buffer area to public network. The range is 10-65535 ms. **Note:** data will be sent out to public network when real serial data size reaches the preset packet size, even though it's within the serial frame interval.	100
MQTT Connection	Select the MQTT connection to send serial port data, it's set up on **Service > MQTT** page.	Null
Type	Select Uplink or Downlink for this transparent. Every type supports to add 10 connections at most.	Null
Topic	Topic name used for publishing serial port data.	Null
Retain	Enable to set the latest message of this topic as retain message.	Null
QoS	QoS0, QoS1 or QoS2 are optional.	Null

Table 3-4-2-3 DTU Parameters

Related Configuration Example

DTU Application Example

3.4.3 Modbus Server (Slave)

This section describes how to achieve I/O status via Modbus TCP, Modbus RTU and Modbus RTU over TCP.

3.4.3.1 Modbus TCP

You can define the address of the DI and DO ports so as to poll DI's status and control DO's status via Modbus TCP protocol.

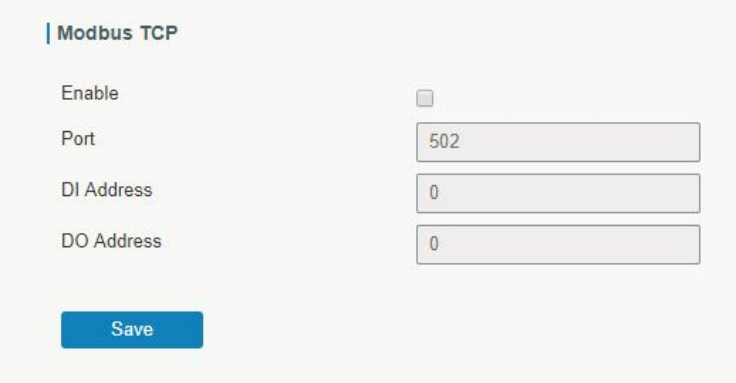


Figure 3-4-3-1

Modbus TCP		
Item	**Description**	**Default**
Enable	Enable/disable Modbus TCP.	Disable
Port	Set the router listening port. Range: 1-65535.	502
DI Address	Define the address of DI, range: 0-255.	0
DO Address	Define the address of DO, range: 0, 2-255.	0

Table 3-4-3-1 Modbus TCP Parameters

3.4.3.2 Modbus RTU

You can define the address of the DI and DO ports so as to poll DI's status and control DO's status via Modbus RTU protocol.

Figure 3-4-3-2

Modbus RTU		
Item	**Description**	**Default**
Enable	Enable/disable Modbus RTU.	Disable
Serial Port	Select the corresponding serial port.	serial
Server ID	Set server ID is used for distinguishing different devices on the same link.	1
DI Address	Define the address of DI, range: 0-255.	0
DO Address	Define the address of DO, range: 0, 2-255.	0

Table 3-4-3-2 Modbus RTU Parameters

3.4.3.3 Modbus RTU Over TCP

You can define the address of the DI and DO ports so as to poll DI's status and control DO's status via Modbus RTU over TCP.

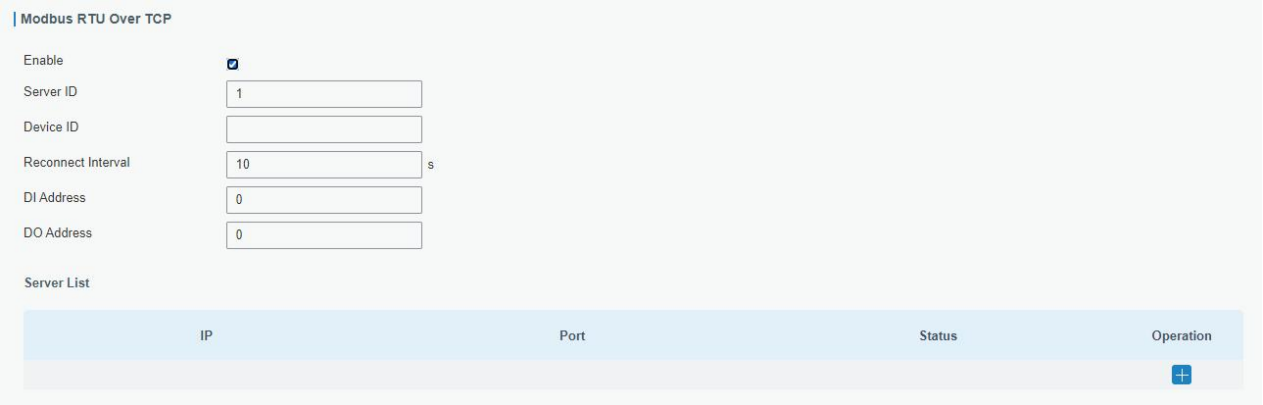


Figure 3-4-3-3

Modbus RTU Over TCP		
Item	**Description**	**Default**
Enable	Enable/disable Modbus RTU over TCP function.	Disable
Server ID	Set server ID is used for distinguishing different devices on the same link.	1
Device ID	Set device ID. The server will get the device ID to the server for identifying identity so that the server can manage multiple devices.	--
Reconnection Interval	The reconnection interval when the device and the server fails to establish connection or disconnected.	10
DI Address	Define the address of DI, range: 0-255.	0
DO Address	Define the address of DO, range: 0, 2-255.	0
Server List		
IP	Enter the IP address of the server.	
Port	Enter the port of the server.Range: 0-65535.	
Status	Show the connection status between the router and the server.	

Table 3-4-3-3 Modbus RTU Over TCP Parameters

3.4.4 Modbus Client (Master)

UR32 router can be set as Modbus Client to poll the remote Modbus Server and send alarm according to the response.

3.4.4.1 Modbus Client

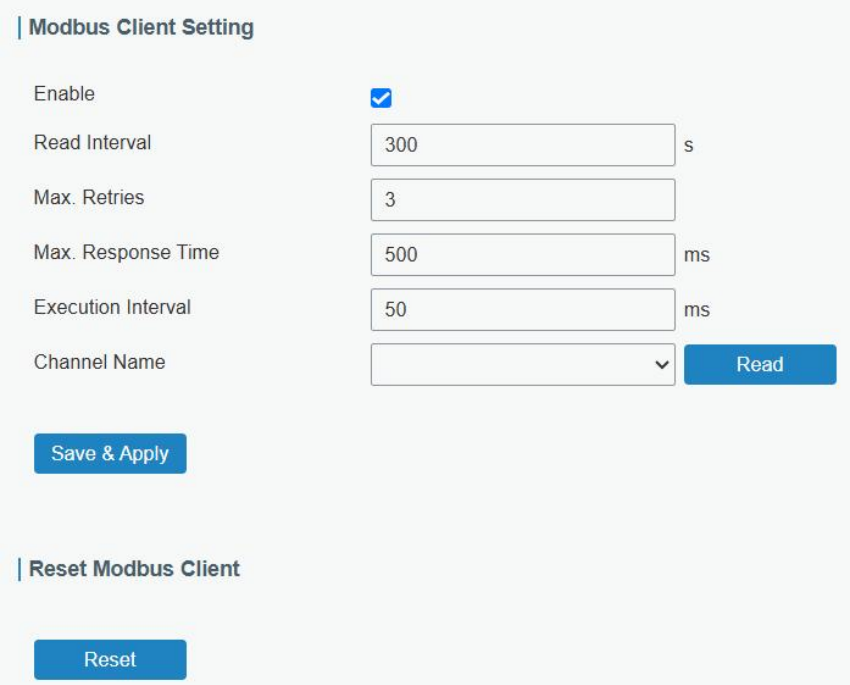


Figure 3-4-4-1

Modbus Client		
Item	**Description**	**Default**
Enable	Enable/disable Modbus client.	--
Read Interval/s	Set the interval for reading remote channels. When the read cycle ends, the commands which haven't been sent out will be discard, and the new read cycle begins. If it is set to 0, the device will restart the new read cycle after all channels have been read. Range: 0-600.	300
Max. Retries	Set the maximum retry times after it fails to read, range: 0-5.	3
Max. Response Time/ms	Set the maximum response time that the router waits for the response to the command. If the device does not get a response after the maximum response time, it's determined that the command has timed out. Range: 10-1000.	500
Execution Interval/ms	The execution interval between each command. Range: 10-1000.	50
Channel Name	Select a readable channel form the channel list.	--
Reset Modbus Client		
Reset	Clear all configurations of the Modbus Client.	--

Table 3-4-4-1

3.4.4.2 Channel Settings

On this page, you can add channels and configure the client parameters , so as to connect the router to the remote Modbus Server and execute the read/write function.

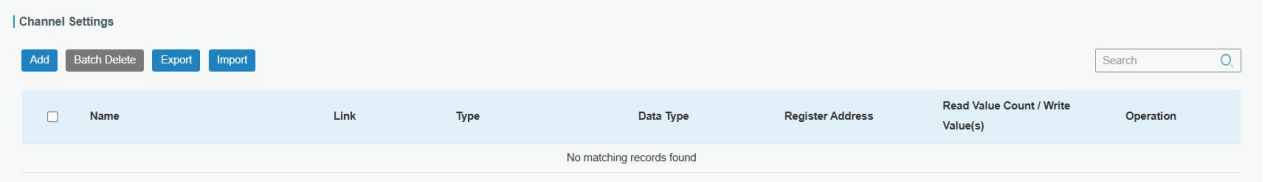


Figure 3-4-4-2

Channel Setting	
Item	**Description**
Add	Add a single Modbus channel.
Batch Delete	Delete multiple selected Modbus channels in bulk.
Export	Export all added Modbus channels as a table.
Import	Batch-add Modbus channels using a CSV file.

Table 3-4-4-2

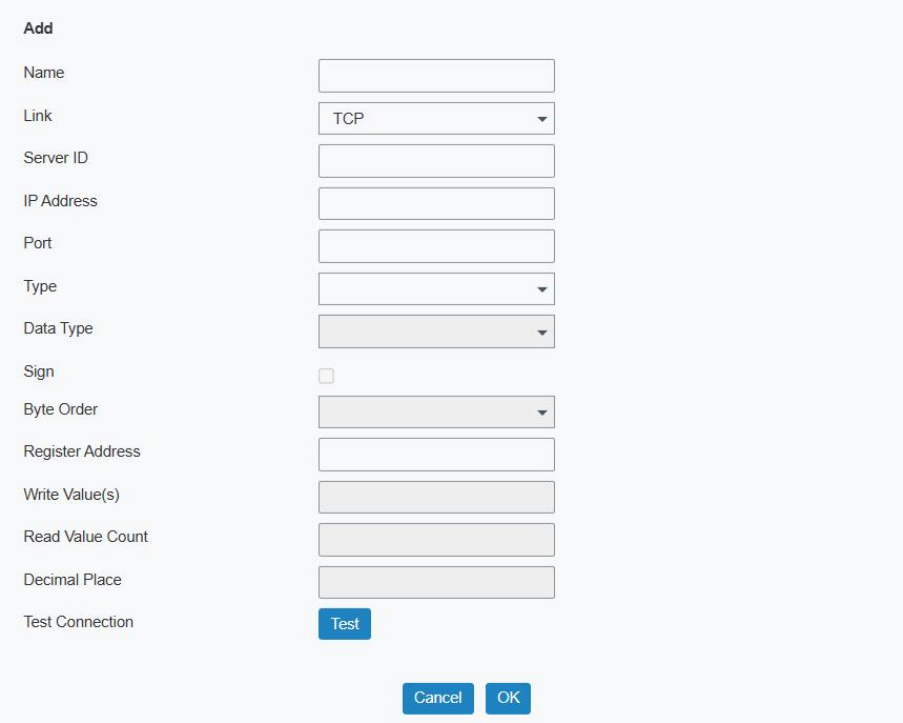


Figure 3-4-4-3

Add	
Item	**Description**
Name	Set the name to identify the remote channel. It cannot be blank.
Link	Select serial port or TCP connection. **Serial Port:** the router communicates with devices via Modbus RTU protocol. **TCP:** the router communicates with devices via Modbus TCP protocol.
Server ID	Set Modbus server ID.
IP address	When link is TCP, fill in the IP address of the remote Modbus TCP device.
Port	When link is TCP, fill in the port of the remote Modbus TCP device.

Type	Select the Modbus function to execute, including read or write commands. Options are Read Coils, Read Discrete Inputs, Read Holding Registers Read Input Registers, Write Single Coil, Write Single Holding Register Write Multiple Coils,Write Multiple Holding Registers.
Data Type	Data type used during read or write operations. Options are INT16, INT32, INT64, Float32, Float64, ASCII, HEX
Sign	When type is holding register or input register, enable or disable to identify whether this channel is signed.
Byte Order	Order of storage or transmission of multibyte data. Big-Endian: AB, ABCD, ABCDEFGH; Little-Endian:BA, CDAB, GHEFCDAB; Mixed-Endian: BADC, DCBA, HGFEDCBA, BADCFEHG
Register Address	The starting register address for read operations, or the target register address for write operations.
Write Value(s)	The actual value(s) to be written into the register. Values must comply with rules of the selected data type. Multiple values are separated by commas. Rules for different data types: ● INT16, INT32, INT64: Integer values, within the valid range of the data type.Maximum count: 123 / 61 / 30 values. ● Float32, Float64: Floating-point numbers, scientific notation supported. Maximum count: 61 / 30 values. ● BOOL: Only 0 or 1 allowed.Maximum count: 123 values. ● ASCII: Any ASCII character except space, ";", "(" mark.Values do not need separate by commas.Maximum: 246 characters. ● HEX: Four-digit hexadecimal values 0000 – FFFF.Maximum count: 123 values.
Read Value Count	Number of values to read when executing a read command. Maximum supported values: ● INT16, ASCII, HEX, BOOL: 125 ● INT32, Float32: 62 ● INT64, Float64: 31
Decimal Place	When type is holding register or input register, indicate a dot in the read into the position of the channel. For example: read the channel value is 1234 and a Decimal Place is equal to 2, then the actual value is 12.34.
Test Connection	Sends a Modbus request to the remote device to verify whether the link and parameters are valid. If the request fails, will return an error code and description.

Table 3-4-4-3

3.4.4.3 Alarm Settings

On this page, you can configure the alarm settings. If the read Modbus values meets the specified condition, the device performs a user-specified action, for example, sending a alarm content or a Modbus write request.

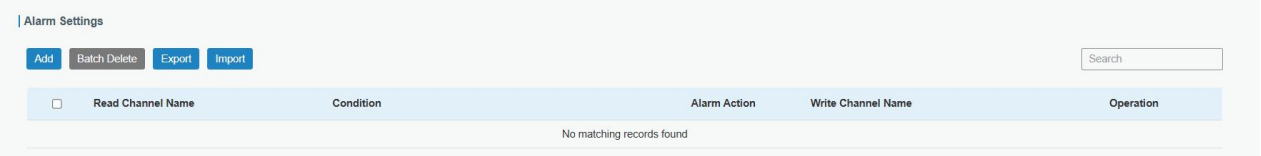


Figure 3-4-4-4

Channel Setting	
Item	**Description**
Add	Add a single Alarm.
Batch Delete	Delete multiple selected Alarms in bulk.
Export	Export all added Alarms as a CSV file.
Import	Batch-add Alarms using a CSV file.

Table 3-4-4-4

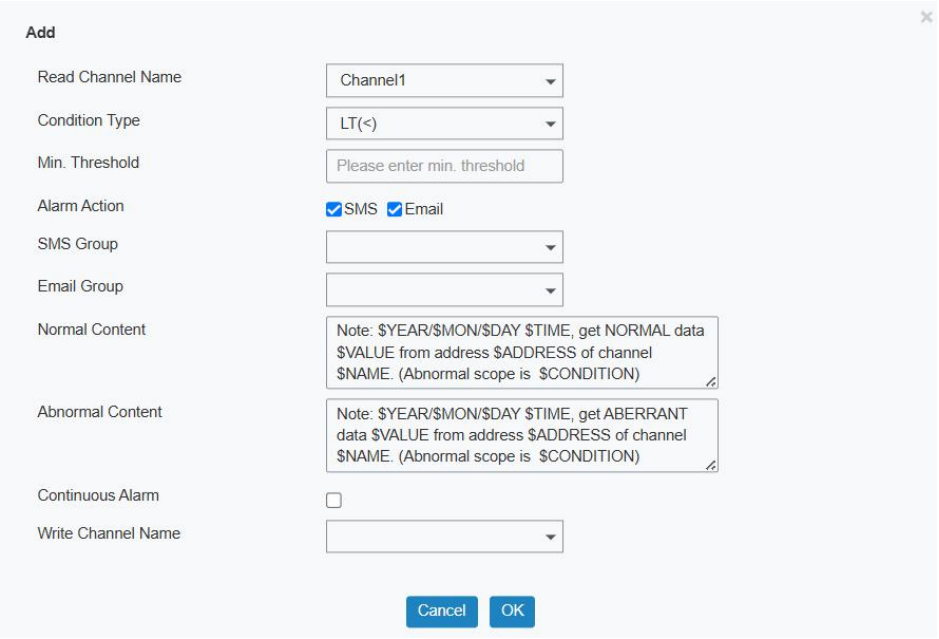


Figure 3-4-4-5

Add	
Item	**Description**
Read Channel Name	Name of the channel to be read. Only channels configured with a read function code can be selected.
Condition	The condition that triggers alert.
Min. Threshold	Set the min. value to trigger the alert. When the actual value is less than this value, the alarm will be triggered.
Max. Threshold	Set the max. value to trigger the alert. When the actual value is more than this value, the alarm will be triggered.
Alarm	Select the alarm method as SMS or Email.
SMS	The preset alarm content will be sent to the specified phone number.
Phone	Select the phone group to receive the alarm SMS.

Group	
Email Group	Select the Email group to receive the alarm Email.
Normal Content	When the actual value is restored to the normal value from exceeding the threshold value, the router will automatically cancel the abnormal alarm and send the preset normal content to the specified phone group.
Abnormal Content	When the actual value exceeds the preset threshold, the router will automatically trigger the alarm and send the preset abnormal content to the specified phone group.
Continuous Alarm	Once it is enabled, the same alarm will be continuously reported. Otherwise, the same alarm will be reported only one time.
Write Channel Name	Name of the channel to be written when an alarm is triggered. Only channels configured with a write function code can be selected.

Table 3-4-4-5

3.4.4.4 Data Forwarding

UR32 router supports MQTT forwarding and TCP forwarding.

The MQTT forwarding function is used to transfer Modbus data (send requests, receive responses) over MQTT. When it is enabled, the router subscribes to a REQUEST topic and publishes on a RESPONSE topic on a specified MQTT broker. It translates received MQTT message payload to a Modbus request and relays it to the specified Modbus server.

Figure 3-4-4-6

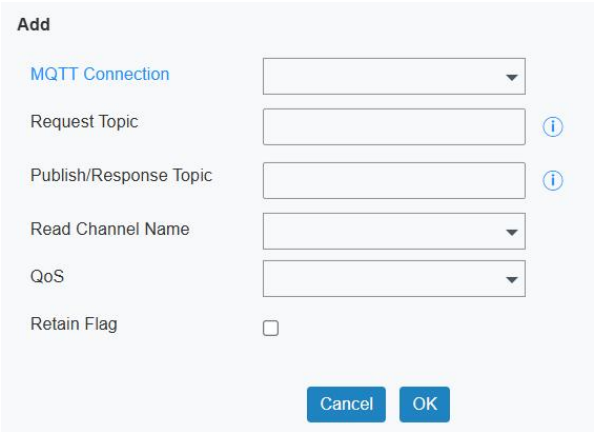


Figure 3-4-4-7

Add	
Item	**Description**
MQTT Connections	Select the MQTT connection to send Modbus channel data, it's set up on **Service > MQTT** page.
Request Topic	Topic name used for receiving Modbus channel data.
Publish/Response Topic	Topic name used for publishing Modbus channel data or responding to requests.
Read Channel Name	Name of the channel to be read. Only channels configured with a read function code can be selected.
QoS	QoS0, QoS1 or QoS2 are optional.
Retain	Enable to set the latest message of this topic as retain message.

Table 3-4-4-6

When TCP forwarding is enabled, router reads the register data from the specified channel and forwards it to the designated TCP server.

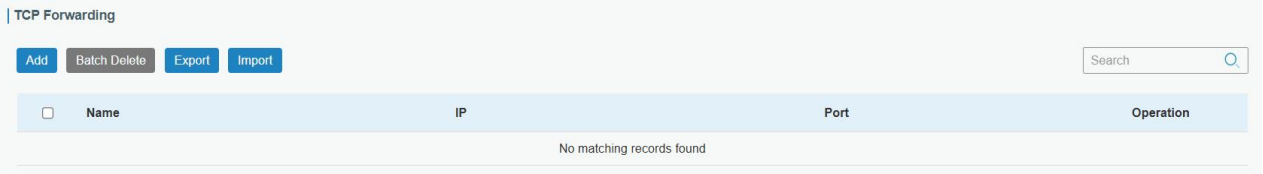


Figure 3-4-4-8

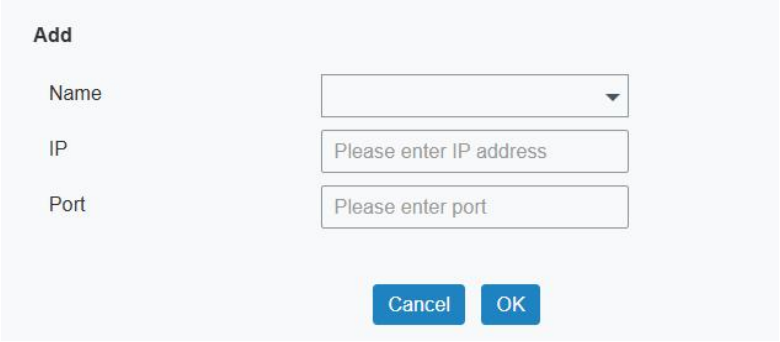


Figure 3-4-4-9

Add	
Item	**Description**
Name	The name of Modbus Client's channel.
IP	The IP address of the server which the packets are forwarded to.
Port	The port of the server's which the packets are forwarded to.

Table 3-4-4-7

3.4.5 GPS (Only Applicable to GPS Version)

When you want to receive GPS data, you should enable GPS function on this page.

Figure 3-4-5-1

3.4.5.1 GPS IP Forwarding

GPS IP forwarding means that GPS data can be forwarded over the Internet.

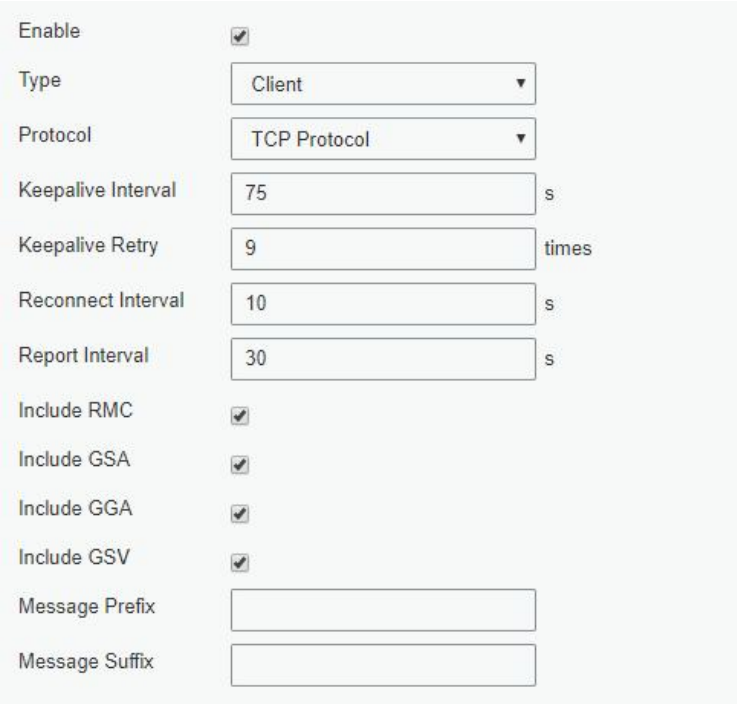


Figure 3-4-5-2

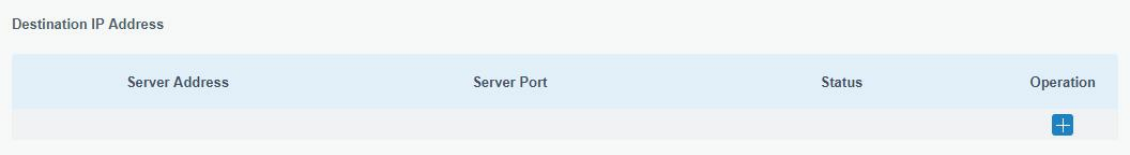


Figure 3-4-5-3

GPS IP Forwarding		
Item	**Description**	**Default**
Enable	Forward the GPS data to the client or server.	Disable
Type	Select connection type of the router as Client or Server.	Client
Protocol	Select protocol of data transmission as TCP or UDP.	TCP
Keepalive Interval	After it's connected with server/client, the router will send heartbeat packet regularly to the server/client to keep alive. The interval range is 1-3600 s.	75
Keepalive Retry	When TCP heartbeat times out, the router will resend heartbeat. After it reaches the preset retry times, router will reconnect to TCP server.	9

	The range is 1-16.	
Local Port	Set the router listening port. Range: 1-65535.	
Reconnect Interval	After connection failure, router will reconnect to the server at the preset interval. The range is 10-60 s.	10
Report Interval	Router will send GPS data to the server/client at the preset interval. The range is 1-60 s.	30
Include RMC	RMC includes time, date, position, course and speed data.	--
Include GSA	GSA includes GPS receiver operating mode, satellites used in the position solution, and DOP values.	--
Include GGA	GGA includes time, position and fix type data.	--
Include GSV	GSV includes the number, elevation, azimuth of GPS satellites and SNR values.	--
Message Prefix	Add a prefix to the GPS data.	Null
Message Suffix	Add a suffix to the GPS data.	Null
Destination IP Address		
Server Address	Fill in the server address to receive GPS data (IP/domain name).	--
Server Port	Fill in the port to receive GPS data. Range: 1-65535.	--
Status	Show the connection status between the router and the server.	--

Table 3-4-5-1 GPS IP Forwarding Parameters

3.4.5.2 GPS Serial Forwarding

GPS IP forwarding means that GPS data can be forwarded to the serial port.

Figure 3-4-5-4

GPS Serial Forwarding		
Item	**Description**	**Default**
Enable	Forward the GPS data to the preset serial port.	Disable

Serial Type	Select the serial port to receive GPS data. Ensure that the serial port is enabled on **Service > Serial Port**.	--
Report Interval	Router will forward the GPS data to the serial port at the preset interval. The range is 1-60 s.	30
Include RMC	RMC includes time, date, position, course and speed data.	--
Include GSA	GSA includes GPS receiver operating mode, satellites used in the position solution, and DOP values.	--
Include GGA	GGA includes time, position and fix type data.	--
Include GSV	GSV includes the number, elevation, azimuth of GPS satellites and SNR values.	--

Table 3-4-5-2 GPS Serial Forwarding Parameters

3.4.5.3 GPS MQTT Forward

GPS MQTT forward means that GPS raw data can be forwarded to MQTT broker automatically.

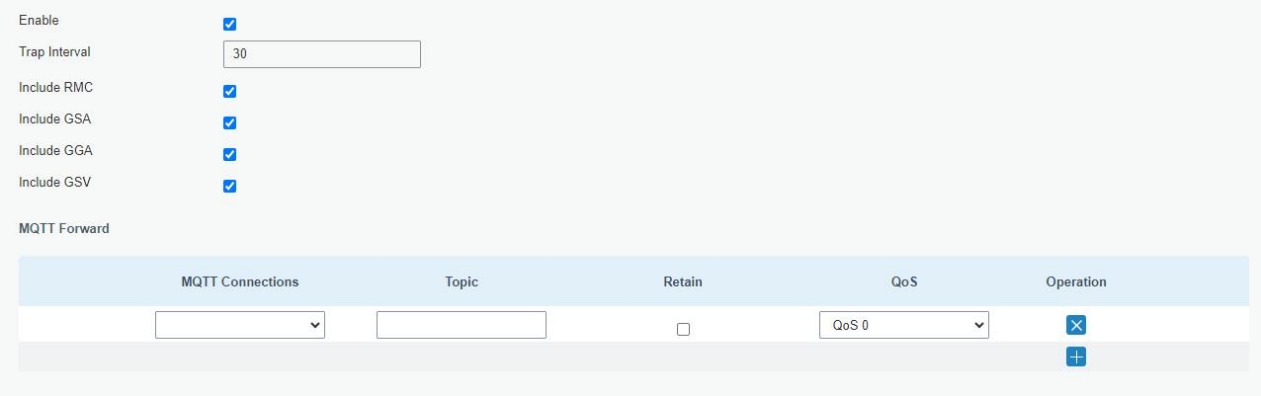


Figure 3-4-5-5

GPS MQTT Forward		
Item	**Description**	**Default**
Enable	Forward the GPS data to MTT broker automatically.	Disable
Trap Interval	The interval to locate and forward the GPS data to the MQTT broker. The range is 1-60 s.	30
Include RMC	RMC includes time, date, position, course and speed data.	--
Include GSA	GSA includes GPS receiver operating mode, satellites used in the position solution, and DOP values.	--
Include GGA	GGA includes time, position and fix type data.	--
Include GSV	GSV includes the number, elevation, azimuth of GPS satellites and SNR values.	--
MQTT Forward		
MQTT Connections	Select the MQTT connection to send GPS data, it's set up on **Service > MQTT** page.	
Topic	Topic name for publishing GPS raw data.	
Retain	Enable to set the latest message of this topic as retain message.	
QoS	QoS0, QoS1 or QoS2 are optional.	

Table 3-4-5-3 GPS MQTT Forward Parameters

3.4.6 MQTT

UR32 supports to work as MQTT client to forward data and router information to MQTT broker in two ways:

1. Users send requests to the router to enquire the router information;
2. The router publishes the data automatically.

Figure 3-4-6-1

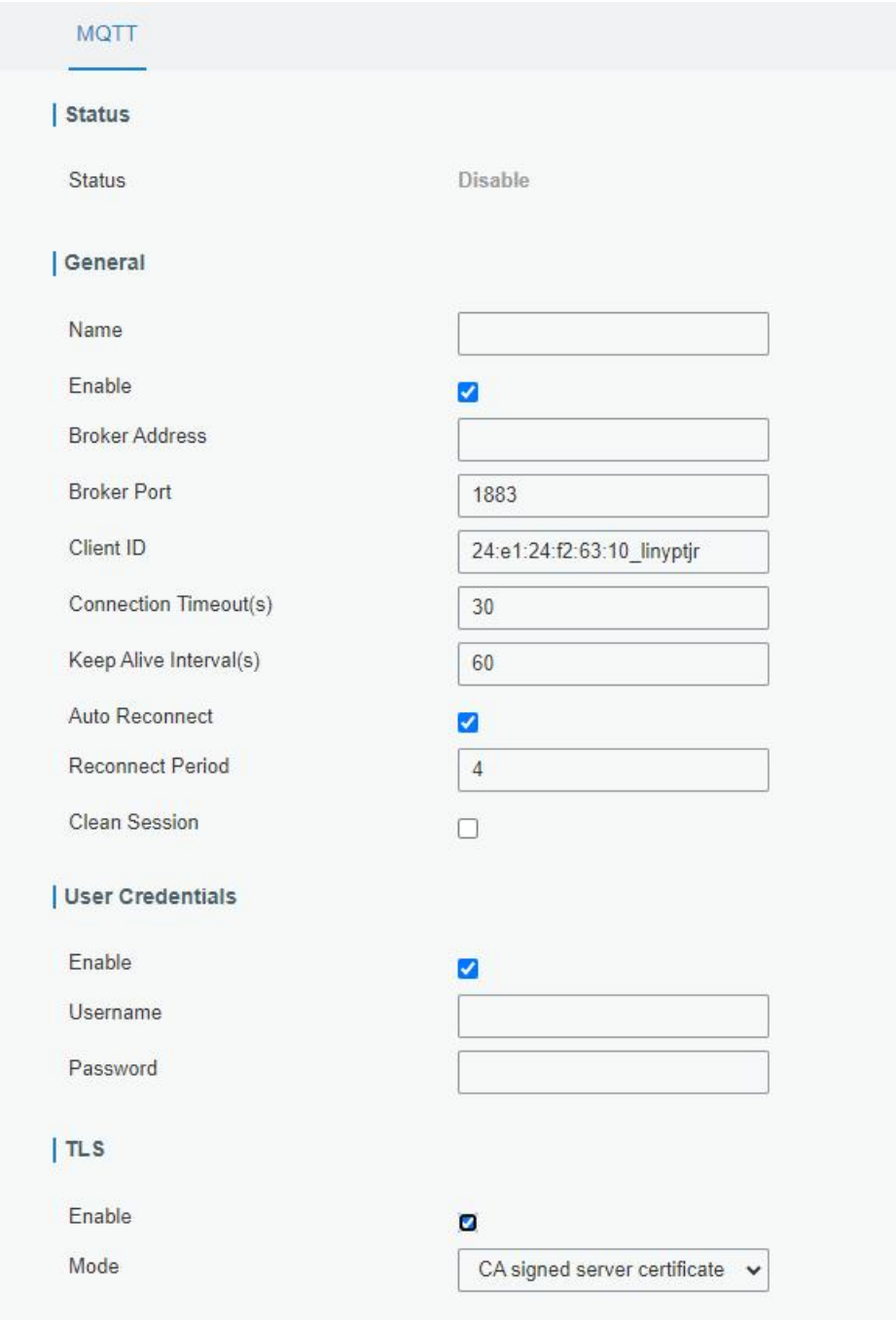

MQTT
Status
Status
Disable
General
Name
Enable
Broker Address
Broker Port
1883
Client ID
24:e1:24:f2:63:10_linyptjr
Connection Timeout(s)
30
Keep Alive Interval(s)
60
Auto Reconnect
Reconnect Period
4
Clean Session
User Credentials
Enable
Username
Password
TLS
Enable
Mode
CA signed server certificate

Figure 3-4-6-2

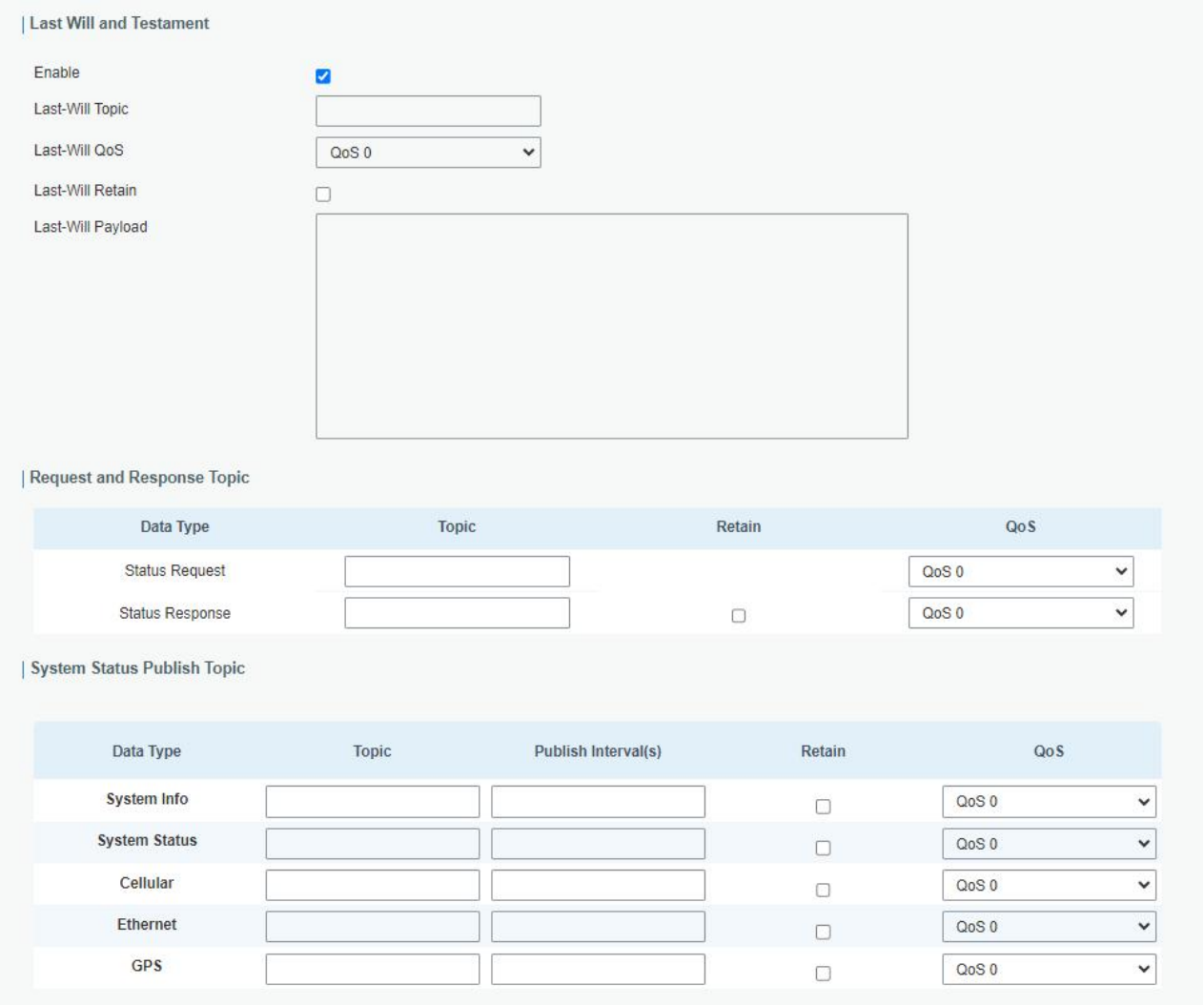


Figure 3-4-6-3

MQTT Settings	
Item	**Description**
Status	Show connection status between router and MQTT broker.
General	
Name	Customize a unique connection name. It is not allowed to change after save.
Enable	Enable or disable this MQTT connection.
Broker Address	MQTT broker address to receive data.
Broker Port	MQTT broker port to receive data.
Client ID	Client ID is the unique identity of the client to the server. It must be unique when all clients are connected to the same server, and it is the key to handle messages at QoS 1 and 2.
Connection Timeout/s	If the client does not get a response after the connection timeout, the connection will be considered as broken. The Range: 1-65535.
Keep Alive Interval/s	After the client is connected to the server, the client will send heartbeat packet to the server regularly to keep alive. Range: 1-65535.
Auto	When connection is broken, try to reconnect the server automatically.

Reconnect	
Reconnect Period	When connection is broken, the period to reconnect the server periodically.
Clean Session	When enabled, the connection will create a temporary session and all information will lose when the client is disconnected from broker; when disabled, the connection will create a persistent session that will remain and save offline messages until the session logs out overtime.
User Credentials	
Enable	Enable user credentials.
Username	The username used for connecting to the MQTT broker.
Password	The password used for connecting to the MQTT broker.
TLS	
Enable	Enable the TLS encryption in MQTT communication.
Mode	Select from Self signed certificates, CA signed server certificate. **CA signed server certificate:** verify with the certificate issued by Certificate Authority (CA) that pre-loaded on the device. **Self signed certificates:** upload the custom CA certificates, client certificates and secret key for verification.
Last Will and Testament	
Enable	Last will message is automatically sent when the MQTT client is abnormally disconnected. It is usually used to send device status information or inform other devices or proxy servers of the device's offline status.
Last-Will Topic	Customize the topic to receive last will messages.
Last-Will QoS	QoS0, QoS1 or QoS2 are optional.
Last-Will Retain	Enable to set last will message as retain message.
Last-Will Payload	Customize the last will message contents.
Request and Response Topic	

Topic	The router supports to send requests to enquire router information.
	Status Request: users is able to send requests to this topic to enquire router information. Request format:
	{
	"id":"1",
	"status":"systeminfo",
	"sn": "64E1213132456",
	"need_response":1 //1 means need response
	}
	The id is a random value, and the status can be set as 5 types: systeminfo, systemstatus, cellular, ethernet, gps.
	Status Response: users is able to subscribe this topic to get the replies.

Retain	Enable to set the latest message of this topic as retain message.
QoS	QoS0, QoS1 or QoS2 are optional.
System Status Publish Topic	

Data Type	Data type sent to MQTT broker automatically. Note that the GPS in this page is not raw data but decoded location data.
Topic	Topic name of the data type used for publishing.
Publish Interval (s)	The interval to publish data to MQTT broker automatically.
Retain	Enable to set the latest message of this topic as retain message.
QoS	QoS0, QoS1 or QoS2 are optional.

Table 3-4-6-1 MQTT Parameters

3.4.7 SNMP

SNMP is widely used in network management for network monitoring. SNMP exposes management data with variables form in managed system. The system is organized in a management information base (MIB) which describes the system status and configuration. These variables can be remotely queried by managing applications.

Configuring SNMP in networking, NMS, and a management program of SNMP should be set up at the Manager.

Configuration steps are listed as below for achieving query from NMS:

1. Enable SNMP setting.
2. Download MIB file and load it into NMS.
3. Configure MIB View.
4. Configure VCAM.

Related Configuration Example

SNMP Application Example

3.4.7.1 SNMP

UR32 supports SNMPv1, SNMPv2c and SNMPv3 version. SNMPv1 and SNMPv2c employ community name authentication. SNMPv3 employs authentication encryption by username and password.

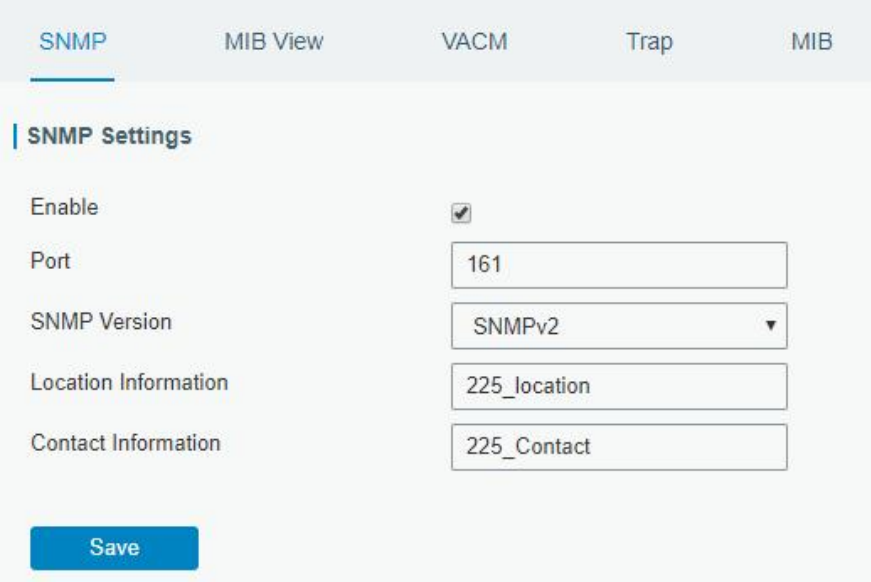


Figure 3-4-7-1

SNMP Settings	
Item	**Description**
Enable	Enable or disable SNMP function.
Port	Set SNMP listened port. Range: 1-65535. The default port is 161.
SNMP Version	Select SNMP version; support SNMP v1/v2c/v3.
Location Information	Fill in the location information.
Contact Information	Fill in the contact information.

Table 3-4-7-1 SNMP Parameters

3.4.7.2 MIB View

This section explains how to configure MIB view for the objects.

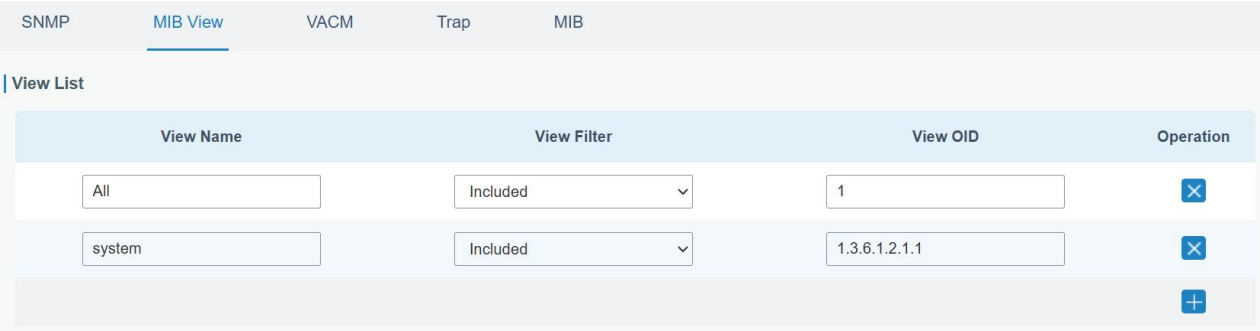


Figure 3-4-7-2

MIB View	
Item	**Description**
View Name	Set MIB view's name.
View Filter	Select from "Included" and "Excluded".
View OID	Enter the OID number.
Included	You can query all nodes within the specified MIB node.

Excluded	You can query all nodes except for the specified MIB node.

Table 3-4-7-2 MIB View Parameters

3.4.7.3 VACM

This section describes how to configure VCAM parameters.

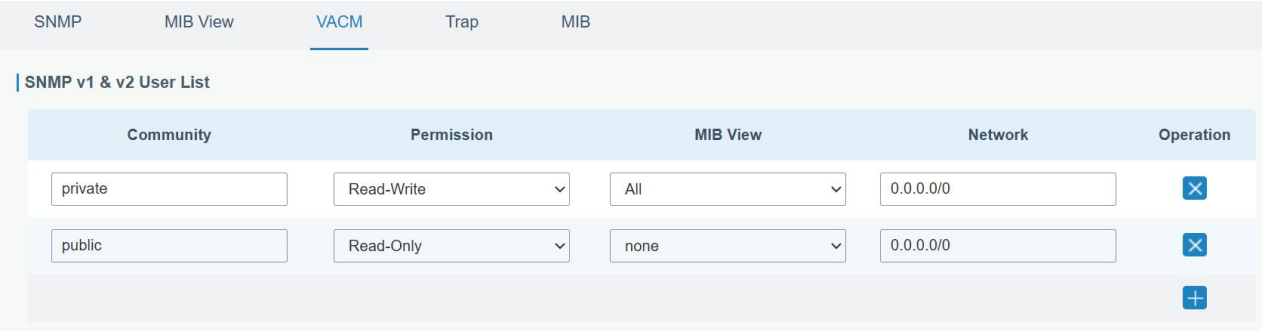


Figure 3-4-7-3

VACM	
Item	**Description**
SNMP v1 & v2 User List	
Community	Set the community name.
Permission	Select from "Read-Only" and "Read-Write".
MIB View	Select an MIB view to set permissions from the MIB view list.
Network	The IP address and bits of the external network accessing the MIB view.
Read-Write	The permission of the specified MIB node is read and write.
Read-Only	The permission of the specified MIB node is read only.
SNMP v3 User Group	
Group Name	Set the name of SNMPv3 group.
Security Level	Select from "NoAuth/NoPriv", "Auth/NoPriv", and " Auth/Priv".
Read-Only View	Select an MIB view to set permission as "Read-only" from the MIB view list.
Read-Write View	Select an MIB view to set permission as "Read-write" from the MIB view list.
Inform View	Select an MIB view to set permission as "Inform" from the MIB view list.
SNMP v3 User List	
Username	Set the name of SNMPv3 user.
Group Name	Select a user group to be configured from the user group.
Authentication	Select from "MD5", "SHA", and "None".
Authentication Password	The password should be filled in if authentication is "MD5" and "SHA".
Encryption	Select from "AES", "DES", and "None".
Encryption Password	The password should be filled in if encryption is "AES" and "DES".

Table 3-4-7-3 VACM Parameters

3.4.7.4 Trap

This section explains how to enable network monitoring by SNMP trap.

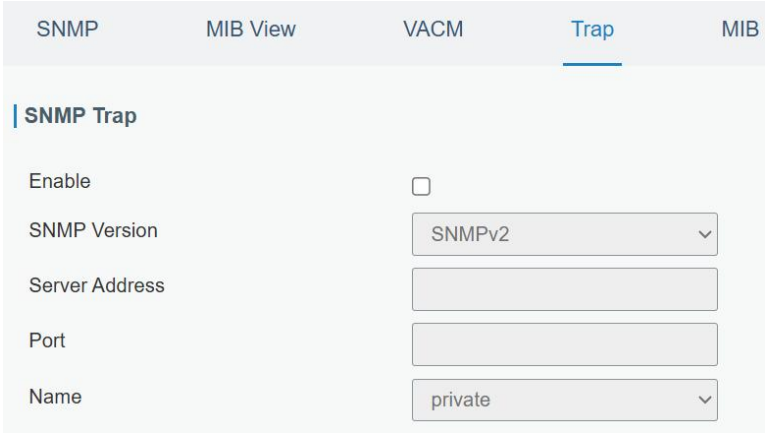


Figure 3-4-7-4

SNMP Trap	
Item	**Description**
Enable	Enable or disable SNMP Trap function.
SNMP Version	Select SNMP version; support SNMP v1/v2c/v3.
Server Address	Fill in NMS's IP address or domain name.
Port	Fill in UDP port. Port range is 1-65535. The default port is 162.
Name	Fill in the group name when using SNMP v1/v2c; fill in the username when using SNMP v3.
Auth/Priv Mode	Select from "NoAuth & No Priv", "Auth & NoPriv", and "Auth & Priv".

Table 3-4-7-4 Trap Parameters

3.4.7.5 MIB

This section describes how to download MIB files. The last MIB file “LTE-ROUTER-MIB.txt” is for the UR32 router.

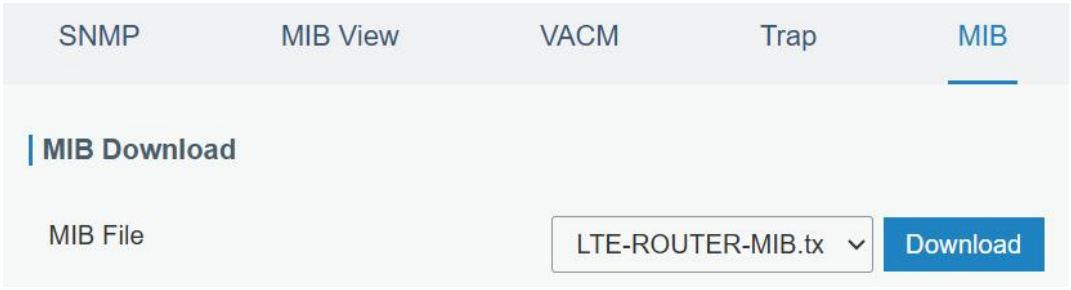


Figure 3-4-7-5

MIB	
Item	**Description**
MIB File	Select the MIB file you need.
Download	Click "Download" button to download the MIB file to PC.

Table 3-4-7-5 MIB Download

3.4.8 TR069

Technical Report 069 (TR-069) is a technical specification of Broadband Forum that defines an application layer protocol for remote management and provisioning of customer-premises equipment

(CPE) connected to an Internet Protocol (IP) network.

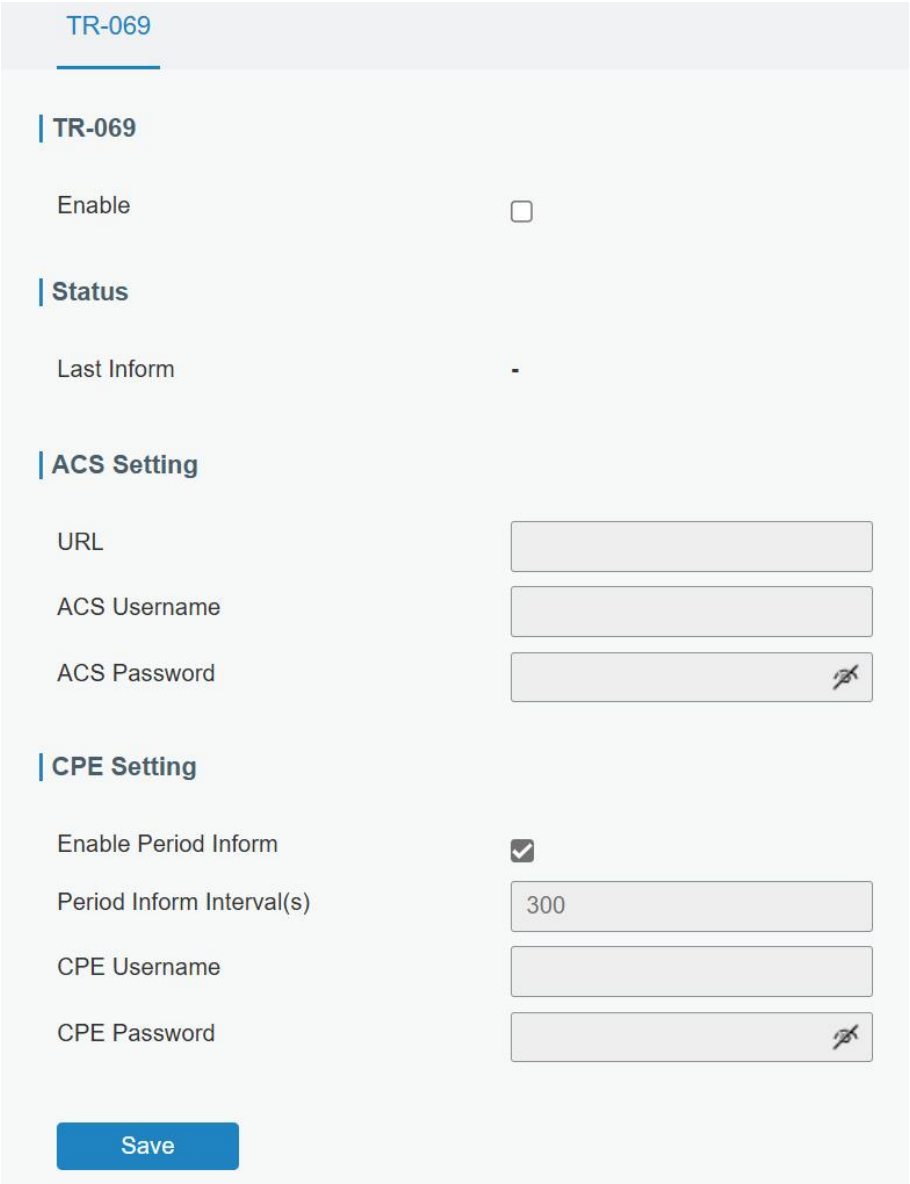


Figure 3-4-8-1

TR-069	
Item	**Description**
Enable	Enable or disable TR069 feature.
Last Inform	The last time the router informed to TR069 ACS.
ACS Setting	
URL	The URL of TR069 auto configuration server (ACS).
ACS Username	The username used by ACS to authenticate the CPE when it initiates a connection request.
ACS Password	The password used by ACS to authenticate the CPE when it initiates a connection request.
CPE Setting	
Enable Period Inform	Enable or disable inform periodically.

Period Inform Interval (s)	The interval to report information to ACS, this should be less than the timeout of peer ACS.
CPE Username	The username used by CPE to authenticate the ACS when it initiates a connection request.
CPE Password	The password used by CPE to authenticate the ACS when it initiates a connection request.

Table 3-4-8-1 TR069 Parameters

3.4.9 DLMS

UR32 supports periodically enquiring data from meters and uploading it to the platform.

3.4.9.1 Physical Device Settings

This section describes how to configure the defined data frame format and interactive command mode on the router to achieve mutual authentication with the meter, mode selection, and data read and write request reply.

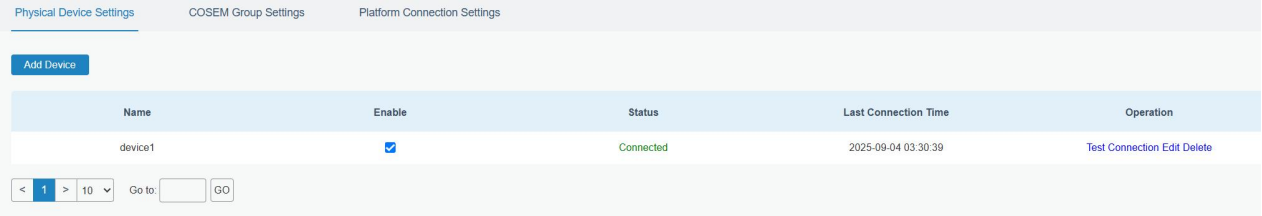


Figure 3-4-9-1

Physical Device List	
Item	**Description**
Add Device	Add a new physical device. The number of physical device is limited to 30.
Name	The name of the physical device.
Enable	Enable/disable the physical device.
Status	Displays the connection status of the physical device.
Last Connection Time	Displays the last connection time of the physical device.
Operation	**Test Connection:** Tests whether the physical device can be accessed normally. The test result will be returned after completion. **Edit:** Edit the parameters of an added physical device. **Delete:** Delete the added physical device. Devices in use cannot be deleted.

Table 3-4-9-1 Physical Device Setting

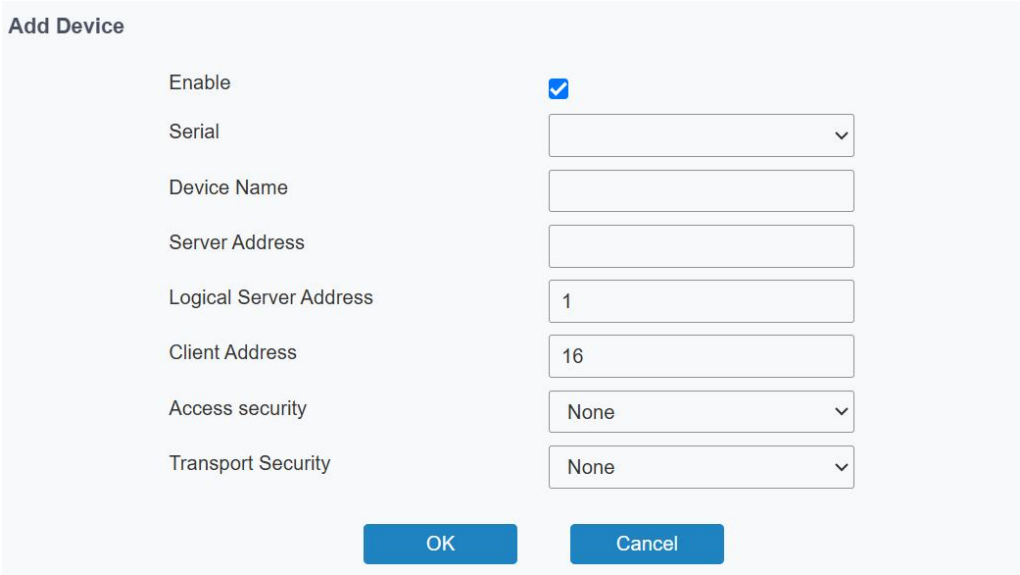


Figure 3-4-9-2

Add Device		
Item	**Description**	**Default**
Enable	Enable/disable the physical device.	Enable
Serial	Select the serial port where the physical device is connected.	--
Device Name	The name of the physical device. This name is used in the COSEM group settings to reference the added physical device.	--
Server Address	Enter the server address of the physical device. This information is usually provided in the physical device's user manual.	--
Logical Server Address	Enter the logical server address of the physical device. This information is usually provided in the physical device's user manual. The server address and logical server address of different physical devices cannot both be identical.	1
Client Address	According to standard definitions, the client address is related to user permissions. Each client address represents a different access security level. This information is usually provided in the physical device's user manual.	16
Access security	Authentication allows the physical device (Server) to permit this device (Client) to access data with different permission levels. If set to None, no authentication will be performed, and only read access will be allowed.	None
Password	Set the password for this device (Client) to access the physical device (Server).	--
Transport security	Configure the transmission encryption method for this device (Client) when accessing the physical device	None

	(Server).	
Invocation Counter OBIS Code	Used in specific connection security modes. It specifies the OBIS Code of the device's Invocation Counter. Each time encrypted communication is initiated, the device increments the Invocation Counter by one for comparison and security verification.	--
Authentication Key	Used in specific authentication and connection security modes. Set the authentication key of the physical device, usually provided in the physical device's user manual.	--
Block Cipher Key	Used in specific authentication and connection security modes. Set the block cipher key of the physical device, usually provided in the physical device's user manual.	--
Dedicated Key	A 16-octet value sent by the client to the server during connection establishment. The dedicated key may be regenerated randomly before each connection. Some physical devices expect the dedicated key to be a fixed value.	--

Table 3-4-9-2 Physical Device Parameters

3.4.9.2 COSEM Group Settings

COSEM groups are a convenient way to organize the OBIS codes that you want to send to the remote data collection server. You can add OBIS from different physical devices to the same COSEM group.

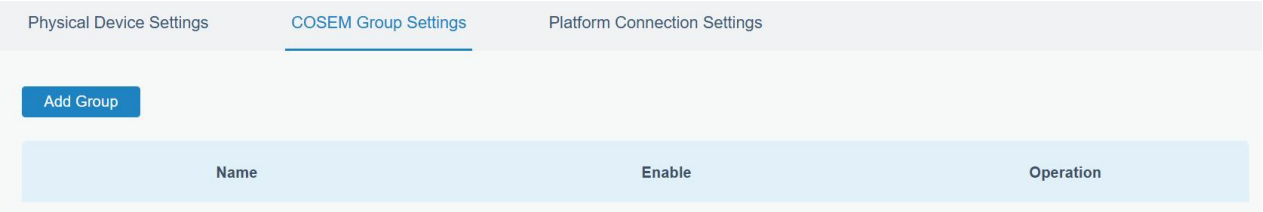


Figure 3-4-9-3

COSEM Group List	
Item	**Description**
Add Group	Add a new COSEM group. The number of COSEM groups is up to 10 and the COSEM objects is up to 30 in each group.
Name	The name of the COSEM group.
Enable	Enable/disable the COSEM group.
Operation	**Test:** Test whether the COSEM group can successfully collect data. The test result will be returned after completion. **Edit**: Edit the parameters of the COSEM group. **Delete**: Delete the added COSEM group. COSEM groups in use cannot be deleted.

Table 3-4-9-3 COSEM Group List

Figure 3-4-9-4

Edit		
Item	**Description**	**Default**
Enable	Enable/disable the COSEM group.	/
Name	The name of the COSEM group. This name is used in places such as platform connections to select the COSEM group for reporting.	/
Interval	Read data from the COSEM group at the specified time interval. If the COSEM group is selected in a platform connection, the data will be reported immediately after reading.	60
COSEM Value	Add a new COSEM Value to the COSEM group.	

Table 3-4-9-4 COSEM Group Parameters

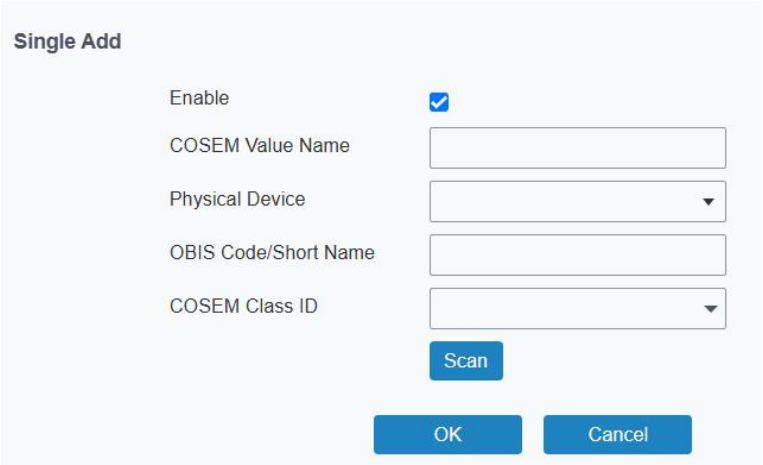


Figure 3-4-9-5

Item	Description
COSEM Value Name	Set the name of the COSEM Value.
Physical Device	Select the physical device(s) associated with the COSEM Value. Multiple selections are allowed.
OBIS Code	The OBIS Code value of the COSEM Value.
COSEM Class ID	The Class ID to which the COSEM Value belongs.
Scan	Scan the selected physical devices for OBIS objects they have in common. Click Apply to fill the parameters of the OBIS object into the

	corresponding configuration fields above.

Table 3-4-9-5 COSEM Value Parameters

3.4.9.3 Platform Connection Settings

The router supports data reporting via MQTT or HTTP and data caching.

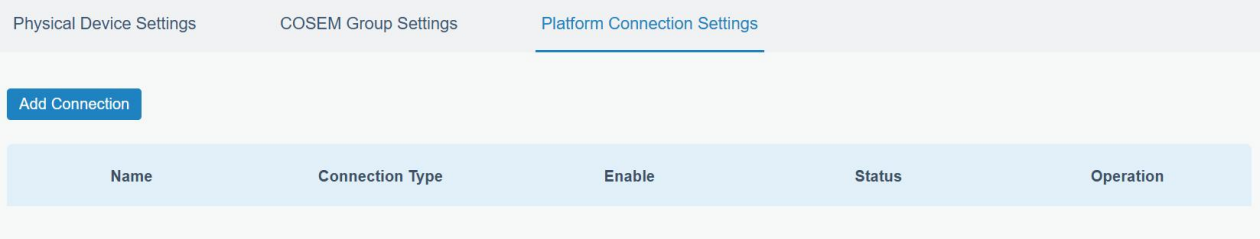


Figure 3-4-9-6

Platform Connection Settings	
Item	**Description**
Add Connection	Add a new platform connection.The number of connection platforms is up to 3.
Name	Set the name of the platform connection.
Connection Type	Set the connection type to MQTT or HTTP.
Enable	Enable/disable the platform connection.
Status	Show the status of platform connection.
Operation	You can edit the platform configuration or delete the platform.

Table 3-4-9-6 Platform Connection Settings

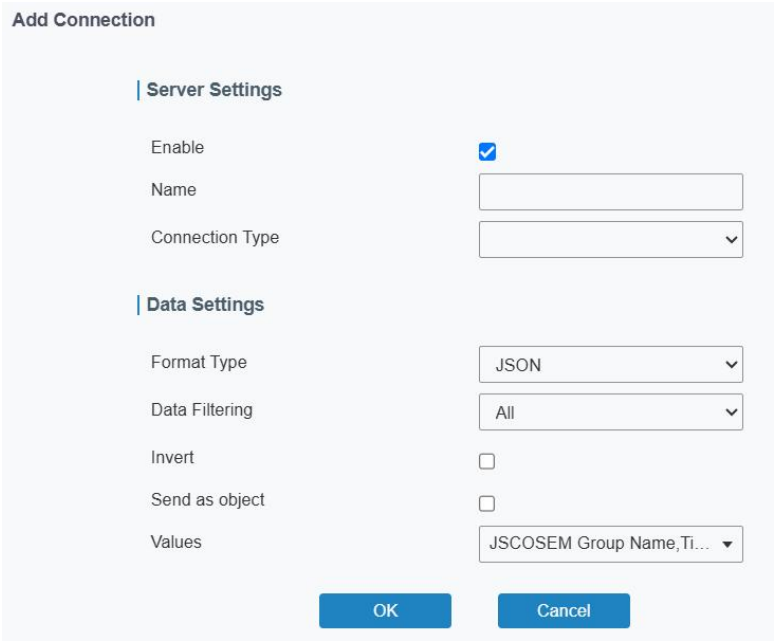


Figure 3-4-9-7

Add Connection		
Item	**Description**	
Server Settings		
Enable	Enable/disable the platform connection.	Enable

Name	Set the name of the platform connection.	/
Connection Type	Set the connection type to MQTT or HTTP.	/
Server Address	The HTTP server address to which the data will be sent.	/
HTTP Header	Headers are name/value pairs that appear in both request and response messages. HTTP headers provide the web server with information about the type of browser making the request. The format must be [Key: Value], e.g., [Content-Type:application/json]. Up to 30 pairs can be added.	/
Retry	Whether to attempt resending when sending fails.	Disable
Retry Count	The number of resend attempts.	3
Retry Interval	The time interval between each resend attempt.	10
MQTT Connection	Select an MQTT connection that has already been added in **Service** > **MQTT**.	/
Topic	The MQTT topic for subscription or publication.	/
Retain	Enable/disable the MQTT retained message flag. When enabled, a published message will be stored on the broker so that any client subscribing to the topic later can receive the message.	Disable
QoS	**QoS 0**: At most once delivery. **QoS 1**: At least once delivery, until a PUBACK is received from the service; may result in multiple retransmissions. **QoS 2**: Exactly once delivery; ensures each message is received only once, the safest but slowest service level.	Qos0
Data Settings		
Format Type	Select the message format type used for sending data. **JSON**: Standard JSON format. **Custom**: Custom format, supports custom variables.	JSON
Data Filter	Specify which COSEM group(s) to include in the transmitted COSEM data. **All**: All COSEM groups. **Custom**: Custom selection of COSEM groups.	All
COSEM Group	Select the COSEM group whose data will be sent to the server.	/
Invert	Reverse filtering. When selected, the system will send data from all COSEM groups except those selected above.	Disable
Cache Segmented Sending	Specify whether multiple cached data segments that failed to send should be sent separately.	Enable
Values	Select which data to include in the reported JSON.	/
Format String	Customize the reported content. Supports variables and text.	/

Table 3-4-9-7 Platform Connection Parameters

3.5 Maintenance

This section describes system maintenance tools and management.

3.5.1 Tools

Troubleshooting tools includes ping, traceroute, packet analyzer and qxdmlog.

3.5.1.1 Ping

Ping tool is engineered to ping outer network.

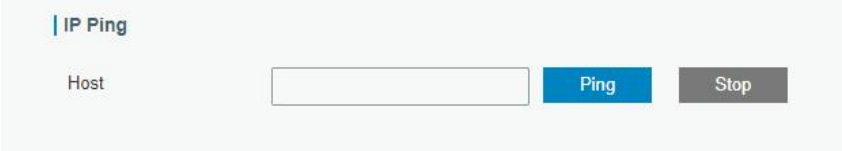


Figure 3-5-1-1

PING	
Item	**Description**
Host	Ping outer network from the router.

Table 3-5-1-1 IP Ping Parameters

3.5.1.2 Traceroute

Traceroute tool is used for troubleshooting network routing failures.

Figure 3-5-1-2

Traceroute	
Item	**Description**
Host	Address of the destination host to be detected.

Table 3-5-1-2 Traceroute Parameters

3.5.1.3 Packet Analyzer

Packet Analyzer is used for capturing the packet of different interfaces.

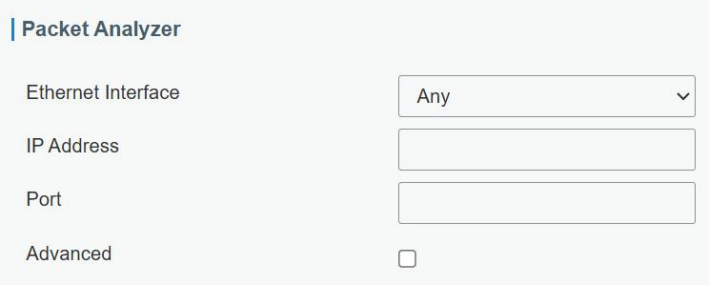


Figure 3-5-1-3

Packet Analyzer	
Item	**Description**
Ethernet Interface	Select the interface to capture packages.
IP Address	Set the IP address that the router will capture.
Port	Set the port that the router will capture.
Advanced	Set the rules for sniffer. The format is tcpdump.

Table 3-5-1-3 Packet Analyzer Parameters

3.5.1.4 Qxdmlog

This section allow collecting diagnostic logs via QXDM tool.

Figure 3-5-1-4

3.5.2 Debugger

3.5.2.1 Cellular Debugger

This section explains how to send AT commands to router and check cellular debug information.

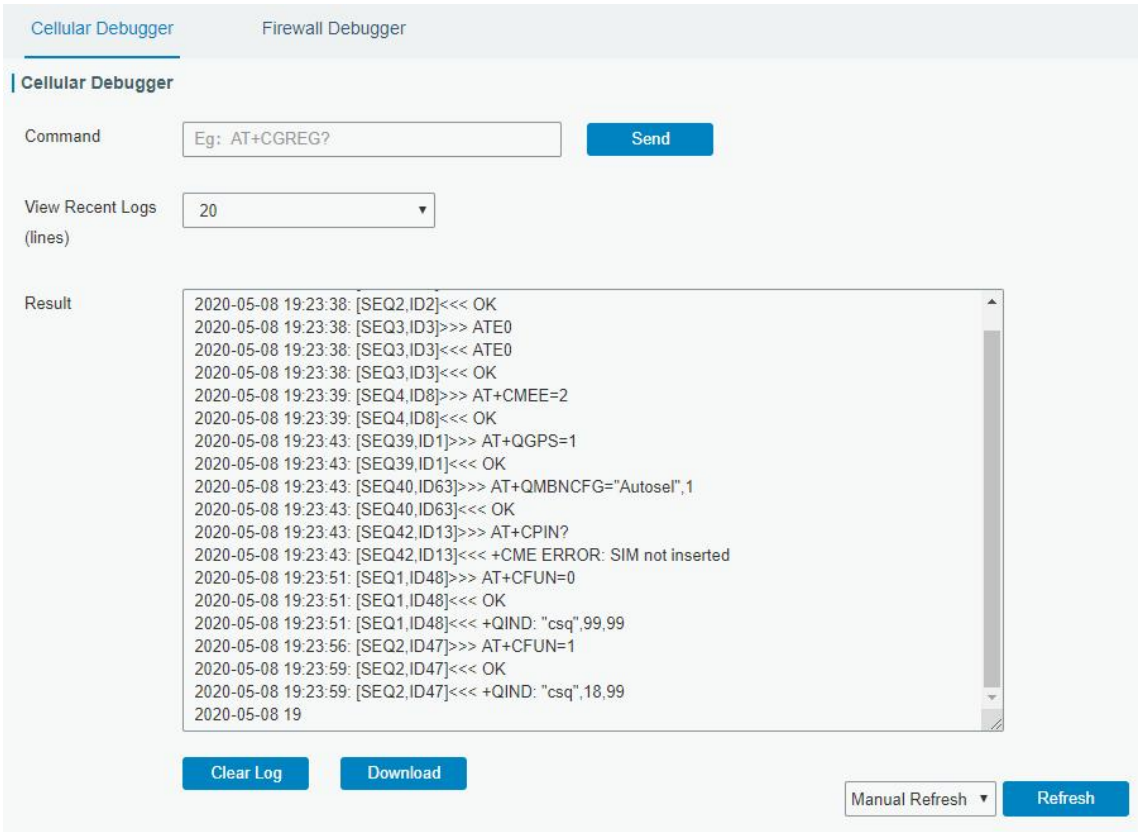


Figure 3-5-2-1

Cellular Debugger	
Item	**Description**
Command	Enter the AT command that you want to send to cellular modem.
View Recent Logs (lines)	View the specified lines of the result.
Result	Show the response result from cellular modem.

Table 3-5-2-1 Cellular Debugger Parameters

3.5.2.2 Firewall Debugger

This section explains how to send commands to router and check firewall information.

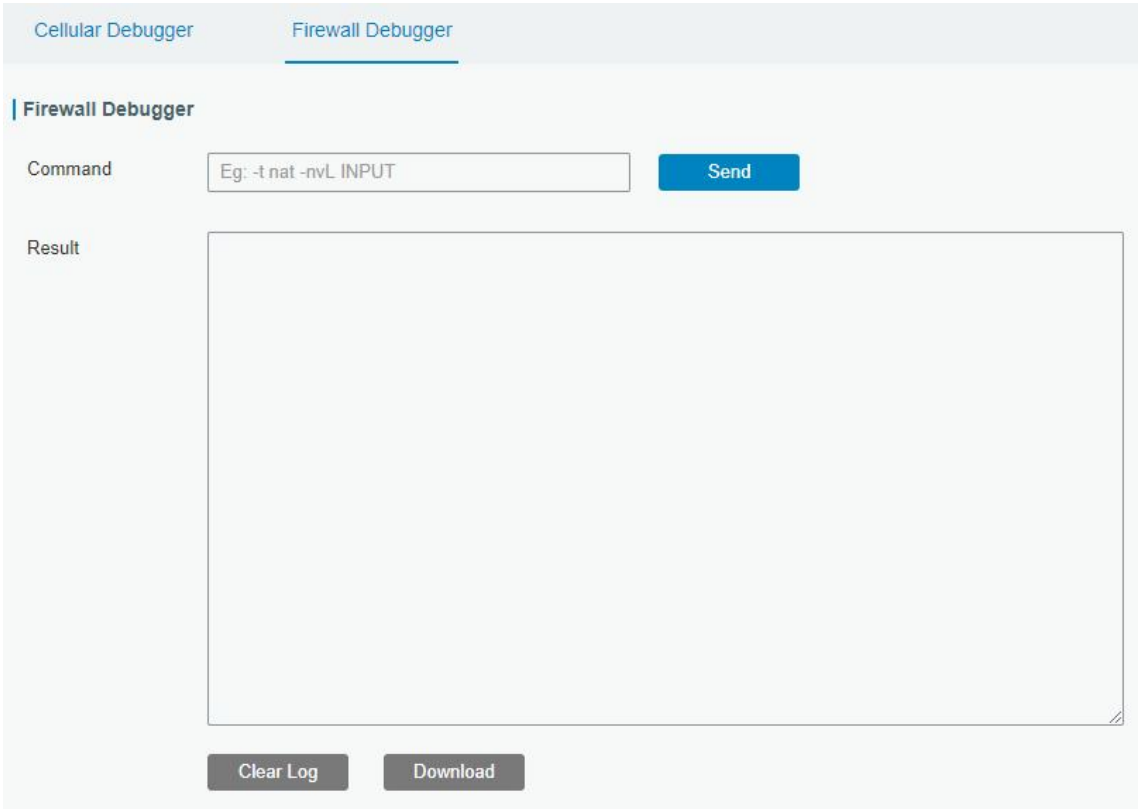


Figure 3-5-2-2

Firewall Debugger	
Item	**Description**
Command	Enter the AT command that you want to send to firewall module.
Result	Show the response result from firewall module.

Table 3-5-2-2 Firewall Debugger Parameters

3.5.3 Log

The system log contains a record of informational, error and warning events that indicates how the system processes. By reviewing the data contained in the log, an administrator or user troubleshooting the system can identify the cause of a problem or whether the system processes are loading successfully. Remote log server is feasible, and router will upload all system logs to remote log server such as Syslog Watcher.

3.5.3.1 System Log

This section describes how to view the recent log on web.

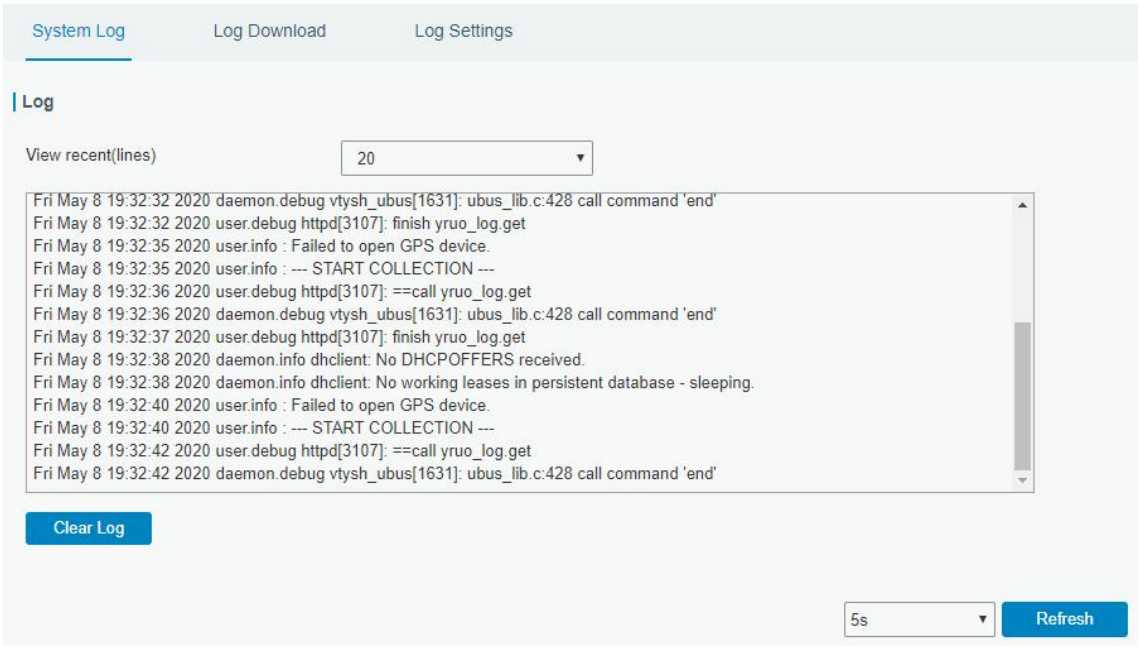


Figure 3-5-3-1

System Log	
Item	**Description**
View recent (lines)	View the specified lines of system log.
Clear Log	Clear the current system log.

Table 3-5-3-1 System Log Parameter

3.5.3.2 Log Download

This section describes how to download log files.

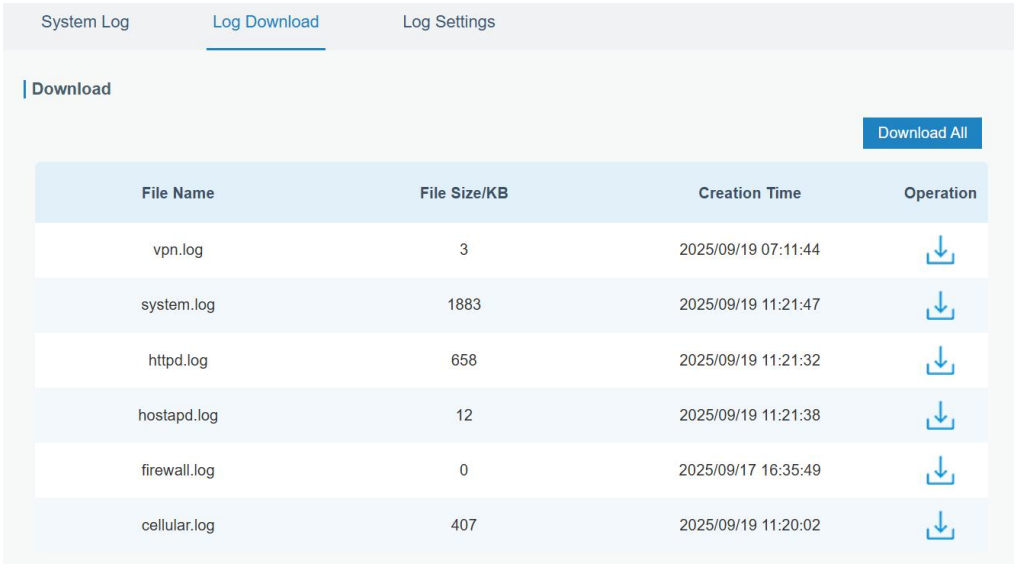


Figure 3-5-3-2

Log Download	
Item	**Description**
Download All	Download all log files.
File Name	Show the name of log files.
File Size/KB	Show the size of log files.
Creation Time	Show the creation time of log files.
Operation	Click to download every log file.

Table 3-5-3-2 System Log Parameter

3.5.3.3 Log Settings

This section explains how to enable remote log server and local log setting.

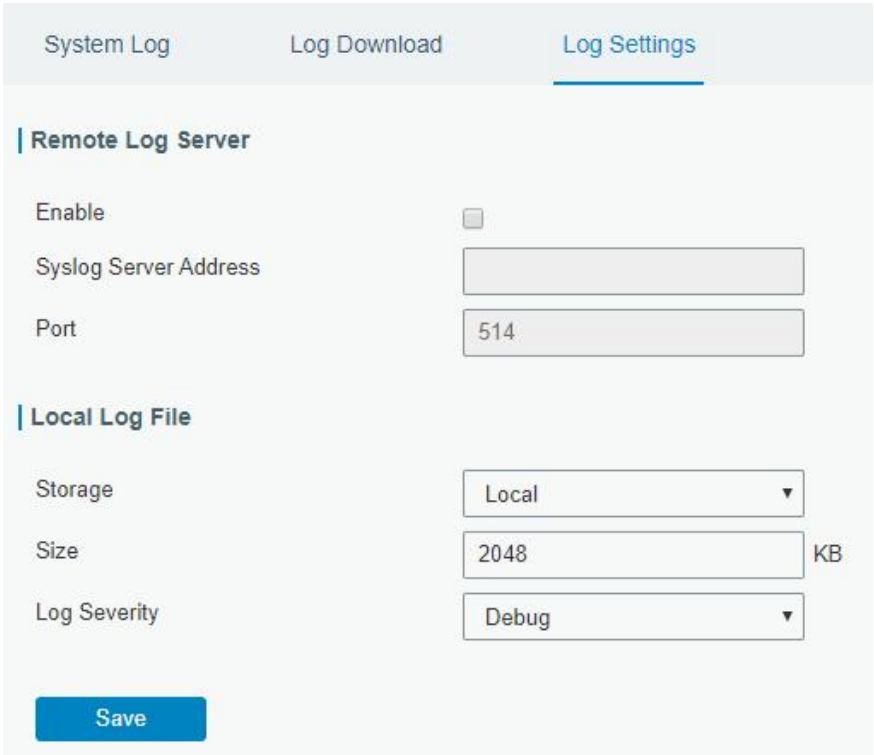


Figure 3-5-3-3

Log Settings	
Item	**Description**
Remote Log Server	
Enable	With “Remote Log Server” enabled, router will send all system logs to the remote server.
Syslog Server Address	Fill in the remote system log server address (IP/domain name).
Port	Fill in the remote system log server port.
Local Log File	
Storage	User can store the log file in memory or TF card.
Size	Set the size of the log file to be stored.
Log Severity	The list of severities follows the syslog protocol.

Table 3-5-3-3 Log Settings Parameters

3.5.4 Upgrade

This section describes how to upgrade the router firmware via web. Generally you don't need to do the firmware upgrade.

Note: any operation on web page is not allowed during firmware upgrade, otherwise the upgrade will be interrupted, or even the device will break down.

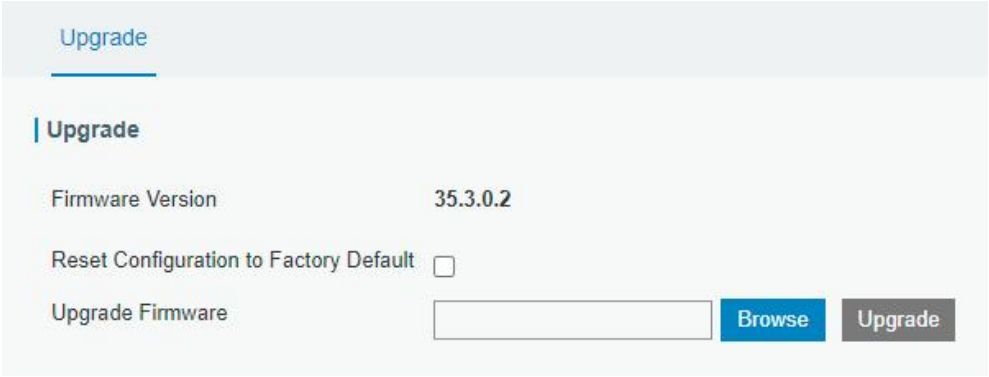


Figure 3-5-4-1

Upgrade	
Item	**Description**
Firmware Version	Show the current firmware version.
Reset Configuration to Factory Default	When this option is checked, the router will be reset to factory defaults after upgrade.
Upgrade Firmware	Click "Browse" button to select the new firmware file, and click "Upgrade" to upgrade firmware.

Table 3-5-4-1 Upgrade Parameters

Related Configuration Example

Firmware Upgrade

3.5.5 Backup and Restore

This section explains how to create a complete backup of the system configurations to a file, restore the config file to the router and reset to factory defaults.

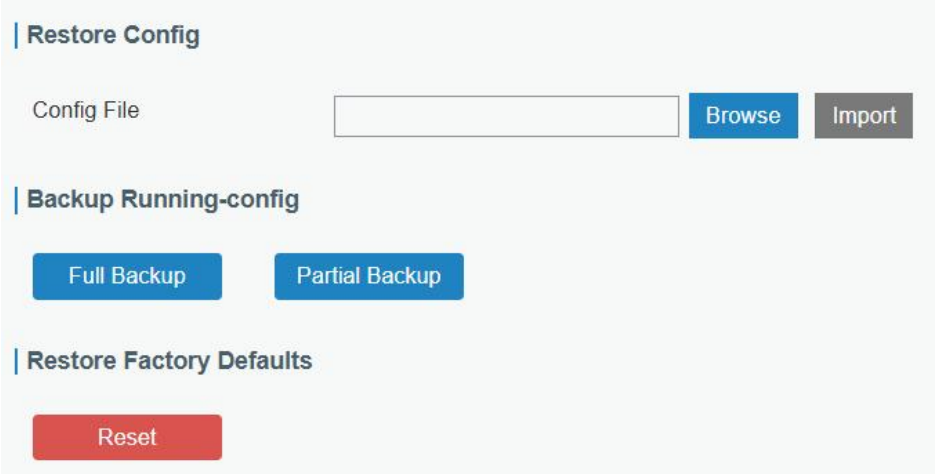


Figure 3-5-5-1

Backup and Restore	
Item	**Description**
Config File	Click "Browse" button to select configuration file, and then click "Import" button to upload the configuration file to the router.
Full Backup	Export the all configurations file to the PC.
Partial Backup	Export all configurations except for the following pages to the PC. Configurations not included in partial backup: ● Network → Interfaces → WAN: All configurations ● Network → Interfaces → WLAN: Configurations when set to AP mode ● System → User Management: All configurations ● System → Device Management → Device Management: Configurations when DeviceHub iPythons selected and activated via authorization code ● System → Device Management → MilesightVPN: All configurations ● APP → Python: All configurations
Reset	Click "Reset" button to reset factory default settings. Router will restart after reset process is done.

Table 3-5-5-1 Backup and Restore Parameters

Related Configuration Example

Restore Factory Defaults

3.5.6 Reboot

On this page you can reboot the router immediately or regularly. We strongly recommend clicking “Save” and “Apply” button before rebooting the router so as to avoid losing the new configuration.

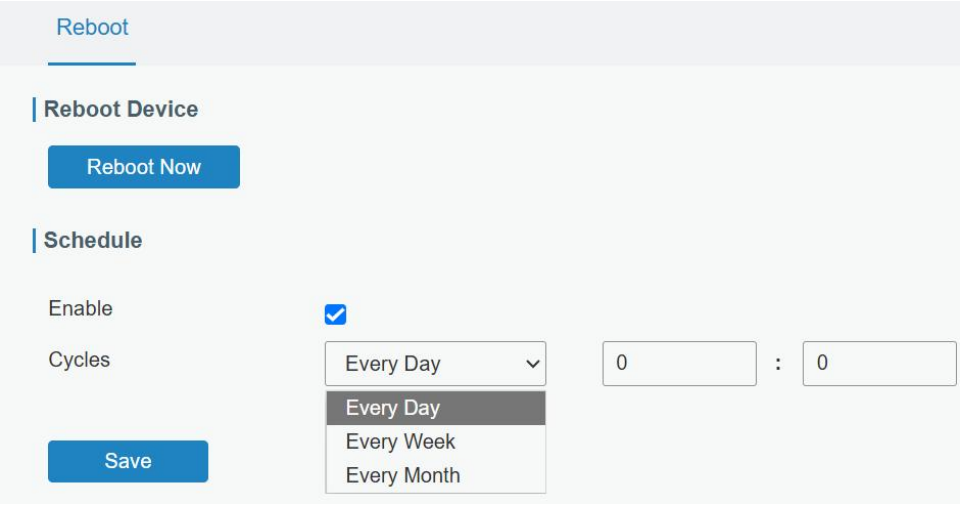


Figure 3-5-6-1

Reboot

Item	Description
Reboot Now	Reboot the router immediately.
Schedule	
Enable	Reboot the router at a scheduled frequency.
Cycles	Select the date and time to execute the schedule.

Table 3-5-2-1 Schedule Parameters

3.6 APP

3.6.1 Python

Python is an object-oriented programming language that has gained popularity because of its clear syntax and readability.

As an interpreted language, Python has a design philosophy that emphasizes code readability, notably using whitespace indentation to delimit code blocks rather than curly brackets or keywords, and a syntax that allows programmers to express concepts in fewer lines of code than it's used in other languages such as C++ or Java. The language provides constructs and intends to enable writing clear programs on both small and large scale.

Users can use Python to quickly generate the prototype of the program, which can be the final interface of the program, rewrite it with a more appropriate language, and then encapsulate the extended class library that Python can call.

This section describes how to view the relevant running status such as App-manager, SDK version, extended storage, etc. Also you can change the App-manager configuration, and import the Python App package from here.

3.6.1.1 Python

Micro SD card must be installed for Python App.

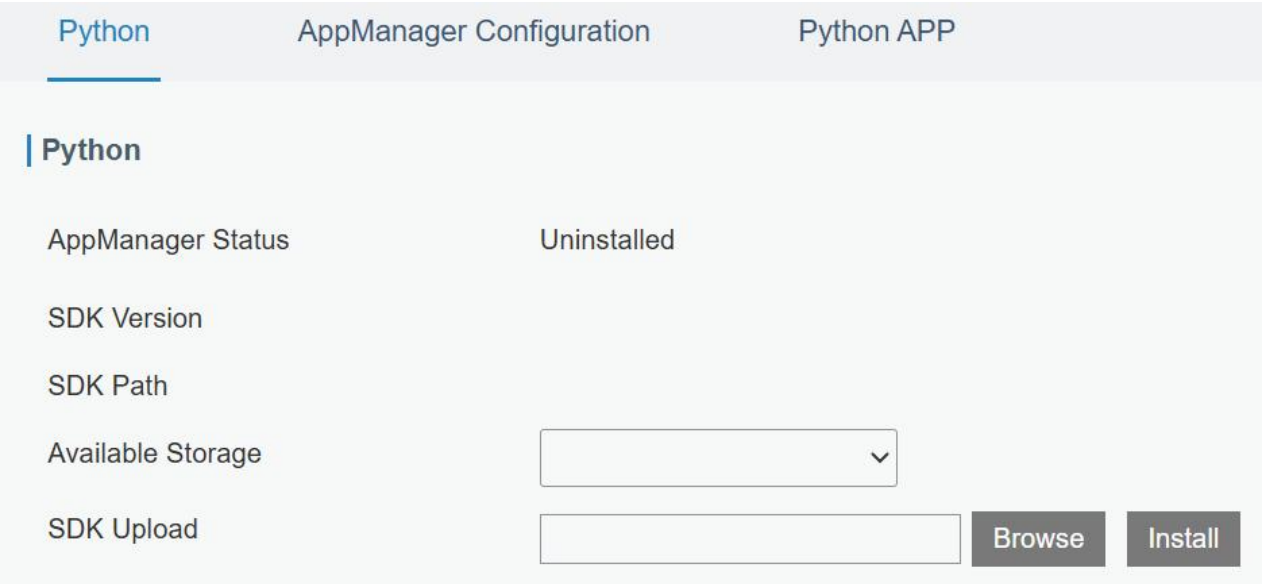


Figure 3-6-1-1

Python	
Item	**Description**
AppManager Status	Show AppManager's running status, like "Uninstalled", "Running" or "Stopped".
SDK Version	Show the version of the installed SDK.
SDK Path	Show the SDK installation path.
Available Storage	Select available storage such as Micro SD to install SDK.
SDK Upload	Upload and install SDK for Python.
Uninstall	Uninstall SDK.
View	View application status managed by AppManager.

Table 3-6-1-1 Python Parameters

3.6.1.2 App Manager Configuration

Figure 3-6-1-2

AppManager Configuration	
Item	**Description**
Enable	After enabling Python AppManager, user can click "View" button on the "Python" webpage to view the application status managed by AppManager.
App Management	
ID	Show the ID of the imported App.
App Command	Show the name of the imported App.
Logfile Size(MB)	User-defined Logfile size. Range: 1-50.
Uninstall	Uninstall APP.
App Status	
App Name	Show the name of the imported App.
App Version	Show the version of the imported App.
SDK Version	Show the SDK version which the imported App is based on.

Table 3-6-1-2 APP Manager Parameters

3.6.1.3 Python App

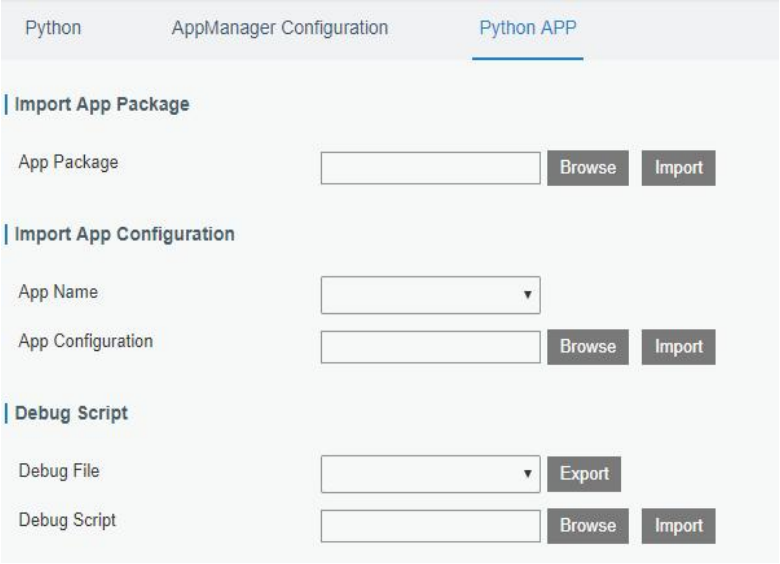


Figure 3-6-1-3

Python APP	
Item	**Description**
App Package	Select App package and import.
App Name	Select App to import configuration.
App Configuration	Select configuration file and import.
Debug File	Export script file.
Debug Script	Select Python script to be debugged and import.

Table 3-6-1-3 APP Parameters

Chapter 4 Application Examples

4.1 Network Connection

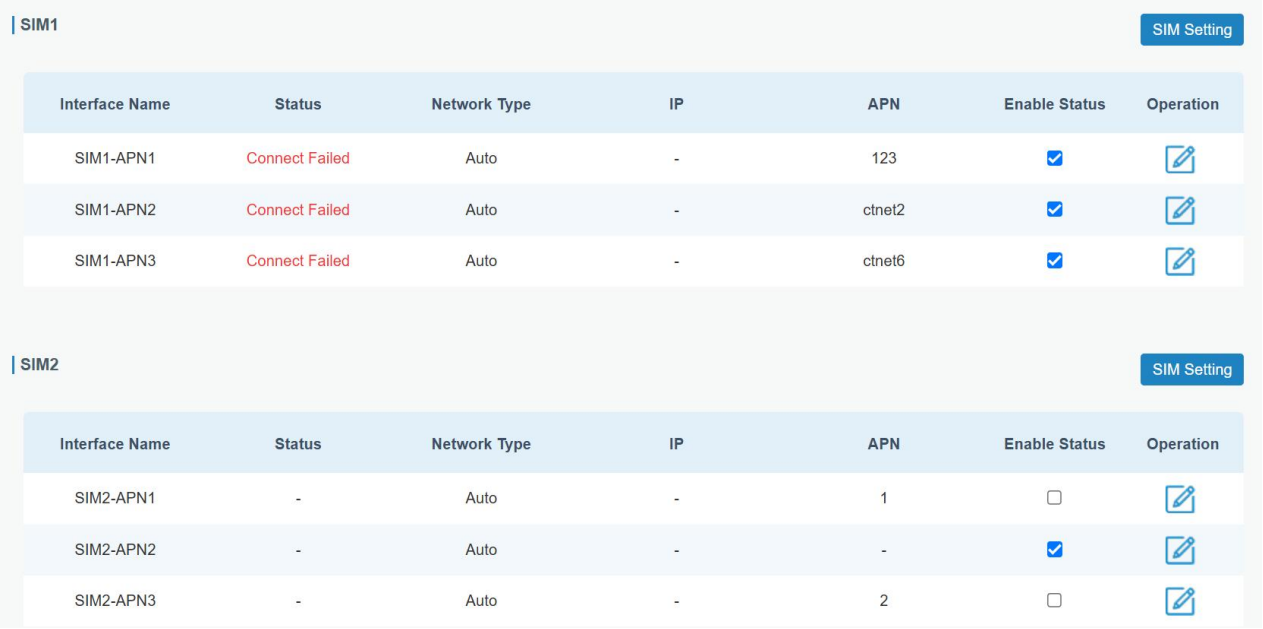
4.1.1 Cellular Connection

The UR32 routers have two cellular interfaces, named SIM1 & SIM2. Only one cellular interface is active at one time. We are about to take an example of inserting a SIM card into SIM1 slot of the UR32 and configuring the router to get Internet access through cellular.

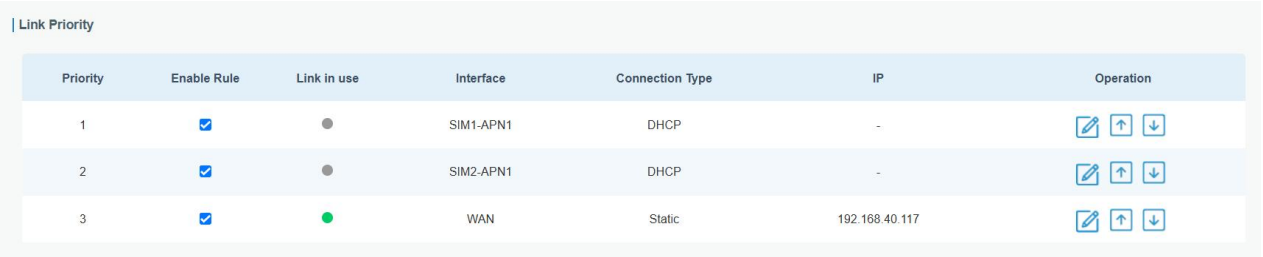
Configuration Steps

1. Ensure the SIM card is inserted well before powering on and all cellular antennas are connected to the correct connectors.

2. Go to **Network > Interface > Cellular > SIM Setting** to configure the SIM info, then click  to configure the cellular interfaces, click **OK** to save configuration.



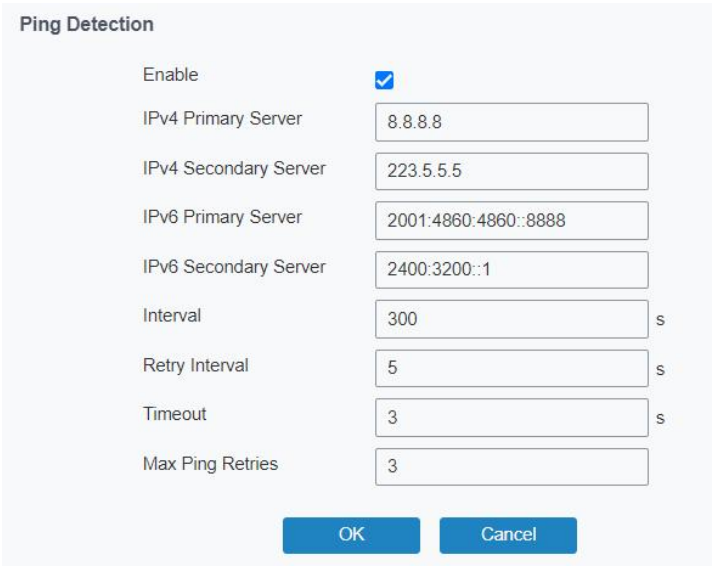
3. Go to **Network > Interface > Link Failover** to enable correspond cellular interface and drag buttons to change link priority.



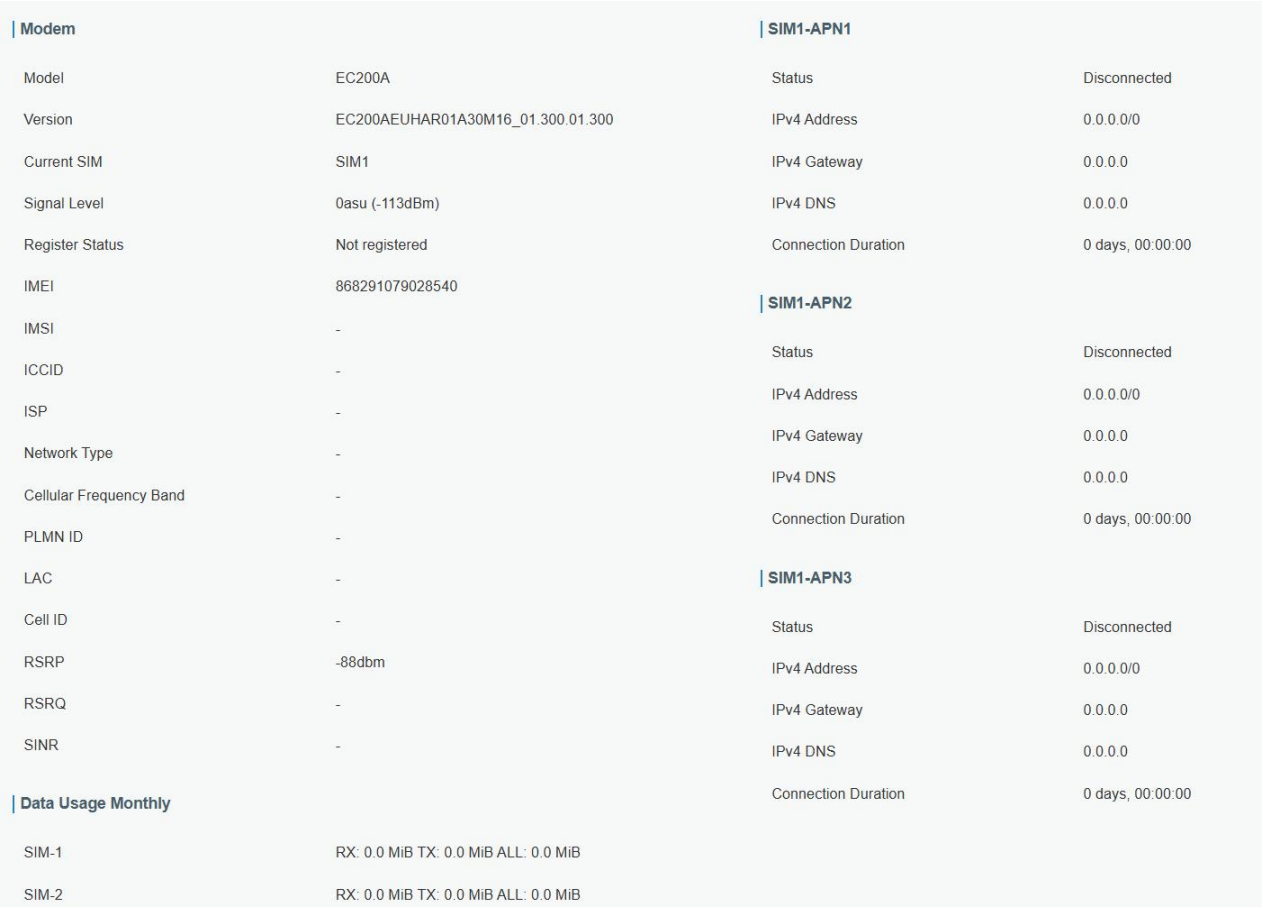
4. Click  to configure ICMP ping detection information. When ping probe is enabled, the router will send ICMP packets to detection server to check if this link is valid. If no response and

exceeding max retries, it will switch to the lower priority link.

Note: if you use private SIM card, please change a private server address or disable the ping probe.



5. Go to **Status > Cellular** to view the status of the cellular connection. If it shows Connected, SIM1-APN1 has dialed up successfully.



Related Topic

Cellular Setting

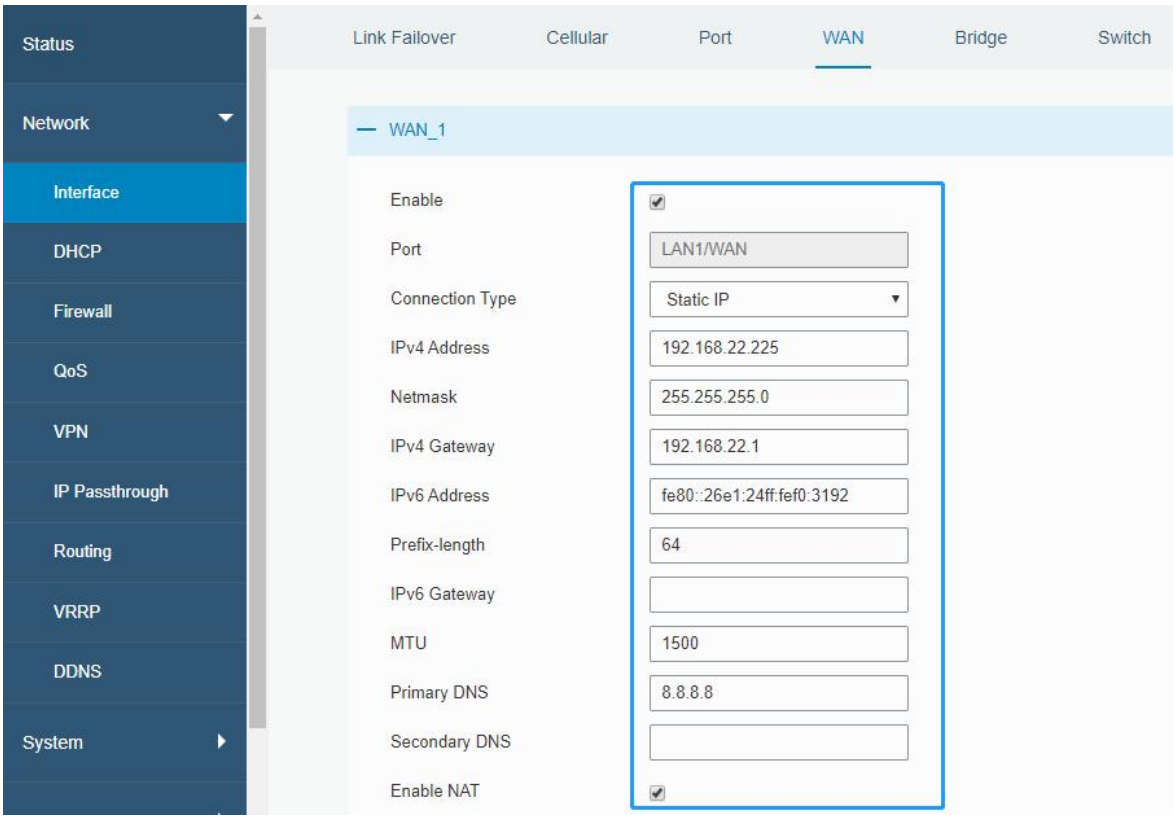
Cellular Status

4.1.2 Ethernet WAN Connection

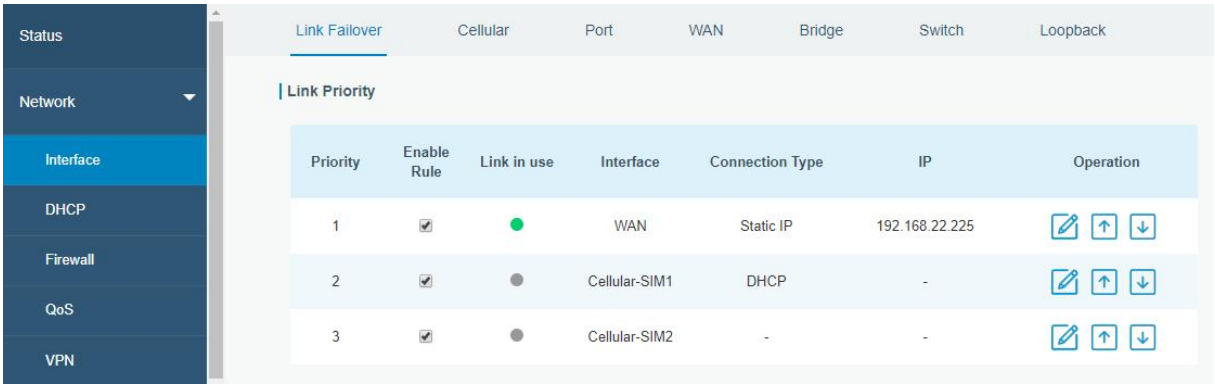
UR32 supports to get Internet access via WAN port.

Configuration Steps

1. Go to **Network > Interface > WAN** to select connection type and configure WAN parameters, then save all settings. The following examples of static IP type, DHCP Client type, and PPPoE type are listed for your reference.



2. Go to **Network > Interface > Link Failover** to enable WAN and drag buttons to change link priority.



Related Topic

WAN Setting

WAN Status

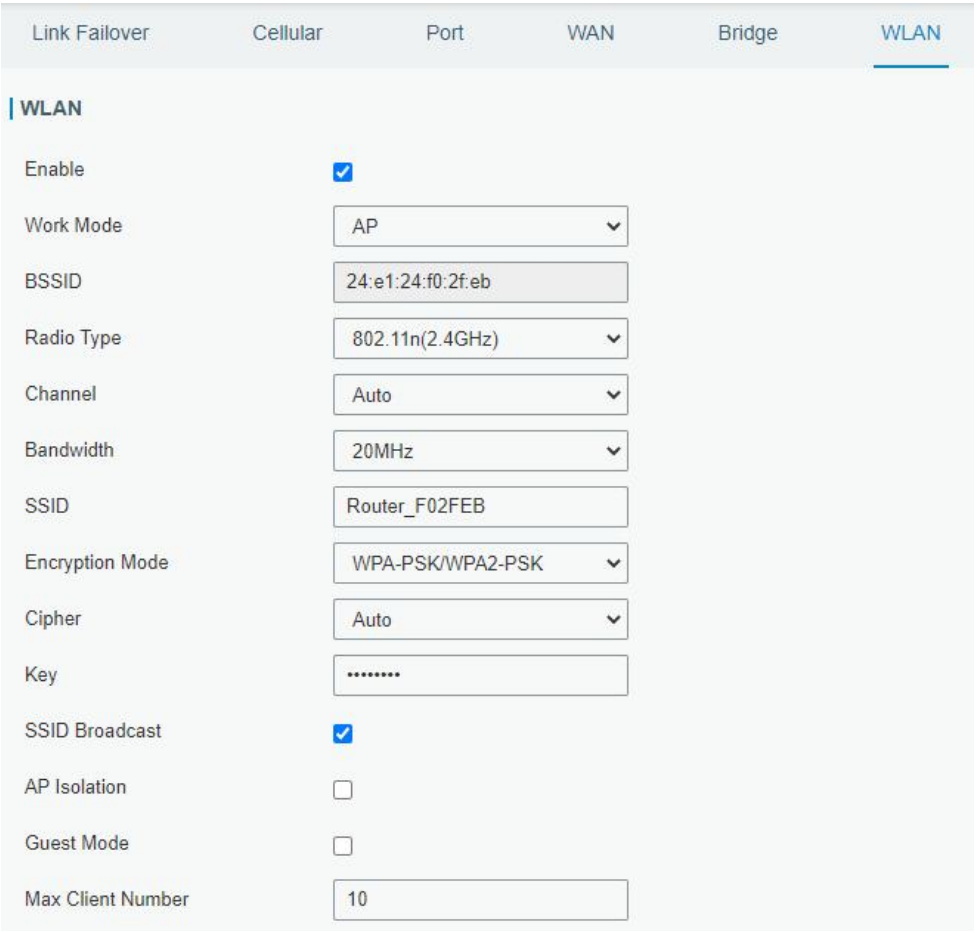
4.2 Wi-Fi Application Example (Only Applicable to Wi-Fi Version)

4.2.1 AP Mode

UR32 supports to work as access point (AP) to provide network access to other devices.

Configuration Steps

1. Go to **Network > Interface > WLAN** to select work mode as AP and define the wireless parameters as required, then save all settings.



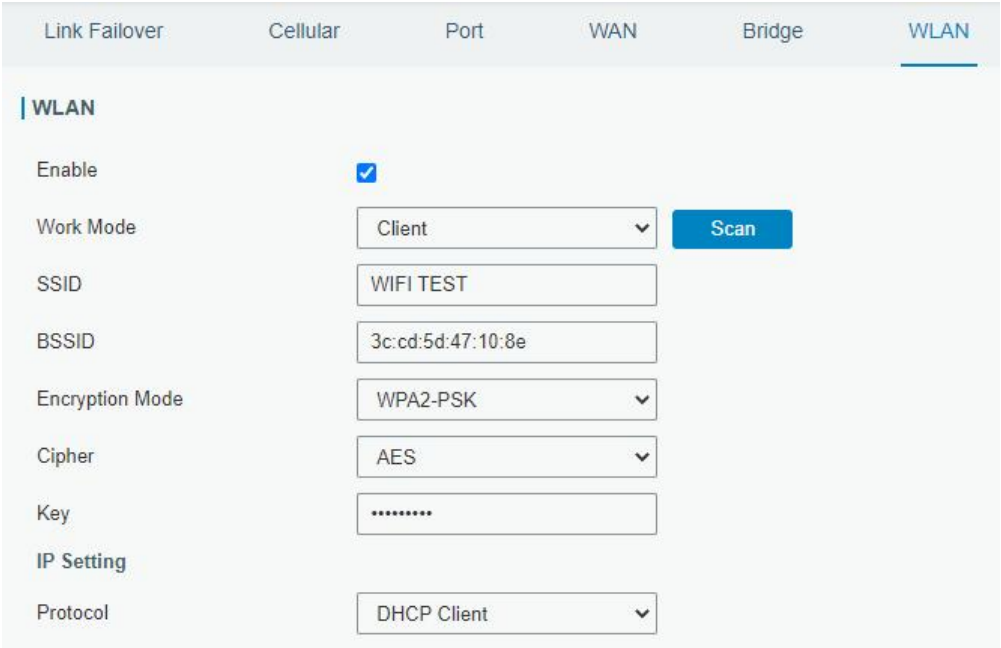
2. Use a smart phone to connect the access point of UR32. Go to **Status > WLAN**, and you can check the AP settings and information of the connected client/user.

4.2.2 Client Mode

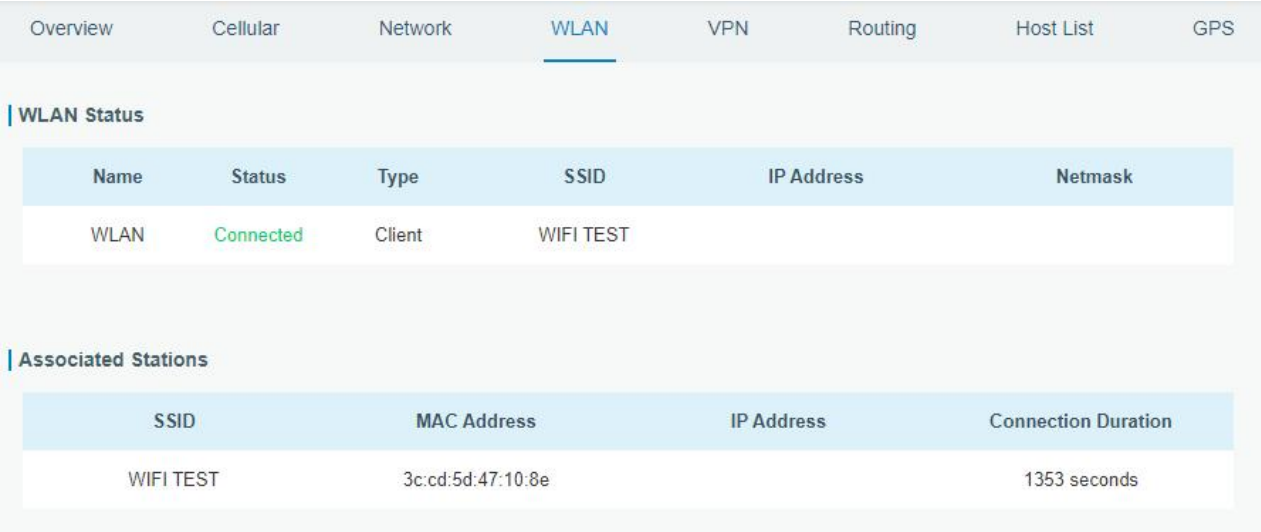
UR32 supports to work as Wi-Fi client to connect to an access point to get Internet access.

Configuration Steps

1. Go to **Network > Interface > WLAN**, click **Scan** to search for access points and click **Join Network**, then save the settings. For some access points, it is necessary to fill in the Wi-Fi password.



2. Go to **Status > WLAN**, and you can check the connection status of the client.



Related Topic

WLAN Setting

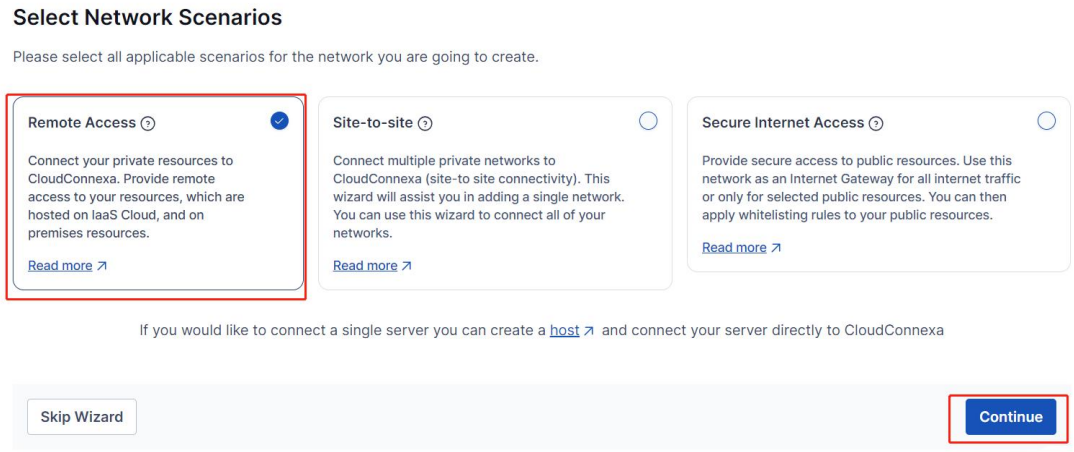
WLAN Status

4.3 OpenVPN Client Application Example

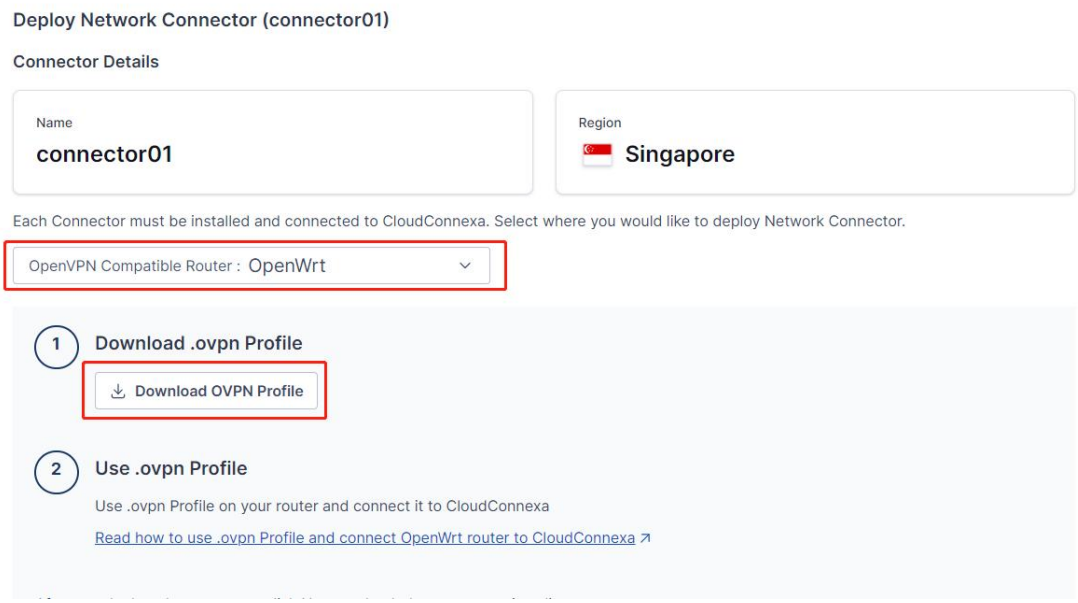
UR32 routers can work as OpenVPN clients or OpenVPN servers. We are about to take an example of configuring an OpenVPN client to connect to OpenVPN CloudConnexa.

Configuration Steps

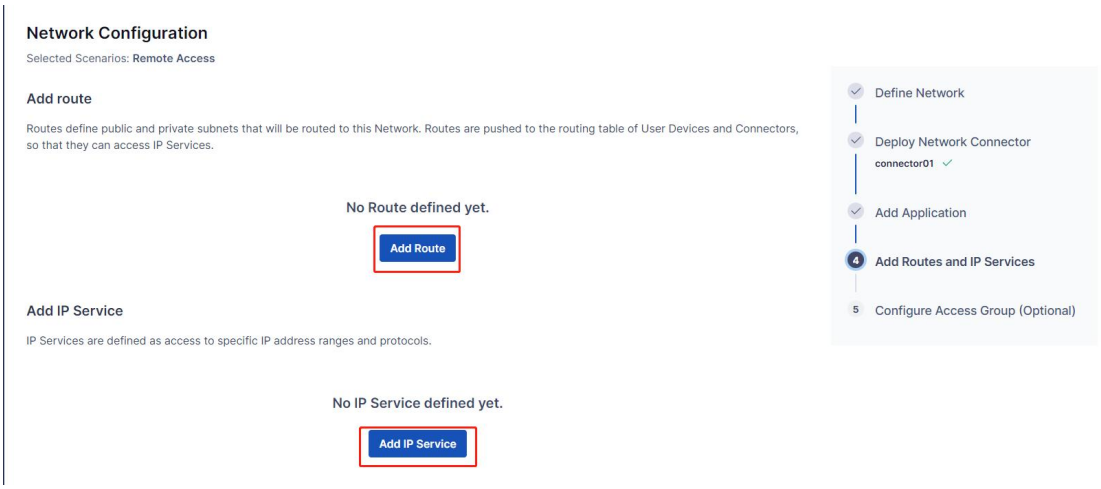
1. Ensure the UR32 has gotten access to the Internet.
2. Log in to the CloudConnexa account, select the Network section and select the service depending on your requirement and follow the wizard to continue the settings.



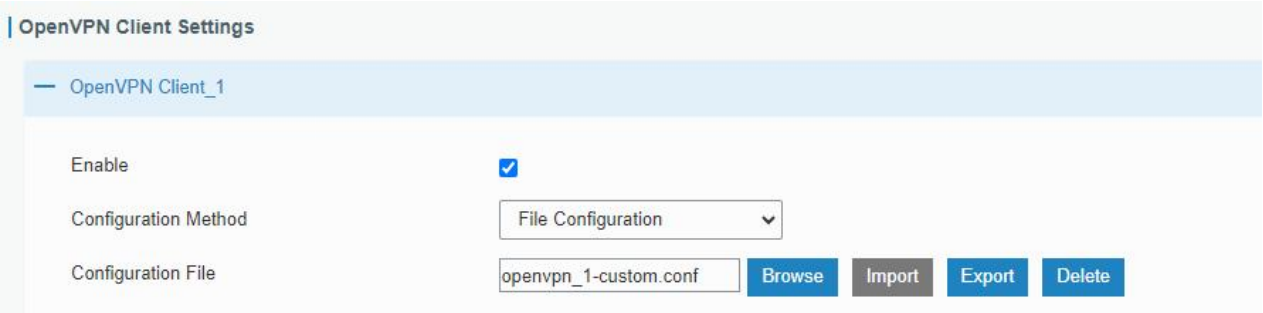
3. Select the provider type as OpenWrt and download the OVPN file.



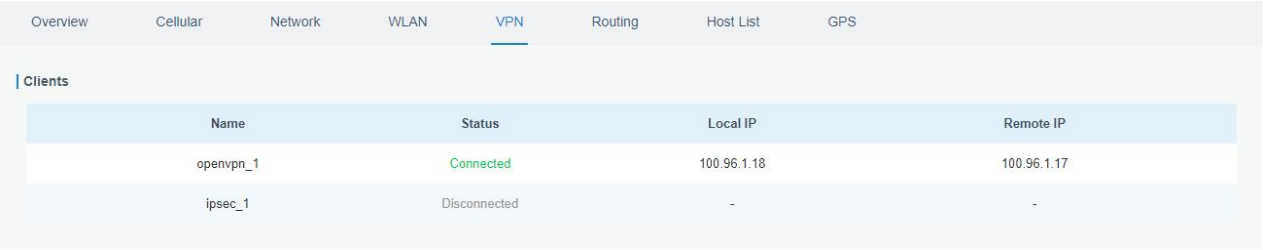
4. If you need to access the terminal devices under subnet, it's necessary to add the route and IP service as LAN subnet of the router.



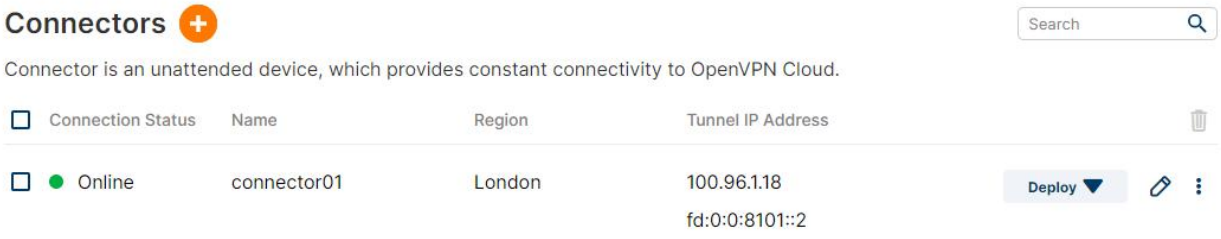
5. Go to **Network > VPN > OpenVPN Client**, select configuration method as File Configuration, then import the OVPN file.



6. Go to **Status > VPN** page to check if the client is connected.



You can also check the connection status on CloudConnexa.



Related Topic

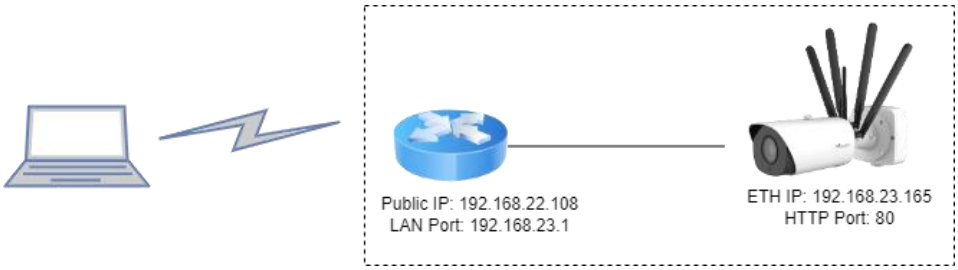
OpenVPN Client

VPN Status

4.4 NAT Application Example

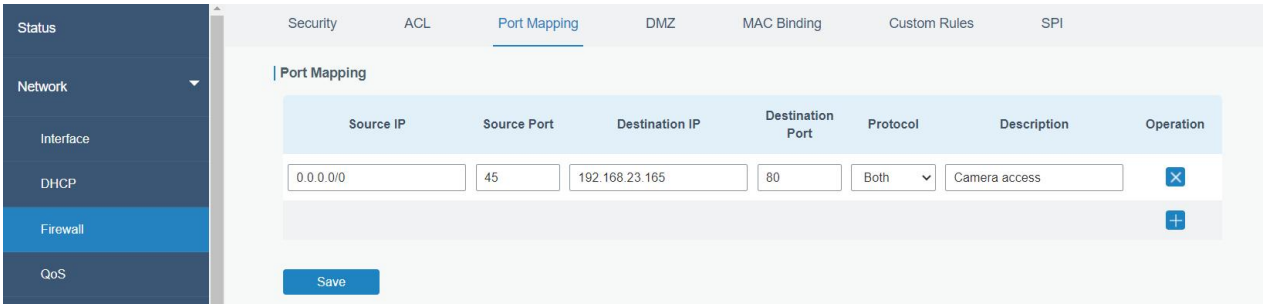
Example

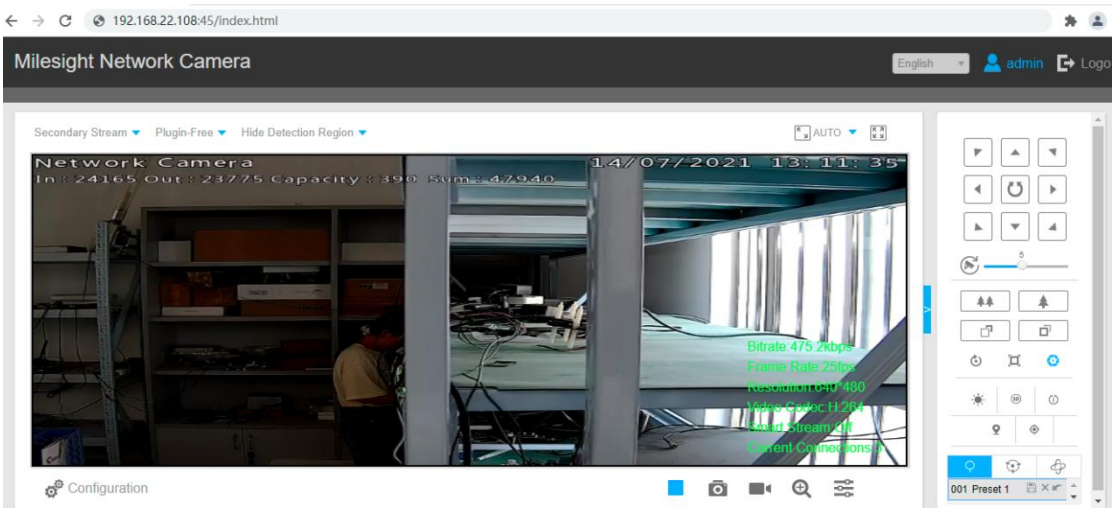
An UR32 router can access to the Internet via cellular and get a public IP address. LAN port is connected with an IP camera whose IP address is 192.168.23.165 and HTTP port is 80. This IP camera can be accessed by public IP address via the below port mapping settings.



Configuration Steps

Go to **Firewall > Port Mapping** and configure port mapping parameters as below. Source IP address 0.0.0.0/0 means all external addresses are allowed to access. After that, users can use public IP: external port to access the IP camera.





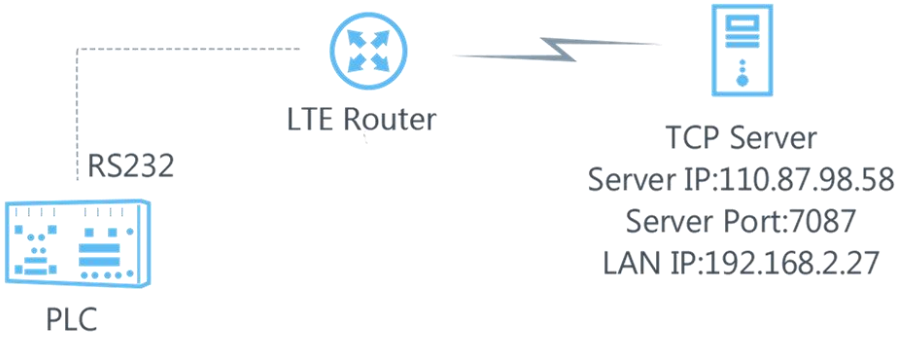
Related Topic

Port Mapping

4.5 DTU Application Example

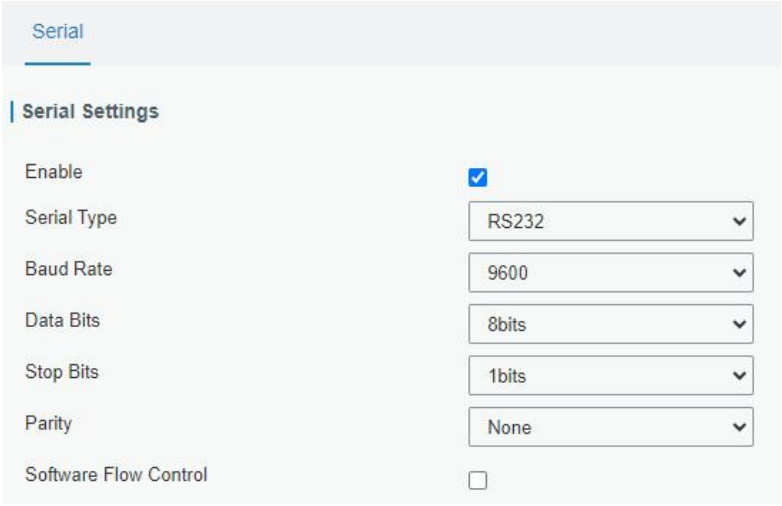
Example

A PLC is connected with the UR32 via RS232 and need to forward the data to a remote TCP server transparently.

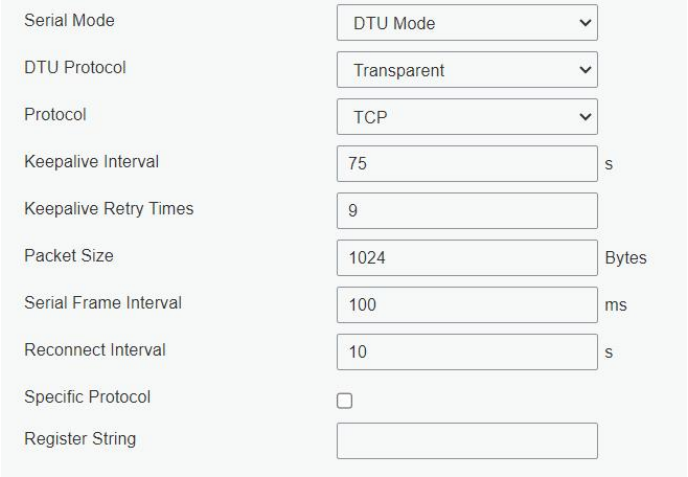


Configuration Steps

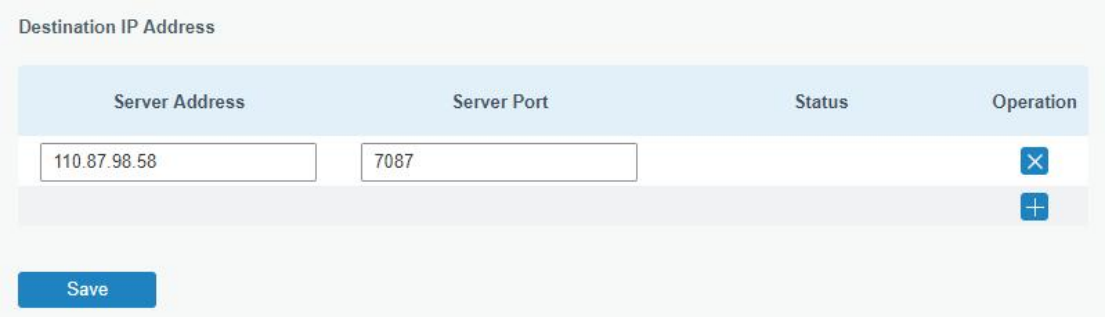
1. Go to **Service > Serial Port > Serial1**, enable Serial 1 and configure serial port parameters. The serial port parameter shall be kept in consistency with those of PLC, as shown in figure below.



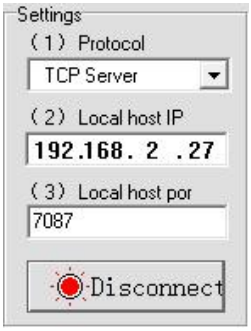
2. Configure Serial Mode as DTU Mode, DTU protocol as Transparent and protocol as TCP.



3. Configure TCP server IP and port.



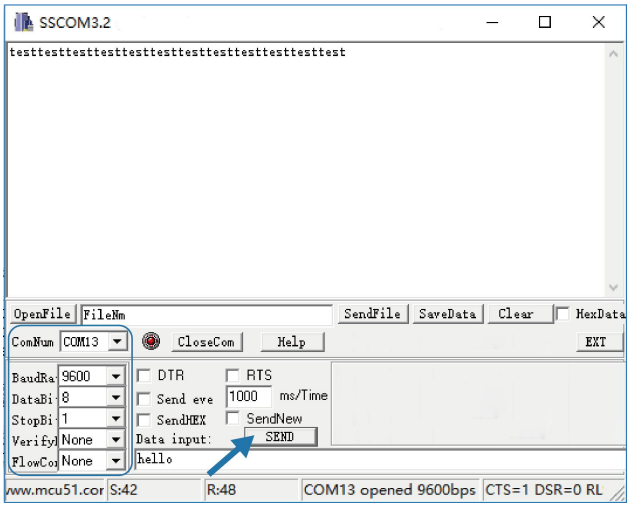
4. Start TCP server on PC. Take **Netassist** test software as example. Make sure port mapping is already done.



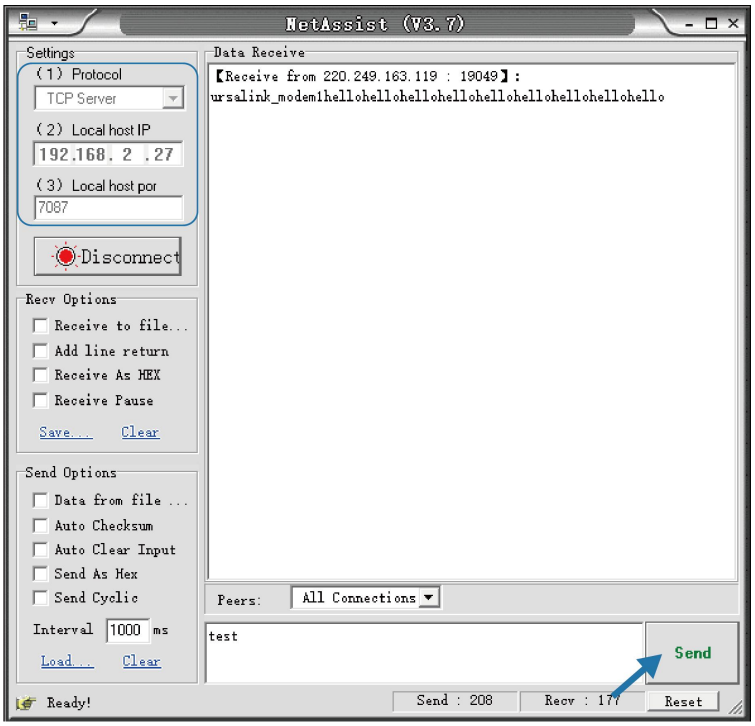
5. Connect the UR32 to PC via RS232 for PLC simulation. Then start **sscom** software on the PC to test communication through serial port.

6. After connection is established between the UR32 and the TCP server, you can send data between sscom and Netassit.

PC side



TCP server side



7. After serial communication test is done, you can connect PLC to RS232 port of the UR32 for test.

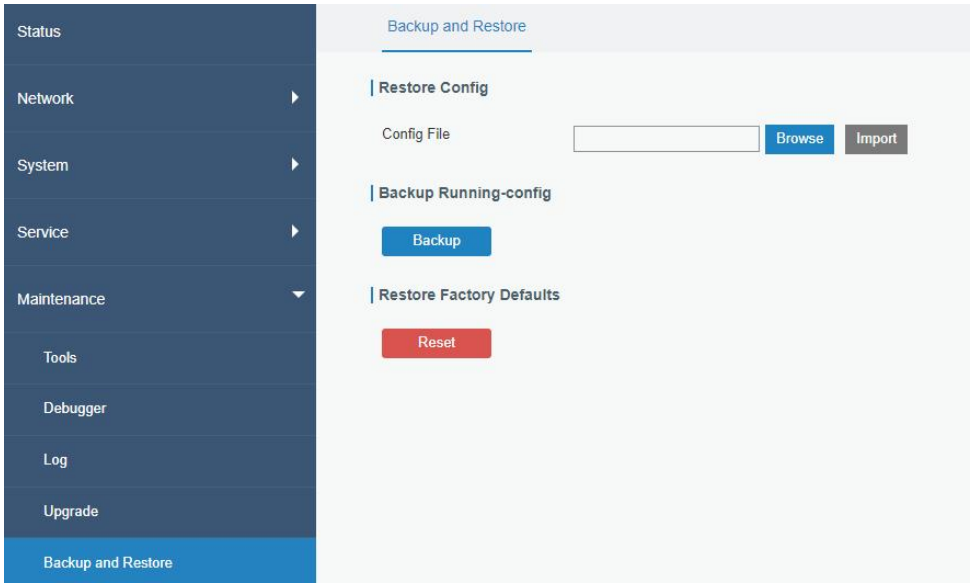
Related Topic

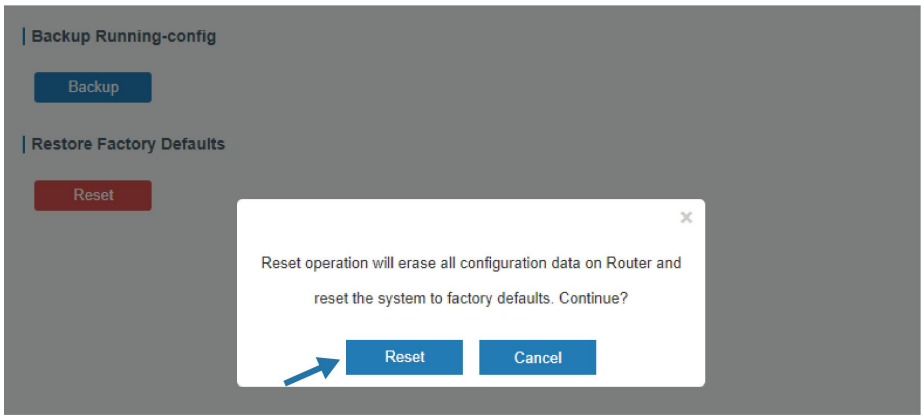
Serial Port

4.6 Restore Factory Defaults

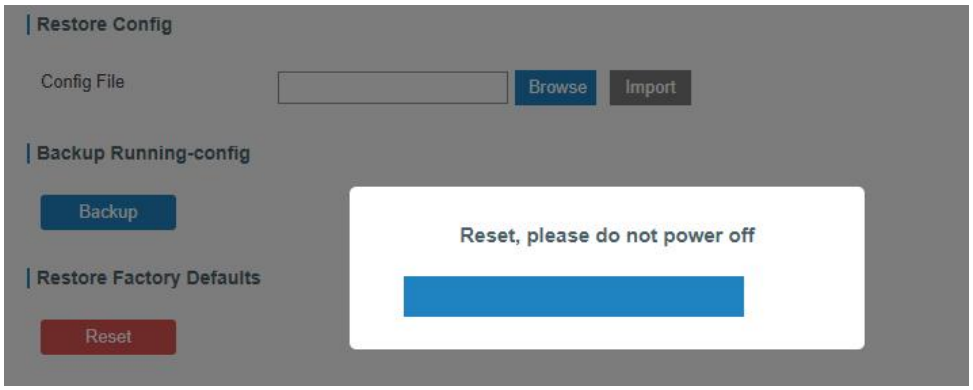
Method 1:

Log in web interface, and go to **Maintenance > Backup and Restore**, click **Reset** button.
You will be asked to confirm if you'd like to reset it to factory defaults. Then click **Reset** button.





Then the router will reboot and restore to factory settings immediately.



Please wait till the SYSTEM LED blinks slowly and login page pops up again, which means the router has already been reset to factory defaults successfully.

Related Topic

Restore Factory Defaults

Method 2:

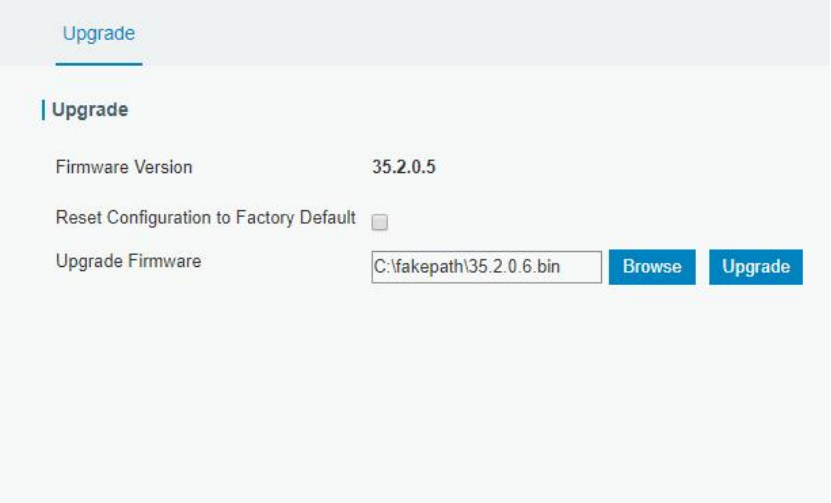
Locate the reset button on the router, press and hold the reset button for more than 5s until the LED blinks.

4.7 Firmware Upgrade

It is suggested that you contact Milesight technical support first before you upgrade router firmware. After getting firmware file please refer to the following steps to complete the upgrade.

1. Go to **Maintenance > Upgrade**, click **Browse** and select the correct firmware file from the PC.
2. Click **Upgrade** and the router will check if the firmware file is correct. If it's correct, the firmware will be imported to the router, and then the router will start to upgrade.

Note: It is recommended to check the box of Reset Configuration to Factory Default before upgrade.



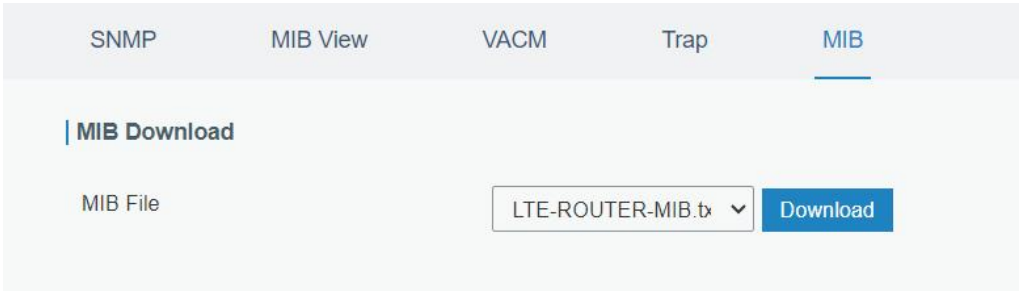
Related Topic

Upgrade

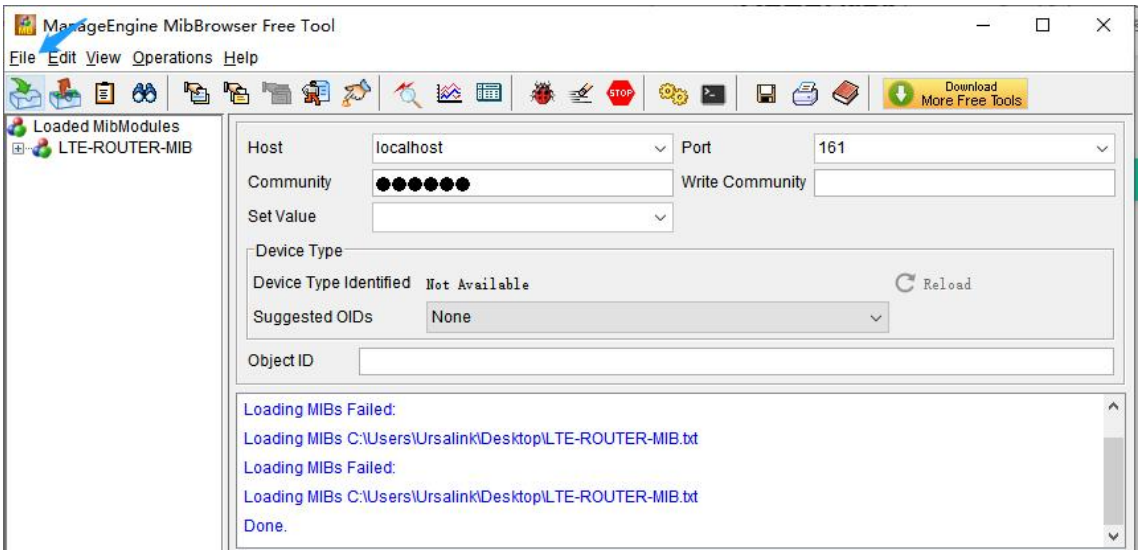
4.8 SNMP Application Example

Before you configure SNMP parameters, please download the relevant MIB file from the UR32's WEB GUI first, and then upload it to any software or tool which supports standard SNMP protocol. Here we take ManageEngine MibBrowser Free Tool as an example to access the router to query cellular information.

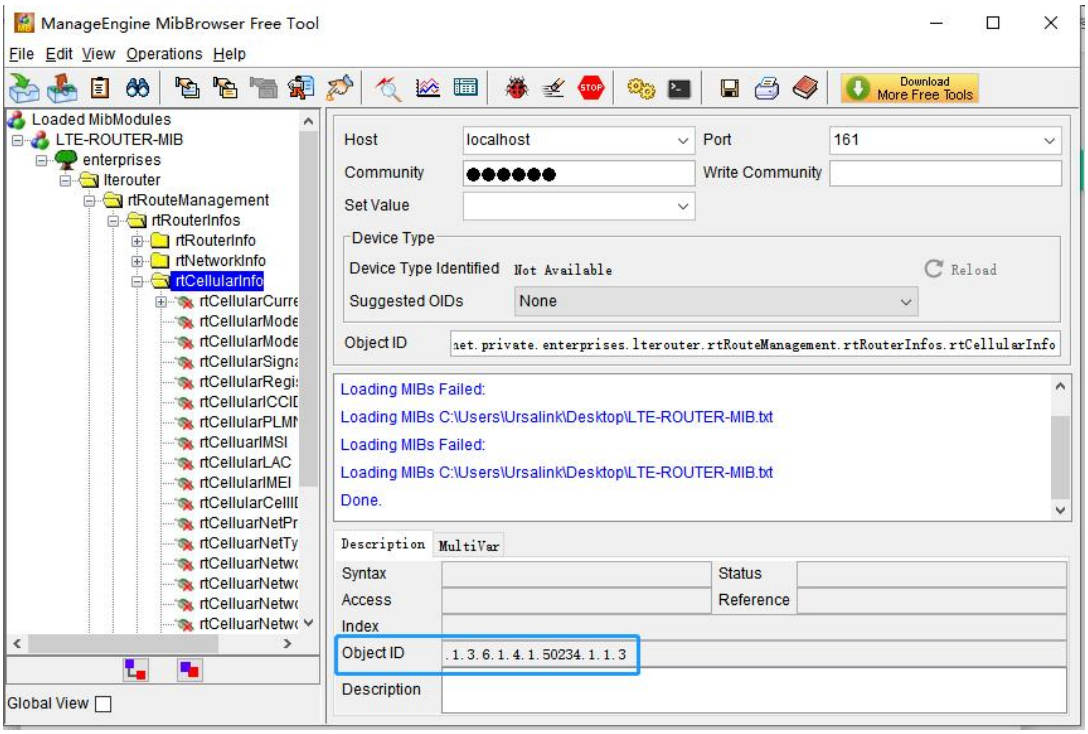
1. Go to **Service > SNMP > MIB** and download the MIB file **LTE-ROUTER-MIB.txt** to PC.



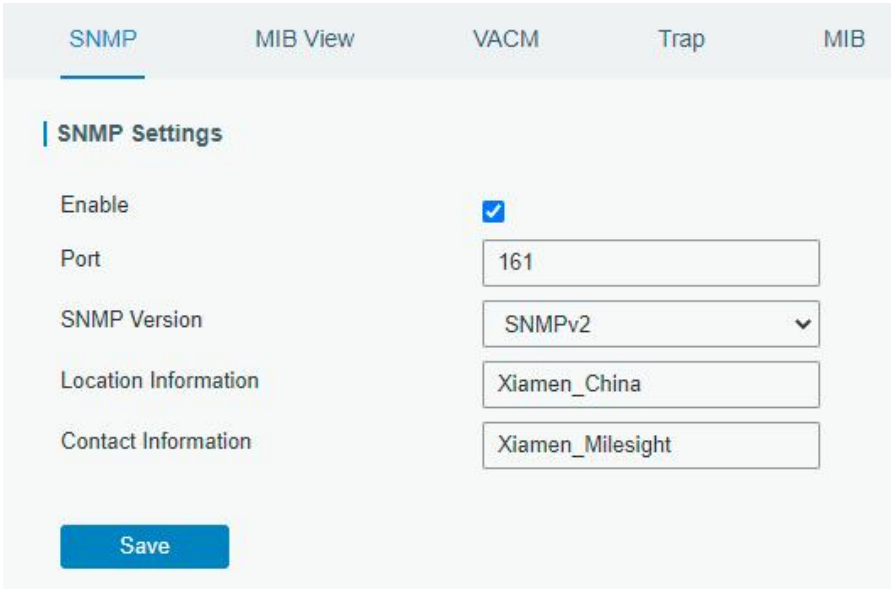
2. Start ManageEngine MibBrowser Free Tool on the PC. Click **File > Load MIB** on the menu bar. Then select **LTE-ROUTER-MIB.txt** file from PC and upload it to the software.



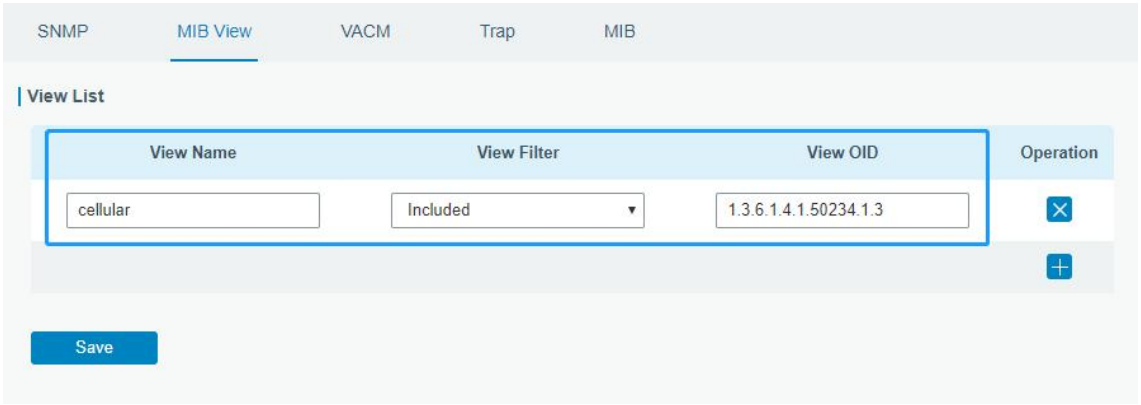
Click the "+" button beside LTE-ROUTER-MIB, which is under the **Loaded MibModules** menu, and find **usCellularinfo**. And then you will see the OID of cellular info is ".1.3.6.1.4.1.50234", which will be filled in the MIB View settings.



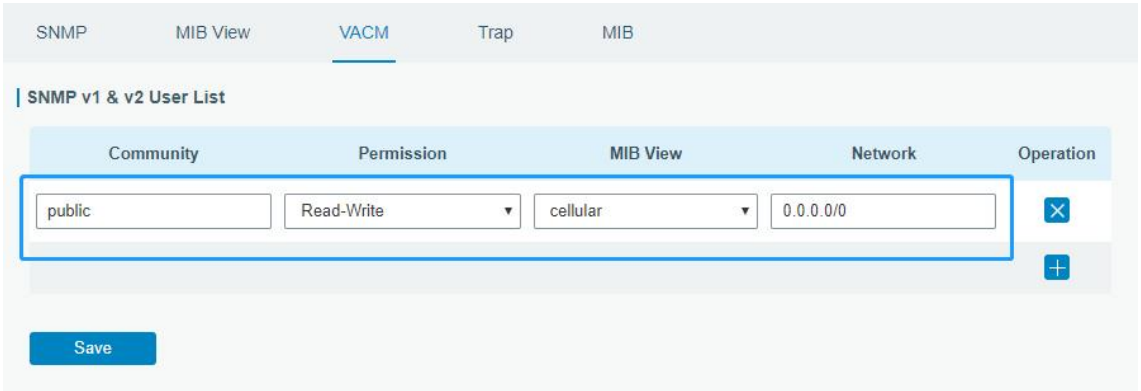
3. Go to **Service > SNMP > SNMP** to enable SNMP feature.



4. Click  to add a new MIB view and define the view to be accessed from the outside network. Then click “Save” button.

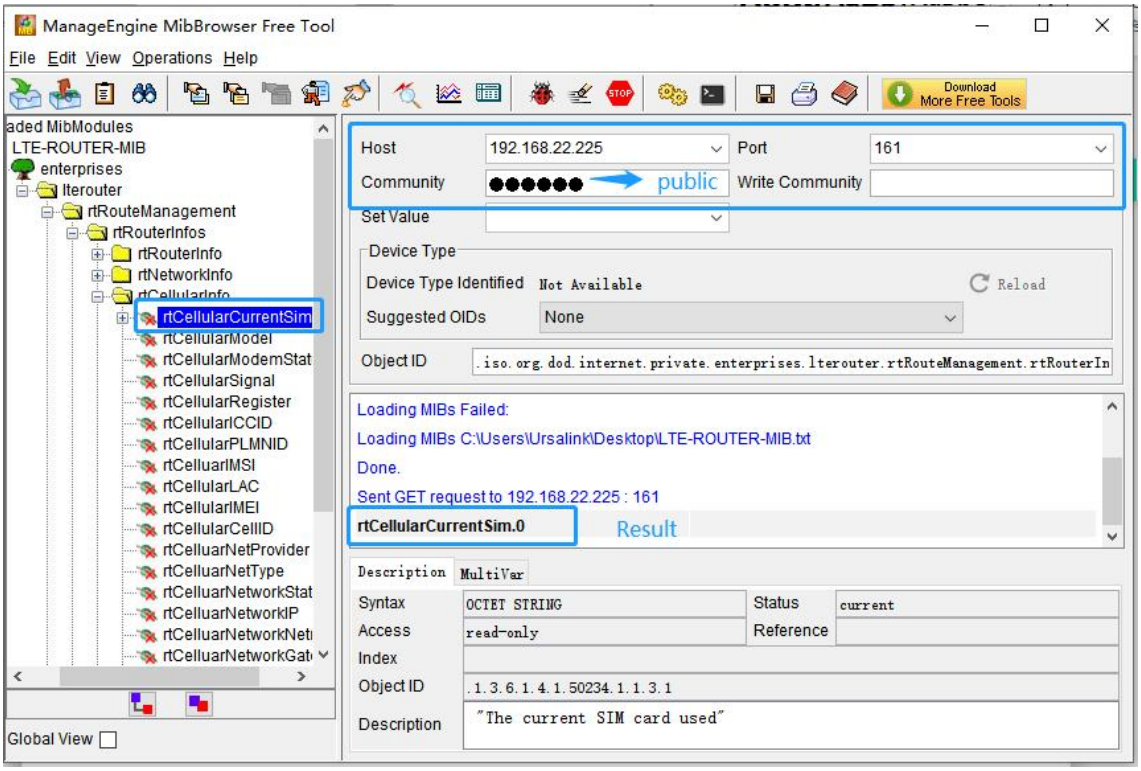


5. Click  to add a new VACM setting to define the access authority for the specified view from the specified outside network, then save all settings.



6. Go to MibBrowser, enter host IP address, port and community. Right click **usCellular CurrentSim** and then click **FET**. Then you will get the current SIM info on the result box. You can get other

cellular info in the same way.



Related Topic

SNMP

4.9 VRRP Application Example

Application Example

A Web server requires Internet access through the UR32 router. To avoid data loss caused by router breakdown, two UR32 routers can be deployed as VRRP backup group, so as to improve network reliability.

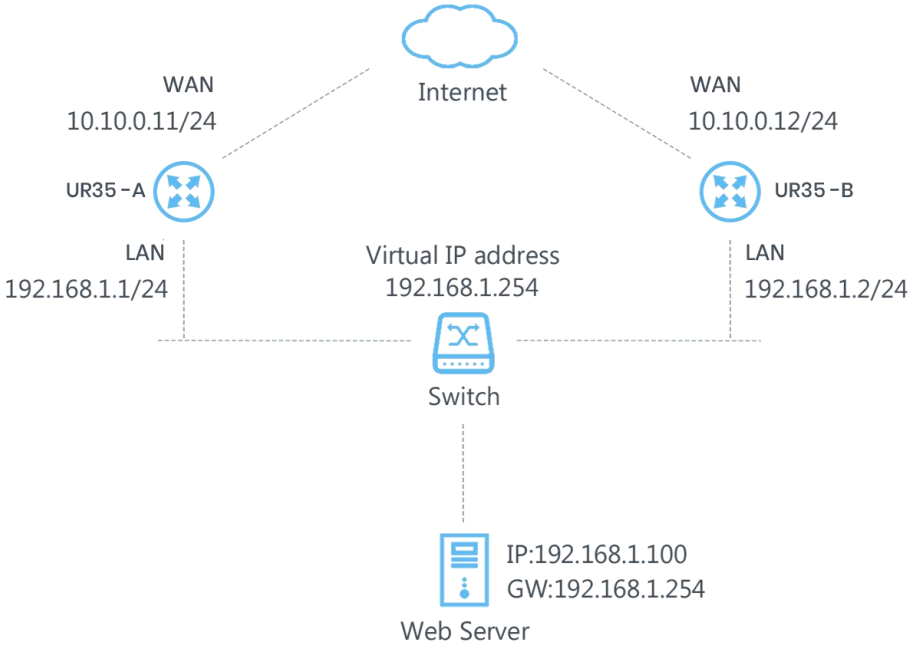
VRRP group:

WAN ports of the UR32 Router A and Router B are connected to the Internet via wired network. And LAN ports of them are connected to a switch.

Virtual IP is 192.168.1.254/24.

Router	Virtual Router ID (Same for A and B)	Port connected with switch	LAN IP Address	Priority	Preemption Mode
A	1	LAN2	192.168.1.1	110	Enable
B	1	LAN2	192.168.1.2	100	Disable

Refer to the topological below.

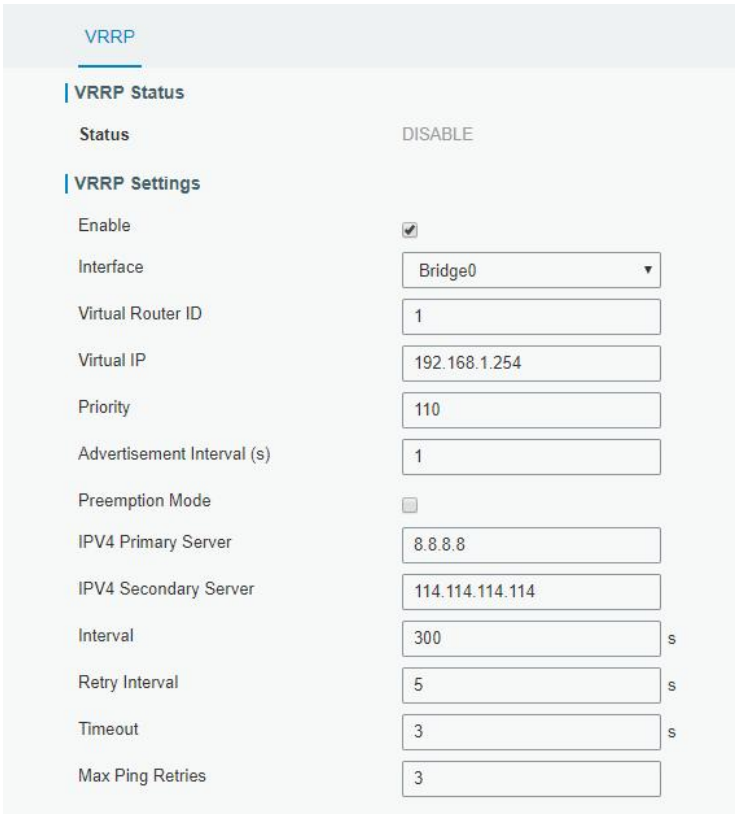


Configuration Steps

Router A Configuration

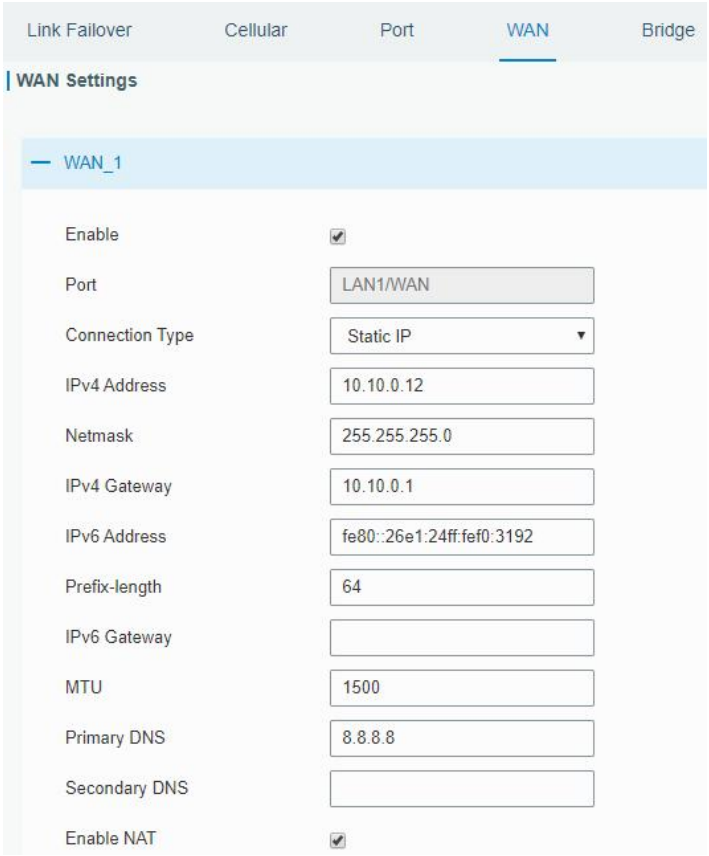
1. Go to **Network > Interface > WAN** and configure wired WAN connection as below.

2. Go to **Network > VRRP > VRRP** and configure VRRP parameters as below.

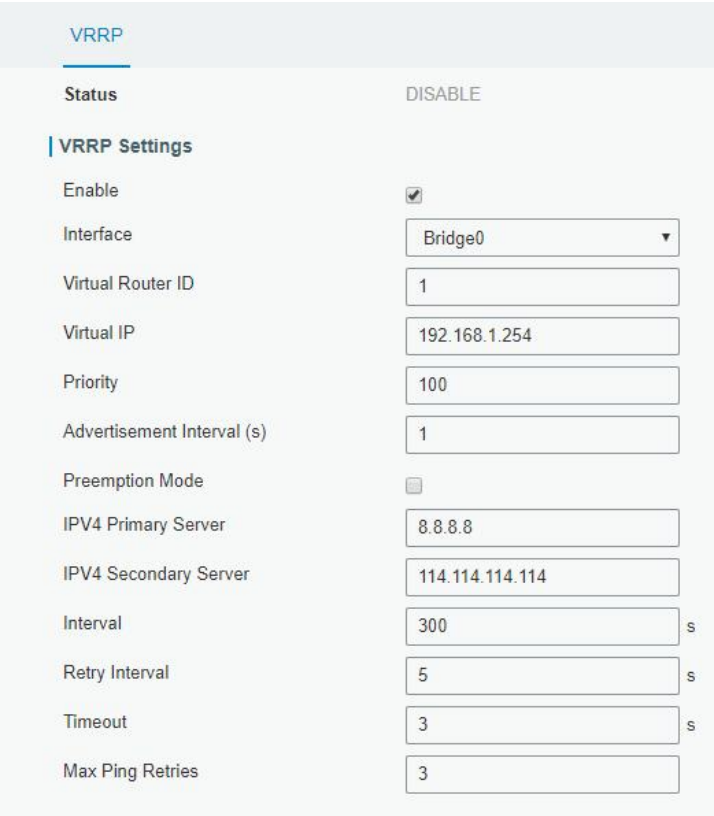


Router B Configuration

1. Go to **Network > Interface > WAN** and configure wired WAN connection as below.



2. Go to **Network > VRRP > VRRP** and configure VRRP parameters as below.



Once you complete all configurations, click **Apply** button on the top-right corner to make changes take effect.

Result: normally, A is the master router, used as the default gateway. When the power of Router A is down or Router A suffers from failure, Router B will become the master router, used as the default gateway. With Preemption Mode enabled, Router A will be master and Router B will demote back to be the backup once Router A can access the Internet again.

Related Topics

VRRP Setting

4.10 QoS Application Example

Example

Configure the UR32 router to distribute local preference to different FTP download channels. The total download bandwidth is 75000 kbps.

Note: the "Total Download Bandwidth" should be less than the real maximum bandwidth of WAN or cellular interface.

FTP Server IP & Port	Percent	Max Bandwidth(kbps)	Min Bandwidth(kbps)
110.21.24.98:21	40%	30000	25000
110.32.91.44:21	60%	45000	40000

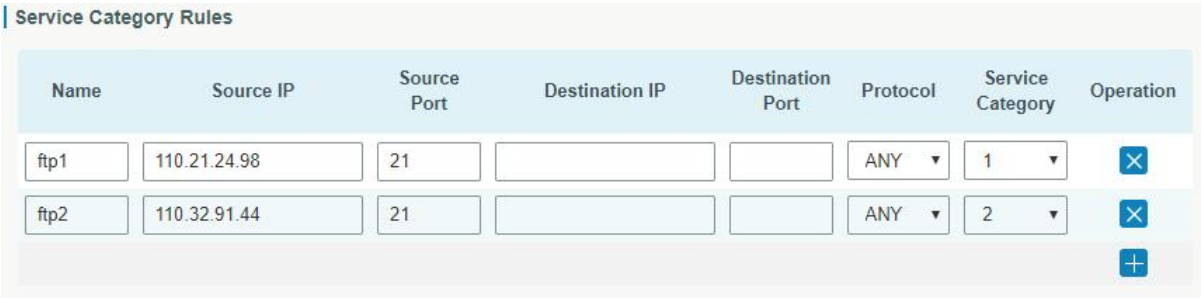
Configuration Steps

1. Go to **Network > QoS > QoS(Download)** to enable QoS and set the total download bandwidth.

2. Click "+" to set up service classes.

Note: the percents must add up to 100%.

3. Click "+" to set up service category rules.



Note:

IP/Port: null refers to any IP address/port.

Click **Save** and **Apply** button.

Related Topic

QoS Setting

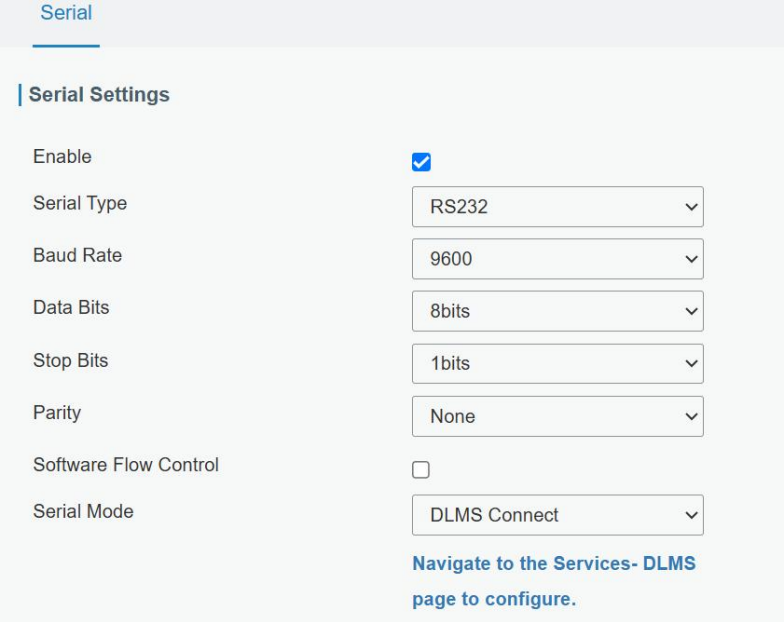
4.11 DLMS Client Example

UR32 routers can work as DLMS clients. We are about to take an example of configuring router to read data from meters and upload it to the platform.

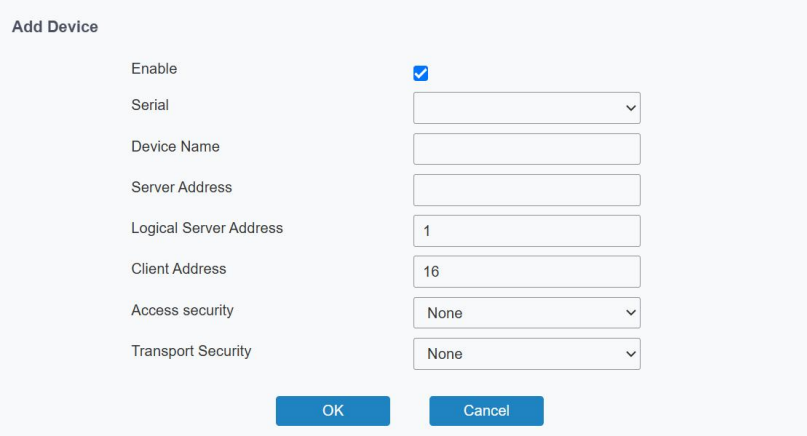
Configuration Steps

1. Connect the meter to the serial port of the router.

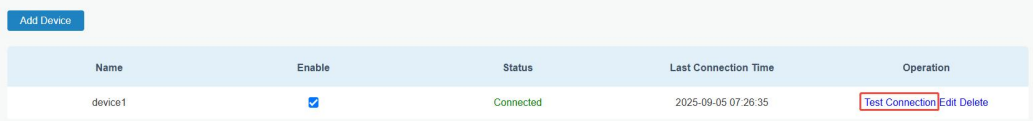
2. Go to **Service > Serial Port > Serial**, enable Serial and configure serial port parameters. The serial port parameters must be consistent with those of the DLMS meter. Then configure Serial Mode as DLMS Connection, and click “Navigate to the Services- DLMS page to configure”.



3. Jump to **DLMS > Physical Device Settings**, click “Add Device” to create a new DLMS physical device interface and configure device parameters.

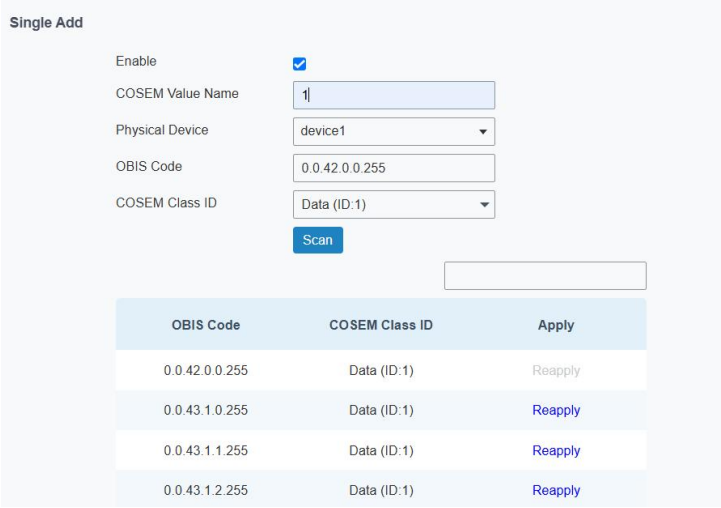


After configuring the DLMS physical device, press the "Test Connection" button to verify whether the configuration is correct. If the connection fails, an error message will be returned to prompt the user to reconnect or modify the configuration parameters.

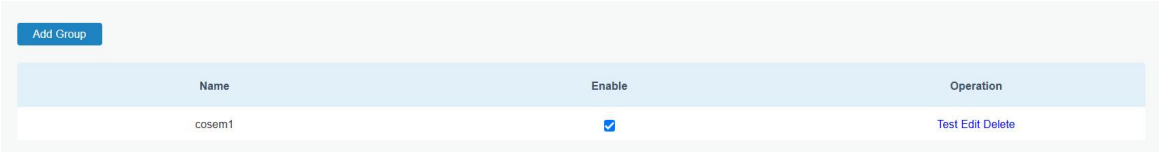


4. Go to **DLMS > COSEM Group Settings**, click “Add Group” to create a new DLMS group and configure how frequently you want to read the data from the devices.

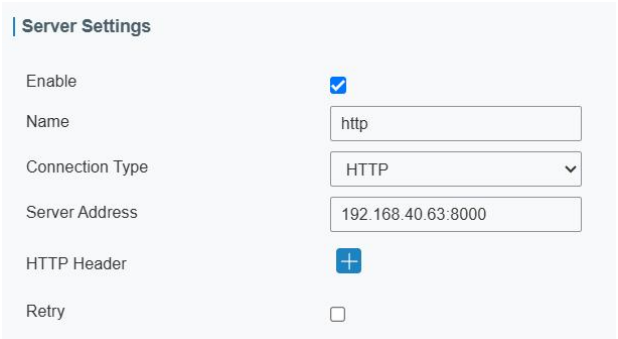
Click “Single Add” button, you can configure the COSEM value name and select the physical value device created earlier. Then click the “Scan” button, the COSEM object of the selected device will be displayed below. When you click the "Reapply" button, the OBIS Code and Class ID will be automatically filled in the above configuration items.

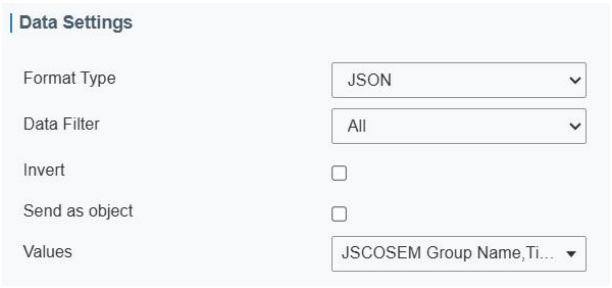


Once all of the configuration is enabled and saved, we can re-open the COSEM group we have created, and press the TEST button.

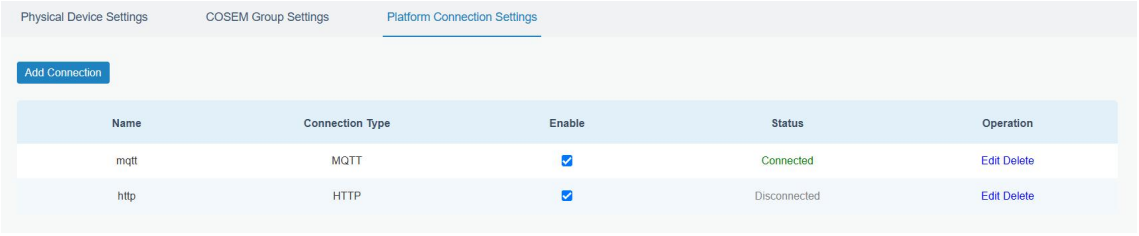


5. Go to **DLMS > Platform Connection Settings**, click “Add Connection” to create a new platform connection and configure the parameters.





Check if the platform is connected.



Related Topic

Serial Port

[END]