Industrial Router Ultra Series

UR75

User Guide

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

UR75 is in conformity with the essential requirements and other relevant provisions of the CE 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
Nov. 25, 2022	V 3.0	Initial version based on hardware 3.x
Jan. 17, 2023	V 3.1	1. Web GUI Design Change 2. Add LT2P and PPTP VPN client feature 3. Add VLAN feature 4. Add HTTPS certificate import feature

Contents

Chapter 1 Product Introduction

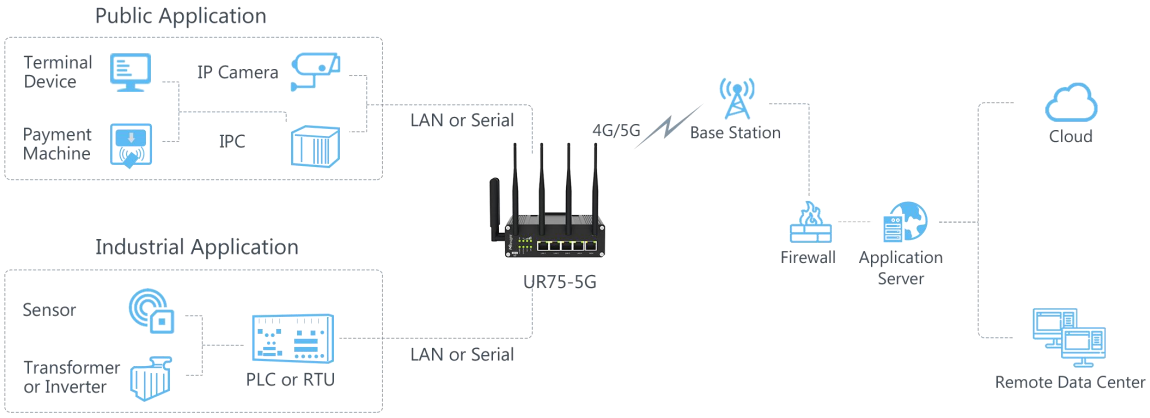
1.1 Overview

UR75 is an industrial cellular router with embedded intelligent software features that are designed for multifarious M2M/IoT applications. Upgraded to the latest cellular technology - 5G, the UR75 makes it possible to enjoy ultra-fast broadband access with a 5G cellular network.

Adopting high-performance and low-power consumption industrial grade CPU and wireless module, the UR75 is capable of providing a wire-speed network with low power consumption and an ultra-small package to ensure an extremely safe and reliable connection to the wireless network.

Meanwhile, the UR75 also supports Gigabit Ethernet ports, serial ports (RS232/RS485) and I/O (input/output), which enables you to scale up M2M application by combining data and video in a limited time and budget.

The UR75 is particularly ideal for smart grids, digital media installations, industrial automation, telemetry equipment, medical device, digital factory, finance, payment device, environment protection, water conservancy and so on.



1.2 Advantages

Ultra Fast Connectivity

- Industrial-grade quad-core CPU ARM Cortex-A55 with big memory, providing high performance for data transmission
- Global 5G (NSA/SA)/4G LTE network with dual SIM cards for backup between multiple carrier networks
- Dual carrier aggregation (2CC CA) is supported in the 5G Sub-6GHz, enabling wider signal coverage with superb download speed up to 4.67 Gbps
- Plug& play, supply lightning transmission via Gigabit Ethernet ports or USB Type-C interface

- Support Wi-Fi 6, allows 2.4G & 5G dual band concurrent connections up to 1.8 Gbps download speed

Security & Reliability

- Automated failover/failback backup via Ethernet, Cellular (dual SIM) and Wi-Fi
- Secure transmission with VPN tunnels like IPsec/OpenVPN
- Embedded with hardware watchdog to automatically recover from various failures, ensuring the highest level of availability
- Equipped with multiple security protection measures such as ACL, DMZ, SYN-Flood protection, and data filtering to ensure that the network is secured
- Support policy routing and NAT for more secure intranet access

Easy Maintenance

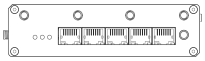
- Milesight DeviceHub provides easy setup, mass configuration, and centralized management of remote devices
- The user-friendly web interface design and several upgrade options help administrator to manage the device easily
- Support multilevel user authorities for security management

Industrial-Grade Design

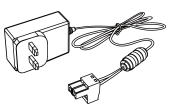
- Wide operating temperature range from -30°C to 60°C and industrial design for harsh environments
- Rugged enclosure with IP30 protection, optimized for DIN rail or shelf mounting.
- Equipped with I/O, serial port, and GPS for industrial transmission applications
- 3-year warranty included

Chapter 2 Hardware Introduction

2.1 Packing List

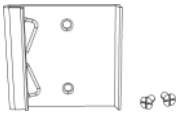


1 × UR75 Device



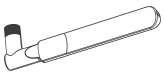
1 × Power Adapter

1 × 8-Pin Pluggable Terminal

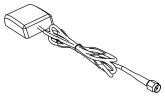


1 × DIN Rail Kit

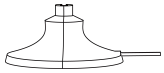
4 × Stubby Cellular Antennas



4 × Stubby Wi-Fi Antennas (Wi-Fi Version only)



1 × GPS Antenna



Antenna Magnetic Mounts (Optional)

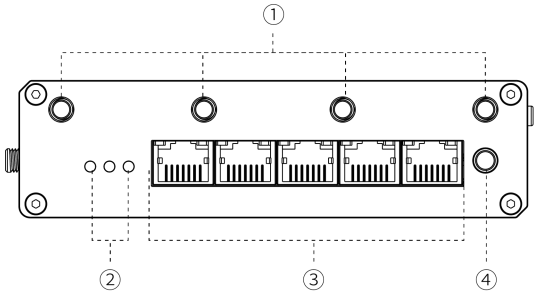
1 × Quick Guide

1 × Warranty Card

If any of the above items is missing or damaged, please contact your sales representative.

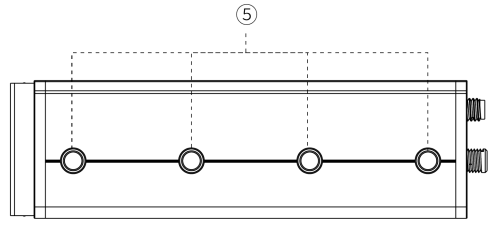
2.2 Hardware Overview

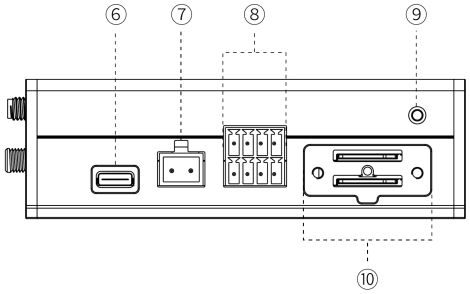
A. Front Panel



① Wi-Fi Antenna Connectors (Wi-Fi Version Only)
② LED Indicator Area
SYSTEM: Power & Status Indicator
SIM 1& SIM 2: SIM Status Indicator
③ Ethernet Ports & Indicators
④ GPS Antenna Connector

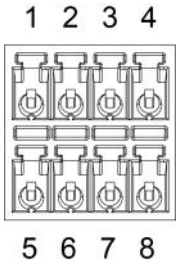
B. Left & Right Side Panel



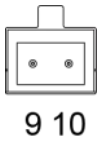


⑤ Cellular Antenna Connectors
⑥ USB Type-C Port
⑦ Power Connector
⑧ Serial Ports & I/O Ports
⑨ Grounding Stud
⑩ SIM slots and Reset Button

2.3 Serial & IO & Power Pinouts



PIN	RS232	RS485	DI	DO	Description
1	---	---	IN	---	Digital Input
2	GND	---	GND	---	Ground
3	---	B	---	---	Data -
4	TXD	---	---	---	Transmit Data
5	---	---	---	COM	Common Ground
6	---	---	---	OUT	Digital Output
7	---	A	---	---	Data +
8	RXD	---	---	---	Receive Data

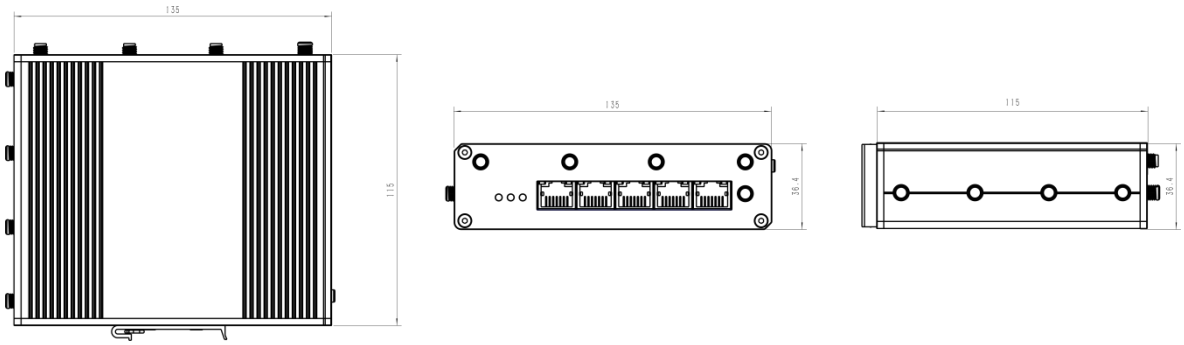


PIN	Description	Wire Color
9	Positive	Red
10	Negative	Black

2.4 LED Indicators

LED	Indication	Status	Description
SYSTEM	Power & System Status	Off	The power is switched off
		Orange	Static: The system is booting
		Green	Static: The system is running properly
		Red	Static: The system goes wrong
SIM1/SIM2	Cellular & Signal Status	Off	SIM card is registering or fails to register (or there are no SIM cards inserted)
		Green	Blinking rapidly: SIM card has been registered and is dialing up now
			Static: SIM card has been registered and dialed up to 5G network
		Orange	Static: SIM card has been registered and dialed up to 4G network
Ethernet Port	Link Indicator (Orange)	Off	Disconnected or connect failure
		On	Connected
		Blinking	Transmitting data
	Rate Indicator (Green)	Off	100 Mbps mode
		On	1000 Mbps mode

2.5 Dimensions (mm)



2.6 Reset Button

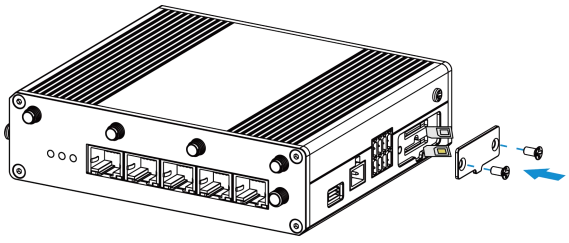
The reset button is beside SIM slots.

Function	Description	
	SYSTEM & SIM	Action
Reset	Static	Press and hold the reset button for more than 5 seconds.
	Static → Blinking	Release the button and wait.
	Off → Static Green	The device resets to factory default.

Chapter 3 Hardware Installation

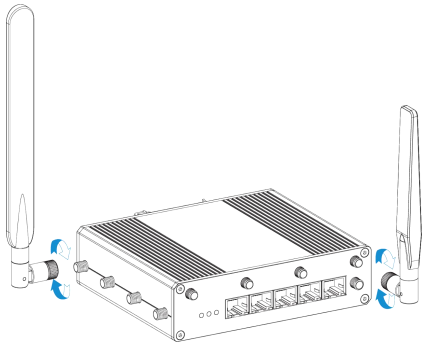
3.1 SIM Installation

Unscrew the holder of SIM card, insert the SIM card into the slot according to the direction icon on the device, then fix the holder back to the device with screws.



3.2 Antenna Installation

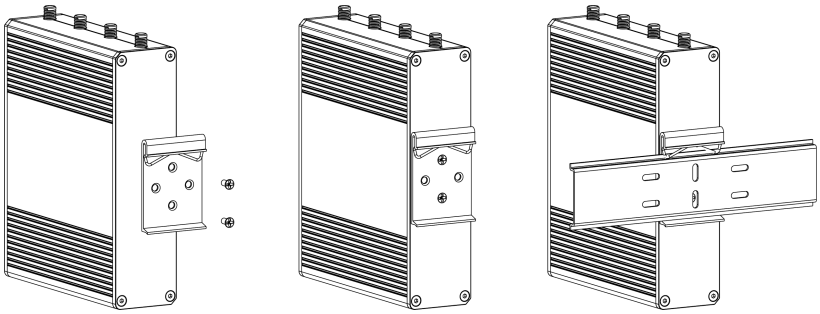
Rotate the antenna into the antenna connector accordingly. Antennas should be installed vertically and be always on a site with a good signal.



3.3 Device Installation

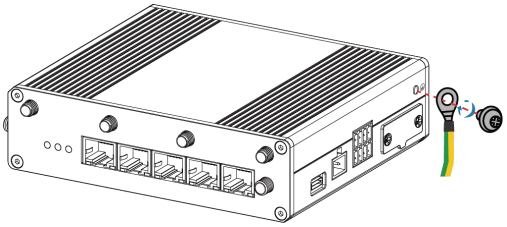
UR75 device can be placed on a desktop or mounted to a DIN rail. For DIN rail mounting, use 2 pcs of M3 × 6 flat head Phillips screws to fix the mount clip to the device, and then hang the device to the DIN rail. The width of DIN rail is 3.5 cm.

Recommended torque for mounting is 1.0 N·m, and the maximum allowed is 1.2 N·m.



3.4 Protective Grounding Installation

Connect the grounding ring of the cabinet's grounding wire onto the grounding stud and screw up the grounding nut.



Chapter 4 Access to Web GUI

UR75 provides user-friendly web GUI for configuration and users can access it via LAN port. This chapter explains how to access to Web GUI of the UR75 router.

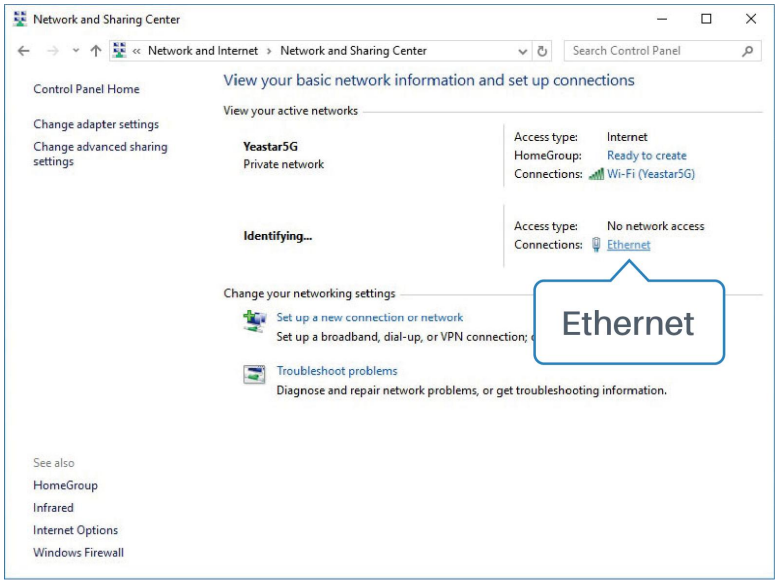
Username: **admin**

Password: **password**

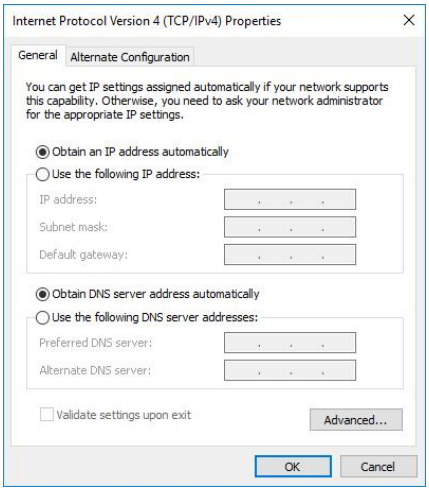
IP Address: **192.168.1.1**

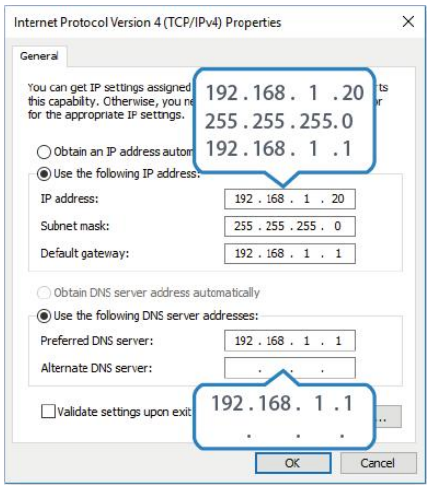
Connect PC to LAN port or USB port of U75 router directly. The following steps are based on Windows 10 operating system for your reference.

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

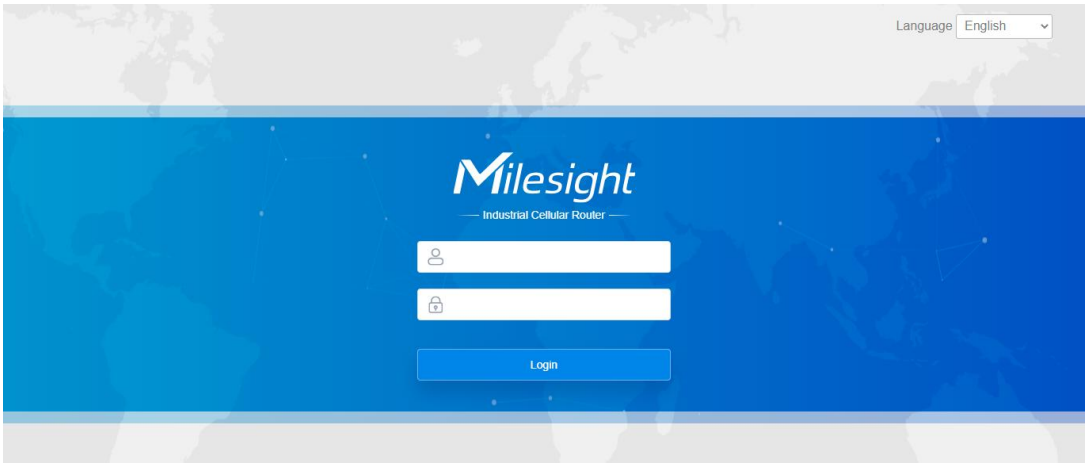


2. Go to **Properties → Internet Protocol Version 4(TCP/IPv4)**, select **Obtain an IP address automatically** or **Use the following IP address**, then assign a static IP manually within the same subnet of the device.



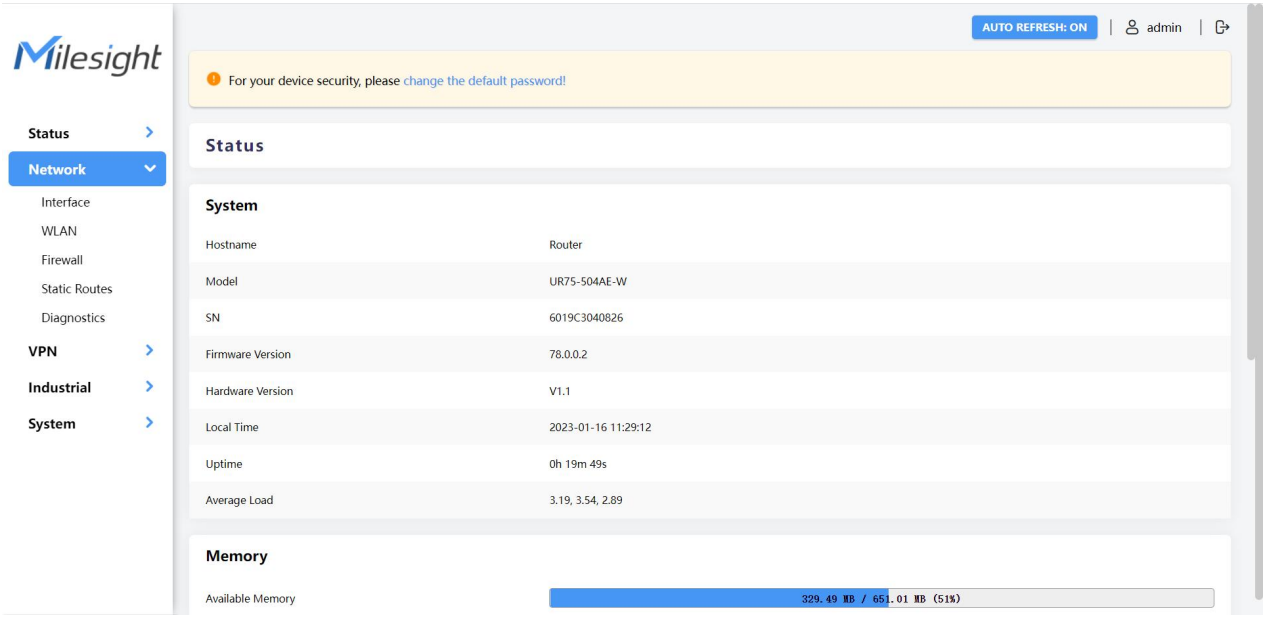


3. Open a Web browser on your PC (Chrome is recommended), type in the IP address 192.168.1.1 to access the web GUI, then enter the default username and password, and click **Login**.



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

4. After you login the Web GUI, you can view system information and perform configuration on the router.



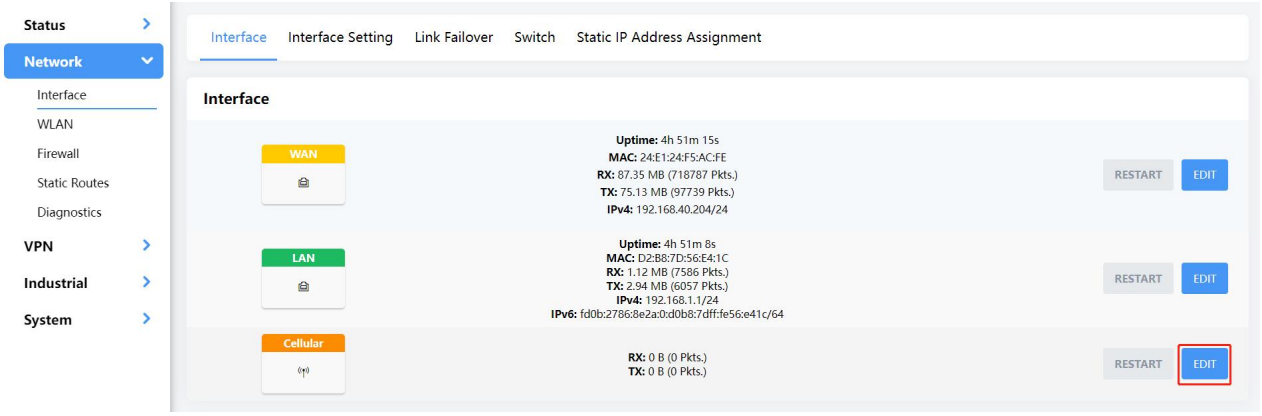
Chapter 5 Application Examples

5.1 Configure Cellular Connection

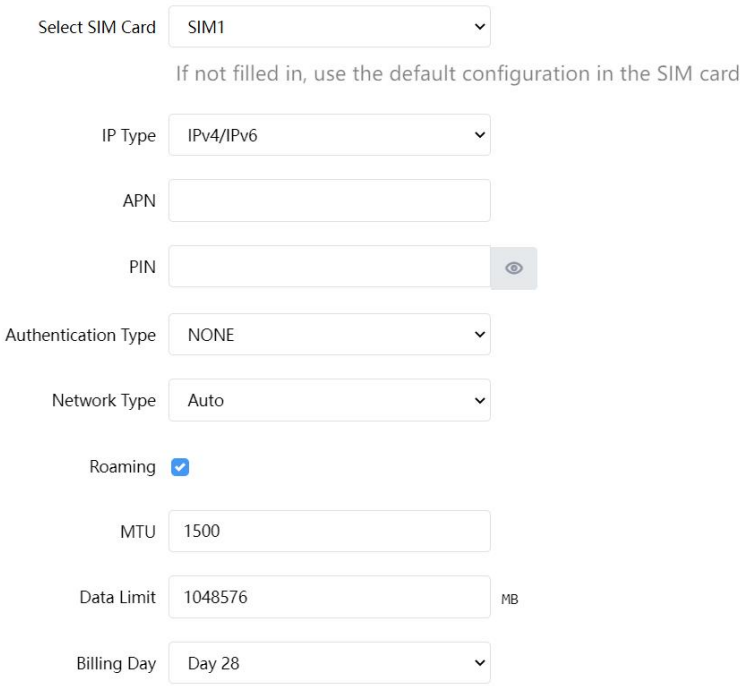
UR75 routers have two cellular interfaces SIM1 & SIM2. Only one cellular interface is active at a time. We are about to take an example of inserting a SIM card into the SIM1 slot of the UR75 and configuring the router to get access to the Internet through cellular.

Configuration Steps

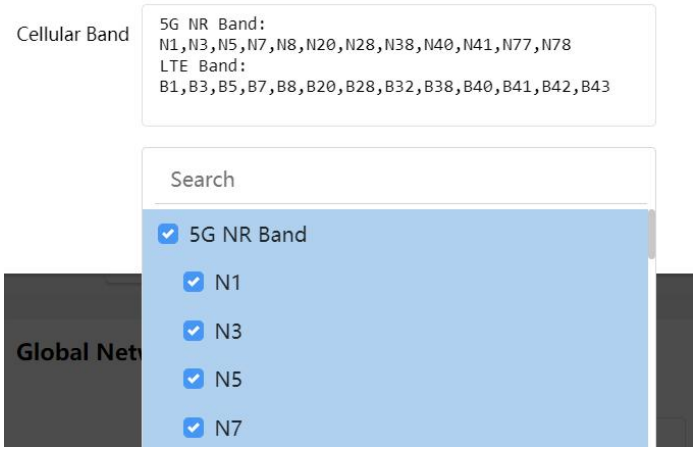
1. Ensure the SIM card is inserted well and all cellular antennas are connected to the correct connectors.
2. Go to **Network > Interface > Interface** page, find the cellular interface and click **Edit** button.



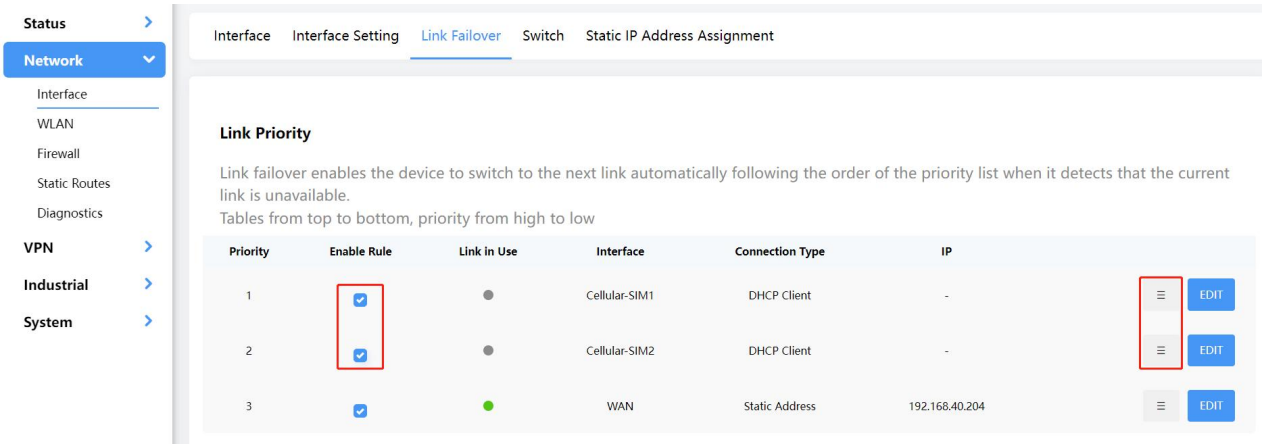
3. Select the SIM card you need to configure and fill in the necessary info of SIM card, then save all settings.



For 5G connection, you can choose specific bands to ensure high network speed.

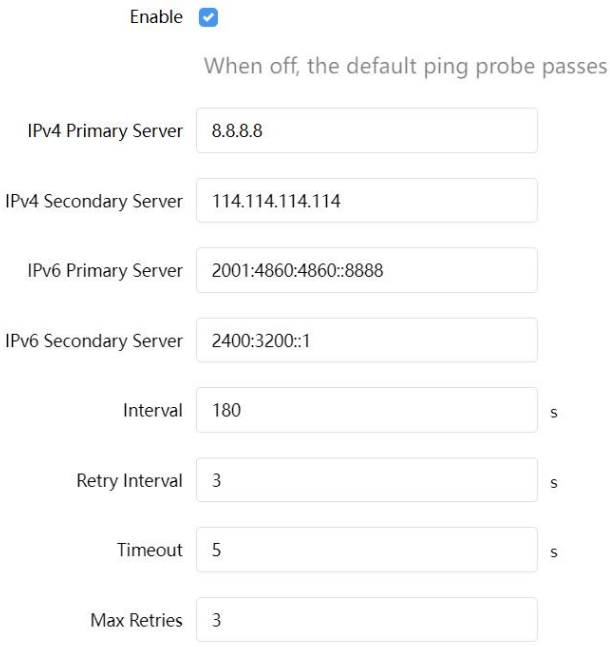


4. Go to **Network > Interface > Link Failover** to enable correspond SIM and drag the buttons to change link priority.

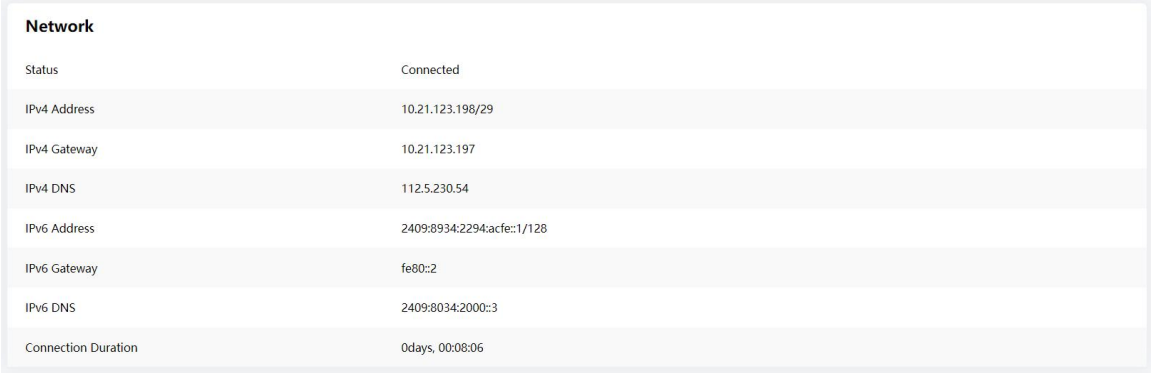


5. Click **Edit** of a link to configure ICMP ping detection information. When ping probe is enabled, the router will send ICMP packets to detection server to check if this link is valid. If no response and exceeding max retries, it will switch to the lower priority link.

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



6. Go to **Status > Cellular** to check the status of the cellular connection. If modem status is ready and network status shows **Connected**, the SIM has been dialed up successfully.



Related Topic

Cellular Setting

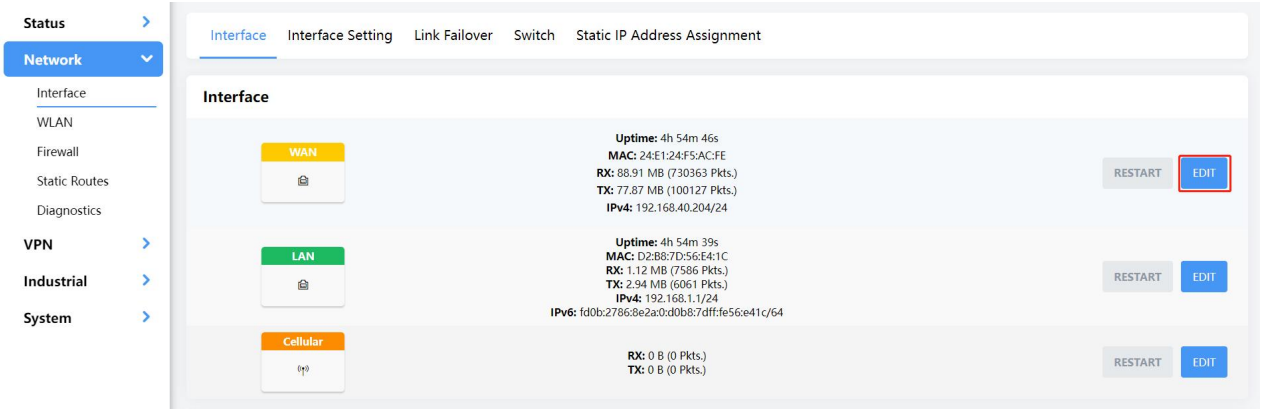
Cellular Status

5.2 Configure Ethernet Connection

UR75 routers support getting network access via WAN port.

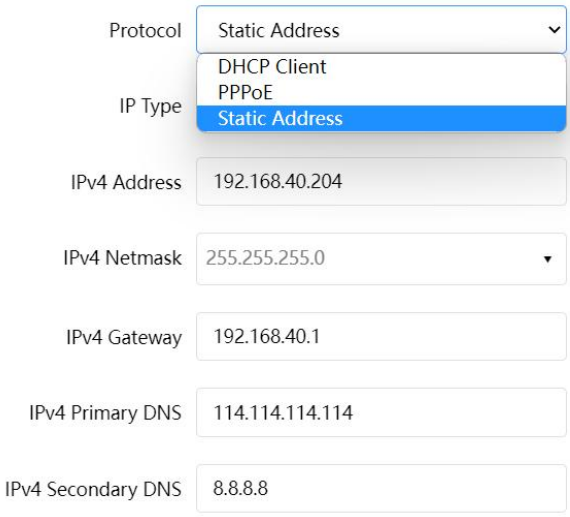
Configuration Steps

1. Go to **Network > Interface > Interface** page, find the WAN interface and click **Edit** button.

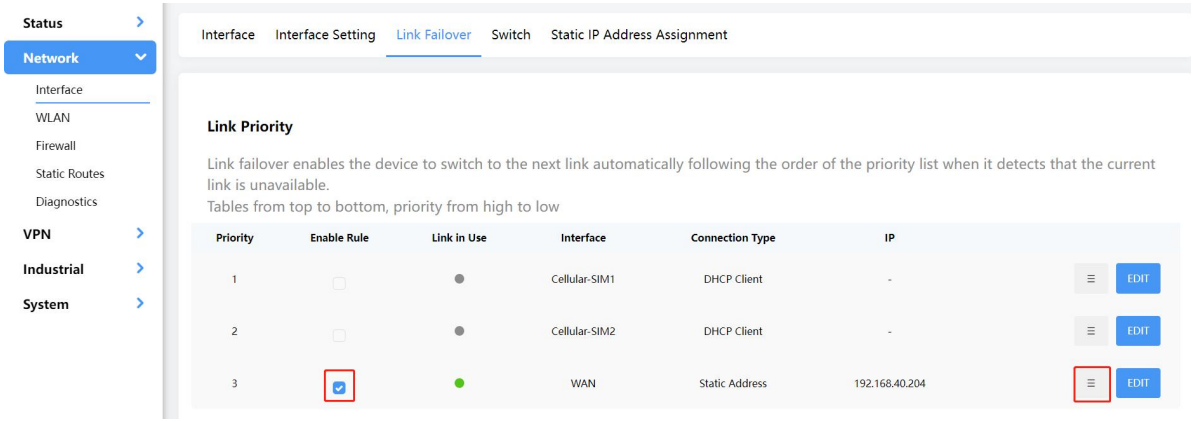


2. Select the protocol according to your network router mode or network provider types and configure the corresponding parameters, then save all settings.

- **DHCP:** upper network router will assign an IP address to UR75 WAN port. This is the easiest way and requires the upper route to enable the DHCP server.
- **Status Address:** assign a static IP address with the same subnet as the LAN subnet of the upper network router. Besides, it's necessary to configure at least one DNS server.
- **PPPoE:** type your PPPoE account username and password, this should contact your network provider.

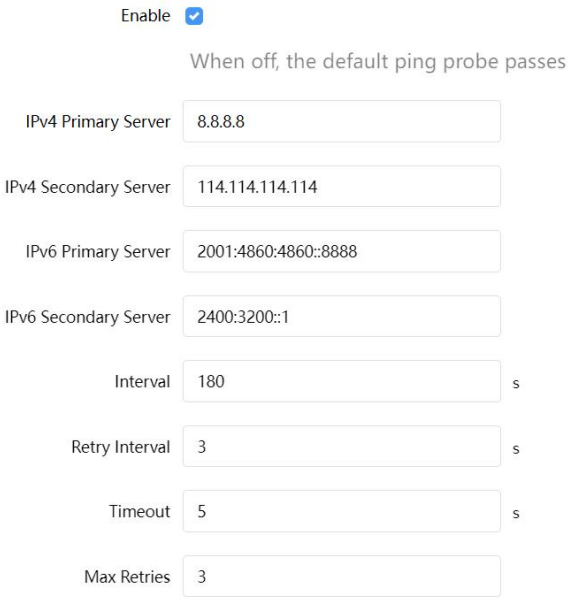


3. Go to **Network > Interface > Link Failover** to enable WAN and drag the button to change link priority.

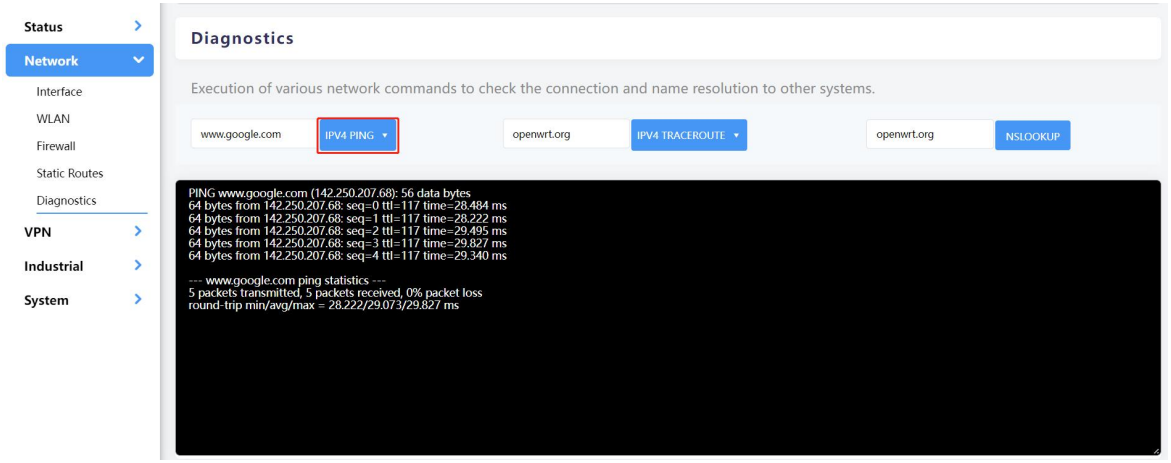


4. Click **Edit** of a link to configure ICMP ping detection information. When ping probe is enabled, the router will send ICMP packets to detection server to check if this link is valid. If no response and exceeding max retries, it will switch to the lower priority link.

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



5. Click **Network > Diagnostics** to check the network connectivity.



Related Topic

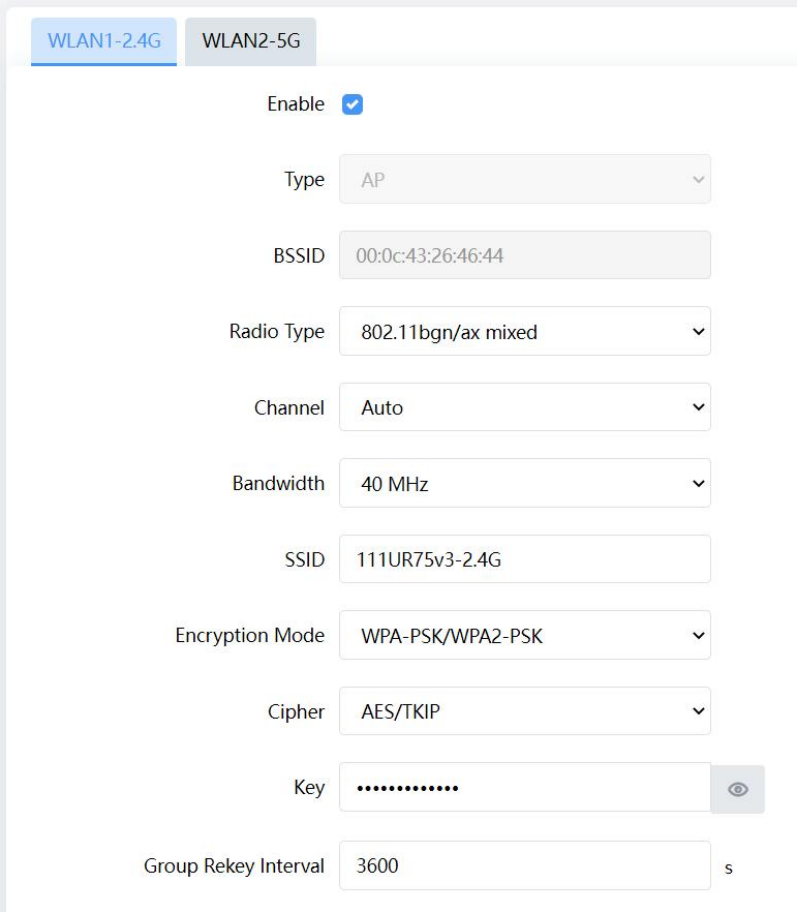
WAN Setting

5.3 Configure Wi-Fi Access Point

UR75 routers support both 2.4G and 5G Wi-Fi and they can work as access points to provide network access to other devices at the same time. We are about to take an example of configuring a 2.4G Wi-Fi access point.

Configuration Steps

1. Ensure the router supports Wi-Fi and the Wi-Fi antennas are connected to the correct connectors.
2. Go to **Network > WLAN** page to enable 2.4G Wi-Fi mode, then users can modify the radio type, SSID and other parameters. For security access, it's suggested to select an encryption mode and define a key for devices to connect to Wi-Fi.



3. Use a smart phone to connect the access point of UR75. You can check the information of the connected client/user on **Status > Overview** page.

Active DHCP Leases

Hostname	IPv4-Address	MAC-Address	Remaining Lease Time
HUAWEI_P20-9c88dbba544dae	192.168.1.147	C4:9F:4C:64:B3:B7	22h 35m 12s
ANA-AN00	192.168.1.119	D2:17:2E:4D:C0:BB	20h 34m 20s

Related Topic

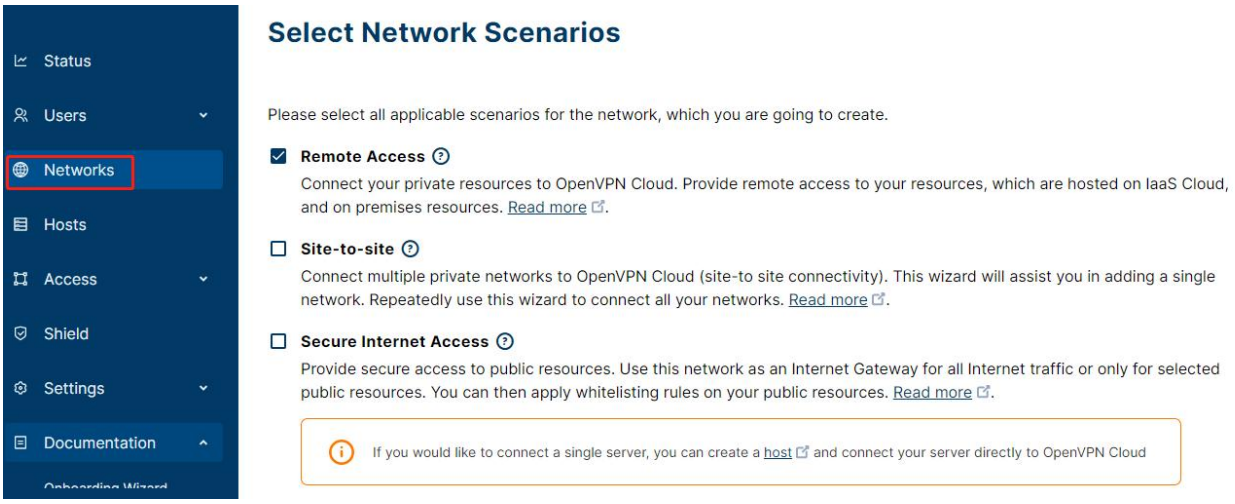
WLAN Setting

5.4 Configure OpenVPN Client

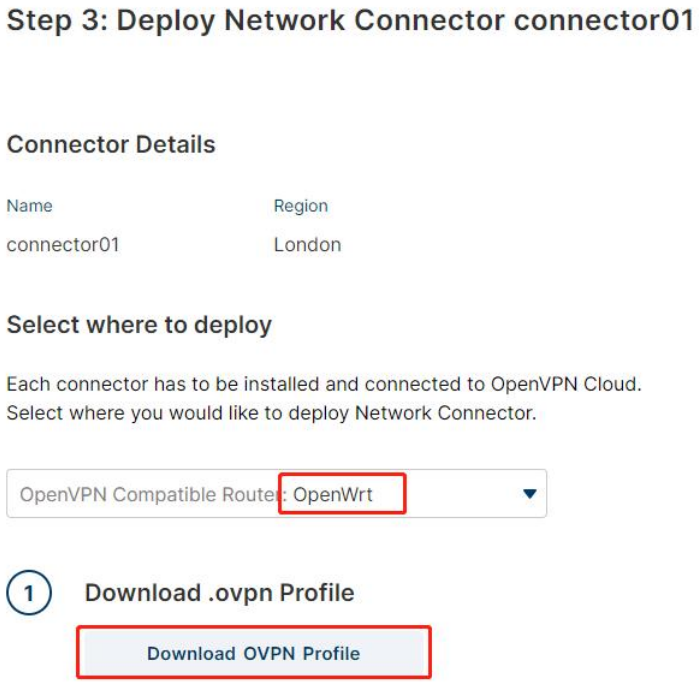
UR75 routers can work as OpenVPN clients or OpenVPN servers. We are about to take an example of configuring OpenVPN client to connect to OpenVPN cloud.

Configuration Steps

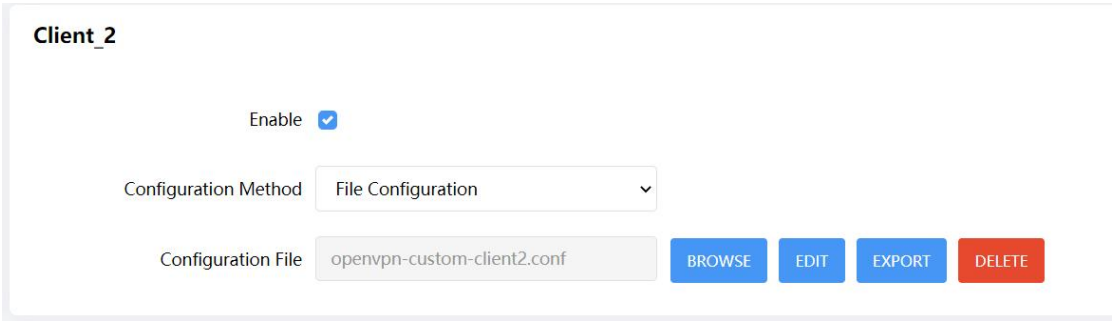
1. Ensure the UR75 has gotten access to the Internet.
2. Log in the openVPN cloud account, select Network section and select the service depending on your requirement and follow the wizard to continue the settings.



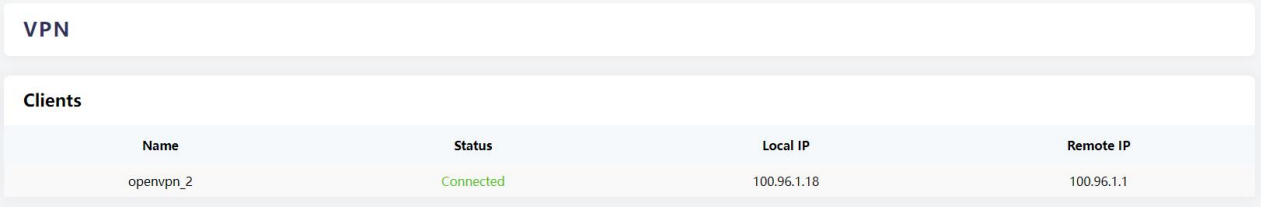
3. Select the location as OpenWrt and download the OVPN file.



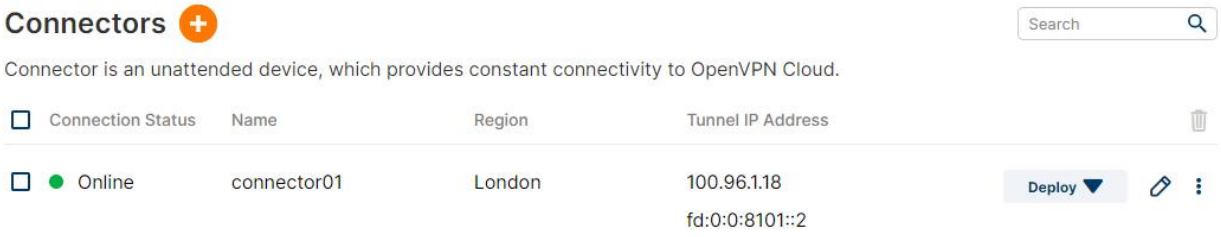
4. Go to **VPN > OpenVPN > OpenVPN Client** page of UR75, select configuration method as File Configuration, then import the OVPN file.



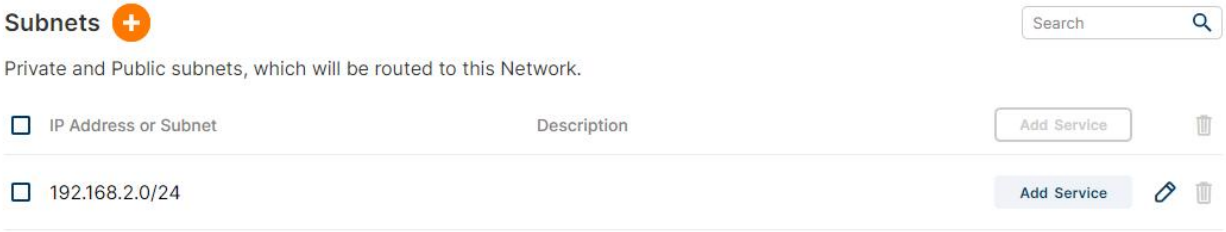
5. Go to **Status > VPN** page to check if the client is connected.



You can also check the connection status on OpenVPN cloud.



6. You can remotely get access to this router via OpenVPN Connect software. If you need to access the terminal devices under UR75 subnet, it's necessary to assign the subnet on OpenVPN cloud.



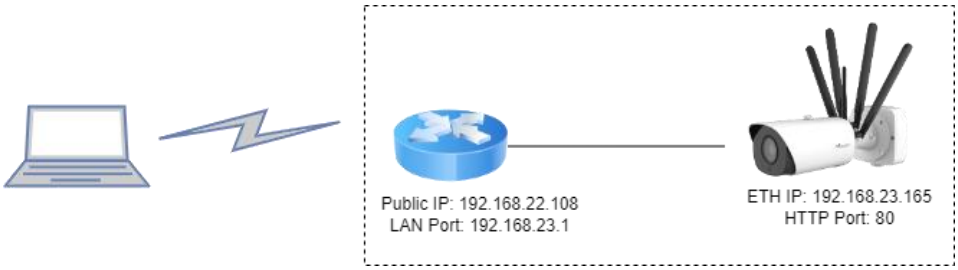
Related Topic

OpenVPN Client

5.5 Configure NAT Rule

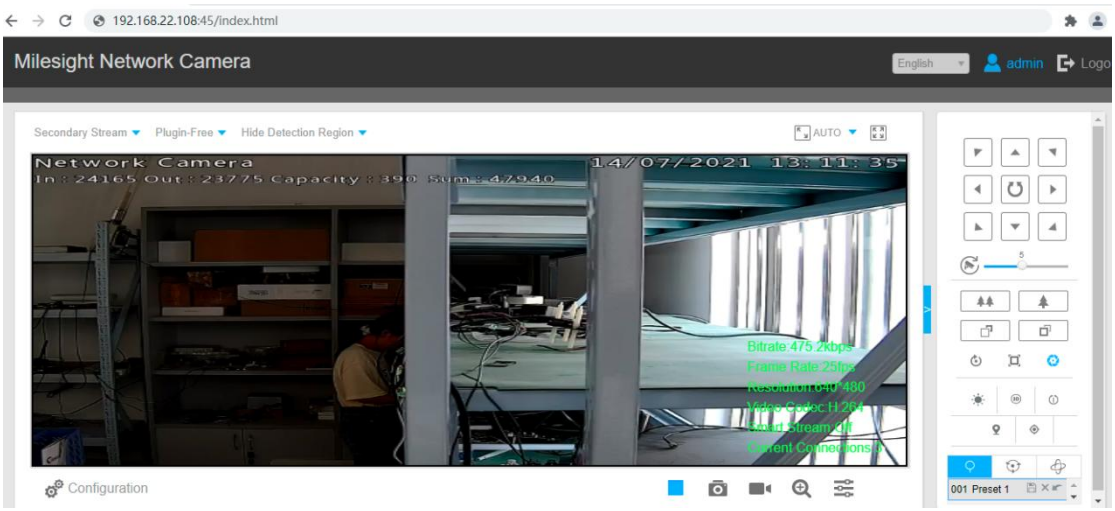
Example

An UR75 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 **Network > Firewall > Port Mapping** and configure port mapping parameters as below. External 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.



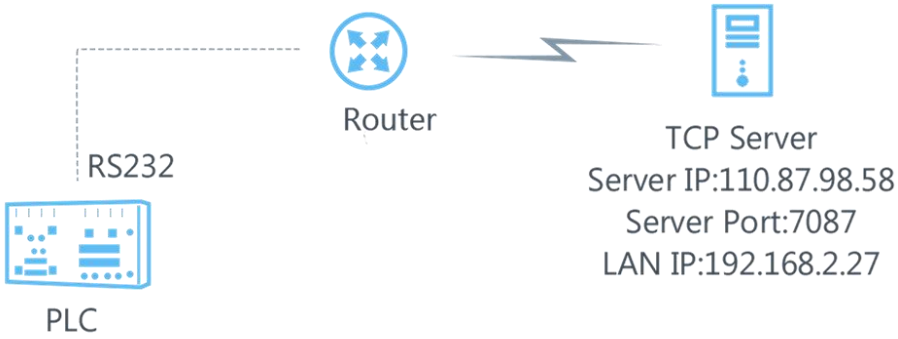
Related Topic

Port Mapping

5.6 Configure Serial DTU Connection

Example

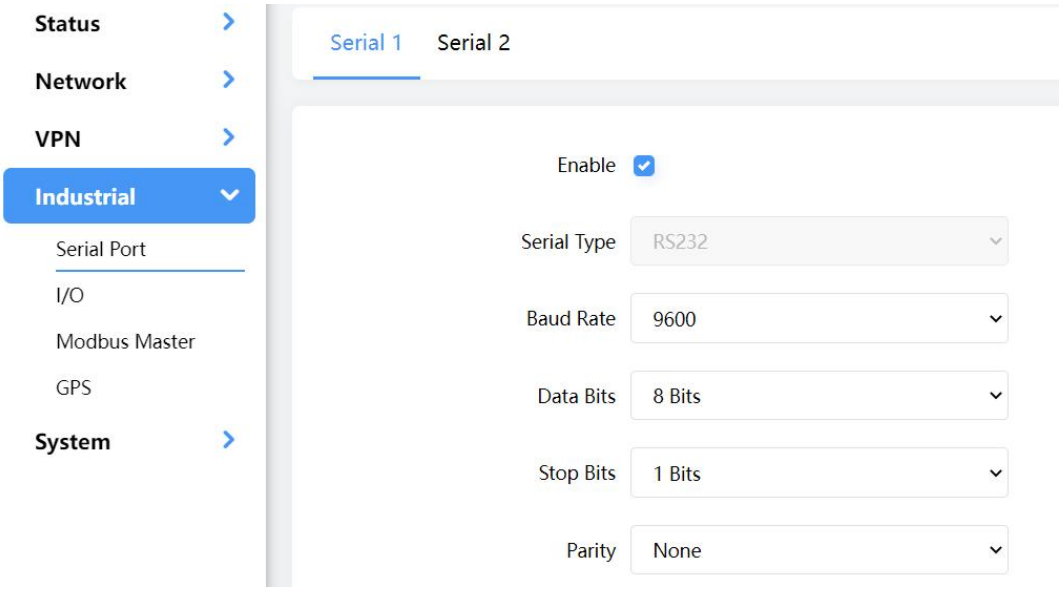
A PLC is connected with the UR75 via RS232 and need to transfer the data to a remote TCP server transparently.



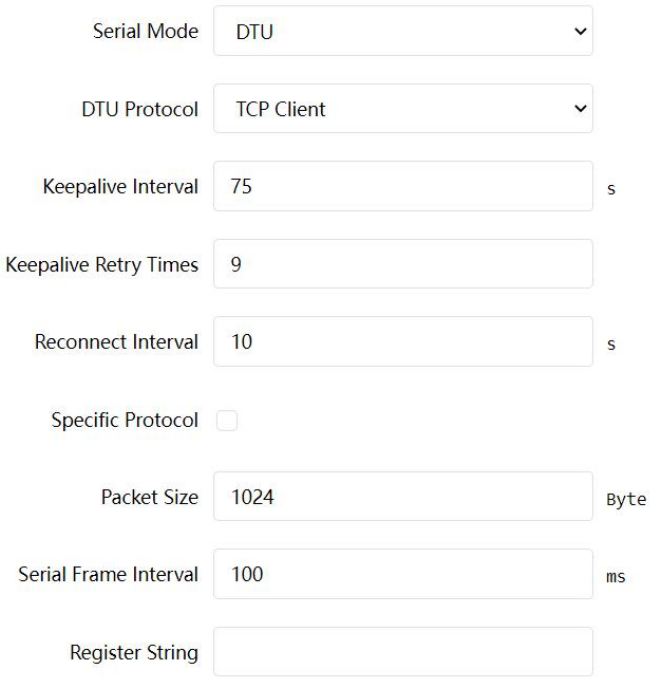
Configuration Steps

1. Go to **Industrial > Serial Port**, 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.

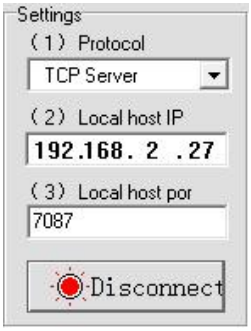


2. Configure Serial Mode as **DTU Mode** and protocol as **TCP Client**.



3. Configure TCP server IP and port.

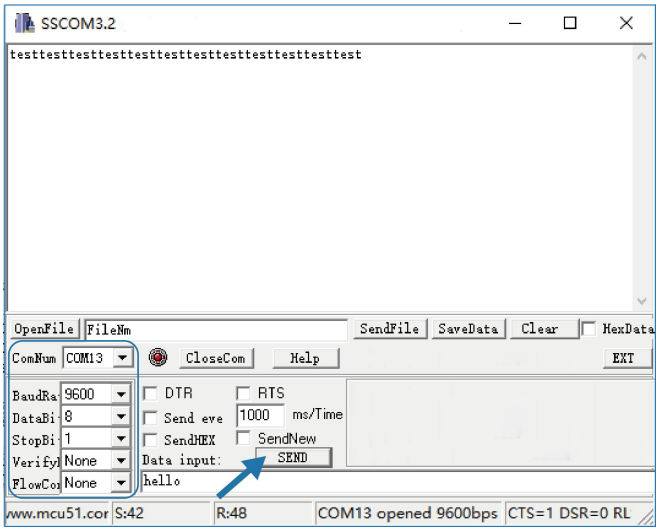
4. Start TCP server on PC. Take **Netassist** test software as example. Make sure port mapping is done.



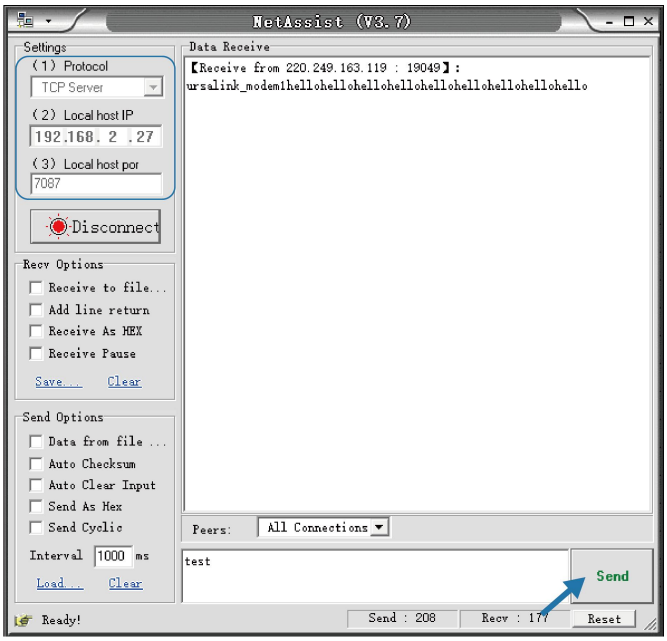
5. Connect the UR75 to PC via RS232 for PLC simulation. Then start **sscom** software on the PC to test communication through serial port.

6. After connection is established between the UR75 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 UR75 for test.

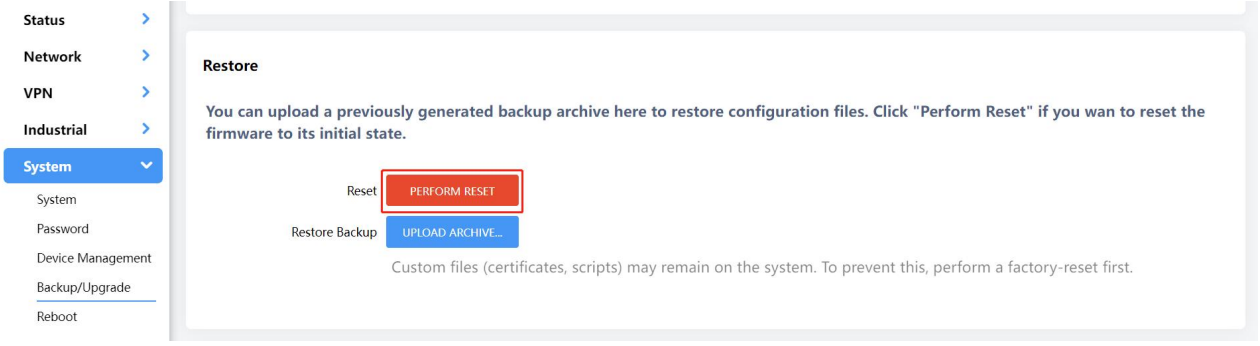
Related Topic

Serial Port

5.7 Restore Factory Defaults

Method 1:

Go to **System > Backup/Upgrade** page, click **Perform Reset** button, you will be asked to confirm if you'd like to reset it to factory defaults. Then click **OK** button.



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

Please wait till the SYSTEM LED shines in green, which means the device has already been reset to factory defaults successfully.

Related Topic

Backup / Flash Firmware

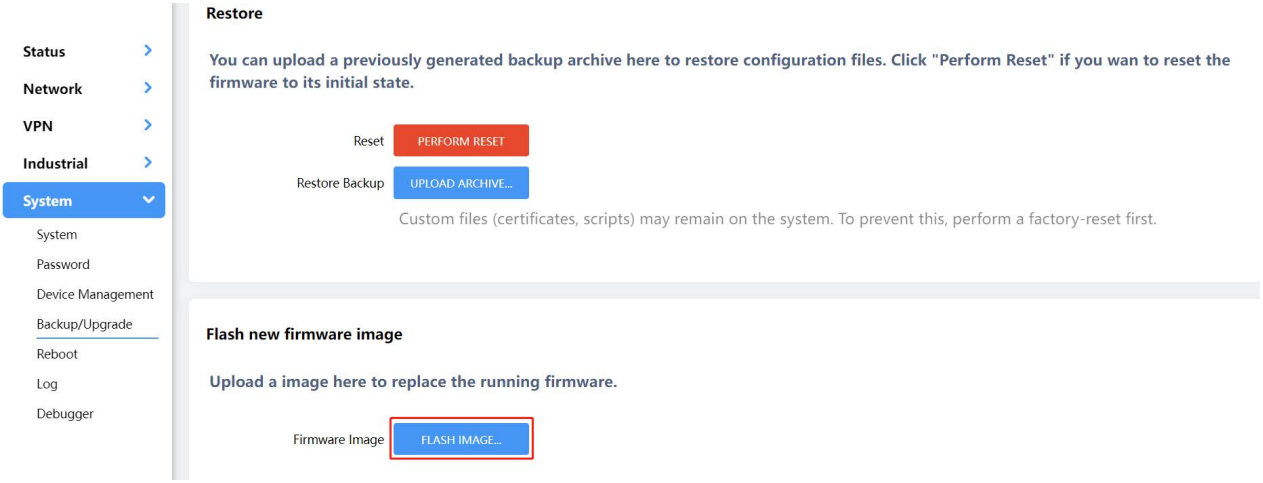
Method 2:

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

5.8 Firmware Upgrade

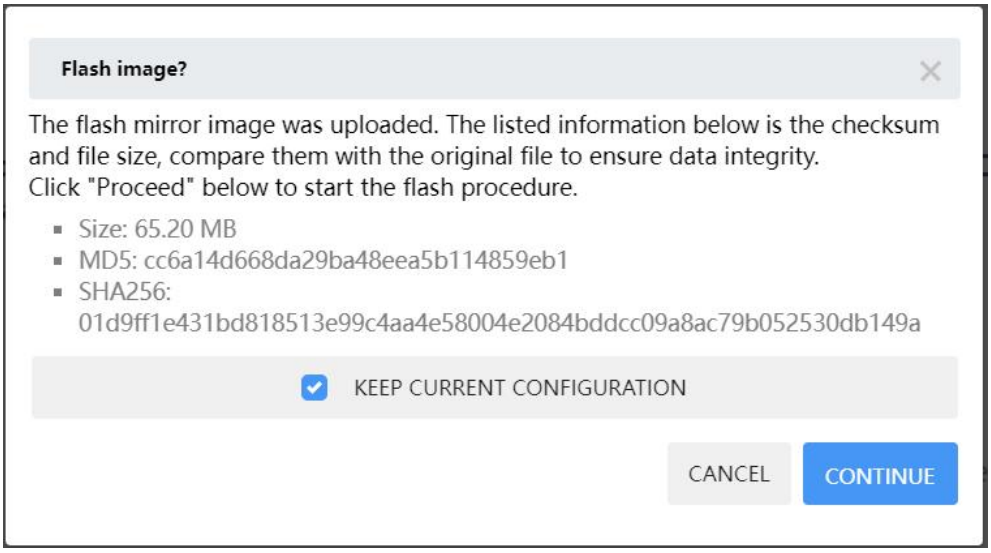
It is suggested that you contact Milesight technical support first before you upgrade the device. After getting the image file please refer to the following steps to complete the upgrade.

1. Go to **System > Backup/Upgrade** page, and click **Flash image...**.



2. Browse the correct firmware file from the PC, click **Upload** and the device will check if the firmware file is correct. If it's correct, the firmware will be imported to the device.

3. After upload, click **Continue** to upgrade the device. When SYS LED changes from orange to green and stay statically, the upgrade is completed. Do not perform any operation or disconnect the power during the upgrade.



Related Topic

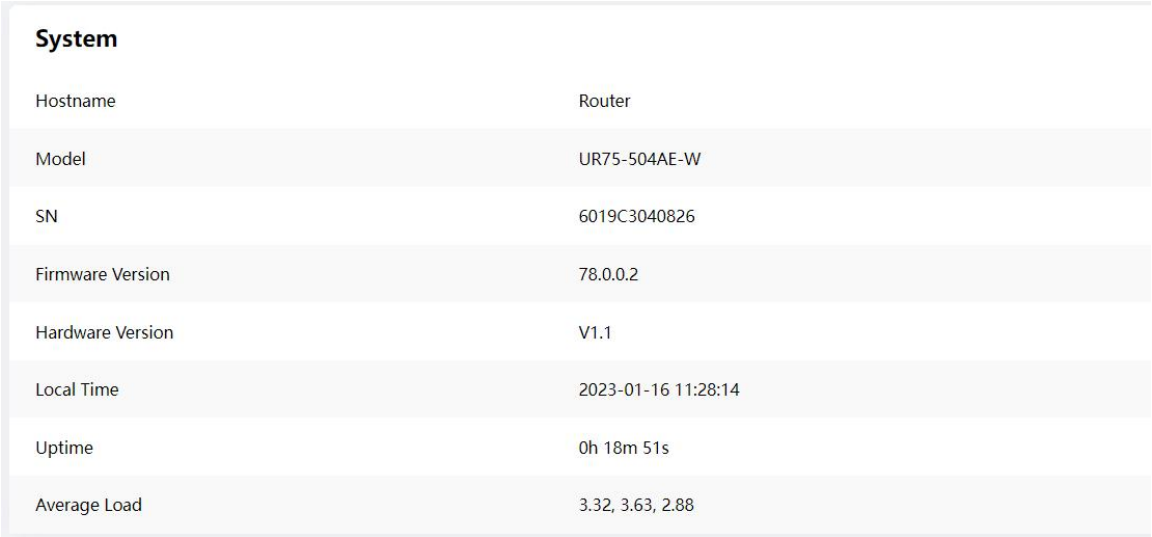
Backup / Flash Firmware

Chapter 6 Web Configuration

6.1 Status

6.1.1 Overview

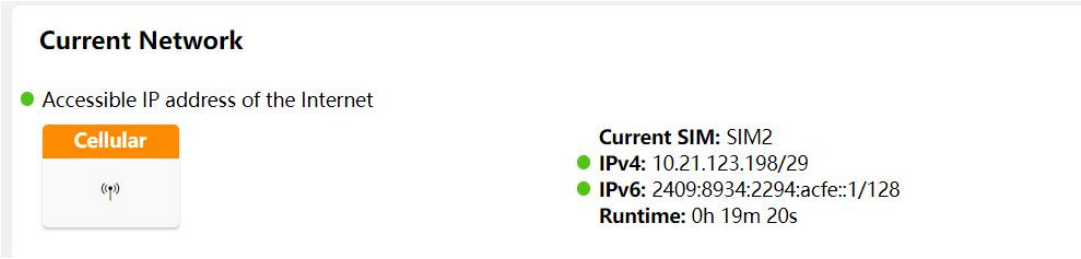
The System tab contains the basic information of the router on this page.

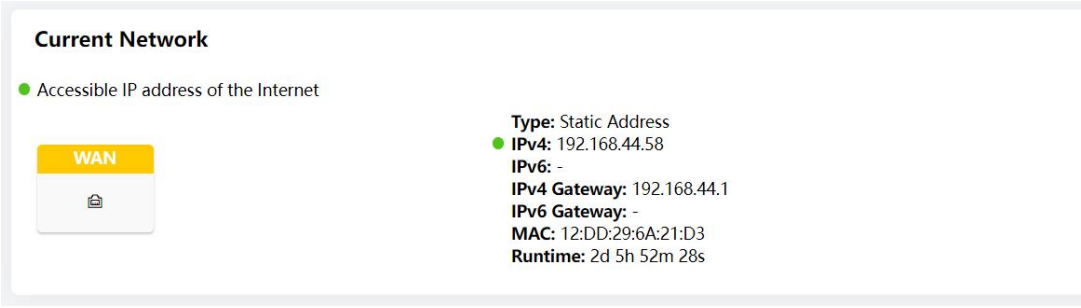


System	
Item	**Description**
Hostname	The hostname of device, it can be modified on **System > System > General Settings**.
Model	The model name of the device.
SN	The serial number of the device.
Firmware Version	The current firmware version of the device.
Hardware Version	The current hardware version of the device.
Local Time	The current system time of the device , it can be modified on **System > System > General Settings**.
Uptime	The time since the device has been powered and running.
Average Load	Averages over progressively longer periods of time (1, 5 and 15 minutes averages), the smaller numbers are better.

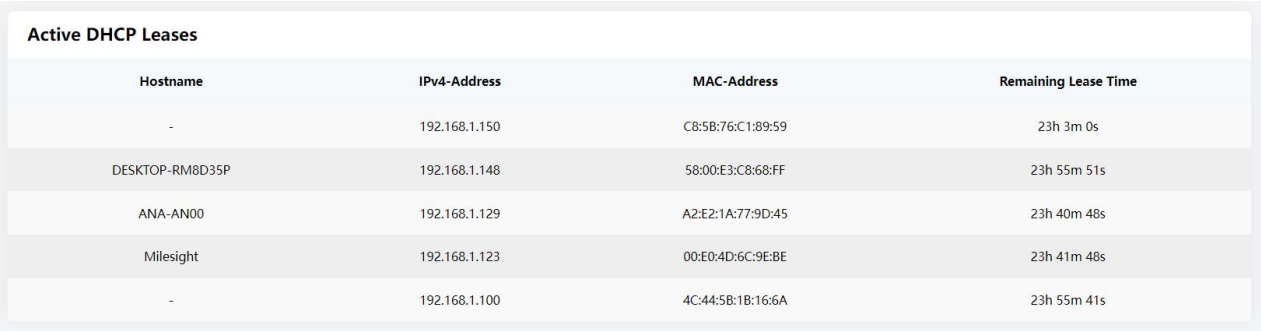
Memory	
Item	**Description**
Available Memory	The percentage of available RAM.
Remaining Memory	The percentage of used RAM.

The **Current Network** tab displays the basic information of link in use, click Interface chapter for details.





The Active DHCP Leases tab displays the basic information of connected devices.



Active DHCP Leases

Hostname	IPv4-Address	MAC-Address	Remaining Lease Time
-	192.168.1.150	C8:5B:76:C1:89:59	23h 3m 0s
DESKTOP-RM8D35P	192.168.1.148	58:00:E3:C8:68:FF	23h 55m 51s
ANA-AN00	192.168.1.129	A2:E2:1A:77:9D:45	23h 40m 48s
Milesight	192.168.1.123	00:E0:4D:6C:9E:BE	23h 41m 48s
-	192.168.1.100	4C:44:5B:1B:16:6A	23h 55m 41s

Active DHCP Leases	
Item	**Description**
Hostname	The hostname of the connected device.
IPv4-Address	Tthe IPv4 address of the connected device.
MAC-Address	The MAC address of the connected device.
Remaining Lease Time	The time remaining for this lease.

6.1.2 Cellular

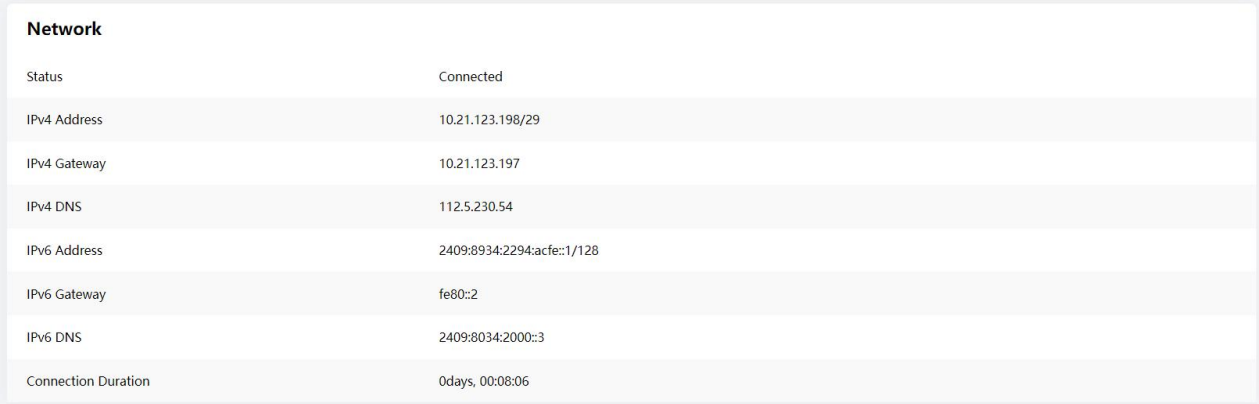
You can view the cellular network status of router on this page.

Cellular Status

Status	Ready
Module Model	RG500L-EU
Version	RG500LEUACR04A01M8G_OCPU_20.001.20.001
Current SIM	SIM2
Cellular Band	N41
Signal Strength	-68dBm
Register Status	Registered(Home network)
IMEI	869263050336332
IMSI	460028688541190
ICCID	89860016111591001190
ISP	CHINA MOBILE
Network Type	5G SA
PLMN ID	46000
LAC	3259E7
Cell ID	203959107
CQI	-
DL Bandwidth	100MHz
UL Bandwidth	100MHz
SINR	29.5dB
PCI	23F
RSRP	-68dBm
RSRQ	-11dB
EARFCN	7B49E

Modem Information	
Item	**Description**
Status	Corresponding detection status of module and SIM card.
Module Model	The model name of cellular module.
Version	The firmware version of cellular module.
Current SIM	The current SIM card used.
Cellular Band	The cellular band which the router used to register to network.
Signal Strength	The RSSI (Received Signal Indicator) of registered cellular network.

Register Status	The registration status of SIM card.
IMEI	The IMEI of the cellular module.
IMSI	The IMSI of the SIM card.
ICCID	The ICCID of the SIM card.
ISP	The network provider which the SIM card registers on.
Network Type	The connected network type, such as LTE, 3G, etc.
PLMN ID	The current PLMN ID, including MCC, MNC, LAC and Cell ID.
LAC	The location area code of the SIM card.
Cell ID	The Cell ID of the SIM card location.
CQI	The Channel Quality Indicator of the cellular network.
DL Bandwidth	The DL bandwidth of the cellular network.
UL Bandwidth	The UL bandwidth of the cellular network.
SINR	The Signal Interference + Noise Ratio of the cellular network.
PCI	The physical-layer cell identity of the cellular network.
RSRP	The Reference Signal Received Power of the cellular network.
RSRQ	The Reference Quality Received Power of the cellular network.
EARFCN	The E-UTRA Absolute Radio Frequency Channel Number.

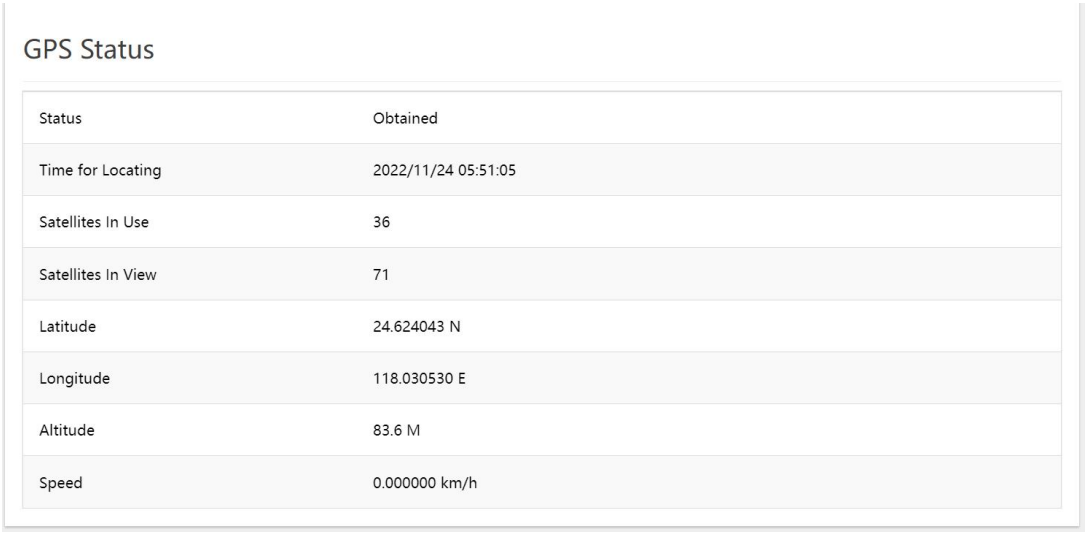


Network	
Item	**Description**
Status	The connection status of cellular network.
IPv4/IPv6 Address	The IPv4/IPv6 address and netmask of cellular network.
IPv4/IPv6 Gateway	The IPv4/IPv6 gateway and netmask of cellular network.
IPv4/IPv6 DNS	The DNS sever of cellular network.
Connection Duration	The information on how long the cellular network has been connected.
RX	The data volume and packets received of this month.
TX	The data volume and packets transmitted of this month.

ALL	Total data volume and packets of this month.

6.1.3 GPS

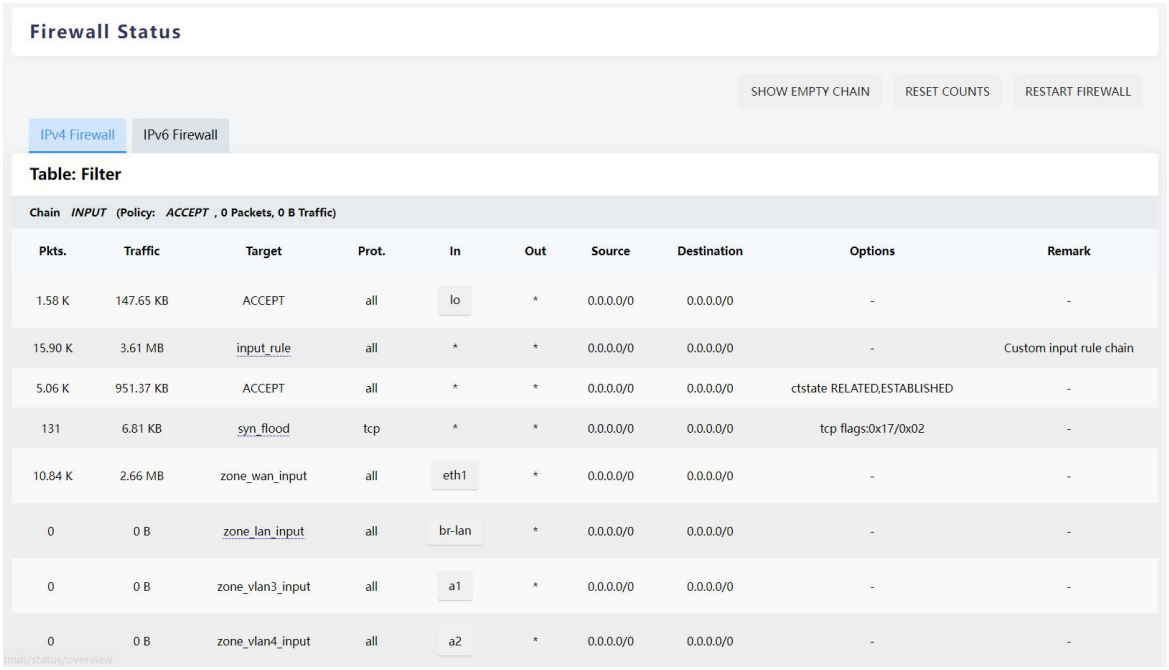
When GPS function is enabled and the GPS information is obtained successfully, you can view the latest GPS information including GPS time, latitude, longitude and speed on this page.



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

6.1.4 Firewall

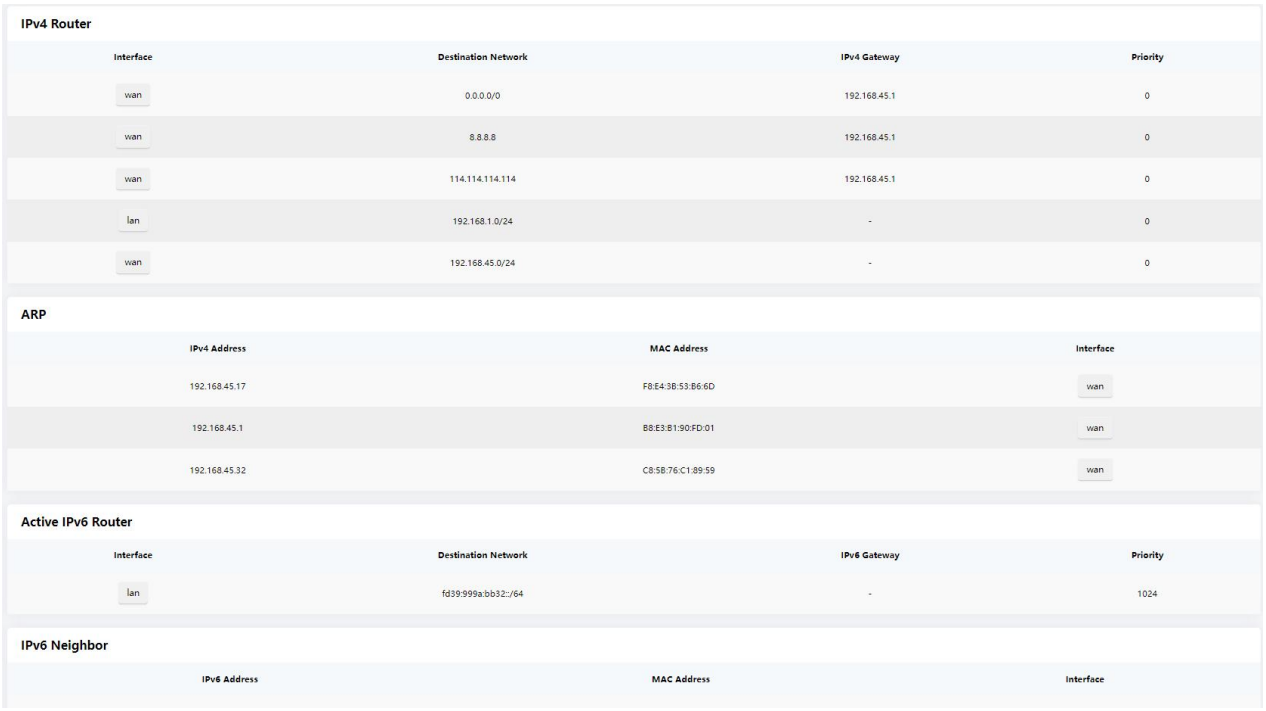
On this page you can check all IPv4/IPv6 chains of iptables. Users can click the targets with dashed line to jump to the corresponding chains.



Firewall Status	
Item	**Description**
Table: Filter	The default table for handing network packets.
Table: NAT	Used to alter packets that create a new connection and used for Network Address Translation (NAT).
Table: Mangle	Used for specific types of packet alternation.
Show/Hide Empty Chain	Show/hide the chain without any rule.
Reset Counts	Reset the traffic counts of all chains.
Restart Firewall	Restart the whole firewall process.

6.1.5 Routing Table

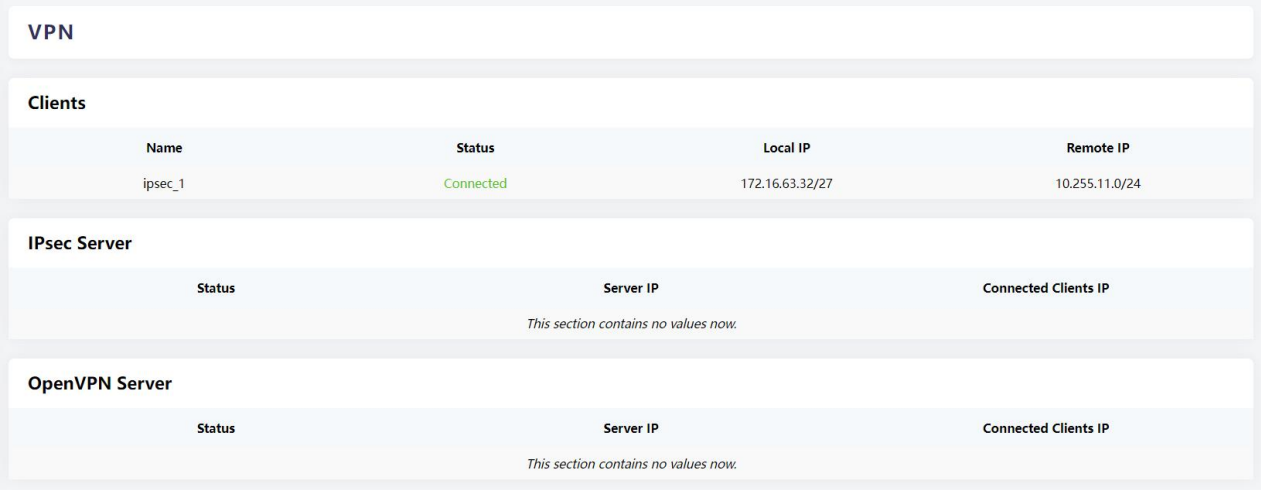
You can check routing status on this page, including the routing table and ARP cache.



Item	Description
Active IPv4/IPv6 Router	
Interface	The outbound interface of the route.
Destination Network	The IP address and netmask of destination host or destination network.
IPv4/IPv6 Gateway	The IP address of the gateway to send packets from.
Priority	The metric number indicating interface priority of usage.
ARP Cache	
IPv4 Address	The IP address of ARP pool.
MAC Address	The IP address's corresponding MAC address.
Interface	The binding interface of ARP.
IPv6 Neighbor	
IPv6 Address	The IP address of neighbor.
MAC Address	The IP address's corresponding MAC address.
Interface	The binding interface of neighbor.

6.1.6 VPN

You can check VPN status on this page.

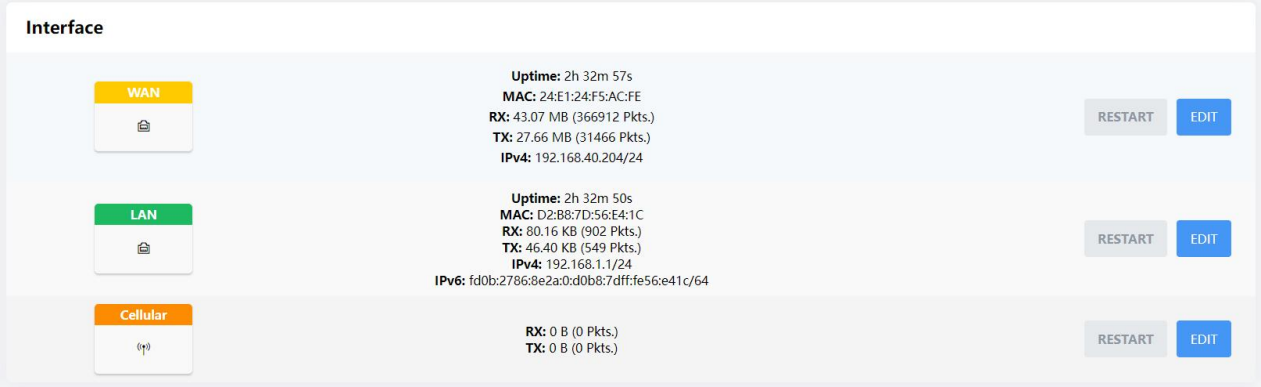


VPN Status	
Item	**Description**
Clients	
Name	The name of the enabled VPN clients.
Status	The connection status of client.
Local IP	The local IP address and subnet of the VPN tunnel.
Remote IP	The real remote IP address and subnet of the VPN tunnel.
IPsec/OpenVPN Server	
Status	The status of Server.
Server IP	The server IP address and subnet of the VPN tunnel.
Connected Clients IP	The IP address of the client which is connected to the server.

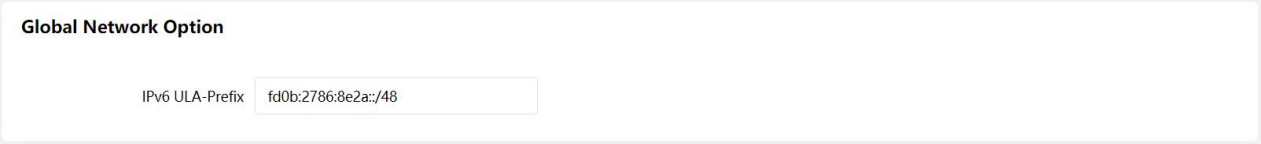
6.2 Network

6.2.1 Interfaces

This menu allows to configure the basic settings of cellular, WAN and LAN interfaces.



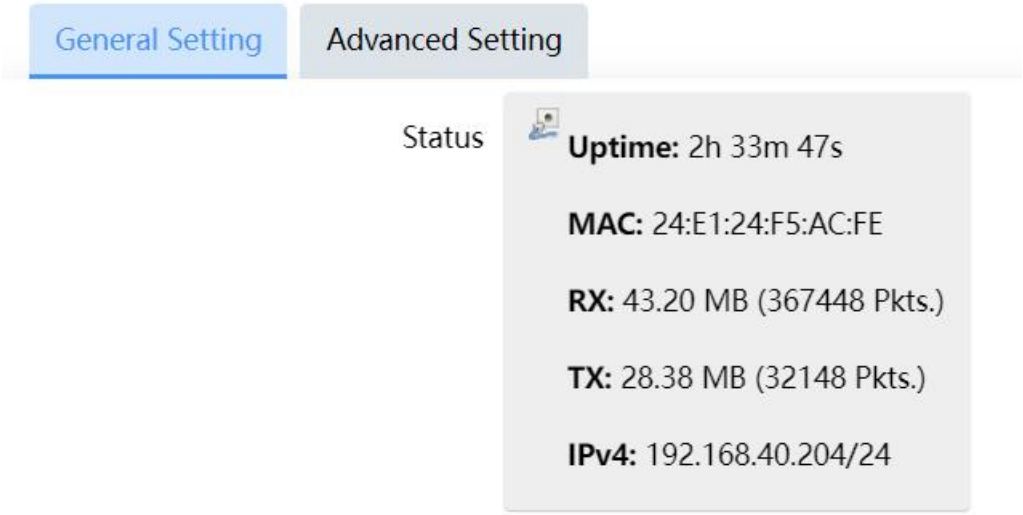
Interfaces	
Item	**Description**
Restart	Click to restart this network interface.
Edit	Click to edit general settings of this network interface.



Global Network Options	
Item	**Description**
IPv6 ULA-Prefix	The IPv6 unique local address (ULA) prefix of this device.

6.2.1.1 WAN

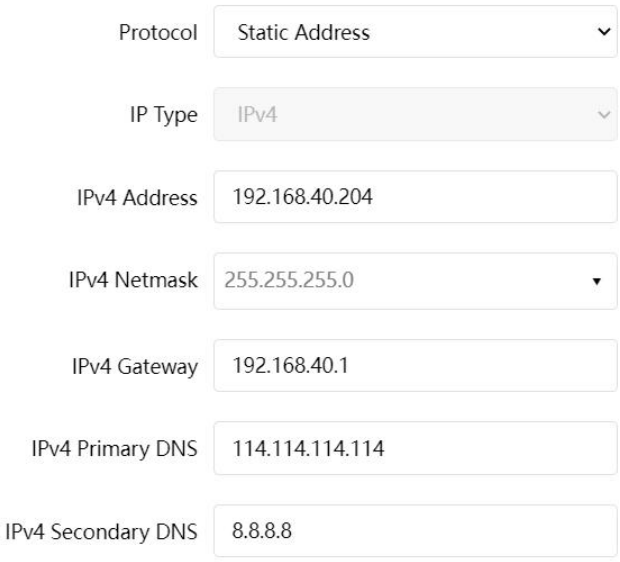
The WAN port can be connected with an Ethernet cable to get Internet access. It supports 3 connection types which can work with both IPv4 and IPv6.
- **Static IP**: configure IPv4 address, netmask and gateway for Ethernet WAN interface.
- **DHCP Client**: configure Ethernet WAN interface as DHCP Client to obtain IPv4 address automatically.
- **PPPoE**: configure Ethernet WAN interface as PPPoE or PPPoEv6 Client.



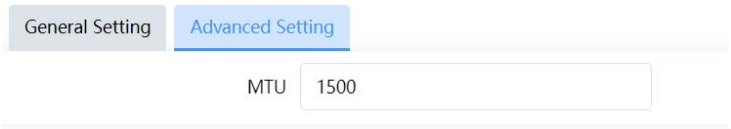
WAN - Status	
Item	**Description**
Uptime	How long has the device been running.
MAC	MAC address of WAN interface.
RX	RX: the data volume and packets received in this interface.
TX	TX: the data volume and packets transmitted from this interface.
IPv4	IPv4 address of WAN interface.

1. Static IP Configuration

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



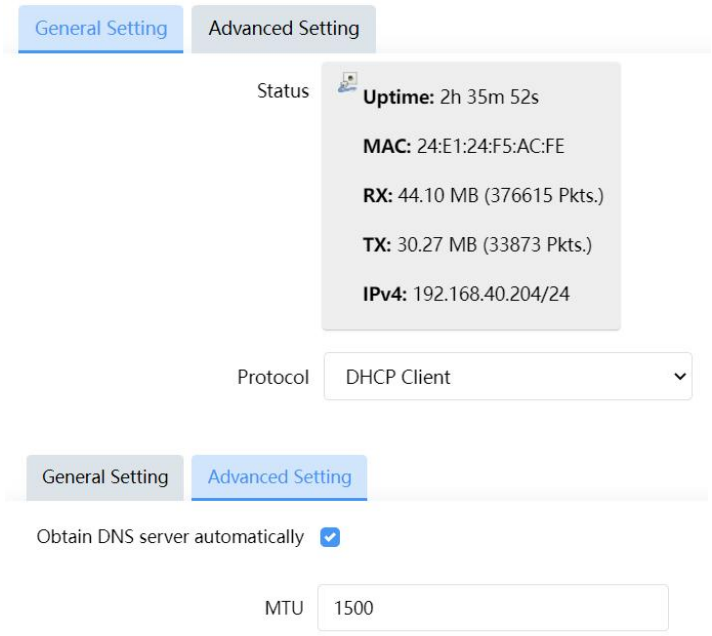
Static Address - General Settings		
Item	**Description**	**Default**
IP Type	It's fixed as IPv4.	IPv4
IPv4 Address	Set the IPv4 address of the WAN port.	--
IPv4 Netmask	Set the Netmask for WAN port.	255.255.255.0
IPv4 Gateway	Set the gateway for WAN port's IPv4 address.	--
IPv4 Primary DNS	Set the primary IPv4 DNS server.	114.114.114.114
IPv4 Secondary DNS	Set the secondary IPv4 DNS server.	8.8.8.8



Static Address - Advanced Settings	
Item	**Description**
MTU	Set the maximum transmission unit. Range: 68-1500.

2. DHCP Client

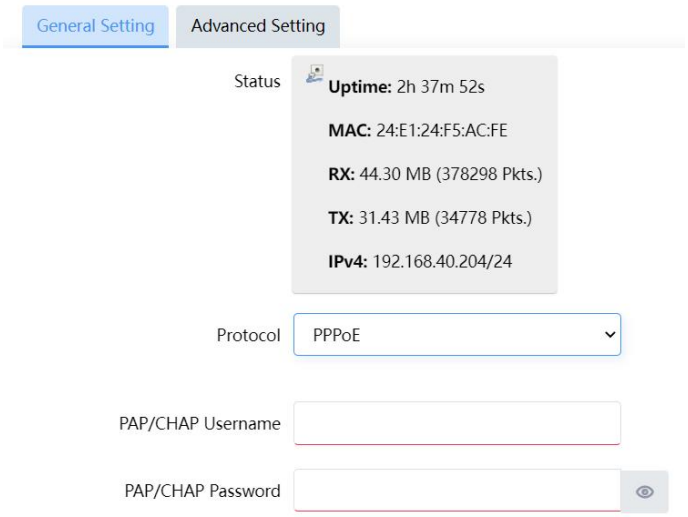
If the external network has DHCP server enabled and has assigned IP addresses to the Ethernet WAN interface, please select this mode to obtain IP address automatically.



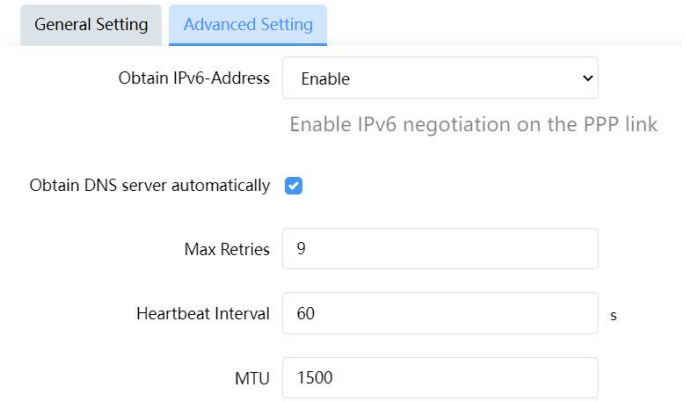
DHCP Client - Advanced Settings	
Item	**Description**
Obtain DNS server automatically	Obtain peer DNS automatically. DNS is necessary when visiting domain name.
MTU	Set the maximum transmission unit. Range: 68-1500.

3. PPPoE/PPPoEv6

PPPoE refers to a point to point protocol over Ethernet. If IPv6 negotiation is enabled, router can get both IPv4 and IPv6 address.



PPPoE - General Settings	
Item	**Description**
PAP/CHAP Username	Enter the username provided by your Internet Service Provider (ISP).
PAP/CHAP Password	Enter the password provided by your Internet Service Provider (ISP).

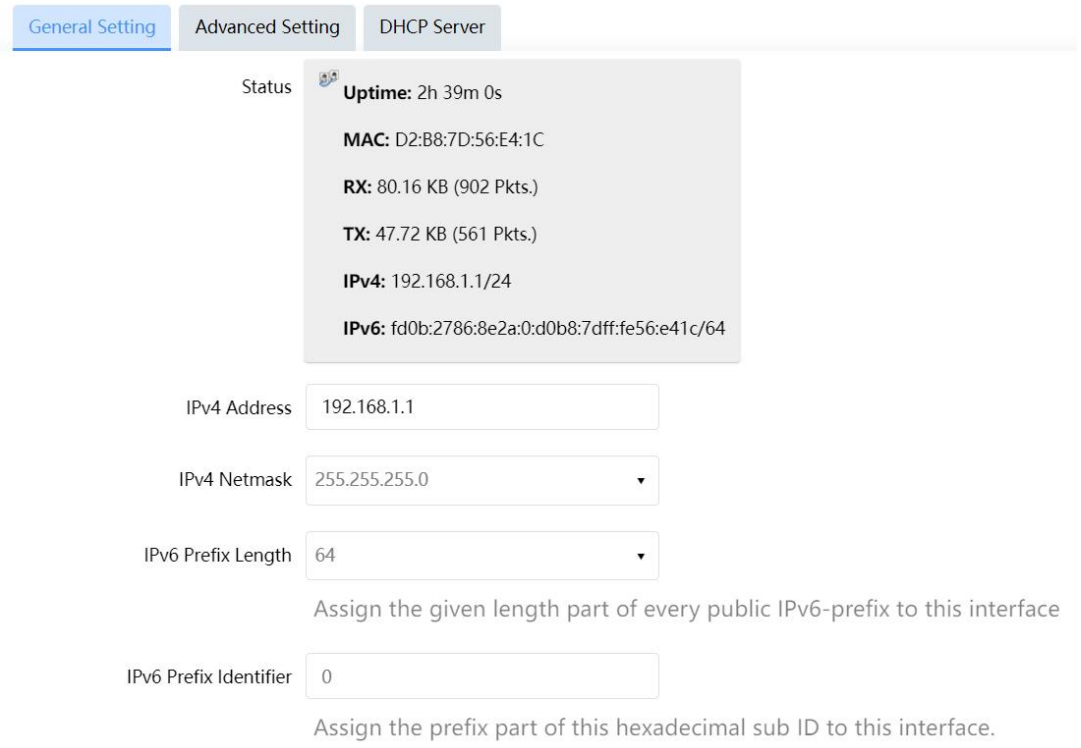


PPPoE - Advanced Settings	
Item	**Description**
Obtain IPv6-Address	Enable IPv6 negotiation on the PPP link.
Obtain DNS server automatically	Obtain peer DNS automatically during PPP dialing. DNS is necessary when visiting domain name.
Max Retries	Set the maximum retry times after it fails to dial up. Range: 0-9.
Heartbeat Interval (s)	Set the heartbeat interval for link detection. Range: 1-600.
MTU	Set the maximum transmission unit. Range: 68-1500.

Related Configuration Example

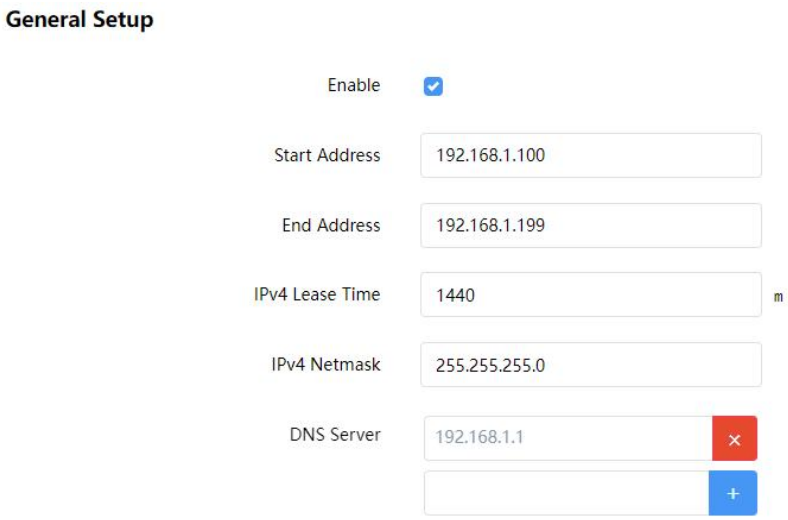
Ethernet WAN Connection

6.2.1.2 LAN/DHCP Server



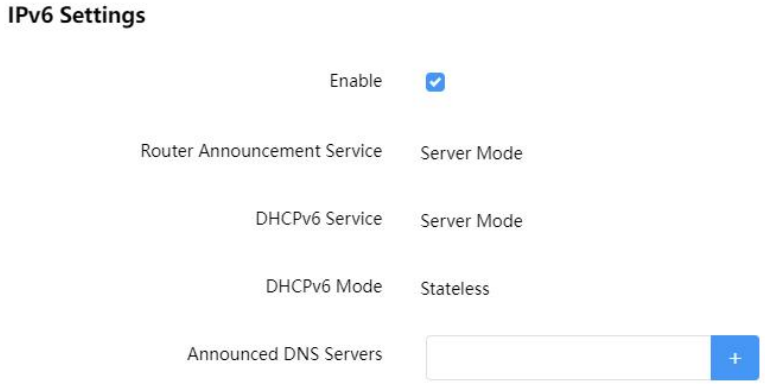
LAN - General Settings	
Item	**Description**
Status	**Uptime:** how long has the device been running.
	MAC: MAC address of LAN interfaces.
	RX: the data volume and packets received in this interface.
	TX: the data volume and packets transmitted from this interface.
	IPv4/IPv6: IPv4/IPv6 address of LAN interfaces.
IPv4 Address	Set the IPv4 address of LAN interface.
IPv4 Netmask	Set the netmask for LAN interface.
IPv6 Prefix Length	Assign a part of given length of every public IPv6-prefix to this interface.
IPv6 Prefix Identifier	Assign prefix parts using this hexadecimal sub-prefix ID for this interface.

LAN - Advanced Settings	
Item	**Description**
MTU	Set the maximum transmission unit. Range: 68-1500.



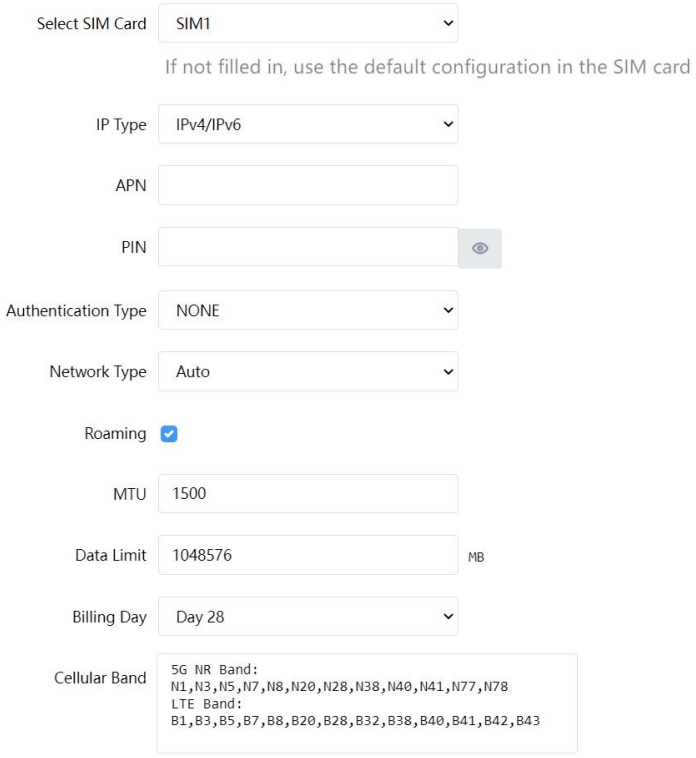
DHCP Server-General Setup	
Item	**Description**
Enable	Enable to disable DHCP for this interface.
Start Address	Define the beginning of the pool of IP addresses which will be leased to DHCP clients.
End Address	Define the end of the pool of IP addresses which will be leased to DHCP clients.
IPv4 Lease time	Set the expiry time of leased addresses, the minimum is 2 minutes

	(2m).
IPv4-Netmask	Set to override the netmask sent to clients. Normally it is calculated from the subnet that is served.
DNS Server	Set the DNS server list for clients.



DHCP Server-IPv6 Settings	
Item	**Description**
Enable	Choose to enable DHCPv6 server when using cellular IPv6 or PPPoE v6.
Router Advertisement Service	It's fixed as server mode.
DHCPv6 Service	It's fixed as server mode.
DHCPv6 Mode	It's fixed as stateless mode.
Announced DNS Servers	Set the DNS server list for clients.

6.2.1.3 Cellular



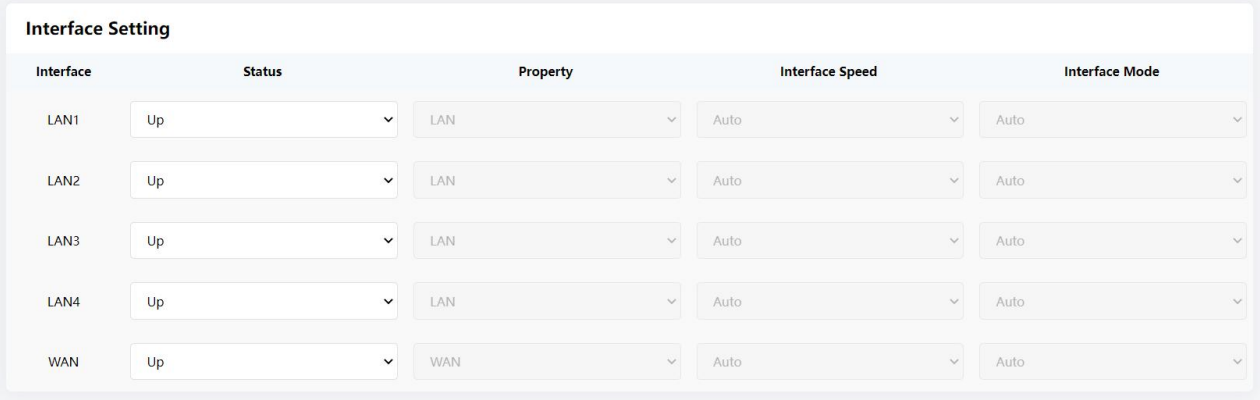
Cellular	
Item	**Description**
Select SIM Card	Select the SIM card you need to configure the settings.
IP Type	Show the Internet protocol type to use for this interface. Option: IPv4, IPv6 and IPv4/IPv6.
APN	Enter the Access Point Name for cellular dial-up connection provided by local ISP.
PIN	Enter a 4-8 characters PIN code to unlock the SIM.
Authentication Type	Select from NONE, PAP, CHAP and PAP/CHAP.
Network Type	Select from Auto, 5G Only, 4G Only and 3G Only. Auto: connect to the network with the strongest signal automatically. 5G Only: connect to 5G network only. And so on.
Roaming	Enable or disable roaming.
MTU	Set the maximum transmission units. Range: 68-1500.
Data Limit	Set the data limit of this month. If data traffic exceeds the limit, the SIM card will be forbidden this month. The default is blank (no limited).
Billing Day	Clear the monthly data statistics when reaching the billing day of this month.
Cellular Band	Select the 5G NR and 4G LTE bands used to register cellular network. It can be used to optimize cellular speeds by selecting specific bands.

Related Application

Cellular Application

6.2.1.4 Interface Settings

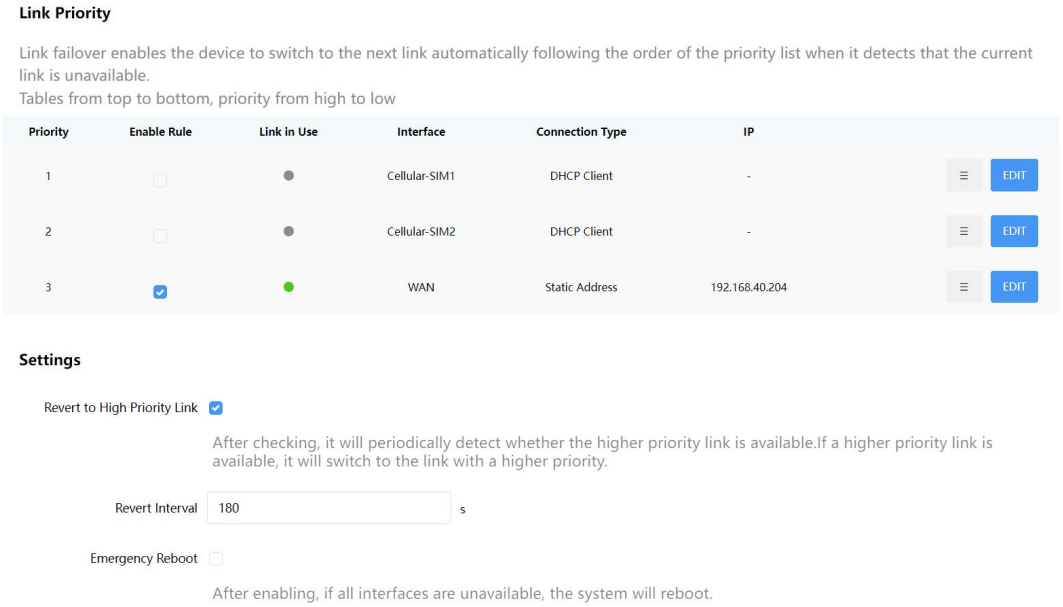
UR75 cellular router supports 5 Gigabit Ethernet ports. This page display the properties of all Ethernet ports and allows to control the status of these ports.



Interface Setting	
Item	**Description**
Interface	Users can define the Ethernet ports according to their needs.
Status	Set the status of Ethernet port; select **Up** to enable and **Down** to disable.
Property	The Ethernet port's type, fixed as a WAN port or a LAN port.
Interface Speed	Ethernet port speed is fixed as Auto.
Interface Mode	Ethernet port mode is fixed as Auto.

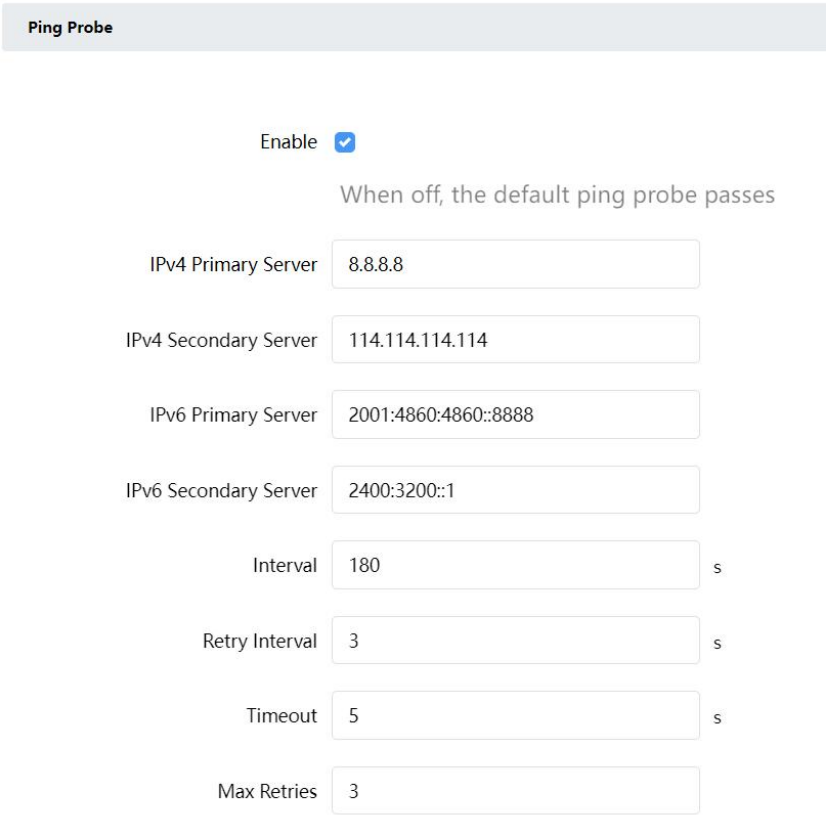
6.2.1.5 Link Failover

This section describes how to configure link failover strategies, their priority and the ping settings, each rule owns its ping rules by default. The router will follow the priority to choose the next available interface to access the internet, make sure you have enabled the full interface that you need to use here. If priority 1 can only use IPv4, UR75 will select a second link in which IPv6 works as the main IPv6 link and vice versa.



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 choose 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. For cellular interface, it only supports as DHCP client.

IP	Display the IP address of the interface.
☰	Drag this button to adjust the priority of network links. The top of the list has the highest priority.
Edit	Click to edit ping probe settings of every network link.
Settings	
Revert to high priority link	When enabled, periodically detect whether the high-priority link can be pinged, and if so, switch the link with a higher priority.
Revert Interval	Specify the number of seconds that you should wait for switching to the link with higher priority, range: 1 - 21600s.
Emergency Reboot	Enable to reboot the device if not any link is available.

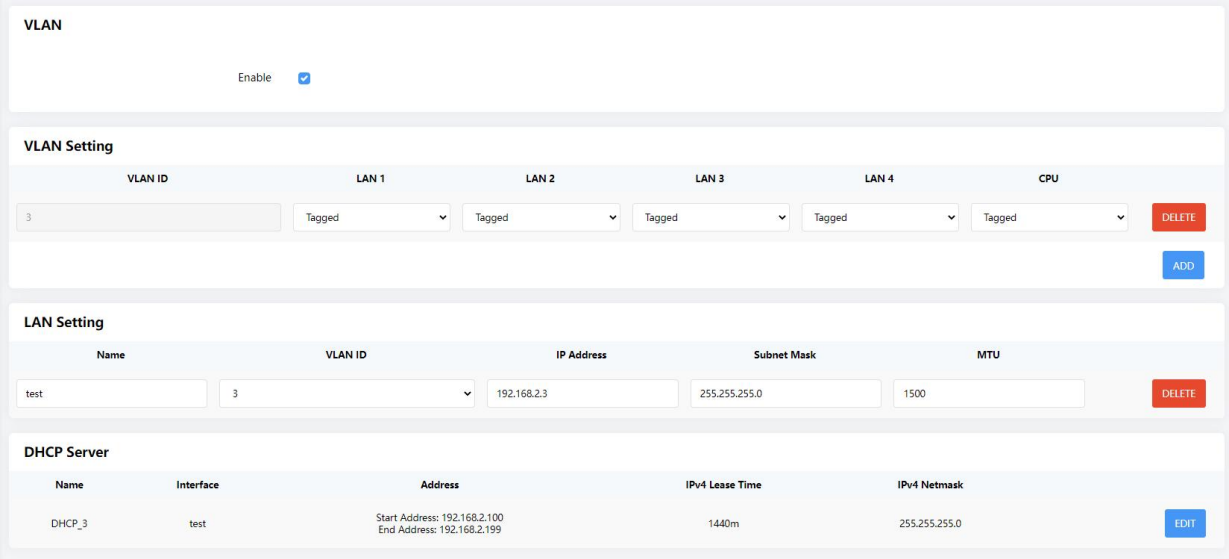


Ping Probe	
Item	**Description**
Enable	If enabled, the router will periodically detect the connection status of the link by sending ICMP packets.
IPv4/IPv6 Primary Server	The router will send ICMP packet to the IPv4/IPv6 address to determine whether the network connection is still available or not.
IPv4/IPv6 Secondary Server	The router will try to ping the alternative server address 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

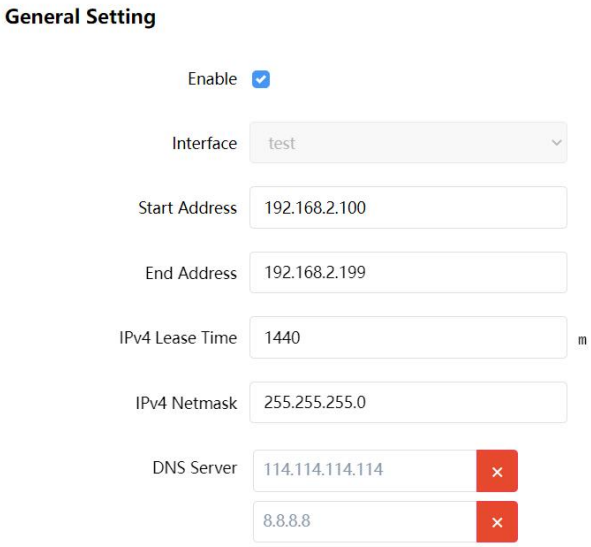
	response to a ping request. If it does not receive a response for the amount of time predefined in this field, the ping request will be considered as fail.
Max Retries	The retry times of the router sending ping request until determining that the connection has failed.

6.2.1.6 Switch (VLAN)

VLAN is a new data exchange technology that realizes virtual work groups by logically dividing the LAN devices into network segments.



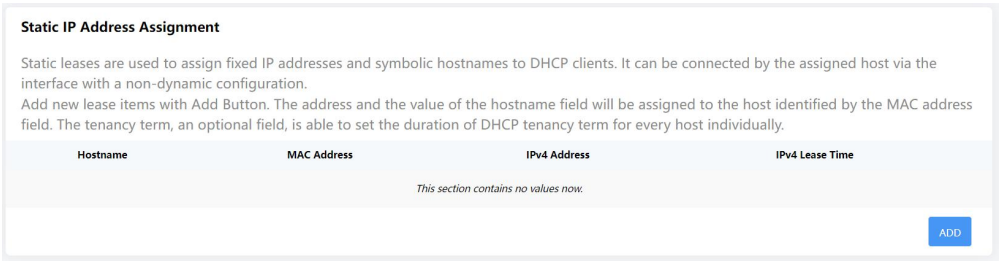
Switch	
Item	**Description**
VLAN	Enable or disable VLAN feature.
VLAN Settings	
VLAN ID	Set the label ID of the VLAN. Range: 3-4094.
LAN 1/2/3/4	Make the VLAN bind with the corresponding ports and select status from Tagged, Untagged and"Close for Ethernet frame on trunk link.
CPU	Control communication between VLAN and other networks.
LAN Settings	
Name	Set interface name of VLAN.
VLAN ID	Select VLAN ID of the interface.
IP Address	Set IP address of LAN port which is different from WAN, LAN and other VLANs.
Subnet Mask	Set Netmask of LAN port.
MTU	Set the maximum transmission unit of LAN port. Range: 68-1500.



Switch - DHCP Server	
Item	**Description**
Enable	Enable to disable DHCP for this VLAN interface. The DHCP server can only be deleted when you deleted corresponding LAN settings,
Interface	Show the VLAN interface name of the DHCP server.
Start Address	Define the beginning of the pool of IP addresses which will be leased to DHCP clients.
End Address	Define the end of the pool of IP addresses which will be leased to DHCP clients.
IPv4 Lease time	Set the expiry time of leased addresses, the minimum is 2 minutes (2m).
IPv4 Netmask	Set to override the netmask sent to clients. Normally it is calculated from the subnet that is served.
DNS Server	Set the DNS server list for clients.

6.2.1.7 Static IP Address Assignment

When LAN/VLAN interface works as DHCP server, users can assign fixed IP addresses and symbolic hostnames to devices with fixed MAC addresses.

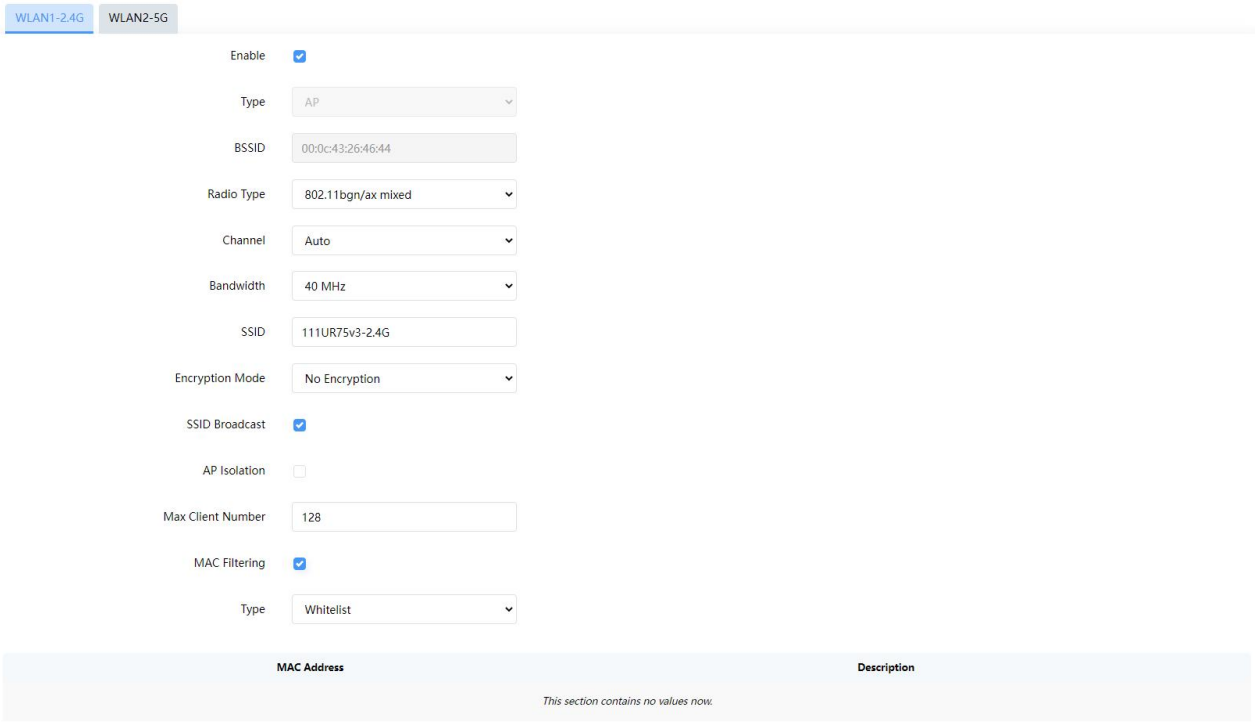


Static IP Address Assignment	
Item	**Description**
Hostname	The hostname of static leases.
MAC Address	The MAC address of the DHCP client.

IPv4 Address	The IPv4 address assigned to the client.
IPv4 Lease time	Time remaining for the client.

6.2.2 WLAN (Wi-Fi Version Only)

This section explains how to set the related parameters for Wi-Fi network. UR75 supports both 2.4G and 5G Wi-Fi and they can work at the same time.



WLAN	
Item	**Description**
Enable	Enable/disable WLAN.
Type	The work type is fixed as AP.
BSSID	The MAC address of the access point.
Radio Type	Select radio type.
Channel	Select wireless channel from 1 to 13 or select Auto.
Bandwidth	Select bandwidth. The options are 20MHz and 40MHz.
SSID	Define the SSID of the access point.
Encryption Mode	Select encryption mode. The options are No Encryption, WEP Open System , WEP Auto, WEP Shared Key, WPA-PSK, WPA2-PSK, WPA3-PSK, WPA-PSK/WPA2-PSK and WPA2-PSK/WPA3-PSK.
Cipher	Select cipher when using PSK type encryption mode. The options are AES, TKIP and AES/TKIP.
Key	Define the key of access point.
Group Rekey Interval	The interval of changing the cipher key.
SSID	When SSID broadcast is disabled, other wireless devices can't find the SSID,

Broadcast	and users have to enter the SSID manually to access to the wireless network.
AP Isolation	When AP isolation is enabled, all users that access to the AP are isolated without communicating with each other.
Max Client Number	Type the max client number that the access point supports, range: 1-128.
MAC Filtering	
MAC Filtering	Enable or disable the filter of Wi-Fi client MAC addresses.
Type	**Whitelist:** Only the listed MAC addresses are allowed to connect to the router's wireless access point. **Blacklist:** The listed MAC addresses are not allowed to connect to the router's wireless access point.

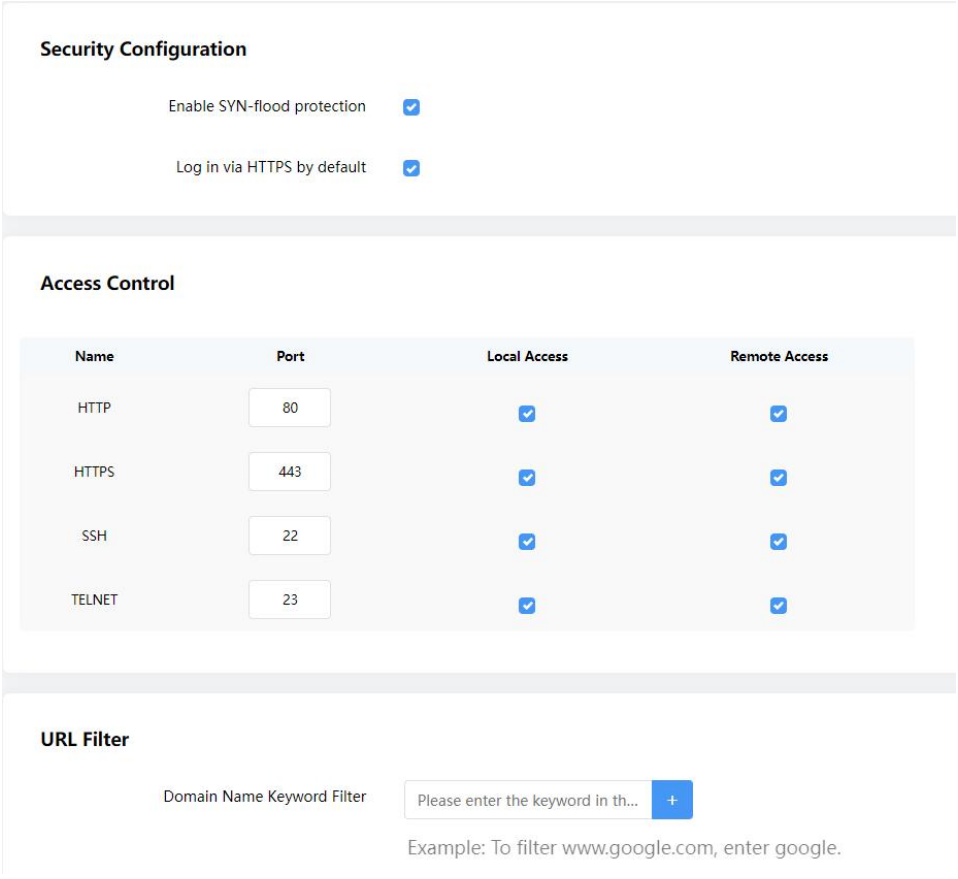
Related Topic

Wi-Fi Application Example

6.2.3 Firewall

This section describes how to set the firewall parameters, including security, ACL, DMZ, Port Mapping and custom iptables rules. After setting, users can go to **Status > Firewall** to check if firewall settings work.

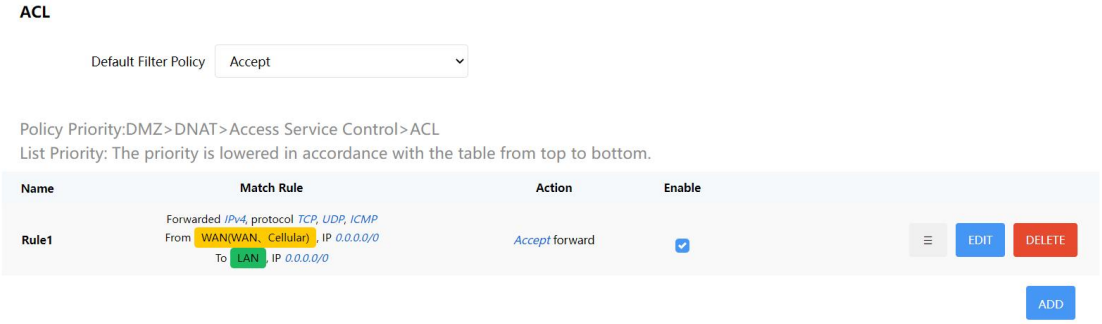
6.2.3.1 General Settings



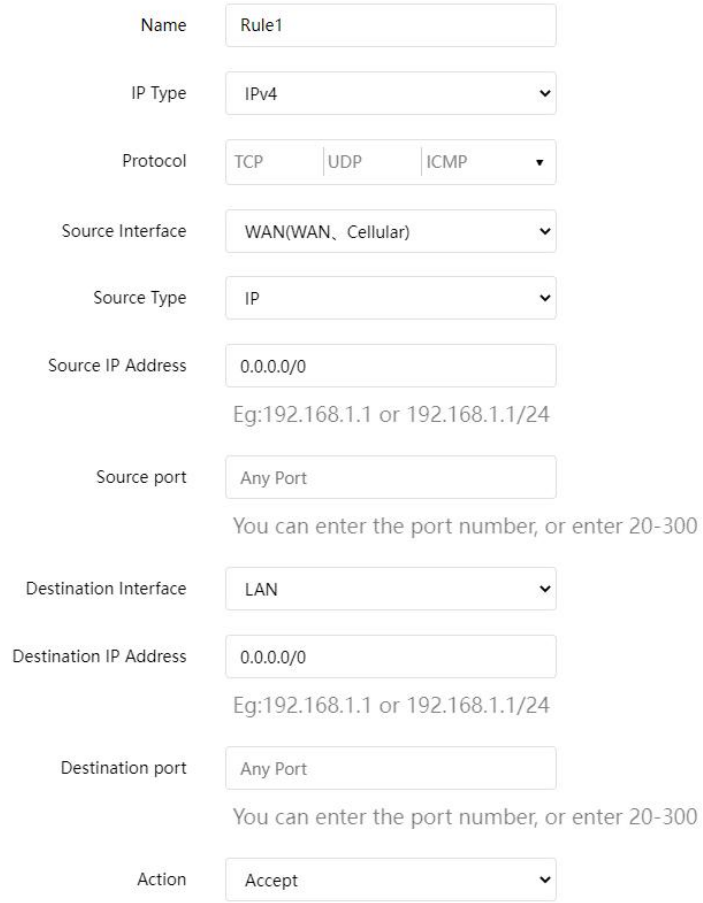
General Setting		
Item	**Description**	**Default**
Security Configuration		
Enable SYN-flood Protection	Enable/disable SYN-flood protection. SYN-flood protection allows to protect from a DDoS attack that exploits part of the normal TCP three-way handshake to consume resources on the targeted server and render it unresponsive.	Enable
Log in using HTTPS by default	Log in the web GUI of device via HTTPS by default.	Enable
Access Control		
Port	Set port number of the services. Range: 1-65535.	--
Local Access	Access the router locally.	Enable
Remote Access	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 the 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 via SSH after the option is checked.	22
URL Filter		
Domain Name Keyword Filtering	You can block specific website by entering keyword from a domain name. After filtering, the devices under LAN ports can not access corresponding websites. The maximum number of characters allowed is 64.	

6.2.3.2 ACL

The 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 a router receives a 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.



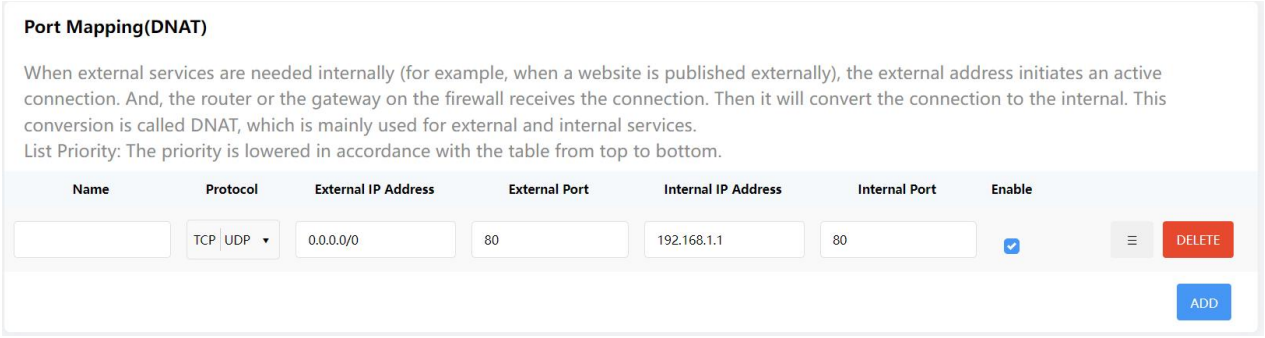
ACL	
Item	**Description**
Default Filter Policy	The packets which are not included in the access control list will be processed by the default filter policy. **Accept:** allow all traffic out of devices under LAN ports. **Drop:** deny all traffic out of devices under LAN ports.
Enable	Enable this ACL rule.
☰	Drag this button to adjust the priority of ACL rules. The top of the list has the highest priority.
Edit	Click to edit the details of this ACL rule.
Delete	Delete this ACL rule.



ACL - Add/Edit	
Name	Define a unique name for this ACL rule.
Type	Select type as IPv4 or IPv6.
Protocol	Select protocol among TCP, UDP and ICMP.
Source Interface	Select the source interface type from Device Output, LAN, VLAN or WAN (WAN, Cellular, WLAN). Device Output means the packets coming from router itself.
Source Type	When using IPv4 type, select the address type as IP, MAC or IP+MAC.
Source IP/MAC Address	Set source network address according to address type. (0.0.0.0/0 means all).
Source Port	Set specific source port number or port range, example: 20-300.
Destination Interface	Select the destination interface type from LAN, WAN (WAN, Cellular, WLAN), VLAN or Device Input. Device Input means the packets going to router itself.
Destination IP Address	Set destination network address (0.0.0.0/0 means all).
Destination Port	Set specific source port number or port range, example: 20-300.
Action	Select action as Accept or Drop.

6.2.3.3 Port Mapping (DNAT)

When external services are needed internally (for example, when a website is published externally), th e external address initiates an active connection. And, the router or the gateway on the firewall receiv es 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.



Port Mapping (DNAT)	
Item	**Description**
Name	Define a unique name of the port mapping rule.
Protocol	Select TCP or UDP for your application requirements.
External IP Address	Specify the host or network which can access local IP address. 0.0.0.0/0 means all.
External Port	Set the port or port range from which incoming packets are forwarded, example: 20-300.
Internal IP Address	Enter the IP address that packets are forwarded to after

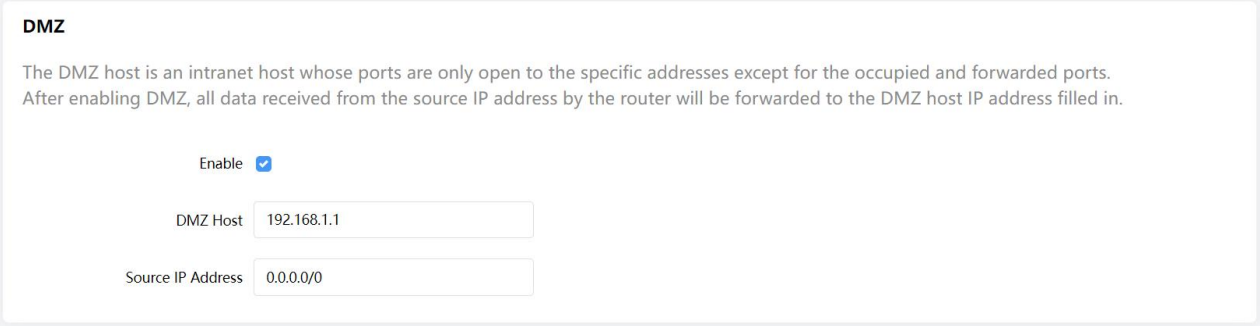
	receiving from the incoming interface.
Internal Port	Enter the port or port range that packets are forwarded to after receiving from the incoming port(s). When setting port range, the value should be the same as external port range.
Enable	Enable or disable this port mapping rule.
☰	Drag this button to adjust the priority of port mapping rules. The top of the list has the highest priority.
Delete	Delete this rule.

Related Configuration Example

NAT Application Example

6.2.3.4 DMZ

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



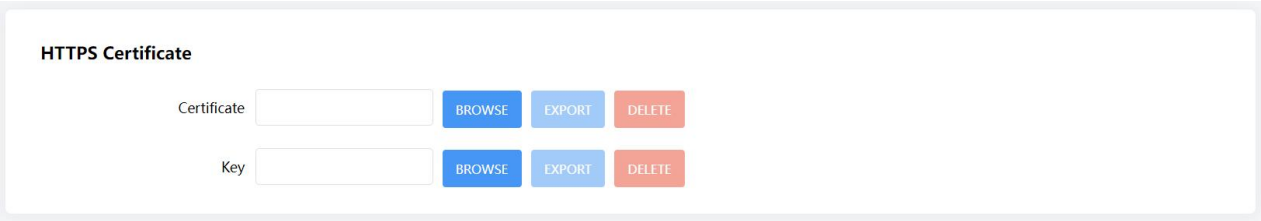
DMZ	
Item	**Description**
Enable	Enable or disable DMZ.
DMZ Host	Enter the IP address of the DMZ host on the internal network.
Source IP Address	Set the source IP address which can access to DMZ host. "0.0.0.0/0" means any address.

6.2.3.5 Custom Rules

In this page, you can enter your own custom firewall iptables rules and these will get executed as a Linux shell script.

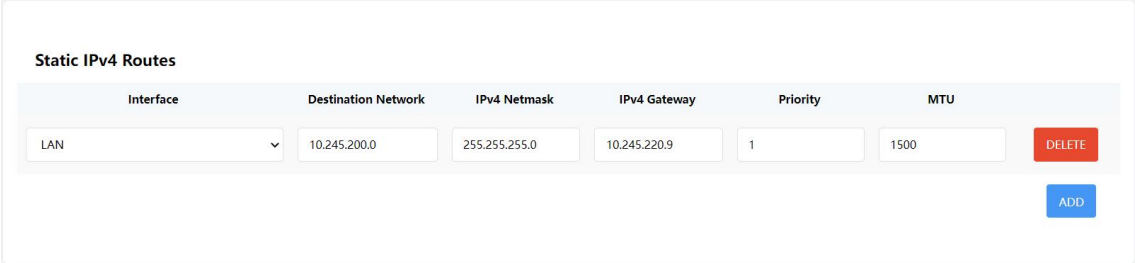
6.2.3.6 Certificates

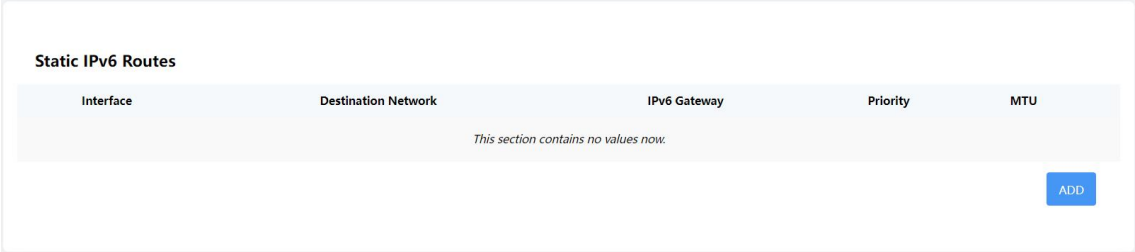
In this page, you can import the HTTPS certificates for router web GUI secure access.



6.2.4 Static Routes

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 users.

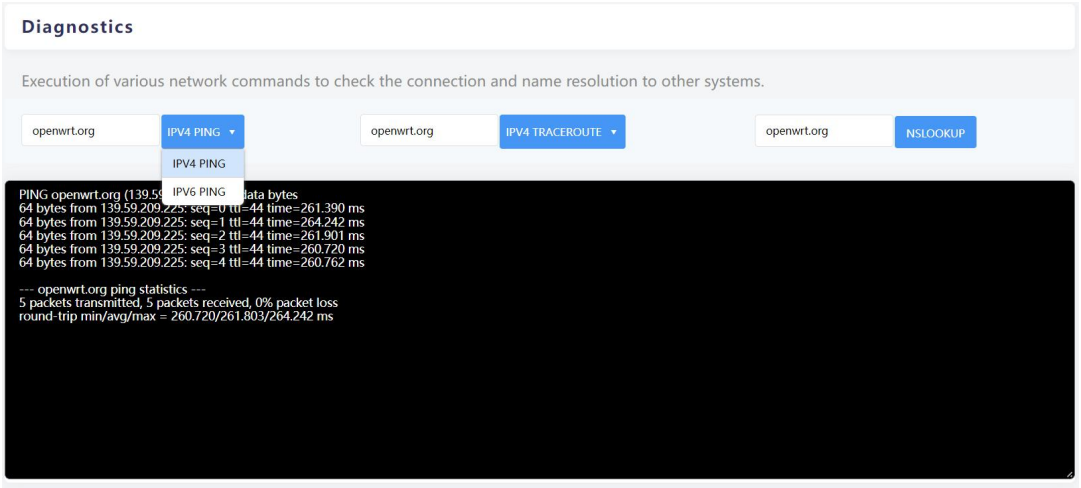




Static Routes	
Item	**Description**
Interface	The interface allows the data to reach the destination address.
Destination Network	Enter the destination IPv4/IPv6 address.
IPv4 Netmask	Enter the subnet mask of IPv4 destination address.
IPv4/IPv6 Gateway	IPv4/IPv6 address of the next router that will be passed by before the input data reaches the destination address.
Priority	Smaller value refers to higher priority. Range: 1-255.
MTU	Set the maximum transmission unit. Range: 68-1500.

6.2.5 Diagnostics

Network Utilities includes IPv4/IPv6 ping, IPv4/IPv6 traceroute, nslookup the command-line tool.



Network Utilities	
Item	**Description**
IPv4 Ping	Click to ping outer network from the device in IPv4.
IPv6 Ping	Click to ping outer network from the device in IPv6.
IPv4 Traceroute	Address of the destination host to be detected in IPv4.
IPv6 Traceroute	Address of the destination host to be detected in IPv6.
Nslookup	Click to obtain the mapping between domain name and IP address, or other DNS records.

6.3 VPN

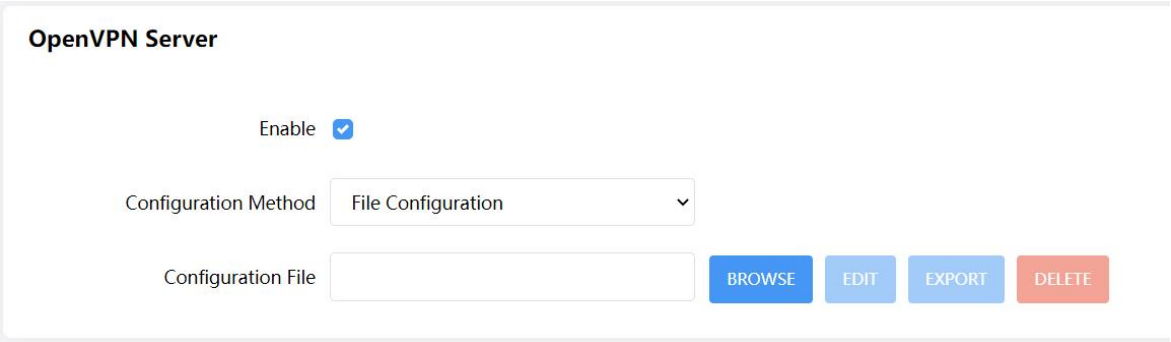
Virtual Private Networks, also called VPNs, are used to securely connect two private networks together so that devices can connect from one network to the other network via secure channels.

6.3.1 OpenVPN

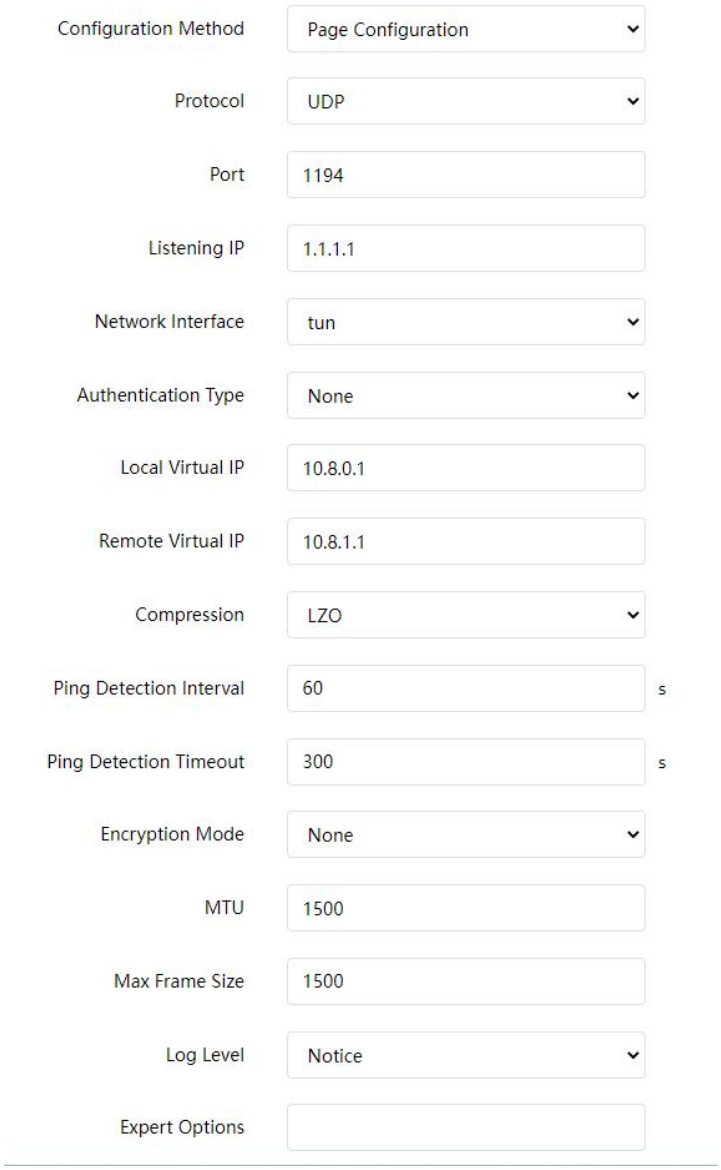
OpenVPN is an open source virtual private network (VPN) product that offers a simplified security framework, modular network design, and cross-platform portability. The default OpenVPN version of UR75 is 2.5.3.

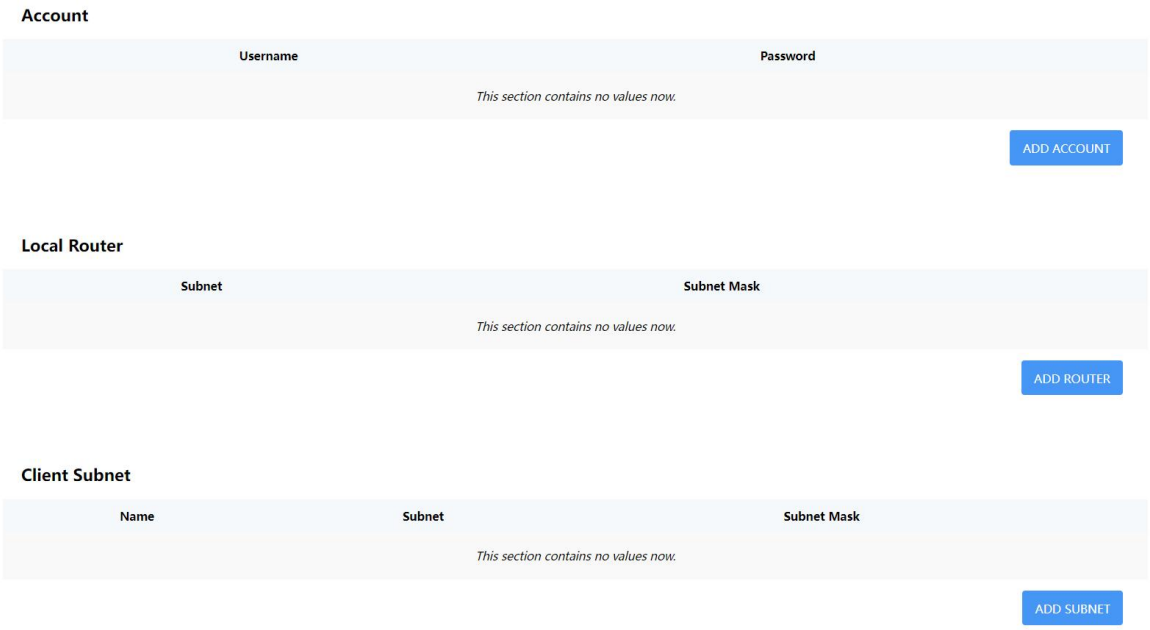
6.3.1.1 OpenVPN Server

UR75 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.



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.



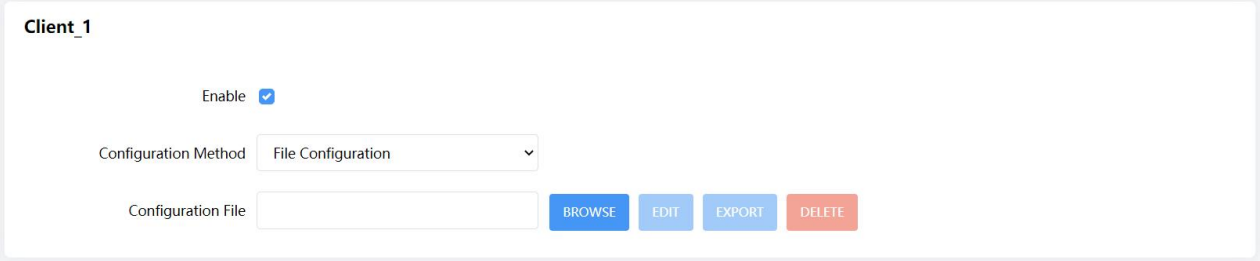


OpenVPN Server - Page Configuration	
Item	**Description**
Protocol	Select a transport protocol used by connection from UDP and TCP.
Listening IP	Enter the local hostname or IP address for bind. If left blank, OpenVPN server will bind to all interfaces.
Port	Enter the TCP/UCP service number for OpenVPN client connection. Range: 1-65535.
Network 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 **VPN > OpenVPN > 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 **VPN > OpenVPN > 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: 1-128.

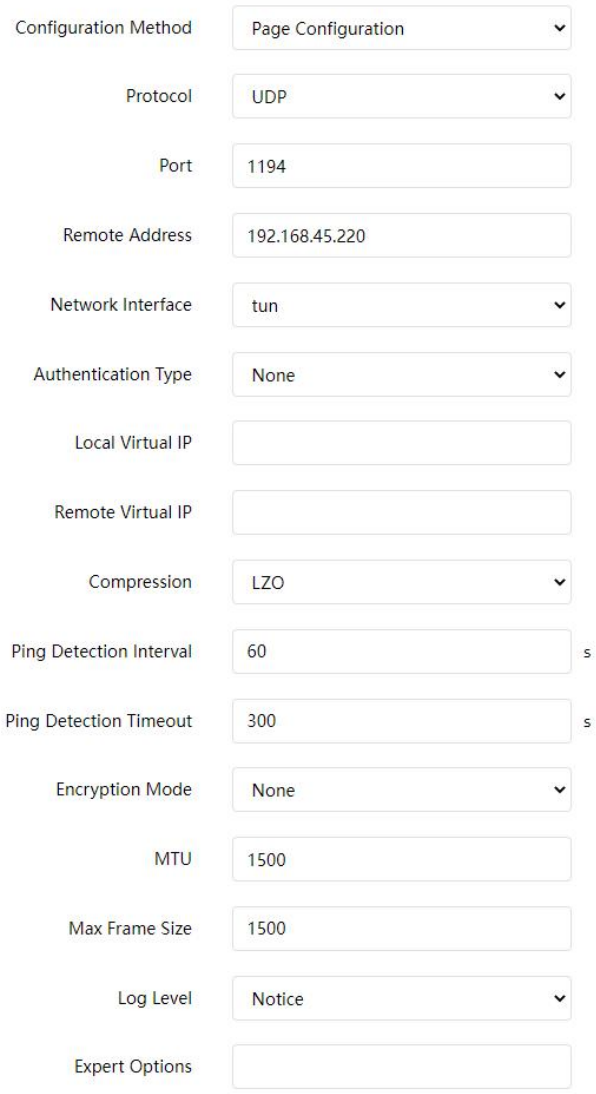
	Note: please adjust log severity to Info if you need to connect many clients.
Enable CRL	Enable or disable CRL verify.
Enable Client to Client	When enabled, openVPN clients can communicate with each other.
Enable Dup Client	Allow multiple clients to connect with the same common name or certification.
Enable TLS Authentication	Disable or enable TLS authentication when authentication type is X.509 cert. After being enabled, go to **VPN > OpenVPN > Certifications** page to import a ta.key to **TA** field. **Note:** this option only supports tls-auth. For tls-crypt, please add this format string on expert option: tls-crypt /etc/openvpn/openvpn-client1-ta.key
Compression	Select to enable or disable LZO to compress data.
Ping Detection Interval	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.
Ping Detection Timeout	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.
Encryption Mode	Select from NONE, BF-CBC, DES-CBC, DES-EDE3-CBC, AES-128-CBC, AES-192-CBC and AES-256-CBC.
MTU	Enter the maximum transmission unit. Range: 68-1500.
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:** auth SHA256; key direction 1
Account	
Username & Password	Set username and password for OpenVPN client when authentication type is username/password.
Local Router	
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.

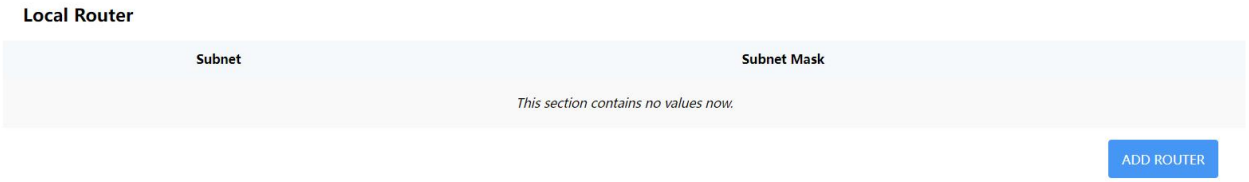
6.3.1.2 OpenVPN Client

UR75 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.



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.





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.
Network 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 **VPN > OpenVPN > 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 **VPN > OpenVPN > 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	Disable or enable TLS authentication when authentication type is X.509 cert. After being enabled, go to **VPN > OpenVPN > Certifications** page to import a ta.key to **TA** field. **Note:** this option only supports tls-auth. For tls-crypt, please add this format string on expert option: tls-crypt /etc/openvpn/openvpn-client1-ta.key
Compression	Select to enable or disable LZO to compress data.
Ping Detection Interval	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.
Ping Detection Timeout	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.
Encryption Mode	Select from NONE, BF-CBC, DES-CBC, DES-EDE3-CBC, AES-128-CBC,

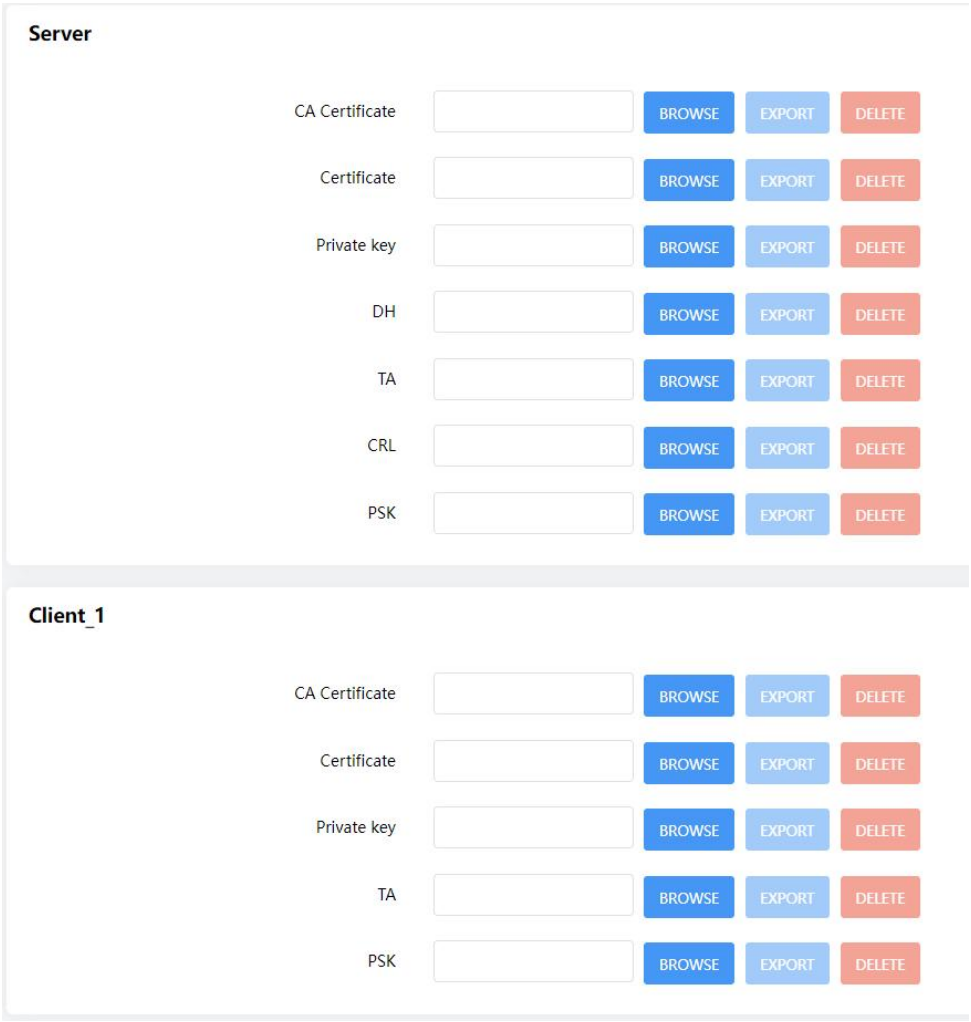
	AES-192-CBC and AES-256-CBC.
MTU	Enter the maximum transmission unit. Range: 128-1500.
Max Frame Size	Set the maximum frame size. Range: 128-1500.
Verbose Level	Select from ERROR, WARING, NOTICE and DEBUG.
Expert Options	User can enter some initialization strings in this field and separate the strings with semicolon. **Example:** auth SHA256; key direction 1
Local Route	
Subnet	Set the local route's IP address.
Subnet Mask	Set the local route's netmask.

Related Configuration Example

OpenVPN Client Application Example

6.3.1.3 Certificate

When using page configuration of OpenVPN server or client, user can import/export necessary certificate and key files to this page according to the authentication types.

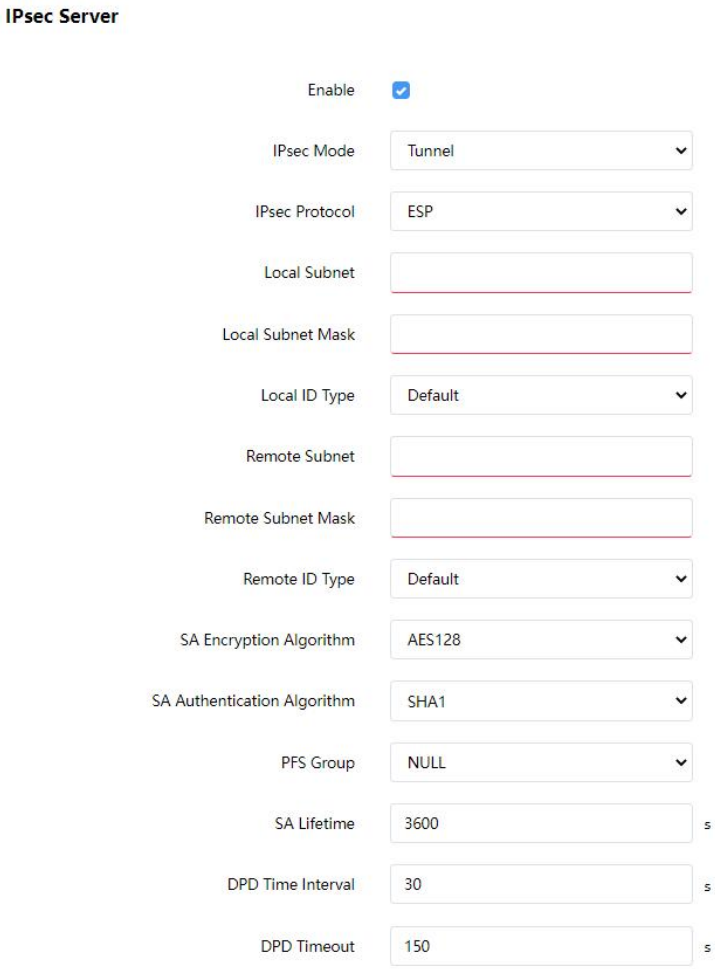


6.3.2 IPsecVPN

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 computer.

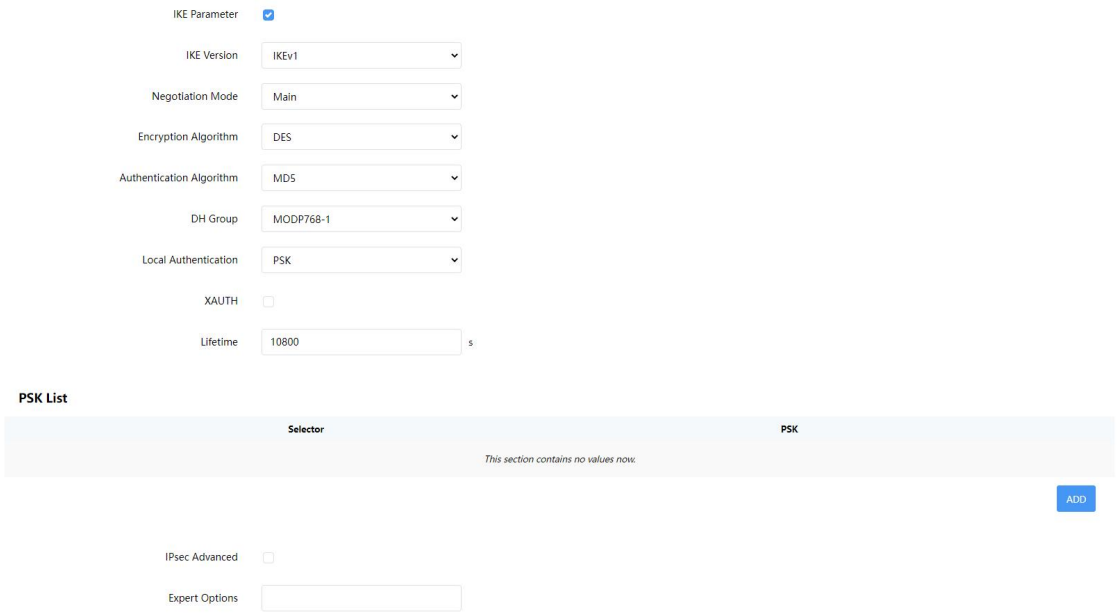
IPsec provides three choices of security service: Authentication Header (AH), Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE). AH essentially allows authentication of the senders' data. ESP supports both authentications of the sender and data encryption. IKE is used for cipher code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

6.3.2.1 IPSec Server



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.
Local Subnet Netmask	Enter the local LAN netmask on the IPsec tunnel.

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.
Remote Subnet Mask	Enter the remote LAN netmask on the IPsec tunnel.
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
SA Encryption Algorithm	Select AES128, AES192 or AES256.
SA Authentication Algorithm	Select SHA1 or SHA2-256.
PFS Group	Select NULL, MODP768_1 , MODP1024_2 or MODP1536_5.
SA Lifetime	Set the lifetime of IPsec SA. Range: 60-86400 s.
DPD Interval Time	Set DPD retry interval to send DPD requests. Range: 2-60 s
DPD Timeout	When using IKE V1, set DPD timeout to detect the remote side fails. Range: 10-3600s.

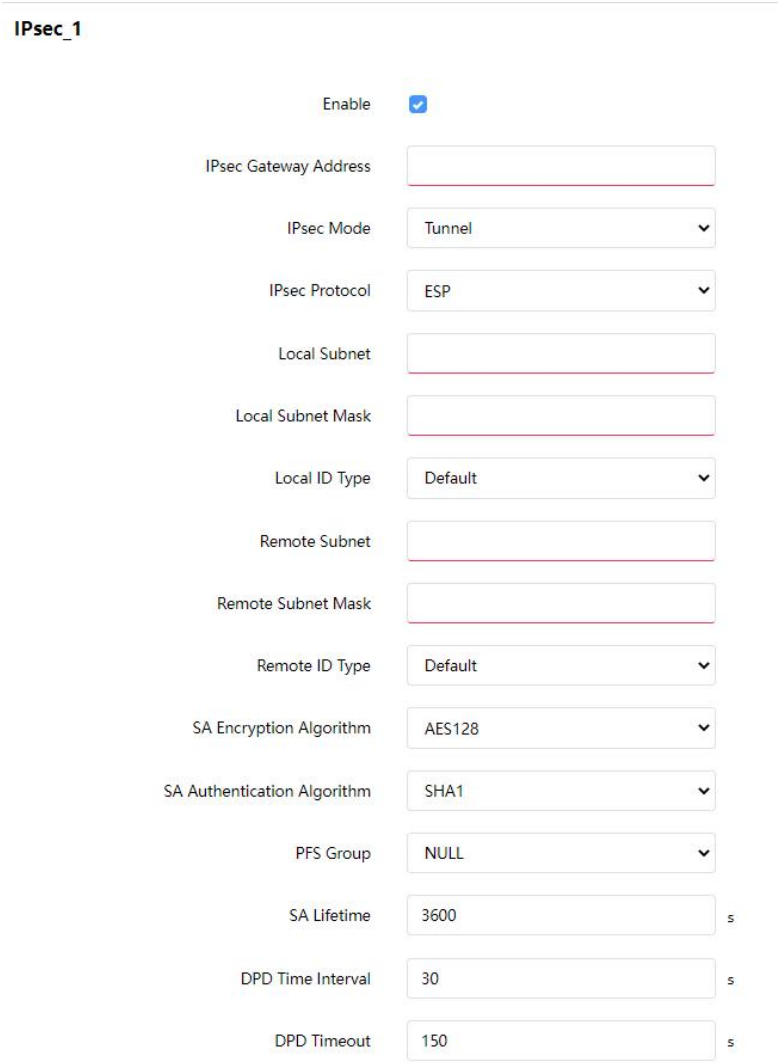


IKE Parameter	
Item	**Description**
IKE Version	Select the method of key exchange from IKEv1 and IKEv2.

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 or MODP1536_5.
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 **VPN > IPsec > 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.
XAUTH	When using IKEv1, define XAUTH username and password after XAUTH is enabled.
Lifetime	Set the lifetime in IKE negotiation. Range: 60-86400 s.
XAUTH List	
Username	Define the username used for the client xauth authentication.
Password	Define the password used for the client xauth authentication.
PSK List	
Selector	Set the selector as IP address or local ID of IPsec client. If it is left blank, all clients can use this PSK to complete authentication.
PSK	Define the pre-shared key.
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.
Expert Options	User can enter some other initialization strings in this field to add extra settings and separate the strings with semicolon.

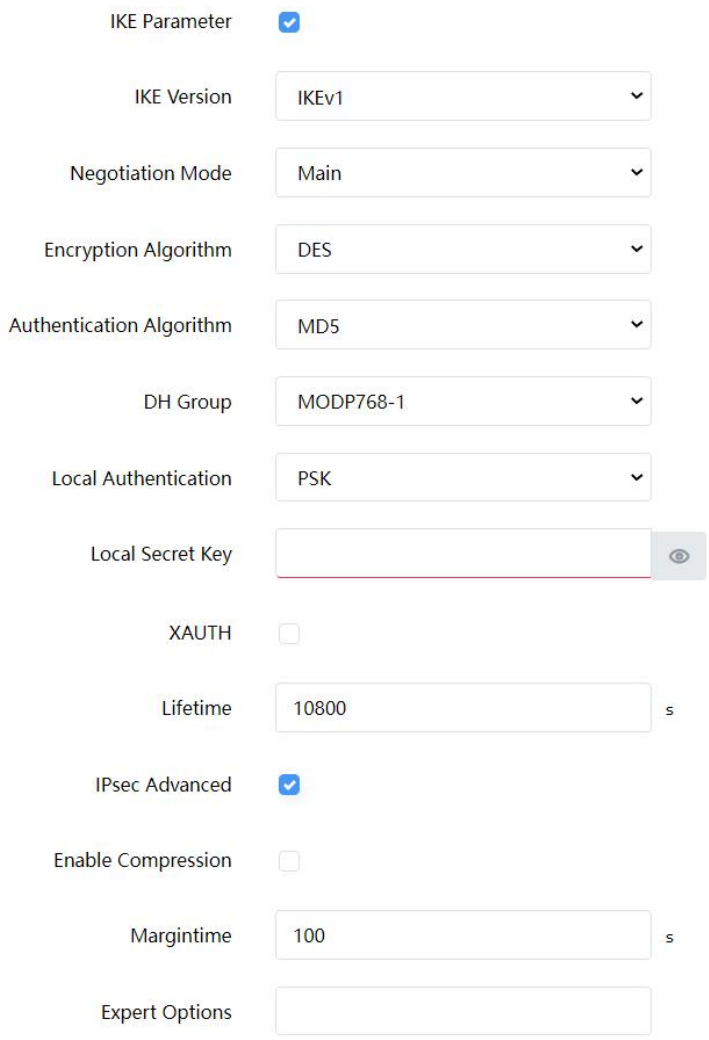
6.3.2.2 IPSec Client

UR75 supports running at most 3 IPsec clients at the same time.



IPsec Client	
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 ESP or AH.
Local Subnet	Enter the local LAN subnet IP address on the IPsec tunnel.
Local Subnet Netmask	Enter the local LAN netmask on the IPsec tunnel.
Local ID Type	Select the identifier type to send 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 that on the IPsec tunnel.
Remote Subnet Mask	Enter the remote LAN netmask on the IPsec tunnel.
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
SA Encryption Algorithm	Select AES128, AES192 or AES256.
SA Authentication Algorithm	Select SHA1 or SHA2-256.
PFS Group	Select NULL, MODP768_1 , MODP1024_2 or MODP1536_5.
SA Lifetime	Set the lifetime of IPsec SA. Range: 60-86400 s.
DPD Interval Time	Set DPD retry interval to send DPD requests. Range: 2-60 s
DPD Timeout	When using IKEv1, set DPD timeout to detect the remote side fails. Range: 10-3600 s.

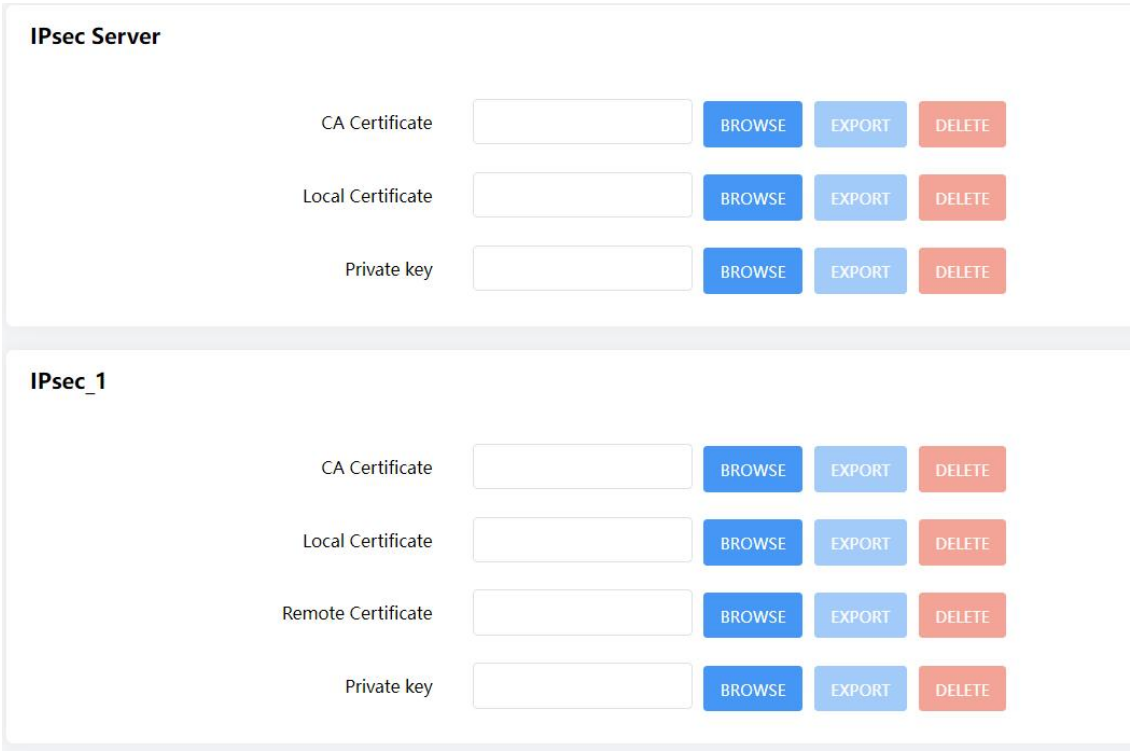


IKE Parameter

Item	Description
IKE Version	Select the method of key exchange of IKEv1 or 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 or MODP1536_5.
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 **VPN > IPsec > Certifications** page to import CA certificate, local certificate and private key to corresponding fields.
Local Secret Key	Enter the pre-shared key which is defined on serer side.
Remote Authentication	Select PSK or CA. **PSK:** use pre-shared key to complete the authentication. **CA:** use certificate to complete the authentication.
Remote Key	Enter the pre-shared key which is defined on server side.
XAUTH	When using IKEv1, define XAUTH username and password after XAUTH is enabled.
Lifetime	Set the lifetime in IKE negotiation. Range: 60-86400 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.
Expert Options	User can enter some other initialization strings in this field to add extra settings and separate the strings with semicolon.

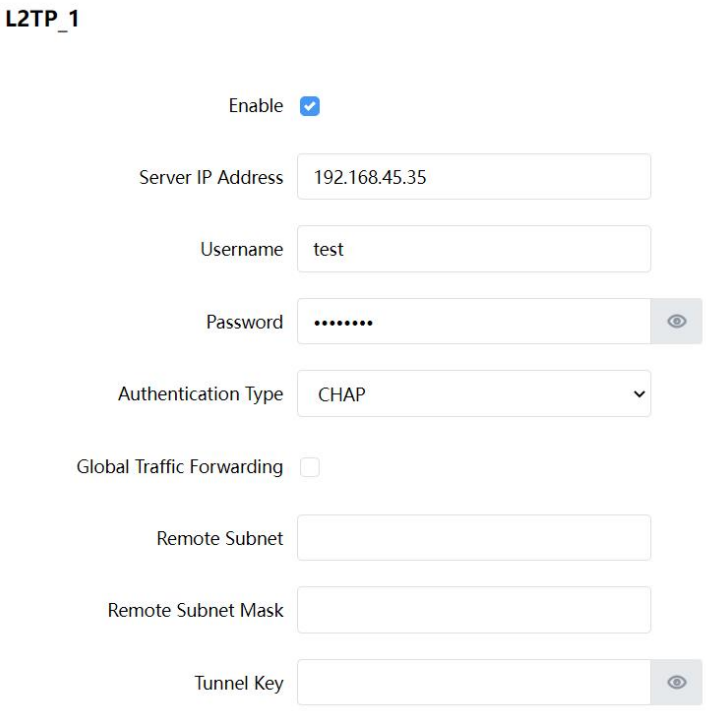
6.3.2.3 Certificate

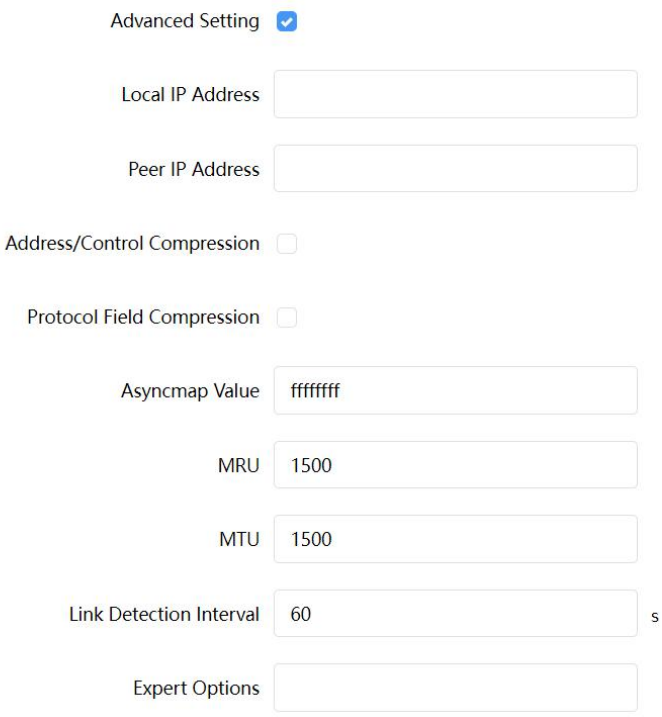
When using local authentication of IPsec server or client as CA, user can import/export necessary certificate and key files to this page.



6.3.3 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.



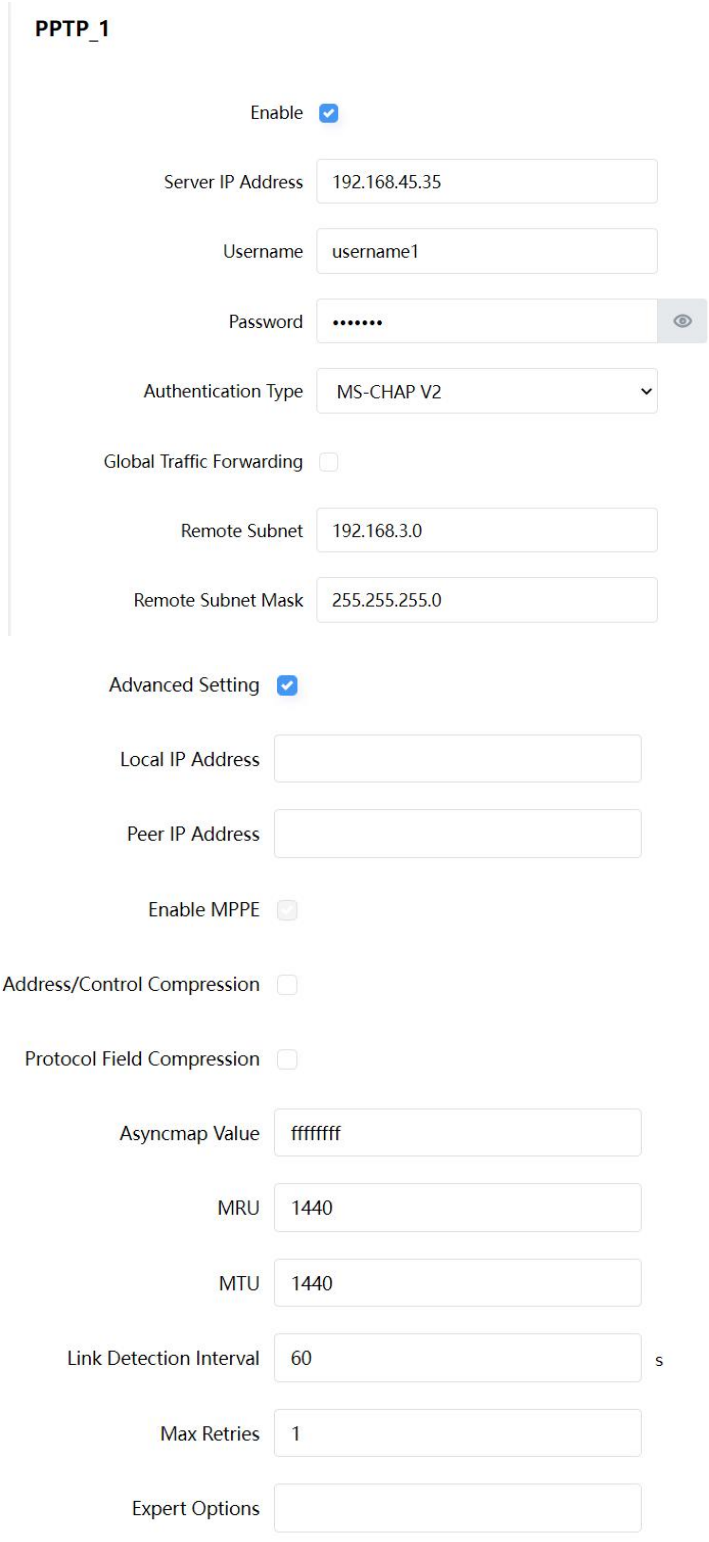


L2TP	
Item	**Description**
Enable	Enable or disable L2TP client.
Server IP Address	Enter remote L2TP server's IP address or domain name.
Username	Enter the username that L2TP server provides.
Password	Enter the password that L2TP server provides.
Authentication Type	Select authentication type used to secure data sessions.
Global Traffic Forwarding	All the data traffic will be sent out via L2TP VPN tunnel when this function is enabled.
Remote Subnet	Enter the remote subnet of L2TP VPN server.
Remote Subnet Mask	Enter the remote netmask of L2TP VPN server.
Tunnel Key	Enter the password of L2TP tunnel.
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 MPPE	Enable or disable MPPE(Microsoft Point to Point 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 L2TP 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: 68-1500.
Link Detection Interval	Set the link detection interval time to ensure tunnel connection. Range: 0-600.

Expert Options	User can enter some initialization strings in this field and separate the strings with semicolon.

6.3.4 PPTP

Point-to-Point Tunneling Protocol (PPTP) is a protocol that uses a TCP control channel and a Generic Routing Encapsulation tunnel to encapsulate PPP packets.



PPTP	
Item	**Description**
Enable	Enable or disable PPTP client.
Server IP Address	Enter remote PPTP server's IP address or domain name.
Username	Enter the username that PPTP server provides.
Password	Enter the password that PPTP server provides.
Authentication Type	Select authentication type used to secure data sessions.
Global Traffic Forwarding	All the data traffic will be sent out viaPPTP VPN tunnel when this function is enabled.
Remote Subnet	Enter the remote subnet of PPTP VPN server.
Remote Subnet Mask	Enter the remote netmask of PPTP VPN server.
Local IP Address	Set tunnel IP address of PPTP client. Client will obtain tunnel IP address automatically from the server when it's null.
Peer IP Address	Enter tunnel IP address of PPTP server.
Enable MPPE	Enable MPPE(Microsoft Point to Point 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 PPTP initialization strings. User can keep the default value. Range: 0-ffffffff.
MRU	Set the maximum receive unit. Range: 64-1440.
MTU	Set the maximum transmission unit. Range: 68-1440.
Link Detection Interval	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 initialization strings in this field and separate the strings with semicolon.

6.4 Industrial Interface

UR75 router is capable of connecting terminals through industrial interfaces so as to realize wireless communication between terminals and remote data centers.

There are two types of the router's industrial interface: serial ports (RS232 and RS485) and I/O (digital input and digital output).

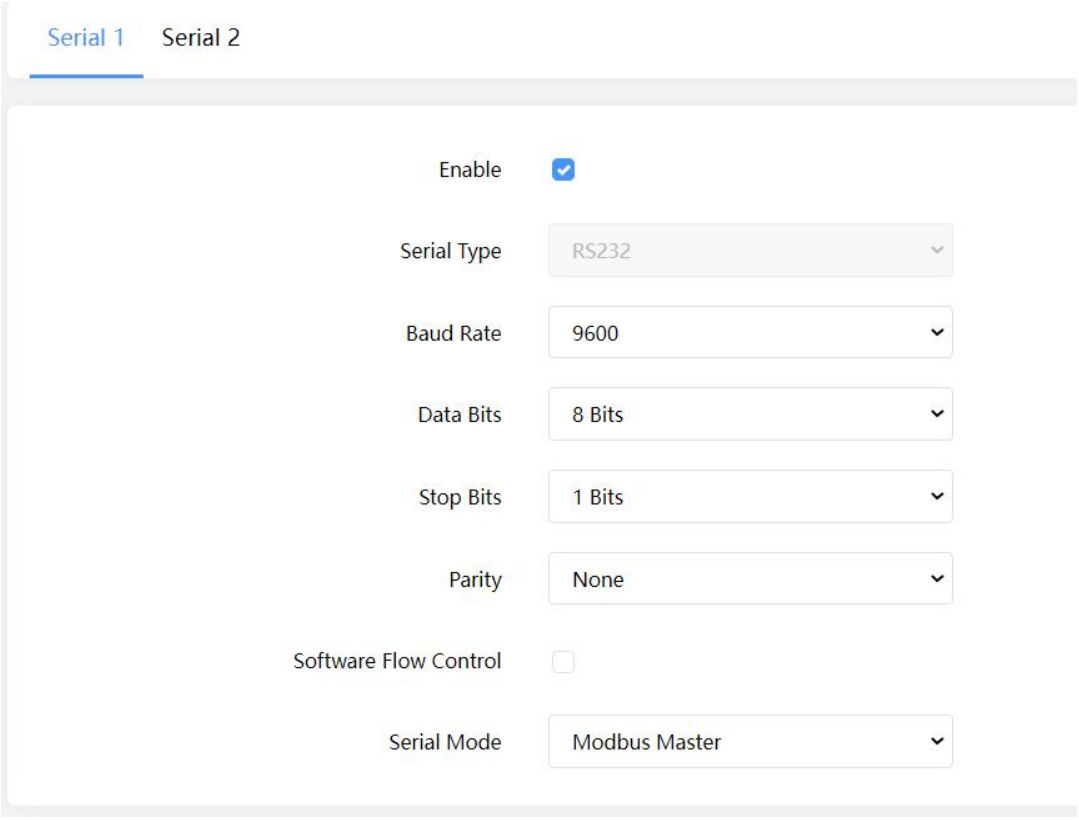
RS232 adopts full-duplex communication. It's generally used for communication within 20 m.

RS485 adopts half-duplex communication to achieve transmission of serial communication data with distance up to 120 m.

Digital input of I/O interface is a logical variable or switch variable with only two values of 0 and 1. 0 refers to a low level and 1 refers to a high level.

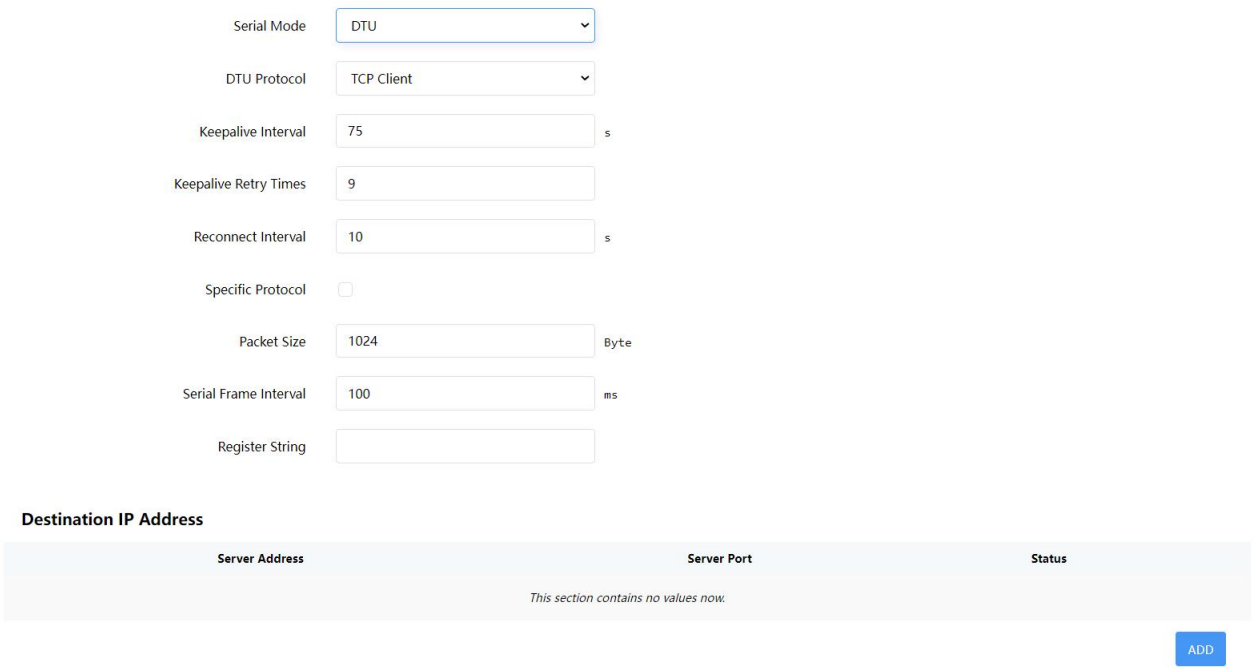
6.4.1 Serial Port

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 centers, so as to achieve two-way communication between serial terminals and remote data centers.



Serial Setting		
Item	**Description**	**Default**
Enable	Enable or disable serial port function.	Disable
Serial Type	Serial Port 1 is a RS232 port and Serial Port 2 is a RS485 port.	--
Baud Rate	The range is 300-230400. Same with the baud rate of the connected terminal device.	9600
Data Bits	8 bits or 7 bits optional. Same with the data bits of the connected terminal device.	8
Stop Bits	1 bit or 2 bits optional. Same with the stop bits of the connected terminal device.	1
Parity	Options are None, Odd and Even. Same with the parity of the connected terminal device.	None
Software Flow Control	Enable or disable software flow control.	Disable
Serial Mode	Select work mode of the serial port. **DTU Mode:** In DTU mode, the serial port can establish communication with the remote server/client. **GPS:** In GPS mode, go to **Industrial > GPS > GPS Serial Forwarding** to configure basic parameters to send GPS data to serial port.	Disable

	Modbus Master: In Modbus Master mode, go to **Industrial > Modbus Master** to configure basic parameters and channels.	



DTU Mode		
Item	**Description**	**Default**
DTU Protocol	Select from below protocols: **TCP Client:** the router is used as TCP client and transmits data to TCP server transparently. **UDP Client:** the router is used as UDP client and transmits data to UDP 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.	--
TCP/UDP Server		
Local port	Set the local port of this TCP/UDP server. 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 1-3600 s.	75
Max Retries	When TCP heartbeat times out, router will resend heartbeat. After it reaches the limitation of 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 reaches the limitation. The size range is 1-1024 byte.	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.	100

	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.	
TCP/UDP Client		
Keepalive Interval	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 run 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
Reconnect Interval	When connection failes, router will reconnect to the server at the preset interval. The range is 10-60 s.	10
Specific Protocol	With Specific Protocol, the router will be able to connect to the TCP2COM software.	Disable
Heartbeat Interval	With Specific Protocol, the router will send heartbeat packet to the server regularly to keep alive. The interval range is 1-3600s.	30
ID	Define unique ID of each router. No longer than 63 characters and do not contain space character.	--
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 byte.	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
Register String	When setting UDP client, 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
Max TCP Clients	Specify the maximum number of TCP clients allowed to connect the r outer which act as a TCP server.	32
Connection Timeout	If the TCP server does not receive any data from the slave device with in the connection timeout period, the TCP connection will be broken.	60
Read Interval	Set the interval for reading remote channels. When a read cycle ends, 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 rea d.	100
Response Timeout	Set the maximum response time that the router waits for the respons e to the command. If the device does not get a response after the ma ximum response time, it's determined that the command has run out of time.	3000

Max Retries	Set the maximum retry times after it fails to read.	3

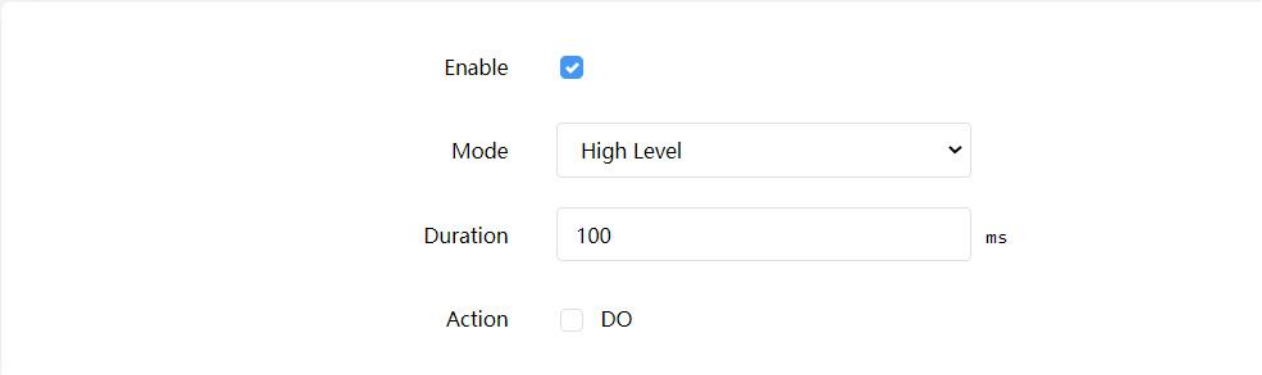
Related Configuration Example

DTU Application Example

6.4.2 I/O

6.4.2.1 DI

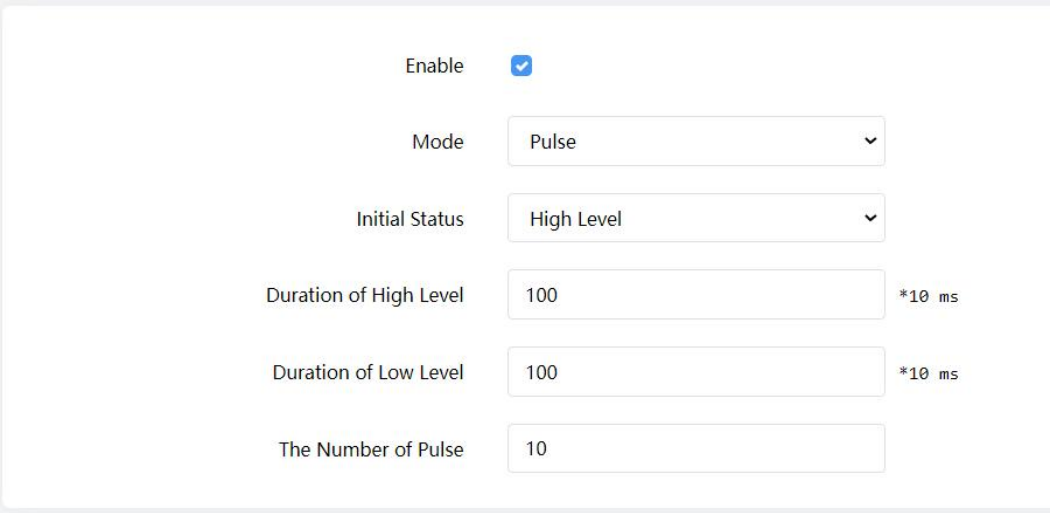
This section explains how to configure monitoring condition on digital input, and take certain actions once the condition is reached.



DI	
Item	**Description**
Enable	Enable or disable DI.
Mode	Select the working mode of DI. **High Level:** when it detects high level, trigger the action. **Low Level:** when it detects low level, trigger the action. **Counter:** when it detects a pulse, the counter value will increase by 1.
Duration (ms)	When the mode is high/low level, set the continuous duration of high/low level. Range: 1-10000.
Trigger Condition	When mode is counter, select the counter trigger condition. **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.
Trigger 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. **DO:** Control output status of DO.

6.4.2.2 DO

This section describes how to configure digital output mode.



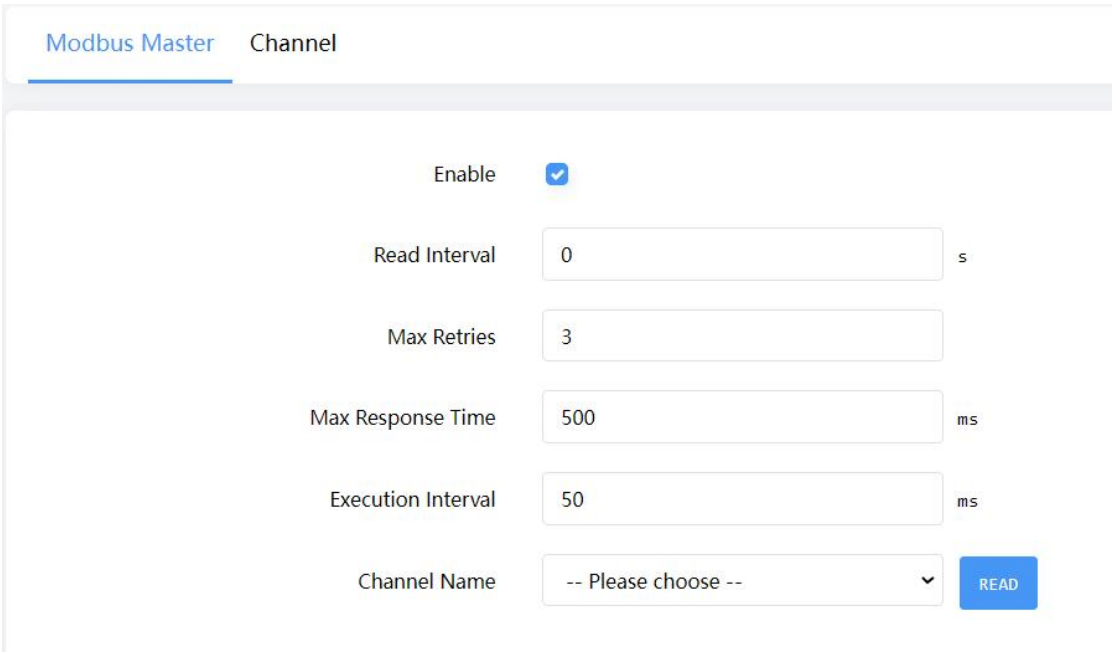
DO	
Item	**Description**
Enable	Enable or disable DO.
Mode	Select the working mode of DO. **High Level:** trigger the DO to send high level signal. **Low Level:** trigger the DO to send low level signal. **Counter:** trigger the DO to send pulses.
Initial Status	Select high level or low level as the initial status of the pulse.
Duration of High Level (*10ms)	Set the duration of pulse's high level. Range: 1-10000.
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.

6.4.3 Modbus Master

UR75 router can be set as Modbus RTU/TCP Master to poll the remote Modbus Slave and send data to TCP server.

6.4.3.1 Modbus Master

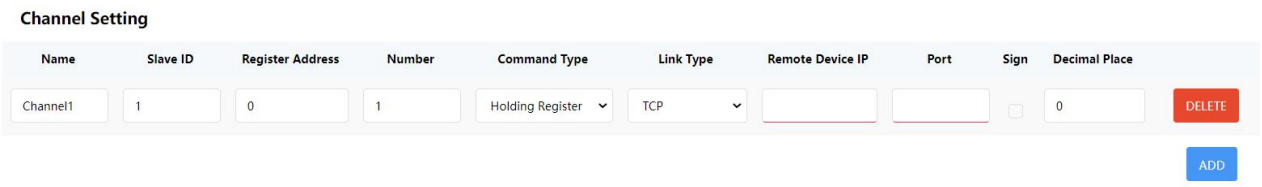
You can configure Modbus Master's parameters on this page.



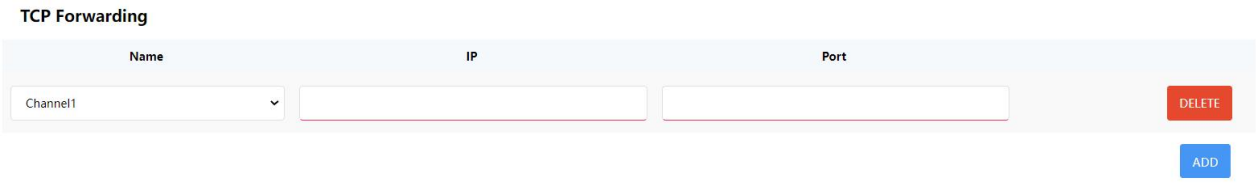
Modbus Master		
Item	**Description**	**Default**
Enable	Enable/disable Modbus master.	--
Read Interval	Set the interval for reading remote channels. When the read cycle ends, the commands which haven't been sent out will be discard, and the new read cycle begins. If it is set as 0, the device will restart the new read cycle after all channels have been read. Range: 0-600 s.	0
Max Retries	Set the maximum retry times when it fails to read, range: 0-5.	3
Max Response Time	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 run out of time. Range: 10-1000 ms.	500
Execution Interval	The execution interval between each command. Range: 10-1000 ms.	50
Channel Name	Select a readable channel form **Industrial > Channel > Channel Setting.**	--

6.4.3.2 Channel

You can add the channels and configure alarm setting on this page, so as to connect the router to the remote Modbus Slave to poll the address on this page and receive alarms from the router in different conditions.



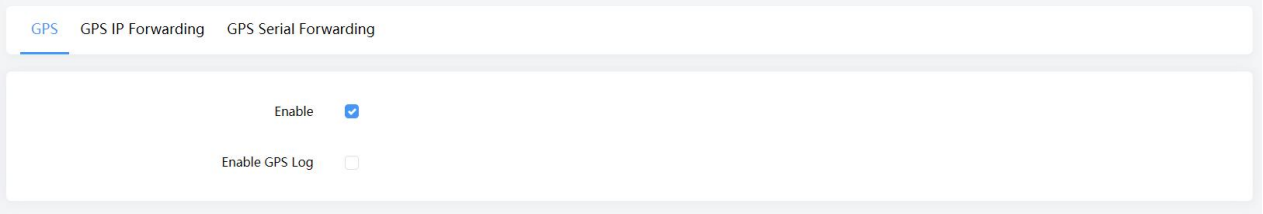
Channel Setting	
Item	**Description**
Name	Set the name to identify the remote channel. It cannot be blank.
Slave ID	Set Modbus slave ID.
Address	The starting address for Modbus reading.
Number	The reading quantity from starting address.
Command Type	Read command data type, options are Coil, Discrete, Holding Register (INT16), Input Register (INT16), Holding Register (INT32) and Holding Register (Float).
Link Type	Select serial port or TCP connection. **Serial Port:** the router communicate with devices via Modbus RTU protocol. **TCP:** the router communicate with devices via Modbus TCP protocol.
Remote Device IP	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.
Sign	When command data type is holding register or input register, enable or disable to identify whether this channel is signed.
Decimal Place	When command data 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.



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

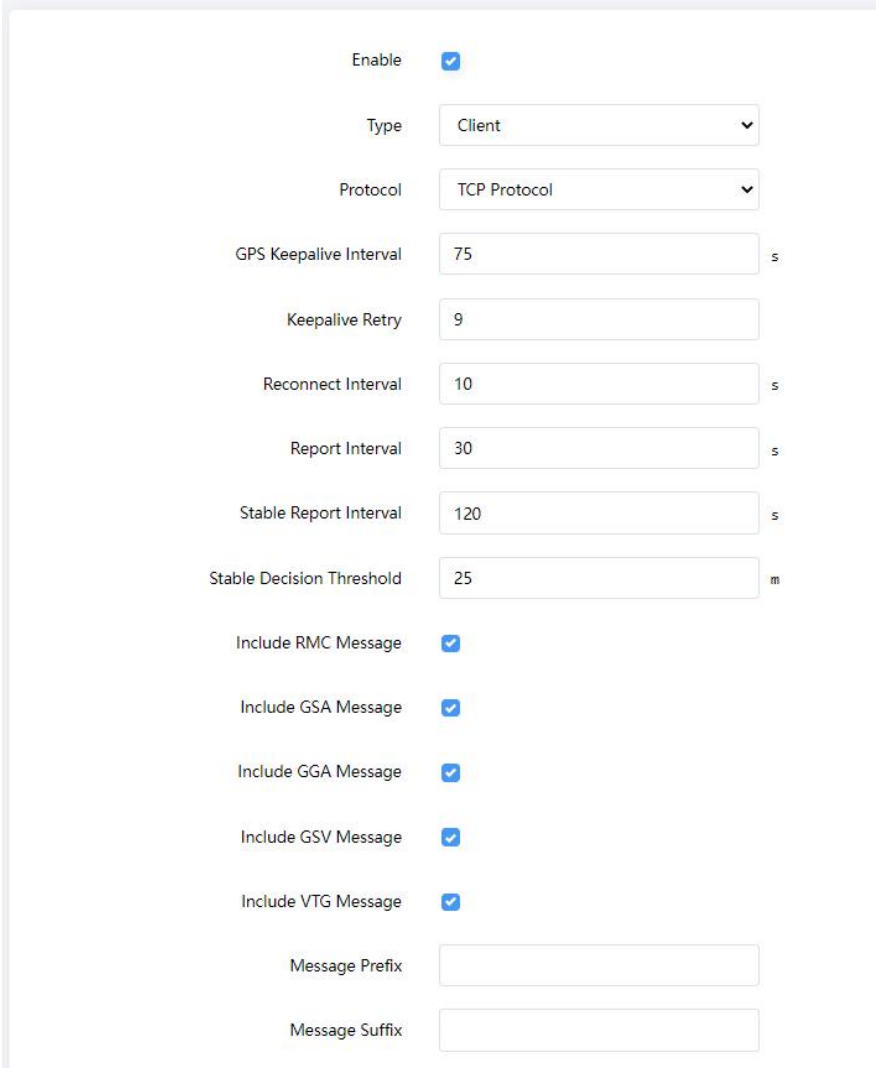
6.4.4 GPS

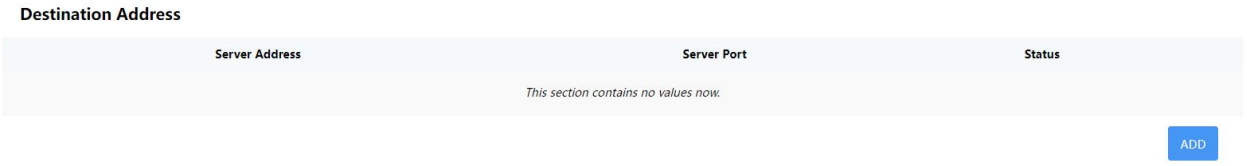
Users can enable GPS feature here. For more debug information, please also enable GPS log.



6.4.4.1 GPS IP Forwarding

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



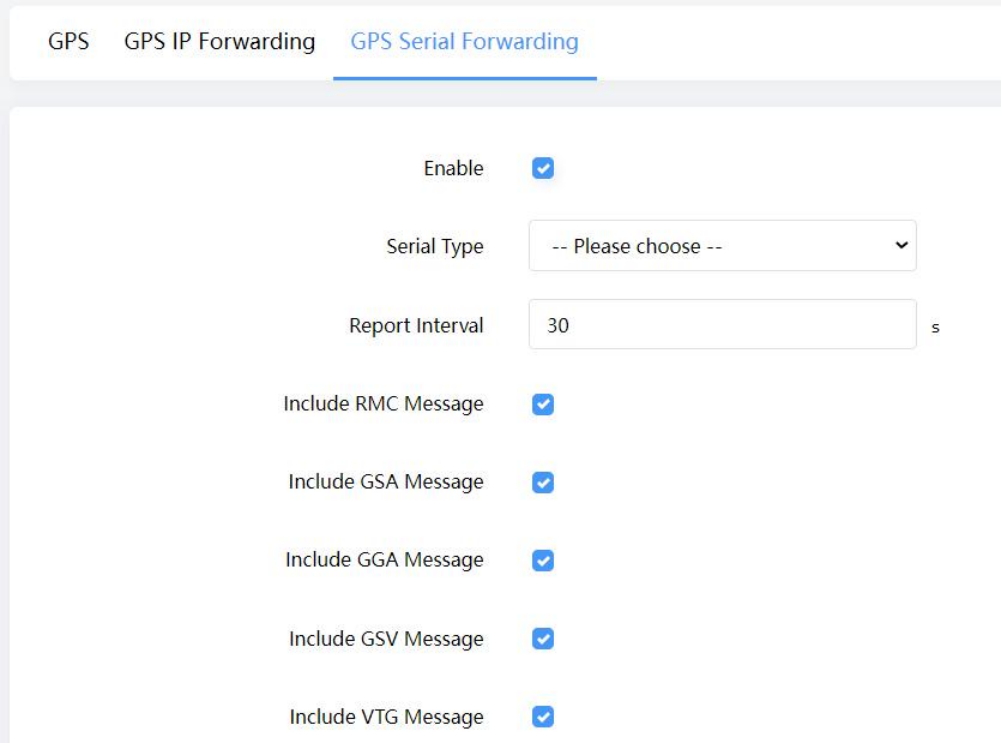


GPS IP Forwarding		
Item	**Description**	**Default**
Enable	Forward the GPS data to the client or server.	Disable
Type	Select connection type of the router as Client or Server.	Client
Protocol	Select protocol of data transmission as TCP or UDP.	TCP
GPS Keepalive Interval	When it's connected with server/client,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

	server. The range is 1-16.	
Local Port	Set the router listening port when using as a Server. Range: 1-65535.	
Reconnect Interval	When the connection failes, router will reconnect to the server at the preset interval. The range is 10-60 s.	10
Report Interval	The device will send GPS data to the server/client according to this interval if it reaches the stable decision threshold. The range is 1-65535 s.	30
Stable Report Interval	The device will send GPS data to the server/client according to this interval if it does not reach the stable decision threshold. The range is 1-65535 s.	120
Stable Decision Threshold	The GPS location deviation within this distance can be regarded as no change. The range is 1-65535 m.	25
Include RMC Message	RMC includes time, date, position, course and speed data.	Enable
Include GSA Message	GSA includes GPS receiver operating mode, satellites used in the position solution, and DOP values.	Enable
Include GGA Message	GGA includes time, position and fix type data.	Enable
Include GSV Message	GSV includes the number, elevation, azimuth of GPS satellites and SNR values.	Enable
Include VTG Message	VTG includes course and speed information relative to the ground.	Enable
Message Prefix	Add a prefix to the GPS data.	Null
Message Suffix	Add a suffix to the GPS data.	Null
Destination Address		
Server Address	Fill in the server address to receive GPS data (IP/domain name).	--
Server Port	Fill in the server port to receive GPS data. Range: 1-65535.	--
Status	Show the connection status between the router and the server.	--

6.4.4.2 GPS Serial Forwarding

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

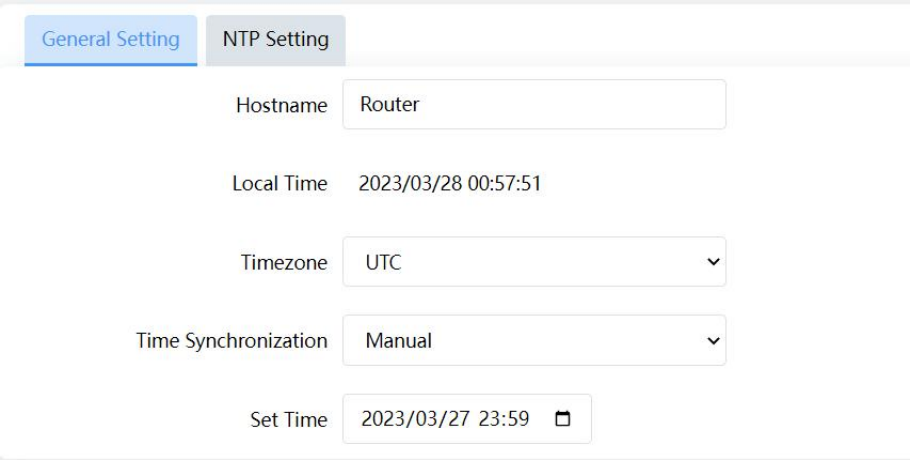


GPS Serial Forwarding		
Item	**Description**	**Default**
Enable	Forward the GPS data to the preset serial port.	Disable
Serial Type	Select the serial port to receive GPS data. Ensure that the serial port is enabled on **Industrial > Serial Port**.	--
Report Interval	The device will forward the GPS data to the serial port according to this interval. The range is 1-65535s.	30
Include RMC Message	RMC includes time, date, position, course and speed data.	Enable
Include GSA Message	GSA includes GPS receiver operating mode, satellites used in the position solution, and DOP values.	Enable
Include GGA Message	GGA includes time, position and fix type data.	Enable
Include GSV Message	GSV includes the number, elevation, azimuth of GPS satellites and SNR values.	Enable
Include VTG Message	VTG includes course and speed information relative to the ground.	Enable

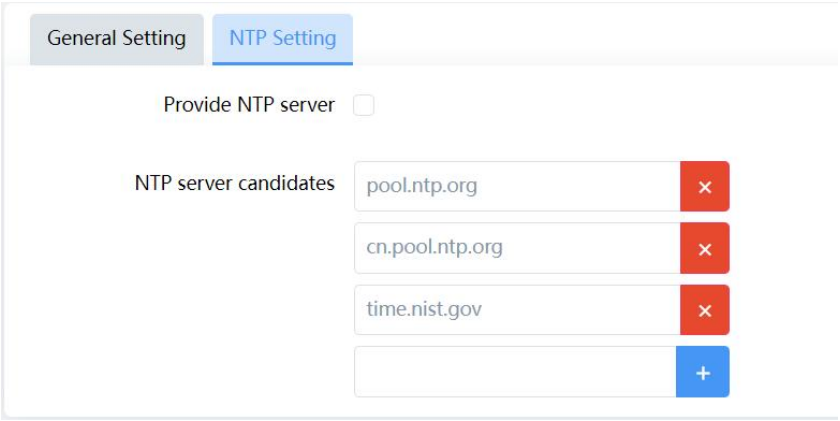
6.5 System

This section describes how to configure general settings and debugs, such as administration account, system time, common user management, device management, download logs, etc.

6.5.1 System



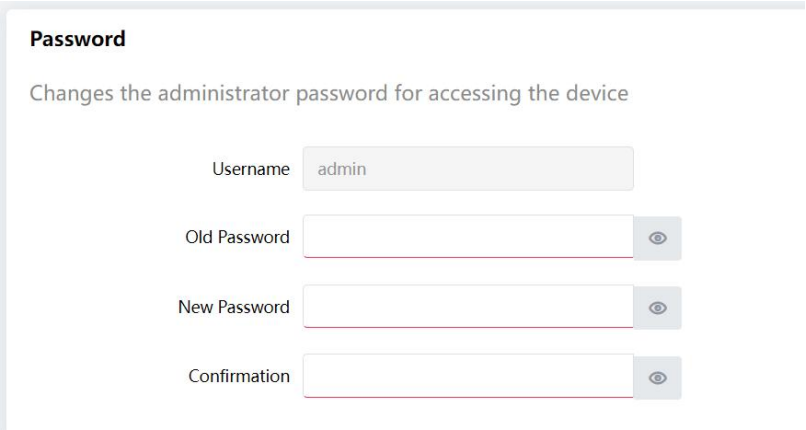
System - General Setting	
Item	**Description**
Hostname	Define the device name, needs to start with a letter.
Local Time	Show the current system time.
Timezone	Click the drop-down list to select the time zone you are in.
Time Synchronization	Select the time synchronization mode. **Sync Browser Time:** Synchronize time with browser. **Sync with NTP Server:** Synchronize time with NTP Server. **GPS Time Synchronization:** Synchronize time with GPS per hour. Ensure that GPS is enabled on **Industrial > GPS >GPS**. **Manual:** configure the time manually.



System - NTP Setting	
Item	**Description**
Provide NTP server	Enable to provide NTP server for connected devices.
NTP server candidates	Enter NTP Server's IP address or domain name to synchronize time. It can add 5 servers at most.

6.5.2 Password

You can change the administrator password for accessing the device.

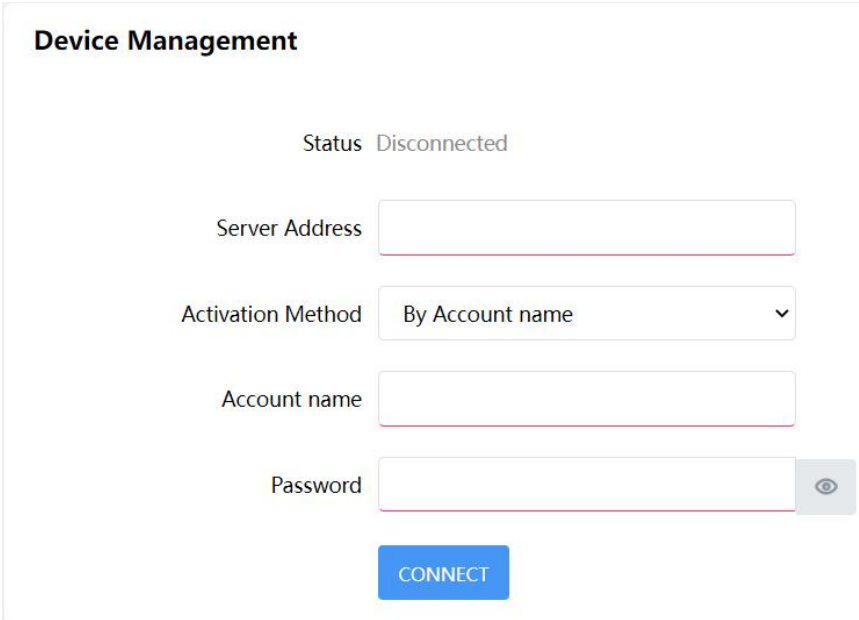


Password	
Item	**Description**
Username	It's fixed as admin.
Old Password	Enter the old password to verify the authority.
New Password	Enter a new password.
Confirmation	Enter the new password again.

6.5.3 Device Management

6.5.3.1 Device Management

You can connect the device to the Milesight DeviceHub management platform on this page so as to manage the device centrally and remotely. For more details, please refer to ***DeviceHub User Guide***.

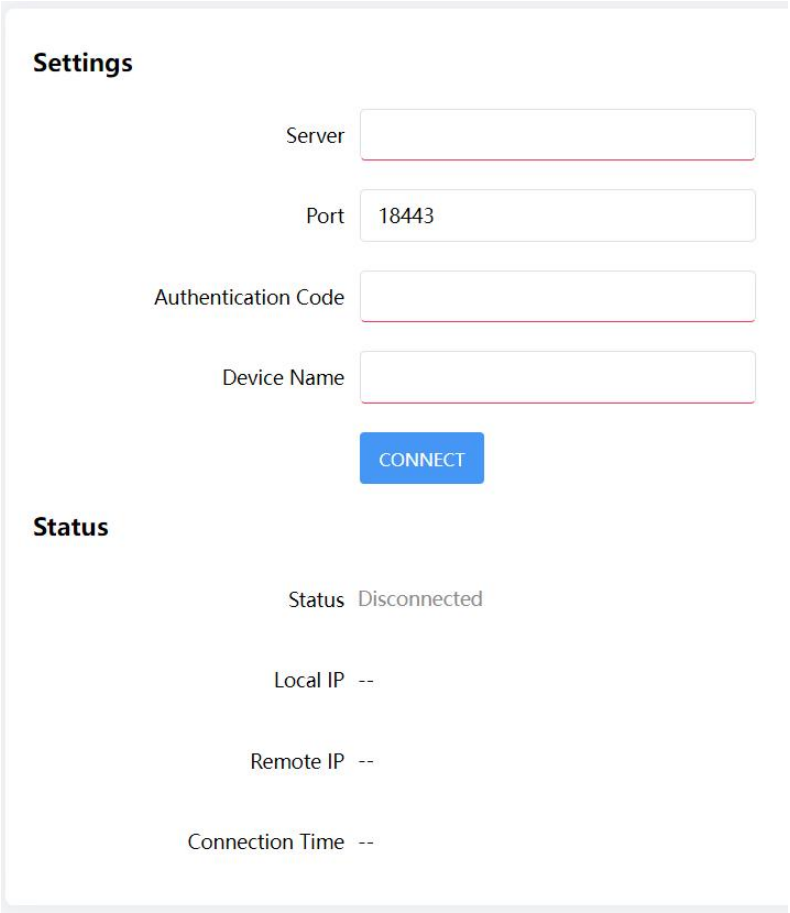


Device Management	
Item	**Description**

Status	Show the connection status between the device and the DeviceHub.
Server Address	IP address or domain of the DeviceHub management server.
Activation Method	Select activation method to connect the device 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	
Connect/Disconnect	Click this button to connect/disconnect the device from the DeviceHub.

6.5.3.2 Cloud VPN

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



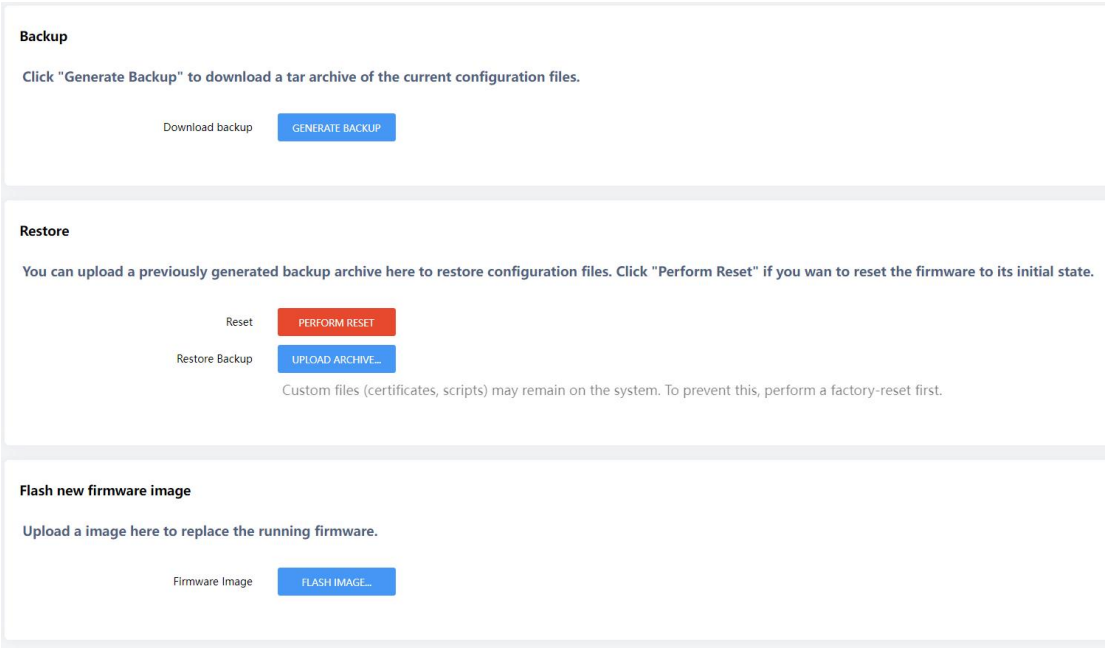
Cloud VPN	
Item	**Description**
Settings	
Server	Enter the IP address or domain name of MilesightVPN.
Port	Enter the HTTPS port number.
Authorization code	Enter the authorization code which generated by MilesightVPN.

Device Name	Enter the name of the device.
Status	
Status	Show the connection information about whether the router is connected to the MilesightVPN.
Local IP	Show the virtual IP of the router.
Remote IP	Show the virtual IP of the Milesight VPN server.
Connection Time	Show the information on how long has the router been connected to the Milesight VPN.

6.5.4 Backup / Upgrade

This section describes how to create a complete backup of the system configurations to a file, reset to factory defaults, restore the config file to the device and upgrade the flash image via the 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 worse the device will break down.



Backup/Upgrade	
Item	**Description**
Generate Backup	Click to download a tar archive of the current configuration file.
Perform Reset	Click to reset the device to factory default.
Upload Archive...	To restore configuration files, you can upload a previously generated backup archive here. Custom files (certificates, scripts) may remain on the system. To prevent this, you can perform a factory-reset first.
Flash Image...	Upload an image here to replace the running firmware.

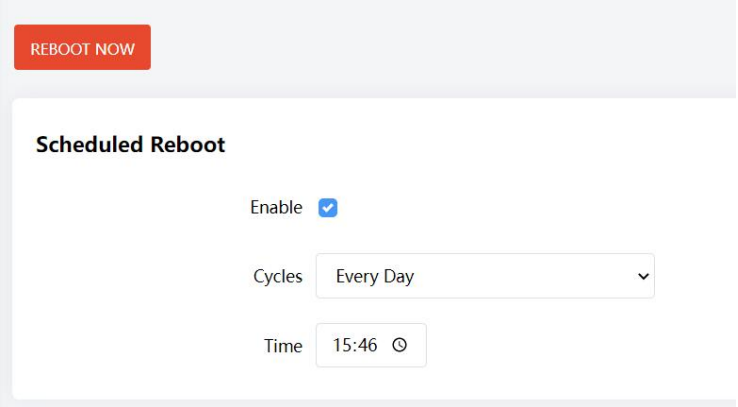
Related Configuration Example

Firmware Upgrade

Restore Factory Defaults

6.5.5 Reboot

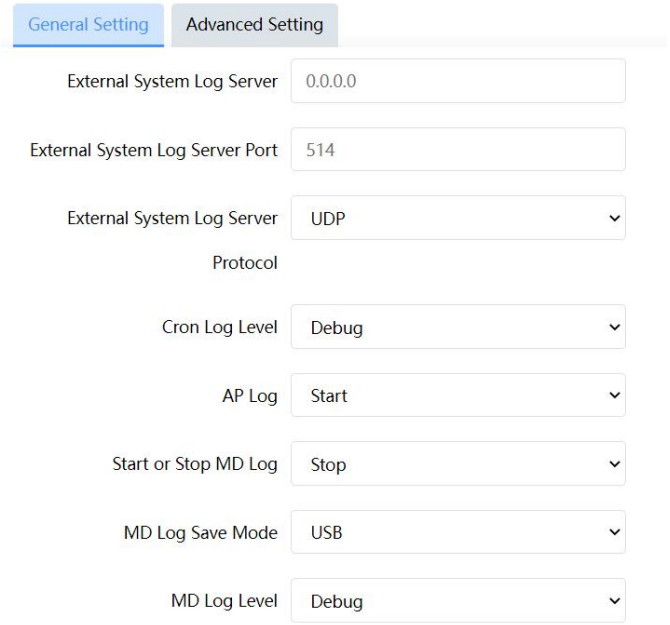
This page allows to reboot the device immediately or regularly.



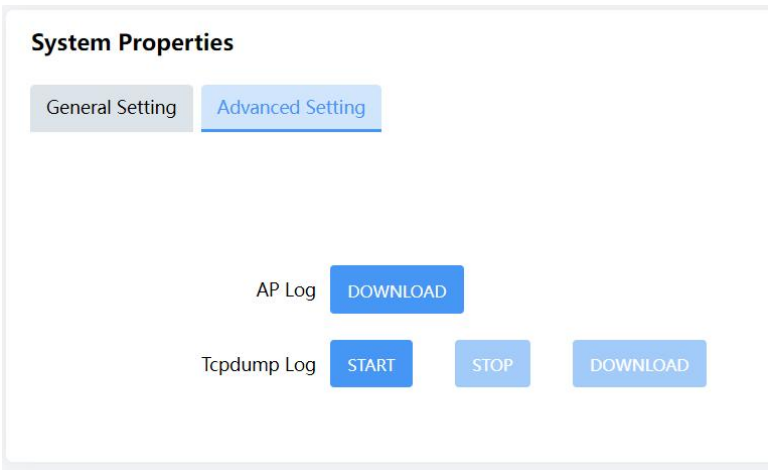
Reboot	
Item	**Description**
Reboot Now	Reboot the device immediately.
Schedule	
Enable	Click to enable reboot schedule.
Cycles	Reboot the device at a scheduled frequency.
Time	Select the time to execute the schedule.

6.5.6 Log

Users can download logs contains a record of informational, error and warning events that indicates how the system processes. By reviewing the data 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 the device will upload all system logs to remote log server such as Syslog Watcher.



Log Control - General Settings	
Item	**Description**
External system log server	Fill in the remote log server address (IP/domain name) which the router sends.
External system log server port	Fill in the remote log server port which the router sends.
External system log server protocol	Choose UDP or TCP from the drop-down list to transmit log file in corresponding protocol.
Cron Log Level	The severities to print the AP log: Normal, Warning, Debug.
AP Log	Select to start or stop recording system log.
Start or Stop MD Log	Select to start or stop recording cellular module log.
MD Log Save Mode	Select the save and output mode of MD log.
MD Log Level	The severities to print the MD log: Info, Notice, Warning, Error, Critical, Alert, Emergency, Debug.

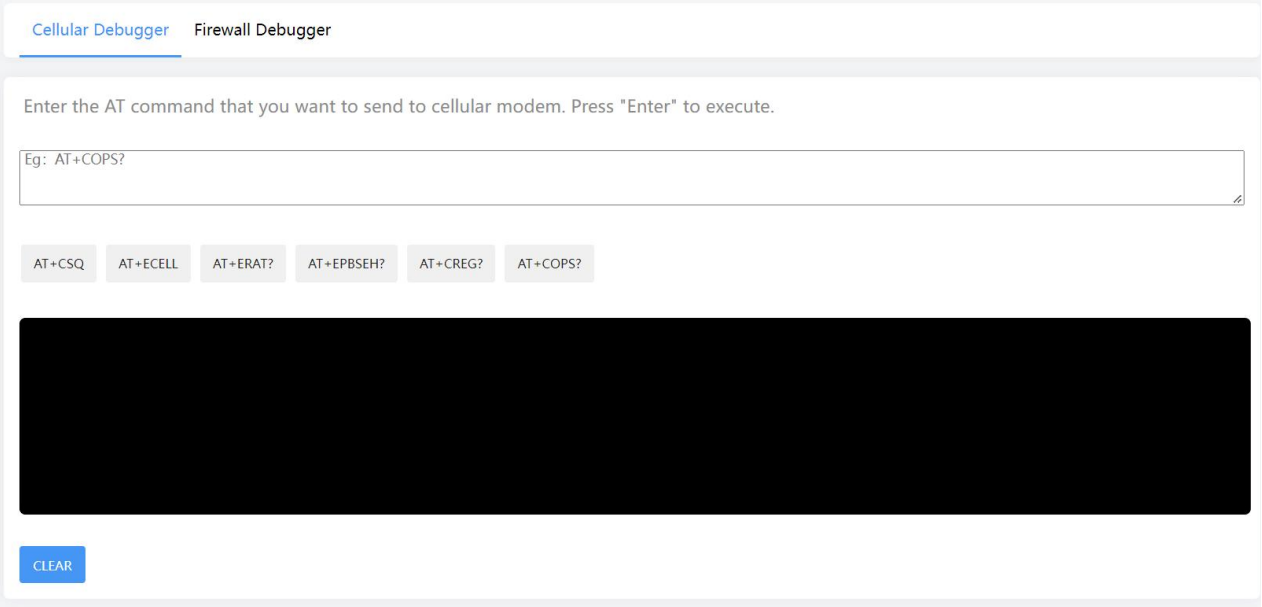


Log Control - Advanced Settings	
Item	**Description**
AP log	
Download	Click to download the last AP log recorded.
Tcpdump log	
Start	Click to start recording tcpdump log.
Stop	Click to stop recording tcpdump log.
Download	Click to download the last tcpdump log recorded.

6.5.7 Debugger

6.5.7.1 Cellular Debugger

This tool allows to use AT commands to check cellular debug information. You can press the buttons on the top of black frame directly to execute common commands directly or enter the AT command that you want to send to cellular modem and press **Enter** to execute.



Common command description:

AT+CSQ?----Get cellular network signal

AT+ECELL?----Get current cell information

AT+ERAT?----Get RAT status and network type

AT+EPBSEH? ----Get using bands

AT+CREG?----Get network registration status

AT+COPS?----Get operator and access technology info

6.5.7.2 Firewall Debugger

This tool allows to use iptables commands to check firewall information and download results.


Cellular Debugger
Firewall Debugger
Command
Eg: -t nat -nvL INPUT
CLEAR
DOWNLOAD

[END]