Mini Industrial Router

UR41

User Guide

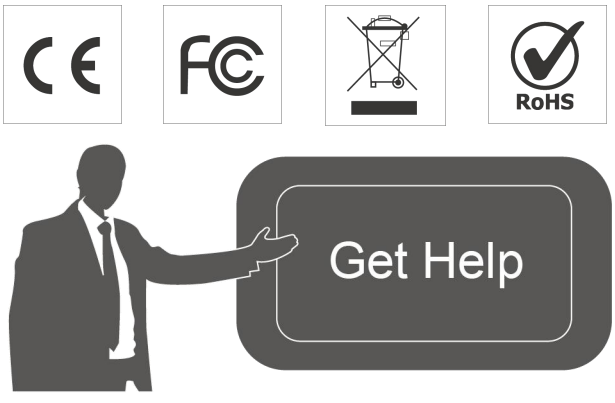
Safety Precautions Preface

Milesight will not shoulder responsibility for any loss or damage resulting form 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.
- Do not power on the device or connect it to other electrical device when installing.
- Do not connect or power the device using cables that have been damaged.

Declaration of Conformity

UR41 is in conformity with the essential requirements and other relevant provisions of the CE, FCC, and RoHS.



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

Revision History

Date	Doc Version	Description
Feb. 8, 2023	V 1.0	Initial version
Sept. 5, 2023	V 1.1	1. Add MQTT and TR069 feature; 2. Support customized cellular MTU and IMS; 3. Support to import openVPN file configurations, add tls-crypt mode and authentication mode; 4. Update Modbus Master/Slave to Modbus Client/Server; 5. Support to configure L2TP hostname.

Contents

Chapter 1 Product Introduction 8
1.1 Overview 8
1.2 Advantages 8
Chapter 2 Hardware Introduction 9
2.1 Packing List 9
2.2 Hardware Overview 10
2.3 Serial & IO & Power 10
2.4 LED Indicators 11
2.5 Reset Button 11
2.6 Dimensions (mm) 12
Chapter 3 Hardware Installation 12
3.1 SIM Card Installation 12
3.2 Antenna Installation 12
3.3 Router Installation 12
Chapter 4 Access to Web GUI 13
Chapter 5 Web Configuration 15
5.1 Status 15
5.1.1 Overview 15
5.1.2 Cellular 16
5.1.3 Network 17
5.1.4 VPN 17
5.1.5 Routing 18
5.1.6 Host List 19
5.1.7 GPS 20
5.2 Network 20
5.2.1 Interface 20
5.2.1.1 Cellular 20
5.2.1.2 Port 24
5.2.1.3 USB 24
5.2.1.4 Bridge 24
5.2.1.5 Loopback 25
5.2.2 DHCP 26
5.2.2.1 DHCP Server/DHCPv6 Server 26
5.2.2.2 DHCP Relay 28
5.2.3 Firewall 28
5.2.3.1 Security 29
5.2.3.2 ACL 30
5.2.3.3 Port Mapping 31
5.2.3.4 DMZ 32
5.2.3.5 MAC Binding 32
5.2.3.6 Custom Rules 32

5.2.3.7 SPI 33
5.2.4 QoS 34
5.2.5 VPN 35
5.2.5.1 DMVPN 35
5.2.5.2 IPSec Server 37
5.2.5.3 IPSec 40
5.2.5.4 GRE 42
5.2.5.5 L2TP 43
5.2.5.6 PPTP 46
5.2.5.7 OpenVPN Client 48
5.2.5.8 OpenVPN Server 50
5.2.5.9 Certifications 53
5.2.6 IP Passthrough 54
5.2.7 Routing 55
5.2.7.1 Static Routing 55
5.2.7.2 RIP 55
5.2.7.3 OSPF 58
5.2.7.4 Routing Filtering 63
5.2.8 VRRP 64
5.2.9 DDNS 66
5.3 System 67
5.3.1 General Settings 67
5.3.1.1 General 67
5.3.1.2 System Time 68
5.3.1.3 Email 69
5.3.2 Phone&SMS 70
5.3.2.1 Phone 70
5.3.2.2 SMS 71
5.3.3 Power Management 73
5.3.4 User Management 76
5.3.4.1 Account 76
5.3.4.2 User Management 77
5.3.5 AAA 77
5.3.5.1 Radius 77
5.3.5.2 TACACS+ 78
5.3.5.3 LDAP 78
5.3.5.4 Authentication 79
5.3.6 Device Management 80
5.3.6.1 DeviceHub 80
5.3.6.2 Milesight VPN 81
5.3.7 Events 82
5.3.7.1 Events 82
5.3.7.2 Events Settings 82
5.4 Service 84

5.4.1 I/O 84
5.4.1.1 DI 84
5.4.1.2 DO 85
5.4.2 Serial Port 86
5.4.3 Modbus Server (Slave) 89
5.4.3.1 Modbus TCP 89
5.4.3.2 Modbus RTU 90
5.4.3.3 Modbus RTU Over TCP 90
5.4.4 Modbus Client (Master) 91
5.4.4.1 Modbus Client 91
5.4.4.2 Channel 92
5.4.5 GPS 94
5.4.5.1 GPS IP Forwarding 94
5.4.5.2 GPS Serial Forwarding 96
5.4.5.3 GPS MQTT Forward 96
5.4.6 MQTT 97
5.4.7 SNMP 101
5.4.7.1 SNMP 101
5.4.7.2 MIB View 102
5.4.7.3 VACM 102
5.4.7.4 Trap 103
5.4.7.5 MIB 104
5.4.8 TR069 104
5.5 Maintenance 105
5.5.1 Tools 105
5.5.1.1 Ping 105
5.5.1.2 Traceroute 105
5.5.1.3 Packet Analyzer 106
5.5.1.4 Qxdmlog 106
5.5.2 Debugger 106
5.5.2.1 Cellular Debugger 106
5.5.2.2 Firewall Debugger 107
5.5.3 Log 108
5.5.3.1 System Log 108
5.5.3.2 Log Download 109
5.5.3.3 Log Settings 110
5.5.4 Upgrade 110
5.5.5 Backup and Restore 111
5.5.6 Reboot 112
Chapter 6 Application Examples 112
6.1 Cellular Connection 112
6.2 OpenVPN Client Application Example 114
6.3 NAT Application Example 116
6.4 DTU Application Example 117

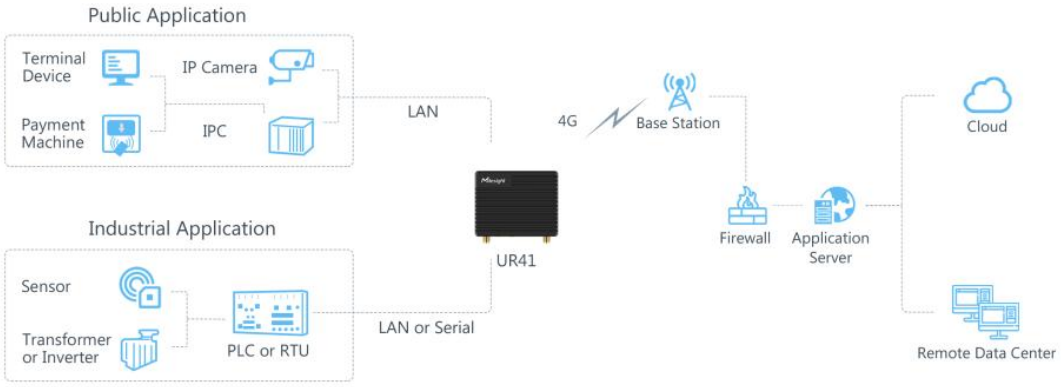
6.5 Restore Factory Defaults 120
6.6 Firmware Upgrade 122
6.7 SNMP Application Example 122
6.8 QoS Application Example 126

Chapter 1 Product Introduction

1.1 Overview

Milesight mini industrial router UR41 supports 4G connection, and also satisfies multi-type local data access requirements through rich industrial interfaces, including DI, DO, RS232 or RS485. UR41 make it easy for forming a reliable, secure, and maintainable solution through its built-in watchdog and secure VPN tunnels, realizing stable data transmission and high-speed mobile connectivity.

With a compact size and industry-grade design, UR41 is more flexible in a variety of installation and deployment scenarios. UR41 adopts a power-saving design with both idle mode and standby mode for providing users with an energy-saving option. UR41 could be managed and monitored remotely by Milesight DeviceHub, UR41 could be applied in wide scenarios including vending machines, robots, industrial equipment, and other IoT applications with optimal cost and performance.



1.2 Advantages

Highlight Features

- Compact size for suiting small embedded scenarios
- Global 4G LTE CAT4/3G network with multiple carrier networks
- Easy to connect with diverse wired devices through DI/DO/RS232/RS485 interfaces
- Power-saving design for both idle mode and standby mode for providing users with an energy-saving option

Industrial-Grade Design

- NXP industrial grade processor
- Rugged enclosure with IP30 protection
- Desk of wall mounting
- Wide operating temperature range from -40°C to 60°C/-40 °F to + 140°F

Easy Maintenance

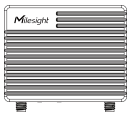
- DeviceHub provides easy setup, mass configuration, and centralized management of remote devices
- The user-friendly web interface design and more than one option of upgrade help administrators to manage the device as easy as pie
- WEB GUI and CLI enable the admin to achieve simple management and quick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

Security & Reliability

- Secure transmission with VPN tunnels like IPsec/OpenVPN/GRE/L2TP/PPTP/DMVPN
- Embeds hardware watchdog to automatically recover from various failures, ensuring highest level of availability
- Support access control lists, DMZ, DDoS Protection, Filters, SPI firewalls
- Establishes a secured mechanism on centralized authentication and authorization of device accessed by supporting AAA (Radius, TACACS+, LDAP, local Authentication) and multiple levels of user authority

Chapter 2 Hardware Introduction

2.1 Packing List

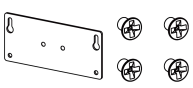


1 × UR41 Device

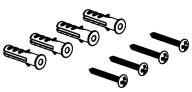
1 × Power Adapter

1 × 8-Pin Pluggable Terminal

1 × SIM Card Ejector Tool



1 × Wall Mounting Bracket with Screws

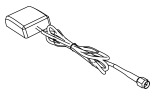


4 × Wall Mounting Kits

1 × Warranty Card

1 × Quick Start Guide

1 × Magnetic Cellular Antenna



1 × GPS Antenna

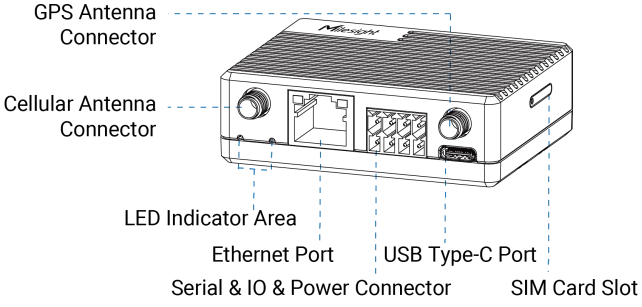
1 × 108mm Stubby Cellular Antenna (Optional)

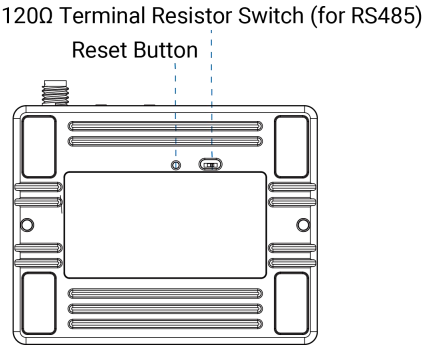
1 × Mini Stubby Cellular Antenna (Optional)

1 × USB 2.0 Cable (Optional)

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

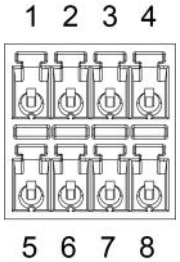
2.2 Hardware Overview





120Ω Terminal Resistor Switch: the device will add a 120Ω termination resistor to avoid data-corrupting reflections if RS485 data rate is too high or cable length is too long.

2.3 Serial & IO & Power



PIN	RS232/ RS485	DI	DO	Power	Description
1	---	---	OUT	---	Digital Output
2	---	IN	---	---	Digital Input
3	TX/A	---	---	---	Transmit Data
4	---	---	---	DC+	Positive
5	---	---	COM	---	Common Ground
6	GND	GND	---	---	Ground
7	RX/B	---	---	---	Receive Data
8	---	---	---	DC-	Negative

2.4 LED Indicators

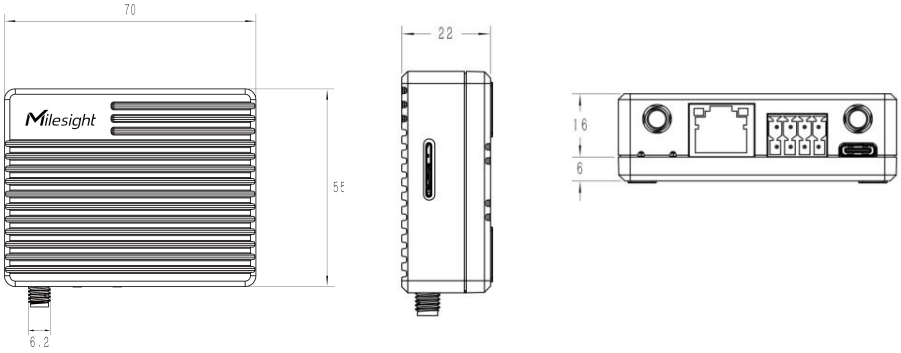
LED	Indication	Status	Description
SYSTEM	Power & System Status	Off	The power is switched off
		Orange	Static: the power is switched on, the system is on standby mode
			Blinking three times: the power is switched on, the system is starting up
		Green	Static: The system is running properly
		Red	Static: The system goes wrong
LTE	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 4G network
		Orange	Static: SIM card has been registered and dialed up to 3G/2G network
Ethernet Port	Link Indicator (Orange)	Off	Disconnected or fail to connect
		On	Connected
		Blinking	Transmitting data
	Rate Indicator (Green)	Off	10 Mbps mode
		On	100 Mbps mode

Note: It will take around 1 minute for UR41 to completely start up, then the SYSTEM light will be green.

2.5 Reset Button

Function	Description	
	SYSTEM LED	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 router is now reset to factory defaults.
Weakup	Orange Static → Green Static	If standby mode is enabled, press and hold on reset button for 3 seconds to weak up the router for 1 hour.

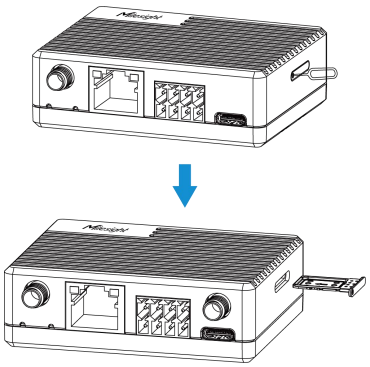
2.6 Dimensions (mm)



Chapter 3 Hardware Installation

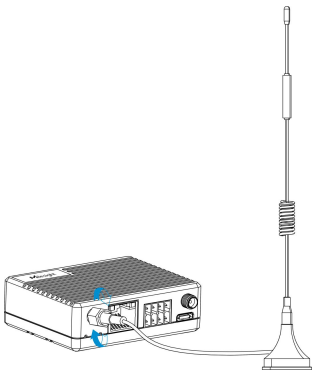
3.1 SIM Card Installation

Use an ejector tool to open the SIM card slot, insert the nano SIM card, then put the slot with SIM card back to the device.



3.2 Antenna Installation

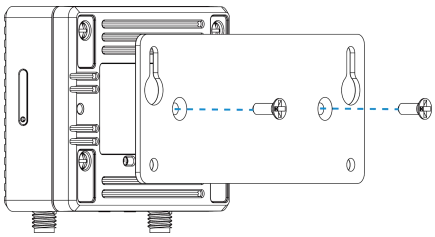
Rotate the antenna into the antenna connector accordingly. The external antenna should be installed vertically, and always on a site with a good signal.



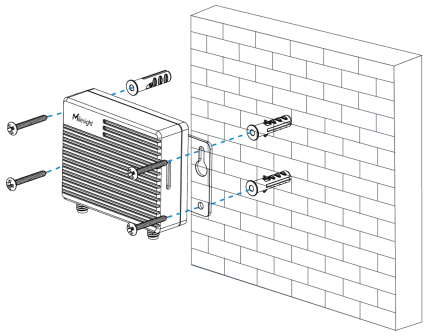
3.3 Router Installation

UR41 router can be mounted to a wall. Before you start, make sure that a SIM card has been inserted, antennas have been attached and all cables have been installed.

1. Fix the wall mounting bracket to the device with 2 screws.



2. Drill 4 holes on the wall according to wall mounting bracket, then fix the wall plugs to the wall.
3. Fix the device to the wall plugs with screws. When installing, it's suggested to fix the upper two screws first.

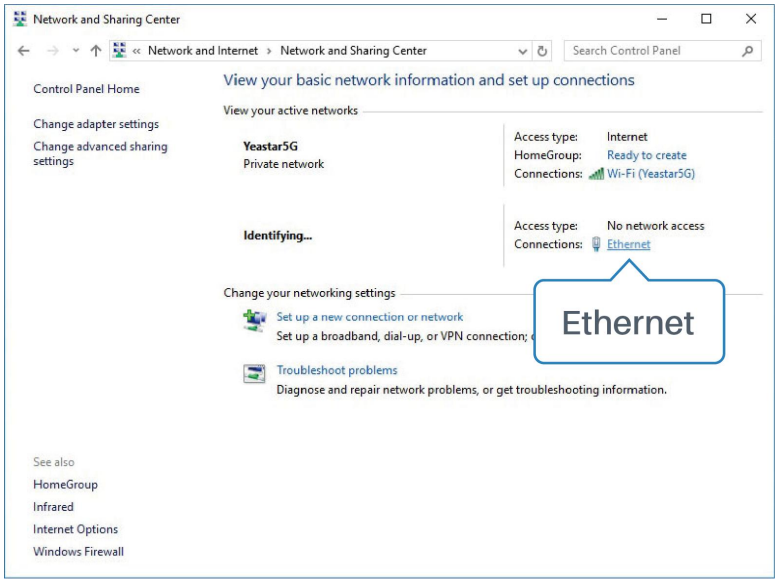


Chapter 4 Access to Web GUI

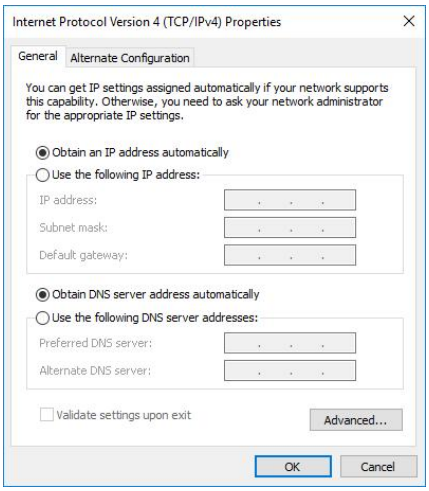
This chapter explains how to access to Web GUI of the UR41 router. Connect PC to LAN port of UR41 router directly. The following steps are based on Windows 10 operating system for your reference.

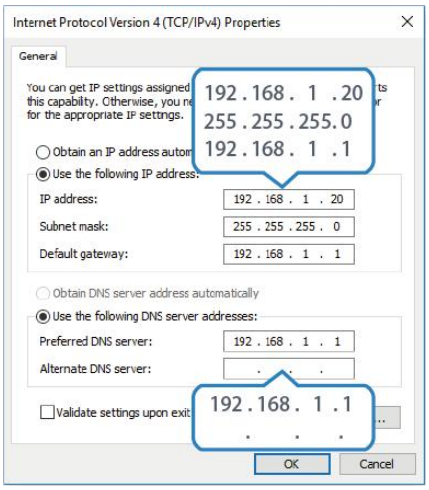
Username: **admin**
Password: **password**
IP Address: **192.168.1.1**

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



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



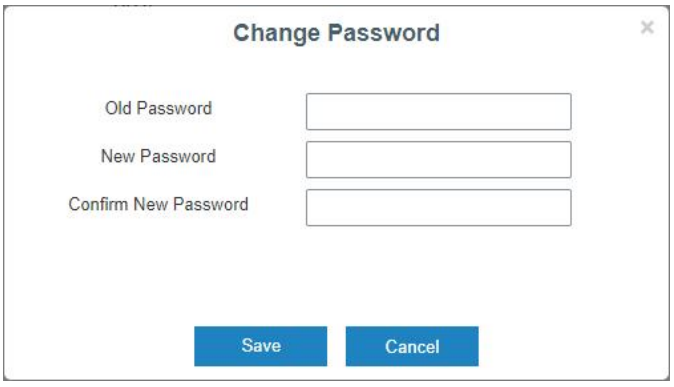


3. Open a Web browser on your PC (Chrome is recommended), type in the IP address 192.168.1.1, and press Enter on your keyboard.

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

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

5. When you login with the default username and password, you will be asked to modify the password. It’s suggested that you change the password for the sake of security. Click "Cancel" button if you want to modify it later.



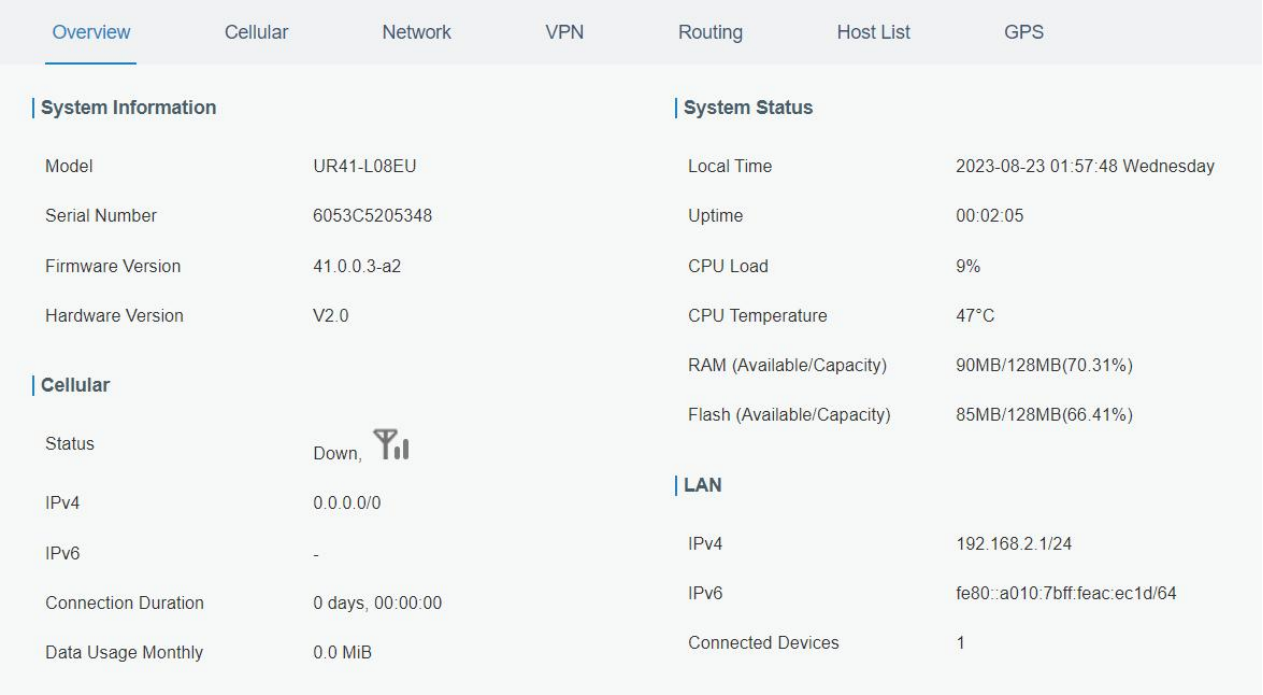
6. After you login the Web GUI, you can view system information and perform configuration on the router.

Chapter 5 Web Configuration

5.1 Status

5.1.1 Overview

You can view the system information of the router on this page. For UPS items please refer to ***Milesight UPS User Guide***.

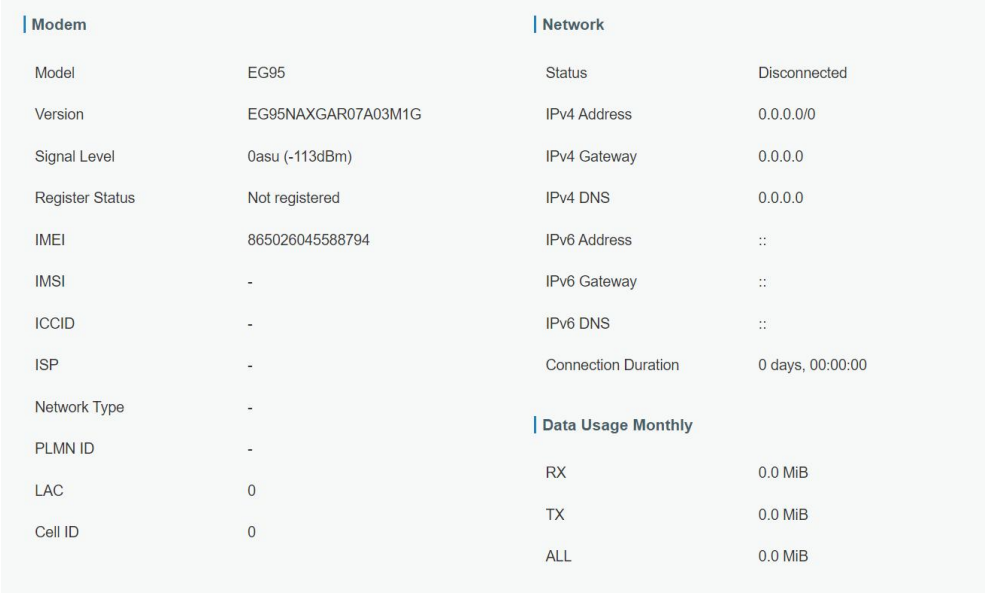


System Information	
Item	**Description**
Model	Show the model name of router.
Serial Number	Show the serial number of router.
Firmware Version	Show the currently firmware version of router.
Hardware Version	Show the currently hardware version of router.
System Status	
Item	**Description**
Local Time	Show the currently local time of system.
Uptime	Show the information on how long the router has been running.
CPU Load	Show the current CPU utilization of the router.
CPU Temperature	Show current CPU temperature.
RAM (Available/Capacity)	Show the RAM capacity and the available RAM memory.
Flash (Available/Capacity)	Show the Flash capacity and the available Flash memory.

Cellular	
Item	**Description**
Status	Show the real-time status of the currently SIM card
IPv4	Show the IPv4 address obtained from the mobile carrier.
IPv6	Show the IPv6 addresses obtained from the mobile carrier.
Connection Duration	Show the connection duration of the currently SIM card.
Data Usage Monthly	Show the monthly data usage statistics of currently used SIM card.
LAN	
Item	**Description**
IPv4	Show the IPv4 address of the LAN port.
IPv6	Show the IPv6 addresses of the LAN port.
Connected Devices	Number of devices that connected to the router's LAN.

5.1.2 Cellular

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



Modem Information	
Item	**Description**
Model	Show the model name of cellular module.
Version	Show the cellular module firmware version.
Signal Level	Show the cellular signal level.
Register Status	Show the registration status of SIM card.
IMEI	Show the IMEI of the module.
IMSI	Show IMSI of the SIM card.
ICCID	Show ICCID of the SIM card.
ISP	Show the network provider which the SIM card registers on.
Network Type	Show the connected network type, such as LTE, 3G, etc.

PLMN ID	Show the current PLMN ID, including MCC, MNC, LAC and Cell ID.
LAC	Show the location area code of the SIM card.
Cell ID	Show the Cell ID of the SIM card location.

Network	
Item	**Description**
Status	Show the connection status of cellular network.
IPv4/IPv6 Address	Show the IPv4/IPv6 address and netmask of cellular network.
IPv4/IPv6 Gateway	Show the IPv4/IPv6 gateway and netmask of cellular network.
IPv4/IPv6 DNS	Show the IPv4/IPv6 DNS of cellular network.
Connection Duration	Show information on how long the cellular network has been connected.

Data Usage Monthly	
Item	**Description**
RX	Show the data volume and packets received of this month.
TX	Show the data volume and packets transmitted of this month.
ALL	Show the total volume and packets of this month.

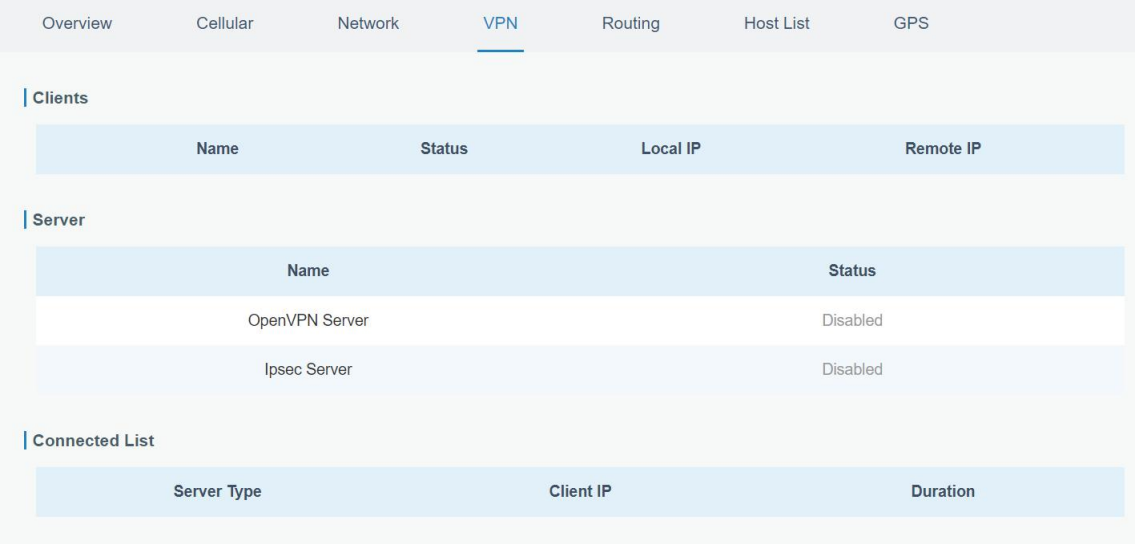
5.1.3 Network

On this page you can check the Bridge status of the router.

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

5.1.4 VPN

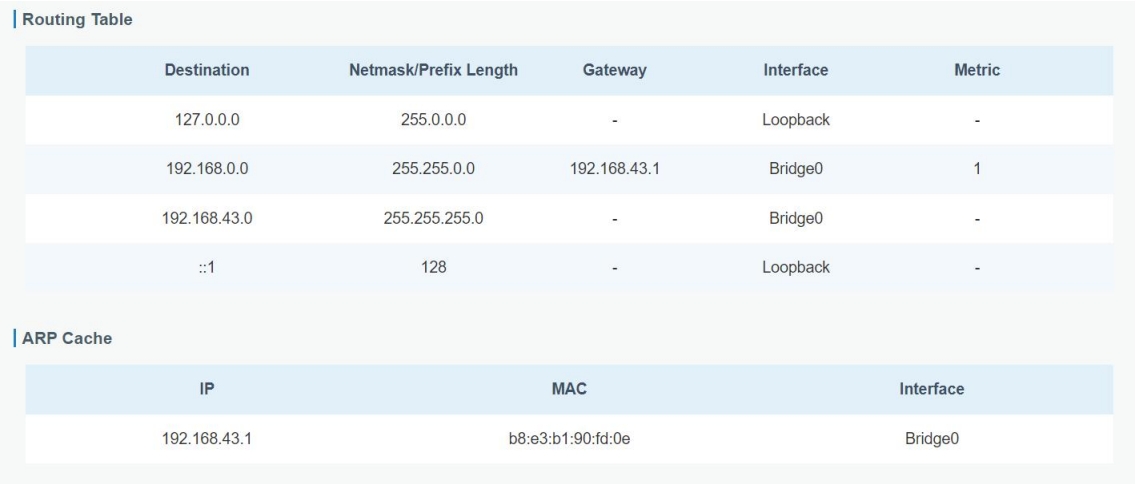
You can check VPN status on this page, including PPTP, L2TP, IPsec, OpenVPN and DMVPN.



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

5.1.5 Routing

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



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

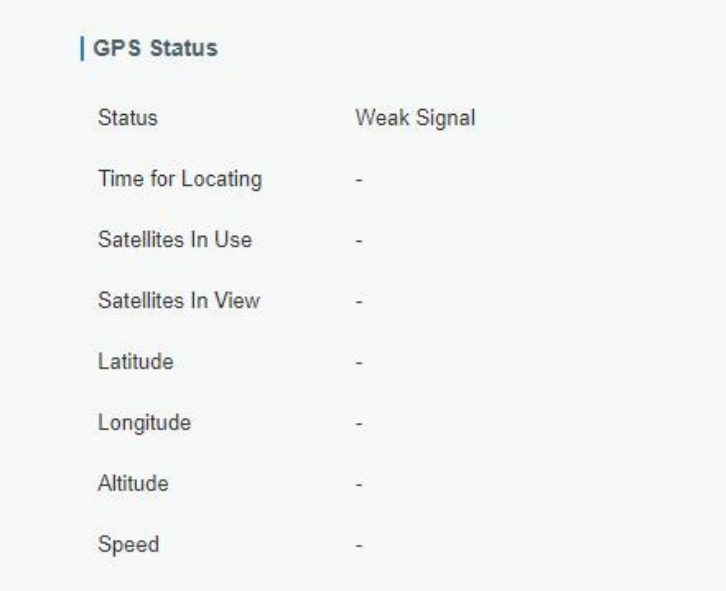
5.1.6 Host List

You can view the host information on this page.

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

5.1.7 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.



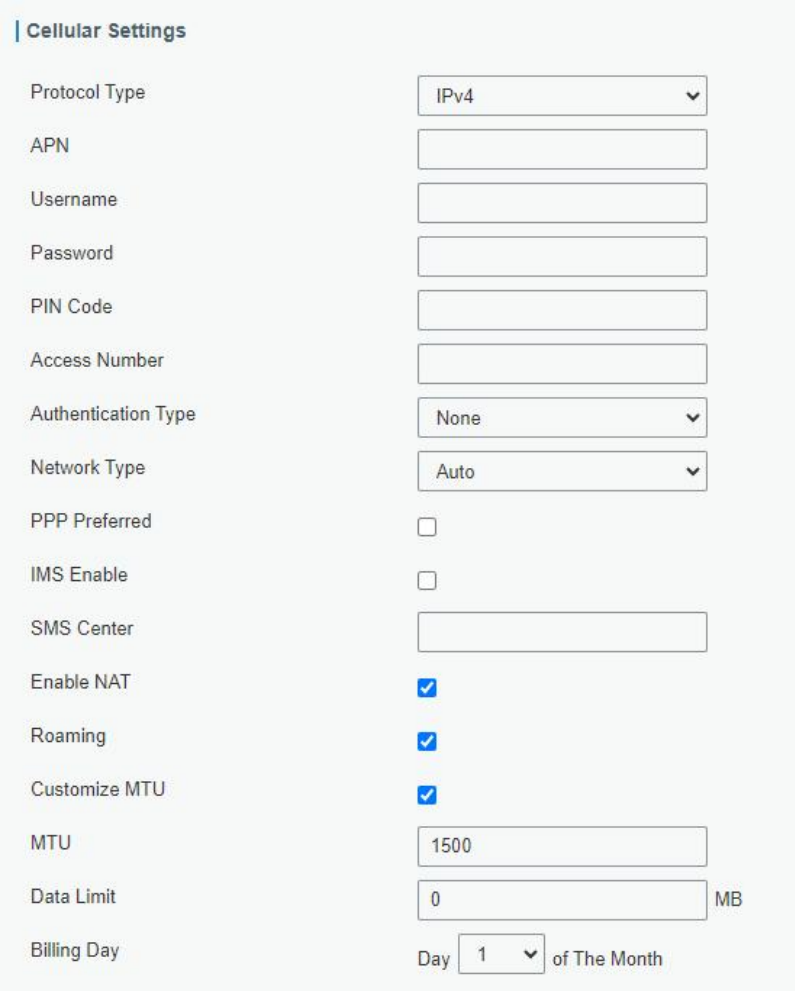
GPS Status	
Item	**Description**
Status	Show the status of GPS.
Time for Locating	Show the time for locating.
Satellites In Use	Show the quantity of satellites in use.
Satellites In View	Show the quantity of satellites in view.
Latitude	Show the Latitude of the location.
Longitude	Show the Longitude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

5.2 Network

5.2.1 Interface

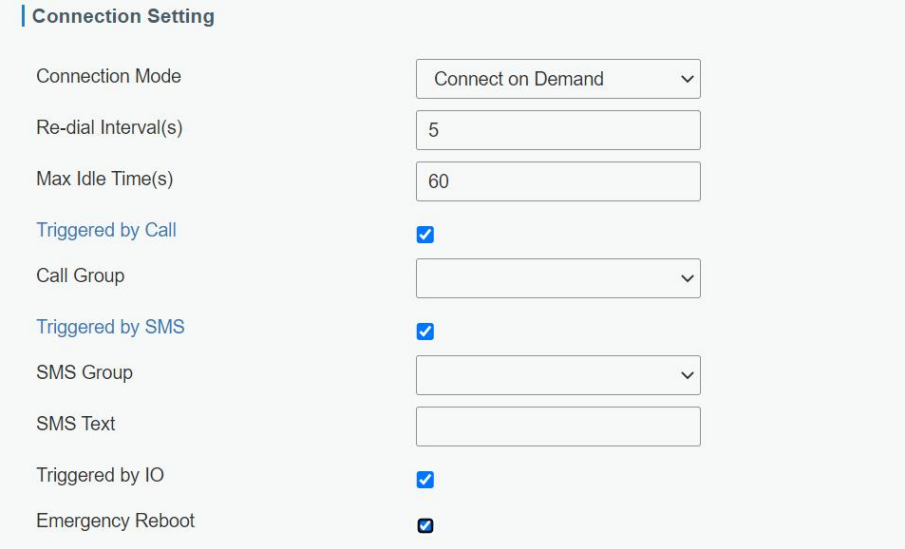
5.2.1.1 Cellular

This section explains how to set the related parameters for cellular network.



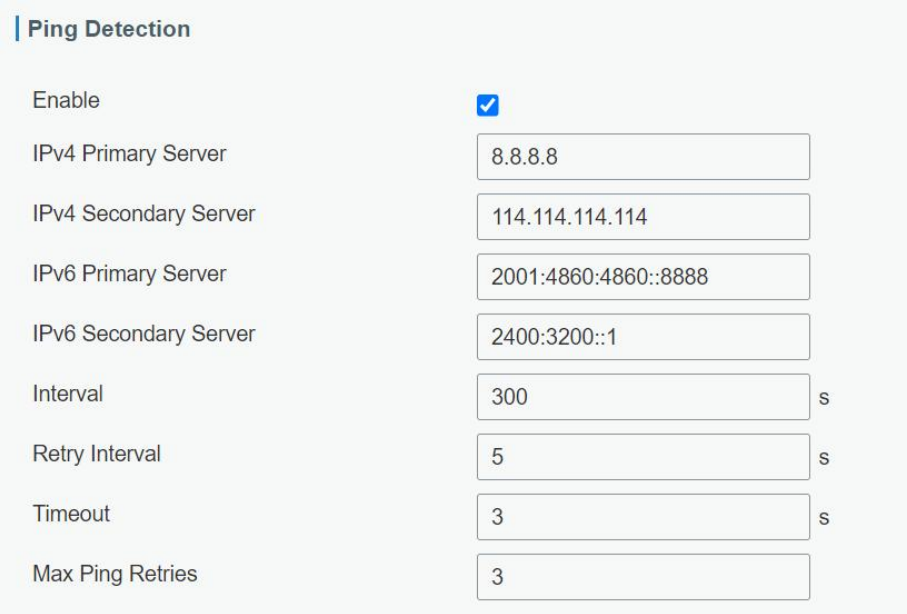
Cellular Settings	
Item	**Description**
Protocol Type	Select from "IPv4", "IPv6" and "IPv4/IPv6".
APN	Enter the Access Point Name for cellular dial-up connection provided by local ISP.
Username	Enter the username for cellular dial-up connection provided by local ISP.
Password	Enter the password for cellular dial-up connection provided by local ISP.
PIN Code	Enter a 4-8 characters PIN code to unlock the SIM.
Access Number	Enter the dial-up center NO. For cellular dial-up connection provided by local ISP.
Authentication Type	Select from "None", "PAP" and "CHAP".
Network Type	Select from "Auto", "4G Only", "3G Only", and "2G Only". Auto: connect to the network with the strongest signal automatically. 4G Only: connect to 4G network only. And so on.
PPP Preferred	The PPP dial-up method is preferred.
IMS Enable	Enable or disable IMS function.

SMS Center	Enter the local SMS center number for storing, forwarding, converting and delivering SMS message.
Enable NAT	Enable or disable NAT function.
Roaming	Enable or disable roaming.
Customize MTU	Enable or disable to customize the maximum transmission units. When disabled, the device will use operator's MTU settings.
MTU	Customize the maximum transmission units.
Data Limit	When you reach the specified data usage limit, the data connection of currently used SIM card will be disabled. 0 means disable the function.
Billing Day	Choose the billing day of the SIM card, the router will reset the data used to 0.



Connection Setting	
Item	**Description**
Connection Mode	Select from "Always Online" and "Connect on Demand".
Re-dial Interval(s)	Set the interval to dial into ISP when it lost connection, the default value is 5s.
Max Idle Times	Set the maximum duration of router when current link is under idle status. Range: 10-3600
Triggered by Call	The router will switch from offline mode to cellular network mode automatically when it receives a call from the specific phone number.
Call Group	Select a call group for call trigger. Go to "System > General > Phone" to set up phone group.
Triggered by SMS	The router will switch from offline mode to cellular network mode automatically when it receives a specific SMS from the specific mobile phone.
SMS Group	Select an SMS group for trigger. Go to "System > General > Phone" to set up SMS group.

SMS Text	Fill in the SMS content for triggering.
Triggered by IO	The router will switch from offline mode to cellular network mode automatically when the DI status is changed. Go to "Industrial > I/O > DI" to configure trigger condition.
Emergency Reboot	Enable or disable emergency reboot function.



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

Related Topics

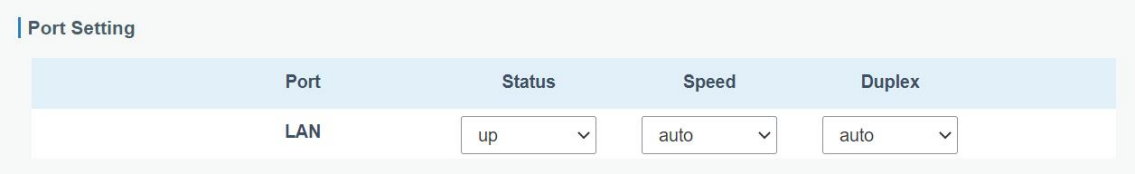
Cellular Network Connection

Phone Group

DI Setting

5.2.1.2 Port

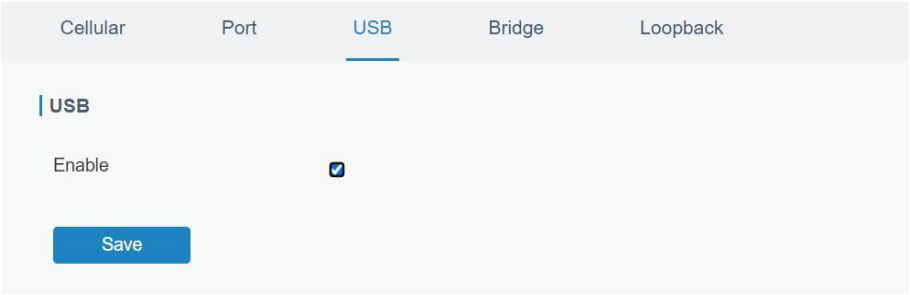
This section describes how to configure the Ethernet port parameters.
UR41 cellular router supports 1 Fast Ethernet port.



Port Setting	
Item	**Description**
Port	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.
Speed	Set the Ethernet port's speed. The options are "auto", "100 Mbps", and "10 Mbps".
Duplex	Set the Ethernet port's mode. The options are "auto", "full", and "half".

5.2.1.3 USB

UR41 equips with a USB 2.0 port for power supply or can work as a LAN port to provide network to terminal devices.



5.2.1.4 Bridge

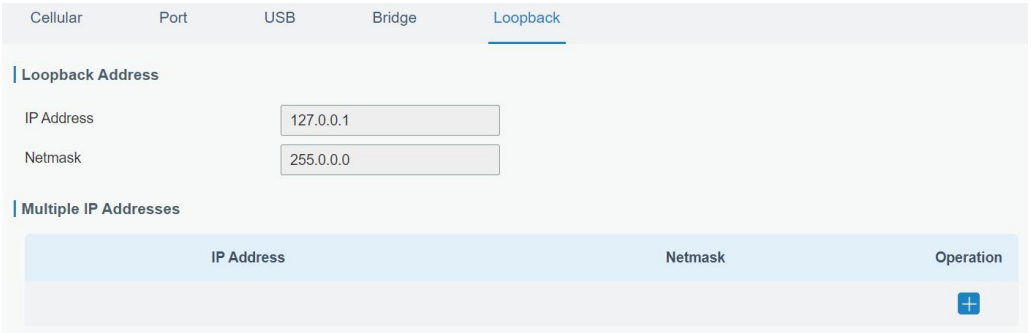
Bridge setting is used for managing local area network devices which are connected to LAN ports of the UR41, allowing each of them to access the Internet.

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

5.2.1.5 Loopback

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

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



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

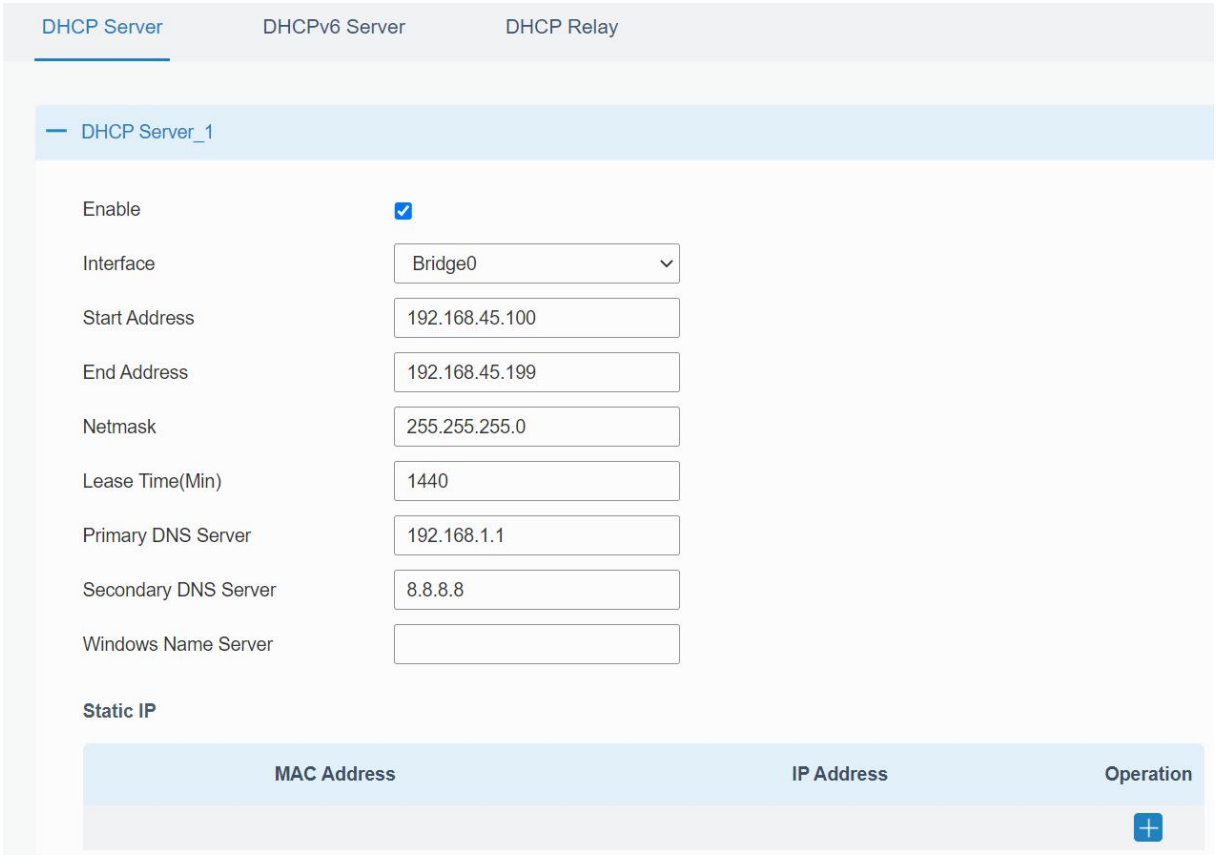
Addresses	other IP addresses.	

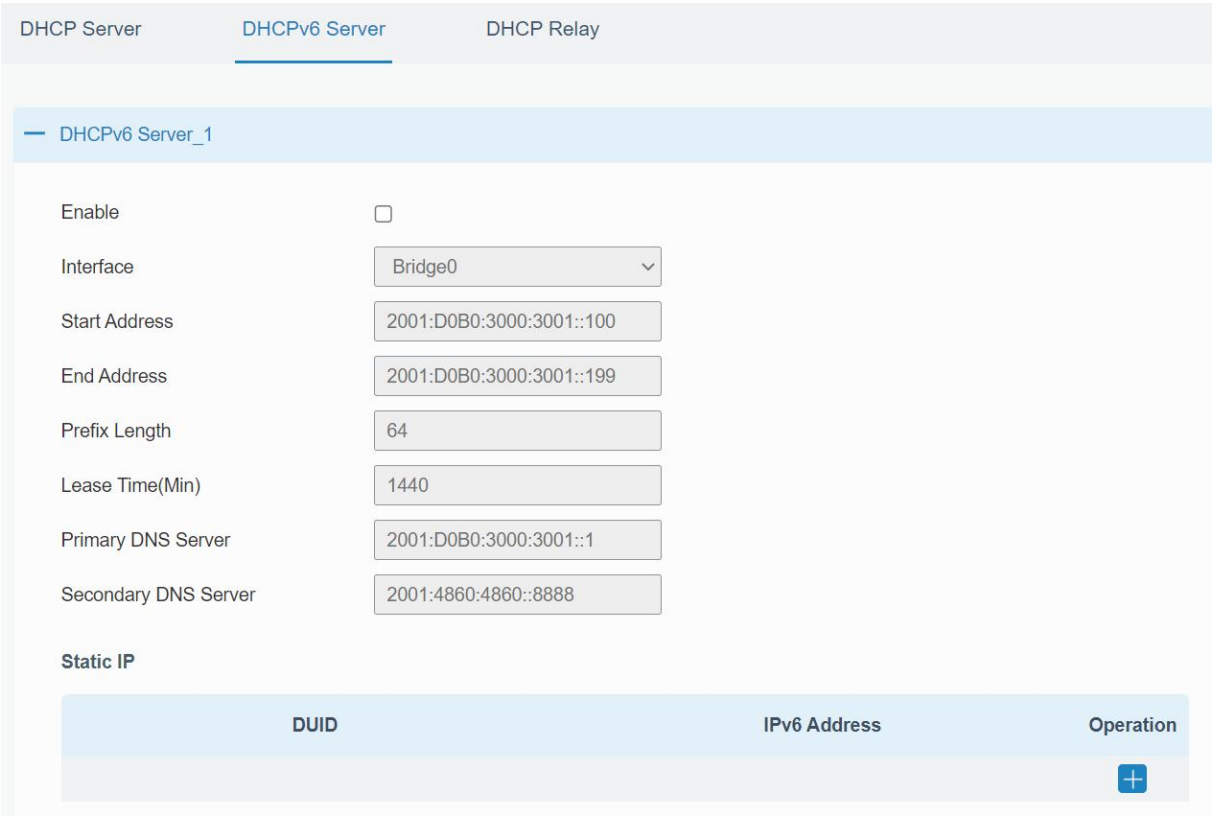
5.2.2 DHCP

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

5.2.2.1 DHCP Server/DHCPv6 Server

UR41 can be set as a DHCP server or DHCPv6 server to distribute IP address when a host logs on and ensures each host is supplied with different IP addresses. DHCP Server has simplified some previous network management tasks requiring manual operations to the largest extent. UR41 only supports stateful DHCPv6 when working as DHCPv6 server.





DHCP Server		
Item	**Description**	**Default**
Enable	Enable or disable DHCP server.	Enable
Interface	Select interface.	Bridge0
Start Address	Define the beginning of the pool of IP addresses which will be leased to DHCP clients.	192.168.1.100
End Address	Define the end of the pool of IP addresses which will be leased to DHCP clients.	192.168.1.199
Netmask	Define the subnet mask of IPv4 address obtained by DHCP clients from DHCP server.	255.255.255.0
Prefix Length	Set the IPv6 prefix length of IPv6 address obtained by DHCP clients from DHCP server.	64
Lease Time (Min)	Set the lease time on which the client can use the IP address obtained from DHCP server. Range: 1-10080.	1440
Primary DNS Server	Set the primary DNS server.	192.168.1.1
Secondary DNS Server	Set the secondary DNS server.	Null
Windows Name Server	Define the Windows Internet Naming Service obtained by DHCP clients from DHCP sever. Generally you can leave it blank.	Null
Static IP		
MAC Address	Set a static and specific MAC address for the DHCP client (it should be different from other MACs so as to avoid	Null

	conflict).	
DUID	Set a static and specific DUID for the DHCPv6 client (it should be different from other DUID so as to avoid conflict).	Null
IP Address	Set a static and specific IP address for the DHCP client (it should be outside of the DHCP range).	Null

5.2.2.2 DHCP Relay

UR41 can be set as DHCP Relay to provide a relay tunnel to solve the problem that DHCP Client and DHCP Server are not in the same subnet.

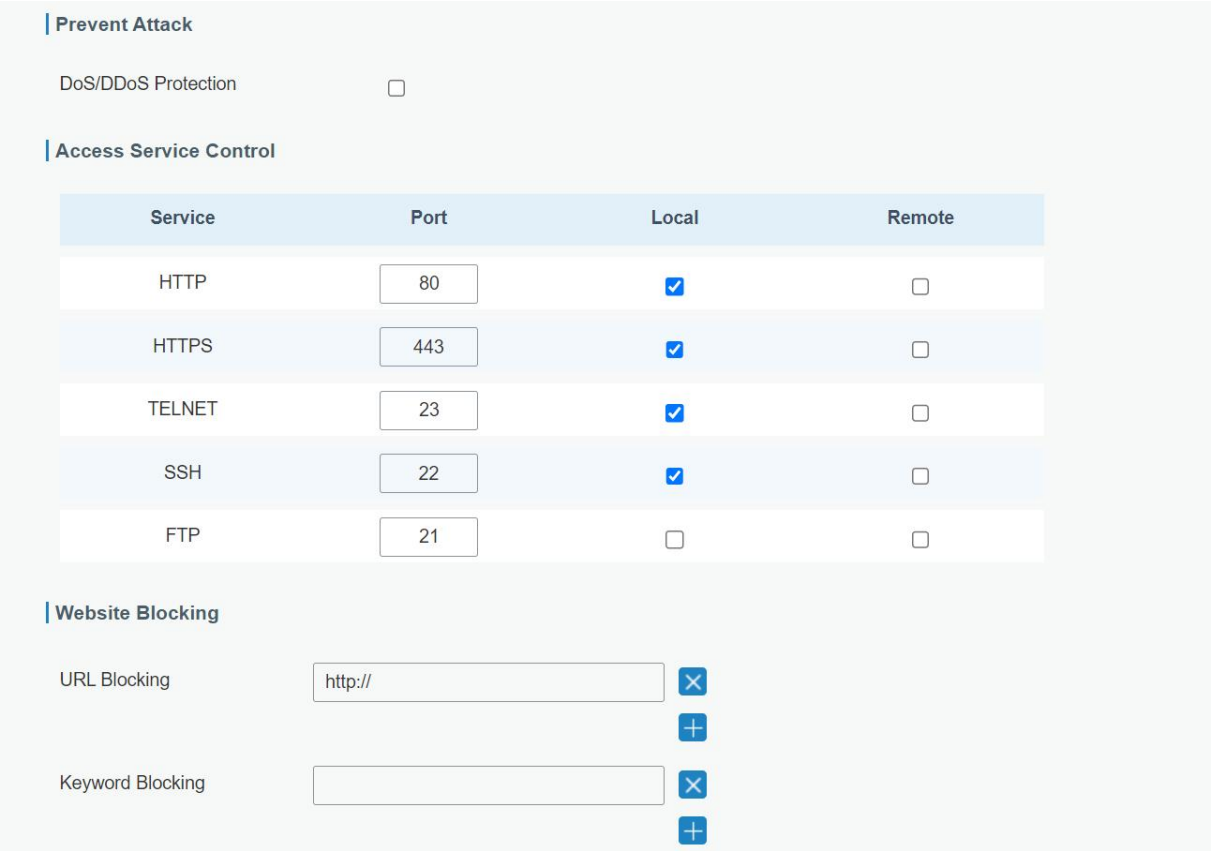
DHCP Relay	
Item	**Description**
Enable	Enable or disable DHCP relay.
DHCP Server	Set DHCP server, up to 10 servers can be configured; separate them by blank space or ",".

5.2.3 Firewall

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

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

5.2.3.1 Security



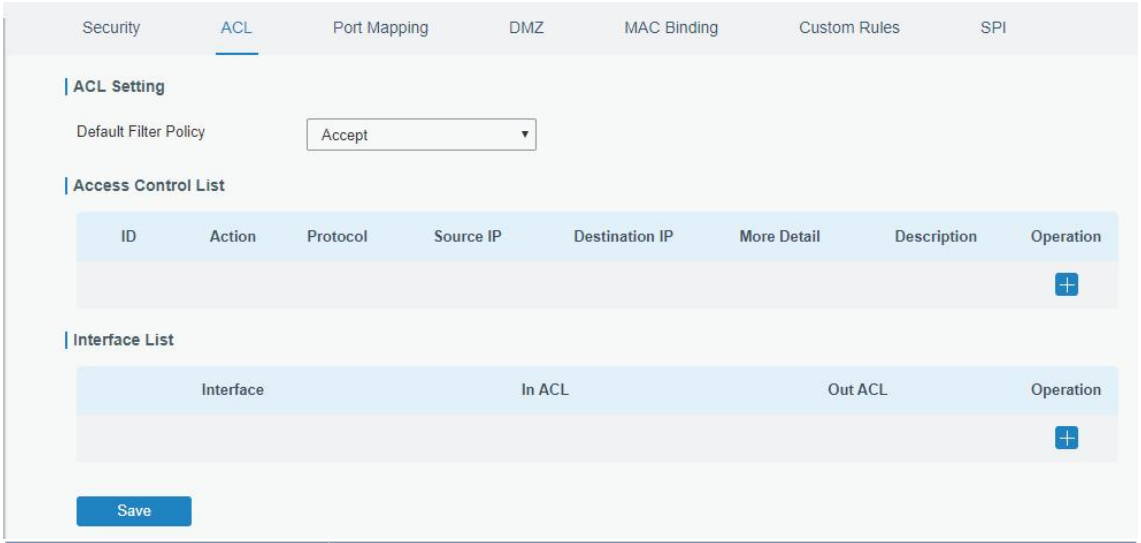
Item	Description	Default
Prevent Attack		
DoS/DDoS Protection	Enable/disable Prevent DoS/DDoS Attack.	Disable
Access Service Control		
Port	Set port number of the services. Range: 1-65535.	--
Local	Access the router locally.	Enable
Remote	Access the router remotely.	Disable
HTTP	Users can log in the device locally via HTTP to access and control it through Web after the option is checked.	80
HTTPS	Users can log in the device locally and remotely via HTTPS to access and control it through Web after option is checked.	443
TELNET	Users can log in the device locally and remotely via Telnet after the option is checked.	23
SSH	Users can log in the device locally and remotely via SSH after the option is checked.	22
FTP	Users can log in the device locally and remotely via FTP after the option is checked.	21
Website Blocking		
URL Blocking	Enter the HTTP address which you want to block.	

Keyword Blocking	You can block specific website by entering keyword. The maximum number of character allowed is 64.

5.2.3.2 ACL

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

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



Item	Description
ACL Setting	
Default Filter Policy	Select from "Accept" and "Deny". The packets which are not included in the access control list will be processed by the default filter policy.
Access Control List	
Type	Select type from "Extended" and "Standard".
ID	User-defined ACL number. Range: 1-199.
Action	Select from "Permit" and "Deny".
Protocol	Select protocol from "ip", "icmp", "tcp", "udp", and "1-255".
Source IP	Source network address (leaving it blank means all).
Source Wildcard Mask	Wildcard mask of the source network address.
Destination IP	Destination network address (0.0.0.0 means all).
Destination Wildcard Mask	Wildcard mask of destination address.
Description	Fill in a description for the groups with the same ID.
ICMP Type	Enter the type of ICMP packet. Range: 0-255.

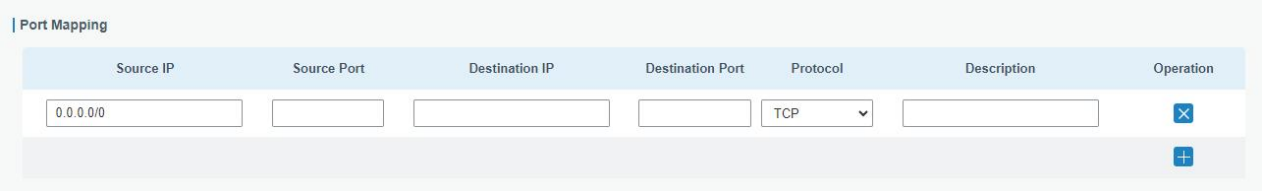
ICMP Code	Enter the code of ICMP packet. Range: 0-255.
Source Port Type	Select source port type, such as specified port, port range, etc.
Source Port	Set source port number. Range: 1-65535.
Start Source Port	Set start source port number. Range: 1-65535.
End Source Port	Set end source port number. Range: 1-65535.
Destination Port Type	Select destination port type, such as specified port, port range, etc.
Destination Port	Set destination port number. Range: 1-65535.
Start Destination Port	Set start destination port number. Range: 1-65535.
End Destination Port	Set end destination port number. Range: 1-65535.
More Details	Show information of the port.
Interface List	
Interface	Select network interface for access control.
In ACL	Select a rule for incoming traffic from ACL ID.
Out ACL	Select a rule for outgoing traffic from ACL ID.

Related Configuration Example

Access Control Application Example

5.2.3.3 Port Mapping

Port mapping is an application of network address translation (NAT) that redirects a communication request from the combination of an address and port number to another while the packets are traversing a network gateway such as a router or firewall.



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

Related Configuration Example

NAT Application Example

5.2.3.4 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 Address	Set the source IP address which can access to DMZ host. "0.0.0.0/0" means any address.

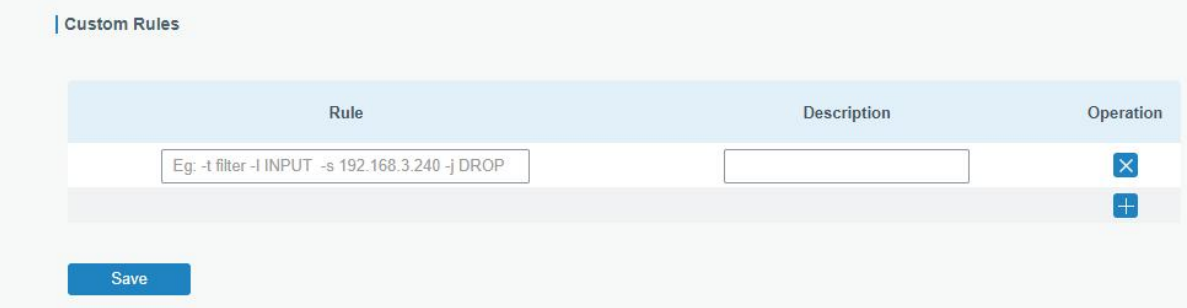
5.2.3.5 MAC Binding

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

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

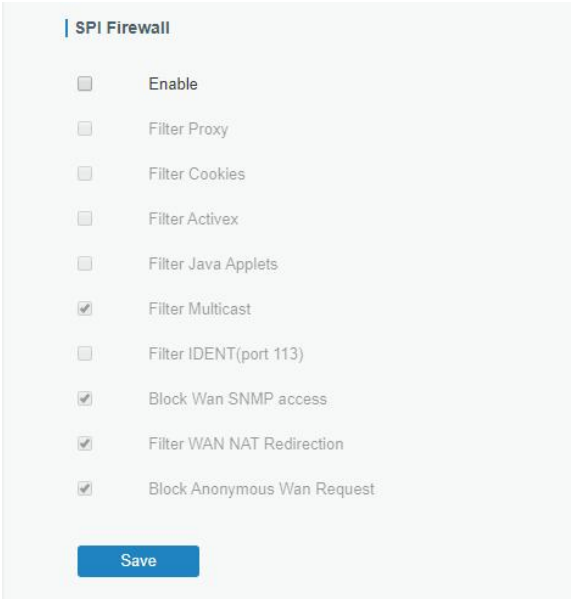
5.2.3.6 Custom Rules

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



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

5.2.3.7 SPI

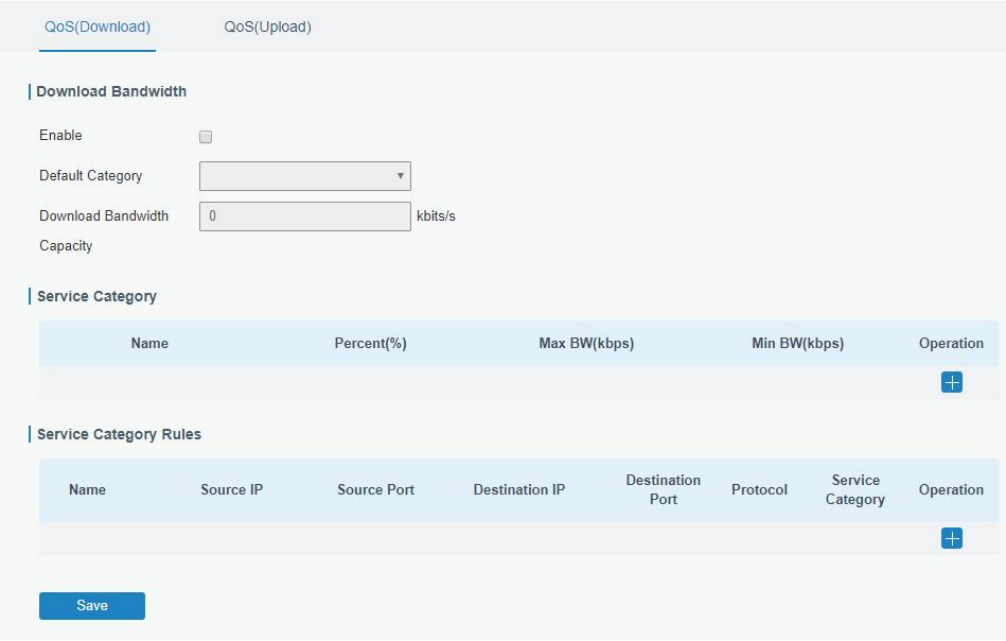


SPI Firewall	
Item	**Description**
Enable	Enable/disable SPI firewall.
Filter Proxy	Blocks HTTP requests containing the "Host": string.
Filter Cookies	Identifies HTTP requests that contain "Cookie": String and mangle the cookie. Attempts to stop cookies from being used.
Filter ActiveX	Blocks HTTP requests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

	connect servers on the LAN (which have been configured using port redirection).
Block Anonymous WAN Requests	Stop the router from responding to "pings" from the WAN.

5.2.4 QoS

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



QoS	
Item	**Description**
Download/Upload	
Enable	Enable or disable QoS.
Default Category	Select the default category from Service Category list.
Download/Upload Bandwidth Capacity	The download/upload bandwidth capacity of the network that the router is connected with, in kbps. Range: 1-8000000.
Service Category	
Name	You can use characters such digits, letters and "-".
Percent (%)	Set percent for the service category. Range: 0-100.
Max BW(kbps)	The maximum bandwidth that this category is allowed to consume, in kbps. The value should be less than the "Download/Upload Bandwidth Capacity" when the traffic is blocked.
Min BW(kbps)	The minimum bandwidth that can be guaranteed for the category, in kbps.The value should be less than the "MAX

	BW" value.
Service Category Rules	
Item	**Description**
Name	Give the rule a descriptive name.
Source IP	Source address of flow control (leaving it blank means any).
Source Port	Source port of flow control. Range: 0-65535 (leaving it blank means any).
Destination IP	Destination address of flow control (leaving it blank means any).
Destination Port	Destination port of flow control. Range: 0-65535 (leaving it blank means any).
Protocol	Select protocol from "ANY", "TCP", "UDP", "ICMP", and "GRE".
Service Category	Set service category for the rule.

Related Configuration Example

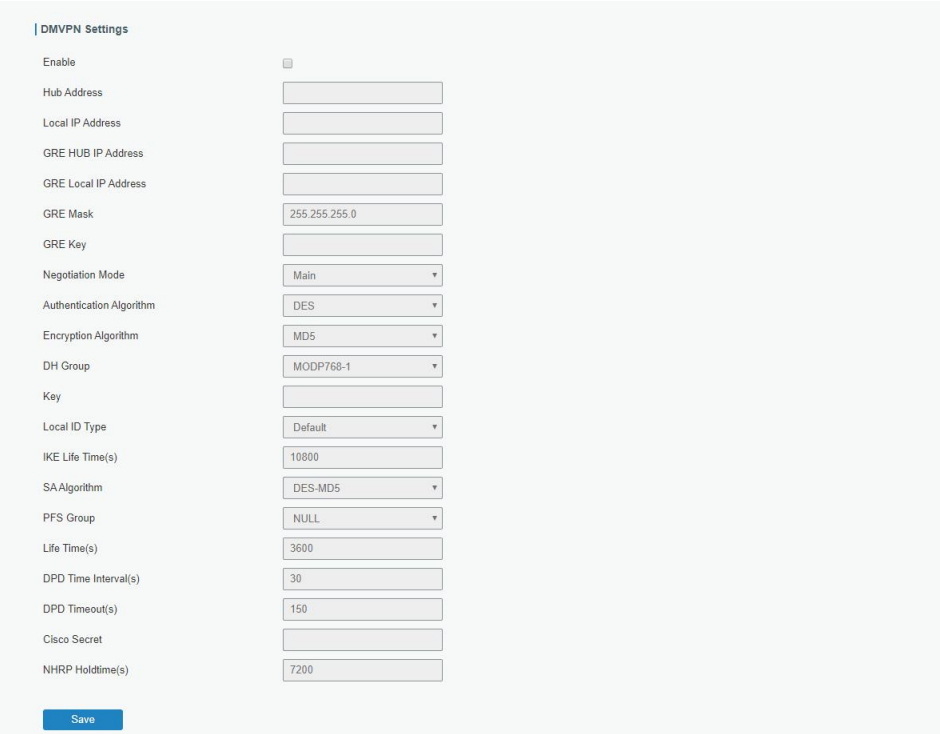
QoS Application Example

5.2.5 VPN

Virtual Private Networks, also called VPNs, are used to securely connect two private networks together so that devices can connect from one network to the other network via secure channels.
The UR41 supports DMVPN, IPsec, GRE, L2TP, PPTP, OpenVPN, as well as GRE over IPsec and L2TP over IPsec.

5.2.5.1 DMVPN

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



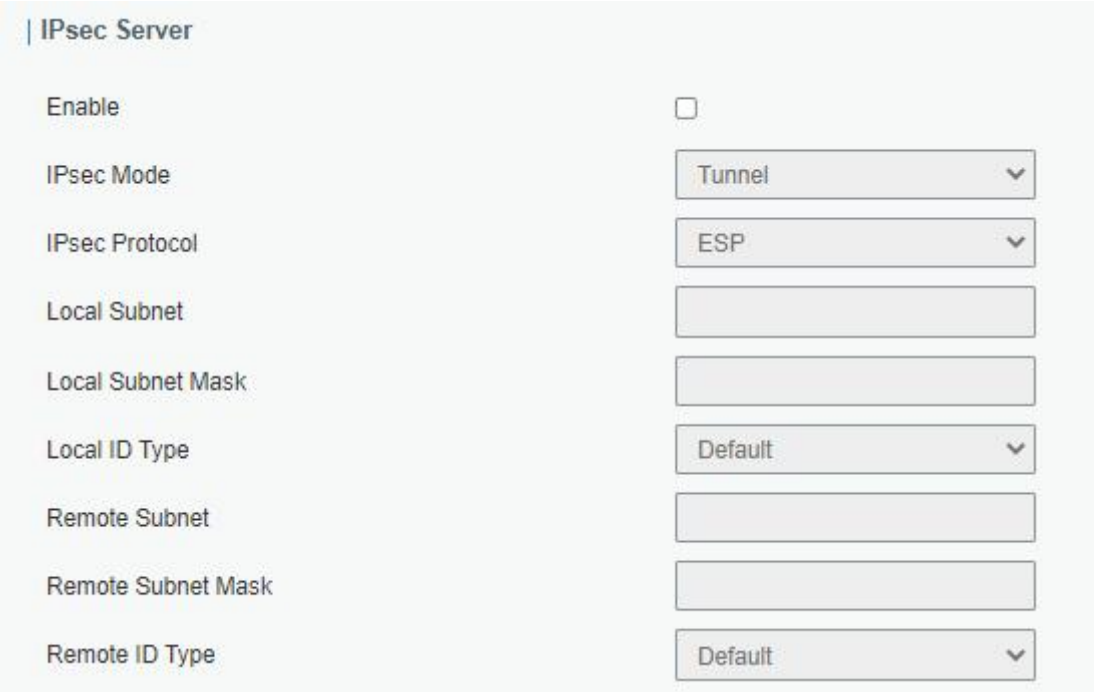
DMVPN	
Item	**Description**
Enable	Enable or disable DMVPN.
Hub Address	The IP address or domain name of DMVPN Hub.
Local IP address	DMVPN local tunnel IP address.
GRE Hub IP Address	GRE Hub tunnel IP address.
GRE Local IP Address	GRE local tunnel IP address.
GRE Netmask	GRE local tunnel netmask.
GRE Key	GRE tunnel key.
Negotiation Mode	Select from "Main" and "Aggressive".
Authentication Algorithm	Select from "DES", "3DES", "AES128", "AES192" and "AES256".
Encryption Algorithm	Select from "MD5" and "SHA1".
DH Group	Select from "MODP768_1", "MODP1024_2" and "MODP1536_5".
Key	Enter the preshared key.
Local ID Type	Select from "Default", "ID", "FQDN", and "User FQDN"
IKE Life Time (s)	Set the lifetime in IKE negotiation. Range: 60-86400.
SA Algorithm	Select from "DES_MD5", "DES_SHA1", "3DES_MD5", "3DES_SHA1", "AES128_MD5", "AES128_SHA1", "AES192_MD5", "AES192_SHA1", "AES256_MD5" and "AES256_SHA1".
PFS Group	Select from "NULL", "MODP768_1", "MODP1024_2" and "MODP1536-5".
Life Time (s)	Set the lifetime of IPsec SA. Range: 60-86400.
DPD Interval Time (s)	Set DPD interval time

DPD Timeout (s)	Set DPD timeout.
Cisco Secret	Cisco Nhrp key.
NHRP Holdtime (s)	The holdtime of NHRP protocol.

5.2.5.2 IPSec Server

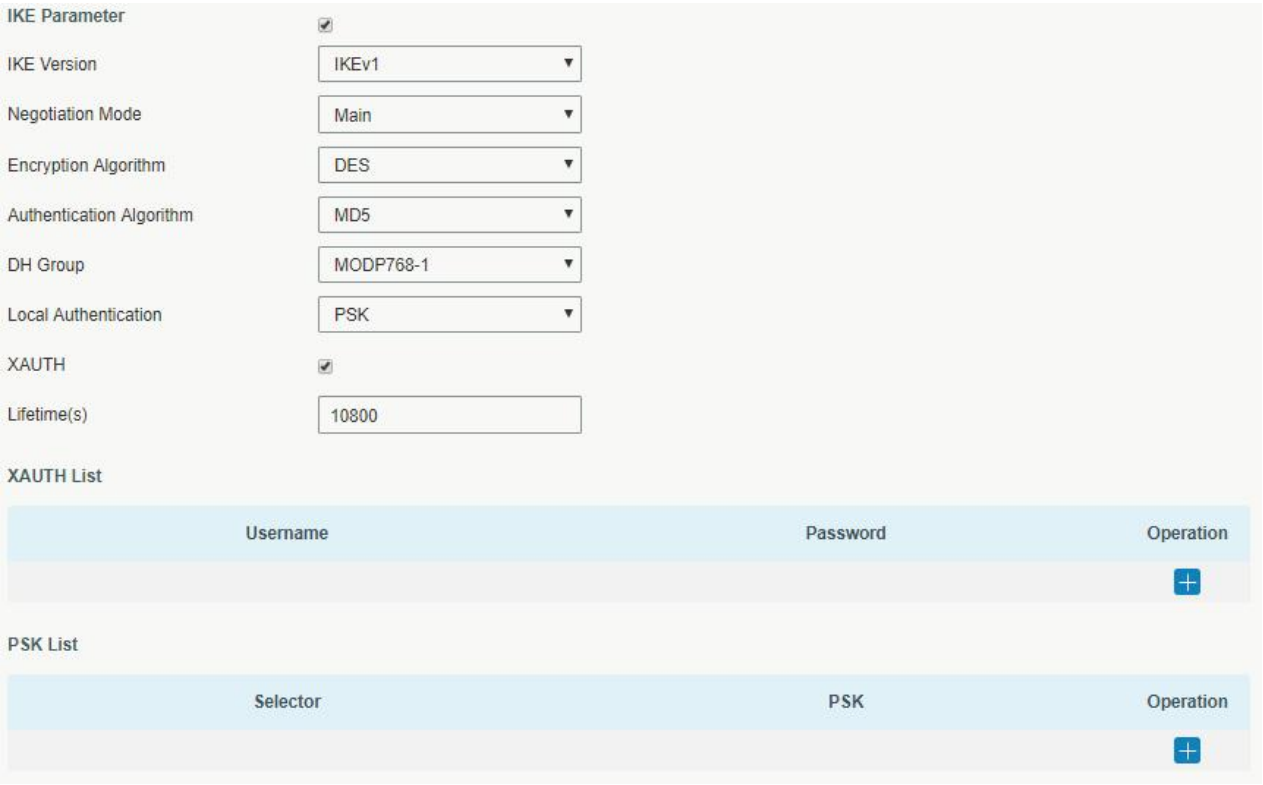
IPsec is especially useful for implementing virtual private networks and for remote user access through dial-up connection to private networks. A big advantage of IPsec is that security arrangements can be handled without requiring changes to individual user computers.

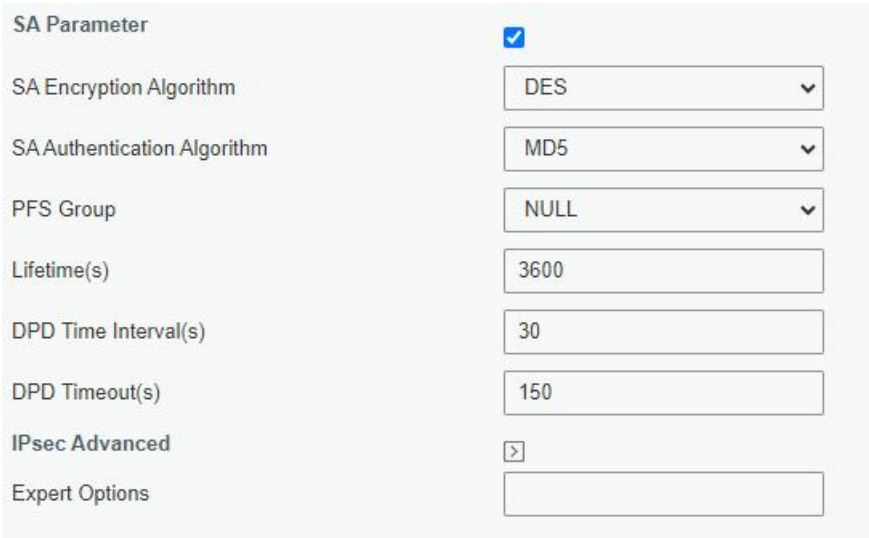
IPsec provides three choices of security service: Authentication Header (AH), Encapsulating Security Payload (ESP), and Internet Key Exchange (IKE). AH essentially allows authentication of the senders' data. ESP supports both authentication of the sender and data encryption. IKE is used for cipher code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



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



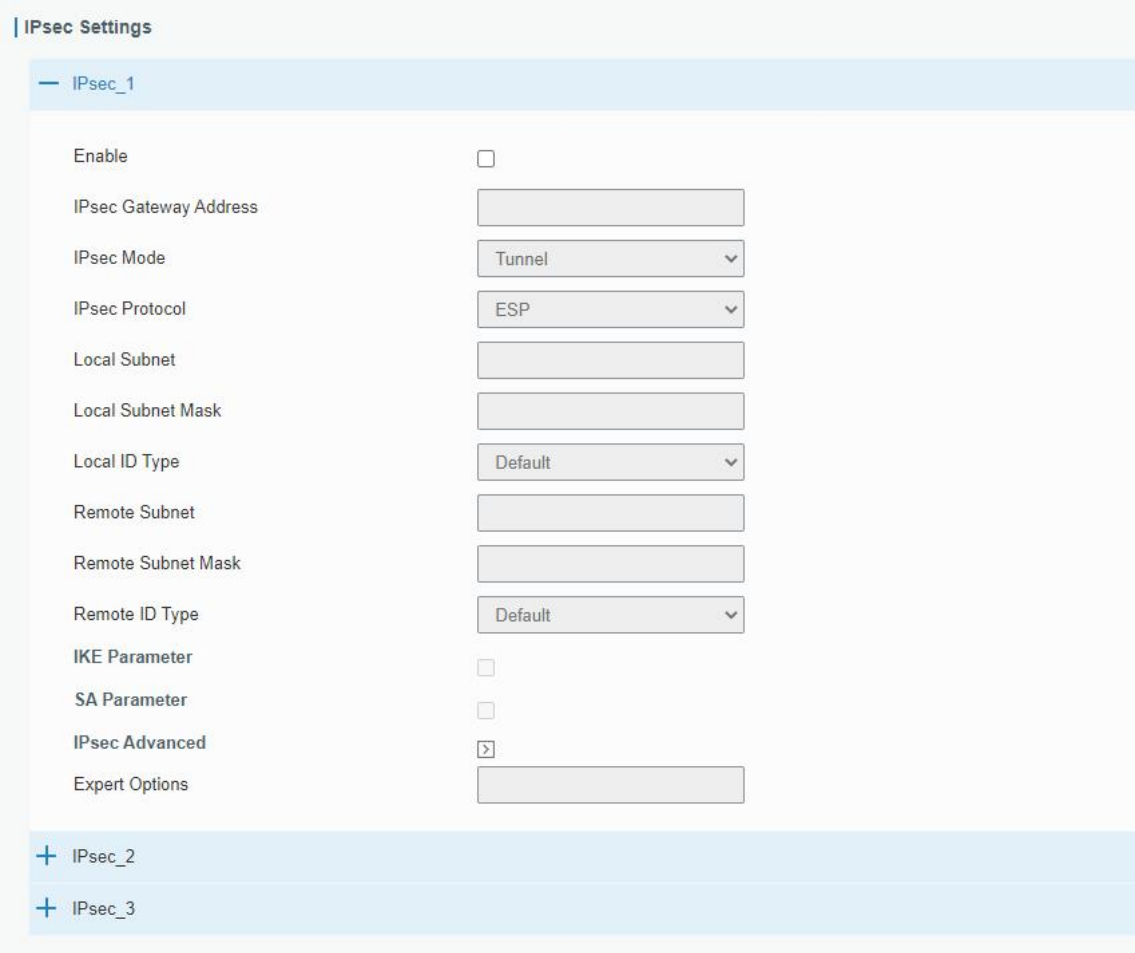


IKE Parameter	
Item	**Description**

IKE Version	Select the method of key exchange from IKEv1 and IKEv2.
Negotiation Mode	When using IKEv1, select Main or Aggressive.
Encryption Algorithm	Select DES, 3DES, AES128, AES192 or AES256.
Authentication Algorithm	Select MD5, SHA1 or SHA2-256.
DH Group	Select MODP768-1, MODP1024-2, MODP1536-5, MODP2048-14 or MODP3072-15.
Local Authentication	Select PSK or CA. **PSK:** use pre-shared key to complete the authentication. **CA:** use certificate to complete the authentication. After selecting, go to **Network > VPN > Certifications** page to import CA certificate, local certificate and private key to corresponding fields.
Remote Authentication	When using IKEv2, select PSK or CA. **PSK:** use pre-shared key to complete the authentication. **CA:** use certificate to complete the authentication. After selecting, go to **Network > VPN > Certifications** page to import remote certificate to corresponding fields.
XAUTH	When using IKEv1, define XAUTH username and password after XAUTH is enabled.
Lifetime (s)	Set the lifetime in IKE negotiation. Range: 60-86400.
XAUTH List	
Username	Enter the username used for the xauth authentication.
Password	Enter the password used for the xauth authentication.
PSK List	
Selector	Enter the corresponding identification number for PSK authentication.
PSK	Enter the pre-shared key.
SA Parameter	
SA Encryption Algorithm	Select DES, 3DES, AES128, AES192 or AES256.
SA Authentication Algorithm	Select MD5, SHA1 or SHA2-256.
PFS Group	Select NULL, MODP768-1 , MODP1024-2 or MODP1536-5.
Lifetime (s)	Set the lifetime of IPsec SA. Range: 60-86400 s.
DPD Time Interval(s)	Set DPD retry interval to send DPD requests. Range: 1-86400 s
DPD Timeout(s)	Set DPD timeout to detect the remote side fails. Range: 10-86400 s.
IPsec Advanced	
Enable Compression	The head of IP packet will be compressed after it's enabled.
Margintime	Set advanced time before the lifetime expires to begin the re-negotiation.
VPN Over IPsec Type	Select from NONE, GRE and L2TP.
Expert Options	User can enter some other initialization strings in this field and separate the strings with semicolon.

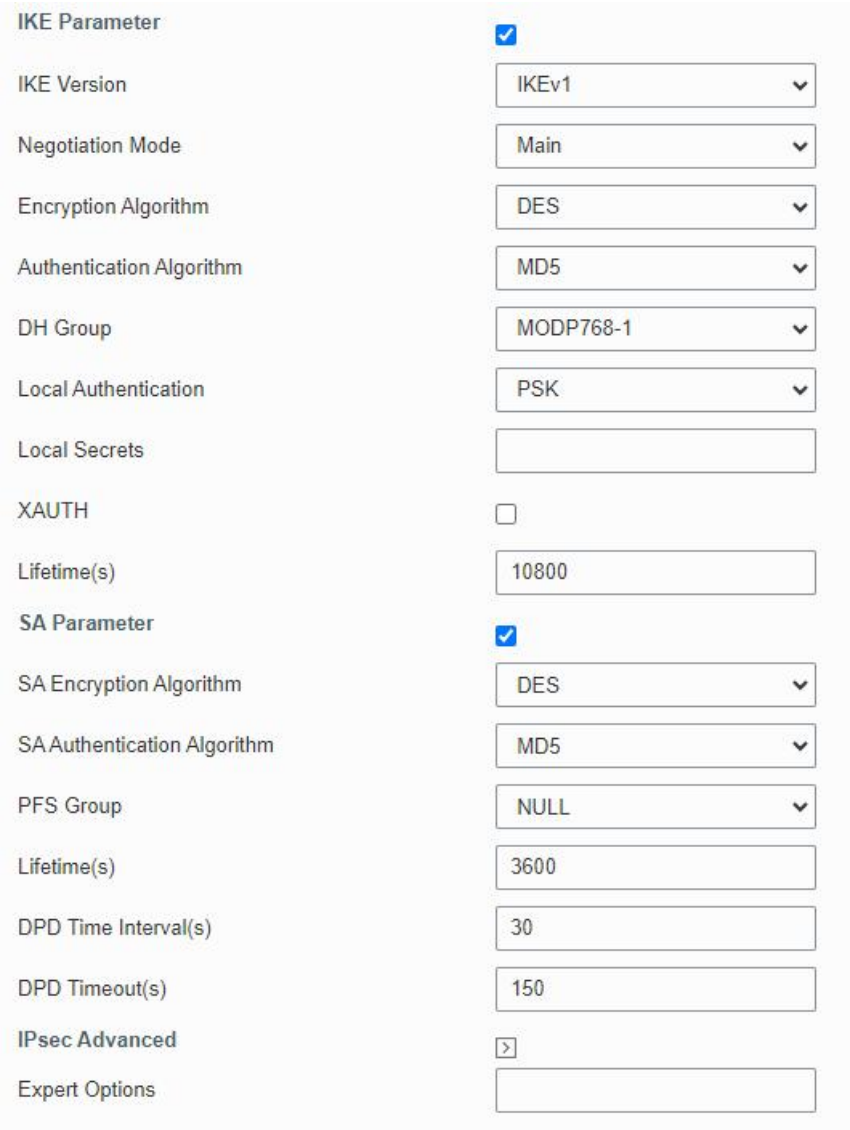
5.2.5.3 IPSec

UR41 supports running at most 3 IPsec clients at the same time.



IPsec	
Item	**Description**
Enable	Enable or disable IPsec client mode. A maximum of 3 tunnels is allowed.
IP Gateway Address	Enter the remote IPsec server address.
IPsec Mode	Select Tunnel or Transport.
IPsec Protocol	Select from ESP or AH.
Local Subnet	Enter the local LAN subnet IP address on the IPsec tunnel.
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



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

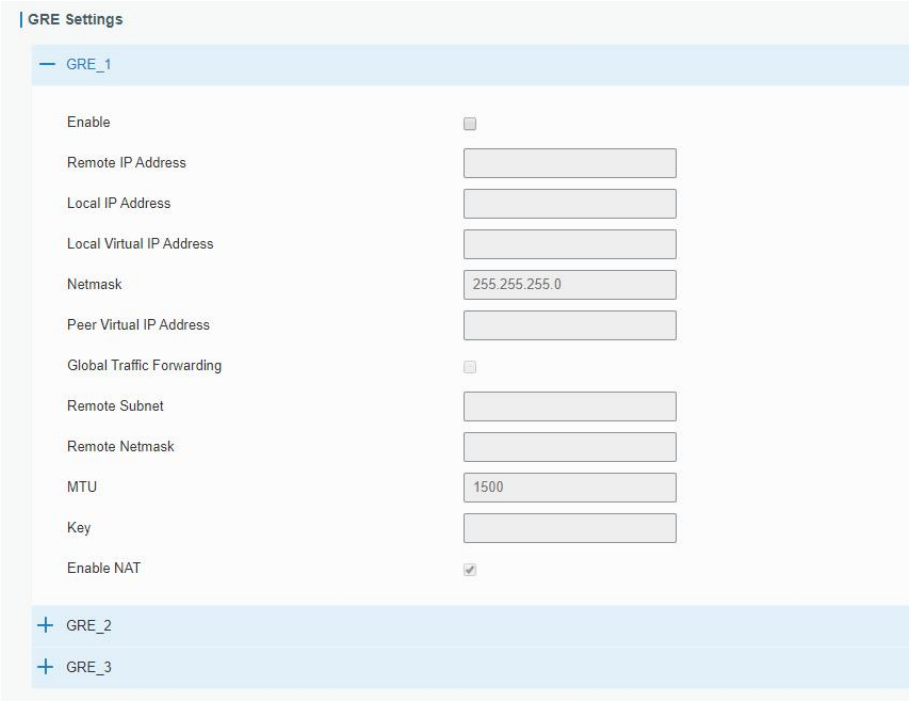
	CA: use certificate to complete the authentication. After selecting, go to **Network > VPN > Certifications** page to import CA certificate, local certificate and private key to corresponding fields.
Local Secrets	Enter the pre-shared key which is defined on serer side.
Remote Authentication	When using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

5.2.5.4 GRE

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

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

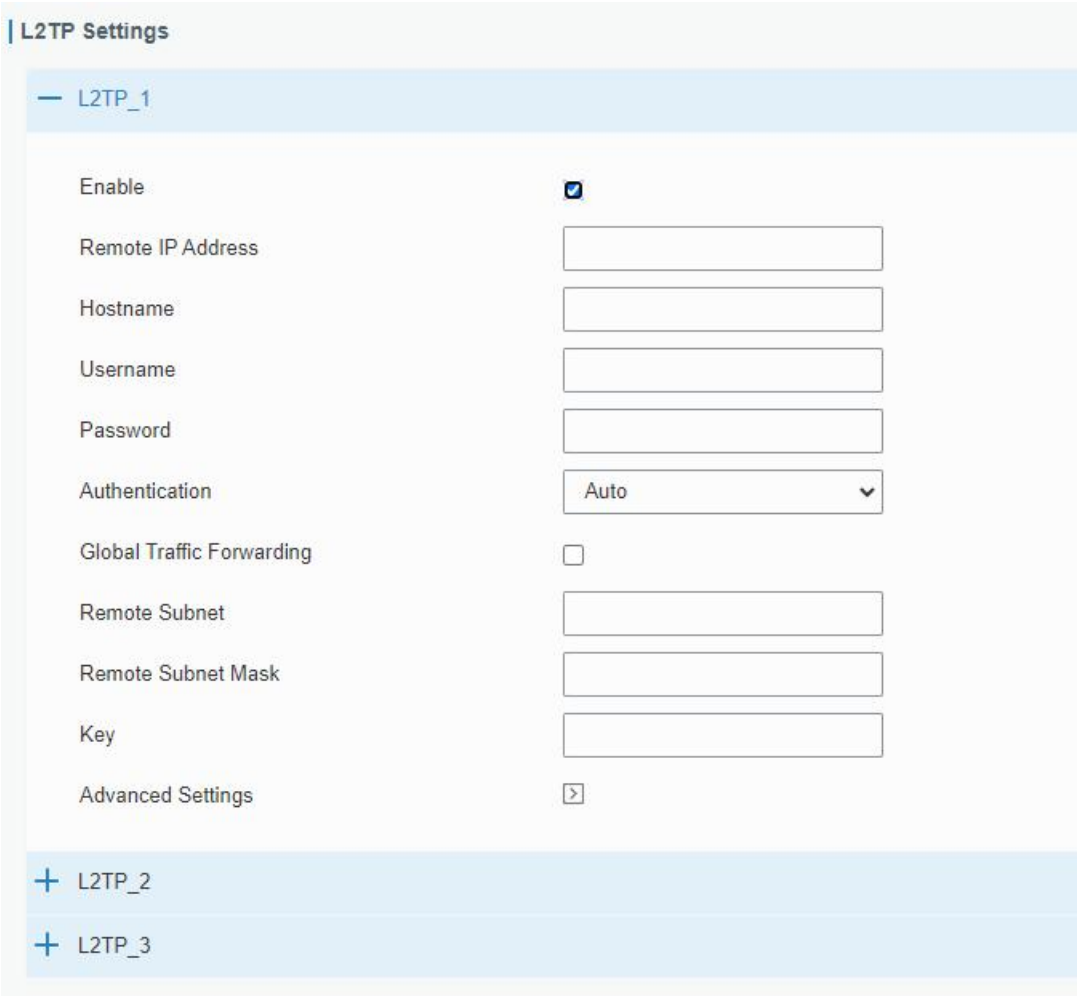
- GRE tunnel could transmit multicast data packets as if it were a true network interface. Single use of IPSec cannot achieve the encryption of multicast.
- A certain protocol adopted cannot be routed.
- A network of different IP addresses shall be required to connect other two similar networks.



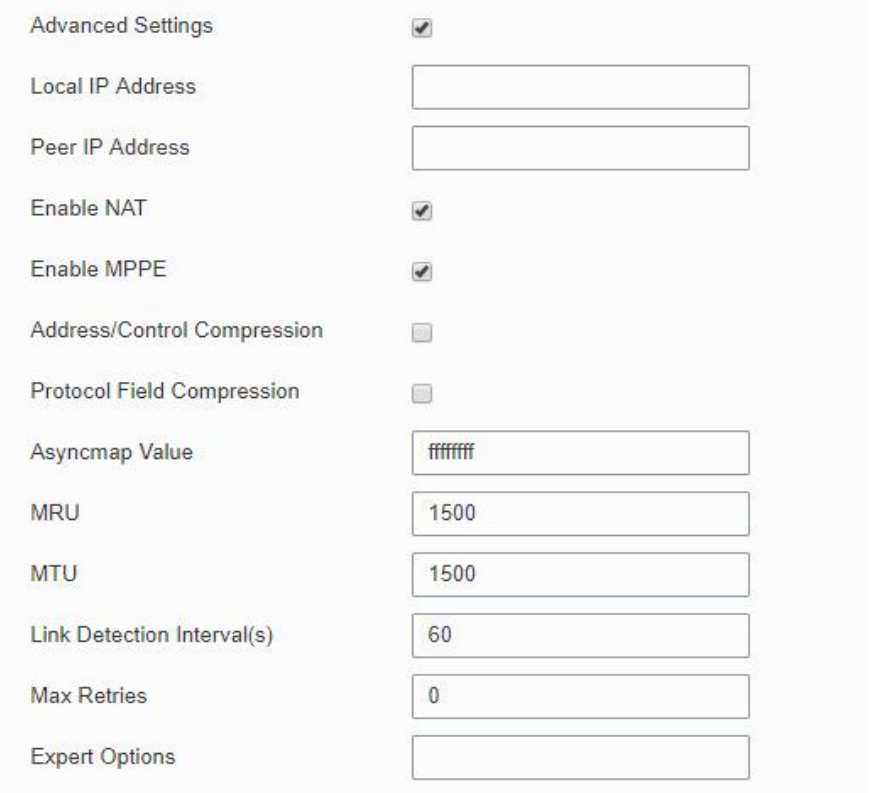
GRE	
Item	**Description**
Enable	Check to enable GRE function.
Remote IP Address	Enter the real remote IP address of GRE tunnel.
Local IP Address	Set the local IP address.
Local Virtual IP Address	Set the local tunnel IP address of GRE tunnel.
Netmask	Set the local netmask.
Peer Virtual IP Address	Enter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

5.2.5.5 L2TP

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



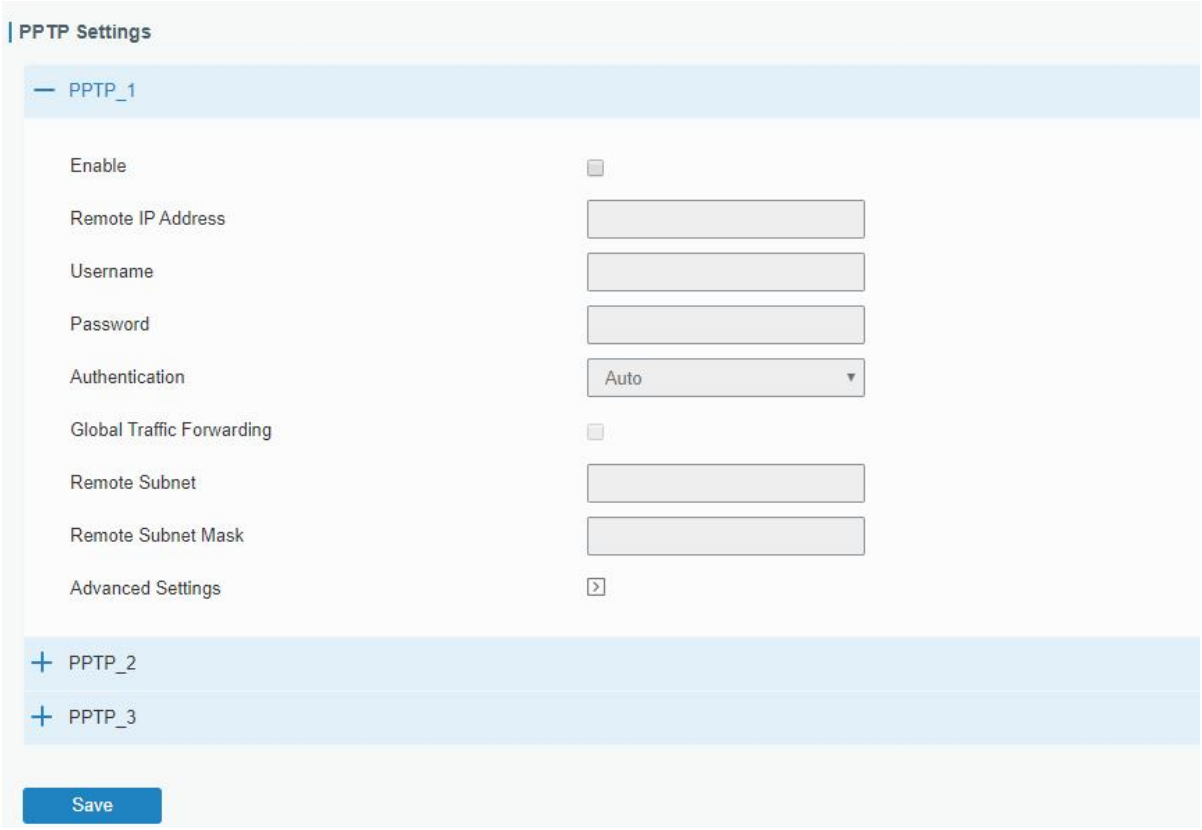
L2TP	
Item	**Description**
Enable	Check to enable L2TP function.
Remote IP Address	Enter the public IP address or domain name of L2TP server.
Hostname	Enter the hostname to verify with L2TP server.
Username	Enter the username that L2TP server provides.
Password	Enter the password that L2TP server provides.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



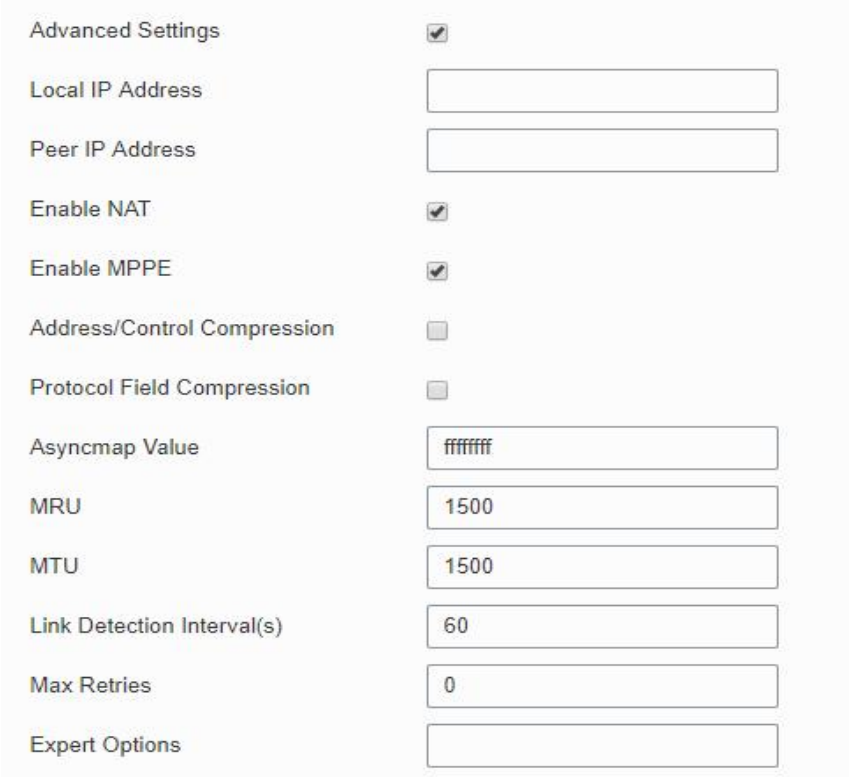
Advanced Settings	
Item	**Description**
Local IP Address	Set tunnel IP address of L2TP client. Client will obtain tunnel IP address automatically from the server when it's null.
Peer IP Address	Enter tunnel IP address of L2TP server.
Enable NAT	Enable NAT traversal function.
Enable MPPE	Enable MPPE encryption.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

5.2.5.6 PPTP

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



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



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

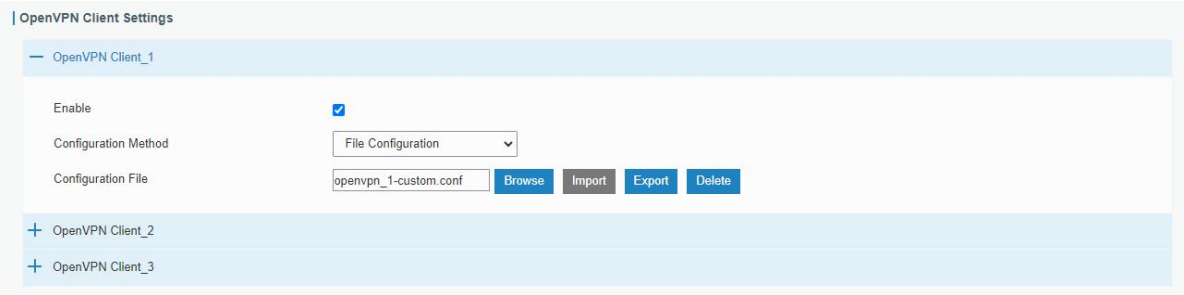
Related Configuration Example

PPTP Application Example

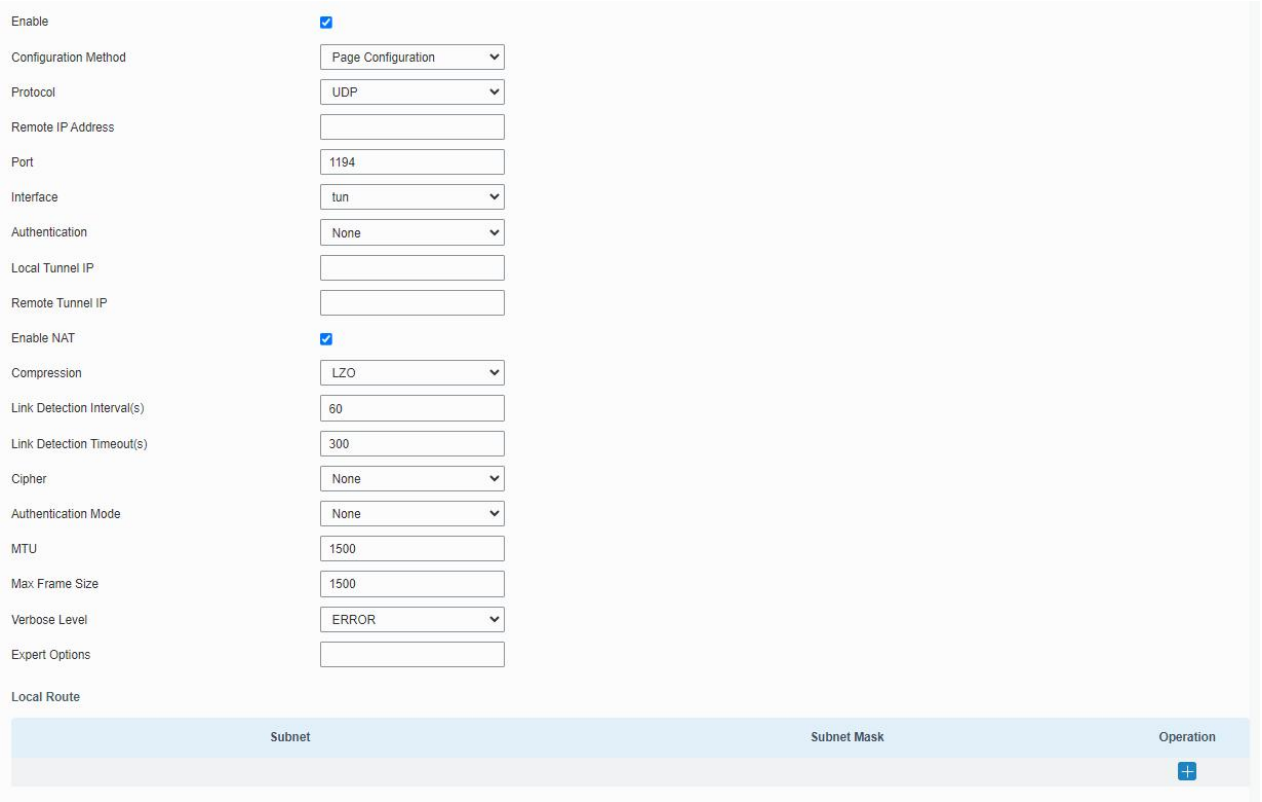
5.2.5.7 OpenVPN Client

OpenVPN is an open source virtual private network (VPN) product that offers a simplified security framework, modular network design, and cross-platform portability. The default OpenVPN version of UR41 is 2.4.9.

UR41 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.
Interface	Select virtual VPN network interface type from TUN and TAP. TUN devices encapsulate IPv4 or IPv6 (OSI Layer 3) while TAP devices encapsulate Ethernet 802.3 (OSI Layer 2).
Authentication Type	Select authentication type used to secure data sessions. **Pre-shared:** use the same secret key as server to complete the authentication. After selecting, go to **Network > VPN > Certifications** page to import a static.key to **PSK** field. **Username/Password:** use username/password which is preset in server side to complete the authentication. **X.509 cert:** use X.509 type certificate to complete the authentication. After selecting, go to **Network > VPN > Certifications** page to import CA certificate, client certificate and client private key to corresponding fields. **X.509 cert + user:** use both username/password and X.509 cert authentication type.
Local Virtual IP	Set local tunnel address when authentication type is **None** or **Pre-shared**.
Remote Virtual IP	Set remote tunnel address when authentication type is **None** or **Pre-shared**.
Global Traffic Forwarding	All the data traffic will be sent out via OpenVPN tunnel when this function is enabled.
Enable TLS Authentication	Select from None, TLS Auth and TLS Crypt. When selecting TLS Auth or TLS Crypt, go to **Network > VPN > Certifications** page to import a ta.key.
Compression	Select to enable or disable LZO to compress data.
Link Detection Interval (s)	Set link detection interval time to ensure tunnel connection. If this is set on both server and client, the value pushed from server will override the client local values. Range: 10-1800 s.
Link Detection Timeout (s)	OpenVPN will be reestablished after timeout. If this is set on both server and client, the value pushed from server will override the client local values. Range: 60-3600 s.
Cipher	Select from NONE, BF-CBC, DES-CBC, DES-EDE3-CBC, AES-128-CBC, AES-192-CBC and AES-256-CBC.
Authentication Mode	Select from NONE, MD5, SHA1, SHA256, and SHA512.
MTU	Enter the maximum transmission unit. Range: 128-1500.
Max Frame Size	Set the maximum frame size. Range: 128-1500.
Verbose Level	Select from ERROR, WARING, NOTICE and DEBUG.
Expert Options	User can enter some initialization strings in this field and separate the strings with semicolon. **Example:** ncp-ciphers AES-128-GCM; key direction 1
Local Route	
Subnet	Set the local route's IP address.

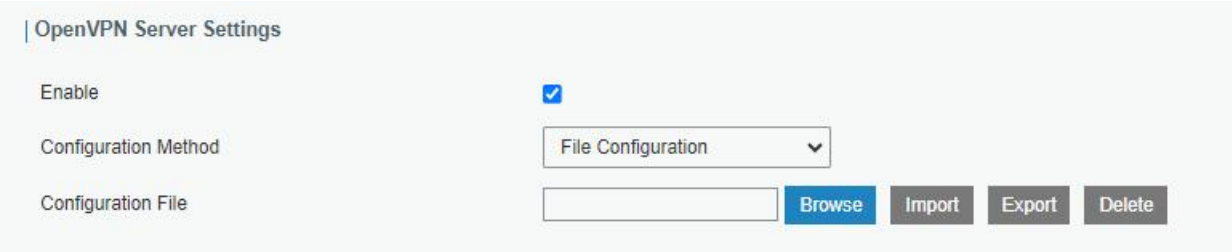
Subnet Mask	Set the local route's netmask.

Related Topic

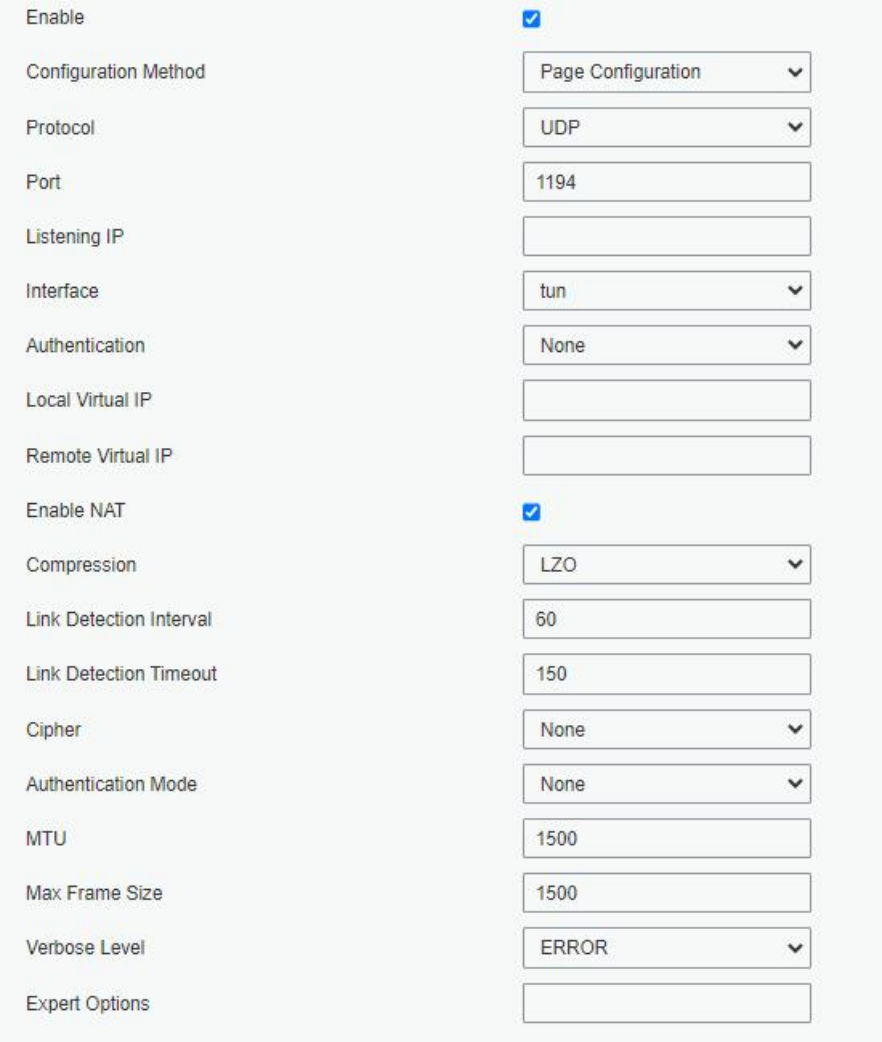
OpenVPN Client Application Example

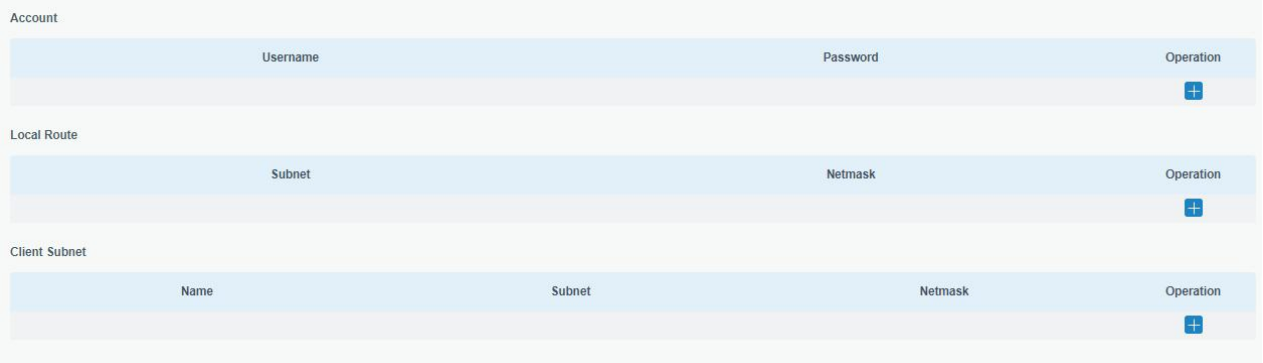
5.2.5.8 OpenVPN Server

The UR41 supports OpenVPN server to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities. Users can import the ovpn file directly or configure the parameters on this page to set this server. UR41 supports at most 20 openVPN clients connections.



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.





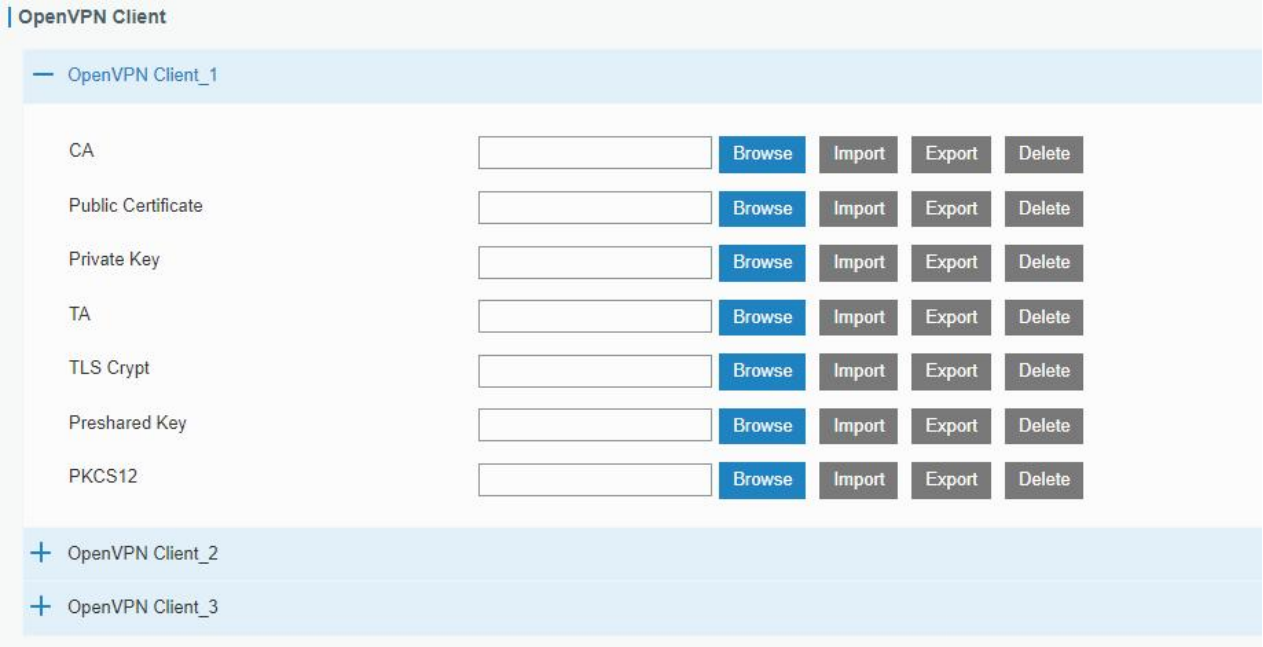
OpenVPN Server - Page Configuration	
Item	**Description**
Protocol	Select a transport protocol used by connection from UDP and TCP.
Listening IP	Enter the local hostname or IP address for bind. If left blank, OpenVPN server will bind to all interfaces.
Port	Enter the TCP/UCP service number for OpenVPN client connection. Range: 1-65535.
Interface	Select virtual VPN network interface type from TUN and TAP. TUN devices encapsulate IPv4 or IPv6 (OSI Layer 3) while TAP devices

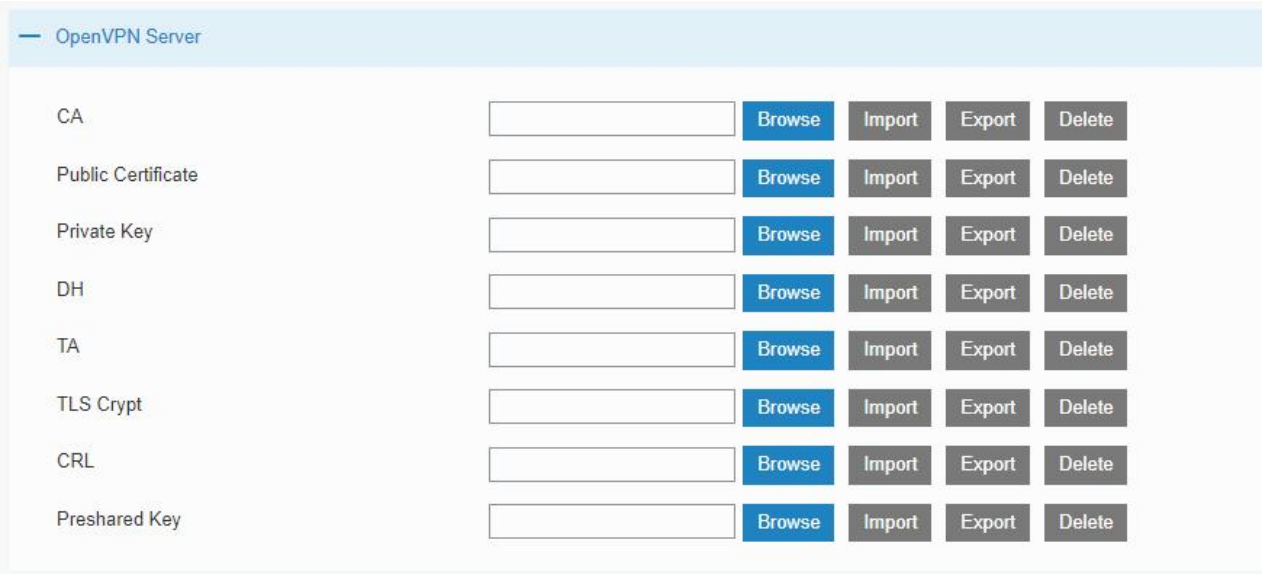
	encapsulate Ethernet 802.3 (OSI Layer 2).
Authentication Type	Select authentication type used to secure data sessions. **Pre-shared:** use the same secret key as server to complete the authentication. After select, go to **Network > VPN > Certifications** page to import a static.key to **PSK** field.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

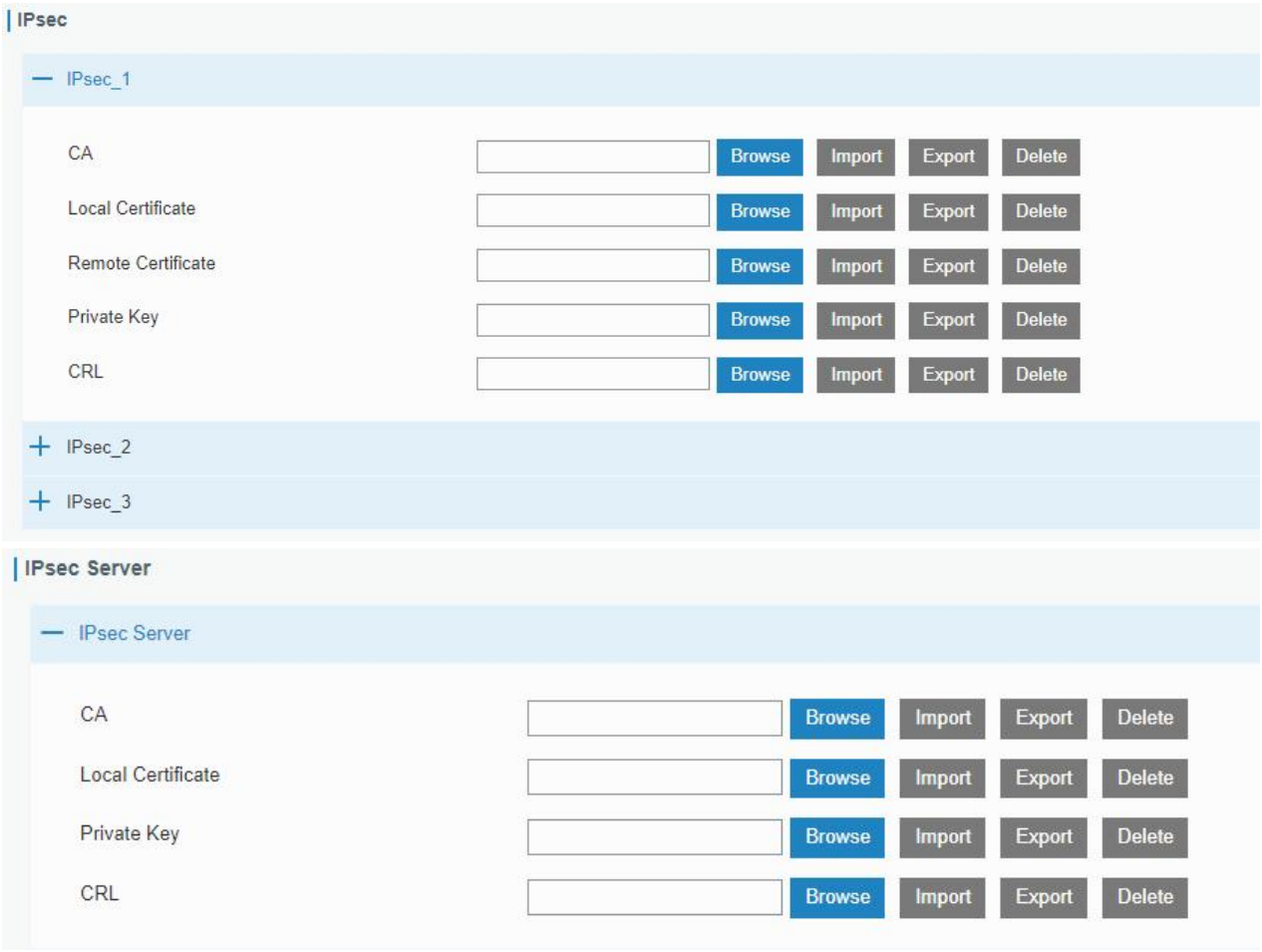
Username & Password	Set username and password for OpenVPN client when authentication type is username/password.
Local Route	
Subnet	Set the local route's IP address.
Subnet Mask	Set the local route's netmask.
Client Subnet	
Name	Set the name as OpenVPN client certificate common name.
Subnet	Set the subnet of OpenVPN client.
Subnet Mask	Set the subnet netmask of OpenVPN client.

5.2.5.9 Certifications

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

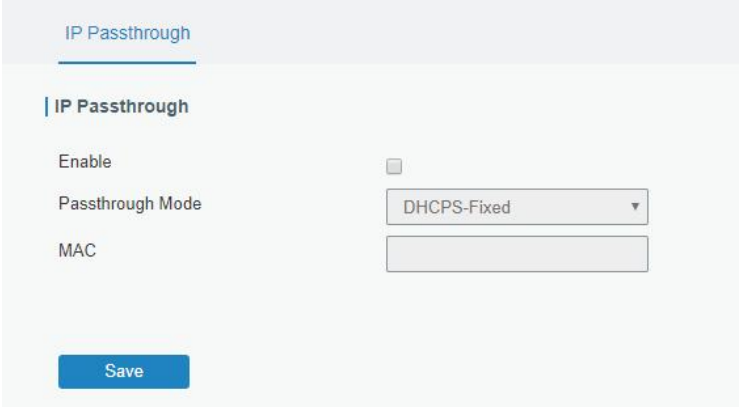






5.2.6 IP Passthrough

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

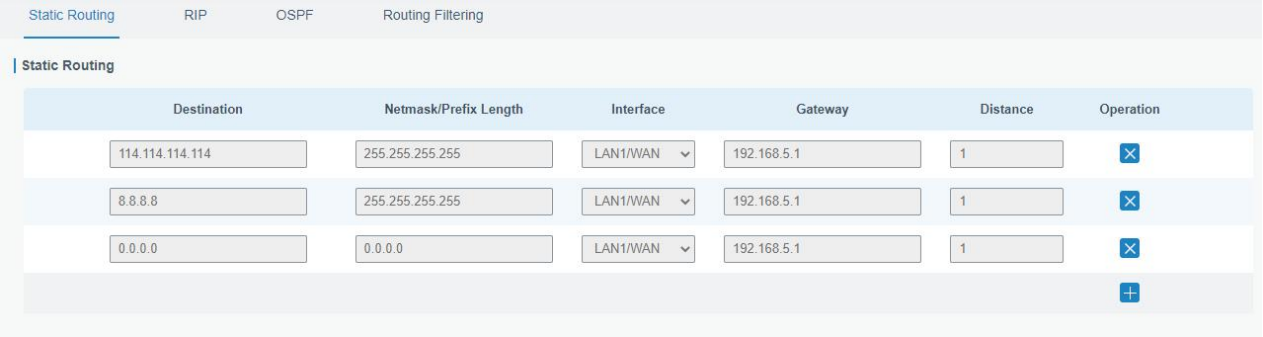


IP Passthrough	
Item	**Description**
Enable	Enable or disable IP Passthrough.
Passthrough Mode	Select passthrough mode from DHCPS-Fixed and DHCPS-Dynamic.
MAC	Set MAC address.

5.2.7 Routing

5.2.7.1 Static Routing

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

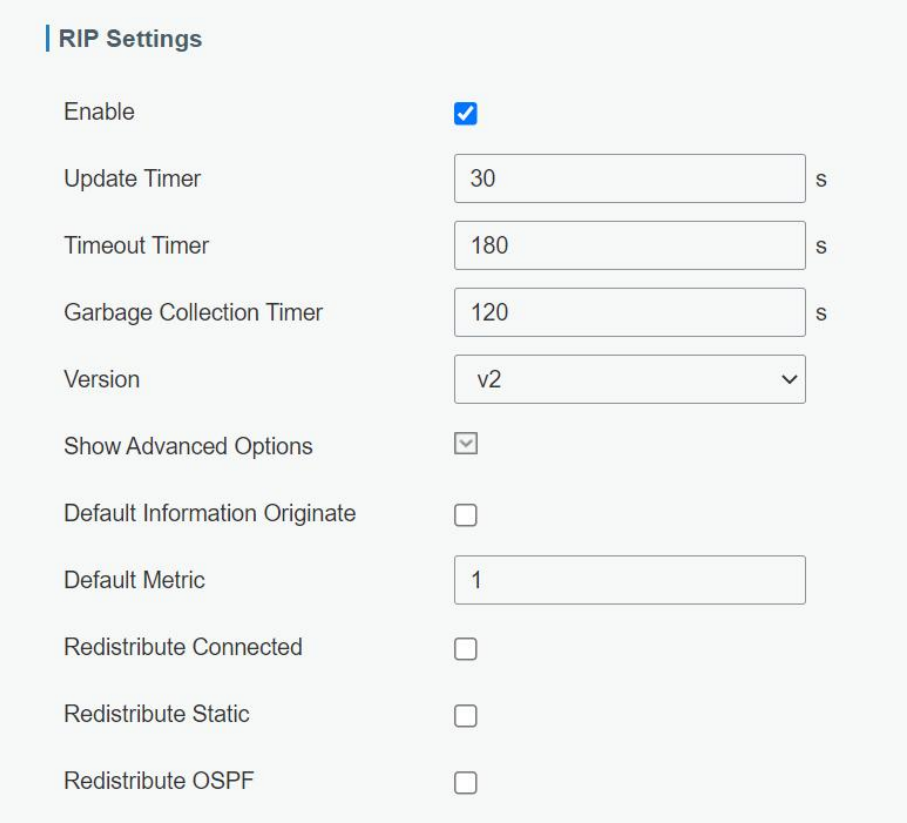


Static Routing	
Item	**Description**
Destination	Enter the destination IP address.
Netmask/Prefix Length	Enter the subnet mask or prefix length of destination address.
Interface	The interface through which the data can reach the destination address.
Gateway	IP address of the next router that will be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

5.2.7.2 RIP

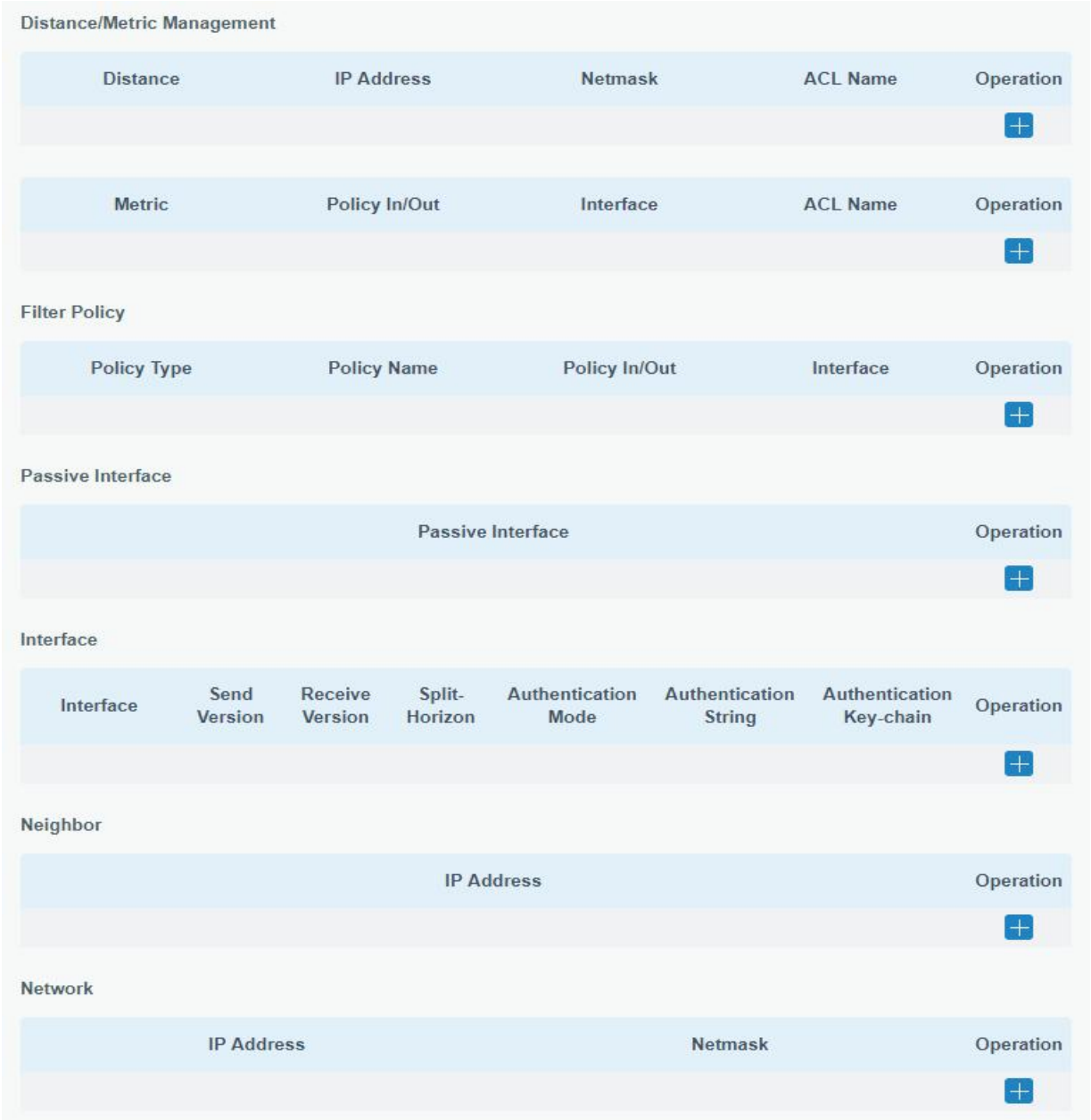
RIP is mainly designed for small networks. RIP uses Hop Count to measure the distance to the destination address, which is called Metric. In RIP, the hop count from the router to its directly connected network is 0 and the hop count of network to be reached through a router is 1 and so on. In order to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

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



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

Redistribute OSPF	Check to enable.
Metric	Set metric after "Redistribute OSPF" is enabled. Range: 0-16.



Item	Description
Distance/Metric Management	
Distance	Set the administrative distance that a RIP route learns. Range: 1-255.
IP Address	Set the IP address of RIP route.
Netmask	Set the netmask of RIP route.
ACL Name	Set ACL name of RIP route.
Metric	The metric of received route or sent route from the interface.

	Range: 0-16.
Policy in/out	Select from "in" and "out".
Interface	Select interface of the route.
ACL Name	Access control list name of the route strategy.
Filter Policy	
Policy Type	Select from "access-list" and "prefix-list".
Policy Name	User-defined prefix-list name.
Policy in/out	Select from "in" and "out".
Interface	Select interface from "cellular0", "LAN1/WAN" and "Bridge0".
Passive Interface	
Passive Interface	Select interface from "cellular0" and "LAN1/WAN", "Bridge0".
Interface	
Interface	Select interface from "cellular0", "LAN1/WAN" and "Bridge0".
Send Version	Select from "default", "v1" and "v2".
Receive Version	Select from "default", "v1" and "v2".
Split-Horizon	Select from "enable" and "disable".
Authentication Mode	Select from "text" and "md5".
Authentication String	The authentication key for package interaction in RIPV2.
Authentication Key-chain	The authentication key-chain for package interaction in RIPV2.
Neighbor	
IP Address	Set RIP neighbor's IP address manually.
Network	
IP Address	The IP address of interface for RIP publishing.
Netmask	The netmask of interface for RIP publishing.

5.2.7.3 OSPF

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

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

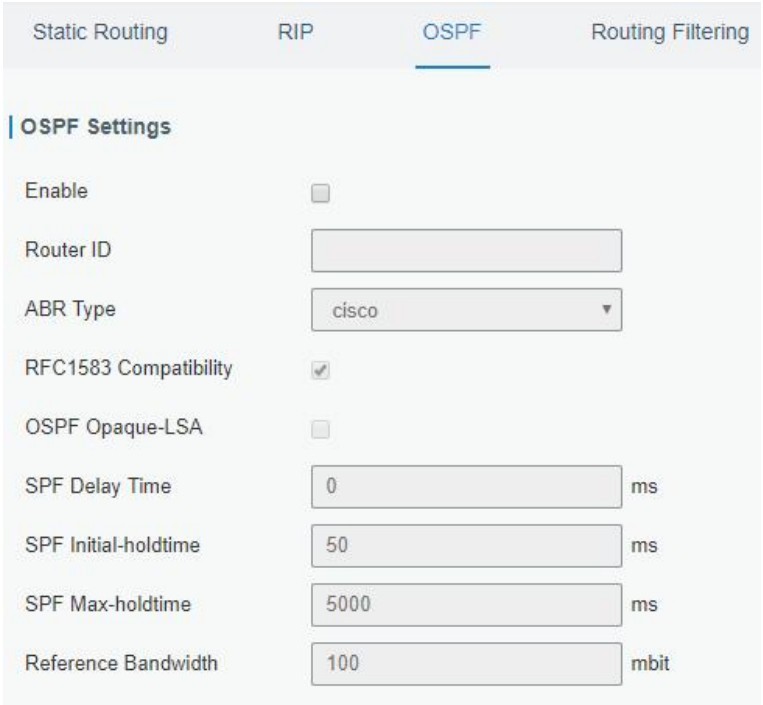
- If a Loopback interface address is configured, then the last configured IP address of Loopback interface will be used as the Router ID;
- If no Loopback interface address is configured, the system will choose the interface with the biggest IP address as the Router ID.

Five types of packets of OSPF:

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

Neighbor and Neighboring

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



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

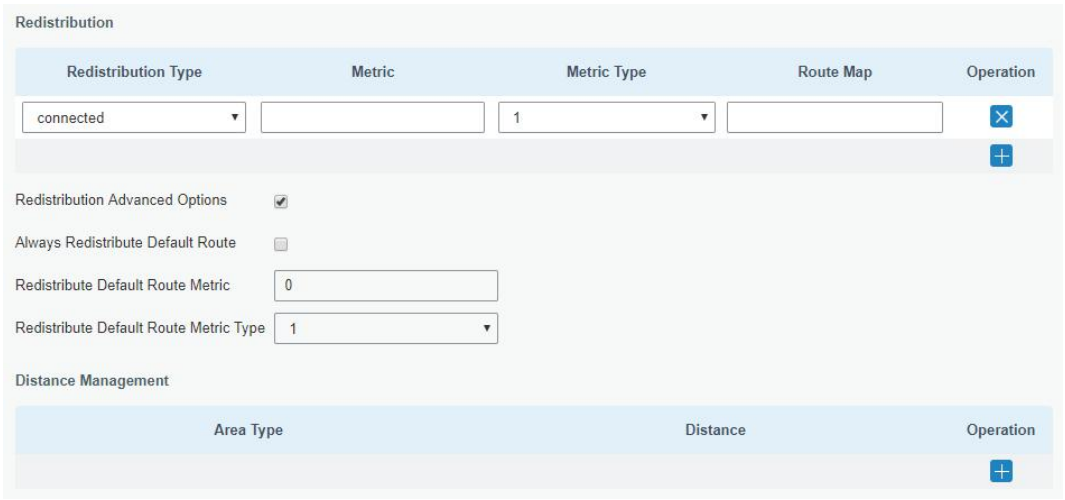
SPF Initial-holdtime	Set the initialization time of OSPF SPF. Range: 0-6000000, in milliseconds.
SPF Max-holdtime	Set the maximum time of OSPF SPF. Range: 0-6000000, in milliseconds.
Reference Bandwidth	Range: 1-4294967, in Mbit.

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

	confirmed again. MD5: MD5 key & password should be configured and confirmed again.
Key ID	It only takes effect when MD5 is selected. Range 1-255.
Key	The authentication key for OSPF packet interaction.

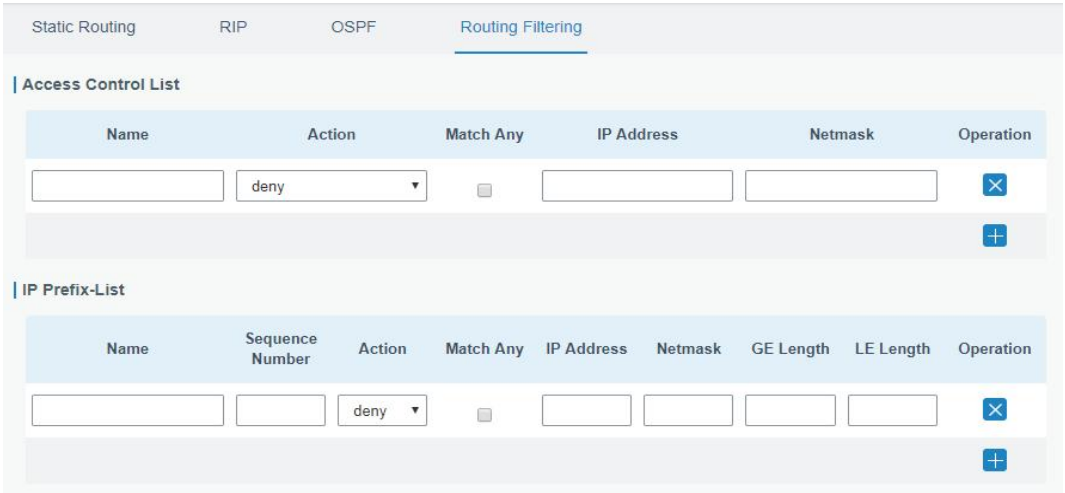
Item	Description
Passive Interface	
Passive Interface	Select interface from "cellular0" and "Bridge0".
Network	
IP Address	The IP address of local network.
Netmask	The netmask of local network.
Area ID	The area ID of original LSA's router.
Area	
Area ID	Set the ID of the OSPF area (IP address).
Area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

Area Advanced Options	
Item	**Description**
Area Range	
Area ID	The area ID of the interface when it runs OSPF (IP address).
IP Address	Set the IP address.
Netmask	Set the netmask.
No Advertise	Forbid the route information to be advertised among different areas.
Cost	Range: 0-16777215
Area Filter	
Area ID	Select an Area ID for Area Filter.
Filter Type	Select from "import", "export", "filter-in", and "filter-out".
ACL Name	Enter an ACL name which is set on "Routing > Routing Filtering" webpage.
Area Virtual Link	
Area ID	Set the ID number of OSPF area.
ABR Address	ABR is the router connected to multiple outer areas.
Authentication	Select from "simple" and "md5".
Key ID	It only takes effect when MD5 is selected. Range 1-15.
Key	The authentication key for OSPF packet interaction.
Hello Interval	Set the interval time for sending Hello packets through the interface. Range: 1-65535.
Dead Interval	The dead interval time for sending Hello packets through the interface. Range: 1-65535.
Retransmit Interval	The retransmission interval time for re-sending LSA. Range: 1-65535.
Transmit Delay	The delay time for LSA transmission. Range: 1-65535.



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

5.2.7.4 Routing Filtering



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

5.2.8 VRRP

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

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

In VRRP, routers need to be aware of failures in the virtual master router. To achieve this, the virtual master router sends out multicast “alive” announcements to the virtual backup routers in the same VRRP group.

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

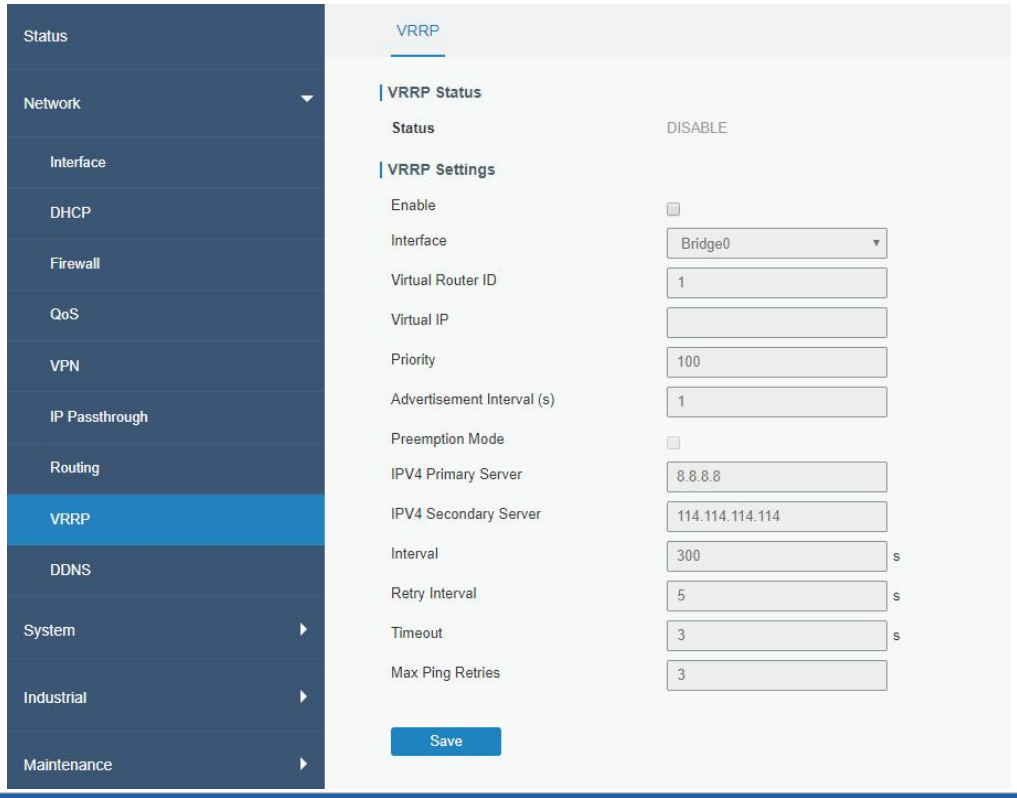
If the current virtual master router receives an announcement from a group member (Router ID) with a higher priority, then the latter will pre-empt and become the virtual master router.

VRRP has the following characteristics:

- The virtual router with an IP address is known as the Virtual IP address. For the host in LAN, it is only required to know the IP address of virtual router, and set it as the address of the next hop of the default route.
- The network Host communicates with the external network through this virtual router.

- A router will be selected from the set of routers based on its priority to undertake the gateway function. Other routers will be used as backup routers to perform the duties of gateway for the gateway router in the case of any malfunction, so as to guarantee uninterrupted communication between the host and external network.

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



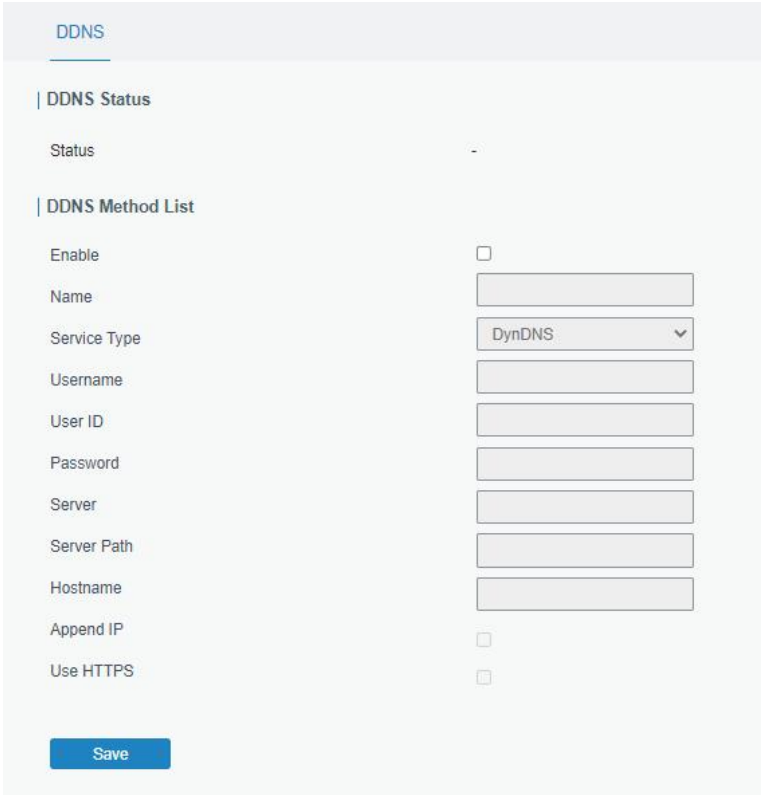
VRRP		
Item	**Description**	**Default**
Enable	Enable or disable VRRP.	Disable
Interface	Select the interface of Virtual Router.	None
Virtual Router ID	User-defined Virtual Router ID. Range: 1-255.	None
Virtual IP	Set the IP address of Virtual Router.	None
Priority	The VRRP priority range is 1-254 (a bigger number indicates a higher priority). The router with higher priority will be more likely to become the gateway router.	100
Advertisement Interval (s)	Heartbeat package transmission time interval between routers in the virtual ip group. Range: 1-255.	1
Preemption Mode	If the router works in the preemption mode, once it finds that its own priority is higher than that of the current gateway router, it will send VRRP notification package, resulting in re-election of gateway router and eventually replacing the original gateway router. Accordingly, the original gateway router will become a Backup router.	Disable
IPV4 Primary Server	The router will send ICMP packet to the IP address or hostn	8.8.8.8

	ame to determine whether the Internet connection is still av ailable or not.	
IPV4 Secondary Server	The router will try to ping the secondary server name if prim ary server is not available.	114.114. 114.114
Interval	Time interval (in seconds) between two Pings.	300
Retry Interval	Set the ping retry interval. When ping failed, the router will pi ng again every retry interval.	5
Timeout	The maximum amount of time the router will wait for a resp onse to a ping request. If it does not receive a response for the amount of time defined in this field, the ping request will be considered as failure.	3
Max Ping Retries	The retry times of the router sending ping request until dete rmining that the connection has failed.	3

5.2.9 DDNS

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

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



DDNS	
Item	**Description**
Enable	Enable/disable DDNS.
Name	Give the DDNS a descriptive name.

Interface	Set interface bundled with the DDNS.
Service Type	Select the DDNS service provider.
Username	Enter the username for DDNS register.
User ID	Enter User ID of the custom DDNS server.
Password	Enter the password for DDNS register.
Server	Enter the name of DDNS server.
Server Path	By default the hostname is appended to the path.
Hostname	Enter the hostname for DDNS.
Append IP	Append your current IP to the DDNS server update path.
Use HTTPS	Enable HTTPS for some DDNS providers.

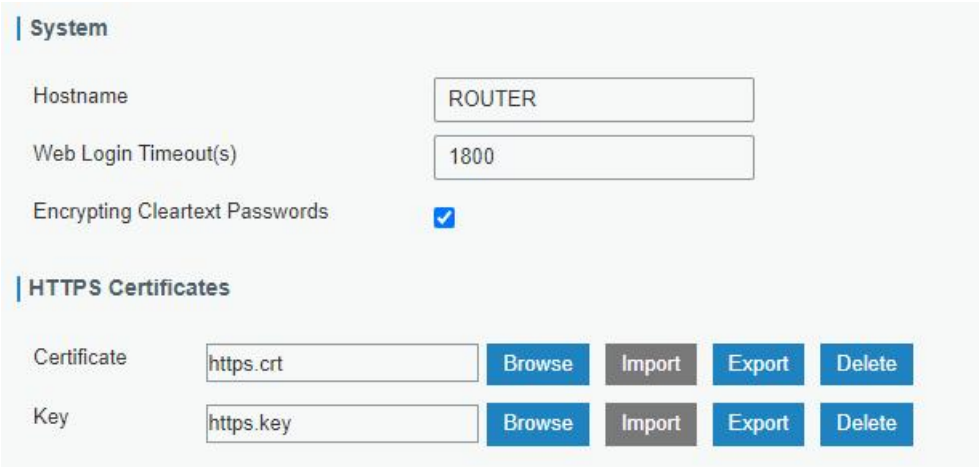
5.3 System

This section describes how to configure general settings, such as administration account, access service, system time, common user management, SNMP, AAA, event alarms, etc.

5.3.1 General Settings

5.3.1.1 General

General settings include system info and HTTPS certificates.



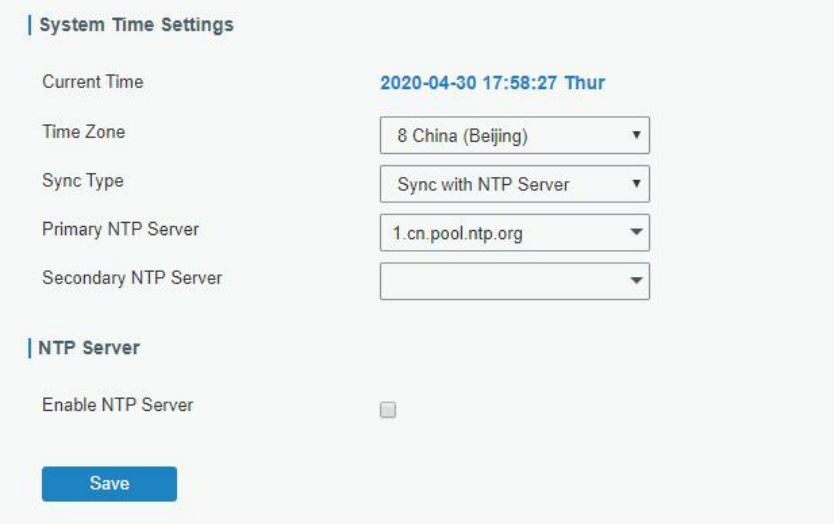
General		
Item	**Description**	**Default**
System		
Hostname	User-defined router name which should be start with a letter.	ROUTER
Web Login Timeout (s)	You need to log in again if it times out. Range: 100-3600.	1800
Encrypting Cleartext Passwords	This function will encrypt all of cleartext passwords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

	router. Clicking "Export" button will export the file to the PC. Clicking "Delete" button will delete the file.	
Key	Clicking "Browse" button, choose key file on the PC, and then click "Import" button to upload the file into router. Clicking "Export" button will export file to the PC. Click "Delete" button will delete the file.	--

5.3.1.2 System Time

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

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

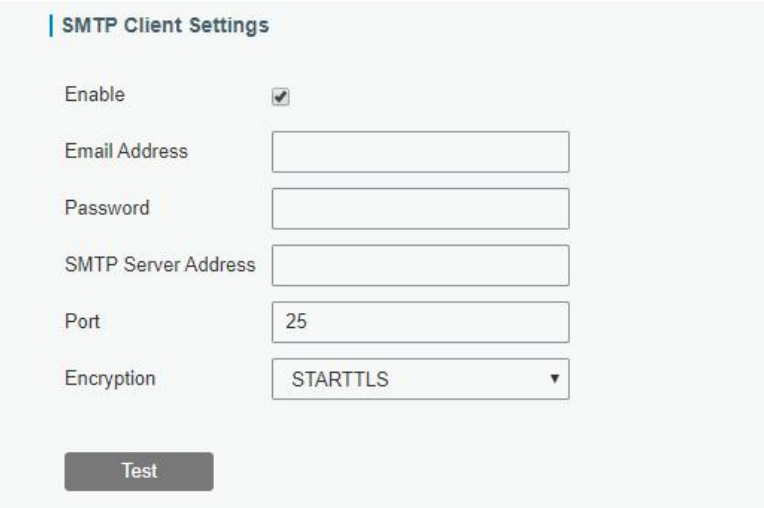


System Time	
Item	**Description**
Current Time	Show the current system time.
Time Zone	Click the drop down list to select the time zone you are in.
Sync Type	Click the drop down list to select the time synchronization type. **Sync with Browser:** Synchronize time with browser. **Sync with NTP Server:** Synchronize time with NTP Server. **Set up Manually:** configure the time manually. **GPS Time Synchronization:** Synchronize time with GPS per hour. This is only applicable with GPS version and ensure that GPS is enabled on **Service > GPS > GPS**.
Sync with Browser	Synchronize time with browser.
Browser Time	Show the current time of browser.
Set up Manually	Manually configure the system time.
GPS Time Synchronization	Synchronize time with GPS.
Primary NTP Server	Enter primary NTP Server's IP address or domain name.
Secondary NTP Server	Enter secondary NTP Server's IP address or domain name.
NTP Server	

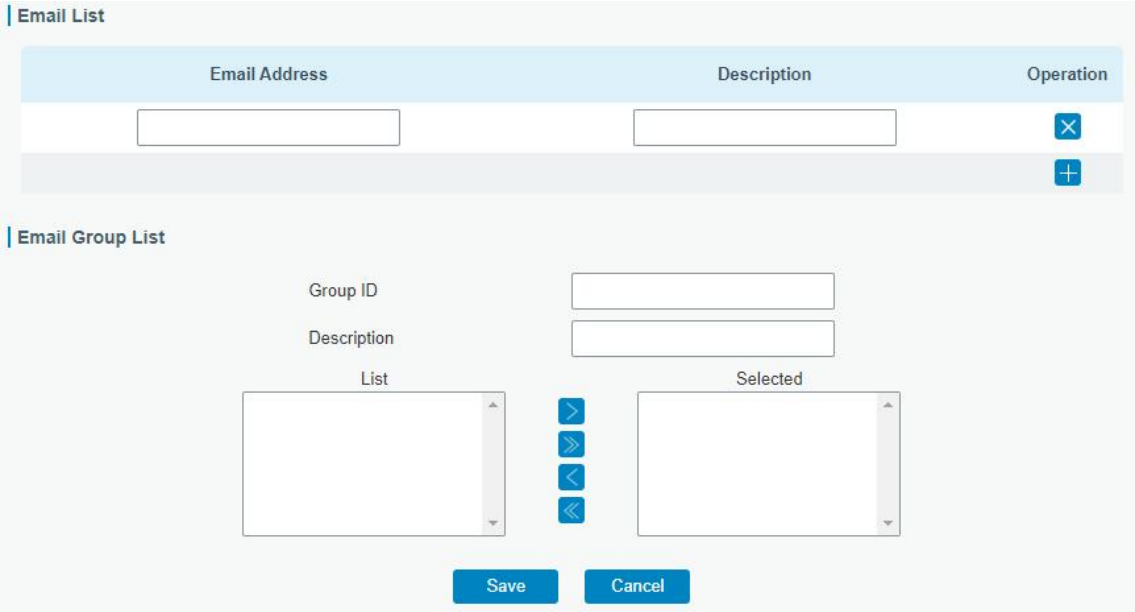
Enable NTP Server	NTP client on the network can achieve time synchronization with router after "Enable NTP Server" option is checked.

5.3.1.3 Email

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



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



Item	Description
Email List	
Email Address	Enter the Email address.
Description	The description of the Email address.
Email Group List	
Group ID	Set number for email group. Range: 1-100.
Description	The description of the Email group.
List	Show the Email address list.
Selected	Show the selected Email address.

Related Topics

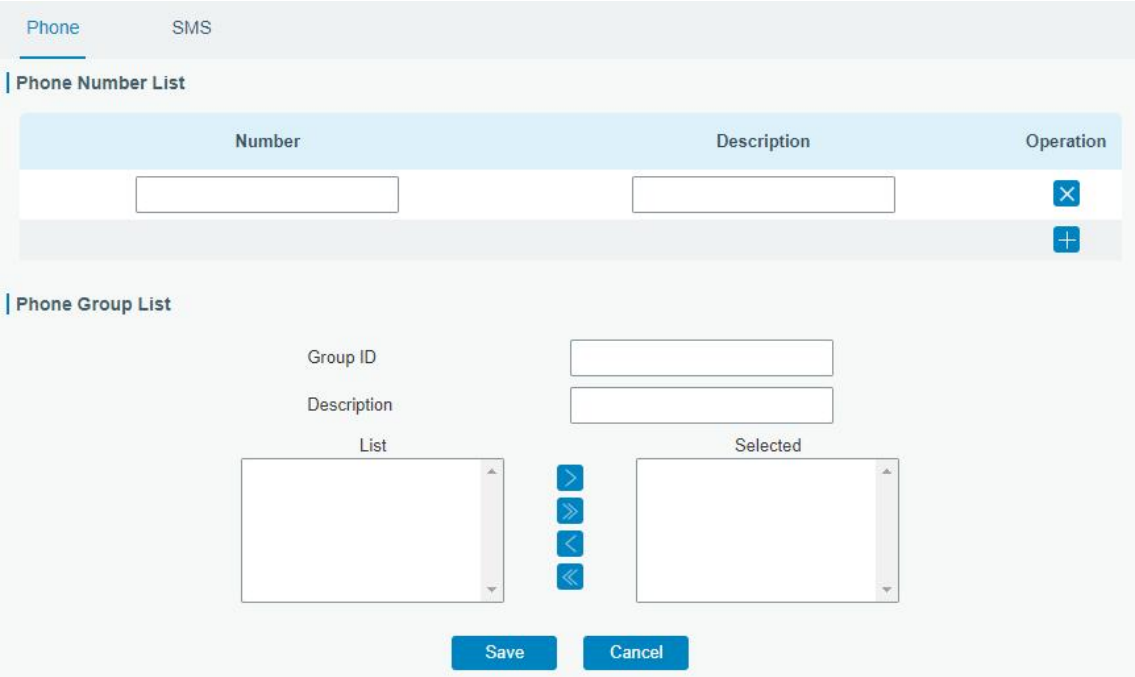
DI Setting

Events Setting

5.3.2 Phone&SMS

5.3.2.1 Phone

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



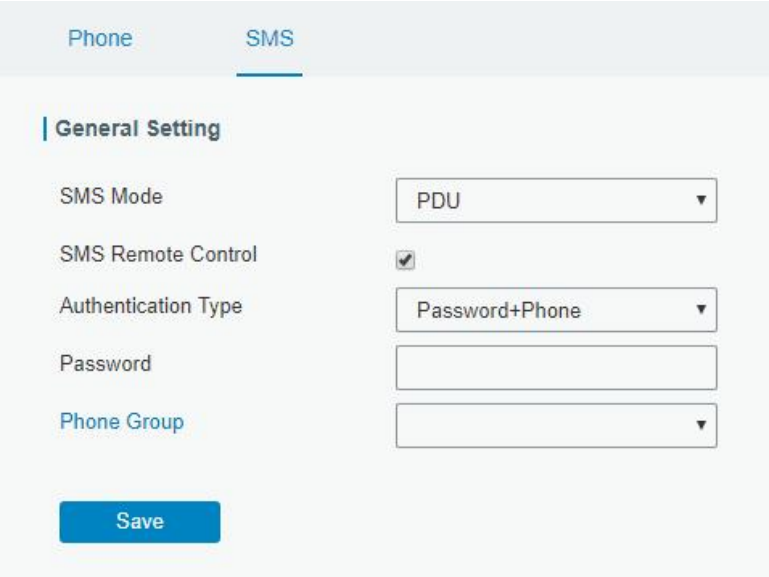
Phone	
Item	**Description**
Phone Number List	
Number	Enter the telephone number. Digits, "+" and "-" are allowed.
Description	The description of the telephone number.
Phone Group List	
Group ID	Set number for phone group. Range: 1-100.
Description	The description of the phone group.
List	Show the phone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

Related Topic

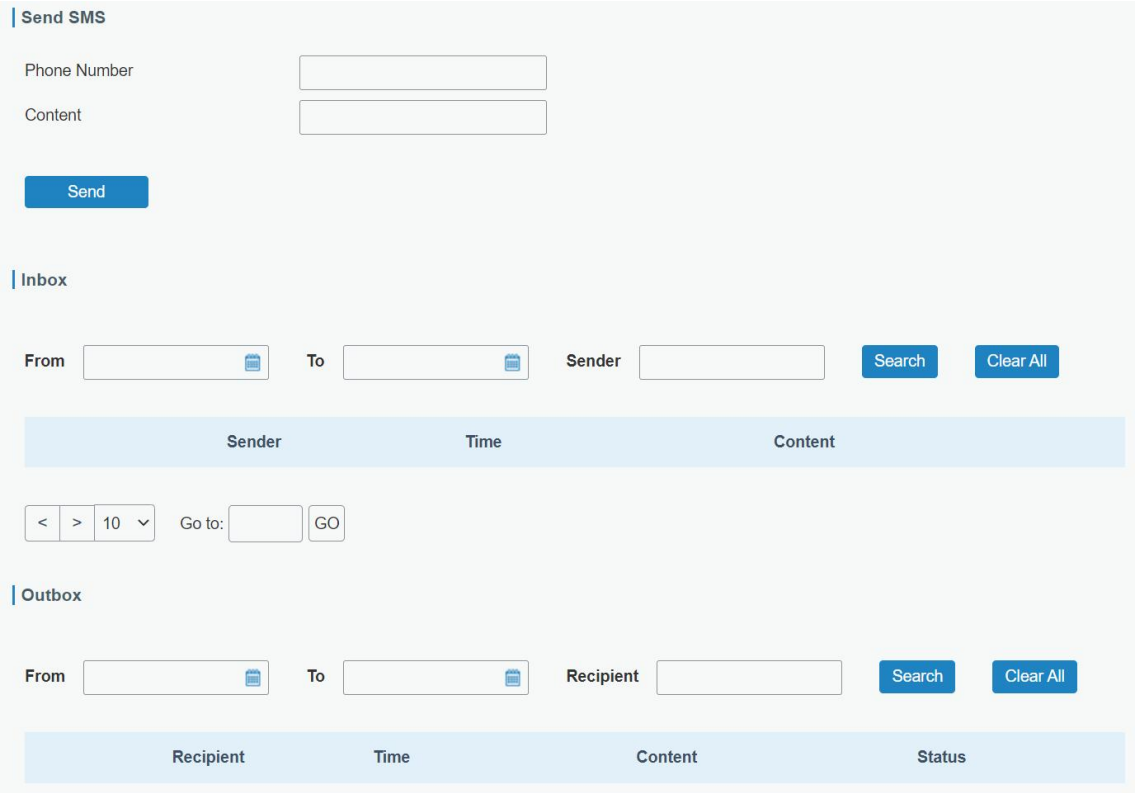
Connect on Demand

5.3.2.2 SMS

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



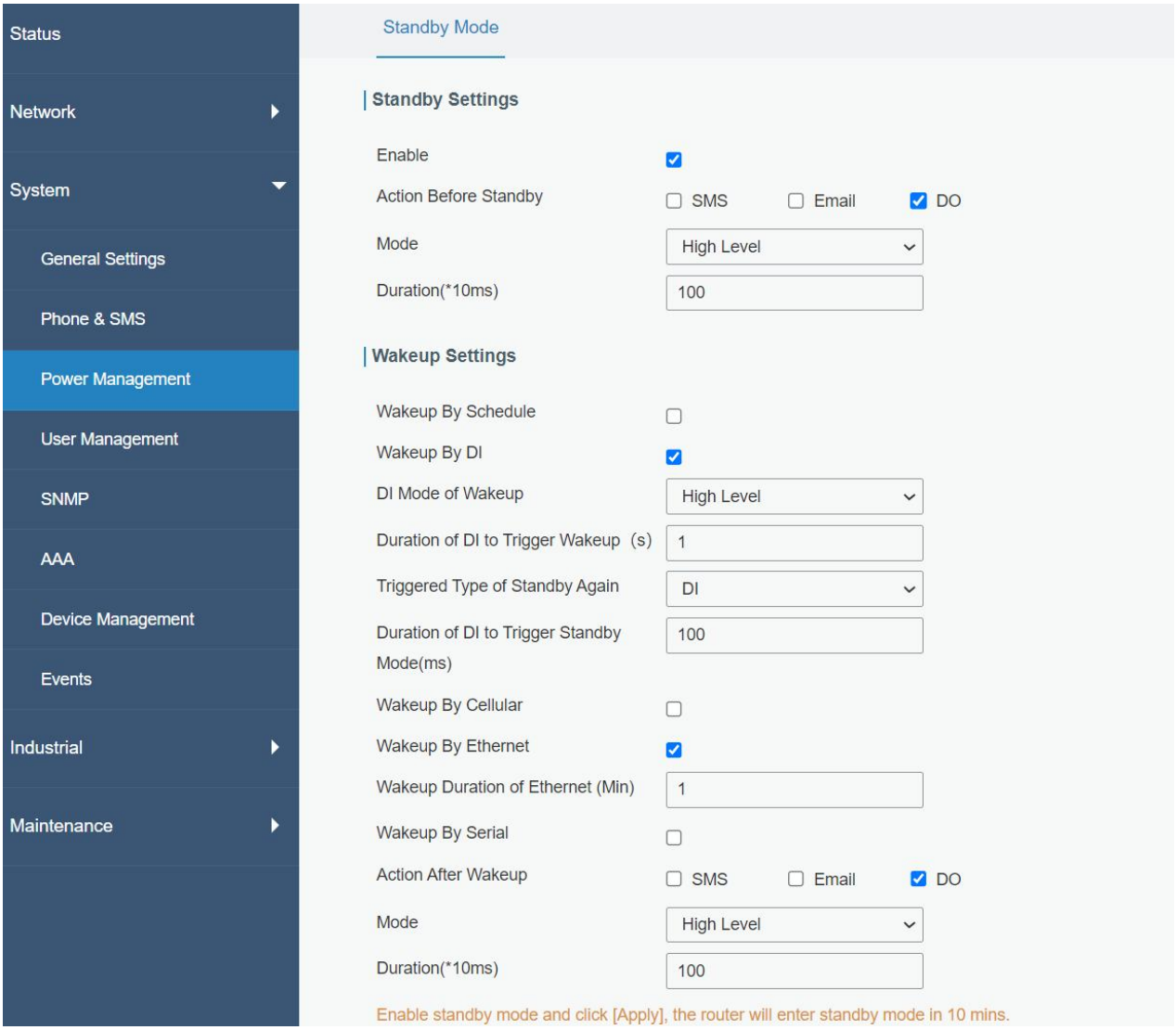
SMS Settings	
Item	**Description**
SMS Mode	Select SMS mode: **Text:** Pure text mode, mainly used in Europe and America. Technically, it can also be used to send Short Messages in Chinese. When CLI commands will be sent to control the router, Text mode is recommended to choose. **PDU:** It's the default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



SMS	
Item	**Description**
Send SMS	
Phone Number	Enter the number to receive the SMS.
Content	SMS content.
Inbox/Outbox	
Sender	SMS sender from outside.
Recipient	SMS recipient which UR41 send to.
From	Select the start date.
To	Select the end date.
Search	Search for SMS record.
Clear All	Clear all SMS records in web GUI.

5.3.3 Power Management

This section will describe how to setup standby settings and wakeup settings.



Standby Mode	
Item	**Description**
Standby Settings	
Enable	Enable or disable standby mode.
Action Before Standby	Set the action before the router enters the standby mode. If the settings is enabled, the router will execute the action before entering the standby mode.
SMS	Tick to enable SMS alarm before the router enters the standby mode.
Phone Group	Set phone number to receive SMS alarm.
SMS Content	Fill in the SMS alarm content.
Email	Tick to enable Email alarm before the router enters the standby mode.
Email Group	Set email address to receive email alarm.
Email Content	Fill in the email alarm content.
DO	Tick to enable DO before the router enters the standby

	mode.
Mode	Options include “High Level”, “Low Level”, and “pulse”.
Duration(*10ms)	Set the duration of high/low level in digital input.
Initial Status	Set initial state of DO when pulse mode is selected.
Duration of High Level	Set the duration of pulse’s high level.
Duration of Low Level	Set the duration of pulse’s low level.
The Number of Pulse	Set the quantity of pulse.
Wakeup Setting	
Wakeup By Schedule	If enabled, the router will be woken up periodically by the schedule when it is on standby mode.
Repeat Mode	Set the repeat mode as hour or day.
Repeat Frequency	Set the repeat frequency for schedule wakeup.
Wakeup Time	Set the time period for the router to wake up. In this time period, the router will be waken up and work. **Example:** current time is 0:30. when weakup time is set to 0:00 to 0:10, router will weak up during 1:00 to 1:10, 2:00 to 2:10 until repeat frequency reaches.
Wakeup By DI	If enabled, when the router is in standby mode and receives DI, the router will wake up from standby mode and turn to working mode.
DI Mode of Wakeup	Set the DI mode to wake up router from standby mode.
Duration of DI to Trigger Wakeup	Set the DI duration to wake up router from standby mode.
Triggered Type of Standby Again	Set the trigger type to trigger the router to enter standby mode again after being woken up by DI. **DI**: when router receives a DI signal which is opposite to “DI Mode of Wakeup” and satisfies the “DI Duration of Standby”, the router will enter standby mode immediately. **Time**: the router will enter the standby mode again after reaching the wake-up duration.
DI Duration of Standby	Set the DI duration for the router to enter standby mode again after being woken up by DI.
Wakeup Duration of DI	Set the duration of entering standby mode again after the router is woken up by DI from standby mode to operation mode.
Wakeup By Cellular	The router will be woken up when cellular receives SMS or call and switch from standby mode to working mode. Ensure that the router has registered to cellular network before standby.
Call Group	Select a call group for cellular wakeup. Go to “System > Phone & SMS > Phone” to set up the phone group.
SMS Group	Select a SMS group for cellular wakeup. Go to “System > Phone & SMS > Phone” to set up the phone group.
SMS Text	Fill in the SMS content for wakeup.

Wakeup Duration of Cellular	Set the duration of entering standby mode again after the router is woken up by cellular.
Wakeup By Ethernet	The router will be woken up when Ethernet interface receives a special frame (E8:E8:B7:07:FB:BD).
Wakeup Duration of Ethernet	Set the duration of entering standby mode again after the router is woken up by Ethernet.
Wakeup By Serial	The router will be woken up when serial port receives a 1-byte data packet. **Note:** the serial device need to send 1-byte wake-up data before sending normal data.
Wakeup Duration of Serial	Set the duration of entering standby mode again after the router is woken up by serial.
Action After Wakeup	Set the action after the router wakes up.
SMS	Enable SMS alarm after the router wakes up.
Email	Enable Email alarm after the router wakes up.
DO	Enable to trigger DO after the router wakes up.

Note:

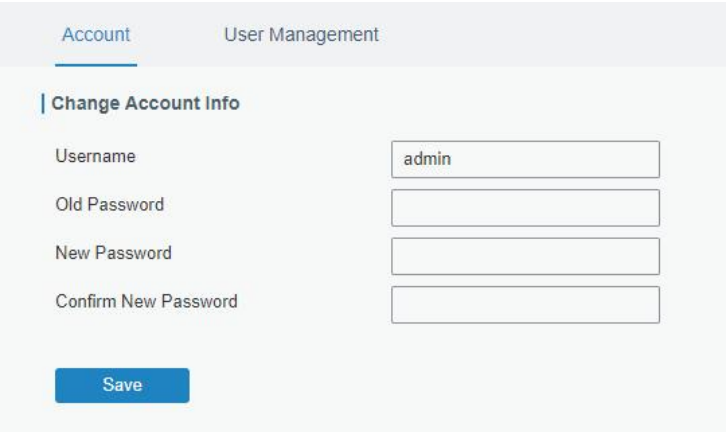
1. When standby mode is enabled, press and hold on reset button for 3s to weak up router for 1 hour.
2. If multiple weakup conditions are enabled, the router will only execute the maximum weakup duration.

5.3.4 User Management

5.3.4.1 Account

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

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

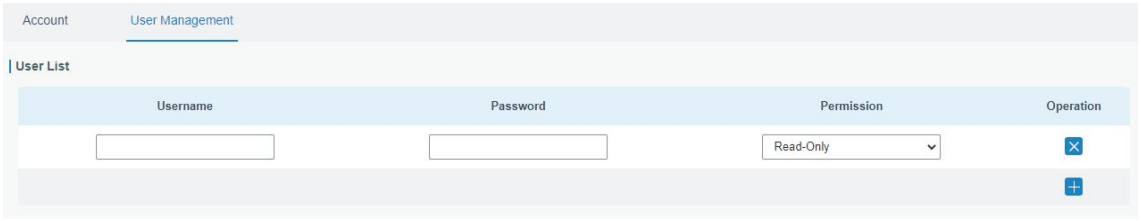


Account	
Item	**Description**
Username	Enter a new username. You can use characters such as a-z, 0-9, "_", "-". The first character can't be a digit.
Old Password	Enter the old password.
New Password	Enter a new password.

Confirm New Password	Enter the new password again.

5.3.4.2 User Management

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



User Management	
Item	**Description**
Username	Enter a new username. Only lowercase letters, digits, "_", "-" are allowed. The first character can't be a digit.
Password	Set password.
Permission	Select user permission from “Read-Only” and “Read-Write”. **Read-Only:** users can only view the configuration of router in this level. **Read-Write:** users can view and set the configuration of router in this level.

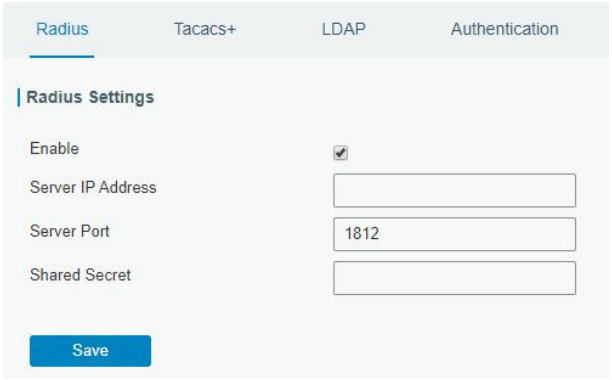
5.3.5 AAA

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

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

5.3.5.1 Radius

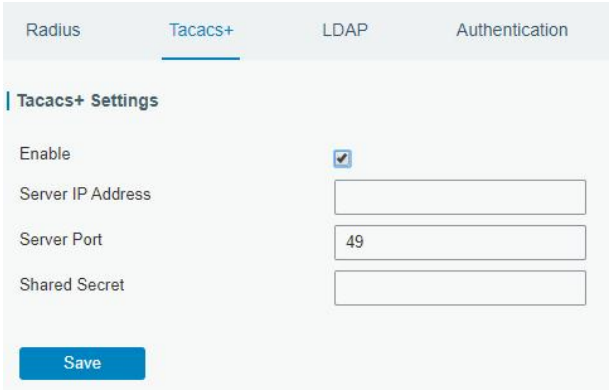
Using UDP for its transport, Radius is generally applied in various network environments with higher requirements of security and permission of remote user access.



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

5.3.5.2 TACACS+

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

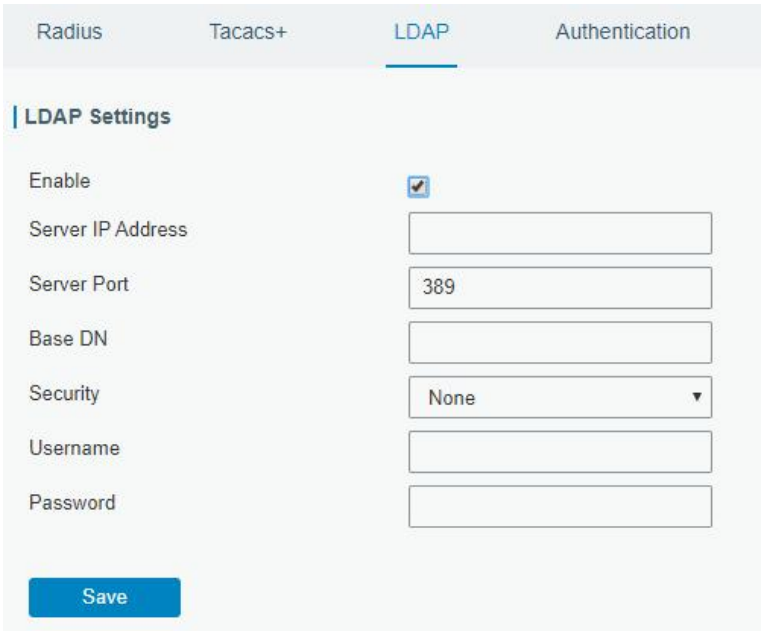


TACACS+	
Item	**Description**
Enable	Enable or disable TACACS+.
Server IP Address	Fill in the TACACS+ server IP address/domain name.
Server Port	Fill in the TACACS+ server port. Range: 1-65535.
Key	Fill in the key consistent with that of TACACS+ server in order to get connected with TACACS+ server.

5.3.5.3 LDAP

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

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



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

5.3.5.4 Authentication

AAA supports the following authentication ways:

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

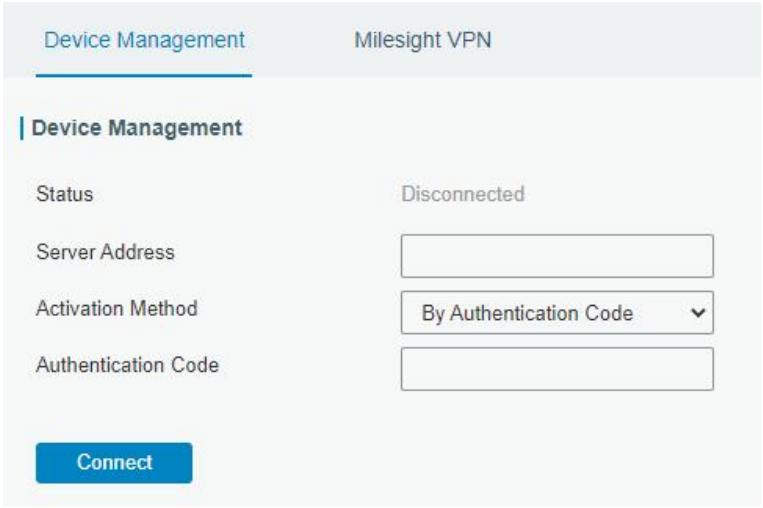
When radius, TACACS+, and local are configured at the same time, the priority level is: 1 >2 >3.

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

5.3.6 Device Management

5.3.6.1 DeviceHub

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

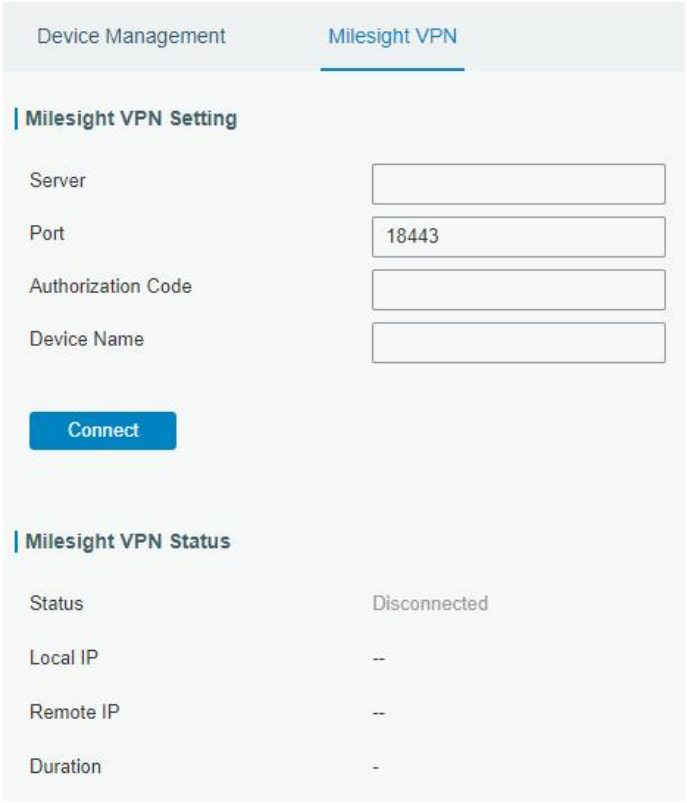


DeviceHub	
Item	**Description**
Status	Show the connection status between the router and the DeviceHub.
Disconnected	Click this button to disconnect the router from the DeviceHub.

Server Address	IP address or domain of the device management server.
Activation Method	Select activation method to connect the router to the DeviceHub server, options are "By Authentication Code" and "By Account name".
Authentication Code	Fill in the authentication code generated from the DeviceHub.
Account name	Fill in the registered DeviceHub account (email) and password.
Password	

5.3.6.2 Milesight VPN

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



Milesight VPN	
Item	**Description**
Milesight VPN Settings	
Server	Enter the IP address or domain name of Milesight VPN.
Port	Enter the HTTPS port number.
Authorization code	Enter the authorization code which generated by Milesight VPN.
Device Name	Enter the name of the device.
Milesight VPN Status	
Status	Show the connection information about whether the router is connected to the Milesight VPN.
Local IP	Show the virtual IP of the router.

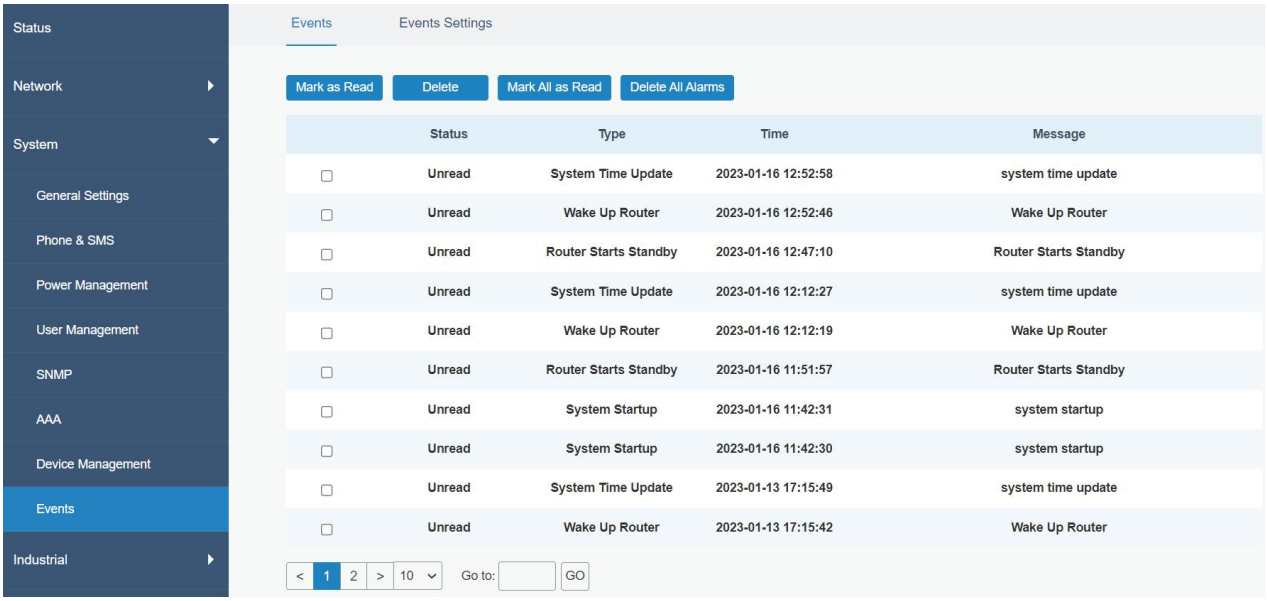
Remote IP	Show the virtual IP of the Milesight VPN.
Duration	Show the information on how long the router has been connected to the Milesight VPN.

5.3.7 Events

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

5.3.7.1 Events

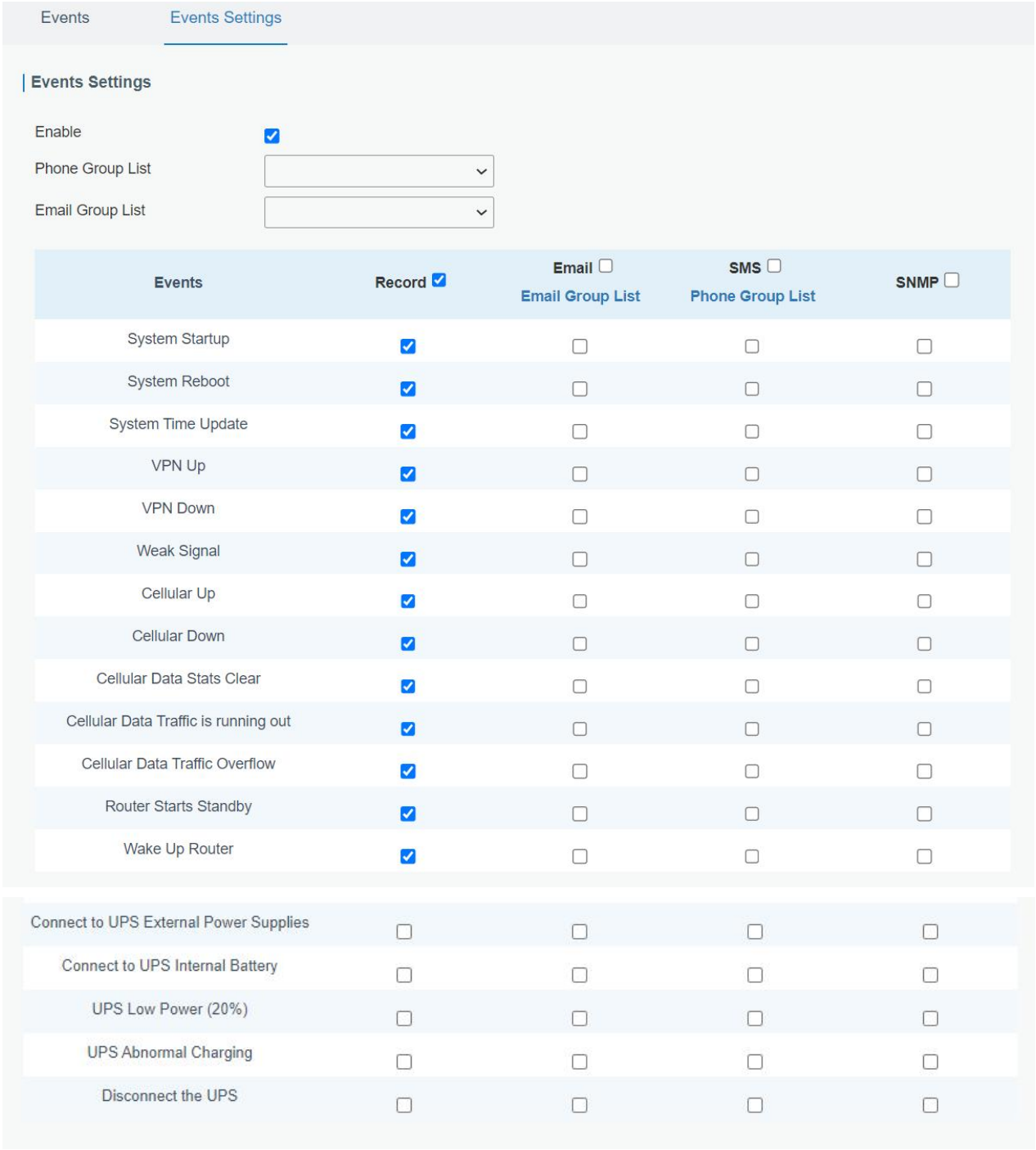
You can view alarm messages on this page.



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

5.3.7.2 Events Settings

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



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

Email Setting	Click and you will be redirected to the page **Email** to configure email group list.
SNMP	The relevant content of event alarm will be sent out via SNMP Trap if this option is checked.
SMS	The relevant content of event alarm will be sent out via SMS if this option is checked.
SMS Setting	Click and you will be redirected to the page of **Phone** to configure phone group list.

Related Topics

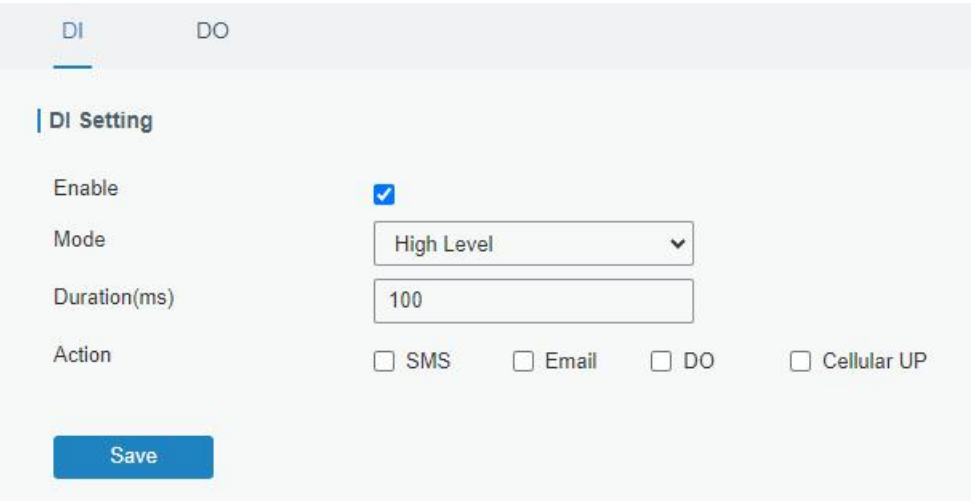
Email Setting

5.4 Service

5.4.1 I/O

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

Action	Select the corresponding actions that the system will take when digital input mode meets the preset condition or duration. **SMS:** enable to send SMS alarms. **Email:** enable to send Email alarms. **DO:** control the DO status as settings on **Service > I/O > DO** page. **Cellular UP:** Trigger the router to switch from offline to register to cellular network.

Related Topics

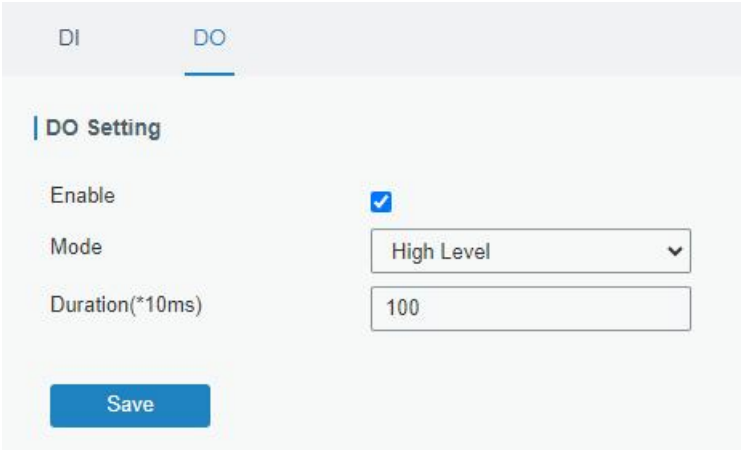
DO Setting

Email Setting

Connect on Demand

5.4.1.2 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. **Pulse:** trigger the DO to send pulses. **Custom:** trigger the DO via SMS on the phone group.
Initial Status	Select the initial status of DO when mode is Custom or Pulse. It is also the initial status when the router restarts.
Duration (*10ms)	When mode is high level or low level, set duration of high/low level on digital output. Range: 1-10000.
Duration of High Level (*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.

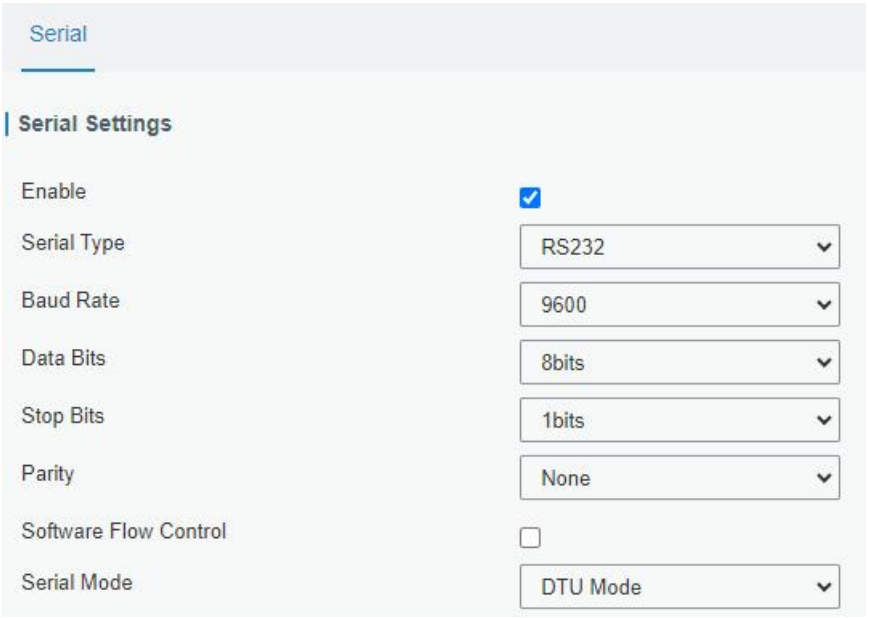
Phone Group	Select phone group which will be used for I/O configuration. User can click the Phone Group and set phone number.

Related Topics

DI Setting

5.4.2 Serial Port

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



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

	Modbus Client: go to **Service > Modbus Client** to configure basic parameters and channels. **Modbus Server:** go to **Service > Modbus Server** to configure basic parameters.

DTU Mode		
Item	**Description**	**Default**
DTU Protocol	Select from below protocols: **Transparent:** the router is used as TCP/UDP client and transmits data to server transparently. **TCP server:** the router is used as TCP server to wait for polling data. **UDP server:** the router is used as UDP server to wait for polling data. **Modbus:** the router will be used as Modbus gateway, which can achieve conversion between Modbus RTU and Modbus TCP. **MQTT:** the router will be used as MQTT client to send data to MQTT broker.	--
TCP/UDP Server		
Listening port	Set the router listening port. Range: 1-65535.	502
Keepalive Interval	After TCP connection is established, client will send heartbeat packet regularly by TCP to keep alive. The interval range is 1-3600s.	75
Keepalive Retry Times	When TCP heartbeat times out, router will resend heartbeat. After it reaches the preset retry times, TCP connection will be reestablished. The retry times range is 1-16.	9
Packet Size	Set the size of the serial data frame. Packet will be sent out when preset frame size is reached. The size range is 1-1024 bytes.	1024
Serial Frame Interval	The interval that the router sends out real serial data stored in the buffer area to public network. The range is 10-65535 ms. **Note:** data will be sent out to public network when real serial data size reaches the preset packet size, even though it's within the serial	100

	frame interval.	
Item	**Description**	**Default**
Transparent		
Protocol	Select TCP or UDP protocol.	TCP
Keepalive Interval (s)	After TCP client is connected with TCP server, the client will send heartbeat packet by TCP regularly to keep alive. The interval range is 1-3600s.	75
Keepalive Retry Times	When TCP heartbeat times out, the router will resend heartbeat. After it reaches the preset retry times, router will reconnect to TCP server. The range is 1-16.	9
Packet Size	Set the size of the serial data frame. Packet will be sent out when preset frame size is reached. The range is 1-1024 bytes.	1024
Serial Frame Interval	The interval that the router sends out real serial data stored in the buffer area to public network. The range is 10-65535 ms. **Note:** data will be sent out to public network when real serial data size reaches the preset packet size, even though it's within the serial frame interval.	100
Reconnect Interval	After connection failure, router will reconnect to the server at the preset interval, in seconds. The range is 10-60s.	10
Specific Protocol	By Specific Protocol, the router will be able to connect to the TCP2COM software.	--
Heartbeat Interval	By Specific Protocol, the router will send heartbeat packet to the server regularly to keep alive. The interval range is 1-3600s.	30
ID	Define unique ID of each router. No longer than 63 characters without space character.	--
Register String	Define register string for connection with the server.	Null
Server Address	Fill in the TCP or UDP server address (IP/domain name).	Null
Server Port	Fill in the TCP or UDP server port. Range: 1-65535.	Null
Status	Show the connection status between the router and the server.	--
Modbus		
Local Port	Set the router listening port. Range: 1-65535.	502
Maximum TCP Clients	Specify the maximum number of TCP clients allowed to connect the router which act as a TCP server.	32
Connection Timeout	If the TCP server does not receive any data from the slave device wit hin the connection timeout period, the TCP connection will be broken .	60
Reading 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, t he device will restart the new read cycle after all channels have been read.	100
Response Timeout	Set the maximum response time that the router waits for the respon se to the command. If the device does not get a response after the maximum response time, it's determined that the command has tim ed out.	3000

Maximum Retries	Set the maximum retry times after it fails to read.	3
MQTT		
Packet Size	Set the size of the serial data frame. Packet will be sent out when preset frame size is reached. The range is 1-1024 bytes.	1024
Serial Frame Interval	The interval that the router sends out real serial data stored in the buffer area to public network. The range is 10-65535 ms. **Note:** data will be sent out to public network when real serial data size reaches the preset packet size, even though it's within the serial frame interval.	100
MQTT Connection	Select the MQTT connection to send serial port data, it's set up on **Service > MQTT** page.	Null
Topic	Topic name used for publishing serial port data.	Null
Retain	Enable to set the latest message of this topic as retain message.	Null
QoS	QoS0, QoS1 or QoS2 are optional.	Null

Related Configuration Example

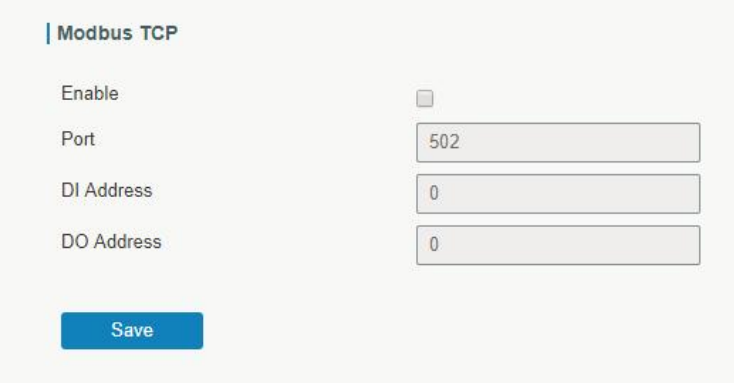
DTU Application Example

5.4.3 Modbus Server (Slave)

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

5.4.3.1 Modbus TCP

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



Modbus TCP		
Item	**Description**	**Default**
Enable	Enable/disable Modbus TCP.	Disable
Port	Set the router listening port. Range: 1-65535.	502

DI Address	Define the address of DI, range: 0-255.	0
DO Address	Define the address of DO, range: 0, 2-255.	0

5.4.3.2 Modbus RTU

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

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

5.4.3.3 Modbus RTU Over TCP

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

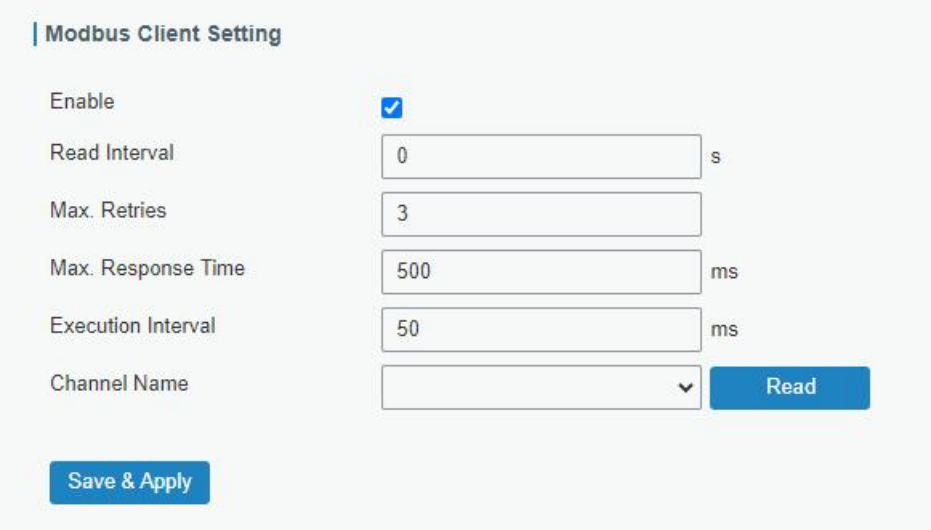
Modbus RTU Over TCP		
Item	**Description**	**Default**

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

5.4.4 Modbus Client (Master)

UR41 router can be set as Modbus Client to poll the remote Modbus Server and send alarm according to the response.

5.4.4.1 Modbus Client

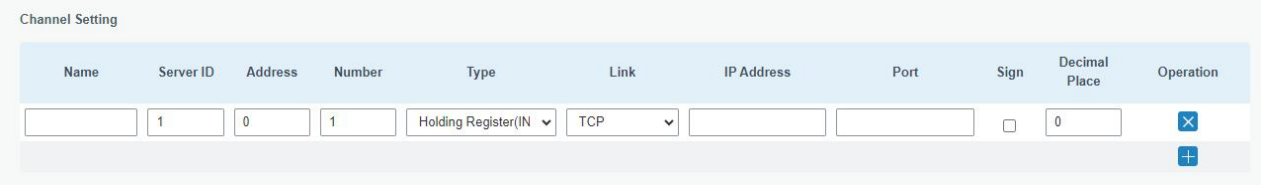


Modbus Master		
Item	**Description**	**Default**
Enable	Enable/disable Modbus client.	--
Read Interval/s	Set the interval for reading remote channels. When the read cycle ends, the commands which haven't been sent out will be discard, and the new read cycle begins. If it is set to 0, the device will restart the new read cycle after all channels have been read. Range: 0-600.	0
Max. Retries	Set the maximum retry times after it fails to read, range: 0-5.	3
Max.	Set the maximum response time that the router waits for the	500

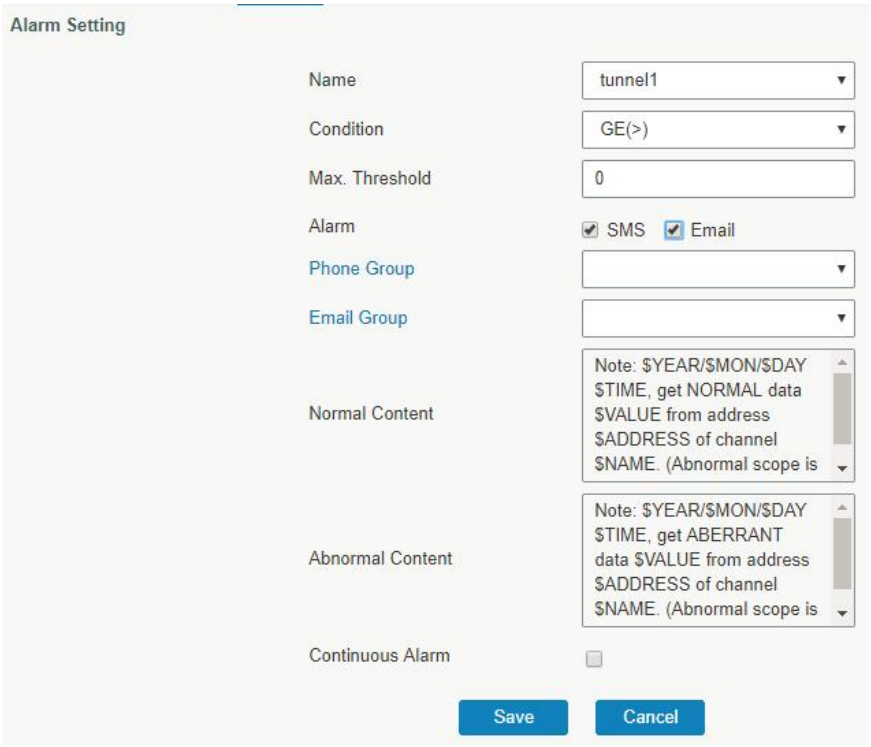
Response Time/ms	response to the command. If the device does not get a response after the maximum response time, it's determined that the command has timed out. Range: 10-1000.	
Execution Interval/ms	The execution interval between each command. Range: 10-1000.	50
Channel Name	Select a readable channel form the channel list.	--
Result	The value read from the selected channel.	--

5.4.4.2 Channel

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

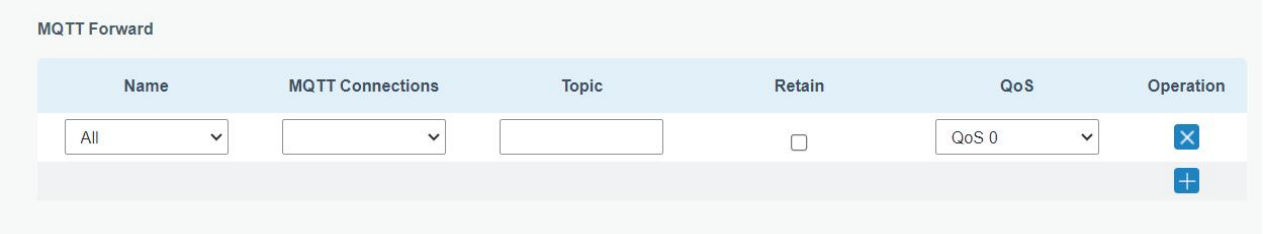


Channel Setting	
Item	**Description**
Name	Set the name to identify the remote channel. It cannot be blank.
Server ID	Set Modbus server ID.
Address	The starting address for reading.
Number	The address number for reading.
Type	Read command data type, options are Coil, Discrete, Holding Register (INT16), Input Register (INT16), Holding Register (INT32) and Holding Register (Float).
Link	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.
IP address	When link is TCP, fill in the IP address of the remote Modbus TCP device.
Port	When link is TCP, fill in the port of the remote Modbus TCP device.
Sign	When type is holding register or input register, enable or disable to identify whether this channel is signed.
Decimal Place	When type is holding register or input register, indicate a dot in the read into the position of the channel. For example: read the channel value is 1234 and a Decimal Place is equal to 2, then the actual value is 12.34.



Alarm Setting	
Item	**Description**
Name	Set the same name with the channel name to identify the remote channel.
Condition	The condition that triggers alert.
Min. Threshold	Set the min. value to trigger the alert. When the actual value is less than this value, the alarm will be triggered.
Max. Threshold	Set the max. value to trigger the alert. When the actual value is more than this value, the alarm will be triggered.
Alarm	Select the alarm method, e.g SMS.
SMS	The preset alarm content will be sent to the specified phone number.
Phone Group	Select the phone group to receive the alarm SMS.
Email Group	Select the Email group to receive the alarm Email.
Normal Content	When the actual value is restored to the normal value from exceeding the threshold value, the router will automatically cancel the abnormal alarm and send the preset normal content to the specified phone group.
Abnormal Content	When the actual value exceeds the preset threshold, the router will automatically trigger the alarm and send the preset abnormal content to the specified phone group.
Continuous Alarm	Once it is enabled, the same alarm will be continuously reported. Otherwise, the same alarm will be reported only one time.

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



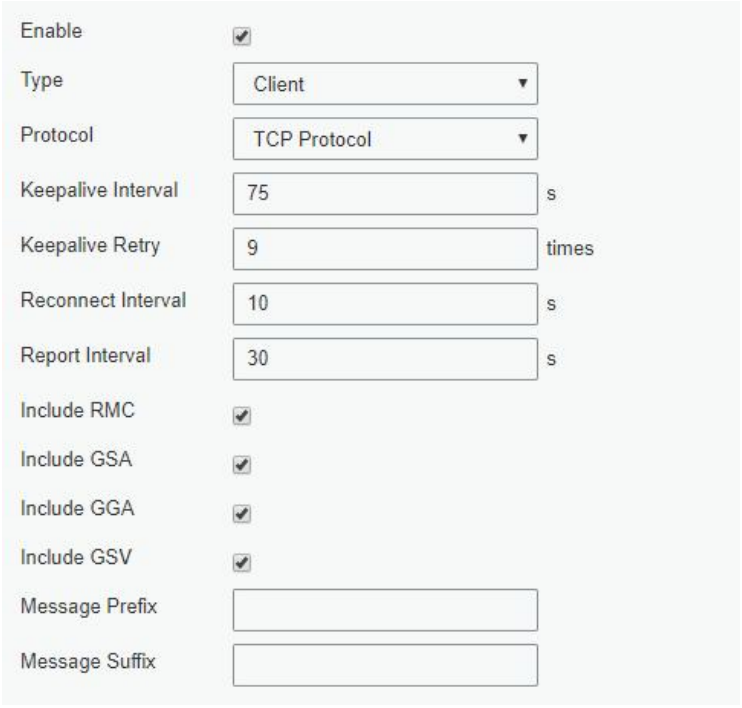
MQTT Forward	
Item	**Description**
Name	The name of Modbus Client's channel.
MQTT Connections	Select the MQTT connection to send Modbus channel data, it's set up on **Service > MQTT** page.
Topic	Topic name used for publishing Modbus channel data.
Retain	Enable to set the latest message of this topic as retain message.
QoS	QoS0, QoS1 or QoS2 are optional.

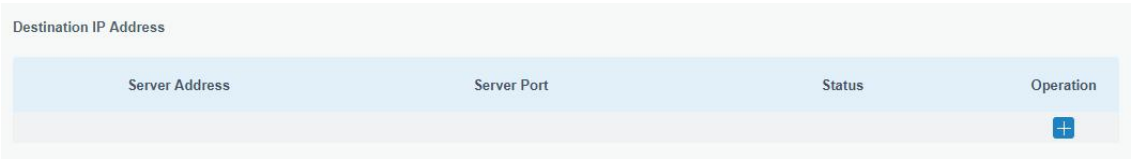
5.4.5 GPS

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

5.4.5.1 GPS IP Forwarding

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



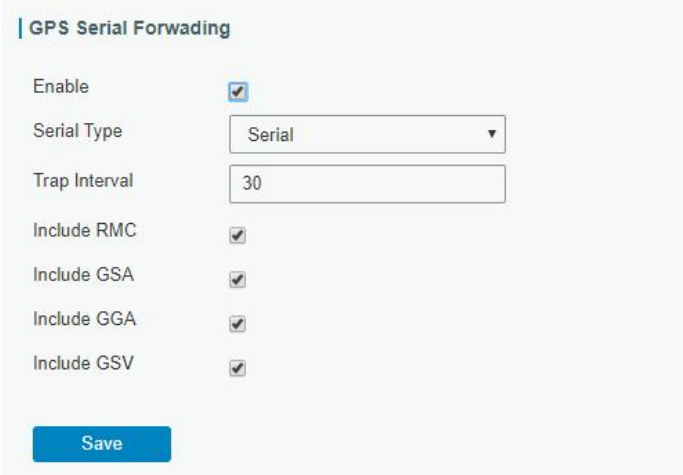


GPS IP Forwarding		
Item	**Description**	**Default**
Enable	Forward the GPS data to the client or server.	Disable
Type	Select connection type of the router as Client or Server.	Client
Protocol	Select protocol of data transmission as TCP or UDP.	TCP
Keepalive Interval	After it's connected with server/client, the router will send heartbeat packet regularly to the server/client to keep alive. The interval range is 1-3600s.	75
Keepalive Retry	When TCP heartbeat times out, the router will resend heartbeat. After it reaches the preset retry times, router will reconnect to TCP server. The range is 1-16.	9
Local Port	Set the router listening port. Range: 1-65535.	
Reconnect Interval	After connection failure, router will reconnect to the server at the preset interval. The range is 10-60s.	10
Report Interval	Router will send GPS data to the server/client at the preset interval. The range is 1-60s.	30
Include RMC	RMC includes time, date, position, course and speed data.	--
Include GSA	GSA includes GPS receiver operating mode, satellites used in the position solution, and DOP values.	--
Include GGA	GGA includes time, position and fix type data.	--
Include GSV	GSV includes the number, elevation, azimuth of GPS satellites and SNR values.	--
Message	Add a prefix to the GPS data.	Null

Prefix		
Message Suffix	Add a suffix to the GPS data.	Null
Destination IP Address		
Server Address	Fill in the server address to receive GPS data (IP/domain name).	--
Server Port	Fill in the port to receive GPS data. Range: 1-65535.	--
Status	Show the connection status between the router and the server.	--

5.4.5.2 GPS Serial Forwarding

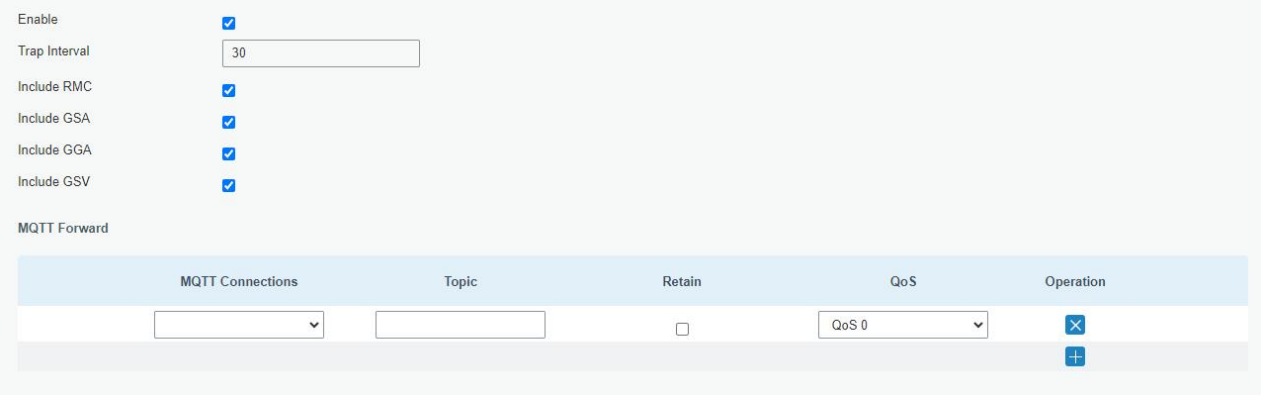
GPS IP forwarding means that GPS data can be forwarded to the serial port.



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

5.4.5.3 GPS MQTT Forward

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



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

5.4.6 MQTT

UR41 supports to work as MQTT client to forward data and router information to MQTT broker in two ways:

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

Figure 3-4-6-1

MQTT

Status

Status	Disable

General

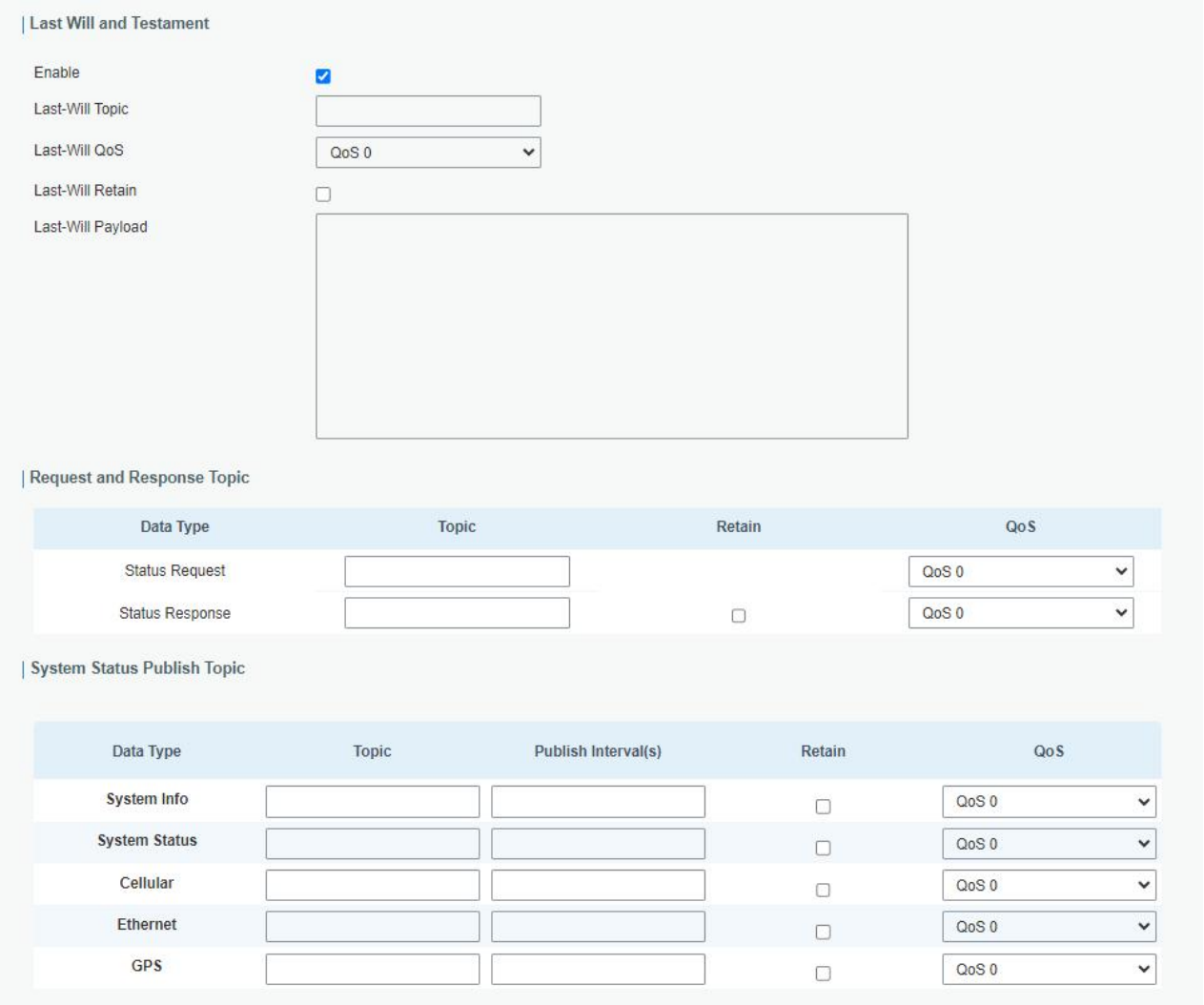
Name	
Enable	☑
Broker Address	
Broker Port	1883
Client ID	24:e1:24:f2:63:10_linyptjr
Connection Timeout(s)	30
Keep Alive Interval(s)	60
Auto Reconnect	☑
Reconnect Period	4
Clean Session	☐

User Credentials

Enable	☑
Username	
Password	

TLS

Enable	☑
Mode	CA signed server certificate



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

Reconnect Period	When connection is broken, the period to reconnect the server periodically.
Clean Session	When enabled, the connection will create a temporary session and all information will lose when the client is disconnected from broker; when disabled, the connection will create a persistent session that will remain and save offline messages until the session logs out overtime.
User Credentials	
Enable	Enable user credentials.
Username	The username used for connecting to the MQTT broker.
Password	The password used for connecting to the MQTT broker.
TLS	
Enable	Enable the TLS encryption in MQTT communication.
Mode	Select from Self signed certificates, CA signed server certificate. **CA signed server certificate:** verify with the certificate issued by Certificate Authority (CA) that pre-loaded on the device. **Self signed certificates:** upload the custom CA certificates, client certificates and secret key for verification.
Last Will and Testament	
Enable	Last will message is automatically sent when the MQTT client is abnormally disconnected. It is usually used to send device status information or inform other devices or proxy servers of the device's offline status.
Last-Will Topic	Customize the topic to receive last will messages.
Last-Will QoS	QoS0, QoS1 or QoS2 are optional.
Last-Will Retain	Enable to set last will message as retain message.
Last-Will Payload	Customize the last will message contents.
Request and Response Topic	
Topic	The router supports to send requests to enquire router information. **Status Request:** users is able to send requests to this topic to enquire router information. Request format: *{* *"id":"1",* *"status":"systeminfo"* *}* The id is a random value, and the status can be set as 5 types: systeminfo, systemstatus, cellular, ethernet, gps. **Status Response:** users is able to subscribe this topic to get the replies.
Retain	Enable to set the latest message of this topic as retain message.
QoS	QoS0, QoS1 or QoS2 are optional.
System Status Publish Topic	
Data Type	Data type sent to MQTT broker automatically. Note that the GPS in this page is not raw data but decoded location data.
Topic	Topic name of the data type used for publishing.

Publish Interval (s)	The interval to publish data to MQTT broker automatically.
Retain	Enable to set the latest message of this topic as retain message.
QoS	QoS0, QoS1 or QoS2 are optional.

5.4.7 SNMP

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

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

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

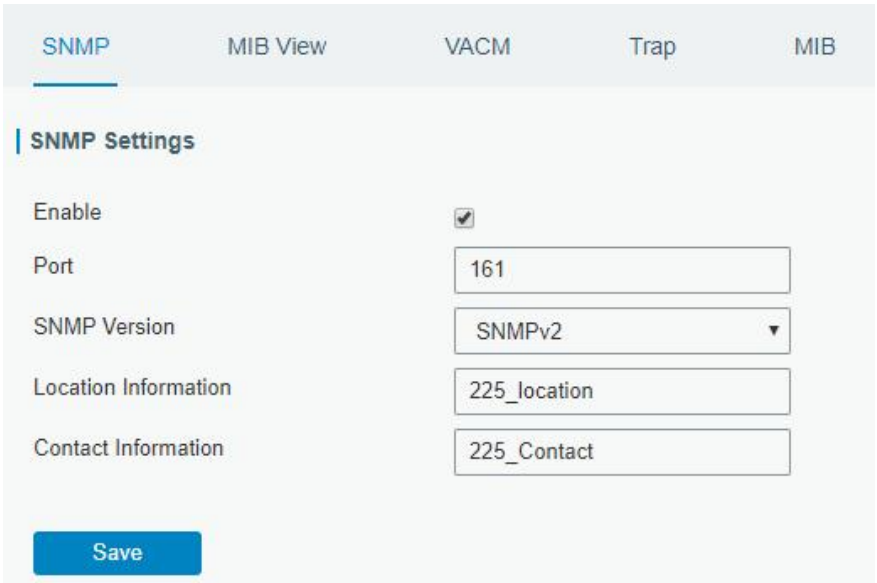
1. Enable SNMP setting.
2. Download MIB file and load it into NMS.
3. Configure MIB View.
4. Configure VCAM.

Related Configuration Example

SNMP Application Example

5.4.7.1 SNMP

UR41 supports SNMPv1, SNMPv2c and SNMPv3 version. SNMPv1 and SNMPv2c employ community name authentication. SNMPv3 employs authentication encryption by username and password.

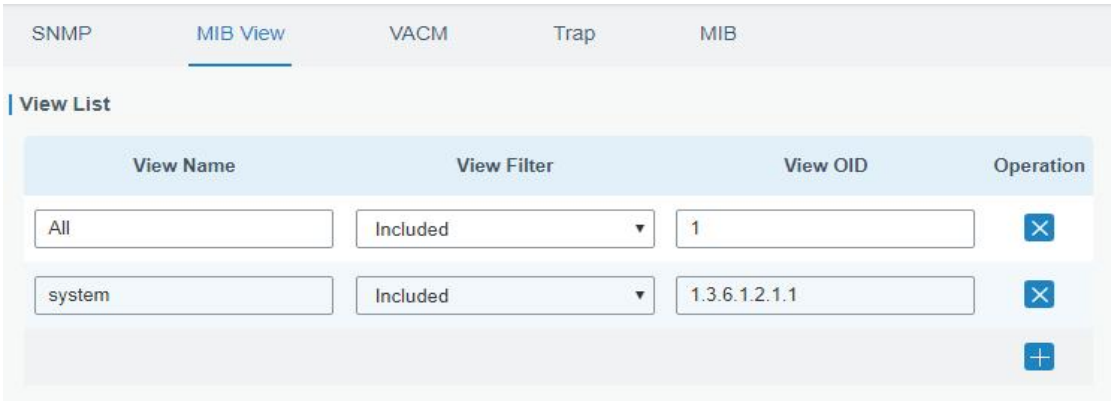


SNMP Settings	
Item	**Description**
Enable	Enable or disable SNMP function.

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

5.4.7.2 MIB View

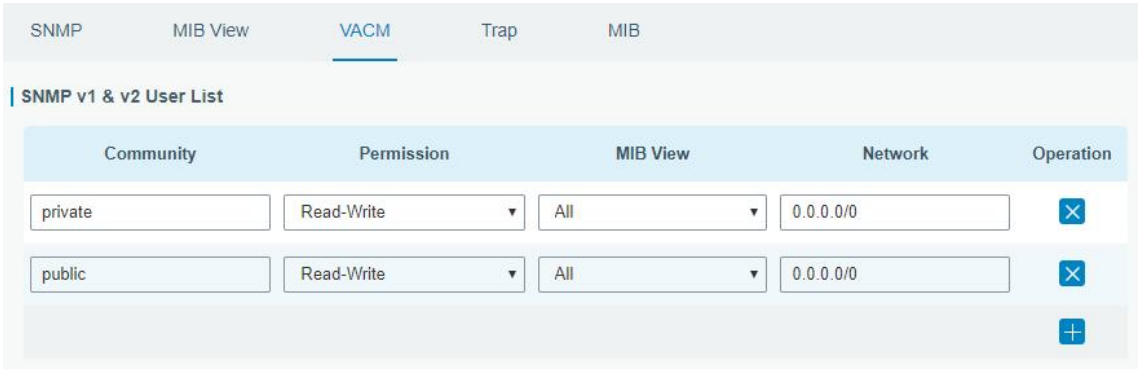
This section explains how to configure MIB view for the objects.



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

5.4.7.3 VACM

This section describes how to configure VCAM parameters.



VACM	
Item	**Description**
SNMP v1 & v2 User List	
Community	Set the community name.
Permission	Select from "Read-Only" and "Read-Write".

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

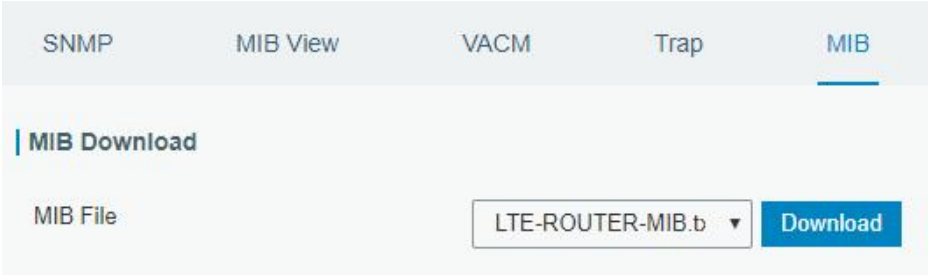
5.4.7.4 Trap

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

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

5.4.7.5 MIB

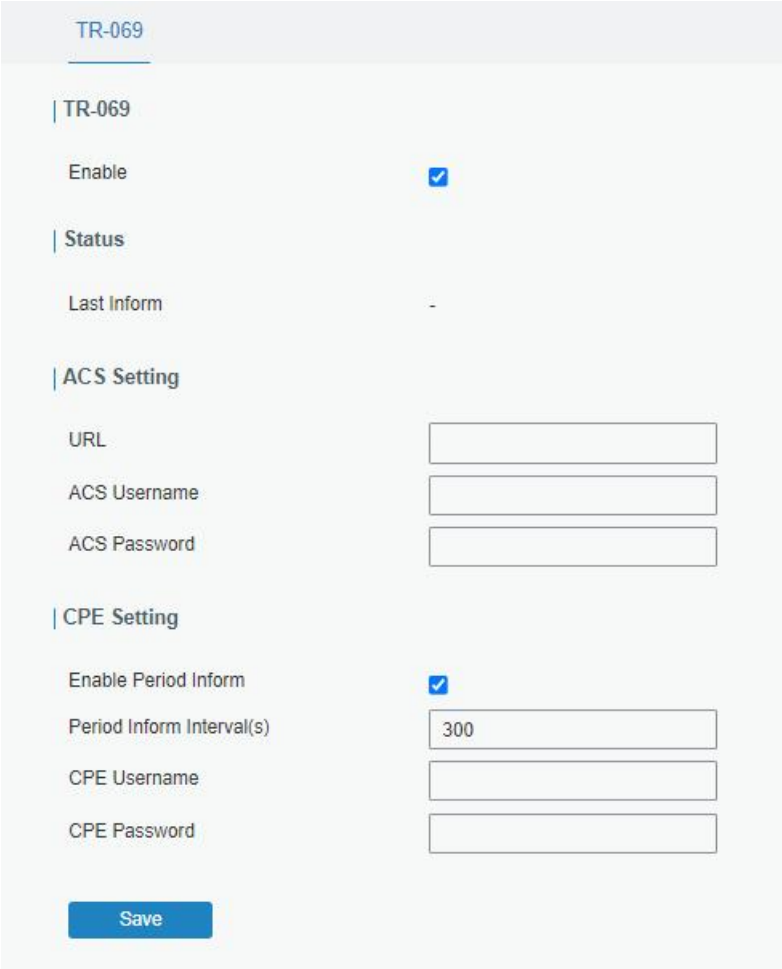
This section describes how to download MIB files. The last MIB file “LTE-ROUTER-MIB.txt” is for the UR41 router.



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

5.4.8 TR069

Technical Report 069 (TR-069) is a technical specification of Broadband Forum that defines an application layer protocol for remote management and provisioning of customer-premises equipment (CPE) connected to an Internet Protocol (IP) network.



TR-069	
Item	**Description**
Enable	Enable or disable TR069 feature.
Last Inform	The last time the router informed to TR069 ACS.
ACS Setting	
URL	The URL of TR069 auto configuration server (ACS).
ACS Username	The username used by ACS to authenticate the CPE when it initiates a connection request.
ACS Password	The password used by ACS to authenticate the CPE when it initiates a connection request.
CPE Setting	
Enable Period Inform	Enable or disable inform periodically.
Period Inform Interval (s)	The interval to report information to ACS, this should be less than the timeout of peer ACS.
CPE Username	The username used by CPE to authenticate the ACS when it initiates a connection request.
CPE Password	The password used by CPE to authenticate the ACS when it initiates a connection request.

5.5 Maintenance

This section describes system maintenance tools and management.

5.5.1 Tools

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

5.5.1.1 Ping

Ping tool is engineered to ping outer network.

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

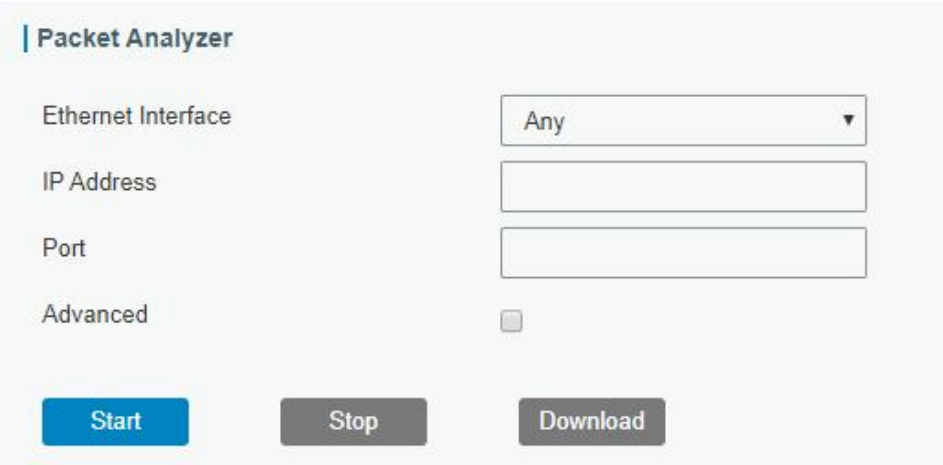
5.5.1.2 Traceroute

Traceroute tool is used for troubleshooting network routing failures.

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

5.5.1.3 Packet Analyzer

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



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

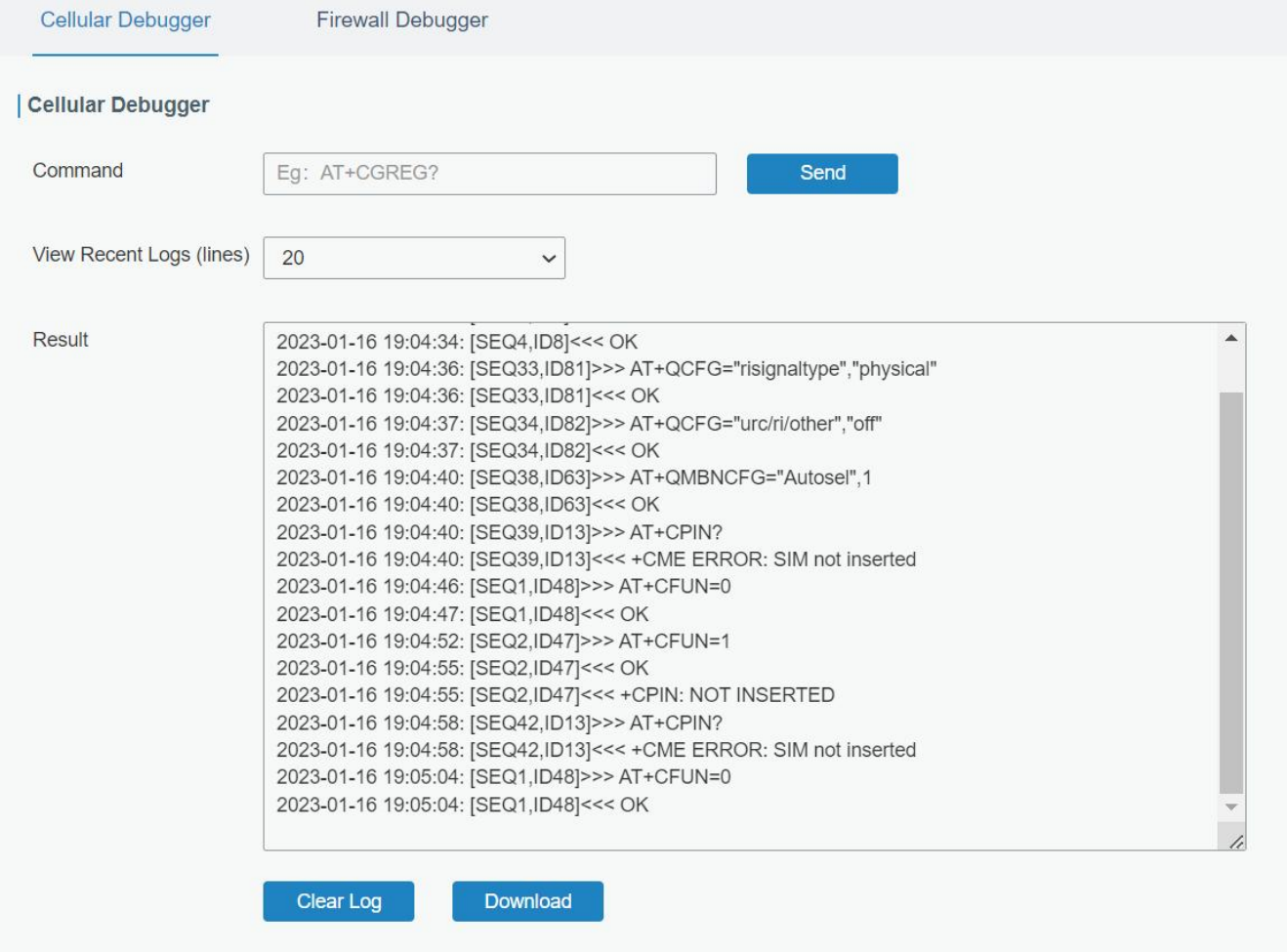
5.5.1.4 Qxdmlog

This section allow collecting diagnostic logs via QXDM tool.

5.5.2 Debugger

5.5.2.1 Cellular Debugger

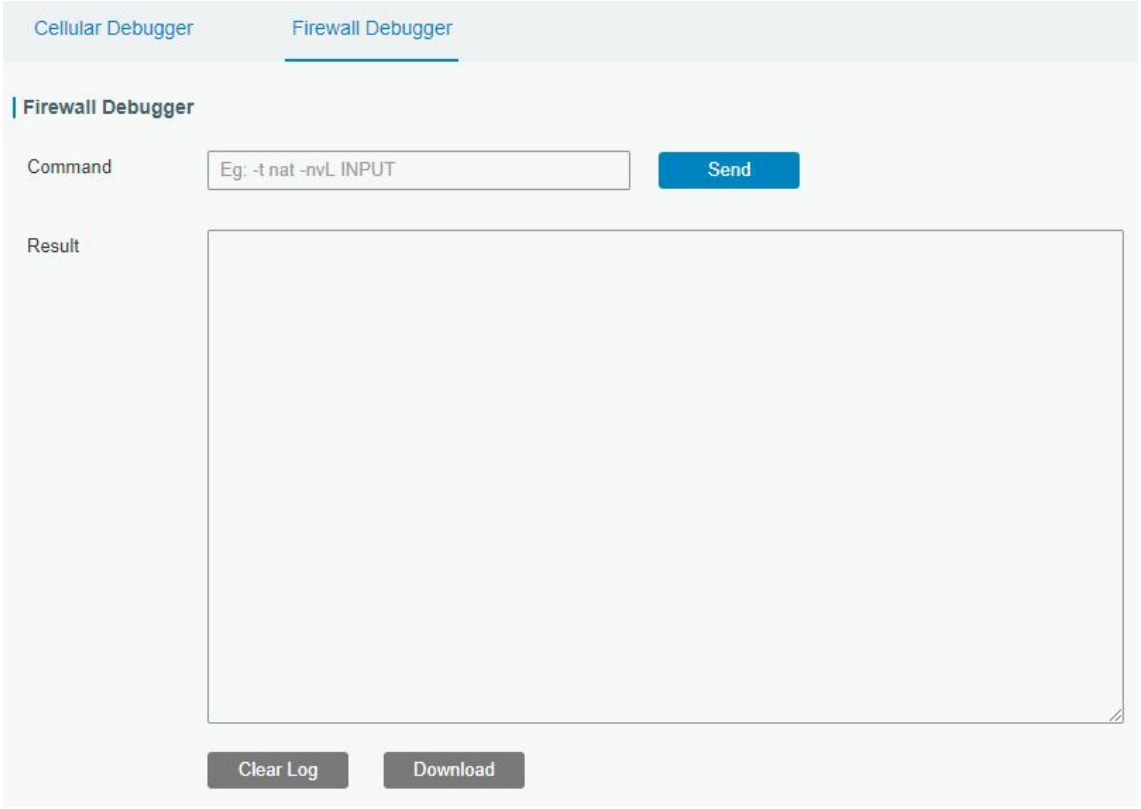
This section explains how to send AT commands to router and check cellular debug information.



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

5.5.2.2 Firewall Debugger

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



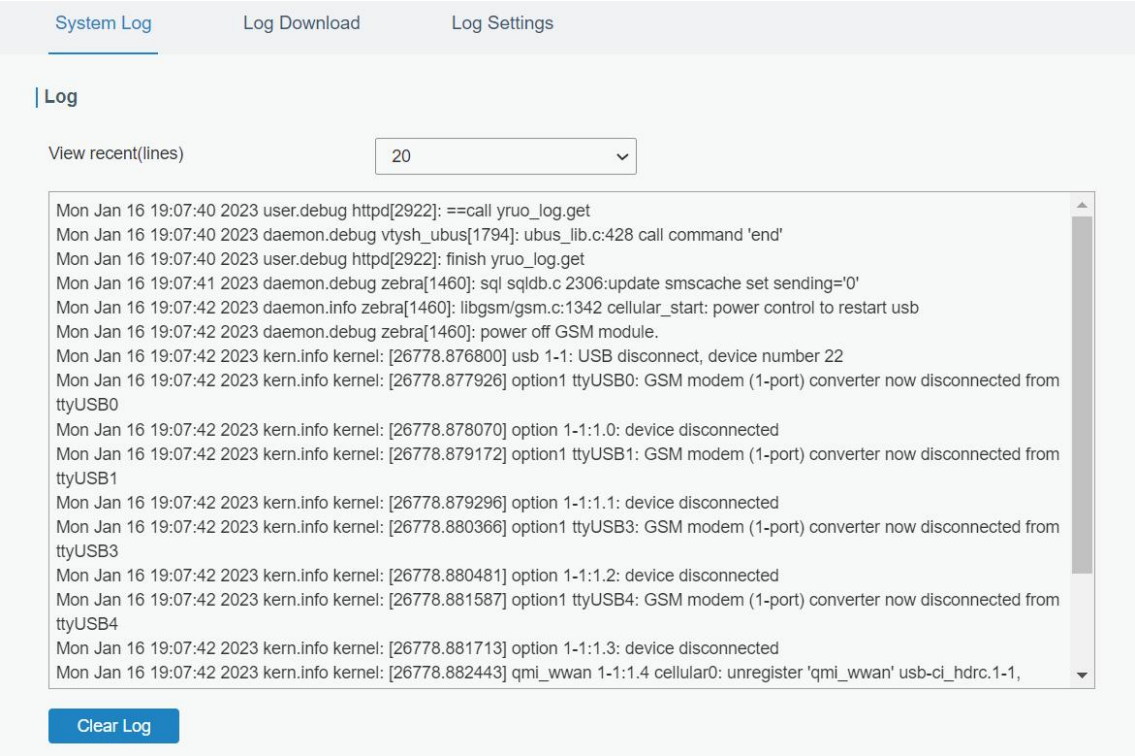
Firewall Debugger	
Item	**Description**
Command	Enter the AT command that you want to send to firewall module.
Result	Show the response result from firewall module.

5.5.3 Log

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

5.5.3.1 System Log

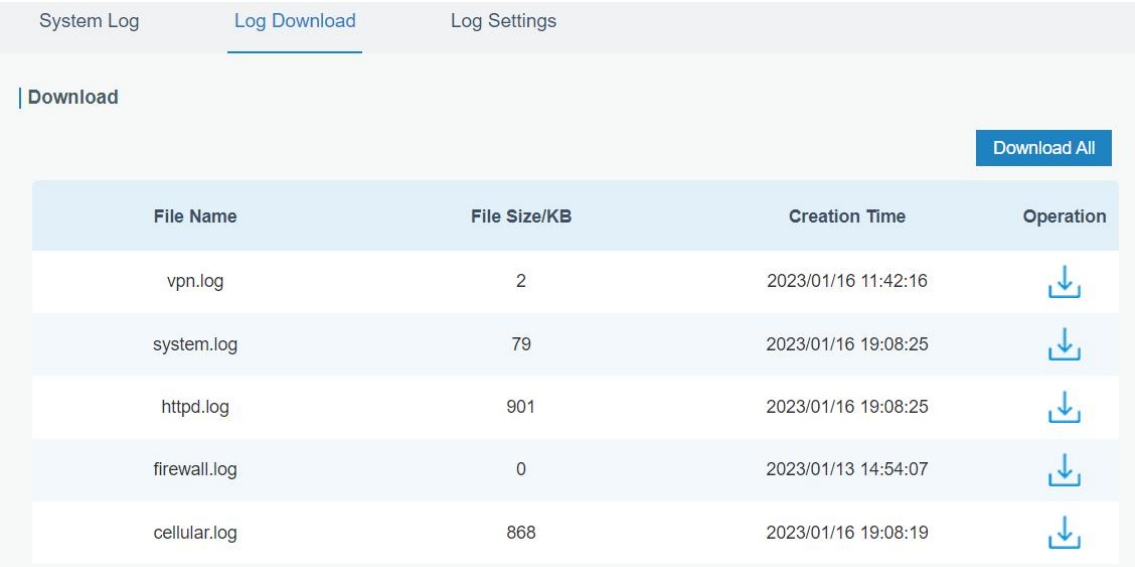
This section describes how to view the recent log on web.



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

5.5.3.2 Log Download

This section describes how to download log files.

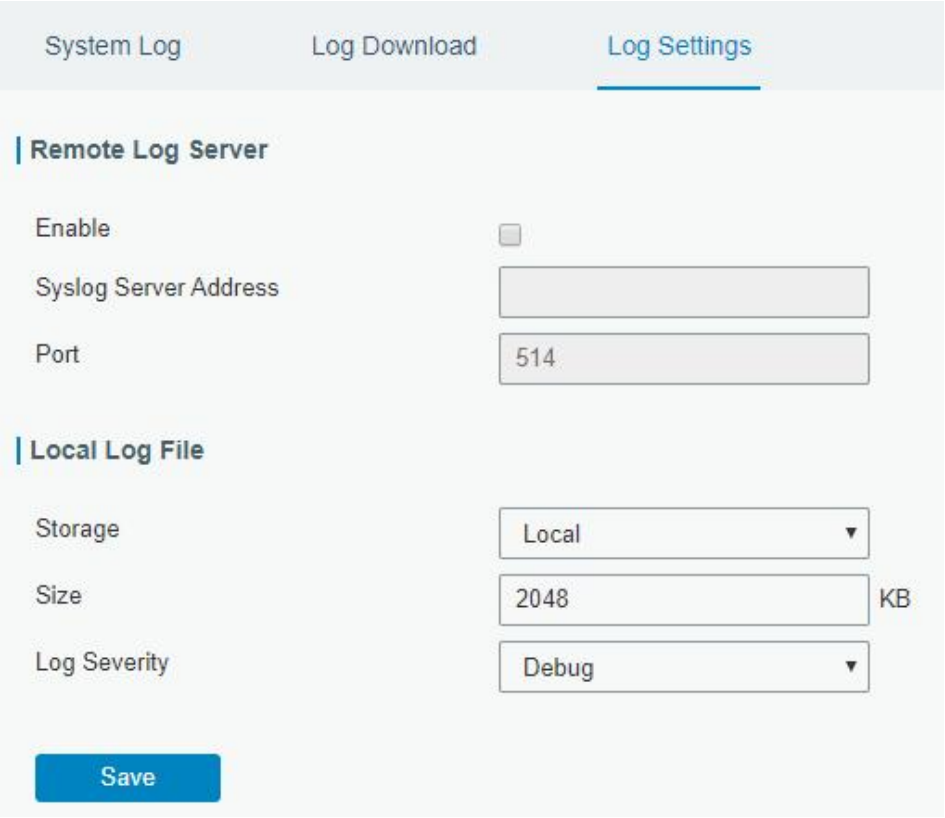


Log Download	
Item	**Description**
Download All	Download all log files.

File Name	Show the name of log files.
File Size/KB	Show the size of log files.
Creation Time	Show the creation time of log files.
Operation	Click to download every log file.

5.5.3.3 Log Settings

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



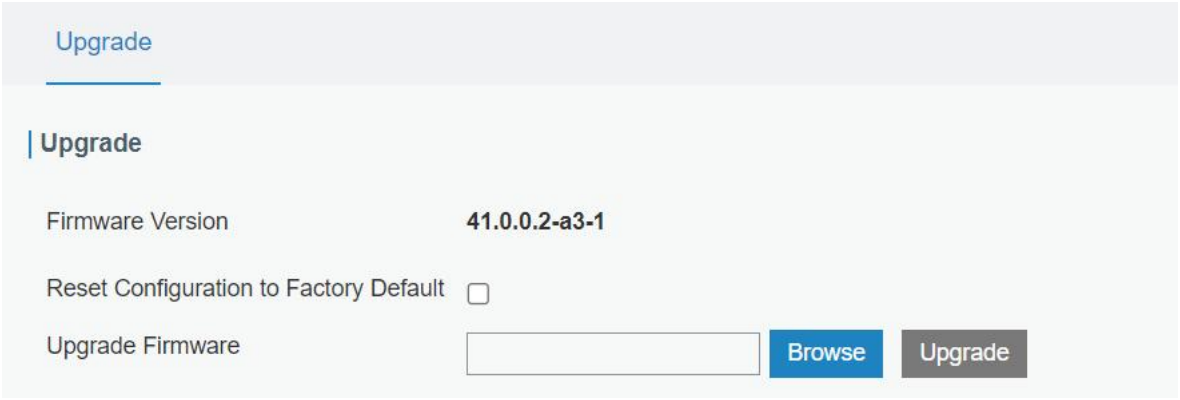
Log Settings	
Item	**Description**
Remote Log Server	
Enable	With “Remote Log Server” enabled, router will send all system logs to the remote server.
Syslog Server Address	Fill in the remote system log server address (IP/domain name).
Port	Fill in the remote system log server port.
Local Log File	
Storage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

5.5.4 Upgrade

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

the firmware upgrade.

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



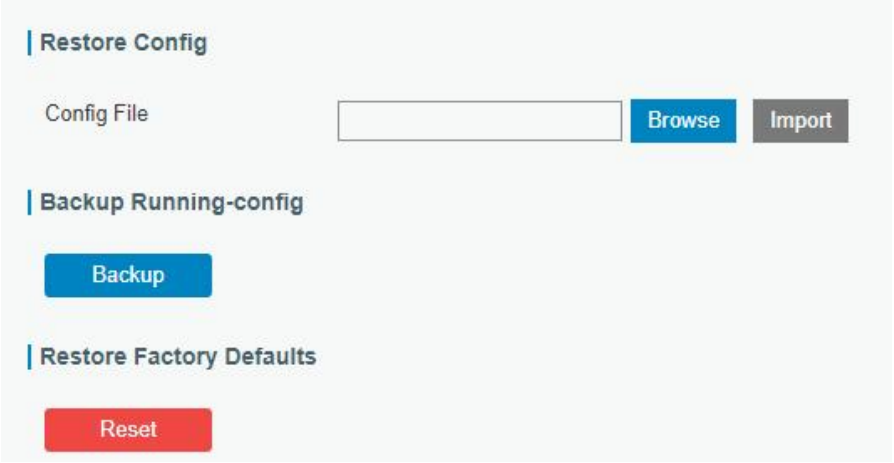
Upgrade	
Item	**Description**
Firmware Version	Show the current firmware version.
Reset Configuration to Factory Default	When this option is checked, the router will be reset to factory defaults after upgrade.
Upgrade Firmware	Click "Browse" button to select the new firmware file, and click "Upgrade"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

Related Configuration Example

Firmware Upgrade

5.5.5 Backup and Restore

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



Backup and Restore	
Item	**Description**
Config File	Click "Browse" button to select configuration file, and then click "Import" button to upload the configuration file to the router.

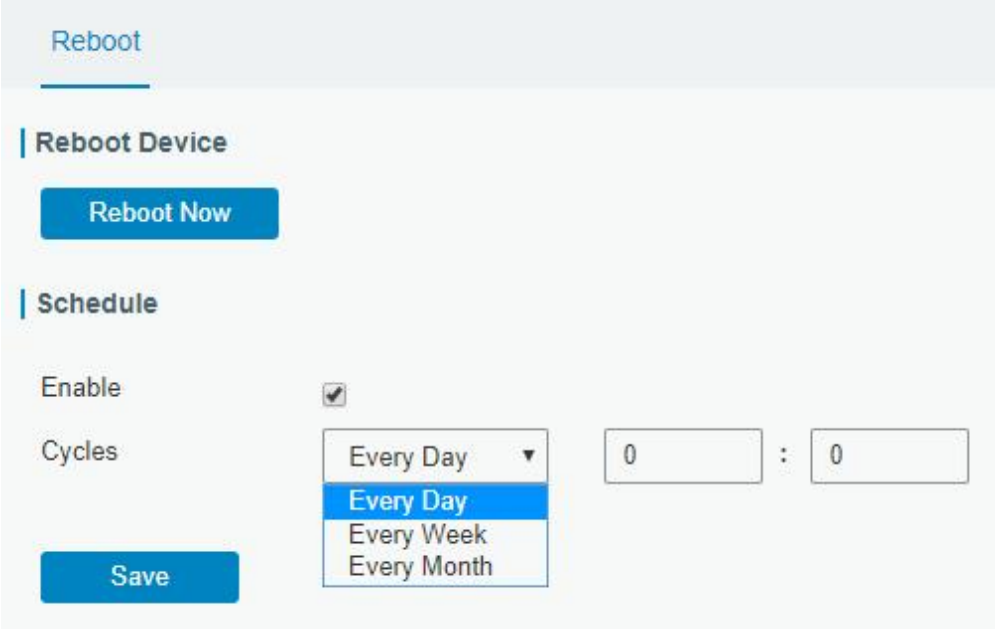
Backup	Click "Backup" to export the current configuration file to the PC.
Reset	Click "Reset" button to reset factory default settings. Router will restart after reset process is done.

Related Configuration Example

Restore Factory Defaults

5.5.6 Reboot

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



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

Chapter 6 Application Examples

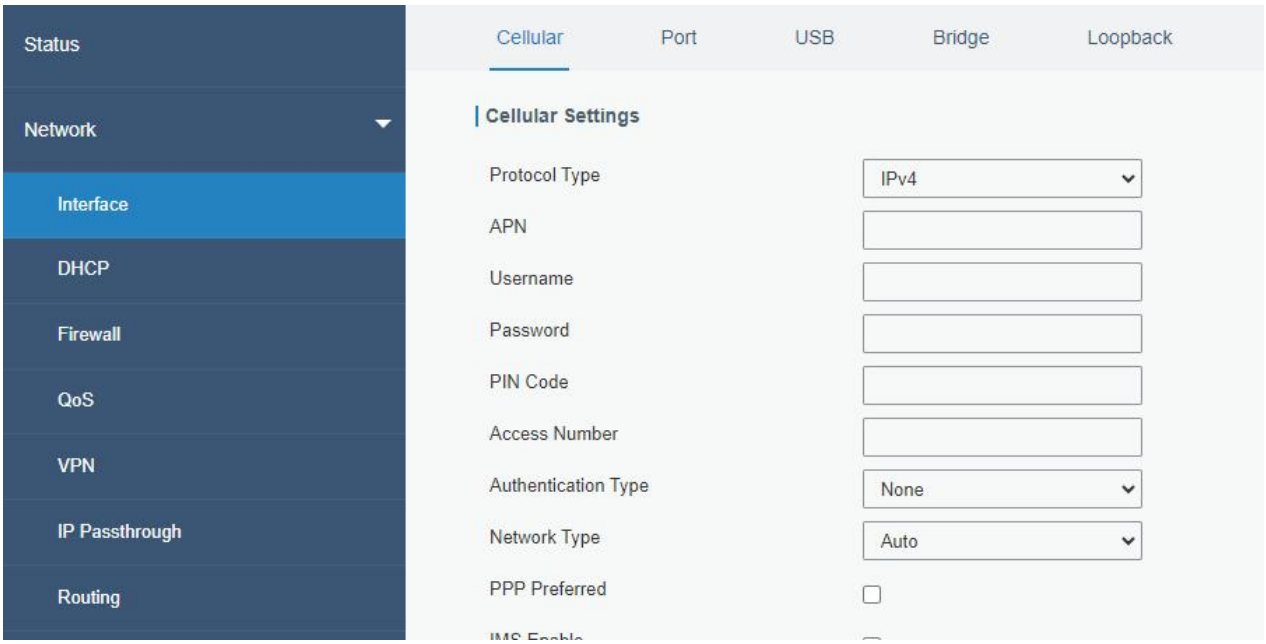
6.1 Cellular Connection

We are about to take an example of inserting a SIM card of the UR41 and configuring the router to get Internet access through cellular.

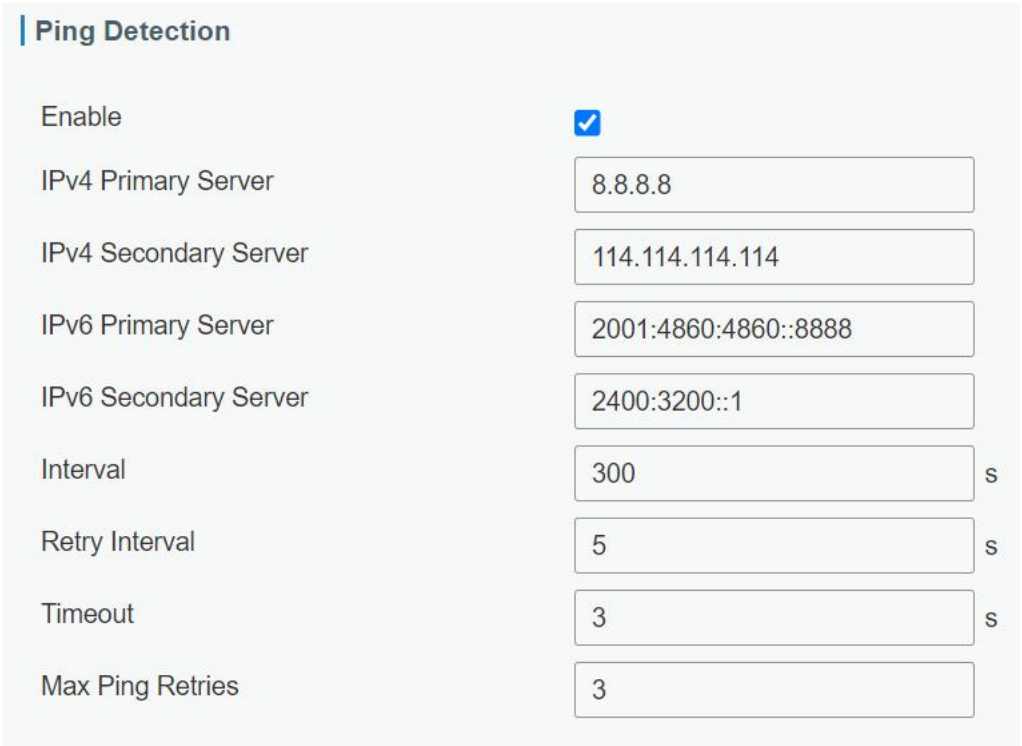
Configuration Steps

1. Ensure the SIM card is inserted well before powering on and all cellular antennas are connected to the correct connectors.
2. Go to **Network > Interface > Cellular > Cellular Setting** to configure the cellular info, then click

Save and **Apply**.



3. Enable **Network > Interface >Cellular > Ping Detection** to configure ping detection information.



4. Go to **Status > Cellular** to view the status of the cellular connection. If it shows Connected, SIM card has dialed up successfully.
5. Open your preferred browser on PC, type any available web address into address bar and see if it is able to visit Internet via the UR41 router.

Related Topic

Cellular Setting

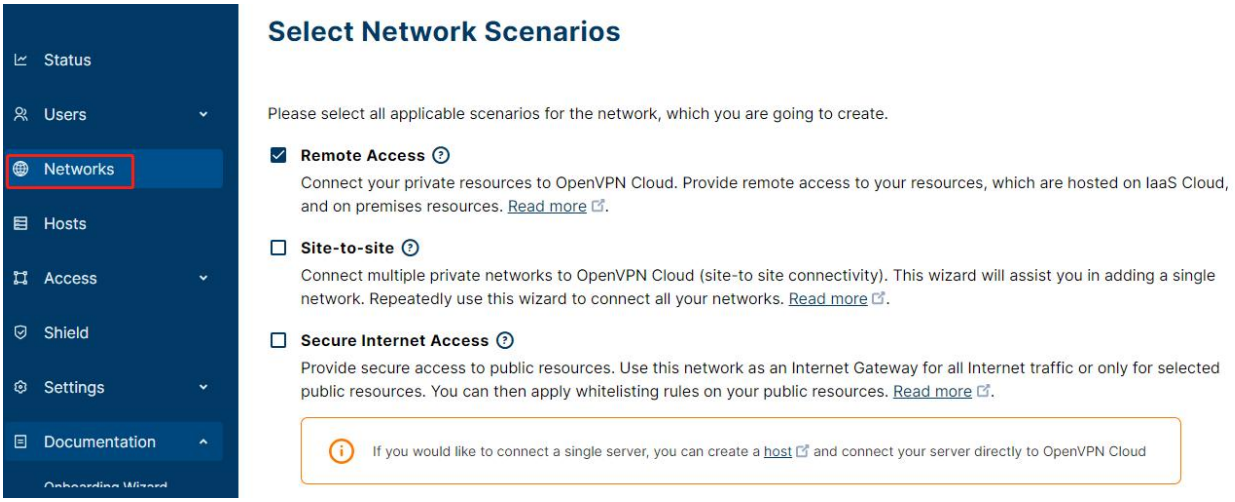
Cellular Status

6.2 OpenVPN Client Application Example

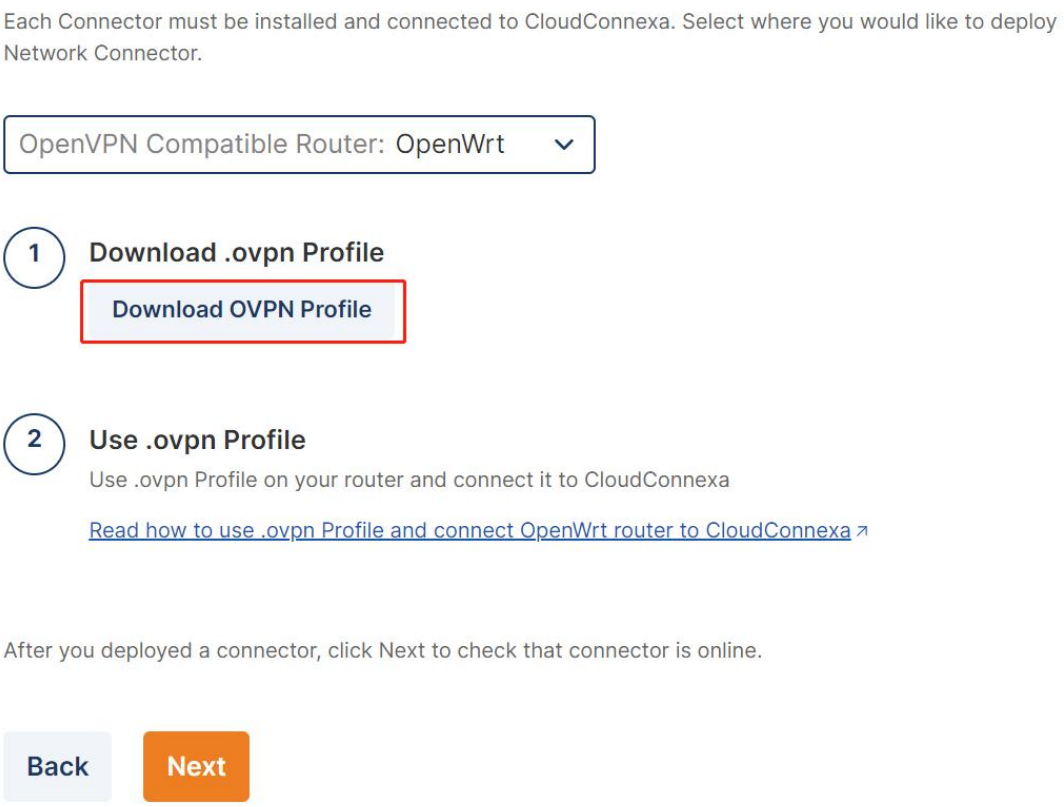
UR41 routers can work as OpenVPN clients or OpenVPN servers. We are about to take an example of configuring OpenVPN client to connect to OpenVPN cloud.

Configuration Steps

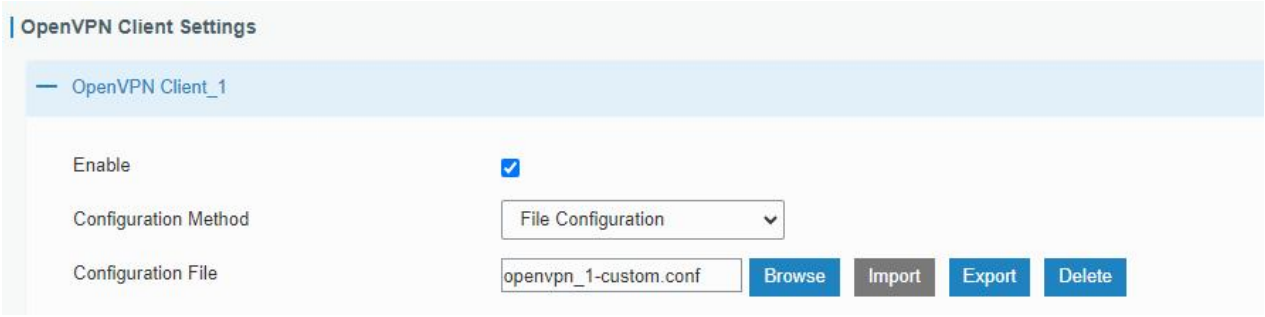
1. Ensure the router has gotten access to the Internet.
2. Log in the openVPN cloud account, select Network section and select the service depending on your requirement and follow the wizard to continue the settings.



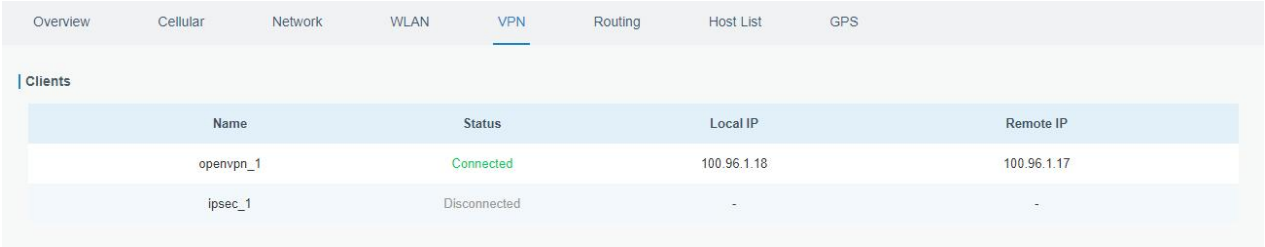
3. Select the location as OpenWrt and download the OVPN file.



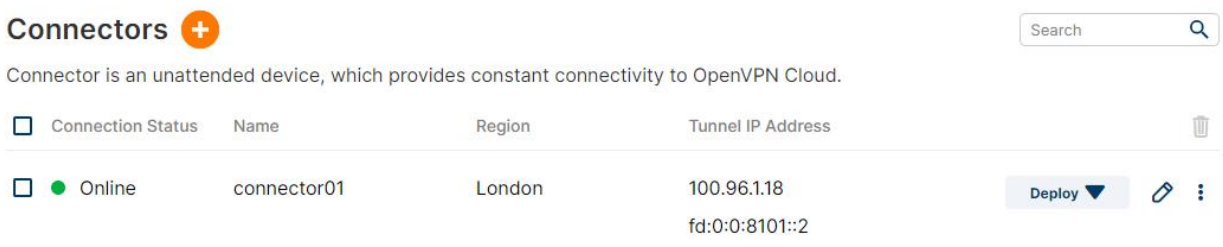
4. Go to **Network > VPN > OpenVPN Client**, select configuration method as File Configuration, then import the OVPN file.



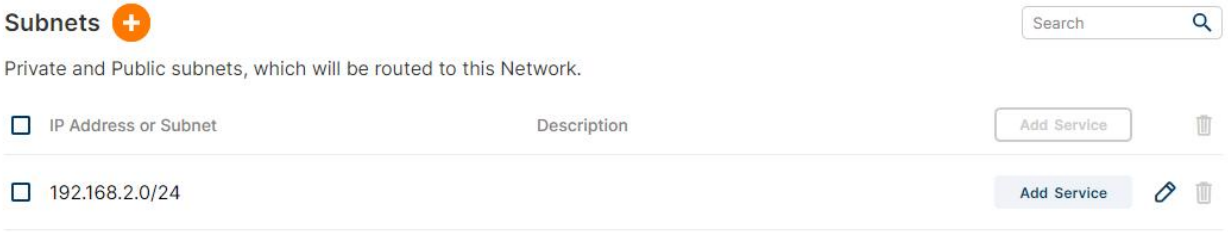
5. Go to **Status > VPN** page to check if the client is connected.



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 subnet, it's necessary to assign the subnet on OpenVPN cloud.



Related Topic

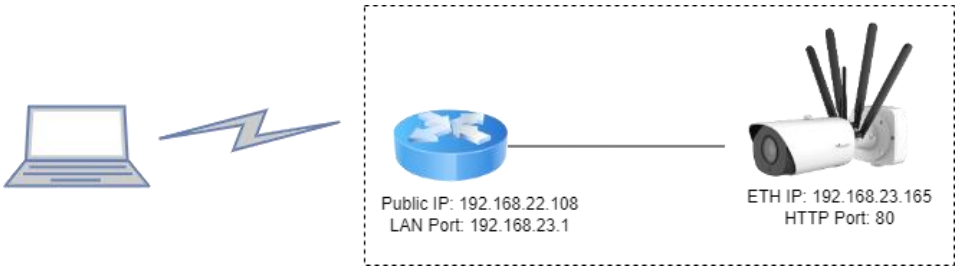
OpenVPN Client

VPN Status

6.3 NAT Application Example

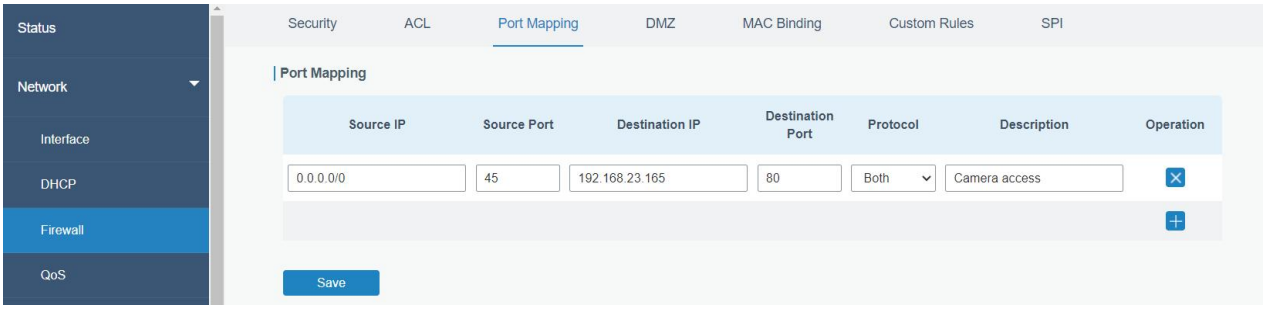
Example

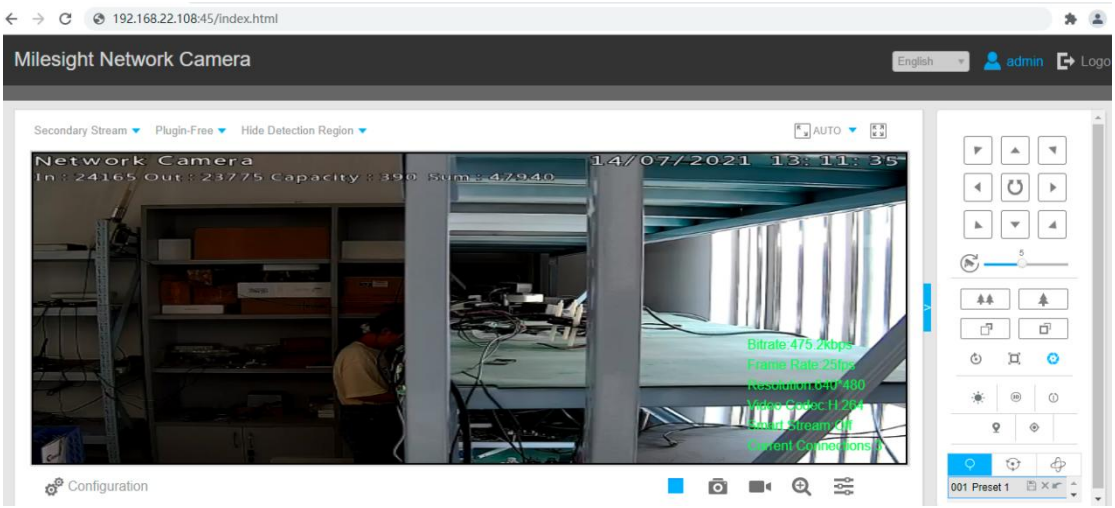
An UR41 router can access to the Internet via cellular and get a public IP address. LAN port is connected with an IP camera whose IP address is 192.168.23.165 and HTTP port is 80. This IP camera can be accessed by public IP address via the below port mapping settings.



Configuration Steps

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





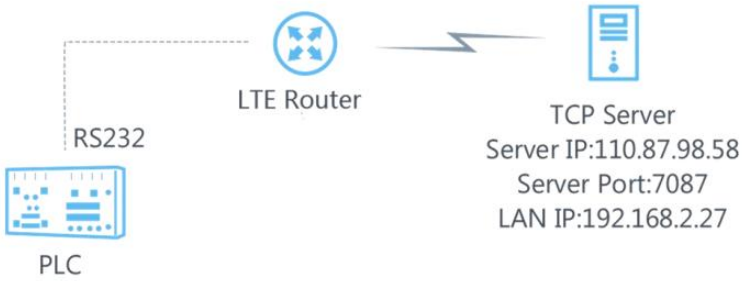
Related Topic

Port Mapping

6.4 DTU Application Example

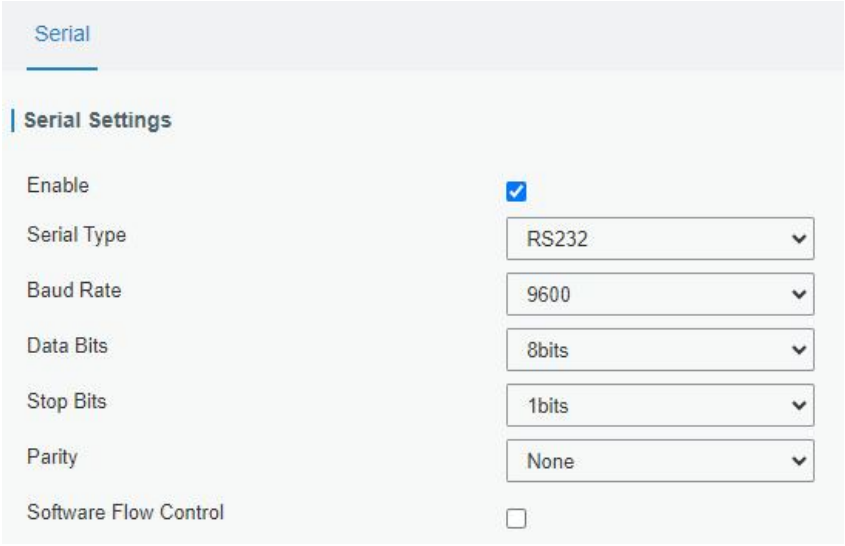
Example

A PLC is connected with the UR41 via RS232. Then enable DTU function of the UR41 to make a remote TCP server communicate with PLC. Refer to the following topological graph.

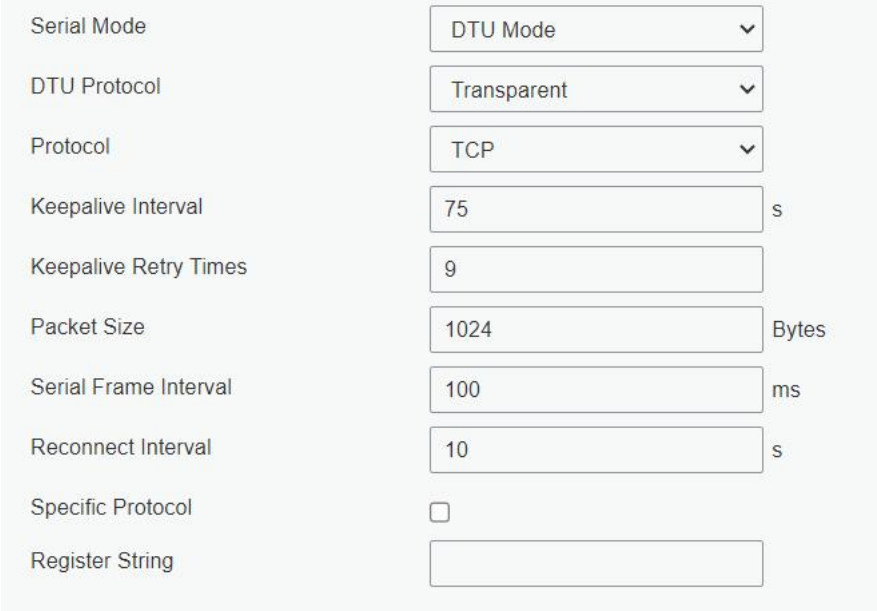


Configuration Steps

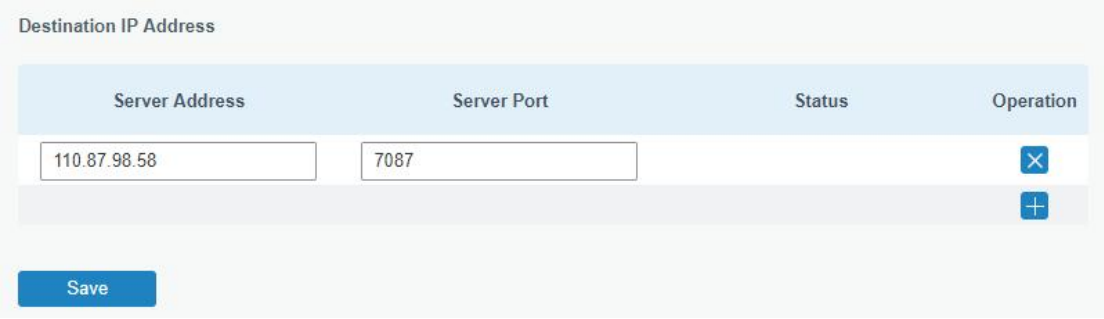
1. Go to **Industrial > Serial Port > Serial** and configure serial port parameters. The serial port parameter shall be kept in consistency with those of PLC, as shown in figure below.



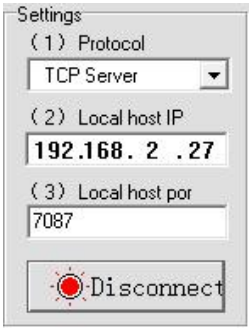
2. Configure Serial Mode as **DTU Mode**, DTU protocol as Transparent and protocol as TCP.



3. Configure TCP server IP and port.



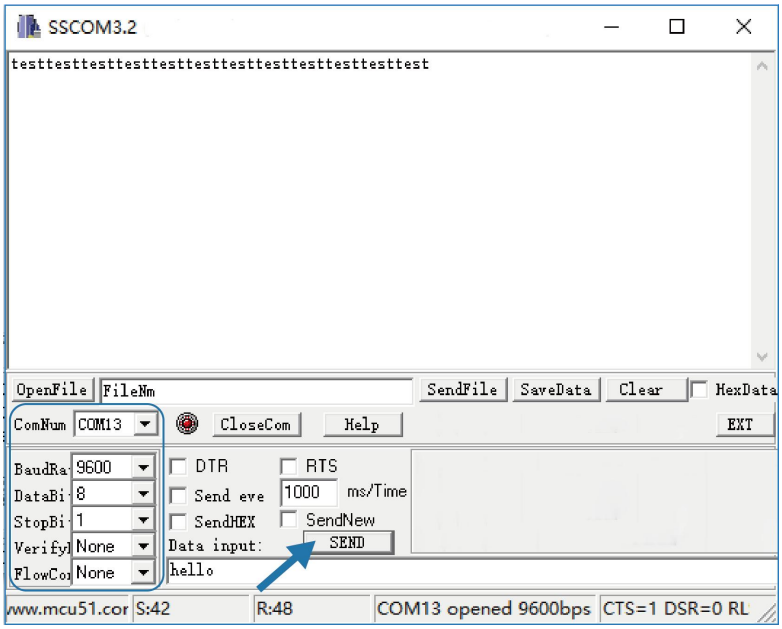
4. Start TCP server on PC. Take “Netassist” test software as example. Make sure port mapping is already done.



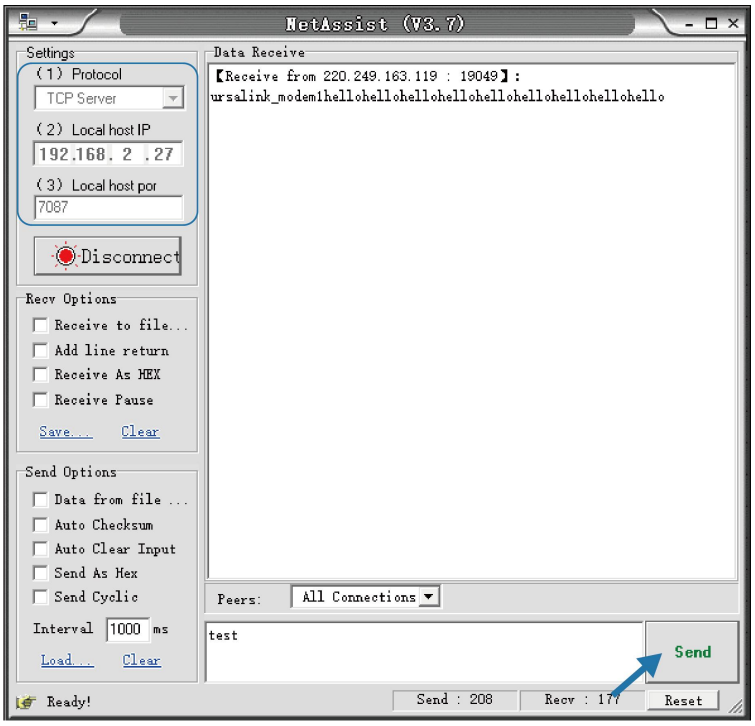
5. Connect the UR41 to PC via RS232 for PLC simulation. Then start **sscom** software on the PC to test communication through serial port.

6. After connection is established between the UR41 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 UR41 for test.

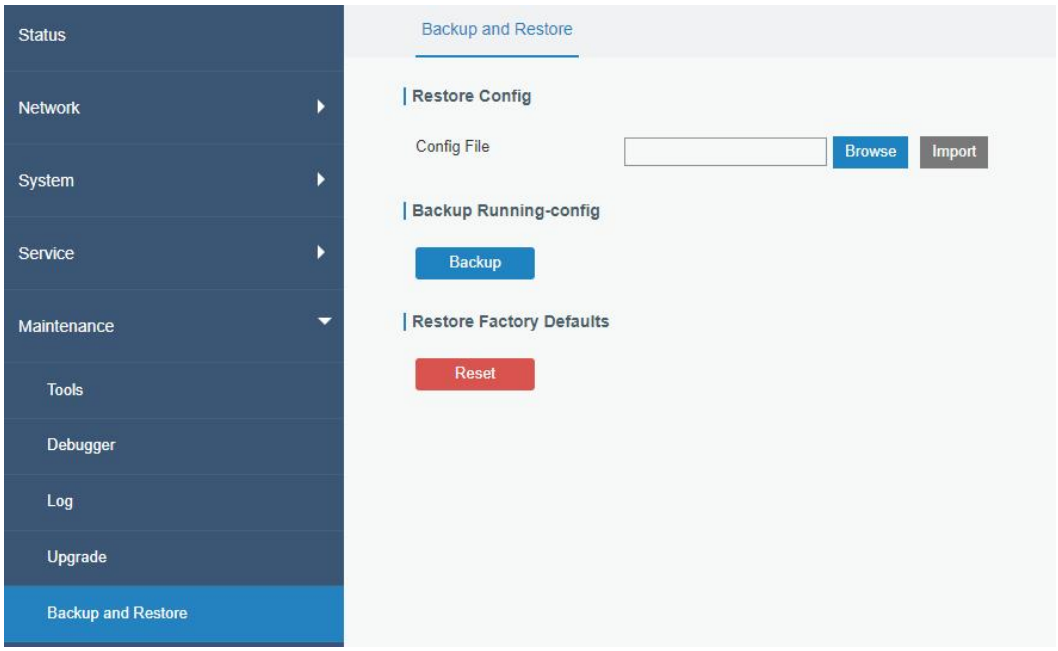
Related Topic

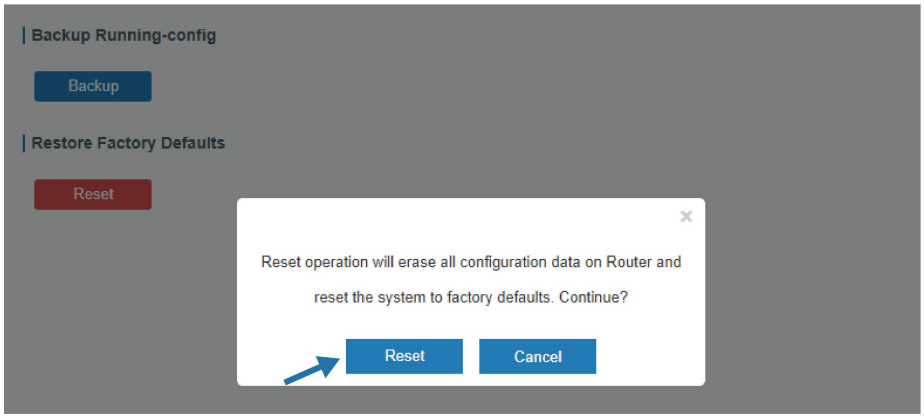
Serial Port

6.5 Restore Factory Defaults

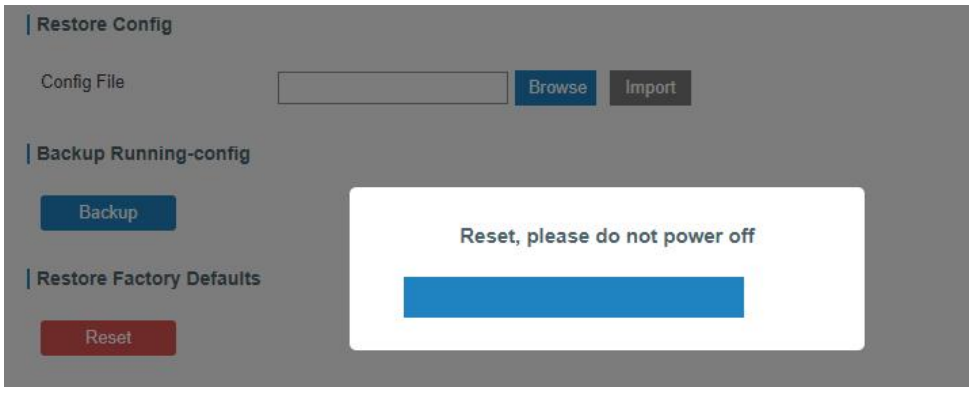
Method 1:

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





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



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

Related Topic

Restore Factory Defaults

Method 2:

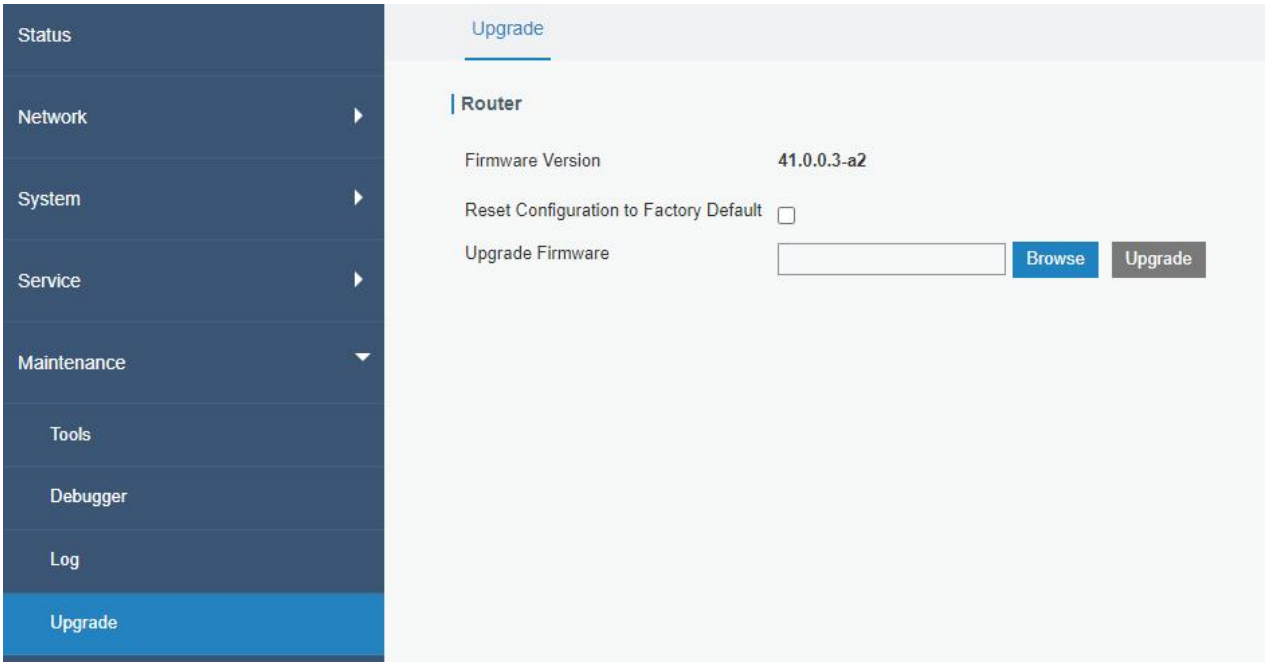
Locate the reset button on the router, press and hold the reset button for more than 5 seconds until SYSTEM LED blinks.

6.6 Firmware Upgrade

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

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

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



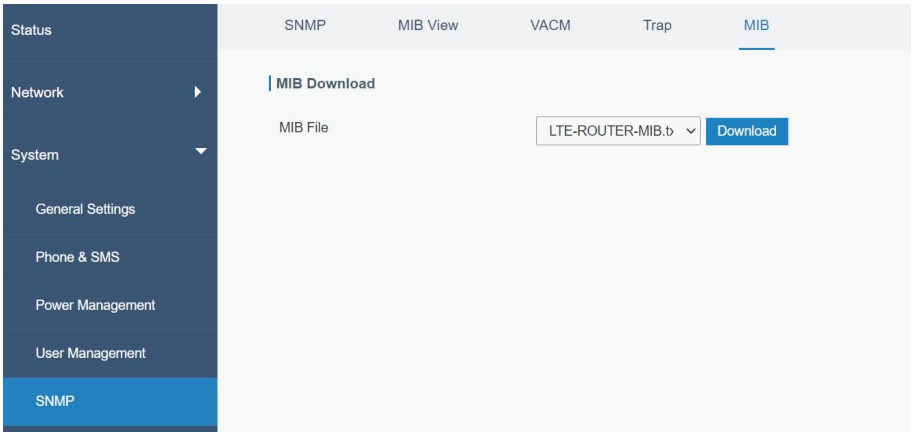
Related Topic

Upgrade

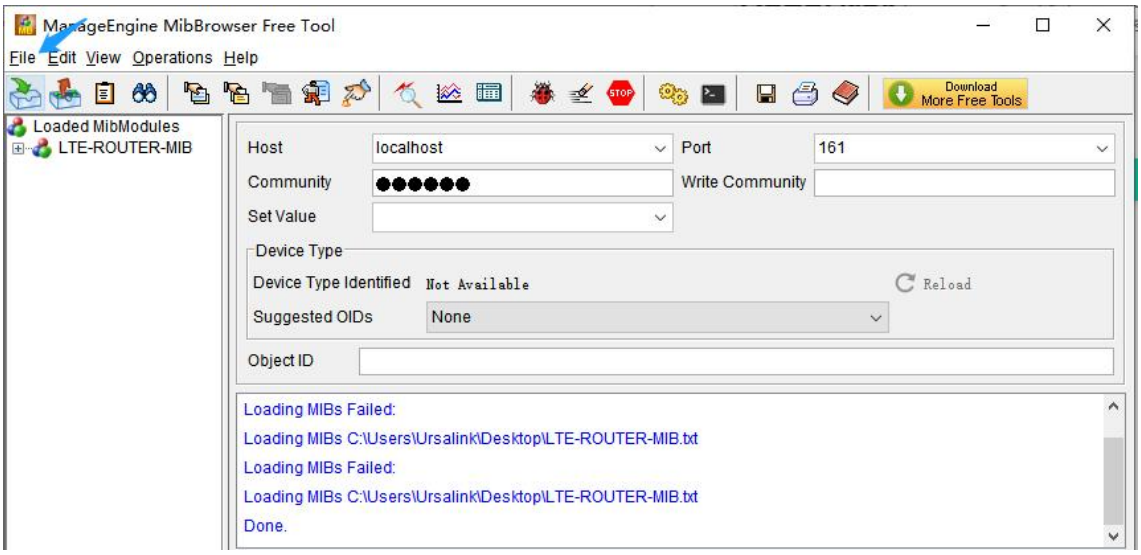
6.7 SNMP Application Example

Before you configure SNMP parameters, please download the relevant **MIB** file from the UR41's WEB GUI first, and then upload it to any software or tool which supports standard SNMP protocol. Here we take **ManageEngine MibBrowser Free Tool** as an example to access the router to query cellular information.

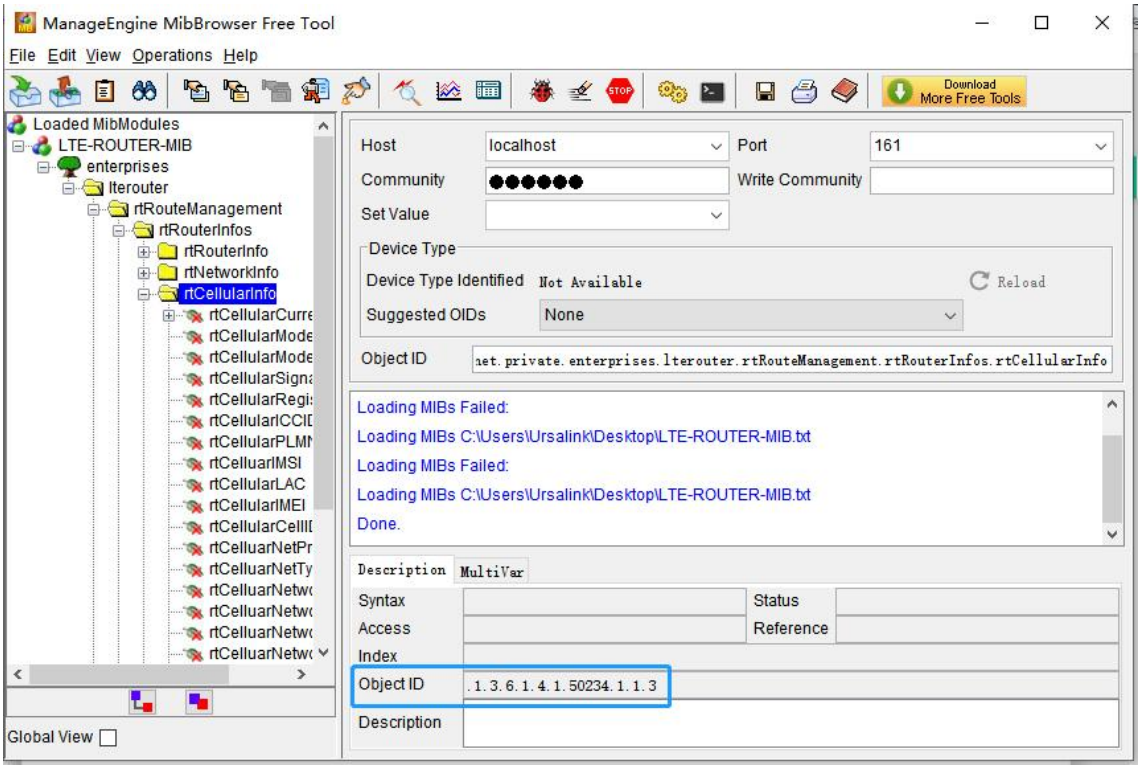
1. Go to **System > SNMP > MIB** and download the MIB file "LTE-ROUTER-MIB.txt" to PC.



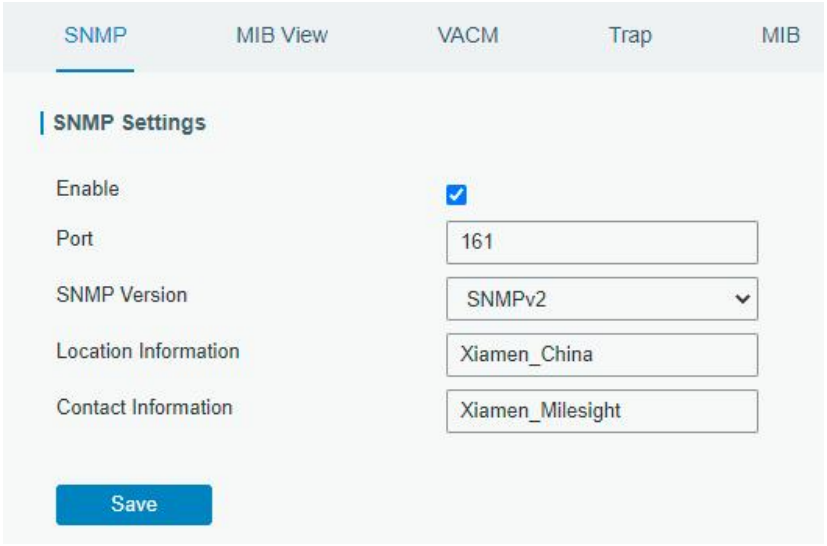
2. Start “ManageEngine MibBrowser Free Tool” on the PC. Click **File > Load MIB** on the menu bar. Then select “LTE-ROUTER-MIB.txt” file from PC and upload it to the software.



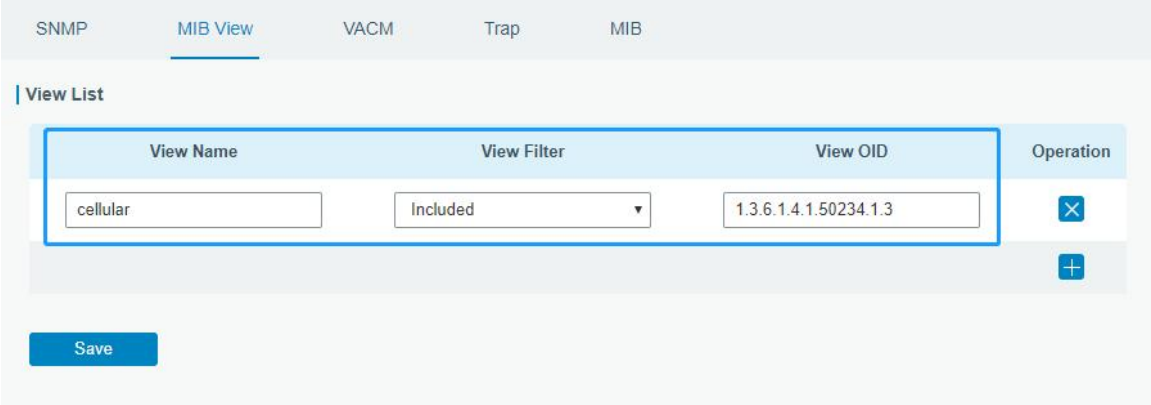
Click the **+** button beside “LTE-ROUTER-MIB”, which is under the “Loaded MibModules” menu, and find “usCellularinfo”. And then you will see the OID of cellular info is “.1.3.6.1.4.1.50234”, which will be filled in the MIB View settings.



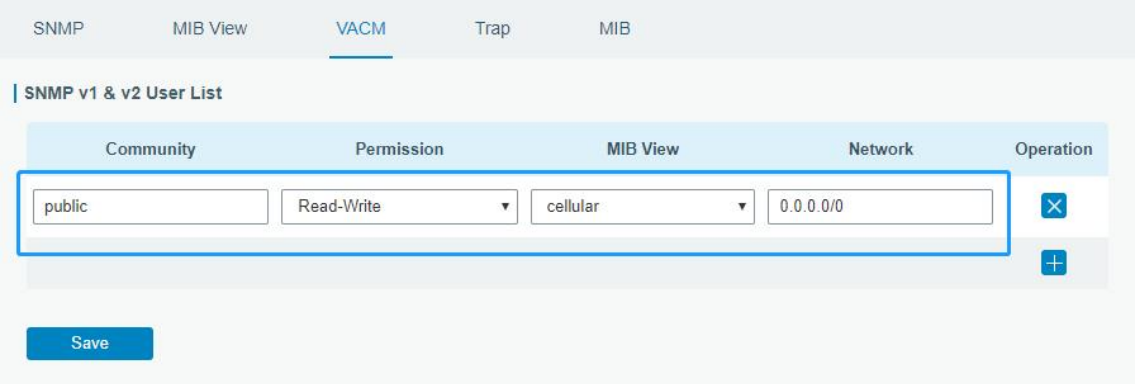
3. Go to **System > SNMP > SNMP** on the router's WEB GUI. Check **Enable** option, then click **Save** button.



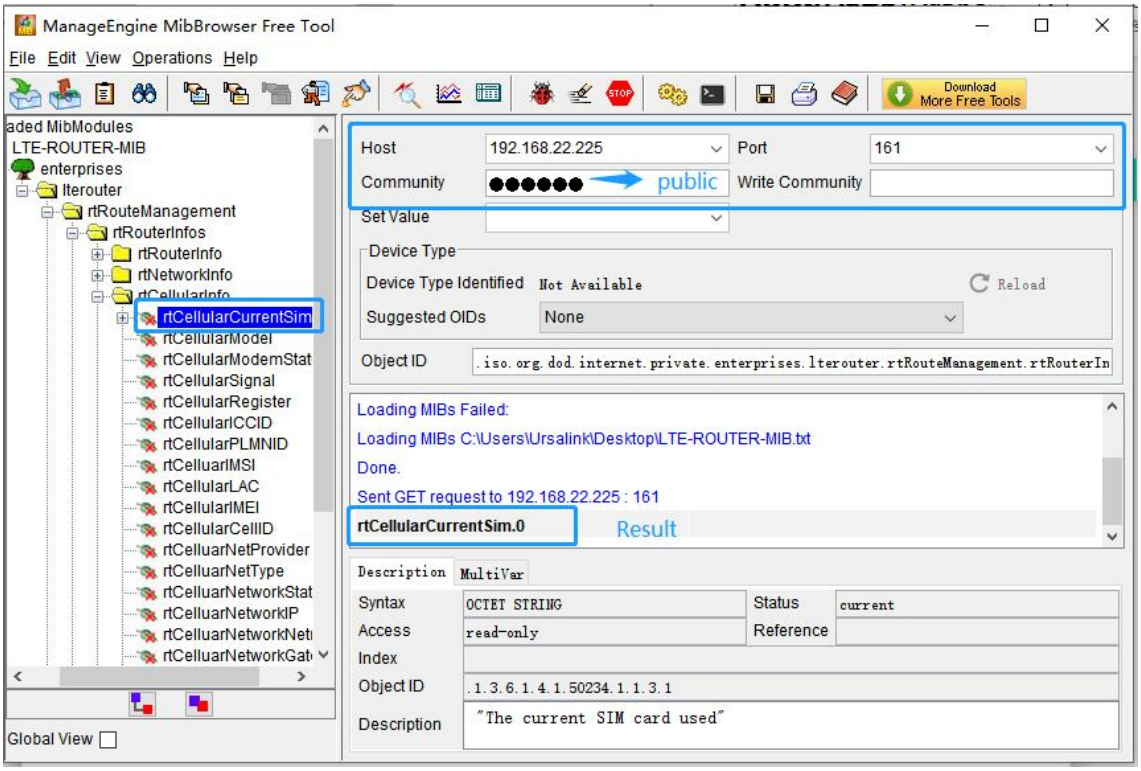
4. Go to **System > SNMP > MIB View**. Click  to add a new MIB view and define the view to be accessed from the outside network. Then click **Save** button.



5. Go to **System > SNMP > VACM**. Click to add a new VACM setting to define the access authority for the specified view from the specified outside network. Click **Save** and **Apply** to make the changes take effect.



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



Related Topic

SNMP

6.8 QoS Application Example

Example

Configure the UR41 router to distribute local preference to different FTP download channels. The total download bandwidth is 75000 kbps.

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

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

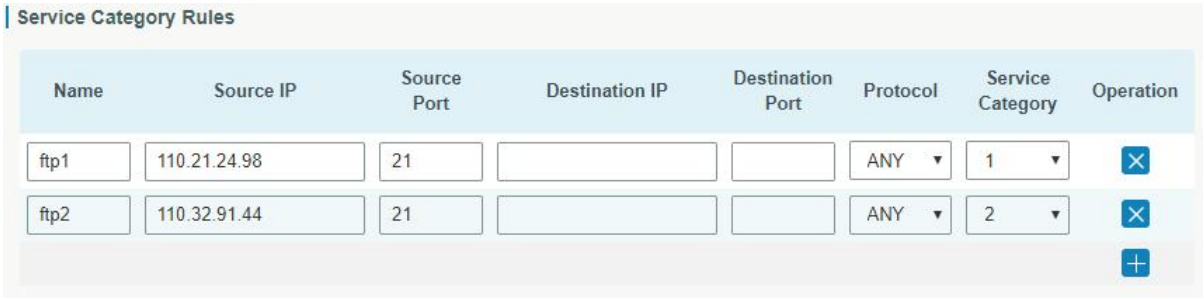
Configuration Steps

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

2. Please find **Service Category** option, and click "+" to set up service classes.

Note: the percents must add up to 100%.

3. Please find **Service Category Rules** option, and click "+" to set up rules.



Note:

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

Click "Save" and "Apply" button.

Related Topic

QoS Setting

[END]