# UR 71

## Industrial Cellular Router User Guide

Xiamen Ursalink Technology Co., Ltd.

www.ursalink.com

# Preface

Thanks for choosing Ursalink UR71 industrial cellular router. The UR71 industrial cellular router delivers tenacious connection over network with full-featured design such as automated failover/failback, extended operating temperature, dual SIM cards, hardware watchdog, VPN, Gigabit Ethernet and beyond.

This guide describes how to configure and operate the UR71 industrial cellular router. You can refer to it for detailed functionality and router configuration.

# Readers

This guide is mainly intended for the following users:

- Network Planners
- On-site technical support and maintenance personnel
- Network administrators responsible for network configuration and maintenance

**Xiamen Ursalink Technology Co., Ltd.**

**All rights reserved.**

All information in this user guide is protected by copyright law. Whereby, no organization or individual shall copy or reproduce the whole or part of this user guide by any means without written authorization from Xiamen Ursalink Technology Co., Ltd.

### Products Covered

This guide explains how to configure the following devices:

• Ursalink UR71 Industrial Cellular Router

### Related Documents

| Document | Description |
|---|---|
| Ursalink UR71 Datasheet | Datasheet for the Ursalink UR7x series industrial cellular router. |
| Ursalink UR71 Quick Start Guide | Quick installation guide for the Ursalink UR7x series industrial cellular router. |

**Declaration of Conformity**

UR71 is in conformity with the essential requirements and other relevant provisions of the CE, FCC, and RoHS.

# FCC Warning

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.
Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

FCC Radiation Exposure Statement:
This equipment complies with FCC radiation exposure limits set forth for an uncontrolled environment .
This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
This equipment should be installed and operated with minimum distance 20cm between the radiator& your body.

For assistance, please contact
Ursalink technical support:
Email: support@ursalink.com
Tel.: 86-592-5023060
Fax: 86-592-5023065

**Revision History**

| Date | Doc Version | Description |
|---|---|---|
| Dec. 22, 2017 | V.1.0.0 | Initial version |

# Contents

Chapter 1 Product Introduction.....8
1.1 Overview.....8
1.2 Advantages.....8
1.3 Specifications.....10
1.4 Dimensions (mm).....12
Chapter 2 Installation.....12
2.1 General Packing List.....12
2.2 Product Overview.....13
2.3 LED Indicators.....13
2.4 Ethernet Port Indicators.....14
2.5 PIN Definition.....14
2.6 Reset Button.....15
2.7 SIM Card Installation.....15
2.8 Micro SD card Installation.....16
2.9 Cellular Antenna Installation.....16

2.10 Mounting the Router....16
2.11 Connect the Router to a Computer.... 17
2.12 Installation of Power Supply and Protective Grounding.... 17
2.12.1 Power Supply Installation.... 17
2.12.2 Protective Grounding Installation....18
Chapter 3 Access to Web GUI.... 19
3.1 PC Configuration for Web GUI Access to Router.... 19
3.2 Access to Web GUI of Router....20
Chapter 4 Web Configuration.... 21
4.1 Status....22
4.1.1 Overview.... 22
4.1.2 Cellular....22
4.1.3 Network....24
4.1.4 VPN....25
4.1.5 Routing Information....26
4.1.6 Host List....27
4.2 Network....27
4.2.1 Interface.... 27
4.2.1.1 Port....27
4.2.1.2 LAN.... 28
4.2.1.3 VLAN Trunk....29
4.2.1.4 Cellular.... 29
4.2.1.5 Loopback....33
4.2.2 Firewall.... 33
4.2.2.1 ACL....34
4.2.2.2 DMZ....35
4.2.2.3 Port Mapping.... 36
4.2.2.4 MAC Binding....37
4.2.3 QoS.... 37
4.2.3.1 QoS (Download/Upload)....37
4.2.4 DHCP....39
4.2.4.1 DHCP Server....39
4.2.4.2 DHCP Relay....40
4.2.5 DDNS.... 40
4.2.6 Link Failover....42
4.2.6.1 SLA....42
4.2.6.2 Track.... 43
4.2.6.3 VRRP....44
4.2.7 Routing.... 46
4.2.7.1 Static Routing.... 46
4.2.7.2 RIP.... 47
4.2.7.3 OSPF.... 51
4.2.7.4 Routing Filtering....56
4.2.8 VPN....57

4.2.8.1 DMVPN....57
4.2.8.2 IPSec....59
4.2.8.3 GRE....62
4.2.8.4 L2TP....64
4.2.8.5 PPTP....66
4.2.8.6 OpenVPN Client....68
4.2.8.7 OpenVPN Server....69
4.2.8.8 Certifications....71
4.3 System....73
4.3.1 General Settings....73
4.3.1.1 General....73
4.3.1.2 Account Management....75
4.3.1.3 System Time....76
4.3.1.4 SMTP....77
4.3.1.5 Phone....78
4.3.1.6 Storage....79
4.3.2 User Management....80
4.3.3 SNMP....80
4.3.3.1 SNMP....81
4.3.3.2 MIB View....82
4.3.3.3 VACM....82
4.3.3.4 Trap....83
4.3.3.5 MIB....84
4.3.4 AAA....84
4.3.4.1 Radius....85
4.3.4.2 Tacacs+....85
4.3.4.3 LDAP....86
4.3.4.4 Authentication....87
4.3.5 Device Management....87
4.3.6 Events....88
4.3.6.1 Events....88
4.3.6.2 Events Settings....89
4.4 Industrial Interface....91
4.4.1 Serial Port....91
4.4.2 Modbus Master....95
4.4.2.1 Modbus Master....95
4.4.2.2 Channel....96
4.5 Maintenance....98
4.5.1 Tools....98
4.5.1.1 Ping....98
4.5.1.2 Traceroute....98
4.5.2 Schedule....99
4.5.3 Log....99
4.5.3.1 System Log....100

4.5.3.2 Log Settings.....100
4.5.4 Upgrade.....101
4.5.5 Backup and Restore.....102
4.5.6 Reboot.....103
4.6 APP.....104
4.6.1 Python.....104
4.6.1.1 Python.....104
4.6.1.2 App Manager Configuration.....105
4.6.1.3 Python App.....106
Chapter 5 Application Examples.....106
5.1 Account Info Management.....106
5.2 Common User Management.....107
5.3 System Time Management.....108
5.4 Backup and Restore Configuration.....109
5.5 Restore Factory Defaults.....111
5.5.1 Via Web Interface.....111
5.5.2 Via Hardware.....112
5.6 Firmware Upgrade.....113
5.7 Events Application Example.....115
5.8 Schedule Application Example.....116
5.9 Logs and Diagnostics.....117
5.10 SNMP Application Example.....118
5.11 Cellular Connection.....121
5.12 Dual SIM Backup Application Example.....123
5.13 VRRP Application Example.....126
5.14 NAT Application Example.....129
5.15 Access Control Application Example.....130
5.16 QoS Application Example.....131
5.17 DTU Application Example.....132
5.18 PPTP Application Example.....136

# Chapter 1 Product Introduction

## 1.1 Overview

Ursalink UR71 is an industrial cellular router with embedded intelligent software features that are designed for multifarious M2M/IoT applications. Supporting global WCDMA and 4G LTE, UR71 provides drop-in connectivity for operators and makes a giant leap in maximizing uptime.

Adopting high-performance and low-power consumption industrial platform of 64-bit CPU and wireless module, the UR71 is capable of providing wire-speed network with a typical 2 W power consumption and ultra-small package to ensure the extremely safe and reliable connection to the wireless network.

Meanwhile, the UR71 also supports Gigabit Ethernet port, serial port (RS232/RS485), which enables you to scale up M2M application combining data and video in limited time and budget.

The UR71 is particularly ideal for smart grid, digital media installations, industrial automation, telemetry equipment, medical device, digital factory, finance, payment device, environment protection, water conservancy and so on.

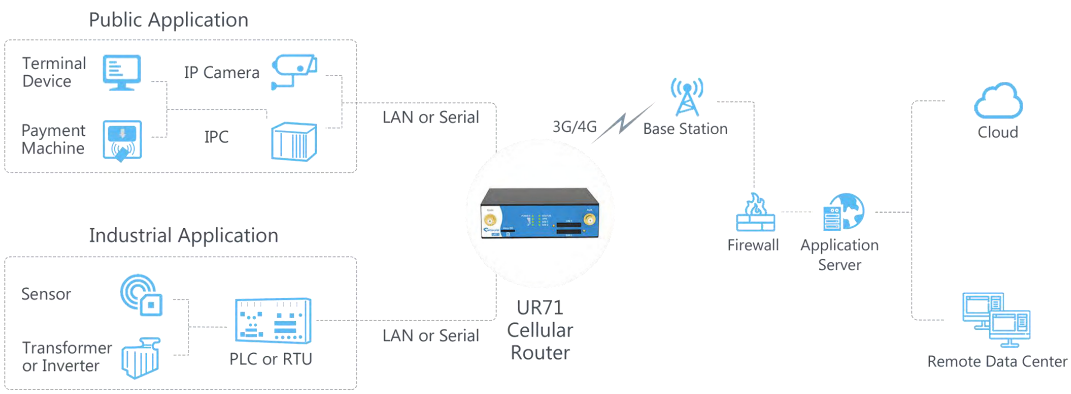



Figure 1-1

## 1.2 Advantages

**Benefits**

- Built-in industrial strong CPU, big memory; Micro SD card is available to support further development and customized requirements
- Gigabit Ethernet is applied to all models of Ursalink routers for lightning transmission of data
- Dual SIM cards for backup between multiple carriers networking and global 3G/LTE options make it easy to get connected

- Embed Ursalink SDK (Python 2.7/C) for secondary development
- Flexible modular design provides users with different connection modules like Ethernet, serial port for connecting diverse field assets
- Rugged enclosure, optimized for DIN rail or shelf mounting
- 3-year warranty included

**Security & Reliability**

- Automated failover/failback between Ethernet and Cellular (dual SIM)
- Enable unit with security frameworks like IPsec/OpenVPN/GRE/L2TP/PPTP/ DMVPN
- Embed hardware watchdog, able to automatically recover from various failure, ensure highest level of availability
- Establish a secured mechanism on centralized authentication and authorization of device access by supporting AAA (Tacacs+, Radius, LDAP, local authentication) and multiple levels of user authority
-

**Easy Maintenance**

- Ursalink Device Management Platform 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 administrator to manage the device as easy as pie
- WEB GUI and CLI enable the admin to achieve simple management and quick configuration among a large quantity of devices
- Efficiently manage the remote routers on the existing platform through the industrial standard SNMP

**Capabilities**

- Link remote devices in an environment where communication technologies are constantly changing
- Industrial 64-bit ARM Cortex-A53 processor, high-performance operating up to 800MHz with low power consumption below 1W, and 256 MB memory available to support more applications
- Support rich protocols like SNMP, MQTT, Modbus bridging, RIP, OSPF
- Support wide operating temperature ranging from -40°C to 50°C/-40°F to 122°F

## 1.3 Specifications

| | |
|---|---|
| **Cellular Interfaces** | |
| Connectors | 2 × 50 Ω SMA (Center pin: female) |
| SIM Slots | 2 |
| **Hardware System** | |
| CPU | 800MHz, 64-bit ARM Cortex-A53 |
| Memory | 64 MB Flash, 256 MB DDR3 RAM |
| Storage | 1 × Micro SD |
| **Ethernet** | |
| Ports | 1 × RJ-45 |
| Physical Layer | 10/100/1000 Base-T (IEEE 802.3) |
| Data Rate | 10/100/1000 Mbps (auto-sensing) |
| Interface | Auto MDI/MDIX |
| Mode | Full or half duplex (auto-sensing) |
| **Serial Interface** | |
| Ports | 1 × RS232 or 1 × RS485 |
| Connector | DB9 Female |
| Baud Rate | 300bps to 230400bps |
| **Software** | |
| Network Protocols | PPP, PPPOE, SNMP v1/v2c/v3, TCP, UDP, DHCP, RIPv1/v2, OSPF, DDNS, VRRP, HTTP, HTTPS, DNS, ARP, QoS, SNTP, Telnet, VLAN, SSH, etc. |
| VPN Tunnel | DMVPN/IPsec/OpenVPN/PPTP/L2TP/GRE |
| Access Authentication | CHAP/PAP/MS-CHAP/MS-CHAPV2 |
| Firewall | ACL/DMZ/Port Mapping/MAC Binding |
| Management | Web, CLI, SMS, On-demand dial up |
| AAA | Radius, Tacacs+, LDAP, Local Authentication |
| Multilevel Authority | Multiple levels of user authority |
| Reliability | VRRP, Dual SIM Backup |
| Serial Port | Transparent (TCP Client/Server, UDP), Modbus Gateway (Modbus RTU to Modbus TCP) |
| **Power Supply and Consumption** | |
| Connector | 2-pin with 5.08 mm terminal block |
| Input Voltage | 9-48 VDC |

| | |
|---|---|
| Power Consumption | Typical 2 W (Max 3 W) |
| **Physical Characteristics** | |
| Ingress Protection | IP30 |
| Housing & Weight | Metal, 369 g (0.81 lb) |
| Dimensions | 100 x 96.1 x 30 mm (3.94 x 3.78 x 1.18 in) |
| Mounting | Desktop, wall or DIN rail mounting |
| **Others** | |
| Reset Button | 1 × RESET |
| LED Indicators | 1 × POWER, 1 × STATUS, 1 × VPN,<br>1 × SIM1, 1 × SIM2, 3 × Signal strength |
| Built-in | Watchdog, RTC, Timer |
| Certifications | RoHS, CE, FCC |
| EMC | IEC 61000-4-2 Level 3<br>IEC 61000-4-3 Level 4<br>IEC 61000-4-4 Level 3<br>IEC 61000-4-5 Level 4<br>IEC 61000-4-6 Level 3<br>IEC 61000-4-8 Level 4 |
| **Environmental** | |
| Operating Temperature | -40°C to 50°C (-40°F to 122°F) Reduced cellular performance above 60°C |
| Storage Temperature | -40°C to +85°C (-40°F to +185°F) |
| Ethernet Isolation | 1.5 kV RMS |
| Relative Humidity | 0% to 95% (non-condensing) at 25°C/77°F |

### 1.4 Dimensions (mm)

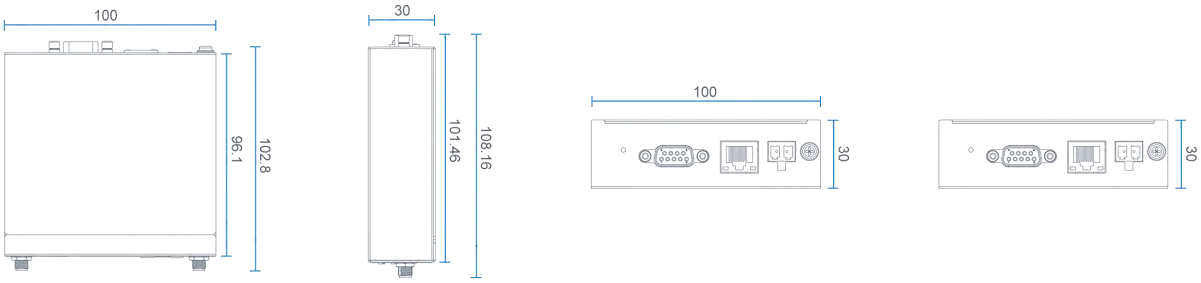
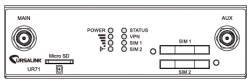



Figure 1-2

## Chapter 2 Installation

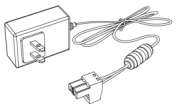
### 2.1 General Packing List

Before you begin to install the UR71 router, please check the package contents to verify that you have received the items below.



1 × UR71 Router

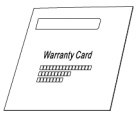
1 × Ethernet Cable



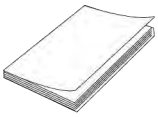
1 × Power Adapter

2 × SIM Card Slots

1 × 2-Pin Pluggable Terminal

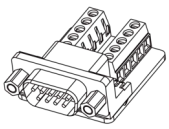



1 × Warranty Card

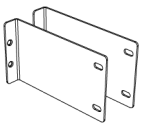


1 × Quick Start Guide

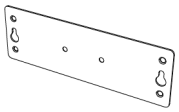
2 × Magnetic Mount Cellular Antennas (Default)



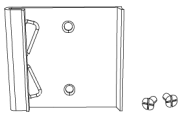
1 × Terminal Block with a DB9 Male Connector for Serial Port Connection (Optional)



2 × Rack Mount Kits (Default)



1 × Wall Mounting Bracket (Optional)

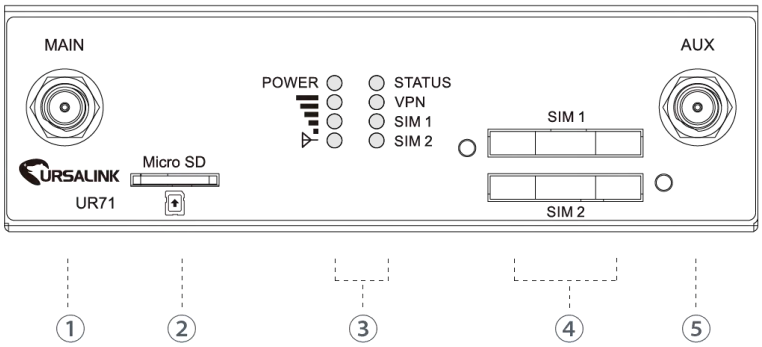


1 × DIN Rail Kit (Optional)

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

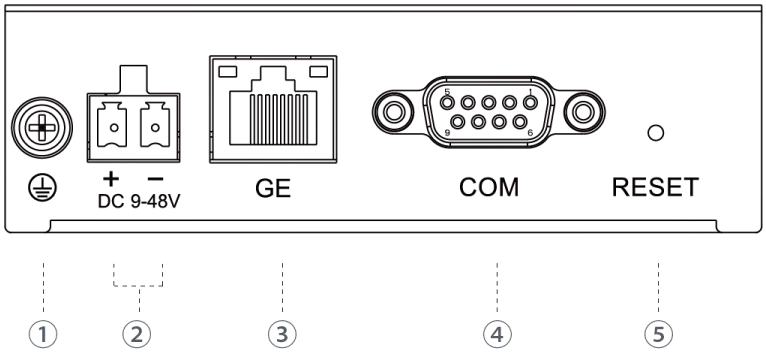
## 2.2 Product Overview

A. Front Panel




① Main Cellular Antenna
② Micro SD Card Interface
③ LED Indicator Area
POWER: Power Indicator
STATUS: Status Indicator
: Signal Strength Indicator
VPN: VPN Indicator
SIM1: SIM1 Status Indicator
SIM2: SIM2 Status Indicator
④ SIM Card Slot 1 & SIM Card Slot 2
⑤ AUX Cellular Antenna

B. Rear Panel




① Grounding Stud
② Power Connector
③ Ethernet Port Indicator:
Orange for data transmission;
Green for network rate
④ Serial Port: RS232 or RS485
⑤ Reset Button

## 2.3 LED Indicators

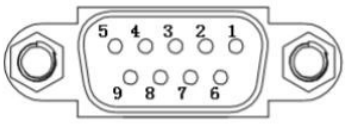
| LED | Indication | Status | Description |
|---|---|---|---|
| POWER | Power Status | On | The power is switched on |
| | | Off | The power is switched off |
| STATUS | System Status | Green Light | Static: Start-up |
| | | | Blinking slowly: the system is running properly |
| | | Off | The system goes wrong |
| VPN | VPN Status | Green Light | VPN is connected |

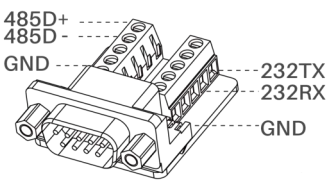
| | | | |
|---|---|---|---|
| | | Off | VPN is disconnected |
| SIM1/SIM2 | SIM Card Status | Off | SIM1 or SIM2 is registering or fails to register (or there are no SIM cards inserted) |
| | | Green Light | Blinking slowly: SIM1 or SIM2 has been registered and is ready for dial-up |
| | | | Blinking rapidly: SIM1 or SIM2 has been registered and is dialing up now |
| | | | Static: SIM1 or SIM2 has been registered and dialed up successfully |
| Signal Strength | Signal 1/2/3 | Off | No signal |
| | | Green Light | Static/Off/Off: weak signals with 1-10 ASU (please check if the antenna is installed correctly, or move the antenna to a suitable location to get better signal) |
| | | | Static/Static/Off: normal signals with 11-20 ASU (average signal strength) |
| | | | Static/Static/Static: strong signals with 21-31 ASU (signal is good) |

## 2.4 Ethernet Port Indicators

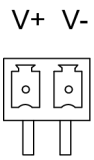
| Indicator | Status | Description |
|---|---|---|
| Link Indicator (Orange) | On | Connected |
| | Blinking | Transmitting data |
| | Off | Disconnected |
| Rate Indicator (Green) | On | 1000Mbps mode |
| | off | 100Mbps mode |

## 2.5 PIN Definition




| PIN | RS232 | RS485 | Description |
|---|---|---|---|
| 1 | --- | A | Data + |
| 2 | RXD | --- | Receive Data |
| 3 | TXD | --- | Transmit Data |
| 4 | --- | --- | --- |
| 5 | GND | --- | Ground |
| 6 | --- | B | Data - |
| 7 | --- | --- | --- |
| 8 | --- | --- | --- |
| 9 | --- | --- | --- |



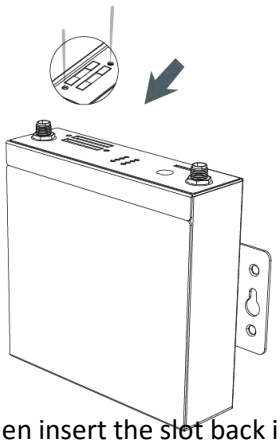

| PIN | Description |
|---|---|
| 11 | Positive |
| 12 | Negative |

## 2.6 Reset Button

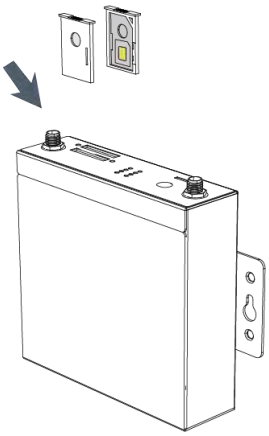
| Function | Description | |
|---|---|---|
| | STATUS LED | Action |
| Reboot | Blinking | Press and hold the reset button for about 5-15 seconds. |
| | Static Green | Release the button and wait for system to reboot. |
| Reset | Blinking | Press and hold the reset button for more than 15 seconds. |
| | Static Green → Rapidly Blinking | Release the button and wait. |
| | Off → Blinking | The router is now reset to factory defaults. |

## 2.7 SIM Card Installation

A. Push the yellow button on left panel of the router, and then you will see the SIM card slot popping out directly.

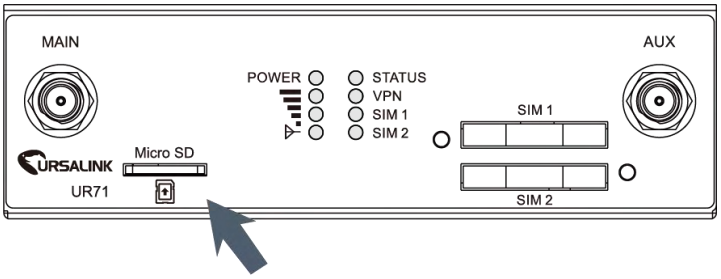


B. Put SIM card onto the slot, and then insert the slot back into the hole.



## 2.8 Micro SD card Installation

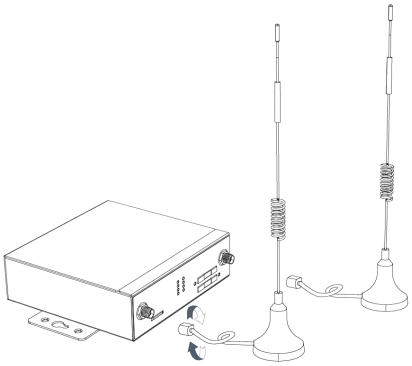
Insert Micro SD card




## 2.9 Cellular Antenna Installation

A. Rotate the antenna into the Antenna Connector.

The external cellular antenna should be installed vertically always on a site with a good cellular signal.



**Note: UR71 router supports dual antennas with "Main" and "AUX" connectors. "Main" interface is for data receiving and transmission. "AUX" interface is for enhancing signal strength, which cannot be used separately.**

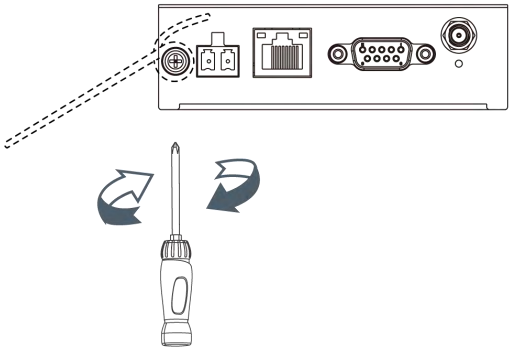
## 2.10 Mounting the Router

The router can be placed on a desktop or mounted to a wall or a DIN rail.

### 2.10.1 Wall Mounting (Measured in mm)

Use 2 pcs of M3×6 flat head Phillips screws to fix the wall mounting kit to the router, and then use 2 pcs of M3 drywall screws to mount the router associated with the wall mounting kit on the wall.

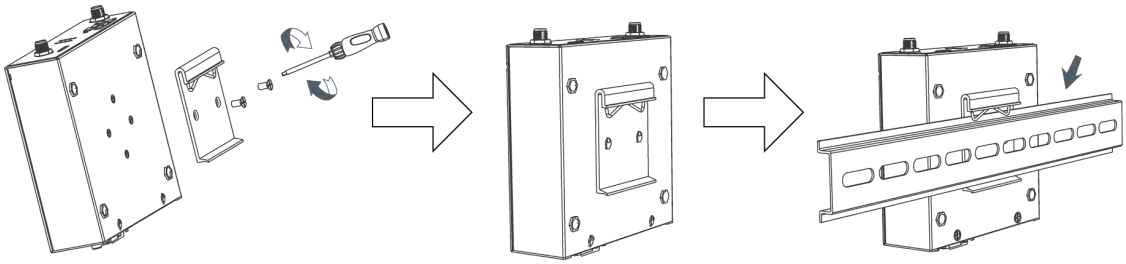
**Recommended torque for mounting is 1.0 N. m, and the maximum allowed is 1.2 N.m.**



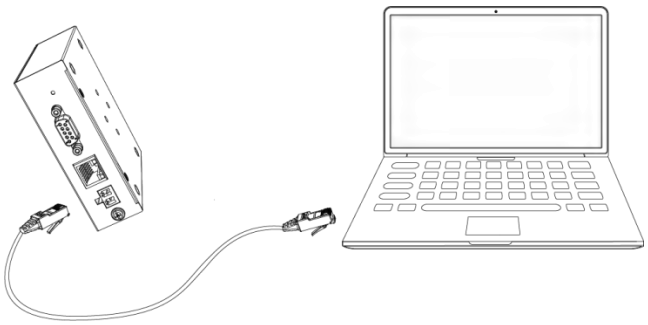
### 2.10.2 DIN Rail Mounting (Measured in mm)

Use 2 pcs of M3×6 flat head Phillips screws to fix the DIN rail to the router, and then hang the DIN rail on the mounting bracket. It is necessary to choose a standard bracket.

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



## 2.11 Connect the Router to a Computer

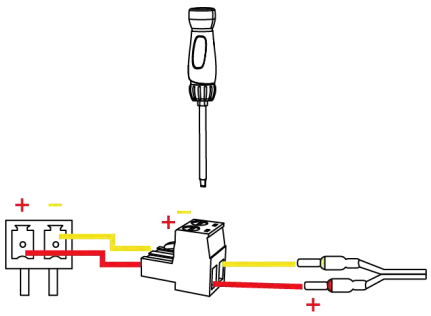


## 2.12 Installation of Power Supply and Protective Grounding

### 2.12.1 Power Supply Installation

A. Take out the terminal from the router and unscrew the bolt on terminal.

B. Screw down the bolt after inserting power cable into the terminal.



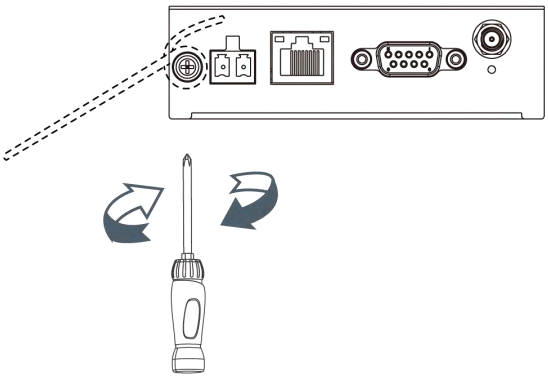

Connecting the Power Cable

| Color | Polarity |
|---|---|
| Red | + |
| Yellow | - |

**If you insert wires into the reverse holes, the router will not start and you must switch the wires into the correct holes.**

### 2.12.2 Protective Grounding Installation

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



**The router must be grounded when deployed. According to operating environment, the ground wire should be connected with grounding stud of router.**

## 2.13 Examine

1. Double check antenna connection.
2. Double check if SIM card is inserted and become available.
3. Power on the UR71 wireless cellular router and check indicators status.

(1) If Status LED blinks slowly, the system is running properly.

(2) If SIM1 or SIM2 indicator is static green, the router is connected to network already.

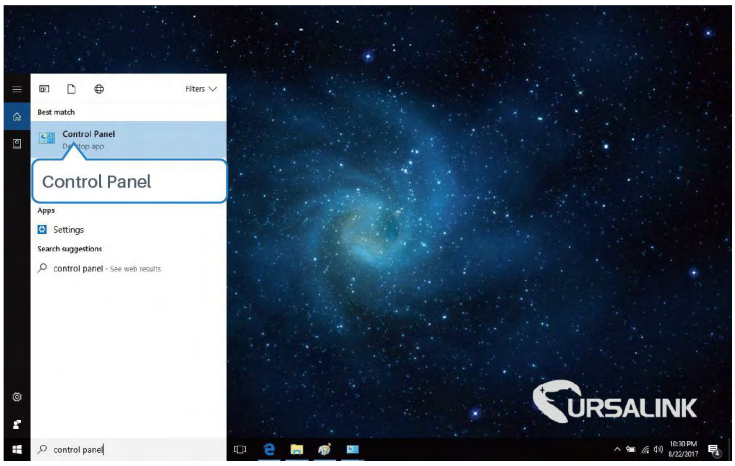
# Chapter 3 Access to Web GUI

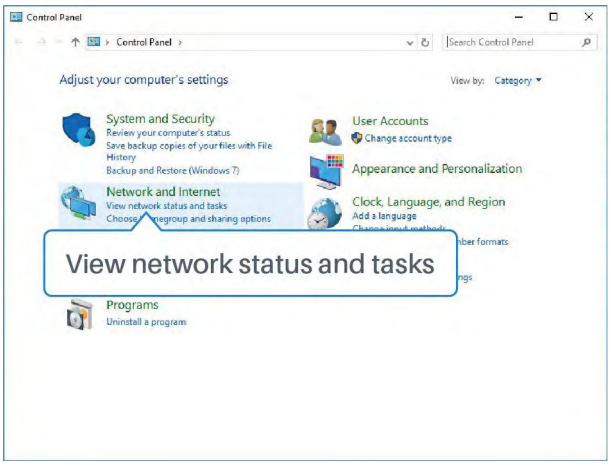
This chapter explains how to access to Web GUI of the UR71 router.

## 3.1 PC Configuration for Web GUI Access to Router

Please connect PC to GE port of UR71 router directly. PC can obtain an IP address, or you can configure a static IP address manually. The following steps are based on Windows 10 operating system for your reference.

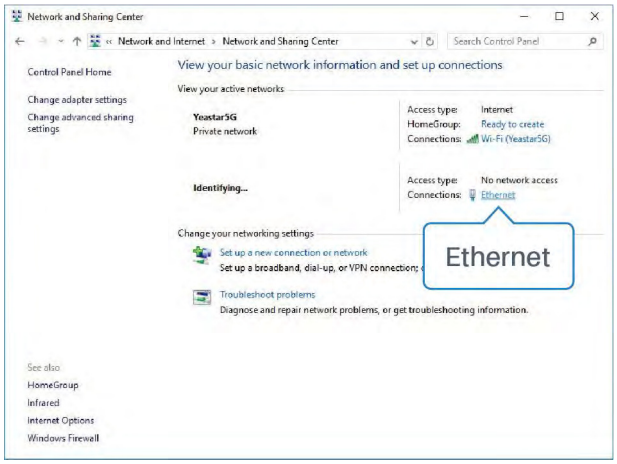
**The following steps are based on Windows 10 operating system for your reference.**

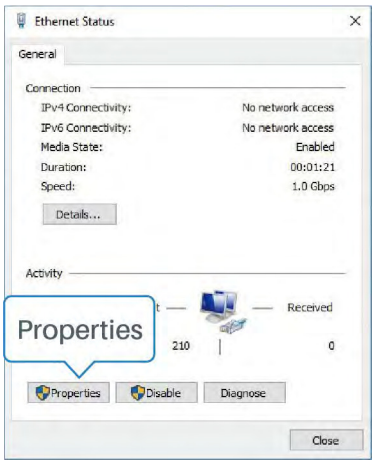



①Click "Search Box" to search "Control Panel" on the Windows 10 taskbar.

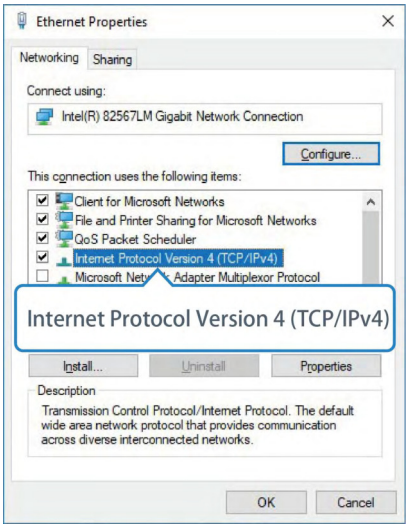
② Click “Control Panel” to open it, and then click “View network status and tasks”.



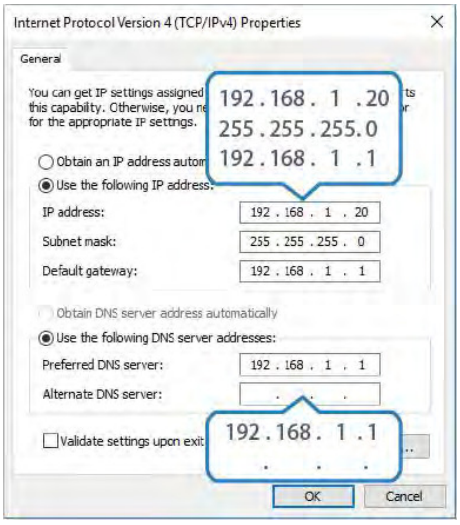

③ Click "Ethernet" (May have different name).

④ Click "Properties".




⑤ Double Click "Internet Protocol Version 4 (TCP/IPv4)" to configure IP address and DNS server.

⑥ Method 1: click "Obtain an IP address automatically";




Method 2: click "Use the following IP address" to assign a static IP manually within the same subnet of the router.

(Note: remember to click “OK” to finish configuration.)

### 3.2 Access to Web GUI of Router

Ursalink router provides Web-based configuration interface for management. If this is the first time you configure the router, please use the default settings below.

**Username**: admin

**Password**: password

**IP Address**: 192.168.1.1

**DHCP Server**: Enabled

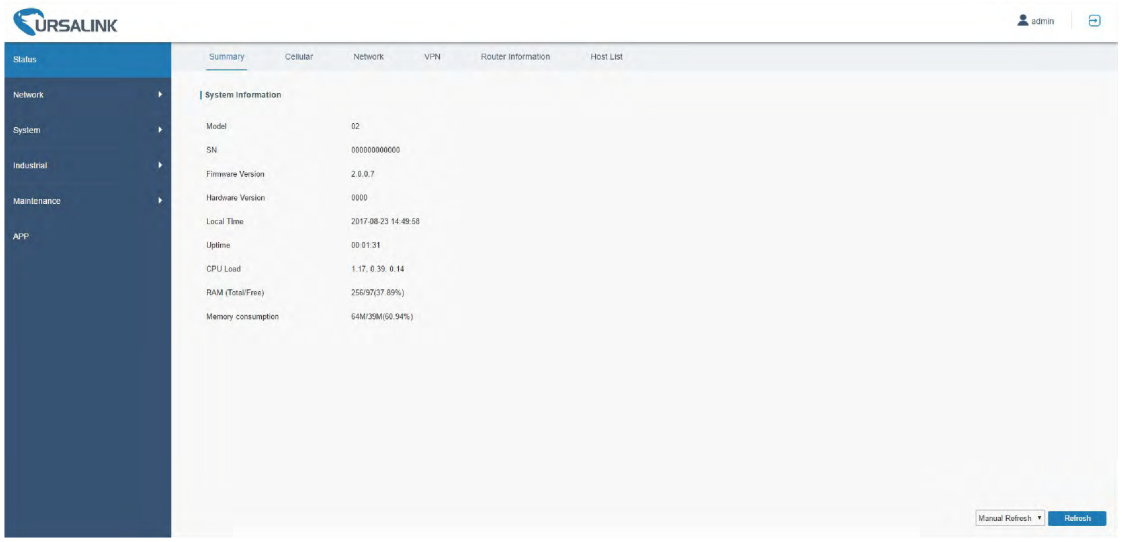
1. Start a Web browser on your PC (Chrome and IE are recommended), type in the IP address, and press Enter on your keyboard.
2. Enter the username, password, and click "Login".

If the SIM card is connected to cellular network with public IP address, you can access WEB GUI remotely via the public IP address when remote access is enabled.

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

3. 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.

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




## Chapter 4 Web Configuration

## 4.1 Status

### 4.1.1 Overview

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

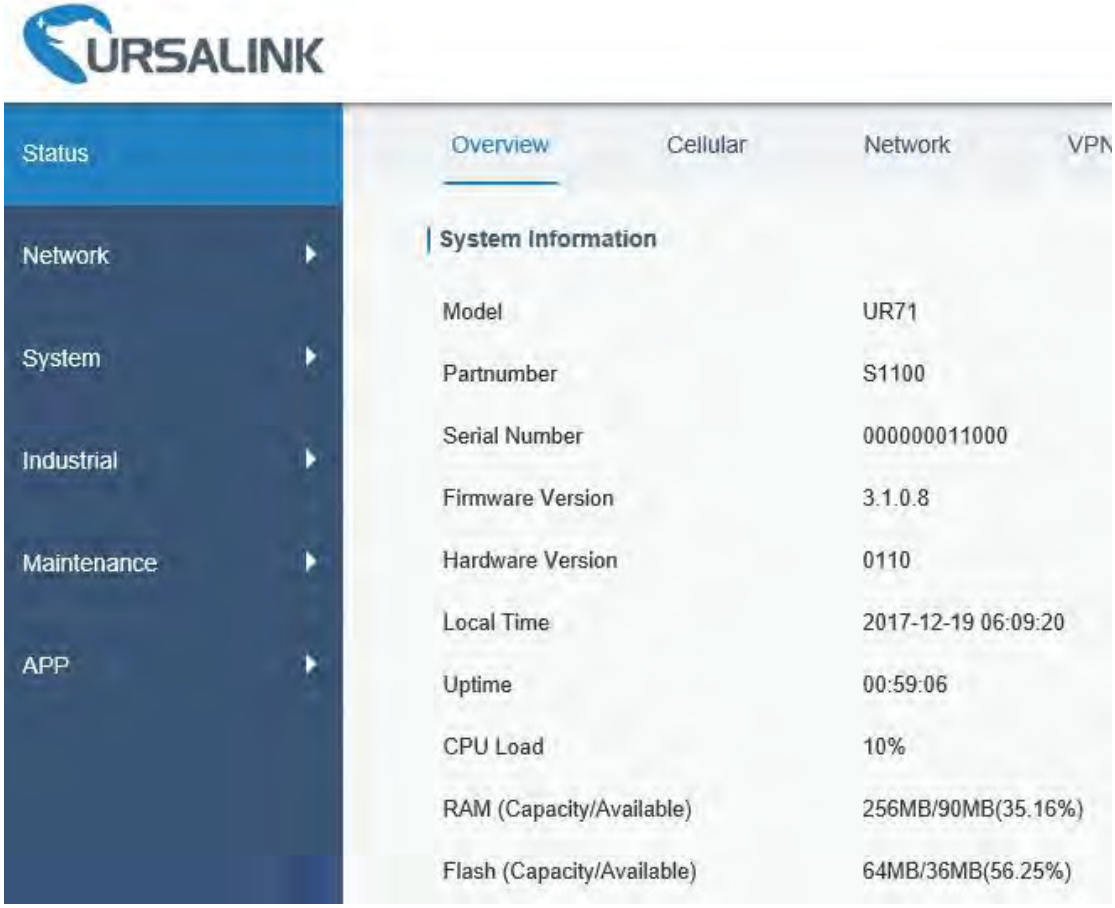



Figure 4-1-1-1

| System Information | |
|---|---|
| **Item** | **Description** |
| Model | Show the model name of router. |
| Serial Number | Show the serial number of router. |
| Firmware Version | Show the currently firmware version of router. |
| Hardware Version | Show the currently hardware version of router. |
| 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. |
| RAM (Capacity/Available) | Show the RAM capacity and the available RAM memory. |
| Flash (Capacity/Available) | Show the Flash capacity and the available Flash memory. |

Table 4-1-1-1 System Information

### 4.1.2 Cellular

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

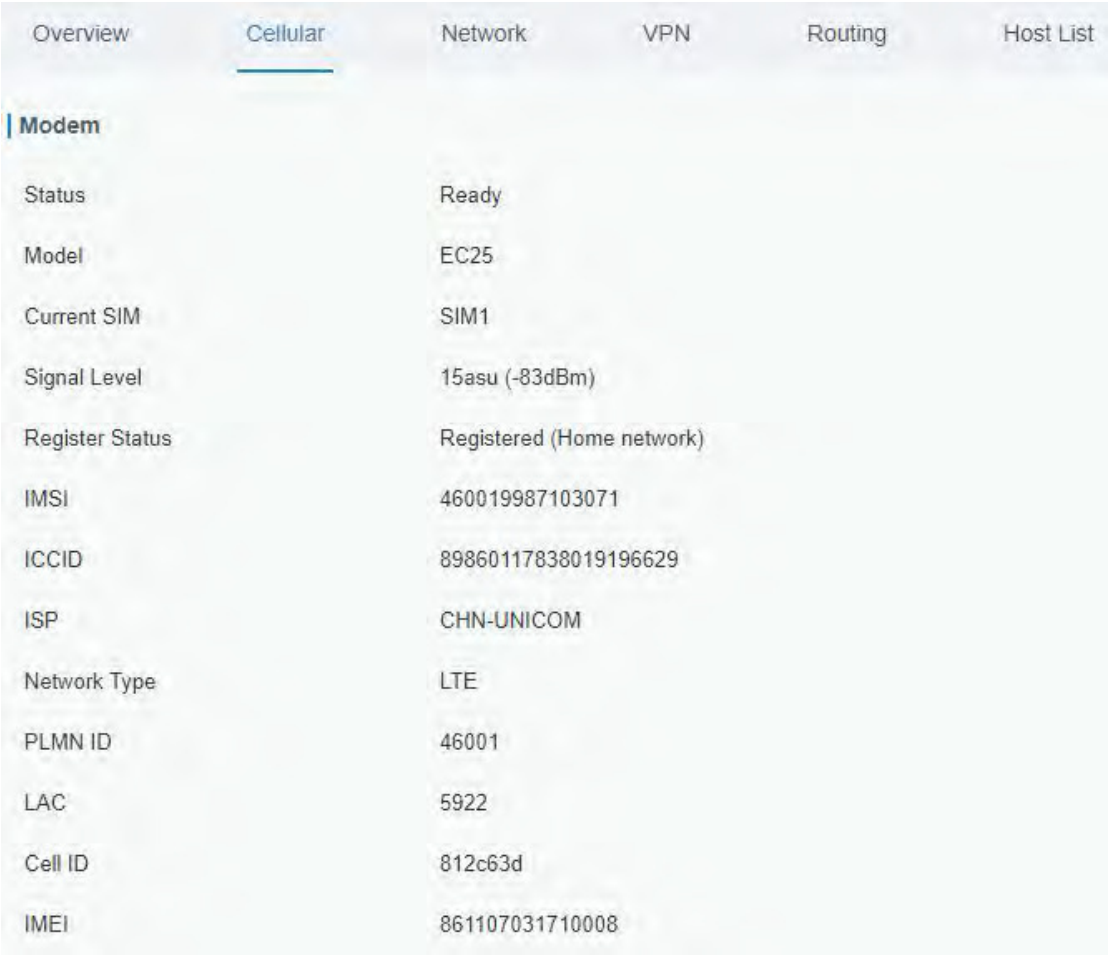



Figure 4-1-2-1

| Modem Information | |
|---|---|
| **Item** | **Description** |
| Status | Show corresponding detection status of module and SIM card. |
| Model | Show the model name of cellular module. |
| Current SIM | Show the current SIM card used. |
| Signal Level | Show the cellular signal level. |
| Register Status | Show the registration status of SIM card. |
| 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. |
| IMEI | Show the IMEI of the module. |

Table 4-1-2-1 Modem Information

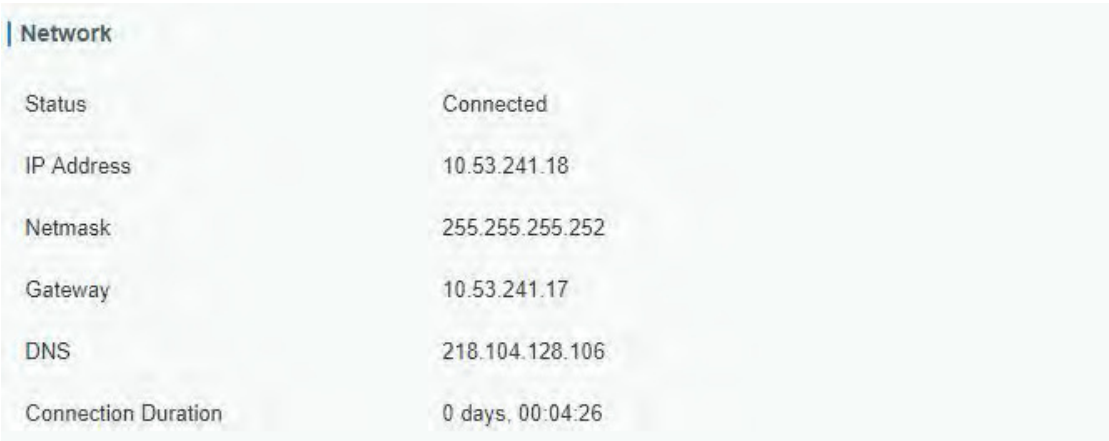



Figure 4-1-2-2

| Network Status | |
|---|---|
| **Item** | **Description** |
| Status | Show the connection status of cellular network. |
| IP Address | Show the IP address of cellular network. |
| Netmask | Show the netmask of cellular network. |
| Gateway | Show the gateway of cellular network. |
| DNS | Show the DNS of cellular network. |
| Connection Duration | Show information on how long the cellular network has been connected. |

Table 4-1-2-2 Network Status

### 4.1.3 Network

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

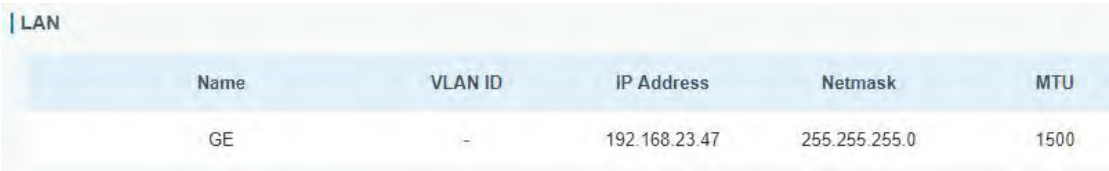



Figure 4-1-3-1

| LAN Status | |
|---|---|
| **Item** | **Description** |
| Port | Show the name of LAN port. |
| VLAN ID | Show the label ID of the VLAN. |
| IP Address | Show the LAN port's IP address. |
| Netmask | Show the LAN port's netmask. |
| MTU | Show the maximum transmission unit of LAN port. |

Table 4-1-3-1 LAN Status

### 4.1.4 VPN

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

Overview | Cellular | Network | VPN | Routing | Host List

**PPTP Tunnel**

| Name | Status | Local IP | Remote IP |
|---|---|---|---|
| pptp_1 | Disconnected | - | - |
| pptp_2 | Disconnected | - | - |
| pptp_3 | Disconnected | - | - |

**L2TP Tunnel**

| Name | Status | Local IP | Remote IP |
|---|---|---|---|
| l2tp_1 | Disconnected | - | - |
| l2tp_2 | Disconnected | - | - |
| l2tp_3 | Disconnected | - | - |

Figure 4-1-4-1

Overview | Cellular | Network | VPN | Routing | Host List

**IPsec Tunnel**

| Name | Status | Local IP | Remote IP |
|---|---|---|---|
| ipsec_1 | Disconnected | - | - |
| ipsec_2 | Disconnected | - | - |
| ipsec_3 | Disconnected | - | - |

**OpenVPN Client**

| Name | Status | Local IP | Remote IP |
|---|---|---|---|
| openvpn_1 | Disconnected | - | - |
| openvpn_2 | Disconnected | - | - |
| openvpn_3 | Disconnected | - | - |

Figure 4-1-4-2

GRE Tunnel

| Name | Status | Local IP | Remote IP |
|---|---|---|---|
| gre_1 | Disconnected | - | - |
| gre_2 | Disconnected | - | - |
| gre_3 | Disconnected | - | - |

DMVPN Tunnel

| Name | Status | Local IP | Remote IP |
|---|---|---|---|
| dmvpn | Disconnected | - | - |

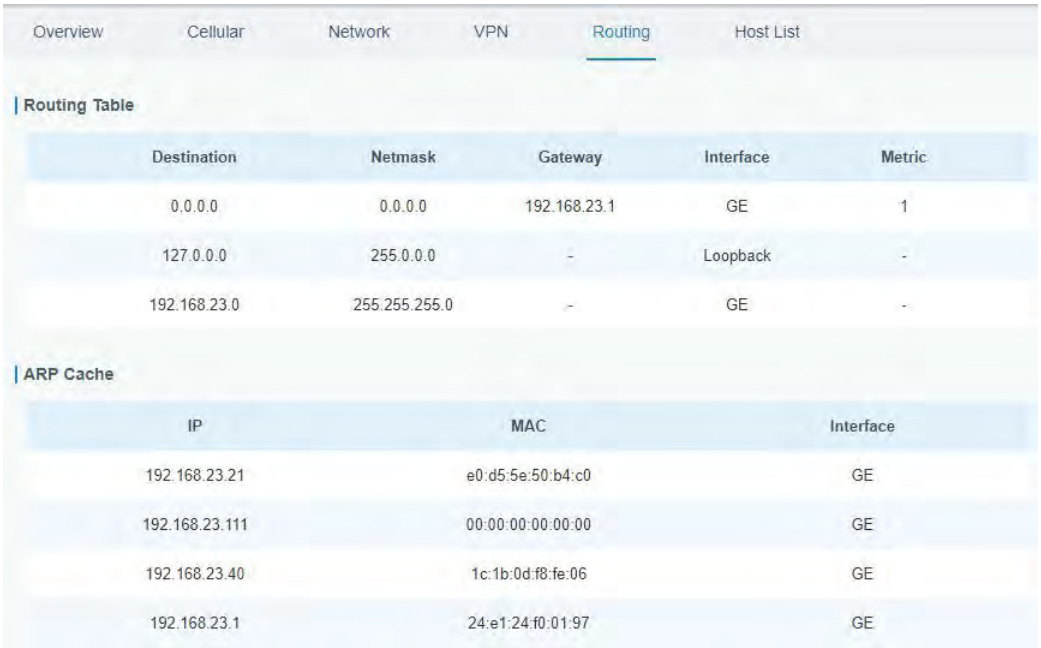
Figure 4-1-4-3

| VPN Status | |
|---|---|
| **Item** | **Description** |
| Name | Show the name of the VPN tunnel. |
| Status | Show the status of the VPN tunnel. |
| Local IP | Show the local tunnel IP of VPN tunnel. |
| Remote IP | Show the remote tunnel IP of VPN tunnel. |

Table 4-1-4-1 VPN Status

### 4.1.5 Routing Information

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



Overview Cellular Network VPN Routing Host List

Routing Table

| Destination | Netmask | Gateway | Interface | Metric |
|---|---|---|---|---|
| 0.0.0.0 | 0.0.0.0 | 192.168.23.1 | GE | 1 |
| 127.0.0.0 | 255.0.0.0 | - | Loopback | - |
| 192.168.23.0 | 255.255.255.0 | - | GE | - |

ARP Cache

| IP | MAC | Interface |
|---|---|---|
| 192.168.23.21 | e0:d5:5e:50:b4:c0 | GE |
| 192.168.23.111 | 00:00:00:00:00:00 | GE |
| 192.168.23.40 | 1c:1b:0d:f8:fe:06 | GE |
| 192.168.23.1 | 24:e1:24:f0:01:97 | GE |

Figure 4-1-5-1

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

Table 4-1-5-1 Routing Information

### 4.1.6 Host List

You can view the host information on this page.

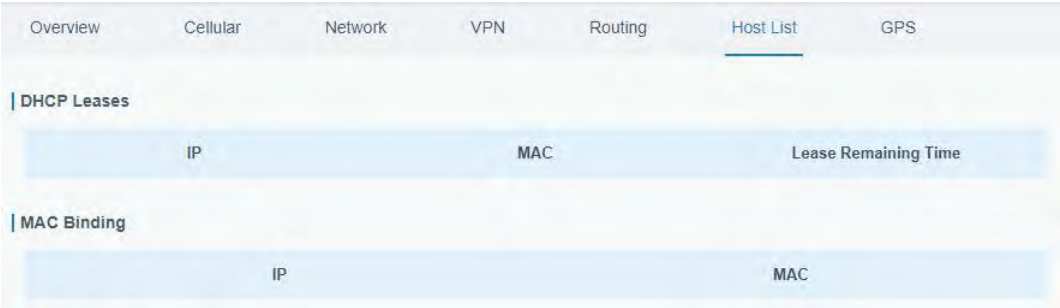



Figure 4-1-6-1

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

Table 4-1-6 Host List Description

## 4.2 Network

### 4.2.1 Interface

#### 4.2.1.1 Port

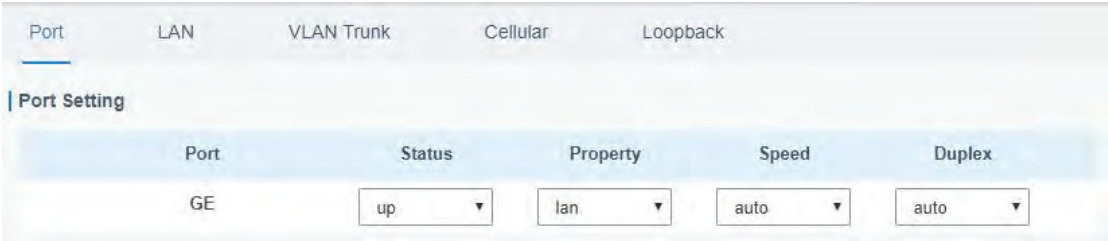



Figure 4-2-1-1

| 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. |
| Property | LAN. User cannot change this setting. |
| Speed | Set the Ethernet port's speed. The options are "auto", "1000 Mbps", "100 Mbps", and "10 Mbps". |
| Duplex | Set the Ethernet port's mode. The options are "auto", "full", and "half". |

Table 4-2-1-1 Port Parameters

#### 4.2.1.2 LAN

LAN setting is used for managing local area network devices which are connected to LAN port of the UR71, allowing each of them to access the Internet.

Click ✕ to delete the existing LAN port setting. Click + to add a new LAN port setting.

Figure 4-2-1-2

| LAN | | |
|---|---|---|
| **Item** | **Description** | **Default** |
| Interface | Select LAN port. | GE 0 |
| IP Address | Set IP address of LAN port. | 192.168.1.1 |
| Netmask | Set Netmask of LAN port. | 255.255.255.0 |
| MTU | Set the maximum transmission unit of LAN port. Range: 68-1500. | 1500 |

Table 4-2-1-2

**Related Configuration Example**

LAN Management

### 4.2.1.3 VLAN Trunk

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

Client to delete the current VLAN setting. Click to add a new VLAN port.

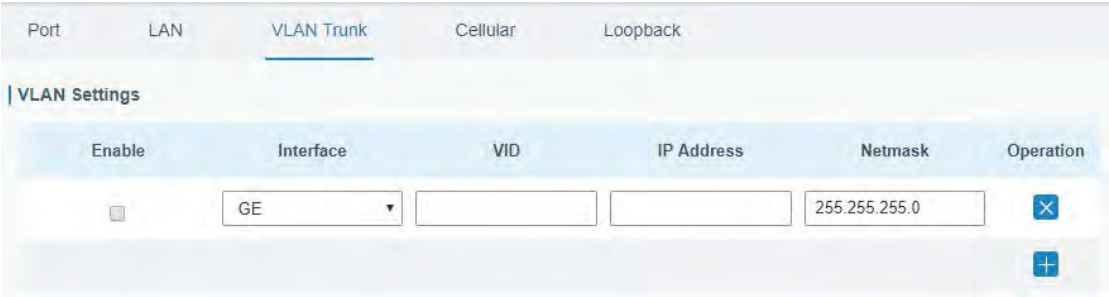



Figure 4-2-1-3

| VLAN Trunk | |
|---|---|
| **Item** | **Description** |
| Enable | The router can encapsulate or decapsulate the virtual LAN tag when this function is enabled. |
| Interface | Select the VLAN interface from the LAN ports. |
| VID | Set the label ID of the VLAN. Range: 1-4094. |
| IP Address | Set VLAN port's IP address. |
| Netmask | Set VLAN port's netmask. |

Table 4-2-1-3 VLAN Trunk Parameters

### 4.2.1.4 Cellular

This section explains how to set the related parameters for cellular network. The UR71 cellular router has two cellular interfaces, namely SIM1 and SIM2. Only one cellular interface is active at one time. If both cellular interfaces are enabled, then SIM1 interface takes precedence by default.

A typical use case would be to have SIM1 configured as the primary cellular interface and SIM2 as a backup. If the UR71 cannot connect to the network via SIM1, it will automatically fail over to SIM2.

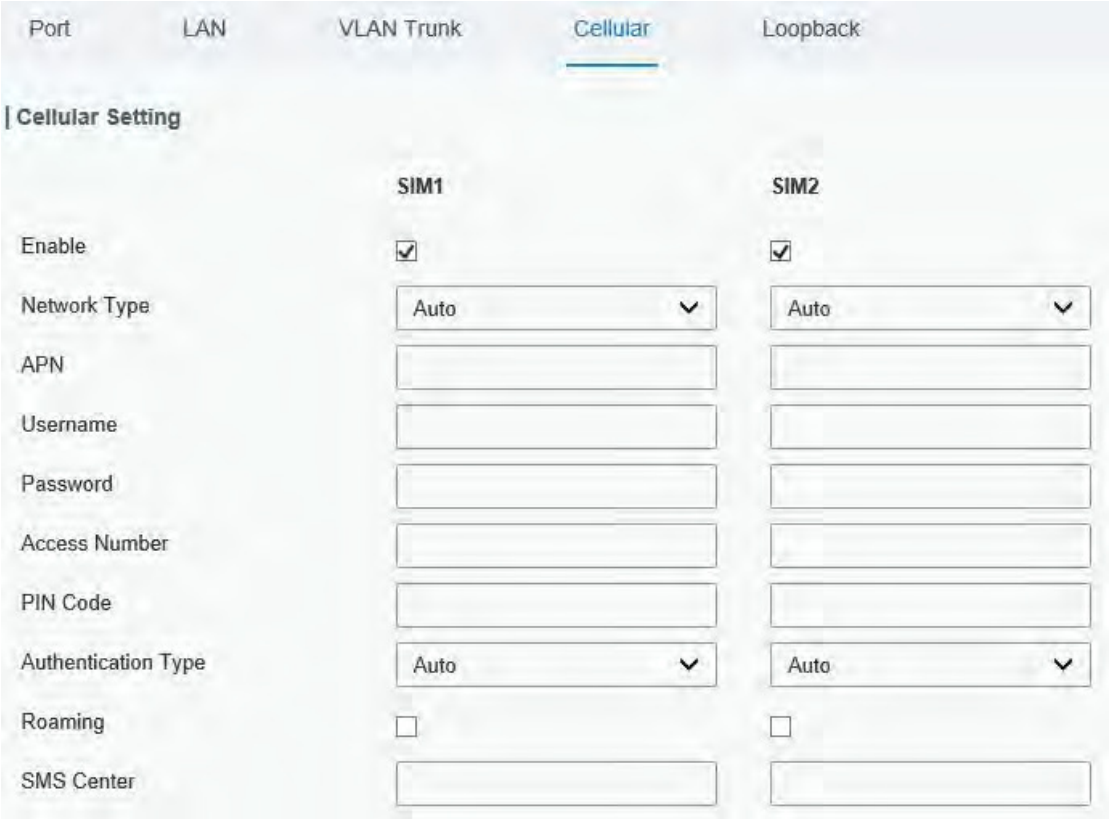



Figure 4-2-1-4

Figure 4-2-1-5

| General Settings | | |
|---|---|---|
| **Item** | **Description** | **Default** |
| Enable | Check the option to enable the corresponding SIM card. | Enable |

| | | |
|---|---|---|
| Network Type | Select from "Auto", "4G First", "4G Only", "3G First", "3G Only".<br>Auto: connect to the network with the strongest signal automatically.<br>4G First: 4G network takes precedence.<br>4G Only: connect to 4G network only.<br>And so on. | Auto |
| APN | Enter the Access Point Name for cellular dial-up connection provided by local ISP. | Null |
| Username | Enter the username for cellular dial-up connection provided by local ISP. | Null |
| Password | Enter the password for cellular dial-up connection provided by local ISP. | Null |
| Access Number | Enter the dial-up center NO. For cellular dial-up connection provided by local ISP. | Null |
| PIN Code | Enter a 4-8 characters PIN code to unlock the SIM. | Null |
| Authentication Type | Select from "Auto", "PAP", "CHAP", "MS-CHAP", and "MS-CHAPv2". | Auto |
| Roaming | Enable or disable roaming. | Disable |
| SMS Center | Enter the local SMS center number for storing, forwarding, converting and delivering SMS message. | Null |
| Enable NAT | Enable or disable NAT function. | Enable |
| ICMP Server | Set the ICMP detection server's IP address. | 8.8.8.8 |
| Secondary ICMP Server | Set the secondary ICMP detection server's IP address. | 114.114.114.114 |
| PING Times | Set PING packet numbers in each ICMP detection. | 5 |
| Packet Loss Rate | Set packet loss rate in each ICMP detection. ICMP detection fails when the preset packet loss rate is exceeded. | 20 |

Table 4-2-1-4 Cellular Parameters

Figure 4-2-5

| Item | Description |
|---|---|
| **Connection Mode** | |
| Connection Mode | Select from "Always Online" and "Connect on Demand". |
| Connect on Demand | "Connect on Demand" includes "Triggered by Call", "Triggered by SMS", and "Triggered by IO". |
| 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. |
| **Dual SIM Strategy** | |
| Current SIM Card | Select between "SIM1" and "SIM2" as a current SIM card used. |
| Switch to backup SIM card when ICMP detection fails | The router will switch to the backup SIM card when packet loss rate in IMCP detection exceeds the preset value. |
| Switch to backup SIM card when the connection fails | The router will switch to the backup SIM card when the primary one fails to connect with cellular network. |
| Switch to backup SIM card when | The router will switch to the backup SIM card when the primary one is roaming. |

| | |
|---|---|
| roaming is detected | |

Table 4-2-1-5 Cellular Parameters

**Related Topics**

Cellular Connection Application Example

Dual SIM Backup Application Example

Phone Group

#### 4.2.1.5 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.

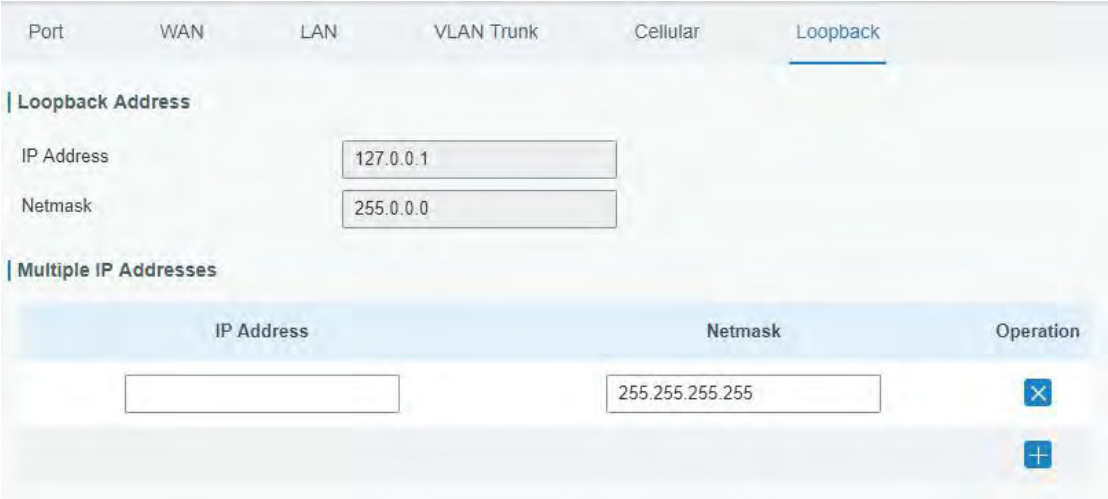



Figure 4-2-1-6

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

Table 4-2-1-6 Loopback Parameters

### 4.2.2 Firewall

This section describes how to set the firewall parameters, including ACL, DMZ, Port Mapping

and MAC Binding.

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.

#### 4.2.2.1 ACL

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

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

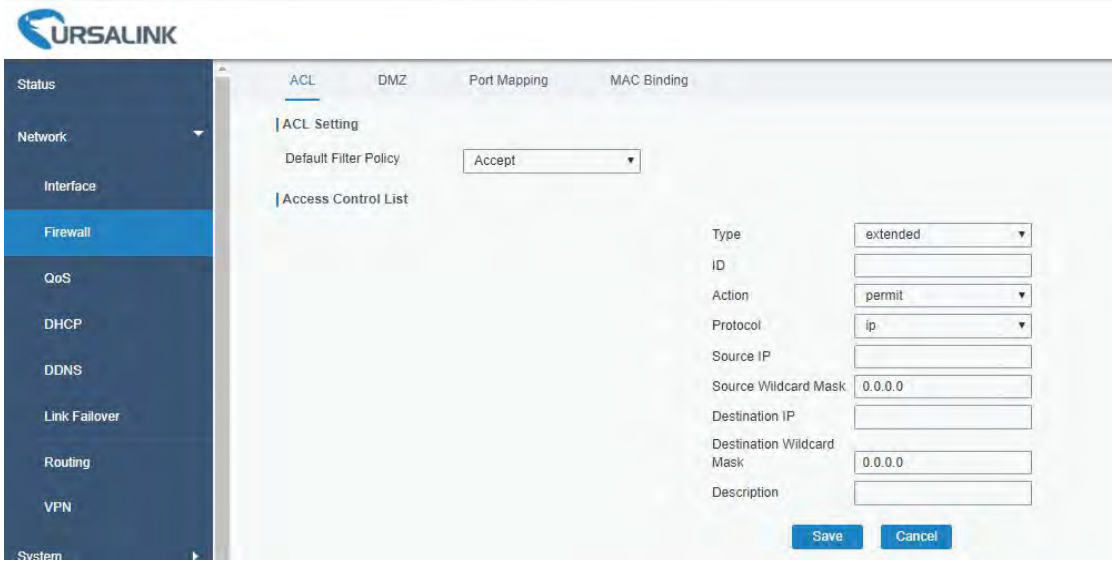



Figure 4-2-2-1

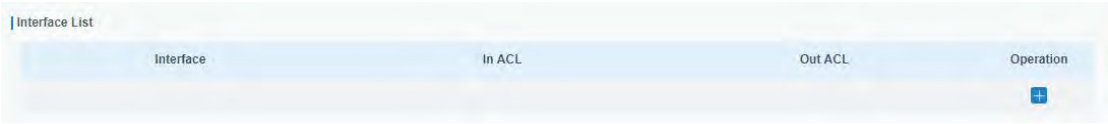



Figure 4-2-2-2

| Item | Description |
|---|---|
| **ACL Setting** | |
| Default Filter Policy | Select from "Accept" and "Deny".<br>The packets which are not included in the access control list will be processed by the default filter policy. |
| **Access Control List** | |
| Type | Select type from "Extended" and "Standard". |
| ID | User-defined ACL number. Range: 1-199. |
| Action | Select from "Permit" and "Deny". |
| Protocol | Select protocol from "ip", "icmp", "tcp", "udp", and "1-255". |

| | |
|---|---|
| Source IP | Source network address (leaving it blank means all). |
| Source Wildcard Mask | Wildcard mask of the source network address. |
| Destination IP | Destination network address (0.0.0.0 means all). |
| Destination Wildcard Mask | Wildcard mask of destination address. |
| Description | Fill in a description for the groups with the same ID. |
| ICMP Type | Enter the type of ICMP packet. Range: 0-255. |
| ICMP Code | Enter the code of ICMP packet. Range: 0-255. |
| Source Port Type | Select source port type, such as specified port, port range, etc. |
| Source Port | Set source port number. Range: 1-65535. |
| Start Source Port | Set start source port number. Range: 1-65535. |
| End Source Port | Set end source port number. Range: 1-65535. |
| Destination Port Type | Select destination port type, such as specified port, port range, etc. |
| Destination Port | Set destination port number. Range: 1-65535. |
| Start Destination Port | Set start destination port number. Range: 1-65535. |
| End Destination Port | Set end destination port number. Range: 1-65535. |
| More Details | Show information of the port. |
| **Interface List** | |
| Interface | Select network interface for access control. |
| In ACL | Select a rule for incoming traffic from ACL ID. |
| Out ACL | Select a rule for outgoing traffic from ACL ID. |

Table 4-2-2-1 ACL Parameters

**Related Configuration Example**

Access Control Application Example

#### 4.2.2.2 DMZ

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

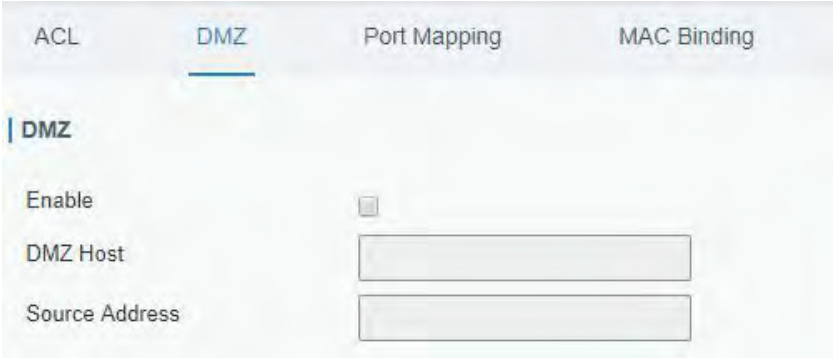



Figure 4-2-2-3

| DMZ |
|---|

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

Table 4-2-2-2 DMZ Parameters

#### 4.2.2.3 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.

Click to add a new port mapping rules.

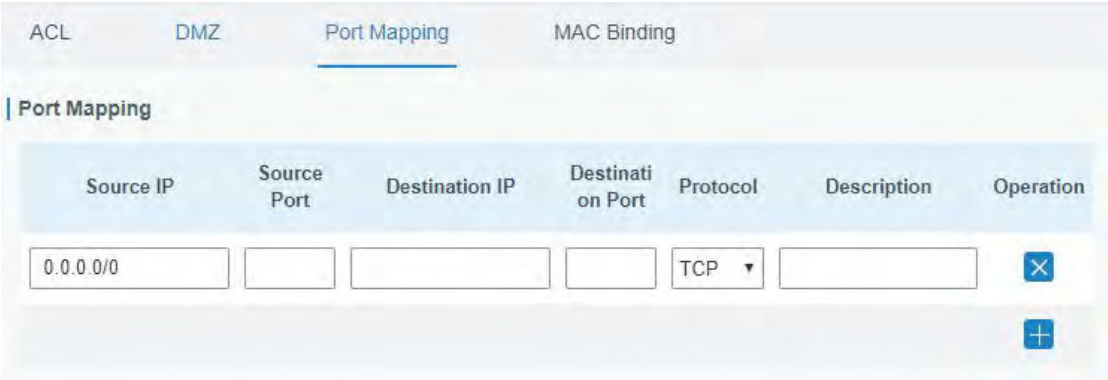



Figure 4-2-2-4

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

Table 4-2-2-3 Port Mapping Parameters

**Related Configuration Example**

NAT Application Example

#### 4.2.2.4 MAC Binding

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

Figure 4-2-2-5

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

Table 4-2-2-4 MAC Binding Parameters

### 4.2.3 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.

#### 4.2.3.1 QoS (Download/Upload)

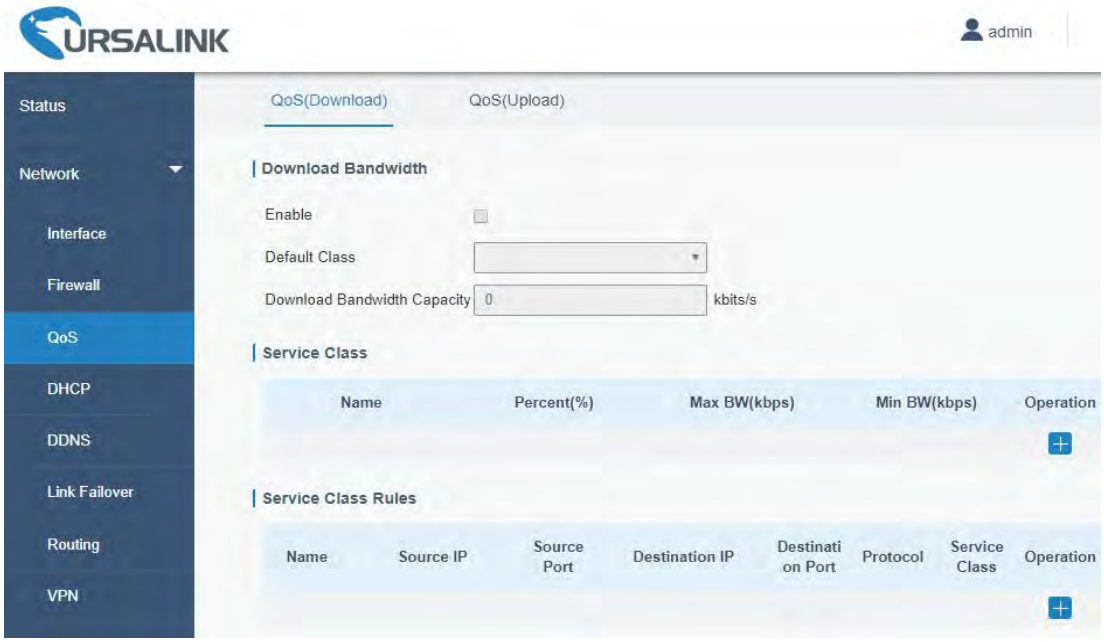



Figure 4-2-3-1

| QoS | |
|---|---|
| **Item** | **Description** |
| **Download/Upload** | |
| Enable | Enable or disable QoS. |
| Default Class | Select default class from Service Class 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 Class** | |
| Name | Give the service class a descriptive name. |
| Percent (%) | The amount of bandwidth that this class should be guaranteed in percentage. Range: 0-100. |
| Max BW(kbps) | The maximum bandwidth that this class is allowed to consume, in kbps. The value should be less than the "Download/Upload Bandwidth Capacity". |
| Min BW(kbps) | The minimum bandwidth that can be guaranteed for the class, in kbps. The value should be less than the "MAX BW" value. |
| **Item** | **Description** |
| **Service Class Rules** | |
| 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 Class | Set service class for the rule. |

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

**Related Application Example**

QoS Application Example

### 4.2.4 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.

#### 4.2.4.1 DHCP Server

The UR71 can be set as a DHCP 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.

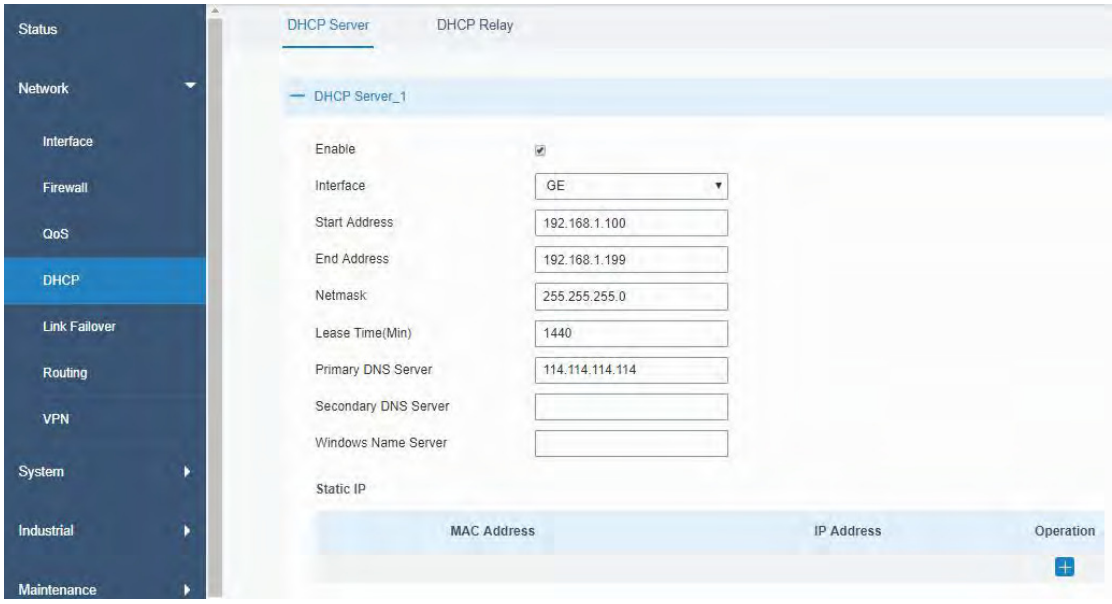



Figure 4-2-4-1

| DHCP Server | | |
|---|---|---|
| **Item** | **Description** | **Default** |
| Enable | Enable or disable DHCP server. | Enable |
| Interface | Select interface, e.g. GE. | GE |
| 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 IP address obtained by DHCP clients from DHCP server. | 255.255.255.0 |
| 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. | 114.114.114.114 |
| Secondary DNS Server | Set the secondary DNS server. | Null |
| Windows Name Server | Define the Windows Internet Naming Service obtained by DHCP clients from DHCP sever. Generally you can leave it blank. | Null |
| **Static IP** | | |
| MAC Address | Set a static and specific MAC address for the DHCP client (it should be different from other MACs so as to avoid conflict). | Null |
| IP Address | Set a static and specific IP address for the DHCP client (it should be outside of the DHCP range). | Null |

Table 4-2-4-1 DHCP Server Parameters

#### 4.2.4.2 DHCP Relay

The UR71 can be set as DHCP Relay to provide a relay tunnel to solve the problem that DHCP Client and DHCP Server are not in the same subnet.

Figure 4-2-4-2

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

Table 4-2-4-2 DHCP Relay Parameters

### 4.2.5 DDNS

Dynamic DNS (DDNS) is a method that automatically updates a name server in the Domain Name System, which allows user to alias a dynamic IP address to a static domain name.
DDNS serves as a client tool and needs to coordinate with DDNS server. Before starting configuration, user shall register on a website of proper domain name provider and apply for a domain name.

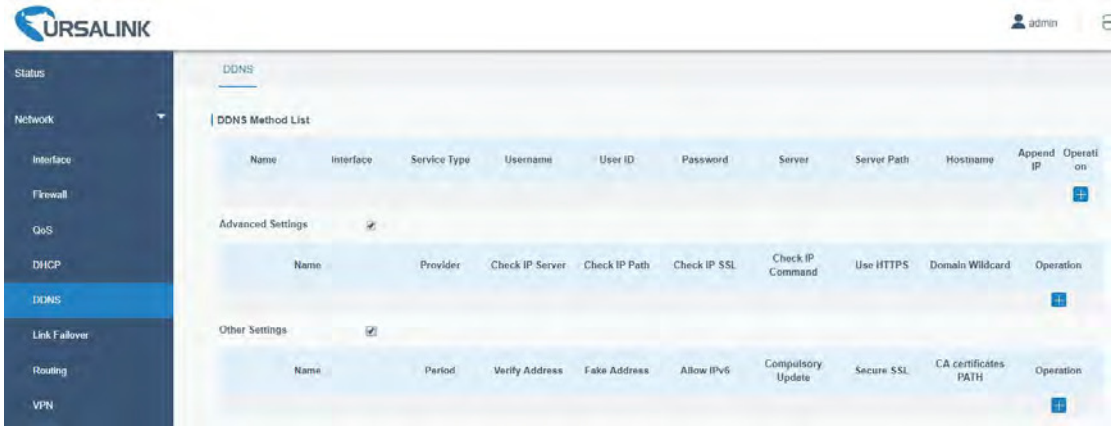



Figure 4-2-5-1

| DDNS | |
|---|---|
| **Item** | **Description** |
| 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. |
| Hostname | Enter the hostname for DDNS. |
| Append IP | Append your current IP to the DDNS server update path. |

Table 4-2-5-1 DDNS Parameters

| Item | Description |
|---|---|
| **Advanced Options** | |
| Name | Select the DDNS name. |
| Provider | Enter DDNS server provider. |
| Check IP Server | Server used for periodic IP address changes. |
| Check IP Path | Optional server path for check IP server. |
| Check IP SSL | This setting usually follows the SSL setting, but can be used to disable HTTPS for the IP address check. This might be needed for some providers that only support HTTPS for the DNS record update. |
| Check IP Command | Shell command, or script for IP address update checking. |

| | |
|---|---|
| Use HTTPS | Use HTTPS or not. |
| Domain Wildcard | Enable/disable domain name wildcard of your domain name. |
| **Other Options** | |
| Name | Select the DDNS name. |
| Period (s) | Decide how often is the IP address checked, in seconds. The default interval is 3600s. Range: 60-864000 |
| Verify Address | Verify IP address, making sure the address is a valid Internet address. |
| Fake Address | This option can be used to fake an address by updating with a "random" address in the 203.0.113.0/24 range. |
| Allow IPv6 | Allow or discard IPv6 addresses. |
| Forced Update (s) | Decide how often the IP should be updated even if it is not changed, in seconds. The default interval is 2592000 s (30 days). |
| Secure SSL | When this option is enabled, the DDNS update will be aborted before sending any credentials if the HTTPS certificate validation fails for a provider. When it's disabled, then will only a warning is issued. |
| CA Certificates PATH | Specify the path to a trusted set of CA certificates. |

Table 4-2-5-2 DDNS Parameters

### 4.2.6 Link Failover

This section describes how to configure link failover strategies, such as VRRP strategies.

**Configuration Steps**

1. Define one or more SLA operations (ICMP probe).
2. Define one or more track objects to track the status of SLA operation.
3. Define applications associated with track objects, such as VRRP or static routing.

#### 4.2.6.1 SLA

SLA setting is used for configuring link probe method. The default probe type is ICMP.

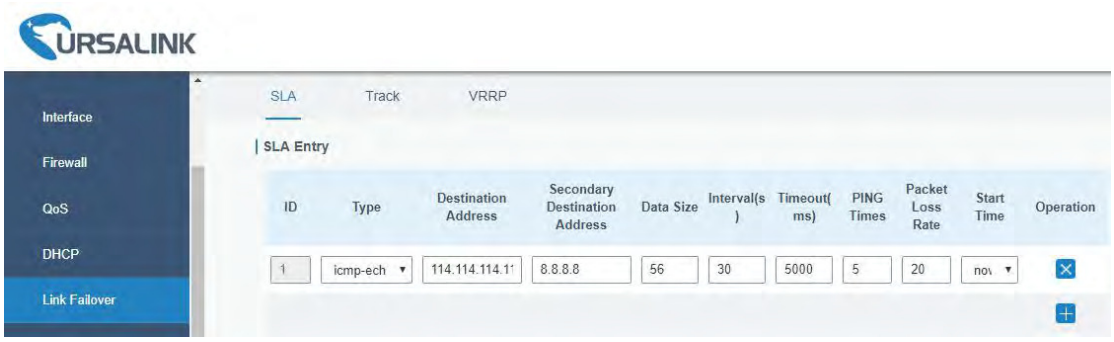



Figure 4-2-6-1

| SLA | | |
|---|---|---|
| **Item** | **Description** | **Default** |
| ID | SLA index. Up to 10 SLA settings can be added. Range: 1-10. | 1 |
| Type | ICMP-ECHO is the default type to detect if the link is alive. | icmp-echo |
| Destination Address | The detected IP address. | 114.114.114.114 |
| Secondary Destination Address | The secondary detected IP address. | 8.8.8.8 |
| Data Size | User-defined data size. Range: 0-1000. | 56 |
| Interval (s) | User-defined detection interval. Range: 1-608400. | 30 |
| Timeout (ms) | User-defined timeout for response to determine ICMP detection failure. Range: 1-300000. | 5000 |
| PING Times | Define PING packet numbers in each SLA probe. Range: 1-1000. | 5 |
| Packet Loss Rate | Define packet loss rate in each SLA probe. SLA probe fails when the preset packet loss rate is exceeded. | 20 |
| Start Time | Detection start time; select from "Now" and blank character. Blank character means this SLA detection doesn't start. | now |

Table 4-2-6-1 SLA Parameters

#### 4.2.6.2 Track

Track setting is designed for achieving linkage among SLA module, Track module and Application module. Track setting is located between application module and SLA module with main function of shielding the differences of various SLA modules and providing unified interfaces for application module.

**Linkage between Track Module and SLA module**

Once you complete the configuration, the linkage relationship between Track module and SLA module will be established. SLA module is used for detection of link status, network performance and notification of Track module. The detection results help track status change timely.

- For successful detection, the corresponding track item is Positive.
- For failed detection, the corresponding track item is Negative.

**Linkage between Track Module and Application Module**

After configuration, the linkage relationship between Track module and Application module will be established. When any change occurs in track item, a notification that requires corresponding treatment will be sent to Application module.

Currently, the application modules like VRRP and static routing can get linkage with track

module.

If it sends an instant notification to Application module, the communication may be interrupted in some circumstances due to routing's failure like timely restoration or other reasons. Therefore, user can set up a period of time to delay notifying application module when the track item status changes.

Figure 4-2-6-2

| Item | Description | Default |
|---|---|---|
| Index | Track index. Up to 10 track settings can be configured. Range: 1-10. | 1 |
| Type | The options are "sla" and "interface". | SLA |
| SLA ID | Defined SLA ID. | 1 |
| Interface | Select the interface whose status will be detected. | cellular0 |
| Negative Delay (s) | When interface is down or SLA probing fails, it will wait according to the time set here before actually changing its status to Down. Range: 0-180 (0 refers to immediate switching). | 0 |
| Positive Delay (s) | When failure recovery occurs, it will wait according to the time set here before actually changing its status to Up. Range: 0-180 (0 refers to immediate switching). | 1 |

Table 4-2-6-2 Track Parameters

#### 4.2.6.3 VRRP

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

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

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

routers in the same VRRP group.

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

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

VRRP has the following characteristics:

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

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

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

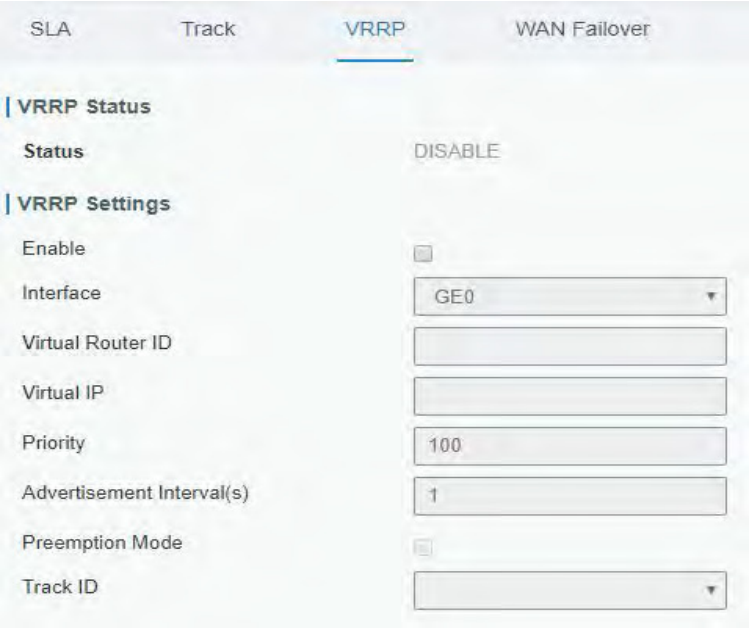



Figure 4-2-6-3

| 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 |
| Track ID | Trace detection, select the defined track ID or blank character. | None |

Table 4-2-6-3 VRRP Parameters

**Related Configuration Example**

VRRP Application Example

### 4.2.7 Routing

#### 4.2.7.1 Static Routing

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

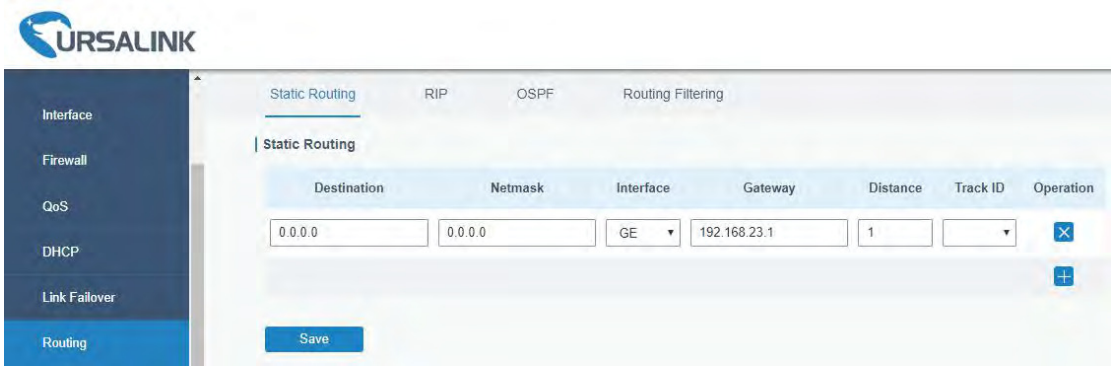



Figure 4-2-7-1

| Static Routing | |
|---|---|
| **Item** | **Description** |
| Destination | Enter the destination IP address. |
| Netmask | Enter the subnet mask 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. |
| Track ID | Track detection, select the defined track ID. You can leave it blank. |

Table 4-2-7-1 Static Routing Parameters

**Related Topic**

Track Setting

#### 4.2.7.2 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.

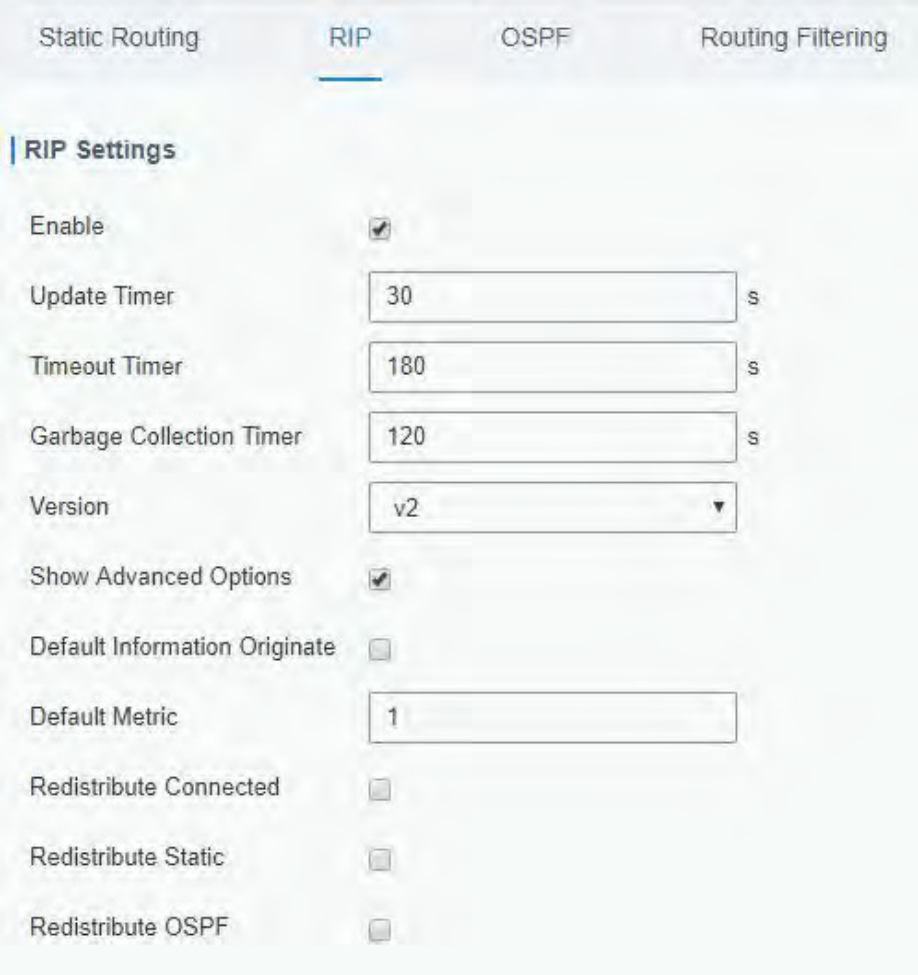



Figure 4-2-7-2

| RIP | |
|---|---|
| **Item** | **Description** |
| Enable | Enable or disable RIP. |
| Update Timer | It defines the interval to send routing updates. Range: 5-2147483647, in seconds. |
| Timeout Timer | It defines the routing aging time. If no update package on a routing is received within the aging time, the routing's Routing Cost in the routing table will be set to 16. Range: 5-2147483647, in seconds. |
| Garbage Collection Timer | It defines the period from the routing cost of a routing becomes 16 to it is deleted from the routing table. In the time of Garbage-Collection, RIP uses 16 as the routing cost for sending routing updates. If Garbage Collection times out and the routing still has not been updated, the routing will be completely removed from the routing table. Range: 5-2147483647, in seconds. |
| Version | RIP version. The options are v1 and v2. |

| Advanced Settings | |
|---|---|
| Default Information Originate | Default information will be released when this function is enabled. |
| Default Metric | The default cost for the router to reach destination. Range: 0-16 |
| Redistribute Connected | Check to enable. |
| Metric | Set metric after "Redistribute Connected" is enabled. Range: 0-16. |
| Redistribute Static | Check to enable. |
| Metric | Set metric after "Redistribute Static" is enabled. Range: 0-16. |
| Redistribute OSPF | Check to enable. |
| Metric | Set metric after "Redistribute OSPF" is enabled. Range: 0-16. |

Table 4-2-7-2 RIP Parameters

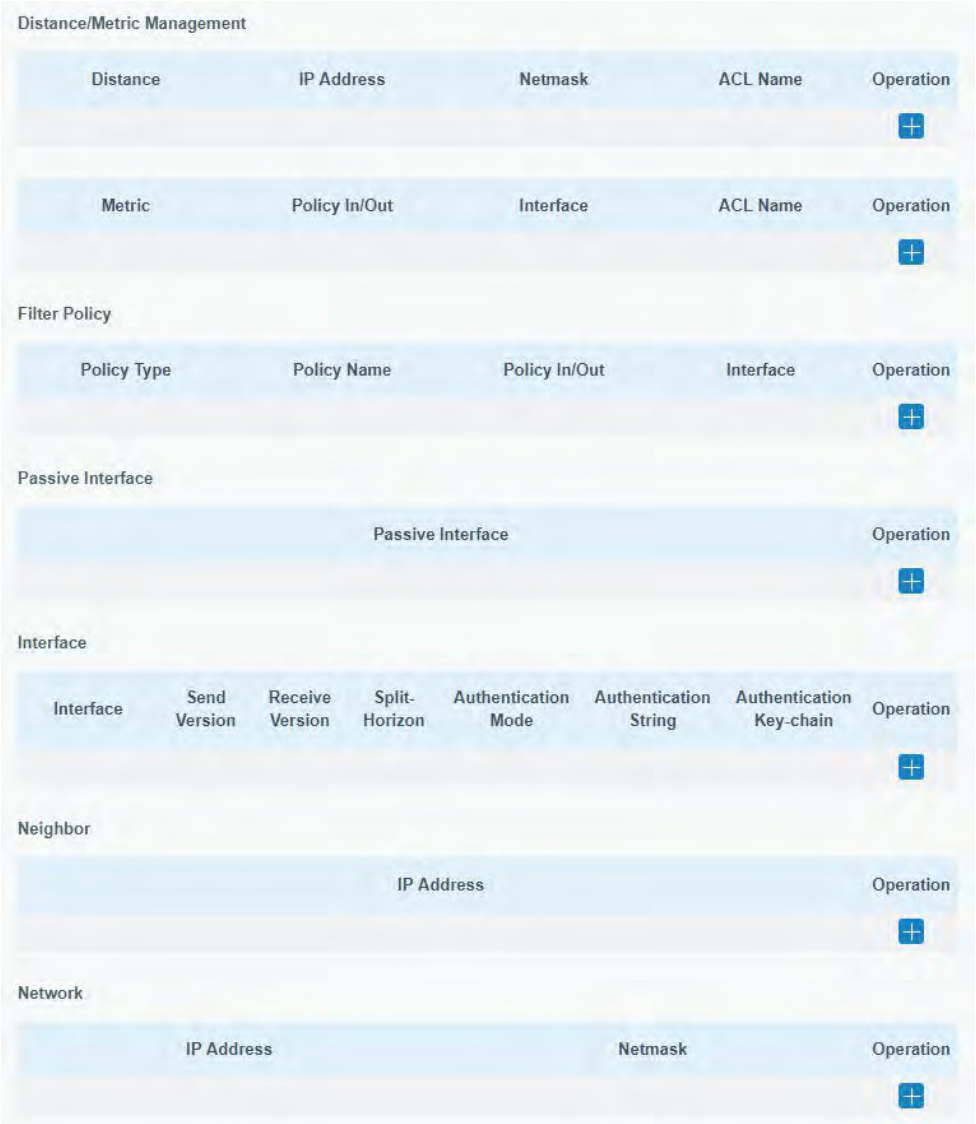



Figure 4-2-7-3

| 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", "GE1" and "GE0". |
| **Passive Interface** | |
| Passive Interface | Select interface from "cellular0" and "GE1", "GE0". |
| **Interface** | |
| Interface | Select interface from "cellular0", "GE1" and "GE0". |
| Send Version | Select from "default", "v1" and "v2". |
| Receive Version | Select from "default", "v1" and "v2". |
| Split-Horizon | Select from "enable" and "disable". |
| Authentication Mode | Select from "text" and "md5". |
| Authentication String | The authentication key for package interaction in RIPV2. |
| Authentication Key-chain | The authentication key-chain for package interaction in RIPV2. |
| **Neighbor** | |
| IP Address | Set RIP neighbor's IP address manually. |
| **Network** | |
| IP Address | The IP address of interface for RIP publishing. |
| Netmask | The netmask of interface for RIP publishing. |

Table 4-2-7-3

#### 4.2.7.3 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.

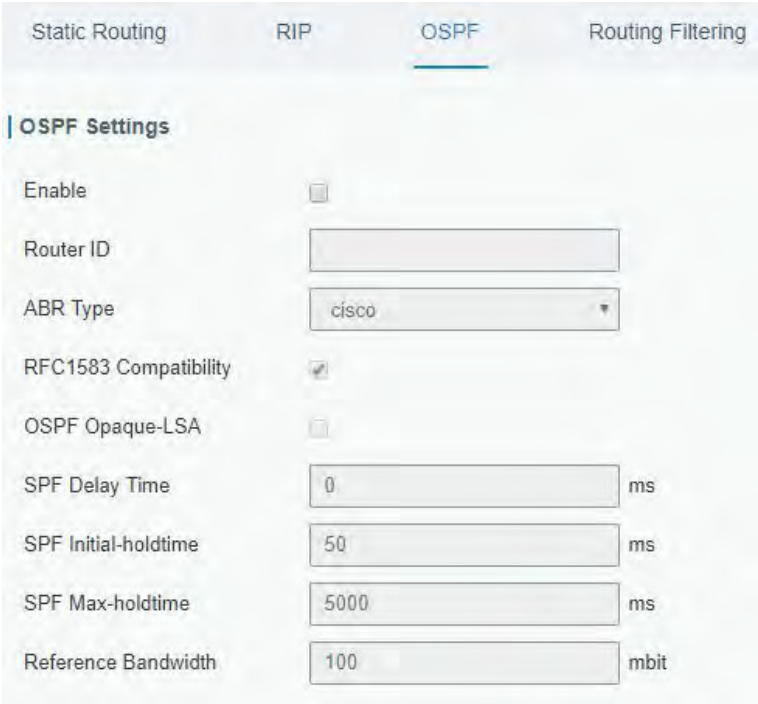



Figure 4-2-7-4

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

Table 4-2-7-4 OSPF Parameters

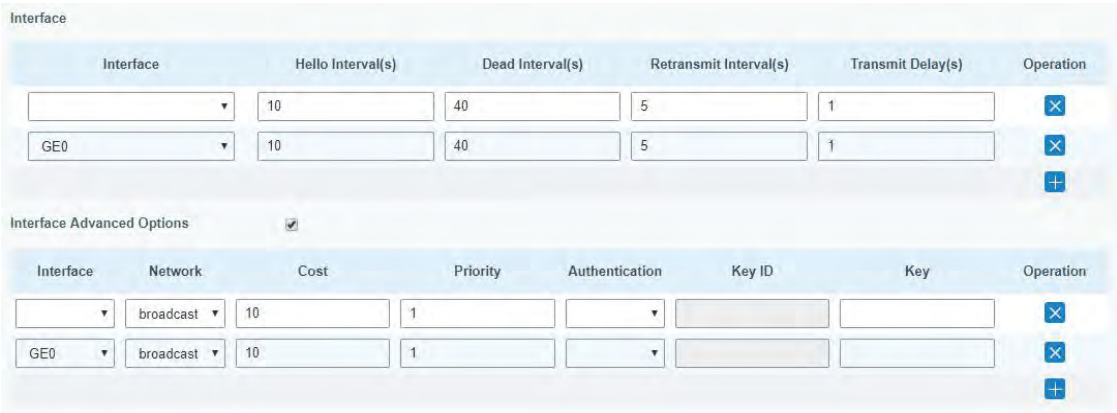



Figure 4-2-7-5

| Item | Description |
|---|---|
| **Interface** | |
| Interface | Select interface from "cellular0" and "GE0". |
| Hello Interval (s) | Send interval of Hello packet. If the Hello time between two adjacent routers is different, the neighbour relationship cannot be established.<br>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.<br>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.<br>Simple: a simple authentication password should be configured and confirmed again.<br>MD5: MD5 key & password should be configured and confirmed again. |
| Key ID | It only takes effect when MD5 is selected. Range 1-255. |
| Key | The authentication key for OSPF packet interaction. |

Table 4-2-7-5 OSPF Parameters

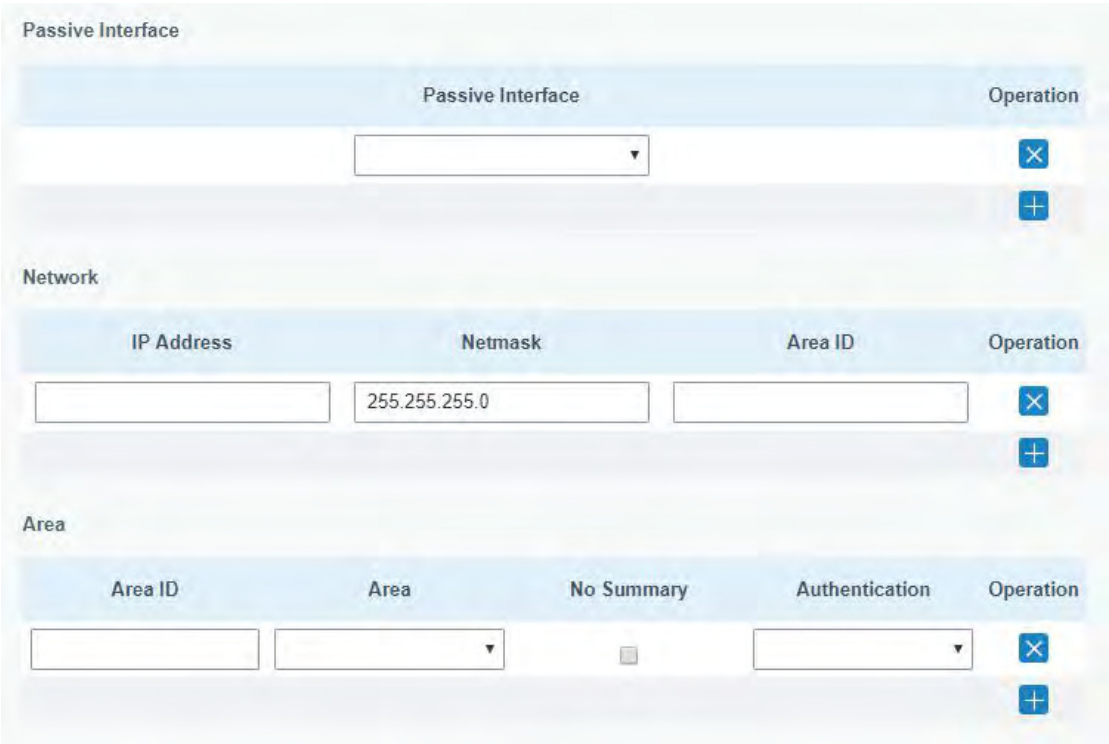



Figure 4-2-7-6

| Item | Description |
|---|---|
| **Passive Interface** | |
| Passive Interface | Select interface from "cellular0", "GE0" and "GE1". |
| **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".<br>The backbone area (area ID 0.0.0.0) cannot be set as "Stub" or "NSSA". |
| No Summary | Forbid route summarization. |
| Authentication | Select authentication from "simple" and "md5". |

Table 4-2--7-6 OSPF Parameters

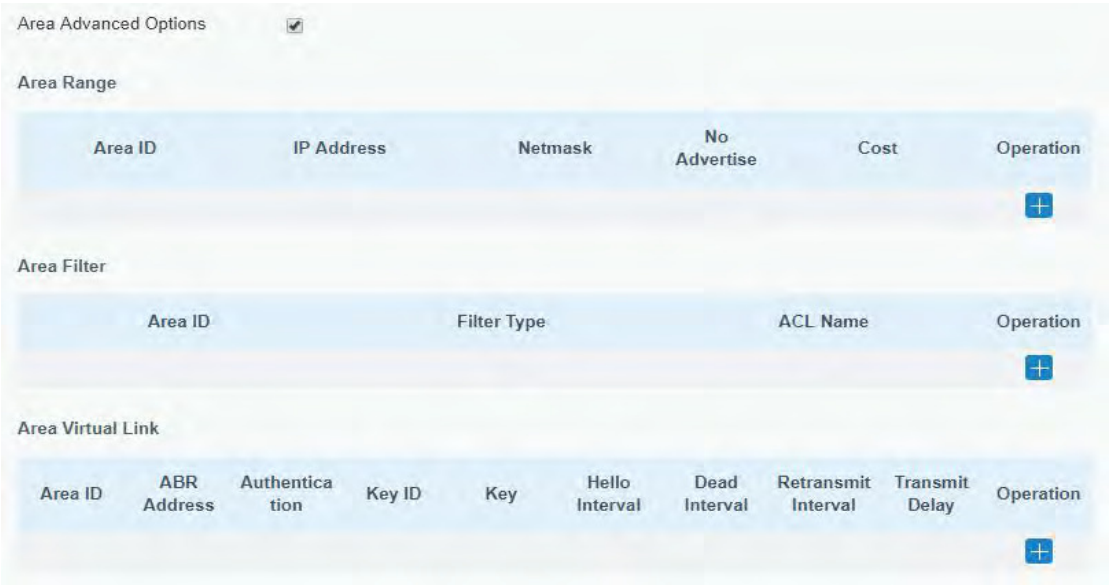



Figure 4-2-7-7

| Area Advanced Options | |
|---|---|
| **Item** | **Description** |
| **Area Range** | |
| Area ID | The area ID of the interface when it runs OSPF (IP address). |
| IP Address | Set the IP address. |
| Netmask | Set the netmask. |
| No Advertise | Forbid the route information to be advertised among different areas. |
| Cost | Range: 0-16777215 |
| **Area Filter** | |

| | |
|---|---|
| Area ID | Select an Area ID for Area Filter. |
| Filter Type | Select from "import", "export", "filter-in", and "filter-out". |
| ACL Name | Enter an ACL name which is set on "Routing > Routing Filtering" webpage. |
| **Area Virtual Link** | |
| Area ID | Set the ID number of OSPF area. |
| ABR Address | ABR is the router connected to multiple outer areas. |
| Authentication | Select from "simple" and "md5". |
| Key ID | It only takes effect when MD5 is selected. Range 1-15. |
| Key | The authentication key for OSPF packet interaction. |
| Hello Interval | Set the interval time for sending Hello packets through the interface. Range: 1-65535. |
| Dead Interval | The dead interval time for sending Hello packets through the interface. Range: 1-65535. |
| Retransmit Interval | The retransmission interval time for re-sending LSA. Range: 1-65535. |
| Transmit Delay | The delay time for LSA transmission. Range: 1-65535. |

Table 4-2-7-7 OSPF Parameters

Figure 4-2-7-8

| Item | Description |
|---|---|
| **Redistribution** | |
| Redistribution Type | Select from "connected", "static" and "rip". |
| Metric | The metric of redistribution router. Range: 0-16777214. |
| Metric Type | Select Metric type from "1" and "2". |
| Route Map | Mainly used to manage route for redistribution. |
| **Redistribution Advanced Options** | |
| Always Redistribute Default Route | Send redistribution default route after starting up. |

| | |
|---|---|
| Redistribute Default Route Metric | Send redistribution default route metric. Range: 0-16777214. |
| Redistribute Default Route Metric Type | Select from "0", "1" and "2". |
| **Distance Management** | |
| Area Type | Select from "intra-area", "inter-area" and "external". |
| Distance | Set the OSPF routing distance for area learning. Range: 1-255. |

Table 4-2-7-8 OSPF Parameters

### 4.2.7.4 Routing Filtering

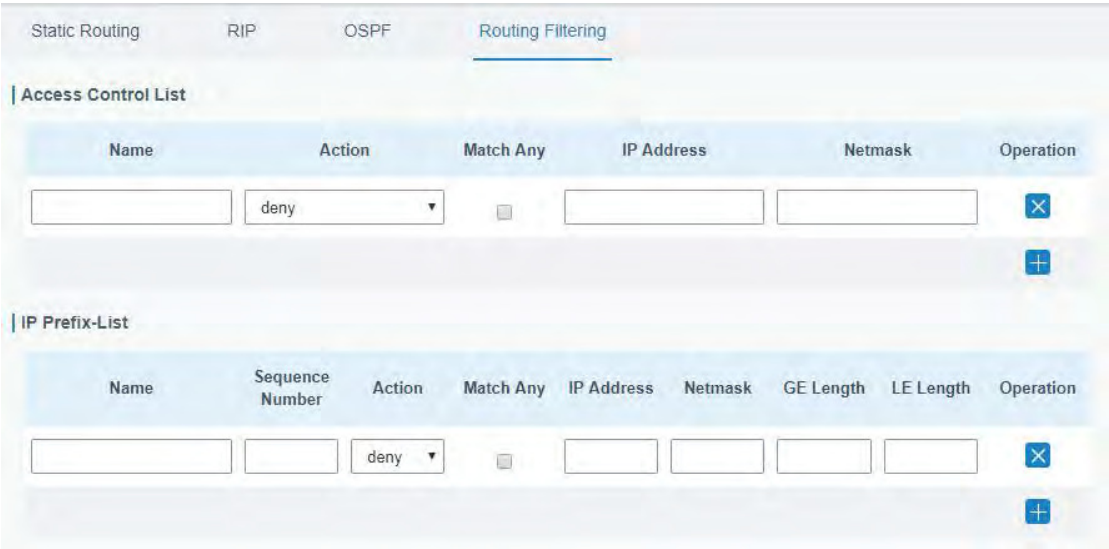



Figure 4-2-7-9

| **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, GE Length, and LE |

| | |
|---|---|
| | Length. |
| IP Address | User-defined. |
| Netmask | User-defined. |
| GE Length | Specify the minimum number of mask bits that must be matched. Range: 0-32. |
| LE Length | Specify the maximum number of mask bits that must be matched. Range: 0-32. |

Table 4-2-7-9 Routing Filtering Parameters

### 4.2.8 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 UR71 supports DMVPN, IPsec, GRE, L2TP, PPTP, OpenVPN, as well as GRE over IPsec and L2TP over IPsec.

#### 4.2.8.1 DMVPN

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

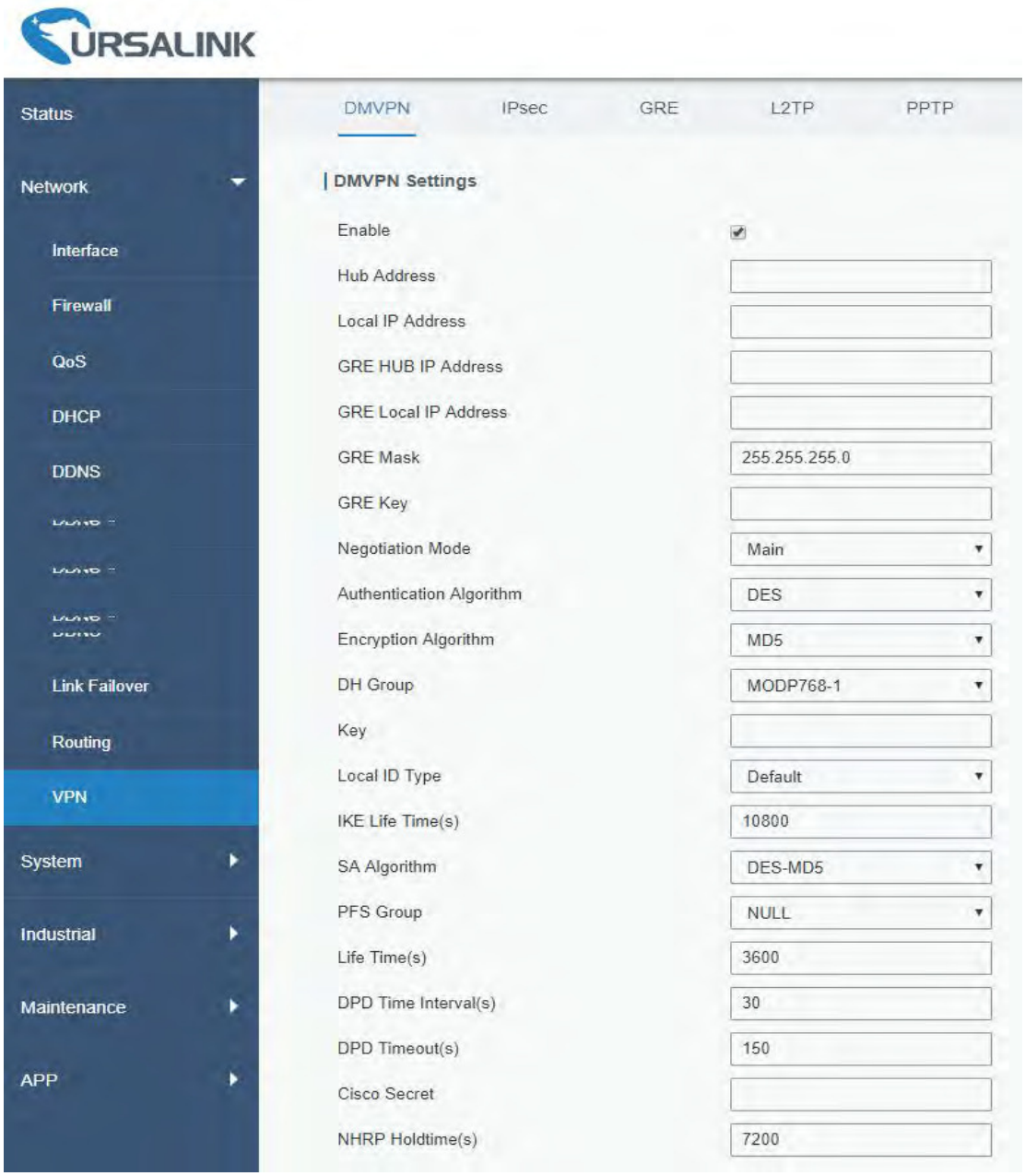



Figure 4-2-8-1

| 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. |

Table 4-2-8-1 DMVPN Parameters

#### 4.2.8.2 IPSec

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

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

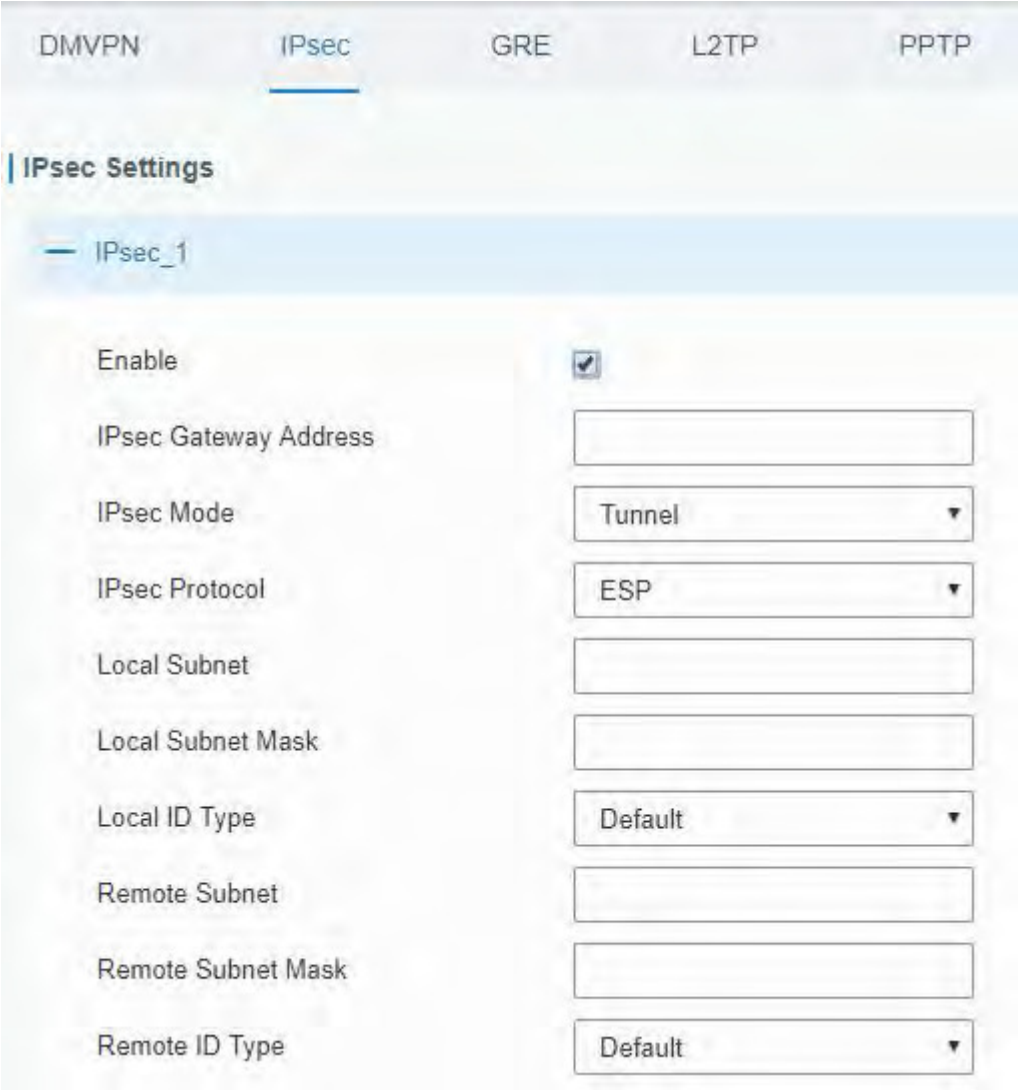



Figure 4-2-8-2

| IPsec | |
|---|---|
| **Item** | **Description** |
| Enable | Enable IPsec tunnel. A maximum of 3 tunnels is allowed. |
| IPsec Gateway Address | Enter the IP address or domain name of remote IPsec server. |
| IPsec Mode | Select from "Tunnel" and "Transport". |
| IPsec Protocol | Select from "ESP" and "AH". |
| Local Subnet | Enter the local subnet IP address that IPsec protects. |
| Local Subnet Netmask | Enter the local netmask that IPsec protects. |
| Local ID Type | Select from "Default", "ID", "FQDN", and "User FQDN". |
| Remote Subnet | Enter the remote subnet IP address that IPsec protects. |
| Remote Subnet Mask | Enter the remote netmask that IPsec protects. |
| Remote ID type | Select from "Default", "ID", "FQDN", and "User FQDN". |

Table 4-2-8-2 IPsec Parameters

| | |
|---|---|
| **IKE Parameter** | ☑ |
| IKE Version | IKEv1 |
| Negotiation Mode | Main |
| Encryption Algorithm | DES |
| Authentication Algorithm | MD5 |
| DH Group | MODP768-1 |
| Local Authentication | PSK |
| Local Secrets | |
| XAUTH | ☐ |
| Lifetime(s) | 10800 |
| **SA Parameter** | ☑ |
| SA Algorithm | DES-MD5 |
| PFS Group | NULL |
| Lifetime(s) | 3600 |
| DPD Time Interval(s) | 30 |
| DPD Timeout(s) | 150 |
| **IPsec Advanced** | ☑ |
| Enable Compression | ☐ |
| VPN Over IPsec Type | NONE |

Figure 4-2-8-3

| IKE Parameter | |
|---|---|
| **Item** | **Description** |
| IKE Version | Select from "IKEv1" and "IKEv2". |
| Negotiation Mode | Select from "Main" and "Aggressive". |
| Encryption Algorithm | Select from "DES", "3DES", "AES128", "AES192" and "AES256". |
| Authentication Algorithm | Select from "MD5" and " SHA1" |
| DH Group | Select from "MODP768_1", "MODP1024_2" and "MODP1536_5". |
| Local Authentication | Select from "PSK" and "CA". |
| Local Secrets | Enter the preshared key. |
| XAUTH | Enter XAUTH username and password after XAUTH is enabled. |
| Lifetime (s) | Set the lifetime in IKE negotiation. Range: 60-86400. |
| **SA Parameter** | |
| 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". |
| Lifetime (s) | Set the lifetime of IPsec SA. Range: 60-86400. |
| DPD Interval Time(s) | Set DPD interval time to detect if the remote side fails. |
| DPD Timeout(s) | Set DPD timeout. Range: 10-3600. |
| **IPsec Advanced** | |
| Enable Compression | The head of IP packet will be compressed after it's enabled. |
| VPN Over IPsec Type | Select from "NONE", "GRE" and "L2TP" to enable VPN over IPsec function. |

Table 4-2-8-3 IPsec Parameters

#### 4.2.8.3 GRE

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

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

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

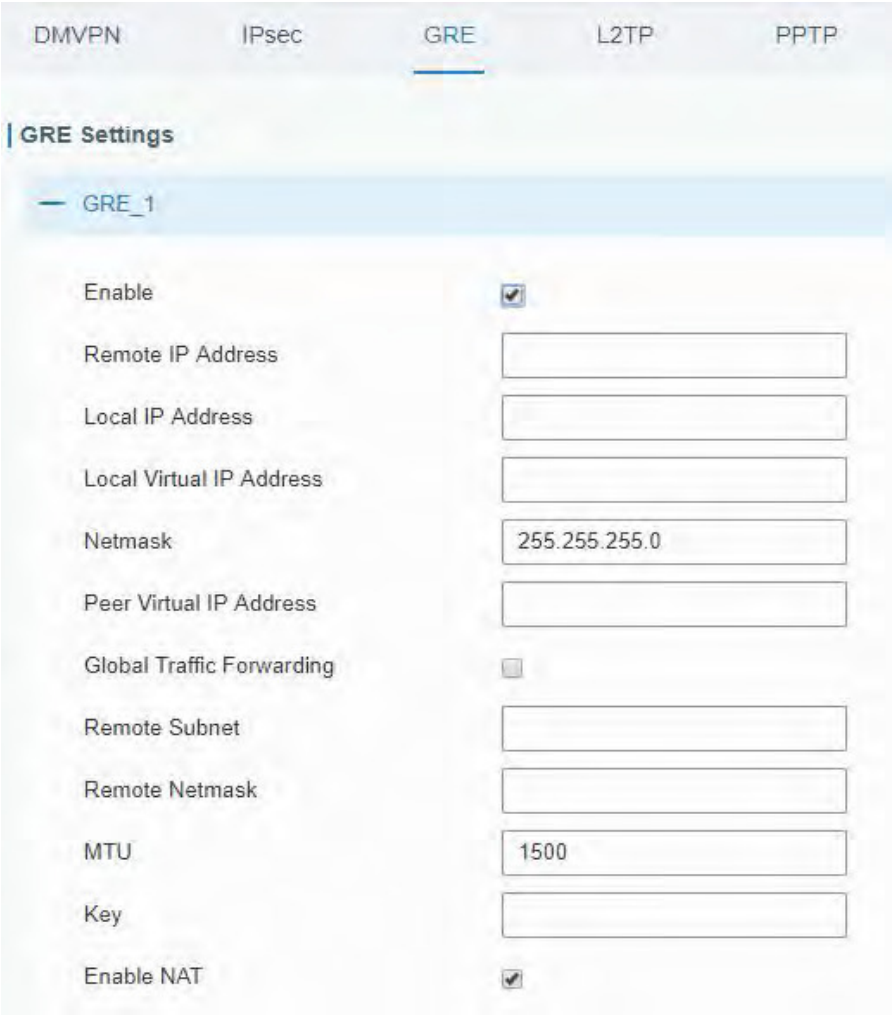



Figure 4-2-8-4

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

Table 4-2-8-4 GRE Parameters

#### 4.2.8.4 L2TP

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

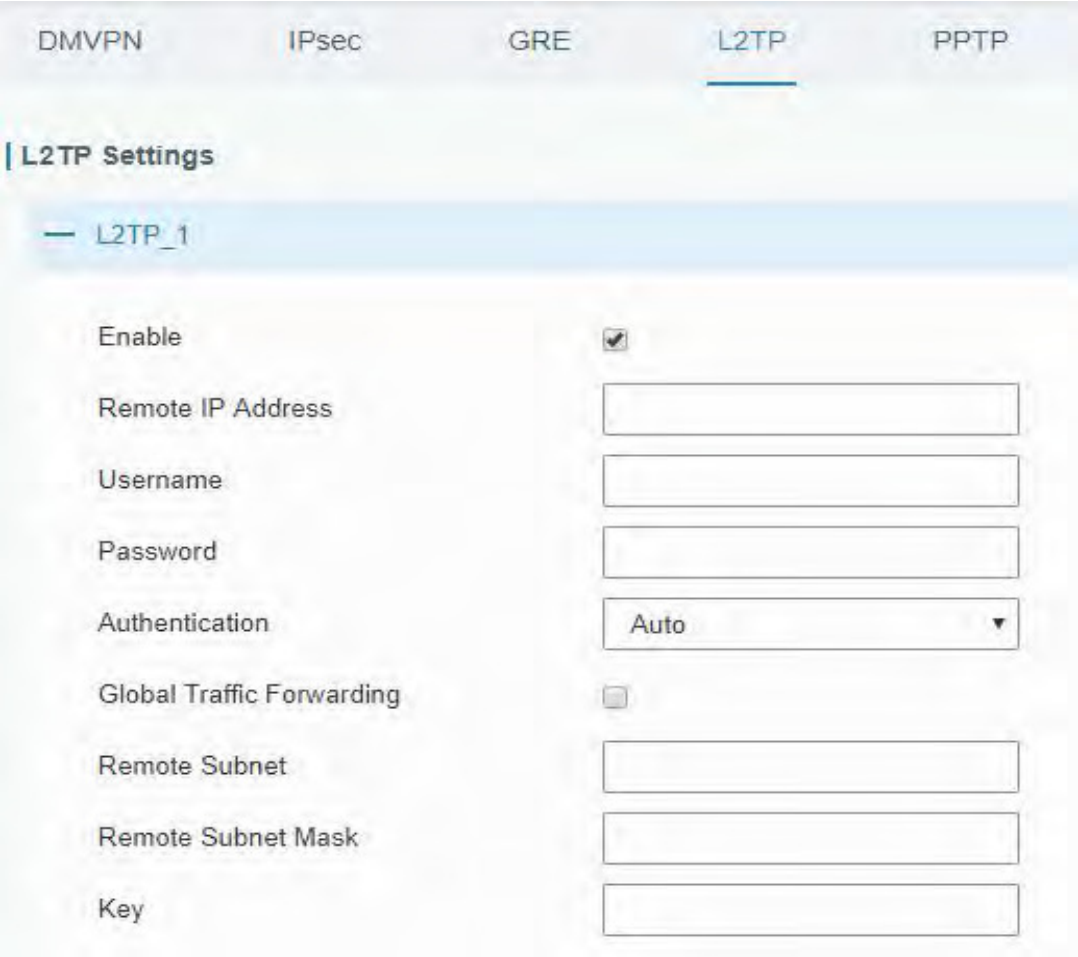



Figure 4-2-8-5

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

Table 4-2-8-5 L2TP Parameters

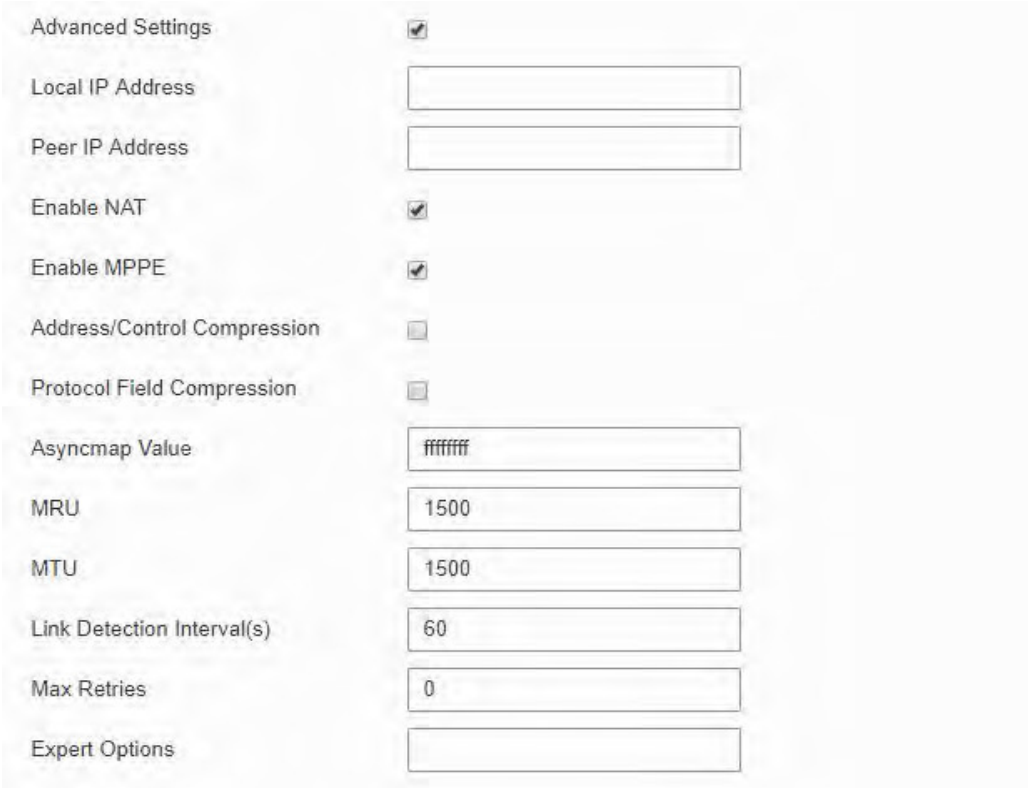



Figure 4-2-8-6

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

Table 4-2-8-6 L2TP Parameters

#### 4.2.8.5 PPTP

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

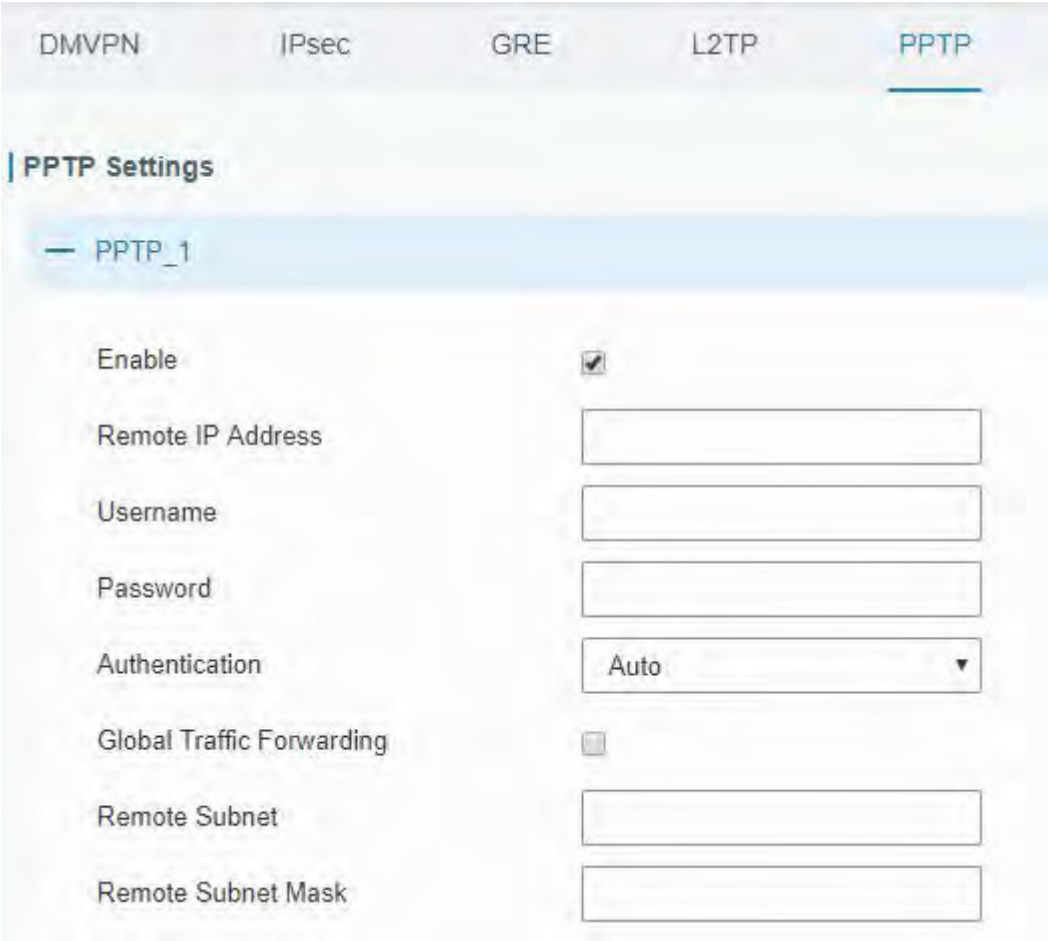



Figure 4-2-8-7

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

Table 4-2-8-7 PPTP Parameters

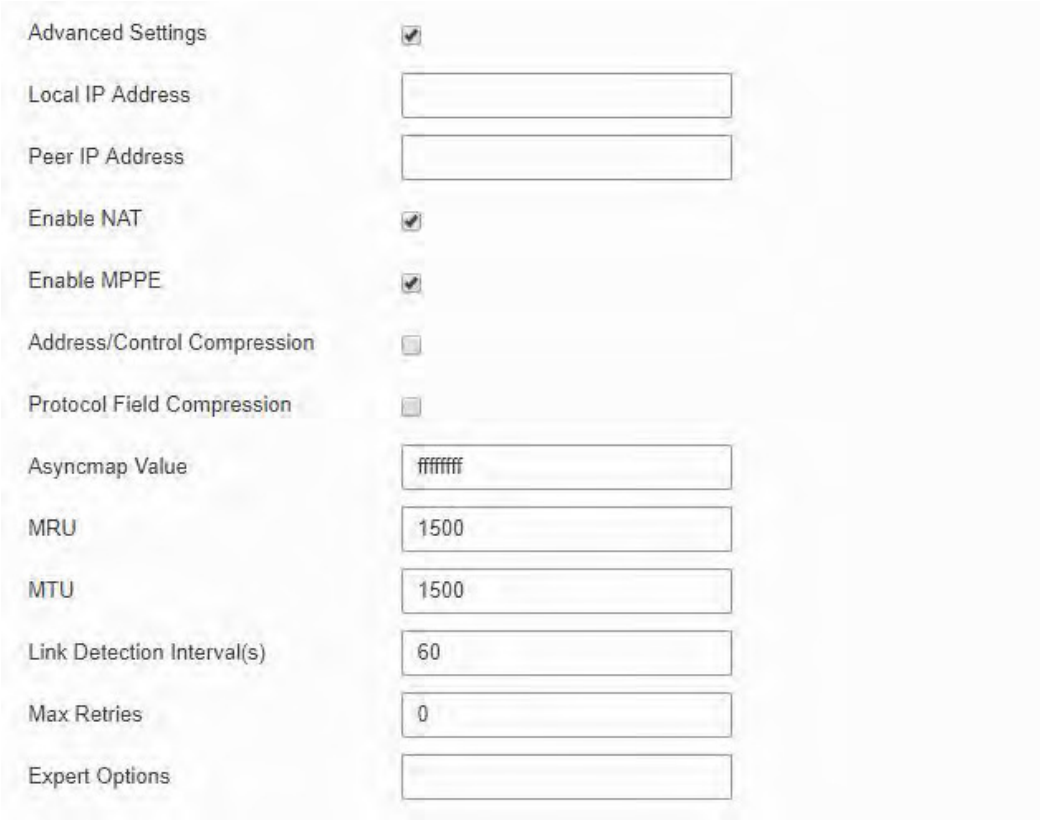



Figure 4-2-8-8

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

Table 4-2-8-8 PPTP Parameters

**Related Configuration Example**

PPTP Application Example

### 4.2.8.6 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.

Advantages of OpenVPN include:

- Security provisions that function against both active and passive attacks.
- Compatibility with all major operating systems.
- High speed (1.4 megabytes per second typically).
- Ability to configure multiple servers to handle numerous connections simultaneously.
- All encryption and authentication features of the OpenSSL library.
- Advanced bandwidth management.
- A variety of tunneling options.
- Compatibility with smart cards that support the Windows Crypt application program interface (API).
-

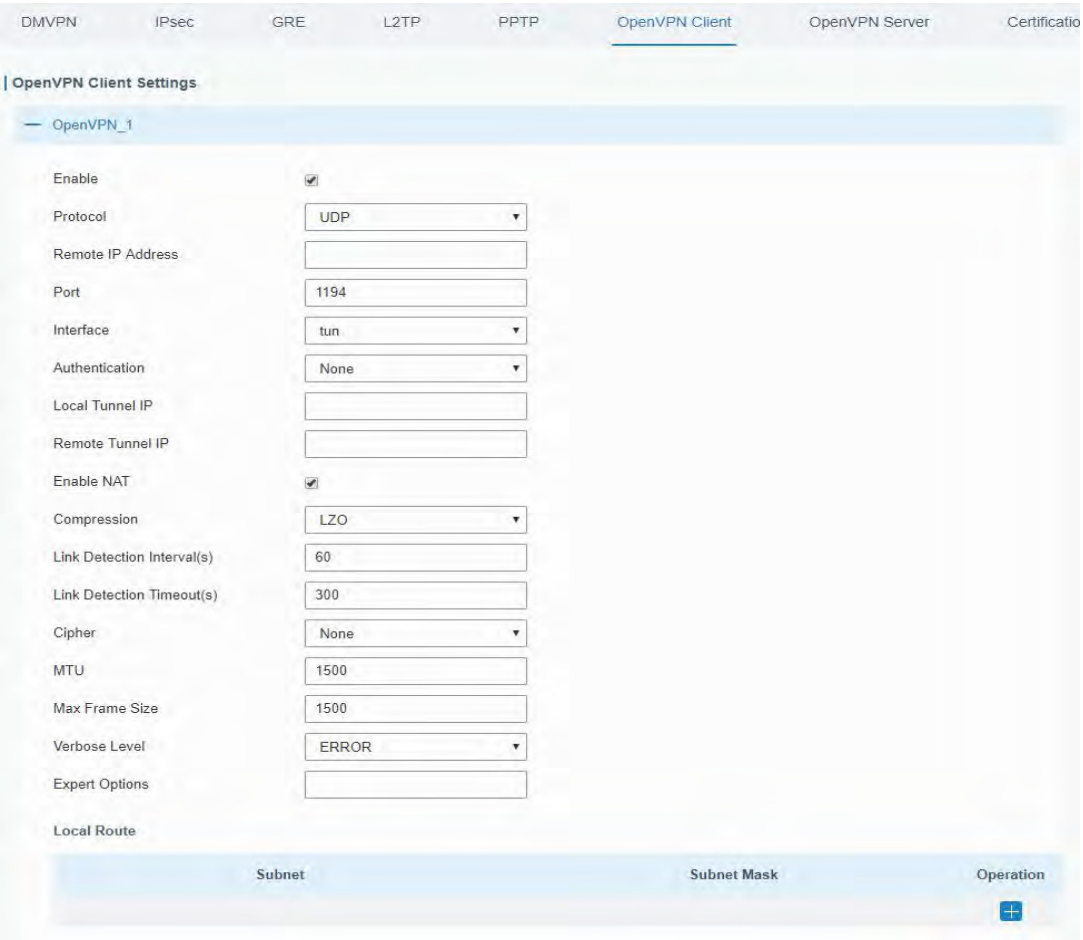



Figure 4-2-8-9

| OpenVPN Client | |
|---|---|
| **Item** | **Description** |
| Enable | Enable OpenVPN client. A maximum of 3 tunnels is allowed. |
| Protocol | Select from "UDP" and "TCP". |
| Remote IP Address | Enter remote OpenVPN server's IP address or domain name. |
| Port | Enter the listening port number of remote OpenVPN server. Range: 1-65535. |
| Interface | Select from "tun" and "tap". |
| Authentication | Select from "None", "Pre-shared", "Username/Password", "X.509 cert", and "X.509 cert+user". |
| Local Tunnel IP | Set local tunnel address. |
| Remote Tunnel IP | Enter remote tunnel address. |
| Global Traffic Forwarding | All the data traffic will be sent out via OpenVPN tunnel when this function is enabled. |
| Enable TLS Authentication | Check to enable TLS authentication. |
| Username | Enter username provided by OpenVPN server. |
| Password | Enter password provided by OpenVPN server. |
| Enable NAT | Enable NAT traversal function. |
| Compression | Select LZO to compress data. |
| Link Detection Interval (s) | Set link detection interval time to ensure tunnel connection. Range: 10-1800. |
| Link Detection Timeout (s) | Set link detection timeout. OpenVPN will be reestablished after timeout. Range: 60-3600. |
| Cipher | Select from "NONE", "BF-CBC", "DE-CBC", "DES-EDE3-CBC", "AES-128-CBC", "AES-192-CBC" and "AES-256-CBC". |
| MTU | Enter the maximum transmission unit. Range: 128-1500. |
| Max Frame Size | Set the maximum frame size. Range: 128-1500. |
| Verbose Level | Select from "ERROR", "WARING", "NOTICE" and "DEBUG". |
| Expert Options | User can enter some other PPP initialization strings in this field and separate the strings with blank space. |
| **Local Route** | |
| Subnet | Set the local route's IP address. |
| Subnet Mask | Set the local route's netmask. |

Table 4-2-8-9 OpenVPN Client Parameters

#### 4.2.8.7 OpenVPN Server

The UR71 supports OpenVPN server to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities.

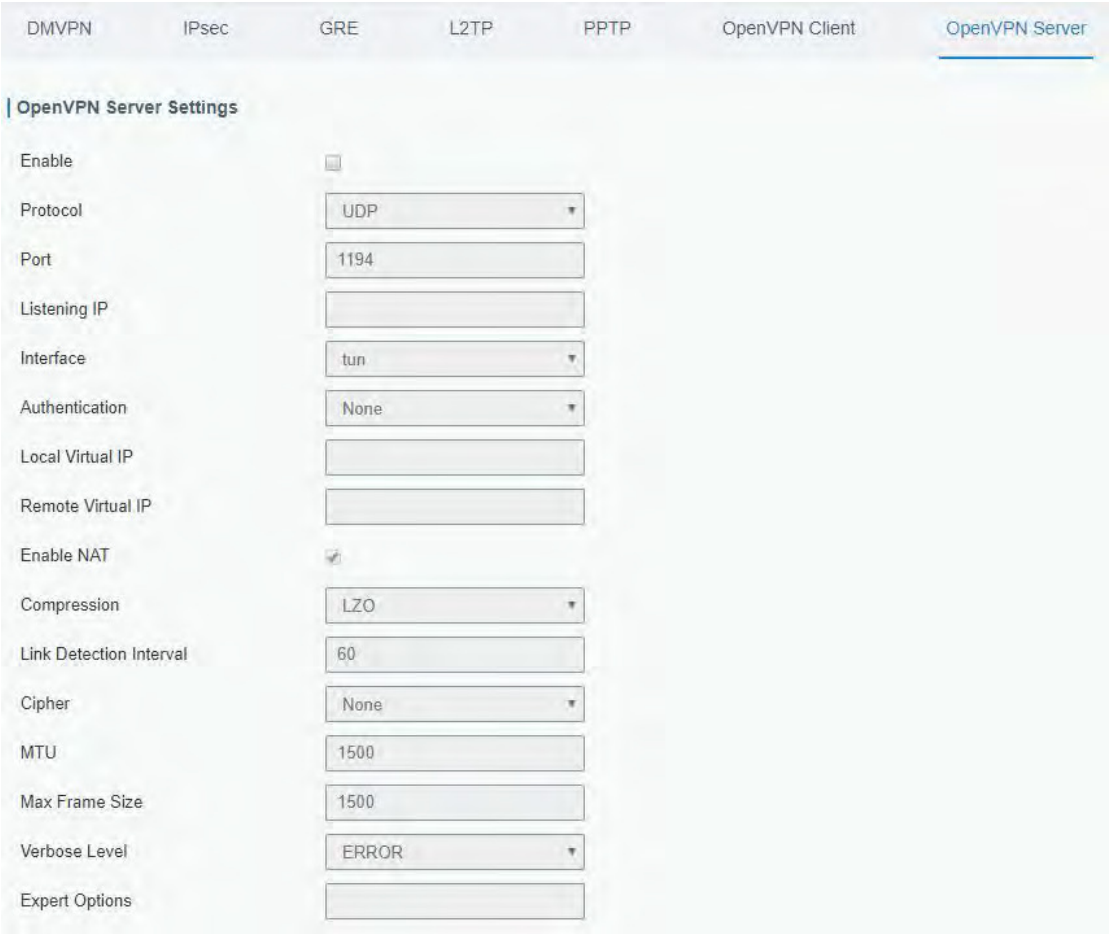



Figure 4-2-8-10

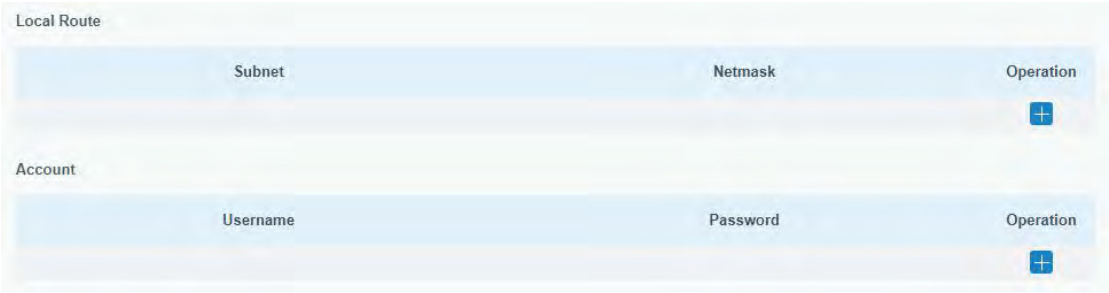



Figure 4-2-8-11

| OpenVPN Server | |
|---|---|
| **Item** | **Description** |
| Enable | Enable/disable OpenVPN server. |
| Protocol | Select from TCP and UDP. |
| Port | Fill in listening port number. Range: 1-65535. |
| Listening IP | Enter WAN IP address or LAN IP address. Leaving it blank refers to all active WAN IP and LAN IP address. |
| Interface | Select from " tun" and "tap". |
| Authentication | Select from "None", "Pre-shared", "Username/Password", |

| | |
|---|---|
| | "X.509 cert" and "X. 509 cert +user". |
| Local Virtual IP | The local tunnel address of OpenVPN's tunnel. |
| Remote Virtual IP | The remote tunnel address of OpenVPN's tunnel. |
| Client Subnet | Local subnet IP address of OpenVPN client. |
| Client Netmask | Local netmask of OpenVPN client. |
| Renegotiation Interval(s) | Set interval for renegotiation. Range: 0-86400. |
| Max Clients | Maximum OpenVPN client number. Range: 1-128. |
| Enable CRL | Enable CRL |
| Enable Client to Client | Allow access between different OpenVPN clients. |
| Enable Dup Client | Allow multiple users to use the same certification. |
| Enable NAT | Check to enable the NAT traversal function. |
| Compression | Select "LZO" to compress data. |
| Link Detection Interval | Set link detection interval time to ensure tunnel connection. Range: 10-1800. |
| Cipher | Select from "NONE", "BF-CBC", "DES-CBC", "DES-EDE3-CBC", "AES-128-CBC", "AES-192-CBC" and "AES-256-CBC". |
| MTU | Enter the maximum transmission unit. Range: 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 other PPP initialization strings in this field and separate the strings with blank space. |
| **Local Route** | |
| Subnet | The real local IP address of OpenVPN client. |
| Netmask | The real local netmask of OpenVPN client. |
| **Account** | |
| Username & Password | Set username and password for OpenVPN client. |

Table 4-2-8-10 OpenVPN Server Parameters

### 4.2.8.8 Certifications

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

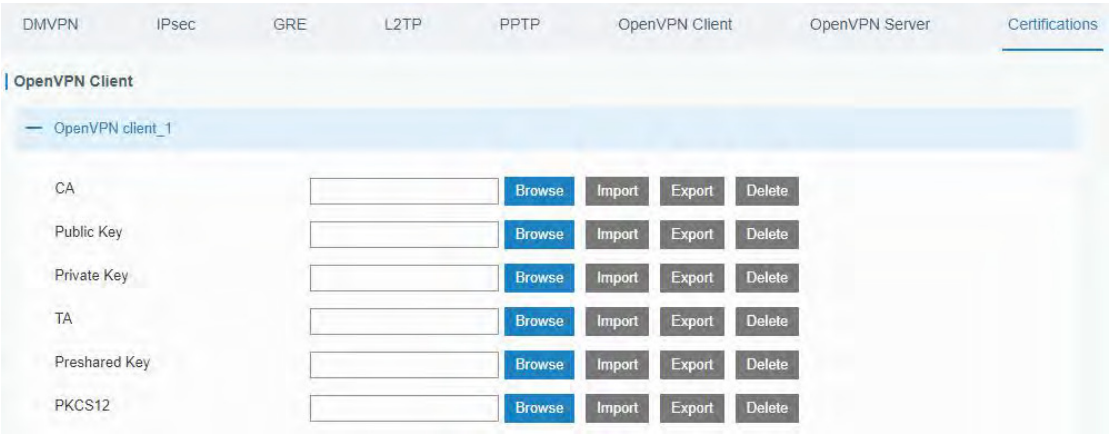



Figure 4-2-8-12

| OpenVPN Client | |
|---|---|
| **Item** | **Description** |
| CA | Import/Export CA certificate file. |
| Public Key | Import/Export public key file. |
| Private Key | Import/Export private key file. |
| TA | Import/Export TA key file. |
| Preshared Key | Import/Export static key file. |
| PKCS12 | Import/Export PKCS12 certificate file. |

Table 4-2-8-11 OpenVPN Client Certification Parameters

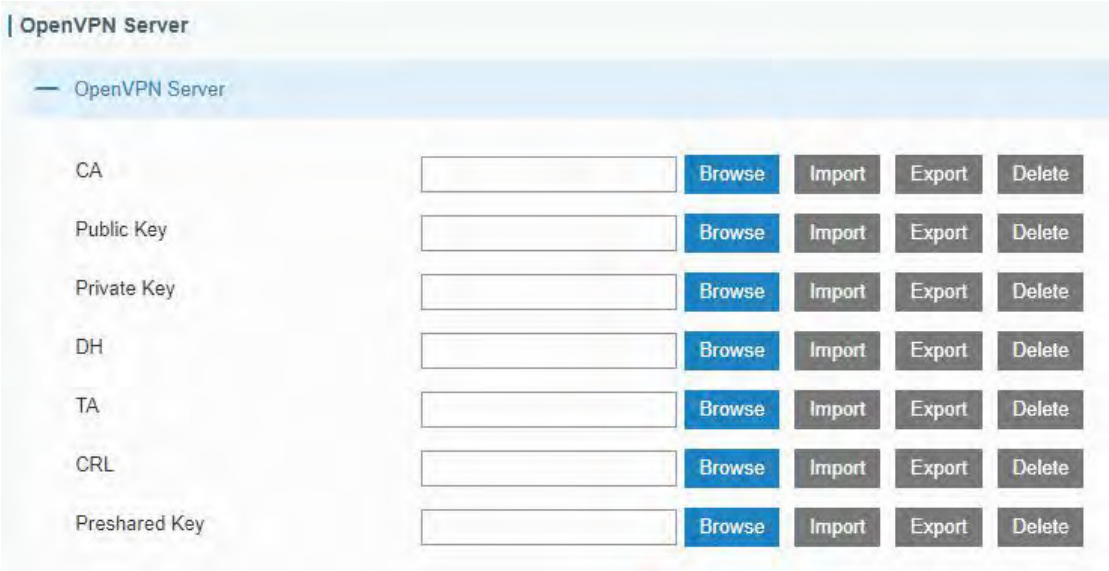



Figure 4-2-8-13

| OpenVPN Server | |
|---|---|
| **Item** | **Description** |
| CA | Import/Export CA certificate file. |
| Public Key | Import/Export public key file. |
| Private Key | Import/Export private key file. |
| DH | Import/Export DH key file. |
| TA | Import/Export TA key file. |
| CRL | Import/Export CRL. |
| Preshared Key | Import/Export static key file. |

Table 4-2-8-12 OpenVPN Server Parameters

Figure 4-2-8-14

| OpenVPN Server | |
|---|---|
| **Item** | **Description** |
| CA | Import/Export CA certificate. |
| Client Key | Import/Export client key. |
| Server Key | Import/Export server key. |
| Private Key | Import/Export private key. |
| CRL | Import/Export certificate recovery list. |

Table 4-2-8-13 IPsec Parameters

## 4.3 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.

### 4.3.1 General Settings

#### 4.3.1.1 General

General settings include system info, access service and HTTPS certificates.

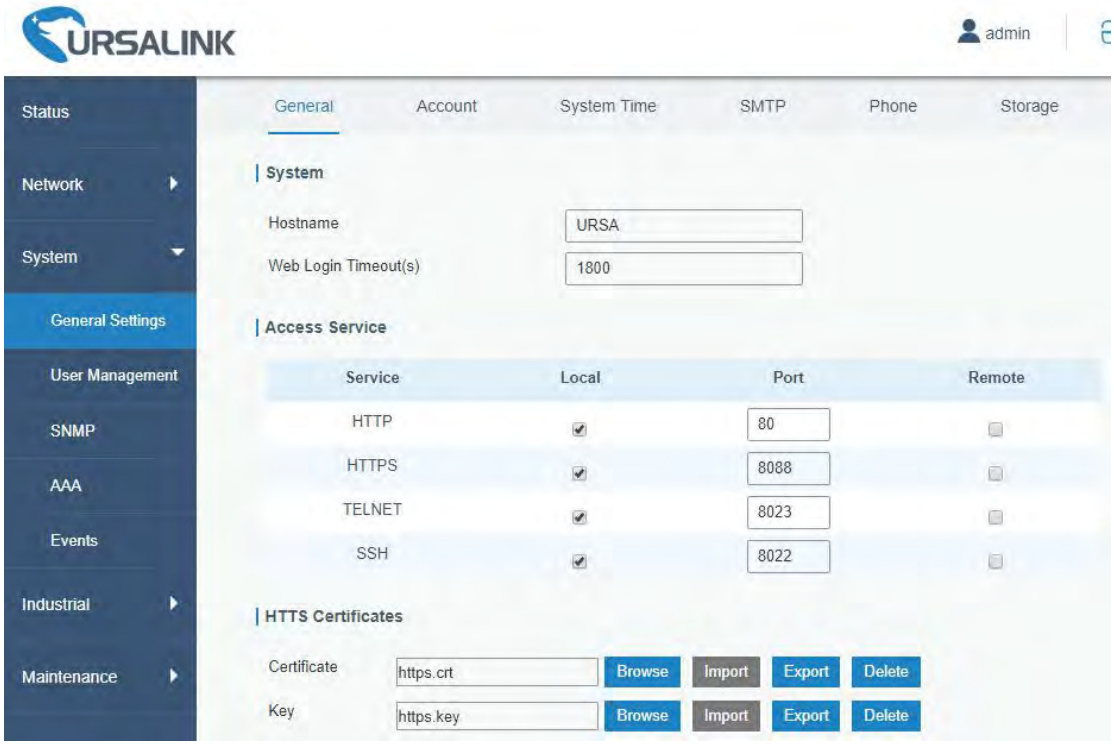



Figure 4-3-1-1

| General | | |
|---|---|---|
| **Item** | **Description** | **Default** |
| **System** | | |
| Hostname | User-defined router name, needs to start with a letter. | URSA |
| Web Login Timeout (s) | You need to log in again if it times out. Range: 100-3600. | 1800 |
| **Access Service** | | |
| Local | Access the router locally. | Enable |
| Port | Set port number of the services. Range: 1-65535. | -- |
| 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. | 8088 |
| TELNET | Users can log in the device locally and remotely via Telnet after the option is checked. | 8023 |
| SSH | Users can log in the device locally and remotely via SSH after the option is checked. | 8022 |

| Item | Description | Default |
|---|---|---|
| **HTTPS Certificates** | | |
| Certificate | Click "Browse" button, choose certificate file on the PC, and then click "Import" button to upload the file into router. Click "Export" button will export the file to the PC. Click "Delete" button will delete the file. | -- |
| Key | Click "Browse" button, choose key file on the PC, and then click "Import" button to upload the file into router. Click "Export" button will export file to the PC. Click "Delete" button will delete the file. | -- |

Table 4-3-1-1 General Setting Parameters

#### 4.3.1.2 Account Management

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

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

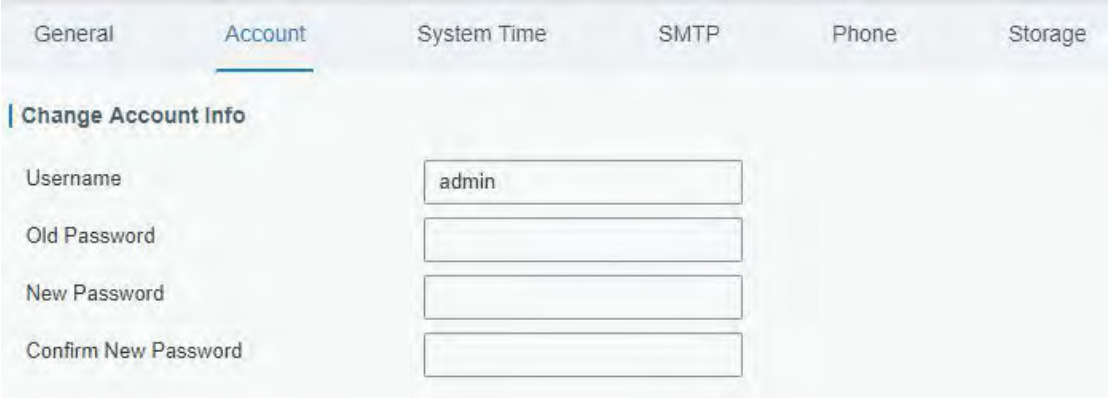



Figure 4-3-1-2

| 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. |

Table 4-3-1-2 Account Information

**Related Configuration Example**

Account Info Management

#### 4.3.1.3 System Time

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

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

Figure 4-3-1-3

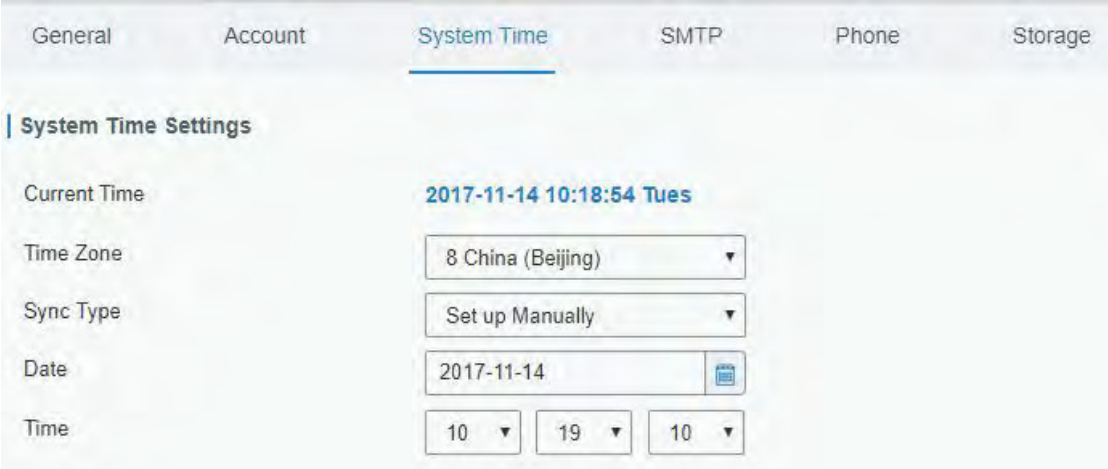



Figure 4-3-1-4

Figure 4-3-1-5

| 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. |
| Browser Time | Show the current time of browser. |
| Set up Manually | Manually configure the system time. |
| Sync with NTP Server | Synchronize time with NTP server so as to achieve time synchronization of all devices equipped with a clock on network. |
| **Sync with NTP Server** | |
| NTP Server Address | Set NTP server address (domain name/IP). |
| Enable NTP Server | NTP client on the network can achieve time synchronization with router after "Enable NTP Server" option is checked. |

Table 4-3-1-3 System Time Parameters

**Related Configuration Example**

System Time Management

#### 4.3.1.4 SMTP

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.

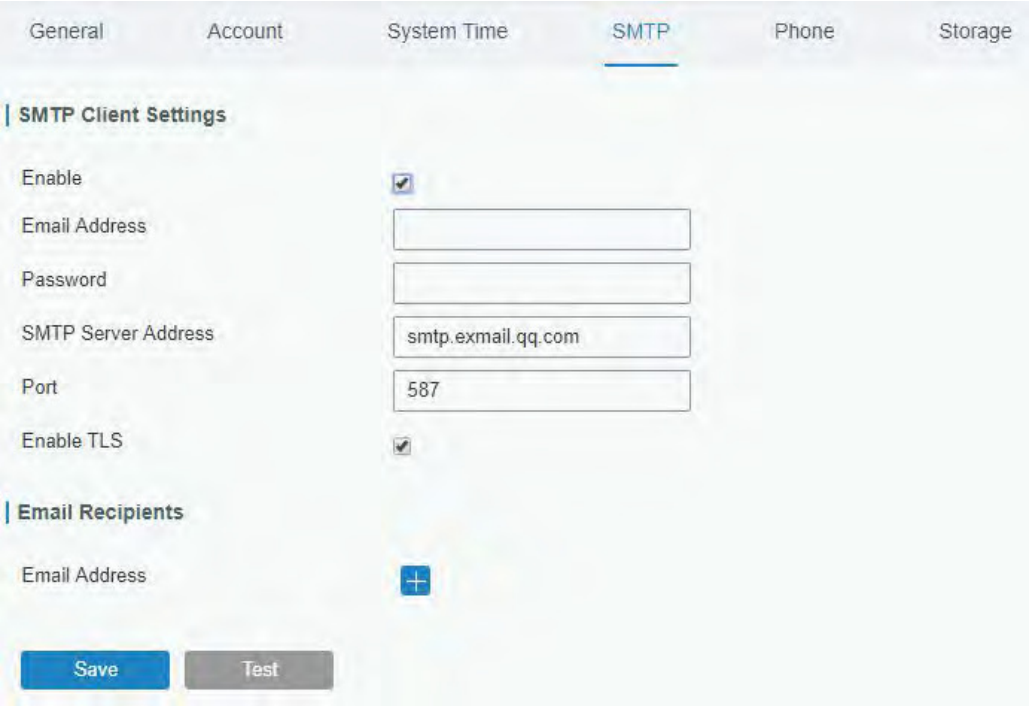



Figure 4-3-1-6

| SMTP | |
|---|---|
| **Item** | **Description** |
| **SMTP Client Settings** | |
| 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. |
| Enable TLS | Enable or disable TLS encryption. |
| **Email Recipients** | |
| Email Address | Add recipients' email address. |
| Test | Check if the recipients can get the mail from sender. |

Table 4-3-1-4 SMTP Setting

**Related Topics**

Events Setting

Events Application Example

### 4.3.1.5 Phone

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

1. Add phone list.
2. Select phone numbers and add them to the phone group.
3. Go to "Network > Interface > Cellular > Connection Mode > Connect on Demand > Trigger by Call / Trigger by SMS" or go to "System > Events > Event Settings > SMS" and then select the phone group ID.

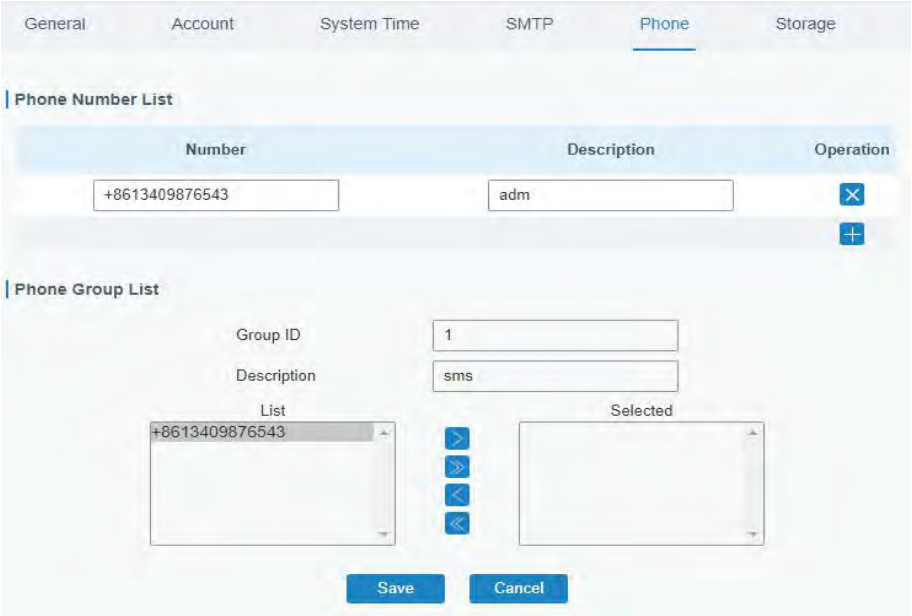



Figure 4-3-1-7

| Phone | |
|---|---|
| **Item** | **Description** |
| **Phone Number List** | |
| Number | Enter the telephone number. Digits, "+" and "-" are allowed. |
| Description | The description of the telephone number. |
| **Phone Group** | |
| 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. |

Table 4-3-1-5 Phone Settings

**Related Topic**

Connect on Demand

#### 4.3.1.6 Storage

You can view Micro SD card and SSD storage information on this page.

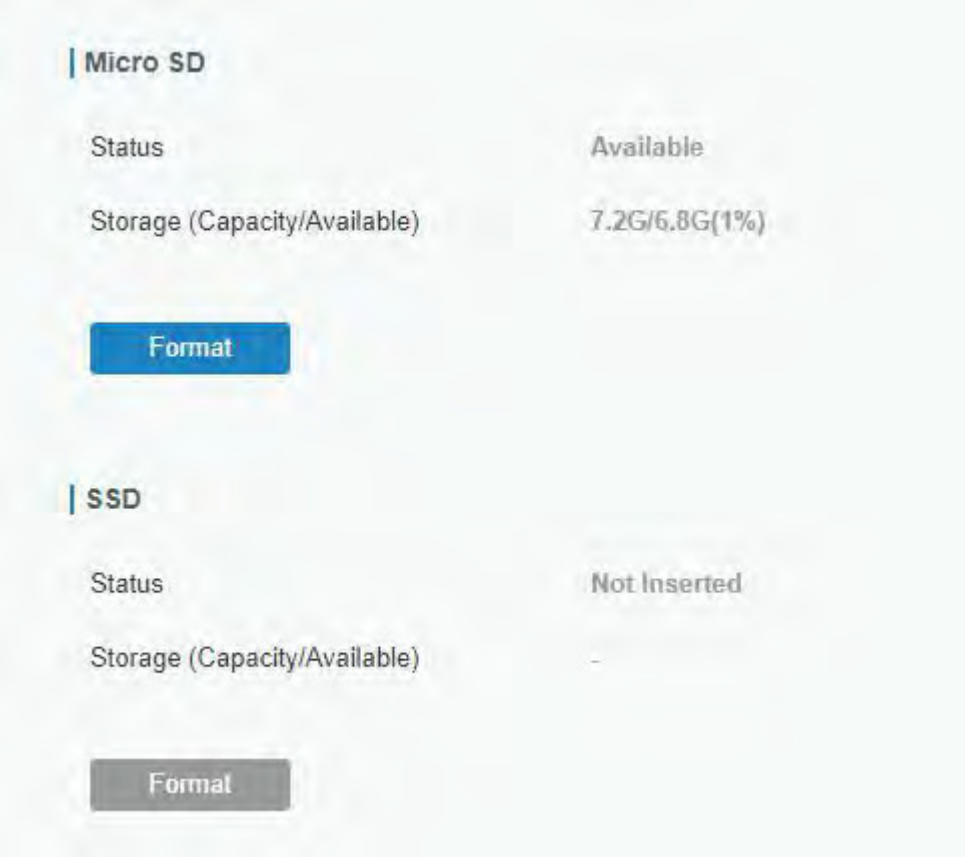



Figure 4-3-1-8

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

Table 4-3-1-6 Storage Information

### 4.3.2 User Management

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

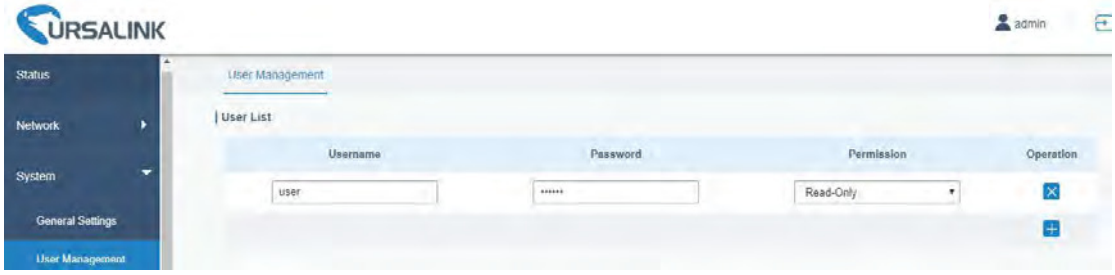



Figure 4-3-2-1

| User Management | |
|---|---|
| **Item** | **Description** |
| Username | Enter a new username. You can use characters such as a-z, 0-9, "_", "-", "$". The first character can't be a digit. |
| Password | Set password. |
| Permission | Select user permission from “Read-Only” and “Read-Write”.<br>- Read-Only: users can only view the configuration of router in this level.<br>- Read-Write: users can view and set the configuration of router in this level. |

Table 4-3-2-1 User Management

**Related Configuration Example**

Common User Management

### 4.3.3 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

### 4.3.3.1 SNMP

The UR71 supports SNMPv1, SNMPv2c and SNMPv3 version. SNMPv1 and SNMPv2c employ community name authentication. SNMPv3 employs authentication encryption by username and password.

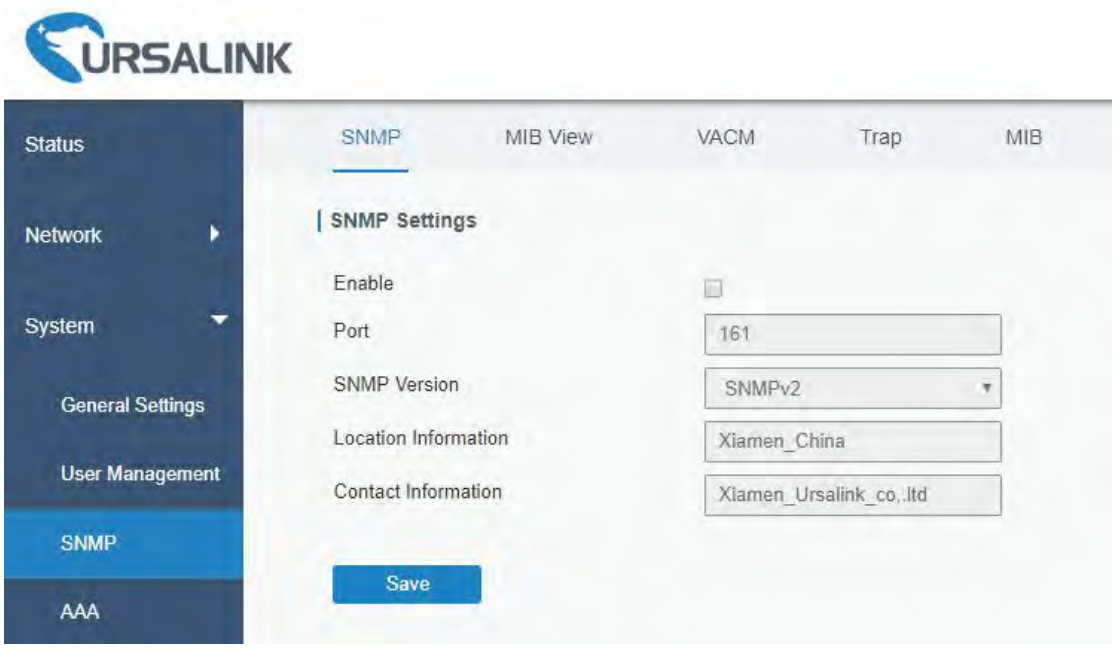



Figure 4-4-3-1

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

Table 4-4-3-1 SNMP Parameters

### 4.3.3.2 MIB View

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

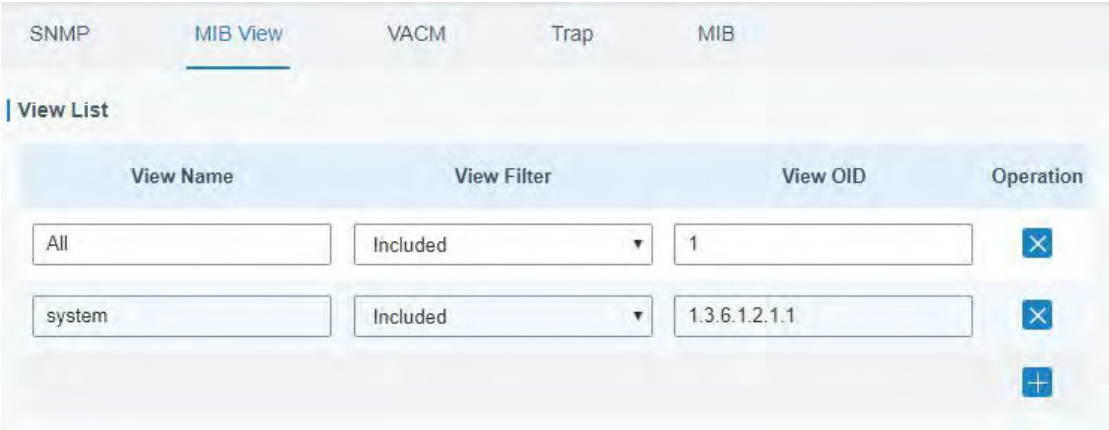



Figure 4-4-3-2

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

Table 4-3-3-2 MIB View Parameters

### 4.3.3.3 VACM

This section describes how to configure VCAM parameters.

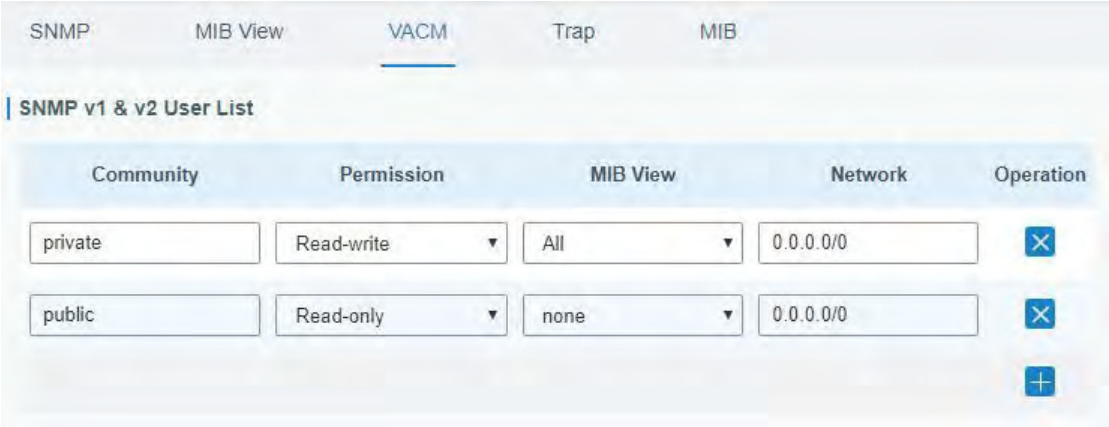



Figure 4-3-3-3

| VACM | |
|---|---|
| **Item** | **Description** |
| **SNMP v1 & v2 User List** | |
| Community | Set the community name. |
| Permission | Select from "Read-Only" and "Read-Write". |
| MIB View | Select an MIB view to set permissions from the MIB view list. |
| Network | The IP address and bits of the external network accessing the MIB view. |
| Read-Write | The permission of the specified MIB node is read and write. |
| Read-Only | The permission of the specified MIB node is read only. |
| **SNMP v3 User List** | |
| 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. |

Table 4-3-3-3 VACM Parameters

#### 4.3.3.4 Trap

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

Figure 4-3-3-4

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

Table 4-3-3-4 Trap Parameters

#### 4.3.3.5 MIB

This section describes how to download MIB files. The last MIB file “URSA-ROUTER-MIB.txt” is for the UR71 router.

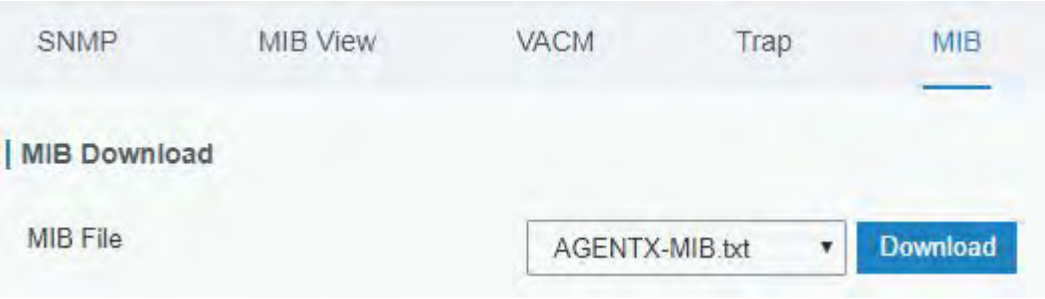



Figure 4-3-3-5

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

Table 4-3-3-5 MIB Download

### 4.3.4 AAA

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

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

#### 4.3.4.1 Radius

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

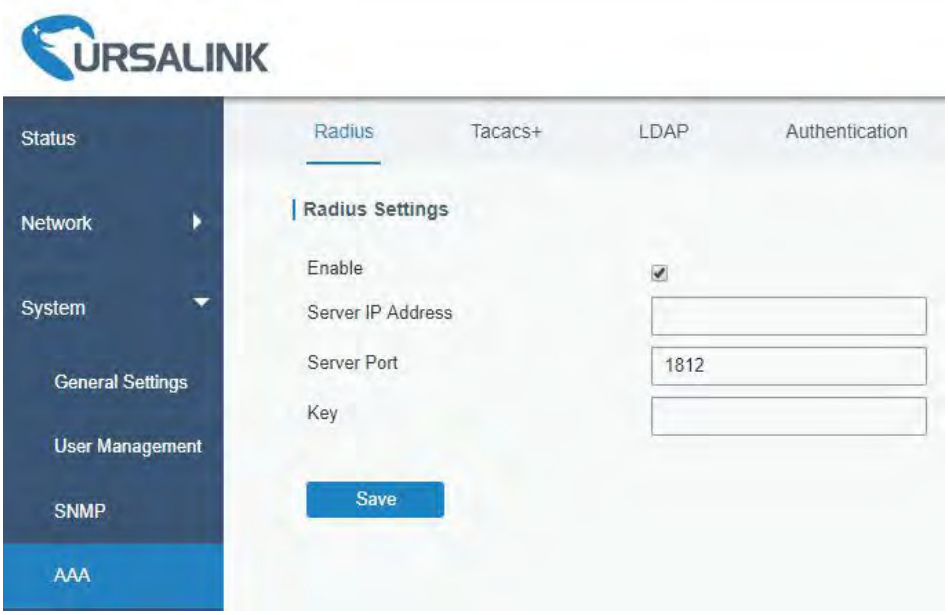



Figure 4-3-4-1

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

Table 4-3-4-1 Radius Parameters

#### 4.3.4.2 Tacacs+

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

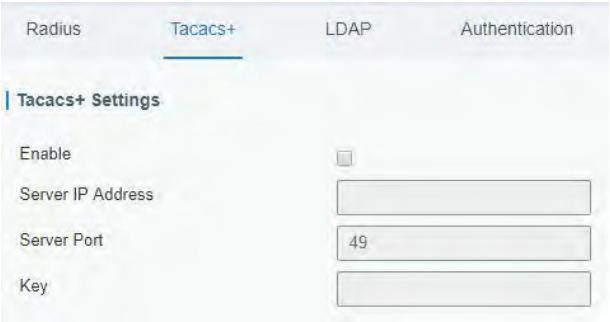



Figure 4-3-4-2

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

Table 4-3-4-2 Tacacs+ Parameters

#### 4.3.4.3 LDAP

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

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

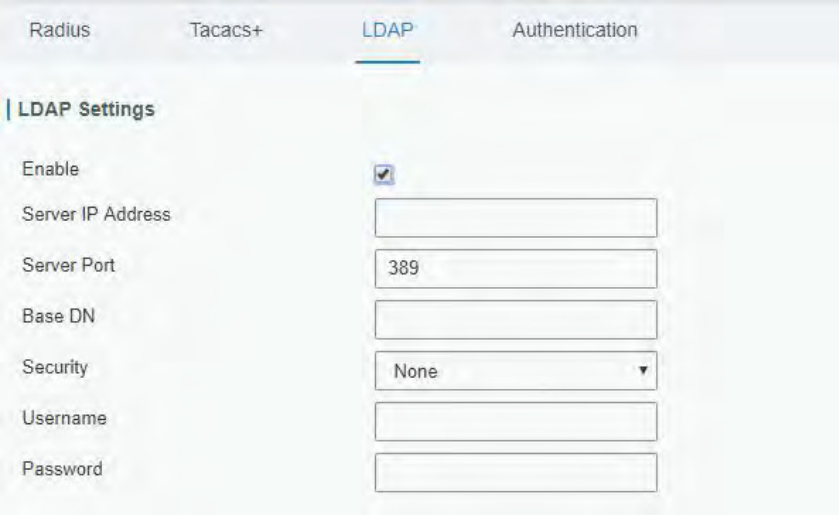



Figure 4-3-4-3

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

Table 4-3-4-3 LDAP Parameters

#### 4.3.4.4 Authentication

AAA supports the following authentication ways:

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

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

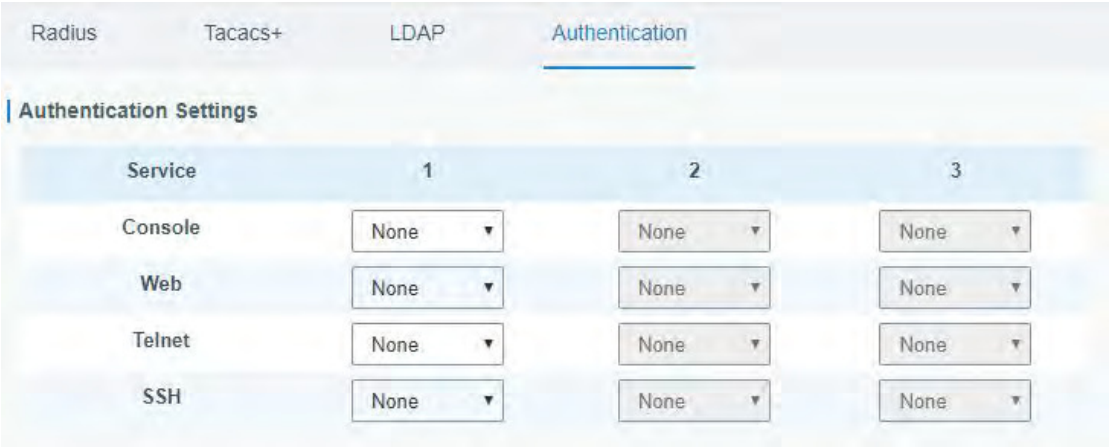



Figure 4-3-4-4

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

Table 4-3-4-4 Authentication Parameters

### 4.3.5 Device Management

You can connect the device to the device management platform on this page so as to manage the router centrally and remotely.

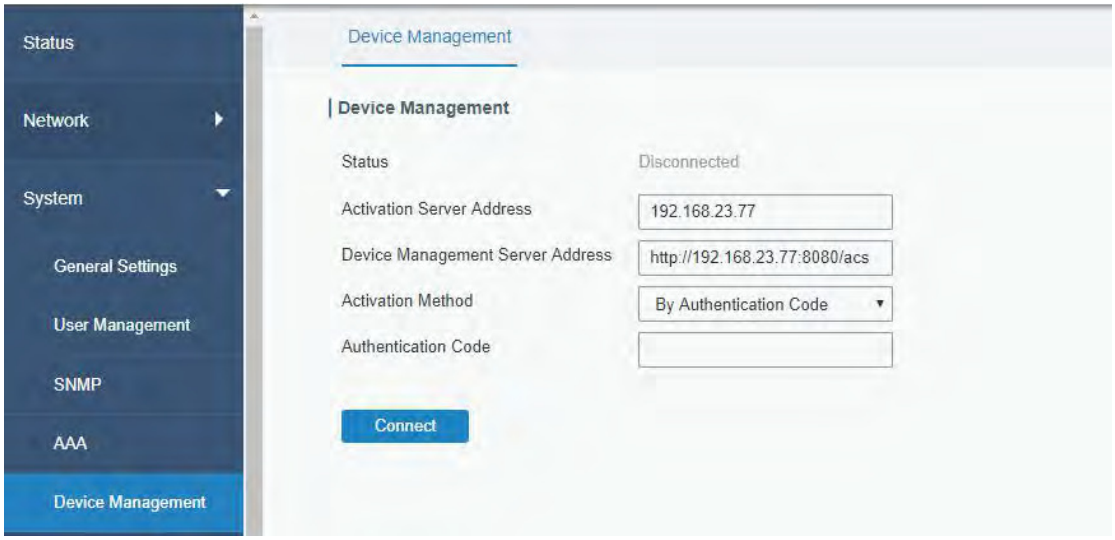



Figure 4-3-5-1

| Device Management | |
|---|---|
| **Item** | **Description** |
| Status | Show the connection status between the router and device management platform. |
| Disconnected | Click this button to disconnect the router from the device management platform. |
| Activation Server Address | IP address or domain of the device management server. |
| Device Management Server Address | The URL address for the device to connect to the device management service, e.g. http://220.82.63.79:8080/acs. |
| Activation Method | Select activation method to connect the router to the device management server, options are "By Authentication ID" and "By ID". |
| Authentication Code | Fill in the authentication code generated from the device management platform. |
| ID | Fill in the registered device management account (email) and password. |
| Password | |

Table 4-3-5-1

### 4.3.6 Events

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

#### 4.3.6.1 Events

You can view alarm messages on this page.

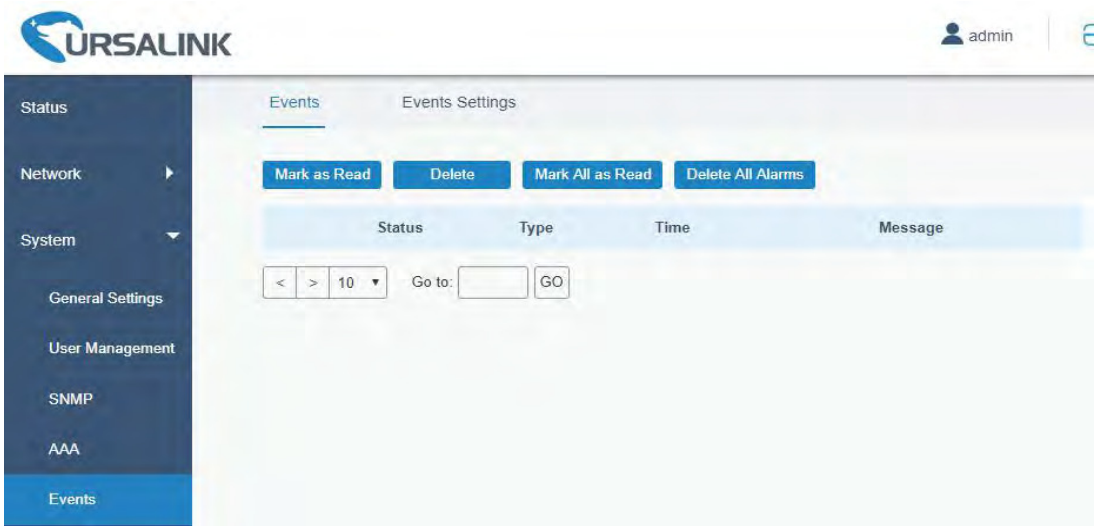



Figure 4-3-6-1

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

Table 4-3-6-1 Events Parameters

### 4.3.6.2 Events Settings

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

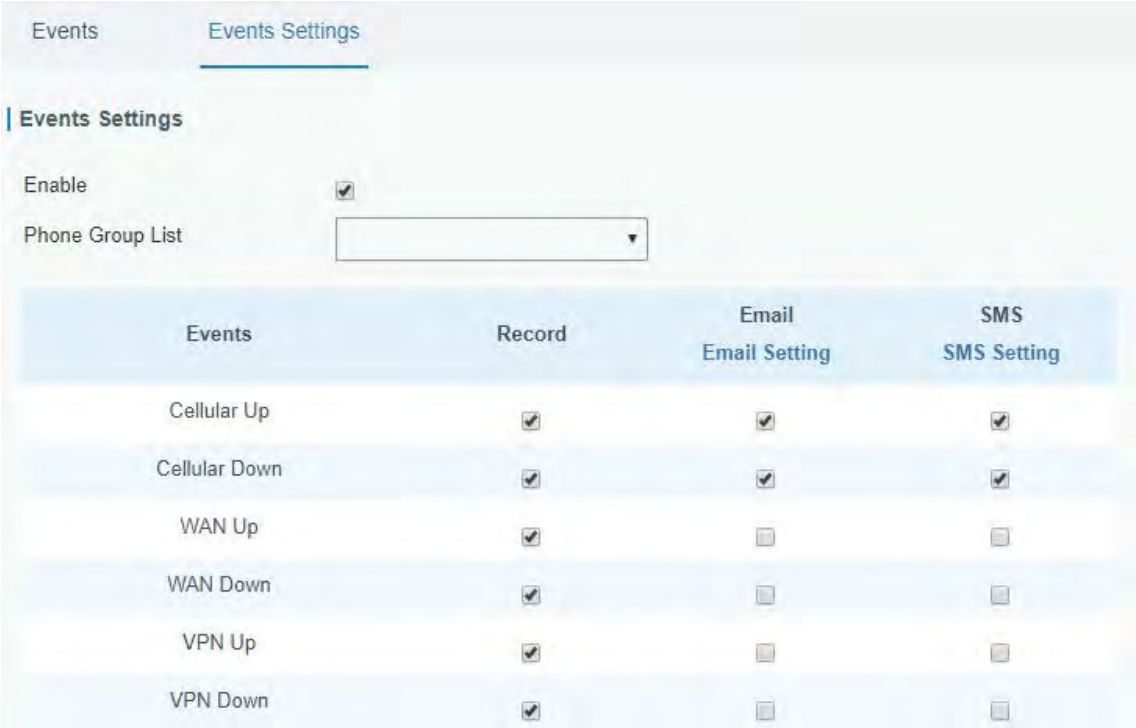



Figure 4-3-6-2

| Event Settings | |
|---|---|
| **Item** | **Description** |
| Enable | Check to enable "Events Settings". |
| Cellular Up | Cellular network is connected. |
| Cellular Down | Cellular network is disconnected. |
| WAN Up | Ethernet cable is connected to WAN port. |
| WAN Down | Ethernet cable is disconnected to WAN port. |
| VPN Up | VPN is connected. |
| VPN Down | VPN is disconnected. |
| 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 "SMTP" to configure the sender's & recipients' info. |
| 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. |
| Phone Group List | Select phone group to receive SMS alarm. |

Table 4-3-6-2 Events Parameters

**Related Topics**

Email Setting

Events Application Example

## 4.4 Industrial Interface

The UR71 router is capable of connecting with terminals through industrial interface so as to realize wireless communication between terminals and remote data center.

The router's industrial interface type is serial port (RS232 and RS485). Either RS232 or RS485 can be used at one time.

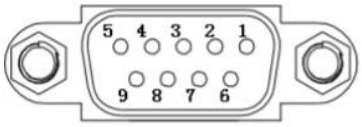



Figure 4-4-1 Pinouts

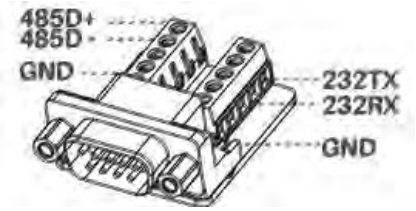



Figure 4-4-2 Terminal Block with a DB9 Male Connector for Serial Port Connection(Optional)

| PIN | RS232 | RS485 | Description |
|---|---|---|---|
| 1 | --- | A | Data + |
| 2 | RXD | --- | Receive Data |
| 3 | TXD | --- | Transmit Data |
| 4 | --- | --- | --- |
| 5 | GND | --- | Ground |
| 6 | --- | B | Data - |
| 7 | --- | --- | --- |
| 8 | --- | --- | --- |
| 9 | --- | --- | --- |

Table 4-4-1 Pinouts Definition

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

RS485 adopts half-duplex communication to achieve transmission of serial communication data with distance up to 1200 m.

### 4.4.1 Serial Port

Serial 1 is used for RS232 or RS485.

This section explains how to configure serial port parameters to achieve communication with serial terminals, and configure work mode to achieve communication with the remote data

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

Figure 4-4-1-1

| Serial Settings | | |
|---|---|---|
| **Item** | **Description** | **Default** |
| Enable | Enable or disable serial port function. | Disable |
| Serial Type | Select from RS232 or RS485 | -- |
| Baud Rate | Range is 300-230400. Same with the baud rate of the connected terminal device. | 9600 |
| Data Bits | Options are “8” and “7”. Same with the data bits of the connected terminal device. | 8 |
| Stop Bits | Options are “1” and “2”. Same with the stop bits of the connected terminal device. | 1 |
| Parity | Options are “None”, “Odd” and “Even”. Same with the parity of the connected terminal device. | None |
| Software Flow Control | Enable or disable software flow control. | Disable |
| Serial Mode | The option is "DTU Mode". The serial port can establish communication with the remote server/client. | DTU Mode |

Table 4-4-1-1 Serial Parameters

Figure 4-4-1-2

| DTU Mode | | |
|---|---|---|
| **Item** | **Description** | **Default** |
| DTU Protocol | Select from "None", "Transparent", "Modbus", and "TCP server".<br>- Transparent: the routed is used as TCP client/UDP and transmits data transparently.<br>- TCP server: the router is used as TCP server and transmits data transparently.<br>- Modbus: the router will be used as TCP server with modbus gateway function, which can achieve conversion between Modbus RTU and Modbus TCP. | -- |
| **TCP Server** | | |
| Listening port | Set the router listening port. Range: 1-65535. | 502 |
| Keepalive Interval | After TCP connection is established, router will send heartbeat packet to the client regularly by TCP to keep alive. The interval range is 1-3600 in seconds. | 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. The unit is byte. | 1024 |
| Serial Frame Interval | The interval that the router sends out real serial data stored in the buffer area to public network. The range is 10-65535, in milliseconds.<br>Note: data will be sent out to public network when real serial data size reaches the preset packet size, even though it's within the serial frame interval. | 100 |

Table 4-4-1-2 DTU Parameters

| Item | Description | Default |
|---|---|---|
| **Transparent** | | |
| Protocol | Select "TCP" or "UDP" protocol. | TCP |
| Keepalive Interval (s) | After TCP client is connected with TCP server, the client will send heartbeat packet by TCP regularly to keep alive. The interval range is 1-3600, in seconds. | 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. The unit is byte. | 1024 |
| Serial Frame Interval | The interval that the router sends out real serial data stored in the buffer area to public network. The range is 10-65535, in milliseconds.<br>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 10-60. | 10 |
| Specific Protocol | By Specific Protocol, the router will be able to connect to the TCP2COM software. | -- |
| Heartbeat Interval | By Specific Protocol, the router will send heartbeat packet to the server regularly to keep alive. The interval range is 1-3600, in seconds. | 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 |

Table 4-4-1-3 DTU Parameters

**Related Configuration Example**

DTU Application Example

### 4.4.2 Modbus Master

UR71 Router can be set as Modbus Master to poll the remote Modbus Slave and send alarm according to the response.

#### 4.4.2.1 Modbus Master

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

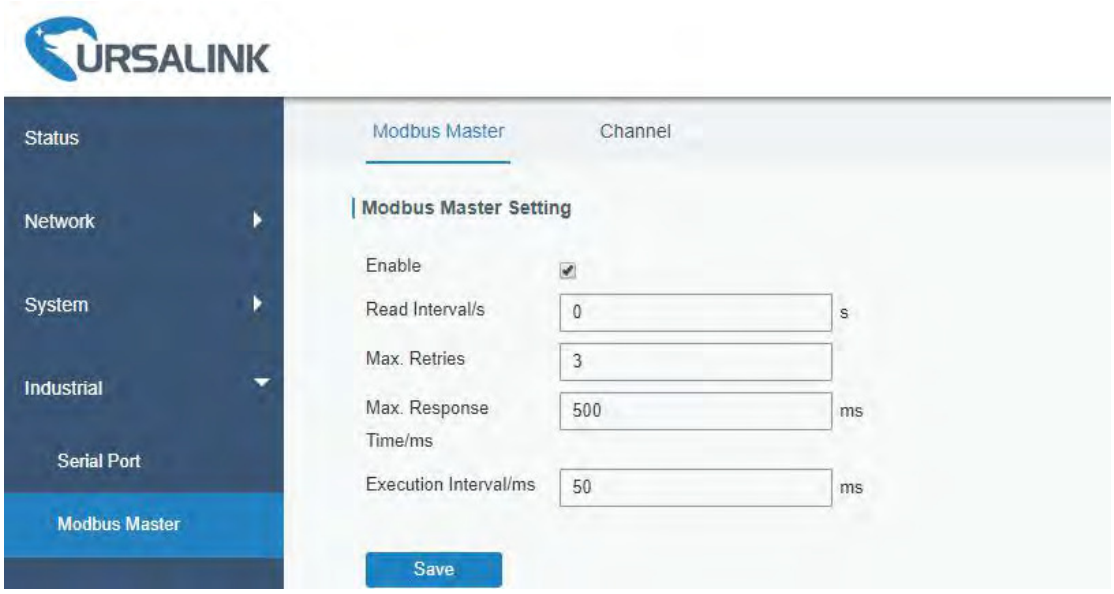



Figure 4-4-2-1

| Modbus Master | | |
|---|---|---|
| **Item** | **Description** | **Default** |
| Enable | Enable/disable Modbus master. | -- |
| 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. Response Time/ms | Set the maximum response time that the router waits for the response to the command. If the device does not get a response after the maximum response time, it's determined that the command has timed out. Range: 10-1000. | 500 |
| Execution Interval/ms | The execution interval between each command. Range: 10-1000. | 50 |

Table 4-4-2-1

#### 4.4.2.2 Channel

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

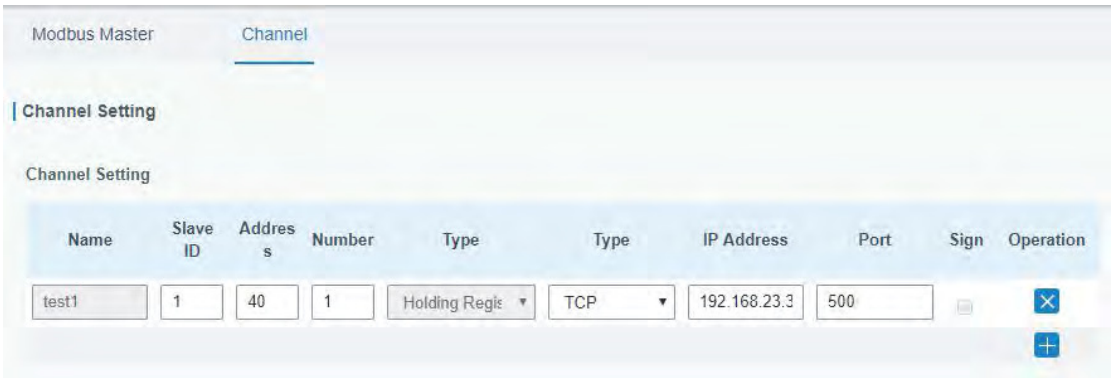



Figure 4-4-2-2

| Channel Setting | |
|---|---|
| **Item** | **Description** |
| Name | Set the name to identify the remote channel. It cannot be blank. |
| Slave ID | Set Modbus slave ID. |
| Address | The starting address for reading. |
| Number | The address number for reading. |
| Type | Read command, options are "Coil", "Discrete", "Holding Register (INT16)", "Input Register (INT16)", "Holding Register (INT32)" and "Holding Register (Float)". |
| Link | Select TCP for transportation. |
| IP address | Fill in the IP address of the remote Modbus device. |
| Port | Fill in the port of the remote Modbus device. |
| Sign | To identify whether this channel is signed. Default: Unsigned. |

Table 4-4-2-2

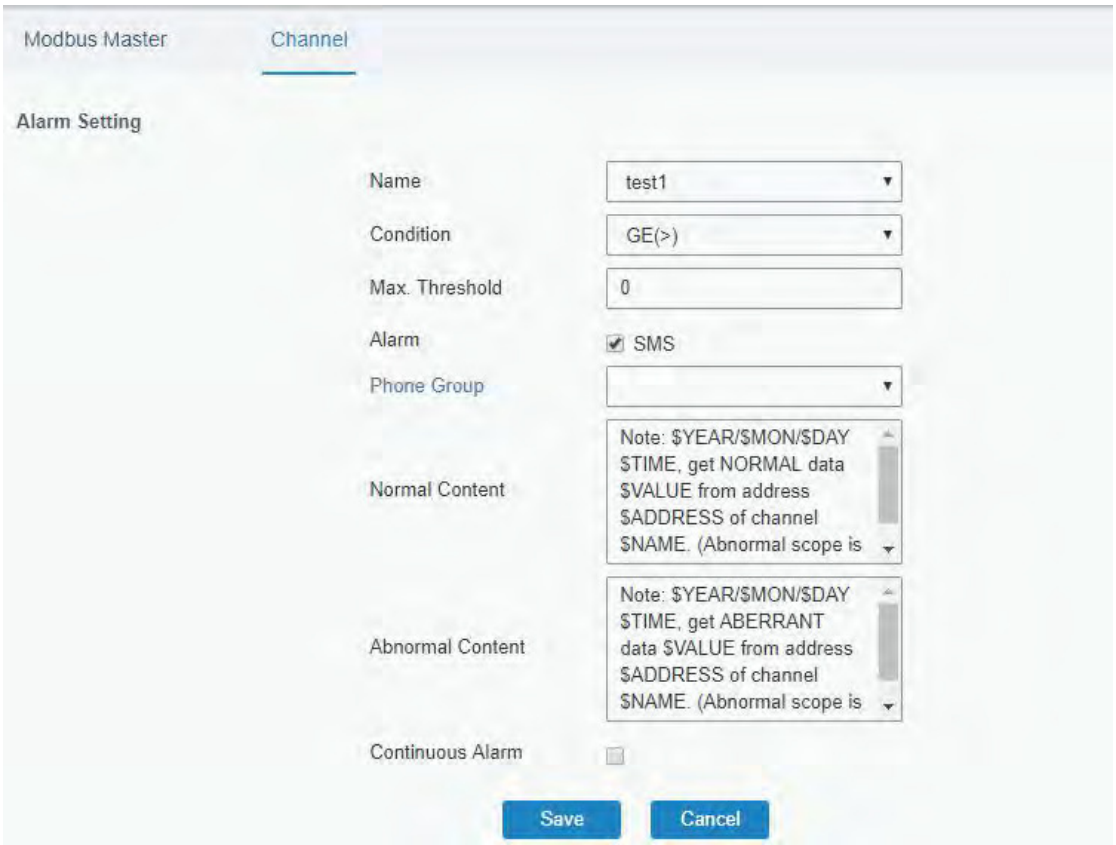



Figure 4-4-2-3

| 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. |
| 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. |

Table 4-4-2-3

## 4.5 Maintenance

This section describes system maintenance tools and management.

### 4.5.1 Tools

Troubleshooting tools includes ping and traceroute.

#### 4.5.1.1 Ping

Ping tool is engineered to ping outer network.

Figure 4-5-1-1

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

Table 4-5-1-1 IP Ping Parameters

#### 4.5.1.2 Traceroute

Traceroute tool is used for troubleshooting network routing failures.

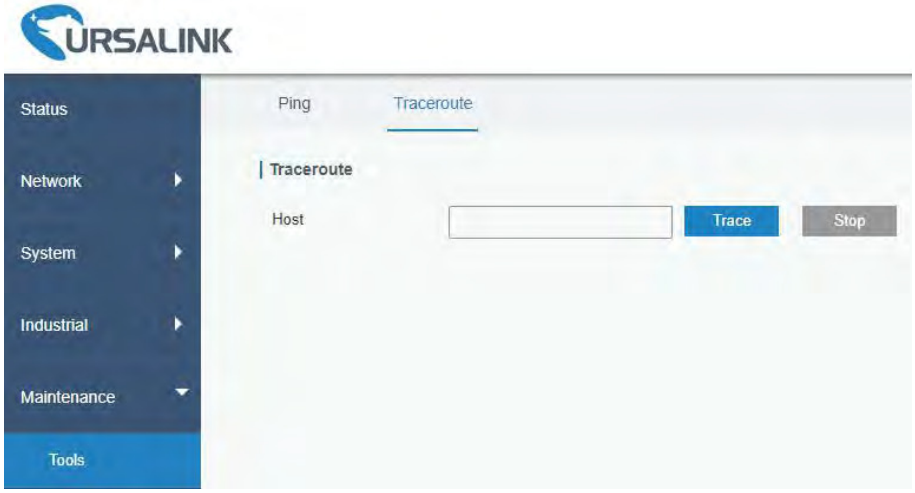



Figure 4-5-1-2

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

Table 4-5-1-2 Traceroute Parameters

### 4.5.2 Schedule

This section explains how to configure scheduled reboot on the router.

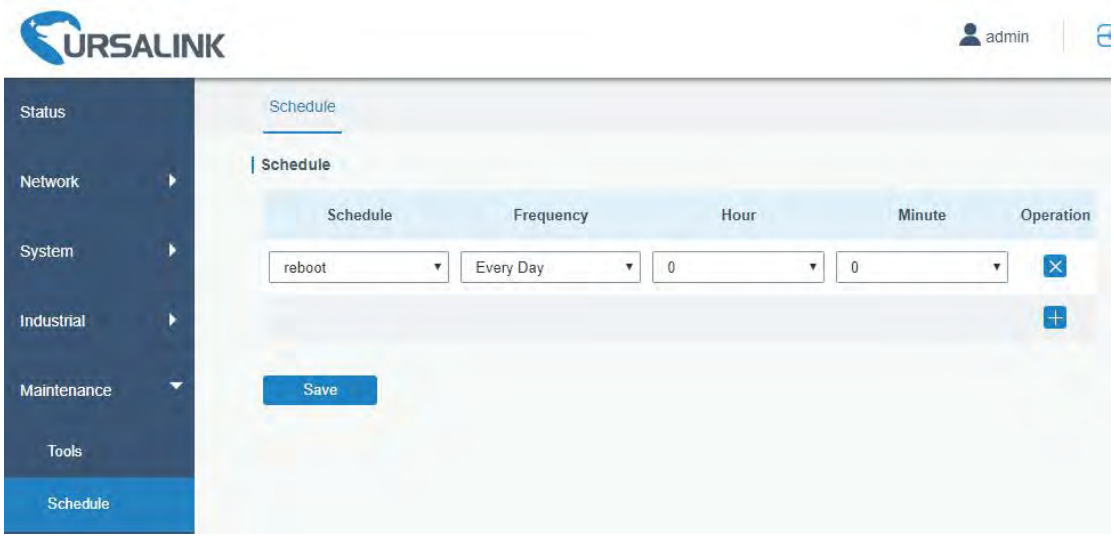



Figure 4-5-2-1

| Schedule | |
|---|---|
| **Item** | **Description** |
| Schedule | Select schedule type. |
| Reboot | Reboot the router regularly. |
| Frequency | Select the frequency to execute the schedule. |
| Hour & Minute | Select the time to execute the schedule. |

Table 4-5-2-1 Schedule Parameters

**Related Configuration Example**

Schedule Application Example

### 4.5.3 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.

**Related Configuration Example**

Logs and Diagnostics

### 4.5.3.1 System Log

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

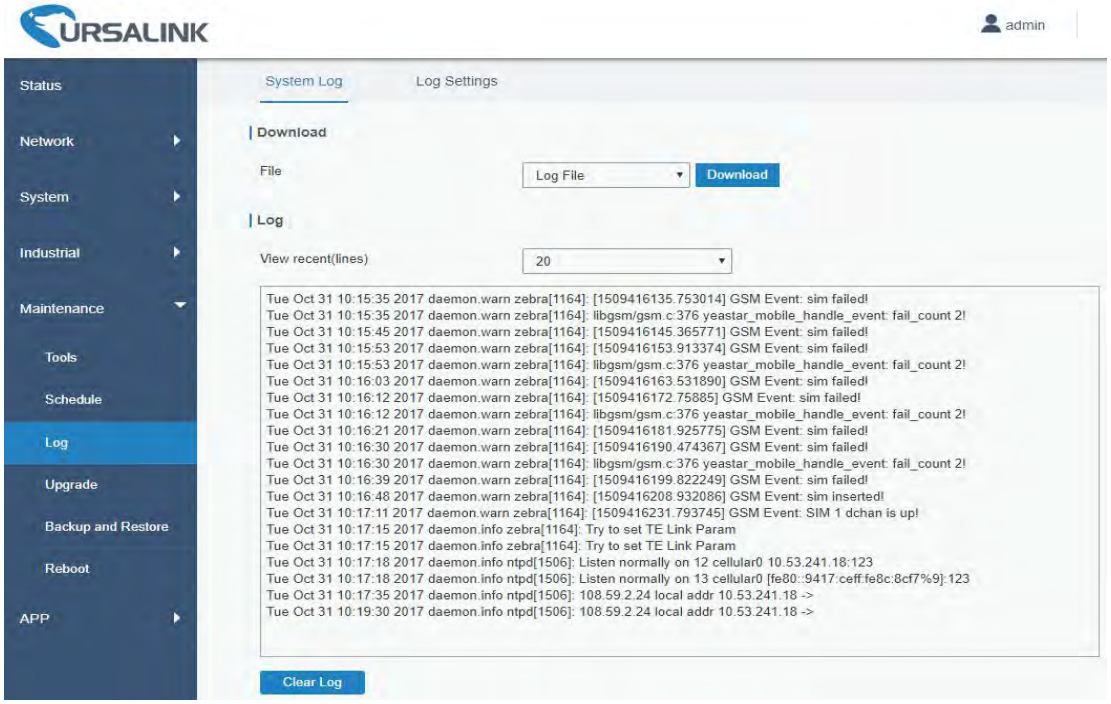



Figure 4-5-3-1

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

Table 4-5-3-1 System Log Parameters

### 4.5.3.2 Log Settings

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

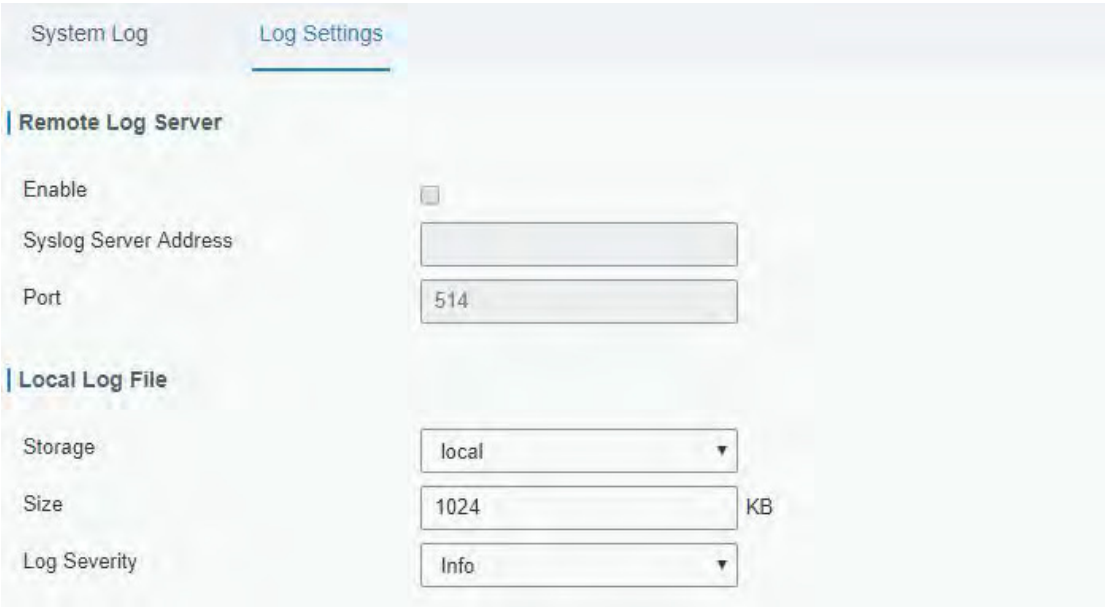



Figure 4-5-3-2

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

Table 4-5-3-2 System Log Parameters

### 4.5.4 Upgrade

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

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

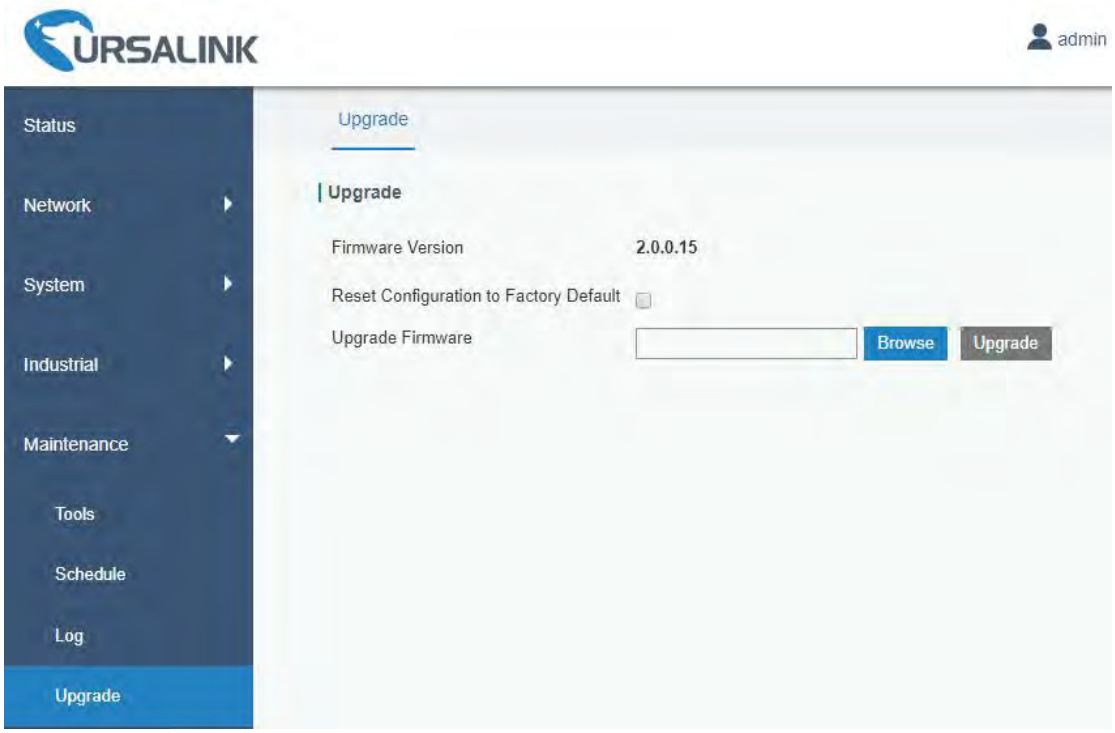



Figure 4-5-4-1

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

Table 4-5-4-1 Upgrade Parameters

**Related Configuration Example**

Firmware Upgrade

### 4.5.5 Backup and Restore

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

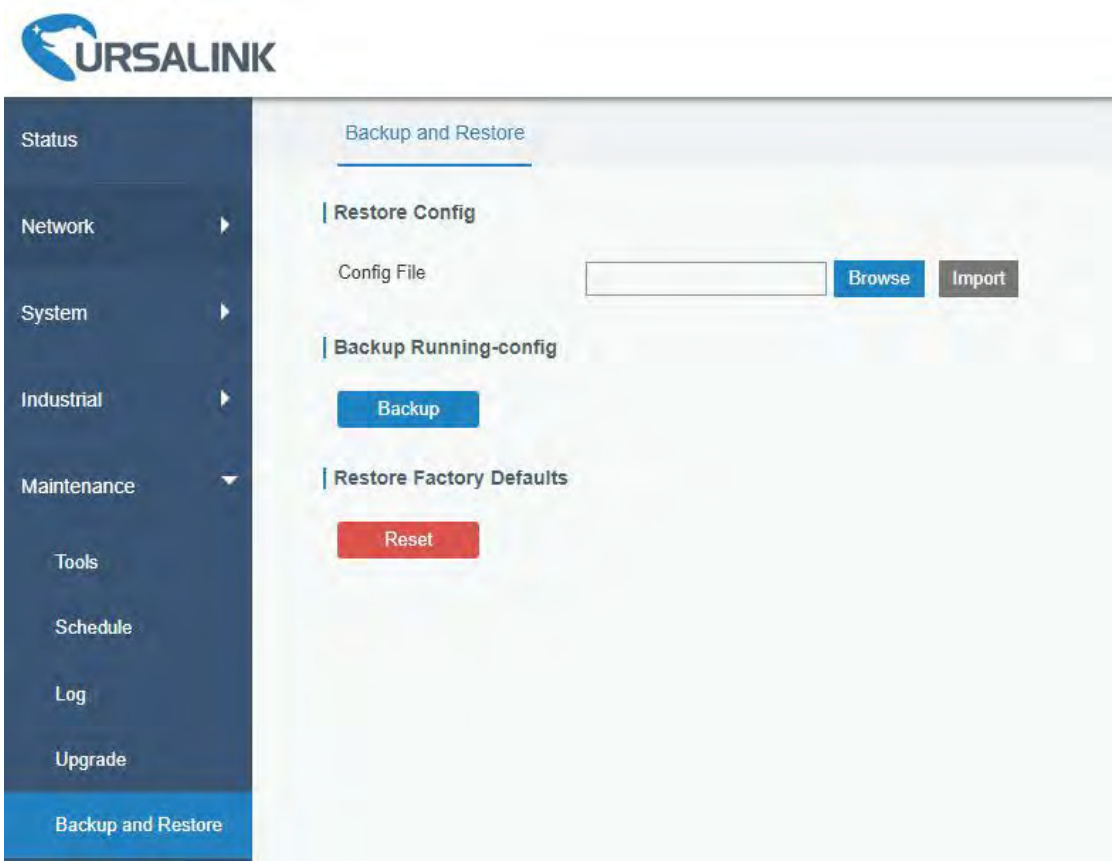



Figure 4-5-5-1

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

Table 4-5-5-1 Backup and Restore Parameters

**Related Configuration Example**

Backup and Restore Configuration

Restore Factory Defaults

### 4.5.6 Reboot

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

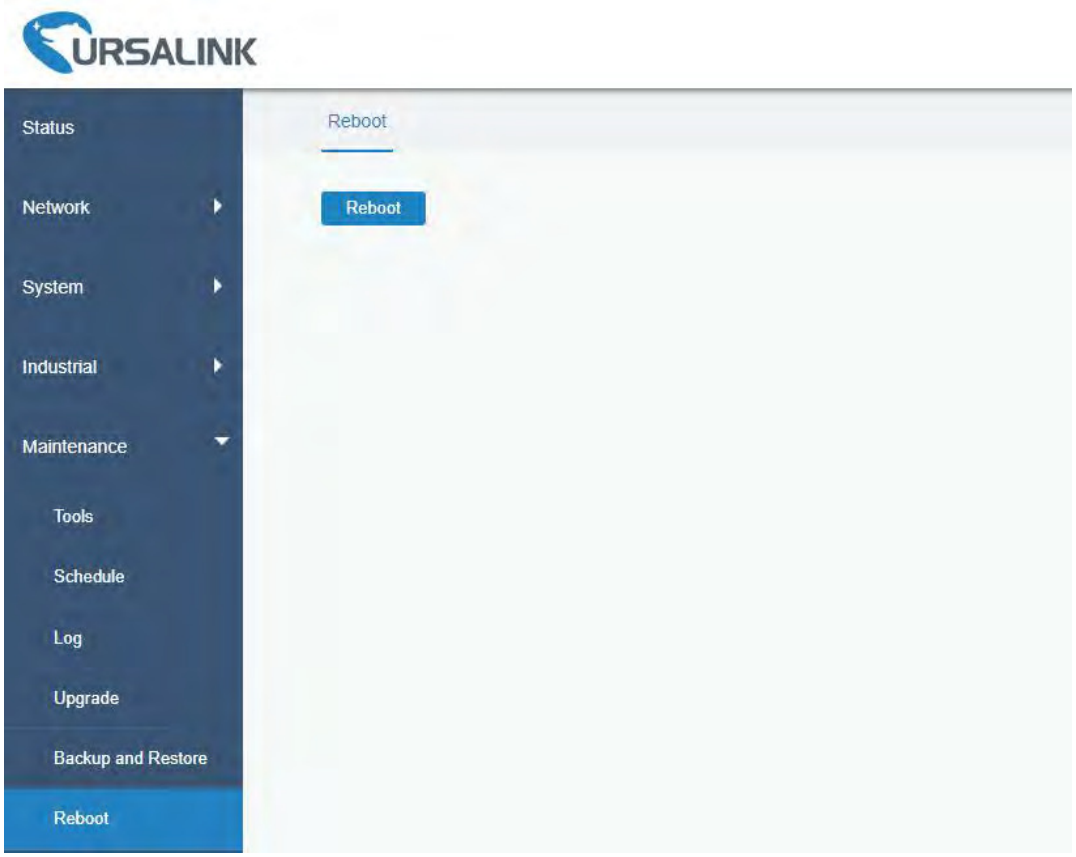



Figure 4-5-6-1

## 4.6 APP

### 4.6.1 Python

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

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

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

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

#### 4.6.1.1 Python

Micro SD card/SSD must be installed for Python App.

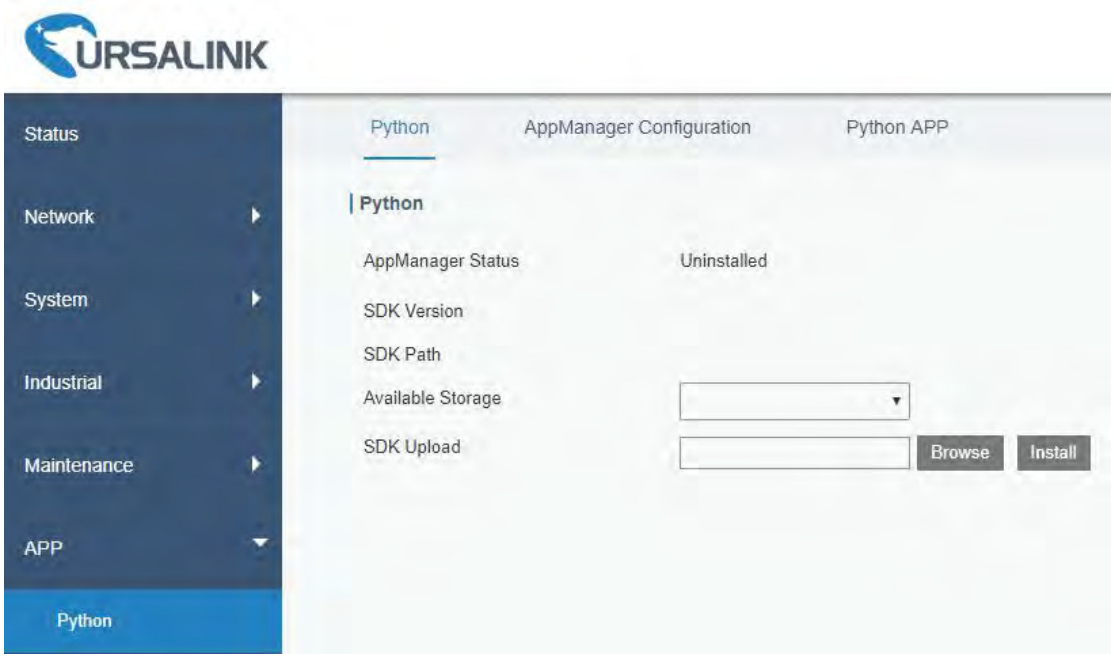



Figure 4-6-1-1

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

Table 4-6-1-1 Python Parameters

### 4.6.1.2 App Manager Configuration

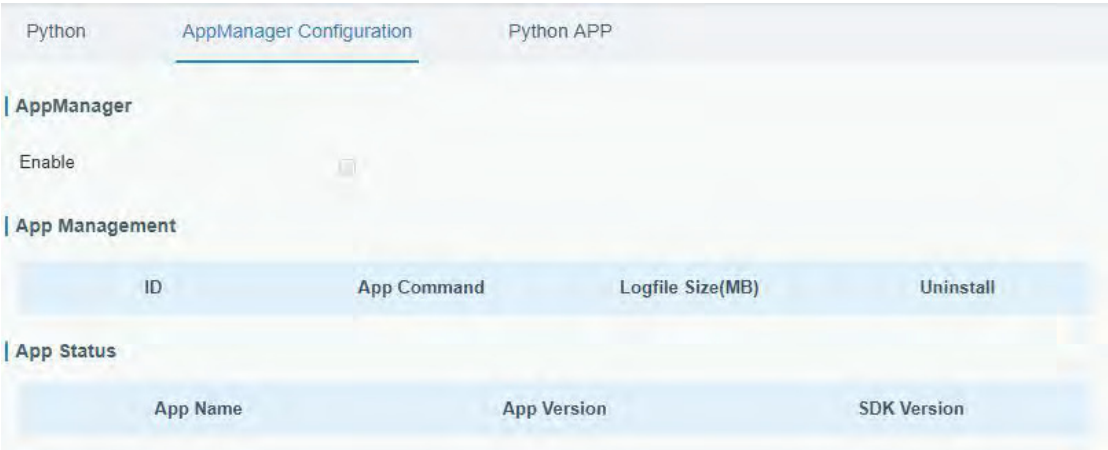



Figure 4-6-1-2

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

Table 4-6-1-2 APP Manager Parameters

#### 4.6.1.3 Python App

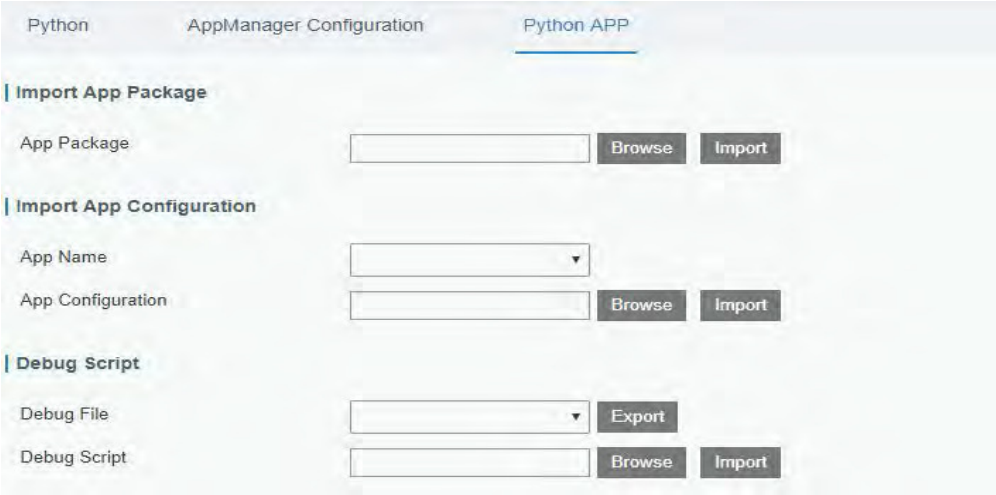



Figure 4-6-1-3

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

Table 4-6-1-3 APP Parameters

# Chapter 5 Application Examples

## 5.1 Account Info Management

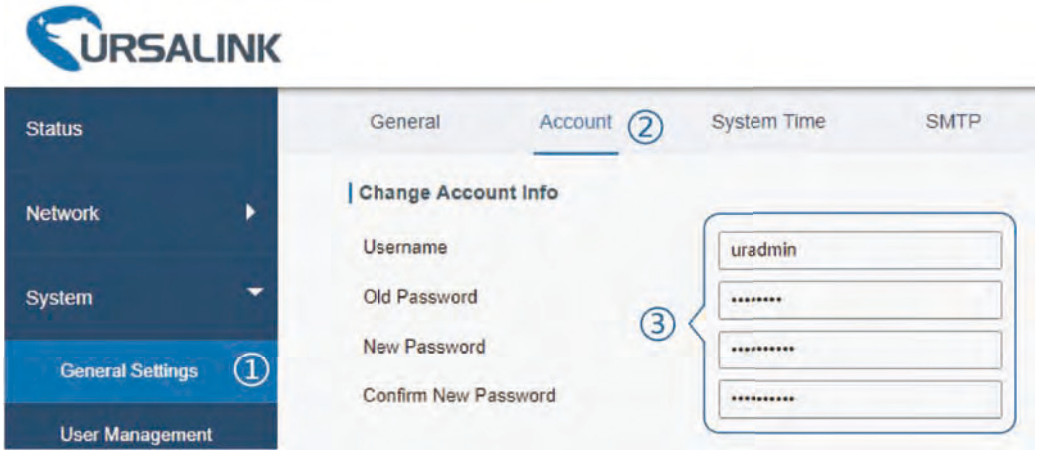
It is strongly recommended that you change the default username and password of the administrator account when you log in Ursalink Router's WEB GUI page at first time for the sake of security.

Example: change the username and password of administrator account to "uradmin" and "URpassword".

The configuration procedures are listed as below.

1. Go to "System > General Settings > Account".
2. Modify the username to "uradmin", fill in the old Password "password", and set the new Password "URpassword".

Click "Save" button, and then you will be asked to login again with the new username and password.




**Related Topic**

Account Management

## 5.2 Common User Management

The UR71 router is capable of creating up to 5 common user accounts that have different authorities, including "Read-Only" and "Read-Write" to manage the router.

"Read-Only" refers to the authority that user is only allowed to view the configuration;

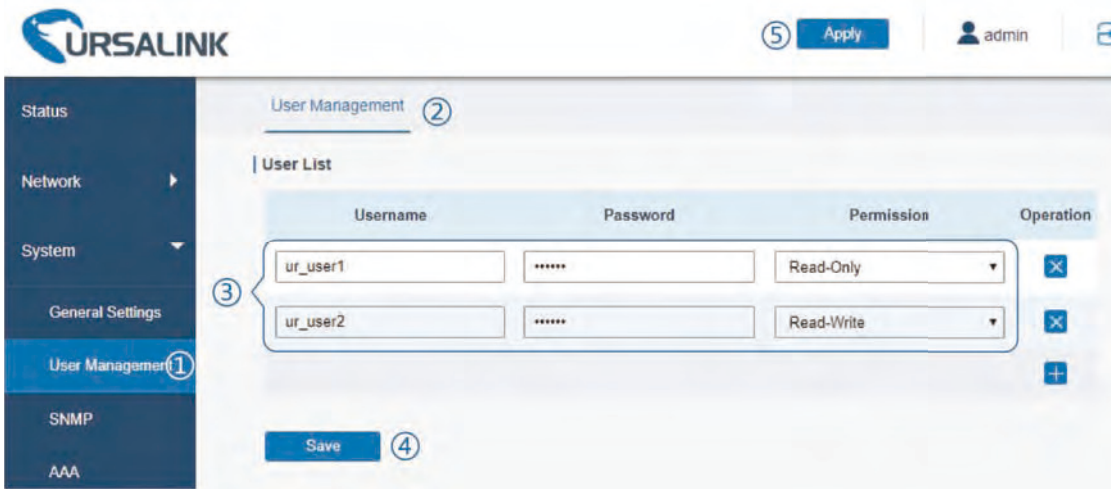
"Read-Write" refers to the authority that user can view and modify all the parameters.

Example: create 2 common user accounts listed below.

| Username | Password | Permission |
|---|---|---|
| ur_user1 | UR_password1 | Read-Only |
| ur_user2 | UR_password2 | Read-Write |

Configuration procedures are listed as blow.

1. Go to "System > User Management > User Management".
2. Click "+" to add a new common user.
3. Set "Username", "Password", and "Permission" as below.




Click “Save” button, and then click “Apply” on the top-right corner to make the changes take effect.

**Related Topic**

User Management

## 5.3 System Time Management

There are 3 ways to synchronize the system time: “Sync with Browser”, “Set up Manually”, and “Sync with NTP Server”.

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

In the following part we take UTC+8 time zone as an example.

### A. Synchronize time with browser

Go to “System > General Settings > System Time”, set time zone as “8 China (Beijing)” and Sync Type as “Sync with Browser”. And Click “Save” button.

### B. Set up time by manual

1. Go to “System > General Settings > System Time”, set time zone as “8 China (Beijing)” and Sync Type as “Set up Manually”.

2. Select the correct local time. And click “Save” button.

**C. Synchronize time with NTP server**

1. Go to “System > General Settings > System Time”, set time zone as “8 China (Beijing)” and Sync Type as “Sync with NTP Server”.
2. Configure an available NTP server address such as “time.windows.com”. Click “Save” button.

**Related Topic**

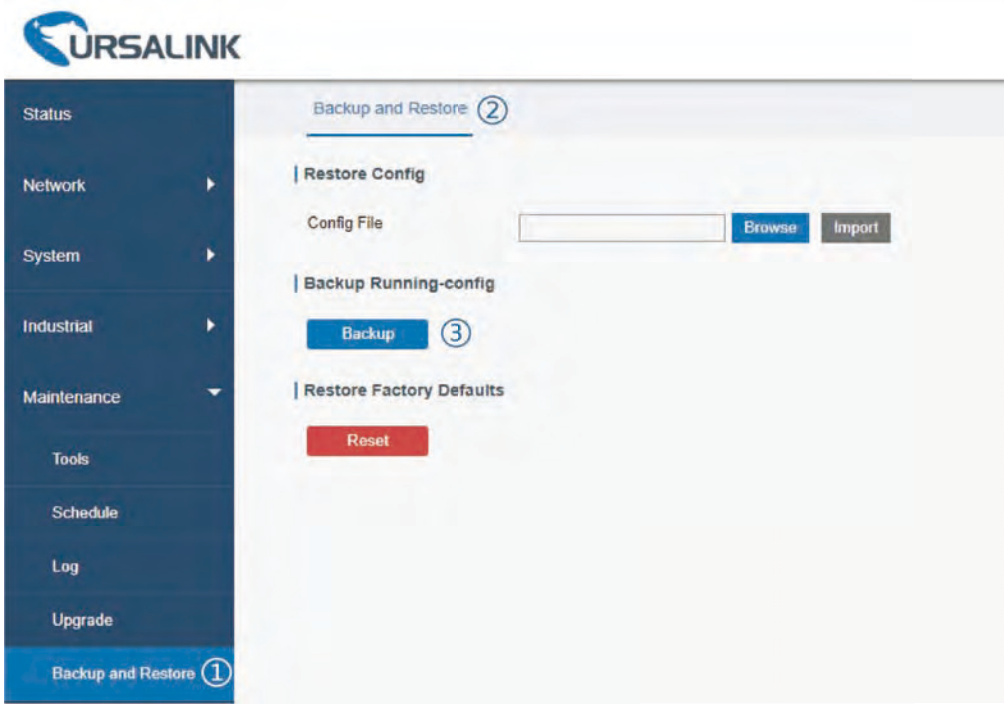
[System Time Setting]

## 5.4 Backup and Restore Configuration

**A. Backup Configuration**

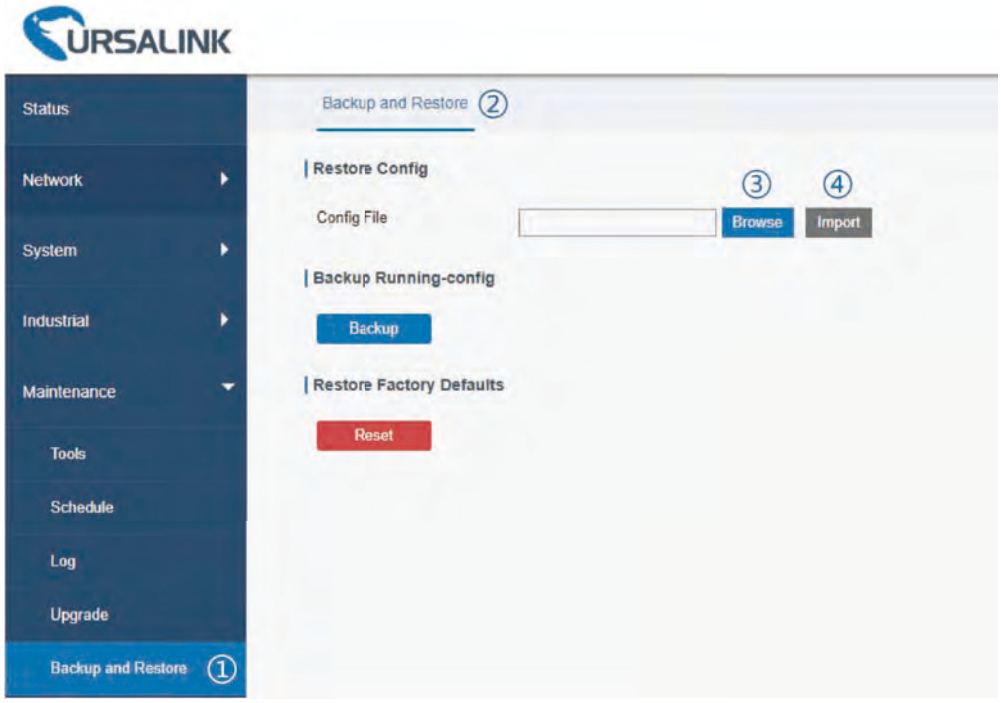
1. Go to “Maintenance > Backup and Restore > Backup and Restore”.
2. Click “Backup” button under “Backup running-config”.

Then the current configuration file will be downloaded to the “Downloads” folder of the PC.




**B. Restore Configuration**

1. Go to “Maintenance > Backup and Restore > Backup and Restore”.
2. Click “Browse” button under the “Restore” to select configuration file from PC.
3. Click “Import” to import the selected configuration file to the router.




**Related Topic**

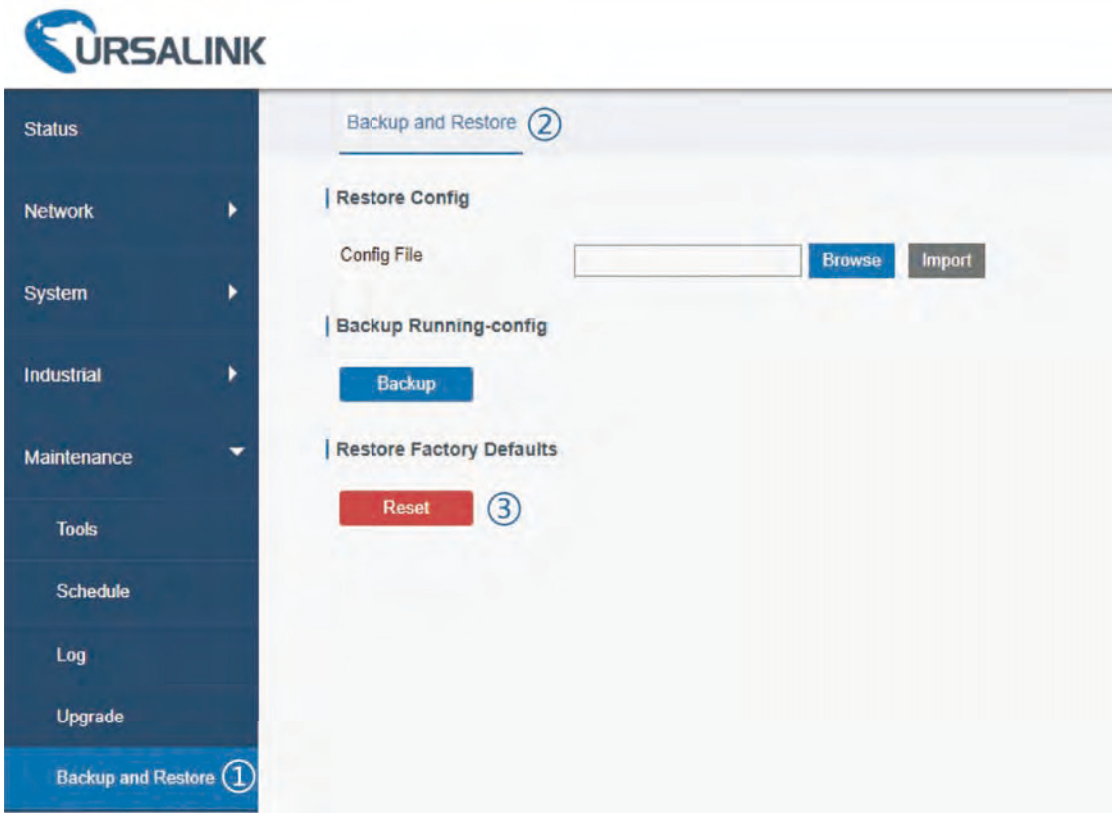
[Backup and Restore]

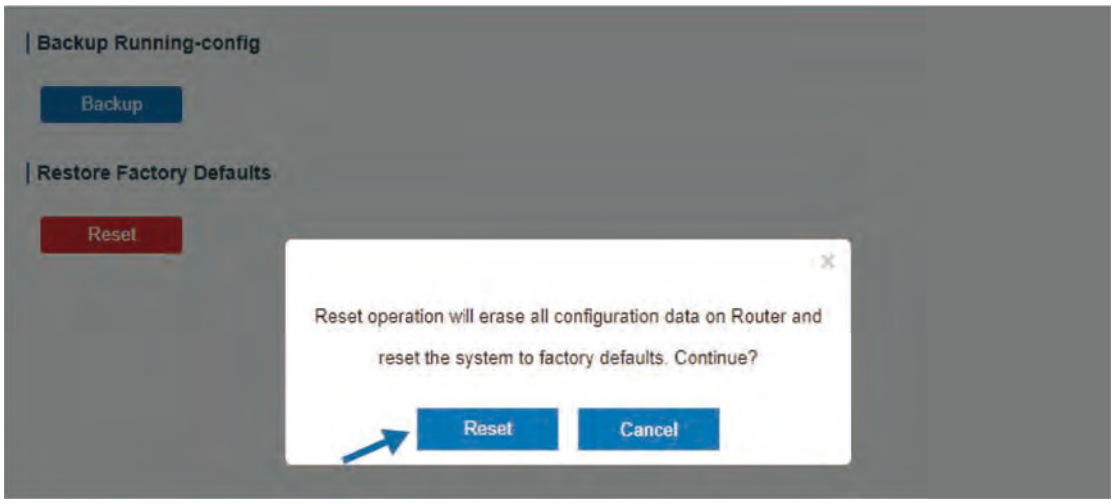
## 5.5 Restore Factory Defaults

### 5.5.1 Via Web Interface

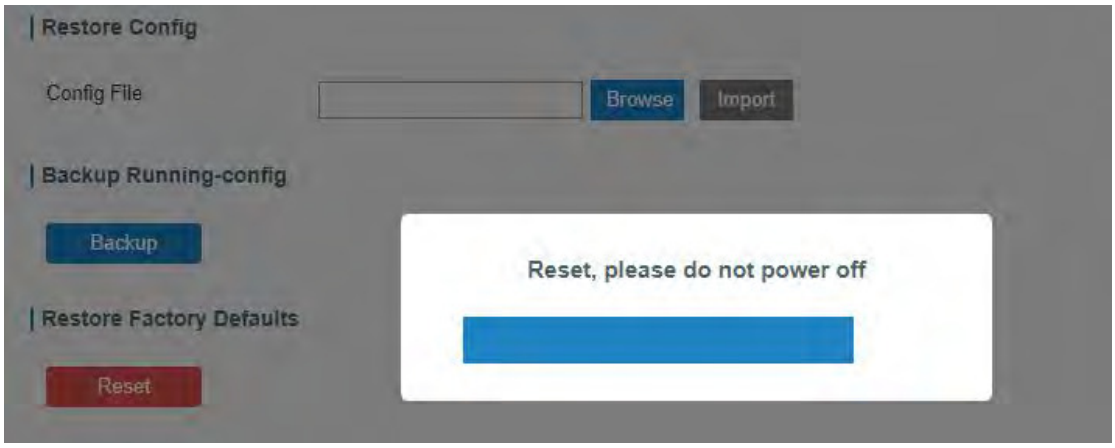
1. Log in web interface, and go to “Maintenance > Backup and Restore”.
2. Click “Reset” button under the “Restore Factory Defaults”.

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 login page pops up again, which means the router has already been reset to factory defaults successfully.

**Related Topic**

Restore Factory Defaults

### 5.5.2 Via Hardware

Locate the reset button on the router, and take corresponding actions based on the status of STATS LED.

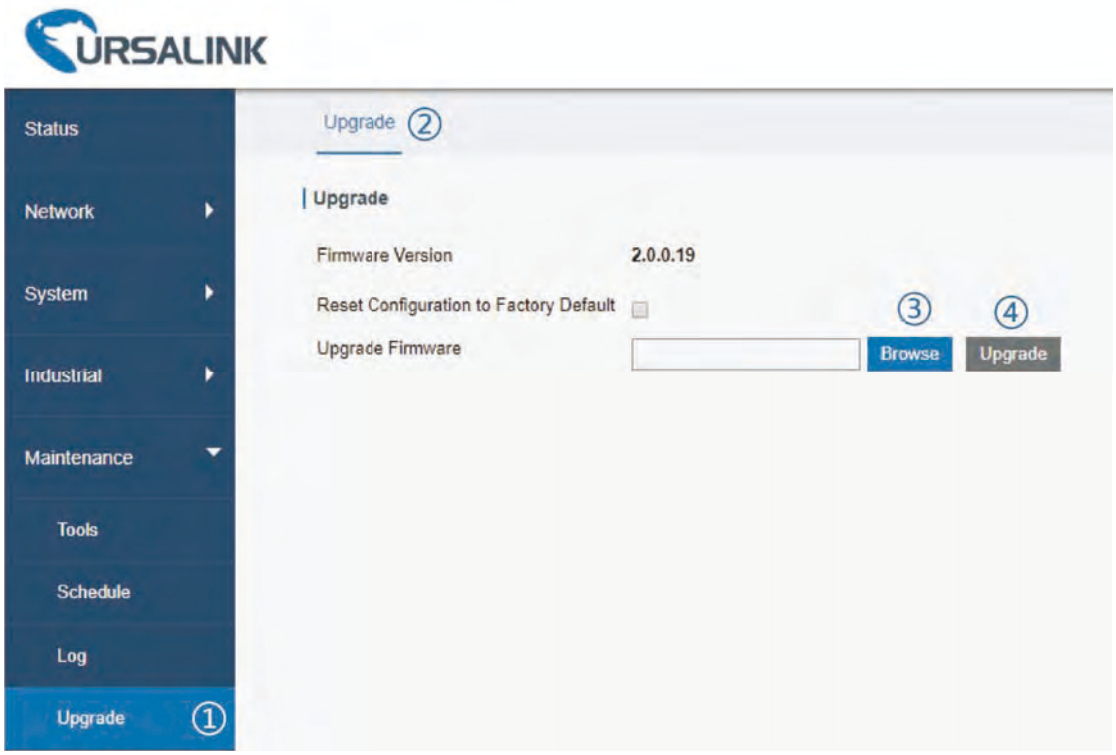
| STATUS LED | Action |
|---|---|
| Blinking | Press and hold the reset button for more than 15 seconds. |
| Static Green → Rapidly Blinking | Release the button and wait. |
| Off → Blinking | The router is now reset to factory defaults. |

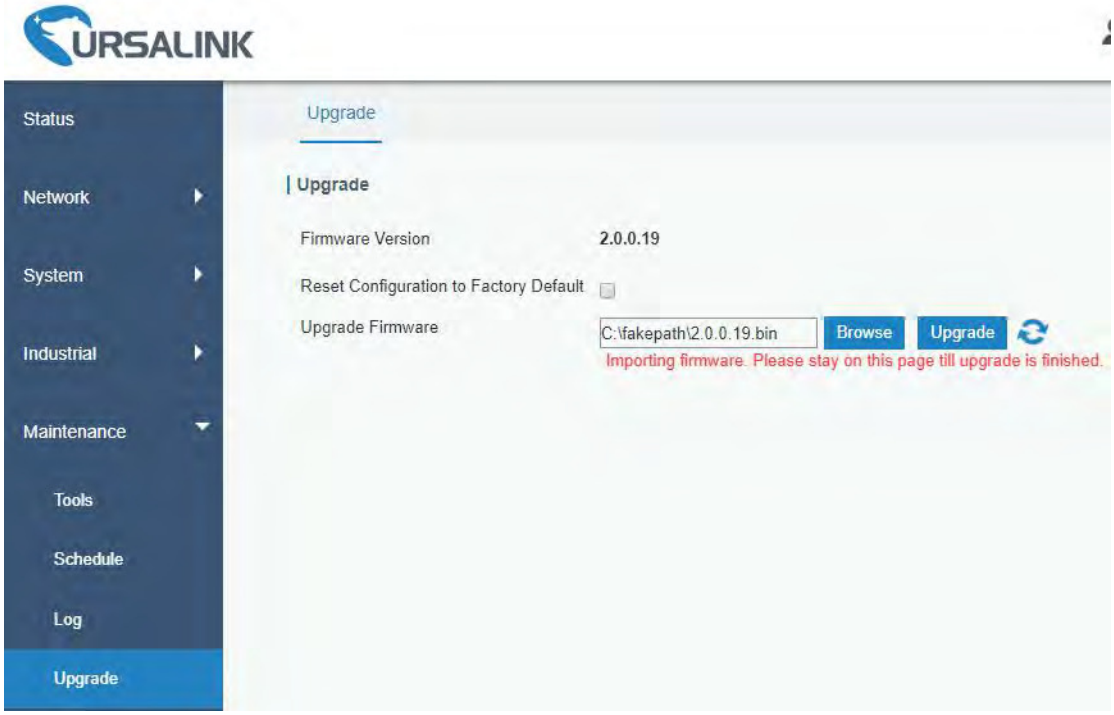
### 5.6 Firmware Upgrade

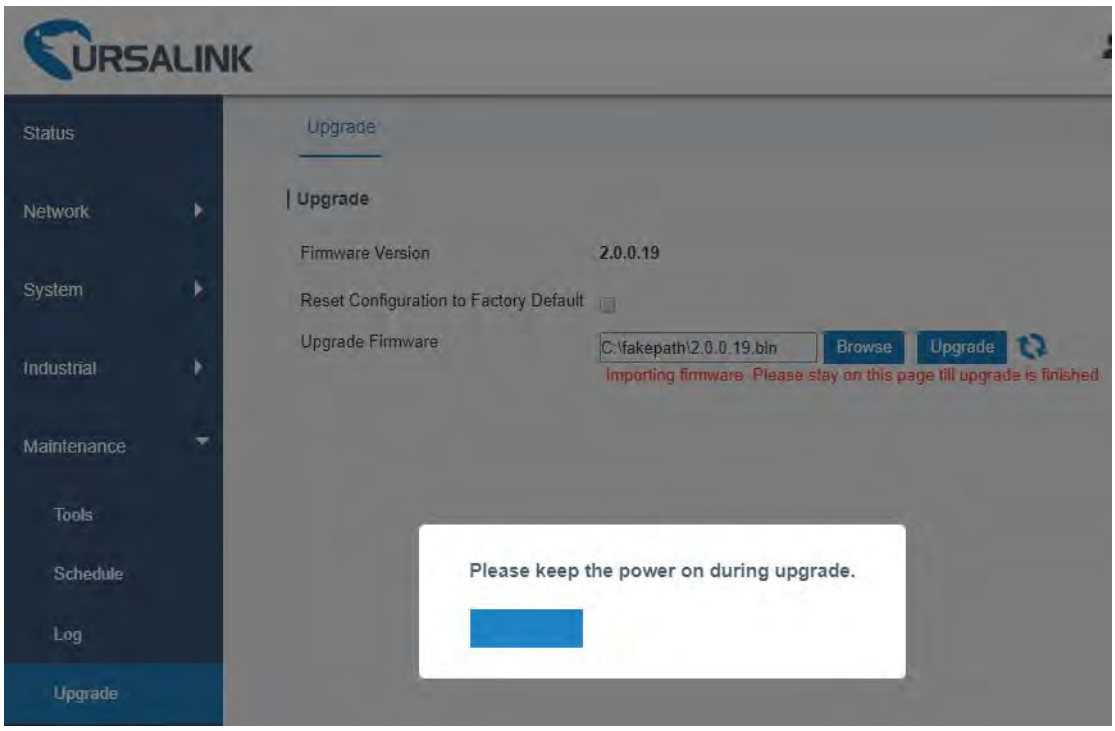
It is suggested that you contact Ursalink technical support first before you upgrade router firmware.

After getting firmware file from Ursalink technical support, please refer to the following steps to complete the upgrade.

1. Go to “Maintenance > Upgrade”.
2. Click “Browse” and select the correct firmware file from the PC.
3. 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.






**Related Topic**

Upgrade

## 5.7 Events Application Example

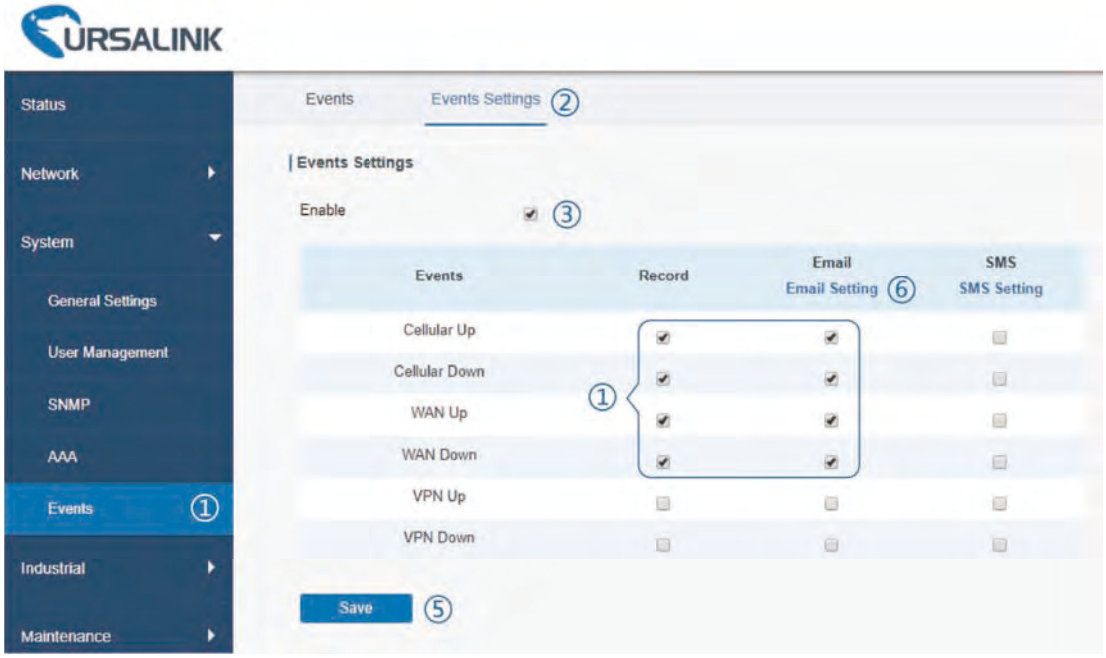
### Example

In this section, we will take an example of sending alarm messages by email when the following events occur and recording the event alarms on the Web GUI.

| Events | Actions to make events occur (for test) |
|---|---|
| Cellular network is connected. | Insert SIM card. |
| Cellular network is disconnected. | Remove SIM card. |
| WAN cable is connected. | Plug WAN cable. |
| WAN cable is disconnected. | Unplug WAN cable. |

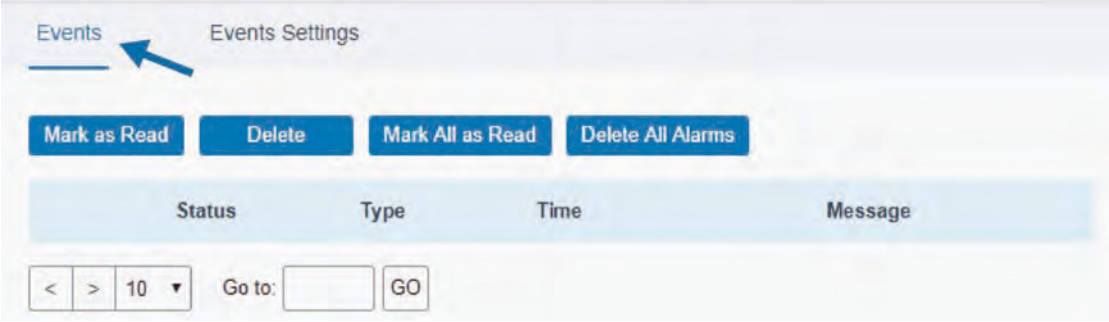
### Configuration Steps

1. Go to “System > Events > Events Settings” and enable Event settings.
2. Check corresponding events for record and email alarm, and then click “Save” button as below. Click “Email Settings” and go to SMTP settings.




Configure the corresponding parameters including email sending settings and recipients as below. Click “Save” and “Apply” button to make the changes take effect.

3. To test the functionality of Alarm, please take the corresponding actions listed above. It will send an alarm e-mail to you when the relevant event occurs. Refresh the web GUI, go to "Events > Events", and you will find the events records.




**Related Topics**

Events

Email Setting

## 5.8 Schedule Application Example

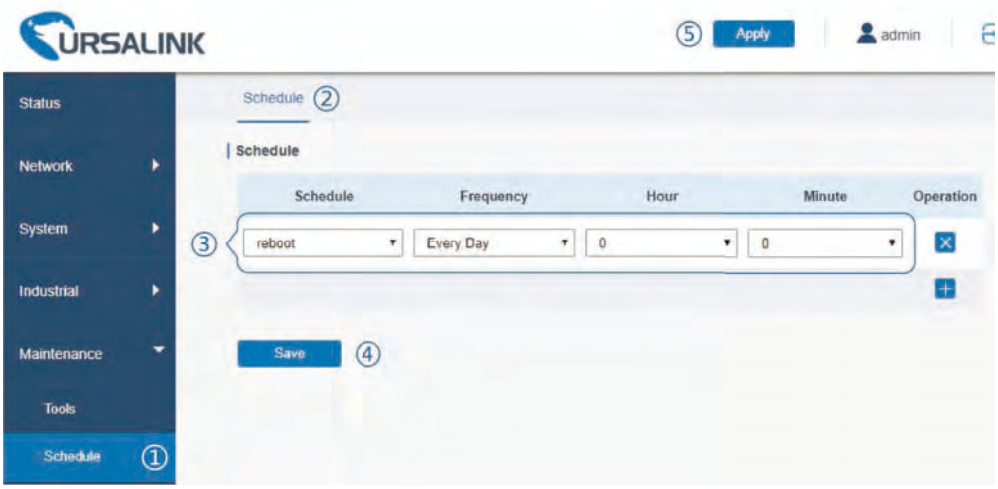
Through schedule configuration, the UR71 can be set to reboot at preset time every day.

**Example**

Configure router to reboot at 0:00 every day.

**Configuration Steps**

1. Go to "Maintenance > Schedule > Schedule".
2. Click "+" to set up a new schedule task as below.
3. Click "Save" and "Apply" button.




**Related Topic**

[Schedule Setting]

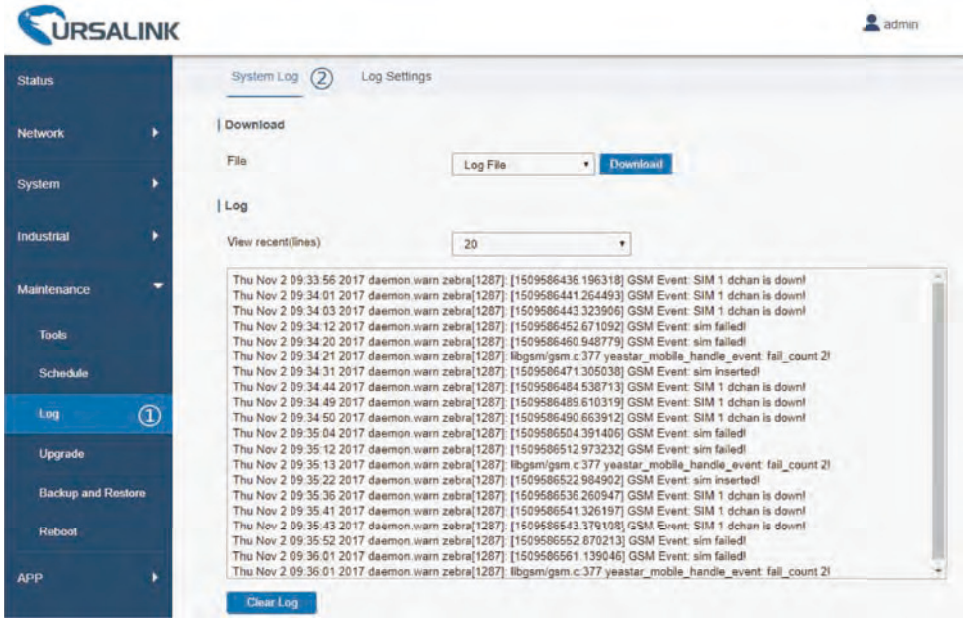
## 5.9 Logs and Diagnostics

System log of the UR71 supports 2 types of output method, including Web, Remote Log Server and Console.

**Application 1**

Obtain system log on Web.

Go to "Maintenance > Log > System log", and you will see the log is listed in the box.

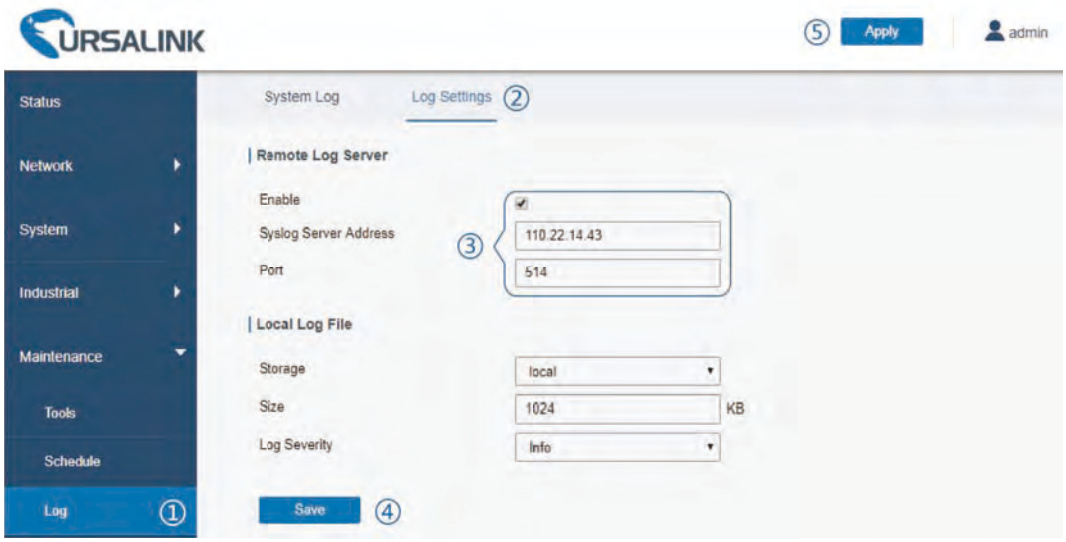



**Application 2**

Send the system log to the remote syslog server.

Server IP: 110.22.14.43; Port: 514

Go to "Maintenance > Log > Log Settings" to configure the parameters as below.




Then click “Save” and “Apply” button.

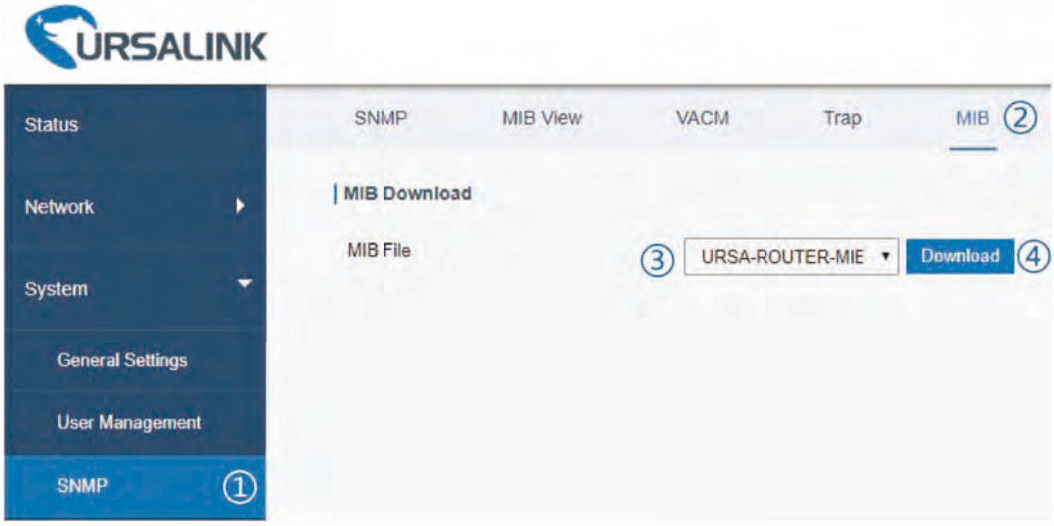
**Related Topic**

System Log

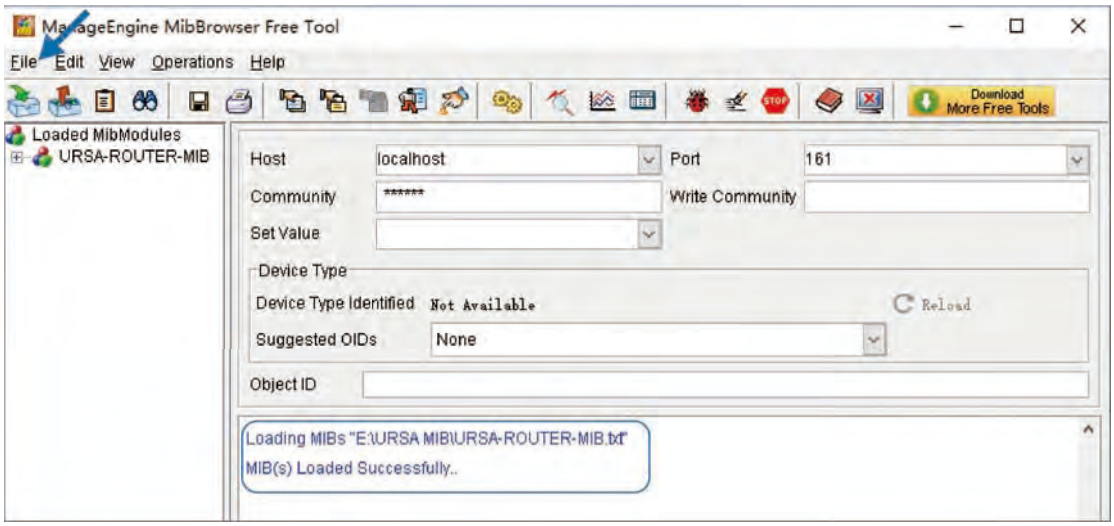
## 5.10 SNMP Application Example

Before you configure SNMP parameters, please download the relevant “MIB” file from the UR71’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.

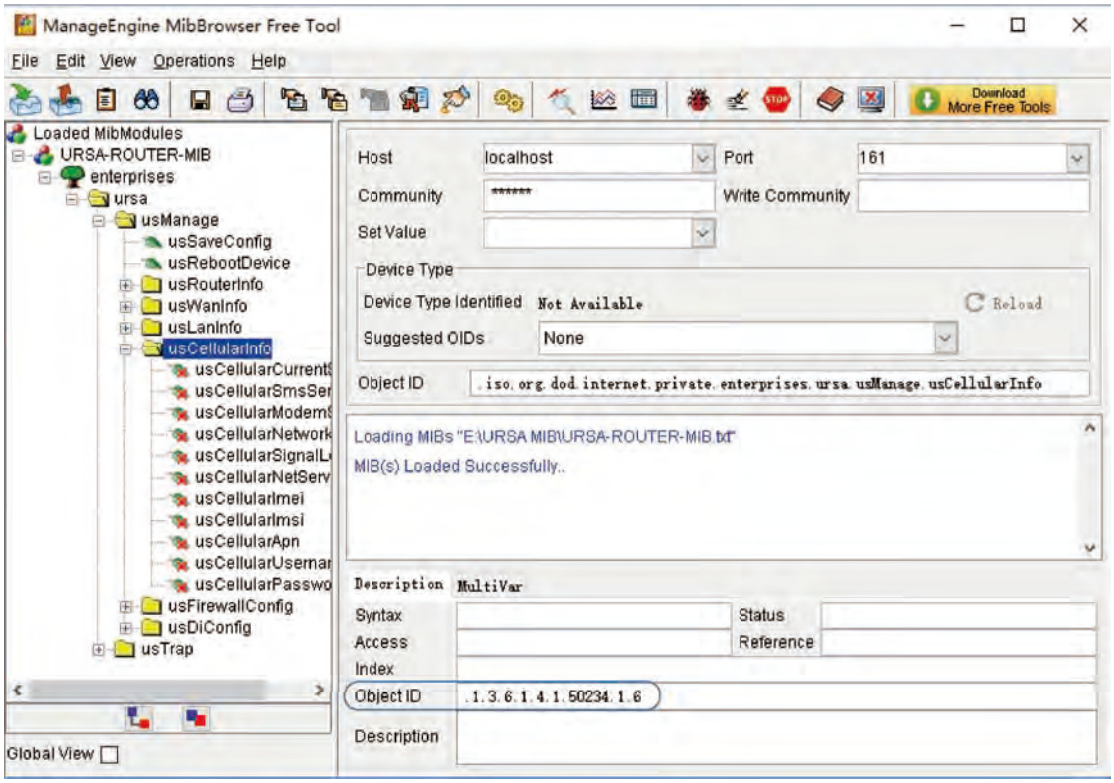
1. Go to “System > SNMP > MIB” and download the MIB file “URSA-ROUTER-MIB.txt” to PC.



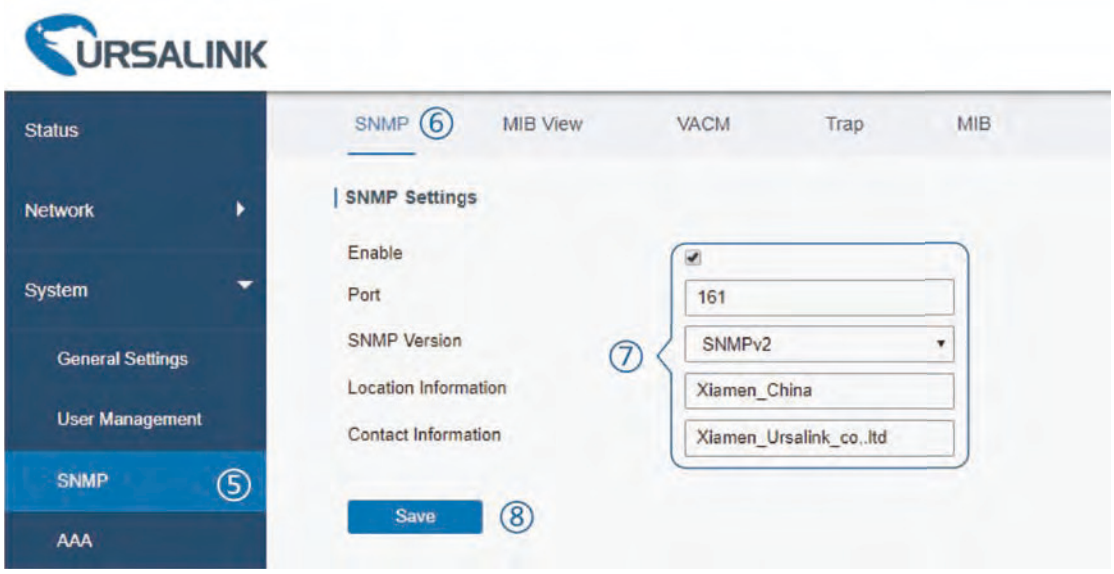

2. Start “ManageEngine MibBrowser Free Tool” on the PC. Click “File > Load MIB” on the menu bar. Then select “BURSA-ROUTER-MIB.txt” file from PC and upload it to the software.



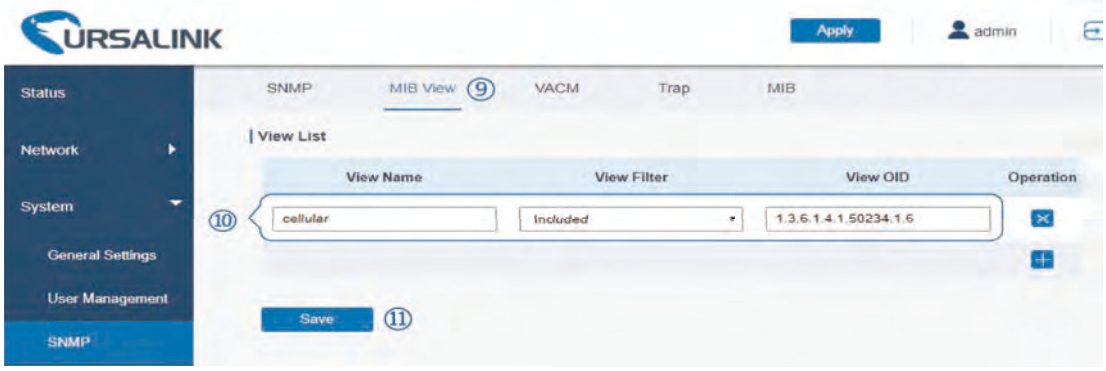

Click the "+" button beside "URSA-ROUTER-MIB", which is under the "Loaded MibModules" menu, and find "usCellularinfo". And then you will see the OID of cellular info is ".1.3.6.1.4.1.50234", which will be filled in the MIB View settings.



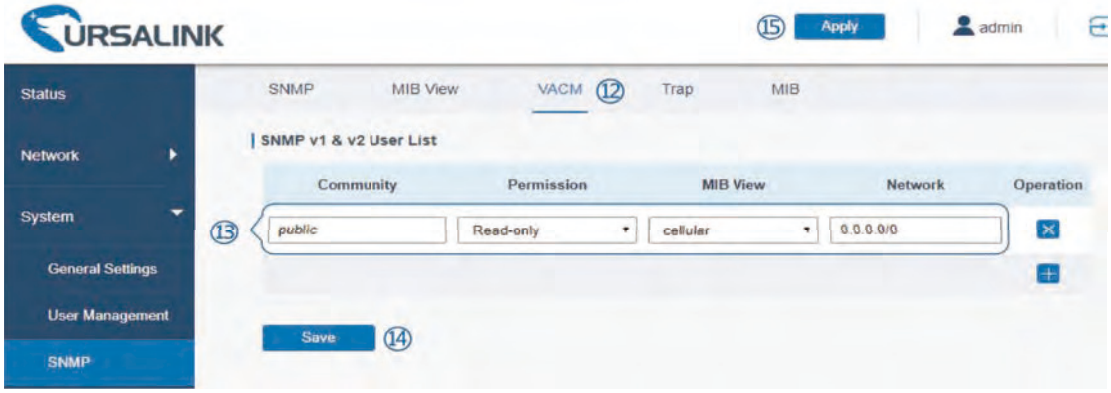

3. Go to "System > SNMP > SNMP" on the router's WEB GUI. Check "Enable" option, then click "Save" button.



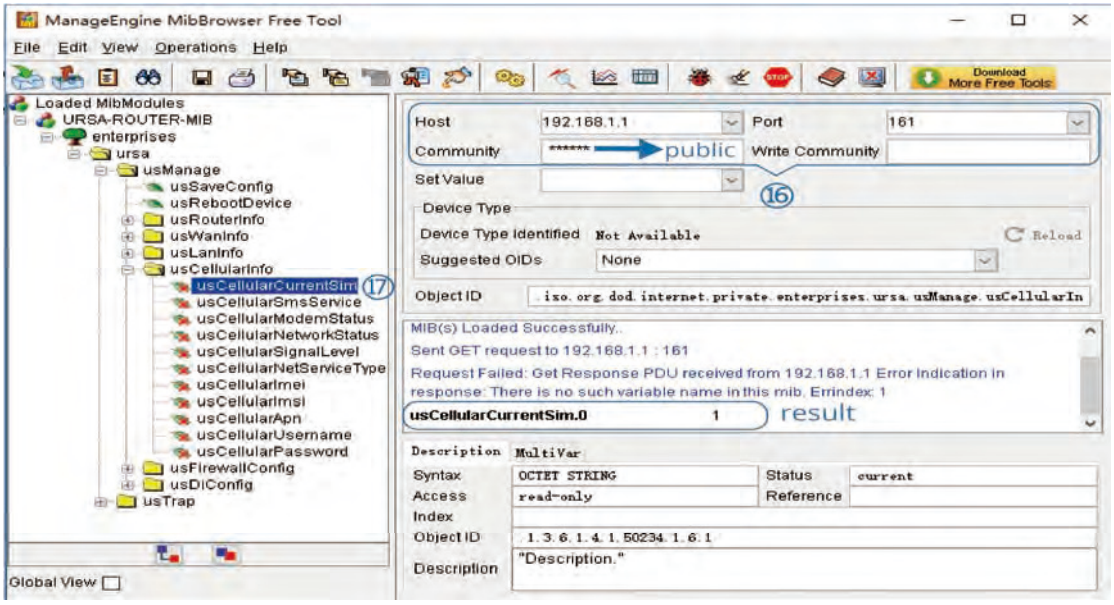

4. Go to “System > SNMP > MIB View”. Click to add a new MIB view and define the view to be accessed from the outside network. Then click “Save” button.




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 “GET”. 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

## 5.11 Cellular Connection

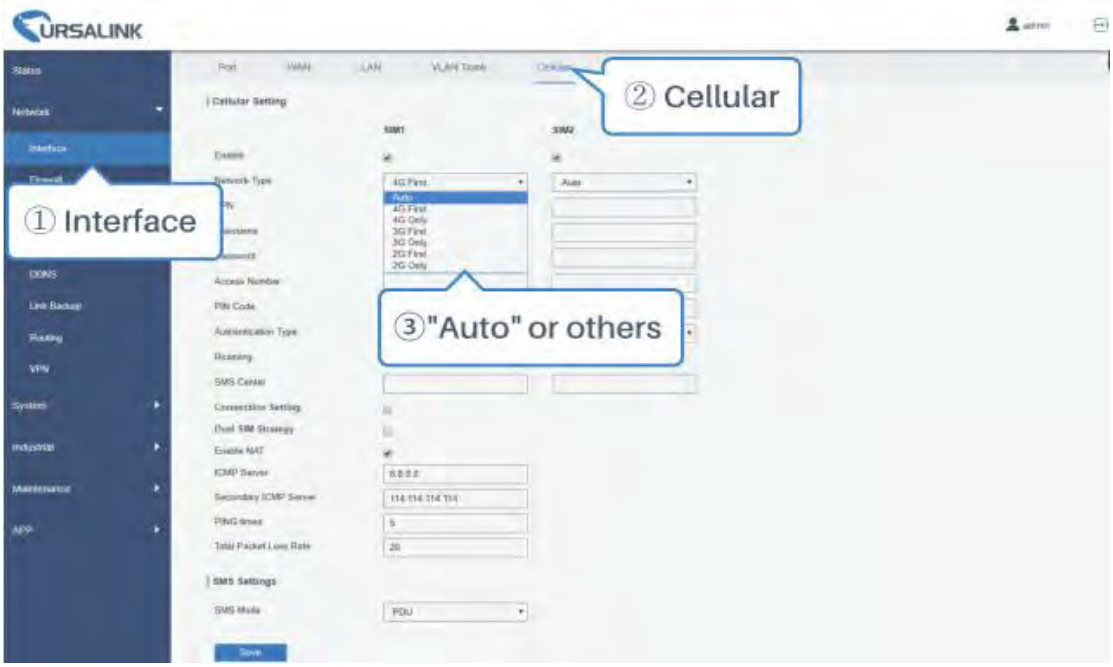
The UR71 routers have two cellular interfaces, named SIM1 & SIM2. Only one cellular interface is active at one time. If both cellular interfaces are enabled, SIM1 interface takes precedence as default.

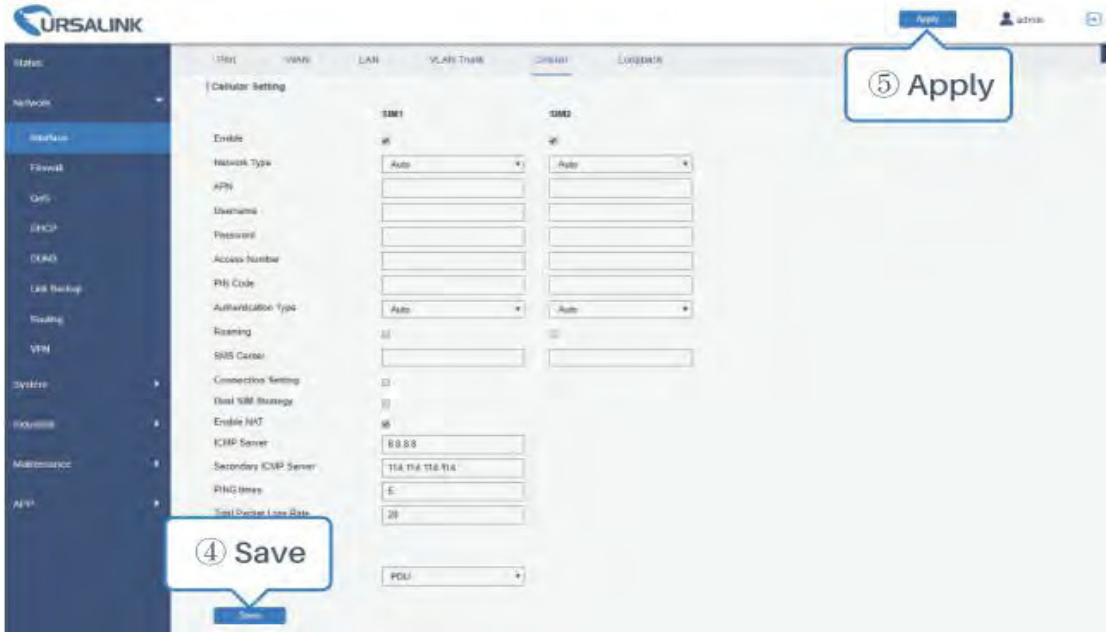
**Example**

We are about to take an example of inserting a SIM card into SIM1 slot of the UR71 and configuring the router to get Internet access through cellular.

**Configuration Steps**

1. Go to “Network > Interface > Cellular > Cellular Setting” and configure the cellular info.
2. Enable SIM1.
3. Choose relevant network type. "Auto", "4G First", “4G Only”, "3G First", “3G Only” are optional.




Click “Save” and “Apply” for configuration to take effect.

**Note:**

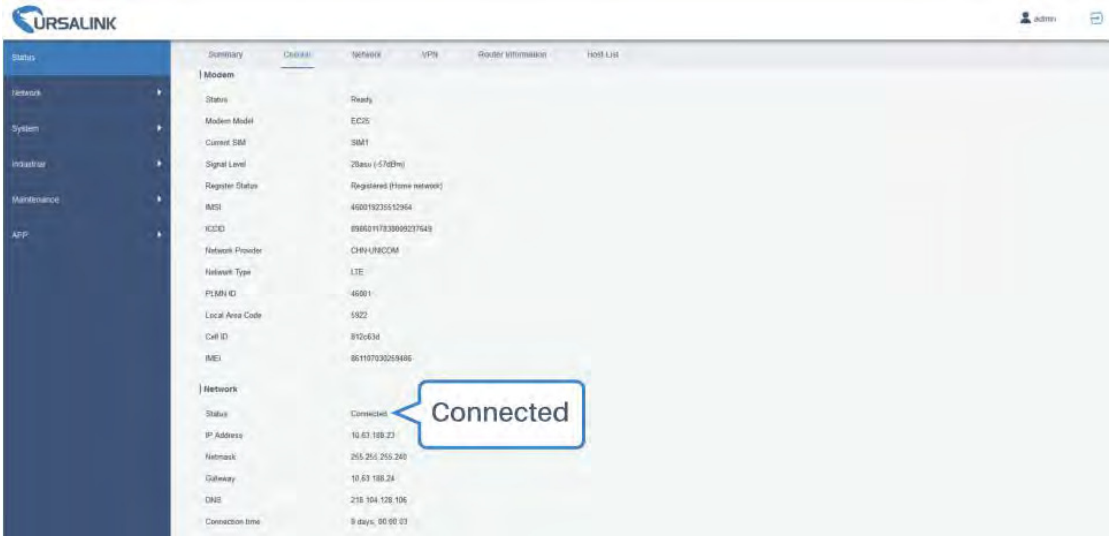
**If you select “Auto”, the router will obtain ISP information from SIM card to set APN, Username, and Password automatically. This option will only be taken effect when the SIM card is issued from well-known ISP.**

If you select “4G First” or “4G Only”**, you can click “Save” to finish the configuration directly.**

If you select “3G First”, “3G Only”, **you should manually configure APN, Username, Password, and Access Number.**

4. Check the cellular connection status by WEB GUI of router.

Click “Status > Cellular” to view the status of the cellular connection. If it shows 'Connected', SIM1 has dialed up successfully.




5. Check out if network works properly by browser on PC.

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 UR71 router.

**Related Topic**

Cellular Setting

Cellular Status

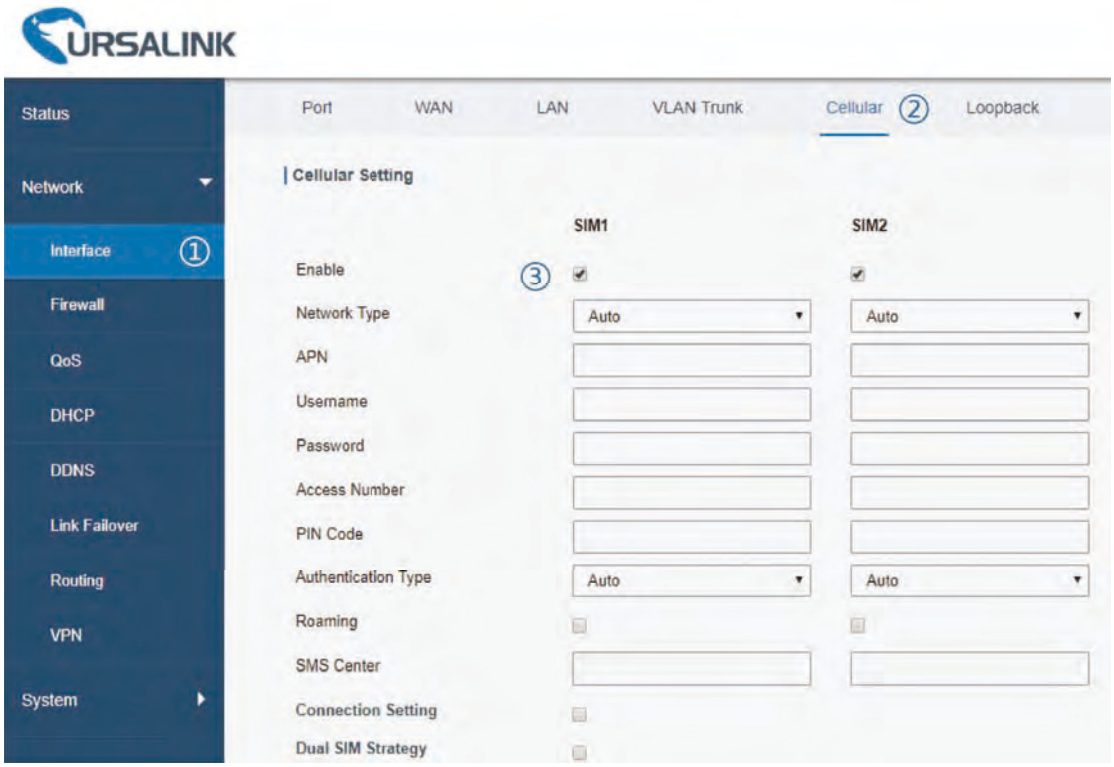
## 5.12 Dual SIM Backup Application Example

**Example**

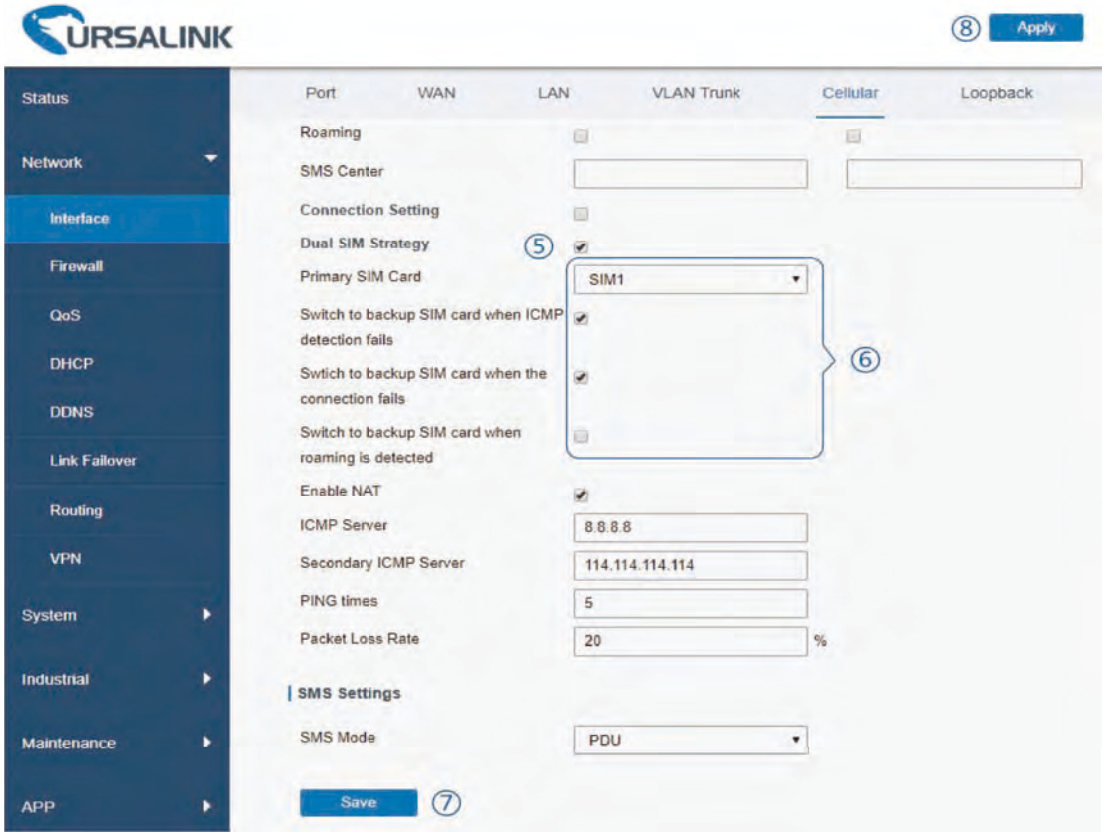
In this section we will take an example of inserting two SIM cards into the UR71. When one SIM fails, router will try to connect with the other SIM as backup link.

**Configuration Steps**

1. Go to “Network > Interface > Cellular” to enable SIM1 and SIM2. Leave the network type as “Auto” by default.

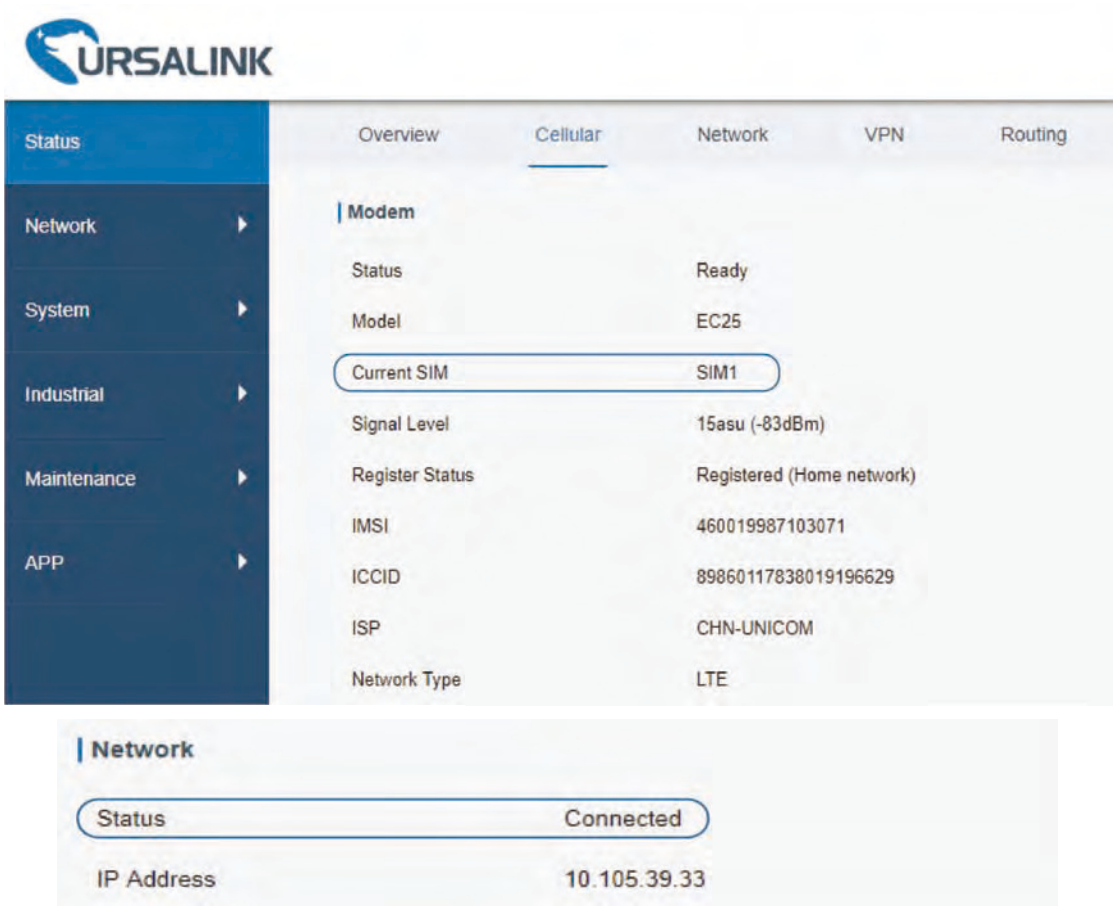



2. Enable "Dual SIM Strategy", and configure the corresponding options as below. ICMP server can be configured as any reachable IP address.

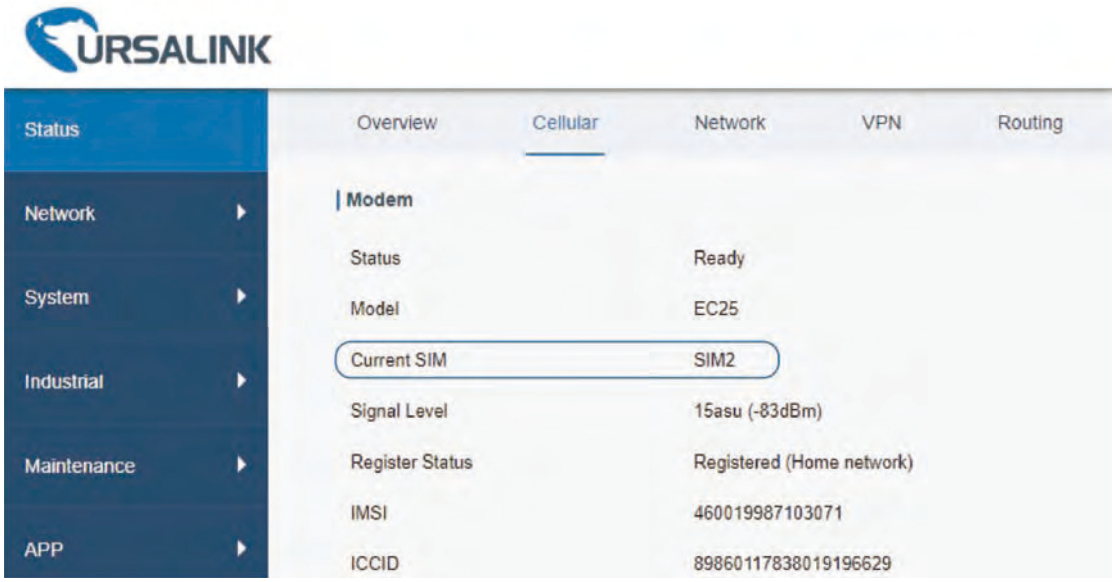



Then click "Save" and "Apply" button.

3. Go to “Status > Cellular”, and you will see the router is connected to the network via SIM1.




4. You can remove SIM1 to make the router fail to connect to network via it. Go to “Status > Cellular” again, and you will see the router is connected to the network through SIM2.



Now SIM2 becomes the main SIM, and SIM1 runs as the backup.

The router won't reconnect via SIM1 until SIM2 fails.

**Related Topic**

Cellular Setting

Cellular Status

## 5.13 VRRP Application Example

**Application Example**

A Web server requires Internet access through the UR71 router. To avoid data loss caused by router breakdown, two UR71 routers can be deployed as VRRP backup group, so as to improve network reliability.

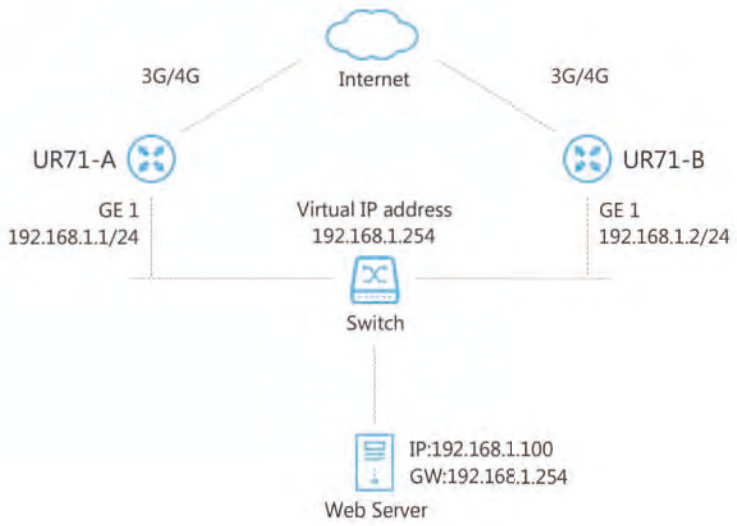
VRRP group:

UR71 Router A and Router B are connected to the Internet via cellular network. .

Virtual IP is 192.168.1.254/24.

| UR71 Router | Virtual Router ID (Same for A and B) | Port connected with switch | LAN IP Address | Priority | Preemption Mode |
|---|---|---|---|---|---|
| A | 1 | GE | 192.168.1.1 | 110 | Enable |
| B | 1 | GE | 192.168.1.2 | 100 | Disable |

Refer to the topological below.

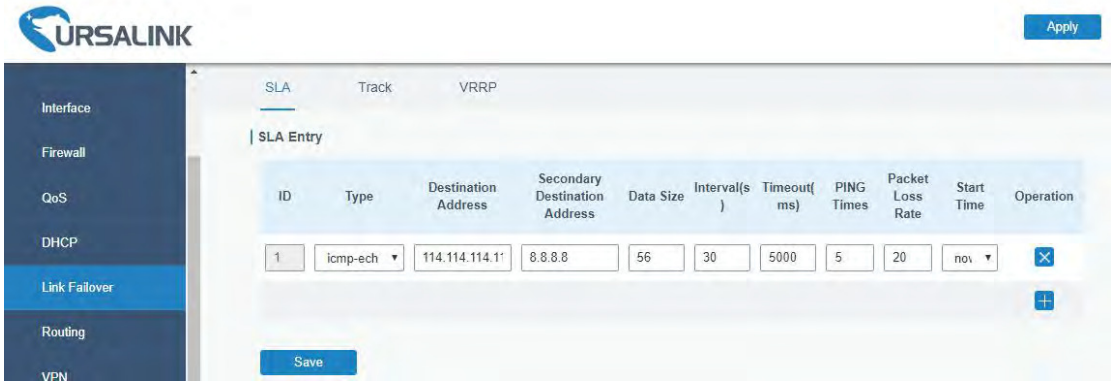


**Configuration Steps**

**Router A Configuration**

1. Go to “Network > Interface > Cellular” and configure cellular connection as per cellular connection application example.

2. Go to “Network > Link Failover > SLA” and configure SLA probe. The default probe type is ICMP. The destination address is the host address which can be probed by ICMP in public network or private network. Other parameters can be kept as default value.



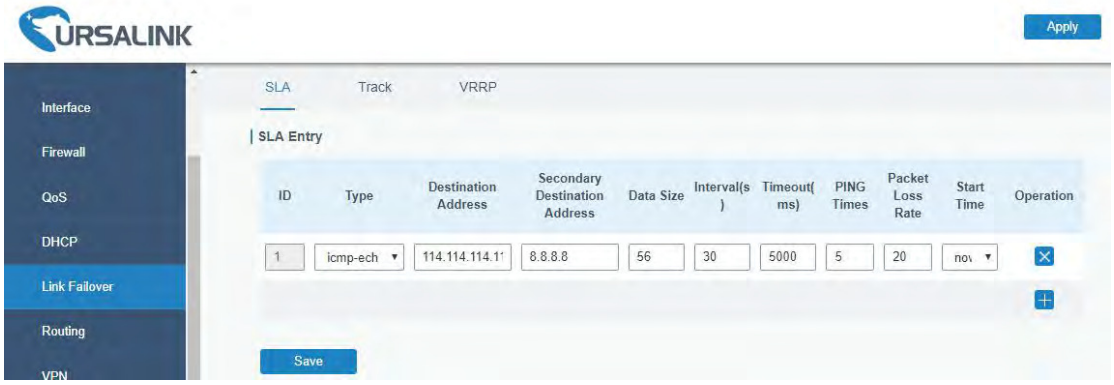

3. Go to “Network > Link Failover > Track” and configure link track parameters. You can use the default Track settings.

4. Go to “Network > Link Failover > VRRP” and configure VRRP parameters as below.

**Router B Configuration**

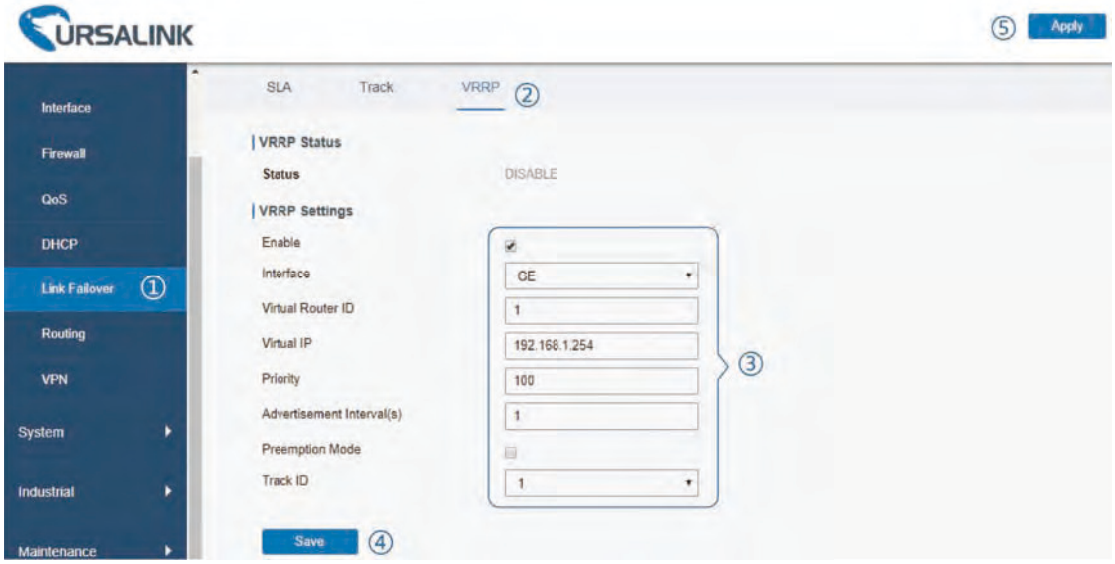
1. Go to "Network > Interface > cellular" and configure cellular connection as per cellular connection application example.

2. Go to "Network > Link Failover > SLA" and configure SLA probe. The default probe type is ICMP. The destination address is the host address which can be probed by ICMP in public network or private network. Other parameters can be kept as default value.




3. Go to "Network > Link Failover > Track" and configure link track parameters. You can use the default Track settings.

4. Go to “Network > Link Failover > VRRP” and configure VRRP parameters as below.




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

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

**Related Topics**

VRRP Setting

Track Setting

SLA Setting

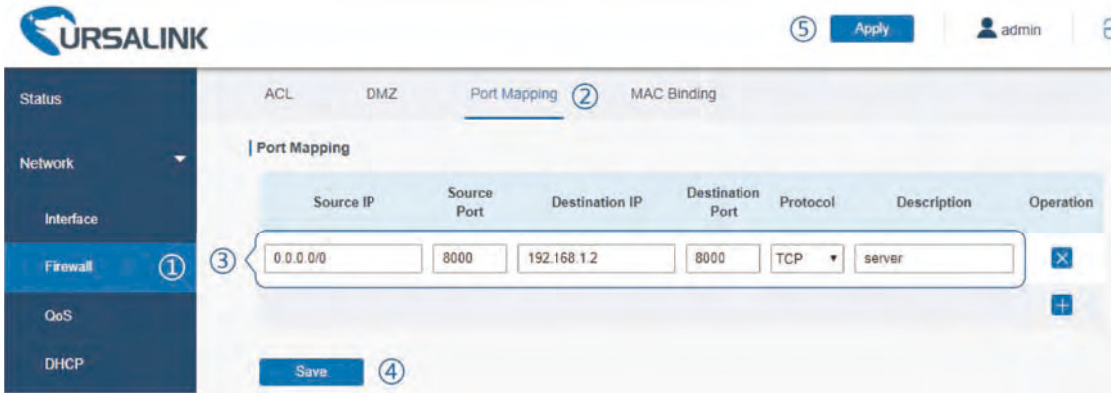
## 5.14 NAT Application Example

**Example**

An UR71 router can access Internet via cellular. GE 0 port is connected with a Web server whose IP address is 192.168.1.2 and port is 8000. Configure the router to make public network access the server.

**Configuration Steps**

Go to “Firewall > Port Mapping” and configure port mapping parameters.




Click “Save” and “Apply” button.

**Related Topic**

Port Mapping

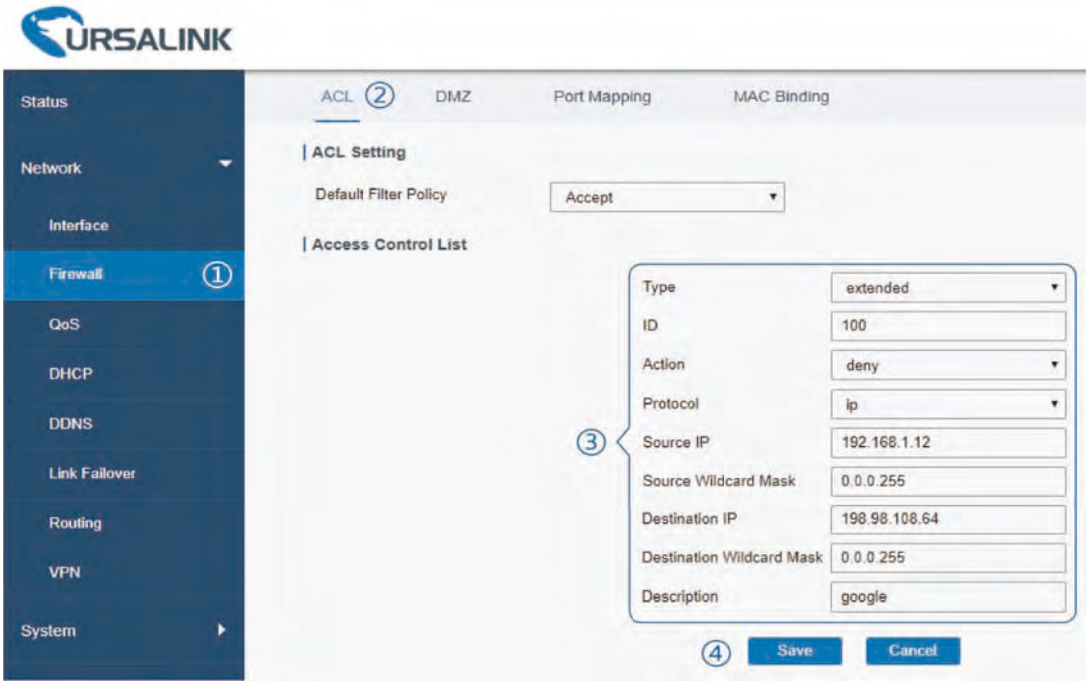
## 5.15 Access Control Application Example

**Application Example**

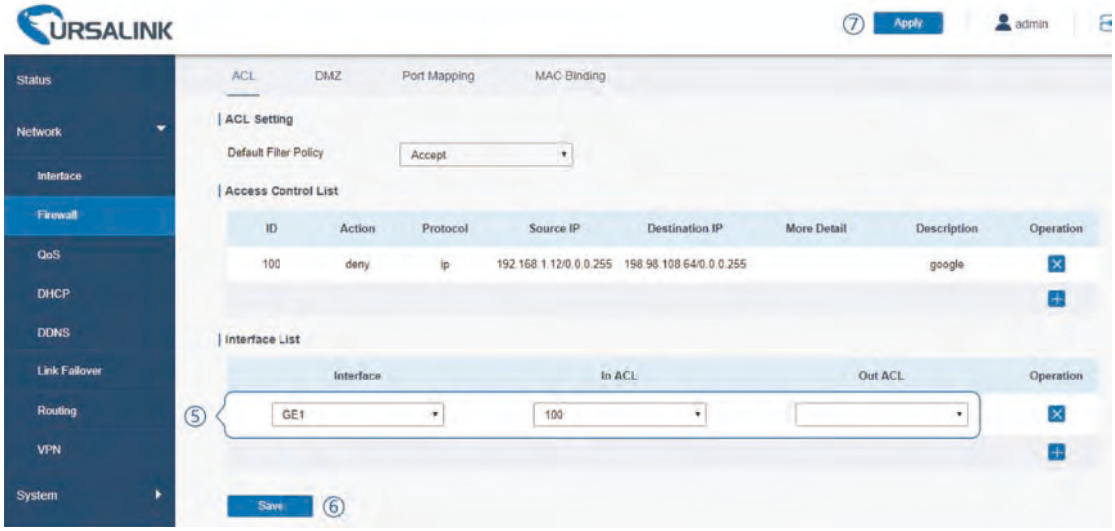
GE port of the UR71 is set as LAN with IP 192.168.1.0/24. Then configure the router to deny accessing to Google IP 198.98.108.64 from local device with IP 192.168.1.12.

**Configuration Steps**

1. Go to “Network > Firewall > ACL” to configure access control list. Click “+” button to set parameters as below. Then click “Save” button.



2. Configure interface list. Then click “Save” and “Apply” button.




**Related Topic**

ACL

## 5.16 QoS Application Example

**Example**

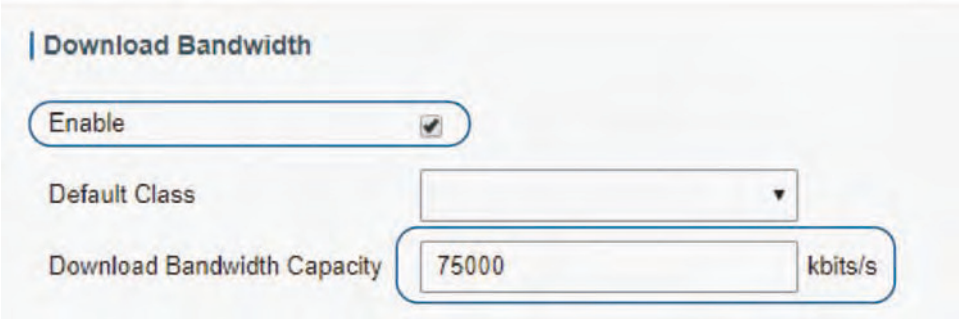
Configure the UR71 router to distribute local preference to different FTP download channels. The total download bandwidth is 75000 kbps.

**Note: the “Total Download Bandwidth” should be less than the real maximum bandwidth of 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 Classes” option, and click “+” to set up service classes.

**Note: the percents must add up to 100%.**

3. Please find "Classification Rules" option, and click "+" to set up rules.

**Note:**

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

Click "Save" and "Apply" button.

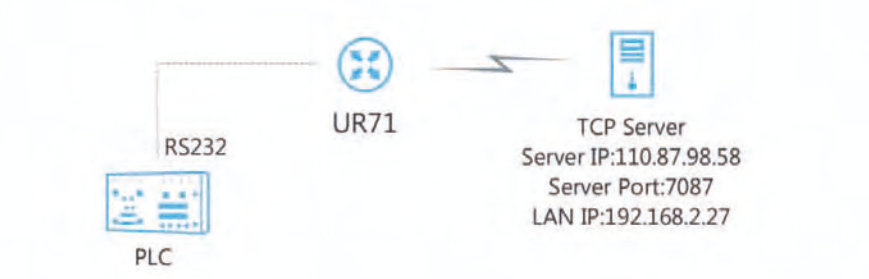
**Related Topic**

QoS Setting

## 5.17 DTU Application Example

**Example**

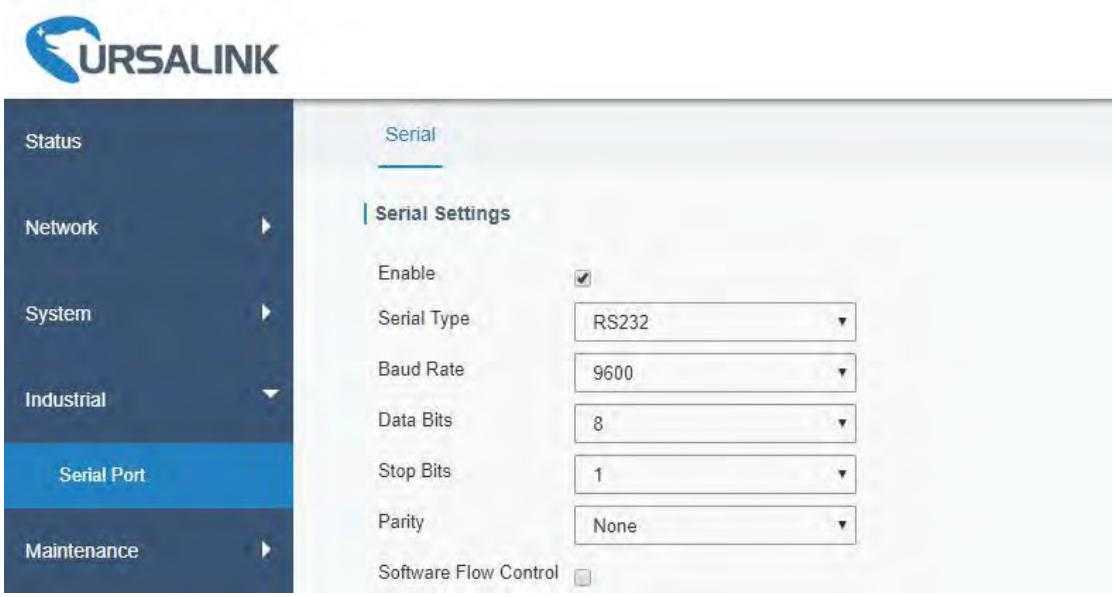
PLC is connected with the UR71 via RS232. Then enable DTU function of the UR71 to make a remote TCP server communicate with PLC. Refer to the following topological graph.



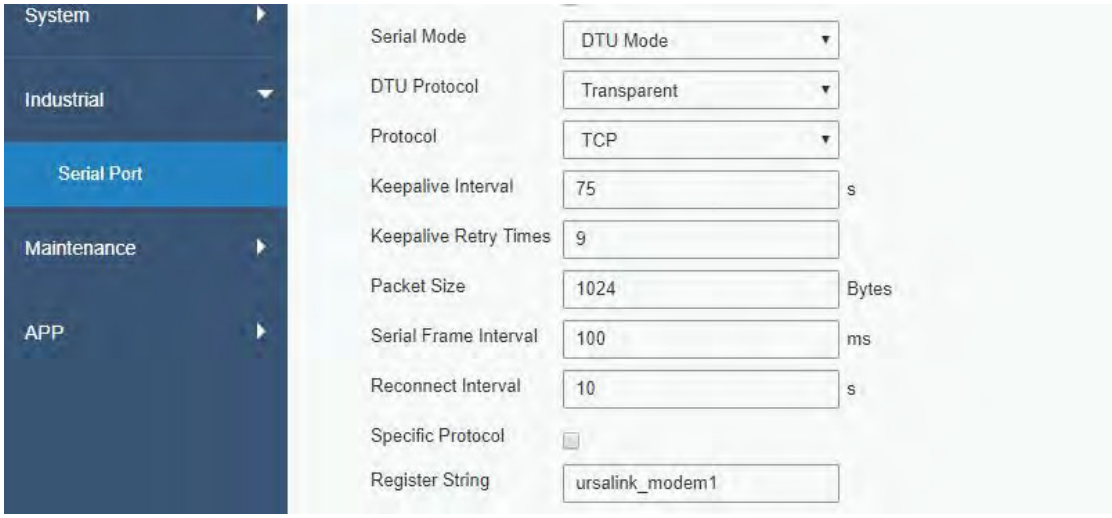

| Serial Parameters of the PLC | |
|---|---|
| Baud Rate | 9600 |
| Data Bit | 8 |
| Stop Bit | 1 |
| Parity | None |

**Configuration Steps**

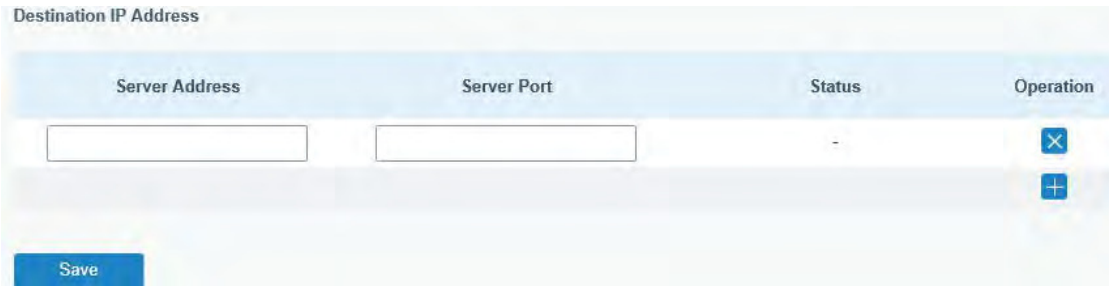
1. Go to "Industrial > Serial Port" and configure serial port parameters. The serial port parameter shall be kept in consistency with those of PLC, as shown in figure below.



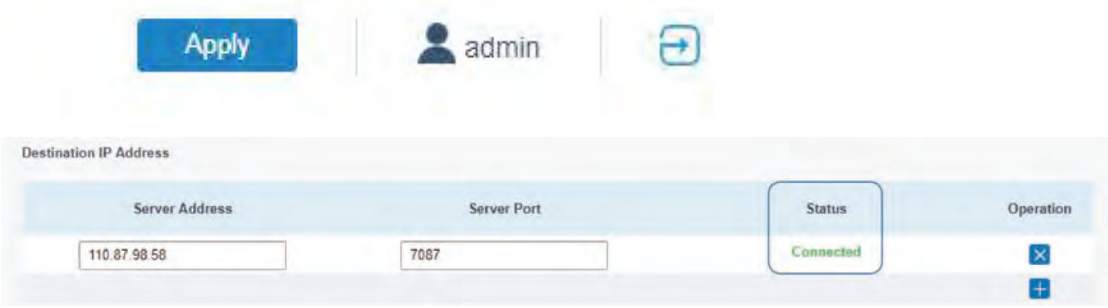

2. Configure Serial Mode as “DTU Mode”. The UR71 is connected as client in “Transparent” protocol.




3. Configure TCP server IP and port.

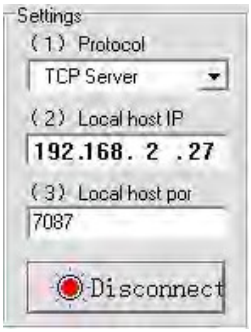


4. Once you complete all configurations, click “Save” and “Apply” button.




5. Start TCP server on PC.

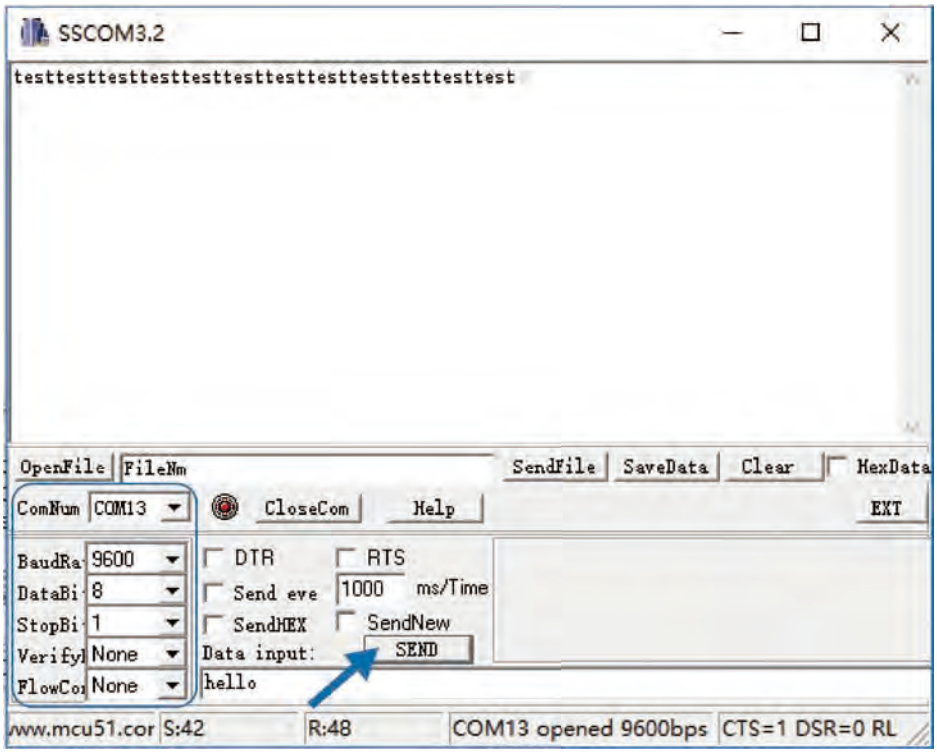
   Take “Netassist” test software as example. Make sure port mapping is already done.



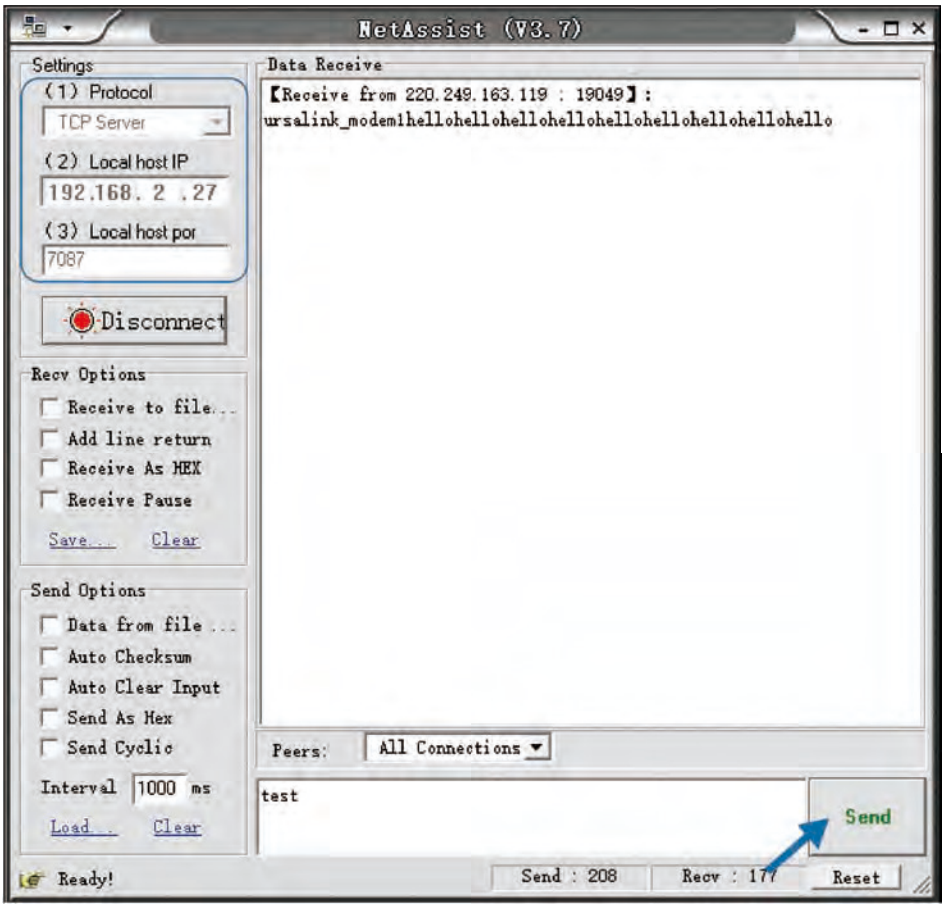

6. Connect the UR71 to PC via RS232 for PLC simulation. Then start “sscom” software on the PC to test communication through serial port.

7. After connection is established between the UR71 and the TCP server, you can send data between sscom and netassit.

**<u>PC side</u>**




## TCP server side



8. After serial communication test is done, you can connect PLC to RS232 port of the UR71 for test.

**Related Topic**

Serial Port

## 5.18 PPTP Application Example

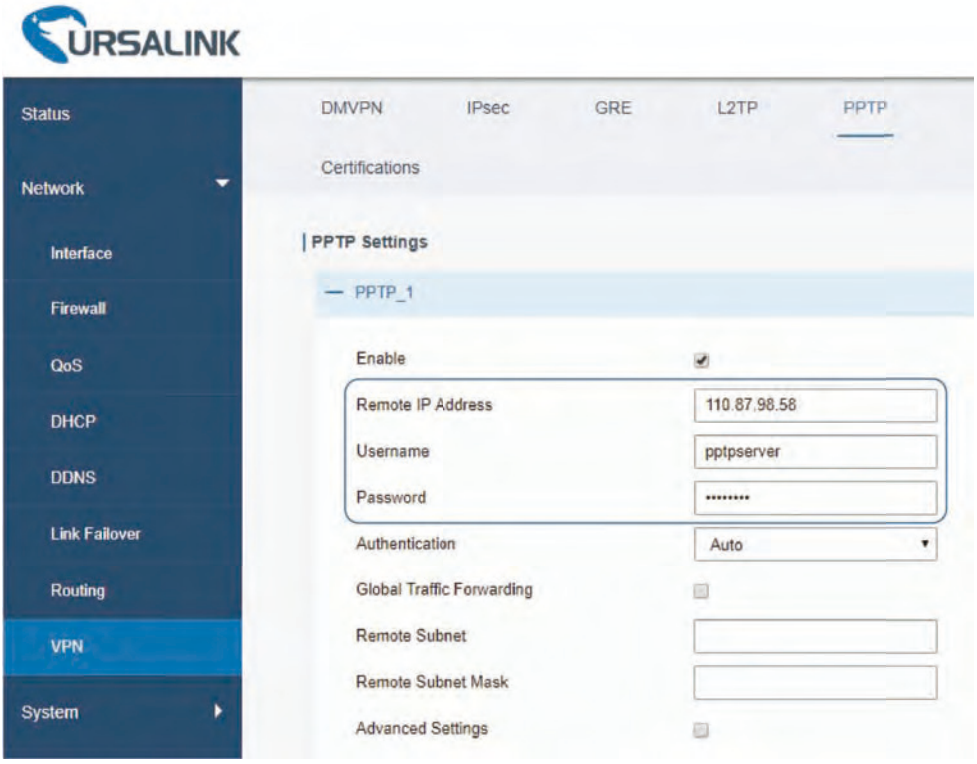
**Example**

Configure the UR71 as PPTP client to connect to a PPTP server in order to have data transferred securely. Refer to the following topological graph.

**Configuration Steps**

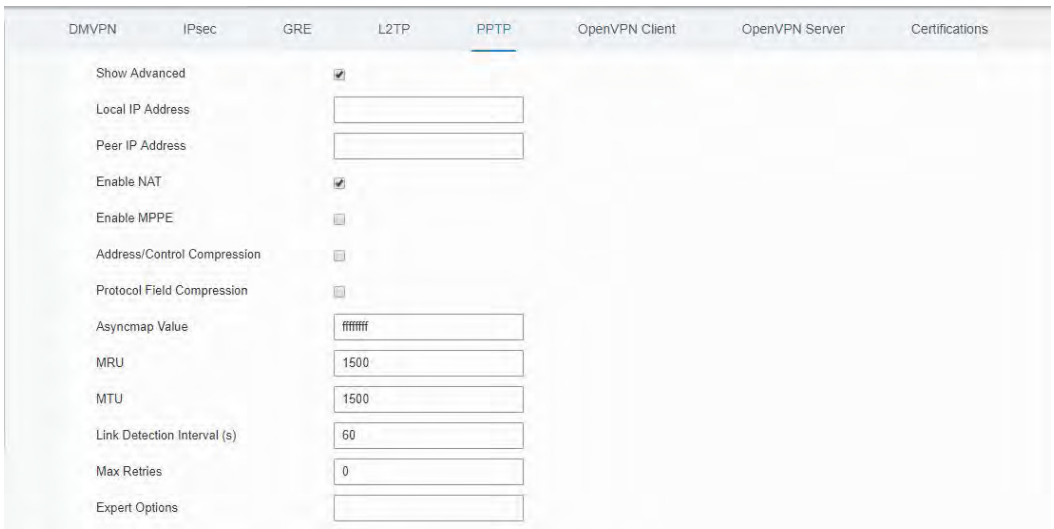
1. Go to "Network > VPN > PPTP", configure PPTP server IP address, username and password provided by PPTP server.

Note: If you want to have all data transferred through VPN tunnel, check "Global Traffic Forwarding" option.



If you want to access peer subnet such as 192.168.3.0/24, you need to configure the subnet and mask to add the route.

2. Check “Show Advanced” option, and you will see the advanced settings.




If the PPTP server requires MPPE encryption, then you need to check “Enable MPPE” option.

If the PPTP server assigns fixed tunnel IP to the client, then you can fill in the local tunnel IP and remote tunnel IP, shown as below.

Otherwise PPTP server will assign tunnel IP randomly.

Click “Save” button when you complete all settings, and then the advanced settings will be hidden again. Then click “Apply” button to have the configurations take effect.

3. Go to “Status > VPN” and check PPTP connection status.

PPTP is established as shown below.

Local IP: the client tunnel IP.

Remote IP: the server tunnel IP.

**Related Topics**

PPTP Setting

PPTP Status

**[END]**