

**LINOVISION**

**Mini Industrial Router  
IOT-R41**

**User Manual**

## Safety Precautions Preface

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

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

© 2007-2023 Linovision Co., Ltd.

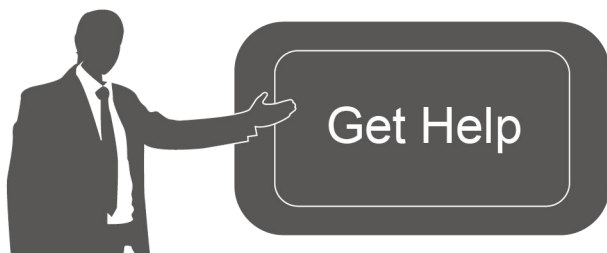
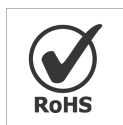
**All rights reserved.**

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 Linovision lot Co., Ltd.

## Declaration of Conformity

IOT-R41 is in conformity with the essential requirements and other relevant provisions of the CE, FCC,

and RoHS.



For assistance, please contact Linovision technical support

Email: [support@linovision.com](mailto:support@linovision.com)

Tel: 469-444-2999 ext 2

Web: <https://support.linovision.com/>

**Revision History**

<b>Date</b>	<b>Doc Version</b>	<b>Description</b>
February 8, 2023	V 1.0	Initial version

# Contents

Chapter 1 Product Introduction .....	8
1.1 Overview .....	8
1.2 Advantages .....	8
Chapter 2 Hardware Introduction .....	9
2.1 Packing List .....	9
2.2 Hardware Overview .....	10
2.3 Serial & IO & Power .....	10
2.4 LED Indicators .....	11
2.5 Reset Button .....	11
2.6 Dimensions (mm) .....	12
Chapter 3 Hardware Installation .....	12
3.1 SIM Card Installation .....	12
3.2 Antenna Installation .....	12
3.3 Router Installation .....	12
Chapter 4 Access to Web GUI .....	13
Chapter 5 Web Configuration .....	15
5.1 Status .....	15
5.1.1 Overview .....	15
5.1.2 Cellular .....	16
5.1.3 Network .....	18
5.1.4 VPN .....	18
5.1.5 Routing .....	19
5.1.6 Host List .....	19
5.1.7 GPS .....	20
5.2 Network .....	21
5.2.1 Interface .....	21
5.2.1.1 Cellular .....	21
5.2.1.2 Port .....	24
5.2.1.3 USB .....	24
5.2.1.4 Bridge .....	24
5.2.1.5 Loopback .....	25
5.2.2 DHCP .....	26
5.2.2.1 DHCP Server/DHCPv6 Server .....	26
5.2.2.2 DHCP Relay .....	28
5.2.3 Firewall .....	28
5.2.3.1 Security .....	29
5.2.3.2 ACL .....	30
5.2.3.3 Port Mapping .....	31
5.2.3.4 DMZ .....	32
5.2.3.5 MAC Binding .....	32
5.2.3.6 Custom Rules .....	33
5.2.3.7 SPI .....	33

5.2.4 QoS.....	34
3.2.5 VPN.....	35
3.2.5.1 DMVPN.....	35
5.2.5.2 IPsec Server.....	37
5.2.5.3 IPsec.....	39
5.2.5.4 GRE.....	41
5.2.5.5 L2TP.....	42
5.2.5.6 PPTP.....	44
5.2.5.7 OpenVPN Client.....	46
5.2.5.8 OpenVPN Server.....	47
5.2.5.9 Certifications.....	49
5.2.6 IP Passthrough.....	51
5.2.7 Routing.....	52
5.2.7.1 Static Routing.....	52
5.2.7.2 RIP.....	52
5.2.7.3 OSPF.....	55
5.2.7.4 Routing Filtering.....	60
5.2.8 VRRP.....	61
5.2.9 DDNS.....	63
5.3 System.....	64
5.3.1 General Settings.....	64
5.3.1.1 General.....	64
5.3.1.2 System Time.....	65
5.3.1.3 Email.....	66
5.3.2 Phone&SMS.....	68
5.3.2.1 Phone.....	68
5.3.2.2 SMS.....	69
5.3.3 Power Management.....	71
5.3.4 User Management.....	73
5.3.4.1 Account.....	73
5.3.4.2 User Management.....	74
5.3.5 SNMP.....	74
5.3.5.1 SNMP.....	75
5.3.5.2 MIB View.....	75
5.3.5.3 VACM.....	76
5.3.5.4 Trap.....	77
5.3.5.5 MIB.....	77
5.3.6 AAA.....	78
5.3.6.1 Radius.....	78
5.3.6.2 TACACS+.....	79
5.3.6.3 LDAP.....	79
5.3.6.4 Authentication.....	80
5.3.7 Device Management.....	80
5.3.7.1 DeviceHub.....	80

5.3.7.2 LINOVISION VPN .....	81
5.3.8 Events .....	82
5.3.8.1 Events .....	82
5.3.8.2 Events Settings .....	83
5.4 Industrial Interface .....	85
5.4.1 I/O .....	85
5.4.1.1 DI .....	85
5.4.1.2 DO .....	86
5.4.2 Serial Port .....	87
5.4.3 Modbus Slave .....	90
5.4.3.1 Modbus TCP .....	90
5.4.3.2 Modbus RTU .....	91
5.4.3.3 Modbus RTU Over TCP .....	92
5.4.4 Modbus Master .....	92
5.4.4.1 Modbus Master .....	92
5.4.4.2 Channel .....	93
5.4.5 GPS .....	95
5.4.5.1 GPS .....	95
5.4.5.2 GPS IP Forwarding .....	96
5.4.5.3 GPS Serial Forwarding .....	97
5.5 Maintenance .....	98
5.5.1 Tools .....	98
5.5.1.1 Ping .....	98
5.5.1.2 Traceroute .....	98
5.5.1.3 Packet Analyzer .....	99
5.5.1.4 Qxdmlog .....	99
5.5.2 Debugger .....	99
5.5.2.1 Cellular Debugger .....	99
5.5.2.2 Firewall Debugger .....	100
5.5.3 Log .....	101
5.5.3.1 System Log .....	101
5.5.3.2 Log Download .....	102
5.5.3.3 Log Settings .....	103
5.5.4 Upgrade .....	103
5.5.5 Backup and Restore .....	104
5.5.6 Reboot .....	105
Chapter 6 Application Examples .....	105
6.1 Restore Factory Defaults .....	105
6.1.1 Via Web Interface .....	105
6.1.2 Via Hardware .....	107
6.2 Firmware Upgrade .....	107
6.3 Events Application Example .....	107
6.4 SNMP Application Example .....	109
6.5 Cellular Connection .....	112

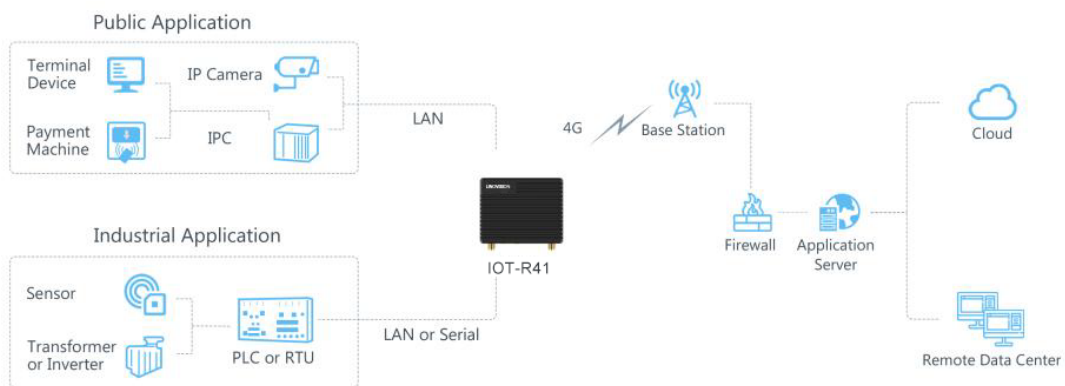
6.6 NAT Application Example .....	114
6.7 Access Control Application Example .....	115
6.8 QoS Application Example .....	116
6.9 DTU Application Example .....	117
6.10 PPTP Application Example .....	120

# Chapter 1 Product Introduction

## 1.1 Overview

LINOVISION mini industrial router IOT-R41 supports 4G connection, and also satisfies multi-type local data access requirements through rich industrial interfaces, including DI, DO, RS232 or RS485. IOT-R41 make it easy for forming a reliable, secure, and maintainable solution through its built-in watchdog and secure VPN tunnels, realizing stable data transmission and high-speed mobile connectivity.

With a compact size and industry-grade design, IOT-R41 is more flexible in a variety of installation and deployment scenarios. IOT-R41 adopts a power-saving design with both idle mode and standby mode for providing users with an energy-saving option. IOT-R41 could be managed and monitored remotely by LINOVISION DeviceHub, IOT-R41 could be applied in wide scenarios including vending machines, robots, industrial equipment, and other IoT applications with optimal cost and performance.



## 1.2 Advantages

### Highlight Features

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

### Industrial-Grade Design

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



## Easy Maintenance

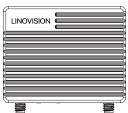
- DeviceHub provides easy setup, mass configuration, and centralized management of remote devices
- The user-friendly web interface design and more than one option of upgrade help administrators to manage the device as easy as pie
- WEB GUI and CLI enable the admin to achieve simple management and quick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

## Security & Reliability

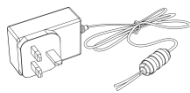
- Secure transmission with VPN tunnels like IPsec/OpenVPN/GRE/L2TP/PPTP/DMVPN
- Embeds hardware watchdog to automatically recover from various failures, ensuring highest level of availability
- Support access control lists, DMZ, DDoS Protection, Filters, SPI firewalls
- Establishes a secured mechanism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

## Chapter 2 Hardware Introduction

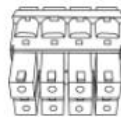
### 2.1 Packing List



1 × IOT-R41 Device



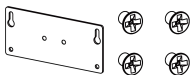
1 × Power Adapter



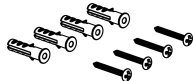
1 × 8-Pin Pluggable  
Terminal



1 × SIM Card Ejector Tool



1 × Wall Mounting  
Bracket with  
Screws



4 × Wall Mounting  
Kits



1 × Warranty Card



1 × Quick Start Guide



1 × Magnetic Cellular Antenna



1 × GPS Antenna



1 × 108mm Stubby Cellular Antenna (Optional)



1 × Mini Stubby Cellular Antenna (Optional)

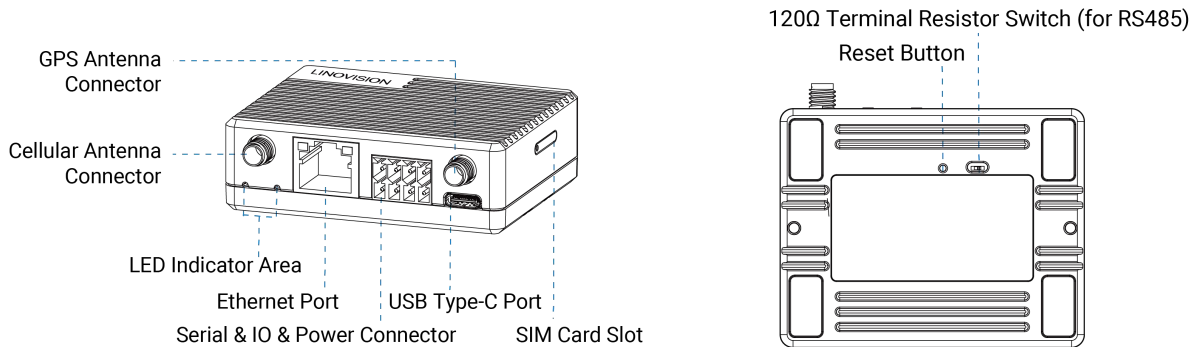


1 × USB 2.0 Cable (Optional)



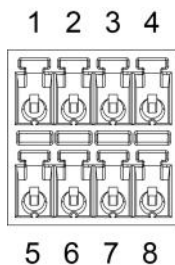
If any of the above items is missing or damaged, please contact your sales representative.

## 2.2 Hardware Overview



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

## 2.3 Serial & IO & Power



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

## 2.4 LED Indicators

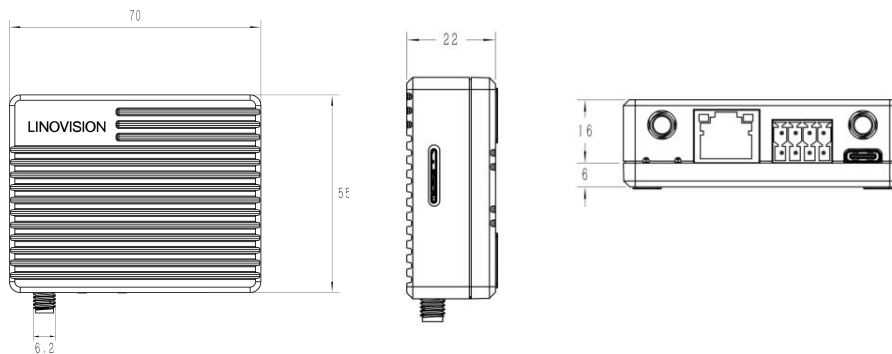
LED	Indication	Status	Description
SYSTEM	Power & System Status	Off	The power is switched off
		Orange	Static: the power is switched on, the system is on standby mode
			Blinking three times: the power is switched on, the system is starting up
		Green	Static: The system is running properly
		Red	Static: The system goes wrong
LTE	Cellular & Signal Status	Off	SIM card is registering or fails to register (or there are no SIM cards inserted)
		Green	Blinking rapidly: SIM card has been registered and is dialing up now
			Static: SIM card has been registered and dialed up to 4G network
		Orange	Static: SIM card has been registered and dialed up to 3G/2G network
Ethernet Port	Link Indicator (Orange)	Off	Disconnected or fail to connect
		On	Connected
		Blinking	Transmitting data
	Rate Indicator (Green)	Off	10 Mbps mode
		On	100 Mbps mode

**Note:** It will take around 1 minute for IOT-R41 to completely start up, then the SYSTEM light will be green.

## 2.5 Reset Button

Function	Description	
	SYSTEM LED	Action
Reset	Static	Press and hold the reset button for more than 5 seconds.
	Static → Blinking	Release the button and wait.
	Off → Static Green	The router is now reset to factory defaults.
Weakup	Orange Static → Green Static	If standby mode is enabled, press and hold on reset button for 3 seconds to weak up the router for 1 hour.

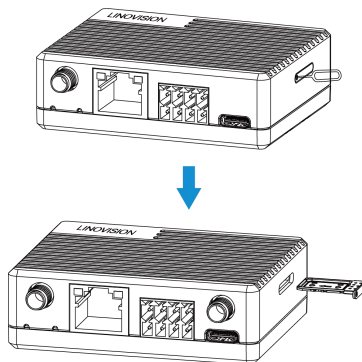
## 2.6 Dimensions (mm)



## Chapter 3 Hardware Installation

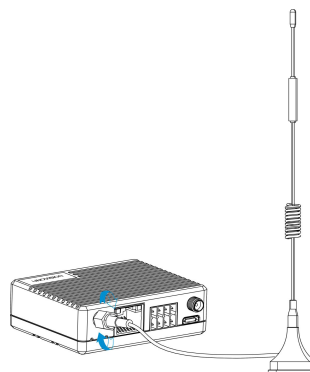
### 3.1 SIM Card Installation

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



### 3.2 Antenna Installation

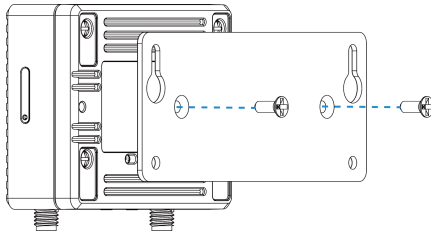
Rotate the antenna into the antenna connector accordingly. The external antenna should be installed vertically, and always on a site with a good signal.



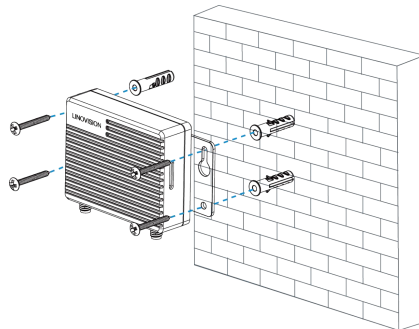
### 3.3 Router Installation

IOT-R41 router can be mounted to a wall. Before you start, make sure that a SIM card has been inserted, antennas have been attached and all cables have been installed.

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



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



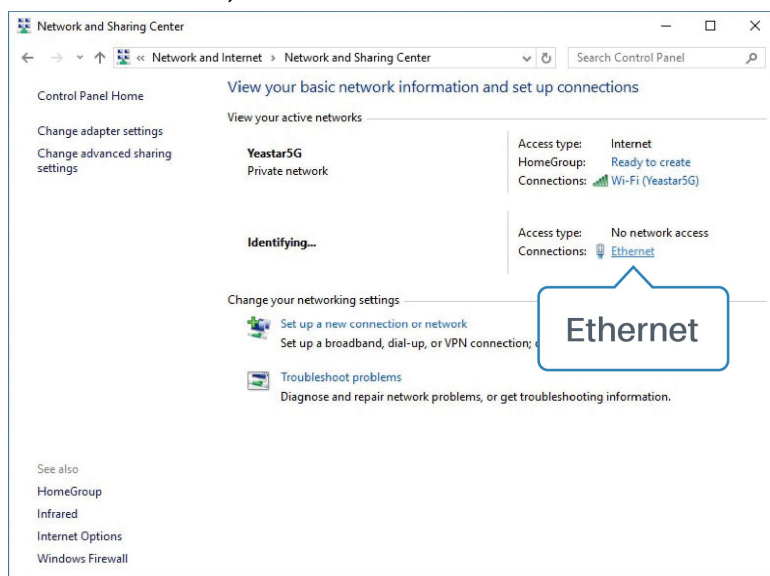
## Chapter 4 Access to Web GUI

This chapter explains how to access to Web GUI of the IOT-R41 router. Connect PC to LAN port of IOT-R41 router directly. The following steps are based on Windows 10 operating system for your reference. Username: **admin**

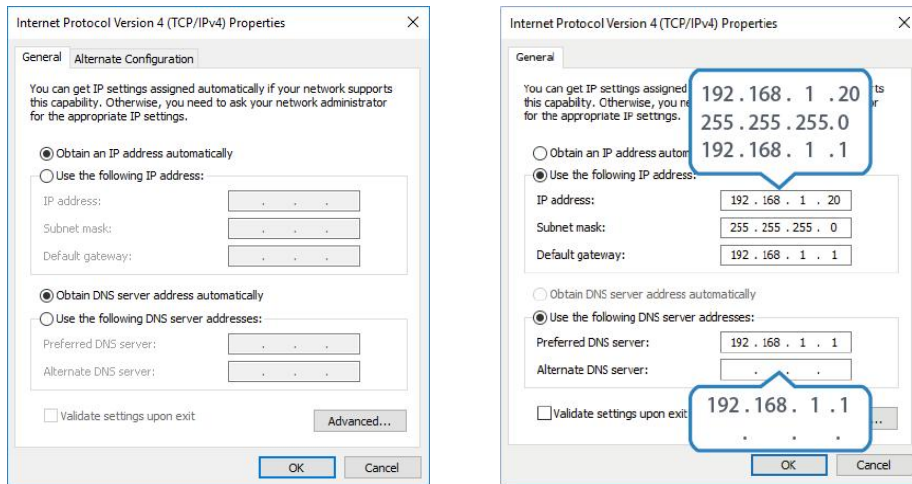
Password: **password**

IP Address: **192.168.1.1**

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

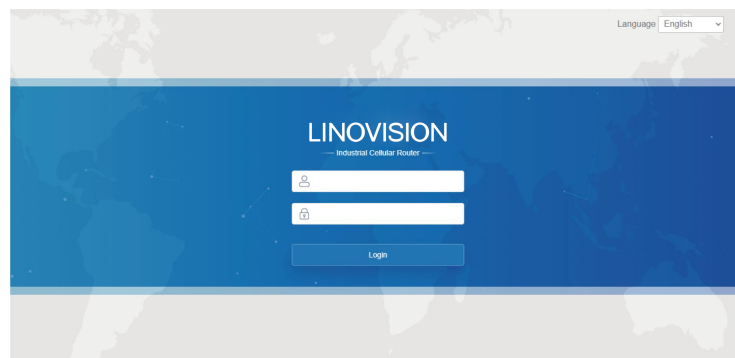


2. Go to “Properties” → “Internet Protocol Version 4(TCP/IPv4)”, select “Obtain an IP address automatically” or “Use the following IP address”, then assign a static IP manually within the same subnet of the device.



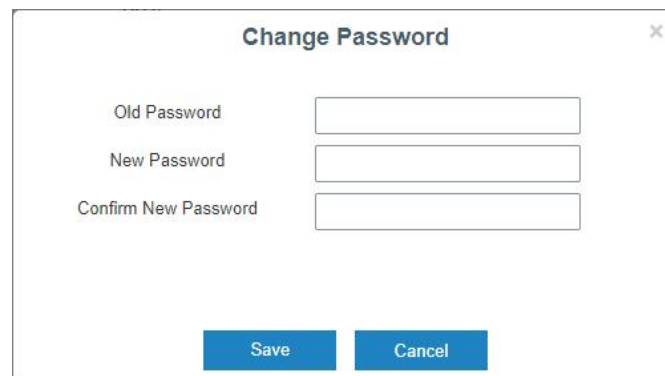
3. Open a Web browser on your PC (Chrome is recommended), type in the IP address 192.168.1.1, and press Enter on your keyboard.

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



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

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



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

The screenshot shows the LINOVISION Web GUI interface. At the top, there is a navigation bar with the LINOVISION logo on the left and a user profile 'admin' on the right. Below the navigation bar is a status bar with the message: "For your device security, please change the default password!". The main content area is divided into several sections:

- Overview**: This section is currently selected and contains:
  - System Information**:
 

Model	R41-L08EU
Serial Number	6053C4611302
Firmware Version	41.0.0.2-t1
Hardware Version	V1.0
  - System Status**:
 

Local Time	2023-01-30 15:03:08 Monday
Uptime	23:23:01
CPU Load	100%
RAM (Available/Capacity)	79MB/128MB(61.72%)
Flash (Available/Capacity)	88MB/128MB(68.75%)
  - Cellular**:
 

Status	No SIM Card
IPv4	0.0.0.0/0
IPv6	fe80::b469:8ff:fece:14cc/64
Connection Duration	0 days, 00:00:00
Data Usage Monthly	0.0 MiB
  - LAN**:
 

IPv4	192.168.43.181/24
IPv6	fe80::b8de:4aff:fe44:a901/64
Connected Devices	1
- Help**: A sidebar on the right with expandable sections:
  - Model**: Show the model name of router.
  - Serial Number**: Show the serial number of router.
  - Firmware Version**: Show the current firmware version of router.
  - Hardware Version**: Show the current hardware version of router.
  - Local Time**: Show the current 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 (Available/Capacity)**: Show the RAM available and the capacity RAM memory.
  - Flash (Available/Capacity)**: Show the Flash available and the capacity Flash memory.

At the bottom right of the main content area, there are two buttons: "Manual Refresh" (with a dropdown arrow) and "Refresh".

## Chapter 5 Web Configuration

### 5.1 Status

#### 5.1.1 Overview

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

This image shows a detailed view of the system information page from the Web GUI. The navigation tabs at the top are: Overview, Cellular, Network, VPN, Routing, Host List, and GPS. The Overview tab is selected.

The page is divided into two main columns of information:

- System Information**:
 

Model	UR41-L08EU
Serial Number	6053C4611302
Firmware Version	41.0.0.2-t1
Hardware Version	V1.0
- System Status**:
 

Local Time	2023-01-30 15:03:08 Monday
Uptime	23:23:01
CPU Load	100%
RAM (Available/Capacity)	79MB/128MB(61.72%)
Flash (Available/Capacity)	88MB/128MB(68.75%)
- Cellular**:
 

Status	No SIM Card
IPv4	0.0.0.0/0
IPv6	fe80::b469:8ff:fece:14cc/64
Connection Duration	0 days, 00:00:00
Data Usage Monthly	0.0 MiB
- LAN**:
 

IPv4	192.168.43.181/24
IPv6	fe80::b8de:4aff:fe44:a901/64
Connected Devices	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.
System Status	
Item	Description
Local Time	Show the currently local time of system.
Uptime	Show the information on how long the router has been running.
CPU Load	Show the current CPU utilization of the router.
RAM (Available/Capacity)	Show the RAM capacity and the available RAM memory.
Flash (Available/Capacity)	Show the Flash capacity and the available Flash memory.
Cellular	
Item	Description
Status	Show the real-time status of the currently SIM card
IPv4	Show the IPv4 address obtained from the mobile carrier.
IPv6	Show the IPv6 addresses obtained from the mobile carrier.
Connection Duration	Show the connection duration of the currently SIM card.
Data Usage Monthly	Show the monthly data usage statistics of currently used SIM card.
LAN	
Item	Description
IPv4	Show the IPv4 address of the LAN port.
IPv6	Show the IPv6 addresses of the LAN port.
Connected Devices	Number of devices that connected to the router's LAN.

### 5.1.2 Cellular

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



Modem		Network	
Model	EG95	Status	Disconnected
Version	EG95NAXGAR07A03M1G	IPv4 Address	0.0.0.0/0
Signal Level	0asu (-113dBm)	IPv4 Gateway	0.0.0.0
Register Status	Not registered	IPv4 DNS	0.0.0.0
IMEI	865026045588794	IPv6 Address	::
IMSI	-	IPv6 Gateway	::
ICCID	-	IPv6 DNS	::
ISP	-	Connection Duration	0 days, 00:00:00
Network Type	-	<b>Data Usage Monthly</b>	
PLMN ID	-	RX	0.0 MiB
LAC	0	TX	0.0 MiB
Cell ID	0	ALL	0.0 MiB

Modem Information	
Item	Description
Model	Show the model name of cellular module.
Version	Show the cellular module firmware version.
Signal Level	Show the cellular signal level.
Register Status	Show the registration status of SIM card.
IMEI	Show the IMEI of the module.
IMSI	Show IMSI of the SIM card.
ICCID	Show ICCID of the SIM card.
ISP	Show the network provider which the SIM card registers on.
Network Type	Show the connected network type, such as LTE, 3G, etc.
PLMN ID	Show the current PLMN ID, including MCC, MNC, LAC and Cell ID.
LAC	Show the location area code of the SIM card.
Cell ID	Show the Cell ID of the SIM card location.
Network	
Item	Description
Status	Show the connection status of cellular network.
IPv4/IPv6 Address	Show the IPv4/IPv6 address and netmask of cellular network.
IPv4/IPv6 Gateway	Show the IPv4/IPv6 gateway and netmask of cellular network.
IPv4/IPv6 DNS	Show the IPv4/IPv6 DNS of cellular network.
Connection Duration	Show information on how long the cellular network has been connected.
Data Usage Monthly	
Item	Description
RX	Show the data volume and packets received of this month.
TX	Show the data volume and packets transmitted of this month.
ALL	Show the total volume and packets of this month.

### 5.1.3 Network

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

Bridge				
Name	STP	IPv4	IPv6	Members
Bridge0	Disabled	192.168.43.181/24	-	eth0,usb0

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

### 5.1.4 VPN

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

Overview	Cellular	Network	VPN	Routing	Host List	GPS
Clients						
Name		Status	Local IP	Remote IP		
Server						
Name			Status			
OpenVPN Server			Disabled			
Ipsec Server			Disabled			
Connected List						
Server Type		Client IP		Duration		

VPN Status	
Item	Description
<b>Clients</b>	
Name	Show the name of the enabled VPN clients.
Status	Show the status of client. "Connected" refers to a status that client is connected to the server. "Disconnected" means client is disconnected to the server.
Local IP	Show the local IP address of the tunnel.
Remote IP	Show the real remote IP address of the tunnel.
<b>Server</b>	
Name	Show the name of the enabled VPN Server.
Status	Show the status of Server.

Connected List	
Server Type	Show the type of the server.
Client IP	Show the IP address of the client which connected to the server.
Duration	Show the information about how long the client has been connected to this server when the server is enabled. Once the server is disabled or connection is disconnected, the duration will stop counting.

### 5.1.5 Routing

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

Routing Table					
Destination	Netmask/Prefix Length	Gateway	Interface	Metric	
127.0.0.0	255.0.0.0	-	Loopback	-	
192.168.0.0	255.255.0.0	192.168.43.1	Bridge0	1	
192.168.43.0	255.255.255.0	-	Bridge0	-	
::1	128	-	Loopback	-	

ARP Cache		
IP	MAC	Interface
192.168.43.1	b8:e3:b1:90:fd:0e	Bridge0

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

### 5.1.6 Host List

You can view the host information on this page.

Overview	Cellular	Network	VPN	Routing	Host List
DHCP Leases					
IP		MAC/DUID		Lease Remaining Time	
MAC Binding					
IP			MAC/DUID		

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

### 5.1.7 GPS

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

GPS Status	
Status	Weak Signal
Time for Locating	-
Satellites In Use	-
Satellites In View	-
Latitude	-
Longitude	-
Altitude	-
Speed	-

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

Longitude	Show the Longitude of the location.
Altitude	Show the Altitude of the location.
Speed	Show the speed of movement.

## 5.2 Network

### 5.2.1 Interface

#### 5.2.1.1 Cellular

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

Cellular
Port
USB
Bridge
Loopback

**Cellular Settings**

Protocol Type IPv4 ▼

APN

Username

Password

PIN Code

Access Number

Authentication Type Auto ▼

Network Type Auto ▼

PPP Preferred

SMS Center

Enable NAT

Roaming

Data Limit  MB

Billing Day Day  of The Month

**Connection Setting**

Connection Mode Always Online ▼

Cellular Settings	
Item	Description
Protocol Type	Select from "IPv4", "IPv6" and "IPv4/IPv6".
APN	Enter the Access Point Name for cellular dial-up connection provided by local ISP.
Username	Enter the username for cellular dial-up connection provided by local ISP.
Password	Enter the password for cellular dial-up connection provided by local ISP.
PIN Code	Enter a 4-8 characters PIN code to unlock the SIM.

Access Number	Enter the dial-up center NO. For cellular dial-up connection provided by local ISP.
Authentication Type	Select from "Auto", "PAP", "CHAP", "MS-CHAP", and "MS-CHAPv2".
Network Type	Select from "Auto", "4G Only", "3G Only", and "2G Only". Auto: connect to the network with the strongest signal automatically. 4G Only: connect to 4G network only. And so on.
PPP Preferred	The PPP dial-up method is preferred.
SMS Center	Enter the local SMS center number for storing, forwarding, converting and delivering SMS message.
Enable NAT	Enable or disable NAT function.
Roaming	Enable or disable roaming.
Data Limit	When you reach the specified data usage limit, the data connection of currently used SIM card will be disabled. 0 means disable the function.
Billing Day	Choose the billing day of the SIM card, the router will reset the data used to 0.

**Connection Setting**

Connection Mode Connect on Demand ▾

Re-dial Interval(s) 5

Max Idle Time(s) 60

Triggered by Call

Call Group ▾

Triggered by SMS

SMS Group ▾

SMS Text

Triggered by IO

Emergency Reboot

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

Triggered by SMS	The router will switch from offline mode to cellular network mode automatically when it receives a specific SMS from the specific mobile phone.
SMS Group	Select an SMS group for trigger. Go to "System > General > Phone" to set up SMS group.
SMS Text	Fill in the SMS content for triggering.
Triggered by IO	The router will switch from offline mode to cellular network mode automatically when the DI status is changed. Go to "Industrial > I/O > DI" to configure trigger condition.
Emergency Reboot	Enable or disable emergency reboot function.

### Ping Detection

Enable

IPv4 Primary Server

IPv4 Secondary Server

IPv6 Primary Server

IPv6 Secondary Server

Interval  s

Retry Interval  s

Timeout  s

Max Ping Retries

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

## Related Topics

[Cellular Network Connection](#)

[Phone Group](#)

[DI Setting](#)

### 5.2.1.2 Port

This section describes how to configure the Ethernet port parameters.

IOT-R41 cellular router supports 1 Fast Ethernet port.

Port	Status	Speed	Duplex
LAN	up	auto	auto

Port Setting	
Item	Description
Port	Users can define the Ethernet ports according to their needs.
Status	Set the status of Ethernet port; select "up" to enable and "down" to disable.
Speed	Set the Ethernet port's speed. The options are "auto", "100 Mbps", and "10 Mbps".
Duplex	Set the Ethernet port's mode. The options are "auto", "full", and "half".

### 5.2.1.3 USB

IOT-R41 equips with a USB 2.0 port for power supply or can work as a LAN port to provide network to terminal devices.

Enable

Save

### 5.2.1.4 Bridge

Bridge setting is used for managing local area network devices which are connected to LAN ports of the IOT-R41, allowing each of them to access the Internet.



**Bridge Setting**

Name

STP

IP Address

Netmask

IPv6 Address

MTU

Multiple IP Address

IP Address	Netmask	Operation
		+

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

### 5.2.1.5 Loopback

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

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

Cellular Port USB Bridge Loopback

**Loopback Address**

IP Address

Netmask

Multiple IP Addresses

IP Address	Netmask	Operation
		+

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

Addresses	other IP addresses.	
-----------	---------------------	--

## 5.2.2 DHCP

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

### 5.2.2.1 DHCP Server/DHCPv6 Server

IOT-R41 can be set as a DHCP server or DHCPv6 server to distribute IP address when a host logs on and ensures each host is supplied with different IP addresses. DHCP Server has simplified some previous network management tasks requiring manual operations to the largest extent. IOT-R41 only supports stateful DHCPv6 when working as DHCPv6 server.

DHCP Server
DHCPv6 Server
DHCP Relay

— DHCP Server\_1

Enable

Interface

Start Address

End Address

Netmask

Lease Time(Min)

Primary DNS Server

Secondary DNS Server

Windows Name Server

**Static IP**

MAC Address	IP Address	Operation
		+

DHCP Server      **DHCPv6 Server**      DHCP Relay

---

— DHCPv6 Server\_1

Enable

Interface

Start Address

End Address

Prefix Length

Lease Time(Min)

Primary DNS Server

Secondary DNS Server

**Static IP**

DUID	IPv6 Address	Operation
		+

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

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

### 5.2.2.2 DHCP Relay

IOT-R41 can be set as DHCP Relay to provide a relay tunnel to solve the problem that DHCP Client and DHCP Server are not in the same subnet.

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

### 5.2.3 Firewall

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

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

### 5.2.3.1 Security

Security    ACL    Port Mapping    DMZ    MAC Binding    Custom Rules    SPI

**Prevent Attack**

DoS/DDoS Protection

**Access Service Control**

Service	Port	Local	Remote
HTTP	<input type="text" value="80"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
HTTPS	<input type="text" value="443"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
TELNET	<input type="text" value="23"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
SSH	<input type="text" value="22"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
FTP	<input type="text" value="21"/>	<input type="checkbox"/>	<input type="checkbox"/>

**Website Blocking**

URL Blocking

Keyword Blocking

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

Website Blocking	
URL Blocking	Enter the HTTP address which you want to block.
Keyword Blocking	You can block specific website by entering keyword. The maximum number of character allowed is 64.

### 5.2.3.2 ACL

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

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

Item	Description
<b>ACL Setting</b>	
Default Filter Policy	Select from "Accept" and "Deny". The packets which are not included in the access control list will be processed by the default filter policy.
<b>Access Control List</b>	
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.
<b>Interface List</b>	
Interface	Select network interface for access control.
In ACL	Select a rule for incoming traffic from ACL ID.
Out ACL	Select a rule for outgoing traffic from ACL ID.

## Related Configuration Example

[Access Control Application Example](#)

### 5.2.3.3 Port Mapping

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

Port Mapping	
Item	Description
Source IP	Specify the host or network which can access local IP address. 0.0.0.0/0 means all.
Source Port	Enter the TCP or UDP port from which incoming packets are forwarded. Range: 1-65535.
Destination IP	Enter the IP address that packets are forwarded to after being received on the incoming interface.

Destination Port	Enter the TCP or UDP port that packets are forwarded to after being received on the incoming port(s). Range: 1-65535.
Protocol	Select from "TCP" and "UDP" as your application required.
Description	The description of this rule.

## Related Configuration Example

[NAT Application Example](#)

### 5.2.3.4 DMZ

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

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

### 5.2.3.5 MAC Binding

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

MAC Binding List	
Item	Description
MAC Address	Set the binding MAC address.



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

### 5.2.3.6 Custom Rules

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

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

### 3.2.3.7 SPI

SPI Firewall	
Item	Description

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

## 5.2.4 QoS

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

QoS	
Item	Description
<b>Download/Upload</b>	
Enable	Enable or disable QoS.
Default Category	Select the default category from Service Category list.
Download/Upload Bandwidth Capacity	The download/upload bandwidth capacity of the network that the router is connected with, in kbps. Range:

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

## Related Configuration Example

[QoS Application Example](#)

### 3.2.5 VPN

Virtual Private Networks, also called VPNs, are used to securely connect two private networks together so that devices can connect from one network to the other network via secure channels. The IOT-R41 supports DMVPN, IPsec, GRE, L2TP, PPTP, OpenVPN, as well as GRE over IPsec and L2TP over IPsec.

#### 3.2.5.1 DMVPN

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

Status	DMVPN	IPsec Server	IPsec	GRE	L2TP	PPTP	OpenVPN Client	OpenVPN Server	Certifications
Network	<b>DMVPN Settings</b>								
Interface	Enable	<input type="checkbox"/>							
DHCP	Hub Address	<input type="text"/>							
Firewall	Local IP Address	<input type="text"/>							
QoS	GRE HUB IP Address	<input type="text"/>							
VPN	GRE Local IP Address	<input type="text"/>							
IP Passthrough	GRE Mask	<input type="text" value="255.255.255.0"/>							
Routing	GRE Key	<input type="text"/>							
VRRP	Negotiation Mode	Main <input type="button" value="v"/>							
DDNS	Authentication Algorithm	DES <input type="button" value="v"/>							
System	Encryption Algorithm	MD5 <input type="button" value="v"/>							
Industrial	DH Group	MODP768-1 <input type="button" value="v"/>							
Maintenance	Key	<input type="text"/>							
	Local ID Type	Default <input type="button" value="v"/>							
	IKE Life Time(s)	<input type="text" value="10800"/>							
	SA Algorithm	DES-MD5 <input type="button" value="v"/>							
	PFS Group	NULL <input type="button" value="v"/>							
	Life Time(s)	<input type="text" value="3600"/>							
	DPD Time Interval(s)	<input type="text" value="30"/>							
	DPD Timeout(s)	<input type="text" value="150"/>							
	Cisco Secret	<input type="text"/>							
	NHRP Holdtime(s)	<input type="text" value="7200"/>							

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

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

### 5.2.5.2 IPsec Server

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

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

IPsec Server	
Item	Description
Enable	Enable IPsec tunnel. A maximum of 3 tunnels is allowed.
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".

**IKE Parameter**

IKE Version: IKEv1

Negotiation Mode: Main

Encryption Algorithm: DES

Authentication Algorithm: MD5

DH Group: MODP768-1

Local Authentication: PSK

XAUTH

Lifetime(s): 10800

**XAUTH List**

Username	Password	Operation
		+

**PSK List**

Selector	PSK	Operation
		+

**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

Expert Options:

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".
XAUTH	Enter XAUTH username and password after XAUTH is enabled.
Lifetime (s)	Set the lifetime in IKE negotiation. Range: 60-86400.
XAUTH List	

Username	Enter the username used for the xauth authentication.
Password	Enter the password used for the xauth authentication.
<b>PSK List</b>	
Selector	Enter the corresponding identification number for PSK authentication.
PSK	Enter the pre-shared key.
<b>SA Parameter</b>	
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.
<b>IPsec Advanced</b>	
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.
Expert Options	User can enter some other initialization strings in this field and separate the strings with ",". For example, if more local or remote subnet need to be added, users can add contents here.

### 5.2.5.3 IPsec

DMVPN
IPsec Server
IPsec
GRE
L2TP
PPTP
OpenVPN Client

**IPsec Settings**

- IPsec\_1

Enable	<input type="checkbox"/>
IPsec Gateway Address	<input type="text"/>
IPsec Mode	<input type="text" value="Tunnel"/>
IPsec Protocol	<input type="text" value="ESP"/>
Local Subnet	<input type="text"/>
Local Subnet Mask	<input type="text"/>
Local ID Type	<input type="text" value="Default"/>
Remote Subnet	<input type="text"/>
Remote Subnet Mask	<input type="text"/>
Remote ID Type	<input type="text" value="Default"/>
IKE Parameter	<input type="checkbox"/>
SA Parameter	<input type="checkbox"/>
IPsec Advanced	<input checked="" type="checkbox"/>
Expert Options	<input type="text"/>

+ IPsec\_2

+ IPsec\_3

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".

IKE Parameter	<input checked="" type="checkbox"/>
IKE Version	IKEv1
Negotiation Mode	Main
Encryption Algorithm	AES128
Authentication Algorithm	SHA1
DH Group	MODP768-1
Local Authentication	PSK
Local Secrets	*****
XAUTH	<input checked="" type="checkbox"/>
Username	
Password	
Lifetime(s)	28800
SA Parameter	<input type="checkbox"/>
IPsec Advanced	<input checked="" type="checkbox"/>
Enable Compression	<input checked="" type="checkbox"/>
VPN Over IPsec Type	NONE
Expert Options	

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 pre-shared 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.
<b>IPsec Advanced</b>	
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.
Expert Option	User can enter some other initialization strings in this field and separate the strings with ";". For example, if more local or remote subnet need to be added, users can add contents here.

#### 5.2.5.4 GRE

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

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

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

The screenshot displays the 'GRE Settings' configuration page. At the top, there are navigation tabs: DMVPN, IPsec Server, IPsec, GRE (selected), L2TP, PPTP, and OpenVPN Client. Below the tabs, the 'GRE Settings' section is visible, containing a list of configuration options for a GRE tunnel named 'GRE\_1':

- Enable:
- Remote IP Address:
- Local IP Address:
- Local Virtual IP Address:
- Netmask:
- Peer Virtual IP Address:
- Global Traffic Forwarding:
- Remote Subnet:
- Remote Netmask:
- MTU:
- Key:
- Enable NAT:

At the bottom of the settings list, there are expandable sections for 'GRE\_2' and 'GRE\_3', each with a plus sign icon.

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

### 5.2.5.5 L2TP

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

L2TP	
Item	Description
Enable	Check to enable L2TP function.

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

Advanced Settings	<input checked="" type="checkbox"/>
Local IP Address	<input type="text"/>
Peer IP Address	<input type="text"/>
Enable NAT	<input checked="" type="checkbox"/>
Enable MPPE	<input type="checkbox"/>
Address/Control Compression	<input type="checkbox"/>
Protocol Field Compression	<input type="checkbox"/>
Asyncmap Value	<input type="text" value="ffffff"/>
MRU	<input type="text" value="1500"/>
MTU	<input type="text" value="1500"/>
Link Detection Interval(s)	<input type="text" value="60"/>
Max Retries	<input type="text" value="0"/>
Expert Options	<input type="text"/>

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-ffffff.

MRU	Set the maximum receive unit. Range: 64-1500.
MTU	Set the maximum transmission unit. Range: 64-1500
Link Detection Interval (s)	Set the link detection interval time to ensure tunnel connection. Range: 0-600.
Max Retries	Set the maximum times of retry to detect the L2TP connection failure. Range: 0-10.
Expert Options	User can enter some other PPP initialization strings in this field and separate the strings with blank space.

### 5.2.5.6 PPTP

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

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

Forwarding	enable this function.
Remote Subnet	Set the peer subnet of PPTP.
Remote Subnet Mask	Set the netmask of peer PPTP server.

Advanced Settings

Local IP Address

Peer IP Address

Enable NAT

Enable MPPE

Address/Control Compression

Protocol Field Compression

Asyncmap Value

MRU

MTU

Link Detection Interval(s)

Max Retries

Expert Options

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 function 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-ffffff.
MRU	Enter the maximum receive unit. Range: 0-1500.
MTU	Enter the maximum transmission unit. Range: 0-1500.
Link Detection Interval (s)	Set the link detection interval time to ensure tunnel connection. Range: 0-600.
Max Retries	Set the maximum times of retrying to detect the PPTP connection failure. Range: 0-10.
Expert Options	User can enter some other PPP initialization strings in this field and separate the strings with blank space.

## Related Configuration Example

[PPTP Application Example](#)

### 5.2.5.7 OpenVPN Client

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

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).

The screenshot displays the 'OpenVPN Client Settings' configuration page. The 'OpenVPN Client\_1' section is expanded, showing the following settings:

- Enable:
- Protocol: UDP
- Remote IP Address: [Empty text box]
- Port: 1194
- Interface: tun
- Authentication: None
- Local Tunnel IP: [Empty text box]
- Remote Tunnel IP: [Empty text box]
- Enable NAT:
- Compression: LZO
- Link Detection Interval(s): 60
- Link Detection Timeout(s): 300
- Cipher: None
- MTU: 1500
- Max Frame Size: 1500
- Verbose Level: ERROR
- Expert Options: [Empty text box]

Below the settings is a 'Local Route' table with columns for Subnet, Subnet Mask, and Operation.

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. <b>Note:</b> this option only supports tls-auth. For tls-crypt, please add this format string on expert option: <code>tls-crypt /etc/openvpn/openvpn-client1-ta.key</code>
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", "WARNING", "NOTICE" and "DEBUG".
Expert Options	User can enter some other PPP initialization strings in this field and separate the strings with semicolon. <b>Example:</b> <code>auth SHA256; key direction 1</code>
<b>Local Route</b>	
Subnet	Set the local route's IP address.
Subnet Mask	Set the local route's netmask.

### 5.2.5.8 OpenVPN Server

The IOT-R41 supports OpenVPN server to create secure point-to-point or site-to-site connections in routed or bridged configurations and remote access facilities.

DMVPN    IPsec    GRE    L2TP    PPTP    OpenVPN Client    **OpenVPN Server**

**OpenVPN Server Settings**

Enable

Protocol

Port

Listening IP

Interface

Authentication

Local Virtual IP

Remote Virtual IP

Enable NAT

Compression

Link Detection Interval

Cipher

MTU

Max Frame Size

Verbose Level

Expert Options

**Account**

Username	Password	Operation
		+

**Local Route**

Subnet	Netmask	Operation
		+

**Client Subnet**

Name	Subnet	Netmask	Operation
			+

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 or disable CRL verify.
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", "WARNING", "NOTICE" and "DEBUG".
Expert Options	User can enter some other PPP initialization strings in this field and separate the strings with semicolon. <b>Example:</b> auth SHA256; key direction 1
<b>Local Route</b>	
Subnet	The real local IP address of OpenVPN client.
Netmask	The real local netmask of OpenVPN client.
<b>Account</b>	
Username & Password	Set username and password for OpenVPN client.

### 5.2.5.9 Certifications

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

The screenshot shows a web interface for managing OpenVPN Client certificates. At the top, there are navigation tabs for DMVPN, IPsec, GRE, L2TP, PPTP, OpenVPN Client, OpenVPN Server, and Certifications. The 'OpenVPN Client' tab is active, and the 'Certifications' sub-tab is selected. Below the navigation, there is a section titled 'OpenVPN Client' with a sub-section 'OpenVPN client\_1'. This section contains a table with the following columns: Certificate Type, File Path, Browse, Import, Export, and Delete. The rows are:

CA	Public Key	Private Key	TA	Preshared Key	PKCS12
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
<input type="button" value="Browse"/>	<input type="button" value="Browse"/>	<input type="button" value="Browse"/>	<input type="button" value="Browse"/>	<input type="button" value="Browse"/>	<input type="button" value="Browse"/>
<input type="button" value="Import"/>	<input type="button" value="Import"/>	<input type="button" value="Import"/>	<input type="button" value="Import"/>	<input type="button" value="Import"/>	<input type="button" value="Import"/>
<input type="button" value="Export"/>	<input type="button" value="Export"/>	<input type="button" value="Export"/>	<input type="button" value="Export"/>	<input type="button" value="Export"/>	<input type="button" value="Export"/>
<input type="button" value="Delete"/>	<input type="button" value="Delete"/>	<input type="button" value="Delete"/>	<input type="button" value="Delete"/>	<input type="button" value="Delete"/>	<input type="button" value="Delete"/>

At the bottom of the screenshot, there is a blue header bar with the text '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.

**OpenVPN Server**

— OpenVPN Server

CA	<input type="text"/>	<a href="#">Browse</a>	<a href="#">Import</a>	<a href="#">Export</a>	<a href="#">Delete</a>
Public Key	<input type="text"/>	<a href="#">Browse</a>	<a href="#">Import</a>	<a href="#">Export</a>	<a href="#">Delete</a>
Private Key	<input type="text"/>	<a href="#">Browse</a>	<a href="#">Import</a>	<a href="#">Export</a>	<a href="#">Delete</a>
DH	<input type="text"/>	<a href="#">Browse</a>	<a href="#">Import</a>	<a href="#">Export</a>	<a href="#">Delete</a>
TA	<input type="text"/>	<a href="#">Browse</a>	<a href="#">Import</a>	<a href="#">Export</a>	<a href="#">Delete</a>
CRL	<input type="text"/>	<a href="#">Browse</a>	<a href="#">Import</a>	<a href="#">Export</a>	<a href="#">Delete</a>
Preshared Key	<input type="text"/>	<a href="#">Browse</a>	<a href="#">Import</a>	<a href="#">Export</a>	<a href="#">Delete</a>

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.

**IPsec**

— IPsec\_1

CA	<input type="text"/>	<a href="#">Browse</a>	<a href="#">Import</a>	<a href="#">Export</a>	<a href="#">Delete</a>
Client Key	<input type="text"/>	<a href="#">Browse</a>	<a href="#">Import</a>	<a href="#">Export</a>	<a href="#">Delete</a>
Server Key	<input type="text"/>	<a href="#">Browse</a>	<a href="#">Import</a>	<a href="#">Export</a>	<a href="#">Delete</a>
Private Key	<input type="text"/>	<a href="#">Browse</a>	<a href="#">Import</a>	<a href="#">Export</a>	<a href="#">Delete</a>
CRL	<input type="text"/>	<a href="#">Browse</a>	<a href="#">Import</a>	<a href="#">Export</a>	<a href="#">Delete</a>

IPsec	
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.

**IPsec Server**

— IPsec Server

CA	<input type="text"/>	<input type="button" value="Browse"/>	<input type="button" value="Import"/>	<input type="button" value="Export"/>	<input type="button" value="Delete"/>
Local Certificate	<input type="text"/>	<input type="button" value="Browse"/>	<input type="button" value="Import"/>	<input type="button" value="Export"/>	<input type="button" value="Delete"/>
Private Key	<input type="text"/>	<input type="button" value="Browse"/>	<input type="button" value="Import"/>	<input type="button" value="Export"/>	<input type="button" value="Delete"/>
CRL	<input type="text"/>	<input type="button" value="Browse"/>	<input type="button" value="Import"/>	<input type="button" value="Export"/>	<input type="button" value="Delete"/>

IPsec Server	
Item	Description
CA	Import/Export CA certificate.
Local Certificate	Import/Export Local Certificate file.
Private Key	Import/Export private key.
CRL	Import/Export certificate recovery list.

## 5.2.6 IP Passthrough

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

Status

Network ▾

Interface

DHCP

Firewall

QoS

VPN

**IP Passthrough**

**IP Passthrough**

Enable

Passthrough Mode

MAC

**IP Passthrough**

Item	Description
Enable	Enable or disable IP Passthrough.
Passthrough Mode	Select passthrough mode from "DHCP-Static" and "DHCP-Dynamic".
MAC	Set MAC address.

## 5.2.7 Routing

### 5.2.7.1 Static Routing

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

Destination	Netmask/Prefix Length	Interface	Gateway	Distance	Operation
114.114.114.114	255.255.255.255	LAN1/WAN	192.168.5.1	1	X
8.8.8.8	255.255.255.255	LAN1/WAN	192.168.5.1	1	X
0.0.0.0	0.0.0.0	LAN1/WAN	192.168.5.1	1	X
					+

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

### 5.2.7.2 RIP

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

also introduces routing obtained by other routing protocols.

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

Static Routing	<b>RIP</b>	OSPF	Routing Filtering
<b>RIP Settings</b>			
Enable	<input checked="" type="checkbox"/>		
Update Timer	<input type="text" value="30"/>		s
Timeout Timer	<input type="text" value="180"/>		s
Garbage Collection Timer	<input type="text" value="120"/>		s
Version	<input type="text" value="v2"/>		
Show Advanced Options	<input checked="" type="checkbox"/>		
Default Information Originate	<input type="checkbox"/>		
Default Metric	<input type="text" value="1"/>		
Redistribute Connected	<input type="checkbox"/>		
Redistribute Static	<input type="checkbox"/>		
Redistribute OSPF	<input type="checkbox"/>		

<b>RIP</b>	
<b>Item</b>	<b>Description</b>
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.
<b>Advanced Settings</b>	

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.

**Distance/Metric Management**

Distance	IP Address	Netmask	ACL Name	Operation
				+

Metric	Policy In/Out	Interface	ACL Name	Operation
				+

**Filter Policy**

Policy Type	Policy Name	Policy In/Out	Interface	Operation
				+

**Passive Interface**

Passive Interface	Operation
	+

**Interface**

Interface	Send Version	Receive Version	Split-Horizon	Authentication Mode	Authentication String	Authentication Key-chain	Operation
							+

**Neighbor**

IP Address	Operation
	+

**Network**

IP Address	Netmask	Operation
		+

Item	Description
<b>Distance/Metric Management</b>	

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

### 5.2.7.3 OSPF

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

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

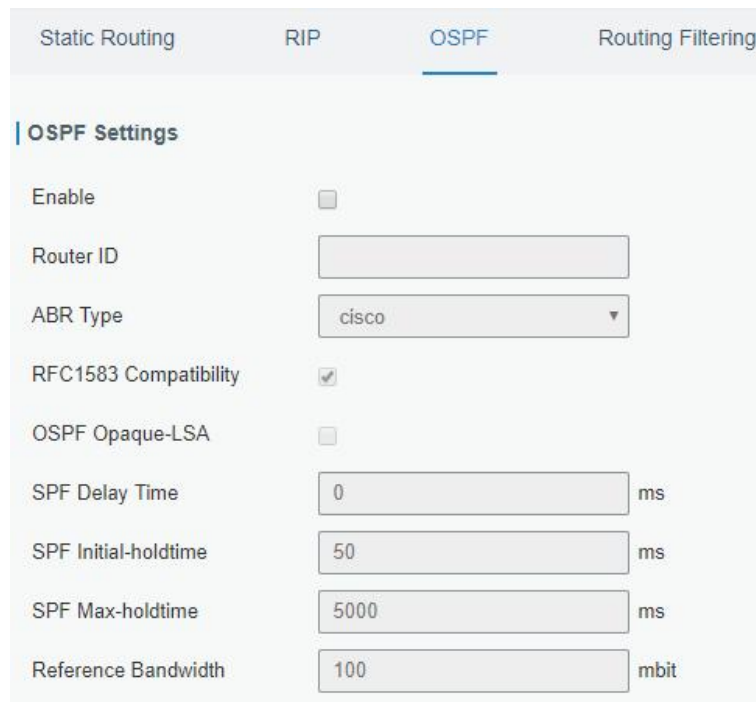
- If a Loopback interface address is configured, then the last configured IP address of Loopback interface will be used as the Router ID;
- If no Loopback interface address is configured, the system will choose the interface with the biggest IP address as the Router ID.

### Five types of packets of OSPF:

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

### Neighbor and Neighboring

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





OSPF	
Item	Description
Enable	Enable or disable OSPF.
Router ID	Router ID (IP address) of the originating LSA.
ABR Type	Select from cisco, ibm, standard and shortcut.





RFC1583 Compatibility	Enable/Disable.
OSPF Opaque-LSA	Enable/Disable LSA: a basic communication means of the OSPF routing protocol for the Internet Protocol (IP).
SPF Delay Time	Set the delay time for OSPF SPF calculations. Range: 0-6000000, in milliseconds.
SPF Initial-holdtime	Set the initialization time of OSPF SPF. Range: 0-6000000, in milliseconds.
SPF Max-holdtime	Set the maximum time of OSPF SPF. Range: 0-6000000, in milliseconds.
Reference Bandwidth	Range: 1-4294967, in Mbit.

Interface

Interface	Hello Interval(s)	Dead Interval(s)	Retransmit Interval(s)	Transmit Delay(s)	Operation
Bridge0	10	40	5	1	 

Interface Advanced Options

Interface	Network	Cost	Priority	Authenticat ion	Key ID	Key	Operation
Bridge	broad	10	1				 

Item	Description
<b>Interface</b>	
Interface	Select interface from "cellular0"and "Bridge0".
Hello Interval (s)	Send interval of Hello packet. If the Hello time between two adjacent routers is different, the neighbour relationship cannot be established. Range: 1-65535.
Dead Interval (s)	Dead Time. If no Hello packet is received from the neighbours within the dead time, then the neighbour is considered failed. If dead times of two adjacent routers are different, the neighbour relationship cannot be established.
Retransmit Interval (s)	When the router notifies an LSA to its neighbour, it is required to make acknowledgement. If no acknowledgement packet is received within the retransmission interval, this LSA will be retransmitted to the neighbour. Range: 3-65535.
Transmit Delay (s)	It will take time to transmit OSPF packets on the link. So a certain delay time should be increased before transmission the aging time of LSA. This configuration needs to be further considered on the low-speed link. Range: 1-65535.
<b>Interface Advanced Options</b>	

Interface	Select interface.
Network	Select OSPF network type.
Cost	Set the cost of running OSPF on an interface. Range: 1-65535.
Priority	Set the OSPF priority of interface. Range: 0-255.
Authentication	Set the authentication mode that will be used by the OSPF area. Simple: a simple authentication password should be configured and confirmed again. MD5: MD5 key & password should be configured and confirmed again.
Key ID	It only takes effect when MD5 is selected. Range 1-255.
Key	The authentication key for OSPF packet interaction.

**Passive Interface**

Passive Interface			Operation
			+

**Network**

IP Address	Netmask	Area ID	Operation
			+

**Neighbor**

IP Address	Priority	Poll	Operation
			+

**Area**

Area ID	Area	No Summary	Authentication	Operation
				+

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

Area Advanced Options

Area Range

Area ID	IP Address	Netmask	No Advertise	Cost	Operation

Area Filter

Area ID	Filter Type	ACL Name	Operation

Area Virtual Link

Area ID	ABR Address	Authentication	Key ID	Key	Hello Interval	Dead Interval	Retransmit Interval	Transmit Delay	Operation

Area Advanced Options	
Item	Description
<b>Area Range</b>	
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
<b>Area Filter</b>	
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.
<b>Area Virtual Link</b>	
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.

Redistribution

Redistribution Type	Metric	Metric Type	Route Map	Operation
connected		1		<input type="button" value="X"/>
				<input type="button" value="+"/>

Redistribution Advanced Options

Always Redistribute Default Route

Redistribute Default Route Metric

Redistribute Default Route Metric Type

Distance Management

Area Type	Distance	Operation
		<input type="button" value="+"/>

Item	Description
<b>Redistribution</b>	
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.
<b>Redistribution Advanced Options</b>	
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".
<b>Distance Management</b>	
Area Type	Select from "intra-area", "inter-area" and "external".
Distance	Set the OSPF routing distance for area learning. Range: 1-255.

### 5.2.7.4 Routing Filtering

Static Routing   RIP   OSPF   Routing Filtering

**Access Control List**

Name	Action	Match Any	IP Address	Netmask	Operation
<input type="text"/>	deny	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="X"/>
					<input type="button" value="+"/>

**IP Prefix-List**

Name	Sequence Number	Action	Match Any	IP Address	Netmask	GE Length	LE Length	Operation
<input type="text"/>	<input type="text"/>	deny	<input type="checkbox"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="button" value="X"/>
								<input type="button" value="+"/>

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

## 5.2.8 VRRP

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

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

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

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

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

VRRP has the following characteristics:

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

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

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

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

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

### 5.2.9 DDNS

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

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

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

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

## 5.3 System

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

### 5.3.1 General Settings

#### 5.3.1.1 General

General settings include system info and HTTPS certificates.

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



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

### 5.3.1.2 System Time

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

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

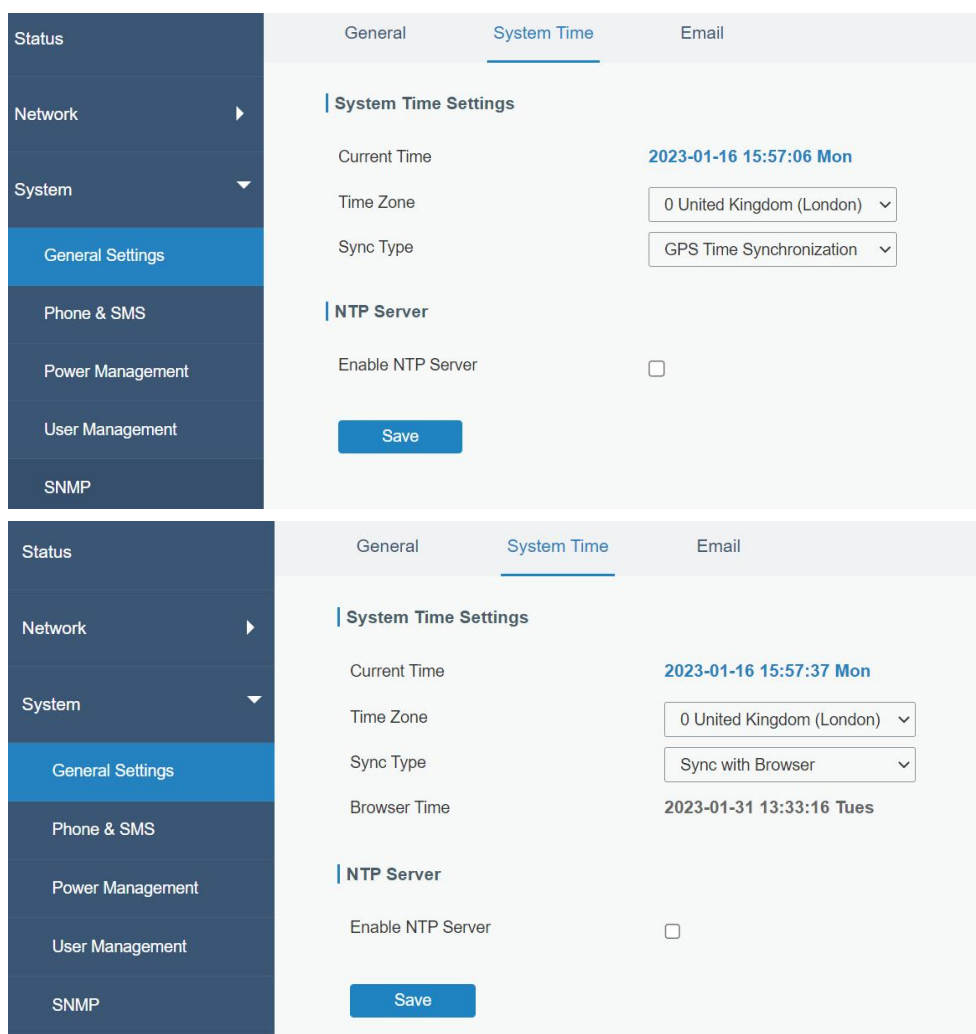
The image displays two screenshots of the router's configuration interface, specifically the 'System Time' settings page. The left sidebar shows the navigation menu with 'General Settings' selected.

**Top Screenshot: NTP Synchronization**

- Current Time: 2023-01-16 15:55:33 Mon
- Time Zone: 0 United Kingdom (London)
- Sync Type: Sync with NTP Server
- Primary NTP Server: pool.ntp.org
- Secondary NTP Server: (empty)
- Enable NTP Server:

**Bottom Screenshot: Manual Time Setting**

- Current Time: 2023-01-16 15:56:01 Mon
- Time Zone: 0 United Kingdom (London)
- Sync Type: Set up Manually
- Date: 2023-01-31
- Time: 13:36
- Enable NTP Server:



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.
GPS Time Synchronization	Synchronize time with GPS.
Primary NTP Server	Enter primary NTP Server's IP address or domain name.
Secondary NTP Server	Enter secondary NTP Server's IP address or domain name.
NTP Server	
Enable NTP Server	NTP client on the network can achieve time synchronization with router after "Enable NTP Server" option is checked.

### 5.3.1.3 Email

SMTP, short for Simple Mail Transfer Protocol, is a TCP/IP protocol used in sending and receiving

e-mail. This section describes how to configure email settings and add email groups for alarms and events.

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

General   System Time   Email

**Test**

**Email List**

Email Address	Description	Operation
<input type="text"/>	<input type="text"/>	<input type="button" value="X"/>
<input type="button" value="+"/>		

**Email Group List**

Group ID

Description

List

Selected

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

## Related Topics

[DI Setting](#)

[Events Setting](#)

[Events Application Example](#)

## 5.3.2 Phone&SMS

### 5.3.2.1 Phone

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

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

### Related Topic

[Connect on Demand](#)

### 5.3.2.2 SMS

SMS settings involve in remote SMS control, sending SMS and SMS receiving and sending status.

SMS Settings	
Item	Description
SMS Mode	Select SMS mode from "TEXT" and "PDU".
SMS Remote Control	Enable/disable SMS Remote Control.
Authentication Type	You can choose "phone number" or "password + phone number". Phone number: Use phone number for authentication. Password + phone number: Use both ""Password"" and ""Phone number"" for authentication.
Password	Set password for authentication.
Phone Group	Select the Phone group which used for remote control. User can click the Phone Group and set phone number.

**Send SMS**

Phone Number

Content

**Inbox**

From  To  Sender

Sender	Time	Content
--------	------	---------

< > 10 ▾ Go to:

**Outbox**

From  To  Recipient

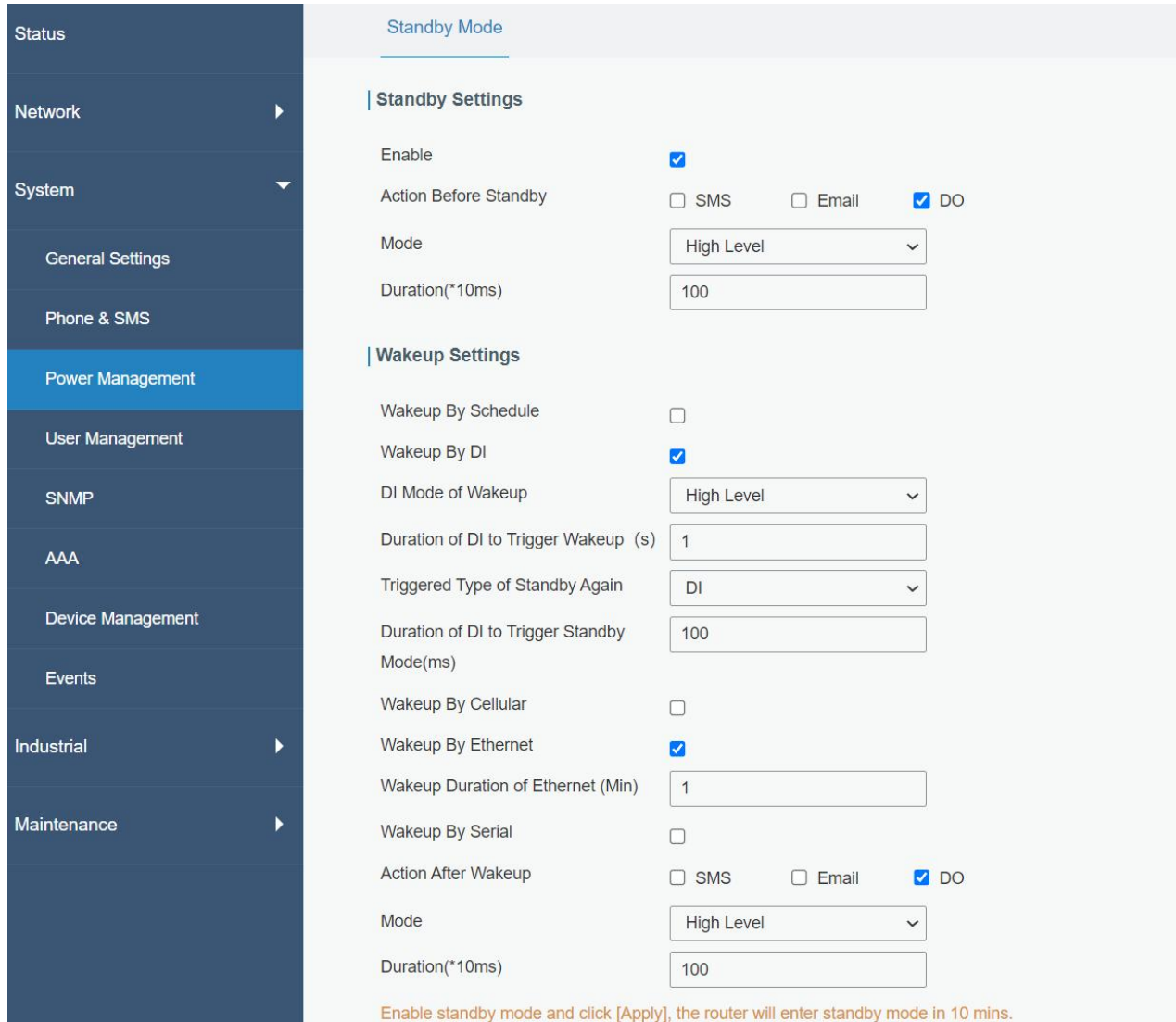
Recipient	Time	Content	Status
-----------	------	---------	--------

SMS	
Item	Description
<b>Send SMS</b>	
Phone Number	Enter the number to receive the SMS.
Content	SMS content.
<b>Inbox/Outbox</b>	
Sender	SMS sender from outside.
Recipient	SMS recipient which IOT-R41 send to.
From	Select the start date.
To	Select the end date.

Search	Search for SMS record.
Clear All	Clear all SMS records in web GUI.

### 5.3.3 Power Management

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



Standby Mode	
Item	Description
<b>Standby Settings</b>	
Enable	Enable or disable standby mode.
Action Before Standby	Set the action before the router enters the standby mode. If the settings is enabled, the router will execute the action before entering the standby mode.
SMS	Tick to enable SMS alarm before the router enters the standby mode.
Phone Group	Set phone number to receive SMS alarm.

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



	Ensure that the router has registered to cellular network before standby.
Call Group	Select a call group for cellular wakeup. Go to "System > Phone & SMS > Phone" to set up the phone group.
SMS Group	Select a SMS group for cellular wakeup. Go to "System > Phone & SMS > Phone" to set up the phone group.
SMS Text	Fill in the SMS content for wakeup.
Wakeup Duration of Cellular	Set the duration of entering standby mode again after the router is woken up by cellular.
Wakeup By Ethernet	The router will be woken up when Ethernet interface receives a special frame (E8:E8:B7:07:FB:BD).
Wakeup Duration of Ethernet	Set the duration of entering standby mode again after the router is woken up by Ethernet.
Wakeup By Serial	The router will be woken up when serial port receives a 1-byte data packet. <b>Note:</b> the serial device need to send 1-byte wake-up data before sending normal data.
Wakeup Duration of Serial	Set the duration of entering standby mode again after the router is woken up by serial.
Action After Wakeup	Set the action after the router wakes up.
SMS	Enable SMS alarm after the router wakes up.
Email	Enable Email alarm after the router wakes up.
DO	Enable to trigger DO after the router wakes up.

**Note:**

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

### 5.3.4 User Management

#### 5.3.4.1 Account

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

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

The screenshot shows a web interface for 'User Management' with a sidebar on the left containing 'Status', 'Network', 'System', 'General Settings', 'Phone & SMS', 'Power Management', and 'User Management'. The main content area is titled 'Account' and 'User Management'. Below this is a section for 'Change Account Info' with four input fields: 'Username' (containing 'admin'), 'Old Password', 'New Password', and 'Confirm New Password'. A blue 'Save' button is located below the fields.

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

### 5.3.4.2 User Management

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

The screenshot shows a 'User List' table with four columns: 'Username', 'Password', 'Permission', and 'Operation'. The 'Username' and 'Password' columns have empty input boxes. The 'Permission' column has a dropdown menu currently set to 'Read-Only'. The 'Operation' column contains a delete icon (X) and a plus icon (+).

User Management	
Item	Description
Username	Enter a new username. Only lowercase letters, digits, "_", "-" are allowed. The first character can't be a digit.
Password	Set password.
Permission	Select user permission from "Read-Only" and "Read-Write". <ul style="list-style-type: none"> <li>- Read-Only: users can only view the configuration of router in this level.</li> <li>- Read-Write: users can view and set the configuration of router in this level.</li> </ul>

### 5.3.5 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 VACM.

## Related Configuration Example

[SNMP Application Example](#)

### 5.3.5.1 SNMP

IOT-R41 supports SNMPv1, SNMPv2c and SNMPv3 version. SNMPv1 and SNMPv2c employ community name authentication. SNMPv3 employs authentication encryption by username and password.

The screenshot shows the 'SNMP Settings' configuration page. It includes a navigation bar with tabs for 'SNMP', 'MIB View', 'VACM', 'Trap', and 'MIB'. The 'SNMP' tab is selected. Below the navigation bar, the 'SNMP Settings' section contains the following fields:

- Enable:** A checkbox that is checked.
- Port:** A text input field containing the value '161'.
- SNMP Version:** A dropdown menu currently set to 'SNMPv2'.
- Location Information:** A text input field containing the value '225\_location'.
- Contact Information:** A text input field containing the value '225\_Contact'.

A blue 'Save' button is located at the bottom of the configuration area.

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

### 5.3.5.2 MIB View

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

SNMP    MIB View    VACM    Trap    MIB

**View List**

View Name	View Filter	View OID	Operation
<input type="text" value="All"/>	<input type="text" value="Included"/>	<input type="text" value="1"/>	<input type="button" value="X"/>
<input type="text" value="system"/>	<input type="text" value="Included"/>	<input type="text" value="1.3.6.1.2.1.1"/>	<input type="button" value="X"/>
			<input type="button" value="+"/>

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

### 5.3.5.3 VACM

This section describes how to configure VACM parameters.

SNMP    MIB View    VACM    Trap    MIB

**SNMP v1 & v2 User List**

Community	Permission	MIB View	Network	Operation
<input type="text" value="private"/>	<input type="text" value="Read-Write"/>	<input type="text" value="All"/>	<input type="text" value="0.0.0.0/0"/>	<input type="button" value="X"/>
<input type="text" value="public"/>	<input type="text" value="Read-Write"/>	<input type="text" value="All"/>	<input type="text" value="0.0.0.0/0"/>	<input type="button" value="X"/>
				<input type="button" value="+"/>

VACM	
Item	Description
SNMP v1 & v2 User List	
Community	Set the community name.
Permission	Select from "Read-Only" and "Read-Write".
MIB View	Select an MIB view to set permissions from the MIB view list.
Network	The IP address and bits of the external network accessing the MIB view.
Read-Write	The permission of the specified MIB node is read and write.
Read-Only	The permission of the specified MIB node is read only.
SNMP v3 User Group	
Group Name	Set the name of SNMPv3 group.
Security Level	Select from "NoAuth/NoPriv", "Auth/NoPriv", and "Auth/Priv".
Read-Only View	Select an MIB view to set permission as "Read-only" from the MIB view list.
Read-Write View	Select an MIB view to set permission as "Read-write" from the MIB view list.

Inform View	Select an MIB view to set permission as "Inform" from the MIB view list.
<b>SNMP v3 User List</b>	
Username	Set the name of SNMPv3 user.
Group Name	Select a user group to be configured from the user group.
Authentication	Select from "MD5", "SHA", and "None".
Authentication Password	The password should be filled in if authentication is "MD5" and "SHA".
Encryption	Select from "AES", "DES", and "None".
Encryption Password	The password should be filled in if encryption is "AES" and "DES".

### 5.3.5.4 Trap

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

**SNMP Trap**

Enable

SNMP Version

Server Address

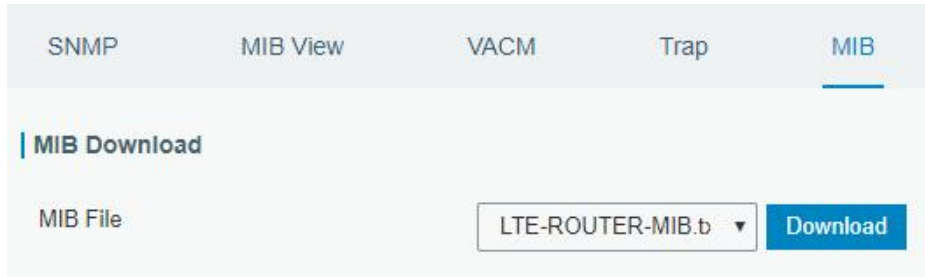
Port

Name

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

### 5.3.5.5 MIB

This section describes how to download MIB files. The last MIB file "LTE-ROUTER-MIB.txt" is for the IOT-R41 router.



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

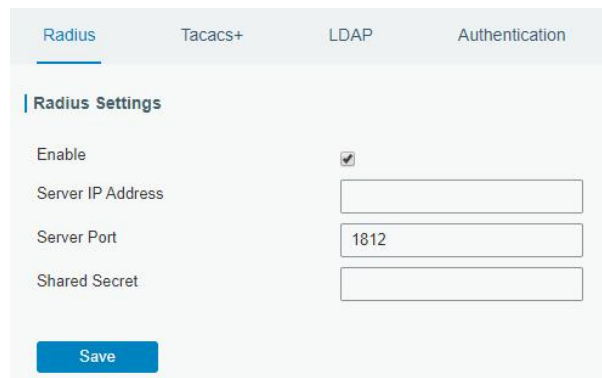
### 5.3.6 AAA

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

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

#### 5.3.6.1 Radius

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



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

### 5.3.6.2 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.

Radius   Tacacs+   LDAP   Authentication

**Tacacs+ Settings**

Enable

Server IP Address

Server Port

Shared Secret

Save

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

### 5.3.6.3 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.

Radius   Tacacs+   LDAP   Authentication

**LDAP Settings**

Enable

Server IP Address

Server Port

Base DN

Security

Username

Password

Save

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

### 5.3.6.4 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.

Service	1	2	3
Console	None	None	None
Web	None	None	None
Telnet	None	None	None
SSH	None	None	None

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

### 5.3.7 Device Management

#### 5.3.7.1 DeviceHub

You can connect the device to the LINOVISION DeviceHub on this page so as to manage the router



centrally and remotely. For more details please refer to *DeviceHub User Guide*.

DeviceHub	
Item	Description
Status	Show the connection status between the router and the DeviceHub.
Disconnected	Click this button to disconnect the router from the DeviceHub.
Server Address	IP address or domain of the device management server.
Activation Method	Select activation method to connect the router to the DeviceHub server, options are "By Authentication Code" and "By Account name".
Authentication Code	Fill in the authentication code generated from the DeviceHub.
Account name	Fill in the registered DeviceHub account (email) and password.
Password	

### 5.3.7.2 LINOVISION VPN

You can connect the device to the LINOVISION VPN on this page so as to manage the router and connected devices centrally and remotely.

Device Management
Milesight VPN

---

**Milesight VPN Setting**

Server

Port

Authorization Code

Device Name

[Connect](#)

**Milesight VPN Status**

Status Disconnected

Local IP --

Remote IP --

Duration -

LINOVISION VPN	
Item	Description
LINOVISION VPN Settings	
Server	Enter the IP address or domain name of LINOVISION VPN.
Port	Enter the HTTPS port number.
Authorization code	Enter the authorization code which generated by LINOVISION VPN.
Device Name	Enter the name of the device.
LINOVISIONVPN Status	
Status	Show the connection information about whether the router is connected to the LINOVISION VPN.
Local IP	Show the virtual IP of the router.
Remote IP	Show the virtual IP of the LINOVISION VPN.
Duration	Show the information on how long the router has been connected to the LINOVISION VPN.

### 5.3.8 Events

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

#### 5.3.8.1 Events

You can view alarm messages on this page.

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

### 5.3.8.2 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.

## | Events Settings

Enable

Phone Group List

Email Group List

Events	Record <input checked="" type="checkbox"/>	Email <input type="checkbox"/>	SMS <input type="checkbox"/>	SNMP <input type="checkbox"/>
		Email Group List	Phone Group List	
System Startup	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System Reboot	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System Time Update	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VPN Up	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
VPN Down	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Weak Signal	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Cellular Up	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Cellular Down	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Cellular Data Stats Clear	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Cellular Data Traffic is running out	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Cellular Data Traffic Overflow	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Router Starts Standby	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Wake Up Router	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

## Event Settings

Item	Description
Enable	Check to enable "Events Settings".
Phone Group List	Select phone group to receive SMS alarm.
Email Group List	Select email group to receive alarm.
Events	The name of alarm events.
Record	The relevant content of event alarm will be recorded on "Event" page if this option is checked.
Email	The relevant content of event alarm will be sent out via email if this option is checked.
Email Setting	Click and you will be redirected to the page "Email" to configure email group list.
SNMP	The relevant content of event alarm will be sent out via SNMP Trap if this option is checked.
SMS	The relevant content of event alarm will be sent out via SMS if this option is checked.
SMS Setting	Click and you will be redirected to the page of "Phone" to configure phone group list.

VPN Up	VPN is connected.
VPN Down	VPN is disconnected.
Weak Signal	The signal level of cellular is low.
Cellular Up	Cellular network is connected.
Cellular Down	Cellular network is disconnected.
Cellular Data Stats Clear	Zero out the data usage of the main SIM card.
Cellular Data Traffic is running out	The main SIM card is reaching the data usage limit.
Cellular Data Traffic Over Flow	The main SIM card has exceeded the data usage plan.
Enter Standby	The router enters standby mode.
Wake Up	The router wake up from standby mode to operation mode.

## Related Topics

[Email Setting](#)

[Events Application Example](#)

## 5.4 Industrial Interface

IOT-R41 router is capable of connecting with terminals through industrial interfaces so as to realize wireless communication between terminals and remote data center.

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

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

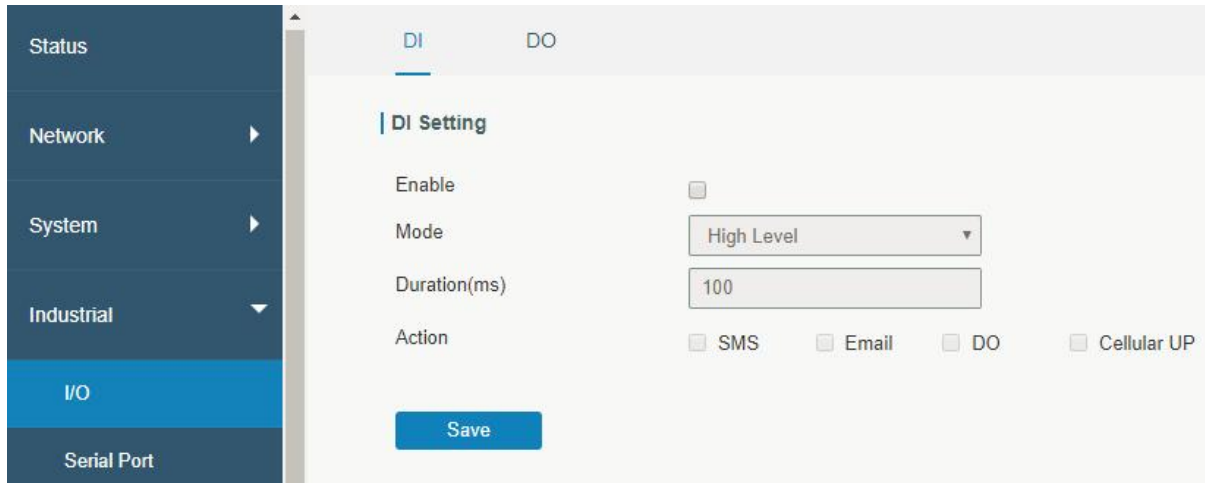
RS485 adopts half-duplex communication to achieve transmission of serial communication data with distance up to 120m.

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

### 5.4.1 I/O

#### 5.4.1.1 DI

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



DI	
Item	Description
Enable	Enable or disable DI.
Mode	Options are "High Level", "Low Level", and "Counter".
Duration (ms)	Set the duration of high/low level in digital input. Range: 1-10000.
Condition	Select from "Low->High", and "High-> Low".
Low->High	The counter value will increase by 1 if digital input's status changes from low level to high level.
High->Low	The counter value will increase by 1 if digital input's status changes from high level to low level.
Counter	The system will take actions accordingly when the counter value reach the preset one, and then reset the counter value to 0. Range: 1-100.
Action	Select the corresponding actions that the system will take when digital input mode meets the preset condition or duration.
SMS	Check to enable SMS alarm.
Phone Group	Set phone group to receive SMS alarm.
SMS Content	Set the content of SMS alarm.
Email	Check to enable Email alarm.
Email Group	Set phone group to receive email alarm.
Email Content	Set the content of email alarm.
DO	Control output status of DO.
Cellular UP	Trigger the router to switch from offline mode to cellular network mode.

## Related Topics

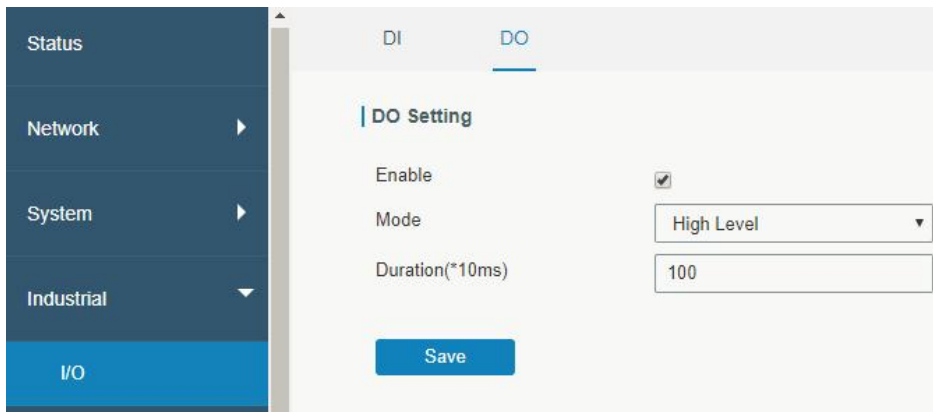
[DO Setting](#)

[Email Setting](#)

[Connect on Demand](#)

### 5.4.1.2 DO

This section describes how to configure digital output mode.



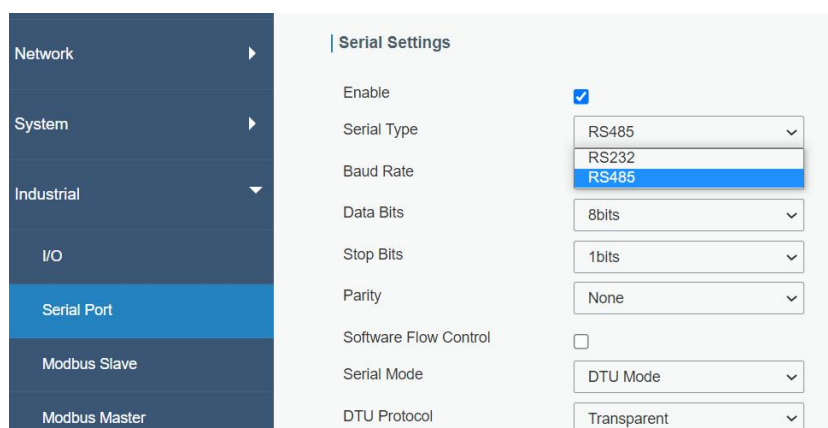
DO	
Item	Description
Enable	Enable or disable DO.
Mode	Select from "High Level", "Low Level", "Pulse" and "Custom" .
Duration (*10ms)	Set duration of high/low level on digital output. Range: 1-10000.
Initial Status	Select high level or low level as the initial status of the pulse.
Duration of High Level (*10ms)	Set the duration of pulse's high level. Range: 1-10000.
Duration of Low Level (*10ms)	Set the duration of pulse's low level. Range: 1-10000.
The Number of Pulse	Set the quantity of pulse. Range: 1-100.
Phone Group	Select phone group which will be used for I/O configuration. User can click the Phone Group and set phone number.

## Related Topics

[DI Setting](#)

### 5.4.2 Serial Port

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



Serial Settings		
Item	Description	Default
Enable	Enable or disable serial port function.	Disable
Serial Type	RS232 or RS485 is optional.	--
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	Select work mode of the serial port. Options are "DTU Mode", "Modbus Master", "Modbus Slave" and "GPS".	Disable
DTU Mode	In DTU mode, the serial port can establish communication with the remote server/client.	--
GPS	In GPS mode, go to "Industrial > GPS > GPS Serial Forwarding" to select corresponding Serial Type, then GPS data will be forwarded to this serial port.	--
Modbus Master	In Modbus Master mode, go to "Industrial > Modbus Master" to configure basic parameters and channels.	--
Modbus Slave	In Modbus Slave mode, go to "Industrial > Modbus Slave" to configure basic parameters.	--

Serial Mode: DTU Mode

DTU Protocol: Transparent

Protocol: TCP

Keepalive Interval: 75 s

Keepalive Retry Times: 9

Packet Size: 1024 Bytes

Serial Frame Interval: 100 ms

Reconnect Interval: 10 s

Specific Protocol:

Register String:

Destination IP Address

Server Address	Server Port	Status	Operation
			<a href="#">+</a>

DTU Mode		
Item	Description	Default



DTU Protocol	<p>Select from "None", "Transparent", "Modbus", "UDP server" and "TCP server".</p> <ul style="list-style-type: none"> <li>- Transparent: the router is used as TCP client/UDP and transmits data transparently.</li> <li>- TCP server: the router is used as TCP server and transmits data transparently.</li> <li>- UDP server: the router is used as UDP server and transmits data transparently.</li> <li>- Modbus: the router will be used as TCP server with modbus gateway function, which can achieve conversion between Modbus RTU and Modbus TCP.</li> </ul>	--
<b>TCP/UDP Server</b>		
Listening port	Set the router listening port. Range: 1-65535.	502
Keepalive Interval	After TCP connection is established, client will send heartbeat packet regularly by TCP to keep alive. The interval range is 1-3600 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	<p>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.</p> <p>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.</p>	100
<b>Item</b>	<b>Description</b>	<b>Default</b>
<b>Transparent</b>		
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	<p>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.</p> <p>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</p>	100

	frame interval.	
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.	--
<b>Modbus</b>		
Local Port	Set the router listening port. Range: 1-65535.	502
Maximum TCP Clients	Specify the maximum number of TCP clients allowed to connect the router which act as a TCP server.	32
Connection Timeout	If the TCP server does not receive any data from the slave device within the connection timeout period, the TCP connection will be broken.	60
Reading Interval	Set the interval for reading remote channels. When a read cycle ends, the new read cycle begins until this interval expires. If it is set to 0, the device will restart the new read cycle after all channels have been read.	100
Response Timeout	Set the maximum response time that the router waits for the 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.	3000
Maximum Retries	Set the maximum retry times after it fails to read.	3

## Related Configuration Example

[DTU Application Example](#)

### 5.4.3 Modbus Slave

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

#### 5.4.3.1 Modbus TCP

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

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

### 5.4.3.2 Modbus RTU

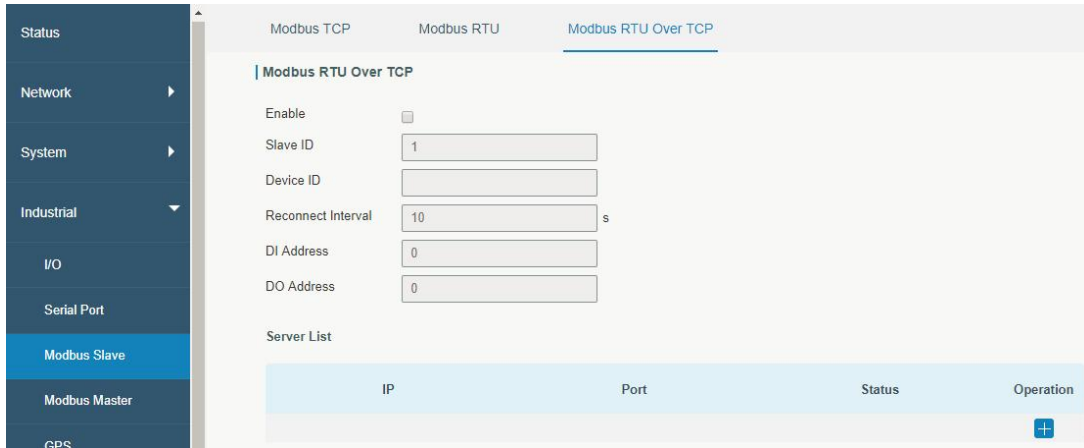
You can define the address of the DI and DO ports so as to poll DI's status and control DO's status via Modbus RTU protocol.

Modbus RTU		
Item	Description	Default
Enable	Enable/disable Modbus RTU.	Disable
Serial Port	Select the corresponding serial port.	serial

Slave ID	Set slave ID is used for distinguishing different devices on the same link.	1
DI Address	Define the address of DI, range: 0-255.	0
DO Address	Define the address of DO, range: 0, 2-255.	0

### 5.4.3.3 Modbus RTU Over TCP

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



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

### 5.4.4 Modbus Master

IOT-R41 router can be set as Modbus Master to poll the remote Modbus Slave and send alarm according to the response.

#### 5.4.4.1 Modbus Master

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

Modbus Master		
Item	Description	Default
Enable	Enable/disable Modbus master.	--
Read Interval/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
Channel Name	Select a readable channel form the channel list.	--
Result	The value read from the selected channel.	--

#### 5.4.4.2 Channel

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

Modbus Master Channel

Channel Setting

Channel Setting

Name	Slave ID	Address	Number	Type	Link	IP Address	Port	Sign	Decimal Place	Operation
	1	0	1	Holding Register	TCP			<input type="checkbox"/>	0	<input type="button" value="X"/>
<input type="button" value="+"/>										

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.
Decimal Place	Used to indicate a dot in the read into the position of the channel. For example: read the channel value is 1234, and a Decimal Place is equal to 2, then the actual value is 12.34.

Alarm Setting

Name	tunnel1
Condition	GE(>)
Max. Threshold	0
Alarm	<input checked="" type="checkbox"/> SMS <input checked="" type="checkbox"/> Email
Phone Group	
Email Group	
Normal Content	Note: \$YEAR/\$MON/\$DAY \$TIME, get NORMAL data \$VALUE from address \$ADDRESS of channel \$NAME. (Abnormal scope is
Abnormal Content	Note: \$YEAR/\$MON/\$DAY \$TIME, get ABERRANT data \$VALUE from address \$ADDRESS of channel \$NAME. (Abnormal scope is
Continuous Alarm	<input type="checkbox"/>

Alarm Setting	
Item	Description

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

TCP Forwarding

Name	IP	Port	Operation
All			
			

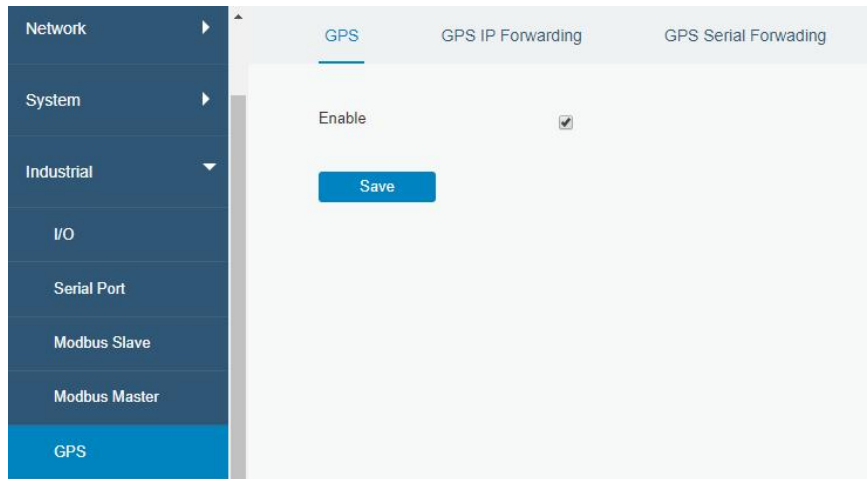
TCP Forwarding	
Item	Description
Name	The name of Modbus Master's channel.
IP	The IP address of the server which the packets are forwarded to.
Port	The port of the server's which the packets are forwarded to.

## 5.4.5 GPS

This section give you a detailed introduction to GPS settings, including GPS IP forwarding and GPS serial forwarding.

### 5.4.5.1 GPS

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



### 5.4.5.2 GPS IP Forwarding

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

The screenshot displays the 'GPS IP Forwarding' configuration page. It features three tabs: GPS, GPS IP Forwarding (selected), and GPS Serial Forwarding. The configuration includes:
 

- Enable:** Checked checkbox.
- Type:** Dropdown menu set to 'Client'.
- Protocol:** Dropdown menu set to 'TCP Protocol'.
- Keepalive Interval:** Input field with '75' and 's' unit.
- Keepalive Retry:** Input field with '9' and 'times' unit.
- Reconnect Interval:** Input field with '10' and 's' unit.
- Report Interval:** Input field with '30' and 's' unit.
- Include RMC, GSA, GGA, GSV:** Each has a checked checkbox.
- Message Prefix:** Empty input field.
- Message Suffix:** Empty input field.

Destination IP Address

Server Address	Server Port	Status	Operation
			+

GPS IP Forwarding		
Item	Description	Default
Enable	Forward the GPS data to the client or server.	Disable
Type	Select connection type of the router. The options are "Client" and "Server".	Client



Protocol	Select protocol of data transmission. The options are "TCP" and "UDP".	TCP
Keepalive Interval	After it's connected with server/client, the router will send heartbeat packet regularly to the server/client to keep alive. The interval range is 1-3600, in seconds.	75
Keepalive Retry	When TCP heartbeat times out, the router will resend heartbeat. After it reaches the preset retry times, router will reconnect to TCP server. The range is 1-16.	9
Local Port	Set the router listening port. Range: 1-65535.	
Reconnect Interval	After connection failure, router will reconnect to the server at the preset interval, in seconds. The range is 10-60.	10
Report Interval	Router will send GPS data to the server/client at the preset interval, in seconds. The range is 1-60.	30
Include RMC	Whether include RMC in GPS data.	--
Include GSA	Whether include GSA in GPS data.	--
Include GGA	Whether include GGA in GPS data.	--
Include GSV	Whether include GSV in GPS data.	--
Message Prefix	Add a prefix to the GPS data.	Null
Message Suffix	Add a suffix to the GPS data.	Null
<b>Destination IP Address</b>		
Server Address	Fill in the server address to receive GPS data (IP/domain name).	--
Server Port	Fill in the port to receive GPS data. Range: 1-65535.	--
Status	Show the connection status between the router and the server.	--

### 5.4.5.3 GPS Serial Forwarding

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

The screenshot shows the configuration interface for GPS Serial Forwarding. It includes the following settings:

- Enable:**
- Serial Type:** Serial
- Trap Interval:** 30
- Include RMC:**
- Include GSA:**
- Include GGA:**
- Include GSV:**

A **Save** button is located at the bottom of the configuration area.

GPS Serial Forwarding		
Item	Description	Default
Enable	Forward the GPS data to the preset serial port.	Disable
Serial Type	Select the serial port to receive GPS data.	Serial
Report Interval	Router will forward the GPS data to the serial port at the preset interval, in seconds. The range is 1-60.	30
Include RMC	Whether include RMC in GPS data.	--
Include GSA	Whether include GSA in GPS data.	--
Include GGA	Whether include GGA in GPS data.	--
Include GSV	Whether include GSV in GPS data.	--

## 5.5 Maintenance

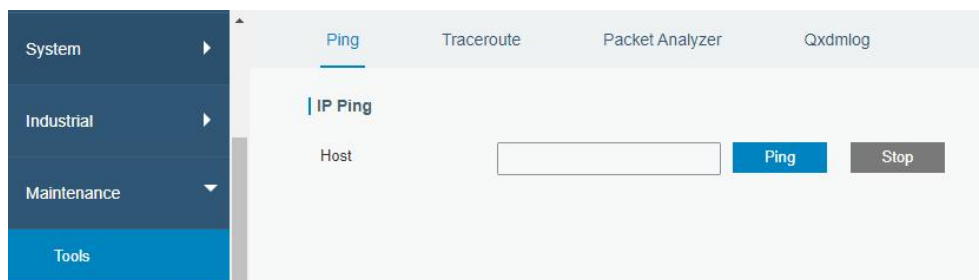
This section describes system maintenance tools and management.

### 5.5.1 Tools

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

#### 5.5.1.1 Ping

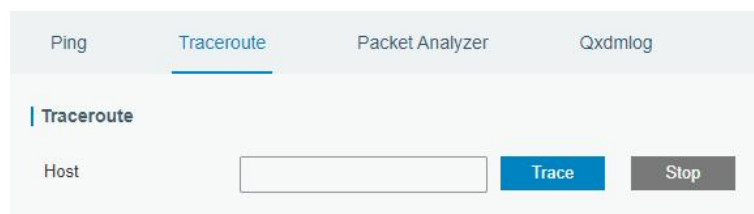
Ping tool is engineered to ping outer network.



PING	
Item	Description
Host	Ping outer network from the router.

#### 5.5.1.2 Traceroute

Traceroute tool is used for troubleshooting network routing failures.



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

### 5.5.1.3 Packet Analyzer

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

The screenshot shows a web interface with four tabs: Ping, Traceroute, Packet Analyzer, and Qxdmlog. The Packet Analyzer tab is active. Below the tabs, there is a section titled 'Packet Analyzer' with the following fields: 'Ethernet Interface' (a dropdown menu showing 'Any'), 'IP Address' (a text input field), 'Port' (a text input field), and 'Advanced' (a checkbox). At the bottom of this section are three buttons: 'Start' (blue), 'Stop' (grey), and 'Download' (grey).

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

### 5.5.1.4 Qxdmlog

This section allow collecting diagnostic logs via QXDM tool.

The screenshot shows a web interface with four tabs: Ping, Traceroute, Packet Analyzer, and Qxdmlog. The Qxdmlog tab is active. Below the tabs, there are three buttons: 'Start' (blue), 'Stop' (grey), and 'Download' (grey).

## 5.5.2 Debugger

### 5.5.2.1 Cellular Debugger

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

Cellular Debugger
Firewall Debugger

**Cellular Debugger**

Command  Send

View Recent Logs (lines)  ▼

Result

```

2023-01-16 19:04:34: [SEQ4,ID8]<<< OK
2023-01-16 19:04:36: [SEQ33,ID81]>>> AT+QCFG="risignatype","physical"
2023-01-16 19:04:36: [SEQ33,ID81]<<< OK
2023-01-16 19:04:37: [SEQ34,ID82]>>> AT+QCFG="urc/ri/other","off"
2023-01-16 19:04:37: [SEQ34,ID82]<<< OK
2023-01-16 19:04:40: [SEQ38,ID63]>>> AT+QMBNCFG="Autosel",1
2023-01-16 19:04:40: [SEQ38,ID63]<<< OK
2023-01-16 19:04:40: [SEQ39,ID13]>>> AT+CPIN?
2023-01-16 19:04:40: [SEQ39,ID13]<<< +CME ERROR: SIM not inserted
2023-01-16 19:04:46: [SEQ1,ID48]>>> AT+CFUN=0
2023-01-16 19:04:47: [SEQ1,ID48]<<< OK
2023-01-16 19:04:52: [SEQ2,ID47]>>> AT+CFUN=1
2023-01-16 19:04:55: [SEQ2,ID47]<<< OK
2023-01-16 19:04:55: [SEQ2,ID47]<<< +CPIN: NOT INSERTED
2023-01-16 19:04:58: [SEQ42,ID13]>>> AT+CPIN?
2023-01-16 19:04:58: [SEQ42,ID13]<<< +CME ERROR: SIM not inserted
2023-01-16 19:05:04: [SEQ1,ID48]>>> AT+CFUN=0
2023-01-16 19:05:04: [SEQ1,ID48]<<< OK
                
```

Clear Log
Download

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

### 5.5.2.2 Firewall Debugger

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

The screenshot shows a web interface for a 'Firewall Debugger'. At the top, there are two tabs: 'Cellular Debugger' and 'Firewall Debugger', with the latter being selected. Below the tabs, the title 'Firewall Debugger' is displayed. There is a 'Command' input field containing the text 'Eg: -t nat -nvL INPUT' and a blue 'Send' button to its right. Below the command field is a large, empty rectangular area labeled 'Result'. At the bottom of the interface, there are two buttons: 'Clear Log' and 'Download'.

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

### 5.5.3 Log

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

#### 5.5.3.1 System Log

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

System Log    Log Download    Log Settings

**Log**

View recent(lines)

```

Mon Jan 16 19:07:40 2023 user.debug httpd[2922]: ==call yruo_log.get
Mon Jan 16 19:07:40 2023 daemon.debug vtysh_ubus[1794]: ubus_lib.c:428 call command 'end'
Mon Jan 16 19:07:40 2023 user.debug httpd[2922]: finish yruo_log.get
Mon Jan 16 19:07:41 2023 daemon.debug zebra[1460]: sql sqldb.c 2306:update smscache set sending='0'
Mon Jan 16 19:07:42 2023 daemon.info zebra[1460]: libgsm/gsm.c:1342 cellular_start: power control to restart usb
Mon Jan 16 19:07:42 2023 daemon.debug zebra[1460]: power off GSM module.
Mon Jan 16 19:07:42 2023 kern.info kernel: [26778.876800] usb 1-1: USB disconnect, device number 22
Mon Jan 16 19:07:42 2023 kern.info kernel: [26778.877926] option1 ttyUSB0: GSM modem (1-port) converter now disconnected from ttyUSB0
Mon Jan 16 19:07:42 2023 kern.info kernel: [26778.878070] option 1-1:1.0: device disconnected
Mon Jan 16 19:07:42 2023 kern.info kernel: [26778.879172] option1 ttyUSB1: GSM modem (1-port) converter now disconnected from ttyUSB1
Mon Jan 16 19:07:42 2023 kern.info kernel: [26778.879296] option 1-1:1.1: device disconnected
Mon Jan 16 19:07:42 2023 kern.info kernel: [26778.880366] option1 ttyUSB3: GSM modem (1-port) converter now disconnected from ttyUSB3
Mon Jan 16 19:07:42 2023 kern.info kernel: [26778.880481] option 1-1:1.2: device disconnected
Mon Jan 16 19:07:42 2023 kern.info kernel: [26778.881587] option1 ttyUSB4: GSM modem (1-port) converter now disconnected from ttyUSB4
Mon Jan 16 19:07:42 2023 kern.info kernel: [26778.881713] option 1-1:1.3: device disconnected
Mon Jan 16 19:07:42 2023 kern.info kernel: [26778.882443] qmi_wwan 1-1:1.4 cellular0: unregister 'qmi_wwan' usb-ci_hdrc.1-1,

```

[Clear Log](#)

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

### 5.5.3.2 Log Download

This section describes how to download log files.

System Log    **Log Download**    Log Settings

**Download**

[Download All](#)

File Name	File Size/KB	Creation Time	Operation
vpn.log	2	2023/01/16 11:42:16	
system.log	79	2023/01/16 19:08:25	
httpd.log	901	2023/01/16 19:08:25	
firewall.log	0	2023/01/13 14:54:07	
cellular.log	868	2023/01/16 19:08:19	

Log Download	
Item	Description
Download All	Download all log files.

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

### 5.5.3.3 Log Settings

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

Log Settings	
Item	Description
<b>Remote Log Server</b>	
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.
<b>Local Log File</b>	
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.

### 5.5.4 Upgrade

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

the firmware upgrade.

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

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

## Related Configuration Example

[Firmware Upgrade](#)

### 5.5.5 Backup and Restore

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

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



Reset	Click "Reset" button to reset factory default settings. Router will restart after reset process is done.
-------	--

## Related Configuration Example

[Restore Factory Defaults](#)

### 5.5.6 Reboot

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

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

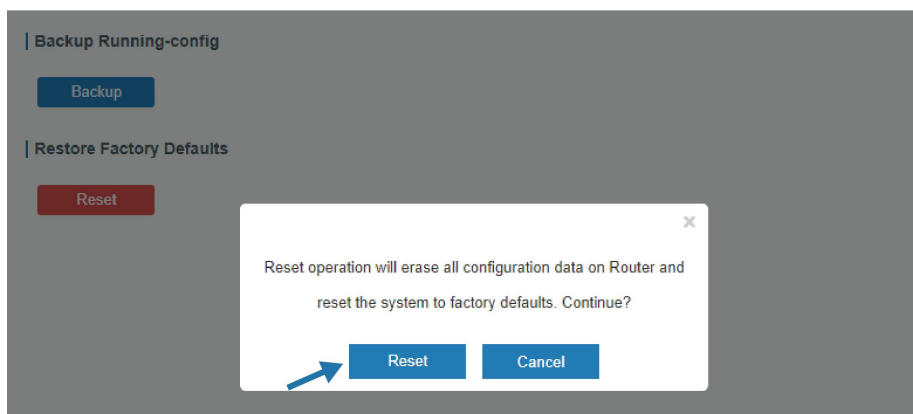
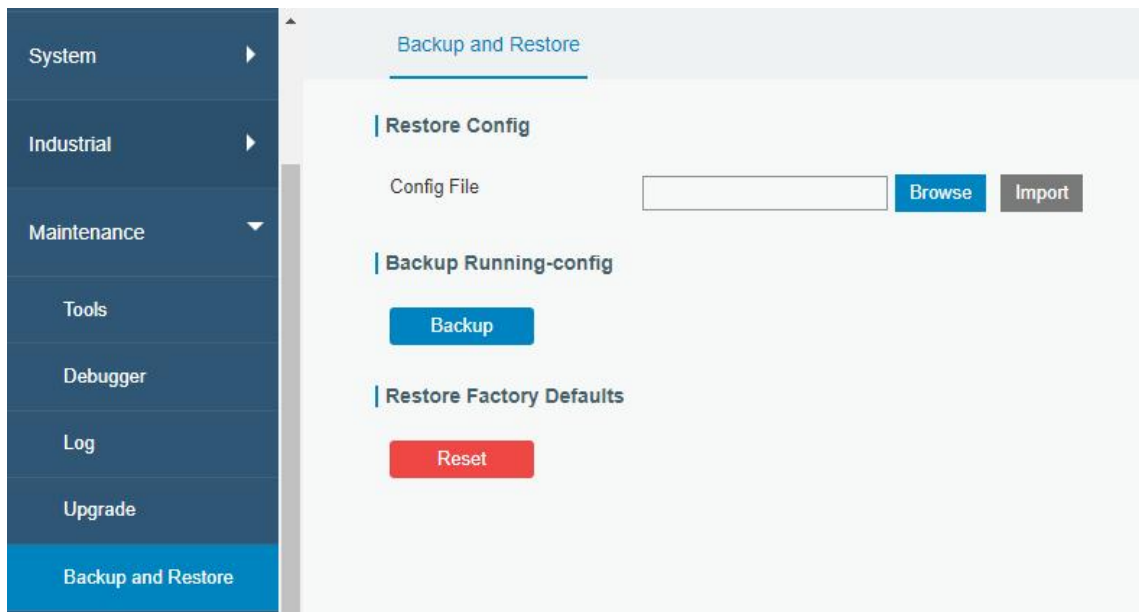
## Chapter 6 Application Examples

### 6.1 Restore Factory Defaults

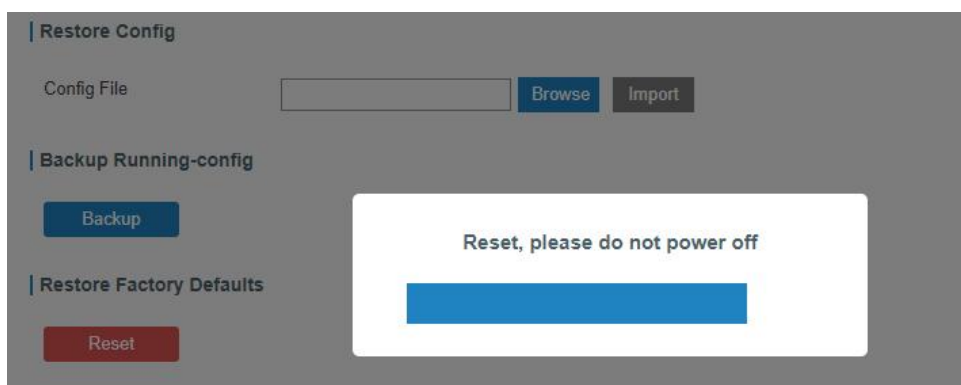
#### 6.1.1 Via Web Interface

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

### Related Topic

[Restore Factory Defaults](#)

## 6.1.2 Via Hardware

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

## 6.2 Firmware Upgrade

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

1. Go to **Maintenance > Upgrade**.
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.

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

The screenshot shows the router's web interface. On the left is a dark blue sidebar with menu items: Status, Network, System, Industrial, Maintenance, Tools, Debugger, Log, and Upgrade (highlighted in light blue). The main content area is light gray and titled 'Upgrade'. It contains the following fields and controls:

- Upgrade** (sub-header)
- Firmware Version**: 41.0.0.2-a3-1
- Reset Configuration to Factory Default**:
- Upgrade Firmware**:  **Browse** **Upgrade**

### Related Topic

[Upgrade](#)

## 6.3 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)
Router system start up.	Plug the power supply of the router.
Router system time update.	Set up system time manually.

## 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.

Events Events Settings

**Events Settings**

Enable

Phone Group List

Email Group List

Events	Record	Email Email Setting	SMS SMS Setting	SNMP
System Startup	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System Reboot	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
System Time Update	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

3. Configure the corresponding parameters including email sending settings and email groups as below. Click **Save** and **Apply** button to make the changes take effect.

General System Time Email

**SMTP Client Settings**

Enable

Email Address

Password

SMTP Server Address

Port

Encryption

**Test**

Email List		
Email Address	Description	Operation
iot.contact@milesight.com	support	<input type="checkbox"/>
		<input type="checkbox"/>

Email Group List			
Group ID	Description	Email Address	Operation
1	support	iot.contact@milesight.com	<input type="checkbox"/> <input type="checkbox"/>
			<input type="checkbox"/>

- 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.

Events		Events Settings	
<input type="button" value="Mark as Read"/> <input type="button" value="Delete"/> <input type="button" value="Mark All as Read"/> <input type="button" value="Delete All Alarms"/>			
Status	Type	Time	Message
<input type="checkbox"/>	Unread	System Time Update	2019-05-15 09:39:08
<input type="checkbox"/>	Unread	System Startup	2019-05-09 11:48:25

< 1 > 10 ▾ Go to:

## Related Topics

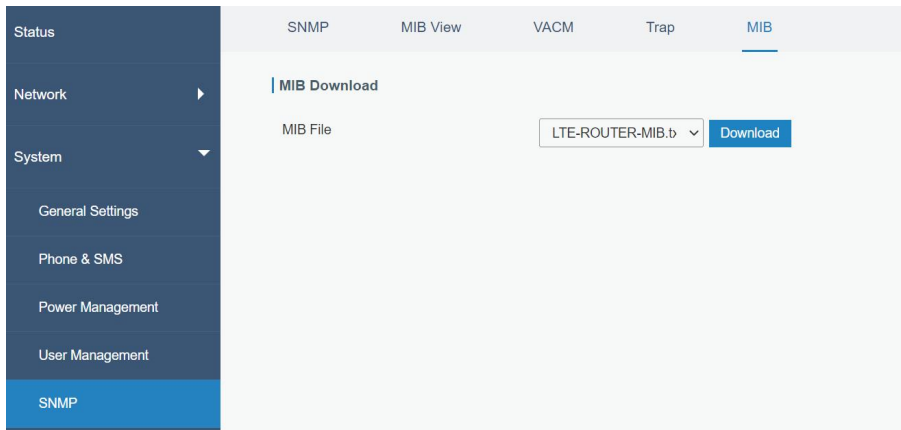
[Events](#)

[Email Setting](#)

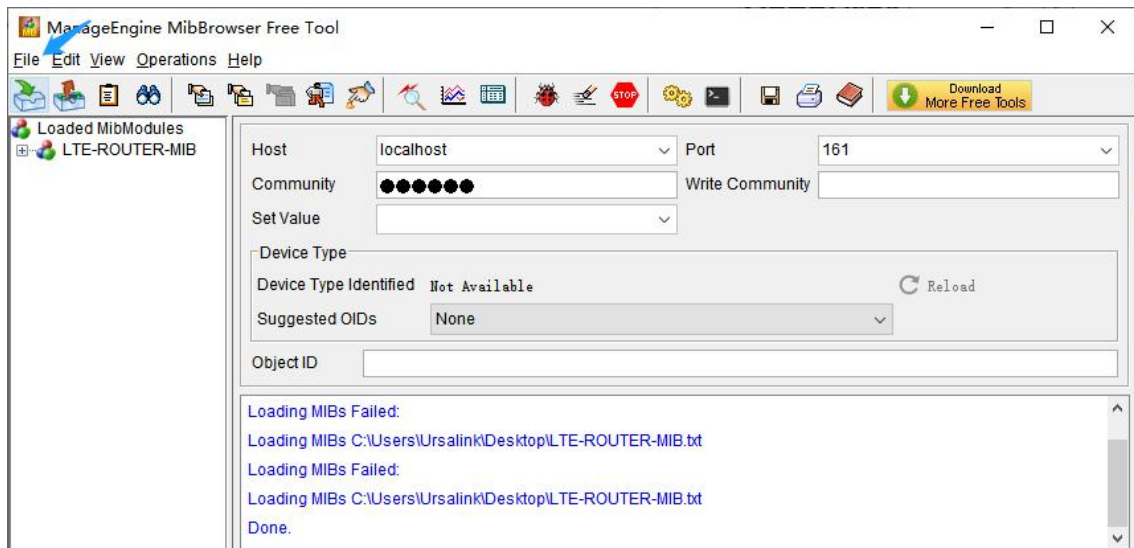
## 6.4 SNMP Application Example

Before you configure SNMP parameters, please download the relevant **MIB** file from the IOT-R41'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.

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




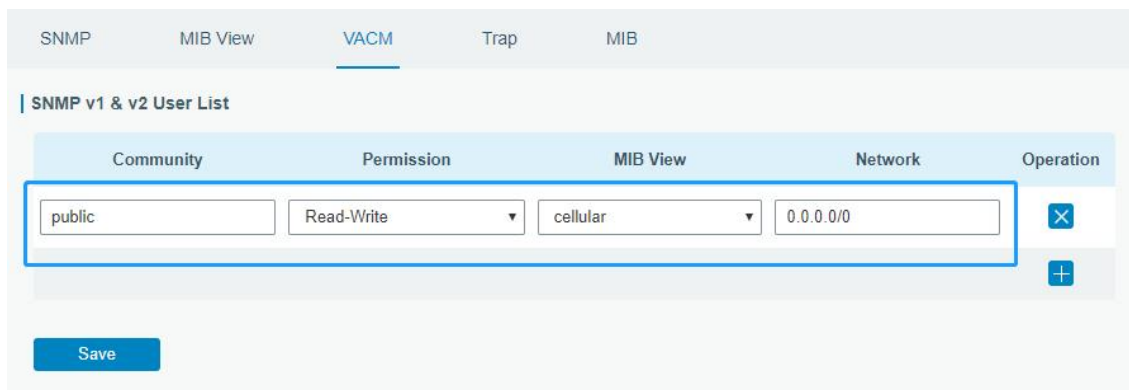
2. Start “ManageEngine MibBrowser Free Tool” on the PC. Click **File > Load MIB** on the menu bar. Then select “LTE-ROUTER-MIB.txt” file from PC and upload it to the software.



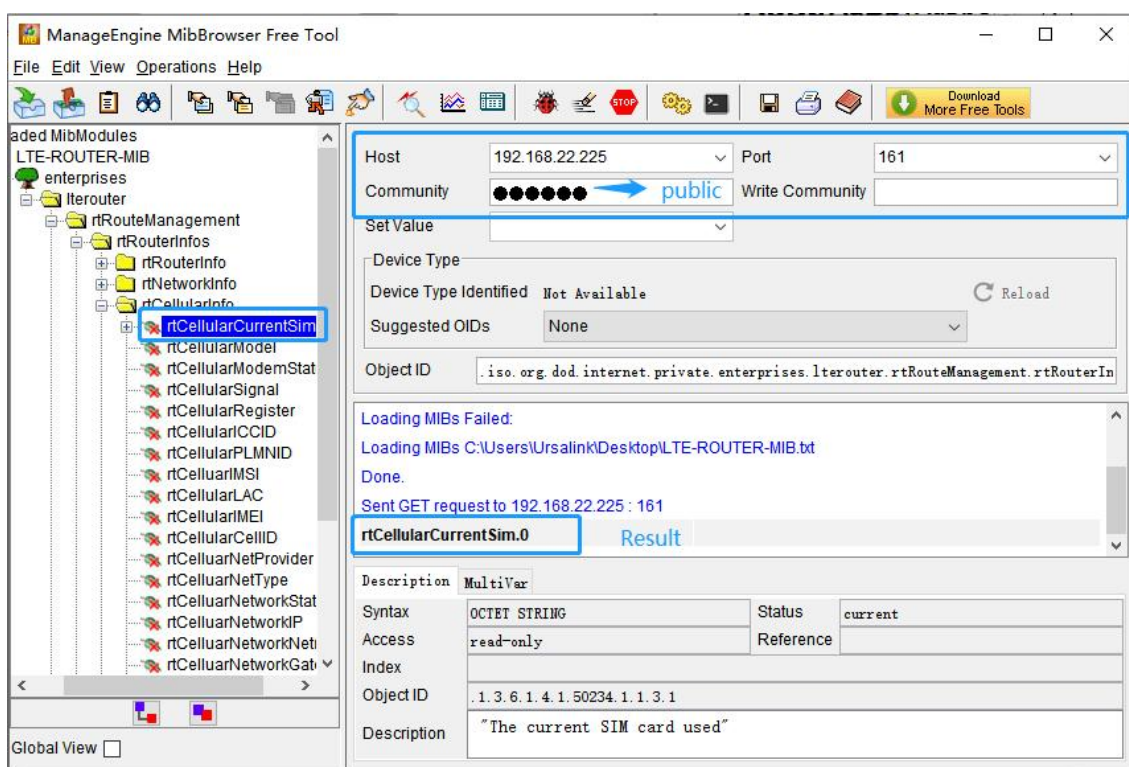
Click the + button beside “LTE-ROUTER-MIB”, which is under the “Loaded MibModules” menu, and find “usCellularinfo”. And then you will see the OID of cellular info is “.1.3.6.1.4.1.50234”, which will be filled in the MIB View settings.



- 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.



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



## Related Topic

[SNMP](#)

## 6.5 Cellular Connection

### Example

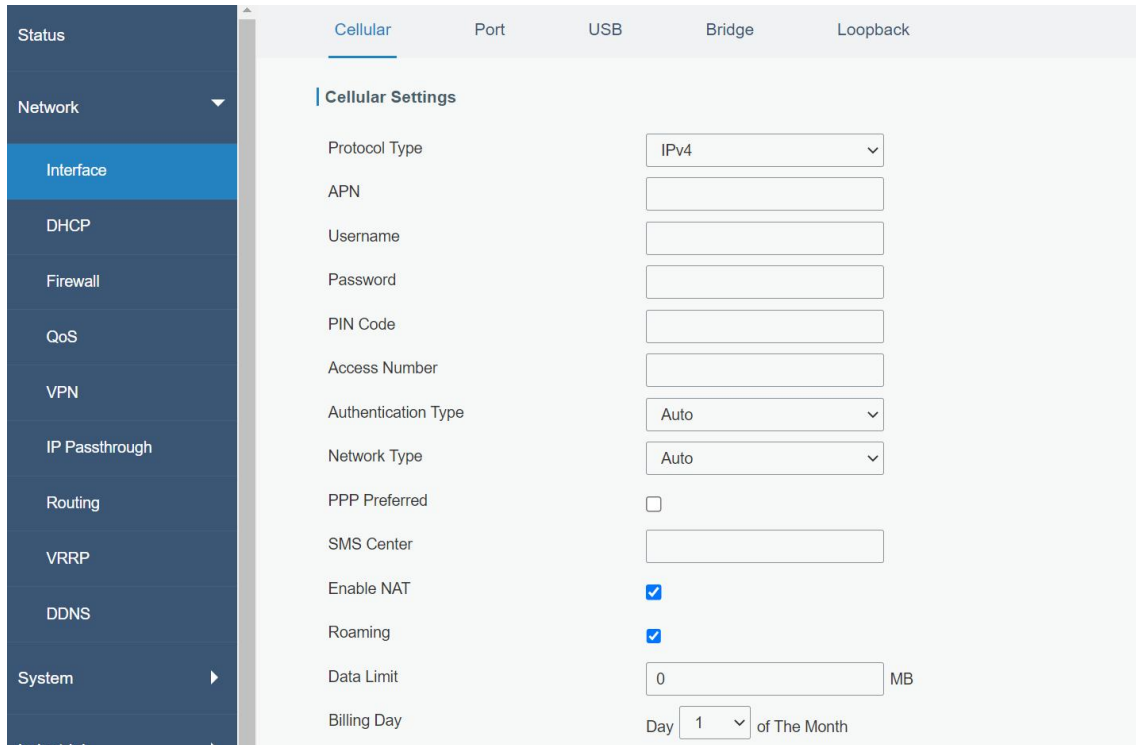
We are about to take an example of inserting a SIM card of the IOT-R41 and configuring the router to get



Internet access through cellular.

### Configuration Steps

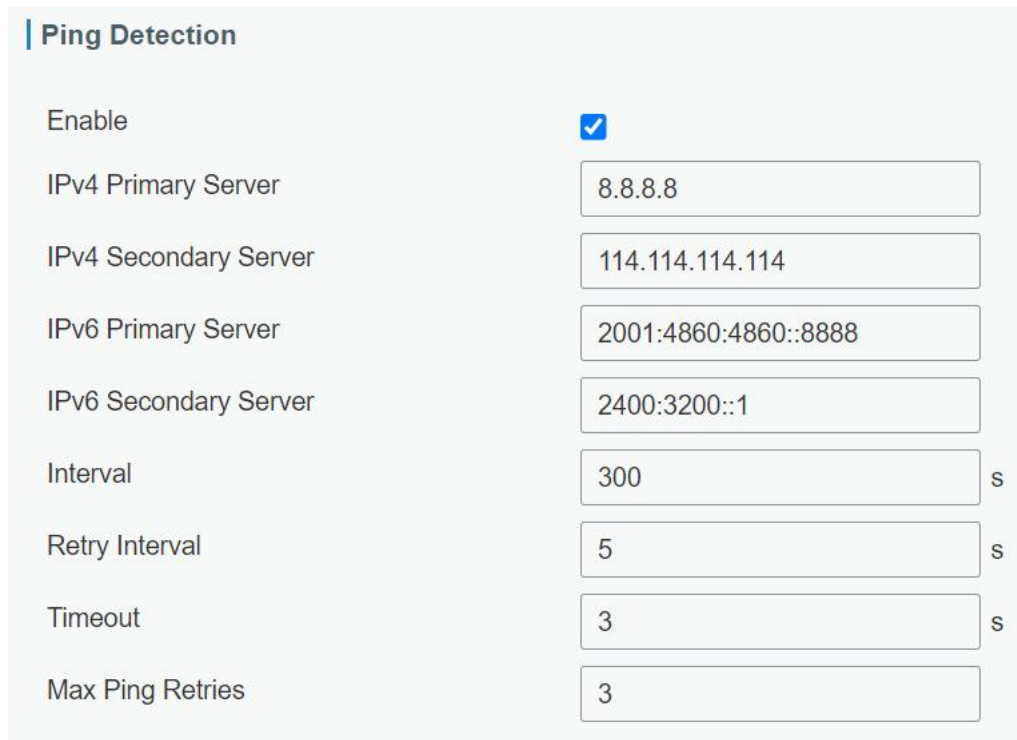
1. Go to **Network > Interface > Cellular > Cellular Setting** and configure the cellular info.



Cellular	Port	USB	Bridge	Loopback
<b>Cellular Settings</b>				
Protocol Type	IPv4			
APN				
Username				
Password				
PIN Code				
Access Number				
Authentication Type	Auto			
Network Type	Auto			
PPP Preferred	<input type="checkbox"/>			
SMS Center				
Enable NAT	<input checked="" type="checkbox"/>			
Roaming	<input checked="" type="checkbox"/>			
Data Limit	0 MB			
Billing Day	Day 1 of The Month			

Click **Save** and **Apply** for configuration to take effect.

2. Click **Network > Interface > Cellular > Ping Detection** to configure ping detection information.



Ping Detection	
Enable	<input checked="" type="checkbox"/>
IPv4 Primary Server	8.8.8.8
IPv4 Secondary Server	114.114.114.114
IPv6 Primary Server	2001:4860:4860::8888
IPv6 Secondary Server	2400:3200::1
Interval	300 s
Retry Interval	5 s
Timeout	3 s
Max Ping Retries	3

3. 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', SIM card

has dialed up successfully.

Overview	Cellular	Network	VPN	Routing	Host List	GPS
<b>Modem</b>		<b>Network</b>				
Model	EG95	Status	Disconnected			
Version	EG95EXGAR08A03M1G	IPv4 Address	0.0.0.0/0			
Signal Level	0asu (-113dBm)	IPv4 Gateway	0.0.0.0			
Register Status	Not registered	IPv4 DNS	0.0.0.0			
IMEI	864004046848336	IPv6 Address	fe80::e816:f9ff:fea3:377e/64			
IMSI	-	IPv6 Gateway	::			
ICCID	-	IPv6 DNS	::			
ISP	-	Connection Duration	0 days, 00:00:00			
Network Type	-	<b>Data Usage Monthly</b>				
PLMN ID	-	RX	0.0 MiB			
LAC	0	TX	0.0 MiB			
Cell ID	0	ALL	0.0 MiB			

4. 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 IOT-R41 router.

## Related Topic

[Cellular Setting](#)

[Cellular Status](#)

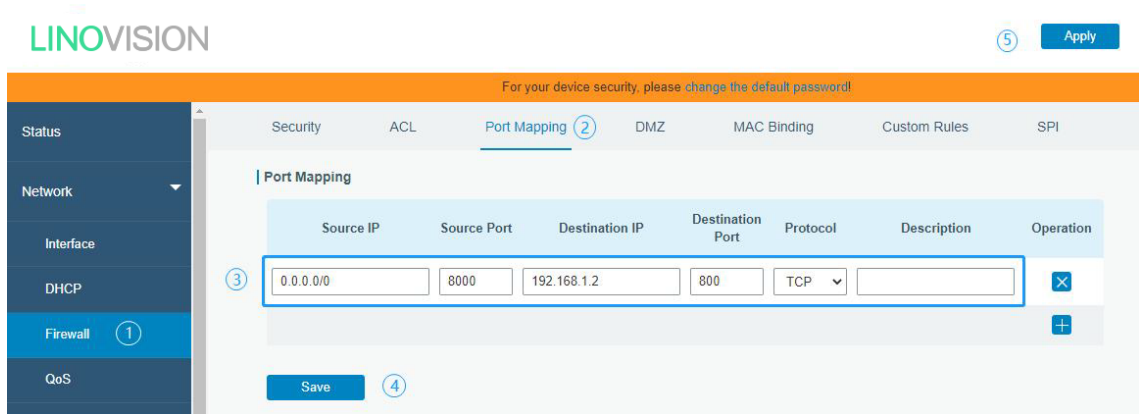
## 6.6 NAT Application Example

### Example

An IOT-R41 router can access Internet via cellular. LAN 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](#)

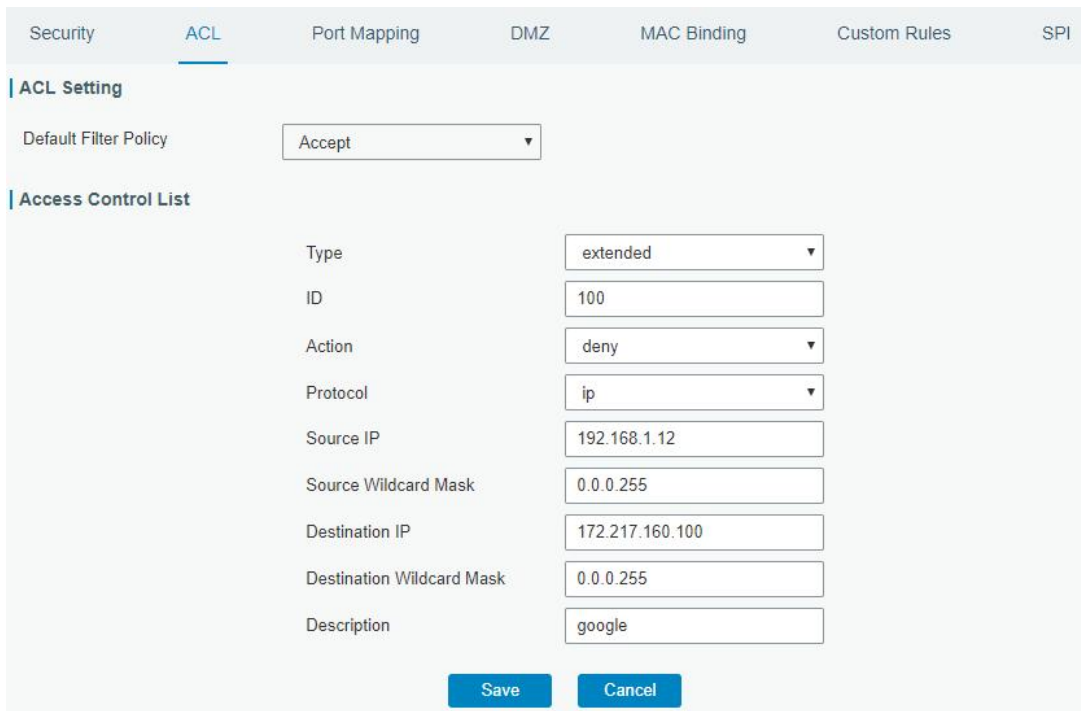
## 6.7 Access Control Application Example

### Application Example

LAN port of the IOT-R41 is set with IP 192.168.1.0/24. Then configure the router to deny accessing to Google IP 172.217.160.100 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.

Security **ACL** Port Mapping DMZ MAC Binding Custom Rules SPI

**ACL Setting**

Default Filter Policy

**Access Control List**

ID	Action	Protocol	Source IP	Destination IP	More Detail	Description	Operation
100	deny	ip	192.168.1.12/0.0.0.255	172.217.160.100/0.0.255		google	<input type="button" value="X"/> <input type="button" value="+"/>

**Interface List**

Interface	In ACL	Out ACL	Operation
<input type="text" value="Bridge0"/>	<input type="text" value="100"/>	<input type="text"/>	<input type="button" value="X"/> <input type="button" value="+"/>

## Related Topic

[ACL](#)

## 6.8 QoS Application Example

### Example

Configure the IOT-R41 router to distribute local preference to different FTP download channels. The total download bandwidth is 75000 kbps.

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

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

### Configuration Steps

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

**Download Bandwidth**

Enable

Default Category

Download Bandwidth  kbits/s

Capacity

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

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

Service Category				
Name	Percent(%)	Max BW(kbps)	Min BW(kbps)	Operation
1	40	30000	25000	<input type="button" value="X"/>
2	60	45000	40000	<input type="button" value="X"/>
				<input type="button" value="+"/>

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

Service Category Rules							
Name	Source IP	Source Port	Destination IP	Destination Port	Protocol	Service Category	Operation
ftp1	110.21.24.98	21			ANY	1	<input type="button" value="X"/>
ftp2	110.32.91.44	21			ANY	2	<input type="button" value="X"/>
							<input type="button" value="+"/>

**Note:**

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

Click “Save” and “Apply” button.

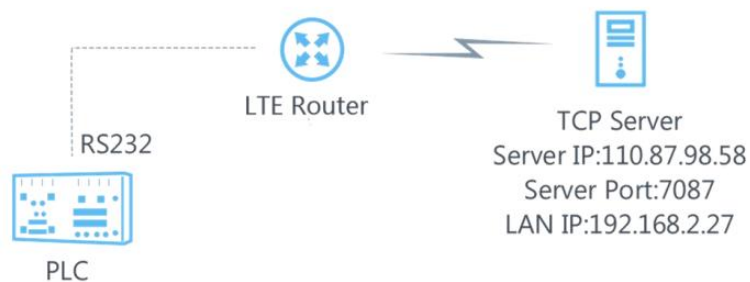
**Related Topic**

[QoS Setting](#)

**6.9 DTU Application Example**

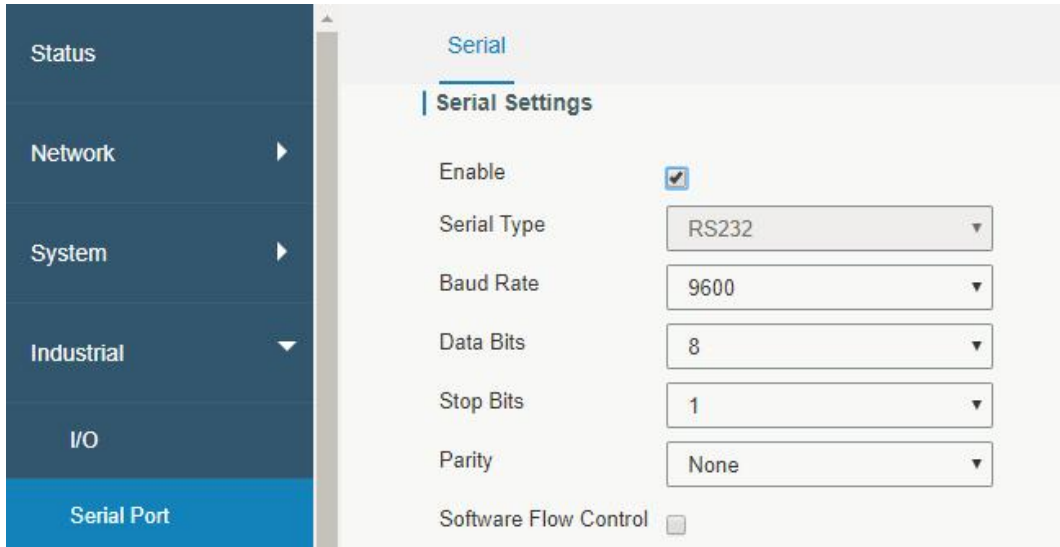
**Example**

PLC is connected with the IOT-R41 via RS232. Then enable DTU function of the IOT-R41 to make a remote TCP server communicate with PLC. Refer to the following topological graph.

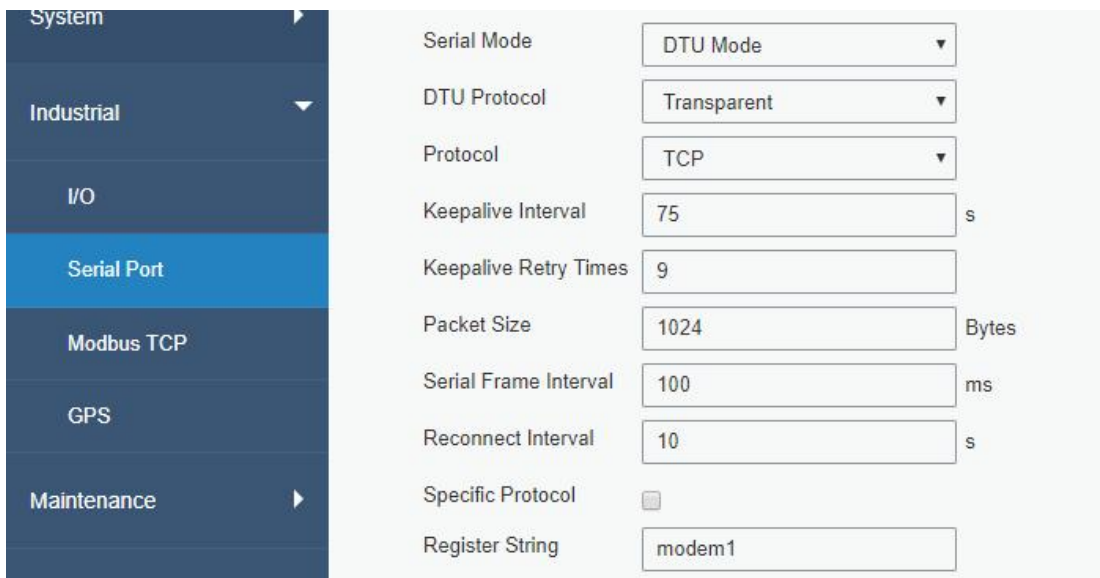


**Configuration Steps**

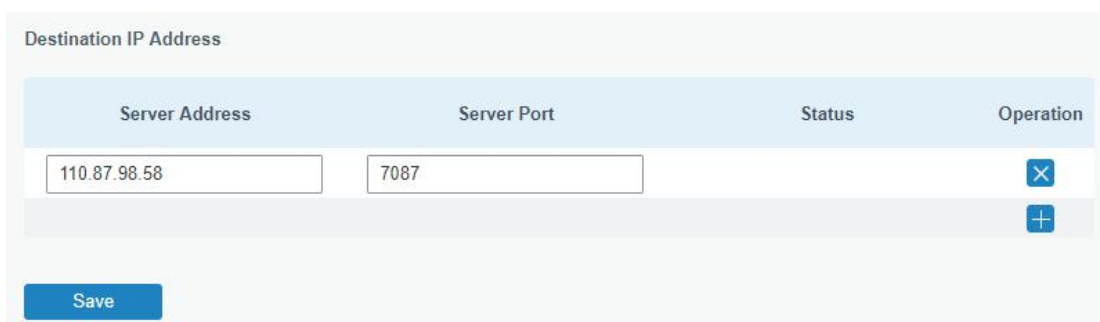
1. Go to **Industrial > Serial Port > Serial** and configure serial port parameters. The serial port parameter shall be kept in consistency with those of PLC, as shown in figure below.



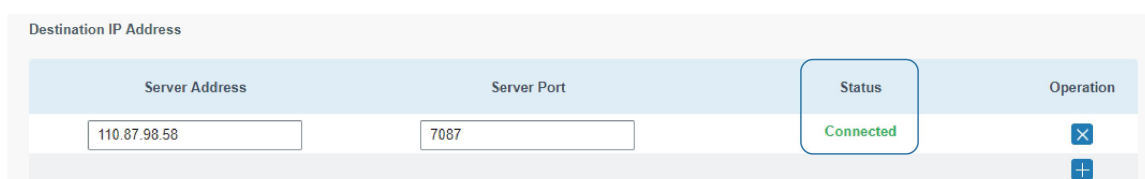
2. Configure Serial Mode as **DTU Mode**. The IOT-R41 is connected as client in “Transparent” protocol.



3. Configure TCP server IP and port.



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

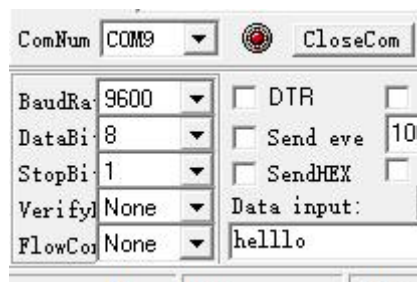


5. Start TCP server on PC.

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

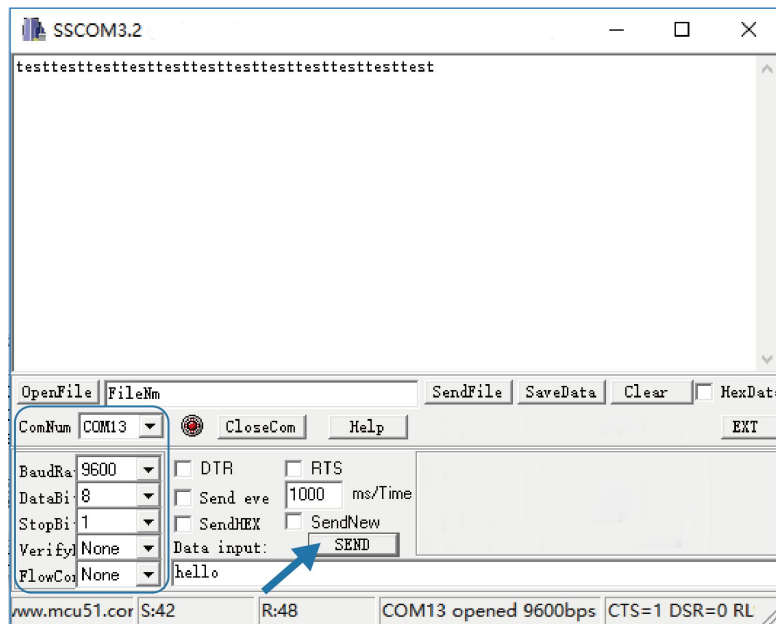


6. Connect the IOT-R41 to PC via RS232 for PLC simulation. Then start "sscom" software on the PC to test communication through serial port.

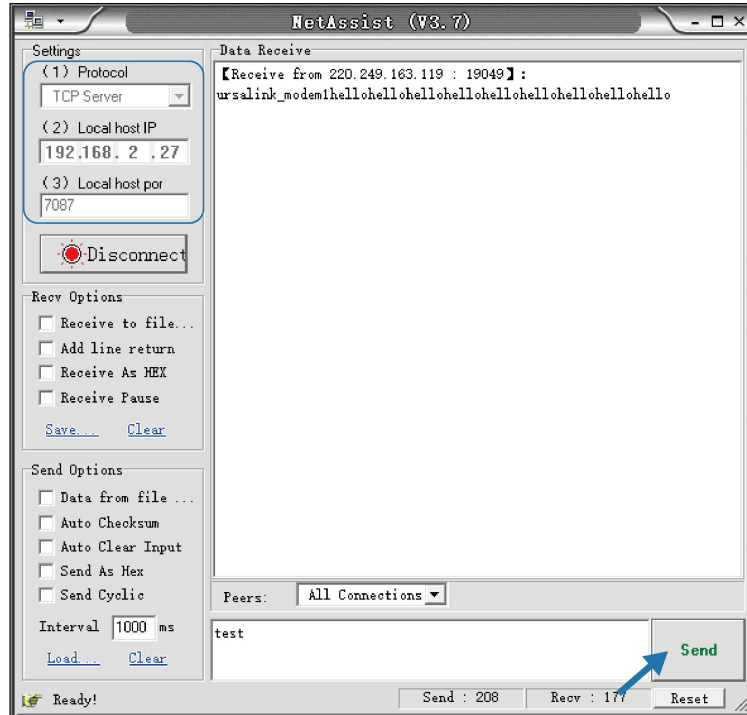


7. After connection is established between the IOT-R41 and the TCP server, you can send data between sscom and Netassist.

**PC side**



**TCP server side**



8. After serial communication test is done, you can connect PLC to RS232 port of the IOT-R41 for test.

## Related Topic

[Serial Port](#)

## 6.10 PPTP Application Example

### Example



Configure the IOT-R41 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.



DMVPN	IPsec	GRE	L2TP	<u>PPTP</u>
Certifications				
<b>PPTP Settings</b>				
— PPTP_1				
Enable	<input checked="" type="checkbox"/>			
Remote IP Address	<input type="text" value="110.87.98.58"/>			
Username	<input type="text" value="pptpserver"/>			
Password	<input type="password" value="*****"/>			
Authentication	<input type="text" value="Auto"/>			
Global Traffic Forwarding	<input type="checkbox"/>			
Remote Subnet	<input type="text"/>			
Remote Subnet Mask	<input type="text"/>			
Advanced Settings	<input type="checkbox"/>			

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.

Remote Subnet	<input type="text" value="192.168.3.0"/>
Remote Subnet Mask	<input type="text" value="255.255.255.0"/>

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

DMVPN	IPsec	GRE	L2TP	<u>PPTP</u>
Show Advanced	<input checked="" type="checkbox"/>			
Local IP Address	<input type="text"/>			
Peer IP Address	<input type="text"/>			
Enable NAT	<input checked="" type="checkbox"/>			
Enable MPPE	<input type="checkbox"/>			
Address/Control Compression	<input type="checkbox"/>			
Protocol Field Compression	<input type="checkbox"/>			
Asyncmap Value	<input type="text" value="ffffff"/>			
MRU	<input type="text" value="1500"/>			
MTU	<input type="text" value="1500"/>			
Link Detection Interval (s)	<input type="text" value="60"/>			
Max Retries	<input type="text" value="0"/>			
Expert Options	<input type="text"/>			

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

Enable MPPE

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.

Local IP Address	<input type="text" value="205.205.0.100"/>
Peer IP Address	<input type="text" value="205.205.0.1"/>

Otherwise PPTP server will assign tunnel IP randomly.

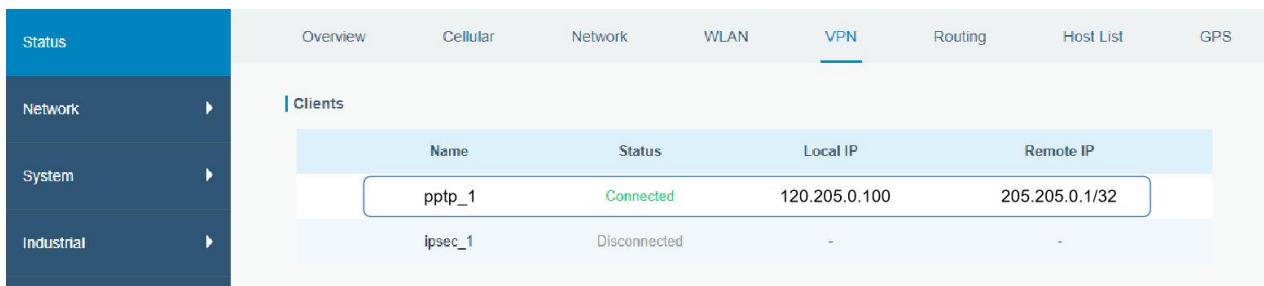
Click “Save” button when you complete all settings, and then the advanced settings will be hidden again. Then click “Apply” button to have the configurations take effect.

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.



The screenshot shows the 'VPN' status page with a table of clients. The table has columns for Name, Status, Local IP, and Remote IP. The 'pptp\_1' client is shown as 'Connected' with a local IP of 120.205.0.100 and a remote IP of 205.205.0.1/32. The 'ipsec\_1' client is shown as 'Disconnected' with no IP addresses.

Name	Status	Local IP	Remote IP
pptp_1	Connected	120.205.0.100	205.205.0.1/32
ipsec_1	Disconnected	-	-

## Related Topics

[PPTP Setting](#)

[PPTP Status](#)

**[END]**