User Guide

R3000 Lite

Industrial Dual SIM Cellular VPN Router

1 Eth + 1 RS-232 + 1 RS-485 + 1 USB Host

robustOS

Guangzhou Robustel Technologies Co., Limited
www.robustel.com

About This Document

This document provides hardware and software information of the Robustel R3000 Lite Router, including introduction, installation, configuration and operation.

Trademarks and Permissions

robustel、robustOS are trademarks of Guangzhou Robustel Technologies Co., Limited. All other trademarks and trade names mentioned in this document are the property of their respective owners.

Disclaimer

No part of this document may be reproduced in any form without the written permission of the copyright owner. The contents of this document are subject to change without notice due to continued progress in methodology, design and manufacturing. Robustel shall have no liability for any error or damage of any kind resulting from the use of this document.

Technical Support

Tel: +86-20-29019902
Fax: +86-20-82321505
E-mail: support@robustel.com
Web: www.robustel.com

Important Notice

Due to the nature of wireless communications, transmission and reception of data can never be guaranteed. Data may be delayed, corrupted (i.e., have errors) or be totally lost. Although significant delays or losses of data are rare when wireless devices such as the router is used in a normal manner with a well-constructed network, the router should not be used in situations where failure to transmit or receive data could result in damage of any kind to the user or any other party, including but not limited to personal injury, death, or loss of property. Robustel accepts no responsibility for damages of any kind resulting from delays or errors in data transmitted or received using the router, or for failure of the router to transmit or receive such data.

Safety Precautions

General

- The router generates radio frequency (RF) power. When using the router, care must be taken on safety issues related to RF interference as well as regulations of RF equipment.
- Do not use your router in aircraft, hospitals, petrol stations or in places where using cellular products is prohibited.
- Be sure that the router will not be interfering with nearby equipment. For example: pacemakers or medical equipment. The antenna of the router should be away from computers, office equipment, home appliance, etc.
- An external antenna must be connected to the router for proper operation. Only uses approved antenna with the router. Please contact authorized distributor on finding an approved antenna.
- Always keep the antenna with minimum safety distance of 20 cm or more from human body. Do not put the antenna inside metallic box, containers, etc.
- RF exposure statements
  1. For mobile devices without co-location (the transmitting antenna is installed or located more than 20cm away from the body of user and nearby person)
- FCC RF Radiation Exposure Statement
  1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
  2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and human body.

***Note**: Some airlines may permit the use of cellular phones while the aircraft is on the ground and the door is open.* Router *may be used at this time.*

Using the Router in Vehicle

- Check for any regulation or law authorizing the use of cellular devices in vehicle in your country before installing the router.
- The driver or operator of any vehicle should not operate the router while driving.
- Install the router by qualified personnel. Consult your vehicle distributor for any possible interference of electronic parts by the router.
- The router should be connected to the vehicle’s supply system by using a fuse-protected terminal in the vehicle’s fuse box.
- Be careful when the router is powered by the vehicle’s main battery. The battery may be drained after extended period.

Protecting Your Router

To ensure error-free usage, please install and operate your router with care. Do remember the following:

- Do not expose the router to extreme conditions such as high humidity / rain, high temperature, direct sunlight, caustic / harsh chemicals, dust, or water.
- Do not try to disassemble or modify the router. There is no user serviceable part inside and the warranty would be void.
- Do not drop, hit or shake the router. Do not use the router under extreme vibrating conditions.
- Do not pull the antenna or power supply cable. Attach/detach by holding the connector.
- Connect the router only according to the instruction manual. Failure to do it will void the warranty.
- In case of problem, please contact authorized distributor.

Regulatory and Type Approval Information

Table 1: Directives

2011/65/EC	Directive 2011/65/EU of the European Parliament and of the Council of 8 June 2011 on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS)
2012/19/EU	Directive 2012/19/EU the European Parliament and of the Council of 4 July 2012 on waste electrical and electronic equipment (WEEE)

Table 2: Standards of the Ministry of Information Industry of the People's Republic of China

SJ/T 11363-2006	"Requirements for Concentration Limits for Certain Hazardous Substances in Electronic Information Products" (2006-06).
SJ/T 11364-2006	"Marking for Control of Pollution Caused by Electronic Information Products" (2006-06). According to the "Chinese Administration on the Control of Pollution caused by Electronic Information Products" (ACPEIP) the EPUP, i.e., Environmental Protection Use Period, of this product is 20 years as per the symbol shown here, unless otherwise marked. The EPUP is valid only as long as the product is operated within the operating limits described in the Hardware Interface Description. Please see **Table 3** for an overview of toxic or hazardous substances or elements that might be contained in product parts in concentrations above the limits defined by SJ/T 11363-2006.

Table 3: Toxic or Hazardous Substances or Elements with Defined Concentration Limits

Name of the Part	Hazardous Substances					
	(Pb)	(Hg)	(Cd)	(Cr (VI))	(PBB)	(PBDE)
Metal parts	o	o	o	o	o	o
Circuit modules	x	o	o	o	o	o
Cables and cable assemblies	o	o	o	o	o	o
Plastic and polymeric parts	o	o	o	o	o	o
o: Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in SJ/T11363-2006. x: Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part *might exceed* the limit requirement in SJ/T11363-2006.						

Document History

Updates between document versions are cumulative. Therefore, the latest document version contains all updates made to previous versions.

Date	Firmware Version	Doc Version	Change Description
24 March, 2017	2.9.1	v.1.0.0	Initial release

Contents

Chapter 1 Product Concept

1.1 Overview

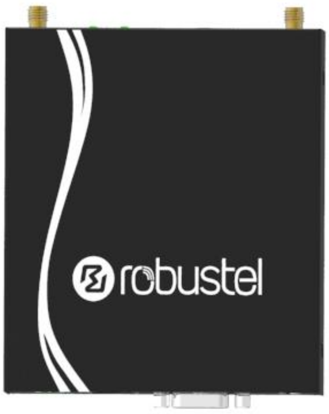
Robustel GoRugged R3000 Lite is a rugged cellular router offering state-of-the-art mobile connectivity for machine to machine (M2M) applications.

- Dual SIM redundancy for persistent 4G cellular network connections, enhanced keep alive feature support
- VPN tunnel - IPsec/OpenVPN/GRE/PPTP/L2TP/DMVPN
- Supports GRE over IPsec/L2TP over IPsec
- Supports 802.1Q VLAN Trunk
- Supports PPPoE Bridge
- Supports Modbus gateway (Modbus RTU/ASCII to Modbus TCP) and Modbus Master
- Auto reboot via SMS/Incoming Call/Timing
- Supports alarm via Email/SMS/SNMP trap
- Supports AAA and FTP
- Supports RobustLink (a centralized M2M management platform for remote monitoring, configuration and firmware upgrade)
- Supports RobustVPN (a Cloud VPN Portal providing easy and secure remote access for PLCs and machines)
- Flexible management methods - Web/CLI/SNMP/RobustLink
- Firmware upgrading via Web/CLI/USB/SMS/RobustLink

1.2 Package Contents

Before installing your R3000 Lite Router, verify the kit contents as following.

- 1 x Robustel GoRugged R3000 Lite Industrial Dual SIM Cellular VPN Router



OR

Two antennas **One antenna**

- 1 x 3-pin pluggable terminal block with lock for power connector

- 1 x *Quick Start Guide* with download link of other documents or tools x 1

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

Optional accessories (sold separately):

- SMA cellular antenna

  The number of SMA antenna depends on the model of the router. For more details, please refer to **1.3 Specifications**.

Magnet antenna

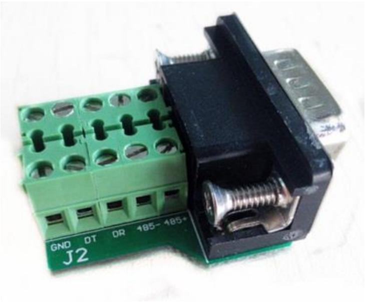
- Wall mounting kit

- 35 mm DIN rail mounting kit

- Ethernet cable

- AC/DC power adapter (12V DC, 1.5 A; EU/US/UK/AU plug optional)

- Terminal block with a male DB9 connector for serial port connection
  For details about the PIN assignment, see **2.2 PIN assignment**.



1.3 Specifications

Cellular Interface

- Number of ports: 2 (MAIN + AUX)
- Connector: SMA, female

Ethernet Interface

- Number of ports: 1 x 10/100 LAN Ethernet port
- Magnet isolation protection: 1.5 KV

Serial Interface

- Number of ports: 1 x RS232 + 1 x RS485
- Connector: DB9, female
- ESD protection: ±15 KV
- Parameters: 8E1, 8O1, 8N1, 8N2, 7E2, 7O2, 7N2, 7E1
- Baud rate: 300 bps to 230400 bps
- RS232: TxD, RxD, RTS, CTS, GND
- RS485: Data+ (A), Data- (B)

System

- Reset button: 1 x RST
- SIM slot: 2 x SIM card slot (3 V& 1.8 V)
- LED indicators: 1 x RUN, 1 x PPP, 1 x USR, 3 x RSSI
- Expansion: 1 x USB 2.0 host up to 480 Mbps
- Built-in RTC, Watchdog, Timer

Software

- Network protocols: PPP, PPPoE, TCP, UDP, DHCP, ICMP, NAT, DMZ, RIP v1/v2, OSPF, DDNS, VRRP, HTTP, HTTPs, DNS, ARP, QoS, SNTP, Telnet, IP Passthrough, etc.
- VPN tunnel: IPsec/OpenVPN/GRE/PPTP/L2TP
- Firewall: SPI, anti-DoS, Filter, Access Control
- Management: Web, CLI, SNMP v1/v2/v3, SMS, RobustLink
- Serial port: TCP client/server, UDP, Modbus RTU/ASCII to Modbus TCP, Virtual COM (COM port redirector)
- RobustLink: a centralized M2M management platform developed by Robustel
- RobustVPN: a Cloud VPN Portal

Power Supply and Consumption

- Connector: 3.5 mm terminal block
- Power consumption: 150 mA @ 12 V

Physical Characteristics

- Housing & Weight: Metal, 300 g
- Dimensions: 105 x 98 x 29.5 mm
- Installations: desktop or wall mounting or 35 mm DIN rail mounting

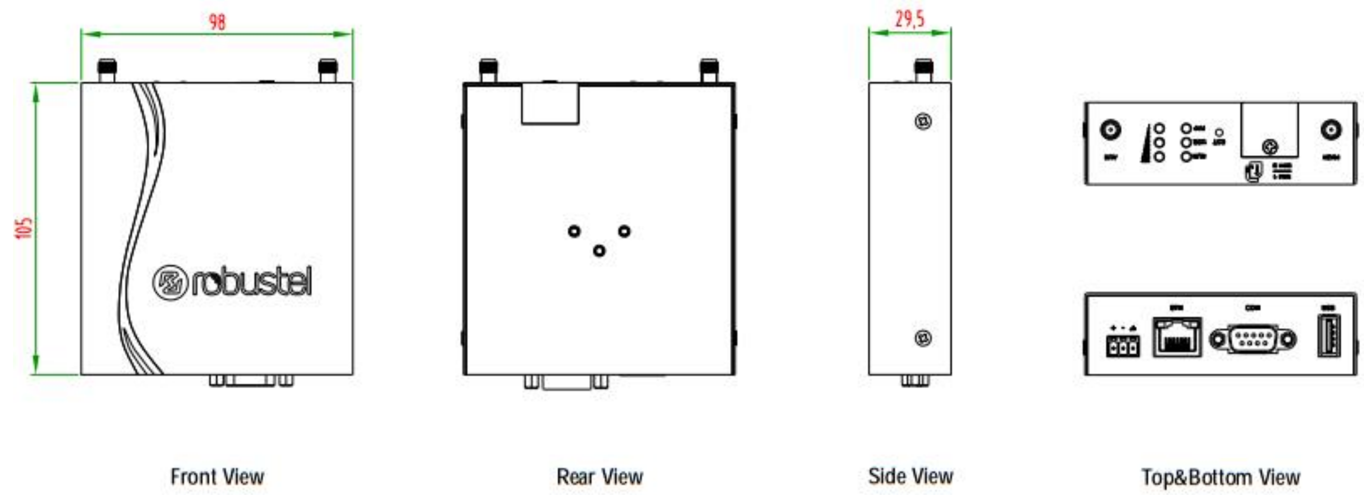
Regulatory and Type Approvals

- Approvals & Certificates: CE, R&TTE, RCM, RoHS, WEEE
- EMC:

EMI: EN 55022: 2006/A1: 2007 (CE&RE) Class B

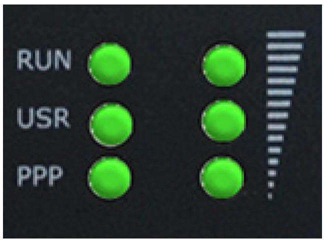
EMS: IEC 61000-4-2 (ESD) Level 3, IEC 61000-4-3 (RS) Level 4
IEC 61000-4-4 (EFT) Level 3, IEC 61000-4-5 (Surge) Level 3
IEC 61000-4-6 (CS) Level 3, IEC 61000-4-8 (M/S) Level 4

1.4 Dimensions



Chapter 2 Installation

2.1 LED Indicators

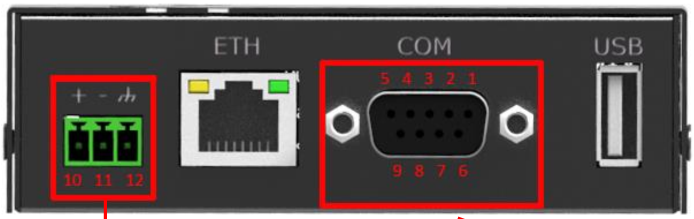


Name	Color	Status	Description
RUN	Green	On, solid	Router is powered on
		On, blinking	Router is starting up
		Off	Router is powered off
PPP	Green	On, solid	PPP connection is up
		On, blinking	Null
		Off	PPP connection is down
USR	Green	On, blinking	SIM: using backup SIM card NET: access to a low level network
		Off after blinking	SIM: working NET: working
		On	OpenVPN is connected IPsec is connected GRE is connected
		Off	OpenVPN is disconnected IPsec is disconnected GRE is disconnected
📶	Green	On	Signal level: 21-31 (High Signal)
	Yellow	On	Signal level: 11-20 (Medium Signal)
	Red	On	Signal level: 1-10 (Low Signal)
	When the network disconnected, those three signal LEDs are designed as a binary combination code to indicate a series of error report. (Green Yellow Red) On: 1 Off: 0 001 AT command failed 010 no SIM card detected 011 it need to enter the PIN code 100 it need to enter the PUK code 101 registration failed 110 something wrong happened in the module		

Note: You can choose the display type of USR LED. For more details, please refer to **3.27 Services > Advanced**.

2.2 PIN Assignment

The R3000 Lite has been designed to be placed on a desktop. Below is the bottom of the R3000 Lite.



Terminal block

PIN	Power
10	Positive
11	Negative
12	GND

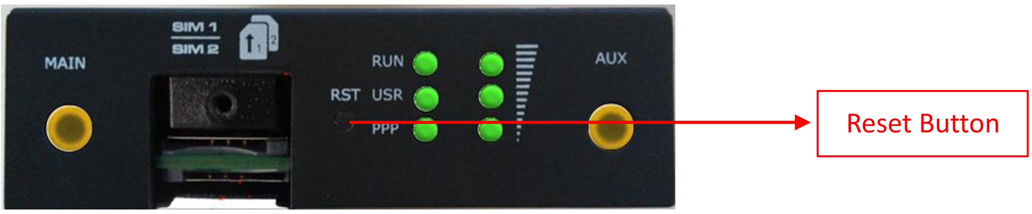
DB9 Female Connector

PIN	Debug	RS-232	RS-485 (2-wire)	Terminal block	Direction
1	CR	--	Data+ (A)	485+	--
2	CT	RXD	--	RXD	R3000 Lite → Device
3	--	TXD	--	TXD	Device → R3000 Lite
4	DRXD	--	--	DT	Device → R3000 Lite
5	GND	GND	--	GND x2	--
6	--	--	Data- (B)	485-	--
7	--	RTS	--	RTS	Device → R3000 Lite
8	--	CTS	--	CTS	R3000 Lite → Device
9	DTXD	--	--	DR	R3000 Lite → Device

2.3 USB Interface

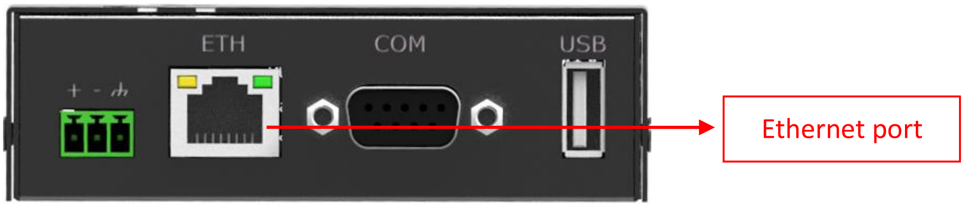
USB interface is used for batch firmware upgrade, cannot used to send or receive data from slave devices which with USB interface. Users can insert a USB storage device, such as U disk or hard disk, into the router's USB interface, if there is configuration file or firmware of R3000 Lite inside the USB storage devices, R3000 Lite will automatically update the configuration file or firmware. For more details, please go to **3.10 Interface > USB**.

2.4 Reset Button



Function	Operation
Reboot	Press the button for at least 5 seconds in operating status
Restore to factory default setting	After powering up the router, press the RST button by a small non-conductive stick with a blunt end in about 60 seconds until all three LEDs (RUN, PPP, USR) on the left side blinking 5 times simultaneously. Then the router will be restored to factory default settings

2.5 Ethernet Port



The Ethernet port has two LED indicators. The yellow one is **Link Indicator** and the green one is **Speed Indicator**. Each indicator has three statuses, for details see the table below:

Indicator	Status	Description
Link Indicator	On	Connection is enabled
	On, blinking	Data is being transmitted
	Off	Connection is disabled
Speed Indicator	On	100 Mbps mode
	Off	10 Mbps mode

2.6 Mount the Router

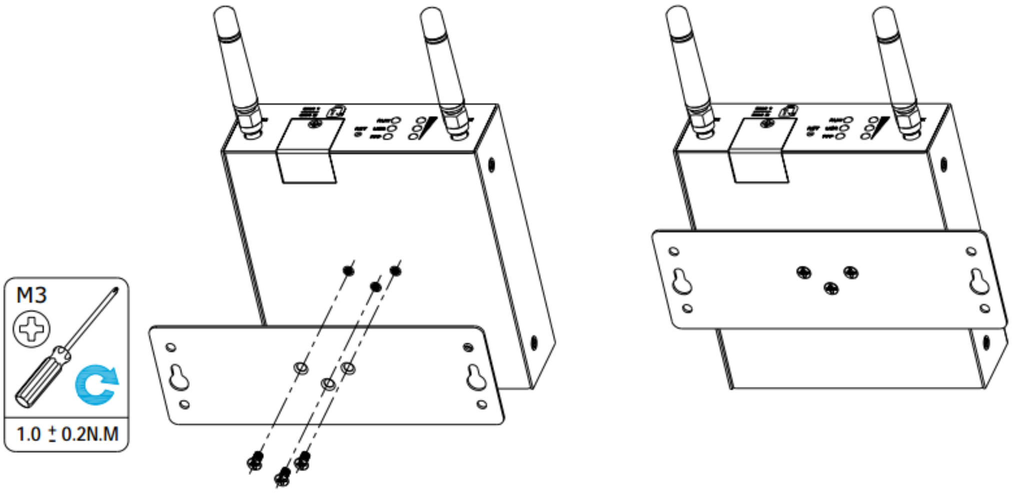
R3000 Lite router supports for horizontal surface placement, DIN rail mounting and wall mounting.

- **Two ways for mounting the router**

1. **Wall mounting**

   Use 3 pcs of M3*4 countersunk Phillips screws to fix the router on the wall mounting kit, and then use 2 pcs of M3 drywall screws to mount the router associated with the wall mounting kit on the wall.

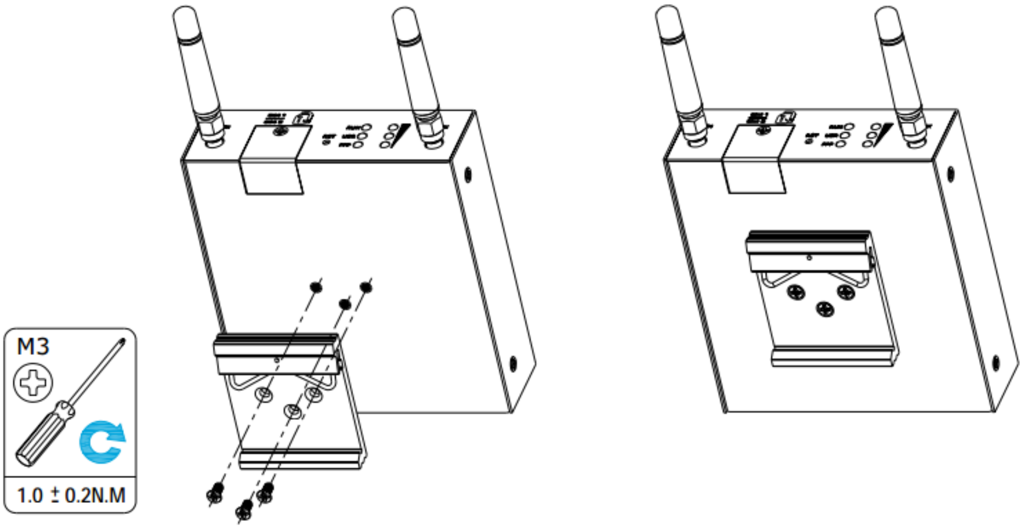
   Note: Recommended torque for mounting is 1.0 N.m, and the maximum allowed is 1.2 N.m.



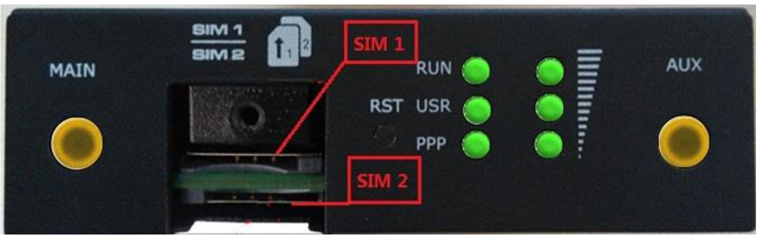
2. **DIN rail mounting**

   Use 3 pcs of M3*4 countersunk phillips screws to fix the router on the DIN rail, and then hang the DIN rail on the bracket. It is necessary to choose the standard bracket.

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



2.7 Install the SIM Card



- **Remove slot cover**

1. Make sure router is powered off.
2. To remove cover, loosen the screws associated with the cover by using a screwdriver and then find the SIM card slot.

- **Insert SIM card**

3. To insert SIM card, press the card with fingers until snap on and then tighten the screws associated with the cover by using a screwdriver.

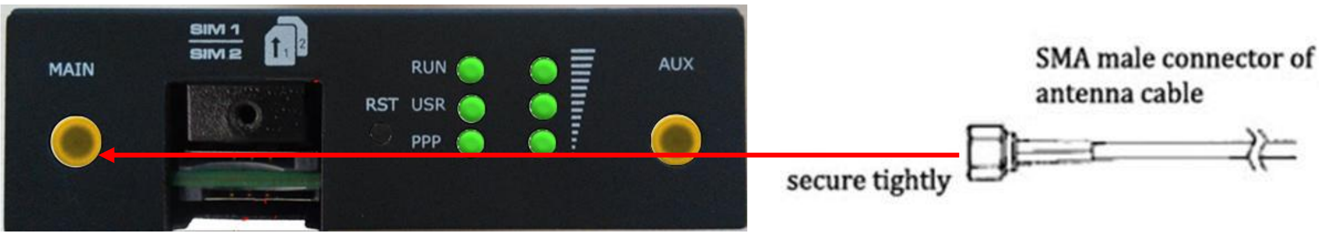
- **Remove SIM card**

4. Make sure router is powered off.
5. To remove SIM card, press the card with fingers until pop out and then take out the SIM card.

Note:

1. Use the specific M2M SIM card when the device is working in extreme temperature, because the regular SIM card for long-time working in harsh environment will be disconnected frequently.
2. Do not forget to twist the cover tightly to avoid being stolen.
3. Do not touch the metal of the SIM card surface in case information in the card will lost or be destroyed.
4. Do not bend or scratch the SIM card.
5. Keep the SIM card away from electricity and magnetism.
6. Make sure router is powered off before inserting or removing the SIM card.

2.8 Connect the External Antenna (SMA Type)



Connect the SMA external antenna connector to the router's antenna interface and twist tightly. Make sure the antenna is within the correct frequency range provided by the operator and with 50 Ohm impedance.

Note: Recommended torque for mounting is 0.35 N.m.

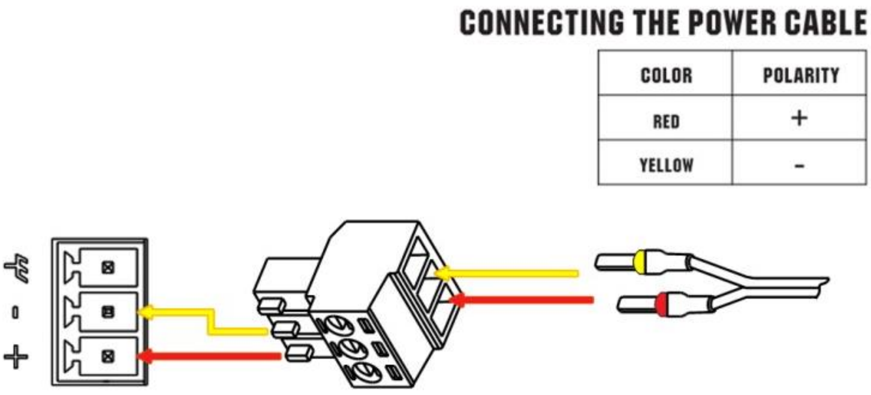
2.10 Grounding the Router

Router grounding helps prevent the noise effect due to electromagnetic interference (EMI). Connect the router to the site ground wire by the ground screw before powering on.
Note: This product is appropriate to be mounted on a sound grounded device surface, such as a metal panel.

2.11 Connect the Router to PC

Connect the router’s Ethernet port to a PC through a standard crossed network cable.

2.11 Power Supply



CONNECTING THE POWER CABLE

COLOR	POLARITY
RED	+
YELLOW	-

R3000 Lite router supports reverse polarity protection, but always refers to the figure above to connect the power adapter correctly. There are two cables associated with the power adapter. Following to the color of the head, connect the cable marked red to the positive pole through a terminal block, and connect the yellow one to the negative in the same way.

Chapter 3 Configuration Settings over Web Browser

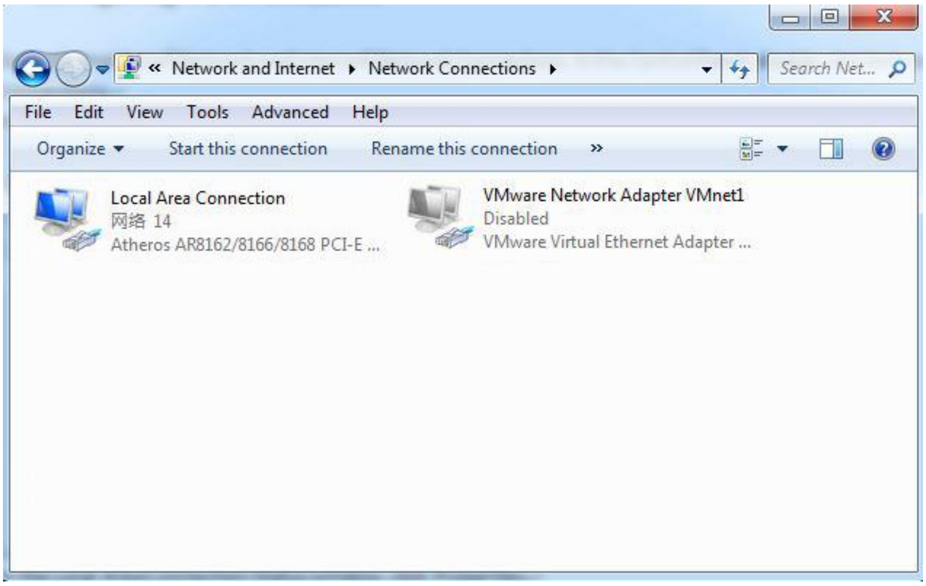
The router can be configured through web browser including IE 8.0 or above, Chrome and Firefox, etc. And the supported operating systems are: Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista/7/8, etc. There are various ways to connect to the router, either through an external repeater/hub or to PC directly. When the router connects to the PC's Ethernet port directly, and if the router works as the DHCP server, then the PC can obtain IP from router directly; or the PC can be configured with a static IP address in the same network segment with the router, and then the PC and the router will form a small local area network. After the connection has been established successfully, enter the device's default login address in the browser and access the router's web login interface.

3.1 Configuring for the PC

There are two methods to configure the IP address on PC, one is to obtain an IP address automatically from Local Area Connection, and another is to configure a static IP address manually within the same subnet of R3000 Lite router. Please refer to the steps below:

Window 7 System (the configuration for Windows system is similar)

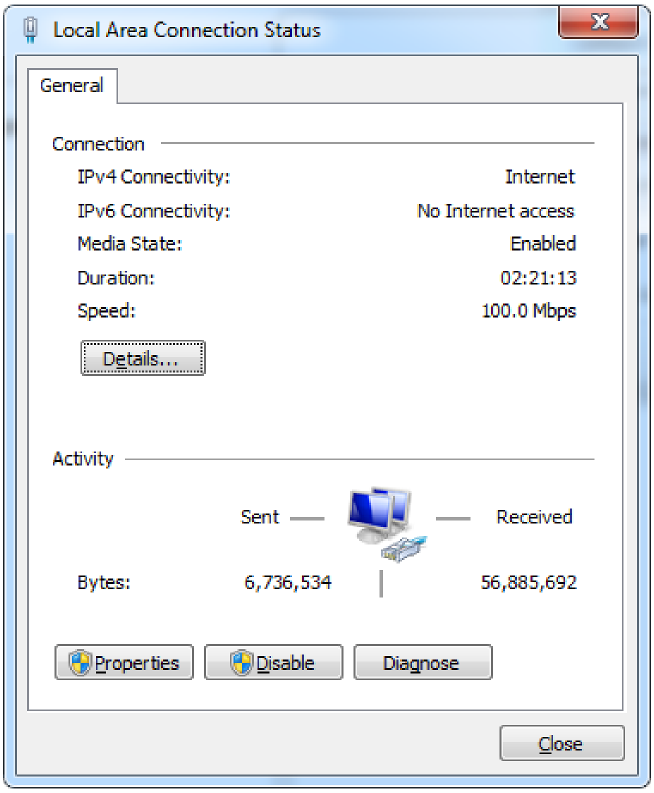
1. Click **Start > Control panel** (in classic view), double-click **Network and Sharing Center**, and then double-click **Local Area Connection**.


« Network and Internet ▸ Network Connections ▸
Search Net...
File Edit View Tools Advanced Help
Organize ▾ Start this connection Rename this connection »

Local Area Connection
网络 14
Atheros AR8162/8166/8168 PCI-E ...

VMware Network Adapter VMnet1
Disabled
VMware Virtual Ethernet Adapter ...

2. Click **Properties** in the window of **Local Area Connection Status**.



Local Area Connection Status

General

Connection

IPv4 Connectivity: Internet

IPv6 Connectivity: No Internet access

Media State: Enabled

Duration: 02:21:13

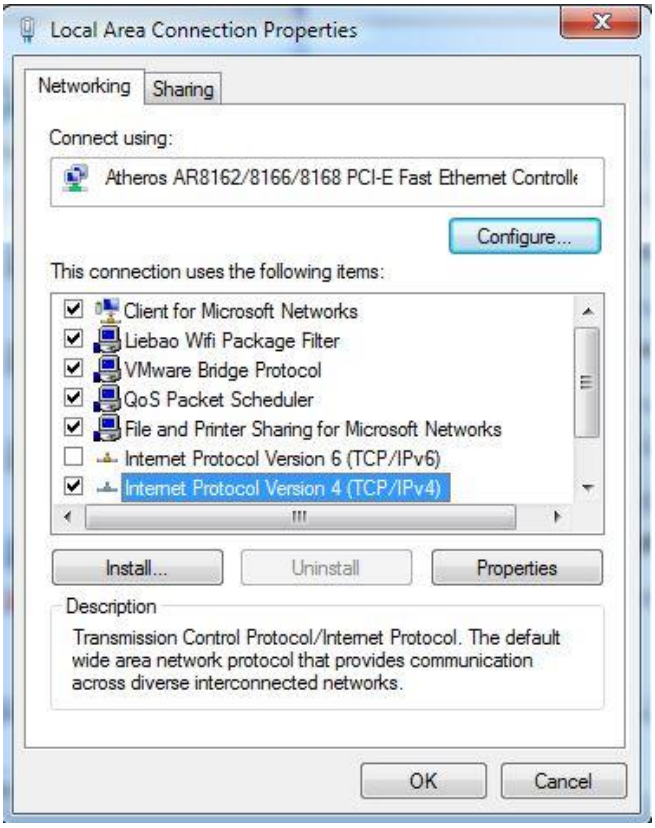
Speed: 100.0 Mbps

Activity

Sent — — Received

Bytes: 6,736,534 | 56,885,692

3. Choose **Internet Protocol Version 4 (TCP/IPv4)** and click **Properties**.



Local Area Connection Properties

Networking Sharing

Connect using:

Atheros AR8162/8166/8168 PCI-E Fast Ethernet Controll

This connection uses the following items:

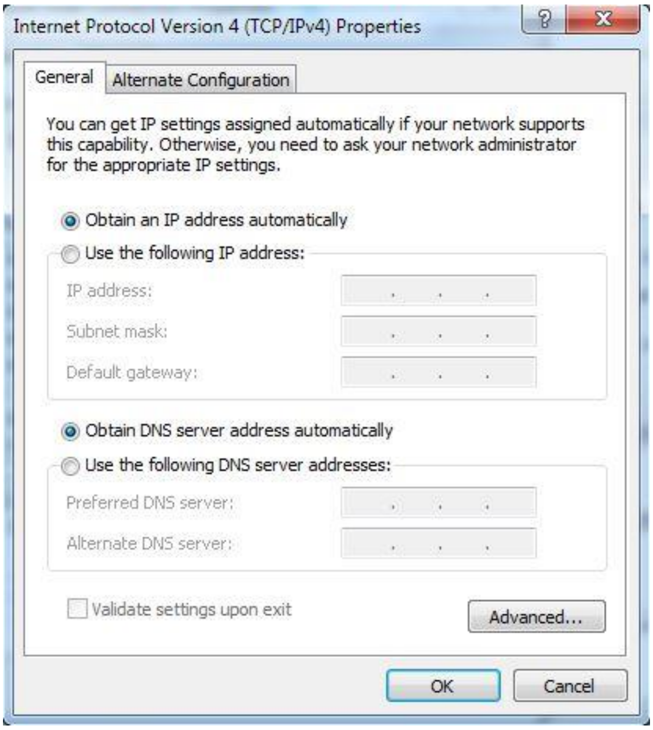
- ☑ Client for Microsoft Networks
- ☑ Liebao Wifi Package Filter
- ☑ VMware Bridge Protocol
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☐ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

4. Two ways for configuring the IP address of PC:

   Obtain an IP address automatically:



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

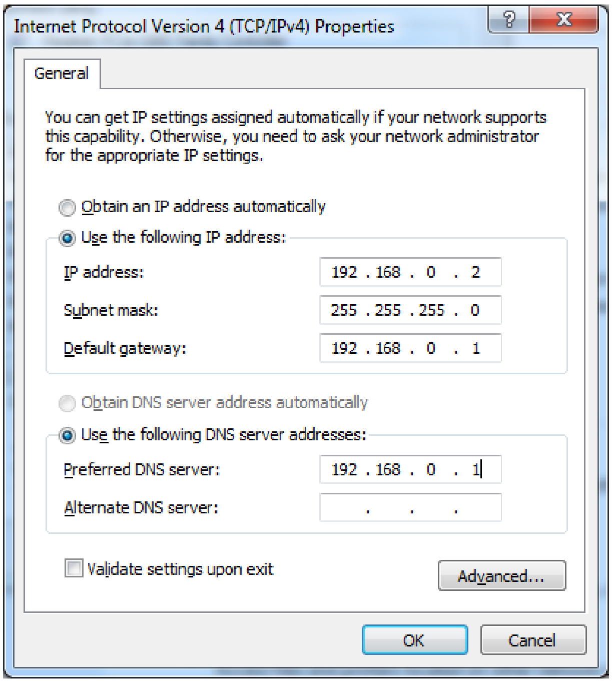
○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Use the following IP address (configured a static IP address manually within the same subnet of R3000 Lite router):



You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

○ Obtain an IP address automatically

● Use the following IP address:

IP address: 192 . 168 . 0 . 2

Subnet mask: 255 . 255 . 255 . 0

Default gateway: 192 . 168 . 0 . 1

○ Obtain DNS server address automatically

● Use the following DNS server addresses:

Preferred DNS server: 192 . 168 . 0 . 1

Alternate DNS server: . . .

□ Validate settings upon exit

5. Click **OK** to finish the configuration.

3.2 Factory Default Settings

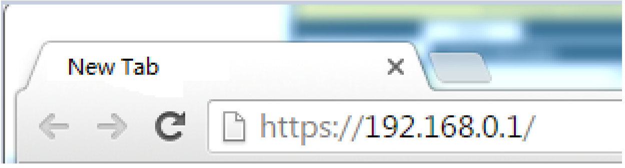
Before configuring your router, you need to know the following default settings.

Item	Description
Username	admin
Password	admin
Ethernet	192.168.0.1/255.255.255.0, LAN mode
DHCP Server	Enabled.

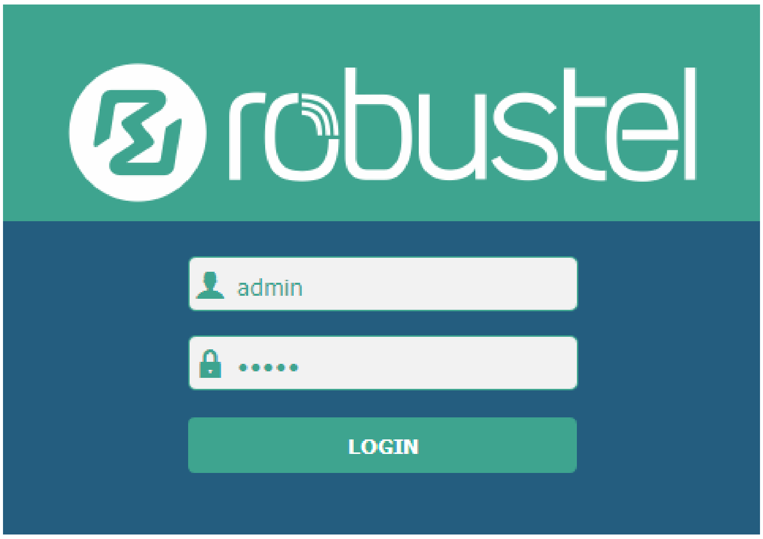
3.3 Login Router

1. On the PC, open a web browser such as Internet Explorer, Google and Firefox etc.

2. From your web browser, enter the IP address of the router. The default IP address of R3000 Lite is 192.168.0.1, though the actual address may vary.
Note: If a public SIM card is inserted in the R3000 Lite router, you can enter the corresponding public IP address of the SIM card in the browser's address bar, so that to access the R3000 Lite router wirelessly by this public IP.



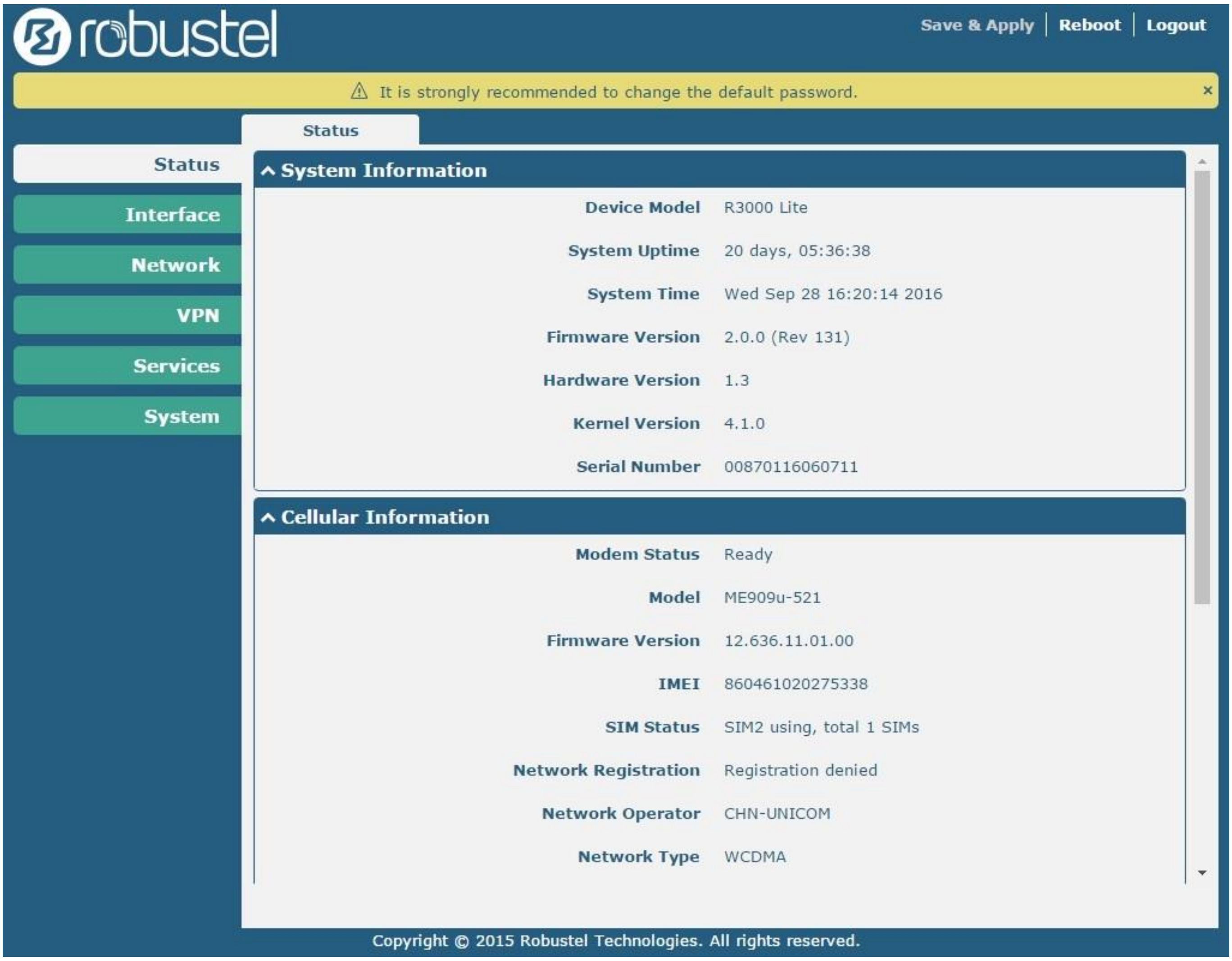
3. In the login page, enter the username and password of R3000 Lite router, choose language and then click **Login**. If enter the wrong username or password over six times, the login web will be locked for 5 minutes.



3.4 Control Panel

After logging in the R3000 Lite, the home page of the R3000 Lite router's web interface is displayed, just like the screenshot below.

This section allows users to save configuration, reboot router and logout. When you are first time to login R3000 Lite, there will be a pop-up tab "⚠ It is strongly recommended to change the default password.", click × to close the pop-up tab. And if you want to change the password, please refer to **3.31 System > User Management s**ection**.**


Save & Apply | Reboot | Logout
⚠ It is strongly recommended to change the default password. ×
Status
Status
Interface
Network
VPN
Services
System

^ System Information

Device Model	R3000 Lite
System Uptime	20 days, 05:36:38
System Time	Wed Sep 28 16:20:14 2016
Firmware Version	2.0.0 (Rev 131)
Hardware Version	1.3
Kernel Version	4.1.0
Serial Number	00870116060711

^ Cellular Information

Modem Status	Ready
Model	ME909u-521
Firmware Version	12.636.11.01.00
IMEI	860461020275338
SIM Status	SIM2 using, total 1 SIMs
Network Registration	Registration denied
Network Operator	CHN-UNICOM
Network Type	WCDMA

Copyright © 2015 Robustel Technologies. All rights reserved.

Control Panel		
Item	**Description**	**Button**
Save & Apply	Click to save the current configuration into router's flash and apply the modification on every configuration page, to make the modification taking effect.	Save & Apply
Reboot	Click to reboot the router. When the Reboot button is in yellow, it means that some completed configurations will take effect only by reboot.	Reboot

Logout	Click to exit safely, then it will switch to login page. Shut down web page directly without logout, the next one can login web on this browser without a password before timeout.	Logout
Submit	Click to submit the modification on current configuration page.	Submit
Cancel	Click to cancel the modification on current configuration page.	Cancel

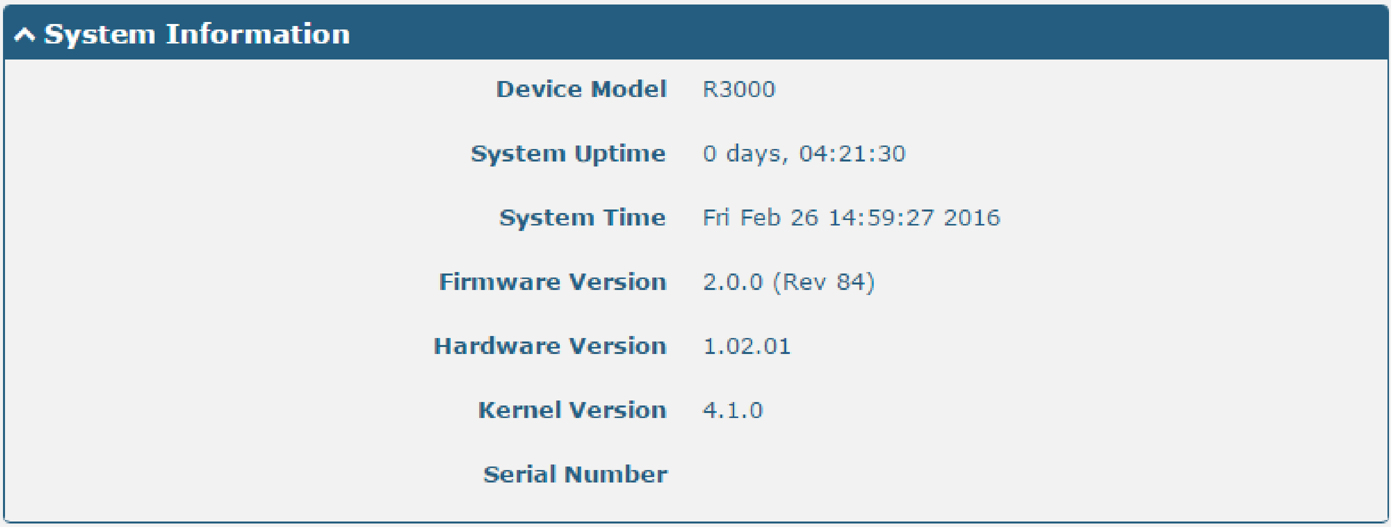
Note: The steps of how to modify configuration are as bellow:

1. Modify in one page;
2. Click Submit under this page;
3. Modify in another page;
4. Click Submit under this page;
5. Complete all modification;
6. Click Save & Apply .

3.5 Status

This section displays the router's status, which shows you a number of helpful information such as System Information, Cellular Information, Internet Status and LAN Status.

System Information



^ System Information

Device Model R3000

System Uptime 0 days, 04:21:30

System Time Fri Feb 26 14:59:27 2016

Firmware Version 2.0.0 (Rev 84)

Hardware Version 1.02.01

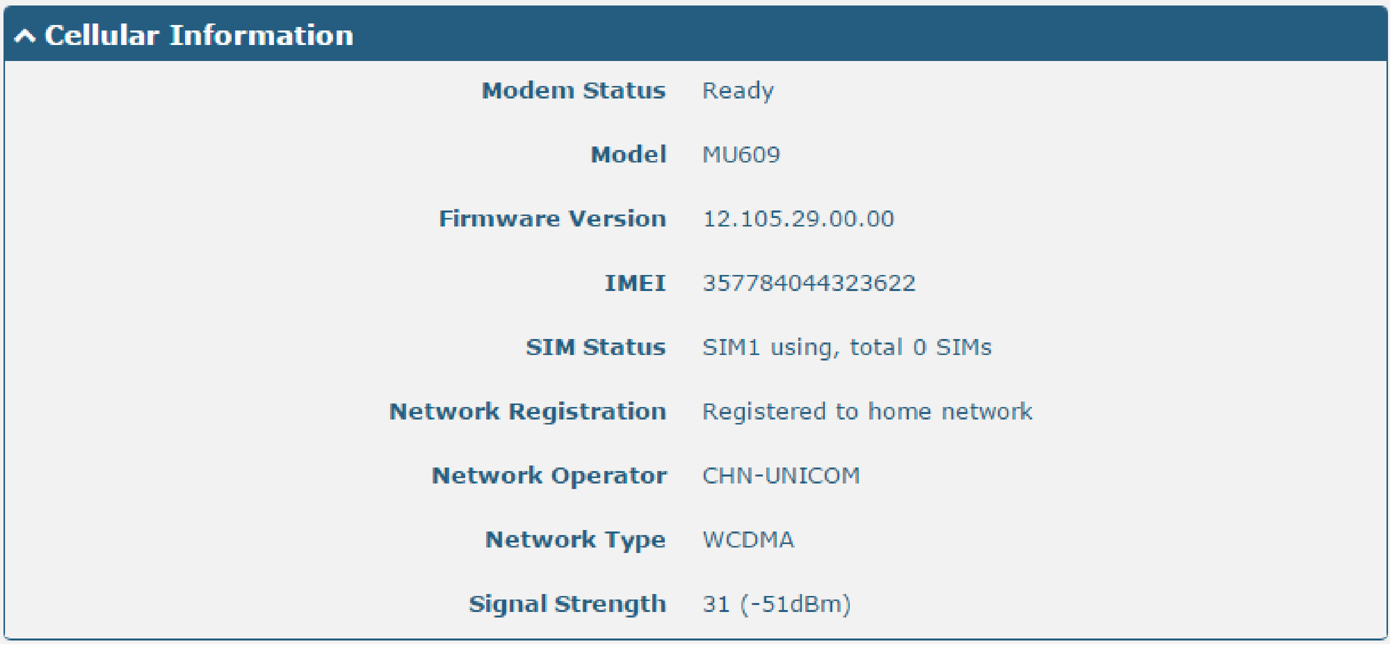
Kernel Version 4.1.0

Serial Number

System Information	
Item	**Description**
Device Model	Show the model name of this device.
System Uptime	Show how long the router has been working since power on.

System Time	Show the current system time.
Firmware Version	Show the current firmware version.
Hardware Version	Show the current hardware version.
Kernel Version	Show the current kernel version.
Serial Number	Show the serial number of this device.

Cellular Information



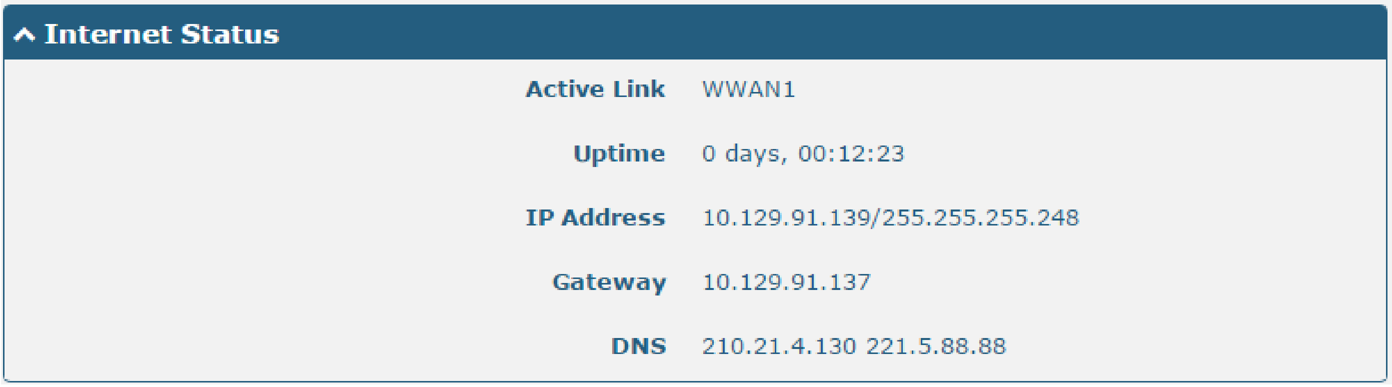
^ Cellular Information

Modem Status	Ready
Model	MU609
Firmware Version	12.105.29.00.00
IMEI	357784044323622
SIM Status	SIM1 using, total 0 SIMs
Network Registration	Registered to home network
Network Operator	CHN-UNICOM
Network Type	WCDMA
Signal Strength	31 (-51dBm)

Cellular Information	
Item	**Description**
Modem Status	Show the status of modem. There are 8 different status: 1. Initializing 2. Modem not found 3. No response 4. SIM not detected 5. SIM PIN required 6. SIM PUK required 7. Register failed 8. Ready
Modem Model	Show the current radio module type.
Firmware Version	Show the current radio firmware version.
IMEI	Show the IMEI number of the radio module.
SIM Status	Show the SIM card which the router works with currently: SIM1 or SIM2. And show the total SIM cards in the router.
Network Registration	Show the status of Registration. There are 6 different status: 1. Not registered, search stopped 2. Registered to home network

Cellular Information	
Item	**Description**
	3. Not registered, searching 4. Registration denied 5. Unknown 6. Registered, roaming
Network Operator	Show the current network provider.
Network Type	Show the current network service type, e.g. GPRS.
Signal Strength	Show the current signal strength.

Internet Status



^ Internet Status

Active Link WWAN1

Uptime 0 days, 00:12:23

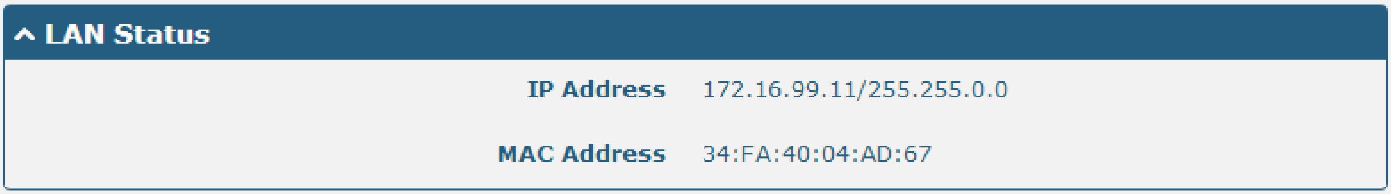
IP Address 10.129.91.139/255.255.255.248

Gateway 10.129.91.137

DNS 210.21.4.130 221.5.88.88

Internet Status	
Item	**Description**
Active Link	Show the current WAN link: WWAN1, WWAN2 or WAN.
Uptime	Show how long the current WAN have been working.
IP Address	Show the current WAN IP address.
Gateway	Show the current gateway.
DNS	Show the current primary DNS server and Secondary server.

LAN Status



^ LAN Status

IP Address 172.16.99.11/255.255.0.0

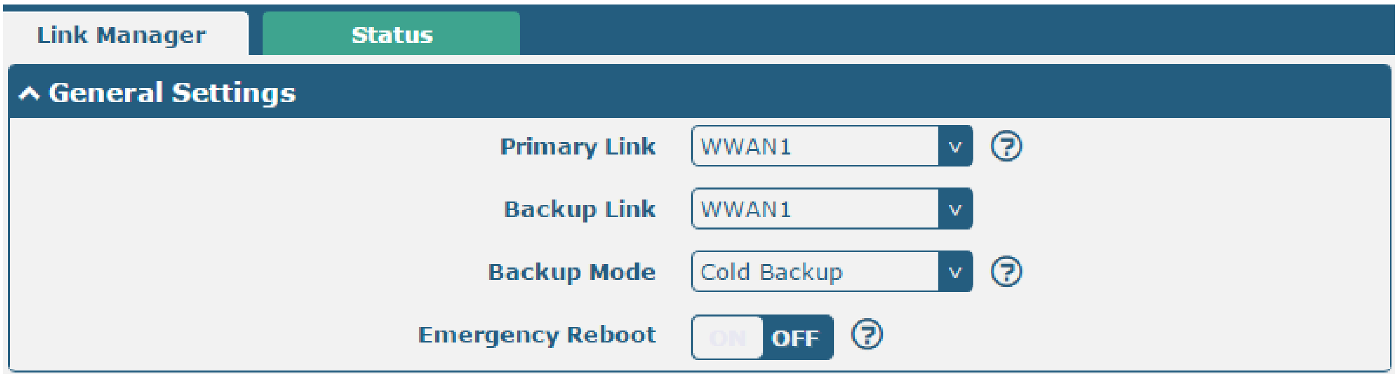
MAC Address 34:FA:40:04:AD:67

Router Information	
Item	**Description**
IP Address	Show the current IP Address and the Netmask.
MAC Address	Show the current MAC Address.

3.6 Interface > Link Manager

Link Manager

User can manage the link connection in this section. R3000 Lite support Cellular and Ethernet link connection.



Primary Link: WWAN1

Backup Link: WWAN1

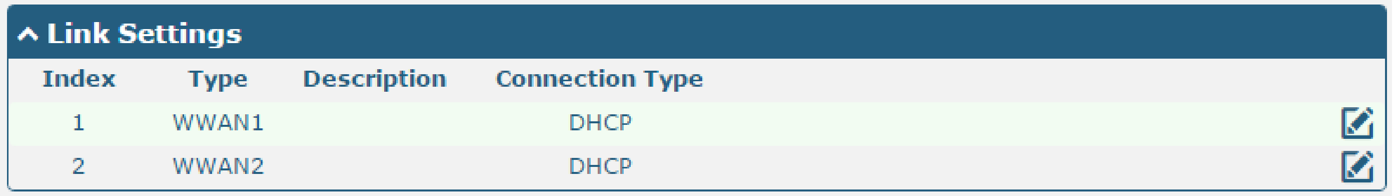
Backup Mode: Cold Backup

Emergency Reboot: ON OFF

Link Manager		
Item	**Description**	**Default**
Primary Link	Select from "WWAN1", "WWAN2". • WWAN1: Select to make SIM1 as the primary wireless link. ***Note:*** *insert SIM card please refer to the installation quick guide.* • WWAN2: Select to make SIM2 as the primary wireless link.	WWAN1
Backup Link	Select from "None", "WWAN1", "WWAN2". • None: Do not select backup interface. • WWAN1: Select to make SIM1 as backup wireless WAN. • WWAN2: Select to make SIM2 as backup wireless WAN.	None
Backup Mode	Cold backup: The inactive link is offline on standby. Warm backup: The inactive link is online on standby. Warm backup mode is not available for dual SIM backup.	Cold backup
Emergency Reboot	Enable to reboot the whole system if no links available.	OFF

Note: *Click"? " for help.*

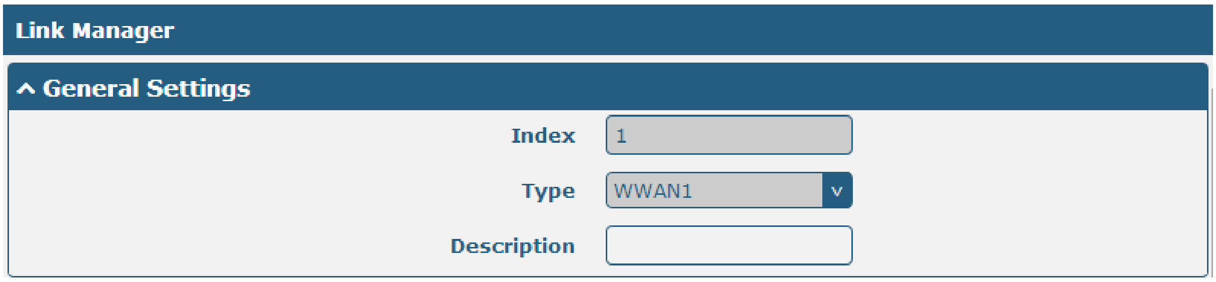
Link Setting section allows user to configure the parameter of link connection, include the WWAN1 and WWAN2. It is recommended to enable Ping detection to keep router always online.
The Ping detection increases the reliability and also cost data traffic.



Index	Type	Description	Connection Type
1	WWAN1		DHCP
2	WWAN2		DHCP

Click ✎ to enter the link configuration window.

WWAN1/WWAN2

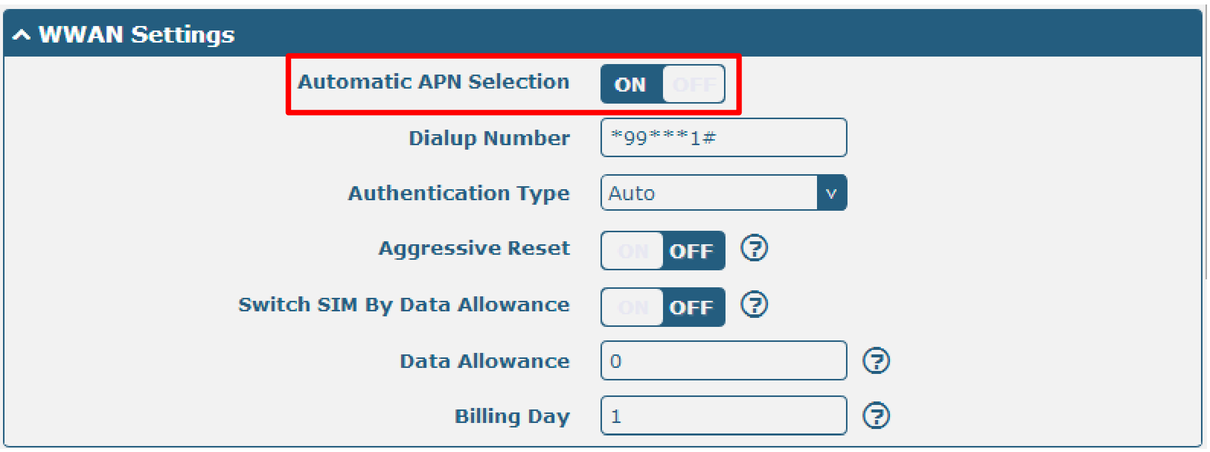


Link Manager

General Settings

Index	1
Type	WWAN1
Description	

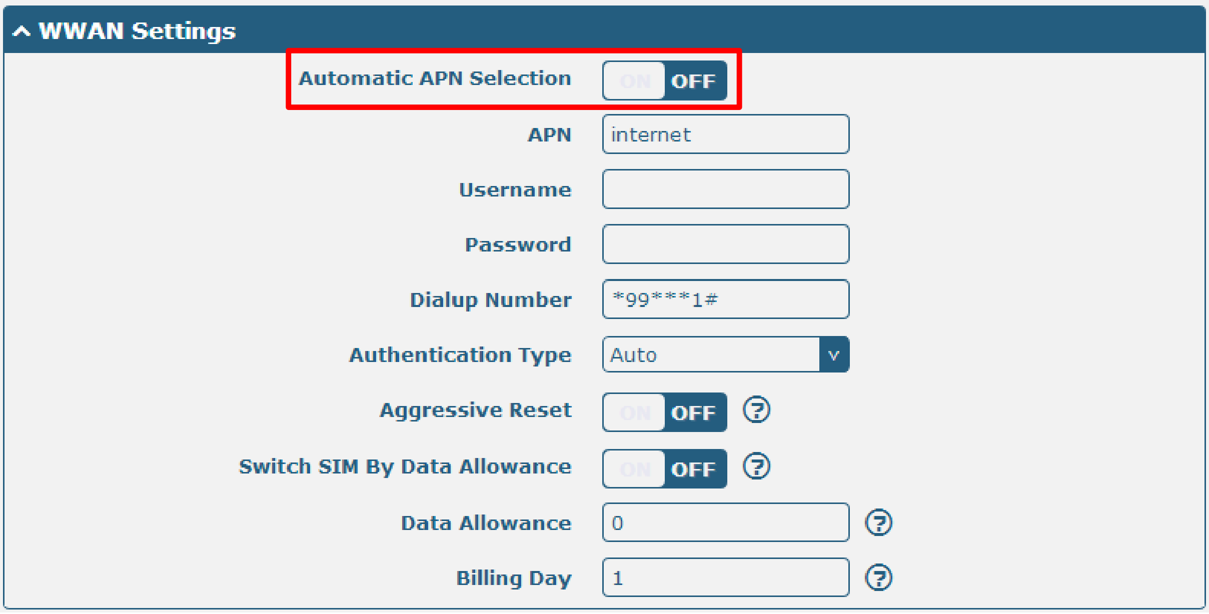
When enable “Automatic APN Selection”, the window will display just like the following screenshot.



WWAN Settings

Automatic APN Selection	ON
Dialup Number	*99***1#
Authentication Type	Auto
Aggressive Reset	OFF
Switch SIM By Data Allowance	OFF
Data Allowance	0
Billing Day	1

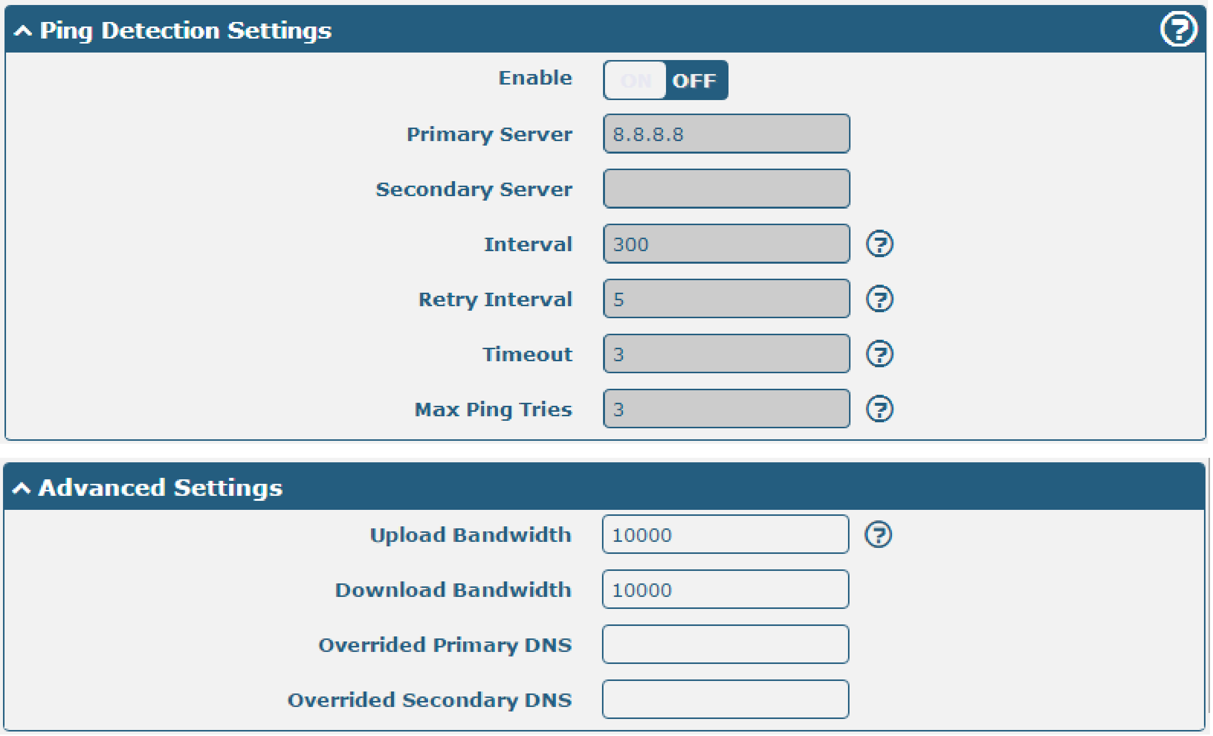
When disable “Automatic APN Selection”, the window will display just like the following screenshot.



WWAN Settings

Automatic APN Selection	OFF
APN	internet
Username	
Password	
Dialup Number	*99***1#
Authentication Type	Auto
Aggressive Reset	OFF
Switch SIM By Data Allowance	OFF
Data Allowance	0
Billing Day	1

WWAN Setting		
Item	**Description**	**Default**
Automatic APN Selection	R3000 Lite will recognize the access point name automatically.	ON
Dialup Number	Dialup number for cellular dial-up connection, provided by local ISP.	*99***1#
Authentication Type	Select from “Auto”, “PAP” and “CHAP” as the local ISP required.	Auto
Aggressive Reset	The module will be reset when the link become unreachable.	OFF
Switch SIM By Data Allowance	Switch to another SIM when reach data allowance, only use for dual SIM backup.	OFF
Data Allowance	Set the monthly data traffic limitation. The system will record the data traffic statistics when data traffic limitation (MiB) is specified. The traffic record will display in **Link Manager > Status > WWAN Data Usage Statistics** section. 0 means disable data traffic record.	0
Billing Day	This option specifies the day of month for billing, the data traffic statistics will be recalculated from this day.	1
Redial Interval	Seconds to wait for redial.	10
APN	Access Point Name for cellular dial-up connection, provided by local ISP.	internet
Username	User Name for cellular dial-up connection, provided by local ISP.	Null
Password	Password for cellular dial-up connection, provided by local ISP.	Null



^ Ping Detection Settings

Enable: ON OFF

Primary Server: 8.8.8.8

Secondary Server:

Interval: 300

Retry Interval: 5

Timeout: 3

Max Ping Tries: 3

^ Advanced Settings

Upload Bandwidth: 10000

Download Bandwidth: 10000

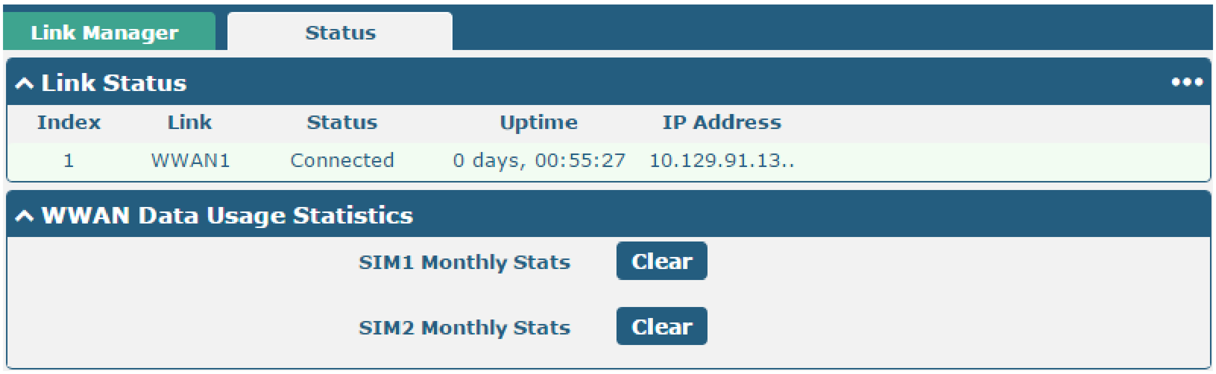
Overrided Primary DNS:

Overrided Secondary DNS:

Ping Detection Settings/Advanced Setting		
Item	**Description**	**Default**
Enable	To enable “ping detection”. It was a keepalive policy of R3000 Lite router.	OFF

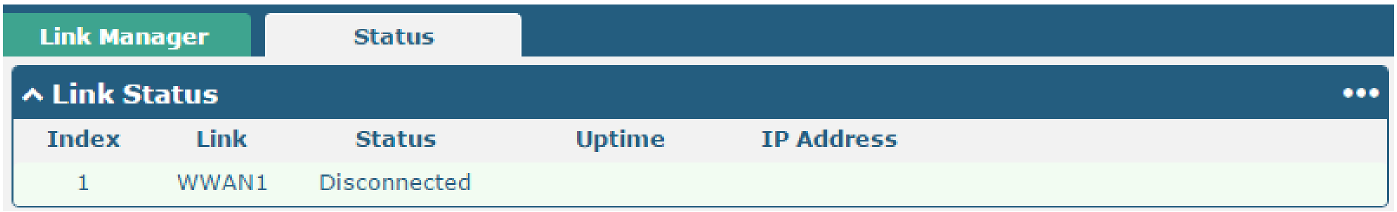
Ping Detection Settings/Advanced Setting		
Item	**Description**	**Default**
Primary Server	Router will ping this primary address/domain name to check that if the current connectivity is active.	8.8.8.8
Secondary Server	Router will ping this secondary address/domain name to check that if the current connectivity is active.	Null
Interval	Set the ping interval.	300
Retry Interval	Set the ping retry interval.	5
Tmeout	Set the ping timeout.	3
Max Ping Tries	Switch to another link or take emergency action if max continuous ping tries reached.	3
Upload Bandwith	used for QoS, unit: kbps	10000
Download Bandwith	used for QoS, unit: kbps	10000
Overrided Primary DNS	Overrided DNS will override the automatically obtained DNS.	Null
Overrided Secondary DNS	Overrided DNS will override the automatically obtained DNS.	Null

User can check the status of WWAN connection and clear the monthly data usage record in Status page.



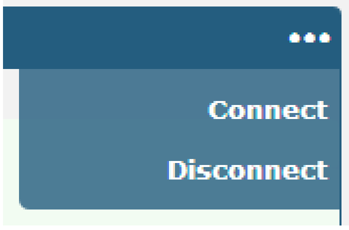
Index	Link	Status	Uptime	IP Address
1	WWAN1	Connected	0 days, 00:55:27	10.129.91.13..

Status

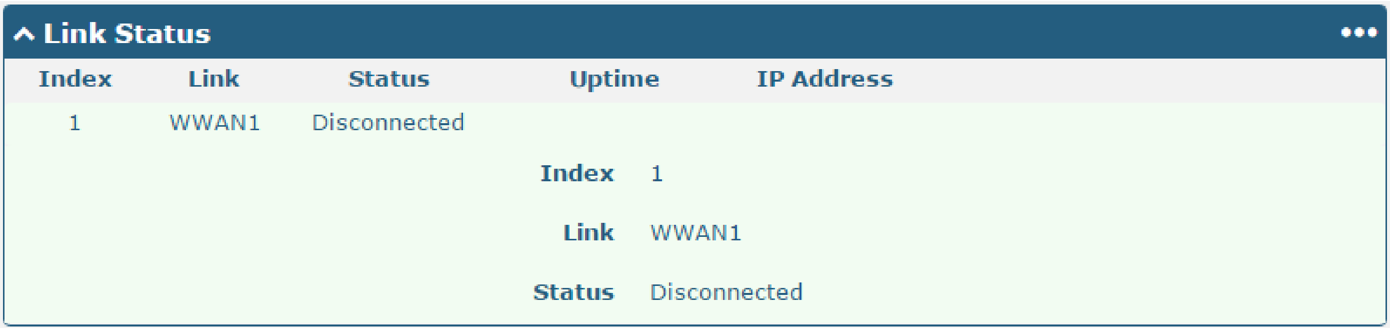


Index	Link	Status	Uptime	IP Address
1	WWAN1	Disconnected		

Click the button ••• which is in the top right of the Link Status window. Select the connection status of the current link.



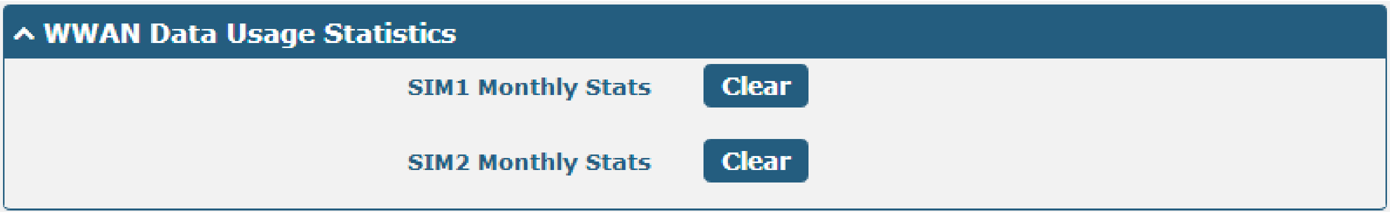
Click the row of the link, and it will show the details information of the current link connection under the row.



Link Status

Index	Link	Status	Uptime	IP Address
1	WWAN1	Disconnected		

Index	1
Link	WWAN1
Status	Disconnected



WWAN Data Usage Statistics

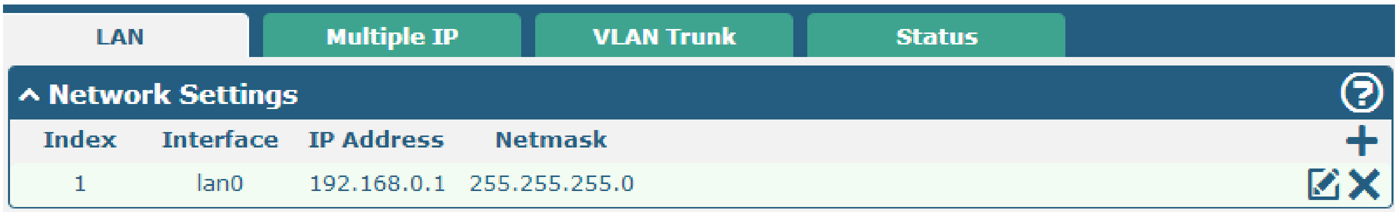
SIM1 Monthly Stats	Clear
SIM2 Monthly Stats	Clear

Click Clear button to clear SIM1 or SIM2 monthly data traffic usage statistics. Data statistics will display only if enable the Data Allowance function in **Link Manager > Link Setting > WWAN Setting**.

3.7 Interface > LAN

This section allows user to set the related parameters of LAN interfaces.
R3000 Lite's LAN interface IP default to 192.168.0.1.

LAN

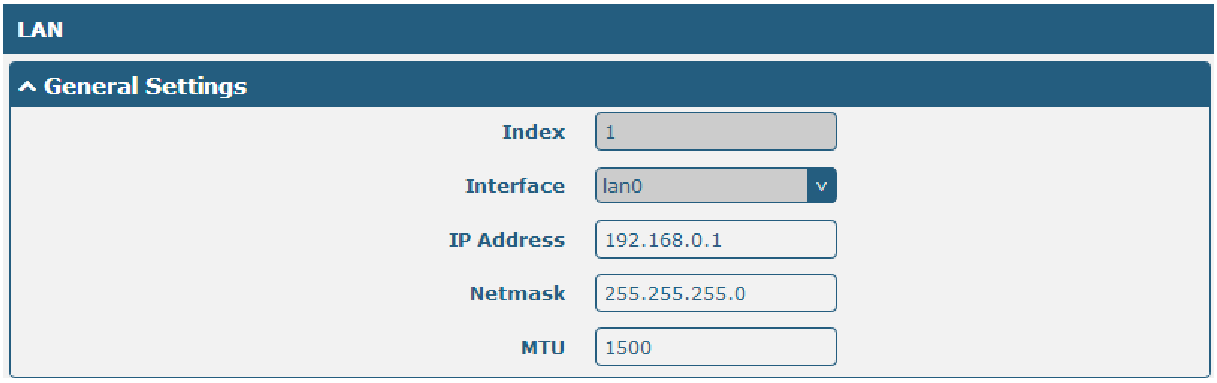


Network Settings

Index	Interface	IP Address	Netmask	+
1	lan0	192.168.0.1	255.255.255.0	✎ ✕

Click ✎ to edit the configuration of the current LAN interface. Click ✕ to delete the current LAN interface.

Note: *Interface lan0 cannot be deleted.*



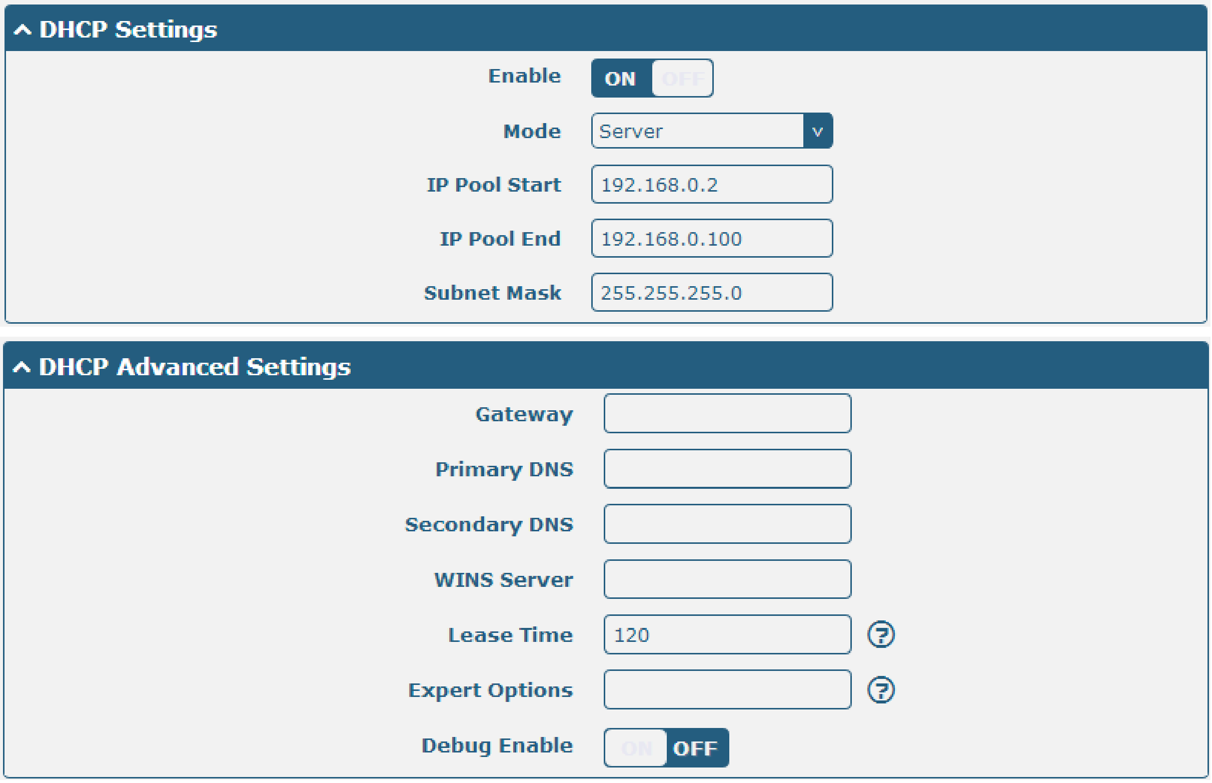
LAN

General Settings

Index	1
Interface	lan0
IP Address	192.168.0.1
Netmask	255.255.255.0
MTU	1500

General Settings		
Item	**Description**	**Default**
Interface	R3000 Lite's LAN interface names lan0.	lan0
IP Address	Set the IP Address of the LAN interface.	192.168.0.1
Netmask	Set the Netmask of the LAN interface.	255.255.255.0
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1500

When select DHCP Mode as Server, the window will display as the following screenshot.



^ DHCP Settings

Enable: ON

Mode: Server

IP Pool Start: 192.168.0.2

IP Pool End: 192.168.0.100

Subnet Mask: 255.255.255.0

^ DHCP Advanced Settings

Gateway:

Primary DNS:

Secondary DNS:

WINS Server:

Lease Time: 120

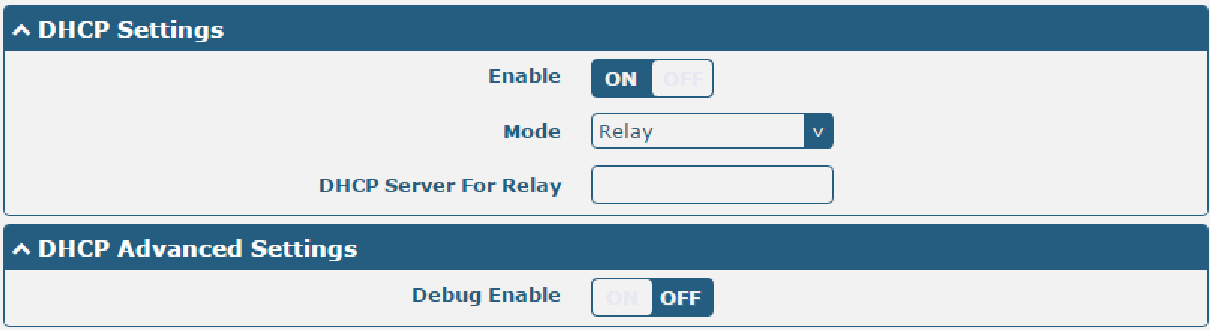
Expert Options:

Debug Enable: OFF

DHCP Server		
Item	**Description**	**Default**
Enable	Click the switch to show "ON" and to enable DHCP function.	ON
Mode	Server: Lease IP address to DHCP clients which connect to LAN. Relay: Router can be DHCP Relay, which will provide a relay tunnel to solve problem that DHCP Client and DHCP Server is not in a same subnet.	DHCP Server
IP Pool Start	Define the beginning of the pool of IP addresses which will lease to DHCP clients.	192.168.0.2
IP Pool End	Define the end of the pool of IP addresses which will lease to DHCP clients.	192.168.0.100
Subnet Mask	Define the Subnet Mask which the DHCP clients will obtain from DHCP server.	255.255.255.0
Gateway	Define the Gateway which the DHCP clients will obtain from DHCP server.	Null
Primary DNS	Define the Primary DNS Server which the DHCP clients will obtain from DHCP server.	Null

DHCP Server		
Item	**Description**	**Default**
Secondary DNS	Define the Secondary DNS Server which the DHCP clients will obtain from DHCP server.	Null
WINS Server	Define the Windows Name Server which the DHCP clients will obtain from DHCP server.	Null
Lease Time	Define the time which the client can use the IP address which obtained from DHCP server.	120
Expert Options	You can enter some other options of DHCP server in this field. format: config-desc;config-desc, e.g. log-dhcp;quiet-dhcp	Null
Debug Enable	Enable this function; it will output the DHCP information to syslog.	OFF

When select DHCP Mode as Relay, the window will display as the following screenshot.



^ DHCP Settings

Enable: ON

Mode: Relay

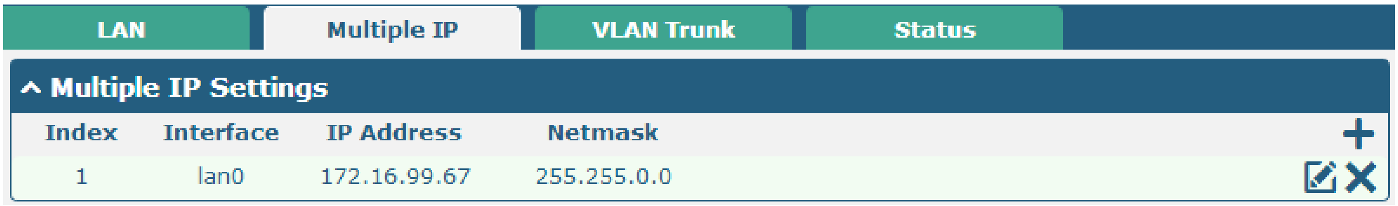
DHCP Server For Relay:

^ DHCP Advanced Settings

Debug Enable: OFF

DHCP Server		
Item	Description	Default
DHCP Server for Relay	Enter the DHCP Relay server IP address.	Null
Debug Enable	Enable this function; it will output the DHCP information to syslog.	OFF

Multiple IP

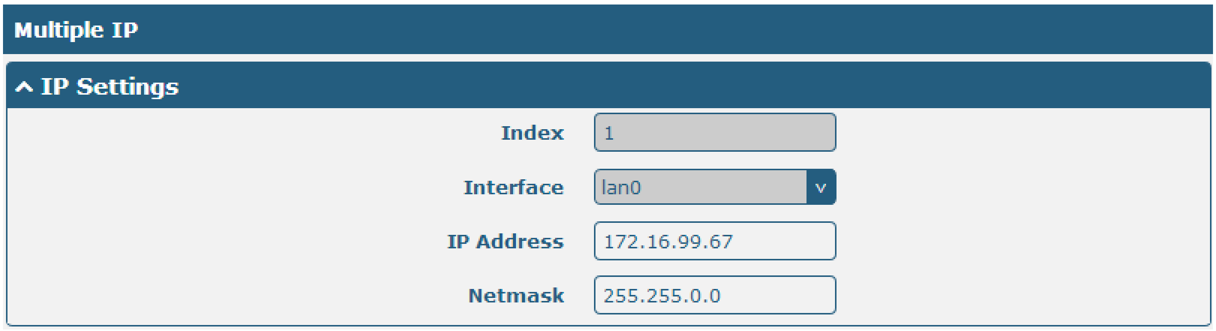


^ Multiple IP Settings

Index	Interface	IP Address	Netmask
1	lan0	172.16.99.67	255.255.0.0

Click ✎ to edit the Multiple IP of the LAN interface. Click ✕ to delete the Multiple IP of the LAN interface.

Click + to add a multiple IP to the LAN interface.



Multiple IP

^ IP Settings

Index: 1

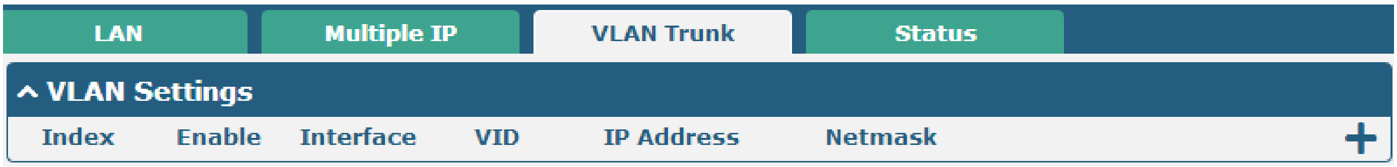
Interface: lan0

IP Address: 172.16.99.67

Netmask: 255.255.0.0

Multiple IP		
Item	**Description**	**Default**
Interface	R3000 Lite's LAN interface names lan0.	lan0
IP Address	Set the multiple IP Address of the LAN interface.	Null
Netmask	Set the multiple Netmask of the LAN interface.	Null

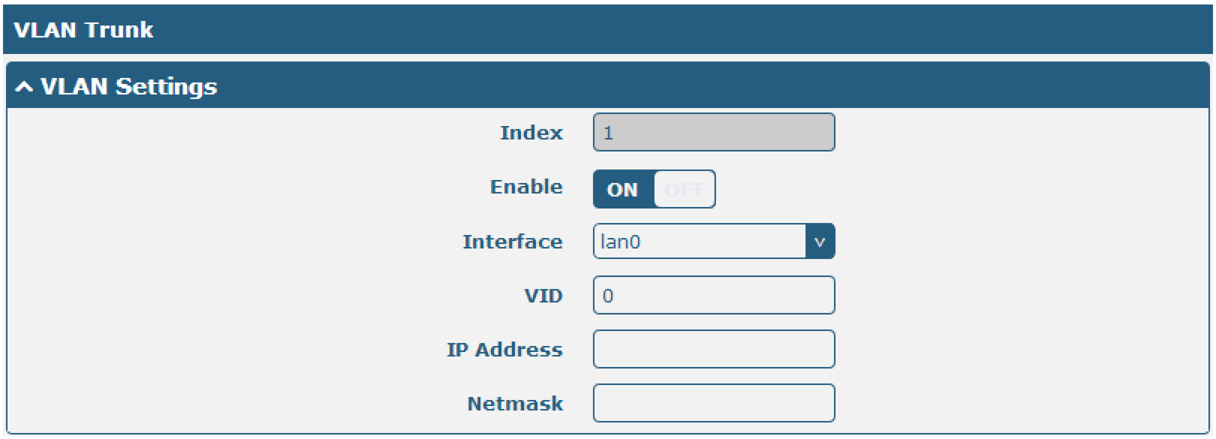
VLAN Trunk



^ VLAN Settings

Index	Enable	Interface	VID	IP Address	Netmask	+

Click + to add a VLAN. The maximum number of the VLAN is eight.



VLAN Trunk

^ VLAN Settings

Index: 1

Enable: ON OFF

Interface: lan0

VID: 0

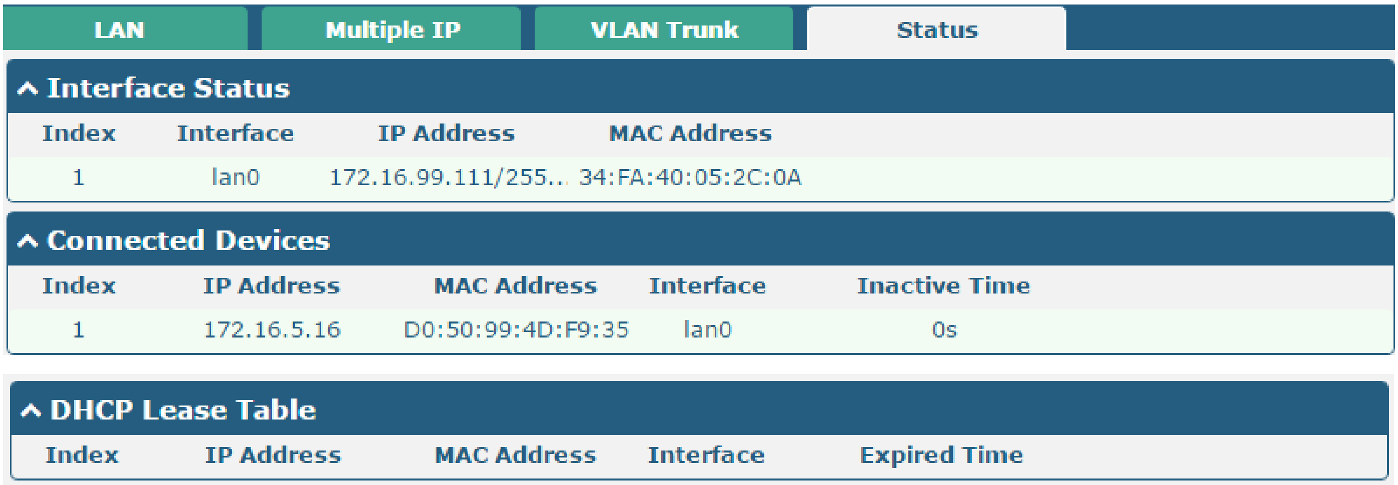
IP Address:

Netmask:

VLAN Trunk		
Item	**Description**	**Default**
Enable	Enable to make router can encapsulate and de-encapsulate the VLAN tag.	ON
Interface	R3000 Lite's LAN interface names lan0.	lan0
VID	Set the Tag ID of VLAN, values range from 1 to 4094.	100
IP Address, Netmask	Set the IP address, Netmask of VLAN interface	Null

Status

This section shows the LAN connection status.



^ Interface Status

Index	Interface	IP Address	MAC Address
1	lan0	172.16.99.111/255..	34:FA:40:05:2C:0A

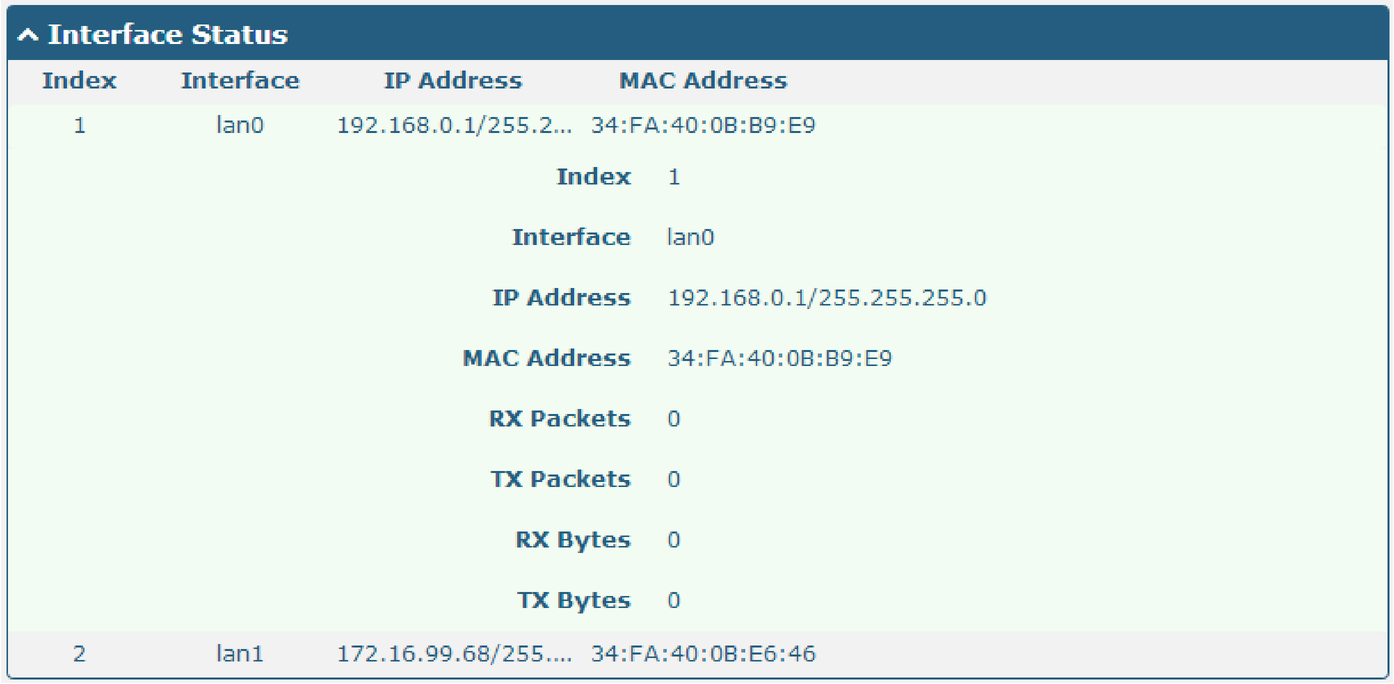
^ Connected Devices

Index	IP Address	MAC Address	Interface	Inactive Time
1	172.16.5.16	D0:50:99:4D:F9:35	lan0	0s

^ DHCP Lease Table

Index	IP Address	MAC Address	Interface	Expired Time

Click the row of status, the details status information will be display under the row. Please refer to the screenshot below.



^ Interface Status

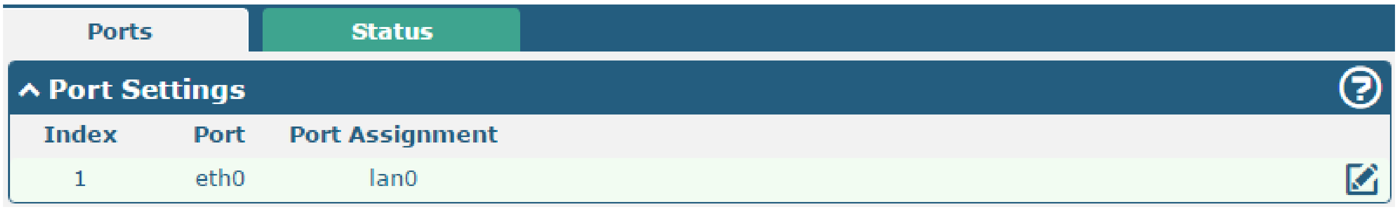
Index	Interface	IP Address	MAC Address
1	lan0	192.168.0.1/255.2...	34:FA:40:0B:B9:E9

Index	1
Interface	lan0
IP Address	192.168.0.1/255.255.255.0
MAC Address	34:FA:40:0B:B9:E9
RX Packets	0
TX Packets	0
RX Bytes	0
TX Bytes	0

Index	Interface	IP Address	MAC Address
2	lan1	172.16.99.68/255....	34:FA:40:0B:E6:46

3.8 Interface > Ethernet

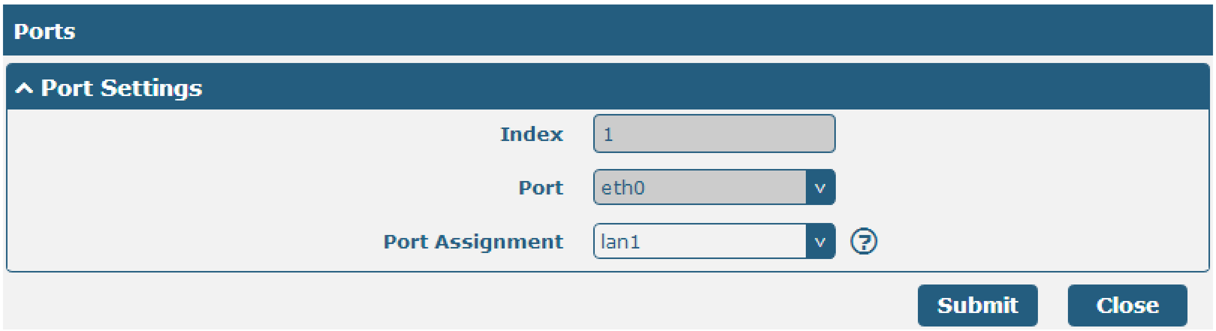
This section allow user to set the parameter of the Ethernet port. One port should be assigned to lan0 a least.



^ Port Settings

Index	Port	Port Assignment
1	eth0	lan0

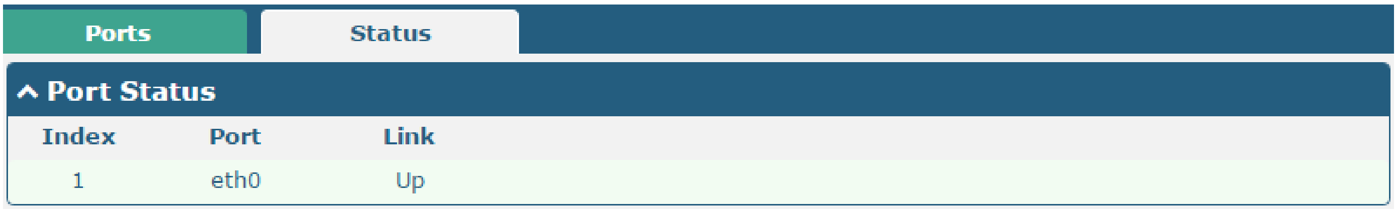
Click ✎ button, configure the port setting.



Index	1
Port	eth0
Port Assignment	lan1

Ethernet		
Item	**Description**	**Default**
Index	The index of Ethernet port. Read only.	1
Port	R3000 Lite's Ethernet port names eth0	eth0
Port Assignment	R3000 Lite's Ethernet port eth0 with be assign to lan0.	lan0

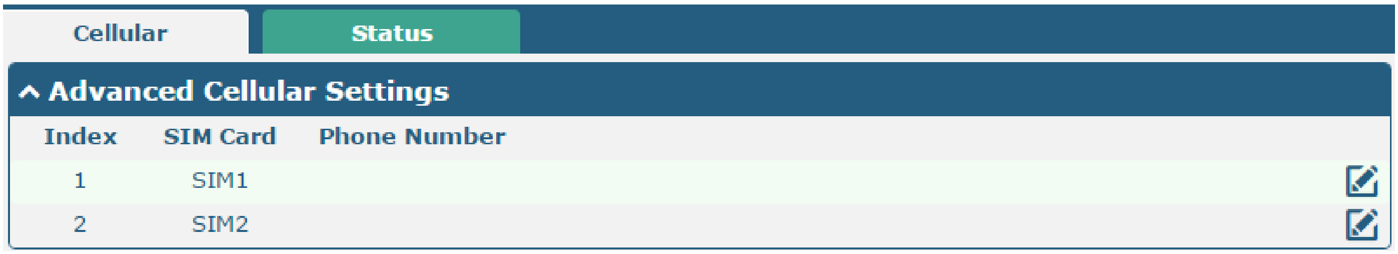
User can check the status of Ethernets in this page.



Index	Port	Link
1	eth0	Up

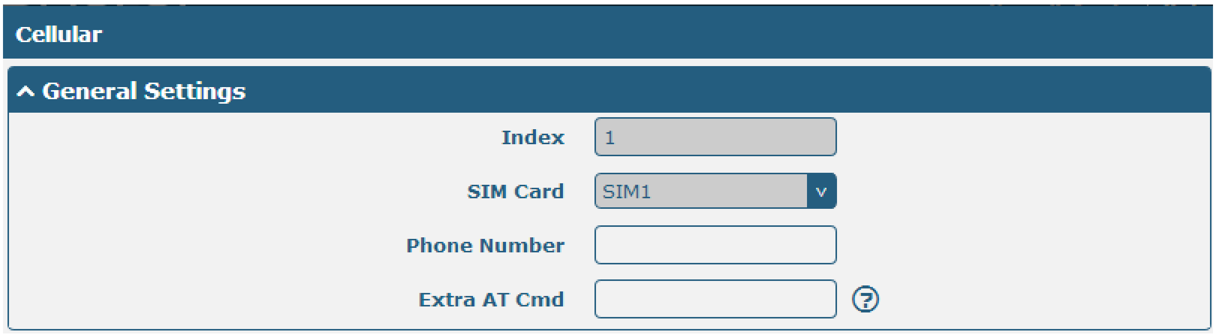
3.9 Interface > Cellular

This section allows users to set the Cellular WAN and the related parameters.
When it is the first time to insert single SIM card, SIM card 1 and SIM card 2 slots are available.



Index	SIM Card	Phone Number
1	SIM1	
2	SIM2	

Click" ✎" to edit the parameters.



Cellular

General Settings

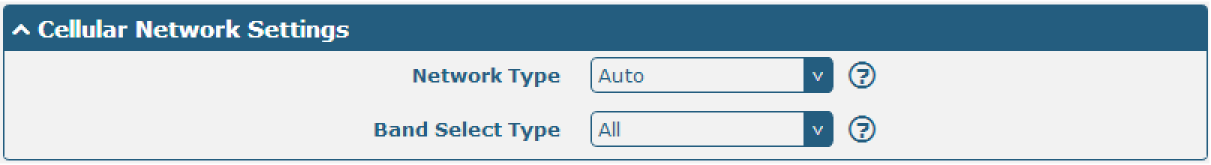
Index: 1

SIM Card: SIM1

Phone Number:

Extra AT Cmd:

When choose “Network Type type” is “Auto”;

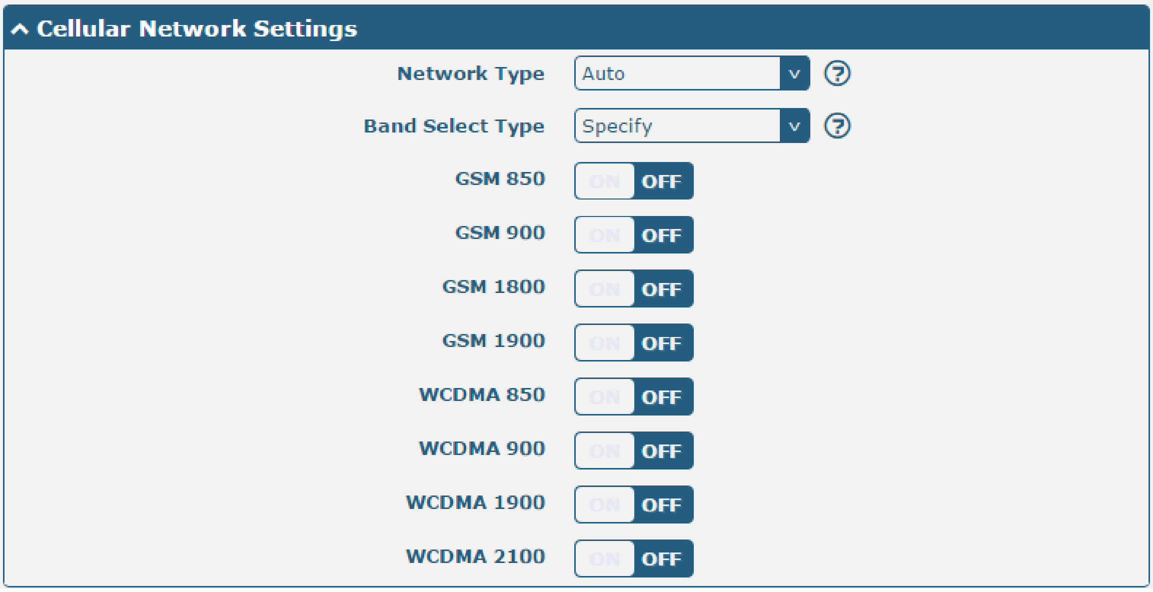


Cellular Network Settings

Network Type: Auto

Band Select Type: All

When choose “band select type” is “Specify”.



Cellular Network Settings

Network Type: Auto

Band Select Type: Specify

GSM 850: OFF

GSM 900: OFF

GSM 1800: OFF

GSM 1900: OFF

WCDMA 850: OFF

WCDMA 900: OFF

WCDMA 1900: OFF

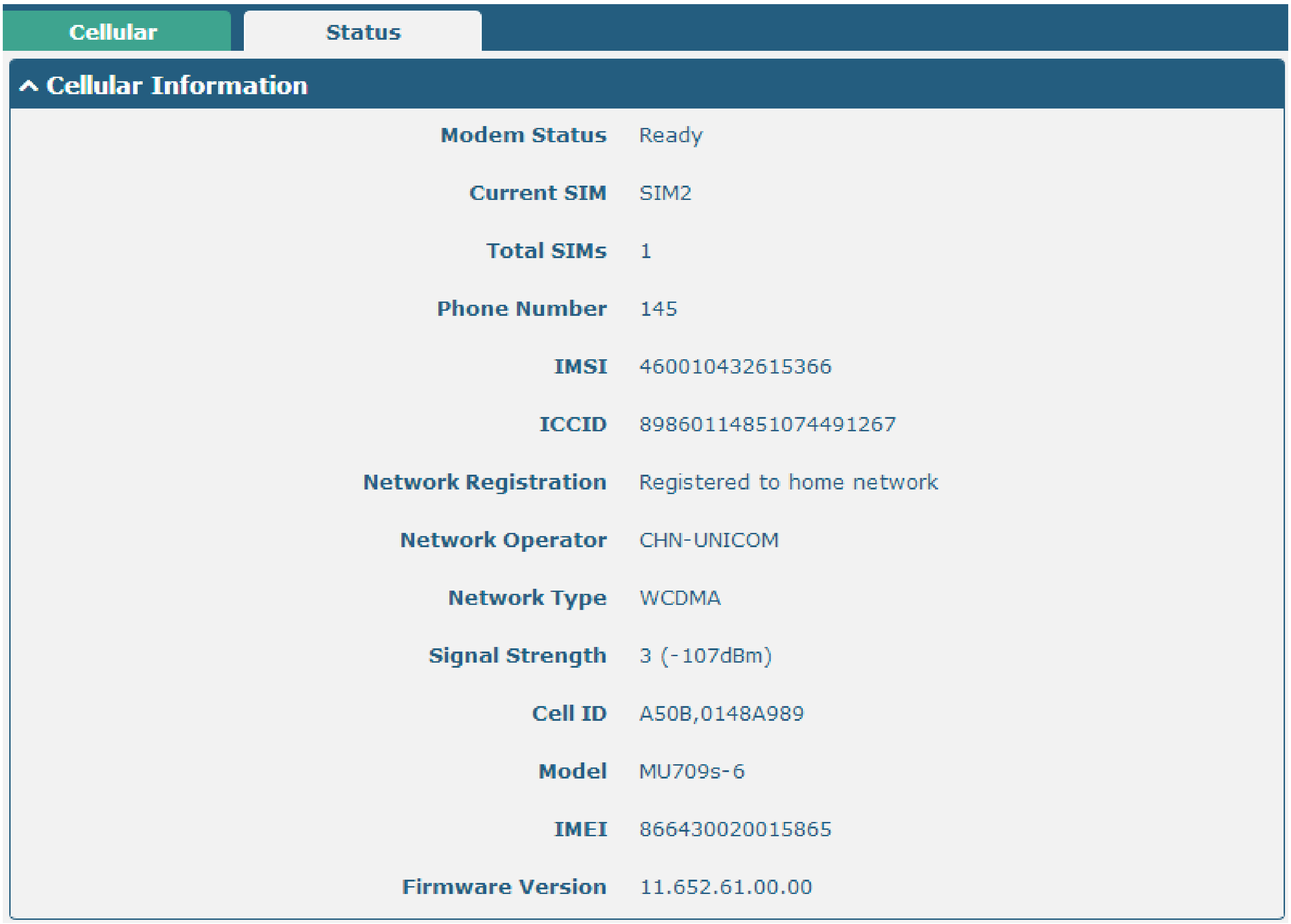
WCDMA 2100: OFF

Cellular		
Item	**Description**	**Default**
Index	Show the index of the SIM.	1
SIM Card	Set the current SIM card.	SIM1
Link Name	Set the current Link Name.	WWAN1
Phone Number	Define the phone number of the SIM card.	Null
Extra AT Cmd	AT commands used for cellular initialization.	Null
Network Type	Select from “Auto”, “4G Only”, “4G First”. Auto: Router will connect to the best signal network when choose Auto as network type. 4G Only: Router only connects to 4G network. 4G First: Router will connect to 4G Network preferentially.	Auto

Cellular		
Item	**Description**	**Default**
Band Select Type	Select from "All", "Specify". When select "Specify", user can choose certain bands.	All

Status

This section allow user to check the cellular status information.



Cellular Information

Modem Status: Ready
Current SIM: SIM2
Total SIMs: 1
Phone Number: 145
IMSI: 460010432615366
ICCID: 89860114851074491267
Network Registration: Registered to home network
Network Operator: CHN-UNICOM
Network Type: WCDMA
Signal Strength: 3 (-107dBm)
Cell ID: A50B,0148A989
Model: MU709s-6
IMEI: 866430020015865
Firmware Version: 11.652.61.00.00

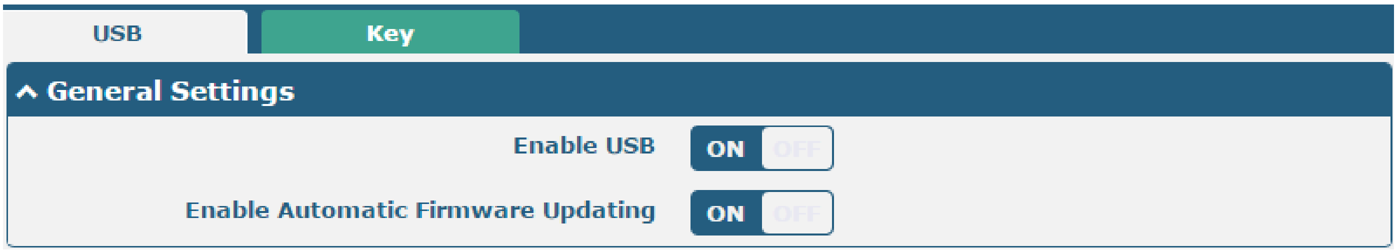
Status	
Item	**Description**
Modem Status	Show the status of the radio module.
Current SIM	Show the SIM card which the router works with currently: SIM1 or SIM2.
Total SIMs	Show the number of SIM cards that is installed in the router.
Phone Number	Show the phone number of the current SIM.
IMSI	Show the IMSI number of the current SIM.
ICCID	Show the ICCID number of the current SIM.
Network Registration	Show the current network status.
Network Operator	Show the name of Network Provider.
Network Type	Show the current network service type, e.g. GPRS.

Status	
Item	**Description**
Signal Strength	Show the current signal strength.
Cell ID	Show the current cell ID, which can locate the router.
Model	Show the model of the radio module.
IMEI	Show the IMEI number of the radio module.
Firmware Version	Show the current firmware version of the radio module.

3.10 Interface > USB

This section allows users to set the USB parameters.

Note: *Users can insert a USB storage device, such as U disk and hard disk, into the router's USB interface. If there is firmware of R3000 Lite inside the USB storage devices, R3000 Lite will automatically update the firmware. We will provide another file "application note" to show how to do USB automatic update.*



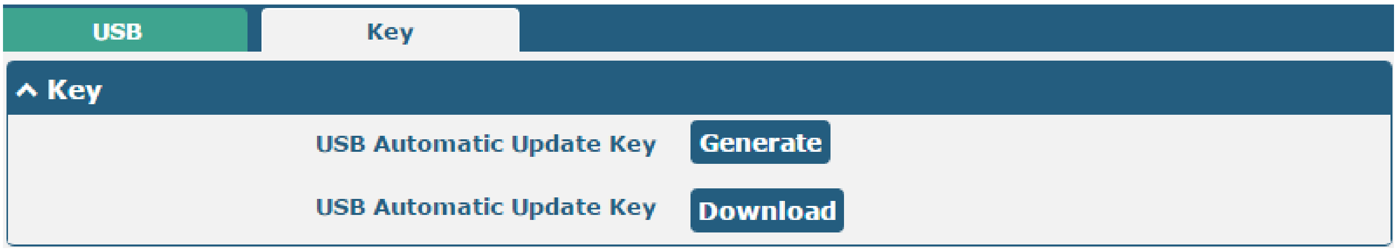
Enable USB: ON

Enable Automatic Firmware Updating: ON

USB		
Item	**Description**	**Default**
Enable USB	Click to enable USB feature.	ON
Enable Automatic Firmware Updating	Click Enable to automatically update the firmware of R3000 Lite when insert the USB storage devices which has R3000 Lite's firmware.	ON

R3000 Lite has the key for USB automatic update. User can generate the key in this page.

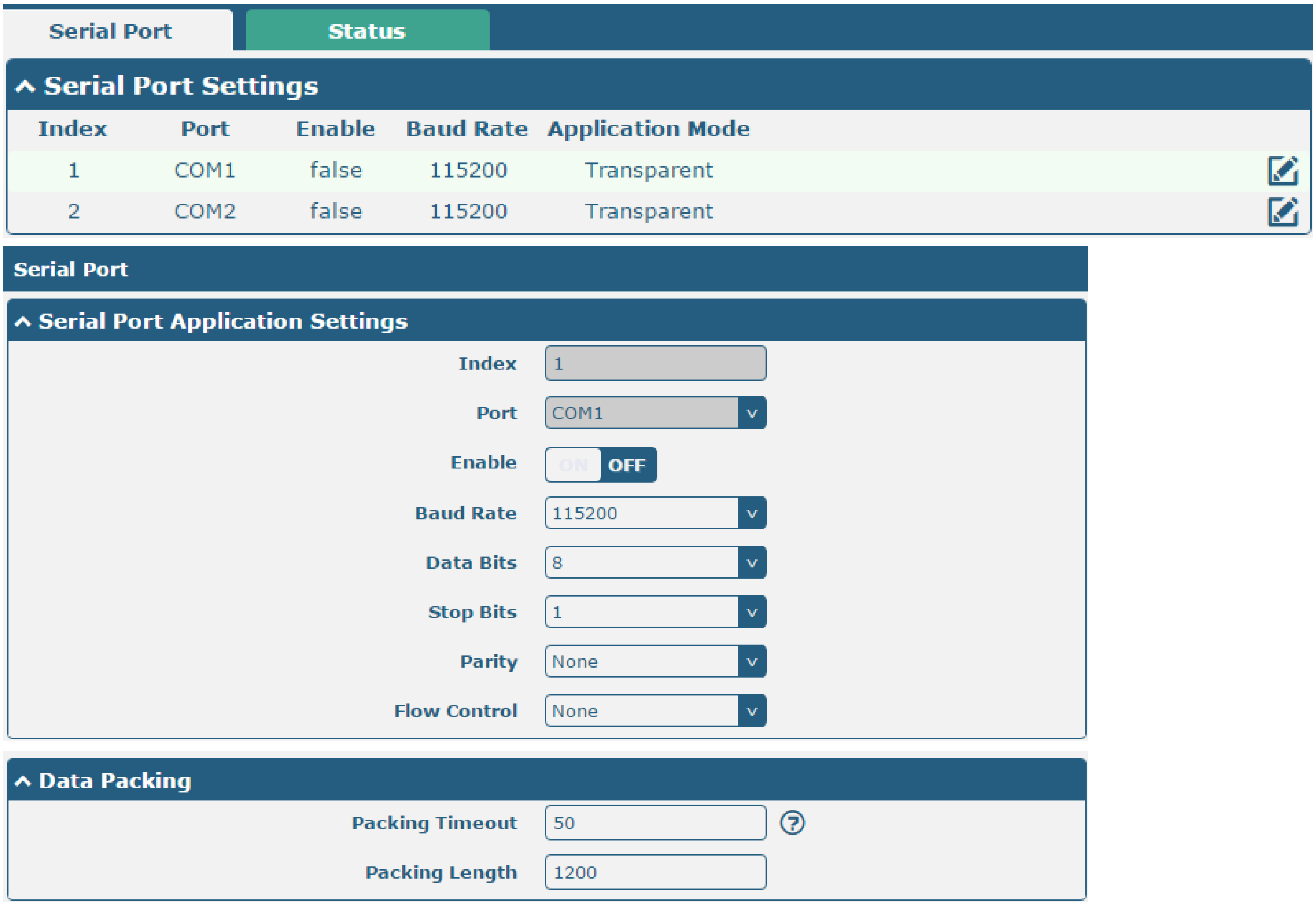
Click Generate , it will generate a key below. Click Download to download the key.



3.11 Interface > Serial Port

This section allows users to set the serial (RS232/RS485) parameters, the type of COM1 is RS232 and the type of COM2 is RS485.

Serial Port



Serial Port Settings

Index	Port	Enable	Baud Rate	Application Mode
1	COM1	false	115200	Transparent
2	COM2	false	115200	Transparent

Serial Port

Serial Port Application Settings

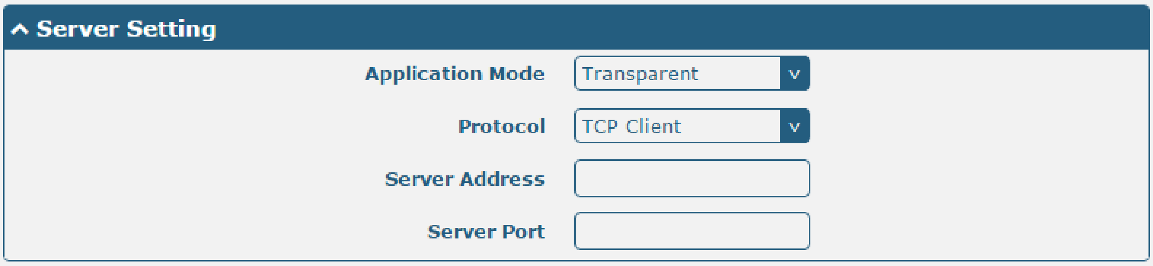
Index	1
Port	COM1
Enable	ON OFF
Baud Rate	115200
Data Bits	8
Stop Bits	1
Parity	None
Flow Control	None

Data Packing

Packing Timeout	50
Packing Length	1200

Serial setting@COM1		
Item	**Description**	**Default**
Port	Show the current serial's name. In default, COM1 is RS232 and COM2 is RS485.	/
Enable	Click to enable this serial port. When the status is OFF, the serial port is not available.	OFF
Baud Rate	Select from "300", "600", "1200", "2400", "4800", "9600", "19200", "38400", "57600" , "115200"and "230400".	115200
Data bit	Select from "7" and "8".	8
Stop bit	Select from "1" and "2".	1
Parity	Select from "None", "Odd" and "Even".	None
Flow control	Select from "None", "Software" and "Hardware".	None
Packing Timeout	The serial port will queue the data in the buffer and send the data to the Cellular WAN/Ethernet WAN when it reaches the Interval Timeout in the field. ***Note***: *Data will also be sent as specified by the packet length even when data is not reaching the interval timeout in the field.*	50
Packing Length	The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. When a packet length between 1 and 3000 bytes is specified, data in the buffer will be sent as	1200

Serial setting@COM1		
Item	**Description**	**Default**
	soon it reaches the specified length.	



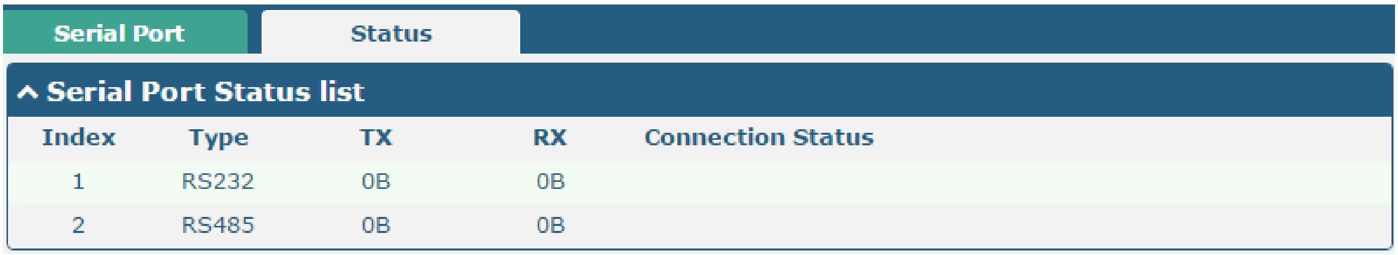
Server Setting

Application Mode	Transparent
Protocol	TCP Client
Server Address	
Server Port	

Server Setting@COM1		
Item	**Description**	**Default**
Application Mode	Select from "Transparent", "Modbus RTU Gateway". • Transparent: Router will transmit the serial data transparently. • Modbus: Router will translate the Modbus RTU data to Modbus TCP data and sent out. Vice versa.	Transparent
Protocol	Select from "TCP Client", "TCP Server", "UDP", "Robustlink". • TCP Client: Router works as TCP client, initiate TCP connection to TCP server. Server address supports both IP and domain name. • TCP Server: Router works as TCP server, listening for connection request from TCP client. • UDP: Router works as UDP client. • Robustlink: Router will automatically upload the serial data to Robustlink platform under the Robustlink protocol. Robustlink is a management platform from Robustel. This function only available when Router is connects to Robustlink.	TCP Client
Server Address	Enter the address of server which will receive the data sent from R3000 Lite's serial port. IP address or domain name will be available.	Null
Server Port	Enter the specified port of server which is use to receive the serial data.	Null

Status

User can check the status of RS232 and RS485. The type of COM1 is RS232 and the type of COM2 is RS485.



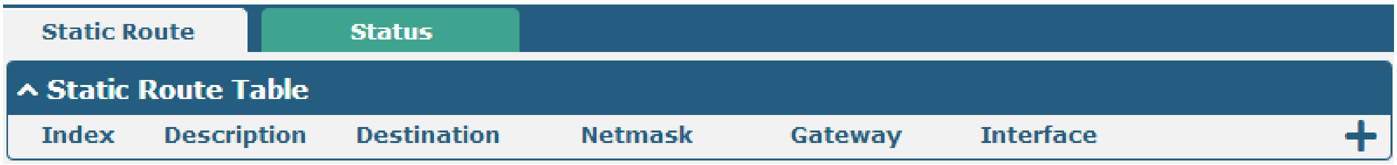
Serial Port Status list

Index	Type	TX	RX	Connection Status
1	RS232	0B	0B	
2	RS485	0B	0B	

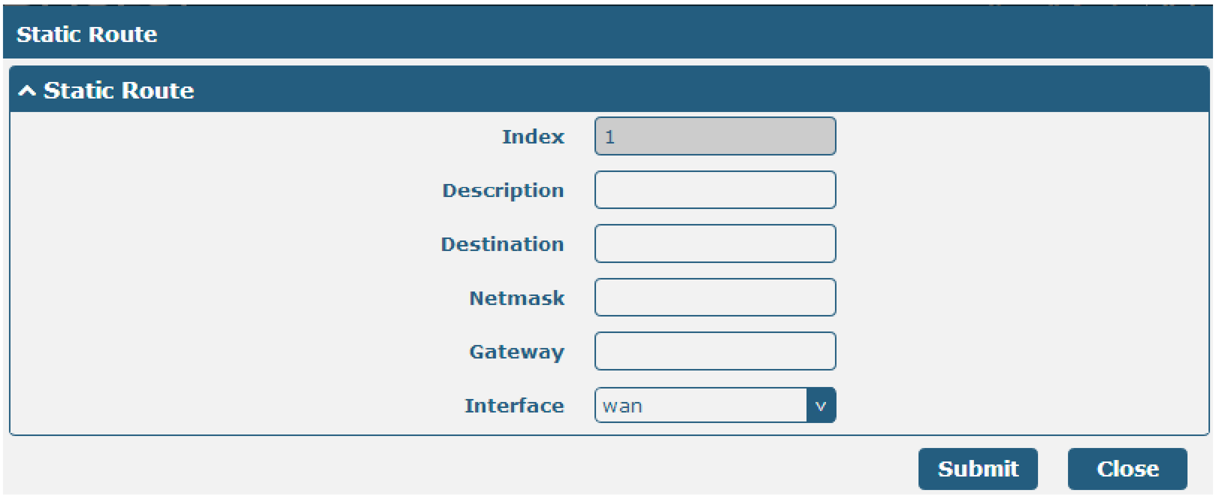
3.12 Network > Route

This section allows user to set the static route. (The maximum number of the static route is twenty.)

Static Route



Click "+" to add static routes, the maximum number of static routes is 20.



Static Route

Static Route

Index: 1

Description:

Destination:

Netmask:

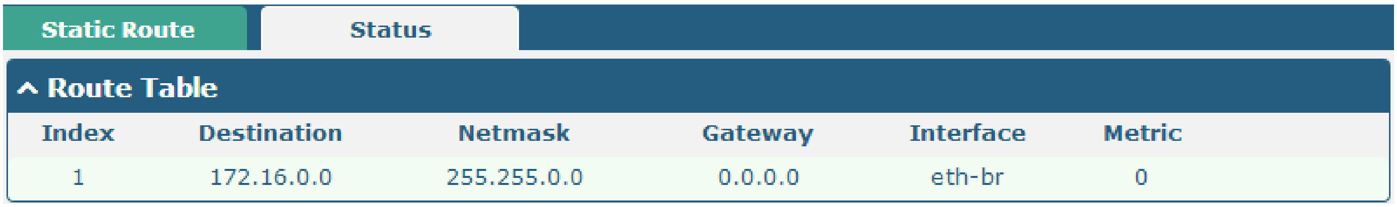
Gateway:

Interface: wan

Static Route		
Item	**Description**	**Default**
Index	Show the index of the static route.	1
Description	Enter some simple words about this route. It can be null.	Null
Destination	Define the destination IP address.	Null
Netmask	Define the Netmask of the destination.	Null
Gateway	Define the gateway of the destination.	Null
Interface	Select from "LAN", "WAN", "TUN"	LAN

Status

User can check the status of route in this page.



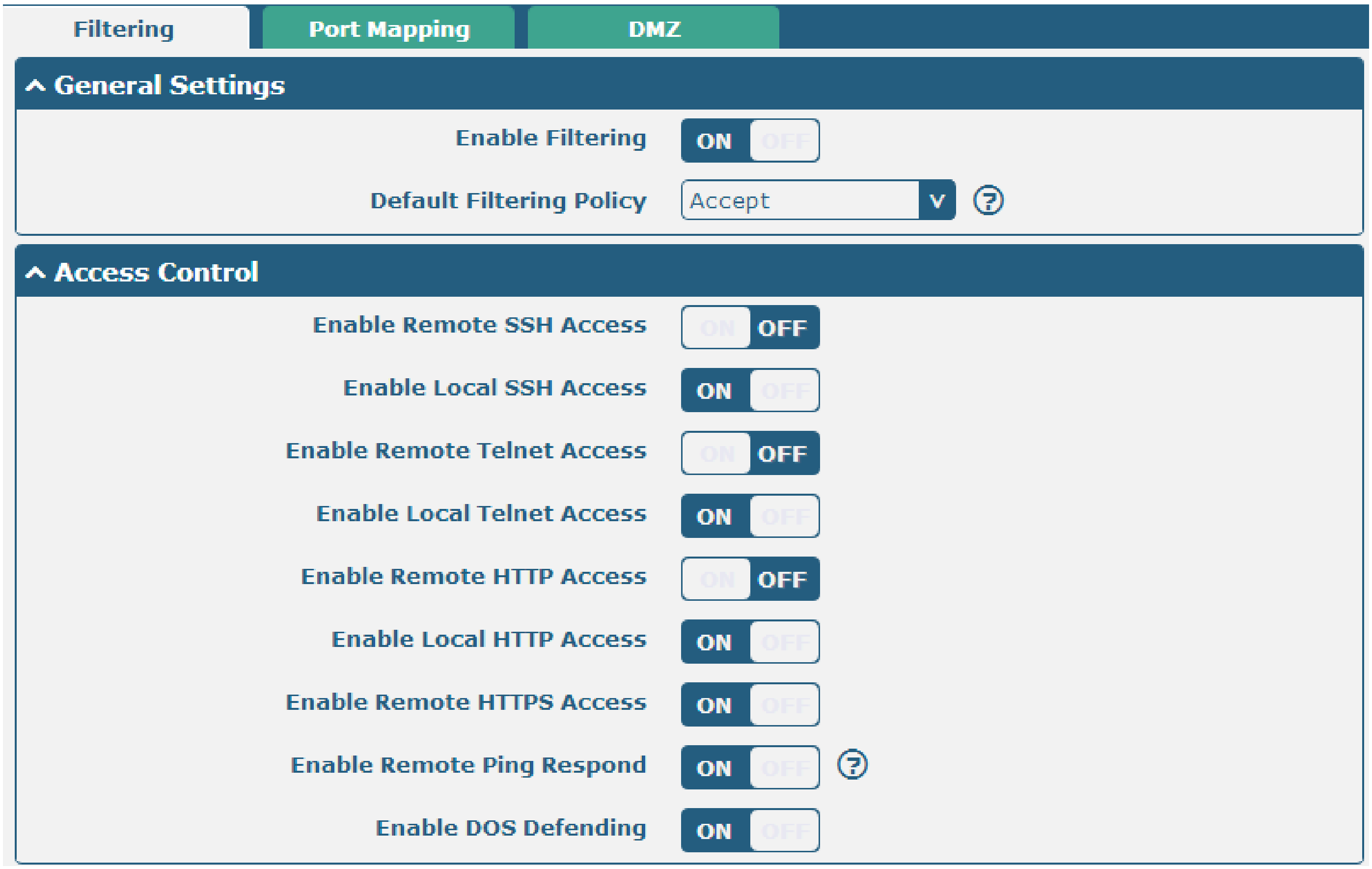
Route Table

Index	Destination	Netmask	Gateway	Interface	Metric
1	172.16.0.0	255.255.0.0	0.0.0.0	eth-br	0

3.13 Network > Firewall

This section allows users to set the Firewall and the related parameters, which includes "Filter", "Port Mapping" and "DMZ".

Filtering



General Settings

Enable Filtering: ON

Default Filtering Policy: Accept

Access Control

Enable Remote SSH Access: OFF

Enable Local SSH Access: ON

Enable Remote Telnet Access: OFF

Enable Local Telnet Access: ON

Enable Remote HTTP Access: OFF

Enable Local HTTP Access: ON

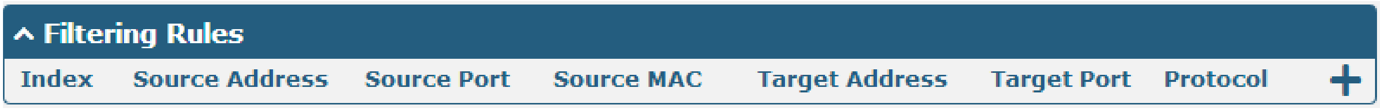
Enable Remote HTTPS Access: ON

Enable Remote Ping Respond: ON

Enable DOS Defending: ON

General Setting & Access Control		
Item	**Description**	**Default**
Enable Filtering	Enable filtering rules.	ON
Default Filtering Policy	Select from “Accept” and “Drop”. Cannot be changed when filtering rules table is not empty. Accept: Router will accept all the connecting requests except the hosts which fit the drop filter list. Drop: Router will drop all the connecting requests except the hosts which fit the accept filter list.	accept
Enable Remote SSH Access	Enable to allow users to access the router remotely on the internet side via SSH.	OFF
Enable Local SSH Access	Enable to allow users to access the router on the local Ethernet via SSH.	ON
Enable Remote Telnet Access	Enable to allow users to access the router remotely on the internet side via Telnet.	OFF
Enable Local Telnet Access	Enable to allow users to access the router on the local Ethernet via Telnet.	ON

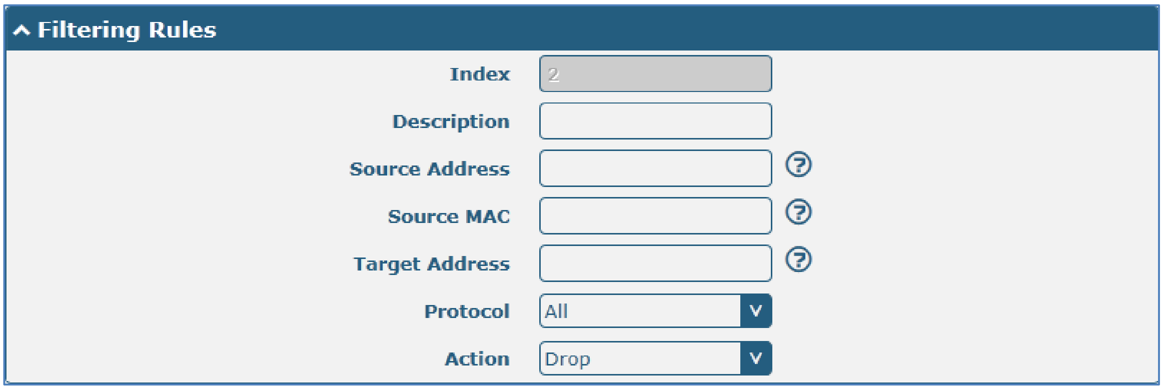
General Setting & Access Control		
Item	**Description**	**Default**
Enable Remote Http Access	Enable to allow users to access the router remotely on the internet side via Http.	OFF
Enable Local Http Access	Enable to allow users to access the router on the local Ethernet via Http.	ON
Enable Remote Https Access	Enable to allow users to access the router remotely on the internet side via Https.	ON
Enable Remote Ping Respond	Enable to make router reply the Ping requests from the internet side.	ON
Enable DOS Defending	Enable to defend dos attack. Dos attack is an attempt to make a machine or network resource unavailable to its intended users.	ON



^ Filtering Rules

Index	Source Address	Source Port	Source MAC	Target Address	Target Port	Protocol	+

Click "+" to add filtering rules. (The maximum number of the filtering rule is twenty.)



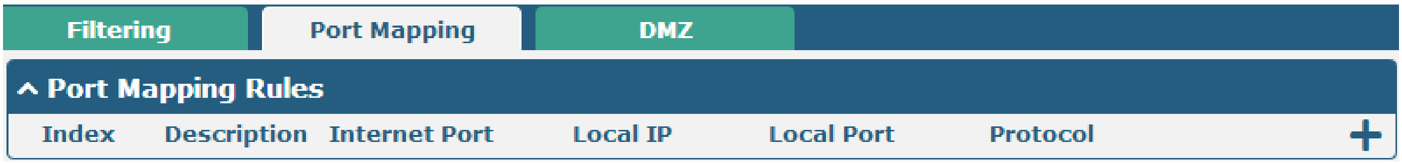
^ Filtering Rules

Index	2
Description	
Source Address	
Source MAC	
Target Address	
Protocol	All
Action	Drop

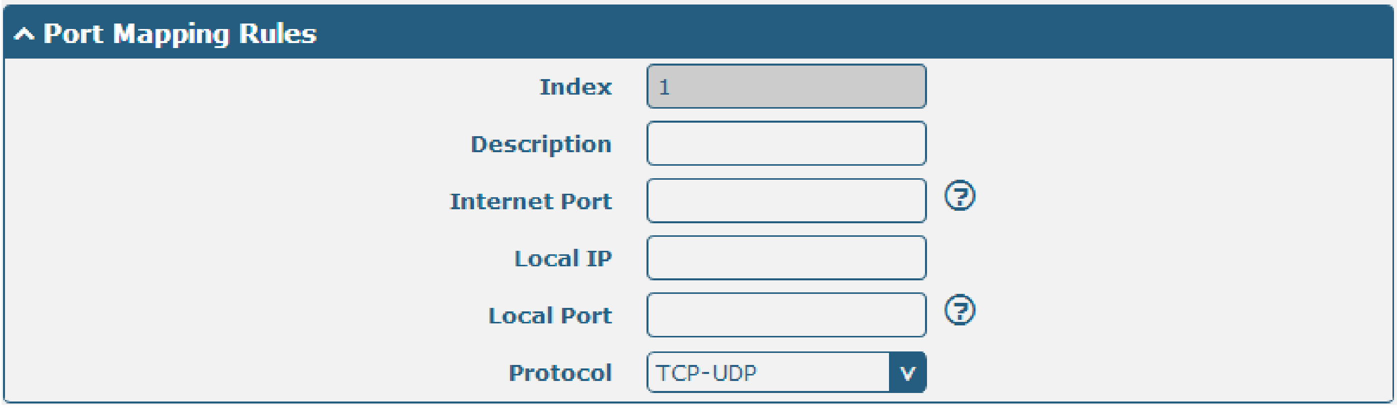
Filtering Rules		
Item	**Description**	**Default**
Index	Show the index of the filtering rule or the MAC binding rule.	1
Description	Enter some simple words about this filtering rule. It can be null.	Null
Source Address	Defines if access is allowed from one or a range of IP addresses which are defined by Source IP Address, or every IP addresses.	Null
Source MAC	Enter the MAC address of the defined source IP address.	Null
Target Address	Defines if access is allowed to one or a range of IP addresses which are defined by Target IP Address, or every IP addresses.	Null
Protocol	Select from "All", "TCP", "UDP", "ICMP", "TCP-UDP". If you don't know what kinds of protocol of your application, we recommend you select "ALL".	All

Filtering Rules		
Item	**Description**	**Default**
Action	Select from “Accept”, “Drop”. Accept: When Default Filtering Policy is drop, router will drop all the connecting requests except the hosts which fit this accept filtering list. Drop: When Default Filtering Policy is accept, router will accept all the connecting requests except the hosts which fit this drop filtering list.	Drop

Port Mapping



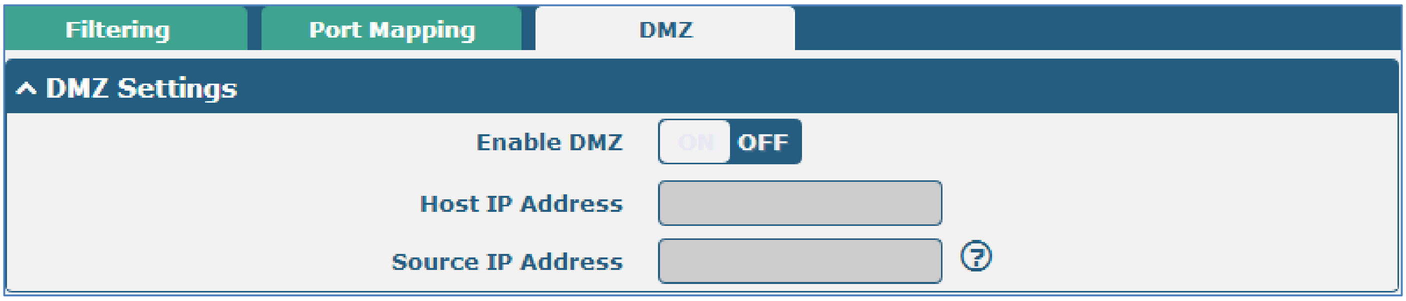
Click “+” to add port mapping rules. (The maximum number of the port mapping rule is forty.)


Port Mapping Rules

Index	1
Description	
Internet Port	
Local IP	
Local Port	
Protocol	TCP-UDP

Port Mapping		
Item	**Description**	**Default**
Index	Show the index of the port mapping rule.	1
Description	Enter some simple words about this port mapping. It can be null.	Null
Internet Port	Set the internet port of router which can be accessed by other hosts from internet.	Null
Local IP	Enter router’s LAN IP which will forward to the internet port of router.	Null
Local Port	Enter the port of router’s LAN IP.	Null
Protocol	Select from “TCP”, “UDP” and “TCP-UDP”.	TCP-UDP

DMZ



Enable DMZ: ON OFF

Host IP Address

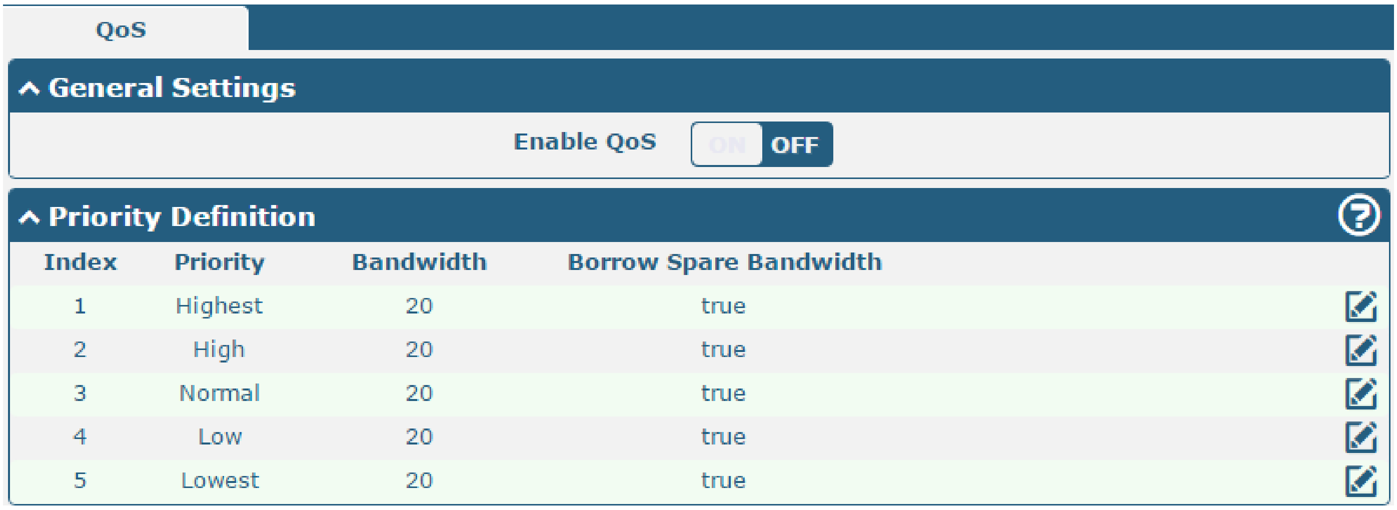
Source IP Address

DMZ		
Item	Description	Default
Enable DMZ	Select to enable the DMZ function. DMZ host is a host on the internal network that has all ports exposed, except those ports otherwise forwarded.	OFF
Host IP Address	Enter the IP address of the DMZ host which on the internal network.	Null
Source IP Address	Set the address which can talk to the DMZ host. Null means for any addresses.	Null

3.14 Network > QoS

This section allows users to set the QoS parameters.

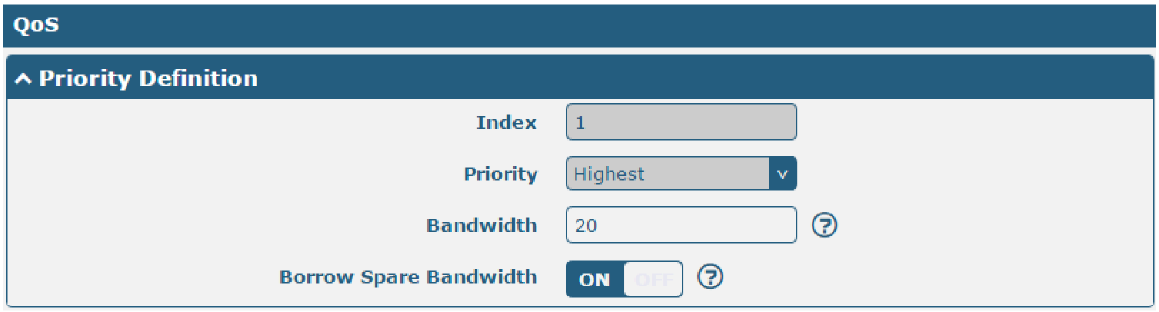
Please remember to set QoS upload and download bandwidth in the **Interface > Link Manager WWAN/WAN** before Configure Qos parameters.



Enable QoS: ON OFF

Index	Priority	Bandwidth	Borrow Spare Bandwidth
1	Highest	20	true
2	High	20	true
3	Normal	20	true
4	Low	20	true
5	Lowest	20	true

Select the priority, click ✎ to enter the priority definition configuration window.



QoS

^ Priority Definition

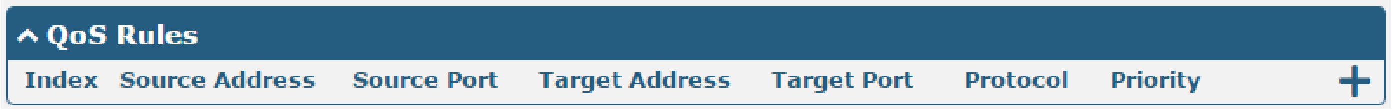
Index: 1

Priority: Highest

Bandwidth: 20

Borrow Spare Bandwidth: ON

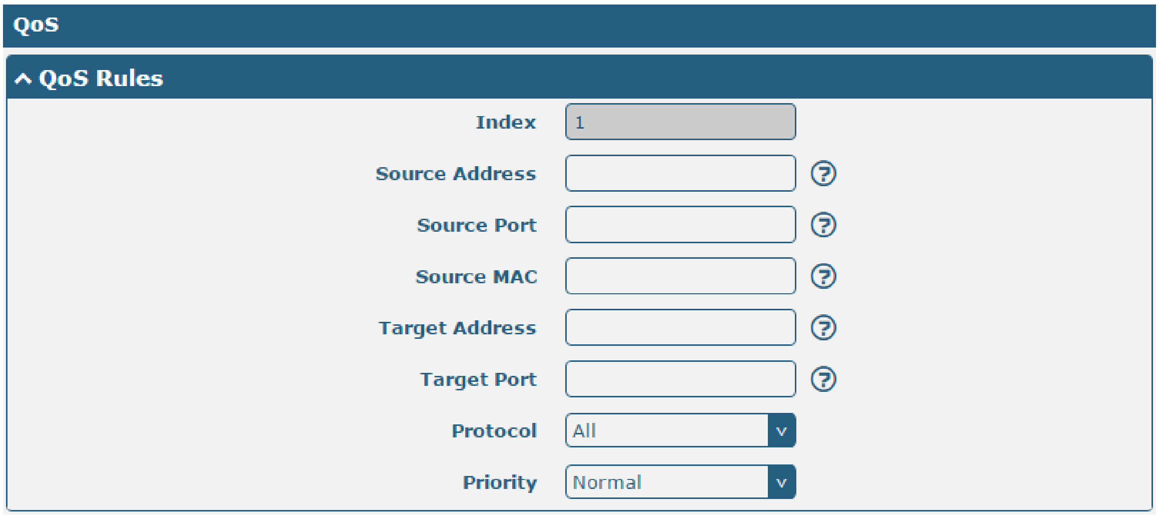
QoS		
Item	**Description**	**Default**
Enable QoS	Click to enable “QoS” function.	Disable
Index	Show the index of priority.	/
Priority	Select from “Highest”, “High”, “Normal”, “Low”, “Lowest”. User can select the priority level according to the requirement.	/
Bandwidth	Define bandwidth percent of “Highest”, “High”, “Normal”, “Low” and “Lowest”. All the bandwidth percent of priority are defaulted to 20%. User can configure the bandwidth percent of priority according to the requirement. The sum of bandwidth of all the priorities cannot be greater than 100%.	20
Borrow Spare Bandwidth	The traffic associated with this priority will borrow unused bandwidth from other priorities when this function is enabled, and will be limited to the specified bandwidth when this function is disabled. Limited specified bandwidth algorithm: priority defined percent x uoad/download bandwidth set in **Interface > Link Manager WWAN/WAN.**	ON



^ QoS Rules

Index	Source Address	Source Port	Target Address	Target Port	Protocol	Priority	+

Click + to add a new QoS rule.



QoS

^ QoS Rules

Index: 1

Source Address:

Source Port:

Source MAC:

Target Address:

Target Port:

Protocol: All

Priority: Normal

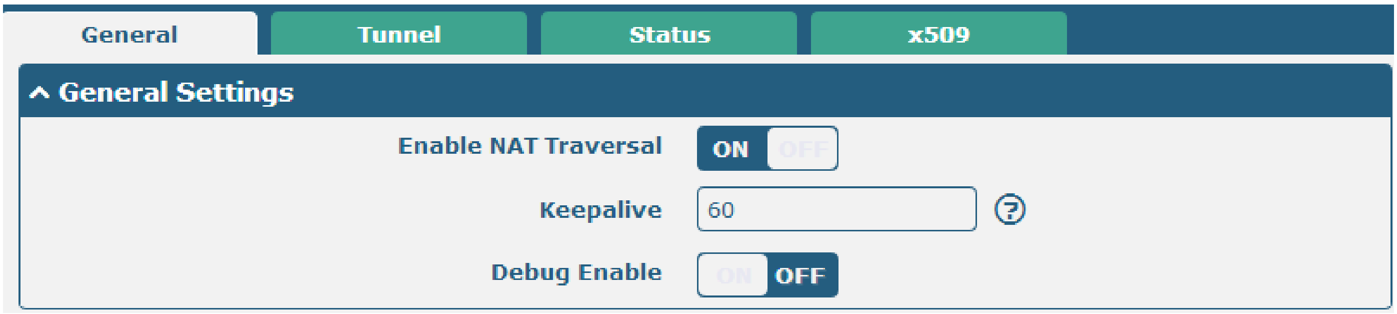
QoS		
Item	**Description**	**Default**
Source Address	Enter the IP address of the source host. format: x.x.x.x, x.x.x.x/xx, x.x.x.x-x.x.x.x, empty means anywhere	Null
Source Port	Enter the port number of the source host.	Null
Source MAC	Enter MAC address of the source host. Router supports up to 20 users set with QoS MAC Control. Priority of QoS MAC Control is higher than that of QoS IP control.	Null
Target Address	Enter the IP address of the target host.	
Target Port	Enter the port number of the target host.	
Protocol	Select from "All", "TCP", "UDP", "ICMP" and "TCP&UDP".	All
Priority	Select from "Highest", "High", "Normal", "Low", "Lowest". Those priorities had been defined in **Network > QoS > Priority Definition**.	Normal

Note:
1. *If services are in the same priority level, router will automatically start Stochastic Fairness Queueing (SFQ) strategy to make a fair bandwidth allocation.*
2. If the link between a source host and target host had set QoS 3 rules. At this time it won't consider the priority but will only choose the ranked first one to take effect.

3.15 VPN > IPSec

This section allows users to set the IPSec and the related parameters.

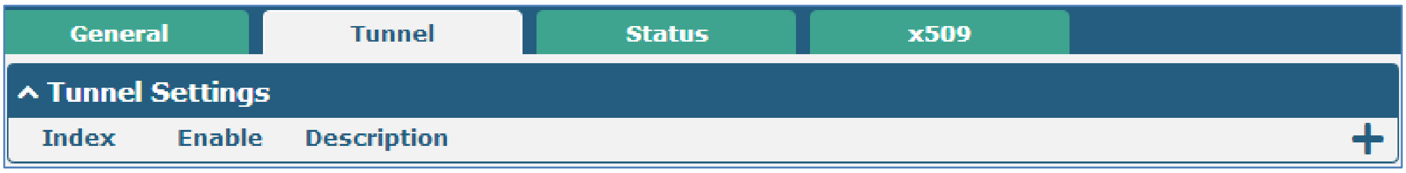
General



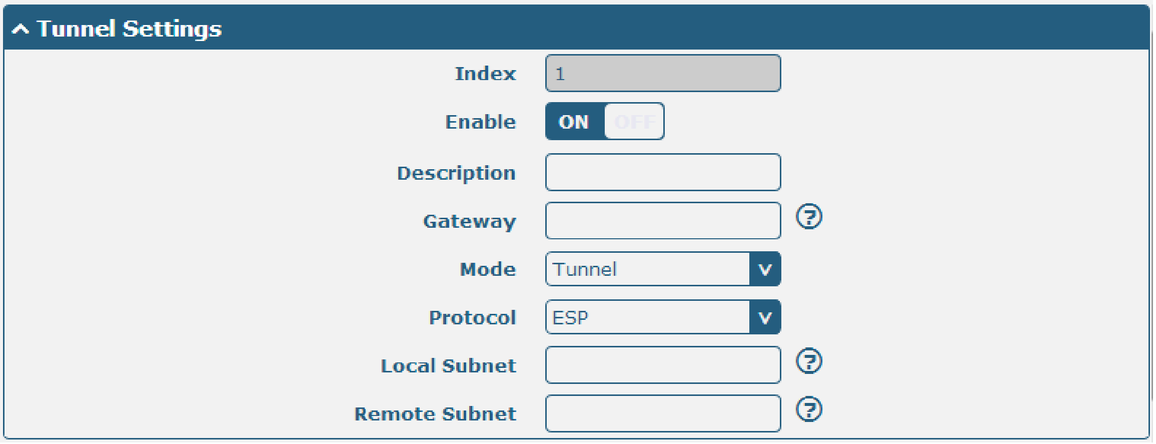
Enable NAT Traversal: ON
Keepalive: 60
Debug Enable: OFF

General		
Item	**Description**	**Default**
Enable NAT Traversal	Tick to enable NAT Traversal for IPSec. This item must be enabled when router under NAT environment.	ON
Keepalive	The interval that router sends packets to NAT box so that to avoid it remove the NAT mapping.	60
Debug Enable	Enable this function, and it will output IPSec information to the debug port.	OFF

Tunnel



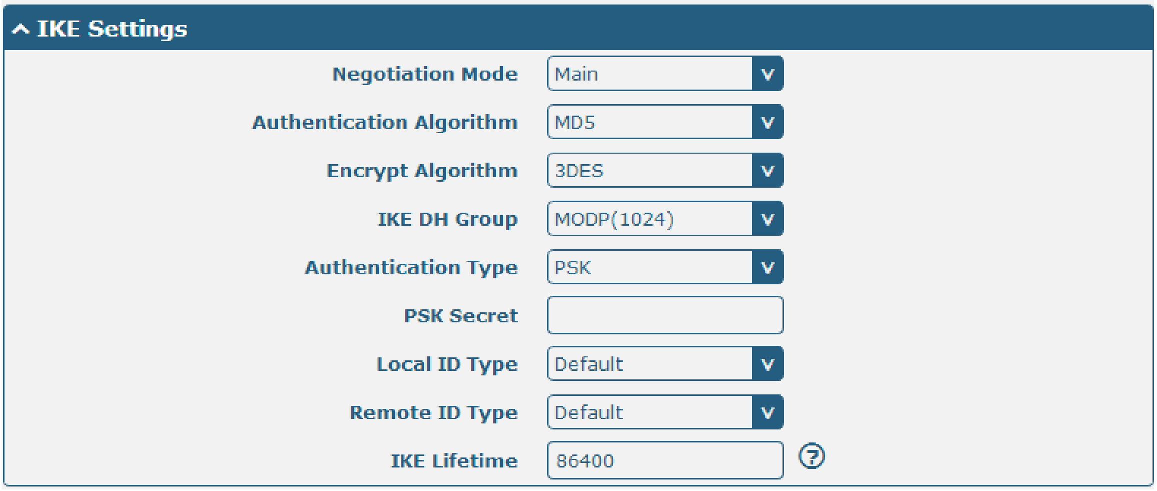
Click “+” to add tunnel settings. (The maximum number of the tunnel is three.)



Index 1
Enable ON OFF
Description
Gateway
Mode Tunnel
Protocol ESP
Local Subnet
Remote Subnet

Tunnel Settings		
Item	**Description**	**Default**
Index	Show the index of the tunnel.	1
Enable	Enable IPSec Tunnel.	ON
Description	Enter some simple words about the IPSec Tunnel.	Null
Gateway	Enter the address of remote side IPSec VPN server.	Null
Mode	Select from “Tunnel” and “Transport”. Tunnel: Commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it. Transport: Used between end-stations or between an end-station and a gateway, if the gateway is being treated as a host-for example, an encrypted Telnet session from a workstation to a router, in which the router is the actual destination.	Tunnel
Protocol	Select the security protocols from “ESP” and “AH”. ESP: Uses the ESP protocol. AH: Uses the AH protocol.	ESP
Local Subnet	Enter IPSec Local Protected subnet’s address with mask, e.g. 192.168.1.0/24	Null
Remote Subnet	Enter IPSec Remote Protected subnet’s address with mask, e.g. 10.8.0.0/24	Null

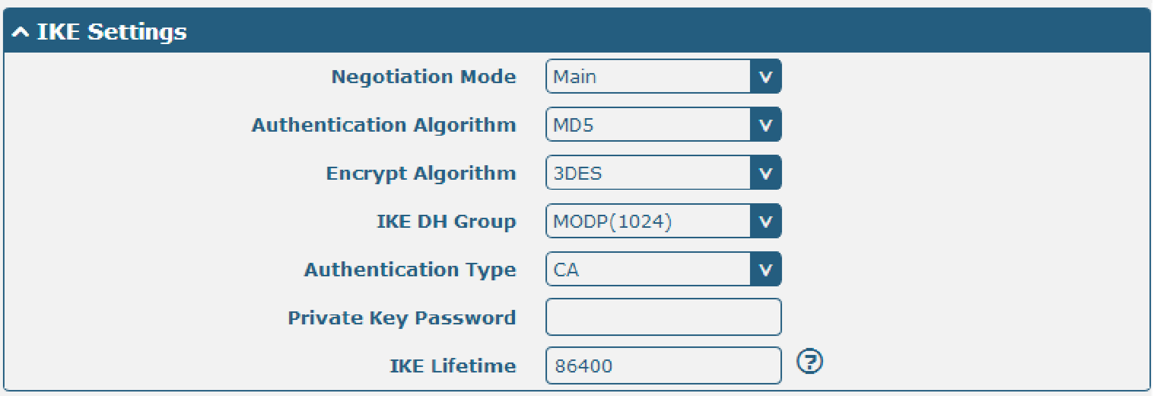
When choose “Authentication Type” to “PSK”.



^ IKE Settings

Negotiation Mode	Main
Authentication Algorithm	MD5
Encrypt Algorithm	3DES
IKE DH Group	MODP(1024)
Authentication Type	PSK
PSK Secret	
Local ID Type	Default
Remote ID Type	Default
IKE Lifetime	86400

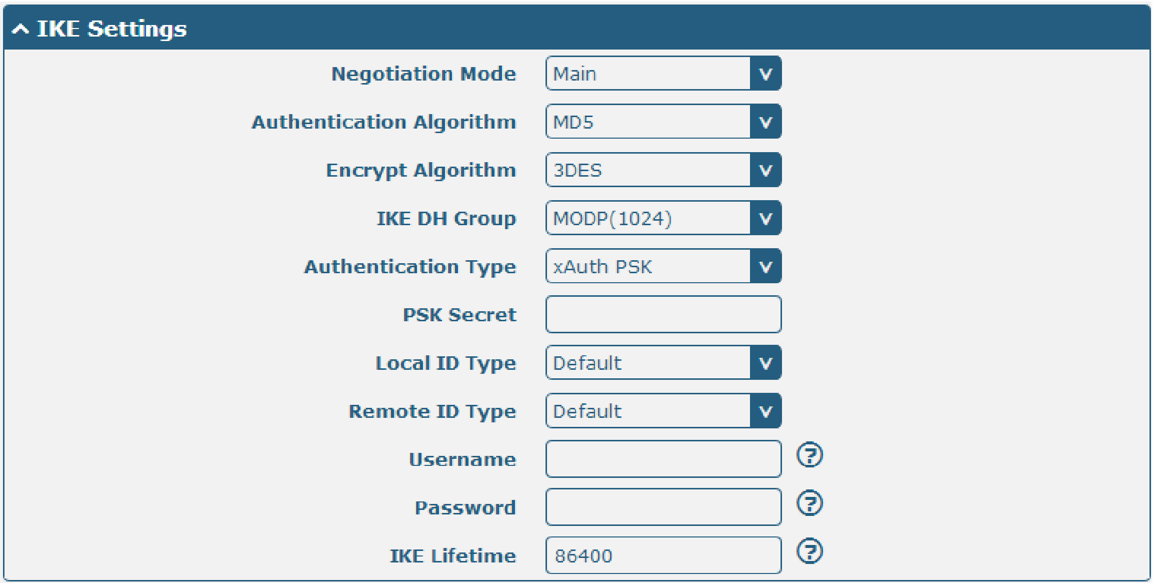
When choose “Authentication Type” to “CA”.



^ IKE Settings

Negotiation Mode	Main
Authentication Algorithm	MD5
Encrypt Algorithm	3DES
IKE DH Group	MODP(1024)
Authentication Type	CA
Private Key Password	
IKE Lifetime	86400

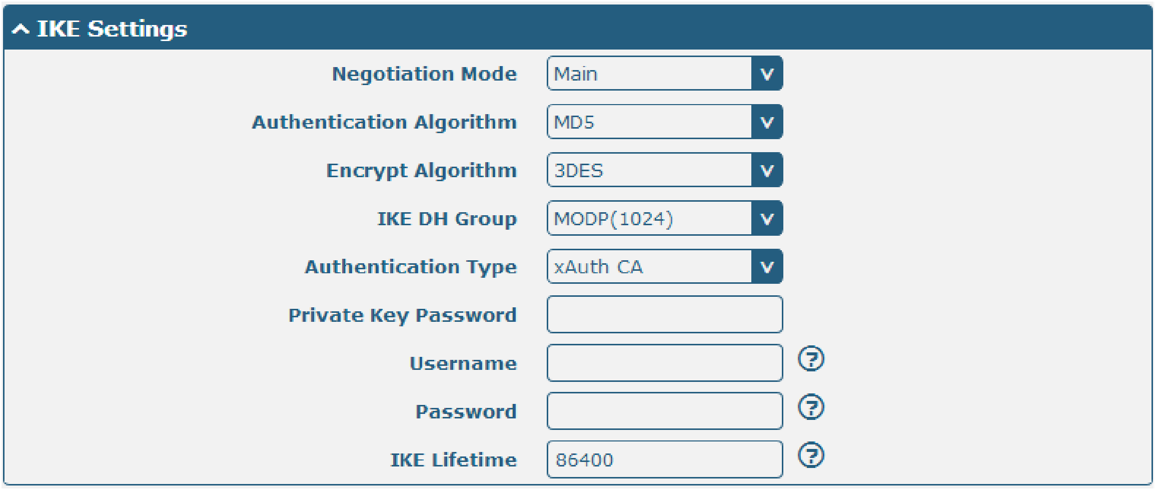
When choose “Authentication Type” to “xAuth PSK”.



^ IKE Settings

Negotiation Mode	Main
Authentication Algorithm	MD5
Encrypt Algorithm	3DES
IKE DH Group	MODP(1024)
Authentication Type	xAuth PSK
PSK Secret	
Local ID Type	Default
Remote ID Type	Default
Username	
Password	
IKE Lifetime	86400

When choose “Authentication Type” to “xAuth CA”.



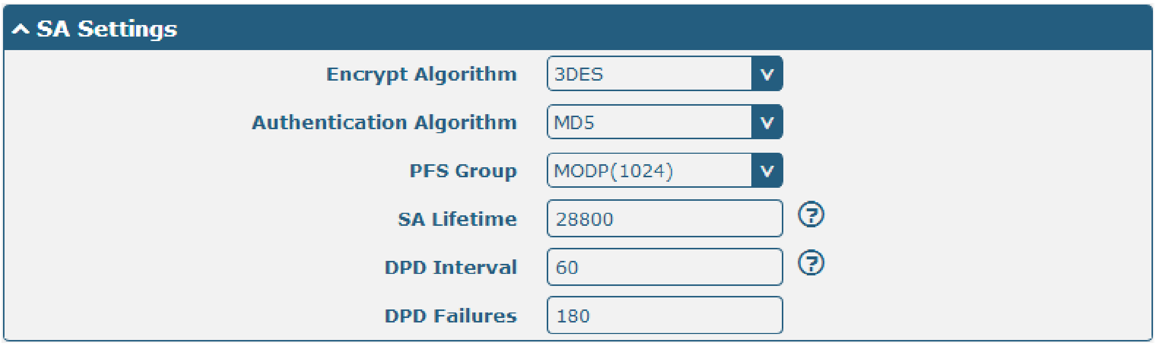
IKE Settings

Negotiation Mode	Main
Authentication Algorithm	MD5
Encrypt Algorithm	3DES
IKE DH Group	MODP(1024)
Authentication Type	xAuth CA
Private Key Password	
Username	
Password	
IKE Lifetime	86400

IKE Settings		
Item	**Description**	**Default**
Negotiation Mode	Select from “Main” and “Aggressive” for the IKE negotiation mode in phase 1. If the IP address of one end of an IPSec tunnel is obtained dynamically, the IKE negotiation mode must be aggressive. In this case, SAs can be established as long as the username and password are correct.	Main
Authentication Algorithm	Select from “MD5” and “SHA1”to be used in IKE negotiation. MD5: Uses HMAC-SHA1. SHA1: Uses HMAC-MD5.	MD5
Encrypt Algorithm	Select from “3DES”, “AES128” and “AES256”to be used in IKE negotiation. 3DES: Uses the 3DES algorithm in CBC mode and 168-bit key. AES128: Uses the AES algorithm in CBC mode and 128-bit key. AES256: Uses the AES algorithm in CBC mode and 256-bit key.	3DES
IKE DH Group	Select from “MODP (1024)” and “MODP (1536)”to be used in key negotiation phase 1. MODP (1024): Uses the 1024-bit Diffie-Hellman group. MODP (1536): Uses the 1536-bit Diffie-Hellman group.	MODP (1024)
Authentication Type	Select from “PSK”, “CA”, “xAuth PSK” and “xAuth CA” to be used in IKE negotiation. PSK: Pre-shared Key. CA: Certification Authority. xAuth: Extended Authentication to AAA server.	PSK
PSK Secret	Enter the pre-shared key.	Null
Local ID Type	Select from “IP Address”, “FQDN” and “User FQDN” for IKE negotiation. “Default” stands for “IP Address”. IP Address: Uses an IP address as the ID in IKE negotiation. FQDN: Uses an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security gateway, e.g., test.robustel.com. User FQDN: Uses a user FQDN type as the ID in IKE negotiation. If this option	Default

IKE Settings		
Item	**Description**	**Default**
	is selected, type a name string with a sign "@" for the local security gateway, e.g., test@robustel.com.	
Remote ID Type	Select from "IP Address", "FQDN" and "User FQDN" for IKE negotiation. IP Address: Uses an IP address as the ID in IKE negotiation. FQDN: Uses an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security gateway, e.g., test.robustel.com. User FQDN: Uses a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with a sign "@" for the local security gateway, e.g., test@robustel.com.	Default
IKE Lifetime	Set the lifetime in IKE negotiation. Before an SA expires, IKE negotiates a new SA. As soon as the new SA is set up, it takes effect immediately and the old one will be cleared automatically when it expires.	86400
Private Key Password	Enter the private key.	Null
Username	User name used for xAuth.	Null
Password	Password used for xAuth.	Null

When choose the "Tunnel Setting > General Setting > Protocol" to "ESP".


^ SA Settings

Encrypt Algorithm: 3DES

Authentication Algorithm: MD5

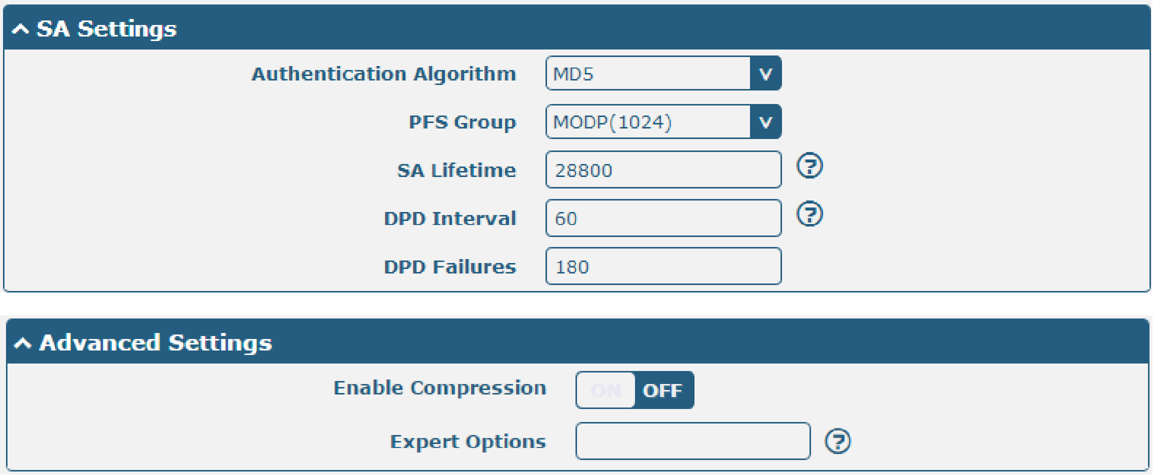
PFS Group: MODP(1024)

SA Lifetime: 28800

DPD Interval: 60

DPD Failures: 180

When choose the "Tunnel Setting > Protocol" to "AH".



SA Settings

Authentication Algorithm	MD5
PFS Group	MODP(1024)
SA Lifetime	28800
DPD Interval	60
DPD Failures	180

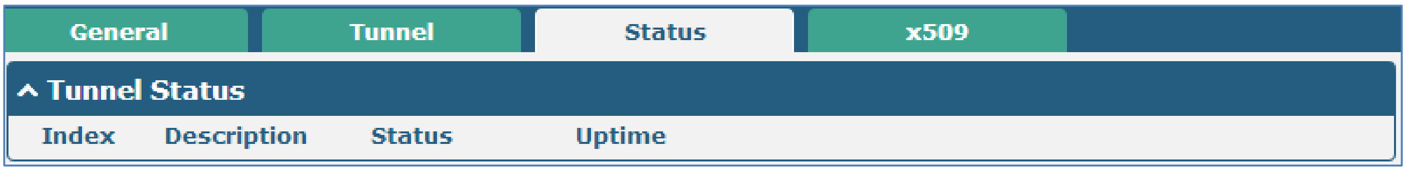
Advanced Settings

Enable Compression	ON OFF
Expert Options	

SA Settings		
Item	**Description**	**Default**
Encrypt Algorithm	Select from "3DES", "AES128" and "AES256" when you select "ESP" in "Protocol"; Note: Higher security means more complex implementation and lower speed. DES is enough to meet general requirements. Use 3DES when high confidentiality and security are required.	3DES
Authentication Algorithm	Select from "MD5" and "SHA1"to be used in SA negotiation.	MD5
PFS Group	Select from "PFS (N/A)", "MODP (1024)" and"MODP (1536)". PFS (N/A): Disable PFS Group MODP (1024): Uses the 1024-bit Diffie-Hellman group. MODP (1536): Uses the 1536-bit Diffie-Hellman group.	MODP (1024)
SA Lifetime	Set the IPSec SA lifetime. Note: When negotiating to set up IPSec SAs, IKE uses the smaller one between the lifetime set locally and the lifetime proposed by the peer.	28800
DPD Interval	Set the interval after which DPD is triggered if no IPSec protected packets is received from the peer. DPD: Dead peer detection. DPD irregularly detects dead IKE peers. When the local end sends an IPSec packet, DPD checks the time the last IPSec packet was received from the peer. If the time exceeds the DPD interval, it sends a DPD hello to the peer. If the local end receives no DPD acknowledgment within the DPD packet retransmission interval, it retransmits the DPD hello. If the local end still receives no DPD acknowledgment after having made the maximum number of retransmission attempts, it considers the peer already dead, and clears the IKE SA and the IPSec SAs based on the IKE SA.	60
DPD Failures	Set the timeout of DPD packets.	180
Advanced Settings		
Enable Compression	Tick to enable compressing the inner headers of IP packets.	OFF
Expert Options	format: config-desc;config-desc, e.g. protostack=netkey;plutodebug=none	Null

Status

This section allow user to check the status of the IPSec tunnel.



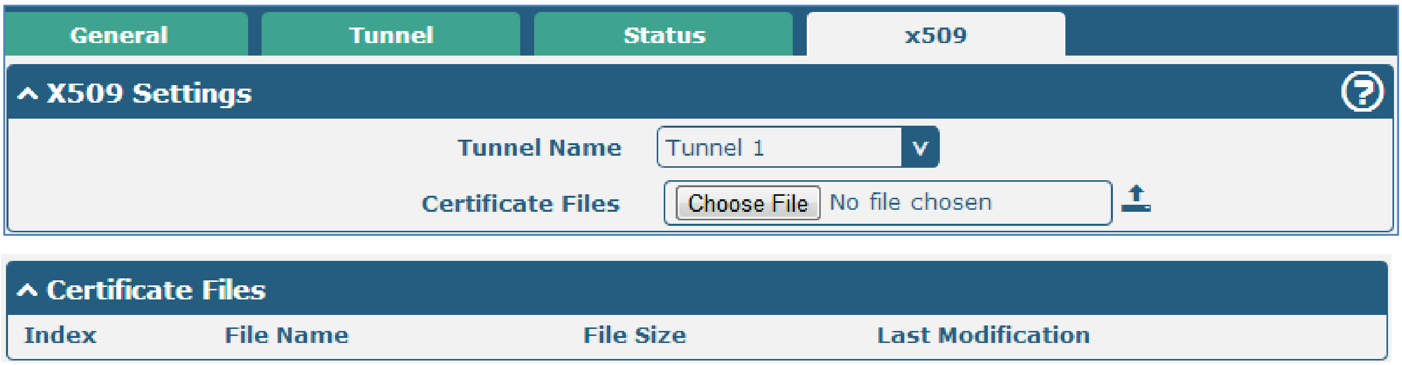
General | Tunnel | Status | x509

^ Tunnel Status

Index | Description | Status | Uptime

x509

User can upload the X509 certificate for the IPSec tunnel in this section.



General | Tunnel | Status | x509

^ X509 Settings

Tunnel Name: Tunnel 1

Certificate Files: Choose File No file chosen

^ Certificate Files

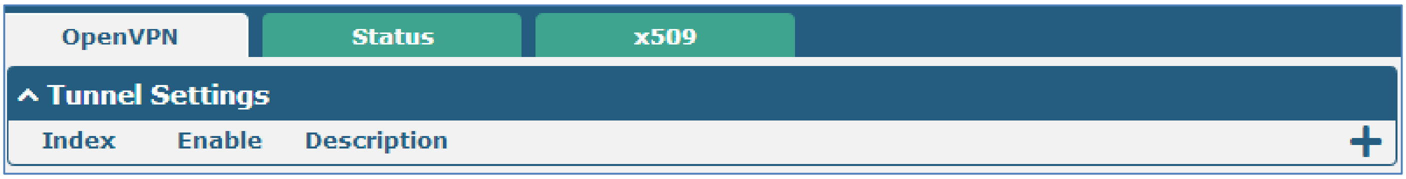
Index | File Name | File Size | Last Modification

x509		
Item	**Description**	**Default**
Tunnel Name	Select the name of the tunnel.	Tunnel 1
Certificate Files	Choose the correct file to import the certificate into the router. The correct file format as followings: @ca.crt @remote.crt @local.crt @private.key @crl.pem	Null
Index	Show the index of the certificate file.	Null
Filename	Show the name of the certificate file.	Null
File Size	Show the size of the certificate file.	Null
Last Modification	Show the timestamp of that the last time to modify the certificate file.	Null

3.16 VPN > OpenVPN

This section allows users to set the OpenVPN and the related parameters.

OpenVPN

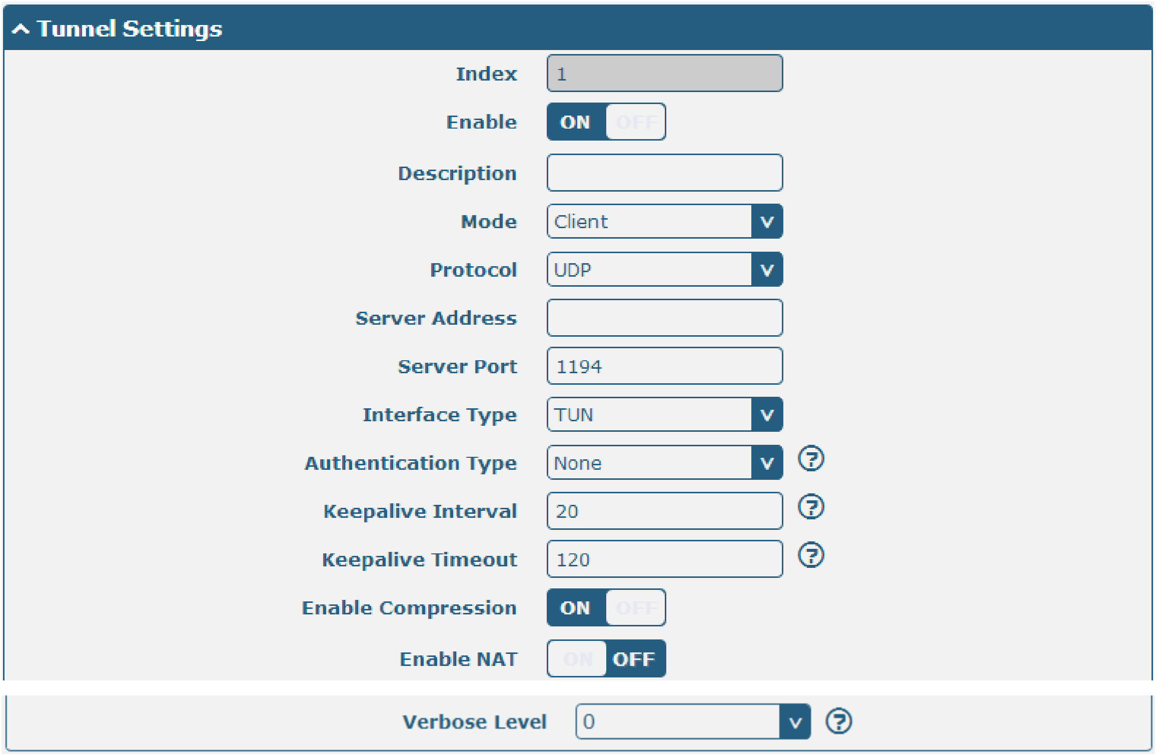


^ Tunnel Settings

Index	Enable	Description	+

Click “+” to add tunnel settings. (The maximum number of the tunnel is three.)

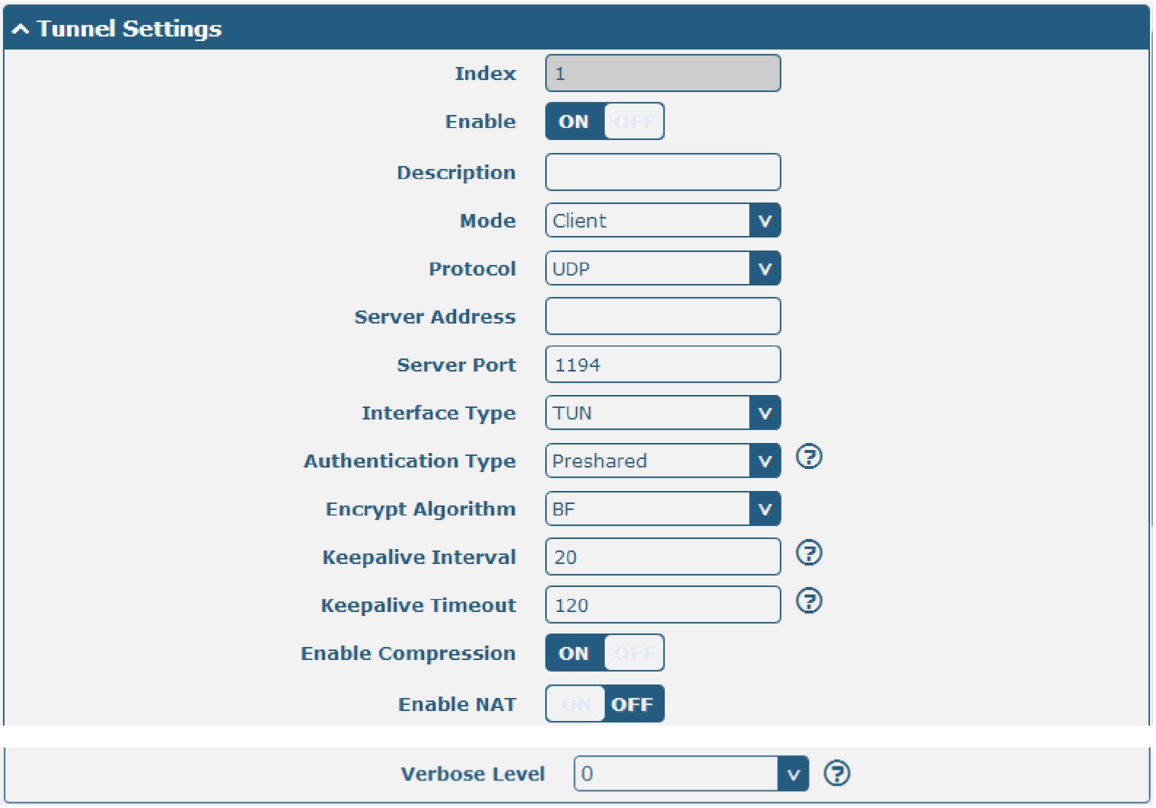
When choose “Authentication Type” to “None”.



^ Tunnel Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Server Address	
Server Port	1194
Interface Type	TUN
Authentication Type	None
Keepalive Interval	20
Keepalive Timeout	120
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

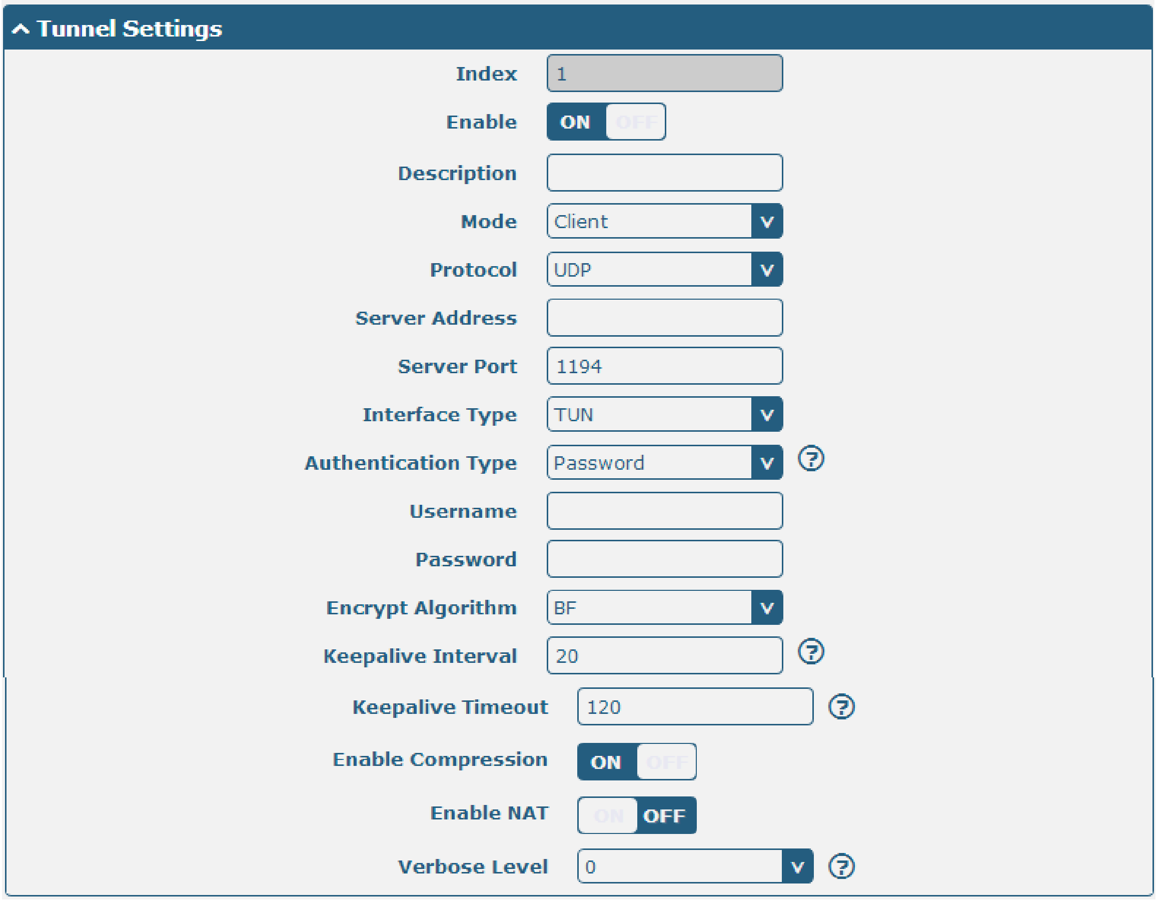
When choose “Authentication Type” to “Preshared”.



^ Tunnel Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Server Address	
Server Port	1194
Interface Type	TUN
Authentication Type	Preshared
Encrypt Algorithm	BF
Keepalive Interval	20
Keepalive Timeout	120
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

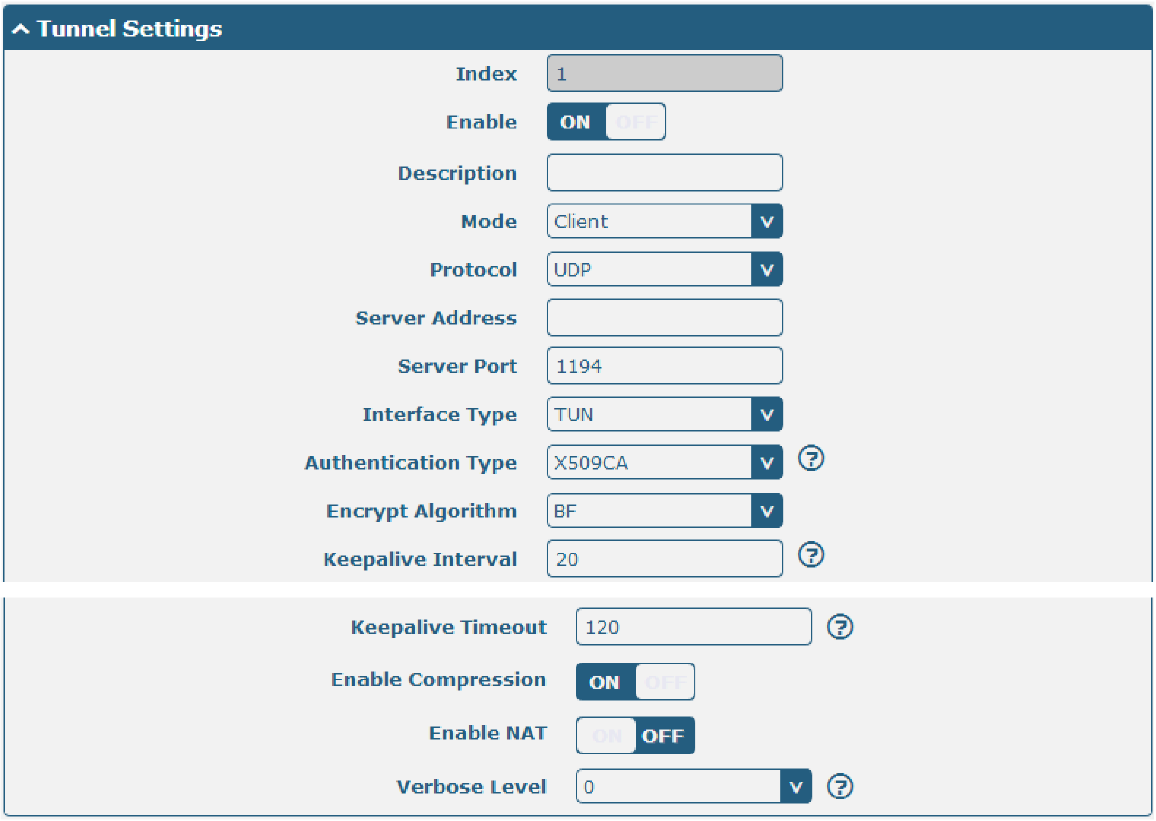
When choose “Authentication Type” to “Password”.



^ Tunnel Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Server Address	
Server Port	1194
Interface Type	TUN
Authentication Type	Password
Username	
Password	
Encrypt Algorithm	BF
Keepalive Interval	20
Keepalive Timeout	120
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

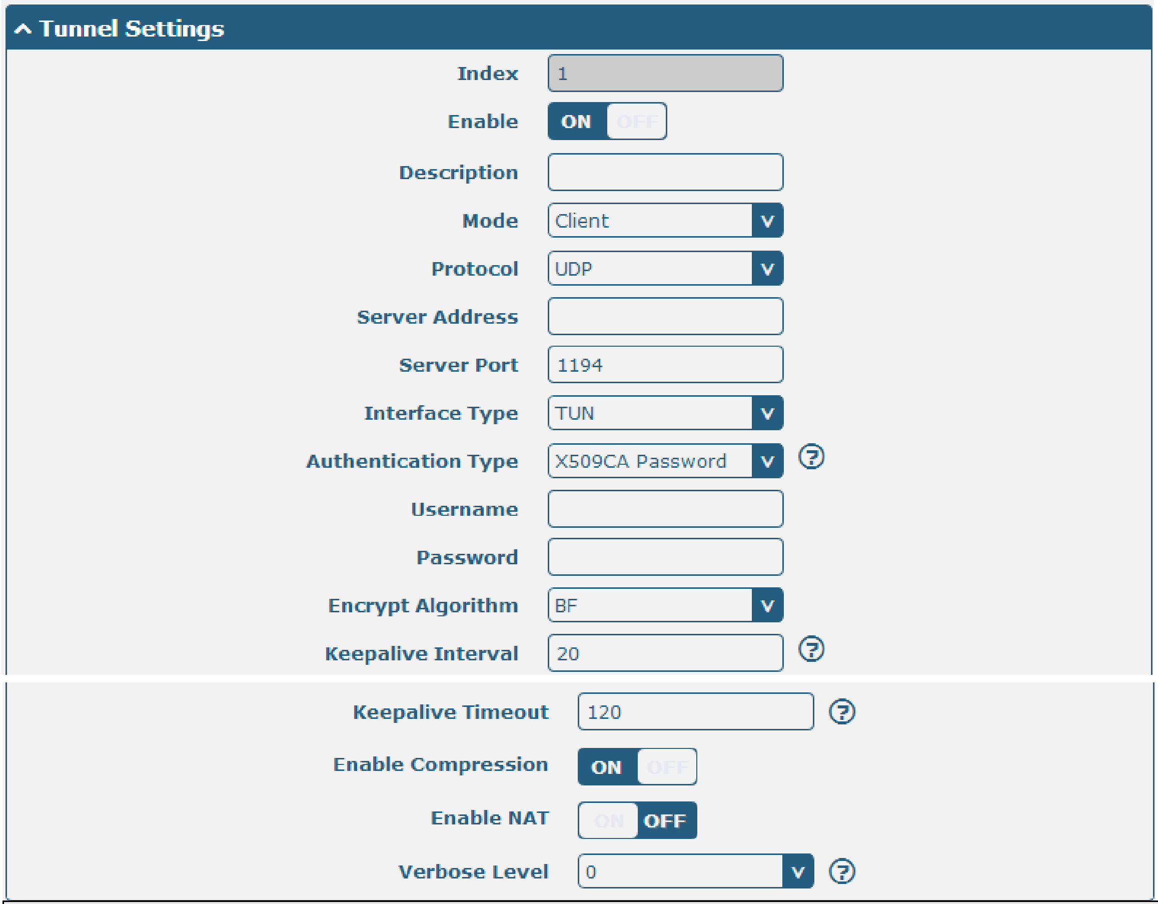
When choose “Authentication Type” to “X509CA”.



^ Tunnel Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Server Address	
Server Port	1194
Interface Type	TUN
Authentication Type	X509CA
Encrypt Algorithm	BF
Keepalive Interval	20
Keepalive Timeout	120
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

When choose “Authentication Type” to “X509CA Password”.



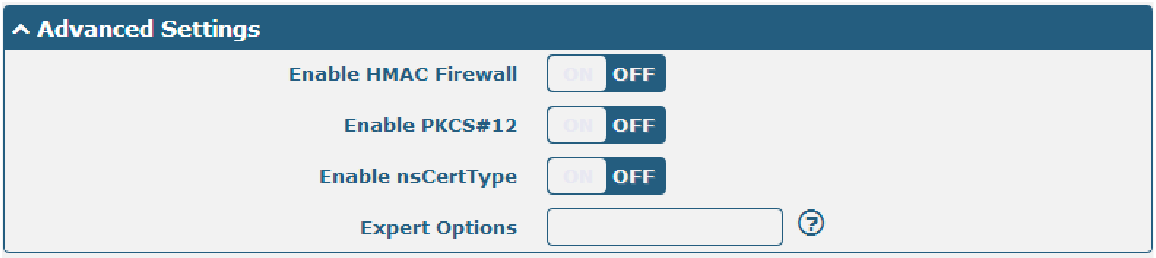
^ Tunnel Settings

Index	1
Enable	ON
Description	
Mode	Client
Protocol	UDP
Server Address	
Server Port	1194
Interface Type	TUN
Authentication Type	X509CA Password
Username	
Password	
Encrypt Algorithm	BF
Keepalive Interval	20
Keepalive Timeout	120
Enable Compression	ON
Enable NAT	OFF
Verbose Level	0

Tunnel Settings		
Item	Description	Default

Tunnel Settings		
Item	**Description**	**Default**
Index	Show the index of the tunnel.	1
Enable	Enable OpenVPN tunnel.	ON
Description	Enter some simple words about the OpenVPN Tunnel.	Null
Mode	Select from “P2P”, “Client”.	Client
Protocol	Select from “UDP”, “TCP-Client”.	UDP
Server Address	Enter the OpenVPN server address.	Null
Server Port	Enter the OpenVPN server port	1194
Interface Type	Select from “TUN”, “TAP” which are two different kinds of device interface for OpenVPN. The difference between TUN and TAP device is this: a TUN device is a virtual IP point-to-point device and a TAP device is a virtual Ethernet device.	TUN
Authentication Type	Select from “None”, “Preshared”, “Password”, “X509CA” and “X509CA Password”. “None” and “Preshared” type just work with p2p mode.	None
Local IP	When the “Mode” is “P2P”. Define the local IP address of OpenVPN tunnel.	Null
Remote IP	When the “Mode” is “P2P”. Define the remote IP address of OpenVPN tunnel.	Null
Username	User name used for Authentication Type “Password” or “X509CA Password”.	Null
Password	Password used for Authentication Type “Password” or “X509CA Password”.	Null
Encrypt Algorithm	Select from “BF”, “DES”, “DES-EDE3”, “AES128”, “AES192” and “AES256”. BF: Uses the BF algorithm in CBC mode and 128-bit key. DES: Uses the DES algorithm in CBC mode and 64-bit key. DES-EDE3: Uses the 3DES algorithm in CBC mode and 192-bit key. AES128: Uses the AES algorithm in CBC mode and 128-bit key. AES192: Uses the AES algorithm in CBC mode and 192-bit key. AES256: Uses the AES algorithm in CBC mode and 256-bit key.	BF
Keepalive Interval	Set keepalive (ping) interval to check if the tunnel is active.	20
Keepalive Timeout	Trigger OpenVPN restart after n seconds pass without reception of a ping or other packet from remote.	120
Private Key Password	Password of Private Key for Authentication Type “X509CA”	Null
Enable Compression	Enable to compress the data stream.	ON
Enable NAT	Tick to enable NAT for OpenVPN. The source IP address of host behind R3000 Lite will be disguised before accessing the remote OpenVPN client.	OFF

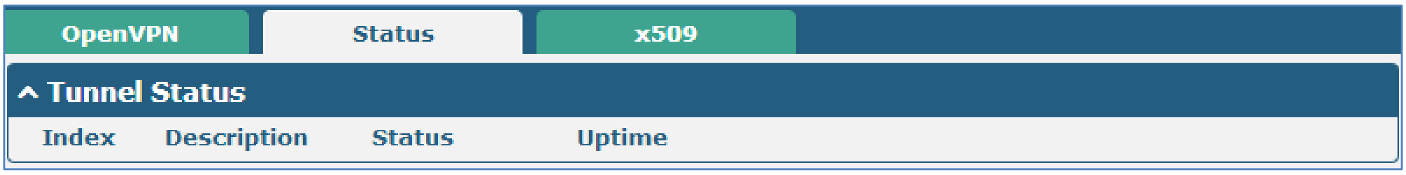
Tunnel Settings		
Item	**Description**	**Default**
Verbose Level	Select the level of the output log. Values range from 0 to 11. 0 -- No output except fatal errors. 1 to 4 -- Normal usage range. 5 -- Output R and W characters to the console for each packet read and write. 6 to 11 -- Debug info range	0



Enable HMAC Firewall	ON OFF
Enable PKCS#12	ON OFF
Enable nsCertType	ON OFF
Expert Options	

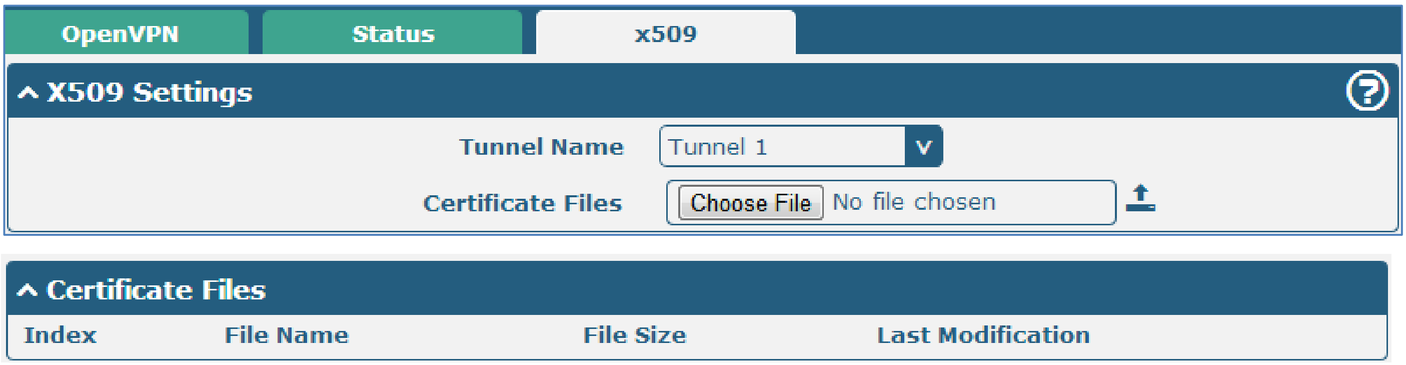
Advanced Settings		
Item	**Description**	**Default**
Enable HMAC Firewall	Add an additional layer of HMAC authentication on top of the TLS control channel to protect against DoS attacks.	OFF
Enable PKCS#12	Enable the PKCS#12 certificate. It is an exchange of digital certificate encryption standard, used to describe personal identity information.	OFF
Enable nsCertType	Require that peer certificate was signed with an explicit nsCertType designation of "server".	OFF
Expert Options	You can enter some other options of OpenVPN in this field. Each expression can be separated by a ';'.	Null

Status



Index	Description	Status	Uptime

x509



Tunnel Name	Tunnel 1
Certificate Files	No file chosen

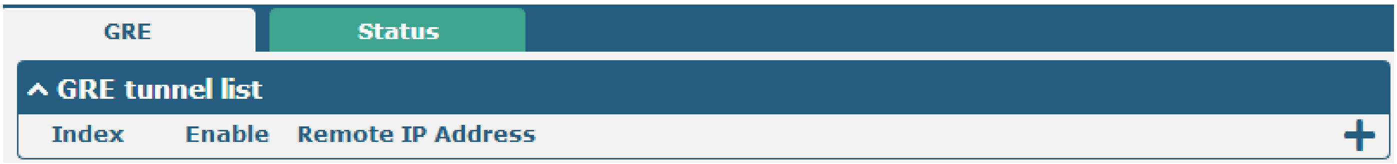
Index	File Name	File Size	Last Modification

x509

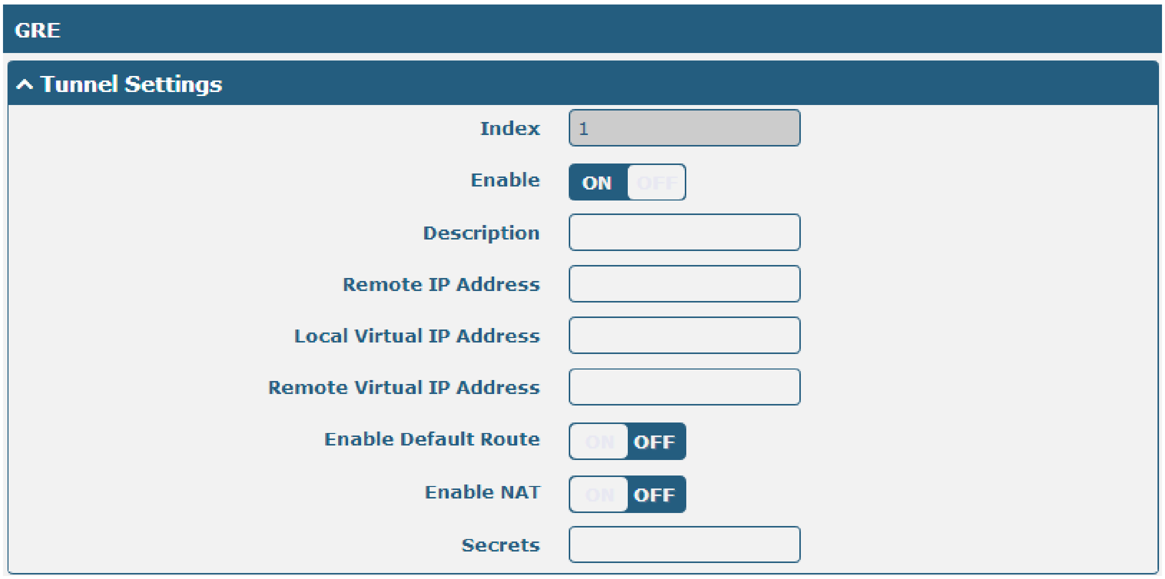
Item	Description	Default
Tunnel Name	Select the name of the Tunnel1 to Tunnel3. Because the maximum number of the tunnel is three.	Tunnel 1
Certificate Files	Choose the correct file to import the certificate into the router. The correct file format as followings: @ca.crt @remote.crt @local.crt @private.key @crl.pem	Null
Index	Show the index of the certificate file.	Null
Filename	Show the name of the certificate file.	Null
File Size	Show the size of the certificate file.	Null
Last Modification	Show the timestamp of that the last time to modify the certificate file.	Null

3.18 VPN > GRE

This section allows users to set the OpenVPN and the related parameters.



Click “+” to add tunnel settings. (The maximum number of the tunnel is three.)



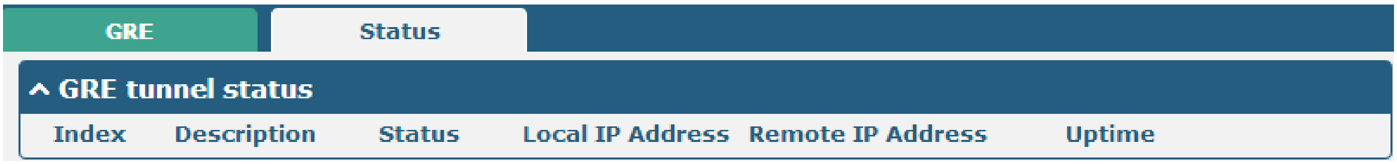
Index	1
Enable	ON
Description	
Remote IP Address	
Local Virtual IP Address	
Remote Virtual IP Address	
Enable Default Route	OFF
Enable NAT	OFF
Secrets	

GRE

Item	Description	Default
Index	Show the index of the tunnel.	1
Enable	Enable GRE tunnel. GRE (Generic Routing Encapsulation) is a protocol that	ON

	encapsulates packets in order to route other protocols over IP networks.	
Description	Enter some simple words about the GRE Tunnel.	Null
Remote IP Address	Set remote IP Address of the virtual GRE tunnel.	Null
Local Virtual IP	Set local IP Address of the virtual GRE tunnel.	Null
Remote virtual IP	Set remote IP Address of the virtual GRE tunnel.	Null
Enable Default Route	All the traffics of R3000 Lite router will go through the GRE VPN.	OFF
Enable NAT	Tick to enable NAT for GRE. The source IP address of host Behind R3000 Lite will be disguised before accessing the remote GRE server.	Disable
Secrets	Set Tunnel Key of GRE.	Null

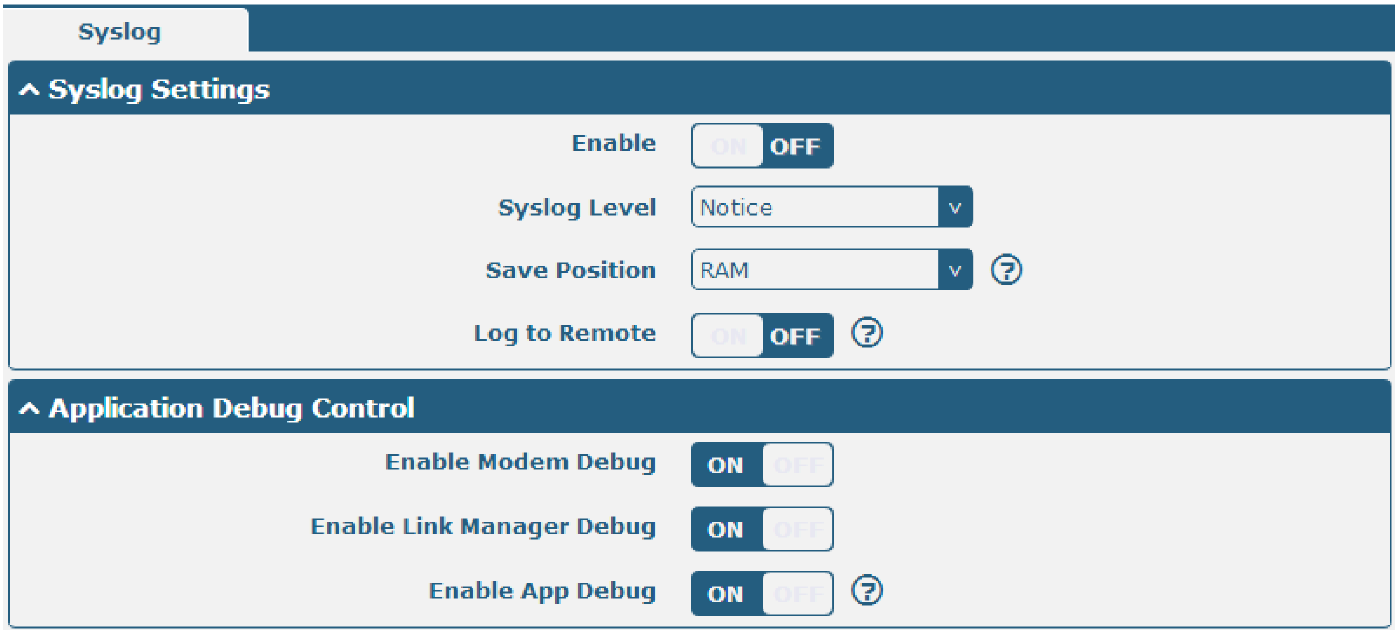
This section allow user to check the status of GRE tunnel.



Index	Description	Status	Local IP Address	Remote IP Address	Uptime

3.19 Services > Syslog

This section allows users to set the syslog parameters.



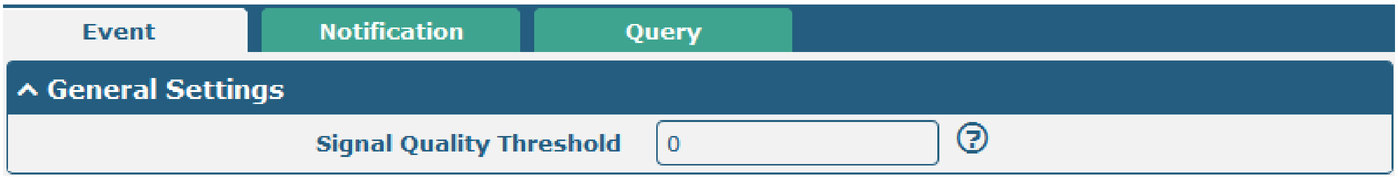
Enable: ON OFF
Syslog Level: Notice
Save Position: RAM
Log to Remote: ON OFF
Enable Modem Debug: ON OFF
Enable Link Manager Debug: ON OFF
Enable App Debug: ON OFF

Syslog		
Syslog Settings		
Item	**Description**	**Default**
Enable	Click to enable Syslog setting.	OFF
Syslog Level	Select form “Debug”, “Info”, “Notice”, “Warning”, “Error” which from low to high. The lower level will output more syslog in detail.	Notice

Save Position	Select the save position from “RAM”, “NVM” and “Console”. Choose “RAM”, the data will be cleared after reboot. But it's not recommended that saving syslog to NVM (Non-Volatile Memory) for a long time.	RAM
Log to Remote	Enable to allow router sending syslog to the remote syslog server. You need to enter the IP and Port of the syslog server.	OFF
Application Debug Control		
Enable Modem Debug	Click to enable router to debug Modem.	ON
Enable Link Manager Debug	Click to enable router to debug Link Manager.	ON
Enable APP Debug	Click to enable router’s debug control for all other applications.	ON

3.20 Services > Event

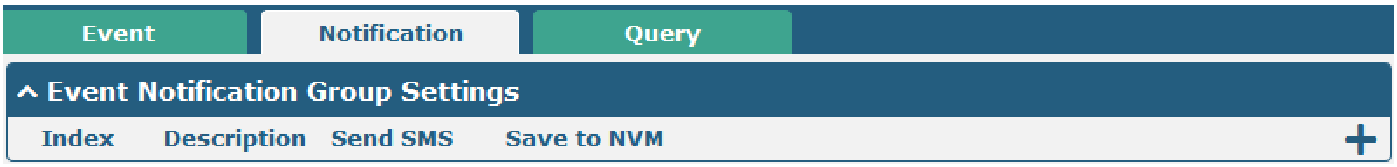
This section allows users to set the Event parameters.



^ General Settings

Signal Quality Threshold: 0

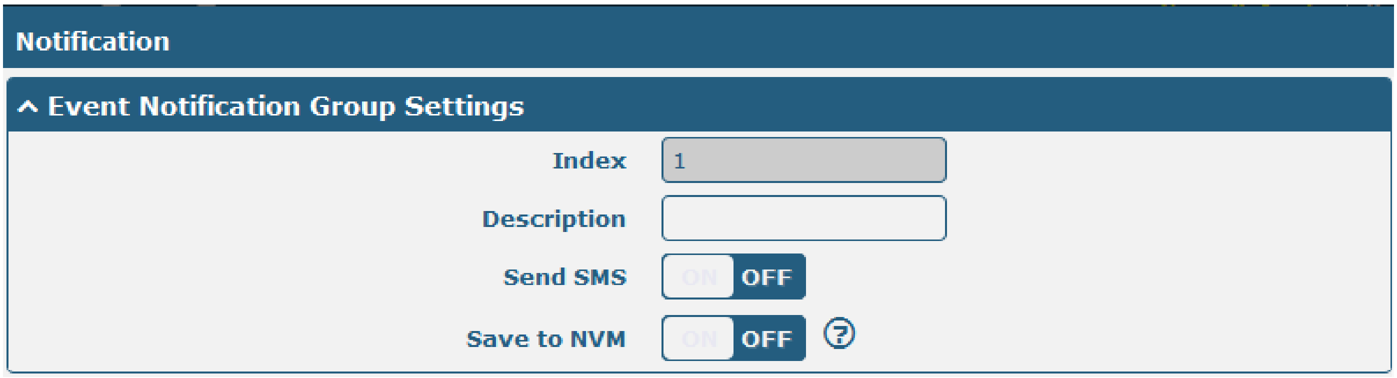
Event @ Event		
Item	Description	Default
Signal Quality Threshold	Router will generate log event when signal quality less than the threshold, 0 means disable.	0



^ Event Notification Group Settings

Index | Description | Send SMS | Save to NVM | +

Click “+” button to add an Event parameters.


Notification

^ Event Notification Group Settings

Index: 1

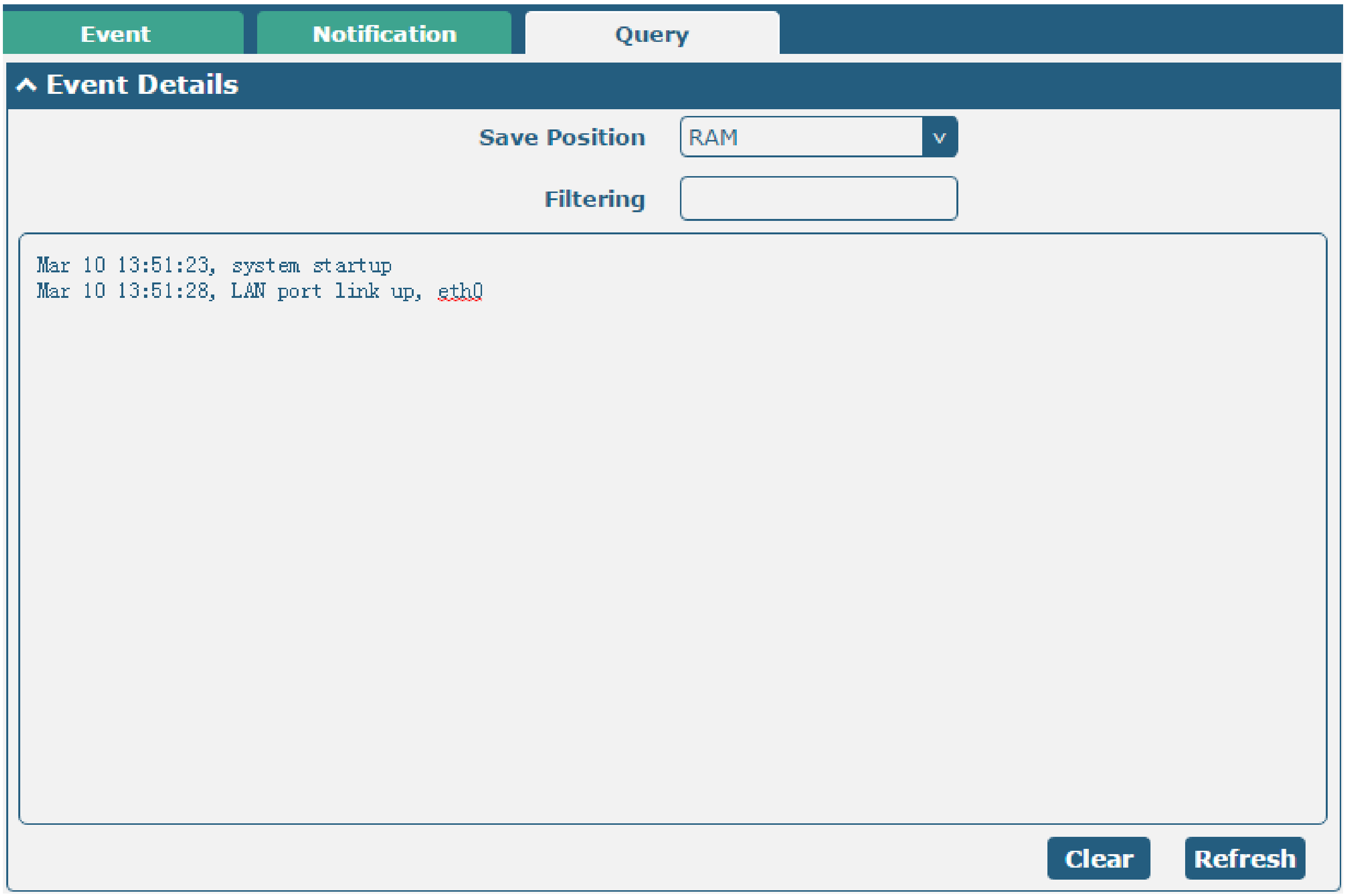
Description:

Send SMS: ON OFF

Save to NVM: ON OFF

Notification@ Event		
Item	**Description**	**Default**
Index	The index of event notification group.	1

Description	Enter some simple words to describe the Notify Group.	Null
Sent SMS	Click to enable router to send event notification SMS. Set the phone number that is used for receiving event notification, and use ';'to separate each number.	OFF
Save to NVM	Click to enable router to save event to nonvolatile memory.	OFF
Event Selector	Click to enable Event feature. There are numbers of R3000 Lite's main running event code you can select, such as "System Startup", "System Reboot", "System Time Update", etc.	OFF

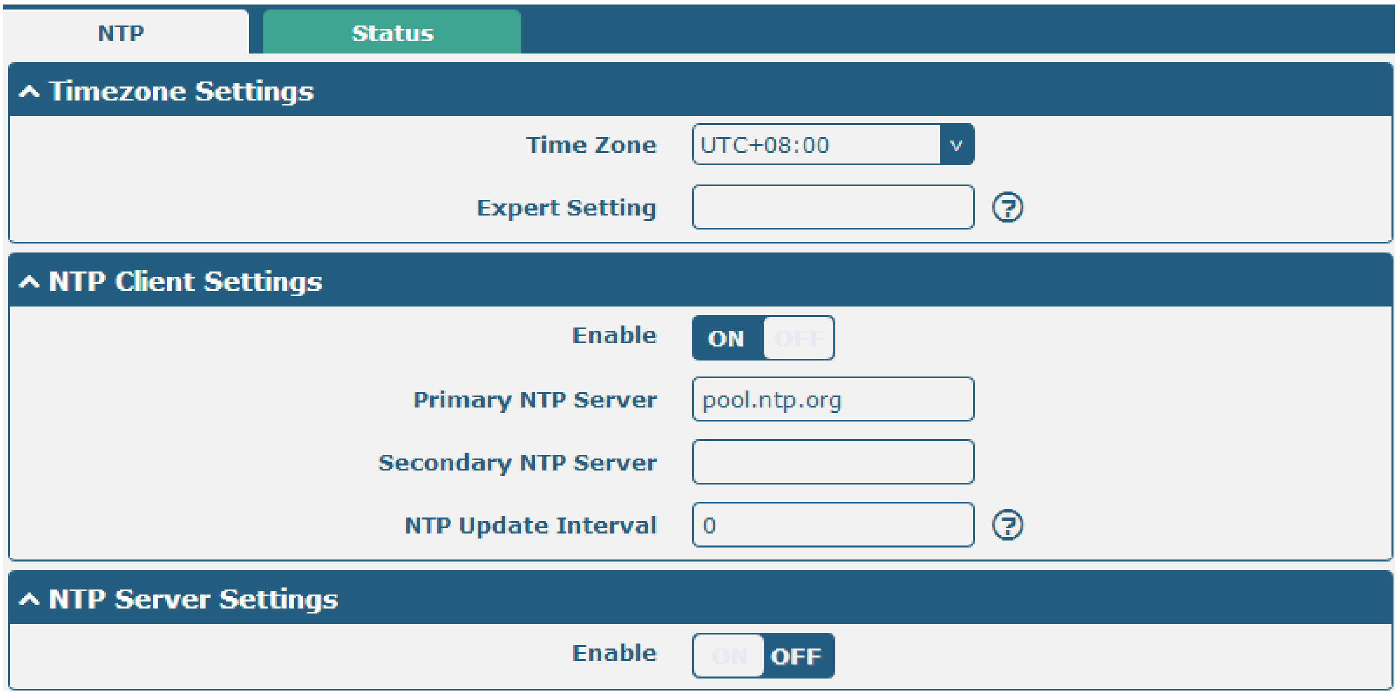


```
Mar 10 13:51:23, system startup
Mar 10 13:51:28, LAN port link up, eth0
```

Query @ Event		
Item	**Description**	**Default**
Save Position	Select the events' save position from "RAM", "NVM". RAM: Random-access memory. NVM: Non-Volatile Memory.	RAM
Filter Message	Event will be filtered according to the Filter Message that the user set. Click the Refresh button, the filtered event will be displayed in the follow box. Use "&" to separate more than one filter message, such as message1&message2.	Null

3.21 Services > NTP

This section allows users to set the NTP parameters.



Timezone Settings

Time Zone	UTC+08:00
Expert Setting	

NTP Client Settings

Enable	ON
Primary NTP Server	pool.ntp.org
Secondary NTP Server	
NTP Update Interval	0

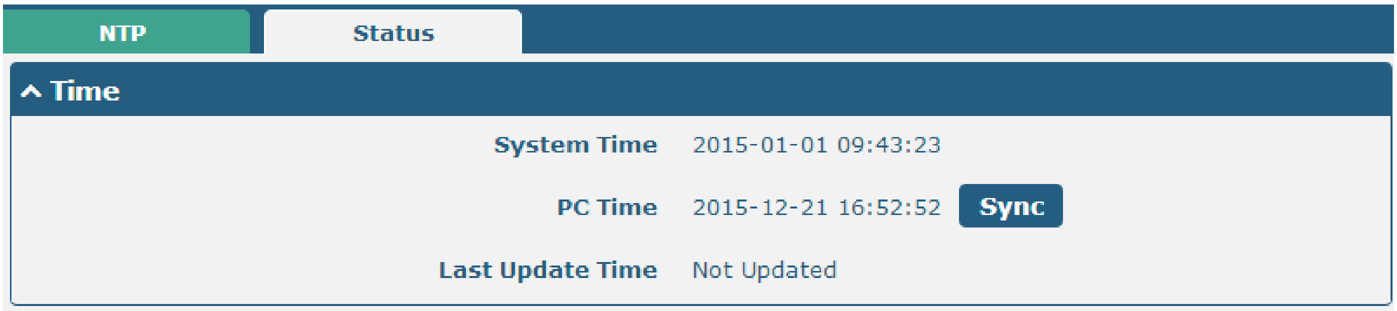
NTP Server Settings

Enable	OFF

Timezone Settings @ NTP		
Item	**Description**	**Default**
Time Zone	Select your local time zone.	UTC +08:00
Expert Setting	Specify the time zone with Daylight Saving Time in TZ environment variable format. The Time Zone option will be ignored in this case.	Null
NTP Client Setting @ NTP		
Enable	Click to enable the router to synchronize time from NTP server. ***Note:*** *R3000 Lite doesn't have the RTC, so NTP client function must always be ON.*	ON
Primary NTP Server	Enter primary NTP Server's IP address or domain name.	pool.ntp.org
Secondary NTP Server	Enter secondary NTP Server's IP address or domain name.	Null
NTP Update interval	Enter the interval (minutes) which NTP client synchronize the time from NTP server. Minutes wait for next update, 0 means update only once.	0
NTP Server Setting @ NTP		
Enable	Click to enable the NTP server function of router.	OFF

The status part of NTP allows user to check the current time of R3000 Lite and also synchronize the router time with PC.

Click **Sync** button to make the router time synchronize with PC.



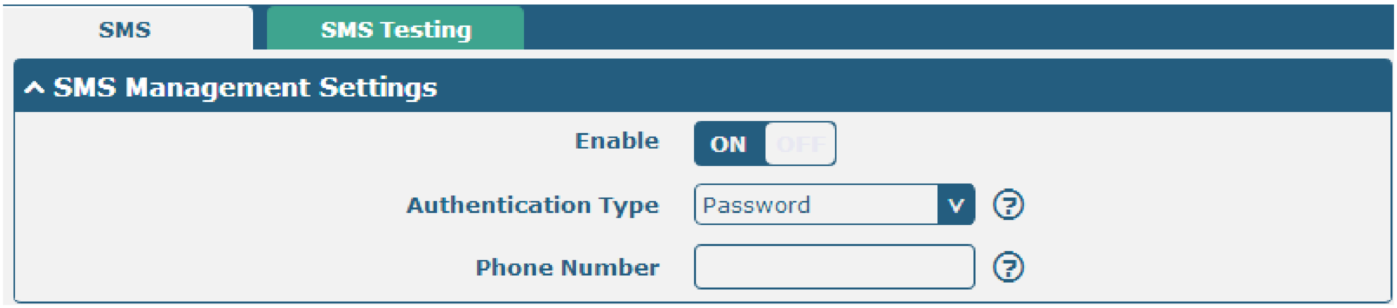
System Time 2015-01-01 09:43:23

PC Time 2015-12-21 16:52:52

Last Update Time Not Updated

3.22 Services > SMS

This section allows users to set the SMS parameters.



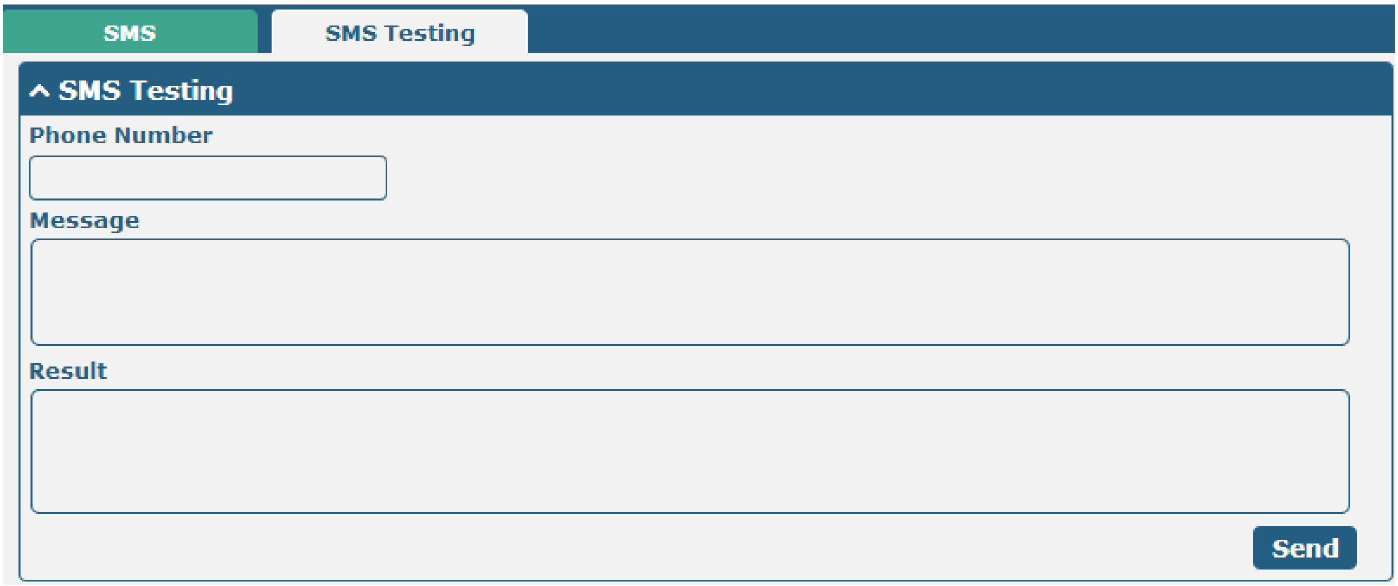
Enable ON OFF

Authentication Type Password

Phone Number

SMS		
Item	**Description**	**Default**
Enable SMS Management	Click to enable SMS Management function.	ON
Authentication Type	Select Authentication Type from “Password”, “Phonenum”, “Both”. Password: use the same username and password as WEB manager for authentication. For example, the format of the SMS should be “username: password; cmd1; cmd2; …” ***Note:*** *Set the WEB manager password in* ***System > User Management*** *section.* Phonenum: use the Phone number for authenticating, user should set the Phone Number that is allowed for SMS management. The format of the SMS should be “cmd1; cmd2; …” Both: use both the “Password” and “Phonenum” for authentication. User should set the Phone Number that is allowed for SMS management. The format of the SMS should be “username: password; cmd1; cmd2; …”	Password
Phone Number	Set the Phone Number that is allowed for SMS management, and use ‘; ‘to separate each number.	Null

User can test the current SMS service whether it is available in this section.

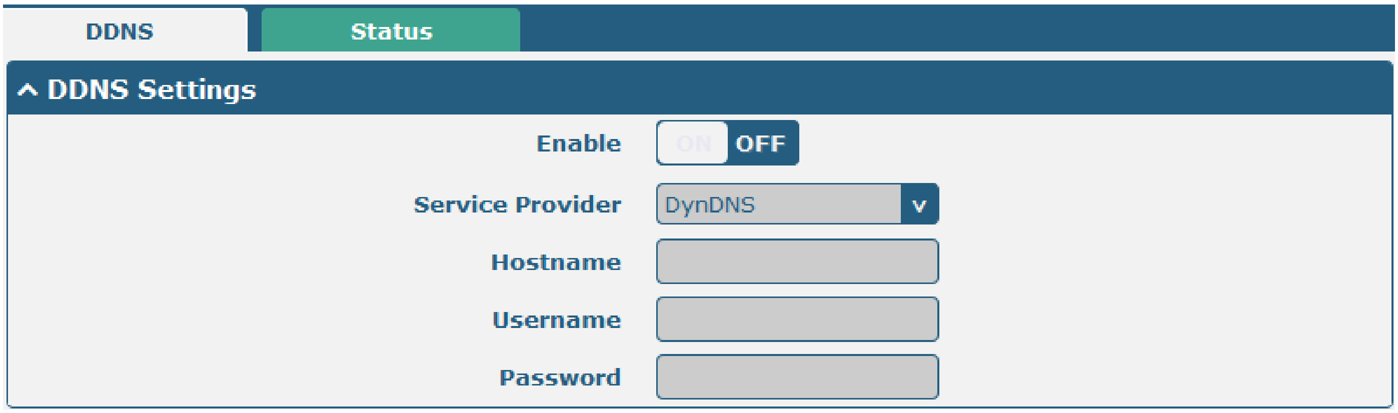


SMS Testing		
Item	**Description**	**Default**
Phone Number	Enter the specified phone number which will receive the SMS from R3000 Lite router.	Null
Message	Enter the message that R3000 Lite router will sent it to the specified phone number.	Null
Result	The result of the SMS test will display in the result box.	Null

3.23 Services > DDNS

This section allows users to set the DDNS parameters.

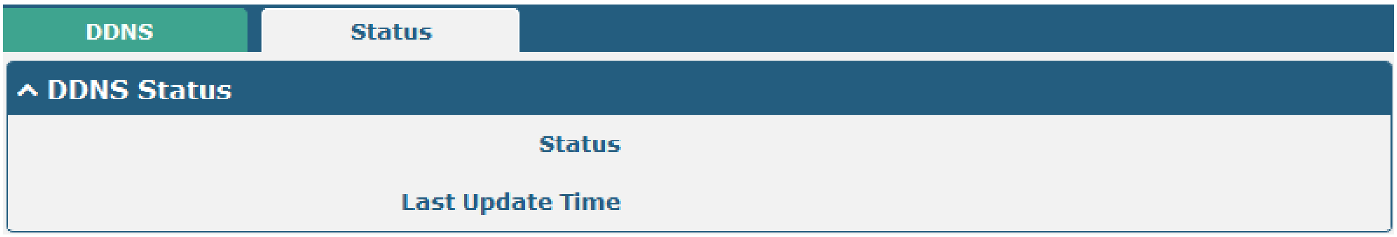
The Dynamic DNS function allows you to alias a dynamic IP address to a static domain name, allows users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.



Service Provider: DynDNS

DDNS

Item	Description	Default
Enable	Click to enable DDNS function.	OFF
Service Provider	Select the DDNS service from “DynDNS”, “NO-IP”, “3322”. ***Note:*** the DDNS service only can be used after registered by Corresponding service provider.	DynDNS
Hostname	Enter the Host name of the DDNS server provided.	Null
Username	Enter the user name of the DDNS server provided.	Null
Password	Enter the password of the DDNS server provided.	Null



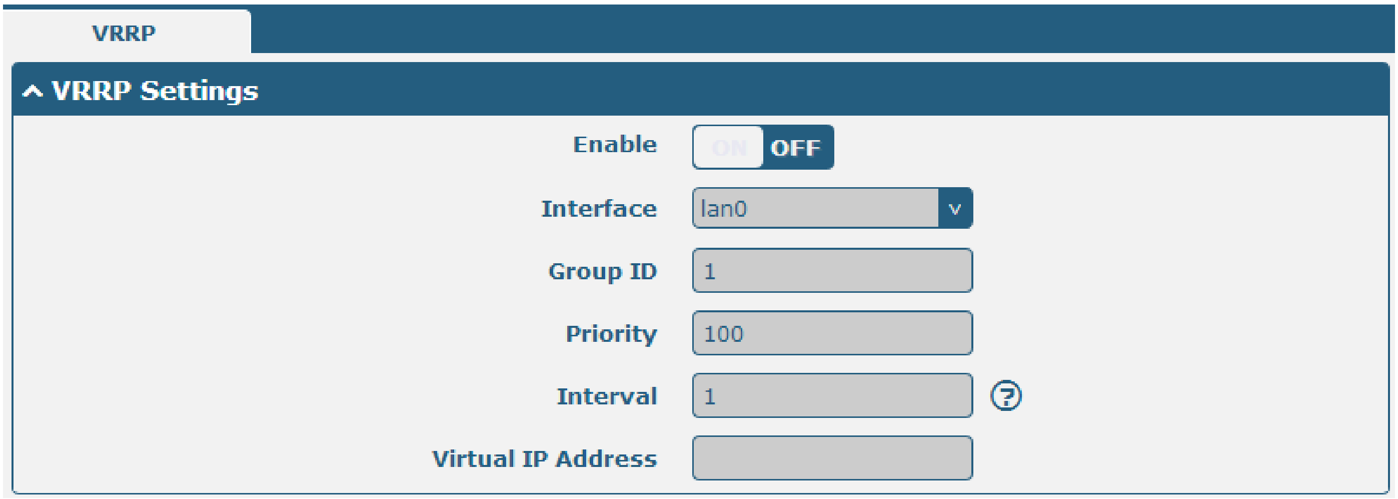
Status

Last Update Time

Status		
Item	**Description**	**Default**
Status	Show current status of DDNS service.	Null
Last Update Time	Show the time that DDNS updated successfully at last time.	Null

3.24 Services > VRRP

This section allows users to set the VRRP parameters.

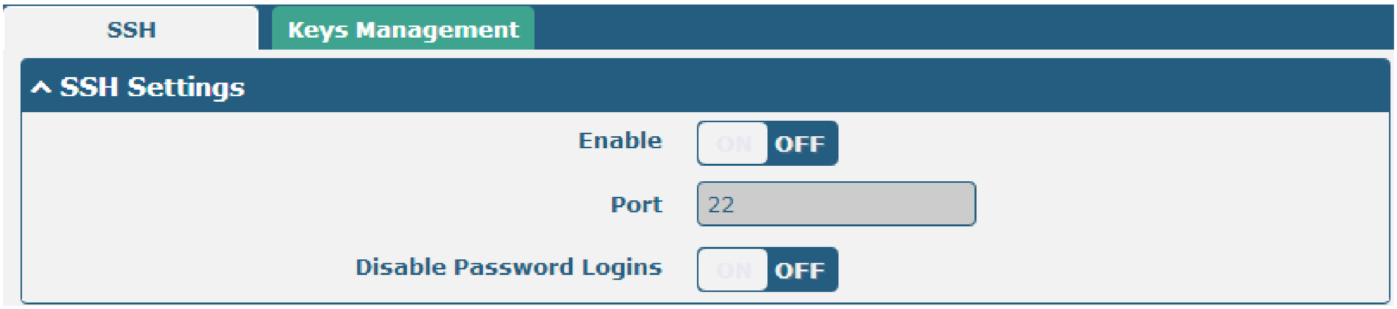


Enable	ON OFF
Interface	lan0
Group ID	1
Priority	100
Interval	1
Virtual IP Address	

VRRP		
Item	**Description**	**Default**
VRRP	VRRP (Virtual Router Redundancy Protocol) is an Internet protocol that provides a way to have one or more backup routers when using a statically configured router on a local area network (LAN).Using VRRP, a virtual IP address can be specified manually.	Null

VRRP		
Item	**Description**	**Default**
Enable	Click to enable VRRP protocol.	OFF
Interface	Display “lan0”.	lan0
Group ID	Specify which VRRP group of this router belong to.	1
Priority	Enter the priority value from 1 to 255. The larger value has higher priority.	120
Interval	The interval that master router sends VRRP packets to backup routers.	5
Virtual IP Address	A virtual IP address is shared among the routers, with one designated as the master router and the others as backups. In case the master fails, the virtual IP address is mapped to a backup router's IP address. (This backup becomes the master router)	192.168.0.1

3.25 Services > SSH

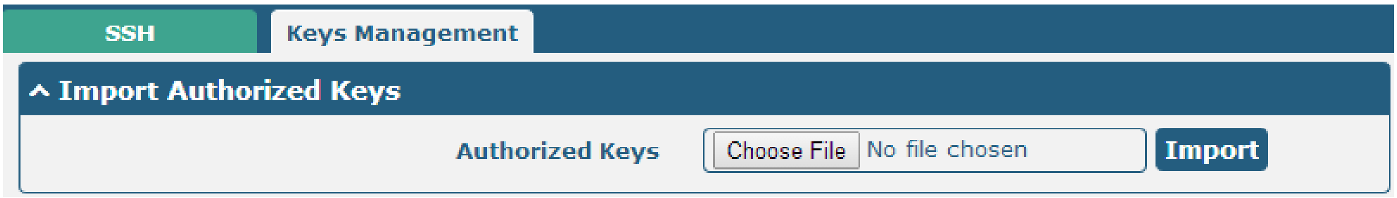


Enable: ON OFF

Port: 22

Disable Password Logins: ON OFF

SSH		
Item	**Description**	**Default**
Enable	Enable the function that user can access R3000 Lite Router via SSH.	OFF
Port	Set the port of the SSH access.	22
Disable Password Logins	Switch to “ON” and disable password logins, so that user cannot access R3000 Lite via SSH. In this situation, you should import the authorized key into R3000 Lite in **Keys Management** part for accessing R3000 Lite. Switch to “OFF”, you can access R3000 Lite via SSH normally.	OFF



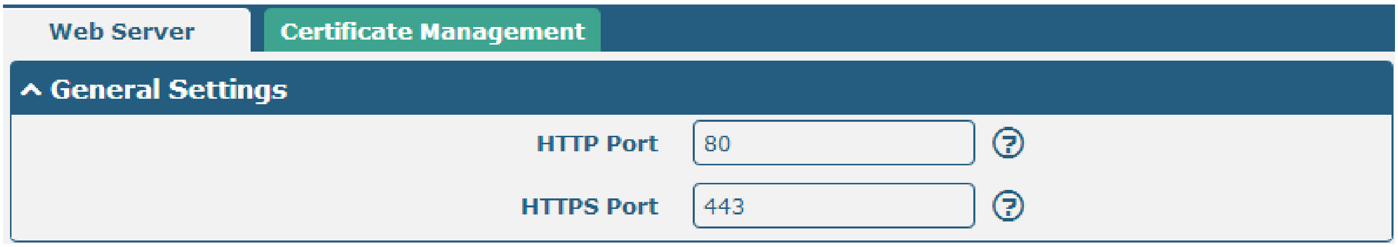
Authorized Keys: No file chosen

Keys Management	
Item	**Description**

Authorized Keys	Effective when **SSH > Disable Password Logins** is "ON". Select a key file from PC, then click **Import** button to import the key file in R3000 Lite. So that you can access R3000 Lite via SSH without password.

3.26 Services > Web Server

This section allows users to modify the parameters of Web Server.

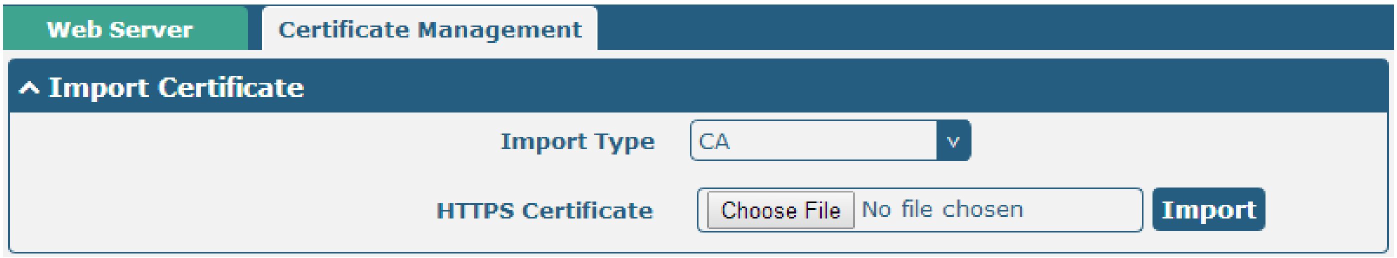


HTTP Port: 80

HTTPS Port: 443

Basic @ Web Server		
Item	**Description**	**Default**
HTTP Port	Enter the HTTP port number you want to change in R3000 Lite's Web Server. On a Web server, port 80 is the port that the server "listens to" or expects to receive from a Web client. If you configure the router with other HTTP Port number except 80, only adding that port number then you can login R3000 Lite's Web Server.	80
HTTPS Port	Enter the HTTPS port number you want to change in R3000 Lite's Web Server. On a Web server, port 443 is the port that the server "listens to" or expects to receive from a Web client. If you configure the router with other HTTPS Port number except 443, only adding that port number then you can login R3000 Lite's Web Server. ***Note**: HTTPS is more secure than HTTP. In many cases, clients may be exchanging confidential information with a server, which needs to be secured in order to prevent unauthorized access. For this reason, HTTP was developed by Netscape corporation to allow authorization and secured transactions.*	443
Login Timeout (s)	Enter the Login timeout you want to change in R3000 Lite's Web Server. After "Login Timeout", R3000 Lite will force to log out the Web GUI and then you need to re-login again to Web GUI.	1800

This section allows users to import the certificate file into the route.



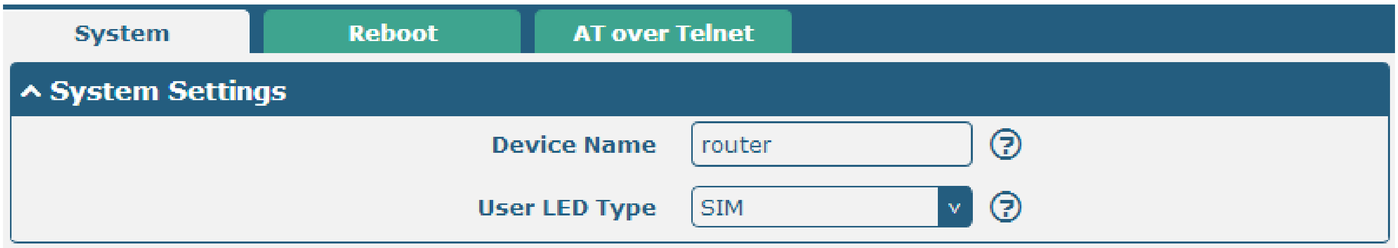
Import Type: CA

HTTPS Certificate: No file chosen

Certificate Management		
Item	**Description**	**Default**
Import Type	Select from "CA" and "Private Key". CA: a digital certificate issued by CA center. Private Key: a private key file.	CA
HTTPS Certificate	Click "Browse" to select the certificate file in your computer, and then click "Import" to import this file into your router.	

3.27 Services > Advanced

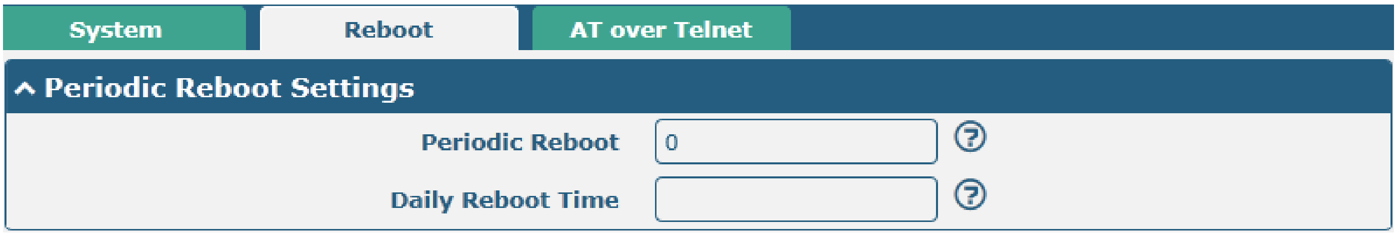
This section allows users to set the Advanced and parameters.



Device Name: router

User LED Type: SIM

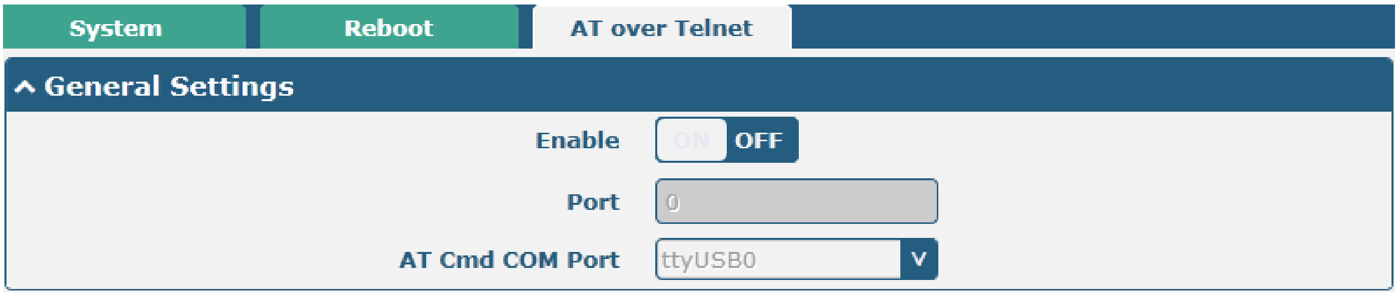
System @ Advanced		
Item	**Description**	**Default**
Device Name	Set the device name to distinguish different devices you have installed. Valid characters: a-z, A-Z, 0-9, ., -.	router
User LED Type	Select from "None", "SIM", "NET", "OpenVPN" and "IPSec".	SIM



Periodic Reboot: 0

Daily Reboot Time:

Reboot		
Item	**Description**	**Default**
Periodic Reboot	Set the reboot period of the router, 0 means disable.	0
Daily Reboot Time	Set the daily reboot time of the router, you should follow the format as HH: MM, in 24h time frame, otherwise the data will be invalid. Leave it empty means disable.	Null



Enable: ON OFF

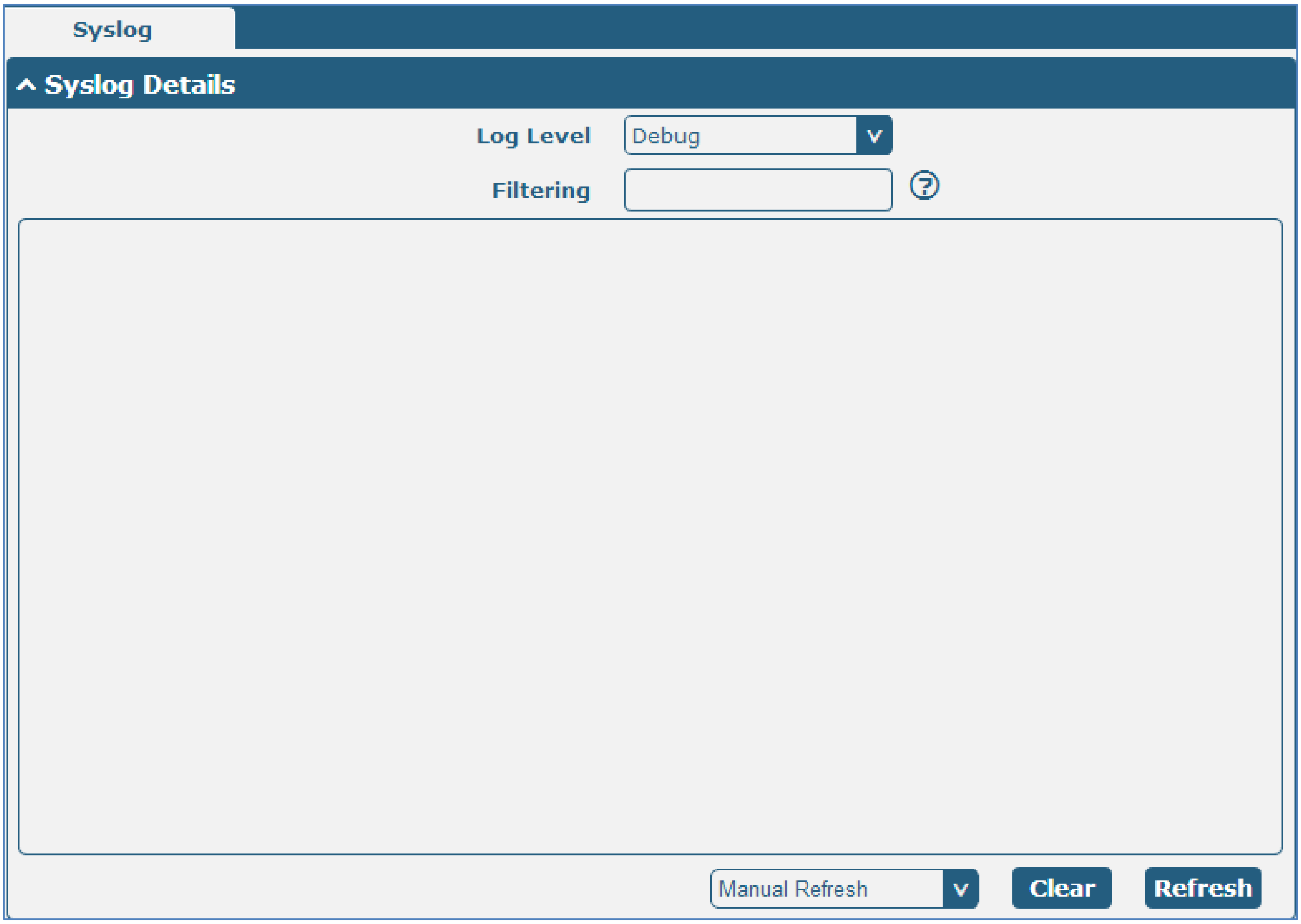
Port: 0

AT Cmd COM Port: ttyUSB0

AT over Telnet @ Advanced		
Item	**Description**	**Default**
Enable	Click to enable AT over Telnet function.	OFF
Port	Enter a specific port number to allow user sent AT command to this router over telnet.	0
AT Cmd COM Port	Select a COM port used for identifying the AT command.	ttyUSB0

3.28 System > Debug

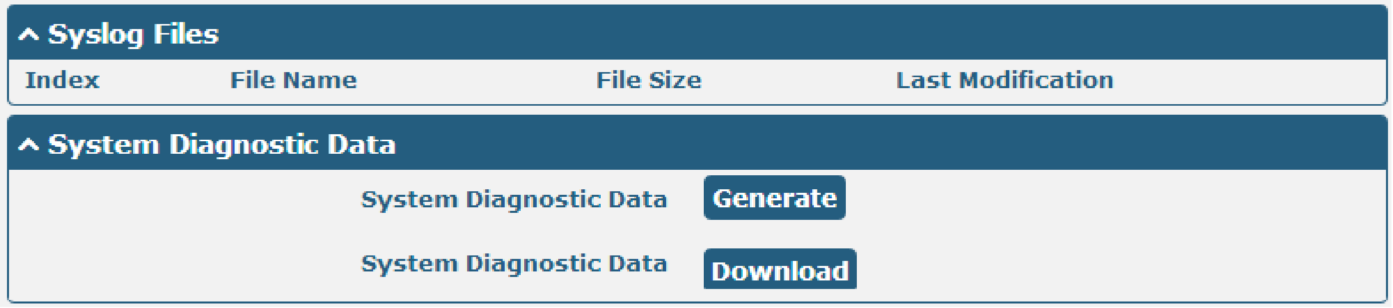
This section allow user to check and download the syslog details.



Log Level: Debug

Filtering:

Manual Refresh



^ Syslog Files

Index	File Name	File Size	Last Modification

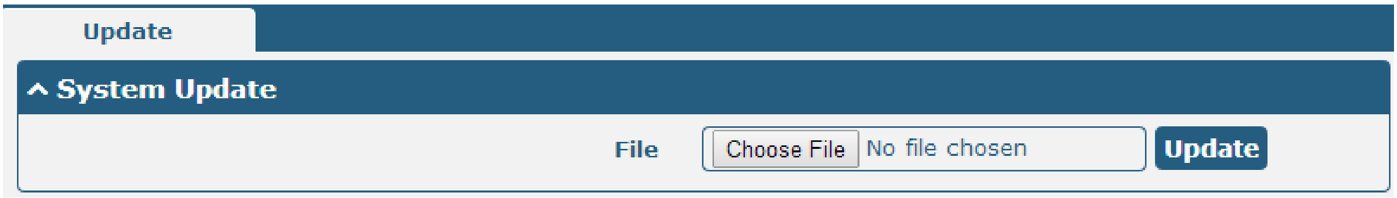
^ System Diagnostic Data

System Diagnostic Data

System Diagnostic Data

Syslog Details @ Syslog		
Item	**Description**	**Default**
Log Level	Select form "Debug", "Info", "Notice", "Warn", "Error" which from low to high. The lower level will output more syslog in detail.	Debug
Filtering	Log will be filtered according to the Filter Message that the user set. Click the Refresh button, the filtered log will be displayed in the follow box. Use "&" to separate more than one filter message, such as "keyword1&keyword2".	Null
Refresh	Select from "Manual Refresh", "5 Seconds", "10 Seconds", "20 Seconds"and"30 Seconds". User can select these intervals to refresh the log information displayed in the follow box. Select "manual refresh", user should click the refresh button to refresh the syslog.	Manual Refresh
Syslog Files List @ Syslog		
Syslog Files List	It can show at most 5 syslog files in the list, the files' name range from message0 to message 4. And the newest syslog file will be placed on the top of the list.	/
System Diagnosing Data @ Syslog		
Generate	Click to generate the syslog diagnosing file.	/
Download	Click to download system diagnosing file.	/

3.29 System > Update



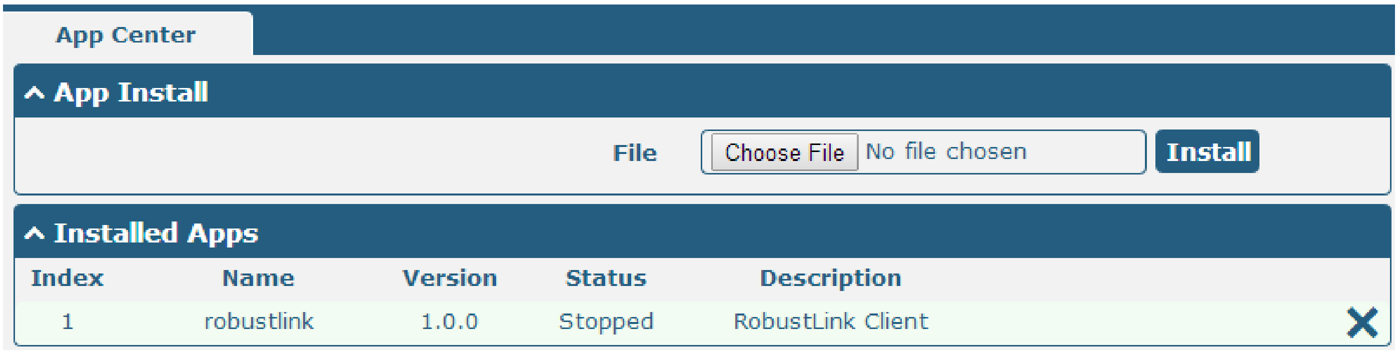
^ System Update

File: Choose File No file chosen

Update		
Item	**Description**	**Default**
System Update	Click "Browse" button to select the correct firmware in your PC, and then click "Update" button to update. After updating successfully, you need to click "save and apply", and then reboot the router to take effect.	Null

3.30 System > APP Center

This section allow user to add a new function to R3000 Lite router. And the new function will be in the form of an APP file which could be installed in R3000 Lite router. In general, the App which had installed will display in **Service** section.

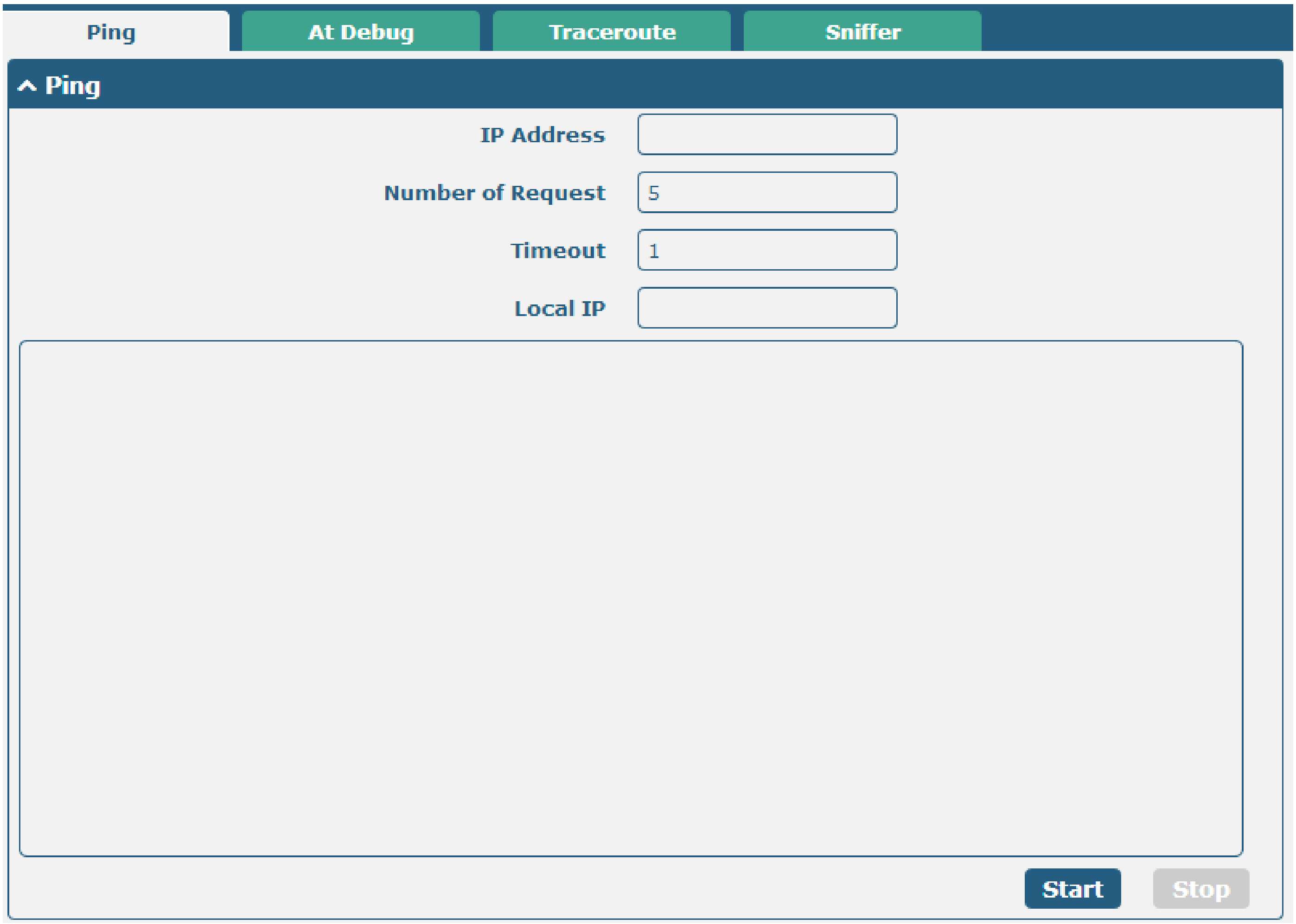


Index	Name	Version	Status	Description	
1	robustlink	1.0.0	Stopped	RobustLink Client	✕

App Center		
Item	Description	Default
File	Choose the correct App file from your PC, and click **Install** button to import to R3000 Lite router. File format: xxx.rpk, e.g. R3000-robustlink-1.0.0.rpk.	/
Install Apps	Those Apps which had installed in R3000 Lite will be listed in **Installed Apps**.	Null
Index	Show the index of the App.	Null
Name	Show the name of the App.	Null
Version	Show the version of the App.	Null
Status	Show the Status of the App.	Null
Description	Show the description of the App.	Null

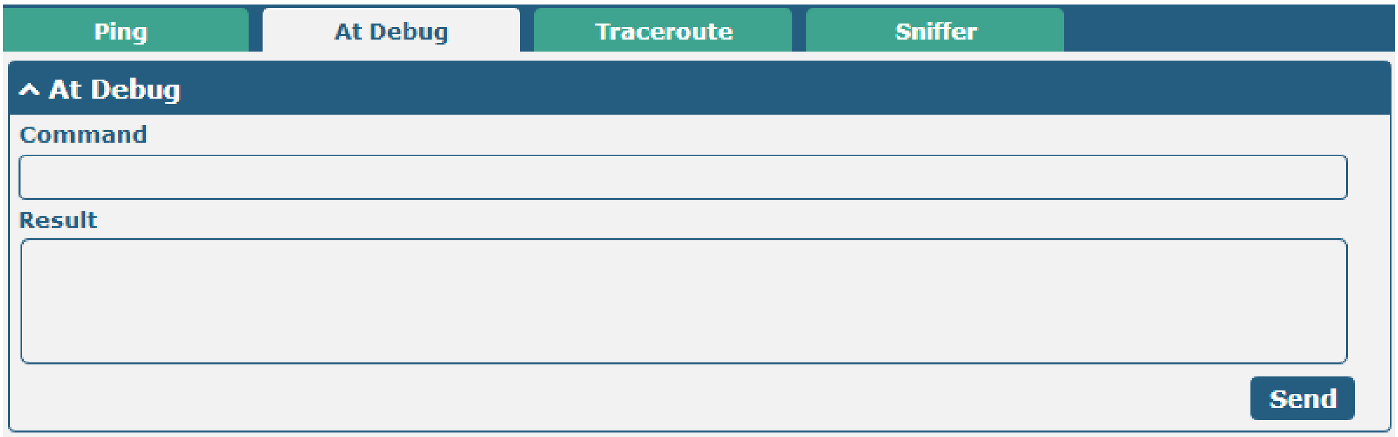
3.31 System > Tools

This section provides users three tools: Ping, Traceroute and Sniffer.

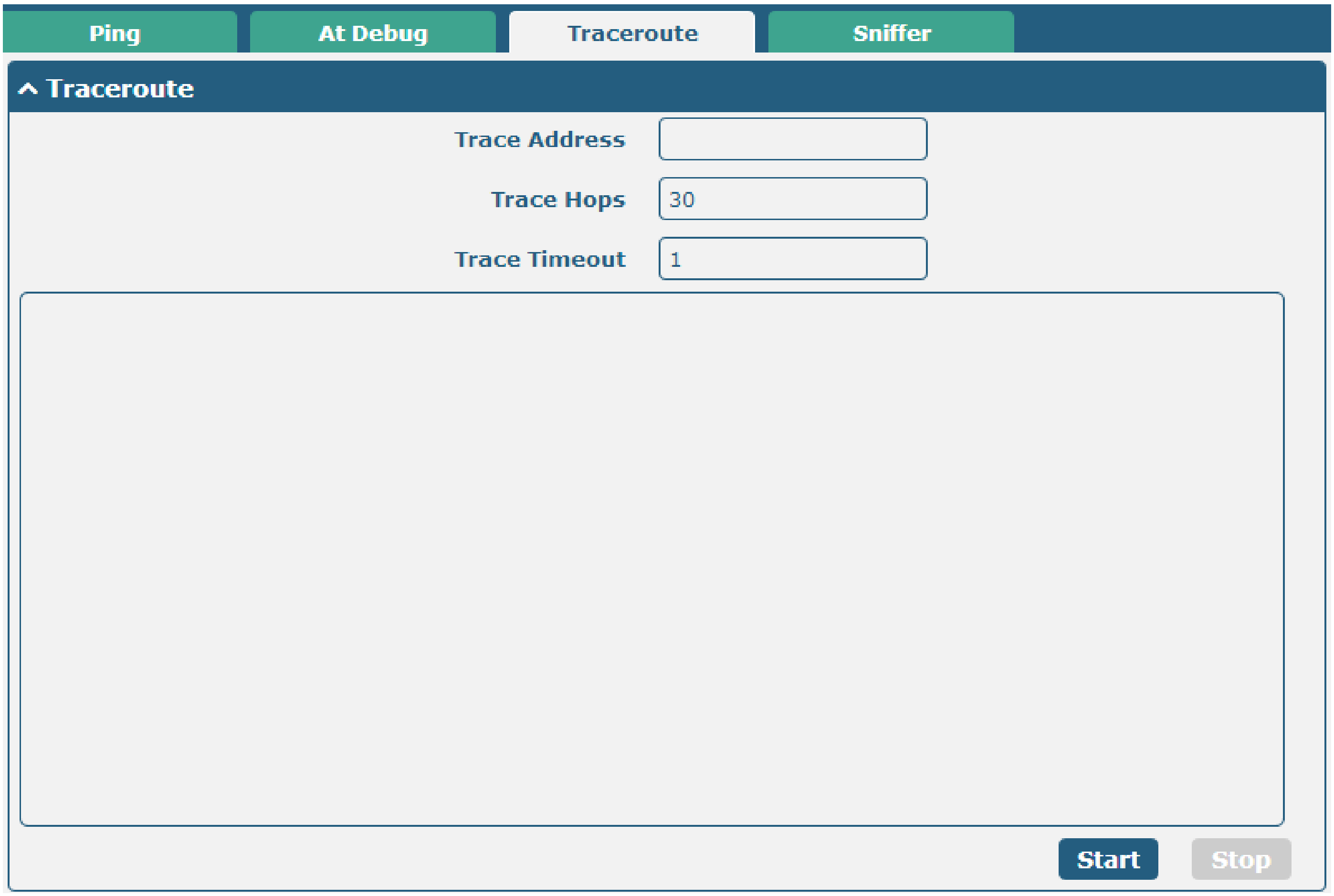


IP Address	
Number of Request	5
Timeout	1
Local IP	

Ping @ Tools		
Item	**Description**	**Default**
IP address	Enter the ping destination IP address or domain name.	Null
Number of requests	Specify the number of ping requests.	5
Timeout	Specify timeout of ping request.	1
Local IP	Specify the local IP from cellular WAN, Ethernet WAN or Ethernet LAN. Null stands for selecting local IP address from these three automatically.	Null
Start	Click this button to start ping request, and the log will be displayed in the follow box.	Null
Stop	Click this button to stop ping request.	



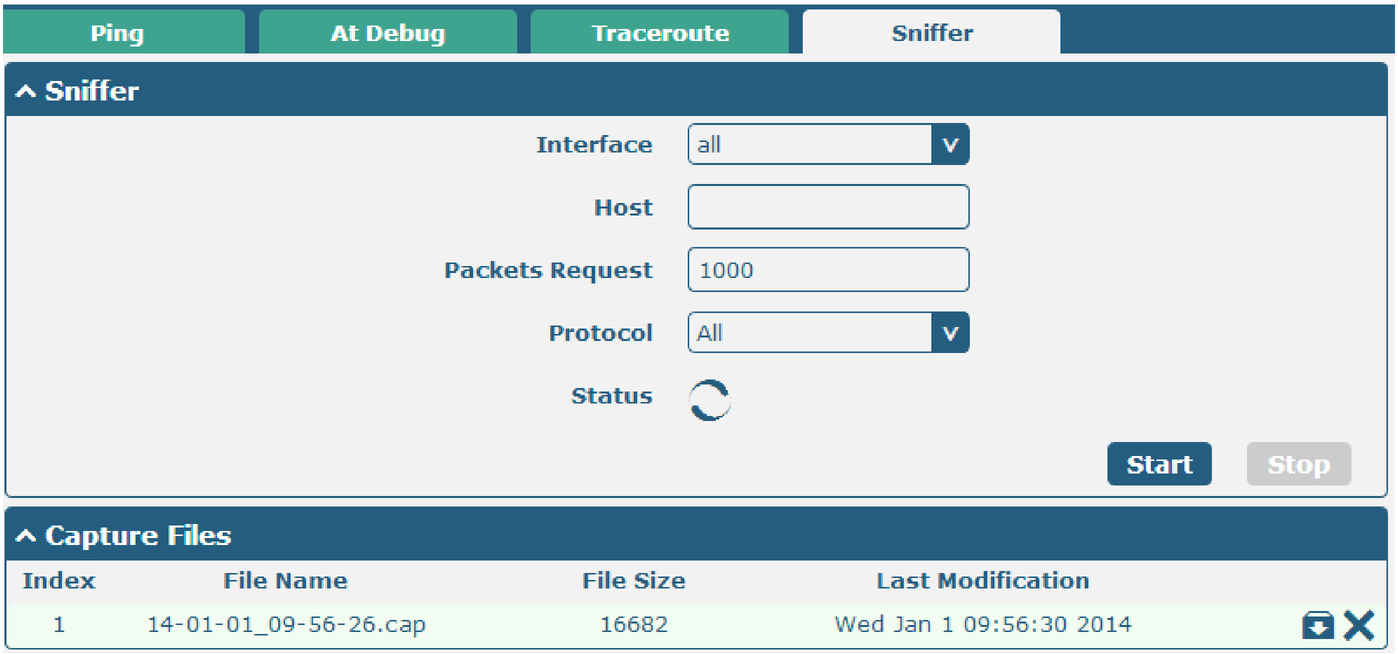
At Debug @ Tools	
Item	**Description**
Command	Enter a At command in Command box, then click **Send** button to send the At command to the cellular module.
Result	It will display the AT commands which respond from the cellular module in this box.



Trace Address
Trace Hops 30
Trace Timeout 1

Traceroute @ Tools

Item	Description	Default
Trace Address	Enter the trace destination IP address or domain name.	Null
Trace Hops	Specify the max trace hops. Router will stop tracing if the trace hops has met max value no matter the destination has been reached or not.	30
Trace Timeout	Specify timeout of Traceroute request.	1
Start	Click this button to start Traceroute request, and the log will be displayed in the follow box.	
Stop	Click this button to stop Traceroute request	



^ Sniffer

Interface	all
Host	
Packets Request	1000
Protocol	All
Status	

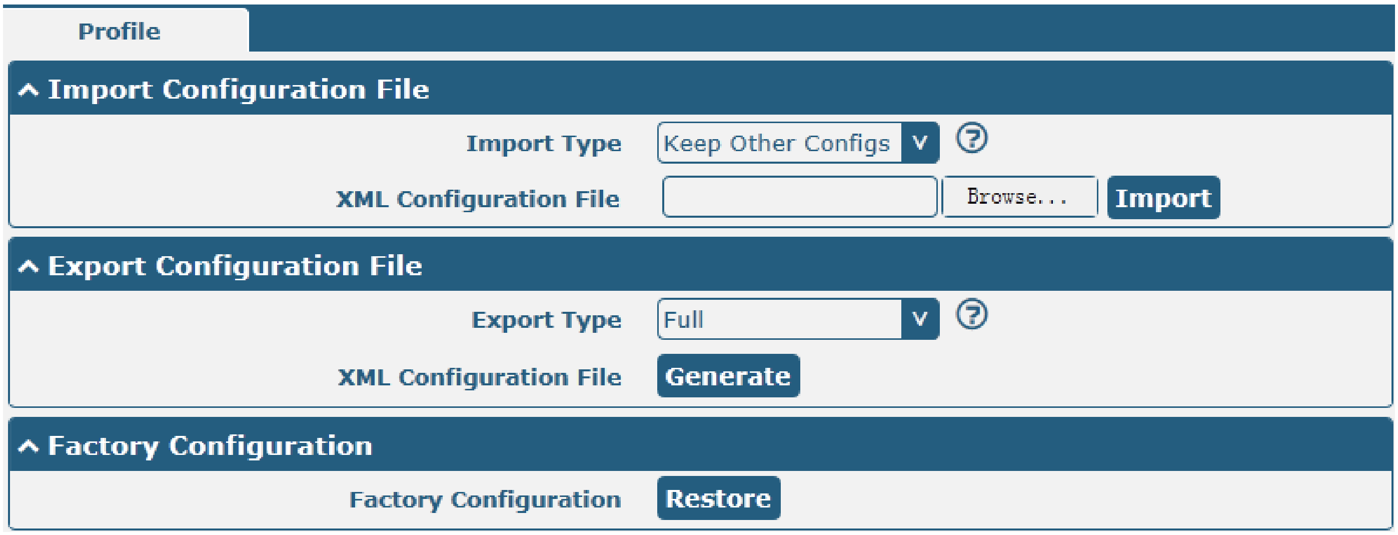
^ Capture Files

Index	File Name	File Size	Last Modification	
1	14-01-01_09-56-26.cap	16682	Wed Jan 1 09:56:30 2014	⤓ ✕

Sniffer @ Tools		
Item	**Description**	**Default**
Interface	Select form “All”, “ETH1”, and “ETH2”: All: contain all the interface; ETH1: Ethernet interface1; ETH2: Cellular WAN.	All
Host	Filter the packet that contain the specify IP address.	Null
Packets Request	Set the packet number that the router can sniffer at a time.	1000
Protocol	Select from “All”, “IP”, “TCP”, “UDP” and “ARP”.	All
Port	Set the port number for TCP or UDP that is used in sniffer.	Null
Status	Show the current status of sniffer.	Null
Start	Click this button to start the sniffer.	/
Stop	Click this button to stop the sniffer. Once click the stop button, a new log file will be displayed in the follow List.	/
Capture Files	Every times of sniffer log will be saved automatically as a new file. You can find the file from this Sniffer Traffic Data List and click ⤓ to download the log, click ✕ to delete the log file. It can cache a maximum of 5 files.	Null

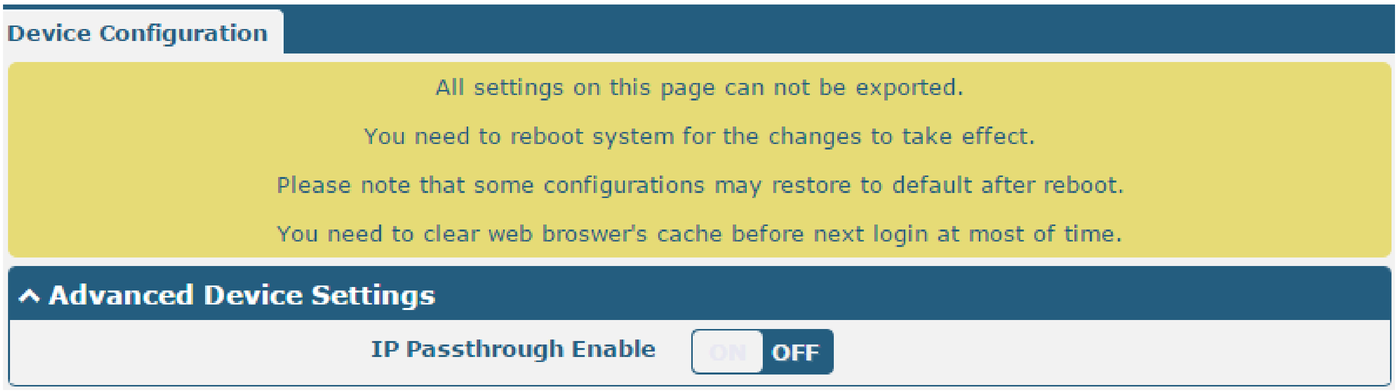
3.32 System > Profile

This section allows users to import or export the configuration file, and restore the router to factory default setting.



Import Configuration File @ Profile		
Import Type	Define what to do about the configs that is not contained in the imported file. There are two Import Types: Keep Other Configs: Keep other configuration unchanged when import XML configuration file. Set Others To Default: Set other configuration to factory default when import XML configuration file.	Keep Other Configs
XML Configuration File	Click “Browse” to select the XML file in your computer, and then click “Import” to import this file into your router.	
Export Configuration File @ Profile		
Export Type	There are four export Types : Essential: export the configuration file that only include enabled features. Essential && Detailed: export the configuration file that only include enabled features, and attach extra information such as **range** and **default** setting of those enable config option. Full: export the configuration file of all features; include both the enabled and disabled features. Full && Detailed: export the configuration file of all features, and attach extra information such as **range** and **default** setting of every config option.	Full
Export	Click “Export” and the configuration will be showed in the new popup browser window, then you can save it as a XML file.	
Factory Configuration @ Profile		
Restore	Click the “Restore” button to restore the router to factory default setting.	

3.33 System > Device Configuration



Device Configuration

All settings on this page can not be exported.

You need to reboot system for the changes to take effect.

Please note that some configurations may restore to default after reboot.

You need to clear web broswer's cache before next login at most of time.

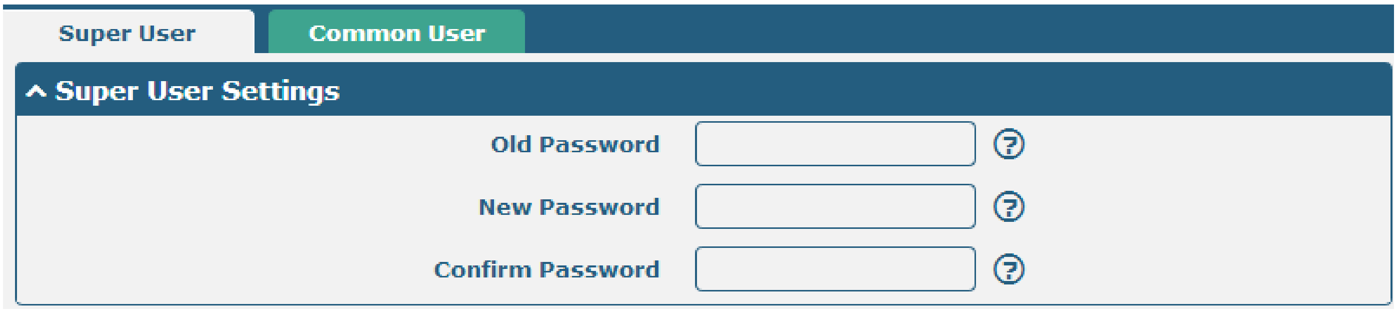
^ Advanced Device Settings

IP Passthrough Enable: ON OFF

Advanced Device Settings		
Item	**Description**	**Default**
IP Passthrough Enable	Click to enable the IP Passthrough feature.	OFF

3.34 System > User Management

This section allows users to modify or add management user accounts.



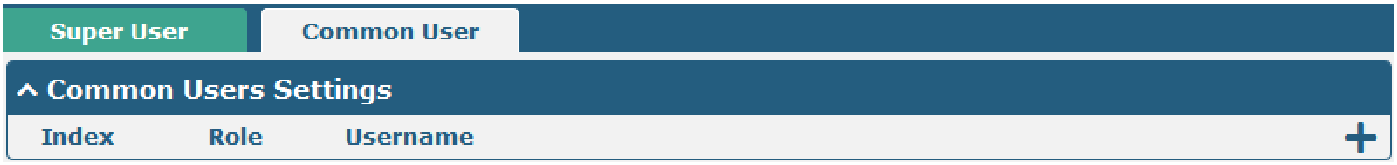
^ Super User Settings

Old Password

New Password

Confirm Password

Super User		
Item	**Description**	**Default**
Super User	One router has only one super user account. Under this account, user has the highest authority include modify, add and manage those user accounts.	/
Old Password	The old password of super user which default is “admin”, valid characters: a-z, A-Z, 0-9, @, ., -, #, $, *.	Null
New Password	Enter a new password for the super user, valid characters: a-z, A-Z, 0-9, @, ., -, #, $, *.	Null
Confirm Password	Enter the new password again which had added in New Password item.	Null



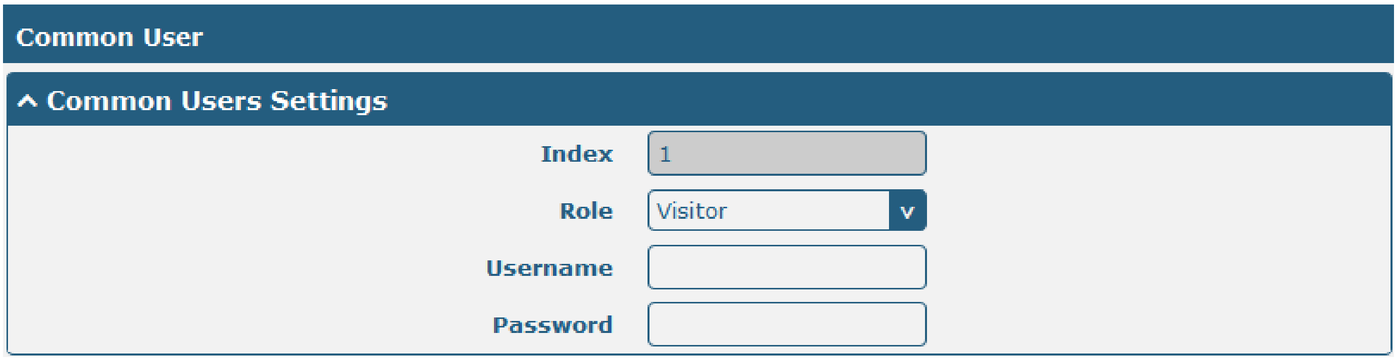
Super User | Common User

^ Common Users Settings

Index | Role | Username

Click the "+" button to add a new common user.

***Note**: One router has 5 common user accounts at most.*



Common User

^ Common Users Settings

Index: 1

Role: Visitor

Username:

Password:

Common User		
Item	**Description**	**Default**
Role	Select from “Visitor” and “Editor”. Visitor: Users only can view the configuration of router under this level; Editor: Users can view and set the configuration of router under this level.	Visitor
Username	Set the Username. Valid characters: a-z, A-Z, 0-9, ., -.	Null
Password	Set the password which at least contains 5 characters. Valid characters: a-z, A-Z, 0-9, @, ., -, #, $, *.	Null

Chapter 4 Configuration Examples

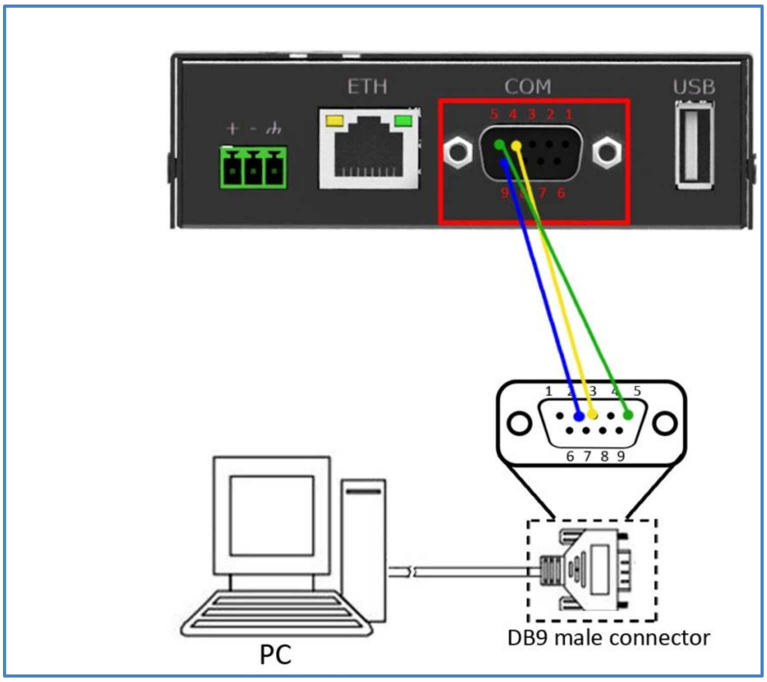
4.1 Interface

DB9 Female Connector

PIN	Debug	RS232	RS485 (2-wire)	Direction
1			Data+ (A)	-
2		RXD		R3000 Lite → Device
3		TXD		Device → R3000 Lite
4	DRXS			Device → R3000 Lite
5	GND	GND		-
6			Data- (B)	-
7		RTS		Device → R3000 Lite
8		CTS		R3000 Lite → Device
9	DTXD			R3000 Lite → Device

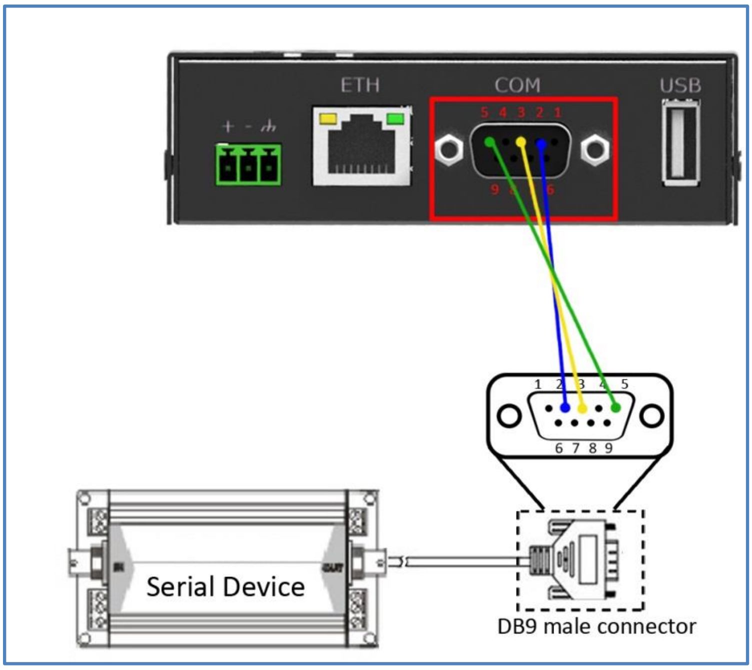
4.1.1 Console Port

User can use the console port to manage the router via CLI commands.
Please check section Introductions for CLI.



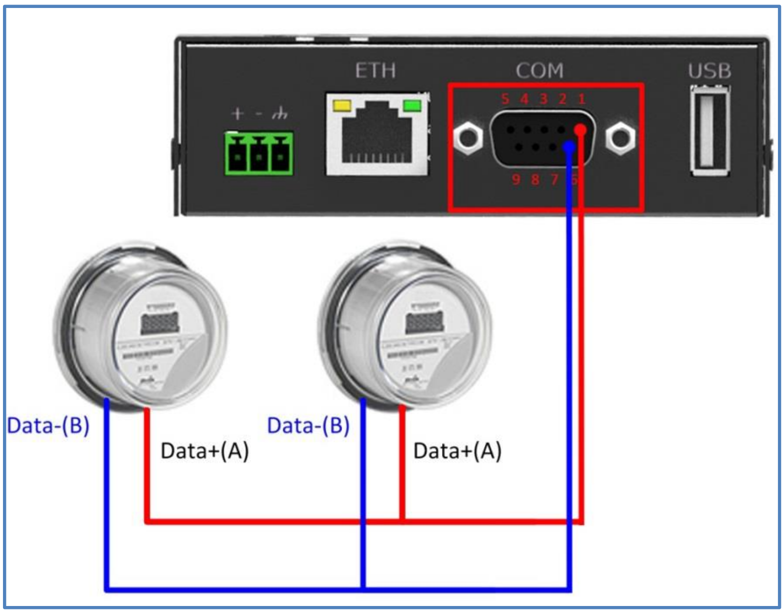
4.1.2 RS232

R3000 Lite supports one RS232 for serial data communication.
Please refer to the connection diagram at the right site.



4.1.3 RS485

R3000 Lite supports one RS485 for serial data communication.
Please refer to the connection diagram at the right site.



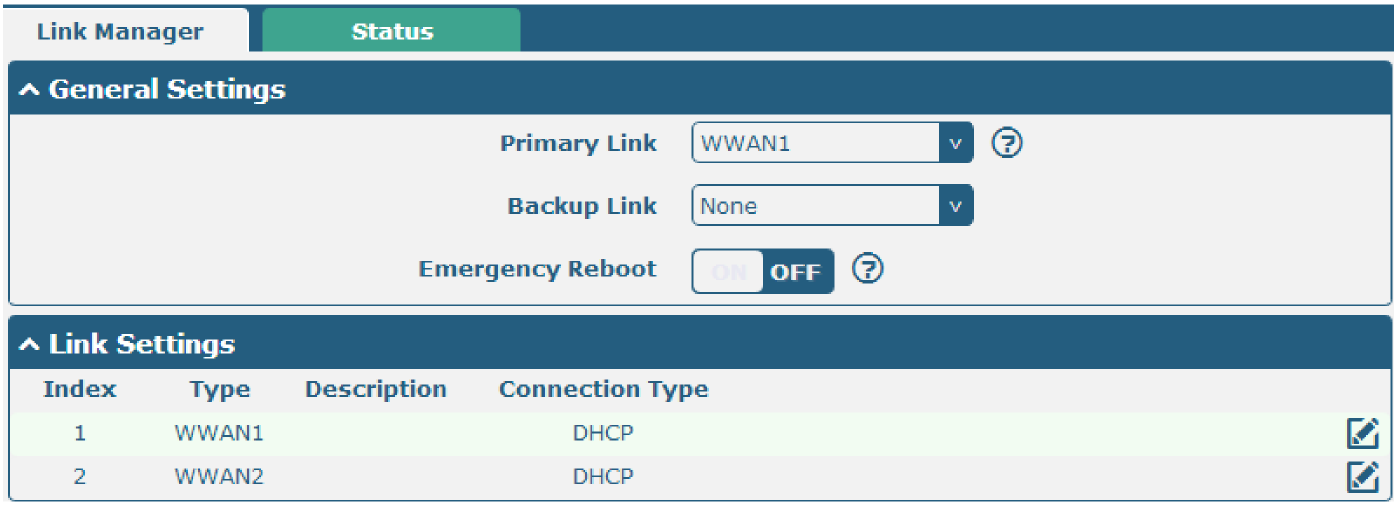
4.2 Cellular

2.2.1 Cellular Dial-Up

This section shows users how to configure the primary and backup SIM card of Cellular Dial-up.

Interface > Link Manager > General Setting

Select WWAN1 as Primary Link.



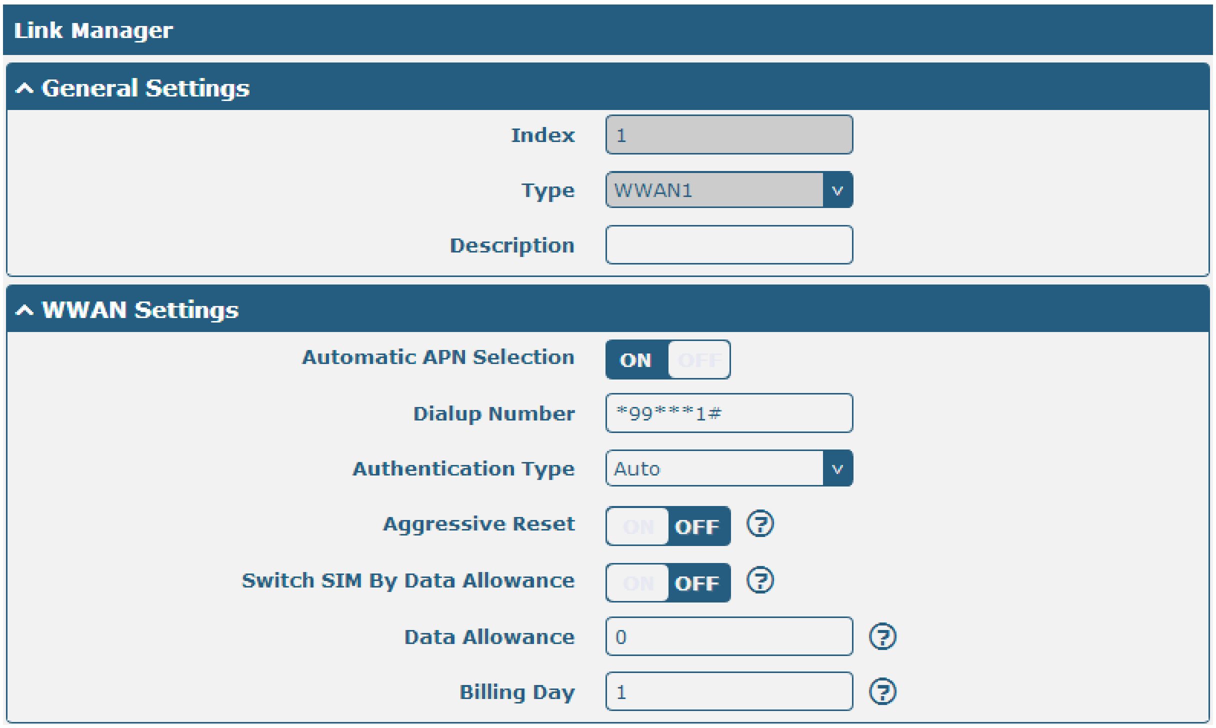
General Settings

Primary Link	WWAN1
Backup Link	None
Emergency Reboot	OFF

Link Settings

Index	Type	Description	Connection Type
1	WWAN1		DHCP
2	WWAN2		DHCP

Click ✎ to set the WWAN1's parameter according to the current ISP.

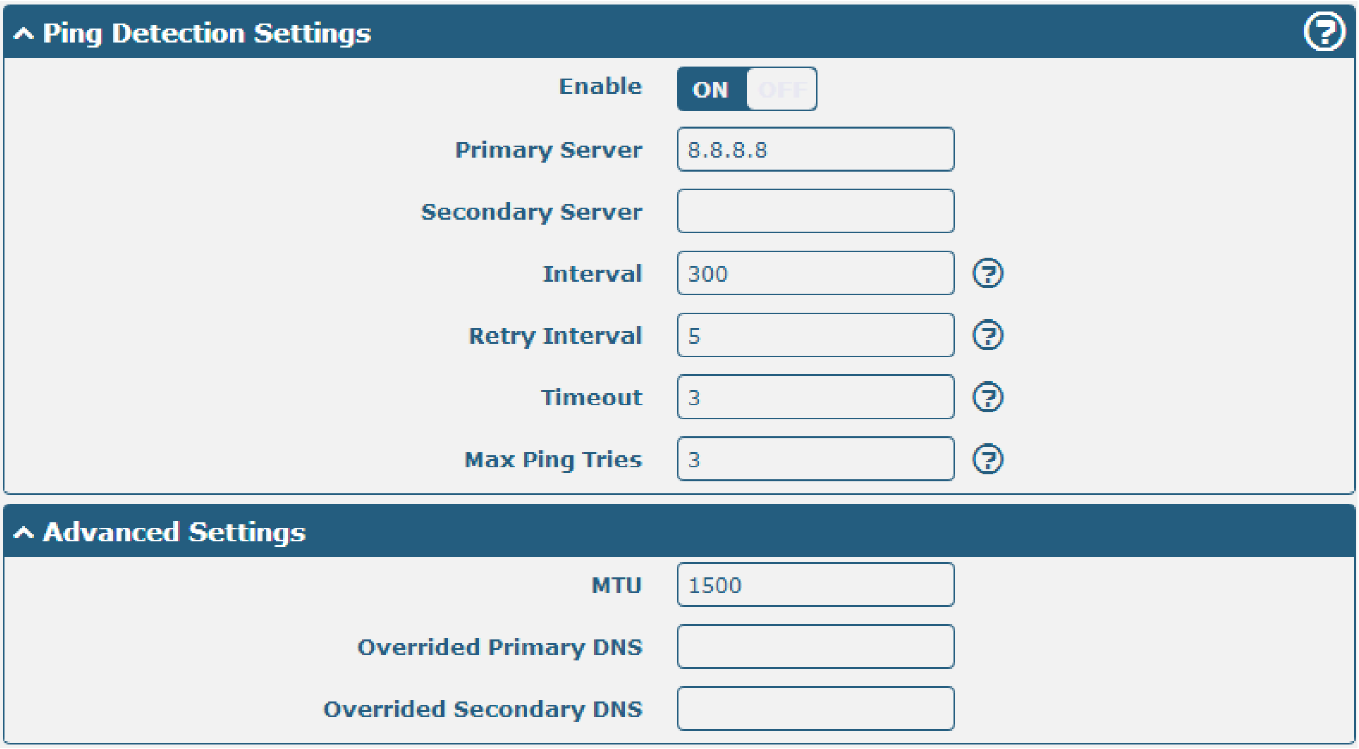


General Settings

Index	1
Type	WWAN1
Description	

WWAN Settings

Automatic APN Selection	ON
Dialup Number	*99***1#
Authentication Type	Auto
Aggressive Reset	OFF
Switch SIM By Data Allowance	OFF
Data Allowance	0
Billing Day	1



Ping Detection Settings

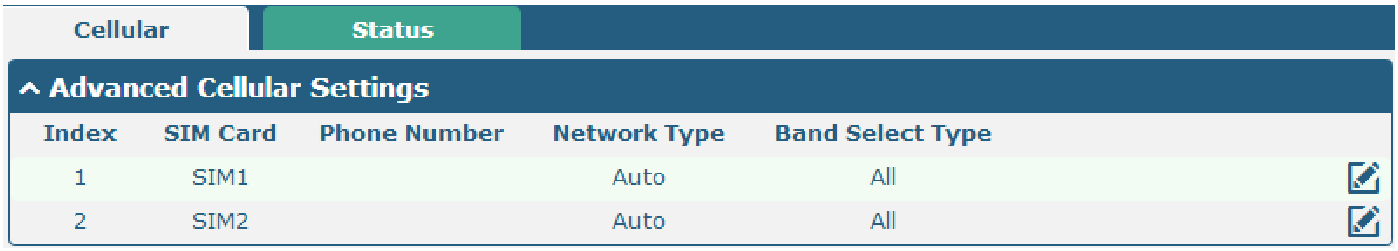
Enable	ON
Primary Server	8.8.8.8
Secondary Server	
Interval	300
Retry Interval	5
Timeout	3
Max Ping Tries	3

Advanced Settings

MTU	1500
Overrided Primary DNS	
Overrided Secondary DNS	

The modifications will take effect after click "Submit" and "save and apply" button.

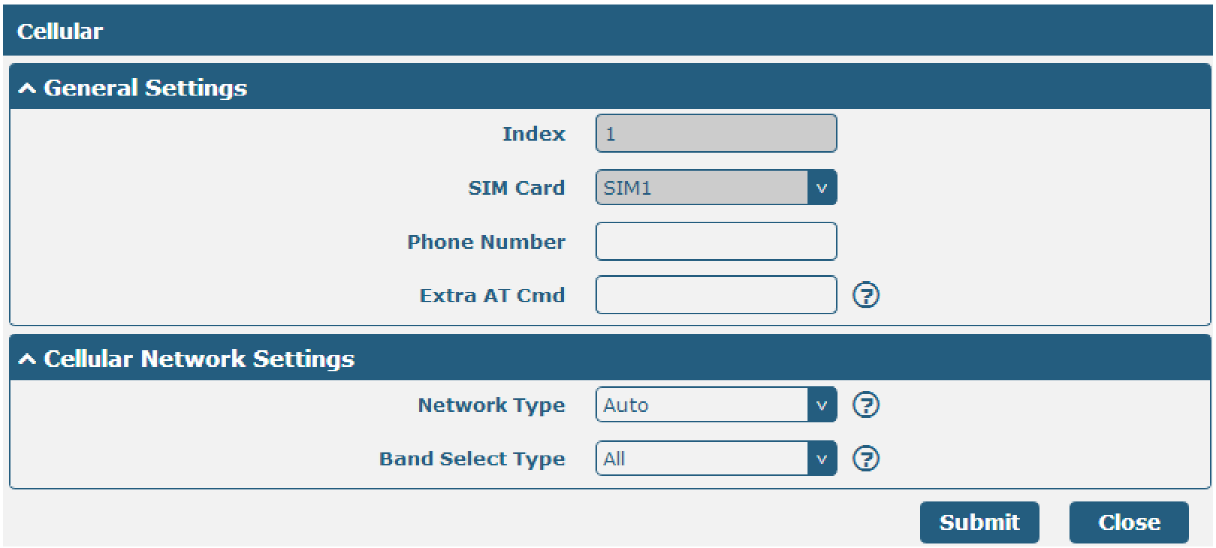
Interface > Cellular



Advanced Cellular Settings

Index	SIM Card	Phone Number	Network Type	Band Select Type
1	SIM1		Auto	All
2	SIM2		Auto	All

Click ✎ to set the SIM card's parameter according to the application requirement.



Cellular

General Settings

Index	1
SIM Card	SIM1
Phone Number	
Extra AT Cmd	

Cellular Network Settings

Network Type	Auto
Band Select Type	All

The modifications will take effect after click "Submit" and "save and apply" button.

3.2.1 SMS Remote Control

R3000 Lite supports remote control via SMS. User can use following commands to get the status of R3000 Lite, and set all the parameters of R3000 Lite.

There are three authentication types for SMS control. You can select from “Password”, “Phonenum” and “Both”.

An SMS command has following structure:

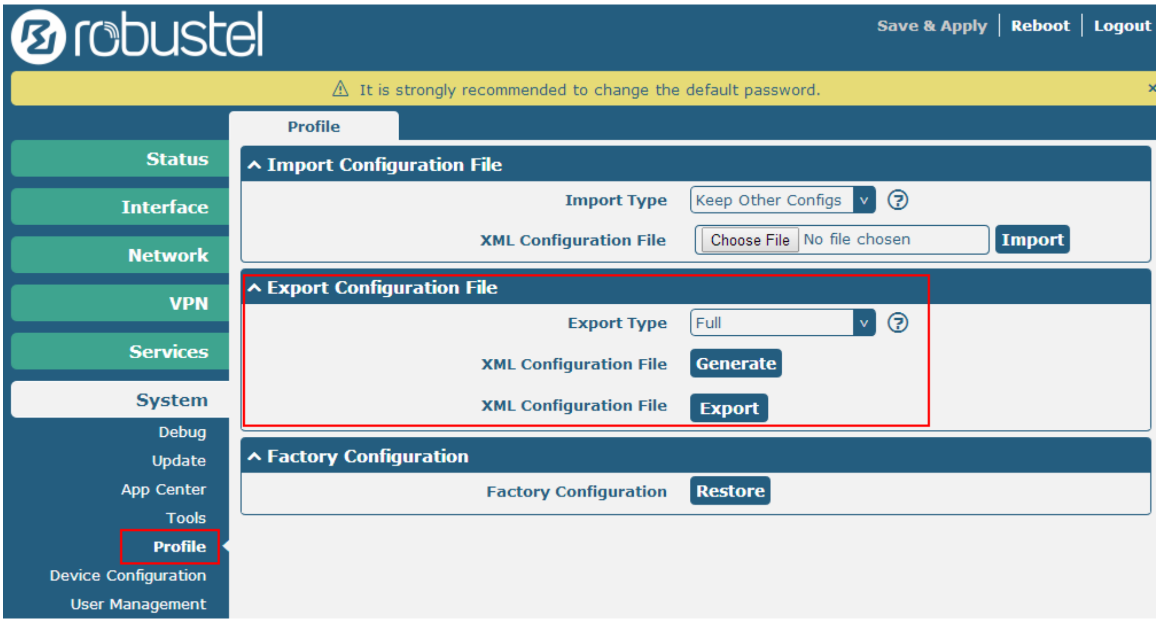
1. Password mode—Username: Password;cmd1;cmd2;cmd3; …cmdn (available every phone number).
2. Phonenum mode--cmd1; cmd2; cmd3; … cmdn (available when the SMS was sent from the phone number which had been added in R3000 Lite’s phone group).
3. Both mode-- Username: Password;cmd1;cmd2;cmd3; …cmdn (available when the SMS was sent from the phone number which had been added in R3000 Lite’s phone group).

SMS command Explanation:

1. User name and Password: it uses the same username and password as WEB manager for authentication.
2. cmd1, cmd2, cmd3 to Cmdn, the command format is the same as the CLI command, more details about CLI cmd please refer to **chapter 5 Introductions for CLI**.

   Note: Download the configure XML file from the configured web browser. The format of SMS control command can refer to the data of the XML file.

   *Go to System > Profile > Export Configuration File, select Export type as **Full**, click* Generate to generate the XML file and then click Export to export the XML file.



Import Type: Keep Other Configs
XML Configuration File: Choose File No file chosen
Export Type: Full
XML Configuration File: Generate
XML Configuration File: Export
Factory Configuration: Restore

XML command:

```
<lan>
<network max_entry_num="2">
<id>1</id>
<interface>lan0</interface>
<ip>172.16.99.11</ip>
<netmask>255.255.0.0</netmask>
```

```
<mtu>1500</mtu>
```

SMS cmd:

```
set lan network 1 interface lan0
set lan network 1 ip 172.16.99.11
set lan network 1 netmask 255.255.0.0
set lan network 1 mtu 1500
```

3. The semicolon character (‘;’) is used to separate more than one commands packed in a single SMS.
4. E.g.

admin:admin;status system

In this command, username is admin, password is admin, and the function of the command is getting the system status.

SMS received:

```
hardware_version = 1.0
firmware_version = "1.2.0 (Rev 399)"
kernel_version = 3.10.49
device_model = R3000 Lite
serial_number = 15090140040008
uptime = "0 days, 00:04:07"
system_time = "Tue Dec 22 15:02:36 2015"
```

admin:admin;reboot

In this command, username is admin, password is admin, and the command is reboot R3000 Lite.

SMS received:

```
OK
```

admin:admin;set firewall remote_ssh_access false;set firewall remote_telnet_access false

In this command, username is admin, password is admin, and the function of the command is disabling the remote_ssh and remote_telnet access.

SMS received:

```
OK
OK
```

admin:admin; set lan network 1 interface lan0;set lan network 1 ip 172.16.99.11;set lan network 1 netmask 255.255.0.0;set lan network 1 mtu 1500

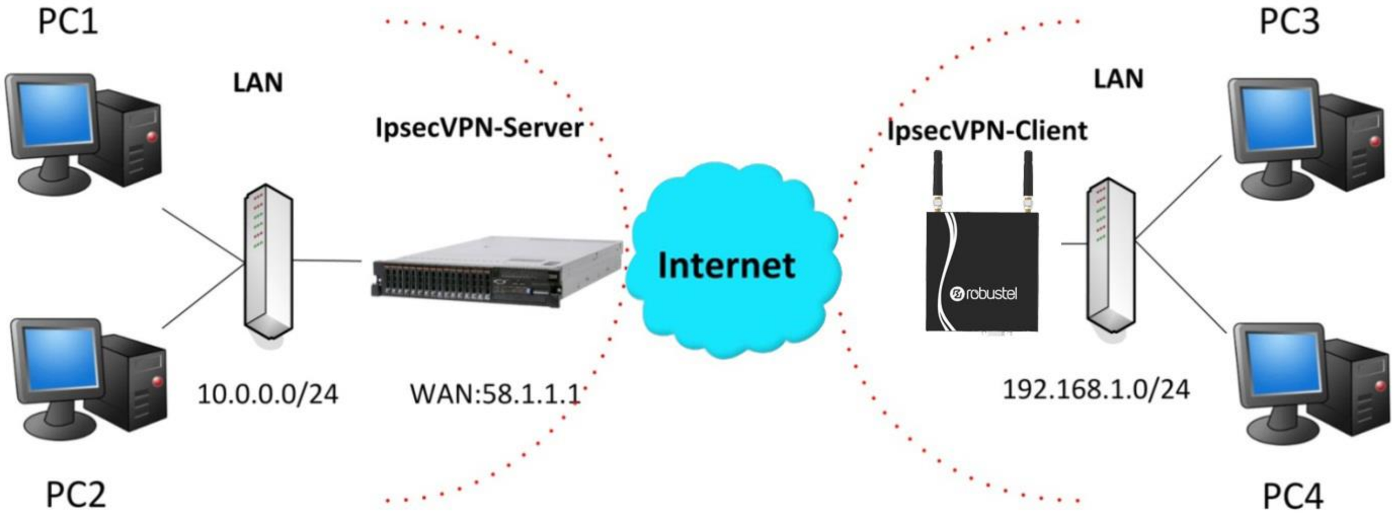
In this command, username is admin, password is admin, and the function of those commands is configuring the LAN parameter.

SMS received:

```
OK
OK
OK
OK
```

4.3 Network

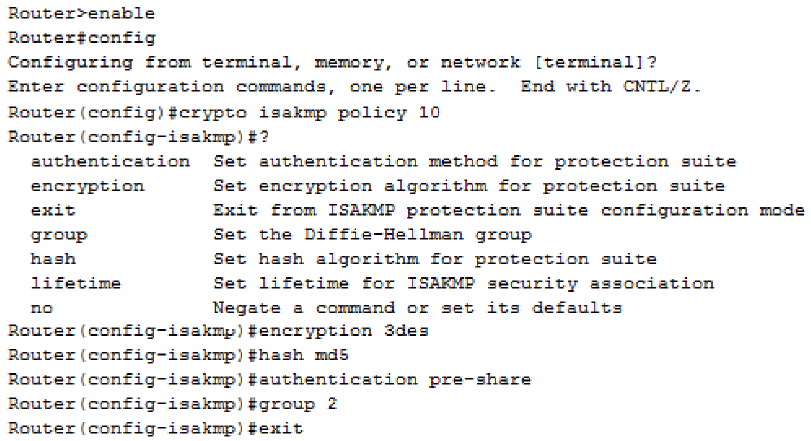
4.3.1 IPSEC VPN



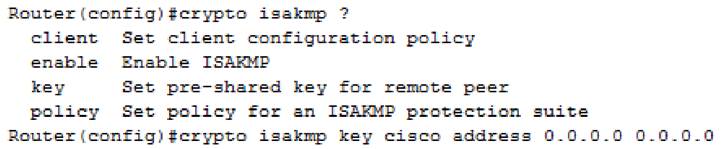
Note: *the configuration of server and client is as follows.*

IPSecVPN_SERVER:

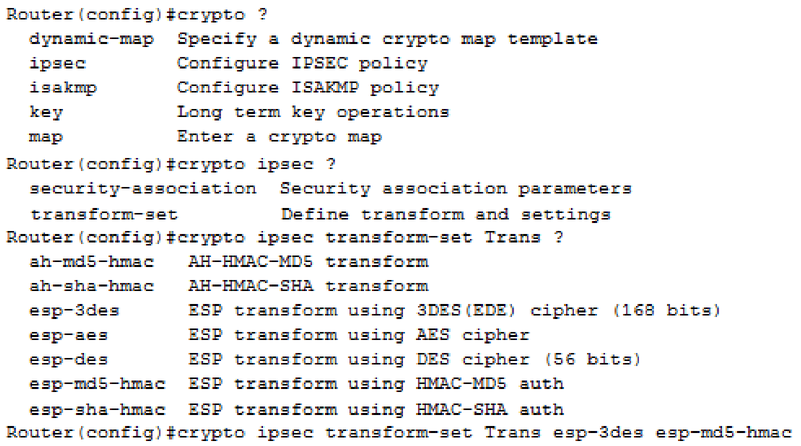
Cisco 2811:



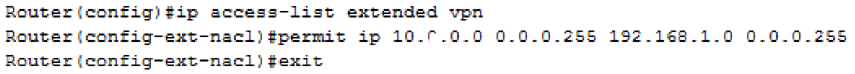
```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#?
  authentication  Set authentication method for protection suite
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#exit
```



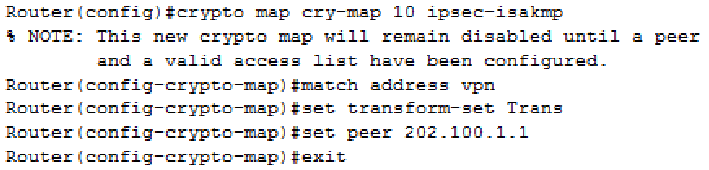
```
Router(config)#crypto isakmp ?
  client  Set client configuration policy
  enable  Enable ISAKMP
  key     Set pre-shared key for remote peer
  policy  Set policy for an ISAKMP protection suite
Router(config)#crypto isakmp key cisco address 0.0.0.0 0.0.0.0
```



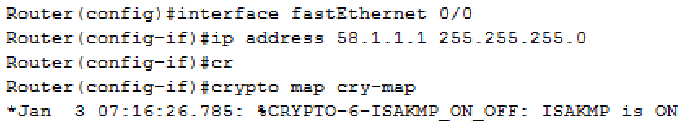
```
Router(config)#crypto ?
  dynamic-map  Specify a dynamic crypto map template
  ipsec        Configure IPSEC policy
  isakmp       Configure ISAKMP policy
  key          Long term key operations
  map          Enter a crypto map
Router(config)#crypto ipsec ?
  security-association  Security association parameters
  transform-set         Define transform and settings
Router(config)#crypto ipsec transform-set Trans ?
  ah-md5-hmac   AH-HMAC-MD5 transform
  ah-sha-hmac   AH-HMAC-SHA transform
  esp-3des      ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes       ESP transform using AES cipher
  esp-des       ESP transform using DES cipher (56 bits)
  esp-md5-hmac  ESP transform using HMAC-MD5 auth
  esp-sha-hmac  ESP transform using HMAC-SHA auth
Router(config)#crypto ipsec transform-set Trans esp-3des esp-md5-hmac
```



```
Router(config)#ip access-list extended vpn
Router(config-ext-nacl)#permit ip 10.0.0.0 0.0.0.255 192.168.1.0 0.0.0.255
Router(config-ext-nacl)#exit
```



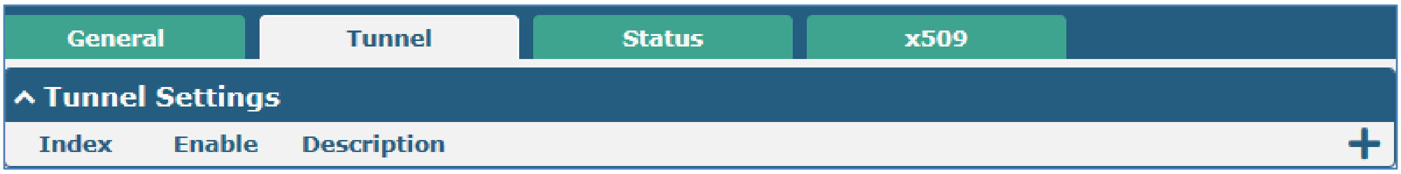
```
Router(config)#crypto map cry-map 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#match address vpn
Router(config-crypto-map)#set transform-set Trans
Router(config-crypto-map)#set peer 202.100.1.1
Router(config-crypto-map)#exit
```



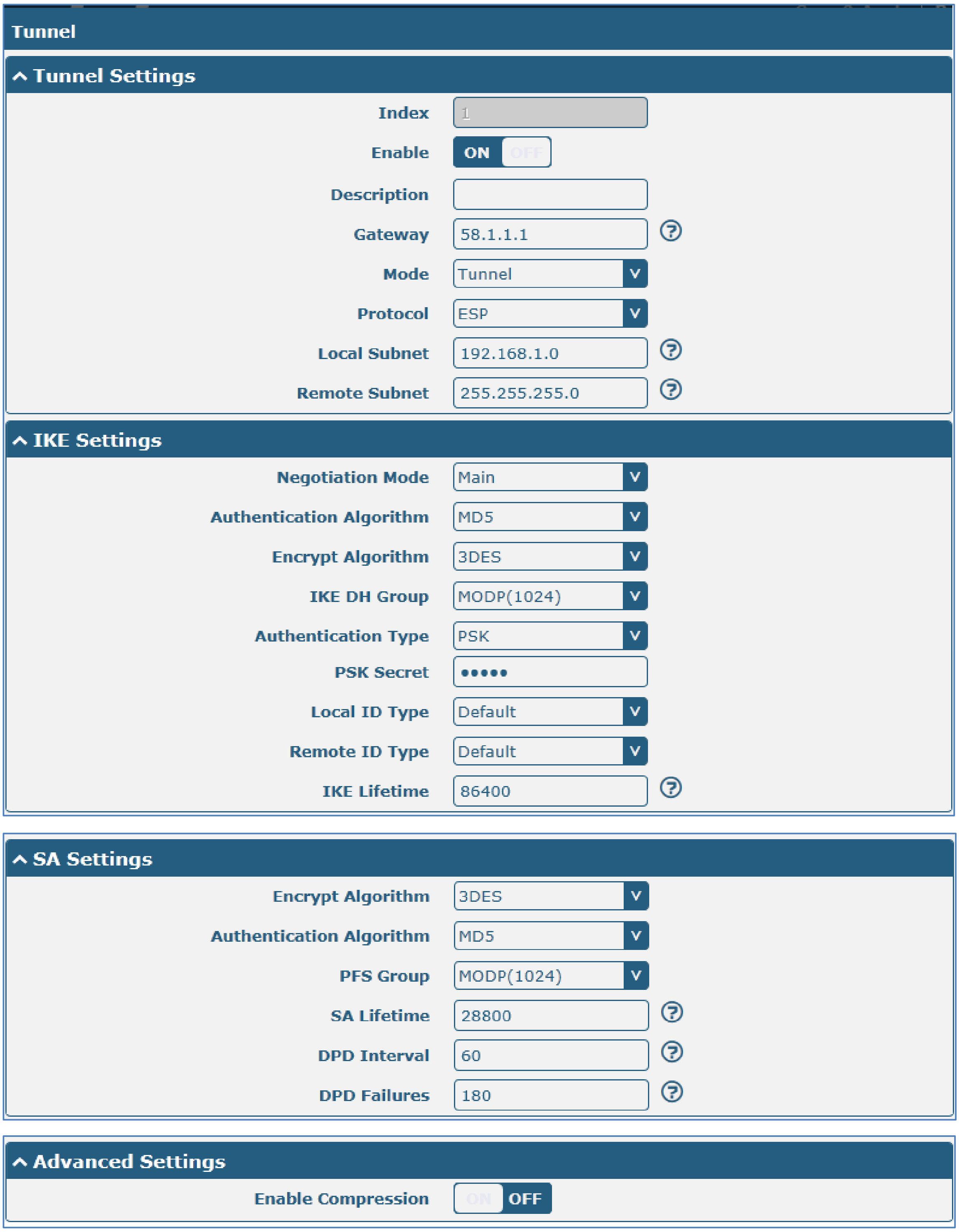
```
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 58.1.1.1 255.255.255.0
Router(config-if)#cr
Router(config-if)#crypto map cry-map
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

IPSecVPN_CLIENT:

VPN > IPSec > Tunnel



Then click "+".



Tunnel

Tunnel Settings

Index	1
Enable	ON
Description	
Gateway	58.1.1.1
Mode	Tunnel
Protocol	ESP
Local Subnet	192.168.1.0
Remote Subnet	255.255.255.0

IKE Settings

Negotiation Mode	Main
Authentication Algorithm	MD5
Encrypt Algorithm	3DES
IKE DH Group	MODP(1024)
Authentication Type	PSK
PSK Secret	●●●●●
Local ID Type	Default
Remote ID Type	Default
IKE Lifetime	86400

SA Settings

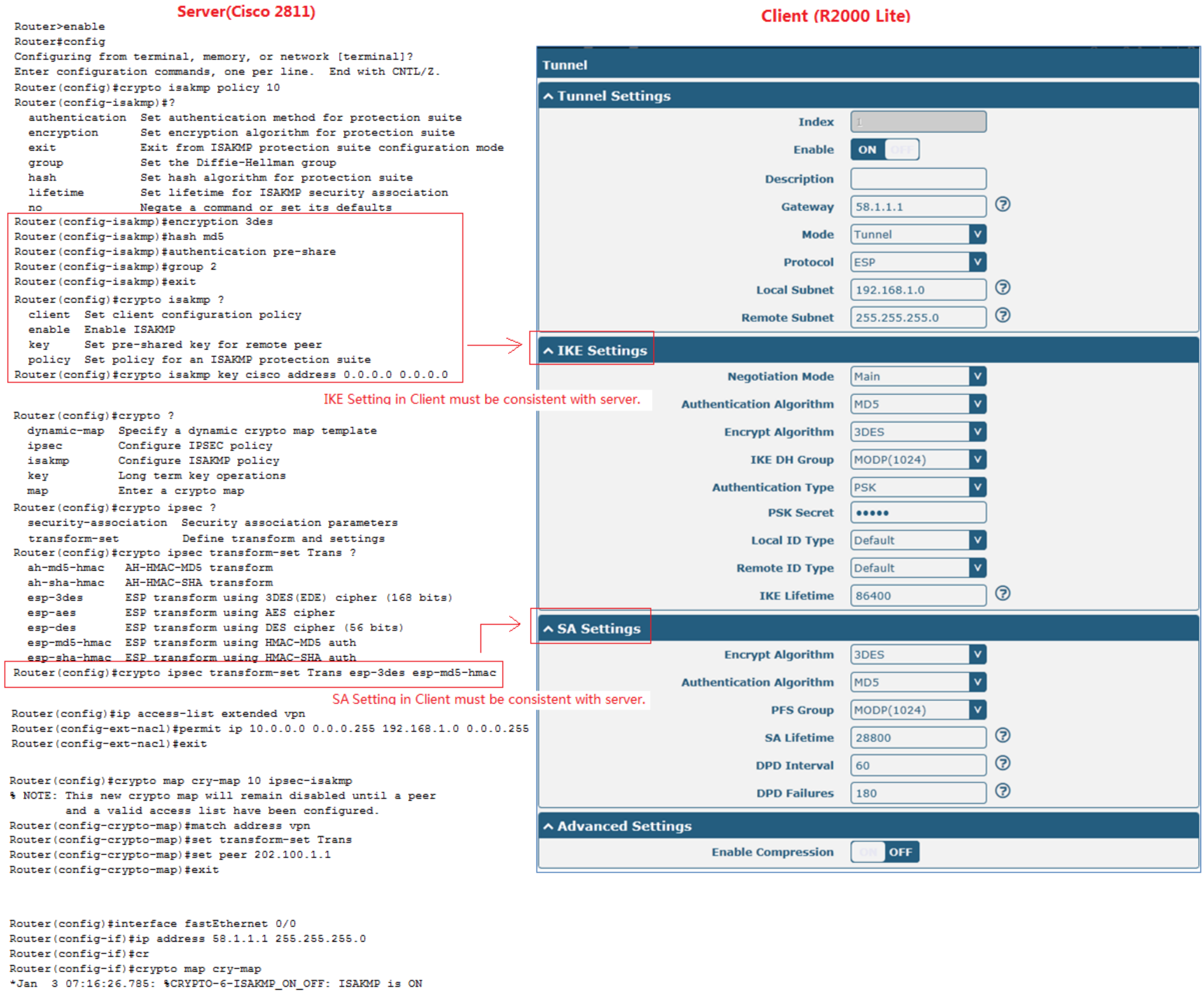
Encrypt Algorithm	3DES
Authentication Algorithm	MD5
PFS Group	MODP(1024)
SA Lifetime	28800
DPD Interval	60
DPD Failures	180

Advanced Settings

Enable Compression	OFF

The modification will take effect after clink **Submit > Save & Apply > Reboot**.

The comparison between server and client is as following picture:



Server(Cisco 2811)

```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#?
  authentication  Set authentication method for protection suite
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#exit
Router(config)#crypto isakmp ?
  client  Set client configuration policy
  enable  Enable ISAKMP
  key     Set pre-shared key for remote peer
  policy  Set policy for an ISAKMP protection suite
Router(config)#crypto isakmp key cisco address 0.0.0.0 0.0.0.0
```

IKE Setting in Client must be consistent with server.

```
Router(config)#crypto ?
  dynamic-map  Specify a dynamic crypto map template
  ipsec        Configure IPSEC policy
  isakmp       Configure ISAKMP policy
  key          Long term key operations
  map          Enter a crypto map
Router(config)#crypto ipsec ?
  security-association  Security association parameters
  transform-set         Define transform and settings
Router(config)#crypto ipsec transform-set Trans ?
  ah-md5-hmac   AH-HMAC-MD5 transform
  ah-sha-hmac   AH-HMAC-SHA transform
  esp-3des      ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes       ESP transform using AES cipher
  esp-des       ESP transform using DES cipher (56 bits)
  esp-md5-hmac  ESP transform using HMAC-MD5 auth
  esp-sha-hmac  ESP transform using HMAC-SHA auth
Router(config)#crypto ipsec transform-set Trans esp-3des esp-md5-hmac
```

SA Setting in Client must be consistent with server.

```
Router(config)#ip access-list extended vpn
Router(config-ext-nacl)#permit ip 10.0.0.0 0.0.0.255 192.168.1.0 0.0.0.255
Router(config-ext-nacl)#exit


Router(config)#crypto map cry-map 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#match address vpn
Router(config-crypto-map)#set transform-set Trans
Router(config-crypto-map)#set peer 202.100.1.1
Router(config-crypto-map)#exit



Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 58.1.1.1 255.255.255.0
Router(config-if)#cr
Router(config-if)#crypto map cry-map
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Client (R2000 Lite)

Tunnel

^ Tunnel Settings

Index	1
Enable	ON
Description	
Gateway	58.1.1.1
Mode	Tunnel
Protocol	ESP
Local Subnet	192.168.1.0
Remote Subnet	255.255.255.0

^ IKE Settings

Negotiation Mode	Main
Authentication Algorithm	MD5
Encrypt Algorithm	3DES
IKE DH Group	MODP(1024)
Authentication Type	PSK
PSK Secret	•••••
Local ID Type	Default
Remote ID Type	Default
IKE Lifetime	86400

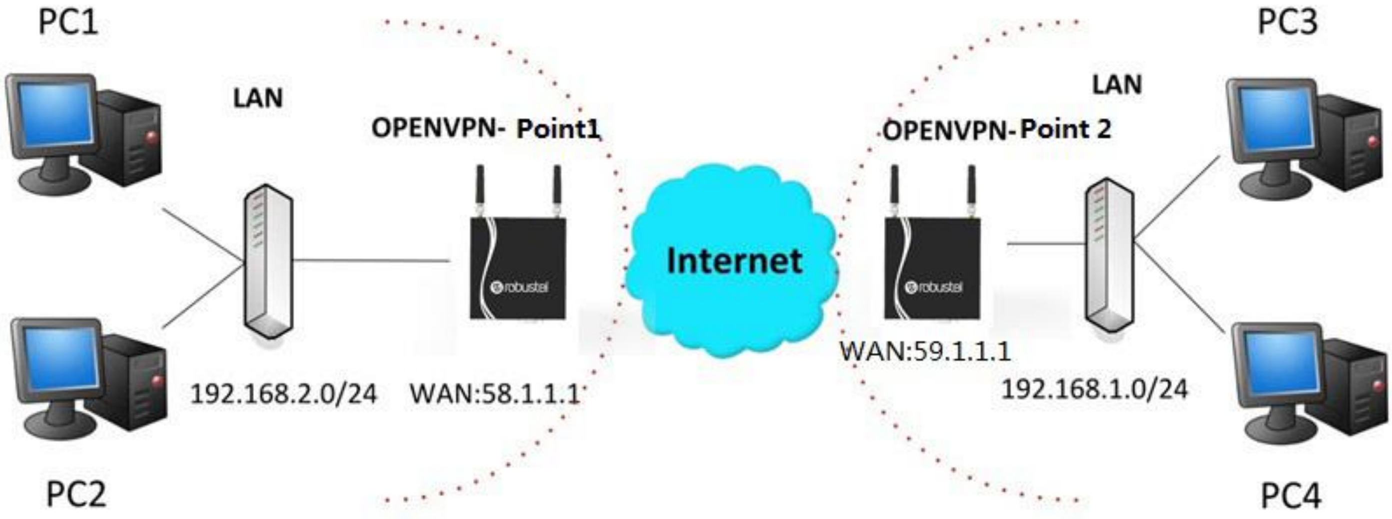
^ SA Settings

Encrypt Algorithm	3DES
Authentication Algorithm	MD5
PFS Group	MODP(1024)
SA Lifetime	28800
DPD Interval	60
DPD Failures	180

^ Advanced Settings

Enable Compression	OFF

4.3.2 OPENVPN

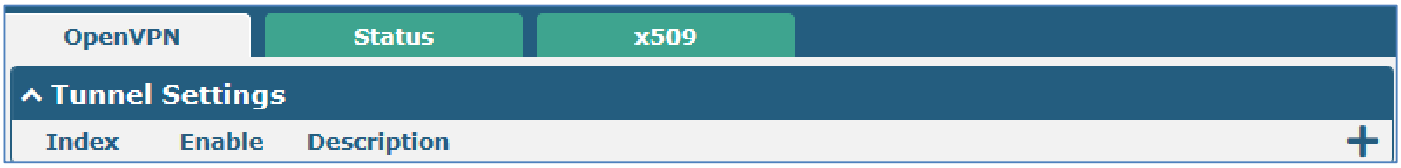


Note: *the configuration of two points is as follows.*

OPENVPN (p2p):

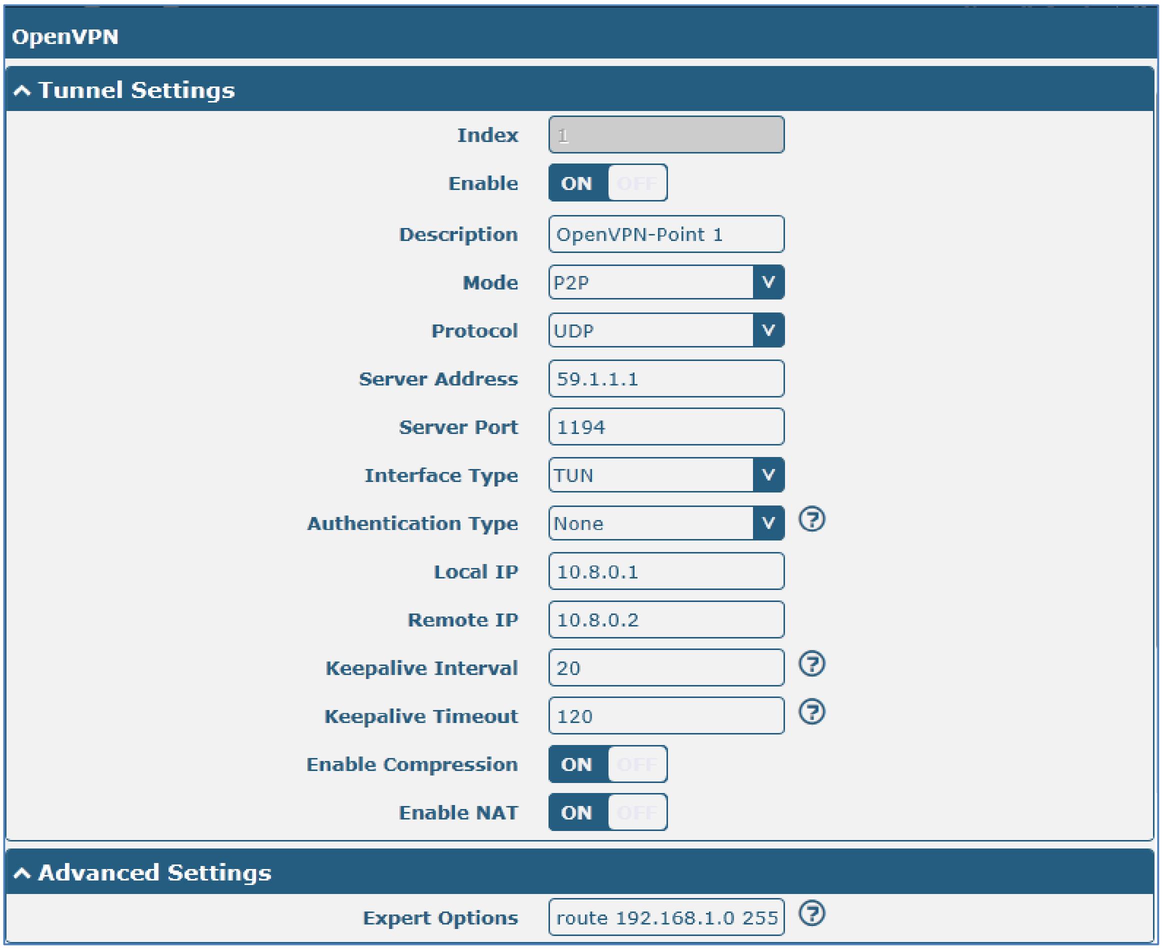
Point 1

VPN > OpenVPN > OpenVPN



Index	Enable	Description

Click “+”.



OpenVPN

^ Tunnel Settings

Index	1
Enable	ON OFF
Description	OpenVPN-Point 1
Mode	P2P
Protocol	UDP
Server Address	59.1.1.1
Server Port	1194
Interface Type	TUN
Authentication Type	None
Local IP	10.8.0.1
Remote IP	10.8.0.2
Keepalive Interval	20
Keepalive Timeout	120
Enable Compression	ON OFF
Enable NAT	ON OFF

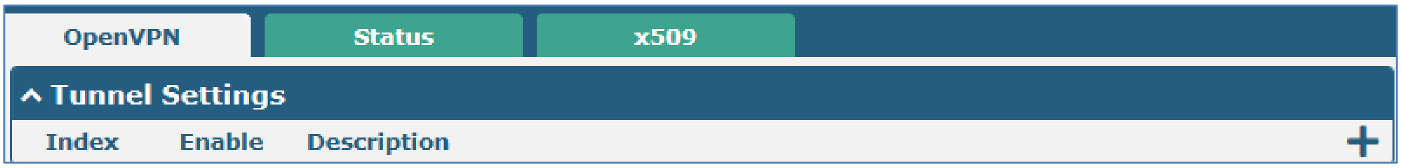
^ Advanced Settings

Expert Options	route 192.168.1.0 255

The modifications will take effect after click “Submit > Save & Apply”.

Point 2

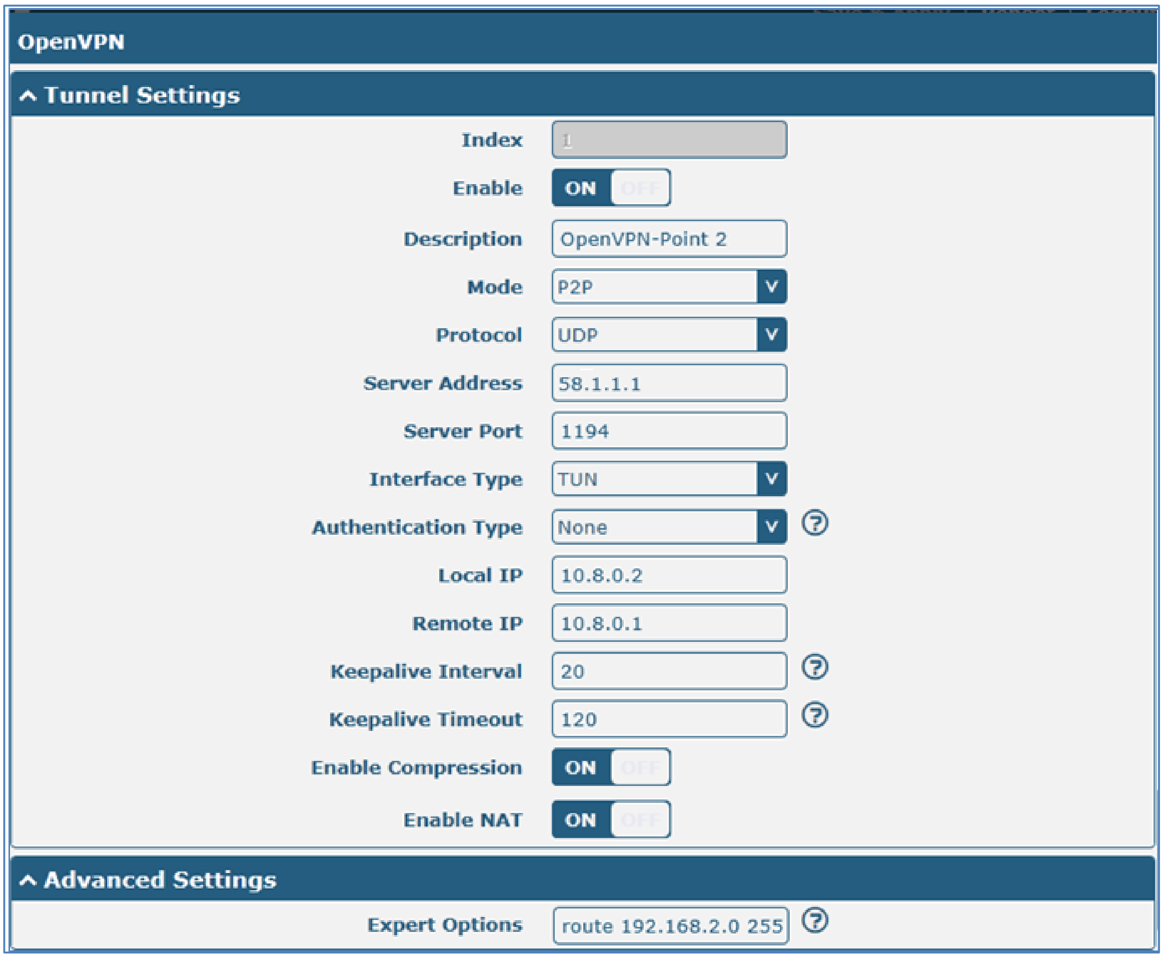
VPN > OpenVPN > OpenVPN



^ Tunnel Settings

Index	Enable	Description

Click “+”.



OpenVPN

Tunnel Settings

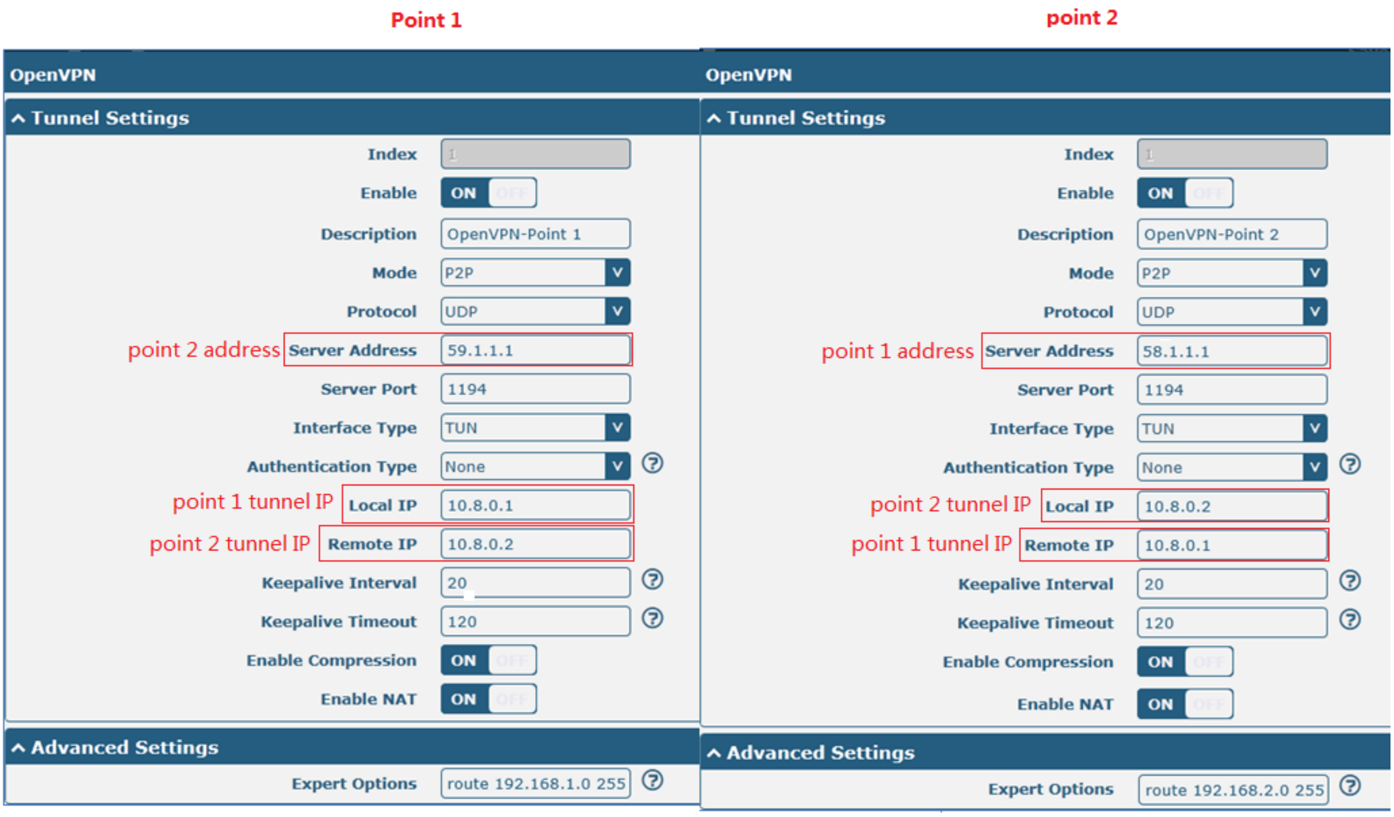
Index	1
Enable	ON
Description	OpenVPN-Point 2
Mode	P2P
Protocol	UDP
Server Address	58.1.1.1
Server Port	1194
Interface Type	TUN
Authentication Type	None
Local IP	10.8.0.2
Remote IP	10.8.0.1
Keepalive Interval	20
Keepalive Timeout	120
Enable Compression	ON
Enable NAT	ON

Advanced Settings

Expert Options	route 192.168.2.0 255

The modifications will take effect after click **Submit > Save & Apply**.

The comparison between point 1 and point 2 is as following picture:



Point 1

OpenVPN

^ Tunnel Settings

	Index	1
	Enable	ON OFF
	Description	OpenVPN-Point 1
	Mode	P2P
	Protocol	UDP
point 2 address	Server Address	59.1.1.1
	Server Port	1194
	Interface Type	TUN
	Authentication Type	None
point 1 tunnel IP	Local IP	10.8.0.1
point 2 tunnel IP	Remote IP	10.8.0.2
	Keepalive Interval	20
	Keepalive Timeout	120
	Enable Compression	ON OFF
	Enable NAT	ON OFF

^ Advanced Settings

	Expert Options	route 192.168.1.0 255

point 2

OpenVPN

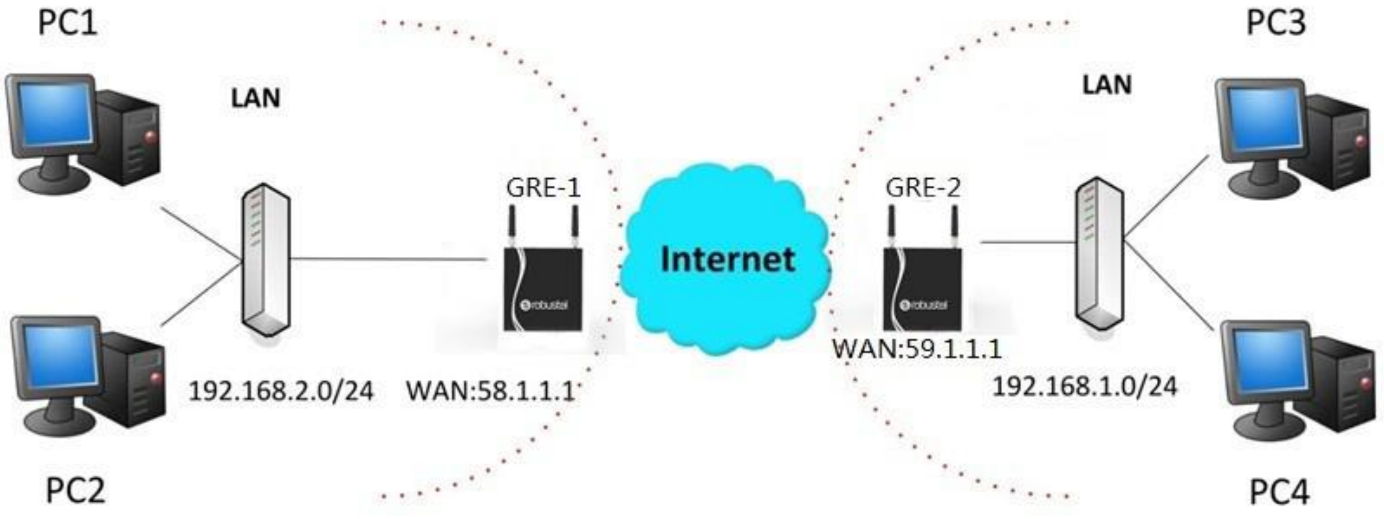
^ Tunnel Settings

	Index	1
	Enable	ON OFF
	Description	OpenVPN-Point 2
	Mode	P2P
	Protocol	UDP
point 1 address	Server Address	58.1.1.1
	Server Port	1194
	Interface Type	TUN
	Authentication Type	None
point 2 tunnel IP	Local IP	10.8.0.2
point 1 tunnel IP	Remote IP	10.8.0.1
	Keepalive Interval	20
	Keepalive Timeout	120
	Enable Compression	ON OFF
	Enable NAT	ON OFF

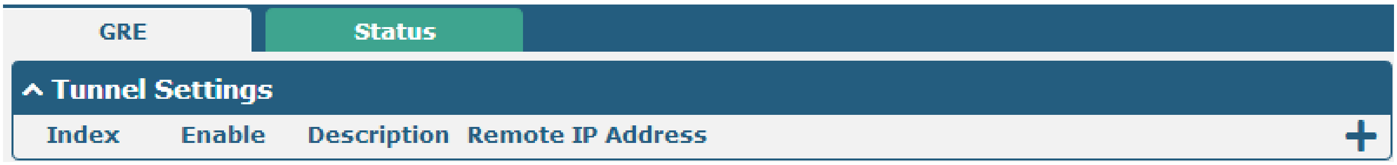
^ Advanced Settings

	Expert Options	route 192.168.2.0 255

4.3.3 GRE VPN



VPN > GRE > GRE

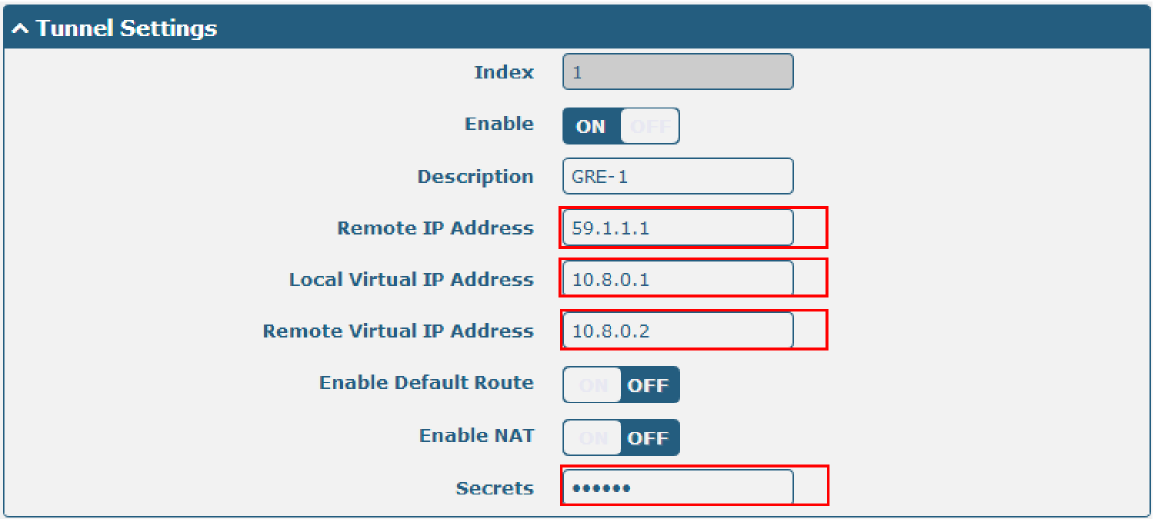


Tunnel Settings

Index	Enable	Description	Remote IP Address	+

Click “+”.

GRE-1:

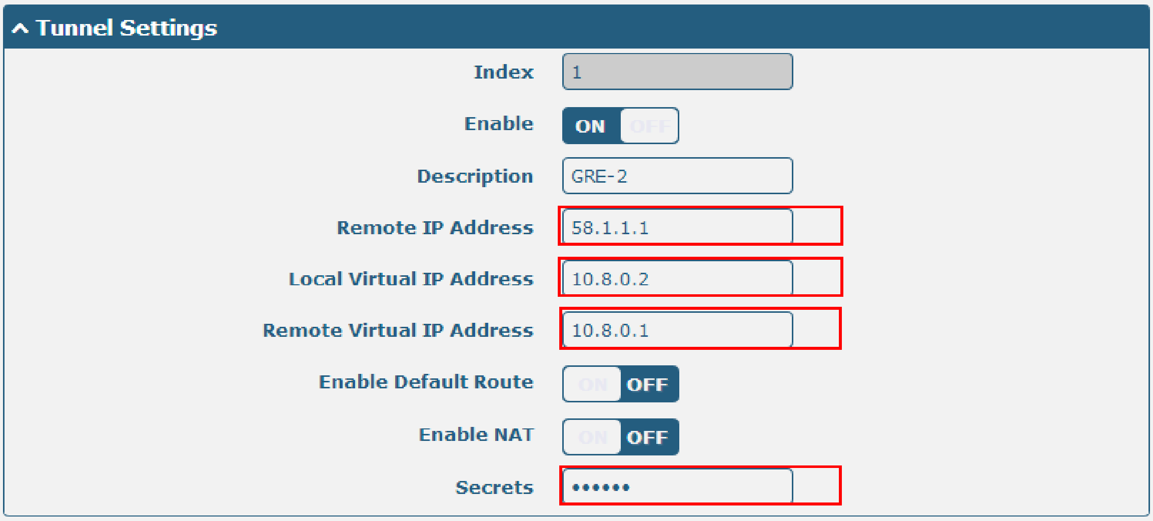


Tunnel Settings

Index	1
Enable	ON
Description	GRE-1
Remote IP Address	59.1.1.1
Local Virtual IP Address	10.8.0.1
Remote Virtual IP Address	10.8.0.2
Enable Default Route	OFF
Enable NAT	OFF
Secrets	••••••

The modifications will take effect after click **Submit > Save & Apply**.

GRE-2:

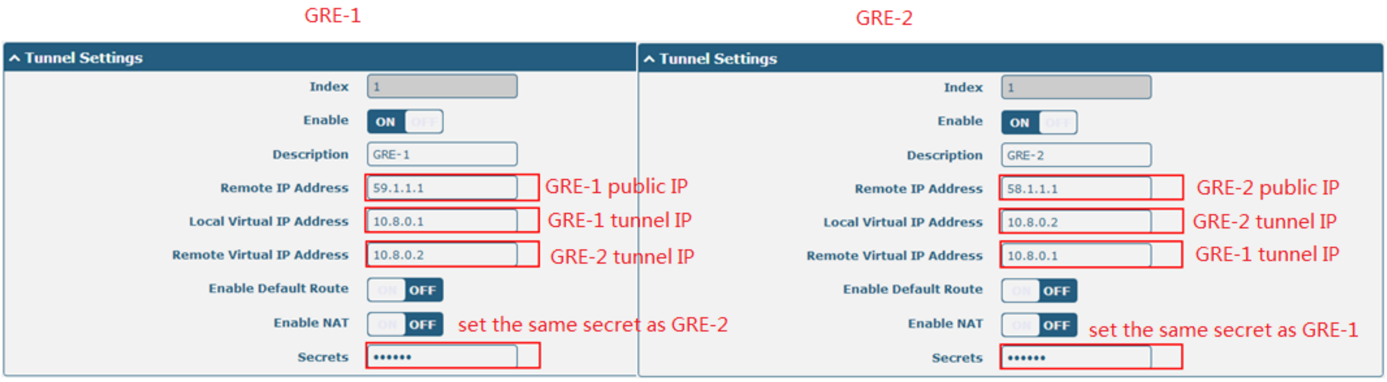


Tunnel Settings

Index	1
Enable	ON
Description	GRE-2
Remote IP Address	58.1.1.1
Local Virtual IP Address	10.8.0.2
Remote Virtual IP Address	10.8.0.1
Enable Default Route	OFF
Enable NAT	OFF
Secrets	••••••

The modifications will take effect after click **Submit > Save & Apply**.

The comparison between point 1 and point 2 is as following picture:



GRE-1

^ Tunnel Settings

Index	1	
Enable	ON	
Description	GRE-1	
Remote IP Address	59.1.1.1	GRE-1 public IP
Local Virtual IP Address	10.8.0.1	GRE-1 tunnel IP
Remote Virtual IP Address	10.8.0.2	GRE-2 tunnel IP
Enable Default Route	OFF	
Enable NAT	OFF	set the same secret as GRE-2
Secrets	••••••	

GRE-2

^ Tunnel Settings

Index	1	
Enable	ON	
Description	GRE-2	
Remote IP Address	58.1.1.1	GRE-2 public IP
Local Virtual IP Address	10.8.0.2	GRE-2 tunnel IP
Remote Virtual IP Address	10.8.0.1	GRE-1 tunnel IP
Enable Default Route	OFF	
Enable NAT	OFF	set the same secret as GRE-1
Secrets	••••••	

Chapter 5 Introductions for CLI

5.1 What's CLI

The R3000 Lite command-line interface (CLI) is a software interface providing another way to set the parameters of equipment from the SSH or through a telnet network connection.

Route login:

Router login: admin

Password: admin

#

CLI commands:

# ? (***Note***: the '?' won't display on the page.)

!	Comments
add	Add a list entry of configuration
clear	Clear statistics
config	Configuration operation
debug	Output debug information to the console
del	Delete a list entry of configuration
exit	Exit from the CLI
help	Display an overview of the CLI syntax
ping	Send messages to network hosts
reboot	Halt and perform a cold restart
route	Static route modify dynamically, this setting will not be saved
set	Set system configuration
show	Show system configuration
status	Show running system information
tftpupdate	Update firmware using tftp
traceroute	Print the route packets trace to network host
urlupdate	Update firmware using http or ftp
ver	Show version of firmware

5.2 How to Configure the CLI

Following is a list about the description of help and the error should be encountered in the configuring program.

Commands /tips	Description
?	Typing a question mark "?" will show you the help information.
Ctrl+c	Press these two keys at the same time, except its "copy" function but also can be used for "break" out of the setting program.
Syntax error: The command is not completed	Command is not completed.
Tick space key+ Tab key	It can help you finish you command. Example: # config (tick Enter key) Syntax error: The command is not completed # config (tick space key+ Tab key) commit save_and_apply loaddefault
# config save_and_apply / #config commit	When you finish your setting, you should enter those commands to make your setting take effect on the device. ***Note:*** commit and save_and_apply plays the same role.

5.2.1 QuickStart with Configuration Examples

The best and quickest way to master CLI is firstly to view all features from the webpage and then reading all CLI commands at a time, finally learn to configure it with some reference examples.

Example 1: Show current version

```
# status system
hardware_version = 1.0
firmware_version = "1.2.0 (Rev 399)"
kernel_version = 3.10.49
device_model = R3000 Lite
serial_number = 15090140040008
uptime = "0 days, 00:04:07"
system_time = "Tue Dec 22 15:02:36 2015"
```

Example 2: Update firmware via tftp

```
# tftpupdate (space+?)
   firmware    New firmware
# tftpupdate firmware (space+?)
   String    Firmware name
# tftpupdate firmware R3000-firmware-sysupgrade-unknown.bin host 192.168.100.99 //enter a new firmware name
Downloading
R3000-firmware-s 100% |*******************************|    5018k    0:00:00 ETA
Flashing
Checking 100%
Decrypting 100%
```

```
Flashing 100%
Verifying 100%
Verfify Success
upgrade success                                    //update success
# config save_and_apply
OK                                         // save and apply current configuration, make you configuration effect
```

Example 3: Set link-manager

```
# set
# set
   at_over_telnet        AT Over Telnet
   cellular              Cellular
   ddns                  Dynamic DNS
   ethernet              Ethernet
   event                 Event Management
   firewall              Firewall
   gre                   GRE
   ipsec                 IPSec
   lan                   Local Area Network
   link_manager          Link Manager
   ntp                   NTP
   openvpn               OpenVPN
   reboot                Automatic Reboot
   robustlink            Robustlink
   route                 Route
   sms                   SMS
   snmp                  SNMP agent
   ssh                   SSH
   syslog                Syslog
   system                System
   user_management       User Management
   vrrp                  VRRP
   web_server            Web Server
# set link_manager
   primary_link          Primary Link
   backup_link           Backup Link
   backup_mode           Backup Mode
   emergency_reboot      Emergency Reboot
   link                 Link Settings
# set link_manager primary_link (space+?)
Enum    Primary Link (wwan1/wwan2/wan)
# set link_manager primary_link wwan1                    //select “wwan1” as primary_link
OK                                                       //setting succeed
# set link_manager link 1
```

```
   type                 Type
   desc                 Description
   connection_type      Connection Type
   wwan                 WWAN Settings
   static_addr          Static Address Settings
   pppoe                PPPoE Settings
   ping                 Ping Settings
   mtu                  MTU
   dns1_overrided       Overrided Primary DNS
   dns2_overrided       Overrided Secondary DNS
# set link_manager link 1 type wwan1
OK
# set link_manager link 1 wwan
   auto_apn                       Automatic APN Selection
   apn                            APN
   username                       Username
   password                       Password
   dialup_number                  Dialup Number
   auth_type                      Authentication Type
   aggressive_reset               Aggressive Reset
   switch_by_data_allowance       Switch SIM By Data Allowance
   data_allowance                 Data Allowance
   billing_day                    Billing Day
# set link_manager link 1 wwan switch_by_data_allowance true
OK
#
# set link_manager link 1 wwan data_allowance 100                //open cellular switch_by_data_traffic
OK                                                               //setting succeed
# set link_manager link 1 wwan billing_day 1                  //setting specifies the day of month for billing
OK                                                               // setting succeed
…
# config save_and_apply
OK                                      // save and apply current configuration, make you configuration effect
```

Example 4: Set LAN IP address

```
# show lan all
network {
    id = 1
    interface = lan0
    ip = 192.168.0.1
    netmask = 255.255.255.0
    mtu = 1500
    dhcp {
        enable = true
```

```
                mode = server
                relay_server = ""
                pool_start = 192.168.0.2
                pool_end = 192.168.0.100
                netmask = 255.255.255.0
                gateway = ""
                primary_dns = ""
                secondary_dns = ""
                wins_server = ""
                lease_time = 120
                expert_options = ""
                debug_enable = false
        }
}
multi_ip {
        id = 1
        interface = lan0
        ip = 172.16.99.11
        netmask = 255.255.0.0
}
#
# set lan
    network      Network Settings
    multi_ip    Multiple IP Address Settings
    vlan          VLAN
# set lan network 1(space+?)
    interface    Interface
    ip                IP Address
    netmask       Netmask
    mtu               MTU
    dhcp             DHCP Settings
# set lan network 1 interface lan0
OK
# set lan network 1 ip 172.16.99.22                    //set IP address for lan
OK                                                     //setting succeed
# set lan network 1 netmask 255.255.0.0
OK
#
…
# config save_and_apply
OK                                            // save and apply current configuration, make you configuration effect
```

Example 5: CLI for setting Cellular

```
# show cellular all
```

```
sim {
        id = 1
        card = sim1
        phone_number = ""
        extra_at_cmd = ""
        network_type = auto
        band_select_type = all
        band_lte_800 = false
        band_lte_850 = false
        band_lte_900 = false
        band_lte_1800 = false
        band_lte_1900 = false
        band_lte_2100 = false
        band_lte_2600 = false
        band_lte_1700 = false
        band_lte_700 = false
        band_tdd_lte_2600 = false
        band_tdd_lte_1900 = false
        band_tdd_lte_2300 = false
        band_tdd_lte_2500 = false
}
sim {
        id = 2
        card = sim2
        phone_number = ""
        extra_at_cmd = ""
        network_type = auto
        band_select_type = all
        band_lte_800 = false
        band_lte_850 = false
        band_lte_900 = false
        band_lte_1800 = false
        band_lte_1900 = false
        band_lte_2100 = false
        band_lte_2600 = false
        band_lte_1700 = false
        band_lte_700 = false
        band_tdd_lte_2600 = false
        band_tdd_lte_1900 = false
        band_tdd_lte_2300 = false
        band_tdd_lte_2500 = false
}
# set(space+?)
at_over_telnet      cellular       ddns           dhcp           dns
event               firewall       ipsec          lan            link_manager
```

```
ntp                 openvpn             reboot              route               serial_port
sms                 snmp                syslog              system              user_management
vrrp
# set cellular(space+?)
  sim    SIM Settings
# set cellular sim(space+?)
  Integer    Index (1..2)

# set cellular sim 1(space+?)
  card                    SIM Card
  phone_number            Phone Number
  extra_at_cmd            Extra AT Cmd
  network_type            Network Type
  band_select_type        Band Select Type
  band_lte_800          LTE 800 (band 20)
  band_lte_850          LTE 850 (band 5)
  band_lte_900          LTE 900 (band 8)
  band_lte_1800         LTE 1800 (band 3)
  band_lte_1900         LTE 1900 (band 2)
  band_lte_2100         LTE 2100 (band 1)
  band_lte_2600         LTE 2600 (band 7)
  band_lte_1700         LTE 1700 (band 4)
  band_lte_700          LTE 700 (band 17)
  band_tdd_lte_2600    TDD LTE 2600 (band 38)
  band_tdd_lte_1900    TDD LTE 1900 (band 39)
  band_tdd_lte_2300    TDD LTE 2300 (band 40)
  band_tdd_lte_2500    TDD LTE 2500 (band 41)
# set cellular sim 1 phone_number 18620435279
OK
…
# config save_and_apply
OK                                      // save and apply current configuration, make you configuration effect
```

5.3 Commands Reference

commands	**syntax**	**description**
Debug	Debug *parameters*	Turn on or turn off debug function
Show	Show *parameters*	Show current configuration of each function , if we need to see all please using “show running ”
Set	Set *parameters*	All the function parameters are set by commands set and add, the difference is that set is for the single parameter and add is for the list parameter
Add	Add *parameters*	

Note: Download the config.XML file from the configured web browser. The command format can refer to the config.XML file format.

Glossary

Abbreviations	Description
AC	Alternating Current
APN	Access Point Name of GPRS Service Provider Network
ASCII	American Standard Code for Information Interchange
CE	Conformité Européene (European Conformity)
CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface for batch scripting
CSD	Circuit Switched Data
CTS	Clear to Send
dB	Decibel
dBi	Decibel Relative to an Isotropic radiator
DC	Direct Current
DCD	Data Carrier Detect
DCE	Data Communication Equipment (typically modems)
DCS 1800	Digital Cellular System, also referred to as PCN
DI	Digital Input
DO	Digital Output
DSR	Data Set Ready
DTE	Data Terminal Equipment
DTMF	Dual Tone Multi-frequency
DTR	Data Terminal Ready
EMC	Electromagnetic Compatibility
EMI	Electro-Magnetic Interference
ESD	Electrostatic Discharges
ETSI	European Telecommunications Standards Institute
EVDO	Evolution-Data Optimized
FDD LTE	Frequency Division Duplexing Long Term Evolution
GND	Ground
GPRS	General Packet Radio Service
GRE	generic route encapsulation
ID	identification data
IMEI	International Mobile Equipment Identification
IP	Internet Protocol
IPSec	Internet Protocol Security
kbps	kbits per second
L2TP	Layer 2 Tunneling Protocol
LAN	local area network

LED	Light Emitting Diode
M2M	Machine to Machine
MAX	Maximum
Min	Minimum
MO	Mobile Originated
MS	Mobile Station
MT	Mobile Terminated
OpenVPN	Open Virtual Private Network
PAP	Password Authentication Protocol
PC	Personal Computer
PCN	Personal Communications Network, also referred to as DCS 1800
PDU	Protocol Data Unit
PIN	Personal Identity Number
PLCs	Program Logic Control System
PPP	Point-to-point Protocol
PPTP	Point to Point Tunneling Protocol
PSU	Power Supply Unit
PUK	Personal Unblocking Key
R&TTE	Radio and Telecommunication Terminal Equipment
RF	Radio Frequency
RTC	Real Time Clock
RTS	Request to Send
RTU	Remote Terminal Unit
Rx	Receive Direction
SDK	Software Development Kit
SIM	subscriber identification module
SMS	Short Message Service
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TE	Terminal Equipment, also referred to as DTE
Tx	Transmit Direction
UART	Universal Asynchronous Receiver-transmitter
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
USSD	Unstructured Supplementary Service Data
VDC	Volts Direct current
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VSWR	Voltage Stationary Wave Ratio
WAN	Wide Area Network