Robustel GoRugged R3000-3P

Industrial Cellular Router

User Guide

Document Name:		**User Guide**
Firmware	:	**1.01.00**
Date	:	**2014-03-11**
Status	:	**Confidential**
Doc ID	:	**RT_UG_R3000-3P_v.1.0.0**

Robustel

www.robustel.com

About This Document

This document describes hardware and software of Robustel R3000-3P, Dual SIM Industrial Cellular Router.

Copyright© Guangzhou Robustel Technologies Co., Limited
All Rights Reserved.

Trademarks and Permissions

Robustel are trademark of Guangzhou Robustel Technologies Co. Limited.
All other trademarks and trade names mentioned in this document are the property of their respective holders.

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 revision 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 Contact Information

Tel : +86-18924045664
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 are 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 3G 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.

***Note**: Some airlines may permit the use of 3G 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 3G in vehicle in your country before installing the router.
- The driver or operator of any vehicle should not operate the route while in control of a vehicle.
- 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 follow:
- Do not expose the router to extreme conditions such as high humidity / rain, high temperatures, 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.

FCC INFORMATION

This device complies with part 15 of the FCC Rules. Operation is subject to the condition that this device does not cause harmful interference.

Caution: Any changes or modifications not expressly approved by the party responsible for compliance could void the user´s authority to operate this equipment.

RF Exposure: A distance of 20 cm shall be maintained between the antenna and users, and the transmitter module may not be co-located with any other transmitter or antenna

Regulatory and Type Approval Information

Table 1: Directives

2002/95/EC	Directive of the European Parliament and of the Council of 27 January 2003 on the restriction of the use of certain hazardous substances in electrical and electronic equipment (RoHS)
2002/96/EC	Directive of the European Parliament and of the Council on waste electrical and electronic equipment (WEEE)
2003/108/EC	Directive of the European Parliament and of the Council of 8 December 2003 amending directive 2002/96/ec 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.

Revision History

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

Release Date	Firmware Version	Doc Version	Details
2013-03-11	1.00	v.1.0.0	First Release

Contents

Chapter 1. Product Concept 8
1.1 Overview 8
1.2 Packing List 8
1.3 Specifications 10
Chapter 2. Installation 14
2.1 LED Indicators 14
2.2 PIN assignment 15
2.3 USB interface 15
2.4 Reset Button 16
2.5 Ethernet ports 16
2.6 Mount the Router 17
2.7 Install SIM Card and Micro SD Card 17
2.8 Connect the External Antenna (SMA Type) 18
2.9 Ground the Router 18
Chapter 3. Configuration settings over web browser 20
3.1 Configuring PC in Windows 20
3.2 Factory Default Settings 22
3.3 Control Panel 23
3.4 Status -> System 24
3.5 Status -> Network 27
3.6 Status -> Route 28
3.7 Status -> VPN 28
3.8 Status -> Services 29
3.9 Status -> Event/Log 30
3.10 Configuration -> Link Management 31
3.11 Configuration -> Cellular WAN 32
3.12 Configuration -> Ethernet 38
3.13
3.14 Configuration -> Serial 46
3.15 Configuration -> DI/DO 53
3.16 Configuration -> USB 56
3.17 Configuration -> GPS 57
3.18 Configuration -> NAT/DMZ 60
3.19 Configuration -> Firewall 61
3.20 Configuration -> QoS 62
3.21 Configuration -> IP Routing 65
3.22 Configuration -> DynDNS 68
3.23 Configuration -> IPSec 69
3.24 Configuration -> Open VPN 74
3.25 Configuration -> GRE 78
3.26 Configuration -> L2TP 79
3.27 Configuration -> PPTP 83

3.28 Configuration -> SNMP 87
3.29 Configuration -> VRRP 89
3.30 Configuration -> IP Passthrough 89
3.31 Configuration -> AT over IP 91
3.32 Configuration -> Phone Book 91
3.33 Configuration -> SMS 92
3.34 Configuration -> Reboot 93
3.35 Configuration -> RobustLink 94
3.36 Configuration -> Syslog 95
3.37 Configuration -> Event 96
3.38 Configuration -> USR LED 96
3.39 Administration -> Profile 97
3.40 Administration -> Tools 98
3.41 Administration -> Clock 101
3.42 Administration -> Web Server 102
3.43 Administration -> User Management 103
3.44 Administration -> SDK Management 104
3.45 Administration -> Update Firmware 105
Chapter 4. Configuration Examples 107
4.1 Interface 107
4.1.1 Console port 107
4.1.2 Digital Input 108
4.1.3 Digital Output 108
4.1.4 RS232 109
4.1.5 RS485 109
4.2 Cellular 110
4.2.1 Cellular Dial-Up 110
4.2.2 SMS Remote Status Reading 112
4.3 Network 114
4.3.1 NAT 114
4.3.2 L2TP 115
4.3.3 PPTP 117
4.3.4 IPSEC VPN 119
4.3.5 OPENVPN 121
Chapter 5. Introductions for CLI 124
5.1 What’s CLI and hierarchy level Mode 124
5.2 How to configure the CLI 126
5.3 Commands reference 130

Chapter 1. Product Concept

1.1 Overview

Robustel GoRugged R3000-3P is a rugged 3G router offering state-of-the-art mobile connectivity for machine to machine (M2M) applications.

- Dual SIM redundancy for continuous cellular connections.
- WAN link management: cellular WAN/Ethernet WAN backup.
- VPN tunnel: IPSec/OpenVPN/PPTP/L2TP/GRE.
- Supports Modbus gateway (Modbus RTU/ASCII to Modbus TCP).
- Supports GPS (optional), provides real time location and tracking.

- Supports SDK, provides user programmatic interface.
- Auto reboot via SMS/Caller ID/Timing.
- Supports RobustLink (Centralized M2M management platform).
- Flexible Management methods: Web/CLI/SNMP/RobustLink.
- Firmware upgrade via Web/CLI/USB/SMS/RobustLink.
- Various interfaces: RS232/RS485/Console/DI/DO/USB/Ethernet.
- Wide range input voltages from 9 to 60 VDC and extreme operating temperature.
- The metal enclosure can be mounted on a DIN-rail or on the wall, also with extra ground screw.

1.2 Packing List

Check your package to make sure it contains the following items:

- Robustel GoRugged R3000-3P router x 1

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

- 7-pin pluggable terminal block with lock for serial port, I/O and console port x 2

- CD with user guide x 1

***Note**: Please notify your sales representative if any of the above items are missing or damaged.*

Optional accessories (can be purchased separately):

- SMA antenna (Stubby antenna or Magnet antenna optional) x 1

Stubby antenna *Magnet antenna*

- Ethernet cable x 1

- Wall Mounting Kit

- 35mm Din-Rail mounting kit

- AC/DC Power Supply Adapter (12VDC, 1.5A) x 1 (EU, US, UK, AU plug optional)

1.3 Specifications

Cellular Interface

- Standards: GSM/GPRS/EDGE/UMTS
- GPRS/EDGE: 850/900/1800/1900 MHz
- HSDPA/HSUPA: Band II/IV/V
- SIM: 2 x (3V & 1.8V)
- Antenna Interface: SMA Female

Ethernet Interface

- Number of Ports: 2 x 10/100 Mbps, 2 LANs or 1 LAN 1 WAN
- Magnet Isolation Protection: 1.5KV

GPS Interface (Optional)

- Antenna Interface: SMA Female, 50 ohms impedance
- Tracking Sensitivity: better than -158 dBm
- Protocol: NMEA-0183 V2.3

Serial Interface

- Number of Ports: 1 x RS-232, 1 x RS-485 or 2 x RS232 or 2 x RS485
- ESD Protection: ±15KV
- Parameters: 8E1, 8O1, 8N1, 8N2, 7E2, 7O2, 7N2, 7E1
- Baud Rate: 300bps to 230400bps
- RS-232: TxD, RxD, RTS, CTS, GND
- RS-485: Data+ (A), Data- (B), GND
- Interface: 3.5mm terminal block with lock

Digital Input

- Type: 2 x DI, Dry Contact
- Dry Contact: On: open, Off: short to GND
- Isolation: 3K VDC or 2K Vrms
- Digital Filtering Time Interval: Software selectable

- Interface: 3.5mm terminal block with lock

Digital Output

- Type: 2 x DO, Sink
- Isolation: 3K VDC or 2K Vrms
- Absolute Maximum VDC: 36V
- Absolute Maximum ADC: 50mA
- Interface: 3.5mm terminal block with lock

System

- LED Indicators: RUN, PPP , USR, RSSI, NET, SIM
- Built-in RTC, Watchdog, Timer
- Expansion: 1 x USB 2.0 host up to 480 Mbps
- Storage: 1 x MicroSD

Software

- Network protocols: PPP, PPPoE, TCP, UDP, DHCP, ICMP, NAT, DMZ, RIP v1/v2, OSPF, DDNS, VRRP, HTTP, HTTPs, DNS, ARP, QoS, SNTP, Telnet, etc
- VPN tunnel: IPSec/OpenVPN/PPTP/L2TP/GRE
- 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: Centralized M2M management platform

Power Supply and Consumption

- Power Supply Interface: 5mm terminal block with lock
- Input Voltage: 9 to 60 VDC
- Power Consumption: Idle: 100 mA @ 12 V
- Data Link: 400 mA (peak) @ 12 V

Physical Characteristics

- Housing & Weight: Metal, 500g

- Dimension: (L x W x H): 125 x 108 x 45 mm
- Installation: 35mm Din-Rail or wall mounting or desktop

Environmental Limits

- Operating Temperature & Humidity: -40 to 85°C, 5 to 95% RH

Regulatory and Type Approvals

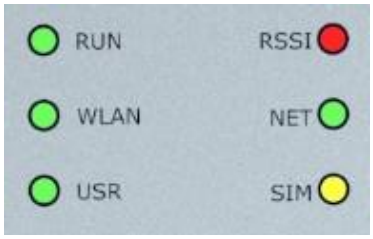
- Approval & Detective: CE, R&TTE, FCC, RCM, RoHS, WEEE
- EMC: EN 61000-4-2 (ESD) Level 4, EN 61000-4-3 (RS) Level 4

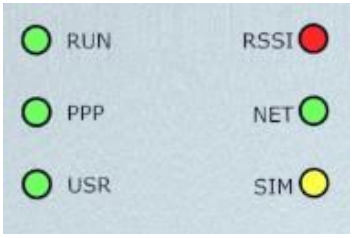
  EN 61000-4-4 (EFT) Level 4, EN 61000-4-5 (Surge) Level 3

  EN 61000-4-6 (CS) Level 4, EN 61000-4-8, EN 61000-4-12

Chapter 2. Installation

2.1 LED Indicators

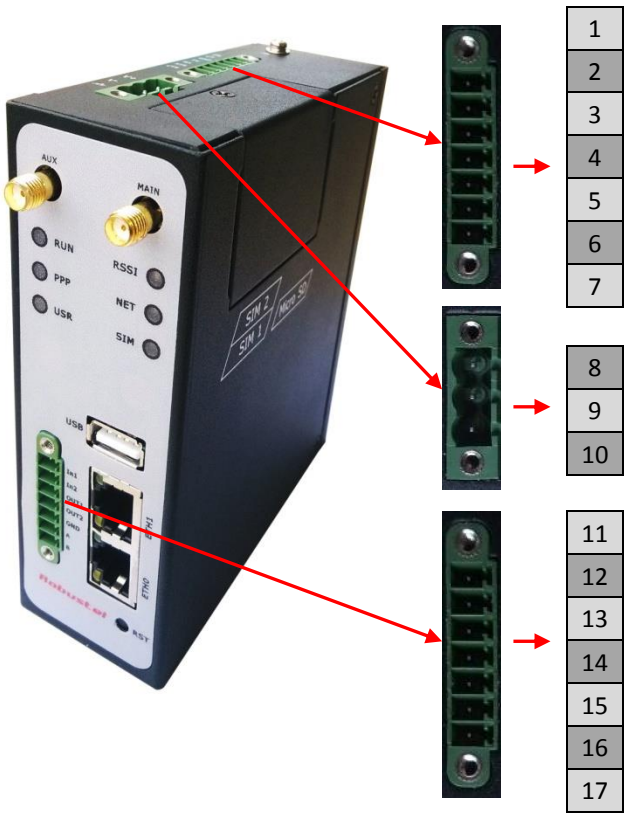




Name	Color	Status	Function
RUN	Green	Blinking	Router is ready.
		On	Router is starting.
		Off	Router is power off.
PPP	Green	Blinking	**PPP Indicator:** Null
		On	**PPP Indicator:** PPP connection is up.
		Off	**PPP Indicator:** PPP connection is down.
USR	Green	On/Blinking	VPN tunnel/PPPoE/DynDNS/GPS is up.
		Off	VPN tunnel/PPPoE/DynDNS/GPS is down.
RSSI	Green	On	Signal level: 21-31 (Perfect signal level).
	Yellow	On	Signal level: 11-20 (Average signal level).
	Red	On	Signal level: 1-10 (Exceptional signal level).
NET	Yellow	Blinking	3G is connected but PPP connection is failed.
		On	3G is connected and PPP connection is established.
	Red	Blinking	2G is connected but PPP connection is failed.
		On	2G is connected and PPP connection is established.
	/	Off	Cannot register to any network.
SIM	Green	Blinking	Only SIM 1 is detected, but PIN code is incorrect.
		On	Working with SIM 1 normally.
	Yellow	Blinking	Only SIM 2 is detected, but PIN code is incorrect.
		On	Working with SIM 2 normally.
	Green&Yellow	Blinking between two colors	Two SIMs are detected, but both of their PIN codes are incorrect.
	/	Off	No SIM inside.

***Note**: User can select display status of USR LED. Please check section 23.38.*

2.2 PIN assignment



PIN	Debug	RS232	Power	Digital I/O	RS485
1	RXD				
2	TXD				
3	GND	GND			
4		TXD			
5		RXD			
6		RTS			
7		CTS			
8			Positive		
9			Negative		
10			GND		
11				Input 1	
12				Input 2	
13				Output 1	
14				Output 2	
15				GND	
16					Data+(A)
17					Data- (B)

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 an USB storage device, such as U disk or hard disk, into the router's USB interface, if there is configuration file or firmware of R3000-3P inside the USB storage devices, R3000-3P will automatically update the configuration file or firmware. Details please refer to section 23.16.

2.4 Reset Button

Function	Operation
Reboot	Push the button for 5 seconds under working status.
Restore to factory default setting	Push the button for 60 seconds once you power on the router until all the three LEDs at the left side (RUN, PPP, USR) blink at the same time for 5 times.

2.5 Ethernet ports

Each Ethernet port has two LED indicators (please check the following picture). The yellow one is **Speed indicator** and the green one is **Link indicator**. There are three status of each indicator. Please refer to the form below.

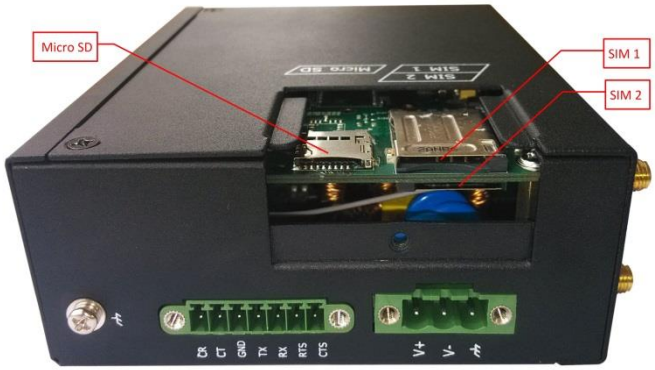
Indicator	Status	Description
Speed Indicator	Off	10 Mbps mode.
	On	100 Mbps mode.
Link Indicator	Off	Connection is down.
	On	Connection is up.
	Blink	Data is being transmitted

2.6 Mount the Router

Use 2 pcs of M3 screw to mount the router on the wall.

Or mount the router on a DIN rail with 3 M3 screws.

2.7 Install SIM Card and Micro SD Card



■ **Inserting SIM Card or Micro SD Card**

1. Make sure power supply is disconnected.
2. Use a screwdriver to unscrew the screw on the cover, and then remove the cover, you could find the SIM Card slots and the Micro SD slot.
3. Insert the SIM card or Micro SD card, and you need press the card with your fingers until you hear “a cracking sound”. Then use a screwdriver to screw the cover.

■ **Removing SIM Card or Micro SD Card**

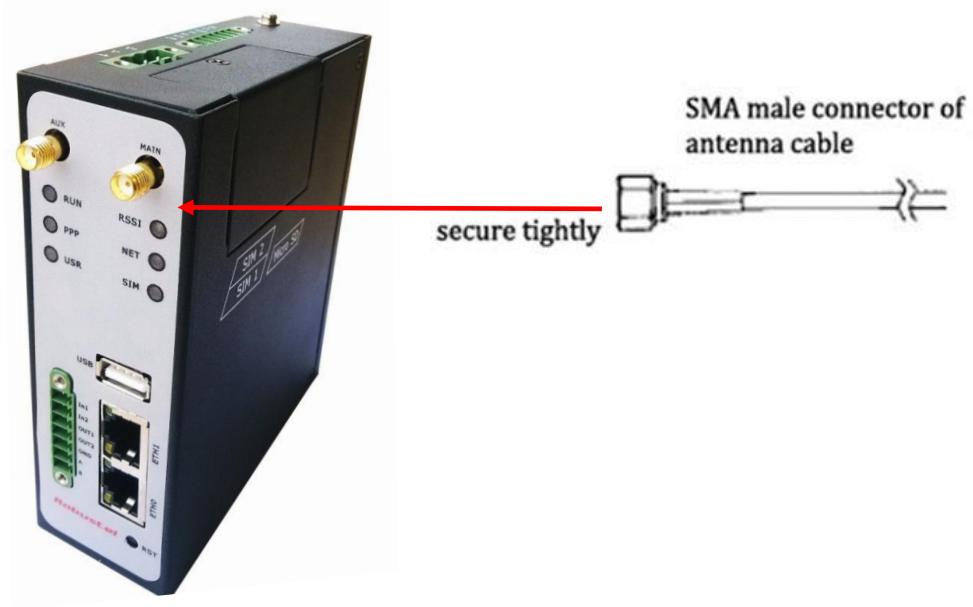
1. Make sure router is power off.
2. Press the card until you hear “a cracking sound”, when the card will pop up to be pulled out.

***Note*:**

1. *Don’t forget screw the cover for again-theft.*
2. *Don’t touch the metal surface of the SIM card in case information in the card is lost or destroyed.*
3. *Don’t bend or scratch your SIM card. Keep the card away from electricity and magnetism.*
4. *Make sure router is power off before inserting or removing your SIM card or Micro SD card.*

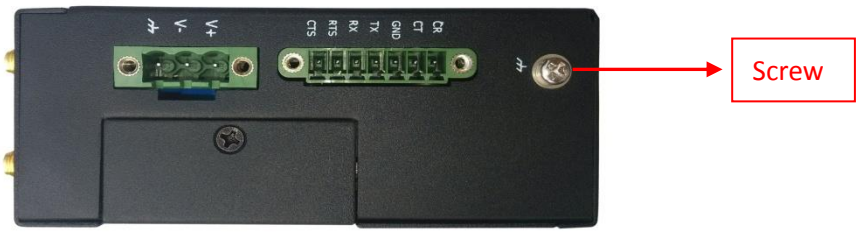
2.8 Connect the External Antenna (SMA Type)

Connect router to an external antenna with SMA male connector. Make sure the antenna is for the correct frequency as your GSM/3G operator with impedance of 50ohm, and also connector is secured tightly.



2.9 Ground the Router

Grounding and wire routing help limit the effects of noise due to electromagnetic interference (EMI). Run the ground connection from the ground screw to the grounding surface prior to connecting devices.



***Note**: This product is intended to be mounted to a well-grounded mounting surface, such as a metal panel.*

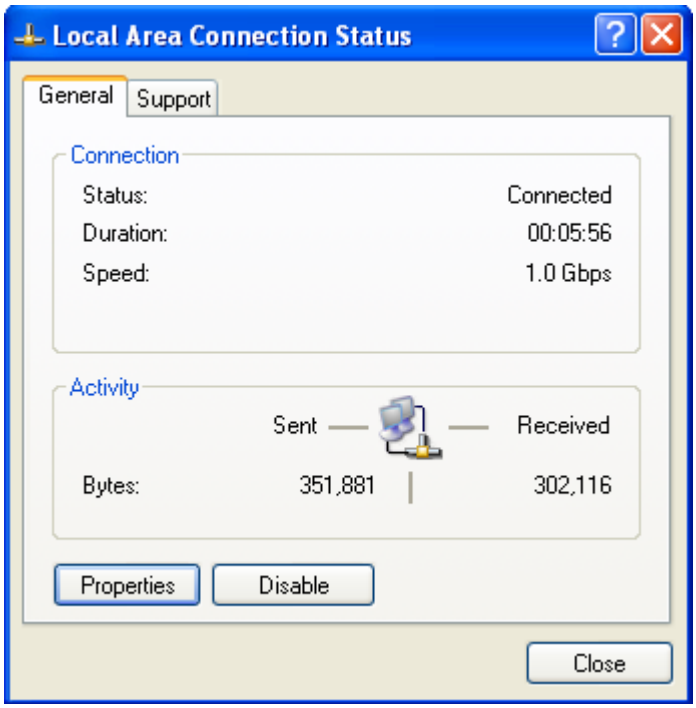
Chapter 3. Configuration settings over web browser

The router can be configured through your web browser. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista/7/8, etc. The product provides an easy and user-friendly interface for configuration.
There are various ways to connect the router, either through an external repeater/hub or connect directly to your PC. However, make sure that your PC has an Ethernet interface properly installed prior to connecting the router.
You must configure your PC to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problems accessing the router web interface it is advisable to uninstall your firewall program on your PC, as these tend to cause problems accessing the IP address of the router.

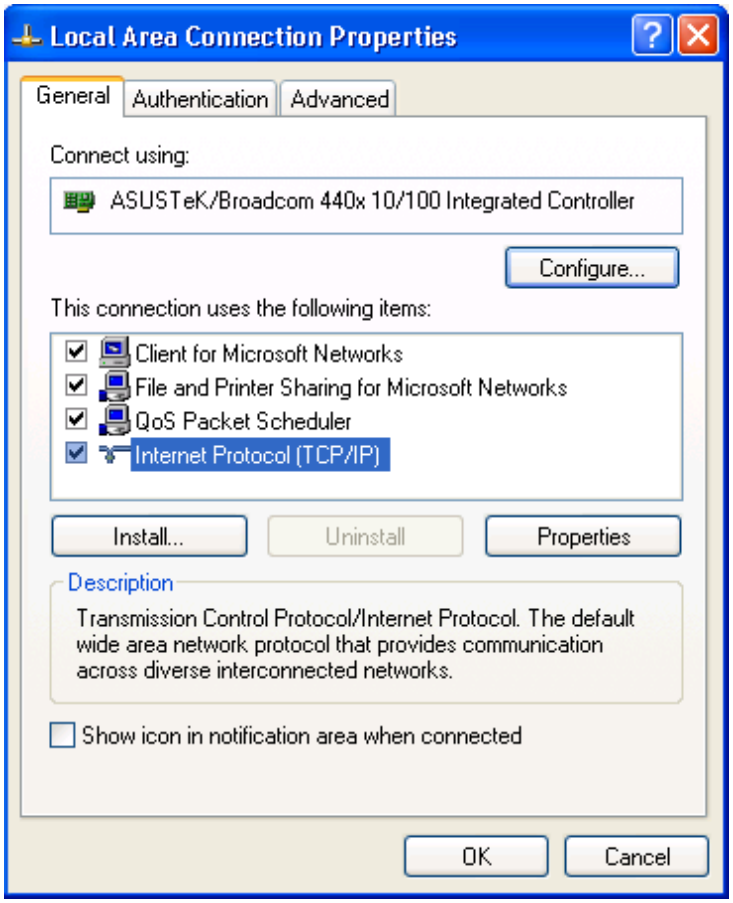
3.1 Configuring PC in Windows

1. Go to Start / Control Panel (in Classic View). In the Control Panel, double-click Network Connections.
2. Double-click Local Area Connection.

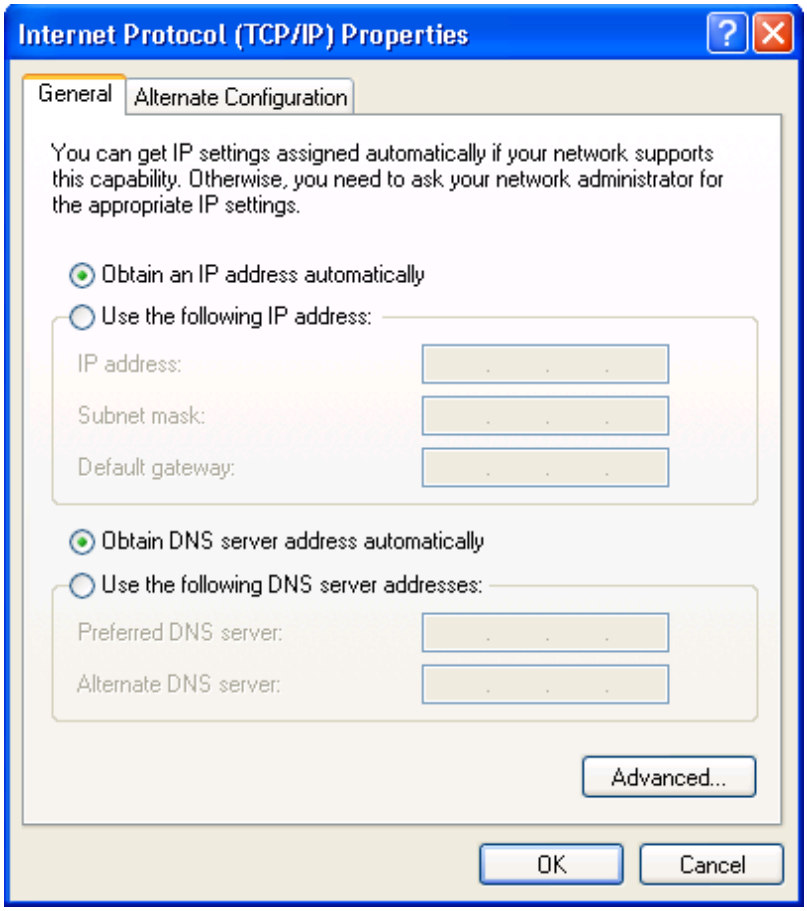
3. In the Local Area Connection Status window, click Properties.



4. Select Internet Protocol (TCP/IP) and click Properties.



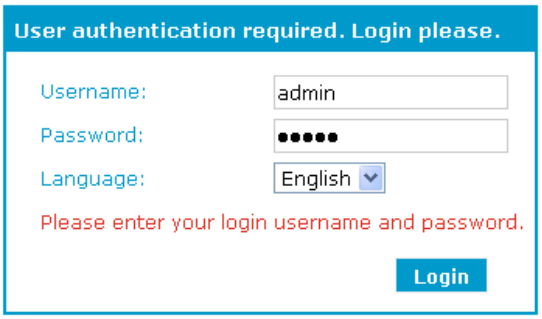
5. Select the Obtain an IP address automatically and Obtain DNS server address automatically radio buttons.



6. 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
Eth0	192.168.0.1/255.255.255.0, LAN mode
Eth1	192.168.0.1/255.255.255.0, LAN mode

DHCP Server	Enabled.

3.3 Control Panel

This section allows users to save configuration, reboot router, logout and select language.

Control Panel		
Item	Description	Button
Save	Click to save the current configuration into router's flash.	• Save
Reboot	After save the current configuration, router needs to be rebooted to make the modification taking effect.	• Reboot
Logout	Click to return to the login page.	• Logout
Language	Select from Chinese, English, German, French and Spanish.	• English
Refresh	Click to refresh the status.	Refresh
Apply	Click to apply the modification on every configuration page.	Apply
Cancel	Click to cancel the modification on every configuration page.	Cancel

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

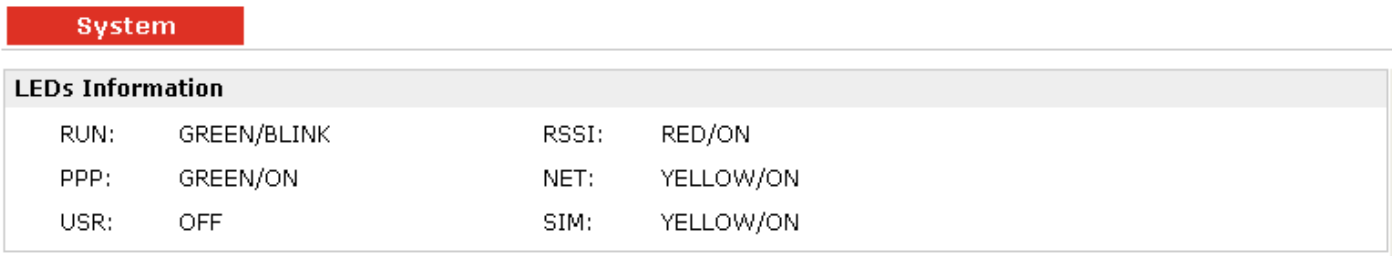
1. *Modify in one page;*
2. *Click* Apply *under this page;*
3. *Modify in another page;*
4. *Click* Apply *under this page;*
5. *Complete all modification;*
6. *Click* • Save *;*
7. *Click* • Reboot .

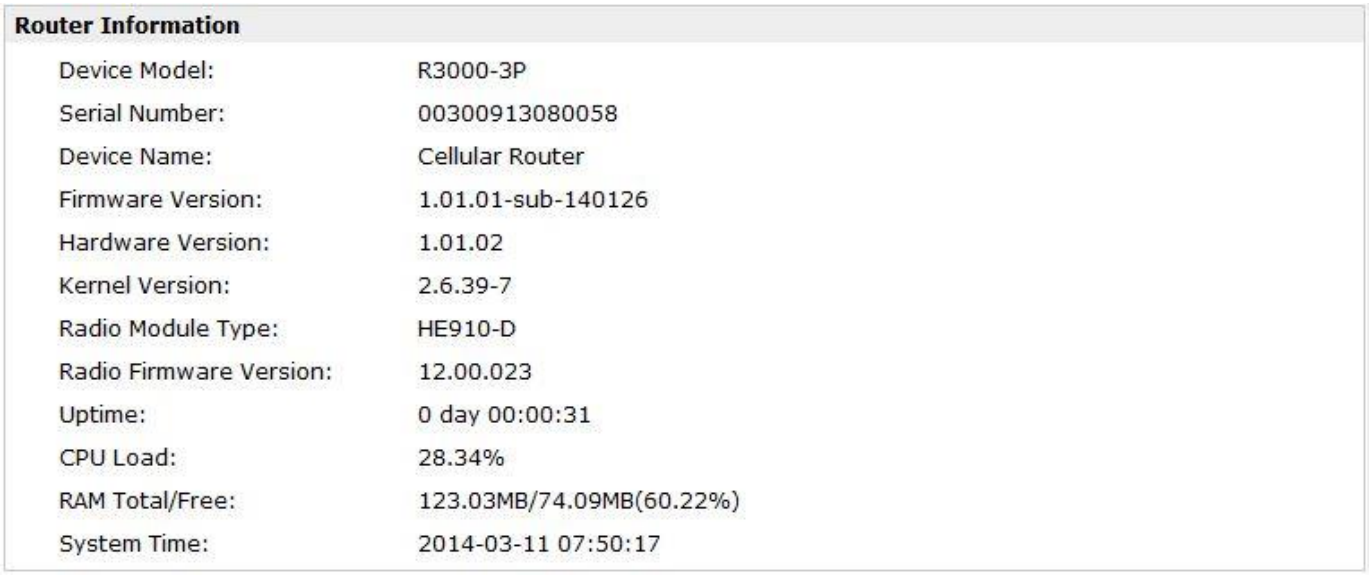
3.4 Status -> System

This section displays the router's system status, which shows you a number of helpful information such as the LEDs information, Router information, Current WAN Link and Cellular Information.

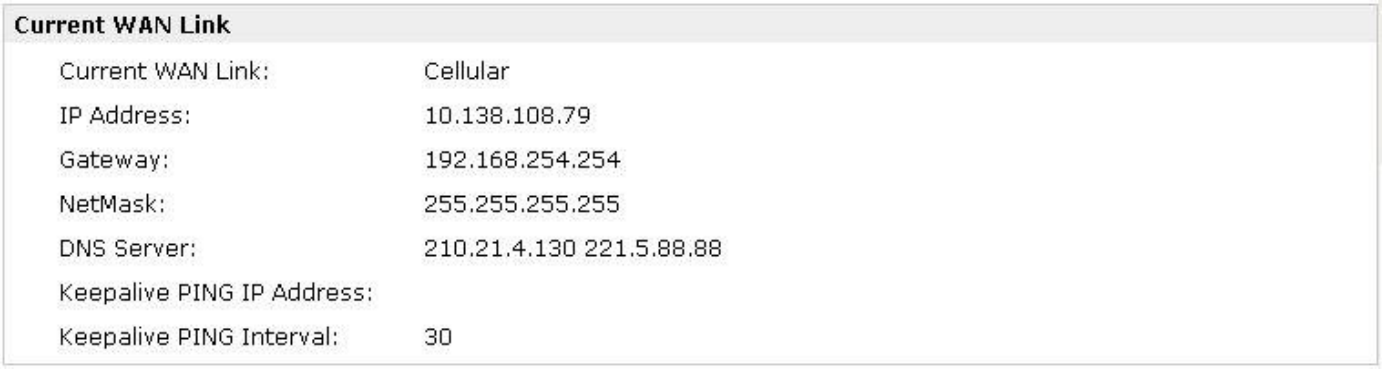
LEDs Information

For the detail description, please refer to 2.1LED Indicators.



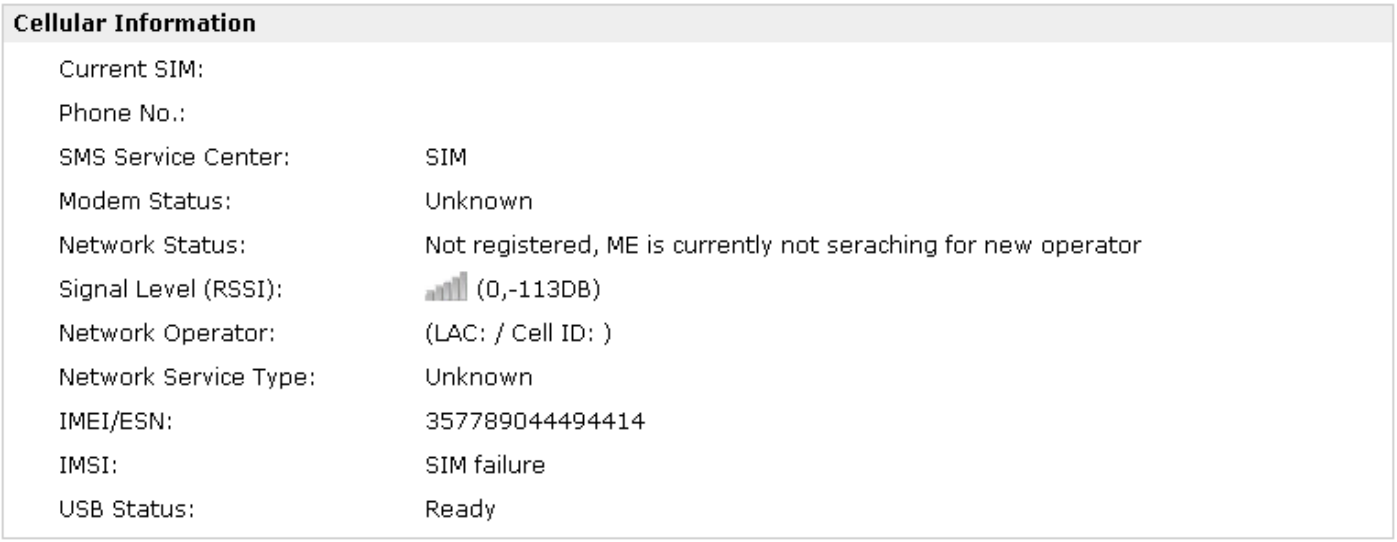


Router Information	
Item	Description
Device Model	Show the model name of this device
Serial Number	Show the serial number of this device
Device Name	Show the device name to distinguish different devices you have installed.
Firmware Version	Show the current firmware version
Hardware Version	Show the current hardware version
Kernel Version	Show the current kernel version
Radio Module Type	Show the current radio module type
Radio Firmware Version	Show the current radio firmware version
Uptime	Show how long the router have been working since power on
CPU Load	Show the current CPU load
RAM Total/Free	Show the total capacity /Free capacity of RAM
System Time	Show the current system time



Current WAN Link	
Item	Description
Current WAN Link	Show the current WAN link: Cellular WAN or Ethernet WAN.

IP Address	Show the current WAN IP address
Gateway	Show the current gateway
NetMask	Show the current netmask
DNS Server	Show the current primary DNS server and Secondary server
Keeping PING IP Address	Show the current ICMP detection server which you can set in “Configuration->Link Management”.
Keeping PING Interval	Show the ICMP Detection Interval (s) which you can set in “Configuration->Link Management”.

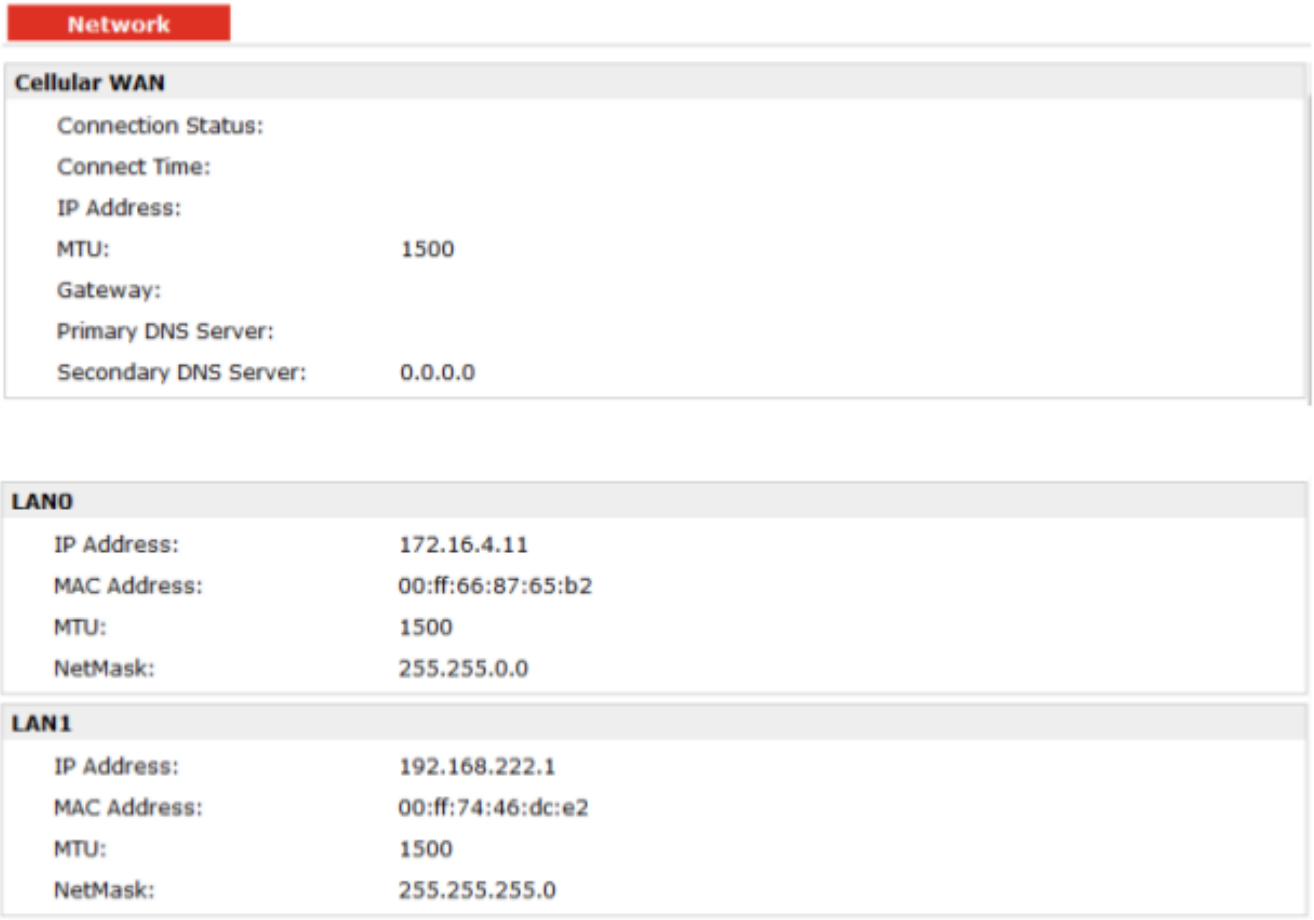


Cellular Information	
Item	Description
Current SIM	Show the SIM card which the router work with currently: SIM1 or SIM2
Phone No.	Show the phone number of the current SIM.
SMS Service Center	Show the SMS Service Center.
Modem Status	Show the status of modem. There are 8 different status: 1. Unknown. 2. Ready. 3. Checking AT. 4. Need PIN. 5. Need PUK. 6. Signal level is low. 7. No registered. 8. Initialize APN failed.
Network Status	Show the current network status. There are 6 different status: 1. Not registered, ME is currently not searching for new operator! 2. Registered to home network. 3. Not registered, but ME is currently searching for a new operator. 4. Registration denied. 5. Registered, roaming.

	6. Unknown.
Signal Level (RSSI)	Show the current signal level.
Network Operator	Show Mobile Country Code (MCC) +Mobile Network Code (MNC), e.g. 46001. Also it will show the Location Area Code (LAC) and Cell ID.
Network Service Type	Show the current network service type, e.g. GPRS.
IMEI/ESN	Show the IMEI/ESN number of the radio module.
IMSI	Show the IMSI number of the current SIM.
USB Status	Show the current status of USB host.

3.5 Status -> Network

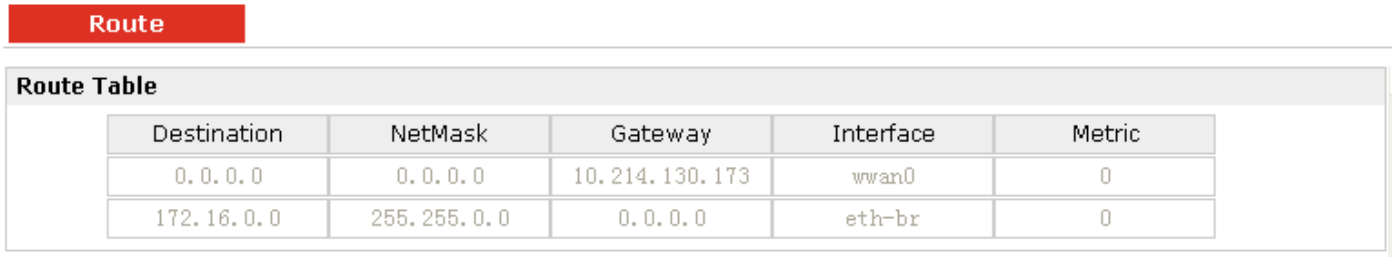
This section displays the router's Network status, which include status of Cellular WAN, ETH0, ETH11



***Note**: ETH0 WAN information will not be shown if you select "Cellular Only" in "Configuration"->"Link Management"->"WAN Link".*

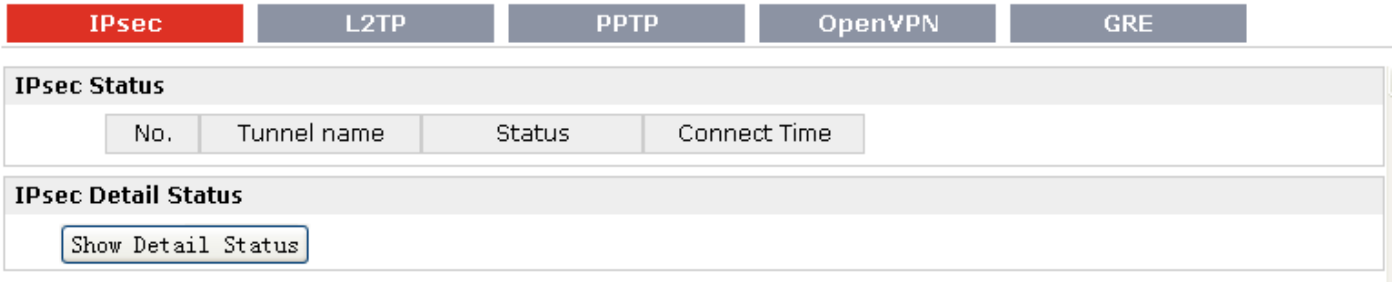
3.6 Status -> Route

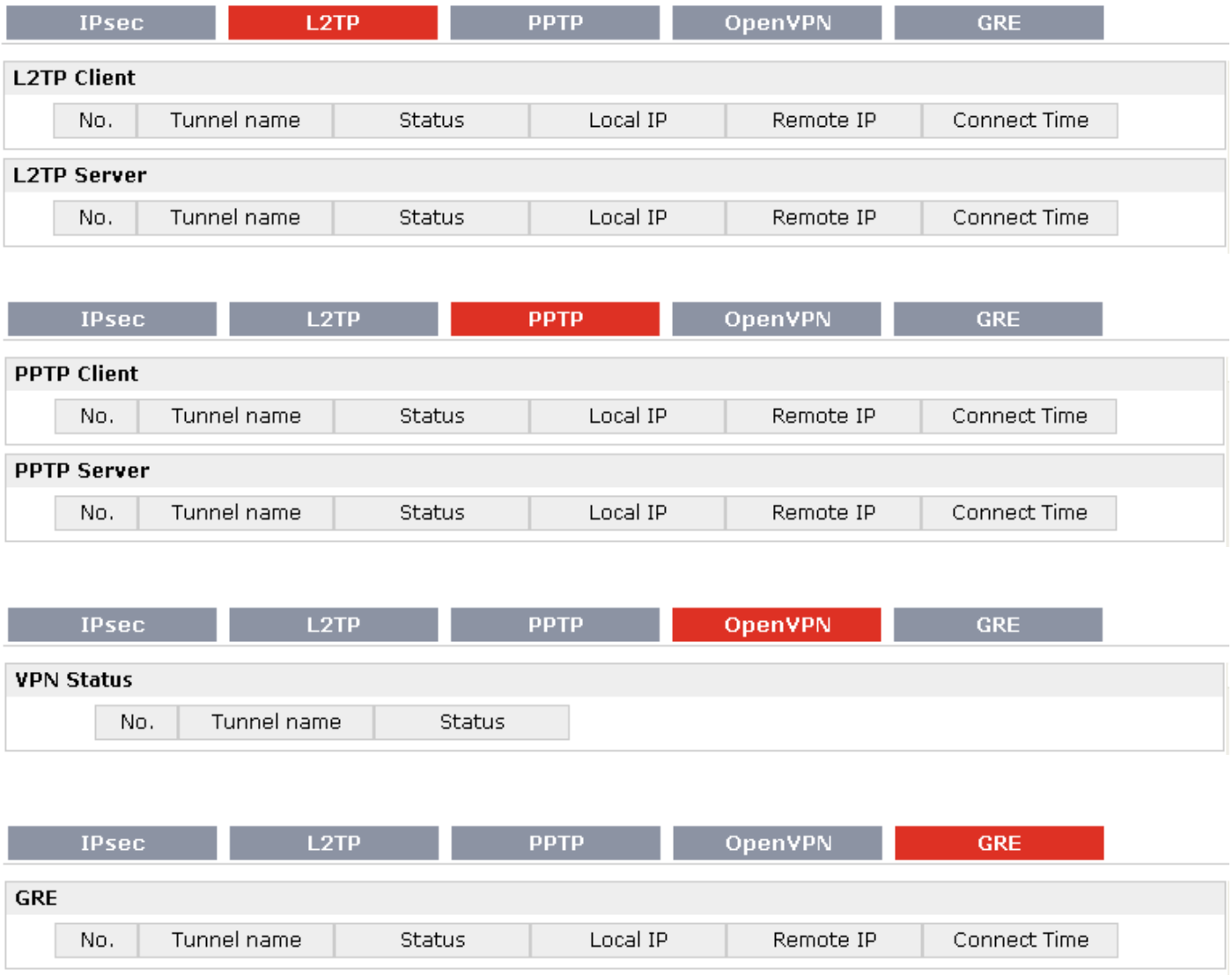
This section displays the router's route table.



3.7 Status -> VPN

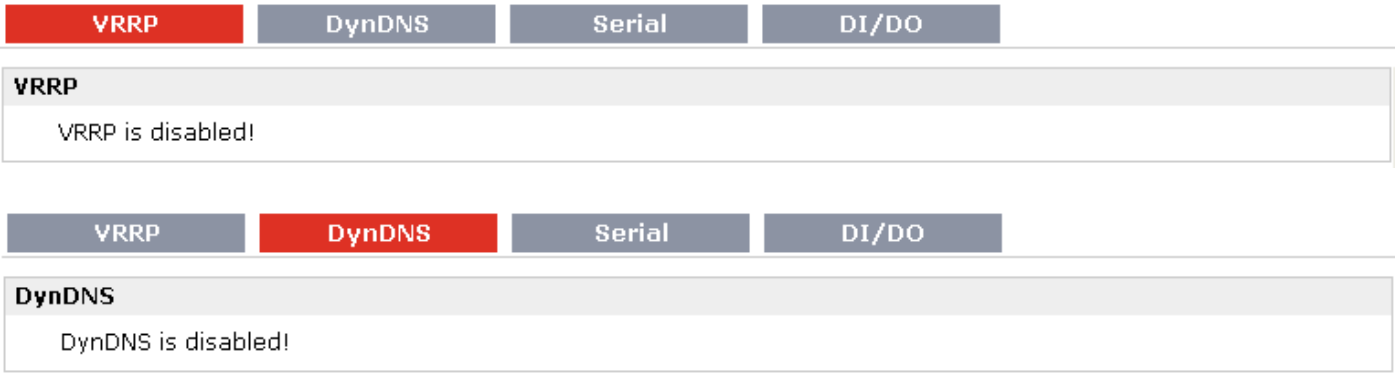
This section displays the router's VPN status, which includes IPSec, L2TP, PPTP, OpenVPN and GRE.

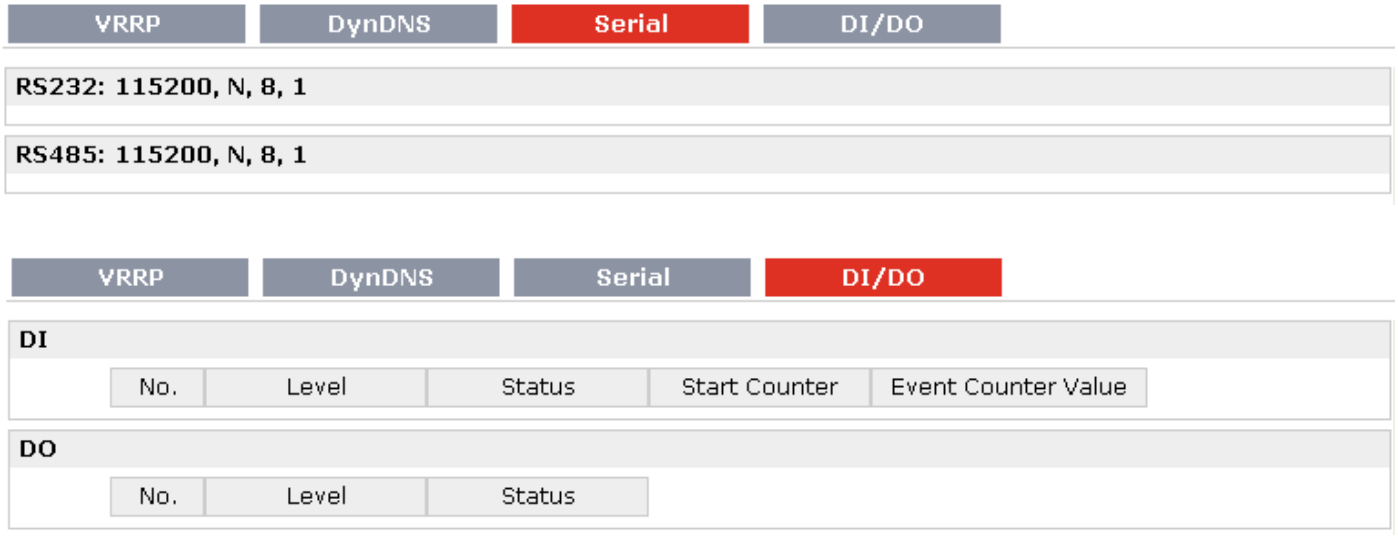




3.8 Status -> Services

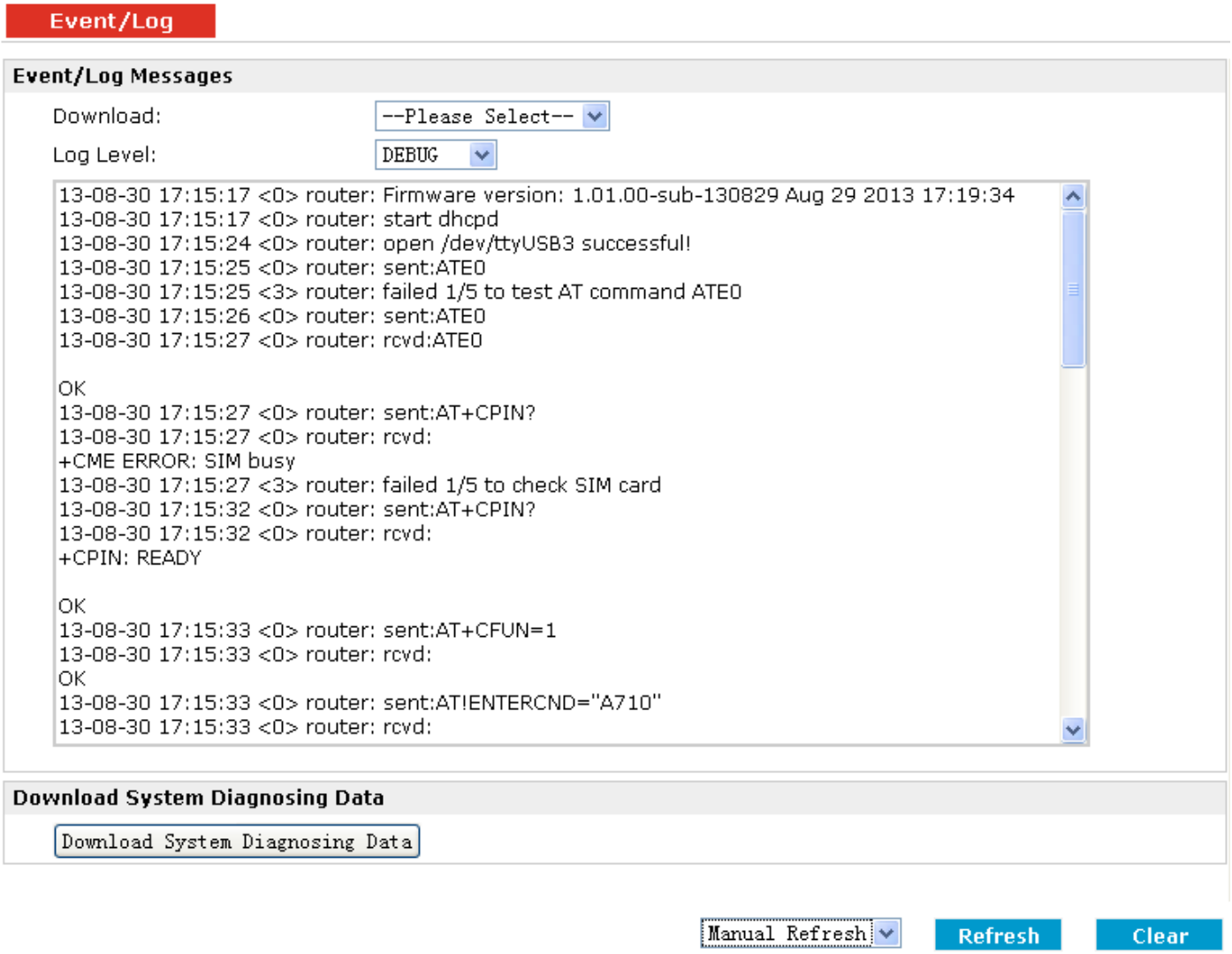
This section displays the router's Services' status, including VRRP, DynDNS, Serial and DI/DO.





3.9 Status -> Event/Log

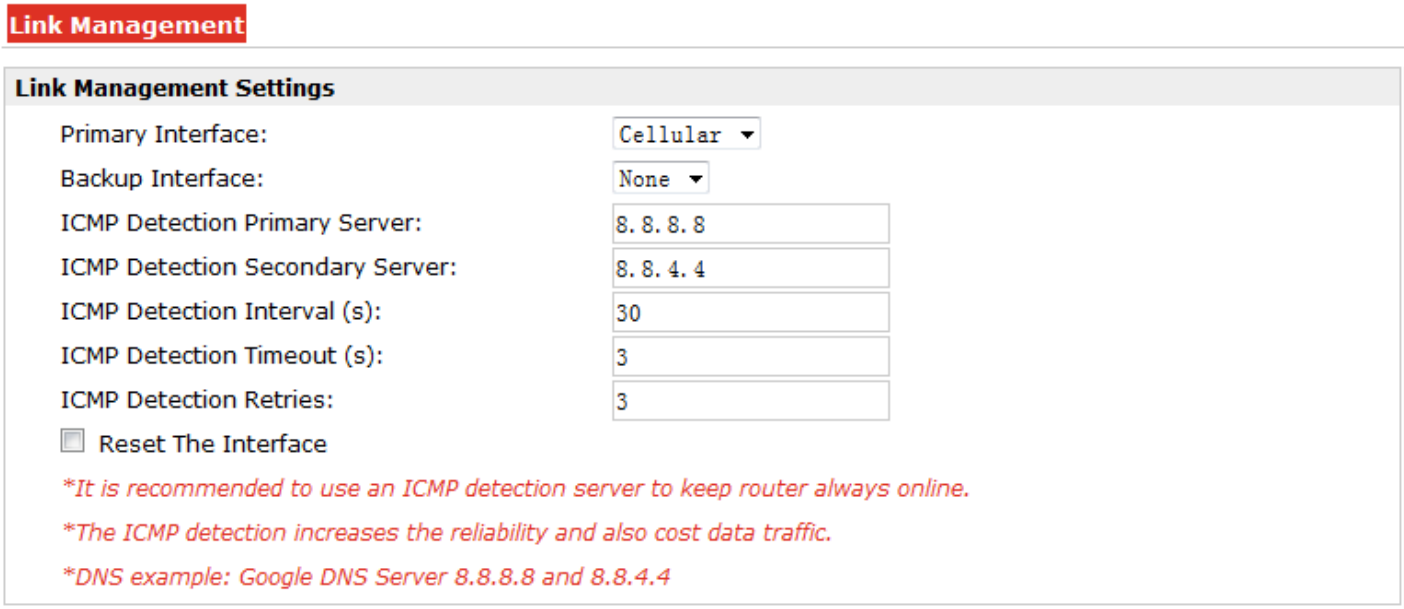
This section displays the router's event/log information. You need to enable router to output the log and select the log level first, then you can view the log information here. Also you can click *Download System Diagnosing Data* to download diagnose data.



Event/Log	
Item	Description
Download	Select the log messages you want to download.
Log Level	Select the Log level in the drop-down menu: DEBUG, INFO, NOTICE, WARNING, ERR, CRIT, ALERT, EMERG.
Download Sytem Diagnosing Data	Click *Download System Diagnosing Data* to download diagnose file.
Manual Refresh	Select from “5 Seconds”, “10 Seconds”, “15 Seconds”, “30 Seconds” and “1 Minute”. User can select these intervals to refresh the log information.

3.10 Configuration -> Link Management

This section allows users to set the WAN link and the related parameters.



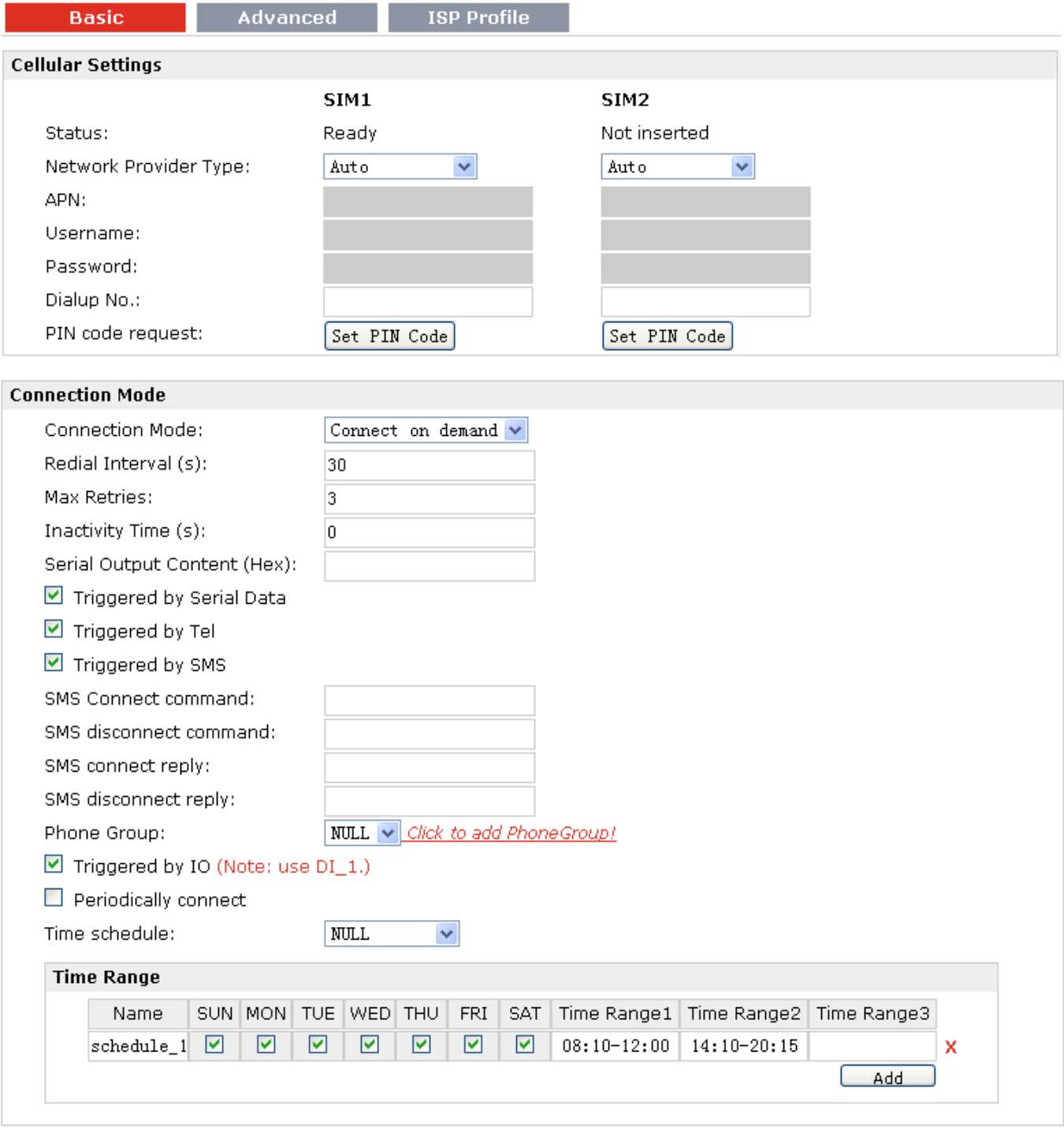
Link Management		
Item	Description	Default
Primary Interface	Selected from "Cellular", "Eth0", 1. Cellular: Select to make cellular as the primary WAN link. 2. Eth0: Select to make Eth0 as the primary WAN link.	Cellular
Backup Interface	Selected from "None", "Eth0", 1. None: Do not select backup interface. 2. Cellular: Select Cellular as the backup WAN link. 3. Eth0: Select Eth0 as the backup WAN link.	None
ICMP Detection Primary Server	Router will ping this primary address/domain name to check that if the current connectivity is active.	Null
ICMP Detection Secondary Server	Router will ping this secondary address/domain name to check that if the current connectivity is active.	Null
ICMP Detection Interval	Set the ping interval.	Null
ICMP Detection Timeout	Set the ping timeout.	30
ICMP Detection Retries	If Router ping the preset address/domain name time out continuously for Max Retries time, it will consider that the connection has been lost.	3
Reset The Interface	Enable to reset the cellular/ETH0 interface after the max ICMP detection retries.	3

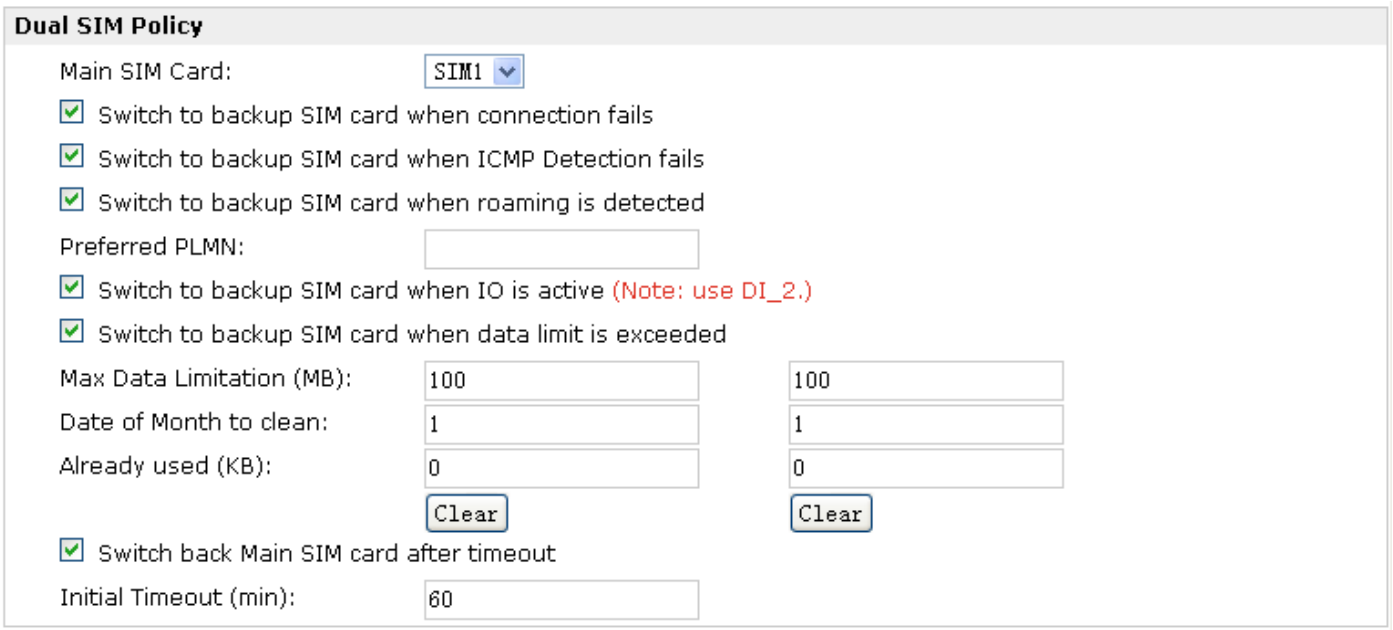
3.11 Configuration -> Cellular WAN

This section allows users to set the Cellular WAN and the related parameters.

***Note**: This section will not be displayed if you select* "Eth0 Only" in *"Configuration"->"Link Management"->"WAN*

Link".


Basic
Advanced
ISP Profile
Cellular Settings
SIM1
SIM2
Status:
Ready
Not inserted
Network Provider Type:
Auto
Auto
APN:
Username:
Password:
Dialup No.:
PIN code request:
Set PIN Code
Set PIN Code
Connection Mode
Connection Mode:
Connect on demand
Redial Interval (s):
30
Max Retries:
3
Inactivity Time (s):
0
Serial Output Content (Hex):
Triggered by Serial Data
Triggered by Tel
Triggered by SMS
SMS Connect command:
SMS disconnect command:
SMS connect reply:
SMS disconnect reply:
Phone Group:
NULL
Click to add PhoneGroup!
Triggered by IO (Note: use DI_1.)
Periodically connect
Time schedule:
NULL
Time Range
Name
SUN
MON
TUE
WED
THU
FRI
SAT
Time Range1
Time Range2
Time Range3
schedule_1
08:10-12:00
14:10-20:15
Add

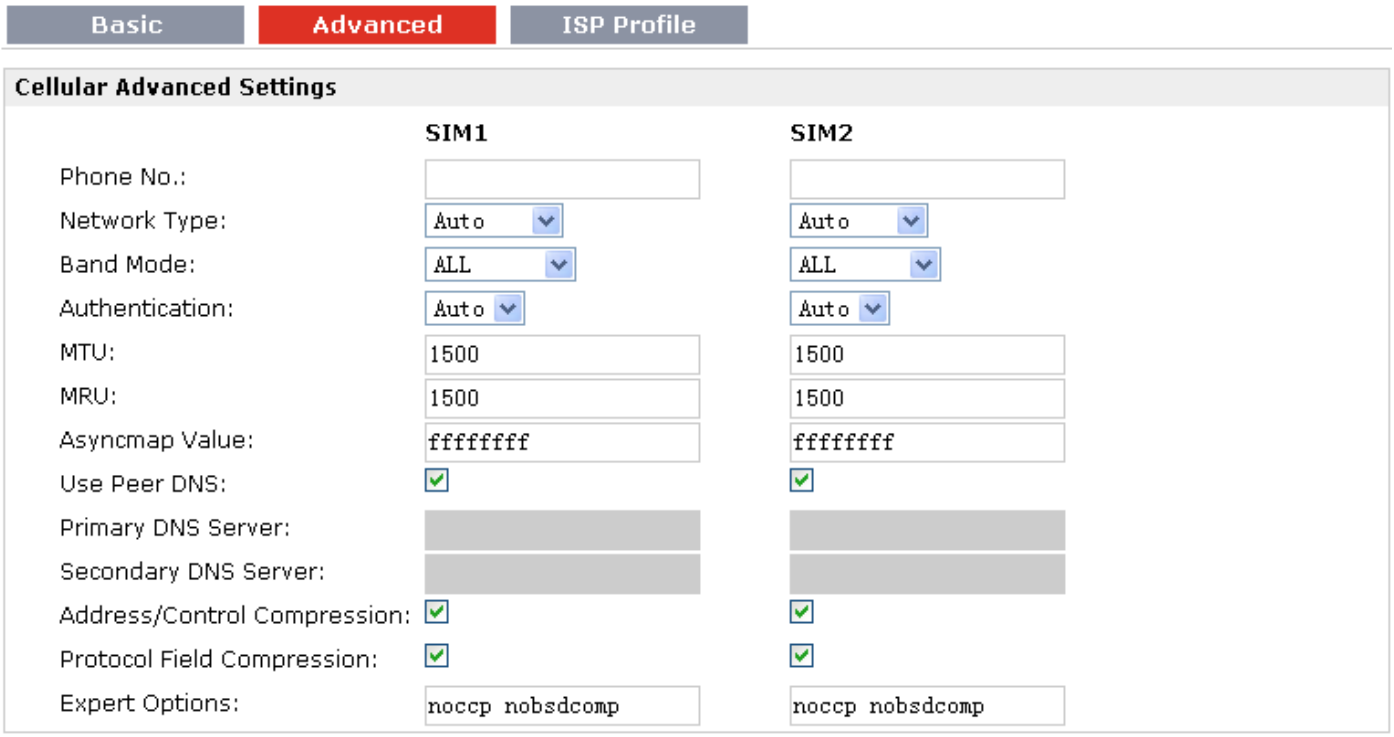


Basic @Cellular WAN		
Cellular Settings		
Item	Description	Default
Network Provider Type	Select from "Auto", "Custom" or the ISP name you preset in *"Configuration"->"Cellular WAN"->"ISP Profile".* Auto: Router will get the ISP information from SIM card, and set the APN, username and password automatically. This option only works when the SIM card is from well-known ISP. Custom: Users need to set the APN, username and password manually.	Auto
APN	Access Point Name for cellular dial-up connection, provided by local ISP.	Null
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
Dialup No.	Dialup number for cellular dial-up connection, provided by local ISP.	*99***1#
PIN Type	Select from "None", "Input", "Lock", "Unlock". None: Select when SIM card does not enable PIN lock or PUK lock. Input: Select when SIM card has enabled with PIN lock or PUK lock. Correct PIN/PUK code need to be entered. Lock: Select when user needs to lock the SIM card with PIN or PUK code. Unlock: Select when user needs to unlock the SIM card with PIN or PUK code. ***Note**: Please ask your local GSM ISP to see whether your SIM card requiring PIN or not.* *If you want to change with a new PIN code, you need to input new PIN code in item "New PIN Code" and "Confirm New PIN Code".* *You can go to tab "Status" -> "Event/Log" and find out "AT+CPIN?" to check what the status of the SIM card is.*	None

Connection Mode		
Connection Mode	Select from “Always Online” and “Connect On Demand”. Always Online: Auto activates PPP and keeps the link up after power on. Connect On Demand: After selection this option, user could configure Triggered by Serial Data, Triggered by Periodically Connect and Triggered by Time Schedule. ***Note***: *If you select several connect on demand polices, router only have to meet one of them to be triggered.*	Connect On Demand
Redial Interval	Router will automatically re-dial with this interval when it fails communicating to peer via TCP or UDP.	30
Max Retries	The maximum retries times for automatically re-connect when router fails to dial up. After maximum retries, router will reboot the wireless module. If router still cannot dial up successfully, it will try to switch to the other SIM card. Then router will re-connect with the other SIM card with maximum retries. After successful connection, the Max Retries counter will be set to 0.	3
Inactivity Time	Configurable after “Connect On Demand” was selected. This field specifies the idle time setting for GPRS/3G auto-disconnection and trying to revert back to preferred SIM card. 0 means timeless.	0
Serial Output Content	The content which output to the serial device which connect to router and inform it that router is ready to receive serial data.	Null
Triggered by Serial Data	Tick this check box to allow router automatically connects to cellular network from idle mode when there is data comes out from serial port.	Enable
Triggered by Tel	Tick this check box to allow router automatically connects to cellular network from idle mode when make a voice call to router.	Disable
Triggered by SMS	Tick this check box to allow router automatically connects to cellular network from idle mode when send a specific SMS to router.	Disable
SMS Connect Command	Users shall send this specific SMS to trigger router to connect to cellular network.	Null
SMS Disconnect Command	Users shall send this specific SMS to trigger router to disconnect to cellular network.	Null
SMS Connect Reply	When router connects to cellular network, it will automatically send out this SMS to specific users (set in the Phone Group).	Null
SMS Disconnect Reply	When router disconnect from cellular network, it will automatically send out this SMS to specific users (set in the Phone Group).	Null
Phone Group	Click to add Phone Group to Set specific users’ phone Book and which phone Group they are belonged to.	Null
Triggered by IO	Tick this check box to allow router automatically connects to cellular network from idle mode when there is a DI (DI_1) alarm input.	Disable
Periodically Connect	Tick this check box to allow router automatically connects to cellular network with preset interval which you preset in *Periodically Connect Interval*.	Enable

Periodically Connect Interval	Periodically Connect Interval for Periodically Connect.	300
Time Schedule	Select the Time Range to allow router automatically connects to cellular network during this time range.	NULL
Time Range	Adding the Time Range for Time Schedule. You can set the days of one week and at most three ranges of time of one day.	Null
Dual SIM Policy		
Main SIM Card	Set the preferred SIM card from SIM 1, SIM 2 or Auto.	SIM1
Switch to backup SIM card when connection fails	Router will switch to another SIM card if main SIM card fail to connect to network.	Disable
Switch to backup SIM card when roaming is detected	Router will switch to backup SIM card when preferred SIM card is roaming.	Disable
Preferred PLMN	The identifier for Router to check if it is in home location area or in roaming area, and decide if it needs to switch back to preferred SIM card.	Null
Switch to backup SIM card when IO is active	Router will switch to another SIM card if it detect there is DI (DI_2) alarm input.	Diaable
Switch to backup SIM card when data limit is exceeded	If the SIM card that the router worked with currently has reached the data traffic limitation you preset, it will switch to the other SIM card.	Disable
Max Data limitation(MB)	Set the monthly data traffic limitation.	100
Date of Month to Clean	Set one day of month to restore the used data to 0.	1
Already used	This tab will show how many data traffic has been used.	0
Switch back Main SIM card after timeout(min)	Enable to Switch back Main SIM card after the Initial timeout.	Disable
Initial Timeout(min)	Set the initial timeout.	60

***Note**: This section will not be displayed if you select* "Eth0 Only" in *"Configuration"->"Link Management"->"WAN Link".*

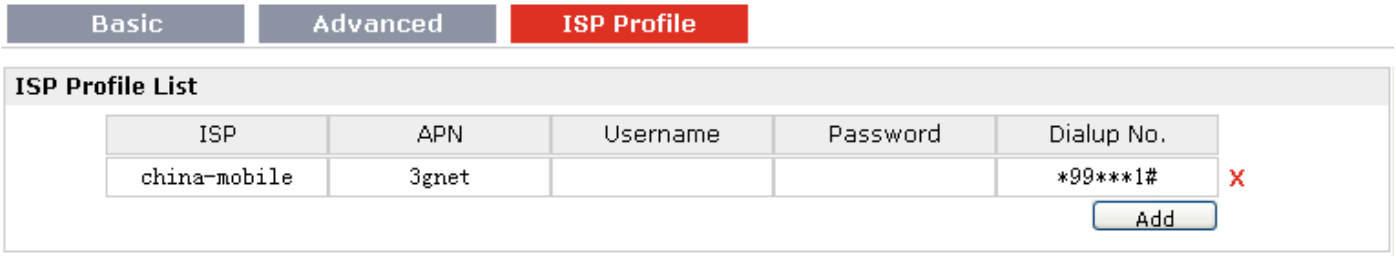


Advanced @Cellular WAN		
Item	Description	Default
Phone No.	Set the SIM card's phone number, and it will be showed in "Status"->"System"->"System"->"Cellular WAN Information"-"SIM Phone Number". In general, you don't need to set this number because router will read it from the SIM card automatically.	Null
Authentication	Select from "Auto", "PAP" and "CHAP" as the local ISP required.	Auto
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1500
MRU	Maximum Receiving Unit. It is the identifier of the maximum size of packet, which is possible to receive in a given environment.	1500
Asyncmap Value	One of the PPP initialization strings. In general, you don't need to modify this value.	1
Use Peer DNS	Enable to obtain the DNS server's address from the ISP.	Enable
Primary DNS Server	Set the primary DNS server's address. This item will be unavailable if you enable "Use Peer DNS".	Null
Secondary DNS Server	Set the secondary DNS server's address. This item will be unavailable if you enable "Use Peer DNS".	Null
Address/Control Compression	Used for PPP initialization. In general, you need to enable it as default.	Enable
Protocol Field Compression	Used for PPP initialization. In general, you need to enable it as default.	Enable
Expert Options	You can enter some other PPP initialization strings in this field. Each string	noccp

	can be separated by a space.	nobsdcomp

ISP Profile

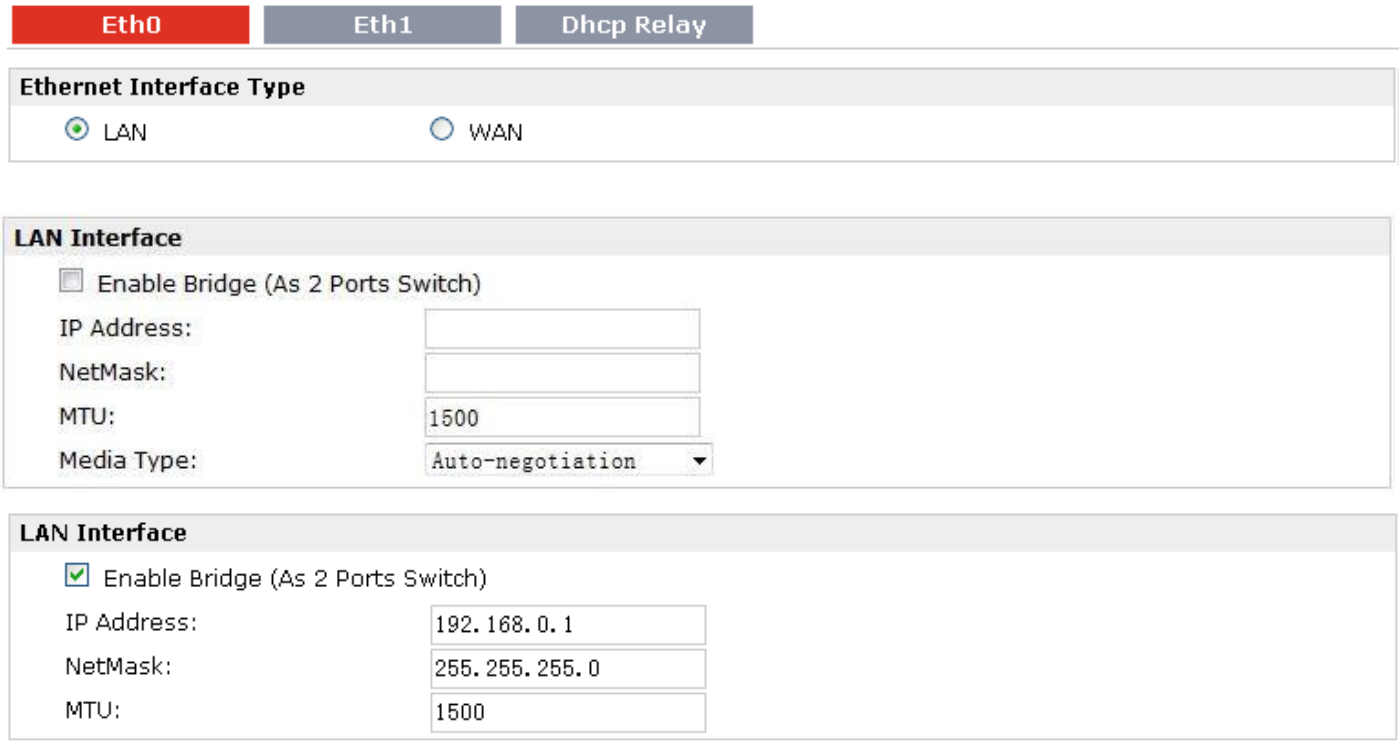
This section allow users to preset some ISP profiles which will be shown in the selection list of "Configuration"->"Cellular WAN"->"Network Provider Type".

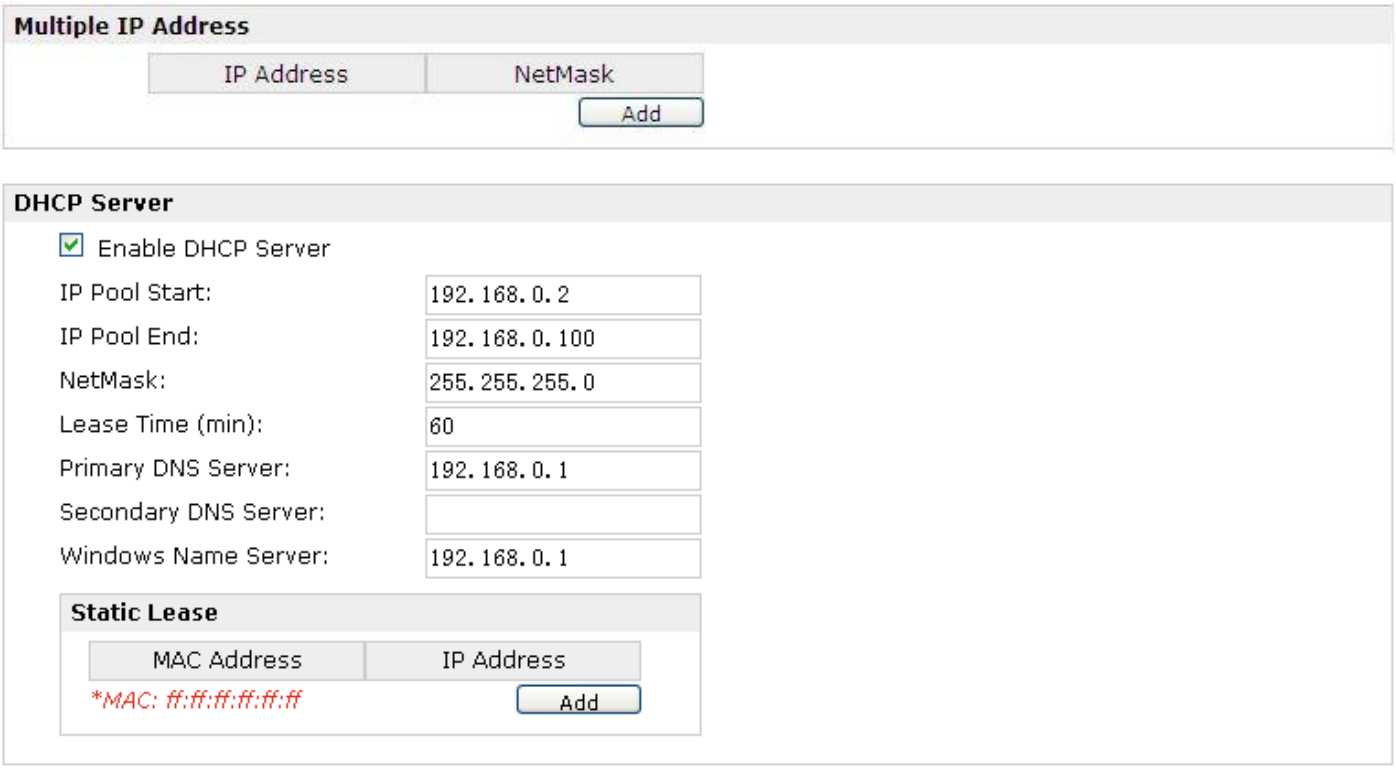


ISP Profile @Cellular WAN		
Item	Description	Default
ISP	Input the ISP's name which will be shown in the selection list of "Configuration"->"Cellular WAN"->"Network Provider Type".	Null
APN, Username, Password, Dialup No.	All these parameters were provided by the ISP.	Null

3.12 Configuration -> Ethernet

This section allows users to set the Ethernet WAN and LAN parameters of Eth0.

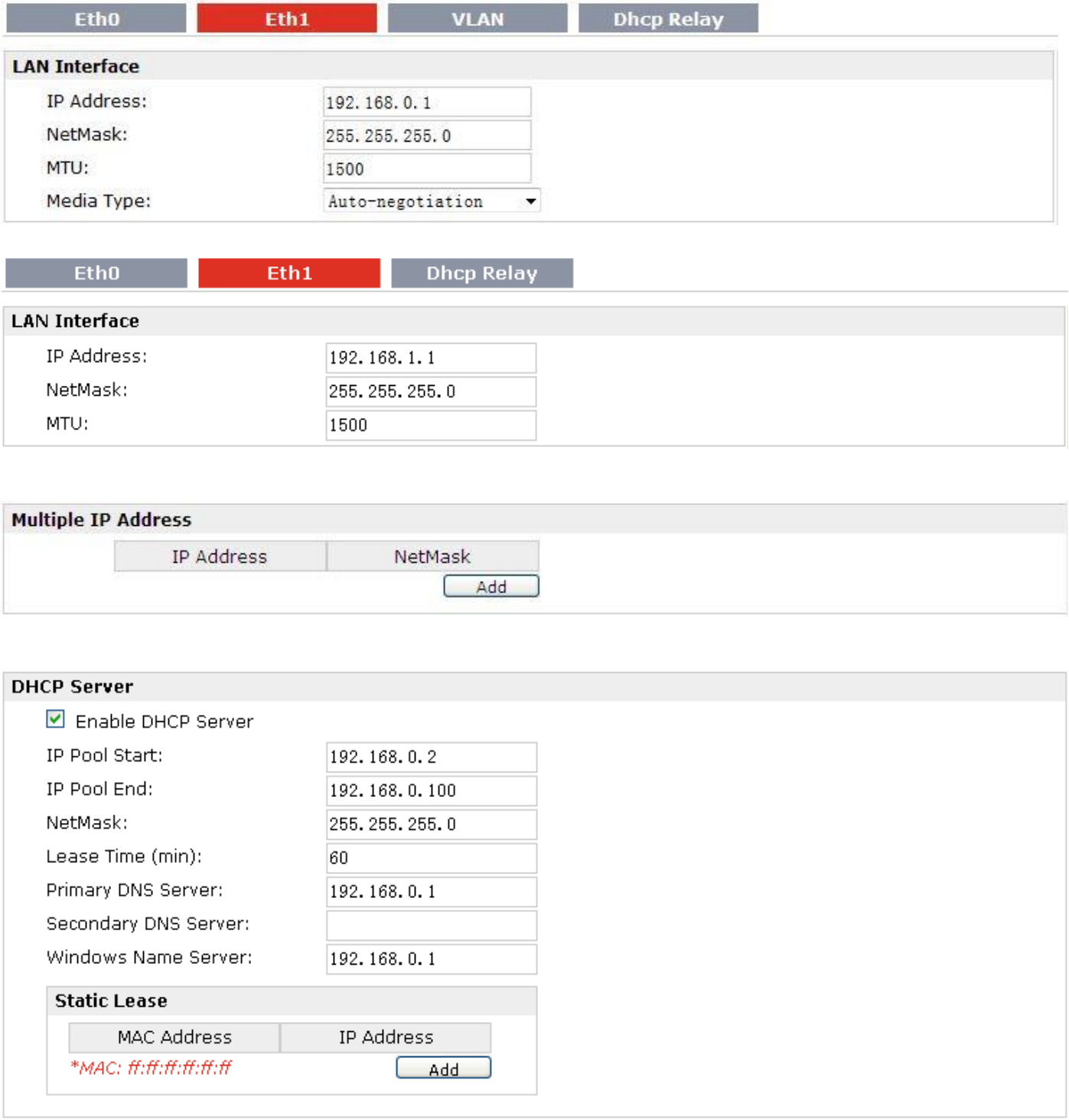




Eth0@Ethernet		
Item	Description	Default
Ethernet Interface Type	Eth0 can work under two different kinds of mode: LAN and WAN.	LAN
Enable Bridge @ LAN Interface	Enable to make Eth0 works under bridge mode with Eth1. Eth0 and Eth1 will have the same IP address under this mode.	Enable
IP Address, Netmask, MTU, Media Type@ LAN Interface	Set the IP address, Netmask, MTU and Media Type of Eth0. These parameters will be un-configurable if you enable Bridge.	Null
Multiple IP Address @ LAN Interface	Assign multiple IP addresses for Eth0.	Null
Enable DHCP Server @ DHCP Server	Enable to make router can lease IP address to DHCP clients which connect to Eth0.	Disable
IP Pool Start, IP Pool End @ DHCP Server	Define the beginning (IP Pool Start) and end (IP Pool End) of the pool of IP addresses which will lease to DHCP clients.	Null
Netmask @ DHCP Server	Define the Netmask which the DHCP clients will obtain from DHCP server.	Null
Lease Time @ DHCP Server(min)	Define the time which the client can use the IP address which obtained from DHCP server.	60
Primary/Secondary DNS Server @ DHCP Server	Define the primary/secondary DNS Server which the DHCP clients will obtain from DHCP server.	Null
Windows Name Server @ DHCP Server	Define the WINS Server which the DHCP clients will obtain from DHCP server.	Null

Static Lease @ DHCP Server	Define to lease static IP Addresses, which conform to MAC Address of the connected equipment.	Null

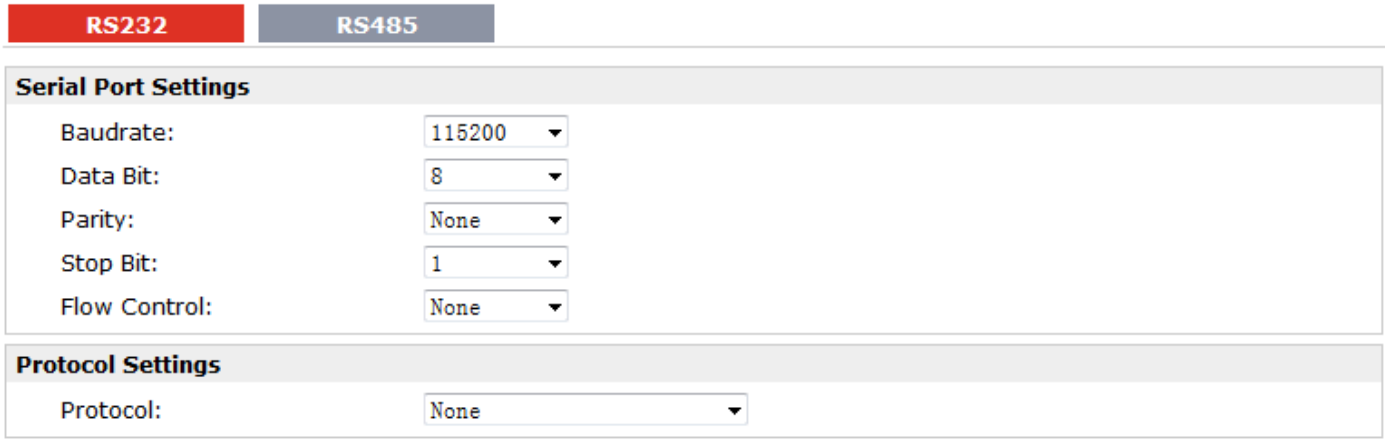
This section allows users to set the Ethernet WAN and LAN parameters of Eth1.



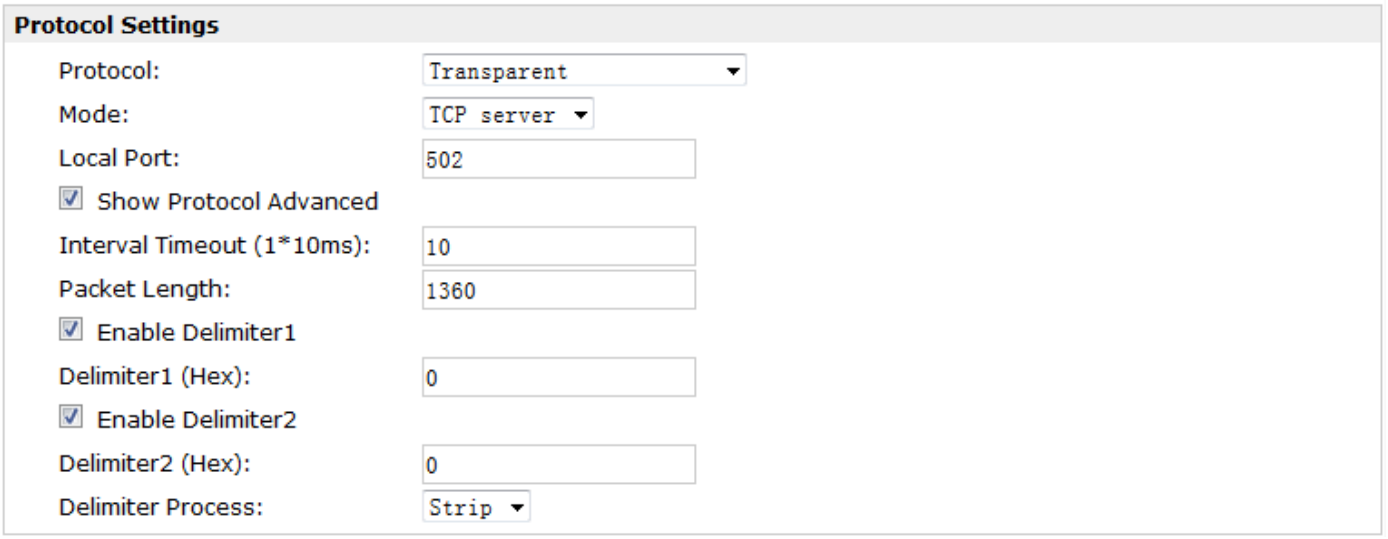
Eth1@Ethernet		
Item	Description	Default

3.14 Configuration -> Serial

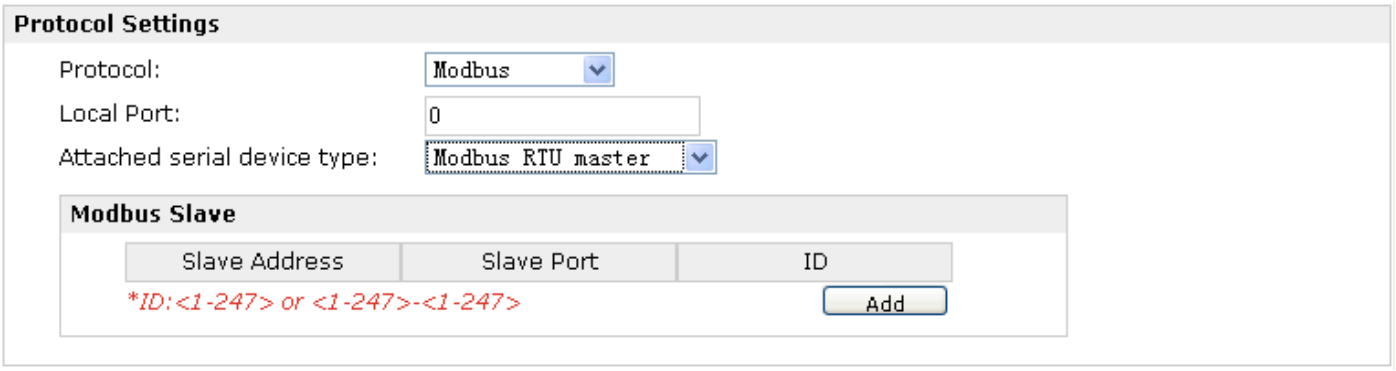
This section allows users to set the serial (RS232/RS485) parameters.



- When Select Protocol “Transparent”:



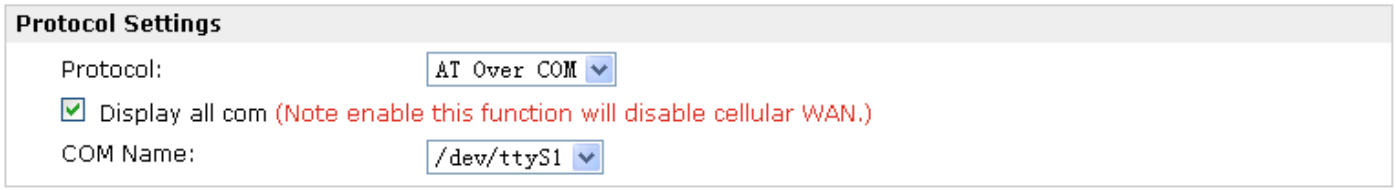
- When Select Protocol “Modbus”:



- When Select Protocol "Transparent Over Rlink":

- When Select Protocol "Modbus Over Rlink":

- When Select Protocol "AT Over COM":



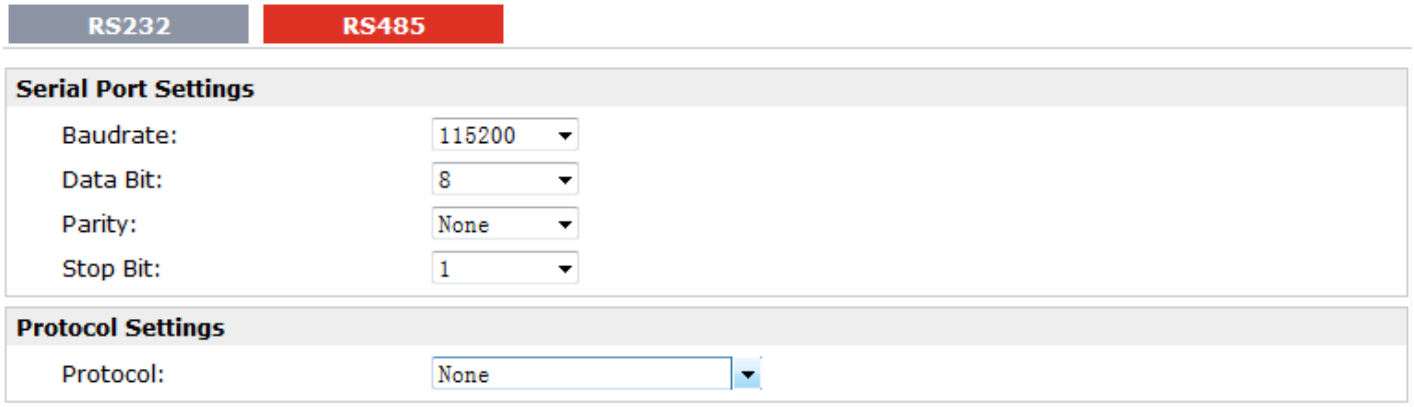
- When Select Protocol "GPS Report":

RS232 @ Serial		
Item	Description	Default
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
Parity	Select from "None", "Odd" and "Even".	None
Stop bit	Select from "1" and "2".	1
Flow control	Select from "None", "Software" and "Hardware".	None
Protocol	Select from "None", "Transparent", "Modbus", "Transparent Over Rlink",	None

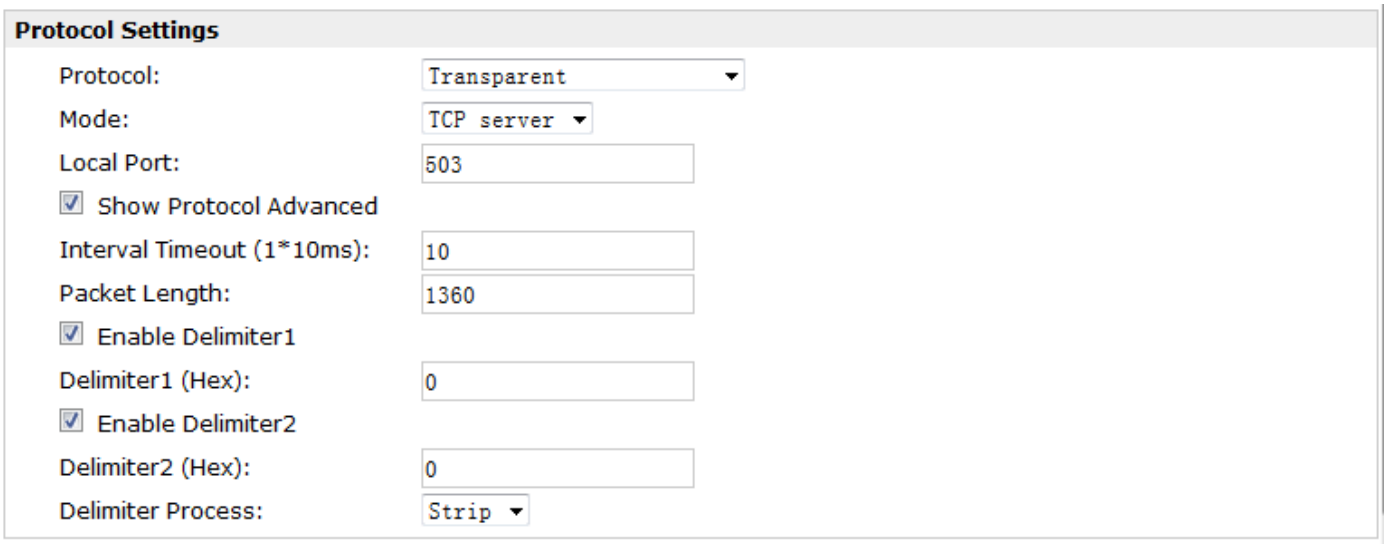
	"Modbus Over Rlink" "AT Over COM" and "GPS Report". 1. None: Router will do nothing in RS232 serial port. 2. Transparent: Router will transmit the serial data transparently without any protocols. 3. Modbus: Router will translate the Modbus RTU data to Modbus TCP data and vice versa. 4. Transparent Over Rlink: Router will send all data from RS232 serial port to Robustlink, then Robustlink will forward the data to another destination site. 5. Modbus Over Rlink: Router will translate all data from RS232 serial port to Modbus TCP protocol data, and then send to Robustlink, after that Robustlink will forward the data to another destination site. 6. AT Over COM: select to operate router via RS232 COM port. For example, enter AT commands to router via RS232 COM port. 7. GPS Report: select to enable router to output GPS status data through RS232 port.	
Mode @Transparent	Select from "TCP Server", "TCP Client" and "UDP". 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.	TCP Client
Local Port @Transparent	Enter the Local port for TCP or UDP.	0
Multiple Server @Transparent	Click "Add" button to add multiple server. You need to enter the server's IP and port, and enable or disable "Send data to serial". If you disable "Send data to serial", router will not transmit the data from this server to serial port. ***Note:*** *This section will not be displayed if you select "TCP server" in "Mode".*	None
show Protocol Advanced @ Transparent	Tick to enable protocol advanced setting.	Disable
Local IP @ Transparent	This item will show up when you enable any VPN tunnel of R3000-3P, it means serial data can be matched to this local IP address and be transmitted or received via VPN tunnel. ***Note****: when you do not enable any VPN tunnel, this item will not show up.*	Null
Interval Timeout @Transparent	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 or delimiter settings even when data is not reaching the interval timeout in the field.*	10
Packet Length @Transparent	The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. 0 for packet length, no maximum amount is specified and data in the buffer will be sent as specified by the interval timeout or delimiter settings or when the buffer is full. When a packet length between 1 and 1024 bytes is specified, data in the buffer will be	1360

	sent as soon it reaches the specified length. ***Note**: Data will also be sent as specified by the interval timeout or delimiter settings even when data is not reaching the preset packet length.*	
Enable Delimiter1/2	When Delimiter 1 is enabled, the serial port will queue the data in the buffer and send the data to the Cellular WAN/Ethernet WAN when a specific character, entered in hex format, is received. A second delimiter character may be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to control when data should be sent.	Disable
Delimiter1/2 (Hex) @Transparent	Enter the delimiter in Hex.	0
Delimiter Process @Transparent	The Delimiter process field determines how the data is handled when a delimiter is received. None: Data in the buffer will be transmitted when the delimiter is received; the data also includes the delimiter characters. Strip: Data in the buffer is first stripped of the delimiter before being transmitted.	Strip
Local IP @ Modbus	This item will show up When you enable any VPN tunnel of R3000-3P, it means serial data can be matched to this local IP address and be transmitted or received via VPN tunnel. ***Note**: when you do not enable any VPN tunnel, this item will not show up.*	0
Local Port @ Modbus	Enter the Local port for Modbus.	0
Attached serial device type @Modbus	Select From "Modbus RTU slave", "Modbus ASCⅡ slave", "Modbus RTU master" and "Modbus ASCⅡ master". Modbus RTU slave: router connects to Modbus slave device which works under Modbus RTU protocol. Modbus ASCⅡ slave: router connects to Modbus slave device which works under Modbus ASCⅡ protocol. ***Note**: When select "Modbus RTU slave" and "Modbus ASCⅡ slave" protocol, router is as TCP Server site, user need to enter a local port number in "Local Port @Modbus" and wait to be connected.* Modbus RTU master: router connects to master device which works under Modbus RTU protocol. Modbus ASCⅡ master: router connects to master device which works under Modbus ASCⅡ protocol. ***Note**: When select "Modbus RTU* master*" and "Modbus ASCⅡ*master*" protocol, router is as TCP Client site, user need to enter slave address and slave port number in "*Slave Address @ Modbus Slave *" and "*Slave Port @ Modbus Slave*", and connect to Server site.*	Modbus RTU slave
Modbus Slave @Modbus	Add the Modbus slaves which will be polled by Modbus master (router). This section only displayed when you select "Modbus RTU master" or "Modbus ASCⅡ master" in "Attached serial device type".	Null
Slave Address @ Modbus Slave	This connection is usually used to connect to the Modbus slave devices which as TCP server. Enter IP address of the TCP server.	Null
Slave Port @ Modbus	Enter the port number of TCP server.	Null

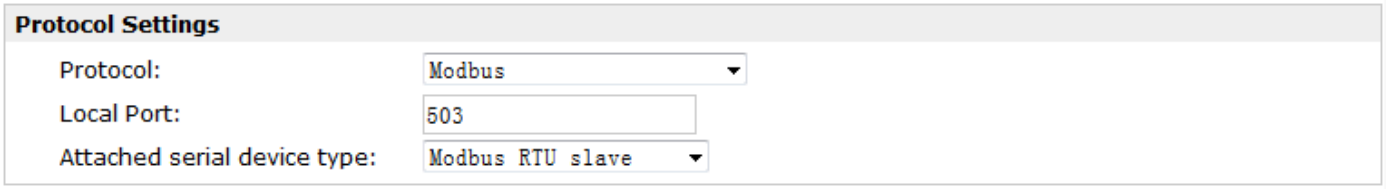
Slave		
ID @ Modbus Slave	Enter the ID number of TCP server.	Null
Interval Timeout @ Transparent Over Rlink	The serial port will queue the data in the buffer and send the data to the Cellular WAN/Ethernet WAN when it reaches the Interval Timeout in the field.	10
Attached serial device type @ Modbus Over Rlink	Select From "Modbus RTU slave", "Modbus ASCⅡ slave". Modbus RTU slave: router connects to slave device which works under Modbus RTU protocol. Modbus ASCⅡ slave: router connects to slave device which works under Modbus ASCⅡ protocol.	Null
Display all com @ AT Over COM	Enable to display all virtual com of the module inside the router. Generally, router will occupy /dev/ttyUSB0 and /dev/ttyUSB2 for dialing up to GPRS. ***Note**: Enable this function will disable Cellular WAN function.*	Disable
COM Name	Show the virtual com name of the module inside.	/dev/ttyUSB1



- When Select Protocol "Transparent":



- When Select Protocol “Modbus”:



- When Select Protocol “Transparent Over Rlink”:

- When Select Protocol “Modbus Over Rlink”:

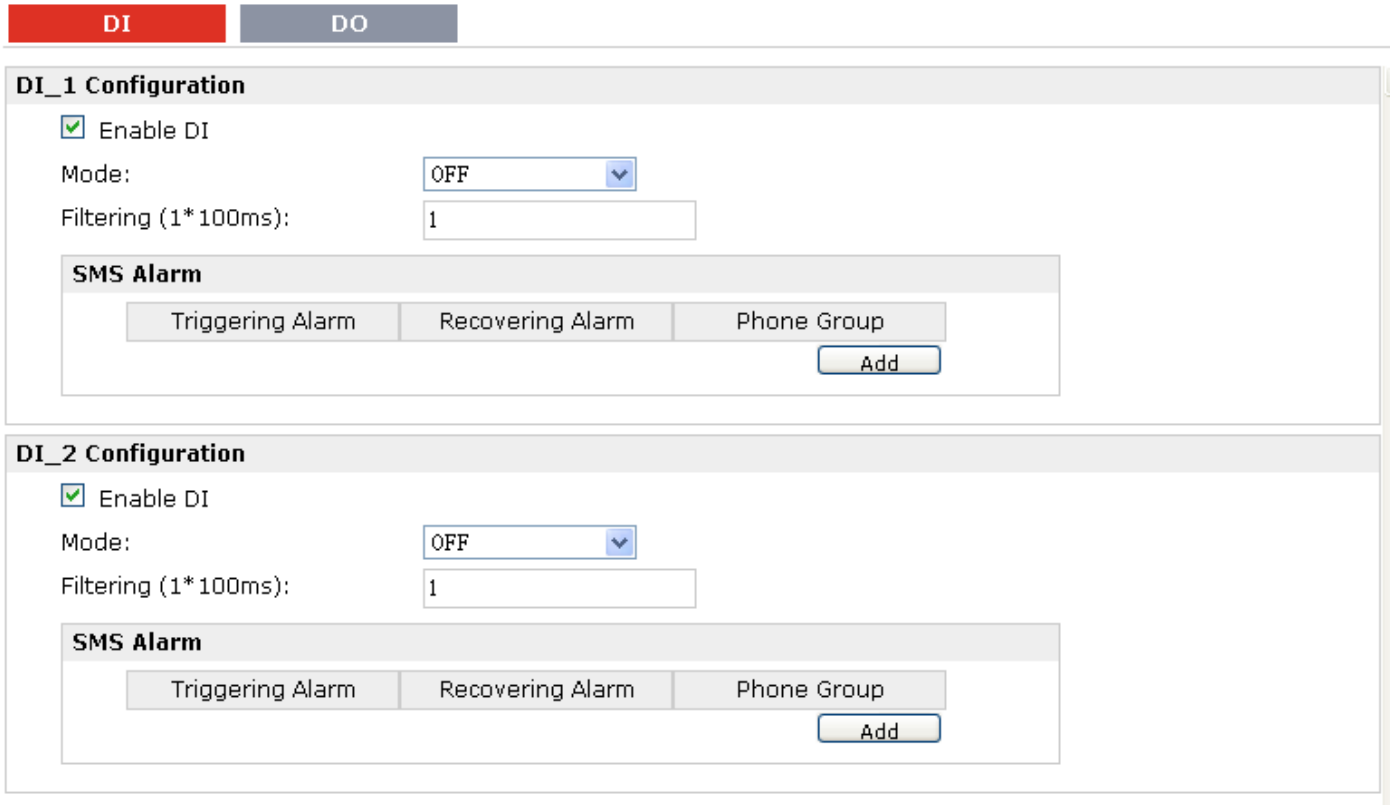
RS485 @ Serial		
Item	Description	Default
Baud-rate	Select from “300”, “600”, “1200”, “2400”, “4800”, “9600”, “19200”, “38400”, “57600” , “115200”and “230400”.	115200
Data bit	Select from “7” and “8”.	8
Parity	Select from “None”, “Odd” and “Even”.	None
Stop bit	Select from “1” and “2”.	1
Protocol	Select from “None”, “Transparent” and “Modbus”. Transparent: Router will transmit the serial data transparently without any protocols. Modbus: Router will transmit the serial data with Modbus protocol.	Transparent
Mode @Transparent	Select from “TCP Server”, “TCP Client” and “UDP”.	TCP Client
Local Port @Transparent	Enter the Local port for TCP or UDP.	0
Multiple Server @Transparent	Click “Add” button to add multiple server. You need to enter the server’s IP and port, and enable or disable “Send data to serial”. If you disable “Send data to serial”, router will not transmit the data from this server to serial port. ***Note:*** *This section will not be displayed if you select “TCP server” in “Mode”.*	Null
Enable Protocol @Transparent	Tick to enable protocol advanced setting.	Disable
Local IP @ Transparent	This item will show up When you enable any VPN tunnel of R3000-3P, it means serial data can be matched to this local IP address and be transmitted or received via VPN tunnel.	0

	***Note**: when you do not enable any VPN tunnel, this item will not show up.*	
Interval Timeout @Transparent	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 or delimiter settings even when data is not reaching the interval timeout in the field.*	10
Packet Length @Transparent	The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. 0 for packet length, no maximum amount is specified and data in the buffer will be sent as specified by the interval timeout or delimiter settings or when the buffer is full. When a packet length between 1 and 1024 bytes is specified, data in the buffer will be sent as soon it reaches the specified length. ***Note**: Data will also be sent as specified by the interval timeout or delimiter settings even when data is not reaching the preset packet length.*	1360
Enable Delimiter1	When Delimiter 1 is enabled, the serial port will queue the data in the buffer and send the data to the Cellular WAN/Ethernet WAN when a specific character, entered in hex format, is received. A second delimiter character may be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to control when data should be sent.	Disable
Delimiter1 (Hex) @ Transparent	Enter the delimiter in Hex.	0
Delimiter Process @ Transparent	The Delimiter process field determines how the data is handled when a delimiter is received. None: Data in the buffer will be transmitted when the delimiter is received; the data also includes the delimiter characters. Strip: Data in the buffer is first stripped of the delimiter before being transmitted.	Strip
Local IP @ Modbus	This item will show up When you enable any VPN tunnel of R3000-3P, it means serial data can be matched to this local IP address and be transmitted or received via VPN tunnel. ***Note**: when you do not enable any VPN tunnel, this item will not show up.*	0
Local Port @ Modbus	Enter the Local port for Modbus.	0
Attached serial device type @ Modbus	Select From “Modbus RTU slave”, “Modbus ASCⅡ slave”, “Modbus RTU master” and “Modbus ASCⅡ master”. Modbus RTU slave: router connects to slave device which works under Modbus RTU protocol. Modbus ASCⅡ slave: router connects to slave device which works under Modbus ASCⅡ protocol. Modbus RTU master: router connects to master device which works under Modbus RTU protocol. Modbus ASCⅡ master: router connects to master device which works under Modbus ASCⅡ protocol.	Modbus RTU slave
Modbus Slave @	Add the Modbus slaves which will be polled by Modbus master (router). This	Null

Modbus	section only displayed when you select “Modbus RTU master” or “Modbus ASCII master” in “Attached serial device type”.	
Slave Address @ Modbus Slave	This connection is usually used to connect to the Modbus slave devices which as TCP server. Enter IP address of the TCP server.	Null
Slave Port @ Modbus Slave	Enter the port number of TCP server.	Null
ID @ Modbus Slave	Enter the ID number of TCP server.	Null
Interval Timeout @ Transparent Over Rlink	Serial port will queue the data in buffer and then send it to the Cellular WAN/Ethernet WAN when it reaches the Interval Timeout in this field.	10
Attached serial device type @ Modbus Over Rlink	Select From “Modbus RTU slave”, “Modbus ASCⅡ slave”. Modbus RTU slave: router connects to slave device which works under Modbus RTU protocol. Modbus ASCⅡ slave: router connects to slave device which works under Modbus ASCⅡ protocol.	Modbus RTU slave

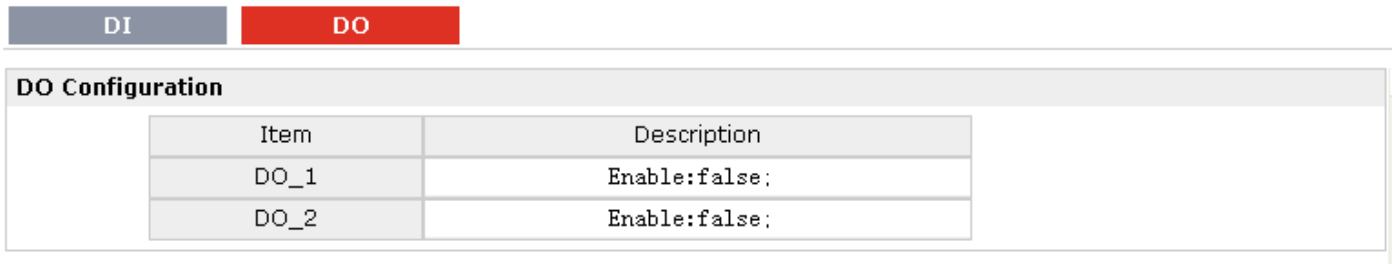
3.15 Configuration -> DI/DO

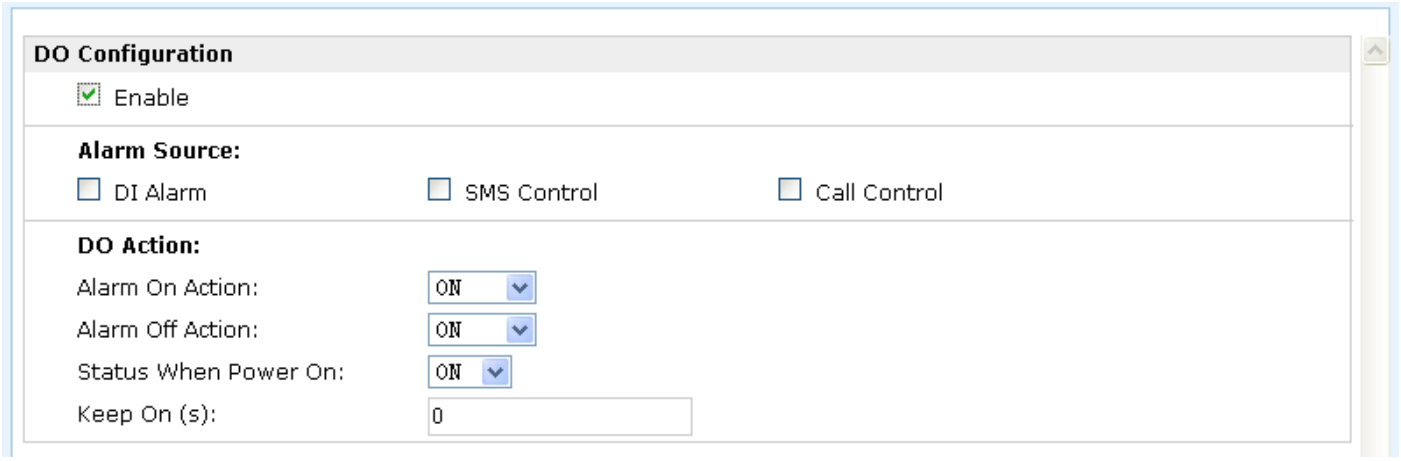
This section allows users to set the DI/DO parameters.



DI @ DI/DO		
Item	Description	Default

Enable DI	Click to Enable DI.	Disable
Mode	Select from “OFF”, “ON”, “EVENT_COUNTER”. OFF: Connect to GND (logic 0). When pin DI connects to GND, R3000-3P will detect there is a DI alarm input. ON: Open from GND (logic 1). When pin DI does not connect to GND, R3000-3P will detect there is a DI alarm input. EVENT_COUNTER: under event counter mode.	OFF
Filtering	Software filtering is used to control switch bounces. Input from 0 to 10000ms.	1
Count Trigger	Available when DI under Event Counter mode. Input from 0 to 100. (0=will not trigger alarm) It will trigger alarm when counter reaches this figure. After triggering alarm, DI will keep counting but not trigger alarm again.	0
Counter Active	Available when DI under Event Counter mode. Select from “Hi to Lo”, “Lo to Hi”. In Event Counter mode, the channel accepts limit or proximity switches and counts events according to the ON/OFF status. When “Lo to Hi” is selected, the counter value increases when the attached switch is pushed. When “Hi to Lo” is selected, the counter value increases when the switch is pushed and released.	Lo to Hi
Counter Start When Power On	Available when DI under Event Counter mode. Start counting as soon as possible on the modem when enable this option. When R3000-3P need to work under Event Counter mode, user shall enable “Counter Start When Power On”. If “Counter Start When Power On” is disabled, it will also start counting when receiving SMS command. Refer to another document *SMS command of R3000-3P*.	Disable
Triggering Alarm	The SMS to receive upon triggering alarm. (70 ASIC II char max)	Null
Recovering Alarm	The SMS to receive upon recovering alarm. (70 ASIC II char max)	Null
Phone Group	The alarm SMS will send to specified phone group. Each phone group include up to 10 phone numbers.	Null





DO @ DI/DO		
Item	Description	Default
Enable	Click to enable DO.	Disable
Alarm Source	Digital Output initiates according to different alarm source. Selected from “DI Alarm”, “SMS Control”, “Call Control”, selections can be one or more. DI Alarm: Digital Output triggers the related action when there is alarm from Digital Input. SMS Control: Digital Output triggers the related action when receiving SMS from the number in the phone book. Call Control: Digital Output triggers the related action when receiving phone call from the number in the phone book.	Null
Alarm On Action	Digital Output initiates when there is an alarm. Selected from “OFF”, “ON”, “Pulse”. OFF: Open from GND when triggered. ON: Short contact with GND when triggered. Pulse: Generates a square wave as specified in the pulse mode parameters when triggered.	ON
Alarm Off Action	Digital Output initiates when alarm recovered. Selected from “OFF”, “ON”, “Pulse”. OFF: Open from GND when triggered. ON: Short contact with GND when triggered. Pulse: Generates a square wave as specified in the pulse mode parameters when triggered.	ON
Status When Power On	Specify the Digital Output status when power on. Selected from “OFF”, “ON”. OFF: Open from GND. ON: Short contact with GND.	ON
Keep On (s)	Available when digital output Alarm On Action/Alarm Off Action status is ON, input the Digital Output keep on status time. Input from 0 to 255 seconds. (0=keep on until the next action)	0

Delay	Available when enable Pulse in Alarm On Action/Alarm Off Action. The first pulse will be generated after a "Delay". Input from 0 to 30000ms. (0=generate pulse without delay)	0
Low	Available when enable Pulse in Alarm On Action/Alarm Off Action. In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The low level widths are specified here. Input from 1 to 30000 ms.	10
High	Available when enable Pulse in Alarm On Action/Alarm Off Action. In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The high level widths are specified here. Input from 1 to 30000 ms.	10
Output	Available when enable Pulse in Alarm On Action/Alarm Off Action. The number of pulses, input from 0 to 30000. (0 for continuous pulse output)	0
SMS Content On	Available when enable SMS Control in Alarm Source. Input the SMS content to enable "Alarm On Action" by SMS (70 ASIC II char max).	Null
SMS Content Off	Available when enable SMS Control in Alarm Source. Input the SMS content to enable "Alarm Off Action" by SMS. (70 ASIC II char max)	Null
SMS Content On Reply	Input the SMS content, which will be sent after DO was triggered. (70 ASIC II char max).	Null
SMS Content Off Reply	Input the SMS content, which will be sent after DO was recovered. (70 ASIC II char max).	Null
Phone Group	Click to add phone groups.	Null

3.16 Configuration -> USB

This section allows users to set the USB parameters.

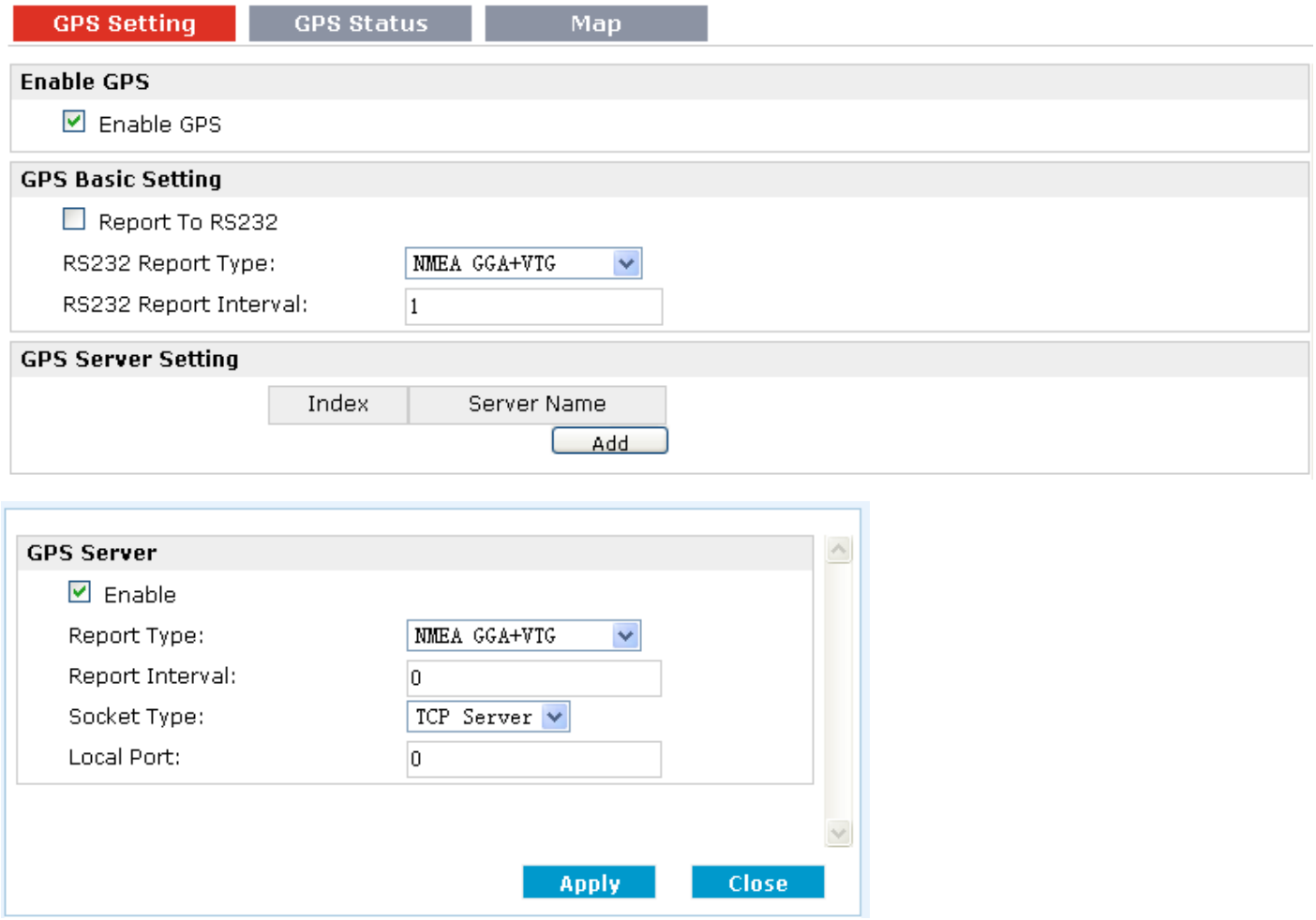
***Note**: Users can insert an USB storage device, such as U disk and hard disk, into the router's USB interface. If there is configuration file or firmware of R3000-3P inside the USB storage devices, R3000-3P will automatically update the configuration file or firmware. We will provide another file to show how to do USB automatic update.*

USB		
Item	Description	Default
Enable automatic update	Click Enable to automatically update the configuration file of R3000-3P when	Disable

of configuration	insert the USB storage devices which has R3000-3P's configuration file.	
Enable automatic update of firmware	Click Enable to automatically update the firmware of R3000-3P when insert the USB storage devices which has R3000-3P's firmware.	Disable

3.17 Configuration -> GPS

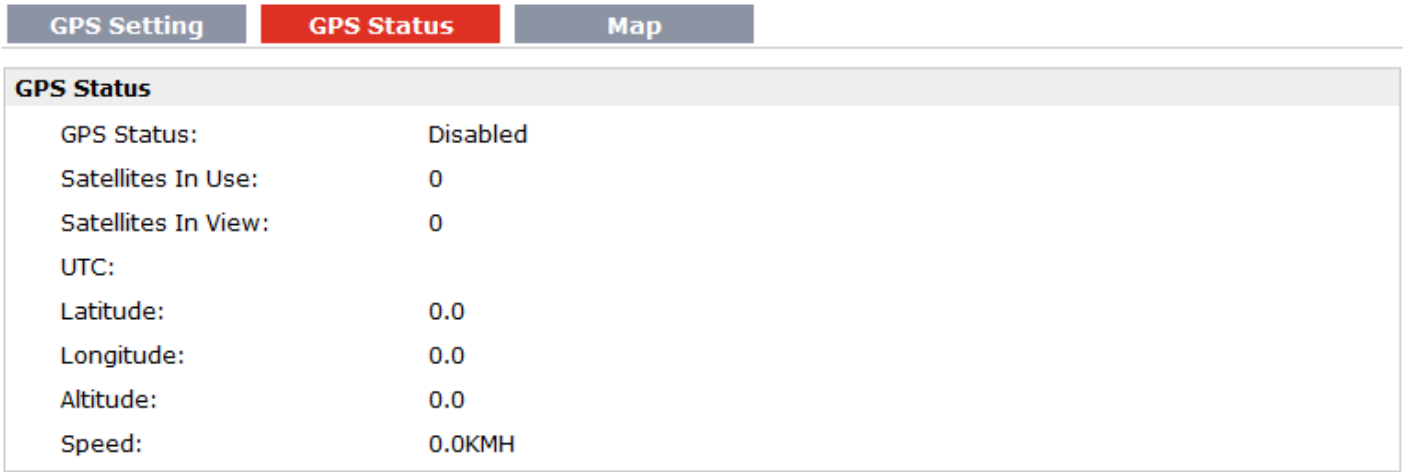
This section allows users to set the GPS setting parameters.



GPS Setting @ GPS		
Item	Description	Default
Enable GPS	Click to enable GPS function.	Disable
Report To RS232	Click to enable GPS report to RS232 serial port of router.	Disable
RS232 Report Type	Select from "NMEA GGA+VTG", "NMEA GGA+VTG+RMC" and "NMEA RMC". NMEA GGA+VTG: Global Positioning System Fix Data（GGA）+ Track Made Good and Ground Speed（VTG）. NMEA GGA+VTG+RMC: Global Positioning System Fix Data（GGA）+ Track Made Good and Ground Speed（VTG）+ Recommended Minimum Specific	NMEA GGA+VTG

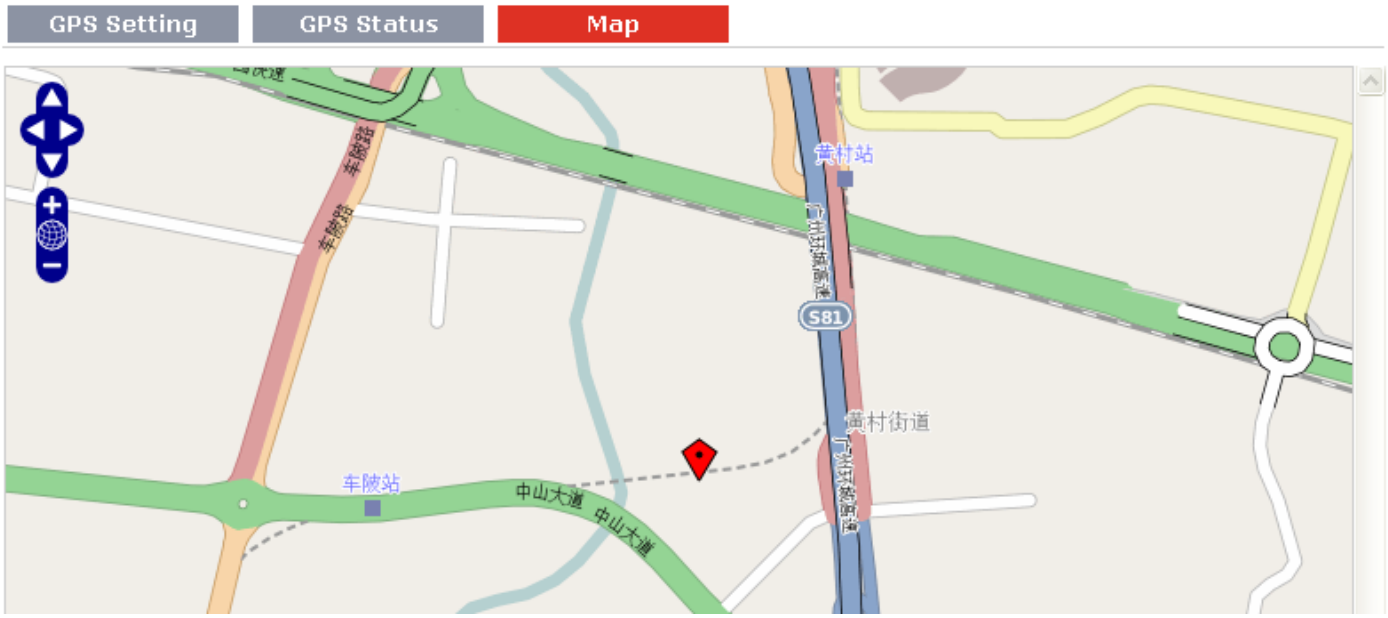
	GPS/TRANSIT Data（RMC）. NMEA RMC: Recommended Minimum Specific GPS/TRANSIT Data（RMC）.	
RS232 Report Interval	Set the interval to report GPS status to RS232 serial port of router.	1
Index @ GPS Server Setting	Show the index of GPS Server.	Null
Server Name @ GPS Server Setting	Show the type of GPS Server.	Null
Add	Click “Add” to add GPS Server.	
Report Type	Select from “NMEA GGA+VTG”, “NMEA GGA+VTG+RMC” and “NMEA RMC”. NMEA GGA+VTG: Global Positioning System Fix Data（GGA）+ Track Made Good and Ground Speed（VTG）. NMEA GGA+VTG+RMC: Global Positioning System Fix Data（GGA）+ Track Made Good and Ground Speed（VTG）+ Recommended Minimum Specific GPS/TRANSIT Data（RMC）. NMEA RMC: Recommended Minimum Specific GPS/TRANSIT Data（RMC）.	NMEA GGA+VTG
Report Interval	Set the interval to report GPS status to GPS Server.	0
Socket Type	Select from “TCP Server”, “TCP Client” and “UDP”. TCP Client: Router works as TCP client, initiate TCP connection to TCP server (GPS Server), the server address supports both IP and domain name. TCP Server: Router works as TCP server (GPS Server), listening for connection request from TCP client. UDP: Router works as UDP client.	TCP Server
Local Port @ TCP Server	Set the local port number of TCP server.	0
Server Address @ TCP Client	Set the Server address of TCP server.	Null
Server Port @ TCP Client	Set the remote Port number of TCP server. ***Note**: router supports up to 3 GPS servers, supports re-connect when the TCP connection is down.*	0

This section allows users to check the GPS status.



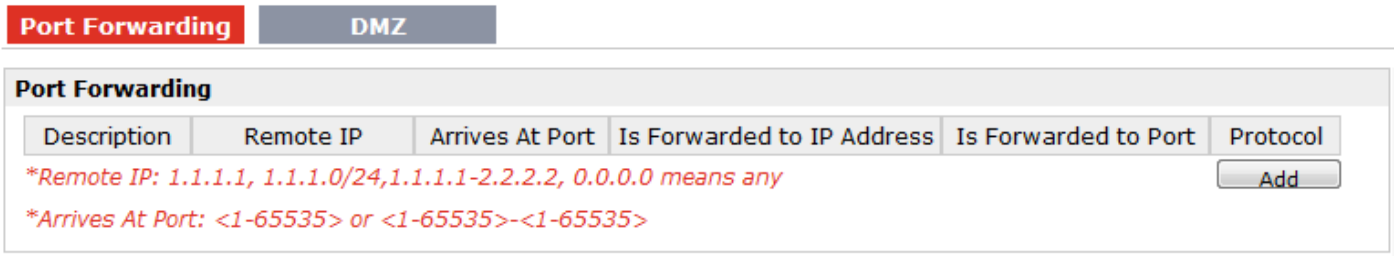
GPS Status @ GPS		
Item	Description	Default
GPS Status	Show the GPS Status. GPS status includes: Not Installed, Disabled, No Fix/Invalid, Standalone GPS Fix, Differential GPS Fix. Not Installed: No GPS module inside. Disabled: GPS function is not enabled (not click “Enable GPS” in item “GPS Setting” yet). No Fix/Invalid: GPS function is enabled, but do not get GPS signal (User should put router outdoor to get stronger GPS signal). Standalone GPS Fix: Standalone GPS techniques is a mature, universal GPS positioning mode, only get position from satellite. Differential GPS Fix: Differential GPS techniques are used to enhance the quality of location data. It can be applied in real-time directly in the field or when post processing data in the office.	Not Installed
Satellites In Use	Show how many satellites are in use.	0
Satellites In View	Show how many satellites are in view.	0
UTC	Show the UTC of satellites, which is world unified time, not local time.	Null
Latitude	Show the latitude status of router.	0.0
Longitude	Show the Longitude status of router.	0.0
Altitude	Show the Altitude status of router.	0.0
Speed	Show the movement speed of router.	0.0KMH

This section allows users to check the real time GPS status of router in the map.

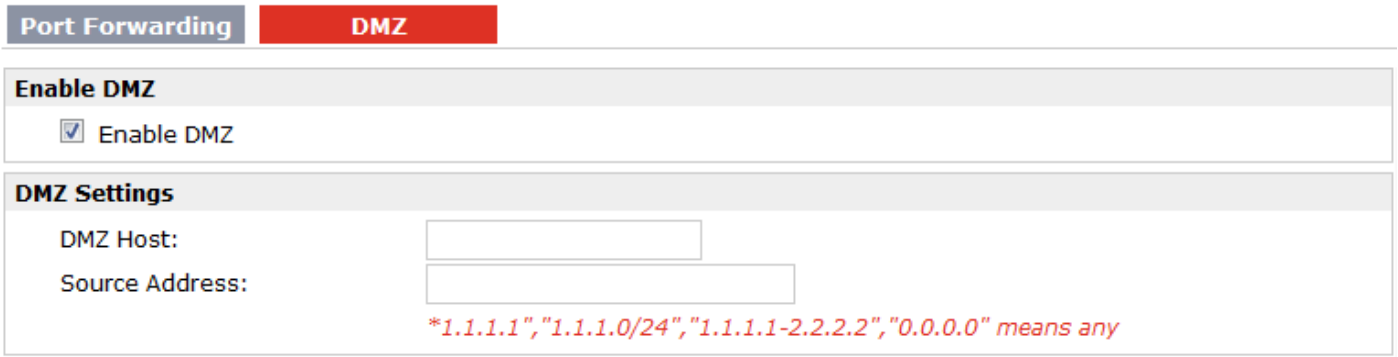


3.18 Configuration -> NAT/DMZ

This section allows users to set the NAT/DMZ parameters.



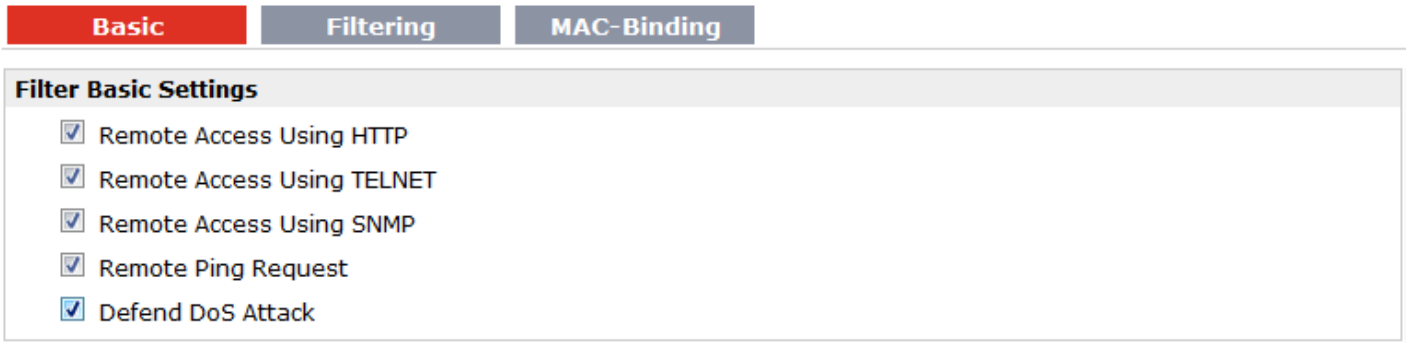
Port Forwarding @ NAT/DMZ		
Item	Description	Default
Port Forwarding	Manually defining a rule in the router to send all data received on some range of ports on the internet side to a port and IP address on the LAN side.	Null
Remote IP	Set the remote IP address.	Null
Arrives At Port	The port of the internet side which you want to forward to LAN side.	Null
Is Forwarded to IP Address	The device's IP on the LAN side which you want to forward the data to.	Null
Is Forwarded to Port	The device's port on the LAN side which you want to forward the data to.	Null
Protocol	Select from "TCP", "UDP" or "TCP&UDP" which depends on the application.	TCP



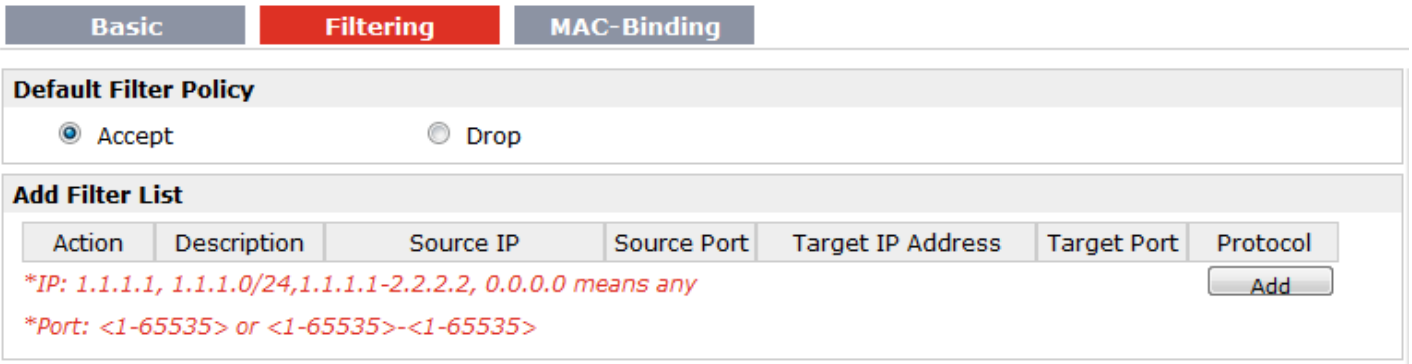
DMZ @ NAT/DMZ		
Item	Description	Default
DMZ	DMZ host is a host on the internal network that has all ports exposed, except those ports otherwise forwarded.	Null
Enable DMZ	Select to enable the DMZ function.	Enable
DMZ Host	Enter the IP address of the DMZ host which on the internal network.	0.0.0.0
Source Address	Set the address which can talk to the DMZ host. Null means for any addresses.	0.0.0.0

3.19 Configuration -> Firewall

This section allows users to set the firewall parameters.



Basic @ Firewall		
Item	Description	Default
Remote Access Using HTTP	Enable to allow users to access the router remotely on the internet side via HTTP.	Enable
Remote Access Using TELNET	Enable to allow users to access the router remotely on the internet side via Telnet.	Enable
Remote Access Using SNMP	Enable to allow users to access the router remotely on the internet side via SNMP.	Enable
Remote Ping Request	Enable to make router reply the Ping requests from the internet side.	Enable
Defend Dos Attack	Enable to defend dos attack. Dos attack is an attempt to make a machine or network resource unavailable to its intended users.	Enable

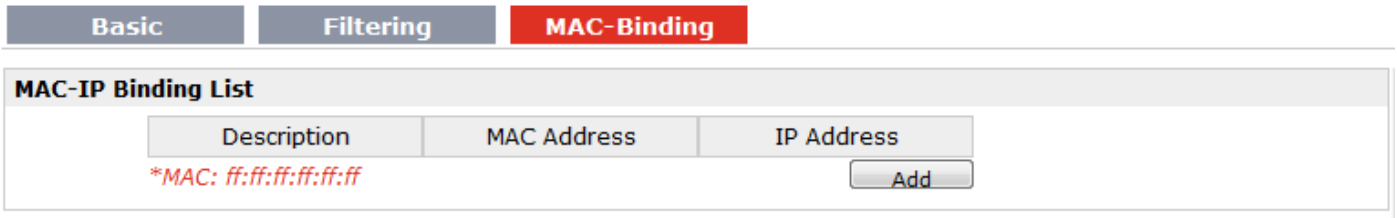


Filtering @ Firewall		
Item	Description	Default
Default Filter Policy	Select from “Accept” and “Drop”. Accept: Router will reject all the connecting requests except the hosts which fit the filter list. Drop: Router will only accept the connecting requests from the hosts which fit the filter list.	Accept

Add Filter List	Click “Add” to add a filter list.	Null
Action	Select from “Accept” and “Drop”. Accept: Router will reject all the connecting requests except the hosts which fit this filter rule. Drop: Router will only accept the connecting requests from the hosts which fit this filter rule.	Accept
Source IP	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 Port	Defines if access is allowed from one or a range of port which is defined by Source Port.	Null
Target IP 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
Target Port	Defines if access is allowed tone or a range of port which is defined by Target Port.	Null
Protocol	Select from “TCP”, “UDP”, “TCP&UDP”, “ICMP” or “ALL”. If you don’t know what kinds of protocol of your application, we recommend you select “ALL”.	TCP

***Note**: You can use “-“to define a range of IP addresses or ports, e.g. 1.1.1.1-2.2.2.2, 10000-12000.*

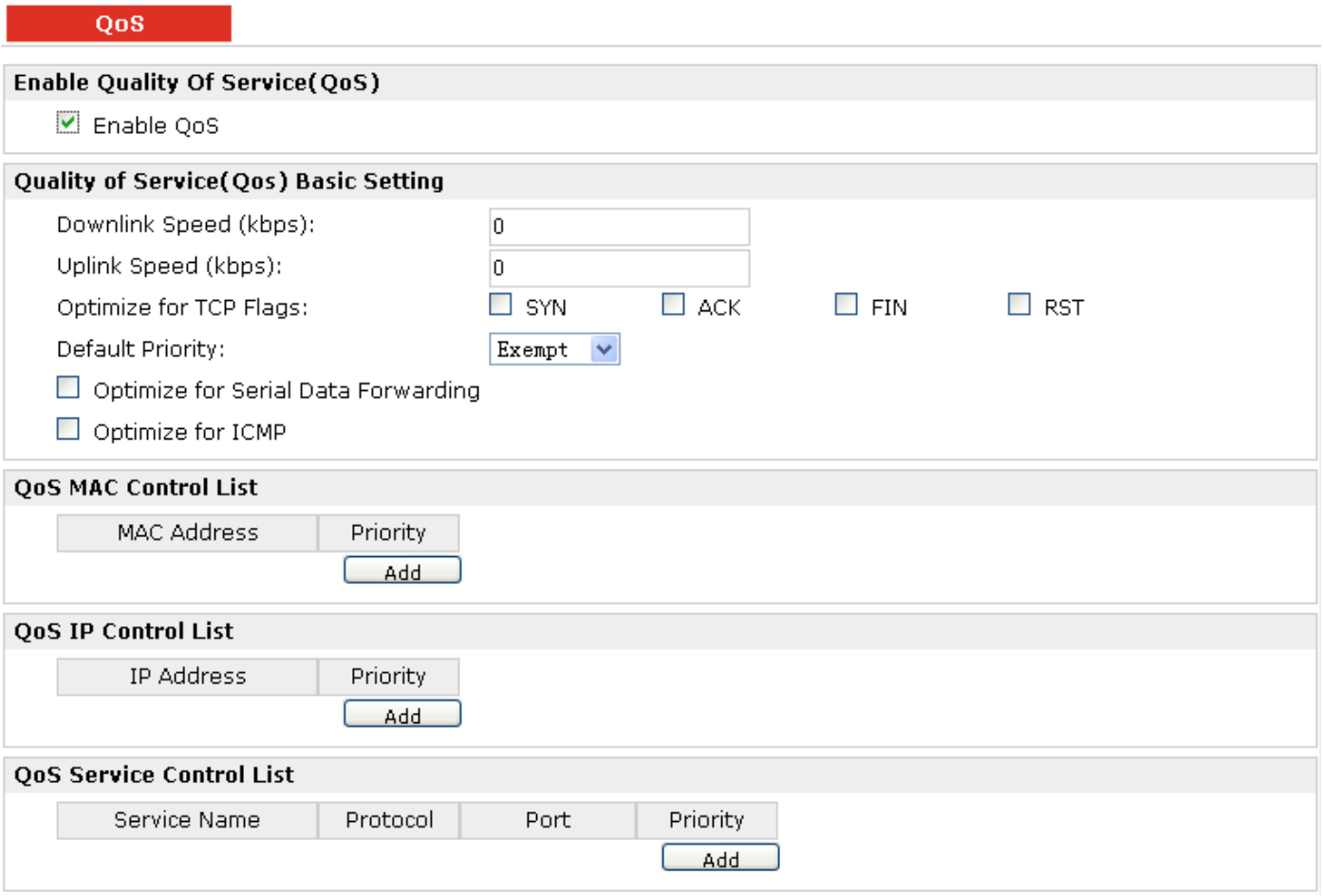
***Note:** the filtering settings should be divided into two parts. Part 1 is the Exact Filter List and Part 2 is the Default Filter Policy. The priority of Exact Filter List is higher than Default Filter Policy. It means that while Router receive IP packets from WAN side, it will check the Exact Filter List first, if the IP packets mismatch the Exact Filter List, then Router will execute the Default Filter Policy.*



Mac-Binding @ Firewall		
Item	Description	Default
Mac-IP Bounding	The defined host (MAC) on the LAN side only can use the defined IP address to communicate with router, or will be rejected.	Null
Mac Address	Enter the defined host’s Mac Address.	Null
IP Address	Enter the defined host’s IP Address.	Null

3.20 Configuration -> QoS

This section allows users to set the QoS parameters.



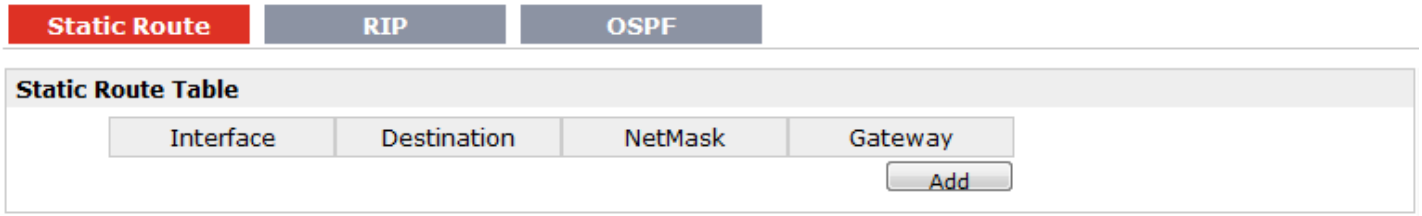
QoS		
Item	Description	Default
Enable QoS	Click to enable "QoS" function.	Disable
Downlink Speed (kbps)	Prescribe downlink speed of router. ***Note**: Default setting"0" means that there is no limitation of downlink speed.*	0
uplink Speed (kbps)	Prescribe uplink speed of router. ***Note**: Default setting"0" means that there is no limitation of uplink speed.*	0
Optimize for TCP Flags	User can choose to enable TCP flags: "SYN", "ACK", "FIN", "RST", which means data with above TCP Flags will get the highest priority to occupy bandwidth. After enabled, router will enhance respond timeout of TCP control, in case that data resend frequently.	Disable
Default Priority	Select from "Exempt", "Premium", "Express", "Normal" and "Bulk". Users (Services) with no other pre-priority set will use this default priority. Exempt: this is the highest priority which guarantees that the minimum global rate of router is 50% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed". Premium: guarantees that the minimum global rate of router is 25% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed". Express: guarantees that the minimum global rate of router is 15% of "Downlink	Normal

	Speed", and the maximum rate can reach to 100% of "Downlink Speed". Normal: guarantees that the minimum global rate of router is 10% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed". Bulk: guarantees that the minimum global rate of router is 1% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed".	
Optimize for Serial Data Forwarding	Enable to optimize for serial data forwarding, which means serial data forwarding will get the highest priority to occupy bandwidth. When enable serial data forwarding it need to enable local port number for controlling. Therefore, it needs to set local port number of router even if router is as TCP Client.	Disable
Optimize for ICMP	Enable to optimize for ICMP, which means ICMP will get the highest priority to occupy bandwidth. After enabled respond interval of PING control will be shorter. ***Note**: if user click to enable "Optimize for TCP Flags", "Optimize for Serial Data Forwarding", and "Optimize for ICMP" at the same time (these three services are in the same priority level), router will automatically start Stochastic Fairness Queueing (SFQ) strategy to make a fair bandwidth allocation, in case of one service occupy all the bandwidth.*	Disable
MAC Address @ QoS MAC Control List	Enter MAC address of the user (for example, PC) who you want to set it with QoS Control. 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
Priority @ QoS MAC Control List	Select from "Exempt", "Premium", "Express", "Normal" and "Bulk". Select the priority of the user (for example, PC) who you want to set it with QoS Control. Exempt: this is the highest priority which guarantees that the minimum global rate of router is 50% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed". Premium: guarantees that the minimum global rate of router is 25% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed". Express: guarantees that the minimum global rate of router is 15% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed". Normal: guarantees that the minimum global rate of router is 10% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed". Bulk: guarantees that the minimum global rate of router is 1% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed".	Exempt
IP Address @ QoS IP Control List	Enter IP address of the user (for example, PC) who you want to set it with QoS Control. Router supports up to 20 users set with QoS IP Control. If want to control one network segment, user can set "IP Address" as format "x.x.x.x/24" or "x.x.x.x/255.255.255.0". For example, if we to control network segment "172.16. x.x", we can set "172.16.0.0/16" or "172.16.0.0/255.255.0.0" in "IP Address".	Null
Priority @ QoS IP Control List	Select from "Exempt", "Premium", "Express", "Normal" and "Bulk". Select the priority of the user (for example, PC) who you want to set it with QoS Control.	Exempt

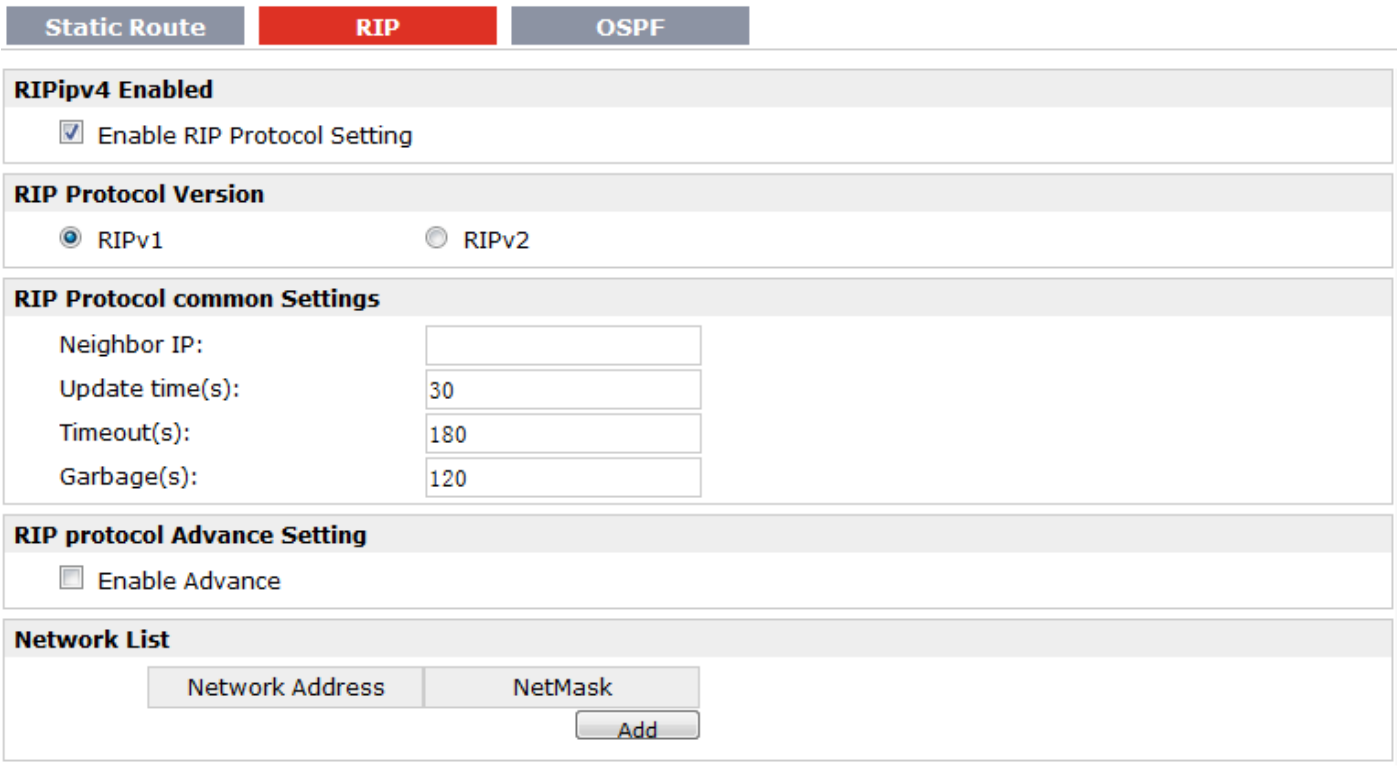
	Exempt: this is the highest priority which guarantees that the minimum global rate of router is 50% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed". Premium: guarantees that the minimum global rate of router is 25% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed". Express: guarantees that the minimum global rate of router is 15% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed". Normal: guarantees that the minimum global rate of router is 10% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed". Bulk: guarantees that the minimum global rate of router is 1% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed".	
Service Name @ QoS Service Control List	Set server name of the service that you want to set it with QoS Control. Router supports up to 20 users set with QoS Service Control. Priority of QoS Service Control is higher than that of both QoS IP control and QoS MAC control.	Null
Protocol @ QoS Service Control List	Select from "TCP", "UDP" and "TCP&UDP".	TCP
Port @ Service Control List	Enter the port number of the service that you want to set it with QoS Control.	Null
Priority @ QoS Service Control List	Select from "Exempt", "Premium", "Express", "Normal" and "Bulk". Select the priority of the service that you want to set it with QoS Control. Exempt: this is the highest priority which guarantees that the minimum global rate of router is 50% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed". Premium: guarantees that the minimum global rate of router is 25% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed". Express: guarantees that the minimum global rate of router is 15% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed". Normal: guarantees that the minimum global rate of router is 10% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed". Bulk: guarantees that the minimum global rate of router is 1% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed".	Exempt
Note: *If services are in the same priority level, router will automatically start Stochastic Fairness Queueing (SFQ) strategy to make a fair bandwidth allocation.*		

3.21 Configuration -> IP Routing

This section allows users to set the IP routing parameters.



Static Route @ IP Routing		
Item	Description	Default
Static Route Table	Allow users to add, delete or modify static route rules manually.	Null
Interface	Select from “WAN”, “LAN_0” or “LAN_1”.	WAN
Destination	Enter the destination host’s IP address or destination network.	Null
Netmask	Enter the Netmask of the destination or destination network.	Null
Gateway	Enter the gateway’s IP address of this static route rule. Router will forward all the data which fit for the destination and Netmask to this gateway.	Null



RIP @ IP Routing		
Item	Description	Default
RIP	RIP (Routing Information Protocol) is a distance-vector routing protocol, which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination.	Null
Enable RIP Protocol	Tick to enable RIP function.	Disable

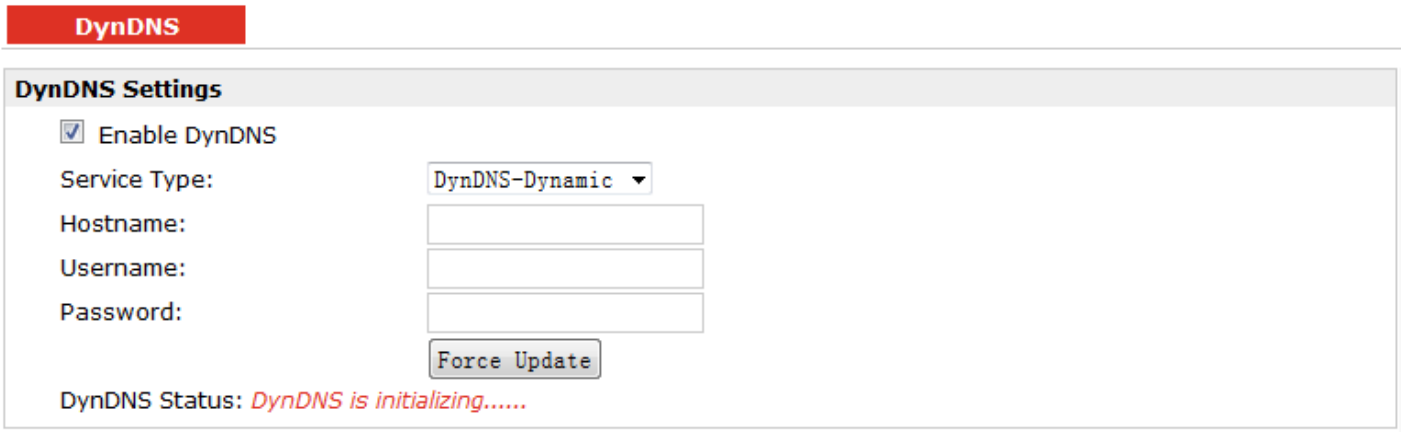
Setting		
RIP Protocol Version	Select from “RIPv1” and “RIPv2”.	RIPv1
Neighbor IP	If you input this neighbor IP, router will only send RIP request massage to this IP instead of broadcast. This item only needs to be set in some unicast network.	0.0.0.0
Update times	Defines the interval between routing updates.	30
Timeout	Defines the route aging time. If no update for a route is received after the aging time elapses, the metric of the route is set to 16 in the routing table.	180
Garbage	Defines the interval from when the metric of a route becomes 16 to when it is deleted from the routing table. During the Garbage-Collect timer length, RIP advertises the route with the routing metric set to 16. If no update is announced for that route after the Garbage-Collect timer expires, the route will be deleted from the routing table.	120
Enable Advance	Tick to enable RIP protocol Advance Setting.	Disable
Default Metric	This value is used for redistributed routes.	1
Distance	The first criterion that a router uses to determine which routing protocol to use if two protocols provide route information for the same destination.	120
Passive	Select from “None”, “Eth0”, “Eth1” and “Default”. This command sets the specified interface to passive mode. On passive mode interface, all receiving packets are processed as normal and Rip info does not send either multicast or unicast RIP packets except to RIP neighbors specified with neighbor command. The default is to be passive on all interfaces.	None
Enable Default Origination	Enable to make router send the default route to the other routers which in the same IGP AS.	Disable
Enable Redistribute Connect	Redistribute connected routes into the RIP tables.	Disable
Enable Redistribute Static	Redistributes routing information from static route entries into the RIP tables.	Disable
Enable Redistribute OSPF	Redistributes routing information from OSPF route entries into the RIP tables.	Disable
Network List	Router will only report the RIP information in this list to its neighbor.	Null
Network Address	Enter the Network address which Eth0 or Eth 1 connects directly.	Null
Netmask	Enter the Network’s Netmask which Eth0 or Eth 1 connects directly.	Null

OSPF @ IP Routing		
Item	Description	Default
OSPF	OSPF (Open Shortest Path First) is a link-state routing protocol for IP networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS).	Null

Enable OSPFv2	Tick to enable OSPF function.	Disable

3.22 Configuration -> DynDNS

This section allows users to set the DynDNS parameters.

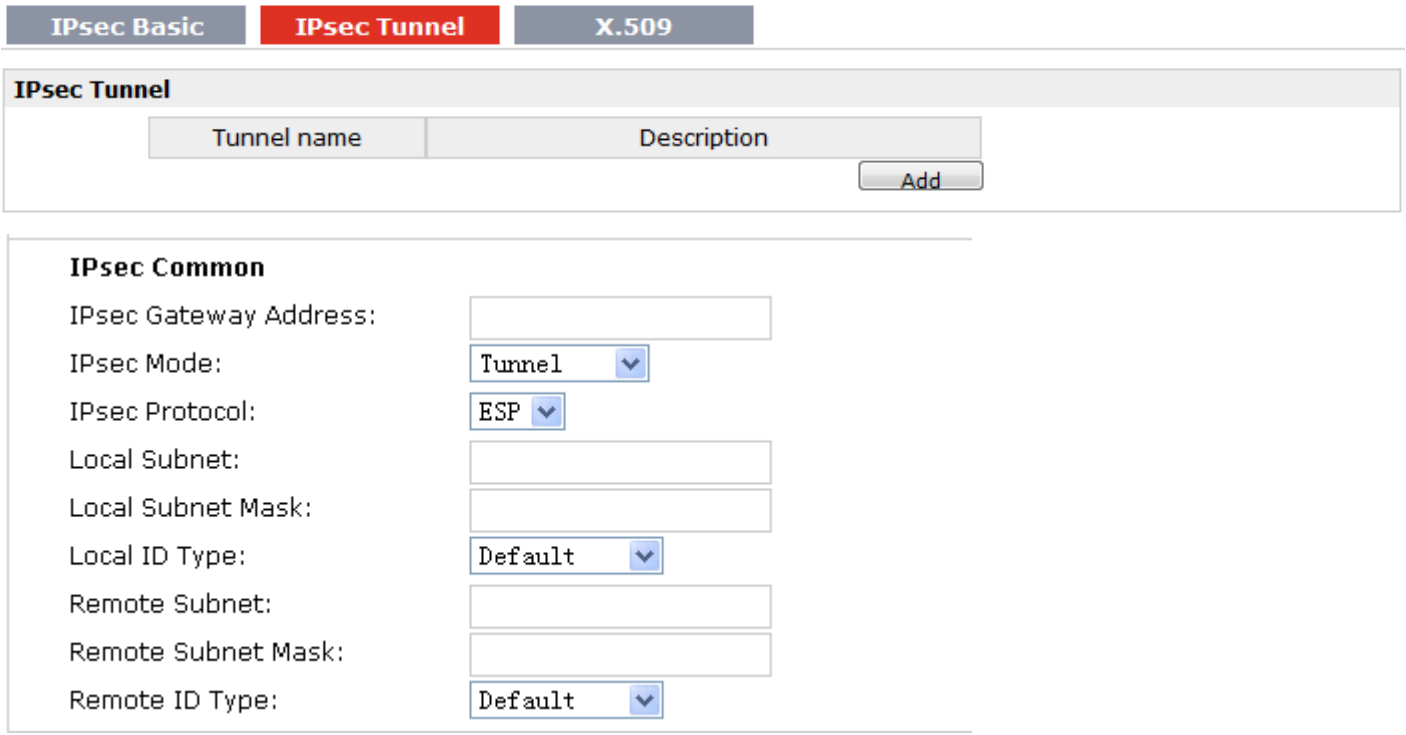


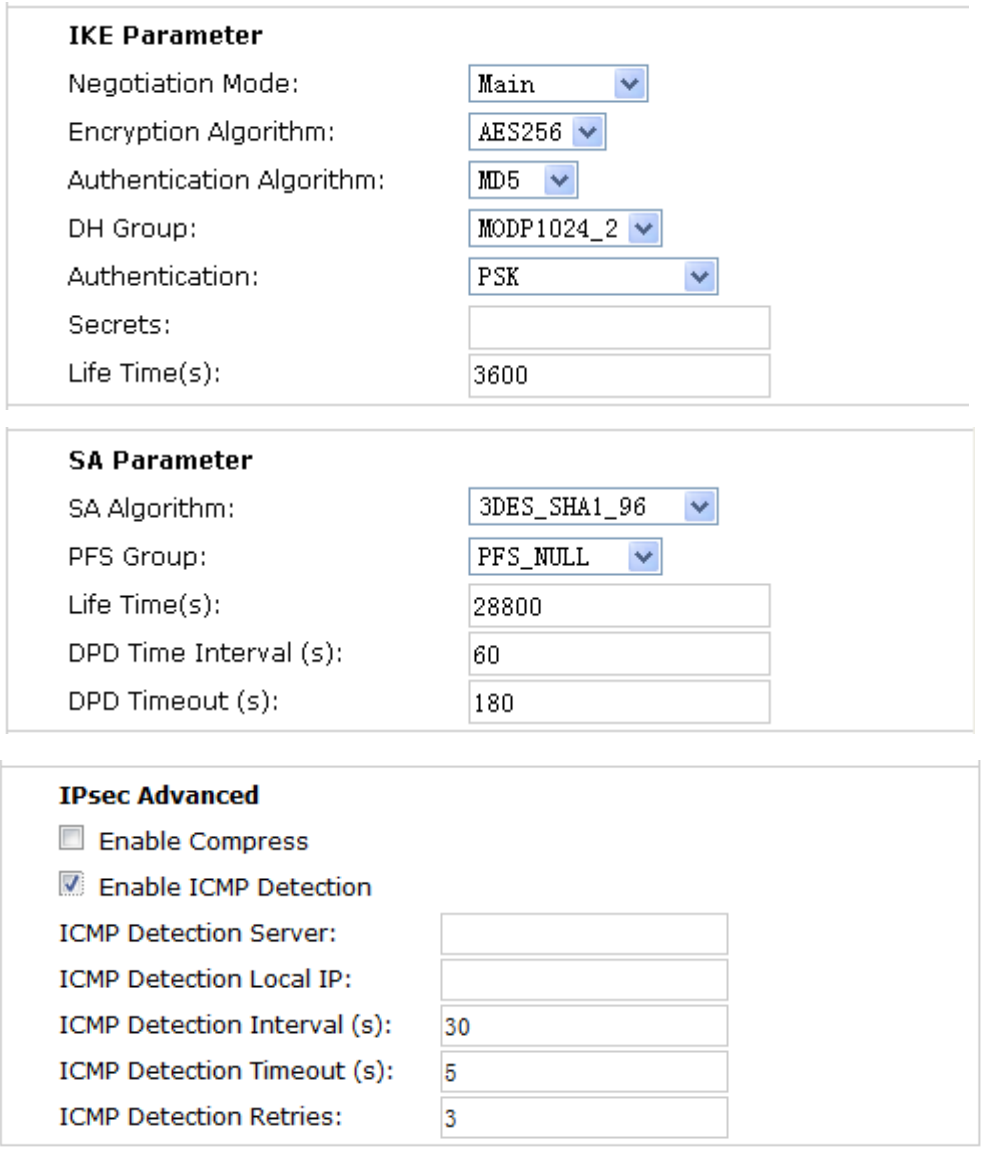
DynDNS		
Item	Description	Default
DynDNS	The Dynamic DNS function allows you to alias a dynamic IP address to a static domain name, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your connection, so that anyone 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.	Null
Enable DynDNS	Tick to enable DynDNS function.	Disable
Service Type	Select the DDNS service from “DynDNS–Dynamic”, “QDNS (3322)” and “NOIP” which you have established an account with. “Custom” could be used for linking custom DDNS server.	DynDNS–Dynamic
hoastmen	Enter the Host name the DDNS server provided.	Null
Username	Enter the user name the DDNS server provided.	Null
Password	Enter the password the DDNS server provided.	Null
URL	Enter the connection address of custom DDNS server.	Null
Force Update	Click to the update and use the DynDNS settings.	Null
DynDNS Status	Show current status of DynDNS	Null

3.23 Configuration -> IPSec

This section allows users to set the IPSec parameters.

IPSec Basic @ IPSec		
Item	Description	Default
Enable NAT Traversal	Tick to enable NAT Traversal for IPSec. This item must be enabled when router under NAT environment.	Enable
Keepalive Interval	The interval that router sends keepalive packets to NAT box so that to avoid it to remove the NAT mapping.	30



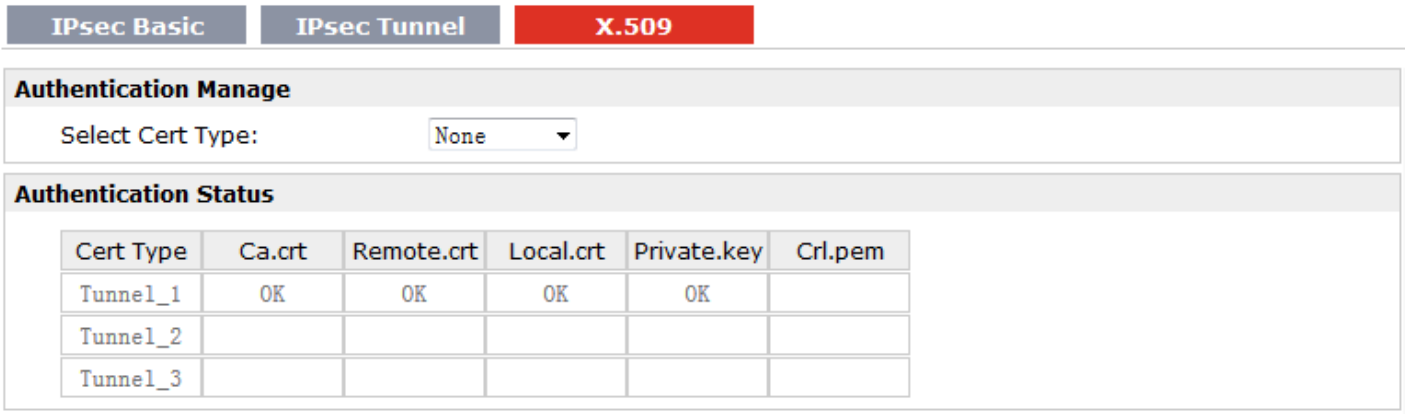


IPSec Tunnel @ IPSec		
Item	Description	Default
Add	Click Add to add new IPSec Tunnel	Null
Enable	Enable IPSec Tunnel, the max tunnel account is 3	Null
IPSec Gateway Address	Enter the address of remote side IPSec VPN server.	Null
IPSec Mode	Select from “Tunnel” and “Transport”. Tunnel: Commonly used 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
IPSec Protocol	Select the security protocols from “ESP” and “AH”.	ESP

	ESP: Uses the ESP protocol. AH: Uses the AH protocol.	
Local Subnet	Enter IPSec Local Protected subnet's address.	0.0.0.0
Local Subnet Mask	Enter IPSec Local Protected subnet's mask.	0.0.0.0
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 is selected, type a name string with an sign "@" for the local security gateway, e.g., test@robustel.com.	Default
Remote Subnet	Enter IPSec Remote Protected subnet's address.	0.0.0.0
Remote Subnet Mask	Enter IPSec Remote Protected subnet's mask.	0.0.0.0
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
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
Encryption Algorithm	Select from "DES", "3DES", "AES128", "AES192" and "AES256"to be used in IKE negotiation. DES: Uses the DES algorithm in CBC mode and 56-bit key. 3DES: Uses the 3DES algorithm in CBC mode and 168-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.	3DES
Authentication Algorithm	Select from "MD5" and "SHA1"to be used in IKE negotiation. MD5: Uses HMAC-SHA1. SHA1: Uses HMAC-MD5.	MD5
DH Group	Select from "MODP768_1", "MODP1024_2" and "MODP1536_5"to be used in key negotiation phase 1. MODP768_1: Uses the 768-bit Diffie-Hellman group. MODP1024_2: Uses the 1024-bit Diffie-Hellman group. MODP1536_5: Uses the 1536-bit Diffie-Hellman group.	MODP1024_2

Authentication	Select from “PSK”, “CA”, “XAUTH Init PSK” and “XAUTH Init CA” to be used in IKE negotiation. PSK: Pre-shared Key. CA: Certification Authority. XAUTH: Extended Authentication to AAA server.	PSK
Secrets	Enter the Pre-shared Key.	Null
Life Time @ IKE Parameter	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
SA Algorithm	Select from “DES_MD5_96”, “DES_SHA1_96”, “3DES_MD5_96”, “3DES_ SHA1_96”, “AES128_MD5_96”, “AES128_ SHA1_96”, “AES192_MD5_96”, “AES192_ SHA1_96”, “AES256_MD5_96” and “AES256_ SHA1_96” when you select “ESP” in “Protocol”; Select from “AH_MD5_96” and “AH_ SHA1_96” when you select “AH” 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_MD5_96
PFS Group	Select from “PFS_NULL”, “MODP768_1”, “MODP1024_2” and “MODP1536_5”. PFS_NULL: Disable PFS Group MODP768_1: Uses the 768-bit Diffie-Hellman group. MODP1024_2: Uses the 1024-bit Diffie-Hellman group. MODP1536_5: Uses the 1536-bit Diffie-Hellman group.	PFS_NULL
Life Time @ SA Parameter	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 Time 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.	180
DPD Timeout	Set the timeout of DPD packets.	60
Enable Compress	Tick to enable compressing the inner headers of IP packets.	Disable
Enable ICMP Detection	Click to enable ICMP detection.	Disable

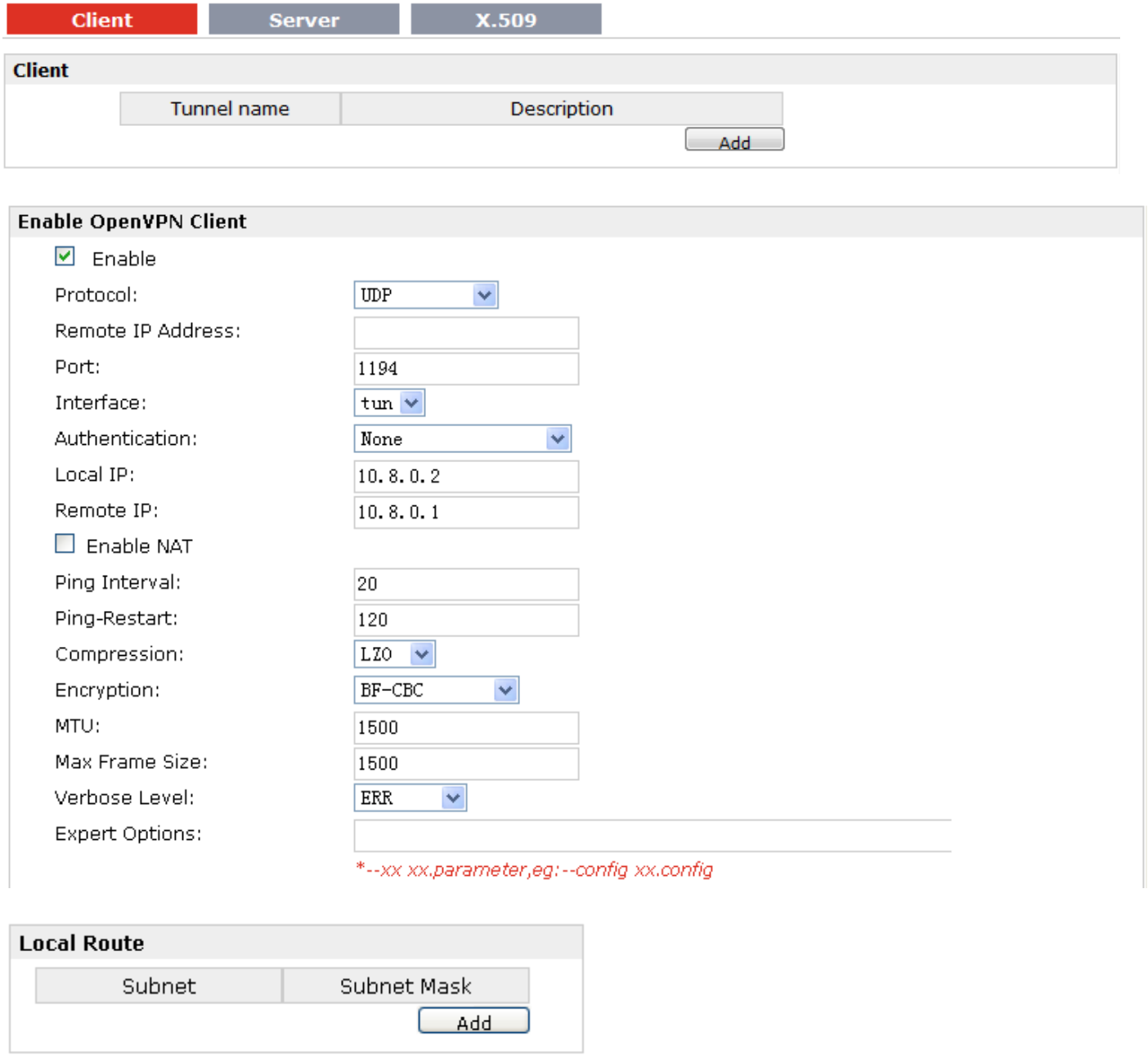
ICMP Detection Server	Enter the IP address or domain name or remote server. Router will ping this address/domain name to check that if the current connectivity is active.	Null
ICMP Detection Local IP	Set the local IP address.	Null
ICMP Detection Interval	Set the ping interval time.	30
ICMP Detection Timeout	Set the ping timeout.	5
ICMP Detection Retries	If Router ping the preset address/domain name time out continuously for Max Retries time, it will try to re-establish the VPN tunnel.	3



X.509 @ IPSec		
Item	Description	Default
Select Cert Type	Select the IPSec tunnel which the certification used for.	Null
CA	Click “Browse” to select the correct CA file from your PC, and then click “Import” to import it to the router. Click “Export” you can export the CA file from router to your PC.	Null
Remote Public Key	Click “Browse” to select the correct Remote Public Key file from your PC, and then click “Import” to import it to the router. Click “Export” you can export the Remote Public Key file from router to your PC.	Null
Local Public Key	Click “Browse” to select the correct Local Public Key file from your PC, and then click “Import” to import it to the router. Click “Export” you can export the Local Public Key file from router to your PC.	Null
Local Private Key	Click “Browse” to select the correct Local Private Key file from your PC, and then click “Import” to import it to the router. Click “Export” you can export the Local Private Key file from router to your PC.	Null
CRL	Click “Browse” to select the correct CRL file from your PC, and then click “Import” to import it to the router. Click “Export” you can export the CRL file from router to your PC.	Null
Authentication Status	Show current status parameters of IPSec.	Null

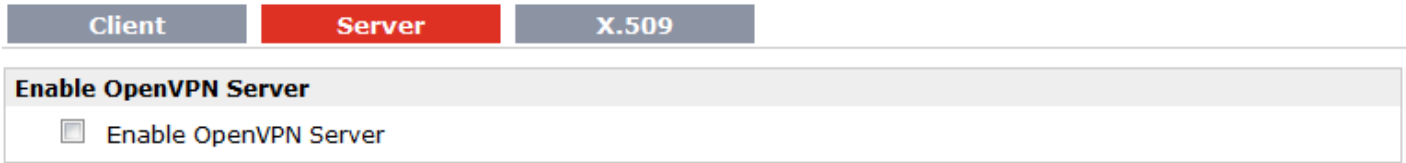
3.24 Configuration -> Open VPN

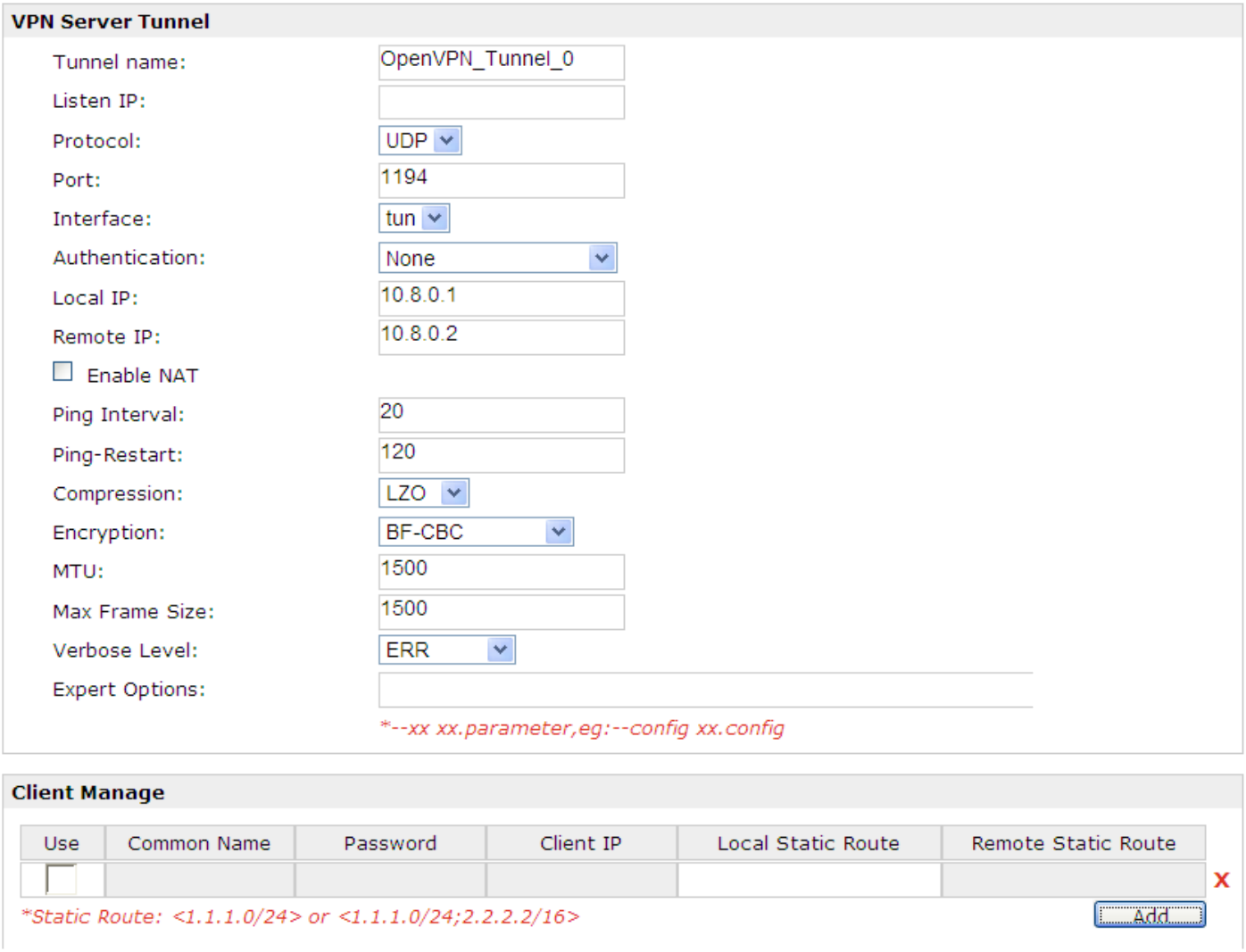
This section allows users to set the Open VPN parameters.



Client @ Open VPN		
Item	Description	Default
Enable	Enable OpenVPN Client, the max tunnel account is 3	Null
Protocol	Select from “UDP” and “TCP Client” which depends on the application.	UDP
Remote IP Address	Enter the remote IP address or domain name of remote side OpenVPN server.	Null
Port	Enter the listening port of remote side OpenVPN server.	1194

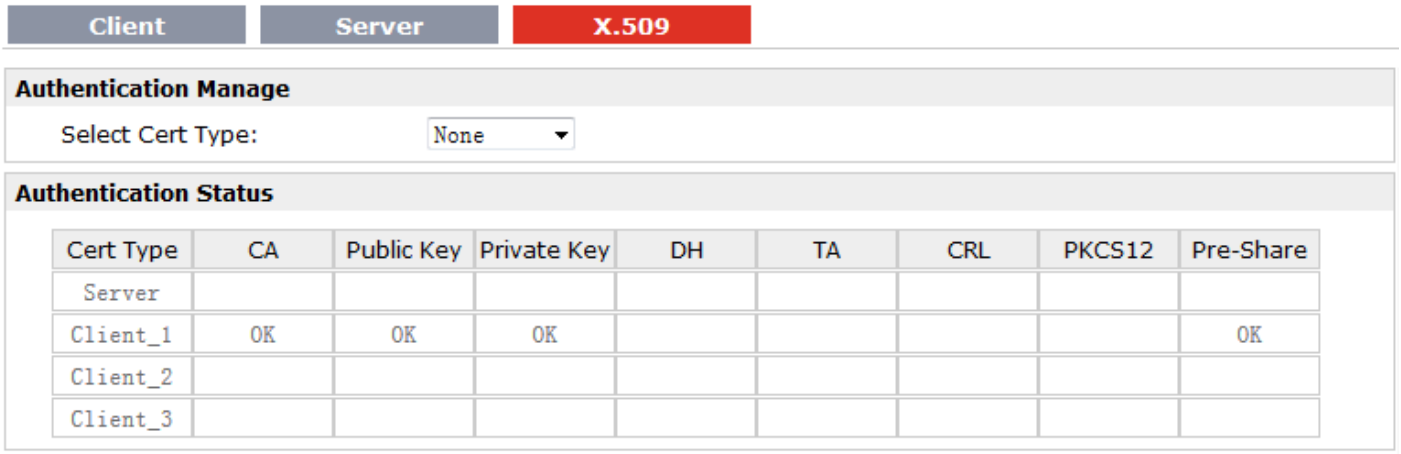
Interface	Select from “tun” and “tap” which are two different kinds of device interface for OpenVPN. The difference between tun and tap device is this: a tun device is a virtual IP point-to-point device and a tap device is a virtual Ethernet device.	tun
Authentication	Select from four different kinds of authentication ways: “Pre-shared”, “Username/Password”, “X.509 cert” and “X.509 cert+user”.	None
Local IP	Define the local IP address of OpenVPN tunnel.	10.8.0.2
Remote IP	Define the remote IP address of OpenVPN tunnel.	10.8.0.1
Enable NAT	Tick to enable SNAT for OpenVPN. The source IP address of host Behind R3000-3P will be disguised before accessing the remote OpenVPN server.	Disable
Ping Interval	Set ping interval to check if the tunnel is active.	20
Ping -Restart	Restart to establish the OpenVPN tunnel if ping always timeout during this time.	120
Compression	Select “LZO” to use the LZO compression library to compress the data stream.	LZO
Encryption	Select from “BF-CBC”, “DES-CBC”, “DES-EDE3-CBC”, “AES128-CBC”, “AES192-CBC” and “AES256-CBC”. BF-CBC: Uses the BF algorithm in CBC mode and 128-bit key. DES-CBC: Uses the DES algorithm in CBC mode and 64-bit key. DES-EDE3-CBC: Uses the 3DES algorithm in CBC mode and 192-bit key. AES128-CBC: Uses the AES algorithm in CBC mode and 128-bit key. AES192-CBC: Uses the AES algorithm in CBC mode and 192-bit key. AES256-CBC: Uses the AES algorithm in CBC mode and 256-bit key.	BF-CBC
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1500
Max Frame Size	Set the Max Frame Size for transmission.	1500
Verbose Level	Select the log output level which from low to high: “ERR”, “WARNING”, “NOTICE” and “DEBUG”. The higher level will output more log information.	ERR
Expert Options	You can enter some other PPP initialization strings in this field. Each string can be separated by a space.	Null
Subnet&Subnet Mask@Local Route	Set the subnet and subnet Mask of local route.	Null





Server @ Open VPN		
Item	Description	Default
Enable OpenVPN Server	Tick to enable OpenVPN server tunnel.	Disable
Tunnel name	Name the OpenVPN server tunnel.	Tunnel_OpenVPN_0
Listen IP	You can enter the IP address of cellular WAN, Ethernet WAN or Ethernet LAN. Null or 0.0.0.0 stands for using the active WAN link currently-cellular WAN or Ethernet WAN.	0.0.0.0
Protocol	Select from “UDP” and “TCP Client” which depends on the application.	UDP
Port	Set the local listening port	1194
Interface	Select from “tun” and “tap” which are two different kinds of device interface for OpenVPN. The difference between a 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	tun

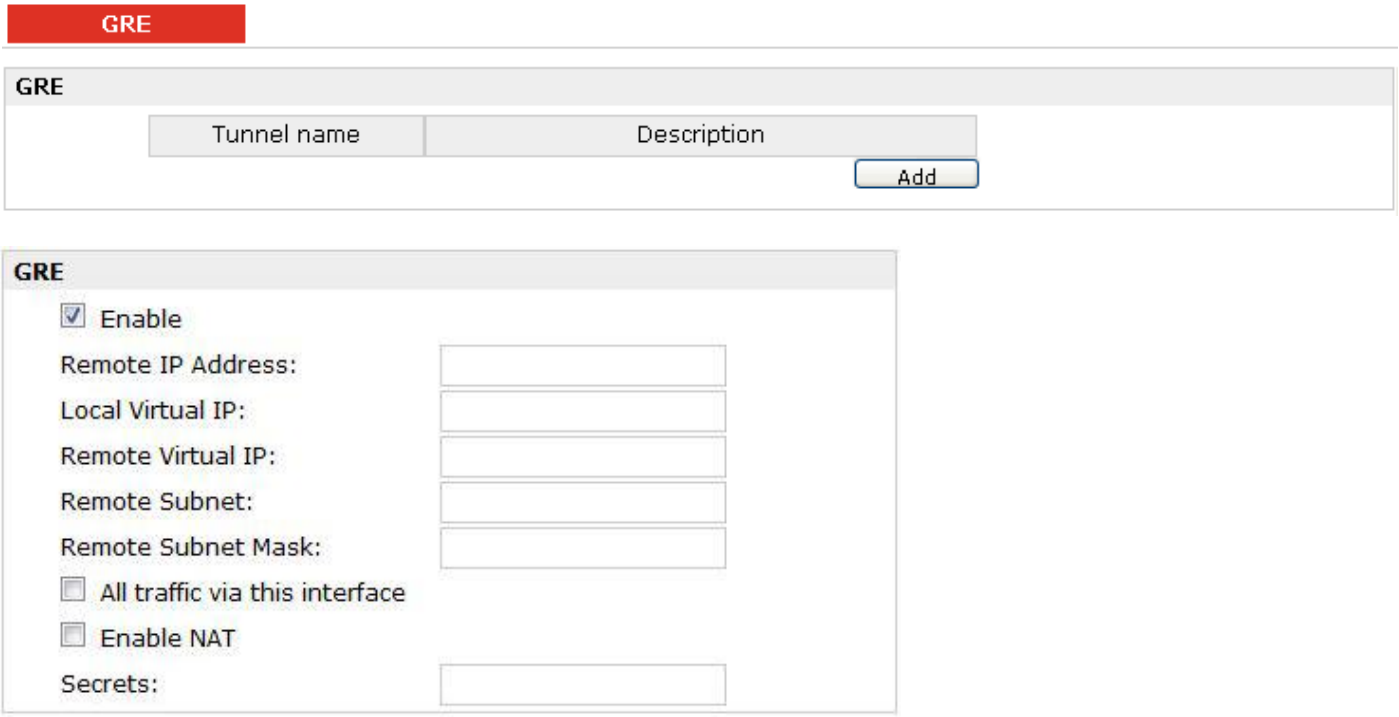
	device.	
Authentication	Select from four different kinds of authentication ways: “Pre-shared”, “Username/Password”, “X.509 cert” and “X.509 cert+user”.	None
Local IP	Define the local IP address of OpenVPN tunnel.	10.8.0.1
Remote IP	Define the remote IP address of OpenVPN tunnel.	10.8.0.2
Enable NAT	Tick to enable SNAT for OpenVPN. The source IP address of host Behind R3000-3P will be disguised before accessing the remote OpenVPN client.	Disable
Ping Interval	Set ping interval to check if the tunnel is active.	20
Ping -Restart	Restart to establish the OpenVPN tunnel if ping always timeout during this time.	120
Compression	Select from “None”and”LZO”, Select “LZO” to use the LZO compression library to compress the data stream.	LZO
Encryption	Select from “BF-CBC”, “DES-CBC”, “DES-EDE3-CBC”, “AES128-CBC”, “AES192-CBC” and “AES256-CBC”. BF-CBC: Uses the BF algorithm in CBC mode and 128-bit key. DES-CBC: Uses the DES algorithm in CBC mode and 64-bit key. DES-EDE3-CBC: Uses the 3DES algorithm in CBC mode and 192-bit key. AES128-CBC: Uses the AES algorithm in CBC mode and 128-bit key. AES192-CBC: Uses the AES algorithm in CBC mode and 192-bit key. AES256-CBC: Uses the AES algorithm in CBC mode and 256-bit key.	BF-CBC
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1500
Max Frame Size	Set the Max Frame Size for transmission.	1500
Verbose Level	Select the log output level which from low to high: “ERR”, “WARNING”, “NOTICE” and “DEBUG”. The higher level will output more log information.	ERR
Expert Options	You can enter some other PPP initialization strings in this field. Each string can be separated by a space.	Null
Client Manage	Click “Add” to add a OpenVPN client info which include “Common Name”, “Password”, “Client IP”, “Local Static Route” and “Remote Static Route”. This field only can be configured when you select “Username/Password” in “Authentication”.	Null



X.509 @ Open VPN		
Item	Description	Default
Select Cert Type	Select the OpenVPN client or server which the certification used for.	Null
CA	Click “Browse” to select the correct CA file from your PC, and then click “Import” to import it to the router. Click “Export” you can export the CA file from router to your PC.	Null
Public Key	Click “Browse” to select the correct Public Key file from your PC, and then click “Import” to import it to the router. Click “Export” you can export the Public Key A file from router to your PC.	Null
Private Key	Click “Browse” to select the correct Private Key file from your PC, and then click “Import” to import it to the router. Click “Export” you can export the Private Key file from router to your PC.	Null
DH	Click “Browse” to select the correct DH A file from your PC, and then click “Import” to import it to the router. Click “Export” you can export the DH file from router to your PC.	Null
TA	Click “Browse” to select the correct TA file from your PC, and then click “Import” to import it to the router. Click “Export” you can export the TA file from router to your PC.	Null
CRL	Click “Browse” to select the correct CRL file from your PC, and then click “Import” to import it to the router. Click “Export” you can export the CRL file from router to your PC.	Null
Pre-Share Static Key	Click “Browse” to select the correct Pre-Share Static Key file from your PC, and then click “Import” to import it to the router. Click “Export” you can export the Pre-Share Static Key file from router to your PC.	Null

3.25 Configuration -> GRE

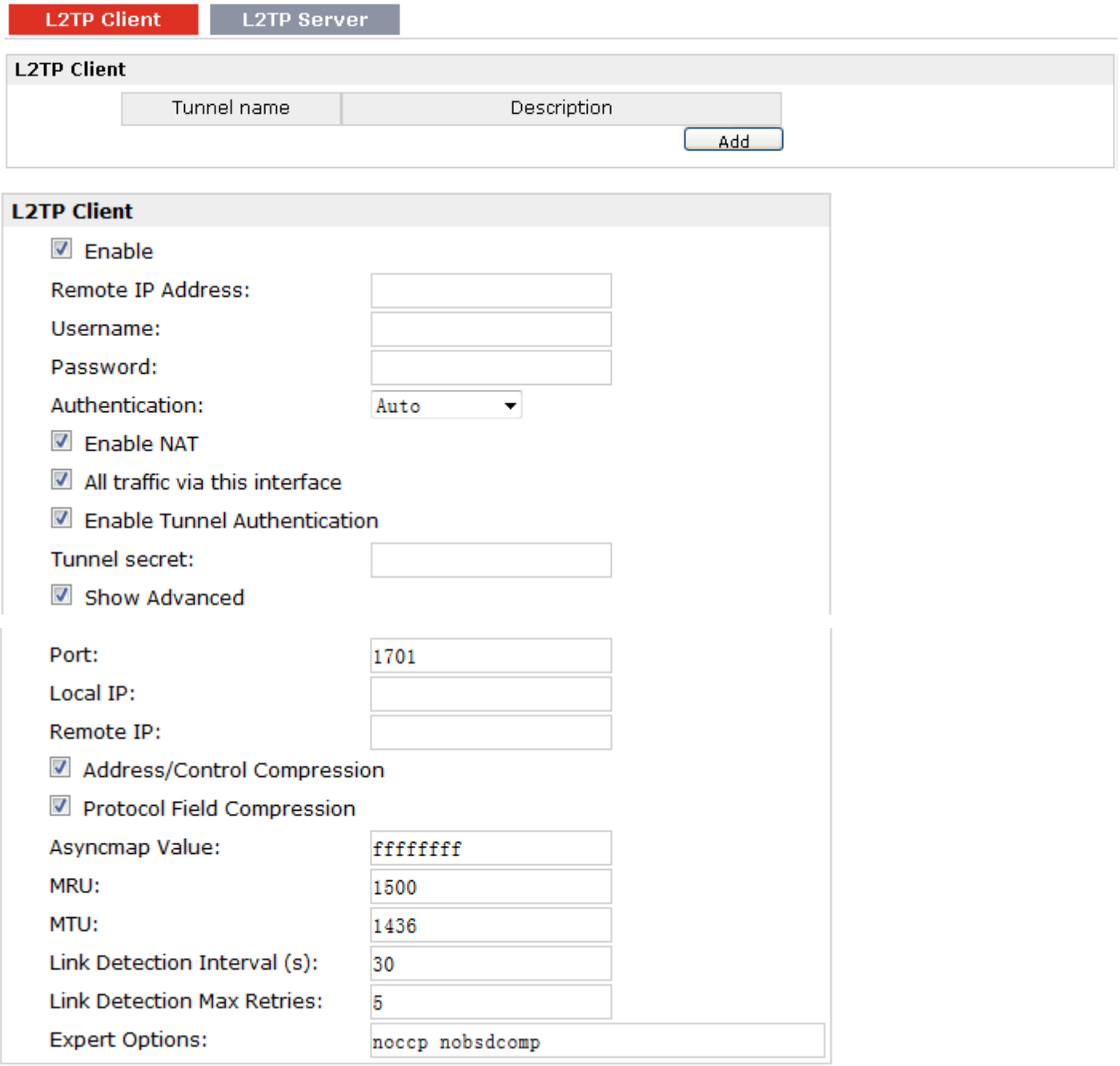
This section allows users to set the GRE parameters.



GRE		
Item	Description	Default
Add	Click “Add” to add a GRE tunnel.	
Enable	Click to enable GRE (Generic Routing Encapsulation). GRE is a protocol that encapsulates packets in order to route other protocols over IP networks.	Disable
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
Remote Subnet	Add a static route to the remote side’s subnet so that the remote network is known to the local network.	Null
Remote Subnet Mask	Set remote subnet net mask.	Null
All traffic via this interface	After click to enable this feature, all data traffic will be sent via L2TP tunnel.	Disable
Enable NAT	Tick to enable SNAT for GRE. The source IP address of host Behind R3000-3P will be disguised before accessing the remote GRE server.	Disable
Secrets	Set Tunnel Key of GRE.	Null

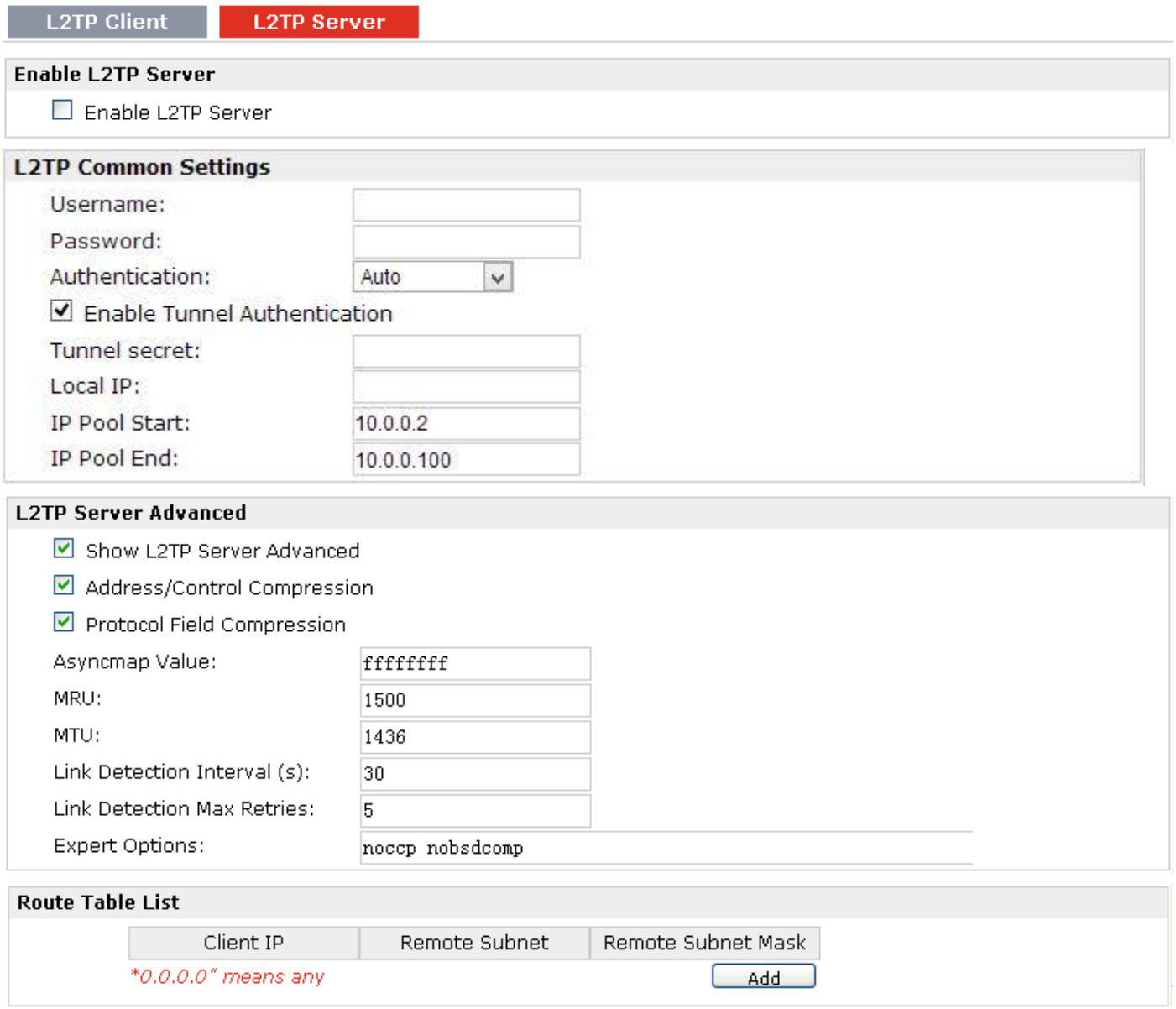
3.26 Configuration -> L2TP

This section allows users to set the L2TP parameters.



L2TP Client @ L2TP		
Item	Description	Default
Add	Click “Add” to add a L2TP client. You can add at most 3 L2TP clients.	Null
Remote IP Address	Enter your L2TP server’s public IP or domain name.	Null
Username	Enter the username which was provided by your L2TP server.	Null
Password	Enter the password which was provided by your L2TP server.	Null
Authentication	Select from “Auto”, “PAP”, “CHAP”, “MS-CHAP v1” and “MS-CHAP v2”. You need to select the corresponding authentication method based on the	Disable

	server's authentication method. When you select "Auto", router will auto select the correct method based on server.	
Remote Subnet	Enter L2TP remote Protected subnet's address.	Null
Remote Subnet Mask	Enter L2TPremote Protected subnet's mask.	Null
Enable NAT	Click to enable NAT feature of L2TP. The source IP address of host Behind R3000-3P will be disguised before accessing the remote L2TP server.	Disable
All traffic via this interface	After click to enable this feature, all data traffic will be sent via L2TP tunnel.	Disable
Enable Tunnel Authentication	Tick to enable tunnel authentication and enter the tunnel secret which provided by L2TP server.	Disable
Tunnel Secret	Enter L2TP tunnel secret in this item.	Null
Show Advanced	Tick to enable the L2TP client advanced setting.	Disable
Port	Set the Port number of the L2TP client.	Null
Local IP	Set the IP address of the L2TP client. You can enter the IP which assigned by L2TP server. Null means L2TP client will obtain an IP address automatically from L2TP server's IP pool.	Null
Remote IP	Enter the remote peer's private IP address or remote subnet's gateways address.	Null
Address/Control Compression	Used for PPP initialization. In general, you need to enable it as default.	Enable
Protocol Field Compression	Used for PPP initialization. In general, you need to enable it as default.	Enable
Asyncmap Value	One of the L2TP initialization strings. In general, you don't need to modify this value.	ffffffff
MRU	Maximum Receiving Unit. It is the identifier of the maximum size of packet, which is possible to receive in a given environment.	1500
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1436
Link Detection Interval	Specify the interval between L2TP client and server. To check the connectivity of a tunnel, the client and server regularly send PPP Echo to each other. If the client or server receives no response from the peer within a specified period of time, it retransmits the PPP echo. If it receives no response from the peer after transmitting the PPP echo for max retries times, it considers that the L2TP tunnel is down and tries tore-establish a tunnel with the peer.	30
Link Detection Max Retries	Specify the max retries times for L2TP link detection.	5
Expert Options	You can enter some other PPP initialization strings in this field. Each string can be separated by a space.	noccp nobsdcomp

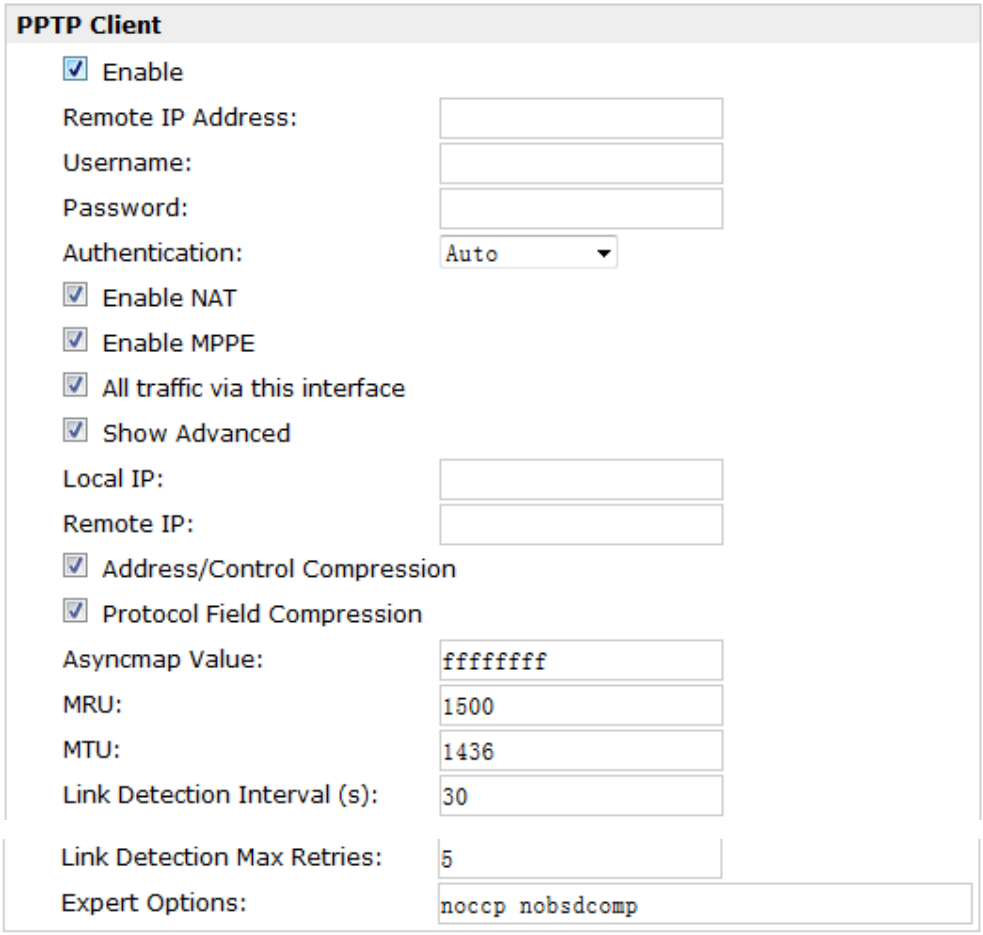


L2TP Server @ L2TP		
Item	Description	Default
Enable L2TP Server	Tick to enable L2TP server.	Disable
Username	Set the username which will assign to L2TP client.	Null
Password	Set the password which will assign to L2TP client.	Null
Authentication	Select from “PAP”, “CHAP”, “MS-CHAP v1” and “MS-CHAP v2”. L2TP client need to select the same authentication method based on this server’s authentication method.	CHAP
Enable Tunnel Authentication	Tick to enable tunnel authentication and enter the tunnel secret which will provide to L2TP client.	Disable
Local IP	Set the IP address of L2TP server.	10.0.0.1
IP Pool Start	Set the IP pool start IP address which will assign to the L2TP clients.	10.0.0.2
IP Pool End	Set the IP pool end IP address which will assign to the L2TP clients.	10.0.0.100

Show L2TP Server Advanced	Tick to show the L2TP server advanced setting.	Disable
Address/Control Compression	Used for PPP initialization. In general, you need to enable it as default.	Enable
Protocol Field Compression	Used for PPP initialization. In general, you need to enable it as default.	Enable
Asyncmap Value	One of the L2TP initialization strings. In general, you don't need to modify this value.	ffffffff
MRU	Maximum Receiving Unit. It is the identifier of the maximum size of packet, which is possible to receive in a given environment.	1500
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1436
Link Detection Interval	Specify the interval between L2TP client and server. To check the connectivity of a tunnel, the client and server regularly send PPP Echo to each other. If the client or server receives no response from the peer within a specified period of time, it retransmits the PPP echo. If it receives no response from the peer after transmitting the PPP echo for max retries times, it considers that the L2TP tunnel is down and tries tore-establish a tunnel with the peer.	30
Link Detection Max Retries	Specify the max retries times for L2TP link detection.	5
Expert Options	You can enter some other PPP initialization strings in this field. Each string can be separated by a space.	noccp nobsdcomp
Route Table List	Click "Add" to add a route rule from L2TP server to L2TP client.	Null

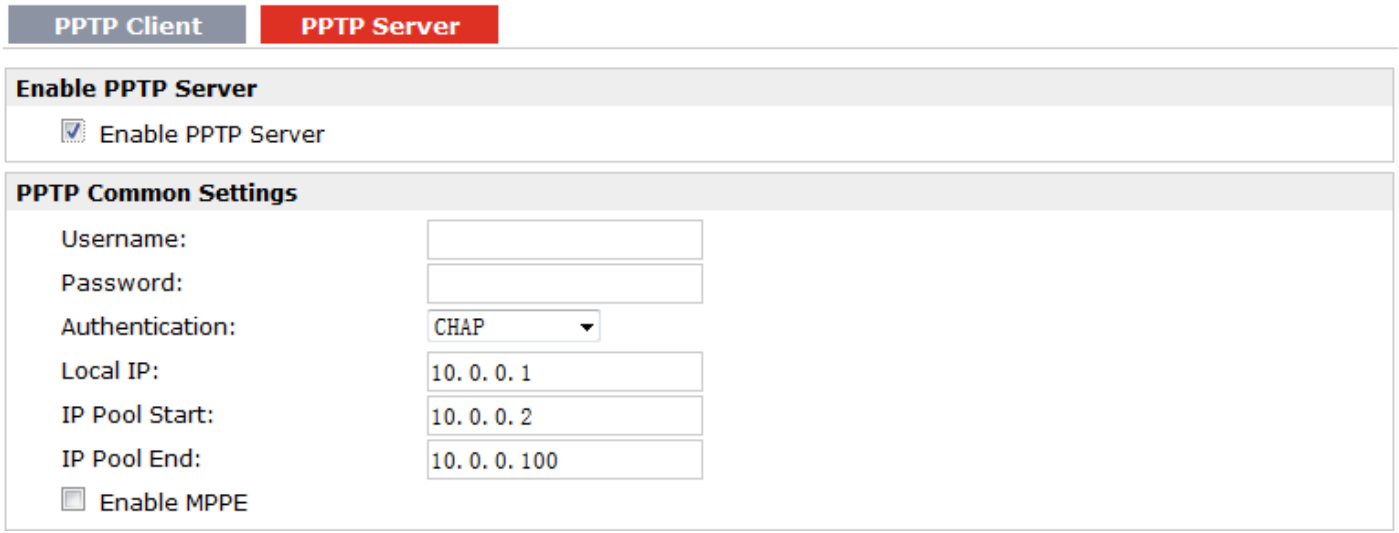
3.27 Configuration -> PPTP

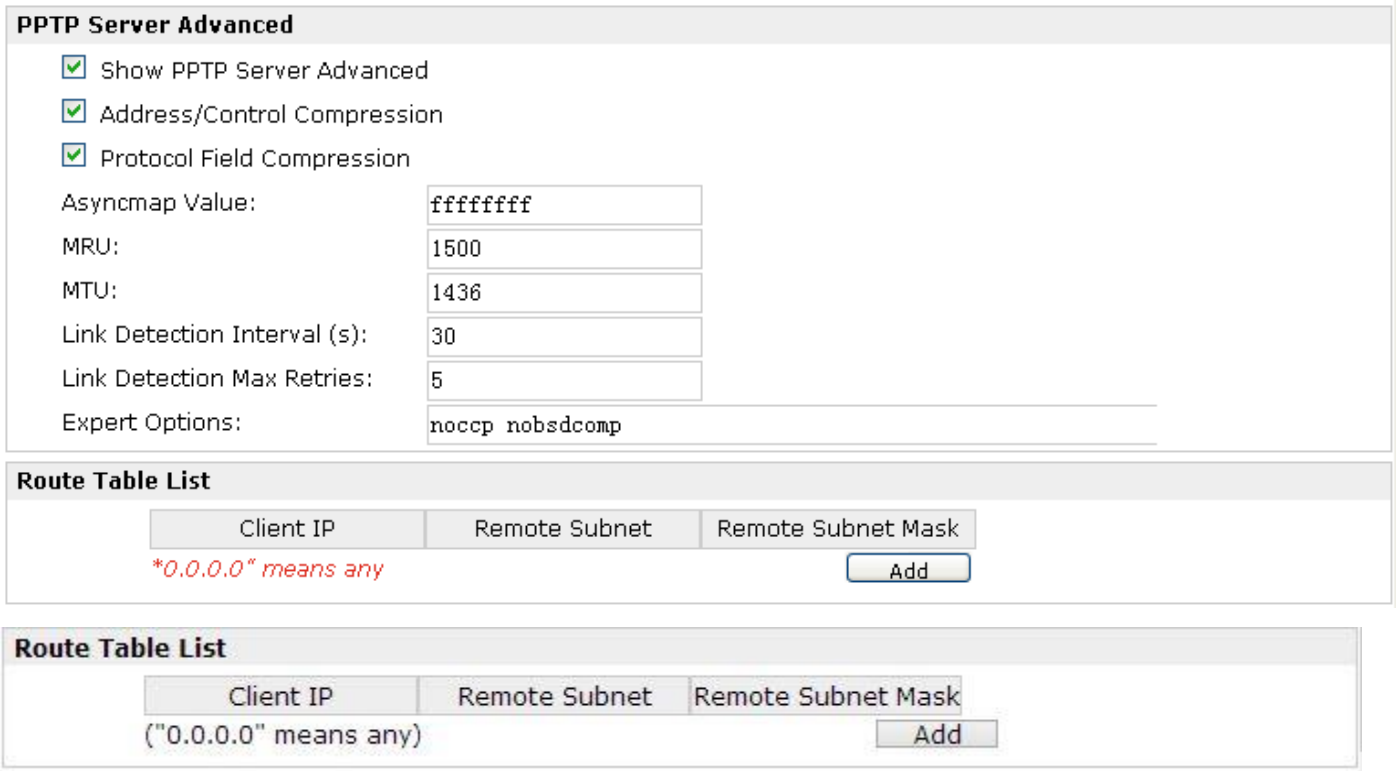
This section allows users to set the PPTP parameters.



PPTP Client @ PPTP		
Item	Description	Default
Add	Click “Add” to add a PPTP client	
Enable	Enable PPTP Client. The max tunnel accounts are 3.	Null
Disable	Disable PPTP Client.	Null
Remote IP Address	Enter your PPTP server’s public IP or domain name.	Null
Username	Enter the username which was provided by your PPTP server.	Null
Password	Enter the password which was provided by your PPTP server.	Null
Authentication	Select from “Auto”, “PAP”, “CHAP”, “MS-CHAP v1” and “MS-CHAP v2”. You need to select the corresponding authentication method based on the server’s authentication method. When you select “Auto”, router will auto select the correct method based on server’s method.	Auto
Enable NAT	Click to enable NAT feature of PPTP. The source IP address of host Behind R3000-3P will be disguised before accessing the remote PPTP server.	Disable
Enable MPPE	Tick to enable MPPE (Microsoft Point-to-Point Encryption). It’s a protocol for encrypting data across PPP and VPN links.	Disable
All traffic via this interface	After click to enable this feature, all data traffic will be sent via PPTP tunnel.	Disable
Show Advanced	Tick to enable the PPTP client advanced setting.	Disable

Local IP	Set the IP address of the PPTP client. You can enter the IP which assigned by PPTP server. Null means PPTP client will obtain an IP address automatically from PPTP server's IP pool.	Null
Remote IP	Enter the remote peer's private IP address or remote subnet's gateways address.	Null
Address/Control Compression	Used for PPP initialization. In general, you need to enable it as default.	Enable
Protocol Field Compression	Used for PPP initialization. In general, you need to enable it as default.	Enable
Asyncmap Value	One of the PPTP initialization strings. In general, you don't need to modify this value.	ffffffff
MRU	Maximum Receiving Unit. It is the identifier of the maximum size of packet, which is possible to receive in a given environment.	1500
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1436
Link Detection Interval	Specify the interval between PPTP client and server. To check the connectivity of a tunnel, the client and server regularly send PPP Echo to each other. If the client or server receives no response from the peer within a specified period of time, it retransmits the PPP echo. If it receives no response from the peer after transmitting the PPP echo for max retries times, it considers that the PPTP tunnel is down and tries tore-establish a tunnel with the peer.	30
Link Detection Max Retries	Specify the max retries times for PPTP link detection.	5
Expert Options	You can enter some other PPP initialization strings in this field. Each string can be separated by a space.	noccp nobsdcomp



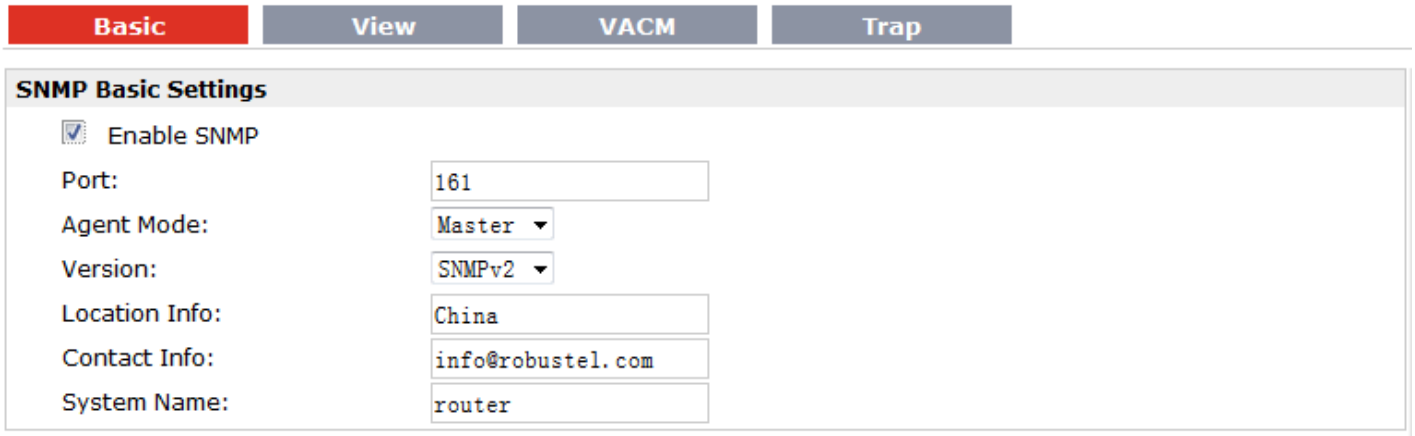


PPTP Server @ PPTP		
Item	Description	Default
Enable PPTP Server	Tick to enable PPTP server.	Disable
Username	Set the username which will assign to PPTP client.	Null
Password	Set the password which will assign to PPTP client.	Null
Authentication	Select from “PAP”, “CHAP”, “MS-CHAP v1” and “MS-CHAP v2”. PPTP client need to select the same authentication method based on this server’s authentication method.	CHAP
Local IP	Set the IP address of PPTP server.	10.0.0.1
IP Pool Start	Set the IP pool start IP address which will assign to the PPTP clients.	10.0.0.2
IP Pool End	Set the IP pool end IP address which will assign to the PPTP clients.	10.0.0.100
Enable MPPE	Tick to enable MPPE (Microsoft Point-to-Point Encryption). It’s a protocol for encrypting data across PPP and VPN links.	Disable
Show PPTP Server Advanced	Tick to show the PPTP server advanced setting.	Disable
Address/Control Compression	Used for PPP initialization. In general, you need to enable it as default.	Enable
Protocol Field Compression	Used for PPP initialization. In general, you need to enable it as default.	Enable
Asyncmap Value	One of the PPTP initialization strings. In general, you don’t need to modify this value.	ffffffff
MRU	Maximum Receiving Unit. It is the identifier of the maximum size of packet, which is possible to receive in a given environment.	1500

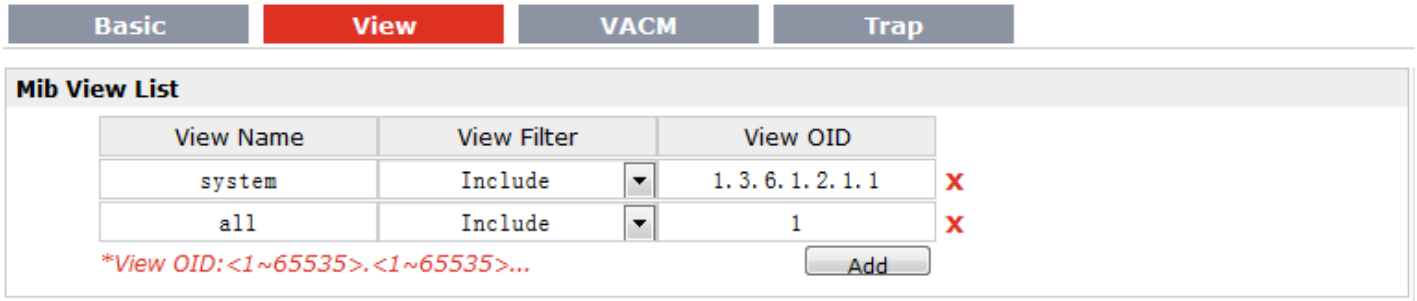
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1436
Link Detection Interval	Specify the interval between PPTP client and server. To check the connectivity of a tunnel, the client and server regularly send PPP Echo to each other. If the client or server receives no response from the peer within a specified period of time, it retransmits the PPP echo. If it receives no response from the peer after transmitting the PPP echo for max retries times, it considers that the PPTP tunnel is down and tries tore-establish a tunnel with the peer.	30
Link Detection Max Retries	Specify the max retries times for PPTP link detection.	5
Expert Options	You can enter some other PPP initialization strings in this field. Each string can be separated by a space.	noccp nobsdcomp
Route Table List	Click “Add” to add a route rule from PPTP server to PPTP client.	Null

3.28 Configuration -> SNMP

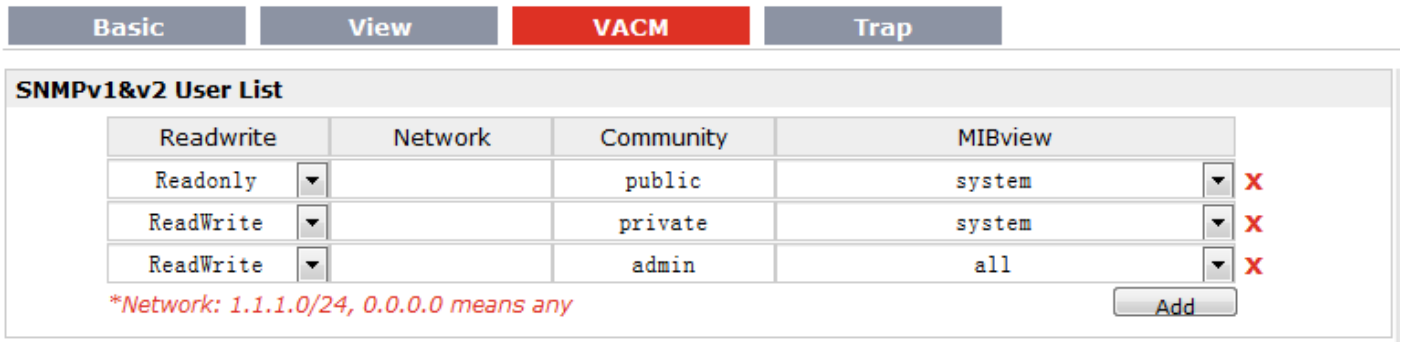
This section allows users to set the SNMP parameters.



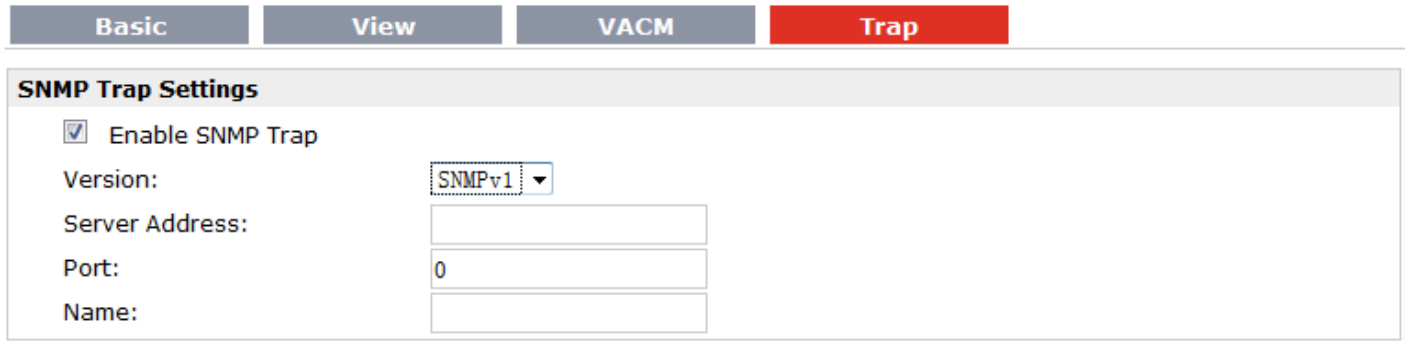
Basic @ SNMP		
Item	Description	Default
Port	UDP port for sending and receiving SNMP requests.	161
Agent Mode	Select the correct agent mode.	Master
Version	Select from “SNMPv1”, “SNMPv2” and “SNMPv3”.	SNMPv2
Location Info	Enter the router’s location info which will send to SNMP client.	China
Contact Info	Enter the router’s contact info which will send to SNMP client.	info@robustel.com
System name	Enter the router’s system name which will send to SNMP client.	router



View @ SNMP		
Item	Description	Default
View Name	Enter the View Name	Null
View Filter	Select from “Include” and “Exclude”.	Include
View OID	Enter the Object Identifiers (OID)	Null



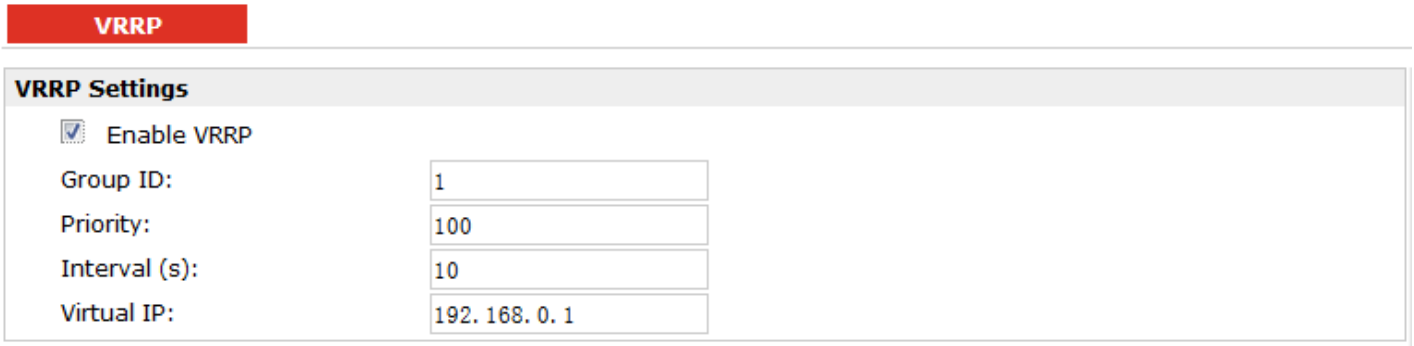
VACM @ SNMP		
Item	Description	Default
Readwrite	Select the access rights from “Readonly” and “ReadWrite”.	Readonly
Network	Define the network from which is allowed to access. E.g. 172.16.0.0.	Null
Community	Enter the community name.	Null
MIBview	Select from “none”, “system” and “all”	none



Trap @ SNMP		
Item	Description	Default
Enable SNMP Trap	Click to enable SNMP Trap feature.	Disable
Version	Select from “SNMPv1”, “SNMPv2” and “SNMPv3”.	SNMPv1
Server Address	Enter SNMP server’s IP address.	Null
Port	Enter SNMP server’s port number	0
Name	Enter SNMP server’s name.	Null

3.29 Configuration -> VRRP

This section allows users to set the VRRP parameters.

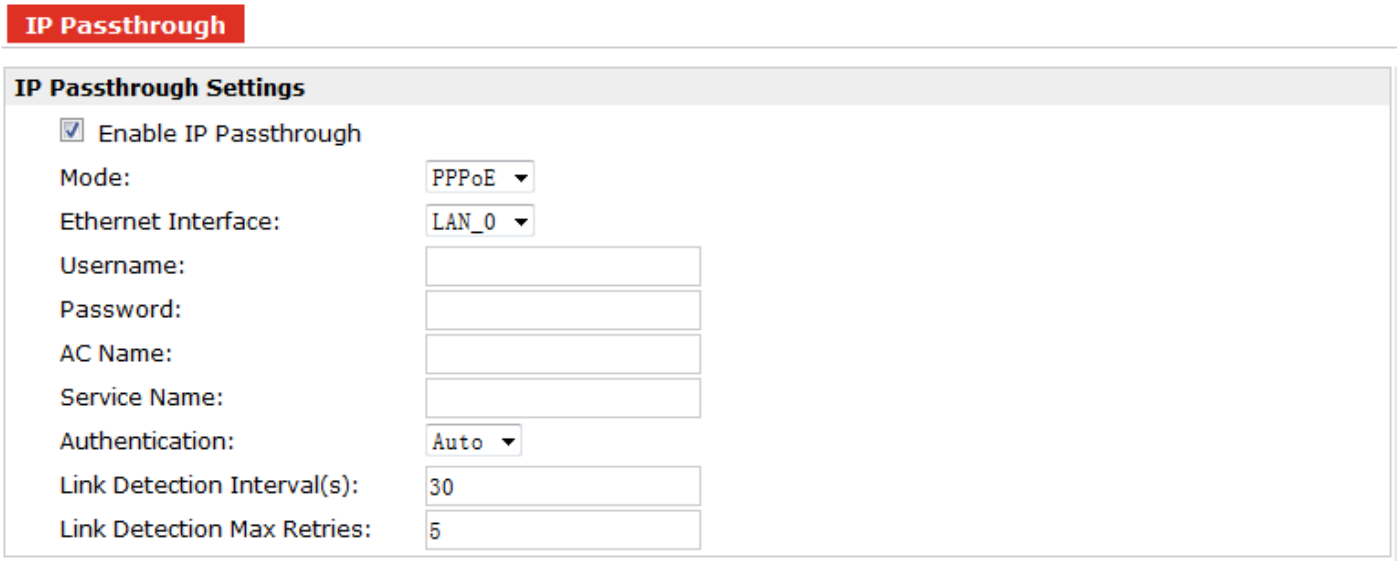


VRRP		
Item	Description	Default
Enable VRRP	Tick to enable VRRP protocol. VRRP (Virtual Router Redundancy Protocol) is an Internet protocol that provides a way to have one or more backup routers when using a statically configured router on a local area network (LAN).Using VRRP, a virtual IP address can be specified manually.	Disable
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.	100
Interval	The interval that master router sends keepalive packets to backup routers.	10
Virtual IP	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

3.30 Configuration -> IP Passthrough

In IP Passthrough mode, R3000-3P acts as PPPoE server, it will pass its WAN IP address to PPPoE client directly. Packets received from the WAN interface are delivered directly to the LAN interface. Similarly, packets received for the LAN interface (everything except broadcasts/multicasts) are sent to the WAN interface.

This section allows users to set the IP Pass through parameters.

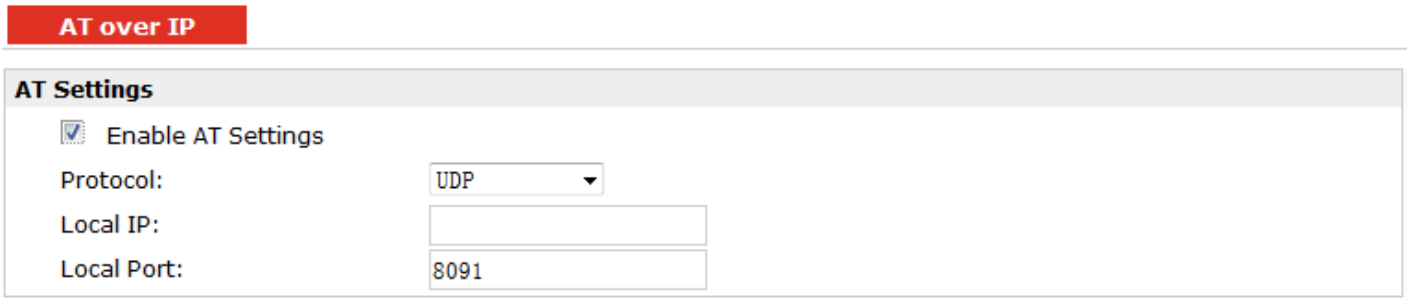


IP Passthrough		
Item	Description	Default
Enable IP Passthrough	Tick to enable IP Passthrough feature. ***Note**: Firstly you need to select "Cellular" as "Primary Interface" in tab "Configuration"-> "Link Management".*	Disable
Mode	User can only select "PPPoE" mode at present.	PPPoE
Ethernet Interface	Set the LAN interface from "LAN_0", "LAN_1". PPPoE client dials up to R3000-3P (PPPoE server) corresponding to different LAN interface. For example when you select "LAN_0" and connect PPPoE client (such as PC) to LAN 0 through Ethernet cable, PC will dial up to R3000-3P (PPPoE server) through LAN 0. ***Note**: It doesn't matter whether you select "LAN_0" or "LAN_1" If you click to enable "Enable Bridge" in tab "Configuration" -> "Ethernet" -> "LAN Interface".*	LAN_0
Username	Set the username of PPPoE server.	Null
Password	Set the password of PPPoE server.	Null
AC Name	Set the AC (Access Concentrator) name of PPPoE server.	Null
Service Name	Set the service name of PPPoE server. ***Note**: PPPoE client needs to set the same username, password, AC name, service name of PPPoE server, or it cannot succeed to dial up to PPPoE server.*	Null
Authentication	Set the different PPP authentication from "Auto", "PAP", "CHAP". Auto: Automatic detection. PAP: Password Authentication Protocol CHAP: Challenge Response Protocol	Auto
Link Detection Interval(s)	When PPPoE client dial up to R3000-3P (PPPoE server), R3000-3P will send "LCP Echo Request" to PPPoE client after this interval. "Link Detection Interval" ranges from 3 to 30 times.	30
Link Detection Max	If R3000-3P re-sends "LCP Echo Request" packet continuously for Max Retries	5

Retries	times and still do not receive correct respond packets from PPPoE client, it will send “LCP Terminal Request” packet to disconnect the connection between PPPoE server and PPPoE client. “Max Retries” ranges from 3 to 5 times.	

3.31 Configuration -> AT over IP

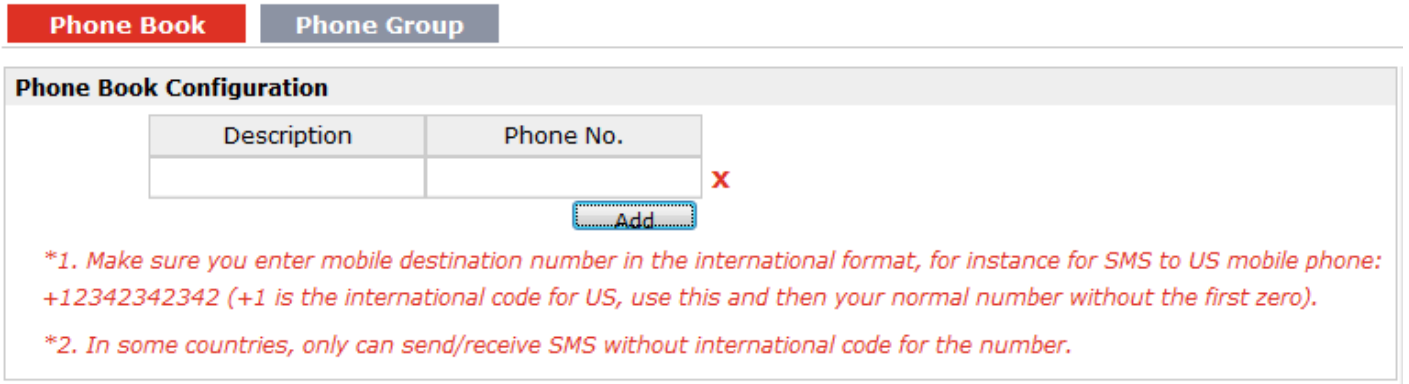
This section allows users to set the AT over IP parameters.



AT over IP		
Item	Description	Default
Enable AT Settings	Tick to enable AT over IP to control cellular module via AT command remotely.	Disable
Protocol	Select from “TCP server” or “UDP”	UDP
Local IP	You can enter the IP address of cellular WAN, Ethernet WAN or Ethernet LAN. Null stands for all these three IP addresses.	0.0.0.0
Local Port	Enter the local TCP or UDP listening port.	8091

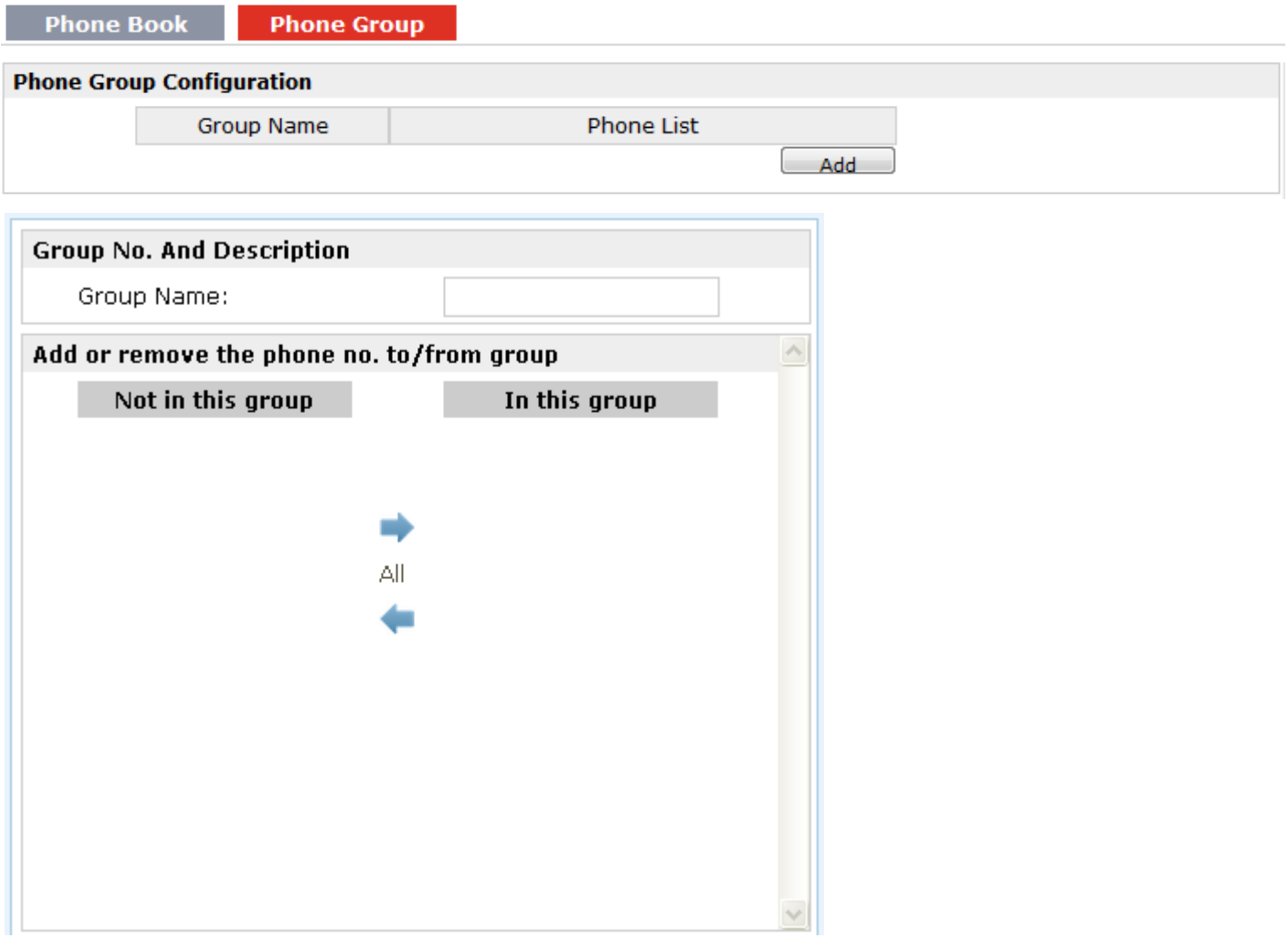
3.32 Configuration -> Phone Book

This section allows users to set the Phone Book parameters.



Phone Book		
Item	Description	Default

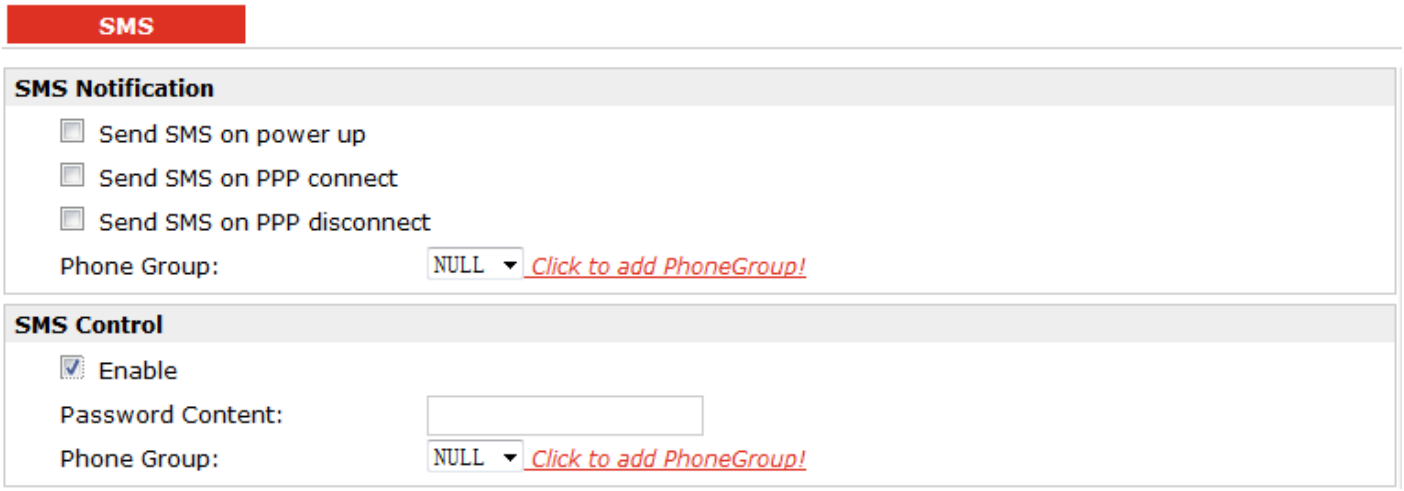
Description	Set the name to your relevant phone No.	Null
Phone No.	Enter your phone No. ***Note:*** *In some countries, the **Phone NO.** is required to be written in international format, starting with "**+**" followed by the country code.*	Null



Phone Group		
Group Name	Set the Group Name.	Null
Phone List	Show the phone list in the Group.	Null
Add or remove the phone no.to/from group	Click right arrow to add the phone no.to this group; Click left arrow to remove the phone no.from group.	Null

3.33 Configuration -> SMS

This section allows users to set the SMS Notification and SMS Control parameters.

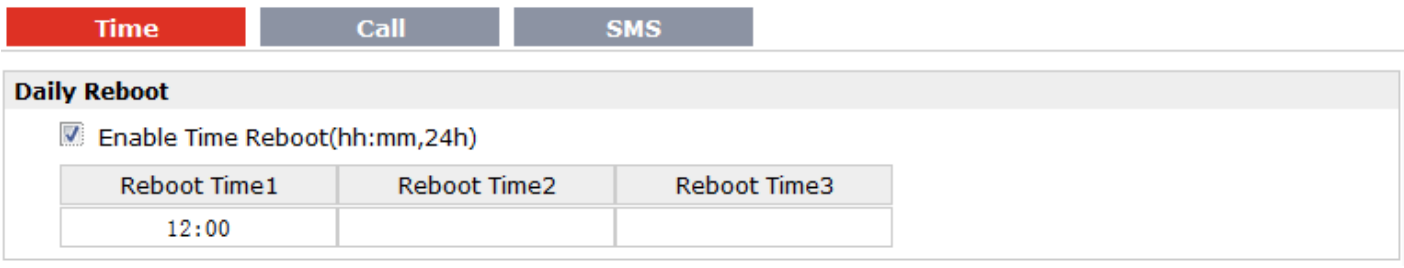


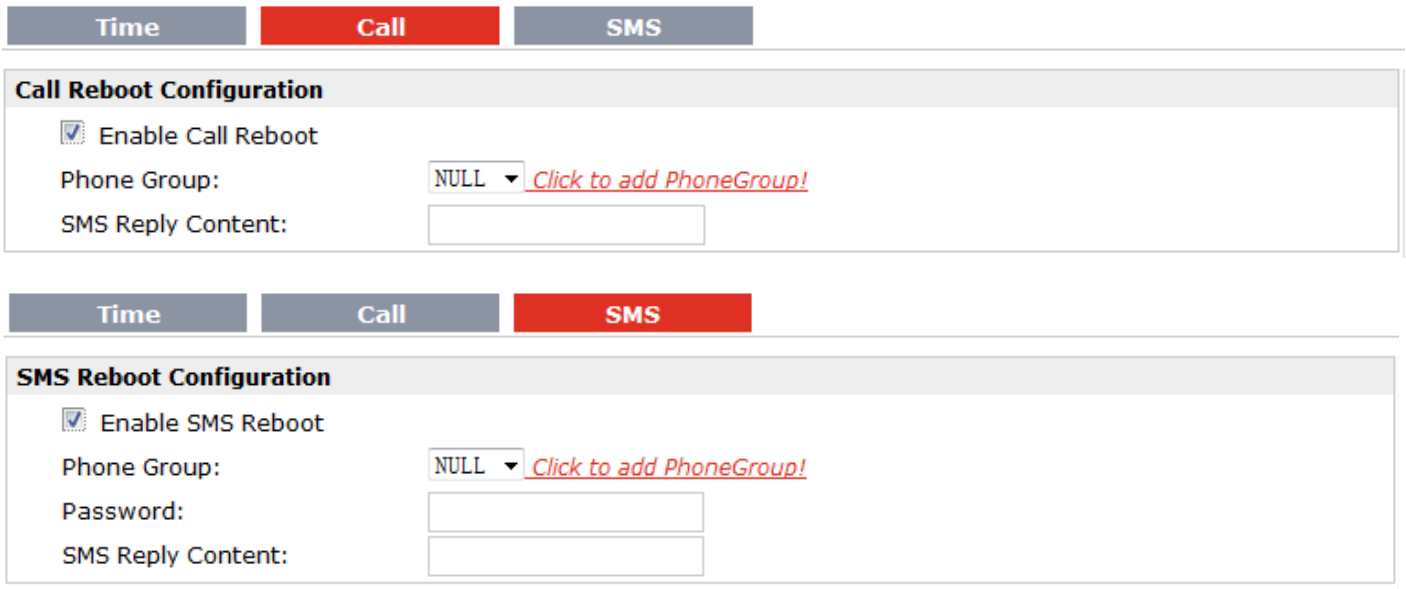
SMS		
Item	Description	Default
Send SMS on power up	Enable to send SMS to specific user after router was powered up.	Disable
Send SMS on PPP connect	Enable to send SMS to specific user when router PPP up.	Disable
Send SMS on PPP disconnect	Enable to send SMS to specific user when router PPP down.	Disable
Phone Group	Select the Phone Group you set in *3.2.27 Configuration -> Phone Book*	Null
Enable @ SMS Control	Click to enable SMS remote control.	Disable
Password Content	Set the password content characters. ***Note**: Only support text format. For example 123 or ABC123.*	Null
Phone Group	Select the Phone Group you set in *3.2.27 Configuration -> Phone Book*	Null

***Note**: please refer to section 4.7 SMS Commands for Remote Control.*

3.34 Configuration -> Reboot

This section allows users to set the Reboot policies.





Time @ Reboot		
Item	Description	Default
Enable(ahh:mm,24h)	Enable daily reboot, you should follow ahh:mm,24h time frame, or the data will be invalid.	Disable
Reboot Time1	Specify time1 when you need router reboot.	Null
Reboot Time2	Specify time2 when you need router reboot.	Null
Reboot Time3	Specify time3 when you need router reboot.	Null
Call @ Reboot		
Enable Call Reboot	Click to enable call reboot function	Disable
Phone Group	Set the Phone Group which was allowed to reboot the router by call.	Null
SMS Reply Content	Send reply short message after auto Call reboot from specified Caller ID (e.g. Reboot ok!). ***Note**: Only support text format SMS.*	Null
SMS @ Reboot		
Enable SMS Reboot	Click to enable SMS reboot function	Disable
Phone Group	Set the Phone Group which was allowed to reboot the router by SMS.	Null
Password	**Password for triggering the Reboot mechanism.**	**Null**
SMS Reply Content	Send reply short message after auto SMS reboot from specified Caller ID (e.g. Reboot ok!). ***Note**: Only support text format SMS.*	Null

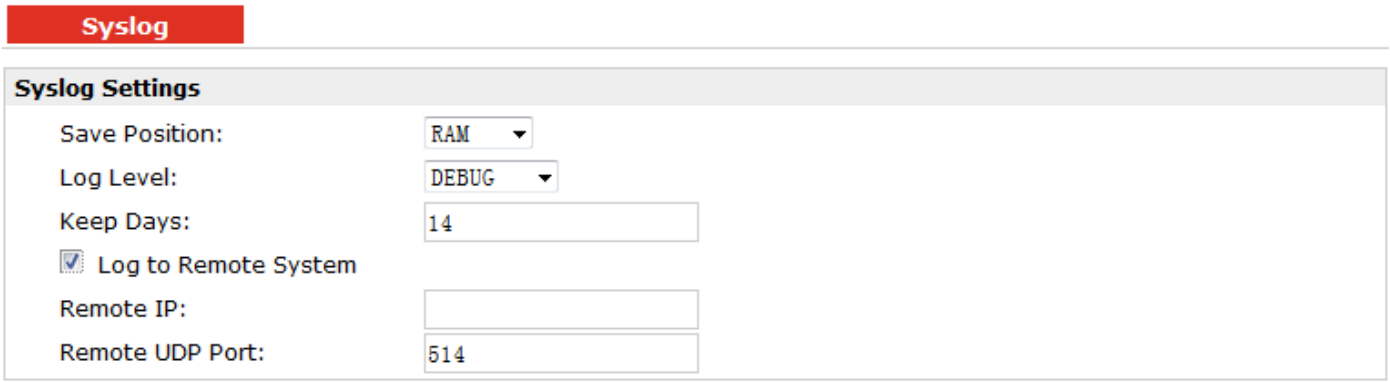
3.35 Configuration -> RobustLink

This section allows users to configure parameters about RobustLink, which is an industrial-grade centralized management and administration system for the R3000-3P. It allows you to monitor, configure and manage large numbers of remote devices on a private network over the web.

RobustLink		
Item	Description	Default
Enable RobustLink	Click to enable RobustLink feature.	Disable
Server address	Enter IP address of RobustLink.	Null
Port	Enter port number of RobustLink.	1883
Password	Enter the password preset in RobustLink. *Note: The passwords set in R3000-3P and RobustLink need to be the same.*	Null

3.36 Configuration -> Syslog

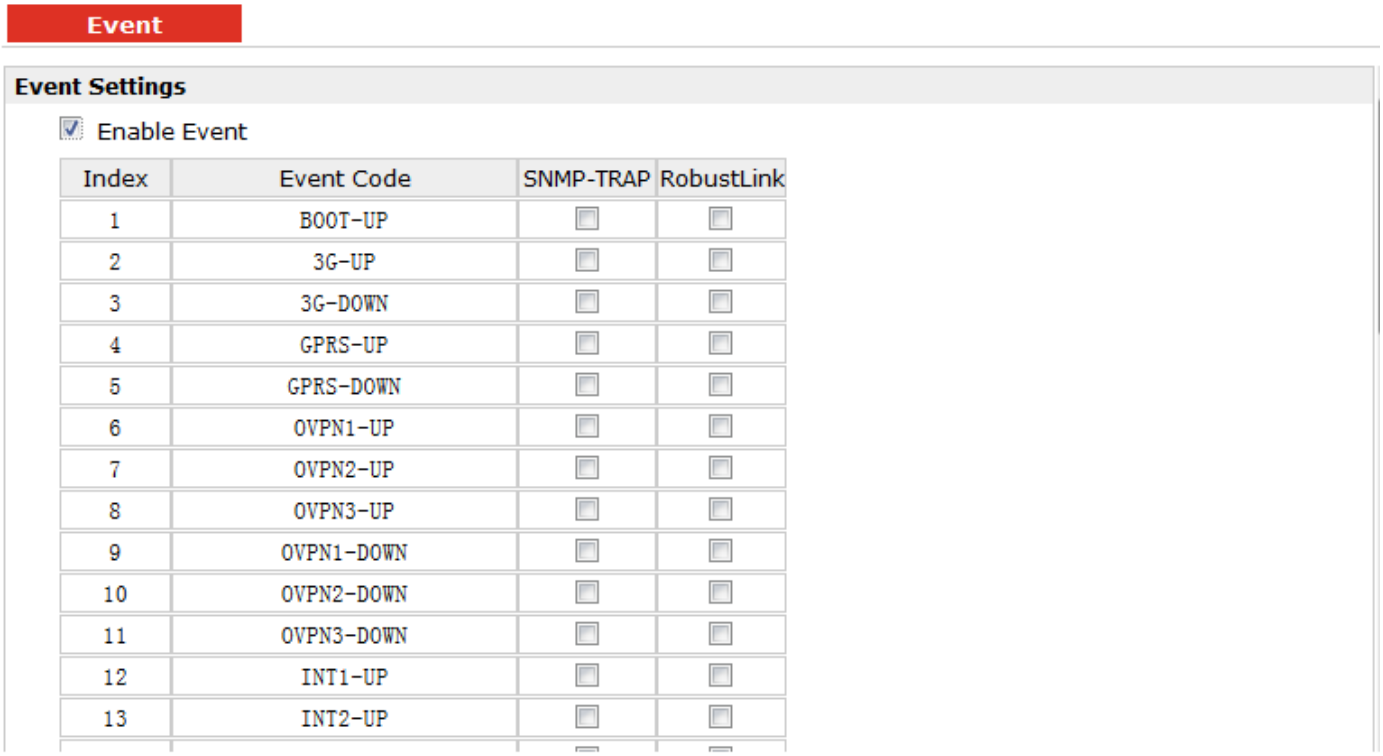
This section allows users to set the syslog parameters.



Syslog		
Item	Description	Default
Save Position	Select the save position from “None”, “Flash” and “SD”. “None” means syslog is only saved in RAM, and will be cleared after reboot.	NONE
Log Level	Select form “DEBUG”, “INFO”, “NOTICE”, “WARNING”, “ERR”, “CRIT”, “ALERT” and “EMERG” which from low to high. The lower level will output more syslog in detail.	DEBUG
Keep Days	Specify the syslog keep days for router to clear the old syslog.	14
Log to Remote System	Enable to allow router sending syslog to the remote syslog server. You need to enter the IP and Port of the syslog server.	Disable

3.37 Configuration -> Event

This section allows users to set the Event parameters.



Event		
Item	Description	Default
Enable Event	Click to enable Event feature. This feature is used to report R3000-3P's main running event to SNMP-TRAP or RobustLink. There are numbers of Event code you can select, such as "BOOT-UP", "3G-UP", "3G-DOWN", etc. For example if you click "3G-UP" and select "RobustLink" as the server, when R3000-3P dial up to connect to 3G network, it will send event code "3G-UP" as well as relevant information to RobustLink.	Disable

3.38 Configuration -> USR LED

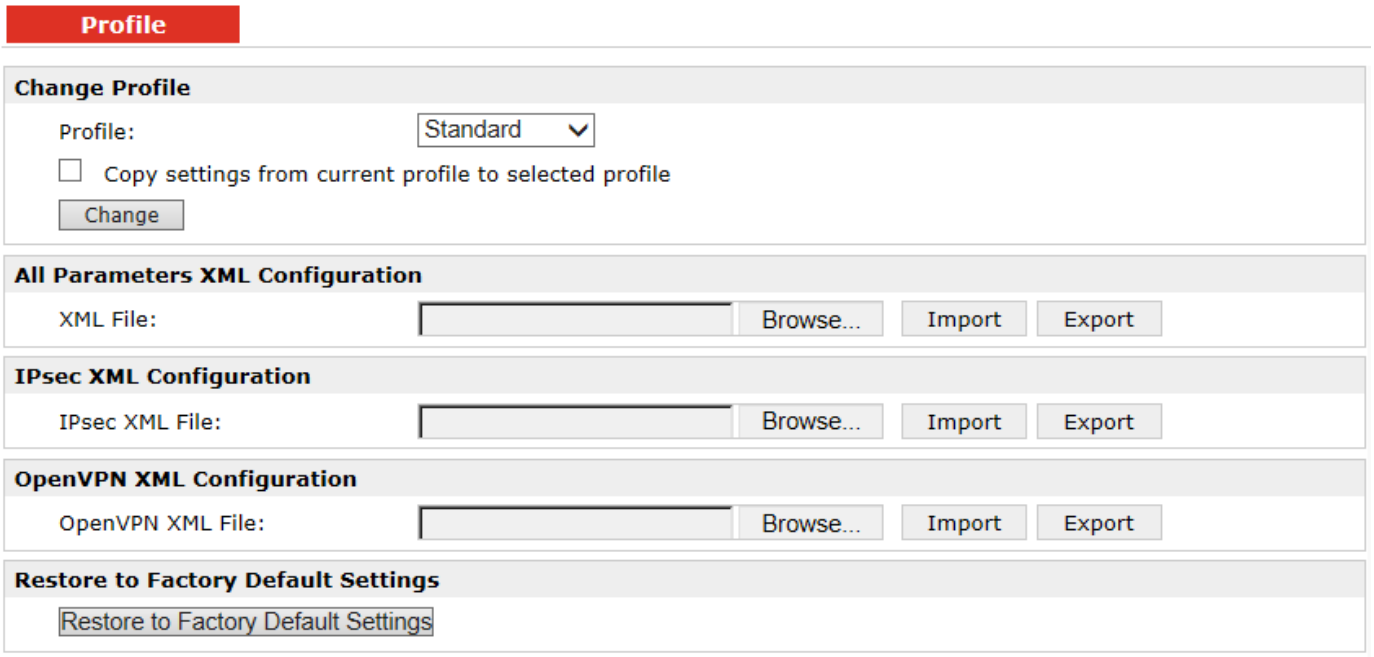
This section allows users to change the display status of USR LED.

***Note**: Please refer to "Status" -> "System" -> "LEDs Information" -> "USR".*

USR LED		
Item	Description	Default
USR LED Type	Select from “VPN”, “PPPoE”, “DynDNS” and “GPS”.	VPN
Indication	Select from “ON”, “Blink”. For example, if “USR LED Type” is set as “VPN” and “Indication” is set as “Blink”, when any VPN tunnel is up USR LED will blink.	ON

3.39 Administration -> Profile

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



Profile		
Item	Description	Default
Profile	This item allow users store different configuration profiles into different positions; or save one configuration profile into different positions just for configuration data backup. Selected from “Standard”, “Alternative 1”, “Alternative 2”, “Alternative 3”.	Standard
XML Configuration	Import: Click “Browse” to select the XML file in your computer, then click	Null

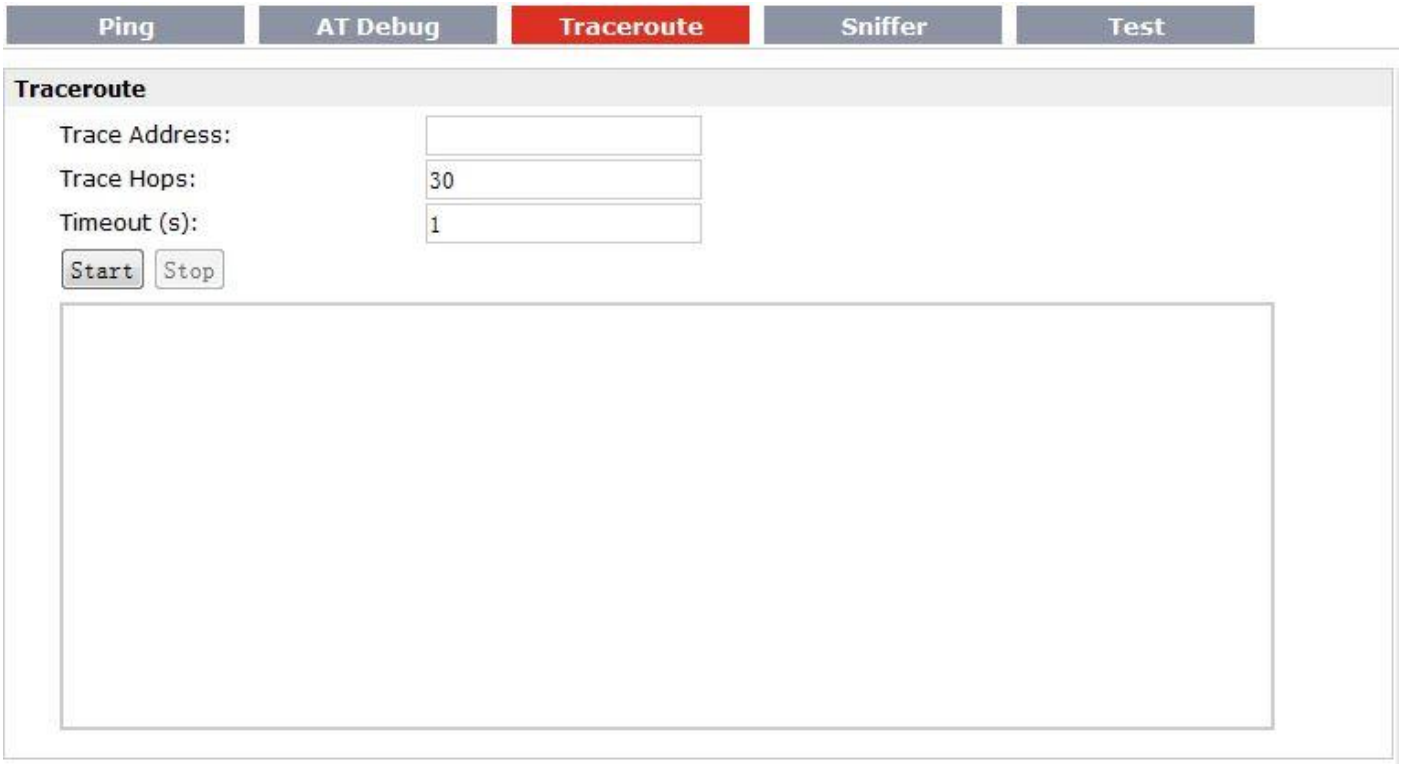
	"Import" to import this file into your router. Export: Click "Export" and the configuration will be showed in the new popup browser window, then you can save it as a XML file.	
Restore to Factory Default Settings	Click the button of "Restore to Factory Default Settings" to restore the router to factory default setting.	Null

3.40 Administration -> Tools

This section provides users four tools: Ping, AT Debug, Traceroute and Test.

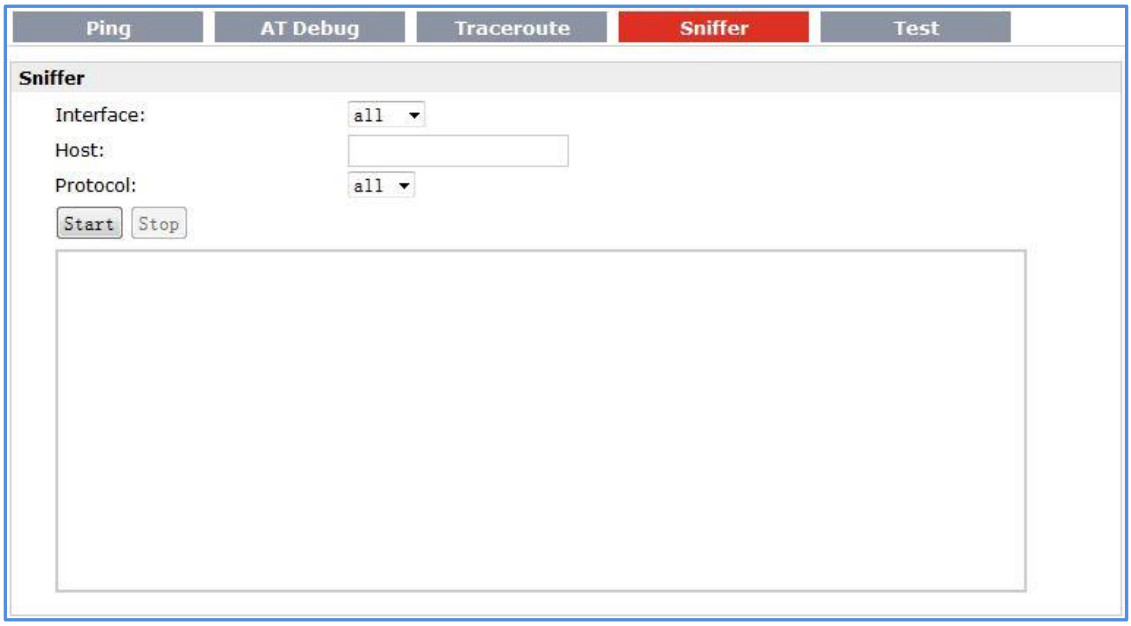
Ping @ Tools		
Item	Description	Default
Ping IP address	Enter the ping destination IP address or domain name.	Null
Number of requests	Specify the number of ping requests.	5
Timeout	Specify timeout of ping request.	1
Local IP	Specify the local IP from cellular WAN, Ethernet WAN or Ethernet LAN. Null stands 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

AT Debug @ Tools		
Item	Description	Default
Send AT Commands	Enter the AT commands which you need to send to cellular module in this box.	Null
Send	Click this button to send the AT commands.	Null
Receive AT Commands	Router will display the AT commands which respond from the cellular module in this box.	Null

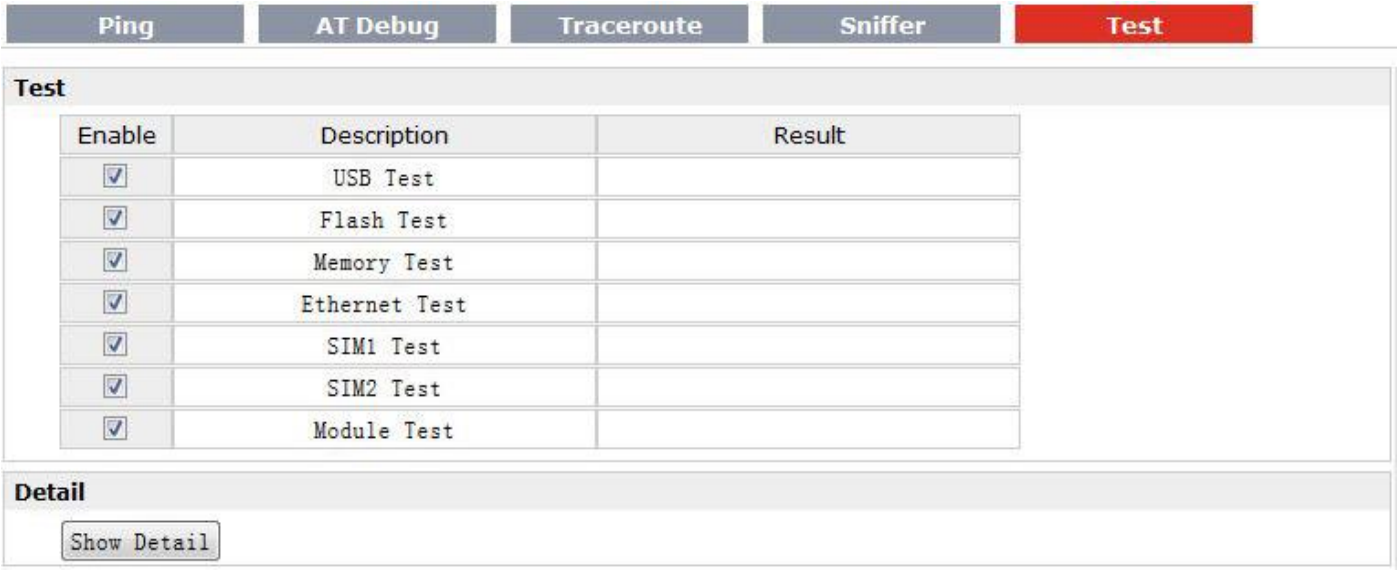


Traceroute @ Tools		
Item	Description	Default

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
Timeout	Specify timeout of Traceroute request.	1
Send	Click this button to start Traceroute request, and the log will be displayed in the follow box.	Null



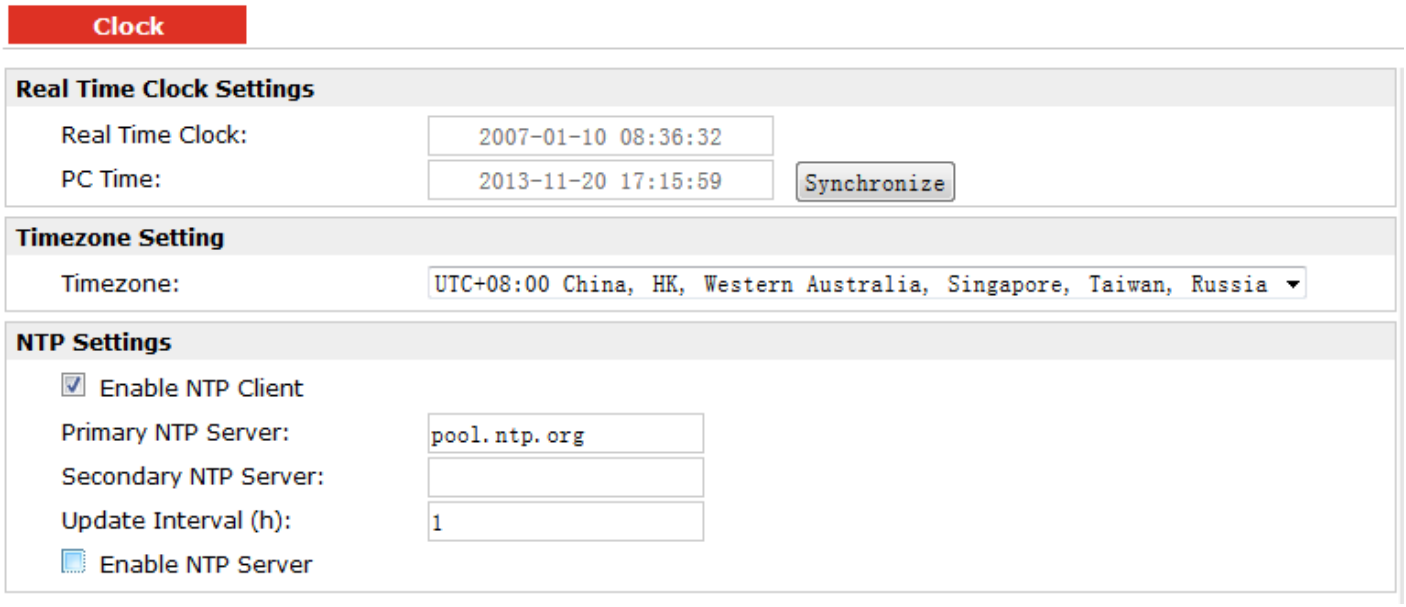
Sniffer @ Tools		
Item	Description	Default
Interface	Select form “all”, “lo”, “imq0”, “imq1”, “eth0”, “gre0”, and “ppp0”: all: contain all the interface; lo: Local Loopback interface; imq0/1: virtual interface for QoS, which used to limit the download and upload speed; eth0: Ethernet interface; gre0: GRE tunnel interface; ppp0: Cellular PPP interface;	All
Host	Filter the packet that contain the specify IP address.	Null
Protocol	Select from “all”, “ip”, “arp”, “tcp” and “udp”.	All
Start	Click this button to start the sniffer, and the log will be displayed in the follow box.	Null



Test @ Tools		
Item	Description	Default
Enable	Click “Enable” to select the hardware component whose status you want to check.	Enable
Description	Select from “SD Test”, “USB Test”, “Flash Test”, “Memory Test”, “Ethernet Test”, “SIM1 Test”, “SIM2 Test” and “Module Test”.	N/A
Result	Show the current status of the selected hardware component. There are 3 status “Testing”, “Success” and “Failure”. Testing: Router is testing the selected hardware component. Success: Correspond hardware component is properly inserted and detected. Failure: Correspond hardware component is not inserted into the router or the router fails to detect.	Null
Show Detail	Show the current test details of the hardware component.	Null
***Note**: click “Apply” to start testing.*		

3.41 Administration -> Clock

This section allows users to set clock of router and NTP server.



Clock		
Item	Description	Default
Real Time Clock	Router's RTC can be showed and modified in this field.	Null
PC Time	You PC's time can be showed here.	Null
Synchronize	Synchronize router's RTC with PC.	Null
Enable NTP Client	Enable to synchronize the time from NTP server.	Disable
Timezone @ Client	Select your local time zone.	UTC +08:00
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
Update interval (h)	Enter the interval which NTP client synchronize the time from NTP server.	1
Enable NTP Server	Click to enable the NTP server function of router.	Disable
Timezone @ Server	Select your local time zone.	UTC +08:00

3.42 Administration -> Web Server

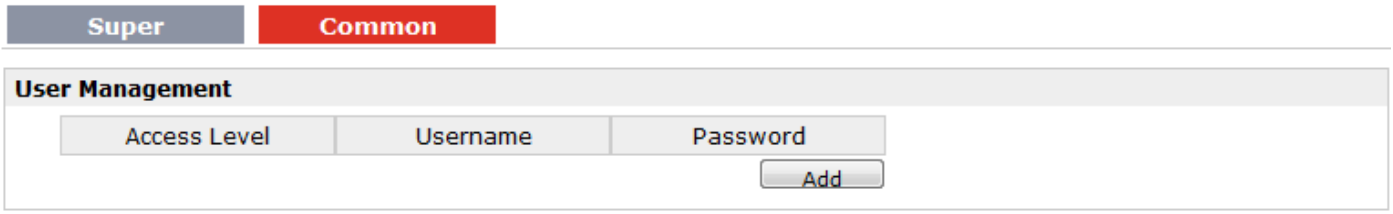
This section allows users to modify the parameters of Web Server.

Basic @ Web Server		
Item	Description	Default
HTTP Port	Enter the HTTP port number you want to change in R3000-3P'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 R3000-3P's Web Server.	80
HTTPS Port	Enter the HTTPS port number you want to change in R3000-3P'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 R3000-3P'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
X.509 @ Web Server		
HTTPS Certificate	In this tab, user can import or export "Public Key" and "Private Key" for HTTPS certification.	Null

3.43 Administration -> User Management

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

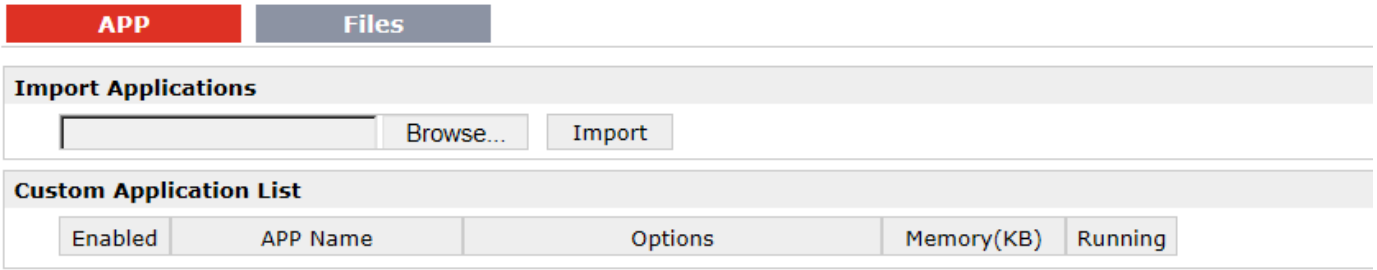
Super @ User Management		
Item	Description	Default
Super	One router has only one super user account. Under this account, user has the highest authority include modify and add management user accounts.	Admin
User Management	Set Username and Password.	Null
Login Timeout	Specify the login timeout value. You need to re-login after this timeout of user inactively.	1800



Common @ User Management		
Item	Description	Default
Common	One router has at most 9 common user accounts. There are two access level of common user account: “ReadWrite” and “ReadOnly”.	Null
Access Level	Select from “ReadWrite” and “ReadOnly”. ReadWrite: Users can view and set the configuration of router under this level; ReadOnly: Users only can view the configuration of router under this level	Null
Username/ Password	Set Username and Password.	Null
Add	Click this button to add a new account.	Null

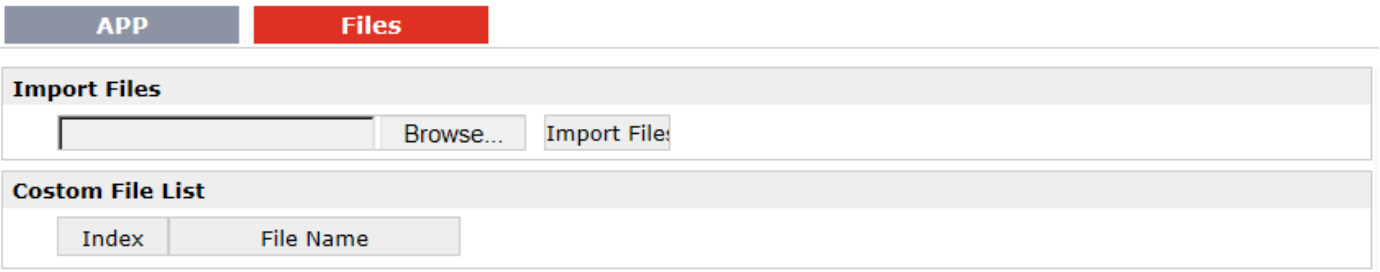
3.44 Administration -> SDK Management

This section allows users to set SDK Management parameters of router.



APP @ SDK Management		
Item	Description	Default
Firmware Version	Show the current firmware version.	Null
Import Files	Click to import APP files in this item.	Null
Custom Application	This list shows which APP files you have imported to the router, which APP file	Null

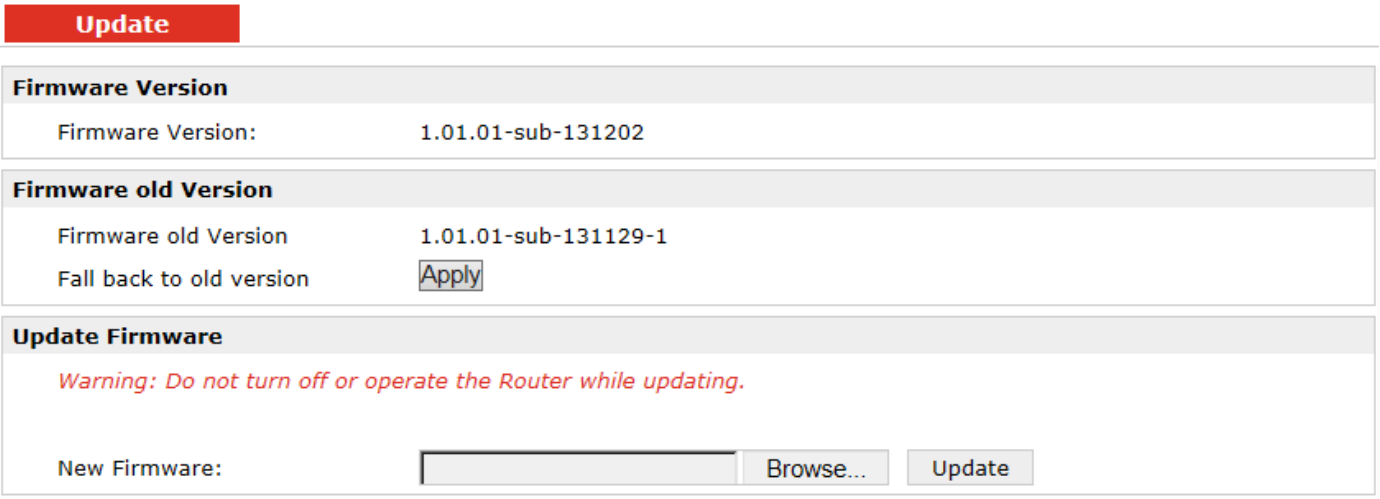
List	you want to start up, as well as the running information. Enable: Click to enable the APP file. APP Name: Shows the name of the APP files. Options: It is an optional items, user can choose to configure startup parameters here. Memory (KB): Shows the memory resources occupied by the APP files. Running: Shows whether the APP files are running.	



Files @ SDK Management		
Item	Description	Default
Import Files	Click to import configuration files in this item.	Null
Custom File List	This list shows which Configuration files you have imported to the router.	Null

3.45 Administration -> Update Firmware

This section allows users to update the firmware of router.



Update		
Item	Description	Default
Firmware Version	Show the current firmware version.	Null
Update firmware	Click “Select File” button to select the correct firmware in your PC, and then click	Null

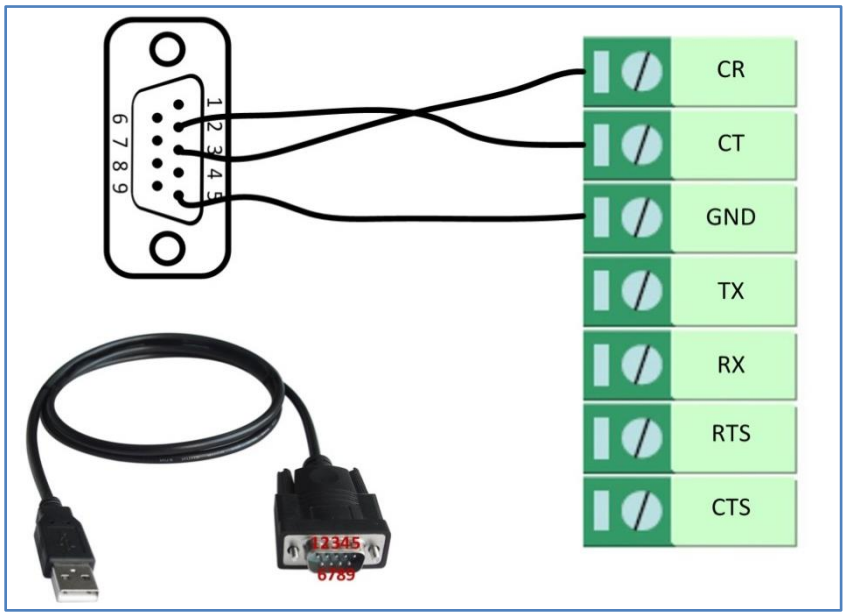
	“Update” button” to update. After updating successfully, you need to reboot router to take effect.	

Chapter 4. Configuration Examples

4.1 Interface

4.1.1 Console port

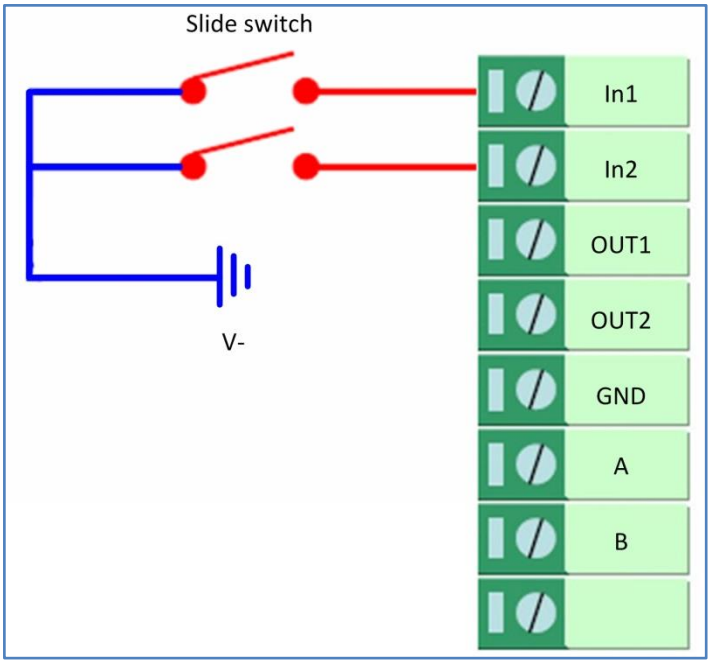
User can use the console port to manage the router via CLI commands, please check section Introductions for CLI.



4.1.2 Digital Input

There are two digital inputs of R3000-3P, it just support dry contact (do not supports wet contact).

Please check the connector interface of R3000-3P, you can find out "**V-**" easily at one of the pin of power input connector.



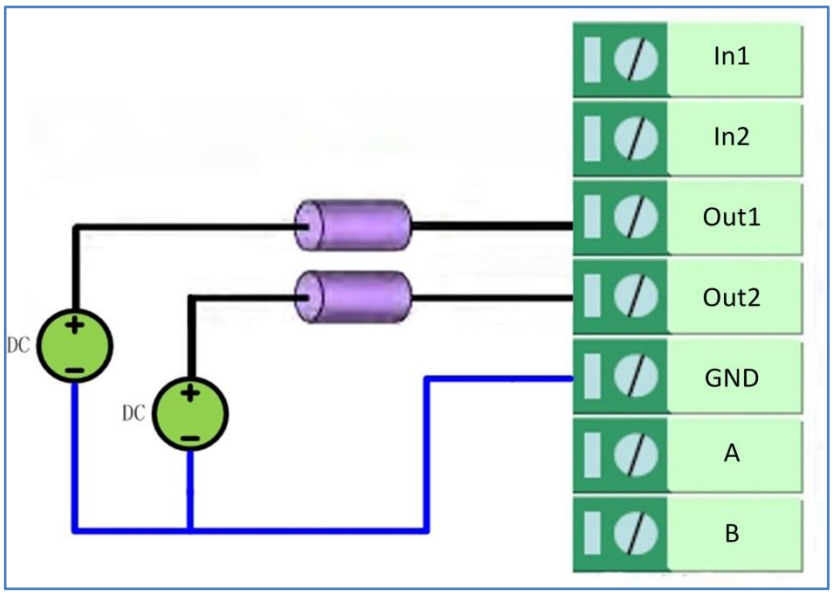
4.1.3 Digital Output

There are two digital outputs of R3000-3P.

Power negative of DC should connect to "GND"

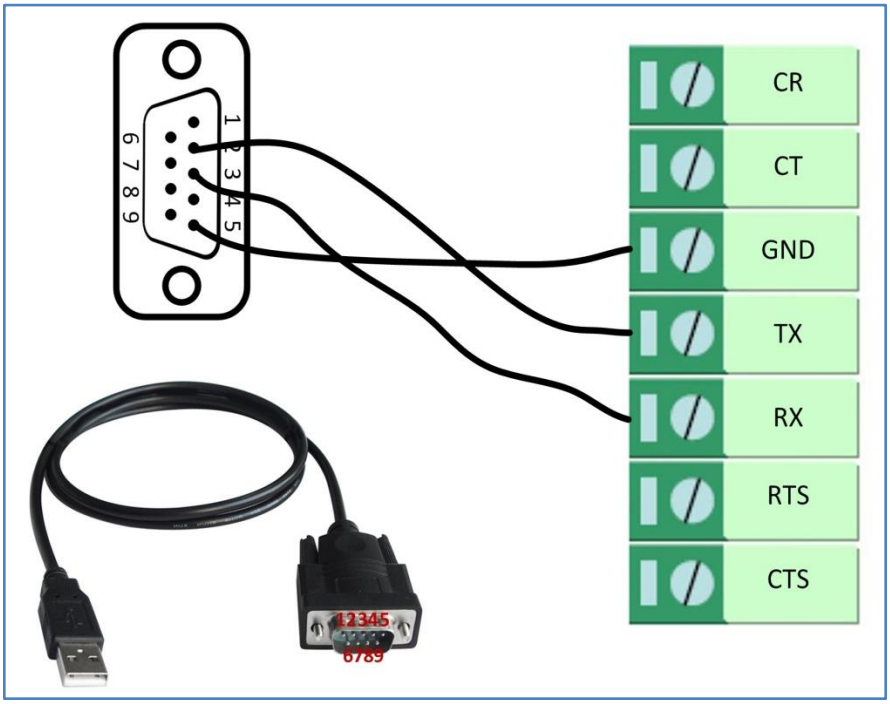
Please refer to connection diagram at the right site.

Maximum voltage/current/output power of DO is 36VDC/0.05A/0.3W. It means voltage difference between Out1/Out2 and GND cannot exceed to 36VDC; the current value through Out1/Out2 cannot exceed to 50mA. And the output power dissipated by Out1/Out2 cannot exceed to 0.3W. Otherwise DO will be damaged.



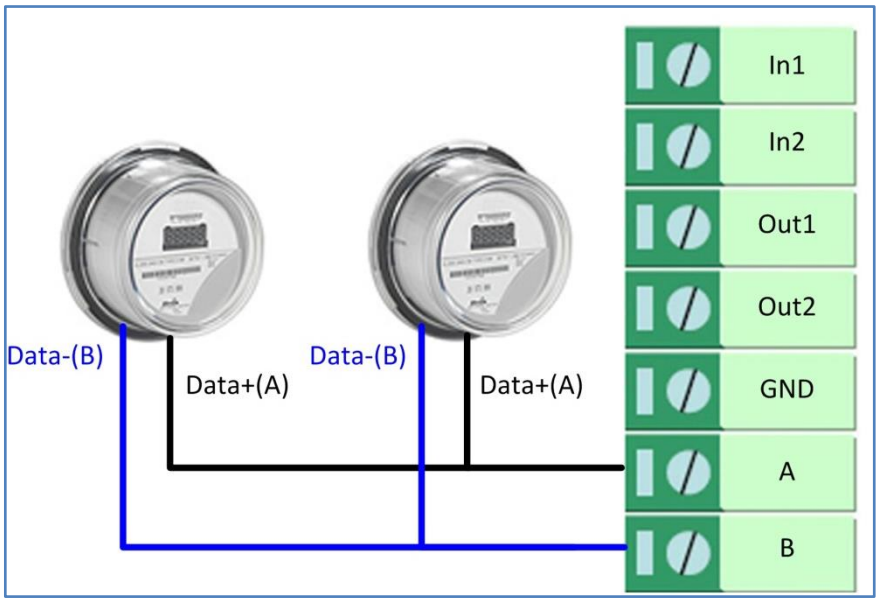
4.1.4 RS232

R3000-3P supports one RS232 for serial data communication.
Please refer to the connection diagram at the right site.



4.1.5 RS485

R3000-3P supports one RS485 for serial data communication.
Please refer to the connection diagram at the right site.



4.2 Cellular

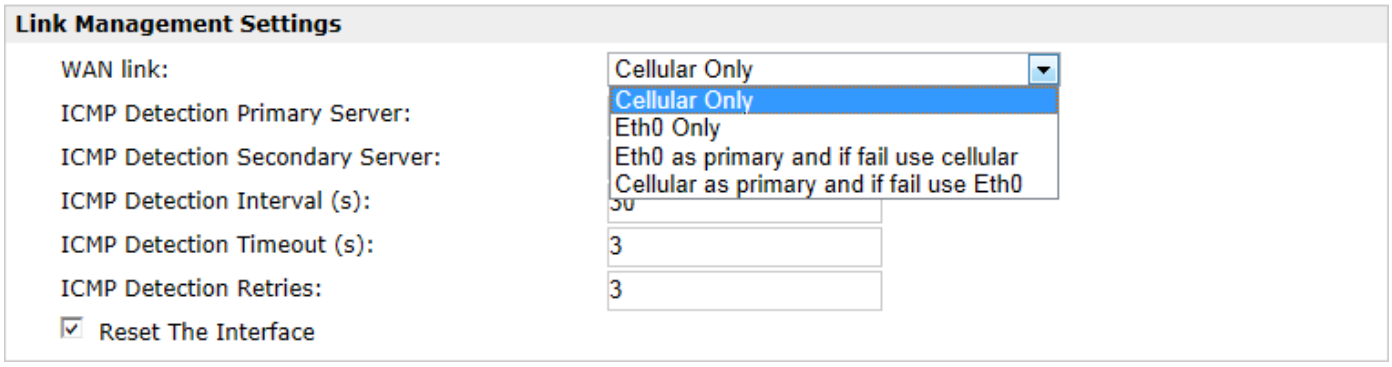
4.2.1 Cellular Dial-Up

This section shows users how to configure the parameters of Cellular Dial-up which are with two different policies "Always Online" and "Connect on Demand".

***Note**: This section will be hidden if user selects "Eth0 Only" in "Configuration ->Link Management".*

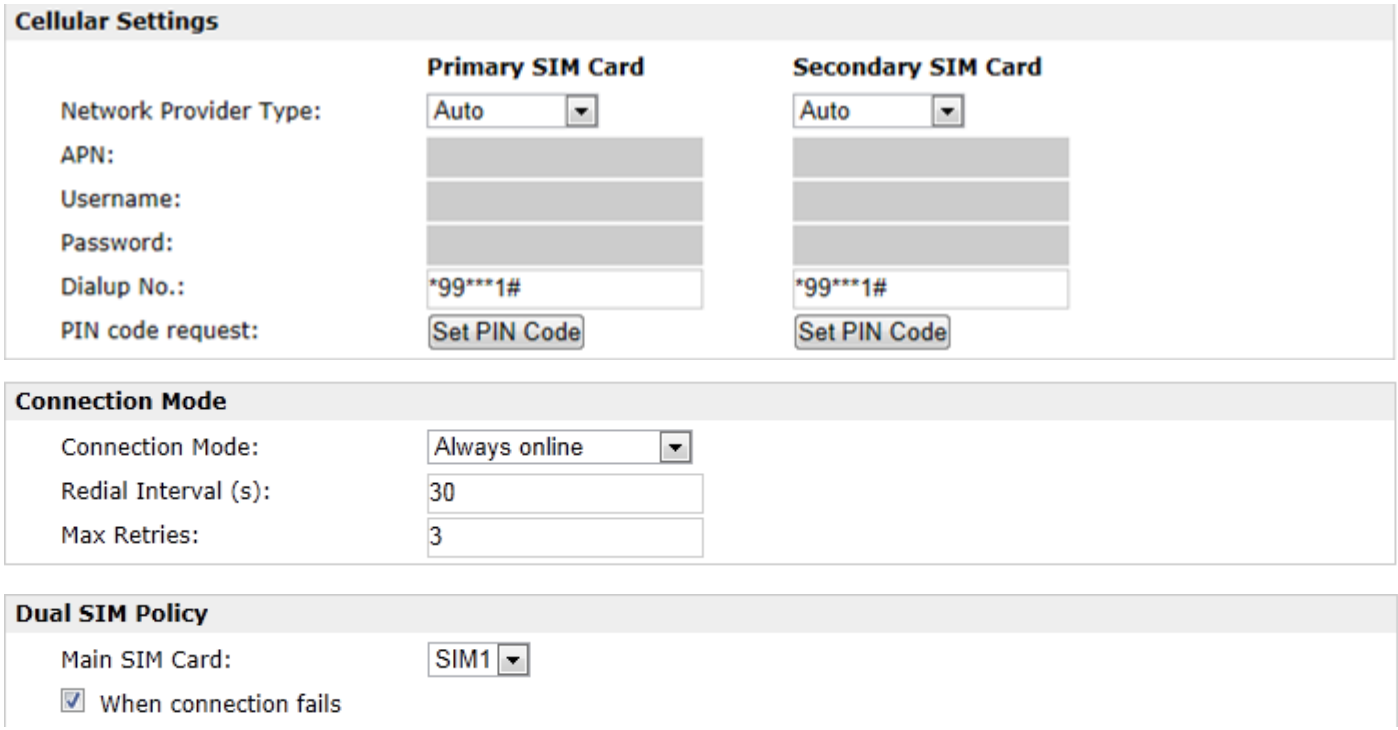
1. Always Online

Configuration-->Link Management-->Cellular Only



The modifications will take effect after click "Apply" button.

Configuration-->Cellular WAN -->Basic

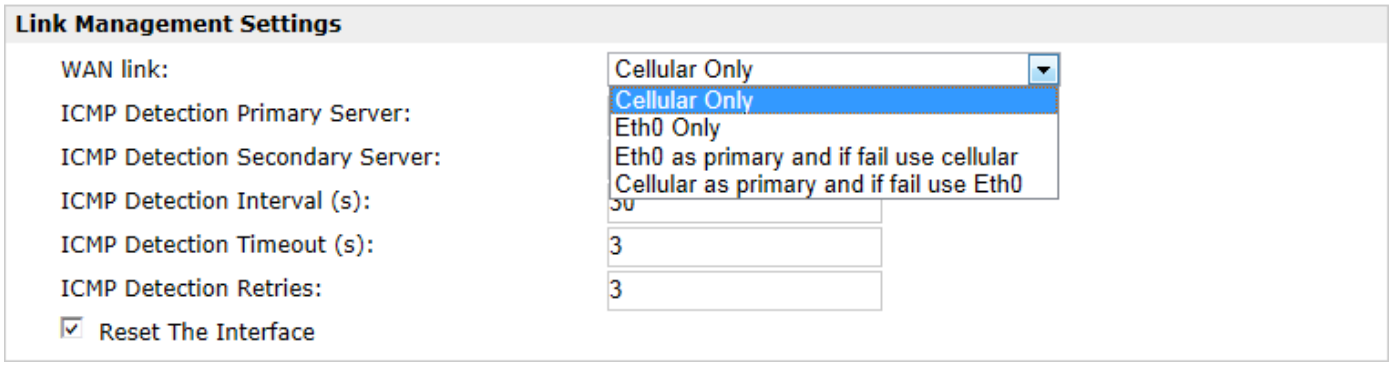


The modifications will take effect after click “Apply” button.

If a customized SIM card is using, please select “Custom” instead of “Auto” in “Network Provider Type”, and some relative settings should be filled in manually.

2. Connect on Demand

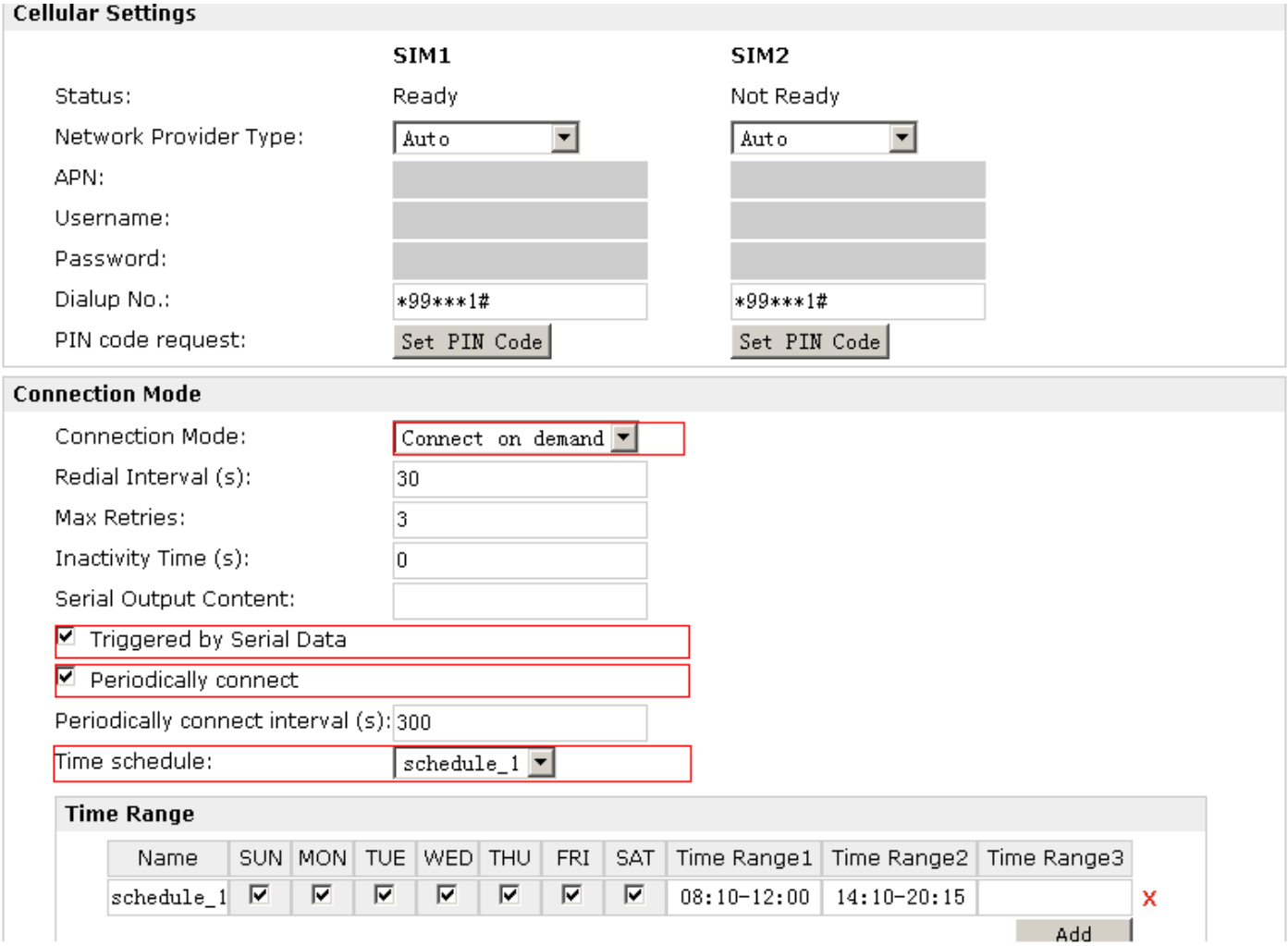
Configuration-->Link Management-->Cellular Only



The modifications will take effect after click “Apply” button.

Note: *This section will be hidden if user selects “Cellular as primary and if fail use Eth0” in “Configuration ->Link Management”.*

Configuration-->Cellular WAN -->Basic



Select the trigger policy you need.

Note: *If you select multiple trigger policies, the router will be triggered under anyone of them.*

4.2.2 SMS Remote Status Reading

R3000-3P supports remote control via SMS. User can use following commands to get the status of R3000-3P, cannot set new parameters of R3000-3P at present.

An SMS command has following structure:

Password:cmd1,a,b,c;cmd2,d,e,f;cmd3,g,h,i;...;cmdn,j,k,n

SMS command Explanation:

1. Password: SMS control password is configured at **Basic->SMS Control->Password**, which is an optional parameter.
   a) When there is no password, SMS command has following structure: **cmd1;cmd2;cmd3;…;cmdn**
   b) When there is a password, SMS command has following structure: **Password:cmd1;cmd2;cmd3;…;cmdn**
2. cmd1, cmd2, cmd3 to Cmdn, which are command identification number 0001 – 0010.
3. a, b, c to n, which are command parameters.

4. The semicolon character (';') is used to separate more than one commands packed in a single SMS.
5. E.g., 1234:0001

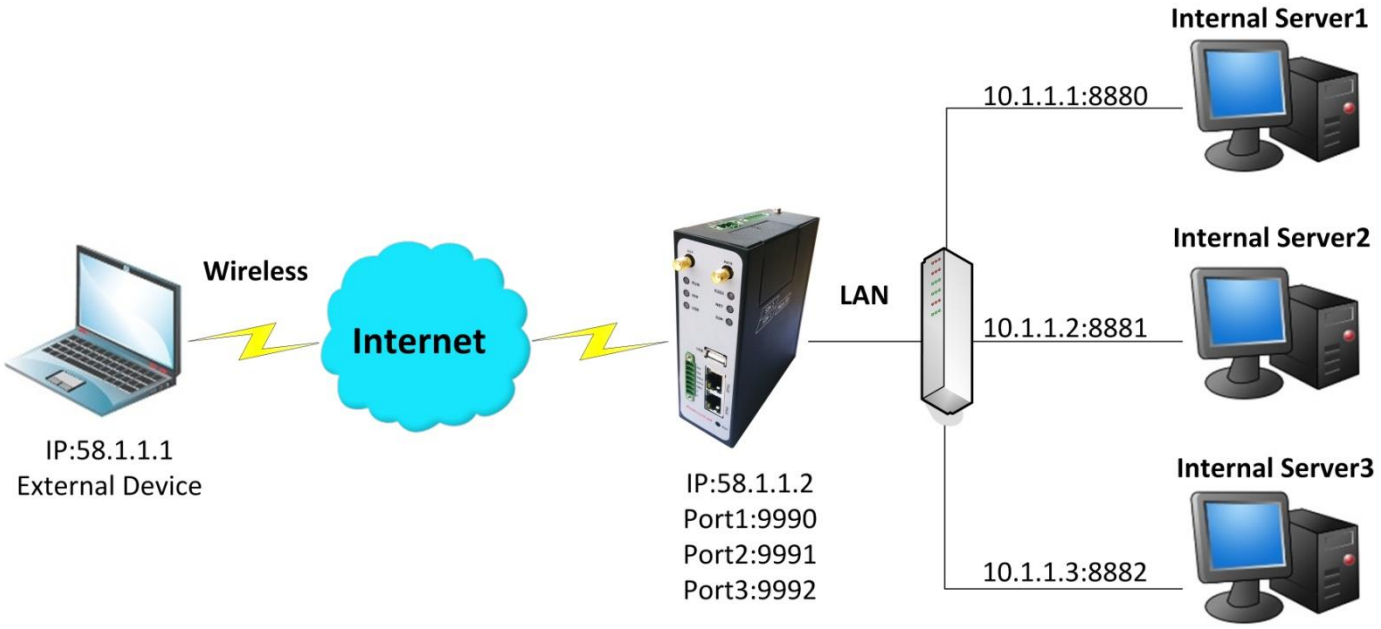
In this command, password is 1234, 0001 is the command to reset R3000-3P.

Cmd	Description	Syntax	Comments
Control Commands			
0001	Reset Device	cmd	if no password, please use command "cmd", or use command" password: cmd" cmd1 + cmd2: cmd1;cmd2 * - means can be null
0002	Save Parameters	cmd	
0003	Save Parameters and Reset Device	cmd	
0004	Start PPP Dialup	cmd	
0005	Stop PPP	cmd	
0006	Switch Sim Card	cmd	
0007	Enable/Disable Event Counter	cmd,channel,flag	channel: 1 - DI_1 2 - DI_2 flag: 0 - disable 1 - enable
0008	Get Event Count Value	cmd,channel	channel: 1 - DI_1 2 - DI_2
0009	Clear Event Count	cmd,channel	channel: 1 - DI_1 2 - DI_2
0010	Clear SIM Card's Data Limitation	cmd,simNumber	simNumber: 1 - SIM_1 2 - SIM_2

4.3 Network

4.3.1 NAT

This section shows users how to set the NAT configuration of router.
Parameter Remote IP defines if access is allowed to route to the Forwarded IP and Port via WAN IP and "Arrives At Port".



Configuration--->NAT/DMZ--->Port Forwarding

Port Forwarding

Remote IP	Arrives At Port	Is Forwarded to IP Address	Is Forwarded to Port	Protocol
58.1.1.1	9990	10.1.1.1	8880	TCP
58.1.1.1	9991	10.1.1.2	8881	UDP
58.1.1.1	9992	10.1.1.3	8882	TCP&UDP

**Remote IP: 1.1.1.1, 1.1.1.0/24,1.1.1.1-2.2.2.2, 0.0.0.0 means any*

**Arrives At Port: <1-65536> or <1-65536>-<1-65536>*

Add

Note: *This section will be hidden if user selects "Cellular as primary and if fail use Eth0" in "Configuration ->Link Management".*

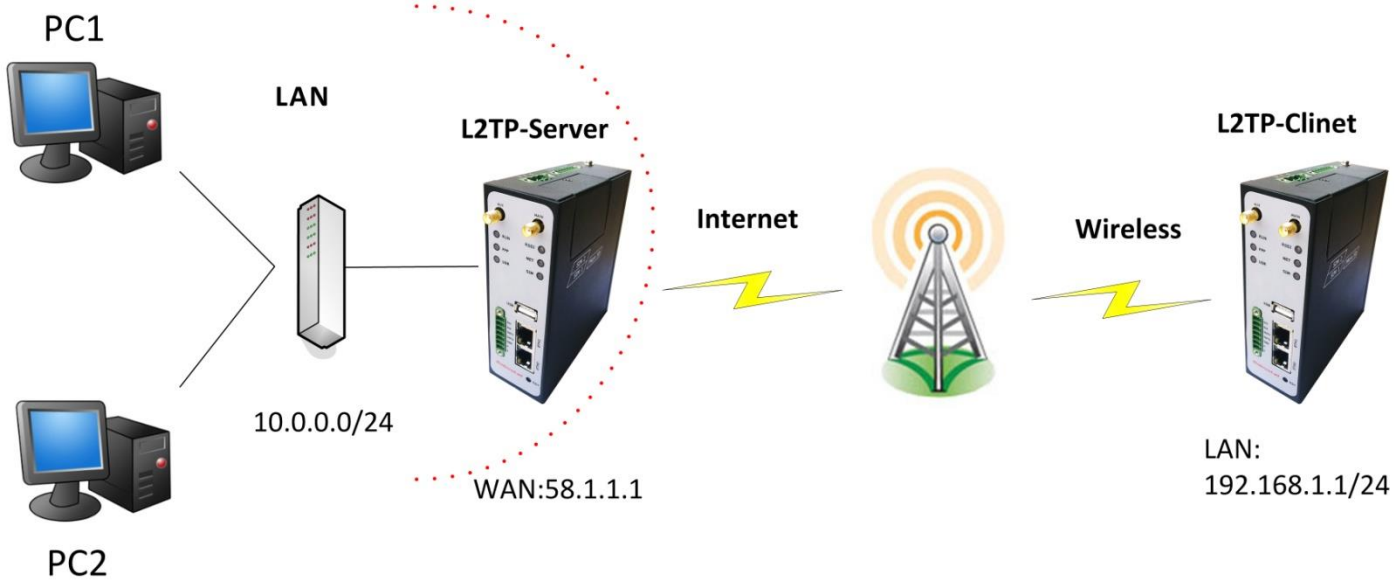
Explanations for above diagram:

If there are two IP addresses 58.1.1.1 and 59.1.1.1 for the External Devices, that the result will be different from the test when the NAT is working at R3000-3P.

58.1.1.1----------access to--------->58.1.1.2:9990----------be forwarded to------->10.1.1.1:8000 TCP

58.1.1.1----------access to--------->58.1.1.2:9991----------be forwarded to------->10.1.1.2:8001 UDP
58.1.1.1----------access to--------->58.1.1.2:9992----------be forwarded to------->10.1.1.3:8002 TCP&UDP

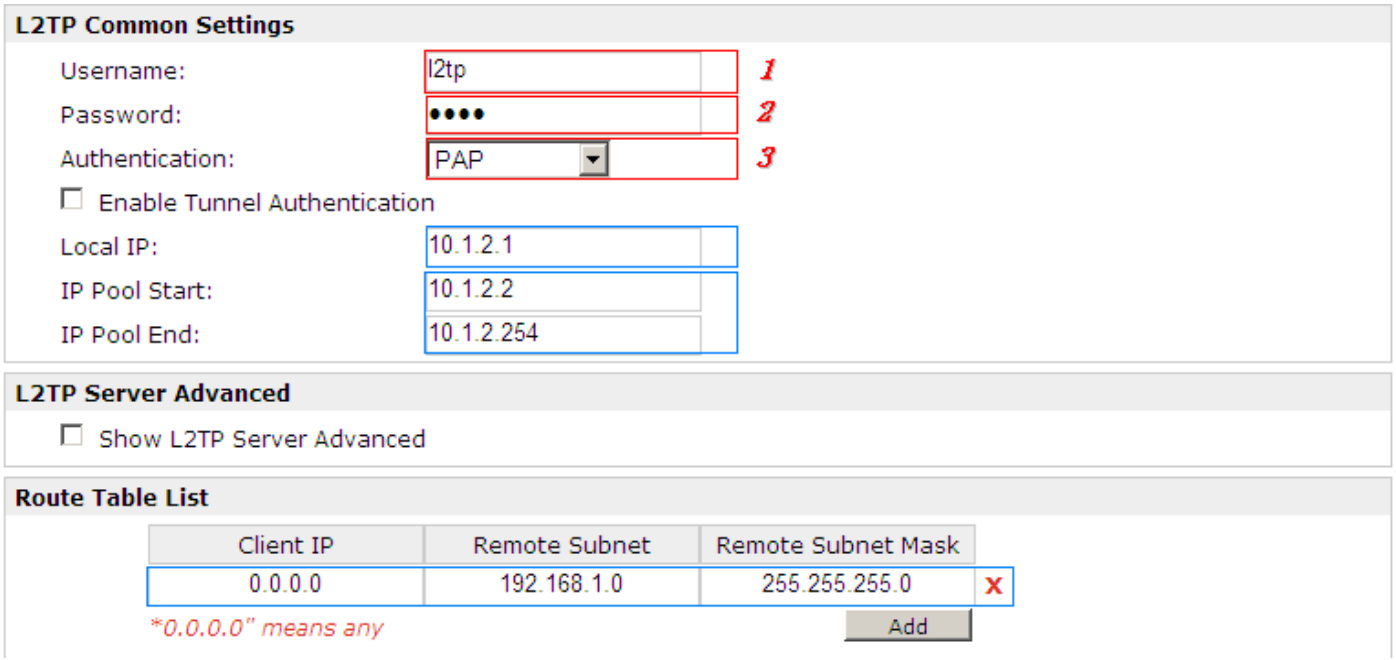
4.3.2 L2TP



L2TP_SERVER:

Configuration--->L2TP--->L2TP Server

Tick “Enable L2TP Server”, and fill in the blank textbox



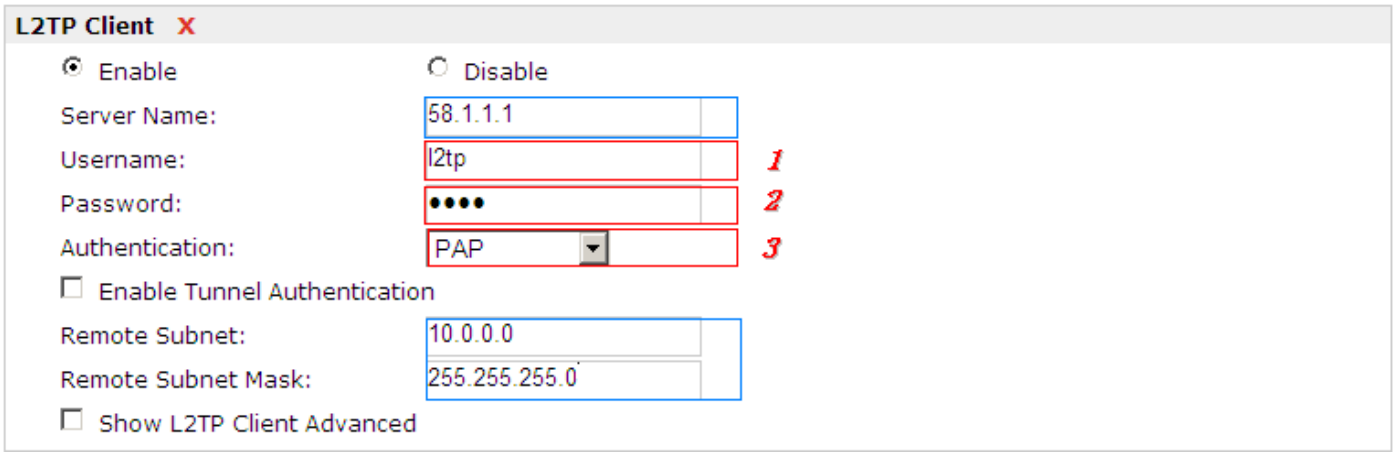
The modification will take effect after "Apply-->Save-->Reboot".

Note: *The following diagrams with red color numbers mean these are the matches between server and client, and with the blue color number means it must be set locally for the tunnel.*

L2TP_CLIENT:

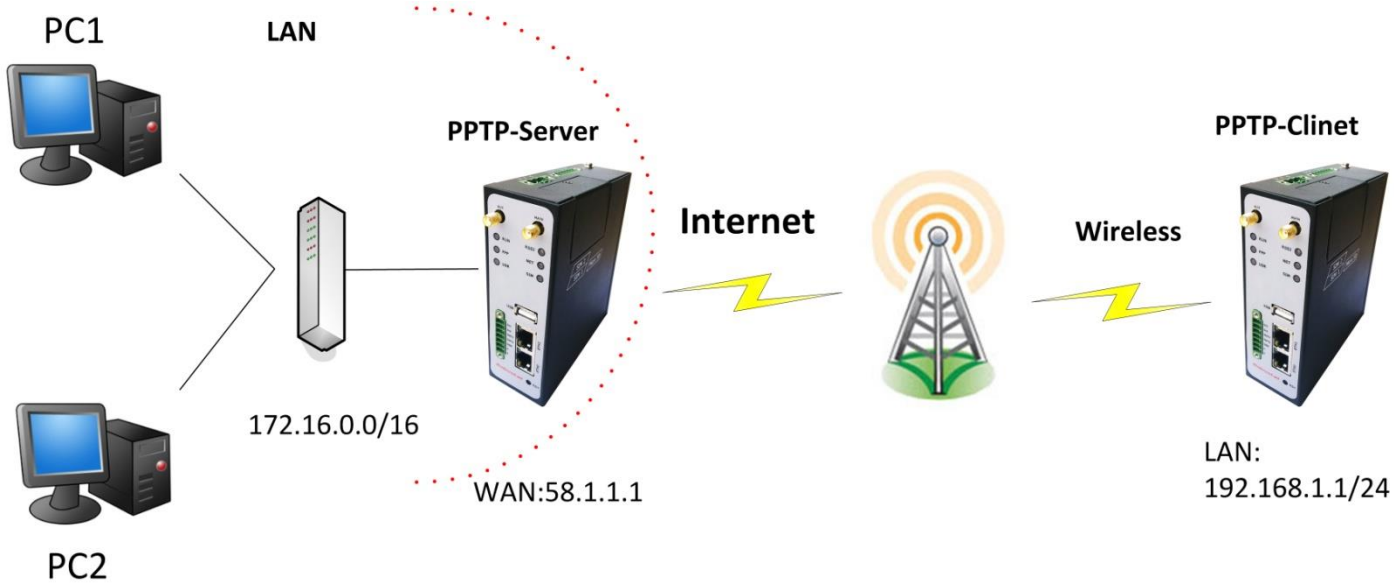
Configuration--->L2TP--->L2TP Client

Click "Add" button, and fill in the blank textbox



The modification will take effect after "Apply-->Save-->Reboot".

4.3.3 PPTP

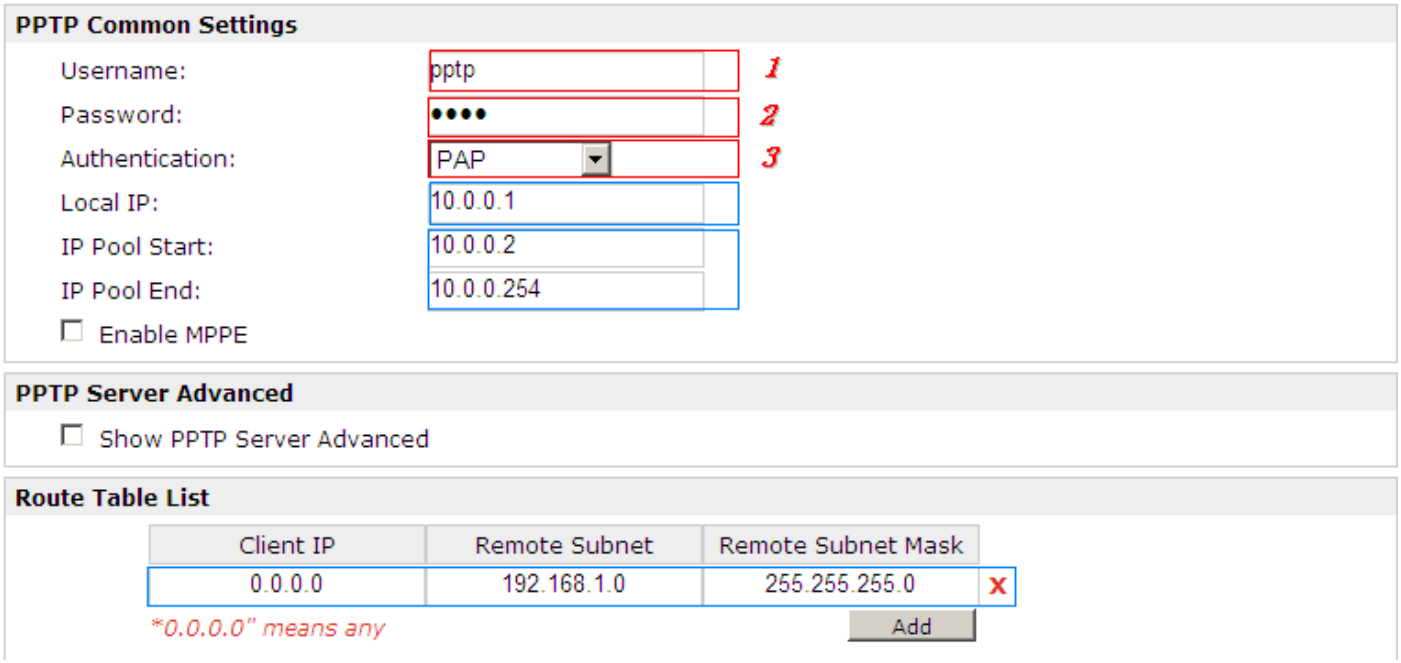


Note: *The following diagrams with red color numbers mean these are the matches between server and client, and with the blue color number means it must be set locally for the tunnel .*

PPTP_SERVER:

Configuration--->PPTP--->PPTP Server

Tick “Enable PPTP Server”, and fill in the blank textbox

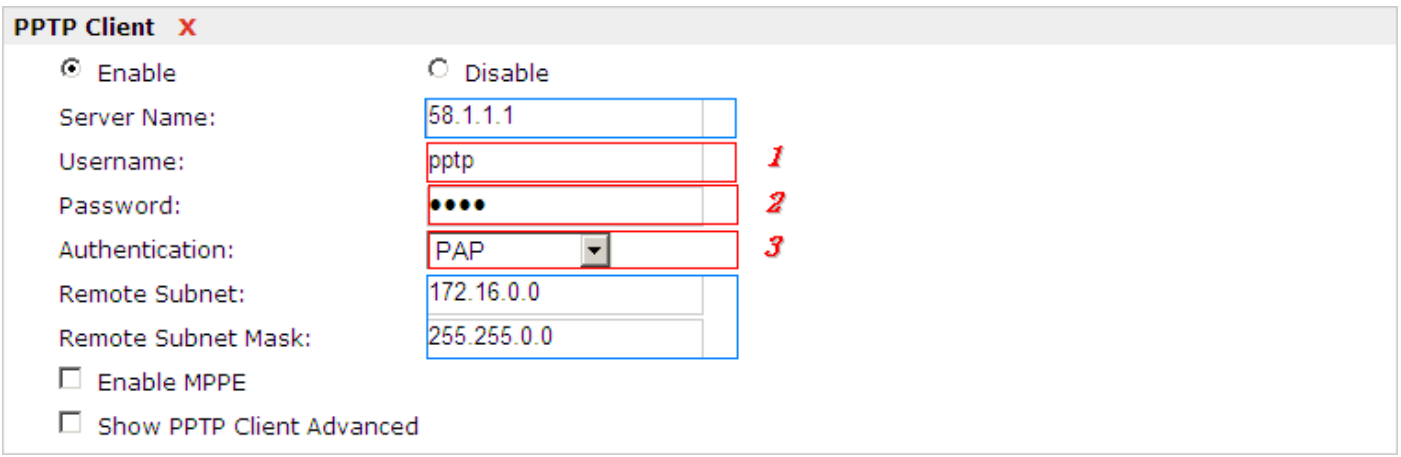


The modification will take effect after “Apply-->Save-->Reboot”.

PPTP_CLIENT:

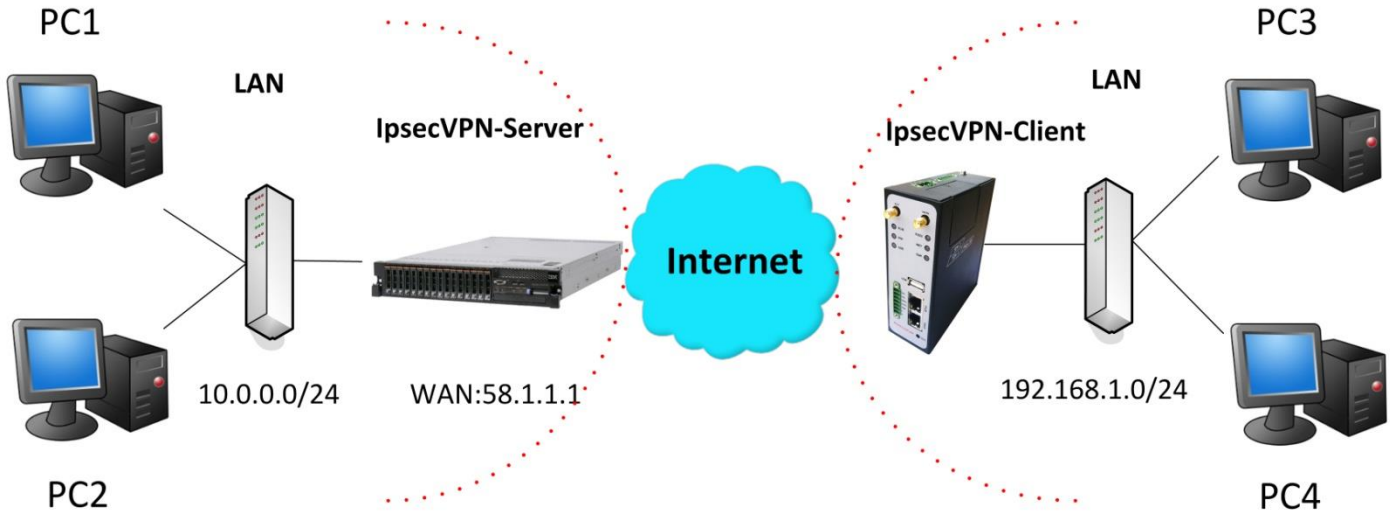
Configuration--->PPTP--->PPTP Client

Click “Add” button, and fill in the blank textbox



The modification will take effect after “Apply-->Save-->Reboot”.

4.3.4 IPSEC VPN



Note: *The following diagrams with red color numbers mean these are the matches between server and client, and with the blue color number means it must be set locally for the tunnel.*

IPsecVPN_SERVER:

Cisco 2811:

```
crypto isakmp policy 10
 encr aes 256                                   8
 hash md5                                       9
 authentication pre-share                       11
 group 2                                        10
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
                                12
!
crypto ipsec transform-set trans esp-3des esp-md5-hmac   2, 13
!
crypto dynamic-map dyn 10
  set transform-set trans
  match address 101
!
crypto map map1 10 ipsec-isakmp dynamic dyn
!
interface FastEthernet0/0
  crypto map map1
!
access-list 101 permit ip 10.0.0.0 0.0.0.255 any   3, 5
!
```

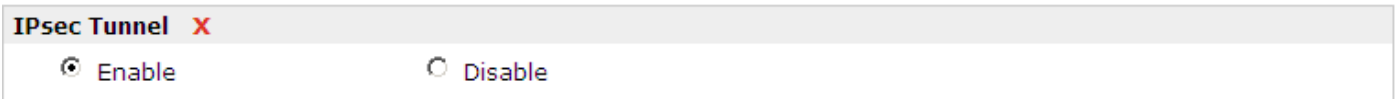
Note: *Polices 1,4,6,7 are default for Cisco router and do not display at the CMD.*

IPsecVPN_CLIENT:

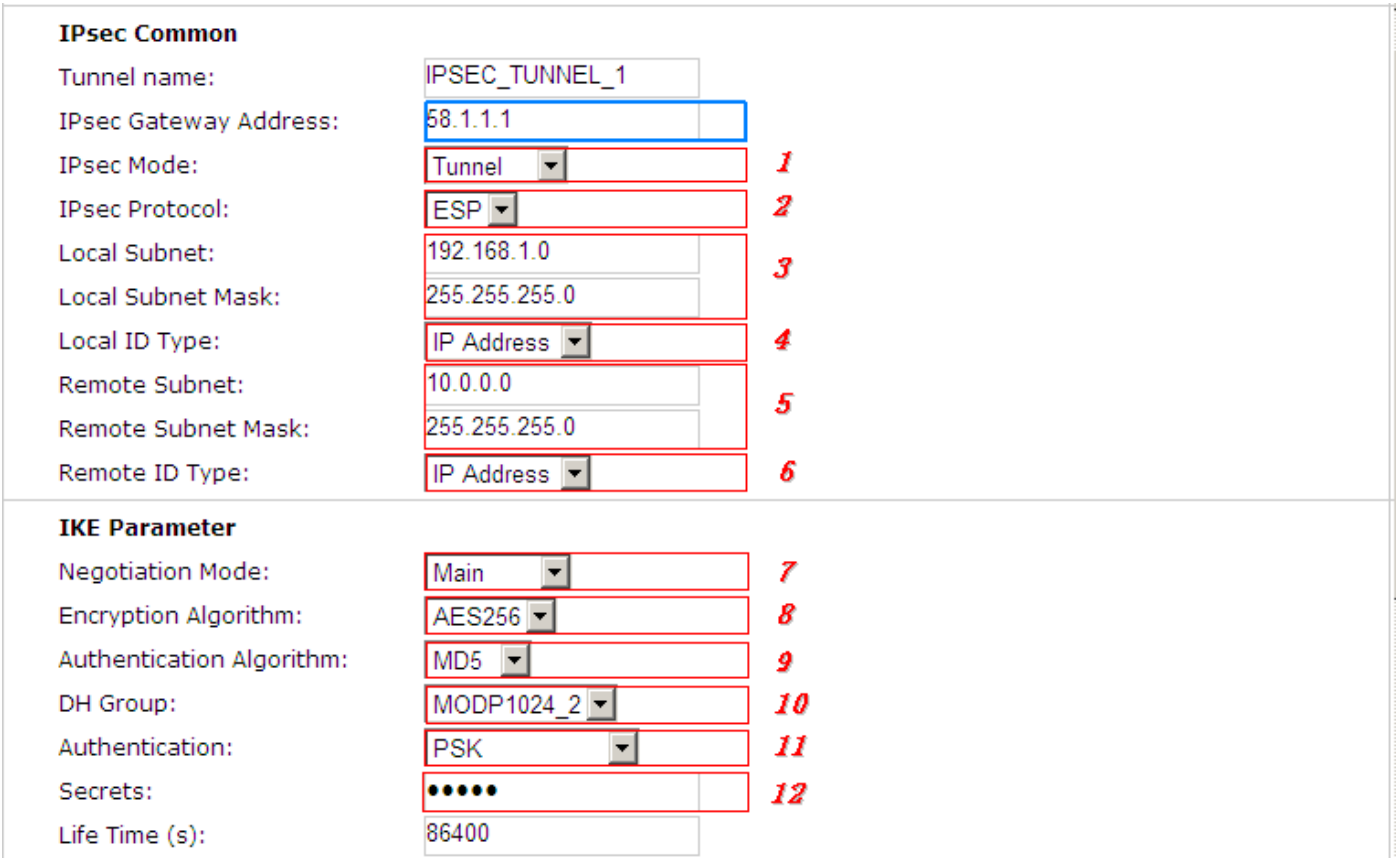
Configuration--->IPSec--->IPSec Basic

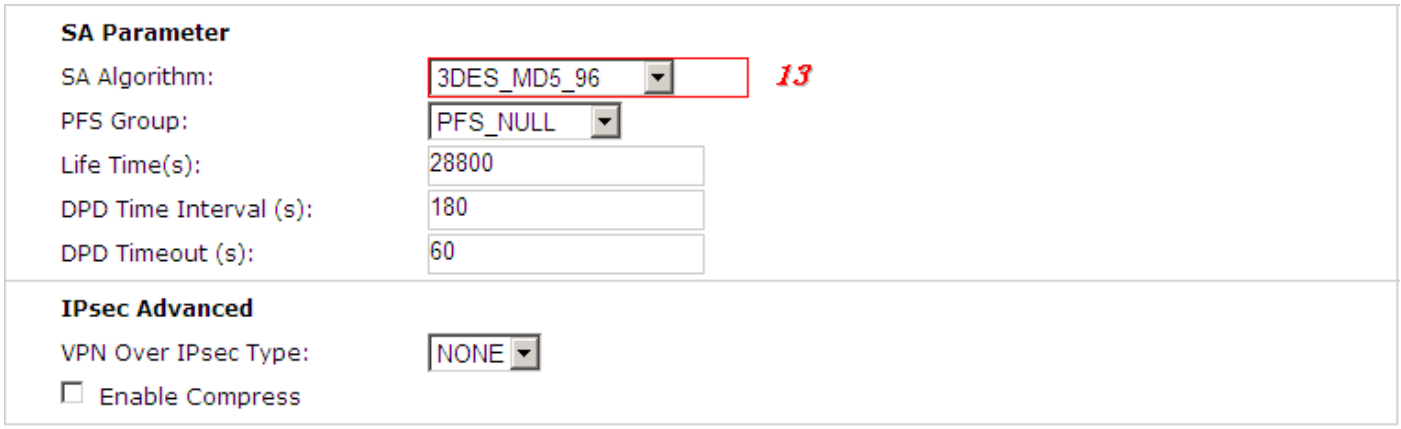
Then click “Apply”.

Configuration--->IPSec--->IPSec Tunnel



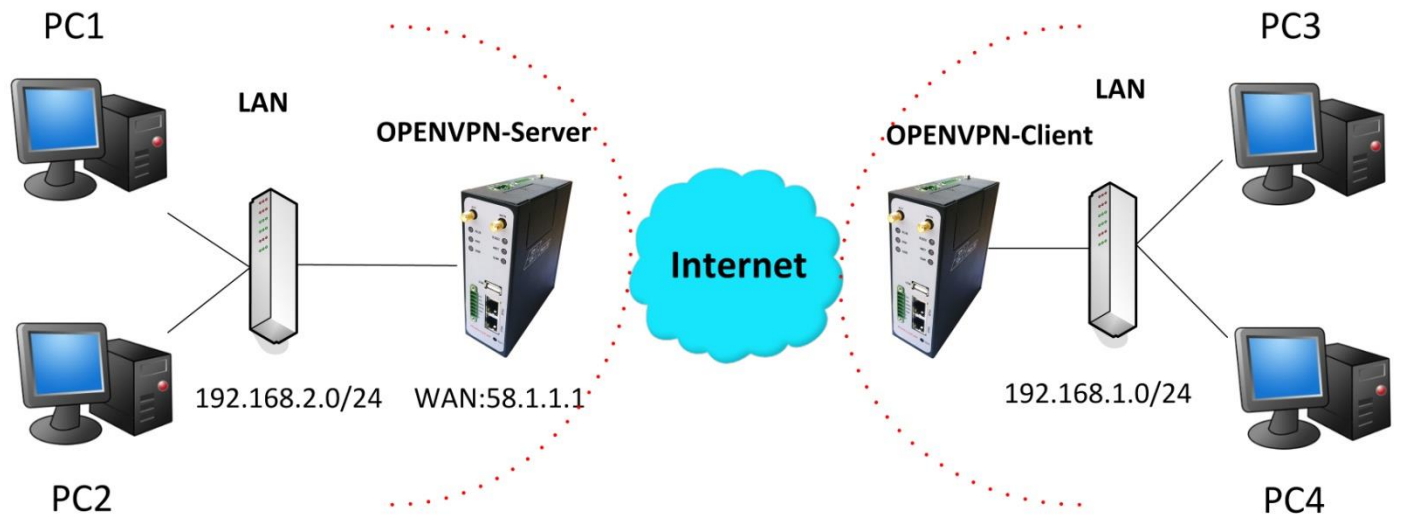
Tick “Enable IPSec Tunnel1”





The modification will take effect after "Apply-->Save-->Reboot".

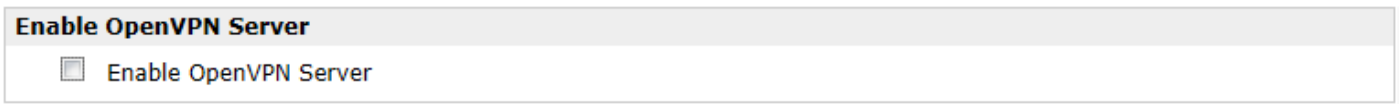
4.3.5 OPENVPN



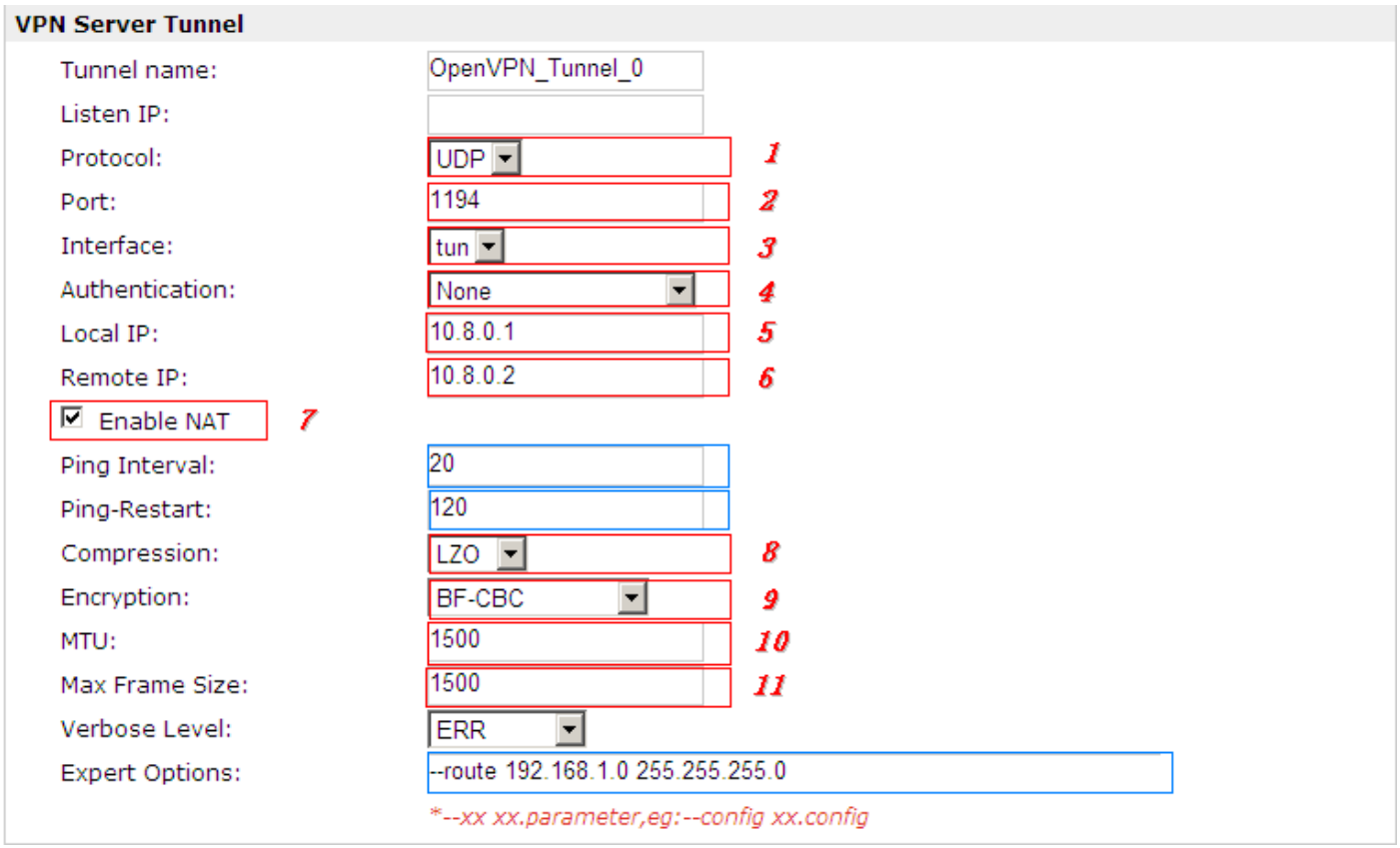
Note: *The following diagrams with red color numbers mean these are the matches between server and client, and with the blue color number means it must be set locally for the tunnel.*

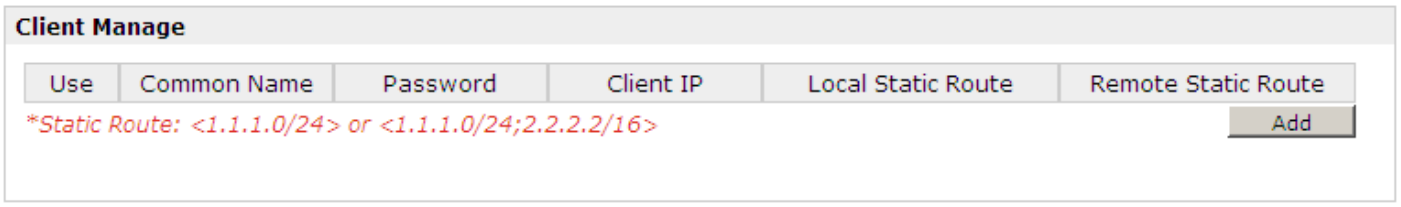
OPENVPN_SERVER:

Configuration--->OpenVPN--->Server



Tick "Enable OpenVPN Server".



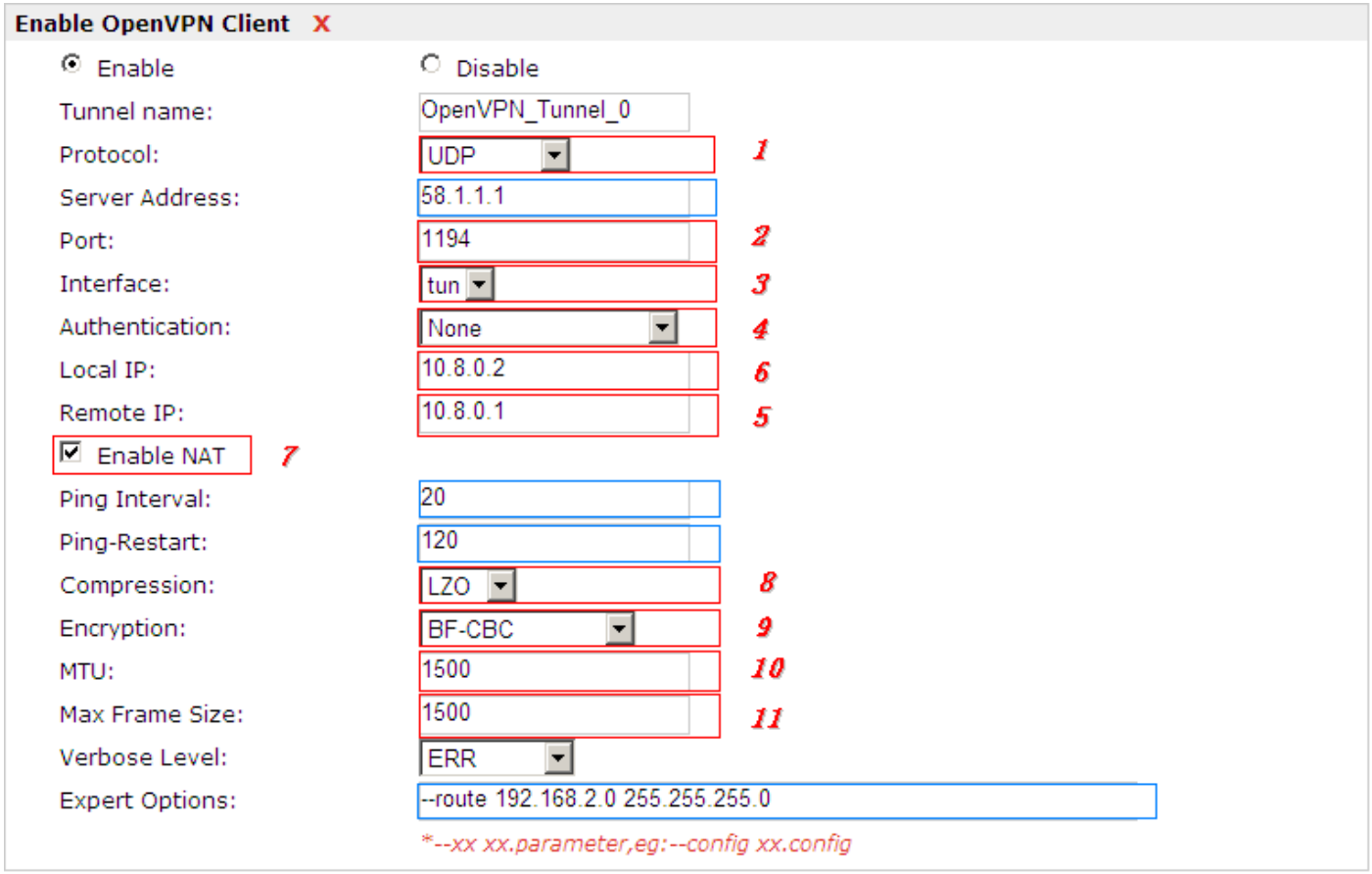


The modifications will take effect after click “Apply-->Save-->Reboot”.

OPENVPN_CLIENT:

Configuration--->OpenVPN--->Client

Tick “Enable OpenVPN Client1”, and fill in the blank textbox



The modification will take effect after “Apply-->Save-->Reboot”.

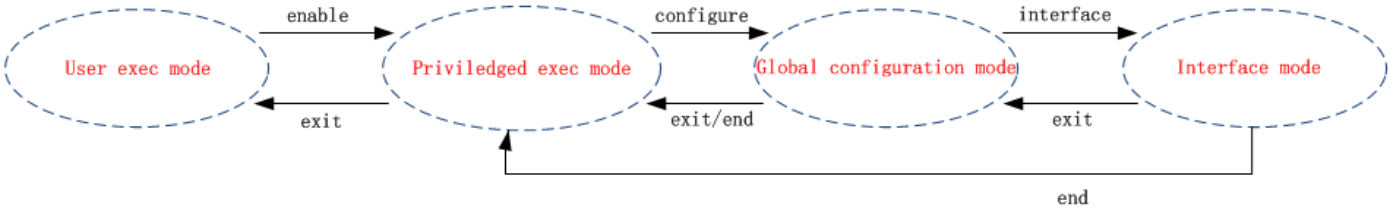
Chapter 5. Introductions for CLI

5.1 What's CLI and hierarchy level Mode

The R3000-3P command-line interface (CLI) is a software interface providing another way to set the parameters of equipment from the console or through a telnet network connection. Before using them better a few of details will be introduced on four different CLI hierarchy level modes which have different access rights:

- User exec mode—The command prompt ">" shows you are in the user mode , in this mode user can only use some simple commands to see the current configuration and the status of the device, or enter the "ping" command to troubleshoot the network connectivity.
- Privileged exec mode—When you enter Privileged mode ,the prompt will change to "#" which user can do not only what is allowed in the user exec mode but also the new additions like importing and exporting for files , system log , debug and so on .
- Global configuration mode—The global configuration mode with prompt "<config>#" allows user to add, set,modify and delete current configuration .
- Interface mode—Prompt "<config-xx>" means in this mode we can set both IP address and mtu for this interface.

Following is a relationship diagram about how to access or quit among the different modes :



USER EXEC MODE:

R3000-3P Configure Environment

Username: admin

Password: *****

R3000> ? //check what commands can be used in **user exec mode**

enable	Turn on privileged commands
exit	Exit from current mode
ping	Ping test
reload	Halt and perform a cold restart
tracert	Tracert test
show	Show running system information

PRIVILEDGED EXEC MODE:

```
R3000> enable
Password: *****
R3000# ?                    //check what commands can be used in Privileged exec mode
  debug                      Debug configure information
  enable                     Turn on privileged commands
  exit                       Exit from current mode
  export                     Export file using tftp
  syslog                     Export system log
  import                     Import file using tftp
  load                       Load configure information
  ping                       Ping test
  reload                     Halt and perform a cold restart
  tracert                    Tracert test
  write                      Write running configuration
  tftp                       Copy from tftp: file system
  show                       Show running system information
  configure                  Enter configuration mode
  end                        Exit to Normal mode
```

GLOBAL CONFIGURATION MODE:

```
R3000# configure
R3000(config)# ?            //check what commands can be used in global configuration mode
  exit                       Exit from current mode
  end                        Exit to Normal mode
  interface                  Configure an interface
  set                        Set system parameters
  add                        Add system parameters list
  modify                     Modify system parameters list
  delete                     Delete system parameters list
```

INTERFACE MODE:

```
R3000(config)# interface Ethernet 0
R3000(config-e0)# ?         //check what commands can be used in interface mode
  exit                       Exit from current mode
  end                        Exit to Normal mode
  ip                         Set the IP address of an interface
  mtu                        Set the IP address of an interface
```

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.
Invalid command "xxx"	Parameters "xxx" are not supported by the system, in this case, enter a mark "?" instead of "xxx" will help to find out the correct parameters about this issue.
Incomplete command	Command is not incomplete.
% Invalid input detected at '^' marker	'^' marker indicates the location where the error is.

***Note**: Most of the parameters setting are in the **Global configuration mode**. Commands **set ,add** are very important for this mode. If some parameters can't be found in the Global configuration mode, please move back to **Privileged exec mode** or move up to **Interface mode**.*

*Note: Knowing the **CLI hierarchy level modes** is necessary before configuring the CLI. If not, please go back and read it quickly in chapter 5.*

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

```
R3000> show version
  software version : 1.01.00
  kernel version      : v2.6.39
  hardware version : 1.01.00
```

Example 2: Update firmware via tftp

```
R3000> enable
Password: *****
R3000#
R3000# tftp 172.16.3.3 get rootfs R3k.1.01.00.02_130325

Tftp transfering
tftp succeeded!downloaded
R3000# write                                    //save current configuration
```

```
Building configuration...
OK
R3000#reload
!Reboot the system?'yes'or 'no':yes                    //reload to take effect
```

Example 3: Set link-management

```
R3000> enable
Password: *****
R3000#
R3000# configure
R3000(config)# set link-management
wan link :
  1.Cellular Only
  2.Eth0 Only
  3.Eth0 as primary and if fail use Cellular
  4.Cellular as primary and if fail user Eth0
->please select mode(1-4)[1]:2                          //select “Eth0 Only” as wan-link
->ICMP detection primary server[]:8.8.8.8
->ICMP detection second server[]:8.8.8.4
->ICMP detection interval(3-1800)[30]:
->ICMP detection timeout(1-10)[3]:
->ICMP detection retries(1-20)[3]:
->reset the interface?'yes'or'no'[no]:

this parameter will be take effect when reboot!
really want to modify[yes]:
R3000# write                                            //save current configuration
Building configuration...
OK
R3000# reload
!Reboot the system ?'yes'or 'no':yes                    //reload to take effect
```

Example 4: Set IP address, Gateway and DNS for Eth0

```
R3000> enable
Password: *****
R3000#
R3000# show link-management                             //show current link-management

*******************************************
   wan link                    : Eth0 Only              // now “Eth0 Only” as wan-link
   ICMP primary server         : 8.8.8.8
   ICMP second server          : 8.8.8.4
```

```
   ICMP detection interval      : 30 seconds
   ICMP detection timeout       : 3 seconds
   ICMP detection retries       : 3
   reset the interface          : no
*****************************************

R3000 # configure
R3000 (config) # set eth0
ethernet interface type: WAN
type select:
  1.  Static IP
  2.  DHCP
  3.  PPP0E
->please select mode (1-3) [1]:
->IP address [192.168.0.1]:58.1.1.1                    //set IP address for eth0
->Netmask [255.255.255.0]:255.0.0.0
->gateway [192.168.0.254]:58.1.1.254                   //set gateway for eth0
->mtu value (1024-1500)[1500]:
->input primary DNS [192.168.0.254]:58.1.1.254         //set dns for eth0
->input secondary DNS [0.0.0.0]:

this parameter will be take effect when reboot!
really want to modify[yes]:
R3000 (config) # end
R3000# write                                           //save current configuration
Building configuration...
OK
R3000 # reload
! Reboot the system? 'yes' or 'no': yes                //reload to take effect
```

Example 5: CLI for Cellular dialup

```
R3000> enable
Password: *****
R3000#
R3000# show link-management

*****************************************
   wan link                     : Cellular Only      // now “Cellular Only” as wan-link
   ICMP primary server          : 8.8.8.8
   ICMP second server           : 8.8.8.4
   ICMP detection interval      : 30 seconds
```

```
   ICMP detection timeout       : 3 seconds
   ICMP detection retries       : 3
   reset the interface          : no
*****************************************
R3000 (config) # set cellular
  1. set SIM_1 parameters
  2. set SIM_2 parameters
->please select mode (1-2)[1]:
SIM 1 parameters:
network provider
  1. Auto
  2. Custom
  3. china-mobile
->please select mode(1-3)[1]:
->dial out using numbers[*99***1#]:
->pin code[]:
connection Mode:
  1. Always online
  2. Connect on demand
->please select mode(1-2)[1]:
->redial interval(1-120)[30]:
->max connect try(1-60)[3]:
R3000(config)# end
R3000# write                                    //save current configuration
Building configuration...
OK

R3000# show      cellular
*********************************************
   Cellular enable              : yes
  1. show SIM_1 parameters
  2. show SIM_2 parameters
->please select mode(1-2)[1]:
SIM 1 parameters:
   network provider             : Auto
   dial numbers                 : *99***1#
   pin code                     : NULL
   connection Mode              : Always online
   redial interval              : 30 seconds
```

```
   max connect try                 : 3
   main SIM select                 : SIM_1
   when connect fail               : yes
   when roaming is detected    : no
   month date limitation          : no
   SIM phone number                 :
   network select Type             : Auto
   authentication type             : AUTO
   mtu value                       : 1500
   mru value                       : 1500
   asyncmap value                  : 0xffffffff
   use peer DNS                    : yes
   primary DNS                     : 0.0.0.0
   secondary DNS                   : 0.0.0.0
   address/control compression: yes
   protocol field compression: yes
   expert options                  : noccp nobsdcomp
************************************************
R3000# reload
!Reboot the system ?'yes'or 'no':yes                    //reload to take effect
```

5.3 Commands reference

commands	syntax	description
Debug	Debug *parameters*	Turn on or turn off debug function
Export	Export *parameters*	Export vpn ca certificates
Import	Import *parameters*	Import vpn ca cerfiticates
Syslog	syslog	Export log information to tftp server
Load	Load default	Restores default values
Write	Write	Save current configuration parameters
tftp	Tftp *IP-address* get {cfg|rootfs} *file-name*	Import configuration file or update firmware via tftp
Show	Show *parameters*	Show current configuration of each function , if we need to see all please using “show running ”
Set	Set *parameters* Add *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		