

Robustel GoRugged R3000-3P

Dual SIM Industrial Cellular VPN Router For UMTS Network

User Guide

Document Name: **User Guide**
Firmware : **1.01.00**
Date : **2013-05-21**
Status : **Confidential**
Doc ID : **RT_R3000-3P_v01.03**



Robustel

www.robustel.com

About This Document

This document describes hardware and software of Robustel R3000-3P, Dual SIM Industrial 3G 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 : +86-2023354618

Fax : +86-2032016426

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 UMTS products is prohibited.
- Be sure that the router will not be interfering with nearby equipment. For example: pacemakers or medical equipment. The antenna of the router should be away from computers, office equipment, home appliance, etc.
- An external antenna must be connected to the router for proper operation. Only uses approved antenna with the router. Please contact authorized distributor on finding an approved antenna.
- Always keep the antenna with minimum safety distance of 26.6 cm or more from human body. Do not put the antenna inside metallic box, containers, etc.
- RF exposure statements
 1. For mobile devices without co-location (the transmitting antenna is installed or located more than 20cm away from the body of user and nearby person)
- FCC RF Radiation Exposure Statement
 1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
 2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.
-

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

Using the router in vehicle

- Check for any regulation or law authorizing the use of UMTS 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.

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
2013-01-24	1.00	1.00	First Release.
2013-03-15	1.01	1.01	Update firmware; Add configuration examples.
2013-05-09	1.01	1.02	Update firmware; Add configuration examples.
2013-05-21	1.01	1.03	Modify application diagrams and some characters

Contents

Chapter 1.	Product Concept.....	1
1.1	Overview	1
1.2	Packing List	1
1.3	Specifications	3
1.4	Selection and Ordering Data	5
Chapter 2.	Installation.....	6
2.1	LED Indicators.....	6
2.2	Mounting the Router.....	6
2.3	Install the SIM Card and Micro SD Card	7
2.4	Connect the External Antenna (SMA Type).....	8
2.5	PIN assignment for Router	9
2.6	Grounding the Router	9
2.7	Reset Button.....	10
Chapter 3.	Configuration settings over web browser	11
3.1	Configuring PC in Windows	11
3.2	Factory Default Settings	13
3.3	Control Panel.....	14
3.4	Status -> System	15
3.5	Status -> Network.....	18
3.6	Status -> Route	18
3.7	Status -> VPN.....	19
3.8	Status -> Services	20
3.9	Status -> Event/Log	20
3.10	Configuration -> Link Management.....	21
3.11	Configuration -> Cellular WAN	22
3.12	Configuration -> Ethernet.....	27
3.13	Configuration -> Serial.....	29
3.14	Configuration -> USB	34
3.15	Configuration -> NAT/DMZ	35
3.16	Configuration -> Firewall	36
3.17	Configuration -> IP Routing	37
3.18	Configuration -> DynDNS	40
3.19	Configuration -> IPSec	40
3.20	Configuration -> Open VPN	45
3.21	Configuration -> GRE	50
3.22	Configuration -> L2TP	51
3.23	Configuration -> PPTP.....	55
3.24	Configuration -> SNMP	58
3.25	Configuration -> VRRP	59
3.26	Configuration -> AT over IP.....	60
3.27	Configuration -> Phone Book	60
3.28	Configuration -> SMS.....	61
3.29	Configuration -> Reboot	62
3.30	Configuration -> Portal	63

3.31	Configuration -> Syslog.....	64
3.32	Administration -> Profile	64
3.33	Administration -> Tools	65
3.34	Administration -> User Management.....	67
3.35	Administration -> Clock.....	68
3.36	Administration -> Update Firmware.....	69
Chapter 4.	Examples of configuration.....	70
4.1	Cellular Dial-Up	70
4.2	NAT	72
4.3	L2TP	74
4.4	PPTP.....	75
4.5	IPSEC VPN	77
4.6	OPENVPN.....	80
4.7	SMS Remote Control	82
Chapter 5.	Introductions for CLI.....	84
5.1	What's CLI and hierarchy level Mode.....	84
5.2	How to configure the CLI.....	86
5.3	Commands reference	91

Chapter 1. Product Concept

1.1 Overview

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

- Dual SIM redundancy for continuous cellular connection, supports 2G/3G.
- Antenna diversity for improved fringe performance optional.
- Two Ethernet ports, can be configured as two LANs or one LAN one WAN (supports wireless WAN and wired WAN backup).
- One RS232, one RS485, one console port, two digital inputs, two digital outputs, one high speed USB host up to 480 Mbps.
- Six LED indicators provide status and signal strength (RSSI).
- Wide range input voltages from 9 to 60 VDC and wide range operating temperature: -25 to 65 °C.
- The metal enclosure can be mounted on a DIN-rail or on the wall, also with extra ground screw.
- Network protocols such as PPP, PPPoE, TCP, UDP, DHCP, ICMP, NAT, DMZ, RIP, OSPF, DDNS, VRRP, HTTP, HTTPS.
- VPN tunnel: IPSec/OpenVPN/PPTP/L2TP client/server, GRE.
- Management via Web, CLI, SNMP.
- Supports Modbus/RTU to Modbus/TCP gateway.
- Auto reboot during a preset time of a day.
- Firmware upgrade via web interface.

1.2 Packing List

Check your package to make certain 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 1



- 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: UMTS
 - HSUPA: 900/2100 or 850/1900 MHz optional, DL/UL 7.2/5.76 Mbps, fallback to 2G
 - SIM: 2 x (3V & 1.8V)
 - Antenna Interface: SMA Female, 50 ohms impedance
- ### **Ethernet Interface**
- Number of Ports: 2 x 10/100 Mbps, 2 LANs or 1 LAN 1 WAN
 - Magnet Isolation Protection: 1.5KV

Serial Interface

- Number of Ports: 1 x RS-232, 1 x RS-485
- ESD Protection: 15KV
- Parameters: 8E1, 8O1, 8N1, 8N2, 7E2, 7O2, 7N2, 7E1
- Baud Rate: 2000bps to 115200bps
- Flow Control: RTS/CTS, XON/XOFF
- 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: short to GND, Off: open
- Isolation: 3K VDC or 2K Vrms
- Digital Filtering Time Interval: Software selectable
- Over-voltage Protection: 36 VDC
- Interface: 3.5mm terminal block with lock

Digital Output

- Type: 2 x DO, Sink
- Over-voltage Protection: 40 VDC
- Over-current Protection: 0.5 A
- Isolation: 3K VDC or 2K Vrms
- Interface: 3.5mm terminal block with lock

System

- LED Indicators: 6 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, can expand up to 32G

Software

- Network protocols: PPP, PPPoE, TCP, UDP, DHCP, ICMP, NAT, DMZ, RIP v1/v2, OSPF, DDNS, VRRP, HTTP, HTTPS, DNS, ARP, SSH, SNTP, Telnet
- LinkGo: PPP LCP Echo/Reply, ICMP to keep always online
- VPN tunnel: IPSec/OpenVPN/PPTP/L2TP, GRE
- Firewall: SPI, anti-DoS, Filter, Access Control
- Management: Web, CLI, Telnet, SNMP v1/v2/v3
- Serial Port: TCP client/server, UDP, Virtual COM

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: 500 to 1000 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: -25 to 65°C, 5 to 95% RH
- Storage Temperature: -40 to 85°C

Regulatory and Type Approvals

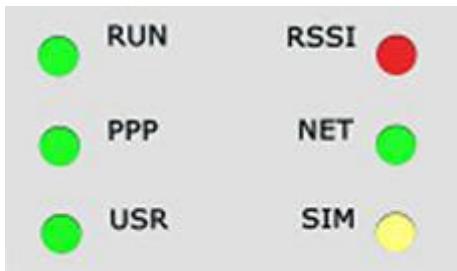
- Approval & Detective: CE, FCC, PTCRB, A-Tick, RoHS, WEEE
- EMC: EN 61000-4-2 (ESD) Level 4, EN 61000-4-3 (RS) Level 4
EN 61000-4-4 (EFT) Level 4, EN 61000-4-5 (Surge) Level 3
EN 61000-4-6 (CS) Level 3, EN 61000-4-8, EN 61000-4-12

1.4 Selection and Ordering Data

Please refer to corresponding R3000-3P datasheet.

Chapter 2. Installation

2.1 LED Indicators



Name	Color	Function
RUN	Green	Indicating the system status. Blinking: Router is ready. On: Router is starting. Off: Router is power off.
PPP	Green	Indicating the PPP connection status. On: PPP connection is established. Off: PPP connection is failed.
USR	Green	Indicating the VPN status. On: VPN tunnel is established. Off: No VPN tunnel.
RSSI	Green	Signal level: 21-31 (Perfect signal level)
	Yellow	Signal level: 11-20 (Normal signal level)
	Red	Signal level: 1-10 (Bad signal level)
NET		
	Yellow	Working under 3G network.
SIM	Green	2 SIM cards are inserted.
	Yellow	Only SIM 1 is inserted.
	Red	Only SIM 2 is inserted.

2.2 Mounting the Router

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



Or to mount the router on a DIN rail, you need three pcs of M3 screws.



2.3 Install the 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

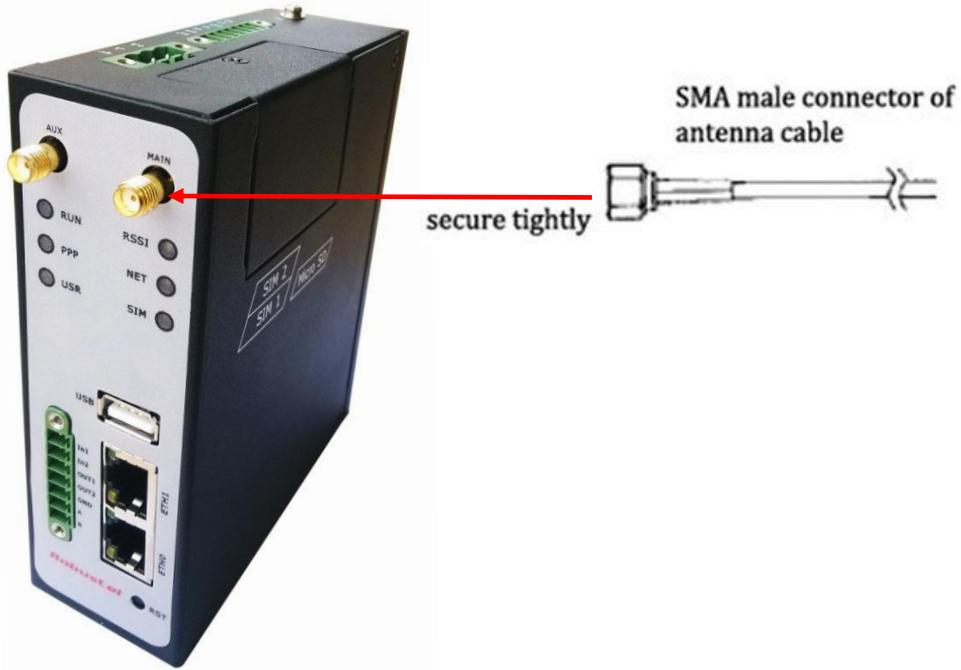
1. Make sure your charger is disconnected, and then press and hold down the power key until the *router* is powered off.
2. Press the card until you hear “a cracking sound”, when the card will pop up to be pulled out.

Note:

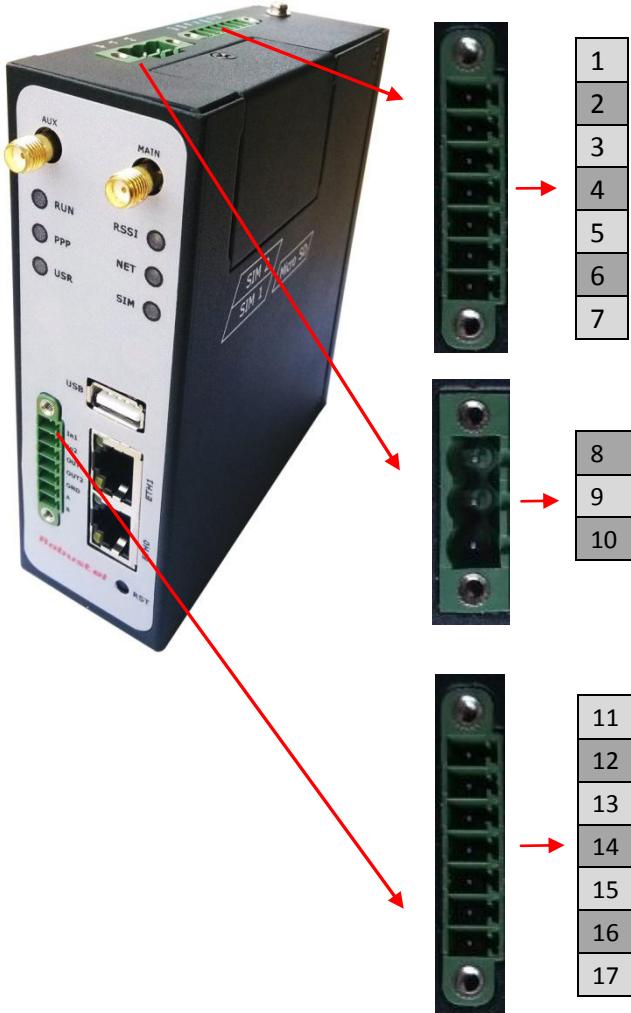
1. *Don't forget screw the cover for again-theft.*
2. *Don't touch the metal surface of the SIM card in case information in the card is lost or destroyed.*
3. *Don't bend or scratch your SIM card. Keep the card away from electricity and magnetism.*
4. *Make sure to disconnect the power source from your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

2.4 Connect the External Antenna (SMA Type)

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



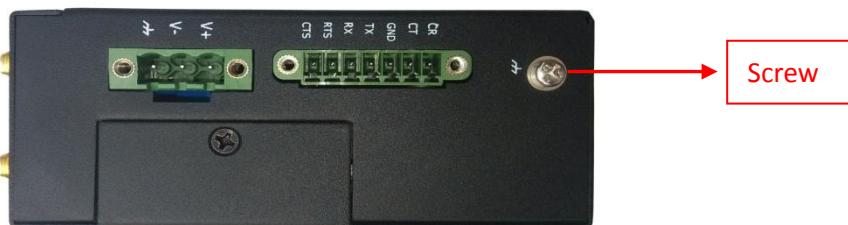
2.5 PIN assignment for Router



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)

Note: The power supply range is 12 to 70VDC. Please take care about the polarity, and do not make reverse connection.

2.6 Grounding 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.

2.7 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.

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.

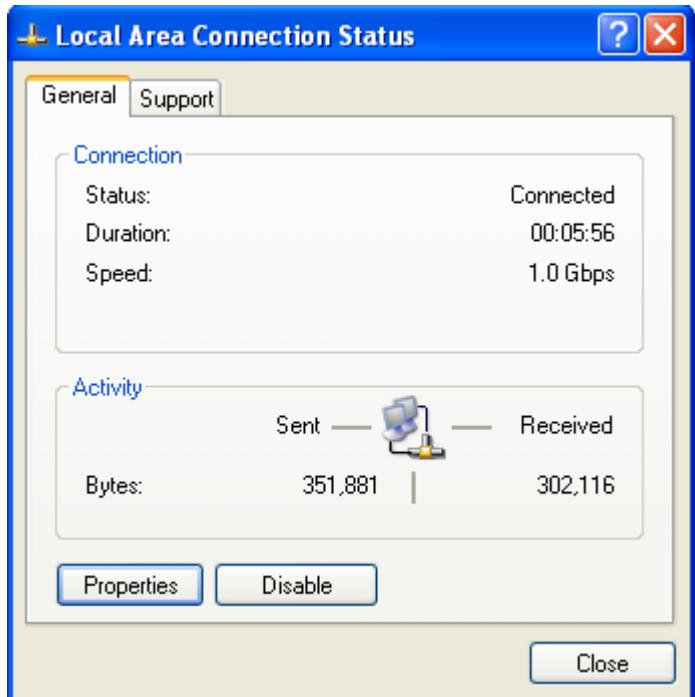
You must configure your PC to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problems accessing the router 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

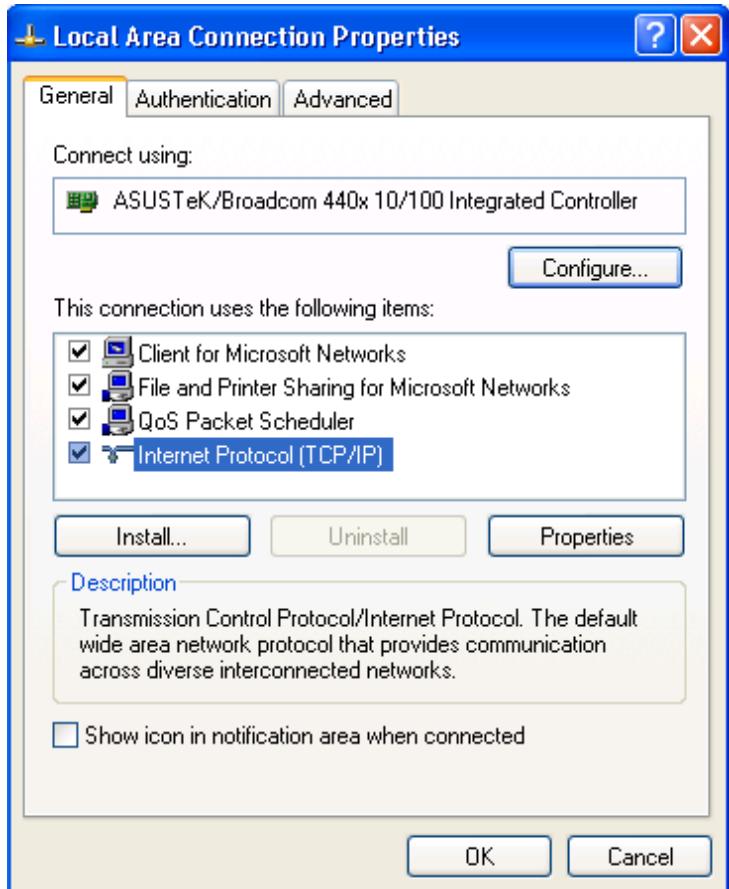
1. Go to Start / Control Panel (in Classic View). In the Control Panel, double-click Network Connections.
2. Double-click Local Area Connection.



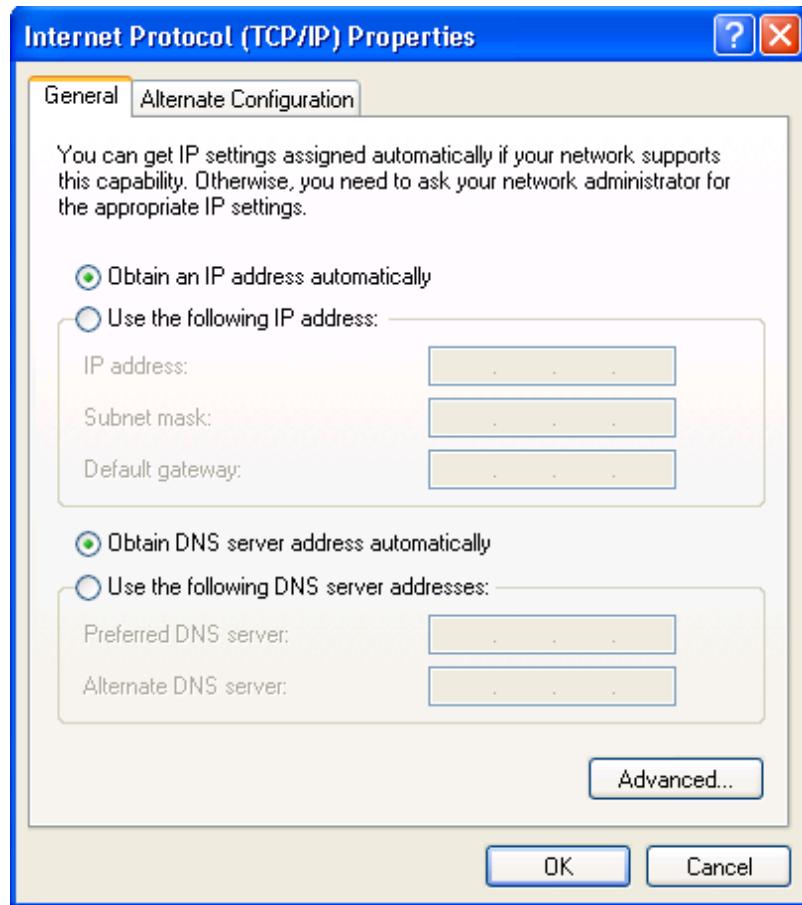
3. In the Local Area Connection Status window, click Properties.



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.

User authentication required. Login please.

Username:	<input type="text" value="admin"/>
Password:	<input type="password" value="*****"/>
Language:	English <input type="button" value="▼"/>

Please enter your login username and password.

3.3 Control Panel

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

Robustel

• Save • Reboot • Logout • English ▾
Logged in as: admin

Status	System
System	RUN: GREEN/BLINK PPP: OFF USR: GREEN/ON
Network	RSSI: OFF NET: OFF
Route	SIM: YELLOW/ON
VPN	
Services	
Event/Log	
Configuration	Router Information
Link Management	Device Model: Serial Number: robustel sn Device Name: Cellular Router Firmware Version: 1.01.00 Hardware Version: 1.01.00 Kernel Version: 2.6.39-4 Radio Module Type: BGS2 Radio Firmware Version: Uptime: 0 days 00:15:38 CPU Load: 09.64% RAM Total/Free: 123.10MB/74.90MB(60.84%) System Time: 2007-01-02 02:19:28
Ethernet	
Serial	
USB	
NAT/DMZ	
Firewall	
IP Routing	
DynDNS	
IPsec	
OpenVPN	
GRE	
L2TP	
PPTP	
SNMP	
VRRP	
AT over IP	
Phone Book	

Copyright © 2013 Robustel Technologies. All rights reserved.

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, Spanish.	• English ▾
Help	Click to get some help from our website.	• Help
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 2.2 LED Indicators.

LEDs Information			
RUN:	GREEN/BLINK	RSSI:	RED/ON
PPP:	GREEN/ON	NET:	RED/ON
USR:	OFF	SIM:	RED/ON

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

Router Information

Device Model:	R3000
Serial Number:	robustel sn
Device Name:	Cellular Router
Firmware Version:	1.01.00
Hardware Version:	1.01.00
Kernel Version:	2.6.39-3
Radio Module Type:	EM770W
Radio Firmware Version:	11.126.10.87.809
Uptime:	0 days 06:37:42
CPU Load:	00.00%
RAM Total/Free:	123.11MB/72.60MB(58.97%)
System Time:	2013-03-13 14:56:16

Current WAN Link

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

Current WAN Link	
Current WAN Link:	Cellular
IP Address:	10.138.108.79
Gateway:	192.168.254.254
NetMask:	255.255.255.255
DNS Server:	210.21.4.130 221.5.88.88
Keepalive PING IP Address:	
Keepalive PING Interval:	30

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, such as "ready", "unknown". This tab allow user to check whether router has dialed up to network (modem function).
Network Status	Show the current network status. There are 5 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.
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.

Cellular Information

Current SIM:	
Phone No.:	
SMS Service Center:	SIM
Modem Status:	Unknown
Network Status:	Not registered, ME is currently not searching for new operator
Signal Level (RSSI):	 (0,-113DB)
Network Operator:	(LAC: / Cell ID:)
Network Service Type:	Unknown
IMEI/ESN:	357789044494414
IMSI:	SIM failure
USB Status:	Ready

3.5 Status -> Network

This section displays the router's Network status, which include status of Cellular WAN, LAN0 and LAN1.

Eth0 WAN

Connection Mode:	Static IP
IP Address:	172.16.2.113
Mac Address:	00:ff:74:46:dc:e1
MTU:	1500
Gateway:	0.0.0.0
NetMask:	255.255.0.0
Primary DNS Server:	0.0.0.0
Secondary DNS Server:	0.0.0.0

LAN1

IP Address:	192.168.1.1
Mac Address:	00:ff:74:46:dc:e2
MTU:	1500
NetMask:	255.255.255.0

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.

Route Table

Destination	NetMask	Gateway	Interface	Metric
172.16.0.0	255.255.0.0	0.0.0.0	eth0	0
192.168.1.0	255.255.255.0	0.0.0.0	eth1	0

3.7 Status -> VPN

This section displays the router's VPN status, including IPsec, L2TP, PPTP, OpenVPN and GRE.

IPsec**L2TP****PPTP****OpenVPN****IPsec Status**

No.	Tunnel name	Status	Connect Time
1		LINK_DOWN	
2		LINK_DOWN	
3		LINK_DOWN	

IPsec Detail Status[Show Detail Status](#)**IPsec****L2TP****PPTP****OpenVPN****L2TP Client**

No.	Tunnel name	Status	Local IP	Remote IP	Connect Time

L2TP Server

No.	Tunnel name	Status	Local IP	Remote IP	Connect Time

IPsec**L2TP****PPTP****OpenVPN****PPTP Client**

No.	Tunnel name	Status	Local IP	Remote IP	Connect Time

PPTP Server

No.	Tunnel name	Status	Local IP	Remote IP	Connect Time

IPsec**L2TP****PPTP****OpenVPN****VPN Status**

No.	Tunnel name	Status

IPsec	L2TP	PPTP	OpenVPN	GRE	
GRE					
No.	Tunnel name	Status	Local IP	Remote IP	Connect Time

3.8 Status -> Services

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

VRRP	DynDNS	Serial
VRRP		
VRRP Status:	Backup	
Group ID:	1	
Priority:	100	
Interval (s):	10	
Virtual IP:	192.168.0.1	

VRRP	DynDNS	Serial
DynDNS		
DynDNS is disabled!		

VRRP	DynDNS	Serial			
RS232: 115200, N, 8, 1					
Protocol:transparent					
TCP server <table border="1"> <tr> <td>Server IP</td> <td>Server Port</td> <td>Status</td> </tr> </table>			Server IP	Server Port	Status
Server IP	Server Port	Status			
RS485: 115200, N, 8, 1					
Protocol:transparent					
TCP server <table border="1"> <tr> <td>Server IP</td> <td>Server Port</td> <td>Status</td> </tr> </table>			Server IP	Server Port	Status
Server IP	Server Port	Status			

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 tab 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.

Event/Log Messages

Download:	--Please Select--
Log Level:	DEBUG
<pre>07-01-05 09:44:49 <0> router: Firmware version: 1.01.00 May 6 2013 11:21:32 07-01-05 09:44:49 <0> router: start dhcpcd 07-01-05 09:44:53 <0> router: snmpd start up. Starting to process data. 07-01-05 09:44:53 <1> Quagga: Zebra 0.99.21 starting: vty@9888 07-01-05 09:44:54 <4> router: no sim card insert</pre>	

Download System Diagnosing Data

<input type="button" value="Download System Diagnosing Data"/>
--

3.10 Configuration -> Link Management

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

Link Management		
Item	Description	Default
WAN Link	<p>Selected from “Cellular Only”, “Eth0 Only”, “Eth0 as primary and if fail use cellular” and “Cellular as primary and if fail use Eth0”.</p> <ol style="list-style-type: none"> 1. Cellular Only: Select to make cellular as the only WAN link. 2. Eth0 Only: Select to make Eth0 as the only WAN link 3. Eth0 as primary and if fail use cellular: Select to make Eth0 as the primary WAN link and cellular as the secondary WAN link. 4. Cellular as primary and if fail use Eth0: Select to make cellular as the primary WAN link and Eth0 as the secondary WAN link. 	Cellular Only
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 time.	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

Link Management Settings

WAN link:	Eth0 Only
ICMP Detection Primary Server:	8.8.8.8
ICMP Detection Secondary Server:	8.8.4.4
ICMP Detection Interval (s):	30
ICMP Detection Timeout (s):	3
ICMP Detection Retries:	3

Reset The Interface

*It is recommended to use an ICMP detection server to keep router always online.

*The ICMP detection increases the reliability and also cost data flow.

*DNS example: Google DNS Server 8.8.8.8 and 8.8.4.4

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 @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 code request	<p>After click this button, you could input your SIM's PIN and store the current PIN in its memory, and then enter the PIN automatically each time the system boots up.</p> <p>Note: Please ask your local ISP to see whether your SIM card requiring PIN or not.</p> <p>If you want to change the SIM PIN, please click the button to enable it, and then input the new PIN.</p>	Null
Connection Mode		
Connection Mode	<p>Select from "Always Online" and "Connect On Demand".</p> <p>Always Online: Router will automatically establish a 3G connection after power on and each restarts, this will remain and will be re-established after an interruption.</p> <p>Connect On Demand: After selection this option, user could configure Triggered by Serial Data, Triggered by Periodically Connect and Triggered by Time Schedule.</p> <p>Note: If you select several connect on demand policies, router only have to meet one of them to be triggered.</p>	Connect On Demand
Redial Interval	Router will automatically re-connect with this interval when it fails communicating to peer via TCP or UDP	30
Max Retries	<p>The maximum retries times for automatically re-connect when router fails to dial up.</p> <p>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.</p> <p>When connecting successful, the Max Retries counter will be set to 0.</p>	3
Inactivity Time	<p>You can configure this field after setting router under "Connect On Demand" mode.</p> <p>This field specifies the idle time setting for 3G auto-disconnection and trying to revert back to preferred SIM card.</p> <p>0 means timeless.</p>	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 automatic connects to cellular network from idle mode when there is data come out from serial port.	Enable
Triggered by Tel	Tick this check box to allow router automatic 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 automatic 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 connect 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
Periodically Connect	Tick this check box to allow router automatically connects to cellular network with preset interval which you preset in <i>Periodically Connect Interval</i> .	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 ICMP Detection fails	Router will switch to another SIM card if it cannot dialup or ping the preset address timeout continuously for Max Retries time,	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 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".

Cellular Settings		
	SIM1	SIM2
Status:	Not Ready	Not Ready
Network Provider Type:	Auto <input type="button" value="▼"/>	Auto <input type="button" value="▼"/>
APN:		
Username:		
Password:		
Dialup No.:	*99***1#	*99***1#
PIN code request:	<input type="button" value="Set PIN Code"/>	<input type="button" value="Set PIN Code"/>

Connection Mode

Connection Mode:	<input style="width: 100px; height: 25px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 10px; font-size: 12px; color: inherit; background-color: inherit;" type="button" value="Connect on demand"/>
Redial Interval (s):	<input type="text" value="30"/>
Max Retries:	<input type="text" value="3"/>
Inactivity Time (s):	<input type="text" value="0"/>
Serial Output Content (Hex):	<input type="text"/>
<input checked="" type="checkbox"/> Triggered by Serial Data <input checked="" type="checkbox"/> Triggered by Tel <input checked="" type="checkbox"/> Triggered by SMS	
SMS Connect command:	<input type="text"/>
SMS disconnect command:	<input type="text"/>
SMS connect reply:	<input type="text"/>
SMS disconnect reply:	<input type="text"/>
Phone Group:	<input style="width: 100px; height: 25px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 10px; font-size: 12px; color: inherit; background-color: inherit;" type="button" value="NULL"/> Click to add PhoneGroup!
<input checked="" type="checkbox"/> Periodically connect	
Periodically connect interval (s):	<input type="text" value="300"/>
Time schedule:	<input style="width: 100px; height: 25px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 10px; font-size: 12px; color: inherit; background-color: inherit;" type="button" value="NULL"/>

Time Range

Name	SUN	MON	TUE	WED	THU	FRI	SAT	Time Range1	Time Range2	Time Range3
schedule_1	<input checked="" type="checkbox"/>	08:10-12:00	14:10-20:15	X						

Dual SIM Policy

Main SIM Card:	<input type="button" value="SIM1 ▾"/>	
<input checked="" type="checkbox"/> Switch to backup SIM card when connection fails <input checked="" type="checkbox"/> Switch to backup SIM card when ICMP Detection fails <input checked="" type="checkbox"/> Switch to backup SIM card when roaming is detected		
Preferred PLMN:	<input type="text"/>	
<input checked="" type="checkbox"/> Switch to backup SIM card when data limit is exceeded		
Max Data Limitation (MB):	<input type="text" value="100"/>	<input type="text" value="100"/>
Date of Month to clean:	<input type="text" value="1"/>	<input type="text" value="1"/>
Already used (KB):	<input type="text" value="0"/>	<input type="text" value="0"/>
	<input type="button" value="Clear"/>	<input type="button" value="Clear"/>
<input checked="" type="checkbox"/> Switch back Main SIM card after timeout		
Initial Timeout (min):	<input type="text" value="60"/>	

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.	UMTS
MRU	Maximum Receiving Unit. It is the identifier of the maximum size of packet, which is possible to receive in a given environment.	Auto
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 Compression Field	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 can be separated by a space.	noccp nobsdcomp

Cellular Advanced Settings

	SIM1	SIM2
Phone No.:	<input type="text"/>	<input type="text"/>
Authentication:	Auto <input type="button" value="▼"/>	Auto <input type="button" value="▼"/>
MTU:	1500	1500
MRU:	1500	1500
Asyncmap Value:	fffffff	fffffff
Use Peer DNS:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Primary DNS Server:	<input type="text"/>	<input type="text"/>
Secondary DNS Server:	<input type="text"/>	<input type="text"/>
Address/Control Compression:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Protocol Field Compression:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Expert Options:	<code>noccp nobsdcomp</code>	

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".

Cellular WAN @ Basic		
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

ISP Profile List

ISP	APN	Username	Password	Dialup No.
CMMC	cmnet			*99***1# X

3.12 Configuration -> Ethernet

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

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 @ LAN Interface	Set the IP address, Netmask and MTU of Eth0/Eth1. These parameters will be un-configurable if you enable Bridge.	Null
Multiple IP Address @	Assign multiple IP addresses for Eth0/Eth1.	Null

LAN Interface		
Enable DHCP Server @ DHCP Server	Enable to make router can lease IP address to DHCP clients which connect to Eth0/Eth1.	Enable
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.	192.168.0.2/ 192.168.0.10 0
Netmask @ DHCP Server	Define the Netmask which the DHCP clients will obtain from DHCP server.	255.255.255. 0
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.	192.168.0.1/ 0.0.0.0
Windows Name Server @ DHCP Server	Define the WINS Server which the DHCP clients will obtain from DHCP server.	192.168.0.1
Static Lease @ DHCP Server	Define to lease static IP Addresses, which conform to MAC Address of the connected equipment.	Null

Ethernet Interface Type

LAN WAN

LAN Interface

Enable Bridge (As 2 Ports Switch)

IP Address:	192.168.0.1
NetMask:	255.255.255.0
MTU:	1500

Multiple IP Address

IP Address	NetMask
<input type="button" value="Add"/>	

DHCP Server

<input checked="" type="checkbox"/> Enable DHCP Server	
IP Pool Start:	192.168.0.2
IP Pool End:	192.168.0.100
NetMask:	255.255.255.0
Lease Time (min):	60
Primary DNS Server:	192.168.0.1
Secondary DNS Server:	
Windows Name Server:	192.168.0.1

Static Lease

MAC Address	IP Address
*MAC: ff:ff:ff:ff:ff:ff	Add

3.13 Configuration -> Serial

This section allows users to set the serial parameters.

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" and "AT Over COM". 1. Transparent: Router will transmit the serial data transparently without any protocols. 2. Modbus: Router will transfer the serial data into Modbus TCP protocol. 3. AT Over COM: select to operate router via RS232 COM port. For example, enter AT commands to router via RS232 COM port.	None
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".	None

show Advanced	Protocol @	Tick to enable protocol advanced setting.	Disable
---------------	------------	---	---------

Transparent		
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 Delimiter1/2	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 Port @Modbus	Enter the Local port for Modbus.	0
Attached serial device type @Modbus	Select From "Modbus RTU slave", "Modbus ASC II slave", "Modbus RTU master" and "Modbus ASC II master". Modbus RTU slave: router connects to slave device which works under Modbus RTU protocol. Modbus ASC II slave: router connects to slave device which works under Modbus ASC II protocol. Modbus RTU master: router connects to master device which works under Modbus RTU protocol. Modbus ASC II master: router connects to master device which works under Modbus ASC II protocol.	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 ASC II master" in "Attached serial device type".	Null
Slave Address	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	Enter the port number of TCP server.	Null
ID	Enter the ID number of TCP server.	Null
Display all com @ AT	Enable to display all virtual com of the module inside the router. Generally,	Disable

Over COM	router will occupy /dev/ttyUSB0 and /dev/ttyUSB2 for dialing up to . Note: Enable this function will disable Cellular WAN function.	
COM Name	Show the virtual com name of the module inside.	/dev/tt yUSB1

Serial Port Settings

Baudrate:	115200
Data bit:	8
Parity:	None
Stop bit:	1
Flow control:	None

When Select Transparent Protocol:

Protocol Settings

Protocol:	Transparent
Mode:	TCP server
Local Port:	502
<input checked="" type="checkbox"/> Show Protocol Advanced	
Interval Timeout (1*10ms):	10
Packet Length:	1360
<input checked="" type="checkbox"/> Enable Delimiter1	
Delimiter1 (Hex):	0
<input checked="" type="checkbox"/> Enable Delimiter2	
Delimiter2 (Hex):	0
Delimiter Process:	Strip

When Select Modbus Protocol:

Protocol Settings

Protocol:	Modbus
Local Port:	0
Attached serial device type:	Modbus RTU master

Modbus Slave

Slave Address	Slave Port	ID
*ID:<1-247> or <1-247>-<1-247>		
		Add

When Select AT Over COM Protocol:

Protocol Settings	
Protocol:	AT Over COM <input type="button" value="▼"/>
<input checked="" type="checkbox"/> Display all com (Note enable this function will disable cellular WAN.)	
COM Name:	/dev/ttys1 <input type="button" value="▼"/>

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
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	Disable
-------------------	--	---------

	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.	
Delimiter1 (Hex) @ Transparent	Enter the delimiter in Hex.	0
Delimiter Process @ Transparent	<p>The Delimiter process field determines how the data is handled when a delimiter is received.</p> <p>None: Data in the buffer will be transmitted when the delimiter is received; the data also includes the delimiter characters.</p> <p>Strip: Data in the buffer is first stripped of the delimiter before being transmitted.</p>	Strip
Local Port @ Modbus	Enter the Local port for Modbus.	0
Attached serial device type @Modbus	<p>Select From “Modbus RTU slave”, “Modbus ASC II slave”, “Modbus RTU master” and “Modbus ASC II master”.</p> <p>Modbus RTU slave: router connects to slave device which works under Modbus RTU protocol.</p> <p>Modbus ASC II slave: router connects to slave device which works under Modbus ASC II protocol.</p> <p>Modbus RTU master: router connects to master device which works under Modbus RTU protocol.</p> <p>Modbus ASC II master: router connects to master device which works under Modbus ASC II protocol.</p>	
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 ASC II master” in “Attached serial device type”.	Null
Slave Address	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	Enter the port number of TCP server.	Null
ID	Enter the ID number of TCP server.	Null

Serial Port Settings

Baudrate:	115200
Data bit:	8
Parity:	None
Stop bit:	1

Protocol Settings

Protocol:	Transparent <input type="button" value="▼"/>
Mode:	TCP client <input type="button" value="▼"/>
Local Port:	503

Multiple Server

Server IP	Server Port	Send data to Serial
<input type="text"/>	<input type="text"/>	<input checked="" type="checkbox"/> X

Show Protocol Advanced

Interval Timeout (1*10ms):

Packet Length:

Enable Delimiter1

Delimiter1 (Hex):

Enable Delimiter2

Delimiter2 (Hex):

Delimiter Process:

Protocol Settings

Protocol:	Modbus <input type="button" value="▼"/>
Local Port:	0 <input type="text"/>
Attached serial device type:	Modbus RTU master <input type="button" value="▼"/>

Modbus Slave

Slave Address	Slave Port	ID
<i>*ID:<1-247> or <1-247>-<1-247></i> <input type="button" value="Add"/>		

3.14 Configuration -> USB

This section allows users to set the USB parameters.

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

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 Configuration

- Enable automatic update of configuration
- Enable automatic update of firmware

3.15 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

Port Forwarding

Remote IP	Arrives At Port	Is Forwarded to IP Address	Is Forwarded to Port	Protocol
				TCP <input checked="" type="button"/>

*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>

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

Enable DMZ

- Enable DMZ

DMZ Settings

DMZ Host:

Source Address:

*1.1.1.1", "1.1.1.1/24", "1.1.1.1-2.2.2.2", "0.0.0.0" means any

3.16 Configuration -> Firewall

This section allows users to set the firewall parameters.

Filter Basic Settings @ 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

Filter Basic Settings

- Remote Access Using HTTP
- Remote Access Using TELNET
- Remote Access Using SNMP
- Remote Ping Request
- Defend DoS Attack

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	Null

	Port.	
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.

Default Filter Policy

Accept Drop

Add Filter List

Action	Source IP	Source Port	Target IP Address	Target Port	Protocol	
Accept					TCP	<input type="button" value="Add"/> X

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

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

Mac-IP Bounding @ 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

MAC-IP Bounding List

MAC Address	IP Address

X

*MAC: ff:ff:ff:ff:ff:ff

3.17 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

Static Route Table

Interface	Destination	NetMask	Gateway
WAN			X
<input type="button" value="Add"/>			

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 Setting	Tick to enable RIP function.	Disable
RIP Protocol Version	Select from "RIPv1" and "RIPv2".	RIPv1
Neighbor IP	If you input this neighbor IP, router will only send RIP request message 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

RIPIpv4 Enabled

Enable RIP Protocol Setting

RIP Protocol Version

RIPv1 RIPv2

RIP Protocol common Settings

Neighbor IP:	<input type="text"/>
Update time(s):	<input type="text" value="30"/>
Timeout(s):	<input type="text" value="180"/>
Garbage(s):	<input type="text" value="120"/>

RIP protocol Advance Setting

Enable Advance

default Metric:	<input type="text" value="1"/>
Distance:	<input type="text" value="120"/>
Passive:	<input style="width: 50px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;" type="text" value="None"/> <input type="button" value="▼"/>
<input type="checkbox"/> Enable Default origination	
<input type="checkbox"/> Enable Redistribute Connect	
<input type="checkbox"/> Enable Redistribute Static	
<input type="checkbox"/> Enable Redistribute Ospf	

Network List

<input style="width: 150px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;" type="text"/> Network Address	<input style="width: 150px; height: 20px; border: 1px solid #ccc; border-radius: 5px; padding: 2px 5px;" type="text"/> NetMask
--	--

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

OSPF Protocol

Enable OSPFv2

3.18 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 hostmen, 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.	DynDNS–Dynamic
hostmen	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
Force Update	Click to the update and use the DynDNS settings.	Null
DynDNS Status	Show current status of DynDNS	Null

DynDNS Settings

<input checked="" type="checkbox"/> Enable DynDNS	
Service Type:	<input type="button" value="DynDNS-Dynamic"/>
Hostname:	<input type="text"/>
Username:	<input type="text"/>
Password:	<input type="text"/>
	<input type="button" value="Force Update"/>
DynDNS Status:	<i>DynDNS is initializing.....</i>

3.19 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 Basic	
<input checked="" type="checkbox"/> Enable NAT Traversal	
Keepalive Interval(s):	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: Uses the ESP protocol. AH: Uses the AH protocol.	ESP
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 a 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	Main

	dynamically, the IKE negotiation mode must be aggressive. In this case, SAs can be established as long as the username and password are correct.	
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	Set the IPSec SA lifetime.	28800

Parameter	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.	
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
VPN Over IPSec Type	Select from "None", "L2TP" and "GRE". L2TP Over IPSec: Encrypt the L2TP tunnels using IPSec. GRE Over IPSec: Encrypt the GRE tunnels using IPSec.	None
Enable Compress	Tick to enable compressing the inner headers of IP packets.	Disable
Please Add IPSec Tunnel	Click Add to add IPSec Tunnel	Null

IPsec Tunnel

Tunnel name	Description	Add
-------------	-------------	-----

IPsec Tunnel

Enable

IPsec Common

IPsec Gateway Address:

IPsec Mode:

IPsec Protocol:

Local Subnet:

Local Subnet Mask:

Local ID Type:

Remote Subnet:

Remote Subnet Mask:

Remote ID Type:

IKE Parameter

Negotiation Mode:	Main <input type="button" value="▼"/>
Encryption Algorithm:	AES256 <input type="button" value="▼"/>
Authentication Algorithm:	MD5 <input type="button" value="▼"/>
DH Group:	MODP1024_2 <input type="button" value="▼"/>
Authentication:	PSK <input type="button" value="▼"/>
Secrets:	<input type="text"/>
Life Time(s):	3600 <input type="text"/>

SA Parameter

SA Algorithm:	3DES_SHA1_96 <input type="button" value="▼"/>
PFS Group:	PFS_NULL <input type="button" value="▼"/>
Life Time(s):	28800 <input type="text"/>
DPD Time Interval (s):	60 <input type="text"/>
DPD Timeout (s):	180 <input type="text"/>

IPsec Advanced

VPN Over IPsec Type:	<input type="button" value="NONE"/> <input type="button" value="▼"/>
<input type="checkbox"/> Enable Compress	

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

Authentication Manage					
Select Cert Type:	Tunnel_1				
CA:	<input type="text"/>		浏览...	Import	Export
Remote Public Key:	<input type="text"/>		浏览...	Import	Export
Local Public Key:	<input type="text"/>		浏览...	Import	Export
Local Private Key:	<input type="text"/>		浏览...	Import	Export
CRL:	<input type="text"/>		浏览...	Import	Export
Authentication Status					
Cert Type	Ca.crt	Remote.crt	Local.crt	Private.key	Crl.pem
Tunnel_1	OK	OK	OK	OK	
Tunnel_2					
Tunnel_3					

3.20 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 NAT Traversal for OpenVPN. This item must be enabled when router under NAT environment.	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

Enable OpenVPN Client

Enable

Protocol:	UDP
Remote IP Address:	
Port:	1194
Interface:	tun
Authentication:	None
Local IP:	10.8.0.2
Remote IP:	10.8.0.1
<input type="checkbox"/> Enable NAT	
Ping Interval:	20
Ping-Restart:	120
Compression:	LZO
Encryption:	BF-CBC
MTU:	1500
Max Frame Size:	1500
Verbose Level:	ERR
Expert Options:	

*--xx xx.parameter,eg:--config xx.config

Local Route

Subnet	Subnet Mask
<input type="button" value="Add"/>	

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 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.	10.8.0.1
Remote IP	Define the remote IP address of OpenVPN tunnel.	10.8.0.2
Enable NAT	Tick to enable NAT Traversal for OpenVPN. This item must be enabled when router under NAT environment.	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

Enable OpenVPN Server

Enable OpenVPN Server

VPN Server Tunnel

Tunnel name:	OpenVPN_Tunnel_0
Listen IP:	
Protocol:	UDP
Port:	1194
Interface:	tun
Authentication:	None
Local IP:	10.8.0.1
Remote IP:	10.8.0.2
<input type="checkbox"/> Enable NAT	
Ping Interval:	20
Ping-Restart:	120
Compression:	LZO
Encryption:	BF-CBC
MTU:	1500
Max Frame Size:	1500
Verbose Level:	ERR
Expert Options:	

*--xx xx.parameter,eg:--config xx.config

Client Manage

Use	Common Name	Password	Client IP	Local Static Route	Remote Static Route
<input type="checkbox"/>					

*Static Route: <1.1.1.0/24> or <1.1.1.0/24;2.2.2.2/16>

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.	Null

	Click "Export" you can export the TA file from router to your PC.	
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

Authentication Manage

Select Cert Type:	Server		
CA:	Browse...	Import	Export
Public Key:	Browse...	Import	Export
Private Key:	Browse...	Import	Export
DH:	Browse...	Import	Export
TA:	Browse...	Import	Export
CRL:	Browse...	Import	Export
Pre-Share Static Key:	Browse...	Import	Export

Authentication Status

Cert Type	CA	Public Key	Private Key	DH	TA	CRL	PKCS12	Pre-Share
Server								
Client_1								
Client_2								
Client_3								

3.21 Configuration -> GRE

This section allows users to set the GRE parameters.

GRE		
Item	Description	Default
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 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
Enable NAT	Tick to enable NAT Traversal for GRE. This item must be enabled when router under NAT environment.	Disable
Secrets	Set Tunnel Key of GRE.	Null

GRE

<input checked="" type="checkbox"/> Enable	
Remote IP Address:	<input type="text"/>
Local Virtual IP:	<input type="text"/>
Remote Virtual IP:	<input type="text"/>
Remote Subnet:	<input type="text"/>
Remote Subnet Mask:	<input type="text"/>
<input type="checkbox"/> Enable NAT	
Secrets:	<input type="text"/>

3.22 Configuration -> L2TP

This section allows users to set the L2TP parameters.

L2TP Client @ L2TP		
Item	Description	Default
Please add L2TP Client	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 server’s authentication method. When you select “Auto”, router will auto select the correct method based on server.	Disable
Enable Tunnel Authentication	Tick to enable tunnel authentication and enter the tunnel secret which provided by L2TP server.	Disable
Remote Subnet	Enter L2TP remote Protected subnet’s address.	Null
Remote Subnet Mask	Enter L2TP remote Protected subnet’s mask.	Null
Show Advanced	Tick to enable the L2TP client advanced setting.	Disable
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.	fffffff
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 to re-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.	noccn nobsdcomp

L2TP Client		
Tunnel name	Description	Add

Enable

Remote IP Address:

Username:

Password:

Authentication:

Enable Tunnel Authentication

Tunnel secret:

Remote Subnet:

Remote Subnet Mask:

Show Advanced

Local IP:

Remote IP:

Address/Control Compression

Protocol Field Compression

Asyncmap Value:

MRU:

MTU:

Link Detection Interval (s):

Link Detection Max Retries:

Expert Options:

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.	ffffffffff
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 to re-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

Enable L2TP Server

Enable L2TP Server

L2TP Common Settings

Username:	<input type="text"/>
Password:	<input type="password"/>
Authentication:	Auto <input type="button" value="▼"/>
<input checked="" type="checkbox"/> Enable Tunnel Authentication	
Tunnel secret:	<input type="text"/>
Local IP:	<input type="text"/>
IP Pool Start:	10.0.0.2
IP Pool End:	10.0.0.100

L2TP Server Advanced

- Show L2TP Server Advanced
- Address/Control Compression
- Protocol Field Compression

Asyncmap Value:	<input type="text" value="ffffffffff"/>
MRU:	<input type="text" value="1500"/>
MTU:	<input type="text" value="1436"/>
Link Detection Interval (s):	<input type="text" value="30"/>
Link Detection Max Retries:	<input type="text" value="5"/>
Expert Options:	<input type="text" value="noccp nobsdcomp"/>

Route Table List		
Client IP	Remote Subnet	Remote Subnet Mask
<i>*0.0.0.0" means any</i>		
<input type="button" value="Add"/>		

3.23 Configuration -> PPTP

This section allows users to set the PPTP parameters.

PPTP Client @ PPTP		
Item	Description	Default
Add		
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
Remote Subnet	Enter PPTP remote Protected subnet's address.	Null
Remote Subnet Mask	Enter PPTP remote Protected subnet's mask.	Null
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 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.	ffffffffff
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	30

	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 to re-establish a tunnel with the peer.	
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 Client

Tunnel name	Description	Add
<input type="checkbox"/> Enable		
Remote IP Address:		
Username:		
Password:		
Authentication:	Auto	
Remote Subnet:		
Remote Subnet Mask:		
<input checked="" type="checkbox"/> Enable MPPE		
<input checked="" type="checkbox"/> Show Advanced		
Local IP:		
Remote IP:		
<input checked="" type="checkbox"/> Address/Control Compression		
<input checked="" type="checkbox"/> Protocol Field Compression		
Asyncmap Value:	ffffffffff	
MRU:	1500	
MTU:	1436	
Link Detection Interval (s):	30	
Link Detection Max Retries:	5	
Expert Options:	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 needs 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.	ffffffffff
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 to re-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.	noccn nobsdcomp
Route Table List	Click "Add" to add a route rule from PPTP server to PPTP client.	Null

Enable PPTP Server

Enable PPTP Server

PPTP Common Settings

Username:
 Password:
 Authentication:
 Local IP:
 IP Pool Start:
 IP Pool End:
 Enable MPPE

PPTP Server Advanced

- Show PPTP Server Advanced
- Address/Control Compression
- Protocol Field Compression

Asyncmap Value:	ffffffffff
MRU:	1500
MTU:	1436
Link Detection Interval (s):	30
Link Detection Max Retries:	5
Expert Options:	noccp nobsdcomp

Route Table List

Client IP	Remote Subnet	Remote Subnet Mask
<i>*0.0.0.0" means any</i>		
<input type="button" value="Add"/>		

Route Table List

Client IP	Remote Subnet	Remote Subnet Mask
<i>("0.0.0.0" means any)</i>		
<input type="button" value="Add"/>		

3.24 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

SNMP Basic Settings

Port:	161
Agent Mode:	Master <input type="button" value="▼"/>
Version:	SNMPv2 <input type="button" value="▼"/>
Location Info:	China
Contact Info:	info@robustel.com
System name:	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

Mib View List

View Name	View Filter	View OID	
system	Include	1.3.6.1.2.1.1	X
all	Include	1	X

*View OID:<1-65535>, <1-65535>...

Add

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

SNMPv1&v2 User List

Readwrite	Network	Community	MIBview	
Readonly		public	system	X
ReadWrite		private	system	X
ReadWrite		robustel	all	X

*Network: 1.1.1.0/24, 0.0.0.0 means any

Add

3.25 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
------------	--	-------------

VRRP Settings

<input checked="" type="checkbox"/> Enable VRRP	<i>suggest to configure ICMP detection to keep alive</i>
Group ID:	1
Priority:	100
Interval (s):	10
Virtual IP:	192.168.0.1

3.26 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

AT Settings

<input checked="" type="checkbox"/> Enable AT Settings	
Protocol:	TCP server
Local IP:	5.5.5.5
Local Port:	8091

3.27 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.	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

Phone Book Configuration

Description	Phone No.
Add	

Phone Group Configuration

Group Name	Phone List
Add	

Group No. And Description

Group Name:

Add or remove the phone no. to/from group

Not in this group	In this group
→ All ←	

3.28 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 when router power up.	Disable
Send SMS on PPP connect	Enable to send SMS to specific user when router establish PPP connection.	Disable

Send SMS on PPP disconnect	Enable to send SMS to specific user when router disconnect PPP connection.	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 SMS. For example 123 or ABC123.	Null
Phone Group	Select the Phone Group you set in 3.2.27 Configuration -> Phone Book	Null

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

SMS Notification

- Send SMS on power up
- Send SMS on PPP connect
- Send SMS on PPP disconnect

Phone Group:

SMS Control

Enable

Password Content:

Phone Group:

3.29 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 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
-------------------	---	------

Daily Reboot

Enable (hh:mm,24h)

Reboot Time1	Reboot Time2	Reboot Time3
12:00		

Call Reboot Configuration

Enable Call Reboot

Phone Group: [Click to add PhoneGroup!](#)

SMS Reply Content:

SMS Reboot Configuration

Enable SMS Reboot

Phone Group: [Click to add PhoneGroup!](#)

Password:

SMS Reply Content:

3.30 Configuration -> Portal

This section allows users to set the Portal parameters. Users can configure this section to select relevant server platform to manager numbers of remote devices.

Portal		
Item	Description	Default
Enable Portal	Click to enable Portal function.	Disable
Server Type	This item allow users to select the different management server platform. Selected from “robustlink”, “Info24”. Robustlink 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
Server address	Set the IP address of the management server platform you select. When router power on it will automatically establish TCP connection to the server platform and login.	Null
Port	Enable to allow router sending syslog to the remote syslog server. You need to enter the IP and Port of the syslog server.	Disable
Password	The password need to be the same as the password preset in the server platform.	Null

Portal Configuration

<input checked="" type="checkbox"/> Enable Portal	
Server Type:	robustlink <input type="button" value="▼"/>
Server Address:	<input type="text"/>
Port:	1883
Password:	<input type="password"/>

3.31 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

Syslog Settings

Save Position:	NONE <input type="button" value="▼"/>
Log Level:	DEBUG <input type="button" value="▼"/>
Keep Days:	14
<input checked="" type="checkbox"/> Log to Remote System	
Remote IP:	<input type="text"/>
Remote Port:	514

3.32 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 "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.	Null
Restore to Factory Default Settings	Click the button of "Restore to Factory Default Settings" to restore the router to factory to factory default setting.	Null

Change Profile

Profile: Standard

Copy settings from current profile to selected profile

All Parameters XML Configuration

XML File:

IPsec XML Configuration

IPsec XML File:

OpenVPN XML Configuration

OpenVPN XML File:

Restore to Factory Default Settings

3.33 Administration -> Tools

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

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 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

Ping

Ping IP address:	<input type="text" value="172.16.1.111"/>
Number of requests:	<input type="text" value="5"/>
Timeout (s):	<input type="text" value="1"/>
Local IP:	<input type="text"/>
<input type="button" value="Start"/> <input type="button" value="Stop"/>	
<pre>PING 172.16.1.111 (172.16.1.111): 56 data bytes 64 bytes from 172.16.1.111: seq=0 ttl=64 time=1.040 ms 64 bytes from 172.16.1.111: seq=1 ttl=64 time=0.842 ms 64 bytes from 172.16.1.111: seq=2 ttl=64 time=0.694 ms 64 bytes from 172.16.1.111: seq=3 ttl=64 time=0.762 ms 64 bytes from 172.16.1.111: seq=4 ttl=64 time=0.781 ms --- 172.16.1.111 ping statistics --- 5 packets transmitted, 5 packets received, 0% packet loss round-trip min/avg/max = 0.694/0.823/1.040 ms</pre>	

AT Debug

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

Send AT Commands

<input type="text" value="at"/>
<input type="button" value="Send"/>

Receive AT Commands

OK

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

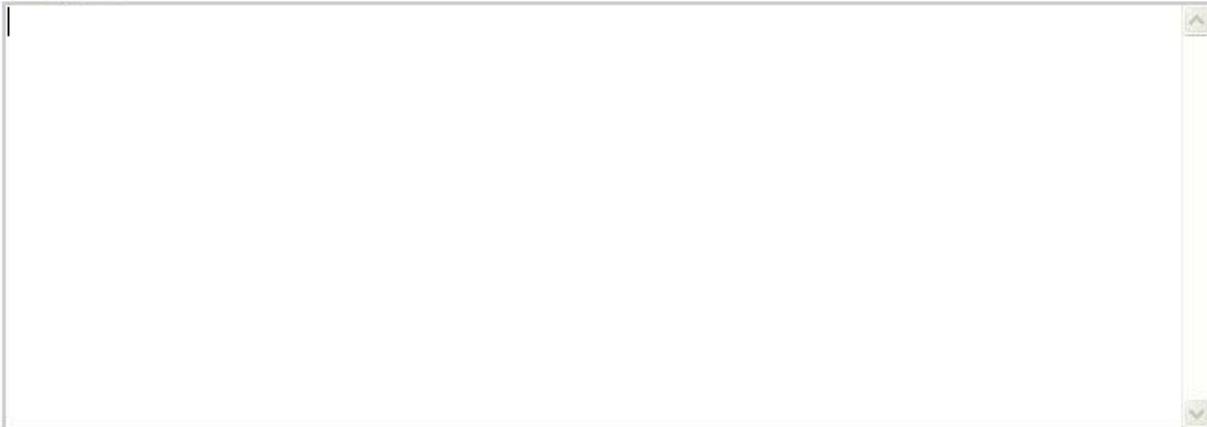
Traceroute

Trace Address:

Trace Hops:

Timeout (s):

Start **Stop**



3.34 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

User Management

Username:

Old Password:

New Password:

Confirm Password:

Login Parameters

Login Timeout(s):

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

User Management

Access Level	Username	Password
ReadWrite	robustel	robustel
ReadOnly	guest	guest

3.35 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	Click enable to enable NTP client which can 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.nt p.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

Real Time Clock Settings	
Real Time Clock:	2013-03-15 11:08:50
PC Time:	2013-03-15 11:08:07
Synchronize	
NTP Settings	
<input checked="" type="checkbox"/> Enable NTP Client	
Timezone:	UTC-12:00 Kwajalein
Primary NTP Server:	pool.ntp.org
Secondary NTP Server:	
Update interval (h):	1
<input checked="" type="checkbox"/> Enable NTP Server	
Timezone:	UTC+00:00 English, Gambia, Libe

3.36 Administration -> Update Firmware

This section allows users to update the firmware of router.

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

Firmware Version	
Firmware Version:	1.01.00
Update Firmware	
<i>Warning: Do not turn off or operate the Router while updating.</i>	
New Firmware:	<input type="file"/> 浏览... Update

Chapter 4. Examples of configuration

4.1 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”.

4.1.1 Always Online:

Configuration-->Link Management-->Cellular Only

Link Management Settings

WAN link:	<input type="button" value="Cellular Only"/> <input style="background-color: #0070C0; color: white; font-weight: bold; font-style: italic; font-size: 10pt; border: none; padding: 0 5px;" type="button" value="Cellular Only"/> <input type="button" value="Eth0 Only"/> <input type="button" value="Eth0 as primary and if fail use cellular"/> <input type="button" value="Cellular as primary and if fail use Eth0"/>
ICMP Detection Primary Server:	
ICMP Detection Secondary Server:	
ICMP Detection Interval (s):	50
ICMP Detection Timeout (s):	3
ICMP Detection Retries:	3
<input checked="" type="checkbox"/> Reset The Interface	

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

Configuration-->Cellular WAN -->Basic

Cellular Settings

Primary SIM Card		Secondary SIM Card	
Network Provider Type:	Auto	Network Provider Type:	Auto
APN:	[redacted]	APN:	[redacted]
Username:	[redacted]	Username:	[redacted]
Password:	[redacted]	Password:	[redacted]
Dialup No.:	*99***1#	Dialup No.:	*99***1#
PIN code request:	Set PIN Code	PIN code request:	Set PIN Code

Connection Mode

Connection Mode:	Always online
Redial Interval (s):	30
Max Retries:	3

Dual SIM Policy

Main SIM Card:	SIM1
<input checked="" type="checkbox"/> When connection fails	

- When roaming is detected
- When IO is active
- Monthly data traffic limitation

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.

4.1.2 Connect on Demand:

Configuration-->Link Management-->Cellular Only

Link Management Settings	
WAN link:	<input type="button" value="Cellular Only"/> <input style="background-color: #0070C0; color: white; font-weight: bold;" type="button" value="Cellular Only"/> <input type="button" value="Eth0 Only"/> <input type="button" value="Eth0 as primary and if fail use cellular"/> <input type="button" value="Cellular as primary and if fail use Eth0"/>
ICMP Detection Primary Server:	50
ICMP Detection Secondary Server:	
ICMP Detection Interval (s):	3
ICMP Detection Timeout (s):	3
ICMP Detection Retries:	3
<input checked="" type="checkbox"/> Reset The Interface	

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

Cellular Settings	
SIM1	SIM2
Status:	Ready
Network Provider Type:	Auto
APN:	
Username:	
Password:	
Dialup No.:	*99***1#
PIN code request:	<input type="button" value="Set PIN Code"/>

Connection Mode	
Connection Mode:	Connect on demand
Redial Interval (s):	30
Max Retries:	3
Inactivity Time (s):	0
Serial Output Content:	
<input checked="" type="checkbox"/> Triggered by Serial Data	
<input checked="" type="checkbox"/> Periodically connect	
Periodically connect interval (s):	300
Time schedule:	schedule_1

Time Range												
Name	SUN	MON	TUE	WED	THU	FRI	SAT	Time Range1	Time Range2	Time Range3		
schedule_1	<input checked="" type="checkbox"/>	08:10-12:00	14:10-20:15		<input type="button" value="X"/>							

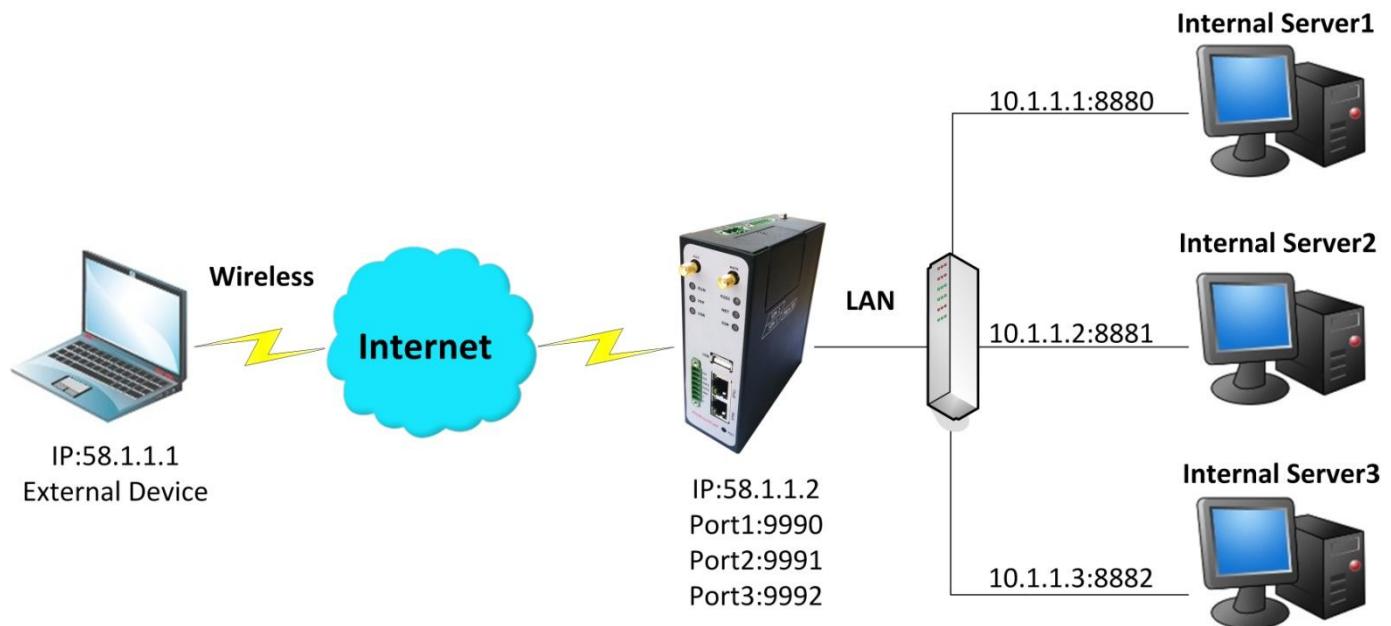
Select the trigger policy you need.

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

4.2 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 <input checked="" type="checkbox"/> X
58.1.1.1	9991	10.1.1.2	8881	UDP <input checked="" type="checkbox"/> X
58.1.1.1	9992	10.1.1.3	8882	TCP&UDP <input checked="" type="checkbox"/> X

*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>

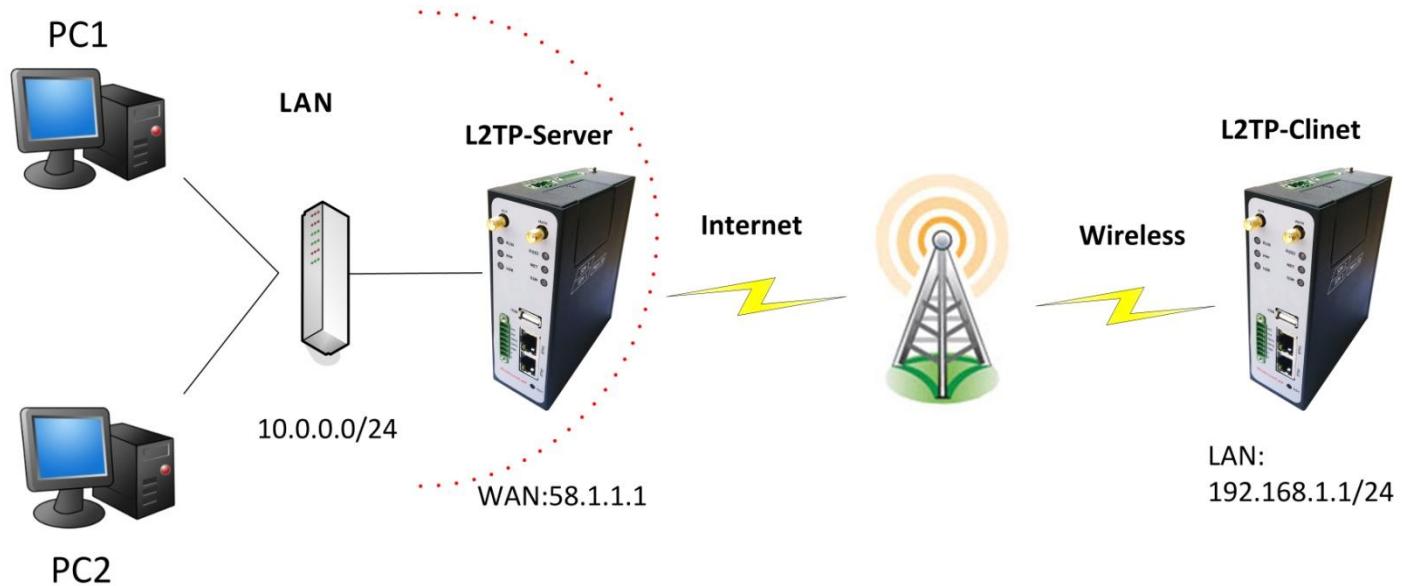
Note: This section will be hidden if user selects "Cellular as primary and if fail use Eth0" in "Configuration ->Link Management".

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 L2TP



L2TP_SERVER:

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

Enable L2TP Server

<input type="checkbox"/> Enable L2TP Server

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

L2TP Common Settings

Username:	<input type="text" value="l2tp"/> 1
Password:	<input type="password" value="*****"/> 2
Authentication:	<input type="text" value="PAP"/> 3
<input type="checkbox"/> Enable Tunnel Authentication	
Local IP:	<input type="text" value="10.1.2.1"/>
IP Pool Start:	<input type="text" value="10.1.2.2"/>
IP Pool End:	<input type="text" value="10.1.2.254"/>

L2TP Server Advanced

<input type="checkbox"/> Show L2TP Server Advanced
--

Route Table List

Client IP	Remote Subnet	Remote Subnet Mask
0.0.0.0	192.168.1.0	255.255.255.0 X
<i>*0.0.0.0 means any</i>		
Add		

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

Please add L2TP Client

Add

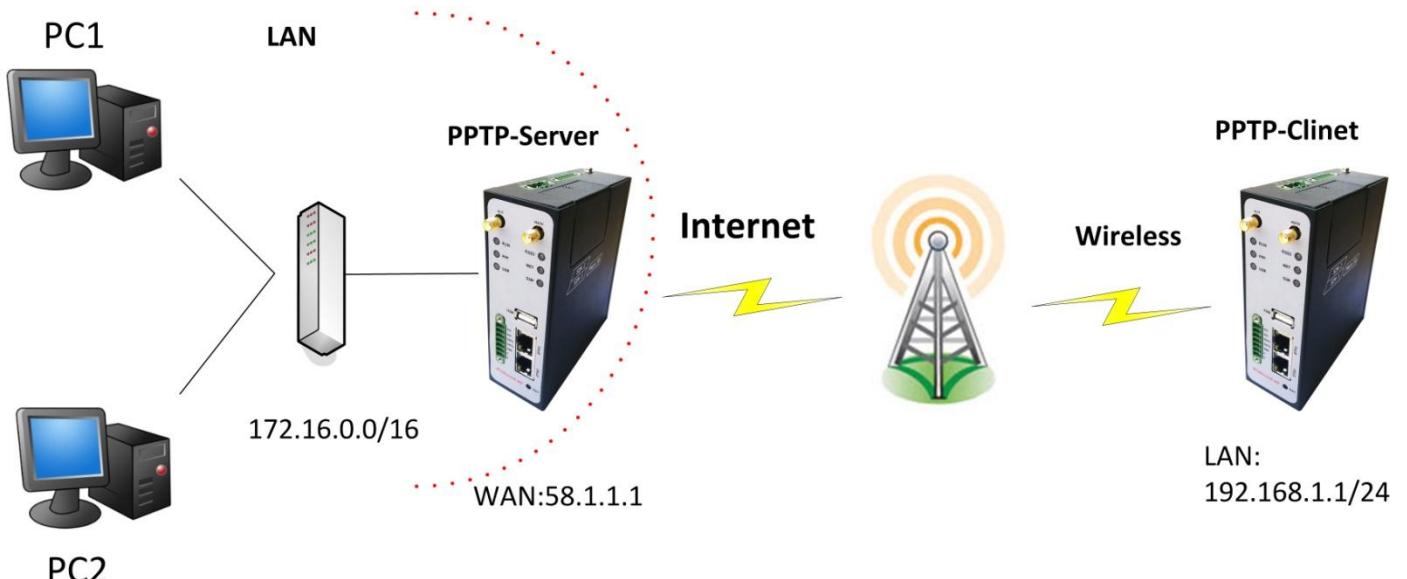
Click “Add” button, and fill in the blank textbox

L2TP Client X

<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
Server Name:	58.1.1.1
Username:	l2tp
Password:	*****
Authentication:	PAP
<input type="checkbox"/> Enable Tunnel Authentication	
Remote Subnet:	10.0.0.0
Remote Subnet Mask:	255.255.255.0
<input type="checkbox"/> Show L2TP Client Advanced	

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

4.4 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**

Enable PPTP Server

Enable PPTP Server

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

PPTP Common Settings

Username:	pptp	1
Password:	*****	2
Authentication:	PAP	3
Local IP:	10.0.0.1	
IP Pool Start:	10.0.0.2	
IP Pool End:	10.0.0.254	
<input type="checkbox"/> Enable MPPE		

PPTP Server Advanced

Show PPTP Server Advanced

Route Table List

Client IP	Remote Subnet	Remote Subnet Mask
0.0.0.0	192.168.1.0	255.255.255.0

*0.0.0.0 means any

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

PPTP_CLIENT:**Configuration--->PPTP--->PPTP Client**

Please add PPTP Client

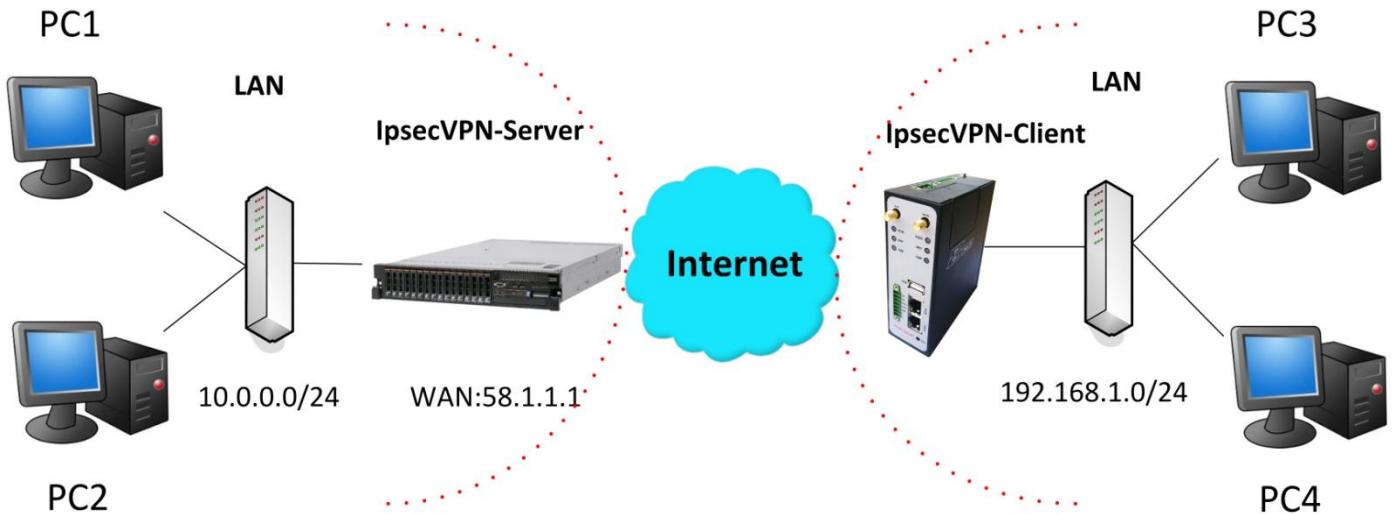
Click “Add” button, and fill in the blank textbox

PPTP Client X

<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	
Server Name:	58.1.1.1	1
Username:	pptp	2
Password:	*****	3
Authentication:	PAP	
Remote Subnet:	172.16.0.0	
Remote Subnet Mask:	255.255.0.0	
<input type="checkbox"/> Enable MPPE		
<input type="checkbox"/> Show PPTP Client Advanced		

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

4.5 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
!
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: Policies 1,4,6,7 are default for Cisco router and do not display at the CMD.

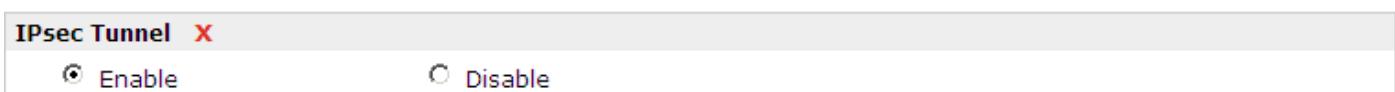
IPsecVPN_CLIENT:

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



Then click “Apply”.

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

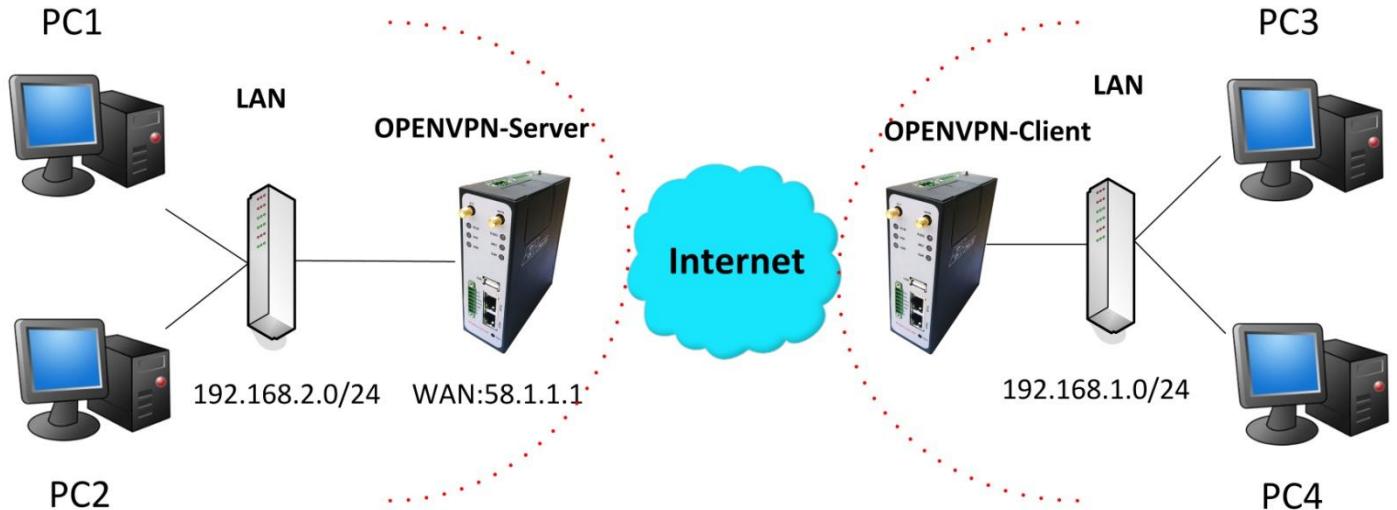


Tick “Enable IPSec Tunnel1”

IPsec Common	
Tunnel name:	IPSEC_TUNNEL_1
IPsec Gateway Address:	58.1.1.1
IPsec Mode:	Tunnel 1
IPsec Protocol:	ESP 2
Local Subnet:	192.168.1.0 3
Local Subnet Mask:	255.255.255.0
Local ID Type:	IP Address 4
Remote Subnet:	10.0.0.0 5
Remote Subnet Mask:	255.255.255.0
Remote ID Type:	IP Address 6
IKE Parameter	
Negotiation Mode:	Main 7
Encryption Algorithm:	AES256 8
Authentication Algorithm:	MD5 9
DH Group:	MODP1024_2 10
Authentication:	PSK 11
Secrets:	***** 12
Life Time (s):	86400
SA Parameter	
SA Algorithm:	3DES_MD5_96 13
PFS Group:	PFS_NULL
Life Time(s):	28800
DPD Time Interval (s):	180
DPD Timeout (s):	60
IPsec Advanced	
VPN Over IPsec Type:	NONE
<input type="checkbox"/> Enable Compress	

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

4.6 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

Enable OpenVPN Server
<input type="checkbox"/> Enable OpenVPN Server

Tick “Enable OpenVPN Server”.

VPN Server Tunnel

Tunnel name:	OpenVPN_Tunnel_0	1
Listen IP:		2
Protocol:	UDP	3
Port:	1194	4
Interface:	tun	5
Authentication:	None	6
Local IP:	10.8.0.1	7
Remote IP:	10.8.0.2	
<input checked="" type="checkbox"/> Enable NAT		
Ping Interval:	20	8
Ping-Restart:	120	9
Compression:	LZO	10
Encryption:	BF-CBC	11
MTU:	1500	
Max Frame Size:	1500	
Verbose Level:	ERR	
Expert Options:	--route 192.168.1.0 255.255.255.0	

*--xx xx.parameter,eg:--config xx.config

Client Manage

Use	Common Name	Password	Client IP	Local Static Route	Remote Static Route
<i>*Static Route: <1.1.1.0/24> or <1.1.1.0/24;2.2.2.2/16></i>					
<input type="button" value="Add"/>					

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

OPENVPN_CLIENT:

Configuration-->OpenVPN--->Client

Enable OpenVPN Client1

<input type="checkbox"/> Enable OpenVPN Client1

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

Enable OpenVPN Client X

<input checked="" type="radio"/> Enable	<input type="radio"/> Disable
Tunnel name:	OpenVPN_Tunnel_0
Protocol:	UDP 1
Server Address:	58.1.1.1 2
Port:	1194 3
Interface:	tun 4
Authentication:	None 5
Local IP:	10.8.0.2 6
Remote IP:	10.8.0.1 7
<input checked="" type="checkbox"/> Enable NAT 8	
Ping Interval:	20
Ping-Restart:	120
Compression:	LZO 9
Encryption:	BF-CBC 10
MTU:	1500
Max Frame Size:	1500 11
Verbose Level:	ERR
Expert Options:	--route 192.168.2.0 255.255.255.0

*--xx xx.parameter,eg:--config xx.config

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

4.7 SMS Remote Control

R3000-3P supports remote control via SMS.

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 0000 – 9999
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. After setting new parameters for R3000-3P, please use 0004 command to save parameters and reset the router, then the new parameters will take effect.
6. E.g., 1234:1001,R3000-3P;0004

In this command, password is 1234, and we set device name as “R3000-3P”, then save parameters and reset the router to take effect with command 0004.

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

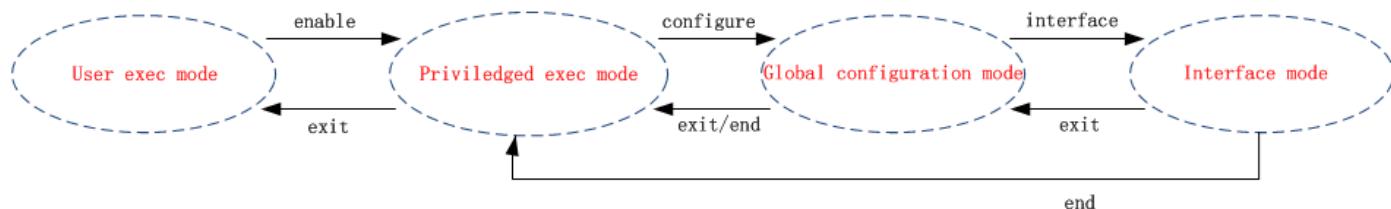
Chapter 5. Introductions for CLI

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: *****

R3000-3P> ?	//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

PRIVILEGED EXEC MODE:

```
R3000-3P> enable  
Password: *****  
R3000-3P# ? //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:

```
R3000-3P# configure  
R3000-3P(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:

```
R3000-3P(config)# interface Ethernet 0
R3000-3P(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 “?” everywhere needed that will show us the helpful 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	Parameters haven’t been finished yet .
% Invalid input detected at '^' marker	'^' marker indicates the location where is set wrong .

Note: Almost all 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** .

NOTICE: Knowing the **CLI hierarchy level modes** is necessary before configuring the CLI. If you don’t , 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

```
R3000-3P> show version
software version : 1.01.00
kernel version   : v2.6.39
hardware version : 1.01.00
```

Example 2 : Update firmware via tftp

```
R3000-3P> enable  
Password: *****  
R3000-3P#  
R3000-3P# tftp 172.16.3.3 get rootfs R3k.1.01.00.02_130325
```

```
Tftp transferring  
tftp succeeded!downloaded  
R3000-3P# write //save current configuration  
Building configuration...  
OK  
R3000-3P# reload  
!Reboot the system ?'yes'or 'no':yes //reload to take effect
```

Example 3: Set link-management

```
R3000-3P> enable  
Password: *****  
R3000-3P#  
R3000-3P# configure  
R3000-3P(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]:

```
R3000-3P# write //save current configuration  
Building configuration...  
OK  
R3000-3P# reload  
!Reboot the system ?'yes'or 'no':yes //reload to take effect
```

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

```
R3000-3P> enable  
Password: *****
```

R3000-3P#

R3000-3P# 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
*****
```

R3000-3P# configure

R3000-3P(config)# set eth0

ethernet interface type:WAN

type select:

1. Static IP
2. DHCP
3. PPPOE

->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

//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]:

R3000-3P(config)# end

R3000-3P# write //save current configuration

Building configuration...

OK

R3000-3P# reload

!Reboot the system ?'yes'or 'no':yes //reload to take effect

Example 5: CLI for Cellular dialup

R3000-3P> enable

Password: *****

R3000-3P#

R3000-3P# 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
*****
```

R3000-3P(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]:

R3000-3P(config)# end

R3000-3P# write //save current configuration

Building configuration...

OK

R3000-3P# 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
```

R3000-3P# reload

!Reboot the system ?'yes'or 'no':yes //reload to take effect

5.3 Commands reference

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