

# Robustel GoRugged R3000 Wireline

## Industrial VPN Router - 4 Ethernet Ports

### User Guide

Document Name: **User Guide**  
Firmware: **1.2.16**  
Date: **2017-02-06**  
Status: **Confidential**  
Doc ID: **RT\_UG\_R3000 Wireline - 4 Ethernet Ports\_v.1.2.2**



## **About This Document**

This document describes hardware and software of Robustel R3000 Wireline, Industrial VPN 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: +86-20-29019902

Fax: +86-20-82321505

E-mail: [support@robustel.com](mailto:support@robustel.com)

Web: [www.robustel.com](http://www.robustel.com)

**Important Notice**

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

**Safety Precautions****General**

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

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

**Using the router in vehicle**

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



### **Protecting your router**

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


- Do not expose the router to extreme conditions such as high humidity / rain, high 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

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

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

SJ/T 11363-2006	“Requirements for Concentration Limits for Certain Hazardous Substances in Electronic Information Products” (2006-06).	
SJ/T 11364-2006	<p>“Marking for Control of Pollution Caused by Electronic Information Products” (2006-06).</p> <p>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.</p> <p>Please see <a href="#">Table 3</a> 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.</p>	

**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
<p><b>o:</b> 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.</p> <p><b>x:</b> Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part <i>might exceed</i> the limit requirement in SJ/T11363-2006.</p>						

**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
2015-01-06	1.02.00	V1.0.0	First Release
2015-07-02	1.2.8	V1.1.0	Increase section: Download MIB Moudles File, GpsGate portal Modify section: Mount the Route, file format, Sentence Revision, Approval & Certification, Regulatory and Type Approval Information, SDK Management, CLI command
2015-11-24	1.2.16	v.1.2.0	Increase section: Modbus Master, Modbus over TCP, Alarms, Remote Channels, AAA, FTP, SMTP, DMVPN Modify section: Serial, Ethernet
2016-11-15	1.2.16	v.1.2.1	Updated section about 2.8 Power Supply Updated LOGO
2017-02-06	1.2.16	v.1.2.2	Changed Tel number to +86-20-29019902 Changed CD information in Chapter 1.2

## Contents

Chapter 1	Product Concept.....	8
1.1	Overview .....	8
1.2	Packing List .....	9
1.3	Specifications .....	10
1.4	Selection and Ordering Data .....	12
Chapter 2	Installation.....	13
2.1	LED Indicators.....	13
2.2	PIN assignment.....	14
2.3	USB interface .....	15
2.4	Reset Button.....	15
2.5	Ethernet ports .....	16
2.6	Mount the Router .....	16
2.7	Ground the Router .....	18
2.8	Power Supply.....	18
Chapter 3	Configuration settings over web browser .....	19
3.1	Configuring PC in Windows 7 .....	19
3.2	Factory Default Settings .....	21
3.3	Control Panel .....	22
3.4	Status -> System .....	23
3.5	Status -> Network.....	25
3.6	Status -> Route .....	26
3.7	Status -> VPN.....	26
3.8	Status -> Services .....	27
3.9	Status -> Channels.....	27
3.10	Status -> Event/Log .....	28
3.11	Configuration -> Link Management.....	29
3.12	Configuration -> Ethernet.....	30
3.13	Configuration -> WiFi .....	36
3.14	Configuration -> Serial.....	40
3.15	Configuration -> USB.....	47
3.16	Configuration -> GPS .....	48
3.17	Configuration -> NAT/DMZ.....	51
3.18	Configuration -> Firewall .....	53
3.19	Configuration -> QoS.....	56
3.20	Configuration -> IP Routing .....	59
3.21	Configuration -> DynDNS .....	61
3.22	Configuration -> DMVPN.....	62
3.23	Configuration -> IPsec.....	64
3.24	Configuration -> RobustVPN.....	69
3.25	Configuration -> Open VPN .....	70
3.26	Configuration -> GRE .....	75
3.27	Configuration -> L2TP .....	76

3.28	Configuration -> PPTP.....	79
3.29	Configuration->Modbus over TCP.....	83
3.30	Configuration ->Modbus Master.....	83
3.31	Configuration ->Remote Channels.....	85
3.32	Configuration ->Alarms.....	86
3.33	Configuration ->SNMP.....	87
3.34	Configuration -> VRRP.....	89
3.35	Configuration -> Reboot.....	89
3.36	Configuration -> Portal.....	90
3.37	Configuration -> Syslog.....	91
3.38	Configuration -> Event.....	92
3.39	Configuration -> USR LED.....	93
3.40	Configuration -> AAA.....	93
3.41	Configuration -> FTP.....	95
3.42	Administration -> Profile.....	96
3.43	Administration -> Tools.....	97
3.44	Administration -> Clock.....	101
3.45	Administration -> Web Server.....	102
3.46	Administration -> User Management.....	103
3.47	Administration -> SDK Management.....	104
3.48	Administration -> Update Firmware.....	105
Chapter 4	Configuration Examples.....	106
4.1	Interface.....	106
4.1.1	Console port.....	106
4.1.2	RS232.....	107
4.1.3	RS485.....	107
4.2	Network.....	108
4.2.1	NAT.....	108
4.2.2	L2TP.....	109
4.2.3	PPTP.....	110
4.2.4	IPsec VPN.....	112
4.2.5	OpenVPN.....	114
Chapter 5	Introductions for CLI.....	118
5.1	What’s CLI and hierarchy level Mode.....	118
5.2	How to configure the CLI.....	120
5.3	Commands reference.....	122
Glossary.....		123



# Chapter 1 Product Concept

## 1.1 Overview

Robustel GoRugged R3000 Wireline is a rugged VPN router offering state-of-the-art secure connectivity for machine to machine (M2M) applications.

- WAN link management: Ethernet WAN/WLAN WAN backup
- VPN tunnel: IPSec/OpenVPN/PPTP/L2TP/GRE
- Supports Modbus gateway (Modbus RTU/ASCII to Modbus TCP)
- Supports GPS&GLONASS (optional), provides real time location and tracking
- Supports 802.11 b/g/n Wi-Fi (optional), AP and client mode
- Supports SDK, provides user programmatic interface
- Supports 802.1Q VLAN Trunk
- Auto reboot via Timing
- Supports RobustLink (Centralized M2M management platform, to remote monitor, configure and update firmware)
- Supports RobustVPN (Cloud VPN Portal, to provide easy and secure remote access for PLCs and machines)
- Flexible Management methods: Web/CLI/SNMP/RobustLink
- Firmware upgrade via Web/CLI/USB/RobustLink
- Various interfaces: RS232/RS485/Console/USB/Ethernet
- Wide range input voltages from 9 to 60 VDC and extreme operating temperature
- The metal enclosure can be mounted on a DIN-rail or on the wall, also with extra ground screw

## 1.2 Packing List

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

- Robustel GoRugged R3000 Wireline 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 and console port x 1



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

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

### Optional Accessories (can be purchased separately)

- Ethernet cable x 1



- Wall mounting kit x 1



- 35 mm DIN rail mounting kit x 1



- AC/DC power supply adapter x 1 (12 VDC, 1.5 A; EU, US, UK, AU plug optional)



## 1.3 Specifications

### Ethernet Interface

- Number of ports: 4 x 10/100 Mbps, 3 LAN + 1 WAN
- Magnet isolation protection: 1.5 KV

### WLAN Interface (Optional)

- Standards: 802.11b/g/n up to 65 Mbps, AP and Client mode
- Frequency band: 2.400 - 2.500 GHz (2.4 GHz ISM band)
- Security: Open ,WPA, WPA2
- Encryption: AES, TKIP
- Antenna interface: SMA female
- Transmission power: 802.11b: 17dBm, 802.11g/n: 15dBm

- Reception sensibility: 1M: -97dBm, 2M: -93dBm, 6M: -91dBm, 11M: -89dBm, 54M: -75dBm, 65M: -72dBm

### **GPS&GLONASS Interface (Optional)**

- Antenna interface: SMA female, with 50 ohms impedance
- Tracking sensitivity: GPS: better than -148 dBm  
GLONASS: better than -140 dBm
- Protocol: NMEA-0183 V2.3

### **Serial Interface**

- Number of ports: 1 x RS-232 or 1 x RS-485
- ESD protection:  $\pm 15KV$
- Parameters: 8E1, 8O1, 8N1, 8N2, 7E2, 7O2, 7N2, 7E1
- Baud rate: 300 bps to 230400 bps
- RS-232: TxD, RxD, RTS, CTS, GND
- RS-485: Data+ (A), Data- (B)
- Interface: 3.5 mm terminal block with lock

### **System**

- LED indicators: RUN, WLAN, USR
- Built-in RTC, Watchdog, Timer
- Expansion: 1 x USB 2.0 host up to 480 Mbps
- Storage: 1 x Micro SD

### **Software**

- Network protocols: PPPoE, TCP, UDP, DHCP, ICMP, NAT, DMZ, RIP v1/v2, OSPF, DDNS, VRRP, HTTP, HTTPS, DNS, ARP, QoS, SNTP, Telnet, VLAN, SSH2, etc
- VPN tunnel: IPSec/OpenVPN/PPTP/L2TP/GRE
- Firewall: SPI, anti-DoS, Filter, Access Control
- Management: Web, CLI, SNMP v1/v2/v3, RobustLink
- Serial port: TCP client/server, UDP, Modbus RTU/ASCII to Modbus TCP, Virtual COM (COM port redirector)
- RobustLink: Centralized M2M management platform
- RobustVPN: Cloud VPN Portal

### Power Supply and Consumption

- Power supply interface: 5 mm terminal block with lock
- Input voltage: 9 to 60 VDC
- Power consumption: Idle: 100 mA@12 V

Data link: 400 mA (peak)@12 V

### Physical Characteristics

- Housing & Weight: Metal, 500 g
- Dimension: 125 mm x 108 mm x 45 mm
- Installation: 35 mm DIN rail, wall mounting or desktop

### Environmental Limits

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

### Regulatory and Type Approvals

- Approval & Certificates: CE, R&TTE, FCC, RCM, RoHS, WEEE

- EMC:

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

EMS: IEC 61000-4-2 (ESD) Level 3,

IEC 61000-4-3 (RS) Level 4,

IEC 61000-4-4 (EFT) Level 4,

IEC 61000-4-5 (Surge) Level 3,

IEC 61000-4-6 (CS) Level 4,

IEC 61000-4-8, Level 4

## 1.4 Selection and Ordering Data

Please refer to corresponding R3000 Wireline datasheet.

## Chapter 2 Installation

### 2.1 LED Indicators



Name	Color	Status	Function
RUN	Green	Blinking	Router is ready.
		On	Router is starting.
		Off	Router is power off.
WLAN	Green	Blinking	WLAN Indicator: Data is being transmitted.
		On	WLAN Indicator: Wi-Fi AP/Client is enabled.
		Off	WLAN Indicator: Wi-Fi AP/Client is disabled.
USR	Green	On/Blinking	VPN tunnel/PPPoE/DynDNS/GPS is up.
		Off	VPN tunnel/PPPoE/ DynDNS/GPS is down.

**Note:** User can select display status of USR LED. For details please refer to section 1.3.39.

## 2.2 PIN assignment

### PIN assignment of R3000-QLA



PIN	Debug	RS232	Direction
1	RXD		Device →R3000
2	TXD		R3000 → Device
3	GND	GND	
4		TXD	R3000 → Device
5		RXD	Device →R3000
6		RTS	R3000 → Device
7		CTS	Device →R3000



PIN	Power	Digital I/O	RS485
8	Positive		
9	Negative		
10	GND		

### PIN assignment of R3000-QLB



PIN	Debug	RS485	Direction
1	RXD		Device →R3000
2	TXD		R3000 → Device
3	GND		
4		Data+(A)	
5		Data- (B)	
6			
7			



PIN	Power	Digital I/O	RS485
8	Positive		
9	Negative		
10	GND		

### 2.3 USB interface



USB interface is used for batch firmware upgrade, cannot used to send or receive data from slave devices which with USB interface.

Users can insert a USB storage device, such as U disk or hard disk, into the router’s USB interface, if there is configuration file or firmware of R3000 inside the USB storage devices, R3000 will automatically update the configuration file or firmware. For details please refer to section 1.3.15.

USB Interface

### 2.4 Reset Button



Function	Operation
Reset	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.

Reset Button



## 2.5 Ethernet ports



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

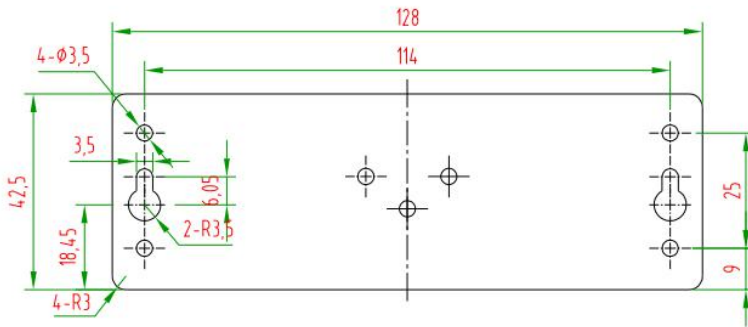
Indicator	Status	Description
Speed Indicator	Off	10 Mbps mode.
	On	100 Mbps mode.
Link Indicator	Off	Connection is down.
	On	Connection is up.
	Blink	Data is being transmitted

Ethernet Ports

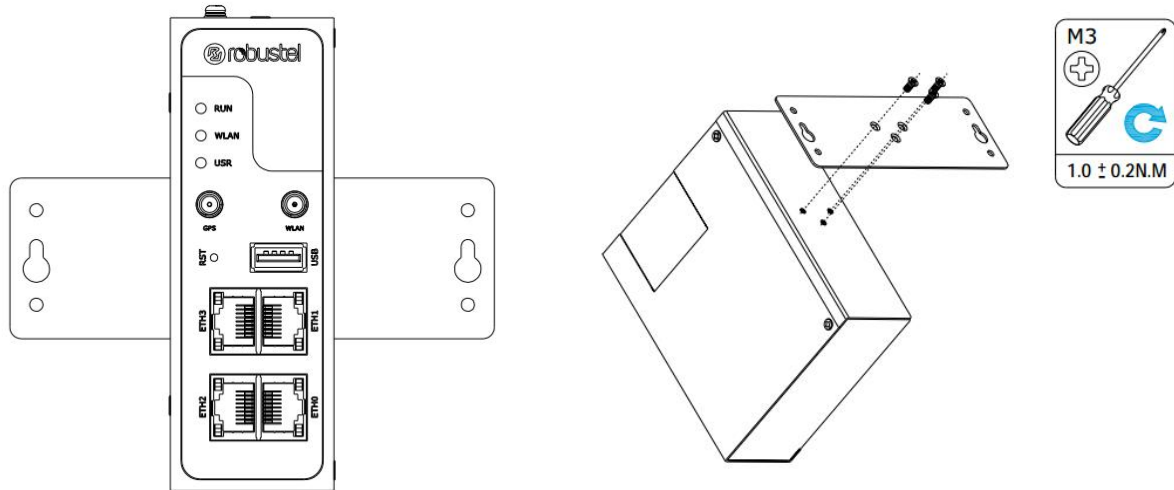
## 2.6 Mount the Router

- Two ways of mounting the router

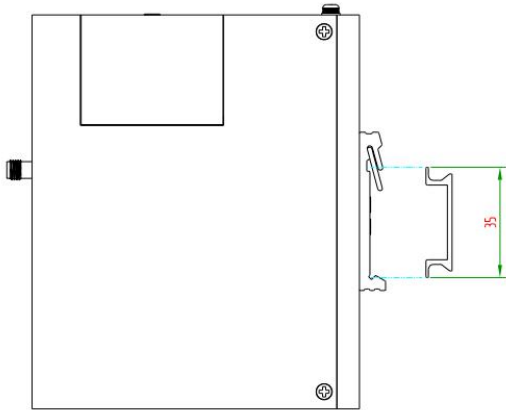
1. Wall mounting



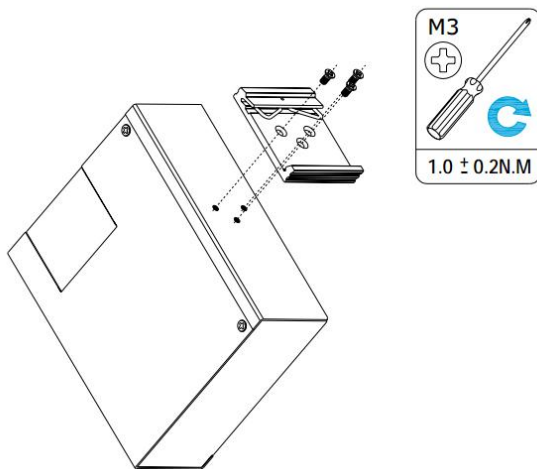
Use 3 pcs of M3 screw to mount the router on the Wall mounting Kit.  
 And then use 2 pcs of M3 screw to mount the Wall mounting Kit on the wall.



## 2. DIN rail mounting

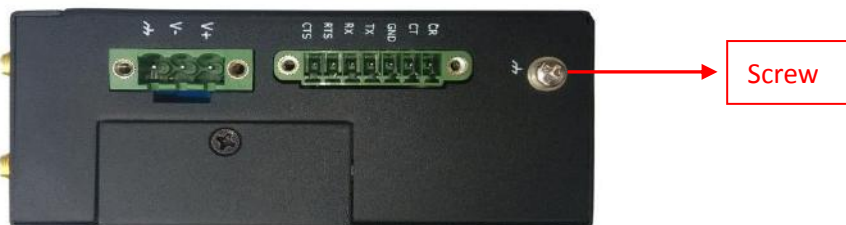


Mount the router on a DIN rail with 3 pcs of M3 screws, and then hang the DIN-Rail on the holder. You need to choose a standard holder.



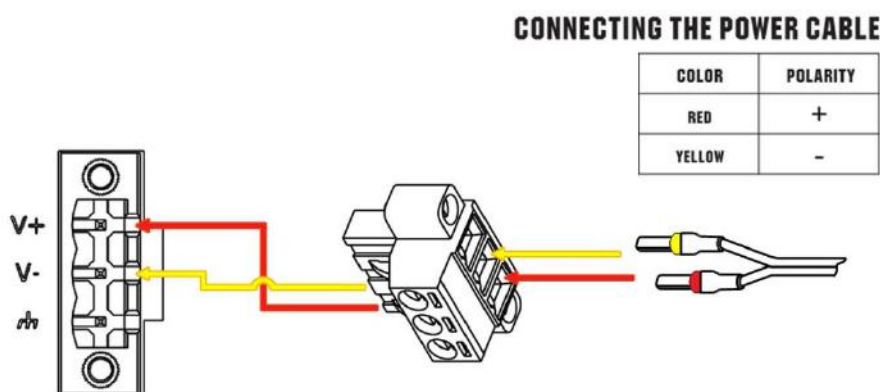
## 2.7 Ground the Router

Grounding and wire router helps limit the effects of noise due to electromagnetic interference (EMI). Run the ground connection from the ground by screwing to the grounding surface before connecting devices.



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

## 2.8 Power Supply



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

**Note:** The range of power voltage is 9 to 60 VDC.

## Chapter 3 Configuration settings over web browser

The router can be configured through your web browser that include IE 8.0 or above, Chrome and Firefox. 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. It provides an easy and user-friendly interface for configuration.

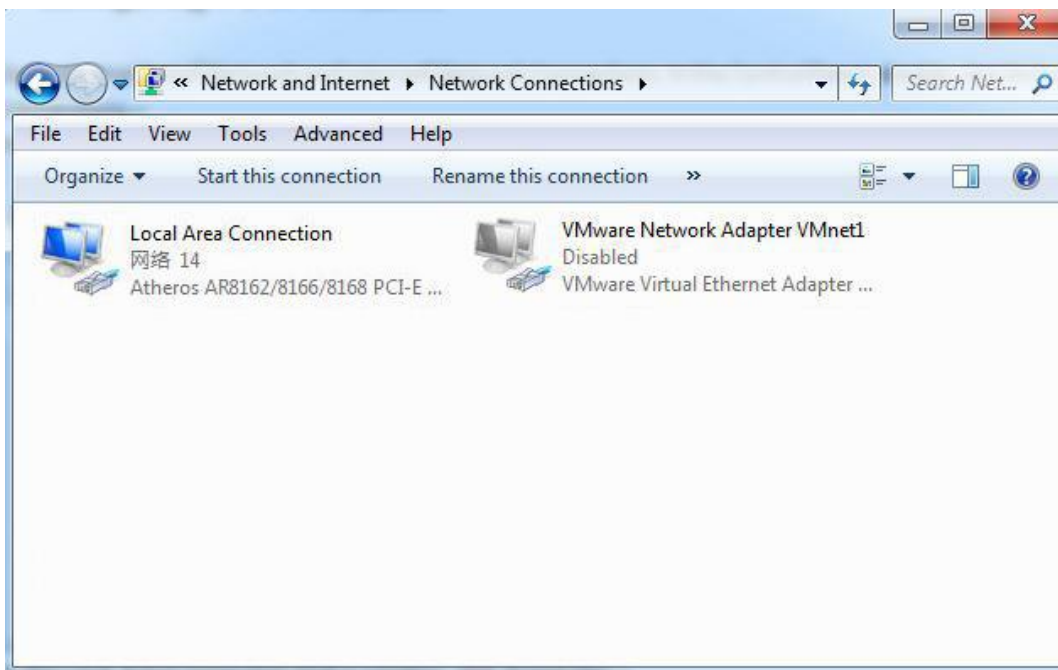
There are various ways to connect the router, either through an external repeater/hub or connect directly to your PC. However, make sure that your PC has an Ethernet interface properly installed prior to connecting the router.

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. If you encounter any problems accessing the router web interface it is advisable to uninstall your firewall program on your PC, as this tends to cause problems accessing the IP address of the router.

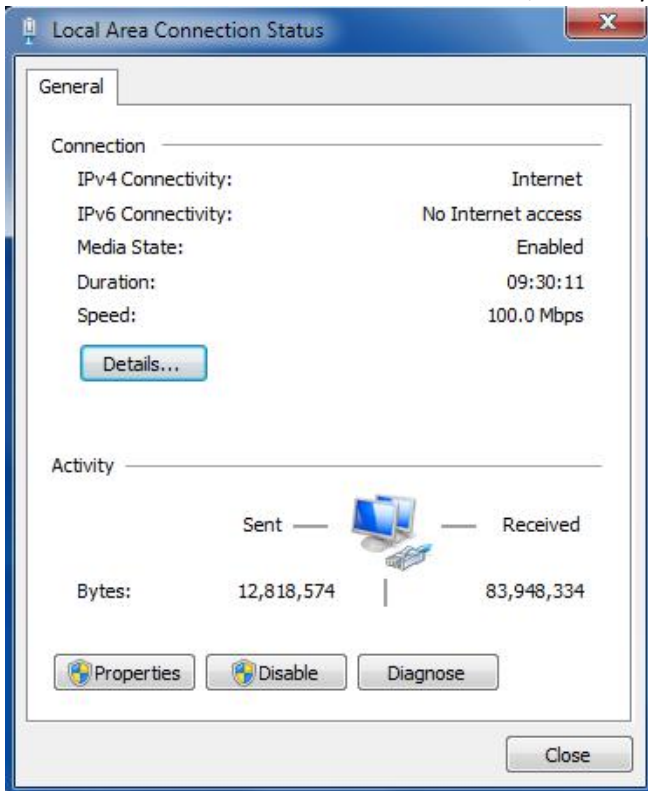
### 3.1 Configuring PC in Windows 7

The configuration for windows system is similar.

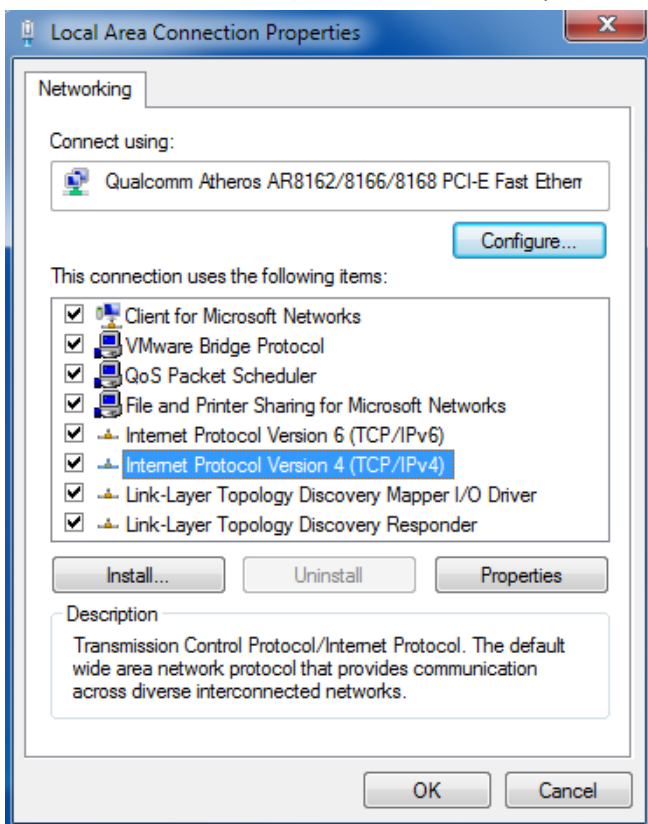
1. Go to *Start / Control Panel* (in Classic View). In the Control Panel, double-click *Network Connections*.
2. Double-click *Local Area Connection*.



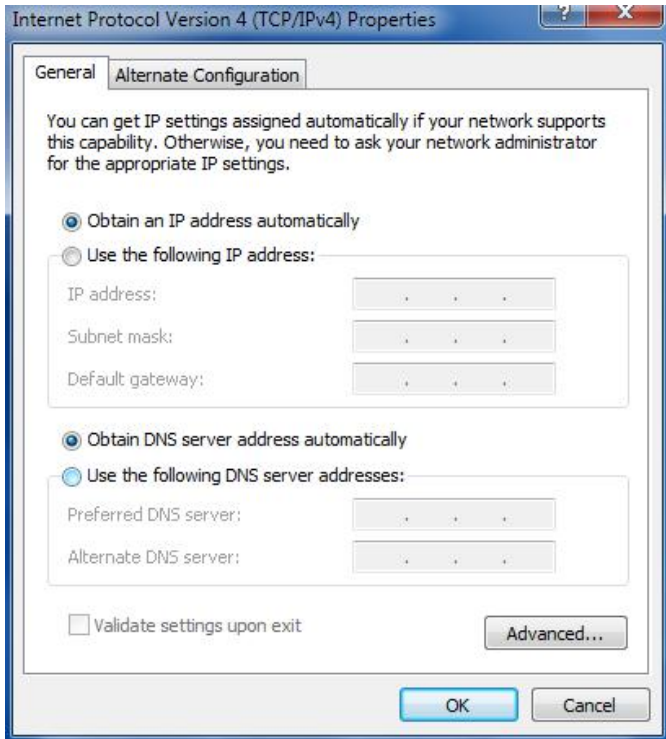
3. In the *Local Area Connection Status* window, click *Properties*.



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



5. Select *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.

**User authentication required. Login please.**

Username:

Password:

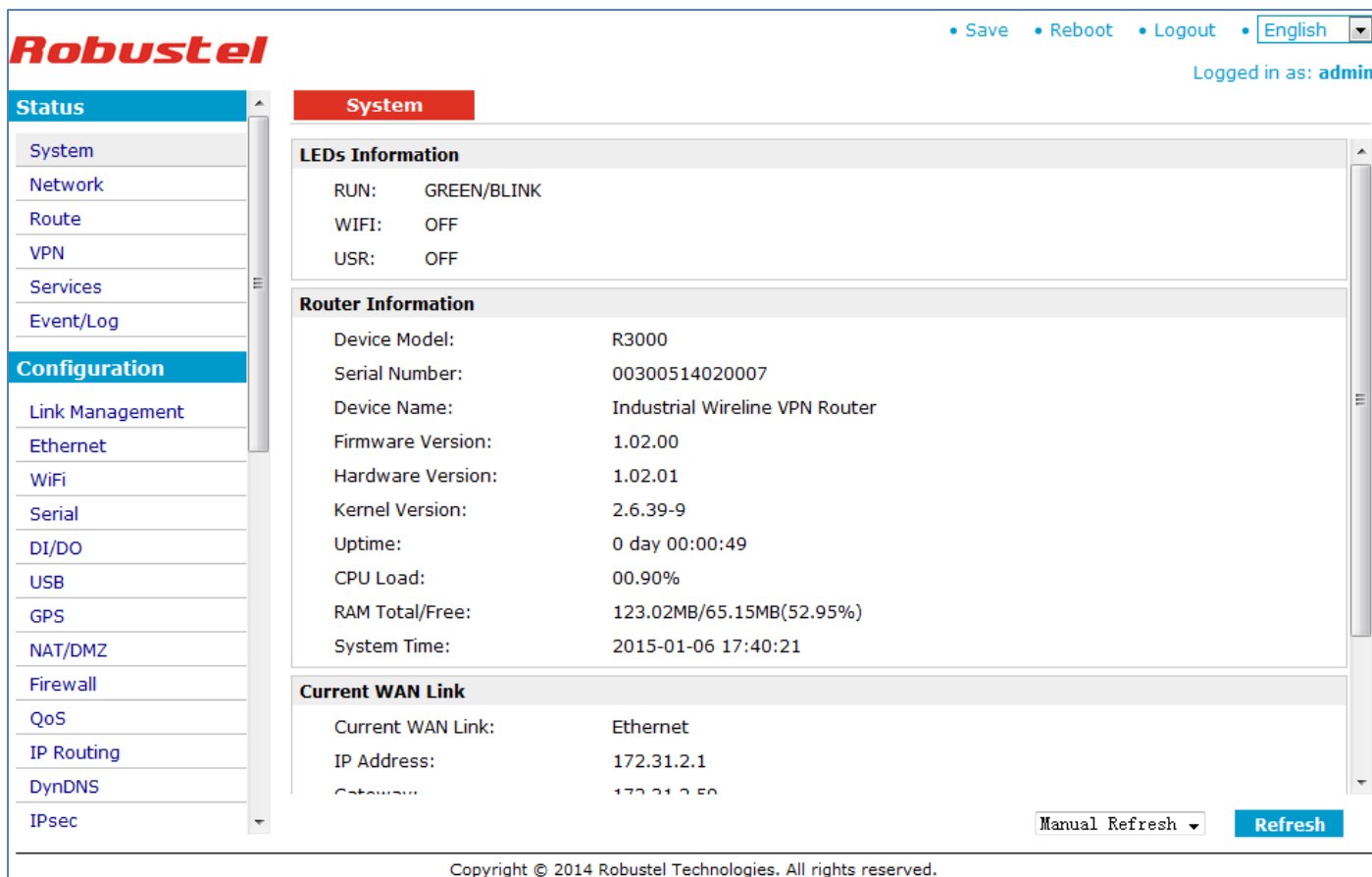
Language:  ▼

Please enter your login username and password.

Item	Description
Username	admin
Password	admin
Eth0	192.168.1.1/255.255.255.0, WAN mode
Eth1	192.168.0.1/255.255.255.0, LAN mode
Eth2	192.168.0.1/255.255.255.0, LAN mode
Eth3	192.168.0.1/255.255.255.0, LAN mode
DHCP Server	Enabled.





### 3.3 Control Panel

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



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

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

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

### 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.

#### LEDs Information

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

System

**LEDs Information**

RUN:	GREEN/BLINK
WIFI:	OFF
USR:	OFF

**Router Information**

Device Model:	R3000
Serial Number:	00300514020007
Device Name:	Industrial Wireline VPN Router
Firmware Version:	1.2.0
Hardware Version:	1.02.01
Kernel Version:	2.6.39-9
Uptime:	0 day 00:00:49
CPU Load:	00.90%
RAM Total/Free:	123.02MB/65.15MB(52.95%)
System Time:	2015-01-06 17:40:21



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
Uptime	Show how long the router have been working since power on
CPU Load	Show the current CPU load
RAM Total/Free	Show the total capacity /Free capacity of RAM
System Time	Show the current system time

Current WAN Link	
Current WAN Link:	Ethernet
IP Address:	172.31.2.1
Gateway:	172.31.2.59
NetMask:	255.255.0.0
DNS Server:	172.31.2.59
Keepalive PING IP Address:	8.8.8.8, 8.8.4.4
Keepalive PING Interval:	30

Current WAN Link	
Item	Description
Current WAN Link	Show the current WAN link: Ethernet WAN.
IP Address	Show the current WAN IP address
Gateway	Show the current gateway
NetMask	Show the current netmask
DNS Server	Show the current primary DNS server and Secondary server
Keepalive PING IP Address	Show the current ICMP detection server which you can set in "Configuration->Link Management".
Keepalive PING Interval	Show the ICMP Detection Interval (s) which you can set in "Configuration->Link Management".

### 3.5 Status -> Network

This section displays the router's Network status, which include status of ETH0, ETH1, ETH2, ETH3, WLAN (AP mode)/WLAN (Client mode).

Network	DHCP	Device List
<b>Eth0 WAN</b>		
Connection Mode:	Static IP	
IP Address:	172.31.2.1	
MAC Address:	00:ff:74:46:dc:e1	
MTU:	1500	
Gateway:	172.31.2.59	
NetMask:	255.255.0.0	
Primary DNS Server:	172.31.2.59	
Secondary DNS Server:	172.31.2.59	
<b>LAN</b>		
IP Address:	192.168.0.1	
MAC Address:	00:ff:74:46:dc:e2	
MTU:	1500	
NetMask:	255.255.255.0	
<b>WiFi</b>		
MAC Address:	00:23:a7:25:23:27	
SSID:	R3K	
Mode:	AP	
WPA State:	Completed	

**Note:** This information will be shown when R3000 Wireline enable WiFi feature and works as AP mode.

<b>WiFi WAN</b>		
Connection Mode:	Dhcp Client	
IP Address:	192.168.199.125	
MAC Address:	00:23:a7:25:23:27	
Gateway:	192.168.199.1	
NetMask:	255.255.255.0	
Primary DNS Server:	192.168.199.1	
Secondary DNS Server:	0.0.0.0	

**Note:** This information will be shown when R3000 Wireline enable WLAN and works as Client mode.

### 3.6 Status -> Route

This section displays the router’s route table.

**Route**

Route Table				
Destination	NetMask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	10.214.130.173	wwan0	0
172.16.0.0	255.255.0.0	0.0.0.0	eth-br	0

### 3.7 Status -> VPN

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

IPsec
L2TP
PPTP
OpenVPN
GRE

IPsec Status			
No.	Tunnel name	Status	Connect Time
<input type="button" value="Show Detail Status"/>			

IPsec
L2TP
PPTP
OpenVPN
GRE

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
GRE

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 GRE

**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 is disabled!

VRRP DynDNS Serial

**DynDNS**

DynDNS is disabled!

VRRP DynDNS Serial

**RS232: 115200, N, 8, 1**

### 3.9 Status -> Channels

This section displays the status of router’s channels.

Channels

**Channels Status**

Channel Name	Tag	Value	Status
Connection Status		disconnect	

### 3.10 Status -> Event/Log

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

**Event/Log**

**Event/Log Messages**

Download: --Please Select-- ▼

Log Level: DEBUG ▼

```
15-01-06 12:15:13 <2> router: change network (Null)->(Ethernet - up)
15-01-06 12:15:13 <0> router: system service starting...
15-01-06 12:15:18 <0> router: Firmware version: 1.02.00 Dec 10 2014 08:25:34
15-01-06 12:15:18 <0> router: sdk-server startup.
15-01-06 12:15:19 <0> router: start dhcpd
```

**Download System Diagnosing Data**

Download System Diagnosing Data

Manual Refresh ▼
 Refresh
Clear

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

### 3.11 Configuration -> Link Management

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

#### Link Management

**Link Management Settings**

Primary Interface:

Backup Interface:

ICMP Detection Primary Server:

ICMP Detection Secondary Server:

ICMP Detection Interval (s):

ICMP Detection Timeout (s):

ICMP Detection Retries:

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 traffic.*

*\*DNS example: Google DNS Server 8.8.8.8 and 8.8.4.4*

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

### 3.12 Configuration -> Ethernet

R3000 Wireline router has four Ethernets, and Ethernet 0 can be configured as LAN or WAN interface, other Ethernets only can be configured as LAN interface.

This section allows users to configure the Ethernet parameters.

Port	IP	VLAN Trunk	DHCP	Loopback
<b>Switch Port Settings</b>				
Network Interface	Assigned To	VLAN	Media Type	Enable
Network Interface For Ethernet 0:	LAN 0 ▼	Vlan 0 ▼	Auto-negotiation ▼	<input checked="" type="checkbox"/>
Network Interface For Ethernet 1:	LAN 0 ▼	Vlan 0 ▼	Auto-negotiation ▼	<input checked="" type="checkbox"/>
Network Interface For Ethernet 2:	LAN 0 ▼	Vlan 0 ▼	Auto-negotiation ▼	<input checked="" type="checkbox"/>
Network Interface For Ethernet 3:	LAN 0 ▼	Vlan 0 ▼	Auto-negotiation ▼	<input checked="" type="checkbox"/>

Port		
Item	Description	Default
Network Interface	Include Ethernet 0~3.	/
Assigned To	Set the Ethernet as WAN or LAN interface. Select from "LAN0~3", "DMZ", "WAN". Only Ethernet 0 can be configured as WAN, only Ethernet can be configured as DMZ, and all the Ethernet can be configured as LAN.	LAN0
VLAN	Select "VLAN0"~"VLAN3".	VLAN1
Media Type	Select from "Auto-negotiation", "10Mbps Half Duplex", "10Mbps Full Duplex", "100Mbps Half Duplex", "100Mbps Full Duplex".	Auto-negotiation
Enable	Click to enable the Ethernet port.	Enable

Port	IP	VLAN Trunk	DHCP	Loopback
<b>WAN Interface</b>				
WAN Interface Type:		DHCP Client ▼		
<b>DHCP Client</b>				
<input checked="" type="checkbox"/> Use Peer DNS				
MTU:		1500		
<b>Override DHCP Server Values:</b>				
Netmask:				
Gateway:				

**WAN Interface**

WAN Interface Type: Static IP ▼

**Static IP**

IP Address:

NetMask:

Gateway:

MTU:

Primary DNS Server:

Secondary DNS Server:

**PPPoE (ADSL)**

Username:

Password:

Connection Mode: Always Online ▼

Redial Interval (s):

Retries:

Show Advanced Options

Service Name:

Local IP Address:

Remote IP Address:

Authentication: Auto ▼

Use Peer DNS

Address/Control Compression

Protocol Field Compression

Asyncmap Value:

MTU:

MRU:

Link Detection Interval (s):

Link Detection Max Retries:

Expert Options:

IP		
Item	Description	Default
WAN Interface	Select from "DHCP Client", "Static IP", "PPPoE (ADSL)".	DHCP Client
DHCP Client@WAN		
Use Peer DNS	Click to enable use peer DNS function, so that the router can obtain DHCP server's DNS address automatically.	Disable
Primary/Secondary DNS Server	Define the primary/secondary DNS Server which the DHCP clients will obtain from DHCP server.	Null



MTU, Netmask, gateway	Set the MTU, Netmask and gateway.	Null
<b>Static IP@WAN</b>		
IP Address, Netmask, Gateway, MTU, Primary/Secondary DNS Server	Set the static IP and related parameters for router which can access the Internet.	Null
<b>PPPoE (ADSL)</b>		
Username, password	Enter the PPPoE username and password which were provided from ISP.	Null
Connection Mode	Select from "Always Online" and "Connect On Demand". Always Online: Auto activates PPP and keeps the link up after power on. Connect On Demand: After selection this option, user could configure Triggered by Serial Data, Triggered by Periodically Connect and Triggered by Time Schedule. <b>Note:</b> If you select several connect on demand polices, router only have to meet one of them to be triggered.	Connect On Demand
Redial Interval	Router will automatically re-dial with this interval when it fails communicating to peer via TCP or UDP.	30
Retries	The maximum retries times for automatically re-connect when router fails to dial up. After successful connection, the Max Retries counter will be set to 0.	3
Inactivity Time	Configurable after "Connect On Demand" was selected. This field specifies the idle time setting for internet auto-disconnection. 0 means timeless.	0
Serial Output Content	The content which output to the serial device which connect to router and inform it that router is ready to receive serial data.	Null
Triggered by Serial Data	Tick this check box to allow router automatically connects to cellular network from idle mode when there is data comes out from serial port.	Enable
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
<b>Show Advanced Options</b>		
Service Name	Specify a PPPoE server's name. In general, can be not specified.	Null
Local IP Address	Specify a PPPoE server, and it will assign IP address for router. Enter the router's IP address in this item.	Null
Remote IP Address	Enter the PPPoE server's IP address. In general, can be not specified.	Null
Authentication	Select from "Auto", "PAP", "CHAP" according to the ISP.	Auto

Use Peer DNS	Click to enable this function; The router will automatically obtain the DNS server's IP address from ISP.	Enable
Address/Control Compression	Used for PPPOE initialization. Recommend default to disable.	Disable
Protocol Field Compression	Used for PPPOE initialization. Recommend default to disable.	Disable
Asynmap Value	Used for PPPOE initialization. Recommend default to disable.	ffffff
MTU	Maximum transmission unit. Set the MTU to allow the maximum length data packet to transmit.	1500
MRU	Maximum Receive unit. Set the MRU to allow the maximum length data packet to receive.	1500
Link Detection Interval (s)	Set the interval to detect the link if is disconnected.	60
Link Detection Max Retries	If it had detected the link is disconnected, router will retry to connect the internet. Please set the maximum retry times in this field.	5
Expert Options	Enter the some other PPP initialization string in this field. Each string separated by Spaces.	noccp nobsdcomp

**LAN Setting**

Name	IP Address	NetMask	MTU
LAN 0	172.16.99.99	255.255.0.0	1500
LAN 1	192.168.1.1	255.255.255.0	1500
LAN 2	192.168.2.1	255.255.255.0	1500
LAN 3	192.168.3.1	255.255.255.0	1500
DMZ	192.168.4.1	255.255.255.0	1500

**Multiple IP Address**

IP Address	NetMask
Add	

*Note: These parameters for LAN 0 only.*

**LAN Setting**

Item	Description	Default
Name , IP Address , Netmask , MTU	This section allow user to set the IP for LAN1~3 and DMZ. Also allow to set the related parameters.	/
Multiple IP Address		
IP Address, Netmask	Add the multiple IP for LAN0, the maximum number of IP address is 5. These parameters for LAN 0 only.	Null

Port IP **VLAN Trunk** DHCP Loopback

**VLAN Trunk Settings**

Enable VLAN Trunk

VLAN ID	IP Address	NetMask
---------	------------	---------

*Note: VLAN Trunk for LAN 0 only.*

VLAN Trunk		
Item	Description	Default
Enable VLAN Trunk	Click to enable the VLAN Trunk. The router can be packing or unpacking the VLAN tag.	Disable
VLAN ID	Set the VLAN ID, the maximum number of VLAN in router is 8.	Null
IP Address, Netmask	Set the IP address and Netmask of the VLAN.	Null

Port IP VLAN Trunk **DHCP** Loopback

**DHCP Server**

Enable DHCP Server

IP Pool Start:

IP Pool End:

NetMask:

Lease Time (min):

Primary DNS Server:

Secondary DNS Server:

Windows Name Server:

**Static Lease**

MAC Address	IP Address
-------------	------------

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

*Note: DHCP Server for LAN 0 only.*

**DHCP Relay Configuration**

Enable DHCP Relay

**DHCP Relay Configuration**

Enable DHCP Relay

DHCP Server:

DHCP		
Item	Description	Default
Enable DHCP Server	Enable to make router can lease IP address to DHCP clients which connect to Eth0.	Disable
IP Pool Start, IP Pool End	Define the beginning (IP Pool Start) and end (IP Pool End) of the pool of IP addresses which will lease to DHCP clients.	Null
Netmask	Define the Netmask which the DHCP clients will obtain from DHCP server.	Null
Lease Time	Define the time which the client can use the IP address which obtained from DHCP server.	60
Primary/Secondary DNS Server	Define the primary/secondary DNS Server which the DHCP clients will obtain from DHCP server.	Null
Windows Name Server	Define the WINS Server which the DHCP clients will obtain from DHCP server.	Null
Static Lease	Define to lease static IP Addresses, which conform to MAC Address of the connected equipment.	Null
DHCP Relay		
DHCP server	Router can support DHCP Relay. When DHCP client and DHCP server are not in the same subnet, DHCP Relay can provide a forwarding channel to those DHCP server and client. Please enter the DHCP server IP address in this field.	Null

Port
IP
VLAN Trunk
DHCP
Loopback

**Loopback Setting**

IP Address:

NetMask:

**Muti-IP Setting**

<input style="width: 95%;" type="text" value="IP Address"/>	<input style="width: 95%;" type="text" value="NetMask"/>
<input type="button" value="Add"/>	

Loopback		
Item	Description	Default
IP Address	Loopback is a virtual interface, we usually set it IP as 127.0.0.1.	127.0.0.1
Netmask	Set the Netmask for loopback	255.0.0.0
Muti-IP Setting	R3000 Wireline can support multiple loopback interface, please set the IP address and netmask in this list.	Null

### 3.13 Configuration -> WiFi

This section allows users to set parameters of WiFi.

Basic
MAC Filter
Status

**WiFi Basic Settings**

Enable WiFi

Mode: AP

Channel: Auto

SSID: Router\_AP

Hide SSID:

Security Mode: Open

---

**WiFi Network Settings**

*\*WiFi interface bridged with eth1, network settings please refer to this page.*

**Note:** when R3000 Wireline enable WiFi feature and works as AP mode

Basic
Status

**WiFi Basic Settings**

Enable WiFi

Mode: Client

Channel: Auto

SSID: Router\_AP Scan

Hide SSID:

Security Mode: Open

---

**WiFi Network Settings**

IP Configuration: DHCP Client

Use Peer DNS

**Override DHCP Server Values:**

Netmask:

Gateway:

**Note:** when R3000 Wireline enable WiFi feature and works as Client mode

Basic @ WiFi		
Item	Description	Default
Enable WiFi	Click to enable WiFi feature.	Null
Mode	This item will show "AP" and "Client", cannot be configured. AP: In a wireless local area network (WLAN), an access point is a station that transmits and receives data. When R3000 Wireline is wanted to work as "AP" mode, please go to tab "Configuration" -> "Link Management" -> "Primary Interface" to select "Eth0" as WAN link.	Null

	<p>Client: When R3000 Wireline works as Client mode, it can be used as an Ethernet-to-wireless (or LAN-to-WLAN) network adaptor. For example, a notebook computer equipped with an Ethernet adaptor but no wireless card can be connected to the router with an Ethernet cable to provide wireless connectivity to another AP. When R3000 Wireline is wanted to work as “Client” mode, please go to tab “Configuration” -&gt; “Link Management” -&gt; “Primary Interface” to select “WiFi” as WAN link.</p>	
Channel	<p>Select the frequency channel, which includes “Auto”, “1”, “2” ..... “13”.</p> <p>Auto: R3000 Wireline will scan all frequencies until it finds one with an available access point or wireless network it can join.</p> <p>1~13: R3000 WIRELINE will be fixed to work with this channel.</p>	Auto
SSID	<p>SSID (service set identifier) is the network name of the WLAN. The SSID of a client and the SSID of the AP must be identical for the client and AP to be able to communicate with each other.</p> <p>When R3000 Wireline works as Client mode, enter SSID of the access point which R3000 Wireline want to connect.</p> <p>Input from 1 to 31 characters.</p>	Router_AP
Hide SSID	<p>When R3000 Wireline works as AP mode, after clicking this check box R3000 Wireline will not broadcast the SSID. Other wireless devices cannot discover this access point automatically. User need to enter the SSID manually to let their wireless devices join this access point.</p> <p>When R3000 Wireline works as Client mode and need to connect to any access point which has ensconced SSID, you need to enter this SSID manually in tab “SSID” and then click “Hide SSID”.</p>	Disable
Security mode	<p>Select from “Open”, “WPA”, “WPA2” and “WEP”.</p> <p>Open: No authentication. For security reasons, you should NOT set security mode to Open System, since authentication and data encryption are NOT performed in Open System mode.</p> <p>WPA/WPA2: Personal versions of WPA/WPA2 (Wi-Fi Protected Access), also known as WPA/WPA-PSK (Pre-Shared Key), provide a simple way of encrypting a wireless connection for high confidentiality. WPA2 is a stronger security feature than WPA.</p> <p>WEP: Wired Equivalent Privacy, provide encryption for wireless device’s data transmission.</p> <p><b>Note:</b> R3000 Wireline supports WPA/WPA2 Personal version, not enterprise version.</p>	Open
Encryption	<p>Select from “TKIP” and “CCMP (AES)”.</p> <p>TKIP: Temporal Key Integrity Protocol (TKIP) encryption is used over the wireless link. TKIP encryption can be used with WPA-PSK and WPA with 802.1x authentication.</p> <p>CCMP (AES): CCMP (AES) encryption is used over the wireless link. CCMP can be used WPA-PSK and WPA with 802.1x authentication.</p> <p><b>Note:</b> CCMP (AES) is a stronger encryption algorithm than TKIP.</p>	CCMP (AES)

Passphrase	<p>When R3000 Wireline works as AP mode, enter Master key to generate keys for encryption. A Passphrase is used as a basis for encryption methods (or cipher types) in a WLAN connection. The passphrases should be complicated and as long as possible. For security reasons, this passphrase should only be disclosed to users who need it, and it should be changed regularly.</p> <p>When R3000 Wireline works as Client mode, enter access point's passphrase which it wants to connect to.</p> <p>Input from 8 to 63 characters.</p>	Null
Key Renewal Interval(s)	<p>Enter the time period of group key renewal.</p> <p><b>Note:</b> Only for AP mode.</p>	3600
WiFi Network Settings	<p>When R3000 Wireline works as AP mode, Click to link to page "Eth1" to check the network settings, WiFi interface bridged with eth1 this time.</p> <p>When R3000 Wireline works as Client mode, this item is used to do IP configuration of access point.</p>	Null

Basic
MAC Filter
Status

**MAC Filter Settings**

Enable ACL:

Mode: Allow ▼

**Access Control List**

Index	MAC Address
<input type="button" value="Add"/>	

**Note:** Available when R3000 Wireline enable WiFi feature and works as AP mode

Mac Filter @ WiFi (Only for AP mode)		
Enable ACL	Click to enable ACL (Access Control List).	Disable
Mode	<p>Select from "Allow" and "Deny".</p> <p>Allow: Only the packets fitting the entities of the "Access Control List" can be allowed.</p> <p>Deny: All the packets fitting the entities of the "Access Control List" will be denied.</p> <p><b>Note:</b> R3000 Wireline can only allow or deny devices which are included in "Access Control List" at one time.</p>	Allow
Access Control List	Click "Add" to add MAC address.	Null

Basic
MAC Filter
Status

**Status**

BSSID:

SSID:

Mode:

Key Management:

Cipher Pairwise:

Cipher Group:

WPA State:

Address:

**Associated Clients**

Index	BSSID	IP Address
-------	-------	------------

Status @ WiFi		
BSSID	Show MAC address of R3000 Wireline’s WiFi interface or the access point which R3000 Wireline connects to.	Null
SSID	Show SSID of R3000 Wireline’s WiFi interface or the access point which R3000 Wireline connects to.	Null
Mode	Show current mode of R3000 Wireline: AP or Client.	Null
Key Management	Show current security mode of R3000 Wireline or the access point which R3000 Wireline connects to.	Null
Cipher Pairwise	Show current encryption algorithm of R3000 Wireline or the access point which R3000 Wireline connects to.	Null
Cipher Group		
WPA State	<p>Show current WPA status. Mainly there are 5 statuses: Disconnected, Scanning, Initializing, Associated, 4way_handshark, Completed.</p> <p>Disconnected: Not associated or connected with any access point, perhaps because the wireless device has not fully initialized, is out of range, or the wireless interface is disconnected because the Ethernet interface is enabled.</p> <p>Scanning: Searching for a wireless network (access point) for connection.</p> <p>Initializing: R3000 Wireline is setting up initial wireless environment.</p> <p>Associated: This state is entered when the driver reports that association has been successfully completed with an AP, but still waiting for authentication.</p> <p>4way_handshark: This state is entered when WPA/WPA2 4-Way Handshake is started. When Passphrase do not match, it will show this status.</p> <p>Completed: The wireless connection of R3000 Wireline and other wireless devices are established.</p>	Null



Address	Show the MAC address of R3000 Wireline’s WiFi interface.	Null
Associated Clients @ AP mode	Show current associated wireless client devices’ BSSID and IP address.	Null
Scan Results @ Client mode	Show current scan results of any wireless network (access point), such as SSID, Channel, Signal Level, Flags (the security mode and encryption algorithm flags of access point).	Null

### 3.14 Configuration -> Serial

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

RS232

**Serial Port Settings**

Baudrate:

Data Bit:

Parity:

Stop Bit:

Flow Control:

---

**Protocol Settings**

Protocol:

None

Transparent

Modbus Gateway

Transparent over Rlink

Modbus over Rlink

AT over COM

GPS Report

- When Select Protocol “Transparent”:

**Protocol Settings**

Protocol:

Mode:

Local Port:

Show Protocol Advanced

Interval Timeout (1\*10ms):

Packet Length:

Enable Delimiter1

Delimiter1 (Hex):

Enable Delimiter2

Delimiter2 (Hex):

Delimiter Process:

- When Select Protocol “Modbus gateway”:

**Protocol Settings**

Protocol:

Local IP:

Local Port:

Attached serial device type:

- When Select Protocol “Transparent Over Rlink”:

**Protocol Settings**

Protocol:

Interval Timeout (1\*10ms):

- When Select Protocol “Modbus Over Rlink”:

**Protocol Settings**

Protocol:

Attached serial device type:

- When Select Protocol “AT Over COM”:

**Protocol Settings**

Protocol:

Display all com (Note enable this function will disable cellular WAN.)

COM Name:

- When Select Protocol “GPS Report”:

**Protocol Settings**

Protocol:

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 gateway”, “Transparent Over Rlink”, “Modbus Over Rlink” “AT Over COM” and “GPS Report”. 1. None: Router will do nothing in RS232 serial port.	None

	<ol style="list-style-type: none"> <li>2. Transparent: Router will transmit the serial data transparently without any protocols.</li> <li>3. Modbus gateway: Router will translate the Modbus RTU data to Modbus TCP data and vice versa.</li> <li>4. Transparent Over Rlink: Router will send all data from RS232 serial port to Robustlink, then Robustlink will forward the data to another destination site.</li> <li>5. Modbus Over Rlink: Router will translate all data from RS232 serial port to Modbus TCP protocol data, and then send to Robustlink, after that Robustlink will forward the data to another destination site.</li> <li>6. AT Over COM: select to operate router via RS232 COM port. For example, enter AT commands to router via RS232 COM port.</li> <li>7. GPS Report: select to enable router to output GPS status data through RS232 port.</li> </ol>	
Mode @Transparent	<p>Select from "TCP Server", "TCP Client" and "UDP".</p> <p>TCP Client: Router works as TCP client, initiate TCP connection to TCP server. Server address supports both IP and domain name.</p> <p>TCP Server: Router works as TCP server, listening for connection request from TCP client.</p> <p>UDP: Router works as UDP client.</p>	TCP Client
Local Port @Transparent	Enter the Local port for TCP or UDP.	0
Multiple Server @Transparent	<p>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.</p> <p><b>Note:</b> This section will not be displayed if you select "TCP server" in "Mode".</p>	None
show Protocol Advanced @Transparent	Tick to enable protocol advanced setting.	Disable
Local IP @Transparent	<p>This item will show up when you enable any VPN tunnel of R3000 Wireline, it means serial data can be matched to this local IP address and be transmitted or received via VPN tunnel.</p> <p><b>Note:</b> when you do not enable any VPN tunnel, this item will not show up.</p>	Null
Interval Timeout @Transparent	<p>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.</p> <p><b>Note:</b> 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.</p>	10
Packet Length @Transparent	<p>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.</p> <p><b>Note:</b> Data will also be sent as specified by the interval timeout or delimiter</p>	1360

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

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

RS485

---

**Serial Port Settings**

Baudrate:

Data Bit:

Parity:

Stop Bit:

**Protocol Settings**

Protocol:

- When Select Protocol “Transparent”:

**Protocol Settings**

Protocol:

Mode:

Local Port:

Show Protocol Advanced

Interval Timeout (1\*10ms):

Packet Length:

Enable Delimiter1

Delimiter1 (Hex):

Enable Delimiter2

Delimiter2 (Hex):

Delimiter Process:

- When Select Protocol “Modbus Master”:

When you select protocol “Modbus Master”, you can configure the “Modbus Master” in section 3.32.

**Protocol Settings**

Protocol:

- When Select Protocol “Modbus gateway”:

**Protocol Settings**

Protocol:

Local IP:

Local Port:

Attached serial device type:

- When Select Protocol “Transparent Over Rlink”:

**Protocol Settings**

Protocol:

Interval Timeout (1\*10ms):

- When Select Protocol “Modbus Over Rlink”:

**Protocol Settings**

Protocol:

Attached serial device type:

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”, “Modbus Master” and “Modbus gateway”, “Transparent Over Rlink” and “Modbus Over Rlink”. Transparent: Router will transmit the serial data transparently without any protocols. Modbus gateway: Router will transmit the serial data with Modbus protocol. Modbus Master: R3000 Wireline router could be configured as a modbus master, and will automatically poll the slave sides. Transparent Over Rlink: Router will send all data from RS232 serial port to Robustlink, and then Robustlink will forward the data to another destination site.	Transparent

	Modbus Over Rlink: Router will translate all data from RS232 serial port to Modbus TCP protocol data, and then send to Robustlink, after that Robustlink will forward the data to another destination site.	
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. <b>Note:</b> This section will not be displayed if you select "TCP server" in "Mode".	Null
Enable Protocol @Transparent	Tick to enable protocol advanced setting.	Disable
Local IP @ Transparent	This item will show up When you enable any VPN tunnel of R3000 Wireline, it means serial data can be matched to this local IP address and be transmitted or received via VPN tunnel. <b>Note:</b> when you do not enable any VPN tunnel, this item will not show up.	0
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. <b>Note:</b> 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. <b>Note:</b> Data will also be sent as specified by the interval timeout or delimiter settings even when data is not reaching the preset packet length.	1360
Enable Delimiter1	When Delimiter 1 is enabled, the serial port will queue the data in the buffer and send the data to the Cellular WAN/Ethernet WAN when a specific character, entered in hex format, is received. A second delimiter character may be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to control when data should be sent.	Disable
Delimiter1 (Hex) @ Transparent	Enter the delimiter in Hex.	0
Delimiter Process @ Transparent	The Delimiter process field determines how the data is handled when a delimiter is received. None: Data in the buffer will be transmitted when the delimiter is received; the data also includes the delimiter characters. Strip: Data in the buffer is first stripped of the delimiter before being	Strip

	transmitted.	
Local IP @ Modbus gateway	This item will show up When you enable any VPN tunnel of R3000 Wireline, it means serial data can be matched to this local IP address and be transmitted or received via VPN tunnel. <b>Note:</b> when you do not enable any VPN tunnel, this item will not show up.	0
Local Port @ Modbus gateway	Enter the Local port for Modbus.	0
Attached serial device type @ Modbus gateway	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 gateway	Add the Modbus slaves which will be polled by Modbus master (router). This section only displayed when you select “Modbus RTU master” or “Modbus ASCII master” in “Attached serial device type”.	Null
Slave Address @ Modbus Slave	This connection is usually used to connect to the Modbus slave devices which as TCP server. Enter IP address of the TCP server.	Null
Slave Port @ Modbus Slave	Enter the port number of TCP server.	Null
ID @ Modbus Slave	Enter the ID number of TCP server.	Null
Interval Timeout @ Transparent Over Rlink	Serial port will queue the data in buffer and then send it to the Cellular WAN/Ethernet WAN when it reaches the Interval Timeout in this field.	10
Attached serial device type @ Modbus Over Rlink	Select From “Modbus RTU slave”, “Modbus ASC II slave”. 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 slave

### 3.15 Configuration -> USB

This section allows users to set the USB parameters.

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



**USB**

**USB Configuration**

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

USB		
Item	Description	Default
Enable automatic update of configuration	Click Enable to automatically update the configuration file of R3000 Wireline when insert the USB storage devices which has R3000 Wireline’s configuration file.	Disable
Enable automatic update of firmware	Click Enable to automatically update the firmware of R3000 Wireline when insert the USB storage devices which has R3000 Wireline’s firmware.	Disable

### 3.16 Configuration -> GPS

This section allows users to set the GPS setting parameters.

**GPS Setting**    **GPS Status**    **Map**

**Enable GPS**

- Enable GPS

**GPS Basic Setting**

- Report To RS232
- RS232 Report Type:
- RS232 Report Interval:

**GPS Server Setting**

Index	Server Name
	<input type="text"/>

**GPS Server**

- Enable
- Report Type:
- Report Interval:
- Socket Type:
- Local Port:

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

This section allows users to check the GPS status.

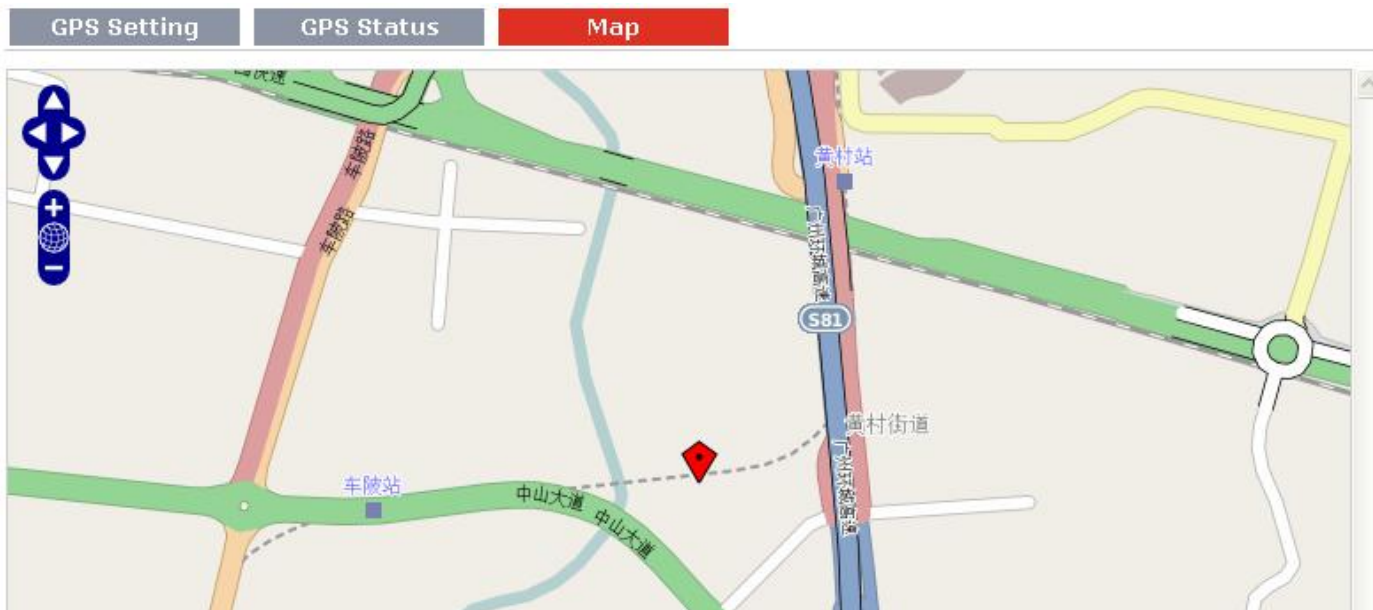
GPS Setting
**GPS Status**
Map

**GPS Status**

GPS Status:	No Fix/Invalid
Last Fixed Time:	
Last Failed Time:	
Satellites In Use:	0
Satellites In View:	1
UTC:	2000-00-00 00:00:00
Latitude:	0.000000
Longitude:	0.000000
Altitude:	0.000000
Speed:	0.000000KMH

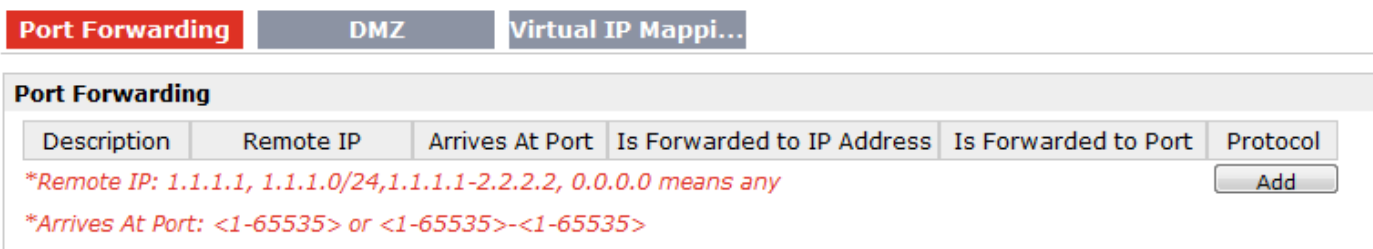
GPS Status @ GPS		
Item	Description	Default
GPS Status	<p>Show the GPS Status.</p> <p>GPS status includes: Not Installed, Disabled, No Fix/Invalid, Standalone GPS Fix, Differential GPS Fix.</p> <p>Not Installed: No GPS module inside.</p> <p>Disabled: GPS function is not enabled (not click "Enable GPS"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

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



### 3.17 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 **DMZ** Virtual IP Mappi...

**Enable DMZ**

Enable DMZ

**DMZ Settings**

DMZ Host:

Source Address:

*\*1.1.1.1", "1.1.1.0/24", "1.1.1.1-2.2.2.2", "0.0.0.0" means any*

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

Port Forwarding **DMZ** **Virtual IP Mappi...**

**Virtual IP Mapping Setting**

Virtual IP for Router:

**Internal PC's IP Mapping List**

Description	Virtual IP	Real IP
<input type="button" value="Add"/>		

Virtual IP Mapping@ NAT/DMZ		
Item	Description	Default
Virtual IP for Router	Set a Virtual IP for router.	Null
Virtual IP @ Internal PC's IP Mapping List	Set a Virtual IP for the Internal PC.	Null
Real IP @ Internal PC's IP Mapping List	The Internal PC's Real IP, which is mapping the PC's Virtual IP one-to-one.	Null

### 3.18 Configuration -> Firewall

This section allows users to set the firewall parameters.

- Basic
- Filtering
- MAC-Binding

**Filter Basic Settings**

- Remote Access Using HTTP
- Remote Access Using TELNET
- Remote Access Using SNMP
- Remote Access Using SSH2
- Remote Ping Request
- Enable DNS Masquerade
- Enable Console CLI
- Defend DoS Attack

Basic @ Firewall		
Item	Description	Default
Remote Access Using HTTP	Enable to allow users to access the router remotely on the internet side via HTTP.	Enable
Remote Access Using TELNET	Enable to allow users to access the router remotely on the internet side via Telnet.	Enable
Remote Access Using SNMP	Enable to allow users to access the router remotely on the internet side via SNMP.	Enable
Remote Access Using SSH2	Enable to allow users to access the router remotely on the internet side via SSH2.	Enable
Remote Ping Request	Enable to make router reply the Ping requests from the internet side.	Enable
Enable DNS Masquerade	Open the 53 port of the router, enable users to use the DNS function of the router.	Enable
Enable Console CLI	Enable to configurate router through Command Line Interface.	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

Basic
Filtering
MAC-Binding

**Default Filter Policy**

Accept
  Drop

**Add Filter List**

Action	Description	Source IP	Source Port	Target IP Address	Target Port	Protocol
*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: <1-65535> or <1-65535>-<1-65535>						
						<input type="button" value="Add"/>

**Blocking By URL Address**

Description	URL
<input type="button" value="Add"/>	

**Blocking By Keyword**

Description	Keyword
<input type="button" value="Add"/>	

Filtering @ Firewall		
Item	Description	Default
Default Filter Policy	Select from "Accept" and "Drop". Accept: Router will accept all the data traffic except the hosts which were added in the drop list. Drop: Router will drop all the data traffic except the hosts which were added in the accept list.	Accept
Add Filter List	Click "Add" to add a filter list.	Null
Action @Add Filter List	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 @ Add Filter List	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 @ Add Filter List	Defines if access is allowed from one or a range of port which is defined by Source Port.	Null
Target IP Address @ Add Filter List	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 @ Add Filter List	Defines if access is allowed to one or a range of port which is defined by Target Port.	Null
Protocol @ Add Filter List	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
Blocking By URL Address	Click "Add" to add a URL list.	Null

URL@ Blocking By URL Address	Block the access according to the URL that filled in the blank.	Null
Blocking By Keywork	Click "Add" to add a Keywork list.	Null
Keywork@ Blocking By Keywork	Block the access according to the Keywork that filled in the blank.	Null

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

Basic
Filtering
MAC-Binding

**MAC-IP Binding List**

Description	MAC Address	IP Address
*MAC: ff:ff:ff:ff:ff:ff		
		<input type="button" value="Add"/>

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



### 3.19 Configuration -> QoS

This section allows users to set the QoS parameters.

QoS

**Enable Quality Of Service(QoS)**

Enable QoS

**Quality of Service(QoS) Basic Setting**

Downlink Speed (kbps):

Uplink Speed (kbps):

Optimize for TCP Flags:  SYN  ACK  FIN  RST

Optimize for ICMP:

Optimize for Serial Data Forwarding:

Priority Percent Definition:

Exempt:

Premium:

Express:

Normal:

Bulk:

Default Priority:  ▾

**QoS Service Control List**

Service Name	Protocol	Port	Priority
<input type="button" value="Add"/>			

**QoS MAC Control List**

MAC Address	Priority
*MAC: ff:ff:ff:ff:ff:ff	<input type="button" value="Add"/>

**QoS IP Control List**

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

QoS		
Item	Description	Default
Enable QoS	Click to enable "QoS" function.	Disable
Downlink Speed (kbps)	Prescribe downlink speed of router. <b>Note:</b> Default setting "0" means that there is no limitation of downlink speed.	0
uplink Speed (kbps)	Prescribe uplink speed of router. <b>Note:</b> Default setting "0" means that there is no limitation of uplink speed.	0
Optimize for TCP Flags	User can choose to enable TCP flags: "SYN", "ACK", "FIN", "RST", which means data with above TCP Flags will get the highest priority to occupy bandwidth. After enabled, router will enhance respond timeout of TCP control, in case that data	Disable

	resend frequently.	
Optimize for ICMP	<p>Enable to optimize for ICMP, which means ICMP will get the highest priority to occupy bandwidth. After enabled respond interval of PING control will be shorter.</p> <p><b>Note:</b> if user click to enable “Optimize for TCP Flags”, “Optimize for Serial Data Forwarding”, and “Optimize for ICMP” at the same time (these three services are in the same priority level), router will automatically start Stochastic Fairness Queueing (SFQ) strategy to make a fair bandwidth allocation, in case of one service occupy all the bandwidth.</p>	Disable
Optimize for Serial Data Forwarding	<p>Enable to optimize for serial data forwarding, which means serial data forwarding will get the highest priority to occupy bandwidth.</p> <p>When enable serial data forwarding it need to enable local port number for controlling. Therefore, it needs to set local port number of router even if router is as TCP Client.</p>	Disable
Priority Percent Definition	<p>Define priority percent of “Exempt”, “Premium”, “Express”, “Normal” and “Bulk”. “Exempt” is defaulted as 50; “Premium” is defaulted as 25; “Express” is defaulted as 15; “Normal” is defaulted as 10; “Bulk” is 1.</p>	
Default Priority	<p>Select from “Exempt”, “Premium”, “Express”, “Normal” and “Bulk”. Users (Services) with no other pre-priority set will use this default priority.</p> <p>Exempt: this is the highest priority which guarantees that the minimum global rate of router is 50% of “Downlink Speed”, and the maximum rate can reach to 100% of “Downlink Speed”.</p> <p>Premium: guarantees that the minimum global rate of router is 25% of “Downlink Speed”, and the maximum rate can reach to 100% of “Downlink Speed”.</p> <p>Express: guarantees that the minimum global rate of router is 15% of “Downlink Speed”, and the maximum rate can reach to 100% of “Downlink Speed”.</p> <p>Normal: guarantees that the minimum global rate of router is 10% of “Downlink Speed”, and the maximum rate can reach to 100% of “Downlink Speed”.</p> <p>Bulk: guarantees that the minimum global rate of router is 1% of “Downlink Speed”, and the maximum rate can reach to 100% of “Downlink Speed”.</p>	Normal
MAC Address @ QoS MAC Control List	<p>Enter MAC address of the user (for example, PC) who you want to set it with QoS Control. Router supports up to 20 users set with QoS MAC Control. Priority of QoS MAC Control is higher than that of QoS IP control.</p>	Null
Priority @ QoS MAC Control List	<p>Select from “Exempt”, “Premium”, “Express”, “Normal” and “Bulk”.</p> <p>Select the priority of the user (for example, PC) who you want to set it with QoS Control.</p> <p>Exempt: this is the highest priority which guarantees that the minimum global rate of router is 50% of “Downlink Speed”, and the maximum rate can reach to 100% of “Downlink Speed”.</p> <p>Premium: guarantees that the minimum global rate of router is 25% of “Downlink Speed”, and the maximum rate can reach to 100% of “Downlink Speed”.</p> <p>Express: guarantees that the minimum global rate of router is 15% of “Downlink Speed”, and the maximum rate can reach to 100% of “Downlink Speed”.</p>	Exempt

	<p>Normal: guarantees that the minimum global rate of router is 10% of “Downlink Speed”, and the maximum rate can reach to 100% of “Downlink Speed”.</p> <p>Bulk: guarantees that the minimum global rate of router is 1% of “Downlink Speed”, and the maximum rate can reach to 100% of “Downlink Speed”.</p>	
IP Address @ QoS IP Control List	<p>Enter IP address of the user (for example, PC) who you want to set it with QoS Control. Router supports up to 20 users set with QoS IP Control. If want to control one network segment, user can set “IP Address” as format “x.x.x.x/24” or “x.x.x.x/255.255.255.0”. For example, if we to control network segment “172.16.x.x”, we can set “172.16.0.0/16” or “172.16.0.0/255.255.0.0” in “IP Address”.</p>	Null
Priority @ QoS IP Control List	<p>Select from “Exempt”, “Premium”, “Express”, “Normal” and “Bulk”.</p> <p>Select the priority of the user (for example, PC) who you want to set it with QoS Control.</p> <p>Exempt: this is the highest priority which guarantees that the minimum global rate of router is 50% of “Downlink Speed”, and the maximum rate can reach to 100% of “Downlink Speed”.</p> <p>Premium: guarantees that the minimum global rate of router is 25% of “Downlink Speed”, and the maximum rate can reach to 100% of “Downlink Speed”.</p> <p>Express: guarantees that the minimum global rate of router is 15% of “Downlink Speed”, and the maximum rate can reach to 100% of “Downlink Speed”.</p> <p>Normal: guarantees that the minimum global rate of router is 10% of “Downlink Speed”, and the maximum rate can reach to 100% of “Downlink Speed”.</p> <p>Bulk: guarantees that the minimum global rate of router is 1% of “Downlink Speed”, and the maximum rate can reach to 100% of “Downlink Speed”.</p>	Exempt
Service Name @ QoS Service Control List	<p>Set server name of the service that you want to set it with QoS Control. Router supports up to 20 users set with QoS Service Control. Priority of QoS Service Control is higher than that of both QoS IP control and QoS MAC control.</p>	Null
Protocol @ QoS Service Control List	<p>Select from “TCP”, “UDP” and “TCP&amp;UDP”.</p>	TCP
Port @ Service Control List	<p>Enter the port number of the service that you want to set it with QoS Control.</p>	Null
Priority @ QoS Service Control List	<p>Select from “Exempt”, “Premium”, “Express”, “Normal” and “Bulk”.</p> <p>Select the priority of the service that you want to set it with QoS Control.</p> <p>Exempt: this is the highest priority which guarantees that the minimum global rate of router is 50% of “Downlink Speed”, and the maximum rate can reach to 100% of “Downlink Speed”.</p> <p>Premium: guarantees that the minimum global rate of router is 25% of “Downlink Speed”, and the maximum rate can reach to 100% of “Downlink Speed”.</p> <p>Express: guarantees that the minimum global rate of router is 15% of “Downlink Speed”, and the maximum rate can reach to 100% of “Downlink Speed”.</p> <p>Normal: guarantees that the minimum global rate of router is 10% of “Downlink Speed”, and the maximum rate can reach to 100% of “Downlink Speed”.</p> <p>Bulk: guarantees that the minimum global rate of router is 1% of “Downlink Speed”, and the maximum rate can reach to 100% of “Downlink Speed”.</p>	Exempt

**Note:** If services are in the same priority level, router will automatically start Stochastic Fairness Queueing (SFQ) strategy to make a fair bandwidth allocation.

### 3.20 Configuration -> IP Routing

This section allows users to set the IP routing parameters.

Static Route
RIP
OSPF

---

**Static Route Table**

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

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
RIP
OSPF

---

**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

---

**Network List**

Network Address	NetMask
<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

Static Route    RIP    **OSPF**

**OSPF Protocol**

Enable OSPFv2

OSPF @ IP Routing		
Item	Description	Default
OSPF	OSPF (Open Shortest Path First) is a link-state routing protocol for IP networks. It uses a link state routing algorithm and falls into the group of interior routing protocols, operating within a single autonomous system (AS).	Null
Enable OSPFv2	Tick to enable OSPF function.	Disable

### 3.21 Configuration -> DynDNS

This section allows users to set the DynDNS parameters.

**DynDNS**

**DynDNS Settings**

Enable DynDNS

Service Type:

Hostname:

Username:

Password:

DynDNS Status: *DynDNS is initializing.....*

DynDNS		
Item	Description	Default
DynDNS	The Dynamic DNS function allows you to alias a dynamic IP address to a static domain name, allowing users whose ISP does not assign them a static IP address to use a domain name. This is especially useful for hosting servers via your connection, so that anyone wishing to connect to you may use your domain name, rather than having to use your dynamic IP address, which changes from time to time. This dynamic IP address is the WAN IP address of the router, which is assigned to you by your ISP.	Null
Enable DynDNS	Tick to enable DynDNS function.	Disable
Service Type	Select the DDNS service from “DynDNS–Dynamic”, “QDNS (3322)” and “NOIP” which you have established an account with. “Custom” could be used for linking custom DDNS server.	DynDNS–Dynamic
hoastmen	Enter the Host name the DDNS server provided.	Null

Username	Enter the user name the DDNS server provided.	Null
Password	Enter the password the DDNS server provided.	Null
URL	Enter the connection address of custom DDNS server.	Null
Force Update	Click to the update and use the DynDNS settings.	Null
DynDNS Status	Show current status of DynDNS	Null

### 3.22 Configuration -> DMVPN

This section allows users to set the DMVPN parameters.

**DMVPN**

**DMVPN Setting**

Enable DMVPN

Hub Address:

GRE Local IP address:

GRE HUB IP address:

GRE Netmask:

GRE Secrets:

Negotiation Mode: Main ▾

Local IP Type: DEFAULT ▾

Encryption Algorithm: 3DES ▾

Authen Algorithm: MD5 ▾

DH Group: MODP1024\_2 ▾

PSK Secrets:

SA Algorithm: 3DES\_MD5\_96 ▾

PFS Group: PFS\_NULL ▾

Nhrp Cisco secrets:

Nhrp Holdtime:

DMVPN		
Item	Description	Default
Hub Address	DMVPN Hub's IP address or domain	Null
GRE Local IP address	GRE Local tunnel IP address	Null
GRE HUB IP address	GRE Hub tunnel IP address	Null
GRE Netmask	GRE tunnel Netmask	Null
GRE Secrets	GRE tunnel secret key	Null
Negotiation Mode	Select from "Main" and "aggressive" for the IKE negotiation mode in phase 1. If the IP address of one end of an IPSec tunnel is obtained dynamically, the IKE negotiation mode must be aggressive. In this case, SAs can be established as long as the username and password are correct.	Main
Local IP Type	Select from "ID", "FQDN" and "User FQDN" for IKE negotiation. "Default" stands	default

	<p>for "Router's extern IP".</p> <p>ID: Uses custom string as the ID in IKE negotiation.</p> <p>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.</p> <p>User FQDN: Uses a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with an sign "@" for the local security gateway, e.g., test@robustel.com.</p>	
Encryption Algorithm	<p>Select from "DES", "3DES" and "AES128" to be used in IKE negotiation.</p> <p>DES: Uses the DES algorithm in CBC mode and 56-bit key.</p> <p>3DES: Uses the 3DES algorithm in CBC mode and 168-bit key.</p> <p>AES128: Uses the AES algorithm in CBC mode and 128-bit key.</p>	3DES
Authen Algorithm	<p>Select from "MD5" and "SHA1" to be used in IKE negotiation.</p> <p>MD5: Uses HMAC-SHA1.</p> <p>SHA1: Uses HMAC-MD5.</p>	MD5
DH Group	<p>Select from "MODP768_1", "MODP1024_2" and "MODP1536_5" to be used in key negotiation phase 1.</p> <p>MODP768_1: Uses the 768-bit Diffie-Hellman group.</p> <p>MODP1024_2: Uses the 1024-bit Diffie-Hellman group.</p> <p>MODP1536_5: Uses the 1536-bit Diffie-Hellman group.</p>	MODP1024_2
PSK Secrets	Enter Pre-shared Key	Null
SA Algorithm	<p>Select from "DES_MD5_96", "DES_SHA1_96", "3DES_MD5_96", "3DES_SHA1_96", "AES128_MD5_96", "AES128_SHA1_96" when you select "ESP" in "Protocol";</p> <p>Select from "AH_MD5_96" and "AH_SHA1_96" when you select "AH" in "Protocol";</p> <p><b>Note:</b> 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.</p>	3DES_MD5_96
PFS Group	<p>Select from "PFS_NULL", "MODP768_1", "MODP1024_2" and "MODP1536_5".</p> <p>PFS_NULL: Disable PFS Group</p> <p>MODP768_1: Uses the 768-bit Diffie-Hellman group.</p> <p>MODP1024_2: Uses the 1024-bit Diffie-Hellman group.</p> <p>MODP1536_5: Uses the 1536-bit Diffie-Hellman group.</p>	PFS_NULL
Nhrp Cisco secret	Cisco Nhrp secret key	Null
Nhrp holdtime	The hold time of Nhrp protocol	60



### 3.23 Configuration -> IPsec

This section allows users to set the IPsec parameters.

IPsec Basic
IPsec Tunnel
X.509

**IPsec Basic**

Enable NAT Traversal

Keepalive Interval(s):

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
IPsec Tunnel
X.509

**IPsec Tunnel**

Tunnel name	Description

**IPsec Common**

IPsec Gateway Address:

IPsec Mode: Tunnel ▼

IPsec Protocol: ESP ▼

Local Subnet:

Local Subnet Mask:

Local ID Type: Default ▼

Remote Subnet:

Remote Subnet Mask:

Remote ID Type: Default ▼

**IKE Parameter**

Negotiation Mode:

Encryption Algorithm:

Authentication Algorithm:

DH Group:

Authentication:

Secrets:

Life Time(s):

**SA Parameter**

SA Algorithm:

PFS Group:

Life Time(s):

DPD Time Interval (s):

DPD Timeout (s):

**IPsec Advanced**

Enable Compress

Enable ICMP Detection

ICMP Detection Server:

ICMP Detection Local IP:

ICMP Detection Interval (s):

ICMP Detection Timeout (s):

ICMP Detection Retries:

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 an sign "@" for the local security gateway, e.g., test@robustel.com.	Default
Remote Subnet	Enter IPSec Remote Protected subnet's address.	0.0.0.0
Remote Subnet Mask	Enter IPSec Remote Protected subnet's mask.	0.0.0.0
Remote ID Type	Select from "IP Address", "FQDN" and "User FQDN" for IKE negotiation. IP Address: Uses an IP address as the ID in IKE negotiation. FQDN: Uses an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security gateway, e.g., test.robustel.com. User FQDN: Uses a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with a sign "@" for the local security gateway, e.g., test@robustel.com.	Default
Negotiation Mode	Select from "Main" and "aggressive" for the IKE negotiation mode in phase 1. If the IP address of one end of an IPSec tunnel is obtained dynamically, the IKE negotiation mode must be aggressive. In this case, SAs can be established as long as the username and password are correct.	Main
Encryption Algorithm	Select from "DES", "3DES", "AES128", "AES192" and "AES256" to be used in IKE negotiation. DES: Uses the DES algorithm in CBC mode and 56-bit key. 3DES: Uses the 3DES algorithm in CBC mode and 168-bit key. AES128: Uses the AES algorithm in CBC mode and 128-bit key. AES192: Uses the AES algorithm in CBC mode and 192-bit key. AES256: Uses the AES algorithm in CBC mode and 256-bit key.	3DES
Authentication Algorithm	Select from "MD5" and "SHA1" to be used in IKE negotiation. MD5: Uses HMAC-SHA1. SHA1: Uses HMAC-MD5.	MD5
DH Group	Select from "MODP768_1", "MODP1024_2" and "MODP1536_5" to be used in key negotiation phase 1. MODP768_1: Uses the 768-bit Diffie-Hellman group.	MODP1024_2

	<p>MODP1024_2: Uses the 1024-bit Diffie-Hellman group.</p> <p>MODP1536_5: Uses the 1536-bit Diffie-Hellman group.</p>	
Authentication	<p>Select from "PSK", "CA", "XAUTH Init PSK" and "XAUTH Init CA" to be used in IKE negotiation.</p> <p>PSK: Pre-shared Key.</p> <p>CA: Certification Authority.</p> <p>XAUTH: Extended Authentication to AAA server.</p>	PSK
Secrets	Enter the Pre-shared Key.	Null
Life Time @ IKE Parameter	<p>Set the lifetime in IKE negotiation.</p> <p>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.</p>	86400
SA Algorithm	<p>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";</p> <p>Select from "AH_MD5_96" and "AH_SHA1_96" when you select "AH" in "Protocol";</p> <p><b>Note:</b> 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.</p>	3DES_MD5_96
PFS Group	<p>Select from "PFS_NULL", "MODP768_1", "MODP1024_2" and "MODP1536_5".</p> <p>PFS_NULL: Disable PFS Group</p> <p>MODP768_1: Uses the 768-bit Diffie-Hellman group.</p> <p>MODP1024_2: Uses the 1024-bit Diffie-Hellman group.</p> <p>MODP1536_5: Uses the 1536-bit Diffie-Hellman group.</p>	PFS_NULL
Life Time @ SA Parameter	<p>Set the IPSec SA lifetime.</p> <p><b>Note:</b> When negotiating to set up IPSec SAs, IKE uses the smaller one between the lifetime set locally and the lifetime proposed by the peer.</p>	28800
DPD Time Interval	<p>Set the interval after which DPD is triggered if no IPSec protected packets is received from the peer.</p> <p>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.</p>	180
DPD Timeout	Set the timeout of DPD packets.	60
Enable Compress	Tick to enable compressing the inner headers of IP packets.	Disable

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

IPsec Basic
IPsec Tunnel
X.509

**Authentication Manage**

Select Cert Type: None ▼

---

**Authentication Status**

Cert Type	Ca.crt	Remote.crt	Local.crt	Private.key	Crl.pem
Tunnel_1	OK	OK	OK	OK	
Tunnel_2					
Tunnel_3					

X.509 @ IPsec		
Item	Description	Default
Select Cert Type	Select the IPsec tunnel which the certification used for.	Null
CA	Click "Browse" to select the correct CA file from your PC, and then click "Import" to import it to the router. Click "Export" you can export the CA file from router to your PC. File format: ca.crt	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. File format: xxx.crt	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. File format: xxx.key	Null

CRL	Click "Browse" to select the correct CRL file from your PC, and then click "Import" to import it to the router. Click "Export" you can export the CRL file from router to your PC.	Null
Authentication Status	Show current status parameters of IPsec.	Null

### 3.24 Configuration -> RobustVPN

This section allows users to configure the settings of RobustVPN, which is based on a hosted web service designed to connect customer to their machines through Internet. The hosted acts as data transit platform and offer communication originated by the customers to their machines. It is intended to be used in the industrial M2M communication sector.

**RobustVPN**

**RobustVPN Connection Settings**

Enable RobustVPN

Server Address:

HTTPS Port:

Username:

Password:

---

**RobustVPN Status**

Status: Disconnected

Local IP:

Remote IP:

Connect Time:

RobustVPN		
Item	Description	Default
Enable RobustVPN	Click to enable RobustVPN.	Disable
Server Address	Enter the IP address or Domain Name of RobustVPN server.	Null
HTTPS Port	Enter the HTTPS Port of RobustVPN server.	443
Username	Enter the Username of RobustVPN server.	admin
Password	Enter the Password of RobustVPN server.	admin
RobustVPN Status	Show status of RobustVPN, including connection status, Local IP, Remote IP and Connect Time.	

### 3.25 Configuration -> Open VPN

This section allows users to set the Open VPN parameters.

Client
Server
X.509

**Client**

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

Add

**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

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
--------	-------------

Add

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

Interface	Select from “tun” and “tap” which are two different kinds of device interface for OpenVPN. The difference between tun and tap device is this: a tun device is a virtual IP point-to-point device and a tap device is a virtual Ethernet device.	Tun
Authentication	Select from four different kinds of authentication ways: “Pre-shared”, “Username/Password”, “X.509 cert” and “X.509 cert+user”.	None
Local IP	Define the local IP address of OpenVPN tunnel.	10.8.0.2
Remote IP	Define the remote IP address of OpenVPN tunnel.	10.8.0.1
Enable NAT	Tick to enable SNAT for OpenVPN. The source IP address of host Behind R3000 Wireline will be disguised before accessing the remote OpenVPN server.	Disable
Ping Interval	Set ping interval to check if the tunnel is active.	20
Ping -Restart	Restart to establish the OpenVPN tunnel if ping always timeout during this time.	120
Compression	Select “LZO” to use the LZO compression library to compress the data stream.	LZO
Encryption	Select from “NONE”, “BF-CBC”, “DES-CBC”, “DES-EDE3-CBC”, “AES-128-CBC”, “AES-192-CBC” and “AES-256-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.	NONE
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

Client

Server

X.509

**Enable OpenVPN Server**
 Enable OpenVPN Server



**VPN Server Tunnel**

Tunnel name:

Listen IP:

Protocol:

Port:

Interface:

Authentication:

Local IP:

Remote IP:

Enable NAT

Ping Interval:

Ping-Restart:

Compression:

Encryption:

MTU:

Max Frame Size:

Verbose Level:

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

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 Ethernet WAN or Ethernet LAN. Null or 0.0.0.0 stands for using the active WAN link currently Ethernet WAN.	0.0.0.0
Protocol	Select from "UDP" and "TCP Client" which depends on the application.	UDP
Port	Set the local listening port	1194
Interface	Select from "tun" and "tap" which are two different kinds of device interface for OpenVPN. The difference between a tun and tap device is this: a tun device is a virtual IP point-to-point device and a tap device is a virtual Ethernet	tun

	device.	
Authentication	Select from four different kinds of authentication ways: "Pre-shared", "Username/Password", "X.509 cert" and "X.509 cert+user".	None
Local IP	Define the local IP address of OpenVPN tunnel.	10.8.0.1
Remote IP	Define the remote IP address of OpenVPN tunnel.	10.8.0.2
Enable NAT	Tick to enable SNAT for OpenVPN. The source IP address of host Behind R3000 Wireline will be disguised before accessing the remote OpenVPN client.	Disable
Ping Interval	Set ping interval to check if the tunnel is active.	20
Ping -Restart	Restart to establish the OpenVPN tunnel if ping always timeout during this time.	120
Compression	Select from "None" and "LZO", Select "LZO" to use the LZO compression library to compress the data stream.	LZO
Encryption	Select from "NONE", "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.	NONE
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

Client      Server      **X.509**

**Authentication Manage**

Select Cert Type:

**Authentication Status**

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

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. File format: ca.crt	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. File format: xxx.crt	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. File format: xxx.key	Null
DH	Click "Browse" to select the correct DH A file from your PC, and then click "Import" to import it to the router. Click "Export" you can export the DH file from router to your PC.	Null
TA	Click "Browse" to select the correct TA file from your PC, and then click "Import" to import it to the router. Click "Export" you can export the TA file from router to your PC.	Null
CRL	Click "Browse" to select the correct CRL file from your PC, and then click "Import" to import it to the router. Click "Export" you can export the CRL file from router to your PC.	Null
Pre-Share Static Key	Click "Browse" to select the correct Pre-Share Static Key file from your PC, and then click "Import" to import it to the router. Click "Export" you can export the Pre-Share Static Key file from router to your PC.	Null

### 3.26 Configuration -> GRE

This section allows users to set the GRE parameters.

GRE

Tunnel name	Description	
		<input type="button" value="Add"/>

GRE

Enable

Remote IP Address:

Local Virtual IP:

Remote Virtual IP:

Remote Subnet:

Remote Subnet Mask:

All traffic via this interface

Enable NAT

Secrets:

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

### 3.27 Configuration -> L2TP

This section allows users to set the L2TP parameters.

L2TP Client
L2TP Server

**L2TP Client**

Tunnel name	Description
<input type="button" value="Add"/>	

**L2TP Client**

Enable

Remote IP Address:

Username:

Password:

Authentication: Auto ▼

Enable NAT

All traffic via this interface

Enable Tunnel Authentication

Tunnel secret:

Show Advanced

---

Port: 1701

Local IP:

Remote IP:

Address/Control Compression

Protocol Field Compression

Asyncmap Value: fffffff

MRU: 1500

MTU: 1436

Link Detection Interval (s): 30

Link Detection Max Retries: 5

Expert Options: noccp nobsdcomp

L2TP Client @ L2TP		
Item	Description	Default
Add	Click "Add" to add a L2TP client. You can add at most 3 L2TP clients.	Null
Remote IP Address	Enter your L2TP server's public IP or domain name.	Null

Username	Enter the username which was provided by your L2TP server.	Null
Password	Enter the password which was provided by your L2TP server.	Null
Authentication	Select from "Auto", "PAP", "CHAP", "MS-CHAP v1" and "MS-CHAP v2". You need to select the corresponding authentication method based on the server's authentication method. When you select "Auto", router will auto select the correct method based on server.	Disable
Remote Subnet	Enter L2TP remote Protected subnet's address.	Null
Remote Subnet Mask	Enter L2TPremote Protected subnet's mask.	Null
Enable NAT	Click to enable NAT feature of L2TP. The source IP address of host Behind R3000 Wireline will be disguised before accessing the remote L2TP server.	Disable
All traffic via this interface	After click to enable this feature, all data traffic will be sent via L2TP tunnel.	Disable
Enable Tunnel Authentication	Tick to enable tunnel authentication and enter the tunnel secret which provided by L2TP server.	Disable
Tunnel Secret	Enter L2TP tunnel secret in this item.	Null
Show Advanced	Tick to enable the L2TP client advanced setting.	Disable
Port	Set the Port number of the L2TP client.	Null
Local IP	Set the IP address of the L2TP client. You can enter the IP which assigned by L2TP server. Null means L2TP client will obtain an IP address automatically from L2TP server's IP pool.	Null
Remote IP	Enter the remote peer's private IP address or remote subnet's gateways address.	Null
Address/Control Compression	Used for PPP initialization. In general, you need to enable it as default.	Enable
Protocol Field Compression	Used for PPP initialization. In general, you need to enable it as default.	Enable
Asyncmap Value	One of the L2TP initialization strings. In general, you don't need to modify this value.	Ffffffff
MRU	Maximum Receiving Unit. It is the identifier of the maximum size of packet, which is possible to receive in a given environment.	1500
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1436
Link Detection Interval	Specify the interval between L2TP client and server. To check the connectivity of a tunnel, the client and server regularly send PPP Echo to each other. If the client or server receives no response from the peer within a specified period of time, it retransmits the PPP echo. If it receives no response from the peer after transmitting the PPP echo for max retries times, it considers that the L2TP tunnel is down and tries 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

**L2TP Client**      **L2TP Server**

**Enable L2TP Server**

Enable L2TP Server

**L2TP Common Settings**

Username:

Password:

Authentication:  ▼

Enable Tunnel Authentication

Tunnel secret:

Local IP:

IP Pool Start:

IP Pool End:

**L2TP Server Advanced**

Show L2TP Server Advanced

Address/Control Compression

Protocol Field Compression

Asyncmap Value:

MRU:

MTU:

Link Detection Interval (s):

Link Detection Max Retries:

Expert Options:

**Route Table List**

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

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
Port	Set the Port number of the L2TP server.	Null
Asynmap Value	One of the L2TP initialization strings. In general, you don't need to modify this value.	ffffff
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

### 3.28 Configuration -> PPTP

This section allows users to set the PPTP parameters.

PPTP Client
PPTP Server

**PPTP Client**

Tunnel name	Description
<input type="button" value="Add"/>	



**PPTP Client**

Enable

Remote IP Address:

Username:

Password:

Authentication:

Enable NAT

Enable MPPE

All traffic via this interface

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:

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

Local IP	Set the IP address of the PPTP client. You can enter the IP which assigned by PPTP server. Null means PPTP client will obtain an IP address automatically from PPTP server's IP pool.	Null
Remote IP	Enter the remote peer's private IP address or remote subnet's gateways address.	Null
Address/Control Compression	Used for PPP initialization. In general, you need to enable it as default.	Enable
Protocol Field Compression	Used for PPP initialization. In general, you need to enable it as default.	Enable
Asyncmap Value	One of the PPTP initialization strings. In general, you don't need to modify this value.	ffffff
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.	noccp nobsdcomp

**PPTP Client**      **PPTP Server**

**Enable PPTP Server**

Enable PPTP Server

---

**PPTP Common Settings**

Username:

Password:

Authentication: CHAP ▾

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:

MRU:

MTU:

Link Detection Interval (s):

Link Detection Max Retries:

Expert Options:

**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
("0.0.0.0" means any)		
<input type="button" value="Add"/>		

PPTP Server @ PPTP		
Item	Description	Default
Enable PPTP Server	Tick to enable PPTP server.	Disable
Username	Set the username which will assign to PPTP client.	Null
Password	Set the password which will assign to PPTP client.	Null
Authentication	Select from "PAP", "CHAP", "MS-CHAP v1" and "MS-CHAP v2". PPTP client need to select the same authentication method based on this server's authentication method.	CHAP
Local IP	Set the IP address of PPTP server.	10.0.0.1
IP Pool Start	Set the IP pool start IP address which will assign to the PPTP clients.	10.0.0.2
IP Pool End	Set the IP pool end IP address which will assign to the PPTP clients.	10.0.0.100
Enable MPPE	Tick to enable MPPE (Microsoft Point-to-Point Encryption). It's a protocol for encrypting data across PPP and VPN links.	Disable
Show PPTP Server Advanced	Tick to show the PPTP server advanced setting.	Disable
Address/Control Compression	Used for PPP initialization. In general, you need to enable it as default.	Enable
Protocol Field Compression	Used for PPP initialization. In general, you need to enable it as default.	Enable
Asyncmap Value	One of the PPTP initialization strings. In general, you don't need to modify this value.	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 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.	noccp nobsdcomp
Route Table List	Click "Add" to add a route rule from PPTP server to PPTP client.	Null

### 3.29 Configuration->Modbus over TCP

This section allows users to configure the Modbus over TCP. Modbus over TCP slave functions, the remote can access the R3000 Wireline's internal registers through Modbus over TCP.

#### Modbus over TCP

Modbus over TCP Setting	
<input checked="" type="checkbox"/> Enable Modbus over TCP	
Slave ID:	<input type="text" value="0"/>
port:	<input type="text" value="0"/>

Modbus over TCP		
Item	Description	Default
Enable Modbus over TCP	Click to enable Modbus over TCP.	Disable
Slave ID	Enter the slave ID.	Null
Port	Enter the port which used to forward data.	Null

### 3.30 Configuration ->Modbus Master

R3000 Wireline router could be configured as a modbus master, and will automatically poll the slave sides and report the collected data to specified server.

This section allows users to configure the Modbus Master.

**Note:** Before the slave device transmits the data via serial interface, you should select protocol as "Modbus Master" in Serial.

**Modbus Master**

**Modbus Master Setting**

Enable Modbus Master

Reading Interval(s)

Attempts

Max Response Time(ms)

Time Between Commands(ms)

Logging Type  ▼

Send via Portal

---

**Multiple Server**

Server IP	Server Port
<input type="text"/>	<input type="text"/>

Modbus Master		
Item	Description	Default
Reading Interval(s)	In this set of cycle, read Remote Channels one by one. The equipment begins the reading of the channels in the order they were created at the time of configuration. This way, it continues reading all the channels, respecting the time between commands, until it has read them all. Every time the reading interval is reached, it restarts the reading of all of the remote channels. If the reading of the channels takes longer that the configured reading interval, it should wait for all channels to be read before starting a new reading interval.	30
Attempts	The max times of instruction attempts. If a read instruction in Remote Channels failure to perform the read command in a row, when the times achieve Attempts, R3000 Wireline identifies automatically this instruction is not read, and the skip this instruction next read cycle. Only when this state duration keep over 30 seconds, it will become a new readable, and then try to execute the command next read cycle.	3
Max Response Time(ms)	The response time of the maximum waiting to read instructions. When you perform a read command, this time is the response time of R3000 Wireline waiting for the command. If it didn't get response from the instructions after the Max Response Time, the instructions read timeout.	500
Time Between Commands(ms)	The execution of the interval between each instruction.	50
Logging Type	Read the save site of Modbus's data. Only save when it can't upload to the server, upload the data after the upload channel recovering. Delete the data after finishing uploading.	Null
Send via Portal	Enable to send data via portal.	

Server IP	Set the server IP address of receive Modbus data.	Null
Server Port	Set the server port of receive Modbus data.	Null

### 3.31 Configuration ->Remote Channels

This section allows users to configure the remote channels.

**Note:** Only configure the Modbus Master parameters at first, it can configure Remote Channels, otherwise it's disabled.

#### Remote Channels

Index	Tag	ID	Modbus Command	Via Interface	Register	Option
<input type="button" value="Add"/>						

**Remote Channels**

Tag:

Slave ID:

Modbus Command:  ▼

Via Interface:  ▼

Initial Register:

Error Value:

Decimal Place:

Unsigned Value

Remote Channels		
Item	Description	Default
Tag	The sign of remote channel, it can be null or not null. If not null, alarm or upload information in platform will carry this description.	Null
Slave ID	Modbus slave ID	1
Modbus Command	Read the command.	Read Holding Registers(INT16)
Via Interface	Select from "RS485", "RS232", "TCP"	RS485
Initial Register	The starting point for execution to read while reading instruction.	0
Error Value	When reading failure, the Error Value in the Value will be assigned to the channel, for the alarm and upload platform.	-100
Decimal Place	Used to indicate a dot in the read into the position of the channel. For example: read the channel value is 1234, and a Decimal Place is equal to 2, then the actual value of 12.34.	0

Unsigned Value	A value used to identify the channel for unsigned.	Disable
----------------	--	---------

### 3.32 Configuration ->Alarms

This section allows users to configure the alarms.

**Alarms Setting**

Alarms	Source	Condition	Setpoint	Alarm Type	Phone Group
--------	--------	-----------	----------	------------	-------------

**Alarms Setting**

Alarm source:

Index:

Condition:

Setpoint:

**Alarm Type**

SMS

E-Mail

SNMP Trap

Continuous:

Content On:

Content Off:

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

Alarms		
Item	Description	Default
Alarm Source	Select from "Remote channel", "CSQ" and "Cellular Status".	Remote channel
Index	Used to identify the way of Remote Channel.	1
Condition	The conditions of trigger the alarm.	Greater than (>)
Setpoint	The alarm threshold.	0
Alarm Type	The alarm types, you can choose more. Select from "SMS", "Email", "SNMP Trap".	off
Content On	The content when the alarm on.(for email)	Null
Content Off	The content when the alarm off.(for email)	Null
Phone Group	You should add PhoneGroup at PhoneBook firstly.	Null

### 3.33 Configuration -> SNMP

This section allows users to set the SNMP parameters.

Basic
View
VACM
Trap
Download MIB..

**SNMP Basic Settings**

Enable SNMP

Port:

Agent Mode:

Version:

Location Info:

Contact Info:

System Name:

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

Basic
View
VACM
Trap
Download MIB..

**Mib View List**

View Name	View Filter	View OID	
system	Included <input type="text" value=""/>	1.3.6.1.2.1.1	X
all	Included <input type="text" value=""/>	1	X

\*View OID: <1~65535>.<1~65535>...

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



Basic View **VACM** Trap Download MIB..

**SNMPv1&v2 User List**

Readwrite	Network	Community	MIBview	
Readonly	0.0.0.0	public	system	X
ReadWrite	0.0.0.0	private	system	X
ReadWrite	0.0.0.0	admin	all	X

*\*Network: 1.1.1.0/24, 0.0.0.0 means any*

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

Basic View VACM **Trap** Download MIB..

**SNMP Trap Settings**

Enable SNMP Trap

Version:

Server Address:

Port:

Name:

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

Basic View VACM Trap **Download MIB..**

**Download MIB Moudles File**

Download MIB Moudles File @ SNMP		
Item	Description	
Download MIB Moudles File	Click to download the MIB Moudles File	

### 3.34 Configuration -> VRRP

This section allows users to set the VRRP parameters.

VRRP

**VRRP Settings**

Enable VRRP

Group ID:

Priority:

Interval (s):

Virtual IP:

VRRP		
Item	Description	Default
Enable VRRP	Tick to enable VRRP protocol. VRRP (Virtual Router Redundancy Protocol) is an Internet protocol that provides a way to have one or more backup routers when using a statically configured router on a local area network (LAN). Using VRRP, a virtual IP address can be specified manually.	Disable
Group ID	Specify which VRRP group of this router belong to.	1
Priority	Enter the priority value from 1 to 255. The larger value has higher priority.	100
Interval	The interval that master router sends keepalive packets to backup routers.	10
Virtual IP	A virtual IP address is shared among the routers, with one designated as the master router and the others as backups. In case the master fails, the virtual IP address is mapped to a backup router's IP address. (This backup becomes the master router.)	192.168.0.1

### 3.35 Configuration -> Reboot

This section allows users to set the Reboot policies.

Time

**Daily Reboot**

Enable Time Reboot(hh:mm,24h)

Reboot Time1	Reboot Time2	Reboot Time3
12:00		

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.	12:00

Reboot Time2	Specify time2 when you need router reboot.	Null
Reboot Time3	Specify time3 when you need router reboot.	Null

### 3.36 Configuration -> Portal

This section allows users to configure parameters about RobustLink, Tingco Cumulocity and GpsGate, which are industrial-grade centralized management and administration system. It allows you to monitor, configure and manage large numbers of remote devices on a private network over the web.

#### Portal

**Portal Settings**

Enable Portal

Server Type:

Server Address:

Port:

Password:

#### Portal

**Portal Settings**

Enable Portal

Server Type:

Server Address:

Port:

UnitID:

CLID:

KeepAlive:

#### Portal

**Portal Settings**

Enable Portal

Server Type:

URL:

Username:

Password:

Device Name:

Device ID(s):

KeepAlive:

**Portal**

**Portal Settings**

Enable Portal

Server Type:

*\*Please configure the GPS Setting parameters at first*

Robustlink @ Portal		
Item	Description	Default
Server address	Enter IP address of RobustLink.	Null
Port	Enter port number of RobustLink.	1883
Password	Enter the password preset in RobustLink. <i>Note: The passwords set in R3000 and RobustLink need to be the same.</i>	Null
Tingco@ Portal		
Server Address, Port, UnitID,CLID, KeepAlive	Fill in the Server Address, Port, UnitID, CLID, KeepAlive. After settings are activated, R3000 will update information to Tingco automatically.	
Cumulosity@Portal		
URL, Username, Password, Device Name, Device ID (S), KeepAlive	Fill in the URL, Username, Password, Device Name, Device ID (S), KeepAlive of Cumulosity. Default settings will be ok. After settings are activated, R3000 will update information to Cumulosity automatically.	
GpsGate@Portal		
GpsGate	Connect to GpsGate portal. You should configure the GpsGPS Setting at first.	

### 3.37 Configuration -> Syslog

This section allows users to set the syslog parameters.

**Syslog**

**Syslog Settings**

Save Position:

Log Level:

Keep Days:

Log to Remote System

Remote IP:

Remote UDP Port:

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

### 3.38 Configuration -> Event

This section allows users to set the Event parameters.

**Event**

**Event Settings**

Enable Event

Index	Event Code	SNMP-TRAP	RobustLink
1	BOOT-UP	<input type="checkbox"/>	<input type="checkbox"/>
2	3G-UP	<input type="checkbox"/>	<input type="checkbox"/>
3	3G-DOWN	<input type="checkbox"/>	<input type="checkbox"/>
4	GPRS-UP	<input type="checkbox"/>	<input type="checkbox"/>
5	GPRS-DOWN	<input type="checkbox"/>	<input type="checkbox"/>
6	OVPN1-UP	<input type="checkbox"/>	<input type="checkbox"/>
7	OVPN2-UP	<input type="checkbox"/>	<input type="checkbox"/>
8	OVPN3-UP	<input type="checkbox"/>	<input type="checkbox"/>
9	OVPN1-DOWN	<input type="checkbox"/>	<input type="checkbox"/>
10	OVPN2-DOWN	<input type="checkbox"/>	<input type="checkbox"/>
11	OVPN3-DOWN	<input type="checkbox"/>	<input type="checkbox"/>
12	INT1-UP	<input type="checkbox"/>	<input type="checkbox"/>
13	INT2-UP	<input type="checkbox"/>	<input type="checkbox"/>

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

### 3.39 Configuration -> USR LED

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

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

USR LED

**USR LED**

USR LED Type:

Indication:

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

### 3.40 Configuration -> AAA

This section allows users to set the Radius, Tacacs+, LDA Pand Authen parameters.

Radius
Tacacs+
LDAP
Authen

**Radius Setting**

Enable Radius

Server Address:

Server Port:

Password:

Radius		
Item	Description	Default
Server Address	Radius server address (domain or IP)	Null
Server Port	Radius server port	1812
Password	The password to access the server	Null

Radius
Tacacs+
LDAP
Authen

**Tacacs Setting**

Enable Tacacs

Server Address:

Server Port:

Password:

Tacacs+		
Item	Description	Default
Server Address	Tacacs+ server address (domain or IP)	Null
Server Port	Tacacs+ server port	49
Password	The password to access the server	Null

Radius
Tacacs+
LDAP
Authen

**LDAP Setting**

Enable LDAP

Authen Algorithm: None ▼

Server Address:

Server Port: 389

Base DN:

Username:

Password:

LDAP		
Item	Description	Default
Authen Algorithm	Select from "None", "StartTLS", "SSL"	
Server Address	LDAP server address (domain or IP)	
Server Port	LDAP server port	389
Base DN	The top of the LDAP directory tree	
Username	The user name to access the server	
Password	The password to access the server	

Radius
Tacacs+
LDAP
Authen

**Authen Setting**

Services	1	2	3
Telnet:	<span style="border: 1px solid #ccc; padding: 2px;">Local</span> ▼	<span style="border: 1px solid #ccc; padding: 2px;">Null</span> ▼	<span style="border: 1px solid #ccc; padding: 2px;">Null</span> ▼
Ssh:	<span style="border: 1px solid #ccc; padding: 2px;">Local</span> ▼	<span style="border: 1px solid #ccc; padding: 2px;">Null</span> ▼	<span style="border: 1px solid #ccc; padding: 2px;">Null</span> ▼
Web:	<span style="border: 1px solid #ccc; padding: 2px;">Local</span> ▼	<span style="border: 1px solid #ccc; padding: 2px;">Null</span> ▼	<span style="border: 1px solid #ccc; padding: 2px;">Null</span> ▼

Radius		
Item	Description	Default
Services	There are "Telnet", "Ssh" and "Web". When set the Radius, Tacacs+ and local in the meanwhile, the priority order to follow: 1>2>3	
1	Select from "Null", "Local", "Radius", "Tacacs+" and "Ldap". Null: No user authorization processing. Local: The authorization according to the relevant properties of local user accounts configured by network access server.	Null

	Radius: Authentication and authorization are tied together; it can't use Radius alone to authorize. Tacacs+: Tacacs+ server authorizes to users. Ladp: Ladp authorization.	
2	Select from "Null", "Local", "Radius", "Tacacs+" and "Ldap".	Null
3	Select from "Null", "Local", "Radius", "Tacacs+" and "Ldap".	Null

### 3.41 Configuration -> FTP

#### Client

**FTP Client Setting**

FTP Client Enable

Server Address:

Server Port:

Username:

Password:

The Filename Prefix:

Use Timestamp

**Upload Source**

Name	Enable
CSV File	<input checked="" type="checkbox"/>
Syslog	<input type="checkbox"/>

Upload Interval(m):

CSV File Write Interval(s):

**CSV File Include List**

Channel Name	Alias	Enable
CSQ	SIGN	<input type="checkbox"/>
Connection Status	COST	<input type="checkbox"/>

FTP		
Item	Description	Default
FTP Client Enable	click to enable FTP client	Null
Server Address	Enter FTP server's IP address or domain name.	Null
Server port	Enter FTP server's port	21
Username	Enter the username which can be used to access FTP server.	Null
Password	Enter the password which can be used to access FTP server.	Null
The Filename Prefix	Set a name for the file which will be sent to the FTP server.	Null



Use Timestamp	Enable Timestamp, the upload file will include the date.	Enable
Upload Source	Choose the file type, CSV file or Syslog. CSV file: sData will be collected in CSV file and save in local memory. Syslog: System log record file.	Null
Upload Interval (m)	Set the upload interval of uploading file.	60
CSV File Write Intervals (s)	Set the interval of data writing.	30
CSV File Include List	All the local CSV files will display in this list.	/
Channel Name	Modbus remote channel name	/
Alias	Set the file's alias.	/
Enable	Select the CSV files which you want to send to the FTP server.	Null

### 3.42 Administration -> Profile

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

Profile

---

**Change Profile**

Profile: Standard ▼

Copy settings from current profile to selected profile

Change

---

**All Parameters XML Configuration**

XML File:  Browse... Import Export

---

**IPsec XML Configuration**

IPsec XML File:  Browse... Import Export

---

**OpenVPN XML Configuration**

OpenVPN XML File:  Browse... Import Export

---

**Restore to Factory Default Settings**

Restore to Factory Default Settings

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	Null

	browser window, then you can save it as a XML file.	
Restore to Factory Default Settings	Click the button of “Restore to Factory Default Settings” to restore the router to factory default setting.	Null

### 3.43 Administration -> Tools

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

Ping
Traceroute
Sniffer
Test

**Ping**

Ping IP address:

Number of requests:

Timeout (s):

Local IP:

Ping @ Tools		
Item	Description	Default
Ping IP address	Enter the ping destination IP address or domain name.	Null
Number of requests	Specify the number of ping requests.	5
Timeout	Specify timeout of ping request.	1
Local IP	Specify the local IP from 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
Traceroute
Sniffer
Test

**Traceroute**

Trace Address:

Trace Hops:

Timeout (s):

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

Ping
AT Debug
Traceroute
Sniffer
Test

### Sniffer

Interface:

Host:

Protocol:

Count:

Sniffer @ Tools		
Item	Description	Default
Interface	Select form "all", "lo", "imq0", "imq1", "eth0", "gre0": all: contain all the interface; lo: Local Loopback interface; imq0/1: virtual interface for QoS, which used to limit the download and upload speed; eth0: Ethernet interface; gre0: GRE tunnel interface;	All
Host	Filter the packet that contain the specify IP address.	Null
Protocol	Select from "all", "ip", "arp", "tcp" and "udp".	All
Count	Set the packet number that can be sniffed at a time.	100
Start	Click this button to start the sniffer, and the log will be displayed in the follow box.	Null

Ping	Traceroute	Sniffer	Test
------	------------	---------	------

**Test**

Enable	Description	Result
<input checked="" type="checkbox"/>	SD Test	
<input checked="" type="checkbox"/>	USB Test	
<input checked="" type="checkbox"/>	Flash Test	
<input checked="" type="checkbox"/>	Memory Test	
<input checked="" type="checkbox"/>	Ethernet Test	

**Detail**

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

### 3.44 Administration -> Clock

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

**Clock**

**Real Time Clock Settings**

Real Time Clock:

PC Time:

**Timezone Setting**

Timezone:

**NTP Settings**

Enable NTP Client

Primary NTP Server:

Secondary NTP Server:

Update Interval (h):

Enable NTP Server

Clock		
Item	Description	Default
Real Time Clock	Router's RTC can be showed and modified in this field.	Null
PC Time	You PC's time can be showed here.	Null
Synchronize	Synchronize router's RTC with PC.	Null
Enable NTP Client	Enable to synchronize the time from NTP server.	Disable
Timezone @ Client	Select your local time zone.	UTC +08:00
Primary NTP Server	Enter primary NTP Server's IP address or domain name.	pool.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

### 3.45 Administration -> Web Server

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

**Basic**    **X.509**

---

**Port Settings**

HTTP Port:	<input type="text" value="80"/>
HTTPS Port:	<input type="text" value="443"/>

**Basic**    **X.509**

---

**HTTPS Certificate**

Public Key:	<input type="text"/>	<input type="button" value="Browse..."/>	<input type="button" value="Import"/>	<input type="button" value="Export"/>
Private Key:	<input type="text"/>	<input type="button" value="Browse..."/>	<input type="button" value="Import"/>	<input type="button" value="Export"/>

Basic @ Web Server		
Item	Description	Default
HTTP Port	<p>Enter the HTTP port number you want to change in R3000 Wireline’s Web Server.</p> <p>On a Web server, port 80 is the port that the server "listens to" or expects to receive from a Web client. If you configure the router with other HTTP Port number except 80, only adding that port number then you can login R3000 Wireline’s Web Server.</p>	80
HTTPS Port	<p>Enter the HTTPS port number you want to change in R3000 Wireline’s Web Server.</p> <p>On a Web server, port 443 is the port that the server "listens to" or expects to receive from a Web client. If you configure the router with other HTTPS Port number except 443, only adding that port number then you can login R3000 Wireline’s Web Server.</p> <p><b>Note:</b> <i>HTTPS is more secure than HTTP. In many cases, clients may be exchanging confidential information with a server, which needs to be secured in order to prevent unauthorized access. For this reason, HTTP was developed by Netscape corporation to allow authorization and secured transactions.</i></p>	443
X.509 @ Web Server		
HTTPS Certificate	In this tab, user can import or export “Public Key” and “Private Key” for HTTPS certification.	Null

### 3.46 Administration -> User Management

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

Super
Common

**User Management**

Username:	<input type="text" value="admin"/>
Old Password:	<input type="password"/>
New Password:	<input type="password"/>
Confirm Password:	<input type="password"/>

**Login Parameters**

Login Timeout (s):	<input type="text" value="1800"/>
--------------------	-----------------------------------

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

Super
Common

**User Management**

Access Level	Username	Password	
			<input type="button" value="Add"/>

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



### 3.47 Administration -> SDK Management

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

APP
Files

**Import Applications**

Browse...
Import

**Custom Application List**

Disable SDK service if not WAN devices dete...

Enabled	APP Name	Options	Memory(KB)	Running	
<input type="checkbox"/>	1.xml		0	N	X

APP @ SDK Management		
Item	Description	Default
Import Applications	Click to import APP files in this item.	Null
Custom Application List	This list shows which APP files you have imported to the router, which APP file you want to start up, as well as the running information. Enable: Click to enable the APP file. APP Name: Shows the name of the APP files. Options: It is an optional items, user can choose to configure startup parameters here. Memory (KB): Shows the memory resources occupied by the APP files. Running: Shows whether the APP files are running.	Null
Disable SDK service if not WAN device dete...	Click to run the SDK APP only after WAN interface is up. If you don't click this option, the SDK APP will run before the WAN interface is up.	Disable

APP
Files

**Import Files**

Browse...
Import File

**Custom File List**

Index	File Name

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

### 3.48 Administration -> Update Firmware

This section allows users to update the firmware of router.

**Update**

**Firmware Version**

Firmware Version: 1.2.0

**Firmware old Version**

Firmware old Version 1.01.35

Fall back to old version

**Update Firmware**

Warning: Do not turn off or operate the Router while updating.

New Firmware:

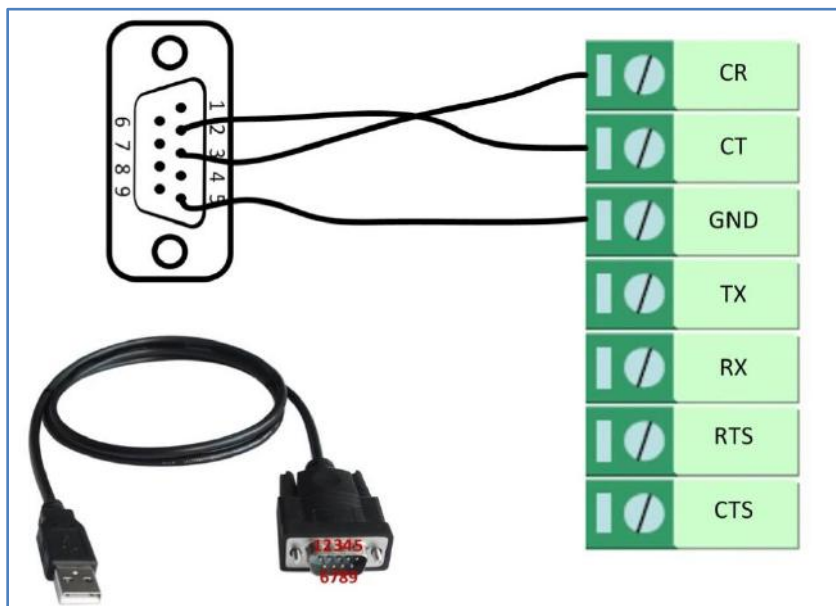
Update		
Item	Description	Default
Firmware Version	Show the current firmware version.	Null
Firmware Old Version	Show the old firmware version of the router. Click "Apply" button to fall back to the old version, after updating successfully, you need to reboot router to take effect.	
Update firmware	Click "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

## Chapter 4 Configuration Examples

### 4.1 Interface

#### 4.1.1 Console port

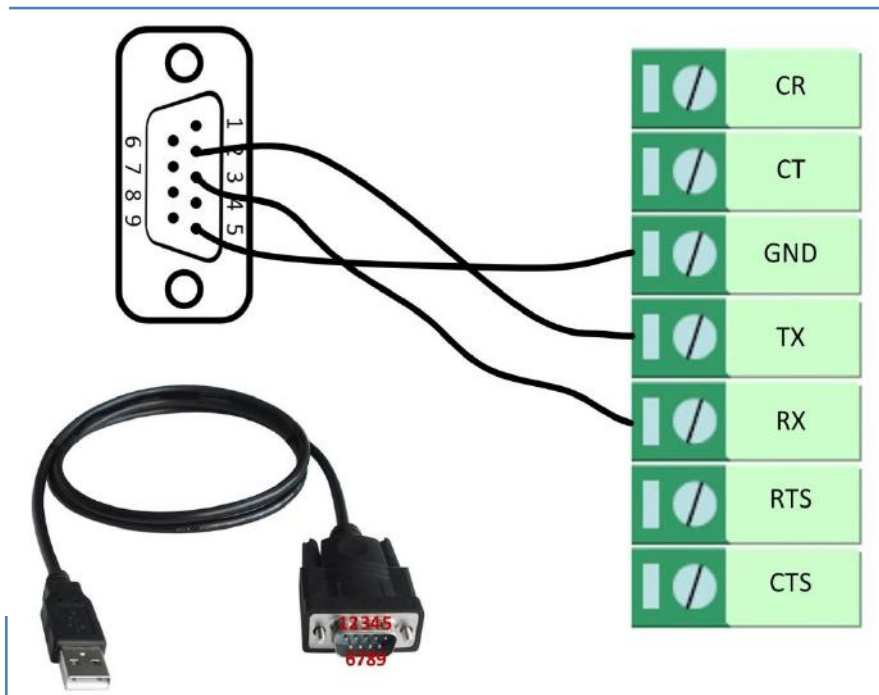
User can use the console port to manage the router via CLI commands, please check section Introductions for CLI.



### 4.1.2 RS232

R3000 Wireline-4 Ethernet Ports supports one RS232 (without RS485) for serial data communication.

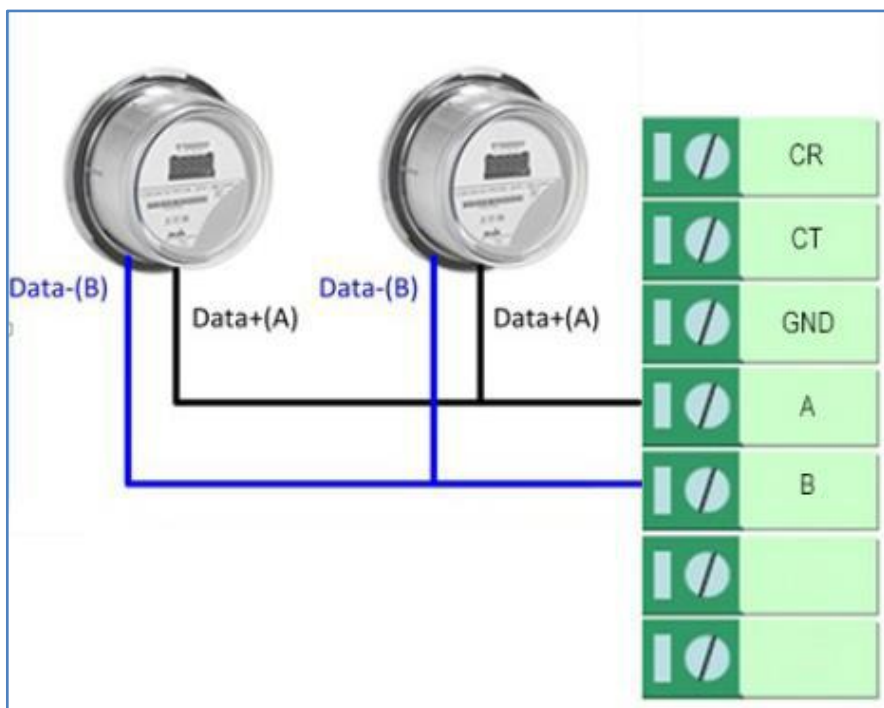
Please refer to the connection diagram at the right site.



### 4.1.3 RS485

R3000 Wireline-4 Ethernet Ports supports one RS485 (without RS232) for serial data communication.

Please refer to the connection diagram at the right site.

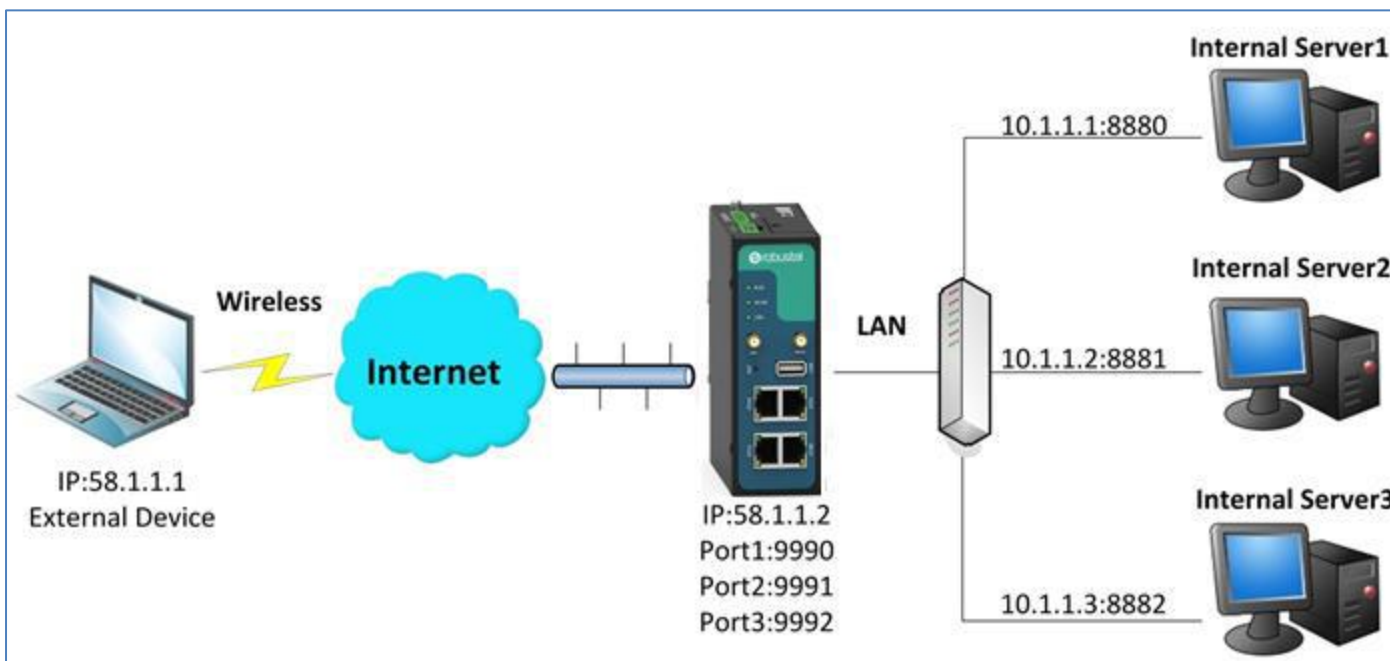


## 4.2 Network

### 4.2.1 NAT

This section shows users how to set the NAT configuration of router.

Parameter Remote IP defines if access is allowed to route to the Forwarded IP and Port via WAN IP and “Arrives At Port”.



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

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

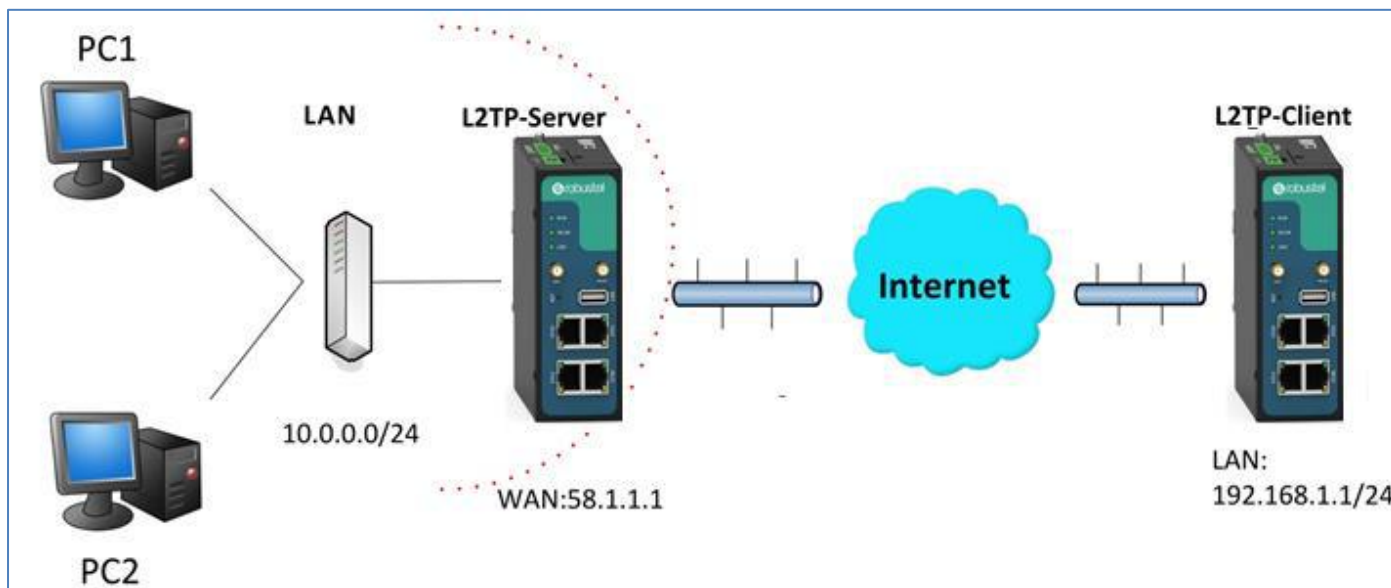
*\*Arrives At Port: <1-65536> or <1-65536>-<1-65536>*

#### 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 Wireline.

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

## 4.2.2 L2TP



### L2TP\_SERVER:

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

##### Enable L2TP Server

Enable L2TP Server

Tick "Enable L2TP Server", and fill in the blank textbox

##### L2TP Common Settings

Username:  **1**  
 Password:  **2**  
 Authentication:  **3**  
 Enable Tunnel Authentication  
 Local IP:   
 IP Pool Start:   
 IP Pool End:

##### L2TP Server Advanced

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

\*"0.0.0.0" means any

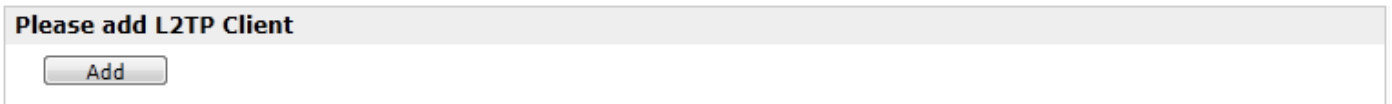
Add

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

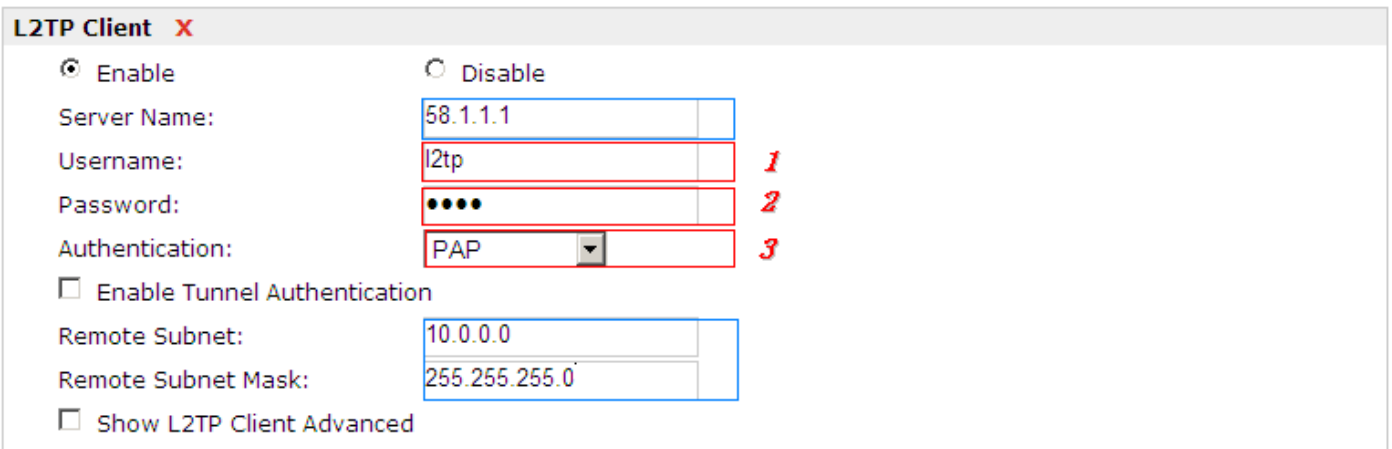
**Note:** The following diagrams with red color numbers mean these are the matches between server and client, and with the blue color number means it must be set locally for the tunnel.

### L2TP\_CLIENT:

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

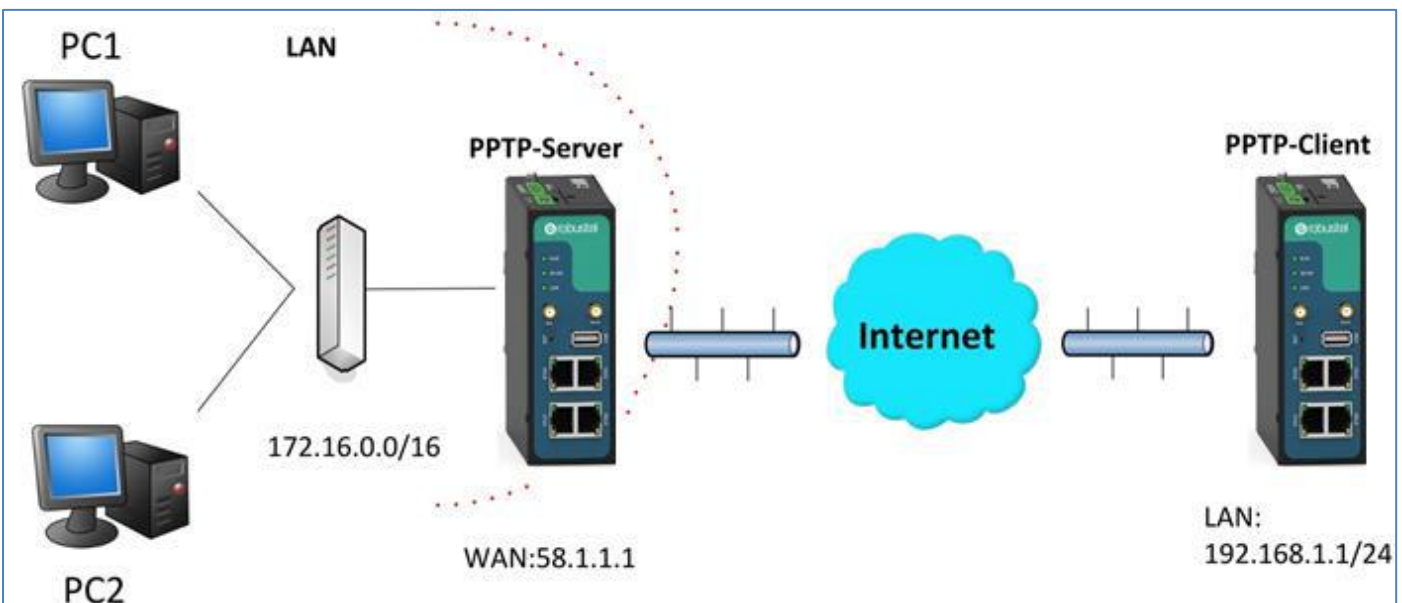


Click “Add” button, and fill in the blank textbox



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

### 4.2.3 PPTP



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

### PPTP\_SERVER:

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

**Enable PPTP Server**

Enable PPTP Server

Tick "Enable PPTP Server", and fill in the blank textbox

**PPTP Common Settings**

Username:  1

Password:  2

Authentication:  3

Local IP:

IP Pool Start:

IP Pool End:

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	X

\*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

Enable       Disable

Server Name:

Username:  1

Password:  2

Authentication:  3

Remote Subnet:

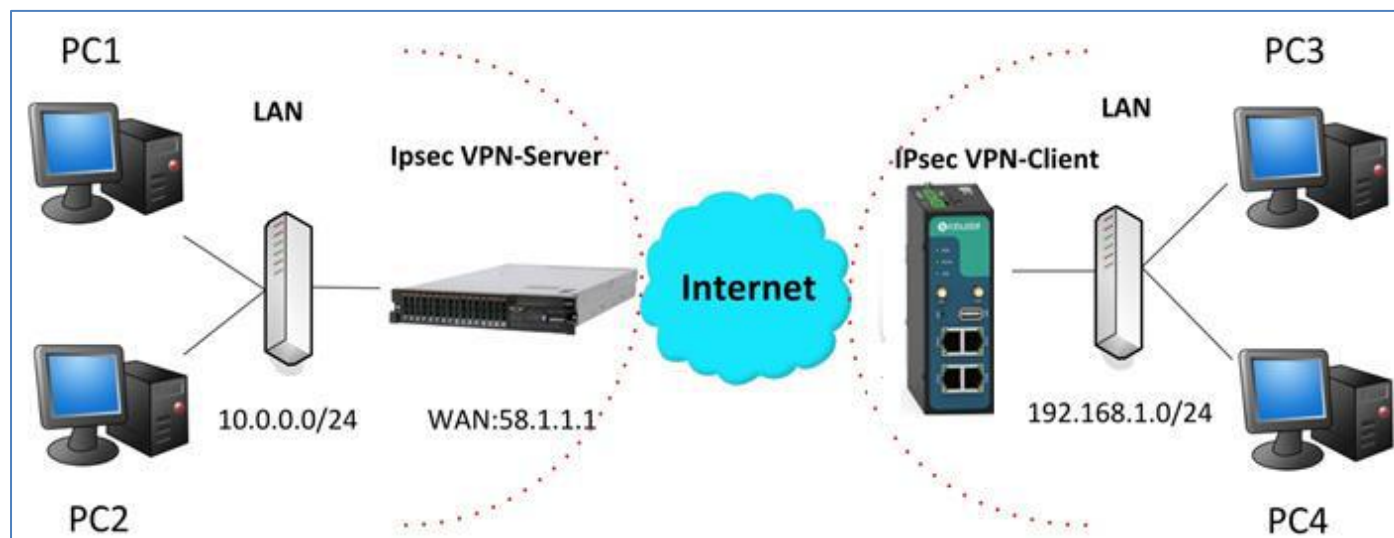
Remote Subnet Mask:

Enable MPPE

Show PPTP Client Advanced

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

### 4.2.4 IPsec VPN



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

## IPsecVPN\_SERVER:

### Cisco 2811:

```

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

```

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

## IPsecVPN\_CLIENT:

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

**IPsec Basic**

Enable NAT Traversal

Keepalive Interval(s):

Then click "Apply".

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

**IPsec Tunnel X**

Enable  Disable

Tick "Enable IPsec Tunnel1"

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

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

## 4.2.5 OpenVPN

c



**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

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

Tick "Enable OpenVPN Server".

**VPN Server Tunnel**

Tunnel name: OpenVPN\_Tunnel\_0

Listen IP:

Protocol: UDP 1

Port: 1194 2

Interface: tun 3

Authentication: None 4

Local IP: 10.8.0.1 5

Remote IP: 10.8.0.2 6

Enable NAT 7

Ping Interval: 20

Ping-Restart: 120

Compression: LZO 8

Encryption: BF-CBC 9

MTU: 1500 10

Max Frame Size: 1500 11

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

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

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

**OPENVPN\_CLIENT:**

**Configuration--->OpenVPN--->Client**

**Enable OpenVPN Client1**

Enable OpenVPN Client1

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

**Enable OpenVPN Client** X

Enable
  Disable

Tunnel name:

Protocol:  1

Server Address:

Port:  2

Interface:  3

Authentication:  4

Local IP:  6

Remote IP:  5

Enable NAT 7

Ping Interval:

Ping-Restart:

Compression:  8

Encryption:  9

MTU:  10

Max Frame Size:  11

Verbose Level:

Expert Options:

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

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

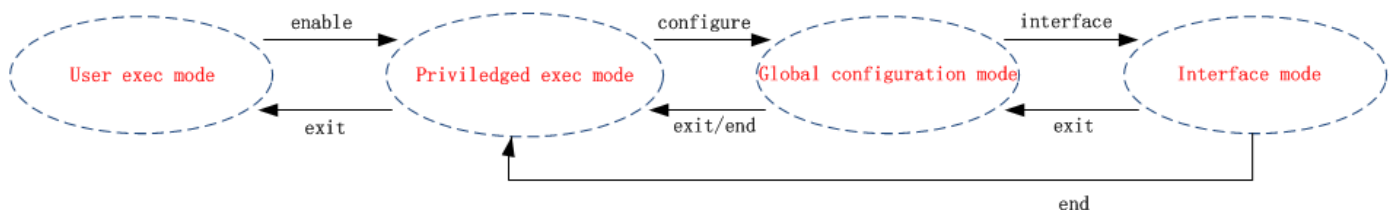
## Chapter 5 Introductions for CLI

### 5.1 What's CLI and hierarchy level Mode

The R3000 Wireline 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. There are 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 the relationship diagram about how to access or quit among the different modes:



#### USER EXEC MODE:

R3000 Wireline Configure Environment

Username: admin

Password: \*\*\*\*\*

R3000 Wireline> ? //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 Wireline> enable

Password: \*\*\*\*\*

```
R3000 Wireline# ? //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 Wireline# configure
```

```
R3000 Wireline(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 Wireline(config)# interface Ethernet 0
```

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



## 5.2 How to configure the CLI

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

Commands /tips	Description
?	Typing a question mark “?” will show you the help information.
Ctrl+c	Press these two keys at the same time, except its “copy” function but also can be used for “break” out of the setting program.
Invalid command “xxx”	Parameters “xxx” are not supported by the system, in this case, enter a mark “?” instead of “xxx” will help to find out the correct parameters about this issue.
Incomplete command	Command is not incomplete.
% Invalid input detected at '^' marker	'^' marker indicates the location where the error is.

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

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

### 5.2.1 QuickStart with configuration examples

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

#### Example 1: Show current version

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

#### Example 2: Update firmware via tftp

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

```
Tftp transferring
tftp succeeded!downloaded
R3000 Wireline# write //save current configuration
Building configuration...
```

```

OK
R3000 Wireline#reload
!Reboot the system?'yes'or 'no':yes                //reload to take effect

```

### Example 3: Set link-management

```

R3000 Wireline> enable
Password: *****
R3000 Wireline#
R3000 Wireline# configure
R3000 Wireline(config)# set link-management
Primary Interface:
  1.Eth0
  2.WiFi
->please select mode(1-2)[1]:                      //select "Eth0" as primary 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 Wireline# write                               //save current configuration
Building configuration...
OK
R3000 Wireline# reload
!Reboot the system ?'yes'or 'no':yes                //reload to take effect

```

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

```

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

*****
Primary Interface      : Eth0                      // now "Eth0 Only" as wan-link
Secondary Interface    : None
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 Wireline # configure
R3000 Wireline (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
->gateway [192.168.0.254]:58.1.1.254 //set gateway for eth0
->mtu value (1024-1500)[1500]:
->input primary DNS [192.168.0.254]:58.1.1.254 //set dns for eth0
->input secondary DNS [0.0.0.0]:

this parameter will be take effect when reboot!
really want to modify[yes]:
R3000 Wireline (config) # end
R3000 Wireline# write //save current configuration
Building configuration...
OK
R3000 Wireline # 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 certificates
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 { <i>cfg</i>   <i>rootfs</i> } <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>	All the function parameters are set by commands set and add, the difference is that set is for the single parameter and add is for the list parameter
Add	Add <i>parameters</i>	

## Glossary

Abbreviations	Description
AC	Alternating Current
APN	Access Point Name of GPRS Service Provider Network
ASCII	American Standard Code for Information Interchange
CE	Conformité Européene (European Conformity)
CHAP	Challenge Handshake Authentication Protocol
CLI	Command Line Interface for batch scripting
CSD	Circuit Switched Data
CTS	Clear to Send
dB	Decibel
dBi	Decibel Relative to an Isotropic radiator
DC	Direct Current
DCD	Data Carrier Detect
DCE	Data Communication Equipment (typically modems)
DCS 1800	Digital Cellular System, also referred to as PCN
DI	Digital Input
DO	Digital Output
DSR	Data Set Ready
DTE	Data Terminal Equipment
DTMF	Dual Tone Multi-frequency
DTR	Data Terminal Ready
EDGE	Enhanced Data rates for Global Evolution of GSM and IS-136
EMC	Electromagnetic Compatibility
EMI	Electro-Magnetic Interference
ESD	Electrostatic Discharges
ETSI	European Telecommunications Standards Institute
EVDO	Evolution-Data Optimized
FDD LTE	Frequency Division Duplexing Long Term Evolution
GND	Ground
GPRS	General Packet Radio Service
GRE	generic route encapsulation
GSM	Global System for Mobile Communications
HSPA	High Speed Packet Access
ID	identification data
IMEI	International Mobile Equipment Identification
IP	Internet Protocol
IPSec	Internet Protocol Security
kbps	kbits per second

L2TP	Layer 2 Tunneling Protocol
LAN	local area network
LED	Light Emitting Diode
M2M	Machine to Machine
MAX	Maximum
Min	Minimum
MO	Mobile Originated
MS	Mobile Station
MT	Mobile Terminated
OpenVPN	Open Virtual Private Network
PAP	Password Authentication Protocol
PC	Personal Computer
PCN	Personal Communications Network, also referred to as DCS 1800
PCS	Personal Communication System, also referred to as GSM 1900
PDU	Protocol Data Unit
PIN	Personal Identity Number
PLCs	Program Logic Control System
PPP	Point-to-point Protocol
PPTP	Point to Point Tunneling Protocol
PSU	Power Supply Unit
PUK	Personal Unblocking Key
R&TTE	Radio and Telecommunication Terminal Equipment
RF	Radio Frequency
RTC	Real Time Clock
RTS	Request to Send
RTU	Remote Terminal Unit
Rx	Receive Direction
SDK	Software Development Kit
SIM	subscriber identification module
SMA antenna	Stubby antenna or Magnet antenna
SMS	Short Message Service
SNMP	Simple Network Management Protocol
TCP/IP	Transmission Control Protocol / Internet Protocol
TE	Terminal Equipment, also referred to as DTE
Tx	Transmit Direction
UART	Universal Asynchronous Receiver-transmitter
UMTS	Universal Mobile Telecommunications System
USB	Universal Serial Bus
USSD	Unstructured Supplementary Service Data
VDC	Volts Direct current
VLAN	Virtual Local Area Network

VPN	Virtual Private Network
VSWR	Voltage Stationary Wave Ratio
WAN	Wide Area Network