## **Robustel GoRugged R3000**

# Dual SIM Industrial Cellular VPN Router For GPRS/EDGE/UMTS/HSPA/LTE Networks

## **User Guide**

Document Name:		User Guide
Firmware	:	1.01.00
Date	:	2014-01-17
Status	:	Confidential
Doc ID	:	RT_UG_R3000_v.2.0.0





www.robustel.com

### **About This Document**

This document describes hardware and software of Robustel R3000, Dual SIM Industrial 2G/3G/4G Router.

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

#### **Trademarks and Permissions**

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

#### Disclaimer

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

#### **Technical Support Contact Information**

 Tel
 :
 +86-18924045664

 Fax
 :
 +86-20-82321505

 E-mail :
 support@robustel.com

 Web
 :
 www.robustel.com

### Important Notice

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

### Safety Precautions

#### General

- The router generates radio frequency (RF) power. When using the router care must be taken on safety issues related to RF interference as well as regulations of RF equipment.
- Do not use your router in aircraft, hospitals, petrol stations or in places where using 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 26.6 cm or more from human body. Do not put the antenna inside metallic box, containers, etc.
- RF exposure statements
  - 1. For mobile devices without co-location (the transmitting antenna is installed or located more than 20cm away from the body of user and nearby person)
- FCC RF Radiation Exposure Statement
  - 1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.
  - 2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

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

### Using the router in vehicle

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

#### Protecting your router

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

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

### Regulatory and Type Approval Information

#### Table 1: Directives

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

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

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

Table 3: Toxic or hazardous substances or elements with defined concentration limits

Name of the part	Hazardo	Hazardous substances				
Name of the part	(Pb)	(Hg)	(Cd)	(Cr(VI))	(PBB)	(PBDE)
Metal Parts	ο	о	о	0	о	0
Circuit Modules	x	0	0	0	0	0
Cables and Cable Assemblies	0	0	0	0	0	0
Plastic and Polymeric parts	0	0	0	0	0	0

o:

Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in SJ/T11363-2006.

Х:

Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part *might exceed* the limit requirement in SJ/T11363-2006.

### **Revision History**

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

Release Date	Firmware Version	Doc Version	Details
2013-01-24	1.00	v.1.0.0	First Release
2014-01-17	1.01	v.2.0.0	Second Release

### Contents

Chapter 1.	Product Concept	
1.1	Overview	
1.2	Packing List	
1.3	Specifications	
1.4	Selection and Ordering Data	
Chapter 2.	Installation	14
2.1	LED Indicators	14
2.2	PIN assignment	15
2.3	USB interface	15
2.4	Reset Button	
2.5	Ethernet ports	
2.6	Mount the Router	
2.7	Install SIM Card and Micro SD Card	
2.8	Connect the External Antenna (SMA Type)	
2.9	Ground the Router	
Chapter 3.	Configuration settings over web browser	20
3.1	Configuring PC in Windows	20
3.2	Factory Default Settings	22
3.3	Control Panel	23
3.4	Status -> System	24
3.5	Status -> Network	27
3.6	Status -> Route	
3.7	Status -> VPN	
3.8	Status -> Services	29
3.9	Status -> Event/Log	
3.10	Configuration -> Link Management	
3.11	Configuration -> Cellular WAN	
3.12	Configuration -> Ethernet	
3.13	Configuration -> WiFi	
3.14	Configuration -> Serial	
3.15	Configuration -> DI/DO	53
3.16	Configuration -> USB	56
3.17	Configuration -> GPS	57
3.18	Configuration -> NAT/DMZ	60
3.19	Configuration -> Firewall	61
3.20	Configuration -> QoS	63
3.21	Configuration -> IP Routing	66
3.22	Configuration -> DynDNS	68
3.23	Configuration -> IPSec	69
3.24	Configuration -> Open VPN	74
3.25	Configuration -> GRE	79
3.26	Configuration -> L2TP	80

3.27       Configuration > PPTP						
3.29       Configuration -> VRRP.       .90         3.30       Configuration -> PT passthrough.       .90         3.31       Configuration -> AT over IP.       .92         3.32       Configuration -> Phone Book.       .92         3.33       Configuration -> Phone Book.       .92         3.33       Configuration -> SMS.       .94         3.44       Configuration -> Reboot.       .94         3.35       Configuration -> RobustLink.       .96         3.36       Configuration -> RobustLink       .96         3.37       Configuration -> Event.       .97         3.38       Configuration -> USR LED       .98         3.39       Administration -> Clock       .002         3.40       Administration -> Clock       .002         3.41       Administration -> USR Management.       .003         3.43       Administration -> Update Firmware.       .006         Chapter 4.       Configuration Examples       .0108         4.1.1       Console port       .008         4.1.1       Console port       .008         4.1.2       Digital Input       .009         4.1.3       Network.       .015         4.3.4       Aministration -> SDK Manageme	3.27	7 C	onfiguration -> PPTP	84		
3.30       Configuration > IP Passthrough	3.28	3 C	onfiguration -> SNMP	88		
3.31       Configuration -> AT over IP.	3.29	э с	onfiguration -> VRRP	90		
3.32       Configuration -> Phone Book       .92         3.33       Configuration -> SMS.       .94         3.34       Configuration -> Reboot       .94         3.35       Configuration -> RebostLink       .96         3.36       Configuration -> Syslog       .96         3.37       Configuration -> Event       .97         3.38       Configuration -> Event       .97         3.39       Administration -> Pofile       .98         3.40       Administration -> Clock       .09         3.41       Administration -> Clock       .02         3.42       Administration -> User Management       .00         3.43       Administration -> User Management       .00         3.44       Administration -> User Management       .00         3.43       Administration -> User Management       .00         3.44       Administration -> User Management       .00         3.45       Administration -> User Management       .00         4.1       Interface       .00         4.1       Interface       .00         4.1.1       Consle port       .00         4.1.2       Digital Dutput       .00         4.1.3       Digital Output       .00	3.30	) C	onfiguration -> IP Passthrough	90		
3.33       Configuration -> SMS	3.31	1 C	onfiguration -> AT over IP	92		
3.34       Configuration -> Reboot	3.32	2 C	onfiguration -> Phone Book	92		
3.35       Configuration -> RobustLink	3.33	з с	onfiguration -> SMS	94		
3.36       Configuration -> Syslog.       96         3.37       Configuration -> Event.       97         3.38       Configuration -> USR LED       98         3.39       Administration -> Drolle       98         3.40       Administration -> Clock       102         3.41       Administration -> Clock       102         3.42       Administration -> User Management.       104         3.43       Administration -> User Management.       104         3.44       Administration -> Update Firmware.       106         Chapter 4.       Configuration Examples       108         4.1       Interface       108         4.1.1       Console port       108         4.1.2       Digital Input       109         4.1.3       Digital Output       109         4.1.4       RS232       110         4.2       Cellular       111         4.2.1       Cellular       111         4.2.2       SMS Remote Status Reading       113         4.3       NAT       115         4.3.1       NAT       115         4.3.1       NAT       115         4.3.2       LIZP       116         4.3.3 </td <td>3.34</td> <td>4 C</td> <td colspan="4">Configuration -&gt; Reboot</td>	3.34	4 C	Configuration -> Reboot			
3.37       Configuration -> Event.       97         3.38       Configuration -> USR LED       98         3.39       Administration -> Tools       99         3.40       Administration -> Clock       102         3.42       Administration -> User Management       103         3.43       Administration -> User Management       104         3.44       Administration -> User Management       105         3.45       Administration -> Update Firmware       106         Chapter 4.       Configuration Examples       108         4.11       Interface       108         4.12.       Digital Output       109         4.13.       Digital Output       109         4.14.       RS232       110         4.15.       RS485       110         4.10.       Cellular       111         4.2.       Cellular       111         4.2.1       Cellular Dial-Up       111         4.2.2       SMS Remote Status Reading       113         4.3       Network       115         4.3.1       NAT       115         4.3.1       IPE       116         4.3.2       L2TP       116         4.3.3 </td <td>3.35</td> <td>5 C</td> <td>onfiguration -&gt; RobustLink</td> <td>96</td>	3.35	5 C	onfiguration -> RobustLink	96		
3.38       Configuration -> USR LED       98         3.39       Administration -> Profile       98         3.40       Administration -> Tools       99         3.41       Administration -> Clock       102         3.42       Administration -> Web Server       103         3.43       Administration -> User Management       104         3.44       Administration -> User Management       105         3.45       Administration -> Update Firmware       106         Chapter 4.       Configuration Examples       108         4.1       Interface       108         4.1.1       Console port       109         4.1.2       Digital Output       109         4.1.3       Digital Output       109         4.1.4       RS232       110         4.1.5       RS485       110         4.1.6       Cellular       111         4.2.1       Cellular Dial-Up       111         4.2.2       SMS Remote Status Reading       113         4.3       Network       115         4.3.1       NAT       115         4.3.2       L2TP       116         4.3.4       IPSEC VPN       120	3.36	5 C	onfiguration -> Syslog	96		
3.39       Administration -> Profile       98         3.40       Administration -> Tools       99         3.41       Administration -> Clock       102         3.42       Administration -> Web Server       103         3.43       Administration -> User Management       104         3.44       Administration -> User Management       104         3.43       Administration -> Update Firmware       106         Chapter 4.       Configuration Examples       108         4.1       Interface       108         4.1.1       Console port       108         4.1.2       Digital Input       109         4.1.3       Digital Output       109         4.1.4       RS232       110         4.1.5       RS485       110         4.2       Cellular       111         4.2.1       Cellular Dial-Up       111         4.2.2       SMS Remote Status Reading       113         4.3       Network       115         4.3.1       NAT       115         4.3.2       L2TP       116         4.3.4       IPSEC VPN       122         Chapter 5       Introductions for CLI       122	3.37	7 C	onfiguration -> Event	97		
3.40       Administration -> Tools       99         3.41       Administration -> Clock       102         3.42       Administration -> Web Server       103         3.43       Administration -> User Management       104         3.44       Administration -> User Management       105         3.45       Administration -> Update Firmware       106         Chapter 4.       Configuration Examples       108         4.1       Interface       108         4.1.1       Console port       109         4.1.2       Digital Input       109         4.1.3       Digital Output       109         4.1.4       R5232       110         4.1.5       R5485       110         4.1       R5485       110         4.1.2       Digital Output       109         4.1.3       Network       111         4.2.1       Cellular Dial-Up       111         4.2.2       SMS Remote Status Reading       113         4.3       Network       115         4.3.1       NAT       115         4.3.2       L2TP       116         4.3.3       PPTP       118         4.3.4       IPSEC VPN	3.38	8 C	onfiguration -> USR LED	98		
3.41       Administration -> Clock       102         3.42       Administration -> Web Server       103         3.43       Administration -> User Management       104         3.44       Administration -> DK Management       105         3.45       Administration -> Update Firmware       106         Chapter 4.       Configuration Examples       108         4.1       Interface       108         4.1.1       Console port       109         4.1.2       Digital Input       109         4.1.3       Digital Output       109         4.1.4       RS232       110         4.15       RS485       110         4.2       Cellular       111         4.2.1       Cellular Dial-Up       111         4.2.2       SMS Remote Status Reading       113         4.3       Network       115         4.3.1       NAT       115         4.3.2       L2PP       116         4.3.3       PPTP       118         4.3.4       IPSEC VPN       120         4.3.5       OPENVPN       122         Chapter 5.       Introductions for CLI       125         5.1       What's CLI and h	3.39	Э А	dministration -> Profile			
3.42       Administration -> Web Server       103         3.43       Administration -> User Management       104         3.44       Administration -> SDK Management       105         3.45       Administration -> Update Firmware       106         Chapter 4.       Configuration Examples       108         4.1       Interface       108         4.1.1       Console port       108         4.1.2       Digital Input       109         4.1.3       Digital Output       109         4.1.4       RS232       110         4.1.5       RS485       110         4.2       Cellular       111         4.2.1       Cellular Dial-Up       111         4.2.2       SMS Remote Status Reading       113         4.3       Network       115         4.3.1       NAT       115         4.3.2       L2TP       116         4.3.4       IPSEC VPN       120         4.3.5       OPENVPN       120         4.3.4       IPSEC VPN       122         Chapter 5       Introductions for CLI       125         5.1       What's CLI and hierarchy level Mode       125         5.2 <td< td=""><td>3.40</td><td>) A</td><td>dministration -&gt; Tools</td><td></td></td<>	3.40	) A	dministration -> Tools			
3.43       Administration -> User Management       104         3.44       Administration -> SDK Management       105         3.45       Administration -> Update Firmware       106         Chapter 4.       Configuration Examples       108         4.1       Interface       108         4.1.1       Console port       108         4.1.2       Digital Input       109         4.1.3       Digital Output       109         4.1.4       RS232       110         4.1.5       RS485       110         4.1.6       Cellular       111         4.2       Cellular Dial-Up       111         4.2.1       Cellular Dial-Up       111         4.2.2       SMS Remote Status Reading       113         4.3       Network       115         4.3.1       NAT       115         4.3.1       NAT       115         4.3.1       NAT       116         4.3.2       L2TP       116         4.3.4       IPSEC VPN       120         4.3.4       IPSEC VPN       120         4.3.5       OPENVPN       122         Chapter 5       Introductions for CLI       125	3.41	1 A	dministration -> Clock			
3.44       Administration -> SDK Management.       105         3.45       Administration -> Update Firmware.       106         Chapter 4.       Configuration Examples       108         4.1       Interface       108         4.1.1       Console port       108         4.1.2       Digital Input       109         4.1.3       Digital Output       109         4.1.4       RS232       110         4.1.5       RS485       110         4.2       Cellular       111         4.2.1       Cellular       111         4.2.2       SMS Remote Status Reading       113         4.3       Network       115         4.3.1       NAT       115         4.3.2       L2TP       116         4.3.3       PPTP       118         4.3.4       IPSEC VPN       120         4.3.5       OPENVPN       120         4.3.4       IPSEC VPN       122         Chapter 5.       Introductions for CLI       125         5.1       What's CLI and hierarchy level Mode       125         5.2       How to configure the CLI       127	3.42	2 A	dministration -> Web Server			
3.45       Administration -> Update Firmware.       106         Chapter 4.       Configuration Examples       108         4.1       Interface       108         4.1       Console port       108         4.1.2       Digital Input       109         4.1.3       Digital Output       109         4.1.4       RS232       110         4.1.5       RS485       110         4.2       Cellular       111         4.2.1       Cellular Dial-Up       111         4.2.2       SMS Remote Status Reading       113         4.3       Network       115         4.3.1       NAT       115         4.3.1       NAT       115         4.3.2       L2TP       116         4.3.3       PPTP       118         4.3.4       IPSEC VPN       120         4.3.5       OPENVPN       122         Chapter 5.       Introductions for CLI       125         5.1       What's CLI and hierarchy level Mode       125         5.2       How to configure the CLI       127	3.43	3 A	dministration -> User Management			
Chapter 4.       Configuration Examples       108         4.1       Interface       108         4.1.1       Console port       108         4.1.2       Digital Input       109         4.1.3       Digital Output       109         4.1.4       RS232       110         4.1.5       RS485       110         4.2       Cellular       111         4.2.1       Cellular Dial-Up       111         4.2.2       SMS Remote Status Reading       113         4.3       Network       115         4.3.1       NAT       115         4.3.2       L2TP       116         4.3.3       PPTP       118         4.3.4       IPSEC VPN       120         4.3.5       OPENVPN.       122         Chapter 5.       Introductions for CLI       125         5.1       What's CLI and hierarchy level Mode       125         5.2       How to configure the CLI       127	3.44	4 A	dministration -> SDK Management			
4.1       Interface       108         4.1.1       Console port       108         4.1.2       Digital Input       109         4.1.3       Digital Output       109         4.1.4       RS232       110         4.1.5       RS485       110         4.1.6       Cellular       111         4.2       Cellular Dial-Up       111         4.2.1       Cellular Dial-Up       111         4.2.2       SMS Remote Status Reading       113         4.3       Network       115         4.3.1       NAT       115         4.3.1       NAT       115         4.3.2       L2TP       116         4.3.3       PPTP       118         4.3.4       IPSEC VPN       120         4.3.5       OPENVPN       122         Chapter 5.       Introductions for CLI       125         5.1       What's CLI and hierarchy level Mode       125         5.2       How to configure the CLI       127	3.45	5 A	dministration -> Update Firmware			
4.1.1       Console port       108         4.1.2       Digital Input       109         4.1.3       Digital Output       109         4.1.4       RS232       110         4.1.5       RS485       110         4.2       Cellular       111         4.2.1       Cellular Dial-Up       111         4.2.2       SMS Remote Status Reading       113         4.3       Network       115         4.3.1       NAT       115         4.3.1       NAT       115         4.3.2       L2TP       116         4.3.3       PPTP       116         4.3.4       IPSEC VPN       120         4.3.5       OPENVPN       122         Chapter 5.       Introductions for CLI       125         5.1       What's CLI and hierarchy level Mode       125         5.2       How to configure the CLI       127	Chapter 4	4. C	onfiguration Examples			
4.1.2       Digital Input       109         4.1.3       Digital Output       109         4.1.4       RS232       110         4.1.5       RS485       110         4.2       Cellular       111         4.2.1       Cellular Dial-Up       111         4.2.2       SMS Remote Status Reading       113         4.3       Network       115         4.3.1       NAT       115         4.3.2       L2TP       116         4.3.3       PPTP       116         4.3.4       IPSEC VPN       120         4.3.5       OPENVPN       122         Chapter 5       Introductions for CL1       125         5.1       What's CLI and hierarchy level Mode       125         5.2       How to configure the CLI       127	4.1	Ir	nterface			
4.1.3       Digital Output       109         4.1.4       RS232       110         4.1.5       RS485       110         4.2       Cellular       111         4.2.1       Cellular Dial-Up       111         4.2.2       SMS Remote Status Reading       113         4.3       Network       115         4.3.1       NAT       115         4.3.2       L2TP       116         4.3.3       PPTP       116         4.3.4       IPSEC VPN       120         4.3.5       OPENVPN       122         Chapter 5.       Introductions for CLI       125         5.1       What's CLI and hierarchy level Mode       125         5.2       How to configure the CLI       127		4.1.1	Console port			
4.1.4       RS232       110         4.1.5       RS485       110         4.2       Cellular       111         4.2.1       Cellular Dial-Up       111         4.2.2       SMS Remote Status Reading       113         4.3       Network       115         4.3.1       NAT       115         4.3.2       L2TP       116         4.3.3       PPTP       116         4.3.4       IPSEC VPN       120         4.3.5       OPENVPN       122         Chapter 5.       Introductions for CLI       125         5.1       What's CLI and hierarchy level Mode       125         5.2       How to configure the CLI       127		4.1.2	Digital Input			
4.1.5       RS485       110         4.2       Cellular       111         4.2.1       Cellular Dial-Up       111         4.2.2       SMS Remote Status Reading       113         4.3       Network       115         4.3.1       NAT       115         4.3.2       L2TP       116         4.3.3       PPTP       116         4.3.4       IPSEC VPN       120         4.3.5       OPENVPN       122         Chapter 5       Introductions for CLI       125         5.1       What's CLI and hierarchy level Mode       125         5.2       How to configure the CLI       127		4.1.3	Digital Output			
4.2       Cellular       111         4.2.1       Cellular Dial-Up       111         4.2.2       SMS Remote Status Reading       113         4.3       Network       115         4.3.1       NAT       115         4.3.2       L2TP       116         4.3.3       PPTP       116         4.3.4       IPSEC VPN       120         4.3.5       OPENVPN       122         Chapter 5.       Introductions for CLI       125         5.1       What's CLI and hierarchy level Mode       125         5.2       How to configure the CLI       127		4.1.4	RS232			
4.2.1       Cellular Dial-Up.       111         4.2.2       SMS Remote Status Reading.       113         4.3       Network.       115         4.3.1       NAT.       115         4.3.2       L2TP       116         4.3.3       PPTP.       116         4.3.4       IPSEC VPN       120         4.3.5       OPENVPN.       122         Chapter 5.       Introductions for CLI       125         5.1       What's CLI and hierarchy level Mode       125         5.2       How to configure the CLI.       127		4.1.5	RS485			
4.2.2       SMS Remote Status Reading       113         4.3       Network       115         4.3.1       NAT       115         4.3.2       L2TP       116         4.3.3       PPTP       116         4.3.4       IPSEC VPN       120         4.3.5       OPENVPN       122         Chapter 5.       Introductions for CLI       125         5.1       What's CLI and hierarchy level Mode       125         5.2       How to configure the CLI       127	4.2	C	ellular			
4.3       Network       115         4.3.1       NAT       115         4.3.2       L2TP       116         4.3.3       PPTP       118         4.3.4       IPSEC VPN       120         4.3.5       OPENVPN       122         Chapter 5.       Introductions for CLI       125         5.1       What's CLI and hierarchy level Mode       125         5.2       How to configure the CLI       127		4.2.1	Cellular Dial-Up			
4.3       Network       115         4.3.1       NAT       115         4.3.2       L2TP       116         4.3.3       PPTP       118         4.3.4       IPSEC VPN       120         4.3.5       OPENVPN       122         Chapter 5.       Introductions for CLI       125         5.1       What's CLI and hierarchy level Mode       125         5.2       How to configure the CLI       127		4.2.2	SMS Remote Status Reading			
4.3.2       L2TP       116         4.3.3       PPTP       118         4.3.4       IPSEC VPN       120         4.3.5       OPENVPN       122         Chapter 5.       Introductions for CLI       125         5.1       What's CLI and hierarchy level Mode       125         5.2       How to configure the CLI       127	4.3	Ν				
4.3.3       PPTP		4.3.1	NAT			
4.3.4       IPSEC VPN       120         4.3.5       OPENVPN       122         Chapter 5.       Introductions for CLI       125         5.1       What's CLI and hierarchy level Mode       125         5.2       How to configure the CLI       127		4.3.2	L2TP			
4.3.5OPENVPN122Chapter 5.Introductions for CLI1255.1What's CLI and hierarchy level Mode1255.2How to configure the CLI127		4.3.3	РРТР			
Chapter 5.Introductions for CLI		4.3.4	IPSEC VPN			
<ul> <li>5.1 What's CLI and hierarchy level Mode</li></ul>		4.3.5	OPENVPN			
<ul> <li>5.1 What's CLI and hierarchy level Mode</li></ul>	Chapter	5. Ir	ntroductions for CLI			
	-		Vhat's CLI and hierarchy level Mode			
	5.2					
	5.3					

## **Chapter 1. Product Concept**

### 1.1 Overview

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

- Dual SIM redundancy for continuous cellular connections, supports 2G/3G/4G.
- WAN link management: cellular WAN/Ethernet WAN/WLAN WAN backup.
- VPN tunnel: IPSec/OpenVPN/PPTP/L2TP/GRE.
- Supports Modbus gateway (Modbus RTU/ASCII to Modbus TCP).
- Supports GPS (optional), provides real time location and tracking.
- Supports 802.11 b/g/n Wi-Fi (optional), AP and client mode.
- Supports SDK, provides user programmatic interface.
- Auto reboot via SMS/Caller ID/Timing.
- Supports RobustLink (Centralized M2M management platform).
- Flexible Management methods: Web/CLI/SNMP/RobustLink.
- Firmware upgrade via Web/CLI/USB/SMS/RobustLink.
- Various interfaces: RS232/RS485/Console/DI/DO/USB/Ethernet.
- Wide range input voltages from 9 to 60 VDC and extreme operating temperature.
- The metal enclosure can be mounted on a DIN-rail or on the wall, also with extra ground screw.

### 1.2 Packing List

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

• Robustel GoRugged R3000 router x 1



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



• 7-pin pluggable terminal block with lock for serial port, I/O and console port x 1



• CD with user guide x 1 **Note**: Please notify your sales representative if any of the above items are missing or damaged.

Optional accessories (can be purchased separately):

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



• Ethernet cable x 1



Wall Mounting Kit



• 35mm Din-Rail mounting kit



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



### 1.3 Specifications

#### **Cellular Interface**

- Standards: GSM/GPRS/EDGE/UMTS/HSPA/EVDO/FDD LTE
- GPRS/EDGE: 850/900/1800/1900 MHz
- HSUPA: 900/2100 or 850/1900 MHz optional, DL/UL 7.2/5.76 Mbps, fallback to 2G
- HSPA+: 850/900/1900/2100, DL/UL 21/5.76 Mbps, fallback to 2G
- FDD LTE: 800/900/1800/2100/2600 MHz, DL/UL 100/50 Mbps, fallback to 3G/2G
- EVDO: 450 or 800/1900 MHz, Rev A/B

- SIM: 2 x (3V & 1.8V)
- Antenna Interface: SMA Female
   Ethernet Interface
- Number of Ports: 2 x 10/100 Mbps, 2 LANs or 1 LAN 1 WAN
- Magnet Isolation Protection: 1.5KV

#### 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 Interface (Optional)**

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

#### Serial Interface

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

#### **Digital Input**

- Type: 2 x DI, Dry Contact
- Dry Contact: On: open, Off: short to GND

- Isolation: 3K VDC or 2K Vrms
- Digital Filtering Time Interval: Software selectable
- Interface: 3.5mm terminal block with lock

#### **Digital Output**

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

#### System

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

#### Software

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

#### Power Supply and Consumption

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

### **Physical Characteristics**

- Housing & Weight: Metal, 500g
- Dimension: (L x W x H): 125 x 108 x 45 mm
- Installation: 35mm Din-Rail or wall mounting or desktop

### **Regulatory and Type Approvals**

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

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

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

#### **Environmental Limits**

Model No.	Description	<b>Operating Environment</b>
R3000-2G	GPRS Router	-40 to 85°C/5 to 95% RH
R3000-2E	EDGE Router	-40 to 75°C/5 to 95% RH
R3000-3H	HSUPA Router	-40 to 85°C/5 to 95% RH
R3000-3P	HSPA+ Router	-40 to 85°C/5 to 95% RH
R3000-3E	EVDO Rev A/B Router	-20 to 60°C/5 to 95% RH
R3000-4L	FDD LTE Router	-25 to 60°C/5 to 95% RH
R3000-NU	Router, no cellular module	-40 to 85°C/5 to 95% RH

### 1.4 Selection and Ordering Data

Please refer to corresponding R3000 datasheet.

## Chapter 2. Installation

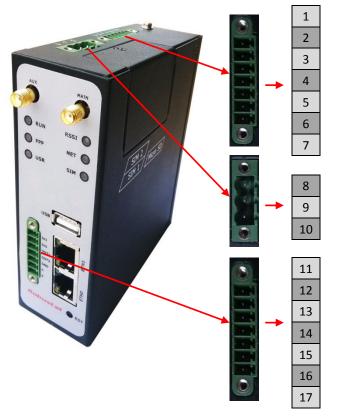
### 2.1 LED Indicators

O RUN	RSSI	O RUN	RSSI
O WLAN		О ррр	NET
O USR	SIMO	O USR	SIMO

Name	Color	Status	Function
		Blinking	Router is ready.
RUN	Green	On	Router is starting.
		Off	Router is power off.
		Dlinking	WLAN Indicator: Data is being transmitted.
		Blinking	PPP Indicator: Null
WLAN/P	Croon	On	WLAN Indicator: Wi-Fi AP/Client is enabled.
РР	Green	On	PPP Indicator: PPP connection is up.
		Off	WLAN Indicator: Wi-Fi AP/Client is disabled.
			PPP Indicator: PPP connection is down.
USR	Croon	On/Blinking	VPN tunnel/PPPoE/DynDNS/GPS is up.
USK	Green	Off	VPN tunnel/PPPoE/DynDNS/GPS is down.
	Green	On	Signal level: 21-31 (Perfect signal level).
RSSI	Yellow	On	Signal level: 11-20 (Average signal level).
	Red	On	Signal level: 1-10 (Exceptional signal level).
	Crean	Blinking	4G is connected but PPP connection is failed.
	Green	On	4G is connected and PPP connection is established.
	Yellow	Blinking	3G is connected but PPP connection is failed.
NET	reliow	On	3G is connected and PPP connection is established.
	Ded	Blinking	2G is connected but PPP connection is failed.
	Red	On	2G is connected and PPP connection is established.
	/	Off	Cannot register to any network.
	Croon	Blinking	Only SIM 1 is detected, but PIN code is incorrect.
	Green	On	Working with SIM 1 normally.
	Yellow	Blinking	Only SIM 2 is detected, but PIN code is incorrect.
SIM		On	Working with SIM 2 normally.
	Green&Y	Blinking between	Two SIMs are detected but both of their DIN sodes are incorrect
	ellow	two colors	Two SIMs are detected, but both of their PIN codes are incorrect.
	/	Off	No SIM inside.

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

### 2.2 PIN assignment



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

### 2.3 USB interface



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

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

### 2.4 Reset Button



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

### 2.5 Ethernet ports



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

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

### 2.6 Mount the Router

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



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



### 2.7 Install SIM Card and Micro SD Card



### ■ Inserting SIM Card or Micro SD Card

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

### Removing SIM Card or Micro SD Card

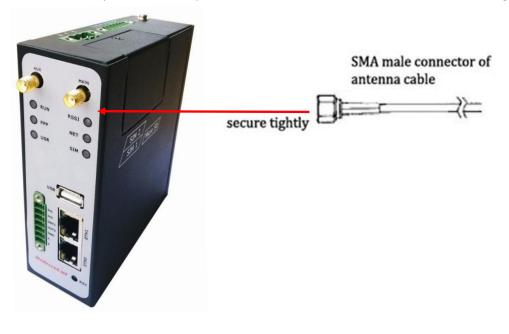
- 1. Make sure router is power off.
- 2. Press the card until you hear "a cracking sound", when the card will pop up to be pulled out.

#### Note:

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

### 2.8 Connect the External Antenna (SMA Type)

Connect router to an external antenna with SMA male connector. Make sure the antenna is for the correct frequency as your GSM/3G/4G operator with impedance of 50ohm, and also connector is secured tightly.



### 2.9 Ground the Router

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



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

## **Chapter 3. Configuration settings over web browser**

The router can be configured through your web browser. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista/7/8, etc. The product provides an easy and user-friendly interface for configuration.

There are various ways to connect the router, either through an external repeater/hub or connect directly to your PC. However, make sure that your PC has an Ethernet interface properly installed prior to connecting the router. You must configure your PC to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problems accessing the router web interface it is advisable to uninstall your firewall program on your PC, as these tend to cause problems accessing the IP address of the router.

### 3.1 Configuring PC in Windows

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



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

📥 Local Area Co	nnection Status	? 🛛
General Support		
Connection		
Status:		Connected
Duration:		00:05:56
Speed:		1.0 Gbps
Activity	Sent — 剩	
Bytes:	351,881	302,116
Properties	Disable	Close

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

🕹 Local Area Connection Properties 🛛 🔹 💽
General Authentication Advanced
Connect using:
B ASUSTeK/Broadcom 440x 10/100 Integrated Controller
Configure
This connection uses the following items:
<ul> <li>Client for Microsoft Networks</li> <li>Guide Printer Sharing for Microsoft Networks</li> <li>QuoS Packet Scheduler</li> <li>Internet Protocol (TCP/IP)</li> </ul>
Install Uninstall Properties
Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.
Show icon in notification area when connected
OK Cancel

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

Internet Protocol (TCP/IP) Prope	rties 🛛 🛛 🛛 🛛				
General Alternate Configuration					
	You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.				
<ul> <li>Obtain an IP address automatical</li> </ul>	y				
OUse the following IP address: —					
IP address:					
Subnet mask:					
Default gateway:					
<ul> <li>Obtain DNS server address autor</li> </ul>	natically				
OUse the following DNS server add	tresses:				
Preferred DNS server:					
Alternate DNS server:					
Advanced					
	OK Cancel				

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 re	quired. Login please.
Username:	admin
Password:	••••
Language:	English 💌
Please enter your login	username and password.
	Login

Item	Description
Username	admin
Password	admin
Eth0	192.168.0.1/255.255.255.0, LAN mode
Eth1	192.168.0.1/255.255.255.0, LAN mode

DHCP Server

```
Enabled.
```

### 3.3 Control Panel

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

lobustel					• Save	• Reboot	• Logout	11 12
atus 🔷	Syste	m					Log	ged in as: <b>adm</b>
ystem	LEDs Infor	nation						
letwork	RUN:	GREEN/BLINK	RSSI:	YELLOW/ON				
oute	PPP:	GREEN/ON	NET:	GREEN/ON				
PN	USR:	OFF	SIM:	YELLOW/ON				
ervices	Router Info							
/ent/Log	23 N2	0. 10. XX						
nfiguration	Device I	17 B.8	R3000					
	Serial N	× *	00300513060001					
nk Management	Device I	10 10	Cellular Router					
ellular WAN	55465 B.S.	e Version:	1.01.00					
hernet		re Version:	1.01.00					
erial	Kernel \	10 10.000 ALMON	2.6.39-9					
/DO		odule Type:	HE910					
SB 📃		rmware Version:	11.126.10.81.00					
PS	Uptime:		0 days 00:15:06					
AT/DMZ	CPU Lo	ad:	00.90%					
rewall	RAM Tot	al/Free:	123.57MB/75.63M	B(61.20%)				
oS	System	Time:	2007-01-01 23:01	.:29				
Routing	Current W/	N Link						
nDNS	Current	WAN Link:	Cellular					
sec	IP Addr	BSS:	10.158.107.212					
penVPN	Gatewa	y:	192.168.254.254					
RE	NetMas		255.255.255.255					
2TP								
ото								Refresh

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

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

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

### 3.4 Status -> System

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

#### **LEDs Information**

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

Syste	m		
LEDs Inform	nation		
RUN:	GREEN/BLINK	RSSI:	RED/ON
PPP:	GREEN/ON	NET:	YELLOW/ON
USR:	OFF	SIM:	YELLOW/ON

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

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

### **Current WAN Link**

Cellular
10.138.108.79
192.168.254.254
255.255.255.255
210.21.4.130 221.5.88.88
30

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

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

#### **Cellular Information**

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

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

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

### 3.5 Status -> Network

This section displays the router's Network status, which include status of Cellular WAN, ETH0, ETH11, WLAN (AP mode)/WLAN (Client mode).

Network		
Cellular WAN		
Connection Status:		
Connect Time:		
IP Address:		
MTU:	1500	
Gateway:		
Primary DNS Server:		
Secondary DNS Server:	0.0.0.0	
LANO		
LANO IP Address:	172.16.4.11	
	172.16.4.11 00:ff:66:87:65:b2	
IP Address:		
IP Address: MAC Address:	00:ff:66:87:65:b2	
IP Address: MAC Address: MTU: NetMask:	00:ff:66:87:65:b2 1500	
IP Address: MAC Address: MTU: NetMask:	00:ff:66:87:65:b2 1500	
IP Address: MAC Address: MTU: NetMask:	00:ff:66:87:65:b2 1500 255.255.0.0	
MAC Address: MTU: NetMask: LAN1 IP Address:	00:ff:66:87:65:b2 1500 255.255.0.0 192.168.222.1	

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

WiFi		
MAC Address:	00:23:a7:25:23:27	
SSID:	R3K	
Mode:	AP	
WPA State:	Completed	

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

WiFi WAN	
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 enable WLAN and works as Client mode.

### 3.6 Status -> Route

This section displays the router's route table.

Rout	te				
te Tabl	e				
	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	РРТР	OpenVPN	GRE					
IPsec Status									
No. T									
IPsec Detail Status									
Show Detail St	atus								

#### Robustel GoRugged R3000 User Guide

IPsec	L2	тр	РРТР	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	L	2ТР	РРТР	OpenVPN	GRE	
РРТ	P Client						
	No.	Tunnel name	Status	Local IP	Remote IP	Connect Time	
РРТ	P Server						
	No.	Tunnel name	Status	Local IP	Remote IP	Connect Time	

I	osec	L2TP	РРТР	OpenVPN	GRE	
VPN Sta	itus					
	No.	Tunnel name	Status			

	IPsec	: L:	2ТР	РРТР	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, Serial and DI/DO.

VRRP	DynDNS	Serial	DI/DO
VRRP			
VRRP is disabled!			
VRRP	DynDNS	Serial	DI/DO
DynDNS			
DynDNS is disable	ed!		

#### Robustel GoRugged R3000 User Guide

VRRP	DynDNS	Seri	al Di	I/DO
RS232: 115200, N	, 8, 1			
RS485: 115200, N	, 8, 1			
VRRP	DynDNS	Seri	ial Di	I/DO
DI				
No.	Level	Status	Start Counter	Event Counter Value
DO				
No.	Level	Status		

### 3.9 Status -> Event/Log

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

### Event/Log

Event/Log Messages		
Download:	Please Select 💌	
Log Level:	DEBUG 🗸	
13-08-30 17:15:17 <0> router 13-08-30 17:15:24 <0> router 13-08-30 17:15:25 <0> router	: open /dev/ttyUSB3 successful! : sent:ATE0 : failed 1/5 to test AT command ATE0 : sent:ATE0	
OK 13-08-30 17:15:27 <0> router 13-08-30 17:15:27 <0> router +CME ERROR: SIM busy 13-08-30 17:15:27 <3> router 13-08-30 17:15:32 <0> router 13-08-30 17:15:32 <0> router +CPIN: READY	: rcvd: : failed 1/5 to check SIM card : sent:AT+CPIN?	
OK 13-08-30 17:15:33 <0> router 13-08-30 17:15:33 <0> router OK 13-08-30 17:15:33 <0> router 13-08-30 17:15:33 <0> router	: rcvd: : sent:AT!ENTERCND="A710"	•
Download System Diagnosing Dat	a	

JUI y

Download System Diagnosing Data

	Manual Refresh 💙 Refresh Clear						
	Event/Log						
Item	Description						
Download	Select the log messages you want to download.						
	Select the Log level in the drop-down menu: DEBUG, INFO, NOTICE, WARNING, ERR,						
Log Level	CRIT, ALERT, EMERG.						
Download Sytem	Click Download System Diggnosing Data to download diagnose file						
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".						
Manual Refresh	User can select these intervals to refresh the log information.						

### 3.10 Configuration -> Link Management

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

#### Link Management

Link Management Settings	
Primary Interface:	Cellular 💌
Backup Interface:	None 🔻
ICMP Detection Primary Server:	8.8.8.8
ICMP Detection Secondary Server:	8.8.4.4
ICMP Detection Interval (s):	30
ICMP Detection Timeout (s):	3
ICMP Detection Retries:	3
Reset The Interface	
*It is recommended to use an ICMP detect	tion server to keep router alv
should be a set of the	

\*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				
	Selected from "Cellular", "Eth0", "WiFi".					
Primary Interface	1. Cellular: Select to make cellular as the primary WAN link.	Cellular				
Findly interface	2. Eth0: Select to make Eth0 as the primary WAN link.	Cellulai				
	3. WiFi: Select to make WiFi as the primary WAN link.					
	Selected from "None", "Eth0", "WiFi".					
	1. None: Do not select backup interface.					
Backup Interface	2. Cellular: Select Cellular as the backup WAN link.	None				
	3. Eth0: Select Eth0 as the backup WAN link.					
	4. WiFi: Select WiFi as the backup WAN link.					
ICMP Detection Primary	Router will ping this primary address/domain name to check that if the	Null				
Server	current connectivity is active.	Null				
ICMP Detection	Router will ping this secondary address/domain name to check that if the	Null				
Secondary Server	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	3				
ICIVIP Detection Retries	Retries time, it will consider that the connection has been lost.					
Deset The Interface	Enable to reset the cellular/ETH0 interface after the max ICMP detection	2				
Reset The Interface	retries.	3				

### 3.11 Configuration -> Cellular WAN

This section allows users to set the Cellular WAN and the related parameters. **Note**: This section will not be displayed if you select "Eth0 Only" in "Configuration"->"Link Management"->"WAN

### Link".

Basic	Advanced	ISP Profile	9	
Cellular Settings				
	SIM	11	SIM2	
Status:	Rea	dy	Not inserted	
Network Provider	r Type: Aut	o 💙	Aut o 😽	
APN:				
Username:				
Password:				
Dialup No.:				
PIN code request	:: Set	: PIN Code	Set PIN Code	
Connection Mode				
o				

Connection Mode:	Connect on de	mand 🔽				
Redial Interval (s):	30					
Max Retries:	3					
Inactivity Time (s):	0					
Serial Output Content (Hex):						
🗹 Triggered by Serial Data						
🗹 Triggered by Tel						
🗹 Triggered by SMS						
SMS Connect command:						
SMS disconnect command:						
SMS connect reply:						
SMS disconnect reply:						
Phone Group:	NULL <u>Click t</u> a	o add Phon	eGroup!			
Triggered by IO (Note: use	DI_1.)					
Periodically connect						
Time schedule:	NULL 🔽					
Time Range						
Name SUN MON T	JE WED THU	FRI SAT	Time Range1	Time Range2	Time Range3	
schedule_1 🗹 🗹			08:10-12:00	14:10-20:15		x
					Add	

al SIM Policy			
Main SIM Card:	SIM1 💌		
🗹 Switch to backup SIM car	d when connection fails		
🗹 Switch to backup SIM car	d when ICMP Detection fail	5	
🗹 Switch to backup SIM car	d when roaming is detecte	t	
Preferred PLMN:			
🗹 Switch to backup SIM car	d when IO is active (Note:	use DI_2.)	
🗹 Switch to backup SIM car	d when data limit is exceed	led	
Max Data Limitation (MB):	100	100	
Date of Month to clean:	1	1	
Already used (KB):	0	0	
	Clear	Clear	
🗹 Switch back Main SIM car	d after timeout		
Initial Timeout (min):	60		

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

i.

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

i.

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

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

Basic Advance	ed ISP Profile	
Cellular Advanced Settings		
	SIM1	SIM2
Phone No.:		
Network Type:	Auto 💌	Auto 💌
Band Mode:	ALL 🔽	ALL 🖌
Authentication:	Auto 💌	Auto 💌
MTU:	1500	1500
MRU:	1500	1500
Asyncmap Value:	fffffff	fffffff
Use Peer DNS:	$\checkmark$	✓
Primary DNS Server:		
Secondary DNS Server:		
Address/Control Compression:		✓
Protocol Field Compression:		
Expert Options:	noccp nobsdcomp	noccp nobsdcomp

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

can be separated by a space.	nobsdcomp

#### **ISP Profile**

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

В	asic A	dvanced	ISP Profile			
(SP Pro	file List					
	ISP	APN	Username	Password	Dialup No.	
	china-mobile	3gnet			*99***1#	x
					Add	

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

### **3.12** Configuration -> Ethernet

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

Eth0	Eth1	Dhcp Relay
Ethernet Interface T	ype	
💿 lan	0 wa	N
LAN Interface		
🔲 Enable Bridge	(As 2 Ports Switch)	
IP Address:		
NetMask:		
MTU:	1500	
Media Type:	Auto-n	egotiation 🝷
LAN Interface		
🗹 Enable Bridge	e (As 2 Ports Switch)	
IP Address:	192.16	38.0.1
NetMask:	255.25	5.255.0
MTU:	1500	

IP Address	NetMask
IF Addless	
	Add
HCP Server	
🗹 Enable DHCP Server	
IP Pool Start:	192.168.0.2
IP Pool End:	192.168.0.100
NetMask:	255.255.255.0
Lease Time (min):	60
Primary DNS Server:	192.168.0.1
Secondary DNS Server:	
Windows Name Server:	192.168.0.1
Static Lease	
MAC Address	IP Address
*MAC: ff:ff:ff:ff:ff:ff	Add

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

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

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

Eth0	Eth1	VLAN	Dhcp Relay
LAN Interface			
IP Address:	192.168	. 0. 1	
NetMask:	255.255	. 255. 0	
MTU:	1500		
Media Type:	Auto-ne	egotiation 🔻	

Eth0	Eth1 Dhcp Relay
LAN Interface	
IP Address:	192.168.1.1
NetMask:	255.255.255.0
MTU:	1500

Multiple IP	Address	
	IP Address	NetMask
	и	Add

HCP Server	
Enable DHCP Server	
IP Pool Start:	192.168.0.2
IP Pool End:	192.168.0.100
NetMask:	255.255.255.0
Lease Time (min):	60
Primary DNS Server:	192.168.0.1
Secondary DNS Server:	
Windows Name Server:	192.168.0.1
Static Lease	
MAC Address	IP Address
*MAC: ff:ff:ff:ff:ff:ff	Add

Eth1@Ethernet		
Item	Description	Default

IP Address, Netmask, MTU, Media Type @ LAN Interface	Set the IP address, Netmask, MTU and Media Type of Eth1. These parameters will be un-configurable if you enable Bridge.	Null
Multiple IP Address @ LAN Interface	Assign multiple IP addresses for Eth1.	Null
Enable DHCP Server @ DHCP Server	Enable to make router can lease IP address to DHCP clients which connect to Eth1.	Enable
IP Pool Start, IP Pool End @ DHCP Server	Define the beginning (IP Pool Start) and end (IP Pool End) of the pool of IP addresses which will lease to DHCP clients.	192.168.0.2/ 192.168.0.10 0
Netmask @ DHCP Server	Define the Netmask which the DHCP clients will obtain from DHCP server.	255.255.255. 0
Lease Time @ DHCP Server(min)	Define the time which the client can use the IP address which obtained from DHCP server.	60
Primary/Secondary DNS Server @ DHCP Server	Define the primary/secondary DNS Server which the DHCP clients will obtain from DHCP server.	192.168.0.1/ 0.0.0.0
Windows Name Server @ DHCP Server	Define the WINS Server which the DHCP clients will obtain from DHCP server.	192.168.0.1
Static Lease @ DHCP Server	Define to lease static IP Addresses, which conform to MAC Address of the connected equipment.	Null

Router can be DHCP Relay, which will provide a relay tunnel to solve problem that DHCP Client and DHCP Server is not in a same subnet. This section allow user to configure DHCP Relay settings.

Eth0	Eth1	Dhcp Relay
DhcpRelay Configura	ation	
🗹 Enable		
DHCP Server:		

DHCP Relay @ Ethernet			
Item	Description	Default	
Enable Eth0/1 VLAN@Eth0/1 VLAN	Enable to make router can encapsulate and de-encapsulate the VLAN	Disable	
Settings	tag.	DISADIE	
VLAN ID@Eth0/1 VLAN Settings	Set the Tag ID of VLAN	10/11	
IP Address, NetMask @Eth0/1 VLAN Settings	Set the IP address, Netmask of VLAN interface	Eth0/1's address, Netmask	IP

Note: IP Address and NetMask will be hidden if user bridge two Ethernet ports.

### 3.13 Configuration -> WiFi

This section allows users to set parameters of WiFi.

Basic	MAC Filter Status					
WiFi Basic Settings	ViFi 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 enable WiFi feature and works as AP mode

Basic	Status	
WiFi Basic Settings		
🗵 Enable WiFi		
Mode:	Client v	
Channel:	Auto 👻	
SSID:	Router_AP Scan	
Hide SSID:		
Security Mode:	Open -	
WiFi Network Settin	lgs	
IP Configuration:	DHCP Client 💌	
🗷 Use Peer DNS		
Override DHCP Server Values:		
Netmask:		
Gateway:		

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

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

	Ethomat to window (on LAN to M/LAN) wetween the deuter. For some	
	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 is wanted to	
	work as "Client" mode, please go to tab "Configuration" -> "Link	
	Management" -> "Primary Interface" to select "WiFi" as WAN link.	
	Select the frequency channel, which includes "Auto", "1", "2" "13".	
Channel	Auto: R3000 will scan all frequencies until it finds one with an available	
Channer	access point or wireless network it can join.	Auto
	1~13: R3000 will be fixed to work with this channel.	
	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	
SSID	to be able to communicate with each other.	Poutor AD
עוכנ	When R3000 works as Client mode, enter SSID of the access point which	Router_AP
	R3000 want to connect.	
	Input from 1 to 31 characters.	
	When R3000 works as AP mode, after clicking this check box R3000 will	
	not broadcast the SSID. Other wireless devices cannot discover this	
	access point automatically. User need to enter the SSID manually to let	
Hide SSID	their wireless devices join this access point.	Disable
	When R3000 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".	
	Select from "Open", "WPA" and "WPA2".	
	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.	
	WPA/WPA2: Personal versions of WPA/WPA2 (Wi-Fi Protected Access),	
Security mode	also known as WPA/WPA-PSK (Pre-Shared Key), provide a simple way of	Open
	encrypting a wireless connection for high confidentiality. WPA2 is a	
	stronger security feature than WPA.	
	<b>Note</b> : R3000 supports WPA/WPA2 Personal version, not enterprise	
	version.	
	Select from "TKIP" and "CCMP (AES)".	
	TKIP: Temporal Key Integrity Protocol (TKIP) encryption is used over the	
	wireless link. TKIP encryption can be used with WPA-PSK and WPA with	
Encryption	802.1x authentication.	CCMP (AES)
	CCMP (AES): CCMP (AES) encryption is used over the wireless link.	
	CCMP can be used WPA-PSK and WPA with 802.1x authentication.	
	<i>Note</i> : CCMP (AES) is a stronger encryption algorithm than TKIP.	
	When R3000 works as AP mode, enter Master key to generate keys for	
Passphrase	encryption. A Passphrase is used as a basis for encryption methods (or	Null
	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.	
	When R3000 works as Client mode, enter access point's passphrase	
	which it wants to connect to.	
Input from 8 to 63 characters.		
Kay Danayyal Interval(a)	Enter the time period of group key renewal.	2600
Key Renewal Interval(s)	<b>Note</b> : Only for AP mode.	3600
	When R3000 works as AP mode, Click to link to page "Eth1" to check	
WiFi Network Settings	the network settings, WiFi interface bridged with eth1 this time.	Null
WITT NELWORK Settings	When R3000 works as Client mode, this item is used to do IP	INUII
	configuration of access point.	

Basic	MAC Filter	Status
MAC Filter Settings		
Enable ACL:		
Mode:	Allow 👻	
Access Control List		
Index MAC Address		
	Add	

### *Note*: Available when R3000 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		
	Select from "Allow" and "Deny".			
	Allow: Only the packets fitting the entities of the "Access Control List"			
	can be allowed.			
Mode	Deny: All the packets fitting the entities of the "Access Control List" will	Allow		
	be denied.			
	Note: R3000 can only allow or deny devices which are included in			
	"Access Control List" at one time.			
Access Control List	Click "Add" to add MAC address.	Null		

Basic	MAC Fi	lter	Status
Status			
BSSID:			
SSID:			
Mode:			
Key Management	:		
Cipher Pairwise:			
Cipher Group:			
WPA State:			
Address:			
Associated Clients			
Index	BSSID	IP Addr	ess

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

Address	Show the MAC address of R3000'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/RS485) parameters.

RS232	RS485	
Serial Port Settings		
Baudrate:	115200	
Data Bit:	8	•
Parity:	None	
Stop Bit:	1	
Flow Control:	None	•
Protocol Settings		
Protocol:	None	

### • When Select Protocol "Transparent":

Protocol Settings		
Protocol:	Transparent	_
Mode:	TCP server 🔻	
Local Port:	502	
Show Protocol Advanced		
Interval Timeout (1*10ms):	10	
Packet Length:	1360	
Enable Delimiter1		
Delimiter1 (Hex):	0	
Enable Delimiter2		
Delimiter2 (Hex):	0	
Delimiter Process:	Strip 🔻	

• When Select Protocol "Modbus":

Protocol Settings			
Protocol:	Modbus 💌		
Local Port:	0		
Attached serial device type:	Modbus RTU master	1	
Modbus Slave			
Slave Address	Slave Port	ID	
*ID:<1-247> or <1-247;	>-<1-247>	bbA	

• When Select Protocol "Transparent Over Rlink":

Protocol Settings	
Protocol:	Transparent Over Rlink -
Interval Timeout (1*10ms):	10

• When Select Protocol "Modbus Over Rlink":

Protocol Settings	
Protocol:	Modbus Over Rlink
Attached serial device type:	Modbus RTU slave 🔽

#### • When Select Protocol "AT Over COM":

Protocol Settings	
Protocol:	AT Over COM 🛩
🗹 Display all com (Note enable	e this function will disable cellular WAN.)
COM Name:	/dev/ttyS1 🐱

#### • When Select Protocol "GPS Report":

Protocol Settings	
Protocol:	GPS Report

RS232 @ Serial				
Item	Description	Default		
Baud-rate	Select from "300", "600", "1200", "2400", "4800", "9600", "19200", "38400",			
Bauu-rale	"57600" , "115200"and "230400".	115200		
Data bit	Select from "7" and "8".	8		
Parity	Select from "None", "Odd" and "Even".	None		
Stop bit	Select from "1" and "2".	1		
Flow control	Select from "None", "Software" and "Hardware".	None		
Protocol	Select from "None", "Transparent", "Modbus", "Transparent Over Rlink",	None		

	"Modbus Over Rlink" "AT Over COM" and "GPS Report".	
	1. None: Router will do nothing in RS232 serial port.	
	2. Transparent: Router will transmit the serial data transparently without any protocols.	
	<ol> <li>Modbus: Router will translate the Modbus RTU data to Modbus TCP data</li> </ol>	
	and vice versa.	
	4. Transparent Over Rlink: Router will send all data from RS232 serial port to	
	Robustlink, then Robustlink will forward the data to another destination site.	
	5. Modbus Over Rlink: Router will translate all data from RS232 serial port to	
	Modbus TCP protocol data, and then send to Robustlink, after that	
	Robustlink will forward the data to another destination site.	
	6. AT Over COM: select to operate router via RS232 COM port. For example,	
	enter AT commands to router via RS232 COM port.	
	7. GPS Report: select to enable router to output GPS status data through RS232	
	port.	
	Select from "TCP Server", "TCP Client" and "UDP".	
	TCP Client: Router works as TCP client, initiate TCP connection to TCP server.	
Mada @Transparant	Server address supports both IP and domain name.	ТСР
Mode @Transparent	TCP Server: Router works as TCP server, listening for connection request from	Client
	TCP client.	
	UDP: Router works as UDP client.	
Local Port	Enter the Local port for TCP or UDP.	0
@Transparent		
	Click "Add" button to add multiple server. You need to enter the server's IP and	
Multiple Server	port, and enable or disable "Send data to serial". If you disable "Send data to	None
@Transparent	serial", router will not transmit the data from this server to serial port.	
ahawa Duata sal	<i>Note:</i> This section will not be displayed if you select "TCP server" in "Mode".	
show Protocol	Tick to enable protocol od grand activity	Disable
Advanced @	Tick to enable protocol advanced setting.	Disable
Transparent	This item will show up when you enable any VPN tunnel of R3000, it means serial	
Local IP @	data can be matched to this local IP address and be transmitted or received via	
c	VPN tunnel.	Null
Transparent	<b>Note</b> : when you do not enable any VPN tunnel, this item will not show up.	
	The serial port will queue the data in the buffer and send the data to the Cellular	
Interval Timeout	WAN/Ethernet WAN when it reaches the Interval Timeout in the field.	
@Transparent	<b>Note</b> : Data will also be sent as specified by the packet length or delimiter settings	10
	even when data is not reaching the interval timeout in the field.	
	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	
Packet Length	maximum amount is specified and data in the buffer will be sent as specified by	1360
@Transparent	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	
		1

	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.	
	When Delimiter 1 is enabled, the serial port will queue the data in the buffer and	
Enable Delimiter1/2	send the data to the Cellular WAN/Ethernet WAN when a specific character,	<b>D</b> : 11
	entered in hex format, is received. A second delimiter character may be enabled	Disable
	and specified in the Delimiter 2 field, so that both characters act as the delimiter	
	to control when data should be sent.	
Delimiter1/2 (Hex)	Enter the delimiter in Hex.	0
@Transparent		
	The Delimiter process field determines how the data is handled when a delimiter	
Delimiter Process	is received.	
@Transparent	None: Data in the buffer will be transmitted when the delimiter is received; the	Strip
	data also includes the delimiter characters.	
	Strip: Data in the buffer is first stripped of the delimiter before being transmitted.	
	This item will show up When you enable any VPN tunnel of R3000, it means serial	
Local IP @ Modbus	data can be matched to this local IP address and be transmitted or received via	0
	VPN tunnel.	Ŭ
	<b>Note</b> : when you do not enable any VPN tunnel, this item will not show up.	
Local Port @ Modbus	Enter the Local port for Modbus.	0
	Select From "Modbus RTU slave", "Modbus ASC ${ m II}~$ 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 $\Pi$ 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	Modbu
Attached serial device	@Modbus" and wait to be connected.	s RTU
type @Modbus	Modbus RTU master: router connects to master device which works under	slave
	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 [] 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.	
	Add the Modbus slaves which will be polled by Modbus master (router). This	
Modbus Slave	section only displayed when you select "Modbus RTU master" or "Modbus ASC II	Null
@Modbus	master" in "Attached serial device type".	
Slave Address @	This connection is usually used to connect to the Modbus slave devices which as	
Slave Address @ Modbus Slave	TCP server. Enter IP address of the TCP server.	Null
		Null
Slave Port @ Modbus	Enter the port number of TCP server.	INUII

Slave		
ID @ Modbus Slave	Enter the ID number of TCP server.	Null
Interval Timeout @ Transparent Over Rlink	Transparent Over 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.	
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/tt yUSB1

#### RS232 RS485 Serial Port Settings 115200 Baudrate: • 8 Data Bit: • Parity: None • 1 Stop Bit: • Protocol Settings Protocol: None -

#### • When Select Protocol "Transparent":

Protocol Settings	
Protocol:	Transparent 💌
Mode:	TCP server 💌
Local Port:	503
Show Protocol Advanced	
Interval Timeout (1*10ms):	10
Packet Length:	1360
Enable Delimiter1	
Delimiter1 (Hex):	0
Enable Delimiter2	
Delimiter2 (Hex):	0
Delimiter Process:	Strip -

#### Robustel GoRugged R3000 User Guide

#### • When Select Protocol "Modbus":

Protocol Settings		
Protocol:	Modbus	•
Local Port:	503	
Attached serial device type:	Modbus RTU slave	-

### • When Select Protocol "Transparent Over Rlink":

Protocol Settings	
Protocol:	Transparent Over Rlink 💌
Interval Timeout (1*10ms):	10

#### • When Select Protocol "Modbus Over Rlink":

Protocol Settings	
Protocol:	Modbus Over Rlink 🗸
Attached serial device type:	Modbus RTU slave 🔽

RS485 @ Serial				
Item	Description	Default		
Baud-rate	ud-rate         Select from "300", "600", "1200", "2400", "4800", "9600", "19200", "38400", "57600", "115200"and "230400".			
Data bit	Select from "7" and "8".	8		
Parity	Select from "None", "Odd" and "Even".	None		
Stop bit	Select from "1" and "2".	1		
Protocol	Select from "None", "Transparent" and "Modbus". Transparent: Router will transmit the serial data transparently without any protocols. Modbus: Router will transmit the serial data with Modbus protocol.			
Mode @Transparent	Node @Transparent Select from "TCP Server", "TCP Client" and "UDP".			
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, it means serial data can be matched to this local IP address and be transmitted or received via VPN tunnel.	0		

	Note: when you do not enable any VPN tunnel, this item will not show up.	
	The serial port will queue the data in the buffer and send the data to the	
Interval Timeout @Transparent	Cellular WAN/Ethernet WAN when it reaches the Interval Timeout in the	
	field.	10
	Note: Data will also be sent as specified by the packet length or delimiter	
	settings even when data is not reaching the interval timeout in the field.	
	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	
Packet Length	as specified by the interval timeout or delimiter settings or when the buffer	1260
@Transparent	is full. When a packet length between 1 and 1024 bytes is specified, data in	1360
	the buffer will be sent as soon it reaches the specified length.	
	Note: Data will also be sent as specified by the interval timeout or delimiter	
	settings even when data is not reaching the preset packet length.	
	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	
Enable Delimiter1	character, entered in hex format, is received. A second delimiter character	Disable
	may be enabled and specified in the Delimiter 2 field, so that both	
	characters act as the delimiter to control when data should be sent.	
Delimiter1 (Hex) @ Transparent	Enter the delimiter in Hex.	0
	The Delimiter process field determines how the data is handled when a	
	delimiter is received.	
Delimiter Process @	None: Data in the buffer will be transmitted when the delimiter is received;	
Transparent	the data also includes the delimiter characters.	Strip
	Strip: Data in the buffer is first stripped of the delimiter before being	
	transmitted.	
	This item will show up When you enable any VPN tunnel of R3000, it means	
	serial data can be matched to this local IP address and be transmitted or	
Local IP @ Modbus	received via VPN tunnel.	0
	<b>Note</b> : when you do not enable any VPN tunnel, this item will not show up.	
Local Port @ Modbus	Enter the Local port for Modbus.	0
	Select From "Modbus RTU slave", "Modbus ASC ${ m II}~$ slave", "Modbus RTU	
	master" and "Modbus ASC ${ m II}$ master".	
Attached serial device	Modbus RTU slave: router connects to slave device which works under	
	Modbus RTU protocol.	
	Modbus ASC $\Pi$ slave: router connects to slave device which works under	Modbus
type @ Modbus	Modbus ASC II protocol.	RTU slave
	Modbus RTU master: router connects to master device which works under	
	Modbus RTU protocol.	
	Modbus ASC $\Pi$ master: router connects to master device which works	
	under Modbus ASC II protocol.	
Modbus Slave @	Add the Modbus slaves which will be polled by Modbus master (router). This	Null

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

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

DI DO		
DI_1 Configuration		
🗹 Enable DI		
Mode:	OFF 💌	
Filtering (1*100ms):	1	
SMS Alarm		
Triggering Alarm	Recovering Alarm	Phone Group
		Add
DI_2 Configuration		
🗹 Enable DI		
Mode:	OFF 🗸 🗸	
Filtering (1*100ms):	1	
SMS Alarm		
Triggering Alarm	Recovering Alarm	Phone Group
		Add

DI @ DI/DO			
Item	Description	Default	

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

### DI DO

DO Configu	DO Configuration				
	Item	Description			
	DO_1	Enable:false;			
	DO_2	Enable:false;			

DO Configuration			
Enable			_
Alarm Source:			
🔲 DI Alarm	SMS Control	Call Control	
DO Action:			
Alarm On Action:	on 🐱		
Alarm Off Action:	on 🐱		
Status When Power On:	on 💌		
Keep On (s):	0		

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

Available when enable Pulse in Alarm On Action/Alarm Off Action.		
Available when chable Fulse in Alarm on Action/Alarm on Action.		
Delay The first pulse will be generated after a "Delay".	0	
Input from 0 to 30000ms. (0=generate pulse without delay)		
Available when enable Pulse in Alarm On Action/Alarm Off Action.		
In Pulse Output mode, the selected digital output channel will generate a square		
Low wave as specified in the pulse mode parameters. The low level widths are specified	10	
here.		
Input from 1 to 30000 ms.		
Available when enable Pulse in Alarm On Action/Alarm Off Action.		
In Pulse Output mode, the selected digital output channel will generate a square		
High wave as specified in the pulse mode parameters. The high level widths are	e 10	
specified here.		
Input from 1 to 30000 ms.		
Available when enable Pulse in Alarm On Action/Alarm Off Action.	0	
Output The number of pulses, input from 0 to 30000. (0 for continuous pulse output)	0	
Available when enable SMS Control in Alarm Source.	N. 11	
SMS Content On Input the SMS content to enable "Alarm On Action" by SMS (70 ASIC II char max).	Null	
Available when enable SMS Control in Alarm Source.	NI	
SMS Content Off Input the SMS content to enable "Alarm Off Action" by SMS. (70 ASIC II char max)	Null	
SMS Content On Input the SMS content, which will be sent after DO was triggered. (70 ASIC II char	NUU	
Reply max).	Null	
SMS Content Off Input the SMS content, which will be sent after DO was recovered. (70 ASIC II char	NUU	
Reply max).	Null	
Phone Group Click to add phone groups.	Null	

*Note:* R3000-4L does not support SMS/Call function, so Call and SMS section will not be displayed on the web page.

### 3.16 Configuration -> USB

This section allows users to set the USB parameters.

**Note**: Users can insert an USB storage device, such as U disk and hard disk, into the router's USB interface. If there is configuration file or firmware of R3000 inside the USB storage devices, R3000 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			
ltem	Description	Default	

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

# 3.17 Configuration -> GPS

This section allows users to set the GPS setting parameters.

0

GPS Setting	GPS Status	Мар	
Enable GPS			
🗹 Enable GPS			
GPS Basic Setting			
🔲 Report To RS2	232		
RS232 Report Typ	pe: N	ÆA GGA+VTG 🛛 🔽	
RS232 Report Int	erval: 1		
GPS Server Setting			
	Index	Server Name	
		Add	
GPS Server			
🗹 Enable			
Report Type:	N	MEA GGA+VTG 🛛 🔽	
Report Interval:	0		
Socket Type:	Т	CP Server 🐱	

GPS Setting @ GPS			
ltem	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	NMEA GGA+VTG	

Close

Apply

Local Port:

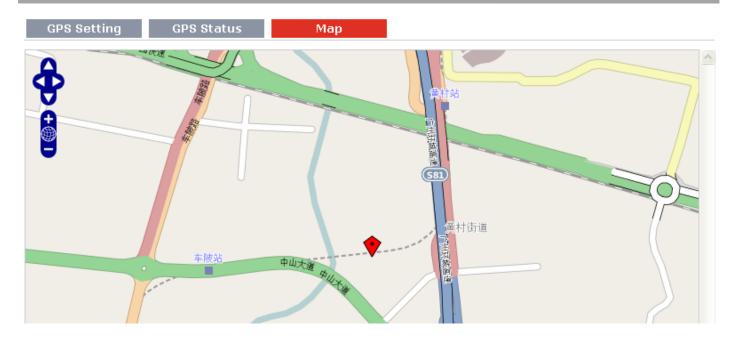
	Made Good and Ground Speed (VTG) + Recommended Minimum Specific	
	GPS/TRANSIT Data (RMC).	
	NMEA RMC: Recommended Minimum Specific GPS/TRANSIT Data (RMC) .	
RS232 Report Interval	Set the interval to report GPS status to RS232 serial port of router.	1
Index @ GPS Server Setting	Show the index of GPS Server.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

This section allows users to check the GPS status.

GPS Setting	GPS Status	Мар
GPS Status		
GPS Status:	Disabled	
Satellites In Use:	0	
Satellites In View:	0	
UTC:		
Latitude:	0.0	
Longitude:	0.0	
Altitude:	0.0	
Speed:	0.0KMH	

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

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



# 3.18 Configuration -> NAT/DMZ

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

Port Forwardi	ng DMZ				
Port Forwarding	9				
Description	Remote IP	Arrives At Port	Is Forwarded to IP Address	Is Forwarded to Port	Protocol
*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		Add
*Arrives At Port:	<1-65535> or <1	-65535>-<1-6553	35>		

Port Forwarding @ NAT/DMZ				
Itom	Description			
ltem	Description	t		
Port Forwarding	Manually defining a rule in the router to send all data received on some range	Null		
Port Forwarding	of ports on the internet side to a port and IP address on the LAN side.	NUII		
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	The device's IP on the LAN side which you want to forward the data to.	Null		
Address	The device's ip on the LAN side which you want to forward the data to.	NUII		
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.	ТСР		

Port Forwarding	DMZ
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	Null		
DIVIZ	those ports otherwise forwarded.	Null		
Enable DMZ	Select to enable the DMZ function.	Enable		
DMZ Host	Enter the IP address of the DMZ host which on the internal network.	0.0.0.0		
Source Address	Set the address which can talk to the DMZ host. Null means for any addresses.	0.0.0.0		

# 3.19 Configuration -> Firewall

This section allows users to set the firewall parameters.

Basic	Filtering	MAC-Binding
Filter Basic Settings		
🗵 Remote Acces	s Using HTTP	
🗵 Remote Acces	s Using TELNET	
Remote Acces	s Using SNMP	
🗷 Remote Ping F	Request	
🗹 Defend DoS A	ttack	

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

network resource unavailable to its intended users.						
Basi	с	Filtering	MAC-Binding			
)efault Filt	er Policy					
Acce	pt	Drop				
Add Filter L	.ist					
Action	Description	Source IP	Source Port	Target IP Address	Target Port	Protocol
*IP: 1.1.1.1	1, 1.1.1.0/24,	1.1.1.1-2.2.2.2, 0.0.	.0.0 means any			Add
*Port: <1-6	55535> or <1-	-65535>-<1-65535:	>			

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

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

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

Basic	Filtering	MAC-Bindin	9	
MAC-IP Binding List				
Des	scription	MAC Address	IP Address	
*MAC: ff:f	ff:ff:ff:ff		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	

### 3.20 Configuration -> QoS

This section allows users to set the QoS parameters.

QoS	
Enable Quality Of Service(	QoS)
🗹 Enable QoS	
Quality of Service(Qos) B	sic Setting
Downlink Speed (kbps):	0
Uplink Speed (kbps):	0
Optimize for TCP Flags:	SYN ACK FIN RST
Default Priority:	Exempt 🔽
🔲 Optimize for Serial D	ata Forwarding
Optimize for ICMP	
QoS MAC Control List	
MAC Address	Priority
	Add
QoS IP Control List	
IP Address	Priority
	Add
QoS Service Control List	
Service Name	Protocol Port Priority
	Add

	QoS	
Item	Description	Default

Enable QoS	Click to enable "QoS" function.	Disable	
Downlink Speed	Prescribe downlink speed of router.		
(kbps)	<i>Note</i> : Default setting"0" means that there is no limitation of downlink speed.		
	Prescribe uplink speed of router.		
uplink Speed (kbps)	<i>Note</i> : Default setting"0" means that there is no limitation of uplink speed.	0	
	User can choose to enable TCP flags: "SYN", "ACK", "FIN", "RST", which means		
Ontimize for TCD Flags	data with above TCP Flags will get the highest priority to occupy bandwidth. After	Disable	
Optimize for TCP Flags	enabled, router will enhance respond timeout of TCP control, in case that data	Disable	
	resend frequently.		
	Select from "Exempt", "Premium", "Express", "Normal" and "Bulk". Users		
	(Services) with no other pre-priority set will use this default priority.		
	Exempt: this is the highest priority which guarantees that the minimum global		
	rate of router is 50% of "Downlink Speed", and the maximum rate can reach to		
	100% of "Downlink Speed".		
	Premium: guarantees that the minimum global rate of router is 25% of "Downlink		
Default Priority	Speed", and the maximum rate can reach to 100% of "Downlink Speed".	Normal	
	Express: guarantees that the minimum global rate of router is 15% of "Downlink		
	Speed", and the maximum rate can reach to 100% of "Downlink Speed".		
	Normal: guarantees that the minimum global rate of router is 10% of "Downlink		
	Speed", and the maximum rate can reach to 100% of "Downlink Speed".		
	Bulk: guarantees that the minimum global rate of router is 1% of "Downlink		
	Speed", and the maximum rate can reach to 100% of "Downlink Speed".		
	Enable to optimize for serial data forwarding, which means serial data forwarding		
Ontimiza for Sorial	will get the highest priority to occupy bandwidth.		
Optimize for Serial Data Forwarding	When enable serial data forwarding it need to enable local port number for	Disable	
Data FOI wai ullig	controlling. Therefore, it needs to set local port number of router even if router is		
	as TCP Client.		
	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.		
Optimize for ICMP	Note: if user click to enable "Optimize for TCP Flags", "Optimize for Serial Data	Disable	
	Forwarding", and "Optimize for ICMP" at the same time (these three services are	Disable	
	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.		
MAC Address @ QoS	Enter MAC address of the user (for example, PC) who you want to set it with QoS		
MAC Address @ Q03	Control. Router supports up to 20 users set with QoS MAC Control. Priority of	Null	
	QoS MAC Control is higher than that of QoS IP control.		
	Select from "Exempt", "Premium", "Express", "Normal" and "Bulk".		
Driarity @ Oas MAC	Select the priority of the user (for example, PC) who you want to set it with QoS		
Priority @ QoS MAC Control List	Control.	Exempt	
Control List	Exempt: this is the highest priority which guarantees that the minimum global	ıl 🔤	
	rate of router is 50% of "Downlink Speed", and the maximum rate can reach to		

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

i.

	Speed", and the maximum rate can reach to 100% of "Downlink Speed".	
	Normal: guarantees that the minimum global rate of router is 10% of "Downlink	
	Speed", and the maximum rate can reach to 100% of "Downlink Speed".	
	Bulk: guarantees that the minimum global rate of router is 1% of "Downlink	
	Speed", and the maximum rate can reach to 100% of "Downlink Speed".	
Note: If services are in	the same priority level, router will automatically start Stochastic Fairness Queueir	ng (SFQ)

strategy to make a fair bandwidth allocation.

### 3.21 Configuration -> IP Routing

This section allows users to set the IP routing parameters.

Static	Route	RIP	OSPF	
Static Ro	oute Table			
	Interface	Destination	NetMask	Gateway
				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".		
Destination	Enter the destination host's IP address or destination network.	Null	
Netmask	Enter the Netmask of the destination or destination network.		
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	I				
🗷 Enable RI	P Protocol Setting	l i i i i i i i i i i i i i i i i i i i			
RIP Protocol Ve	rsion				
RIPv1		RIPv2			
RIP Protocol con	nmon Settings				
Neighbor IP:					
Update time(	s):	30			
Timeout(s):		180			
Garbage(s):		120			
RIP protocol Adv	RIP protocol Advance Setting				
🔲 Enable Ac	lvance				
Network List					
N	etwork Address	NetMask			
		Add			

RIP @ IP Routing			
Item	Description           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.		
RIP			
Enable RIP Protocol Setting	Tick to enable RIP function.	Disable	
<b>RIP Protocol Version</b>	Select from "RIPv1" and "RIPv2".	RIPv1	
Neighbor IP	If you input this neighbor IP, router will only send RIP request massage to this IP instead of broadcast. This item only needs to be set in some unicast network.		
Update times	Defines the interval between routing updates.		
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.		
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.		
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".	None	

	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.	
Enable Default	Enable to make router send the default route to the other routers which in the	Disable
Origination	same IGP AS.	
Enable Redistribute		
Connect	Redistribute connected routes into the RIP tables.	
Enable Redistribute		
Static	Redistributes routing information from static route entries into the RIP tables.	Disable
Enable Redistribute	Padistributes routing information from OCDE route entries into the DID tables	Disable
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	Null	
	protocols, operating within a single autonomous system (AS).		
Enable OSPFv2	Tick to enable OSPF function.	Disable	

### **3.22** Configuration -> DynDNS

This section allows users to set the DynDNS parameters.

DynDNS	
DynDNS Settings	
Enable DynDNS	
Service Type:	DynDNS-Dynamic 💌
Hostname:	
Username:	
Password:	
	Force Update
DynDNS Status: DynDNS	S is initializing

DynDNS				
Item	Description	Default		
	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			
DupDNS	hosting servers via your connection, so that anyone wishing to connect	Null		
DynDNS	to you may use your domain name, rather than having to use your	Null		
	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.			
Enable DynDNS	Tick to enable DynDNS function.	Disable		
	Select the DDNS service from "DynDNS–Dynamic", "QDNS (3322)" and			
Service Type	"NOIP" which you have established an account with. "Custom" could	DynDNS–Dynamic		
	be used for linking custom DDNS server.			
hoastmen	Enter the Host name the DDNS server provided.	Null		
Username	Enter the user name the DDNS server provided.	Null		
Password	Enter the password the DDNS server provided.	Null		
URL	Enter the connection address of custom DDNS server.	Null		
Force Update	Click to the update and use the DynDNS settings.	Null		
DynDNS Status	Show current status of DynDNS	Null		

### 3.23 Configuration -> IPSec

This section allows users to set the IPSec parameters.

IPsec Basic	IPsec Tunnel	X.509	
IPsec Basic			
🗵 Enable NAT Tr	aversal		
Keepalive Interva	al(s): 30		

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.					
Keepalive Interval	The interval that router sends keepalive packets to NAT box so that to avoid it to remove the NAT mapping.	30				

Psec B	Basic IPsec Tuni	nel X.509				
sec Tunnel						
	Tunnel name	Des	scription			
	Common					
	Gateway Address:					
IPsec Mode:		Tunnel 💌				
IPsec Protocol:		ESP 🔽				
Local Subnet:						
Local Subnet Mask:						
Local ID Type:		Default 💌				
Remot	te Subnet:					
Remot	te Subnet Mask:					
Remot	te ID Type:	Default 💌				
ΙΚΕ Ρ	arameter					
Negot	tiation Mode:	Main 🔽				
Encry	ption Algorithm:	AES256 🔽				
Authe	entication Algorithm:	MD5 🔽				
DH Gr	oup:	MODP1024_2 💌				
Authe	entication:	PSK	~			
Secret	ts:					
Life Ti	ime(s):	3600				
		L				
SA Pa	arameter					
SA Alg	gorithm:	3DES_SHA1_96	*			
PFS G	iroup:	PFS_NULL 🔽				
Life Ti	ime(s):	28800				
DPD T	ime Interval (s):	60				
DPD Timeout (s):		180				

IPsec Advanced		
Enable Compress		
Enable ICMP Detection		
ICMP Detection Server:		
ICMP Detection Local IP:		
ICMP Detection Interval (s):	30	
ICMP Detection Timeout (s):	5	
ICMP Detection Retries:	3	

IPSec Tunnel @ IPSec						
Item	Description					
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				
	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.					
IPSec Mode	Transport: Used between end-stations or between an end-station and a	Tunnel				
	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.					
	Select the security protocols from "ESP" and "AH".	565				
IPSec Protocol	ESP: Uses the ESP protocol.	ESP				
	AH: Uses the AH protocol.					
Local Subnet	Enter IPSec Local Protected subnet's address.	0.0.0.0				
Local Subnet Mask	Enter IPSec Local Protected subnet's mask.	0.0.0.0				
	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	Default				
Local ID Type	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					
Remote Subnet	security gateway, e.g., test@robustel.com.	0.0.0.0				
	Enter IPSec Remote Protected subnet's address.					
Remote Subnet Mask	Enter IPSec Remote Protected subnet's mask.	0.0.0.0				
	Select from "IP Address", "FQDN" and "User FQDN" for IKE negotiation.					
Remote ID Type	IP Address: Uses an IP address as the ID in IKE negotiation.	Default				
	FQDN: Uses an FQDN type as the ID in IKE negotiation. If this option is					

		1
	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.	
	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	
Negotiation Mode	dynamically, the IKE negotiation mode must be aggressive. In this case,	Main
	SAs can be established as long as the username and password are	
	correct.	
	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.	
Encryption Algorithm	3DES: Uses the 3DES algorithm in CBC mode and 168-bit key.	3DES
	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.	
	Select from "MD5" and "SHA1" to be used in IKE negotiation.	
Authentication	MD5: Uses HMAC-SHA1.	MD5
Algorithm	SHA1: Uses HMAC-MD5.	
	Select from "MODP768_1", "MODP1024_2" and "MODP1536_5" to be	
	used in key negotiation phase 1.	
DH Group	MODP768_1: Uses the 768-bit Diffie-Hellman group.	MODP1024 2
	MODP1024_2: Uses the 1024-bit Diffie-Hellman group.	_
	MODP1536_5: Uses the 1536-bit Diffie-Hellman group.	
	Select from "PSK", "CA", "XAUTH Init PSK" and "XAUTH Init CA" to be	
	used in IKE negotiation.	
Authentication	PSK: Pre-shared Key.	PSK
	CA: Certification Authority.	
	XAUTH: Extended Authentication to AAA server.	
Secrets	Enter the Pre-shared Key.	Null
	Set the lifetime in IKE negotiation.	
Life Time @ IKE	Before an SA expires, IKE negotiates a new SA. As soon as the new SA is	
Parameter	set up, it takes effect immediately and the old one will be cleared	86400
	automatically when it expires.	
	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";	
SA Algorithm	Select from "AH_MD5_96" and "AH_SHA1_96" when you select "AH"	3DES_MD5_96
	in "Protocol";	
	<b>Note</b> : Higher security means more complex implementation and lower	
	speed. DES is enough to meet general requirements. Use 3DES when	
	speed. Des is enough to meet general requirements. Use SDES WIRT	

	high confidentiality and security are required.	
	Select from "PFS_NULL", "MODP768_1", "MODP1024_2" and	
	"MODP1536_5".	
PFS Group	PFS_NULL: Disable PFS Group	PFS_NULL
	MODP768_1: Uses the 768-bit Diffie-Hellman group.	
	MODP1024_2: Uses the 1024-bit Diffie-Hellman group.	
	MODP1536_5: Uses the 1536-bit Diffie-Hellman group.	
Life Time @ SA	Set the IPSec SA lifetime.	20000
Parameter	<b>Note</b> : When negotiating to set up IPSec SAs, IKE uses the smaller one	28800
	between the lifetime set locally and the lifetime proposed by the peer.	
	Set the interval after which DPD is triggered if no IPSec protected	
	packets is received from the peer.	
	DPD: Dead peer detection. DPD irregularly detects dead IKE peers.	
	When the local end sends an IPSec packet, DPD checks the time the last	
	IPSec packet was received from the peer. If the time exceeds the DPD	
DPD Time Interval	interval, it sends a DPD hello to the peer. If the local end receives no	180
	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.	
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
	Enter the IP address or domain name or remote server. Router will ping	
ICMP Detection	this address/domain name to check that if the current connectivity is	Null
Server	active.	
ICMP Detection Local	Set the local IP address.	Null
IP		
ICMP Detection	Set the ning interval time	30
Interval	Set the ping interval time.	50
ICMP Detection	Set the ning timeout	F
Timeout	Set the ping timeout.	5
ICMP Detection	If Router ping the preset address/domain name time out continuously	2
Retries	for Max Retries time, it will try to re-establish the VPN tunnel.	3

1	(Psec Basic	IPs	sec Tunnel	X.	.509	
Aut	hentication I	Manage				
	Select Cert T	ype:	None	•		
Aut	hentication S	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		
	Click "Browse" to select the correct CA file from your PC, and then click "Import"			
CA	to import it to the router.	Null		
	Click "Export" you can export the CA file from router to your PC.			
	Click "Browse" to select the correct Remote Public Key file from your PC, and			
Remote Public Key	then click "Import" to import it to the router.	Null		
	Click "Export" you can export the Remote Public Key file from router to your PC.			
	Click "Browse" to select the correct Local Public Key file from your PC, and then			
Local Public Key	click "Import" to import it to the router.	Null		
	Click "Export" you can export the Local Public Key file from router to your PC.			
	Click "Browse" to select the correct Local Private Key file from your PC, and then			
Local Private Key	click "Import" to import it to the router.	Null		
	Click "Export" you can export the Local Private Key file from router to your PC.			
	Click "Browse" to select the correct CRL file from your PC, and then click "Import"			
CRL	to import it to the router.	Null		
	Click "Export" you can export the CRL file from router to your PC.			
Authentication Status	Show current status parameters of IPSec.	Null		

## 3.24 Configuration -> Open VPN

This section allows users to set the Open VPN parameters.

Clien	it Server	<b>X.509</b>	
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		
	Select from "tun" and "tap" which are two different kinds of device interface for OpenVPN.			
Interface	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 will be disguised before accessing the remote OpenVPN server.	Disable		

	I	1
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
	Select from "BF-CBC", "DES-CBC", "DES-EDE3-CBC", "AES128-CBC",	
	"AES192-CBC" and "AES256-CBC". BF-CBC: Uses the BF algorithm in CBC mode and 128-bit key.	
Fromution	DES-CBC: Uses the DES algorithm in CBC mode and 64-bit key.	BF-CBC
Encryption	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.	
NATU	Maximum Transmission Unit. It is the identifier of the maximum size of packet,	
MTU	which is possible to transfer in a given environment.	1500
Max Frame Size	Set the Max Frame Size for transmission.	1500
	Select the log output level which from low to high: "ERR", "WARNING", "NOTICE"	500
Verbose Level	and "DEBUG". The higher level will output more log information.	ERR
	You can enter some other PPP initialization strings in this field. Each string can be	NUU
Expert Options	separated by a space.	Null
Subnet&Subnet	Cat the automatic adjacement Marsh of Land up the	Null
Mask@Local Route	Set the subnet and subnet Mask of local route.	

Client

X.509

#### Enable OpenVPN Server

Enable OpenVPN Server

Server

VPN Server Tunnel	
Tunnel name:	OpenVPN_Tunnel_0
Listen IP:	
Protocol:	
Port:	1194
Interface:	tun 💌
Authentication:	None
Local IP:	10.8.0.1
Remote IP:	10.8.0.2
Enable NAT	
Ping Interval:	20
Ping-Restart:	120
Compression:	LZO 💌
Encryption:	BF-CBC
MTU:	1500
Max Frame Size:	1500
Verbose Level:	ERR 💌
Expert Options:	
	*xx xx.parameter,eg:config xx.config

#### **Client Manage**

Use	Common Name	Password	Client IP	Local Static Route	Remote Static Route

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

	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 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	<ul> <li>Select from "BF-CBC", "DES-CBC", "DES-EDE3-CBC", "AES128-CBC", "AES192-CBC" and "AES256-CBC".</li> <li>BF-CBC: Uses the BF algorithm in CBC mode and 128-bit key.</li> <li>DES-CBC: Uses the DES algorithm in CBC mode and 64-bit key.</li> <li>DES-EDE3-CBC: Uses the 3DES algorithm in CBC mode and 192-bit key.</li> <li>AES128-CBC: Uses the AES algorithm in CBC mode and 128-bit key.</li> <li>AES128-CBC: Uses the AES algorithm in CBC mode and 192-bit key.</li> <li>AES128-CBC: Uses the AES algorithm in CBC mode and 192-bit key.</li> </ul>	BF-CBC
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1500
Max Frame Size	Set the Max Frame Size for transmission.	1500
Verbose Level	Select the log output level which from low to high: "ERR", "WARNING", "NOTICE" and "DEBUG". The higher level will output more log information.	ERR
Expert Options	rt Options You can enter some other PPP initialization strings in this field. Each string can be separated by a space.	
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	Authentication Manage							
Select Cert Type: None -								
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	
	Click "Browse" to select the correct CA file from your PC, and then click "Import"		
СА	to import it to the router.	Null	
	Click "Export" you can export the CA file from router to your PC.		
	Click "Browse" to select the correct Public Key file from your PC, and then click		
Public Key	"Import" to import it to the router.	Null	
	Click "Export" you can export the Public Key A file from router to your PC.		
	Click "Browse" to select the correct Private Key file from your PC, and then click		
Private Key	"Import" to import it to the router.	Null	
	Click "Export" you can export the Private Key file from router to your PC.		
	Click "Browse" to select the correct DH A file from your PC, and then click		
DH	"Import" to import it to the router.	Null	
	Click "Export" you can export the DH file from router to your PC.		
	Click "Browse" to select the correct TA file from your PC, and then click "Import"		
ТА	to import it to the router.	Null	
	Click "Export" you can export the TA file from router to your PC.		
	Click "Browse" to select the correct CRL file from your PC, and then click "Import"		
CRL	to import it to the router.	Null	
	Click "Export" you can export the CRL file from router to your PC.		
	Click "Browse" to select the correct Pre-Share Static Key file from your PC, and		
Pre-Share Static Key	then click "Import" to import it to the router.	Null	
	Click "Export" you can export the Pre-Share Static Key file from router to your PC.		

# **3.25** Configuration -> GRE

This section allows users to set the GRE parameters.

GRI	E		
GRE			
	Tunnel name	Description	
GRE			
🗹 Ena	able		
Remote	e IP Address:		
Local V	/irtual IP:		
	e Virtual IP:		
	e Subnet: e Subnet Mask:		
	traffic via this interface		
	able NAT		
Secrets	s:		

	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	Disable		
Ellable	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	Null		
Remote Subnet	known to the local network.	NUII		
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 will be	Disable		
	disguised before accessing the remote GRE server.	Disable		
Secrets	Set Tunnel Key of GRE.	Null		

# **3.26** Configuration -> L2TP

This section allows users to set the L2TP parameters.

L2TP Client L2TP Server				
L2TP Client				
Tunnel name	Description			
		Add		
L2TP Client				
Remote IP Address:				
Username:				
Password:				
Authentication:	Auto 🔻			
Enable NAT	Enable NAT			
All traffic via this interface				
Enable Tunnel Authentication	n			
Tunnel secret:				
Show Advanced				
Port:	1701			
Local IP:				
Remote IP:				
Address/Control Compression	on			
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	Disable	

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

<ul> <li>Enable L2TP Server</li> <li>2TP Common Settings</li> <li>Username: Password: Authentication:</li> <li>In Enable Tunnel Auther Tunnel secret: Local IP: IP Pool Start: IP Pool Start: IP Pool End:</li> <li>2TP Server Advanced</li> <li>Show L2TP Server Adva</li> </ul>	Auto		
Username: Password: Authentication: C Enable Tunnel Auther Tunnel secret: Local IP: IP Pool Start: IP Pool End: 2TP Server Advanced	10.0.2		
Password: Authentication: C Enable Tunnel Auther Tunnel secret: Local IP: IP Pool Start: IP Pool End: 2TP Server Advanced	10.0.2		
Authentication: C Enable Tunnel Auther Tunnel secret: Local IP: IP Pool Start: IP Pool End: 2TP Server Advanced	10.0.2		
<ul> <li>Enable Tunnel Auther Tunnel secret: Local IP: IP Pool Start: IP Pool End:</li> <li>2TP Server Advanced</li> </ul>	10.0.2		
Tunnel secret: Local IP: IP Pool Start: IP Pool End: 2TP Server Advanced	10.0.0.2		
Local IP: IP Pool Start: IP Pool End: 2TP Server Advanced			
IP Pool Start: IP Pool End: 2TP Server Advanced			
IP Pool End: 2TP Server Advanced			
2TP Server Advanced	10.0.0.100		
Show L2TP Server Adva			
	anced		
🗹 Address/Control Compr	ression		
Protocol Field Compres			
Asyncmap Value:	fffffff		
MRU:	1500		
MTU:	1436		
Link Detection Interval (s):	: 30		
Link Detection Max Retries	: 5		
Expert Options:	noccp nobsdcomp		
oute Table List	L		

*0.0.0.0"	means any

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	
	Select from "PAP", "CHAP", "MS-CHAP v1" and "MS-CHAP v2".		
Authentication	L2TP client need to select the same authentication method based on this	СНАР	
	server's authentication method.		
Enable Tunnel	Tick to enable tunnel authentication and enter the tunnel secret which will	Disable	
Authentication	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	

Add

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

# **3.27** Configuration -> PPTP

This section allows users to set the PPTP parameters.

PPTP Cl	ient PPTP Serv	/er	
PPTP Client	t		
	Tunnel name	Description	
			Add

PPTP Client	
Enable	
Remote IP Address:	
Username:	
Password:	
Authentication:	Auto 👻
🗹 Enable NAT	
Enable MPPE	
All traffic via this interface	
Show Advanced	
Local IP:	
Remote IP:	
Address/Control Compressi	on
Protocol Field Compression	
Asyncmap Value:	ffffffff
MRU:	1500
MTU:	1436
Link Detection Interval (s):	30
Link Detection Max Retries:	5
Expert Options:	noccp nobsdcomp

PPTP Client @ PPTP				
Item	Description			
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.			
Enable NAT	Click to enable NAT feature of PPTP. The source IP address of host Behind R3000 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	Show Advanced Tick to enable the PPTP client advanced setting.			

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

PPTP Client

PPTP Server

#### Enable PPTP Server

Enable PPTP Server

#### PPTP Common Settings

-	
Username:	
Password:	
Authentication:	CHAP -
Local IP:	10.0.1
IP Pool Start:	10.0.2
IP Pool End:	10.0.100
Enable MPPE	

PTP Server Advanced			
🗹 Show PPTP Server Advanc	ed		
Address/Control Compres	sion		
🗹 Protocol Field Compression	n		
Asyncmap Value:	fffffff		
MRU:	1500		
MTU:	1436		
Link Detection Interval (s):	30		
Link Detection Max Retries:	5		
Expert Options:	noccp nobsdcomp		
oute Table List			
Client IP	Remote Subnet	Remote Subnet Mask	
*0.0.0.0" means any	•	Add	
Route Table List			
Client IP	Remote Subnet	Remote Subnet Mask	
("0.0.0.0" means an	y)	Add	

	PPTP Server @ PPTP
Item	Description
Enable PPTP Server	Tick to enable PPTP server.
Username	Set the username which will assign to PPTP client.
Password	Set the password which will assign to PPTP client.
	Select from "PAP", "CHAP", "MS-CHAP v1" and "MS-CHAP v2".
Authentication	PPTP client need to select the same authentication method based on thi
	server's authentication method.
Local IP	Set the IP address of PPTP server.
IP Pool Start	Set the IP pool start IP address which will assign to the PPTP clients.
IP Pool End	Set the IP pool end IP address which will assign to the PPTP clients.

Password	vord Set the password which will assign to PPTP client.			
	Select from "PAP", "CHAP", "MS-CHAP v1" and "MS-CHAP v2".			
Authentication	PPTP client need to select the same authentication method based on this			
	server's authentication method.			
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		
	Tick to enable MPPE (Microsoft Point-to-Point Encryption). It's a protocol for			
Enable MPPE	encrypting data across PPP and VPN links.			
Show PPTP Server	Tick to show the DDTD conver advanced setting	Disable		
Advanced	Tick to show the PPTP server advanced setting.	DISADIE		
Address/Control	Used for PPP initialization. In general, you need to enable it as default.	Enable		
Compression	Osed for PPP initialization. In general, you need to enable it as default.	Enable		
Protocol Field	Used for PPP initialization. In general, you need to enable it as default.	Enable		
Compression	Osed for PPP initialization. In general, you need to enable it as default.	Enable		
Asyncman Value	One of the PPTP initialization strings. In general, you don't need to modify			
Asyncmap Value	this value.			
MDU	Maximum Receiving Unit. It is the identifier of the maximum size of packet, which is possible to receive in a given environment.			
MRU				

Default Disable Null

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

# 3.28 Configuration -> SNMP

This section allows users to set the SNMP parameters.

Basic	View	VACM	Trap	
SNMP Basic Setting	5			
🕅 Enable SNMP				
Port:	161			
Agent Mode:	Maste	r 🔻		
Version:	SNMPv	2 🔻		
Location Info:	China			
Contact Info:	info@	robustel.com		
System Name:	route	r		

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	

#### Robustel GoRugged R3000 User Guide

Basic	View		VACM		Trap
b View List					
View Na	ame	View Filter		View OID	
syste	m	Include	-	1.3.6.1.2.1.	1 <b>X</b>
all		Include	-	1	x
*View OID:<1	~65535>.<1~65	535>		A	dd

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	
MPv1&v2 U	ser List				
Re	adwrite	Network	Community	MIBview	
Rea	donly 💌		public	system	<b>▼ X</b>
Read	dWrite 💌		private	system	<b>▼</b> X
Read	dWrite 💌		admin	all	<b>▼</b> X
*Netwo	rk: 1.1.1.0/2	24, 0.0.0.0 means	s any	(	Add

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

Basic	View	VACM	Тгар	
SNMP Trap Settings				
Enable SNMP Tra	эр			
Version:	SNMPv1	•		
Server Address:				
Port:	0			
Name:				

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

#### 3.29 Configuration -> VRRP

This section allows users to set the VRRP parameters.

VRRP		
/RRP Settings		
Enable VRRP		
Group ID:	1	
Priority:	100	
Interval (s):	10	
Virtual IP:	192.168.0.1	

	VRRP				
Item	Description	Default			
	Tick to enable VRRP protocol. VRRP (Virtual Router Redundancy Protocol) is				
Enable VRRP	an Internet protocol that provides a way to have one or more backup routers	Disable			
	when using a statically configured router on a local area network (LAN). Using	DISADIE			
	VRRP, a virtual IP address can be specified manually.				
Group ID	Specify which VRRP group of this router belong to.				
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			
	A virtual IP address is shared among the routers, with one designated as the				
Virtual IP	master router and the others as backups. In case the master fails, the virtual				
VIILUALIP	IP address is mapped to a backup router's IP address. (This backup becomes	1			
	the master router.)				

## **3.30** Configuration -> IP Passthrough

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

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

#### IP Passthrough

P Passthrough Settings	
🗵 Enable IP Passthrough	
Mode:	PPPoE 🔻
Ethernet Interface:	LAN_0 -
Username:	
Password:	
AC Name:	
Service Name:	
Authentication:	Auto 🔻
Link Detection Interval(s):	30
Link Detection Max Retries:	5

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

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

## 3.31 Configuration -> AT over IP

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

AT over IP	
AT Settings	
Enable AT Settings	
Protocol:	UDP -
Local IP:	
Local Port:	8091

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

## **3.32** Configuration -> Phone Book

This section allows users to set the Phone Book parameters.

Phone E	look	Phone Gro	ир					
Phone Book	c Configu	ration						
	Des	scription	Phone No.					
				x				
				dd				
			stination number i		-			-
+123423	42342 (+1	1 is the internat	ional code for US,	use this and th	hen your norma	al number w	ithout the firs	t zero).
*2. In sor	ne countri	ies, only can sei	nd/receive SMS wi	thout internation	onal code for th	ne number.		

Phone Book			
Item	Description	Default	

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

Phone E	BOOK Phone G	roup
Phone Grou	up Configuration	
	Group Name	Phone List
		Add
Curry No		
Group No	o. And Description	
Group	p Name:	
Add or re	emove the phone no	o. to/from group
N	ot in this group	In this group
		All
		<b>*</b>

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

*Note:* R3000-4L does not support SMS/Call function, so PhoneBook section will not be displayed on the web page.

## 3.33 Configuration -> SMS

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

SMS	
SMS Notification	
Send SMS on power up	
Send SMS on PPP conn	ect
Send SMS on PPP disco	nnect
Phone Group:	NULL  Click to add PhoneGroup!
SMS Control	
🕅 Enable	
Password Content:	
Phone Group:	NULL  VULL  VULL

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

**Note**: please refer to section 4.7 SMS Commands for Remote Control. R3000-4L does not support SMS/Call function, SMS section will not be displayed on the web page.

#### 3.34 Configuration -> Reboot

This section allows users to set the Reboot policies.

SMS Reply Content:

Time	Call	SMS
Daily Reboot		
🗵 Enable Time Reboot(	hh:mm,24h)	
Reboot Time1	Reboot Time2	Reboot Time3
12:00		
Time	Call	SMS
Call Reboot Configuration		
🖉 Enable Call Reboot		
Phone Group:	NULL - Clin	ck to add PhoneGroup!
SMS Reply Content:		
Time	Call	SMS
SMS Reboot Configuration		
Enable SMS Reboot		
Phone Group:	NULL - Clic	ck to add PhoneGroup!
Password:		

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

**Note:** R3000-4L does not support SMS/Call function, Call and SMS section will not be displayed on the web page.

#### 3.35 Configuration -> RobustLink

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

RobustLink		
RobustLink Setting	5	
🗵 Enable Robu	stLink	
Server Address:		
Port:	188	83
Password:		

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

#### **3.36 Configuration -> Syslog**

This section allows users to set the syslog parameters.

Syslog	
Syslog Settings	
Save Position:	RAM 💌
Log Level:	DEBUG 👻
Keep Days:	14
🕅 Log to Remot	te System
Remote IP:	
Remote UDP Port	t: 514

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"	DEBUG	

	and "EMERG" which from low to high. The lower level will output more syslog in detail.	
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	Disable
	enter the IP and Port of the syslog server.	

# 3.37 Configuration -> Event

This section allows users to set the Event parameters.

	Event			
/ent	t Setting	5		
1	Enable	Event		
	Index	Event Code	SNMP-TRAP	RobustLink
	1	BOOT-UP		
	2	3G-UP		
	3	3G-DOWN		
	4	GPRS-UP		
	5	GPRS-DOWN		
	6	OVPN1-UP		
	7	OVPN2-UP		
	8	OVPN3-UP		
	9	OVPN1-DOWN		
	10	OVPN2-DOWN		
	11	OVPN3-DOWN		
	12	INT1-UP		
	13	INT2-UP		
	1			

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

#### 3.38 Configuration -> USR LED

This section allows users to change the display status of USR LED. **Note:** Please refer to "Status" -> "System" -> "LEDs Information" -> "USR".

USR LED	
USR LED	
USR LED Type:	VPN -
Indication:	ON 💌

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

#### 3.39 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 V	
Copy settings from	current profile to selected profile	
Change		
All Parameters XML Conf	figuration	
XML File:	Browse Import Export	
IPsec XML Configuration		
IPsec XML File:	Browse Import Export	
OpenVPN XML Configura	tion	
OpenVPN XML File:	Browse Import Export	
Restore to Factory Defau	ılt Settings	
Restore to Factory Defa	ault 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 configuration data backup. Selected from "Standard", "Alternative 1", "Alternative 2", "Alternative 3".		Standard
	Selected from Standard , Alternative I , Alternative 2 , Alternative 3 . Import: Click "Browse" to select the XML file in your computer, then click "Import" to import this file into your router.	
XML Configuration	Export: Click "Export" and the configuration will be showed in the new popup browser window, then you can save it as a XML file.	Null
Restore to Factory Default Settings	Click the button of "Restore to Factory Default Settings" to restore the router to factory default setting.	Null

## 3.40 Administration -> Tools

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

Ping IP address: Number of requests: 5 Timeout (s): 1 Local IP:	Ping A	T Debug	Traceroute	Sniffer	Test
Number of requests:     5       imeout (s):     1       .ocal IP:	g				
imeout (s): 1	Ping IP address:				
ocal IP:	Number of requests:	5			
	Timeout (s):	1			
	Local IP: Start Stop				

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

nd	nd	art Commands and e AT Commands	Ping	AT Debug	Traceroute	Sniffer	Test
-95 -95	-95 -95		AT Command	ls			
	-95 -95						
	-95 -95		Sand				
			e en	ande			

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

Ping	AT Debug	Traceroute	Sniffer	Test	-
ceroute					
Trace Address:					
Trace Hops:	30				
Timeout (s):	1				
Start Stop					
NAME AND A					

	Traceroute @ Tools	
Item	Description	Default

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

Ping	AT Debug	Traceroute	Sniffer	Test	
ff <mark>er</mark>					
Interface: Host: Protocol: Start Stop	all •				

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

#### Robustel GoRugged R3000 User Guide

Enable	Description	Result	
	USB Test		
	Flash Test		
	Memory Test		
	Ethernet Test		
	SIM1 Test		
	SIM2 Test		
	Module Test		

	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	<ul> <li>Show the current status of the selected hardware component. There are 3 status "Testing", "Success" and "Failure".</li> <li>Testing: Router is testing the selected hardware component.</li> <li>Success: Correspond hardware component is properly inserted and detected.</li> <li>Failure: Correspond hardware component is not inserted into the router or the router fails to detect.</li> </ul>	Null
Show Detail	Show the current test details of the hardware component.	Null
Note: click "Apply" to sto	art testing.	

# 3.41 Administration -> Clock

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

eal Time Clock Settings	
Real Time Clock:	2007-01-10 08:36:32
PC Time:	2013-11-20 17:15:59 Synchronize
imezone Setting	
Timezone:	UTC+08:00 China, HK, Western Australia, Singapore, Taiwan, Russia 💌
TP Settings	
TP Settings          Image: Setting sett	
_	pool.ntp.org
	pool.ntp.org

	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
Timozona @ Cliant	Select your local time zone	UTC
Timezone @ Client	Select your local time zone.	
Primary NTP Server	Enter primary NTP Server's IP address or domain name.	pool.nt
Filling NTF Server	Enter primary wire server's readdress of domain name.	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
Timozono @ Convor	Coloct your local time zono	UTC
Timezone @ Server	Select your local time zone.	+08:00

# 3.42 Administration -> Web Server

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

Basic	X.509	
Port Settings		
HTTP Port:	80	
HTTPS Port:	443	

Basic	X.509			
HTTPS Certificate				
Public Key:		Browse	Import	Export
Private Key:		Browse	Import	Export

Basic @ Web Server			
Item	Description	Default	
	Enter the HTTP port number you want to change in R3000's Web Server.		
	On a Web server, port 80 is the port that the server "listens to" or expects to		
HTTP Port	receive from a Web client. If you configure the router with other HTTP Port	80	
	number except 80, only adding that port number then you can login R3000's		
	Web Server.		
	Enter the HTTPS port number you want to change in R3000's Web Server.		
	On a Web server, port 443 is the port that the server "listens to" or expects to		
	receive from a Web client. If you configure the router with other HTTPS Port		
	number except 443, only adding that port number then you can login R3000's		
HTTPS Port	Web Server.	443	
	<b>Note</b> : 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.		
	X.509 @ Web Server	1	
HTTPS Certificate	In this tab, user can import or export "Public Key" and "Private Key" for HTTPS	Null	
	certification.		

# **3.43** Administration -> User Management

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

Super	Common
User Management	
Username:	admin
Old Password:	
New Password:	
Confirm Password	
Login Parameters	
Login Timeout (s):	1800

Super @ User Management			
Item	Description	Default	
Super	One router has only one super user account. Under this account, user has the	Admin	
	highest authority include modify and add management user accounts.		
User Management	Set Username and Password.	Null	
	Specify the login timeout value. You need to re-login after this timeout of user	1900	
Login Timeout	inactively.	1800	

	Super (	Common		
Use	r Management			
	Access Level	Username	Password	
			Add	

Common @ User Management		
Item	Description	Default
Common	One router has at most 9 common user accounts. There are two access level of	N1 11
Common	common user account: "ReadWrite" and "ReadOnly".	Null
	Select from "ReadWrite" and "ReadOnly".	
Access Level	ReadWrite: Users can view and set the configuration of router under this level;	Null
	ReadOnly: Users only can view the configuration of router under this level	
Username/ Password	Set Username and Password.	Null
Add	Click this button to add a new account.	Null

## **3.44** Administration -> SDK Management

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

	АРР	Files		
Impo	Import Applications			
Γ	Browse Import			
Cust	om Applicatio	n List		
	Enabled	APP Name	Options	Memory(KB) Running

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

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

APP	Files	
Import Files		
	Browse Import File	
Costom 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

# 3.45 Administration -> Update Firmware

This section allows users to update the firmware of router.

Update	
Firmware Version	
Firmware Version:	1.01.01-sub-131202
Firmware old Version	
Firmware old Version	1.01.01-sub-131129-1
Fall back to old version	Apply
Update Firmware	
Warning: Do not turn off or ope	erate the Router while updating.
New Firmware:	Browse Update

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

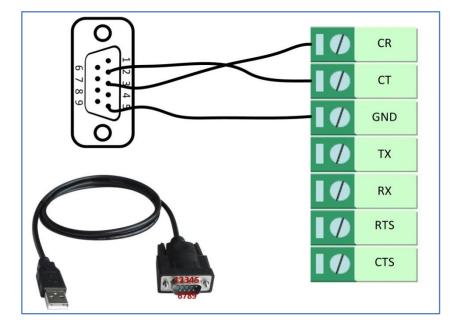
"Update" button" to update. After updating successfully, you need to reboot	
router to take effect.	

# **Chapter 4. Configuration Examples**

# 4.1 Interface

# 4.1.1 Console port

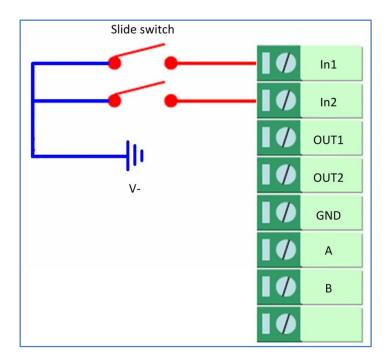
User can use the console port to manage the router via CLI commands, please check section Introductions for CLI.



# 4.1.2 Digital Input

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

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

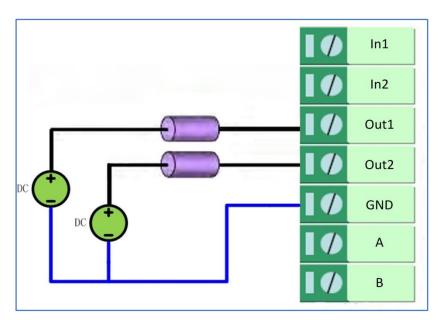


# 4.1.3 Digital Output

There are two digital outputs of R3000. Power negative of DC should connect to "GND"

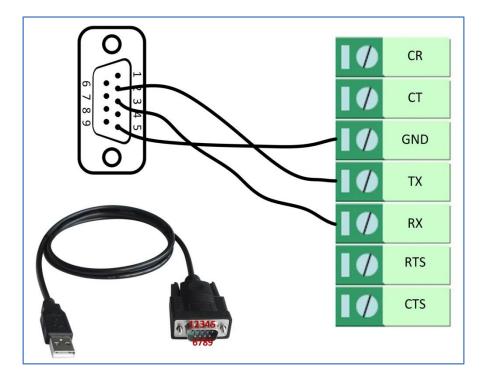
Please refer to connection diagram at the right site.

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



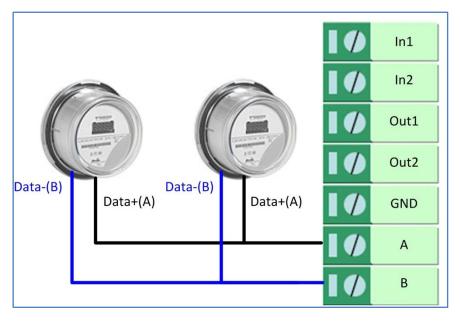
# 4.1.4 RS232

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



# 4.1.5 RS485

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



# 4.2 Cellular

# 4.2.1 Cellular Dial-Up

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

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

#### 1. Always Online

#### Configuration-->Link Management-->Cellular Only

Link Management Settings	
WAN link:	Cellular Only
ICMP Detection Primary Server:	Cellular Only Eth0 Only
ICMP Detection Secondary Server:	Eth0 as primary and if fail use cellular
ICMP Detection Interval (s):	Cellular as primary and if fail use Eth0
ICMP Detection Timeout (s):	3
ICMP Detection Retries:	3
Reset The Interface	

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

#### Configuration --> Cellular WAN --> Basic

Cellular Settings			
	Primary SIM Card	Secondary SIM Card	
Network Provider Type:	Auto 💌	Auto 💌	
APN:			
Username:			
Password:			
Dialup No.:	*99***1#	*99***1#	
PIN code request:	Set PIN Code	Set PIN Code	
Connection Mode			
Connection Mode:	Always online		
Redial Interval (s):	30		
Max Retries:	3		
Dual SIM Policy			
Main SIM Card:	SIM1 💌		

When connection fails

When roaming is detected

When IO is active

Monthly data traffic limitation

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

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

#### 2. Connect on Demand

#### Configuration-->Link Management-->Cellular Only

Link Management Settings	
WAN link:	Cellular Only
ICMP Detection Primary Server:	Cellular Only Eth0 Only
ICMP Detection Secondary Server:	Eth0 as primary and if fail use cellular
ICMP Detection Interval (s):	Cellular as primary and if fail use Eth0
ICMP Detection Timeout (s):	3
ICMP Detection Retries:	3
Reset The Interface	

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

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

#### Configuration-->Cellular WAN -->Basic

Cellular Settings											
			SI	IM1				SIM2			
Status:			Re	eady				Not Read	dy		
Network Provide	er Type	э:	A	uto		•		Auto	•		
APN:											
Username:											
Password:											
Dialup No.:			*9	99***1	#			*99***1	#		
PIN code reque:	st:		S	et PII	∛ Code			Set PIN	[ Code		
Connection Mode											
Connection Mod	le:		С	onnect	t on d	lemand	1 💌				
Redial Interval (	s):		30	D				_			
Max Retries:			3								
Inactivity Time (	s):		0								
Serial Output Co	ontent	:									
Triggered by Serial Data											
Periodically of the second	:onnec	:t									
Periodically con	nect in	terval	(s):30	00							
Time schedule:			s	chedu	le_1 _	•					
Time Range											
Name	SUN	MON	TUE	WED	THU	FRI	SAT	Time Range1	Time Range2	Time Range3	
schedule_1			•	☑	•	~		08:10-12:00	14:10-20:15		x
										Add	

Select the trigger policy you need.

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

# 4.2.2 SMS Remote Status Reading

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

An SMS command has following structure:

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

#### SMS command Explanation:

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

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

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

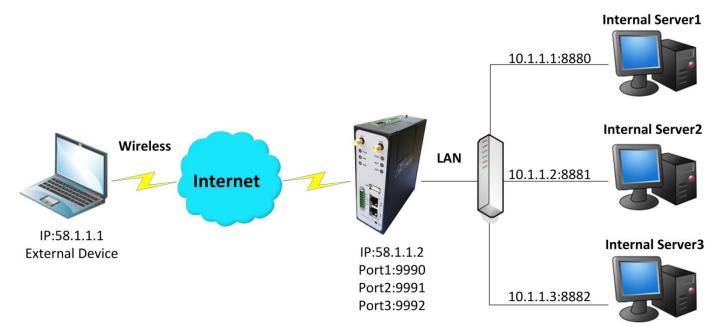
Cmd	Description	Syntax	Comments					
Contro	Control Commands							
0001	Reset Device	cmd	if no password, please use command "cmd", or use command" password: cmd" cmd1 + cmd2: cmd1;cmd2 * - means can be null					
0002	Save Parameters	cmd						
0003	Save Parameters and Reset Device	cmd						
0004	Start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

## 4.3 Network

## 4.3.1 NAT

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

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



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

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

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

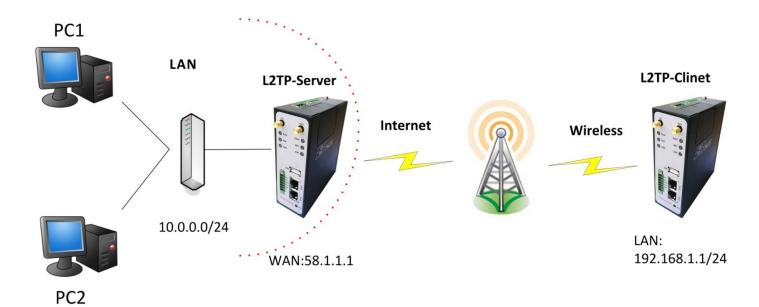
#### Explanations for above diagram:

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

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

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

# 4.3.2 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:	l2tp	1
Password:	••••	2
Authentication:	PAP 💌	3
🗖 Enable Tunnel Authenticati	on	
Local IP:	10.1.2.1	
IP Pool Start:	10.1.2.2	
IP Pool End:	10.1.2.254	
L2TP Server Advanced		
□ Show L2TP Server Advance	d	
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		Add

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

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

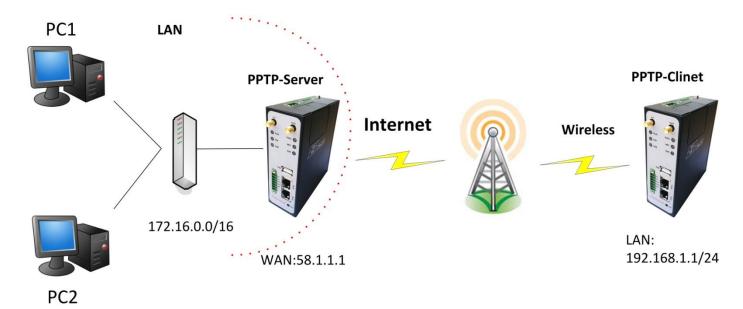
## L2TP\_CLIENT:

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

Please add L2TP Client							
Add							
Click "Add" button, and fill in the	blank textbox						
L2TP Client X							
Enable	O Disable						
Server Name:	58.1.1.1						
Username:	l2tp	1					
Password:	••••	2					
Authentication:	PAP 🔽	3					
🗖 Enable Tunnel Authentica	tion						
Remote Subnet:	10.0.0.0						
Remote Subnet Mask:	255.255.255.0						
Show L2TP Client Advance	ed						

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

## 4.3.3 PPTP



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

## **PPTP\_SERVER:**

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

Enable PPTP Server		
Enable PPTP Server		

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

PPTP Common Settin	igs			
Username:		pptp	1	
Password:		••••	2	
Authentication:		PAP 💌	3	
Local IP:		10.0.0.1		
IP Pool Start:		10.0.0.2		
IP Pool End:		10.0.0.254		
Enable MPPE				
PPTP Server Advance	ed			
□ Show PPTP Se	rver Advanced			
Route Table List				
Cl	ient 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		Add	

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

## **PPTP\_CLIENT:**

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

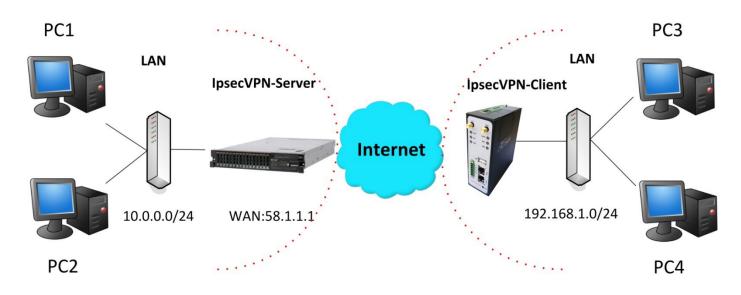
Please add PPTP Client	
Add	

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

PPTP Client X		
Enable	C Disable	
Server Name:	58.1.1.1	
Username:	pptp	1
Password:	••••	2
Authentication:	PAP 💌	3
Remote Subnet:	172.16.0.0	
Remote Subnet Mask:	255.255.0.0	
Enable MPPE		
Show PPTP Client Advance	ced	

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

# 4.3.4 IPSEC VPN



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

## IPsecVPN\_SERVER:

## Cisco 2811:

crypto isakmp policy 10
encriaes 256 🛛 🔗
hash md5 🧳
authentication pre-share 11
group 2 10
crypto isakmp key <mark>cisco</mark> address 0.0.0.0 0.0.0.0
! 12
crypto ipsec transform-set transfesp-3des esp-md5-hmac 🛛 🏼 🎝 🔧 🎝
!
crypto dynamic-map dyn 10
set transform-set trans
match address 101
!
crypto map map1 10 ipsec-isakmp dynamic dyn
!
interface FastEthernet0/0
crypto map map1
!
access-list 101 permit ip 10.0.0.0 0.0.0.255 any 3, 5

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

## IPsecVPN\_CLIENT:

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

IPsec Basic		
Enable NAT Traversal		
Keepalive Interval(s):	30	

#### Then click "Apply".

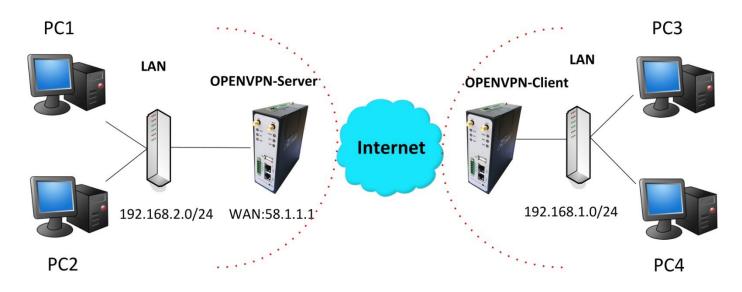
#### Configuration--->IPSec--->IPSec Tunnel

IPsec Tunnel X		
Enable	C Disable	
Tick "Enable IPSec Tunnel1"		
IPsec Common		
Tunnel name:	IPSEC_TUNNEL_1	
IPsec Gateway Address:	58.1.1.1	
IPsec Mode:	Tunnel 💌	1
IPsec Protocol:	ESP 💌	2
Local Subnet:	192.168.1.0	3
Local Subnet Mask:	255.255.255.0	
Local ID Type:	IP Address 💌	4
Remote Subnet:	10.0.0.0	5
Remote Subnet Mask:	255.255.255.0	5
Remote ID Type:	IP Address 💌	6
IKE Parameter		
Negotiation Mode:	Main 💌	7
Encryption Algorithm:	AES256 💌	8
Authentication Algorithm:	MD5 💌	9
DH Group:	MODP1024_2 -	10
Authentication:	PSK 🔻	11
Secrets:	••••	12
Life Time (s):	86400	—

SA Parameter		
SA Algorithm:	3DES_MD5_96	13
PFS Group:	PFS_NULL -	
Life Time(s):	28800	
DPD Time Interval (s):	180	
DPD Timeout (s):	60	
IPsec Advanced		
VPN Over IPsec Type:	NONE -	
Enable Compress		

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

## 4.3.5 OPENVPN



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

#### **OPENVPN\_SERVER:**

#### Configuration--->OpenVPN--->Server

Enable OpenVPN Server	
Enable OpenVPN Server	

Tick "Enable OpenVPN Server".

VPN Server Tunnel	
Tunnel name:	OpenVPN_Tunnel_0
Listen IP:	
Protocol:	
Port:	1194 2
Interface:	tun 💌 🦪
Authentication:	None 🖌 4
Local IP:	10.8.0.1 <b>5</b>
Remote IP:	10.8.0.2 6
Enable NAT 7	
Ping Interval:	20
Ping-Restart:	120
Compression:	LZO 🖌 🛛 🛛 🖁
Encryption:	BF-CBC 👤 🧕
MTU:	1500 10
Max Frame Size:	1500 11
Verbose Level:	ERR
Expert Options:	route 192.168.1.0 255.255.255.0
	*xx xx.parameter,eg:config xx.config

#### **Client Manage**

Use	Common Name	Password	Client IP	Local Static Route	Remote Static Route
*Static R	Route: <1.1.1.0/24>	or <1.1.1.0/24;2.	2.2.2/16>		Add

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	O Disable	
Tunnel name:	OpenVPN_Tunnel_0	
Protocol:	UDP 1	
Server Address:	58.1.1.1	
Port:	1194 2	
Interface:	tun 💌 🦪	
Authentication:	None 4	
Local IP:	10.8.0.2 6	
Remote IP:	10.8.0.1 <b>5</b>	
🗹 Enable NAT 🛛 🌈		
Ping Interval:	20	
Ping-Restart:	120	
Compression:	LZO 💌 🛛 😹	
Encryption:	BF-CBC 9	
MTU:	1500 <b>10</b>	
Max Frame Size:	1500 11	
Verbose Level:	ERR	
Expert Options:	route 192.168.2.0 255.255.255.0	

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

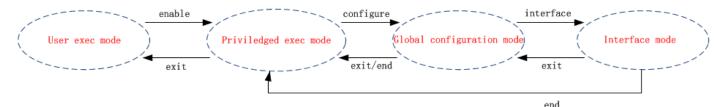
# Chapter 5. Introductions for CLI

# 5.1 What's CLI and hierarchy level Mode

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

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

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



#### USER EXEC MODE:

R3000 Configure Environm	ent
Username: admin	
Password: *****	
R3000>?	//check what commands can be used in user exec mode
enable	Turn on privileged commands
exit	Exit from current mode
ping	Ping test
reload	Halt and perform a cold restart
tracert	Tracert test
show	Show running system information

#### PRIVILEDGED EXEC MODE:

#### R3000> enable

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

#### **GLOBAL CONFIGURATION MODE:**

#### R3000# configure

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

#### INTERFACE MODE:

R3000(config)# interface Ethernet 0

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

# 5.2 How to configure the CLI

Commands /tips	Description	
?	Typing a question mark "?" will show you the help information.	
Ctrluc	Press these two keys at the same time, except its "copy" function but also	
Ctrl+c	can be used for "break" out of the setting program.	
	Parameters "xxx" are not supported by the system, in this case, enter a mark	
Invalid command "xxx"	"?" 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.	

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

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

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

### 5.2.1 QuickStart with configuration examples

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

#### Example 1: Show current version

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

## Example 2: Update firmware via tftp

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

Tftp transfering tftp succeeded!downloaded R3000# write

//save current configuration

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

## Example 3: Set link-management

R3000> enable	
Password: ****	
R3000#	
R3000# configure	
R3000(config)# set link-management	
wan link :	
1.Cellular Only	
2.Eth0 Only	
3.Eth0 as primary and if fail use Cellular	
4.Cellular as primary and if fail user Eth0	
->please select mode(1-4)[1]:2	//select "Eth0 Only" as wan-link
->ICMP detection primary server[]:8.8.8.8	
->ICMP detection second server[]:8.8.8.4	
->ICMP detection interval(3-1800)[30]:	
->ICMP detection timeout(1-10)[3]:	
->ICMP detection retries(1-20)[3]:	
->reset the interface?'yes'or'no'[no]:	
this parameter will be take effect when reboot!	
really want to modify[yes]:	
R3000# write	<pre>//save current configuration</pre>
Building configuration	
ОК	
R3000# reload	
!Reboot the system ?'yes'or 'no':yes	//reload to take effect

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

R3000> enable Password: ***** R3000#		
R3000# show link-managem	ient	//show current link-management
**************************************	:*************************************	*** // now "Eth0 Only" as wan-link
ICMP primary server	: 8.8.8.8	
ICMP second server	: 8.8.8.4	
		17.01.2014

ICMP detection interval ICMP detection timeout ICMP detection retries reset the interface	: 3 seconds : 3 : no	***
R3000 # configure		
R3000 (config) # set eth0		
ethernet interface type: WAI	N	
type select:		
1. Static IP		
2. DHCP		
3. PPPOE		
->please select mode (1-3) [1 ->IP address [192.168.0.1]:58	-	//set IP address for eth0
->Netmask [255.255.255.0]:2		//set if address for etho
->gateway [192.168.0.254]:5		//set gateway for eth0
->mtu value (1024-1500)[150		,,
->input primary DNS [192.168.0.254]:58.1.1.254 //set dns for eth0		
->input secondary DNS [0.0.0	0.0]:	
this parameter will be take e	ffect when reboot!	
really want to modify[yes]:		
R3000 (config) # end		
R3000# write		//save current configuration
Building configuration		
OK R3000 # reload		
! Reboot the system? 'yes' or	'no'' ves	//reload to take effect
incode the system. yes of	110 · yC3	

# Example 5: CLI for Cellular dialup

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

\*\*\*\*\*

wan link	: Cellular Only	// now "Cellular Only" as wan-link
ICMP primary server	: 8.8.8.8	
ICMP second server	: 8.8.8.4	
ICMP detection interval	: 30 seconds	

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

max connect try	: 3	
main SIM select	: SIM_1	
when connect fail	: yes	
when roaming is detected	: no	
month date limitation	: no	
SIM phone number	:	
network select Type	: Auto	
authentication type	: AUTO	
mtu value	: 1500	
mru value	: 1500	
asyncmap value	: Oxffffffff	
use peer DNS	: yes	
primary DNS	: 0.0.0.0	
secondary DNS	: 0.0.0.0	
address/control compression: yes		
protocol field compression	: yes	
expert options	: noccp nobsdcomp	
*****	*******	

```
R3000# reload
!Reboot the system ?'yes'or 'no':yes
```

//reload to take effect

# 5.3 Commands reference

commands	syntax	description
Debug	Debug parameters	Turn on or turn off debug function
Export	Export parameters	Export vpn ca certificates
Import	Import parameters	Import vpn ca cerfiticates
Syslog	syslog	Export log information to tftp server
Load	Load default	Restores default values
Write	Write	Save current configuration parameters
tftp	Tftp IP-address get {cfg rootfs} file-name	Import configuration file or update firmware via tftp
Show	Show parameters	Show current configuration of each function , if we need to see
		all please using "show running "
Set	Sat naramatara	All the function parameters are set by commands set and add,
Add	Set parameters Add parameters	the difference is that set is for the single parameter and add is
		for the list parameter