



Dual SIM Industrial Cellular VPN Router

for GPRS/EDGE/UMTS/HSPA Networks



8E4571 _ 3G Industrial Router VPN Pro

User's Guide
rev. 1.2 07/2017

All rights reserved; no part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, otherwise, without the prior written permission of Digicom S.p.A. The contents of this booklet may be modified without notice. Every possible care has been taken in testing and putting together all the documentation contained in this booklet, however Digicom can not take any responsibility brought by the use of this booklet.

PREFACE

In order to guarantee your safety and a correct functioning, be sure to follow these safety warnings. The whole set (with cables included) must be installed in a place lacking of or distant from:

- Dust, humidity, high temperatures and direct exposure to sunlight.
- Heat irradiating objects, which may damage your device or cause any other problem.
- Objects producing a high electromagnetic field (Hi-Fi speakers, etc.).
- Corrosive liquids or chemical substances.

Any sudden change in temperature and humidity must be avoided.

Use a soft dry cloth and avoid any solvents or abrasive materials.

Caution against shocks or vibrations.

SIMPLIFIED UE DECLARATION OF CONFORMITY

The manufacturer, Digicom S.p.A., declares that this radio equipment **Dual SIM Industrial Cellular VPN Router** is compliant with Directive 2014/53/UE.

The complete text of UE Declaration of Conformity is available at following internet address: www.digicom.it

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. Digicom 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.

SAFETY WARNINGS

Read these instructions and norms carefully before powering the device. Violation of such norms may be illegal and cause hazard situations. For any of the described situations please refer to the specific instructions and norms.

The device is a low power radio transmitter and receiver. When it is ON, it sends and receives radio frequency (RF) signals. The device produces magnetic fields. Do not place it next to magnetic supports such as floppy disks, tapes, etc. Operating your device close to other electrical and electronic equipment - such as a television, phone, radio or a personal computer - may cause interferences.

INTERFERENCES

The device, like all other wireless devices, is subject to interferences that may reduce its performances.

ROAD SAFETY

Do not use your device while driving. In case of use on cars, you must check that the electronic equipment is shielded against RF signals. Do not place the device in the air bag deployment area.

AIRCRAFT SAFETY

Switch off your device when on board aircrafts by disconnecting the power supply and deactivating the internal backup battery. Using GSM devices on aircrafts is illegal.

HOSPITAL SAFETY

Do not use the device near health equipment, especially pacemakers and hearing aids, in order to avoid potential interferences. Take care when utilizing the device inside hospitals and medical centres, which make use of equipment that could be sensitive to external RF signals. Switch it off when use is expressly forbidden.

EXPLOSIVE MATERIALS

Do not use the device in refuelling points, near fuel or chemicals. Do not use the device where blasting is in progress. Observe restrictions and follow any specific regulation or instruction.

INSTRUCTIONS FOR USE

Do not use this device in direct contact with the human body and keep a minimum distance of 20 cm from it and from the antenna. Use approved accessories only. Consult the user's manual of eventual other equipment connected to this device. Do not connect incompatible products.

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
	1.00	v.1.1	First Release

Contents

Chapter 1.	Product Concept	8
1.1	Overview	8
1.2	Packing List.....	8
1.3	Specifications	10
1.4	Dimensions	12
1.5	Selection and Ordering Data	12
Chapter 2.	Installation	13
2.1	LED Indicators	13
2.2	PIN assignment	14
2.3	USB interface	14
2.4	Reset Button	15
2.5	Ethernet port	15
2.6	Mounting the Router	16
2.7	Install the SIM Card.....	16
2.8	Connect the External Antenna (SMA Type)	17
Chapter 3.	Configuration settings over web browser.....	18
3.1	Configuring PC in Windows.....	18
3.2	Factory Default Settings.....	20
3.3	Control Panel	21
3.4	Status -> System.....	22
3.5	Status -> Network	25
3.6	Status -> Route.....	25
3.7	Status -> VPN	26
3.8	Status -> Services	27
3.9	Status -> Event/Log	27
3.10	Configuration -> Cellular WAN.....	28
3.11	Configuration -> Ethernet	34
3.12	Configuration -> Serial	36
3.13	Configuration -> USB.....	43
3.14	Configuration -> NAT/DMZ	44
3.15	Configuration -> Firewall.....	45
3.16	Configuration -> QoS.....	47
3.17	Configuration -> IP Routing.....	51
3.18	Configuration -> DynDNS	53
3.19	Configuration -> IPSec.....	54
3.20	Configuration -> Open VPN.....	59
3.21	Configuration -> GRE.....	64
3.22	Configuration -> L2TP.....	65
3.23	Configuration -> PPTP	69
3.24	Configuration -> SNMP	73
3.25	Configuration -> VRRP.....	75
3.26	Configuration -> IP Passthrough	76

3.27	Configuration -> AT over IP	77
3.28	Configuration -> Phone Book	77
3.29	Configuration -> SMS	79
3.30	Configuration -> Reboot	80
3.31	Configuration -> RobustLink	81
3.32	Configuration -> Syslog	81
3.33	Configuration -> Event	82
3.34	Configuration -> USR LED	83
3.35	Administration -> Profile	83
3.36	Administration -> Tools	84
3.37	Administration -> Clock	88
3.38	Administration -> Web Server	89
3.39	Administration -> User Management	90
3.40	Administration -> Update Firmware	91
Chapter 4.	Configuration Examples	93
4.1	Interface	93
4.1.1	Console port	93
4.1.2	RS232	94
4.1.3	RS485	94
4.2	Cellular	95
4.2.1	Cellular Dial-Up	95
4.2.2	SMS Remote Status Reading	96
4.3	Network	98
4.3.1	NAT	98
4.3.2	L2TP	99
4.3.3	PPTP	100
4.3.4	IPSEC VPN	102
4.3.5	OPENVPN	105
Chapter 5.	Introductions for CLI	108
5.1	What's CLI and hierarchy level Mode	108
5.2	How to configure the CLI	110
5.3	Commands reference	114

Chapter 1. Product Concept

1.1 Overview

Digicom 3G Industrial VPN Pro 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/.
- VPN tunnel: IPSec/OpenVPN/PPTP/L2TP/GRE.
- Supports Modbus gateway (Modbus RTU/ASCII to Modbus TCP).
- 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 /USB/Ethernet.
- Wide range input voltages from 6 to 26 VDC and extreme operating temperature.
- The metal enclosure can be mounted on a DIN-rail or on the wall.

1.2 Packing List

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

- **Digicom 3G Industrial VPN Pro router x 1**
-



- **3-pin pluggable terminal block with lock for power connector 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



- 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

3G/2G Module

- UMTS/HSDPA/HSUPA Quad-Band:
 - Band 5 (850 MHz)
 - Band 8 (900 MHz)
 - Band 2 (1900 MHz)
 - Band 1 (2100 MHz)
- GSM/GPRS/EDGE Quad-Band:
 - GSM 850 MHz - E-GSM 900 MHz - DCS 1800 MHz - PCS 1900 MHz
- UMTS/HSDPA/HSUPA Power Class:
 - Power Class 3 (24 dBm) for UMTS/HSDPA/HSUPA mode
- GSM/GPRS Power Class
 - Power Class 4 (33 dBm) for GSM/E-GSM bands
 - Power Class 1 (30 dBm) for DCS/PCS bands
- EDGE Power Class
 - Power Class E2 (27 dBm) for GSM/E-GSM bands
 - Power Class E2 (26 dBm) for DCS/PCS bands
- SIM: 2 x (3V & 1.8V)
- Antenna Interface: SMA Female

Ethernet Interface

- Number of Ports: 1 x 10/100 Mbps
- Magnet Isolation Protection: 1.5KV

Serial Interface

- Number of Ports: 1 x RS-232 and 1 x RS-485
- ESD Protection: $\pm 15\text{KV}$

- 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: DB9 Female

System

- LED Indicators: RUN, PPP, USR, 3 x RSSI
- Built-in RTC, Watchdog, Timer
- Expansion: 1 x USB 2.0 host up to 480 Mbps

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: 3.5mm terminal block
- Input Voltage: 6 to 26 VDC
- Power Consumption: Idle: 100 mA @ 12 V
 Data Link: 1000 mA (peak) @ 12 V

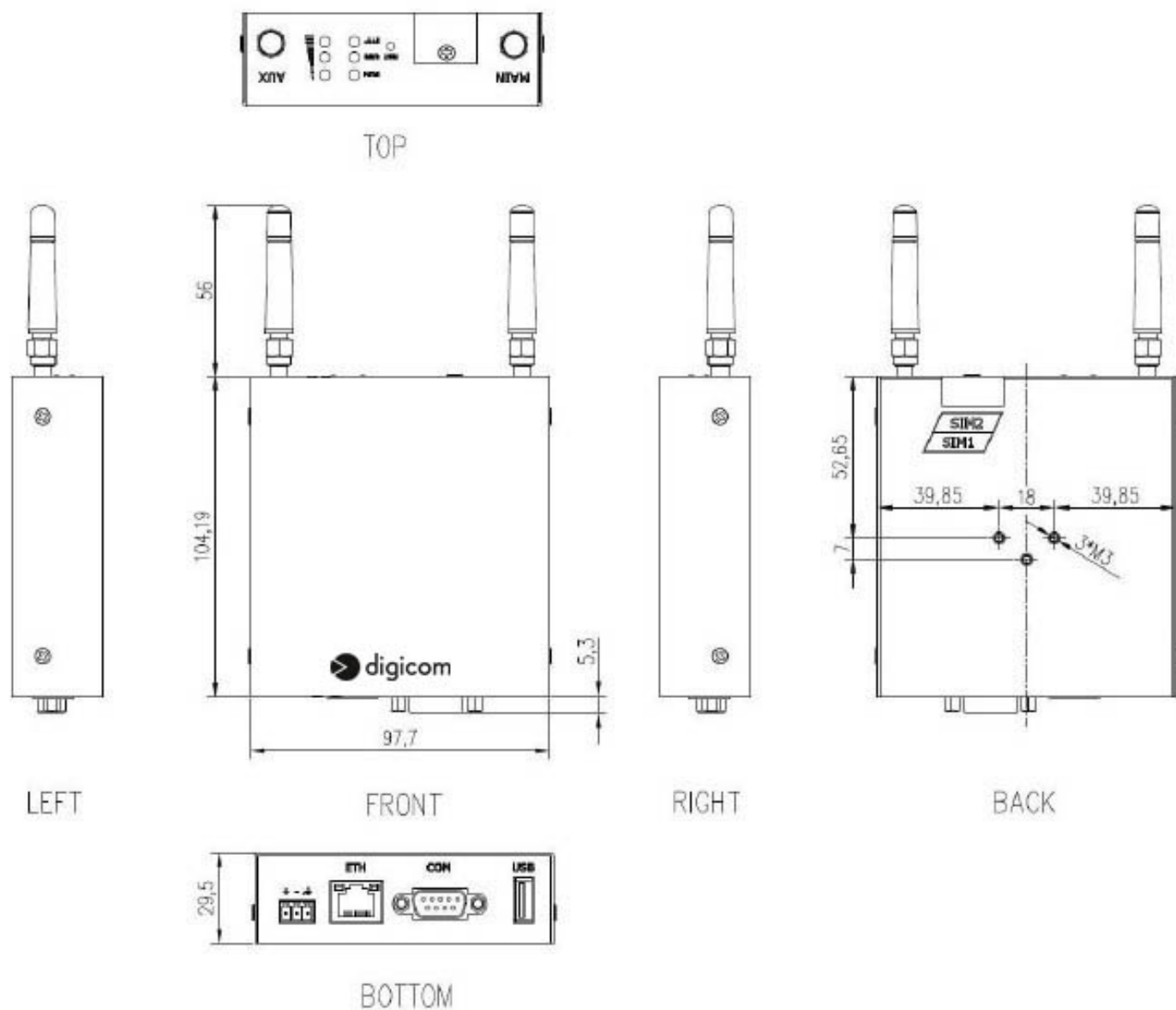
Physical Characteristics

- Housing & Weight: Metal, 300g
- Dimension: (L x W x H): 105 x 100 x 30mm
- Installation: 35mm Din-Rail or wall mounting or desktop

Environmental Limits

-10°C to 60°C
5% to 95% RH

1.4 Dimensions

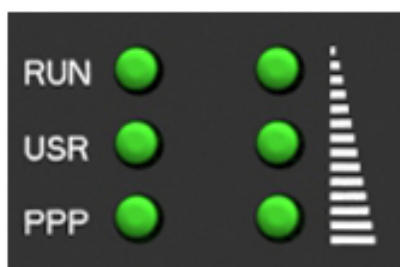


1.5 Selection and Ordering Data

Please refer to corresponding R3G Industrial VPN Pro datasheet.

Chapter 2. Installation

2.1 LED Indicators

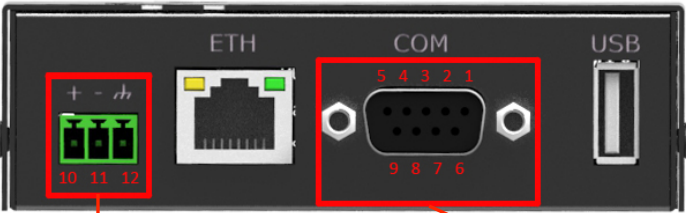


Name	Color	Status	Function
RUN	Green	Blinking	Router is ready.
		On	Router is starting.
		Off	Router is power off.
USR	Green	On/Blinking	VPN tunnel/PPPoE/DynDNS/GPS is up.
		Off	VPN tunnel/PPPoE/DynDNS/GPS is down.
PPP	Green	Blinking	Null
		On	PPP connection is up.
		Off	PPP connection is down.

RSSI LEDs	Function
None	No signal or SIM card not installed properly
1 bar (Only the first LED is on)	Signal level: 1-10 (Exceptional signal level).
2 bars (The first and the second LED are on)	Signal level: 11-20 (Average signal level).
3 bars (All the RSSI LEDs are on) Exceptional	Signal level: 21-31 (Perfect signal level).

Note: User can select display status of USR LED. Please check section [3.34](#).

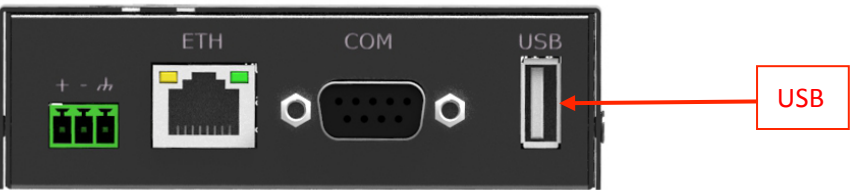
2.2 PIN assignment



PIN	Power
10	Positive
11	Negative
12	GND

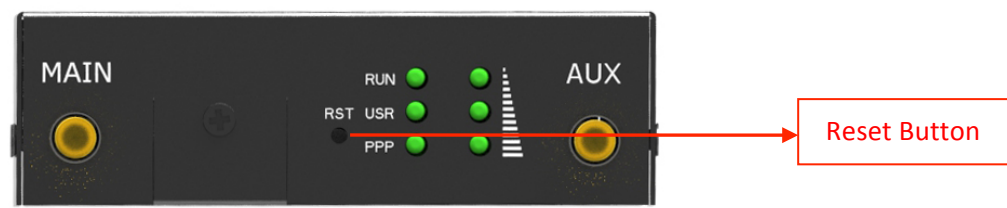
DB9 Female Connector			
PIN	RS232	RS485 (2-wire)	Direction
1		Data+ (A)	-
2	RXD		Router → Device
3	TXD		Device → Router
4			Device → Router
5	GND		-
6		Data- (B)	-
7	RTS		Device → R3G Industrial VPN Pro
8	CTS		R3G Industrial VPN Pro → Device
9			R3G Industrial VPN Pro → Device

2.3 USB interface



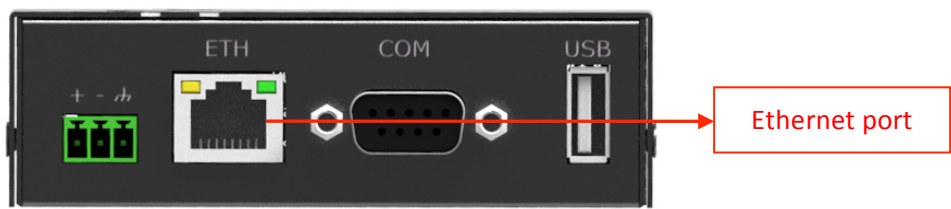
USB interface is used for batch firmware upgrade, cannot used to send or receive data from slave devices which with USB interface. Users can insert an USB storage device, such as U disk or hard disk, into the router’s USB interface, if there is configuration file or firmware of R3G Industrial VPN Pro inside the USB storage devices, R3G Industrial VPN Pro will automatically update the configuration file or firmware. Details please refer to section 3.13.

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 port



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

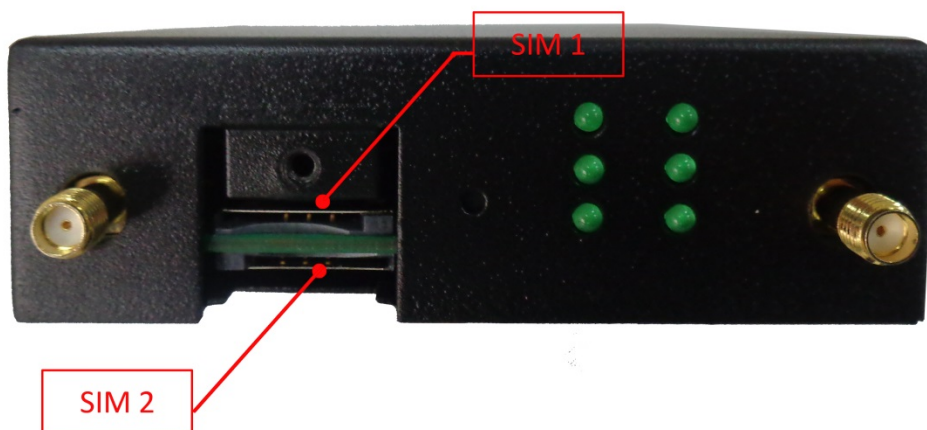
Indicator	Status	Description
Speed Indicator	Off	10 Mbps mode.
	On	100 Mbps mode.
Link Indicator	Off	Connection is down.
	On	Connection is up.
	Blink	Data is being transmitted

2.6 Mounting the Router

Use the router on a DIN rail with 3 M3 screws.



2.7 Install the SIM Card



■ Inserting SIM 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.
3. Insert the SIM 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

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.

2.8 Connect the External Antenna (SMA Type)

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



Chapter 3. Configuration settings over web browser

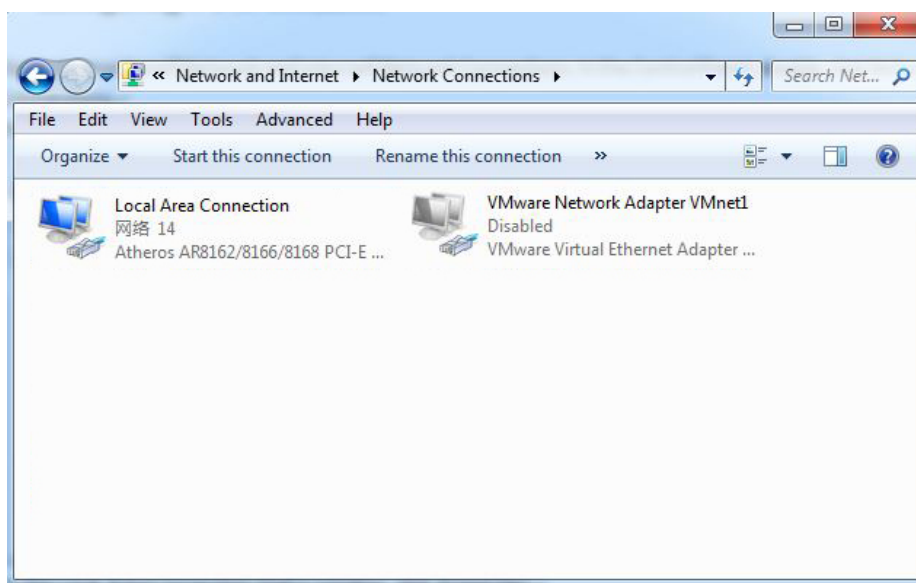
The router can be configured through your web browser. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista/7/8, etc. The product provides an easy and user-friendly interface for configuration.

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.

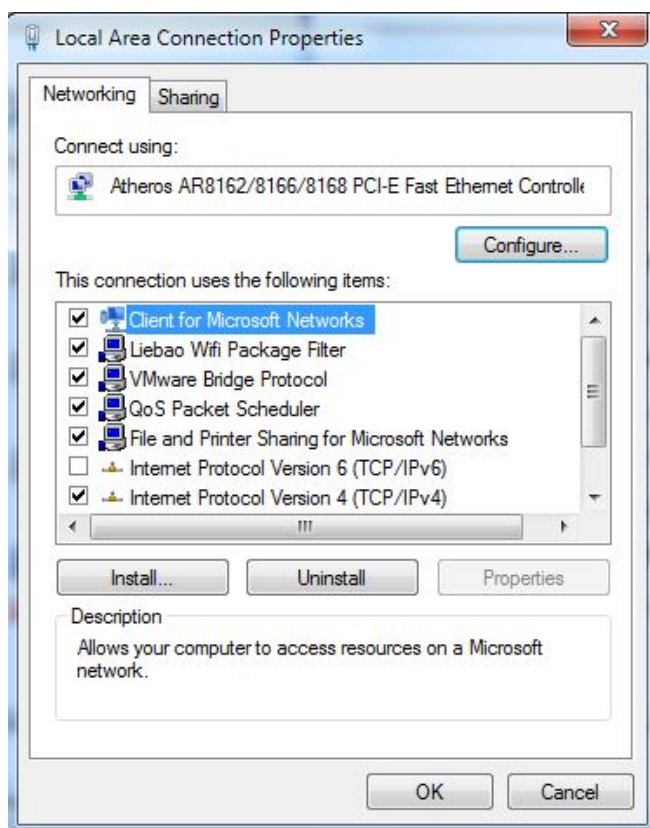
You must configure your PC to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problems accessing the router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

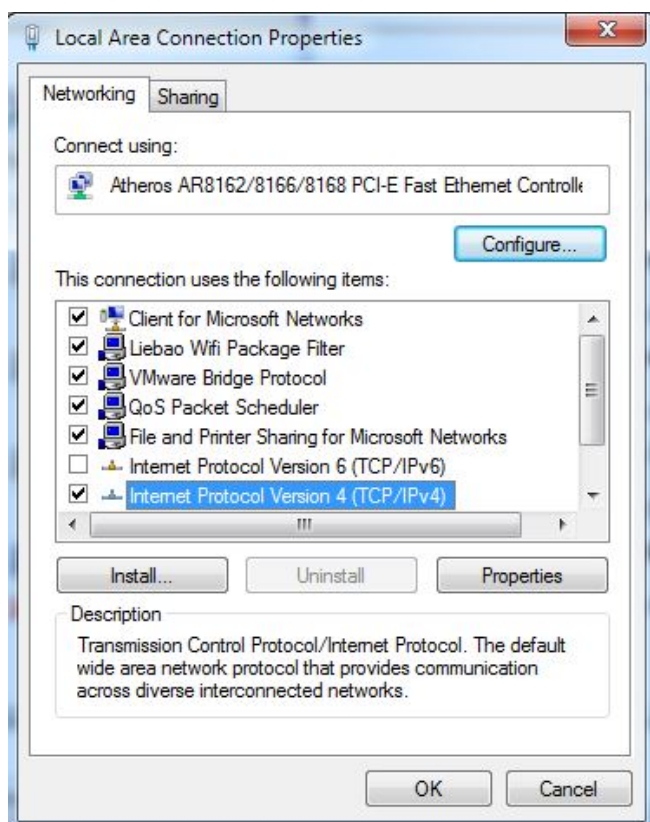
1. Go to **Control Panel\Network and Internet\Network Connections**. In the Control Panel, double-click Network Connections.
2. Double-click Local Area Connection.



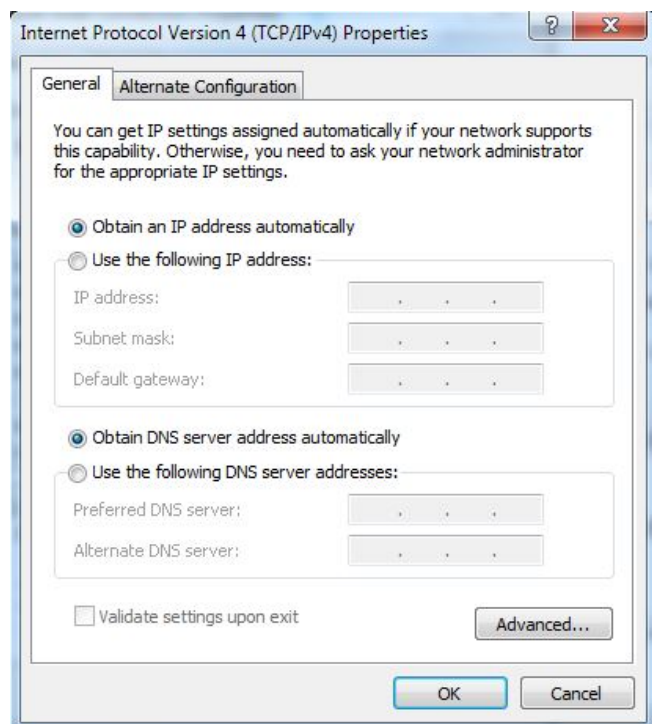
3. In the Local Area Connection Status window, click Properties.



4. Select Internet Protocol (TCP/IPv4) and click Properties.



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



6. Click OK to finish the configuration.

3.2 Factory Default Settings

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

User authentication required. Login please.

Username:

Password:

Language: ▼

Please enter your login username and password.

Item	Description
Username	admin
Password	admin
Ethernet	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.

Status

- System
- Network
- Route
- VPN
- Services
- Event/Log

Configuration

- Cellular WAN
- Ethernet
- Serial
- USB
- NAT/DMZ
- Firewall
- QoS
- IP Routing
- DynDNS
- IPsec
- OpenVPN
- GRE
- L2TP
- PPTP
- SNMP
- VRRP
- IP Passthrough
- AT over IP
- Phone Book
- SMS

System

LEDs Information

RUN:	GREEN/BLINK
USR:	OFF
PPP:	GREEN/ON

Router Information

Device Model:	R3000
Serial Number:	Robustel SN
Device Name:	Cellular Router
Firmware Version:	1.01.01-sub-131211
Hardware Version:	1.00.03
Kernel Version:	2.6.39-5
Radio Module Type:	MU609
Radio Firmware Version:	11.103.63.00.00
Uptime:	0 day 00:03:20
CPU Load:	06.08%
RAM Total/Free:	123.05MB/74.78MB(60.77%)
System Time:	2013-12-11 19:01:40

Current WAN Link

Current WAN Link:	Cellular
IP Address:	10.124.120.213
Gateway:	192.168.254.254
NetMask:	255.255.255.255
DNS Server:	221.179.38.7, 120.196.165.7
Keepalive PING IP Address:	8.8.8.8, 8.8.4.4
Keepalive PING Interval:	30

Manual 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 [2.2](#) LED Indicators.

System	
LEDs Information	
RUN:	GREEN/BLINK
USR:	OFF
PPP:	GREEN/ON

Router Information

Device Model: R3000
 Serial Number:
 Device Name: Cellular Router
 Firmware Version: 1.01.01-sub-131211
 Hardware Version: 1.00.03
 Kernel Version: 2.6.39-5
 Radio Module Type: MU609
 Radio Firmware Version: 11.103.63.00.00
 Uptime: 0 day 00:03:20
 CPU Load: 06.08%
 RAM Total/Free: 123.05MB/74.78MB(60.77%)
 System Time: 2013-12-11 19:01:40

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

Current WAN Link: Cellular
 IP Address: 10.124.120.213
 Gateway: 192.168.254.254
 NetMask: 255.255.255.255
 DNS Server: 221.179.38.7, 120.196.165.7
 Keepalive PING IP Address: 8.8.8.8, 8.8.4.4
 Keepalive PING Interval: 30

Current WAN Link

Item	Description
Current WAN Link	Show the current WAN link: Cellular 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:	SIM1
Phone No.:	
SMS Service Center:	8613800200500
Modem Status:	Ready
Network Status:	Registered, roaming
Signal Level (RSSI):	 (21,-71DB)
Network Operator:	China Mobile (LAC: 2515 / Cell ID: 62DC)
Network Service Type:	GPRS
IMEI/ESN:	357784040029991
IMSI:	460079148174440
APN:	cmnet
Username:	
Password:	
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	Show the SMS Service Center.
Modem Status	Show the status of modem. There are 8 different status: 1. Unknown. 2. Ready. 3. Checking AT. 4. Need PIN. 5. Need PUK. 6. Signal level is low. 7. No registered. 8. Initialize APN failed.
Network Status	Show the current network status. There are 6 different status: 1. Not registered, ME is currently not searching for new operator!

	2. Registered to home network. 3. Not registered, but ME is currently searching for a new operator. 4. Registration denied. 5. Registered, roaming. 6. Unknown.
Signal Level (RSSI)	Show the current signal level.
Network Operator	Show Mobile Country Code (MCC) +Mobile Network Code (MNC), e.g. 46001. Also it will show the Location Area Code (LAC) and Cell ID.
Network Service Type	Show the current network service type, e.g. GPRS.
IMEI/ESN	Show the IMEI/ESN number of the radio module.
IMSI	Show the IMSI number of the current SIM.
USB Status	Show the current status of USB host.

3.5 Status -> Network

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

Network

Cellular WAN

Connection Status:	Connected
Connect Time:	0 day 00:00:08
IP Address:	10.153.113.95
MTU:	1500
Gateway:	192.168.254.254
Primary DNS Server:	221.179.38.7
Secondary DNS Server:	120.196.165.7

LAN

IP Address:	172.16.2.113
MAC Address:	00:ff:74:46:dc:e1
MTU:	1500
NetMask:	255.255.0.0

3.6 Status -> Route

This section displays the router's route table.

Route

Route Table

Destination	NetMask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0	192.168.254.254	ppp0	0
172.16.0.0	255.255.0.0	0.0.0.0	eth0	0
192.168.254.254	255.255.255.255	0.0.0.0	ppp0	0

3.7 Status -> VPN

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

IPsec

L2TP

PPTP

OpenVPN

GRE

IPsec Status

No.	Tunnel name	Status	Connect Time

IPsec Detail Status

[Show Detail Status](#)

IPsec

L2TP

PPTP

OpenVPN

GRE

L2TP Client

No.	Tunnel name	Status	Local IP	Remote IP	Connect Time

L2TP Server

No.	Tunnel name	Status	Local IP	Remote IP	Connect Time

IPsec

L2TP

PPTP

OpenVPN

GRE

PPTP Client

No.	Tunnel name	Status	Local IP	Remote IP	Connect Time

PPTP Server

No.	Tunnel name	Status	Local IP	Remote IP	Connect Time

IPsec

L2TP

PPTP

OpenVPN

GRE

VPN Status

No.	Tunnel name	Status

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

3.8 Status -> Services

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

VRRP	DynDNS	Serial
VRRP		
VRRP is disabled!		

VRRP	DynDNS	Serial
DynDNS		
DynDNS is disabled!		

VRRP	DynDNS	Serial
RS232: 115200, N, 8, 1		
RS485: 115200, N, 8, 1		

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

```

13-12-11 18:58:28 <0> router: Firmware version: 1.01.01-sub-131211 Dec 11 2013 18:58:29
13-12-11 18:58:28 <0> router: start dhcpd
13-12-11 18:58:34 <0> router: open /dev/ttyUSB0 successful!
13-12-11 18:58:35 <0> router: sent:ATE0
13-12-11 18:58:35 <0> router: rcvd:
^SYSSTART
13-12-11 18:58:35 <3> router: failed 1/5 to test AT command ATE0
13-12-11 18:58:36 <0> router: sent:ATE0
13-12-11 18:58:37 <0> router: rcvd:
OK
13-12-11 18:58:37 <0> router: sent:AT+CPIN?
13-12-11 18:58:37 <0> router: rcvd:
+CME ERROR: SIM busy
13-12-11 18:58:37 <3> router: failed 1/5 to check SIM card
13-12-11 18:58:42 <0> router: sent:AT+CPIN?
13-12-11 18:58:42 <0> router: rcvd:
+CPIN: READY
OK

```

Download System Diagnosing Data

Download System Diagnosing Data

Manual Refresh
Refresh
Clear

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

3.10 Configuration -> Cellular WAN

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

Basic

Advanced

ISP Profile

Cellular Settings

	SIM1	SIM2
Status:	Ready	Not inserted
Network Provider Type:	Auto	Auto
APN:		
Username:		
Password:		
Dialup No.:		
PIN Type:	None	None

Connection Mode

Connection Mode:	Connect On Demand
Redial Interval (s):	30
Max Retries:	3
Inactivity Time (s):	0
Serial Output Content (Hex):	
<input checked="" type="checkbox"/> Triggered By Serial Data	
<input checked="" type="checkbox"/> Triggered By Tel	
<input checked="" type="checkbox"/> Triggered By SMS	
SMS Connect Command:	
SMS Disconnect Command:	
SMS Connect Reply:	
SMS Disconnect Reply:	
Phone Group:	NULL Click to add PhoneGroup!
<input checked="" type="checkbox"/> Periodically Connect	
Periodically Connect Interval (s):	300
Time Schedule:	NULL

Time Range

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

Add



Dual SIM Policy

Main SIM Card: SIM1 ▾

- ☒ Switch To Backup SIM Card When Connection Fails
- ☒ Switch To Backup SIM Card When ICMP Detection Fails
- ☒ Switch To Backup SIM Card When Roaming Is Detected

Preferred PLMN:

- ☒ Switch To Backup SIM Card When Data Limit Is Exceeded

Max Data Limitation (MB):

100

100

Date Of Month To Clean:

1

1

Already used (KB):

0

0

Clear

Clear

- ☒ Switch Back Main SIM Card After Timeout

Initial Timeout (min):

60

Basic @Cellular WAN**Cellular Settings**

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

Connection Mode	<p>Select from “Always Online” and “Connect On Demand”.</p> <p>Always Online: Auto activates PPP and keeps the link up after power on.</p> <p>Connect On Demand: After selection this option, user could configure Triggered by Serial Data, Triggered by Periodically Connect and Triggered by Time Schedule.</p> <p>Note: If you select several connect on demand polices, router only have to meet one of them to be triggered.</p>	Connect On Demand
Redial Interval	Router will automatically re-dial with this interval when it fails communicating to peer via TCP or UDP.	30
Max Retries	<p>The maximum retries times for automatically re-connect when router fails to dial up.</p> <p>After maximum retries, router will reboot the wireless module. If router still cannot dial up successfully, it will try to switch to the other SIM card. Then router will re-connect with the other SIM card with maximum retries.</p> <p>After successful connection, the Max Retries counter will be set to 0.</p>	3
ICMP Detection Primary Server	Router will ping this primary address/domain name to check that if the current connectivity is active.	8.8.8.8
ICMP Detection Secondary Server	Router will ping this secondary address/domain name to check that if the current connectivity is active.	8.8.4.4
ICMP Detection Interval	Set the ping interval time.	Null
ICMP Detection Timeout	Set the ping timeout.	30
ICMP Detection Retries	If Router ping the preset address/domain name time out continuously for Max Retries time, it will consider that the connection has been lost.	3
Reset The Interface	Enable to reset the cellular/ETH interface after the max ICMP detection retries.	3
Serial Output Content	The content which output to the serial device which connect to router and inform it that router is ready to receive serial data.	Null
Triggered by Serial Data	Tick this check box to allow router automatically connects to cellular network from idle mode when there is data comes out from serial port.	Enable
Triggered by Tel	Tick this check box to allow router automatically connects to cellular network from idle mode when make a voice call to router.	Disable
Triggered by SMS	Tick this check box to allow router automatically connects to cellular network from idle mode when send a specific SMS to router.	Disable
SMS Connect Command	Users shall send this specific SMS to trigger router to connect to cellular network.	Null
SMS Disconnect Command	Users shall send this specific SMS to trigger router to disconnect to cellular network.	Null
SMS Connect Reply	When router connects to cellular network, it will automatically send out this SMS to specific users (set in the Phone Group).	Null
SMS Disconnect Reply	When router disconnect from cellular network, it will automatically send out this SMS to specific users (set in the Phone Group).	Null
Phone Group	Click to add Phone Group to Set specific users' phone Book and which phone Group they are belonged to.	Null

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

Cellular Advanced Settings

	SIM1	SIM2
Phone No.:	<input type="text"/>	<input type="text"/>
Network Type:	<input type="text" value="Auto"/>	<input type="text" value="Auto"/>
Band Mode:	<input type="checkbox"/> ALL <input type="checkbox"/> GSM850 <input type="checkbox"/> EGSM900 <input type="checkbox"/> PGSM900 <input type="checkbox"/> RGSM900 <input type="checkbox"/> GSM1800 <input type="checkbox"/> GSM1900 <input type="checkbox"/> UMTS800 <input type="checkbox"/> UMTS850 <input type="checkbox"/> UMTS900 <input type="checkbox"/> UMTS1700 <input type="checkbox"/> UMTS1900 <input type="checkbox"/> UMTS2000	<input type="checkbox"/> ALL <input type="checkbox"/> GSM850 <input type="checkbox"/> EGSM900 <input type="checkbox"/> PGSM900 <input type="checkbox"/> RGSM900 <input type="checkbox"/> GSM1800 <input type="checkbox"/> GSM1900 <input type="checkbox"/> UMTS800 <input type="checkbox"/> UMTS850 <input type="checkbox"/> UMTS900 <input type="checkbox"/> UMTS1700 <input type="checkbox"/> UMTS1900 <input type="checkbox"/> UMTS2000
Authentication:	<input type="text" value="Auto"/>	<input type="text" value="Auto"/>
MTU:	<input type="text" value="1500"/>	<input type="text" value="1500"/>
MRU:	<input type="text" value="1500"/>	<input type="text" value="1500"/>
Asynmap Value:	<input type="text" value="ffffffff"/>	<input type="text" value="ffffffff"/>
Use Peer DNS:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Primary DNS Server:	<input type="text"/>	<input type="text"/>
Secondary DNS Server:	<input type="text"/>	<input type="text"/>
Address/Control Compression:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Protocol Field Compression:	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Expert Options:	<input type="text" value="noccp nobsdcomp"/>	<input type="text" value="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"->"System"->"Cellular WAN Information"->"SIM Phone Number". In general, you don't need to set this number because router will read it from the SIM card automatically.	Null
Network Type	Select from "Auto", "2G GSM" and "3G UMTS" as the SIM card supported.	Auto
Band Mode	Tick the Band Mode options to fix the bands router working with.	Disable
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	1500

	packet, which is possible to transfer in a given environment.	
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 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 can be separated by a space.	noccp nobsdcom p

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".

Basic

Advanced

ISP Profile

ISP Profile List

ISP	APN	Username	Password	Dialup No.
china-mobile	3gnet			*99***1#

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

3.11 Configuration -> Ethernet

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

Eth0

Dhcp Relay

LAN Interface

IP Address: 172.16.2.113
NetMask: 255.255.0.0
MTU: 1500

Multiple IP Address

IP Address	NetMask

Add

DHCP 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
IP Address, Netmask, MTU @ LAN Interface	Set the IP address, Netmask and MTU of Eth0. These parameters will be un-configurable if you enable Bridge.	Null
Multiple IP Address @ LAN Interface	Assign multiple IP addresses for Eth0.	Null
Enable DHCP Server @ DHCP Server	Enable to make router can lease IP address to DHCP clients which connect to Eth0.	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/ 192.168.0.100
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	Define the primary/secondary DNS Server which the DHCP clients will	192.168.0.1/

DNS Server @ DHCP Server	obtain from DHCP server.	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

Dhcp Relay

DhcpRelay Configuration☒ Enable Dhcp Relay

DHCP Server:

DHCP Relay @ Ethernet

Item	Description	Default
DHCP Server	Enter DHCP Server's IP address. Note: Please disable DHCP Server and DHCP Client first to make sure DHCP relay can be enabled.	Null

3.12 Configuration -> Serial

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

RS232

RS485

Serial Port Settings

Baudrate:
 Data Bit:
 Parity:
 Stop Bit:
 Flow Control:

Protocol Settings

Protocol:

- 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

Modbus Slave

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

Add

- 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 this function will disable cellular WAN.)

COM Name: /dev/ttyUSB0

RS232 @ Serial		
Item	Description	Default
Baud-rate	Select from "300", "600", "1200", "2400", "4800", "9600", "19200", "38400", "57600", "115200" and "230400".	115200
Data bit	Select from "7" and "8".	8
Parity	Select from "None", "Odd" and "Even".	None
Stop bit	Select from "1" and "2".	1
Flow control	Select from "None", "Software" and "Hardware".	None
Protocol	<p>Select from "None", "Transparent", "Modbus", "Transparent Over Rlink", "Modbus Over Rlink", "AT Over COM" and "GPS Report".</p> <ol style="list-style-type: none"> 1. None: Router will do nothing in RS232 serial port. 2. Transparent: Router will transmit the serial data transparently without any protocols. 3. Modbus: Router will translate the Modbus RTU data to Modbus TCP data and vice versa. 4. Transparent Over Rlink: Router will send all data from RS232 serial port to Robustlink, then Robustlink will forward the data to another destination site. 5. Modbus Over Rlink: Router will translate all data from RS232 serial port to Modbus TCP protocol data, and then send to Robustlink, after that Robustlink will forward the data to another destination site. 6. AT Over COM: select to operate router via RS232 COM port. For example, enter AT commands to router via RS232 COM port. 7. GPS Report: select to enable router to output GPS status data through RS232 port. 	None
Mode @Transparent	<p>Select from "TCP Server", "TCP Client" and "UDP".</p> <p>TCP Client: Router works as TCP client, initiate TCP connection to TCP server. Server address supports both IP and domain name.</p> <p>TCP Server: Router works as TCP server, listening for connection request from TCP client.</p> <p>UDP: Router works as UDP client.</p>	TCP Client
Local Port @Transparent	Enter the Local port for TCP or UDP.	0
Multiple Server @Transparent	<p>Click "Add" button to add multiple server. You need to enter the server's IP and port, and enable or disable "Send data to serial". If you disable "Send data to serial", router will not transmit the data from this server to serial port.</p> <p>Note: This section will not be displayed if you select "TCP server" in "Mode".</p>	None
show Protocol Advanced @Transparent	Tick to enable protocol advanced setting.	Disable
Local IP @Transparent	This item will show up when you enable any VPN tunnel of 3G Industrial VPN Pro, it means serial data can be matched to this local IP address and be transmitted or received via VPN tunnel.	Null

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

	Note: When select “Modbus RTU master” and “Modbus ASCII master” protocol, router is as TCP Client site, user need to enter slave address and slave port number in “Slave Address @ Modbus Slave ” and “Slave Port @ Modbus Slave”, and connect to Server site.	
Modbus Slave @ Modbus	Add the Modbus slaves which will be polled by Modbus master (router). This section only displayed when you select “Modbus RTU master” or “Modbus ASCII master” in “Attached serial device type”.	Null
Slave Address @ Modbus Slave	This connection is usually used to connect to the Modbus slave devices which as TCP server. Enter IP address of the TCP server.	Null
Slave Port @ Modbus Slave	Enter the port number of TCP server.	Null
ID @ Modbus Slave	Enter the ID number of TCP server.	Null
Interval Timeout @ Transparent Over Rlink	The serial port will queue the data in the buffer and send the data to the Cellular WAN/Ethernet WAN when it reaches the Interval Timeout in the field.	10
Attached serial device type @ Modbus Over Rlink	Select From “Modbus RTU slave”, “Modbus ASCII slave”. Modbus RTU slave: router connects to slave device which works under Modbus RTU protocol. Modbus ASCII slave: router connects to slave device which works under Modbus ASCII protocol.	Null
Display all com @ AT Over COM	Enable to display all virtual com of the module inside the router. Generally, router will occupy /dev/ttyUSB0 and /dev/ttyUSB2 for dialing up to GPRS. Note: Enable this function will disable Cellular WAN function.	Disable
COM Name	Show the virtual com name of the module inside.	/dev/ttyUSB0

RS232

RS485

Serial Port Settings

Baudrate: 115200 ▼
 Data Bit: 8 ▼
 Parity: None ▼
 Stop Bit: 1 ▼

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

- 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	Select from “300”, “600”, “1200”, “2400”, “4800”, “9600”, “19200”, “38400”, “57600”, “115200” and “230400”.	115200
Data bit	Select from “7” and “8”.	8
Parity	Select from “None”, “Odd” and “Even”.	None
Stop bit	Select from “1” and “2”.	1
Protocol	Select from “None”, “Transparent” and “Modbus”. Transparent: Router will transmit the serial data transparently without any	Transparent

	protocols. Modbus: Router will transmit the serial data with Modbus protocol.	
Mode @Transparent	Select from "TCP Server", "TCP Client" and "UDP".	TCP Client
Local Port @Transparent	Enter the Local port for TCP or UDP.	0
Multiple Server @Transparent	Click "Add" button to add multiple server. You need to enter the server's IP and port, and enable or disable "Send data to serial". If you disable "Send data to serial", router will not transmit the data from this server to serial port. Note: This section will not be displayed if you select "TCP server" in "Mode".	Null
Enable Protocol @Transparent	Tick to enable protocol advanced setting.	Disable
Local IP @Transparent	This item will show up When you enable any VPN tunnel of 3G Industrial VPN Pro, it means serial data can be matched to this local IP address and be transmitted or received via VPN tunnel. Note: when you do not enable any VPN tunnel, this item will not show up.	0
Interval Timeout @Transparent	The serial port will queue the data in the buffer and send the data to the Cellular WAN/Ethernet WAN when it reaches the Interval Timeout in the field. Note: Data will also be sent as specified by the packet length or delimiter settings even when data is not reaching the interval timeout in the field.	10
Packet Length @Transparent	The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. 0 for packet length, no maximum amount is specified and data in the buffer will be sent as specified by the interval timeout or delimiter settings or when the buffer is full. When a packet length between 1 and 1024 bytes is specified, data in the buffer will be sent as soon it reaches the specified length. Note: Data will also be sent as specified by the interval timeout or delimiter settings even when data is not reaching the preset packet length.	1360
Enable Delimiter1	When Delimiter 1 is enabled, the serial port will queue the data in the buffer and send the data to the Cellular WAN/Ethernet WAN when a specific character, entered in hex format, is received. A second delimiter character may be enabled and specified in the Delimiter 2 field, so that both characters act as the delimiter to control when data should be sent.	Disable
Delimiter1 (Hex) @Transparent	Enter the delimiter in Hex.	0
Delimiter Process @Transparent	The Delimiter process field determines how the data is handled when a delimiter is received. None: Data in the buffer will be transmitted when the delimiter is received; the data also includes the delimiter characters. Strip: Data in the buffer is first stripped of the delimiter before being transmitted.	Strip
Local IP @ Modbus	This item will show up When you enable any VPN tunnel of 3G Industrial	0

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

3.13 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 R3G Industrial VPN Pro inside the USB storage devices, R3G Industrial VPN Pro will automatically update the configuration file or firmware. We will provide another file to show how to do USB automatic update.

USB**USB Configuration**

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

USB

Item	Description	Default
Enable automatic update of configuration	Click Enable to automatically update the configuration file of 3G Industrial VPN Pro when insert the USB storage devices which has 3G Industrial VPN Pro's configuration file.	Disable
Enable automatic update of firmware	Click Enable to automatically update the firmware of 3G Industrial VPN Pro when insert the USB storage devices which has 3G Industrial VPN Pro's firmware.	Disable

3.14 Configuration -> NAT/DMZ

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

Port Forwarding**DMZ****Port Forwarding**

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>-<1-65535>

Port Forwarding @ NAT/DMZ

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

Port Forwarding

DMZ

Enable DMZ

☒ Enable DMZ

DMZ Settings

DMZ Host:

Source Address:

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

DMZ @ NAT/DMZ

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

3.15 Configuration -> Firewall

This section allows users to set the firewall parameters.

Basic

Filtering

MAC-Binding

Filter Basic Settings

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

Basic @ Firewall

Item	Description	Default
Remote Access Using HTTP	Enable to allow users to access the router remotely on the internet side via HTTP.	Enable
Remote Access Using TELNET	Enable to allow users to access the router remotely on the internet side via Telnet.	Enable
Remote Access Using SNMP	Enable to allow users to access the router remotely on the internet side via SNMP.	Enable
Remote 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.

Basic

Filtering

MAC-Binding

Default Filter Policy

☒ Accept☐ Drop

Add Filter List

Action

Description

Source IP

Source Port

Target IP Address

Target Port

Protocol

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

Add

*Port: <1-65535> or <1-65535>-<1-65535>

Filtering @ Firewall

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

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

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

Router will execute the Default Filter Policy.

Basic

Filtering

MAC-Binding

MAC-IP Binding List

Description	MAC Address	IP Address
*MAC: ff:ff: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

3.16 Configuration -> QoS

This section allows users to set the QoS parameters.

Enable Quality Of Service(QoS)

☒ Enable QoS

Quality of Service(Qos) Basic Setting

Downlink Speed (kbps):

0

Uplink Speed (kbps):

0

Optimize for TCP Flags:

☐ SYN
☐ ACK
☐ FIN
☐ RST

Optimize for ICMP:

☐

Optimize for Serial Data Forwarding:

☐

Priority Percent Definition:

Exempt:

50

Premium:

25

Express:

15

Normal:

10

Bulk:

1

Default Priority:

Normal ▼

Qos Port Based Control

☐ Enable Port Based Priority

QoS Service Control List

Service Name	Protocol	Port	Priority
Add			

QoS MAC Control List

MAC Address	Priority
*MAC: ff:ff:ff:ff:ff:ff	Add

QoS IP Control List

IP Address	Priority
Add	

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

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

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

3.17 Configuration -> IP Routing

This section allows users to set the IP routing parameters.

Static Route
RIP
 OSPF

Static Route Table

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

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

Static Route
 RIP
 OSPF

RIPIPv4 Enabled
☒ Enable RIP Protocol Setting

RIP Protocol Version
☒ RIPv1
 ☐ RIPv2

RIP Protocol common Settings

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

RIP protocol Advance Setting
☐ Enable Advance

Network List

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

RIP @ IP Routing		
Item	Description	Default
RIP	RIP (Routing Information Protocol) is a distance-vector routing protocol, which	Null

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

Static Route

RIP

OSPF

OSPF Protocol☐ Enable OSPFv2**OSPF @ IP Routing**

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

3.18 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 is initializing.....*

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

3.19 Configuration -> IPsec

This section allows users to set the IPsec parameters.

IPsec Basic
IPsec Tunnel
X.509

IPsec Basic

☒ Enable NAT Traversal

Keepalive Interval(s):

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

IPsec Basic
IPsec Tunnel
X.509

IPsec Tunnel

Tunnel name	Description

Add

IPsec Tunnel	
<input checked="" type="checkbox"/> Enable	
IPsec Common	
IPsec Gateway Address:	<input type="text"/>
IPsec Mode:	Tunnel ▾
IPsec Protocol:	ESP ▾
Local Subnet:	<input type="text"/>
Local Subnet Mask:	<input type="text"/>
Local ID Type:	Default ▾
Remote Subnet:	<input type="text"/>
Remote Subnet Mask:	<input type="text"/>
Remote ID Type:	Default ▾
IKE Parameter	
Negotiation Mode:	Main ▾
Encryption Algorithm:	AES256 ▾
Authentication Algorithm:	MD5 ▾
DH Group:	MODP1024_2 ▾
Authentication:	PSK ▾
Secrets:	<input type="text"/>
Life Time(s):	3600
SA Parameter	
SA Algorithm:	3DES_SHA1_96 ▾
PFS Group:	PFS_NULL ▾
Life Time(s):	28800
DPD Time Interval (s):	60
DPD Timeout (s):	180
IPsec Advanced	
<input type="checkbox"/> Enable Compress	
<input checked="" type="checkbox"/> Enable ICMP Detection	
ICMP Detection Server:	<input type="text"/>
ICMP Detection Local IP:	<input type="text"/>
ICMP Detection Interval (s):	30
ICMP Detection Timeout (s):	5
ICMP Detection Retries:	3

IPSec Tunnel @ IPSec

Item	Description	Default
Add	Click Add to add new IPSec Tunnel	Null
Enable	Enable IPSec Tunnel, the max tunnel account is 3	Null
IPSec Gateway	Enter the address of remote side IPSec VPN server.	Null

Address		
IPSec Mode	<p>Select from “Tunnel” and “Transport”.</p> <p>Tunnel: Commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it.</p> <p>Transport: Used between end-stations or between an end-station and a gateway, if the gateway is being treated as a host—for example, an encrypted Telnet session from a workstation to a router, in which the router is the actual destination.</p>	Tunnel
IPSec Protocol	<p>Select the security protocols from “ESP” and “AH”.</p> <p>ESP: Uses the ESP protocol.</p> <p>AH: Uses the AH protocol.</p>	ESP
Local Subnet	Enter IPSec Local Protected subnet’s address.	0.0.0.0
Local Subnet Mask	Enter IPSec Local Protected subnet’s mask.	0.0.0.0
Local ID Type	<p>Select from “IP Address”, “FQDN” and “User FQDN” for IKE negotiation. “Default” stands for “IP Address”.</p> <p>IP Address: Uses an IP address as the ID in IKE negotiation.</p> <p>FQDN: Uses an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security gateway, e.g., test.Digicom.com.</p> <p>User FQDN: Uses a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with an sign “@” for the local security gateway, e.g., test@Digicom.com.</p>	Default
Remote Subnet	Enter IPSec Remote Protected subnet’s address.	0.0.0.0
Remote Subnet Mask	Enter IPSec Remote Protected subnet’s mask.	0.0.0.0
Remote ID Type	<p>Select from “IP Address”, “FQDN” and “User FQDN” for IKE negotiation.</p> <p>IP Address: Uses an IP address as the ID in IKE negotiation.</p> <p>FQDN: Uses an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security gateway, e.g., test.Digicom.com.</p> <p>User FQDN: Uses a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with a sign “@” for the local security gateway, e.g., test@Digicom.com.</p>	Default
Negotiation Mode	<p>Select from “Main” and “aggressive” for the IKE negotiation mode in phase 1. If the IP address of one end of an IPSec tunnel is obtained dynamically, the IKE negotiation mode must be aggressive. In this case, SAs can be established as long as the username and password are correct.</p>	Main
Encryption Algorithm	<p>Select from “DES”, “3DES”, “AES128”, “AES192” and “AES256” to be used in IKE negotiation.</p> <p>DES: Uses the DES algorithm in CBC mode and 56-bit key.</p> <p>3DES: Uses the 3DES algorithm in CBC mode and 168-bit key.</p> <p>AES128: Uses the AES algorithm in CBC mode and 128-bit key.</p> <p>AES192: Uses the AES algorithm in CBC mode and 192-bit key.</p>	3DES

	AES256: Uses the AES algorithm in CBC mode and 256-bit key.	
Authentication Algorithm	Select from "MD5" and "SHA1" to be used in IKE negotiation. MD5: Uses HMAC-SHA1. SHA1: Uses HMAC-MD5.	MD5
DH Group	Select from "MODP768_1", "MODP1024_2" and "MODP1536_5" to be used in key negotiation phase 1. MODP768_1: Uses the 768-bit Diffie-Hellman group. MODP1024_2: Uses the 1024-bit Diffie-Hellman group. MODP1536_5: Uses the 1536-bit Diffie-Hellman group.	MODP1024_2
Authentication	Select from "PSK", "CA", "XAUTH Init PSK" and "XAUTH Init CA" to be used in IKE negotiation. PSK: Pre-shared Key. CA: Certification Authority. XAUTH: Extended Authentication to AAA server.	PSK
Secrets	Enter the Pre-shared Key.	Null
Life Time @ IKE Parameter	Set the lifetime in IKE negotiation. Before an SA expires, IKE negotiates a new SA. As soon as the new SA is set up, it takes effect immediately and the old one will be cleared automatically when it expires.	86400
SA Algorithm	Select from "DES_MD5_96", "DES_SHA1_96", "3DES_MD5_96", "3DES_SHA1_96", "AES128_MD5_96", "AES128_SHA1_96", "AES192_MD5_96", "AES192_SHA1_96", "AES256_MD5_96" and "AES256_SHA1_96" when you select "ESP" in "Protocol"; Select from "AH_MD5_96" and "AH_SHA1_96" when you select "AH" in "Protocol"; Note: Higher security means more complex implementation and lower speed. DES is enough to meet general requirements. Use 3DES when high confidentiality and security are required.	3DES_MD5_96
PFS Group	Select from "PFS_NULL", "MODP768_1", "MODP1024_2" and "MODP1536_5". PFS_NULL: Disable PFS Group MODP768_1: Uses the 768-bit Diffie-Hellman group. MODP1024_2: Uses the 1024-bit Diffie-Hellman group. MODP1536_5: Uses the 1536-bit Diffie-Hellman group.	PFS_NULL
Life Time @ SA Parameter	Set the IPSec SA lifetime. Note: When negotiating to set up IPSec SAs, IKE uses the smaller one between the lifetime set locally and the lifetime proposed by the peer.	28800
DPD Time Interval	Set the interval after which DPD is triggered if no IPSec protected packets is received from the peer. DPD: Dead peer detection. DPD irregularly detects dead IKE peers. When the local end sends an IPSec packet, DPD checks the time the last IPSec packet was received from the peer. If the time exceeds the DPD interval, it sends a DPD hello to the peer. If the local end receives no	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
ICMP Detection Server	Enter the IP address or domain name or remote server. Router will ping this address/domain name to check that if the current connectivity is active.	Null
ICMP Detection Local IP	Set the local IP address.	Null
ICMP Detection Interval	Set the ping interval time.	30
ICMP Detection Timeout	Set the ping timeout.	5
ICMP Detection Retries	If Router ping the preset address/domain name time out continuously for Max Retries time, it will try to re-establish the VPN tunnel.	3

IPsec Basic

IPsec Tunnel

X.509

Authentication Manage

Select Cert Type:

None ▼

Authentication Status

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

X.509 @ IPsec

Item	Description	Default
Select Cert Type	Select the IPsec tunnel which the certification used for.	Null
CA	Click "Browse" to select the correct CA file from your PC, and then click "Import" to import it to the router. Click "Export" you can export the CA file from router to your PC.	Null
Remote Public Key	Click "Browse" to select the correct Remote Public Key file from your PC, and then click "Import" to import it to the router. Click "Export" you can export the Remote Public Key file from router to your PC.	Null
Local Public Key	Click "Browse" to select the correct Local Public Key file from your PC, and then click "Import" to import it to the router.	Null

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

3.20 Configuration -> Open VPN

This section allows users to set the Open VPN parameters.

Client **Server** **X.509**

Client

Tunnel name	Description
<div>Add</div>	

Client

☒ Enable OpenVPN Client

Protocol: UDP

Remote IP Address:

Port: 1194

Interface: tun

Authentication: None

Local IP: 10.8.0.2

Remote IP: 10.8.0.1

☐ Enable NAT

Ping Interval: 20

Ping-Restart: 120

Compression: LZO

Encryption: BF-CBC

MTU: 1500

Max Frame Size: 1500

Verbose Level: ERR

Expert Options:

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

Local Route

Subnet

Subnet Mask

Add

Client @ Open VPN		
Item	Description	Default
Enable	Enable OpenVPN Client, the max tunnel account is 3	Null
Protocol	Select from "UDP" and "TCP Client" which depends on the application.	UDP
Remote IP Address	Enter the remote IP address or domain name of remote side OpenVPN server.	Null
Port	Enter the listening port of remote side OpenVPN server.	1194
Interface	Select from "tun" and "tap" which are two different kinds of device interface for OpenVPN. The difference between tun and tap device is this: a tun device is a virtual IP point-to-point device and a tap device is a virtual Ethernet device.	tun
Authentication	Select from four different kinds of authentication ways: "Pre-shared", "Username/Password", "X.509 cert" and "X.509 cert+user".	None
Local IP	Define the local IP address of OpenVPN tunnel.	10.8.0.2
Remote IP	Define the remote IP address of OpenVPN tunnel.	10.8.0.1

Enable NAT	Tick to enable NAT Traversal for OpenVPN. This item must be enabled when router under NAT environment.	Disable
Ping Interval	Set ping interval to check if the tunnel is active.	20
Ping -Restart	Restart to establish the OpenVPN tunnel if ping always timeout during this time.	120
Compression	Select "LZO" to use the LZO compression library to compress the data stream.	LZO
Encryption	<p>Select from "BF-CBC", "DES-CBC", "DES-EDE3-CBC", "AES128-CBC", "AES192-CBC" and "AES256-CBC".</p> <p>BF-CBC: Uses the BF algorithm in CBC mode and 128-bit key.</p> <p>DES-CBC: Uses the DES algorithm in CBC mode and 64-bit key.</p> <p>DES-EDE3-CBC: Uses the 3DES algorithm in CBC mode and 192-bit key.</p> <p>AES128-CBC: Uses the AES algorithm in CBC mode and 128-bit key.</p> <p>AES192-CBC: Uses the AES algorithm in CBC mode and 192-bit key.</p> <p>AES256-CBC: Uses the AES algorithm in CBC mode and 256-bit key.</p>	BF-CBC
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1500
Max Frame Size	Set the Max Frame Size for transmission.	1500
Verbose Level	Select the log output level which from low to high: "ERR", "WARNING", "NOTICE" and "DEBUG". The higher level will output more log information.	ERR
Expert Options	You can enter some other PPP initialization strings in this field. Each string can be separated by a space.	Null
Subnet&Subnet Mask@Local Route	Set the subnet and subnet Mask of local route.	Null

Client

Server

X.509

Enable OpenVPN Server

☒ Enable OpenVPN Server

VPN Server Tunnel

Tunnel name: OpenVPN_Tunnel_1
Listen IP:
Protocol: UDP
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: LZ0
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
<i>*Static Route: <1.1.1.0/24> or <1.1.1.0/24;2.2.0.0/16></i>					
<div>Add</div>					

Server @ Open VPN

Item	Description	Default
Enable OpenVPN Server	Tick to enable OpenVPN server tunnel.	Disable
Tunnel name	Name the OpenVPN server tunnel.	Tunnel_OpenVPN_0
Listen IP	You can enter the IP address of cellular WAN, Ethernet WAN or Ethernet LAN. Null or 0.0.0.0 stands for using the active WAN link currently-cellular WAN or Ethernet WAN.	0.0.0.0
Protocol	Select from "UDP" and "TCP Client" which depends on the application.	UDP
Port	Set the local listening port	1194

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

Client	Server	X.509
--------	--------	--------------

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
CA	Click "Browse" to select the correct CA file from your PC, and then click "Import" to import it to the router. Click "Export" you can export the CA file from router to your PC.	Null
Public Key	Click "Browse" to select the correct Public Key file from your PC, and then click "Import" to import it to the router. Click "Export" you can export the Public Key A file from router to your PC.	Null
Private Key	Click "Browse" to select the correct Private Key file from your PC, and then click "Import" to import it to the router. Click "Export" you can export the Private Key file from router to your PC.	Null
DH	Click "Browse" to select the correct DH A file from your PC, and then click "Import" to import it to the router. Click "Export" you can export the DH file from router to your PC.	Null
TA	Click "Browse" to select the correct TA file from your PC, and then click "Import" to import it to the router. Click "Export" you can export the TA file from router to your PC.	Null
CRL	Click "Browse" to select the correct CRL file from your PC, and then click "Import" to import it to the router. Click "Export" you can export the CRL file from router to your PC.	Null
Pre-Share Static Key	Click "Browse" to select the correct Pre-Share Static Key file from your PC, and then click "Import" to import it to the router. Click "Export" you can export the Pre-Share Static Key file from router to your PC.	Null

3.21 Configuration -> GRE

This section allows users to set the GRE parameters.

GRE

GRE

Tunnel name

Description

Add

GRE

☒ Enable

Remote IP Address:

Local Virtual IP:

Remote Virtual IP:

Remote Subnet:

Remote Subnet Mask:

☐ All traffic via this interface☐ Enable NAT

Secrets:

GRE		
Item	Description	Default
Add	Click "Add" to add a GRE tunnel.	
Enable	Click to enable GRE (Generic Routing Encapsulation). GRE is a protocol that encapsulates packets in order to route other protocols over IP networks.	Disable
Remote IP Address	Set remote IP Address of the virtual GRE tunnel.	Null
Local Virtual IP	Set local IP Address of the virtual GRE tunnel.	Null
Remote virtual IP	Set remote IP Address of the virtual GRE tunnel.	Null
Remote Subnet	Add a static route to the remote side's subnet so that the remote network is known to the local network.	Null
Remote Subnet Mask	Set remote subnet net mask.	Null
All traffic via this interface	After click to enable this feature, all data traffic will be sent via GRE tunnel.	Disable
Enable NAT	Tick to enable NAT Traversal for GRE. This item must be enabled when router under NAT environment.	Disable
Secrets	Set Tunnel Key of GRE.	Null

3.22 Configuration -> L2TP

This section allows users to set the L2TP parameters.

L2TP Client**L2TP Server****L2TP Client**

Tunnel name

Description

Add

L2TP Client☒ Enable

Remote IP Address:

Username:

Password:

Authentication:

Auto ▼

☒ Enable NAT☒ All traffic via this interface☒ Enable Tunnel Authentication

Tunnel secret:

☒ Show Advanced

Port:

1701

Local IP:

Remote IP:

☒ Address/Control Compression☒ Protocol Field Compression

Asyncmap Value:

ffffffff

MRU:

1500

MTU:

1436

Link Detection Interval (s):

30

Link Detection Max Retries:

5

Expert Options:

noccp nobsdcomp

L2TP Client @ L2TP

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

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

L2TP Client

L2TP Server

Enable L2TP Server

☒ Enable L2TP Server

L2TP Common Settings

Username:
Password:
Authentication: CHAP ▾
☒ Enable Tunnel Authentication
Tunnel secret:
Local IP:
IP Pool Start:
IP Pool End:

L2TP Server Advanced

☒ Show L2TP Server Advanced
☒ Address/Control Compression
☒ Protocol Field Compression
Port:
Asyncmap Value:
MRU:
MTU:
Link Detection Interval (s):
Link Detection Max Retries:
Expert Options:

Route Table List

Client IP	Remote Subnet	Remote Subnet Mask
<i>0.0.0.0 means any</i>		

Add

L2TP Server @ L2TP

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

IP Pool End	Set the IP pool end IP address which will assign to the L2TP clients.	10.0.0.100
Show L2TP Server Advanced	Tick to show the L2TP server advanced setting.	Disable
Address/Control Compression	Used for PPP initialization. In general, you need to enable it as default.	Enable
Protocol Field Compression	Used for PPP initialization. In general, you need to enable it as default.	Enable
Asyncmap Value	One of the L2TP initialization strings. In general, you don't need to modify this value.	ffffff
MRU	Maximum Receiving Unit. It is the identifier of the maximum size of packet, which is possible to receive in a given environment.	1500
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1436
Link Detection Interval	Specify the interval between L2TP client and server. To check the connectivity of a tunnel, the client and server regularly send PPP Echo to each other. If the client or server receives no response from the peer within a specified period of time, it retransmits the PPP echo. If it receives no response from the peer after transmitting the PPP echo for max retries times, it considers that the L2TP tunnel is down and tries to re-establish a tunnel with the peer.	30
Link Detection Max Retries	Specify the max retries times for L2TP link detection.	5
Expert Options	You can enter some other PPP initialization strings in this field. Each string can be separated by a space.	noccp nobsdcomp
Route Table List	Click "Add" to add a route rule from L2TP server to L2TP client.	Null

3.23 Configuration -> PPTP

This section allows users to set the PPTP parameters.

PPTP Client

PPTP Server

PPTP Client

Tunnel name	Description
<div>Add</div>	

PPTP Client

☒ Enable

Remote IP Address:

Username:

Password:

Authentication:

☒ Enable NAT

☒ Enable MPPE

☒ All traffic via this interface

☒ Show Advanced

Local IP:

Remote IP:

☒ Address/Control Compression

☒ Protocol Field Compression

Asyncmap Value:

MRU:

MTU:

Link Detection Interval (s):

Link Detection Max Retries:

Expert Options:

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

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

PPTP Client
PPTP Server

Enable PPTP Server
☒ Enable PPTP Server

PPTP Common Settings
Username:
Password:
Authentication: CHAP
Local IP: 10.0.0.1
IP Pool Start: 10.0.0.2
IP Pool End: 10.0.0.100
☒ Enable MPPE

PPTP Server Advanced
☒ Show PPTP Server Advanced
☒ Address/Control Compression
☒ Protocol Field Compression
Asyncmap Value: ffffffff
MRU: 1500
MTU: 1436
Link Detection Interval (s): 30
Link Detection Max Retries: 5
Expert Options: noccp nobsdcomp

Route Table List

Client IP	Remote Subnet	Remote Subnet Mask
*0.0.0.0" means any		

Add

PPTP Server @ PPTP

Item	Description	Default
Enable PPTP Server	Tick to enable PPTP server.	Disable
Username	Set the username which will assign to PPTP client.	Null
Password	Set the password which will assign to PPTP client.	Null
Authentication	Select from "PAP", "CHAP", "MS-CHAP v1" and "MS-CHAP v2". PPTP client need to select the same authentication method based on this server's authentication method.	CHAP
Local IP	Set the IP address of PPTP server.	10.0.0.1
IP Pool Start	Set the IP pool start IP address which will assign to the PPTP clients.	10.0.0.2
IP Pool End	Set the IP pool end IP address which will assign to the PPTP clients.	10.0.0.100
Enable MPPE	Tick to enable MPPE (Microsoft Point-to-Point Encryption). It's a protocol for encrypting data across PPP and VPN links.	Disable
Show PPTP Server	Tick to show the PPTP server advanced setting.	Disable

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

3.24 Configuration -> SNMP

This section allows users to set the SNMP parameters.

Basic

View

VACM

Trap

SNMP Basic Settings

☒ Enable SNMP

Port:

Agent Mode:

Version:

Location Info:

Contact Info:

System Name:

Basic @ SNMP

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

Basic

View

VACM

Trap

Mib View List

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

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

Add

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

SNMPv1&v2 User List

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

*Network: 1.1.1.0/24, 0.0.0.0 means 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

Trap

SNMP Trap Settings☒ Enable SNMP Trap

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

3.25 Configuration -> VRRP

This section allows users to set the VRRP parameters.

VRRP

VRRP Settings☒ Enable VRRP

Group ID:

1

Priority:

100

Interval (s):

10

Virtual IP:

192.168.0.1

VRRP

Item	Description	Default
Enable VRRP	Tick to enable VRRP protocol. VRRP (Virtual Router Redundancy Protocol) is an Internet protocol that provides a way to have one or more backup routers when using a statically configured router on a local area network (LAN). Using VRRP, a virtual IP address can be specified manually.	Disable
Group ID	Specify which VRRP group of this router belong to.	1
Priority	Enter the priority value from 1 to 255. The larger value has higher priority.	100
Interval	The interval that master router sends keepalive packets to backup routers.	10
Virtual IP	A virtual IP address is shared among the routers, with one designated as the	192.168.0.

	master router and the others as backups. In case the master fails, the virtual IP address is mapped to a backup router's IP address. (This backup becomes the master router.)	1
--	---	---

3.26 Configuration -> IP Passthrough

In IP Passthrough mode, 3G Industrial VPN Pro 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

IP 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
Enable IP Passthrough	Tick to enable IP Passthrough feature.	Disable
Mode	User can only select "PPPoE" mode at present.	PPPoE
Ethernet Interface	PPPoE client dials up to 3G Industrial VPN Pro (PPPoE server) corresponding to different LAN interface. For example when you connect PPPoE client (such as PC) to LAN 0 through Ethernet cable, PC will dial up to 3G Industrial VPN Pro (PPPoE server) through LAN 0.	LAN_0
Username	Set the username of PPPoE server.	Null
Password	Set the password of PPPoE server.	Null
AC Name	Set the AC (Access Concentrator) name of PPPoE server.	Null
Service Name	Set the service name of PPPoE server. Note: PPPoE client needs to set the same username, password, service name of PPPoE server, or it cannot succeed to dial up to PPPoE server.	Null
Authentication	Set the different PPP authentication from "Auto", "PAP", "CHAP". Auto: Automatic detection.	Auto

	PAP: Password Authentication Protocol CHAP: Challenge Response Protocol	
Link Detection Interval(s)	When PPPoE client dial up to 3G Industrial VPN Pro (PPPoE server), 3G Industrial VPN Pro will send "LCP Echo Request" to PPPoE client after this interval. "Link Detection Interval" ranges from 3 to 30 times.	30
Link Detection Max Retries	If 3G Industrial VPN Pro re-sends "LCP Echo Request" packet continuously for Max Retries times and still do not receive correct respond packets from PPPoE client, it will send "LCP Terminal Request" packet to disconnect the connection between PPPoE server and PPPoE client. "Max Retries" ranges from 3 to 5 times.	5

3.27 Configuration -> AT over IP

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

AT over IP

AT Settings

☒ Enable AT Settings

Protocol:

Local IP:

Local Port:

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

3.28 Configuration -> Phone Book

This section allows users to set the Phone Book parameters.

Phone Book

Phone Group

Phone Book Configuration

Description	Phone No.

X

*1. Make sure you enter mobile destination number in the international format, for instance for SMS to US mobile phone: +12342342342 (+1 is the international code for US, use this and then your normal number without the first zero).

*2. In some countries, only can send/receive SMS without international code for the number.

Phone Book

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

Phone Book

Phone Group

Phone Group Configuration

Group Name	Phone List

Group No. And Description

Group Name:

Add or remove the phone no. to/from group

Not in this group

In this group



All



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

3.29 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 connect
- ☐ Send SMS on PPP disconnect

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

SMS Control

☒ Enable

Password Content:

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

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

3.30 Configuration -> Reboot

This section allows users to set the Reboot policies.

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
Click to add PhoneGroup!

SMS Reply Content:

Time

Call

SMS

SMS Reboot Configuration

☒ Enable SMS Reboot

Phone Group:

NULL
Click to add PhoneGroup!

Password:

SMS Reply Content:

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

SMS Reply Content	Send reply short message after auto SMS reboot from specified Caller ID (e.g. Reboot ok!). Note: Only support text format SMS.	Null
-------------------	--	------

3.31 Configuration -> RobustLink

This section allows users to configure parameters about RobustLink, which is an industrial-grade centralized management and administration system for the R3G Industrial VPN Pro. It allows you to monitor, configure and manage large numbers of remote devices on a private network over the web.

RobustLink

RobustLink Settings

☒ Enable RobustLink

Server Address:

Port:

Password:

RobustLink		
Item	Description	Default
Enable RobustLink	Click to enable RobustLink feature.	Disable
Server address	Enter IP address of RobustLink.	Null
Port	Enter port number of RobustLink.	1883
Password	Enter the password preset in RobustLink. <i>Note: The passwords set in R3G Industrial VPN Pro and RobustLink need to be the same.</i>	Null

3.32 Configuration -> Syslog

This section allows users to set the syslog parameters.

Syslog

Syslog Settings

Save Position:

Log Level:

Keep Days:

☒ Log to Remote System

Remote IP:

Remote UDP Port:

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

3.33 Configuration -> Event

This section allows users to set the Event parameters.

Event

Event Settings

☒ Enable Event

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

Event		
Item	Description	Default
Enable Event	Click to enable Event feature. This feature is used to report R3G Industrial VPN Pro’s main running event to SNMP-TRAP or RobustLink. There are numbers of Event code you can select, such as “BOOT-UP”, “3G-UP”, “3G-DOWN”, etc. For example if you click “3G-UP” and select “RobustLink” as the server, when R3G Industrial VPN Pro dial up to	Disable

	connect to 3G network, it will send event code “3G-UP” as well as relevant information to RobustLink.	
--	---	--

3.34 Configuration -> USR LED

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

Note: Please refer to “Status” -> “System” -> “LEDs Information” -> “USR”.

USR LED

USR LED

USR LED Type:

Indication:

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

3.35 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: ▼

☐ Copy settings from current profile to selected profile

[Change](#)

All Parameters XML Configuration

XML File: [Browse...](#) [Import](#) [Export](#)

IPsec XML Configuration

IPsec XML File: [Browse...](#) [Import](#) [Export](#)

OpenVPN XML Configuration

OpenVPN XML File: [Browse...](#) [Import](#) [Export](#)

Restore to Factory Default Settings

[Restore to Factory Default Settings](#)

Profile		
Item	Description	Default
Profile	This item allow users store different configuration profiles into different positions; or save one configuration profile into different positions just for configuration data backup. Selected from "Standard", "Alternative 1", "Alternative 2", "Alternative 3".	Standard
XML Configuration	Import: Click "Browse" to select the XML file in your computer, then click "Import" to import this file into your router. Export: Click "Export" and the configuration will be showed in the new popup 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

3.36 Administration -> Tools

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

Ping	AT Debug	Traceroute	Sniffer	Test
Ping				
Ping IP address:		<input type="text"/>		
Number of requests:		<input type="text" value="5"/>		
Timeout (s):		<input type="text" value="1"/>		
Local IP:		<input type="text"/>		
<input type="button" value="Start"/> <input type="button" value="Stop"/>				

Ping @ Tools

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

Ping	AT Debug	Traceroute	Sniffer	Test
Send AT Commands				
<input type="text"/>				
<input type="button" value="Send"/>				
Receive AT Commands				

AT Debug @ Tools

Item	Description	Default
Send AT Commands	Enter the AT commands which you need to send to cellular module in this box.	Null

Send	Click this button to send the AT commands.	Null
Receive AT Commands	Router will display the AT commands which respond from the cellular module in this box.	Null

Ping
AT Debug
Traceroute
Sniffer
Test

Traceroute

Trace Address:
Trace Hops:
Timeout (s):

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

Ping
AT Debug
Traceroute
Sniffer
Test

Sniffer

Interface: all
Host:
Protocol: all
Start Stop

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

Ping	AT Debug	Traceroute	Sniffer	Test
Test				
Enable	Description	Result		
<input checked="" type="checkbox"/>	USB Test			
<input checked="" type="checkbox"/>	Flash Test			
<input checked="" type="checkbox"/>	Memory Test			
<input checked="" type="checkbox"/>	Ethernet Test			
<input checked="" type="checkbox"/>	SIM1 Test			
<input checked="" type="checkbox"/>	SIM2 Test			
<input checked="" type="checkbox"/>	Module Test			
Detail				
<input type="button" value="Show Detail"/>				

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

3.37 Administration -> Clock

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

Clock

Timezone Setting
 Timezone: UTC+08:00 China, HK, Western Australia, Singapore, Taiwan, Russia ▼

NTP Settings
☒ Enable NTP Client
 Primary NTP Server: pool.ntp.org
 Secondary NTP Server:
 Update Interval (h): 1
☒ Enable NTP Server

Clock		
Item	Description	Default
Timezone	Select your local time zone.	UTC +08:00
Primary NTP Server	Enter primary NTP Server's IP address or domain name.	pool.ntp.org
Secondary NTP Server	Enter secondary NTP Server's IP address or domain name.	Null
Update interval (h)	Enter the interval which NTP client synchronize the time from NTP server.	1
Enable NTP Server	Click to enable the NTP server function of router.	Disable

3.38 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...

Private Key:

Browse...

Import

Export

Basic @ Web Server		
Item	Description	Default
HTTP Port	Enter the HTTP port number you want to change in 3G Industrial VPN Pro's Web Server.	80

	On a Web server, port 80 is the port that the server "listens to" or expects to receive from a Web client. If you configure the router with other HTTP Port number except 80, only adding that port number then you can login 3G Industrial VPN Pro's Web Server.	
HTTPS Port	<p>Enter the HTTPS port number you want to change in 3G Industrial VPN Pro's Web Server.</p> <p>On a Web server, port 443 is the port that the server "listens to" or expects to receive from a Web client. If you configure the router with other HTTPS Port number except 443, only adding that port number then you can login 3G Industrial VPN Pro's Web Server.</p> <p>Note: <i>HTTPS is more secure than HTTP. In many cases, clients may be exchanging confidential information with a server, which needs to be secured in order to prevent unauthorized access. For this reason, HTTP was developed by Netscape corporation to allow authorization and secured transactions.</i></p>	443
X.509 @ Web Server		
HTTPS Certificate	In this tab, user can import or export "Public Key" and "Private Key" for HTTPS certification.	Null

3.39 Administration -> User Management

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

Super	Common
User Management	
Username:	<input type="text" value="admin"/>
Old Password:	<input type="text"/>
New Password:	<input type="text"/>
Confirm Password:	<input type="text"/>
Login Parameters	
Login Timeout (s):	<input type="text" value="1800"/>

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

Super

Common

User Management

Access Level

Username

Password

Add

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

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

Chapter 4. Configuration Examples

4.1 Interface

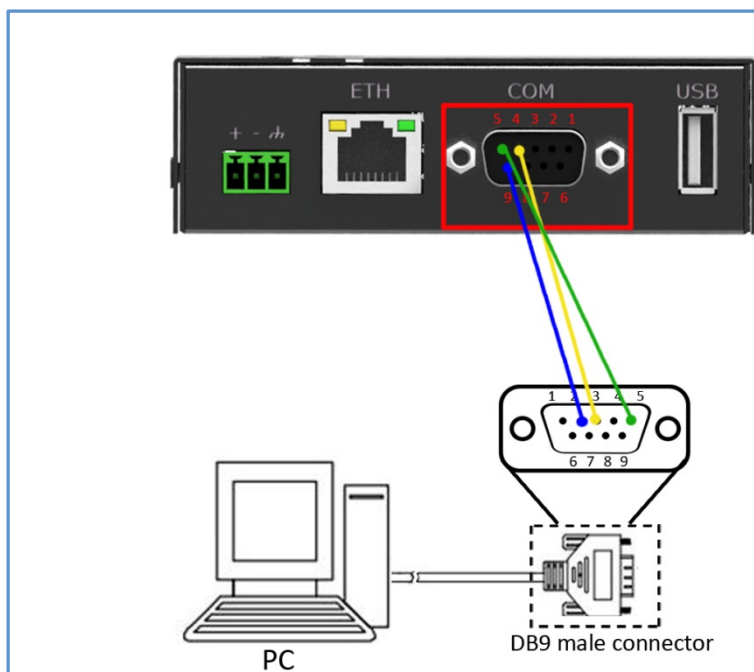
DB9 Female Connector

PIN	Debug	RS232	RS485 (2-wire)	Direction
1			Data+ (A)	-
2		RXD		R3G Industrial VPN Pro → Device
3		TXD		Device → R3G Industrial VPN Pro
4	DRXS			Device → R3G Industrial VPN Pro
5	GND	GND		-
6			Data- (B)	-
7		RTS		Device → R3G Industrial VPN Pro
8		CTS		R3G Industrial VPN Pro → Device
9	DTXD			R3G Industrial VPN Pro → Device

4.1.1 Console port

User can use the console port to manage the router via CLI commands.

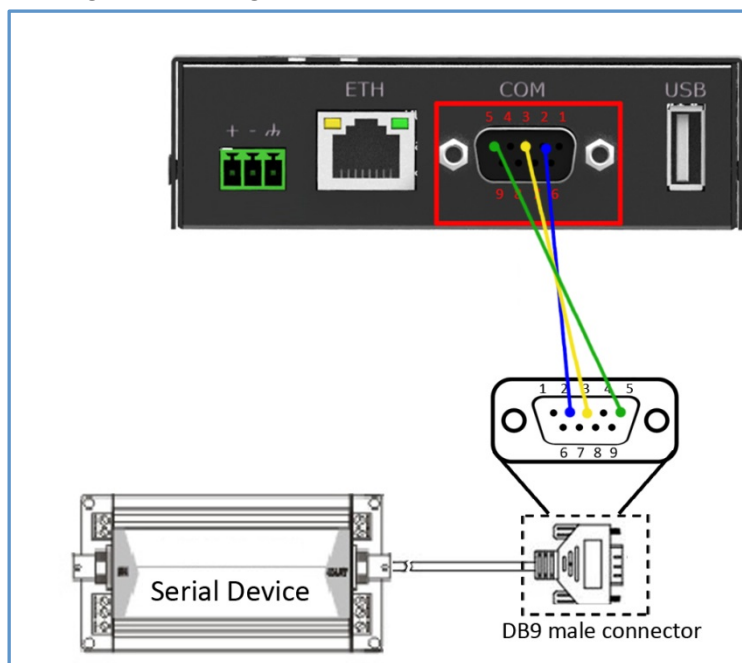
Please check section Introductions for CLI.



4.1.2 RS232

R3G Industrial VPN Pro supports one RS232 for serial data communication.

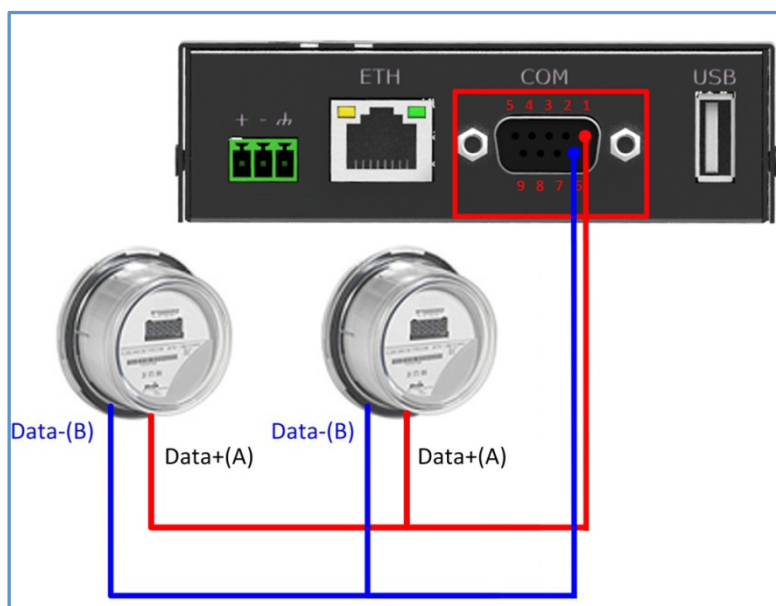
Please refer to the connection diagram at the right site.



4.1.3 RS485

R3G Industrial VPN Pro 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”.

1. Always Online

Configuration-->Cellular WAN -->Basic

Cellular Settings		
Status:	SIM1 Not inserted	SIM2 Not inserted
Network Provider Type:	Custom ▾	Custom ▾
APN:	<input type="text"/>	<input type="text"/>
Username:	<input type="text"/>	<input type="text"/>
Password:	<input type="text"/>	<input type="text"/>
Dialup No.:	*99***1#	*99***1#
PIN Type:	None ▾	None ▾

Connection Mode	
Connection Mode:	Always Online ▾
Redial Interval (s):	<input type="text" value="30"/>
Max Retries:	<input type="text" value="3"/>
ICMP Detection Primary Server:	<input type="text" value="8.8.8.8"/>
ICMP Detection Secondary Server:	<input type="text" value="8.8.4.4"/>
ICMP Detection Interval (s):	<input type="text" value="30"/>
ICMP Detection Timeout (s):	<input type="text" value="3"/>
ICMP Detection Retries:	<input type="text" value="3"/>
<input checked="" type="checkbox"/> Reset The Interface	

Dual SIM Policy	
Main SIM Card:	SIM1 ▾
<input checked="" type="checkbox"/> Switch To Backup SIM Card When Connection Fails	
<input type="checkbox"/> Switch To Backup SIM Card When ICMP Detection Fails	
<input type="checkbox"/> Switch To Backup SIM Card When Roaming Is Detected	
<input type="checkbox"/> Switch To Backup SIM Card When Data Limit Is Exceeded	
<input type="checkbox"/> Switch Back Main SIM Card After Timeout	

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-->Cellular WAN -->Basic

Cellular Settings

	SIM1	SIM2
Status:	Not inserted	Not inserted
Network Provider Type:	Custom	Custom
APN:		
Username:		
Password:		
Dialup No.:	*99***1#	*99***1#
PIN Type:	None	None

Connection Mode

Connection Mode: Connect On Demand

Redial Interval (s): 30

Max Retries: 3

Inactivity Time (s): 0

Serial Output Content (Hex):

☒ Triggered By Serial Data

☒ Triggered By Tel

☒ Triggered By SMS

SMS Connect Command:

SMS Disconnect Command:

SMS Connect Reply:

SMS Disconnect Reply:

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

☒ Periodically Connect

Periodically Connect Interval (s): 300

Time Schedule: NULL

Time Range

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

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

R3G Industrial VPN Pro supports remote control via SMS. User can use following commands to get the status of R3G

Industrial VPN Pro, cannot set new parameters of R3G Industrial VPN Pro 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

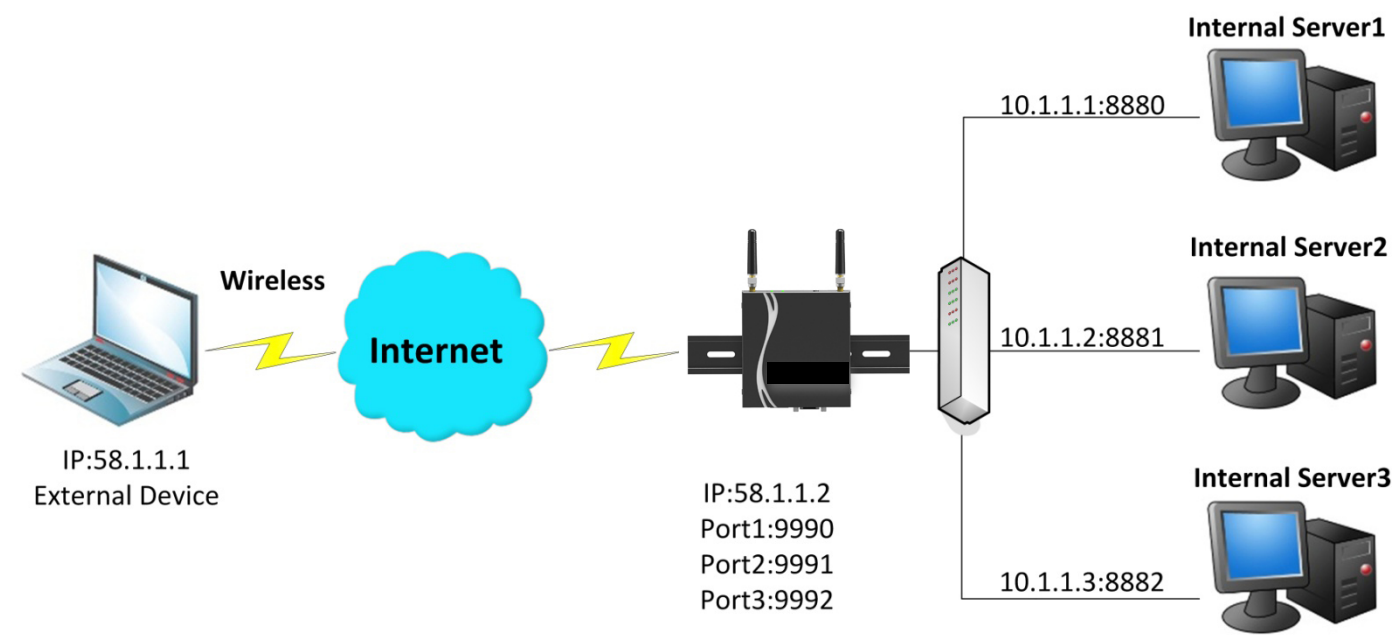
In this command, password is 1234, 0001 is the command to reset R3G Industrial VPN Pro.

Cmd	Description	Syntax	Comments
Control Commands			
0001	Reset Device	cmd	if no password, please use command "cmd", or use command" password: cmd" cmd1 + cmd2: cmd1;cmd2 * - means can be null
0002	Save Parameters	cmd	
0003	Save Parameters and Reset Device	cmd	
0004	Start PPP Dialup	cmd	
0005	Stop PPP	cmd	
0006	Switch Sim Card	cmd	
0007	Clear SIM Card's Data Limitation	cmd,simNumber	simNumber: 1 - SIM_1 2 - SIM_2
0011	Check Cellular status and IP Address.	cmd	

4.3 Network

4.3.1 NAT

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



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

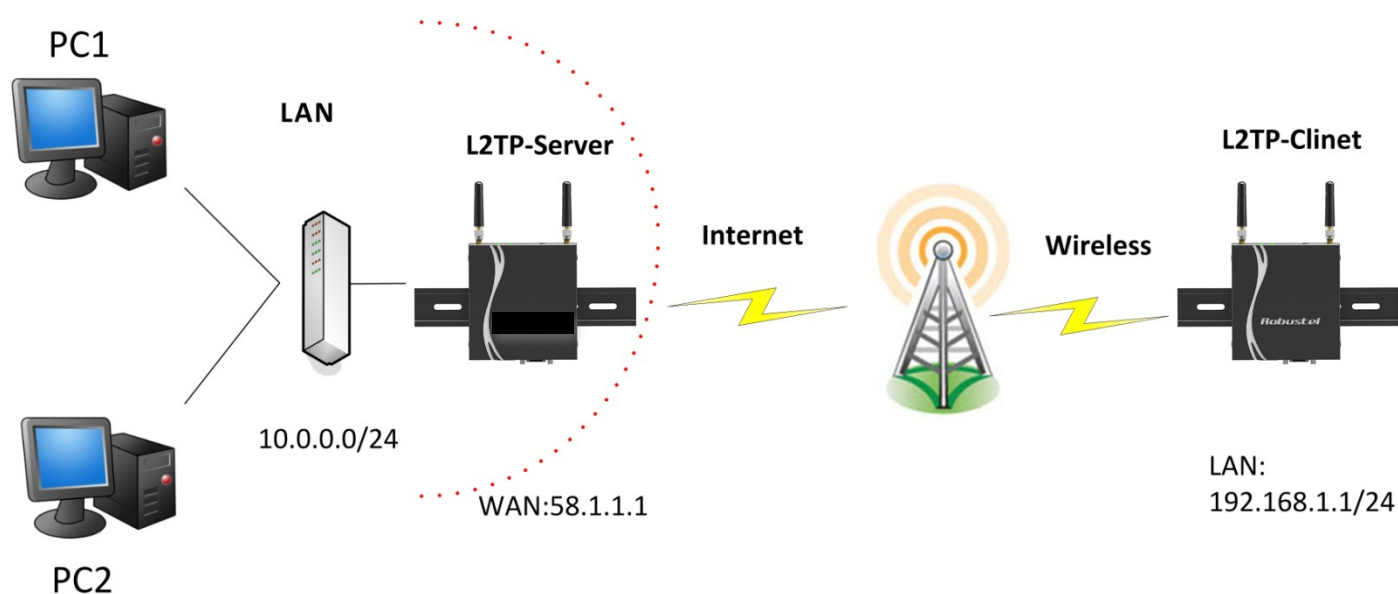
Port Forwarding					
Remote IP	Arrives At Port	Is Forwarded to IP Address	Is Forwarded to Port	Protocol	
58.1.1.1	9990	10.1.1.1	8880	TCP	X
58.1.1.1	9991	10.1.1.2	8881	UDP	X
58.1.1.1	9992	10.1.1.3	8882	TCP&UDP	X
*Remote IP: 1.1.1.1, 1.1.1.0/24,1.1.1.1-2.2.2.2, 0.0.0.0 means any					Add
*Arrives At Port: <1-65536> or <1-65536>-<1-65536>					

Explanations for above diagram:

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

58.1.1.1	-----access to----->	58.1.1.2:9990	-----be forwarded to----->	10.1.1.1:8000	TCP
58.1.1.1	-----access to----->	58.1.1.2:9991	-----be forwarded to----->	10.1.1.2:8001	UDP
58.1.1.1	-----access to----->	58.1.1.2:9992	-----be forwarded to----->	10.1.1.3:8002	TCP&UDP

4.3.2 L2TP



L2TP_SERVER:

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

Enable L2TP Server

☐ Enable L2TP Server

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

L2TP Common Settings

Username: **1**

Password: **2**

Authentication: **3**

☐ Enable Tunnel Authentication

Local IP:

IP Pool Start:

IP Pool End:

L2TP Server Advanced

☐ Show L2TP Server Advanced

Route Table List

Client IP	Remote Subnet	Remote Subnet Mask	
0.0.0.0	192.168.1.0	255.255.255.0	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

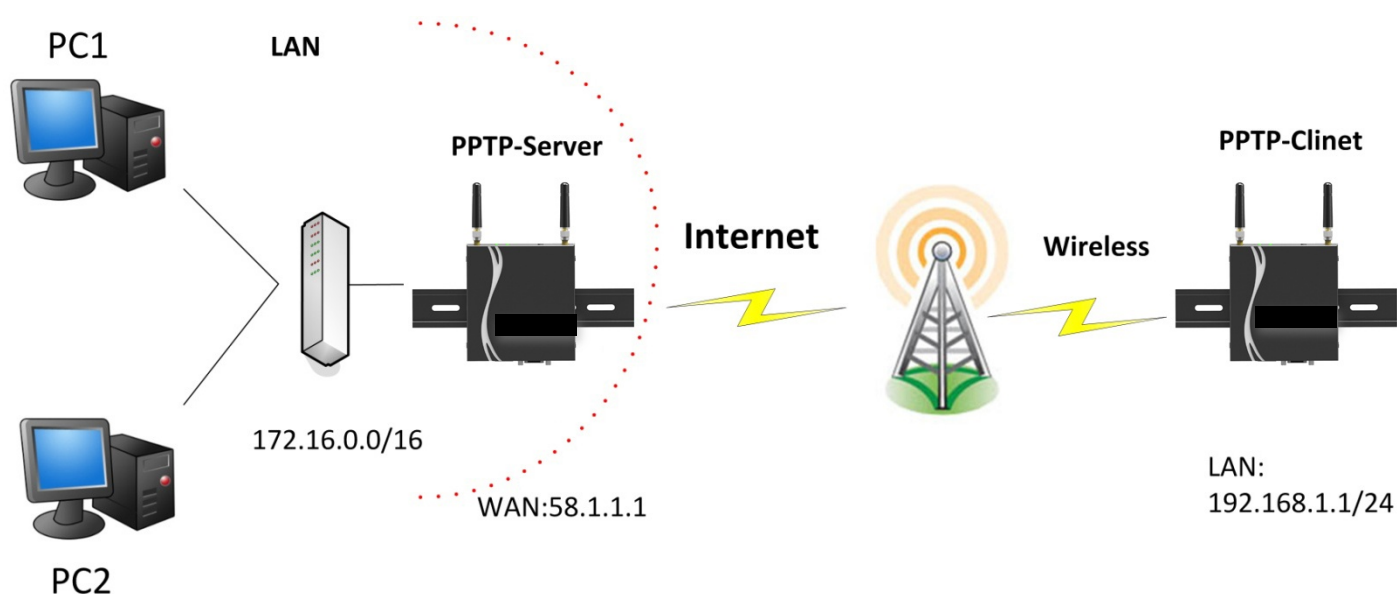
Click “Add” button, and fill in the blank textbox

L2TP Client X

<input checked="" type="radio"/> Enable	<input type="radio"/> Disable	
Server Name:	<input type="text" value="58.1.1.1"/>	
Username:	<input type="text" value="l2tp"/>	1
Password:	<input type="password" value="••••"/>	2
Authentication:	<input type="text" value="PAP"/>	3
<input type="checkbox"/> Enable Tunnel Authentication		
Remote Subnet:	<input type="text" value="10.0.0.0"/>	
Remote Subnet Mask:	<input type="text" value="255.255.255.0"/>	
<input type="checkbox"/> Show L2TP Client Advanced		

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 Settings

Username:	<input type="text" value="pptp"/>	1
Password:	<input type="password" value="••••"/>	2
Authentication:	<input type="text" value="PAP"/>	3
Local IP:	<input type="text" value="10.0.0.1"/>	
IP Pool Start:	<input type="text" value="10.0.0.2"/>	
IP Pool End:	<input type="text" value="10.0.0.254"/>	

☐ Enable MPPE

PPTP Server Advanced
☐ Show PPTP Server Advanced

Route Table List

Client IP	Remote Subnet	Remote Subnet Mask	
<input type="text" value="0.0.0.0"/>	<input type="text" value="192.168.1.0"/>	<input type="text" value="255.255.255.0"/>	<input type="button" value="X"/>

**0.0.0.0" means any*

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

PPTP_CLIENT:

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

Please add PPTP Client

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

PPTP Client X

☒ Enable
 ☐ Disable

Server Name: 58.1.1.1

Username: pptp

Password: ••••

Authentication: PAP

Remote Subnet: 172.16.0.0

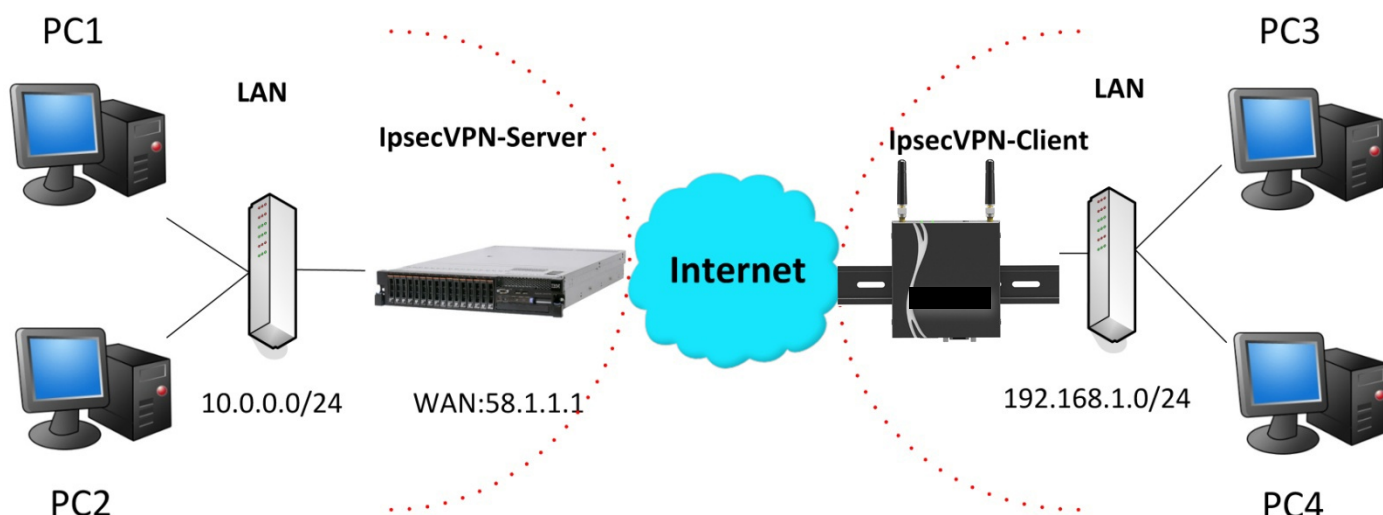
Remote Subnet Mask: 255.255.0.0

☐ Enable MPPE

☐ Show PPTP Client Advanced

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

4.3.4 IPSEC VPN



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

IPsecVPN_SERVER:

Cisco 2811:

```

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

```

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

IPsecVPN_CLIENT:

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

IPsec Basic	
<input checked="" type="checkbox"/>	Enable NAT Traversal
Keepalive Interval(s):	<input type="text" value="30"/>

Then click "Apply".

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

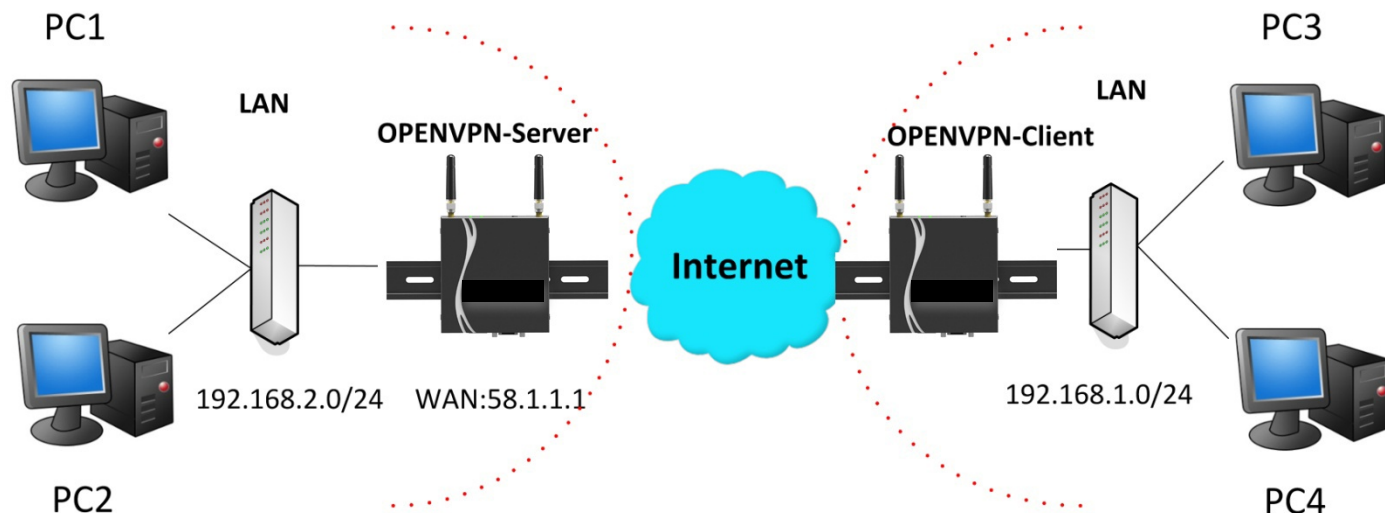
IPsec Tunnel	
<input type="text" value="Tunnel name"/>	<input type="text" value="Description"/>
<input type="button" value="Add"/>	

Tick "Enable IPsec Tunnel1"

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

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

4.3.5 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: UDP **1**
 Port: 1194 **2**
 Interface: tun **3**
 Authentication: None **4**
 Local IP: 10.8.0.1 **5**
 Remote IP: 10.8.0.2 **6**
☒ Enable NAT **7**
 Ping Interval: 20
 Ping-Restart: 120
 Compression: LZO **8**
 Encryption: BF-CBC **9**
 MTU: 1500 **10**
 Max Frame Size: 1500 **11**
 Verbose Level: ERR
 Expert Options: --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 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 OpenVPN Client ✖

☒ Enable
 ☐ Disable

Tunnel name:

Protocol: 1

Server Address:

Port: 2

Interface: 3

Authentication: 4

Local IP: 6

Remote IP: 5

☒ Enable NAT 7

Ping Interval:

Ping-Restart:

Compression: 8

Encryption: 9

MTU: 10

Max Frame Size: 11

Verbose Level:

Expert Options:

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

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

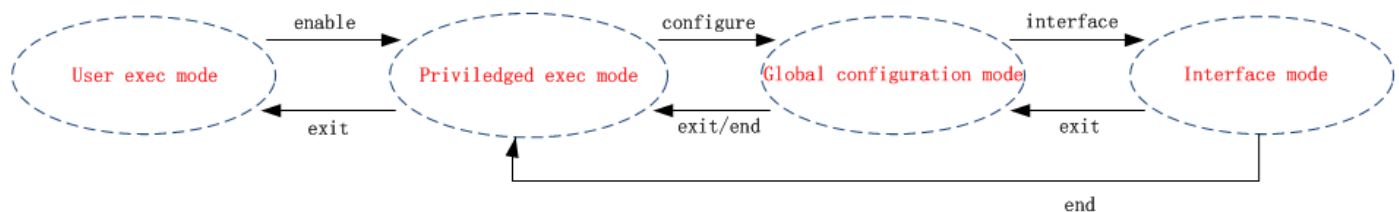
Chapter 5. Introductions for CLI

5.1 What's CLI and hierarchy level Mode

The R3G Industrial VPN Pro command-line interface (CLI) is a software interface providing another way to set the parameters of equipment from the console or through a telnet network connection. Before using them better a few of details will be introduced on four different CLI hierarchy level modes which have different access rights:

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

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



USER EXEC MODE:

3G Industrial VPN Pro Configure Environment

Username: admin

Password: *****

3G Industrial VPN Pro> ?

//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
telnet	Startup a telnet client shell
tracert	Tracert test
show	Show running system information

PRIVILEGED EXEC MODE:

3G Industrial VPN Pro> enable

Password: ***** //type "admin"

3G Industrial VPN Pro# ? //check what commands can be used in **Privileged exec mode**

debug	Debug configure information
enable	Turn on privileged commands
exit	Exit from current mode
export	Export file using tftp
syslog	Export system log
import	Import file using tftp
load	Load configure information
ping	Ping test
reload	Halt and perform a cold restart
telnet	Startup a telnet client shell
module-at	module at test
sniffer	catch network traffic
tracert	Tracert test
write	Write running configuration
wpadebug	set wpa_suppllicant debug level
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:

3G Industrial VPN Pro# configure

3G Industrial VPN Pro(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:

3G Industrial VPN Pro(config)# interface Ethernet 0

3G Industrial VPN Pro(config-e0)# ? //check what commands can be used in **interface mode**

exit	Exit from current mode
end	Exit to Normal mode
ip	Set the IP address of an interface
mtu	Set the IP address of an interface

5.2 How to configure the CLI

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

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

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

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

5.2.1 Quick Start 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

3G Industrial VPN Pro> show version

software version : 1.01.01-sub-131211 Dec 11 2013 18:58:20

kernel version : v2.6.39-5 PREEMPT Mon Dec 9 09:49:58 HKT 2013

hardware version : 1.00.03

Example 2: Update firmware via tftp

```
3G Industrial VPN Pro> enable
Password: *****
3G Industrial VPN Pro#
3G Industrial VPN Pro# tftp 172.16.3.3 get rootfs R3k.1.01.01-sub-131211.01.fs

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

Example 3: Set IP address for Eth0

```
3G Industrial VPN Pro> enable
Password: *****
3G Industrial VPN Pro # configure
3G Industrial VPN Pro (config) # set eth0
ethernet interface type: LAN
->IP address [192.168.0.1]:172.16.1.231                         //set IP address for eth0
->Netmask [255.255.255.0]:255.255.0.0
->mtu value (1024-1500)[1500]:
```

this parameter will be take effect when reboot!

really want to modify[yes]:

```
3G Industrial VPN Pro (config) # end
3G Industrial VPN Pro# write                                     //save current configuration
Building configuration...
OK
3G Industrial VPN Pro # reload
! Reboot the system? 'yes' or 'no': yes                         //reload to take effect
```

Example 4: CLI for Cellular dialup

```
3G Industrial VPN Pro> enable
Password: *****
3G Industrial VPN Pro# configure
3G Industrial VPN Pro (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[]:

PIN mode:

1. input only
2. PIN locked
3. PIN unlocked

->please select mode(1-3)[1]:

->pin code[]:

->PUK[]:

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]:

->ICMP detection primary server[8.8.8.8]:

->ICMP detection second server[8.8.4.4]:

->ICMP detection interval(1-1800)[30]:

->ICMP detection timeout(1-10)[3]:

->ICMP detection retries(1-20)[3]:

->reset the interface?'yes'or'no'[yes]:

main SIM select:

1. Auto
2. SIM_1
3. SIM_2

->please select mode(1-3)[2]:

->when connect fail?'yes'or'no'[yes]:

->when ICMP Detection fails fails?'yes'or'no'[no]:

->when roaming is detected?'yes'or'no'[no]:

->month date limitation?'yes'or'no'[no]:

->Call back Main SIM card after timeout?'yes'or'no'[no]:

->show advanced options?'yes'or'no'[no]:

this parameter will be take effect when reboot!

really want to modify[yes]:3G Industrial VPN Pro(config)# end

3G Industrial VPN Pro# write

//save current configuration

Building configuration...

OK

3G Industrial VPN Pro# 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 :

pin code : NULL

connection Mode : Always online

redial interval : 30 seconds

max connect try : 3

ICMP primary server : 8.8.8.8

ICMP second server : 8.8.4.4

ICMP detection interval : 30 seconds

ICMP detection timeout : 3 seconds

ICMP detection retries : 3

reset the interface : yes

main SIM select : SIM_1

when connect fail : yes

when roaming is detected : no

month date limitation : no

SIM phone number :

network select Type : Auto

authentication type : AUTO

mtu value : 1500

mru value : 1500

asyncmap value : 0xffffffff

use peer DNS : yes

primary DNS : 0.0.0.0

secondary DNS : 0.0.0.0

address/control compressio: yes

protocol field compression: yes

expert options : nccp nobsdcomp

3G Industrial VPN Pro# reload

!Reboot the system ?'yes'or 'no':yes

//reload to take effect

5.3 Commands reference

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

CERTIFICATE OF WARRANTY

Dear Customer,

We are pleased to inform you that a EU directive concerning the sale and the warranty of consumer goods has been implemented in the Italian constitution through the Law Decree n. 24 of 2nd February 2002.

This directive distinguishes between consumption goods for exclusive use in private environment and the ones used in professional environment.

In particular the new regulation is applied only to the consumption goods for private use so that consumption goods used in the own professional or business activity will be guaranteed according to the legal regulation on the sale considered by the civic code.

In both cases Digicom, considering the quality of its own products, applies a period of warranty of 24 months.

In order to distinguish the type of use, the till receipt will be used as evidence of exclusive private use, while in case of purchase with invoice the warranty will be executed according to regulations considered by professional or business use.

A) Management of warranty with till receipt (Consumer)

Given that the Directive 1999/44/CE represents the achievement of a high protection level of the consumer, the decree regulates some aspects concerning the sale contract between **Consumer and Seller** as well as the warranties concerning the consumption goods object of the sale.

For the Law Decree:

- **the Consumer** is any physical person that buys consumption goods to be used exclusively in private environment and then outside the own professional or business activity;
- **the Seller** is any physical or legal, public or private person that uses one of the above mentioned contracts in its own business or professional activity
- **the consumption good** is any movable asset with the express exclusion of forced sale assets; water and gas when not packaged for sale in a limited volume or set quantity.

The Consumer has legal rights according to applicable national legislation governing the sale of consumption goods. The guarantee does not affect those rights.

The warranty is valid in all the Member States of the European Union.

Under the new law, any claim under warranty from the Consumer must be advanced to the dealer and/or to the point of sale where the product has been purchased.

B) Management of warranty with invoice (Professional use)

The warranty of Digicom products purchased with invoice (professional use) must be asked directly to the Reseller/Company or to the Distributor where the products has been purchased.

For any request of technical assistance and in order to integrate the information contained in the User's Manual of the product you purchased and to offer you a better service, we recommend you to visit the "SUPPORT" area of our website at <http://www.digicom.it> where you will find many information and suggestions useful for the configuration, the upgrade, eventual new configurations (always evolving) of the products and the resolution the most common problems.

Furthermore manuals, drivers and firmware upgrades are available on Digicom website.

WARRANTY CLAUSES

- The product is under warranty for a period of 24 (twenty-four) months from the date of purchase.

Digicom undertakes to remedy any defects, lack of quality or non-conformity of the product as stated in the sale contract (and generally in the information on the products) with the repair or the replacement of the product without charging any expense for the labor and for the material.

- The warranty is effective only in case the request for repair under warranty comes with the valid proof of the purchase (receipt or invoice). The broken product must be delivered in the original package with all the accessories.

- The serial number on the product must not be cancelled or erased in any way; failing this condition the purchaser's right to claim for the warranty will be forfeited.

- The warranty is not applicable in case of damages caused by negligence, improper installation/use/care, tampering, modifications of the product or of the serial number, damages due to accidental causes or to the negligence of the customer, particularly referred to the external parts.

Furthermore the warranty is not applicable in case of fault due to wrong connections (i.e. a voltage different from the one indicated on the product) or due to a sudden change in the network voltage to which the product is connected, as well as in case of fault caused by infiltration of liquids, fire, inductive/electrostatic discharges or discharges caused by lightnings, overvoltage or other phenomenon not depending on the device.

- The parts of the product subject to wear and tear are not covered by the warranty, like the battery when supplied, the connection cables, the connectors, the external parts and the plastic support, unless they present a factory defect.

- Periodical controls, software updates, settings and maintenance are not under warranty.

- When the warranty period expires, the replaced parts, the expenses for labor and transportation will be invoiced according to the current rates.

- The warranty of Digicom products must be required directly to the Reseller/Company or to the Distributor where the product has been purchased.



Digicom S.p.A.

Italy - Via Alessandro Volta 39
21010 Cardano al Campo -VA

Tel +39/0331/702611 Fax +39/0331/263733

<http://www.digicom.it>