NOVUS AirGate-3G

Dual SIM Industrial Cellular VPN Router

For GPRS/UMTS/HSPA Networks

User Manual

V1.0x C

About This Document

This document describes hardware and software of NOVUS AIRGATE-3G, Dual SIM Industrial 2G/3G Router.

Trademarks and Permissions

NOVUS are trademark of NOVUS Produtos Eletrônicos LTDA.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Disclaimer

No part of this document may be reproduced in any form without the written permission of the copyright owner.

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. NOVUS shall have no liability for any error or damage of any kind resulting from the use of this document.

Technical Support Contact Information

Tel: +55 51 3323-3600
Fax: +55 51 3323-3644
E-mail: support@novusautomation.com
Web: www.novusautomation.com

Important Notice

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

Safety Precautions

General

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

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

Using the router in vehicle

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

Protecting your router

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

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

Regulatory and Type Approval Information

Table 1: Directives

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

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

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

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

Name of the part	Hazardous substances					
	(Pb)	(Hg)	(Cd)	(Cr(VI))	(PBB)	(PBDE)
Metal Parts	o	o	o	o	o	o
Circuit Modules	x	o	o	o	o	o
Cables and Cable Assemblies	o	o	o	o	o	o
Plastic and Polymeric parts	o	o	o	o	o	o
o: Indicates that this toxic or hazardous substance contained in all of the homogeneous materials for this part is below the limit requirement in SJ/T11363-2006. X: Indicates that this toxic or hazardous substance contained in at least one of the homogeneous materials for this part *might exceed* the limit requirement in SJ/T11363-2006.						

Contents

1. PRODUCT CONCEPT

1.1 OVERVIEW

NOVUS AirGate-3G 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.
- WAN link management: cellular WAN/Ethernet WAN backup.
- VPN tunnel: IPSec/OpenVPN/PPTP/L2TP/GRE.
- Supports Modbus gateway (Modbus RTU/ASCII to Modbus TCP).
- Supports GPS&GLONASS (optional), provides real time location and tracking.
- Supports SDK, provides user programmatic interface.
- Supports 802.1Q VLAN Trunk.
- Supports PPPoE Bridge (IP Passthrough).
- Auto reboot via SMS/Caller ID/Timing.
- Supports NovusLink (Centralized M2M management platform, to remote monitor, configure and update firmware).
- Flexible Management methods: Web/CLI/SNMP/NovusLink.
- Firmware upgrade via Web/CLI/USB/SMS/NovusLink.
- Various interfaces: RS232/RS485/Console/DI/DO/USB/Ethernet.
- Wide range input voltages from 9 to 60 VDC and extreme operating temperature.
- The metal enclosure can be mounted on a DIN-rail or on the wall, also with extra ground screw.

1.2 PACKING LIST

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

- NOVUS AirGate-3G router x 1

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

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

- SMA Antenna (Magnet) x 1

- Ethernet cable x 1

- 35mm Din-Rail mounting kit

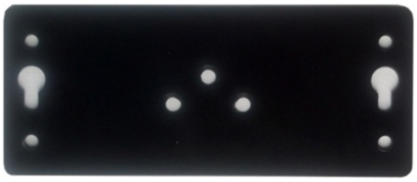
- CD with user guide x 1

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

Optional accessories (purchased separately):

- SMA antenna Stubby - *optional*

- Wall Mounting Kit



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

1.3 SPECIFICATIONS

Cellular Interface

- Standards: GSM/GPRS/EDGE/UMTS/HSPA/EVDO
- GPRS/EDGE: 850/900/1800/1900 MHz
- HSPA+: 850/900/1900/2100 MHz, DL/UL 21/5.76 Mbps, fallback to 2G
- SIM: 2 x (3V & 1.8V)
- Antenna Interface: SMA Female

Ethernet Interface

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

Digital Input

- Type: 2 x DI, Dry Contact
- Dry Contact: On: open, Off: short to GND
- Isolation: 3K VDC or 2K Vrms
- Absolute Maximum VDC: 5V
- Digital Filtering Time Interval: Software selectable
- Interface: 3.5mm terminal block with lock

Digital Output

- Type: 2 x DO, Sink
- Isolation: 3K VDC or 2K Vrms
- Absolute Maximum VDC: 30V
- Absolute Maximum ADC: 300mA
- Interface: 3.5mm terminal block with lock

Serial Interface

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

GPS & GLONASS Interface (Optional)

- Antenna Interface: SMA Female, 50 ohms impedance
- Tracking Sensitivity: GPS: better than -148 dBm
  GLONASS: better than -140 dBm
- Horizontal position accuracy: GPS: 2.5 m
  GLONASS: 4.0 m
- Time-To-First-Fix: GPS: 26 s
  GLONASS: 30 s
- Protocol: NMEA-0183 V2.3

System

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

Software

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

Power Supply and Consumption

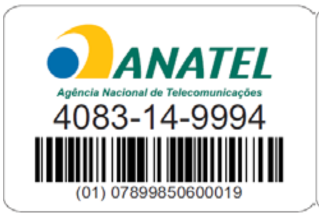
- Power Supply Interface: 5mm terminal block with lock
- Input Voltage: 9 to 60 VDC
- Power Consumption: Idle: 100 mA @ 12 V
  Data Link: 400 mA (peak) @ 12 V

Physical Characteristics

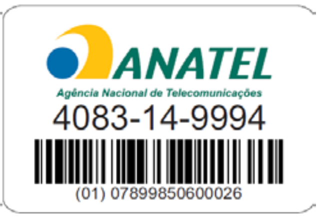
- Housing & Weight: Metal, 500g
- Dimension: (L x W x H): 125 x 108 x 45 mm
- Installation: 35mm Din-Rail or wall mounting or desktop

Regulatory and Type Approvals

- Approval & Detective: ANATEL, CE, R&TTE,FCC, PTCRB, GCF, AT&T, IC,
  Rogers, RCM, CB, E-Mark, NBTC, RoHS, WEEE



ANATEL
Agência Nacional de Telecomunicações
4083-14-9994
(01) 07899850600019



ANATEL
Agência Nacional de Telecomunicações
4083-14-9994
(01) 07899850600026

- EMI : EN 55022 (2006/A1: 2007) Class B
- EMC: EN 61000-4-2 (ESD) Level 4, EN 61000-4-3 (RS) Level 4
  EN 61000-4-4 (EFT) Level 4, EN 61000-4-5 (Surge) Level 3
  EN 61000-4-6 (CS) Level 4, EN 61000-4-8 Level 4

Environmental Limits

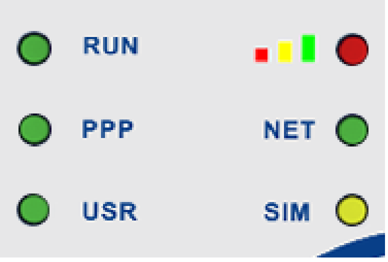
Model No.	Description	Operating Environment
AIRGATE-3G	HSPA+ Router	-40 to 85°C/5 to 95% RH
AIRGATE-3G-GPS	HSPA+ Router & GPS	-40 to 85°C/5 to 95% RH

1.4 SELECTION AND ORDERING DATA

Please refer to corresponding AIRGATE-3G datasheet.

2. INSTALLATION

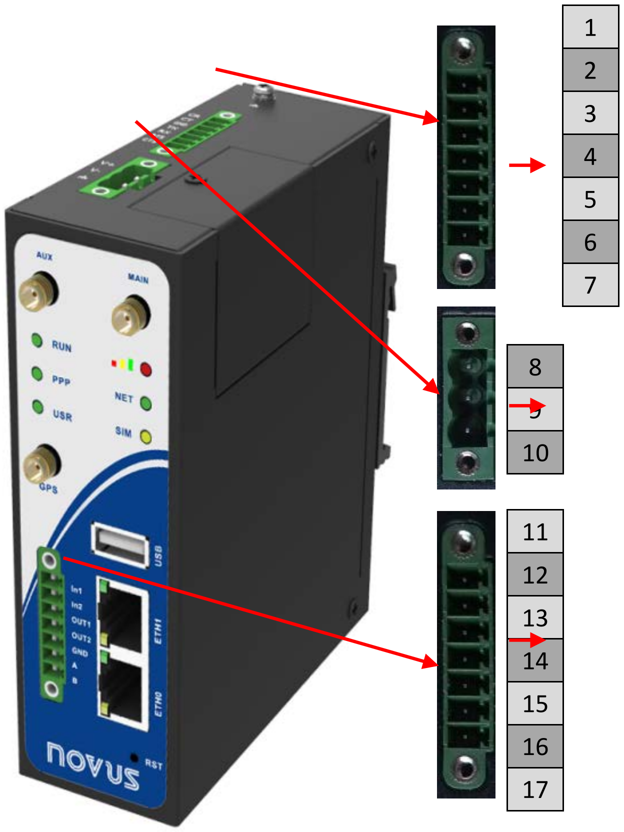
2.1 LED INDICATORS



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

***Note**: User can select display status of USR LED. Please check section 23.37.*

2.2 PIN ASSIGNMENT



PIN	Debug	RS232	Direction
1	RXD		Device →AIRGATE-3G
2	TXD		AIRGATE-3G → Device
3	GND	GND	
4		TXD	AIRGATE-3G → Device
5		RXD	Device →AIRGATE-3G
6		RTS	AIRGATE-3G → Device

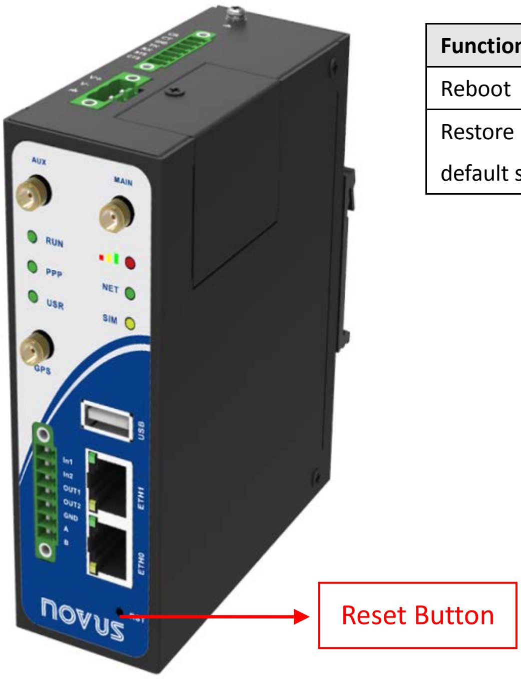
PIN	Power	Digital I/O	RS485
8	Positive		
9	Negative		
10	GND		
11		Input 1	
12		Input 2	
13		Output 1	
14		Output 2	
15		GND	
16			Data+(A)
17			Data- (B)

2.3 USB INTERFACE

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

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

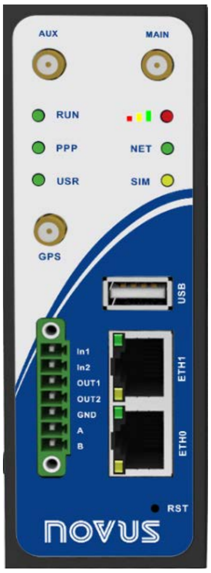
2.4 RESET BUTTON



Function	Operation
Reboot	Push the button for 5 seconds under working status.
Restore to factory default setting	Push the button for 60 seconds once you power on the router until all the LEDs blink at the same time for 5 times.

2.5 ETHERNET PORTS

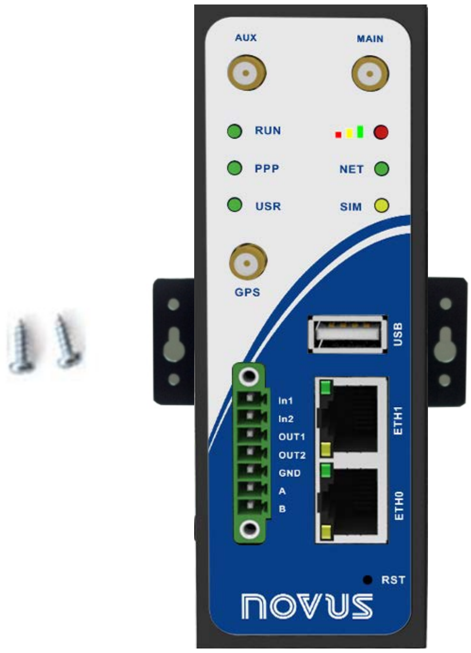
Each Ethernet port has two LED indicators (please check the following picture). The yellow one is **Speed indicator** and the green one is **Link indicator**. There are three status of each indicator. Please refer to the form below.



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

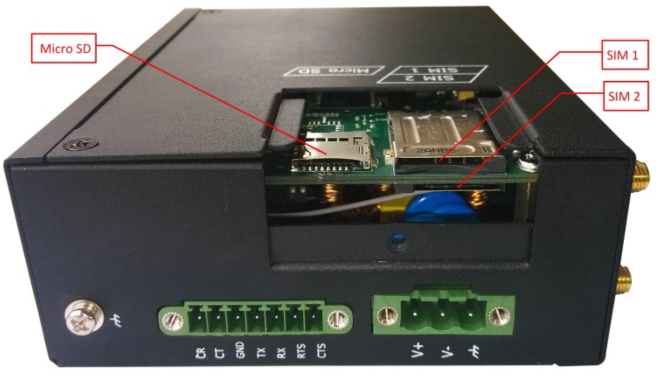
2.6 MOUNT THE ROUTER

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



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

2.7 INSTALL SIM CARD AND MICRO SD CARD



- **Inserting SIM Card or Micro SD Card**

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

- **Removing SIM Card or Micro SD Card**

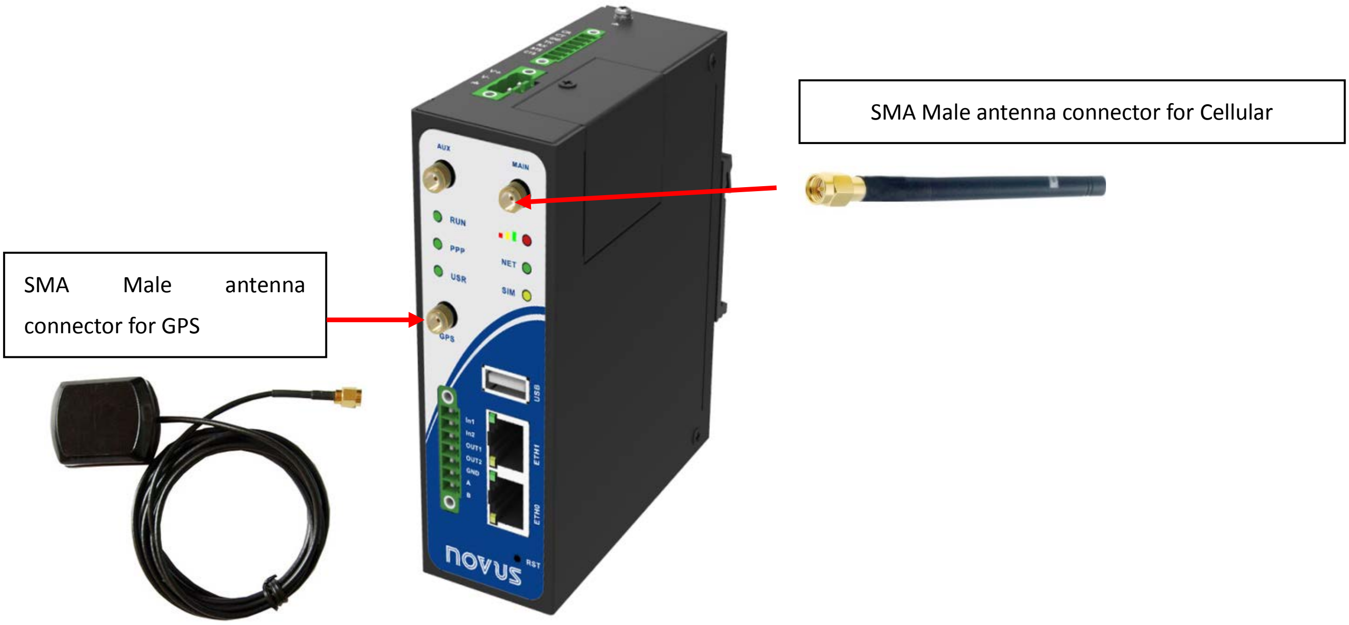
1. Make sure router is power off.
2. Press the card until you hear “a cracking sound”, when the card will pop up to be pulled out.

Note:

1. *Please use the specific M2M SIM card when the device works in extreme temperature (temperature exceeding 0 -40 ℃ because the long-time working of regular SIM card in harsh environment (temperature exceeding 0 - 40℃ may increase the possibility of SIM card failure).*
2. *Don’t forget screw the cover for again-theft.*
3. *Don’t touch the metal surface of the SIM card in case information in the card is lost or destroyed.*
4. *Don’t bend or scratch your SIM card. Keep the card away from electricity and magnetism.*
5. *Make sure router is power off before inserting or removing your SIM card or Micro SD card.*

2.8 CONNECT THE EXTERNAL ANTENNA

Connect router with an external antenna connector. Make sure the antenna is basing on the correct frequency and is screwed tightly.

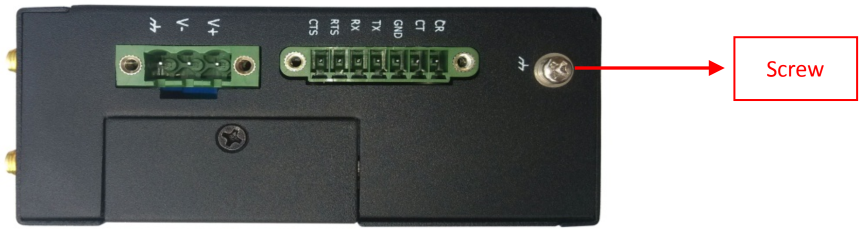


SMA Male antenna connector for Cellular

SMA Male antenna connector for GPS

2.9 GROUND THE ROUTER

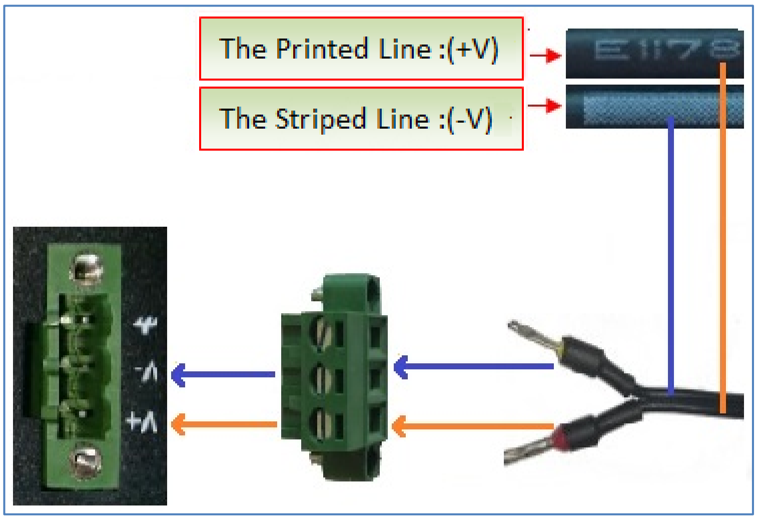
Grounding and wire routing help limit the effects of noise due to electromagnetic interference (EMI). Run the ground connection from the ground screw to the grounding surface prior to connecting devices.



Screw

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

2.10 POWER SUPPLY



The power supply range is 9 to 60 VDC.

Note*: Please take care about the polarity, and do not make reverse connection.* There are two lines connecting to the power supply adapter, as it illustrates on the label. The line printed with letters needs to connect with the positive polarity, and the striped line needs to connect with the negative polarity.

3. CONFIGURATION SETTINGS OVER WEB BROWSER

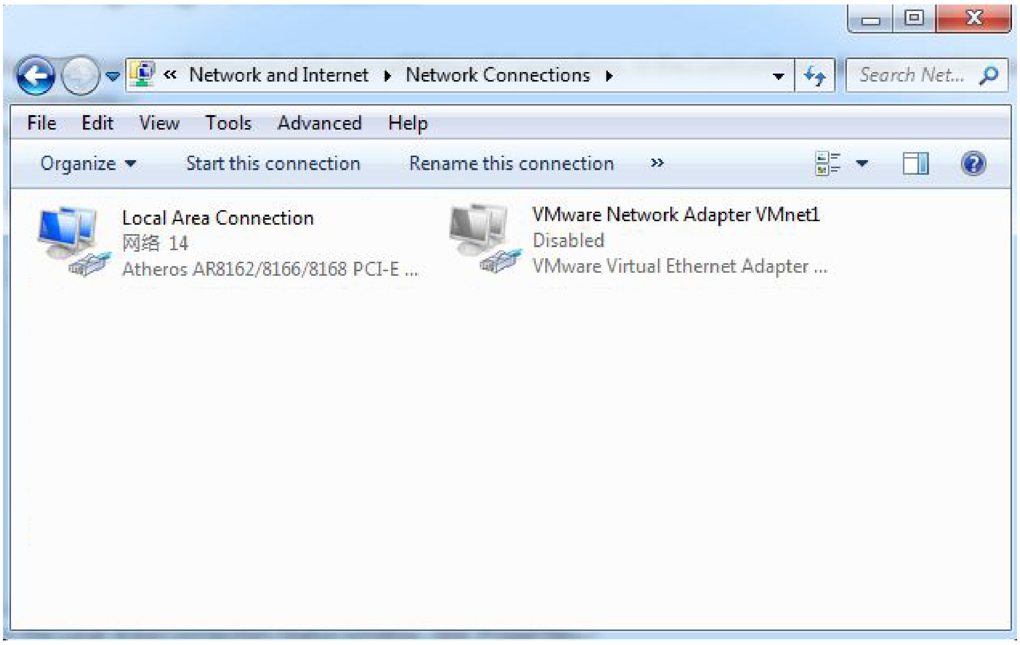
The router can be configured through your web browser. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista/7/8, etc. The product provides an easy and user-friendly interface for configuration.

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

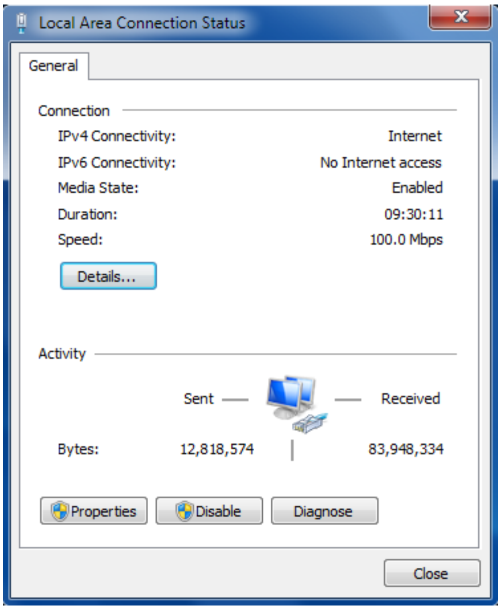
You must configure your PC to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. The best and easiest way is to configure the PC to get an IP address automatically from the router using DHCP. If you encounter any problems accessing the router web interface it is advisable to uninstall your firewall program on your PC, as these tend to cause problems accessing the IP address of the router.

3.1 CONFIGURING PC IN WINDOWS

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


« Network and Internet ▸ Network Connections ▸
Search Net...
File
Edit
View
Tools
Advanced
Help
Organize ▾
Start this connection
Rename this connection
»
Local Area Connection
网络 14
Atheros AR8162/8166/8168 PCI-E ...
VMware Network Adapter VMnet1
Disabled
VMware Virtual Ethernet Adapter ...

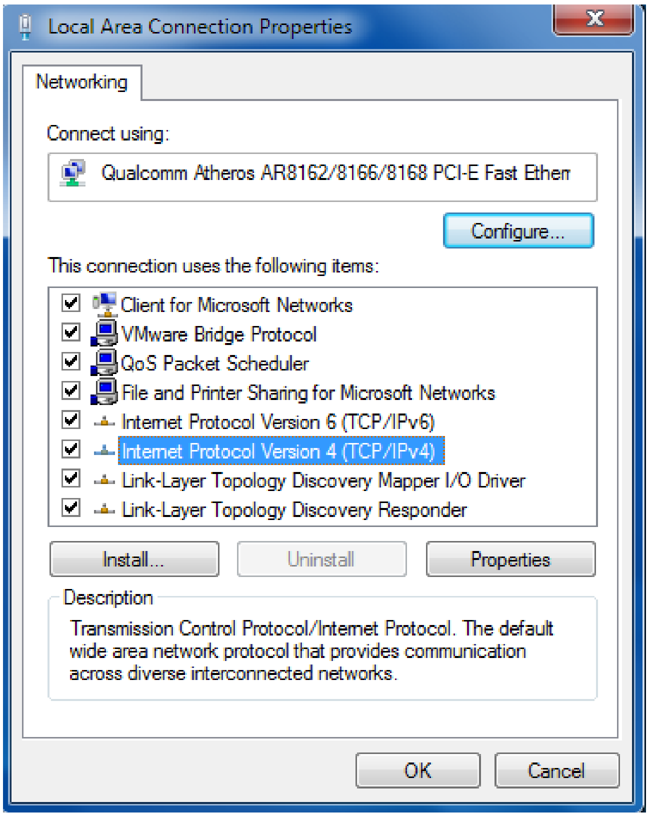
3. In the Local Area Connection Status window, click Properties.



IPv4 Connectivity: Internet
IPv6 Connectivity: No Internet access
Media State: Enabled
Duration: 09:30:11
Speed: 100.0 Mbps

Bytes: Sent 12,818,574 Received 83,948,334

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



Local Area Connection Properties

Networking

Connect using:

Qualcomm Atheros AR8162/8166/8168 PCI-E Fast Ethern

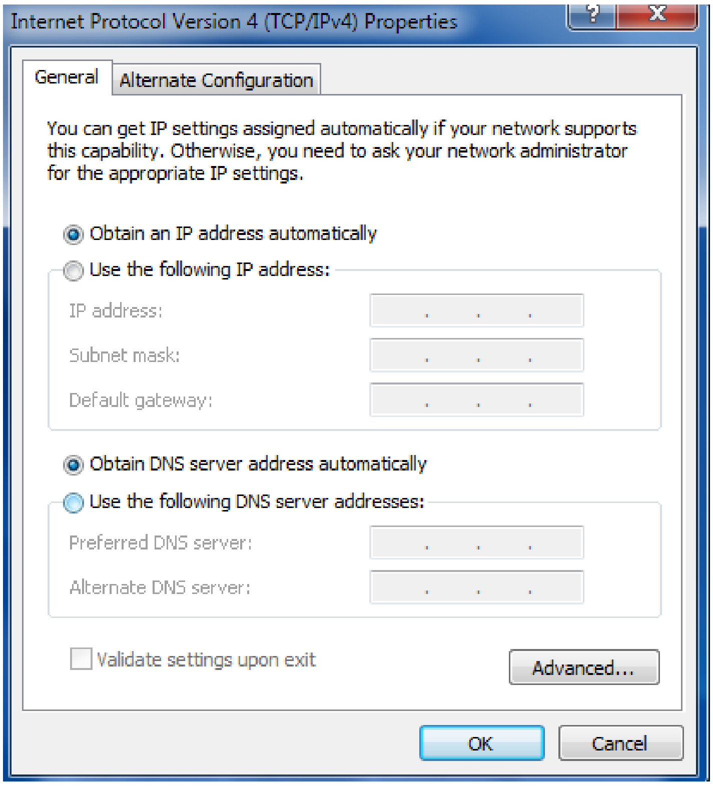
This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ VMware Bridge Protocol
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

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



Internet Protocol Version 4 (TCP/IPv4) Properties

General | Alternate Configuration

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

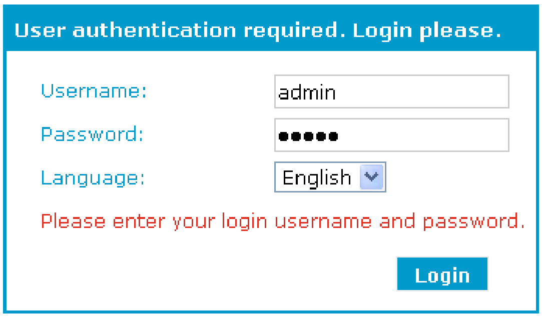
Alternate DNS server: . . .

□ Validate settings upon exit

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: admin

Password: ●●●●●

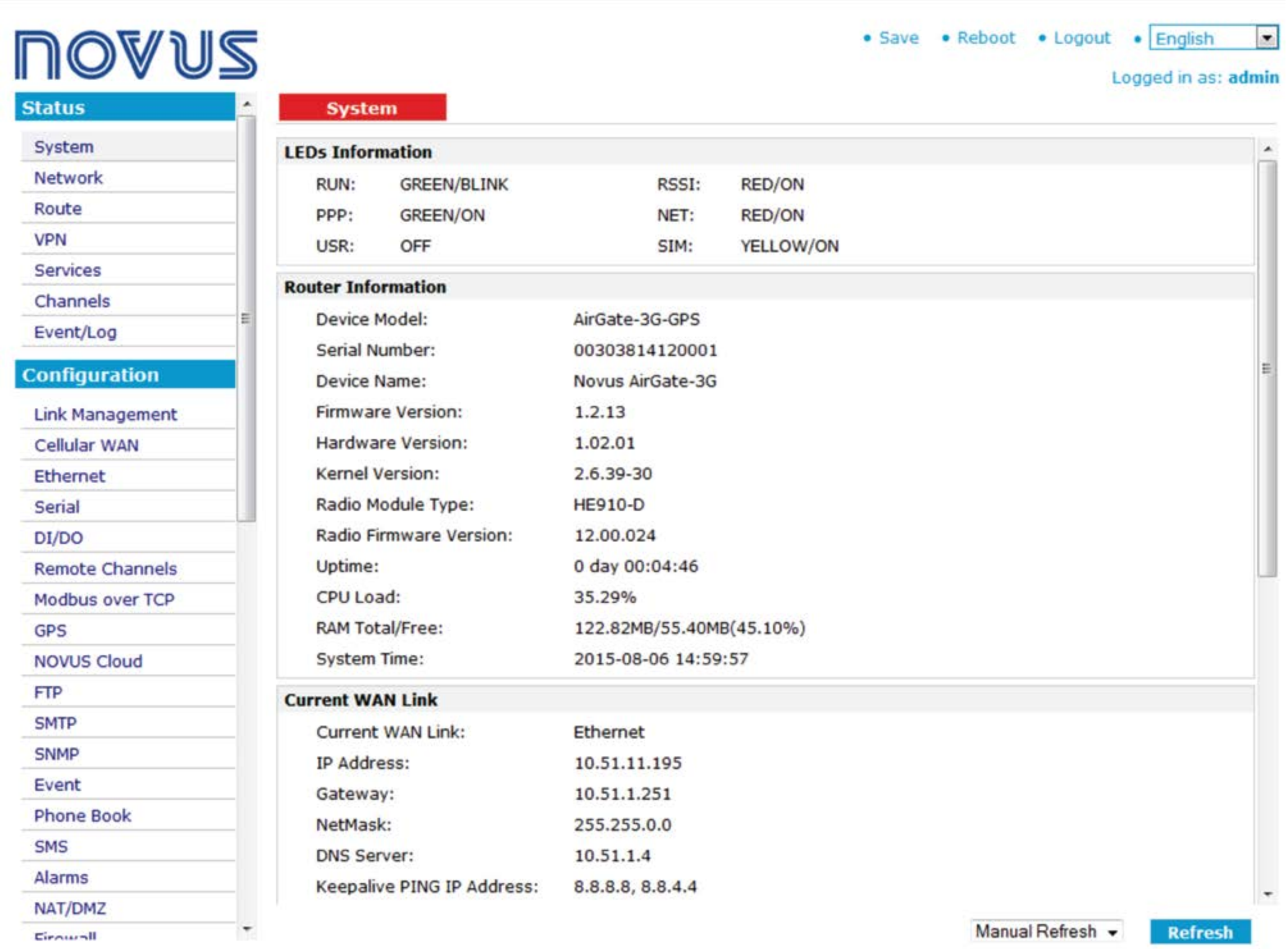
Language: English

Please enter your login username and password.

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

3.3 CONTROL PANEL

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



Logged in as: admin

LEDs Information

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

Router Information

Device Model:	AirGate-3G-GPS
Serial Number:	00303814120001
Device Name:	Novus AirGate-3G
Firmware Version:	1.2.13
Hardware Version:	1.02.01
Kernel Version:	2.6.39-30
Radio Module Type:	HE910-D
Radio Firmware Version:	12.00.024
Uptime:	0 day 00:04:46
CPU Load:	35.29%
RAM Total/Free:	122.82MB/55.40MB(45.10%)
System Time:	2015-08-06 14:59:57

Current WAN Link

Current WAN Link:	Ethernet
IP Address:	10.51.11.195
Gateway:	10.51.1.251
NetMask:	255.255.0.0
DNS Server:	10.51.1.4
Keepalive PING IP Address:	8.8.8.8, 8.8.4.4

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

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

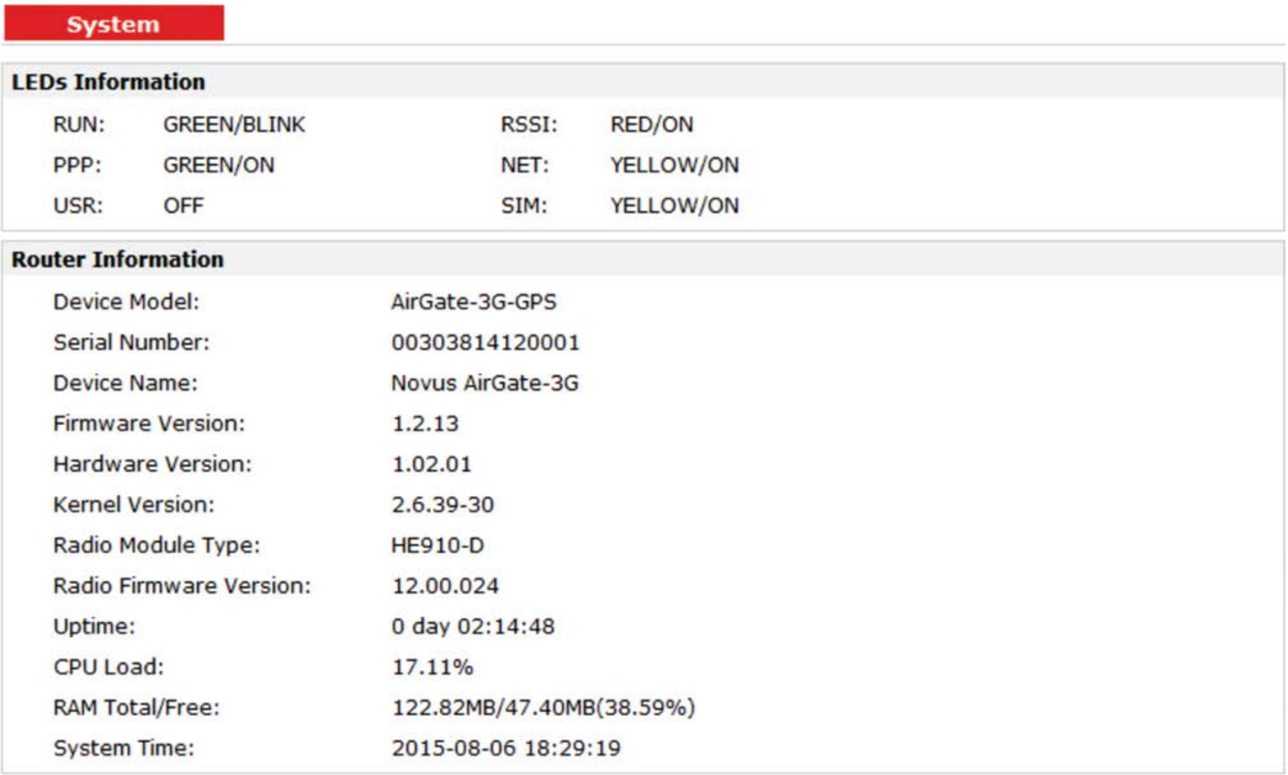
1. *Modify in one page;*
2. *Click* Apply *under this page;*
3. *Modify in another page;*
4. *Click* Apply *under this page;*
5. *Complete all modification;*
6. *Click* • Save *;*
7. *Click* • Reboot *.*

3.4 STATUS -> SYSTEM

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

LEDs Information

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



System

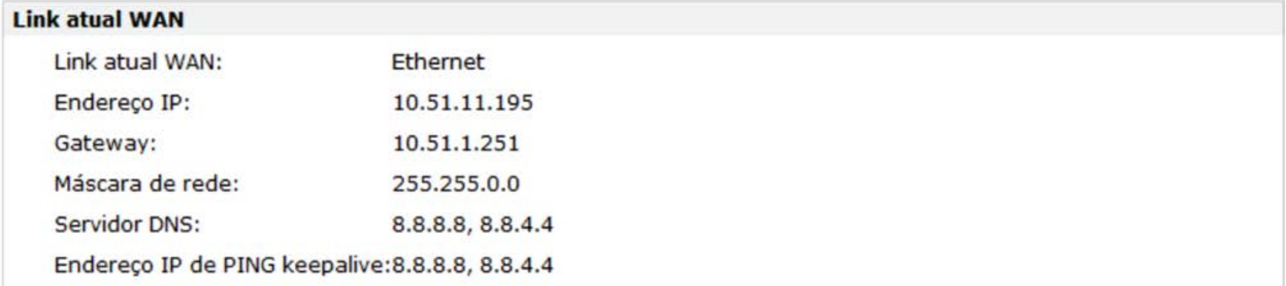
LEDs Information

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

Router Information

Device Model:	AirGate-3G-GPS
Serial Number:	00303814120001
Device Name:	Novus AirGate-3G
Firmware Version:	1.2.13
Hardware Version:	1.02.01
Kernel Version:	2.6.39-30
Radio Module Type:	HE910-D
Radio Firmware Version:	12.00.024
Uptime:	0 day 02:14:48
CPU Load:	17.11%
RAM Total/Free:	122.82MB/47.40MB(38.59%)
System Time:	2015-08-06 18:29:19

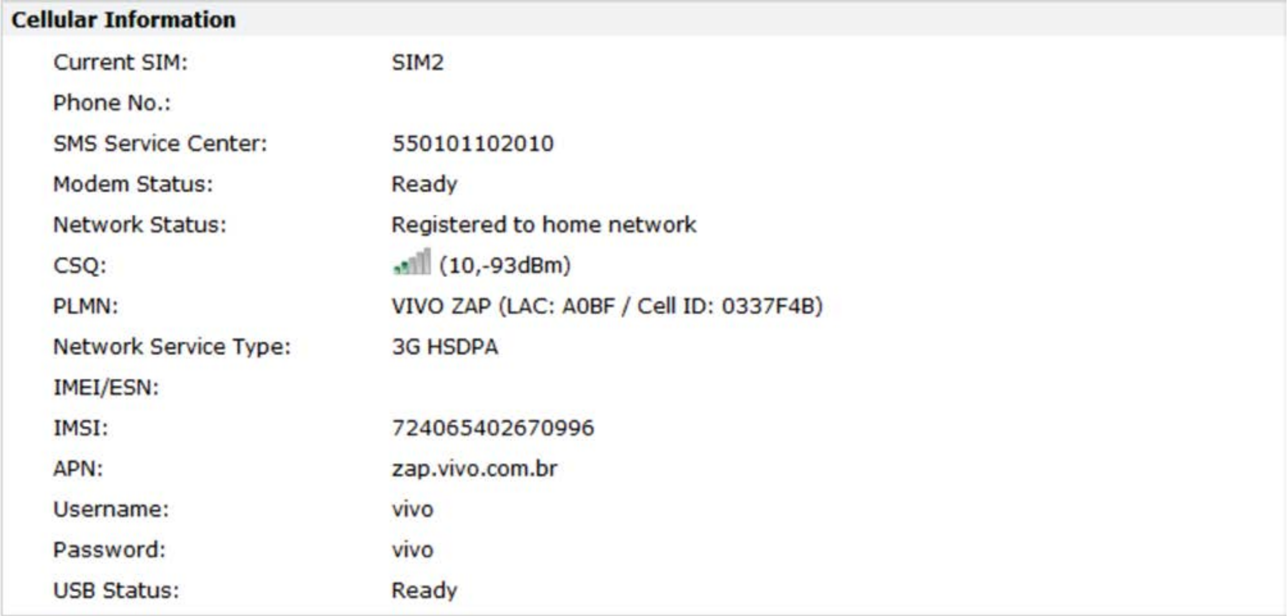
Router Information	
Item	Description
Device Model	Show the model name of this device
Serial Number	Show the serial number of this device
Device Name	Show the device name to distinguish different devices you have installed.
Firmware Version	Show the current firmware version
Hardware Version	Show the current 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



Link atual WAN

Link atual WAN: Ethernet
Endereço IP: 10.51.11.195
Gateway: 10.51.1.251
Máscara de rede: 255.255.0.0
Servidor DNS: 8.8.8.8, 8.8.4.4
Endereço IP de PING keepalive:8.8.8.8, 8.8.4.4

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



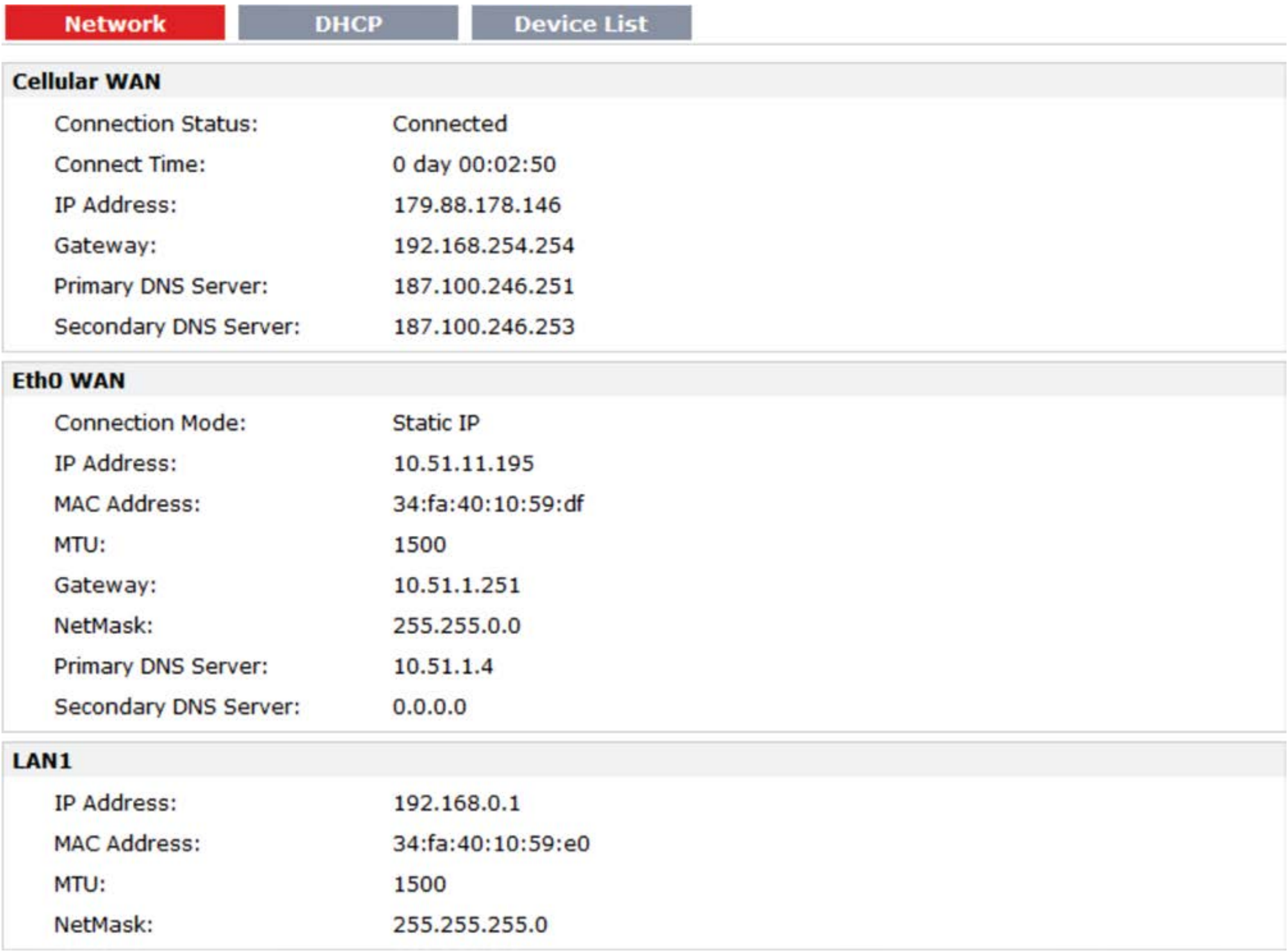
Cellular Information

Current SIM: SIM2
Phone No.:
SMS Service Center: 550101102010
Modem Status: Ready
Network Status: Registered to home network
CSQ: (10,-93dBm)
PLMN: VIVO ZAP (LAC: A0BF / Cell ID: 0337F4B)
Network Service Type: 3G HSDPA
IMEI/ESN:
IMSI: 724065402670996
APN: zap.vivo.com.br
Username: vivo
Password: vivo
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.
CSQ	Show the current signal level.
PLMN	Show Mobile Country Code (MCC) +Mobile Network Code (MNC), e.g. 46001. Also it will show the Location Area Code (LAC) and Cell ID.
Network Service Type	Show the current network service type, e.g. GPRS.
IMEI/ESN	Show the IMEI/ESN number of the radio module.
IMSI	Show the IMSI number of the current SIM.
USB Status	Show the current status of USB host.

3.5 STATUS -> NETWORK

This section displays the router's Network status, which include status of Cellular WAN, ETH0, ETH1, DHCP and Device List.



Cellular WAN

Connection Status:	Connected
Connect Time:	0 day 00:02:50
IP Address:	179.88.178.146
Gateway:	192.168.254.254
Primary DNS Server:	187.100.246.251
Secondary DNS Server:	187.100.246.253

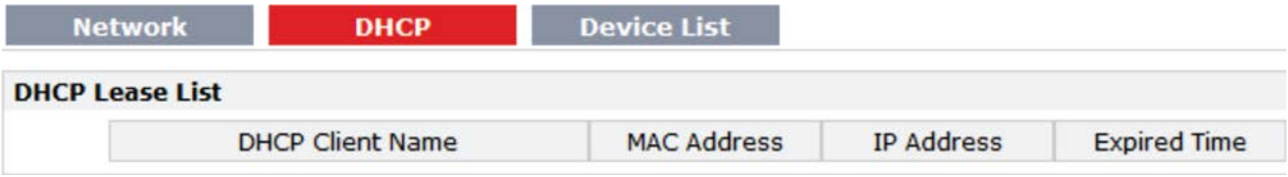
Eth0 WAN

Connection Mode:	Static IP
IP Address:	10.51.11.195
MAC Address:	34:fa:40:10:59:df
MTU:	1500
Gateway:	10.51.1.251
NetMask:	255.255.0.0
Primary DNS Server:	10.51.1.4
Secondary DNS Server:	0.0.0.0

LAN1

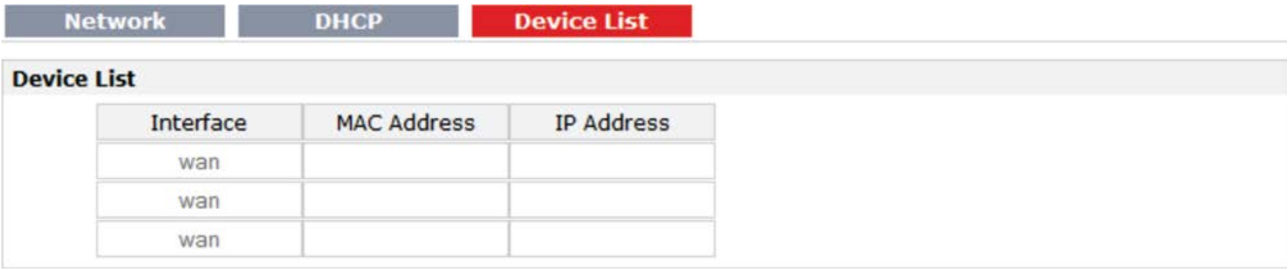
IP Address:	192.168.0.1
MAC Address:	34:fa:40:10:59:e0
MTU:	1500
NetMask:	255.255.255.0

***Note**: "Cellular WAN" information will not be shown if you select "Eth0" in "Configuration"->"Link Management"->"Link Management Settings" ->"Primary Interface".*



DHCP Lease List

DHCP Client Name	MAC Address	IP Address	Expired Time

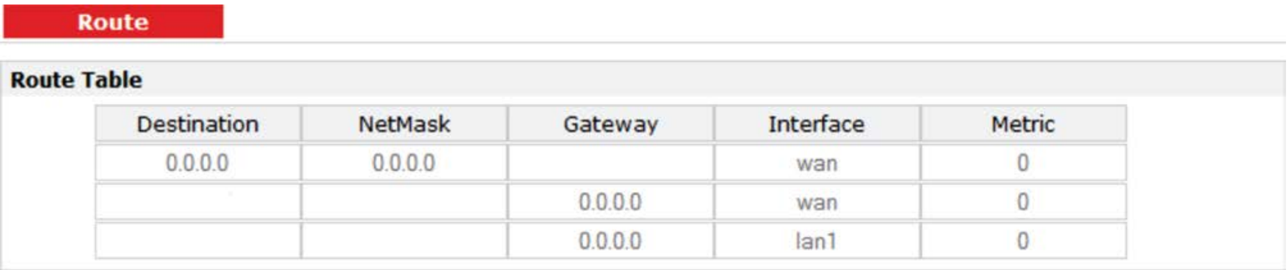


Device List

Interface	MAC Address	IP Address
wan		
wan		
wan		

3.6 STATUS -> ROUTE

This section displays the router's route table.

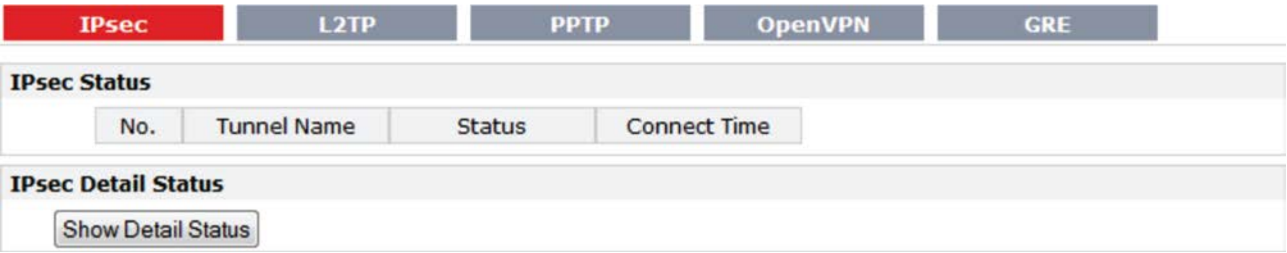


Route Table

Destination	NetMask	Gateway	Interface	Metric
0.0.0.0	0.0.0.0		wan	0
		0.0.0.0	wan	0
		0.0.0.0	lan1	0

3.7 STATUS -> VPN

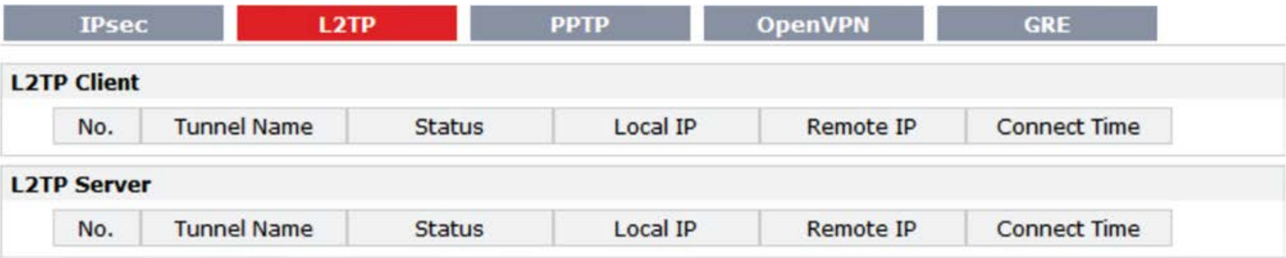
This section displays the router's VPN status, which includes IPSec, L2TP, PPTP, OpenVPN and GRE.



IPsec Status

No.	Tunnel Name	Status	Connect Time

IPsec Detail Status

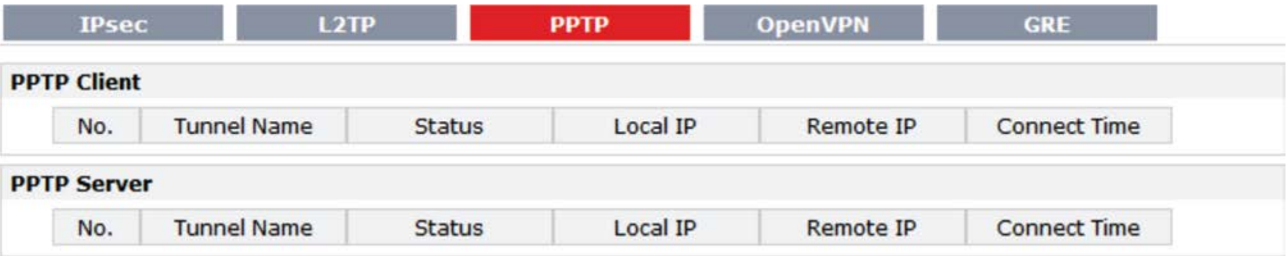


L2TP Client

No.	Tunnel Name	Status	Local IP	Remote IP	Connect Time

L2TP Server

No.	Tunnel Name	Status	Local IP	Remote IP	Connect Time

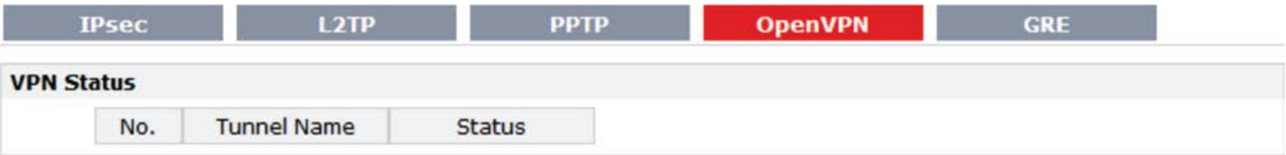


PPTP Client

No.	Tunnel Name	Status	Local IP	Remote IP	Connect Time

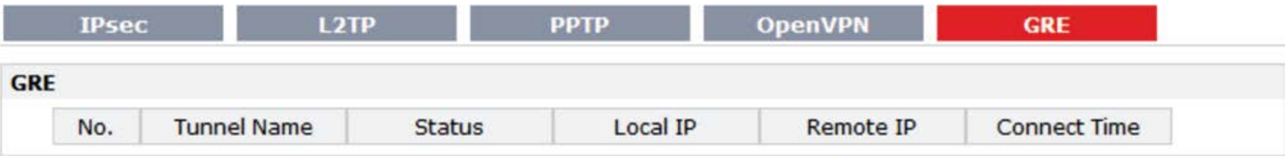
PPTP Server

No.	Tunnel Name	Status	Local IP	Remote IP	Connect Time



VPN Status

No.	Tunnel Name	Status

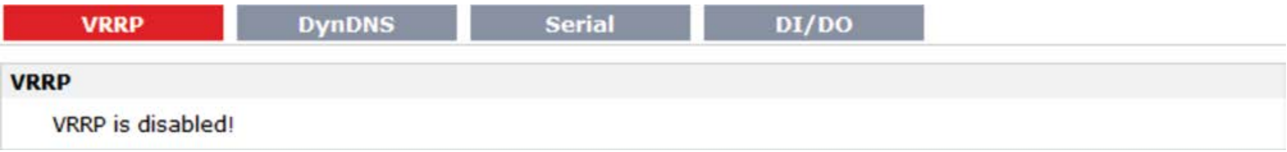


GRE

No.	Tunnel Name	Status	Local IP	Remote IP	Connect Time

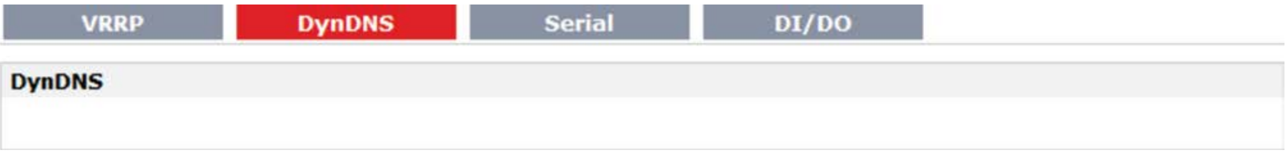
3.8 STATUS -> SERVICES

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

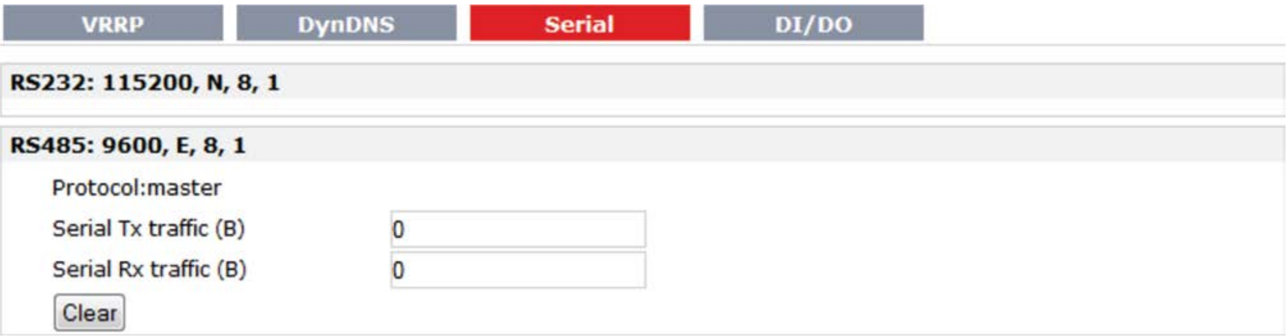


VRRP

VRRP is disabled!



DynDNS



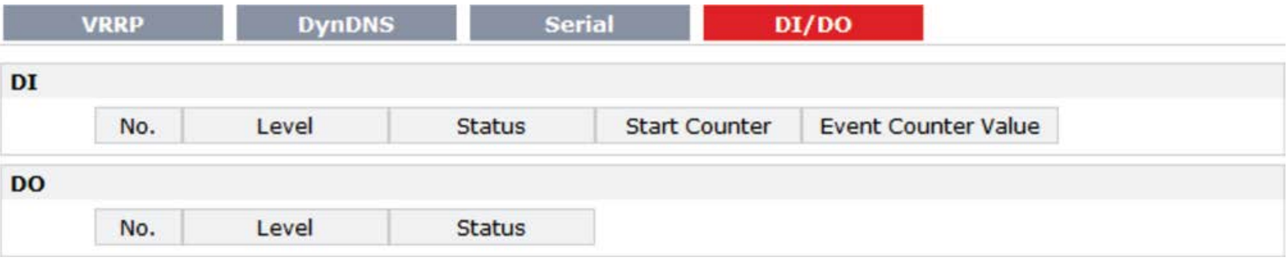
RS232: 115200, N, 8, 1

RS485: 9600, E, 8, 1

Protocol:master

Serial Tx traffic (B) 0

Serial Rx traffic (B) 0



DI

No.	Level	Status	Start Counter	Event Counter Value

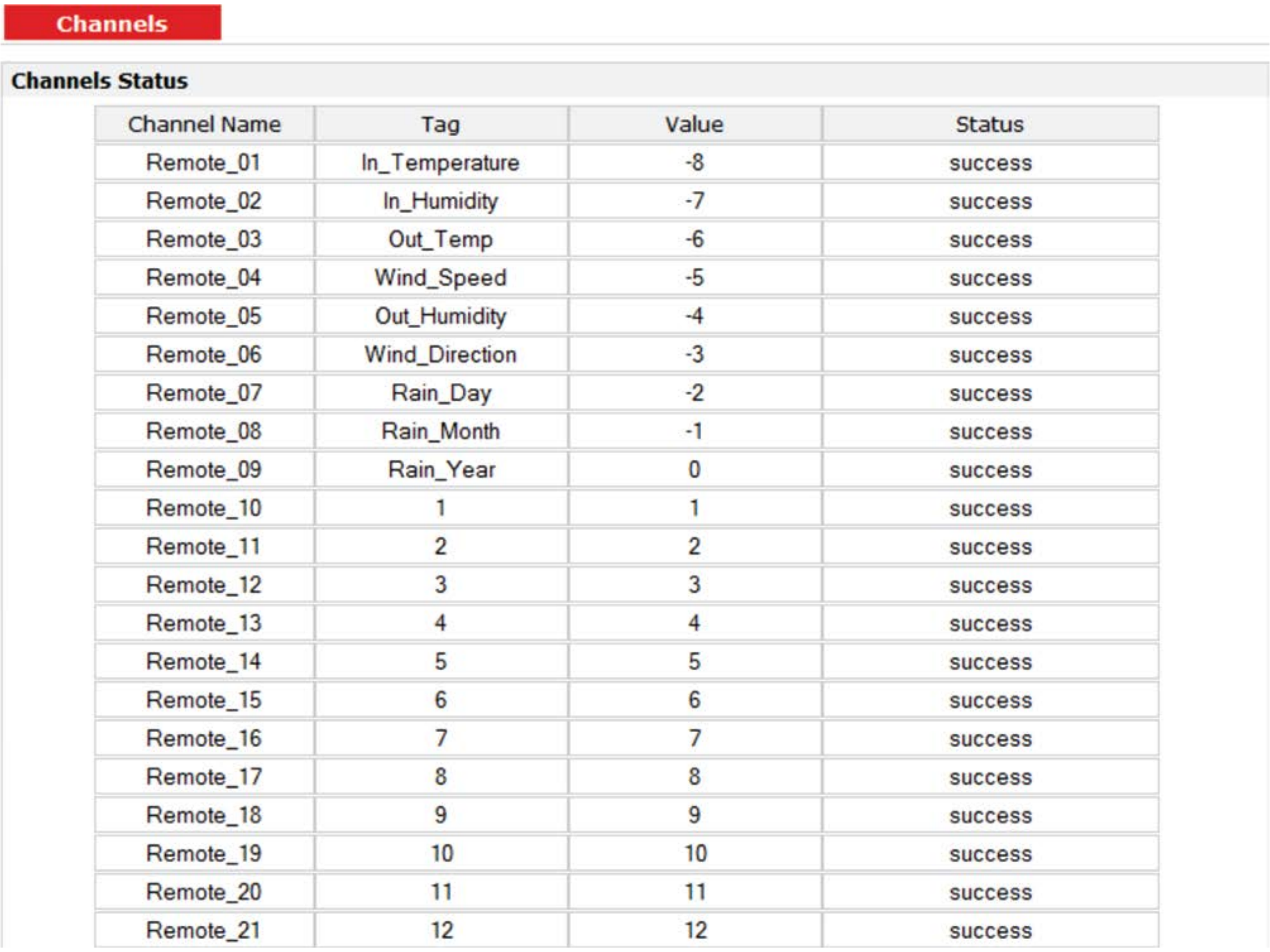
DO

No.	Level	Status

DI/DO	
Item	Description
DI	Show status of DI.
DO	Show status of DO.
DO Control	You can click button to change DO status of both DO_1 and DO_2 via web after you have enable DO in Configuration-> DI/DO-> DO-> DO Configuration -> Enable.

3.9 STATUS ->CHANNELS

This section displays the Channels' status.

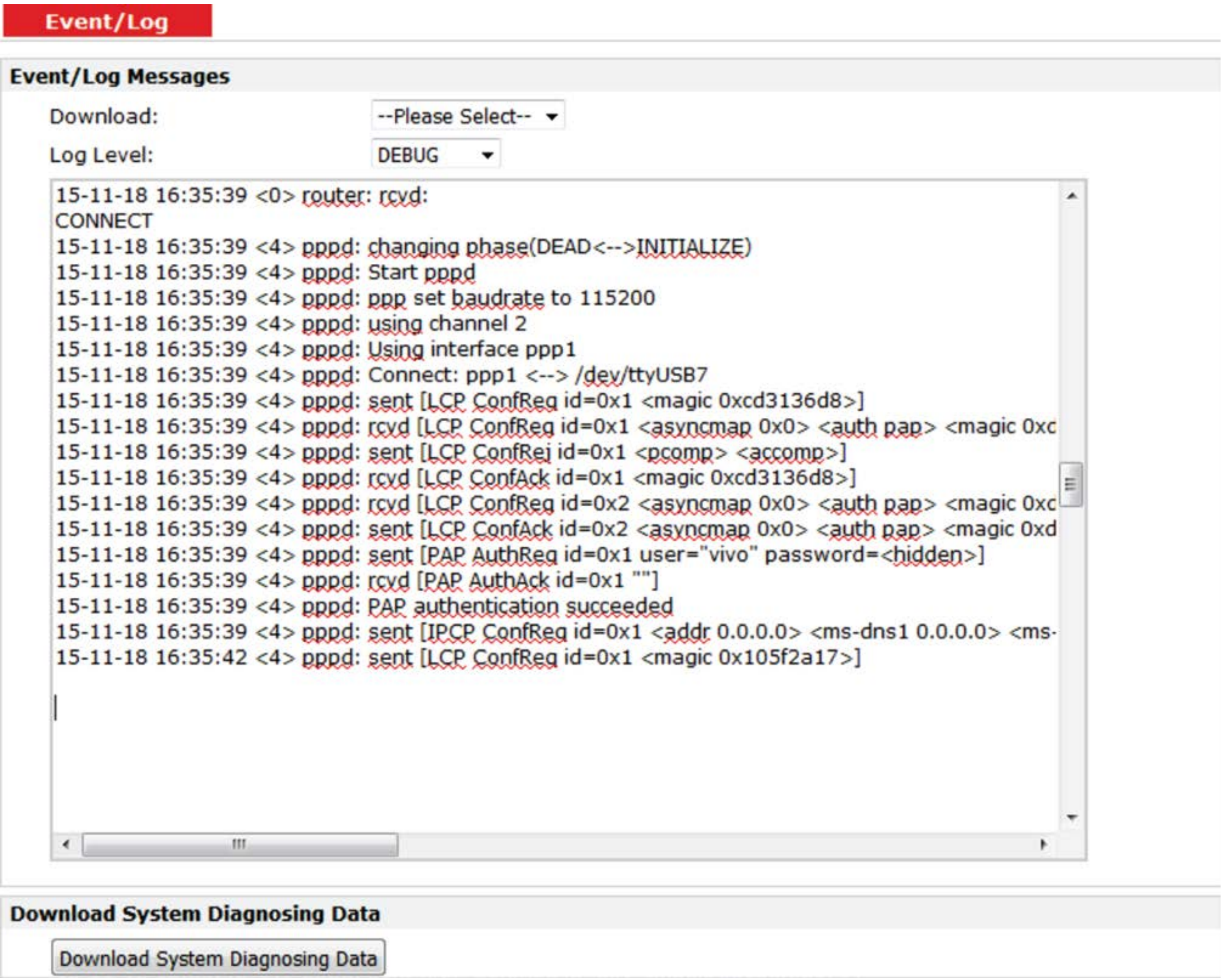


Channels Status

Channel Name	Tag	Value	Status
Remote_01	In_Temperature	-8	success
Remote_02	In_Humidity	-7	success
Remote_03	Out_Temp	-6	success
Remote_04	Wind_Speed	-5	success
Remote_05	Out_Humidity	-4	success
Remote_06	Wind_Direction	-3	success
Remote_07	Rain_Day	-2	success
Remote_08	Rain_Month	-1	success
Remote_09	Rain_Year	0	success
Remote_10	1	1	success
Remote_11	2	2	success
Remote_12	3	3	success
Remote_13	4	4	success
Remote_14	5	5	success
Remote_15	6	6	success
Remote_16	7	7	success
Remote_17	8	8	success
Remote_18	9	9	success
Remote_19	10	10	success
Remote_20	11	11	success
Remote_21	12	12	success

3.10 STATUS -> EVENT/LOG

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


Event/Log
Event/Log Messages
Download System Diagnosing Data
Download System Diagnosing Data

Download: --Please Select--

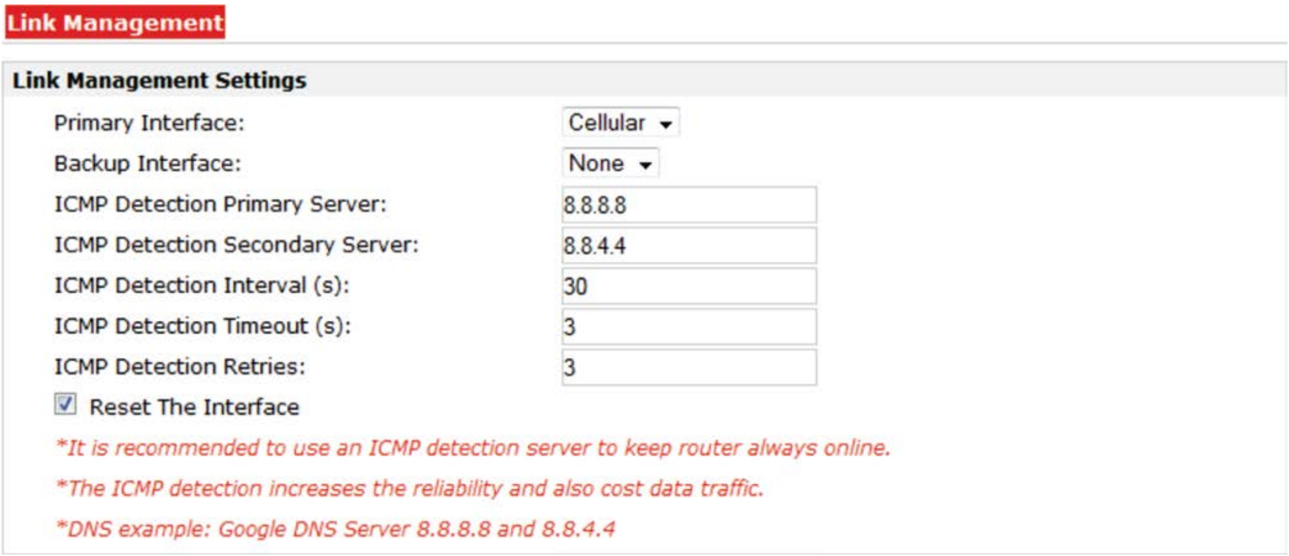
Log Level: DEBUG

```
15-11-18 16:35:39 <0> router: rcvd:
CONNECT
15-11-18 16:35:39 <4> pppd: changing phase(DEAD<-->INITIALIZE)
15-11-18 16:35:39 <4> pppd: Start pppd
15-11-18 16:35:39 <4> pppd: ppp set baudrate to 115200
15-11-18 16:35:39 <4> pppd: using channel 2
15-11-18 16:35:39 <4> pppd: Using interface ppp1
15-11-18 16:35:39 <4> pppd: Connect: ppp1 <--> /dev/ttyUSB7
15-11-18 16:35:39 <4> pppd: sent [LCP ConfReq id=0x1 <magic 0xcd3136d8>]
15-11-18 16:35:39 <4> pppd: rcvd [LCP ConfReq id=0x1 <asyncmap 0x0> <auth pap> <magic 0xc
15-11-18 16:35:39 <4> pppd: sent [LCP ConfRej id=0x1 <pcomp> <accomp>]
15-11-18 16:35:39 <4> pppd: rcvd [LCP ConfAck id=0x1 <magic 0xcd3136d8>]
15-11-18 16:35:39 <4> pppd: rcvd [LCP ConfReq id=0x2 <asyncmap 0x0> <auth pap> <magic 0xc
15-11-18 16:35:39 <4> pppd: sent [LCP ConfAck id=0x2 <asyncmap 0x0> <auth pap> <magic 0xd
15-11-18 16:35:39 <4> pppd: sent [PAP AuthReq id=0x1 user="vivo" password=<hidden>]
15-11-18 16:35:39 <4> pppd: rcvd [PAP AuthAck id=0x1 ""]
15-11-18 16:35:39 <4> pppd: PAP authentication succeeded
15-11-18 16:35:39 <4> pppd: sent [IPCP ConfReq id=0x1 <addr 0.0.0.0> <ms-dns1 0.0.0.0> <ms-
15-11-18 16:35:42 <4> pppd: sent [LCP ConfReq id=0x1 <magic 0x105f2a17>]
```

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 System Diagnosing Data	Click *Download System Diagnosing Data* to download diagnose file.
Manual Refresh	Select from "5 Seconds", "10 Seconds", "15 Seconds", "30 Seconds" and "1 Minute". User can select these intervals to refresh the log information.

3.11 CONFIGURATION -> LINK MANAGEMENT

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


Link Management

Link Management Settings

Primary Interface: Cellular

Backup Interface: None

ICMP Detection Primary Server: 8.8.8.8

ICMP Detection Secondary Server: 8.8.4.4

ICMP Detection Interval (s): 30

ICMP Detection Timeout (s): 3

ICMP Detection Retries: 3

☑ Reset The Interface

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

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

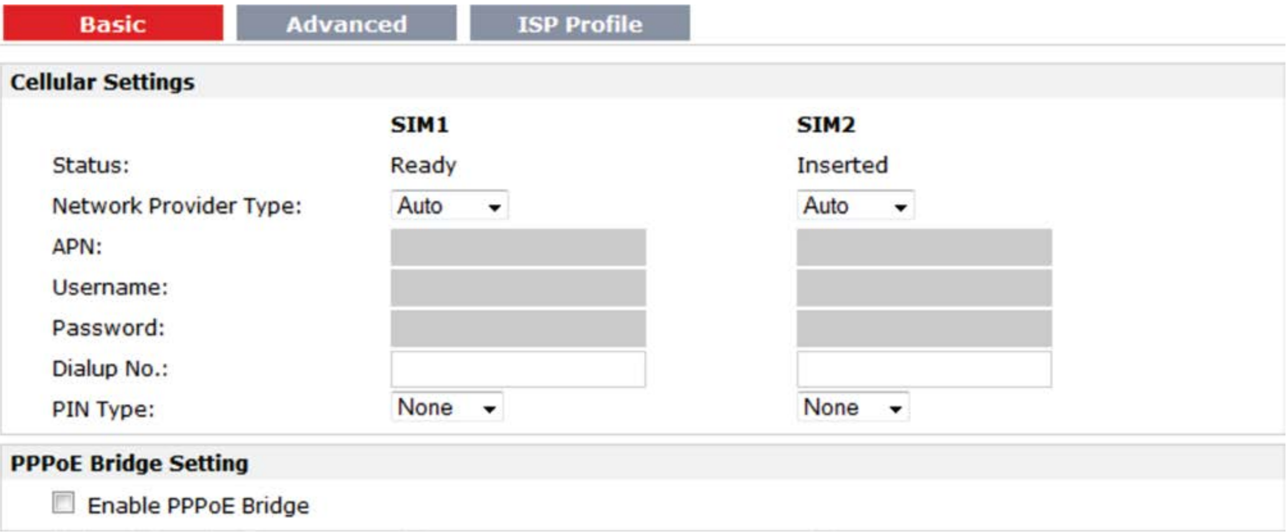
*DNS example: Google DNS Server 8.8.8.8 and 8.8.4.4

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

3.12 CONFIGURATION -> CELLULAR WAN

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

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

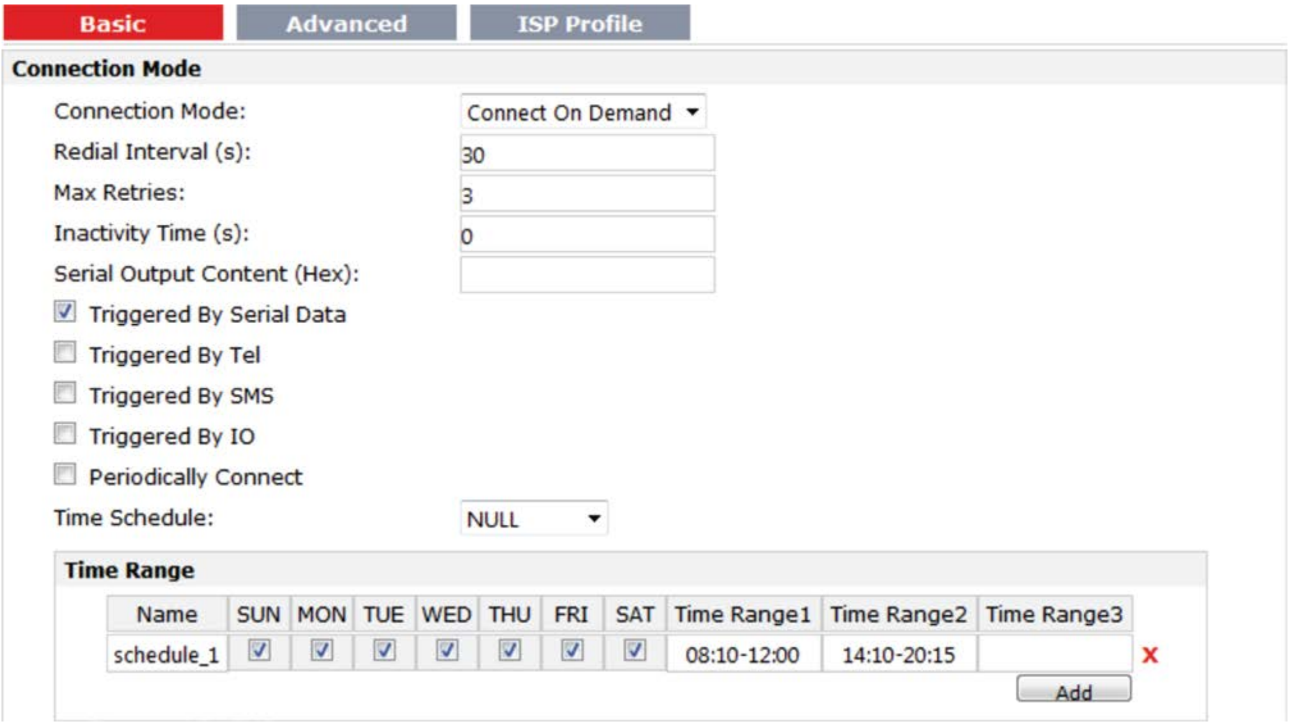


Cellular Settings

	SIM1	SIM2
Status:	Ready	Inserted
Network Provider Type:	Auto	Auto
APN:		
Username:		
Password:		
Dialup No.:		
PIN Type:	None	None

PPPoE Bridge Setting

☐ Enable PPPoE Bridge



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

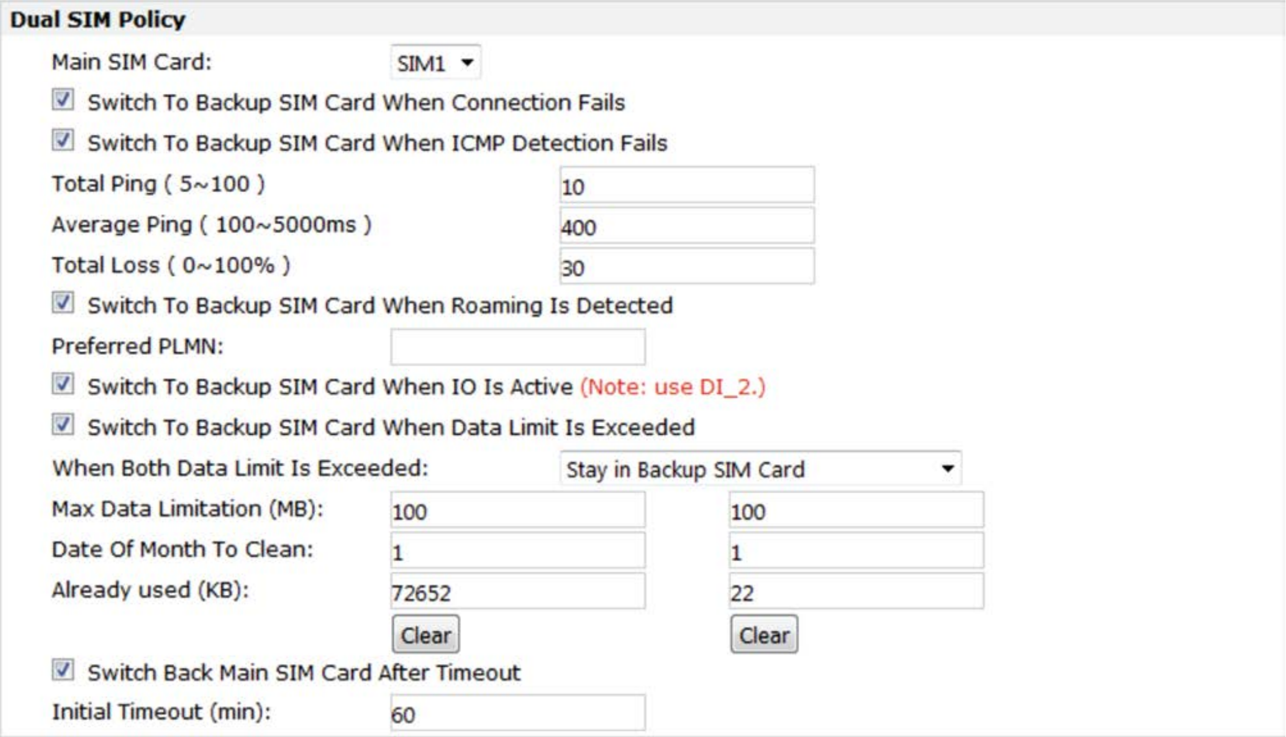
☐ Triggered By IO

☐ Periodically Connect

Time Schedule: NULL

Time Range

Name	SUN	MON	TUE	WED	THU	FRI	SAT	Time Range1	Time Range2	Time Range3	
schedule_1	☑	☑	☑	☑	☑	☑	☑	08:10-12:00	14:10-20:15		X



Dual SIM Policy

Main SIM Card: SIM1

☑ Switch To Backup SIM Card When Connection Fails

☑ Switch To Backup SIM Card When ICMP Detection Fails

Total Ping (5~100) 10

Average Ping (100~5000ms) 400

Total Loss (0~100%) 30

☑ Switch To Backup SIM Card When Roaming Is Detected

Preferred PLMN:

☑ Switch To Backup SIM Card When IO Is Active (Note: use DI_2.)

☑ Switch To Backup SIM Card When Data Limit Is Exceeded

When Both Data Limit Is Exceeded: Stay in Backup SIM Card

Max Data Limitation (MB):	100	100
Date Of Month To Clean:	1	1
Already used (KB):	72652	22
	Clear	Clear

☑ Switch Back Main SIM Card After Timeout

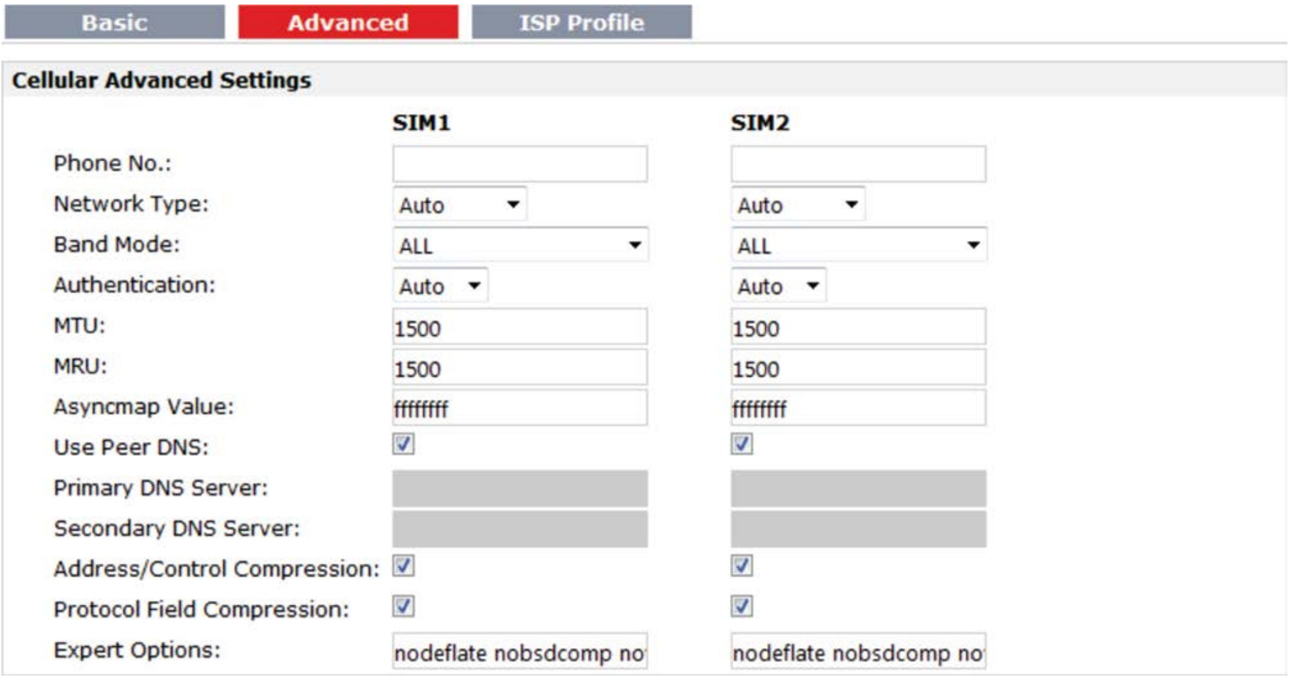
Initial Timeout (min): 60

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
PPPoE Bridge Setting		
Enable PPPoE Bridge	Click to enable PPPoE Bridge setting.	Disable

Connection Mode		
Connection Mode	Select from "Always Online" and "Connect On Demand". Always Online: Auto activates PPP and keeps the link up after power on. Connect On Demand: After selection this option, user could configure Triggered by Serial Data, Triggered by Periodically Connect and Triggered by Time Schedule. ***Note***: *If you select several connect on demand polices, router only have to meet one of them to be triggered.*	Connect On Demand
Redial Interval	Router will automatically re-dial with this interval when it fails communicating to peer via TCP or UDP.	30
Max Retries	The maximum retries times for automatically re-connect when router fails to dial up. After maximum retries, router will reboot the wireless module. If router still cannot dial up successfully, it will try to switch to the other SIM card. Then router will re-connect with the other SIM card with maximum retries. After successful connection, the Max Retries counter will be set to 0.	3
Inactivity Time	Configurable after "Connect On Demand" was selected. This field specifies the idle time setting for GPRS/3G auto-disconnection and trying to revert back to preferred SIM card. 0 means timeless.	0
Serial Output Content	The content which output to the serial device which connect to router and inform it that router is ready to receive serial data.	Null
Triggered by Serial Data	Tick this check box to allow router automatically connects to cellular network from idle mode when there is data comes out from serial port.	Enable
Triggered by Tel	Tick this check box to allow router automatically connects to cellular network from idle mode when make a voice call to router.	Disable
Triggered by SMS	Tick this check box to allow router automatically connects to cellular network from idle mode when send a specific SMS to router.	Disable
SMS Connect Command	Users shall send this specific SMS to trigger router to connect to cellular network.	Null
SMS Disconnect Command	Users shall send this specific SMS to trigger router to disconnect to cellular network.	Null
SMS Connect Reply	When router connects to cellular network, it will automatically send out this SMS to specific users (set in the Phone Group).	Null
SMS Disconnect Reply	When router disconnect from cellular network, it will automatically send out this SMS to specific users (set in the Phone Group).	Null
Phone Group	Click to add Phone Group to Set specific users' phone Book and which phone Group they are belonged to.	Null
Triggered by IO	Tick this check box to allow router automatically connects to cellular network from idle mode when there is a DI (DI_1) alarm input.	Disable
Periodically Connect	Tick this check box to allow router automatically connects to cellular network with preset interval which you preset in *Periodically Connect Interval.*	Enable
Periodically Connect Interval	Periodically Connect Interval for Periodically Connect.	300
Time Schedule	Select the Time Range to allow router automatically connects to cellular network during this time range.	NULL
Time Range	Adding the Time Range for Time Schedule. You can set the days of one week and at most three ranges of time of one day.	Null

Dual SIM Policy		
Main SIM Card	Set the preferred SIM card from SIM 1, SIM 2 or Auto.	SIM1
Switch to backup SIM card when connection fails	Router will switch to another SIM card if main SIM card fail to connect to network.	Disable
Switch To Backup SIM Card When ICMP Detection Fails	Router will switch to another SIM card if it cannot dialup or ping the preset address timeout continuously for Max Retries time. Preset address is set in Configuration-> Link Management-> ICMP Detection Primary Server and ICMP Detection Secondary Server. ***Important Note:*** *You need to fill in tab Configuration-> Link Management-> ICMP Detection Primary Server and ICMP Detection Secondary Server, and then this strategy can be activated.*	Disable
Total Ping (5~100) @ Switch To Backup SIM Card When ICMP Detection Fails	Preset Max Retries time that Router ping the preset address/domain name.	10
Average Ping (100~5000ms) @ Switch To Backup SIM Card When ICMP Detection Fails	Route will count the “Average Ping” timeout interval after router ping the preset address/domain name for “Total Ping” times. After router detects that average ping timeout interval reach to preset “Average Ping” it will switch backup SIM card.	400
Total Loss (0~100%) @ Switch To Backup SIM Card When ICMP Detection Fails	Route will count the “Total Loss” after router ping the preset address/domain name for “Total Ping” times. After router detects that total loss packet reach to preset “Total Loss” it will switch backup SIM card.	30
Switch to backup SIM card when roaming is detected	Router will switch to backup SIM card when preferred SIM card is roaming.	Disable
Preferred PLMN	The identifier for Router to check if it is in home location area or in roaming area, and decide if it needs to switch back to preferred SIM card.	Null
Switch to backup SIM card when IO is active	Router will switch to another SIM card if it detect there is DI (DI_2) alarm input.	Disable
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
When Both Data Limit Is Exceeded	Select from “Stay in Backup SIM Card”, “Switch Back Main SIM Card” and “Disable Cellular Until Data Is Cleared”.	Disable
Max Data limitation(MB)	Set the monthly data traffic limitation.	100
Date of Month to Clean	Set one day of month to restore the used data to 0.	1
Already used	This tab will show how many data traffic has been used.	0
Switch back Main SIM card after timeout(min)	Enable to Switch back Main SIM card after the Initial timeout.	Disable
Initial Timeout(min)	Set the initial timeout.	60

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



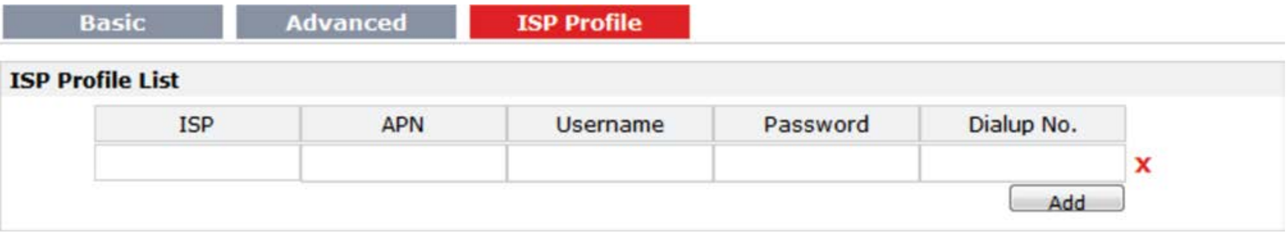
Cellular Advanced Settings

	SIM1	SIM2
Phone No.:		
Network Type:	Auto	Auto
Band Mode:	ALL	ALL
Authentication:	Auto	Auto
MTU:	1500	1500
MRU:	1500	1500
Asyncmap Value:	ffffffff	ffffffff
Use Peer DNS:	☑	☑
Primary DNS Server:		
Secondary DNS Server:		
Address/Control Compression:	☑	☑
Protocol Field Compression:	☑	☑
Expert Options:	nodeflate nobsdcomp no	nodeflate nobsdcomp no

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

ISP Profile

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



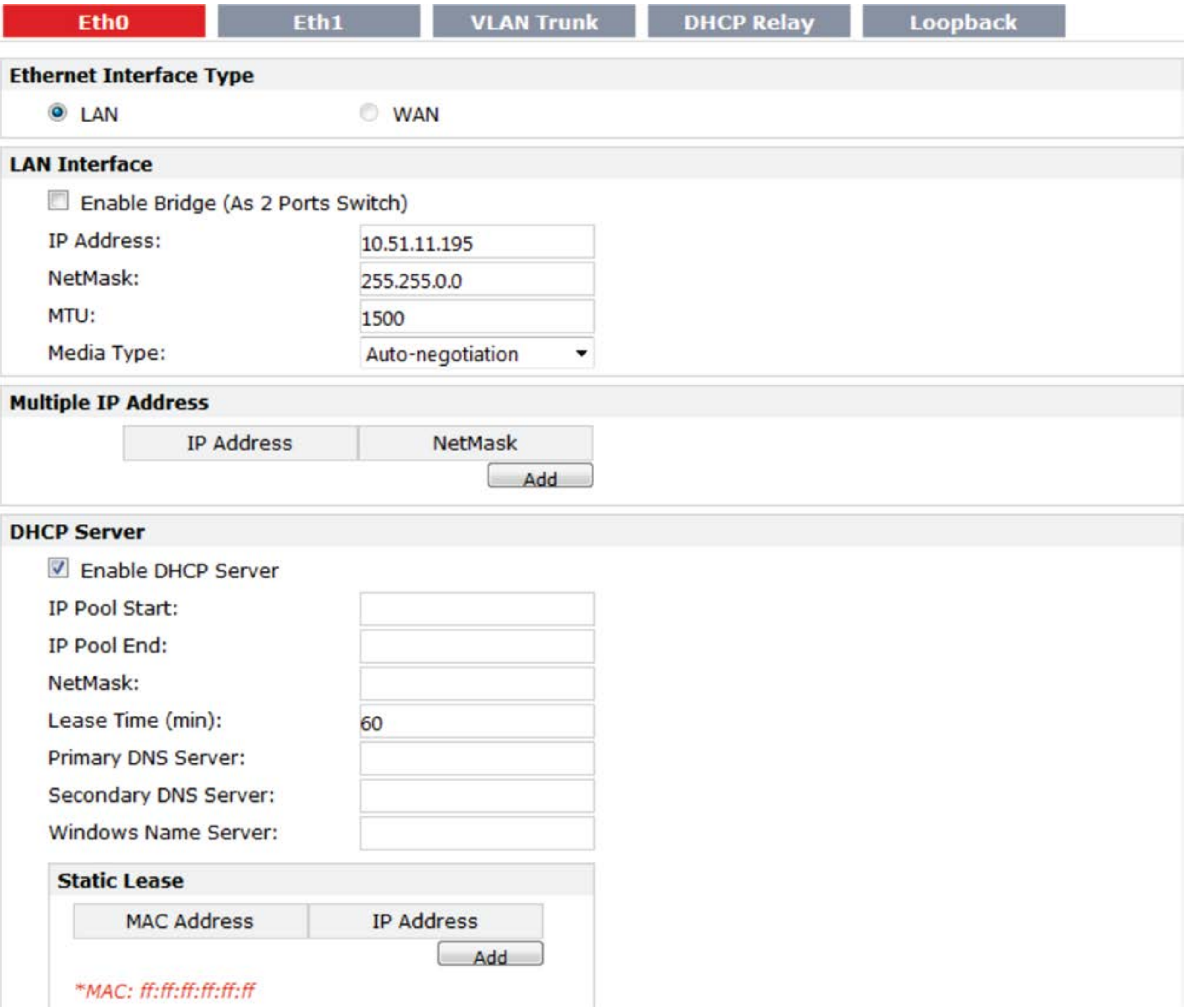
ISP Profile List

ISP	APN	Username	Password	Dialup No.

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

3.13 CONFIGURATION -> ETHERNET

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



Ethernet Interface Type

● LAN ○ WAN

LAN Interface

□ Enable Bridge (As 2 Ports Switch)

IP Address:	10.51.11.195
NetMask:	255.255.0.0
MTU:	1500
Media Type:	Auto-negotiation

Multiple IP Address

IP Address	NetMask

DHCP Server

☑ Enable DHCP Server

IP Pool Start:	
IP Pool End:	
NetMask:	
Lease Time (min):	60
Primary DNS Server:	
Secondary DNS Server:	
Windows Name Server:	

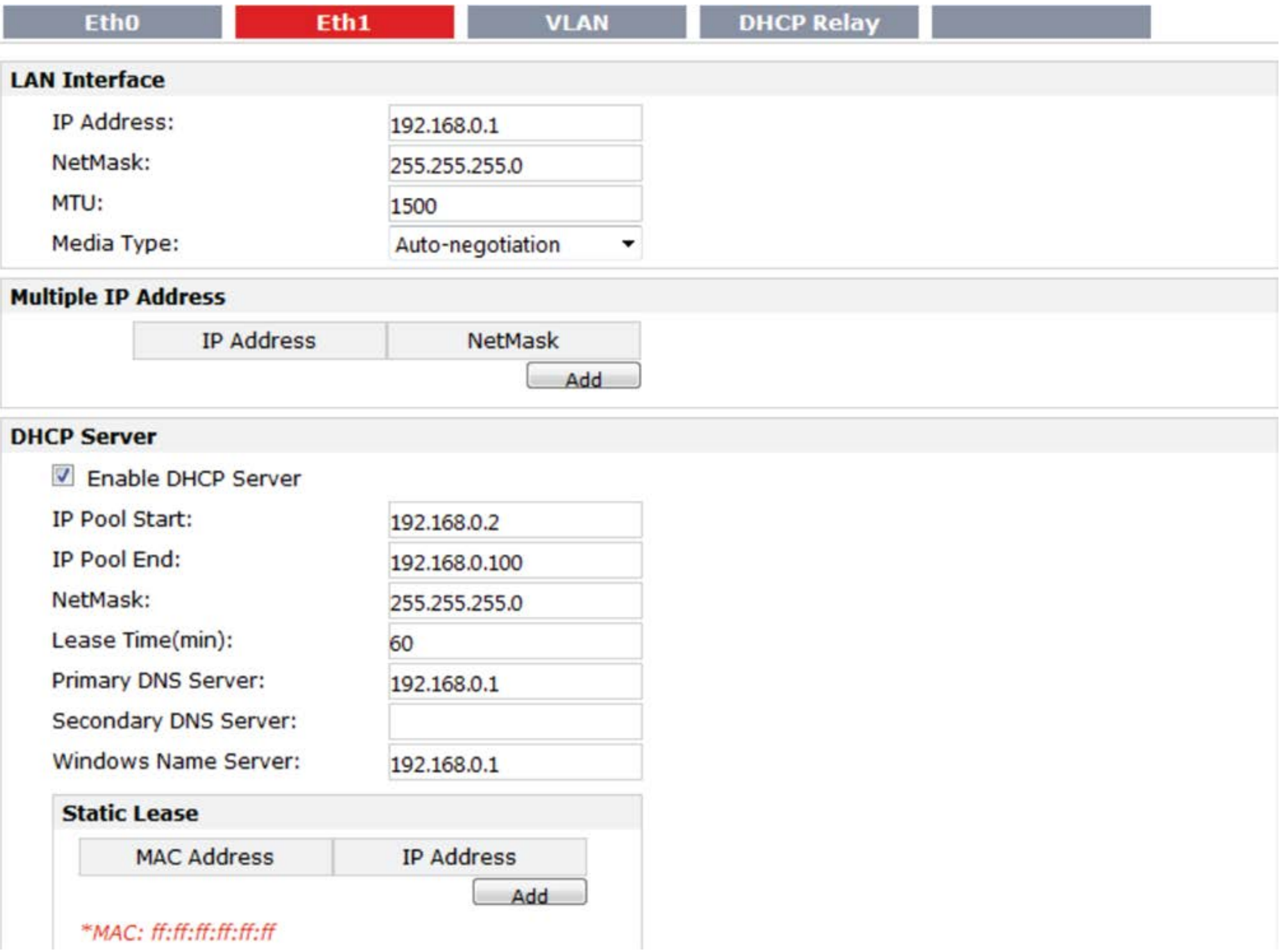
Static Lease

MAC Address	IP Address

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

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

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



LAN Interface

IP Address:	192.168.0.1
NetMask:	255.255.255.0
MTU:	1500
Media Type:	Auto-negotiation

Multiple IP Address

IP Address	NetMask

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

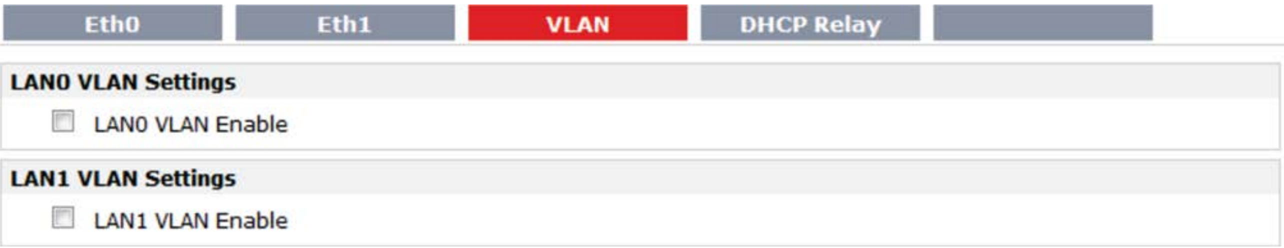
Static Lease

MAC Address	IP Address

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

Eth1@Ethernet		
Item	Description	Default
IP Address, Netmask, MTU, Media Type @ LAN Interface	Set the IP address, Netmask, MTU and Media Type of Eth1. These parameters will be un-configurable if you enable Bridge.	Null
Multiple IP Address @ LAN Interface	Assign multiple IP addresses for Eth1.	Null
Enable DHCP Server @ DHCP Server	Enable to make router can lease IP address to DHCP clients which connect to Eth1.	Enable
IP Pool Start, IP Pool End @ DHCP Server	Define the beginning (IP Pool Start) and end (IP Pool End) of the pool of IP addresses which will lease to DHCP clients.	192.168.0.2/ 192.168.0.100
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 DNS Server @ DHCP Server	Define the primary/secondary DNS Server which the DHCP clients will obtain from DHCP server.	192.168.0.1/ 0.0.0.0
Windows Name Server @ DHCP Server	Define the WINS Server which the DHCP clients will obtain from DHCP server.	192.168.0.1
Static Lease @ DHCP Server	Define to lease static IP Addresses, which conform to MAC Address of the connected equipment.	Null

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



LAN0 VLAN Settings

□ LAN0 VLAN Enable

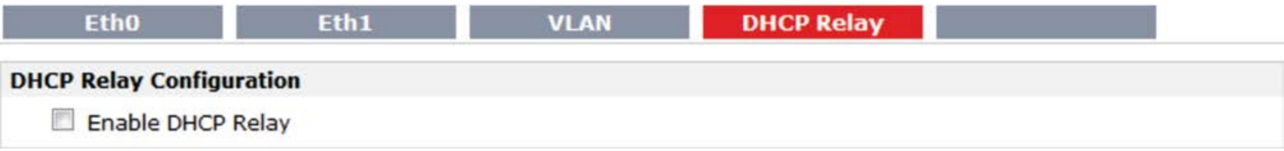
LAN1 VLAN Settings

□ LAN1 VLAN Enable

VLAN @ Ethernet		
Item	Description	Default
LAN 0/1 VLAN Enable	Enable to make router can encapsulate and de-encapsulate the VLAN tag.	Disable
VLAN ID@LAN 0/1 VLAN Enable	Set the Tag ID of VLAN	Null
IP Address, NetMask @LAN0/1 VLAN Settings	Set the IP address, Netmask of VLAN interface	VLAN 0/1's IP address, Netmask

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

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.



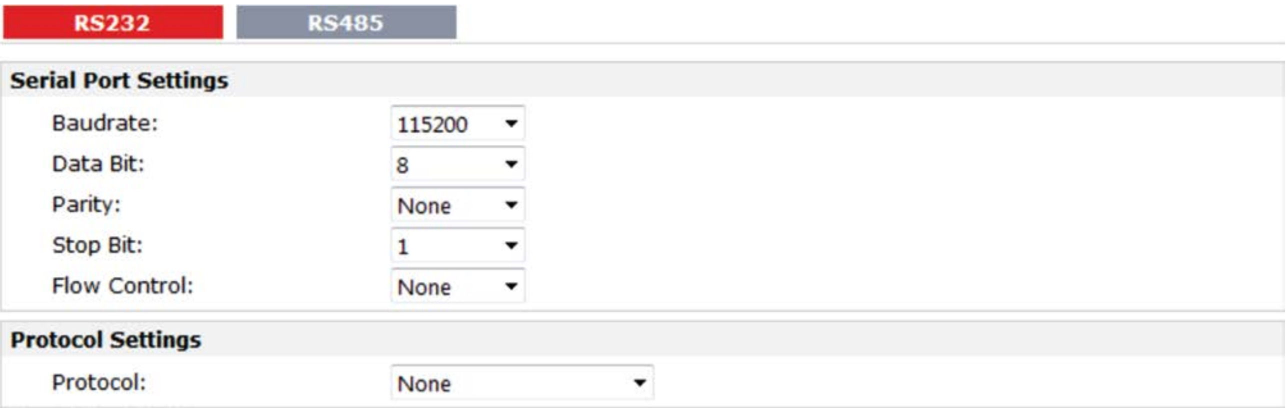
DHCP Relay Configuration

□ Enable DHCP Relay

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

3.14 CONFIGURATION -> SERIAL

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



Serial Port Settings

Baudrate: 115200

Data Bit: 8

Parity: None

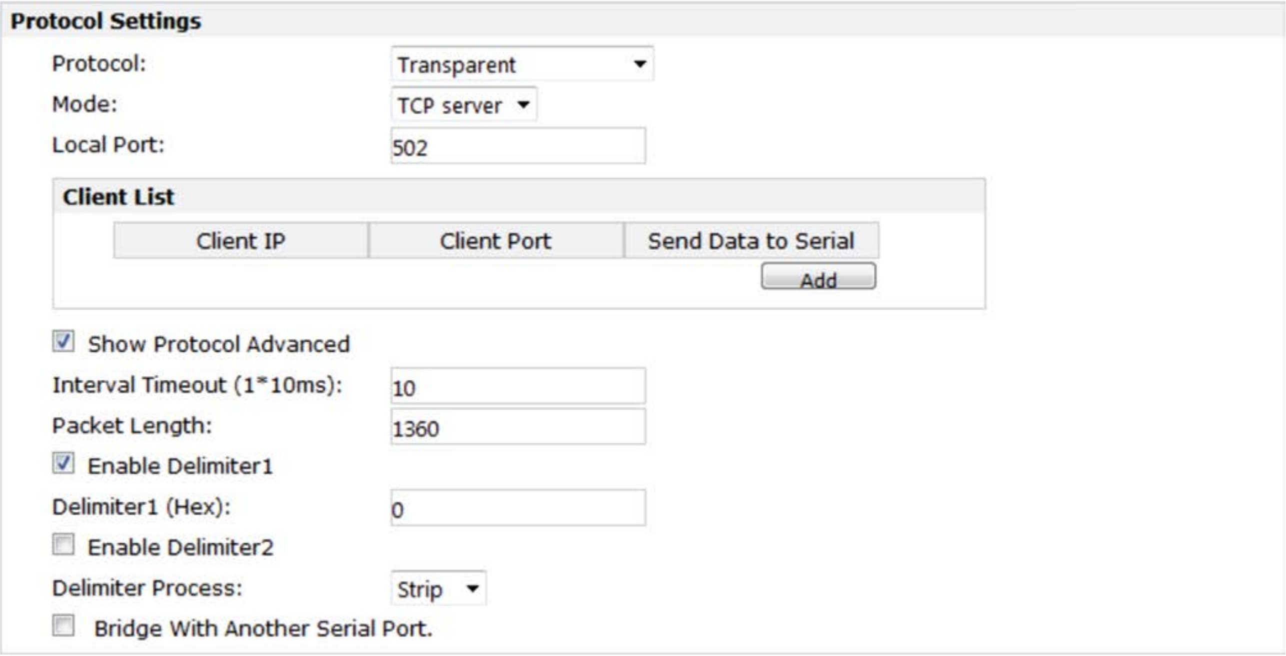
Stop Bit: 1

Flow Control: None

Protocol Settings

Protocol: None

- When Select Protocol "Transparent":



Protocol Settings

Protocol: Transparent

Mode: TCP server

Local Port: 502

Client List

Client IP	Client Port	Send Data to Serial

☑ Show Protocol Advanced

Interval Timeout (1*10ms): 10

Packet Length: 1360

☑ Enable Delimiter1

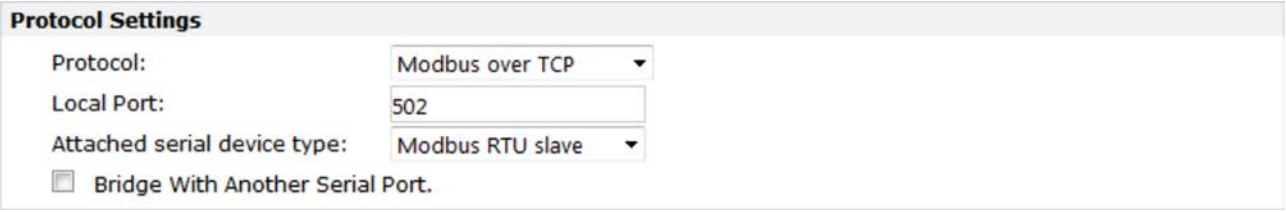
Delimiter1 (Hex): 0

□ Enable Delimiter2

Delimiter Process: Strip

□ Bridge With Another Serial Port.

- When Select Protocol "Modbus over TCP":



Protocol Settings

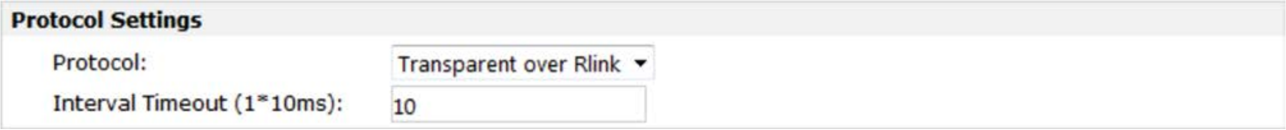
Protocol: Modbus over TCP

Local Port: 502

Attached serial device type: Modbus RTU slave

□ Bridge With Another Serial Port.

- When Select Protocol "Transparent Over Nlink":

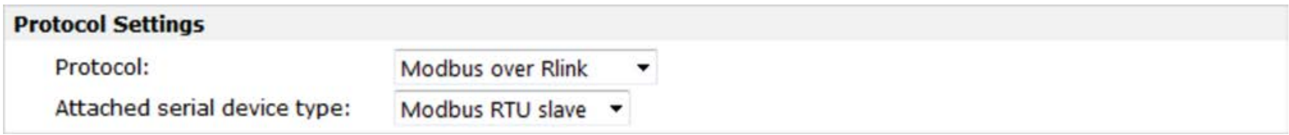


Protocol Settings

Protocol: Transparent over Rlink

Interval Timeout (1*10ms): 10

- When Select Protocol "Modbus Over Nlink":

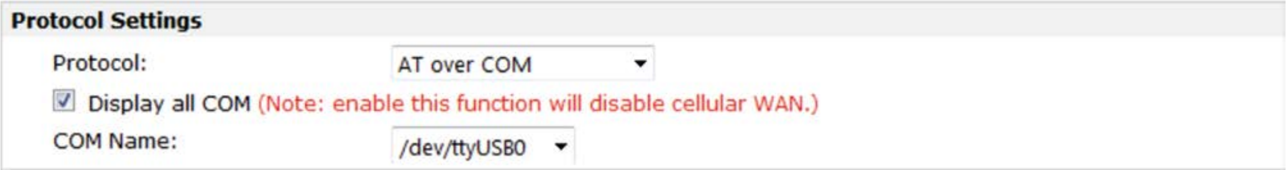


Protocol Settings

Protocol: Modbus over Rlink

Attached serial device type: Modbus RTU slave

- When Select Protocol "AT Over COM":



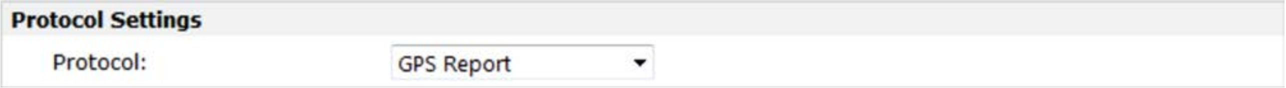
Protocol Settings

Protocol: AT over COM

☑ Display all COM (Note: enable this function will disable cellular WAN.)

COM Name: /dev/ttyUSB0

- When Select Protocol "GPS Report":



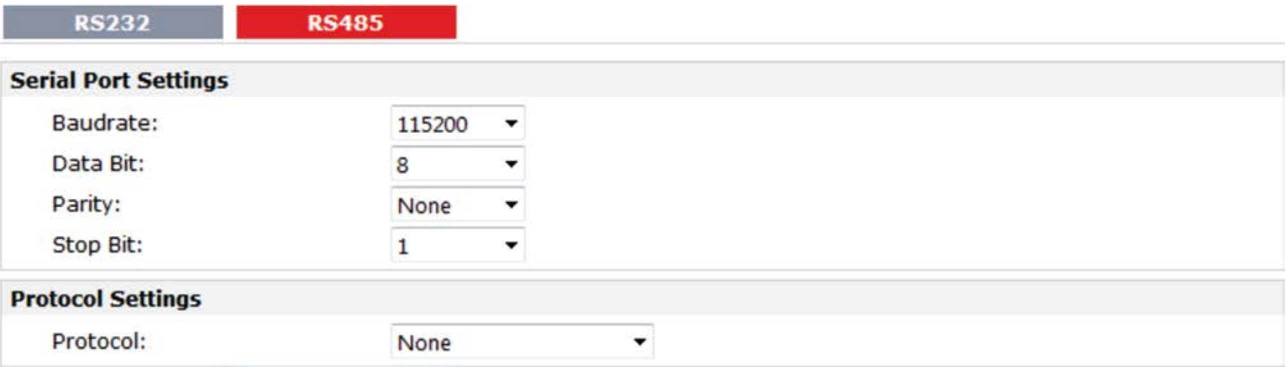
Protocol Settings

Protocol: GPS Report

RS232 @ Serial		
Item	Description	Default
Baud-rate	Select from "300", "600", "1200", "2400", "4800", "9600", "19200", "38400", "57600" , "115200"and "230400".	115200
Data bit	Select from "7" and "8".	8
Parity	Select from "None", "Odd" and "Even".	None
Stop bit	Select from "1" and "2".	1
Flow control	Select from "None", "Software" and "Hardware".	None
Protocol	Select from "None", "Transparent", "Modbus", "Transparent Over Nlink", "Modbus Over Nlink" "AT Over COM" and "GPS Report". 1. None: Router will do nothing in RS232 serial port. 2. Transparent: Router will transmit the serial data transparently without any protocols. 3. Modbus: Router will translate the Modbus RTU data to Modbus TCP data and vice versa. 4. Transparent Over Nlink: Router will send all data from RS232 serial port to NovusLink, then NovusLink will forward the data to another destination site. 5. Modbus Over Nlink: Router will translate all data from RS232 serial port to Modbus TCP protocol data, and then send to NovusLink, after that NovusLink 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	Select from "TCP Server", "TCP Client" and "UDP". TCP Client: Router works as TCP client, initiate TCP connection to TCP server. Server address supports both IP and domain name. TCP Server: Router works as TCP server, listening for connection request from TCP client. UDP: Router works as UDP client.	TCP Client
Local Port @Transparent	Enter the Local port for TCP or UDP.	0
Multiple Server @Transparent	Click "Add" button to add multiple server. You need to enter the server's IP and port, and enable or disable "Send data to serial". If you disable "Send data to serial", router will not transmit the data from this server to serial port. ***Note:*** *This section will not be displayed if you select "TCP server" in "Mode".*	None
show Protocol Advanced @ Transparent	Tick to enable protocol advanced setting.	Disable
Local IP @ Transparent	This item will show up when you enable any VPN tunnel of AIRGATE-3G, it means serial data can be matched to this local IP address and be transmitted or received via VPN tunnel. ***Note****: when you do not enable any VPN tunnel, this item will not show up.*	Null
Interval Timeout @Transparent	The serial port will queue the data in the buffer and send the data to the Cellular WAN/Ethernet WAN when it reaches the Interval Timeout in the field. ***Note****: Data will also be sent as specified by the packet length or delimiter settings even when data is not reaching the interval timeout in the field.*	10
Packet Length @Transparent	The Packet length setting refers to the maximum amount of data that is allowed to accumulate in the serial port buffer before sending. 0 for packet length, no maximum amount is specified and data in the buffer will be sent as specified by the interval timeout or delimiter settings or when the buffer is full. When a packet length between 1 and 1024 bytes is specified, data in the buffer will be 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 over TCP	This item will show up When you enable any VPN tunnel of AIRGATE-3G, 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 over TCP	Enter the Local port for Modbus.	0

Attached serial device type @Modbus over TCP	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 ASCⅡprotocol. **Note**: *When select “Modbus RTU slave” and “Modbus ASC Ⅱ slave” protocol, router is as TCP Server site, user need to enter a local port number in “Local Port @Modbus” and wait to be connected.* Modbus RTU master: router connects to master device which works under Modbus RTU protocol. Modbus ASCⅡ master: router connects to master device which works under Modbus ASCⅡ protocol. **Note**: *When select “Modbus RTU* master*” and “Modbus ASC Ⅱ*master*” protocol, router is as TCP Client site, user need to enter slave address and slave port number in “*Slave Address @ Modbus Slave *” and “*Slave Port @ Modbus Slave*”, and connect to Server site.*	Modbus RTU slave
Modbus Slave @Modbus over TCP	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 Nlink	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 Nlink	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 ASCⅡprotocol.	Null
Display all com @ AT Over COM	Enable to display all virtual com of the module inside the router. Generally, router will occupy /dev/ttyUSB0 and /dev/ttyUSB2 for dialing up to GPRS. **Note**: *Enable this function will disable Cellular WAN function.*	Disable
COM Name	Show the virtual com name of the module inside.	/dev/ttyUSB1



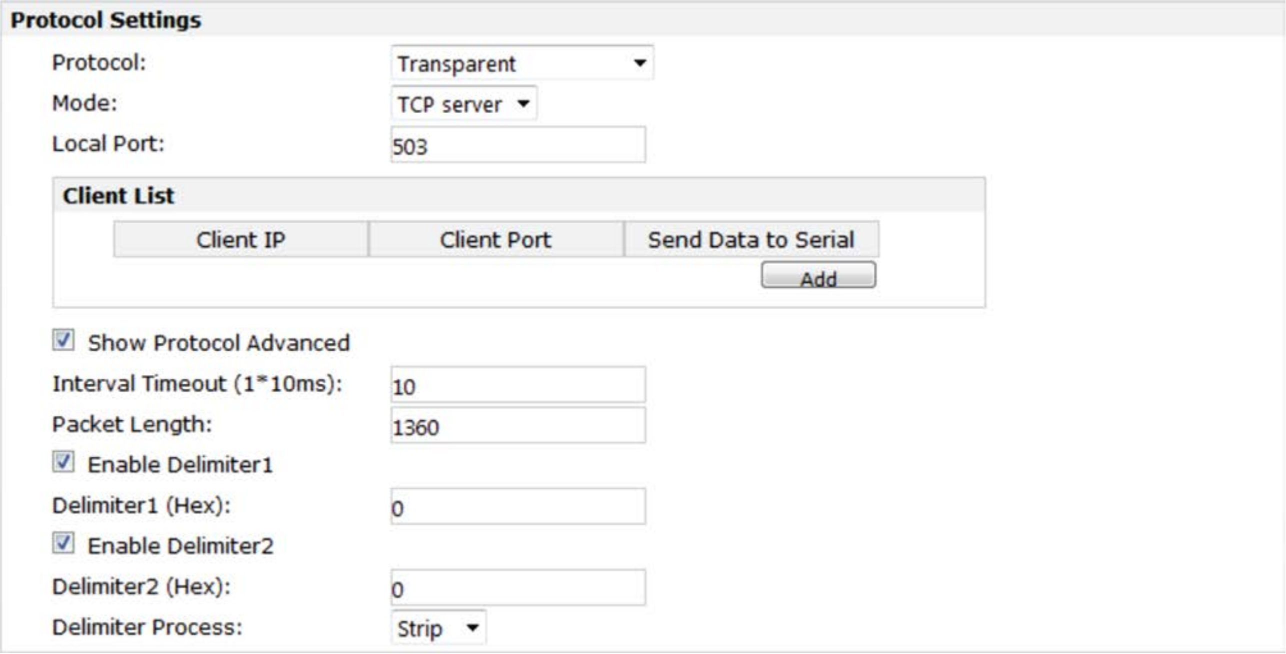
Serial Port Settings

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

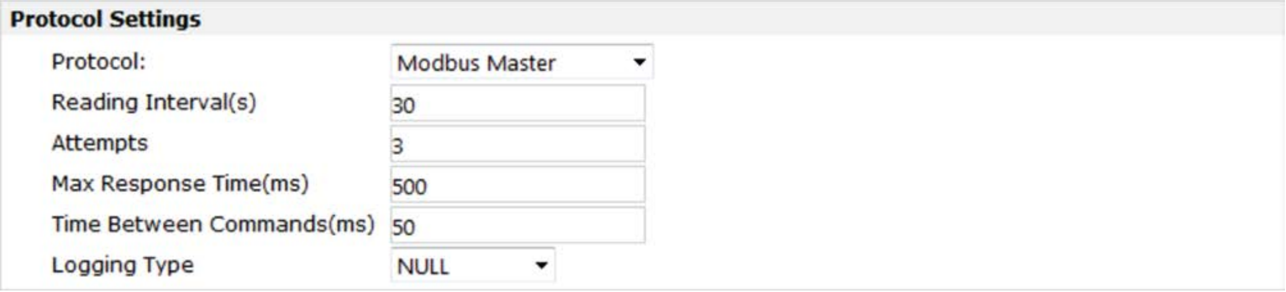
Client List

Client IP	Client Port	Send Data to Serial

☑ Show Protocol Advanced

Interval Timeout (1*10ms):	10
Packet Length:	1360
☑ Enable Delimiter1	
Delimiter1 (Hex):	0
☑ Enable Delimiter2	
Delimiter2 (Hex):	0
Delimiter Process:	Strip ▾

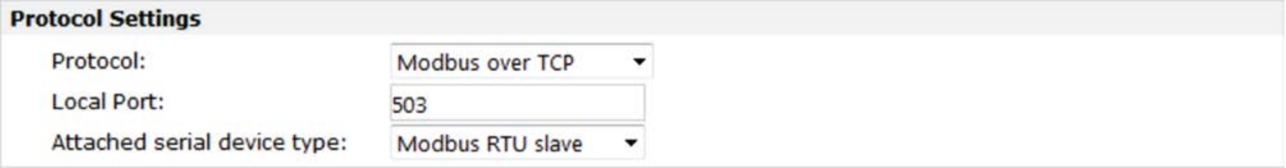
- When Select Protocol “Modbus Master”:



Protocol Settings

Protocol:	Modbus Master ▾
Reading Interval(s)	30
Attempts	3
Max Response Time(ms)	500
Time Between Commands(ms)	50
Logging Type	NULL ▾

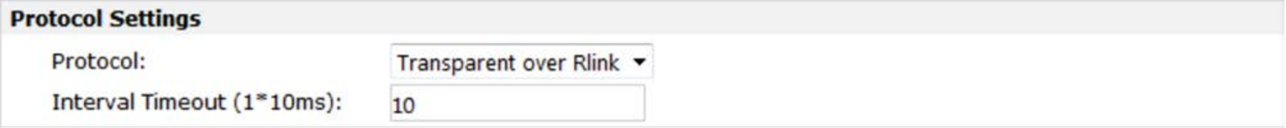
- When Select Protocol “Modbus over TCP”:



Protocol Settings

Protocol:	Modbus over TCP ▾
Local Port:	503
Attached serial device type:	Modbus RTU slave ▾

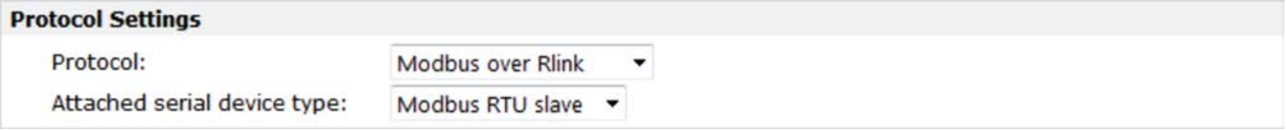
- When Select Protocol “Transparent Over Nlink”:



Protocol Settings

Protocol:	Transparent over Rlink ▾
Interval Timeout (1*10ms):	10

- When Select Protocol “Modbus Over Nlink”:



Protocol Settings

Protocol:	Modbus over Rlink ▾
Attached serial device type:	Modbus RTU slave ▾

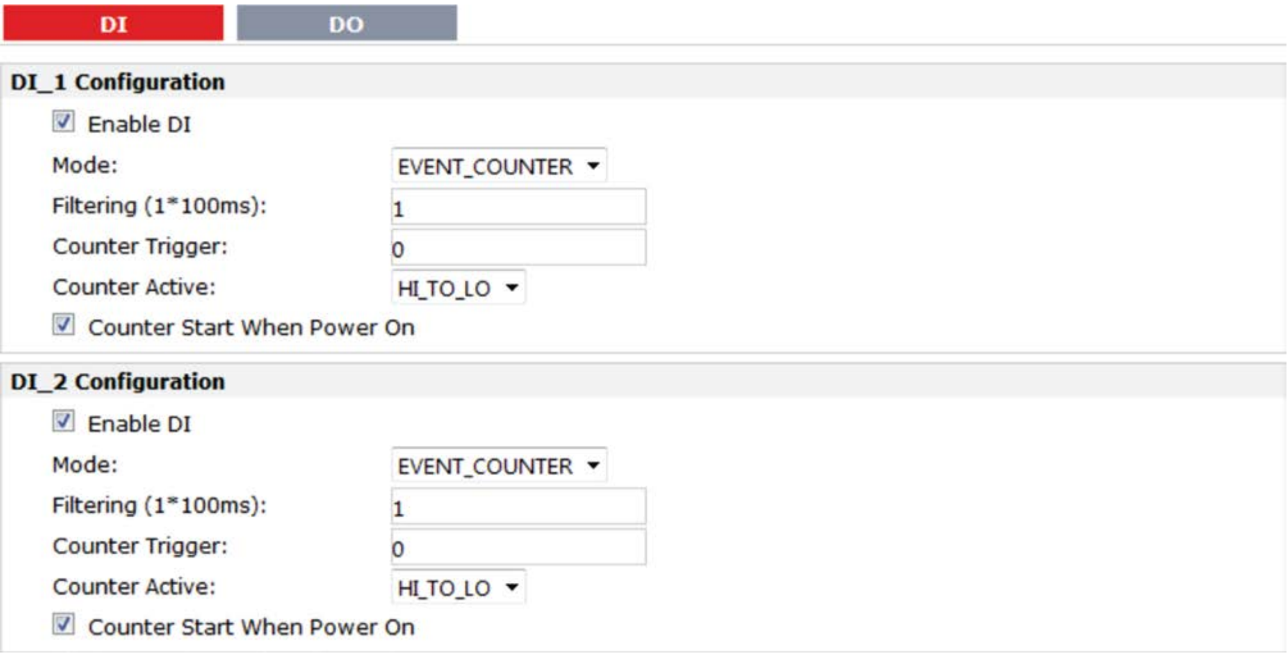
RS485 @ Serial		
Item	Description	Default
Baud-rate	Select from "300", "600", "1200", "2400", "4800", "9600", "19200", "38400", "57600" , "115200"and "230400".	115200
Data bit	Select from "7" and "8".	8
Parity	Select from "None", "Odd" and "Even".	None
Stop bit	Select from "1" and "2".	1
Protocol	Select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

Reading Interval @Modbus Master	Set interval time for reading Remote Channels. If we setup too much Remote Channels, router cannot be fully implemented in the period, router would give up the unfinished command. Note: According to the real environment, configure interval times reasonable.	30
Attempts @Modbus Master	The max times of read attempts. If a read instruction in Remote Channels is failure, and times achieve Attempts, AIRGATE-3G identify this instruction is "not read" status, and skip this instruction next read cycle. Only when this status last than 30 seconds, it will change to readable status, and then try to execute the command next cycle.	3
Max Response Time @Modbus Master	The maximum response time. When AIRGATE-3G execute a read command, this is the time of AIRGATE-3G waiting for responding. If AIRGATE-3G didn't get response from Modbus Slave devices over Max Response Time, AIRGATE-3G identify the instructions reading is timeout.	500
Time Between Commands @Modbus Master	The interval time between each instruction.	50
Logging Type @Modbus Master	The position for saving Modbus data. Only save Modbus data when AIRGATE-3G can't upload to the server. (Once AIRGATE-3G re-connect to server, AIRGATE-3G would upload the data and delete the data after finishing uploading. Flash: saving in Flash SD Card: saving in SD card USB Storage: saving in USB Storage	Null
Local IP @ Modbus over TCP	This item will show up When you enable any VPN tunnel of AIRGATE-3G, 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 over TCP	Enter the Local port for Modbus.	0
Attached serial device type @ Modbus over TCP	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 over TCP	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 Nlink	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 Nlink	Select From "Modbus RTU slave", "Modbus ASCⅡ slave". Modbus RTU slave: router connects to slave device which works under Modbus RTU protocol. Modbus ASCⅡ slave: router connects to slave device which works under Modbus ASCⅡ protocol.	Modbus RTU slave

3.15 CONFIGURATION -> DI/DO

This section allows users to set the parameters for the digital inputs (DI) and digital outputs (DO).



DI_1 Configuration

☑ Enable DI

Mode: EVENT_COUNTER

Filtering (1*100ms): 1

Counter Trigger: 0

Counter Active: HI_TO_LO

☑ Counter Start When Power On

DI_2 Configuration

☑ Enable DI

Mode: EVENT_COUNTER

Filtering (1*100ms): 1

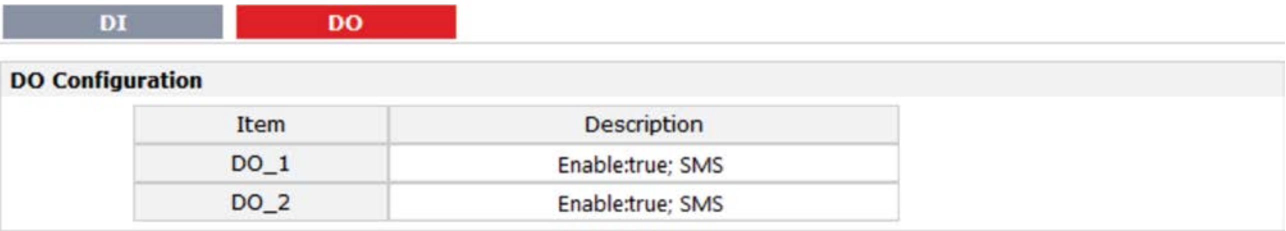
Counter Trigger: 0

Counter Active: HI_TO_LO

☑ Counter Start When Power On

DI @ DI/DO		
Item	Description	Default
Enable DI	Click to Enable DI.	Disable
Mode	Select from "OFF", "ON", "EVENT_COUNTER". OFF: Connect to GND (logic 0). When pin DI connects to GND, AIRGATE-3G will detect there is a DI alarm input. ON: Open from GND (logic 1). When pin DI does not connect to GND, AIRGATE-3G will detect there is a DI alarm input. EVENT_COUNTER: under event counter mode.	OFF
Filtering	Software filtering is used to control switch bounces. Input from 0 to 10000ms.	1
Count Trigger	Available when DI under Event Counter mode. Input from 0 to 100. (0=will not trigger alarm) It will trigger alarm when counter reaches this figure. After triggering alarm, DI will keep counting but not trigger alarm again.	0

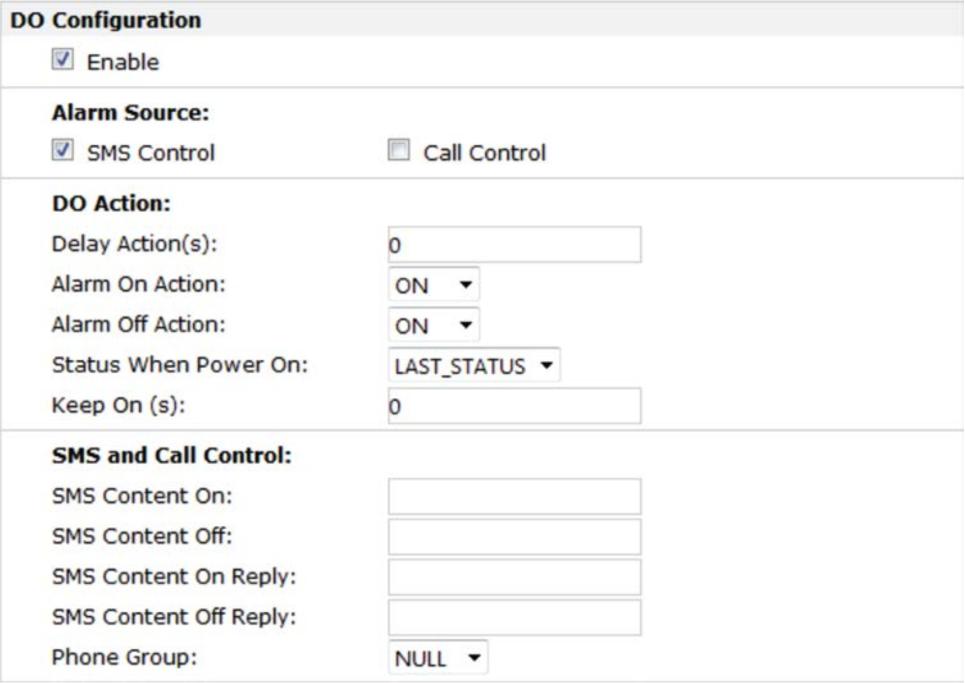
Counter Active	Available when DI under Event Counter mode. Select from “Hi to Lo”, “Lo to Hi”. In Event Counter mode, the channel accepts limit or proximity switches and counts events according to the ON/OFF status. When “Lo to Hi” is selected, the counter value increases when the attached switch is pushed. When “Hi to Lo” is selected, the counter value increases when the switch is pushed and released.	Lo to Hi
Counter Start When Power On	Available when DI under Event Counter mode. Start counting as soon as possible on the modem when enable this option. When AIRGATE-3G need to work under Event Counter mode, user shall enable “Counter Start When Power On”. If “Counter Start When Power On” is disabled, it will also start counting when receiving SMS command. Refer to another document *SMS command of AIRGATE-3G*.	Disable



DO Configuration

Item	Description
DO_1	Enable:true; SMS
DO_2	Enable:true; SMS

To set the digital outputs click on Enable: False.



DO Configuration

☑ Enable

Alarm Source:

☑ SMS Control ☐ Call Control

DO Action:

Delay Action(s): 0

Alarm On Action: ON

Alarm Off Action: ON

Status When Power On: LAST_STATUS

Keep On (s): 0

SMS and Call Control:

SMS Content On:

SMS Content Off:

SMS Content On Reply:

SMS Content Off Reply:

Phone Group: NULL

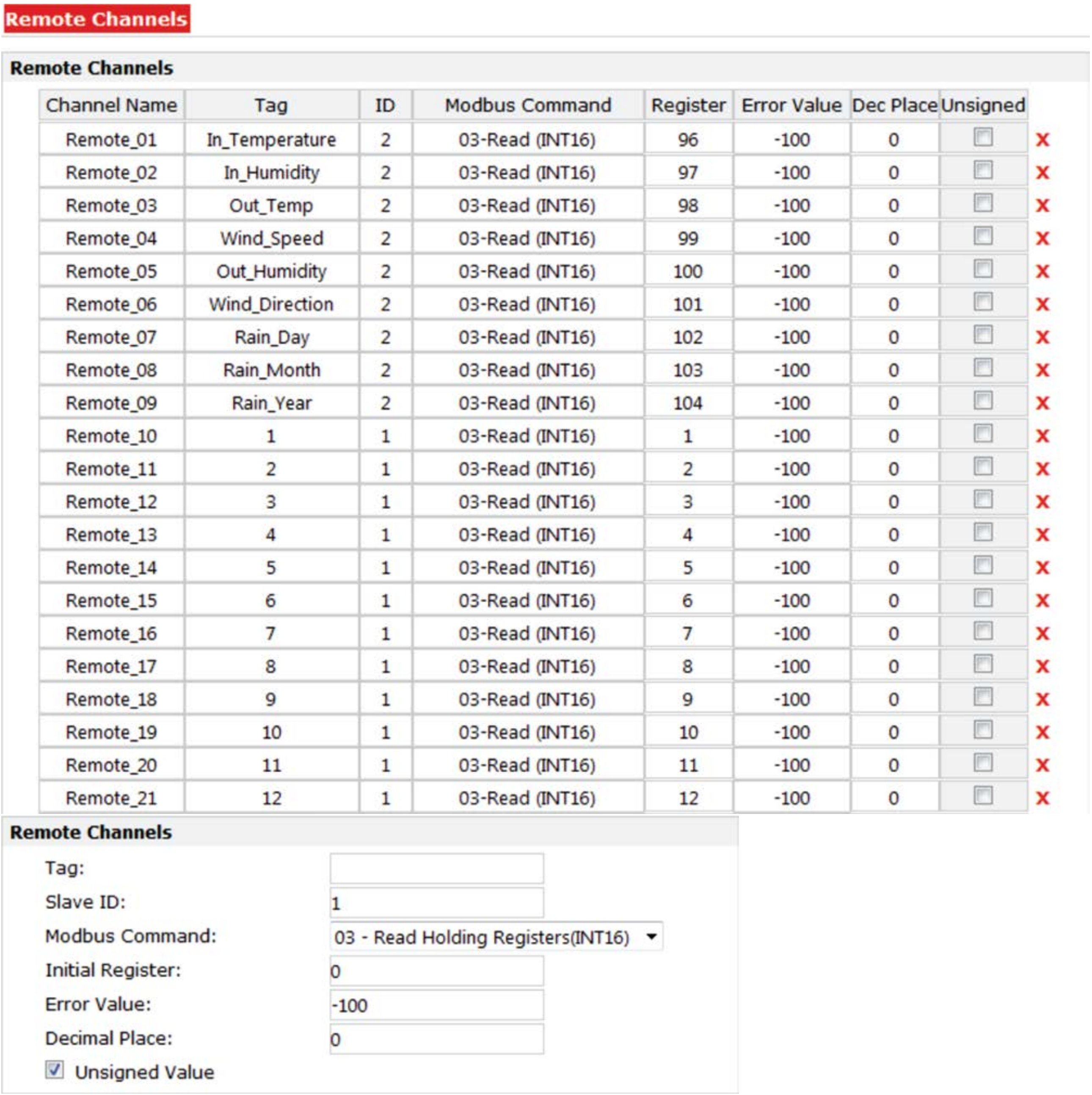
DO @ DI/DO		
Item	Description	Default
Enable	Click to enable DO.	Disable
Alarm Source	Digital Output initiates according to different alarm source. Selected from “SMS Control”, “Call Control”, selections can be one or more. SMS Control: Digital Output triggers the related action when receiving SMS from the number in the phone book. Call Control: Digital Output triggers the related action when receiving phone call from the number in the phone book.	Null

Delay on Action (s)	Time to execute an action.	0
Alarm On Action	Digital Output initiates when there is an alarm. Selected from “OFF”, “ON”, “Pulse”. OFF: Open from GND when triggered. ON: Short contact with GND when triggered. Pulse: Generates a square wave as specified in the pulse mode parameters when triggered.	ON
Alarm Off Action	Digital Output initiates when alarm recovered. Selected from “OFF”, “ON”, “Pulse”. OFF: Open from GND when triggered. ON: Short contact with GND when triggered. Pulse: Generates a square wave as specified in the pulse mode parameters when triggered.	ON
Status When Power On	Specify the Digital Output status when power on. Selected from “OFF”, “ON”. OFF: Open from GND. ON: Short contact with GND.	ON
Keep On (s)	Available when digital output Alarm On Action/Alarm Off Action status is ON, input the Digital Output keep on status time. Input from 0 to 600 seconds. (0=keep on until the next action)	0
Delay	Available when enable Pulse in Alarm On Action/Alarm Off Action. The first pulse will be generated after a “Delay”. Input from 0 to 3000ms. (0=generate pulse without delay)	0
Low	Available when enable Pulse in Alarm On Action/Alarm Off Action. In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The low-level widths are specified here. Input from 1 to 30000 ms.	10
High	Available when enable Pulse in Alarm On Action/Alarm Off Action. In Pulse Output mode, the selected digital output channel will generate a square wave as specified in the pulse mode parameters. The high level widths are specified here. Input from 1 to 3000 ms.	10
Output	Available when enable Pulse in Alarm On Action/Alarm Off Action. The number of pulses, input from 0 to 3000. (0 for continuous pulse output)	0
SMS Content On	Available when enable SMS Control in Alarm Source. Input the SMS content to enable “Alarm On Action” by SMS (1 to 128 ASC II char).	Null
SMS Content Off	Available when enable SMS Control in Alarm Source. Input the SMS content to enable “Alarm Off Action” by SMS. (1 to 128 ASC II char)	Null
SMS Content On Reply	Input the SMS content, which will be sent after DO was triggered. (1 to 128 ASC II char max).	Null
SMS Content Off Reply	Input the SMS content, which will be sent after DO was recovered. (1 to 128 ASC II char).	Null
Phone Group	Click to add phone groups.	Null

3.16 CONFIGURATION -> REMOTE CHANNELS

This section allows users to configure up to 64 remote channels.

***Note**: Modbus Master protocol is only available for RS485 serial port.*



Remote Channels

Remote Channels

Channel Name	Tag	ID	Modbus Command	Register	Error Value	Dec Place	Unsigned	
Remote_01	In_Temperature	2	03-Read (INT16)	96	-100	0	☐	✗
Remote_02	In_Humidity	2	03-Read (INT16)	97	-100	0	☐	✗
Remote_03	Out_Temp	2	03-Read (INT16)	98	-100	0	☐	✗
Remote_04	Wind_Speed	2	03-Read (INT16)	99	-100	0	☐	✗
Remote_05	Out_Humidity	2	03-Read (INT16)	100	-100	0	☐	✗
Remote_06	Wind_Direction	2	03-Read (INT16)	101	-100	0	☐	✗
Remote_07	Rain_Day	2	03-Read (INT16)	102	-100	0	☐	✗
Remote_08	Rain_Month	2	03-Read (INT16)	103	-100	0	☐	✗
Remote_09	Rain_Year	2	03-Read (INT16)	104	-100	0	☐	✗
Remote_10	1	1	03-Read (INT16)	1	-100	0	☐	✗
Remote_11	2	1	03-Read (INT16)	2	-100	0	☐	✗
Remote_12	3	1	03-Read (INT16)	3	-100	0	☐	✗
Remote_13	4	1	03-Read (INT16)	4	-100	0	☐	✗
Remote_14	5	1	03-Read (INT16)	5	-100	0	☐	✗
Remote_15	6	1	03-Read (INT16)	6	-100	0	☐	✗
Remote_16	7	1	03-Read (INT16)	7	-100	0	☐	✗
Remote_17	8	1	03-Read (INT16)	8	-100	0	☐	✗
Remote_18	9	1	03-Read (INT16)	9	-100	0	☐	✗
Remote_19	10	1	03-Read (INT16)	10	-100	0	☐	✗
Remote_20	11	1	03-Read (INT16)	11	-100	0	☐	✗
Remote_21	12	1	03-Read (INT16)	12	-100	0	☐	✗

Remote Channels

Tag:	
Slave ID:	1
Modbus Command:	03 - Read Holding Registers(INT16) ▾
Initial Register:	0
Error Value:	-100
Decimal Place:	0

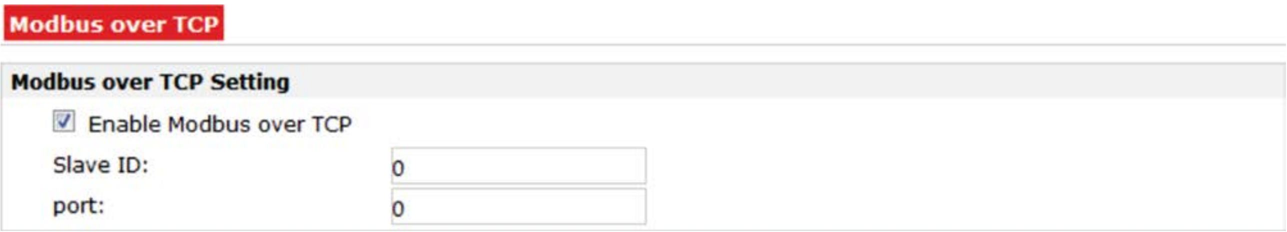
☑ Unsigned Value

Remote Channels		
Item	Description	Default
Tag	The identification of remote channel, it can be null or not null. If it were not null, AIRGATE-3G would upload alarm or information to platform with this identification.	Null
Slave ID	Modbus slave ID	1
Modbus Command	Read the command. 01- Read Coils 02- Read Discrete Input 03- Read Holding Registers(INT16) 03- Read Holding Registers(INT32) 03- Read Holding Registers(FLOAT) 04- Read Input Registers	Read Holding Registers(INT16)
Initial Register	The starting value of registers	0

Error Value	When reading is failed, the Error Value will be assigned to remote channel, then sending by alarm and upload to platform.	-100
Decimal Place	Use the dot to indicate the reading position of remote channel. For example: value of remote channel is 1234, and Decimal Place is equal to 2, and the real value is 12.34.	0
Unsigned Value	Use to identify remote channel for unsigned.	Disable

3.17 CONFIGURATION->MODBUS OVER TCP

This section allows users to configure the Modbus over TCP. Modbus over TCP slave functions, the remote can access the AIRGATE-3G's internal registers through Modbus over TCP.



Modbus over TCP

Modbus over TCP Setting

☑ Enable Modbus over TCP

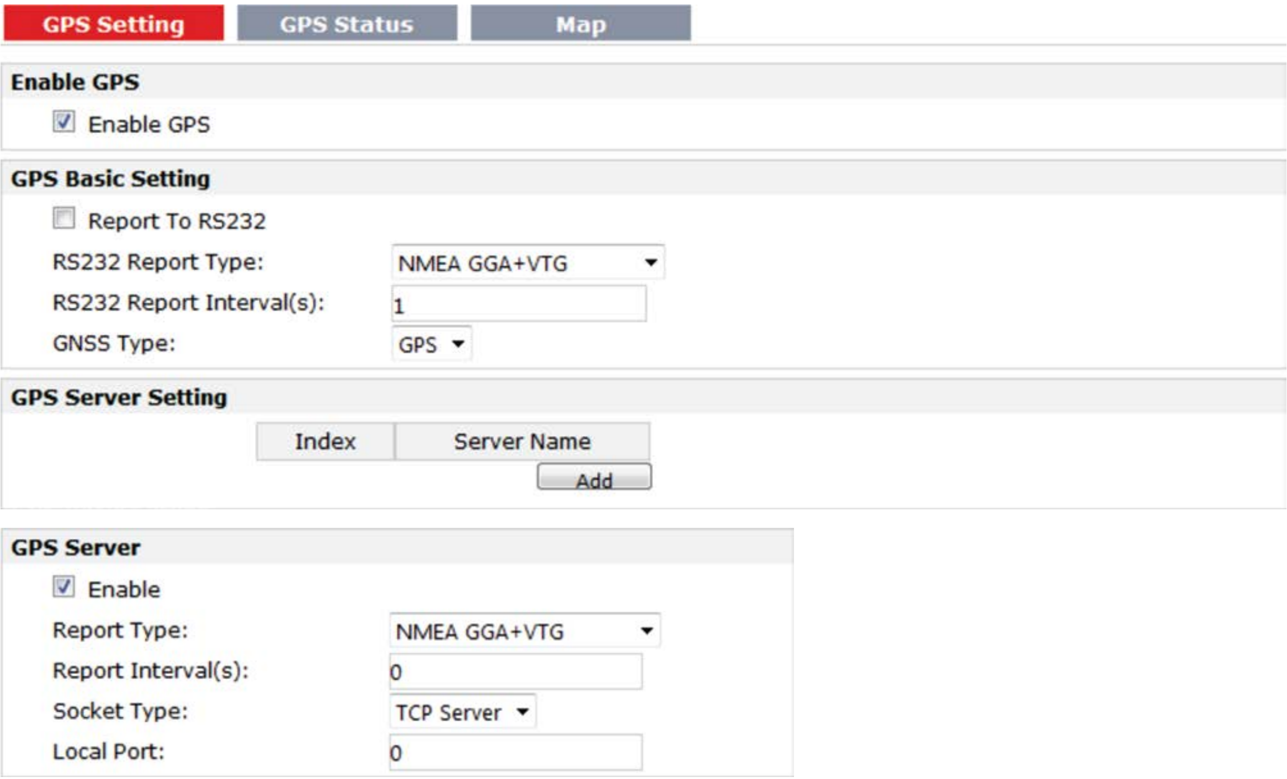
Slave ID: 0

port: 0

Modbus over TCP		
Item	Description	Default
Enable Modbus over TCP	Click to enable Modbus over TCP.	Disable
Slave ID	Enter the slave ID of AIRGATE-3G.	Null
Port	Enter the port for Modbus over TCP connection.	Null

3.18 CONFIGURATION -> GPS

This section allows users to set the GPS setting parameters.



Enable GPS

☑ Enable GPS

GPS Basic Setting

□ Report To RS232

RS232 Report Type: NMEA GGA+VTG

RS232 Report Interval(s): 1

GNSS Type: GPS

GPS Server Setting

Index	Server Name

GPS Server

☑ Enable

Report Type: NMEA GGA+VTG

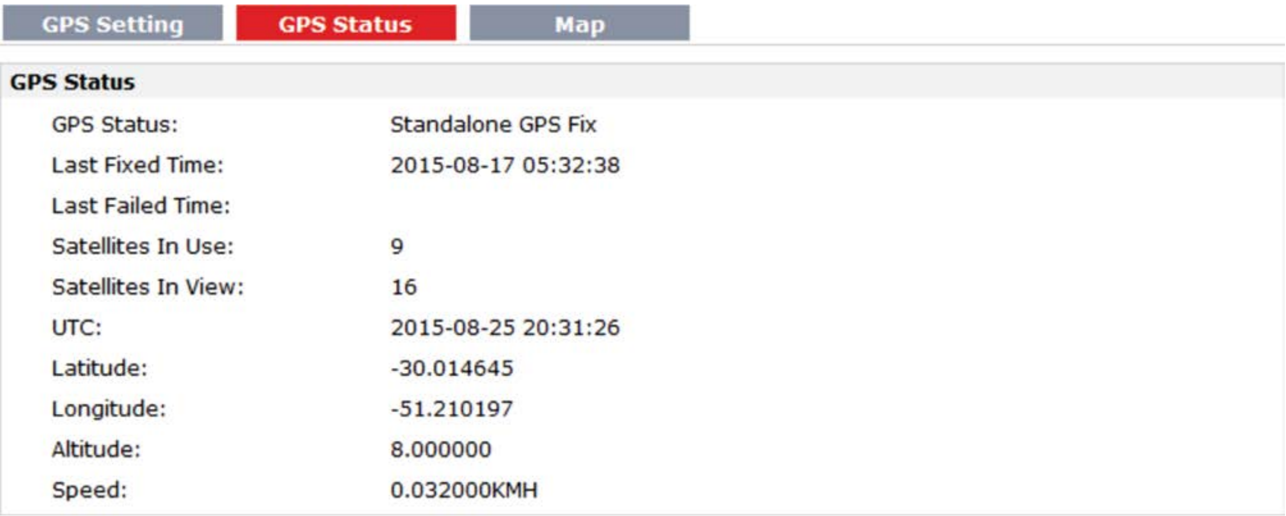
Report Interval(s): 0

Socket Type: TCP Server

Local Port: 0

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

This section allows users to check the GPS status.

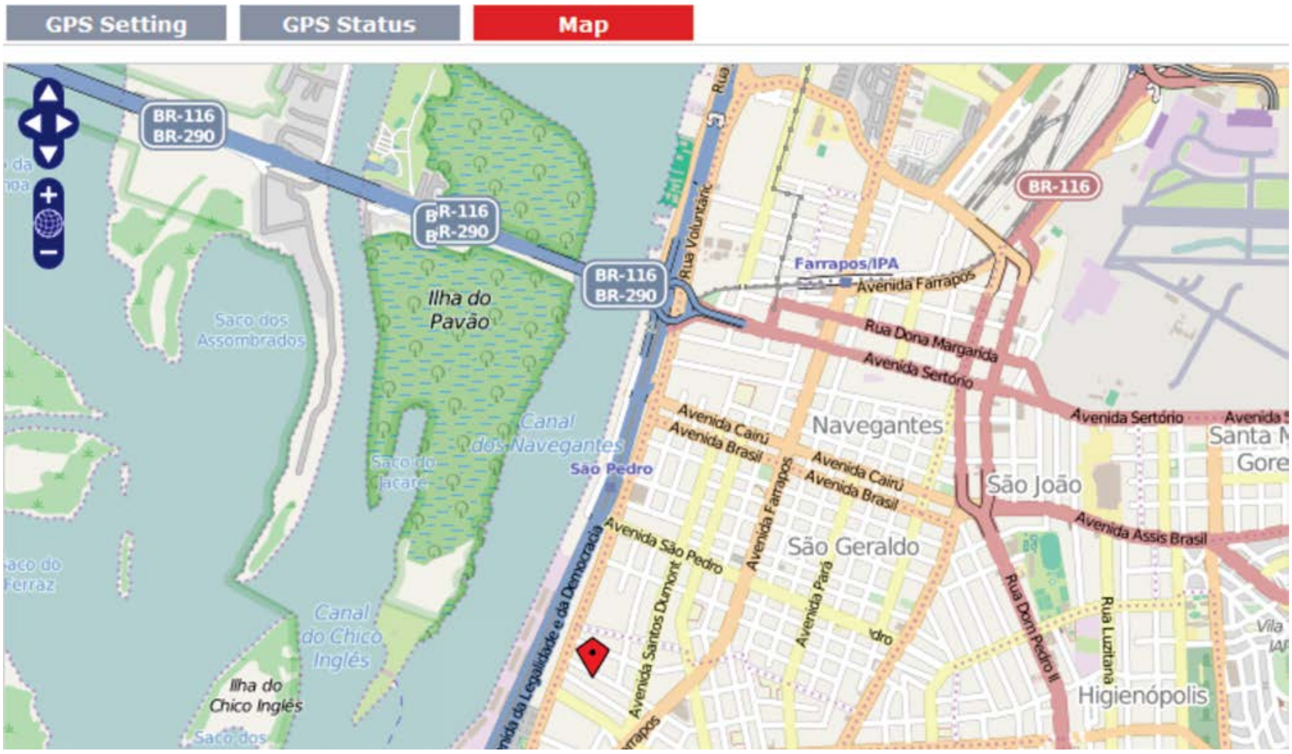


GPS Status

GPS Status:	Standalone GPS Fix
Last Fixed Time:	2015-08-17 05:32:38
Last Failed Time:	
Satellites In Use:	9
Satellites In View:	16
UTC:	2015-08-25 20:31:26
Latitude:	-30.014645
Longitude:	-51.210197
Altitude:	8.000000
Speed:	0.032000KMH

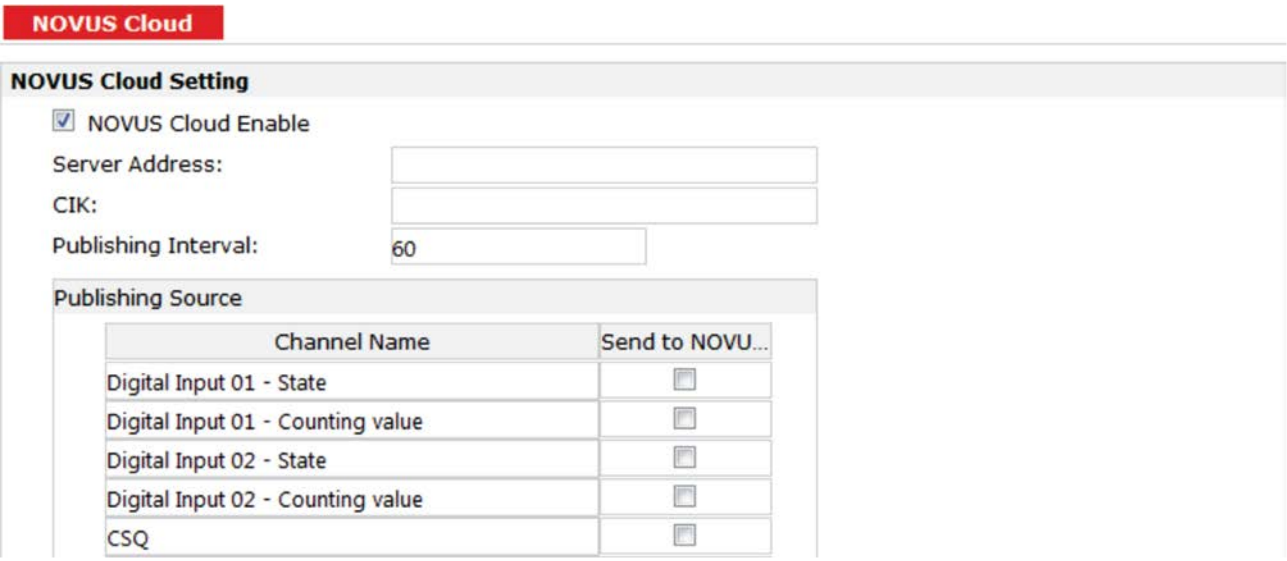
GPS Status @ GPS		
Item	Description	Default
GPS Status	Show the GPS Status. GPS status includes: Not Installed, Disabled, No Fix/Invalid, Standalone GPS Fix, Differential GPS Fix. Not Installed: No GPS module inside. Disabled: GPS function is not enabled (not click “Enable GPS” in item “GPS Setting”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

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



3.19 CONFIGURATION -> NOVUS CLOUD

This section allows users to configure the NOVUS Cloud.


NOVUS Cloud

NOVUS Cloud Setting

☑ NOVUS Cloud Enable

Server Address:

CIK:

Publishing Interval: 60

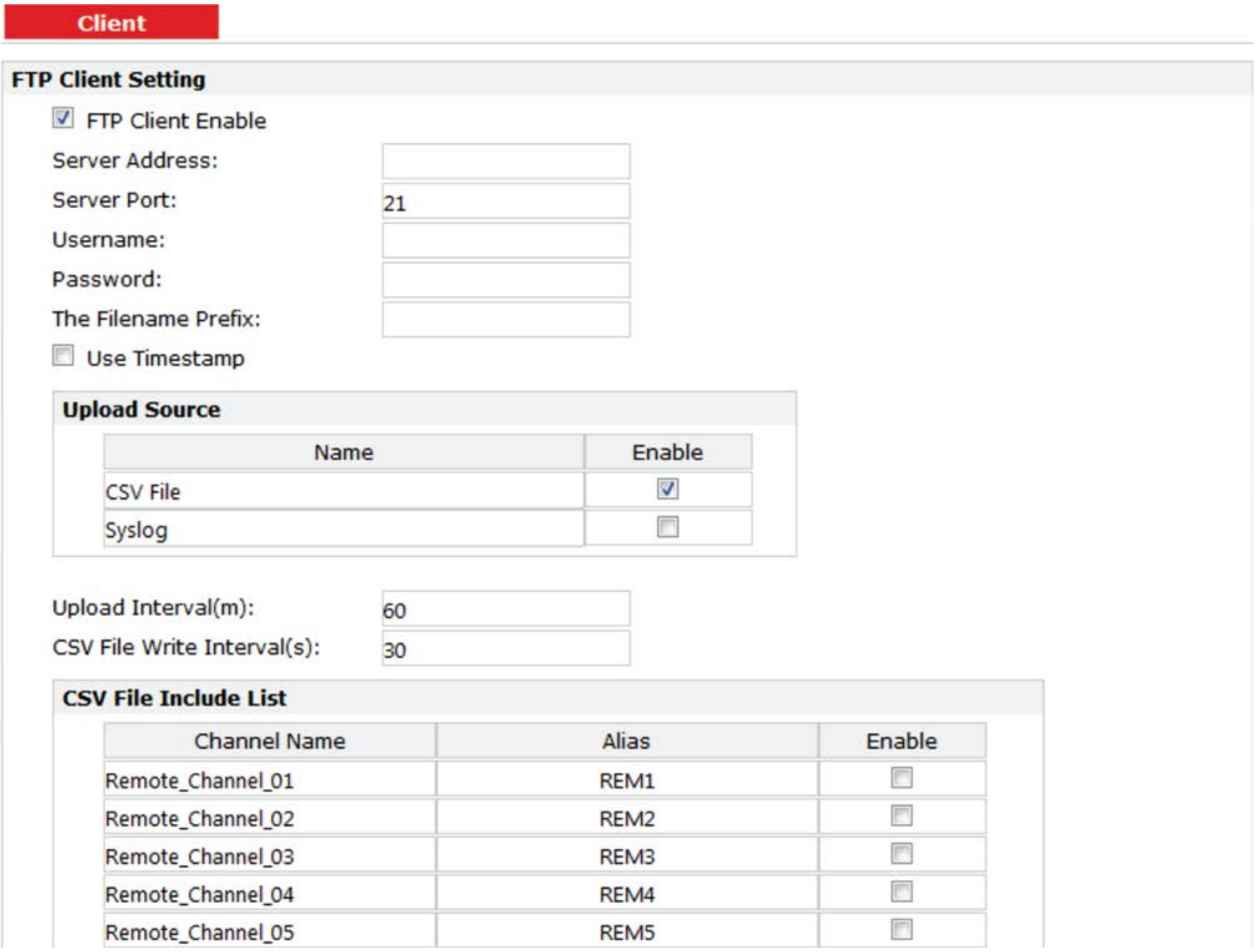
Publishing Source

Channel Name	Send to NOVU...
Digital Input 01 - State	□
Digital Input 01 - Counting value	□
Digital Input 02 - State	□
Digital Input 02 - Counting value	□
CSQ	□

NOVUS Cloud		
Item	Description	Default
Server address	Enter the IP address or domain name of the server.	Null
Port	The port of NOVUS Cloud server that allow user to link in.	1
CIK	This is a unique ID of AIRGATE-3G, which allows its connection to NOVUS Cloud.	Null
Publishing interval	From 1 minute to 24 hours. Time interval for sending AIRGATE-3G's current values to NOVUS Cloud. The first publishing must be made as soon as the setup is completed.	60
Channel Name	The name of those channels that will be published.	
Send to Exosite	Select the channels to publish to NOVUS Cloud.	Disable

3.20 CONFIGURATION -> FTP

By connecting to an FTP server, you can report the previously registered channels on the router.



FTP Client Setting

☑ FTP Client Enable

Server Address:

Server Port: 21

Username:

Password:

The Filename Prefix:

☐ Use Timestamp

Upload Source

Name	Enable
CSV File	☑
Syslog	☐

Upload Interval(m): 60

CSV File Write Interval(s): 30

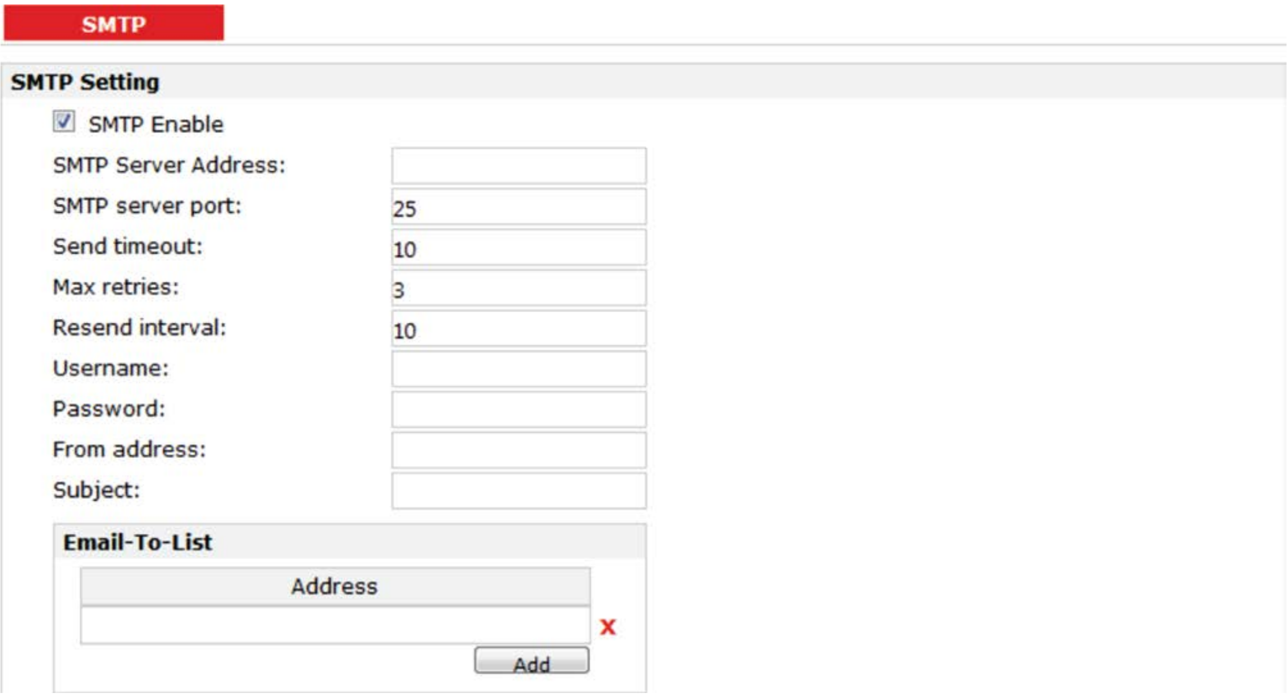
CSV File Include List

Channel Name	Alias	Enable
Remote_Channel_01	REM1	☐
Remote_Channel_02	REM2	☐
Remote_Channel_03	REM3	☐
Remote_Channel_04	REM4	☐
Remote_Channel_05	REM5	☐

FTP		
Item	Description	Default
Server Address	Enter the IP address or server domain name.	Null
Server Port	Set the port number to connect to the FTP server.	21
User	Enter the user name of the FTP server.	Null
Password	Enter the user password for the FTP server.	Null
File Name Prefix	Sets the file name prefix to the FTP server.	Null
Use Timestamp	Enables the format of UNIX timestamp.	Disabled

3.21 CONFIGURATION ->SMTP

This section allows users to configure the SMTP.



SMTP Setting

☑ SMTP Enable

SMTP Server Address:

SMTP server port: 25

Send timeout: 10

Max retries: 3

Resend interval: 10

Username:

Password:

From address:

Subject:

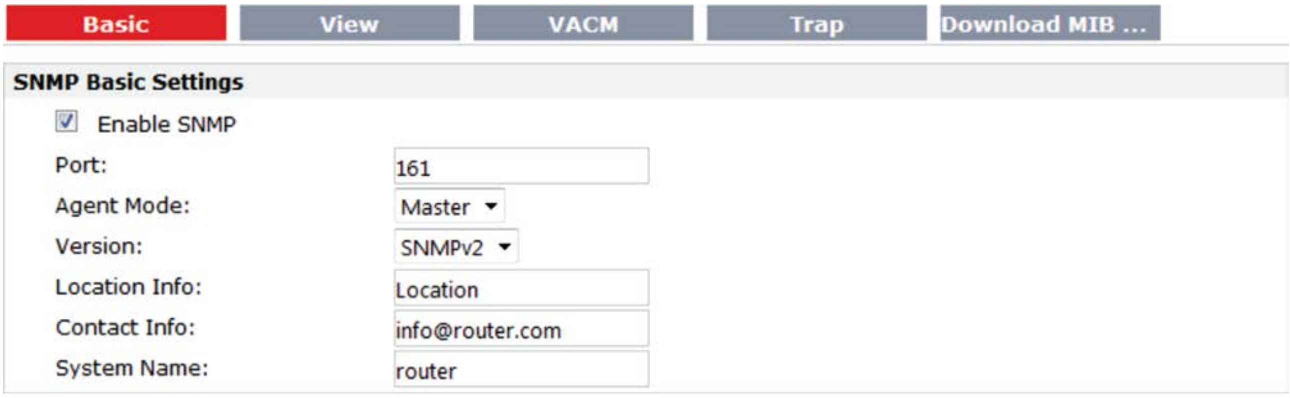
Email-To-List

Address

SMTP		
Item	Description	Default
SMTP	Click to enable SMTP	Disable
SMTP server Address	Enter the SMTP server IP Address or domain name.	Null
SMTP server port	Enter the SMTP server port.	25
Send timeout	The maximum timeout for sending email.	10
Max retries	The max retries times for sending email.	3
Resend interval	The time interval of resending email.	10
Username	The username of SMTP server.	Null
Password	The password of SMTP server.	Null
From address	The source address of the email.	Null
Subject	The subject of this email.	Null
Email-To-List	The receiver address list.	Null

3.22 CONFIGURATION -> SNMP

This section allows users to set the SNMP parameters.



SNMP Basic Settings

☑ Enable SNMP

Port: 161

Agent Mode: Master

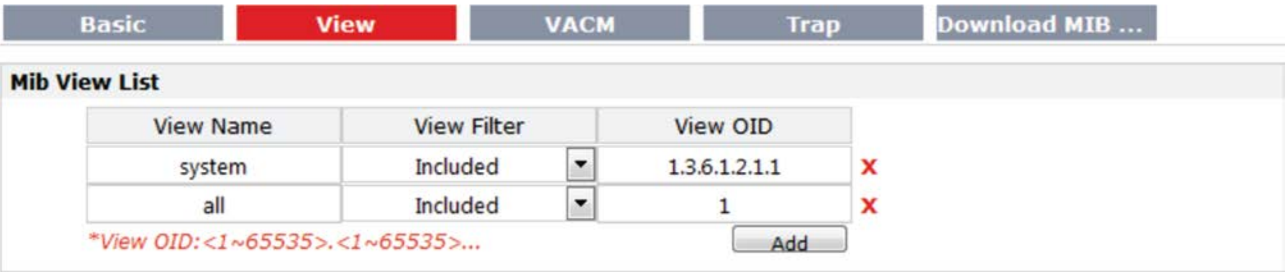
Version: SNMPv2

Location Info: Location

Contact Info: info@router.com

System Name: router

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.	Location
Contact Info	Enter the router’s contact info which will send to SNMP client.	info@NOVUS.com
System name	Enter the router’s system name which will send to SNMP client.	router

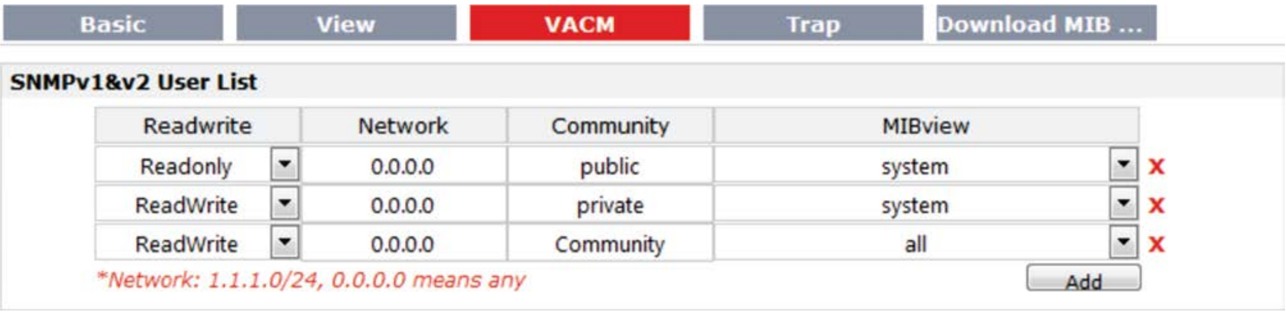


Mib View List

View Name	View Filter	View OID
system	Included	1.3.6.1.2.1.1
all	Included	1

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

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

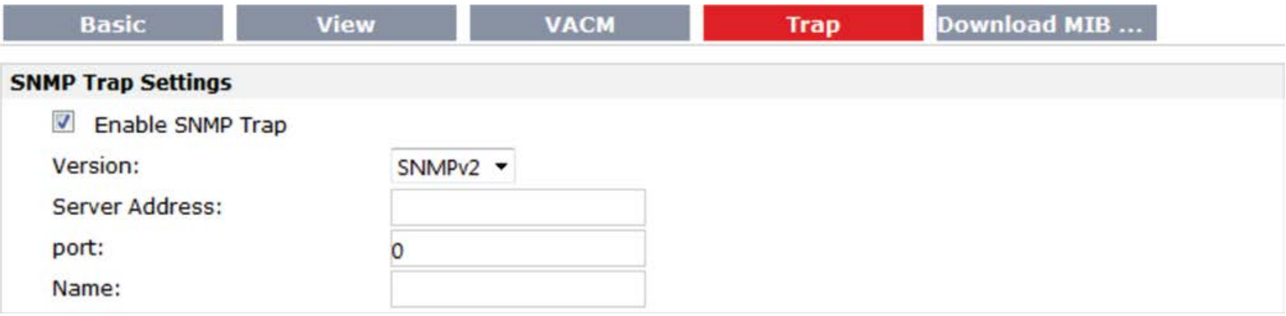


SNMPv1&v2 User List

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

*Network: 1.1.1.0/24, 0.0.0.0 means any

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



SNMP Trap Settings

☑ Enable SNMP Trap

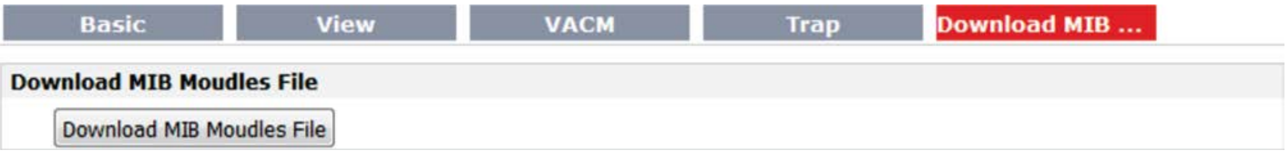
Version: SNMPv2

Server Address:

port: 0

Name:

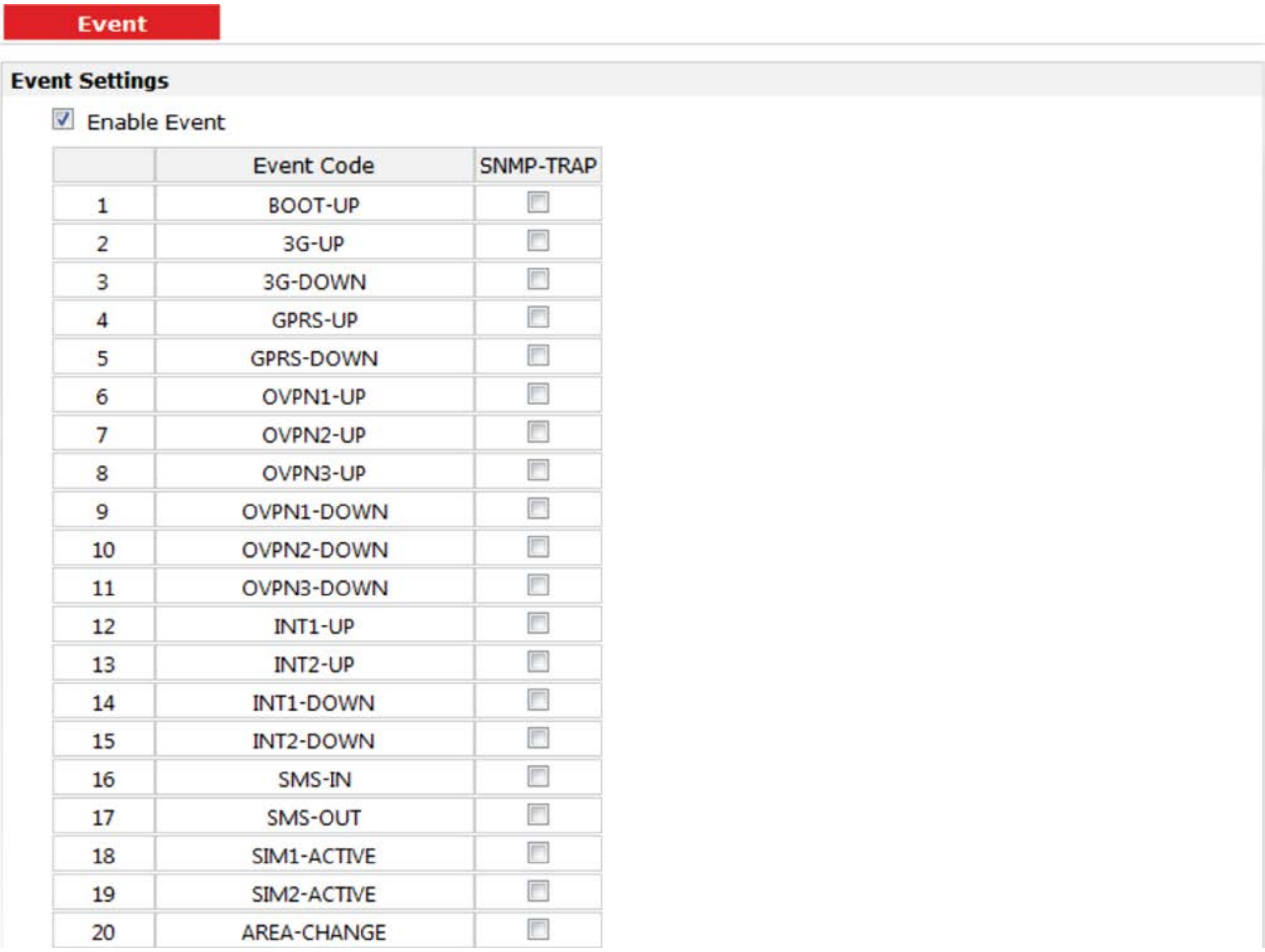
Trap @ SNMP		
Item	Description	Default
Enable SNMP Trap	Click to enable SNMP Trap feature.	Disable
Version	Select from “SNMPv1”, “SNMPv2” and “SNMPv3”.	SNMPv2
Server Address	Enter SNMP server’s IP address.	Null
Port	Enter SNMP server’s port number	0
Name	Enter SNMP server’s name.	Null



Download MIB Moudles File

3.23 CONFIGURATION -> EVENT

This section allows users to set the Event parameters.



Event Settings

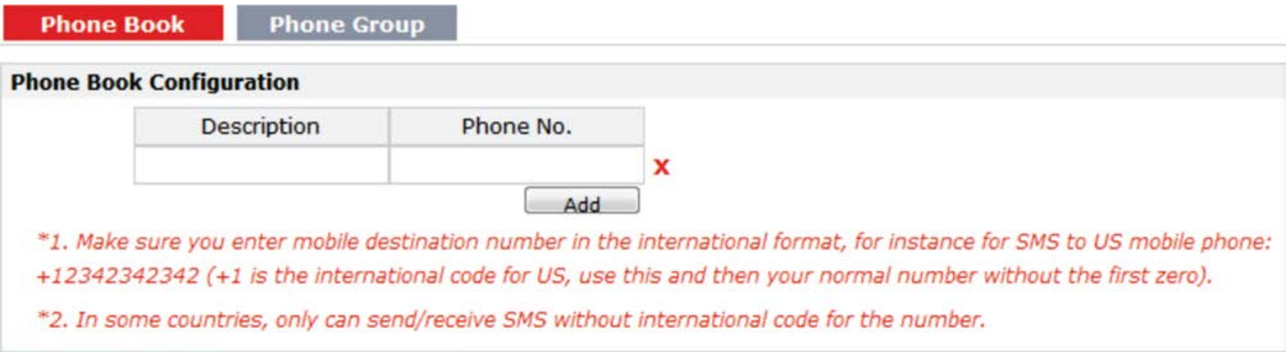
☑ Enable Event

	Event Code	SNMP-TRAP
1	BOOT-UP	☐
2	3G-UP	☐
3	3G-DOWN	☐
4	GPRS-UP	☐
5	GPRS-DOWN	☐
6	OVPN1-UP	☐
7	OVPN2-UP	☐
8	OVPN3-UP	☐
9	OVPN1-DOWN	☐
10	OVPN2-DOWN	☐
11	OVPN3-DOWN	☐
12	INT1-UP	☐
13	INT2-UP	☐
14	INT1-DOWN	☐
15	INT2-DOWN	☐
16	SMS-IN	☐
17	SMS-OUT	☐
18	SIM1-ACTIVE	☐
19	SIM2-ACTIVE	☐
20	AREA-CHANGE	☐

Event		
Item	Description	Default
Enable Event	Click to enable Event feature. This feature is used to report AIRGATE-3G’s main running event to SNMP-TRAP or NovusLink. 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 “NovusLink” as the server, when AIRGATE-3G dial up to connect to 3G network, it will send event code “3G-UP” as well as relevant information to NovusLink.	Disable

3.24 CONFIGURATION -> PHONE BOOK

This section allows users to set the Phone Book parameters.



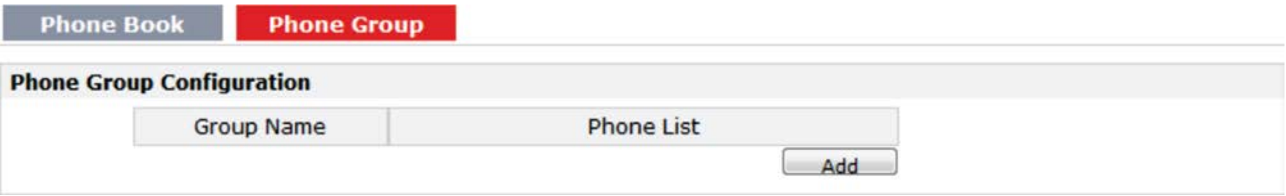
Phone Book Configuration

Description	Phone No.

*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).

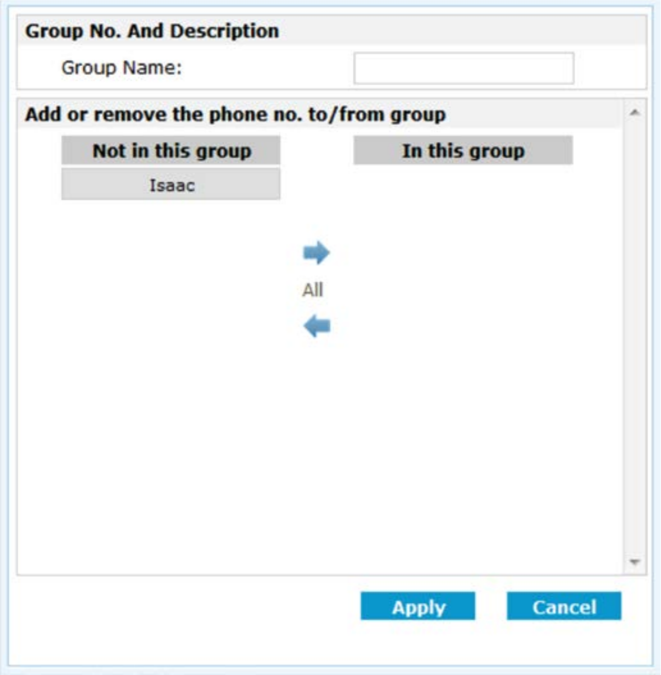
*2. In some countries, only can send/receive SMS without international code for the number.

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



Phone Group Configuration

Group Name	Phone List



Group No. And Description

Group Name:

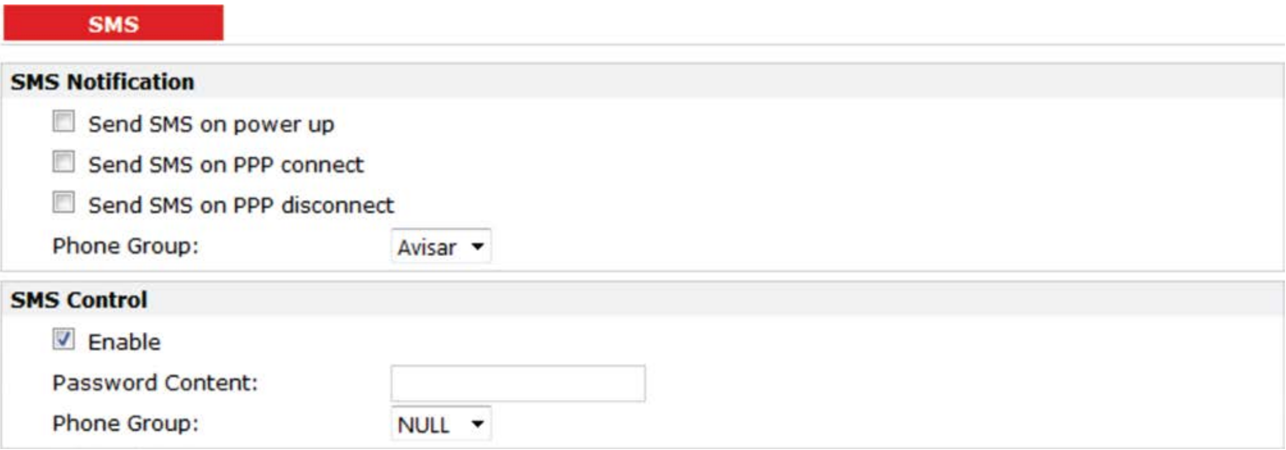
Add or remove the phone no. to/from group

Not in this group	In this group
Isaac	

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

3.25 CONFIGURATION -> SMS

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



SMS Notification

□ Send SMS on power up

□ Send SMS on PPP connect

□ Send SMS on PPP disconnect

Phone Group: Avisar

SMS Control

☑ Enable

Password Content:

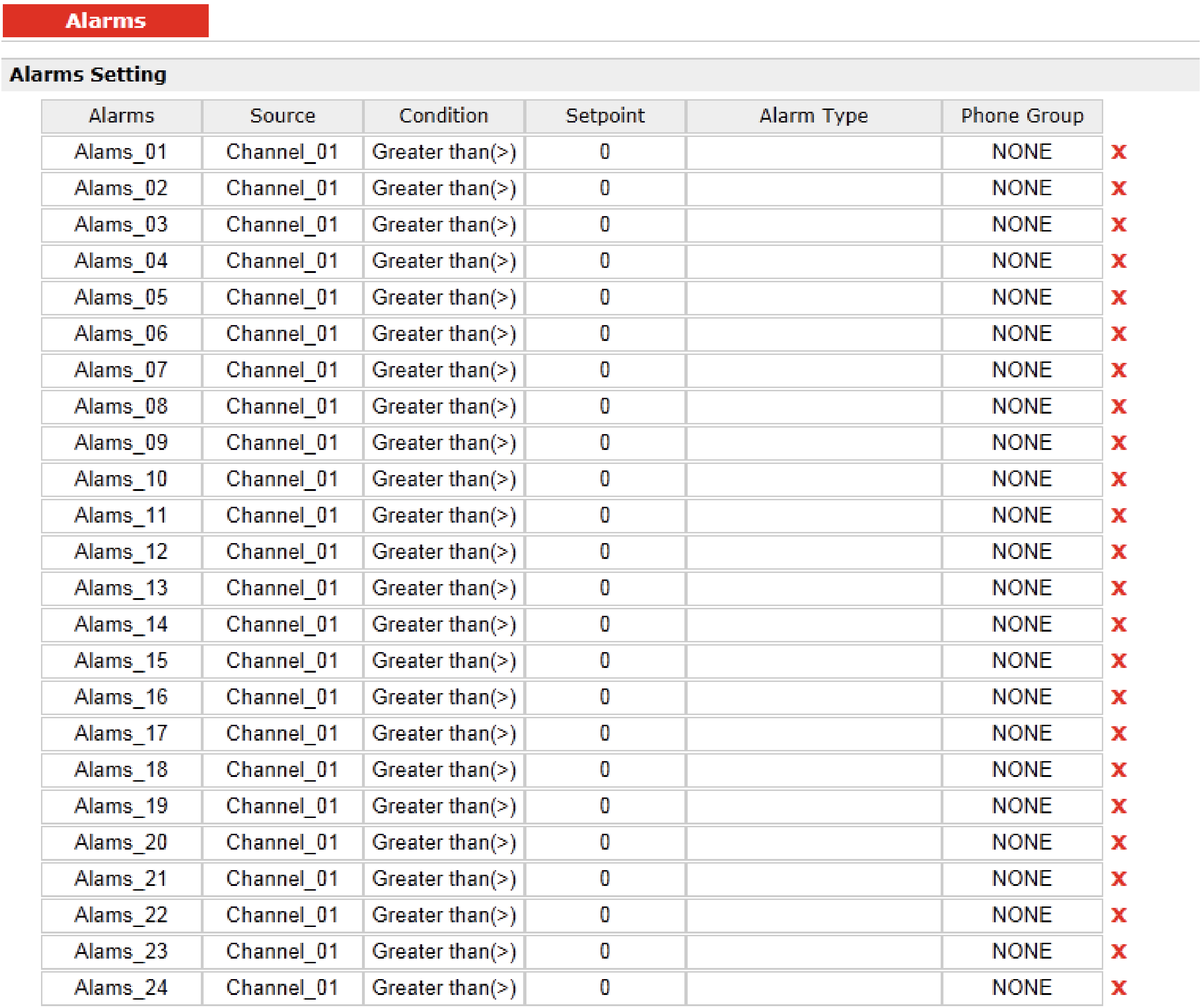
Phone Group: NULL

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

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

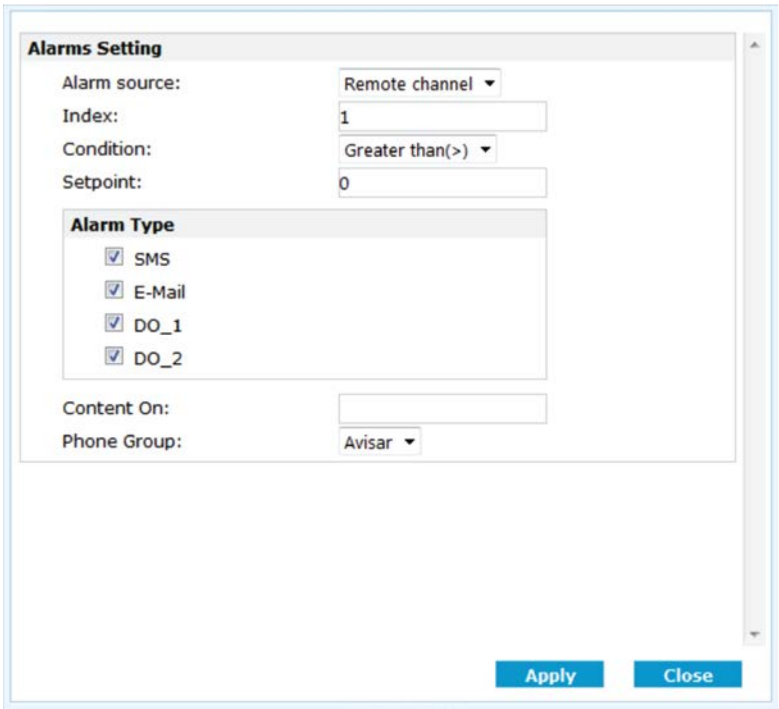
3.26 CONFIGURATION ->ALARMS

This section allows users to configure the alarms.



Alarms Setting

Alarms	Source	Condition	Setpoint	Alarm Type	Phone Group	
Alams_01	Channel_01	Greater than(>)	0		NONE	x
Alams_02	Channel_01	Greater than(>)	0		NONE	x
Alams_03	Channel_01	Greater than(>)	0		NONE	x
Alams_04	Channel_01	Greater than(>)	0		NONE	x
Alams_05	Channel_01	Greater than(>)	0		NONE	x
Alams_06	Channel_01	Greater than(>)	0		NONE	x
Alams_07	Channel_01	Greater than(>)	0		NONE	x
Alams_08	Channel_01	Greater than(>)	0		NONE	x
Alams_09	Channel_01	Greater than(>)	0		NONE	x
Alams_10	Channel_01	Greater than(>)	0		NONE	x
Alams_11	Channel_01	Greater than(>)	0		NONE	x
Alams_12	Channel_01	Greater than(>)	0		NONE	x
Alams_13	Channel_01	Greater than(>)	0		NONE	x
Alams_14	Channel_01	Greater than(>)	0		NONE	x
Alams_15	Channel_01	Greater than(>)	0		NONE	x
Alams_16	Channel_01	Greater than(>)	0		NONE	x
Alams_17	Channel_01	Greater than(>)	0		NONE	x
Alams_18	Channel_01	Greater than(>)	0		NONE	x
Alams_19	Channel_01	Greater than(>)	0		NONE	x
Alams_20	Channel_01	Greater than(>)	0		NONE	x
Alams_21	Channel_01	Greater than(>)	0		NONE	x
Alams_22	Channel_01	Greater than(>)	0		NONE	x
Alams_23	Channel_01	Greater than(>)	0		NONE	x
Alams_24	Channel_01	Greater than(>)	0		NONE	x



Alarms Setting

Alarm source: Remote channel

Index: 1

Condition: Greater than(>)

Setpoint: 0

Alarm Type

☑ SMS

☑ E-Mail

☑ DO_1

☑ DO_2

Content On:

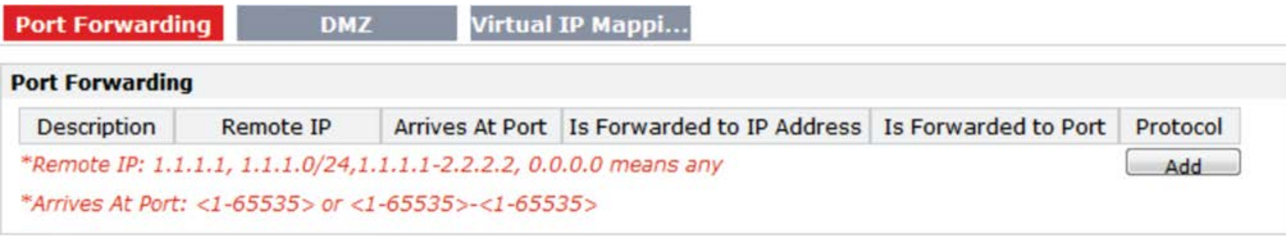
Phone Group: Avisar

Alarms		
Item	Description	Default
Alarm Source	Select from “Remote Channel”, ”GPS”, “CSQ”, “DI”, ”Cellular Status”.	Remote channel
Index	Use to identify the position of Remote Channel or DI.	1
Condition	The conditions of trigger alarm. # Greater than(>) # Less than(<) # Equal(=) # Unequal(!=)	Greater than (>)
Setpoint	The alarm threshold.	0
Alarm Type	The alarm types. # SMS # E-Mail # DO_1 # DO_2	off
Content ON	The content of alarm on.	null

3.27 CONFIGURATION -> NAT/DMZ

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

Port Forwarding enables to set manually a rule in the router to send all data received on a set of Internet ports to another port and LAN IP address.



Port Forwarding

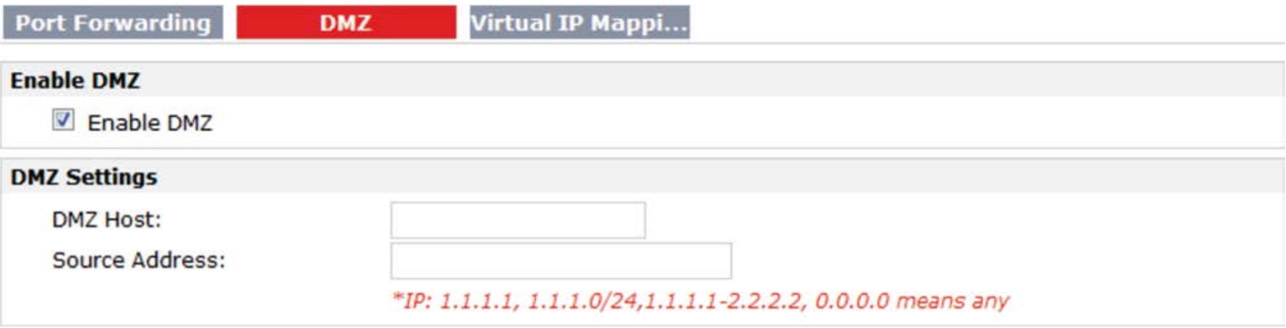
Description	Remote IP	Arrives At Port	Is Forwarded to IP Address	Is Forwarded to Port	Protocol

*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

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

To add a rule you must click on Add button and fill the NAT rule fields.

Port Forwarding @ NAT/DMZ		
Item	Description	Default
Description	Set a description for this rule.	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.	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



Enable DMZ

☑ Enable DMZ

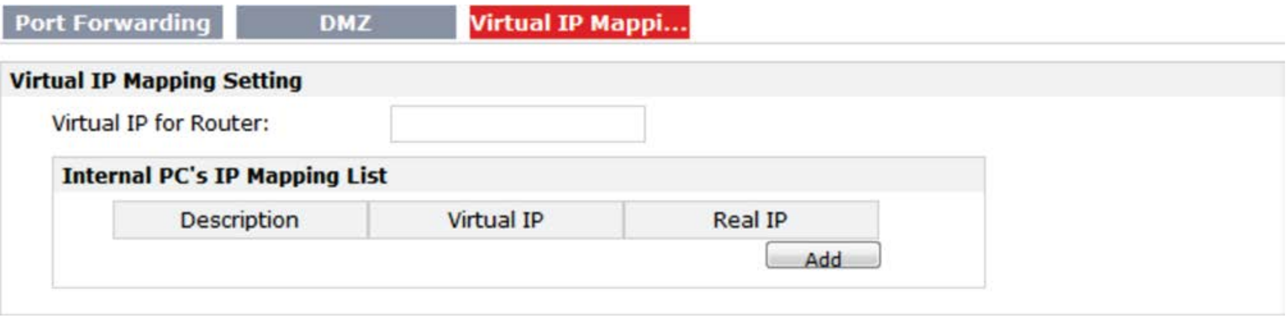
DMZ Settings

DMZ Host:

Source Address:

*IP: 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.	Disabled
DMZ Host	Enter the IP address of the DMZ host which on the internal network.	Null
Source Address	Set the address which can talk to the DMZ host. Null means for any addresses.	Null

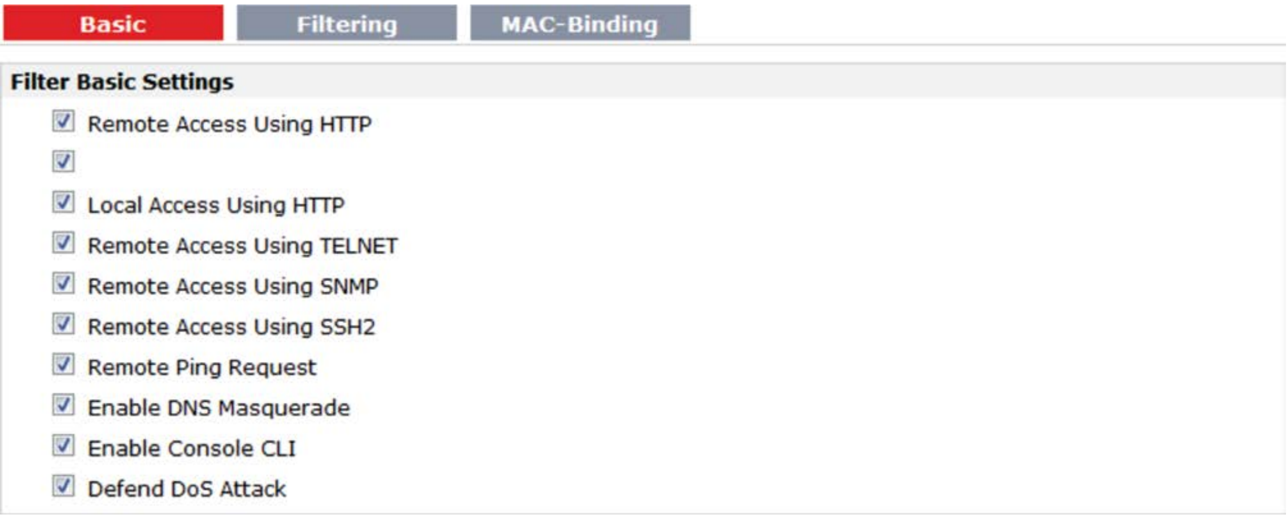


To add a rule you must click on Add button and fill the fields.

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

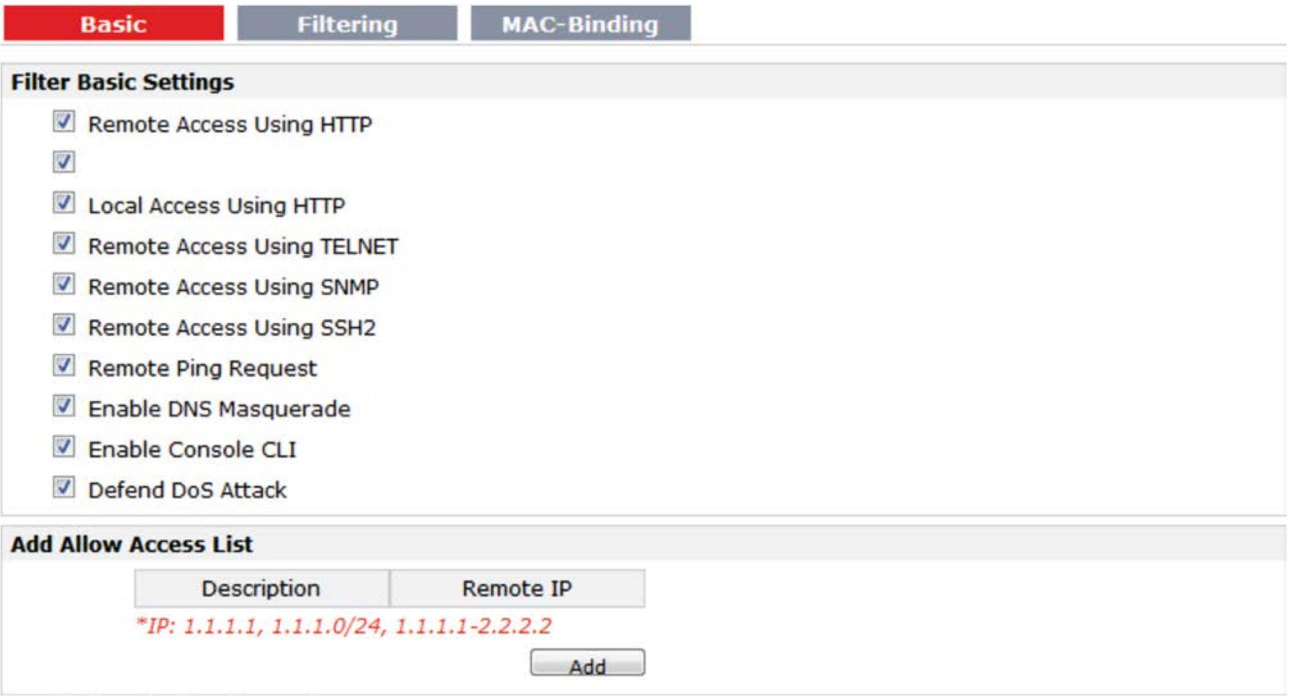
3.28 CONFIGURATION -> FIREWALL

This section allows users to set the firewall parameters.



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

If you disable one of tabs: “Remote Access Using HTTP”, “Remote Access Using TELNET”, “Remote Access Using SNMP”, “Remote Access Using SSH2” or “Remote Ping Request”, it will pop up “Add Allow Access List” to allow you to preset specific user to access to WAN interface of AIRGATE-3G. For example, if you disable “Remote Ping Request” and add “Remote IP” then only these specific users can ping to WAN interface of AIRGATE-3G.



Filter Basic Settings

☑ Remote Access Using HTTP

☑

☑ Local Access Using HTTP

☑ Remote Access Using TELNET

☑ Remote Access Using SNMP

☑ Remote Access Using SSH2

☑ Remote Ping Request

☑ Enable DNS Masquerade

☑ Enable Console CLI

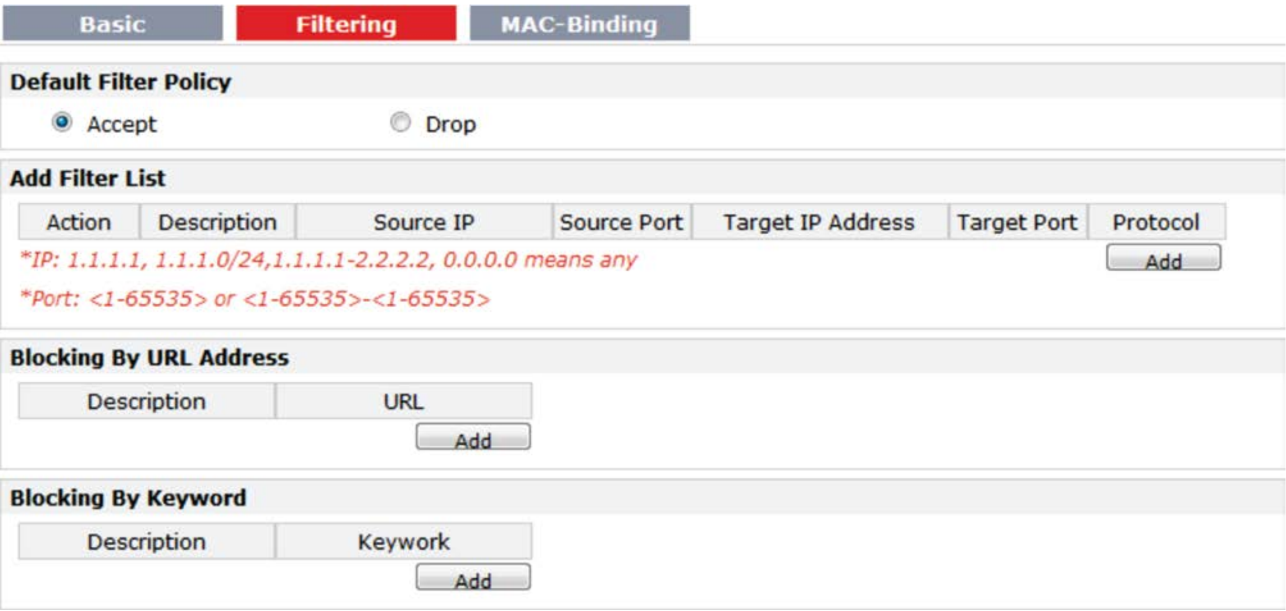
☑ Defend DoS Attack

Add Allow Access List

Description	Remote IP

*IP: 1.1.1.1, 1.1.1.0/24, 1.1.1.1-2.2.2.2

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
Local Access Using HTTP	Enable to allow users to access the router by LAN via HTTP	Enable
Remote Access Using TELNET	Enable to allow users to access the router remotely on the internet side via Telnet.	Enable
Remote Access Using SNMP	Enable to allow users to access the router remotely on the internet side via SNMP.	Enable
Remote Access Using SSH2	Enable to allow users to access the router remotely on the internet side via SSH2.	Enable
Remote Ping Request	Enable to make router reply the Ping requests from the internet side.	Enable
Enable DNS Masquerade	Open the 53 port of the router, enable users to use the DNS function of the router.	Enable
Enable Console CLI	Enable to configurate router through Command Line Interface.	Enable
Defend DoS Attack	Enable to defend DoS attack. DoS attack is an attempt to make a machine or network resource unavailable to its intended users.	Enable



Default Filter Policy

● Accept ○ Drop

Add Filter List

Action	Description	Source IP	Source Port	Target IP Address	Target Port	Protocol

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

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

Blocking By URL Address

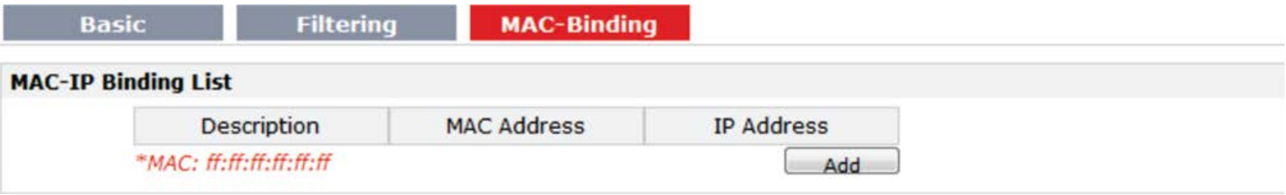
Description	URL

Blocking By Keyword

Description	Keywork

Filtering @ Firewall		
Item	Description	Default
Default Filter Policy	Select from “Accept” and “Drop”. Accept: Router will accept all the connecting requests except the hosts which fit the filter list. Drop: Router will only reject 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
Description	Define a description for the filter.	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”.	TCP
Blocking By URL Address	Click “Add” to add a URL list (max 10).	Null
Description	Define a description for the blocked URL.	Null
URL	Block the access according to the URL address that filled in the blank.	Null
Blocking By Keywork	Click “Add” to add a Keywork list.	Null
Description	Definer a description for the word blocked key.	Null
Keywork	Block the access according to the Keywork that filled in the blank.	Null

***Note**: You can use “-“to define a range of IP addresses or ports, e.g. 1.1.1.1-2.2.2.2, 10000-12000. The priority of **Filter List** is higher than **Default Filter Policy**. Firewall policy would not take effect on the packet receive to AIRGATE-3G itself, but only take effect on packet "pass through" the AIRGATE-3G.*



MAC-IP Binding List

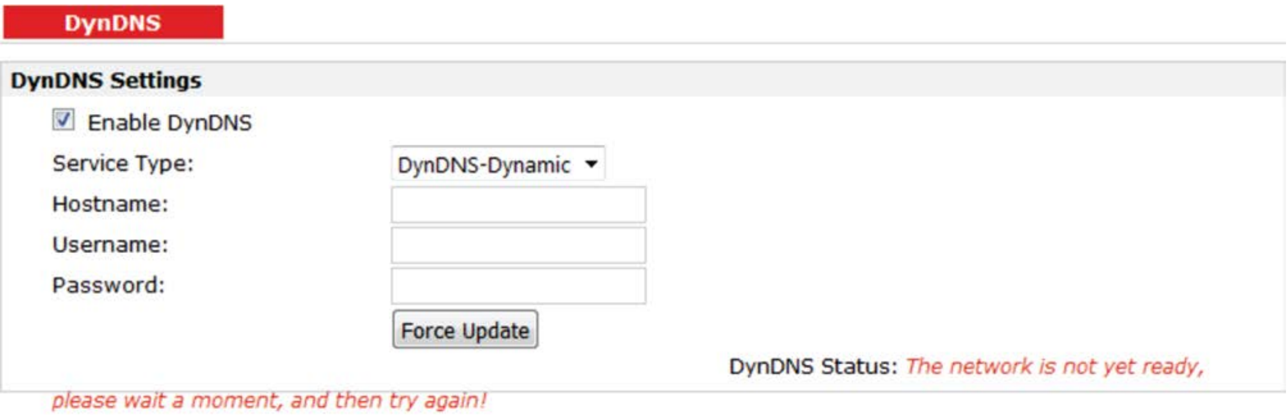
Description	MAC Address	IP Address

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

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. (Max 20)	Null
Description	Define a description for the MAC-IP link.	Null
Mac Address	Enter the defined host's Mac Address.	Null
IP Address	Enter the defined host's IP Address.	Null

3.29 CONFIGURATION -> DYNDNS

This section allows users to set the DynDNS parameters.



DynDNS Settings

☑ Enable DynDNS

Service Type: DynDNS-Dynamic

Hostname:

Username:

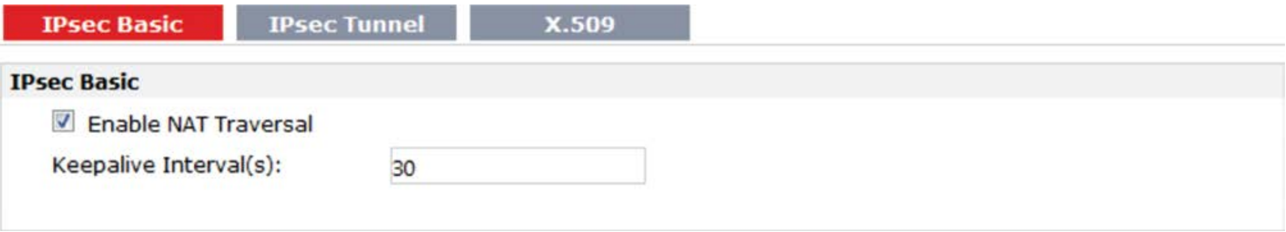
Password:

DynDNS Status: *The network is not yet ready, please wait a moment, and then try again!*

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" which you have established an account with. "Custom" could be used for linking custom DDNS server.	DynDNS–Dynamic
hoastmen	Enter the Host name the DDNS server provided.	Null
Username	Enter the user name the DDNS server provided.	Null
Password	Enter the password the DDNS server provided.	Null
URL	Enter the connection address of custom DDNS server.	Null
Force Update	Click to the update and use the DynDNS settings.	Null
DynDNS Status	Show current status of DynDNS	Null

3.30 CONFIGURATION -> IPSEC

This section allows users to set the IPSec parameters.

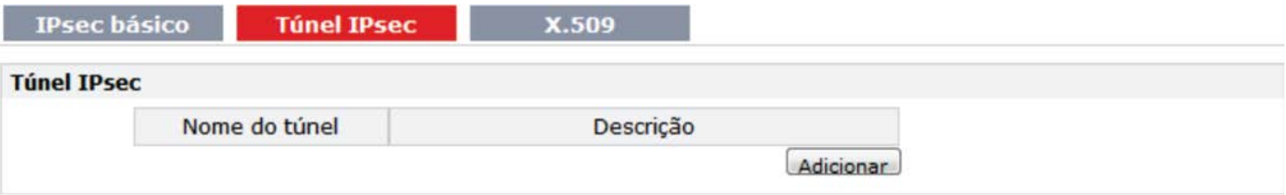


IPsec Basic

☑ Enable NAT Traversal

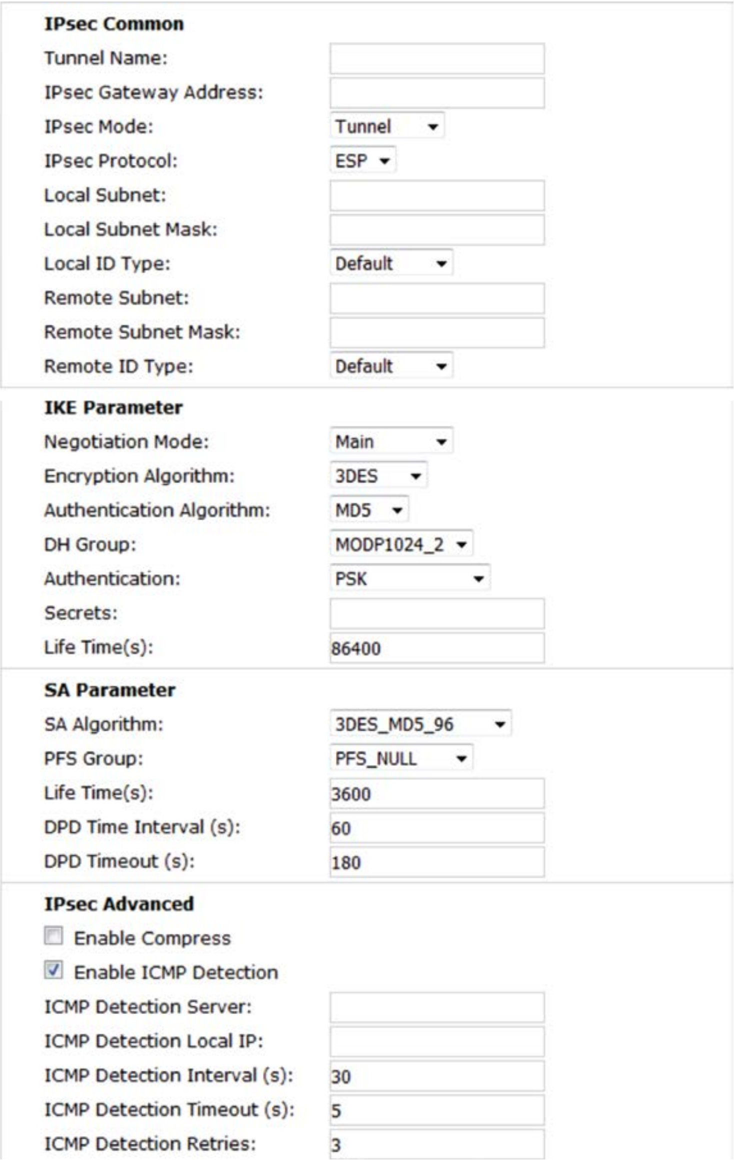
Keepalive Interval(s):	30

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



Túnel IPsec

Nome do túnel	Descrição



IPsec Common

Tunnel Name:	
IPsec Gateway Address:	
IPsec Mode:	Tunnel
IPsec Protocol:	ESP
Local Subnet:	
Local Subnet Mask:	
Local ID Type:	Default
Remote Subnet:	
Remote Subnet Mask:	
Remote ID Type:	Default

IKE Parameter

Negotiation Mode:	Main
Encryption Algorithm:	3DES
Authentication Algorithm:	MD5
DH Group:	MODP1024_2
Authentication:	PSK
Secrets:	
Life Time(s):	86400

SA Parameter

SA Algorithm:	3DES_MD5_96
PFS Group:	PFS_NULL
Life Time(s):	3600
DPD Time Interval (s):	60
DPD Timeout (s):	180

IPsec Advanced

☐ Enable Compress

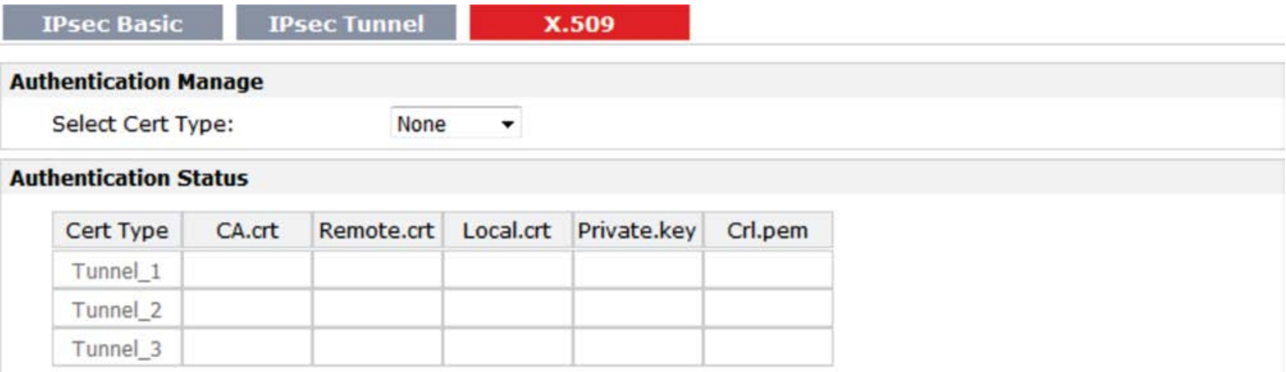
☑ Enable ICMP Detection

ICMP Detection Server:	
ICMP Detection Local IP:	
ICMP Detection Interval (s):	30
ICMP Detection Timeout (s):	5
ICMP Detection Retries:	3

IPSec Tunnel @ IPSec		
Item	Description	Default
Add	Click Add to add new IPSec Tunnel	Null
Enable	Enable IPSec Tunnel, the max tunnel account is 3	Null
IPSec Gateway Address	Enter the address of remote side IPSec VPN server.	Null
IPSec Mode	Select from “Tunnel” and “Transport”. Tunnel: Commonly used between gateways, or at an end-station to a gateway, the gateway acting as a proxy for the hosts behind it. Transport: Used between end-stations or between an end-station and a gateway, if the gateway is being treated as a host—for example, an encrypted Telnet session from a workstation to a router, in which the router is the actual destination.	Tunnel
IPSec Protocol	Select the security protocols from “ESP” and “AH”. ESP: Uses the ESP protocol. AH: Uses the AH protocol.	ESP
Local Subnet	Enter IPSec Local Protected subnet’s address.	0.0.0.0
Local Subnet Mask	Enter IPSec Local Protected subnet’s mask.	0.0.0.0
Local ID Type	Select from “IP Address”, “FQDN” and “User FQDN” for IKE negotiation. “Default” stands for “IP Address”. IP Address: Uses an IP address as the ID in IKE negotiation. FQDN: Uses an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security gateway, e.g., test.NOVUS.com. User FQDN: Uses a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with an sign “@” for the local security gateway, e.g., test@NOVUS.com.	Default
Remote Subnet	Enter IPSec Remote Protected subnet’s address.	0.0.0.0
Remote Subnet Mask	Enter IPSec Remote Protected subnet’s mask.	0.0.0.0
Remote ID Type	Select from “IP Address”, “FQDN” and “User FQDN” for IKE negotiation. IP Address: Uses an IP address as the ID in IKE negotiation. FQDN: Uses an FQDN type as the ID in IKE negotiation. If this option is selected, type a name without any at sign (@) for the local security gateway, e.g., test.NOVUS.com. User FQDN: Uses a user FQDN type as the ID in IKE negotiation. If this option is selected, type a name string with a sign “@” for the local security gateway, e.g., test@NOVUS.com.	Default
Negotiation Mode	Select from “Main” and “aggressive” for the IKE negotiation mode in phase 1. If the IP address of one end of an IPSec tunnel is obtained dynamically, the IKE negotiation mode must be aggressive. In this case, SAs can be established as long as the username and password are correct.	Main

Encryption Algorithm	Select from “DES”, “3DES”, “AES128”, “AES192” and “AES256”to be used in IKE negotiation. DES: Uses the DES algorithm in CBC mode and 56-bit key. 3DES: Uses the 3DES algorithm in CBC mode and 168-bit key. AES128: Uses the AES algorithm in CBC mode and 128-bit key. AES192: Uses the AES algorithm in CBC mode and 192-bit key. AES256: Uses the AES algorithm in CBC mode and 256-bit key.	3DES
Authentication Algorithm	Select from “MD5” and “SHA1”to be used in IKE negotiation. MD5: Uses HMAC-SHA1. SHA1: Uses HMAC-MD5.	MD5
DH Group	Select from “MODP768_1”, “MODP1024_2” and “MODP1536_5”to be used in key negotiation phase 1. MODP768_1: Uses the 768-bit Diffie-Hellman group. MODP1024_2: Uses the 1024-bit Diffie-Hellman group. MODP1536_5: Uses the 1536-bit Diffie-Hellman group.	MODP1024_2
Authentication	Select from “PSK”, “CA”, “XAUTH Init PSK” and “XAUTH Init CA” to be used in IKE negotiation. PSK: Pre-shared Key. CA: Certification Authority. XAUTH: Extended Authentication to AAA server.	PSK
Secrets	Enter the Pre-shared Key.	Null
Life Time @ IKE Parameter	Set the lifetime in IKE negotiation. Before an SA expires, IKE negotiates a new SA. As soon as the new SA is set up, it takes effect immediately and the old one will be cleared automatically when it expires.	86400
SA Algorithm	Select from “DES_MD5_96”, “DES_SHA1_96”, “3DES_MD5_96”, “3DES_ SHA1_96”, “AES128_MD5_96”, “AES128_ SHA1_96”, “AES192_MD5_96”, “AES192_ SHA1_96”, “AES256_MD5_96” and “AES256_ SHA1_96” when you select “ESP” in “Protocol”; Select from “AH_MD5_96” and “AH_ SHA1_96” when you select “AH” in “Protocol”; ***Note***: *Higher security means more complex implementation and lower speed. DES is enough to meet general requirements. Use 3DES when high confidentiality and security are required.*	3DES_MD5_96
PFS Group	Select from “PFS_NULL”, “MODP768_1”, “MODP1024_2” and “MODP1536_5”. PFS_NULL: Disable PFS Group MODP768_1: Uses the 768-bit Diffie-Hellman group. MODP1024_2: Uses the 1024-bit Diffie-Hellman group. MODP1536_5: Uses the 1536-bit Diffie-Hellman group.	PFS_NULL
Life Time @ SA Parameter	Set the IPSec SA lifetime. ***Note***: *When negotiating to set up IPSec SAs, IKE uses the smaller one between the lifetime set locally and the lifetime proposed by the peer.*	3600

DPD Time Interval	Set the interval after which DPD is triggered if no IPSec protected packets is received from the peer. DPD: Dead peer detection. DPD irregularly detects dead IKE peers. When the local end sends an IPSec packet, DPD checks the time the last IPSec packet was received from the peer. If the time exceeds the DPD interval, it sends a DPD hello to the peer. If the local end receives no DPD acknowledgment within the DPD packet retransmission interval, it retransmits the DPD hello. If the local end still receives no DPD acknowledgment after having made the maximum number of retransmission attempts, it considers the peer already dead, and clears the IKE SA and the IPSec SAs based on the IKE SA.	60
DPD Timeout	Set the timeout of DPD packets.	180
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



Authentication Manage

Select Cert Type: None

Authentication Status

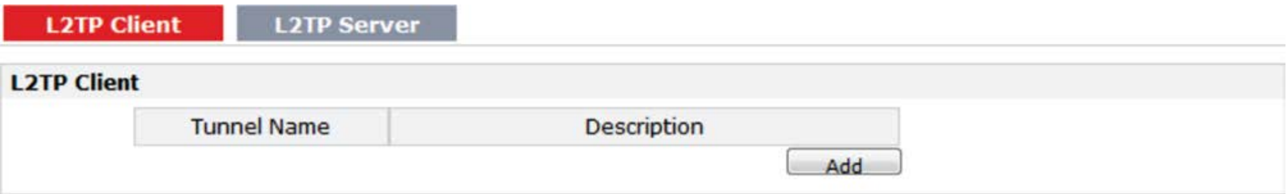
Cert Type	CA.crt	Remote.crt	Local.crt	Private.key	Crl.pem
Tunnel_1					
Tunnel_2					
Tunnel_3					

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. Click “Export” you can export the Local Public Key file from router to your PC.	Null
Local Private Key	Click “Browse” to select the correct Local Private Key file from your PC, and then click “Import” to import it to the router. Click “Export” you can export the Local Private Key file from router to your PC.	Null

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

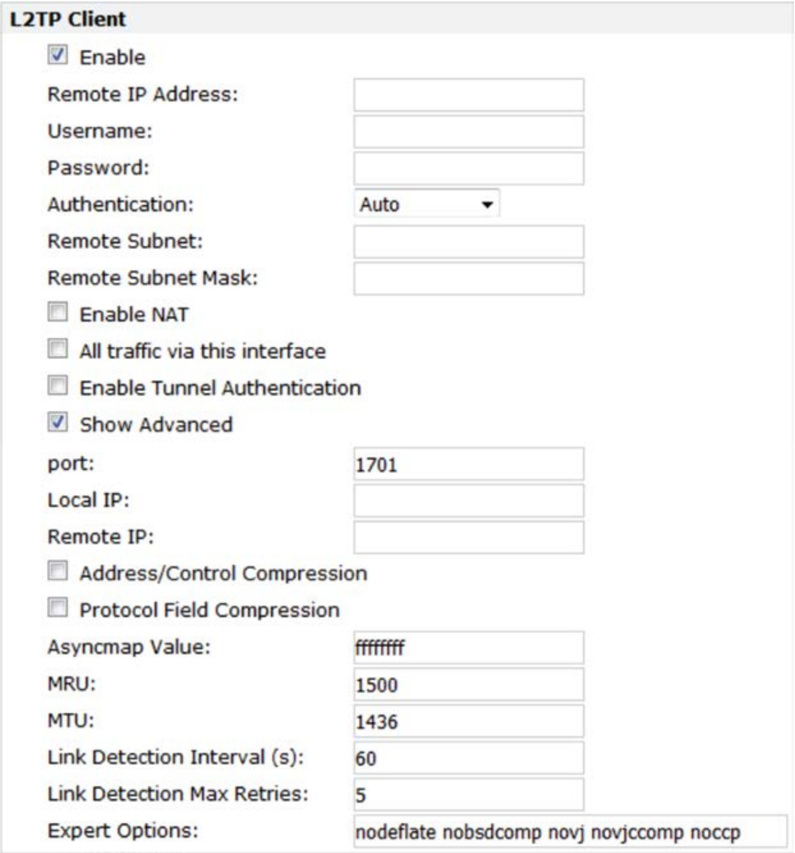
3.31 CONFIGURATION -> L2TP

This section allows users to set the L2TP parameters.



L2TP Client

Tunnel Name	Description


L2TP Client

☑ Enable

Remote IP Address:

Username:

Password:

Authentication: Auto

Remote Subnet:

Remote Subnet Mask:

□ Enable NAT

□ All traffic via this interface

□ Enable Tunnel Authentication

☑ Show Advanced

port: 1701

Local IP:

Remote IP:

□ Address/Control Compression

□ Protocol Field Compression

Asyncmap Value: ffffffff

MRU: 1500

MTU: 1436

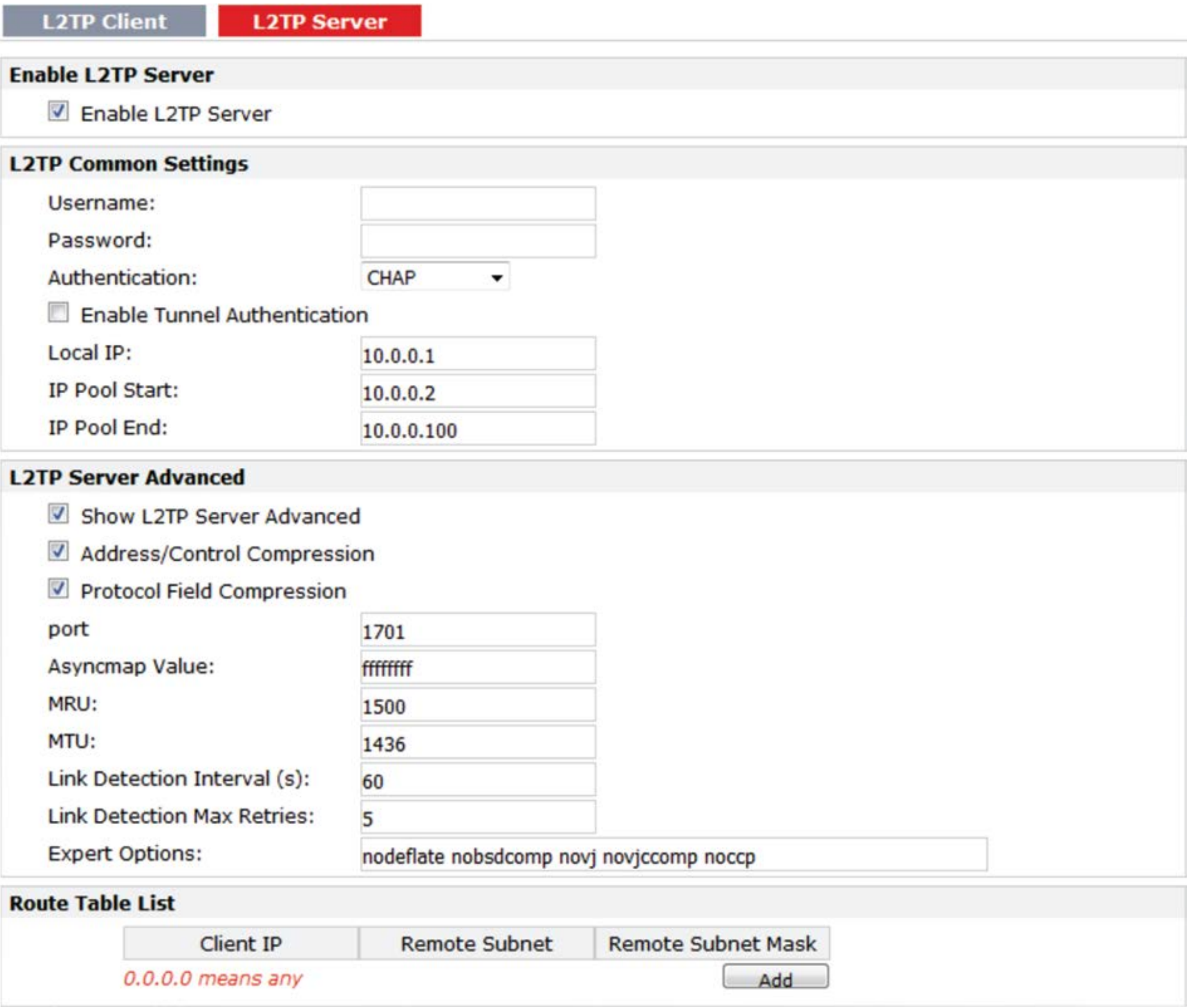
Link Detection Interval (s): 60

Link Detection Max Retries: 5

Expert Options: nodeflate nobsdcomp novj novjccomp noccp

L2TP Client @ L2TP		
Item	Description	Default
Add	Click “Add” to add a L2TP client. You can add at most 3 L2TP clients.	Null
Remote IP Address	Enter your L2TP server’s public IP or domain name.	Null
Username	Enter the username which was provided by your L2TP server.	Null
Password	Enter the password which was provided by your L2TP server.	Null
Authentication	Select from “Auto”, “PAP”, “CHAP”, “MS-CHAP v1” and “MS-CHAP v2”. You need to select the corresponding authentication method based on the server’s authentication method. When you select “Auto”, router will auto select the correct method based on server.	Disable
Remote Subnet	Enter L2TP remote Protected subnet’s address.	Null
Remote Subnet Mask	Enter L2TPremote Protected subnet’s mask.	Null

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



Enable L2TP Server

☑ Enable L2TP Server

L2TP Common Settings

Username:	
Password:	
Authentication:	CHAP
☐ Enable Tunnel Authentication	
Local IP:	10.0.0.1
IP Pool Start:	10.0.0.2
IP Pool End:	10.0.0.100

L2TP Server Advanced

☑ Show L2TP Server Advanced

☑ Address/Control Compression

☑ Protocol Field Compression

port	1701
Asyncmap Value:	ffffffff
MRU:	1500
MTU:	1436
Link Detection Interval (s):	60
Link Detection Max Retries:	5
Expert Options:	nodeflate nobsdcomp novj novjccomp noccp

Route Table List

Client IP	Remote Subnet	Remote Subnet Mask

0.0.0.0 means any

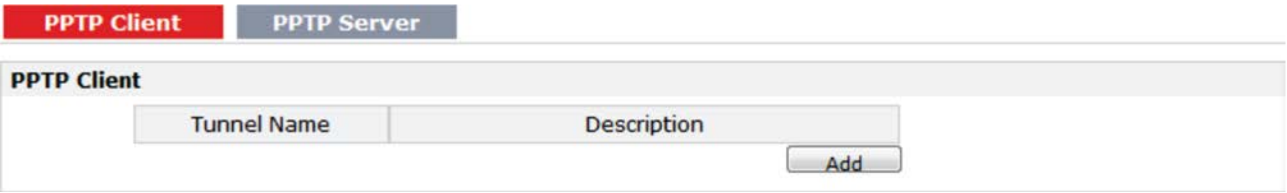
Add

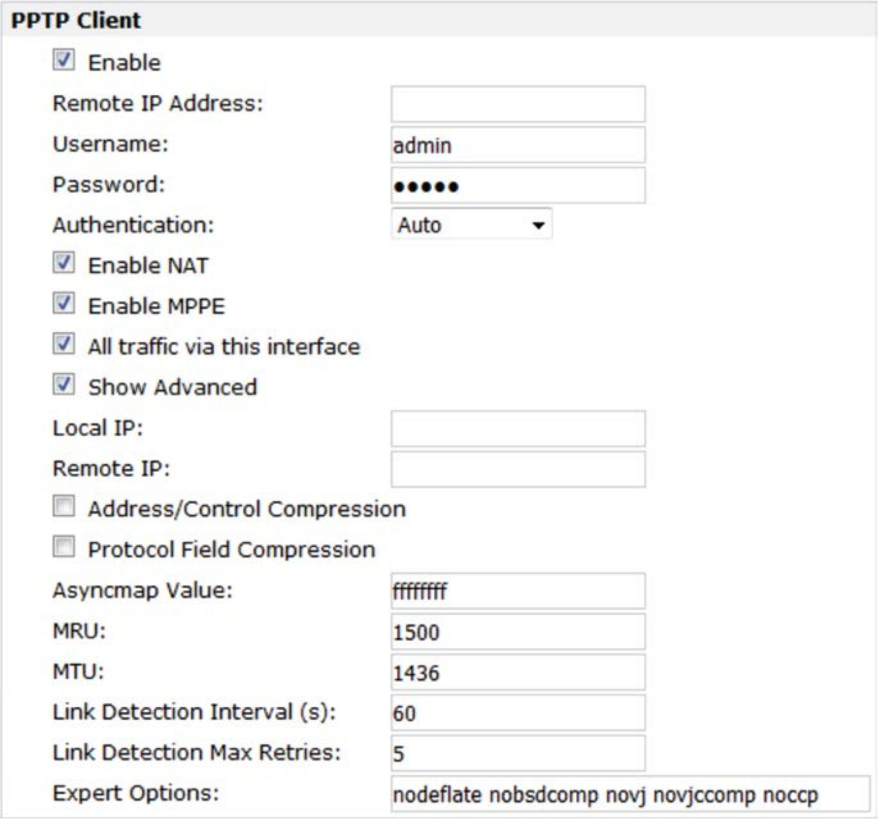
L2TP Server @ L2TP		
Item	Description	Default
Enable L2TP Server	Tick to enable L2TP server.	Disable
Username	Set the username which will assign to L2TP client.	Null
Password	Set the password which will assign to L2TP client.	Null
Authentication	Select from “PAP”, “CHAP”, “MS-CHAP v1” and “MS-CHAP v2”. L2TP client need to select the same authentication method based on this server’s authentication method.	CHAP
Enable Tunnel Authentication	Tick to enable tunnel authentication and enter the tunnel secret which will provide to L2TP client.	Disable
Local IP	Set the IP address of L2TP server.	10.0.0.1
IP Pool Start	Set the IP pool start IP address which will assign to the L2TP clients.	10.0.0.2
IP Pool End	Set the IP pool end IP address which will assign to the L2TP clients.	10.0.0.100
Show L2TP Server Advanced	Tick to show the L2TP server advanced setting.	Disable
Address/Control Compression	Used for PPP initialization. In general, you need to enable it as default.	Enable
Protocol Field Compression	Used for PPP initialization. In general, you need to enable it as default.	Enable
Port	Set the Port number of the L2TP server.	Null
Asyncmap Value	One of the L2TP initialization strings. In general, you don’t need to modify this value.	ffffffff

MRU	Maximum Receiving Unit. It is the identifier of the maximum size of packet, which is possible to receive in a given environment.	1500
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1436
Link Detection Interval	Specify the interval between L2TP client and server. To check the connectivity of a tunnel, the client and server regularly send PPP Echo to each other. If the client or server receives no response from the peer within a specified period of time, it retransmits the PPP echo. If it receives no response from the peer after transmitting the PPP echo for max retries times, it considers that the L2TP tunnel is down and tries tore-establish a tunnel with the peer.	30
Link Detection Max Retries	Specify the max retries times for L2TP link detection.	5
Expert Options	You can enter some other PPP initialization strings in this field. Each string can be separated by a space.	noccp nobsdcomp
Route Table List	Click “Add” to add a route rule from L2TP server to L2TP client.	Null

3.32 CONFIGURATION -> PPTP

This section allows users to set the PPTP parameters.




PPTP Client

☑ Enable

Remote IP Address:

Username: admin

Password: ●●●●●

Authentication: Auto

☑ Enable NAT

☑ Enable MPPE

☑ All traffic via this interface

☑ Show Advanced

Local IP:

Remote IP:

☐ Address/Control Compression

☐ Protocol Field Compression

Asyncmap Value: ffffffff

MRU: 1500

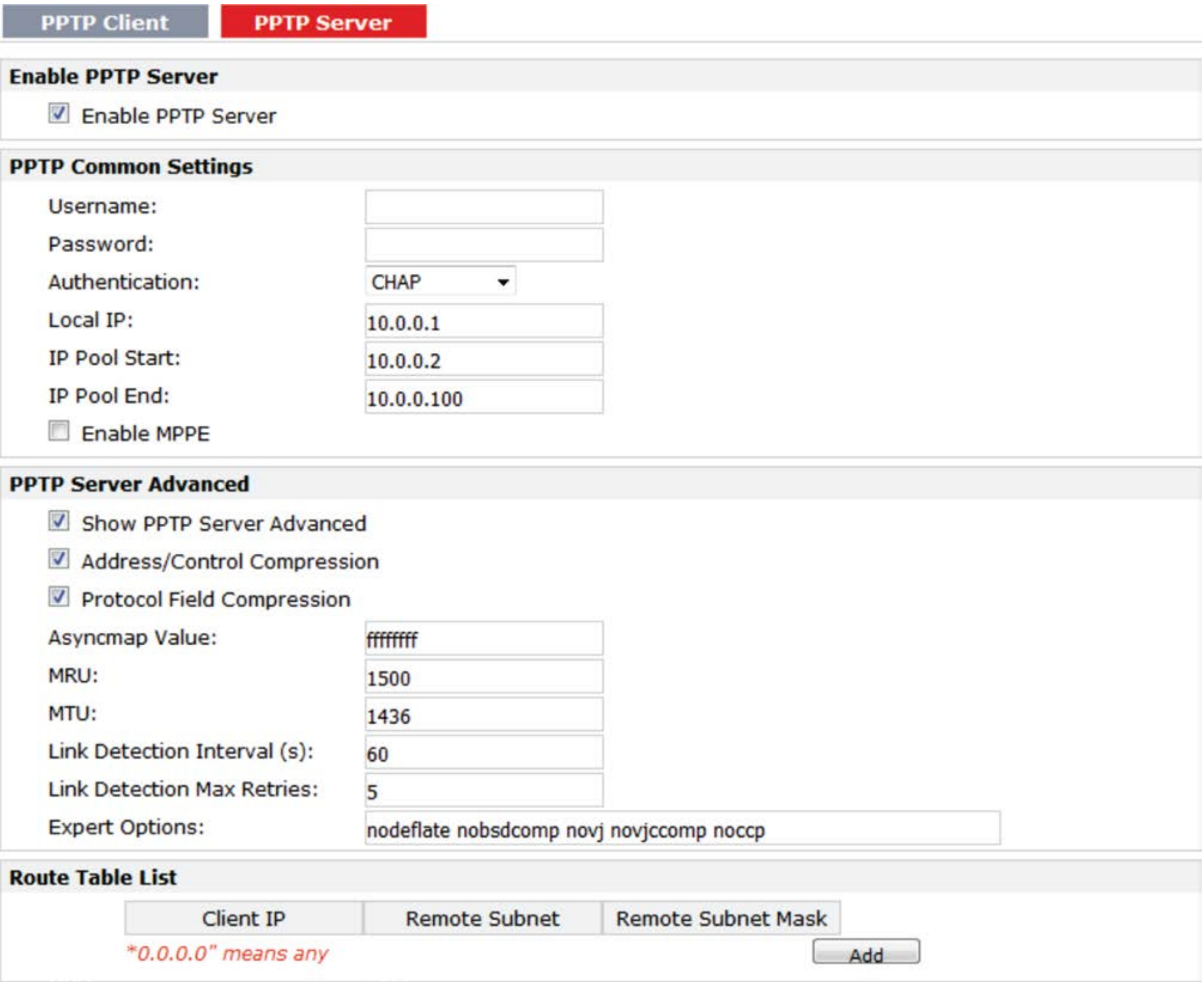
MTU: 1436

Link Detection Interval (s): 60

Link Detection Max Retries: 5

Expert Options: nodeflate nobsdcomp novj novjccomp noccp

PPTP Client @ PPTP		
Item	Description	Default
Add	Click “Add” to add a PPTP client	
Enable	Enable PPTP Client. The max tunnel accounts are 3.	Null
Disable	Disable PPTP Client.	Null
Remote IP Address	Enter your PPTP server’s public IP or domain name.	Null
Username	Enter the username which was provided by your PPTP server.	Null
Password	Enter the password which was provided by your PPTP server.	Null
Authentication	Select from “Auto”, “PAP”, “CHAP”, “MS-CHAP v1” and “MS-CHAP v2”. You need to select the corresponding authentication method based on the server’s authentication method. When you select “Auto”, router will auto select the correct method based on server’s method.	Auto
Enable NAT	Click to enable NAT feature of PPTP. The source IP address of host Behind AIRGATE-3G will be disguised before accessing the remote PPTP server.	Disable
Enable MPPE	Tick to enable MPPE (Microsoft Point-to-Point Encryption). It’s a protocol for encrypting data across PPP and VPN links.	Disable
All traffic via this interface	After click to enable this feature, all data traffic will be sent via PPTP tunnel.	Disable
Show Advanced	Tick to enable the PPTP client advanced setting.	Disable
Local IP	Set the IP address of the PPTP client. You can enter the IP which assigned by PPTP server. Null means PPTP client will obtain an IP address automatically from PPTP server’s IP pool.	Null
Remote IP	Enter the remote peer’s private IP address or remote subnet’s gateways address.	Null
Address/Control Compression	Used for PPP initialization. In general, you need to enable it as default.	Enable
Protocol Field Compression	Used for PPP initialization. In general, you need to enable it as default.	Enable
Asyncmap Value	One of the PPTP initialization strings. In general, you don’t need to modify this value.	ffffffff
MRU	Maximum Receiving Unit. It is the identifier of the maximum size of packet, which is possible to receive in a given environment.	1500
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1436
Link Detection Interval	Specify the interval between PPTP client and server. To check the connectivity of a tunnel, the client and server regularly send PPP Echo to each other. If the client or server receives no response from the peer within a specified period of time, it retransmits the PPP echo. If it receives no response from the peer after transmitting the PPP echo for max retries times, it considers that the PPTP tunnel is down and tries tore-establish a tunnel with the peer.	30
Link Detection Max Retries	Specify the max retries times for PPTP link detection.	5
Expert Options	You can enter some other PPP initialization strings in this field. Each string can be separated by a space.	noccp nobsdcomp



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):	60
Link Detection Max Retries:	5
Expert Options:	nodeflate nobsdcomp novj novjccomp noccp

Route Table List

Client IP	Remote Subnet	Remote Subnet Mask

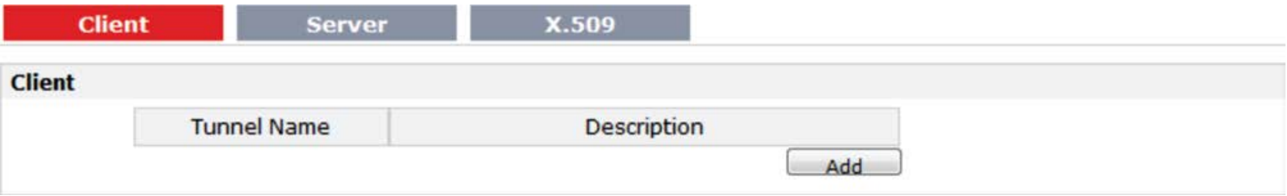
*0.0.0.0" means any

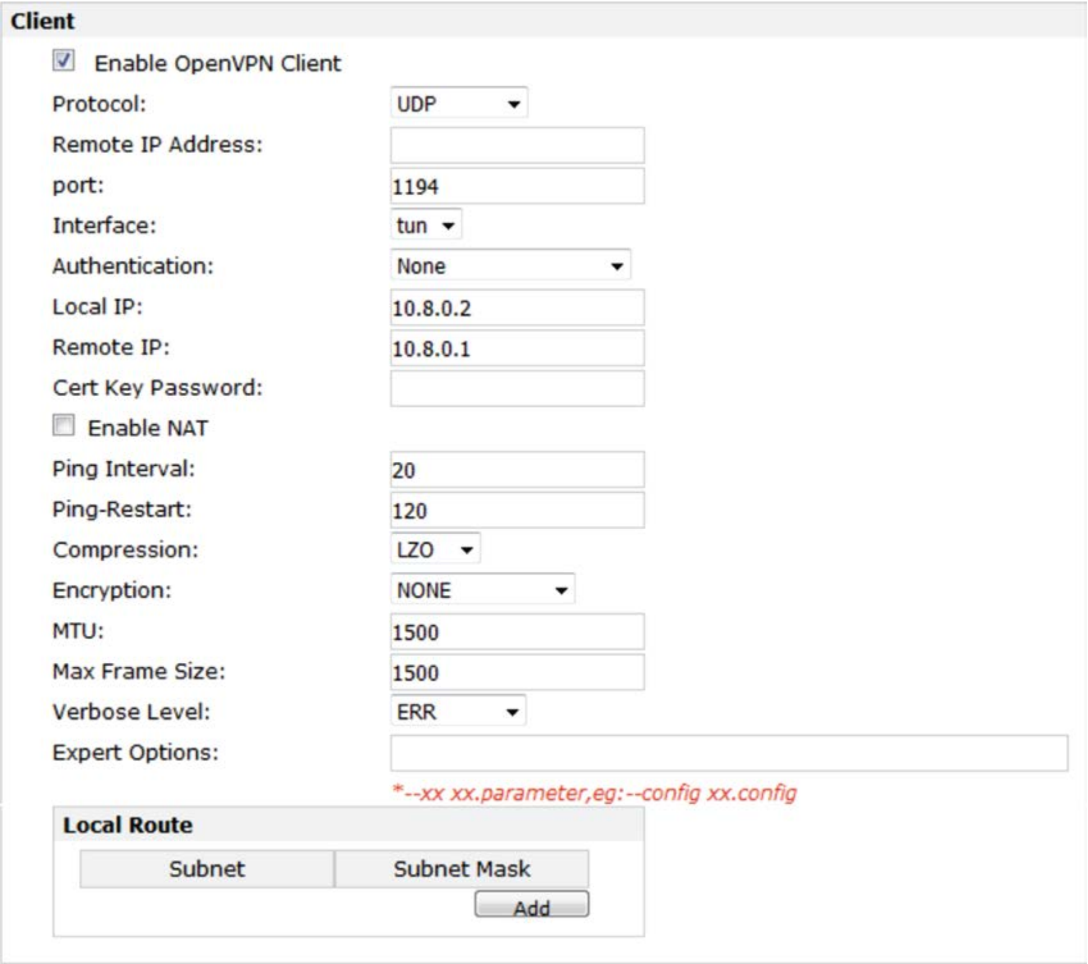
PPTP Server @ PPTP		
Item	Description	Default
Enable PPTP Server	Tick to enable PPTP server.	Disable
Username	Set the username which will assign to PPTP client.	Null
Password	Set the password which will assign to PPTP client.	Null
Authentication	Select from “PAP”, “CHAP”, “MS-CHAP v1” and “MS-CHAP v2”.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

MRU	Maximum Receiving Unit. It is the identifier of the maximum size of packet, which is possible to receive in a given environment.	1500
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1436
Link Detection Interval	Specify the interval between PPTP client and server. To check the connectivity of a tunnel, the client and server regularly send PPP Echo to each other. If the client or server receives no response from the peer within a specified period of time, it retransmits the PPP echo. If it receives no response from the peer after transmitting the PPP echo for max retries times, it considers that the PPTP tunnel is down and tries tore-establish a tunnel with the peer.	30
Link Detection Max Retries	Specify the max retries times for PPTP link detection.	5
Expert Options	You can enter some other PPP initialization strings in this field. Each string can be separated by a space.	noccp nobsdcomp
Route Table List	Click “Add” to add a route rule from PPTP server to PPTP client.	Null

3.33 CONFIGURATION -> OPENVPN

This section allows users to set the Open VPN parameters.





☑ Enable OpenVPN Client

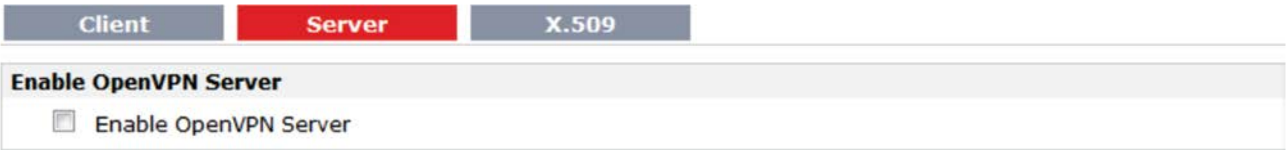
Protocol:	UDP
Remote IP Address:	
port:	1194
Interface:	tun
Authentication:	None
Local IP:	10.8.0.2
Remote IP:	10.8.0.1
Cert Key Password:	

□ Enable NAT

Ping Interval:	20
Ping-Restart:	120
Compression:	LZO
Encryption:	NONE
MTU:	1500
Max Frame Size:	1500
Verbose Level:	ERR
Expert Options:	

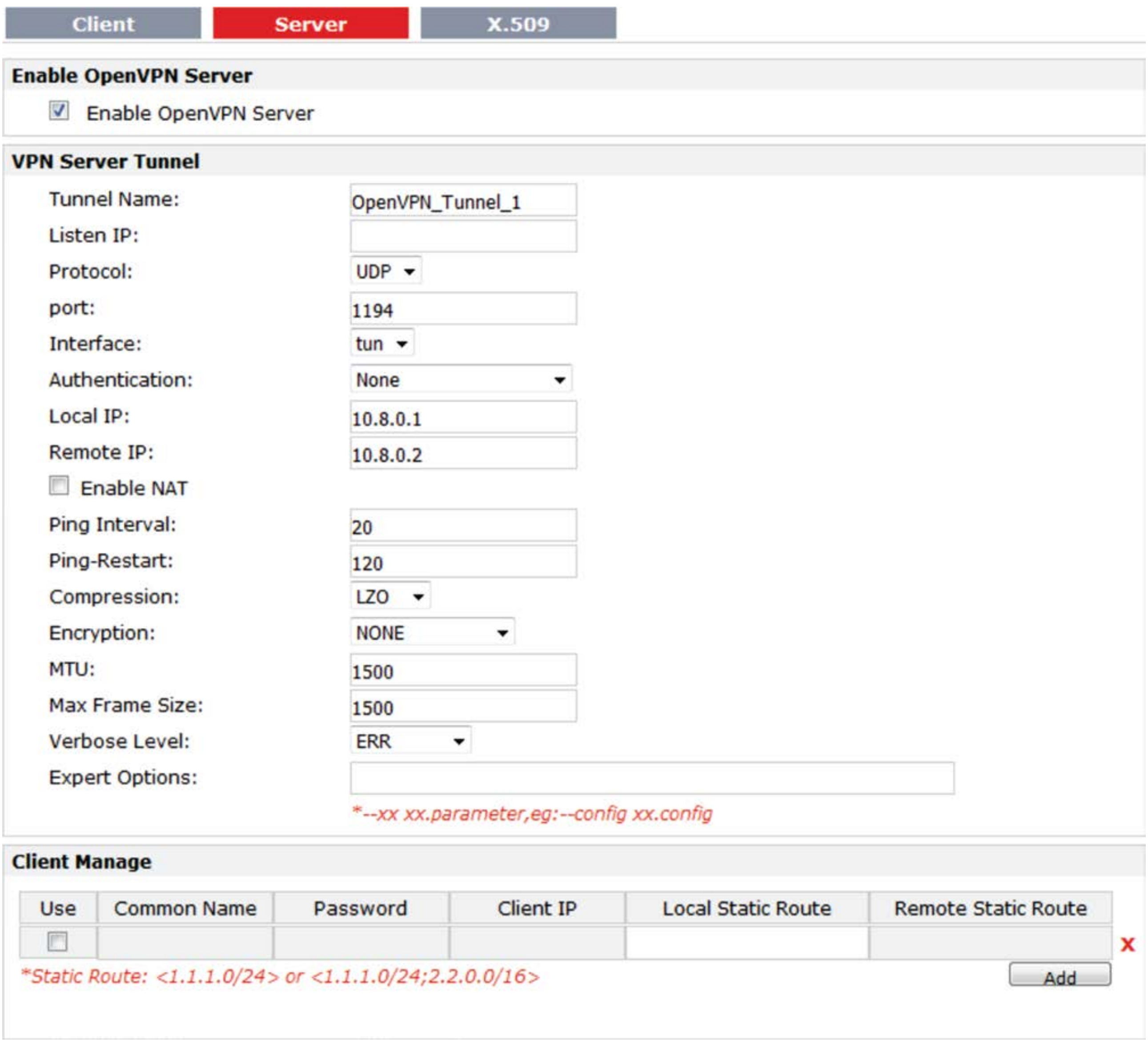
*--xx xx.parameter,eg:--config xx.config

Client @ Open VPN		
Item	Description	Default
Enable	Enable OpenVPN Client, the max tunnel account is 3	Null
Protocol	Select from “UDP” and “TCP Client” which depends on the application.	UDP
Remote IP Address	Enter the remote IP address or domain name of remote side OpenVPN server.	Null
Port	Enter the listening port of remote side OpenVPN server.	1194
Interface	Select from “tun” and “tap” which are two different kinds of device interface for OpenVPN. The difference between tun and tap device is this: a tun device is a virtual IP point-to-point device and a tap device is a virtual Ethernet device.	tun
Authentication	Select from four different kinds of authentication ways: “Pre-shared”, “Username/Password”, “X.509 cert” and “X.509 cert+user”.	None
Local IP	Define the local IP address of OpenVPN tunnel.	10.8.0.2
Remote IP	Define the remote IP address of OpenVPN tunnel.	10.8.0.1
Enable NAT	Tick to enable SNAT for OpenVPN. The source IP address of host Behind AIRGATE-3G will be disguised before accessing the remote OpenVPN server.	Disable
Ping Interval	Set ping interval to check if the tunnel is active.	20
Ping -Restart	Restart to establish the OpenVPN tunnel if ping always timeout during this time.	120
Compression	Select “LZO” to use the LZO compression library to compress the data stream.	LZO
Encryption	Select from “NONE”, “BF-CBC”, “DES-CBC”, “DES-EDE3-CBC”, “AES-128-CBC”, “AES-192-CBC” and “AES-256-CBC”. BF-CBC: Uses the BF algorithm in CBC mode and 128-bit key. DES-CBC: Uses the DES algorithm in CBC mode and 64-bit key. DES-EDE3-CBC: Uses the 3DES algorithm in CBC mode and 192-bit key. AES128-CBC: Uses the AES algorithm in CBC mode and 128-bit key. AES192-CBC: Uses the AES algorithm in CBC mode and 192-bit key. AES256-CBC: Uses the AES algorithm in CBC mode and 256-bit key.	NONE
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1500
Max Frame Size	Set the Max Frame Size for transmission.	1500
Verbose Level	Select the log output level which from low to high: “ERR”, “WARNING”, “NOTICE” and “DEBUG”. The higher level will output more log information.	ERR
Expert Options	You can enter some other PPP initialization strings in this field. Each string can be separated by a space.	Null
Subnet&Subnet Mask@Local Route	Set the subnet and subnet Mask of local route.	Null



Enable OpenVPN Server

□ Enable OpenVPN Server



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: LZO

Encryption: NONE

MTU: 1500

Max Frame Size: 1500

Verbose Level: ERR

Expert Options:

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

Client Manage

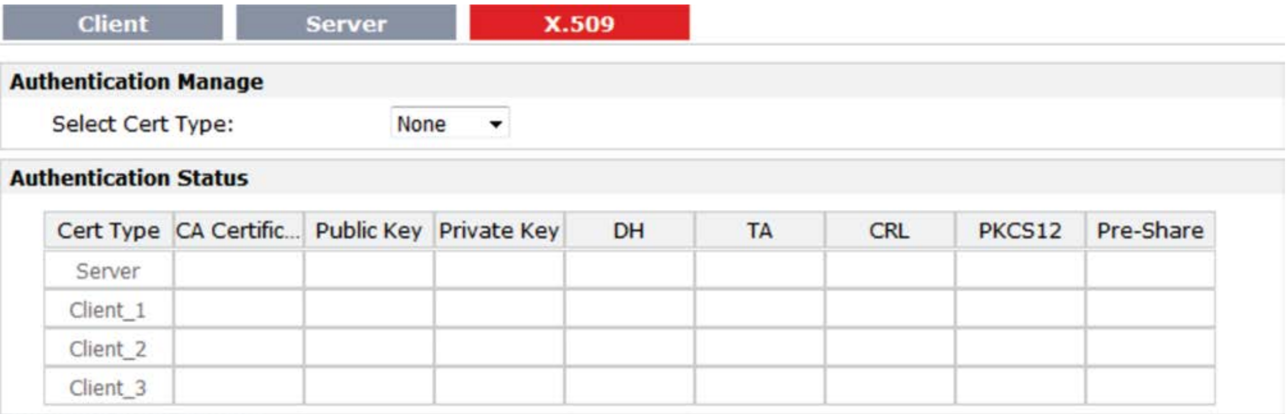
Use	Common Name	Password	Client IP	Local Static Route	Remote Static Route
□					

*Static Route: <1.1.1.0/24> or <1.1.1.0/24;2.2.0.0/16>

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_1
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 SNAT for OpenVPN. The source IP address of host Behind AIRGATE-3G will be disguised before accessing the remote OpenVPN client.	Disable

Ping Interval	Set ping interval to check if the tunnel is active.	20
Ping -Restart	Restart to establish the OpenVPN tunnel if ping always timeout during this time.	120
Compression	Select from “None”and”LZO”, Select “LZO” to use the LZO compression library to compress the data stream.	LZO
Encryption	Select from “NONE”, “BF-CBC”, “DES-CBC”, “DES-EDE3-CBC”, “AES128-CBC”, “AES192-CBC” and “AES256-CBC”. BF-CBC: Uses the BF algorithm in CBC mode and 128-bit key. DES-CBC: Uses the DES algorithm in CBC mode and 64-bit key. DES-EDE3-CBC: Uses the 3DES algorithm in CBC mode and 192-bit key. AES128-CBC: Uses the AES algorithm in CBC mode and 128-bit key. AES192-CBC: Uses the AES algorithm in CBC mode and 192-bit key. AES256-CBC: Uses the AES algorithm in CBC mode and 256-bit key.	NONE
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1500
Max Frame Size	Set the Max Frame Size for transmission.	1500
Verbose Level	Select the log output level which from low to high: “ERR”, “WARNING”, “NOTICE” and “DEBUG”. The higher level will output more log information.	ERR
Expert Options	You can enter some other PPP initialization strings in this field. Each string can be separated by a space.	Null
Enable HMAC Firewall @ VPN Server Advanced	In order to prevent malicious attacks, such as DOS, UDP port flooding, we ge nerate a "HMAC is firewall"	Disable
Enable Crl @ VPN Server Advanced	Generate a certificate revoked chain file, to prevent someone lost certific ate in the future, users access VPN by illegal. You could find the certificate tab of AIRGATE-3G, there is one option for Crl.	Disable
Enable Client to Client @ VPN Server Advanced	Uncomment this directive to allow different clients to be able to "see" each other. By default, clients will only see the server. To force clients to only see the server, you will also need to appropriately firewall the server's TUN/TAP interface.	Disable
Enable Dup Client @ VPN Server Advanced	While establish OpenVPN with keys, must open this option, otherwise only allows one VPN connection with the same certificate.	Disable
Enable IP Persist @ VPN Server Advanced	Maintain a record of client <-> virtual IP address associations in this file. If OpenVPN goes down or is restarted, reconnecting clients can be assigned the same virtual IP address from the pool that was previously assigned.	Enable
Enable IP pool @ VPN Server Advanced	Define the range of virtual IP address.	Disable
IP Pool Start	Define start virtual IP address	10.8.0.5
IP Pool End	Define end virtual IP address	10.8.0.254
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

Note: “VPN Server Advanced” will show up when you select “Authentication” type as “Username/Password”, “X.509 cert” and “X.509 cert+user”.



Authentication Manage

Select Cert Type: None

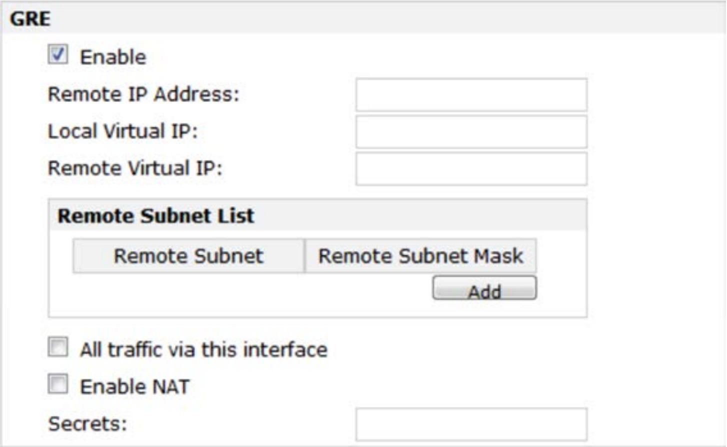
Authentication Status

Cert Type	CA Certific...	Public Key	Private Key	DH	TA	CRL	PKCS12	Pre-Share
Server								
Client_1								
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
PKCS12	Click “Browse” to select the correct PKCS12file from your PC, and then click “Import” to import it to the router. Click “Export” you can export the PKCS12file from router to your PC.	Null
Pre-Share	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

3.34 CONFIGURATION -> GRE

This section allows users to set the GRE parameters.



GRE

☑ Enable

Remote IP Address:

Local Virtual IP:

Remote Virtual IP:

Remote Subnet List

Remote Subnet	Remote Subnet Mask

□ All traffic via this interface

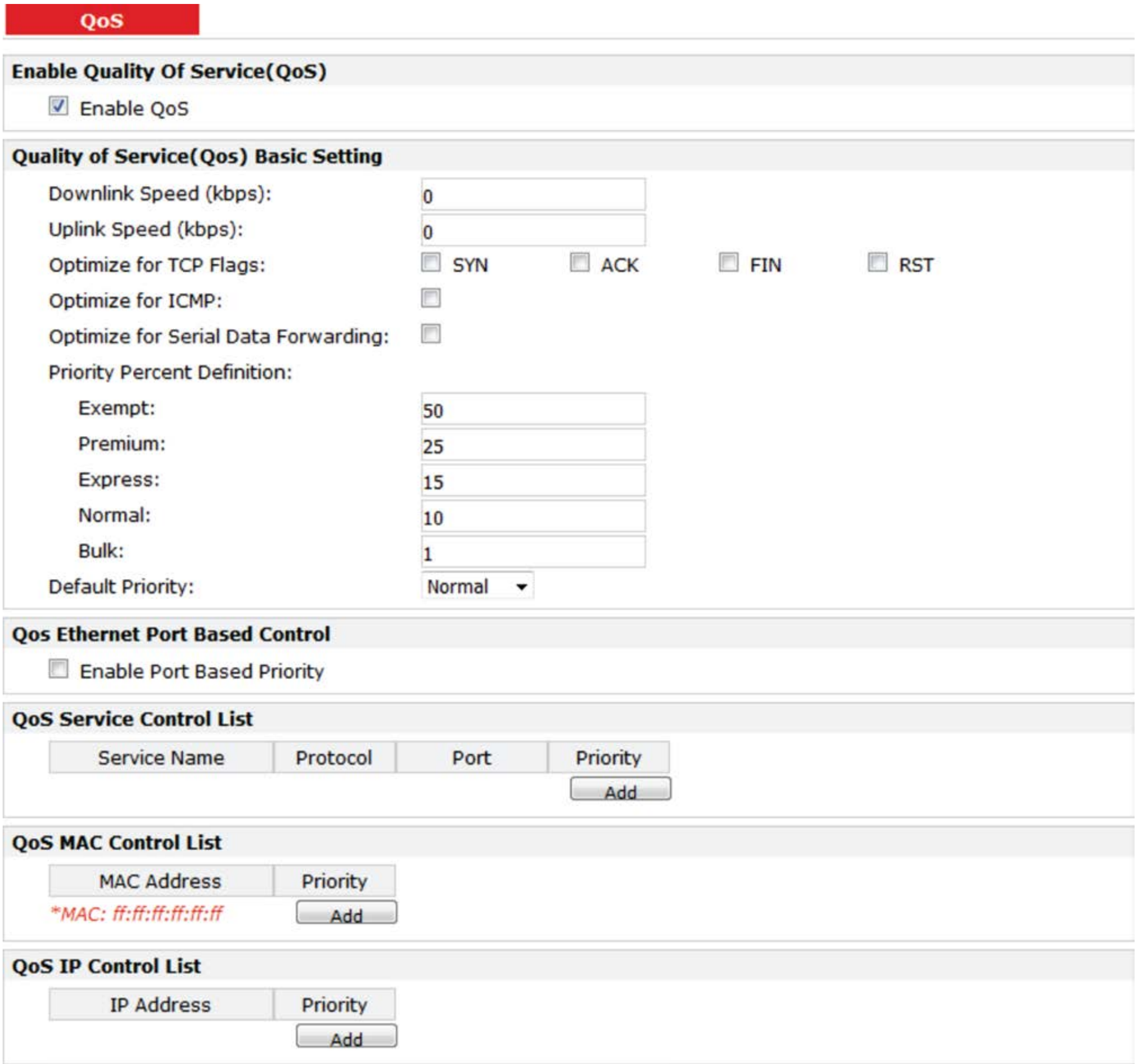
□ Enable NAT

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 @ Remote Subnet List	Add a static route to the remote side’s subnet so that the remote network is known to the local network. The max count is 10.	Null
Remote Subnet Mask @ Remote Subnet List	Set remote subnet net mask. The max count is 10.	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 SNAT for GRE. The source IP address of host Behind AIRGATE-3G will be disguised before accessing the remote GRE server.	Disable
Secrets	Set Tunnel Key of GRE.	Null

3.35 CONFIGURATION -> QOS

This section allows users to set the QoS parameters.



QoS

Enable Quality Of Service(QoS)

☑ Enable QoS

Quality of Service(Qos) Basic Setting

Downlink Speed (kbps): 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 Ethernet 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

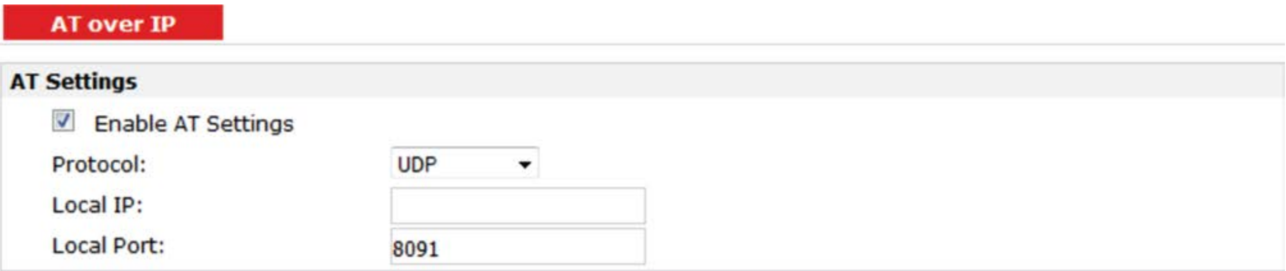
Optimize for ICMP	Enable to optimize for ICMP, which means ICMP will get the highest priority to occupy bandwidth. After enabled respond interval of PING control will be shorter. ***Note****: if user click to enable "Optimize for TCP Flags", "Optimize for Serial Data Forwarding", and "Optimize for ICMP" at the same time (these three services are in the same priority level), router will automatically start Stochastic Fairness Queueing (SFQ) strategy to make a fair bandwidth allocation, in case of one service occupy all the bandwidth.*	Disable
Optimize for Serial Data Forwarding	Enable to optimize for serial data forwarding, which means serial data forwarding will get the highest priority to occupy bandwidth. When enable serial data forwarding it need to enable local port number for controlling. Therefore, it needs to set local port number of router even if router is as TCP Client.	Disable
Priority Percent Definition	Define priority percent of "Exempt", "Premium", "Express", "Normal" and "Bulk". "Exempt" is defaulted as 50; "Premium" is defaulted as 25; "Express" is defaulted as 15; "Normal" is defaulted as 10; "Bulk" is 1.	
Default Priority	Select from "Exempt", "Premium", "Express", "Normal" and "Bulk". Users (Services) with no other pre-priority set will use this default priority. Exempt: this is the highest priority which guarantees that the minimum global rate of router is 50% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed". Premium: guarantees that the minimum global rate of router is 25% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed". Express: guarantees that the minimum global rate of router is 15% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed". Normal: guarantees that the minimum global rate of router is 10% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed". Bulk: guarantees that the minimum global rate of router is 1% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed".	Normal
Enable Port Based Priority @ Qos Port Base Control	Click to enable Ethernet port base priority control.	Disable
Eth0 Priority @ Qos Port Base Control	Define Qos of Eth0 interface. Different slave device that connect to AIRGATE-3G's Eth0 interface will be assigned specific Qos.	Exempt
Eth1 Priority @ Qos Port Base Control	Define Qos of Eth1 interface. Different slave device that connect to AIRGATE-3G's Eth1 interface will be assigned specific Qos.	Exempt
MAC Address @ QoS MAC Control List	Enter MAC address of the user (for example, PC) who you want to set it with QoS Control. Router supports up to 20 users set with QoS MAC Control. Priority of QoS MAC Control is higher than that of QoS IP control.	Null

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

Priority @ QoS Service Control List	Select from "Exempt", "Premium", "Express", "Normal" and "Bulk". Select the priority of the service that you want to set it with QoS Control. Exempt: this is the highest priority which guarantees that the minimum global rate of router is 50% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed". Premium: guarantees that the minimum global rate of router is 25% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed". Express: guarantees that the minimum global rate of router is 15% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed". Normal: guarantees that the minimum global rate of router is 10% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed". Bulk: guarantees that the minimum global rate of router is 1% of "Downlink Speed", and the maximum rate can reach to 100% of "Downlink Speed".	Exempt
***Note**: If services are in the same priority level, router will automatically start Stochastic Fairness Queueing (SFQ) strategy to make a fair bandwidth allocation.*		

3.36 CONFIGURATION -> AT OVER IP

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



AT Settings

☑ Enable AT Settings

Protocol: UDP

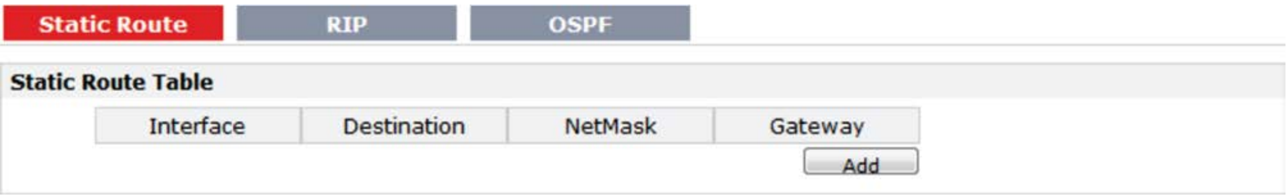
Local IP:

Local Port: 8091

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

3.37 CONFIGURATION -> IP ROUTING

This section allows users to set the IP routing parameters. You must click on Add button to add a static route.

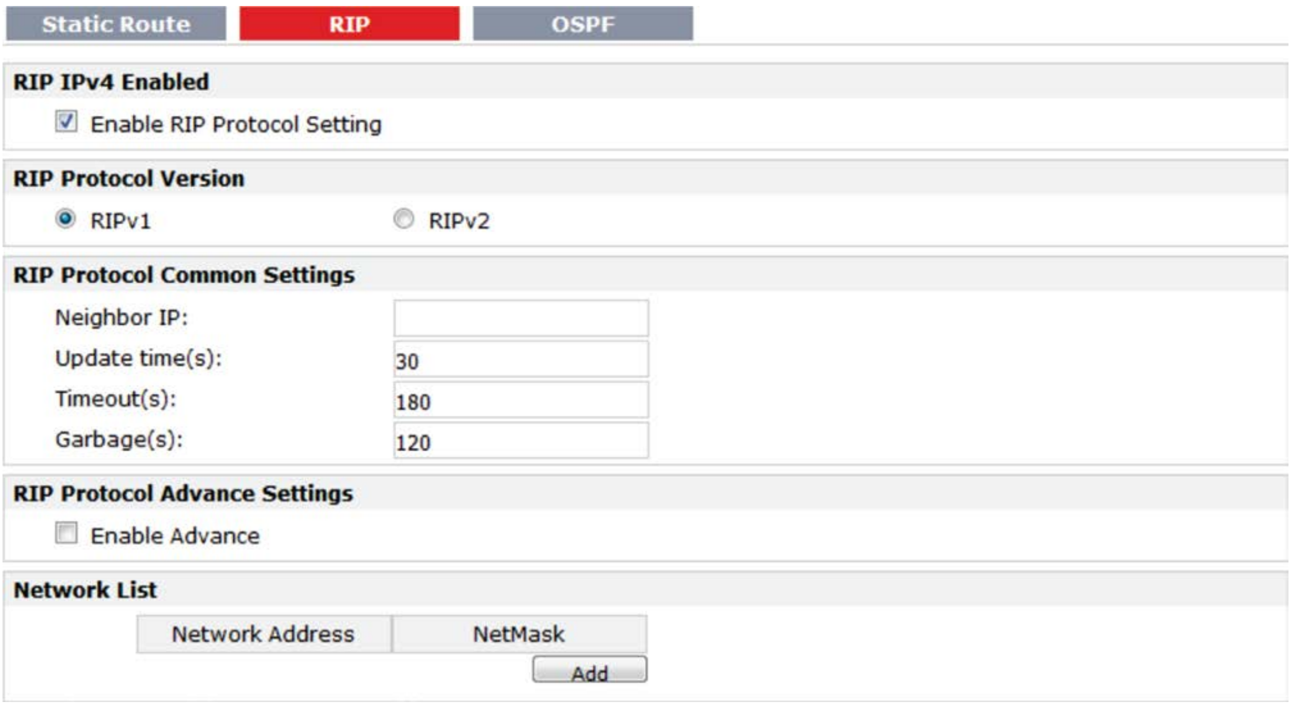


Static Route Table

Interface	Destination	NetMask	Gateway

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

By enabling RIP IPv4, you can define their configuration parameters.



RIP IPv4 Enabled

☑ Enable RIP Protocol Setting

RIP Protocol Version

● RIPv1 ○ RIPv2

RIP Protocol Common Settings

Neighbor IP:

Update time(s): 30

Timeout(s): 180

Garbage(s): 120

RIP Protocol Advance Settings

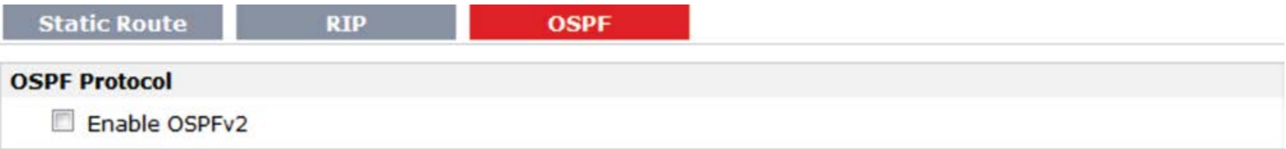
□ Enable Advance

Network List

Network Address	NetMask

RIP @ IP Routing		
Item	Description	Default
RIP	RIP (Routing Information Protocol) is a distance-vector routing protocol, which employs the hop count as a routing metric. RIP prevents routing loops by implementing a limit on the number of hops allowed in a path from the source to a destination.	Null
Enable RIP Protocol Setting	Tick to enable RIP function.	Disable
RIP Protocol Version	Select from “RIPv1” and “RIPv2”.	RIPv1
Neighbor IP	If you input this neighbor IP, router will only send RIP request massage to this IP instead of broadcast. This item only needs to be set in some unicast network.	0.0.0.0
Update times	Defines the interval between routing updates.	30
Timeout	Defines the route aging time. If no update for a route is received after the aging time elapses, the metric of the route is set to 16 in the routing table.	180
Garbage	Defines the interval from when the metric of a route becomes 16 to when it is deleted from the routing table. During the Garbage-Collect timer length, RIP advertises the route with the routing metric set to 16. If no update is announced for that route after the Garbage-Collect timer expires, the route will be deleted from the routing table.	120
Enable Advance	Tick to enable RIP protocol Advance Setting.	Disable
Default Metric	This value is used for redistributed routes.	1
Distance	The first criterion that a router uses to determine which routing protocol to use if two protocols provide route information for the same destination.	120
Passive	Select from “None”, “Eth0”, “Eth1” and “Default”. This command sets the specified interface to passive mode. On passive mode interface, all receiving packets are processed as normal and Rip info does not send either multicast or unicast RIP packets except to RIP neighbors specified with neighbor command. The default is to be passive on all interfaces.	None
Enable Default Origination	Enable to make router send the default route to the other routers which in the same IGP AS.	Disable
Enable Redistribute Connect	Redistribute connected routes into the RIP tables.	Disable

Enable Redistribute Static	Redistributes routing information from static route entries into the RIP tables.	Disable
Enable Redistribute OSPF	Redistributes routing information from OSPF route entries into the RIP tables.	Disable
Network List	Router will only report the RIP information in this list to its neighbor.	Null
Network Address	Enter the Network address which Eth0 or Eth 1 connects directly.	Null
Netmask	Enter the Network's Netmask which Eth0 or Eth 1 connects directly.	Null



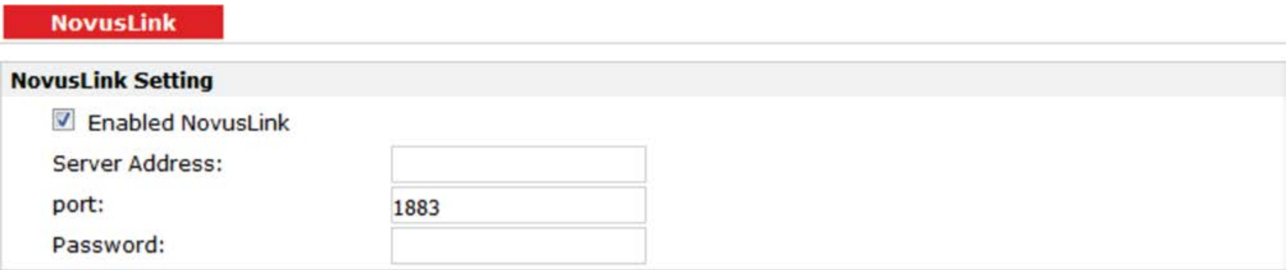
OSPF Protocol

☐ 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

3.38 CONFIGURATION -> NOVUSLINK

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



NovusLink Setting

☑ Enabled NovusLink

Server Address:

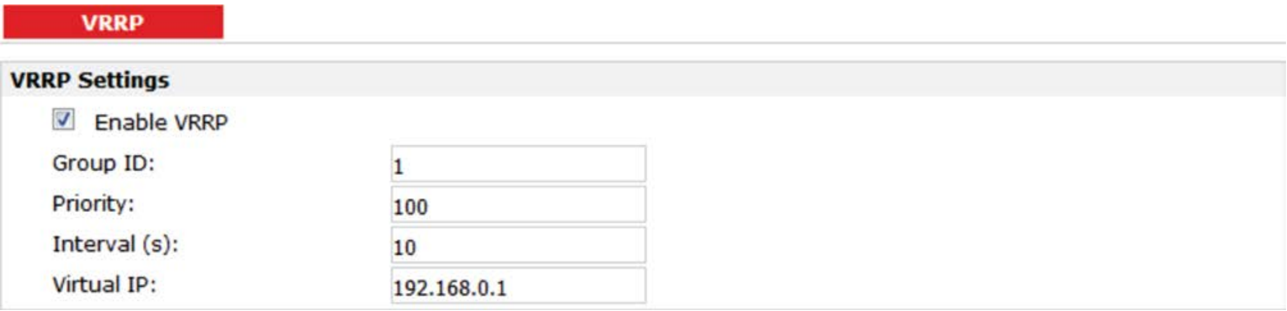
port: 1883

Password:

NovusLink @ Portal		
Item	Description	Default
Server address	Enter IP address of NovusLink.	Null
Port	Enter port number of NovusLink.	1883
Password	Enter the password preset in NovusLink. *Note: The passwords set in AIRGATE-3G and NovusLink need to be the same.*	Null

3.39 CONFIGURATION -> VRRP

This section allows users to set the VRRP parameters.



VRRP Settings

☑ Enable VRRP

Group ID: 1

Priority: 100

Interval (s): 10

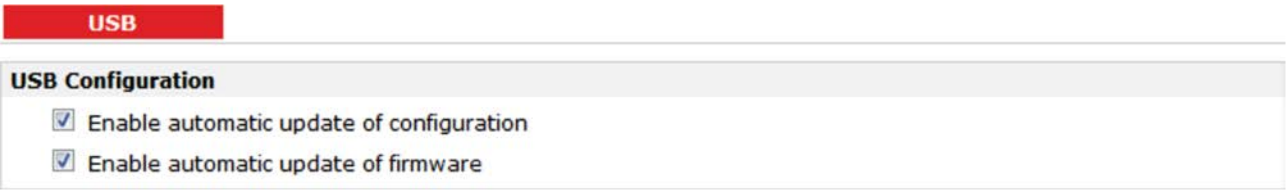
Virtual IP: 192.168.0.1

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 master router and the others as backups. In case the master fails, the virtual IP address is mapped to a backup router's IP address. (This backup becomes the master router.)	192.168.0.1

3.40 CONFIGURATION -> USB

This section allows users to set the USB parameters.

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



USB Configuration

☑ Enable automatic update of configuration

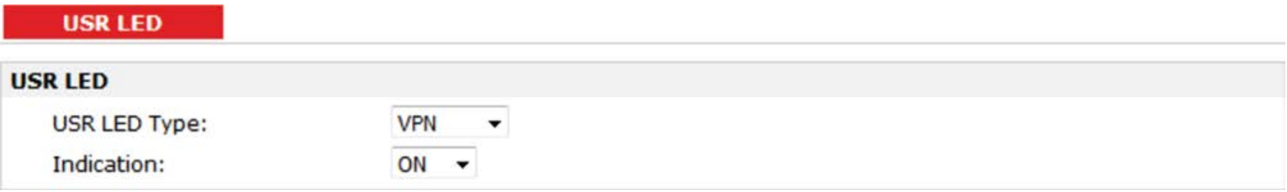
☑ Enable automatic update of firmware

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

3.41 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

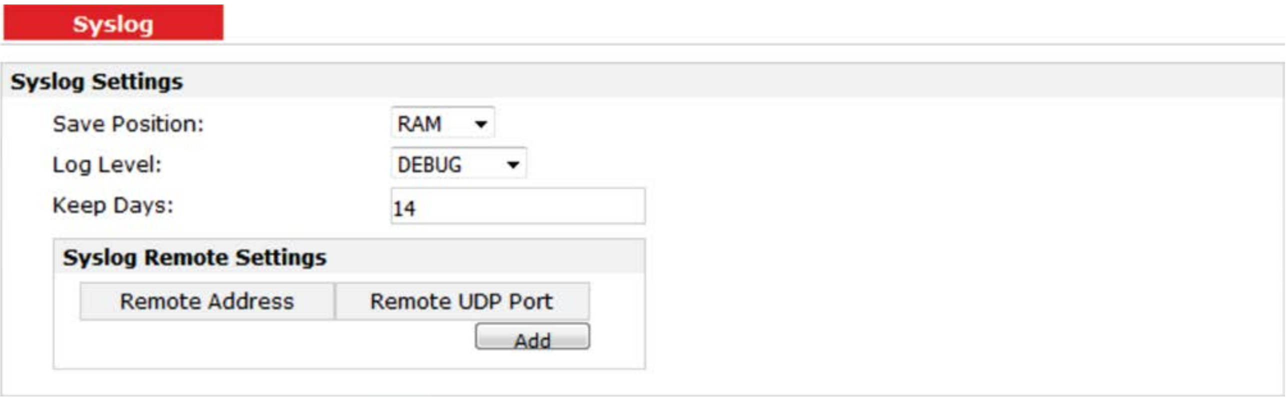
USR LED Type: VPN

Indication: ON

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

3.42 CONFIGURATION -> SYSLOG

This section allows users to set the Syslog parameters.



Syslog Settings

Save Position: RAM

Log Level: DEBUG

Keep Days: 14

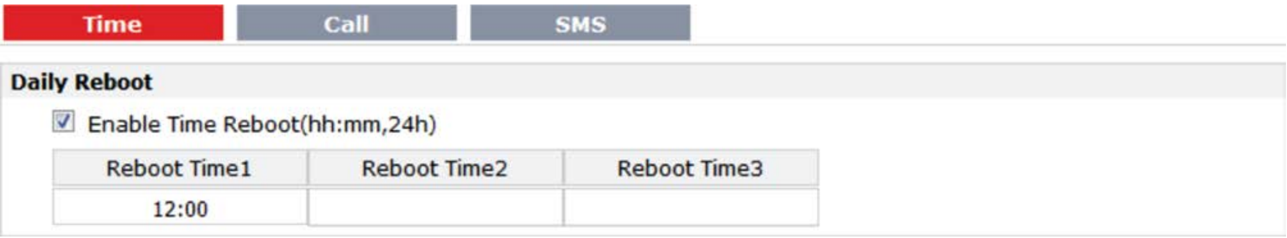
Syslog Remote Settings

Remote Address	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
Syslog Remote Settings	Setting to allow router sending syslog to the remote syslog server. You need to enter the IP and Port of the syslog server.	Disable

3.43 CONFIGURATION -> REBOOT

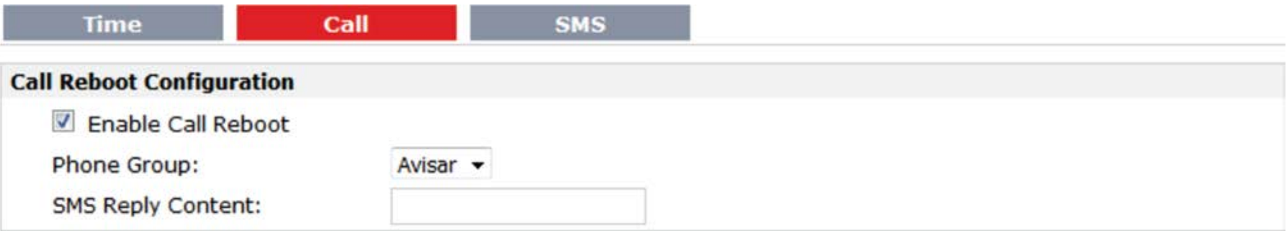
This section allows users to set the Reboot policies.



Daily Reboot

☑ Enable Time Reboot(hh:mm,24h)

Reboot Time1	Reboot Time2	Reboot Time3
12:00		

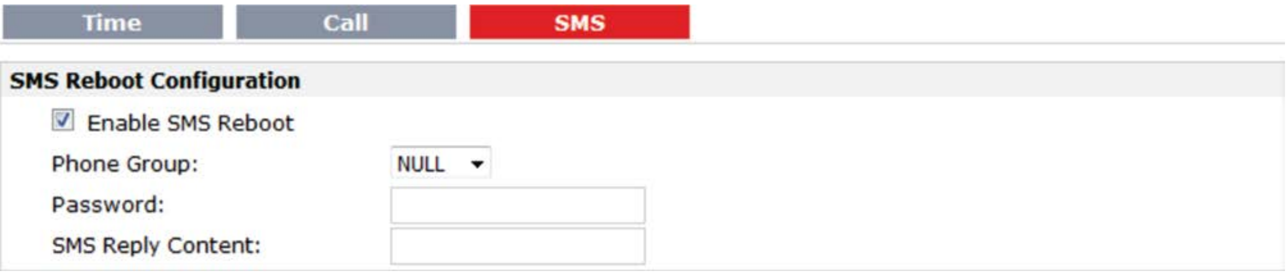


Call Reboot Configuration

☑ Enable Call Reboot

Phone Group: Avisar

SMS Reply Content:



SMS Reboot Configuration

☑ Enable SMS Reboot

Phone Group: NULL

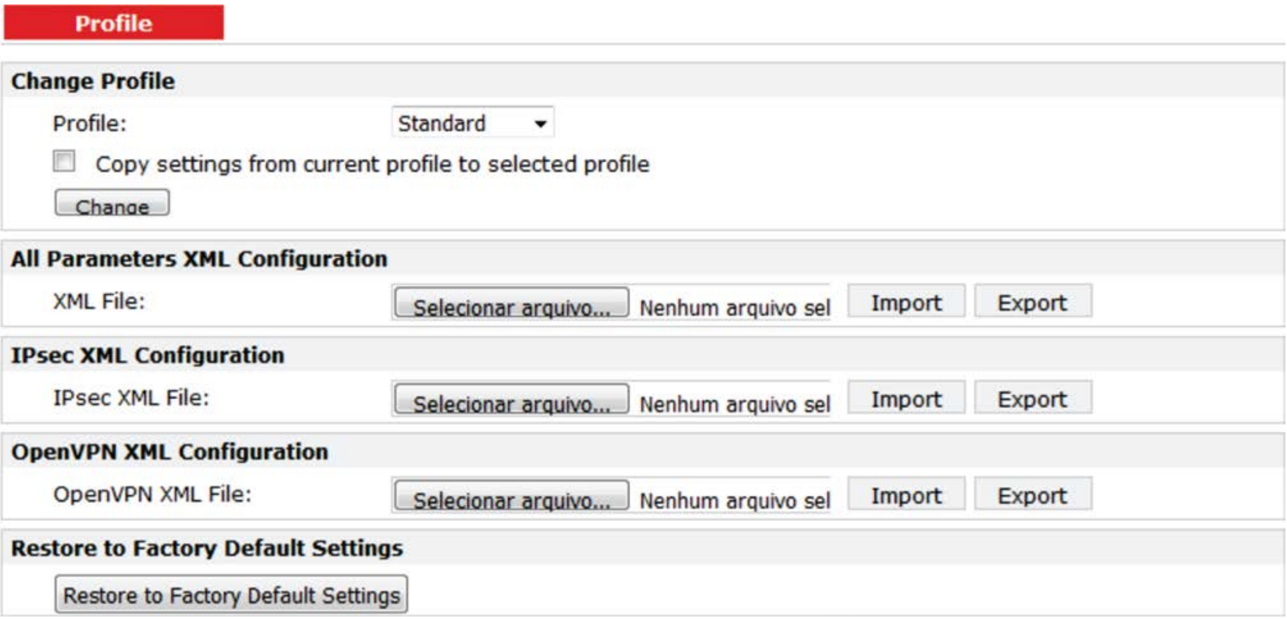
Password:

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

3.44 ADMINISTRATION -> PROFILE

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



Profile

Change Profile

Profile: Standard

□ Copy settings from current profile to selected profile

All Parameters XML Configuration

XML File:

IPsec XML Configuration

IPsec XML File:

OpenVPN XML Configuration

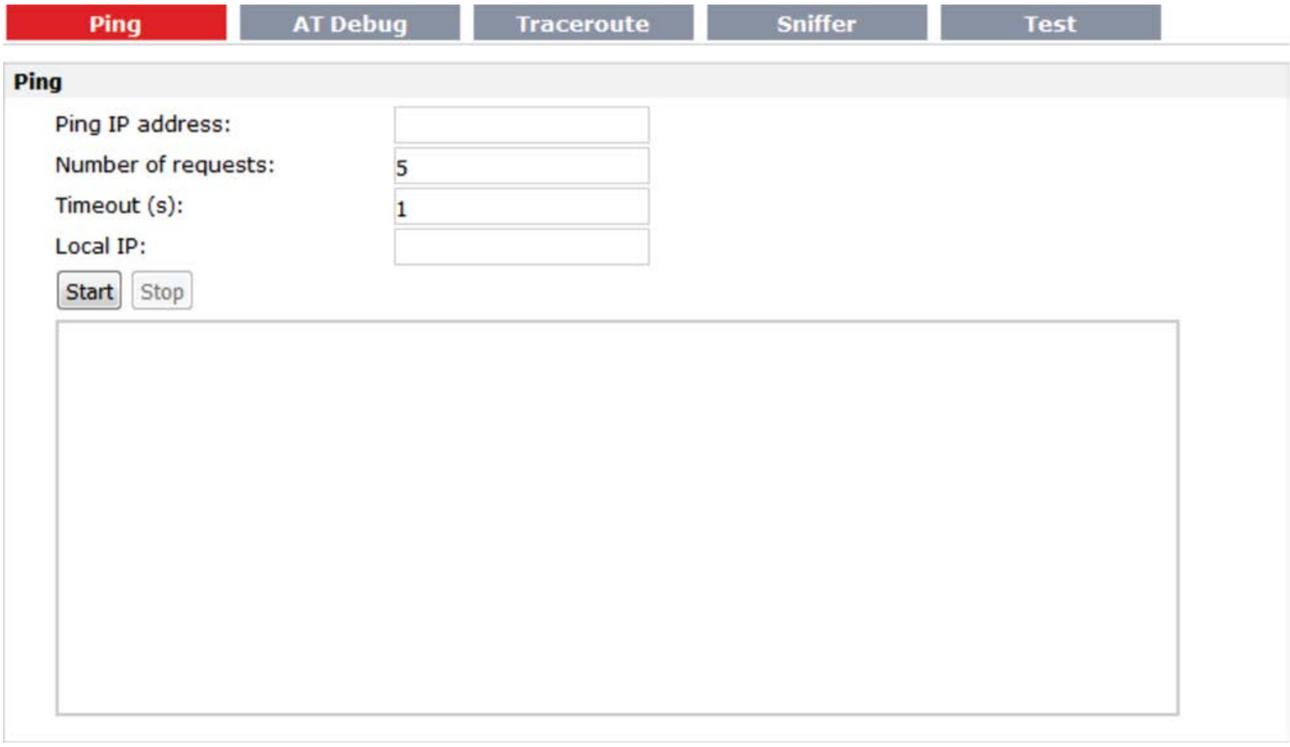
OpenVPN XML File:

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

3.45 ADMINISTRATION -> TOOLS

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



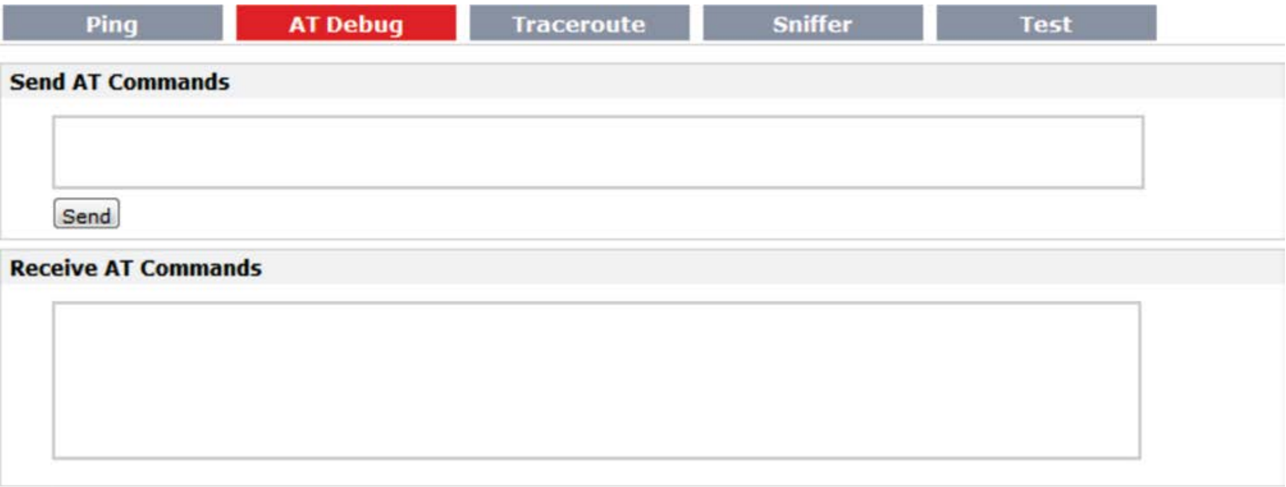
Ping IP address:

Number of requests: 5

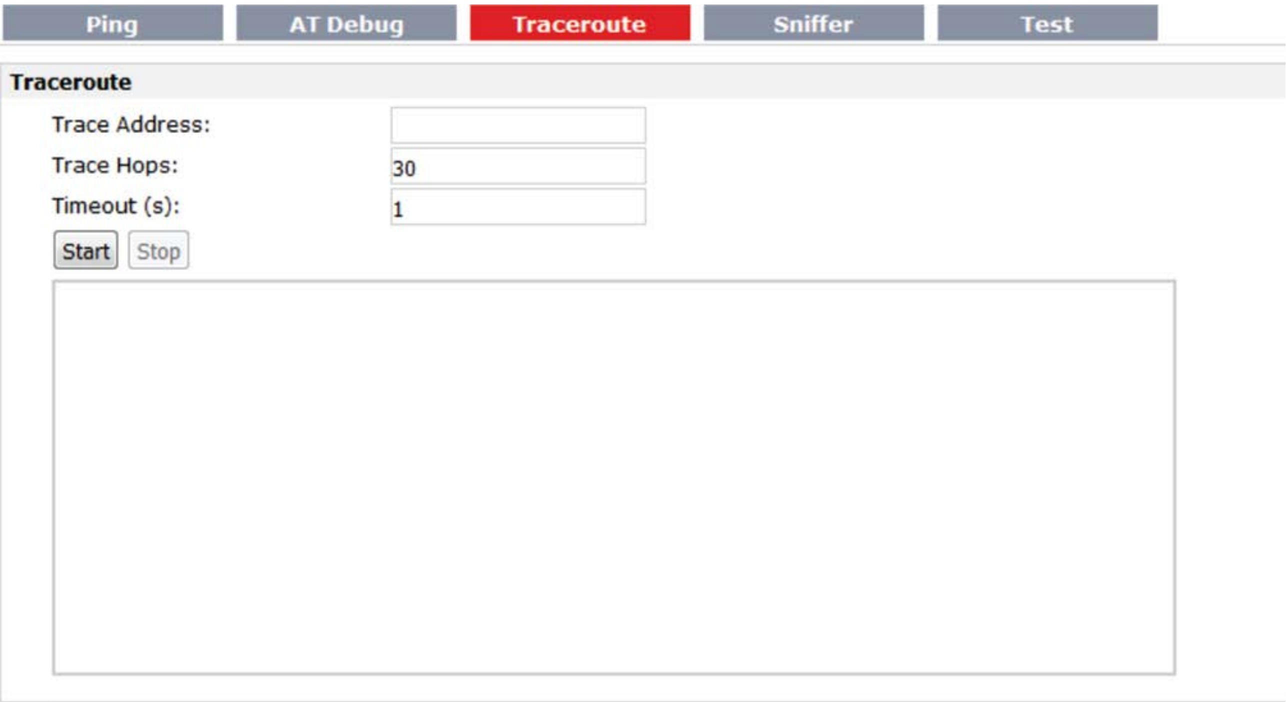
Timeout (s): 1

Local IP:

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



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

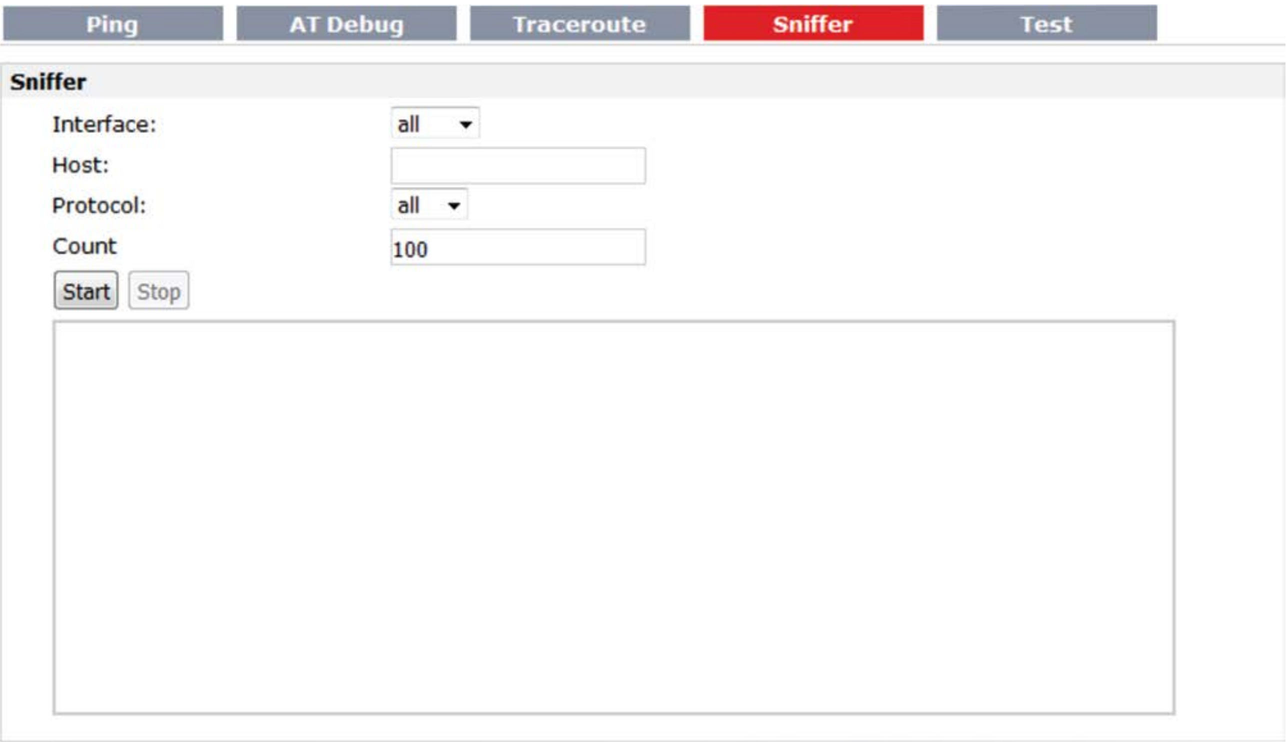


Trace Address:

Trace Hops: 30

Timeout (s): 1

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



Sniffer

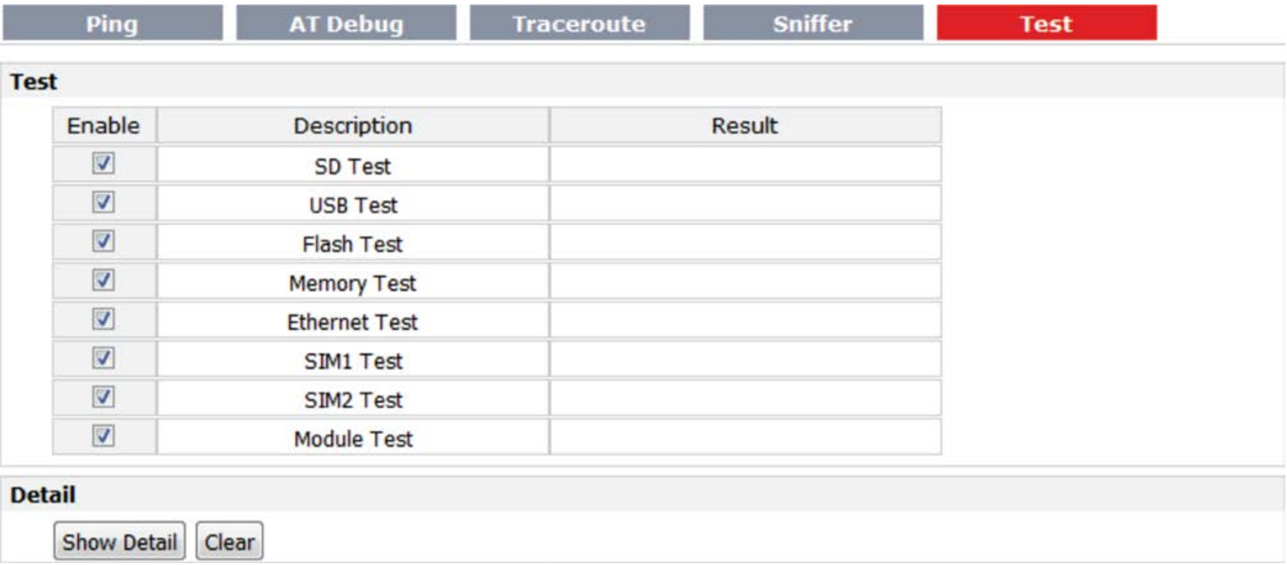
Interface:	all
Host:	
Protocol:	all
Count	100

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
Count	Set the packet number that can be sniffered at a time.	100
Start	Click this button to start the sniffer, and the log will be displayed in the follow box.	Null



Test

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

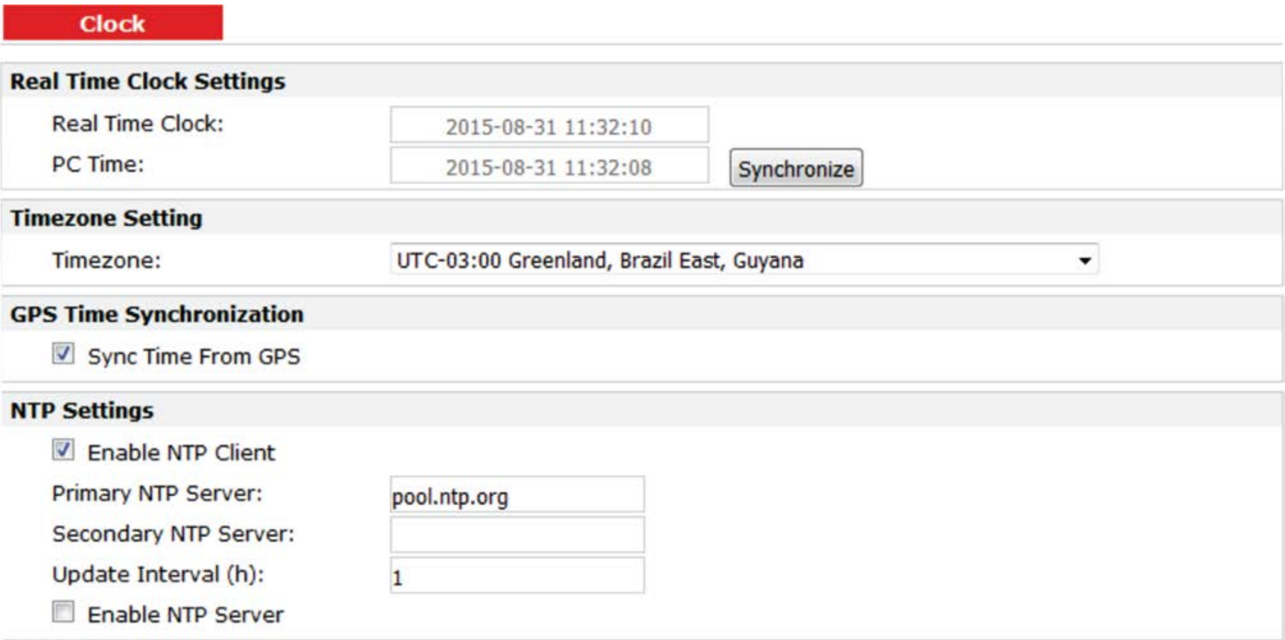
Detail

Show Detail Clear

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

3.46 ADMINISTRATION -> CLOCK

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



Real Time Clock Settings

Real Time Clock: 2015-08-31 11:32:10

PC Time: 2015-08-31 11:32:08

Timezone Setting

Timezone: UTC-03:00 Greenland, Brazil East, Guyana

GPS Time Synchronization

☑ Sync Time From GPS

NTP Settings

☑ Enable NTP Client

Primary NTP Server: pool.ntp.org

Secondary NTP Server:

Update Interval (h): 1

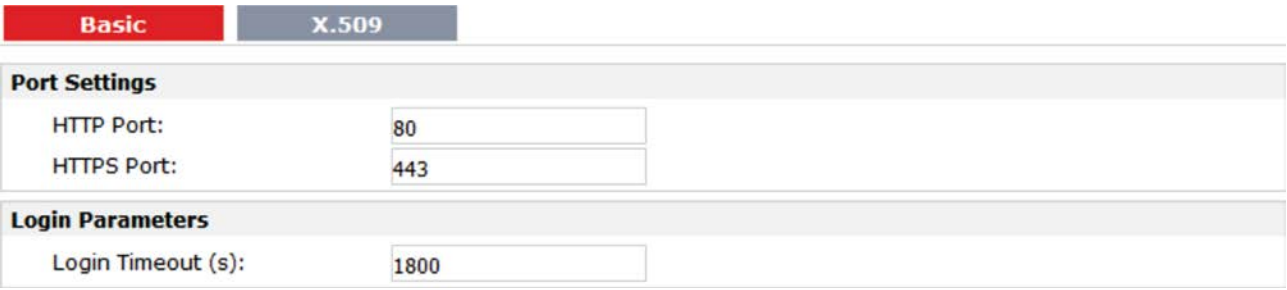
☐ Enable NTP Server

Clock		
Item	Description	Default
Real Time Clock	Router’s RTC can be showed and modified in this field.	Null
PC Time	You PC’s time can be showed here.	Null
Synchronize	Synchronize router’s RTC with PC.	Null
Enable NTP Client	Enable to synchronize the time from NTP server.	Disable
Timezone @ Client	Select your local time zone.	UTC +08:00
Sync Time From GPS @ GPS Time Synchronization	Synchronize router’s RTC from GPS.	Disable
Primary NTP Server	Enter primary NTP Server’s IP address or domain name.	pool.ntp.org
Secondary NTP Server	Enter secondary NTP Server’s IP address or domain name.	Null
Update interval (h)	Enter the interval which NTP client synchronize the time from NTP server.	1

Enable NTP Server	Click to enable the NTP server function of router.	Disable
Timezone @ Server	Select your local time zone.	UTC +08:00

3.47 ADMINISTRATION -> WEB SERVER

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



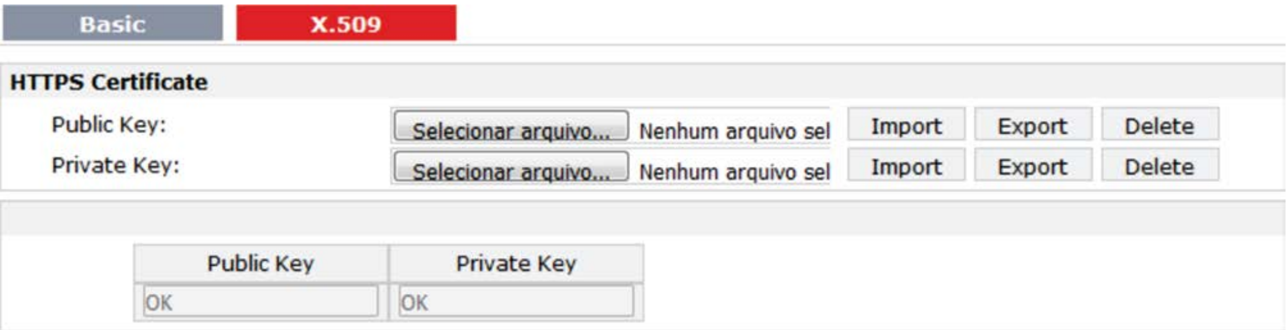
Port Settings

HTTP Port: 80

HTTPS Port: 443

Login Parameters

Login Timeout (s): 1800



HTTPS Certificate

Public Key:

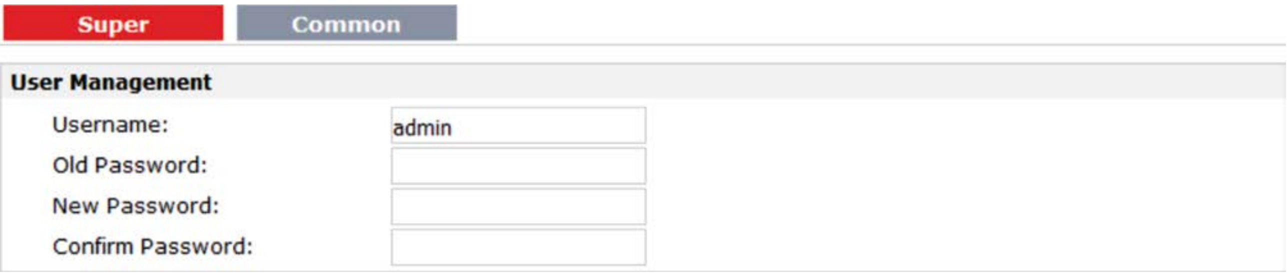
Private Key:

Public Key	Private Key
OK	OK

Basic @ Web Server		
Item	Description	Default
HTTP Port	Enter the HTTP port number you want to change in AIRGATE-3G's Web Server. On a Web server, port 80 is the port that the server "listens to" or expects to receive from a Web client. If you configure the router with other HTTP Port number except 80, only adding that port number then you can login AIRGATE-3G's Web Server.	80
HTTPS Port	Enter the HTTPS port number you want to change in AIRGATE-3G's Web Server. On a Web server, port 443 is the port that the server "listens to" or expects to receive from a Web client. If you configure the router with other HTTPS Port number except 443, only adding that port number then you can login AIRGATE-3G's Web Server. ***Note**: HTTPS is more secure than HTTP. In many cases, clients may be exchanging confidential information with a server, which needs to be secured in order to prevent unauthorized access. For this reason, HTTP was developed by Netscape corporation to allow authorization and secured transactions.*	443
Login Timeout (s)	Enter the Login timeout you want to change in AIRGATE-3G's Web Server. After "Login Timeout", AIRGATE-3G will force to log out the Web GUI and then you need to re-login again to Web GUI.	1800
X.509 @ Web Server		
HTTPS Certificate	In this tab, user can import, export or delete "Public Key" and "Private Key" for HTTPS certification.	Null

3.48 ADMINISTRATION -> USER MANAGEMENT

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



User Management

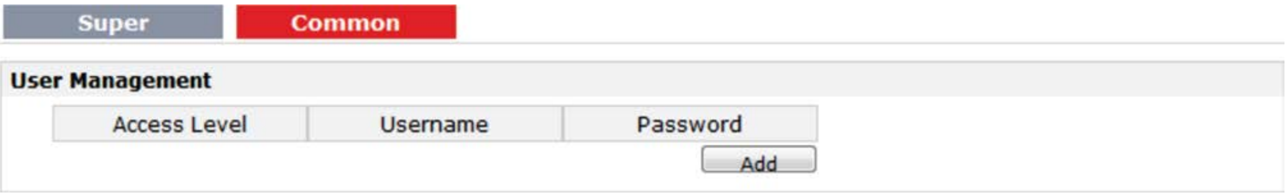
Username: admin

Old Password:

New Password:

Confirm Password:

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. ***Note**: AIRGATE-3G support SSH2 for management. Details you can check Application Note of AIRGATE-3G.*	Null



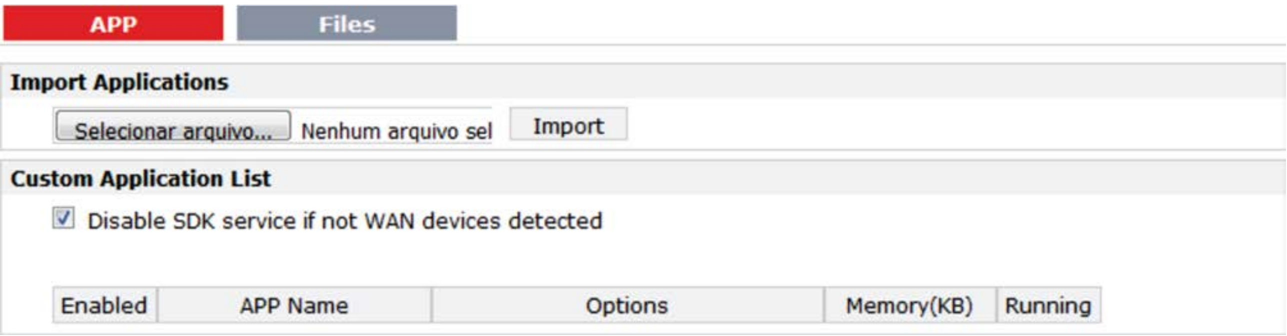
User Management

Access Level	Username	Password

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

3.49 ADMINISTRATION -> SDK MANAGEMENT

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



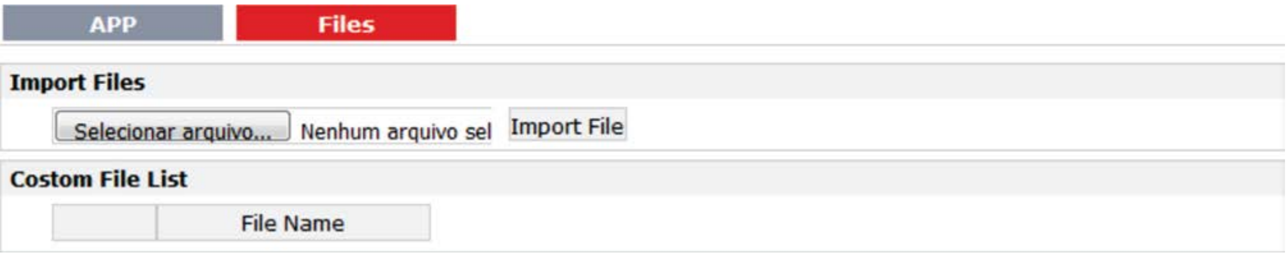
Import Applications

Custom Application List

☑ Disable SDK service if not WAN devices detected

Enabled	APP Name	Options	Memory(KB)	Running

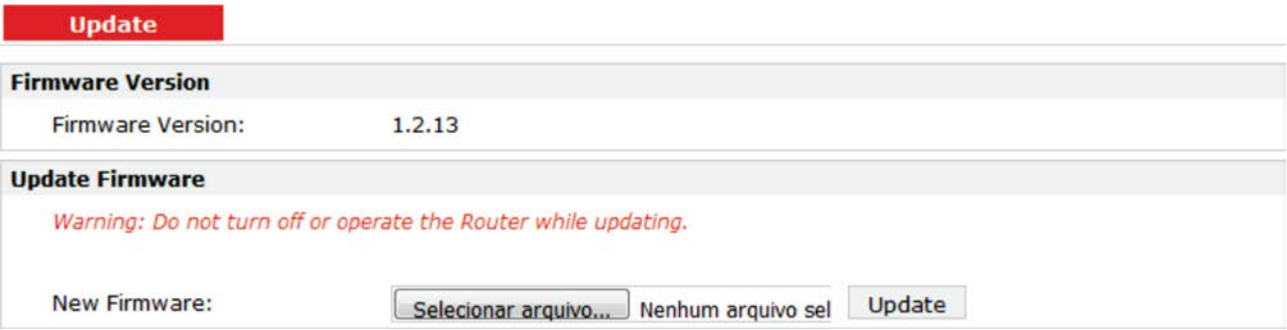
APP @ SDK Management		
Item	Description	Default
Firmware Version	Show the current firmware version.	Null
Import Files	Click to import APP files in this item.	Null
Custom Application List	This list shows which APP files you have imported to the router, which APP file you want to start up, as well as the running information. Enable: Click to enable the APP file. APP Name: Shows the name of the APP files. Options: It is an optional items, user can choose to configure startup parameters here. Memory (KB): Shows the memory resources occupied by the APP files. Running: Shows whether the APP files are running.	Null



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

3.50 ADMINISTRATION -> UPDATE FIRMWARE

This section allows users to update the firmware of router.



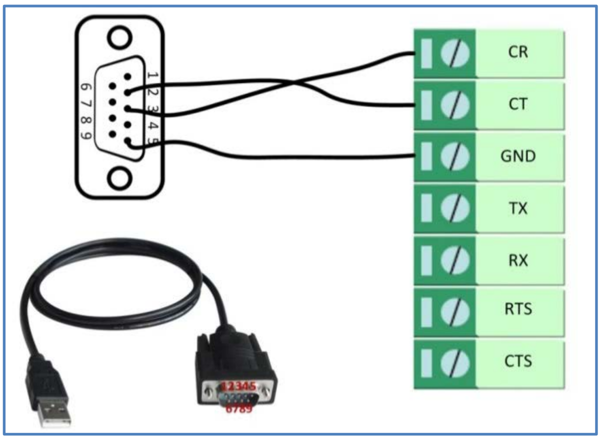
Update		
Item	Description	Default
Firmware Version	Show the current firmware version.	
Firmware Old Version	Show the old firmware version of the router. Click "Apply" button to fall back to the old version, after updating successfully, you need to reboot router to take effect.	
Update firmware	Click "Select File" button to select the correct firmware in your PC, and then click "Update" button" to update. After updating successfully, you need to reboot router to take effect.	Null

4. CONFIGURATION EXAMPLES

4.1 INTERFACE

4.1.1 CONSOLE PORT

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

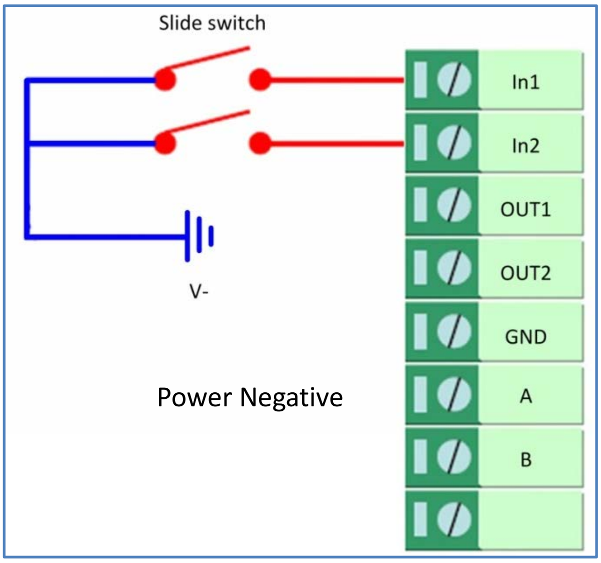


4.1.2 DIGITAL INPUT

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

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

*Import note: **do not** connect In1/In2 and Slide switch directly to "**GND**" of the terminal block, or DI will not work.*



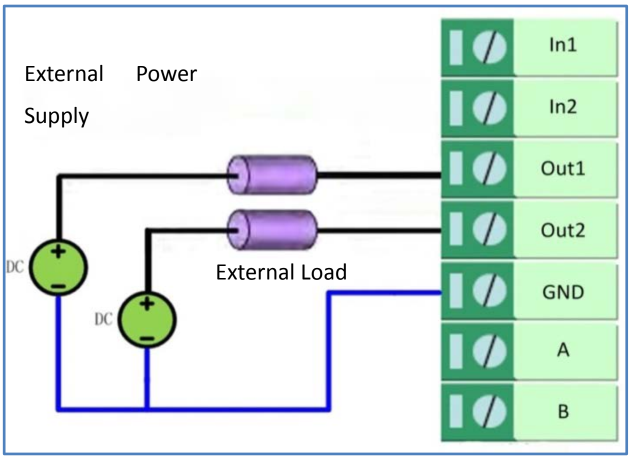
4.1.3 DIGITAL OUTPUT

There are two digital outputs of AIRGATE-3G.

Power negative of DC should connect to "GND"

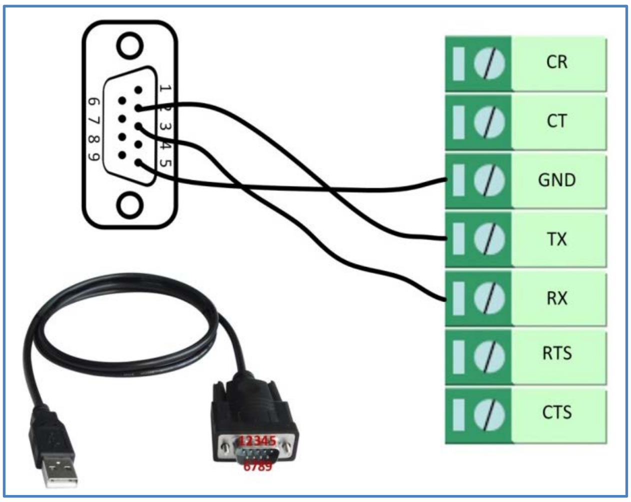
Please refer to connection diagram at the right site.

Maximum voltage/current/output power of DO is 30VDC/0.3A/0.3W. It means voltage difference between Out1/Out2 and GND cannot exceed to 30VDC; the current value through Out1/Out2 cannot exceed to 300mA. And the output power dissipated by Out1/Out2 cannot exceed to 0.3W. Otherwise DO will be damaged.



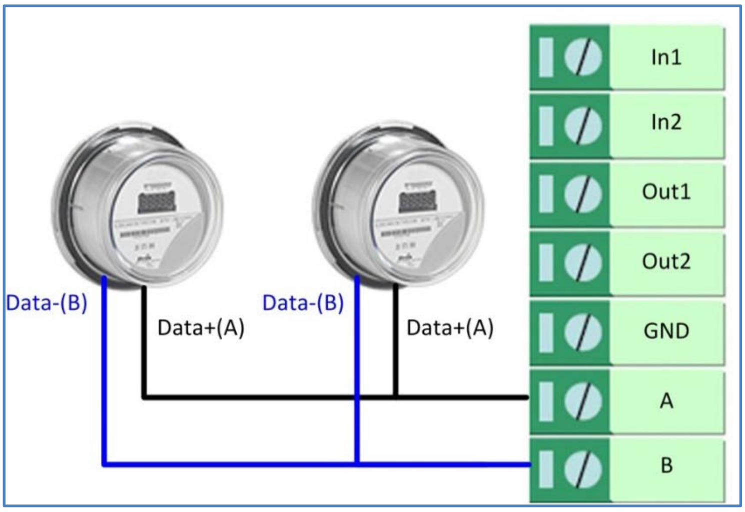
4.1.4 RS232

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



4.1.5 RS485

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



4.2 CELLULAR

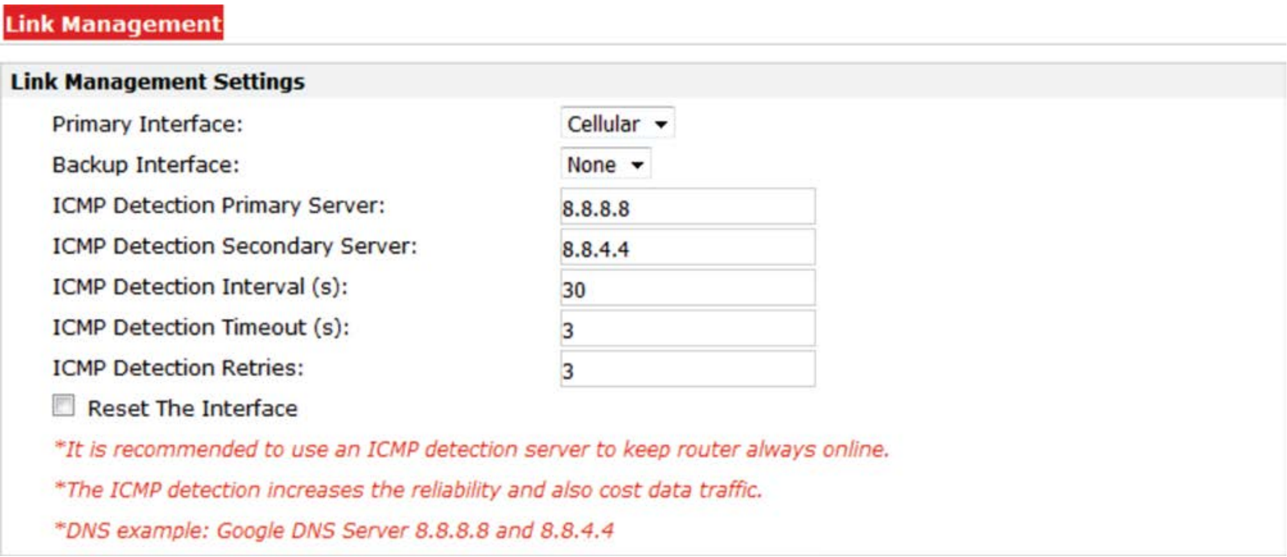
4.2.1 CELLULAR DIAL-UP

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

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

1. Always Online

Configuration-->Link Management-->Cellular



Link Management

Link Management Settings

Primary Interface:	Cellular ▾
Backup Interface:	None ▾
ICMP Detection Primary Server:	8.8.8.8
ICMP Detection Secondary Server:	8.8.4.4
ICMP Detection Interval (s):	30
ICMP Detection Timeout (s):	3
ICMP Detection Retries:	3

□ Reset The Interface

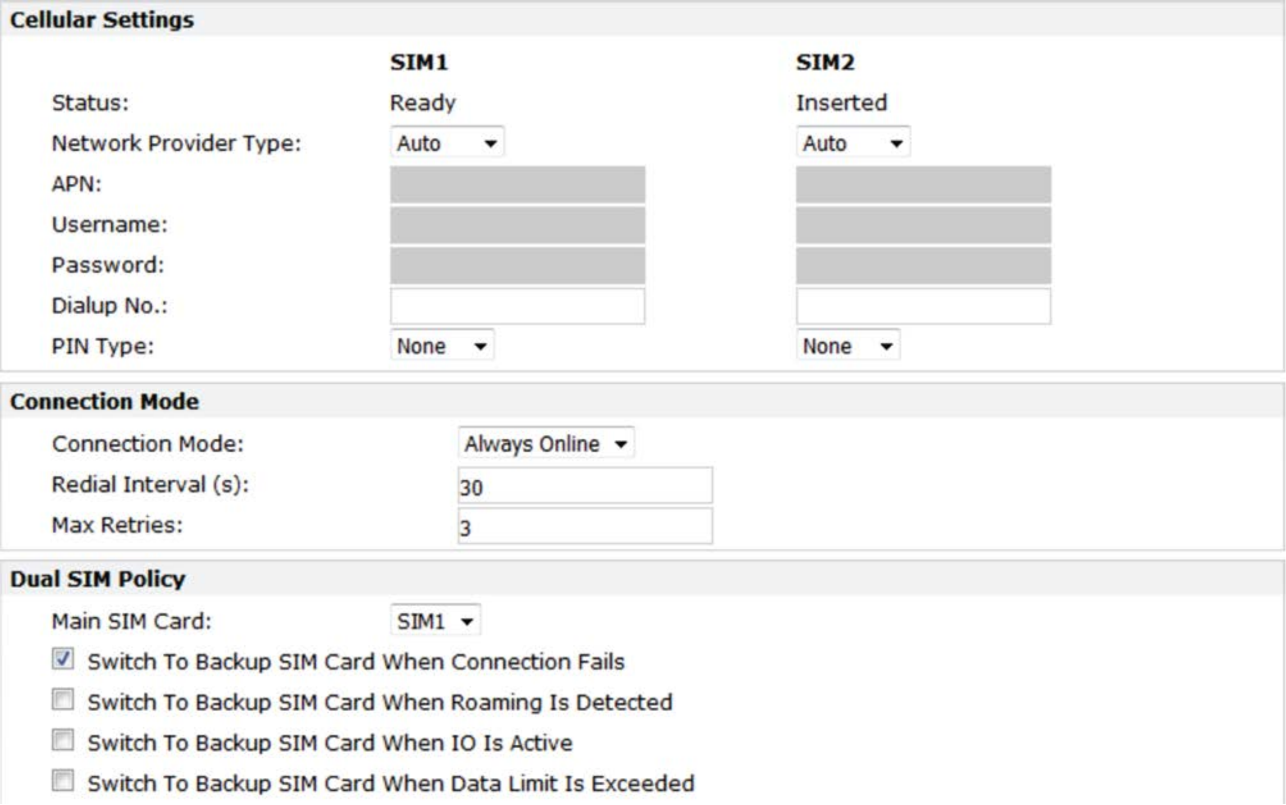
*It is recommended to use an ICMP detection server to keep router always online.

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

*DNS example: Google DNS Server 8.8.8.8 and 8.8.4.4

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

Configuration-->Cellular WAN -->Basic



Cellular Settings

	SIM1	SIM2
Status:	Ready	Inserted
Network Provider Type:	Auto ▾	Auto ▾
APN:		
Username:		
Password:		
Dialup No.:		
PIN Type:	None ▾	None ▾

Connection Mode

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

Dual SIM Policy

Main SIM Card: SIM1 ▾

☑ Switch To Backup SIM Card When Connection Fails

□ Switch To Backup SIM Card When Roaming Is Detected

□ Switch To Backup SIM Card When IO Is Active

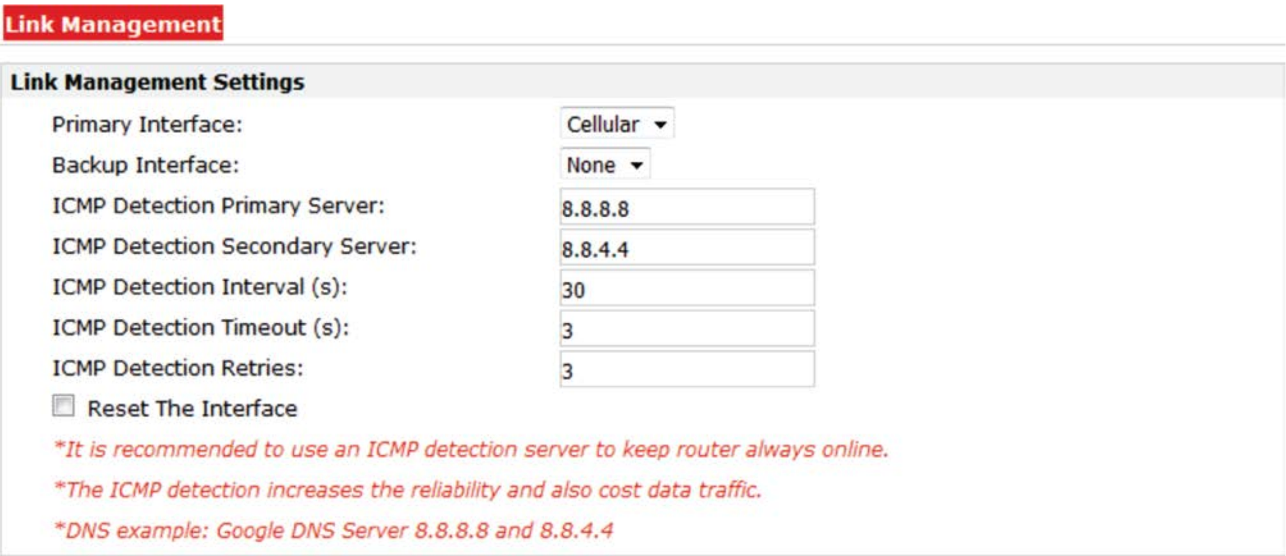
□ Switch To Backup SIM Card When Data Limit Is Exceeded

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

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

2. Connect on Demand

Configuration-->Link Management-->Cellular



Link Management Settings

Primary Interface:	Cellular ▾
Backup Interface:	None ▾
ICMP Detection Primary Server:	8.8.8.8
ICMP Detection Secondary Server:	8.8.4.4
ICMP Detection Interval (s):	30
ICMP Detection Timeout (s):	3
ICMP Detection Retries:	3

☐ Reset The Interface

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

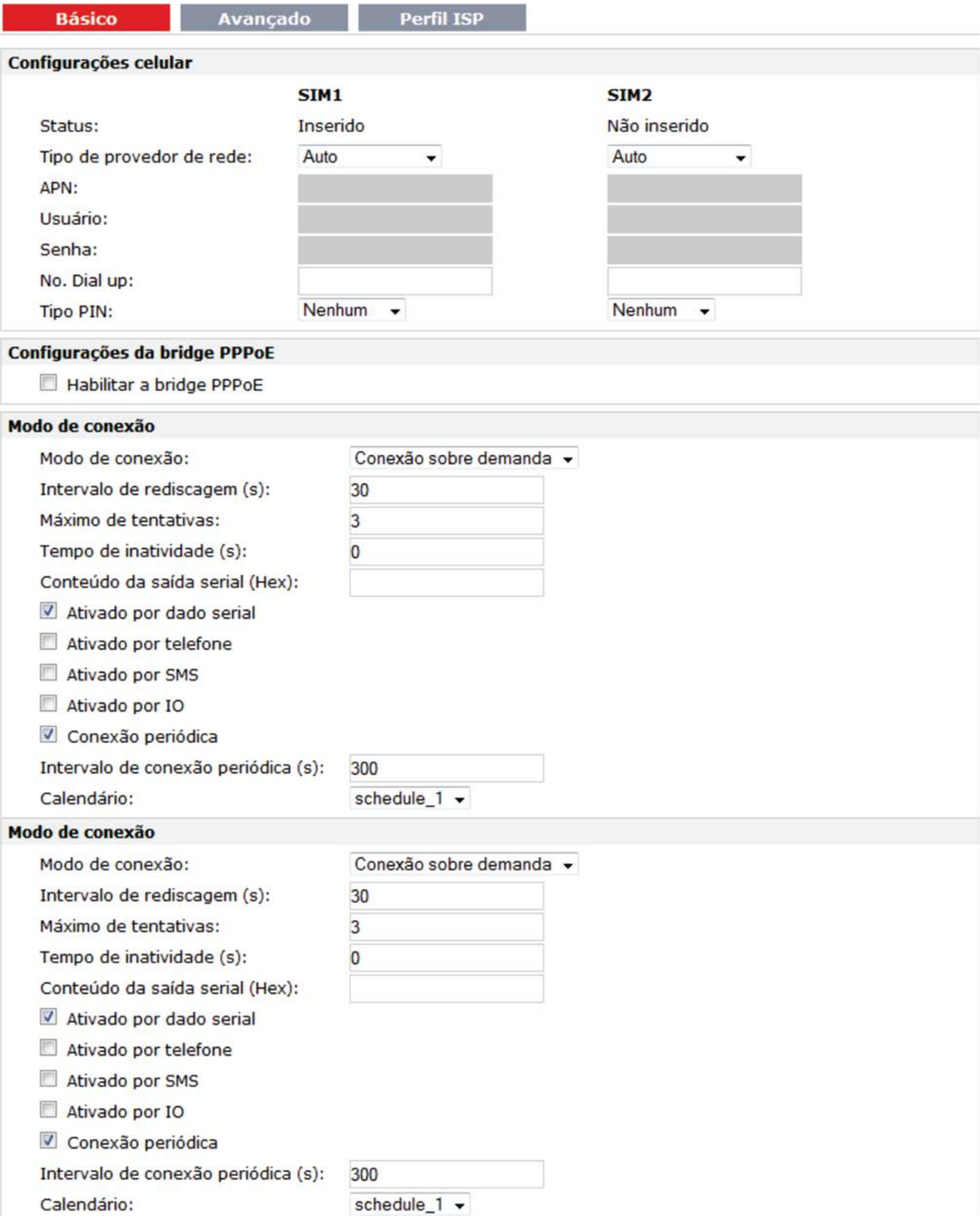
*The ICMP detection increases the reliability and also cost data traffic.

*DNS example: Google DNS Server 8.8.8.8 and 8.8.4.4

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

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

Configuration-->Cellular WAN -->Basic



Básico | Avançado | Perfil ISP

Configurações celular

	SIM1	SIM2
Status:	Inserido	Não inserido
Tipo de provedor de rede:	Auto	Auto
APN:		
Usuário:		
Senha:		
No. Dial up:		
Tipo PIN:	Nenhum	Nenhum

Configurações da bridge PPPoE

☐ Habilitar a bridge PPPoE

Modo de conexão

Modo de conexão: Conexão sobre demanda

Intervalo de rediscagem (s): 30

Máximo de tentativas: 3

Tempo de inatividade (s): 0

Conteúdo da saída serial (Hex):

☑ Ativado por dado serial

☐ Ativado por telefone

☐ Ativado por SMS

☐ Ativado por IO

☑ Conexão periódica

Intervalo de conexão periódica (s): 300

Calendário: schedule_1

Modo de conexão

Modo de conexão: Conexão sobre demanda

Intervalo de rediscagem (s): 30

Máximo de tentativas: 3

Tempo de inatividade (s): 0

Conteúdo da saída serial (Hex):

☑ Ativado por dado serial

☐ Ativado por telefone

☐ Ativado por SMS

☐ Ativado por IO

☑ Conexão periódica

Intervalo de conexão periódica (s): 300

Calendário: schedule_1

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

AIRGATE-3G supports remote control via SMS. User can use following commands to get the status of AIRGATE-3G, cannot set new parameters of AIRGATE-3G 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 AIRGATE-3G.

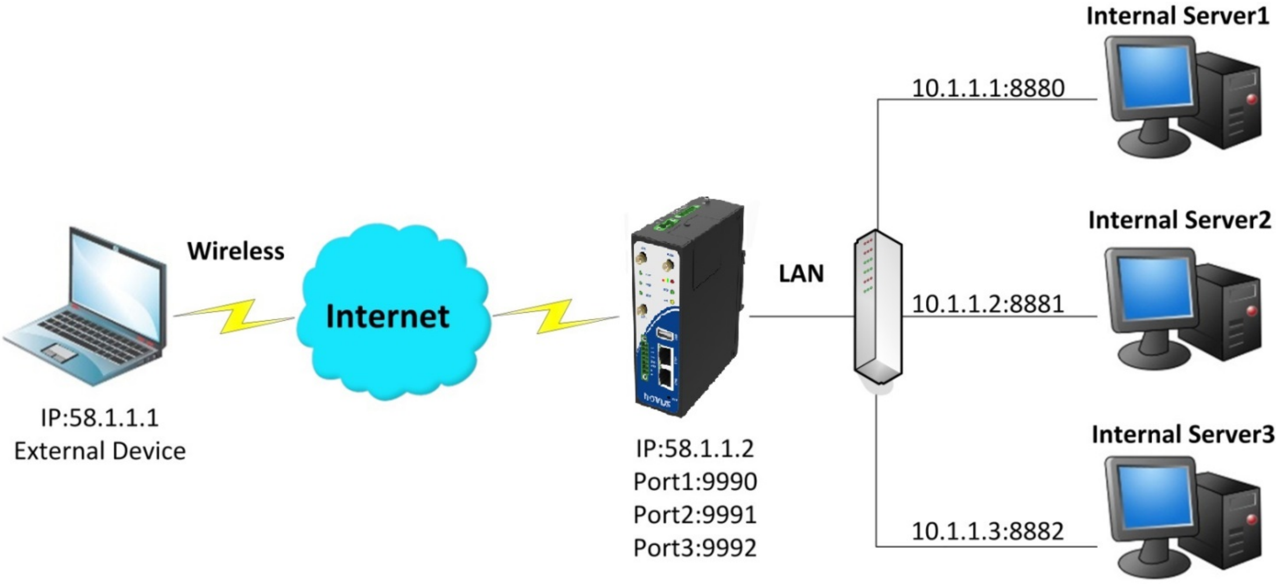
Cmd	Description	Syntax	Comments
Control Commands			
0001	Reset Device	cmd	if no password, please use command "cmd", or use command" password: cmd" cmd1 + cmd2: cmd1;cmd2 * - means can be null
0002	Save Parameters	cmd	
0003	Save Parameters and Reset Device	cmd	
0004	Start PPP Dialup	cmd	
0005	Stop PPP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

4.3 NETWORK

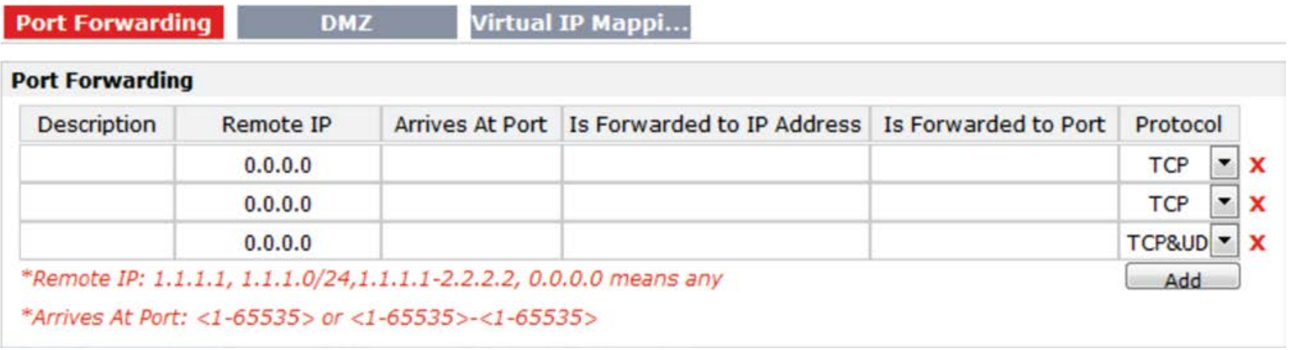
4.3.1 NAT

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

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



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



Port Forwarding

Description	Remote IP	Arrives At Port	Is Forwarded to IP Address	Is Forwarded to Port	Protocol
	0.0.0.0				TCP
	0.0.0.0				TCP
	0.0.0.0				TCP&UD

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

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

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

Explanations for above diagram:

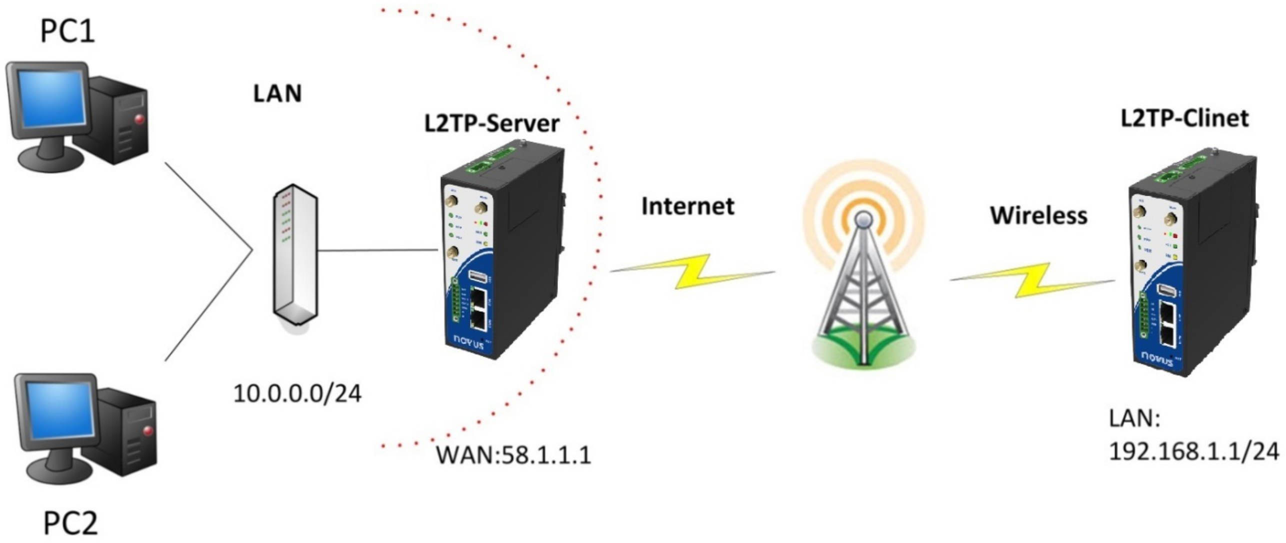
If there are two IP addresses 58.1.1.1 and 59.1.1.1 for the External Devices, that the result will be different from the test when the NAT is working at AIRGATE-3G.

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

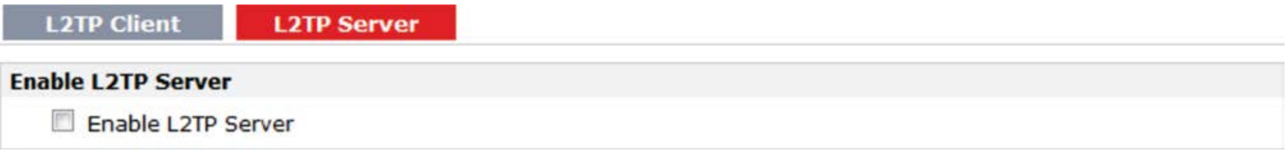
58.1.1.1----------access to--------->58.1.1.2:9991----------be forwarded to------->10.1.1.2:8001 UDP

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



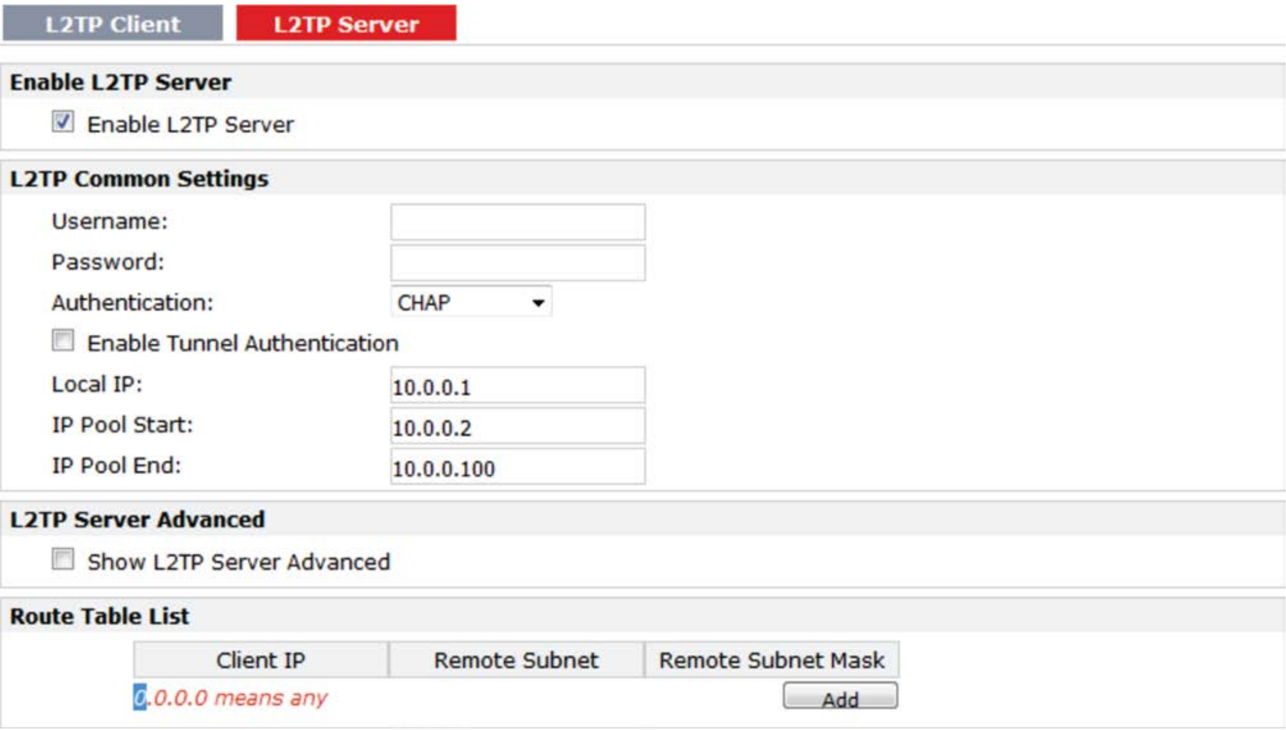
L2TP_SERVER:
Configuration--->L2TP--->L2TP Server



Enable L2TP Server

□ Enable L2TP Server

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



Enable L2TP Server

☑ Enable L2TP Server

L2TP Common Settings

Username:

Password:

Authentication: CHAP

□ Enable Tunnel Authentication

Local IP: 10.0.0.1

IP Pool Start: 10.0.0.2

IP Pool End: 10.0.0.100

L2TP Server Advanced

□ Show L2TP Server Advanced

Route Table List

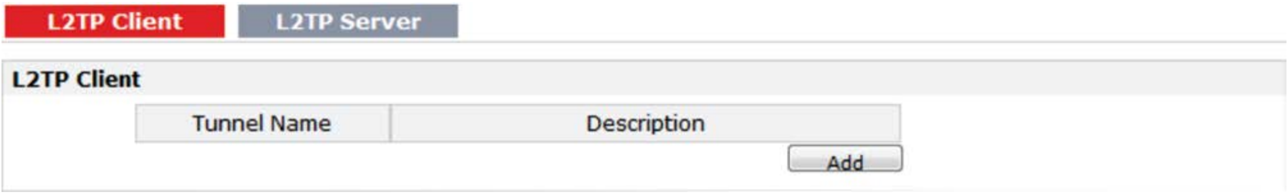
Client IP	Remote Subnet	Remote Subnet Mask
0.0.0.0 means any		

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

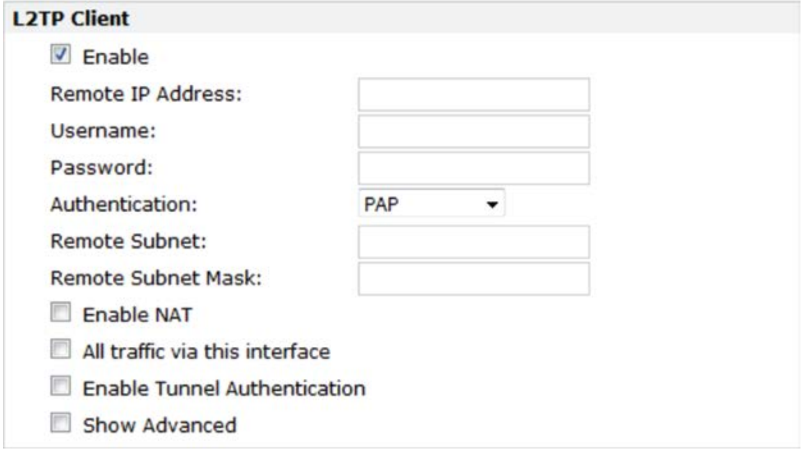
***Note:** The following diagrams with red color numbers mean these are the matches between server and client, and with the blue color number means it must be set locally for the tunnel.*

L2TP_CLIENT:

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



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


L2TP Client

☑ Enable

Remote IP Address:

Username:

Password:

Authentication: PAP

Remote Subnet:

Remote Subnet Mask:

☐ Enable NAT

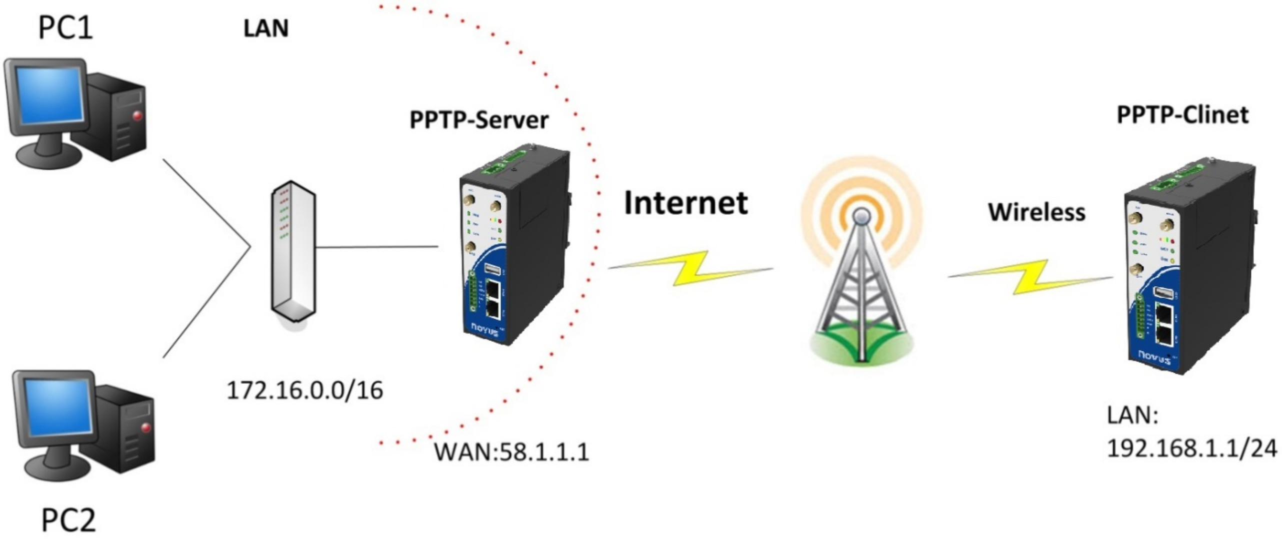
☐ All traffic via this interface

☐ Enable Tunnel Authentication

☐ Show Advanced

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

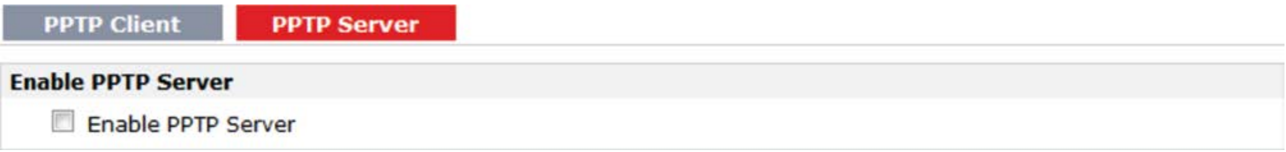
4.3.3 PPTP



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:

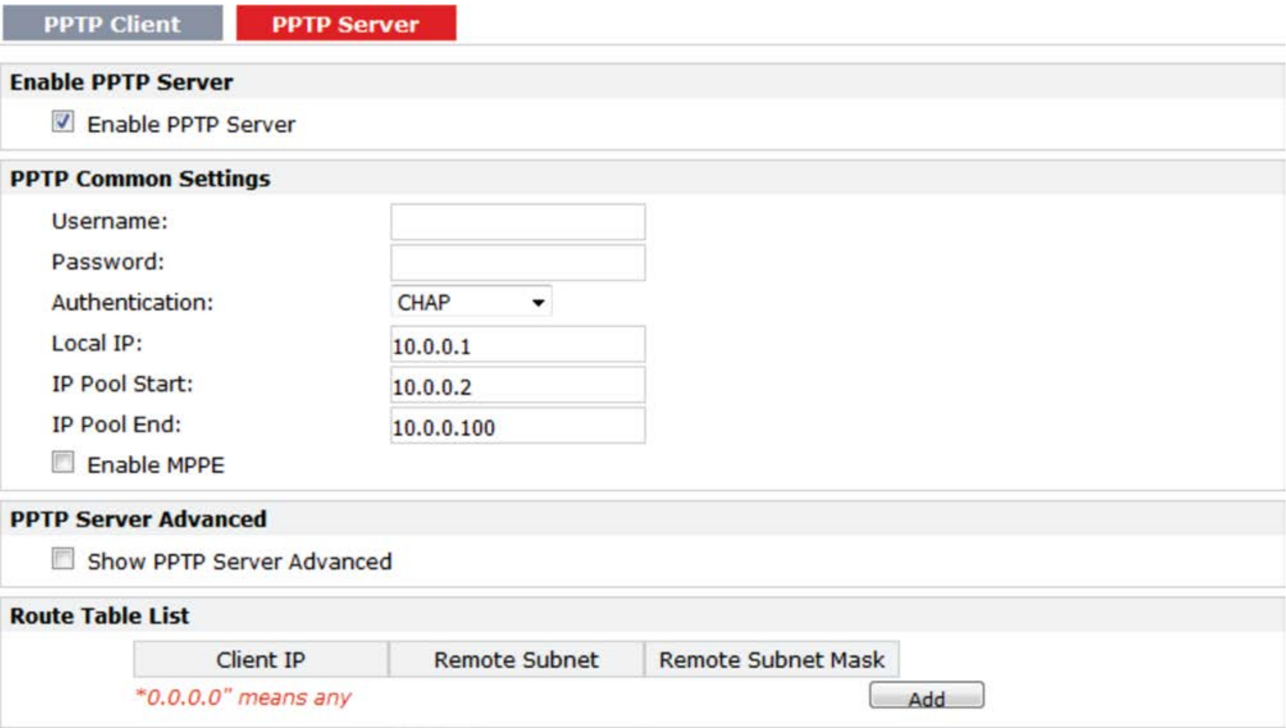
Configuration--->PPTP--->PPTP Server



Enable PPTP Server

□ Enable PPTP Server

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



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

Route Table List

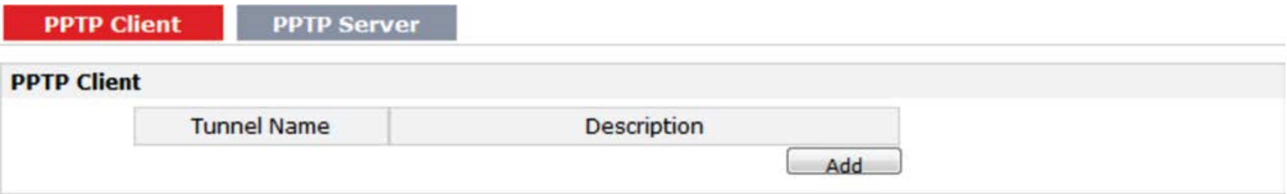
Client IP	Remote Subnet	Remote Subnet Mask

"0.0.0.0" means any

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

PPTP_CLIENT:

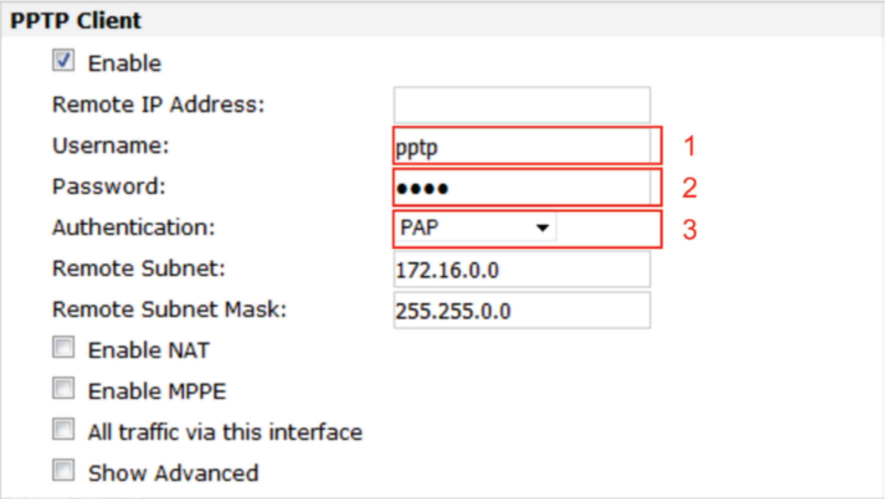
Configuration--->PPTP--->PPTP Client



PPTP Client

Tunnel Name	Description

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



PPTP Client

☑ Enable

Remote IP Address:	
Username:	pptp
Password:	●●●●
Authentication:	PAP
Remote Subnet:	172.16.0.0
Remote Subnet Mask:	255.255.0.0

□ Enable NAT

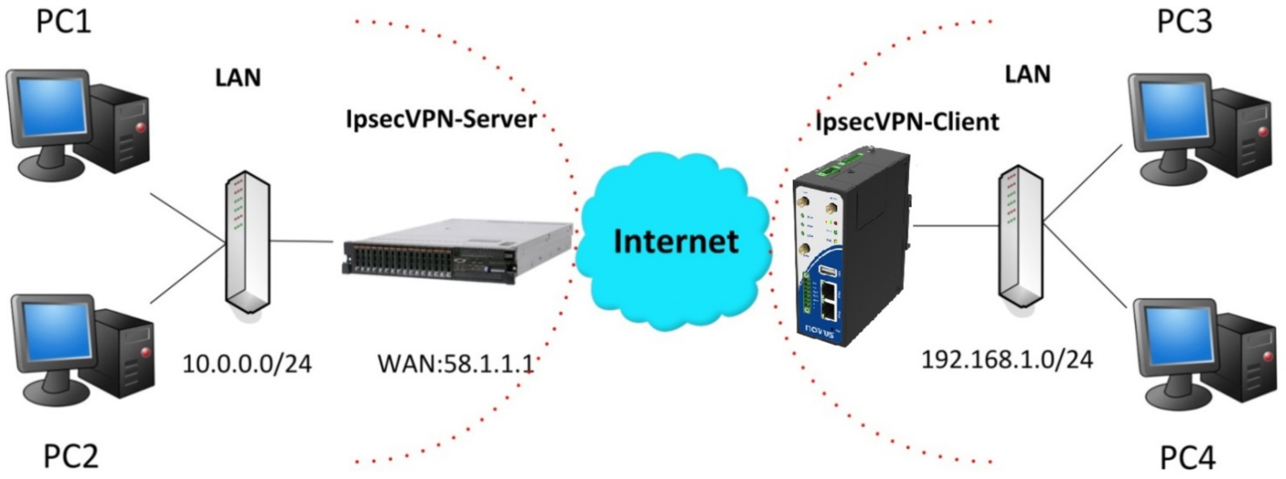
□ Enable MPPE

□ All traffic via this interface

□ Show Advanced

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

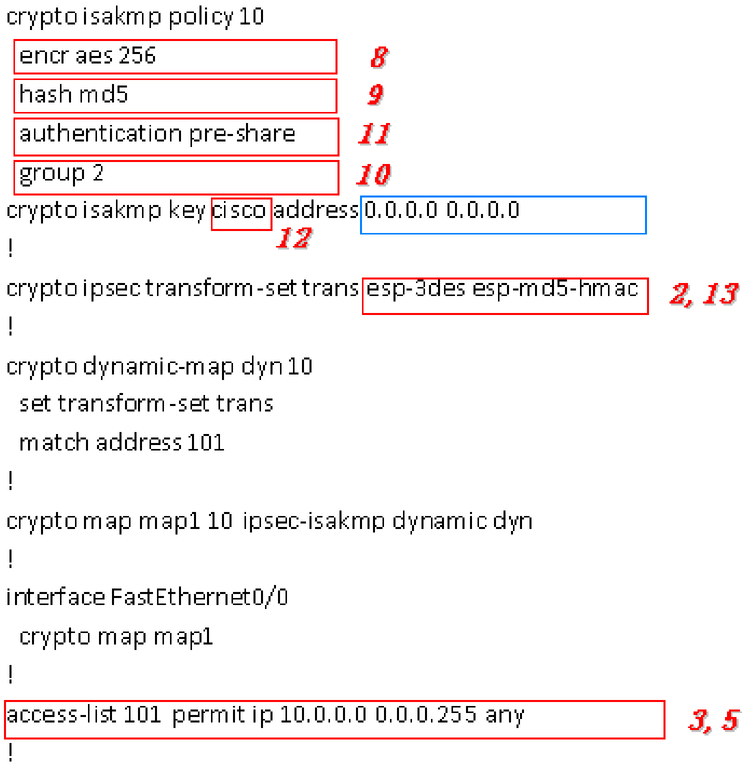
4.3.4 IPSEC VPN



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:

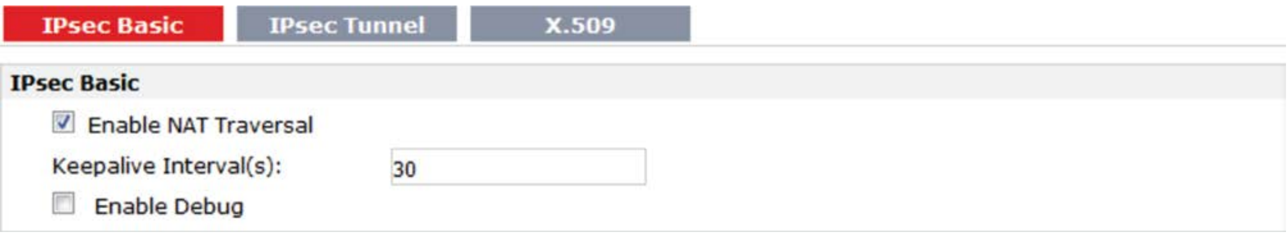


```
crypto isakmp policy 10
 encr aes 256
 hash md5
 authentication pre-share
 group 2
crypto isakmp key cisco address 0.0.0.0 0.0.0.0
!
crypto ipsec transform-set trans esp-3des esp-md5-hmac
!
crypto dynamic-map dyn 10
 set transform-set trans
 match address 101
!
crypto map map1 10 ipsec-isakmp dynamic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

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

IPsecVPN_CLIENT:

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



IPsec Basic

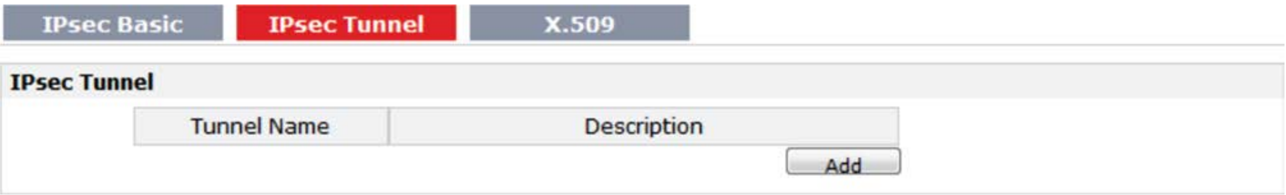
☑ Enable NAT Traversal

Keepalive Interval(s): 30

□ Enable Debug

Then click "Apply".

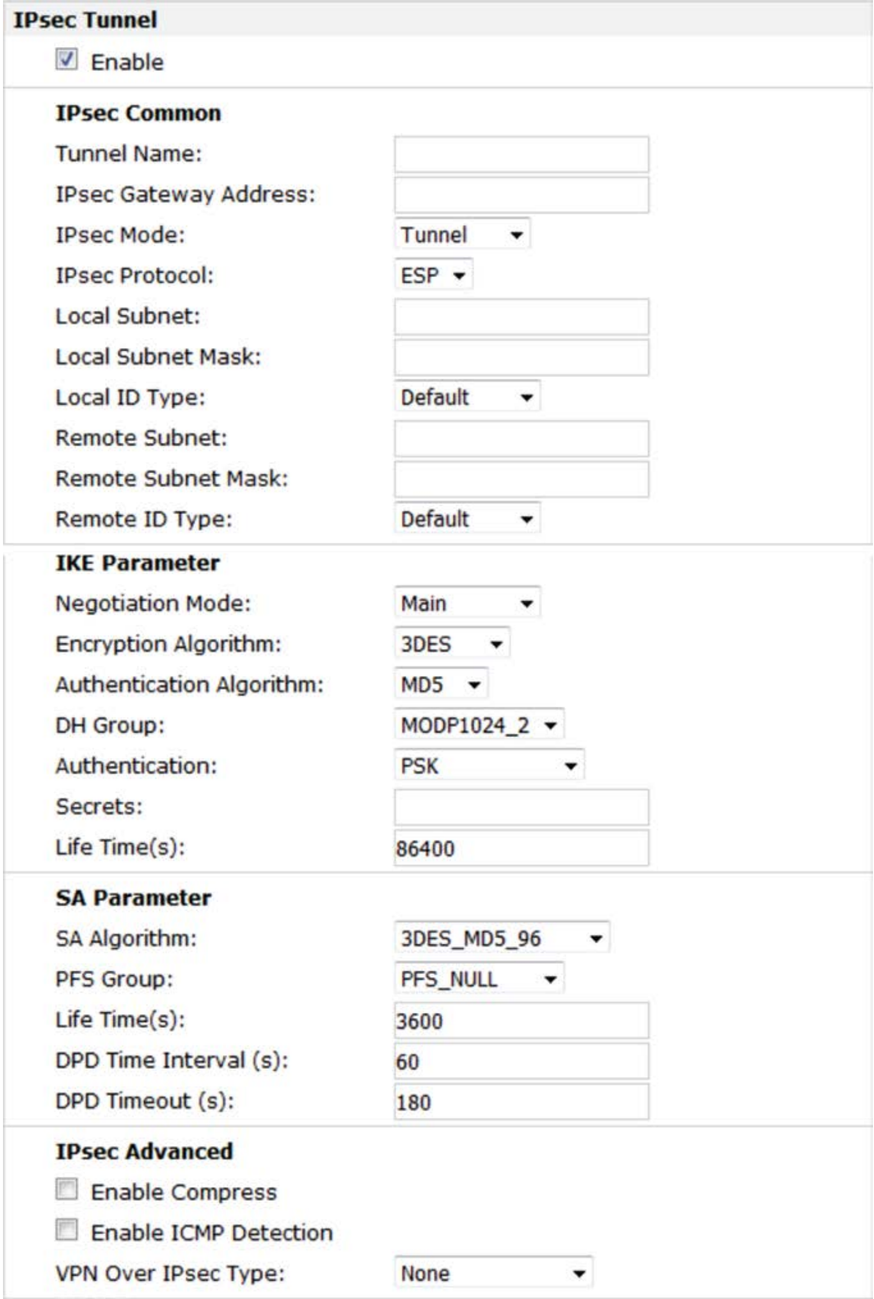
Configuration--->IPSec--->IPSec Tunnel



IPsec Tunnel

Tunnel Name	Description

Tick “Enable IPSec Tunnel1”



IPsec Tunnel

☑ Enable

IPsec Common

Tunnel Name:	
IPsec Gateway Address:	
IPsec Mode:	Tunnel
IPsec Protocol:	ESP
Local Subnet:	
Local Subnet Mask:	
Local ID Type:	Default
Remote Subnet:	
Remote Subnet Mask:	
Remote ID Type:	Default

IKE Parameter

Negotiation Mode:	Main
Encryption Algorithm:	3DES
Authentication Algorithm:	MD5
DH Group:	MODP1024_2
Authentication:	PSK
Secrets:	
Life Time(s):	86400

SA Parameter

SA Algorithm:	3DES_MD5_96
PFS Group:	PFS_NULL
Life Time(s):	3600
DPD Time Interval (s):	60
DPD Timeout (s):	180

IPsec Advanced

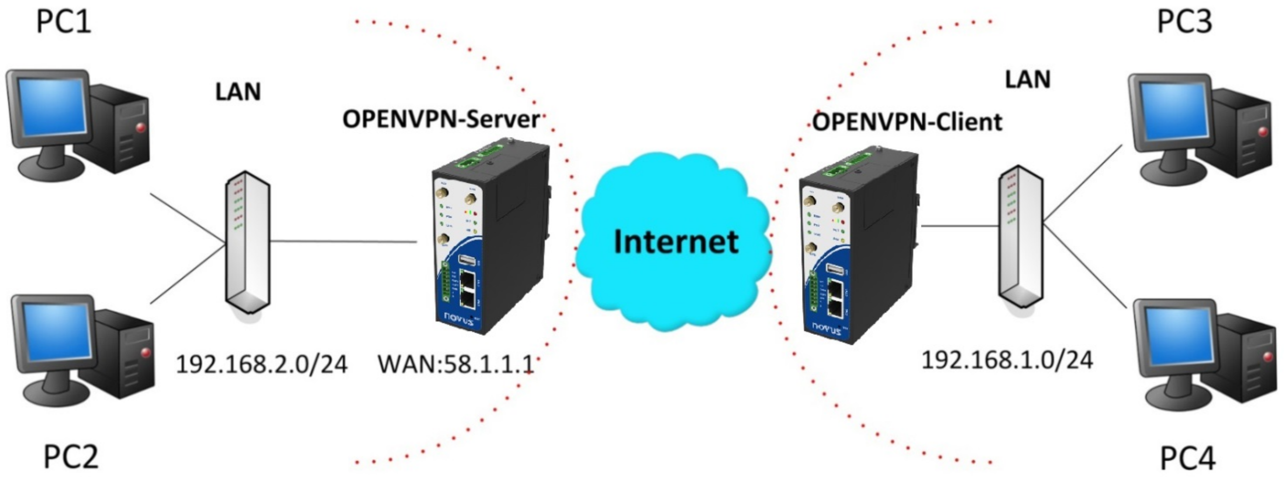
□ Enable Compress

□ Enable ICMP Detection

VPN Over IPsec Type:	None

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

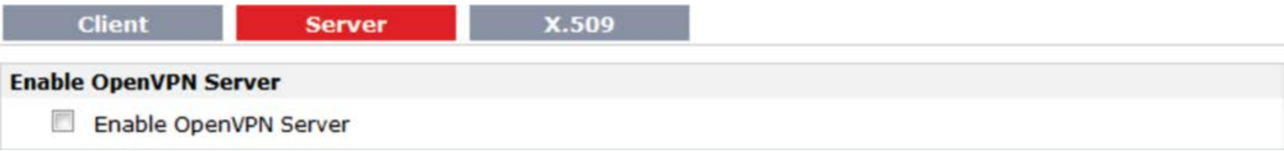
4.3.5 OPENVPN



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:

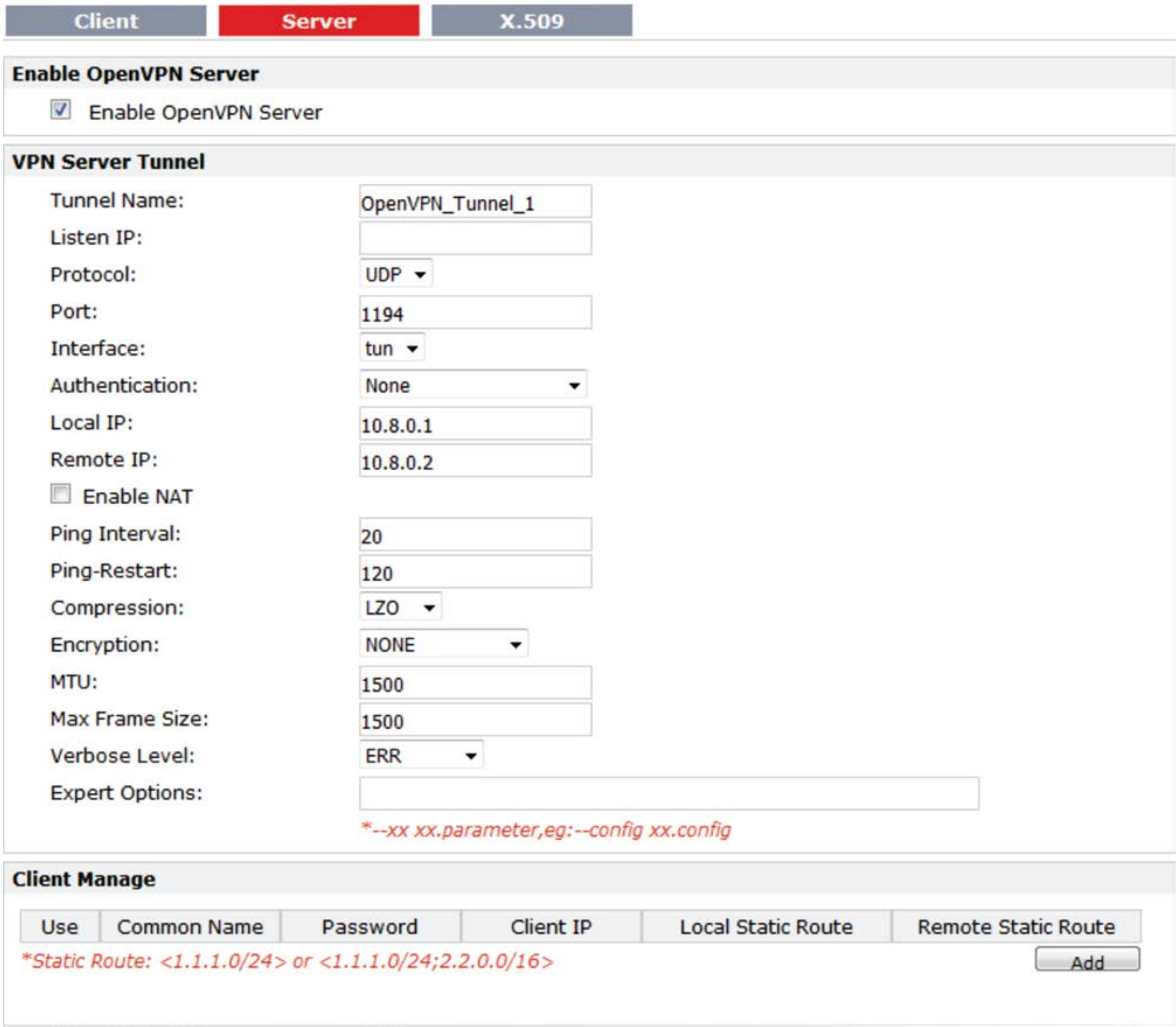
Configuration--->OpenVPN--->Server



Enable OpenVPN Server

□ Enable OpenVPN Server

Tick “Enable OpenVPN Server”.



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:	LZO
Encryption:	NONE
MTU:	1500
Max Frame Size:	1500
Verbose Level:	ERR
Expert Options:	

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

Client Manage

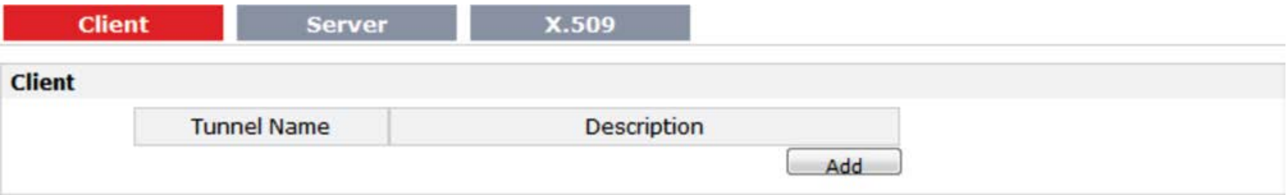
Use	Common Name	Password	Client IP	Local Static Route	Remote Static Route

*Static Route: <1.1.1.0/24> or <1.1.1.0/24;2.2.0.0/16>

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

OPENVPN_CLIENT:

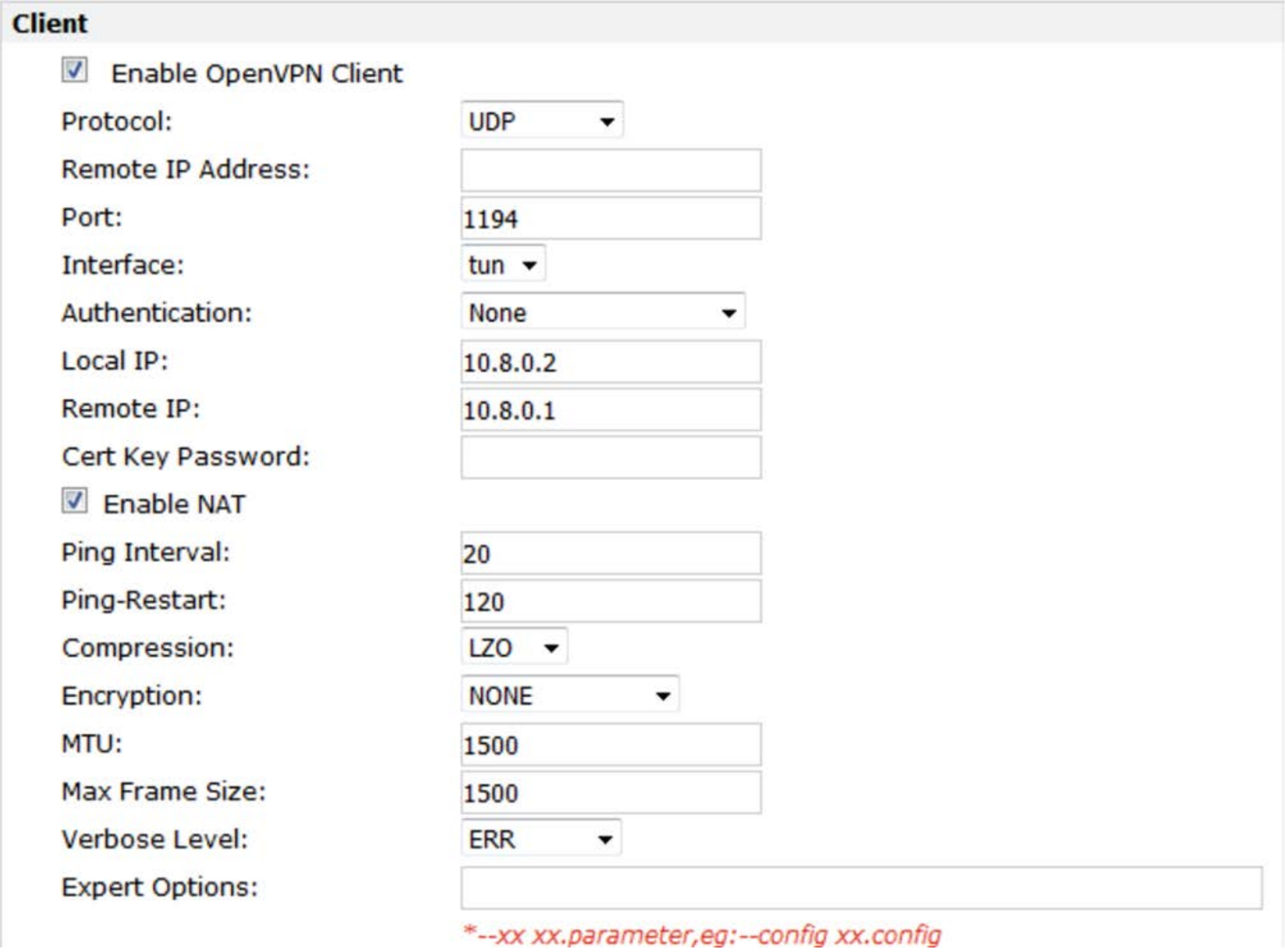
Configuration--->OpenVPN--->Client



Client

Tunnel Name	Description

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



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
Cert Key Password:	

☑ Enable NAT

Ping Interval:	20
Ping-Restart:	120
Compression:	LZO
Encryption:	NONE
MTU:	1500
Max Frame Size:	1500
Verbose Level:	ERR
Expert Options:	

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

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

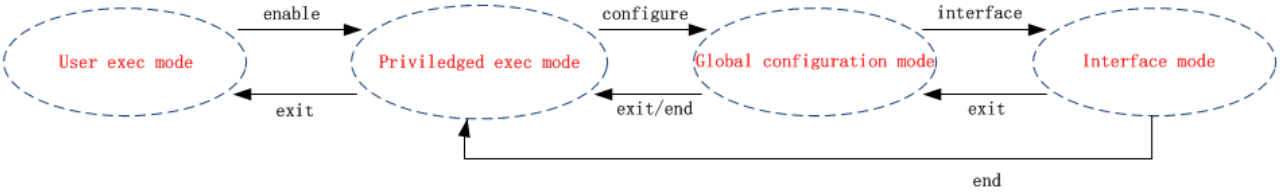
5. INTRODUCTIONS FOR CLI

5.1 WHAT'S CLI AND HIERARCHY LEVEL MODE

The AIRGATE-3G 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:

```
AIRGATE-3G Configure Environment
Username: admin
Password: *****
AIRGATE-3G> ?               //check what commands can be used in user exec mode
  enable                     Turn on privileged commands
  exit                    Exit from current mode
  ping                       Ping test
  reload                    Halt and perform a cold restart
  tracert                    Tracert test
  show                      Show running system information
```

PRIVILEDGED EXEC MODE:

```
AIRGATE-3G> enable
Password: *****
AIRGATE-3G# ?                   //check what commands can be used in Privileged exec mode
  debug                     Debug configure information
  enable                   Turn on privileged commands
  exit                      Exit from current mode
  export                     Export file using tftp
  syslog                    Export system log
  import                   Import file using tftp
  load                     Load configure information
  ping                     Ping test
  reload                    Halt and perform a cold restart
  tracert                  Tracert test
  write                    Write running configuration
  tftp                    Copy from tftp: file system
  show                    Show running system information
  configure               Enter configuration mode
  end                     Exit to Normal mode
```

GLOBAL CONFIGURATION MODE:

```
AIRGATE-3G# configure
AIRGATE-3G(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:

```
AIRGATE-3G(config)# interface Ethernet 0
AIRGATE-3G(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.*

QUICKSTART WITH CONFIGURATION EXAMPLES

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

Example 1: Show current version

```
AIRGATE-3G> show version
  software version : 1.01.00
  kernel version     : v2.6.39
  hardware version : 1.01.00
```

Example 2: Update firmware via tftp

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

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

Example 3: Set link-management

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

this parameter will be take effect when reboot!
really want to modify[yes]:
AIRGATE-3G# write                                             //save current configuration
Building configuration...
OK
AIRGATE-3G# reload
!Reboot the system ?'yes'or 'no':yes                   //reload to take effect
```

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

```
AIRGATE-3G> enable
Password: *****
AIRGATE-3G#
AIRGATE-3G# show link-management                         //show current link-management
**********************************************
```

```
    wan link                          : Eth0 Only                   // now “Eth0 Only” as wan-link
    ICMP primary server             : 8.8.8.8
    ICMP second server               : 8.8.8.4
    ICMP detection interval      : 30 seconds
    ICMP detection timeout        : 3 seconds
    ICMP detection retries        : 3
    reset the interface              : no
*********************************************

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

this parameter will be take effect when reboot!
really want to modify[yes]:
AIRGATE-3G (config) # end
AIRGATE-3G# write                                                           //save current configuration
Building configuration...
OK
AIRGATE-3G # reload
! Reboot the system? 'yes' or 'no': yes                         //reload to take effect
```

Example 5: CLI for Cellular dialup

```
AIRGATE-3G> enable
Password: *****
AIRGATE-3G#
AIRGATE-3G# show link-management

*********************************************
    wan link                          : Cellular        // now “Cellular ” as wan-link
    ICMP primary server             : 8.8.8.8
    ICMP second server               : 8.8.8.4
    ICMP detection interval      : 30 seconds
    ICMP detection timeout        : 3 seconds
    ICMP detection retries        : 3
    reset the interface              : no
```

```
********************************************
AIRGATE-3G (config) # set cellular
  1. set SIM_1 parameters
  2. set SIM_2 parameters
->please select mode (1-2)[1]:
SIM 1 parameters:
network provider
  1. Auto
  2. Custom
  3. china-mobile
->please select mode(1-3)[1]:
->dial out using numbers[*99***1#]:
->pin code[]:
connection Mode:
  1. Always online
  2. Connect on demand
->please select mode(1-2)[1]:
->redial interval(1-120)[30]:
->max connect try(1-60)[3]:
AIRGATE-3G(config)# end
AIRGATE-3G# write                                           //save current configuration
Building configuration...
OK

AIRGATE-3G# show      cellular
************************************************
    Cellular enable                  : yes
  1. show SIM_1 parameters
  2. show SIM_2 parameters
->please select mode(1-2)[1]:
SIM 1 parameters:
    network provider                 : Auto
    dial numbers                     : *99***1#
    pin code                         : NULL
    connection Mode                  : Always online
    redial interval                  : 30 seconds
    max connect try                  : 3
    main SIM select                  : SIM_1
    when connect fail                : yes
    when roaming is detected         : no
    month date limitation            : no
    SIM phone number                 :
    network select Type              : Auto
    authentication type              : AUTO
    mtu value                        : 1500
    mru value                        : 1500
    asyncmap value                   : 0xffffffff
    use peer DNS                   : yes
    primary DNS                    : 0.0.0.0
    secondary DNS                  : 0.0.0.0
    address/control compression: yes
    protocol field compression: yes
    expert options                 : noccp nobsdcomp
**************************************************
AIRGATE-3G# reload
!Reboot the system ?'yes'or 'no':yes                //reload to take effect
```

5.3 COMMANDS REFERENCE

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

6. WARRANTY

Warranty conditions are available on our web site www.novusautomation.com/warranty.