Dual SIM Industrial 4G VPN Router with Wi-Fi

for 4G LTE/ HSPA/UMTS/EDGE/GPRS Networks

8E4589 _ 4G Industrial VPN

User's Guide
rev. 1.0 04/2016

digicom

PREFACE

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

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

ENVIRONMENTAL CONDITIONS

Environment temperature: from -20° C to +65°C Relative humidity: from 5% to 95% RH

CLEANING INFORMATION

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

SHOCKS OR VIBRATIONS

Caution against shocks or vibrations.

DECLARATION CE of CONFORMITY

We, Digicom S.p.A. registered office at: Via Volta 39 – 21010 Cardano al Campo (Varese – Italy) declare under our sole responsability that the product with name **4G Industrial VPN** Type: Dual SIM Industrial 4G VPN Router with Wi-Fi, Category: Device for the Information Technology satisfies the basic requirement of the below indicated Directive:

- 1999/5/EC 9th March 1999, R&TTE (concerning radio equipment and telecommunication terminal equipment and the acknowledgment of their conformity) Law Decree 9th May 2001, n.269, (G.U. n. 156 of 7-7-2001).

As indicated in conformity with the requirements of following Reference Standards or of other regulations documents:

EN 301 489-1 EN 301 489-7 EN 301 489-17 EN 301 489-24 EN 300 328
EN 62311 EN 301 511 EN 301 908-1 EN 301 908-2
EN 60950-1 +A11 +A1 +A12 +A2

CE

Assistance and Contacts

Most of questions can be answered by looking up in the Support > F.A.Q. section of our website at www.digicom.it.
If you can't find the answer you're looking for, please contact our Technical Support at **support@digicom.it**

I**NFORMATION TO USERS**

according to Art. 26 **"Information to Users" - Legislative Decree 14 March 2014, n. 49 "Actuation of the Directive 2012/19/UE on the waste of electrical and electronic devices (RAEE)."**

The symbol of a crossed waste container marked on the apparatus or on its package indicates that at the end of its useful life the product must be collected separately from other waste materials.

The user must therefore take the apparatus which has reached the end of its useful life to appropriate separate collection centres for electronic and electro-technical waste materials, or deliver it back to the reseller when purchasing a new apparatus of an equivalent type for a domestic unit, giving one piece in for one piece out, according to Art. 11, paragraph 3 of the above mentioned Legislative Decree.

Furthermore, as per Art.11, paragraph 3 of the above mentioned Legislative Decree it is possible, in the sale point, the free insertion of recyclable materials into appropriate receptacle, without any purchasing obligation for the very small size RAEE, coming from domestic units.

Suitable separate waste collection for then sending the cast-off apparatus for recycling, treatment and environmentally friendly disposal, contributes towards preventing any possible negative effects on the environment and on health and encourages recycling of the materials the apparatus is made up of.

Unauthorised disposal of the product by the user will lead to payment of the administrative sanctions in force in the country where it is put on the market.

SAFETY WARNINGS

Read these instructions and norms carefully before powering the device. Violation of such norms may be illegal and cause hazard situations. For any of the described situations please refer to the specific instructions and norms.
The device is a low power radio transmitter and receiver. When it is ON, it sends and receives radio frequency (RF) signals.
The device produces magnetic fields. Do not place it next to magnetic supports such as floppy disks, tapes, etc.
Operating your device close to other electrical and electronic equipment - such as a television, phone, radio or a personal computer - may cause interferences.

INTERFERENCES

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

ROAD SAFETY

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

AIRCRAFT SAFETY

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

HOSPITAL SAFETY

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

EXPLOSIVE MATERIALS

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

INSTRUCTIONS FOR USE

Do not use the device in direct contact with the human body and do not touch the antenna if not strictly necessary.
Use approved accessories only. Consult documentation regarding any possible device connected to the device. Do not connect incompatible products.

Contents

Chapter 1 Product Concept

1.1 Overview

Digicom 4G INDUSTRIAL VPN is an enterprise-class cellular router offering state-of-the-art mobile connectivity for machine to machine (M2M) applications.

- Dual SIM redundancy for continuous cellular connections; it supports 2G/3G/4G.
- Various interfaces: 2xLAN/ 1xLAN, 1xWAN.
- WAN: static, PPPOE and DHCP client.
- Multiple links backup and ICMP detection.
- VPN tunnel: IPSec/ OpenVPN/GRE.
- Auto reboot via SMS/ Timing.
- Flexible Management methods: Web/SMS/CLI.
- Firmware upgrade via Web/CLI/SMS.
- Advanced Firewall: filtering, port mapping, DMZ.
- Support DDNS.
- Support VRRP.
- Wide range input voltages from 9 to 26 VDC.
- The metal case can be mounted on a DIN-rail, on the wall or it can be put on desktop.
- Built-in Watchdog, Timer

1.2 Package content

The package contains the following items:

- Digicom 4G Industrial VPN Router
- 1 3-pin pluggable terminal block for power connector
- 1 Ethernet cable
- 1 35mm Din-Rail mounting kit
- 1 AC/DC Power Supply Adapter (12VDC, 1A)
- 1 4G/3G/2G omnidirectional antenna (3m. cable)
- 2 Wi-Fi omnidirectional antenna

1.3 Specifications

Cellular Interface

- Standards: GSM/GPRS/EDGE/UMTS/HSPA+/FDD LTE
- FDD LTE: max. 150/50 Mbps (DL/UL)
- TDD LTE: max.112/10 Mbps (DL/UL)
- DC-HSPA+: 42/5.76 Mbps (DL/UL)
- HSPA+: max. 21.6/5.76 Mbps (DL/UL)
- EDGE: 236.8 kbps (DL/UL)
- GPRS: 85.6 kbps (DL/UL)
- SIM: 2 x (3V & 1.8V)
- Antenna Interface: SMA Female (1xMAIN and 1xAUX)

Ethernet Interface

- Number of Ports: 2 x LAN or 1 x LAN, 1xWAN (10/100Mbps)
- Isolation Protection: 1.5KV

WLAN Interface (Optional)

- Standards: 802.11b/g/n, support AP and Client mode
- Data speed: 2*2 MIMO, 300Mbps
- Frequency Band: 2.412 - 2.485 GHz
- Security: WEP, WPA, WPA2
- Encryption: 64/128 AES, TKIP
- Antenna Interface: RP-SMA Female

System

- Reset button
- LED Indicators: RUN, PPP, USR, 3 x RSSI

CPU & Memory

- CPU: 535MHz
- SDRAM: 64MB

- FLASH: 16MB

Software

- Network protocols: PPP, TCP, UDP, DHCP, ICMP, NAT, DMZ, DDNS, VRRP, HTTP, HTTPs, DNS, ARP, SNTP, Telnet, etc.
- VPN tunnel: IPSec/OpenVPN/GRE
- Firewall: SPI, anti-DoS, Filter, Access Control
- Management: Web, SMS

Power Supply and Consumption

- Power Supply Interface: 3.5mm terminal block
- Input Voltage: 9 to 26 VDC
- Power Consumption: Idle: 100 mA @ 12 V

  Data Link: 500 mA (peak) @ 12 V

Mechanical Characteristics

- Housing & Weight: Metal, 300g
- Dimension: (L x W x H): 127.5mm x 82.5mm x 29.5mm
- Installation: 35mm Din-Rail or wall mounting or desktop

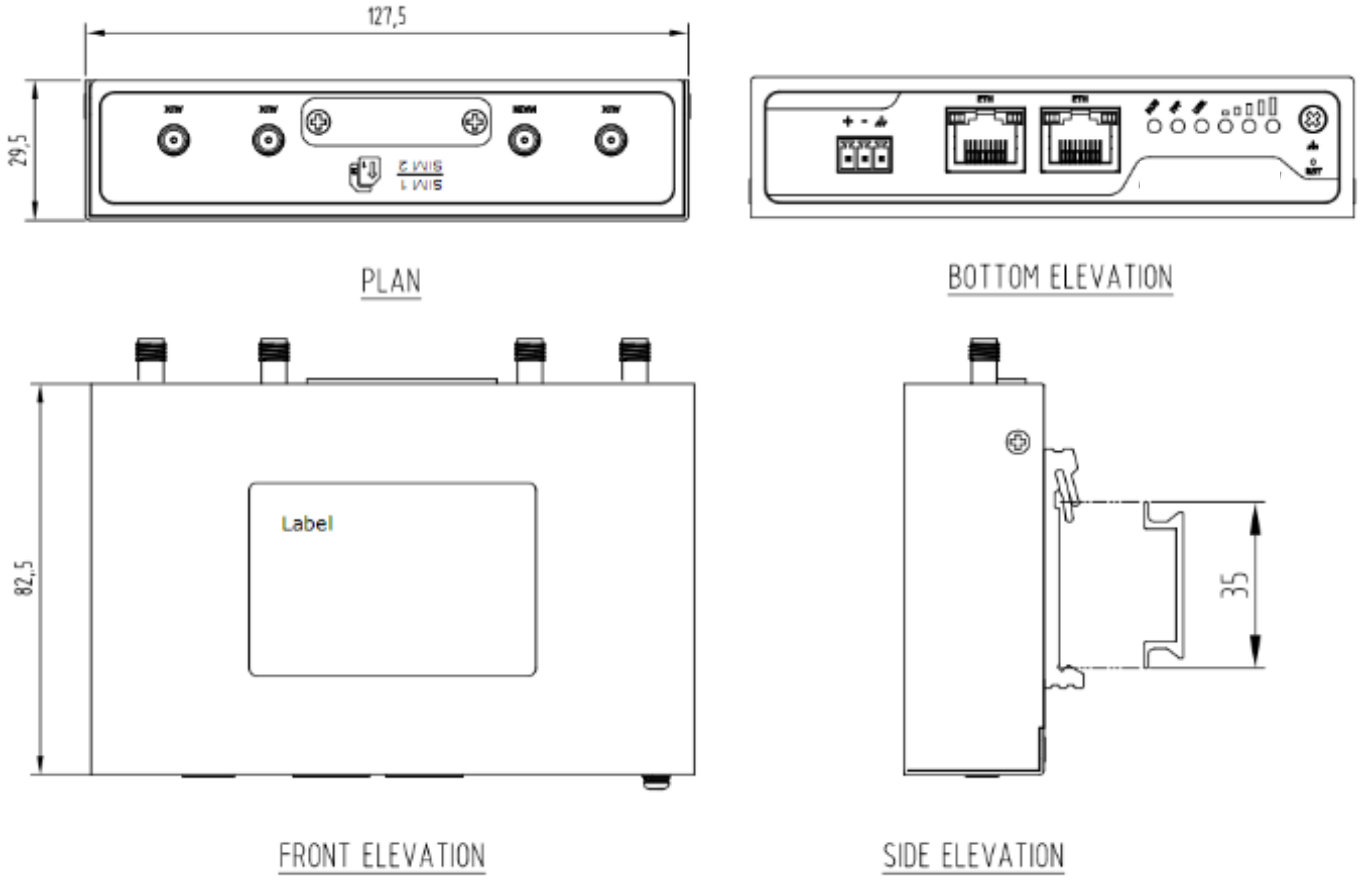
Regulatory and Type Approvals

- Approval & Detective: CE, R&TTE, RoHS, WEEE
- EMI : EN 55022 (2006/A1: 2007) Class B
- EMC: EN 61000-4-2 (ESD) Level 3, EN 61000-4-3 (RS) Level 4

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

  EN 61000-4-6 (CS) Level 3, EN 61000-4-8 Level 4

1.4 Dimensions



1.5 Selection and Ordering Data

Model No.	Frequency band	Operating Environment
4G INDUSTRIAL VPN-4L	LTE FDD: B1, B2, B3, B4, B5, B7, B8, B20 LTE TDD: B38, B39, B40, B41 UMTS/DC-HSPA+/HSPA+/HSPA: 2100/1900/850/900/1800 MHz GSM/GPRS/EDGE: 850/900/1800/1900 MHz	-20 to +65°C/ 5 to 95% RH

Chapter 2 Installation

2.1 Overview

As shown in the following pictures, 4G INDUSTRIAL VPN router has 6 Leds, the Reset button, 2 Ethernet ports on the front panel, and the 2 Sim holder, the antennas on the rear panel.

2.2 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	Blinking	SIM: using backup SIM card. NET: register to a low level network.
		Off after blinking	SIM: working fine. NET: working fine.
		Light up	OpenVPN: OpenVPN is connected. IPSec: IPSec is connected. GRE: GRE is connected.
		Off after lighting up	OpenVPN: OpenVPN is disconnected. IPSec: IPSec is disconnected. GRE: GRE is disconnected.
	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).
	When the network is disconnected, those three signal LEDs are designed as a binary combination code to indicate a series of error report. (Green Yellow Red) On: 1 Off: 0 001 AT command failed 010 no SIM card detected 011 requires PIN code 100 requires PUK code 101 registration failed 110 something wrong happened in the module		

***Note**: The user can select display status of USR LED. For details please refer to 3.20 Service->Advanced section.*

2.3 Reset Button

Function	Operation
Reboot	Push the button for 2~7 seconds under working status.
Restore to factory default setting	Please keep pressing the "RST" button once power on the router, until LED lights blink one by one circularly. When the six LED lights start blinking one by one, please release the pressing operation within 5 seconds. In this time the router loads default successfully

2.4 Ethernet Port

There are two Ethernet ports in 4G INDUSTRIAL VPN router, ETH1 is the LAN interface and ETH0 can be the LAN or WAN interface. The Eth0 factory default is as LAN interface. Each Ethernet port has two LED indicators. The yellow one is **Link indicator** and the green is not connected. There are three status of Link indicator. Please refer to the table below.

Indicator	Status	Description
Link Indicator	Off	Connection is down.
	On	Connection is up.
	Blink	Data is being transmitted

2.5 Install SIM Card

- **Remove slot cover**

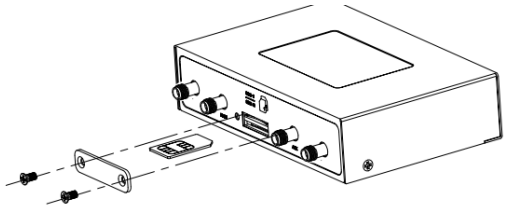
1. Make sure power supply is disconnected.
2. Use a screwdriver to remove the screw on the cover, and then remove the cover, you will find the SIM Card slots.

- **Inserting SIM Card**

3. Insert the SIM card. Press the card with your fingers until you hear “a click sound”. Then use a screwdriver to screw the cover.

- **Removing SIM Card**

4. Make sure router is powered off.
5. Press the card until you hear “a click sound” till the card will pop up to be pulled out.



***Notes*:**

1. *Please use the specific M2M SIM card when the device works under extreme temperature conditions (temperature exceeding 0-40 C), because the long-time working of regular SIM card in harsh environment (temperature exceeding 0-40 C) may increase the possibility of SIM card failure.*
2. *Don’t forget to 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 magnetic fields.*
5. *Make sure router is powered off before inserting or removing your SIM card.*

2.6 Connect the External Antenna

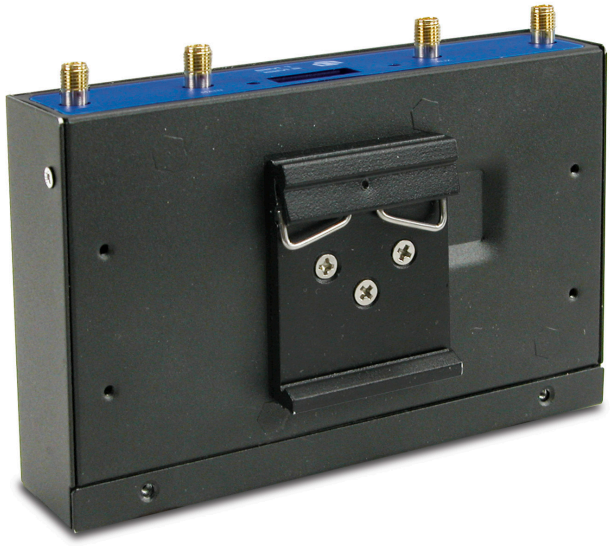
Connect the router to an external antenna connector. Make sure the antenna is within the correct frequency range and it is screwed tightly.

2.7 Ground the Router

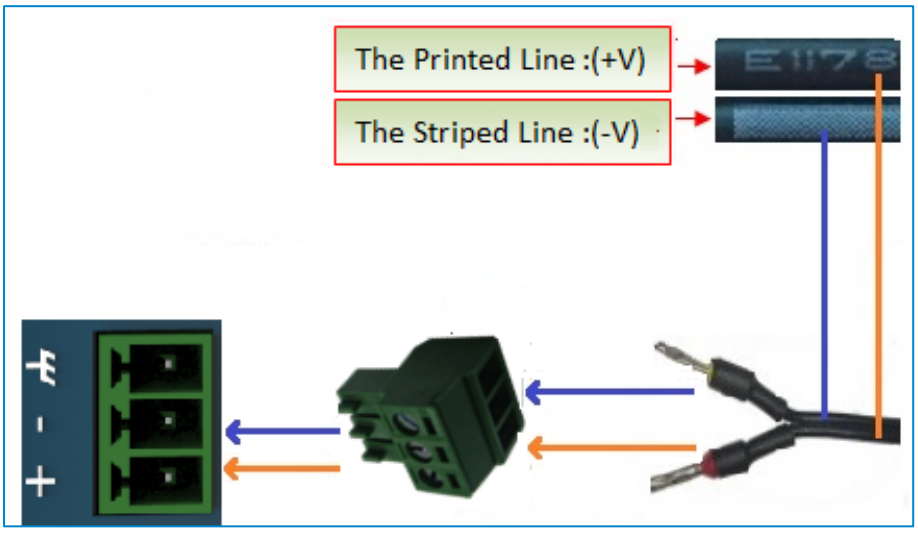
Grounding and wiring the router helps limiting the effects of noise due to electromagnetic interference (EMI). We suggest to connect the ground connector to a well-grounded mounting surface such as a metal panel.

2.8 Mount the Router

The router may be placed on a horizontal surface such as a desktop, mounted on a DIN-rail.



2.9 Power Supply



The power supply range is 9 to 26 VDC.
***Note**: Please take care about the polarity, and do not make reverse connection.*

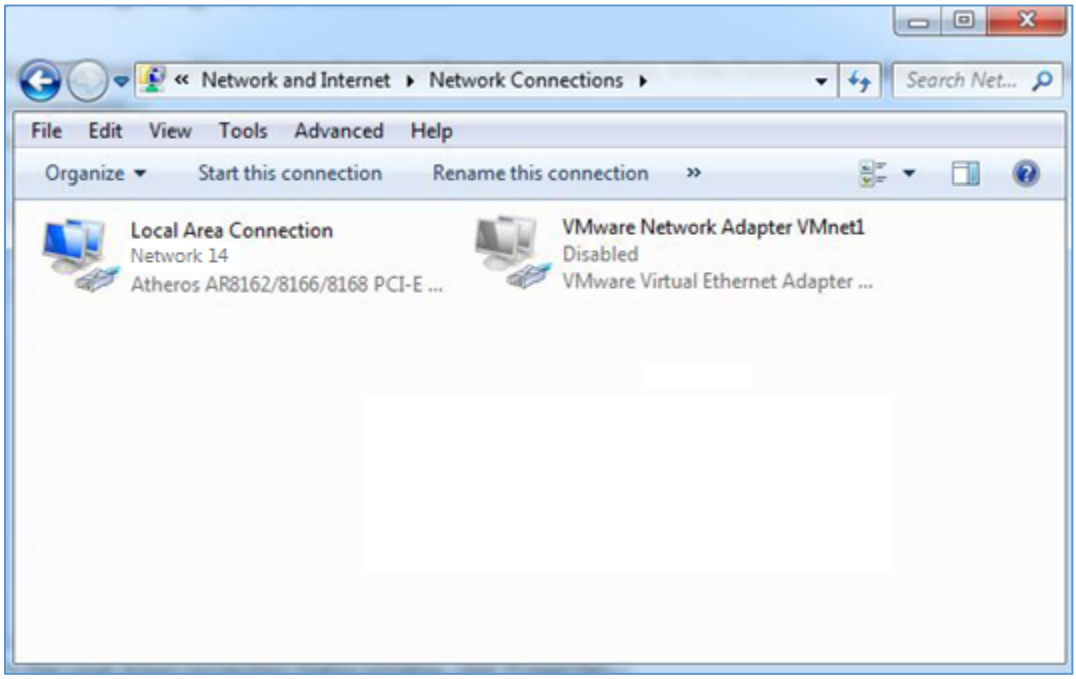
Chapter 3 Configure Settings over Web Browser

The router can be configured through your web browser that include IE 8.0 or above, Chrome and Firefox. A web browser is included as a standard application in the following operating systems: Linux, Mac OS, Windows 98/NT/2000/XP/Me/Vista/7/8, etc. It provides an easy and user-friendly interface for configuration.
There are various ways to connect the router, either through an external repeater/hub or connect directly to your PC. However, make sure that your PC has an Ethernet interface properly installed prior to connecting the router.
You must configure your PC to obtain an IP address through a DHCP server or a fixed IP address that must be in the same subnet as the router. If you encounter any problems accessing the router web interface it is advisable to uninstall your firewall program on your PC, as this tends to cause problems accessing the IP address of the router.

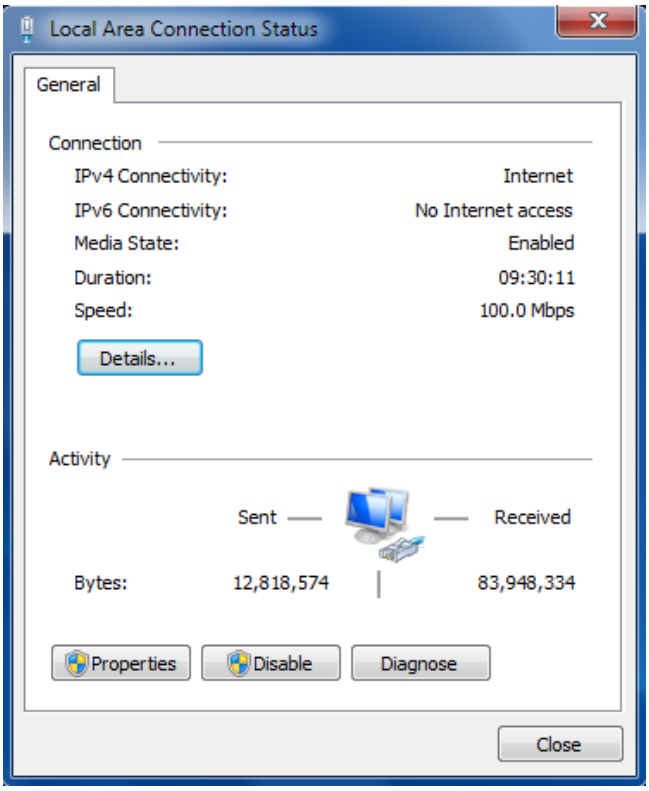
3.1 Configuring PC in Windows 7

There are two methods to obtain IP address for the PC, one is automatically obtain IP address from DHCP server, and another is manually configured static IP address within the same subnet of 4G INDUSTRIAL VPN router.

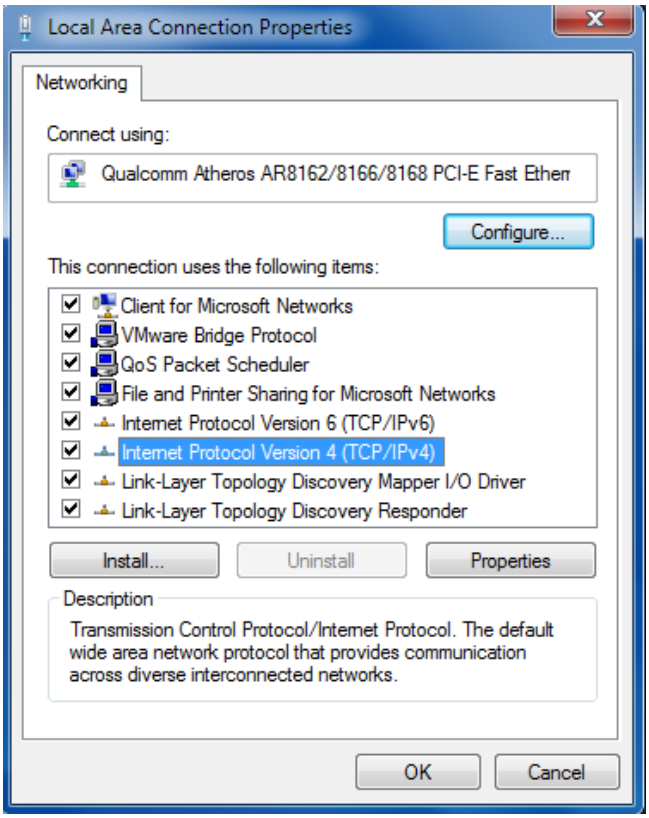
The configuration for windows system is similar.
1. Go to *Start* *Control Panel* *Network and Internet**Network Connections*. Double-click *Local Area Connection*.



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

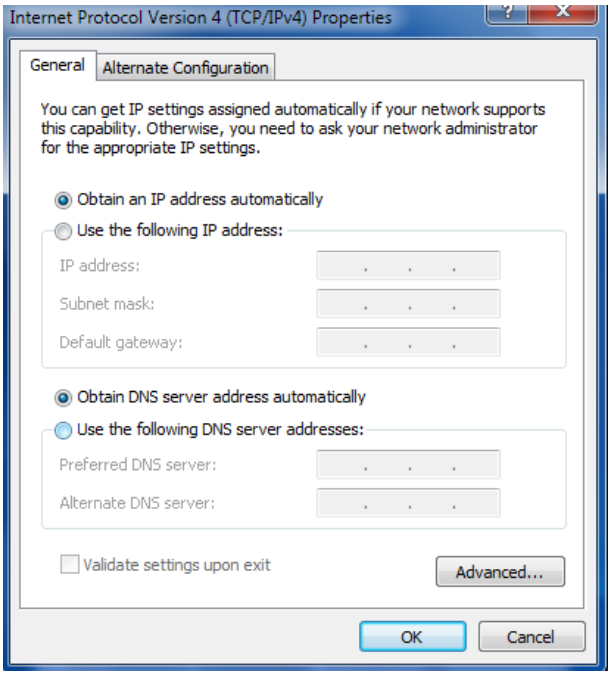


3. Select *Internet Protocol (TCP/IP)* and click *Properties*.

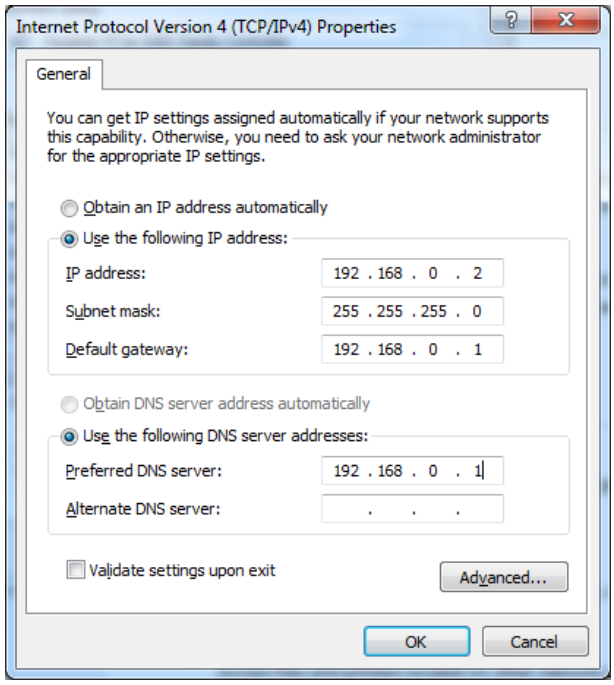


4. Configure the IP address of PC.

Automatically obtain IP address from DHCP server



Manually configured static IP address within the same subnet of 4G INDUSTRIAL VPN router



5. Click *OK* to finish the configuration.

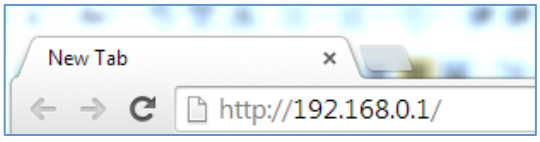
3.2 Factory Default Settings

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

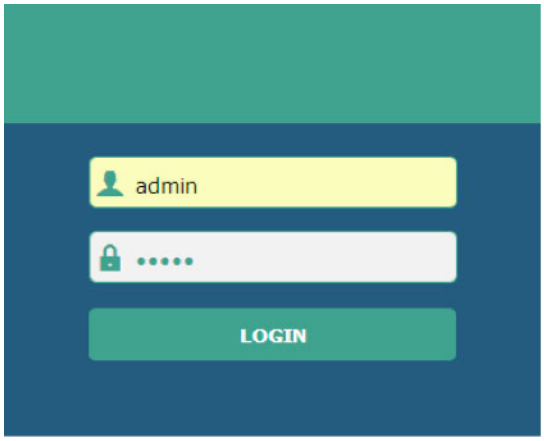
Item	Description
Username	admin
Password	admin
Eth0	192.168.0.1/255.255.255.0, LAN
Eth1	192.168.0.1/255.255.255.0, LAN
DHCP Server	Enabled

3.3 Login Router

1. On the PC, open a web browser such as Internet Explorer.
2. In the browser's address bar, enter the IP address of the Router. The default IP address is 192.168.0.1, though the actual address may vary.



3. Input the username and password and login the 4G INDUSTRIAL VPN. If enter the wrong username or password six times, the login web will be locked for 5 minutes.

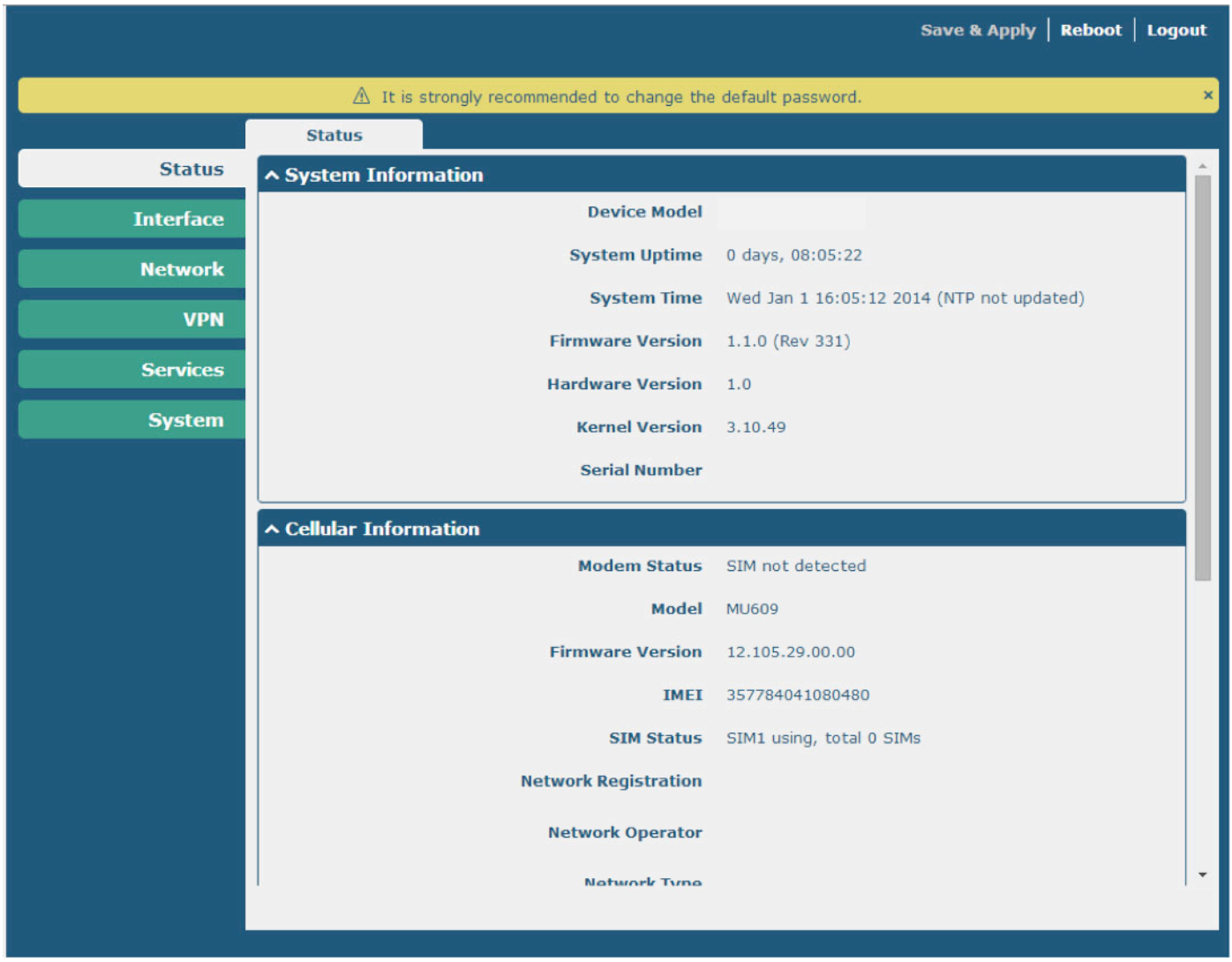


3.4 Control Panel

After logging in the 4G INDUSTRIAL VPN, the home page of the 4G INDUSTRIAL VPN router's web interface is displayed, just like the screenshot below.
This section allows users to save configuration, reboot router, logout. When you are first time to login 4G INDUSTRIAL VPN, there will be a pop-up tab " 

", click 

to close the pop-up tab. And if you want to change the password, please refer to **3.27 System -> User Management** section**.**



Control Panel		
Item	Description	Button
Save & Apply	Click to save the current configuration into router's flash and apply the modification on every configuration page, to make the modification taking effect.	Save & Apply
Reboot	Click to reboot the router. When the Reboot button is in yellow, it means that some completed configurations will take effect only by reboot.	Reboot
Logout	Click to exit safely, then it will switch to login page. Shut down web page directly without logout, the next one can login web on this browser without a password before timeout.	Logout
Submit	Click to submit the modification on current configuration page.	Submit
Cancel	Click to cancel the modification on current configuration page.	Cancel

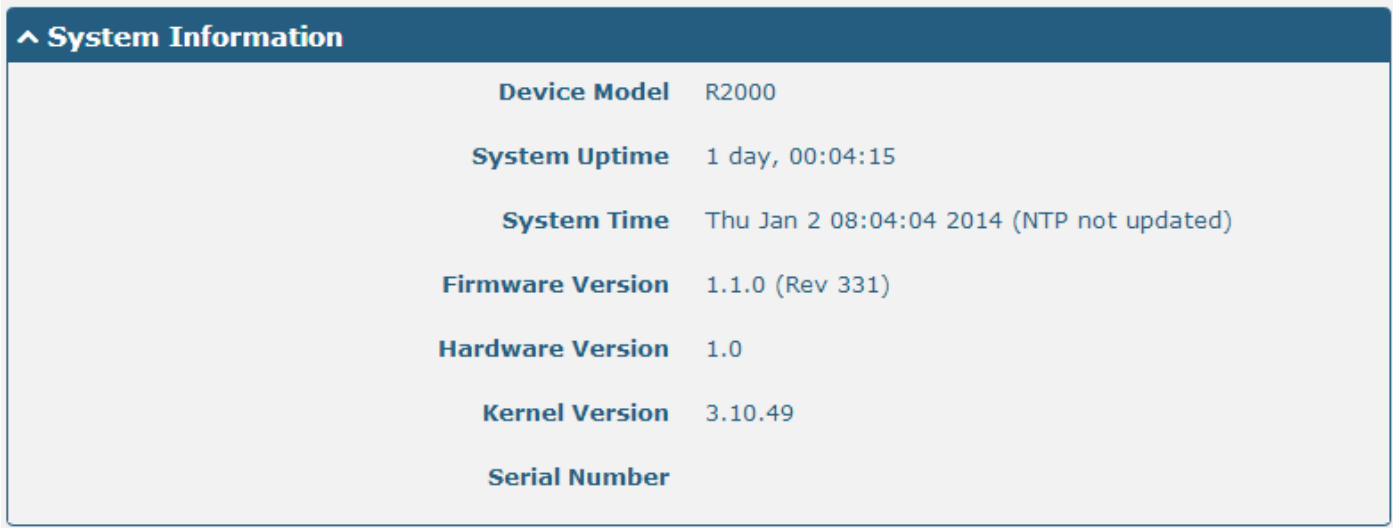
Note: *The steps of how to modify configuration are as bellow:*

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

3.5 Status

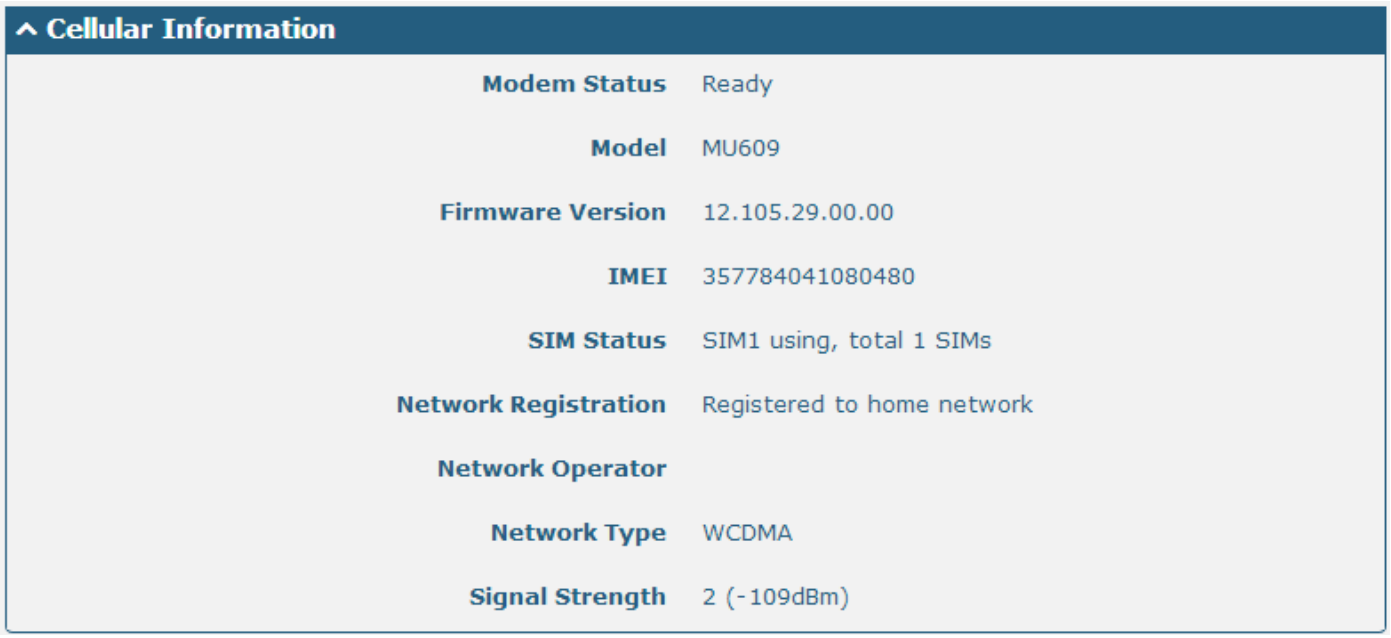
This section displays the router's status, which shows you a number of helpful information such as System Information, Cellular Information, WAN Status and LAN Status.

System Information



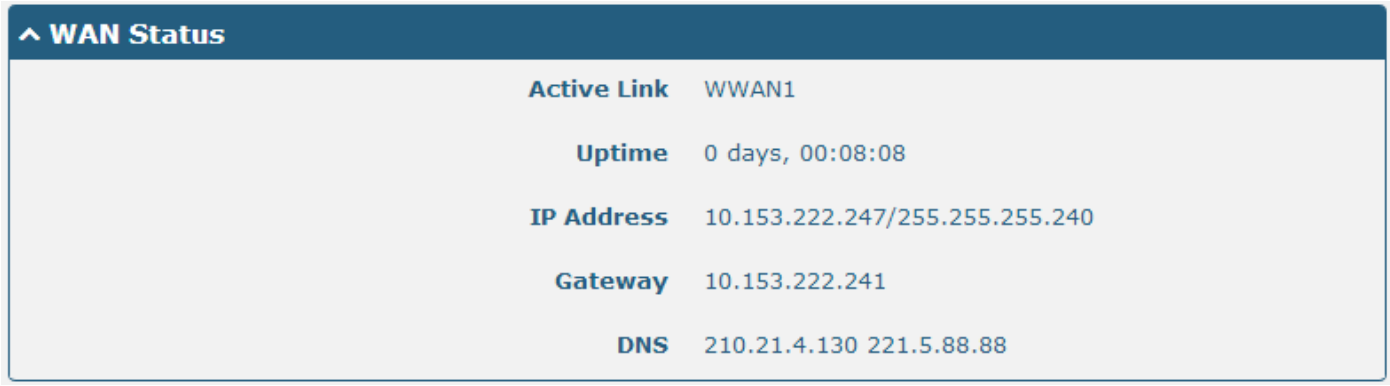
System Information	
Item	Description
Device Model	Show the model name of this device.
System Uptime	Show how long the router has been working since power on.
System Time	Show the current system time.
Firmware Version	Show the current firmware version.
Hardware Version	Show the current hardware version.
Kernel Version	Show the current kernel version.
Serial Number	Show the serial number of this device.

Cellular Information



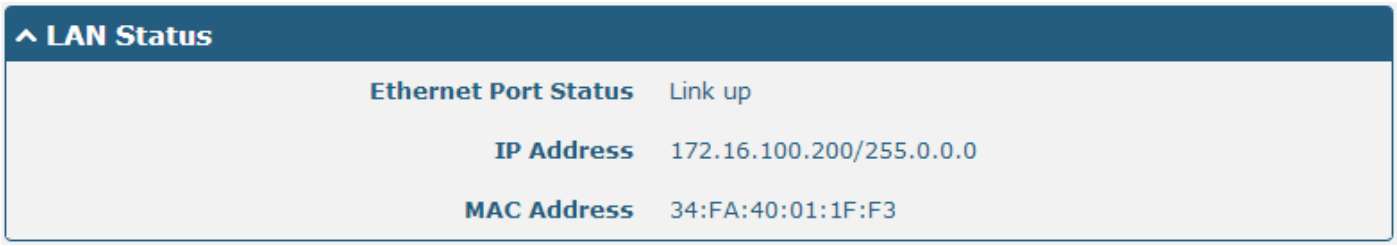
Cellular Information	
Item	Description
Modem Status	Show the status of modem. There are 8 different status: 1. Initializing 2. Modem not found 3. No response 4. SIM not detected 5. SIM PIN required 6. SIM PUK required 7. Register failed 8. Ready
Modem Model	Show the current radio module type.
Firmware Version	Show the current radio firmware version.
IMEI	Show the IMEI number of the radio module.
SIM Status	Show the SIM card which the router works with currently: SIM1 or SIM2. And show the total SIM cards in the router.
Network Registration	Show the status of Registration. There are 6 different status: 1. Not registered, search stopped 2. Registered to home network 3. Not registered, searching 4. Registration denied 5. Unknown 6. Registered, roaming
Network Provider	Show the current network provider.
Network Type	Show the current network service type, e.g. GPRS.
Signal Strength	Show the current signal strength.

WAN Status



WAN Status	
Item	Description
Active Link	Show the current WAN link: WWAN1, WWAN2 or WAN.
Uptime	Show how long the current WAN have been working.
IP Address	Show the current WAN IP address.
Gateway	Show the current gateway.
DNS	Show the current primary DNS server and Secondary server.

LAN Status



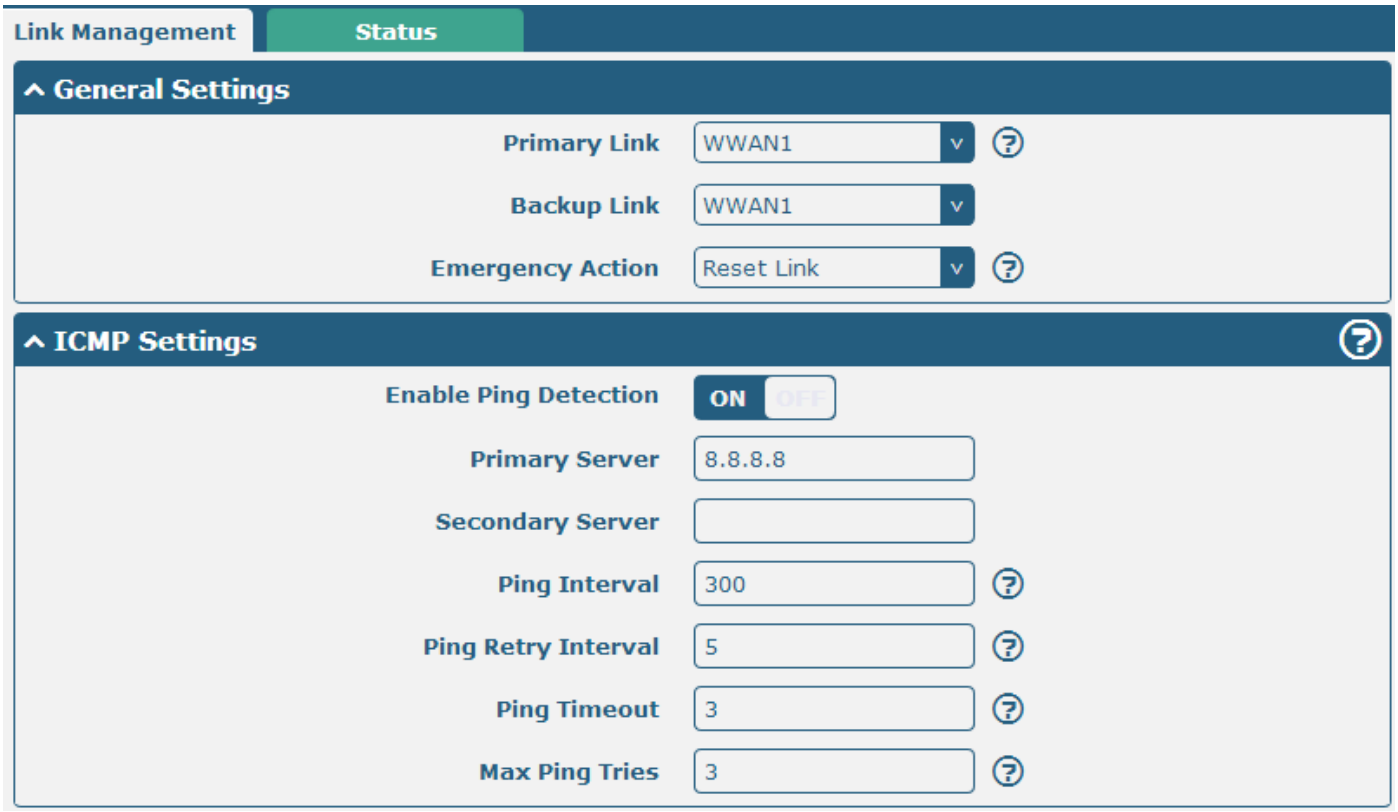
Router Information	
Item	Description
Ethernet Port Status	Show the current Ethernet port status.
IP Address	Show the current IP Address and the Netmask.
MAC Address	Show the current MAC Address.

3.6 Interface->Link Management

Link Management

It is recommended to enable ICMP detection to keep router always online.

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

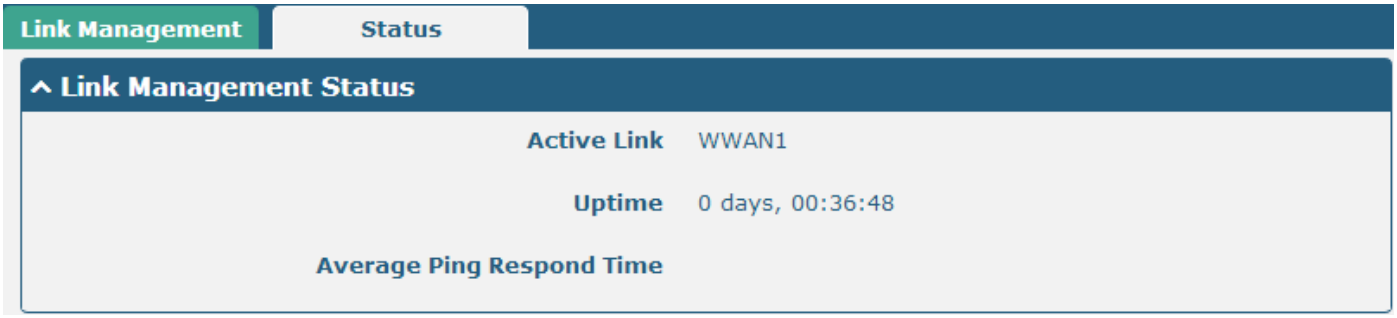


Link Management		
Item	Description	Default
Primary Link	Select from “WWAN1”, “WWAN2”, “WAN”. 1. WWAN1: Select to make SIM1 as the primary wireless WAN. ***Note:*** *When it is the first time to insert single SIM card, SIM card 1 and SIM card 2 slots are available. If the single card was inserted in SIM card 2 slot, and default primary link WWAN1 can be used for SIM2 in this situation.* 2. WWAN2: Select to make SIM2 as the primary wireless WAN. 3. WAN: Select to make WAN Ethernet port as the primary WAN.	WWAN1
Backup link	Select from “None”, “WWAN1”, “WWAN2”. 1. None: Do not select backup interface. 2. WWAN1: Select to make SIM1 as backup wireless WAN. 3. WWAN2: Select to make SIM2 as backup wireless WAN. 4. WAN: Select to make WAN Ethernet port as the backup WAN.	None
Emergency Action	Action to take if no link available. Select from “Redial only”, “Reset Link”, “Reboot System”.	Reset Link
Enable Ping Detection	To enable “ping detection”. It was a keep alive policy of 4G INDUSTRIAL VPN router.	OFF
Primary Server	Router will ping this primary address/domain name to check that if the current connectivity is active.	8.8.8.8
Secondary Server	Router will ping this secondary address/domain name to check that if the current connectivity is active.	Null
Ping Interval	Set the ping interval.	300

Ping Retry Interval	Set the ping retry interval.	5
Ping Timeout	Set the ping timeout.	3
Max Ping Tries	Switch to another link or take emergency action if max continuous ping tries reached.	3

Note: *Click"* *" for help.*

Status

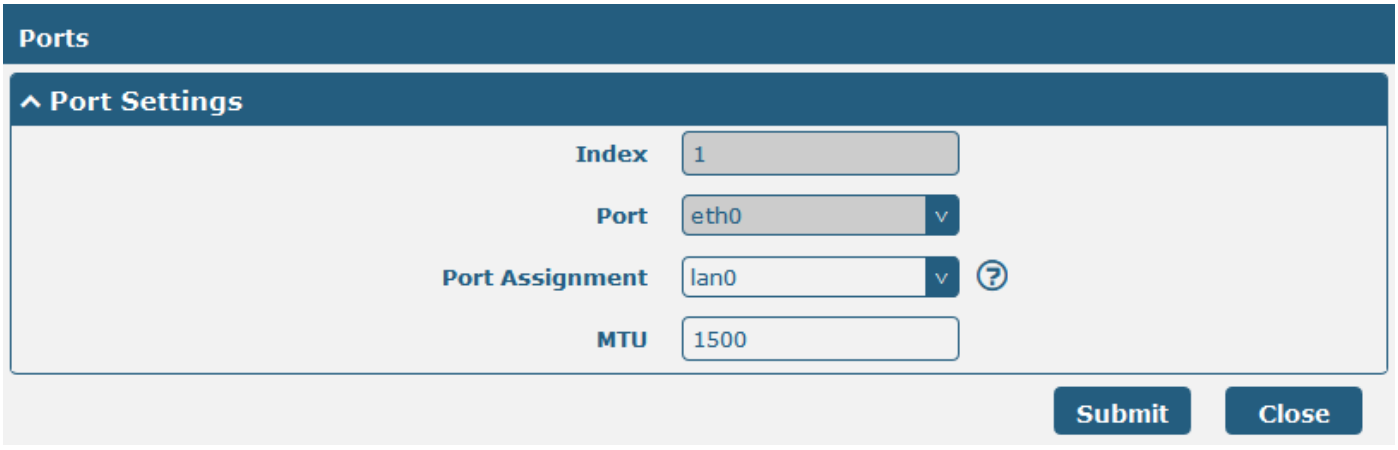


Status	
Item	Description
Active Link	Show the current active link.
Uptime	Show how long the current link has been active.
Average Ping Respond Time	Show the average ping respond time of the active link.

3.7 Interface->Ethernet

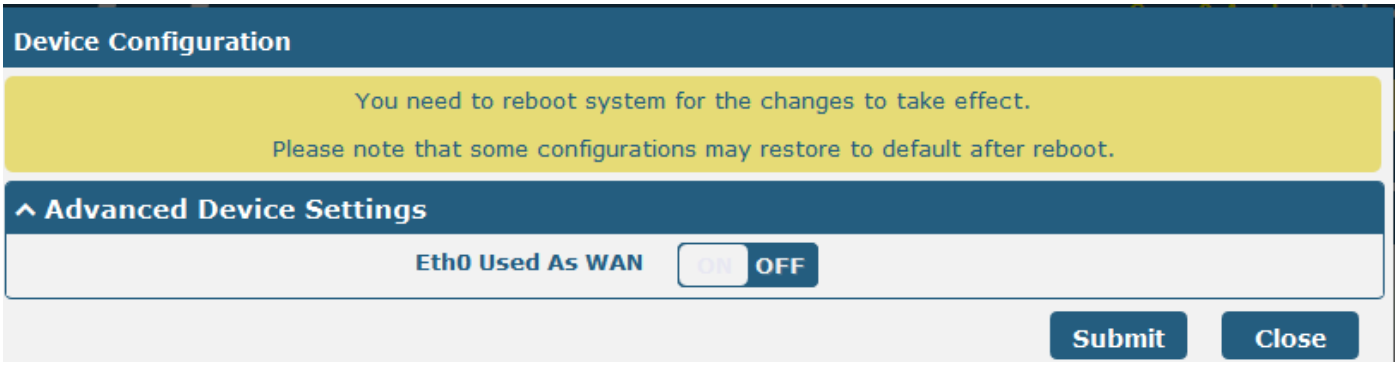
This section allow user to set the parameter of the Ethernet port. At least one port should be assigned to lan0.

Click button, configure the port setting.



Ethernet		
Item	Description	Default
Index	The index of Ethernet port, cannot edit.	1 or 2
Port	Eth1 or Eth2	
Port Assignment	Select from lan0 or lan1. lan0: configure lan0 in **Interface->LAN->IP Settings** section. lan1: configure lan1 in **Interface->LAN->Multiple IP** section. Click button, it will pop up the following window. Help: Close Only eth0 can be assigned as wan. To assign eth0 as wan, click here. Click "here", and configure Eth0 as WAN interface in the pop-up window. Then click Submit button, it will pop up the reboot confirm window. Click OK to reboot the router. Router Web Manager Operation successfully completed. Do you want to reboot immediately? OK Cancel	lan0
Eth0 Used As WAN	Switch button to ON to configure Eth0 as WAN interface. Switch button to OFF, it will disable the WAN interface, Eth0 will recovery to be LAN interface.	OFF
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1500

Enable or disable the WAN interface.

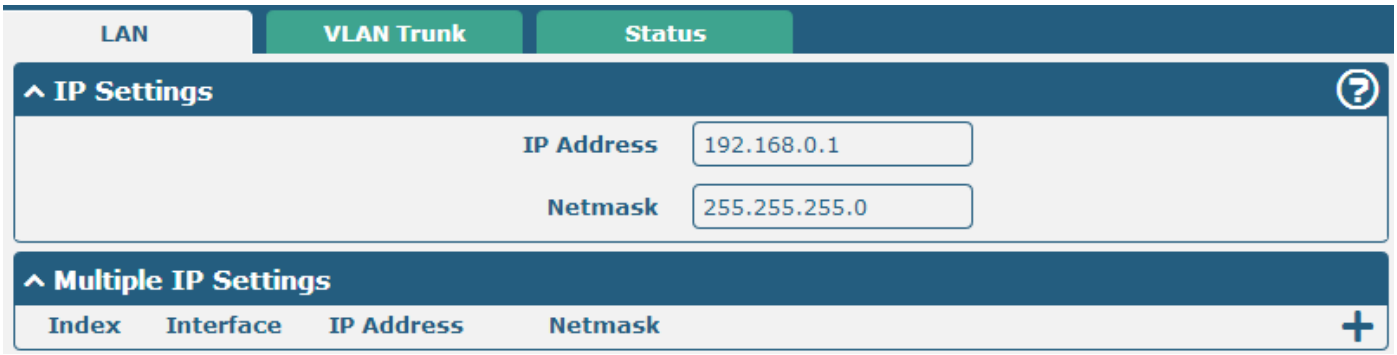


Advanced Device Settings		
Item	Description	Default
Eth0 Used As WAN	Switch button to ON to configure Eth0 as WAN interface. Switch button to OFF, it will disable the WAN interface, Eth0 will recovery to be LAN interface.	OFF

3.8 Interface->LAN

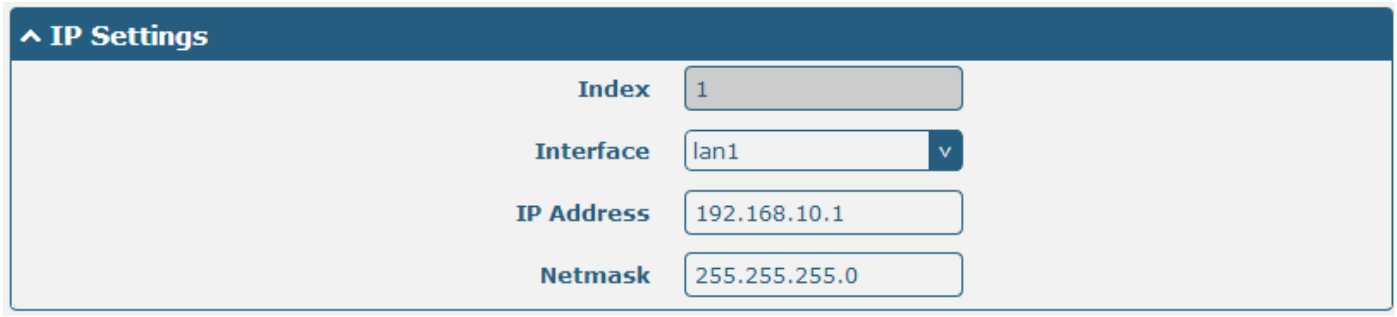
This section allows user to set the LAN and the related parameters.

LAN



IP Setting section is used to configure the IP of lan0.

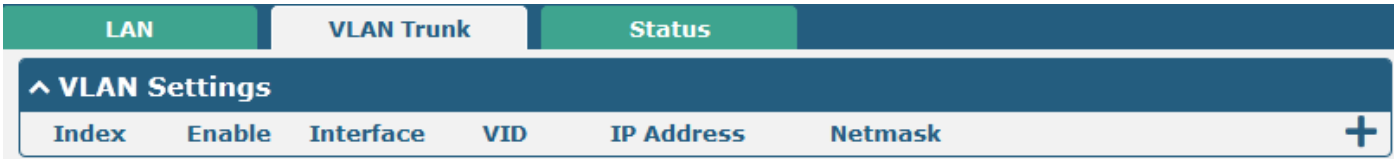
Click + to set the IP of lan1 or add multiple IP address for lan0 and lan1.



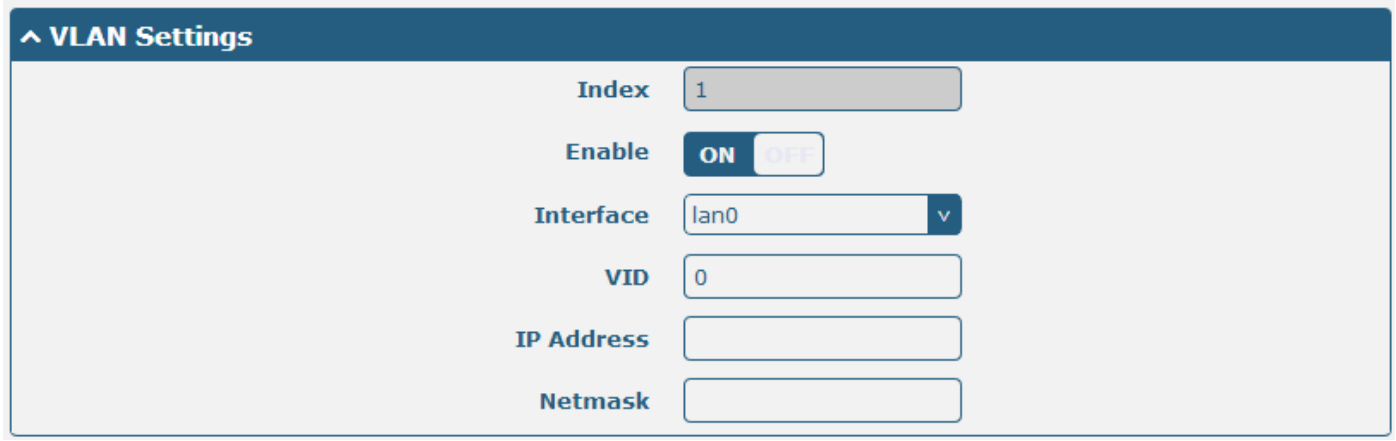
LAN		
Item	Description	Default
IP Address	Set the IP Address of the lan0 interface.	192.168.0.1

Netmask	Set the Netmask of the lan0 interface.	255.255.255.0
IP Address@ Multiple IP	Set the IP of lan1 or set the multiple IP Address of the LAN interface.	Null
IP Netmask@ Multiple IP	Set the Netmask of lan1 or set the multiple Netmask of the LAN interface.	Null

VLAN Trunk



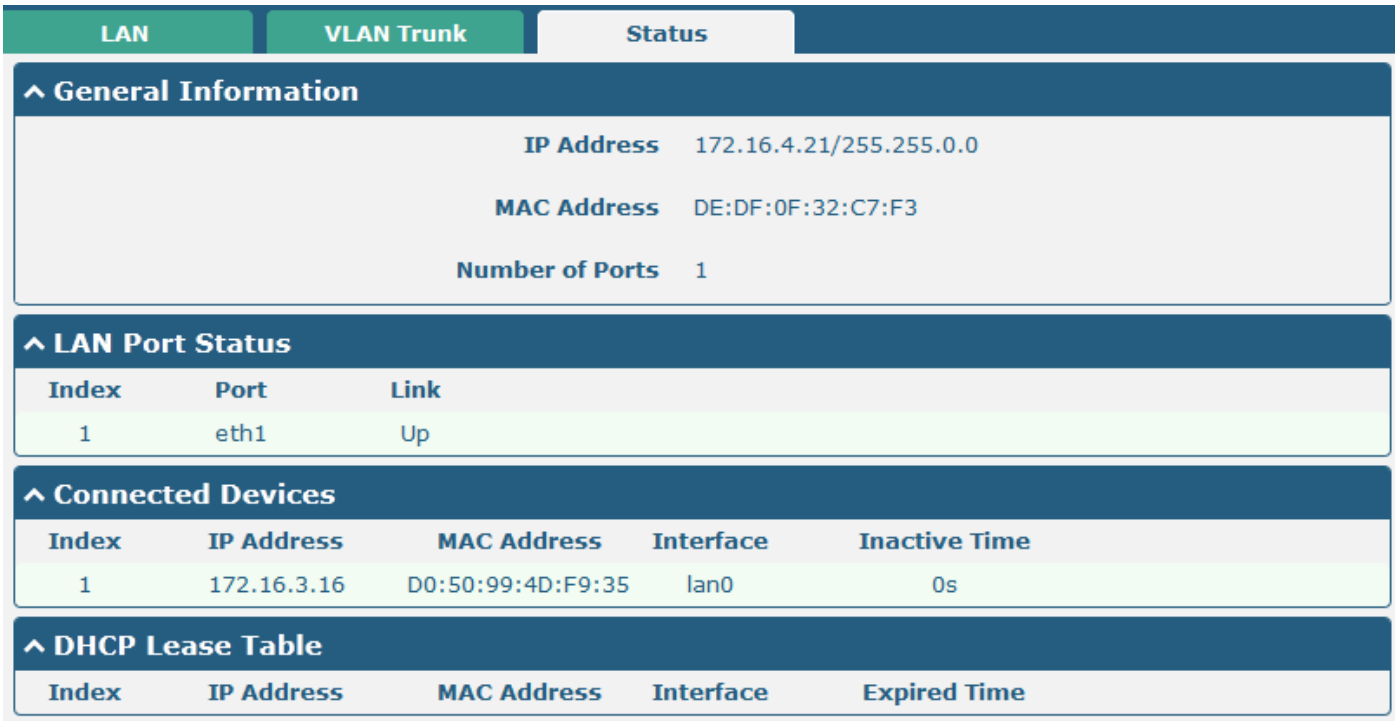
Click + to add a VLAN. The maximum number of the VLAN is eight.



VLAN Trunk		
Item	Description	Default
Enable	Enable to make router can encapsulate and de-encapsulate the VLAN tag.	ON
Interface	Select lan0 or lan1.	lan0
VID	Set the Tag ID of VLAN, values range from 1 to 4094.	0
IP Address, Netmask	Set the IP address, Netmask of VLAN interface	Null

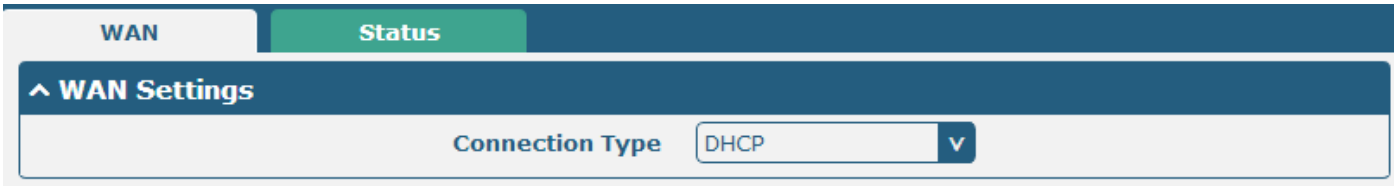
Status

This section shows the Ethernet port status and connected devices.



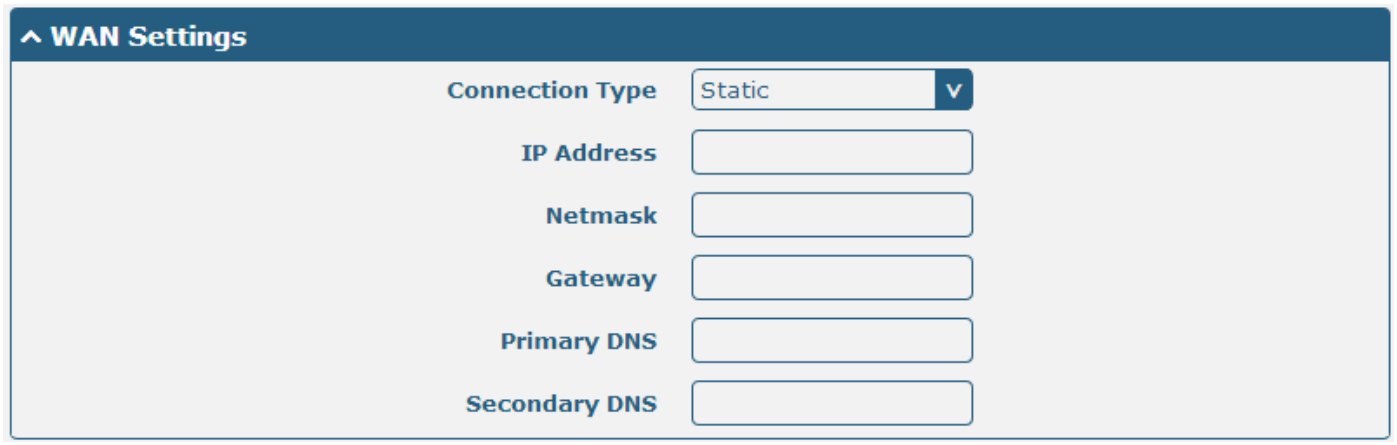
3.9 Interface->WAN (display when Eth0 as WAN port)

When choose the WAN Connection Type as DHCP, 4G INDUSTRIAL VPN will obtain IP automatically from DHCP server.



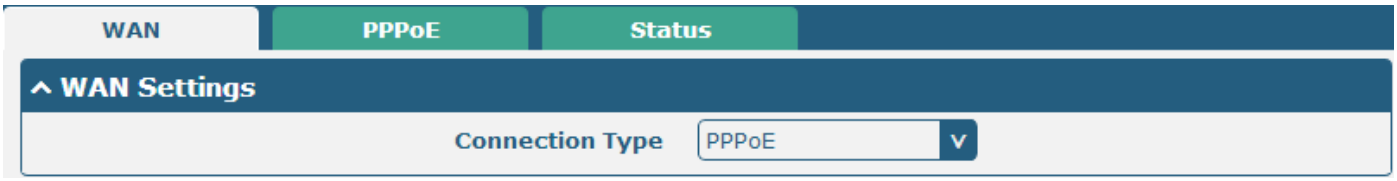
DHCP@WAN		
Item	Description	Default
Connection Type	Select from “DHCP”, “Static” and “PPPoE”.	DHCP

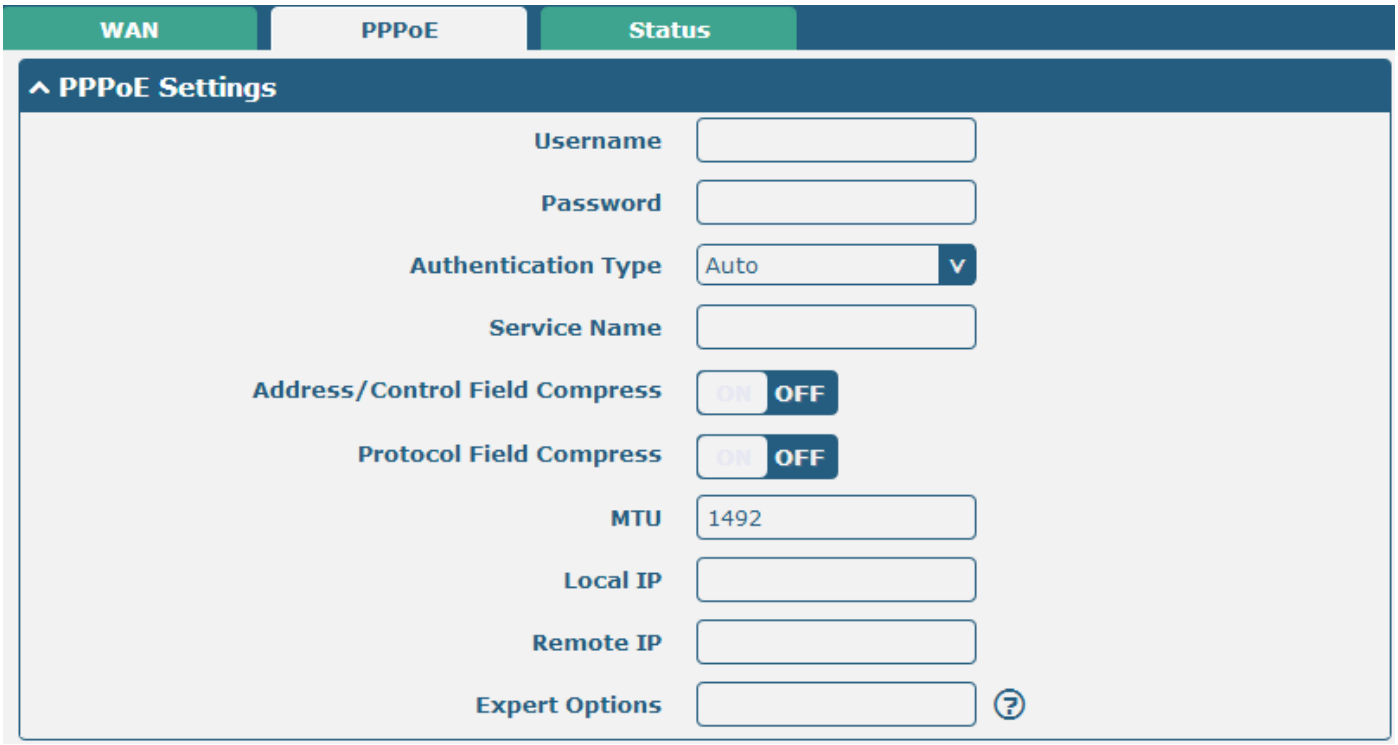
When choose the WAN Connection Type as Static.



Static		
Item	Description	Default
IP Address	Set the IP address which can access the internet.	DHCP
Netmask	Set the Netmask of the WAN IP.	Null
Gateway	Set the gateway of the WAN IP.	Null
Primary DNS	Set the Primary DNS.	Null
Secondary DNS	Set the Secondary DNS.	Null

When choose the WAN Connection Type as PPPoE. User can set the parameters of the PPPoE in **PPPoE** window.

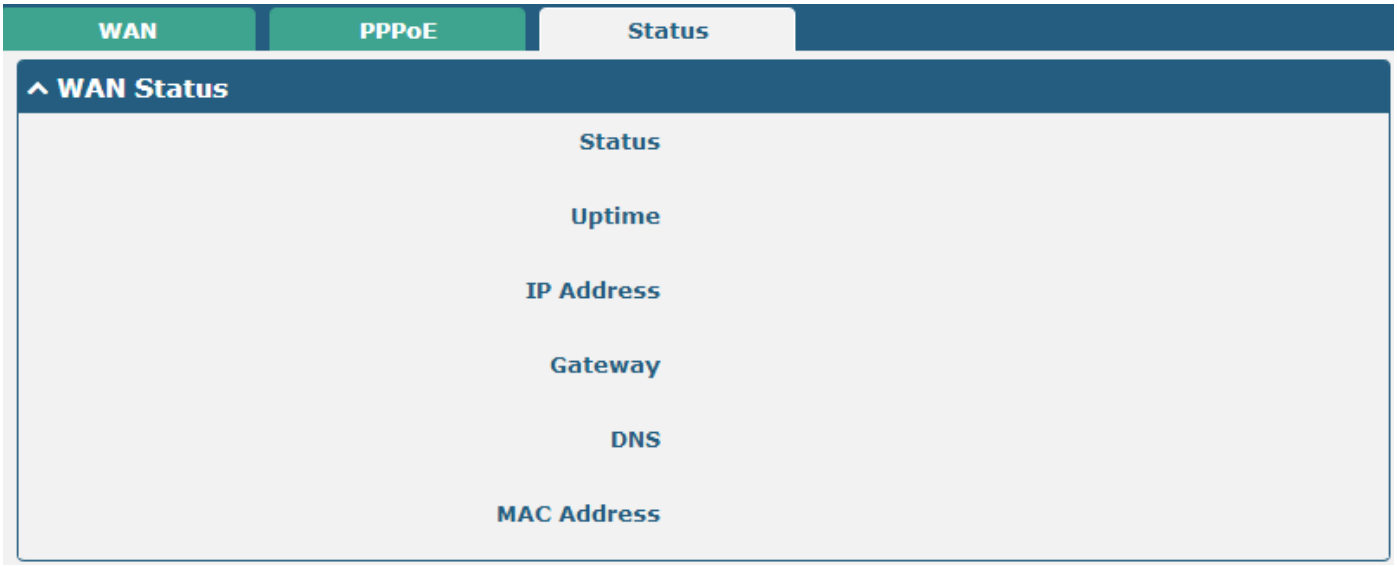




PPPoE		
Item	Description	Default
Username	Enter the username which was provided by your Internet Service Provider.	Null
Password	Enter the password which was provided by your Internet Service Provider.	Null
Authentication Type	Select from “Auto”, “PAP” and “CHAP” as the local ISP required.	Auto
Service Name	Set the service name of PPPoE server.	Null
Address/Control Field Compress	Used for PPP initialization.	OFF
Protocol Field Compress	Used for PPP initialization.	OFF
MTU	Maximum Transmission Unit. It is the identifier of the maximum size of packet, which is possible to transfer in a given environment.	1492

Local IP	Enter the specified IP address which was assigned by PPPoE server. This item always can be null. If you need to specify the PPPoE client IP, please reply to your ISP.	Null
Remote IP	Enter the specified PPPoE server address from your ISP. This item always can be null. If you need to specify the PPPoE server, please reply to your ISP.	Null
Expert Options	Expert options used for PPPoE dialup. You can enter some other PPP initialization strings in this field. Each string can be separated by a space.	Null

In this section, user can check the status of the WAN link.

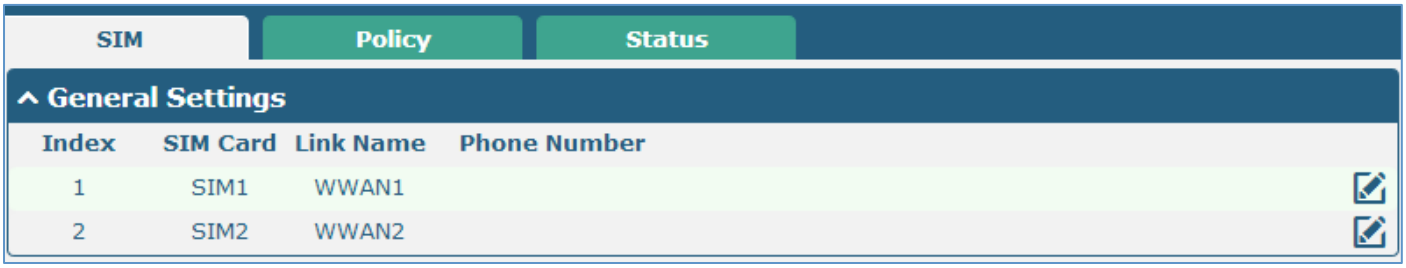


3.10 Interface->Cellular

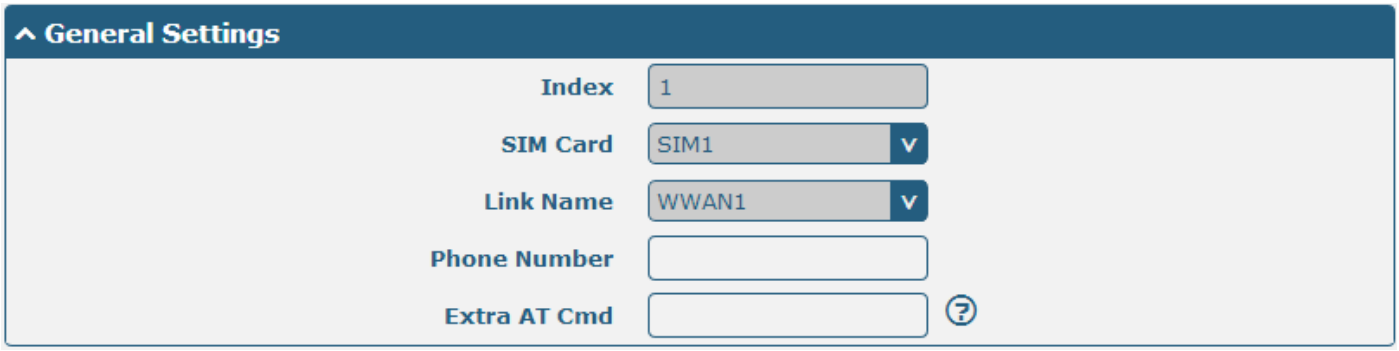
This section allows users to set the Cellular WAN and the related parameters.

When it is the first time to insert single SIM card, SIM card 1 and SIM card 2 slots are available.

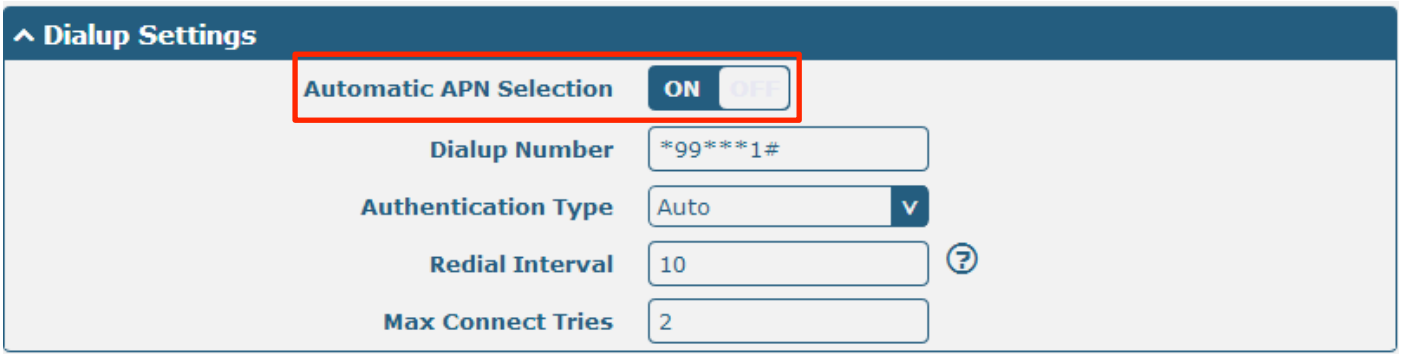
SIM



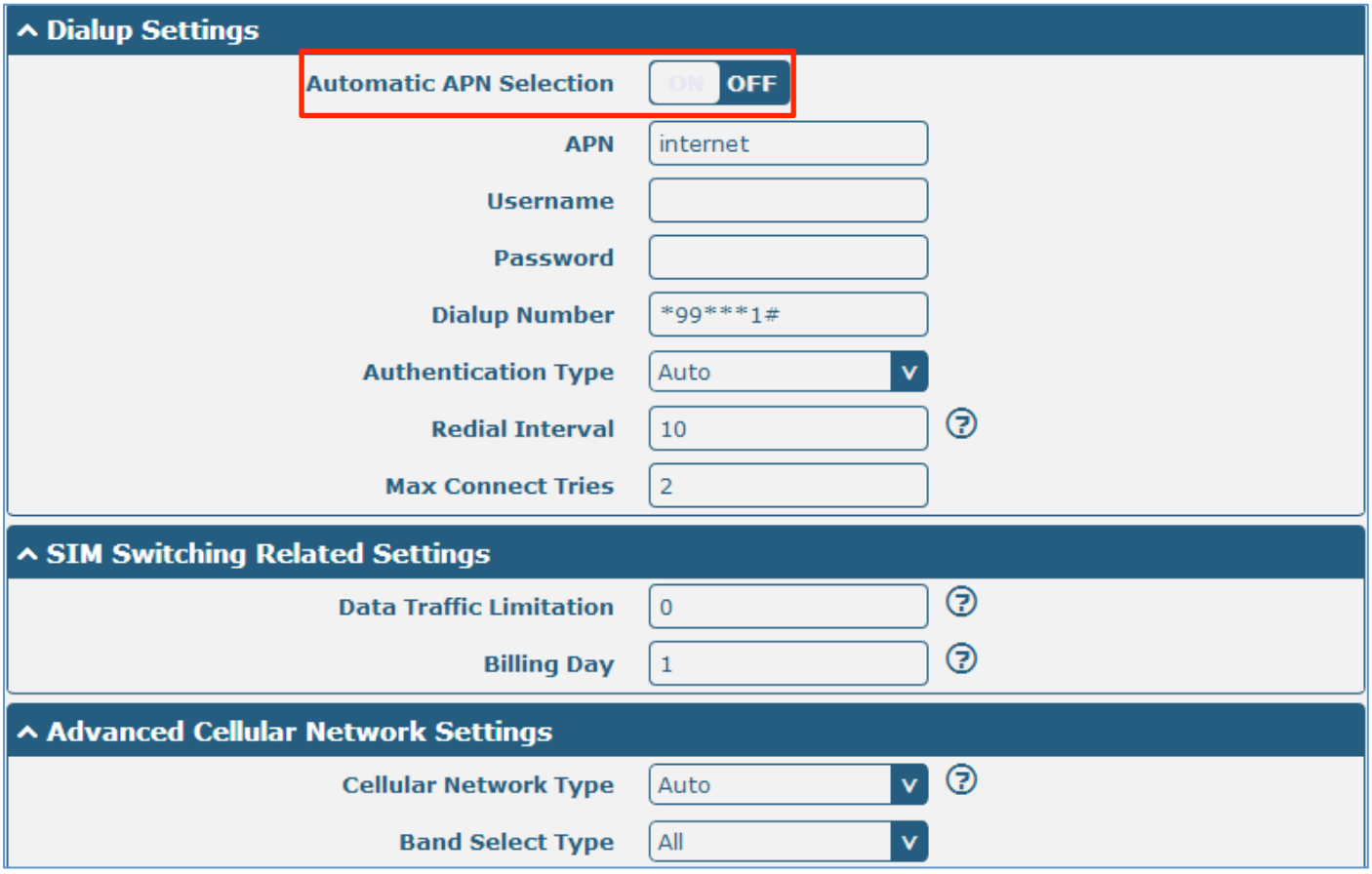
Click" " to edit the parameters.



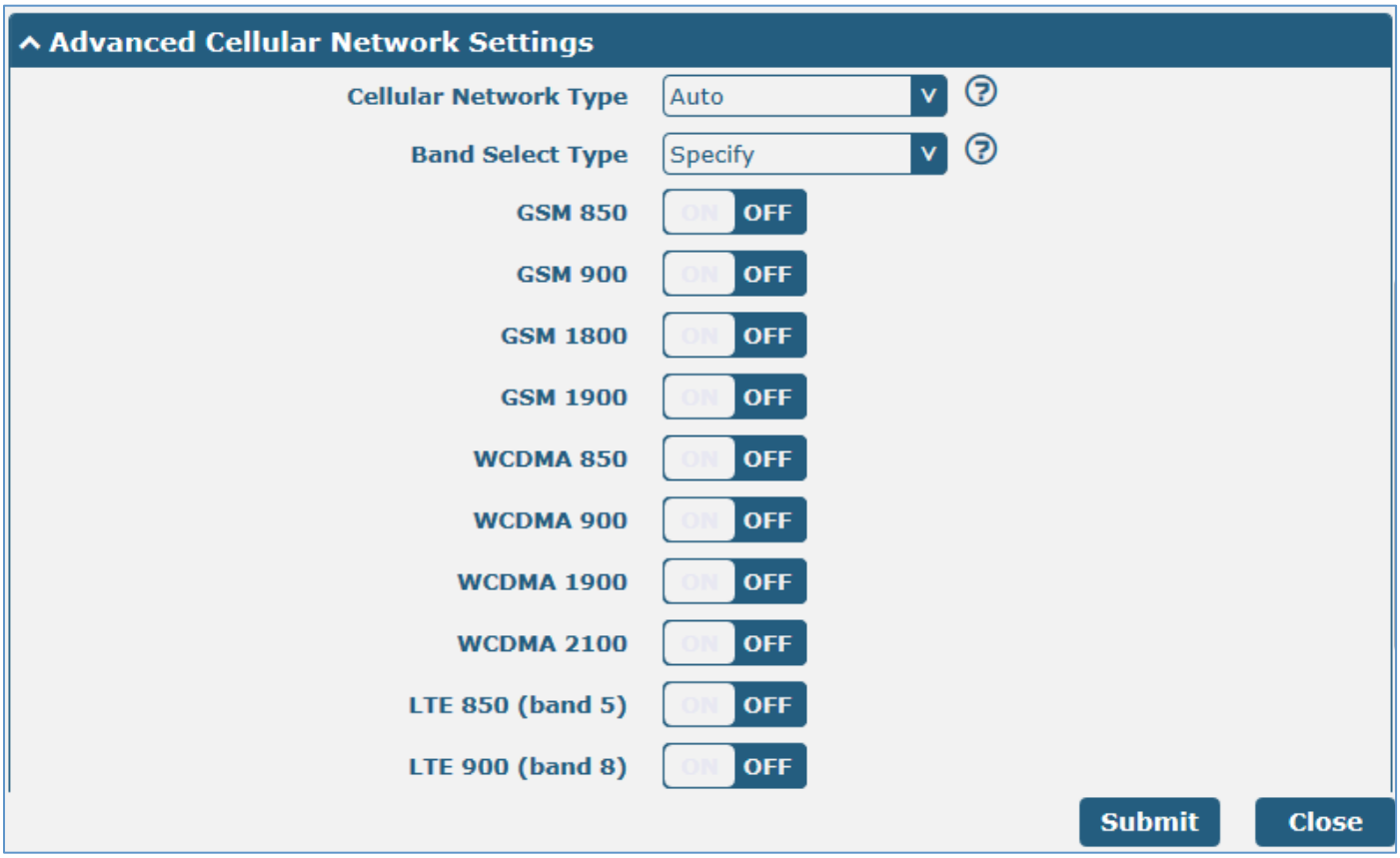
When click “Automatic APN Selection” on.



When click “Automatic APN Selection” off.



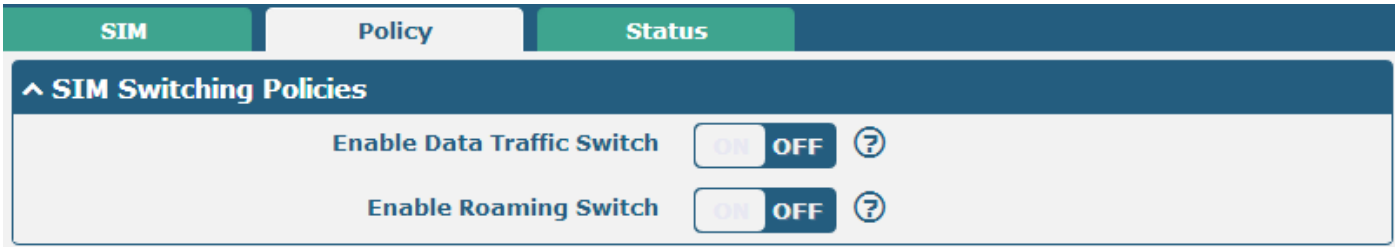
When “choose band select type” is “Specify”;



SIM		
Item	Description	Default
Index	Show the index of the SIM.	1
SIM Card	Set the current SIM card.	SIM1
Link Name	Set the current Link Name.	WWAN1
Phone Number	Define the phone number of the SIM card.	Null
Extra AT Cmd	AT commands used for cellular initialization.	Null
Automatic APN Selection	ON: Select access point name automatically. OFF: Select access point name manually.	ON
Dialup Number	Dialup number for cellular dial-up connection, provided by local ISP.	*99***1#
Authentication Type	Select from “Auto”, “PAP” and “CHAP” as the local ISP required.	Auto
Redial Interval	Seconds to wait for redial.	10
Max Connect Tries	The maximum connect tries times for automatically re-connect when router fails to dial up. After reaching maximum retries, router will switch to the other SIM card. If it fails to switch to the other SIM card, it will take emergency action which you had set in Link management. After successful connection, the Max Connect Tries counter will be set to 0.	2
APN	Access Point Name for cellular dial-up connection, provided by local ISP.	internet
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
Data Traffic Limitation	Set the monthly data traffic limitation.	0

	The system will record the data traffic statistics when data traffic limitation (MiB) is specified. The traffic record will display in **Cellular->Status** section.	
Billing Day	Set one day of month to restore the used data to 0.	1
Cellular Network Type	Select from “Auto”, “2G Only”, “2G First”, “3G Only”, “3G First”, “4G Only”, “4G First”.	Auto
Band Select Type	Select from “All”, “Specify”. When select “Specify”, user can choose certain bands.	All

Policy



Policy		
Item	Description	Default
Enable Data Traffic Switch	Switch to another SIM when reach limited data traffic, only use for dual SIM backup.	OFF
Enable Roaming Switch	Switch to backup SIM when preferred SIM is roaming, only use for dual SIM backup.	OFF

Status

SIM | Policy | Status

Cellular Information

Modem Status	Ready
Current SIM	SIM1
Total SIMs	1
Phone Number	
IMSI	460016642227120
ICCID	89860113225101168811
Registration	Registered to home network
Network Provider	CHN-UNICOM
Network Type	WCDMA
Signal Strength	7 (-99dBm)
Cell ID	A50B,148058D
Modem Model	ME909u-521
IMEI	860461020236850
Firmware Version	11.234.77.00.00

Data Connection Status

Status	Connected
Interface	eth2
Uptime	0 days, 00:05:48
IP Address	10.178.116.6/255.255.255.252
Gateway	10.178.116.5
DNS	210.21.4.130 221.5.88.88
APN	3gnet
User Name	

Data Connection Statistics

Current Connection Stats	TX:2548B RX:1580B
SIM1 Monthly Stats	Clear
SIM2 Monthly Stats	Clear

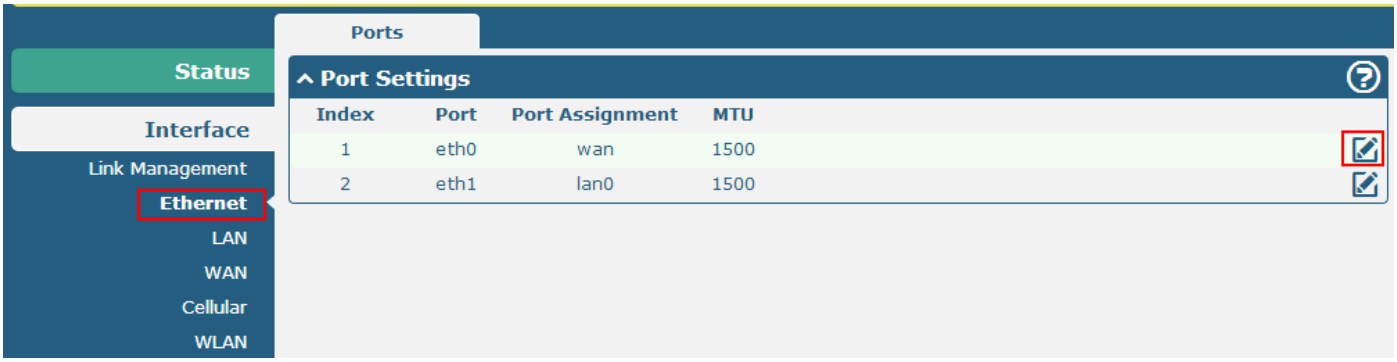
Status	
Item	Description
Modem Status	Show the status of the radio module.
Current SIM	Show the SIM card which the router works with currently: SIM1 or SIM2.
Total SIMs	Show the number of SIM cards that is installed in the router.
Phone Number	Show the phone number of the current SIM.
IMSI	Show the IMSI number of the current SIM.
ICCID	Show the ICCID number of the current SIM.
Registration	Show the current network status.
Network Provider	Show the name of Network Provider.
Network Type	Show the current network service type, e.g. GPRS.
Signal Strength	Show the current signal strength.
Cell ID	Show the current cell ID, which can locate the router.
Modem Model	Show the model of the radio module.
IMEI	Show the IMEI number of the radio module.
Firmware Version	Show the current firmware version of the radio module.
Status	Show the status of the data connection.
Interface Name	Show the current cellular name.
Uptime	Show the duration of the dial-up connection, this Uptime will be set to 0 after redial.
IP Address	Show the current IP address of the cellular WAN.
Gateway	Show the current gateway of the cellular WAN.
DNS	Show the current DNS of cellular WAN.
APN	Show the current APN.
User Name	Show the user name.
Current Connection Stats	Show the current TX and RX data.
SIM1 Monthly Stats	Show the amount of data connection in this month.
SIM2 Monthly Stats	Show the amount of data connection in this month.

3.11 Interface->Wi-Fi (Optional)

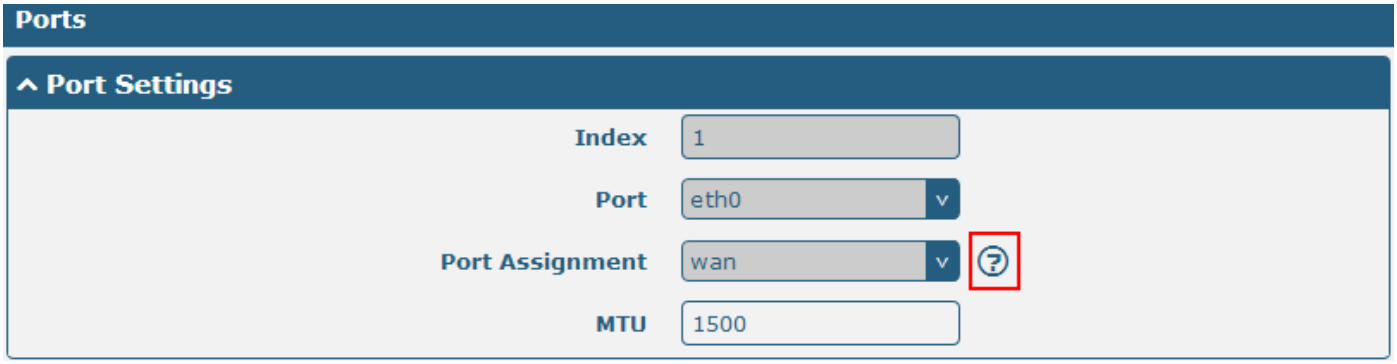
4G INDUSTRIAL VPN router support both Wi-Fi AP and Wi-Fi client. The factory default setting of 4G INDUSTRIAL VPN is as Wi-Fi AP.
This section allow user to configure the parameters of Wi-Fi AP.

Wi-Fi AP

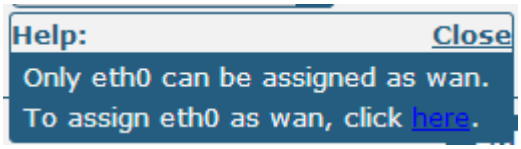
Configure 4G INDUSTRIAL VPN as a Wi-Fi AP
Go to Ethernet tab.



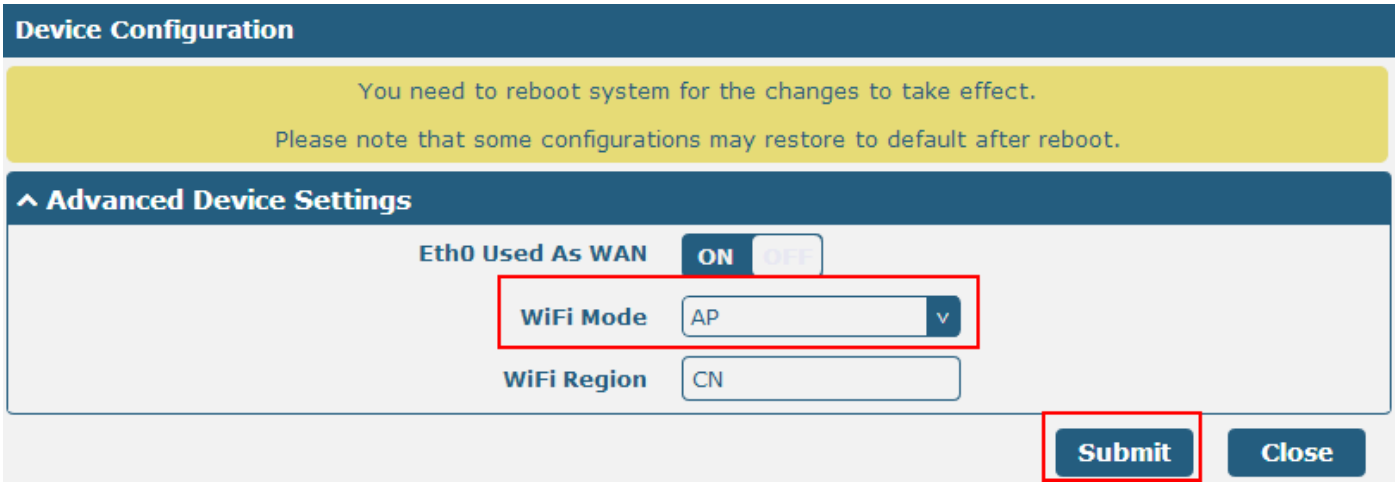
Click  to open a new window. And then click  to get the help.



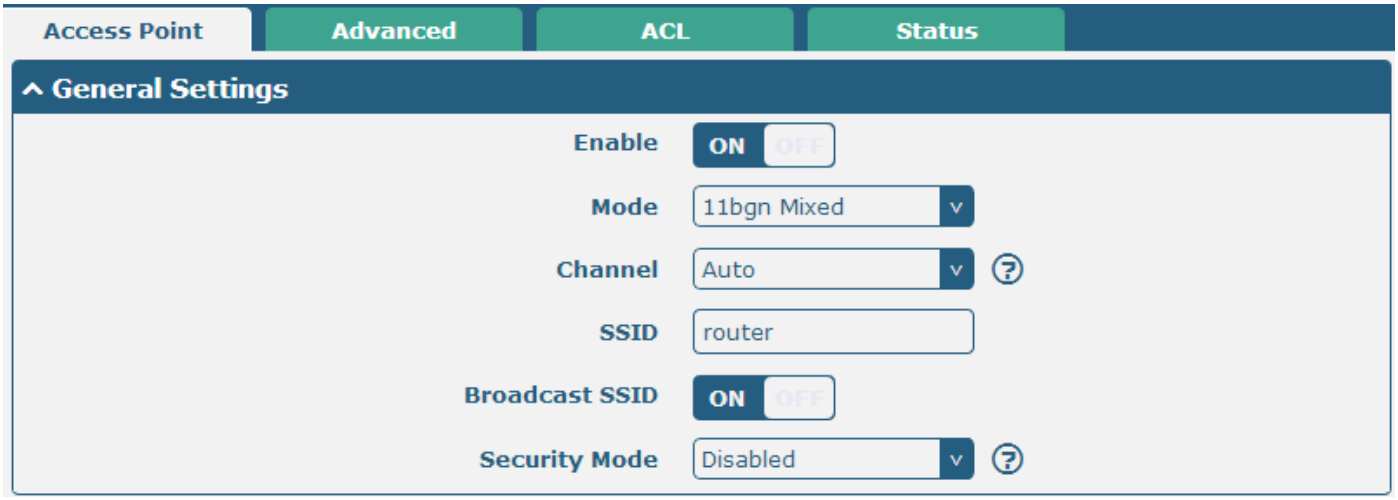
Click “here” in the help tip box.



Select the Wi-Fi mode as AP, click “Submit” and reboot the device to make the setting effect.

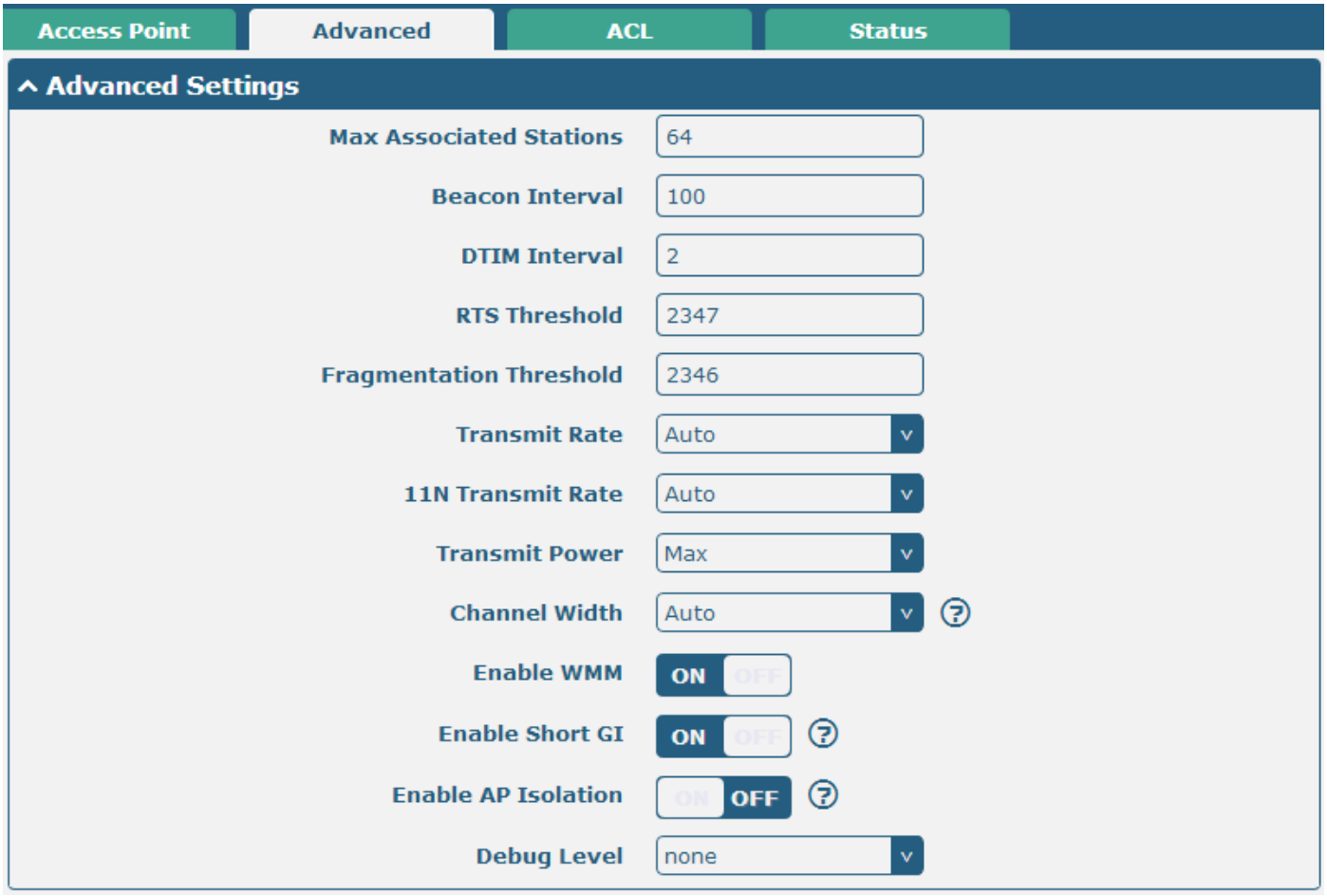


When 4G INDUSTRIAL VPN router was set as a Wi-Fi AP, we can find the Wi-Fi item in the Interface menu. Just like the screenshot below.



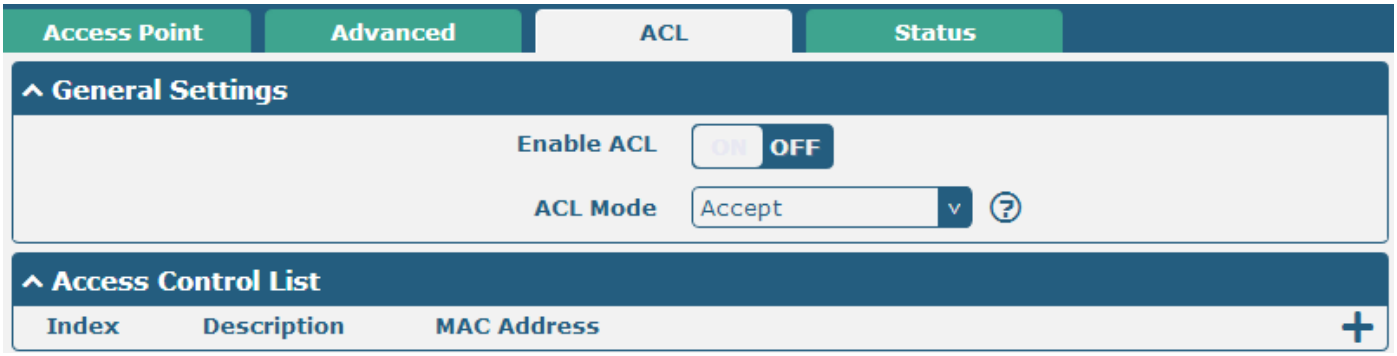
Access Point		
Item	Description	Default
Enable	Click to “ON” side, enable the Wi-Fi access point function.	OFF
Mode	Select from “11bgn Mixed”, “11b only”, “11g only” and “11n only”. 11bgn Mixed: Three protocols mixed in order to backward compatibility 11b only: IEEE 802.11b, 11Mbit/s-- 2.4GHz 11g only: IEEE 802.11g, 54Mbit/s--2.4GHz 11n only: IEEE 802.11n, 300Mbps~600Mbps	11bgn Mixed
Channel	Select the frequency channel, which includes “Auto”, “1”, “2”…… “11. Auto: 4G INDUSTRIAL VPN will scan all frequencies until it finds one with an available access point or wireless network it can join. 1~11: 4G INDUSTRIAL VPN will be fixed to work with this channel. Following are the frequency of 1~6 channel. 1 - 2412 MHz 2 - 2417 MHz 3 - 2422 MHz 4 - 2427 MHz 5 - 2432 MHz 6 - 2437 MHz	Auto
SSID	SSID (service set identifier) is the network name of the Wi-Fi. The SSID of a client and the SSID of the AP must be identical for the client and AP to be able to communicate with each other. Input from 1 to 31 characters.	Null
Broadcast SSID	Click “ON” to enable the SSID broadcasting. So that the entire client can scan the SSID. If you disable this feature, none of client could scan the SSID. If you want to connect to the router AP, you must need to enter the SSID of router AP at Wi-Fi client side manually.	NO
Security Mode	Select from “Disable”, “WPA” and “WEP”. Disable: User can access the Wi-Fi without the password when disable security. WPA: Include WPA and WPA2. Personal versions of WPA (Wi-Fi Protected	Disable

	Access), also known as WPA/WPA-PSK (Pre-Shared Key), provide a simple way of encrypting a wireless connection for high confidentiality. WEP: Wired Equivalent Privacy, provide encryption for wireless device's data transmission. It's not recommended to use WEP.	
WPA Version	Select from "Auto", "WPA" and "WPA2". Auto: 4G INDUSTRIAL VPN will choose the most suitable selection automatically. WPA2 is a stronger security feature than WPA.	WPA
Encryption	Select from "Auto", "TKIP" and "AES". Auto: 4G INDUSTRIAL VPN will choose the most suitable Encryption automatically. TKIP: Temporal Key Integrity Protocol (TKIP) encryption is used over the wireless link. TKIP encryption can be used with WPA-PSK and WPA with 802.1x authentication. It's not recommended to use TKIP encryption in 802.11n mode. AES: AES encryption is used over the wireless link. AES can be used WPA-PSK and WPA with 802.1x authentication. ***Note**: AES is a stronger encryption algorithm than TKIP.*	Auto
PSK Password	PSK password–Pre share key password. When 4G INDUSTRIAL VPN works as AP mode, enter Master key to generate keys for encryption. A PSK Password is used as a basis for encryption methods (or cipher types) in a WLAN connection. The PSK Password should be complicated and as long as possible. For security reasons, this PSK Password should only be disclosed to users who need it, and it should be changed regularly. Input from 8 to 63 characters.	Null
Group Key Update Interval	Enter the time period of group key renewal.	3600



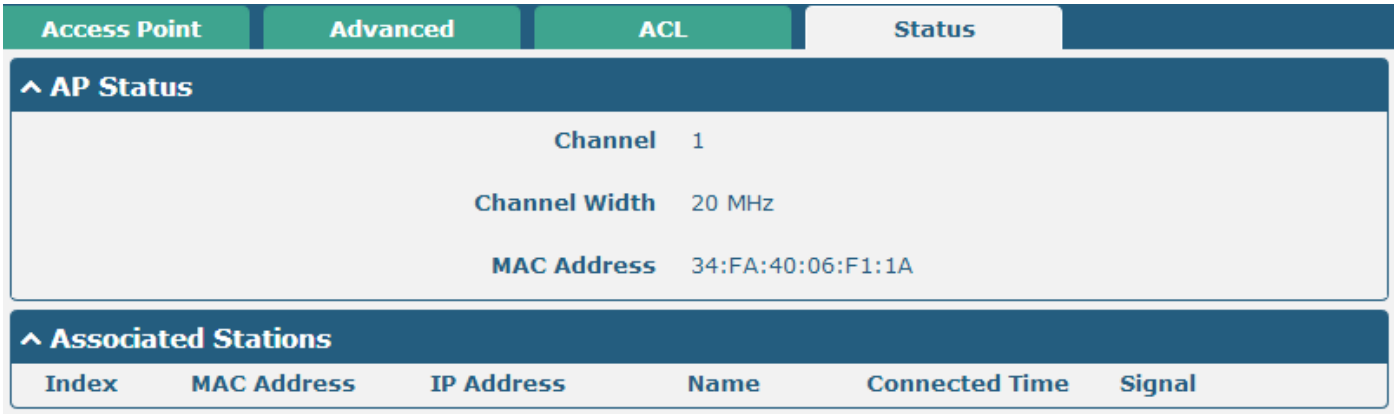
Advanced		
Item	Description	Default
Max Associated Stations	Set the max number of association station to access the router AP.	64
Beacon Interval	Set the frequency of the router AP broadcast Beacon, which was used for wireless network synchronization.	100
DTIM Interval	DTIM (Delivery Traffic Indication Message), router AP will send the multicast traffic according to this interval.	2
RTS Threshold	Set RTS (request to send) threshold to 2347, router AP will never sent the signal before sending out data. Set RTS threshold to 0, router AP will send the signal once it sending out data.	2347
Fragmentation Threshold	Set the fragmentation threshold for Wi-Fi AP data packet. Recommend remain at 2346.	2346
Transmit Rate	Set the transmit rate, you can choose Auto or specify a Transmit Rate.	Auto
11N Transmit Rate	Set the data transmit rate under the IEEE 802.11n Wi-Fi mode. Select “Auto” or a specified transmit rate.	Auto
Transmit Power	Select from “Max”, “High”, “Medium” and “Low”.	Max
Channel Width	Select from “20MHz”, “40MHz”. 40 MHz channel width provides twice the data rate available over a single 20 MHz channel.	Auto

Enable WMM	Click “ON” to enable WMM.	ON
Enable Short GI	Click “ON” to enable Short GI (Short Guard Interval), short GI is a blank time between two symbols, it can provide a long buffer time to delay signal. Using the Short Guard Interval would provide an 11% increase in data rates, but also may result in higher packet error rates.	ON
Enable AP Isolation	Isolate all connected wireless stations so that wireless stations cannot access each other through WLAN.	OFF
Debug Level	Select from “verbose”, “debug”, “info”, “notice”, “warning”, “none”.	none



ACL		
Item	Description	Default
Enable ACL	Click to enable ACL (Access Control List).	Disable
ACL Mode	Select from “Accept” and “Deny”. Accept: Only the packets fitting the entities of the “Access Control List” can be allowed. Deny: All the packets fitting the entities of the “Access Control List” will be denied. ***Note**: 4G INDUSTRIAL VPN can only allow or deny devices which are included in “Access Control List” at one time.*	Accept
Access Control List	Click “+” to add MAC address.	Null

This section allow user to check the AP status and those Wi-Fi client had connected to 4G INDUSTRIAL VPN AP.



3.12 Interface->WLAN (Optional)

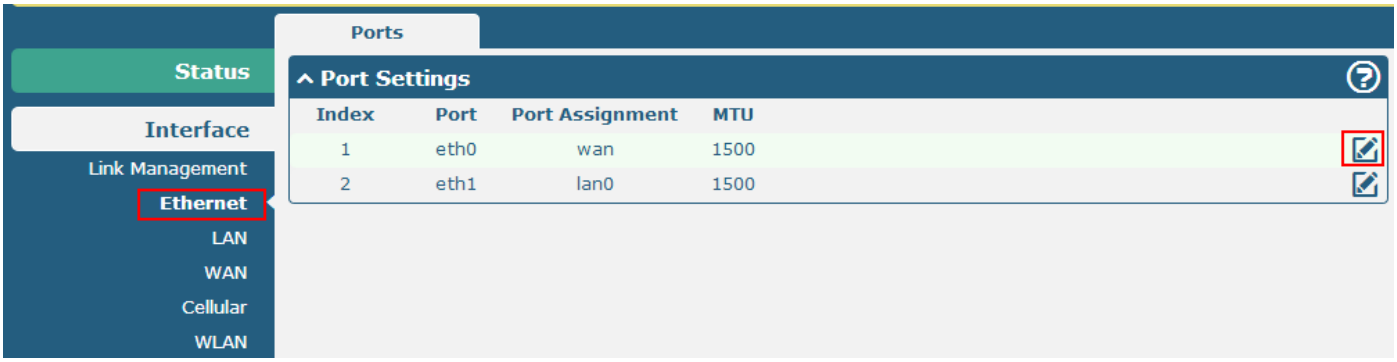
4G INDUSTRIAL VPN router support both Wi-Fi AP and Wi-Fi client. The factory default setting of 4G INDUSTRIAL VPN is as Wi-Fi AP.

This section allow user to configure the parameters of Wi-Fi client.

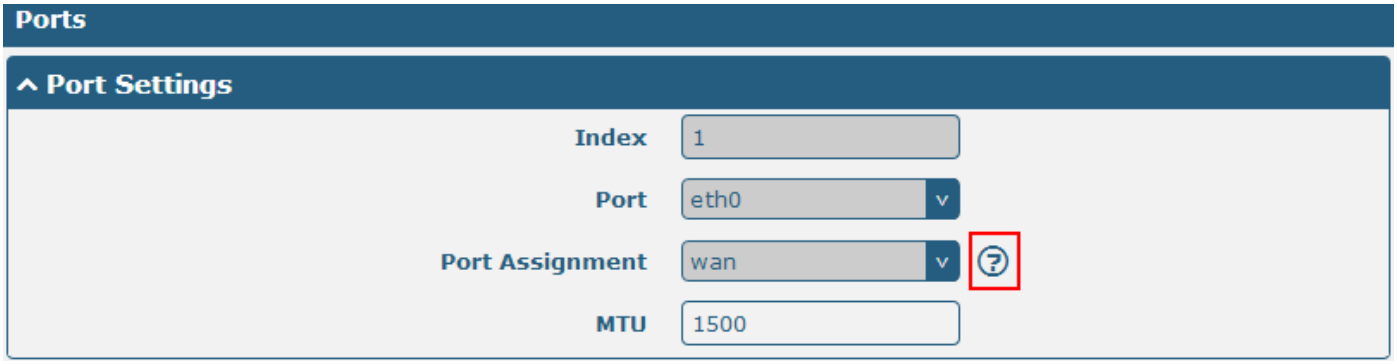
Wi-Fi Client

Configure 4G INDUSTRIAL VPN as a Wi-Fi client

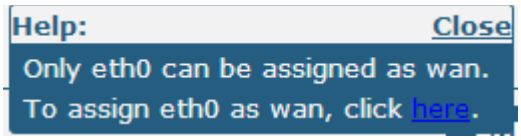
Go to Ethernet tab.



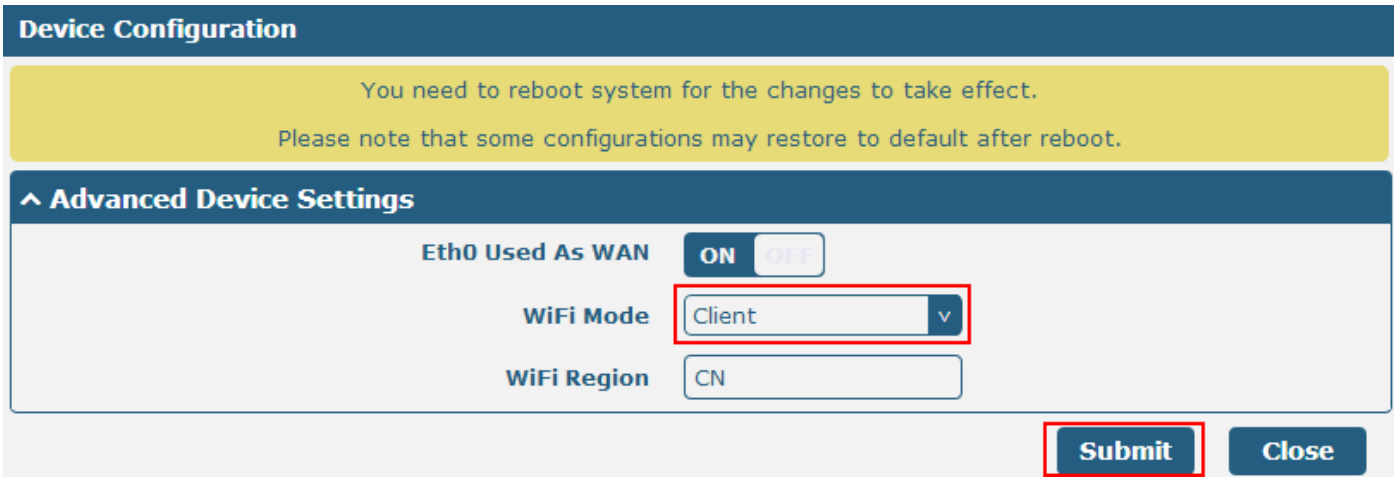
Click  to open a new window. And then click  to get the help.



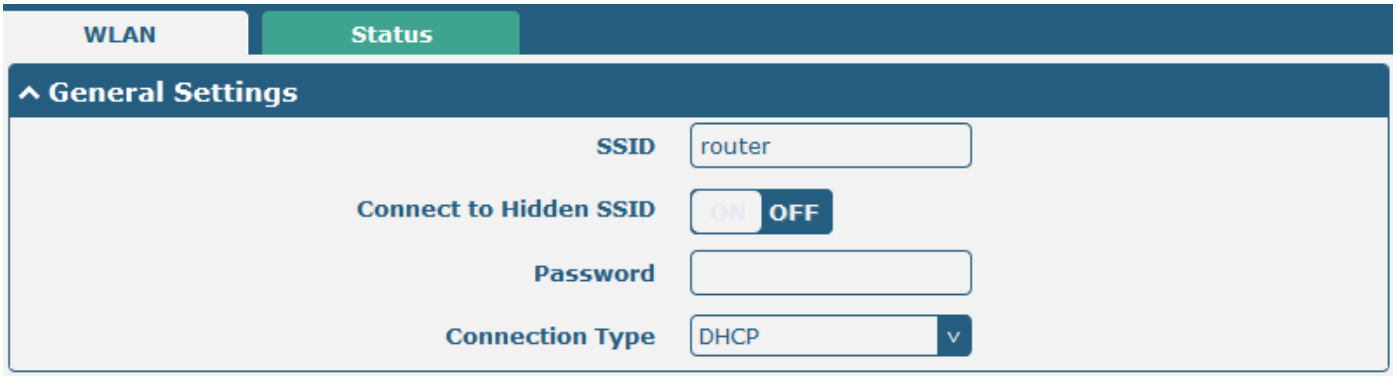
Click “here” in the help tip box.

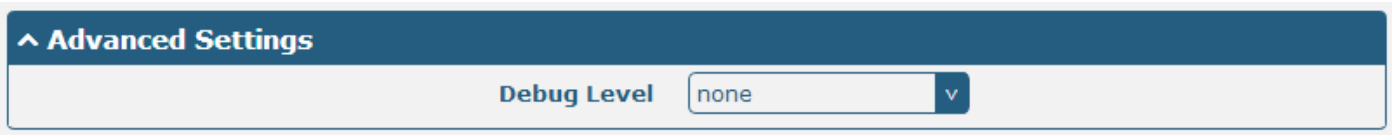


Select the Wi-Fi mode as Client, click “Submit” and reboot the device to make the setting effect.



After 4G INDUSTRIAL VPN was configured successfully as a Wi-Fi client, there will appear a WLAN tab in the Interface menu, just as the screenshot below.





WLAN		
Item	Description	Default
SSID	Enter SSID of the access point which R3000 want to connect. Input from 1 to 31 characters.	router
Connect to Hidden SSID	When 4G INDUSTRIAL VPN works as Client mode and need to connect to any access point which has hidden SSID, you need to enable this feature.	OFF
Password	Enter access point's passphrase which it wants to connect to. Input from 8 to 63 characters.	Null
Connection Type	Select from "DHCP" and "Static". DHCP: 4G INDUSTRIAL VPN will obtain the IP from Wi-Fi AP DHCP IP pool automatically. Static: You need to enter the related parameter from Wi-Fi AP.	DHCP
Debug Level @ Advanced Settings	Select from "verbose", "debug", "info", "notice", "warning", "none".	None

This section allows user to check the WLAN connection status. It includes WLAN status, Link status and WPA status.

WLAN | Status

WLAN Status

Status	
Uptime	
IP Address	
Gateway	
DNS	
MAC Address	

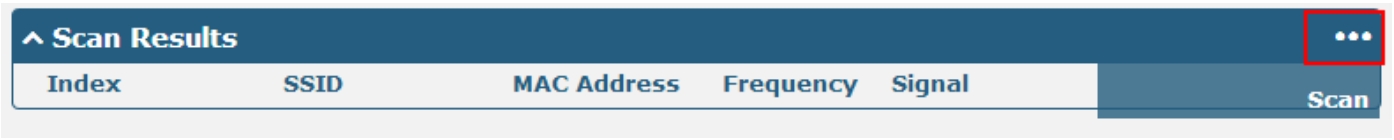
Link Status

Signal	
Noise	
Width	
TX Bitrate	
TX	
RX	

WPA Status

WPA State	
Frequency	
BSSI	
Mode	
Key Management	
Pairwise Cipher	
Group Cipher	

User can scan the surrounding SSIDs in this section. Please click , and click “Scan” to scan the surrounding SSIDs.

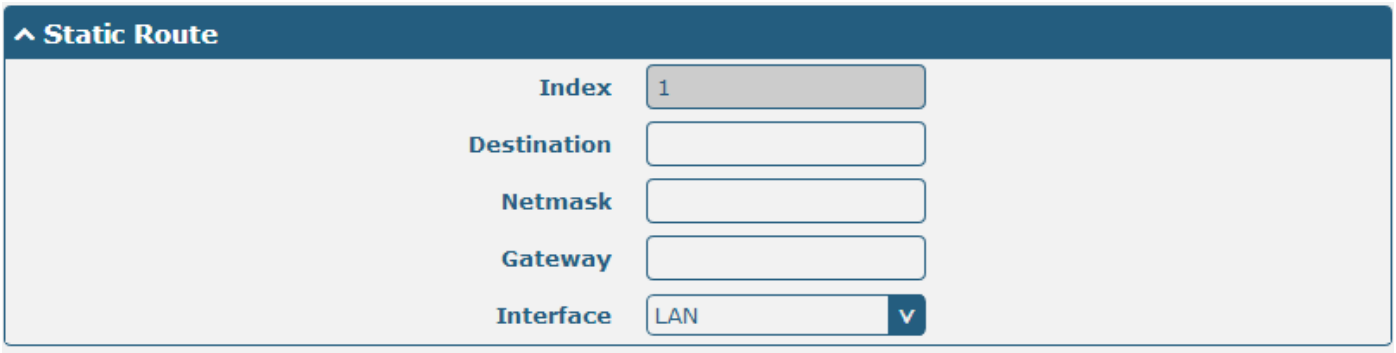


3.13 Network->Route

This section allows user to set the static route. (The maximum number of the static route is twenty.)

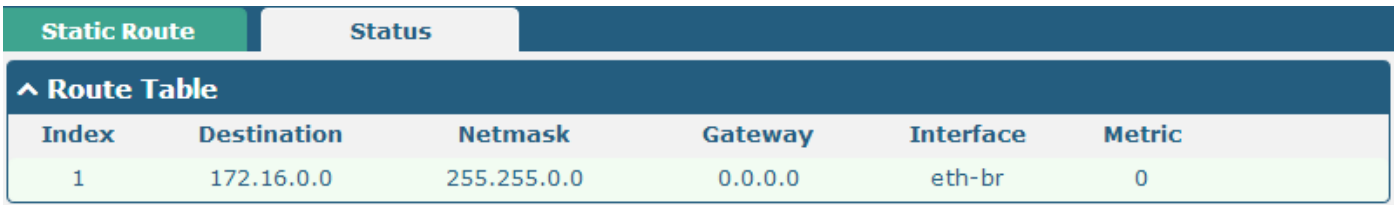
Static Route

Click “ ” to add static routes.



Static Route		
Item	Description	Default
Index	Show the index of the static route.	1
Destination	Define the destination IP address.	Null
Netmask	Define the Netmask of the destination.	Null
Gateway	Define the gateway of the destination.	Null
Interface	Select from “LAN”, “WAN”, “TUN1”, “TUN2”, “TUN3”, “TAP1”, ”TAP2”, ”TAP3”.	LAN

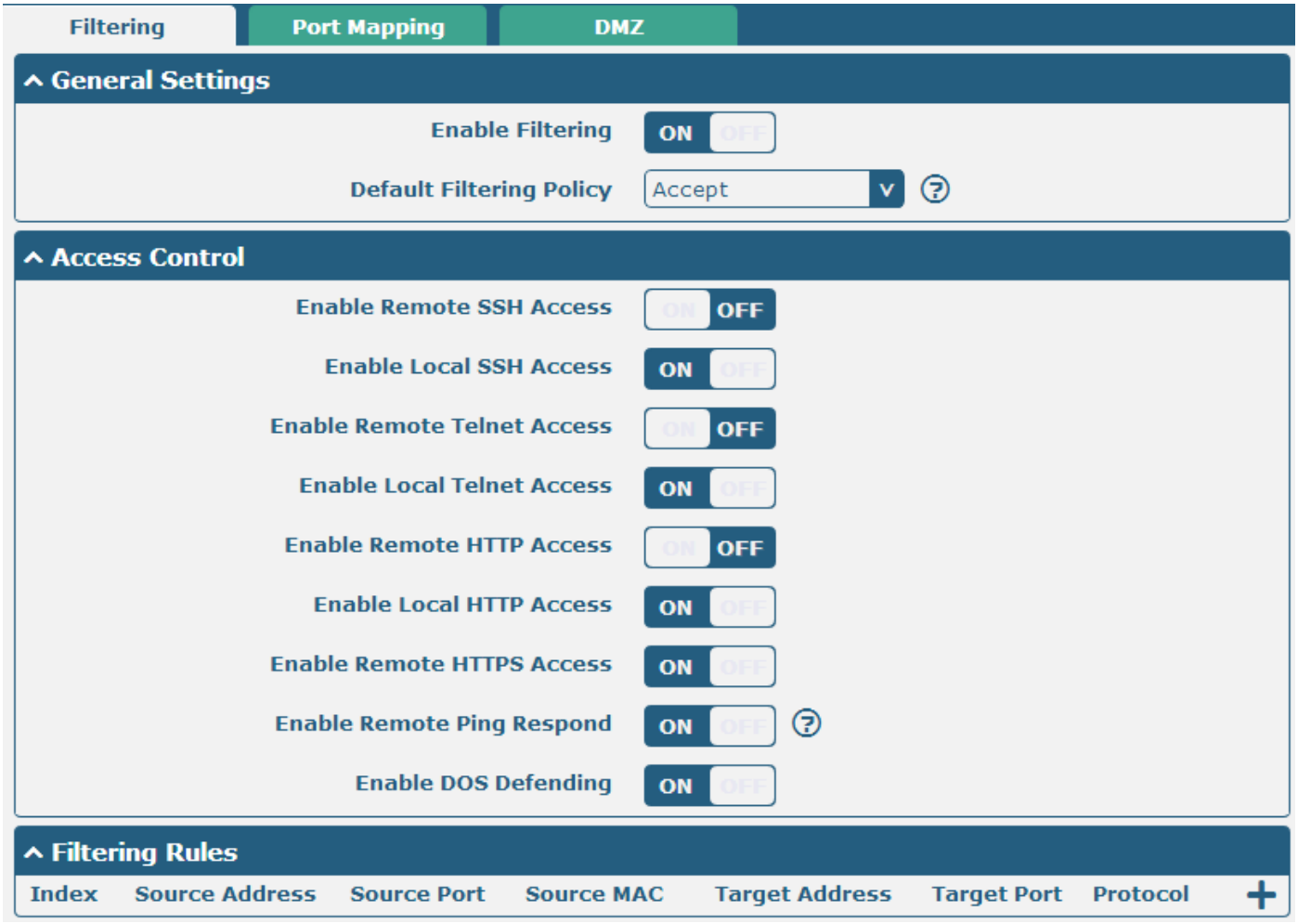
Status



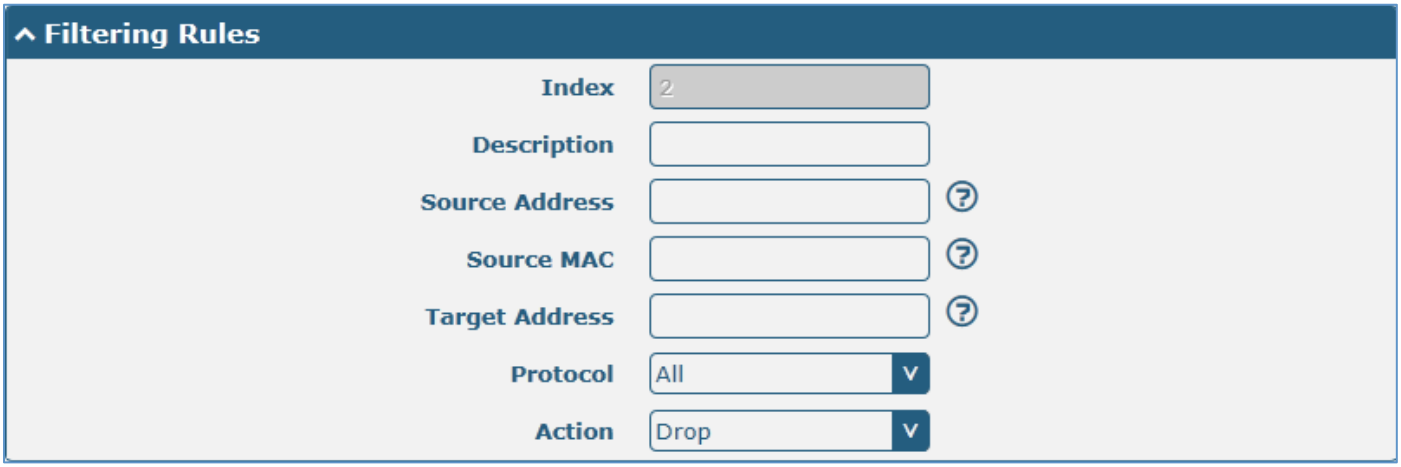
3.14 Network->Firewall

This section allows users to set the Firewall and the related parameters, which includes “Filter”, “Port Mapping” and “DMZ”.

Filtering

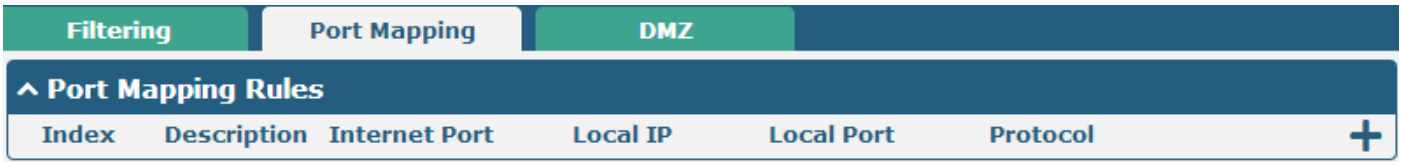


Click “+” to add filtering rules. (The maximum number of the filtering rule is twenty.)

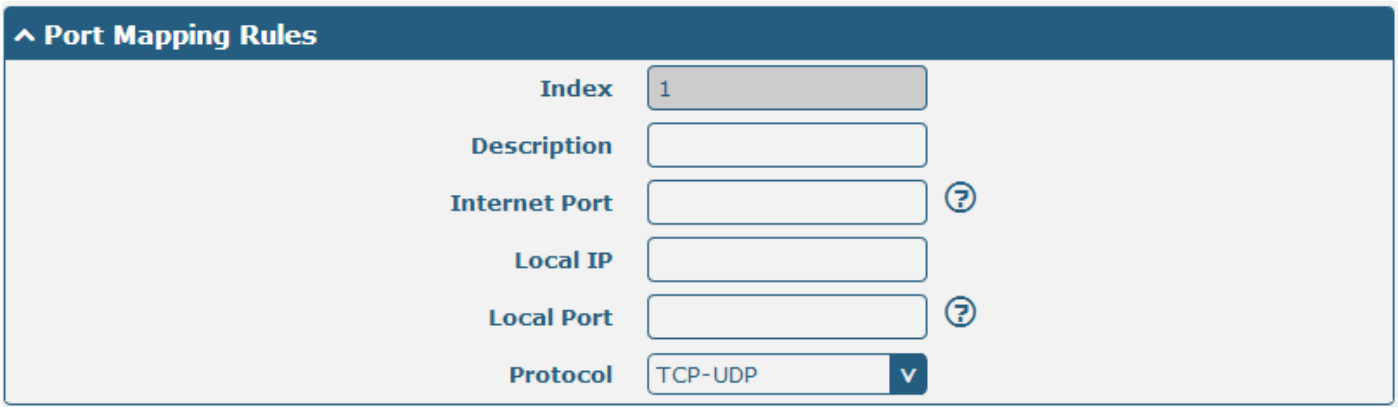


Filtering		
Item	Description	Default
Enable Filtering	Enable filtering rules.	ON
Default Filtering Policy	Select from “Accept” and “Drop”. Accept: Router will accept all the connecting requests except the hosts which fit the filter list. Drop: Router will only reject the connecting requests from the hosts which fit the filter list.	accept
Enable Remote SSH Access	Enable to allow users to access the router remotely on the internet side via SSH.	OFF
Enable Local SSH Access	Enable to allow users to access the router on the local Ethernet via SSH.	ON
Enable Remote Telnet Access	Enable to allow users to access the router remotely on the internet side via Telnet.	OFF
Enable Local Telnet Access	Enable to allow users to access the router on the local Ethernet via Telnet.	ON
Enable Remote Http Access	Enable to allow users to access the router remotely on the internet side via Http.	OFF
Enable Local Http Access	Enable to allow users to access the router on the local Ethernet via Http.	ON
Enable Remote Https Access	Enable to allow users to access the router remotely on the internet side via Https.	ON
Enable Remote Ping Respond	Enable to make router reply the Ping requests from the internet side.	ON
Enable DOS Defending	Enable to defend dos attack. Dos attack is an attempt to make a machine or network resource unavailable to its intended users.	ON
Index	Show the index of the filtering rule or the MAC binding rule.	1
Source Address	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 MAC	Enter the MAC address of the defined source IP address.	Null
Target 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
Protocol	Select from “All”, “TCP”, “UDP”, “ICMP”, “TCP-UDP”. If you don’t know what kinds of protocol of your application, we recommend you select “ALL”.	All
Action	Select from “Accept”, “Drop”.	Drop

Port Mapping

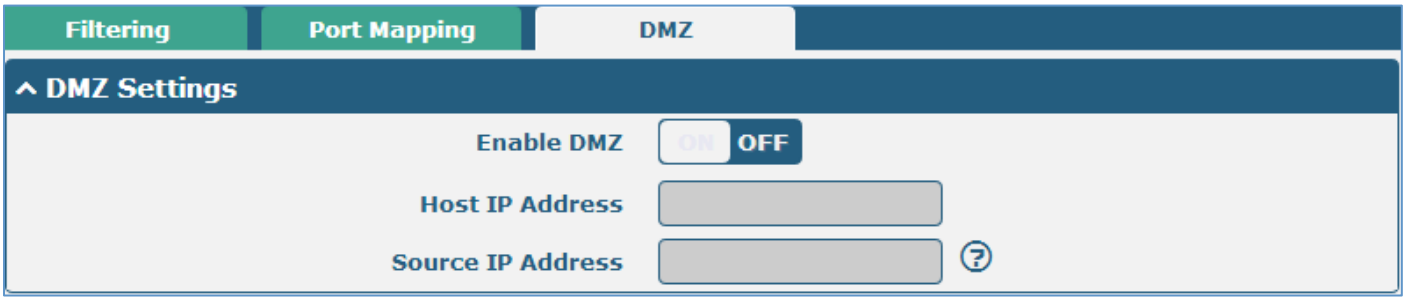


Click “+” to add port mapping rules. (The maximum number of the port mapping rule is forty.)



Port Mapping		
Item	Description	Default
Index	Show the index of the port mapping rule.	1
Internet Port	The port of the internet side which you want to forward to LAN side.	Null
Local IP	The device's IP on the LAN side which you want to forward the data to.	Null
Local Port	The device's port on the LAN side which you want to forward the data to.	Null
Protocol	Select from "TCP", "UDP" and "TCP-UDP".	TCP-UDP

DMZ

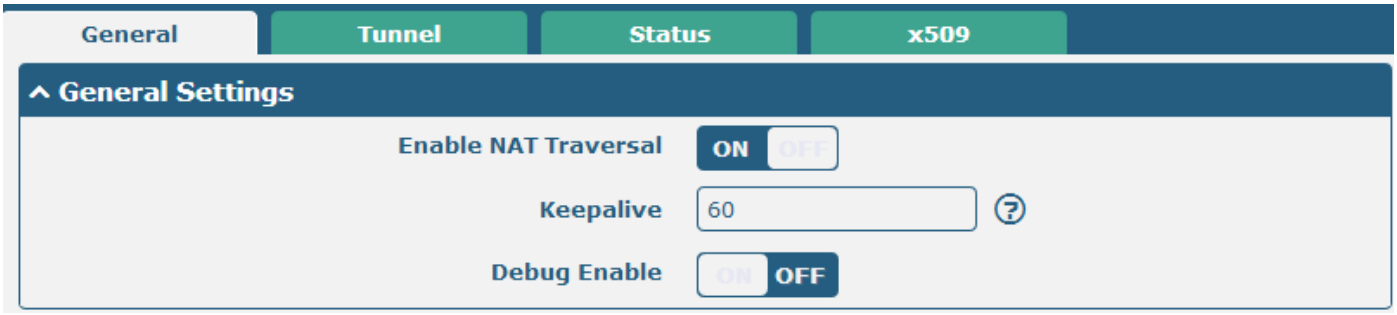


DMZ		
Item	Description	Default
Enable DMZ	Select to enable the DMZ function. DMZ host is a host on the internal network that has all ports exposed, except those ports otherwise forwarded.	OFF
Host IP Address	Enter the IP address of the DMZ host which on the internal network.	Null
Source IP Address	Set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

3.15 VPN->IPSec

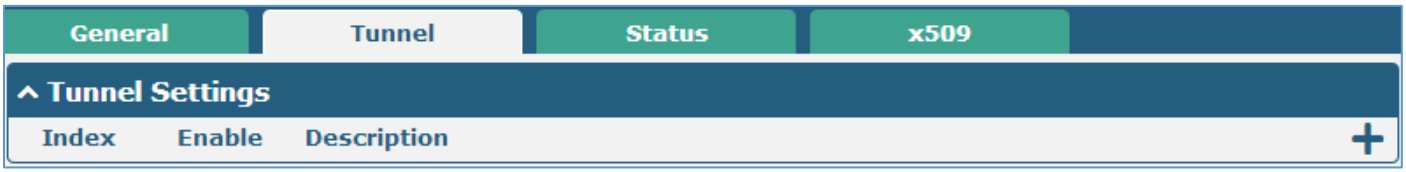
This section allows users to set the IPSec and the related parameters.

General

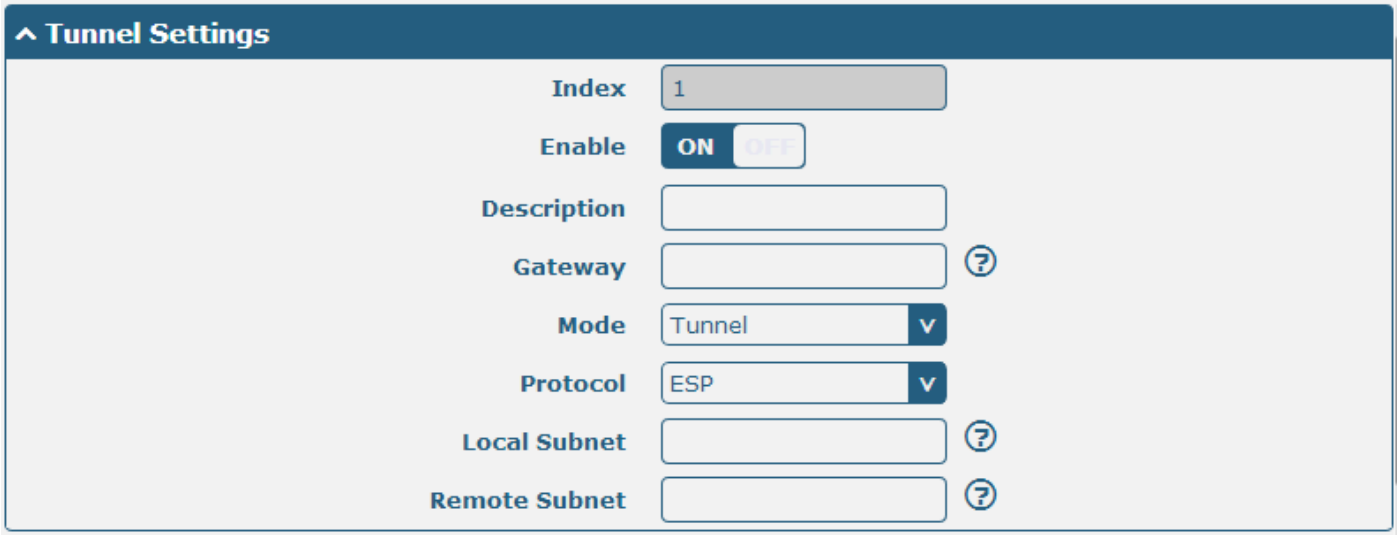


General		
Item	Description	Default
Enable NAT Traversal	Tick to enable NAT Traversal for IPSec. This item must be enabled when router under NAT environment.	ON
Keepalive	The interval that router sends packets to NAT box so that to avoid it remove the NAT mapping.	60
Debug Enable	Enable this function, and it will output IPSec information to the debug port.	OFF

Tunnel



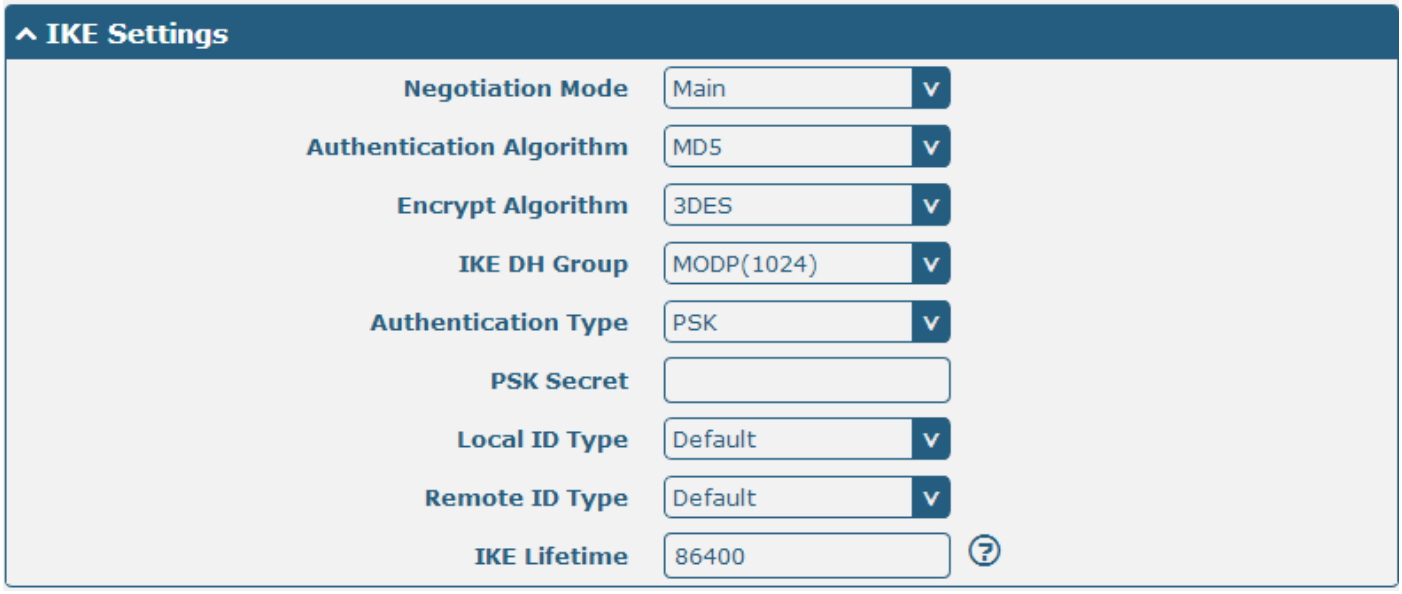
Click "+" to add tunnel settings. (The maximum number of the tunnel is three.)



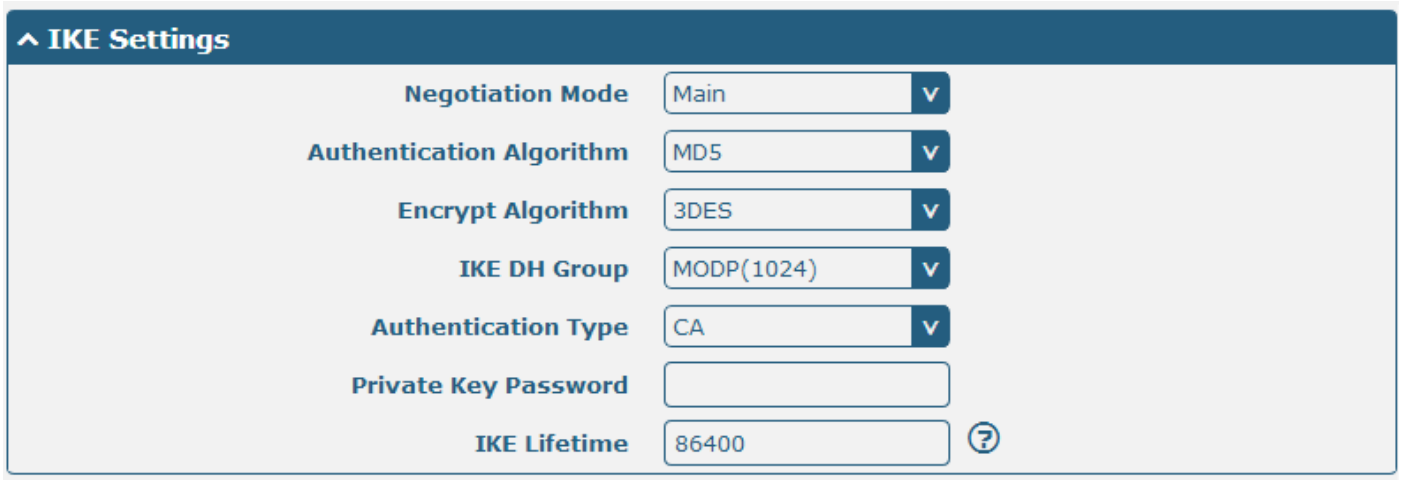
Tunnel Settings		
Item	Description	Default
Index	Show the index of the tunnel.	1
Enable	Enable IPSec Tunnel.	ON
Description	Enter some simple words about the IPSec Tunnel.	Null
Gateway	Enter the address of remote side IPSec VPN server.	Null

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
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 with mask, e.g. 192.168.1.0/24	Null
Remote Subnet	Enter IPSec Remote Protected subnet’s address with mask, e.g. 10.8.0.0/24	Null

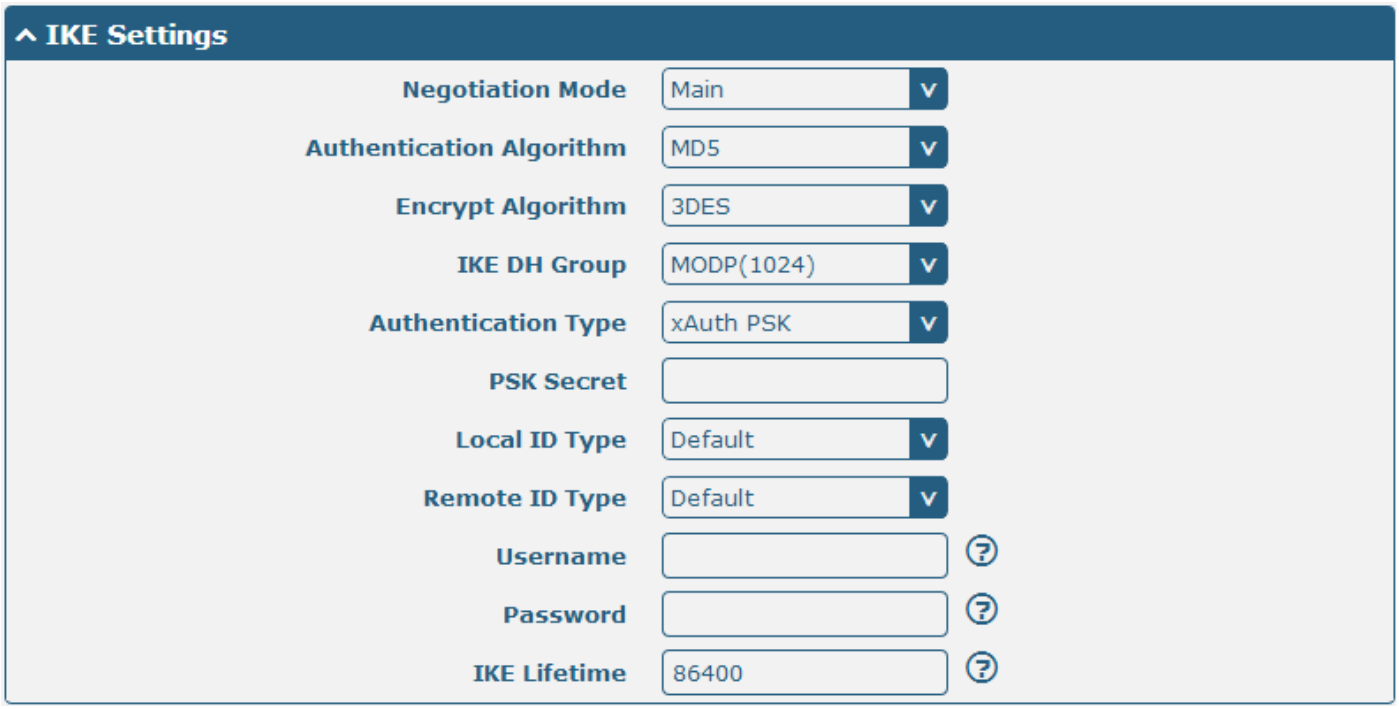
When choose “Authentication Type” to “PSK”.



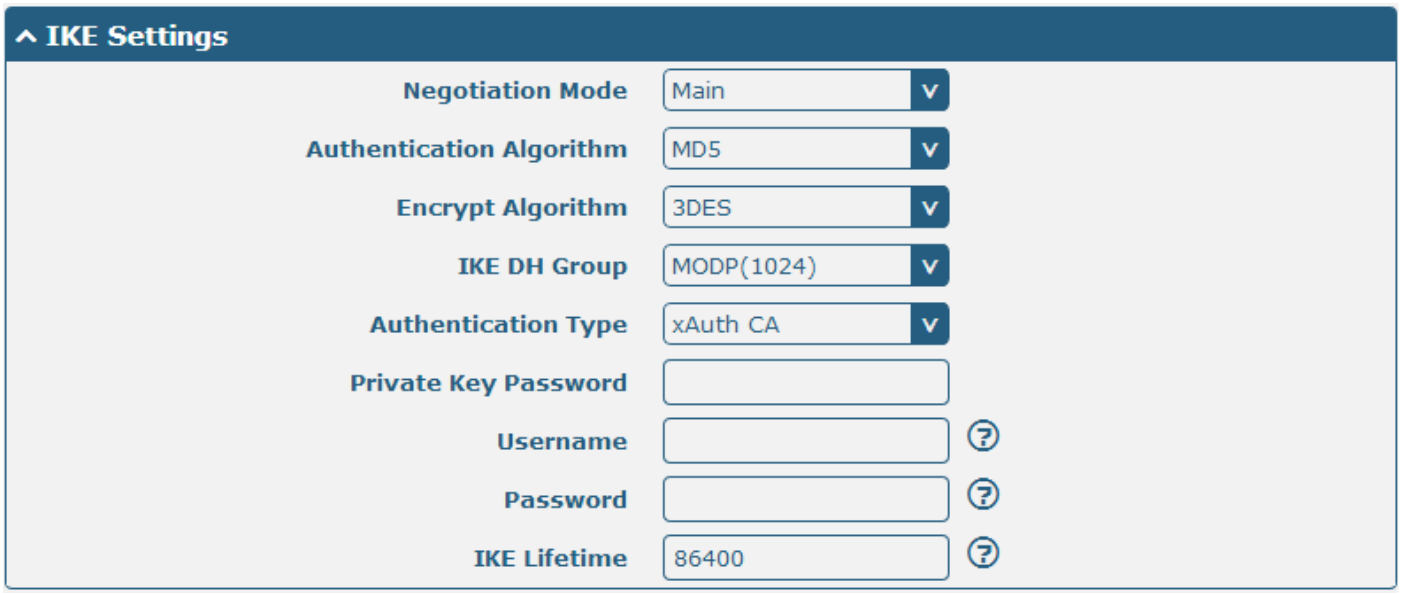
When choose “Authentication Type” to “CA”.



When choose “Authentication Type” to “xAuth PSK”.



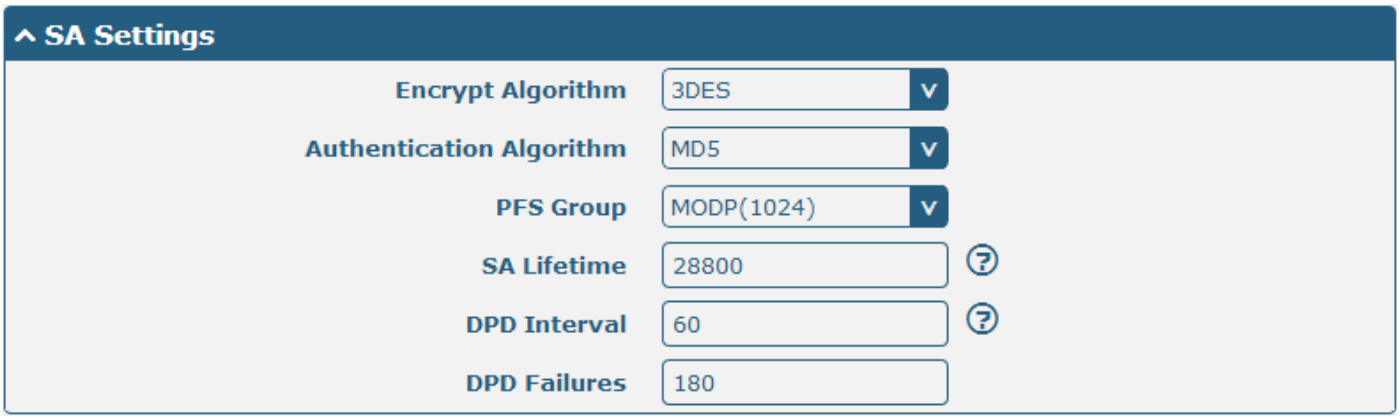
When choose “Authentication Type” to “xAuth CA”.



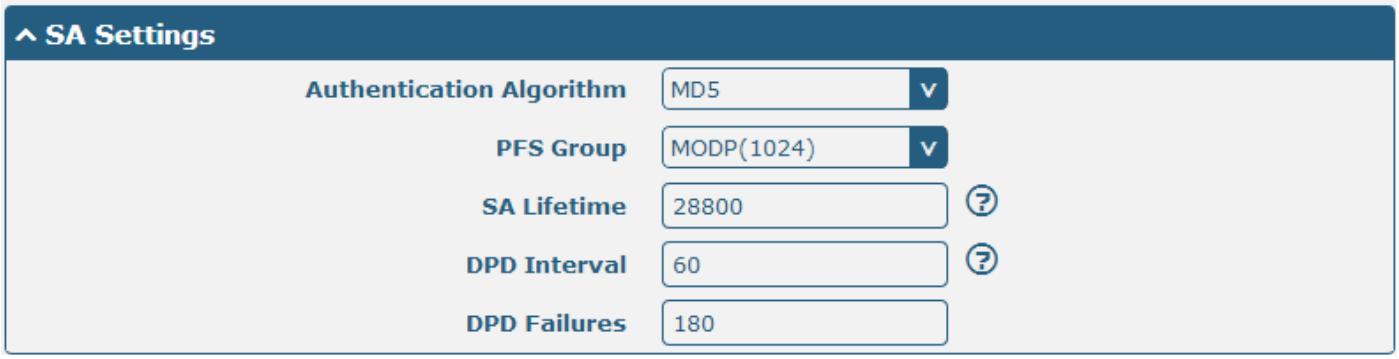
IKE Settings		
Item	Description	Default
Negotiation Mode	Select from “Main” and “Aggressive” for the IKE negotiation mode in phase 1. If the IP address of one end of an IPSec tunnel is obtained dynamically, the IKE negotiation mode must be aggressive. In this case, SAs can be established as long as the username and password are correct.	Main
Authentication Algorithm	Select from “MD5” and “SHA1”to be used in IKE negotiation. MD5: Uses HMAC-SHA1. SHA1: Uses HMAC-MD5.	MD5
Encrypt Algorithm	Select from “3DES”, “AES128” and “AES256”to be used in IKE negotiation. 3DES: Uses the 3DES algorithm in CBC mode and 168-bit key.	3DES

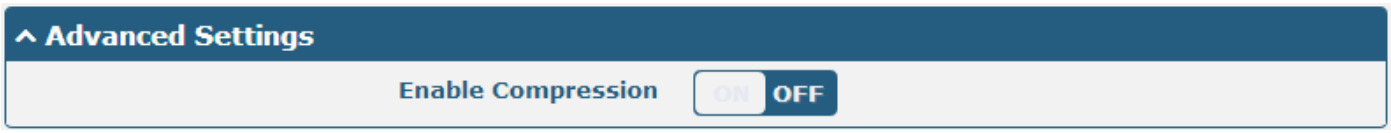
	AES128: Uses the AES algorithm in CBC mode and 128-bit key. AES256: Uses the AES algorithm in CBC mode and 256-bit key.	
IKE DH Group	Select from “MODP (1024)” and “MODP (1536)”to be used in key negotiation phase 1. MODP (1024): Uses the 1024-bit Diffie-Hellman group. MODP (1536): Uses the 1536-bit Diffie-Hellman group.	MODP (1024)
Authentication Type	Select from “PSK”, “CA”, “xAuth PSK” and “xAuth CA” to be used in IKE negotiation. PSK: Pre-shared Key. CA: Certification Authority. xAuth: Extended Authentication to AAA server.	PSK
PSK Secret	Enter the pre-shared key.	Null
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.Digicom.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@Digicom.com.	Default
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.Digicom.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@Digicom.com.	Default
IKE Lifetime	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
Private Key Password	Enter the private key.	Null
Username	User name used for xAuth.	Null
Password	Password used for xAuth.	Null

When choose the “Tunnel Setting->General Setting->Protocol” to “ESP”.



When choose the “Tunnel Setting->Protocol” to “AH”.



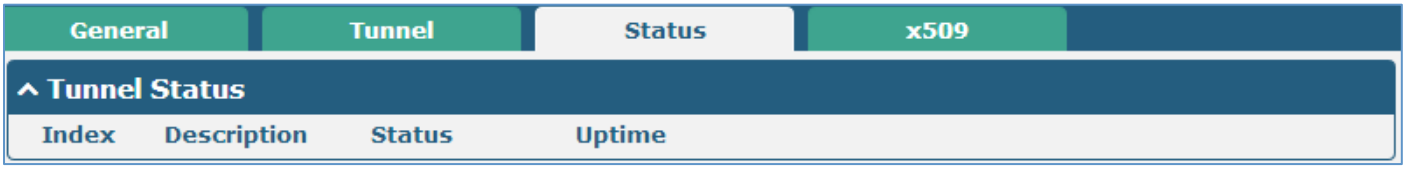


SA Settings		
Item	Description	Default
Encrypt Algorithm	Select from “3DES”, “AES128” and “AES256” when you select “ESP” in “Protocol”; Note: Higher security means more complex implementation and lower speed. DES is enough to meet general requirements. Use 3DES when high confidentiality and security are required.	3DES
Authentication Algorithm	Select from “MD5” and “SHA1”to be used in SA negotiation.	MD5
PFS Group	Select from “PFS (N/A)”, “MODP (1024)” and“MODP (1536)”. PFS (N/A): Disable PFS Group MODP (1024): Uses the 1024-bit Diffie-Hellman group. MODP (1536): Uses the 1536-bit Diffie-Hellman group.	MODP (1024)
SA Lifetime	Set the IPSec SA lifetime. Note: When negotiating to set up IPSec SAs, IKE uses the smaller one between the lifetime set locally and the lifetime proposed by the peer.	28800
DPD 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	60

	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.	
DPD Failures	Set the timeout of DPD packets.	180
Advanced Settings		
Enable Compression	Tick to enable compressing the inner headers of IP packets.	OFF

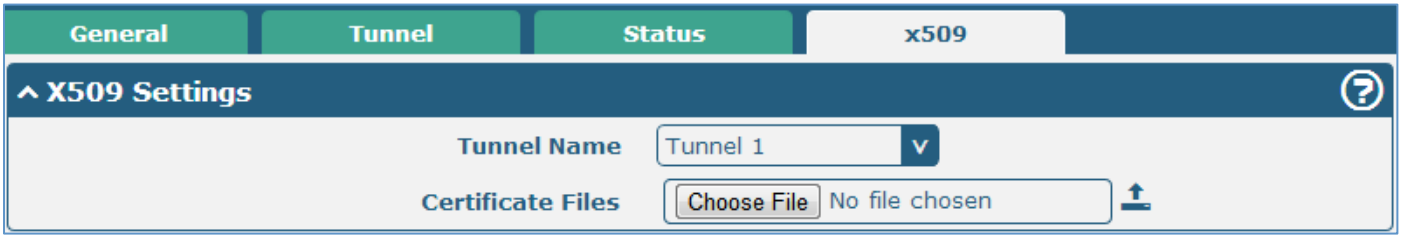
Status

This section allow user to check the status of the IPSec tunnel.



x509

User can upload the X509 certificate for the IPSec tunnel in this section.



x509		
Item	Description	Default
Tunnel Name	Select the name of the tunnel.	Tunnel 1
Certificate Files	Choose the correct file to import the certificate into the router. The correct file format as followings: @ca.crt @remote.crt @local.crt @private.key @crl.pem	Null
Index	Show the index of the certificate file.	Null
Filename	Show the name of the certificate file.	Null
File Size	Show the size of the certificate file.	Null
Last Modification	Show the timestamp of that the last time to modify the certificate file.	Null

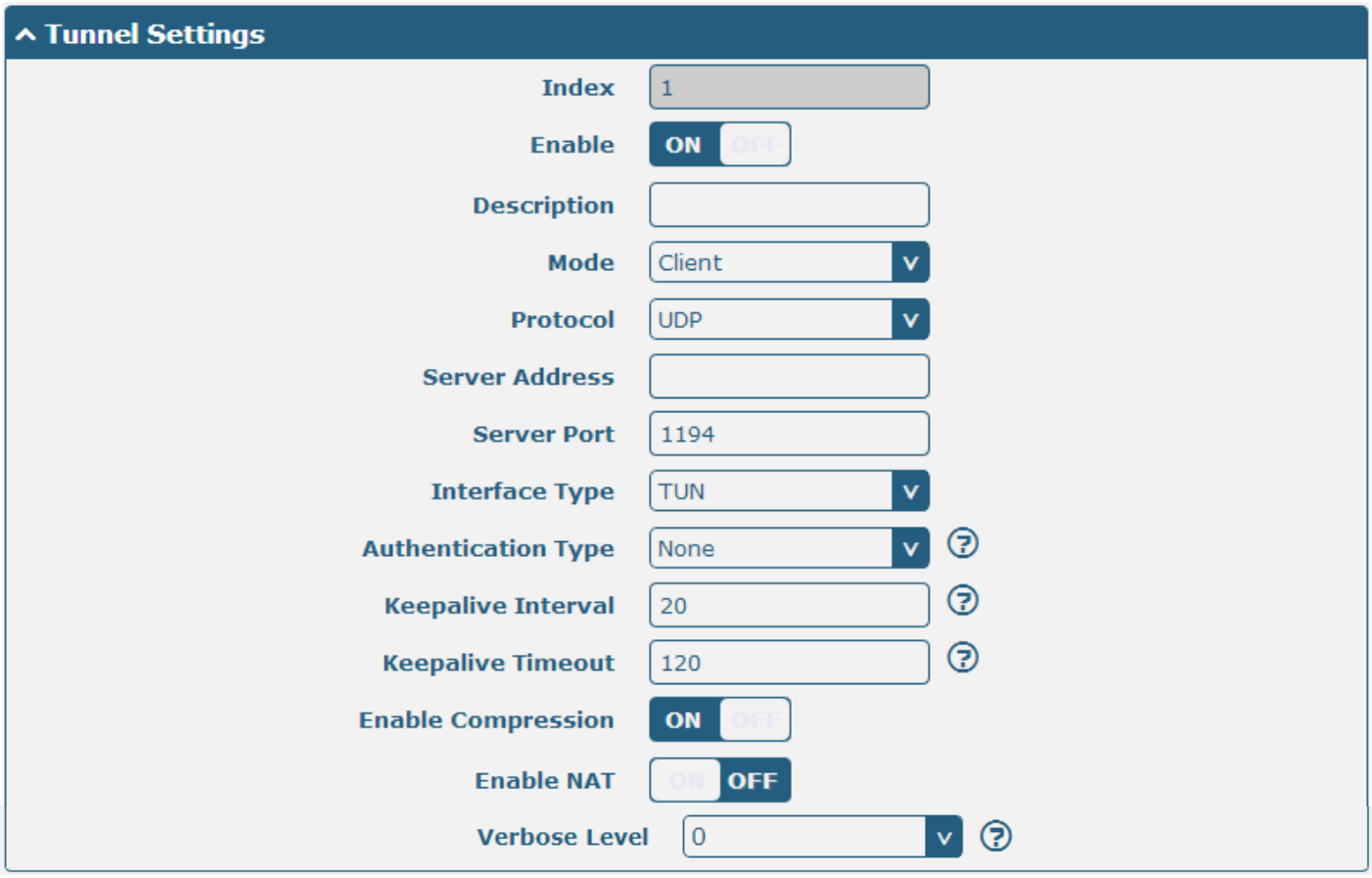
3.16 VPN->OpenVPN

This section allows users to set the OpenVPN and the related parameters.

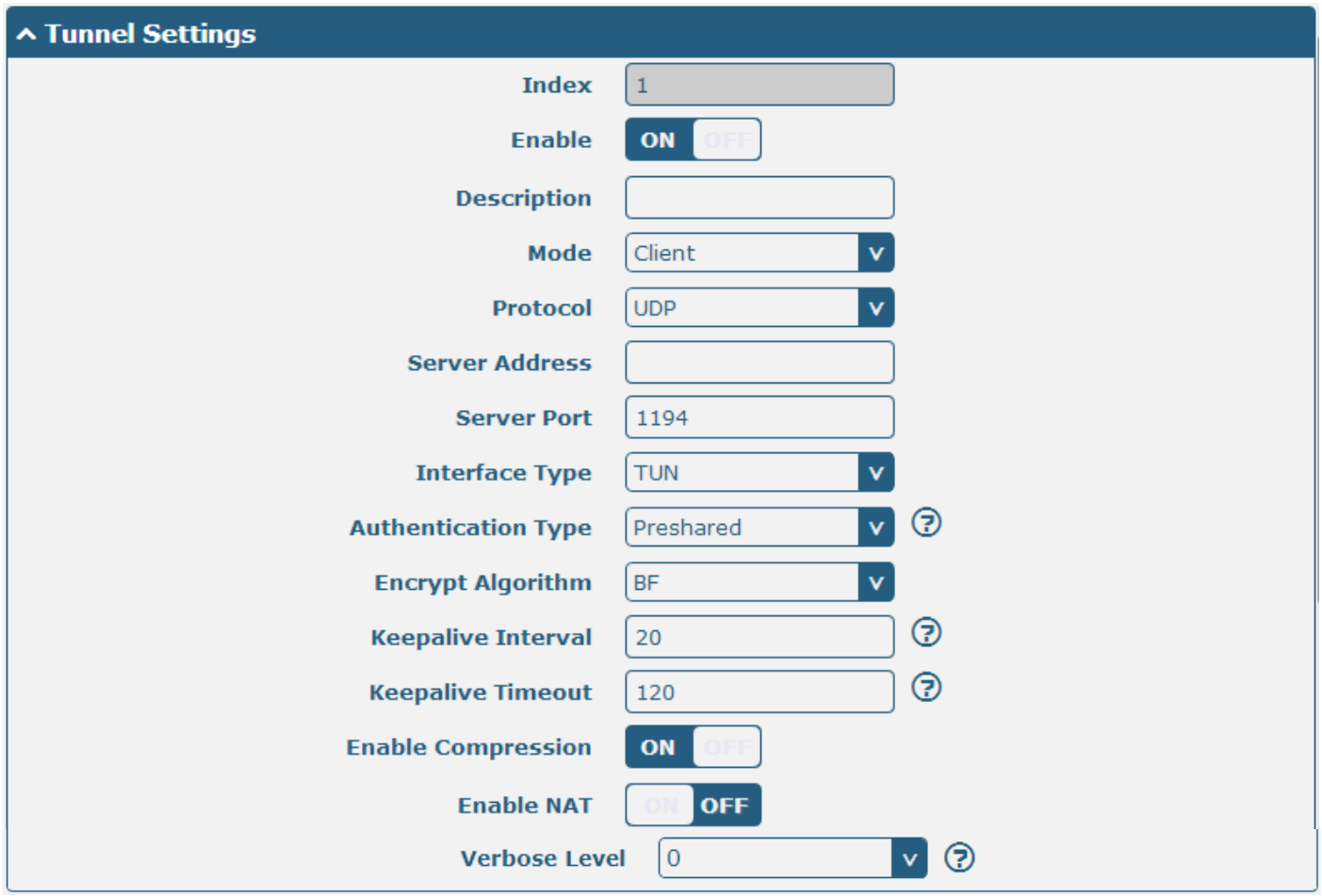
OpenVPN

Click “+” to add tunnel settings. (The maximum number of the tunnel is three.)

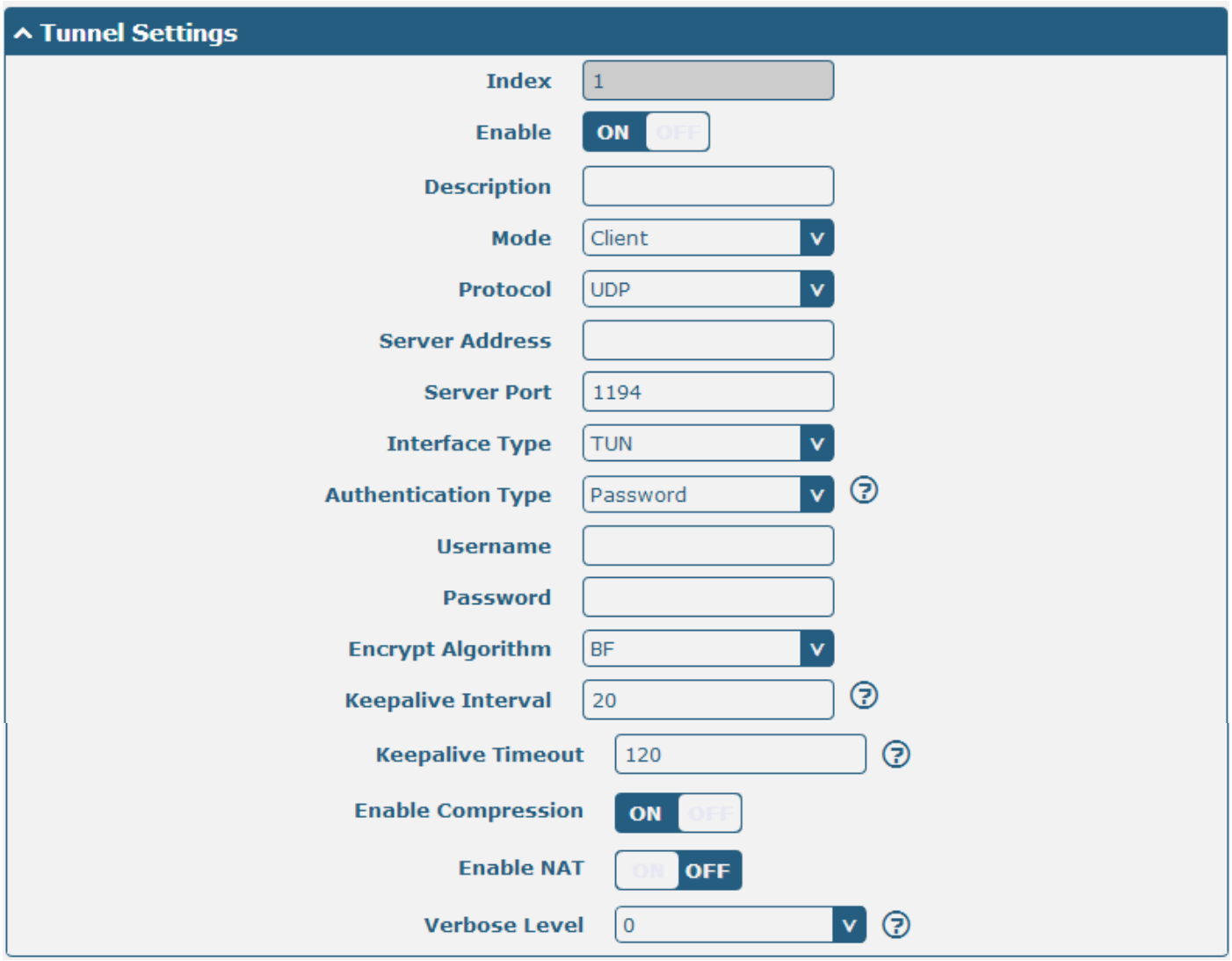
When choose “Authentication Type” to “None”.



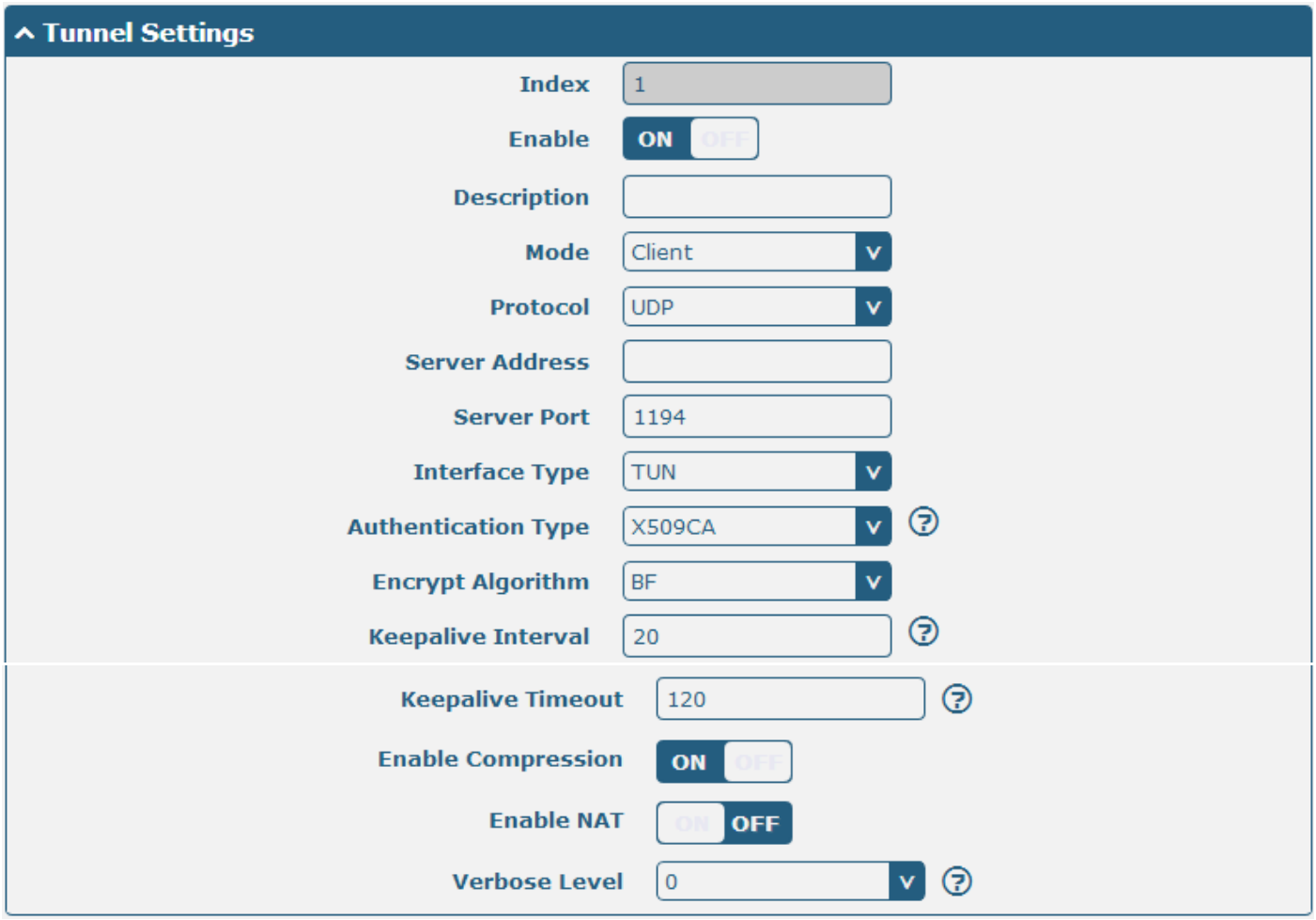
When choose “Authentication Type” to “Preshared”.



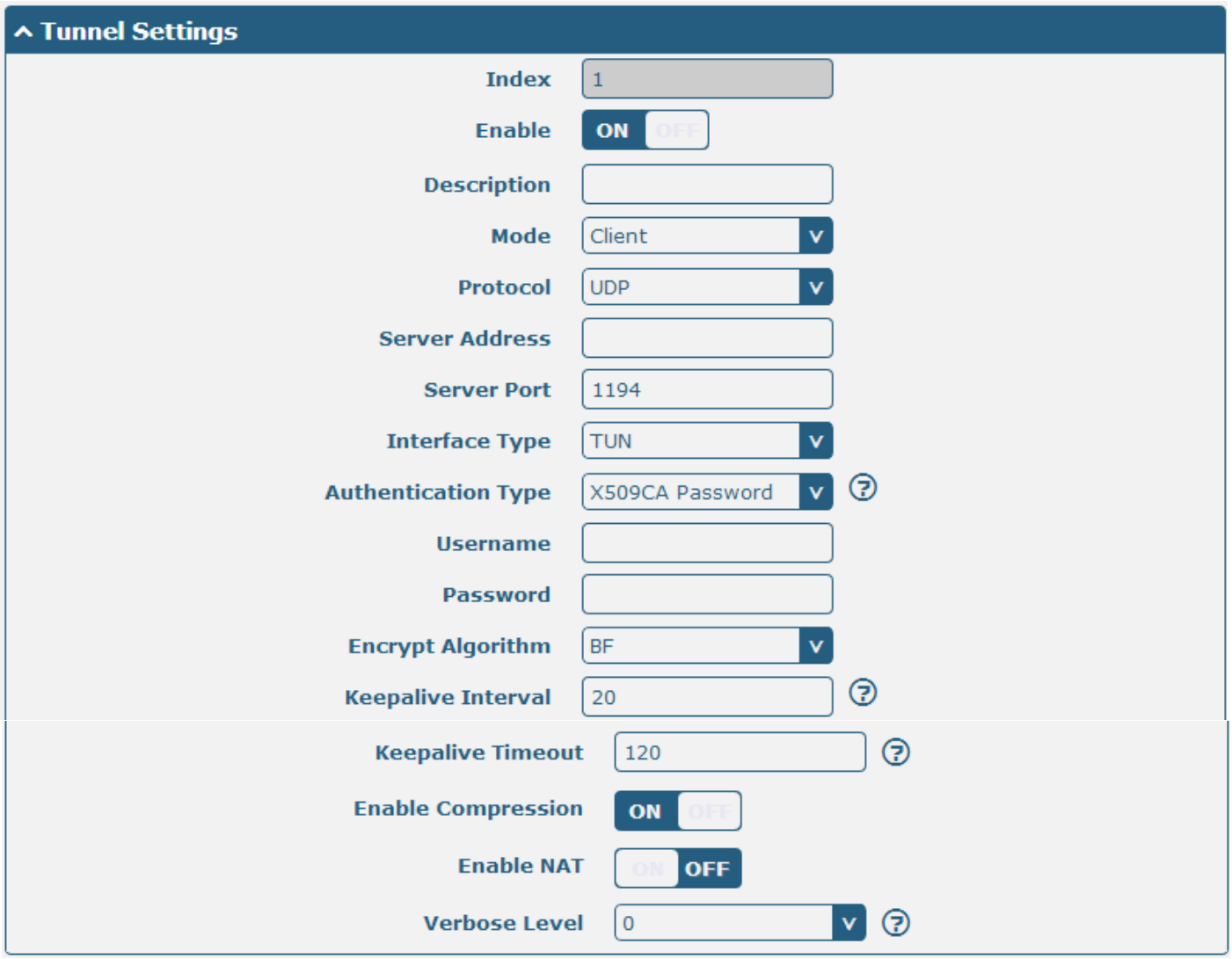
When choose “Authentication Type” to “Password”.



When choose “Authentication Type” to “X509CA”.

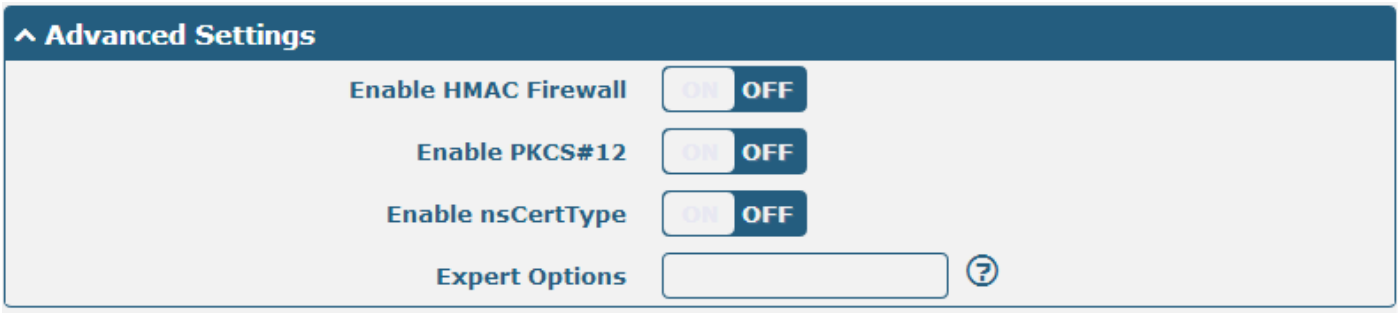


When choose “Authentication Type” to “X509CA Password”.



Tunnel Settings		
Item	Description	Default
Index	Show the index of the tunnel.	1
Enable	Enable OpenVPN tunnel.	ON
Description	Enter some simple words about the OpenVPN Tunnel.	Null
Mode	Select from “P2P”, “Client”.	Client
Protocol	Select from “UDP”, “TCP-Client”.	UDP
Server Address	Enter the OpenVPN server address.	Null
Server Port	Enter the OpenVPN server port	1194
Interface Type	Select from “TUN”, “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 Type	Select from “None”, “Preshared”, “Password”, “X509CA” and “X509CA Password”. “None” and “Preshared” type just work with p2p mode.	None

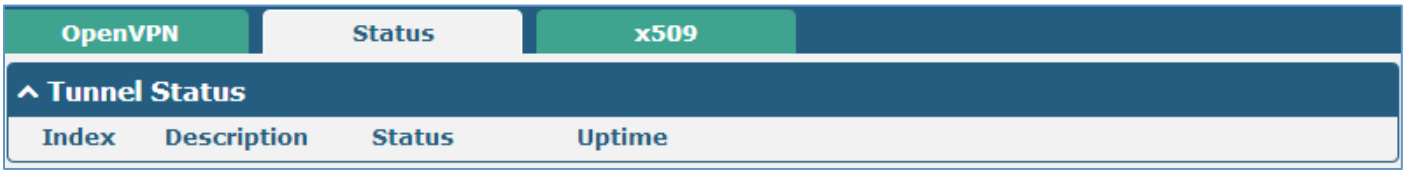
Local IP	When the “Mode” is “P2P”. Define the local IP address of OpenVPN tunnel.	Null
Remote IP	When the “Mode” is “P2P”. Define the remote IP address of OpenVPN tunnel.	Null
Username	User name used for Authentication Type “Password” or “X509CA Password”.	Null
Password	Password used for Authentication Type “Password” or “X509CA Password”.	Null
Encrypt Algorithm	Select from “BF”, “DES”, “DES-EDE3”, “AES128”, “AES192” and “AES256”. BF: Uses the BF algorithm in CBC mode and 128-bit key. DES: Uses the DES algorithm in CBC mode and 64-bit key. DES-EDE3: Uses the 3DES algorithm in CBC mode and 192-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.	BF
Keepalive Interval	Set keepalive (ping) interval to check if the tunnel is active.	20
Keepalive Timeout	Trigger OpenVPN restart after n seconds pass without reception of a ping or other packet from remote.	120
Private Key Password	Password of Private Key for Authentication Type “X509CA”	Null
Enable Compression	Enable to compress the data stream.	ON
Enable NAT	Tick to enable NAT for OpenVPN. The source IP address of host behind 4G INDUSTRIAL VPN will be disguised before accessing the remote OpenVPN client.	OFF
Verbose Level	Select the level of the output log. Values range from 0 to 11. 0 -- No output except fatal errors. 1 to 4 -- Normal usage range. 5 -- Output R and W characters to the console for each packet read and write. 6 to 11 -- Debug info range	0



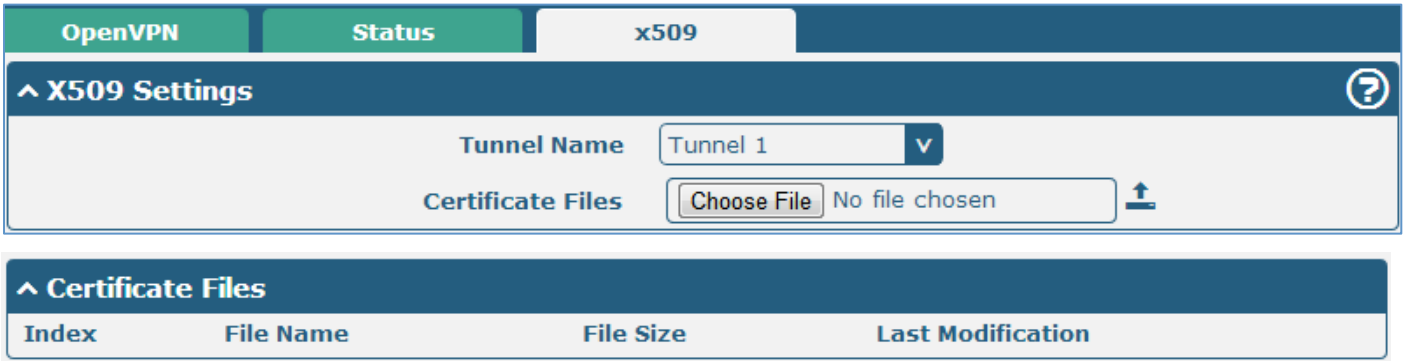
Advanced Settings		
Item	Description	Default
Enable HMAC Firewall	Add an additional layer of HMAC authentication on top of the TLS control channel to protect against DoS attacks.	OFF
Enable PKCS#12	Enable the PKCS#12 certificate. It is an exchange of digital certificate encryption standard, used to describe personal identity information.	OFF

Enable nsCertType	Require that peer certificate was signed with an explicit nsCertType designation of "server".	OFF
Expert Options	You can enter some other options of OpenVPN in this field. Each expression can be separated by a ';'.	Null

Status



x509

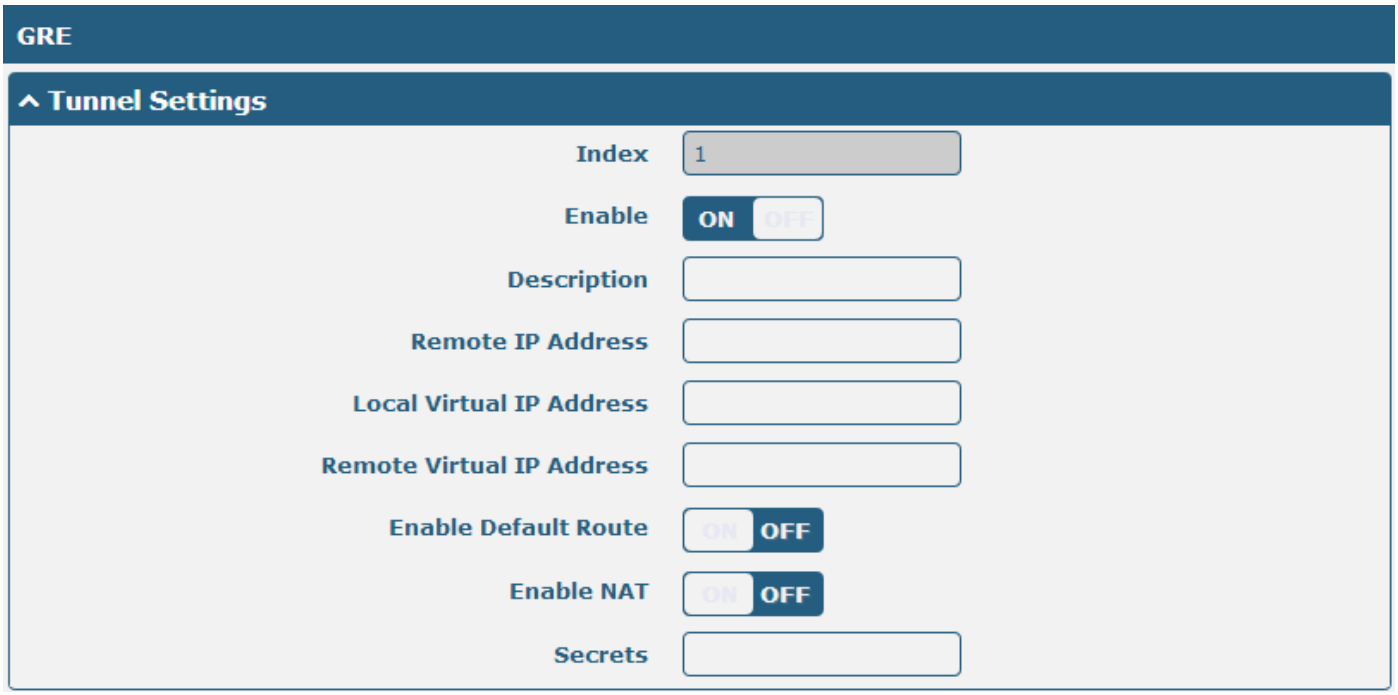


x509		
Item	Description	Default
Tunnel Name	Select the name of the Tunnel1 to Tunnel3. Because the maximum number of the tunnel is three.	Tunnel 1
Certificate Files	Choose the correct file to import the certificate into the router. The correct file format as followings: @ca.crt @remote.crt @local.crt @private.key @crl.pem	Null
Index	Show the index of the certificate file.	Null
Filename	Show the name of the certificate file.	Null
File Size	Show the size of the certificate file.	Null
Last Modification	Show the timestamp of that the last time to modify the certificate file.	Null

3.15 VPN->GRE

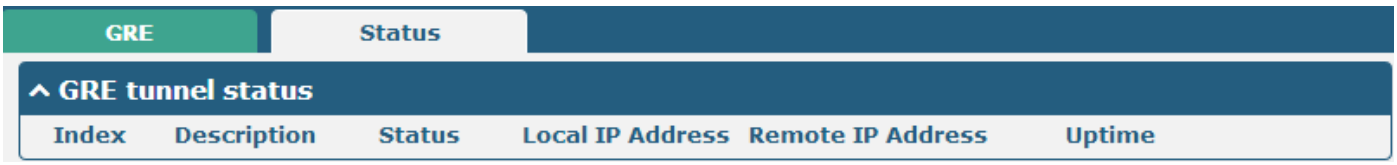
This section allows users to set the OpenVPN and the related parameters.

Click “ ” to add tunnel settings. (The maximum number of the tunnel is three.)



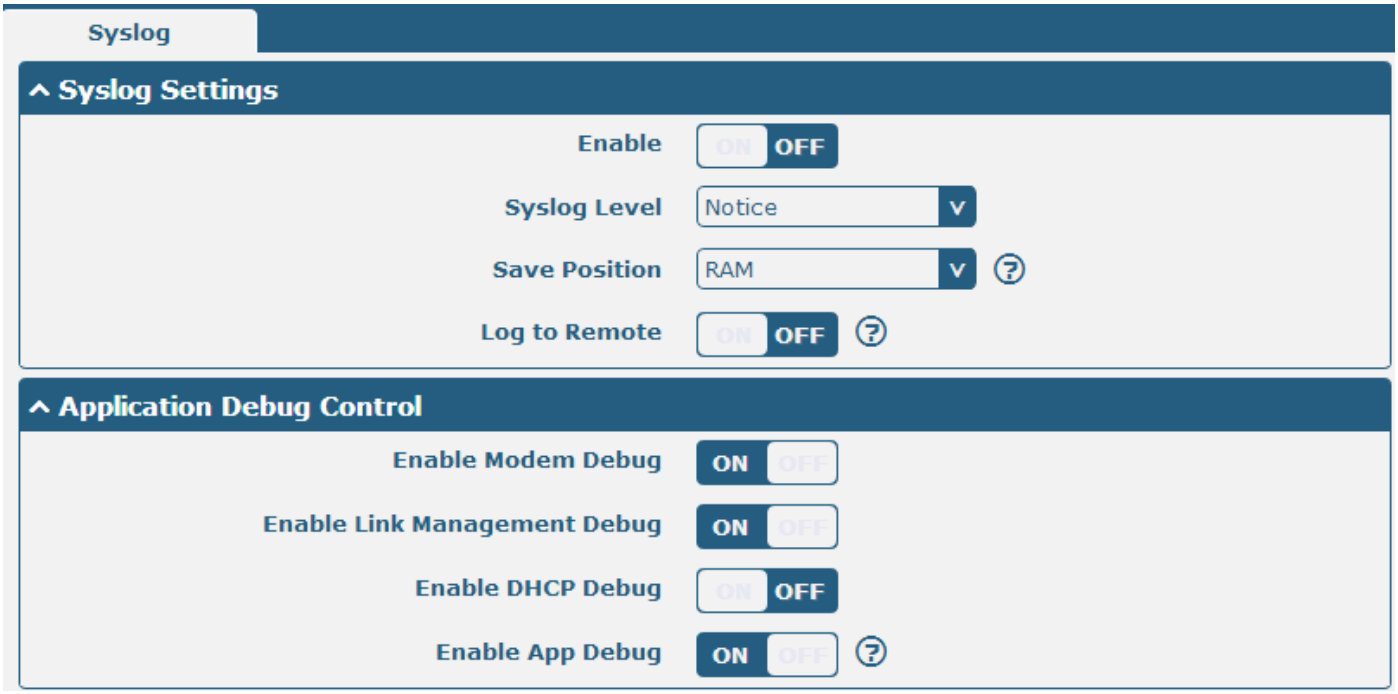
GRE		
Item	Description	Default
Index	Show the index of the tunnel.	1
Enable	Enable GRE tunnel. GRE (Generic Routing Encapsulation) is a protocol that encapsulates packets in order to route other protocols over IP networks.	ON
Description	Enter some simple words about the GRE Tunnel.	Null
Remote IP Address	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
Enable Default Route	All the traffics of 4G INDUSTRIAL VPN router will go through the GRE VPN.	OFF
Enable NAT	Tick to enable NAT for GRE. The source IP address of host Behind 4G INDUSTRIAL VPN will be disguised before accessing the remote GRE server.	Disable
Secrets	Set Tunnel Key of GRE.	Null

This section allow user to check the status of GRE tunnel.



3.16 Services->Syslog

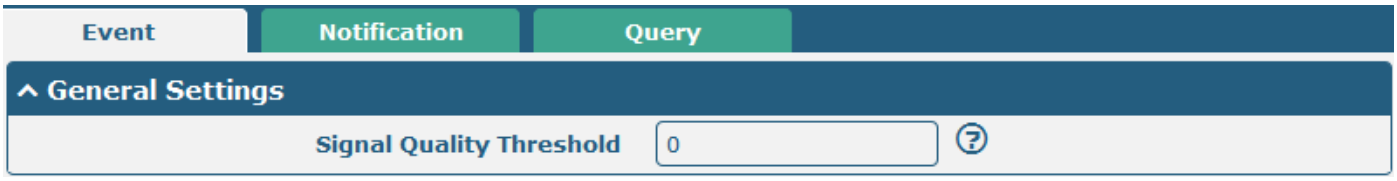
This section allows users to set the syslog parameters.



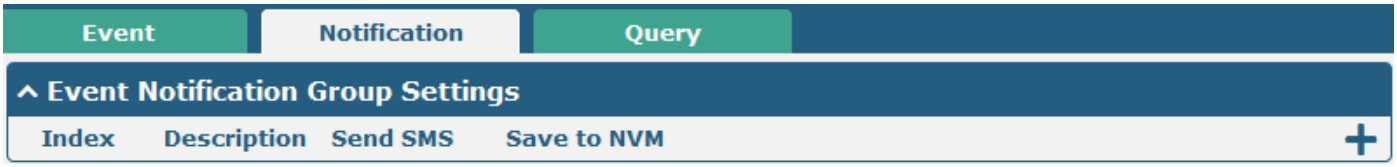
Syslog		
Syslog Settings		
Item	Description	Default
Enable	Click to enable Syslog setting.	OFF
Syslog Level	Select form “Debug”, “Info”, “Notice”, “Warning”, “Error” which from low to high. The lower level will output more syslog in detail.	Notice
Save Position	Select the save position from “RAM”, “NVM” and “Console”. Choose “RAM”, the data will be cleared after reboot. But it's not recommended that saving syslog to NVM (Non-Volatile Memory) for a long time.	RAM
Log to Remote	Enable to allow router sending syslog to the remote syslog server. You need to enter the IP and Port of the syslog server.	OFF
Application Debug Control		
Enable Modem Debug	Click to enable router to debug Modem.	ON
Enable Link Management Debug	Click to enable router to debug Link Management.	ON
Enable DHCP Debug	Click to enable router’s debug control for DHCP.	OFF
Enable APP Debug	Click to enable router’s debug control for all other applications.	ON

3.17 Services->Event

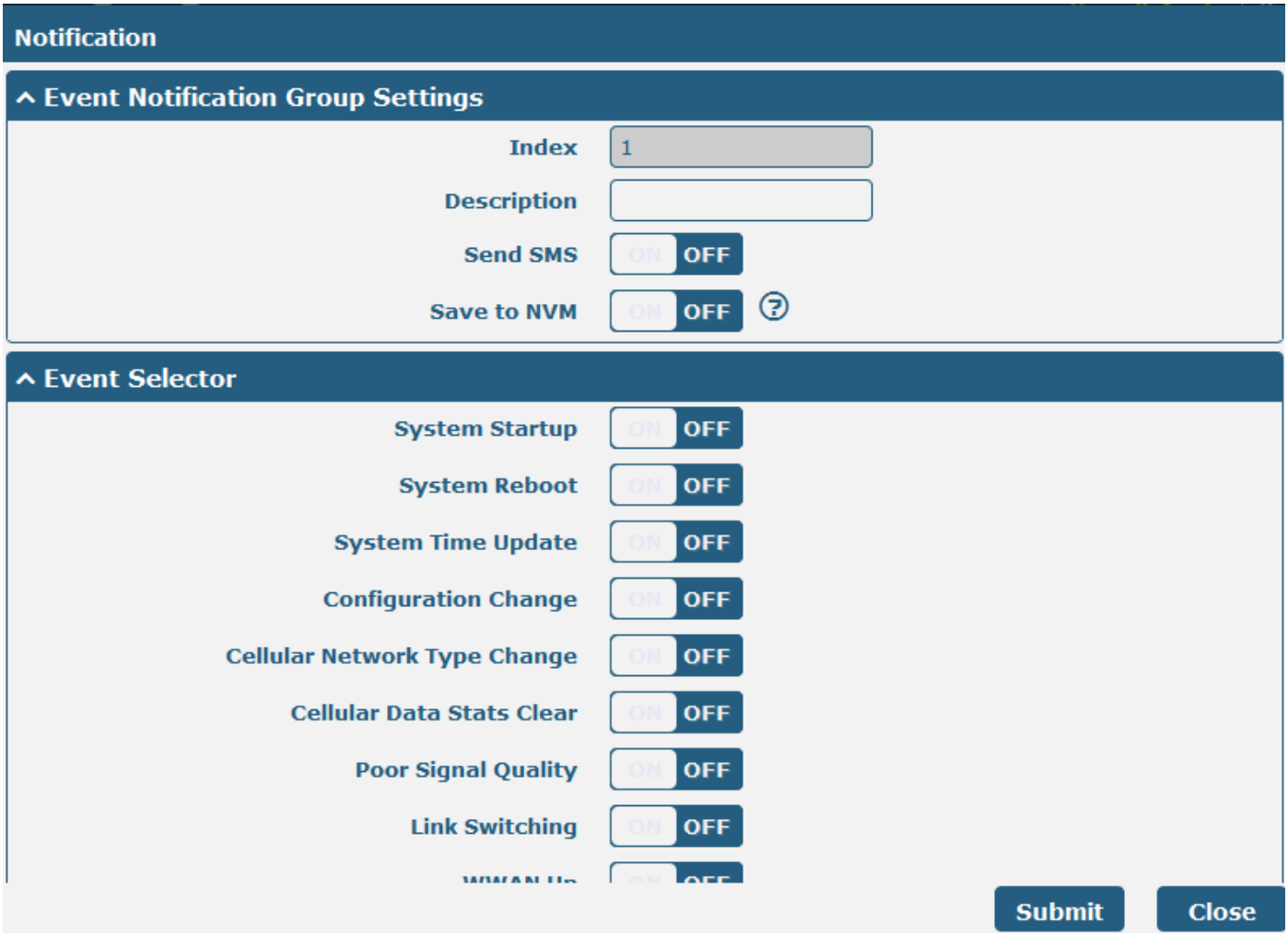
This section allows users to set the Event parameters.



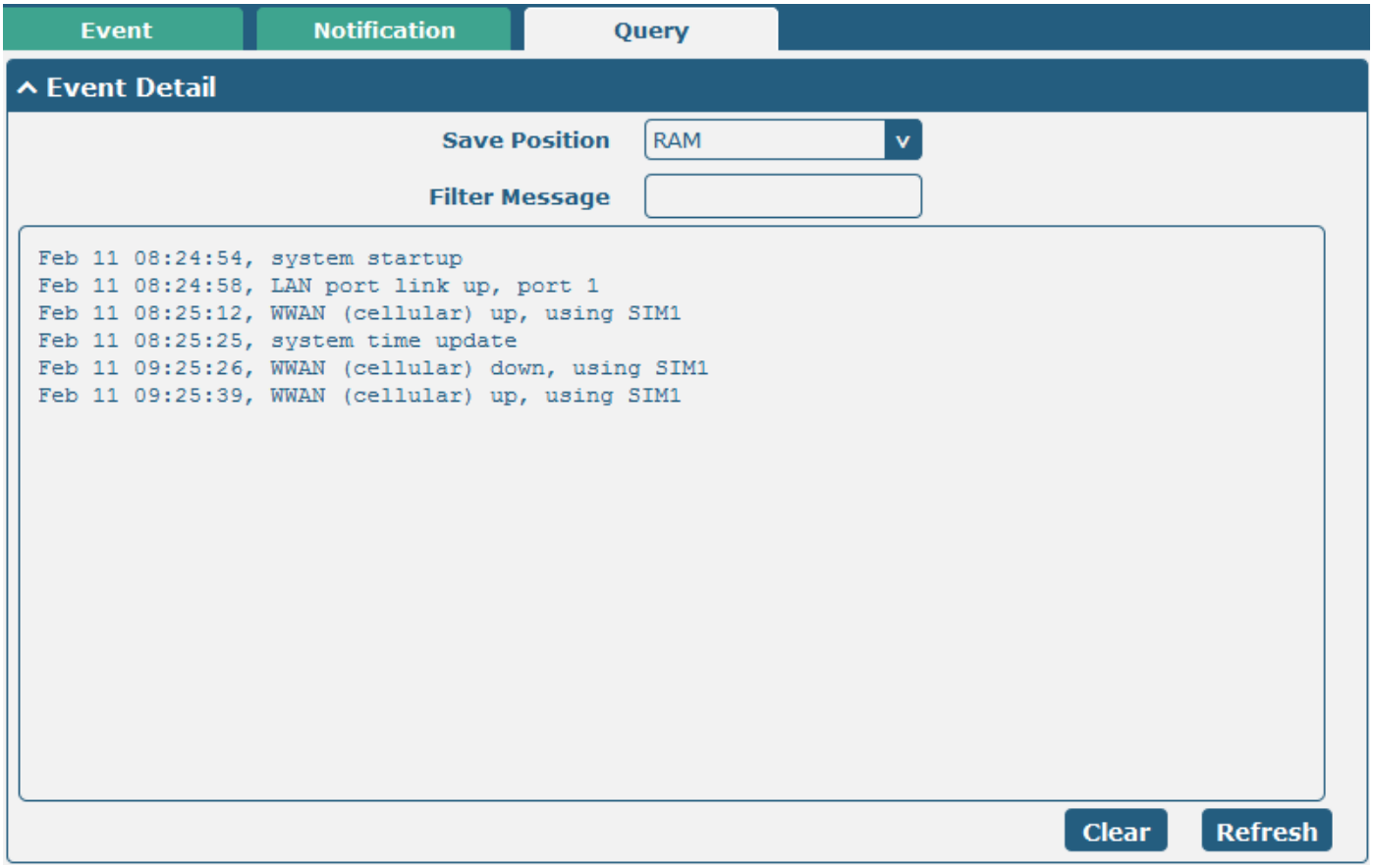
Event @ Event		
Item	Description	Default
Signal Quality Threshold	Router will generate log event when signal quality less than the threshold, 0 means disable.	0



Click “ + ” button to add an Event parameters.

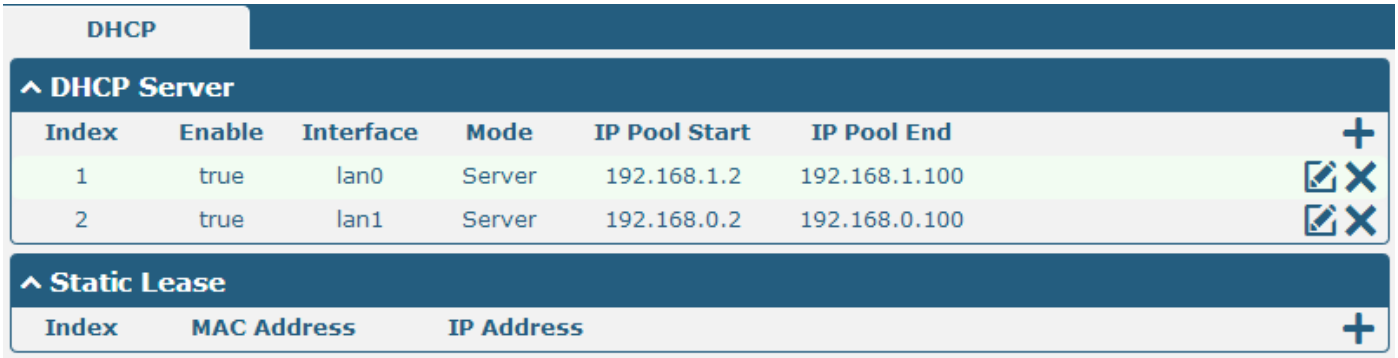


Notification@ Event		
Item	Description	Default
Index	The index of event notification group.	1
Description	Enter some simple words to describe the Notify Group.	Null
Sent SMS	Click to enable router to send event notification SMS. Set the phone number that is used for receiving event notification, and use ';'to separate each number.	OFF
Save to NVM	Click to enable router to save event to nonvolatile memory.	OFF
Event Selector	Click to enable Event feature. There are numbers of 4G INDUSTRIAL VPN's main running event code you can select, such as "System Startup", "System Reboot", "System Time Update", etc.	OFF



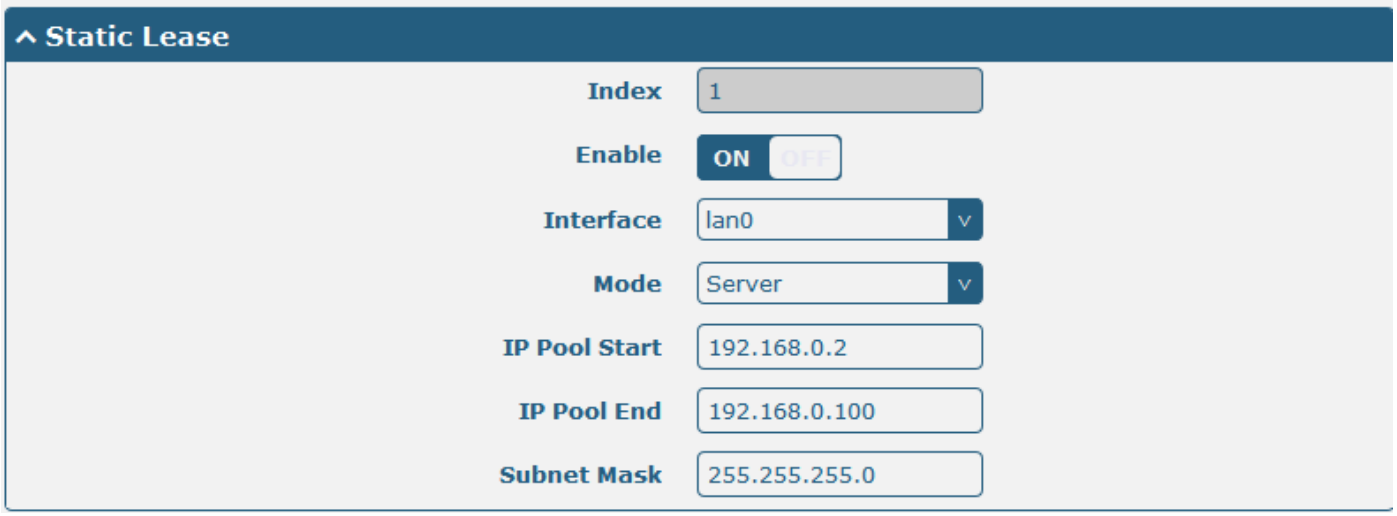
Query @ Event		
Item	Description	Default
Save Position	Select the events' save position from "RAM", "NVM". RAM: Random-access memory. NVM: Non-Volatile Memory.	RAM
Filter Message	Event will be filtered according to the Filter Message that the user set. Click the Refresh button, the filtered event will be displayed in the follow box. Use "&" to separate more than one filter message, such as message1&message2.	Null

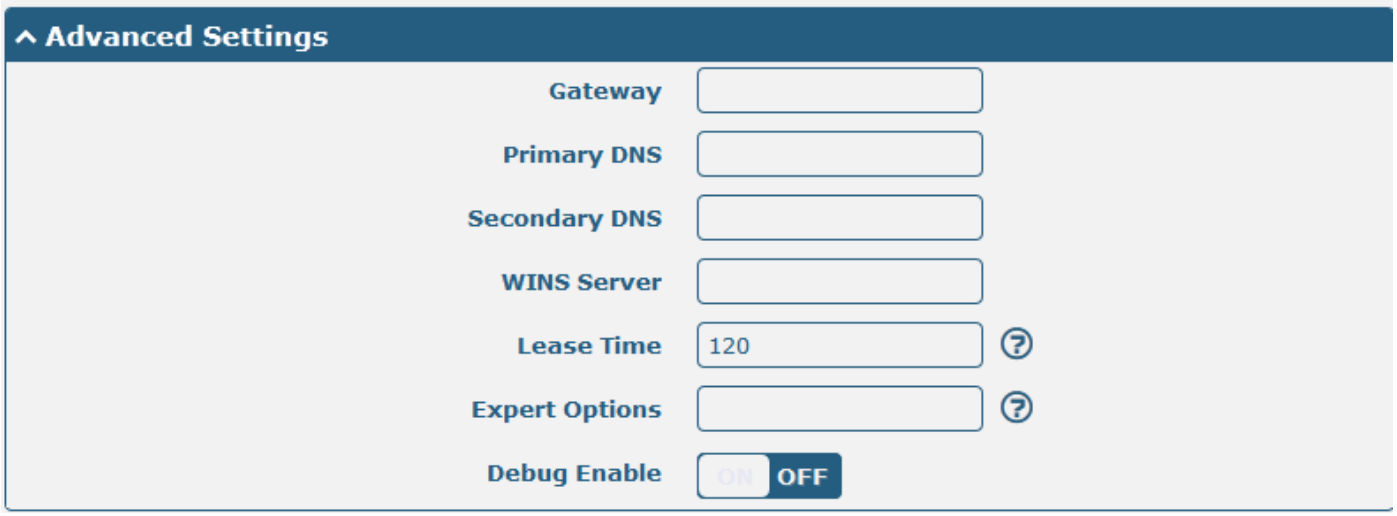
3.18 Services->DHCP



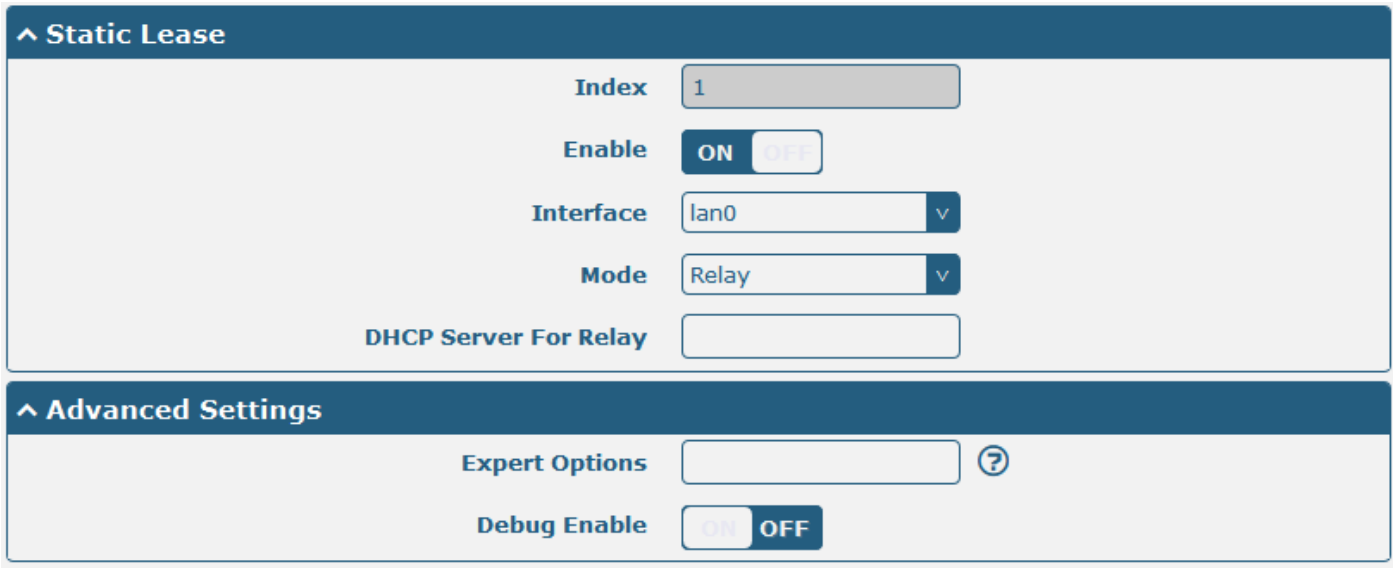
Click button to modify the parameter DHCP server.

When choose DHCP Mode as server.

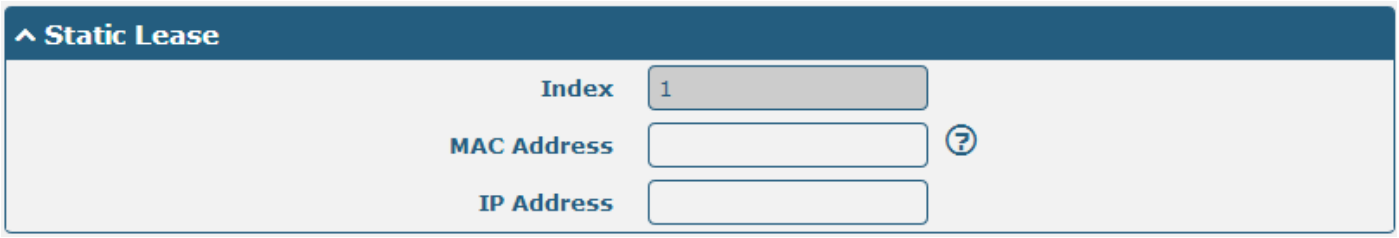




When choose DHCP Mode as Relay.



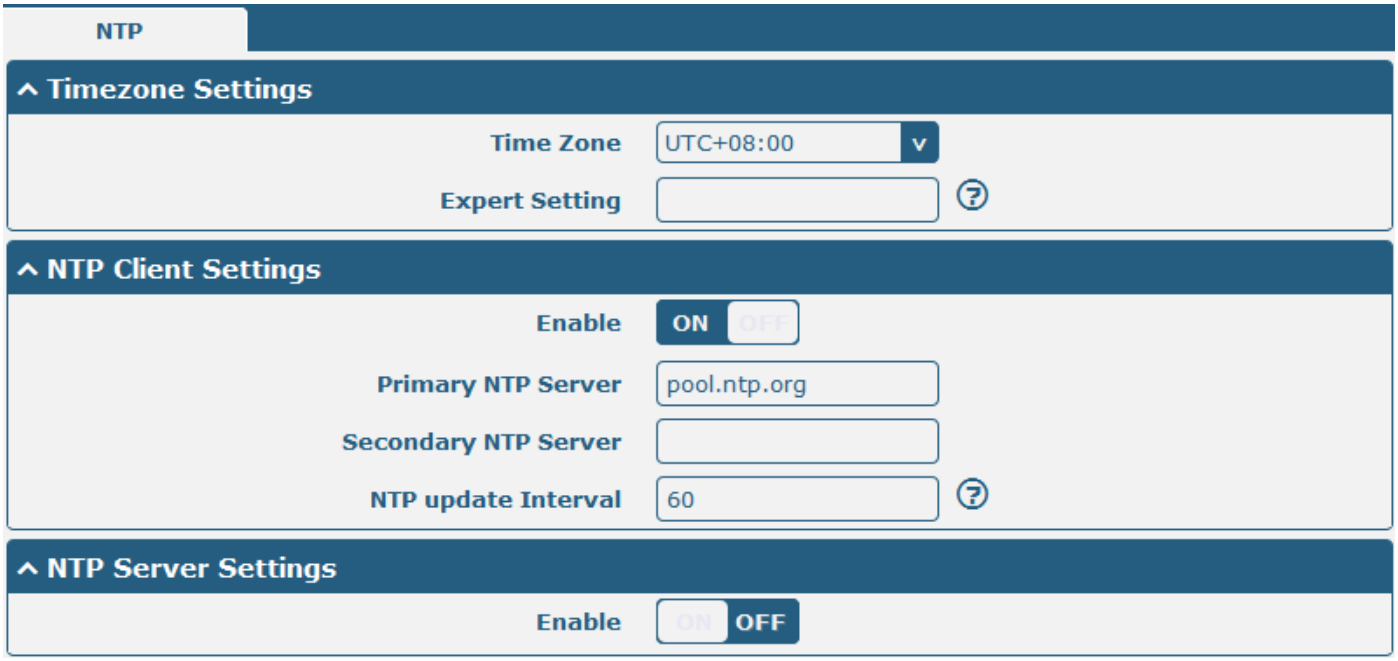
Click “ ” to add static lease.



DHCP		
Item	Description	Default
Enable	Enable DHCP as DHCP Server or DHCP Relay.	ON
Interface	Select from lan0 or lan1.	lan0
Mode	Server: Lease IP address to DHCP clients which connect to LAN. Relay: 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.	DHCP Server
DHCP Server for Relay	Enter the DHCP Relay server IP address.	Null
IP Pool Start	Define the beginning of the pool of IP addresses which will lease to DHCP clients.	192.168.0.2
IP Pool End	Define the end of the pool of IP addresses which will lease to DHCP clients.	192.168.0.100
Subnet Mask	Define the Subnet Mask which the DHCP clients will obtain from DHCP server.	255.255.255.0
Gateway	Define the Gateway which the DHCP clients will obtain from DHCP server.	Null
Primary DNS	Define the Primary DNS Server which the DHCP clients will obtain from DHCP server.	Null
Secondary DNS	Define the Secondary DNS Server which the DHCP clients will obtain from DHCP server.	Null
WINS Server	Define the Windows Name Server which the DHCP clients will obtain from DHCP server.	Null
Lease Time	Define the time which the client can use the IP address which obtained from DHCP server.	120
Expert Options	You can enter some other options of DHCP server in this field. format: config-desc;config-desc, e.g. log-dhcp;quiet-dhcp	Null
Debug Enable	Enable this function; it will output the DHCP information to syslog.	OFF
Index	Show the index of the static lease.	1
MAC Address	Define the MAC address which can obtain statically leased IP address.	Null
IP Address	Define the IP address which conforms to MAC address of the connected equipment.	Null

3.19 Services->NTP

This section allows users to set the NTP parameters.

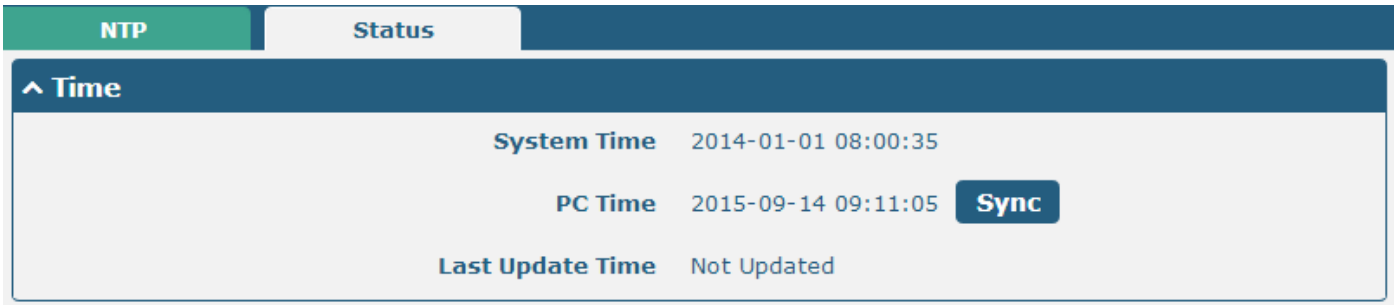


Timezone Settings @ NTP		
Item	Description	Default
Time Zone	Select your local time zone.	UTC +08:00
Expert Setting	Specify the time zone with Daylight Saving Time in TZ environment variable format. The Time Zone option will be ignored in this case.	Null
NTP Client Setting @ NTP		
Enable	Click to enable the router to synchronize time from NTP server. ***Note:*** *4G INDUSTRIAL VPN doesn't have the RTC, so NTP client function must always be ON.*	ON
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
NTP Update interval	Enter the interval (minutes) which NTP client synchronize the time from NTP server. Minutes wait for next update, 0 means update only once.	0
NTP Client Setting @ NTP		
Enable	Click to enable the NTP server function of router.	OFF

The status part of NTP allows user to check the current time of 4G INDUSTRIAL VPN and also synchronize the router time with PC.

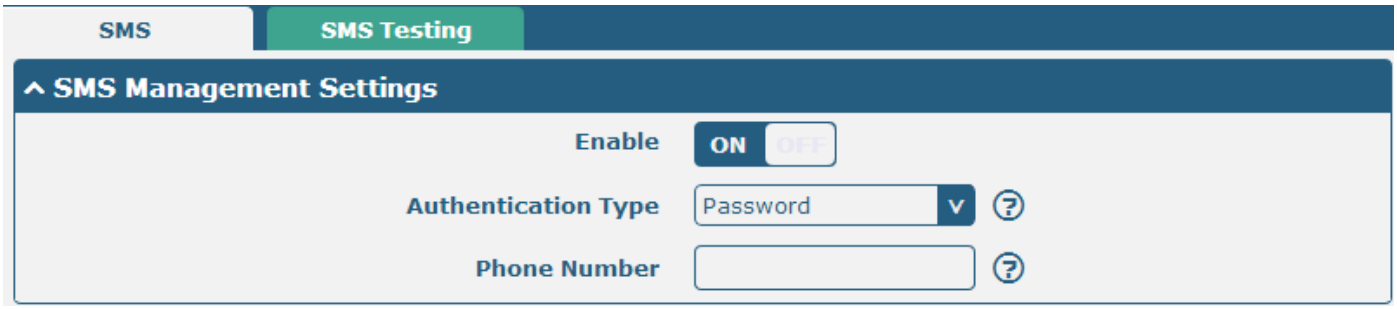
Click 

button to make the router time synchronize with PC.



3.20 Services->SMS

This section allows users to set the SMS parameters.



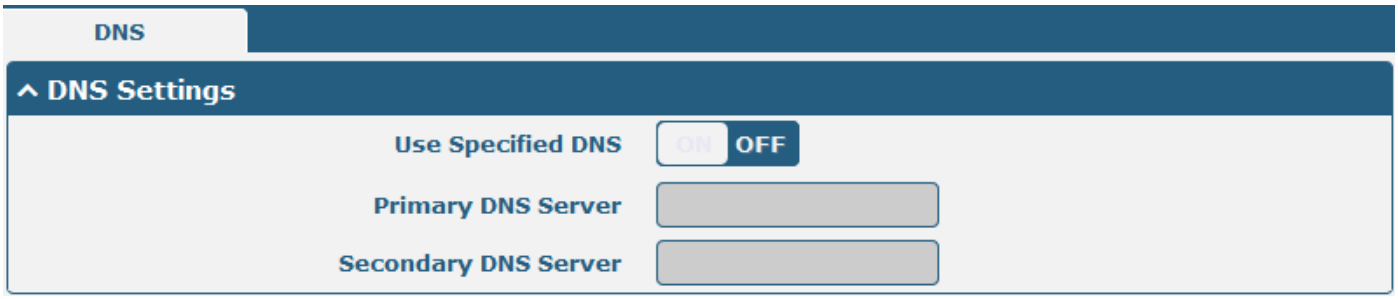
SMS		
Item	Description	Default
Enable SMS Management	Click to enable SMS Management function.	ON
Authentication Type	Select Authentication Type from “Password”, “Phonenum”, “Both”. Password: use the same username and password as WEB manager for authentication. For example, the format of the SMS should be “username: password; cmd1; cmd2; …” ***Note:*** *Set the WEB manager password in* ***System->User Management*** *section.* Phonenum: use the Phone number for authenticating, user should set the Phone Number that is allowed for SMS management. The format of the SMS should be “cmd1; cmd2; …” Both: use both the “Password” and “Phonenum” for authentication. User should set the Phone Number that is allowed for SMS management. The format of the SMS should be “username: password; cmd1; cmd2; …”	Password
Phone Number	Set the Phone Number that is allowed for SMS management, and use ‘; ‘to separate each number.	Null

User can test the current SMS service whether it is available in this section.

SMS Testing		
Item	Description	Default
Phone Number	Enter the specified phone number which will receive the SMS from 4G INDUSTRIAL VPN router.	Null
Message	Enter the message that 4G INDUSTRIAL VPN router will sent it to the specified phone number.	Null
Result	The result of the SMS test will display in the result box.	Null

3.21 Services->DNS

This section allows users to set the DNS parameters.

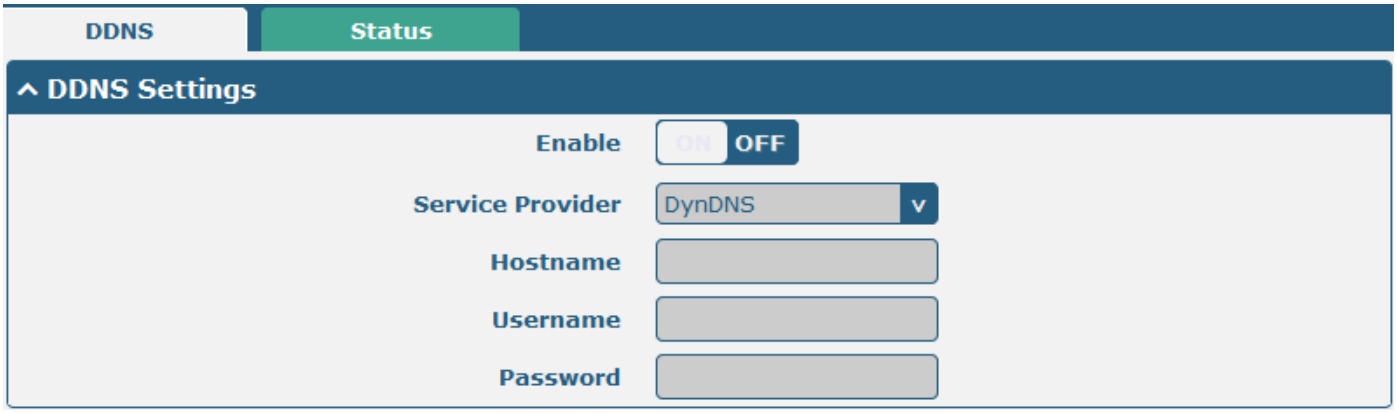


DNS		
Item	Description	Default
Enable Specified DNS	Click to enable DNS function.	OFF
Primary DNS Server	Define the primary DNS Server which the clients will obtain from DHCP server.	Null
Secondary DNS Server	Define the secondary DNS Server which the clients will obtain from DHCP server.	Null

3.22 Services->DDNS

This section allows users to set the DDNS parameters.

The Dynamic DNS function allows you to alias a dynamic IP address to a static domain name, allows 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.

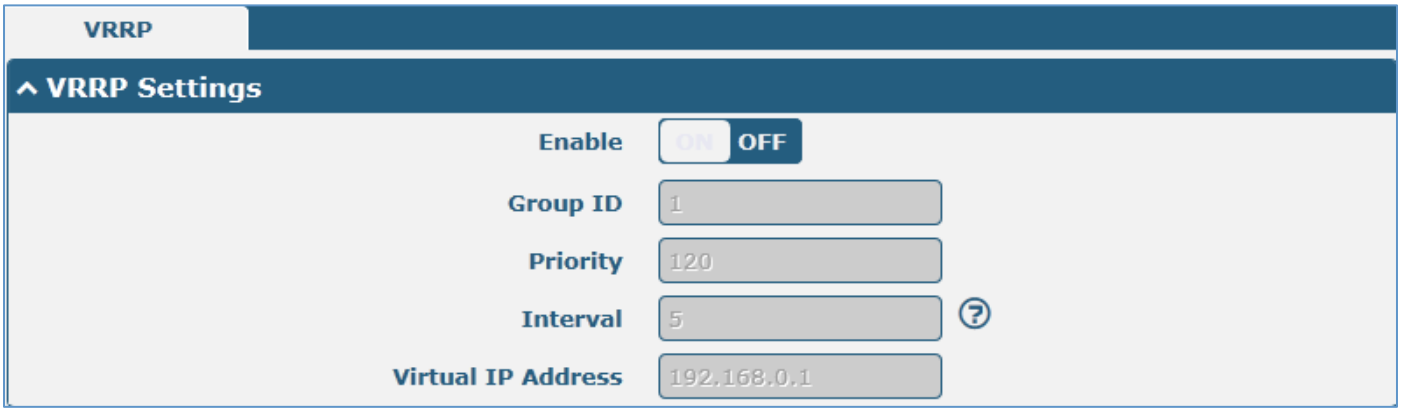


DDNS		
Item	Description	Default
Enable	Click to enable DDNS function.	OFF
Service Provider	Select the DDNS service from “DynDNS”, “NO-IP”, “3322”. ***Note:*** the DDNS service only can be used after registered by Corresponding service provider.	DynDNS
Hostname	Enter the Host name of the DDNS server provided.	Null
Username	Enter the user name of the DDNS server provided.	Null
Password	Enter the password of the DDNS server provided.	Null

Status		
Item	Description	Default
Status	Show current status of DDNS service.	Null
Last Update Time	Show the time that DDNS updated successfully at last time.	Null

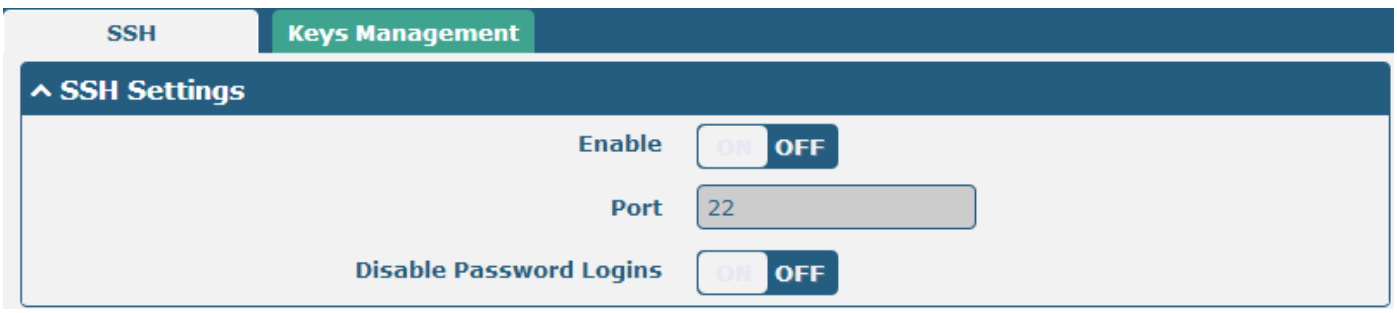
3.23 Services->VRRP

This section allows users to set the VRRP parameters.



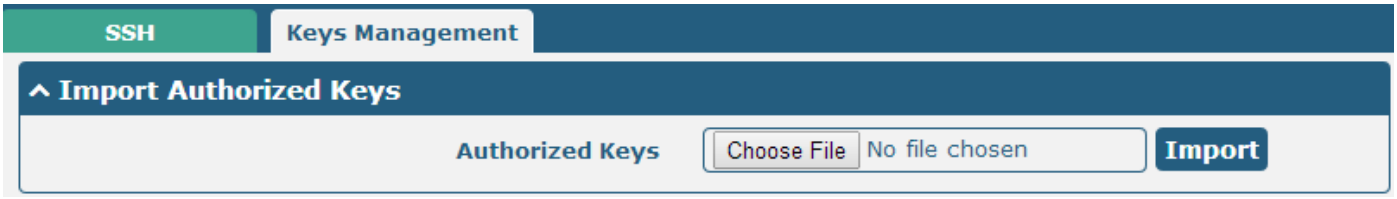
VRRP		
Item	Description	Default
VRRP	VRRP (Virtual Router Redundancy Protocol) is an Internet protocol that provides a way to have one or more backup routers when using a statically configured router on a local area network (LAN).Using VRRP, a virtual IP address can be specified manually.	Null
Enable	Click to enable VRRP protocol.	OFF
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.	120
Interval	The interval that master router sends VRRP packets to backup routers.	5
Virtual IP Address	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

3.24 Services->SSH



SSH		
Item	Description	Default

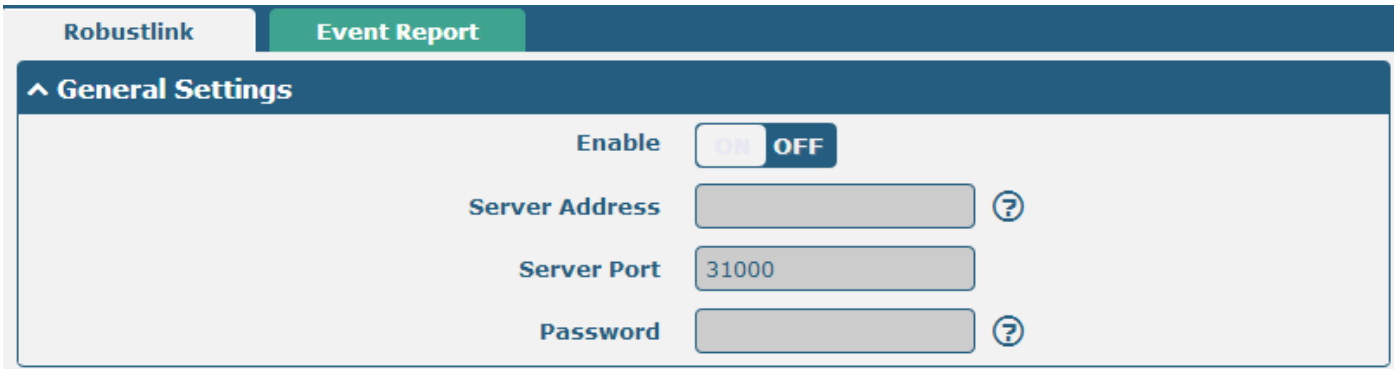
Enable	Enable the function that user can access 4G INDUSTRIAL VPN Router via SSH.	OFF
Port	Set the port of the SSH access.	22
Disable Password Logins	Switch to “ON” and disable password logins, so that user cannot access 4G INDUSTRIAL VPN via SSH. In this situation, you should import the authorized key into 4G INDUSTRIAL VPN in **Keys Management** part for accessing 4G INDUSTRIAL VPN. Switch to “OFF”, you can access 4G INDUSTRIAL VPN via SSH normally.	OFF



Keys Management	
Item	Description
Authorized Keys	Effective when **SSH->Disable Password Logins** is “ON”. Select a key file from PC, then click **Import** button to import the key file in 4G INDUSTRIAL VPN. So that you can access 4G INDUSTRIAL VPN via SSH without password.

3.25 Services->CloudLink (optional APP)

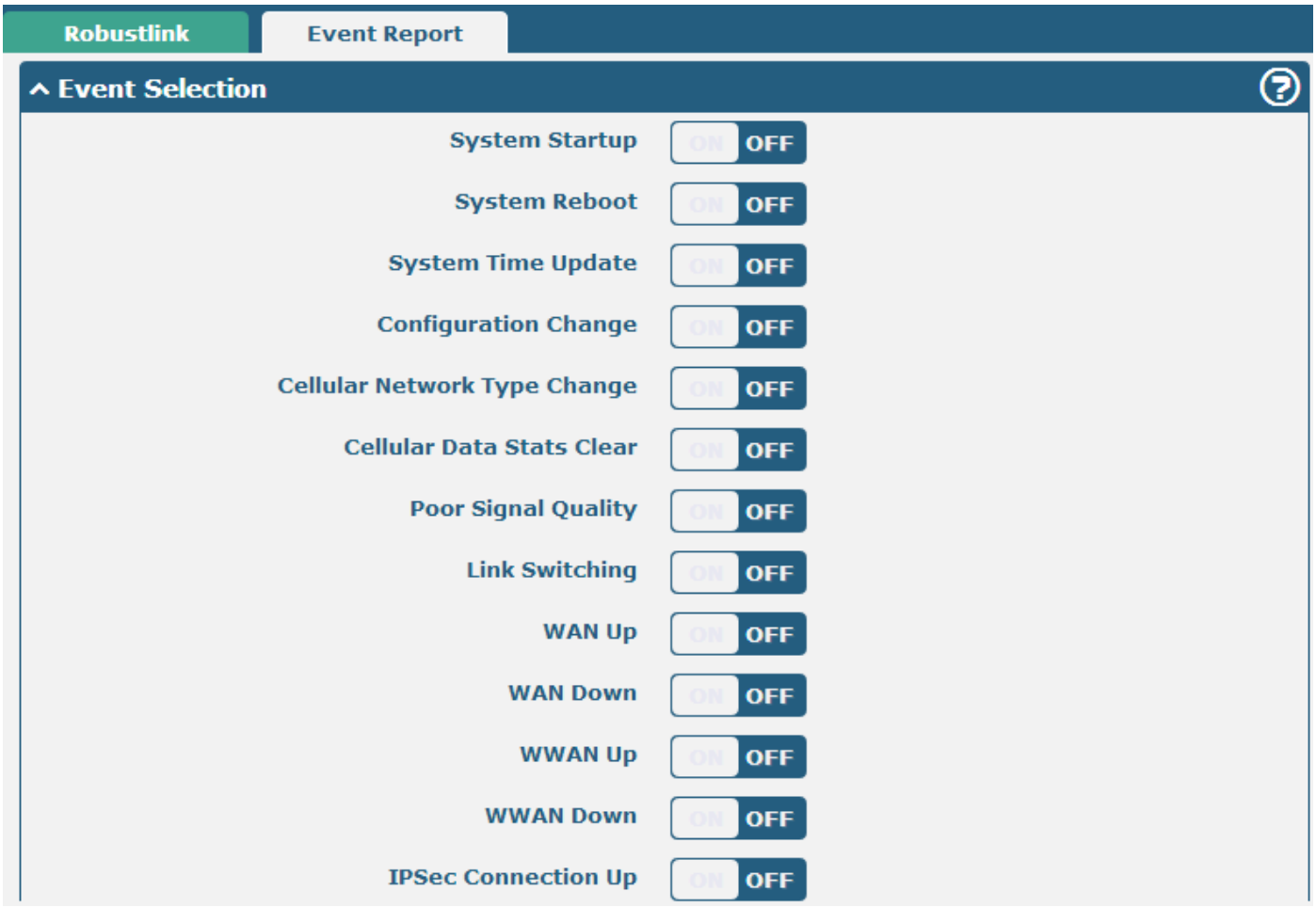
CloudLink is a M2M management platform, which is developed independently by the Digicom Company. 4G INDUSTRIAL VPN can be managed by CloudLink. User can set the relative parameters in this section. This function is as an APP which needs to install into 4G INDUSTRIAL VPN in **System->APP Center** unit.



CloudLink		
Item	Description	Default
Enable	Switch to ON to enable the CloudLink.	
Server address	Enter IP address or domain name of CloudLink.	Null
Port	Enter port number of CloudLink.	31000
Password	Enter the password preset in CloudLink.	Null

	Valid characters: a-z, A-Z, 0-9, @, ., -, #, $, *. *Note: The passwords set in 4G INDUSTRIAL VPN and CloudLink need to be the same.*	

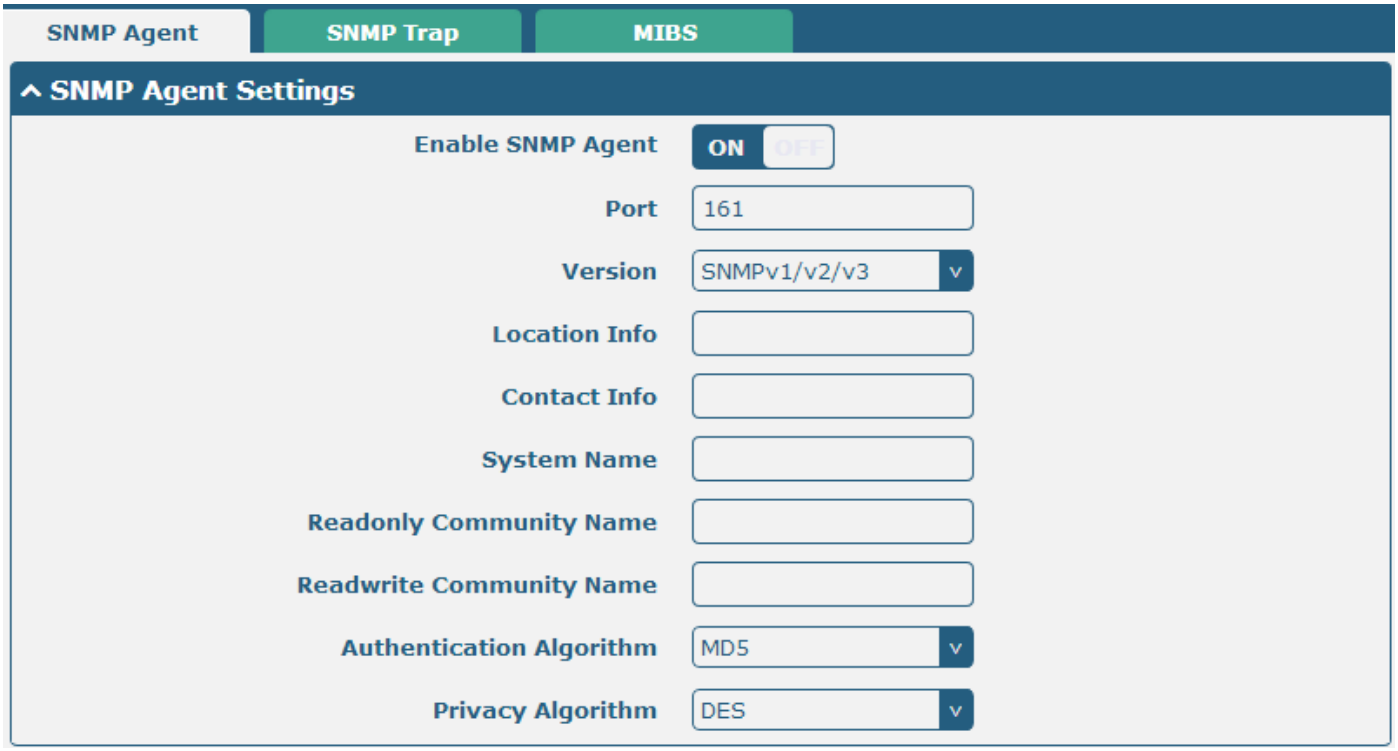
4G INDUSTRIAL VPN support report the Event which has happened to CloudLink platform. In this section, user can select the events those will be reported to CloudLink.



Event Report	
Item	Description
Events	Switch “ON” to enable the event.

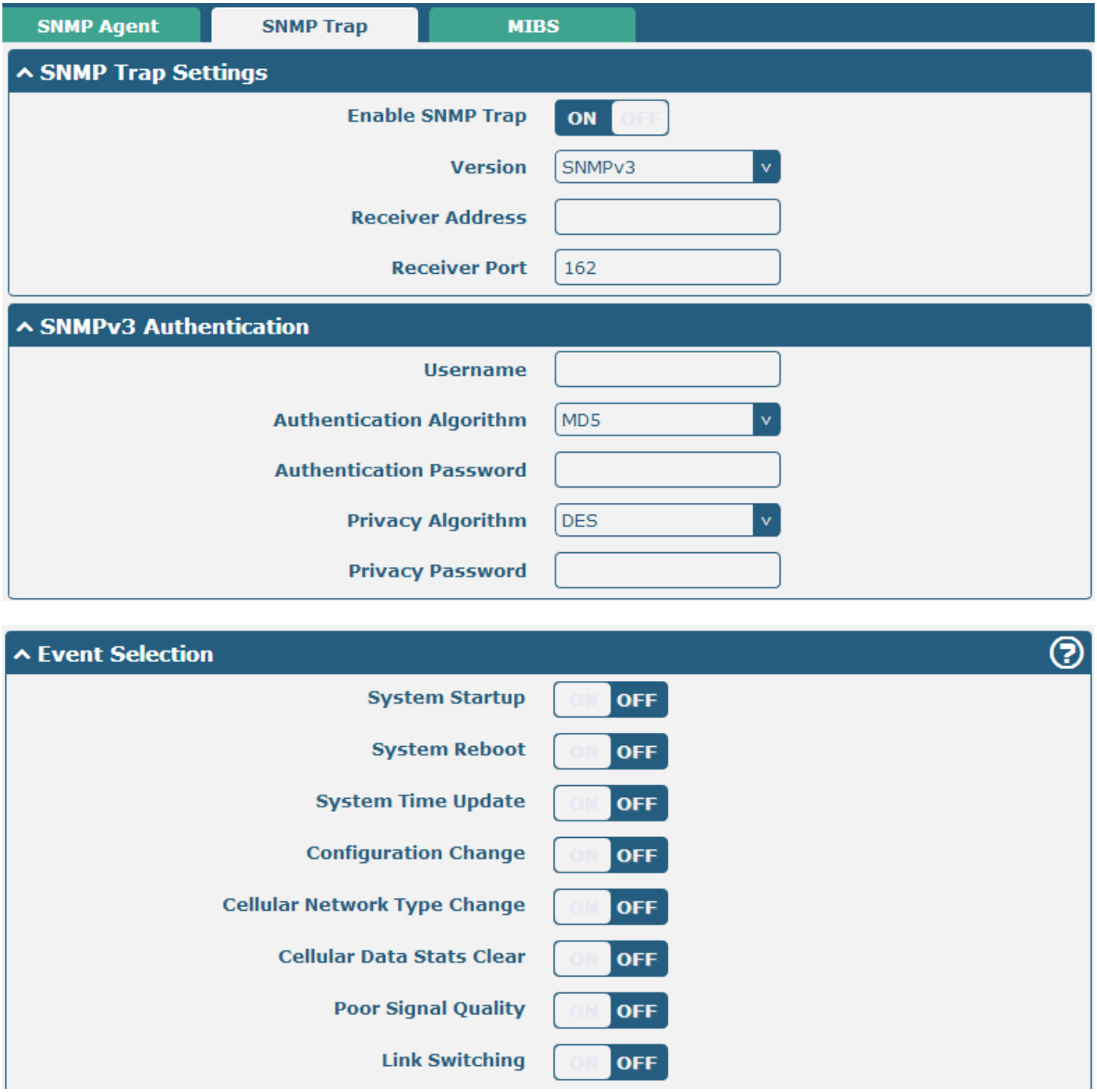
3.26 Services->SNMP (optional APP)

This function is as an APP which needs to install into 4G INDUSTRIAL VPN in **System->APP Center** unit. We can download the MIB file directly from web interface. And then we can manage the 4G INDUSTRIAL VPN router via SNMP tool with the MIB file.



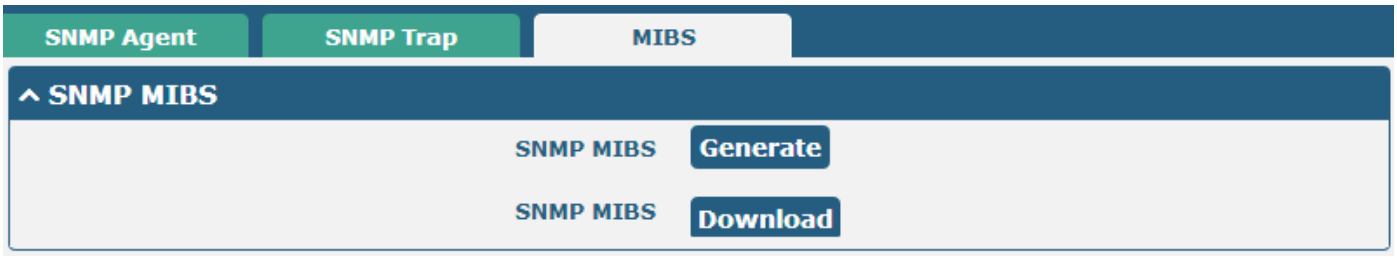
SNMP Agent @ SNMP		
Item	Description	Default
Enable SNMP Agent	Switch “ON” to enable SNMP Agent.	OFF
Port	UDP port for sending and receiving SNMP requests.	161
Version	Select from “SNMPv1”, “SNMPv2” and “SNMPv3”.	SNMPv3
Location Info	Enter the router’s location info which will send to NMS (Network Management System).	null
Contact Info	Enter the router’s contact info which will send to NMS	null
System name	Enter the router’s system name which will send to NMS.	null
Readonly Community Name	Enter the community name which was allowed only to get the status of router.	null
Readwrite Community Name	Enter the community name which was allowed to get the status and set the configuration of router.	null
Authentication Algorithm	Select from “MD5” or “SHA”. The authentication password default to be the login password of router. The Factory Default login password of router is “admin”. We can change the password in **System-> User Management** section. The authentication password must be the same as privacy password on NMS.	MD5

Privacy Algorithm	Select from “DES” or “AES”. The privacy password default to be the login password of router. The Factory Default login password of router is “admin”. We can change the password in **System-> User Management** section. The privacy password must be the same as authentication password on NMS.	DES



SNMP Trap		
Item	Description	Default
Enable SNMP Trap	Switch “ON” to enable SNMP Trap feature.	Disable
Version	Select from “SNMPv1”, “SNMPv2” and “SNMPv3”.	SNMPv2
Receiver Address	Enter NMS (Network Management System) IP address.	Null

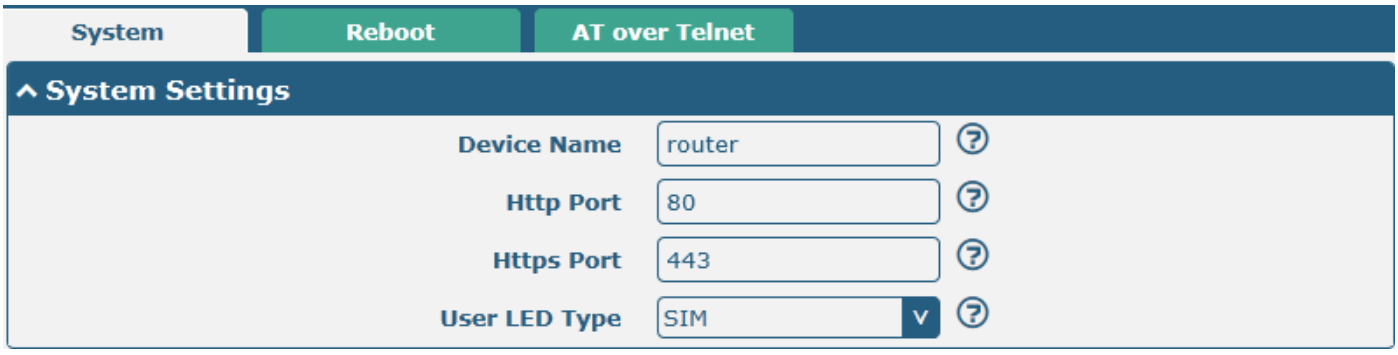
Receiver Port	Enter NMS port number	0
SNMPv3 Authentication		
Username	Set the username for NMS to receive the SNMP trap.	null
Authentication Algorithm	Select from “MD5” or “SHA”.	MD5
Authentication Password	Set the authentication password for NMS to receive the SNMP trap.	null
Privacy Algorithm	Select from “DES” or “AES”.	DES
Privacy password	Set the privacy password for NMS to receive the SNMP trap.	null
Event Selection		
Switch “ON” to enable the event. When the enabled event occurs, router will sent the related SNMP trap to NMS.		



MIBS	
Item	Description
Generate	Click to generate the SNMP MIB file.
Download	Click to download the SNMP MIB file that is used to manage the 4G INDUSTRIAL VPN router via SNMP tool.

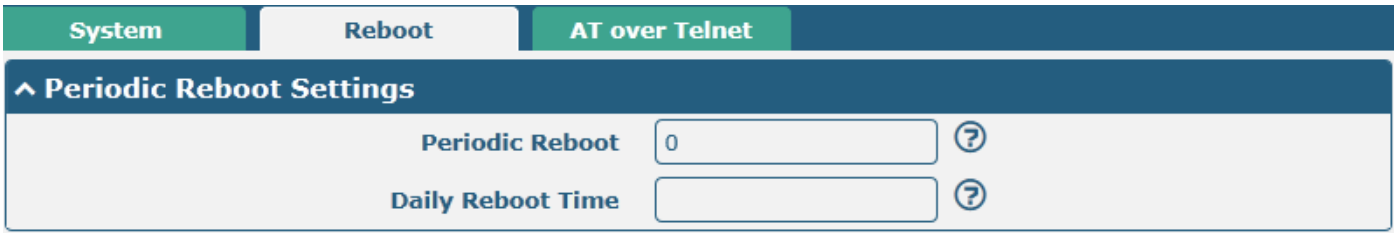
3.27 Services->Advanced

This section allows users to set the Advanced parameters.

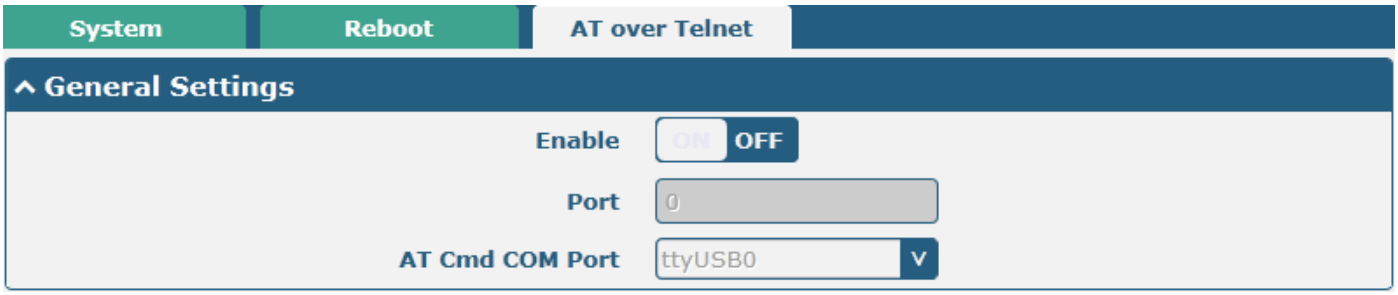


System @ Advanced		
Item	Description	Default
Device Name	Set the device name to distinguish different devices you have installed. Valid characters: a-z, A-Z, 0-9, ., -.	router

Http Port	Enter the HTTP port number you want to manage in 4G INDUSTRIAL VPN'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.	80
Https Port	Enter the HTTPS port number you want to manage in 4G INDUSTRIAL VPN'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 4G INDUSTRIAL VPN'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.*	443
User LED Type	Select from "None", "SIM", "NET", "OpenVPN" and "IPSec".	SIM



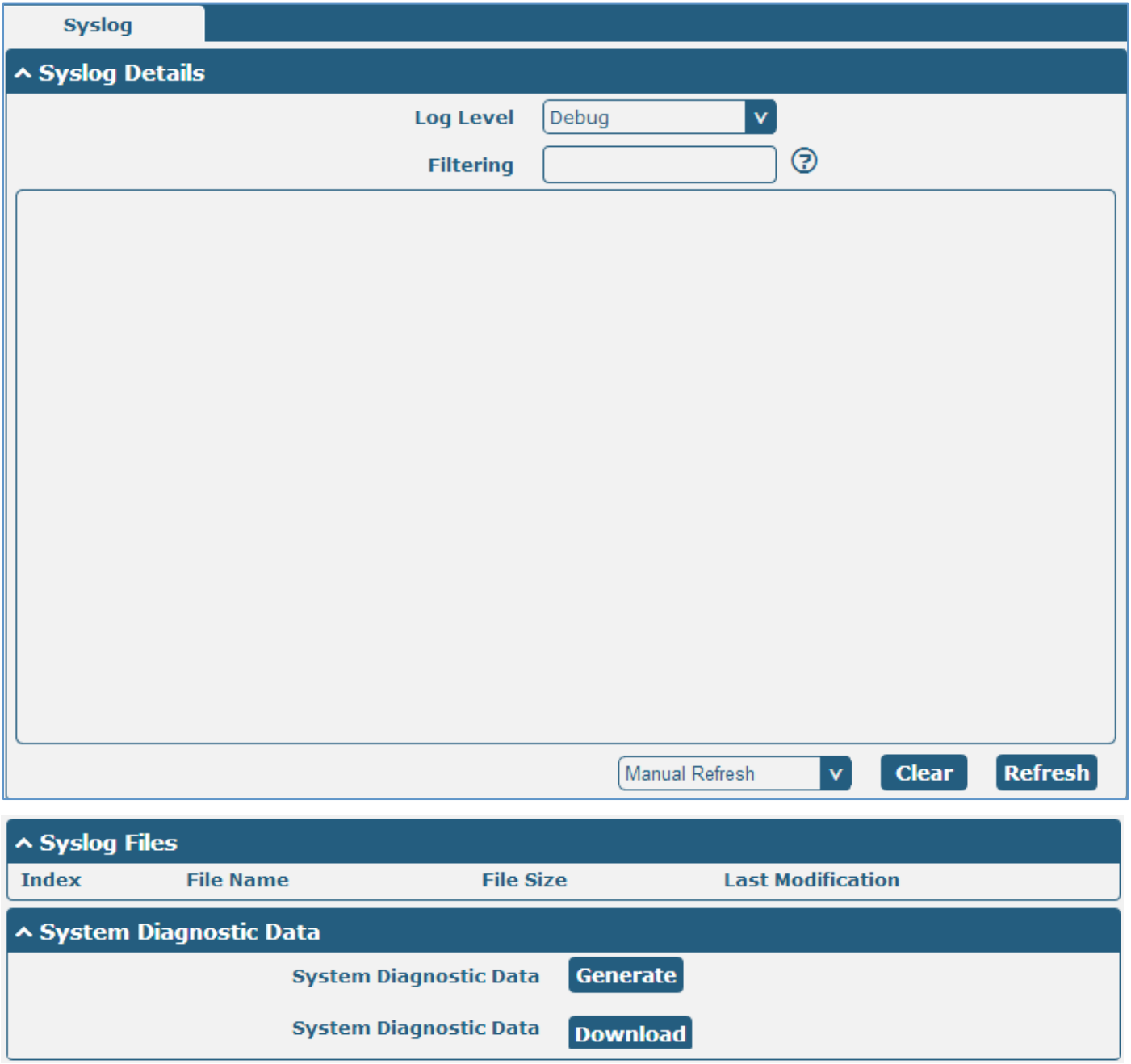
Reboot		
Item	Description	Default
Periodic Reboot	Set the reboot period of the router, 0 means disable.	0
Daily Reboot Time	Set the daily reboot time of the router, you should follow the format as HH: MM, in 24h time frame, otherwise the data will be invalid. Leave it empty means disable.	Null



AT over Telnet @ Advanced		
Item	Description	Default
Enable	Click to enable AT over Telnet function.	OFF
Port	Enter a specific port number to allow user sent AT command to this router over telnet.	0
AT Cmd COM Port	Select a COM port used for identifying the AT command.	ttyUSB 0

3.28 System->Debug

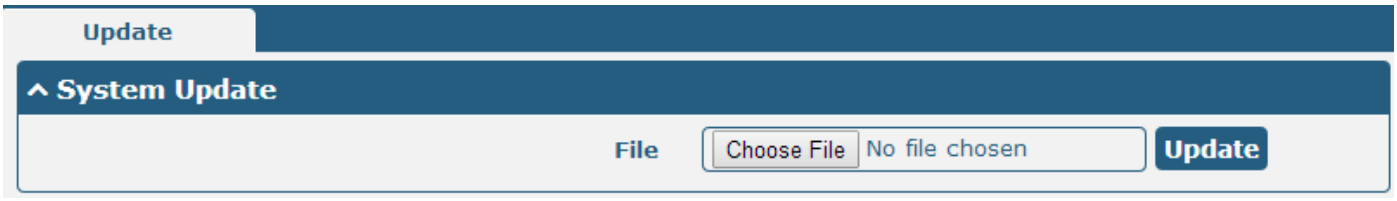
This section allows the user to check and download the syslog details.



Syslog Details @ Syslog		
Item	Description	Default
Log Level	Select form “Debug”, “Info”, “Notice”, “Warn”, “Error” which from low to high. The lower level will output more syslog in detail.	Debug
Filtering	Log will be filtered according to the Filter Message that the user set. Click the Refresh button, the filtered log will be displayed in the follow box. Use “&” to separate more than one filter message, such as “keyword1&keyword2”.	Null

Refresh	Select from “Manual Refresh”, “5 Seconds”, “10 Seconds”, “20 Seconds”and“30 Seconds”. User can select these intervals to refresh the log information displayed in the follow box. Select “manual refresh”, user should click the refresh button to refresh the syslog.	Manual Refresh
Syslog Files List @ Syslog		
Syslog Files List	It can show at most 5 syslog files in the list, the files’ name range from message0 to message 4. And the newest syslog file will be placed on the top of the list.	/
System Diagnosing Data @ Syslog		
Generate	Click to generate the syslog diagnosing file.	/
Download	Click to download system diagnosing file.	/

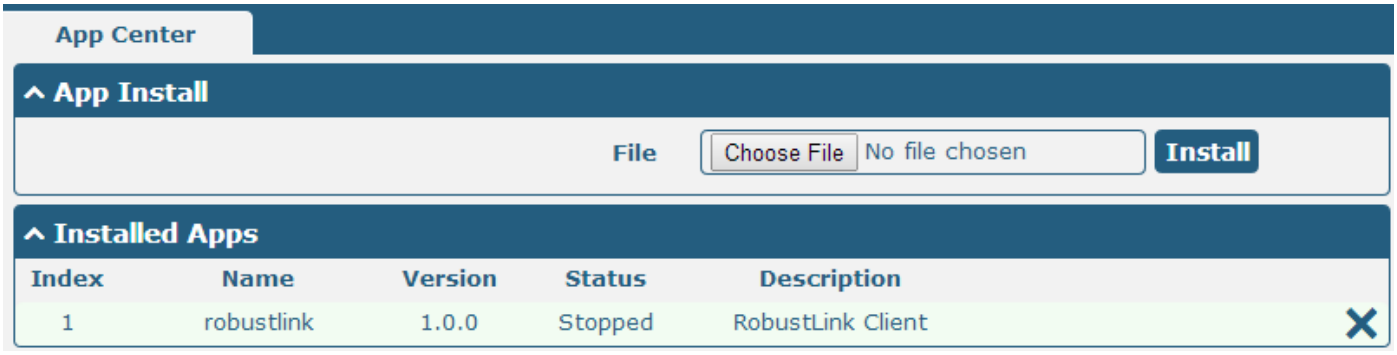
3.29 System->Update



Update		
Item	Description	Default
System Update	Click “Browse” button to select the correct firmware in your PC, and then click “Update” button to update. After updating successfully, you need to click “save and apply”, and then reboot the router to take effect.	Null

3.30 System->APP Center

This section allow user to add a new function to 4G INDUSTRIAL VPN router. And the new function will be in the form of an APP file which could be installed in 4G INDUSTRIAL VPN router. In general, the App which had installed will display in **Service** section.

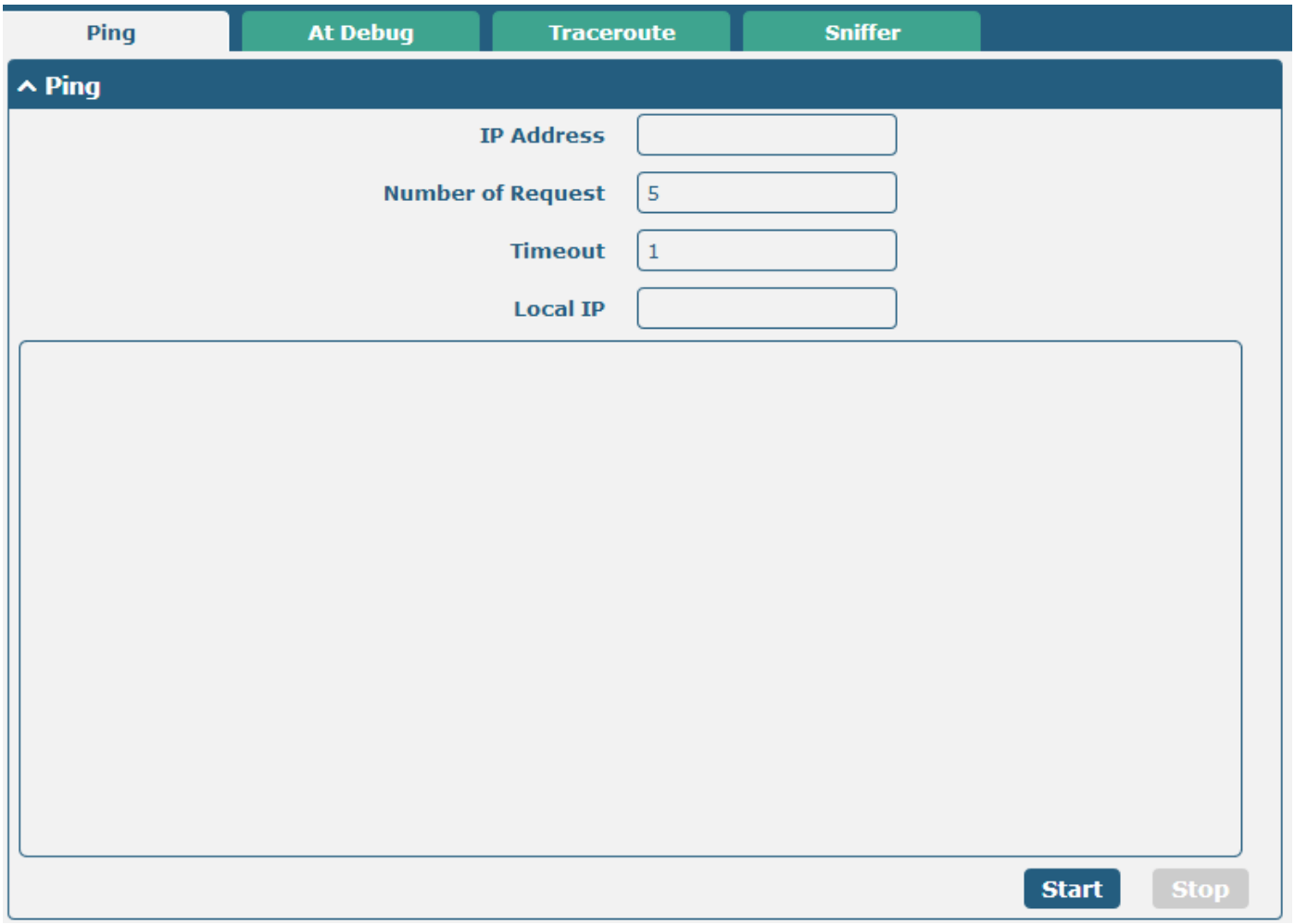


App Center

Item	Description	Default
File	Choose the correct App file from your PC, and click Install button to import to 4G INDUSTRIAL VPN router. File format: xxx.rpk, e.g. 4G Industrial VPN-CloudLink-1.0.0.rpk.	/
Install Apps	Those Apps which had installed in 4G INDUSTRIAL VPN will be listed in **Installed Apps**.	Null
Index	Show the index of the App.	Null
Name	Show the name of the App.	Null
Version	Show the version of the App.	Null
Status	Show the Status of the App.	Null
Description	Show the description of the App.	Null

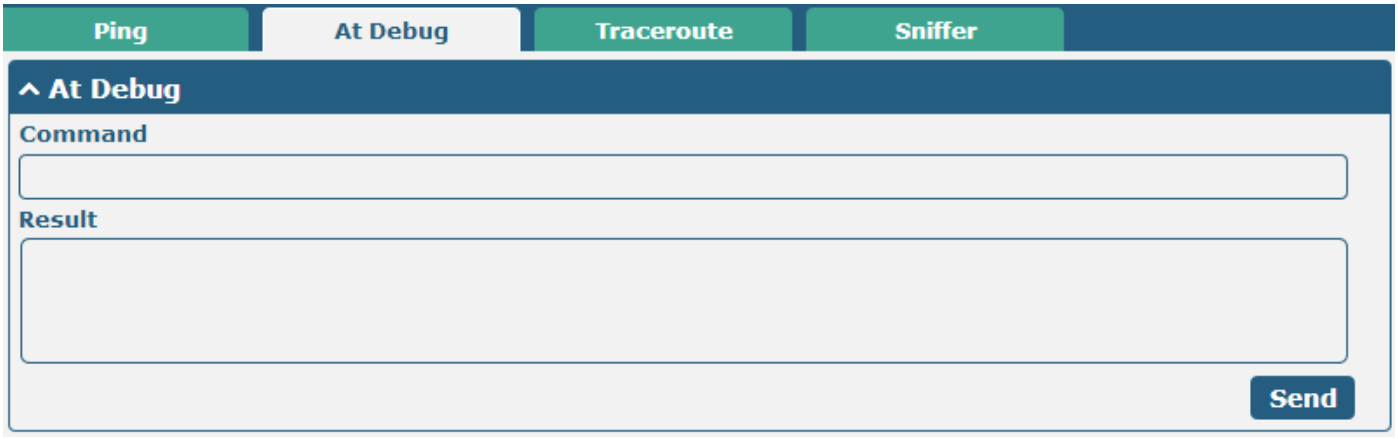
3.31 System->Tools

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

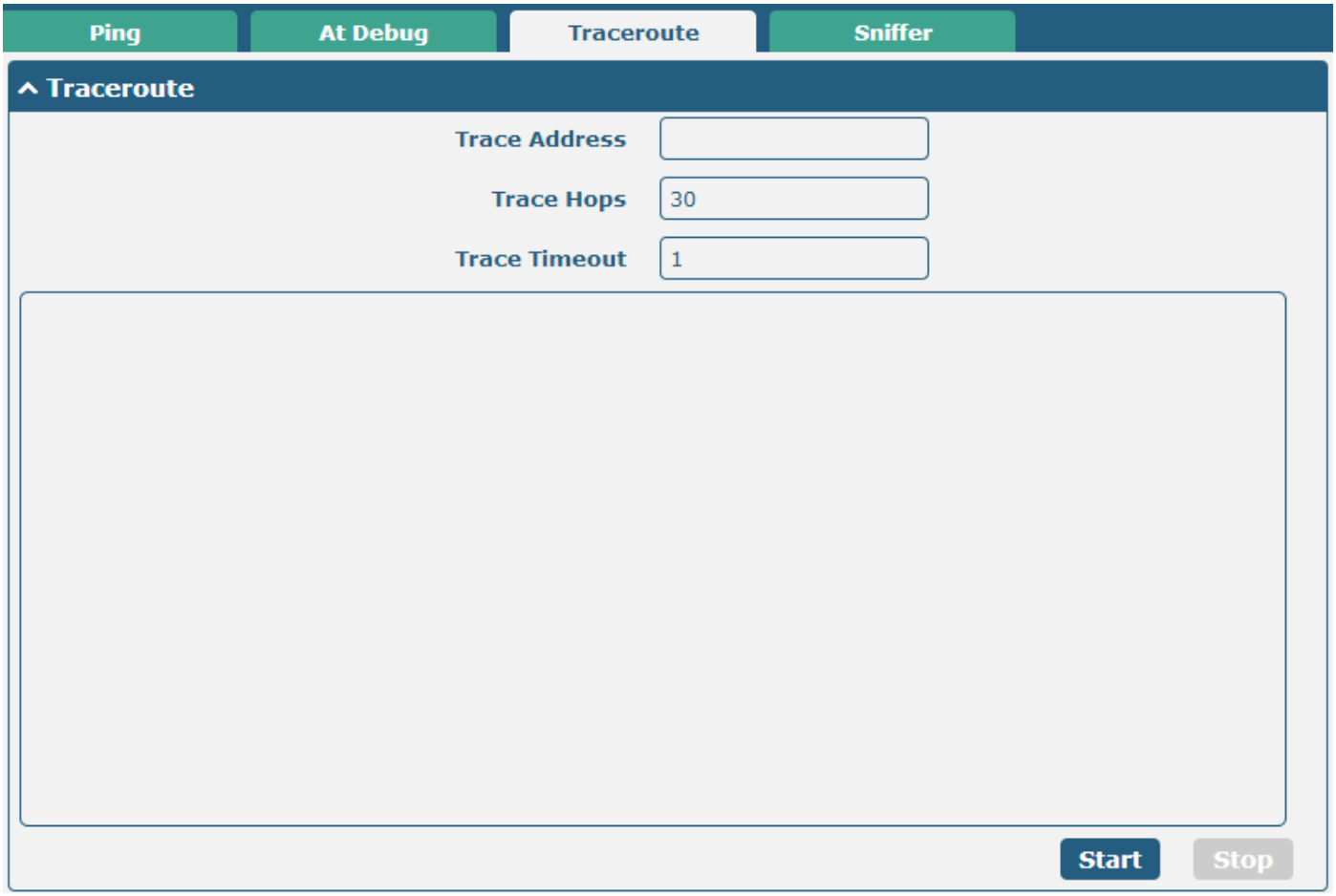


Ping @ Tools

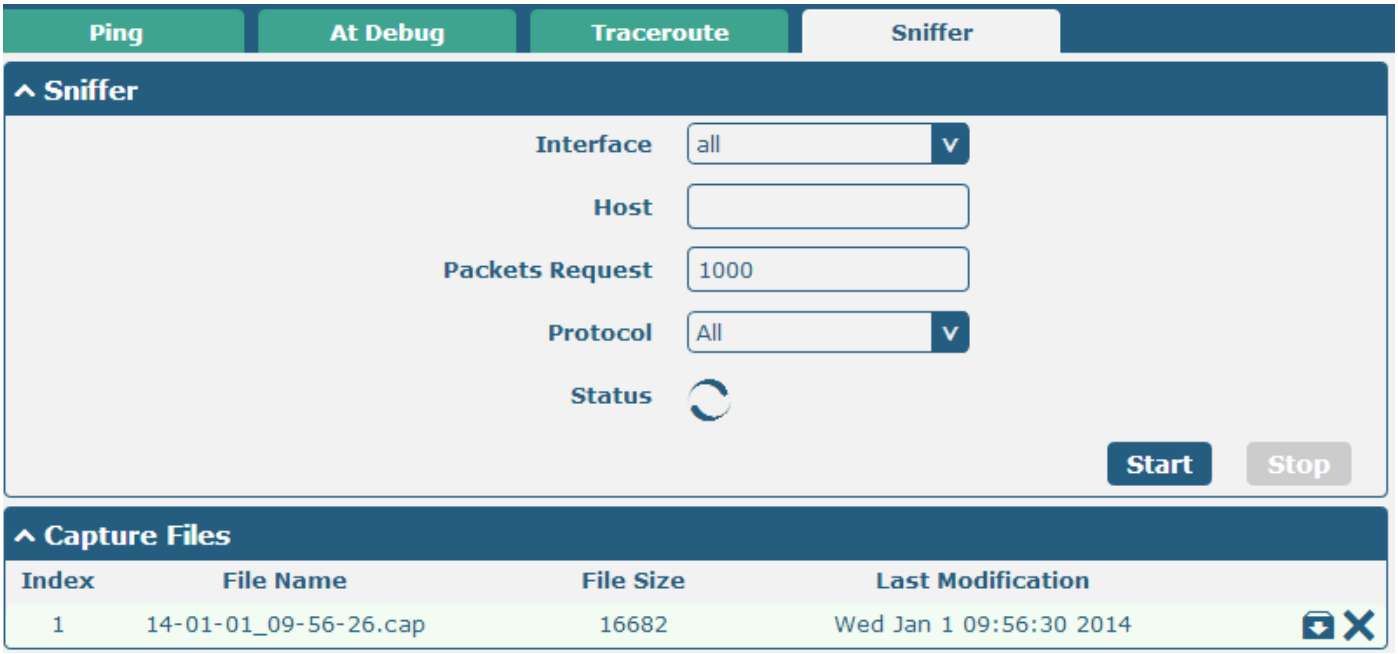
Item	Description	Default
IP address	Enter the ping destination IP address or domain name.	Null
Number of requests	Specify the number of ping requests.	5
Timeout	Specify timeout of ping request.	1
Local IP	Specify the local IP from cellular WAN, Ethernet WAN or Ethernet LAN. Null stands for selecting 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
Stop	Click this button to stop ping request.	



At Debug @ Tools	
Item	Description
Command	Enter a At command in Command box, then click Send button to send the At command to the cellular module.
Result	It will display the AT commands which respond from the cellular module in this box.



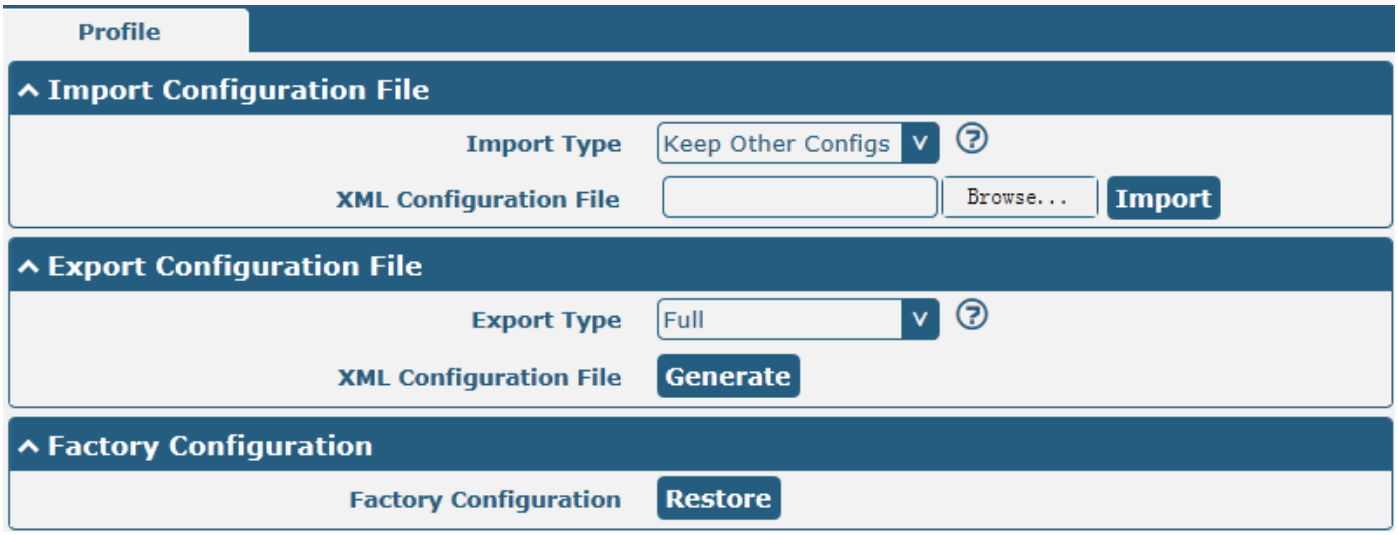
Traceroute @ Tools		
Item	Description	Default
Trace Address	Enter the trace destination IP address or domain name.	Null
Trace Hops	Specify the max trace hops. Router will stop tracing if the trace hops has met max value no matter the destination has been reached or not.	30
Trace Timeout	Specify timeout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



Sniffer @ Tools		
Item	Description	Default
Interface	Select form “All”, “ETH1”, and “ETH2”: All: contain all the interface; ETH1: Ethernet interface1; ETH2: Cellular WAN.	All
Host	Filter the packet that contain the specify IP address.	Null
Packets Request	Set the packet number that the router can sniffer at a time.	1000
Protocol	Select from “All”, “IP”, “TCP”, “UDP” and “ARP”.	All
Port	Set the port number for TCP or UDP that is used in sniffer.	Null
Status	Show the current status of sniffer.	Null
Start	Click this button to start the sniffer.	/
Stop	Click this button to stop the sniffer. Once click the stop button, a new log file will be displayed in the follow List.	/
Capture Files	Every times of sniffer log will be saved automatically as a new file. You can find the file from this Sniffer Traffic Data List and click to download the log, click to delete the log file. It can cache a maximum of 5 files.	Null

3.32 System->Profile

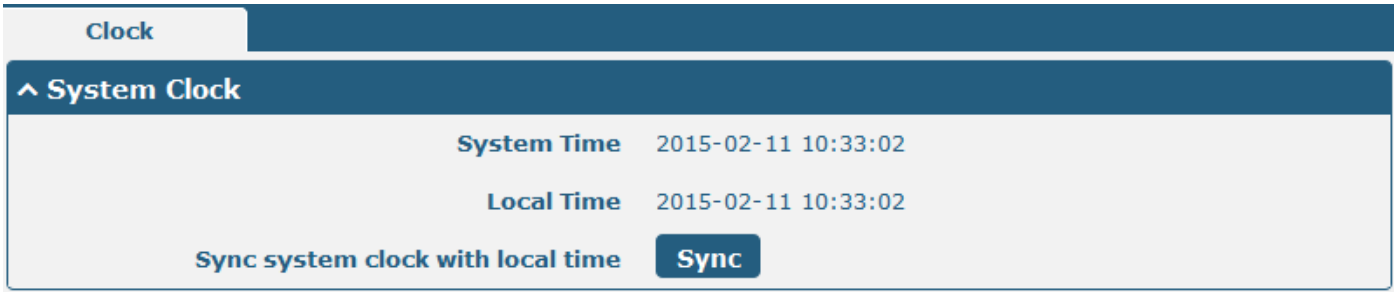
This section allows users to import or export the configuration file, and restore the router to factory default setting.



Import Configuration File @ Profile		
Import Type	Define what to do about the configs that is not contained in the imported file. There are two Import Types: Keep Other Configs: Keep other configuration unchanged when import XML configuration file. Set Others To Default: Set other configuration to factory default when import XML configuration file.	Keep Other Configs
XML Configuration File	Click “Browse” to select the XML file in your computer, and then click “Import” to import this file into your router.	
Export Configuration File @ Profile		
Export Type	There are four export Types : Essential: export the configuration file that only include enabled features. Essential && Detailed: export the configuration file that only include enabled features, and attach extra information such as **range** and **default** setting of those enable config option. Full: export the configuration file of all features; include both the enabled and disabled features. Full && Detailed: export the configuration file of all features, and attach extra information such as **range** and **default** setting of every config option.	Full
Export	Click “Export” and the configuration will be showed in the new popup browser window, then you can save it as a XML file.	
Factory Configuration @ Profile		
Restore	Click the “Restore” button to restore the router to factory default setting.	

3.33 System->Clock

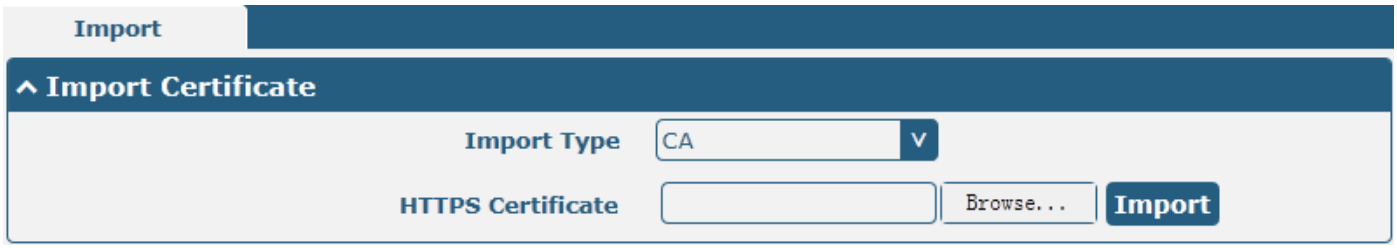
This section allows users to set clock of router and NTP server.



Clock		
Item	Description	Default
System Time	Router's system time will be showed in this field.	Null
Local Time	You PC's time will be showed here.	Null
Sync	Synchronize router's system time with PC.	Null

3.34 System->HTTPS

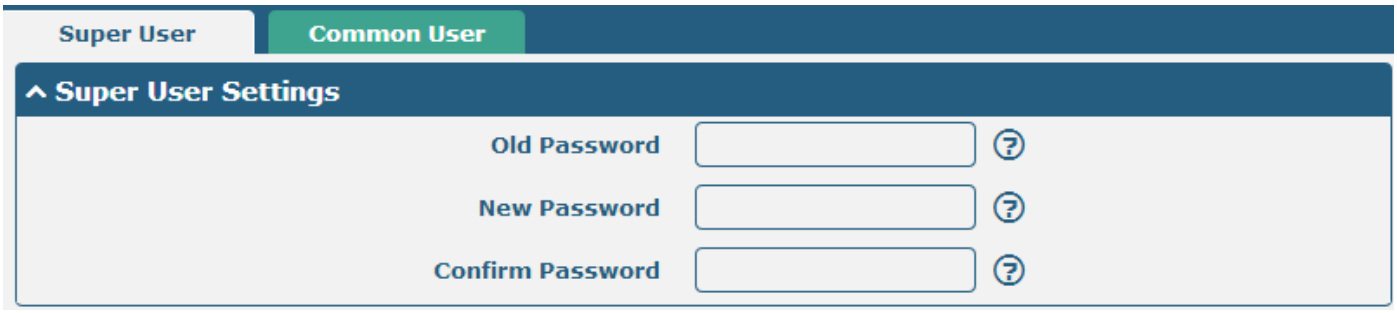
This section allows users to import the certificate file into the route.



HTTPS		
Item	Description	Default
Import Type	Select from "CA" and "Private Key". CA: a digital certificate issued by CA center. Private Key: a private key file.	CA
HTTPS Certificate	Click "Browse" to select the certificate file in your computer, and then click "Import" to import this file into your router.	

3.35 System->User Management

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



Super User		
Item	Description	Default
Super User	One router has only one super user account. Under this account, user has the highest authority include modify, add and manage those user accounts.	/
Old Password	The old password of super user which default is “admin”, valid characters: a-z, A-Z, 0-9, @, ., -, #, $, *.	Null
New Password	Enter a new password for the super user, valid characters: a-z, A-Z, 0-9, @, ., -, #, $, *.	Null
Confirm Password	Enter the new password again which had added in New Password item.	Null

Click the “ ” button to add a new common user.

***Note**: One router has 5 common user accounts at most.*

Common User		
Item	Description	Default
Role	Select from “Visitor” and “Editor”. Visitor: Users only can view the configuration of router under this level;	Visitor

	Editor: Users can view and set the configuration of router under this level.	
Username	Set the Username. Valid characters: a-z, A-Z, 0-9, ., -.	Null
Password	Set the password which at least contains 5 characters. Valid characters: a-z, A-Z, 0-9, @, ., -, #, $, *.	Null

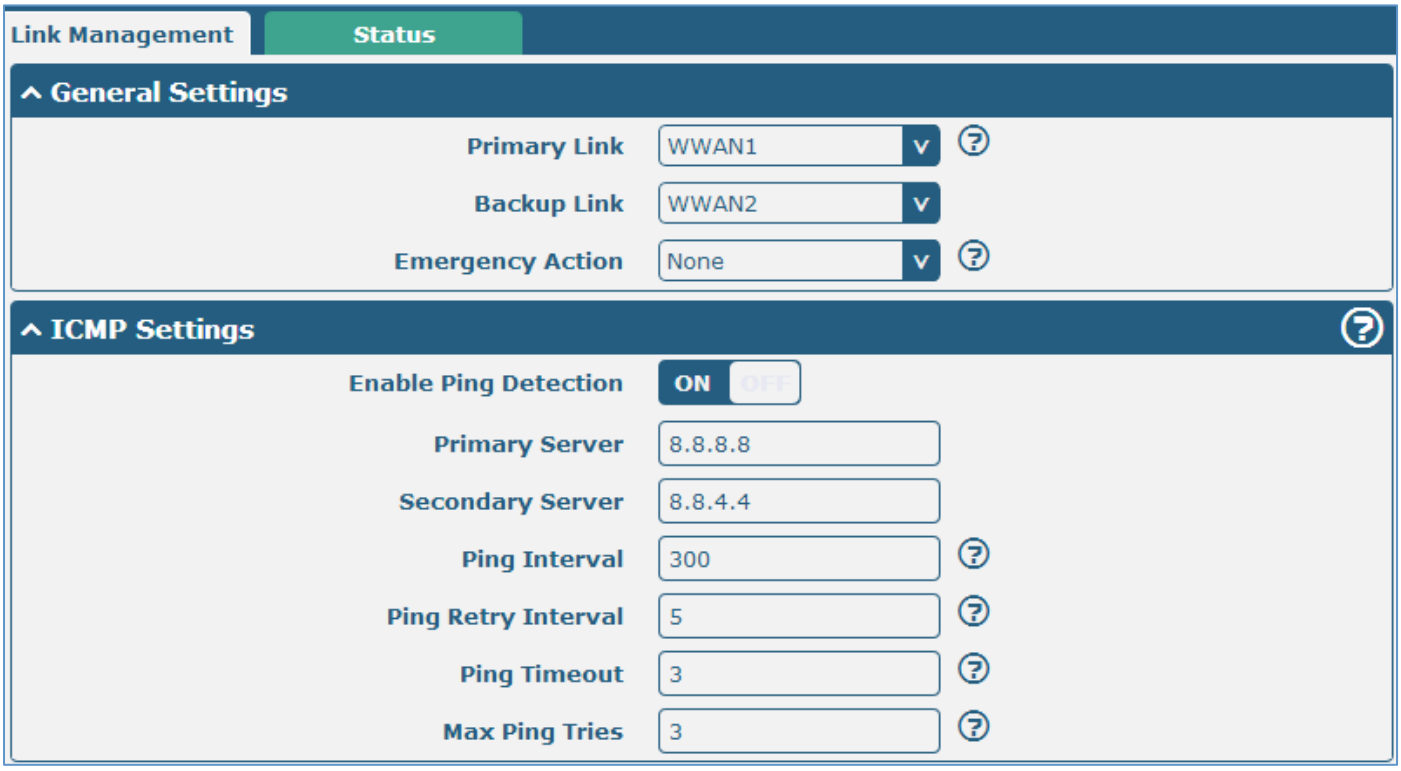
Chapter 4 Configuration Examples

4.1 Cellular

4.1.1 Cellular Dial-Up

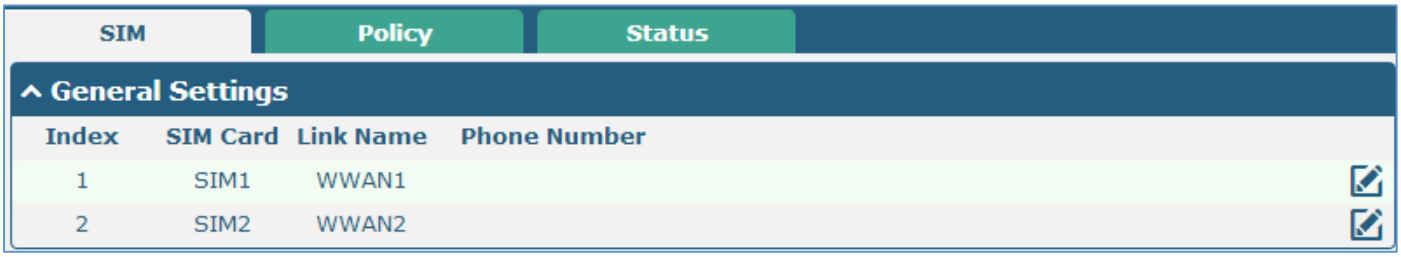
This section shows users how to configure the primary and backup SIM card of Cellular Dial-up.

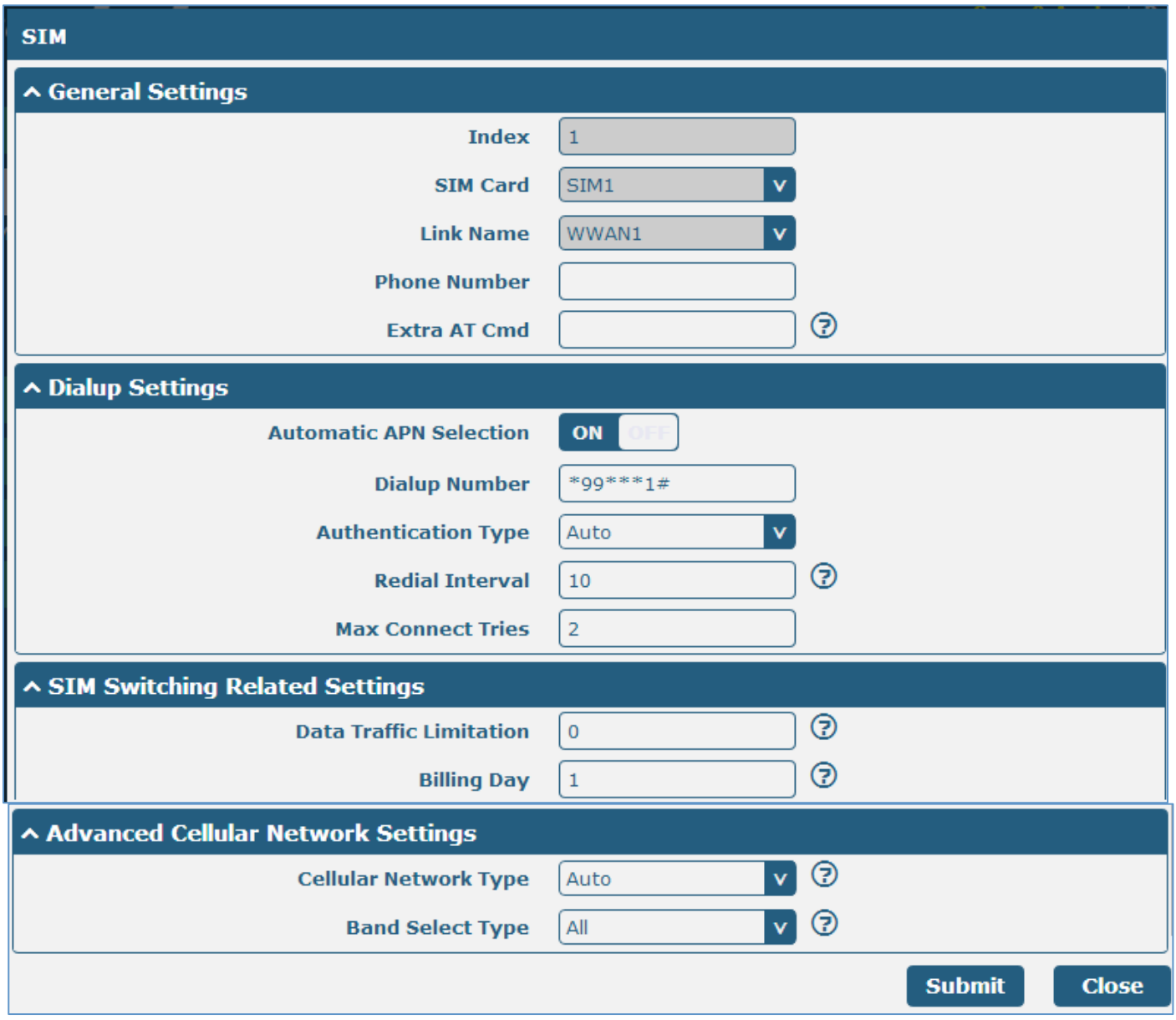
Interface-->Link Management



The modifications will take effect after click “Submit” and “save and apply” button.

Interface-->Cellular





The modifications will take effect after click “Submit” and “save and apply” button.

4.1.2 SMS Remote Control

4G INDUSTRIAL VPN supports remote control via SMS. User can use following commands to get the status of 4G INDUSTRIAL VPN, and set all the parameters of 4G INDUSTRIAL VPN.

There are three authentication types for SMS control. You can select from "Password", "Phonenum" and "Both".

An SMS command has following structure:

1. Password mode—Username: Password;cmd1;cmd2;cmd3; …cmdn.
2. Phonenum mode--cmd1; cmd2; cmd3; … cmdn.
3. Both mode-- Username: Password;cmd1;cmd2;cmd3; …cmdn.

SMS command Explanation:

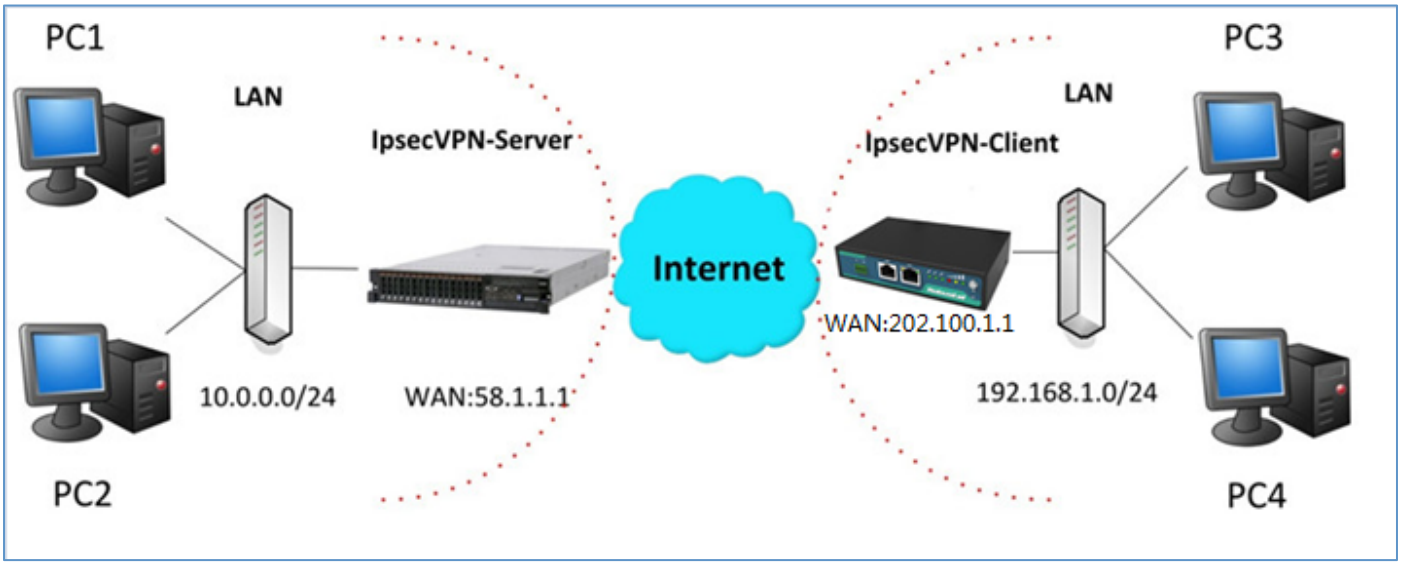
1. User name and Password: it uses the same username and password as WEB manager for authentication.
2. cmd1, cmd2, cmd3 to Cmdn, the command format is the same as the CLI command.

   Note: Download the configure xml file from the configured web browser. The format of SMS control command can refer to the data of the xml file.
3. The semicolon character (';') is used to separate more than one commands packed in a single SMS.
4. E.g., admin:admin;reboot

   In this command, username is admin, password is admin, and the command is reboot 4G INDUSTRIAL VPN.

4.2 Network

4.2.1 IPSEC VPN



Note: *the configuration of server and client is as follows.*

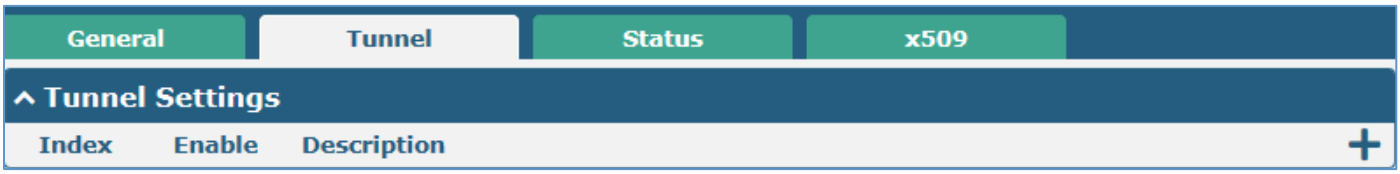
IPSecVPN_SERVER:

Cisco 2811:

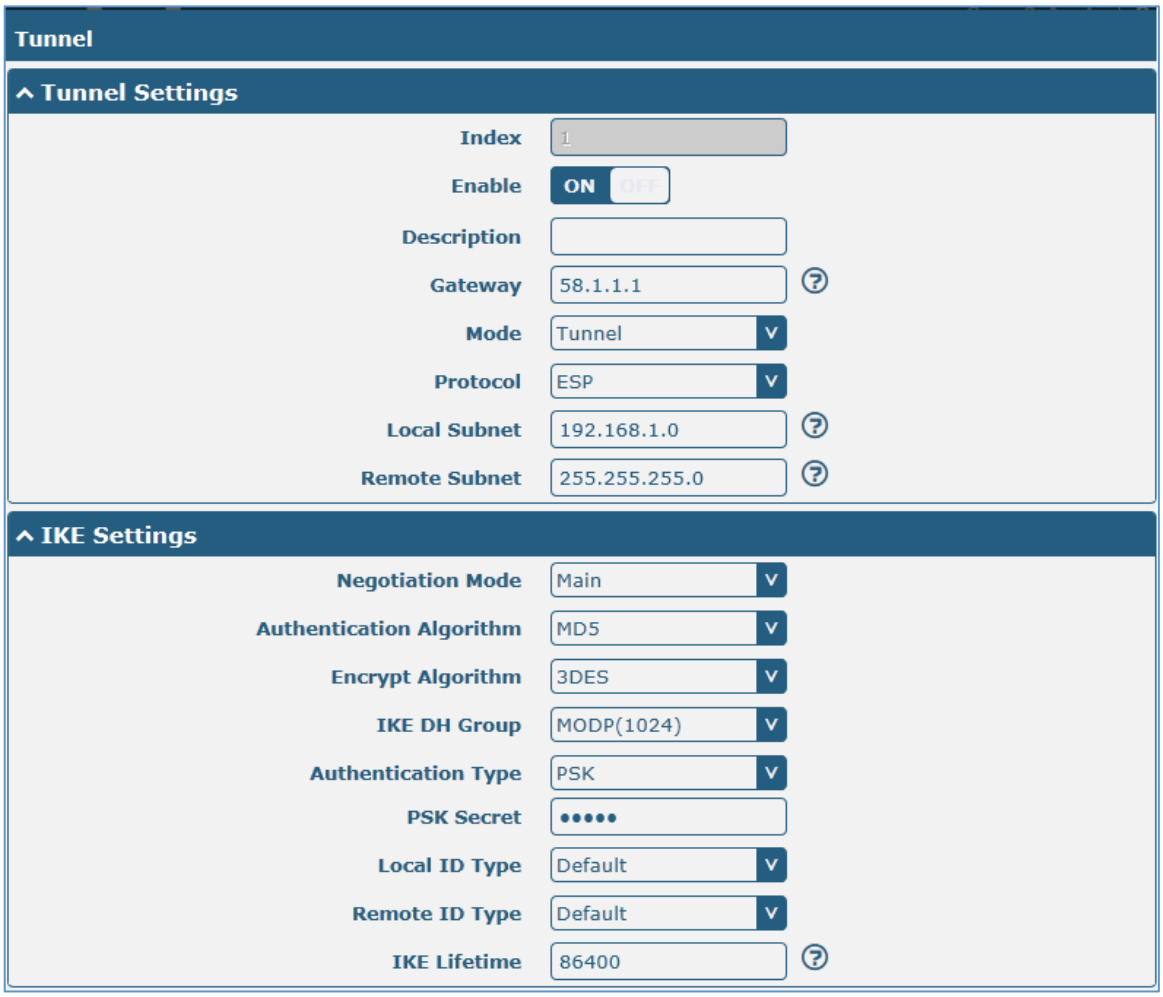
```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#?
  authentication  Set authentication method for protection suite
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#exit
Router(config)#crypto isakmp ?
  client  Set client configuration policy
  enable  Enable ISAKMP
  key     Set pre-shared key for remote peer
  policy  Set policy for an ISAKMP protection suite
Router(config)#crypto isakmp key cisco address 0.0.0.0 0.0.0.0


Router(config)#crypto ?
  dynamic-map  Specify a dynamic crypto map template
  ipsec        Configure IPSEC policy
  isakmp       Configure ISAKMP policy
  key          Long term key operations
  map          Enter a crypto map
Router(config)#crypto ipsec ?
  security-association  Security association parameters
  transform-set         Define transform and settings
Router(config)#crypto ipsec transform-set Trans ?
  ah-md5-hmac   AH-HMAC-MD5 transform
  ah-sha-hmac   AH-HMAC-SHA transform
  esp-3des      ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes       ESP transform using AES cipher
  esp-des       ESP transform using DES cipher (56 bits)
  esp-md5-hmac  ESP transform using HMAC-MD5 auth
  esp-sha-hmac  ESP transform using HMAC-SHA auth
Router(config)#crypto ipsec transform-set Trans esp-3des esp-md5-hmac


Router(config)#ip access-list extended vpn
Router(config-ext-nacl)#permit ip 10.0.0.0 0.0.0.255 192.168.1.0 0.0.0.255
Router(config-ext-nacl)#exit


Router(config)#crypto map cry-map 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#match address vpn
Router(config-crypto-map)#set transform-set Trans
Router(config-crypto-map)#set peer 202.100.1.1
Router(config-crypto-map)#exit



Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 58.1.1.1 255.255.255.0
Router(config-if)#cr
Router(config-if)#crypto map cry-map
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

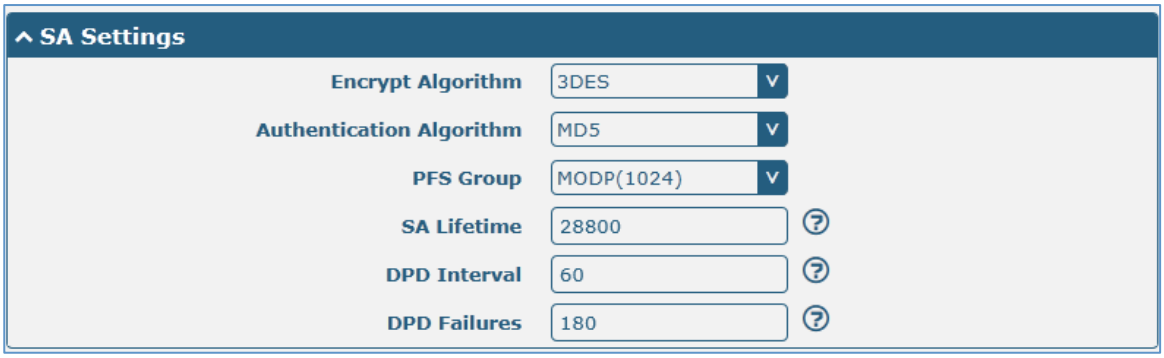
IPSecVPN_CLIENT:

VPN--->IPSec--->Tunnel



Then click “ ”.





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

The comparison between server and client is as following picture:

Server(Cisco 2811)

```
Router>enable
Router#config
Configuring from terminal, memory, or network [terminal]?
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)#crypto isakmp policy 10
Router(config-isakmp)#?
  authentication  Set authentication method for protection suite
  encryption      Set encryption algorithm for protection suite
  exit            Exit from ISAKMP protection suite configuration mode
  group           Set the Diffie-Hellman group
  hash            Set hash algorithm for protection suite
  lifetime        Set lifetime for ISAKMP security association
  no              Negate a command or set its defaults
Router(config-isakmp)#encryption 3des
Router(config-isakmp)#hash md5
Router(config-isakmp)#authentication pre-share
Router(config-isakmp)#group 2
Router(config-isakmp)#exit
Router(config)#crypto isakmp ?
  client  Set client configuration policy
  enable  Enable ISAKMP
  key     Set pre-shared key for remote peer
  policy  Set policy for an ISAKMP protection suite
Router(config)#crypto isakmp key cisco address 0.0.0.0 0.0.0.0
```

IKE Setting in Client must be consistent with server.

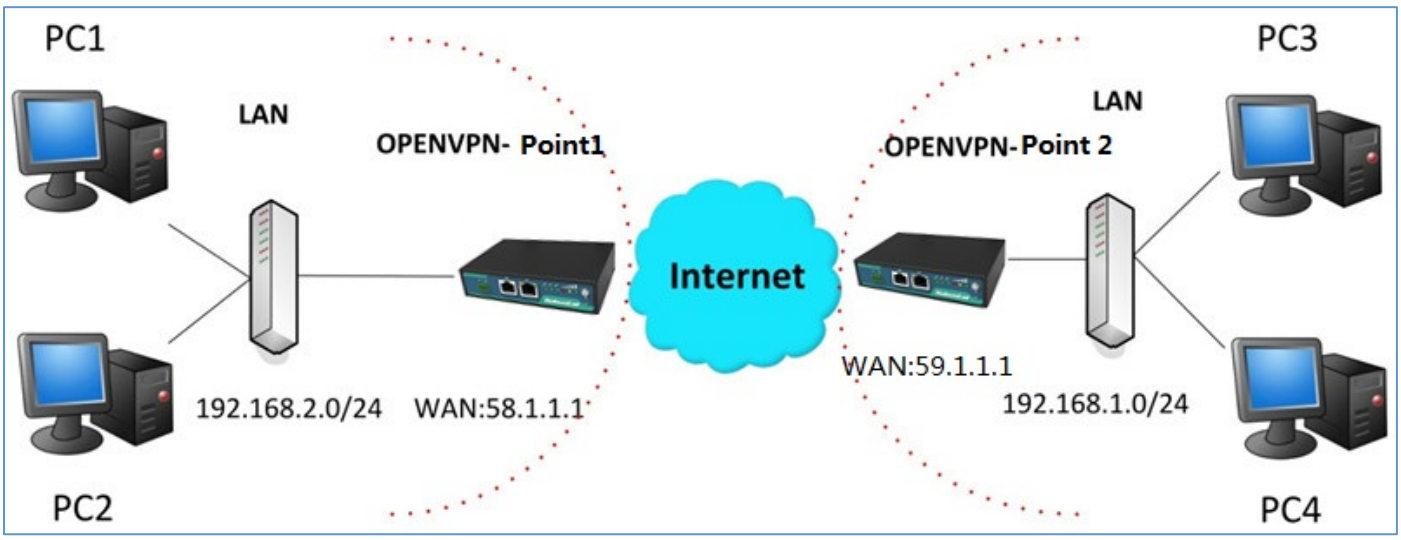
```
Router(config)#crypto ?
  dynamic-map  Specify a dynamic crypto map template
  ipsec        Configure IPSEC policy
  isakmp       Configure ISAKMP policy
  key          Long term key operations
  map          Enter a crypto map
Router(config)#crypto ipsec ?
  security-association  Security association parameters
  transform-set         Define transform and settings
Router(config)#crypto ipsec transform-set Trans ?
  ah-md5-hmac   AH-HMAC-MD5 transform
  ah-sha-hmac   AH-HMAC-SHA transform
  esp-3des      ESP transform using 3DES(EDE) cipher (168 bits)
  esp-aes       ESP transform using AES cipher
  esp-des       ESP transform using DES cipher (56 bits)
  esp-md5-hmac  ESP transform using HMAC-MD5 auth
  esp-sha-hmac  ESP transform using HMAC-SHA auth
Router(config)#crypto ipsec transform-set Trans esp-3des esp-md5-hmac
```

SA Setting in Client must be consistent with server.

```
Router(config)#ip access-list extended vpn
Router(config-ext-nacl)#permit ip 10.0.0.0 0.0.0.255 192.168.1.0 0.0.0.255
Router(config-ext-nacl)#exit

Router(config)#crypto map cry-map 10 ipsec-isakmp
% NOTE: This new crypto map will remain disabled until a peer
        and a valid access list have been configured.
Router(config-crypto-map)#match address vpn
Router(config-crypto-map)#set transform-set Trans
Router(config-crypto-map)#set peer 202.100.1.1
Router(config-crypto-map)#exit


Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 58.1.1.1 255.255.255.0
Router(config-if)#cr
Router(config-if)#crypto map cry-map
*Jan  3 07:16:26.785: %CRYPTO-6-ISAKMP_ON_OFF: ISAKMP is ON
```

Client (R2000 Lite)

4.2.2 OPENVPN

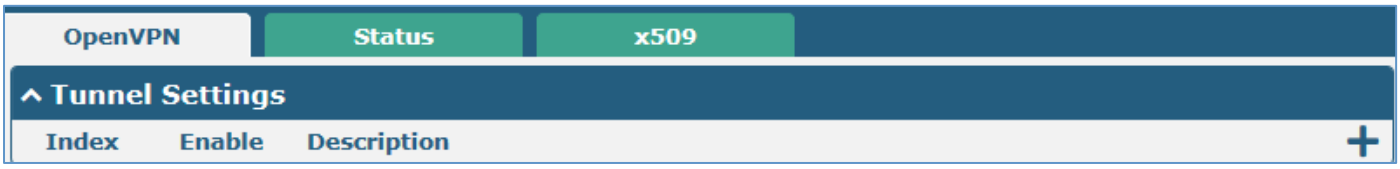


Note: *the configuration of two points is as follows.*

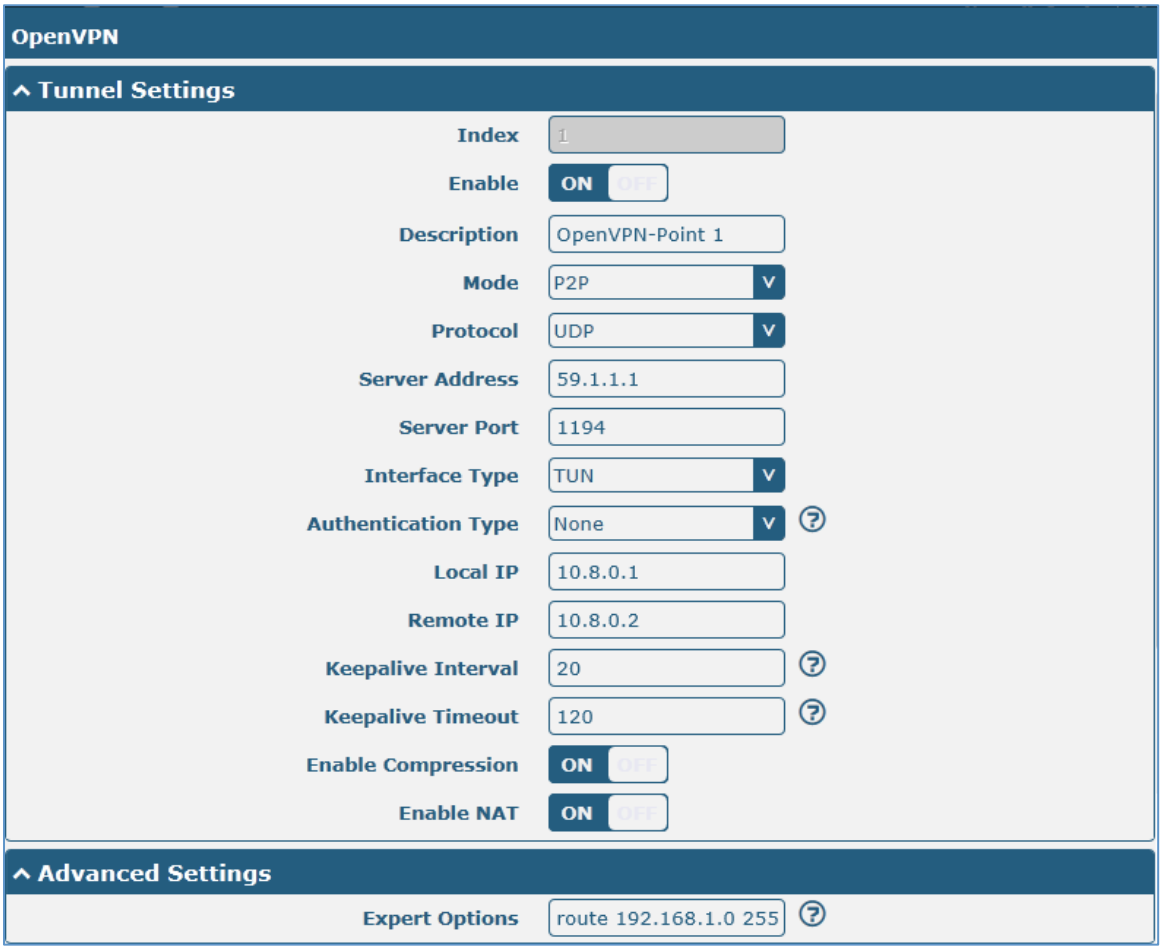
OPENVPN (p2p):

Point 1

VPN--->OpenVPN--->OpenVPN



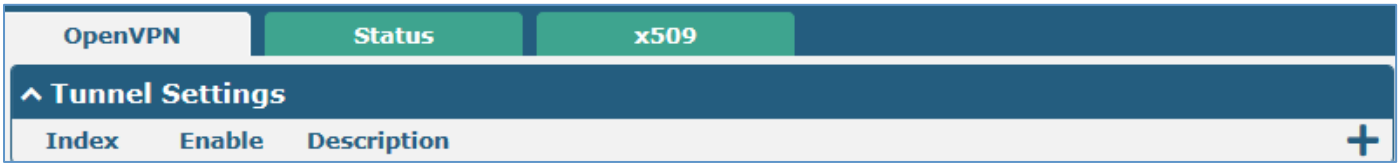
Click “ + ”.



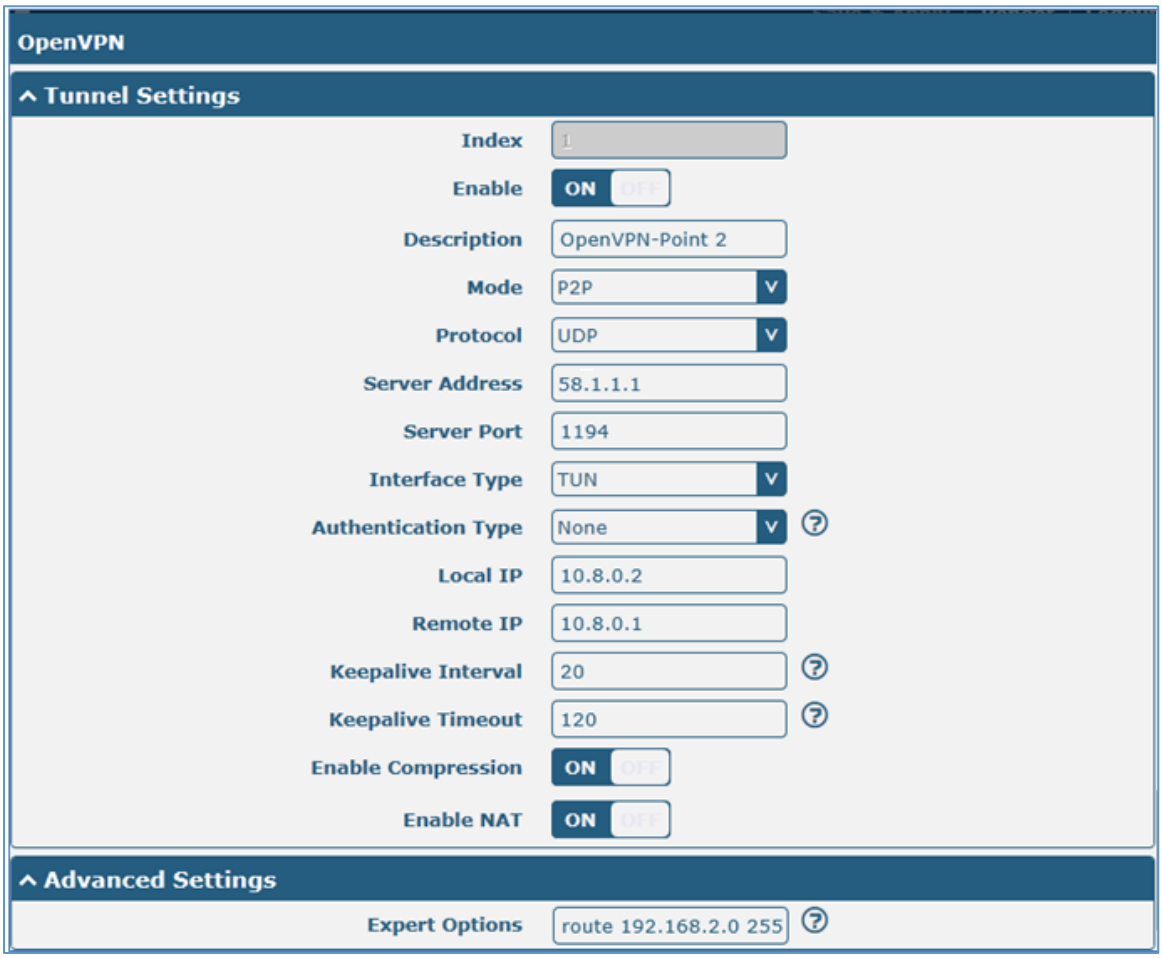
The modifications will take effect after click “Submit-->Save&Apply”.

Point 2

VPN--->OpenVPN--->OpenVPN



Click “ + ”.



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

The comparison between point 1 and point 2 is as following picture:

Point 1

OpenVPN

Tunnel Settings

Index	1
Enable	ON
Description	OpenVPN-Point 1
Mode	P2P
Protocol	UDP
point 2 address Server Address	59.1.1.1
Server Port	1194
Interface Type	TUN
Authentication Type	None
point 1 tunnel IP Local IP	10.8.0.1
point 2 tunnel IP Remote IP	10.8.0.2
Keepalive Interval	20
Keepalive Timeout	120
Enable Compression	ON
Enable NAT	ON

Advanced Settings

Expert Options	route 192.168.1.0 255

point 2

OpenVPN

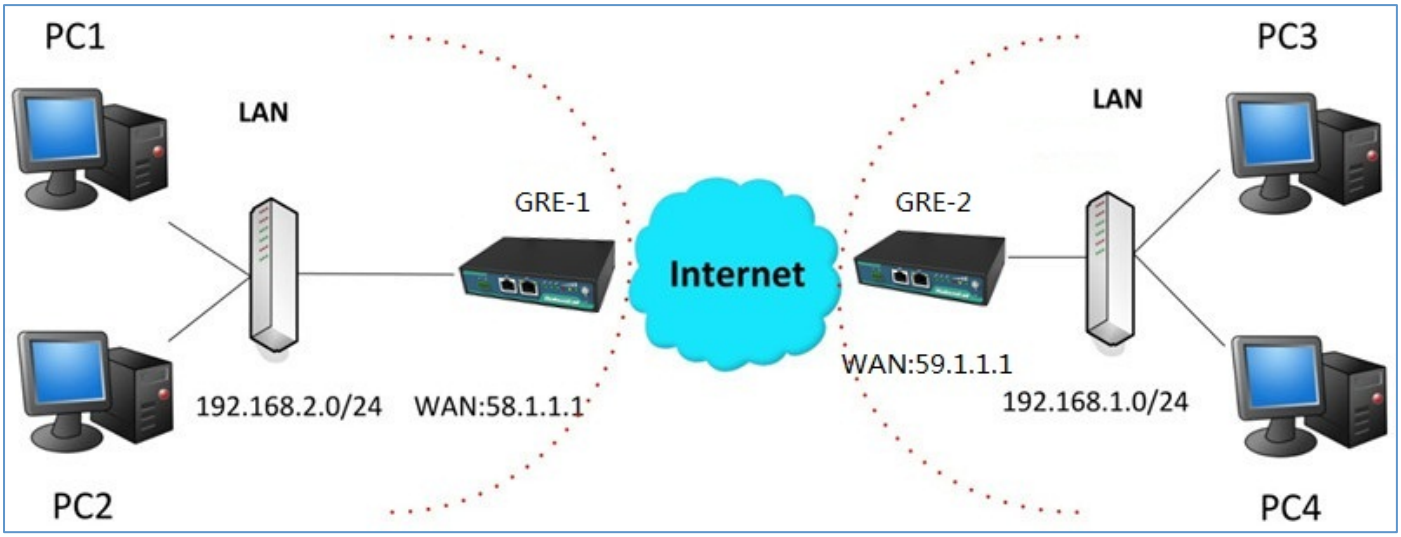
Tunnel Settings

Index	1
Enable	ON
Description	OpenVPN-Point 2
Mode	P2P
Protocol	UDP
point 1 address Server Address	58.1.1.1
Server Port	1194
Interface Type	TUN
Authentication Type	None
point 2 tunnel IP Local IP	10.8.0.2
point 1 tunnel IP Remote IP	10.8.0.1
Keepalive Interval	20
Keepalive Timeout	120
Enable Compression	ON
Enable NAT	ON

Advanced Settings

Expert Options	route 192.168.2.0 255

4.2.3 GRE VPN



VPN--->GRE--->GRE

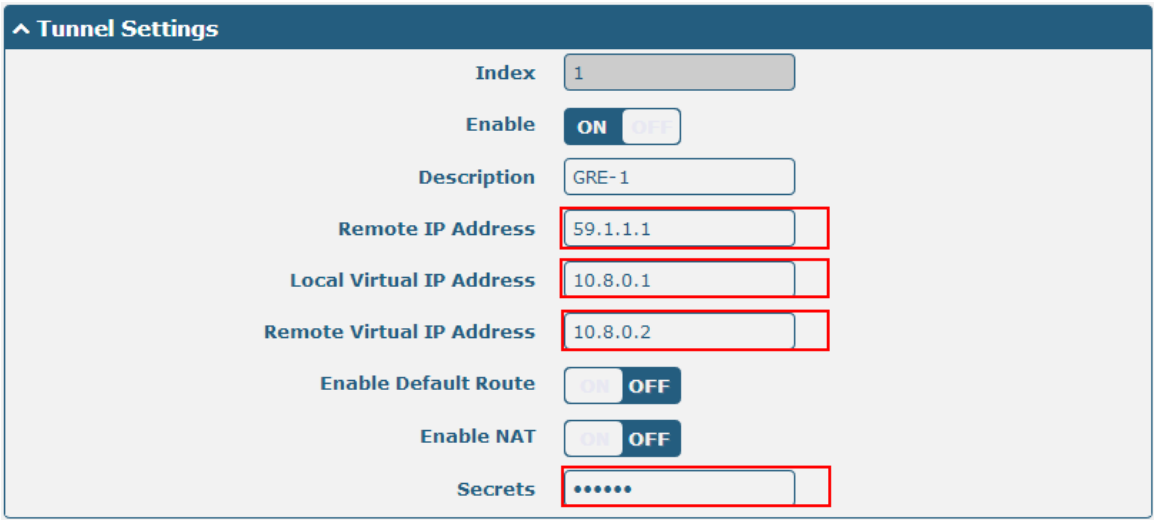
GRE | Status

Tunnel Settings

Index | Enable | Description | Remote IP Address | +

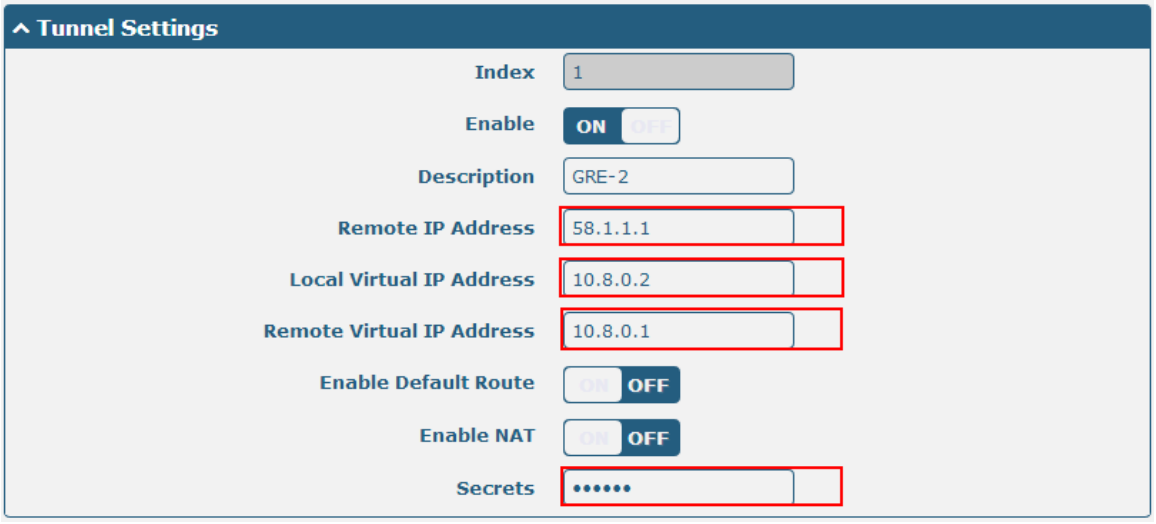
Click “ + ”.

GRE-1：



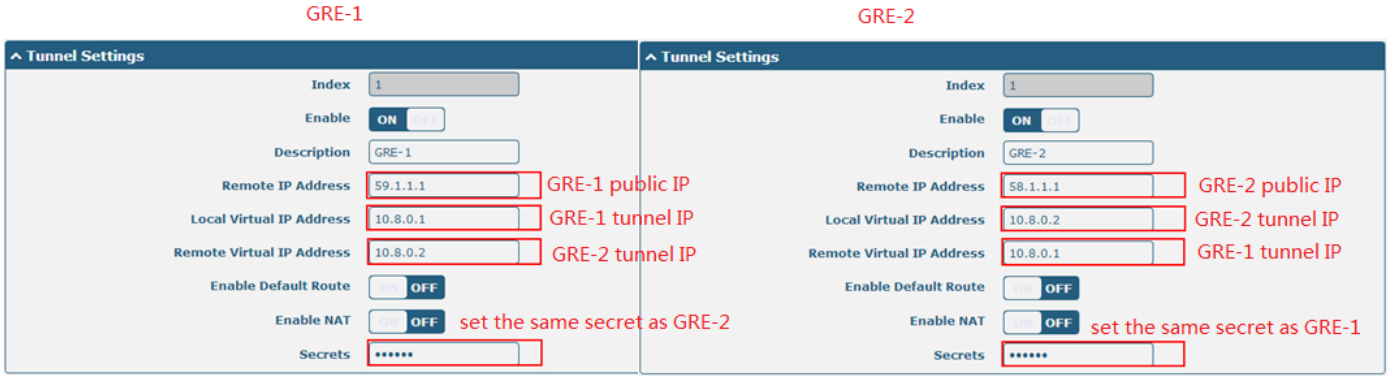
The modifications will take effect after click “Submit-->Save&Apply”.

GRE-2:



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

The comparison between point 1 and point 2 is as following picture:



Chapter 5 Introductions for CLI

5.1 What's CLI

The 4G INDUSTRIAL VPN command-line interface (CLI) is a software interface providing another way to set the parameters of equipment from the SSH or through a telnet network connection.

Route login:

Router login: admin

Password: admin

#

CLI commands:

? (***Note***: the '?' won't display on the page.)

!	Comments
add	Add a list entry of configuration
clear	Clear statistics
config	Configuration operation
debug	Output debug information to the console
del	Delete a list entry of configuration
exit	Exit from the CLI
help	Display an overview of the CLI syntax
ping	Send messages to network hosts
reboot	Halt and perform a cold restart
route	Static route modify dynamically, this setting will not be saved
set	Set system configuration
show	Show system configuration
status	Show running system information
tftpupdate	Update firmware using tftp
traceroute	Print the route packets trace to network host
urlupdate	Update firmware using http or ftp
ver	Show version of firmware

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.
Syntax error: The command is not completed	Command is not completed.
Tick space key+ Tab key	It can help you finish you command. Example: # config (tick Enter key) Syntax error: The command is not completed # config (tick space key+ Tab key) commit save_and_apply loaddefault
# config save_and_apply / #config commit	When you finish your setting, you should enter those commands to make your setting take effect on the device. ***Note:*** commit and save_and_apply plays the same role.

5.2.1 QuickStart with Configuration Examples

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

Example 1: Show current version

```
# status system
firmware_version = "1.0.0 (Rev 106)"
hardware_version = 1.1
kernel_version = 3.10.49
device_model = "4G INDUSTRIAL VPN"
serial_number = ""
uptime = "0 days, 01:09:49"
system_time = "Fri Mar  6 10:46:31 2015"
```

Example 2: Update firmware via tftp

```
# tftpupdate (space+?)
   firmware    New firmware
# tftpupdate firmware (space+?)
   String    Firmware name
# tftpupdate firmware 4G Industrial VPN-firmware-sysupgrade-unknown.bin host 192.168.100.99 //enter a new firmware name
Downloading
4G INDUSTRIAL VPN-firmware-s 100% |*******************************|    5018k    0:00:00 ETA
Flashing
Checking 100%
```

Decrypting 100%
Flashing 100%
Verifying 100%
Verfify Success
upgrade success //update success
config save_and_apply
OK // save and apply current configuration, make you configuration effect

Example 3: Set link-management

set
set
at_over_telnet AT Over Telnet
cellular Cellular
ddns Dynamic DNS
dhcp DHCP
dns DNS
ethernet Ethernet
event Event Management
firewall Firewall
gre GRE
ipsec IPSec
lan Local Area Network
link_management Link Management
ntp NTP
openvpn OpenVPN
pppoe PPPoE
reboot Automatic Reboot
CloudLink CloudLink
robustvpn RobustVPN
route Route
sms SMS
ssh SSH
syslog Syslog
system System
user_management User Management
vlan VLAN
vrrp VRRP
wan Ethernet WAN
set link_management
primary_link Primary Link
backup_link Backup Link
backup_mode Backup Mode
emergency_action Emergency Action
ping_enable Enable Ping Detection

```
   ping_primary_server        Primary Server
   ping_secondary_server    Secondary Server
   ping_interval                Ping Interval
   ping_retry_interval        Ping Retry Interval
   ping_timeout                  Ping Timeout
   ping_tries                     Max Ping Tries
# set link_management primary_link (space+?)
Enum    Primary Link (wwan1/wwan2/wan)
# set link_management primary_link wwan1                    //select “wwan1” as primary_link
OK                                                                    //setting succeed
…
# config save_and_apply
OK                                          // save and apply current configuration, make you configuration effect
```

Example 4: Set LAN IP address and DNS

```
# show lan all
ip = 192.168.20.1
netmask = 255.255.255.0
# set lan (space+?)
   ip                  IP Address
   netmask          Netmask
   multiple_ip    Multiple IP Address Settings
# set lan ip 192.168.100.49                    //set IP address for lan
OK                                                    //setting succeed
# set lan netmask 255.255.255.0
OK
# set dns (space+?)
   specify_dns       Use Specified DNS
   primary_dns       Primary DNS Server
   secondary_dns    Secondary DNS Server# set dns specify_dns
true    false
# set dns specify_dns false                    //set specify_dns
OK                                                    //setting succeed
# set dns primary_dns 58.1.1.254          //set primary_dns
OK                                                    //setting succeed
#
…
# config save_and_apply
OK                                          // save and apply current configuration, make you configuration effect
```

Example 5: CLI for setting Cellular (PRELIMINARY)

```
# show cellular all
sim {
        id = 1
        card = sim1
        link = wwan1
        phone_number = ""
        extra_at_cmd = ""
        auto_apn = true
        apn = internet
        username = ""
        password = ""
        dialup_number = *99***1#
        auth_type = auto
        redial_interval = 10
        max_connect_tries = 2
        lcp_echo_interval = 30
        lcp_echo_failure = 3
        dialup_mtu = 1500
        dialup_mru = 1500
        address_compress = true
        protocol_compress = true
        expert_options = ""
        data_traffic_limit = 0
        billing_day = 1
        network_type = auto
        band_select_type = all
        band_gsm_850 = false
        band_gsm_900 = false
        band_gsm_1800 = false
        band_gsm_1900 = false
        band_wcdma_850 = false
        band_wcdma_900 = false
        band_wcdma_1900 = false
        band_wcdma_2100 = false
        band_lte_800 = false
        band_lte_850 = false
        band_lte_900 = false
        band_lte_1800 = false
        band_lte_1900 = false
        band_lte_2100 = false
        band_lte_2600 = false
}
```

```
sim {
	id = 2
	card = sim2
	link = wwan2
	phone_number = ""
	extra_at_cmd = ""
	auto_apn = true
	apn = internet
	username = ""
	password = ""
	dialup_number = *99***1#
	auth_type = auto
	redial_interval = 10
	max_connect_tries = 2
	lcp_echo_interval = 30
	lcp_echo_failure = 3
	dialup_mtu = 1500
	dialup_mru = 1500
	address_compress = true
	protocol_compress = true
	expert_options = ""
	data_traffic_limit = 0
	billing_day = 1
	network_type = auto
	band_select_type = all
	band_gsm_850 = false
	band_gsm_900 = false
	band_gsm_1800 = false
	band_gsm_1900 = false
	band_wcdma_850 = false
	band_wcdma_900 = false
	band_wcdma_1900 = false
	band_wcdma_2100 = false
	band_lte_800 = false
	band_lte_850 = false
	band_lte_900 = false
	band_lte_1800 = false
	band_lte_1900 = false
	band_lte_2100 = false
	band_lte_2600 = false
}
switch_by_data_traffic = false
switch_by_roaming = false
home_operator_code = ""
```

```
# set
at_over_telnet    cellular          ddns              dhcp              dns
event             firewall          ipsec             lan               link_management
ntp               openvpn           reboot            route             serial_port
sms               snmp              syslog            system            user_management
vrrp
# set cellular
   sim                          Sim Settings
   switch_by_data_traffic    Enable Data Traffic Switch
   switch_by_roaming         Enable Roaming Switch
   home_operator_code        LAC of preferred SIM
# set cellular switch_by_data_traffic true                    //open cellular switch_by_data_traffic
OK                                                            //setting succeed
# set cellular switch_by_roaming false                        //close cellular switch_by_roaming false
OK                                                            // setting succeed
…
# config save_and_apply
OK                                    // save and apply current configuration, make you configuration effect
```

5.3 Commands Reference

commands	syntax	description
Debug	Debug *parameters*	Turn on or turn off debug function
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		

Note: Download the config.xml file from the configured web browser. The command format can refer to the config.xml file format.

Glossary

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

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

Abbreviations	Description
USSD	Unstructured Supplementary Service Data
VDC	Volts Direct current
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VSWR	Voltage Stationary Wave Ratio
WAN	Wide Area Network

Digicom S.p.A.
Italy - Via Alessandro Volta 39
21010 Cardano al Campo -VA
Tel +39/0331/702611 Fax +39/0331/263733
http://www.digicom.it